Thomas Joos

Microsoft Windows Server 2008 – Das Handbuch 2. Auflage

Thomas Joos

Microsoft Windows Server 2008 – Das Handbuch 2. Auflage

Thomas Joos: Microsoft Windows Server 2008 – Das Handbuch, 2. Auflage
Microsoft Press Deutschland, Konrad-Zuse-Str. 1, 85716 Unterschleißheim

15 14 13 12 11 10 9 8 7 6 5 4 3 2
10 09 08

ISBN 978-3-86645-130-8

Fachlektorat: Georg Weiherer, Münzenberg
Korrektorat: Jutta Alfes, Dorothee Klein, Siegen
Layout und Satz: Gerhard Alfes, mediaService, Siegen (www.media-service.tv)
Umschlaggestaltung: Hommer Design GmbH, Haar (www.HommerDesign.com)
Gesamtherstellung: Kösel, Krugzell (www.KoeselBuch.de)

Übersicht

Inhaltsverzeichnis

Vorwort

Mit Windows Server 2008 stellt Microsoft die neue Version seines Serverbetriebssystems zur Verfügung. Vor allem die Themen Sicherheit und Zuverlässigkeit sind mit der neuen Version verbessert worden. Es gibt neue Funktionen, um externe Mitarbeiter besser an das Unternehmen anzubinden. Beispiele hierfür sind die neuen Möglichkeiten der Terminaldienste, Anwendungen ohne den ganzen Desktop zur Verfügung zu stellen, oder eine Verbindung per HTTPS zum Terminalserver aufzubauen, aber auch den neuen Terminaldienste-Webzugriff. Auch der neue Netzwerkzugriffschutz, der Netzwerke vor unsicheren Arbeitsstationen sichern soll, und die BitLocker-Funktion, mit der Serverfestplatten verschlüsselt werden, sind Beispiele für Verbesserungen. Die neuen Internetinformationsdienste sind in der Version 7.0 noch sicherer und zuverlässiger. Im Bereich Active Directory gibt es eine neue Art Domänencontroller, den schreibgeschützten Domänencontroller, mehr Gruppenrichtlinien und wichtige Detailverbesserungen wie beispielsweise die Möglichkeit, Active Directory zur Wartung als Dienst zu beenden. Die Verwaltungswerkzeuge wurden überarbeitet und mit dem Server-Manager wird ein zentrales Verwaltungswerkzeug zur Verfügung gestellt.

Mit der neuen Server Core Edition kann Windows Server 2008 quasi ohne grafische Oberfläche installiert werden, was die Sicherheit erhöht und die Leistung verbessert. Cluster können jetzt mit Windows Server 2008 einfacher erstellt werden und sind ebenfalls stabiler als in den Vorgängerversionen. Mit dem neuen TCP/IP-Stack wird jetzt auch offiziell IPv6 unterstützt, was an vielen Serverdiensten wie DNS oder DHCP produktiv verwendet werden kann. Die Installation von USB-Sticks kann genauso über Gruppenrichtlinien verhindert werden wie Arbeitsstationen mit Windows Vista automatisch in den Energiesparmodus versetzt werden können.

In diesem Buch zeigen wir Ihnen alle Neuerungen im Praxiseinsatz auf und gehen auf alle Themen ein, die bei der Verwaltung eines Netzwerks unter Windows Server 2008 wichtig sind. Windows Server 2008 kann problemlos parallel zu Windows Server 2003 eingesetzt werden und bietet auch in diesem Fall weitere produktive Vorteile. Die automatisierte Installation des Servers und auch der Arbeitsstationen ist mit neuen Mitteln deutlich einfacher als unter Windows Server 2003. Neben allen diesen Neuerungen spielen Detailverbesserungen in der Bedienung eine wichtige Rolle. Auch auf diese Bereiche gehen wir in diesem Buch ein.

Dieses Buch soll Ihnen das notwendige Wissen zur Verwaltung von Windows Server 2008 vermitteln, aber auch als Nachschlagewerk dienen, wenn Fragen bei einzelnen Themen bestehen.

Kapitel 1

Einführung

In diesem Kapitel:

Mit Windows Server 2008 liefert Microsoft eine neue Version seines Serverbetriebssystem aus. In diesem Buch zeigen wir Ihnen, welche Neuerungen in Windows Server 2008 im Vergleich zum Vorgänger Windows Server 2003 (SP2 und R2) enthalten sind und wie Windows Server 2008 produktiv im Netzwerk eingesetzt wird. Windows Server 2008 enthält zahlreiche neue Funktionen, und auch an der Sicherheit hat Microsoft einiges optimiert. Windows Server 2008 und Windows Vista basieren auf der gleichen Codebasis. Im Gegensatz zu seinen Vorgängern besteht Windows Server 2008 aus einem sprachunabhängigen Paket und ist nicht komplett lokalisiert. Dadurch besteht die Möglichkeit, auch ausländische Versionen zu kaufen und diese durch ein deutsches Sprachpaket zu lokalisieren. Durch die einheitliche Basis des Kernels werden zukünftig Sicherheitspatches deutlich schneller erscheinen können, da auch diese nicht erst lokalisiert werden müssen. Windows Server 2008 bietet vor allem Verbesserungen im Bereich der Sicherheit und der Installation von Serverfunktionen. Das System wird deutlich flexibler und einfacher verwaltbar, ohne dabei auf notwendige Sicherheitsfunktionen zu verzichten. Windows Server 2008 ist bereits nach der Installation gehärtet und abgesichert, der Sicherheitskonfigurationsassistent (Security Configuration Wizard, SCW) wird nicht mehr benötigt. Windows Vista und auch Windows Server 2008 wurden im Rahmen der neuen Secure Development Lifecycle (SDLC) entwickelt. Bei SDLC handelt es sich nicht um ein Feature, sondern um eine Firmenphilosophie von Microsoft. Die bisherigen Windows-Versionen wurden hauptsächlich so entwickelt, dass diese funktional sind und ansprechend aussehen. Die Sicherheit spielte meist nur eine untergeordnete Rolle. Bei der Entwicklung von Windows Vista und Windows Server 2008 hat Microsoft Wert darauf gelegt, dass die Entwickler regelmäßig geschult wurden, wie man Funktionen sicher integrieren kann. Alle neuen Funktionen wurden bereits in der Entwicklung auf Angriffsmöglichkeiten hin getestet und bezüglich der Sicherheit optimiert. Die einzelnen Funktionen und die Sicherheit wurden regelmäßig überprüft und zertifiziert. In diesem Kapitel zeigen wir Ihnen zusammenfassend die Neuerungen von Windows Server 2008. In den weiteren Kapiteln dieses Buches erfahren Sie, wie Sie mit den Funktionen umgehen, um Windows Server 2008 optimal im Unternehmen einsetzen zu können.

Die verschiedenen Editionen von Windows Server 2008

Wie bereits seine Vorgänger ist Windows Server 2008 in verschiedenen Editionen erhältlich. Abhängig von der Edition werden verschiedene Rollen und Funktionen unterstützt. Die Installation von Windows Server 2008 kann jetzt, wie bei Exchange Server 2007 auch, rollenbasiert erfolgen (siehe Kapitel 4). Die neuen Editionen von Windows Server 2008 orientieren sich an Windows Server 2003. Für die Installation wird mindestens ein 1 GHz-Prozessor und 512 MB Arbeitsspeicher sowie mindestens 12 GB freier Festplattenplatz empfohlen. Allerdings sollten nur in Testumgebungen solche kleinen Festplatten verwendet werden. Auf produktiven Servern empfiehlt Microsoft mindestens 40 bis 80 GB.

HINWEIS Windows Server 2008 Standard Edition, Windows Server 2008 Enterprise Edition, Windows Server 2008 Datacenter Edition und Windows Server 2008 für Itanium-basierte Systeme gibt es auch in 64-Bit-Versionen.

Folgende Editionen von Windows Server 2008 gibt es:

- **Windows Server 2008 Standard Edition** Diese Edition ist vor allem für mittelständische Unternehmen gedacht und unterstützt die meisten Funktionen und Rollen von Windows Server 2008. Auch die neue Core-Server-Rolle ist in dieser Edition bereits integriert. Die Standard Edition unterstützt maximal 4 GB Arbeitsspeicher in der 32-Bit-Version und 32 GB in der 64-Bit-Version.
- **Windows Server 2008 Enterprise Edition** Wie auch unter Windows Server 2003 dient diese Funktion zur Unterstützung größerer Unternehmen. Diese Version unterstützt alle Rollen und Funktionen und ist, im Gegensatz zur Standard Edition, clusterfähig und unterstützt die Active Directory Federation Services. Außerdem unterstützt diese Edition mehr Arbeitsspeicher. Die Enterprise Edition unterstützt maximal 64 GB Arbeitsspeicher in der 32-Bit-Version und 2 TB in der 64-Bit-Version.
- **Windows Server 2008 Datacenter Edition** Diese Version ist für sehr große Rechenzentren gedacht und wird nur zusammen mit entsprechender Hardware verkauft. Die Funktionen sind mit der Enterprise Edition identisch, es werden aber mehr Arbeitsspeicher, mehr Prozessoren und eine optimalere Virtualisierung geboten. Die Datacenter Edition unterstützt maximal 64 GB Arbeitsspeicher in der 32-Bit-Version und 2 TB in der 64-Bit-Version.
- **Windows Web Server 2008** Dieser Server dient ausschließlich dem Aufbau von Webserver-Applikationen und -Infrastrukturen. Der Windows Web Server 2008 unterstützt im Gegensatz zu den anderen Editionen keine Core-Server-Installation (siehe Kapitel 2). Als Serverrollen wird nur der Webserver und der Anwendungsserver unterstützt, die anderen Rollen sind nicht aktivierbar.
- **Windows Server 2008 für Itanium-basierte Systeme** Diese Version unterstützt die 64-Bit Intel Itanium-Prozessoren. Der Funktionsumfang ist mit dem Windows Webserver 2008 identisch, andere Rollen werden nicht unterstützt. Die Itanium-Edition unterstützt maximal 2 TB Arbeitsspeicher. Für Windows Server 2008 für Itanium-basierte Systeme ist ein Intel Itanium 2-Prozessor erforderlich.

Außerdem gibt es die verschiedenen Versionen mit und ohne Hyper-V. Bei Hyper-V handelt es sich um die neue Virtualisierungstechnologie von Windows Server 2008, die in Kapitel 25 noch etwas ausführlicher erläutert wird.

Neue Oberfläche in Windows Server 2008

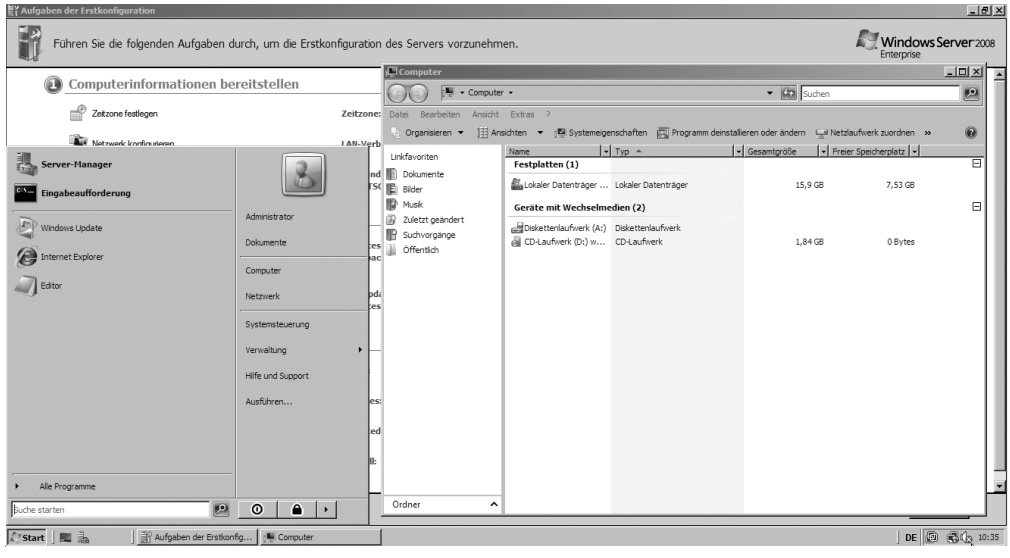
Das Erste, was nach der Installation von Windows Server 2008 auffällt, ist die geänderte Oberfläche für die Verwaltung. Windows Vista und Windows Server 2008 haben eine fast identische grafische Oberfläche. Auch die Bedienung der beiden Betriebssysteme ist nahezu identisch. Auffällig nach dem Start (siehe Kapitel 2) ist der neue Server-Manager, der automatisch nach dem Hochfahren des Betriebssystems gestartet wird (Abbildung 1.3). Die Ansicht des Windows-Explorers wurde ebenfalls angepasst und auch die Bedienung wurde optimiert (Abbildung 1.1). Zusätzlich wurde auch das Startmenü optimiert und erleichtert so die Navigation und Verwaltung.

Der neue Windows-Explorer in Windows Server 2008

Auch wenn es sich beim Windows-Explorer nicht um die wichtigste Funktion des Servers handelt, gehen wir zunächst kurz auf dessen neue Oberfläche ein. Diese wird dazu benötigt, Installationsdateien zu kopieren und Daten zu sichern. Daher sollte vor dem Umgang mit den Serverrollen erst der Umgang mit der Oberfläche beherrscht werden. Wer bereits Windows Vista einsetzt, muss sich nicht umgewöhnen, da die Oberflächen der beiden Betriebssysteme sehr ähnlich sind.

Der Windows-Explorer zeigt in Windows Server 2008 deutlich mehr Informationen an, und auch die Suchfunktionen wurden stark verbessert. Für die meisten Dateitypen werden Vorschaufenster angezeigt, deren Größe und Aussehen angepasst werden können. Das Explorerfenster listet auf der linken Seite zusätzliche Favoriten auf, mit denen der Administrator schnell zu den Ordnern wechseln kann, die er am häufigsten verwendet, zum Beispiel die Systemverzeichnisse oder Archivordner mit Installationsdateien von Programmen. Die übliche Ordnerstruktur des Windows-Explorers wurde darunter angeordnet und ist von der Ansicht ebenfalls angepasst worden. Haben Sie sich etwas mit der neuen Bedienung auseinandergesetzt, werden Sie sicherlich auf diese Funktionen nicht mehr verzichten wollen. Viele Tätigkeiten lassen sich intuitiv durchführen, und es ist nicht mehr notwendig, sich durch verschiedene Menüs zu hangeln, um zum Beispiel eine Datei zu kopieren oder Einstellungen vorzunehmen. Im Rahmen der Weiterentwicklung des Windows-Explorers wurde auch die Suchfunktion im Betriebssystem deutlich erweitert. Windows Vista und Windows Server 2008 arbeiten bei der Suche auch im Netzwerk Hand in Hand (siehe Kapitel 24). Die Suche ist direkt über das Startmenü erreichbar und kann beliebig konfiguriert werden. Vor allem die neue Suche ist für Unternehmenskunden ein erheblicher Vorteil. In Anwendungen, dem Startmenü, dem Windows-Explorer und in der Systemsteuerung steht die Suche zur Verfügung. Da auch die Anzahl der Programme in der Systemsteuerung stark erweitert wurde, lassen sich spezielle Einstellungsmöglichkeiten in der Suche schneller finden, als über das Klicken durch die verschiedenen Menüs.

Abbildg. 1.1 Die Benutzeroberfläche wurde in Windows Server 2008 komplett überarbeitet

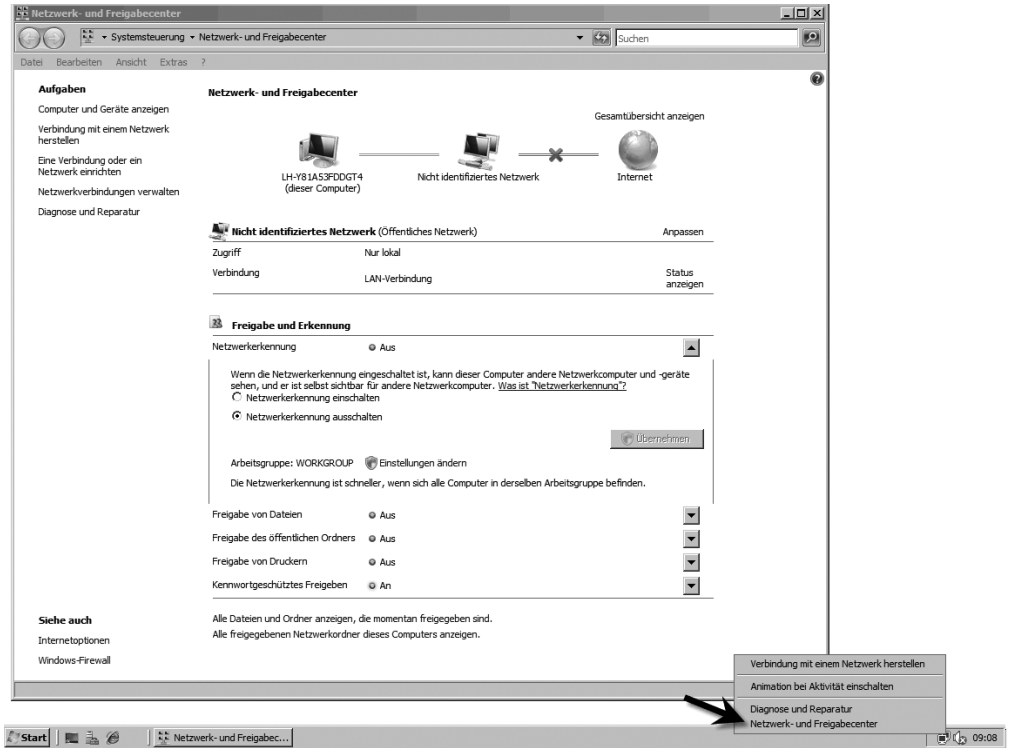


Die Anzeige des Suchergebnisses in Windows Server 2008 wurde ebenfalls deutlich überarbeitet und zeigt die Suchergebnisse in einem Explorer-Fenster an, unabhängig davon wo die Speicherorte der Dateien sind. Die Suche wird im Windows-Explorer standardmäßig auf den aktuellen Ordner fokussiert. Suchabfragen können gespeichert werden und stehen durch diese Funktion als virtuelle Ordner zur Verfügung. Die virtuellen Ordner in Windows Server 2008 sind keine statischen Verzeichnisse auf dem Dateisystem, sondern enthalten verschiedene Filter, die nach Schlüsselwörtern unterteilt sind. So kann zum Beispiel ein virtueller Ordner erstellt werden, der als Filter alle Dateien enthält, für die als Besitzer der Benutzer *Administrator* angegeben ist. Der virtuelle Ordner sammelt dann auf dem kompletten Server alle Dateien zusammen, deren Besitzer der Administrator ist und zeigt diese an.

Netzwerk- und Freigabecenter – Optimale Verwaltung des Netzwerkes

Die Konfiguration und Verwaltung von Netzwerkfunktionen wurden in 2008 ebenfalls verbessert (siehe Kapitel 7). Die Konfiguration der Netzwerkfunktionen in Windows Server 2008 ist in das neue *Netzwerk- und Freigabecenter* integriert. Alle netzwerkrelevanten Einstellungen können in diesem Center verwaltet werden (Abbildung 1.2). Sie erreichen dieses am besten über die Systemsteuerung oder durch einen Klick mit der rechten Maustaste auf das Netzwerksymbol unten rechts im Infobereich der Taskleiste. Im *Netzwerk und Freigabecenter* kann auch eine detaillierte Karte des Netzwerks angezeigt werden und Sie erkennen, an welcher Position des Netzwerkes sich Ihr Server befindet. Windows Vista-Arbeitsstationen werden automatisch angezeigt, auf Windows XP-Rechnern muss zur Anzeige erst ein Patch installiert werden. Dieser wird auf der Seite http://go.microsoft.com/fwlink/?LinkId=70582 zum Download angeboten. Es gibt zahlreiche neue Assistenten, um die Konfiguration der verschiedenen Netzwerkeinstellungen zu optimieren und zu konfigurieren. Die Konfiguration der Netzwerkverbindungen finden Sie ebenfalls im Netzwerk- und Freigabecenter. Sie erreichen die Eigenschaften der Netzwerkverbindungen aber am schnellsten über *Start/Ausführen/ncpa.cpl*. Mehr zu diesem Thema und ausführliche Anleitungen zur Anbindung von Windows Server 2008 an ein Netzwerk finden Sie in Kapitel 7.

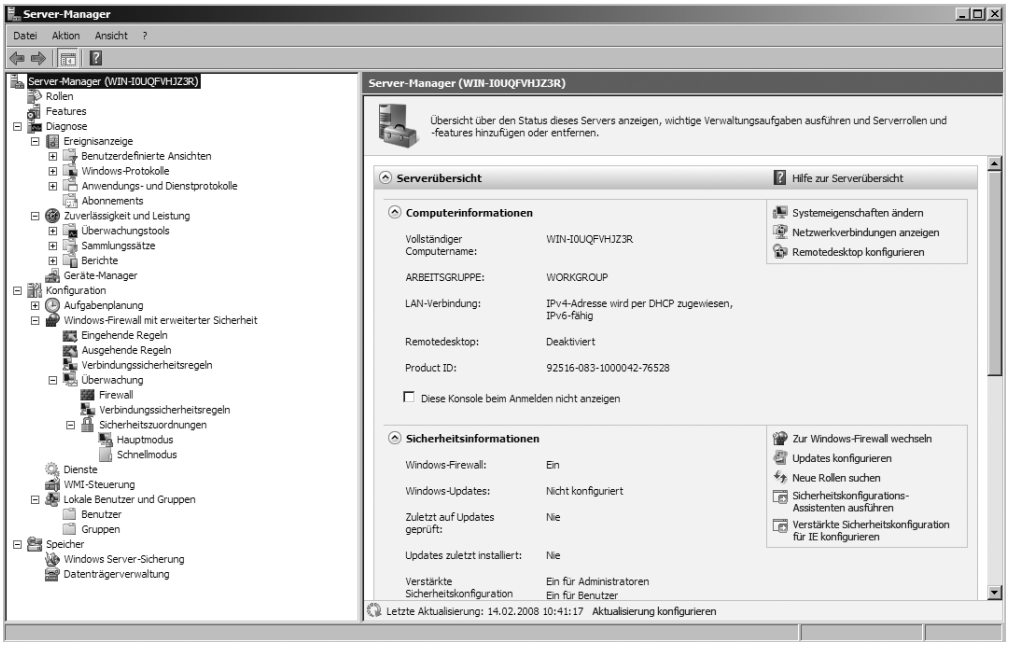
Abbildg. 1.2 Das Netzwerk- und Freigabecenter in Windows Server 2008



Der neue Server-Manager

Der Server-Manager ist vielen Administratoren vom Namen her noch aus Windows NT-Zeiten bekannt, hatte aber in dieser Version noch nicht die vielfältigen Möglichkeiten die das Programm unter Windows Server 2008 bietet. Mit dieser Verwaltungsoberfläche, die Sie auch in der Schnellstartleiste finden, können Sie die Funktionen von Windows Server 2008 zentral verwalten. Sie können den Server-Manager auch über *Start/Ausführen/servermanager.msc* starten. Alle wichtigen Funktionen eines Servers finden Sie an dieser Stelle. Die Bedienung der Oberfläche erinnert etwas an die Serververwaltungskonsole in Small Business Server 2003 R2, die ebenfalls alle relevanten Verwaltungstasks in einer Verwaltungsoberfläche bündelt. Installieren Sie zusätzliche Rollen oder Features werden diese automatisch in den Server-Manager integriert. Zur Verwaltung eines Windows Server 2008-Netzwerkes wird daher fast kein anderes Tool mehr außer dem Server-Manager benötigt. Es ist jedoch auch weiterhin möglich, eigene Managementkonsolen zu bauen.

Abbildg. 1.3 Der neue Server-Manager in Windows Server 2008

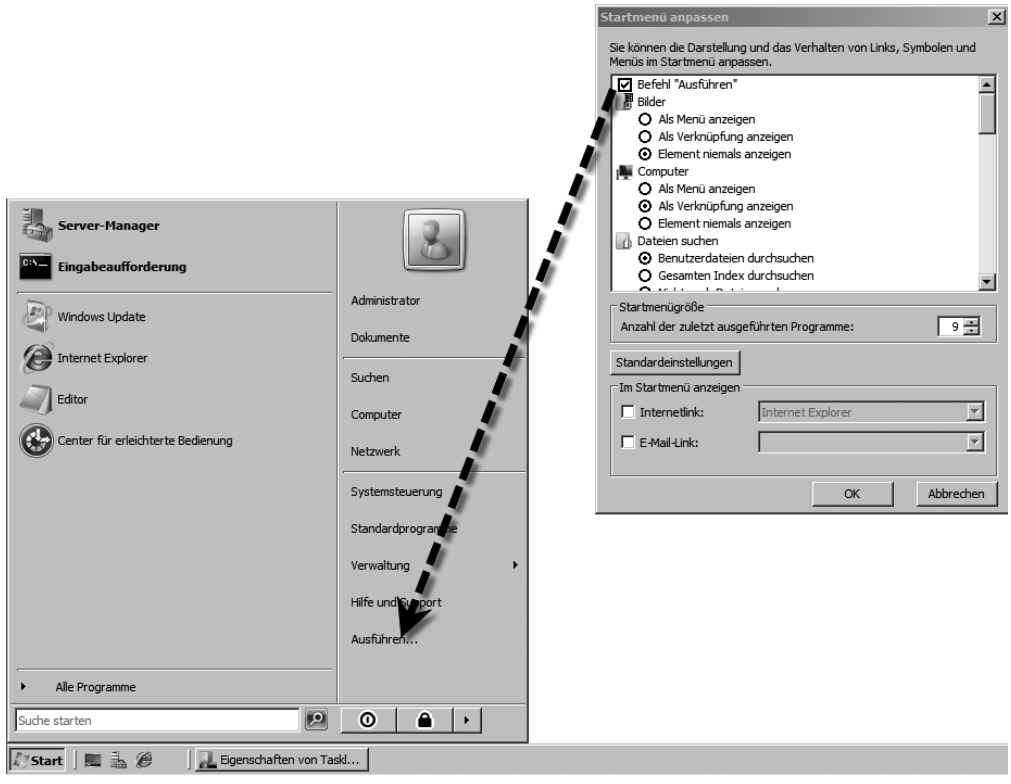


Der neue Server-Manager ersetzt nicht die verschiedenen Snap-Ins für die Verwaltung des Servers, sondern dient hauptsächlich der zusätzlichen zentralen Konfiguration und Überwachung des Servers. Auch zusätzliche Serverrollen- oder Features werden über den Server-Manager konfiguriert oder installiert. Fügen Sie neue Windows-Komponenten hinzu, findet dies nicht mehr über die Systemsteuerung statt, sondern über den neuen Server-Manager. Es gibt zwar noch den entsprechenden Link in der Systemsteuerung. Dieser stellt jedoch nur eine Verknüpfung zum Server-Manager dar. Installieren Sie über den Server-Manager zusätzliche Features, werden diese bereits standardmäßig mit maximaler Sicherheit installiert. Der Sicherheitskonfigurations-Assistent (Security Configuration Wizard, SCW) von Windows Server 2003 wird nicht mehr zwingend benötigt. Mit dem neuen Tool wird die Verwaltung von Windows-Servern wesentlich verbessert. Der Server-Manager hat hauptsächlich folgende Aufgaben:

- Installation und Konfiguration der verschiedenen Serverrollen und -funktionen
- Verwaltung der lokalen Benutzerkonten
- Dienste starten und stoppen
- Serverüberwachung und Kontrolle der Ereignisanzeigen

Auf der Internetseite *http://go.microsoft.com/fwlink/?LinkId=48541* finden Sie weitere Infos (in englischer Sprache) zu den einzelnen Aufgaben des Server-Managers. Nur Administratoren haben Zugriff auf diese Konsole.

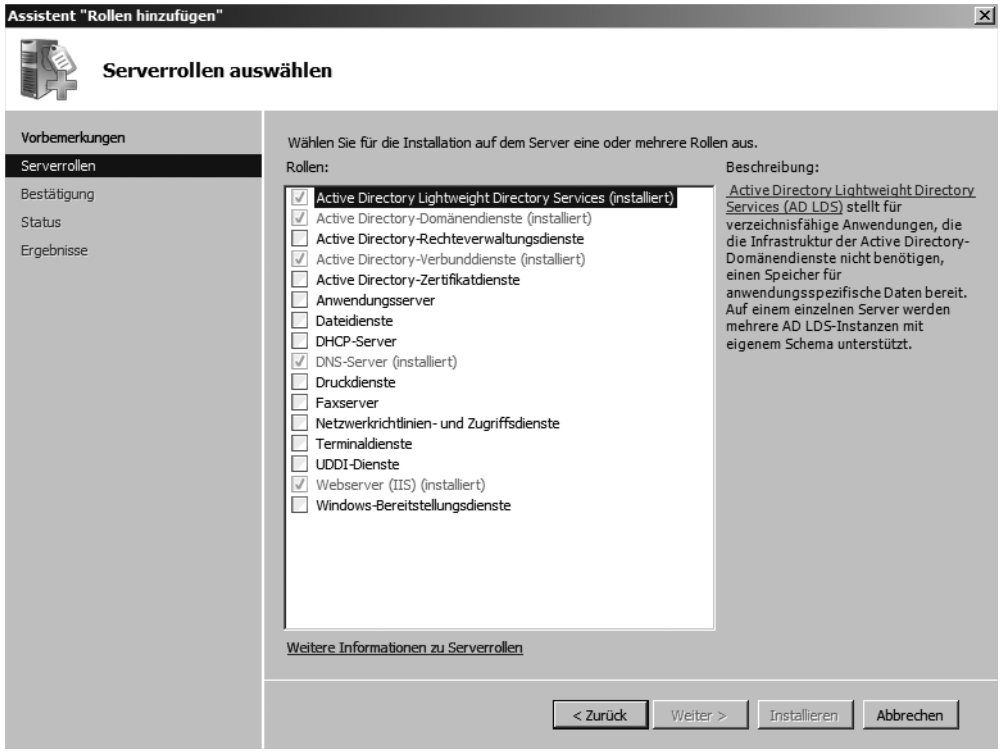
Abbildg. 1.4 Aktivieren des Ausführen-Menüs in der Startleiste von Windows Server 2008



Serverrollen und -Funktionen

Microsoft hat die verschiedenen Rollen eines Windows-Servers in Serverrollen aufgeteilt, die einzeln oder zusammen auf einem Server installiert werden können (siehe Kapitel 3). Features erweitern die Serverrollen um zusätzliche Funktionen. Serverrollen definieren die primäre Funktion eines Servers, zum Beispiel Domänencontroller oder Dateiserver, Features erweitern diese Rollen. Auf einem Windows-Server werden dadurch nur noch die Funktionen installiert, die auch benötigt werden, alle anderen Serverrollen werden aus Sicherheitsgründen nicht installiert. Dies hat den Vorteil, dass durch diese Minimalinstallationen mögliche Angriffe auf nicht benötige Funktionen oder Rollen unterbunden werden.

Abbildg. 1.5 Zusätzliche Installation von Serverrollen auf einem Server

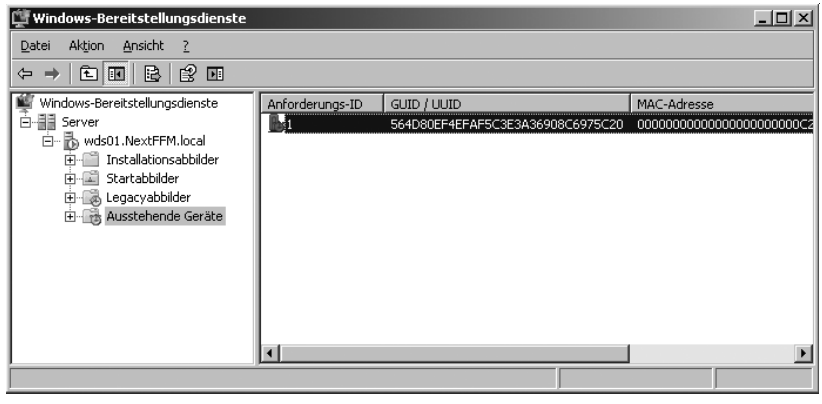


Windows-Bereitstellungsdienste

Windows Vista und Windows Server 2008 können nicht über die Remote Installation Service (RIS)-Technologie von Windows Server 2000/2003 installiert werden. Der Nachfolger von RIS sind die Windows-Bereitstellungsdienste (Windows Deployment Services, WDS), die auch unter Windows Server 2003 nachträglich installiert werden können (siehe Kapitel 16). Verwechseln Sie die Windows Deployment Services (WDS) nicht mit den Automated Deployment Services (ADS) für Windows Server 2003. Automated Deployment Services unterstützen Sie bei der Verteilung von Windows Server-Betriebssystemen in großen Umgebungen. Mit den WDS können auch Windows Server 2003, XP und 2000 installiert werden, vor allem aber Windows Vista und Windows Server 2008. Die Installation von Windows Vista und auch Windows Server 2008 findet imagebasiert über das neue Windows-Imaging-Format (WIM) statt und wird so deutlich schneller abgeschlossen, als die Installation von Windows Server 2003 oder Windows XP. Die WDS können kostenlos über das Windows Automated Installation Kit (WAIK) auf einem Windows Server 2003 installiert werden. In Windows Server 2008 werden die WDS bereits als Serverrolle implementiert. Da RIS keine WIM-Images lesen kann, besteht keine Möglichkeit, Windows Vista oder Windows Server 2008 über RIS zu verteilen. Eine Verteilung über das Netzwerk per Booten auf PXE-Basis (Preboot Execution Environment) kann nur noch über die WDS erfolgen. WDS ist ebenfalls für den neuen System Center Configuration Manager 2007, den Nachfolger des Systems Management Server 2003 optimiert. In den WDS lassen sich detaillierte Einstellungen über die PXE-Funktionalität vornehmen (siehe Kapitel 16).

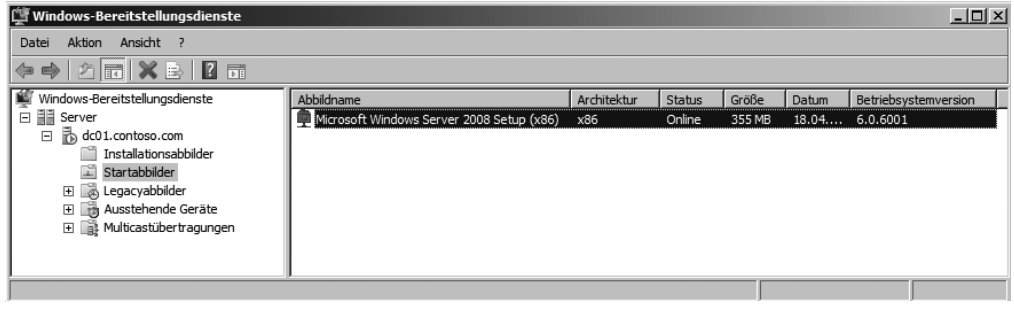
WDS unterstützt Active Directory und es können Einstellungen vorgenommen werden, wie die installierten Clients bezeichnet werden sollen. In die WDS können direkt WIM-Images integriert werden. Auch Windows PE (Preinstallation Environment) lässt sich über WDS verteilen. Mehr dazu erfahren Sie im Kapitel 16. Dadurch können Clients, die über das Netzwerk mit PXE booten, Windows PE starten und über dieses Windows PE dann Windows Vista oder Windows Server 2008 installieren. Auf dem Client kann die Auswahl getroffen werden, welches Image vom WDS-Server gezogen werden soll und wo dieses installiert wird. WDS kann auch 64-Bit-Betriebssysteme verteilen. Durch die effiziente grafische Oberfläche der WDS können in den Eigenschaften von WIM-Images Dateien integriert oder auch andere Antwortdateien zugewiesen werden. Sie können in den Einstellungen von WDS festlegen, dass die Images entweder vollkommen automatisiert installiert werden, oder dass einzelnen Anwendern die Möglichkeit gegeben wird, das Image selbst auszuwählen. Wenn der Anwender sein Image selbst auswählen darf, sieht die Installation über WDS aus wie die Installation von Windows Vista mit der DVD, mit dem Unterschied, das weniger Auswahlmöglichkeiten existieren. Der Anwender kann beim Booten selbst auswählen, welches WIM-Image er auf seinem Computer installieren will.

Abbildg. 1.6 Verwaltung der WDS auf Windows Server 2008



Damit Sie PCs oder Server über die WDS installieren können, muss im Netzwerk neben dem ohnehin notwendigen DNS-Server auch ein DHCP-Server eingerichtet sein. Auf diesem müssen ein aktivierter Bereich (Scope) und entsprechende Optionen erstellt werden. Fehler aus RIS wurden behoben, wie zum Beispiel das instabile Verhalten bei großen Installationen.

Abbildg. 1.7 Windows Server 2008 und Windows Vista können über die Windows-Bereitstellungsdienste im Netzwerk verteilt werden



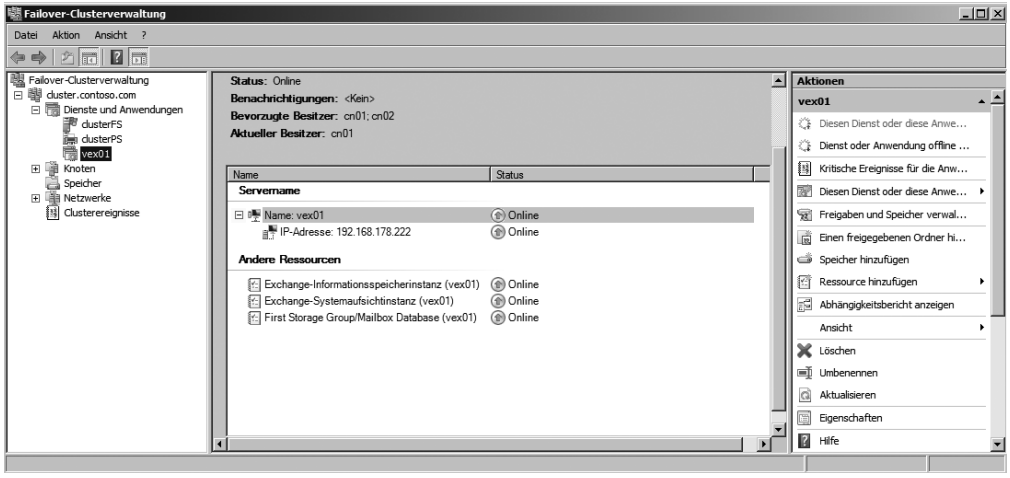
Ein Clientcomputer mit PXE wird im Netzwerk gestartet. Nach dem Laden des BIOS sendet das PXE-ROM auf der Netzwerkkarte eine Netzwerk-Dienstanforderung an den nächstgelegenen DHCP-Server. Mit der Anforderung sendet der Client seine GUID (Globally Unique Identifier). Der DHCP-Server erteilt dem Client eine IP-Lease mit Optionen für DNS (006), Domäne (015) und PXE-Server (060). Als Nächstes startet das Bootimage mit Windows PE, das in den Hauptspeicher geladen wird. Über einen Eintrag in der Antwortdatei wird die Festplatte angepasst. Das Setup führt die in der Antwortdatei enthaltene Anmeldung an den WDS-Server aus. Existiert dieser Eintrag nicht, wird um eine Authentifizierung gebeten. Soll eine unbeaufsichtigte Installation durchgeführt werden, darf immer nur ein Image in der Image-Gruppe existieren. Wurde die Antwortdatei mit Informationen, wie Installations-Key, Sprachversion und Domänenkonto korrekt konfiguriert, läuft die Installation vollkommen automatisch ab. Das Befehlszeilentool *wdsutil.exe* bietet eine erweiterte Funktionalität. Außerdem kann mit dem Tool auch ein bestehendes RIPREP-Image zu einem WIM-Image konvertiert werden. Der Umgang mit dem WDS ist recht einfach. Zur Image-Verteilung von Windows Vista und Windows Server 2008 stehen zwei Möglichkeiten zur Verfügung:

- Die Verwendung eines kompletten Image, bei dem keine Anpassungen mehr durchgeführt werden.
- Die Verwendung eines Image, welches noch über eine Antwortdatei angepasst werden muss (siehe Kapitel 16). Ein komplettes Vista-Image kann über die Tools ImageX oder Sysprep erstellt werden. Diese kompletten Images können dann auch weitere Applikationen beinhalten.

Neues Failover-Clustering

Wollen Kunden ein ausfallsicheres Server-System einführen, ist der Einsatz eines Failover-Clusters oft der beste Weg (siehe auch Kapitel 19). Mit Windows Server 2008 hat Microsoft die Clustertechnologie des Betriebssystems weiter verbessert, die Installation erleichtert und die Stabilität erhöht. Der Microsoft Product Support Service (PSS) und die unabhängige Gartner-Group haben festgestellt, dass die meisten Probleme in Clusterumgebungen durch Fehler in der Konfiguration oder der Verwaltung verursacht werden. Aus diesem Grund scheuen sich viele Unternehmen, einen Cluster einzusetzen, aus Furcht, dass der Aufwand für die Verwaltung und die Kosten der Installation zu hoch sind. Häufige Probleme in Clusterkonfigurationen sind eine fehlerhafte Verkabelung, unpassende oder fehlende Treiber und Hotfixes und natürlich falsche Einstellungen. Aus diesem Grund führt Microsoft mit Windows Server 2008 das *Cluster Validation Tool* ein. Mit diesem Tool können Clusterverwalter, ähnlich wie beim Exchange Best Practices Analyzer (ExBPA), einen Cluster vor der Installation effizient mit einem von Microsoft zusammengestellten Regelwerk für die korrekte Konfiguration überprüfen. Mit diesem Tool können Fehler in der Hardware und der Konfiguration bereits aufgedeckt werden, bevor der Cluster in Produktion geht. Auch bereits erstellte Cluster können mit diesem Tool überprüft werden, sodass Microsoft-Partner auch Kunden, die bereits einen Cluster einsetzen oder planen, ihre Cluster auf Windows Server 2008 zu migrieren, effizient beraten können, ob die Hardware und Konfiguration kompatibel und vor allem stabil ist. Das Tool führt verschiedene Tests durch, um den Stand des Betriebssystems, der installierten Patches, der Systemkonfiguration, der Netzwerkeinstellungen und -verbindungen sowie der Datenträger zu überprüfen.

Abbildg. 1.8 Failover-Clusterverwaltung in Windows Server 2008 im Betrieb mit Exchange Server 2007 SP1



Auch die Erstellung eines Clusters wird mit Windows Server 2008 extrem vereinfacht. Microsoft hat dazu die grafische Oberfläche zur Clusterverwaltung überarbeitet und optimiert (Abbildung 1.8). Mit Windows Server 2008 ist es möglich, einen Cluster skriptbasiert und vollständig automatisiert zu installieren. Ein Cluster wird unter Windows Server 2008 in einem Schritt erstellt. Es ist nicht mehr notwendig, erst einen Knoten, dann die restlichen zu installieren. Früher mussten die Cluster-Knoten dem Cluster einzeln zugewiesen werden. Unter Windows Server 2008 können Sie mehrere Server gleichzeitig in einen Cluster integrieren. Dies hat den Vorteil, dass die Konsistenz und die Stabilität der einzelnen Clusterknoten bereits bei der Installation sichergestellt werden kann und keine komplexen Installationsprozesse mehr ablaufen müssen. Auch die Assistenten zur Erstellung eines Clusters wurden vereinfacht und verbessert. Mit diesen Assistenten können Clusterressourcen von Clustern unter Windows Server 2003 auch zu Windows Server 2008 migriert werden. Auch auf diesen Sachverhalt gehen wir in Kapitel 19 ein.

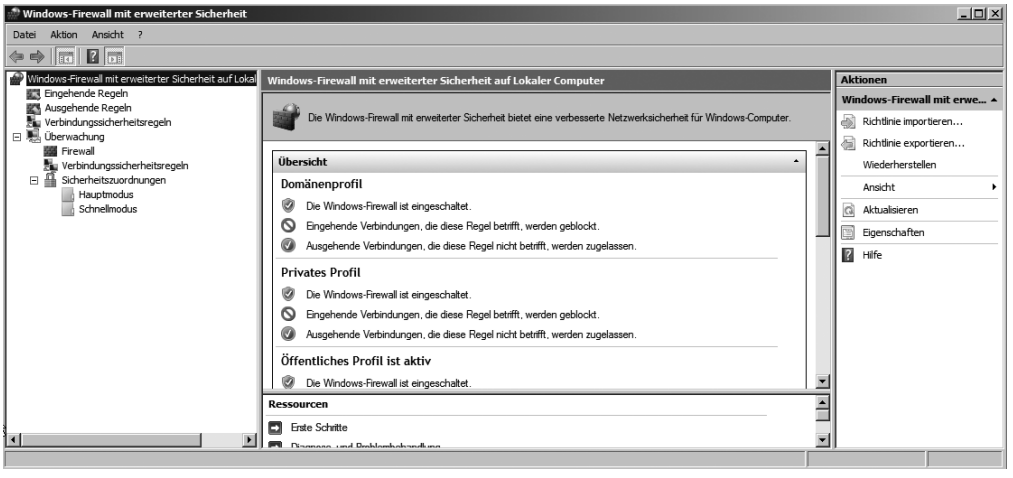
Windows-Firewall mit erweiterter Sicherheit

Die neue Firewall mit erweiterter Sicherheit ist Bestandteil sowohl von Windows Server 2008 als auch von Windows Vista. Die wesentlichen Neuerungen sind, dass die Firewall jetzt auch ausgehenden Datenverkehr überprüfen kann und dass die Verwaltung von IPSec-Richtlinien jetzt in die Verwaltung der Firewall integriert worden ist. Die Verwaltungsoberfläche der neuen Firewall können Sie über *Start/Ausführen/wf.msc* starten. Die Firewall für erweiterte Sicherheit ersetzt die verschiedenen Verwaltungskonsolen für IPSec-Richtlinien (Abbildung 1.9).

HINWEIS Im Gegensatz zu Windows Server 2003 ist die Firewall in Windows Server 2008 standardmäßig nach der Installation bereits aktiviert. Administratoren müssen daher bei älteren Anwendungen darauf achten, dass entsprechende Firewallregeln erstellt werden, um die Kommunikation mit dem Netzwerk zu erlauben. Aktualisieren Sie einen Server mit Windows Server 2003 auf Windows Server 2008, bleibt die Firewall deaktiviert. Nur wenn Sie die Firewall unter Windows Server 2003, zum Beispiel mit dem Security Configuration Wizard (SCW), aktiviert haben, wird diese bei der Installation ebenfalls aktiviert. Microsoft empfiehlt jedoch, die Firewall

unter Windows Server 2008 in jedem Fall zu aktivieren. Installieren Sie eine der Standardfunktionen von Windows Server 2008, wie zum Beispiel IIS 7.0 oder Dateiserver, werden entsprechende Regeln automatisch erstellt und Ports freigeschaltet.

Abbildg. 1.9 Die Verwaltung der neuen Windows-Firewall mit erweiterter Sicherheit



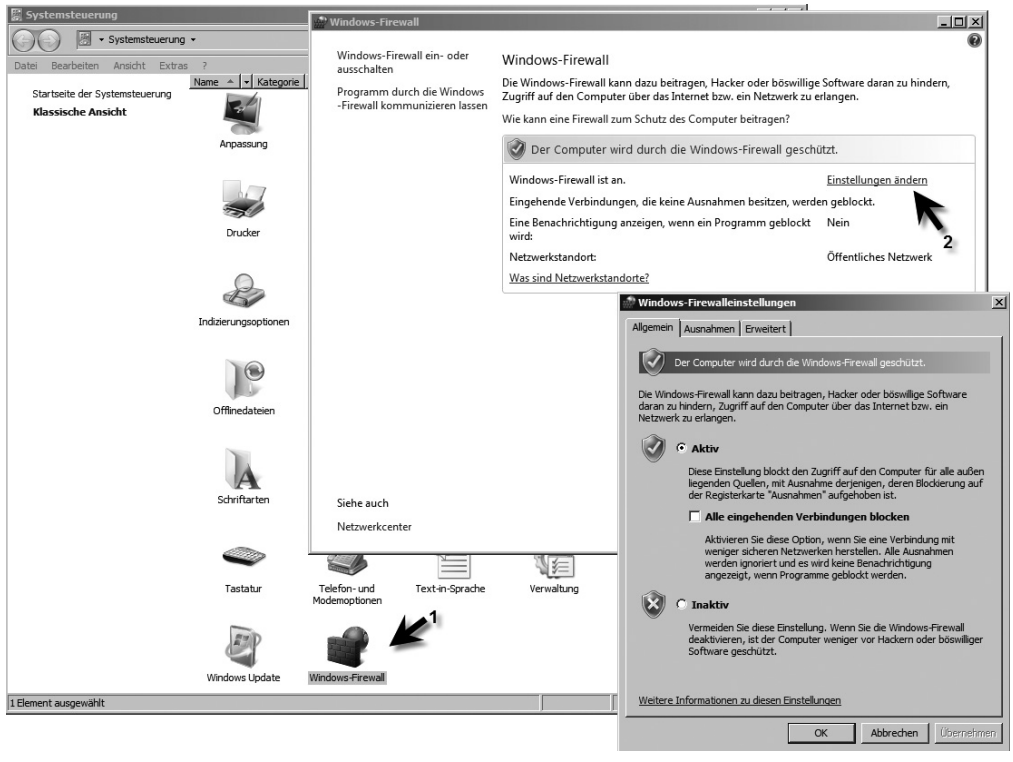
Die neue Windows-Firewall mit erweiterter Sicherheit kann auch über den Befehl *netsh advfirewall* in der Befehlszeile verwaltet werden (Abbildung 1.10).

Abbildg. 1.10 Verwalten der neuen Windows-Firewall mit erweiterter Sicherheit in der Befehlszeile

Die neue Windows-Firewall filtert den ein- und ausgehenden IPv4- und auch IPv6-Verkehr. Außerdem können Sie vielfältige Regeln basierend auf Port, IPv4-Adresse, IPv6-Adresse, Pfad und Name

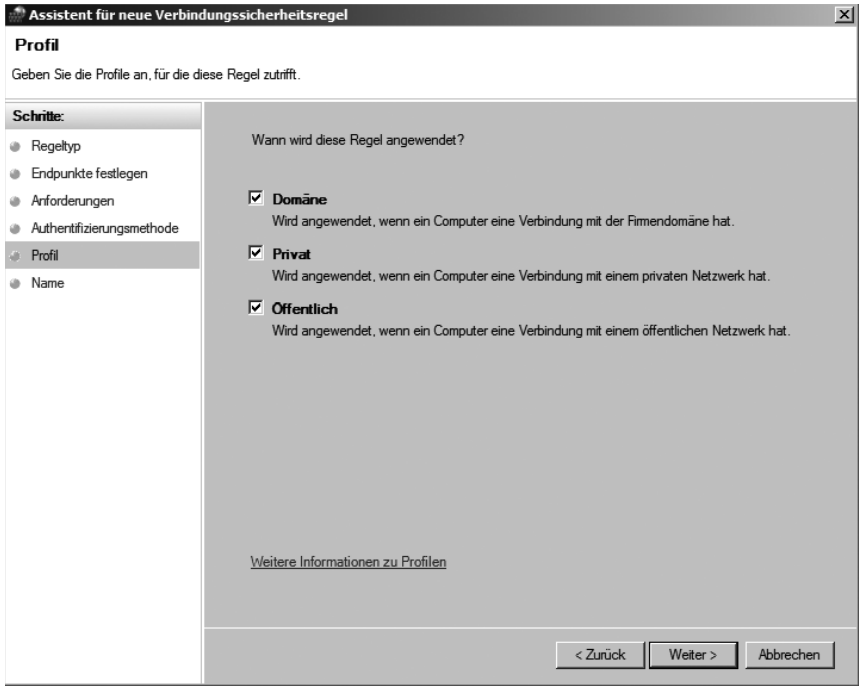
der Applikation oder IPSec-Richtlinien erstellen. Sie können mit der grafischen Verwaltungsoberfläche *wf.msc* sowie mit der Befehlszeile *netsh advfirewall* die Einstellungen der lokalen Firewall und die Einstellungen von anderen Servern im Netzwerk konfigurieren. In der Systemsteuerung gibt es zwar auch ein Symbol für die Windows-Firewall, allerdings können hier nur sehr rudimentäre Einstellungen vorgenommen werden (Abbildung 1.11). Die verschiedenen Regeln lassen sich nur über die erweiterte Verwaltung konfigurieren.

Abbildg. 1.11 Verwalten der Windows-Firewall über die Systemsteuerung



Die Windows-Firewall unter Windows Server 2008 und Windows Vista unterstützt verschiedene Regeln, abhängig vom jeweiligen Netzwerkprofil. Dabei unterscheidet die Firewall, ob sich der Server aktuell in einer Domäne oder in einem privaten oder öffentlichen Netzwerk befindet (Abbildung 1.12).

Abbildg. 1.12 Verwenden von Firewallregeln abhängig vom Netzwerkprofil



Da sich ein Windows-Server eher selten bewegt, sollten Sie bei der Erstellung von Firewallregeln möglichst immer alle drei Profile auswählen.

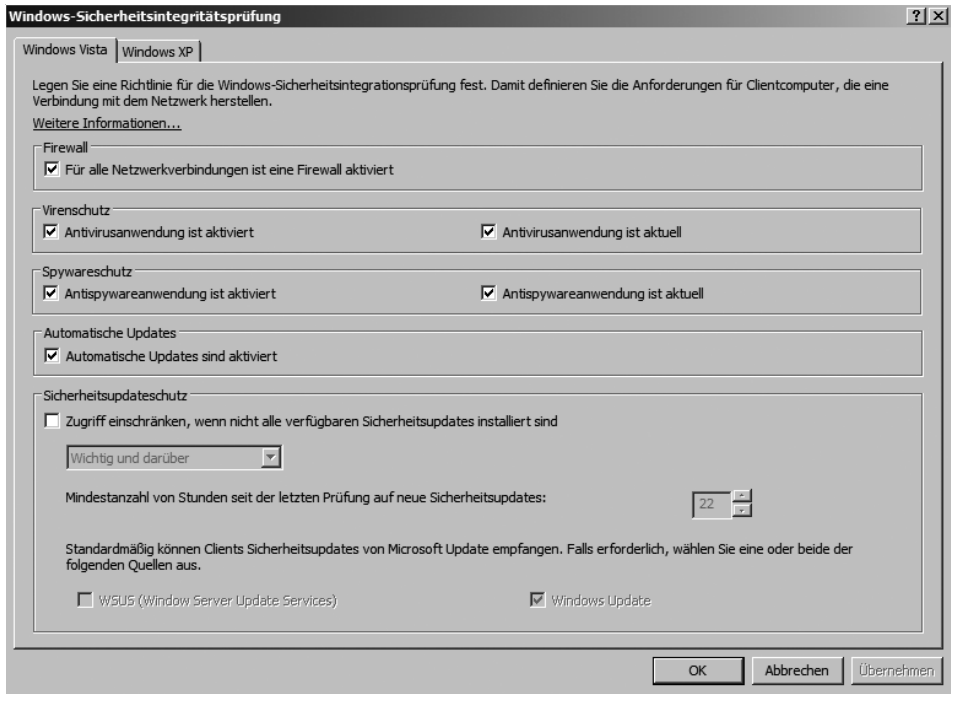
IPSec-Verbesserungen

Unter Windows Server 2003 war die Konfiguration von IPSec noch eine relativ komplexe Angelegenheit. Durch die Integration der IPSec-Verwaltung in die Firewall-Konsole wird diese Konfiguration enorm vereinfacht. Verwenden Sie mit Windows Server 2008 IPSec-Richtlinien, verhalten sich die Server wie folgt: Ein Server, für den IPSec aktiviert wurde, sendet Pakete über IPSec. Antwortet der empfangende Server ebenfalls mit IPSec, wird der Datenverkehr verschlüsselt. Unterstützt der empfangende Server kein IPSec, wird der Datenverkehr nicht verschlüsselt. Dieser Datenverkehr findet gleichzeitig statt. Unter Windows Server 2003 wurden zunächst IPSec-Pakete verschickt, dann drei Sekunden gewartet und dann erst die unverschlüsselten Pakete gesendet. So konnten oft starke Performance-Probleme auftreten, die durch das gleichzeitige Versenden der Pakete in 2008 vermieden werden. Durch diese Funktion können Server IPSec-Verkehr unterstützen, aber nicht mehr zwingend voraussetzen, um eine möglichst sichere Verbindung zu erstellen. Bisher hat IPSec unter Windows nur Internet Key Exchange (IKE) unterstützt. Windows Vista und Windows Server 2008 unterstützen eine neue Funktion, die Authenticated IP (AuthIP) genannt wird. Diese neue Funktion unterstützt weitergehende Authentifizierungsfunktionen als IKE, zum Beispiel die Gültigkeit von Zertifikaten, die Bestandteil der neuen Network Access Protection (NAP) in Windows Server 2008 sind (NAP wird in Kapitel 12 im Rahmen der Einrichtung eines Terminalservers ausführlicher besprochen).

Network Access Protection (NAP)

Windows Server 2008 enthält den so genannten Next Generation TCP/IP-Stack, der deutlich stabiler und schneller ist und vor allem IPv6 unterstützt (siehe Kapitel 7).

Abbildg. 1.13 Windows Server 2008 kann Netzwerkrichtlinien für den Zugriff verwenden



Ein neues Sicherheits-Feature stellt die *Network Access Protection (NAP)* dar. Über diesen Netzwerkzugriffsschutz können Unternehmen anhand entsprechender Richtlinien sicherstellen, dass nur solche Clients Zugang zum Firmennetz erhalten, die bestimmten Sicherheitskriterien genügen (siehe Abbildung 1.13 und Kapitel 15). Die für NAP erforderliche Client-Software ist in Vista und Windows Server 2008 bereits enthalten, während für Windows XP SP2 oder Windows Server 2003 eine separat zu installierende NAP-Client-Software angeboten wird. Im Service Pack 3 für Windows XP ist der Client ebenfalls bereits enthalten. Ein NAP-Server kann feststellen, ob Remote-PCs, die über ein VPN Verbindung mit dem Firmennetz herstellen möchten oder auch Computer im Netzwerk, die Sicherheitsrichtlinien des Unternehmens einhalten. Trifft dies nicht zu, lehnt der VPN-Server die Verbindung ab. Genauso kann der Netzwerkzugriffsschutz ermitteln, ob ein im LAN befindlicher Computer die gesetzten Sicherheitskriterien erfüllt und ihm damit Zugang zum Firmennetz gewähren oder verweigern. Durch den Einsatz von NAP können Sie feststellen, ob Sicherheitspatches aufgespielt sind oder der Computer durch eine Antiviren- sowie eine Antispyware-Software geschützt wird. Erfüllt ein Client diese Kriterien nicht, weist NAP ihn ab oder leitet ihn in eine eingeschränkte Umgebung um, wo er automatisch aktualisiert werden kann. Dort können Clients von einem FTP-Server oder WSUS (siehe Kapitel 23) Aktualisierungen herunterladen und aufspielen, um ihre Sicherheitskonfiguration auf den neuesten Stand zu bringen und so die von NAP aufgestell-

ten Zugangsvoraussetzungen zu erfüllen. Windows Server 2008 und Windows Vista beinhalten folgende Technologien für die NAP-Erzwingung:

- Mit der *DHCP-Erzwingung* können DHCP-Server Richtlinien für Integritätsanforderungen immer dann erzwingen, wenn ein Computer versucht, im Netzwerk eine IP-Adresskonfiguration zu leasen oder zu erneuern. Bei der DHCP-Erzwingung handelt es sich um die einfachste Erzwingung für die Bereitstellung, da sämtliche DHCP-Clientcomputer IP-Adressen leasen müssen.
- Mithilfe der *VPN-Erzwingung* können VPN-Server Richtlinien für Integritätsanforderungen immer dann erzwingen, wenn ein Computer versucht, eine VPN-Verbindung mit dem Netzwerk herzustellen. Die VPN-Erzwingung bietet einen sicheren eingeschränkten Netzwerkzugriff für alle Computer, die auf das Netzwerk über eine VPN-Verbindung zugreifen. Die VPN-Erzwingung mit NAP unterscheidet sich von der Quarantänesteuerung für Netzwerkzugriffe in Windows Server 2003.
- Mithilfe der *802.1X-Erzwingung* weist ein Netzwerkrichtlinienserver (Network Policy Server, NPS) einen 802.1X-basierten Zugriffspunkt (ein Ethernet-Switch oder ein drahtloser Zugriffspunkt) an, für den 802.1X-Client so lange ein eingeschränktes Zugriffsprofil zu verwenden, bis eine Reihe von Korrekturfunktionen ausgeführt wurden. NPS ist die Microsoft-Implementierung eines Remote Authentication Dial-In User Service-(RADIUS-)Servers und -Proxys. NPS ersetzt den Internetauthentifizierungsdienst (Internet Authentication Service, IAS) von Windows Server 2003. Der Dienst führt sämtliche Funktionen von IAS in Windows Server 2003 für die VPN- und 802.1X-basierte drahtlose und verdrahtete Verbindungsauthentifizierung durch. Zusätzlich werden eine Integritätsprüfung und das Gewähren von uneingeschränktem oder eingeschränktem Zugriff auf NPS-Clients durchgeführt. NPS unterstützt außerdem das Senden von RADIUS-Verkehr über IPv6 (gemäß RFC 3162). Ein eingeschränktes Zugriffsprofil kann aus einer Reihe von IP-Paketfiltern oder einer virtuellen LAN-ID bestehen, mit der der Verkehr eines 802.1X-Clients eingeschränkt wird. Die 802.1X-Erzwingung bietet einen sicheren eingeschränkten Netzwerkzugriff für alle Computer, die auf das Netzwerk über eine 802.1X-Verbindung zugreifen.
- Mithilfe der *IPsec-Erzwingung* kann die Kommunikation in einem Netzwerk auf kompatible Computer beschränkt werden. Da IPsec verwendet wird, können Sie Anforderungen für eine geschützte Kommunikation mit kompatiblen Clients definieren. Dies kann für einzelne IP-Adressen oder pro TCP/UDP-Portnummer erfolgen. Anders als bei der DHCP-, VPN- und 802.1X-Erzwingung beschränkt die IPsec-Erzwingung die Kommunikation auf kompatible Computer, nachdem diese erfolgreich eine Verbindung hergestellt und eine gültige IP-Adresskonfiguration abgerufen haben. Bei der IPsec-Erzwingung handelt es sich um die sicherste Form eines eingeschränkten NAP-Netzwerkzugriffs.

Neue Funktionen in Active Directory

Auch im Bereich Active Directory bietet Windows Server 2008 zahlreiche Neuerungen. In Kapitel 8 besprechen wir diese Funktionen noch ausführlicher als in dieser Einführung.

Read-Only-Domänencontroller

Für Unternehmen, die sich um die Datensicherheit in ihren Außenstellen sorgen, bietet Windows Server 2008 einen neuen Domänencontroller-Typ »Read-Only Domain Controller« (RODC) an (siehe Kapitel 8). Hierbei wird auf dem Domänencontroller ein Replikat der Active Directory-

Datenbank gespeichert, die keinerlei Änderungen akzeptiert. Außerdem lässt sich die Berechtigung zur RODC-Verwaltung an einen beliebigen Domänenbenutzer delegieren, um beispielsweise Aktualisierungen von Gerätetreibern vor Ort rasch durchführen zu können. Schreibende Domänencontroller richten keine Replikationsverbindung zu RODCs ein, da eine Replikation nur von normalen DCs zu RODCs erfolgen kann. RODCs richten Replikationsverbindungen zu den schreibenden Domänencontrollern ein, die Sie bei der Heraufstufung angeben. Bei RODCs handelt es sich um keine Wiederbelebung der Backup-Domänencontroller (BDC) von Windows NT 4.0, sondern um eine vollständige Neuentwicklung, die viele Möglichkeiten offenbart.

Neue Gruppenrichtlinien

Eine sehr wichtige Neuerung für Unternehmen sind die neuen Gruppenrichtlinienfunktionen in Windows Server 2008 (siehe Kapitel 9). Natürlich lassen sich die meisten dieser Funktionen erst im Zusammenspiel mit Windows Vista einsetzen. USB-Speichersticks sind die Achillesferse in den meisten Sicherheitskonzepten. Die bisherigen Windows-Versionen bringen keine Verwaltung für die mobilen Speicher mit. Ein böswilliger Nutzer kann damit problemlos Daten in das Firmennetz einschleusen oder entwenden. Windows Vista und Windows Server 2008 gehen dieses Problem direkt in den Gruppenrichtlinien an. Je nach Einstellung können Administratoren künftig den Zugriff auf USB-Geräte sperren oder einen reinen Lese- oder Schreibzugriff gewähren. Administratoren können jetzt entscheiden, wer USB-Sticks nutzen darf.

Unter Windows XP und Windows Server 2003 gab es für unterschiedliche Sprachversionen von Windows unterschiedliche Versionen der Vorlagendateien (**.adm*-Dateien). Da dies vor allem für internationale Unternehmen nicht sehr effizient ist, hat Microsoft das Design der Vorlagendateien angepasst. Änderungen in Gruppenrichtlinien müssen dadurch nicht in jeder Sprachversion eingestellt werden, sondern nur noch einmal zentral im Unternehmen. Die alten Vorlagen-Dateien (**.adm*) können unter Windows Server 2008 weiterhin verwendet werden. Windows Server 2008 verwendet für seine neuen Vorlagendateien sprachneutrale **.admx*-Dateien. Diese bauen auf XML auf. Diese **.admx*-Dateien werden nicht mehr für jede einzelne Gruppenrichtlinie hinterlegt, sondern zentral im Policyordner (siehe Kapitel 9).

Richtlinien für Kennwörter

Unter Windows Server 2008 können mehrere Richtlinien für Kennwörter definiert werden, sodass besonders sensiblen Bereichen des Unternehmens komplexere Kennwörter zugewiesen werden als anderen. Kennwortrichtlinien können jetzt auch einzelnen OUs zugewiesen werden. Wichtig für diese neue Funktion ist die OU *Passwort Setting Container*, die unterhalb der OU *System* im Snap-In *Active Directory-Benutzer und -Computer* angezeigt wird. In dieser OU werden nach Erstellung die Passwort Settings Objects (PSO) gespeichert. Eine PSO enthält alle notwendigen Einstellungen zur Konfiguration von Kennwortrichtlinien. Sicherheitsrichtlinien für Kennwörter können jetzt auch globalen Sicherheitsgruppen zugewiesen werden. Spezielle Kennwortrichtlinien die einzelnen Anwendern, Gruppen oder OUs zugewiesen werden, überschreiben automatisch die Einstellungen in der Default Domain Policy. Damit diese neue Funktion genutzt werden kann, muss sich die Domäne im Betriebsmodus Windows Server 2008 befinden.

Active Directory-Dienst manuell starten und anhalten

Unter Windows Server 2008 ist es möglich, den Systemdienst für Active Directory im laufenden Betrieb zu stoppen und wieder zu starten. Durch diese Funktion kann Active Directory auf einem Server auch neu gestartet werden, während die anderen Dienste des Servers weiter funktionieren. Das kann zum Beispiel für die Offlinedefragmentation der AD-Datenbank sinnvoll sein, oder für die Installation von Updates.

Active Directory Snapshot-Viewer

Mit dem neuen Active Directory Snapshot-Viewer können versehentlich gelöschte Objekte der Domäne angezeigt werden. Mit dieser Funktion lassen sich zwar keine Objekte wiederherstellen, Sie erkennen aber, welche Objekte versehentlich gelöscht worden sind. Dazu kann unter Windows Server 2008 mit *Ntdsutil.exe* ein Snapshot von Active Directory durchgeführt und mit dem Snapshot-Viewer dieses auf gelöschte Objekte untersucht werden.

Einheitliche Bezeichnung der Active Directory-Komponenten

Microsoft hat in Windows Server 2008 auch die Bezeichnung der Komponenten angepasst, die zur Identitätsverwaltung verwendet werden. Alle diese Funktionen und Serverrollen erhalten vor der eigentlichen Bezeichnung noch das Präfix *Active Directory* hinzu. So wird schnell ersichtlich, welche der Dienste direkt auf Active Directory aufbauen oder mit Active Directory einen erweiterten Funktionsumfang erhalten: *Die Active Directory-Zertifikatdienste* (Active Directory Certificate Services, AD CS) stellen die neue Version der Zertifikatsdienste unter Windows Server 2003 dar (siehe Kapitel 17). *Active Directory-Domänendienste* (Active Directory Domain Services, AD DS) ist die Serverrolle, mit der ein Server zum Domänencontroller heraufgestuft werden kann, um entweder einer Gesamtstruktur beizutreten oder eine neue zu erstellen (siehe Kapitel 8). Die *Active Directory-Verbunddienste* (Active Directory Federation Services, AD FS) bieten eine webbasierte Single Sign-On (SSO)-Infrastruktur (siehe Kapitel 17). Mit den *Active Directory-Rechteverwaltungsdiensten* (Active Directory Rights Management Services, AD RMS) werden Daten mit digitalen Signaturen versehen, um sie vor unerwünschtem Zugriff zu sichern (siehe Kapitel 17).

Active Directory Lightweight Directory Services (AD LDS)

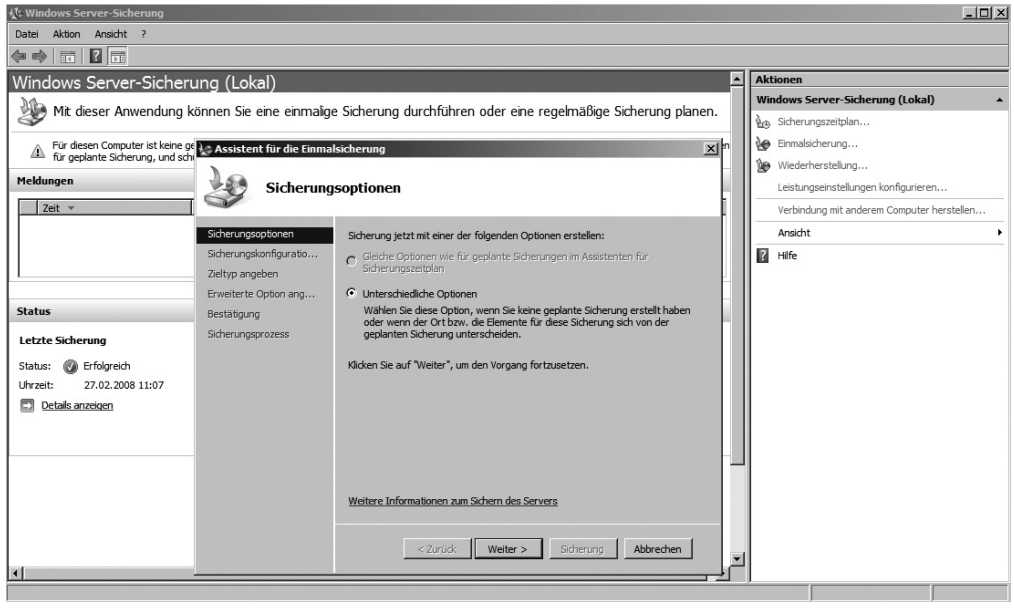
Mit AD LDS können unter anderem spezielle Anforderungen von Applikationen an einen Verzeichnisdienst abgebildet werden. Einer Applikation kann zum Beispiel ein eigenes Verzeichnis mit eigenem Schema zur Verfügung gestellt werden, ohne andere Anwendungen oder die Anmeldungen im Unternehmen zu beeinträchtigen. Die Verwaltung eines Extranets und die damit verbundene Identitätsverwaltung lassen sich ebenfalls mit AD LDS verbessern. Sollen X.500/LDAP-Verzeichnisdienste migriert werden, bietet AD LDS eine optimale Schnittstelle zum Verzeichnis des Unterneh-

mens. Auch zur Identitätsverwaltung in kleineren Niederlassungen oder in DMZs können die AD LDS wertvolle Dienste leisten. Die AD LDS verfügen dazu, genauso wie ein normales Active Directory, über eine eigene Benutzerverwaltung. Mit AD LDS können aber auch lokale Benutzerkonten und Gruppen genauso verwendet werden, wie Benutzer und Gruppen aus Active Directory. Dazu wird die Authentifizierung mit diesen Objekten automatisch entweder zur lokalen Maschine oder einem Active Directory-Domänencontroller umgeleitet und anschließend der Zugriff auf die Daten innerhalb der AD LDS gestattet.

Windows Server-Sicherung

Das Datensicherungsprogramm wurde ebenfalls komplett überarbeitet (siehe Kapitel 21). Bandlaufwerke werden vom Server-Backup nicht mehr unterstützt. Das standardmäßige Datensicherungsprogramm von Windows Server 2008 wird nicht mehr automatisch installiert, sondern muss manuell nachinstalliert werden. Die Sicherung unterstützt jetzt besser die Schattenkopien (siehe Kapitel 5 und 6) sowie die integrierten Sicherungsfunktionen von SQL Server 2005/2008 und SharePoint Server 2007. Die Verwaltung der Sicherung findet über die Microsoft Management Console (MMC) statt. So können Sie auch über das Netzwerk mit der MMC die Datensicherung von mehreren Servern verwalten. Neu sind die Unterstützung für DVD-Brenner sowie die automatische Überwachung des freien Festplattenplatzes auf dem Sicherungsmedium. Datensicherungen, die Sie mit älteren Versionen von *Ntbackup.exe* erstellt haben sind nicht mehr kompatibel zur neuen Windows Server-Sicherung. Sollten Sie eine solche Sicherung benötigen, stellt Microsoft kostenlos die Vorgängerversion von *Ntbackup.exe* auf der Internetseite *http://go.microsoft.com/fwlink/?LinkId=82917* zur Verfügung.

Abbildg. 1.14 Das neue Datensicherungsprogramm in Windows Server 2008



Verbesserungen im NTFS-Dateisystem

Korruptionen im Dateisystem konnten bisher nur mittels *Chkdsk.exe* behoben werden. Unter Windows Server 2008 erkennt das Dateisystem selbst korrupte Bereiche und repariert diese automatisch. Verbesserungen an der NTFS-Kernelcodebasis berichtigen erkannte Probleme, während das System läuft. Transactional NTFS ermöglicht transacted Filesystem-Operationen im NTFS. Dadurch sind NTFS und die Registry in der Lage, ihre Arbeit in einer Transaktion zu koordinieren. Transactional NTFS wendet Transactional-Datenbankkonzepte am Dateisystem an. Das Dateisystem wird dadurch wesentlich stabiler. Durch diese Funktion kann Windows Server 2008 auch besser mit dem neuen SQL Server 2008 zusammenarbeiten. Heutzutage speichern viele Anwendungen die Daten nicht mehr relational. SharePoint speichert zum Beispiel seine Daten in SQL-Datenbanken, was in sehr große Datenbanken resultiert, abhängig von den gespeicherten Dateien. SQL Server 2008 unterstützt die transaktionale Speicherung von Dateien auf dem Dateisystem, die aber weiterhin mit der Datenbank verbunden sind. Auch wenn die Daten auf dem Dateisystem gespeichert werden, verhalten sich diese so, als ob sie ausschließlich in der Datenbank gespeichert sind, und können daher auch transaktional verwendet werden. Damit diese Funktion stabil und sicher funktioniert, wird das transaktionale Dateisystem von Windows Server 2008 verwendet. Der Lese- und Schreibzugriff erfolgt dadurch mit NTFS-Performance und mit SQL-Sicherheit. Es gibt 2D- und 3D-Daten, also ortsabhängige Verknüpfungen in SQL Server 2008. Sie können zum Beispiel alle geografischen Punkte in einem gewissen Bereich von Daten einer Datenbank anzeigen lassen und diese mit Virtual Earth sogar visualisieren. Die geografischen Daten werden dazu mit in der Datenbank gespeichert, was zum Beispiel bei Vertriebsgebieten sehr sinnvoll ist.

Änderungen in den Terminaldiensten

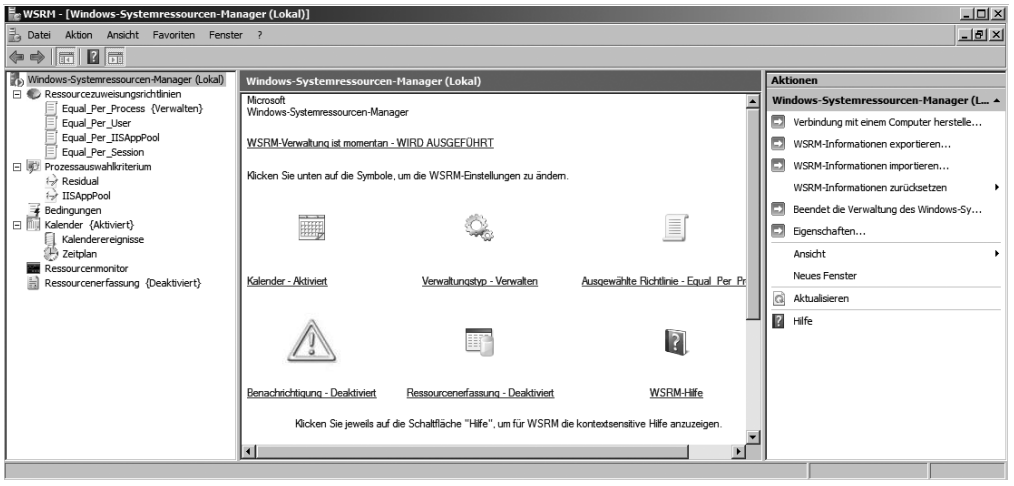
Die weiterentwickelte Version 6.0 des Remote Desktop Protocol (RDP) unterstützt Auflösungen im Breitbildformat und den Multimonitorbetrieb (siehe auch Kapitel 12). Auf Wunsch stellt der Terminalserver des 2008-Servers für Vista-basierte Clients die Aero-Oberfläche bereit. Eine weitere wichtige Funktion der Terminaldienste wird als *RemoteApps* bezeichnet. Sie ermöglicht es, eine auf dem Terminalserver befindliche Anwendung auf dem Client in einem normalen Programmfenster ablaufen zu lassen. Dies geschieht parallel zu anderen, lokal auf dem Client installierten Anwendungen. Terminalserver mit Citrix Presentation Server kennen diesen Modus als »Seamless Mode«. Der Anwender kann nicht unterscheiden, ob die Anwendung lokal oder über einen Terminalserver läuft. Neu sind auch die Möglichkeiten, über ein HTTPS-Gateway auf Terminalserver zuzugreifen, sowie das neue Web Access für die Terminaldienste. Über diese Funktion können Anwender auf einer Weboberfläche auf den Server zugreifen. Weitere Verbesserungen bei den Terminaldiensten sind die Unterstützung von deutlich höheren Auflösungen, Single Sign-On und die Integration der Terminaldienste in den Windows-Systemressourcen-Manager (siehe Kapitel 12).

Abbildg. 1.15 Mit Windows Server 2008 können Anwender auch über ein Webportal auf Anwendungen zugreifen

Windows-Systemressourcen-Manager (WSRM)

WSRM erlaubt, die CPU-Zeit und Speichergröße individuell einer Anwendung zuzuordnen, ohne dass die Einstellungen vom Benutzer geändert werden können. Hauptzweck ist die kontrollierte Verwaltung der Ressourcen auf einem Server mit vielen Anwendungen und Benutzern. Das Tool weist zum Beispiel mehreren Anwendungen oder Terminalserverbenutzern auf einem Server unter Windows CPU- und Arbeitsspeicherressourcen zu (siehe auch Kapitel 12). Der Windows-Systemressourcen-Manager (Windows System Resource Manager, WSRM) ist eine Verbesserung der Version für Windows Server 2003. Das Produkt kann nur für Windows Server 2003 Enterprise-Edition eingesetzt werden, Windows Server 2003 Standard- und Web-Edition werden nicht unterstützt. WSRM kann von der Internetseite *http://www.microsoft.com/technet/downloads/winsrvr/wsrm.mspx* heruntergeladen werden. In Windows Server 2008 ist der WSRM bereits standardmäßig integriert und deutlich erweitert worden. Um die Ressourcen auf einem Terminalserver zu verwalten, dienen hauptsächlich die beiden Ressourcezuweisungsrichtlinien *Equal_Per_User* und *Equal_Per_Session*. Die Richtlinie *Equal_Per_Session* ist neu in Windows Server 2008. Idealerweise setzen Sie diese Richtlinie ein, um die Ressourcen auf einem Terminalserver zu steuern. In diesem Fall erhalten die Anwender und deren gestartete Prozesse gleichmäßig CPU und Speicher zugeteilt.

Abbildg. 1.16 Ressourcen lassen sich mit dem WSRM effizient unter Windows Server 2008 aufteilen, wovon hauptsächlich Terminalserver profitieren

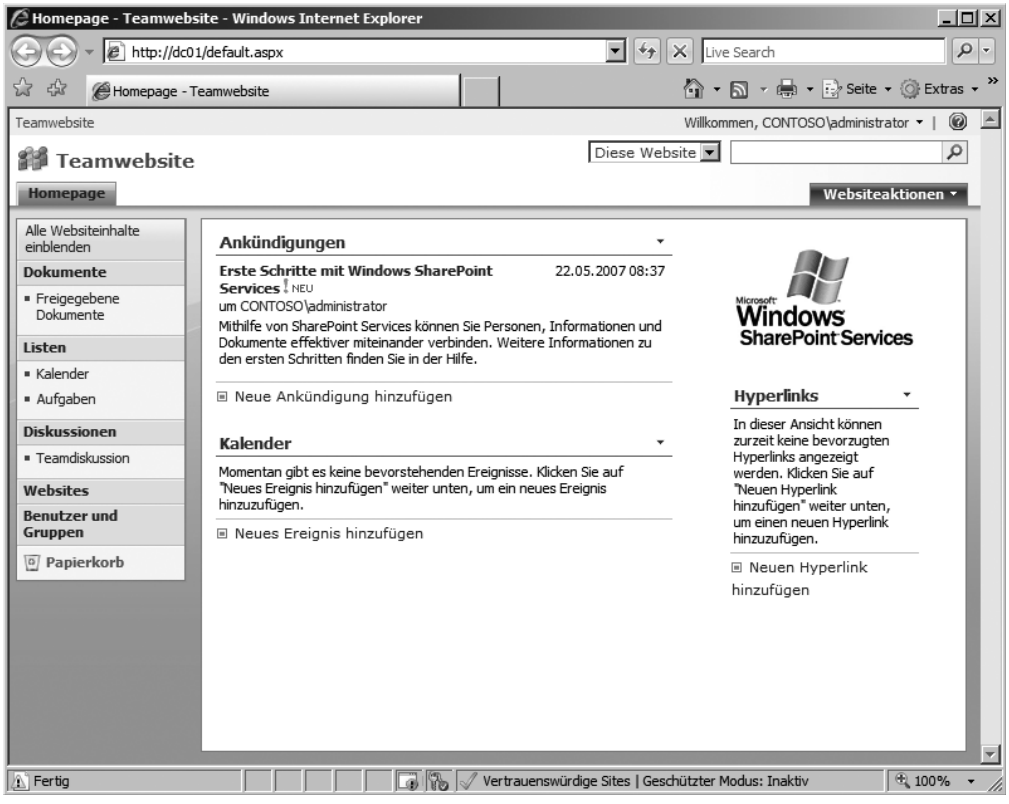


Mehr zu diesem Thema erfahren Sie ausführlich in Kapitel 12.

Windows SharePoint Services 3.0 SP1

In Windows Server 2008 sind die Windows SharePoint Services 3.0 SP1 (WSS) zwar nicht direkt integriert, aber mit dem Service Pack 1 vollkommen kompatibel zu Windows Server 2008. Microsoft bietet WSS kostenlos für Windows Server 2003 zum Download an (*http://www.microsoft.com/downloads/details.aspx?FamilyId=EF93E453-75F1-45DF-8C6F-4565E8549C2A&displaylang=de*). Wesentliche Neuerungen in den SharePoint Services 3.0 mit SP1 sind ein Papierkorb, über den Sie gelöschte Objekte wiederherstellen können, und die Interaktion mit den aktuellen Office 2007-Produkten von Microsoft. Mit den SharePoint Services 3.0, können Sie außerdem Wiki-Bibliotheken erstellen, also Knowledge-Datenbanken ähnlich wie die Wikipeda. Außerdem unterstützt die neue Version auch Blog-Arbeitsbereiche, sowie RSS-Feeds. Mit Outlook 2007 können Benutzer Informationen gemeinsam nutzen und gemeinsam an Aufgaben und Projekten arbeiten. Dadurch haben Sie Zugriff auf verschiedene Bereiche für die Zusammenarbeit in Windows SharePoint Services 3.0, mit deren Hilfe Sie Diskussionen beginnen, Kalender freigeben, gemeinsame Kontaktlisten aktualisieren und bei gemeinsam verfassten Dokumenten Versionsüberprüfungen durchführen können. Kalenderinhalte können leichter und schneller freigegeben werden. Durch die Integration von Features aus Outlook und Windows SharePoint Services wird das Senden eines Projektzeitplans an Mitarbeiter so einfach wie das Erstellen einer neuen E-Mail-Nachricht. Empfänger können bei der empfangenen Freigabenachricht auf die neue, in der Nachricht enthaltene Schaltfläche *Diesen Kalender öffnen* klicken. Das Freigabenachricht-Feature kann auch mit anderen Arten von SharePoint-Listen und -Bibliotheken verwendet werden, wie z.B, mit Kontakte-, Aufgaben- und Diskussionslisten. Die SharePoint Services 3.0 benötigen .NET Framework 3.0, welches ebenfalls mit Windows Server 2008 ausgeliefert wird.

Abbildg. 1.17 Mit den SharePoint Services 3.0 von Windows Server 2008 lässt sich ein Intranet aufbauen



Mehr zu WSS und deren Integration in Windows Server 2008 erfahren Sie in Kapitel 22.

Neue Installationsmechanismen – WIM-Images

Die Windows Server 2008-Installationsoberfläche ist deutlich effizienter als die Variante unter Windows Server 2003. Windows Server 2008 verwendet zur Installation jetzt standardmäßig WinPE (Microsoft Windows Pre-Installation Environment). Im Gegensatz zur Windows XP-PE-Version ist die Windows Server 2008-Variante für jedermann erhältlich. WinPE kommt bei der Installation, bei Recovery-Funktionen und beim Troubleshooting zum Einsatz. Es enthält sämtliche Kernfunktionen von Windows Server 2008 und ist damit den bisherigen Notfallkonsolen deutlich überlegen. So kann WinPE unter anderem auf Netzwerklaufwerke zugreifen und enthält alle Netzwerktreiber, die auch Vista beiliegen. Sollten Treiber fehlen, lassen sich diese nachladen – egal, ob von USB, CD/DVD oder einer Freigabe. WinPE unterstützt neben der 32- auch die 64-Bit-Architektur. Der größte Vorteil ist allerdings, dass sich Win32-Anwendungen direkt aus WinPE starten lassen. Damit stehen beispielsweise auch unter einem Notfallsystem dieselben Anwendungen zur Verfügung, wie direkt unter Windows Server 2008. Ein weiterer Vorteil ist, dass WinPE sowohl Multithreading als auch

Multitasking unterstützt. Die Windows Server 2008-Bereitstellung basiert auf Images (siehe Kapitel 2 und 16). Aus diesem Grund läuft die Installation von Windows Server 2008 deutlich schneller ab, als in den Vorgängerversionen, da keine einzelnen Daten übertragen werden müssen, sondern nur ein komplettes Image. Windows Vista und Windows Server 2008 arbeiten mit dem WIM-Imageformat (Microsoft Windows Imaging). Statt eines sektorbasierten Imageformats, wie es heutzutage fast überall existiert, ist das WIM-Format dateibasiert. Dies hat mehrere Vorteile:

- WIM ist hardwareunabhängig. Das bedeutet, Sie brauchen nur ein Image für verschiedene Hardwarekonfigurationen.
- Mit WIM können mehrere Images in einer Datei gespeichert werden. Sie können Images mit und ohne Anwendungen in einer Datei speichern.
- WIM nutzt eine Kompression und ein Single-Instance-Verfahren. So wird die Größe von Imagedateien deutlich reduziert. Single-Instancing ist eine Technologie, bei der jede Datei nur einmal gespeichert wird. Wenn zum Beispiel Image 1, 2 und 3 alle die Datei A enthalten, dann sorgt Single-Instancing dafür, dass Datei A tatsächlich nur einmal gespeichert wird.
- WIM ermöglicht die Offlinebearbeitung von Images. Sie können Betriebssystemkomponenten, Patches und Treiber hinzufügen oder löschen, ohne ein neues Image erstellen zu müssen.
- Mit WIM können Images auf Partitionen jeder Größe installiert werden. Sektorbasierte Imageformate benötigen eine Partition der gleichen Größe oder eine größere Partition.
- Windows Server 2008 stellt eine API für das WIM-Imageformat zur Verfügung, die WIMGAPI. Diese kann von Entwicklern für die Arbeit mit WIM-Imagedateien genutzt werden.
- Mit WIM können auf dem Zielvolumen vorhandene Daten beibehalten werden. Das Einrichten eines Images löscht nicht zwingend alle vorhandenen Daten auf der Festplatte.

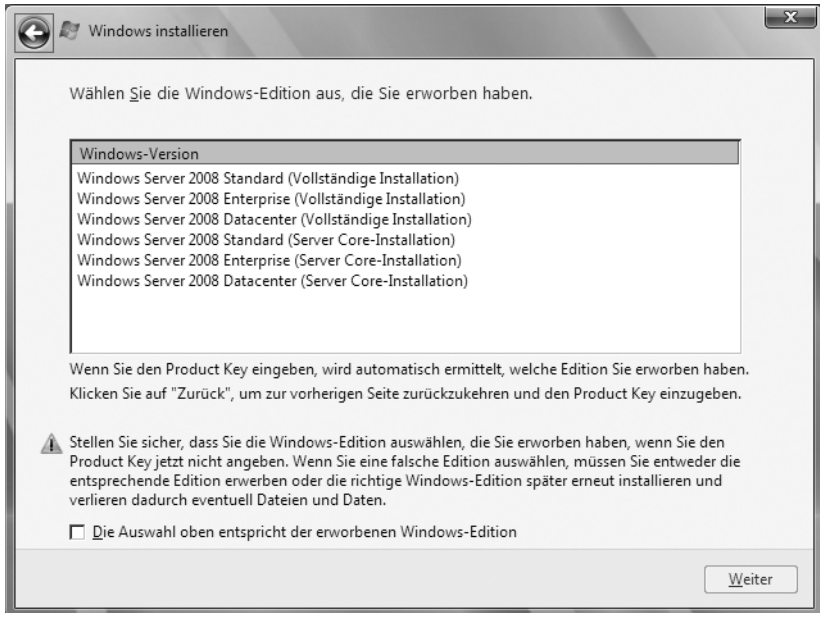
Core-Server-Installation

Während der Installation von Windows Server 2008 können Sie auswählen, ob Sie den Server komplett installieren, oder ob Sie eine Core-Version installieren wollen (siehe Abbildung 1.18 und Kapitel 2). Nach der Installation bietet ein Core-Server allerdings nicht die gewohnte grafische Benutzeroberfläche. Die Verwaltung eines solchen Servers findet über die Befehlszeile statt. Es gibt kein Startmenü, keine Systemsteuerungen, keine Snap-Ins für die MMC. Es besteht aber die Möglichkeit, einen solchen Server über das Netzwerk mit den Snap-Ins auf anderen Servern zu verwalten.

Die Server Core-Installation dient der Installation eines Servers, der nur diese Rollen annehmen kann:

- Dateiserver
- Druckserver
- Streaming Media Services
- Domänencontroller
- Active Directory Lightweight Directory Services (AD LDS, unter Windows Server 2003 ADAM genannt)
- DNS-Server
- DHCP-Server

Abbildg. 1.18 Auswählen der Server Core-Installation



Alle anderen Rollen können auf einem Core-Server nicht installiert werden. Sie haben bei einem Core-Server gegenüber der vollen Installation einige Vorteile:

- Es werden nur die notwendigen Komponenten installiert. Dadurch erhöht sich die Sicherheit, weil kein Angriff auf unnötige Funktionen stattfinden kann.
- Die Stabilität des Servers wird erhöht, weil nicht benötigte Komponenten keinen Absturz verursachen.
- Die Installation benötigt deutlich weniger Platz.

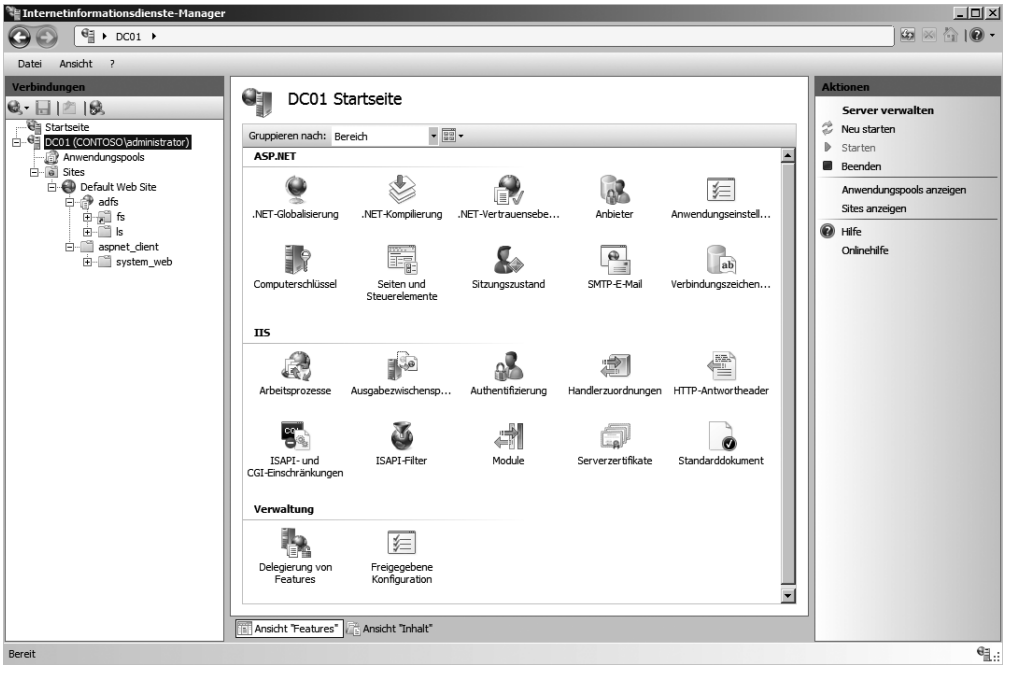
Core-Server als Domänencontroller

Soll auf einem Core-Server Active Directory installiert werden, muss eine Antwortdatei erstellt und diese bei der Heraufstufung verwendet werden. Die unbeaufsichtigte Installation von Active Directory kann auch auf herkömmlichen Servern durchgeführt werden, zum Beispiel als Skript um Server in Niederlassungen zu Domänencontrollern heraufzustufen. Um das Active Directory unbeaufsichtigt zu installieren, wird in der Befehlszeile *dcpromo /answer:<Antwortdatei>* oder *dcpromo /unattend:<Antwortdatei>* eingegeben. Die Antwortdatei ist eine normale Textdatei. Alle möglichen Variablen für die unbeaufsichtigte Installation von Active Directory unter Windows Server 2008 werden über den Befehl *dcpromo /?:unattend* mit ausführlicher Hilfe angezeigt.

Internetinformationsdienste (IIS 7.0)

Mit jeder neuen Serverversion bringt Microsoft auch eine neue Version der Internetinformationsdienste (Internet Information Services, IIS) auf den Markt. In Windows Server 2008 ist IIS 7.0 integriert, der gegenüber IIS 6.0 von Windows Server 2003 noch mal deutlich verbessert wurde (siehe Kapitel 13). Die meisten Anwendungen die auf Basis von ASP, ASP.NET 1.1 oder ASP.Net 2.0 entwickelt wurden, sollten auch problemlos unter IIS 7.0 laufen. Auch die Verwaltungsoberfläche für IIS sieht unter Windows Server 2008 anders aus. Die Verwaltung der Webanwendungen ist zwar ähnlich zu den Vorgängern, allerdings sind viele Aufgaben an eine andere Stelle gewandert. Bei der Installation von einzelnen Komponenten können jetzt noch detaillierter die Funktionen ausgewählt werden, die auch gebraucht werden. Alle anderen Komponenten werden nicht installiert. Vor allem im Bereich der Webanwendungen ist dies ein deutlicher Sicherheitsfortschritt. Die Konfiguration des Webservers und dessen Anwendungen wird in XML-Dateien gespeichert, was die Verwaltung noch mal deutlich vereinfacht. Es besteht mit IIS 7.0 die Möglichkeit die Verwaltung von einzelnen Webseiten und Anwendungen an andere Administratoren zu delegieren. Dies geschieht durch die neuen Verwaltungswerkzeuge, die für Administratoren deutlich mehr Möglichkeiten bieten, als noch bei den Vorgängerversionen.

Abbildg. 1.19 Die neue Verwaltungsoberfläche für IIS 7.0



Interaktion von Windows Server 2008 und Windows Vista

Viele Vorteile bei der Einführung von Windows Server 2008, ergeben sich durch die Interaktion mit Windows Vista (siehe auch Kapitel 24). So können zum Beispiel die Gruppenrichtlinieneinstellungen für die Benutzerkontensteuerung, die Windows-Firewall, und die Installation und Verwendung von USB-Sticks verwendet werden. Windows Vista und Windows Server 2008 wurden ursprünglich als Teile desselben Projekts entwickelt und haben eine Reihe neuer Technologien in den Bereichen Netzwerk, Speicher, Sicherheit und Verwaltung gemein. Weitere Gemeinsamkeiten sind:

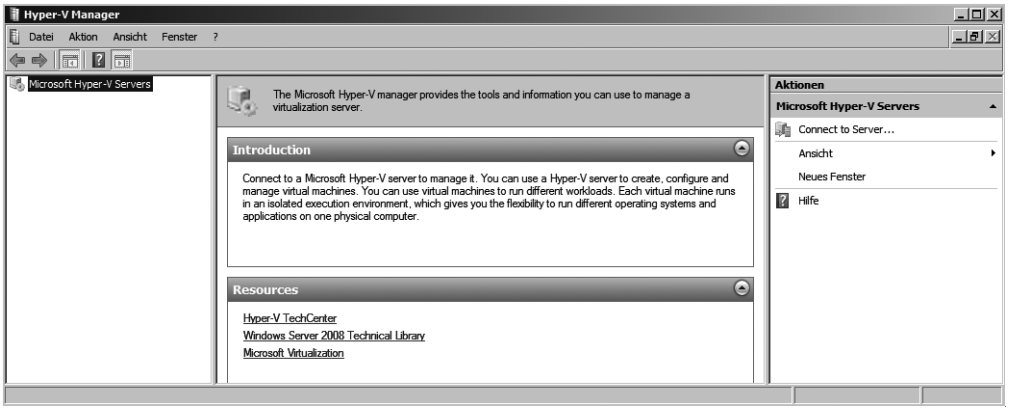
- Durchgängiger Netzwerkzugriffsschutz (NAP) für Clients und Server
- Leichtere Bereitstellung und sofortige Nutzung der Terminaldienste-Neuerungen in Windows Server 2008
- Höhere Verfügbarkeit dank skalierbarem Druckserver und richtlinienbasiertes QoS (Quality of Service)
- Schnellere Kommunikation dank erweiterter Indizierungs- und Caching-Funktionen
- Höhere Geschwindigkeit im Netz, da die durchgängige IPv4/IPv6-Fähigkeit von Windows Server 2008 und Windows Vista mehr Skalierbarkeit und Zuverlässigkeit bietet
- Clients können Druckaufträge vor dem Senden an die Druckserver lokal darstellen, um die Serverlast zu senken und dessen Verfügbarkeit zu erhöhen.
- Serverressourcen werden lokal zwischengespeichert, sodass sie auch dann verfügbar sind, wenn der Server nicht verfügbar ist (Offlinedateien). Kopien werden automatisch aktualisiert, sobald die Verbindung zwischen Client und Server erneut hergestellt wird.
- Anwendungen oder Skripts, die auf Client und Server ausgeführt werden müssen, können die Vorteile des Transactional File System nutzen, um das Fehlerrisiko bei Datei- und Registrierungsoperationen zu reduzieren und im Falle eines Fehlers oder Abbruchs zu einem vorherigen fehlerfreien Status zurückzukehren.
- Die Suche von Windows Server 2008-Servern über einen Windows Vista-Client bietet aufgrund der auf beiden Systemen erweiterten Index- und Zwischenspeichertechnologien eine deutliche Verbesserung bei der Suche.

Windows Server-Virtualisierung mit Hyper-V

Mit Windows Server-Virtualisierung (Windows Server Virtualization, WSV) liefert Microsoft eine integrierte Lösung zur Virtualisierung. Mit Windows Server 2008, Windows Server Virtualization und System Center Virtual Machine Manager (SCVMM) 2007 erreichen Unternehmen eine neue, ganzheitliche Stufe der Virtualisierung, bei der unterschiedliche Produkte Hand in Hand zusammenarbeiten: Dabei ist die Virtualisierung als fester Bestandteil in Windows Server 2008 integriert. Virtuelle Rechner erstellen Administratoren mit Windows Server Virtualization unter Windows Server 2008 oder mit Virtual Server 2005 R2 unter Windows Server 2003. Mit Hilfe von SCVMM lassen sich diese dann verwalten und mit System Center Operations Manager überwachen. Im Gegensatz zu Virtual Server 2005 R2 bietet die Windows Server Virtualisation mit der Hypervisor-Technologie eine direkte Verbindung mit den Virtualisierungsfunktionen der aktuellen AMD- und Intel-Prozessoren. Nach der Installation von

Hyper-V auf einem Server ist WSV aktiv und kann über eine eigene Verwaltungsoberfläche verwaltet werden. Über diese zentrale Konsole werden virtuelle Maschinen erstellt und überwacht.

Abbildg. 1.20 Die Verwaltung von WSV findet über den Hyper-V-Manager statt



Sie besteht aus einer kleinen hochspezialisierten Softwareschicht, die direkt zwischen der Serverhardware und den virtuellen Maschinen positioniert ist. WSV partitioniert die Hardware-Ressourcen eines Servers. Dabei können übergeordnete und untergeordnete Partitionen, so genannte Parent-VMs und Child-VMs erstellt werden. Während in der Parent-VM die VMware Worker Prozesse, der WMI-Provider und der VM-Dienst laufen, können in den Child-VMs die Anwendungen positioniert werden. Dabei tauscht nur die Parent-VM Informationen mit Windows HyperVisor direkt aus. Untergeordnete Partitionen stellen die Anwendungen im Benutzermodus zur Verfügung, während im Kernelmodus nur die Virtualization Service Clients (VSC) und der Windows Kernel betrieben werden. Dadurch wird neben der Geschwindigkeit natürlich auch die Stabilität der Maschinen gesteigert. Zu weiteren Möglichkeiten gehören die Virtualisierung von Desktops über die Terminaldienste, sowie die Applikationsvirtualisierung, bei der Anwendungen zentral konfiguriert und den Clients dann virtuell zur Verfügung gestellt werden. Für diese Bereiche bietet Microsoft mit neuen Funktionen in den Terminaldiensten von Windows Server 2008 und mit SoftGrid Application Virtualization die passenden Lösungen an. Und auch im Bereich der herkömmlichen Server- und Desktop-Virtualisierung mit Virtual Server 2005 R2 SP1 und Virtual PC 2007 stehen entsprechende Produkte zur Verfügung.

In den aktuellen Prozessoren von AMD und Intel sind bereits Virtualisierungsfunktionen eingebaut. Sie können aber nur genutzt werden, wenn auf den entsprechenden Servern auch virtuelle Rechner installiert werden, und die Virtualisierungsinfrastruktur diese Funktionen unterstützt. Mit Windows Server Virtualization zeigt sich hier eine der Stärken von Windows Server 2008: Die Lösung unterstützt die neuen AMD- und Intel-Virtualisierungsfunktionen für x64-Server-Prozessoren und setzt diese für den Einsatz voraus. Technologische Basis ist dabei ein HyperVisor, eine 64-Bit-Softwareschicht, die zwischen der Hardware und dem Betriebssystem platziert wird und die die Hardwareressourcen des physischen Windows Server 2008-Systems auf die einzelnen virtuellen Rechner verteilt. Mit ihr ordnen Administratoren die Ressourcen CPU und Arbeitsspeicher den virtuellen Betriebssystemsitzungen exakt zu. WSV verwendet synthetische Gerätetreiber, sodass für I/O-Zugriffe keine Softwareemulation erforderlich ist. Die Geschwindigkeit der virtuellen Maschinen wird durch diese Funktion stark gesteigert. Wie aktuell Virtual Server 2005 R2 wird auch HyperVisor künftig Linux oder andere Plattformen, die Intels x86-Prozessorarchitektur nutzen, als Gastbe-

triebssysteme unterstützen. So ist es beispielsweise möglich, auf einem Windows Server 2008-Host-System mit Windows Server Virtualization einen virtuellen 64-Bit-Server, einen 32-Bit-Server und ein Linux-System parallel zu betreiben. Neben 32-Bit- und 64-Bit-Systemen unterstützt Windows Server Virtualization auch Mehrprozessorsysteme als Gast.

Windows Server Virtualization lässt sich in System Center Virtual Machine Manager integrieren, aber auch in einer eigenständigen Microsoft Management Console (MMC) unter Windows Server 2008 verwalten. Die neuen Server-Funktionen werden auch dadurch optimal verbunden, dass Windows Server Virtualization eine Server-Rolle für den Server Core-Betriebsmodus von Windows Server 2008 ist. Durch das reduzierte Host-Betriebssystem können Administratoren ihre ganze Aufmerksamkeit den virtuellen Computern widmen. Auch Windows PowerShell, ebenfalls in Windows Server 2008 integriert, enthält Befehle, mit denen Sie virtuelle Server starten und stoppen können. In der Windows PowerShell lassen sich zudem Skripte zur Automatisierung erstellen. Microsoft verbesserte auch den Windows Server 2008-Clusterdienst für die Virtualisierung. Er bindet virtuelle Computer und deren Festplatten jetzt optimal in einen Failover-Cluster ein. Fällt zum Beispiel ein physischer Server aus, der mehrere virtuelle Rechner verwaltet, erkennt Windows Server Virtualization dies und führt eine so genannte *Quick Migration* durch. Voraussetzung ist, dass die Rechner in einem Speichernetzwerk (SAN) vorhanden sind. Der zweite physische Knoten im Cluster startet die virtuellen Computer, so dass diese den Anwendern sofort wieder zur Verfügung stehen. Diese Funktion unterstützt geplante, aber auch ungeplante Ausfälle von Clusterknoten.

System Center Virtual Machine Manager ermöglicht die zentrale Verwaltung und Konfiguration der gesamten virtuellen Infrastruktur: Administratoren können Server in Gruppen zusammenfassen, den Status abrufen und auch die Host-Systeme in der gleichen Konsole überwachen. SCVMM enthält außerdem Migrationswerkzeuge, mit denen physische Server oder virtuelle Festplatten von anderen Virtualisierungslösungen zum VHD-Format der Windows Server 2008-Virtualisierung migriert werden können. Vor allem die Migration von physischen zu virtuellen Servern, auch P2V genannt, wurde in SCVMM erheblich verbessert. SCVMM unterstützt darüber hinaus den Schattenkopiedienst von Windows Server 2003 beziehungsweise 2008 und eine blockbasierte Übertragung der Festplatten, ähnlich wie Imageprogramme von Drittanbietern. Das ermöglicht die Überführung von physischen Festplatten zu virtuellen Rechnern ohne lange Ausfallzeiten für die Anwender. Um die Auslastung in virtuellen Infrastrukturen zu steuern, verwendet SCVMM Informationen aus System Center Operation Manager. Abhängig vom Ressourcenverbrauch der installierten Anwendungen werden den virtuellen Computern mehr oder weniger Ressourcen auf den physischen Servern zugeteilt. Der Zugriff auf die virtuellen Rechner kann durch eine Active Directory-integrierte Authentifizierung geschützt werden. Neben Windows Server Virtualization unterstützt SCVMM auch Virtual Server 2005 R2 uneingeschränkt. Durch Gruppierung von virtuellen Servern können Administratoren physische Ressourcen gezielt bestimmten Servern zur Verfügung stellen. Weitere Informationen zum Thema Virtualisierung finden Sie in Kapitel 25.

Zusammenfassung

Wie Sie in diesem Kapitel feststellen konnten, hat Microsoft in Windows Server 2008 zahlreiche Neuerungen integriert, die den produktiven Nutzen des Servers verbessern. In den weiteren Kapiteln dieses Buches gehen wir ausführlich auf diese Funktionen ein und wie diese im produktiven Netzwerk genutzt werden können. Im nächsten Kapitel widmen wir uns der Installation und Aktualisierung auf Windows Server 2008. Auch die Core-Server-Installation und die Aktivierung wird im nächsten Kapitel behandelt.

Kapitel 2

Installation, Treiberverwaltung und Aktivierung

In diesem Kapitel:

In diesem Kapitel gehen wir mit Ihnen die Installation von Windows Server 2008 durch. Die Installation ist sehr ähnlich zur Installation von Windows Vista. Außerdem erfahren Sie, welche ersten Schritte nach der Installation des Servers durchzuführen sind. Windows Server 2008 verwendet, wie auch Windows Vista, ein Image-basiertes Setup. Außerdem ist der Anschluss eines Diskettenlaufwerks an den Server, um beispielsweise gerätespezifische Zusatztreiber für Festplatten- oder Netzwerkadapter zu installieren, nicht mehr erforderlich. Windows Server 2008 kann Treiberdateien direkt von CD-ROM oder von einem USB-Stick einbinden. Installieren Sie Windows Server 2008 neu oder möchten Sie eine bereits vorhandene Windows Server 2003-Installation löschen und Windows Server 2008 neu installieren, legen Sie am besten die Windows Server 2008-DVD in Ihr DVD-Laufwerk ein, stellen sicher, dass im BIOS das Booten von DVD/CD erlaubt ist, und booten von der DVD. Im Anschluss startet der Installationsassistent, mit dessen Hilfe Sie die Installation durchführen können. Diese Oberfläche basiert auf Windows PE 2.0 (siehe auch Kapitel 16), einen textorientierten Teil gibt es nicht mehr. Hier noch einige wichtige Hinweise, die Sie vor der Installation beachten sollten:

- Sie sollten Windows Server 2008 nur auf Servern mit mindestens 512 MB Arbeitsspeicher, besser 1 GB und mehr installieren, abhängig vom Nutzungszweck des Servers. Bei dem Server sollte es sich um ein aktuelles Modell handeln, mit mindestens einem 3 GHz-Prozessor.

HINWEIS Microsoft empfiehlt, vor der Installation eine eventuell vorhandene unterbrechungsfreie Stromversorgung (USV) vom Server zu trennen. Damit ist nicht der Stromanschluss an die USV gemeint, sondern ein eventuell vorhandener serieller oder USB-Anschluss, über den die USV gesteuert werden kann. Windows Server 2008 versucht während der Installation über eine solche serielle Schnittstelle auf das Gerät zuzugreifen, womit einige USVs mangels Kompatibilität Probleme haben.

- Sie sollten auf der Festplatte, auf der Sie Windows Server 2008 installieren, mindestens 10 GB freien Festplattenplatz haben, besser deutlich mehr. Das gilt auch für Testumgebungen.
- Außerdem muss die Partition als aktiv und primär konfiguriert sein (siehe Kapitel 5). Wenn Sie vorher von dieser Partition auch Windows Server 2003 gestartet haben, sollten keine Probleme auftauchen.
- Vermeiden Sie Partitionierungstools von Drittherstellern, die nur für Windows XP oder Windows Server 2003 konzipiert sind.
- Achten Sie darauf, wenn Sie die 64-Bit-Version von Windows Server 2008 installieren, dass Sie in diesem Fall auch 64-Bit-kompatible Programme und 64-Bit-kompatible Treiber benötigen. Viele Hardware-Hersteller bieten derzeit noch keine 64-Bit-Treiber an.
- Sie können testweise Windows Server 2008 x64 parallel zu Windows Server 2008 32 Bit x86 installieren, benötigen dazu aber zwei Partitionen. Achten Sie bei der Erstellung der ersten Partition auf diesen Sachverhalt. Die 64-Bit-Version ist nicht zwingend schneller, vor allem wenn die installierten Applikationen nicht für den 64-Bit-Einsatz optimiert sind.

Neuinstallation des Servers

Für eine Neuinstallation von Windows Server 2008 legen Sie zunächst die Boot-DVD ein, booten den Server mit dieser DVD und wählen den Start der Installation aus. Anschließend öffnet sich die Installationsoberfläche, die sich ähnlich zu Windows Vista verhält. Wählen Sie die notwendigen Daten aus und klicken Sie auf *Weiter*, um die Installation fortzusetzen (Abbildung 2.1).

Abbildg. 2.1 Startfenster der Installation von Windows Server 2008

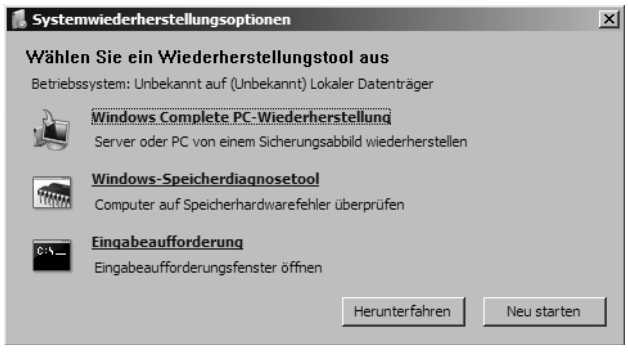
Die Installation von Windows Server 2008 findet bereits beim Starten in einer grafischen Oberfläche statt, es gibt keinen textorientierten Teil mehr. Die Installation von Windows Server 2008 ist weit weniger aufwändig, als noch unter Windows Server 2003. Es gibt weniger Fenster und es sind weniger Eingaben für die Installation erforderlich. Außerdem werden die meisten Eingaben bereits vor Beginn der Installation durchgeführt, sodass der Server während der Installation nicht die ganze Zeit beaufsichtigt werden muss. Sie benötigen für die Installation ein bootfähiges DVD-Laufwerk.

Abbildg. 2.2 Starten der Installation oder auswählen der Computerreparaturoptionen

Auf der nächsten Seite des Assistenten können Sie neben dem Fortführen der Installation die *Computerreparaturoptionen* aufrufen, um eine vorhandene Windows Server 2008-Installation zu reparieren. Dazu werden verschiedene Reparaturprogramme zur Verfügung gestellt. Klicken Sie auf die Schaltfläche *Jetzt installieren*, um die Installation fortzusetzen (Abbildung 2.2).

Klicken Sie auf *Computerreparaturoptionen*, können Sie entweder eine Eingabeaufforderung starten, um ein bestehendes Betriebssystem zu reparieren, oder Sie können den Arbeitsspeicher des Servers testen.

Abbildg. 2.3 Starten der Systemwiederherstellungsoptionen



Außerdem können Sie ein Image des Servers aus einer Sicherung mit der Funktion *Windows Complete PC-Wiederherstellung* wieder über den Server installieren. Um einen Server neu zu installieren, gehen Sie auf die nächste Seite des Assistenten und geben die Seriennummer ein.

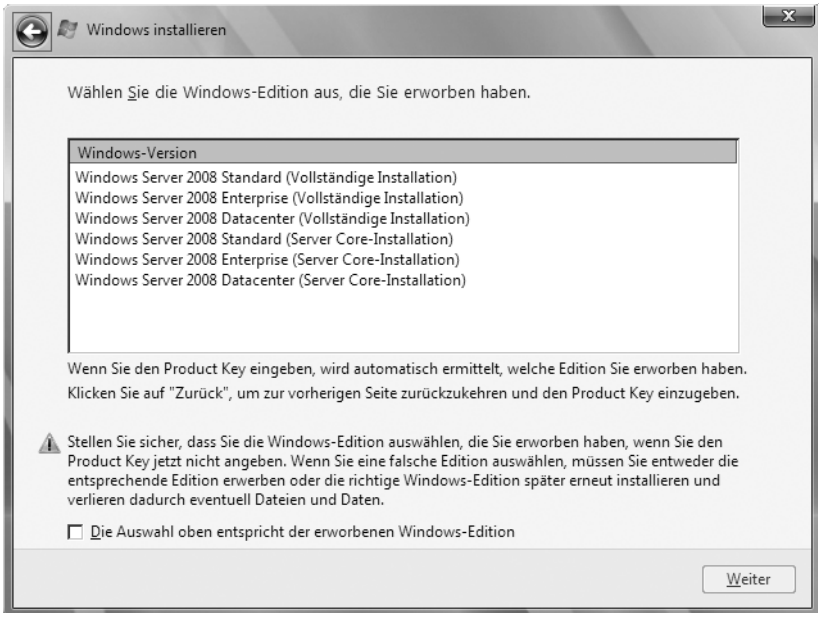
Abbildg. 2.4 Weiterführen der Installation und Eingabe des Produktschlüssels

Es ist nicht notwendig, dass Sie die Bindestriche zwischen den einzelnen Abschnitten abtippen, diese werden automatisch hinzugefügt. Unter Umständen kann es vorkommen, dass der deutsche Tastaturtreiber noch nicht richtig installiert wurde. In diesem Fall sind die Tasten *Y* und *Z* miteinander vertauscht. Wenn in Ihrer Seriennummer diese beiden Zeichen enthalten sind und der Tastaturtreiber die Zeichen nicht richtig angibt, wird die Seriennummer nicht übernommen. Verwenden Sie dann einfach die Taste [Z] für das *Y* und umgekehrt. Neben dem Eingabefeld der Seriennummer wird ein kleines blaues Symbol einer Tastatur angezeigt. Klicken Sie auf das Symbol, öffnen sich eine Bildschirmtastatur und Sie können die Seriennummer auch durch Klicken mit der Maus eingeben. Sie können noch das Kontrollkästchen *Windows automatisch aktivieren, wenn eine Internetverbindung besteht* aktivieren oder nicht aktivieren, das spielt keine Rolle. Bei den meisten Servern wird nach der Installation ohnehin keine Internetverbindung bestehen, da erst die Netzwerkverbindung eingerichtet werden muss.

Sie müssen aber nicht zwingend eine Seriennummer eingeben und können dadurch auf der nächsten Seite des Assistenten festlegen, welche Version von Windows Server 2008 installiert werden soll. In diesem Fall müssen Sie aber spätestens nach 60 Tagen eine gültige Seriennummer für eine Windows Server 2008-Lizenz eintragen. Es besteht aber die Möglichkeit diesen Testzeitraum mit dem Befehl slmgr.vbs -rearm auf bis zu 240 Tage zu verlängern, nachdem die erste Testphase abgelaufen ist, doch dazu später mehr.

Durch diese Funktion haben Sie die Möglichkeit, eine Testumgebung mit einer anderen Windows Server 2008-Lizenz zu testen, also zum Beispiel auch der Enterprise-Edition oder des Webservers. Die Seriennummer kann jederzeit nachträglich eingetragen werden. Wir zeigen Ihnen diese Vorgehensweise im Abschnitt »Aktivierung von Windows Server 2008« weiter hinten in diesem Kapitel.

Abbildg. 2.5 Geben Sie keine Seriennummer während der Installation ein, können Sie die Testversion aus allen Editionen auswählen



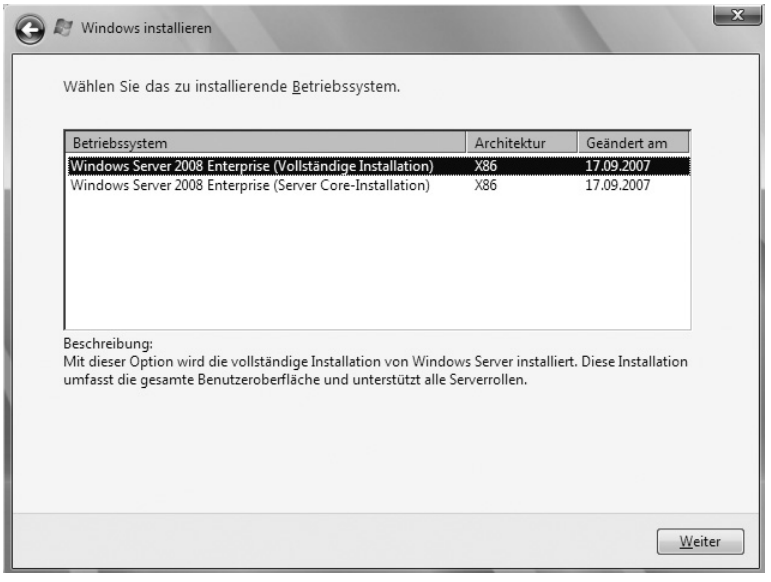
Haben Sie die Seriennummer eingetragen, gelangen Sie mit *Weiter* zur nächsten Seite des Setup-Assistenten, auf der Sie die Installationsvariante festlegen (Abbildung 2.6). Falls Sie die *Server Core-Installation* auswählen, erhalten Sie ein Betriebssystem, das bis auf rudimentäre Anzeigen, wie zum Beispiel Task-Manager und Windows Editor (*Notepad.exe*), komplett ohne grafische Benutzeroberfläche auskommt und in der Befehlszeile verwaltet wird. Wir kommen zu den einzelnen Funktionen dieser Neuheit noch ausführlicher in diesem und den nächsten beiden Kapiteln zu sprechen. Wird diese Variante ausgewählt, findet die gesamte Installation und Konfiguration über die Befehlszeile in einer Eingabeaufforderung oder von einem Remoteserver aus statt. Mit dieser Version steht Ihnen eine kompakte Servervariante zur Verfügung. Ein Core-Server ermöglicht auf diese Weise den Betrieb von Systemen, die als DHCP- und DNS-Server, Domänencontroller oder Dateiserver konfiguriert sind. Bei Bedarf können noch ausgewählte optionale Features wie Datensicherung, Failover-Cluster, Netzwerklastenausgleich usw. zusätzlich installiert werden. In diesen Fällen werden lediglich die für diese Rollen erforderlichen Systemdateien auf dem Server installiert, wobei die grafische Benutzeroberfläche nicht dazu zählt. Dieser Ansatz bietet mehrere Vorteile: Da nur sehr wenige Dienste zur Verfügung stehen, reduziert sich der Konfigurationsaufwand auf die damit verbundenen Rollen. Des Weiteren gewährt der Core-Modus Hackern und Viren nur minimale Angriffsflächen, was potenzielle Sicherheitsrisiken ebenfalls deutlich verringern kann. Installieren Sie die Core-Variante des Servers, stehen allerdings nicht alle Rollen nach der Installation zur Verfügung (siehe Kapitel 3 und Kapitel 4). Ein Core-Server wird über die Befehlszeile verwaltet und unterstützt nur folgende Serverrollen:

- **Dateiserver** siehe die Kapitel 3, 4 und 6
- **Druckserver** siehe die Kapitel 3, 4 und 6
- **Streaming Media Services** *http://technet2.microsoft.com/windowsserver2008/en/servermanager/streamingmediaservices.mspx*
- **Domänencontroller** siehe die Kapitel 3, 4 und 8
- **Active Directory Lightweight Directory Services** AD LDS, unter Windows Server 2003 ADAM genannt, siehe Kapitel 17
- **DNS-Server** siehe Kapitel 3, 4 und 11
- **DHCP-Server** siehe Kapitel 3, 4 und 11
- **Windows Server Virtualization** (WSV)

Ein Core-Server verfügt über keine grafische Oberfläche, keine Shell, keine Media-Funktionen, keinerlei Zusatzkomponenten, außer den notwendigen Serverdiensten. Die Anmeldemaske sieht allerdings identisch aus, Sie müssen sich nach der Installation über die Tastenkombination Strg + Alt + Entf anmelden. Sobald Sie sich angemeldet haben, sehen Sie nur eine Befehlszeile. Zur Bearbeitung des Servers können Sie den Windows Editor (*Notepad.exe*) öffnen, aber zum Beispiel keinen Windows-Explorer oder Internet Explorer und keinen Registrierungseditor (*Regedit.exe*). Durch diese Funktion können die beschriebenen Standardfunktionen von Windows Server 2008 betrieben werden, ohne dass der Server durch unwichtige Komponenten belastet oder kompromittiert werden kann.

TIPP Über den Befehl *setup /unattend:<Pfad>\unattend.xml* können Sie auch einen Core-Server unbeaufsichtigt installieren. Eine *unattend.xml*-Datei erstellen Sie mit dem Windows System Image Manager aus dem Windows Automated Installation Kit (WAIK). Mehr zu diesem Thema finden Sie in Kapitel 16. Sie können das WAIK kostenlos von der Internetseite *http://www.microsoft.com/downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=de* herunterladen. Speziell für Windows Server 2008 und Windows Vista SP1 gibt es eine neue Version des WAIK.

Abbildg. 2.6 Auswahl der zu installierenden Edition, wenn eine Seriennummer eingegeben wird



Neben der eingeschränkten Möglichkeit der Rolleninstallation, können auf einem Core-Server auch nicht alle Funktionen installiert werden. Ein Core-Server unterstützt nur folgende Funktionen, die nachträglich installiert werden können (siehe die Kapitel 3 und 4):

- Backup
- BitLocker Drive Encryption
- Failover Clustering
- Multipath IO
- Network Load Balancing
- Removable Storage
- Simple Network Management Protocol (SNMP)
- Subsystem for UNIX-based applications
- Telnet client
- Windows Internet Name Service (WINS)

HINWEIS Es gibt keine Möglichkeit von einem Core-Server zu einem normalen Windows Server 2008 zu aktualisieren. Der umgekehrte Weg ist ebenfalls nicht möglich. Es muss immer neu installiert werden.

Auch die Aktualisierung von Windows Server 2003 zu einem Windows Server 2008-Core-Server ist nicht möglich.

Die Anbindung eines Core-Servers an den System Center Configuration Manager 2007 (Nachfolger des Systems Management Server 2003), ist genauso möglich, wie die Anbindung an den Microsoft System Center Operations Manager 2007 über die jeweiligen Agenten der Server, damit der Server überwacht werden kann.

Nachdem Sie ausgewählt haben, ob Sie eine Vollinstallation oder nur die Core-Version installieren wollen, gelangen Sie mit *Weiter* zur nächsten Seite des Assistenten. Hier bestätigen Sie die Lizenzbedingungen (Abbildung 2.7).

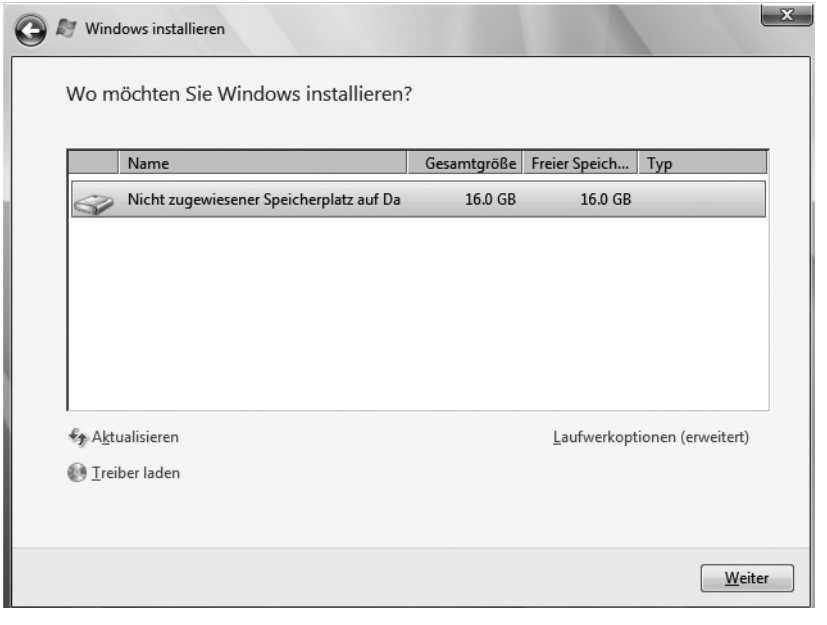
Abbildg. 2.7 Bestätigen der Lizenzbedingungen

Nachdem Sie die Lizenzbedingungen bestätigt haben, gelangen Sie mit *Weiter* zur nächsten Seite des Assistenten. Hier wählen Sie aus, ob Sie einen Windows Server 2003 auf Windows Server 2008 aktualisieren wollen, oder ob Sie eine Neuinstallation durchführen (Abbildung 2.8). Wollen Sie eine Neuinstallation durchführen, klicken Sie auf *Benutzerdefiniert (erweitert)*. Durch diese Auswahl haben Sie auch die Möglichkeit, erweiterte Einstellungen für die Partitionierung durchzuführen. Die Upgrade-Option steht nur dann zur Verfügung, wenn Sie das Setup-Programm aus jener Windows-Installation heraus starten, die Sie aktualisieren wollen. Booten Sie das Windows Server 2008-Installationsprogramm von DVD, können Sie nur die Option *Benutzerdefiniert* auswählen.

Nachdem Sie die Installationsart ausgewählt haben, gelangen Sie zum nächsten Fenster der Installationsoberfläche (Abbildung 2.9). Hier wählen Sie die Partition aus, auf der Windows Server 2008 installiert werden soll. In diesem Fenster können Sie auch zusätzliche Treiber laden, wenn die Controller für die Festplatten nicht erkannt werden. Im Gegensatz zu Windows Server 2003 benötigen Sie diese Treiber nicht mehr in Diskettenform, sondern können diese direkt per CD/DVD oder USB-Stick in die Installation einbinden. Klicken Sie dazu auf den Link *Treiber laden*.

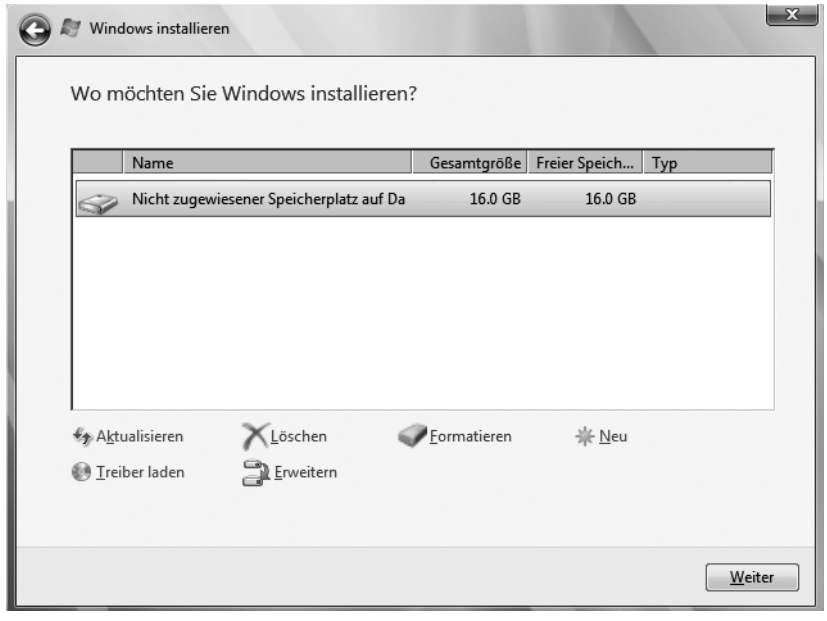
Abbildg. 2.8 Auswählen der Installationsart

Abbildg. 2.9 Auswählen der Partition für die Installation



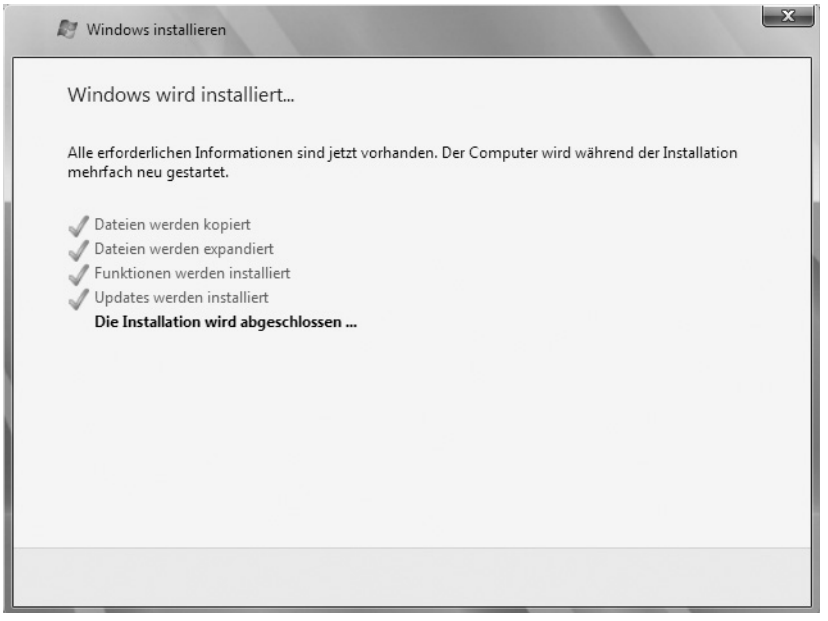
Wollen Sie die Partitionierung ändern oder eine Partition zunächst löschen, klicken Sie auf *Laufwerkoptionen (erweitert)*. In diesem Fall erscheinen weitere Menüs. Mit diesen neuen Optionen können Sie bequem Partitionen auf Ihren Laufwerken erstellen, Partitionen löschen und bestehende Partitionen auf zusätzlichen Festplattenplatz erweitern (Abbildung 2.10).

Abbildg. 2.10 Konfigurieren von Partitionen



Anschließend beginnt die Installation. Diese ist wie bei Windows Vista Image-basiert und kann so deutlich schneller durchgeführt werden, als noch die Installation von Windows Server 2003. Abhängig von der Leistung des Rechners startet die Installationsroutine den Server nach 10 bis 20 Minuten automatisch neu. Sie müssen keine Eingaben machen und keine Taste drücken. Sollten Sie versehentlich eine Taste gedrückt haben und die Installation startet wieder von der DVD, schalten Sie den Rechner aus und starten Sie ihn erneut. Der Computer bootet und es wird ein Fenster geöffnet, über das Sie informiert werden, dass der Rechner für den ersten Start von Windows vorbereitet wird. Lassen Sie den Rechner am besten ungestört weiterarbeiten. Es kann sein, dass der Bildschirm während der Installation der Monitor- und Grafikkartentreiber ein paar Mal flackert oder schwarz wird. Dies ist normal und muss Sie nicht beunruhigen.

Abbildg. 2.11 Die Installation von Windows Server 2008 läuft Image-basiert ab und ist schnell abgeschlossen



Nach der Installation muss zunächst ein Kennwort für den Administrator festgelegt werden. Erst dann ist eine Anmeldung möglich. Bestätigen Sie die Meldung.

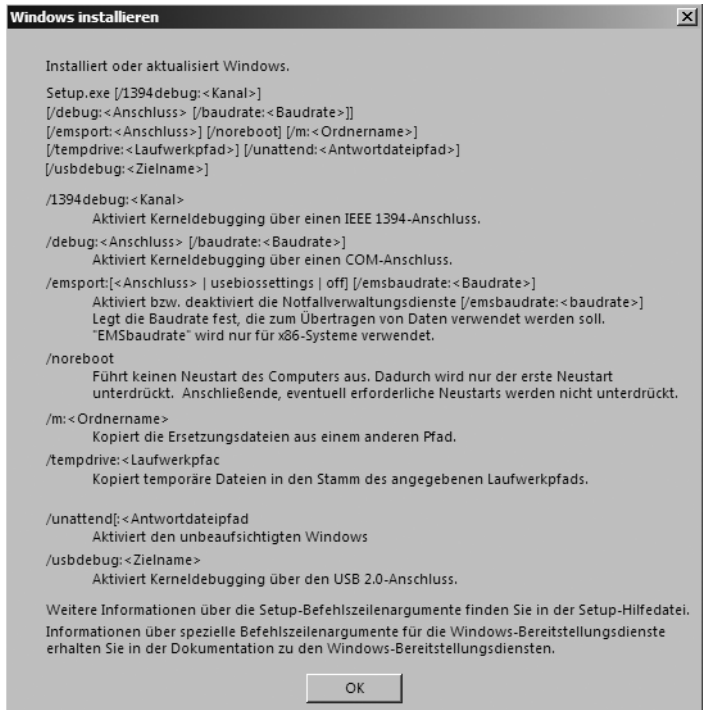
Abbildg. 2.12 Nach der Installation muss zunächst ein Kennwort für das lokale Administratorkonto festgelegt werden

Legen Sie ein Kennwort für den Administrator fest, damit die erste Anmeldung erfolgen kann. Standardmäßig sind bereits die Komplexitätsvoraussetzungen für Kennwörter aktiviert und müssen beachtet werden. Im Kennwort sollten daher auch Zeichen und Zahlen berücksichtigt werden. Sie werden daraufhin angemeldet und können mit den ersten Schritten zur Serverkonfiguration beginnen.

Verschiedene Startoptionen des Windows Server 2008-Setup-Programms

Wenn Sie die Installation von Windows Server 2008 über die Datei *Setup.exe* auf der DVD starten, können Sie noch zusätzliche Optionen angeben, die das Setup-Verhalten beeinflussen. Diese Optionen können Sie zum Beispiel auch verwenden, wenn Sie einen Windows Server 2003-Computer aktualisieren. Die Syntax des Befehls lautet folgendermaßen:

Abbildg. 2.13 Setup-Optionen der Windows Server 2008-Installation



Im Folgenden sind lediglich jene Optionen aufgeführt, die von den meisten Anwendern tatsächlich verwendet werden:

- **/m:<Ordnername>** Legt fest, dass Treiber erst aus diesem Verzeichnis installiert werden sollen
- **/tempdrive:<Laufwerkspfad>** Laufwerk und Pfad, auf dem temporäre Dateien abgelegt werden sollen
- **/unattend:<Antwortdatei>** Die Installation wird ohne Benutzereingaben durchgeführt. Alle Benutzereingaben werden von der Antwortdatei bezogen.

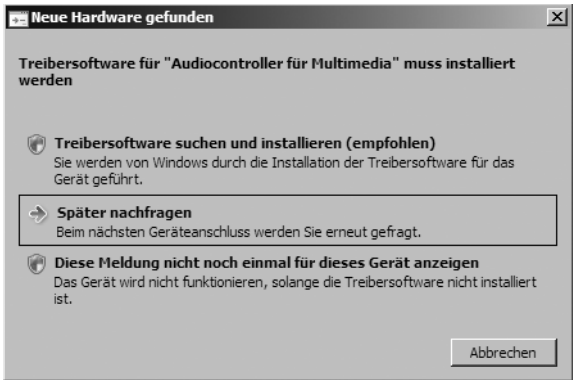
Treiber und Hardware installieren und verwalten

Auch wenn Windows Server 2008, wie alle neuen Betriebssysteme von Microsoft, bereits Treiber für eine Vielzahl von Geräten mitbringt, müssen einige Anwender manuell ins System eingreifen, um die Treiber anzupassen oder neue Treiber zu installieren. Ein Gerät, das an den PC angeschlossen ist, funktioniert erst dann, wenn es Windows bekannt gemacht wurde und im Geräte-Manager angezeigt wird. Sie sollten aus Performance- und Stabilitätsgründen immer die wichtigsten Treiber, also Chipsatz, Grafikkarte und Netzwerkkarte direkt vom jeweiligen Hersteller herunterladen und verwenden. Diese Treiber sind meist besser an das System angepasst, als jene, die das Betriebssystem mitbringt. Sie finden die entsprechenden Treiber entweder auf den Herstellerseiten oder übersichtlicher unter den folgenden Internetadressen:

- www.heise.de/ct/treiber
- www.treiber.de

Sobald Sie eine neue Komponente mit dem Server verbinden, startet der Assistent für die Installation von Hardware. Kann Windows keinen Treiber finden, erhalten Sie ein Informationsfenster angezeigt, über das Sie auswählen können, wie Windows mit der Komponente verfahren soll (Abbildung 2.14).

Abbildg. 2.14 Installieren von neuer Hardware



In diesem Fenster stehen Ihnen drei Optionen zur Verfügung:

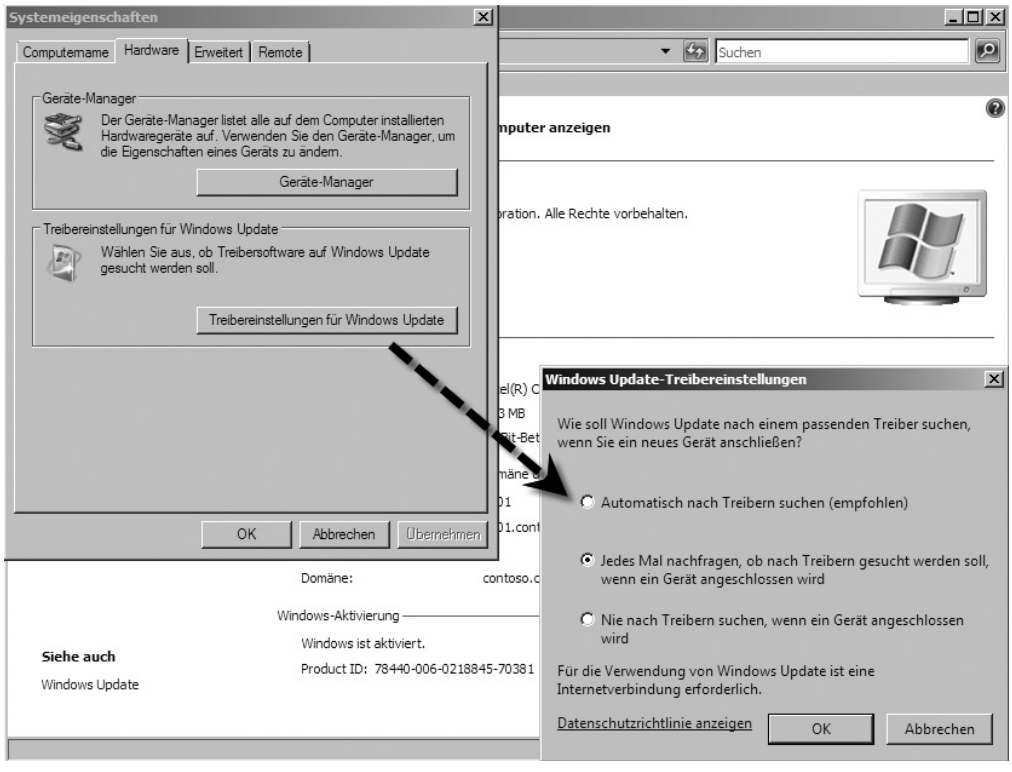
- Treibersoftware suchen und installieren (empfohlen)
- Später nachfragen
- Diese Meldung nicht noch einmal für dieses Gerät anzeigen

Neben den beiden Optionen *Treibersoftware suchen und installieren* und *Diese Meldung nicht noch einmal für dieses Gerät anzeigen* wird ein Schutzschild in den Windows-Farben angezeigt. Dieses Schild wird in Windows Server 2008 an jeder Stelle angezeigt, an dem administrative Berechtigungen im System notwendig sind. Wählen Sie die Option *Treibersoftware suchen und installieren* aus, versucht Windows noch einmal einen passenden Treiber zu installieren. Wird kein interner Treiber gefunden, werden Sie aufgefordert, Windows einen Treiber bereitzustellen. Laden Sie in diesem Fall einen passenden

Treiber aus dem Internet beim Hersteller des Gerätes herunter. Achten Sie aber darauf, möglichst einen Windows Server 2008-Treiber zu verwenden. Windows Server 2008 kommt zwar auch teilweise mit Windows Server 2003-Treibern zurecht, diese sollten aber aus Performance- und Stabilitätsgründen nur dann verwendet werden, wenn kein Windows Server 2008-Treiber zur Verfügung steht. Wählen Sie die Option *Später nachfragen* aus, wird kein Treiber installiert und es werden auch keine weiteren Warnungen gezeigt. Erst beim nächsten Systemstart oder dem Suchen von neuer Hardware werden Sie erneut dazu aufgefordert, einen Treiber bereitzustellen. Verwenden Sie die Option *Diese Meldung nicht noch einmal für dieses Gerät anzeigen*, wird das Gerät in Windows als nicht aktiv gekennzeichnet und kann daher nicht verwendet werden. Sie werden später auch nicht gefragt, ob Sie einen Treiber installieren wollen. Es erscheint eine Meldung, die Sie darauf hinweist, dass das Gerät nicht verwendet werden kann. Für die weiteren Aktionen mit dieser neuen Hardware wird der Geräte-Manager verwendet, den wir im nächsten Abschnitt ausführlicher besprechen.

TIPP Wenn in Windows Server 2008 kein Treiber für eine Hardwarekomponente enthalten ist und Sie auch keinen Treiber auf der Herstellerseite finden, haben Sie unter Umständen Chancen, bei einem Windows-Update über das Internet einen Treiber zu finden. Ein manuelles Windows-Update können Sie zum Beispiel im Internet Explorer über *Extras/Windows Update* starten.

Abbildg. 2.15 Konfigurieren des automatischen Treiber-Downloads über Windows-Update



Die Konfiguration des Downloads von Treibern über Windows-Update kann über *Start/Systemsteuerung/System/Erweiterte Systemeinstellungen*, Registerkarte *Hardware*, Schaltfläche *Treibereinstellungen für Windows Update* gesteuert werden (Abbildung 2.15). Über die gleiche Registerkarte können Sie auch den Geräte-Manager starten. Zu dieser Registerkarte gelangen Sie auch, wenn Sie mit der rechten Maustaste im Startmenü oder dem Desktop auf *Computer* klicken und *Eigenschaften* auswählen. Das *Computer*-Symbol kann nach einen Klick mit der rechten Maustaste darauf und der Auswahl des Eintrags *Auf dem Desktop anzeigen* im Kontextmenü auf dem Desktop angezeigt werden.

TIPP Die 64-Bit-Versionen von Windows Server 2008 benötigen signierte Treiber. Installieren Sie nicht signierte Treiber direkt oder über eine Anwendung, startet unter Umständen der Server nicht mehr. Drücken Sie in diesem Fall beim Starten die F8-Taste und wechseln Sie zu den erweiterten Bootoptionen. Hier kann die Erzwingung der Signierung von Treibern deaktiviert werden. Nach der Deaktivierung sollte sich der Server starten lassen. Allerdings ist dieser Vorgang bei produktiven Servern nicht empfohlen.

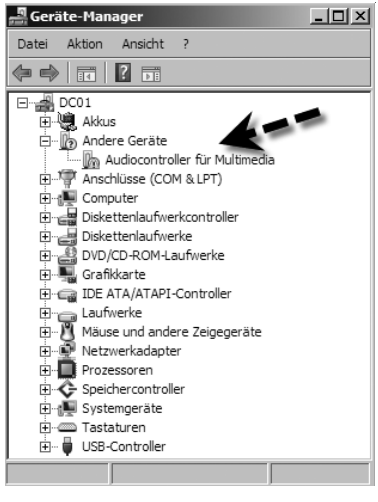
Der Geräte-Manager

Neue Treiber, installierte Hardware und auch die Fehlerbehebung von Treibern und Hardware werden über den Geräte-Manager integriert und verwaltet. Der Geräte-Manager kann über verschiedene Wege gestartet werden:

- Sie können über *Start/Ausführen/devmgmt.msc* den Geräte-Manager starten.
- Eine weitere Variante ist der Aufruf des Kontextmenübefehls *Eigenschaften* zum *Computer*-Symbol im Startmenü.

Der Geräte-Manager sollte nach der Installation alle Hardwarekomponenten des Computers in der entsprechenden Kategorie anzeigen. Wenn ganz oben im Geräte-Manager noch einzelne Geräte als *Andere Geräte* angezeigt werden, können diese in Windows Server 2008 nicht verwendet werden. Erst wenn ein Treiber für die Komponente installiert ist und Windows diesen akzeptiert, lässt sich das entsprechende Gerät verwenden (Abbildung 2.16).

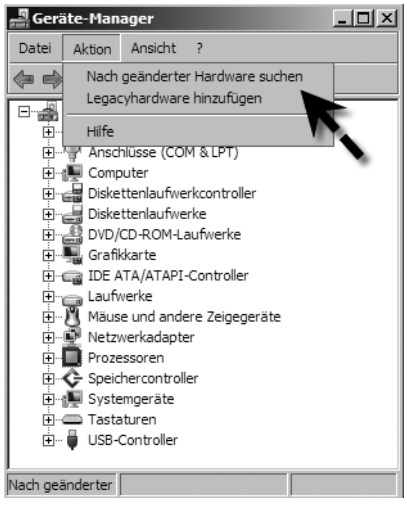
Abbildg. 2.16 Geräte ohne installierten Treiber werden unter *Andere Geräte* aufgeführt



Im Geräte-Manager nach neuer Hardware suchen

Normalerweise beginnt Windows Server 2008 automatisch einen Treiber zu installieren oder anzufordern, wenn ein Gerät mit dem Computer verbunden wird. In manchen Fällen startet diese Suche allerdings nicht automatisch. Trifft das bei Ihnen zu, können Sie im Geräte-Manager den Namen Ihres Computers ganz oben im Navigationsbereich auswählen und anschließend in der Symbolleiste des Geräte-Managers die Schaltfläche *Nach geänderter Hardware suchen* anklicken. Alternativ starten Sie diese Aktion auch über den Menübefehl *Aktion/Nach geänderter Hardware suchen* (Abbildung 2.17). Sobald Sie diese Aktion gestartet haben, beginnt der Installationsassistent nach neuer Hardware zu suchen und installiert entweder automatisch einen Windows-Treiber oder fordert Sie auf, einen Treiber bereitzustellen.

Abbildg. 2.17 Neue Hardware in den Geräte-Manager integrieren



TIPP Über den Befehl *driverquery* in der Befehlszeile wird eine Liste aller aktuell geladenen Treiber angezeigt. Mit dem Befehl *driverquery >c:\treiber.txt* werden alle Treiber in die Textdatei *treiber.txt* geschrieben, die Sie mit Windows Editor (*Notepad.exe*) bearbeiten und überprüfen können.

Verwalten der einzelnen Hardware-Komponenten im Geräte-Manager

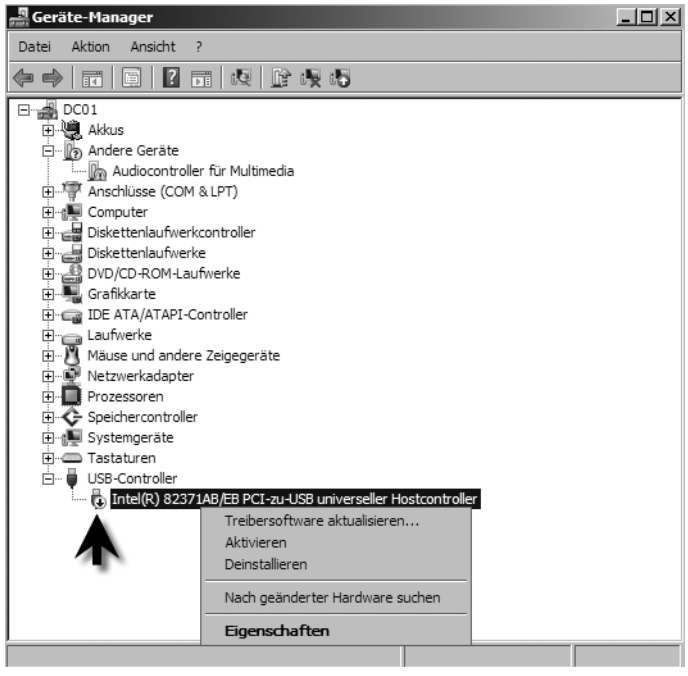
Um eine Komponente zu entfernen, markieren Sie diese und drücken die Entf-Taste. Alternativ können Sie das Gerät auch mit der rechten Maustaste anklicken und im Kontextmenü den Eintrag *Deinstallieren* wählen oder die entsprechende Schaltfläche im Geräte-Manager anklicken, die angezeigt wird, sobald ein Gerät markiert ist. Nachdem Sie die Deinstallation des Gerätes veranlasst haben, erscheint ein Warnfenster mit dem Hinweis, dass das Gerät entfernt wird. Bestätigen Sie diese Meldung. Im Anschluss wird das Gerät entfernt und nicht mehr im Geräte-Manager angezeigt.

Deaktivieren von Komponenten

Sie können Komponenten auch deaktivieren. In diesem Fall wird die Komponente weiterhin im Geräte-Manager angezeigt, aber als nicht aktiv markiert. Sie werden nicht dazu aufgefordert, einen Treiber für das Gerät zu installieren. Wenn Sie die Deaktivierung verwenden, erhalten Sie zunächst

eine Warnmeldung, dass das Gerät im Anschluss nicht mehr funktioniert. Nach der Deaktivierung wird das Gerät mit einem entsprechenden Hinweissymbol im Geräte-Manager versehen. Deaktivierte Geräte können jederzeit wieder aktiviert werden, indem Sie die Komponente im Geräte-Manager mit der rechten Maustaste anklicken und im zugehörigen Kontextmenü den Eintrag *Aktivieren* auswählen.

Abbildg. 2.18 Deaktivieren von Geräten im Geräte-Manager



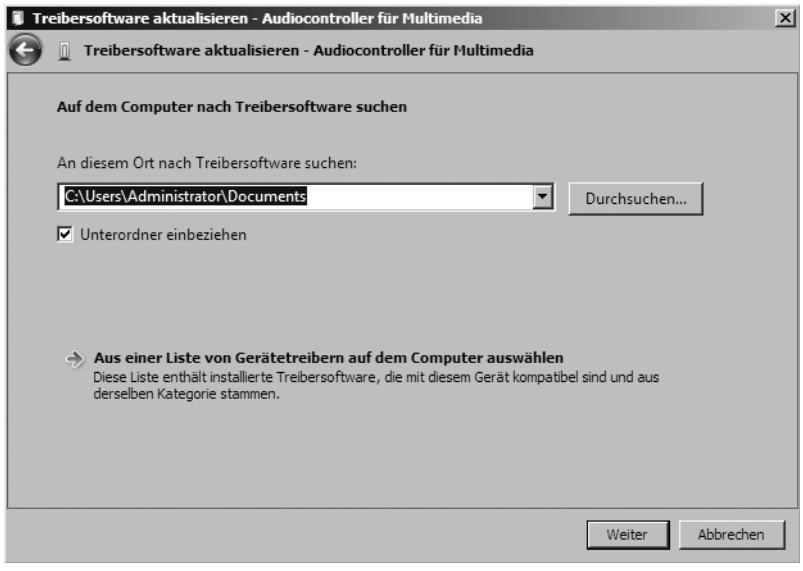
Treiber aktualisieren

Sie können im Kontextmenü zu einem Geräteeintrag die Option *Treibersoftware aktualisieren* auswählen. Im Anschluss werden Sie aufgefordert, die Option für die Aktualisierung des Treibers zu wählen. Auch wenn die Hardwarekomponente in Windows Server 2008 erkannt und der Treiber ordnungsgemäß installiert wurde, sollten Sie für wichtige Komponenten wie Netzwerkkarte, Controller oder auch Drucker möglichst einen aktuellen Treiber verwenden. Zwei Möglichkeiten stehen Ihnen zur Auswahl:

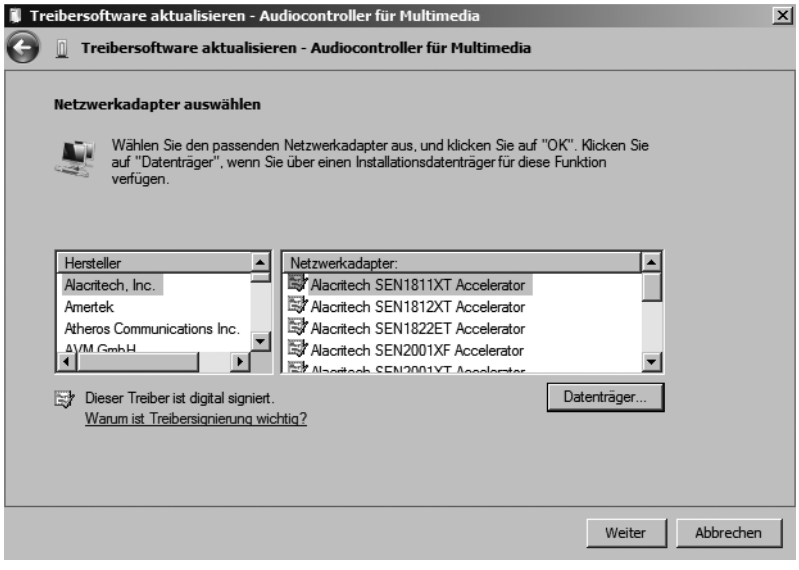
- Automatisch nach aktueller Treibersoftware suchen
- Auf dem Computer nach Treibersoftware suchen

Wenn Sie den Treiber beim Hersteller heruntergeladen haben, sollten Sie die Option *Auf dem Computer nach Treibersoftware suchen* verwenden, da die automatische Suche auch nur nach internen Treibern fahndet. Wenn Sie den Speicherplatz des Treibers kennen, ist die manuelle Installation immer der bessere Weg. Viele Hersteller bieten eigene Installationsroutinen für ihre Treiber. Diese müssen nur noch selten über den Geräte-Manager installiert werden, sondern lassen sich bequem über ein eigenständiges Setup-Programm einrichten. Haben Sie die Option *Auf dem Computer nach Treibersoftware suchen* ausgewählt, erscheint ein neues Fenster, in dem Sie den Pfad zum Treiber auswählen.

Abbildg. 2.19 Aktualisieren eines Treibers



Abbildg. 2.20 Auswählen des Gerätetyps für die Aktualisierung des Treibers



Auch hier stehen Ihnen verschiedene Möglichkeiten zur Verfügung (Abbildung 2.19). Sie können entweder den Ordner und dazugehörigen Unterordner auswählen, in dem sich der Treiber befinden soll, oder aus einer Liste auswählen. Normalerweise verwenden Sie diese Option zur Installation und wählen den Ordner aus, in dem Sie den Treiber gespeichert haben. Wenn Sie auf die Option *Aus einer Liste von Gerätetreibern auf dem Computer auswählen* klicken, öffnet Windows Server 2008 ein neues Fenster, in dem Sie den Hersteller und das genaue Produkt auswählen können (Abbildung 2.20). Ist das

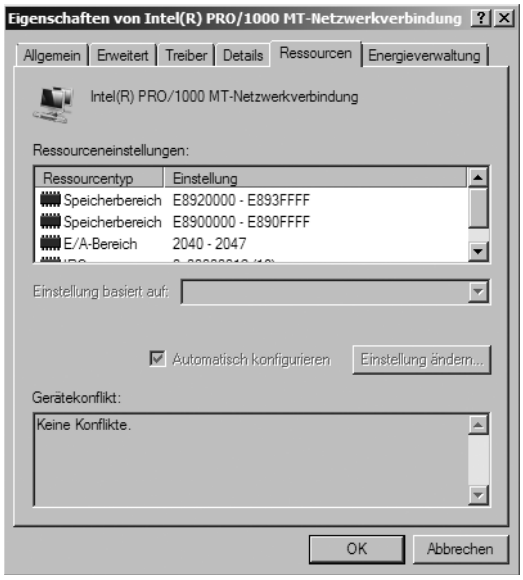
Kontrollkästchen *Kompatible Hardware anzeigen* aktiviert, werden nur die Treiber angezeigt, die mit dem Gerät kompatibel sind. Über die Schaltfläche *Datenträger* können Sie direkt einen Treiber auswählen. Diese Option ist dann sinnvoll, wenn Sie über die Suche in einem Verzeichnis keinen Erfolg haben. Sie können über diese Schaltfläche bis zur **.inf*-Datei des Treibers navigieren und diesen zur Installation auswählen. Nachdem Sie den Treiber ausgewählt haben, werden die notwendigen Treiberdateien automatisch mit den jeweils zutreffenden Einstellungen installiert.

Nach der Auswahl wird das Gerät in der Treiberauswahl angezeigt. Markieren Sie das passende Gerät und klicken Sie auf *Weiter*. Anschließend beginnt Windows mit der Installation.

Eigenschaften von Hardwarekomponenten verwalten und Treiber reparieren

Neben der Installation neuer Hardware und der Aktualisierung von Treibern können Sie auch die Eigenschaften der einzelnen Hardwarekomponenten im Geräte-Manager verwalten. Um die Eigenschaften des Treibers bzw. des Geräts aufzurufen, klicken Sie im Geräte-Manager das betreffende Gerät mit der rechten Maustaste an und rufen im Kontextmenü den Eintrag *Eigenschaften* auf. Anschließend können Sie auf mehreren Registerkarten (abhängig vom Gerät) das Gerät verwalten (Abbildung 2.21). Auf der Registerkarte *Allgemein* werden einige Informationen über das Gerät und dessen Status angezeigt. Diese Informationen sind weniger wertvoll. Auf den Registerkarten *Details* und *Ressourcen* (sofern vorhanden) können Sie weitere Informationen über die Komponente und die einzelnen Bereiche des Gerätes abfragen. Diese Informationen werden allerdings eher selten gebraucht und wenn überhaupt, nur dann, wenn ein Problem mit dem Gerät auftritt. Durch die Plug & Play-Funktionalitäten in Windows Server 2008 werden alle Ressourcen automatisch zugewiesen, sodass ein manuelles Eingreifen nur selten notwendig ist. Konflikte treten dann auf, wenn das automatische Erkennen und die Installation von Treibern fehlschlagen und Windows ein- und dieselbe Ressource mehreren Geräten zuweist. Da die meisten aktuellen Geräte ebenfalls Plug & Play unterstützen und notwendige Informationen bei der Verbindung an Windows schicken, sollten keine Probleme auftreten. Windows untersucht bei der Anbindung eines neuen Gerätes zwei Informationen, die vom angeschlossenen Gerät übermittelt werden. Auf Basis dieser Informationen kann Windows entscheiden, ob ein eigener Treiber installiert werden kann, oder ob der Treiber des Drittherstellers verwendet werden soll. Auch zusätzliche Funktionen der Endgeräte können dadurch aktiviert werden. Diese beiden Informationen zur Installation von Gerätetreibern sind die *Geräte-Identifikations-Strings* und die *Geräte-Setup-Klasse*. Diese Informationen werden benötigt, wenn zum Beispiel die Installation von spezieller Hardware verhindert werden soll. Das kann in Windows Server 2008 und Windows Vista über Gruppenrichtlinien durchgeführt werden (siehe Kapitel 9).

Abbildg. 2.21 Konfigurieren der Eigenschaften eines Gerätes im Geräte-Manager



Geräte-Identifikations-String

Ein Gerät verfügt normalerweise über mehrere *Geräte-Identifikations-Strings*, die der Hersteller festlegt. Dieser String wird auch in der **.inf*-Datei des Treibers mitgegeben. Auf dieser Basis entscheidet Windows, welchen Treiber es installieren soll. Es gibt zwei Arten von Geräte-Identifikations-Strings:

- **Hardware-IDs** Diese Strings liefern eine detaillierte und spezifische Information über ein bestimmtes Gerät. Hier wird der genaue Name, das Modell und die Version des Gerätes als so genannte Geräte-ID festgelegt. Teilweise werden nicht alle Informationen, zum Beispiel die Version, mitgeliefert. In diesem Fall kann Windows selbst entscheiden, welche Version des Treibers installiert wird.
- **Kompatible IDs** Diese IDs werden verwendet, wenn Windows keinen passenden Treiber zum Gerät finden kann. Diese Informationen sind allerdings optional und sehr allgemein. Wenn diese ID zur Treiberinstallation verwendet wird, können zumindest die Grundfunktionen des Geräts verwendet werden.

Windows weist Treiberpaketen einen gewissen Rang zu. Je niedriger der Rang, umso besser passt der Treiber zum Gerät. Der beste Rang für einen Treiber ist 0. Je höher der Rang, umso schlechter passt der Treiber. Mehr Infos zu dieser Technologie finden Sie in diversen Microsoft TechNet-Artikeln auf den Seiten:

- http://go.microsoft.com/fwlink/?LinkID=54881
- http://go.microsoft.com/fwlink/?LinkID=69208
- http://go.microsoft.com/fwlink/?LinkiD=52665
- http://go.microsoft.com/fwlink/?LinkiD=52662

Das neue an Windows Vista und Windows Server 2008 ist, dass diese beiden Informationen nicht nur zur Identifikation des Gerätetreibers verwendet werden können, sondern auch zur Zuweisung

von Richtlinien, über welche die Funktionen und Berechtigungen des Geräts verwaltet werden können (siehe Kapitel 9).

Geräte-Setup-Klasse

Die *Geräte-Setup-Klassen* sind eigene Arten von Identifikations-Strings. Auch auf diesen String wird im Treiberpaket verwiesen. Alle Geräte, die sich in einer gemeinsamen Klasse befinden, werden auf die gleiche Weise installiert, unabhängig von ihrer eindeutigen Hardware-ID. Das heißt, alle DVD-Laufwerke werden auf exakt die gleiche Weise installiert und alle Netzwerkkarten auch. Die Geräte-Setup-Klasse wird durch einen *Globally Unique Identifier (GUID)* angegeben. Vor allem auf der Registerkarte *Details* können Sie über ein Dropdown-Menü ausführliche Informationen abrufen und in Richtlinien verwenden, um neben der Installation von speziellen Geräten auch allgemein die Installation verschiedener Hardware zu unterbinden, zum Beispiel USB-Sticks. Sollten Ressourcen-Konflikte auftreten, können Sie auf der Registerkarte *Ressourcen* einzelne Systemressourcen unter Umständen manuell zuordnen.

Treiberverwaltung im Geräte-Manager

Interessant ist die Registerkarte *Treiber*. Hier stehen verschiedene Optionen zur Verfügung, um den Treiber eines Gerätes zu verwalten oder zu reparieren. Auf dieser Registerkarte können Sie das Datum und die genaue Versionsnummer des Treibers ermitteln. So lässt sich exakt feststellen, ob es mittlerweile einen neueren Treiber für das Gerät gibt, wie der Hersteller des Treibers heißt (ob also der Treiber auch tatsächlich vom Hersteller oder von Microsoft stammt), und ob der Treiber signiert ist. Neben diesen Informationen können Sie auf dieser Registerkarte über die Schaltfläche *Treiberdetails* noch genauere Informationen über jede einzelne Datei des Treibers beziehen. Über die Schaltfläche *Treiber aktualisieren* erhalten Sie die gleichen Möglichkeiten wie im Kontextmenü des Gerätes. Auch die beiden Schaltflächen *Deinstallieren* und *Deaktivieren* haben die gleiche Bedeutung wie im Kontextmenü.

TIPP Wertvoll ist die Schaltfläche *Vorheriger Treiber*. Diese dient dem Zweck der Systemherstellung. Wenn Sie zum Beispiel für eine Netzwerkkarte einen neuen Treiber installieren und feststellen, dass der Computer danach entweder nicht mehr richtig funktioniert oder die Netzwerkverbindung doch nicht so optimal ist, können Sie durch diese Funktion den vorherigen Treiber wiederherstellen. Der neue Treiber wird anschließend wieder vom System entfernt.

Startet nach der Installation des Treibers der Computer überhaupt nicht mehr, können Sie auch die Option *Letzte als funktionierend bekannte Konfiguration* anstatt des abgesicherten Modus starten, wenn beim Start des Computers F8 gedrückt wird. In diesem Fall wird der Computer ebenfalls mit dem alten Treiber gestartet und der neue deaktiviert. Diese Option funktioniert aber nur dann, wenn der Computer direkt nach einer Treiberinstallation überhaupt nicht mehr hochfährt.

Weitere Möglichkeiten im Geräte-Manager

Über das Menü *Ansicht* können Sie die Sortierreihenfolge des Geräte-Managers anpassen. Sie können die Standardansicht *Geräte nach Typ* wählen oder nach *Ressourcen nach Verbindungen* suchen lassen. Über den Menüpunkt *Ausgeblendete Geräte anzeigen* lassen sich Komponenten anzeigen, die zwar installiert wurden, aber nicht mehr im System enthalten sind. Dadurch besteht die Möglichkeit, nicht mehr benötigte Gerätetreiber vom Computer zu entfernen, da diese das System unnötig belasten. Wählen Sie den Menüpunkt *Ausgeblendete Geräte anzeigen* aus, werden allerdings nur die

Systemkomponenten angezeigt, die Windows Server 2008 zum Schutz des Systems vor dem Anwender versteckt. Damit auch jene Geräte angezeigt werden, die im System installiert wurden, aber nicht mehr vorhanden sind, müssen Sie den Geräte-Manager über einen speziellen Weg aufrufen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie über *Start/Eingabeaufforderung* ein Befehlszeilenfenster.
2. Tippen Sie den Befehl *set devmgr_show_nonpresent_devices=1* ein.
3. Starten Sie im Fenster der Eingabeaufforderung über den Befehl *start devmgmt.msc* den Geräte-Manager.
4. Rufen Sie den Menübefehl *Ansicht/Ausgeblendete Geräte anzeigen* auf. Sofern ältere Treiber auf dem PC vorhanden sind, werden diese jetzt angezeigt. Diese Gerätesymbole erscheinen transparent.

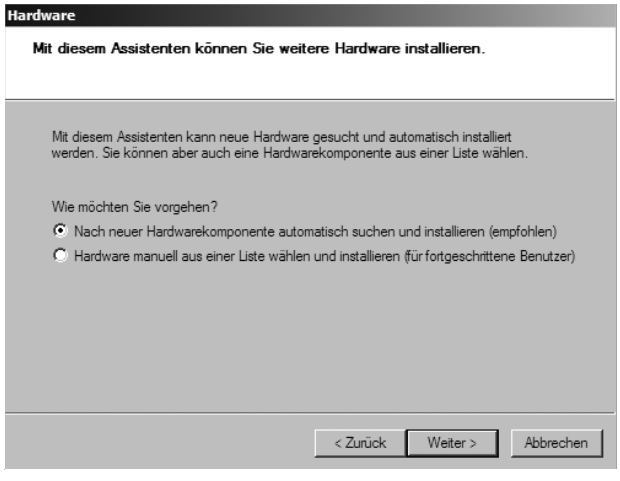
Im Anschluss können Sie nach den nicht mehr benötigen Geräten suchen und diese aus dem Geräte-Manager entfernen.

Ältere Hardware mit dem Geräte-Manager installieren

Manche Unternehmen setzen unter Umständen noch Hardware ein, die kein Plug & Play unterstützt und daher nicht automatisch von Windows installiert werden. Sofern es für diese Geräte einen Windows-Treiber oder einen Treiber des Herstellers gibt, können Sie auch diese in Windows Server 2008 integrieren:

1. Um das Gerät ordnungsgemäß zu installieren, schließen Sie es am Computer an und starten den Geräte-Manager.
2. Markieren Sie im Geräte-Manager den Namen Ihres Computers ganz oben im Baum.
3. Klicken Sie mit der rechten Maustaste auf den Namen des Computers und wählen Sie im Kontextmenü die Option *Legacyhardware hinzufügen*. Daraufhin wird der Assistent gestartet, um die ältere Hardware zu installieren (Abbildung 2.22).
4. Auf der nächsten Seite des Assistenten können Sie auswählen, ob Windows Server 2008 die Hardware automatisch suchen und installieren soll, oder ob Sie die Hardware selbst auswählen möchten. Sie sollten immer zuerst probieren, ob sich die Hardware durch die automatische Suche in Windows finden lässt.

Abbildg. 2.22 Installieren von nicht Plug & Play-fähiger Hardware



5. Wenn das Gerät nicht gefunden werden kann, können Sie anschließend die Option *Hardware manuell aus einer Liste wählen und installieren* wählen. Im nächsten Fenster können Sie dann festlegen, welche Hardware Sie installieren wollen.
6. Nach Auswahl der Hardwarekomponente öffnet sich ein Fenster, in dem Sie den Hersteller und das genaue Gerät auswählen können. Hier haben Sie auch die Möglichkeit, über die Schaltfläche *Datenträger* den Treiber des Gerätes manuell auszuwählen und zu installieren, wenn Sie diesen vom Hersteller direkt bezogen haben.

Aktivierung von Windows Server 2008

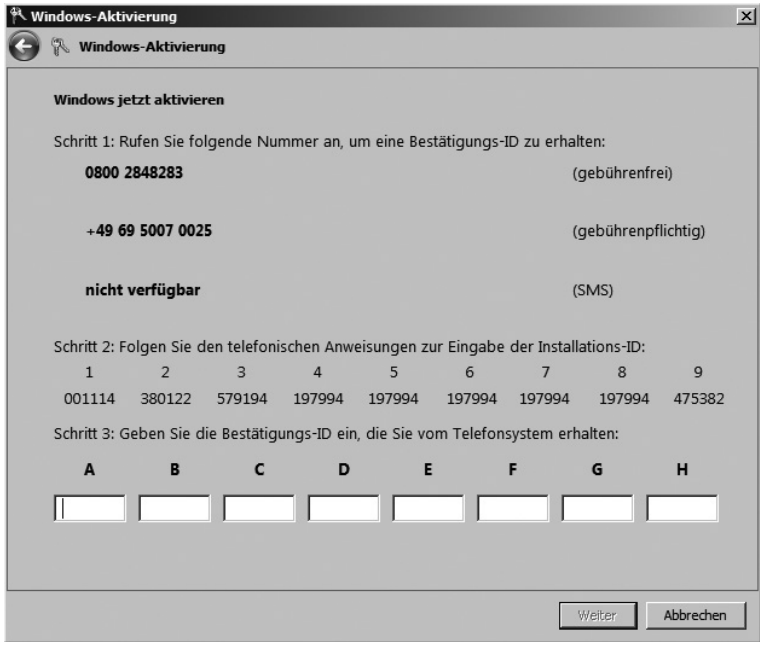
Wird Windows Server 2008 nicht aktiviert bzw. der Testzeitraum nicht verlängert, wird der Betrieb nach 60 Tagen faktisch eingestellt. Sie können Windows Server 2008 entweder über das Internet aktivieren oder per Telefon. Wollen Sie Windows Server 2008 über das Internet aktivieren, sollten Sie zunächst den Server an das Internet anbinden. Dazu muss normalerweise die Netzwerkkonfiguration von Windows Server 2008 durchgeführt werden (siehe Kapitel 7). Ist der Server mit dem Internet verbunden, finden Sie den Aktivierungslink von Windows Server 2008 über *Start/Systemsteuerung/System*. Klicken Sie dazu auf den Link *Aktivieren Sie Windows jetzt*. Im Anschluss öffnet sich das Windows-Aktivierungsfenster. Klicken Sie auf den Link *Windows jetzt online aktivieren*. Bei der Aktivierung per Telefon werden Sie mit einem automatischen Telefonsystem verbunden. Folgen Sie den Anweisungen des Sprachcomputers. Wählen Sie bei der Aktivierung über das Telefon die Option *Andere Aktivierungsmethoden anzeigen*.

TIPP Wenn die Auswahl zur Aktivierung nicht angezeigt wird, schließen Sie alle Fenster und starten Sie die Aktivierung über *Start/Ausführen/slui 0x5*.

Im nächsten Fenster wählen Sie die Option *Automatisches Telefonsystem verwenden* und danach im Listenfeld den Eintrag *Deutschland* aus. Als Nächstes erhalten Sie die zur Aktivierung notwendigen Informationen. Wählen Sie entweder die gebührenfreie Rufnummer *0800-2848283* oder die gebührenpflichtige Rufnummer *069-5007 0025*. Der Telefoncomputer fordert Sie auf, die angegebene Installations-ID anzugeben.

Im Anschluss teilt Ihnen der Telefoncomputer die Zahlenreihenfolge mit, die Sie ganz unten im Fenster eingeben müssen. Wenn Sie eine Zahl nicht verstehen, ist es nicht schlimm, da Sie sich die ganze Zahlenkolonne nochmals vorlesen lassen können. Klicken Sie danach auf *Weiter*, um die Aktivierung abzuschließen. Im Anschluss aktiviert Windows das Betriebssystem auf Basis dieser Nummer. Nach einigen Sekunden wird das Betriebssystem als aktiviert angezeigt und Sie können das Fenster schließen. Sollten Sie Probleme bei der Aktivierung bekommen, überprüfen Sie die Uhrzeit und die Zeitzone Ihres Servers. Sind die entsprechenden Einstellungen nicht korrekt, können Sie Windows nicht aktivieren.

Abbildg. 2.23 Aktivieren von Windows Server 2008



TIPP Sie können das Programm zur Aktivierung auch über *Start/Ausführen/slui* starten. Dieser Weg hilft oft, wenn die herkömmliche Vorgehensweise zur Aktivierung nicht funktioniert. Oft liegt hier ein Problem mit dem Produktschlüssel vor. Über diesen Weg können Sie einen neuen Schlüssel eingeben. Über den Befehl *slui 0x03* wird ein Dialogfeld geöffnet, um einen neuen Produktschlüssel einzugeben, während der Befehl *slui 0x05* die Produktaktivierung startet. Über *slui 0x5* erhalten Sie darüber hinaus noch die Möglichkeit, auch alternative Aktivierungsmethoden auszuwählen.

Weitere Möglichkeit der Anwendung sind:

- **slui.exe 4** Öffnet die Auswahl der Aktivierungshotlines
- **slui.exe 8** Nach diesem Befehl muss Windows Server 2008 sofort neu aktiviert werden.
- **slui.exe 7** Damit aktivieren Sie wieder den Original-Timerwert vor der Option 8.

Slmgr.vbs

Für die Verwaltung und die Abfrage von Lizenzinformationen auf Windows Vista-PCs und Windows Server 2008, stellt Microsoft das Skript *slmgr.vbs* zur Verfügung, welches Sie über *Start/Ausführen* aufrufen können. Diese Optionen für das Lizenzmanagement-Skript *cscript c:\windows\system32\slmgr.vbs* sollten Sie kennen:

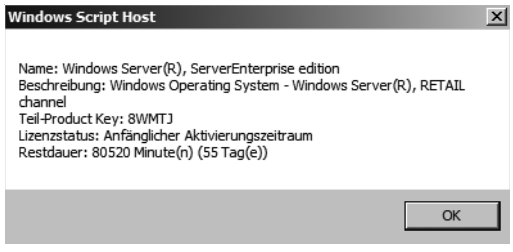
- **–ato** Windows online aktivieren
- **–rearm** Mit dieser Option können Sie den Testzeitraum dreimal verlängern, in denen Sie mit Windows Server 2008 ohne Aktivierung arbeiten können, also von 60 auf bis zu 240 Tage.

- **–dli** Zeigt die aktuellen Lizenzinformationen an
- **–dlv** Zeigt noch mehr Lizenzdetails an
- **–dlv all** Zeigt detaillierte Infos für alle installierten Lizenzen

Status der Aktivierung anzeigen

Möchten Sie den Status der Aktivierung von Windows Server 2008 anzeigen, geben Sie unter *Start/Ausführen* den Befehl *slmgr.vbs –dli* ein, und führen Sie diesen mit einem Klick auf *OK* aus. Anschließend werden der Name und die Beschreibung des Betriebssystems, aber auch ein Teil des Product-Keys und der Lizenzstatus angezeigt (Abbildung 2.24).

Abbildg. 2.24 Abrufen der Aktivierungsinformationen für Windows Server 2008



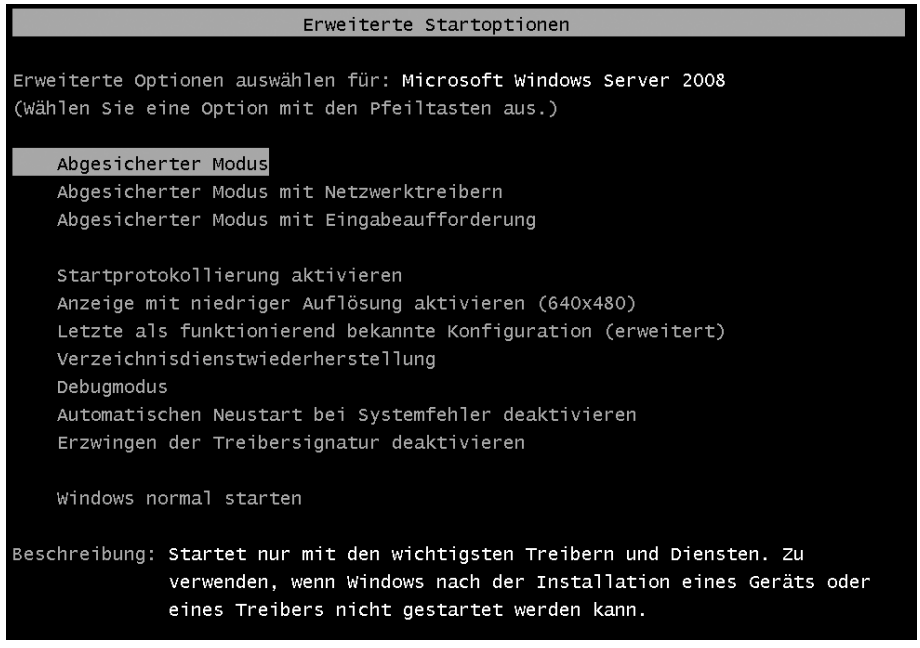
Aktivieren eines Core-Servers

Da ein Core-Server über keine grafische Oberfläche verfügt, müssen Sie einen solchen Server über die Befehlszeile aktivieren. Eine automatische Aktivierung ist für Core-Server nicht möglich. Verwenden Sie zur lokalen Aktivierung des Servers den Befehl *Slmgr.vbs –ato*. Nach Eingabe des Befehls wird die Aktivierung durchgeführt, aber Sie erhalten keine Rückinfo in der Befehlszeile. Sie können einen Windows Server 2008 auch remote über das Netzwerk aktivieren. Verwenden Sie dazu den Befehl *slmgr.vbs <ServerName> <Benutzername> <Kennwort>:–ato.* Um einen Server lokal über das Telefon zu aktivieren, verwenden Sie den Befehl *Slmgr –dti*. Notieren Sie sich die ID, die generiert wird, und rufen Sie die Aktivierungsnummer von Microsoft an. Geben Sie über die Telefontasten die ID ein und Sie erhalten vom Telefoncomputer eine Aktivierungs-ID. Diese geben Sie mit dem Befehl *Slmgr –atp <Aktivierungs-ID>* ein. Mehr zur Aktivierung eines Core-Servers finden Sie in Kapitel 3. Dort gehen wir die ersten Schritte nach der Installation für einen Core-Server ausführlich durch.

Windows Server 2008-Startoptionen

Wenn Windows nicht mehr ordnungsgemäß startet, können Sie beim Starten des Servers mit der Taste F8 die Windows Server 2008-Startoptionen aufrufen, die teilweise bei Startproblemen helfen können. Nach dem Aufruf der erweiterten Startoptionen stehen Ihnen verschiedene Funktionen zur Verfügung. Bei manchen Optionen, wie zum Beispiel im abgesicherten Modus, wird Windows in einem eingeschränkten Zustand gestartet, bei dem lediglich die absolut notwendigen Funktionen verfügbar sind. Werden nicht alle Optionen angezeigt, drücken Sie zunächst auf Entf, bis Windows Server 2008 zum Booten vorgeschlagen wird und dann auf F8.

Abbildg. 2.25 Erweiterte Startoptionen von Windows Server 2008



Falls ein Problem nach dem Starten im abgesicherten Modus nicht mehr auftritt, können die Standardeinstellungen und die Basisgerätetreiber als mögliche Ursache ausgeschlossen werden:

- **Abgesicherter Modus** Startet Windows mit den mindestens erforderlichen Treibern und Diensten. Eine Anbindung an das Netzwerk findet bei diesem Modus nicht statt.
- **Abgesicherter Modus mit Netzwerktreibern** Startet Windows im abgesicherten Modus zusammen mit den für den Zugriff auf das Internet oder auf andere Computer im Netzwerk erforderlichen Netzwerktreibern und -diensten.
- **Abgesicherter Modus mit Eingabeaufforderung** Startet Windows im abgesicherten Modus mit einem Eingabeaufforderungsfenster anstelle der normalen Windows-Benutzeroberfläche.
- **Startprotokollierung aktivieren** Erstellt die Datei *Ntbtlog.txt*, in der alle Treiber aufgelistet werden, die beim Starten installiert werden und für die erweiterte Problembehandlung nützlich sein können.
- **Anzeige mit niedriger Auflösung aktivieren** Startet Windows mithilfe des aktuellen Videotreibers und niedrigen Einstellungen für Auflösung und Aktualisierungsrate. Mithilfe dieses Modus können Sie die Anzeigeeinstellungen zurücksetzen.
- **Letzte als funktionierend bekannte Konfiguration** Startet Windows mit der letzten funktionsfähigen Registrierungs- und Treiberkonfiguration.
- **Verzeichnisdienstwiederherstellung** Mit dieser Option können Sie auf einem Domänencontroller Wiederherstellungsvorgänge durchführen.
- **Debugmodus** Startet Windows in einem erweiterten Problembehandlungsmodus.

- **Automatischen Neustart bei Systemfehler deaktivieren** Verhindert, dass Windows nach einem durch einen Fehler von Windows verursachten Absturz automatisch neu gestartet wird. Wählen Sie diese Option nur aus, wenn Windows in einer Schleife festgefahren ist, die aus Absturz, Neustart und erneutem Absturz besteht.
- **Erzwingen der Treibersignatur deaktivieren** Ermöglicht, dass Treiber mit ungültigen Signaturen installiert werden.
- **Windows normal starten** Startet Windows im normalen Modus.

Normalerweise werden diese Startoptionen nur selten benötigt. Wenn Sie möglichst immer nur aktuelle und kompatible Software installieren, nur signierte Treiber verwenden und nur dann Änderungen am System durchführen, wenn Sie genau wissen, was Sie tun, läuft Windows Server 2008 deutlich stabiler als seine Vorgänger.

Anmeldeprobleme im abgesicherten Modus umgehen

Starten Sie den Server im abgesicherten Modus, kann es unter manchen Umständen passieren, dass die Anmeldung verweigert wird und Sie eine Meldung erhalten, dass der Server nicht aktiviert ist. Dieses Problem können Sie mit dem Hilfsprogramm *msconfig.exe* beheben. Das Problem wird durch den Plug & Play-Dienst verursacht. Gehen Sie zur Behebung des Problems folgendermaßen vor:

1. Starten Sie den Computer im normalen Modus.
2. Geben Sie im Suchfeld des Startmenüs den Befehl *msconfig.exe* ein.
3. Wechseln Sie auf die Registerkarte *Allgemein*.
4. Aktivieren Sie die Option *Diagnosesystemstart.*
5. Klicken Sie auf die Registerkarte *Dienste.*
6. Wählen Sie den Dienst *Plug* & *Play* aus.
7. Klicken Sie auf *OK* und lassen Sie dann den Server neu starten.

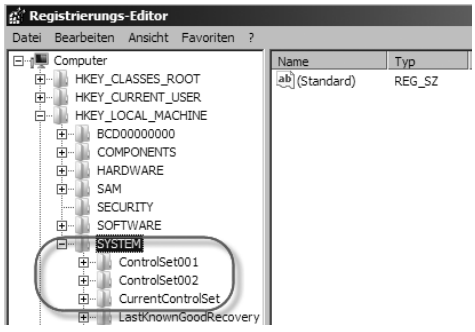
Können Sie den Server nicht neu starten und befinden Sie sich bereits im Diagnosemodus, können Sie einfach Windows im eingeschränkten Modus starten. In diesem Modus wird nur der Internet Explorer ausgeführt. Geben Sie in der Adressleiste den Befehl *%windir%\system32\msconfig.exe* ein und aktivieren Sie auf der Registerkarte *Allgemein* den normalen Systemstart.

Letzte als funktionierend bekannte Konfiguration im Detail

Der abgesicherte Modus und die ergänzenden Startoptionen sind der einfachste Ansatz, um Windows Server 2008 im Fehlerfall neu zu starten. Diese Option ist die erste Wahl, wenn Windows Server 2008 nach einer Konfigurationsänderung nicht mehr startet, da damit auf die Konfiguration zurückgegriffen werden kann, die zuletzt einen korrekten Systemstart erlaubt hat. Erst nach dieser Option sollten die anderen Optionen getestet werden. Die beiden Registry-Unterschlüssel *ControlSet001* und *ControlSet002* sind jeweils Sicherungen der Dienste und Einstellungen, damit in einem Fehlerfall mittels *Letzte als funktionierend bekannte Konfiguration* im abgesicherten Modus wieder gestartet werden kann (Abbildung 2.26).

Unter *HKEY_LOCAL_MACHINE\SYSTEM\Select* sehen Sie, welcher Eintrag gerade aktuell verwendet und in *CurrentControlSet* gespiegelt wird. Zum Beispiel ist der Unterschlüssel *ControlSet001* als *CurrentControlSet* gespiegelt worden. Beim Herunterfahren wird er dann in *ControlSet002* gespiegelt und als *LastKnownGood* eingetragen (Abbildung 2.27) – dieser wird dann genutzt, wenn Sie wie oben beschrieben *Letzte als funktionierend bekannte Konfiguration laden* starten. *ControlSet001* wird dann nicht gelöscht, sondern fortan *ControlSet003* als Sicherung verwendet, was zuvor *ControlSet002* war.

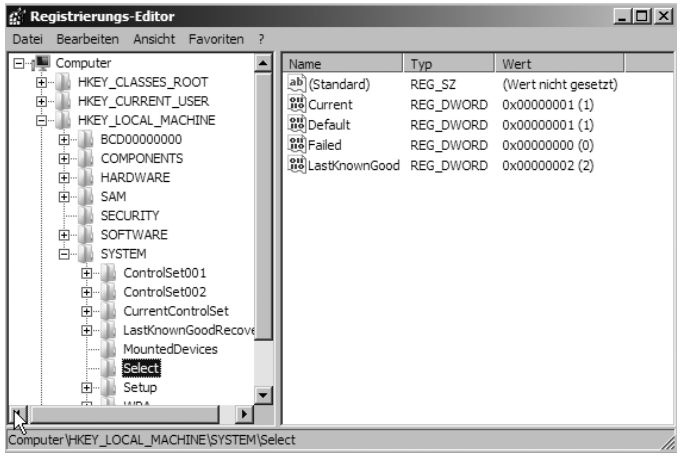
Abbildg. 2.26 Anzeigen der Informationen für die letzte als funktionierend bekannte Konfiguration unter Windows Server 2008



Select-Werte

- **Current** Der Konfigurationsdatensatz, der für einen Systemstart verwendet und dann nach *CurrentControlSet* kopiert wird. Änderungen in der Systemsteuerung oder in der Registrierung werden im Zweig *CurrentControlSet* abgespeichert.
- **Default** Der Konfigurationsdatensatz, der für den nächsten Systemstart verwendet werden soll, wenn kein Fehler auftritt und der Benutzer nicht manuell auf die letzte als funktionierend bekannte Konfiguration zurückgeschaltet hat. Diese Informationen werden beim Herunterfahren gespeichert. In der Regel enthalten die Einträge *Default* und *Current* die gleichen Werte. Der *Default*-Wert kann durch den Wert *LastKnownGood* außer Kraft gesetzt werden.
- **Failed** Dies ist der Konfigurationsdatensatz, mit dem Windows nicht gestartet werden konnte. Hier ist der Wert enthalten, der nach dem Start mit *LastKnownGood* als fehlgeschlagener Wert gekennzeichnet worden ist. Solange Windows problemlos läuft, steht hier der Wert *0*.
- **LastKnownGood** Hier steht die Kopie des Bereiches, der beim letzten erfolgreichen Start von Windows verwendet wurde. Ist die Anmeldung erfolgreich verlaufen, wird *Clone* in den Wert *LastKnownGood* kopiert, also die *Letzte als funktionierend bekannte Konfiguration*.

Abbildg. 2.27 Anzeigen der Registrywerte für die Startoption *Letzte als funktionierend bekannte Konfiguration*

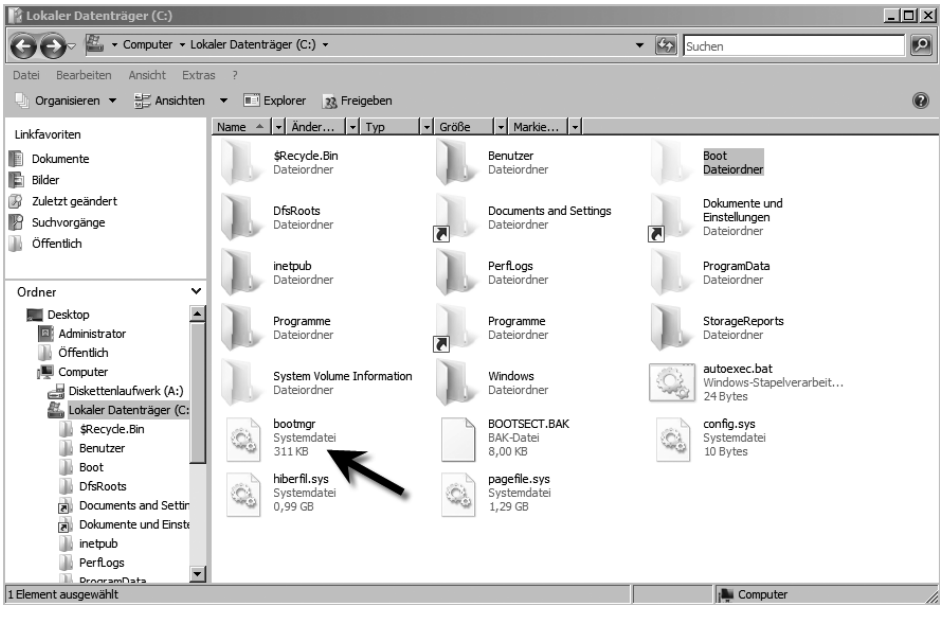


Hat *Current* den Wert *0x1*, zeigt *CurrentControlSet* auf *ControlSet001*. Ist der Wert von *LastKnownGood 0x2* gesetzt, zeigt dieser auf den Steuersatz *ControlSet002*. Für den Start von Windows existieren also stets zwei Sätze – *Default* und *LastKnownGood*. *Clone* ist eine Kopie des *Default*- oder *LastKnownGood*-Wertes, der für die Initialisierung des Rechners verwendet wird.

Anpassen des Bootmenüs – Es gibt keine *boot.ini* mehr

Installieren Sie Windows Server 2008, wird automatisch ein Bootmenü angelegt. Beim Booten wird nicht mehr der unter Windows Server 2003 verwendete NTLDR (NT-Loader) benutzt, sondern das Programm *bootmgr* (Abbildung 2.28). Beide liegen in der Partition, von der aus gebootet wird. Installieren Sie Windows Server 2008 parallel zu Windows Server 2003 und verwenden dazu eine zusätzliche Festplatte, liegen die beiden Dateien im Stammverzeichnis der Festplatte D:. Damit diese Dateien angezeigt werden, müssen Sie im Windows-Explorer zunächst über *Organisieren/Ordner- und Suchoptionen* auf der Registerkarte *Ansicht* das Kontrollkästchen *Geschützte Systemdateien ausblenden* deaktivieren und die Option *Alle Dateien und Ordner anzeigen* im Bereich *Versteckte Dateien und Ordner* aktivieren. Wird im Bootmenü von Windows Server 2008 der Start des älteren Windows-Betriebssystems ausgewählt (also Windows Server 2003), übergibt der Bootmanager (*bootmgr*), den Startvorgang zum NT-Loader (*ntldr*), der dann wiederum die alte Windows-Version startet. Das neue Bootsystem von Windows Server 2008 ist in drei Komponenten aufgeteilt. Es gibt den Windows Bootmanager, die Routine für das Betriebssystem und die Routine zum Fortsetzen von Windows aus dem Ruhezustand, was für einen Server eher selten eine Rolle spielen wird. In Windows Server 2003 wurden diese Aufgaben komplett von *ntldr* erledigt.

Abbildg. 2.28 Der neue Bootmanager in Windows Server 2008



Verwenden von *bcdedit.exe*

bcdedit /?

bcdedit /enum all

bcdedit /export <Dateiname>

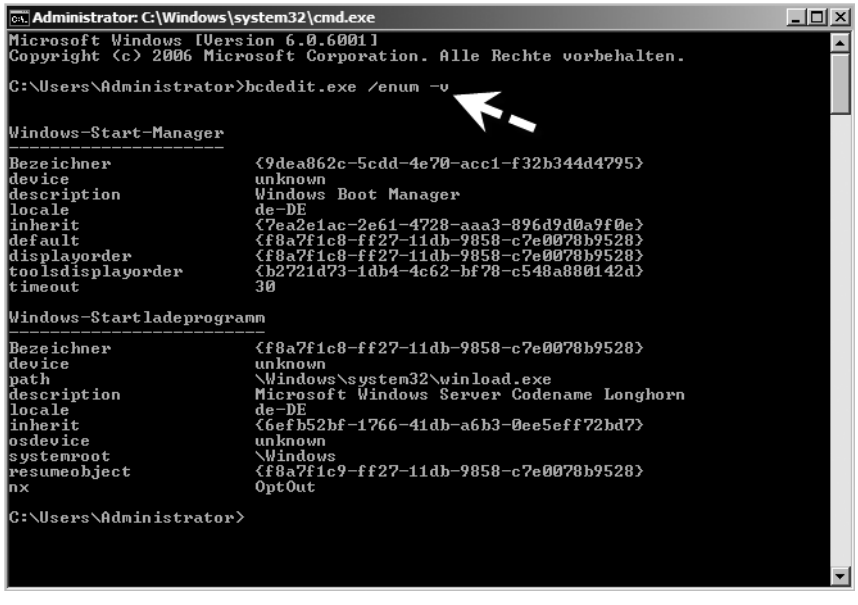
bcdedit /import <Dateiname>

bcdedit /timeout 10

bcdedit /default <Bezeichner> *{current}*

{legacy}

bcdedit /default {legacy}



- Grundsätzlich sollten Optionen mit der *bcdedit /set {GUID} Element Wert* gesetzt werden. Die 32-stellige GUID, die zu ändernde Option und den Wert ersetzen Sie durch den neuen Eintrag. Um zum Beispiel die Anzeigedauer des Boot-Menüs auf 10 Sekunden zu ändern, geben Sie den Befehl *bcdedit /set {9dea862c-5cdd-4e70-acc1-f32b344d4795} timeout 10* ein. Die GUID stimmt bei den meisten Windows Server 2008-Installation mit diesem Beispiel überein. Mit dem Platzhalter *{bootmgr}* erreichen Sie den Windows Server 2008-Bootmanager, mit *{ntldr}* einen eventuell vorhandenen Eintrag für Windows Server 2003 und über *{current}* das aktuell gestartete Betriebssystem. Den Standardeintrag des Bootstores erreichen Sie über *{default}*. Ein Beispiel hierfür wäre *bcdedit /set {bootmgr} timeout 10*. Viele Optionen sind direkt als Parameter verfügbar, auch *timeout*. Sie erreichen daher mit *bcdedit /timeout 10* die gleichen Ergebnisse.
- Haben Sie Windows Server 2008 parallel zu Windows Server 2003 installiert, wird der dafür notwendige Eintrag automatisch erzeugt. Manuell können Sie diesen mit dem Befehl im folgenden Listing erzeugen, vorausgesetzt Windows Server 2003 wurde auf der Partition D: installiert. In der letzten Zeile wird der Eintrag von Windows Server 2003 am Ende des Auswahlmenüs angezeigt.

Listing 2.1 Manuelles Hinzufügen und Sortieren von Windows Server 2003 zum Windows Server 2008-Bootmanager

```
bcdedit /create {legacy} /d "Windows Server 2003"
bcdedit /set {legacy} device partition=D:
bcdedit /set {legacy} osdevice partition=D:
bcdedit /set {legacy} path \ntldr
bcdedit /displayorder {legacy} /addlast
```

Verwenden von VistaBootPRO oder Easy BCD

Optimaler zum Bearbeiten des Bootmenüs sind Freewareprogramme wie VistaBootPRO oder Easy BCD mit denen in einer grafischen Oberfläche bequem das Bootmenü angepasst werden kann. Die Programme funktionieren auch unter Windows Server 2008, sollten aber nur auf Testservern installiert werden. Auf produktiven Servern sollten Sie auf solche Zusatzprogramme möglichst verzichten und mit *bcdedit.exe* arbeiten. Sie können das Programm VistaBootPRO von der Internetseite *http://www.pro-networks.org/vistabootpro* kostenlos herunterladen. EasyBCD finden Sie auf der Seite *http://www.neosmart.net.* Nach der Installation von VistaBootPRO und dem ersten Start bietet das Programm zunächst eine Sicherung der bestehenden Bootkonfiguration an. Haben Sie das Programm gestartet, können Sie über *View Settings* die aktuellen Einstellungen des Bootmenüs anzeigen. Über die anderen Schaltflächen können Sie die Einstellungen des Bootmenüs bearbeiten. Es erscheinen zwar unter Umständen Fehlermeldungen beim Speichern, aber die Konfigurationen werden dennoch übernommen. Wir möchten Sie aber nochmals ausdrücklich darauf hinweisen, solche Freeware-Tools nur in Testumgebungen zu verwenden.

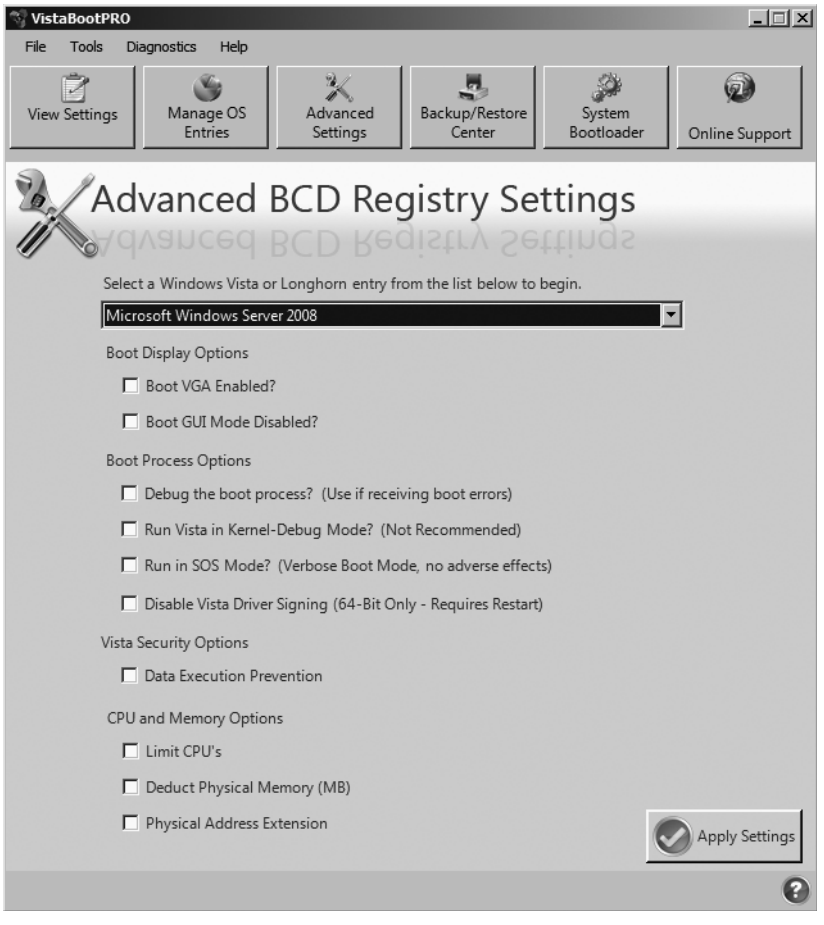
Abbildg. 2.30 Anzeigen der Windows Server 2008-Bootoptionen

TIPP Programme zum Bearbeiten des Bootmanagers von Windows Server 2008 werden unter Umständen von der Dateiausführungsverhinderung blockiert. In Kapitel 14 erfahren Sie, wie diese Funktion konfiguriert wird, damit diese Programme funktionieren (Abbildung 2.31).

Abbildg. 2.31 Die Dateiausführungsverhinderung muss entsprechend konfiguriert werden, damit externe Programme gestartet werden, mit denen der Bootmanager von Windows Server 2008 bearbeitet werden kann

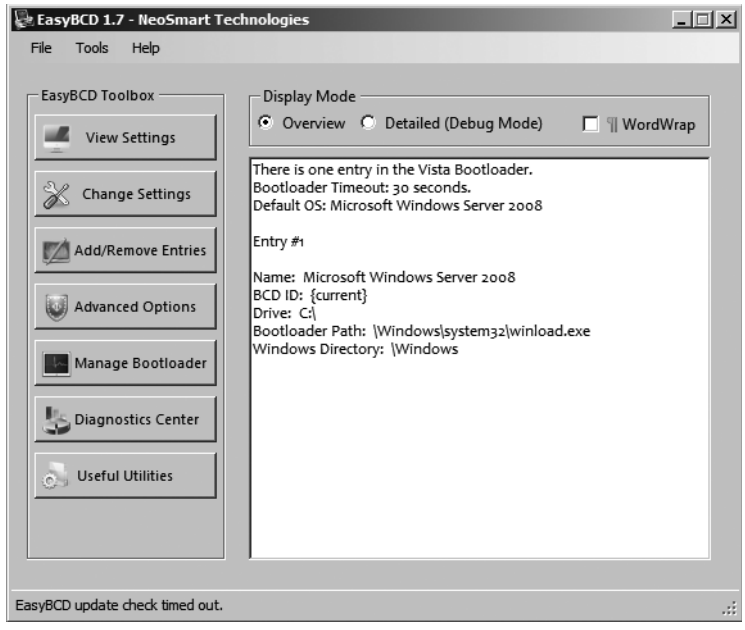
Zusätzlich lassen sich mit VistaBootPRO weitere Einträge erzeugen oder das Startverhalten von Windows Server 2008 anpassen. Wenn Sie Windows Server 2003 auf der Partition C: Ihres Servers installiert haben und Windows Server 2008 auf der Partition D:, dann wird die Festplatte C: unter Windows Server 2008 als D: angezeigt und unter Windows Server 2003 die Festplatte C: von Windows Server 2008 als D:. Die beiden Laufwerksbuchstaben sind also jeweils vertauscht. Achten Sie darauf, wenn Sie hier irgendetwas konfigurieren. Die Bootreihenfolge der Betriebssysteme sowie die Zeitspanne, in der das Bootmenü auf eine Eingabe wartet, können auch in den Eigenschaften des Systems in der Systemsteuerung (*Start/Systemsteuerung/System*, Link *Erweiterte Systemeinstellungen*) auf der Registerkarte *Erweitert* über die Schaltfläche *Einstellungen* im Bereich *Starten und Wiederherstellen* konfiguriert werden. In diesem Fenster können Sie aber die Einträge nicht ändern, keine Sicherung des Bootmanagers durchführen und auch keine neuen Einträge hinzufügen.

Abbildg. 2.32 Bearbeiten der Startoptionen von Windows Server 2008



Die Bedienung von EasyBCD ist ähnlich zur Bedienung von VistaBootPRO. Auch hier lassen sich die Booteinstellungen ansehen und bearbeiten (Abbildung 2.33).

Abbildg. 2.33 Auch mit EasyBCD lässt sich das Bootverhalten von Windows Server 2008 anpassen



Parallele Installation von Windows Server 2008 entfernen

Wollen Sie die parallele Installation von Windows Server 2008 wieder entfernen, genügt es nicht, lediglich die Partition zu löschen, in der Windows Server 2008 installiert ist. Sie müssen zusätzlich auch den Bootmanager entfernen:

1. Booten Sie Ihren Rechner mit der Windows Server 2008-DVD und öffnen Sie über die Systemwiederherstellungsoptionen die Eingabeaufforderung.
2. Anschließend wechseln Sie auf das Laufwerk der Windows Server 2008-DVD und dort durch Eingabe des Befehls *cd \boot* in das Verzeichnis *Boot*.
3. Geben Sie als Nächstes den Befehl *bootsect.exe /nt52 SYS* ein. Dadurch wird der Bootsektor der primären Partition mit dem klassischen Startcode überschrieben. Der Windows Server 2008-Bootmanager wird dabei entfernt. Alternativ können Sie den Bootsektor auch mit der Wiederherstellungskonsole von Windows Server 2003 und dem Befehl *fixboot* wiederherstellen lassen.
4. Anschließend löschen Sie das Verzeichnis *Boot* auf der Systempartition, da die darin enthaltenen Dateien zu Windows Server 2008 gehören und nicht mehr benötigt werden.

Windows Server 2008-Bootmanager reparieren

Unter manchen Umständen kann es passieren, dass der Windows Server 2008-Bootmanager nicht mehr funktioniert oder bei einer parallelen Installation zu Windows Server 2003 nicht mehr alle Betriebssysteme angezeigt werden. Meist tritt ein derartiges Problem auf, wenn auf einem Server

nach der Installation von Windows Server 2008 nochmals Windows Server 2003 installiert wird. Windows Server 2003 lässt sich daraufhin zwar problemlos starten, allerdings wird der Windows Server 2008-Bootmanager nicht mehr angezeigt. Legen Sie in diesem Fall die Windows Server 2008-DVD ein, booten Sie von dieser DVD und wählen Sie die *Computerreparaturoptionen*. Nachdem Sie die Reparaturoptionen ausgewählt haben, wird ein Dialogfeld geöffnet, das Ihnen die Auswahl unter mehreren Optionen ermöglicht. Um den Bootmanager von Windows Server 2008 zu reparieren, wählen Sie die Option *Systemstartreparatur*. Durch diese Auswahl wird der Bootmanager von Windows Server 2008 repariert und der Server startet wieder ordnungsgemäß. Nach der Reparatur des Bootmanagers wird allerdings höchstwahrscheinlich Windows Server 2003 nicht mehr angezeigt. Um Windows Server 2003 nachträglich in den Bootmanager zu integrieren, starten Sie zunächst Windows Server 2008 und gehen dann folgendermaßen vor:

1. Öffnen Sie das *Start*-Menü und klicken Sie mit der rechten Maustaste auf den darin enthaltenen Eintrag *Eingabeaufforderung*.
2. Wählen Sie im Kontextmenü den Befehl *Als Administrator* ausführen.
3. Tippen Sie die folgenden Befehle ein, um Windows Server 2003 in den Bootmanager zu integrieren:

```
Bcdedit /create {legacy} /d "Windows Server 2003"
Bcdedit /set {legacy} device boot
Bcdedit /set {legacy} path \ntldr
Bcdedit /displayorder {legacy} /addlast
```

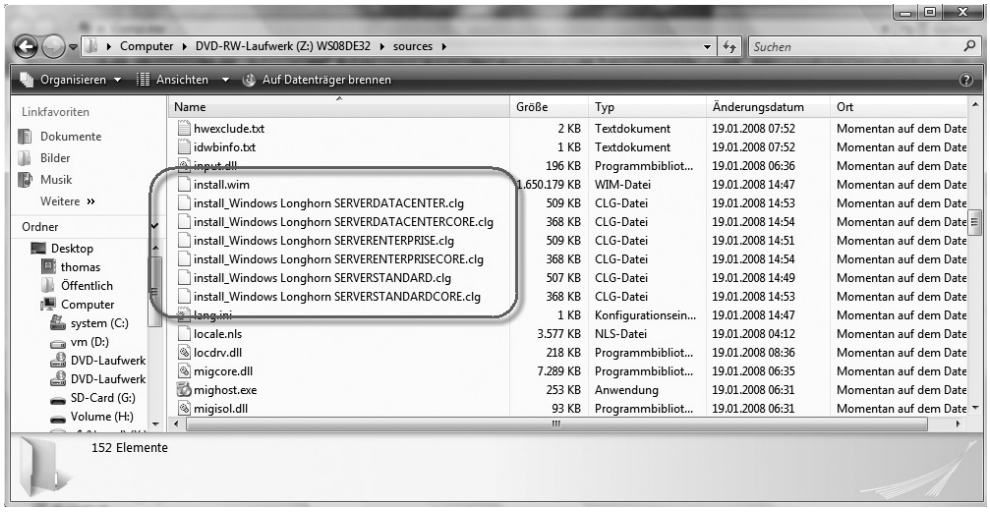
Anschließend sollte sich Windows Server 2008 und auch das frühere Windows-System wieder fehlerfrei starten lassen.

Hintergrundinformationen zum Installationsmechanismus

Mit dem Windows System Image Manager (Windows SIM) können auf einfache Weise Antwortdateien auf XML-Basis erstellt werden (siehe auch Kapitel 16). Auch Netzwerkfreigaben können so konfiguriert werden, dass diese Konfigurationen zur Verteilung von Windows Vista oder Windows Server 2008 enthalten. Mit Windows SIM kann auf einem Computer eine Antwortdatei auf XML-Basis erstellt werden, auf deren Basis sich wiederum ein Installationsimage erstellen lässt. Dieses Image kann entweder über Netzwerkfreigaben auf Ziel-Computern installiert oder durch die Windows Deployment Services (WDS) im Unternehmen verteilt werden (siehe Kapitel 16). Die Antwortdatei enthält alle vordefinierten Optionen, die bei der Installation von Windows Server 2008 gefordert sind. Dadurch lassen sich Eingaben wie Servernamen, Seriennummer und weitere Eingaben in einer Datei vorgeben, sodass während der Installation keinerlei Eingaben mehr erfolgen müssen.

Die Katalogdatei eines Image (**.clg*) enthält die Einstellungen und Pakete, die in einem Image auf WIM-Basis (Windows Imaging, siehe Kapitel 16) enthalten sind. Da auch die normale Installation von Windows Server 2008 auf einem WIM-Image basiert, finden Sie auf der Windows Server 2008-Installations-DVD im Verzeichnis *sources* die **.clg*-Dateien der verschiedenen Windows-Editionen (Abbildung 2.34). WIM-Images haben als Dateityp die Bezeichnung **.wim*. Die Standardinstallationsdatei hat die Bezeichnung *install.wim*. Für jede Windows Server 2008-Edition gibt es eine entsprechende Katalogdatei (**.clg*).

Abbildg. 2.34 Anzeigen der **.clg*-Dateien und des WIM-Image der Windows Server 2008-Installation



In Kapitel 16 gehen wir ausführlicher auf die Möglichkeiten der automatisierten Installation von Windows Vista und Windows Server 2008 ein.

Multilanguage User Interface (MUI)

Windows XP und Windows Server 2003 unterstützten unterschiedliche Sprachen auf zwei Weisen. Sie konnten entweder lokalisierte Versionen von Windows, bei denen für jede Sprache ein anderes Image erforderlich war, oder eine englische MUI-Version (Multilanguage User Interface) mit zusätzlichen Sprachpaketen bereitstellen. Jeder Ansatz hatte seine Vor- und Nachteile, doch entschieden sich Unternehmen, in denen mehrere Sprachen unterstützt werden mussten, in den meisten Fällen für den MUI-Weg und mussten so die Einschränkungen in Kauf nehmen, die sich aus der Ausführung eines Betriebssystems ergaben, dessen Kern im Grunde Englisch war. Unternehmen, in denen nur mit einer Sprache gearbeitet wurde, entschieden sich in der Regel für die Nutzung lokalisierter Versionen. Bei Windows Server 2008 ist jetzt das ganze Betriebssystem sprachneutral. Diesem sprachneutralen Kern werden ein oder mehrere Sprachpakete hinzugefügt. Mit Windows-Sprachpaketen können Sie die Oberfläche von Windows Server 2008 auf eine andere Sprache umstellen, ohne Windows neu zu installieren. Es gibt zwei Arten von Windows-Sprachdateien: Windows Multilanguage User Interface Pack (MUI Pack) und Windows-Benutzeroberflächen-Sprachpakete (Language Interface Pack, LIP). MUIs stellen eine übersetzte Version des größten Teils der Windows-Benutzeroberfläche und LIPs eine übersetzte Version der am häufigsten benutzten Bereiche der Windows-Benutzeroberfläche zur Verfügung. In den *Regions- und Sprachoptionen* in der Systemsteuerung, können Sie nach dem Herunterladen und Installieren die Sprache ändern. Die Wartung von Windows Server 2008 ist ebenfalls sprachneutral, in vielen Fällen ist nur ein Sicherheitsupdate für alle Sprachen erforderlich. Auch die Konfiguration ist sprachneutral, eine einzige *unattend.xml* kann für alle Sprachen verwendet werden. Für die Integration von MUI-Language Packs während der Installation wird zur Anpassung das bereits weiter vorne in diesem Kapitel erwähnte Windows Automated Installation Kit (WAIK) verwendet. Language Packs für Windows Vista und Windows Server 2008 liegen als **.cab*-Dateien vor und enthalten die notwendigen Ressourcen und Schriftarten.

Language Packs während der Installation hinzufügen

Sie können im Rahmen des Rollouts mit ImageX Images erstellen, die verschiedene Language Packs enthalten. Sie benötigen dazu das Windows Server 2008-Installationsmedium sowie die **.cab*-Dateien der Sprachen, die Sie hinzufügen wollen. Um Sprachdateien zu der Distribution hinzuzufügen, gehen Sie folgendermaßen vor:

1. Installieren Sie auf einem Windows Vista-PC das Windows Automated Installation Kit (WAIK) und die BDD 2007 (siehe Kapitel 16).
2. Kopieren Sie in einen Quellordner den Inhalt der Windows Server 2008-DVD und entfernen Sie den Schreibschutz von dem Ordner, den Unterordnern und allen Dateien.
3. Kopieren Sie das Language Pack ebenfalls in einen Ordner auf dem PC. Die Language Packs werden entweder im Rahmen eines Select-Vertrages zur Verfügung gestellt, oder sind auf der Windows-DVD für die entsprechende Sprache vorhanden. Language Packs haben als Verzeichnis auf der DVD die Form von *de-de* oder *en-en*. In diesem Verzeichnis finden Sie die entsprechende **.cab*-Datei, die Sie auf den PC kopieren müssen. Kopieren Sie auch zur Sicherheit die restlichen Dateien, die im Language Pack enthalten sind.
4. Mounten Sie mit ImageX die Datei *install.wim* aus dem Verzeichnis auf dem PC in das Sie die Windows Server 2008-DVD kopiert haben. Die Befehlszeile könnte zum Beispiel folgendermaßen aussehen:

```
Imagex /mountrw c:\-rollout \Sources\install.wim 4 c:\wim_mount
```

5. Als Nächstes muss die Datei *lang.ini* innerhalb der Installation an die Integration des neuen Language Packs angepasst werden. Diese Datei wird während der Installation von Windows dazu verwendet, die entsprechenden Sprachen zu integrieren. Die Datei enthält eine Liste und den Speicherort der integrierten Language Packs. Auch die Standardsprache des Servers nach der Installation wird in der *lang.ini* festgelegt. Die Datei wird dazu neu generiert. Hierzu verwenden Sie das Tool *intlcfg.exe* (International Settings and Configuration Tool). Der Befehl könnte folgendermaßen aussehen:

```
Intlcfg -genlangini -dist:c:\rollout -image:c:\wim_mount -all:de-DE
```

6. Im Anschluss können Sie die Datei *install.wim* wieder unmounten. Der Befehl könnte folgendermaßen aussehen:

```
Imagex /unmount /commit c:\wim_mount
```

7. Als Nächstes können Sie weitere Language Packs integrieren. Wiederholen Sie dazu die Schritte 3 bis 6.

Zusammenfassung

Nachdem Sie die grundlegende Installation von Windows Server 2008 (auch im Server Core-Modus) kennen gelernt sowie Details zur Treiberinstallation und Aktivierung erfahren haben, können Sie sich näher mit dem Server befassen. Im nächsten Kapitel zeigen wir Ihnen erste wichtige Schritte beim Umgang mit Windows Server 2008, sowie wichtige Befehle für Server Core. Auch ausführliche Anleitungen, um einen Core-Server korrekt zu aktivieren, sind im folgenden Kapitel enthalten. Zusätzlich erfahren Sie darin mehr über die Vorteile und den Umgang mit dem neuen Server-Manager.

Kapitel 3

Erste Schritte und Server Core

In diesem Kapitel:

Nachdem Sie den Server installiert haben, können Sie sich mit der Verwaltung vertraut machen. In diesem Kapitel zeigen wir Ihnen die ersten Schritte, die zur Verwaltung eines Windows Server 2008 notwendig sind. Eine der wichtigsten Neuerungen zur Verwaltung in Windows Server 2008 ist der neue Server-Manager sowie die Aufgaben für die Erstkonfiguration. Mit diesen neuen Funktionen wird die Verwaltung eines Servers erheblich erleichtert und übersichtlicher gestaltet. Der Server-Manager ist das neue zentrale Verwaltungsinstrument von Windows Server 2008. Die Aufgaben der Erstkonfiguration (Initial Configuration Tasks, ICT) werden nach der Installation automatisch gestartet und dienen der Einrichtung der wichtigsten Funktionen eines Servers direkt nach dem Start.

Erste Schritte nach der Installation

Nach der Installation des Servers werden in den *Aufgaben der Erstkonfiguration (Initial Configuration Tasks, ICT)* die gegenwärtigen Einstellungen angezeigt. Zusätzlich können Sie hier die Konfiguration verändern und zugehörige Informationen aus der Onlinehilfe aufrufen. Bei dieser neuen Verwaltungsoberfläche handelt es sich um ein wertvolles Instrument zur ersten Einrichtung eines Servers. Im Gegensatz zu Windows Server 2003 sind keine verschiedenen Werkzeuge zur ersten Einrichtung notwendig, sondern alle Aufgaben können jetzt direkt über die ICT durchgeführt werden. Nach der Installation des Servers werden in den Aufgaben für die Erstkonfiguration (Initial Configuration Tasks, ICT) die gegenwärtigen Einstellungen angezeigt. Hier können Einstellungen verändert und zugehörige Informationen aus der Onlinehilfe aufgerufen werden. An dieser Stelle kann zum Beispiel der Name des Servers festgelegt oder das Netzwerk konfiguriert werden. Auch zusätzliche Rollen und Features lassen sich auf diesem Weg direkt nach der Installation aktivieren und konfigurieren. Während der Installation legt Windows Server 2008 automatisch einen Namen für den Server fest, der nachträglich angepasst werden soll. Diese Aufgabe kann direkt nach der Installation in den Aufgaben für die Erstkonfiguration durchgeführt werden. Über die ICT kann die Netzwerkkonfiguration vorgenommen und der Server gleich in die Domäne aufgenommen werden. Auch der Remotedesktop und die Einstellungen für Windows Update sind direkt nach der Installation aktivier- und konfigurierbar. Die Links in den Aufgaben für die Erstkonfiguration sind bewusst einfach gehalten und es werden entsprechende Assistenten gestartet, die Administratoren bei der Einrichtung unterstützen. Die Bedienung von Windows Server 2008 lehnt sich an Vista an. Beispielsweise enthält das Startmenü ein Suchfeld, über das Sie Menüeinträge schneller finden können. Mit dem überarbeiteten Windows-Explorer ist auch beim Serversystem der Wechsel zu häufig benötigten Ordnern über den linken Favoritenbereich möglich. Auf diese Weise sollten sich Administratoren, die sich bereits mit Vista beschäftigt haben, auch auf dem neuen Server-Release zurechtfinden. Im Unterschied zu Vista erfolgt die Anzeige der Benutzeroberfläche beim Server aber standardmäßig nicht im Look der Aero-Oberfläche mit durchsichtigen Fensterrahmen, sondern hier zeigt das System die von Windows Server 2003 her gewohnte Ansicht, was die Einarbeitung vieler Administratoren deutlich erleichtern dürfte.

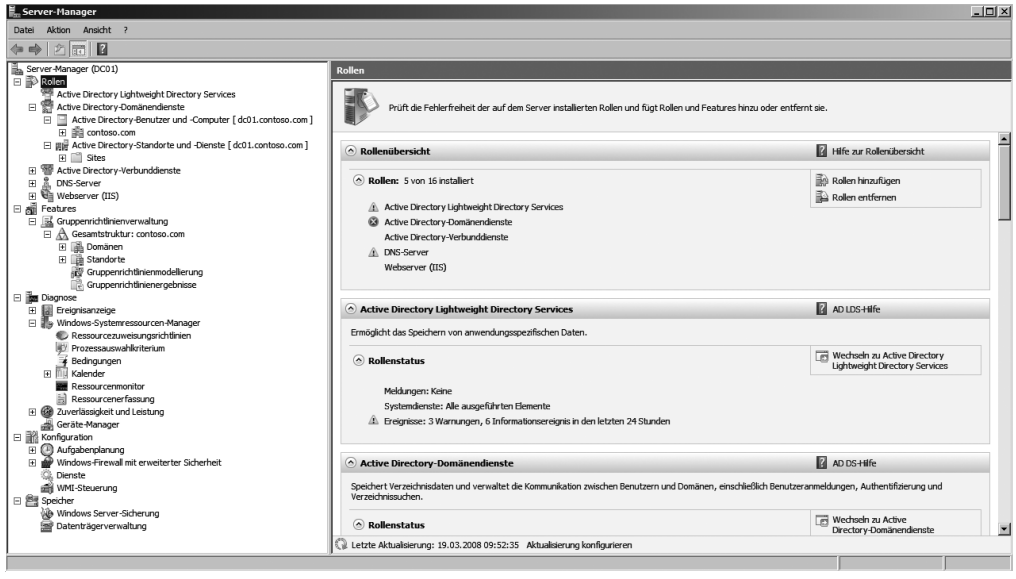
Abbildg. 3.1 Aufgaben der Erstkonfiguration nach der Installation

Arbeiten mit dem Server-Manager

Der Server-Manager ist das neue einheitliche Verwaltungsportal von Windows Server 2008, das mit der zusätzlichen Installation von Rollen und Features mitwächst. Nach dem Start erhalten Administratoren sofort einen Überblick über alle Rollen und Features eines Servers. Über dieses Portal kann der Server vollständig überwacht und verwaltet werden. Auch die Fehlerdiagnose mit den einzelnen Diagnoseprogrammen kann über dieses zentrale Verwaltungsinstrument gestartet werden. Im Vergleich zu Windows Server 2003 haben die Entwickler hier einige Veränderungen im Server-Manager vorgenommen: Im Detailbereich der Verwaltungskonsole zeigt der Server-Manager unter anderem grundlegende Informationen über den Server, seine Sicherheitskonfiguration sowie die installierten Funktionen an. Der Server-Manager listet zudem auf, welche Rollen das System derzeit ausübt und integriert notwendige Snap-Ins für die Verwaltung automatisch. Solche Rollen haben bei Windows Server 2008 eine große Bedeutung. Mit ihrer Hilfe sind Administratoren in der Lage, einen Server für bestimmte Aufgaben zu konfigurieren. Dadurch entfällt die separate Installation und Einrichtung der für eine Rolle erforderlichen Komponenten, was gleichzeitig zur Vereinfachung der Verwaltung beiträgt. Werden zusätzliche Rollen oder Funktionen installiert, werden die zusätzlichen Verwaltungsoberflächen automatisch in den Server-Manager integriert. Administratoren müssen daher nicht für jeden Server manuell eine Microsoft Management Console (MMC) erstellen, sondern können bequem über eine einheitliche Verwaltungsoberfläche arbeiten, die alle notwendigen Programme enthält. Der Server-Manager wird nach der Anmeldung automatisch gestartet.

TIPP Sie können den Server-Manager entweder über das Symbol in der Schnellstartleiste, über die Programmgruppe *Verwaltung* oder über *Start/Ausführen/servermanager.msc* starten.

Abbildg. 3.2 Verwalten eines Servers mit dem Server-Manager

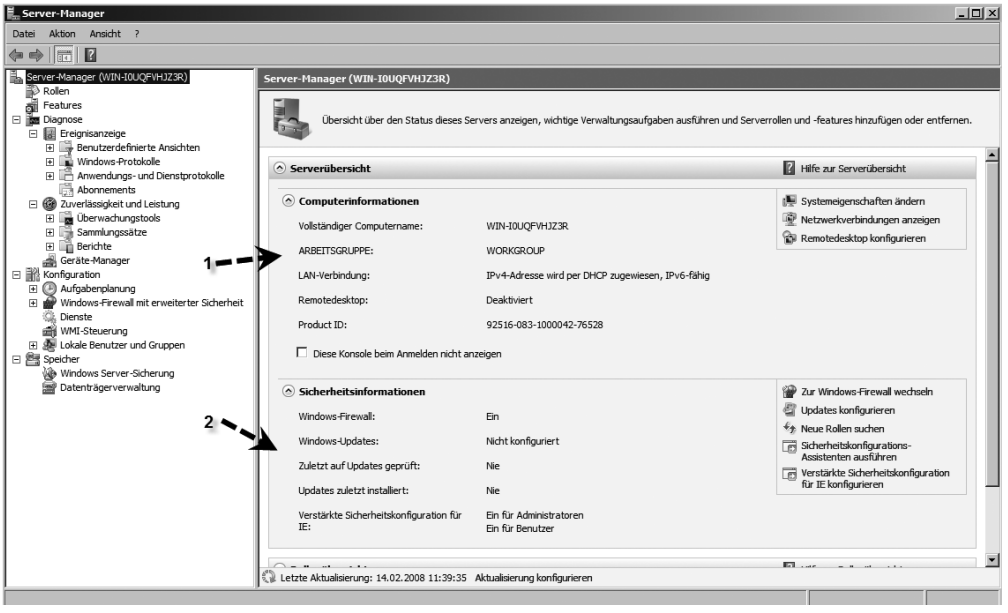


HINWEIS Der Server-Manager kann immer nur zur Verwaltung des lokalen Servers verwendet werden. Es ist keine Verbindung zu anderen Servern im Netzwerk möglich.

Administratoren sehen im Server-Manager auf einen Blick, ob die einzelnen Rollen des Servers funktionieren, und es werden Fehlermeldungen aus den Ereignisanzeigen angezeigt, die diese Rolle betreffen. Neben der Überwachung können die installierten Rollen und Funktionen auch optimal verwaltet werden, da die entsprechenden Snap-Ins automatisch hinzugefügt werden. Im mittleren Bereich des Server-Managers wird eine Zusammenfassung angezeigt, über welche die wichtigsten Informationen zum Server an zentraler Stelle angezeigt werden. Die Informationen in der Mitte des Server-Managers untergliedern sich in verschiedene Bereiche. Diese Bereiche können zur besseren Übersicht ein- und ausgeklappt werden. Der Bereich *Serverübersicht* untergliedert sich in die beiden Bereiche *Computerinformationen* und *Sicherheitsinformationen*. An dieser Stelle sehen Sie den Computernamen, die IP-Adresse, die Domäne, Netzwerkverbindungen und die Produkt-ID. Über diesen Bereich können auch die dazugehörigen Konfigurationsfenster geöffnet werden, um die Servereinstellungen zu verwalten. Durch diese neue Struktur wird eine perfekte Symbiose von Einrichtung und Verwaltung der Serverrollen erreicht. Die Sicherheitsinformationen zeigen die aktivierte Windows-Firewall und Windows-Updates an. Auch die Konfiguration dieser wichtigen Serverfunktionen können direkt über diesen

Bereich vorgenommen werden. Mit dem kleinen Pfeilsymbol neben den Informationsbereichen, werden die Informationen und Konfigurationsmenüs ein- oder ausgeblendet. Neben der Serverübersicht sind die beiden Bereiche *Rollenübersicht* und *Featureübersicht* dafür zuständig, die auf dem Server installierten Rollen und die zusätzlichen Funktionen anzuzeigen.

Abbildg. 3.3 Anzeigen von Serverinformationen im Server-Manager



Über diese beiden Bereiche können auch zusätzliche Rollen oder Features hinzugefügt werden. Serverrollen bestimmen den primären Verwendungszweck eines Servers. Mit den Features im Server-Manager werden untergeordnete Funktionen zu Rollen hinzugefügt. Features erweitern installierte Serverrollen um zusätzliche Möglichkeiten. Zum Beispiel kann das Feature Failover-Clustering auch nach der Installation der Serverrolle *Dateidienste* installiert werden. Es stehen, neben den verschiedenen Rollen, über 30 verschiedene Features zur Verfügung. Manche Rollen haben nur ein Konfigurationsfenster, andere Rollen, wie zum Beispiel die Dateidienste, müssen ausführlicher konfiguriert werden und werden im Server-Manager daher mit mehreren Snap-Ins repräsentiert. Mit Hilfe des Assistenten zur Installation einer Rolle können weitere, untergeordnete Rollendienste und -Features hinzugefügt werden. Werden Rollendienste ausgewählt, die von anderen abhängig sind, werden diese ebenfalls automatisch zur Installation vorgeschlagen. Zusätzlich wird in diesen beiden Bereichen ein Überblick angezeigt, aus dem schnell ersichtlich wird, ob eine Rolle fehlerfrei funktioniert oder ob Fehlermeldungen in den Ereignisanzeigen protokolliert werden. Weist eine Rolle Fehler auf, wird diese in der Rollenübersicht als fehlerhaft dargestellt. Entsprechende Ereignisse können dann direkt über den Server-Manager angezeigt und Verwaltungsaufgaben durchgeführt werden. Administratoren können entweder über den entsprechenden Link die Ereignisanzeige gefiltert nach Ereignissen dieser Rolle anzeigen oder über den Menüpunkt *Verwalten* die jeweilige Rolle konfigurieren, um die Fehler zu beseitigen. Es sind keine verschiedenen Werkzeuge dazu mehr notwendig,

sondern alle diese Aufgaben können direkt im Server-Manager durchgeführt werden. Im Bereich *Ressourcen und Support* können die Fehlerberichtserstattung und die Einstellungen für das Programm zur Verbesserung der Benutzerfreundlichkeit konfiguriert werden. Außerdem lässt sich über diesen Bereich direkt die Microsoft TechNet-Seite von Windows Server 2008 öffnen, um zum Beispiel Informationen über bestimmte Ereignisse in der Ereignisanzeige zu überprüfen.

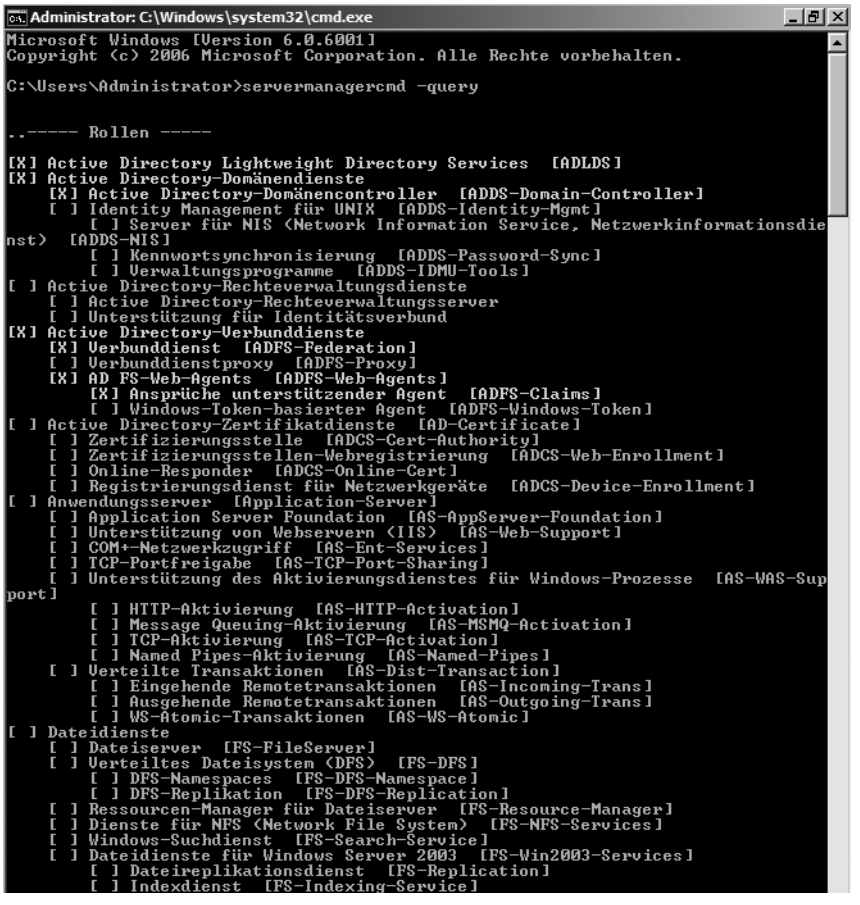
Abbildg. 3.4 Anzeigen und Verwalten der installierten Rollen und Funktionen auf dem Server

Neben den Rollen und Features lassen sich im Server-Manager auch die Diagnoseprogramme sowie die Systemkonfiguration an zentraler Stelle vornehmen. Zur Diagnose von Windows Server 2008 kommen wir noch ausführlich in Kapitel 18 zurück. Da Windows Server 2008 bereits standardmäßig sehr ressourcenschonend installiert wird, sind noch keinerlei Serverrollen und -features installiert.

Server-Manager in der Befehlszeile verwenden

Neben der grafischen Oberfläche bietet der neue Server-Manager auch eine Befehlszeilenoberfläche, über die Sie Rollen und Features in der Befehlszeile und skriptbasiert installieren können. Das Tool hat die Bezeichnung *ServerManagerCMD.exe*. Mit dem Tool können Sie unbeaufsichtigte Installationen von Serverrollen und Features durchführen. Antwortdateien können mit XML übergeben werden. Mit dem Server-Manager können Sie sich auch die installierten Rollen und Features eines Servers anzeigen lassen. Mit dem Befehl *servermanagercmd –query*, können Sie sich eine Übersicht des Servers in der Befehlszeile anzeigen lassen. Installierte Rolle und Features werden besonders hervorgehoben (Abbildung 3.5).

Abbildg. 3.5 Abfrage der installierten Rollen und Funktionen über *ServerManagerCMD.exe*



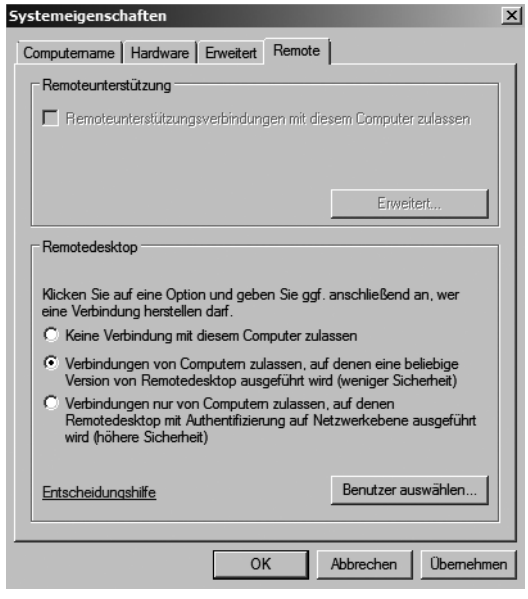
Server über das Netzwerk verwalten – Remotedesktop

Sobald Sie einen neuen Server installiert haben, ist der bequemste und effizienteste Weg die Verwaltung über das Netzwerk. In diesem Fall können Sie den Server von Ihrem Arbeitsplatz aus verwalten und müssen nicht vor dem Server sitzen, um einzelne Einstellungen vorzunehmen. Damit Sie über das Netzwerk auf einen Server effizient zugreifen können, müssen Sie nach der Installation zunächst noch eine Maßnahme durchführen. In Windows Server 2008 wurde der Remotedesktop von Windows Vista integriert. Aktivieren Sie diesen Remotedesktop, können Sie mit einem Zusatzprogramm unter Windows XP oder Windows Vista bequem auf den Server zugreifen. Wenn Sie sich mit einem Remotedesktop über das Netzwerk verbinden, ist die Geschwindigkeit beinahe so schnell, als wenn Sie direkt vor dem Server am Bildschirm sitzen würden. Bei Windows Server 2008 besteht keine Notwendigkeit mehr, unbedingt ein Fernwartungstool zu verwenden. Die Bordmittel sind dazu vollkommen ausreichend.

Aktivieren des Remotedesktops

Um sich mit einem Server verbinden zu können, aktivieren Sie daher zunächst die Funktion des Remotedesktops über die Systemsteuerung. Klicken Sie auf der linken Seite auf *Startseite der Systemsteuerung*, dann auf *System und Wartung* und dann im Abschnitt *System* auf *Remotezugriff zulassen*. Aktivieren Sie dann das Kontrollkästchen *Remoteunterstützungsverbindungen mit diesem Computer zulassen* (Abbildung 3.6). Aktivieren Sie im Dialogfeld *Systemeigenschaften* im Bereich *Remotedesktop* die Option *Verbindungen von Computern zulassen, auf denen eine beliebige Version von Remotedesktop ausgeführt wird*. Bei der anderen Option, dürfen nur PCs mit Windows Vista oder Server unter Windows Server 2008 auf den Server zugreifen. Nachdem Sie eine Sicherheitsmeldung bestätigt und das Dialogfeld über *OK* verlassen haben, ist der Server für den Zugriff über das Netzwerk bereit. Standardmäßig dürfen sich die Benutzer verbinden, die entweder in der lokalen Gruppe *Administratoren* oder *Remotedesktopbenutzer* Mitglied sind.

Abbildg. 3.6 Aktivieren des Remotedesktops unter Windows Server 2008



Verbindungsaufbau über Remotedesktop

Wenn Sie den Remotedesktop aktiviert haben, können Sie auf einem Windows XP- oder Vista-PC oder einen anderen Server mit Windows Server 2008 über *Start/Alle Programme/Zubehör/Kommunikation/Remotedesktopverbindung* das entsprechende Clientprogramm starten. Alternativ können Sie das Programm auch über *Start/Ausführen/mstsc.exe* starten (Abbildung 3.7). Über die Schaltfläche *Optionen* können Sie zahlreiche weitere Optionen einstellen. Für die Verwaltung eines Servers reicht die Standardeinstellung hier allerdings vollkommen aus. Wenn Sie im Eingabefeld die IP-Adresse des Servers eingeben, können Sie sich direkt mit dem Server verbinden. Sie müssen sich in der Anmeldemaske authentifizieren, damit die Verbindung aufgebaut wird. Windows Server 2008 erlaubt standardmäßig nicht die gleichzeitige Verbindung von zwei Sitzungen des gleichen Benut-

zers auf einem Server. Wenn an der Konsole ein Administrator angemeldet war, wird der Bildschirm durch den Verbindungsaufbau mit der Remotedesktopkonsole automatisch gesperrt. Diese Option kann aber in der Terminaldienstekonfiguration angepasst werden. Entsperrt ein Administrator an der Konsole den Bildschirm wieder, wird die Remotedesktopsitzung wiederum getrennt. Es kann daher standardmäßig immer nur ein Administrator an der Konsole arbeiten. Wollen Sie mit mehreren Sitzungen auf einem Server arbeiten, müssen Sie sich mit einem anderen Administrator-Konto anmelden oder die Konfiguration anpassen (siehe auch Kapitel 12). Diese Sitzung ist vollkommen unabhängig vom Desktop auf dem Server. Sie sehen daher in dieser Sitzung zunächst keinerlei Fehlermeldungen, die unter Umständen auf dem Desktop des Servers angezeigt werden, wenn Sie sich mit dem Administrator anmelden, also der Konsole. Wenn ein Administrator über Remotedesktop mit dem Server verbunden ist, kann er die gleichen Aufgaben durchführen, als wenn er direkt am Server lokal angemeldet ist. Seine Tätigkeit wird allerdings nicht am Bildschirm des Servers angezeigt, wenn er sich mit einem eigenen Benutzerkonto anmeldet. Melden sich mehr als zwei verschiedene Administratoren über das Netzwerk an, und ein dritter versucht eine Verbindung aufzubauen, erscheint bei der letzten Anmeldung eine Warnmeldung, da die maximale Anzahl der Verbindungen erreicht ist. In der oberen Bildschirmhälfte wird Ihnen eine Menüleiste angezeigt, mit der Sie die Sitzung minimieren können. Diese Leiste können Sie über das entsprechende Symbol auch ausblenden lassen. Standardmäßig wird die Sitzung im Vollbild aufgebaut. Sie können eine Remotedesktopsitzung parallel zu mehreren Servern aufbauen. In dieser Hinsicht gibt es keinerlei Einschränkungen. Wenn Sie die Arbeit im Remotedesktop beendet haben, können Sie sich regulär über das Startmenü abmelden. Von dieser Abmeldung ist nur Ihre Sitzung betroffen, nicht die Sitzungen der anderen Administratoren oder der Konsole.

Abbildg. 3.7 Konfigurieren des Remotedesktops

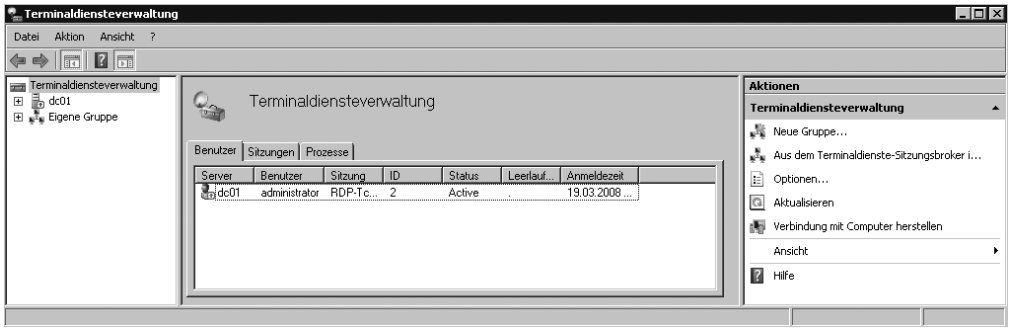
Trennen Sie nur die Sitzung, also schließen Sie das Remotefenster einfach, bleibt die Sitzung auf dem Server aktiv. Beachten Sie, dass in diesem Fall die Sitzung zu den maximalen Sitzungen auf dem Server dazuzählt. Wenn auf dem Server mehr als zwei getrennte Sitzungen laufen, können Sie sich

von einem anderen Computer nicht mehr per Remotedesktop verbinden, da der Server Sie nicht mit der laufenden Sitzung verbindet, sondern eine neue aufbauen will. Wenn Sie daher aus Bequemlichkeit Sitzungen immer nur trennen lassen, besteht die Möglichkeit, dass Sie sich selbst vom Server aussperren. Sie können getrennte Sitzungen auf dem Server wieder freigeben und auch Einstellungen für den Remotedesktop auf dem Server vornehmen.

Zurücksetzen von getrennten Verbindungen

Sie können die Sitzungen eines Servers mit Hilfe des Verwaltungsprogramms (Aufruf über *Start/Verwaltung/Terminaldienste/Terminaldiensteverwaltung*) steuern (Abbildung 3.8). Allerdings müssen dazu die Verwaltungstools der Terminaldienste installiert werden. Installieren Sie dazu am besten auf einem Server das Feature *Remoteserver-Verwaltungstools*. Hier kann ausgewählt werden, welche Verwaltungswerkzeuge installiert werden sollen.

Abbildg. 3.8 Anzeige der Sitzungen auf einem Server



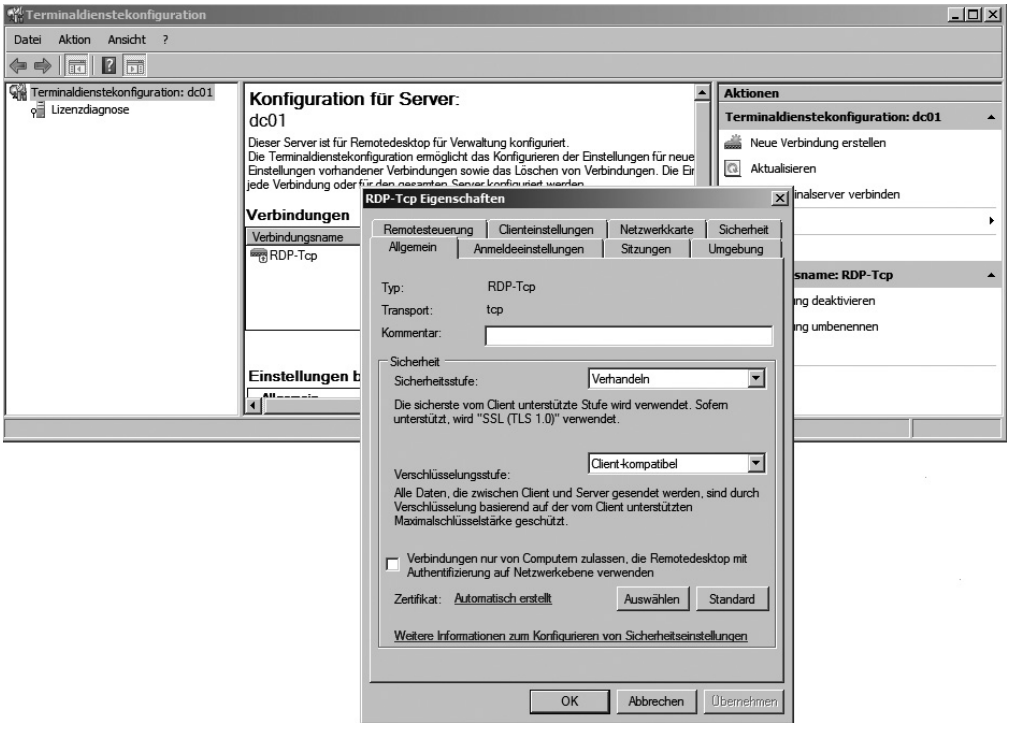
Wenn Sie in der Terminaldiensteverwaltung den lokalen Server markieren, werden Ihnen alle Sitzungen angezeigt. Die getrennten Sitzungen werden mit dem Status *Getrennt* oder *Disconnected* angezeigt. Klicken Sie die Sitzung mit der rechten Maustaste an, können Sie diese Sitzung im Kontextmenü über die Option *Zurücksetzen* wieder freigeben. In diesem Fall ist die Lizenz sofort wieder frei und Administratoren können sich wieder mit dem Server über einen Remotedesktop verbinden. Sie können sich auch mit der Terminaldiensteverwaltung von einem Server mit einen anderen Server verbinden lassen und dort Sitzungen freigeben. Klicken Sie dazu in der Konsolenstruktur mit der rechten Maustaste auf *Terminaldiensteverwaltung* und wählen Sie die Option *Verbindung mit Computer herstellen*. Wenn Sie über genügend Rechte auf dem anderen Server verfügen, können Sie auf diese Weise die Sitzungen auf mehreren Servern wieder freigeben.

Konfigurieren der Verbindungsmöglichkeiten

Sie können aber auch generelle Einstellungen vornehmen, damit Sitzungen nach gewisser Zeit automatisch freigegeben werden. Denken Sie aber daran, dass auch die Programme beendet werden, die in dieser Sitzung erstellt worden sind. Sie finden diese Konfiguration über *Start/Verwaltung/Terminaldienste/Terminaldienstekonfiguration*. Rufen Sie mit der rechten Maustaste die Eigenschaften der Verbindung *RDP-Tcp* auf. Sie finden an dieser Stelle zahlreiche Verwaltungsmöglichkeiten. Auf der Registerkarte *Sitzungen* können Sie das Zeitlimit für getrennte Sitzungen aktivieren und diese nach

einem Tag automatisch beenden lassen (Abbildung 3.9). Sie können hier auch Zeitlimits für verbundene und aktive Sitzungen sowie für Sitzungen, die zwar verbunden sind, über die aber kein Netzwerkverkehr läuft, festlegen.

Abbildg. 3.9 Konfigurieren der Verbindungseinstellungen über RDP



Remotedesktopverbindungen effizient mit Royal TS und VisionApp Remote Desktop verwalten

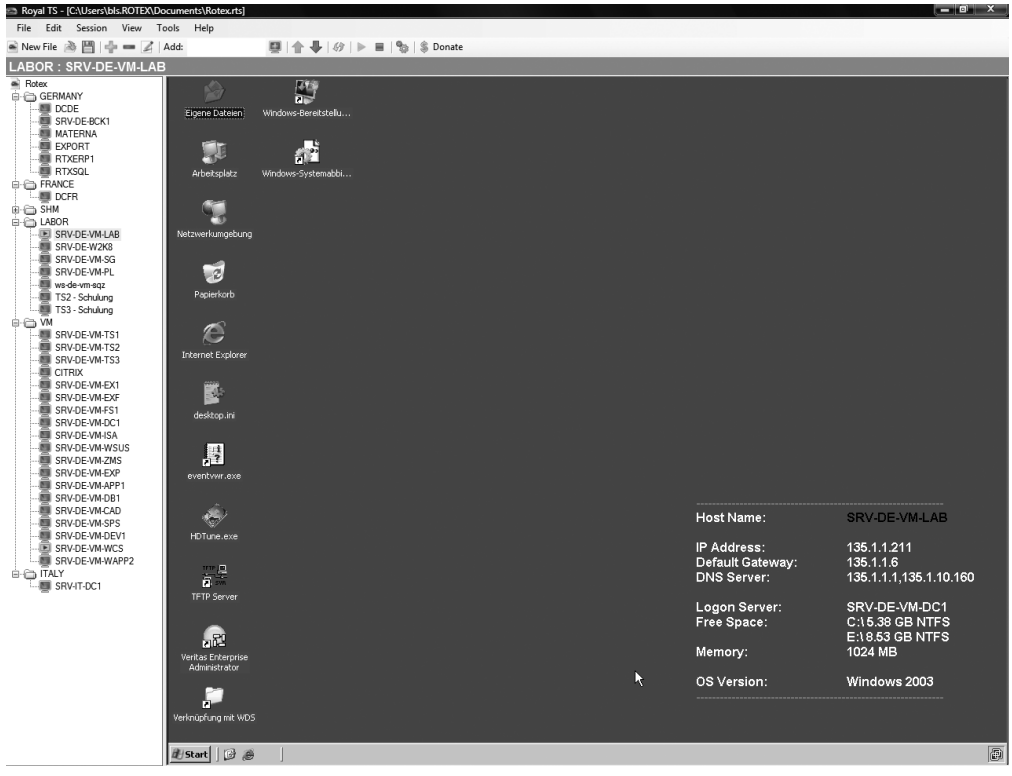
Viele Administratoren kennen das Problem: Im Unternehmen müssen zahlreiche Server verwaltet werden und zwar meistens auch noch gleichzeitig. Vor allem wenn mehrere Verbindungen parallel geöffnet werden, wird die Arbeit schnell unübersichtlich. Zwar gibt es das MMC-Snap-In *Remotedesktops*, allerdings ist dieses Werkzeug nicht so komfortabel wie kostenlose Zusatzprogramme. Optimal geeignet sind die beiden Freeware-Produkte Royal TS und VisionApp Remote Desktop.

Royal TS – Freeware-Verwaltung des Remotedesktops

Das Tool kann von der Internetseite *www.code4ward.net* heruntergeladen werden. Auf der Seite gibt es auch ein Forum, in welchem Fehler und neue Funktionen des Tools besprochen werden, und der Programmierer direkt antwortet. Die Größe des Tools beträgt rund 900 KB. Für die Installation wird .NET Framework 2.0 oder 3.0 vorausgesetzt, welches zu den Features von Windows Server 2008 gehört. Außerdem wird der Remotedesktopverbindungs-Client von Microsoft benötigt. Ist dieser auf dem Computer nicht bereits installiert, kann dieser Client kostenlos auf der Internetseite *http://support.microsoft.com/kb/925876* heruntergeladen werden. Der größte Nutzen des Tools ist die gemeinsame Verwaltung von mehreren Remotedesktops, die auch parallel geöffnet sein können. Administratoren können durch einen Mausklick zwischen den verschiedenen geöffneten RDP-Sit-

zungen wechseln. Der geöffnete Remotedesktop wird in der Mitte der Konsole als Vollbild angezeigt. Wem das nicht gefällt, kann einzelne Verbindungen so konfigurieren, dass diese in einem eigenen Fenster geöffnet werden. Alle gespeicherten Verbindungen zu anderen Servern werden auf der linken Seite der Oberfläche angezeigt. Die einzelnen Remotedesktopverbindungen lassen sich über einen Assistenten erstellen. Neben den Verbindungsoptionen wie Auflösung, verbundene Laufwerke, IP-Adresse oder Name des Servers, lässt sich auch eine Authentifizierung hinterlegen. So kann eine RDP-Verbindung per Doppelklick geöffnet werden.

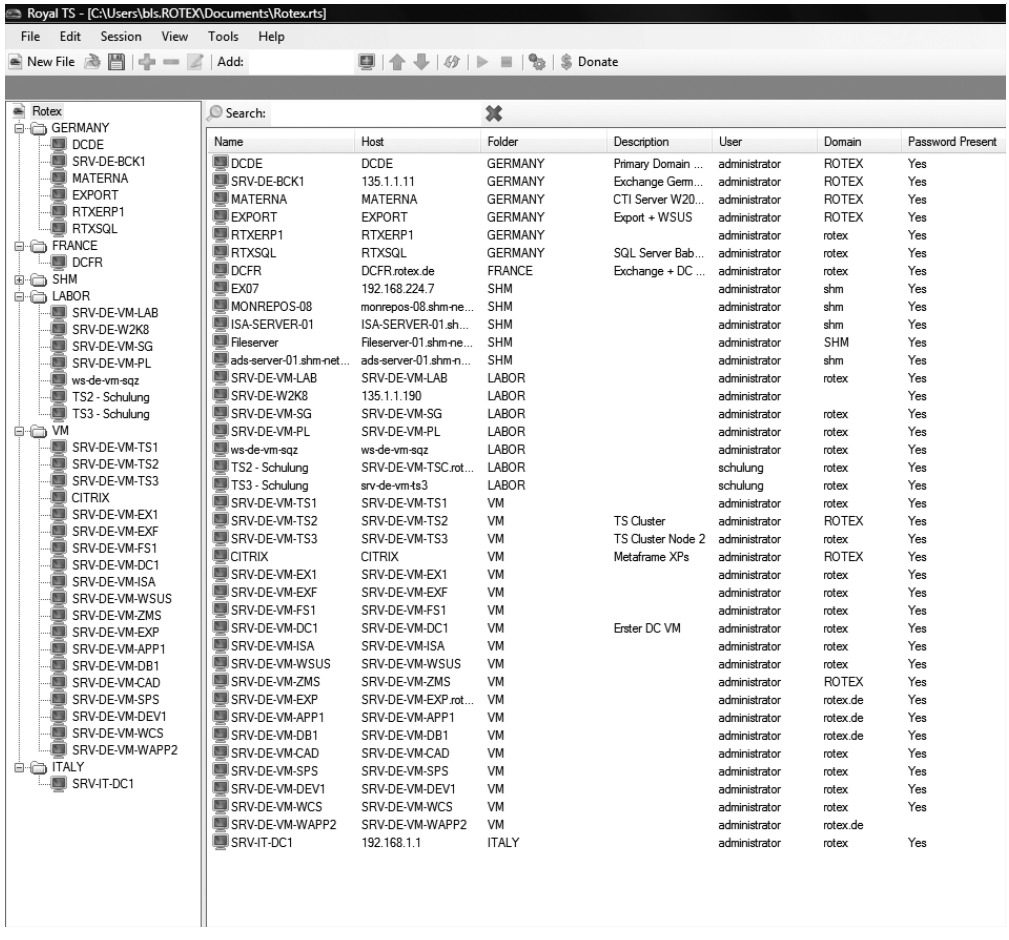
Abbildg. 3.10 Mit Royal TS können effizient Remotedesktopverbindungen unter Windows Server 2003, Windows Server 2008 und Windows 2000 Server parallel verwaltet werden



Die einzelnen Verbindungen lassen sich auch gruppieren. Weiterhin können mehrere Gruppen in einer so genannten RTS-Datei zusammengefasst werden. Royal TS lässt sich so konfigurieren, dass eine bestimmte Datei mit den enthaltenen Gruppen automatisch geöffnet wird. Die einzelnen Verbindungen lassen sich natürlich jederzeit umgruppieren. Die Authentifizierungsdaten werden verschlüsselt in der Verbindungsdatei gespeichert. Die Verschlüsselung ist allerdings nicht sehr zuverlässig und kann über die Windows PowerShell oder von .NET-Programmierern leicht ausgehebelt werden. Aus diesem Grund sollte die Datei, welche die Verbindungen enthält, extrem sicher aufbewahrt oder vom Speichern der Kennwörter abgesehen werden. Wer die Authentifizierungsoptionen speichert, muss diese für alle Verbindungen einzeln hinterlegen. Wird das Kennwort des hinterlegten Benutzerkontos geändert, müssen auch die einzelnen Verbindungen nachträglich angepasst werden. Leider ist eine sichere zentrale Speicherung für Authentifizierungsdaten nicht vorgesehen. Bei aufgebauten Ver-

bindungen kann die Größe des Fensters auch dynamisch vergrößert oder verkleinert werden, der Remotedesktop wird daraufhin automatisch angepasst. Diese Funktion wird in Royal TS *AutoExpand* genannt und automatisch aktiviert. Wer das nicht will, kann für die einzelnen Verbindungen auch eine Auflösung für den Remotedesktop vorgeben. Für jede Verbindung können die Einstellungen über das Kontextmenü nachträglich angepasst werden. Auch der RDP-Port, standardmäßig auf TCP 3389 konfiguriert, kann geändert werden. Für alle Verbindungen stehen über den Menübefehl *Tools/Options* Möglichkeiten zur Verfügung, um die Standardauflösung und Verbindungsoptionen zentral zu bearbeiten. Das Tool unterstützt neben Windows XP auch Windows Vista. Über die Datei *RTSApp.exe.config* im Installationsverzeichnis von Royal TS können zusätzlich einige Einstellungen angepasst werden, die nicht in der grafischen Benutzeroberfläche zur Verfügung stehen. So lässt sich in dieser Datei zum Beispiel über die Einstellung *ConfigurationPath* der Pfad zu den Benutzereinstellungen anpassen, was Unternehmen entgegenkommt, die mit servergespeicherten Profilen arbeiten. Standardmäßig werden die Benutzereinstellungen des Tools im Profil des Anwenders gespeichert. Treten nach Windows-Updates Fehler mit dem Tool auf, besonders unter Windows Vista, hilft oft das Löschen dieser Benutzerdateien, die anschließend automatisch neu erstellt werden.

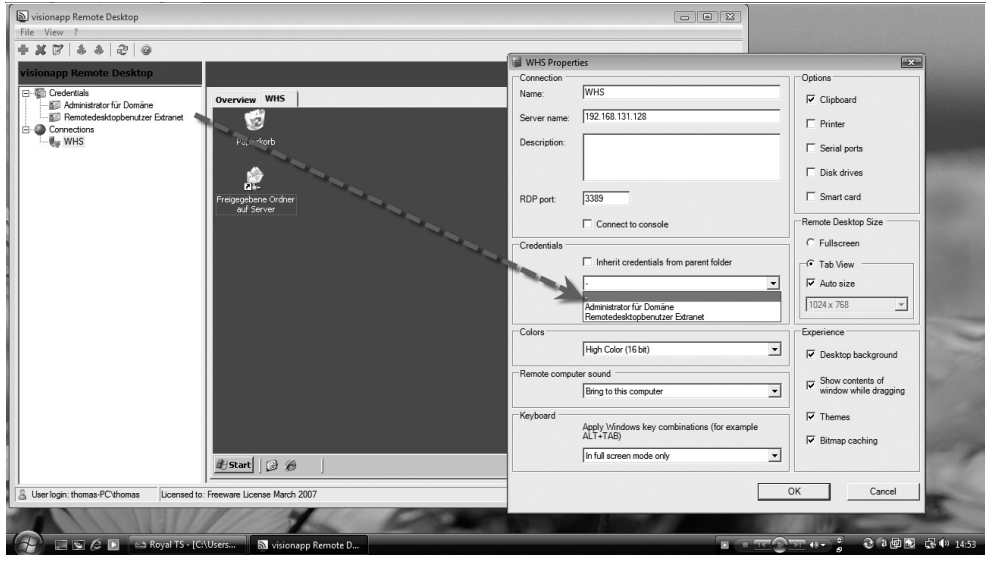
Abbildg. 3.11 Einzelne Server können in Gruppen zusammengefasst werden



visionapp Remote Desktop – Effiziente Gruppering von Remotedesktopverbindungen

In die gleiche Kerbe wie *Royal TS* schlägt die Software *visionapp Remote Desktop*. Das Programm kann von der Internetseite *http://www.visionapp.com* nach erfolgter Registrierung kostenlos heruntergeladen werden. Auch dieses Programm benötigt .NET Framework von Microsoft. Wie bei Royal TS lassen sich die Verbindungsinformationen und Authentifizierungsdaten für die Verbindungen hinterlegen. Die Einstellungsmöglichkeiten sind nahezu identisch. Hier zeigt sich auch der Vorteil von visionapp Remote Desktop im Vergleich zu Royal TS: Authentifizierungsinformationen lassen sich zentral vorgeben. Bei den einzelnen Verbindungen wird die einzelne Authentifizierungsinformation nur noch ausgewählt. Wird so ein Kennwort zentral geändert, müssen nicht alle Serververbindungen angepasst werden, sondern es reicht das Ändern der zentralen Authentifizierungsinformationen, die dadurch auch nur an einer Stelle gespeichert werden. Mit visionapp Remote Desktop können die Verbindungen auch effizienter gruppiert werden als mit Royal TS. Verbindungen können in Ordner zusammengefasst werden und auch eine Verschachtelung dieser Ordner ist möglich. Royal TS bietet keine Verschachtelung an, sondern nur eine einfache Ordnerstruktur. Für jeden Ordner kann eine Authentifizierungsinformation hinterlegt werden, die wiederum aus dem zentralen Bereich *Credentials* übernommen wird.

Abbildg. 3.12 visionapp Remote Desktop unterstützt die zentrale Verwaltung von Authentifizierungsoptionen



Für einzelne Verbindungen kann auch eine eigene Authentifizierung hinterlegt werden. Unternehmen die auch für Administratoren regelmäßig das Kennwort ändern, profitieren von dieser Möglichkeit. Beim Beenden werden Änderungen automatisch gespeichert. Über das Menü *File* können die aktuellen Verbindungsinformationen in einer Datei gesichert werden. Auf die gleiche Weise ist auch eine Wiederherstellung möglich. visionapp Remote Desktop sichert den Zugriff auf die Datei mit einem Kennwort ab, sodass ein Unbefugter, der sich die Datei kopiert, die Verbindungen darin nicht nutzen kann. Das Tool unterstützt ab der Version 1.5 offiziell Windows Vista. Springt bei einer geöffneten Sitzung der Bildschirmschoner an, ist die Maus leider auch bei den anderen geöffneten Sitzungen deaktiviert. Hier hilft es, wenn in die Sitzung mit aktiviertem Bildschirmschoner geklickt wird, damit dieser deaktiviert wird. Bei vielen gleichzeitig geöffneten Verbindungen kann dieses Problem aber sehr stö-

rend wirken, da erst die Verbindung mit dem aktivierten Bildschirmschoner gefunden werden muss. visionapp Remote Desktop bietet im Hauptfenster noch die Registerkarte *Overview* an. Hier werden alle geöffneten Verbindungen in einer kleinen Übersicht angezeigt, sodass schnell erkannt werden kann, wenn in einer Sitzung zum Beispiel ein Meldefenster erscheint. Über diese zentrale Sicht der Verbindungen kann per Doppelklick auch direkt zu einer einzelnen Verbindung gesprungen werden. Alle geöffneten Verbindungen werden nicht nur auf der linken Seite angezeigt, sondern zusätzlich als eigene Registerkarte. So verliert ein Administrator nie die Übersicht, welche Verbindungen aktuell geöffnet sind. Durch die Registerkarten wird die Navigation zwischen den verschiedenen Sitzungen extrem erleichtert. Zusätzlich bietet die Software auch die Unterstützung für Mehr-Monitor-Systeme an.

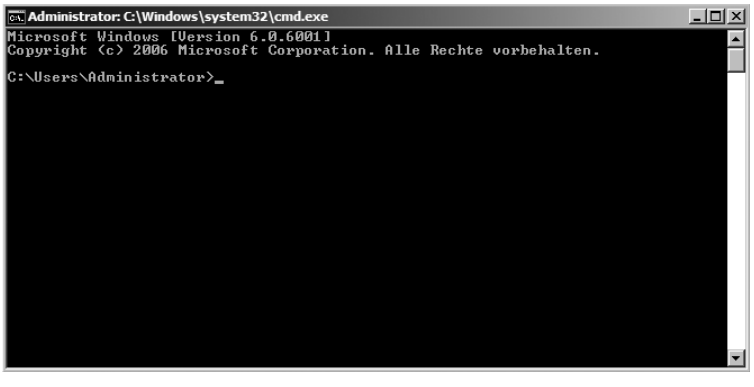
Fazit

Beide Programme sind kostenlos, bieten aber eine Menge Funktionen. Administratoren und Consultants, die mit vielen Remotedesktopverbindungen arbeiten, profitieren von beiden Lösungen. Im Vergleich zu Royal TS überzeugt visionapp Remote Desktop etwas mehr. Zum einen bietet die bessere Gruppierungsmöglichkeit mit verschachtelten Ordnern und den Registerkarten eine bessere Übersicht. Zum anderen sind die zentralen Authentifizierungsinformationen ein klarer Vorteil, wenn häufiger das Kennwort geändert werden muss. Auch die Möglichkeit, die Verbindungsdatei mit einem Kennwort abzusichern, spricht für visionapp. Gelangt ein Unbefugter an eine Royal TS-Datei, kann er diese uneingeschränkt nutzen, was vor allem bei hinterlegten Authentifizierungsinformationen ein großes Problem darstellen kann. Bei visionapp ist allerdings der Bildschirmschoner-Bug etwas störend.

Verwalten eines Core-Servers

Die Verwaltung eines Core-Servers läuft hauptsächlich über die Befehlszeile ab. Mit dem Befehl *start cmd /separate*, öffnen Sie ein neues Befehlszeilenfenster. Wird ein Fenster geschlossen, lässt sich über den Task-Manager durch Erstellen eines neuen Tasks mit dem Befehl *cmd* ein neues Fenster starten, aber mit einem zweiten Fenster ersparen Sie sich diese Arbeit. Alle Tools, die eine grafische Oberfläche verwenden oder sogar den Windows-Explorer benötigen, funktionieren auf einem Core-Server nicht. Aus diesem Grund werden auch keine Meldungen angezeigt, wenn neue Updates zur Verfügung stehen oder das Kennwort eines Benutzers abgelaufen ist. Einige Fenster funktionieren auch auf einem Core-Server, so kann zum Beispiel der Editor (*notepad.exe*) verwendet werden, um Skripts oder Dateien zu bearbeiten.

Abbildg. 3.13 Verwalten eines Core-Servers über die Befehlszeile



TIPP Sie können auch einen Core-Server über die Terminaldienste verwalten. In diesem Fall wird in der Sitzung als Shell ebenfalls die Befehlszeile angezeigt.

HINWEIS Als Befehlszeilenfenster für einen Core-Server wird nicht die PowerShell verwendet, sondern die herkömmliche Befehlszeile, die auch unter Windows Server 2003 verwendet wird.

Grundlegende Optionen müssen zunächst direkt auf dem System gesetzt werden, damit dieses über das Netzwerk ansprechbar ist. Neben einem sicheren Kennwort für das Adminkonto gehören dazu der Servername und natürlich die IP-Adresse. Eine Auflistung aller Netzwerkadapter können Sie mit *netsh interface ipv4 show interface* durchführen. Die LAN-Anbindung lässt sich zum Beispiel durch folgende Befehle durchführen:

netsh interface ipv4

set address "Local Area Connection"

static 10.0.0.2 255.255.255.0 192.168.217.1

Den Namen in Anführungszeichen, also die Bezeichnung der Netzwerkverbindung, sehen Sie, wenn Sie *netsh interface ipv4 show interface* ausführen. Auf dieselbe Weise lassen sich DNS- und WINS-Server eintragen. Die Onlinehilfe von *netsh* gibt die nötigen Auskünfte. Um den Server umzubenennen, verwenden Sie *netdom.* Ein Beispiel könnte sein:

netdom renamecomputer <ALTER NAME> /newname:<NEUER NAME> /force /reboot:30

Für einige Aktionen gibt es keine Befehle. Hierfür verfügt Windows Server 2008 über einen Satz von VBS-Skripts. Dazu zählt zum Beispiel *SCregEdit.wsf*, mit dem Sie über die Registrierungsdatenbank Funktionen wie den administrativen RDP-Zugriff oder die automatischen Updates freischalten sowie die Konfiguration von DNS-Einträgen für Active Directory vornehmen. Die Systemsteuerung beruht auf dem normalen Explorer und ist daher nicht verfügbar. Ausnahme ist die Zeitzone, welche sich über *control timedate.cpl* aufrufen lässt. Auch die Regions- und Sprachoptionen können Sie mit *control intl.cpl* setzen. Haben Sie sich für die Installation eines Core-Servers entschlossen, helfen Ihnen die folgenden Internetseiten weiter, auf denen Sie ausführliche Informationen zur Verwaltung des Servers in der Befehlszeile erhalten:

- **Befehlszeilen-Referenz** *http://go.microsoft.com/fwlink/?LinkId=20331.* Alle diese Befehle können auch in der Befehlszeile eines Core-Servers verwendet werden.
- ***Netsh*-Befehl zur Konfiguration der Netzwerkeinstellungen** *http://go.microsoft.com/fwlink/?LinkId=49654*

Wichtige Administrationsaufgaben

Für die Einrichtung eines Servers sollten Sie noch einige Punkte anpassen. Im folgenden Abschnitt gehen wir genauer auf diese wichtigen ersten Konfigurationsmaßnahmen ein.

Sprach- und Zeiteinstellungen konfigurieren

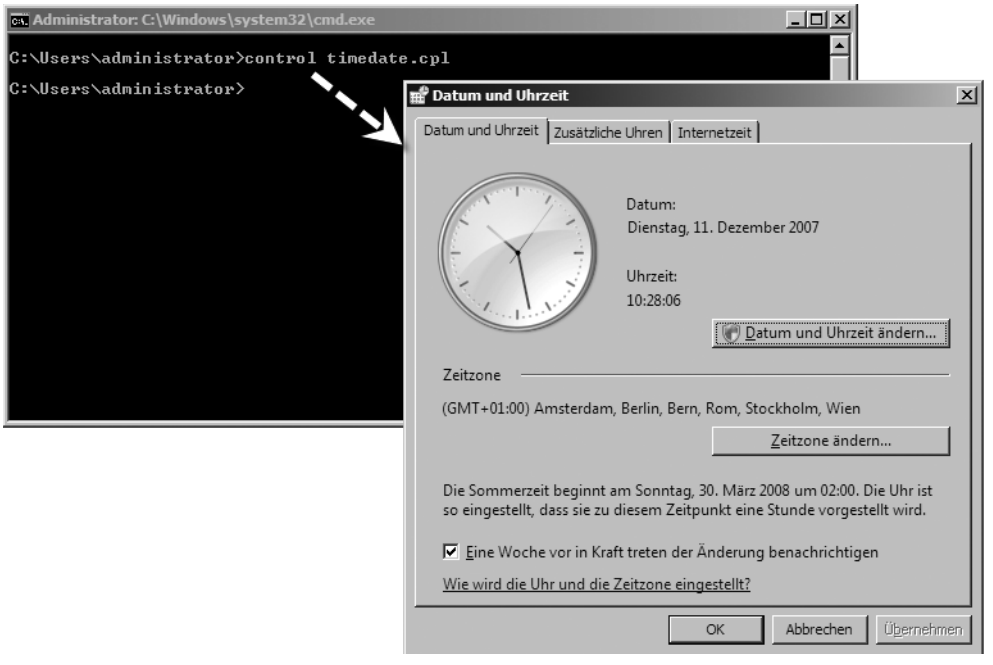
Da es für die Konfiguration der Spracheinstellungen noch keine Möglichkeit in der Befehlszeile gibt, steht für diese Konfiguration eine grafische Oberfläche zur Verfügung. Geben Sie zur Konfiguration

der Sprach- oder Tastatureinstellungen in der Befehlszeile den Befehl *control intl.cpl* ein. Anschließend öffnet sich ein Fenster, über das die Spracheinstellungen vorgenommen werden.

TIPP Sind auf einem Server mehrere Sprachen installiert, kann mit der Tastenkombination ⇧ + Alt die jeweilige Sprache umgeschaltet werden.

Die Zeiteinstellungen werden über *control timedate.cpl* eingestellt. Auch hier steht eine grafische Oberfläche zur Konfiguration der Uhrzeit, des Datums und der Zeitzone zur Verfügung.

Abbildg. 3.14 Für Uhrzeit, Datum, Zeitzone und installierte Sprachen stehen auch auf einem Core-Server grafische Möglichkeiten zur Verfügung



Ändern des Administrator-Kennwortes

Um das lokale Administrator-Kennwort eines Servers anzupassen, gehen Sie folgendermaßen vor:

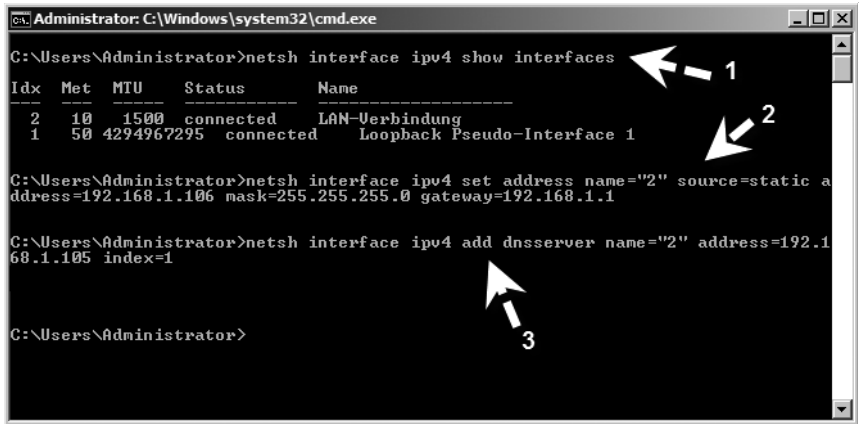
1. Geben Sie in der Befehlszeile den Befehl *net user administrator* * ein. Durch die Eingabe des Platzhalters *, wird das eingegebene Kennwort nicht in Klartext angezeigt.
2. Geben Sie das neue Kennwort ein und bestätigen Sie.
3. Geben Sie das Kennwort noch mal ein und bestätigen Sie erneut.

Konfigurieren einer statischen IP-Adresse

Eine weitere wichtige Aufgabe besteht darin, dem Core-Server eine statische IP-Adresse zuzuweisen. Standardmäßig wird dem Server eine dynamische IP-Adresse per DHCP zugewiesen:

1. Lassen Sie sich mit dem Befehl *netsh interface ipv4 show interfaces* die Konfiguration der Netzwerkkarte anzeigen. Notieren Sie sich in der Spalte *Idx* die ID der Netzwerkkarte, deren Konfiguration Sie anpassen wollen (Abbildung 3.15).
2. Um eine statische IP-Adresse zuzuweisen, geben Sie den Befehl *netsh interface ipv4 set address name="<ID>" source=static address=<IP-Adresse> mask=<Subnetzmaske> gateway=<Standardgateway>* ein.
3. Geben Sie als Nächstes den Befehl *netsh interface ipv4 add dnsserver name="<ID>" address=<DNS-Server IP-Adresse> index=1* ein. Wollen Sie weitere DNS-Server hinterlegen, gehen Sie analog vor und erhöhen jeweils den Index abhängig davon, in welcher Reihenfolge die DNS-Server befragt werden sollen.

Abbildg. 3.15 Konfiguration der Netzwerkverbindung für einen Core-Server



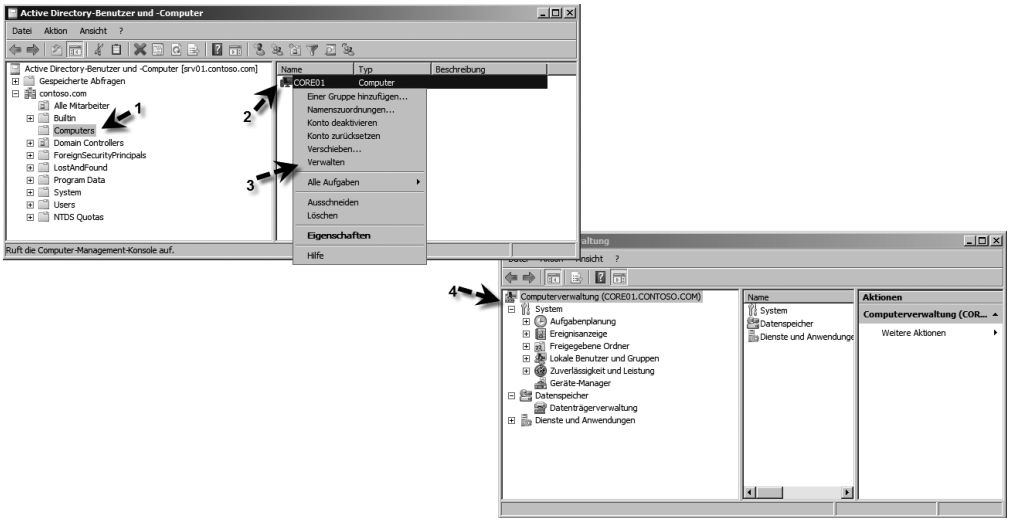
Mit dem Befehl *netsh interface ipv4 set address name="<ID>" source=dhcp* setzen Sie diese Konfiguration wieder zurück. Nachdem Sie die IP-Konfiguration vorgenommen haben, sollten Sie mit *nslookup* überprüfen, ob Sie den DNS-Server erreichen können und Namen aufgelöst werden. Zusätzlich sollten Sie den Domänencontroller oder andere Server im gleichen Netzwerk per Ping erreichen können.

HINWEIS Nachdem Sie einen Core-Server installiert haben, können Sie zwar ohne Weiteres auf andere Server im Netzwerk zugreifen, aber der eingehende Netzwerkverkehr, einschließlich Ping, wird durch den Core-Server blockiert. Damit Sie mit den verschiedenen Verwaltungsprogrammen über das Netzwerk zugreifen können, müssen Sie auf dem Core-Server zunächst die Firewall so konfigurieren, dass die Verwaltungswerkzeuge über das Netzwerk zugelassen werden. Verwenden Sie dazu den Befehl *netsh advfirewall set allprofiles settings remotemanagement enable* oder den Befehl *netsh advfirewall firewall set rule group="remoteverwaltung" new enable=yes*. Auf englischen Servern heißen die Regeln "*Remote Administration*". Den kompletten Netzwerkverkehr auf einem Core-Server können Sie über *netsh advfirewall set allprofiles firewallpolicy allowinbound,allowoutbound* freischalten. Um die Firewallregeln für Core-Server zu steuern, bietet es sich an, dass Sie den Core-Server in eine eigene OU legen, auf die Sie eine Gruppenrichtlinie verknüpfen. In dieser Richtlinie können Sie die Regeln für die Firewall hinterlegen, damit die Kommunikation funktioniert. Anschließend kann zum Beispiel das Snap-In *Computerverwaltung* auf einem anderen Server so konfiguriert werden, dass der Core-Server verwaltet werden kann.

Abbildg. 3.16 Damit von anderen Servern mit Verwaltungswerkzeugen auf den Core-Server zugegriffen werden kann, müssen erst die Firewallregeln angepasst werden

Die *Computerverwaltung* starten Sie zum Beispiel über das Snap-In *Active Directory-Benutzer und -Computer*. Klicken Sie den Core-Server in der Konsole mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Verwalten*. Anschließend kann der Server über eine grafische Oberfläche konfiguriert werden. Über diesen Weg lassen sich zum Beispiel wesentlich einfacher Freigaben und Systemdienste verwalten als über die Befehlszeile des Core-Servers.

Abbildg. 3.17 Nach dem Anpassen der Firewall-Regeln auf dem Core-Server kann die Computerverwaltung über das Netzwerk gestartet werden

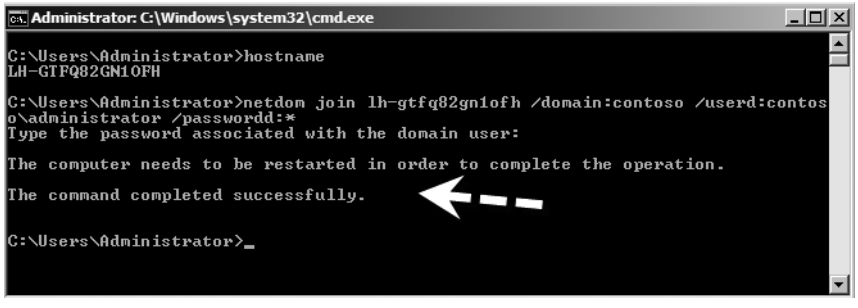


Mit einem Core-Server einer Domäne beitreten

Ein weiterer wichtiger Schritt ist das Beitreten zu einer Windows-Domäne. Auch diese Aufgabe müssen Sie über die Befehlszeile durchführen. Zunächst sollten Sie sicherstellen, dass Sie, wie im vorangegangenen Abschnitt besprochen, die IP-Adresse richtig einstellen und mit *Ping* und *Nslookup* überprüfen, ob der Domänencontroller und DNS-Server erreicht werden kann. Ist dies gewährleistet, können Sie der Domäne beitreten. Gehen Sie dazu folgendermaßen vor:

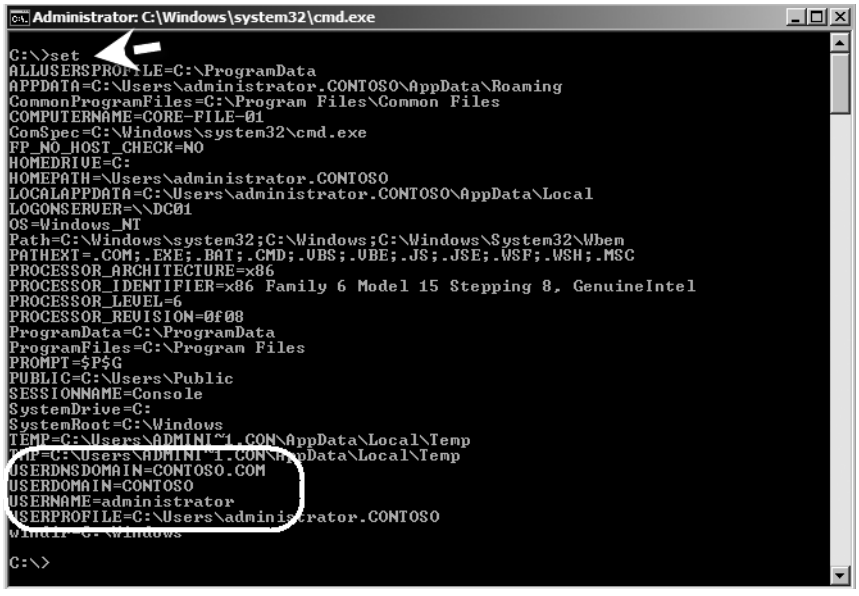
1. Geben Sie den Befehl *hostname* ein und notieren Sie sich den standardmäßig gesetzten Namen. Diesen können Sie später umbenennen. Alternativ können Sie auch *set c* eingeben. Dann erscheint auch der Computername. Auch über *ipconfig /all* oder *Systeminfo* kann der Name angezeigt werden.
2. Geben Sie den Befehl *netdom join <Computername> /domain:<NetBIOS-Domänen-Namen> / userd:<Domäne>\<Benutzernamen> /passwordd:** ein. Wollen Sie später einen Server wieder aus der Domäne entfernen, verwenden Sie den Befehl *netdom remove*.
3. Anschließend müssen Sie das Kennwort für den Administrator eingeben, mit dem Sie den Server in die Domäne aufgenommen haben. Nach einigen Sekunden sollte der erfolgreiche Domänenbeitritt angezeigt werden (Abbildung 3.18). Sollten Sie hier eine Fehlermeldung erhalten, überprüfen Sie zunächst, ob Sie mit Ping den Domänencontroller mit NetBIOS-Namen und IP-Adressen erreichen können, damit sichergestellt ist, dass die IP-Konfiguration stimmt. Da Sie für den Domänenbeitritt auch den Namen des Servers angeben müssen, sollten Sie überprüfen ob Sie diesen richtig eingegeben haben. In der Befehlszeile wird oft die Null »0« mit einem großen »O« verwechselt. Sie können überprüfen, ob Sie den Namen richtig eingegeben haben, indem Sie lokal auf dem Server den Befehl *ping <Servername>* eingeben. Wird auf den Ping erfolgreich geantwortet, haben Sie den korrekten Namen verwendet.

Abbildg. 3.18 Erfolgreicher Domänenbeitritt eines PCs



4. Nach der erfolgreichen Aufnahme in die Domäne müssen Sie den Server neu starten. Geben Sie dazu den Befehl *shutdown /r /t 0* ein. Mit dem Befehl wird der Server neu gestartet. Weitere Optionen zum Herunterfahren zeigen wir Ihnen im nächsten Abschnitt.
5. Nach dem Neustart können Sie sich über die Schaltfläche *Anderer Benutzer* an der Domäne anmelden. Sie können über den Befehl *set* in der Befehlszeile überprüfen, ob die Domänenaufnahme funktioniert hat (Abbildung 3.19). Mit *Nslookup* können Sie überprüfen, ob sich der Server korrekt in die DNS-Zone eingetragen hat.

Abbildg. 3.19 Überprüfen der Domänenmitgliedschaft mit dem Befehl *set*



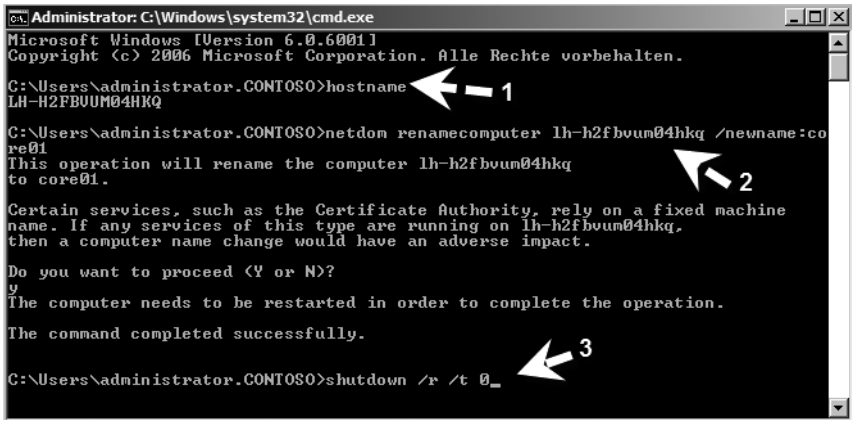
Server über die Befehlszeile umbenennen

Nachdem Sie der Domäne mit dem Standardnamen des Servers beigetreten sind, können Sie den Namen des Servers ändern:

1. Geben Sie in der Befehlszeile den Befehl *netdom renamecomputer <Alter Computername> /newname:<Neuer Computername>* ein.

   Bestätigen Sie das Umbenennen mit der Taste [Y], wenn die Taste [J] nicht funktioniert.
2. Starten Sie den Server mit *shutdown /r /t 0* durch (Abbildung 3.20).

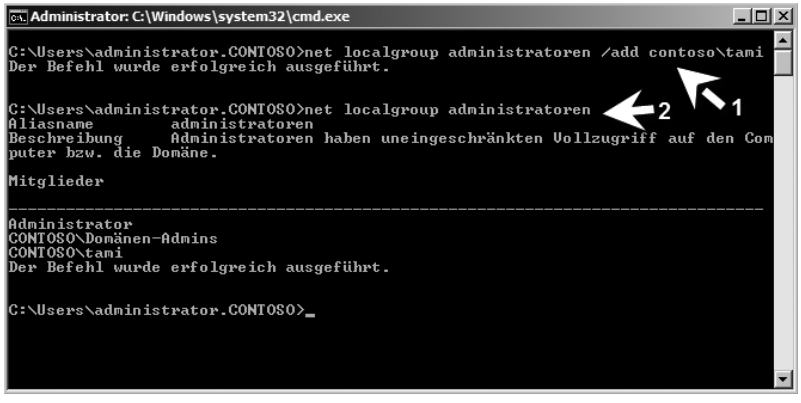
Abbildg. 3.20 Umbenennen eines Core-Servers in der Befehlszeile



Gruppenmitgliedschaften in der Befehlszeile konfigurieren

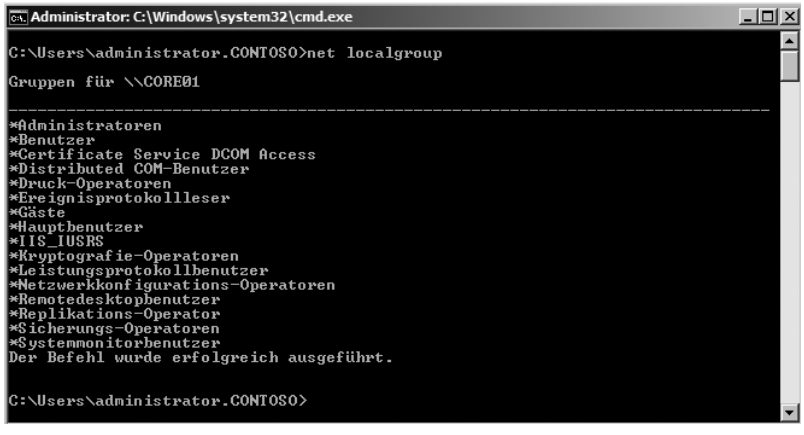
Nehmen Sie einen Server in die Domäne auf, wird die Domänengruppe der Domänen-Admins automatisch in die lokale Administrator-Gruppe aufgenommen. Wollen Sie neben dieser Gruppe einzelne Benutzerkonten oder zusätzliche Gruppen aufnehmen, können Sie diese Aufgabe ebenfalls in der Befehlszeile durchführen. Mit dem Befehl *net localgroup administratoren /add <Domäne>\<Benutzername>* wird der konfigurierte Benutzer der lokalen Administrator-Gruppe auf dem Server hinzugefügt. Mit dem Befehl *net localgroup administratoren* können Sie sich alle Gruppenmitglieder anzeigen lassen (Abbildung 3.21).

Abbildg. 3.21 Überprüfen und Konfigurieren der lokalen Administrator-Gruppe auf einem Core-Server



Mit dem Befehl *net localgroup* können Sie sich alle lokalen Gruppen auf dem Server anzeigen lassen. So können Sie mit diesem Befehl schnell feststellen, welche Gruppen es gibt und welche Benutzerkonten enthalten sind. Außerdem können Sie neue Benutzerkonten hinzufügen.

Abbildg. 3.22 Anzeigen der lokalen Benutzergruppen auf dem Server



Mit dem Befehl *net localgroup administratoren /delete <Domäne>\<Benutzername>* entfernen Sie ein Benutzerkonto wieder aus der Gruppe.

Herunterfahren von Servern mit *Shutdown.exe*

Zum Herunterfahren oder Neustarten wird der Befehl *Shutdown* verwendet. Der Computer fährt daraufhin nach 30 Sekunden herunter und startet wieder. Wird der Befehl *shutdown /r /f /t 0* verwendet, fährt der Computer sofort herunter. Die Option */f* zwingt den PC zum Beenden der laufenden Anwendungen, auch wenn nicht gespeichert wurde. Der Befehl *shutdown /s /f* fährt den Computer herunter und startet ihn nicht neu. Mit dem Befehl *shutdown /a* kann der aktuelle Herunterfahren-Vorgang abgebrochen werden, wenn der Computer noch nicht mit dem Herunterfahren begonnen hat, sondern die Zeit noch läuft. Die wichtigsten Optionen des Shutdown-Befehls sind:

- **/g** Startet den Computer neu und startet registrierte Anwendungen automatisch nach dem Neustart.
- **/i** Zeigt eine grafische Benutzeroberfläche an. Dies muss die erste Option sein.
- **/l** Meldet den aktuellen Benutzer ab. Diese Option kann nicht zusammen mit den Optionen */m* oder */d* verwendet werden.
- **/s** Fährt den Computer herunter
- **/r** Fährt den Computer herunter und startet ihn neu
- **/a** Bricht das Herunterfahren des Systems ab
- **/p** Schaltet den lokalen Computer ohne Zeitlimitwarnung aus. Kann mit den Option */d* und */f* verwendet werden.
- **/h** Versetzt den lokalen Computer in den Ruhezustand
- **/m \\<Computer>** Legt den Zielcomputer fest
- **/t xxx** Stellt die Zeit vor dem Herunterfahren auf xxx Sekunden ein. Der gültige Bereich ist von 0 bis 600, der Standardwert ist 30. Die Verwendung von */t* setzt voraus, dass die Option */f* verwendet wird.
- **/c "Kommentar"** Kommentar bezüglich des Neustarts bzw. Herunterfahrens. Es sind maximal 512 Zeichen zulässig.
- **/f** Erzwingt das Schließen ausgeführter Anwendungen ohne Vorwarnung der Benutzer. */f* wird automatisch angegeben, wenn die Option */t* verwendet wird.
- **/d** [**p**|**u:**]**xx:yy** Gibt die Ursache für den Neustart oder das Herunterfahren an. *p* gibt an, dass der Neustart oder das Herunterfahren geplant ist. *u* gibt an, dass die Ursache vom Benutzer definiert ist. Wenn weder *p* noch *u* angegeben ist, ist das Neustarten oder Herunterfahren nicht geplant.

Rechner über das Netzwerk herunterfahren – *PSShutdown*

Mit dem Befehlszeilentool *psshutdown.exe* aus der Sysinternals-PSTools-Sammlung können Computer über das Netzwerk ebenfalls neu gestartet oder heruntergefahren werden. Die Sammlung und die anderen Sysinternal-Tools erreichen Sie am schnellsten über den Link *www.sysinternal.com*. Das Tool entspricht dem Bordmittel *Shutdown.exe*, bietet aber deutlich mehr Optionen und Möglichkeiten. Mit PSShutdown kann sowohl auf lokalen als auch auf entfernten Systemen gearbeitet werden. Dabei ist es nicht notwendig, dass auf einem Remotesystem eine Software oder Teile davon installiert werden. Das Programm kann nicht nur Computer neu starten, sondern auch ein Notebook in den Energiesparmodus versetzen. Die Option *–m* bekommt als Parameter die Meldung zum Herun-

terfahren in Anführungszeichen. Mit dem Schalter *–t* kann der Standardwert für das Timeout verändert werden. Es ist möglich einen Wert in Sekunden anzugeben, oder den Zeitpunkt festzulegen, zu dem ein Shutdown ausgeführt werden soll. Der Zeitpunkt wird dabei durch die Verwendung der 24-Stunden-Schreibweise festgelegt. Das folgende Beispiel wird das lokale System um 23:00 Uhr neu starten und dabei den Anwendern mitteilen, weshalb dies geschieht: *psshutdown –m "Dieses System muss neu gestartet werden, da Logdateien gelöscht werden müssen" –t 23:00 –r*. Mit *–c* wird dem Meldungsfeld eine *Abbrechen*-Schaltfläche hinzugefügt. Als Zusatz zu der Standardmöglichkeit stellt PSShutdown zwei Operationen zur Verfügung, die zum Bereich der Desktopverwaltung gehören: *lock* und *logoff*. Mit ihrer Hilfe kann ebenfalls lokal oder über das Netz ein Anwender zwangsweise abgemeldet oder der Bildschirm gesperrt werden. Sie können auch gleichzeitig mehrere Systeme neu starten: *psshutdown –r \computer1,computer2,computer3*. Alternativ können die Rechnernamen auch in eine Textdatei aufgenommen werden: *psshutdown –r @rechnerliste.txt*. In dieser Datei darf in jeder Zeile nur ein Computername aufgelistet sein.

Beispiele:

- **Neustart** *psshutdown.exe –r –c –t 5 –m "Neustart in 5 Sekunden"*
- **Ausschalten** *psshutdown.exe –k –f –c –t 5 –m "Shutdown in 5 Sekunden"*
- **Abbruch** *psshutdown.exe –a*

Core-Server aktivieren

Ein wichtiger Schritt, der auch bei einem Core-Server nicht vergessen werden sollte, ist das Aktivieren. Über den Befehl *slmgr.vbs –ato* können Sie den Server aktivieren, wenn dieser über eine funktionsfähige Internetverbindung verfügt.

TIPP Haben Sie keine direkte Internetverbindung auf dem Server und verwenden einen Proxy, können Sie diesen über die Anweisung *netsh winhttp set proxy <Proxy>:<Port>* auf dem Server eintragen.

Wollen Sie den Server über einen KMS aktivieren, verwenden Sie den Befehl *cscript windows\system32\slmgr.vbs <Servername> <Benutzername> <Kennwort>:–ato*. Die wichtigsten Optionen für das Programm sind:

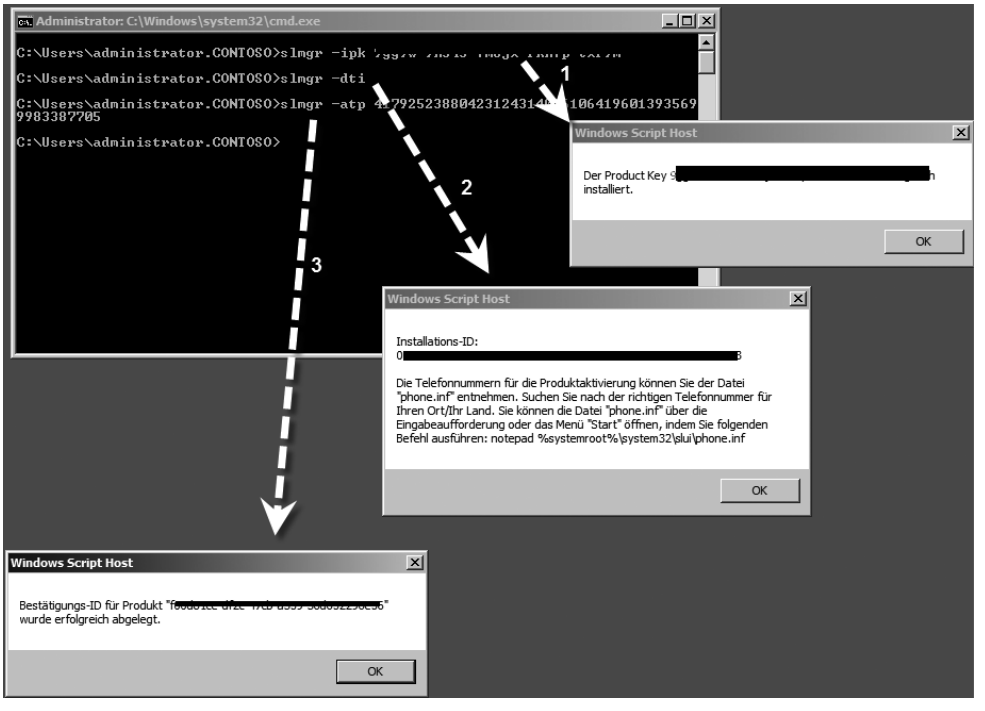
- **–ato** Windows online aktivieren
- **–rearm** Mit dieser Option können Sie den anfänglichen Testzeitraum von 60 Tagen zusätzlich dreimal auf insgesamt 240 Tage verlängern. Während dieser Zeit können Sie mit Windows Server 2008 ohne Aktivierung uneingeschränkt arbeiten.
- **–dli** Zeigt die aktuellen Lizenzinformationen an
- **–dlv** Zeigt noch mehr Lizenzdetails an
- **–dlv all** Zeigt detaillierte Infos für alle installierten Lizenzen

Um einen Server lokal über das Telefon zu aktivieren, verwenden Sie den Befehl *slmgr –dti*. Notieren Sie sich die ID, die generiert wird, und rufen Sie die Aktivierungsnummer von Microsoft an. Wählen Sie entweder die gebührenfreie Rufnummer *0800-284 828 3* oder die gebührenpflichtige Rufnummer *069 5007 0025*. Der Telefoncomputer fordert Sie auf, die angegebene Installations-ID anzu-

geben Geben Sie die ID ein und Sie erhalten vom Telefoncomputer eine Aktivierungs-ID. Diese geben Sie mit dem Befehl *slmgr –atp <Aktivierungs-ID>* ein.

1. Haben Sie während der Installation keine Produkt-ID eingegeben, können Sie diese über den Befehl *slmgr –ipk <Produkt-ID>* eingeben.
2. Anschließend lassen Sie sich über den Befehl *slmgr –dti* die dazugehörige Aktivierungs-ID anzeigen. Im Gegensatz zu einem normalen Server, wird die Aktivierungs-ID nicht in sechs Blöcken dargestellt, sodass die Anzeige etwas verwirrt. Bevor Sie also einen Core-Server über *Slmgr* aktivieren, sollten Sie die Aktivierungs-ID notieren und in Sechserblöcken unterteilen.
3. Anschließend erhalten Sie vom Telefoncomputer die notwendige ID und tragen diese über *slmgr –atp* ein (Abbildung 3.23).

Abbildg. 3.23 Aktivieren eines Core-Servers über das Telefon



Die Installation und die Verwaltung von zusätzlichen Serverrollen erläutern wir Ihnen in Kapitel 4. In diesem Kapitel zeigen wir Ihnen auch die Installation und Verwaltung von Serverrollen auf herkömmlichen Servern.

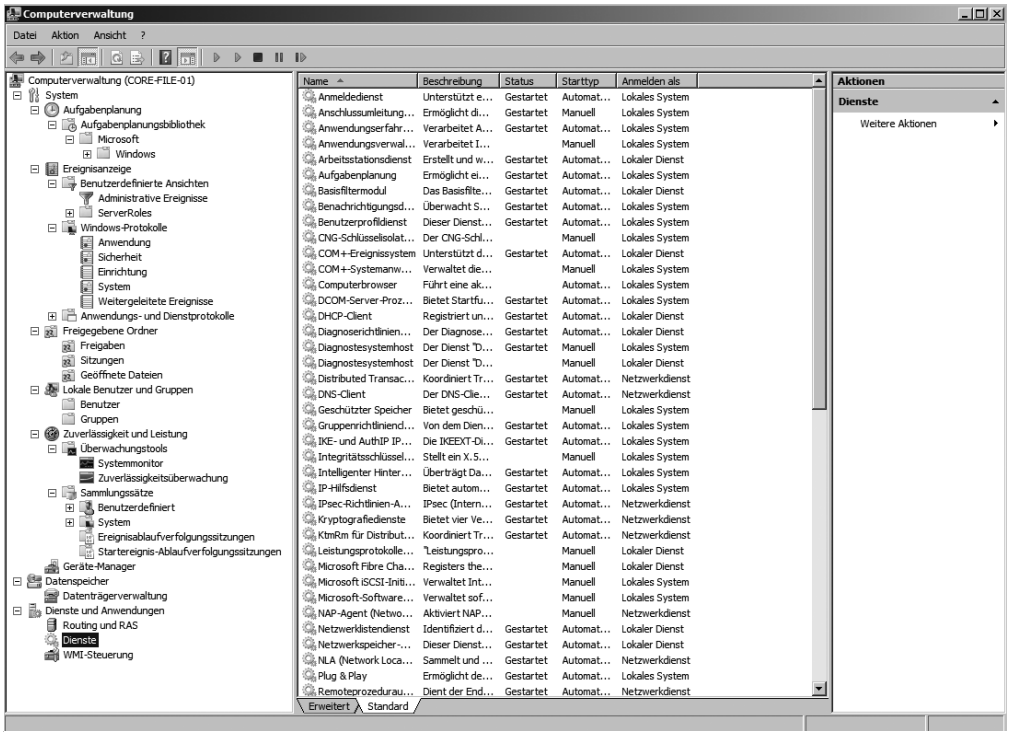
Remoteverwaltung eines Core-Servers

Neben der lokalen Administration können Sie, wie bei herkömmlichen Windows Server 2008-Servern auch über das Netzwerk auf einen Core-Server zugreifen. Dazu stehen mehrere Möglichkeiten zur Verfügung, die wir Ihnen auf den folgenden Seiten zeigen. Die Installation von Serverrollen und Funktionen auf einem Core-Server zeigen wir Ihnen in Kapitel 4. Zur Verwaltung der installierten

Serverrollen können Sie auch die MMC-Snap-Ins auf anderen Servern verwenden und sich über das Snap-In mit dem Core-Server verbinden. Die Administration ist in diesem Fall identisch mit der Verwaltung eines lokalen Servers. Achten Sie darauf, vorher das Remotemanagement in der Firewall freizuschalten. Verwenden Sie dazu den Befehl *netsh advfirewall set allprofiles settings remotemanagement enable*. Den kompletten Netzwerkverkehr auf einem Core-Server können Sie über *netsh advfirewall set allprofiles firewallpolicy allowinbound,allowoutbound* freischalten. Anschließend können Sie über die einzelnen MMCs, zum Beispiel auch direkt über die Computerverwaltung, auf die Funktionen des Core-Servers zugreifen und diesen verwalten (Abbildung 3.24).

TIPP Die Computerverwaltung auf einem Server starten Sie am besten über *Start/Ausführen/compmgmt.msc*. Um sich mit einem anderen Server zu verbinden, zum Beispiel einem Core-Server, klicken Sie mit der rechten Maustaste auf den obersten Eintrag *Computerverwaltung* und wählen im Kontextmenü den Eintrag *Verbindung mit einem anderen Computer herstellen* aus. Anschließend können Sie sich mit jedem anderen Server der Domäne verbinden, auch mit Core-Servern.

Abbildg. 3.24 Verwalten eines Core-Servers über die Computerverwaltung eines herkömmlichen Servers



Konfigurieren eines Core-Servers mit *scregedit.wsf*

Sie können allerdings nicht alle Funktionen auf einem Core-Server über das Netzwerk aktivieren. Dazu gehören zum Beispiel die Aktivierung und Verwaltung der automatischen Updates oder die Aktivierung des Remotedesktops. Für diese Funktionen steht auf einem Core-Server im Verzeichnis

\Windows\System32 das Skript *scregedit.wsf* zur Verfügung. Über dieses Skript können verschiedene Verwaltungsaufgaben durchgeführt werden. Hauptsächlich bearbeiten Sie mit diesem Tool die Registry-Datenbank des Servers:

- Konfiguration der automatischen Updates
- Aktivierung des Remotedesktops
- Aktivierung der Funktion, dass sich Clients mit dem Remotedesktop verbinden können, auf dem nicht Windows Server 2008 oder Windows Vista installiert ist
- Gewichtung und Priorität von DNS-SRV-Records
- Remoteverwaltung des IPSec-Monitors über das Netzwerk

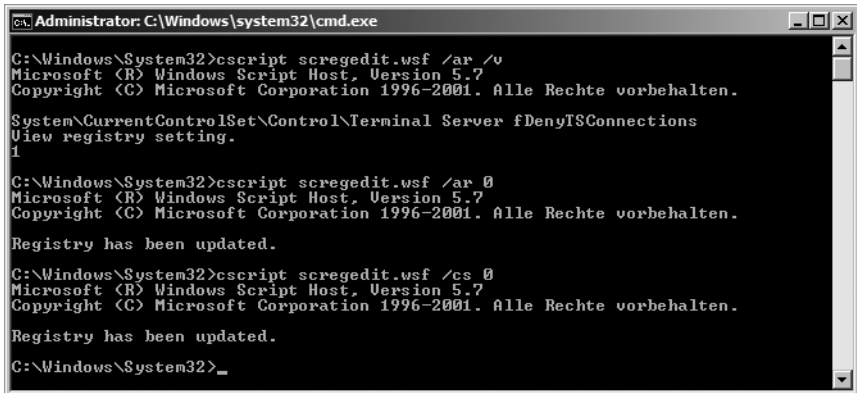
Sie können sich eine ausführliche Hilfe zu den einzelnen Funktionen anzeigen lassen, wenn Sie in das Verzeichnis *\Windows\system32* wechseln und den Befehl *cscript scregedit.wsf /?* eingeben. Geben Sie den Befehl *cscript scregedit.wsf /cli* ein, um sich eine Liste wichtiger Befehlszeilen-Tools anzeigen zu lassen, mit denen Sie, neben *scregedit.wsf*, zusätzlich den Server verwalten können.

Aktivieren des Remotedesktops auf einem Core-Server

Wollen Sie per Remotedesktop auf einen Core-Server zugreifen, müssen Sie zunächst mit *scregedit.wsf* diese Funktion aktivieren. Greift ein Administrator über den Remotedesktop auf einen Core-Server zu, erhält er in seiner Sitzung ebenfalls die Befehlszeile angezeigt. Damit der Remotedesktop funktioniert, müssen Sie diesen mit *scregedit.wsf* aktivieren. Gehen Sie dazu folgendermaßen vor:

1. Geben Sie auf dem Core-Server in der Befehlszeile den Befehl *cscript scregedit.wsf /ar 0* ein, um den Remotedesktop zu aktivieren (Abbildung 3.25).
2. Mit dem Befehl *cscript scregedit.wsf /cs 0* aktivieren Sie die Remotedesktopverbindung für Windows XP- und Windows Server 2003-Clients.
3. Über *cscript scregedit.wsf /ar /v* und *cscript scregedit.wsf /cs /v* können Sie sich den aktuellen Eintrag anzeigen lassen.

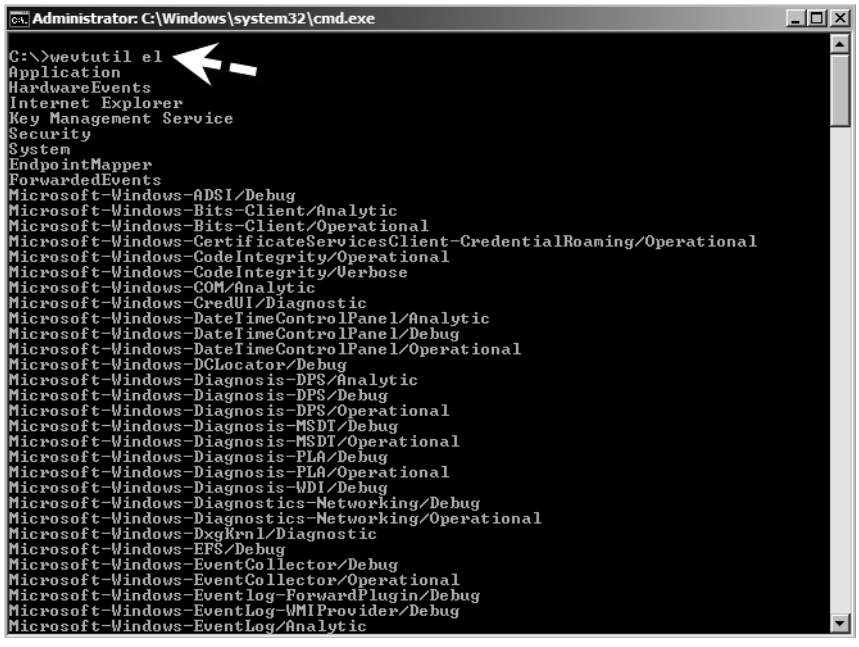
Abbildg. 3.25 Konfigurieren des Remotedesktops auf einem Core-Server



Ereignisanzeige auf einem Core-Server anzeigen

In Kapitel 18 gehen wir ausführlicher auf die neue Ereignisanzeige von Windows Server 2008 ein. Um sich die Ereignisanzeige auf einem Core-Server anzeigen zu lassen, können Sie sich entweder von einem normalen Server aus mit der Ereignisanzeige des Core-Servers verbinden oder Sie lassen sich die Ereignisanzeige in der Befehlszeile des Servers anzeigen. Über den Befehl *wevtutil el* können Sie eine Liste der Ereignisanzeigen aufrufen (Abbildung 3.26).

Abbildg. 3.26 Auflisten der Ereignisanzeigen auf einem Core-Server



Um sich Informationen anzeigen zu lassen, stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Um sich den Inhalt eines Protokolls anzeigen zu lassen, verwenden Sie den Befehl *wevtutil qe /f:text <Protokoll>*. Da normalerweise in einem Protokoll zahlreiche Einträge erstellt werden, können Sie mit der zusätzlichen Option *|more* durch die Anzeige scrollen.
- Mit dem Befehl *wevtutil epl <Protokoll>* können Sie dieses exportieren. Alternativ können Sie mit dem Befehl *wevtutil qe /f:text <Protokoll> >datei.txt* die Anzeige in eine Textdatei umleiten lassen, die Sie dann wieder auf einem anderen Server oder PC betrachten können.
- Mit dem Befehl *wevtutil cl <Protokoll>* löschen Sie den Inhalt eines Protokolls.

Geben Sie in der Befehlszeile *wevtutil.exe /?* ein, erhalten Sie eine ausführliche Hilfe über die verschiedenen Optionen des Tools.

Hardware über die Befehlszeile installieren

Installieren Sie neue Hardware auf einem Windows Server 2008, können Sie die grafische Oberfläche oder die Befehlszeile verwenden. Vor allem auf Core-Servern bleibt Ihnen keine andere Wahl als die Befehlszeile zur verwenden. Haben Sie die neue Hardware mit dem Server verbunden, wird diese durch das Plug & Play automatisch erkannt und der Treiber installiert, das gilt auch auf Core-Servern. Allerdings muss in diesem Fall der Treiber in Windows Server 2008 integriert sein. Ist er das nicht und müssen Sie den Treiber manuell nachinstallieren, gehen Sie folgendermaßen vor:

1. Entpacken Sie die Treiberdateien und kopieren Sie diese in ein Verzeichnis auf dem Server.
2. Geben Sie den Befehl *pnputil –i –a <*.inf-Datei des Treibers>* ein. Mit diesem neuen Tool können Treiber in Windows Server 2008 und Windows Vista hinzugefügt und entfernt werden.
   - Über den Befehl *sc query type= driver* können Sie sich alle installierten Treiber auf einem Server anzeigen lassen (Achten Sie auf das Leerzeichen nach dem Gleichheitszeichen).
   - Mit dem Befehl *sc delete <Treibername>* können Sie den Treiber entfernen, den Sie sich zuvor über den Befehl *sc query type= driver* anzeigen lassen können.

Zusammenfassung

Wie Sie gelesen haben, wurde die Bedienung von Windows Server 2008 im Vergleich zu Windows Server 2003 deutlich verbessert. Mit dem neuen Server-Manager können Server einfacher und effizienter verwaltet werden. Auch die Aktivierung von Windows ist weniger kompliziert, als viele denken. Im nächsten Kapitel zeigen wir Ihnen, welche neue Serverrollen und -features es gibt, und geben kurze Einblicke, welche Nutzen diese haben. In den weiteren Kapiteln dieses Buches gehen wir dann detaillierter auf die Möglichkeiten von Windows Server 2008 ein.

Kapitel 4

Serverrollen und Serverfunktionen

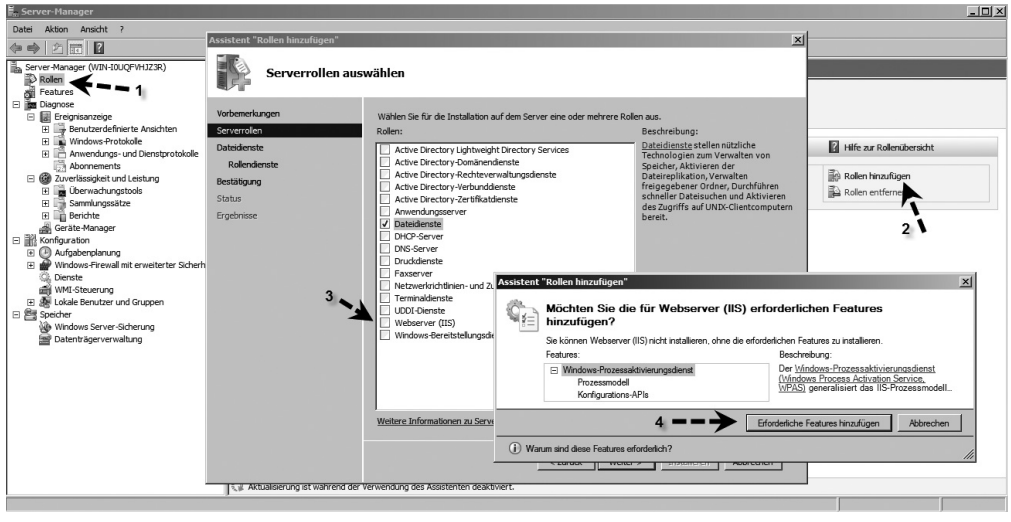
In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, welche verschiedenen Serverrollen und Serverfunktion es gibt. Microsoft hat in Windows Server 2008 den Ansatz von Exchange Server 2007 fortgeführt, bei dem Sie einem Server speziell die Rollen zuweisen können, die diese benötigt. Alle anderen Rollen werden nicht installiert und bieten daher Angreifern keine unnötige Fläche. Serverrollen beschreiben die primäre Funktion eines Servers, zum Beispiel Webserver.

Installieren von Serverrollen auf einem Server

Auf einem Server können auch mehrere Rollen parallel installiert werden. Über den Eintrag *Rollen* und anschließendem Klick auf den Link *Rollen hinzufügen* im Server-Manager startet ein Assistent, über den die einzelnen Rollen ausgewählt und installiert werden können (Abbildung 4.1). Auf den einzelnen Fenstern des Assistenten werden deutlich mehr Informationen angezeigt, als noch bei der Installation von Systemkomponenten von Windows Server 2003.

Abbildg. 4.1 Serverollen werden über einen Assistenten installiert

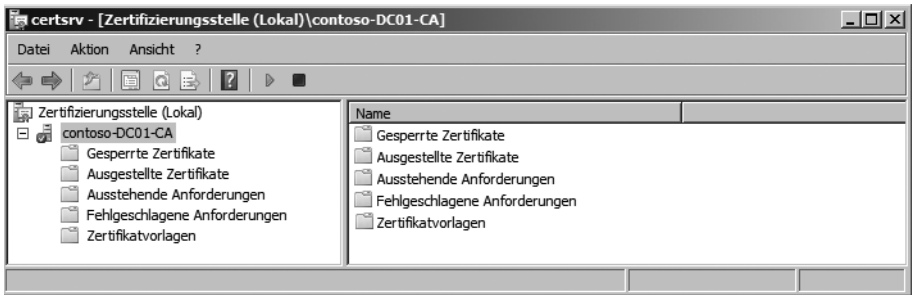


Wird eine Rolle zur Installation ausgewählt, zeigt der Assistent alle abhängigen Rollendienste und Features an, die durch Auswahl dieser Rolle auf dem Server ebenfalls installiert werden. So kann schnell erkannt werden, ob die Installation einer Rolle vielleicht doch nicht gewünscht ist, weil noch andere abhängige Komponenten installiert werden müssen. Der Installations-Assistent kann dann wieder abgebrochen werden. Folgende Rollen stehen für Windows Server 2008 zur Verfügung:

- **Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS)** Diese Rolle ersetzt die Zertifikatdienste unter Windows Server 2003. Sie können mit dieser Rolle eine Public Key Infrastructure (PKI) aufbauen. Die Verwaltung ist noch sehr ähnlich zu den Zertifikatdiensten von Windows Server 2003. Hauptsächlich wurden Verbesserungen im Bereich der automatischen Verteilung von Zertifikaten eingeführt. Außerdem können jetzt auch Netzwerkgeräten wie Router und Firewall Zertifikate zugeteilt werden, ohne dass diese über ein Netzwerkkonto verfü-

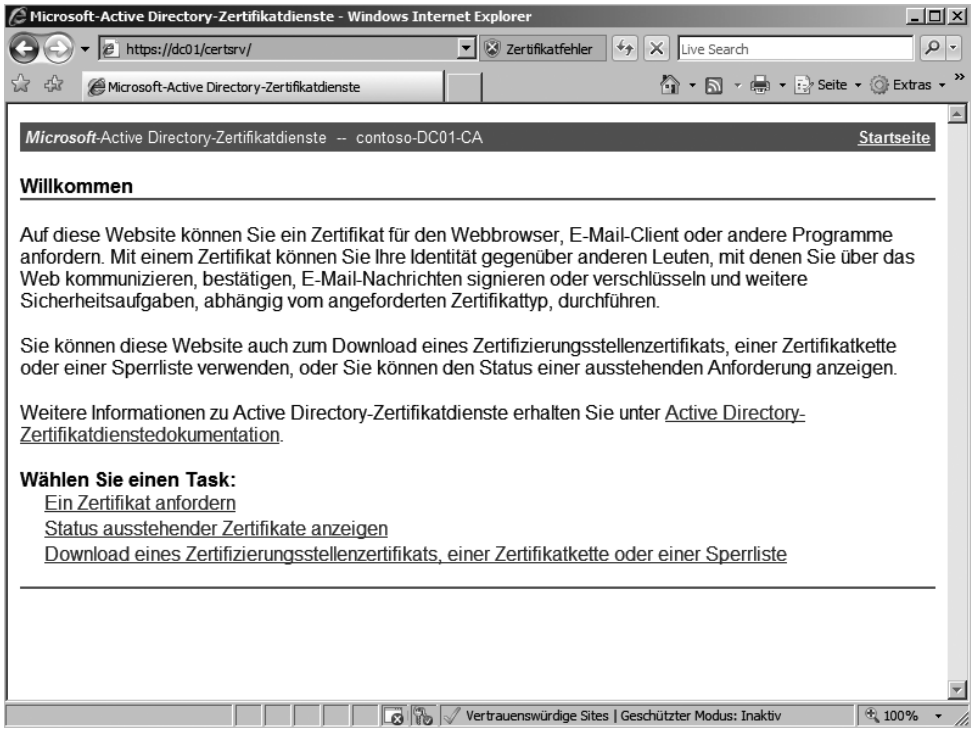
gen müssen. Die Verwaltung dieser Rolle findet über das bekannte Verwaltungsprogramm in der MMC statt. Nach der Installation der Rolle wird diese auch in den Server-Manager integriert.

Abbildg. 4.2 Verwalten der Zertifikatdienste in Windows Server 2008



Auch unter Windows Server 2008 können Sie über einen Browser auf die Zertifizierungsstelle zugreifen. Diese Funktionalität wird allerdings nicht mehr automatisch installiert, sondern muss über den Rollendienst *Zertifizierungsstellen-Webregistrierung* installiert werden. Nach der Installation des Rollendienstes steht auch die Webseite der Zertifizierungsstelle wie bei Windows Server 2003 zur Verfügung. Die Adresse ist die gleiche wie bei Windows Server 2003, *http://<Servername>/certsrv*. Mehr zu diesem Thema erfahren Sie in Kapitel 17.

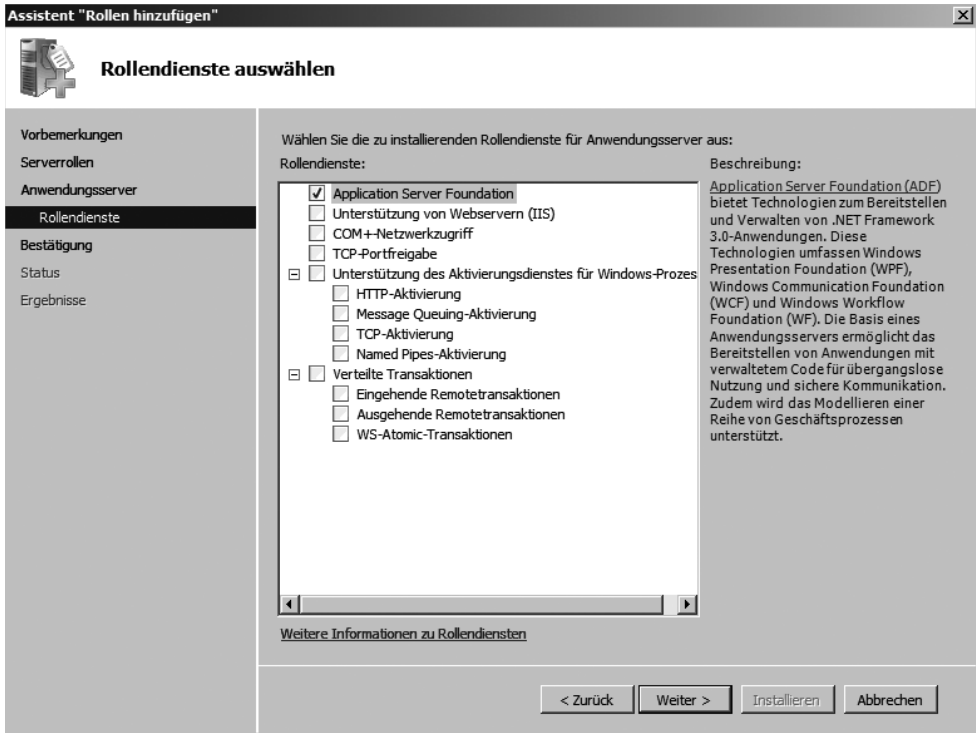
Abbildg. 4.3 Die Webseite der Zertifizierungsdienste von Windows Server 2008



- **Active Directory-Domänendienste (Active Directory Domain Services, AD DS)** Hierbei handelt es sich um die Rolle eines Domänencontrollers für das Active Directory. Bevor Sie einen Server zum Domänencontroller für das Active Directory heraufstufen können, muss diese Rolle installiert sein. Wir haben dieser Rolle ein eigenes Kapitel gewidmet (siehe Kapitel 8).
- **Active Directory-Verbunddienste (Active Directory Federation Services, AD FS)** Mit den AD FS können Sie eine webbasierte Single Sign-On (SSO)-Infrastruktur aufbauen (siehe Kapitel 17). An der Funktionalität von AD FS hat sich im Vergleich zu Windows Server 2003 nichts geändert. Nur die Verwaltungsoberfläche und die Installation der Rolle wurde angepasst. Profitieren sollen hauptsächlich unternehmensinterne Verbände (auch mit mehreren Gesamtstrukturen) sowie B2B Plattformen. Diese Dienste dienen der Vereinfachung von Anmeldeprozeduren bei verteilten Sitzungen auf Umkreisnetzwerke mit Verbindung zum Internet. Der Identitätsverbund ermöglicht es zwei Unternehmen, die in Active Directory gespeicherten Identitätsinformationen eines Benutzers auf sichere Weise über Verbundvertrauensstellungen gemeinsam zu nutzen, wodurch die Zusammenarbeit erheblich vereinfacht werden soll.
- **Active Directory Lightweight Directory Services (AD LDS)** Mit diesen Diensten können Applikationen, welche Informationen in einem Verzeichnis speichern arbeiten. Im Gegensatz zu den Active Directory Domain Services, wird das Verzeichnis nicht als Dienst ausgeführt. Diese Dienste benötigen keinen reinen Domänencontroller. Auf einem Server können mehrere Instanzen laufen. Bei den AD LDS handelt es sich sozusagen um ein »Mini«-Active Directory ohne große Verwaltungsfunktionen. Unter Windows Server 2003 wurden diese Dienste noch Active Directory Application Mode (ADAM) genannt. AD LDS ist eine Low End-Variante von Active Directory. Es basiert auf der gleichen Technologie und unterstützt ebenfalls Replikation. Mit AD LDS können LDAP-Verzeichnisse für Anwendungen erstellt werden, die wiederum mit Active Directory synchronisiert werden können und dieses auch für die Authentifizierung nutzen können. Es können mehrere Instanzen parallel auf einem Server betrieben werden. AD LDS ist eine Alternative zu den Application Directory Partitions in Active Directory. Der Dienst wurde für Organisationen entwickelt, die eine flexible Unterstützung verzeichnisfähiger Anwendungen benötigen. AD LDS ist ein LDAP-Verzeichnisdienst (Lightweight Directory Access Protocol), der als Benutzerdienst und nicht als Systemdienst ausgeführt wird. Mit dem Dienst können Unternehmen zum Beispiel andere LDAP-Verzeichnisse in Testumgebungen installieren, ohne auf Software eines Drittanbieters zurückgreifen zu müssen.
- **Active Directory-Rechteverwaltungsdienste (Active Directory Rights Management Services, AD RMS)** Mit dieser Technologie werden Daten mit digitalen Signaturen versehen, um sie vor unerwünschtem Zugriff zu sichern. Besitzer von Dateien können basierend auf Benutzerinformationen exakt festlegen, was andere Benutzer mit den Dateien machen dürfen. Dokumente können als »Nur Lesen« konfiguriert werden. Die Konfiguration ist allerdings nicht ganz trivial und es werden nur die Microsoft Office-Versionen 2003/2007 sowie Clients mit dem Internet Explorer unterstützt. Installieren Sie diese Rolle, können Sie über den Server-Manager zusätzliche Anleitungen aufrufen. Ausführliche Informationen zur Einrichtung und Verwaltung erhalten Sie auf der Internetseite *http://technet2.microsoft.com/windowsserver2008/en/servermanager/activedirectoryrightsmanagementservices.mspx*.
- **Anwendungsserver (Application Server)** Bei dieser Rolle wird .NET Framework, Unterstützung für Webserver, Messaging Queueing und andere Funktionen installiert. Die Rolle ist für alle Editionen von Windows Server 2008 verfügbar, außer der Windows Webserver 2008-Edition. Sie können der Rolle weitere Dienste und Funktionen hinzufügen. Beim Anwendungsser-

ver werden nur die standardmäßig hinterlegten Rollen installiert (Abbildung 4.4). Wählen Sie die Rolle zur Installation aus, können Sie mit Hilfe des Assistenten diese zusätzlichen Rollen und Funktionen auswählen.

Abbildg. 4.4 Installieren der Rolle eines Anwendungsservers unter Windows Server 2008

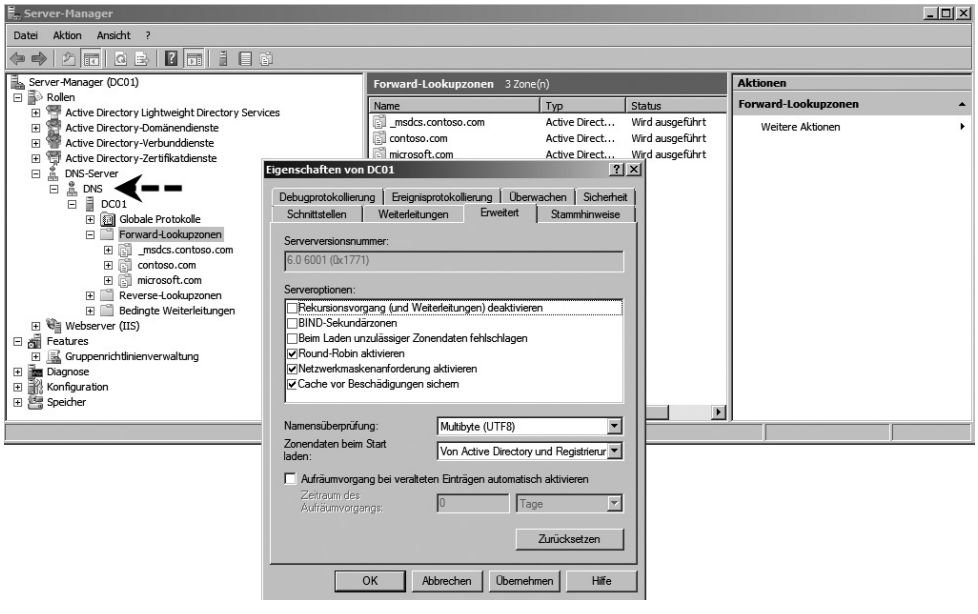


- **DHCP-Server** Diese Rolle beinhaltet die Funktion eines DHCP-Servers. Unter Windows Server 2008 kann der DHCP-Server auch IPv6-Adressen verteilen, ist also vollständig DHCPv6-kompatibel. Bereits bei der Installation dieser Rolle können Sie die wichtigsten Einstellungen für die Rolle vornehmen. Die sonstige Verwaltung der Rolle hat sich aber im Vergleich zu Windows Server 2003 nicht verändert. Im Gegensatz zu Windows Server 2003 können Sie neben den IPv4-Bereichen auch IPv6-Bereiche einrichten, wovon hauptsächlich Clients mit Windows Vista und Windows Server 2008 profitieren. Mehr zu diesem Thema lesen Sie in Kapitel 11.

Abbildg. 4.5 Der DHCP-Server in Windows Server 2008 unterstützt jetzt auch IPv6

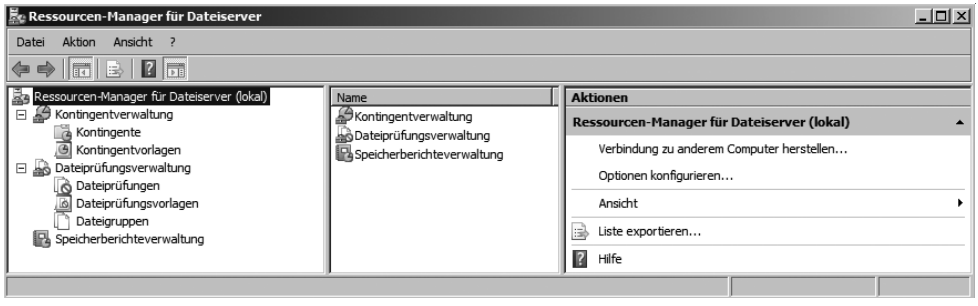
- **DNS-Server** Installieren Sie diese Rolle, erhält der Server die Möglichkeit, DNS-Zonen zu verwalten (siehe die Kapitel 8 und 11). Die Verwaltung und Installation dieser Rolle hat sich nicht grundlegend geändert. Lediglich die Verwaltung der bedingten Weiterleitungen findet jetzt in einem eigenen Menüpunkt statt. Wichtige Neuerungen dieser Rolle sind die Unterstützung für IPv6 und das Laden der Zonen im Hintergrund. Durch dieses Laden im Hintergrund kann ein DNS-Server schneller antworten. Außerdem können Sie IPv6-Reverse-Lookupzonen erstellen.

Abbildg. 4.6 Verwalten eines DNS-Servers unter Windows Server 2008



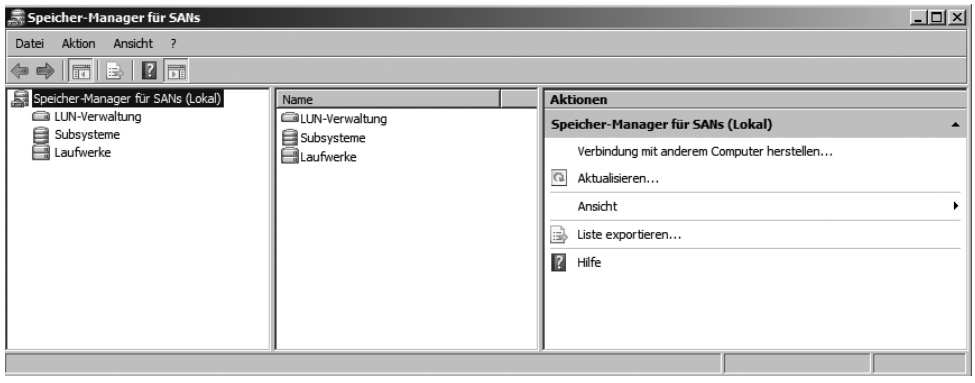
- **Faxserver** Diese Server senden und empfangen Faxe. Auch die Verwaltung von Faxressourcen über das Netzwerk wird durch diese Rolle installiert.
- **Dateidienste (File Services)** Installieren Sie diese Rolle, können Sie den Server als Dateiserver verwenden, um Freigaben zu erstellen. Die Verwaltung eines Dateiservers hat sich im Vergleich zu Windows Server 2003 nicht großartig verändert (siehe hierzu auch die Kapitel 5 und 6). Die Dateidienste beinhalten die gleichen Funktionen wie Windows Server 2003 R2. Neu in diesem Bereich ist die Funktion *Speicher-Manager für SANs*, mit dem Sie Storage Aera Networks (SANs), die über Fibrechannel oder iSCSI angebunden sind, besser verwalten können. Mit dem Speicher-Manager für SANs sollten allerdings nur Administratoren arbeiten, die sich mit dem Thema SAN schon etwas auskennen. Eine weitere Neuerung in Windows Server 2008 im Vergleich zu Windows Server 2003 ist der neue *Ressourcen-Manager für Dateiserver (Fileserver Resource Manager, FSRM)*. Der FSRM ist allerdings Bestandteil von Windows Server 2003 R2 (Abbildung 4.7).

Abbildg. 4.7 Verwalten eines Dateiservers mit dem *Ressourcen-Manager für Dateiserver*



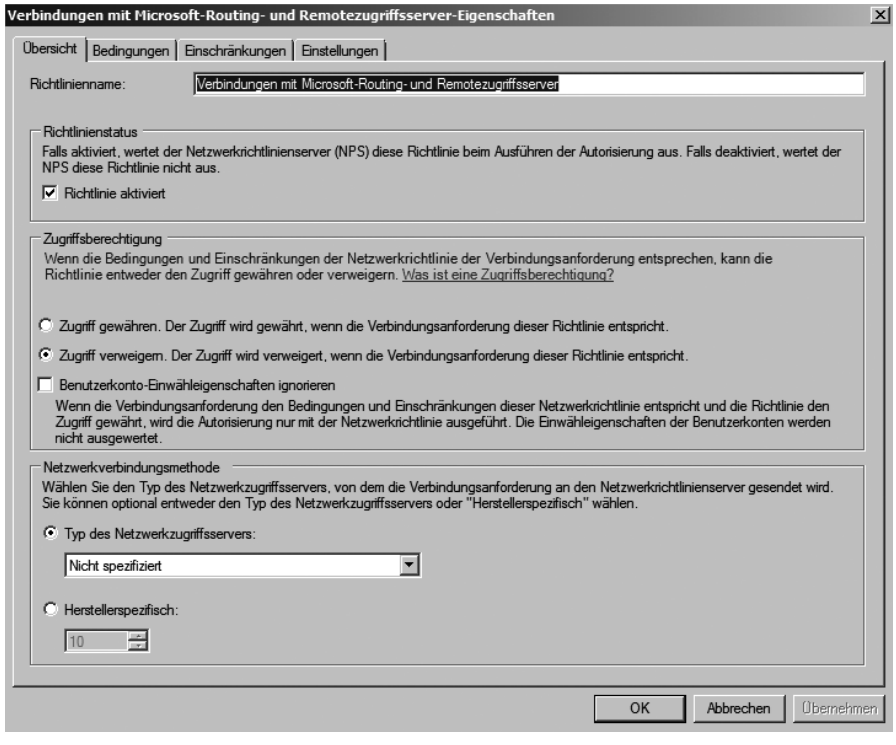
Mit diesem Tool lassen sich an zentraler Stelle alle Dateiserver eines Unternehmens konfigurieren und Datenträgerkontingente (Quotas) steuern. Sie können Anwender daran hindern, unerwünschte Dateien auf den Servern abzulegen, zum Beispiel MP3-Dateien oder Bilder. Mit dem Ressourcen-Manager für Dateiserver können Sie detaillierte Berichte und Vorlagen für Quotas erstellen. Außerdem können Sie sich diese Berichte und auch Alarme der Quotas als E-Mail über den Exchange Server zuschicken lassen. Auch das Network File System (NFS) ist eine Funktion dieser Rolle. Mit dieser Funktion können Sie Daten zwischen Servern unter Windows Server 2008 und Unix-Servern austauschen. Diese Funktion wurde für Windows Server 2008 aktualisiert. Integriert wurde vor allem der Active Directory-Lookup in Zusammenarbeit mit dem Unix Identity Management und die Unterstützung von 64-Bit-Prozessoren. An der Bedienung und dem Funktionsumfang hat sich im Vergleich zu Windows Server 2003 R2 nichts geändert.

Abbildg. 4.8 Verwalten der Anbindung von Windows Server 2008 an SANs mit dem Speicher-Manager für SANs



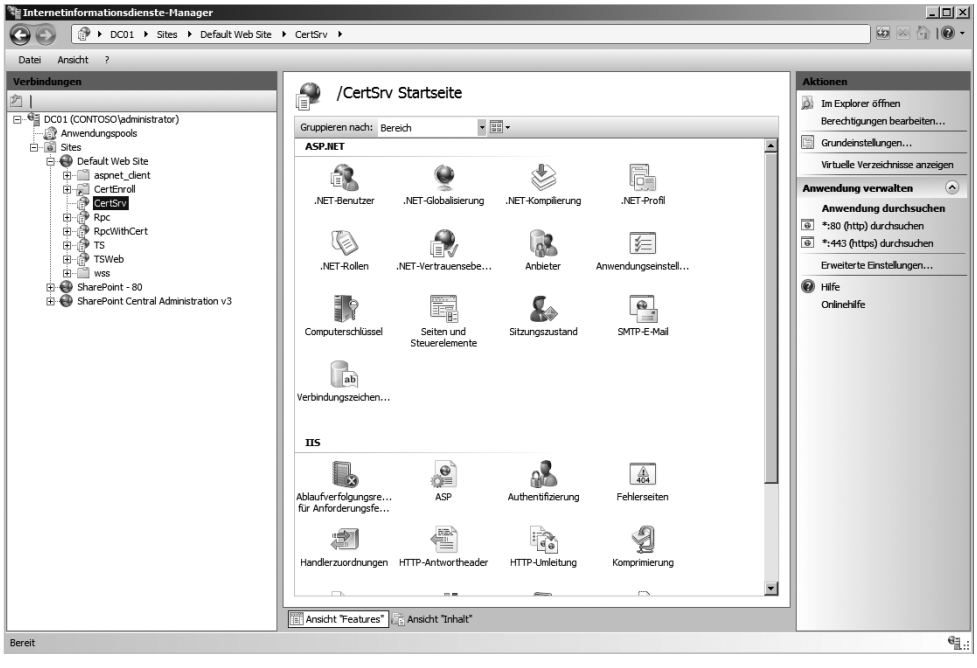
- **Netzwerkrichtlinien- und Zugriffsdienste (Network Policy and Access Services)** Hierbei handelt es sich um die RAS-Funktion von Windows Server 2008. Mit dieser Rolle können Sie Benutzern Zugriff auf verschiedene Netzwerksegmente gewähren (siehe auch Kapitel 15). Mit dieser Rolle können Sie zum Beispiel auch einen VPN-Server oder einen RADIUS-Server zur Verwendung des Connection Manager Administration Kit konfigurieren. Auch wenn Sie einen Server als Router zwischen verschiedenen Netzwerken einsetzen, verwenden Sie diese Rolle. Über diese Rolle können Sie die neuen Network Access Protection (NAP)-Richtlinien erstellen und verwalten.

Abbildg. 4.9 Verwalten von Netzwerkrichtlinien in Windows Server 2008



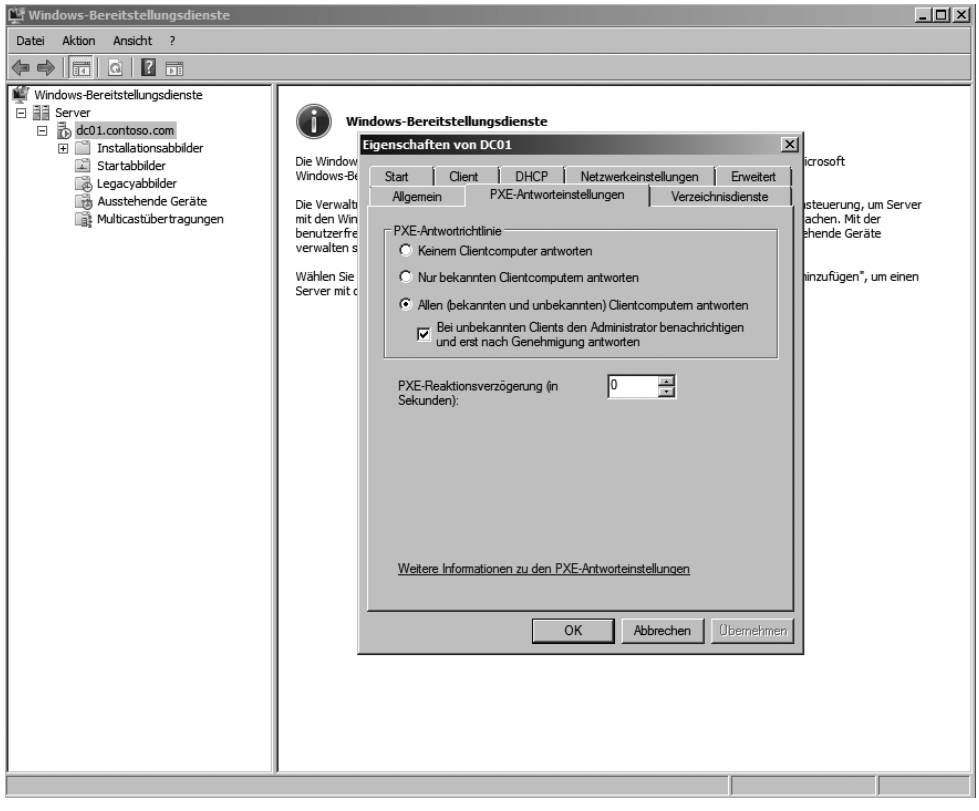
- **Druckdienste (Print Services)** Mit dieser Rolle ermöglichen Sie die Verwaltung von mehreren lokal angeschlossenen Druckern an einem Server (Druckserver). Die Drucker können an diesen Server auch per LAN angeschlossen werden.
- **Terminaldienste** Bei dieser Funktion werden die Terminaldienste im Anwendungsmodus installiert. Für die Verwaltung eines Servers wird der Remotedesktop benutzt. Hierzu brauchen Sie die Terminaldienste nicht. Mehr zu den Terminaldiensten erfahren Sie in Kapitel 12.
- **UDDI-Dienste (Universal Description, Discovery, Integration)** UDDI ist eine Industriespezifikation für das Veröffentlichen und Suchen von Informationen zu Webdiensten. Bei den UDDI-Diensten handelt es sich um eine optionale Komponente von Windows Server 2008. Die UDDI-Dienste bieten einen standardbasierten XML-Webdienst, der Entwicklern in Organisationen das effiziente Veröffentlichen, Erkennen, Freigeben und Wiederverwenden von Webdiensten direkt aus ihren Entwicklungstools und Geschäftsanwendungen ermöglicht. Aufbauend auf Microsoft .NET Framework bieten die UDDI-Dienste eine skalierbare Lösung, die mit Technologien und Tools der Organisation integriert werden kann. IT-Manager können die systemeigene Unterstützung von Standardkategorisierungsschemas, Microsoft SQL Server und der Active Directory-Authentifizierung nutzen. Die UDDI-Dienste sind mit der UDDI-API, Version 1.0 und 2.0, kompatibel und enthalten eine Weboberfläche, die in alle von der Windows Server 2008-Produktfamilie unterstützten Sprachen übersetzt ist. Mit diesen Funktionen können Sie Informationen über ein Unternehmensintranet oder in einem Extranet bereitstellen und aufteilen. Bestehende Funktionen in einem Intranet stehen so auch anderen Bereichen des Unternehmens zur Verfügung und müssen nicht aufgeteilt werden.

Abbildg. 4.10 Verwalten eines Webservers unter Windows Server 2008 mit dem Internetinformationsdienste-Manager



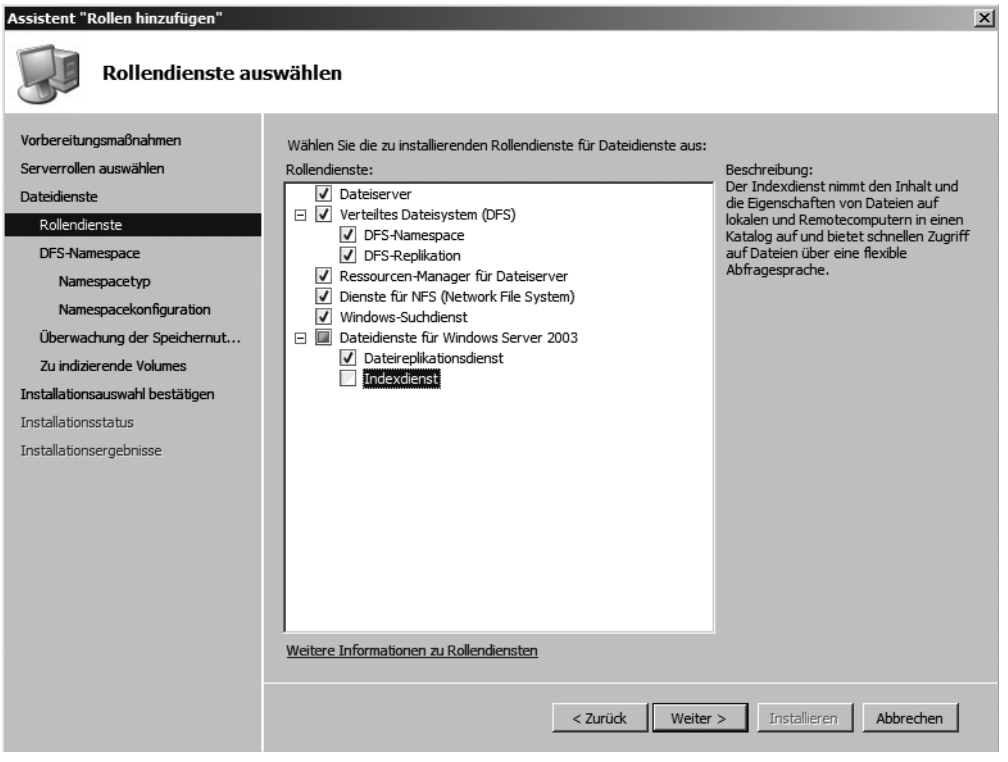
- **Webserver (IIS)** Installieren Sie diese Rolle, werden die Internetinformationsdienste (Internet Information Services, IIS) auf dem Server aktiviert (siehe auch die Kapitel 1 und 13). Mit Windows Server 2008 wird die neue Version 7.0 von IIS installiert. Die Verwaltung dieser Rolle hat sich im Vergleich zu Windows Server 2003 etwas geändert, es gibt aber noch immer den Internetinformationsdienste-Manager, über den die Verwaltung stattfindet. Lediglich die einzelnen Aufgaben für die Verwaltung sind an eine andere Stelle gewandert.
- **Windows-Bereitstellungsdienste (Windows Deployment Services, WDS)** Bei den WDS handelt es sich um den Nachfolger der Remote Installation Services (RIS) von Windows Server 2003. Mit WDS können Sie WIM-basierte Images von Windows Vista verteilen (siehe Kapitel 16). Der RIS-Server unterstützt kein Windows Vista. Aktualisieren Sie einen Windows Server 2003 auf das SP2, wird der RIS ebenfalls durch die WDS ersetzt.

Abbildg. 4.11 Verwalten der Windows-Bereitstellungsdienste in Windows Server 2008



Nachdem Sie die Rollen ausgewählt haben, die Sie auf dem Server installieren wollen, können Sie mit dem Assistent zur Konfiguration dieser Rollen die einzelnen Dienste und Funktionen für diese Rolle hinzufügen und konfigurieren (Abbildung 4.12).

Abbildg. 4.12 Auswählen der zu installierenden Rollendienste auf dem Server



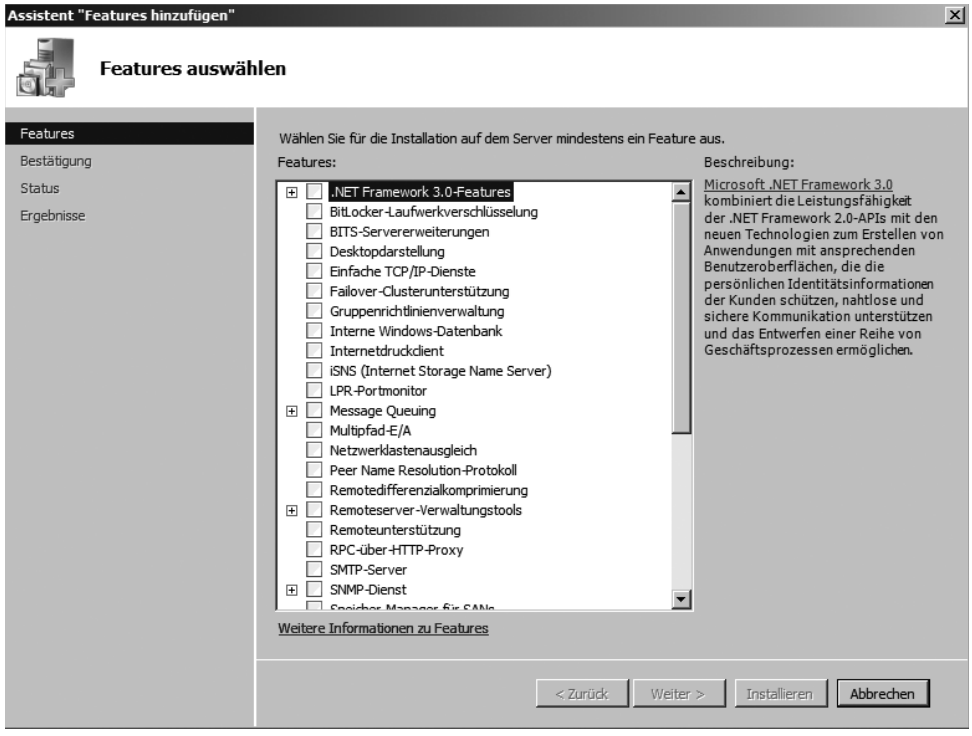
Manche Rollen haben nur ein Konfigurationsfenster, andere Rollen, wie zum Beispiel die Dateidienste müssen ausführlicher konfiguriert werden. Sie können mit Hilfe des Assistenten zur Installation der Rolle weitere Rollendienste und -features hinzufügen. Wählen Sie Rollendienste aus, die von anderen abhängig sind, werden diese ebenfalls automatisch zur Installation vorgeschlagen

Features installieren und verwalten

Serverrollen bestimmen den primären Verwendungszweck eines Servers. Mit den Features im Server-Manager werden untergeordnete Funktionen zu Rollen hinzugefügt. Features erweitern installierte Serverrollen um zusätzliche Möglichkeiten. Auch die Features werden über den Server-Manager installiert. Die Installation von zusätzlichen Features wird im Server-Manager über *Features/Features hinzufügen* durchgeführt. Die Installation von Funktionen läuft analog zur Installation von Serverrollen ab. Ihnen stehen über 30 verschiedene Serverfunktionen zur Verfügung (Abbildung 4.13).

- **.NET Framework 3.0-Features** Diese Funktion erweitert den Server um die neuen Funktionen von .NET Framework 3.0. Unter Windows Server 2003 auch mit R2 wird noch .NET Framework 2.0 installiert. Windows Server 2008 wird mit .NET Framework 3.0 ausgeliefert.

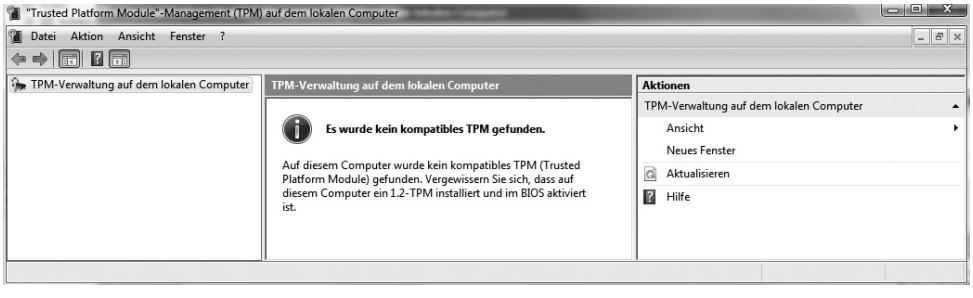
Abbildg. 4.13 Installation von zusätzlichen Features



- **BitLocker-Laufwerksverschlüsselung** BitLocker wurde bereits mit Windows Vista eingeführt und stellt sicher, dass die komplette Partition der Festplatte verschlüsselt wird. BitLocker bietet im Gegensatz zum verschlüsselnden Dateisystem (Encrypting File System, EFS) auch Schutz vor Diebstahl oder dem Ausbau des Datenträgers. BitLocker schützt komplette Partitionen, auch temporäre Dateien und die Auslagerungsdatei, welche ebenfalls vertrauliche Informationen enthalten können. Im Idealfall nutzt das Feature TPM 1.2 (Trusted Platform Module), um die Daten des Benutzer zu schützen. TPM ist ein Mikrochip, der die Nutzung erweiterter Sicherheitsfeatures auf dem Computer ermöglicht. TPM ist in einigen neueren Computern integriert. Ein Computer mit TPM kann Verschlüsselungsschlüssel erstellen, die nur mit TPM entschlüsselt werden können. Der Bootloader von Windows Server 2008 ist in der Lage, die Register des TPM-Chips in jedem Schritt des Bootprozesses richtig zu setzen, so dass der TPM den Volume Encryption Key herausgibt, der für die Entschlüsselung der Festplatte benötigt wird. Deshalb ersetzt Windows Server 2008 bei der Installation auch einen eventuell vorhandenen Master Boot Record (MBR) mit seinem eigenen. Zwar wäre auch der Einsatz eines anderen, TPM-fähigen, Bootloaders theoretisch denkbar. Dies ist aber selten praktikabel. Wenn Sie nicht wissen, ob Ihr PC einen TPM-Chip verbaut hat, können Sie die TPM-Verwaltungskonsole über *Start/Ausführen/tpm.msc* starten. Hier erhalten Sie eine entsprechende Meldung. TPM schützt Verschlüsselungsschlüssel durch einen eigenen Speicherstammschlüssel. Das Speichern des Speicherstammschlüssels im TPM-Chip anstatt auf der Festplatte bietet einen höheren Schutz vor Angriffen, die auf die Verschlüsselungsschlüssel ausgerichtet sind. Wenn Sie einen Computer starten, der über TPM verfügt, überprüft TPM das Betriebssystem auf Bedingungen, die ein Sicherheitsrisiko dar-

stellen können. Zu diesen Bedingungen können Datenträgerfehler, Änderungen am BIOS oder sonstigen Startkomponenten oder ein Hinweis, dass die Festplatte aus einem Computer entfernt und in einem anderen Computer gestartet wurde, gehören. Erkennt TPM eines dieser Sicherheitsrisiken, sperrt BitLocker die Systempartition so lange, bis Sie ein BitLocker-Wiederherstellungskennwort zum Aufheben der Sperrung eingeben. BitLocker verbessert den Datenschutz, indem es zwei wichtige Aufgaben zusammenführt: Die vollständig Verschlüsselung von Laufwerken und die Integritätsüberprüfung von Komponenten beim Systemstart. BitLocker kann auch auf Computern ohne ein kompatibles TPM verwendet werden. In diesem Fall können Sie mit BitLocker zwar die Funktionen zur Volumeverschlüsselung verwenden, Sie erhalten jedoch nicht die zusätzliche Sicherheit durch die frühe Integritätsüberprüfung der Startdatei. Stattdessen wird die Identität des Benutzers beim Starten mithilfe eines USB-Sticks überprüft. Die Laufwerksverschlüsselung schützt die Daten, indem sie verhindert, dass nicht autorisierte Benutzer diese Daten lesen. Sie erreicht dies, indem Sie den gesamten Windows-Datenträger verschlüsselt – inklusive der Auslagerungsdatei und der Datei für den Ruhezustand. Die Integritätsprüfung beim Systemstart führt dazu, dass eine Datenentschlüsselung nur dann stattfindet, wenn die entsprechenden Komponenten unverändert und nicht kompromittiert sind und sich das verschlüsselte Laufwerk im entsprechenden Computer befindet. BitLocker ist eng in Windows Server 2008 integriert und stellt so eine nahtlose, sichere und einfach zu verwaltende Lösung für den Schutz von Daten in Unternehmen dar. BitLocker nutzt beispielsweise vorhandene Active Directory-Domänendienste, um Wiederherstellungsschlüssel zu hinterlegen. Außerdem steht eine Wiederherstellungskonsole zur Verfügung, die in die Bootkomponenten integriert ist. BitLocker nutzt AES mit einer konfigurierbaren Länge von 128 oder 256 Bit. Die Konfiguration kann über Gruppenrichtlinien durchgeführt werden. Der erweiterte Verschlüsselungsstandard (Advanced Encryption Standard, AES) ist eine Form der Verschlüsselung. AES bietet eine sicherere Verschlüsselung als der zuvor verwendete Datenverschlüsselungsstandard (Data Encryption Standard, DES). Mehr zum Thema BitLocker erfahren Sie in Kapitel 14.

Abbildg. 4.14 Verwalten des TPM-Chips unter Windows Server 2008



- **BITS-Servererweiterungen** BITS steht für Background Intelligent Transfer Service. Bei dieser Technologie kann ein Server im Hintergrund Daten empfangen, ohne die Bandbreite im Vordergrund zu beeinträchtigen. Ein Server kann dadurch – zum Beispiel bei installiertem WSUS – Patches aus dem Internet herunterladen. Dazu wird nur soviel Bandbreite verwendet, wie derzeit bei dem Server ungenutzt ist. Andere Netzwerkanwendungen können so auf einem Server weiterhin auf die volle Netzwerkperformance zugreifen.
- **Desktopdarstellung** Installieren Sie diese Funktion, werden die grafischen Funktionen von Windows Vista, sowie der Media Player, Desktop Themes und die Fotogalerie auf dem Server

installiert. Durch die Installation dieser Funktion werden die grafischen Erweiterungen von Windows Vista nicht aktiviert. Diese müssen unter Windows Server 2008 nach der Installation manuell aktiviert werden. Hauptsächlich benötigen Sie diese Funktion auf Terminalservern. Die Anwender erhalten dadurch in den Sitzungen die gleiche Oberfläche wie unter Windows Vista (siehe auch Kapitel 12).

- **Einfache TCP/IP-Dienste** Installieren Sie diese Funktionen, werden auf dem Server noch einige zusätzliche Dienste für TCP/IP aktiviert. Sie sollten diese Dienste nur dann installieren, wenn diese von einer speziellen Applikation benötigt werden. Folgende Funktionen sind in den einfachen TCP/IP-Diensten enthalten: *Zeichengenerator (CHARGEN)*. Dieser sendet Daten, die sich aus einer Folge von 95 druckbaren ASCII-Zeichen zusammensetzen. Dieses Protokoll wird als Debuggingtool zum Testen oder zur Problembehandlung bei Zeilendruckern verwendet. *Daytime* zeigt Meldungen mit Wochentag, Monat, Tag, Jahr, aktueller Uhrzeit (im Format HH:MM:SS) und Informationen zur Zeitzone an. Einige Programme können die Ausgabe dieses Dienstes zum Debuggen oder Überwachen von Abweichungen der Systemuhr oder auf einem anderen Host verwenden. *Discard* verwirft alle über diesen Anschluss empfangenen Meldungen, ohne dass eine Antwort oder Bestätigung gesendet wird. Die Funktion kann als Nullanschluss für den Empfang und die Weiterleitung von TCP/IP-Testnachrichten während der Netzwerkinstallation und -konfiguration verwendet werden. *Echo* erzeugt Echorückmeldungen zu allen über diesen Serveranschluss empfangenen Nachrichten. Echo kann als Debugging- und Überwachungstool in Netzwerken eingesetzt werden. Das *Zitat des Tages (QUOTE)* gibt ein Zitat in Form eines ein- oder mehrzeiligen Textes in einer Meldung zurück. Die Zitate werden nach dem Zufallsprinzip aus der folgenden Datei ausgewählt: *C:\Windows\System32\Drivers\Etc\Quotes*. Eine Beispieldatei mit Zitaten wird mit den einfachen TCP/IP-Diensten installiert. Wenn diese Datei fehlt, kann der Zitatdienst nicht ausgeführt werden.
- **Failover-Clusterunterstützung** Mit dieser Funktion installieren Sie die neue Cluster-Funktionalität von Windows Server 2008 (siehe auch die Kapitel 1 und 19). Auch die Erstellung eines Clusters wird mit Windows Server 2008 extrem vereinfacht. Microsoft hat dazu die grafische Oberfläche zur Clusterverwaltung überarbeitet und optimiert.
- **Gruppenrichtlinienverwaltung** Mit dieser Funktion installieren Sie die Gruppenrichtlinienverwaltungskonsole (Group Policy Management Console, GPMC) mit der Sie die Gruppenrichtlinien im Active Directory verwalten können. Die Bedienung ist noch identisch mit der GPMC unter Windows Server 2003, allerdings müssen Sie diese jetzt nicht mehr separat herunterladen (siehe Kapitel 9).
- **Interne Windows-Datenbank** Auch diese Funktion ist neu in Windows Server 2008. Hierbei handelt es sich um eine kostenlose relationale Datenbank, die zum Beispiel für die SharePoint Services 3.0 verwendet wird. Die Datenbank kann allerdings nicht von Drittthersteller-Produkten verwendet werden, sondern nur von den Funktionen und Rollen in Windows Server 2008, also neben den SharePoint Services 3.0 noch WSUS, UDDI, der Windows Systemressourcen-Manager und die Rechteverwaltung.
- **Internetdruckclient** Mit dieser Funktion können Sie über das HTTP-Protokoll auf die Drucker des Servers zugreifen. Dadurch können Anwender über das Internet auf die Drucker zugreifen. Diese Funktion ist zum Beispiel für mobile Mitarbeiter sinnvoll, die Dokumente von unterwegs in der Firma ausdrucken wollen, zum Beispiel Ausdrucke für Aufträge oder ähnliches.
- **iSNS (Internet Storage Name Server)** Diese Funktion benötigen Unternehmen, die mit iSCSI-Geräten als Speichergerät arbeiten. Ein großer Nachteil von NAS-Systemen ist die Problematik, dass die Anbindung über das LAN erfolgt. Manche Anwendungen haben Probleme damit, wenn

der Datenspeicher im Netzwerk bereitgestellt und mittels IP auf die Daten zugegriffen wird, anstatt den blockbasierten Weg über SCSI oder Fibrechannel zu gehen. Zu diesem Zweck gibt es die iSCSI-Technologie. iSCSI ermöglicht den Zugriff auf NAS-Systeme mit dem bei lokalen Datenträgern üblichen Weg als normales lokales Laufwerk. Die Nachteile der IP-Kommunikation werden kompensiert. iSCSI verpackt dazu die SCSI-Daten in TCP/IP-Pakete. Mit iSNS können auf iSCSI-basierte SAN-Systeme an Windows Server 2008 angebunden werden. Mit dem iSNS-Protokoll werden die verschiedenen Konfigurationen der iSCSI-Geräte und der Geräte von Speichernetzen (SAN) in einem IP-Speichernetz zentralisiert. Das Konzept kennt den Name Service, mit dem alle Geräte registriert werden, die Bereitstellung von Domain-Namen für das Internet Fibre Channel Protocol (iFCP) und die Discovery Domain (DD), die die Geräte in Gruppen unterteilt.

- **LPR-Portmonitor** Windows-Betriebssysteme unterscheiden zwischen lokalen und Netzwerkdruckern. Für andere Druckprotokolle, also auch für das LPR-Druckprotokoll, werden die Verbindungen zu Druckern über so genannte Ports (Anschlüsse) abgewickelt. Sie ergänzen die standardmäßig vorhandenen lokalen Ports. Die Druckerports für das LPR-Protokoll werden LPR-Ports genannt. Jeder LPR-Port verweist auf eine Queue eines Remote Print-Servers. LPR-Ports werden also unter Windows-Betriebssystemen wie lokale Anschlüsse behandelt. Deshalb werden auch Drucker, die über das LPR-Protokoll angesprochen werden, als lokale Drucker angesehen.
- **Message Queuing** Mit dieser Funktion können Nachrichten gesichert und überwacht zwischen Applikationen auf dem Server ausgetauscht werden. Nachrichten können priorisiert werden und es gibt eine Vielzahl an Möglichkeiten, um die Konfiguration anzupassen. Message Queuing (auch als *MSMQ* bezeichnet) ist sowohl eine Kommunikationsinfrastruktur als auch ein Entwicklungswerkzeug. Für Systemadministratoren als auch für Softwareentwickler bietet Message Queuing interessante Möglichkeiten (Installation und Verwaltung der Infrastruktur, Entwicklung von Nachrichtenanwendungen).
- **Multipfad-E/A** Durch Multipfad wird die Verfügbarkeit erhöht, weil mehrere Pfade (Pfad-Failover) von einem Server oder Cluster zu einem Speichersubsystem zugelassen werden. Unterstützt ein Server im SAN *Microsoft Multipfad-E/A (Multipath I/O, MPIO)*, können Sie mehr als einen Pfad zum Lesen und Schreiben für eine LUN (Logical Unit Number, logische Gerätenummer) aktivieren, indem Sie auf diesem Server mehrere Fibre Channel-Ports oder iSCSI-Adapter derselben LUN zuweisen. Dies gilt auch für das Zugreifen auf die LUN von einem Cluster. Stellen Sie zum Vermeiden von Datenverlust vor dem Aktivieren von Zugriff über mehrere Pfade sicher, dass der Server oder Cluster Multipfad-E/A unterstützt.
- **Netzwerklastenausgleich** Mit dieser Funktion können Sie einen Lastenausgleich zwischen mehreren Servern im Netzwerk bereitstellen (siehe hierzu auch Kapitel 8). Zu den Anwendungen, die vom Netzwerklastenausgleich profitieren können, zählen IIS, ISA-Server sowie virtuelle private Netzwerke, Windows Media-Dienste, Mobile Information Server- und Terminaldienste. Mithilfe des Netzwerklastenausgleichs können Sie außerdem die Serverleistung skalieren, sodass der Server mit den steigenden Anforderungen der Internetclients Schritt halten kann. Ausgefallene oder offline geschaltete Computer werden automatisch erkannt und wiederhergestellt. Die Netzwerklast wird nach dem Hinzufügen oder Entfernen von Hosts automatisch umverteilt (siehe auch Kapitel 19).
- **Peer Name Resolution-Protokoll** PNRP ermöglicht die verteilte Auflösung eines Namens in eine IPv6-Adresse und Portnummer. Windows Vista wird ebenfalls mit PNRP Version 2 ausgeliefert. Simpel betrachtet ist PNRP eine P2P-Anwendung, die die Form eines Windows-Dienstes annimmt. PNRP baut auf IPv6 auf.

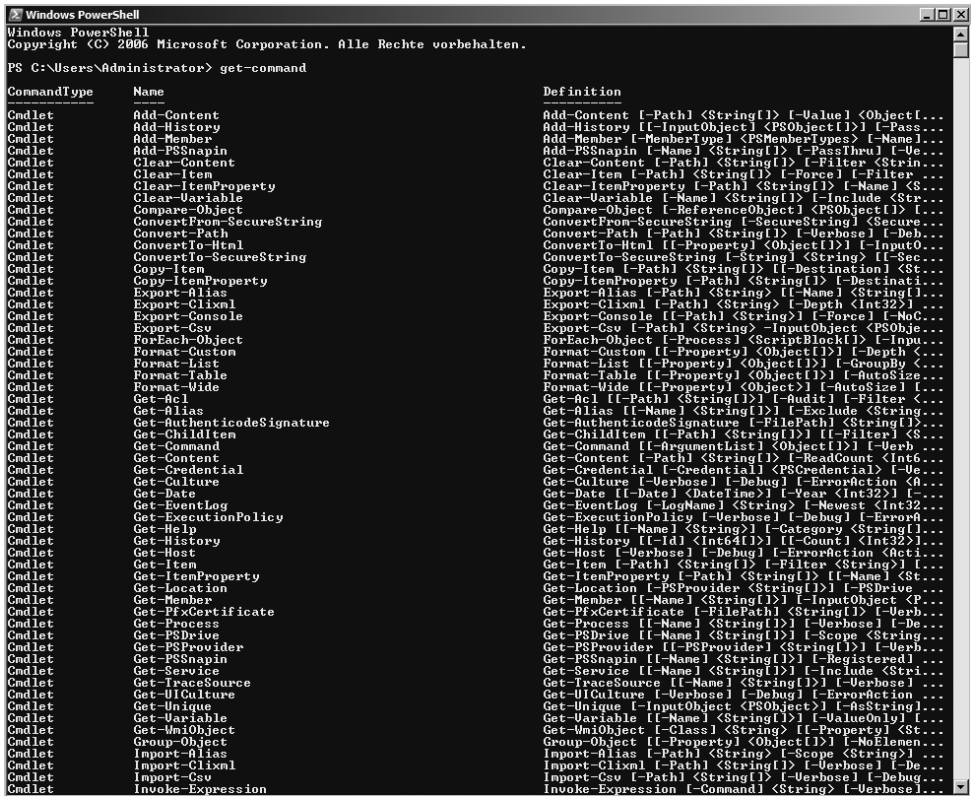
- **Remotedifferentialkomprimierung** Dieses Feature ermöglicht die verbesserte Übertragung von geänderten Daten in schmalbandigen Netzwerken. Ist zum Beispiel ein Server über ein langsames WAN angebunden, erkennt dieses Feature, wenn Änderungen an Dateien vorgenommen wurden, und kopiert nur die geänderten Daten über das Netzwerk, nicht die komplette Datei. Diese Funktion wird zum Beispiel von DFS verwendet (siehe auch Kapitel 6).
- **Remoteserver-Verwaltungstools** Diese Funktion wird auf normal installierten Servern automatisch installiert. Sie können mit diesen Tools die Funktionen von Windows Server 2003 und Windows Server 2008 über das Netzwerk auf einem Windows Server 2008 verwalten.
- **Remoteunterstützung** Installieren Sie diese Funktion, können Sie an Kollegen eine Remoteunterstützungsanforderung schicken, damit sich diese per RDP mit dem Server verbinden können. Diese Funktion wird normalerweise eher für Arbeitsstationen verwendet, als auf Servern. Es spielt keine Rolle, ob die Verbindung mit dem entfernen Rechner über das Netzwerk, Internet oder via Modem per Telefonleitung erfolgt.
- **RPC-über-HTTP-Proxy** Diese Funktion ist ebenfalls unter Windows Server 2003 vorhanden. Mit RPC über HTTP werden RPC-Anfragen in HTTP-Pakete gekapselt. Durch diese Funktion können Anwender zum Beispiel über das Internet mit Outlook auf den Exchange-Server im Unternehmen zugreifen. Unter Exchange Server 2007 wird diese Funktion *Outlook Anywhere* genannt. Die Terminaldienstegateway-Rolle baute ebenfalls auf diese Funktion auf.
- **SMTP-Server** Über diese Funktion installieren Sie einen Mailserver auf dem Server. Unter Exchange Server 2003 haben Sie noch den Windows-internen SMTP-Dienst benötigt. Exchange Server 2007 verwendet seinen eigenen SMTP-Dienst. Manche Mail-Relay-Anwendungen bauen noch auf den lokalen SMTP-Dienst von Windows Server 2008 auf.
- **SNMP-Dienst** Das Simple Network Management Protocol (SNMP) ist ein Standard, mit dem SNMP-fähige Applikationen, hauptsächlich Überwachungsprogramme für Server, Informationen von einem Server abfragen können. Hierbei handelt es sich um einen optionalen Dienst, der im Anschluss an eine erfolgreiche Konfiguration des TCP/IP-Protokolls installiert werden kann. Der SNMP-Dienst stellt einen SNMP-Agenten bereit, der eine zentrale Remoteverwaltung von Computern ermöglicht. Wenn Sie auf die vom SNMP-Agent-Dienst bereitgestellten Informationen zugreifen möchten, benötigen Sie eine Softwareanwendung des SNMP-Verwaltungssystems. Der SNMP-Dienst unterstützt zwar SNMP-Verwaltungssoftware, diese ist jedoch derzeit noch nicht im Lieferumfang enthalten.
- **Speicher-Manager für SANs** Der Speicher-Manager für SANs eröffnet IT-Administratoren grundlegende SAN-Funktionalität. Mit dem Speicher-Manager für SANs lassen sich die folgenden Aufgaben durchführen:
  - Erkennung von Storage-Geräten
  - Speicherplatzbereitstellung, einschließlich der Erstellung, Erweiterung und Entfernung von LUNs
  - Allokierung von SAN-Speicherplatzressourcen für Server
  - Microsoft Multipath I/O (MPIO)-Verwaltung
- **Subsystem für UNIX-basierte Anwendungen** Subsystem für UNIX-basierte Anwendungen (SUA) ist die Weiterentwicklung des Interix-Subsystems, das früher mit Windows Services für UNIX 3.5 ausgeliefert wurde. SUA ist eine UNIX-Umgebung für mehrere Benutzer, die auf Computern unter Windows ausgeführt wird. Subsystem für UNIX-basierte Anwendungen und die dazugehörigen Dienstprogramme stellen Ihnen eine Umgebung zur Verfügung, die jedem anderen UNIX-System gleicht. Enthalten sind die Berücksichtigung von Groß-/Kleinschreibung

bei Dateinamen, die Auftragssteuerung, Kompilierungstools und die Verwendung von mehr als 300 UNIX-Befehlen und -Dienstprogrammen sowie Shellskripts. Da Subsystem für UNIX-basierte Anwendungen auf einer Schicht über dem Windows-Kernel angesiedelt ist, bietet es echte UNIX-Funktionen ohne Emulation. Ein Computer, auf dem SUA ausgeführt wird, bietet zwei verschiedene Befehlszeilenumgebungen: die UNIX-Umgebung und die Windows-Umgebung. Anwendungen werden auf bestimmten Subsystemen und in spezifischen Umgebungen ausgeführt. Wird Subsystem für UNIX-basierte Anwendungen geladen, verwenden Sie eine UNIX-Umgebung. Werden Anwendungen im Windows-Subsystem ausgeführt, verwenden Sie eine Windows-Umgebung.

- **Telnet-Client** Mit dem Telnet-Client können Sie sich per Telnet auf einen anderen Server verbinden. Standardmäßig ist dieser Client unter Windows Server 2008 nicht mehr installiert.
- **Telnet-Server** Bei dieser Funktion handelt es sich um das Gegenstück des Telnet-Clients. Aktivieren Sie diese Funktion, können Sie den lokalen Server per Telnet verwalten.
- **T-(Trivial) FTP-Client** Bei dieser Funktion handelt es sich um einen eingeschränkten FTP-Client, der hauptsächlich für die Updates von Firmware oder das Übertragen von Informationen zu Systemen gedacht ist, auf denen ein TFTP-Server läuft.
- **Verbessertes Windows-Audio-/Video-Streaming** Diese Funktion ist für die Verteilung von Audio- oder Videostreams in Netzwerken gedacht. Mit dieser Funktion können Streams auch überwacht und konfiguriert werden.
- **Verbindungs-Manager-Verwaltungskit** Mit dieser Funktion können Sie Dienstprofile für den Verbindungs-Manager erstellen. Der Verbindungs-Manager unterstützt lokale Verbindungen und Remoteverbindungen mit dem Dienst über ein Netzwerk von Zugriffspunkten, die weltweit zur Verfügung stehen. Falls der Dienst sichere Verbindungen über das Internet erfordert, können Sie mit dem Verbindungs-Manager VPN-Verbindungen einrichten. Wenn Sie eine VPN-Datei einbinden und VPN-Einträge konfigurieren, können die Benutzer auswählen, welchen VPN-Server sie zum Herstellen einer Verbindung verwenden möchten. Protokolldateien für eine Verbindung können erstellt, gelöscht und vom Benutzer angezeigt werden. Die Benutzer können die Eigenschaften einer Verbindung definieren, diese Einstellungen für die spätere Verwendung speichern und den gewünschten Favoriten über die Benutzeroberfläche des Verbindungs-Managers auswählen. Ein Benutzer kann zum Beispiel Standorteigenschaften und Wählregeln für die Verbindung zwischen Büro und Heim und für eine häufig bei Geschäftsreisen verwendete Adresse herstellen. Ein Administrator kann die Felder *Benutzernamen* und *Kennwort* für ein Verbindungs-Manager-Profil im Vorfeld ausfüllen.
- **Wechselmedien-Manager** Mit dieser Funktion können Sie Wechselmedien katalogisieren und verwalten. Der Manager kann einen Katalog mit gemeinsam verwendeten Wechselmedien erstellen und diese verwalten.
- **Windows PowerShell** Die Windows PowerShell ist eine Erweiterung für die Befehlszeile unter Windows Server 2008. Auch neue Serverfunktionen wie zum Beispiel Exchange Server 2007 basieren auf dieser neuen Verwaltungsoberfläche. Die PowerShell erweitert die Funktionen der Befehlszeile stark. Administratoren die Server gerne über die Befehlszeile verwalten wollen, sollten sich in diese neue Shell einarbeiten, da deutlich mehr Funktionen zur Verfügung gestellt werden, als in der normalen Befehlszeile. Windows PowerShell basiert auf .NET Framework. Über 130 Befehlszeilentools (so genannte »Cmdlets«) für allgemeine Systemverwaltungsaufgaben wie die Verwaltung von Diensten, Prozessen, Ereignisprotokollen, Zertifikaten, der Registrierung und der Windows-Verwaltungsinstrumentation (WMI) stehen zur Verfügung. Die

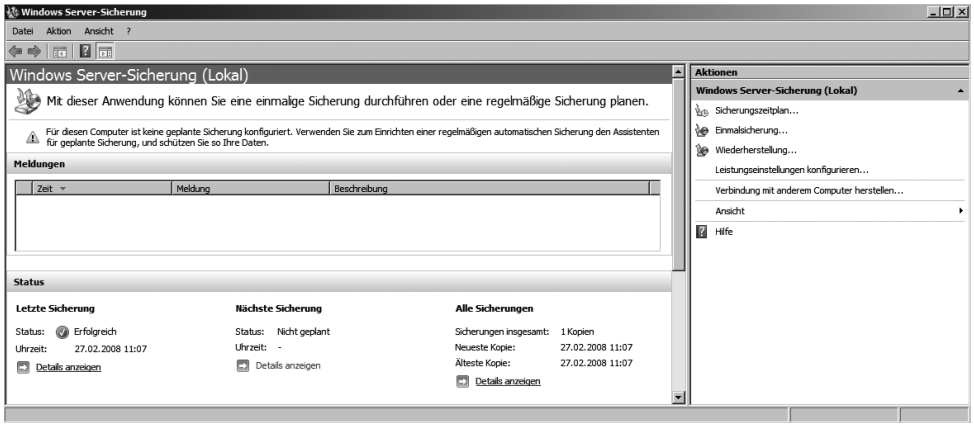
Befehlszeilentools können leicht erlernt und verwendet werden, da Standardnamenskonventionen und übliche Parameter sowie einfache Tools zum Sortieren, Filtern und Formatieren von Daten und Objekten eingesetzt werden. Durch die ausgereifte Ausdrucksanalyse und .NET Framework-Objektmanipulation an der Befehlszeile, einschließlich Pipelining von Objekten, können IT-Spezialisten effizienter und produktiver arbeiten. Sie finden die Startverknüpfung zur PowerShell im Startmenü unter *Alle Programme*. Geben Sie in der PowerShell den Befehl *get-command* ein, um eine Übersicht über alle Befehle der PowerShell zu erhalten (Abbildung 4.15).

Abbildg. 4.15 Windows Server 2008 in der Befehlszeile verwalten



- **Windows Server-Sicherungsfeatures** Das standardmäßige Datensicherungsprogramm von Windows Server wird nicht mehr automatisch installiert, sondern muss manuell nachinstalliert werden. Das Programm wurde für Windows Server 2008 komplett überarbeitet. Die Sicherung unterstützt jetzt besser die Schattenkopien sowie die integrierten Sicherungsfunktionen von SQL Server 2005/2008 und SharePoint Server 2007. Die Verwaltung der Sicherung findet über die MMC statt. So können Sie auch über das Netzwerk mit der MMC die Datensicherung von mehreren Servern verwalten. Neu sind die Unterstützung für DVD-Brenner, sowie die automatische Überwachung des freien Festplattenplatzes auf dem Sicherungsmedium (siehe auch Kapitel 21).

Abbildg. 4.16 Das Datensicherungsprogramm in Windows Server 2008 hat eine neue Oberfläche



HINWEIS Die neue Windows Server-Sicherung unterstützt keine Sicherung auf Band mehr. Datensicherungen, die Sie mit älteren Versionen von *Ntbackup.exe* erstellt haben, sind nicht mehr kompatibel zur neuen Windows Server-Sicherung. Sollten Sie eine solche Sicherung benötigen, stellt Microsoft kostenlos das alte *Ntbackup.exe* auf der Internetseite *http://go.microsoft.com/fwlink/?LinkId=82917* zur Verfügung.

- **Windows-Prozessaktivierungssdienst** Bei der Installation von IIS in Windows Server 2008 fordert Windows als Grundlage die Installation des *Windows-Prozessaktivierungsdienstes* (*Windows Process Activation Service, WPAS)*. WPAS ist in der neuen Windows-Generation der Systembaustein, der für IIS die Anwendungspools und Prozesse verwaltet. Die Basic- und Starter-Edition haben nur eine minimale Variante von IIS, die gleichbedeutend ist mit dem *Windows Process Activation Service (WPAS)*, den die Microsofts Windows Communication Foundation (WCF) benötigt (siehe auch Kapitel 13).
- **Windows-Systemressourcen-Manager** WSRM erlaubt, die CPU-Zeit und Speichergröße individuell einer Anwendung zuzuordnen, ohne dass die Einstellungen vom Benutzer geändert werden können. Hauptzweck ist die kontrollierte Verwaltung der Ressourcen auf einem Server mit vielen Anwendungen und Benutzern (siehe Kapitel 12).
- **WINS-Server** Der Windows Internet Naming Service (WINS) spielt auch unter Windows Server 2008 noch eine Rolle. Funktioniert die Namensauflösung per DNS zum Beispiel nicht mehr, kann der interne Replikationsdienst von Active Directory auf WINS zurückgreifen. WINS dient hauptsächlich der Namensauflösung von NetBIOS-Namen.
- **WLAN-Dienst** Möchten Sie einen Server über ein Drahtlosnetzwerk in das Netzwerk einbinden, müssen Sie diese Funktion installieren. In diesem Fall kann parallel zu einer kabelgebundenen Netzwerkanbindung der Server auch über ein Drahtlosnetzwerk angebunden werden. Der WLAN AutoConfig-Dienst steuert in diesem Fall den Zugriff des Servers auf das Netzwerk.

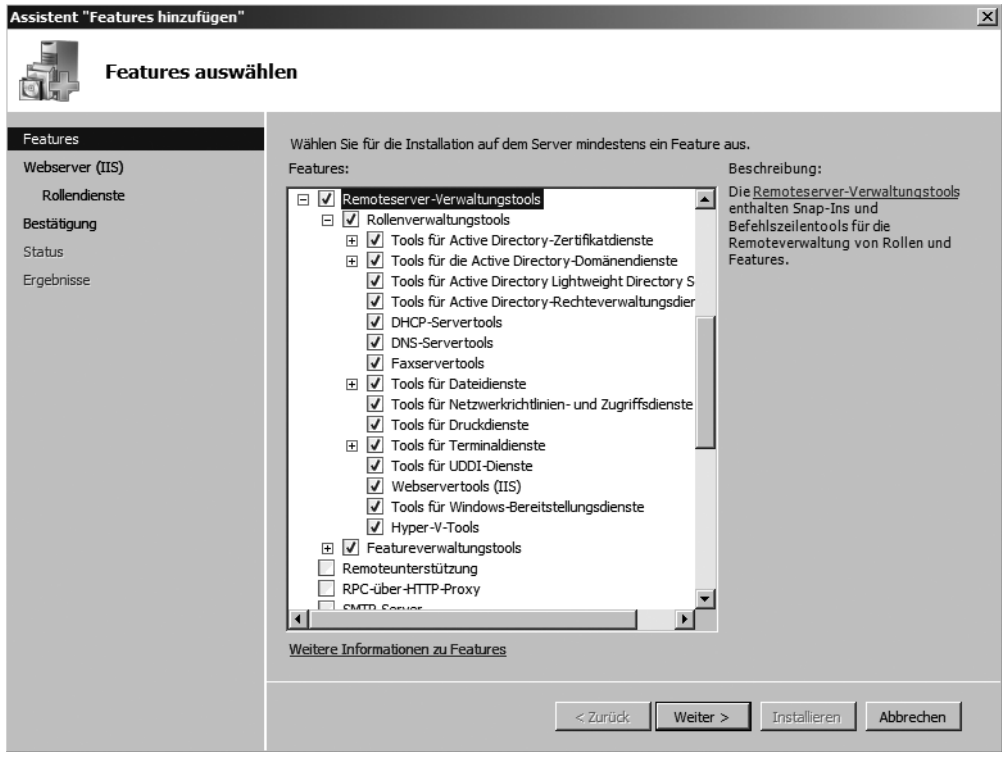
Rollen und Features lassen sich über den jeweiligen Assistenten hinzufügen, verwalten und wieder entfernen. Im Gegensatz zu seinen Vorgängern, bietet Windows Server 2008 dazu mit dem Server-Manager eine einheitliche Oberfläche. In Windows Server 2008 können Sie mehrere Rollen und Funktionen auf einmal installieren, in dem Sie diese markieren und den Assistenten zur Installation

fortfahren. Unter Windows Server 2003 mussten Serverfunktionen noch hintereinander installiert werden. Durch diese neuen Möglichkeiten können Server deutlich schneller installiert und angepasst werden.

Remoteserver-Verwaltungstools

Wollen Sie auf einem Server im Server-Manager lediglich die Snap-Ins zur Verwaltung installieren, nicht die Rolle selbst, stehen Ihnen die *Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT)* zur Verfügung. Diese können für Windows XP und Windows Vista auch im Downloadcenter von Microsoft heruntergeladen werden. Unter Windows Server 2008 können diese Tools als Feature hinzugefügt werden. Sie finden diese im Server-Manager über *Features/Features hinzufügen/Remoteserver-Verwaltungstools* (Abbildung 4.17). Nach der Installation der Tools kann mit diesen jede Rolle eines Windows Server 2008 verwaltet werden, auch wenn die entsprechende Rolle lokal nicht installiert ist.

Abbildg. 4.17 Installieren der Remoteserver-Verwaltungstools



Installation von Serverrollen und Features auf einem Core-Server

Da auf einem Core-Server keine grafische Benutzeroberfläche zur Verfügung steht, läuft die Installation von zusätzlichen Serverrollen und Features auf einem Core-Server anders ab. Auch diese Aufgaben führen Sie in der Befehlszeile durch. Auf den folgenden Seiten zeigen wir Ihnen, wie Sie Serverrollen und Funktionen über die Befehlszeile installieren können. Ein Core-Server verwaltet und unterstützt folgende Serverrollen:

- **Dateiserver**
- **Druckserver** Sie können einen Druckserver auch remote von einem PC mit Windows Vista und der Druckerverwaltungskonsole verwalten. Lokal steht auf einem Core-Server diese Funktion nicht zur Verfügung.
- **Streaming Media Services**
- **Domänencontroller** Für diese Serverrolle können Sie nicht den grafischen Assistenten über *dcpromo.exe* verwenden, sondern müssen eine Antwortdatei erstellen und mit dieser den Server zum Domänencontroller heraufstufen. Nachdem das Active Directory auf einem Server installiert wurde, wird dieser automatisch neu gestartet. Sie können dieses Verhalten mit der Option *RebootOnCompletion=No* in der Antwortdatei anpassen.

HINWEIS Die Installation der Active Directory-Domänendienste auf einem Core-Server erläutern wir Ihnen in Kapitel 8. In diesem Kapitel wird auch die Installation und Verwaltung von Active Directory auf herkömmlichen Servern besprochen.

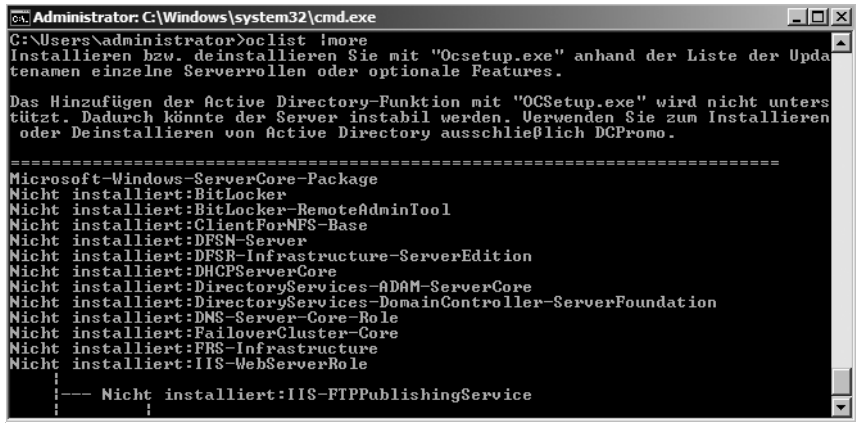
- Active Directory Lightweight Directory Services (AD LDS, unter Windows Server 2003 ADAM genannt)
- DNS-Server
- DHCP-Server

Neben der eingeschränkten Möglichkeit der Rolleninstallation können auf einem Core-Server nicht alle Features installiert werden. Ein Core-Server unterstützt nur folgende Features, die nachträglich installiert werden können:

- Windows Server-Sicherungsfeatures
- BitLocker-Laufwerksverschlüsselung
- Failover-Clusterunterstützung
- Multipfad-E/A
- Netzwerklastenausgleich
- Wechselmedien-Manager
- SNMP-Dienst
- Subsystem für UNIX-basierte Anwendungen
- Telnet-Client
- WINS-Server

TIPP Mit dem Befehl *oclist.exe* können Sie sich in der Befehlszeile eines Core-Servers alle verfügbaren Serverrollen anzeigen lassen. Hier sehen Sie auch, welche dieser Rollen installiert worden ist (Abbildung 4.18). Über den Befehl *ocsetup.exe* können Sie Serverrollen installieren.

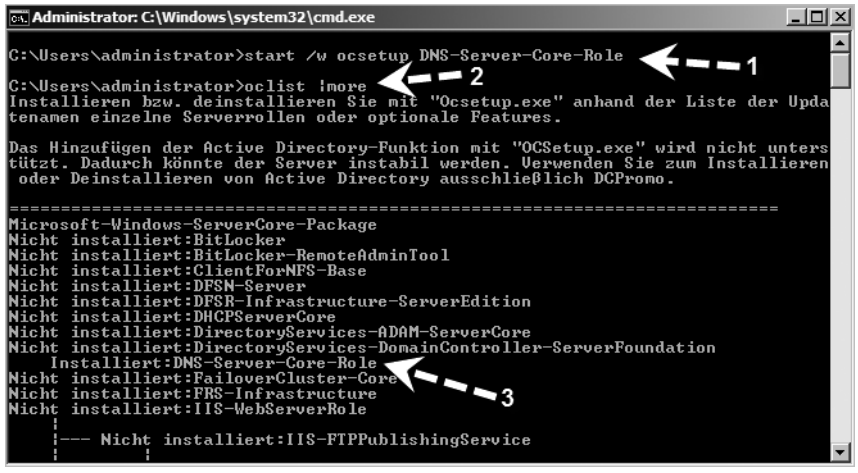
Abbildg. 4.18 Anzeige der verfügbaren Server-Rollen auf einem Core-Server über die Befehlszeile mit *oclist.exe*



Installieren der DNS-Serverrolle auf einem Core-Server

Um auf einem Core-Server die DNS-Serverrolle zu installieren, gehen Sie folgendermaßen vor: Geben Sie in der Befehlszeile den Befehl *start /w ocsetup DNS-Server-Core-Role* ein. Achten Sie darauf, dass der Befehl *ocsetup.exe* case-sensitive ist, also die Eingabe von Groß- und Kleinbuchstaben unterstützt. Durch die Eingabe der Option */w* wird verhindert, dass die Befehlszeile Befehle entgegennimmt, bevor die Installation der Rolle abgeschlossen worden ist. Sie erhalten keinerlei Rückmeldung nach der Installation. Nach der Installation können Sie sich über den Befehl *oclist.exe* die erfolgreiche Installation der Rolle anzeigen lassen. Die Verwaltung eines DNS-Servers auf einem Core-Server nehmen Sie entweder über die Befehlszeile mit dem Befehl *dnscmd.exe* vor, oder Sie verwalten den Server mit einem DNS-Server-Snap-In von einem herkömmlichen Windows Server 2008. Die Verwaltung von DNS-Servern zeigen wir Ihnen in den Kapiteln 8 und 11. Mit dem Befehl *start /w ocsetup DNS-Server-Core-Role /uninstall* deinstallieren Sie die DNS-Server-Rolle auf dem Core-Server wieder.

Abbildg. 4.19 Installieren der DNS-Server-Rolle mit *ocsetup.exe* und verifizieren der Installation über *oclist.exe*



Installieren der DHCP-Serverrolle auf einem Core-Server

Die Installation der DHCP-Serverrolle läuft ähnlich zur Installation eines DNS-Servers ab. Hier verwenden Sie den Befehl *start /w ocsetup DHCPServerCore*. Die Überprüfung der Installation können Sie wieder mit *oclist.exe* überprüfen. Denken Sie daran, dass Sie den DHCP-Server noch authentifizieren müssen. Die Verwaltung eines DHCP-Server nehmen Sie entweder von einem herkömmlichen DHCP-Server und dessen Verwaltungskonsole vor, oder Sie verwenden das Befehlszeilen-Tool *netsh.exe* (siehe Kapitel 3 und 11). Mit dem Befehl *start /w ocsetup DHCPServerCore /uninstall* deinstallieren Sie die Rolle wieder.

Installieren der Dateiserver-Rolle auf einem Core-Server

Im Gegensatz zur DNS- oder DHCP-Serverrolle können Sie die Dateiserver-Rolle etwas detaillierter konfigurieren. Auch ohne die Installation dieser Rolle stehen auf dem Server Freigaben zum Beispiel für administrative Tools zur Verfügung. Nur wenn Sie zusätzliche Funktionen nutzen wollen, um einen Dateiserver zu betreiben, müssen Sie diese manuell nachinstallieren. Dazu stehen folgende Rollen zur Verfügung:

- **Dateireplikationsdienst (File Replication Service, FRS)** *start /w ocsetup FRS-Infrastructure*
- **Verteiltes Dateisystem (Distributed File System, DFS)** *start /w ocsetup DFSN-Server.* Der DFS-Dienst integriert ungleiche Dateifreigaben, die sich in einem LAN oder WAN (Wide Area Network) befinden, in einen einzelnen logischen Namespace. Der DFS-Dienst wird für Active Directory-Domänencontroller benötigt, um den freigegebenen SYSVOL-Ordner zu synchronisieren.

- **Distributed File System Replication** *start /w ocsetup DFSR-Infrastructure-ServerEdition.* Der DFSR-Dienst (Distributed File System Replication) ist eine Replikationsengine, die automatisch Updates zu Dateien und Ordnern zwischen Computern kopiert, die Mitglied einer gemeinsamen Replikationsgruppe sind. DFSR wurde in Windows Server 2003 R2 hinzugefügt und steht auch in Windows Server 2008 zur Verfügung. DFSR wird nicht für SYSVOL-Replikation verwendet.
- **Network File System** *start /w ocsetup ServerForNFS-Base* und *start /w ocsetup ClientForNFS-Base*

Auch diese Rollen können Sie wieder mit der Option */uninstall* deinstallieren.

TIPP Wollen Sie die Datenträgerverwaltung eines Core-Servers über das entsprechende MMC-Snap-In von einem anderen Server aus durchführen, müssen Sie auf dem Core-Server den Virtual Disk Service starten. Geben Sie dazu auf dem Core-Server den Befehl *net start vds* ein.

Installieren der Druckserver-Rolle auf einem Core-Server

Um die Druckserver-Rolle auf einem Core-Server zu installieren, stehen Ihnen zwei verschiedene Funktionen zur Verfügung:

- Die Installation der Standardrolle eines Druckservers führen Sie mit dem Befehl *start /w ocsetup Printing-ServerCore-Role* durch.
- Den Line Printer Daemon (LPD) installieren Sie über *start /w ocsetup Printing-LPDPrintService*. Der TCP/IP-Druckserver-Dienst ermöglicht das Drucken auf TCP/IP-Grundlage mithilfe des LPD-Protokolls (Line Printer Daemon). Der LPD-Dienst auf dem Server erhält Dokumente von LPR-Dienstprogrammen (Line Printer Remote), die zum Beispiel auf UNIX-Computern ausgeführt werden.

Installieren von Active Directory Lightweight Directory Services (AD LDS)

Die AD LDS sind der Nachfolger von ADAM. Dabei handelt es sich um eine Low End-Variante von Active Directory (siehe auch Kapitel 17). Diese Dienste basieren auf der gleichen Technologie und unterstützt ebenfalls Replikation. Mit AD LDS können LDAP-Verzeichnisse für Anwendungen erstellt werden, die wiederum mit Active Directory synchronisiert werden können und dieses auch für die Authentifizierung nutzen können. Es können mehrere AD LDS-Instanzen parallel auf einem Server betrieben werden. AD LDS ist ein LDAP-Verzeichnisdienst (Lightweight Directory Access Protocol), der als Benutzerdienst und nicht als Systemdienst ausgeführt wird. Mit dem Dienst können Unternehmen zum Beispiel andere LDAP-Verzeichnisse in Testumgebungen installieren, ohne auf Software eines Drittanbieters zurückgreifen zu müssen. Um diese Rolle zu installieren, verwenden Sie den Befehl *start /w ocsetup DirectoryServices-ADAM-ServerCore*. Mit dem Befehl *start /w ocsetup DirectoryServices-ADAM-ServerCore /uninstall* deinstallieren Sie die Rolle wieder.

Installieren der Streaming Media Services-Rolle

Um diese Rolle zu installieren, müssen Sie zuvor von einer Arbeitsstation aus, die dazugehörige Installationsdatei herunterladen. Sie finden diese auf der Seite *http://go.microsoft.com/fwlink/?LinkId=88046*.

1. Kopieren Sie die Datei **.msi*-Datei auf den Core-Server.
2. Starten Sie die **.msi*-Datei.
3. Führen Sie anschließend den Befehl *start /w ocsetup MediaServer* aus.

Zur Konfiguration dieser Rolle sollten Sie das entsprechende Snap-In auf einem herkömmlichen Windows Server 2008 verwenden.

Installation von zusätzlichen Features

Die Installation von zusätzlichen Features läuft ähnlich ab, wie die Installation von Serverrollen. Auch hier verwenden Sie zur Auflistung *oclist.exe* und zur Installation *ocsetup.exe.* Um ein Feature zu installieren, geben Sie den Befehl *start /w ocsetup <Feature>* ein. Um ein Feature wieder zu deinstallieren, verwenden Sie den Befehl *start /w ocsetup <Feature> /uninstall*. Zur Installation der einzelnen Features verwenden Sie die folgenden Optionen:

- **Failover-Clusterunterstützung** *FailoverCluster-Core*
- **Netzwerklastenausgleich** *NetworkLoadBalancingHeadlessServer*
- **Subsystem für UNIX-basierte Anwendungen** *SUACore*
- **Multipfad-E/A** *MultipathIo*
- **Wechselmedien-Manager** *Microsoft-Windows-RemovableStorageManagementCore*
- **BitLocker-Laufwerkverschlüsselung** *BitLocker*
- **Verwaltungstool für BitLocker** *BitLocker-RemoteAdminTool*
- **Windows Server-Sicherungsfeatures** *WindowsServerBackup*
- **SNMP-Dienst** *SNMP-SC*
- **WINS-Server** *WINS-SC*
- **Telnet-Client** *TelnetClient*

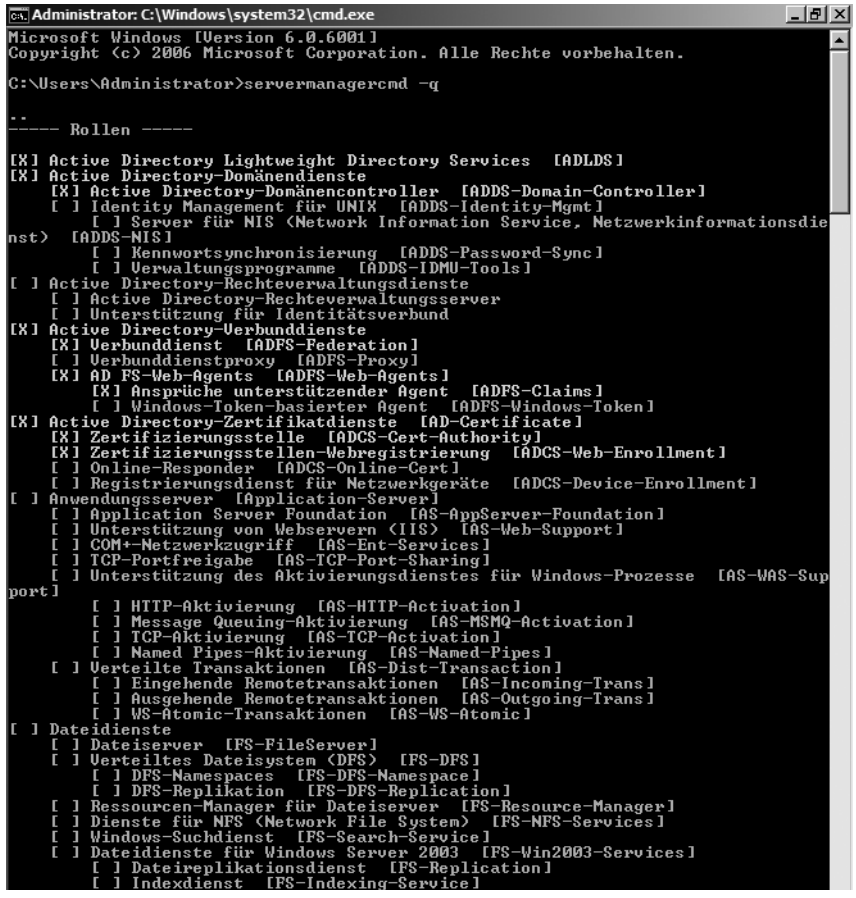
Serverrollen und -features in der Befehlszeile verwalten

Die Installation und Verwaltung von Serverrollen findet hauptsächlich über den Server-Manager statt. Neben der grafischen Oberfläche für dieses Tool gibt es auch ein Befehlszeilen-Tool des Server-Managers mit der Bezeichnung *ServerManagerCMD.exe*. Mit diesem Tool lassen sich alle Funktionen ausführen, die auch in der grafischen Oberfläche durchgeführt werden können. Der Vorteil von *ServerManagerCMD* liegt darin, dass die Installation und Konfiguration von Rollen und Funktionen auch skriptbasiert in der Befehlszeile durchgeführt werden können. Eine ausführliche Übersicht erhalten Sie über *servermanagercmd –help*. Das Tool steht allerdings nicht auf Core-Servern zur Verfügung.

Die installierten Rollen und Funktionen eines Servers in der Befehlszeile

Einen ersten Überblick über die installierten Rollen und Features werden zum Beispiel mit dem Befehl *servermanagercmd –query* angezeigt, auch *servermanagercmd –q* funktioniert (Abbildung 4.20).

Abbildg. 4.20 Anzeigen der installierten Rollen und Funktionen eines Servers in der Befehlszeile



Die Ausgabe lässt sich außerdem mit der zusätzlichen Option *<Datei>.xml* in eine XML-Datei umleiten, die mit anderen Programmen weiterverarbeitet werden kann. Über den Befehl *servermanagercmd –v(ersion)* können Sie sich die aktuelle Version des Server-Managers anzeigen lassen.

Rollen und Features in der Befehlszeile installieren oder deinstallieren

Neben der Anzeige von bereits installierten Rollen und Features können über *ServerManagerCMD.exe* auch Komponenten installiert werden. Hierbei stehen verschiedene Optionen zur Verfügung, die miteinander kombiniert werden können:

- Zur Installation gibt es den Befehl *servermanagercmd –install <Rolle oder Feature>*. Jede Rolle, jeder Rollendienst und jedes Feature besitzt eine eigenständige ID, über welche die Installation gestartet werden kann. Über den Befehl *servermanagercmd –remove <Rolle oder Feature>* wird die entsprechende Rolle oder das Feature deinstalliert.
- Wird zusätzlich noch die Option *–allSubFeatures* angehängt, werden auch alle untergeordneten Rollendienste einer Rolle installiert.

- Das Ergebnis der Installation kann durch die zusätzliche Option *–resultPath <XML-Datei>* in einer XML-Datei ausgegeben werden.
- Eine weitere zusätzliche Option ist *–restart*. Benötigt eine der zu installierenden Rollen oder Features einen Neustart, wird dieser automatisch im Anschluss durchgeführt.
- Alternativ zu *-resultPath*, kann mit der Option *–whatIf* angezeigt werden, was passieren würde, wenn der Befehl ausgeführt wird. Installiert wird dabei nichts, es wird nur simuliert.
- Der Server-Manager führt über die Vorgänge standardmäßig eine Logdatei, die unter *C:\Windows\Temp\servermanager.log* abgelegt wird. Dieser Pfad kann über die Option *–logPath <Datei>.txt* angepasst werden.

Im folgenden Abschnitt gehen wir auf die wichtigsten IDs zur Installation der Rollen und Features ein. Diese IDs können nicht nur für die Installation über die Befehlszeile verwendet werden, sondern auch als ID für die XML-Antwortdateien (siehe nächsten Abschnitt "Unbeaufsichtigte Installation von Rollen und Features).

- **Active Directory-Domänendienste (Active Directory Domain Services, AD DS)** *ADDS-Domain-Controller*
- **DHCP-Server** *DHCP*
- **DNS-Server** *DNS*
- **Terminaldienste** *Terminal-Services*
- **IIS** *Web-Server*

Eine ausführliche Liste erhalten Sie auf der Internetseite *http://technet2.microsoft.com/windowsserver2008/en/library/bab0f1a1-54aa-4cef-9164-139e8bcc44751033.mspx?mfr=true.*

Unbeaufsichtigte Installation von Rollen und Features

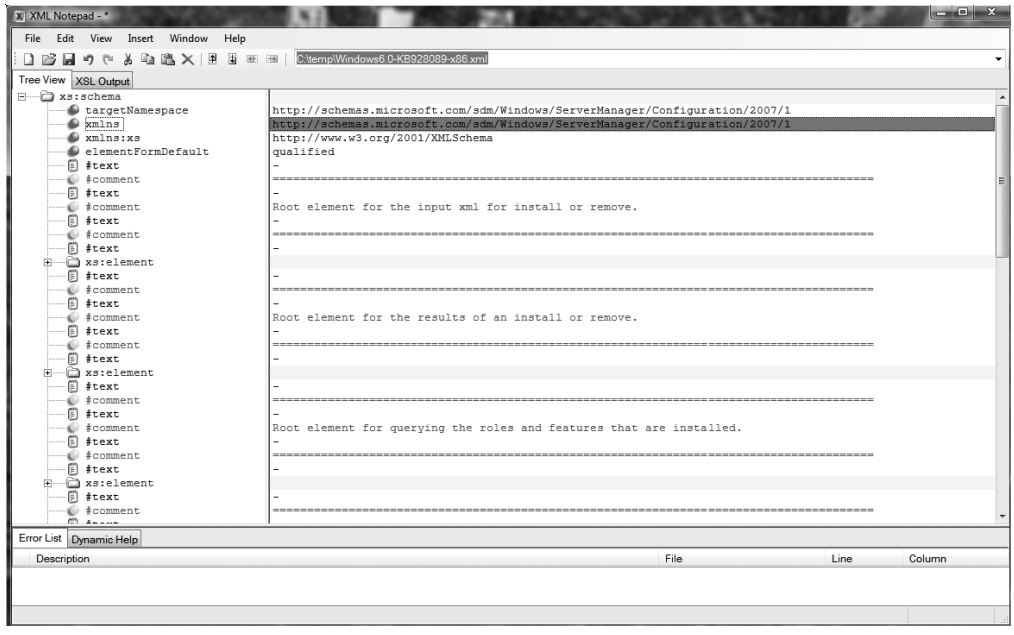
Einer der wichtigsten Vorteile von *ServerManagerCMD* ist die Möglichkeit, Serverrollen und -features unbeaufsichtigt über eine Antwortdatei zu installieren. Dazu wird der Befehl *servermanagercmd –inputPath <Antwortdatei als XML>* verwendet. Die Antwortdatei sollte möglichst als XML-Datei vorliegen. Erstellte Antwortdateien müssen dazu der vorgeschriebenen Syntax entsprechen. Sollen Antwortdateien erstellt werden, bietet sich daher etwas Wissen um den Aufbau von XML-Dateien an. XML-Dateien bearbeiten Sie am besten mit speziellen Editoren für XML. Es funktioniert zwar auch die Bearbeitung der Antwortdateien über normale Editoren, aber XML-Editoren bieten den Vorteil die Anzeige XML-optimiert darzustellen und vor allem das XML-Schema zu validieren.

HINWEIS Genau wie in der grafischen Oberfläche werden auch bei der Installation von Rollen und Funktionen über die Befehlszeile alle abhängigen Komponenten automatisch installiert, wenn diese benötigt werden. Das gilt auch für die untergeordneten Elemente, die auch über die grafische Oberfläche automatisch installiert werden. Ist eine benötigte Rolle oder ein Feature bereits installiert, wird diese/s übersprungen. Wird eine Rolle oder ein Feature über eine Antwortdatei unbeaufsichtigt deinstalliert, dann werden automatisch auch alle abhängigen Rollen und Features deinstalliert. Über die Option *–whatIf* können Sie sich diese Komponenten anzeigen lassen, bevor Sie den Befehl aktivieren.

XML Notepad 2007

Mit XML Notepad 2007 von Microsoft können XML-Dokumente durchsucht und editiert werden. XML (Extensible Markup Language) ist der übergeordnete Standard aller Web-Autoren-Sprachen. Dabei unterstützt das kostenlos herunterladbare Programm den Benutzer bei der Eingabe der Daten und hilft Fehler zu vermeiden. XML-Dokumente werden in einer Baumstruktur dargestellt. Um das XML Notepad 2007 nutzen zu können, muss .NET Framework auf Ihrem Rechner installiert sein. Sie können das Tool auf der Internetseite *http://www.microsoft.com/downloads/details.aspx?FamilyID=72D6AA49-787D-4118-BA5F-4F30FE913628&displaylang=en* herunterladen. Ausführliche Anleitungen für das Tool finden Sie auf der Internetseite *http://www.microsoft.com/germany/msdn/library/data/xml/DesignvonXMLNotepad2006.mspx?mfr=true.*

Abbildg. 4.21 Server-Manager-Antwortdateien mit XML Notepad 2007 bearbeiten



XML-Schema der Antwortdateien mit Beispielen

Das empfohlene Schema für Antwortdateien sehen Sie im folgenden Listing. Im Anschluss daran zeigen wir Ihnen mit ein paar kurzen Beispielen den Umgang mit den XML-Antwortdateien.

Listing 4.1 Empfohlenes Schema für die Installation von Serverrollen und -funktionen über XML-Antwortdateien

```
<?xml version="1.0" encoding="utf-8" ?>
- <xs:schema targetNamespace="http://schemas.microsoft.com/sdm/Windows/ServerManager/
Configuration/2007/1" xmlns="http://schemas.microsoft.com/sdm/Windows/ServerManager/
Configuration/2007/1" xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
- <!--
================================================================================
```

Listing 4.1 Empfohlenes Schema für die Installation von Serverrollen und -funktionen über XML-Antwortdateien *(Fortsetzung)*

```
  -->
- <!--  Root element for the input xml for install or remove.
  -->
- <!--
================================================================================
  -->
- <xs:element name="ServerManagerConfiguration">
- <xs:complexType>
- <xs:choice minOccurs="1" maxOccurs="unbounded">
  <xs:element name="Role" type="FeatureType" minOccurs="0" />
  <xs:element name="RoleService" type="FeatureType" minOccurs="0" />
  <xs:element name="Feature" type="FeatureType" minOccurs="0" />
  <xs:any namespace="##other" processContents="skip" minOccurs="0" />
  </xs:choice>
  <xs:attribute name="Action" type="InstallationActionType" use="required" />
  <xs:anyAttribute namespace="##other" processContents="skip" />
  </xs:complexType>
  </xs:element>
- <!--
================================================================================
  -->
- <!--  Root element for the results of an install or remove.
  -->
- <!--
================================================================================
  -->
- <xs:element name="ServerManagerConfigurationResult">
- <xs:complexType>
- <xs:choice minOccurs="1" maxOccurs="unbounded">
  <xs:element name="Role" type="FeatureResultType" minOccurs="0" />
  <xs:element name="RoleService" type="FeatureResultType" minOccurs="0" />
  <xs:element name="Feature" type="FeatureResultType" minOccurs="0" />
  <xs:element name="Message" type="MessageType" minOccurs="0" />
  <xs:any namespace="##other" processContents="skip" minOccurs="0" />
  </xs:choice>
  <xs:attribute name="Action" type="InstallationActionType" use="required" />
  <xs:attribute name="RequiresReboot" type="xs:boolean" />
  <xs:attribute name="Success" type="xs:boolean" />
  <xs:attributeGroup ref="CommonOutputAttributes" />
  <xs:anyAttribute namespace="##other" processContents="skip" />
  </xs:complexType>
  </xs:element>
- <!--
================================================================================
  -->
- <!--  Root element for querying the roles and features that are installed.
  -->
- <!--
================================================================================
  -->
- <xs:element name="ServerManagerConfigurationQuery">
- <xs:complexType>
- <xs:sequence>
  <xs:element name="Role" type="RoleQueryType" minOccurs="0" maxOccurs="unbounded" />
```

Listing 4.1 Empfohlenes Schema für die Installation von Serverrollen und -funktionen über XML-Antwortdateien *(Fortsetzung)*

```
  <xs:element name="Feature" type="FeatureQueryType" minOccurs="0" maxOccurs="unbounded" />
  <xs:any namespace="##other" processContents="skip" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attributeGroup ref="CommonOutputAttributes" />
  <xs:anyAttribute namespace="##other" processContents="skip" />
  </xs:complexType>
  </xs:element>
- <!--
=================================================================================
  -->
- <!--  Supporting types for the install (or remove) input xml.
  -->
- <!--
=================================================================================
  -->
- <!--  Definition for roles, role services, and features
  -->
- <xs:complexType name="FeatureType">
- <xs:choice minOccurs="0" maxOccurs="unbounded">
  <xs:element name="Setting" type="SettingType" />
  <xs:any namespace="##other" processContents="skip" />
  </xs:choice>
  <xs:attribute name="Id" type="xs:string" use="required" />
- <!--  InstallAllSubFeatures is ignored for features without subfeatures and during remove.
  -->
  <xs:attribute name="InstallAllSubFeatures" type="xs:boolean" />
  <xs:anyAttribute namespace="##other" processContents="skip" />
  </xs:complexType>
- <!--  Definition for settings
  -->
- <xs:complexType name="SettingType">
- <xs:simpleContent>
- <xs:extension base="xs:string">
  <xs:attribute name="Name" use="required" />
  </xs:extension>
  </xs:simpleContent>
  </xs:complexType>
- <!--  Install or Remove action
  -->
- <xs:simpleType name="InstallationActionType">
- <xs:restriction base="xs:string">
  <xs:enumeration value="Install" />
  <xs:enumeration value="Remove" />
  </xs:restriction>
  </xs:simpleType>
- <!--
=================================================================================
  -->
- <!--  Supporting types for the results output of an install or remove.
  -->
- <!--
=================================================================================
  -->
- <xs:complexType name="FeatureResultType">
```

Listing 4.1 Empfohlenes Schema für die Installation von Serverrollen und -funktionen über XML-Antwortdateien *(Fortsetzung)*

```
- <xs:sequence>
  <xs:element name="Message" type="MessageType" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attribute name="DisplayName" type="xs:string" use="required" />
  <xs:attribute name="Success" type="xs:boolean" />
  <xs:attribute name="RootParent" type="xs:string" />
  <xs:attribute name="Id" type="xs:string" />
  <xs:attribute name="RequiresReboot" type="xs:boolean" />
  <xs:attribute name="Skipped" type="xs:boolean" />
  <xs:attribute name="RequestedBy" type="RequestedByType" />
  </xs:complexType>
- <xs:complexType name="MessageType">
- <xs:simpleContent>
- <xs:extension base="xs:string">
  <xs:attribute name="Level" use="required" type="LevelType" />
  <xs:attribute name="Code" type="xs:integer" />
  </xs:extension>
  </xs:simpleContent>
  </xs:complexType>
- <xs:simpleType name="LevelType">
- <xs:restriction base="xs:string">
  <xs:enumeration value="Error" />
  <xs:enumeration value="Warning" />
  <xs:enumeration value="Information" />
  </xs:restriction>
  </xs:simpleType>
- <xs:simpleType name="RequestedByType">
- <xs:restriction base="xs:string">
  <xs:enumeration value="UserSpecified" />
  <xs:enumeration value="Default" />
  <xs:enumeration value="AllChildren" />
  <xs:enumeration value="Dependency" />
  </xs:restriction>
  </xs:simpleType>
- <xs:attributeGroup name="CommonOutputAttributes">
  <xs:attribute name="Time" type="xs:dateTime" />
  <xs:attribute name="Sku" type="xs:string" />
  <xs:attribute name="Language" type="xs:string" />
  <xs:attribute name="Architecture" type="xs:string" />
  </xs:attributeGroup>
- <!--
================================================================================
  -->
- <!--  Supporting types for querying the roles and features that are installed.
  -->
- <!--
================================================================================
  -->
- <xs:complexType name="RoleQueryType">
- <xs:sequence>
  <xs:element name="RoleService" type="RoleServiceQueryType" minOccurs="0"
maxOccurs="unbounded" />
- <!--  The Setting element currently only applies to SharePoint
  -->
```

Listing 4.1 Empfohlenes Schema für die Installation von Serverrollen und -funktionen über XML-Antwortdateien *(Fortsetzung)*

```
  <xs:element name="Setting" type="SettingQueryType" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attributeGroup ref="FeatureQueryAttributes" />
  </xs:complexType>
- <xs:complexType name="RoleServiceQueryType">
- <xs:sequence>
  <xs:element name="RoleService" type="RoleServiceQueryType" minOccurs="0"
maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attributeGroup ref="FeatureQueryAttributes" />
  </xs:complexType>
- <xs:complexType name="FeatureQueryType">
- <xs:sequence>
  <xs:element name="Feature" type="FeatureQueryType" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attributeGroup ref="FeatureQueryAttributes" />
  </xs:complexType>
- <xs:complexType name="SettingQueryType">
- <xs:sequence>
  <xs:element name="Value" type="ValueQueryType" minOccurs="0" maxOccurs="unbounded" />
  </xs:sequence>
  <xs:attribute name="Name" type="xs:string" />
  <xs:attribute name="Description" type="xs:string" />
  </xs:complexType>
- <xs:complexType name="ValueQueryType">
  <xs:attribute name="Name" type="xs:string" />
  <xs:attribute name="Description" type="xs:string" />
  </xs:complexType>
- <xs:attributeGroup name="FeatureQueryAttributes">
  <xs:attribute name="DisplayName" type="xs:string" use="required" />
  <xs:attribute name="Installed" type="xs:boolean" use="required" />
  <xs:attribute name="Id" type="xs:string" />
  <xs:attribute name="Default" type="xs:boolean" />
  </xs:attributeGroup>
  </xs:schema>
```

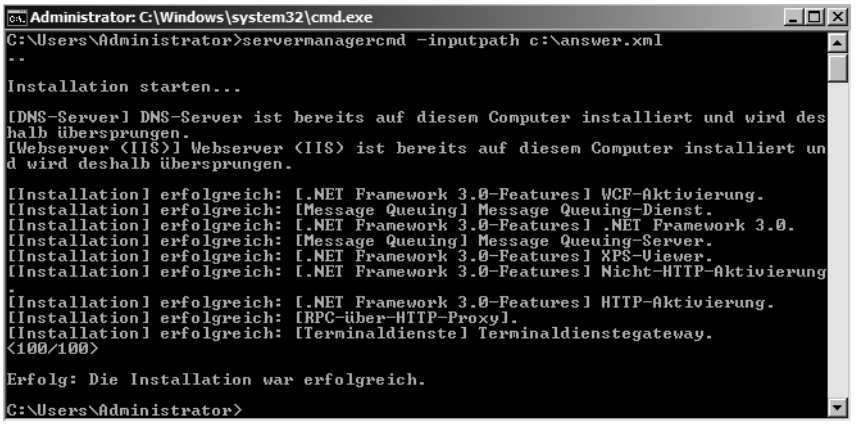
Beispiele

Um eine Antwortdatei zu erstellen, müssen nicht immer solche komplexen Skripts erstellt werden. Oft reichen kurze Texte aus, um das gewünschte Ergebnis zu erzielen. Der folgende Text in einer XML-Datei installiert den DNS-Server, Webserver, Terminaldienstegateway, Message Queuing-Server und .NET Framework 3.0. Dieser Text kann ohne weiteres auch in Windows Editor (*Notepad.exe*) erstellt werden. Wird der Zeilenumbruch aktiviert, können die einzelnen Zeilen auch angepasst werden (Abbildung 4.22).

Abbildg. 4.22 Bearbeiten einer einfachen Antwortdatei für den Server-Manger

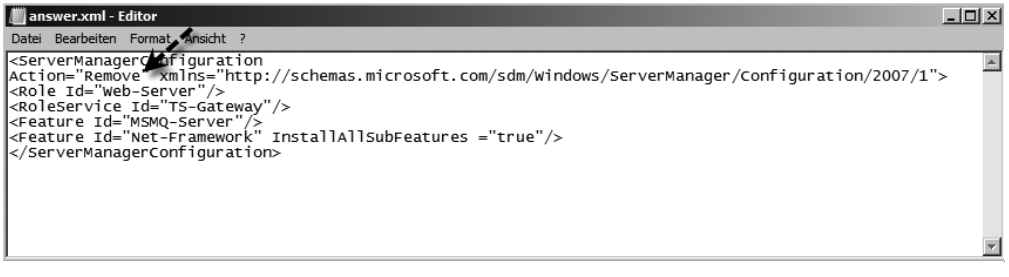
Nach der Bearbeitung kann die Datei einfach als *C:\answer.xml* gespeichert werden. Über den Befehl *servermanagercmd –inputpath c:\answer.xml*, wird diese zur Installation verwendet. Da auf dem Server im Beispiel bereits DNS installiert ist, wird diese Rolle übersprungen (Abbildung 4.23).

Abbildg. 4.23 Installieren von mehreren Rollen und Funktionen über eine Antwortdatei



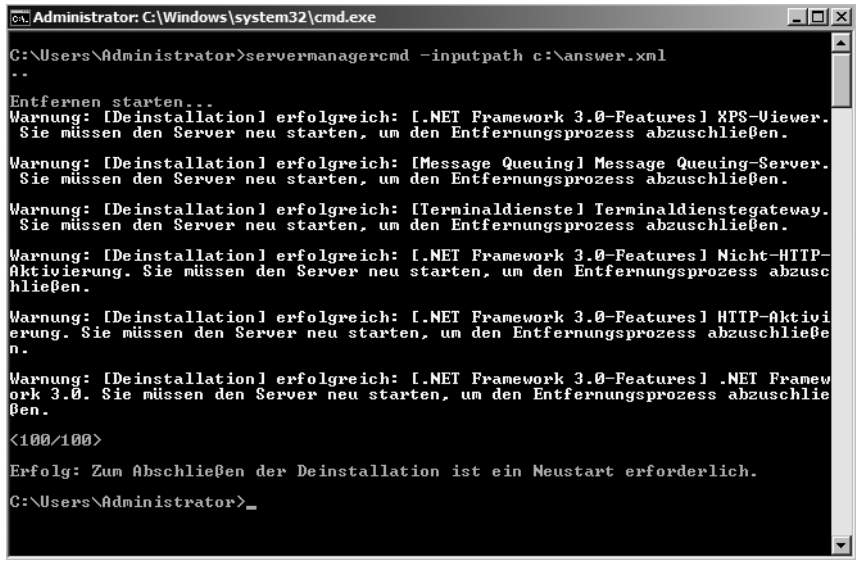
Anschließend arbeitet der Installationsassistent alle Rollen und Funktionen ab und meldet die erfolgreiche Installation. Durch den Befehl *Remove* anstelle des Befehls *Install* in der Antwortdatei werden die entsprechenden Rollen oder Funktionen wieder deinstalliert. Dazu können Sie in einer Testumgebung einfach die bereits erstellte XML-Datei öffnen und den Befehl von *Install* auf *Remove* ändern (Abbildung 4.24).

Abbildg. 4.24 Durchführen einer unbeaufsichtigten Deinstallation über *ServerManagerCMD*



Nachdem Sie auch diesen Befehl über *servermanagercmd –inputpath c:\answer.xml* gestartet haben, beginnt der Assistent mit der Deinstallation entsprechender Komponenten. Nicht installierte Komponenten werden dabei übersprungen, ohne dass der Vorgang abbricht (Abbildung 4.25).

Abbildg. 4.25 Der Assistent entfernt die Komponenten, die in der Antwortdatei zur Deinstallation festgelegt wurden



Zusammenfassung

In diesem Kapitel haben Sie erfahren, welche Serverrollen und -features es gibt, was deren Funktion ist und wie diese installiert werden. Ab den nächsten Kapiteln dieses Buches steigen wir etwas tiefer in die Thematik ein und erläutern Ihnen, wie Sie Windows Server 2008 produktiv einsetzen. Den Anfang macht das folgende Kapitel 5 mit der Verwaltung der Datenträger und des Dateisystems.

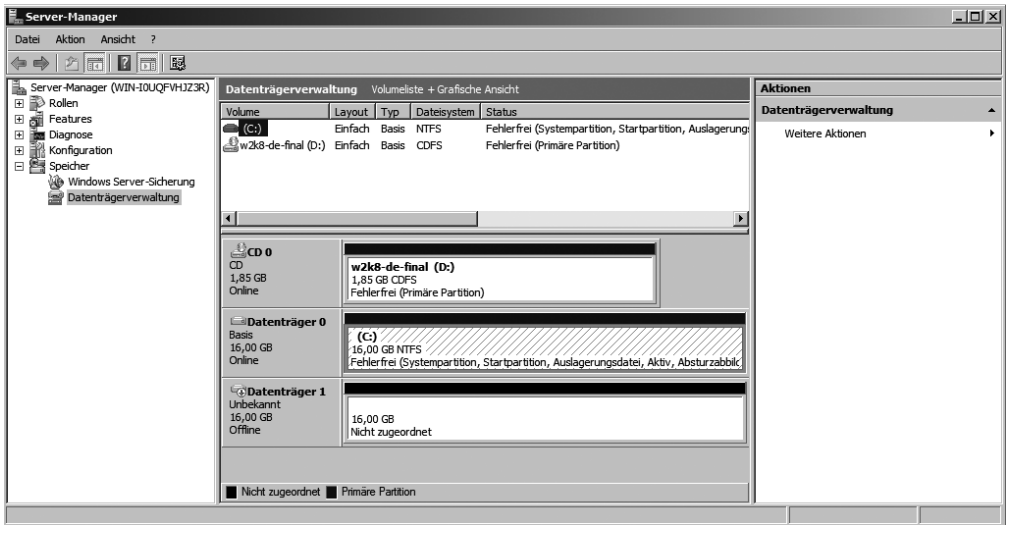
Kapitel 5

Datenträgerverwaltung

In diesem Kapitel:

Microsoft hat auch bezüglich der Datenträgerverwaltung einige Neuerungen in Windows Server 2008 integriert. Die Verwaltung der Datenträger finden Sie am besten im Server-Manager unter *Speicher/Datenträgerverwaltung* (Abbildung 5.1). Sie können die Datenträgerverwaltung ohne Umwege auch über *Start/Ausführen/diskmgmt.msc* aufrufen.

Abbildg. 5.1 Verwalten von Datenträgern in Windows Server 2008

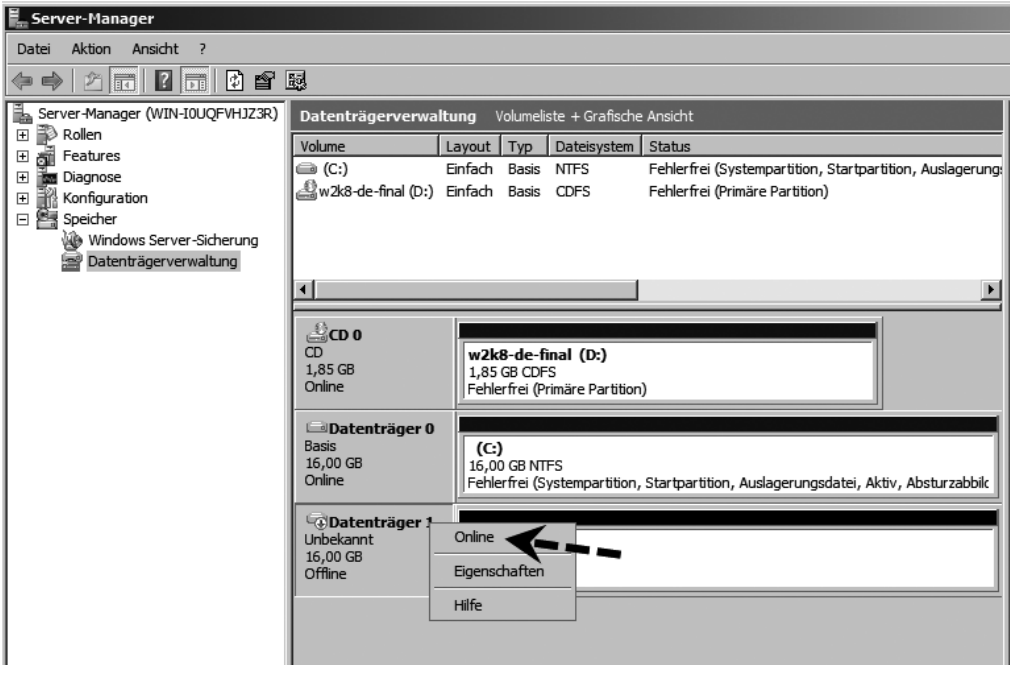


Physische Festplatten und die darauf erstellten Partitionen werden in Windows Server 2008 ähnlich verwaltet wie unter Windows Server 2003. Bereits mit Bordmitteln kann Windows Server 2008 softwarebasierte RAID-Systeme erstellen oder Datenträger auf mehrere physische Festplatten ausdehnen, die dann in Windows Server 2008 wie eine einzelne Festplatte in Erscheinung treten. Wenn Sie die Datenträgerverwaltung in dieser Konsole starten, werden im oberen Dialogfeldbereich alle konfigurierten Datenträger im Sinne von logischen Laufwerken angezeigt. Im unteren Bereich sind dagegen die physischen Datenträger inklusive Wechselmedien zu sehen. Bei Festplatten wird angezeigt, auf welchen der installierten Festplatten sich die logischen Laufwerke befinden und welcher Platz noch nicht zugeordnet ist (Abbildung 5.2). Im Bereich der Datenträgerverwaltung werden oft viele Fachbegriffe verwendet, die bei der Konfiguration von Datenträgern eine wichtige Rolle spielen. Eine *Partition*, auch als *Volume* bezeichnet, ist ein Bereich auf einer Festplatte, der mit einem Dateisystem formatiert und mit einem Buchstaben des Alphabets identifiziert werden kann. Beispielsweise stellt das Laufwerk *C:* auf den meisten Computern unter Windows eine *Partition* dar. Eine *Festplatte* muss *partitioniert* und *formatiert* werden, bevor Daten darauf gespeichert werden können. Auf vielen Computern wird nur eine einzelne Partition eingerichtet, die der Größe der Festplatte entspricht. Es ist nicht erforderlich, eine Festplatte in mehrere kleinere Partitionen aufzuteilen.

Einrichten von Datenträgern

Wird eine zusätzliche Festplatte eingebaut, müssen Sie diese in Windows einbinden. Zunächst müssen Sie festlegen, wie die Festplatte initialisiert werden soll. Unter Windows Server 2008 werden neue Festplatten als »Offline« angezeigt. Sie erkennen dies an dem roten Pfeil, der nach unten zeigt. Bevor Sie eine Festplatte verwenden können, müssen Sie diese zunächst per Klick mit der rechten Maustaste online schalten (Abbildung 5.2).

Abbildg. 5.2 Online schalten eines Datenträgers unter Windows Server 2008



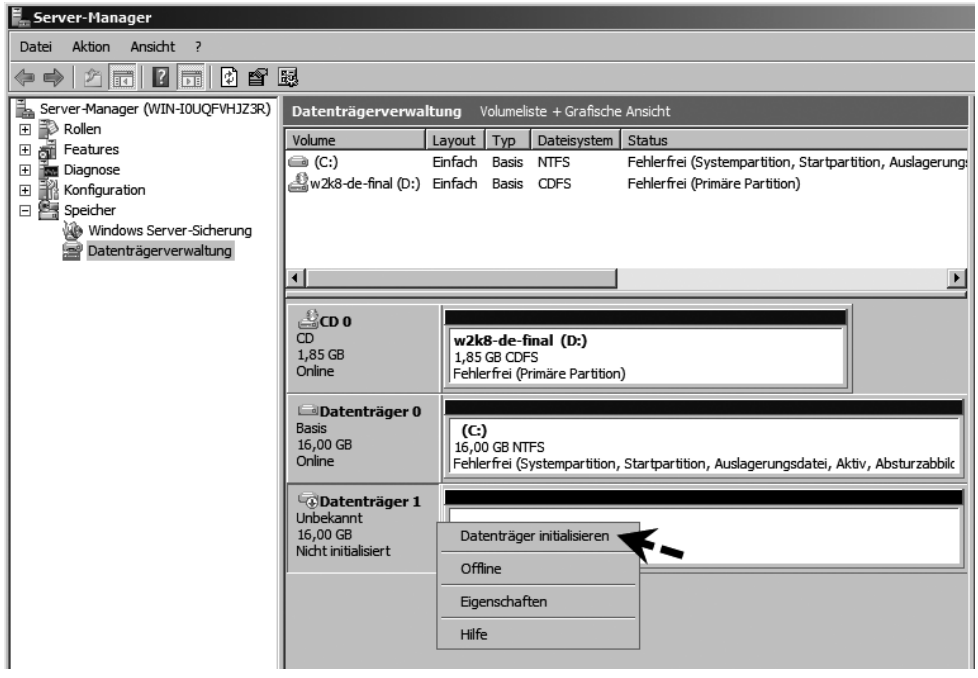
Anschließend müssen Sie die Datenträger wiederum mit einem Klick der rechten Maustaste initialisieren (Abbildung 5.3).

Bestätigen Sie den Vorschlag, MBR (Master Boot Record) oder GPT (GUID-Partitionstabelle) zu verwenden. Bei MBR handelt es sich um einen Code, der sich im ersten Sektor einer Festplatte befindet und Informationen zu den Partitionen auf dem Datenträger enthält. Mit dem MBR beginnt der Startvorgang des Computers. Das Datenträger-Partitionsformat MBR unterstützt Volumes mit einer Größe von bis zu zwei Terabytes und bis zu vier Primärpartitionen pro Datenträger (oder drei Primärpartitionen, eine erweiterte Partition und eine unbegrenzte Anzahl logischer Laufwerke). Im Vergleich dazu unterstützt das GPT-Partitionsformat Volumes mit einer Größe von bis zu 18 Exabytes und bis zu 128 Partitionen pro Datenträger. Anders als bei Datenträgern mit dem MBR-Partitionsformat werden Daten, die für den Betrieb der Plattform zwingend erforderlich sind, in Partitionen abgelegt und nicht in Sektoren ohne Partition oder in versteckten Sektoren. Außerdem besitzen Datenträger mit dem GPT-Partitionsformat redundante Primär- und Sicherungspartitionstabellen, wodurch die Integrität der Partitionsdatenstruktur verbessert wird. Auf GPT-Daten-

trägern können Sie dieselben Aufgaben wie auf MBR-Datenträgern durchführen. Dabei gelten folgende Ausnahmen:

- Auf Computern unter Windows Server 2008 muss sich das Betriebssystem auf einem MBR-Datenträger befinden. Alle weiteren Festplatten können mit MBR oder GPT formatiert sein.
- Auf Itanium-basierten Computern müssen das Ladeprogramm des Betriebssystems und die Startpartition auf einem GPT-Datenträger gespeichert sein. Alle weiteren Festplatten können mit MBR oder GPT formatiert sein.

Abbildg. 5.3 Initialisieren eines Datenträgers unter Windows Server 2008



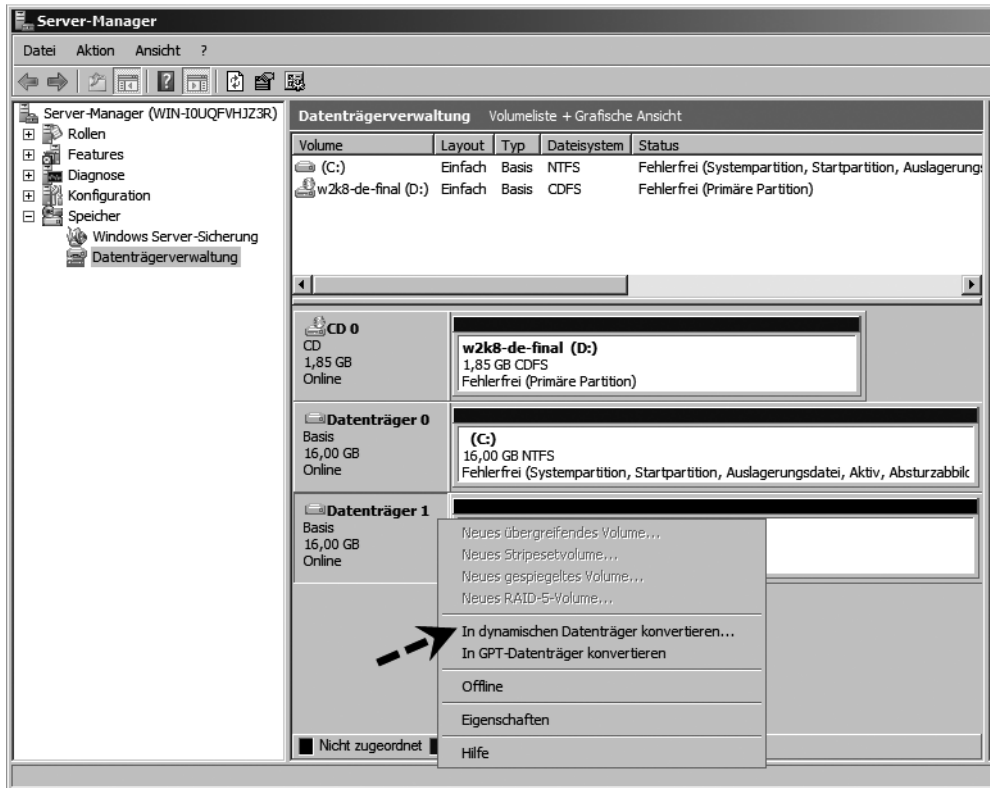
- GPT-Datenträger können nicht auf Computer unter Windows NT 4.0, Windows 2000, Windows Server 2003 oder Windows Server 2008 transferiert werden. Sie können jedoch GPT-Datenträger von Computern unter Windows Server 2003 mit SP1 sowie von x64-basierten Computern auf Itanium-basierte Computer unter Windows Server 2003 oder Windows Server 2008 transferieren und umgekehrt.
- Sie können einen GPT-Datenträger mit einer Itanium-basierten Version von Windows von einem Itanium-basierten Computer nicht auf einen x86-basierten Computer unter Windows Server 2003 mit SP1 oder auf x64-basierte Computer transferieren und dann das betreffende Betriebssystem starten. In Nicht-Itanium-basierten-Computern verwendete GPT-Datenträger dürfen nur für die Datenspeicherung verwendet werden.
- Die Konvertierung eines MBR-Datenträgers in einen GPT-Datenträger und umgekehrt kann nur durchgeführt werden, wenn der Datenträger leer ist.

Nach der Initialisierung werden die Datenträger in der Datenträgerverwaltung angezeigt und können konfiguriert werden. Die leeren Festplatten können in dynamische Datenträger umgestellt werden. Windows Server 2008 unterscheidet zwischen zwei Arten von Festplatten:

- **Basisdatenträger** werden genauso behandelt wie Festplatten unter Windows NT. Das Modell ist weitgehend vergleichbar mit dem, das bereits zu DOS-Zeiten verwendet wurde. Es können feste Partitionen eingerichtet werden, in denen wiederum logische Laufwerke erstellt werden können. Wenn Sie Partitionen auf einer Basisfestplatte erstellen, sind die ersten drei Partitionen, die Sie erstellen, primäre Partitionen. Diese können für den Start eines Betriebssystems verwendet werden. Eine primäre Partition kann ein Betriebssystem hosten und verhält sich wie ein physischer separater Datenträger. Auf einem Basisdatenträger können bis zu vier primäre Partitionen erstellt werden. Wenn Sie mehr als drei Partitionen erstellen möchten, wird die vierte Partition als erweiterte Partition erstellt. Eine erweiterte Partition bietet eine Möglichkeit, eine Beschränkung der möglichen Anzahl von primären Partitionen auf einer Basisfestplatte zu umgehen. Eine erweiterte Partition ist ein Container, der ein oder mehrere logische Laufwerke enthalten kann. Logische Laufwerke haben dieselbe Funktion wie primäre Partitionen, können jedoch nicht für den Start eines Betriebssystems verwendet werden. Erweiterte Partitionen können mehrere logische Laufwerke enthalten, die formatiert werden können und denen Laufwerkbuchstaben zugewiesen werden.
- **Dynamische Datenträger** lassen sich sehr viel einfacher verwalten als die Basisdatenträger. Das betrifft die Veränderung der logischen Laufwerke ohne einen Neustart des Systems. Daher macht es Sinn, generell mit dynamischen Datenträgern zu arbeiten, zumindest wenn Sie Datenträger unter Windows erweitern wollen. Dynamische Datenträger können eine unbegrenzte Anzahl von dynamischen Volumes enthalten und funktionieren wie die primären Partitionen, die auf Basisdatenträgern verwendet werden. Der Hauptunterschied zwischen Basisdatenträgern und dynamischen Datenträgern besteht darin, dass dynamische Datenträger Daten zwischen zwei oder mehreren dynamischen Festplatten eines Computers freigeben und Daten auf mehrere Festplatten verteilen können. Beispielsweise kann sich der Speicherplatz eines einzelnen dynamischen Volumes auf zwei separaten Festplatten befinden. Zudem können dynamische Datenträger Daten zwischen zwei oder mehreren Festplatten duplizieren, um dem Ausfall einer einzelnen Festplatte vorzubeugen. Diese Fähigkeit erfordert mehr Festplatten, erhöht jedoch die Zuverlässigkeit.

Um einen vorhandenen Basisdatenträger in einen dynamischen Datenträger umzuwandeln, müssen Sie im unteren Bereich der Datenträgerverwaltung beim Eintrag der Festplatte über das Kontextmenü den Befehl *In dynamischen Datenträger konvertieren* aufrufen (Abbildung 5.4). Es wird ein Dialogfeld angezeigt, in dem die zu aktualisierenden Basisfestplatten ausgewählt werden können. Es können also in einem Schritt alle noch vorhandenen Basisfestplatten in einem System aktualisiert werden.

Abbildg. 5.4 Konvertieren von Basisdatenträgern zu dynamischen Datenträgern



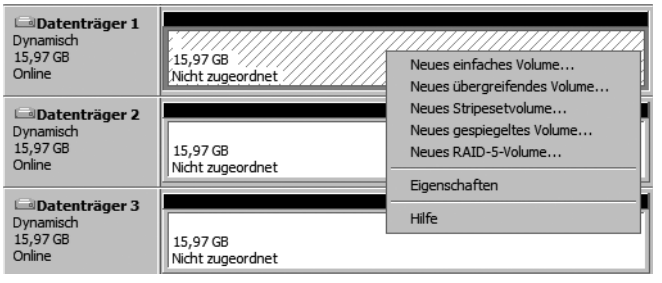
Nach der Auswahl der Festplatten wird ein zweites Dialogfeld angezeigt, in dem die gewählten Festplatten noch einmal aufgeführt sind. Hier können Sie entscheiden, welche der neuen Festplatten in dynamische Datenträger umgewandelt werden können. Sobald der Assistent die Festplatten initialisiert und in dynamische Datenträger umgewandelt hat, stehen diese im System zur Verfügung. Unter Windows Server 2003 musste ein PC während der Konvertierung zu dynamischen Datenträgern noch bis zu zweimal neu gestartet werden. Ein solcher Neustart ist unter Windows Server 2008 nicht mehr notwendig. Basisdatenträger können jederzeit wieder in dynamische Datenträger umgewandelt werden. Wenn Sie Datenträgerkonfigurationen, wie zum Beispiel die Erweiterung eines Laufwerks (siehe später in diesem Kapitel) durchführen wollen, und Sie den Datenträger noch nicht zu einem dynamischen Datenträger konvertiert haben, schlägt der Assistent die Konvertierung vor.

Konfigurieren von Laufwerken

Sobald die Datenträger eingerichtet sind, können auf diesen logische Laufwerke eingerichtet werden. Es empfiehlt sich, zunächst alle Festplatten auf dynamische Datenträger umzustellen und erst im Anschluss zusätzliche Laufwerke einzurichten, vor allem, wenn Sie erweiterte Datenträger einsetzen. Wenn Sie pro Laufwerk einen einzelnen Datenträger erstellen wollen, ist es nicht notwendig, eine Konvertierung durchzuführen. Solche logischen Laufwerke, bei Windows Server 2008 auch als

Datenträger bezeichnet, werden mit dem Befehl *Neues einfaches Volume* angelegt (Abbildung 5.5). Dazu muss entweder ein freier Bereich auf einem Datenträger oder die Festplatte, auf der das neue logische Laufwerk erstellt werden soll, mit der rechten Maustaste angeklickt werden. Klicken Sie mit der rechten Maustaste allerdings direkt auf den Datenträger und nicht auf einen freien Bereich, wird Ihnen die Option *Neues einfaches Volume* nicht angezeigt, sondern nur die erweiterten Optionen wie zum Beispiel *Neues übergreifendes Volume* und *Neues Stripesetvolume*.

Abbildg. 5.5 Erstellen von neuen Volumes unter Windows Server 2008



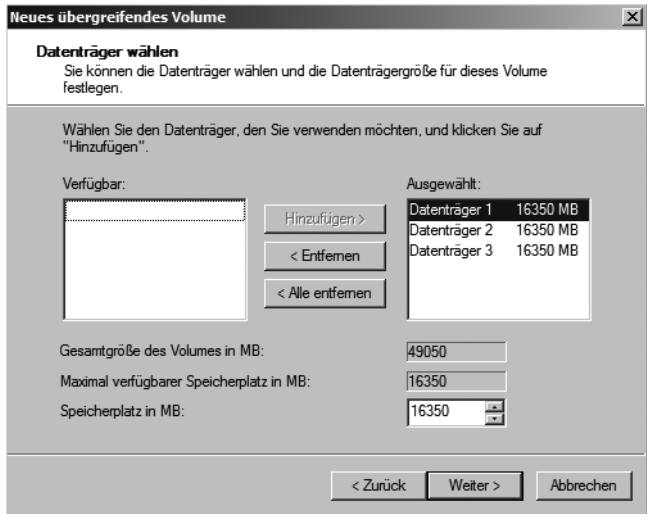
- Ein *einfaches Volume* hält Daten nur auf einer physischen Festplatte.
- Ein *übergreifendes Volume* erstreckt sich über mehrere physische Festplatten. Die Daten darauf werden fortlaufend gespeichert. Wenn der konfigurierte Speicherplatz auf dem ersten physischen Datenträger voll ist, werden weitere Informationen auf dem nächsten konfigurierten Datenträger gespeichert. Dieser Ansatz macht nur Sinn, wenn sehr große logische Datenträger benötigt werden, die größer als die vorhandenen physischen Datenträger sind. Er könnte genutzt werden, wenn die Spiegelung oder RAID der verwendeten Datenträger über die Hardware erfolgt.
- Ein *Stripesetvolume* geht einen Schritt weiter. Bei dieser Variante sind mehrere physische Festplatten beteiligt. Auf jeder dieser Festplatten wird der gleiche Speicherplatz belegt. Die Daten werden in Blöcken von 64 KB zunächst auf der ersten Festplatte, der zweiten und so weiter gespeichert. Wenn eine Datei nur 8 KB groß ist, wird trotzdem ein 64 KB-Block verwendet, die restlichen 56 KB sind dann verschwendet, da diese nicht von anderen Dateien verwendet werden können. Sie werden also über die Festplatten verteilt. Dieser Ansatz bietet keine Fehlertoleranz. Durch die Verteilung der Informationen über mehrere Festplatten wird eine deutlich verbesserte Performance erreicht, allerdings sind die Daten auf dem Datenträger verloren, wenn einer der physischen Datenträger ausfällt.
- Eine fehlertolerante Variante davon ist das *RAID 5-Volume*. Dabei werden ebenfalls mindestens drei und bis zu 32 Festplatten verwendet. Dazu muss auf allen physischen Datenträgern gleich viel Platz belegt werden. Wenn drei Festplatten verwendet werden, werden auf die 64 KB-Blöcke der ersten und zweiten Platte Daten geschrieben und auf der dritten Platte Paritätsinformationen, mit denen sich die Daten im Fehlerfall wiederherstellen lassen. Die nächsten Blöcke von Daten werden auf die zweite und dritte Festplatte geschrieben, während die Paritätsinformationen auf die erste Festplatte gelegt werden. Dieser Ansatz bietet ein Optimum an Fehlertoleranz und gute Performance bei vergleichsweise geringem Verlust an Plattenplatz. Bei einem RAID 5-System mit drei Datenträgern werden 33 % des Plattenplatzes für die Informationen zur Wiederherstellung verwendet, bei fünf Festplatten sind es sogar nur noch 20 %. Allerdings sind RAID-Systeme als Softwarelösung nur eingeschränkt sinnvoll, da sie zum einen keine optimale Performance bieten, da die Paritätsinformationen nicht von einem dedizierten Prozessor

berechnet werden und weil sie zum anderen kein Hot-Swap unterstützen. Hot-Swap bezeichnet den Wechsel von Festplatten im laufenden Betrieb. Es wird daher empfohlen, auf Hardware-Lösungen für RAID-Systeme auszuweichen.

- Schließlich gibt es noch die Plattenspiegelung. Dort werden alle Informationen auf zwei Festplatten geschrieben. Von gespiegelten Festplatten kann auch gebootet werden. Dieser Ansatz lässt sich bei einer reinen Softwarelösung sinnvoll realisieren, weil das System selbst dadurch kaum belastet wird.

Falls ein Datenträger erzeugt wird, der sich über mehr als eine physische Festplatte erstreckt, müssen bei der Definition des Datenträgertyps im nächsten Schritt die Festplatten ausgewählt werden, die beteiligt werden sollen (Abbildung 5.6).

Abbildg. 5.6 Auswählen der physischen Datenträger für das übergreifende Volume



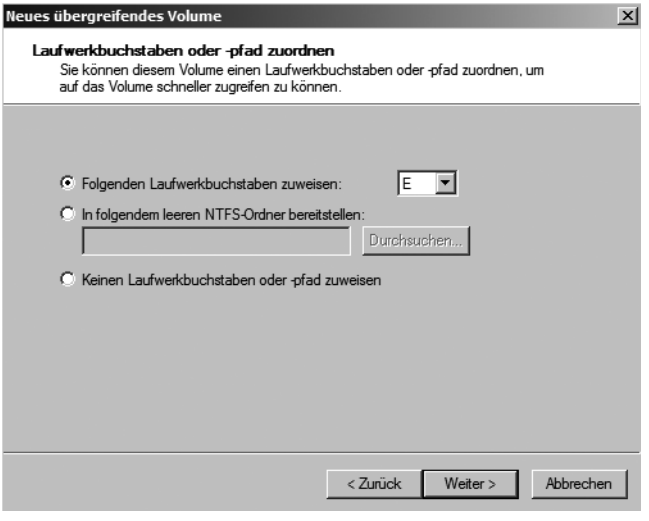
Der nächste generell erfolgende Schritt ist die Zuordnung von Laufwerksbuchstaben und -pfaden. Dieser Schritt kann jederzeit später über den Befehl *Laufwerksbuchstaben und -pfad ändern* im Kontextmenü des entsprechenden Laufwerks durchgeführt werden. Hier finden sich drei Optionen (Abbildung 5.7):

- Dem Laufwerk kann ein Laufwerksbuchstabe fest zugeordnet werden.
- Das Laufwerk kann in einem leeren Ordner eines NTFS-Systems bereitgestellt werden. Damit können bestehende Datenträger erweitert werden. Diese Erweiterung kann im laufenden Betrieb erfolgen und ist sinnvoll, wenn neue Verzeichnisstrukturen geschaffen werden müssen, die viel Platz erfordern werden. Dem Laufwerk wird kein eigener Laufwerks-Buchstabe zugewiesen, sondern Sie können ein bestimmtes Verzeichnis auswählen, dass auf einem bereits konfigurierten Laufwerk liegt. Werden Daten in diesem Verzeichnis gespeichert, lagert Windows diese Daten auf den neuen Datenträger aus.
- Es kann auch auf die Zuordnung von Laufwerkbuchstaben verzichtet werden. Dieses Laufwerk kann dazu verwendet werden, um von einem Ordner einer Festplatte auf einen Ordner einer anderen Festplatte zu gelangen. Dafür können sowohl der Windows-Explorer als auch der Befehl

cd in der Befehlszeile verwendet werden. Dieser Befehl stammt noch aus der DOS-Zeit und ermöglicht das Wechseln zwischen Verzeichnissen in der Befehlszeile. Die ausführliche Syntax erfahren Sie, wenn Sie in der Befehlszeile *cd /?* eingeben.

Die letzten Festlegungen betreffen die Formatierung des Datenträgers. Der Datenträger kann formatiert werden, wobei grundsätzlich das NTFS-Dateisystem als Datenträger verwendet werden sollte (Abbildung 5.7).

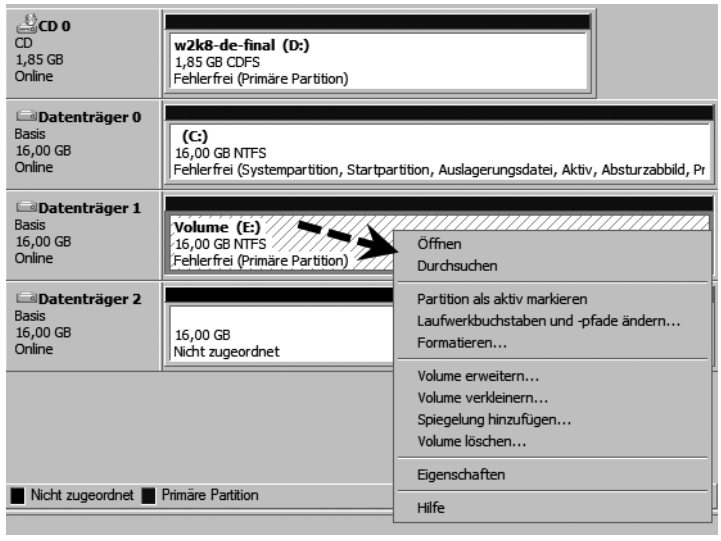
Abbildg. 5.7 Festlegen des Laufwerksbuchstabens für das neue Volume



Um Speicherplatz zu sparen, lassen sich Dateien auf NTFS-Laufwerken komprimieren. Diese Komprimierung erfolgt für den Benutzer völlig transparent. Er muss keine zusätzlichen Programme verwenden und arbeitet mit den Dateien genauso wie mit allen anderen auf dem Laufwerk. Beachten Sie bei der Verwendung der Komprimierung, dass dies zu Lasten der Performance des Servers geht, da dieser die Komprimierung und Dekomprimierung der Dateien übernimmt, sobald ein Benutzer darauf zugreift. Die Komprimierung kann jedoch ohne weiteres für spezielle Archivierungsordner sinnvoll sein. In Zeiten, in denen normalerweise genügend Speicherplatz zur Verfügung steht, sollte die Komprimierung nur für Archivdateien verwendet werden, die ansonsten Speicherplatz verschwenden würden. Sie können auf einem NTFS-Datenträger einzelne Ordner oder Dateien komprimieren, während andere Ordner unkomprimiert bleiben. Die Komprimierung können Sie in den Eigenschaften eines Ordners auswählen. Komprimierte Ordner werden durch eine blaue Farbe der Beschriftung gekennzeichnet. Im Regelfall kann bei der Formatierung die Standardzuordnungseinheit belassen werden. Diese wird in Abhängigkeit von der Größe des Laufwerks gesetzt und ist damit in den meisten Situationen korrekt gewählt. Nur wenn feststeht, dass ausschließlich mit sehr großen Dateien gearbeitet wird, macht es Sinn, einen höheren Wert manuell zu setzen.

Über die Befehle im Kontextmenü von Datenträgern können noch weitere Funktionen ausgeführt werden.

Abbildg. 5.8 Kontextmenü mit weiteren Optionen für Datenträger



- Datenträger können erstmals oder erneut formatiert werden. Bei der Formatierung gehen alle vorhandenen Daten verloren.
- Datenträger können erweitert werden. Damit kann bei dynamischen Datenträgern im laufenden Betrieb weiterer, nicht konfigurierter Platz hinzugefügt werden. Die Erweiterung eines Datenträgers kann dabei auf andere physische Festplatten erfolgen. Damit wird ein übergreifender Datenträger erzeugt. Diese Vorgehensweise ist sinnvoll, wenn mehr Platz in einer bestehenden Verzeichnisstruktur benötigt wird und diese nicht umgestellt werden soll.
- Datenträger können verkleinert werden. Nicht verwendeter Speicherplatz wird in diesem Fall freigegeben.
- Für Datenträger kann die Spiegelung eingerichtet werden, was bereits bei der Erstellung möglich war.

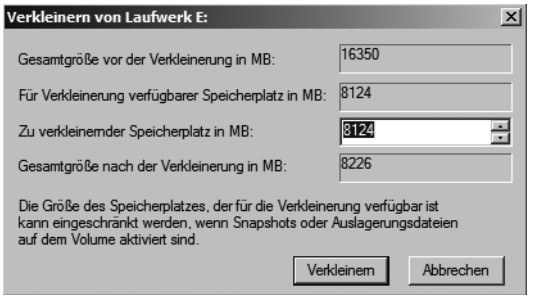
Verkleinern und Erweitern von Datenträgern

Ein Datenträger kann unter Windows Server 2008 auch erweitert oder verkleinert werden. Beim Verkleinern von Laufwerken wird der konfigurierte Speicherplatz, den Sie freigeben wollen, als neuer unpartitionierter Bereich angezeigt. Dieser kann für einen anderen Datenträger verwendet werden, der sich ausschließlich auf diesen freien Bereich erstreckt, oder der Bereich wird zusammen mit einem weiteren Bereich als übergreifender Datenträger verwendet. Es stehen Ihnen verschiedene Möglichkeiten zur Verfügung, um Datenträger zu verbinden. Der verkleinerte Bereich wird genauso angezeigt, als wäre er nie partitioniert gewesen.

Verkleinern von Partitionen

Beim Verkleinern einer Partition werden nicht verschiebbare Dateien (zum Beispiel die Auslagerungsdatei oder der Schattenkopiespeicherbereich) nicht automatisch verschoben, und Sie können den reservierten Speicherplatz nicht über den Punkt hinaus verkleinern, an dem sich die nicht verschiebbaren Dateien befinden. Wenn Sie die Partition weiter verkleinern müssen, verschieben Sie die Auslagerungsdatei auf einen anderen Datenträger, löschen Sie die gespeicherten Schattenkopien, verkleinern Sie das Volume, und verschieben Sie die Auslagerungsdatei dann zurück auf den Datenträger. Sie können nur primäre Partitionen und logische Laufwerke auf unformatierten Partitionen oder Partitionen mit dem NTFS-Dateisystem verkleinern.

Abbildg. 5.9 Verkleinern eines Datenträgers unter Windows Server 2008



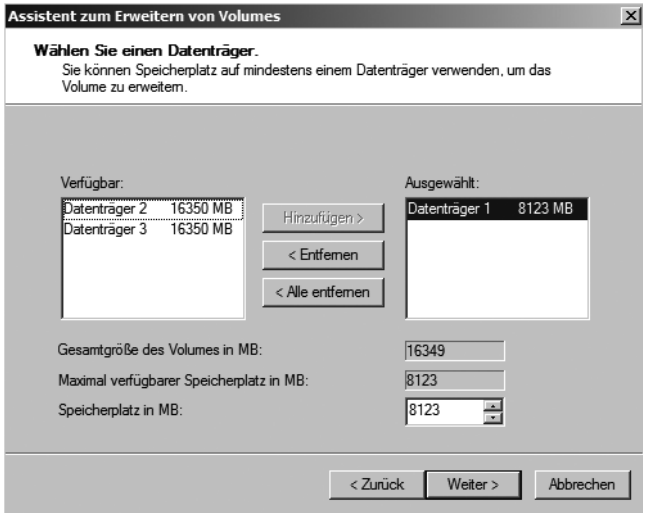
Erweitern von Partitionen

Vorhandenen primären Partitionen und logischen Laufwerken können Sie mehr Speicherplatz hinzufügen, indem Sie sie auf angrenzenden, verfügbaren Speicherplatz auf demselben Datenträger erweitern. Zum Erweitern eines Basisvolumes muss dieses unformatiert oder mit dem NTFS-Dateisystem formatiert sein. Sie können ein logisches Laufwerk innerhalb von zusammenhängendem freien Speicherplatz in der erweiterten Partition, die dieses Laufwerk enthält, erweitern. Wenn Sie ein logisches Laufwerk über den in der erweiterten Partition verfügbaren Speicherplatz erweitern, wird die erweiterte Partition zur Unterbringung des logischen Laufwerks vergrößert. Bei logischen Laufwerken, Start- oder Systemvolumes können Sie das Volume nur innerhalb von zusammenhängendem freiem Speicherplatz erweitern und nur dann, wenn der Datenträger zu einem dynamischen Datenträger aktualisiert werden kann. Bei anderen Volumes können Sie das Volume auch innerhalb von nicht zusammenhängendem Speicherplatz erweitern, werden aber aufgefordert, den Datenträger in einen dynamischen Datenträger zu konvertieren. Um ein Basisvolume zu erweitern, gehen Sie folgendermaßen vor:

1. Klicken Sie in der Datenträgerverwaltung mit der rechten Maustaste auf das Basisvolume, das Sie erweitern möchten.
2. Wählen Sie im Kontextmenü den Eintrag *Volume erweitern*.
3. Wenn die Partition zuvor mit dem NTFS-Dateisystem formatiert wurde, wird das Dateisystem automatisch so erweitert, dass die größere Partition belegt wird. Es gehen keine Daten verloren.

Es ist nicht möglich, die aktuellen System- oder Startpartitionen zu erweitern. Systempartitionen und Startpartitionen sind Namen für Partitionen oder Volumes auf einer Festplatte, die zum Starten von Windows verwendet werden.

Abbildg. 5.10 Auswählen des Datenträgers, mit dem Sie Ihren ausgewählten Datenträger erweitern können

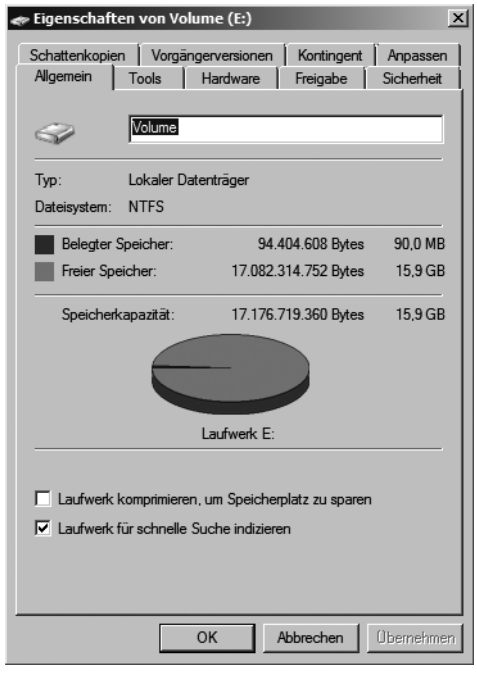


Die Systempartition enthält die hardwarebezogenen Dateien, die einem Computer mitteilen, von wo aus Windows gestartet werden kann. Eine Startpartition ist eine Partition, die die Windows-Betriebssystemdateien enthält, die sich im Windows-Dateiordner befinden. Im Allgemeinen handelt es sich bei der Systempartition und der Startpartition um die gleiche Partition, insbesondere wenn auf dem Computer nur ein Betriebssystem installiert ist. Wenn Sie einen Computer mit Multiboot-Konfiguration besitzen, verfügen Sie über mindestens zwei Startpartitionen. Mit einem weiteren Begriff, der *aktiven Partition*, wird beschrieben, welche Systempartition (und daher welches Betriebssystem) der Computer zum Starten verwendet. Wenn Sie den Computer einschalten, werden die auf der Systempartition verwendeten Informationen zum Starten des Computers verwendet. Auf einem Windows-basierten Computer ist nur eine Systempartition vorhanden, auch wenn auf dem Computer verschiedene Windows-Betriebssysteme installiert sind. Nicht-Windows-Betriebssysteme verwenden andere Systemdateien. Wenn auf einem Multiboot-Computer ein Nicht-Windows-Betriebssystem installiert ist, befinden sich die dazugehörigen Systemdateien auf einer eigenen Partition, getrennt von der Windows-Systempartition. Wenn Sie einen Multiboot-Computer besitzen, auf dem beispielsweise Windows Server 2008 und Windows Server 2003 installiert sind, dann ist jedes dieser Volumes eine Startpartition.

Verwalten von Datenträgern

Sie können erstellte Datenträger mit der rechten Maustaste anklicken und im Kontextmenü den Eintrag *Eigenschaften* wählen. Daraufhin stehen Ihnen verschiedene Registerkarten zur Verfügung (Abbildung 5.11): Auf der Registerkarte *Allgemein* sehen Sie den freien und belegten Speicher. Außerdem können Sie hier die Bezeichnung des Datenträgers festlegen. Sie können den gesamten Datenträger komprimieren, was allerdings aus Performancegründen nicht empfohlen werden kann. Auf dieser Registerkarte legen Sie auch fest, ob das Laufwerk für die Windows-Suche indexiert werden soll.

Abbildg. 5.11 Allgemeine Einstellungen für erstellte Datenträger



Auf der Registerkarte *Tools* stehen die Optionen *Fehlerüberprüfung* und *Defragmentierung* zur Verfügung. Hier können Sie außerdem den Datenträger mit der Windows-Sicherung auch sichern lassen. Die Defragmentierung adressiert ein Problem, das vor allem entsteht, wenn Dateien vergrößert, zusätzliche Dateien erstellt, oder vorhandene gelöscht werden. Die meisten Dateien werden in Form eines Extents nicht direkt in der MFT (Master File Table) gespeichert, sondern in einem oder mehreren zusätzlichen Blöcken, auf die aus der MFT verwiesen wird. NTFS versucht dabei, möglichst zusammenhängende Speicherblöcke zu wählen. Wenn eine Datei vergrößert wird, kann es vorkommen, dass am Ende des bisherigen Extents kein weiterer Speicherplatz mehr frei ist. Damit muss die Datei in mehreren Blöcken gespeichert werden, sie wird also fragmentiert. Durch die Fragmentierung werden wiederum Zugriffe auf Datenträger deutlich verlangsamt, denn nun sind mehr einzelne Zugriffe und Neupositionierungen des Schreib-/Lesekopfs der Festplatte erforderlich, um auf die Datei zuzugreifen. Eine regelmäßige Defragmentierung kann daher zu deutlichen Verbesserungen der Performance führen. Das Defragmentierungsprogramm von Windows Server 2008 ist zeitlich gesteuert, da die Defragmentierung relativ viel Rechenzeit benötigt und durch die logischerweise intensiven Zugriffe auf die Festplatte in diesem Bereich zu einer Beeinträchtigung der Performance führt. Sinn macht das nur, wenn viele Dateien oft in der Größe geändert oder gelöscht werden. Die Defragmentierung kann auch über *defrag* in einer Befehlszeile gestartet werden. Achten Sie aber darauf, diesen Befehl mit Administrator-Berechtigungen zu öffnen. Bei der Eingabe des Befehls werden alle Optionen angezeigt die möglich sind. Da die Defragmentierung in der Befehlszeile durchgeführt wird, kann diese auch sehr gut über Skripte gestartet werden. Der Befehl *defrag -c* defragmentiert alle Festplatten eines Server, *defrag <Laufwerksbuchstabe>* nur die angegebene Partition.

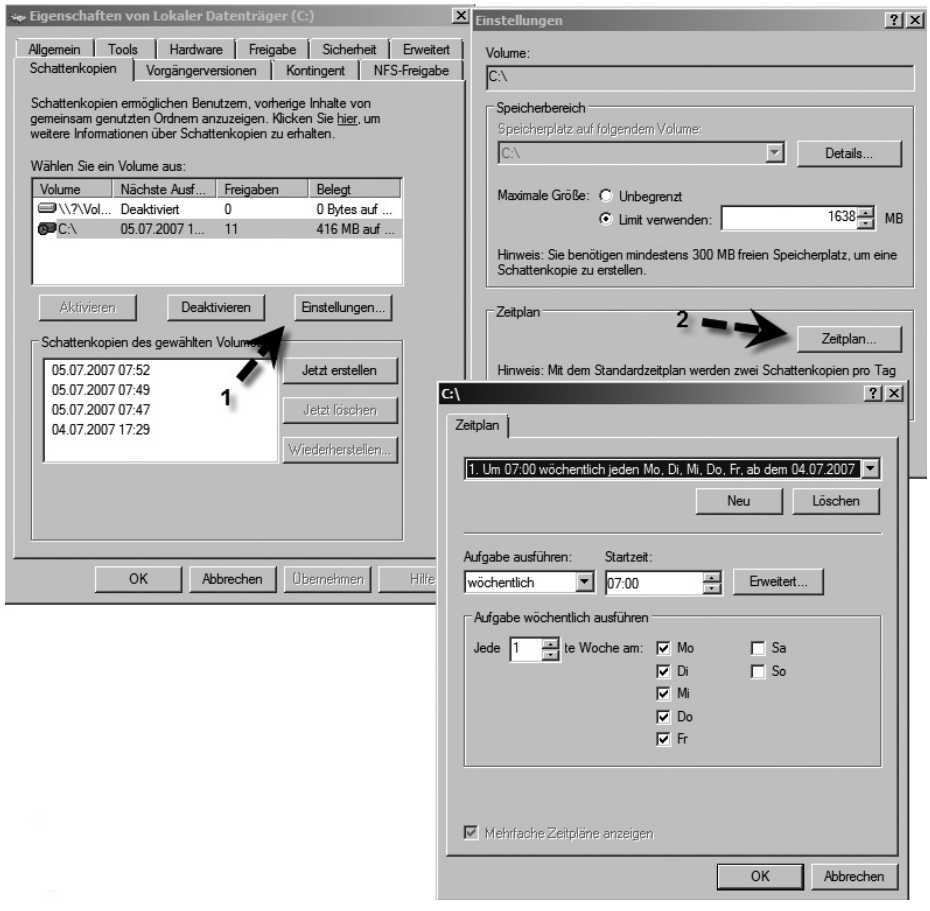
Verwenden von Schattenkopien

Eine wichtige Funktionalität zur Datensicherung von Windows Server 2008 sind die Schattenkopien. Die Idee ist, dass Änderungen auf einem Datenträger regelmäßig erfasst und gesichert werden. Auf diese Weise entstehen sozusagen *Schnappschüsse* des Systems zu unterschiedlichen Zeitpunkten. Damit lässt sich das System und einzelne Dateien wiederherstellen. Benutzer können wieder auf frühere Versionen von Dateien zurückgreifen, indem sie diese aus einer Schattenkopie wiederherstellen. Dafür gibt es einen speziellen Client, der auf Windows XP-Arbeitsstationen installiert werden muss, aber in Windows Vista bereits standardmäßig enthalten ist. Schattenkopien werden bei den Eigenschaften von Datenträgern auf der Registerkarte *Schattenkopien* konfiguriert (Abbildung 5.12). Sie können die Datenträger auswählen, für die Schattenkopien erzeugt werden sollen.

Abbildg. 5.12 Aktivieren von Schattenkopien für einen Datenträger

Konfigurieren Sie zunächst die Datenträger über die Schaltfläche *Einstellungen*, bevor Sie sie aktivieren. Bei der Nutzung von Schattenkopien müssen Sie berücksichtigen, dass dafür einiges an Speicherplatz erforderlich ist, da alle Änderungen gespeichert werden müssen. Wenn Sie zusätzliche Datenträger einbauen, müssen Sie die Schattenkopien zunächst manuell konfigurieren. Bei den Eigenschaften der Schattenkopien können Sie zudem ein Limit für den maximal dadurch belegten Platz auf dem Datenträger definieren. Darüber hinaus können Sie einen Zeitplan für die Erstellung von Schattenkopien erstellen. Sie können sie manuell jederzeit über die Schaltfläche *Jetzt erstellen* erzeugen. Der hauptsächliche Nutzen der Schattenkopien liegt darin, dass versehentlich gelöschte oder veränderte Dateien sehr schnell wiederhergestellt werden können.

Abbildg. 5.13 Konfigurieren der Schattenkopien



Wenn ein Benutzer den Administrator darüber informiert, dass eine Datei gelöscht oder fehlerhaft bearbeitet wurde, kann dieser mit wenigen Mausklicks ältere Versionen der Dateien wiederherstellen. Es muss kein Band in ein Laufwerk gelegt werden, es wird kein Sicherungsprogramm benötigt, sondern der Administrator, oder auch der Anwender selbst, braucht nur in den Eigenschaften des Verzeichnisses, in dem sich die besagte Datei befindet, eine ältere Version der Sicherung wiederherzustellen. Je nach Berechtigungsstruktur kann auch jeder Benutzer selbst seine Dateien wiederherstellen. In jedem Fall wird viel Zeit gespart und Nerven werden geschont. Die Schattenkopien belegen auch bei relativ großen Datenträgern nur eine begrenzte Menge an Speicherplatz. Bevor Sie Schattenkopien einführen, sollten Sie sich Gedanken über die folgenden Punkte machen:

- Schattenkopien werden immer für komplette Laufwerke erstellt. Komprimierte und verschlüsselte Dateien werden ebenfalls gesichert. Damit Sie Schattenkopien verwenden können, muss der Datenträger mit NTFS formatiert sein.
- Wenn Sie Schattenkopien für ein Laufwerk aktivieren, werden standardmäßig 10 % des Datenträgers reserviert (was Sie auf der Registerkarte *Einstellungen* ändern können). Wenn diese 10 % belegt sind, werden die ältesten Versionen der gesicherten Dateien automatisch überschrieben.

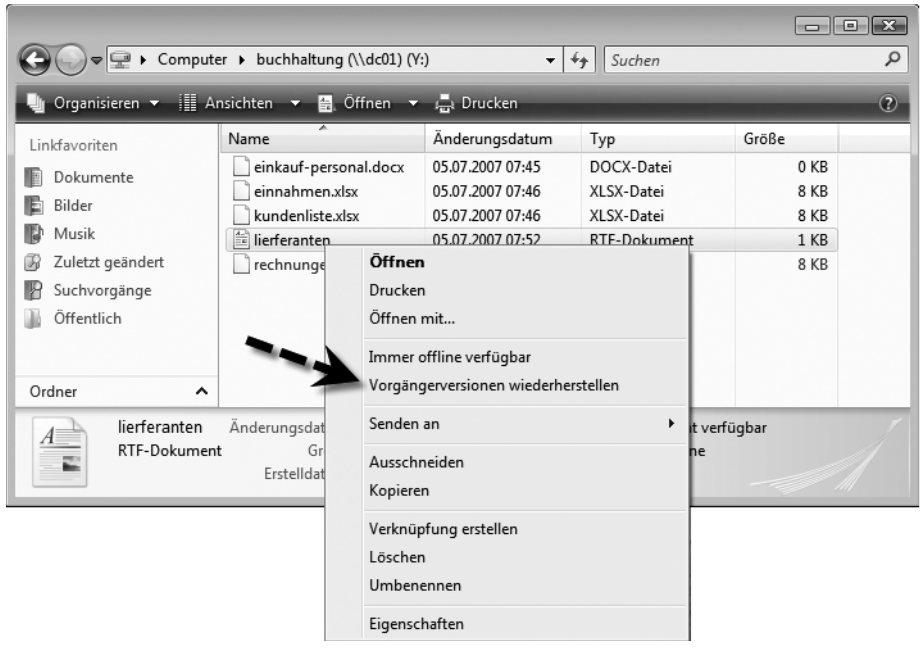
- Während einer Sicherung reagiert die entsprechende Platte aufgrund von Schreibvorgängen eventuell etwas langsamer.
- Passen Sie den Zeitplan für die Erstellung der Schattenkopien Ihren Bedürfnissen an. Standardmäßig erstellt Windows Server 2008 an jedem Wochentag (Montag bis Freitag) um 07:00 Uhr und um 12:00 Uhr eine Schattenkopie. Je öfter Schattenkopien erstellt werden, umso mehr Versionen der Dateien stehen folglich zur Verfügung und können von Ihren Benutzern oder Administratoren wiederhergestellt werden. Maximal können 64 Schattenkopien eines Datenträgers hergestellt werden. Mit steigender Anzahl von Schattenkopien steigt auch der Speicherplatzbedarf.

Damit auf die Schattenkopien zugegriffen werden kann, muss auf dem jeweiligen PC ein zusätzliches Programm, der Schattenkopie-Client, installiert werden. Nur Anwender, auf deren PCs der Schattenkopieclient installiert wurde, können auf Schattenkopien zurückgreifen, um Dateien wiederherstellen zu können. In Windows Vista ist dieser Client bereits standardmäßig installiert und aktiviert. Für Windows XP müssen Sie diesen herunterladen und installieren. Der Client wird auf der Seite http://www.microsoft.com/downloads/details.aspx?displaylang=de&familyid=e382358-f33c3-4de7-acd8-a33ac92d295e zur Verfügung gestellt.

Wiederherstellen von Dateien aus Schattenkopien

Um Schattenkopien wiederherstellen zu können, muss die entsprechende Freigabe, in der eine Wiederherstellung durchgeführt werden kann, als Netzlaufwerk verbunden sein. Innerhalb des Netzlaufwerkes kann der Anwender die Eigenschaften jeder beliebigen Datei oder jedes Verzeichnisses aufrufen und auf die Registerkarte *Vorherige Versionen* wechseln.

Abbildg. 5.14 Wiederherstellen einer Schattenkopie einer Datei



Diese Funktion steht auch über das Kontextmenü eines Verzeichnisses oder einer Datei zur Verfügung (Abbildung 5.14). Er kann im entsprechenden Fenster entweder die Datei oder das Verzeichnis zum ursprünglichen Zeitpunkt wiederherstellen und überschreibt dabei den aktuellen Stand, oder er kann Dateien oder das ganze Verzeichnis an einem anderen Ort wiederherstellen.

Abbildg. 5.15 Auswählen der älteren Version einer Datei für die Wiederherstellung

Verbindungspunkte in NTFS

Die meisten Anwendungen sind bereits standardmäßig kompatibel zu den neuen Verzeichnissen des Profils in Windows Server 2008. Meistens sind daher keinerlei Änderungen notwendig. In Windows Server 2008 wurde dazu die Unterstützung von älteren Dateipfaden integriert. Alle Pfade sind auch für ältere Anwendungen vollkommen transparent. Manche Anwendungen haben unter Umständen dennoch Probleme mit den neuen Verzeichnisstrukturen. Microsoft hat für die Unterstützung solcher Anwendungen auf dem Dateisystem *Verbindungspunkte* eingerichtet. Ein solcher Verbindungspunkt verweist ähnlich wie eine Verknüpfung auf einen anderen Pfad auf dem Server, in dem schließlich die gesuchten Daten liegen. Für alle notwendigen Systemverzeichnisse unter Windows Server 2003 hat Microsoft in Windows Server 2008 Verbindungspunkte eingerichtet.

Beispiel

Das Verzeichnis *C:\Users\<Benutzername>Documents* in Windows Server 2008 stellt das neue Verzeichnis für *C:\Dokumente und Einstellungen\<Benutzername>\Eigene Dateien* in Windows Server 2003 dar. Damit auch ältere Applikationen, die zum Beispiel Zugriff auf den Ordner *Eigene Dateien* haben müssen, weiterhin funktionieren, hat Microsoft einen Verbindungspunkt *Eigene Dateien* im Profil unter Windows Server 2008 eingerichtet. Solche Verbindungspunkte gibt es massenweise in

Windows Server 2003 an verschiedenen Stellen. Im Windows-Explorer werden diese durch einen Verknüpfungspfeil gekennzeichnet. Sie können sich in der Befehlszeile die Verbindungspunkte und deren Zielverzeichnisse anzeigen lassen. Wechseln Sie dazu in einer vorher geöffneten Eingabeaufforderung in das entsprechende Verzeichnis, und geben Sie den Befehl *dir /ad* ein. Sie erhalten eine Auflistung über den Inhalt des Verzeichnisses, und Verbindungspunkte werden als *Verbindung* angezeigt.

Auf der Registerkarte *Hardware* können Sie schließlich die zu Grunde liegende Hardware von Datenträgern konfigurieren und die Eigenschaften feststellen. An dieser Stelle werden Ihnen alle eingebauten Festplatten angezeigt. Wenn Sie eine der Festplatten markieren, können Sie über die Schaltfläche *Eigenschaften* weitere Einstellungen aufrufen. Diese Stelle ist der zentrale Bereich zur Verwaltung der Hardware, die den einzelnen Datenträgern zugeordnet ist. Nachdem Sie ein Laufwerk markiert und die Schaltfläche *Eigenschaften* anklickt haben, werden Ihnen mehrere Registerkarten angezeigt.

Auf der Registerkarte *Richtlinien* können Sie festlegen, dass der Schreibcache auf der Festplatte aktiviert sein soll. Dies hat den Vorteil, dass die Festplatte Daten als auf die Festplatte geschrieben ansieht, wenn Sie im Cache der Platte gespeichert sind. Wenn allerdings der Strom ausfällt, während die Daten noch vom Schreibcache auf die Festplatte geschrieben werden, sind die Daten im Cache verloren. Sie sollten daher nur in Ausnahmefällen die Option *Für Leistung optimieren* verwenden.

Befehlszeilen-Tools für die Verwaltung von Dateiservern

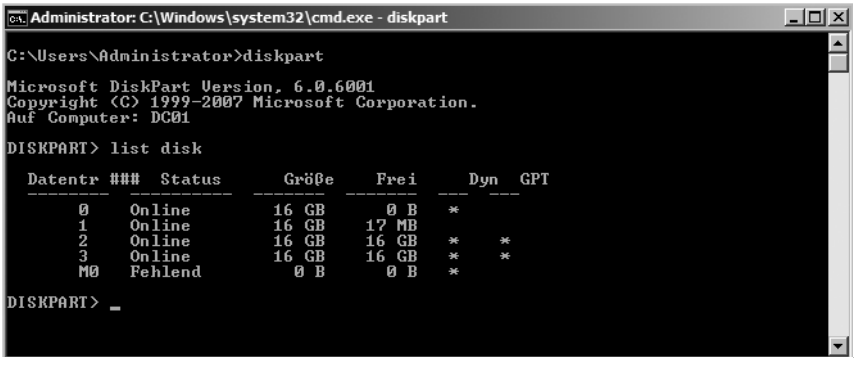
Sie können zwar fast alle Befehlszeilen-Tools auf Core-Servern auch auf herkömmlichen Servern ausführen, allerdings bieten sich hier die grafischen Tools an, da diese bequemer zu bedienen sind. Um einen Core-Server in einer grafischen Oberfläche zu bedienen, rufen Sie die Verwaltungskonsole *Computerverwaltung* auf und verbinden sich mit dem Core-Server. Achten Sie aber darauf, dass Sie in diesem Fall die Remoteverwaltung auf dem Core-Server erst aktivieren müssen (siehe Kapitel 3). Die wichtigsten Befehlszeilen-Tools finden Sie im folgenden Abschnitt. Windows Server 2008 besitzt eine verbesserte Infrastruktur für das Dateisystem. Eines der Schlüsselelemente dieser Infrastruktur ist der Dienst VDS (Virtual Disk Service), den Microsoft zur Vereinfachung des Laufwerks- und Datenmanagements entwickelt hat. In Verbindung mit VDS bietet Microsoft in Windows Server 2008 drei Werkzeuge für die Arbeit mit Laufwerken unterschiedlicher Hersteller: Die Befehlszeilenwerkzeuge *diskraid.exe* und *diskpart.exe* sowie das Snap-In für die Microsoft Management Console (MMC). Die Anwendung *diskpart.exe* kann für die Verwaltung von einzelnen Datenträgern und Aufgaben wie die Partitionierung eingesetzt werden. *Diskraid.exe* wird für die Konfiguration von RAID-Subsystemen benötigt. Mehr zu Diskpart finden Sie bei der Einrichtung von BitLocker in Kapitel 14.

Festplattenverwaltung in der Befehlszeile mit *DiskPart*

Mit dem Befehlszeilenprogramm *DiskPart* können Sie Partitionen auch in der Eingabeaufforderung verwalten. Mithilfe dieses Programms können Speichermedien (Datenträger, Partitionen oder Volumes) via Remotesitzung, Skripts oder Befehlszeile verwaltet werden. Es sollte nur von Experten verwendet werden, da die Möglichkeit einer Fehlkonfiguration und des dadurch eventuell entstehenden Systemausfalls oder Datenverlustes groß ist. Um Befehle mit DiskPart auszuführen, müssen die

entsprechenden Objekte vorher mit einem so genannten *Fokus* versehen werden. Dies bedeutet, ein gewünschtes Objekt muss vorher aufgelistet und ausgewählt werden. Ist das Objekt ausgewählt, werden alle eingegebenen Befehle darauf angewandt. Mithilfe der Befehle *list disk, list partition* und *list volume* werden verfügbare Objekte aufgelistet und die Nummer oder der Laufwerkbuchstaben des Objekts ermittelt. Die Befehle *list disk* und *list volume* zeigen alle Datenträger und Volumes auf dem Computer an, *list partition* jedoch nur Partitionen auf dem Datenträger, der den Fokus hat.

Abbildg. 5.16 Anzeigen und Verwalten der eingebauten Festplatten mit *diskpart.exe*



Ein Objekt wird anhand der Nummer oder des Laufwerkbuchstabens ausgewählt, zum Beispiel: Datenträger 0, Partition 1, Volume 3 oder Volume C. Haben Sie ein Objekt ausgewählt, verbleibt der Fokus darauf, bis ein anderes Objekt ausgewählt wird. Wenn der Fokus beispielsweise auf Datenträger 0 festgelegt ist und Sie Volume 1 auf Datenträger 1 auswählen, wechselt der Fokus von Datenträger 0 zu Datenträger 1, Volume 1. Wird eine neue Partition angelegt, wird der Fokus automatisch gewechselt. Sie können nur einer Partition auf dem ausgewählten Datenträger den Fokus geben. Verfügt eine Partition über den Fokus, besitzt das gegebenenfalls zugehörige Volume ebenfalls den Fokus. Verfügt ein Volume über den Fokus, verfügen der zugehörige Datenträger und die zugehörigen Partitionen ebenfalls über den Fokus, wenn das Volume einer bestimmten Partition zugeordnet ist.

Befehlssyntax von *DiskPart*

Über die Eingabe von *help* in der Befehlszeile werden Ihnen alle Optionen von DiskPart angezeigt. Im Knowledge Base-Artikel auf der Internetseite *http://support.microsoft.com/kb/300415/de* finden Sie eine ausführliche Anleitung für Windows XP, die auch für Windows Server 2008 gilt. Häufig werden vor allem die nachfolgenden Optionen verwendet:

- **assign** Weist einen Laufwerkbuchstaben zu. Gibt man keinen Laufwerkbuchstaben oder Bereitstellungspunkt an, wird der nächste verfügbare Laufwerkbuchstabe zugewiesen.
- **convert basic** Konvertiert einen leeren dynamischen Datenträger in einen Basisdatenträger
- **convert dynamic** Konvertiert einen Basisdatenträger in einen dynamischen Datenträger. Alle auf dem Datenträger vorhandenen Partitionen werden in einfache Volumes konvertiert.
- **create volume simple** Erstellt ein einfaches Volume. Nachdem Sie das Volume erstellt haben, wechselt der Fokus automatisch zum neuen Volume.

- **create volume stripe** Erstellt ein Stripeset mit mindestens zwei angegebenen dynamischen Datenträgern. Nachdem das Volume erstellt wurde, wird der Fokus automatisch an das neue Volume übergeben.
- **delete disk** Löscht einen fehlenden dynamischen Datenträger aus der Datenträgerliste
- **delete partition** Löscht auf einem Basisdatenträger die Partition, die über den Fokus verfügt. Es ist nicht möglich, die Systempartition, die Startpartition oder eine Partition zu löschen, die die aktive Auslagerungsdatei oder ein Absturzabbild (Speicherabbild) enthält.
- **delete volume** Löscht das ausgewählte Volume. Es ist nicht möglich, die System- oder die Startpartition oder ein Volume zu löschen, das die aktive Auslagerungsdatei oder ein Speicherabbild enthält.
- **detail disk** Zeigt die Eigenschaften des ausgewählten Datenträgers und der Volumes auf diesem Datenträger an
- **detail partition** Zeigt die Eigenschaften der ausgewählten Partition an
- **detail volume** Zeigt die Datenträger an, auf denen sich das aktuelle Volume befindet
- **exit** Beendet DiskPart
- **extend** Erweitert das Volume, das über den Fokus verfügt, auf den nachfolgenden, nicht reservierten Speicherplatz. Wenn die Partition zuvor mit dem NTFS-Dateisystem formatiert wurde, wird das Dateisystem automatisch erweitert, um die größere Partition zu belegen. Ein Datenverlust tritt nicht auf. Wenn die Partition zuvor mit einem anderen als dem NTFS-Dateisystem formatiert wurde, schlägt der Befehl fehl, und an der Partition wird keine Änderung vorgenommen. Es ist nicht möglich, die aktuellen System- oder Startpartitionen zu erweitern.
- **list disk** Zeigt eine Liste mit Datenträgern und Informationen zu den Datenträgern an
- **list partition** Zeigt die Partitionen an, die in der Partitionstabelle des aktuellen Datenträgers aufgelistet sind
- **list volume** Zeigt eine Liste der Basisvolumes und dynamischen Volumes auf allen Datenträgern an
- **remove** Entfernt einen Laufwerkbuchstaben oder einen Bereitstellungspunkt von dem Volume, das über den Fokus verfügt. Wurde kein Laufwerkbuchstabe oder Bereitstellungspunkt angegeben, entfernt DiskPart den ersten Laufwerkbuchstaben oder Bereitstellungspunkt, der gefunden wird. Mithilfe des Befehls *remove* können Sie den Laufwerkbuchstaben ändern, der einem austauschbaren Datenträger zugeordnet ist.
- **rescan** Sucht nach neuen Datenträgern, die eventuell zum Computer hinzugefügt wurden
- **select disk** Wählt den angegebenen Datenträger aus und verlagert den Fokus auf den Datenträger
- **select partition** Wählt die angegebene Partition aus und verlagert den Fokus auf die Partition. Wurde keine Partition angegeben, wird durch *select* die Partition aufgeführt, die momentan über den Fokus verfügt. Man kann die Partition anhand ihrer Nummer angeben. Mithilfe des Befehls *list partition* können Sie die Nummern aller Partitionen auf dem aktuellen Datenträger anzeigen. Bevor Sie eine Partition auswählen können, müssen Sie zuerst einen Datenträger mithilfe des Befehls *select disk* auswählen.

Bei Verwendung des Befehls *DiskPart* als Teil eines Skripts wird empfohlen, alle DiskPart-Vorgänge zusammen als Teil eines einzigen DiskPart-Skripts zu vervollständigen. Man kann aufeinander folgende DiskPart-Skripts ausführen, sollte aber zwischen den Skriptausführungen mindestens 15 Sekunden verstreichen lassen, bevor man den DiskPart-Befehl erneut ausführt, damit jedes Skript vollständig beendet wird. Andernfalls schlägt das nachfolgende Skript fehl. Zwischen den aufeinander folgenden DiskPart-Skripts lässt sich eine Pause einfügen, indem der Befehl *Sleep* (aus dem Windows Server 2003 Ressource Kit, welches kostenlos bei *www.microsoft.de* heruntergeladen werden kann) zur Batchdatei zusammen mit den DiskPart-Skripts hinzufügt wird. Um ein DiskPart-Skript aufzurufen, tippen Sie in der Eingabeaufforderung Folgendes ein: *diskpart /s <Skriptname.txt>*, wobei *Skriptname.txt* der Name der Textdatei ist, die das Skript enthält. Um die Skriptausgabe von DiskPart in eine Datei umzuleiten, tippen Sie in der Eingabeaufforderung Folgendes ein: *diskpart /s Skriptname.txt > Protokolldatei.txt*. Dabei ist *Protokolldatei.txt* der Name der Textdatei, in die die Ausgabe von DiskPart geschrieben wird. Wenn DiskPart gestartet wird, werden die DiskPart-Version und der Computername an der Eingabeaufforderung angezeigt. Wenn DiskPart beim Versuch, einen Skripttask auszuführen, einen Fehler ermittelt, beendet DiskPart die Verarbeitung des Skripts und zeigt einen Fehlercode an:

- **0** Es sind keine Fehler aufgetreten. Das gesamte Skript wurde ohne Fehler ausgeführt.
- **1** Es ist eine schwerwiegende Ausnahme aufgetreten. Möglicherweise liegt ein ernstes Problem vor.
- **2** Die für einen DiskPart-Befehl angegebenen Parameter waren falsch.
- **3** DiskPart konnte die angegebene Skript- oder Ausgabedatei nicht öffnen.
- **4** Einer der von DiskPart verwendeten Dienste hat einen Fehler zurückgegeben.
- **5** Es liegt ein Befehlssyntaxfehler vor. Das Skript ist fehlgeschlagen, da ein Objekt nicht ordnungsgemäß ausgewählt wurde oder nicht mit diesem Befehl verwendet werden kann.

Um die aktuelle Festplatten-Konfiguration Ihres PCs anzuzeigen, öffnen Sie zunächst mit *Start/Ausführen/cmd* eine Eingabeaufforderung. Geben Sie als Nächstes *diskpart* ein, um die Konsole für die Verwaltung von Partitionen aufzurufen. Mit dem Befehl *list disk* werden die eingebauten Festplatten angezeigt.

Erstellen von virtuellen Laufwerken mit *Subst.exe*

Auch unter Windows Server 2008 besteht die Möglichkeit, ein beliebiges Verzeichnis als virtuelles Laufwerk zu definieren. Dieses Laufwerk wird dargestellt wie alle anderen Laufwerke auch, verweist aber auf das Verzeichnis, das Sie konfiguriert haben. Diese Virtualisierung von Laufwerken wird mit dem Befehl *Subst.exe* in der Befehlszeile durchgeführt. Durch das Festlegen von Verzeichnissen als virtuelles Laufwerk können Sie sich so manche Klickorgie sparen, da verschachtelte und häufig verwendete Verzeichnisse als Laufwerk angezeigt werden. Wenn Sie in der Befehlszeile nur *subst* eingeben, werden Ihnen alle virtuellen Laufwerke angezeigt. Sie können beliebig viele virtuelle Laufwerke mit *subst.exe* erstellen. Die Syntax zur Erstellung eines virtuellen Laufwerks ist:

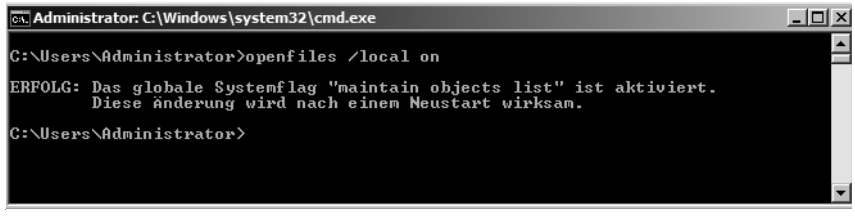
Subst <Laufwerksbuchstabe>: <Pfad zum Verzeichnis>

Wenn Sie zum Beispiel das Verzeichnis *c:\windows\system32* als virtuelles Laufwerk *X:* darstellen wollen, geben Sie in der Befehlszeile *subst x: c:\windows\system32* ein. Mit der Option *subst <Laufwerk>: /d* können Sie erstellte virtuelle Laufwerke auch wieder löschen lassen.

Anzeigen der geöffneten Dateien in der Befehlszeile – *Openfiles.exe*

Mit dem Befehlszeilenprogramm *Openfiles.exe* können Administratoren Dateien und Ordner, die auf einem System geöffnet wurden, auflisten bzw. trennen. Vor jedem Dateinamen sehen Sie eine ID und den Namen des jeweiligen Benutzers. Greifen mehrere Benutzer gleichzeitig auf eine Datei zu, zeigt Openfiles diese Datei unter zwei unterschiedlichen ID-Kennungen entsprechend zwei Mal an. Damit geöffnete Dateien angezeigt werden, müssen Sie zunächst das Systemflag *maintain objects list* aktivieren. Mit dem Befehl *openfiles /local on* wird das Systemflag eingeschaltet. Der Befehl *openfiles /local off* schaltet ihn aus.

Abbildg. 5.17 Aktivieren des Systemflags *maintain object list*



Erst nach der Aktivierung dieses Flags werden mit *Openfiles.exe* geöffnete Dateien angezeigt. Nachdem Sie das Flag gesetzt haben, müssen Sie den Server neu starten. Wenn Sie nach dem Neustart in der Befehlszeile *openfiles* eingeben, werden die geöffneten Dateien angezeigt. Möchten Sie feststellen, welche Dateien auf einem Datenträger geöffnet sind, empfiehlt sich der Befehl *openfiles | find /i "z:"*, wobei *z:* der Laufwerks-Buchstabe des Laufwerks ist. Wenn Sie noch offene Dateien auf Ihrem System vorfinden und diese schließen möchten, verwenden, Sie den Befehl *openfiles /disconnect /id <id>* oder *openfiles /disconnect /a <Benutzer>*. Als *<id>* wird die von *Openfiles* mitgeteilte ID eingetragen, als *<Benutzer>* die mitgeteilte Nutzerkennung.

Weitere Befehlszeilen-Tools für die Datenträgerverwaltung

Neben den bereits beschriebenen Möglichkeiten, werden für die Verwaltung von Datenträgern über die Befehlszeile weitere Tools zur Verfügung gestellt. Sie erhalten in der Befehlszeile zu jedem Tool eine ausführliche Hilfe.

- **Diskraid** Verwalten von RAID-Systemen
- **Defrag** Datenträger defragmentieren
- **Convert <Laufwerksbuchstaben> /FS:NTFS** Datenträger von FAT zu NTFS formatieren
- **Vssadmin** Verwalten der Schattenkopien
- **Fsutil** Verwalten des Dateisystems
- **Sigverif** Verifizieren der Signatur einer Datei
- **Icacls** Besitz eines Verzeichnisses übernehmen

Sysinternals – Tools für die Verwaltung von Dateien und Datenträgern

Microsoft hat im Jahr 2006 den bekannten Softwarehersteller und Windows-Spezialisten Sysinternals übernommen und dessen meist kostenlose und sehr mächtige Tools in das Microsoft TechNet übernommen. Sie finden alle Tools auf der TechNet-Internetseite. Die meisten Tools müssen nicht installiert werden, sondern können nach dem Entpacken sofort verwendet werden. Der Charme dieser Tools liegt darin, dass meistens auch keine DLL-Dateien benötigt werden. Die Tools bestehen fast immer nur aus einer einzelnen **.exe*-Datei und können nach dem Entpacken sofort gestartet werden. Bei manchen Tools handelt es sich um Tools mit grafischer Oberfläche, manche sind Befehlszeilen-Tools. Alle Tools haben gemeinsam, dass sie nur wenige Kilobyte groß sind, aber extrem hilfreich sein können, vor allem wenn es um die Fehlersuche in Windows-Netzwerken geht. Im Forum für Sysinternals finden Sie noch viele Anregungen und Tipps sowie Hilfen zu den Tools. Microsoft hat die komplette Tool-Sammlung von Sysinternals in einer einzigen Datei zum Download bereitgestellt. So können Sie sich das lästige Herunterladen der einzelnen Programme sparen. Zu den Tools gehören etwa *Autoruns*, *Diskmon, Filemon, Portmon, Regmon* und der *Process Explorer*, mit denen sich die Aktivitäten eines Rechners und der darauf laufenden Anwendungen sehr gut beobachten lassen. Auch der *RootkitRevealer* zum Aufspüren von Rootkits gehört zu der Sammlung.

HINWEIS Auf den folgenden Internetseiten erhalten Sie ausführliche Informationen zu den Tools:

- http://www.microsoft.com/technet/sysinternals
- http://forum.sysinternals.com
- http://www.microsoft.com/technet/sysinternals/utilities/sysinternalssuite.mspx
- http://www.ryanvm.net/forum/viewtopic.php?t=1735

Verwalten und Überwachen von Berechtigungen auf Datei- oder Verzeichnisebene

Mit *AccessChk* wird in der Befehlszeile eine ausführliche Liste ausgegeben, welche Rechte ein Benutzer auf Dateien, Dienste oder die Registry hat. Mit dem Tool kann schnell ein Überblick erlangt werden, wie bestimmte Zugriffsrechte für einzelne Benutzer aussehen. Die Syntax lautet:

accesschk [-s][-i|-e][-r][-w][-n][-v][[-k][-c]|[-d]] <Benutzername> <Datei, Verzeichnis, Registrykey oder Dienst>

-c Diese Option wird verwendet, wenn es sich um einen Dienst handelt. Wird der Platzhalter * verwendet, werden die Rechte für alle Systemdienste angezeigt.

-d Verarbeitet nur Verzeichnisse

-k Diese Option wird verwendet, wenn es sich um einen Registrykey handelt, zum Beispiel *HKLM\SOFTWARE*.

-n Zeigt nur Objekte an, für die kein Zugriff besteht

-r Zeigt nur Leserechte an

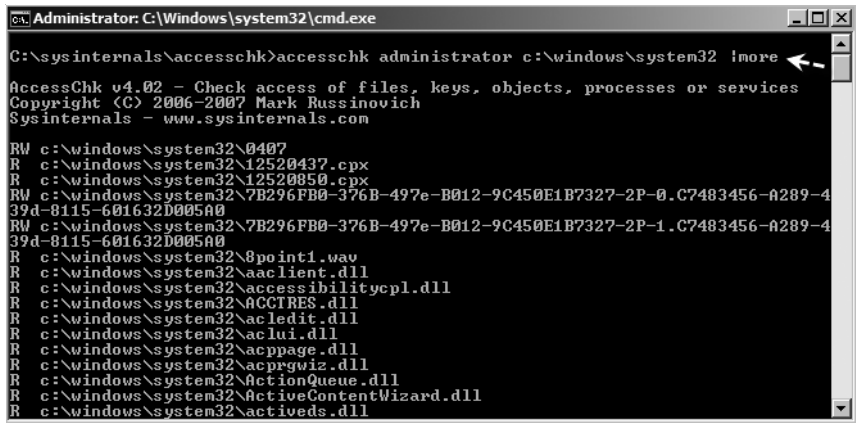
-w Zeigt nur Schreibrechte an

Wird ein Benutzer oder eine Gruppe ausgewählt, werden die effektiven Rechte für diesen Account angezeigt.

Beispiele

Sollen die Rechte des Benutzers *Administrator* für ein Verzeichnis angezeigt werden, wird der Befehl *accesschk administrator c:\windows\system32* verwendet. Bei jeder Datei erhalten Sie die Information, ob Leserechte (R), Schreibrechte (W) oder beides (RW) bestehen.

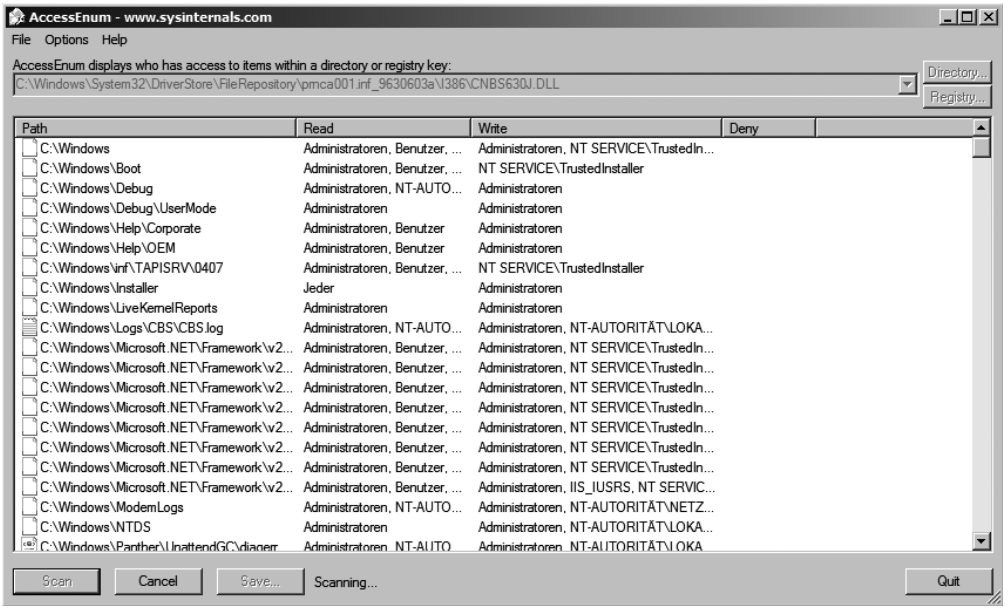
Abbildg. 5.18 Mit *AccessChk* von Sysinternals kann unter Windows Server 2008 die Berechtigungsstruktur eines Verzeichnisses angezeigt werden



Mit dem Befehl *accesschk <Benutzer> –cw ** wird angezeigt, auf welche Windows-Dienste die Benutzergruppe oder der Benutzer Schreibrechte hat. Sollen die Zugriffsberechtigungen für einen Benutzer für einen bestimmten Registrykey abgeprüft werden, wird beispielsweise der Befehl *accesschk –kns contoso\tami hklm\software* verwendet. Das Tool eignet sich daher hervorragend um Server auf Sicherheitsschwachstellen zu untersuchen, auch innerhalb von Skripts. Mit der Option *|more* kann die Ausgabe aufgeteilt werden, über *>Datei.txt* wird die Ausgabe in eine Datei umgeleitet.

AccessEnum bietet eine grafische Oberfläche, mit der für eine komplette Verzeichnisstruktur die Berechtigungen eines Benutzers angezeigt werden. Bei *AccessEnum* handelt es sich um die grafische Oberfläche von *AccessChk*. Der Download enthält beide Dateien, da *AccessEnum* das Programm *AccessChk* zum Abprüfen der Berechtigungen nutzt. Die Bedienung ist sehr einfach und ideal für das Aufdecken von Sicherheitslücken auf Grund mangelhaft gesetzter Berechtigungen. Sie können sich in der Oberfläche ein Verzeichnis aussuchen und dieses auf Berechtigungen scannen lassen. Hier werden auch Verweigerungsrechte angezeigt.

Abbildg. 5.19 *AccessEnum* zeigt in einer grafischen Oberfläche die Berechtigungsstruktur für einzelne Verzeichnisse an



Der Verzeichnisname wird in der Spalte *Path* angezeigt, während der Eintrag für das Anwenderkonto in der Spalte *Read* zu finden ist. Ein Anwender, der beispielsweise die Schreibrechte auf das Verzeichnis *Windows\System32* und alle darunter liegenden Verzeichnisse besitzt, aber über kein Schreibrecht auf das Verzeichnis *Windows* verfügt, wird mit dem Eintrag *Windows\Systems32* und dem Namen des Kontos in der Spalte *Write* dargestellt. Auf diese Art und Weise der verdichteten Darstellung wird erreicht, dass Konten im Zusammenhang mit der entsprechenden Gruppenzugehörigkeit dargestellt werden. Besitzt beispielsweise eine Gruppe den Lesezugriff auf ein Verzeichnis, während sie aber dieses Leserecht auf das übergeordnete Verzeichnis nicht hat, werden eines oder mehrere Gruppenmitglieder, auf die genau diese Konstellation zutrifft, nicht separat in der Read-Spalte dargestellt. Hier wird nur die entsprechende Gruppe auftauchen. Das Menü stellt zwei Einstellmöglichkeiten zur Verfügung. Die erste Option mit der Bezeichnung *Show Local System Account* ist standardmäßig ausgewählt. Wird diese Option deaktiviert, ignoriert das Tool die Zugriffsrechte, die sich auf den lokalen System-Account (NT-AutoritätSystem) beziehen. Dieses Konto wird nur von den Windows-Diensten und den Kernkomponenten des Betriebssystems verwendet. Die zweite Option die hier zur Verfügung gestellt wird, trägt die Bezeichnung *File Display Options*. Durch Auswahl dieser Option wird es möglich, dass Dateien und Verzeichnisse so behandelt werden, dass eine Datei grundsätzlich immer dann angezeigt wird, wenn die Zugriffsrechte von denen des übergeordneten Verzeichnisses abweichen. Mit einem Klick auf die Spaltenüberschriften können die Einträge auf- oder absteigend sortiert werden. Über die Schaltfläche *Registry* wird innerhalb der Registry nach Berechtigungen gescannt.

ShareEnum – Die Netzwerkversion von AccessEnum

ShareEnum ist ein ähnliches Tool wie AccessEnum und hat die Funktion, alle Freigaben und deren Sicherheitseinstellungen anzuzeigen. Auf diese Weise können alle Freigaben eines Servers auf einen Blick angezeigt werden. Das Tool kann entweder einen IP-Bereich oder alle PCs und Server einer

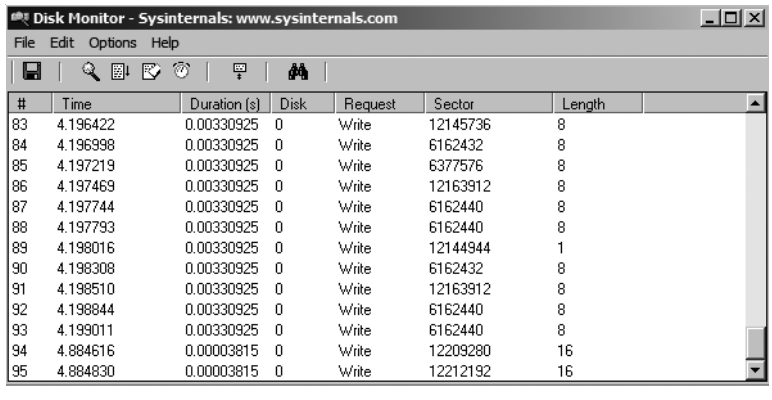
Domäne (oder aller Domänen) auf Freigaben scannen. Damit das Tool auch zuverlässig alle Informationen anzeigt, sollte die Anmeldung mit Domänenadmin-Konto erfolgen, da nur dieses Konto Rechte auf allen PCs und Servern der Domäne hat. Das Tool zeigt nicht nur die Freigaben an, sondern auch den lokalen Pfad der Freigabe auf dem Server. Über die Schaltfläche *Refresh* wird ein neuer Scanvorgang gestartet. Soll nur ein einzelner Server gescannt werden, geben Sie als IP-Bereich als Start- und Endadresse die gleiche IP-Adresse an. Mit dem Tool werden in einem einzelnen Fenster alle Freigaben im Netzwerk mit den entsprechenden Zugriffsberechtigungen angezeigt. In Verbindung mit AccessChk und AccessEnum, ist ShareEnum daher eine wertvolle Ergänzung für die Tool-Sammlung jedes Administrators.

Datenträger- und Partitionsverwaltung

Vor allem auf Servern auf denen viele Partitionen eingerichtet wurden, die sich über mehrere physische Festplatten erstrecken, kann *Diskext.exe* extrem hilfreich sein. Das Tool zeigt an, über welche Festplatten sich eine Partition erstreckt und wo auf der Festplatte die Partition angelegt worden ist. Bei dem Tool handelt es sich um ein einfaches Befehlszeilentool. Die Ausgabe kann zum Beispiel in eine Textdatei umgeleitet werden, wenn bei der Einrichtung eines Servers eine Dokumentation der Konfiguration erstellt wird.

Mit *Diskmon* werden alle Aktivitäten der Festplatte in einem Fenster angezeigt. Es werden detaillierte Informationen über die Nutzung der Festplatten im Server angezeigt. In einem Ausgabefenster werden dabei Aktion, Sektor, Zeit, Dauer und Festplatte angegeben. Zu Diagnosezwecken kann dieses Tool sehr nützlich sein, da schnell erkannt wird, welche Abläufe auf den Platten durchgeführt werden. Neben der Echtzeitanzeige der Festplattenkapazität, bei der mit verschiedenen Optionen und Filtern gearbeitet wird, besteht auch die Möglichkeit, das Programm in die Taskleiste zu minimieren und es an dieser Stelle als Festplattenaktivitäts-LED verwenden. Aktivieren Sie für diese Funktion über *Options* die Funktion *Minimize to Tray Disk Light*. Wird das Programm minimiert, wird neben der Uhr ein kleines Symbol angezeigt, welches die Aktivität der Festplatte anzeigt, wie die Leuchte der Festplatte direkt am Server. Wenn in einen Serverschrank viele Server eingebaut sind, von denen man oft auch die Lampen der Festplattennutzung nicht sieht, kann mit diesem Tool schnell erkannt werden, ob und wie stark aktuell auf die Festplatte des Servers zugegriffen wird.

Abbildg. 5.20 Anzeigen der Festplattenkapazität eines Servers mit *Disk Monitor* von Sysinternals



#	Time	Duration (s)	Disk	Request	Sector	Length
83	4.196422	0.00330925	0	Write	12145736	8
84	4.196998	0.00330925	0	Write	6162432	8
85	4.197219	0.00330925	0	Write	6377576	8
86	4.197469	0.00330925	0	Write	12163912	8
87	4.197744	0.00330925	0	Write	6162440	8
88	4.197793	0.00330925	0	Write	6162440	8
89	4.198016	0.00330925	0	Write	12144944	1
90	4.198308	0.00330925	0	Write	6162432	8
91	4.198510	0.00330925	0	Write	12163912	8
92	4.198844	0.00330925	0	Write	6162440	8
93	4.199011	0.00330925	0	Write	6162440	8
94	4.884616	0.00003815	0	Write	12209280	16
95	4.884830	0.00003815	0	Write	12212192	16

Dateien automatisiert ersetzen und löschen

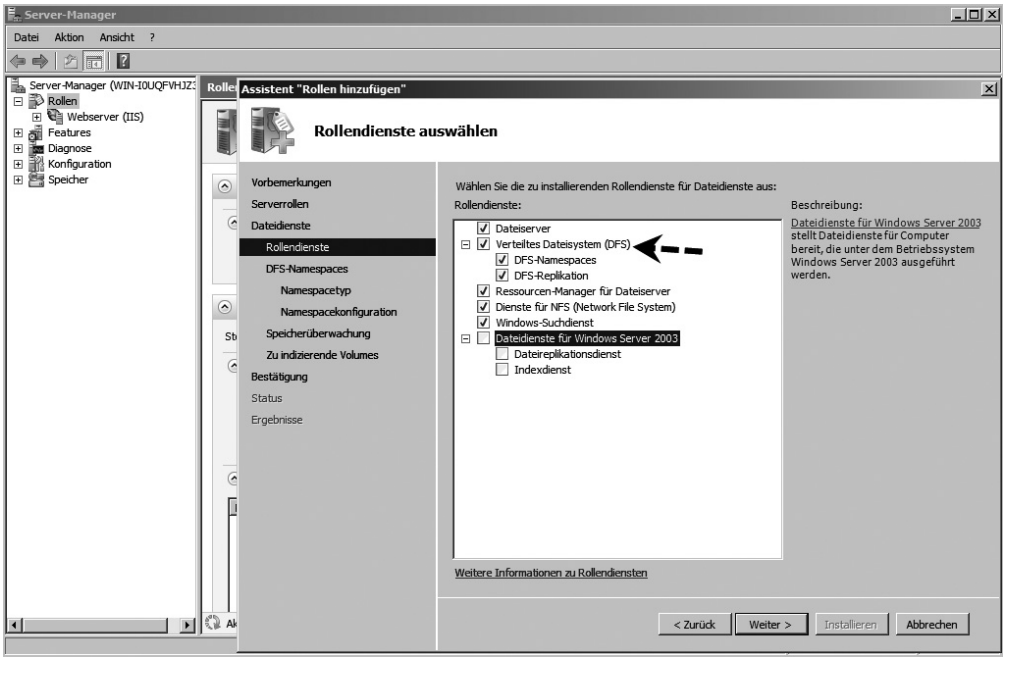
Mit *PendMoves* und *MoveFile* können Sie konfigurieren, dass bestimmte Dateien beim nächsten Neustart ersetzt oder gelöscht werden sollen. Vor allem wenn Dateien, die aktuell im Zugriff sind, ausgetauscht werden müssen, aber der Server nicht neu gestartet werden kann, kann dadurch der Austausch auf die Abendstunden gelegt werden. Diese Aktionen werden vom *Microsoft Session Manager* durchgeführt. Dazu werden die einzelnen Maßnahmen und Konfigurationen aus dem Registryschlüssel *HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations* ausgelesen.

Mit *PendMoves* wird angezeigt, welche Dateien beim nächsten Neustart gelöscht oder verschoben werden sollen. Mit dem zweiten Tool, *MoveFile*, wird ein solcher Vorgang konfiguriert. Die Syntax dazu lautet: *movefile <Quelle> <Ziel>*. Wird als Ziel "" eingeben, wird die Datei gelöscht.

Verteiltes Dateisystem (DFS)

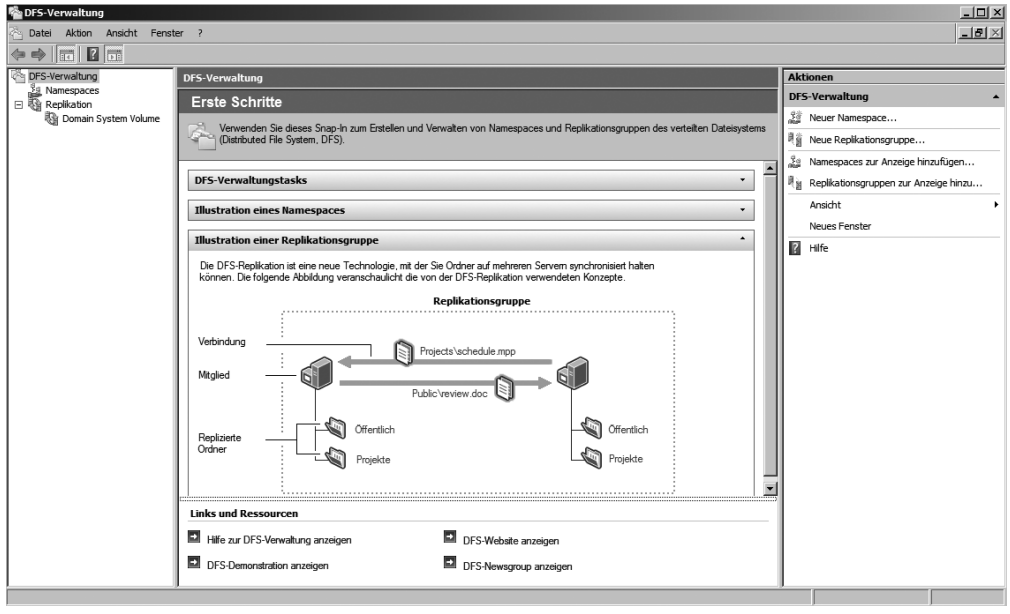
Auch im verteilten Dateisystem (Distributed File System, DFS) hat Microsoft einige Neuerungen eingeführt. Sie können aber ohne weiteres eine gemischte Windows Server 2003/2008-Umgebung betreiben, wenn Sie ein DFS einsetzen. Um auf Windows Server 2008 DFS einzusetzen, müssen Sie zunächst die Rolle *Dateiserver* installieren. DFS wird als zusätzlicher Rollendienst hinzugefügt (siehe Abbildung 5.21 und Kapitel 6).

Abbildg. 5.21 Installation von DFS unter Windows Server 2008



Der generelle Umgang mit DFS ist unter Windows Server 2008 ähnlich zu Windows Server 2003. Nur die Verwaltungsoberfläche hat sich geändert. Die Verwaltung von DFS unter Windows Server 2008 findet ebenfalls über den Server-Manager statt. Hier steht nach der Installation der verschiedenen DFS-Rollendienste der neue Menüpunkt zur Verwaltung von DFS zur Verfügung.

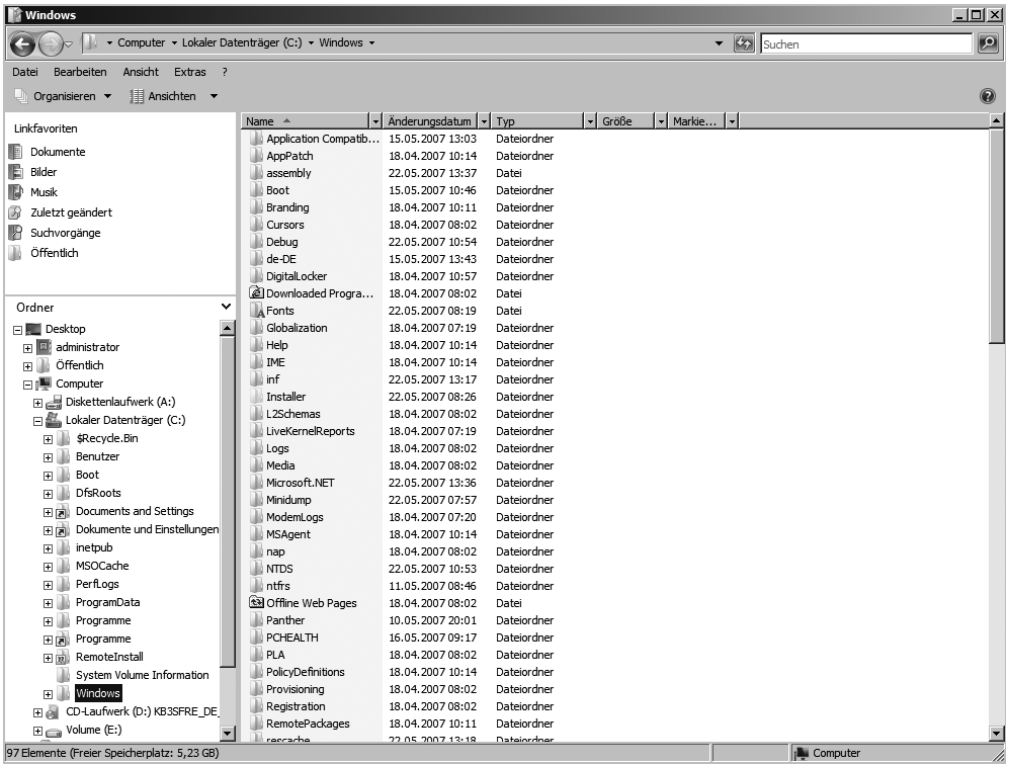
Abbildg. 5.22 Die neue Verwaltungsoberfläche für DFS unter Windows Server 2008



Der neue Windows-Explorer und die neue Windows-Suche

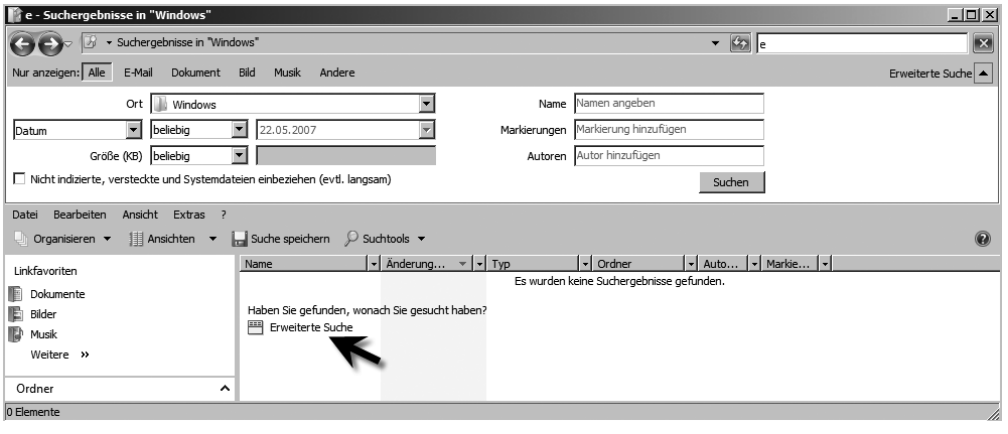
Der Windows-Explorer ist noch immer die Schaltzentrale von Windows zur Navigation innerhalb von Verzeichnissen und der Verwaltung von Dateien. Microsoft hat gerade innerhalb des Explorers einige Änderungen vorgenommen, die auch bei der Verwaltung eines Dateiservers eine Rolle spielen. Oben links im Windows-Explorer-Fenster wird eine Vor- und Zurückschaltfläche eingeblendet (Abbildung 5.23). Mit diesen kann zum vorher geöffneten Verzeichnis zurückgewechselt werden. Diese Funktion wurde vom Internet Explorer übernommen und erleichtert deutlich die Navigation. Die Adressleiste zeigt den genauen Standort des derzeitig geöffneten Verzeichnisses an. Sie können entweder direkt auf einen übergeordneten Ordner klicken, um diesen zu öffnen, oder über das kleine Symbol neben jedem Ordner dessen Unterordner anzeigen und zu diesem navigieren. Klicken Sie auf den ersten Pfeil in der Adressleiste, werden Ihnen einige Standardordner des Betriebssystems angezeigt. Klicken Sie mit der rechten Maustaste auf die Adressleiste, können Sie den derzeitigen Pfad in die Zwischenablage kopieren und in einem anderen Programm wieder einfügen. Mit einem Klick auf den leeren Bereich der Adressleiste wechselt die Ansicht in ein Eingabefeld und Sie können den Pfad manuell eintragen, der im Explorer angezeigt werden soll. Wie beim Internet Explorer kann auch beim Windows-Explorer die Ansicht durch F5 oder per Klick auf die *Aktualisieren*-Schaltfläche neben der Adressleiste aktualisiert werden.

Abbildg. 5.23 Der neue Windows-Explorer in Windows Server 2008



Durch die Einblendung der erweiterten Suche wird im Anschluss auch das Suchfenster eingeblendet. Die erweiterte Suche kann nur verwendet werden, wenn der Systemdienst *Windows-Suche* gestartet ist. Erst dann wird der Inhalt der einzelnen Dateien indexiert und in der Suche angegeben.

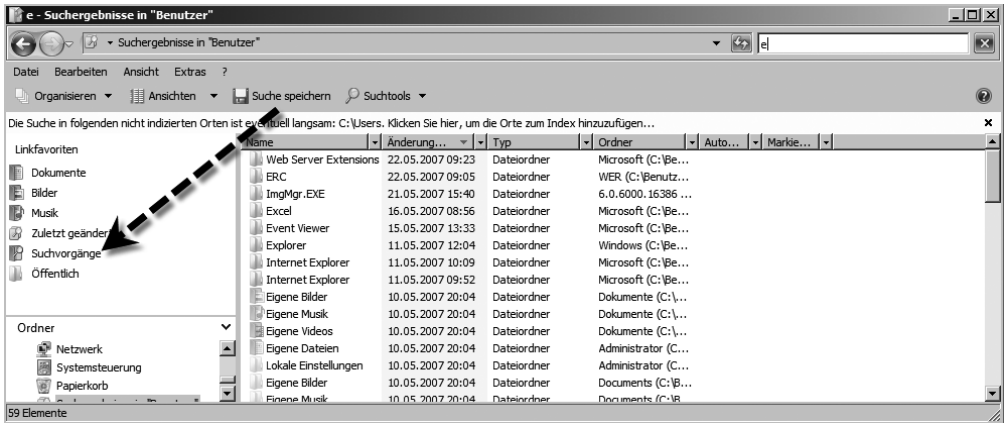
Abbildg. 5.24 Erweiterte Suche in Windows Server 2008



Ebenfalls neu im Windows-Explorer ist der Bereich *Linkfavoriten* auf der linken Seite. Hier werden automatisch die Verzeichnisse angezeigt, die am häufigsten verwendet werden. Diese Liste wird automatisch und dynamisch aufgebaut und zeigt Ihnen auf einen Blick die Ordner an, zu denen Sie am häufigsten navigiert sind. Sie können den Inhalt in dieser Ansicht selbst definieren. Wenn Sie einzelne Linkfavoriten nicht verwenden wollen, können Sie mit der rechten Maustaste in den Bereich der Linkfavoriten klicken und im Kontextmenü den Eintrag *Link entfernen* auswählen. Die Möglichkeit, unnötige Linkfavoriten aus der Ansicht zu entfernen, wird allerdings nur dann richtig sinnvoll, wenn Sie auch selbst bestimmen können, welche Linkfavoriten angezeigt werden. Sie können eigene Ordner bestimmen, die in den Linkfavoriten angezeigt werden. Sobald Sie im Explorer auf einen solchen Linkfavoriten klicken, wechseln Sie sofort zu diesem Ordner, wodurch die Navigation enorm vereinfacht wird. Um einen Linkfavoriten zu erstellen, navigieren Sie zunächst zu dem Ordner den Sie als Linkfavorit festlegen wollen. Im Anschluss klicken Sie auf den Ordner mit der linken Maustaste und ziehen diesen in den Bereich der Linkfavoriten. Auch der Navigationsbereich unterhalb der Linkfavoriten wurde von Microsoft überarbeitet. Dieser kann jetzt im Windows-Explorer über das kleine Pfeilsymbol ein- und ausgeblendet werden. Wenn Sie auf das kleine Dreieck neben einem Ordner einmal mit der linken Maustaste klicken, werden die Unterverzeichnisse angezeigt.

Die neue Suchleiste von Windows Server 2008 ist allgegenwärtig. Sowohl im Startmenü als auch in jedem Explorer-Fenster wird die Suche angezeigt. Suchen Sie nach einem Programm, einer Website im Verlauf des Browsers oder einer Datei, die im persönlichen Ordner gespeichert ist, sollten Sie das Feld *Suchen* unten im Startmenü verwenden. Müssen Sie eine Suche mit mehreren Filtern definieren, können Sie die erstellte Suche speichern, sodass Sie in Zukunft nur einen einzigen Klick benötigen, um dieselbe Menge an Dateien erneut zu suchen (Abbildung 5.25).

Abbildg. 5.25 Speichern von Suchvorgängen



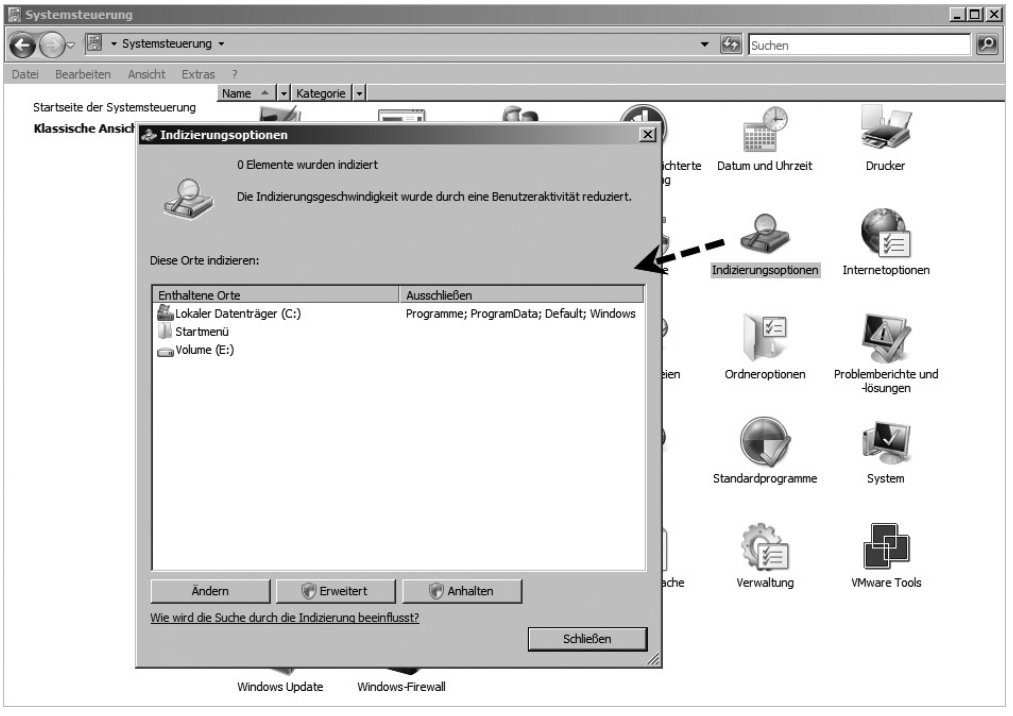
Das Feld *Suchen* befindet sich oben rechts in jedem Ordner. Es filtert die aktuelle Ansicht auf der Grundlage des von Ihnen eingegebenen Texts. Mit dem Feld *Suchen* können Sie Dateien anhand von Text im Dateinamen, von Text innerhalb der Datei, von Markierungen und von anderen gängigen Dateieigenschaften suchen, die Sie an die Datei angefügt haben. Darüber hinaus schließt die Suche den aktuellen Ordner und alle Unterordner ein. Über den Link *Erweiterte Suche* können Sie die Sucheigenschaften noch genauer spezifizieren. Wenn Sie beispielsweise eine Datei mit dem Titel *Einkaufskonditionen 2007* erstellt haben, werden, sobald Sie »Eink« in das Feld *Suchen* eingeben, die

meisten Dateien im Ordner nicht mehr angezeigt, sondern nur die dazu passenden. Wenn Sie beispielsweise die Datei *Rechnung November.xls* suchen, können Sie »Nov« oder »Rech« eingeben.

Indizierung verwenden

Mithilfe des Index kann die Suche nach Dateien erheblich beschleunigt werden. Anstatt die gesamte Festplatte nach einem Dateinamen oder einer Dateieigenschaft durchsuchen zu müssen, muss Windows lediglich den Index überprüfen, sodass das Ergebnis in einem Bruchteil der Zeit verfügbar ist, die für eine Suche ohne Index benötigt würde. Zu den indizierten Speicherorten gehören alle Dateien in Ihrem persönlichen Ordner (z.B. Dokumente, Bilder, Musik und Videos) sowie E-Mail- und Offlinedateien. Zu den nicht indizierten Dateien zählen Programm- und Systemdateien. Die Konfiguration des Index in Windows Server 2008 finden Sie über *Start/Systemsteuerung/Indizierungsoptionen* (Abbildung 5.26). Von dieser Indexierung profitieren auch die Windows Vista-Arbeitsstationen.

Abbildg. 5.26 Indizierungsoptionen in Windows Server 2008



1. Klicken Sie auf *Ändern*.
2. Zum Hinzufügen eines Speicherorts müssen Sie das jeweilige Kontrollkästchen in der Liste *Ausgewählte Orte ändern* aktivieren und dann auf *OK* klicken. Klicken Sie auf *Alle Orte anzeigen*, wenn Ihnen nicht alle Speicherorte auf Ihrem Computer in der Liste *Ausgewählte Orte ändern* angezeigt werden.

3. Wenn Sie einen Ordner, jedoch nicht seine Unterordner, in den Index einschließen möchten, müssen Sie den Ordner erweitern und dann die Kontrollkästchen sämtlicher Ordner deaktivieren, die Sie nicht indizieren möchten. Diese Ordner werden in der Spalte *Ausschließen* angezeigt.
4. Über die Schaltfläche *Erweitert* können Sie zum Beispiel den Speicherort des Index festlegen, den Index neu erstellen lassen oder die Standardeinstellungen wiederherstellen.

Zusammenfassung

Im Vergleich zu Windows Server 2003 hat sich bei der Datenträgerverwaltung des Dateisystems wenig verändert. Neuerungen wie das Verkleinern oder Vergrößern von Partitionen sind kleine, aber wertvolle Möglichkeiten, mit den wachsenden Datenmengen im Unternehmen zurechtzukommen. Wir haben Ihnen in diesem Kapitel die verschiedenen Fachbegriffe, deren Bedeutung, aber auch den Umgang damit in der Praxis gezeigt. Im nächsten Kapitel gehen wir darauf ein, wie Sie Daten im Netzwerk zur Verfügung stellen können und Windows Server 2008 als Dateiserver betreiben.

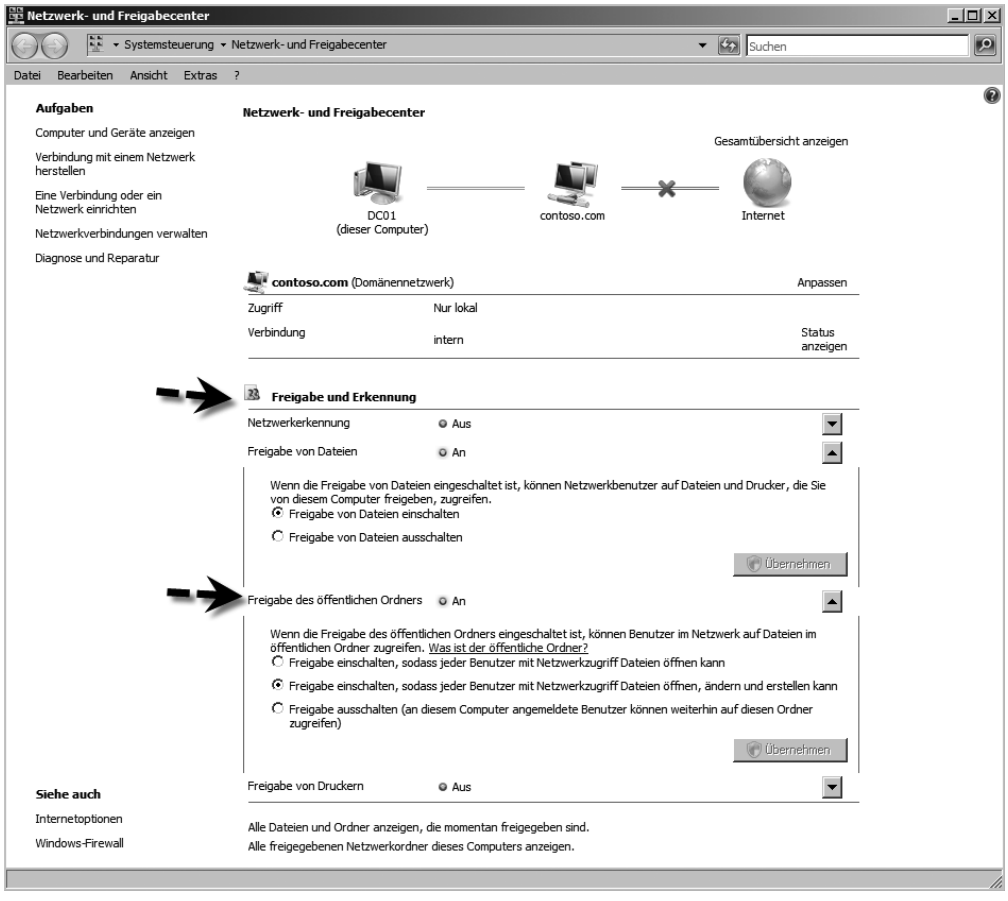
Kapitel 6

Verwalten von Datei- und Druckservern

In diesem Kapitel:

Auch Windows Server 2008 wird in Unternehmen oftmals als Datei- oder Druckserver eingesetzt. In diesem Kapitel zeigen wir Ihnen den Umgang mit Windows Server 2008 als Datei- oder Druckserver. Wir gehen dabei auf die Möglichkeiten ein, Freigaben zu erstellen und zu verwalten, aber auch auf die neuen Sicherheitsoptionen und Einstellungen, die auf einem Dateiserver benötigt werden. Damit auf einen Windows Server 2008 über Freigaben zugegriffen werden kann, müssen Sie zunächst sicherstellen, dass im Netzwerk- und Freigabecenter die Dateifreigaben aktiviert worden sind (Abbildung 6.1). Erst dann ist der Zugriff über das Netzwerk möglich.

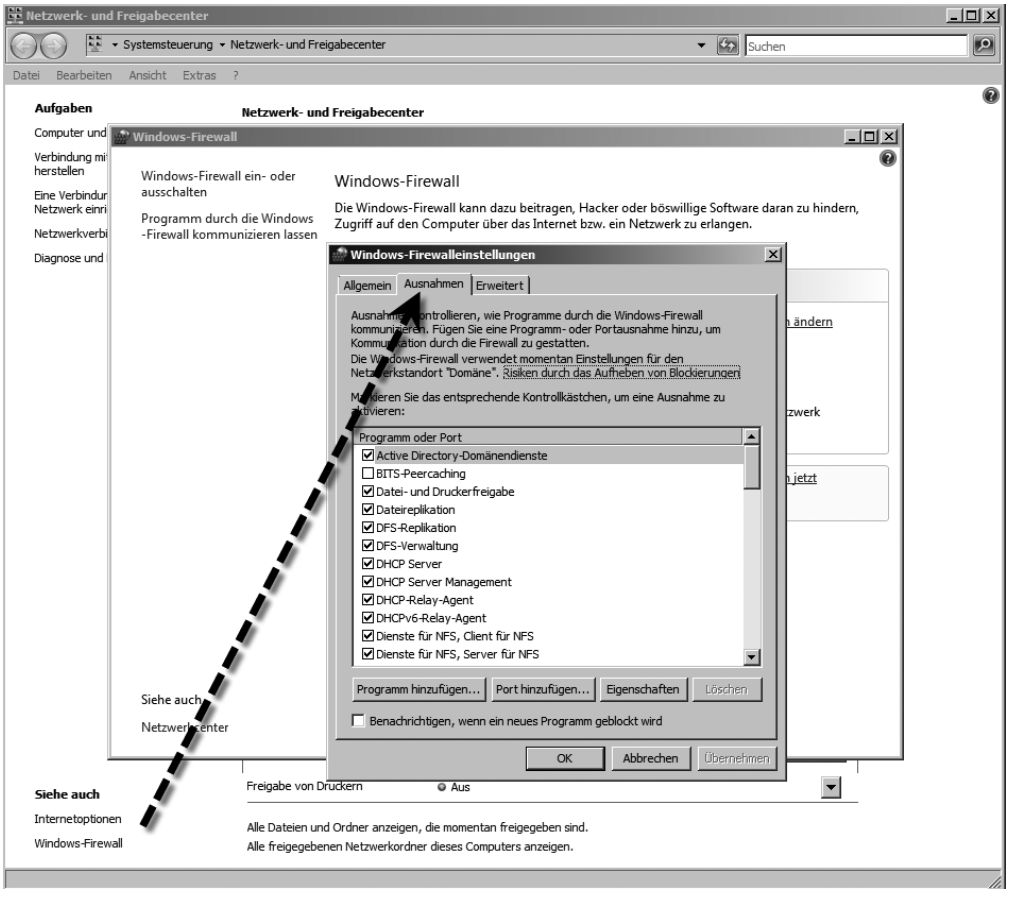
Abbildg. 6.1 Aktivieren der Freigabe und Erkennung unter Windows Server 2008



Der Assistent aktiviert dazu in den Ausnahmen der Windows-Firewall den Zugriff auf den Server. Sie sehen diese Ausnahme, wenn Sie im *Netzwerk- und Freigabecenter* links unten auf den Link *Windows-Firewall* klicken und dann im neuen Fenster auf *Einstellungen ändern*. Es öffnen sich die Einstellungen der Firewall.

Auf der Registerkarte *Ausnahmen* sehen Sie, welchen Netzwerkverkehr die Firewall jetzt zulässt (Abbildung 6.2).

Abbildg. 6.2 Überprüfen der Firewall-Ausnahmen für die Datei- und Druckerfreigabe



Die Aktivierung der Freigaben wird automatisch aktiviert, wenn Sie die Serverrolle *Dateidienste* auf dem Dateiserver installieren. Bevor Sie Freigaben einrichten, sollten Sie daher diese Rolle installieren.

Berechtigungen für Dateien und Verzeichnisse verwalten

Die Berechtigungen im Dateisystem werden in der *Zugriffssteuerungsliste*, der ACL (Access Control List), gespeichert. Während der Anmeldung wird für den Benutzer ein so genanntes Zugriffstoken generiert, das die Security ID (SID) des Benutzerkontos enthält sowie die SIDs der Gruppen in denen der Benutzer Mitglied ist. Beim Zugriff auf eine Datei werden die Einträge des Token mit der ACL verglichen und daraus die Berechtigung ermittelt. Dazu werden die Berechtigungen für jeden übereinstimmenden Eintrag addiert. Ein Benutzer bekommt die Berechtigungen, die seinem Konto zugewiesen wurden, sowie alle Berechtigungen, die den Gruppen zugewiesen wurden, in denen er

Mitglied ist. Wird einem Benutzerkonto die Berechtigung *Lesen* gegeben und bekommt zusätzlich eine Gruppe, in der dieser Benutzer Mitglied ist, die Berechtigung *Schreiben* zugewiesen, ergeben die effektiven Berechtigungen *Lesen* und *Schreiben*. Um die Berechtigungen zu setzen, wählen Sie in den Eigenschaften des Verzeichnisses oder der Datei die Registerkarte *Sicherheit* (Abbildung 6.3).

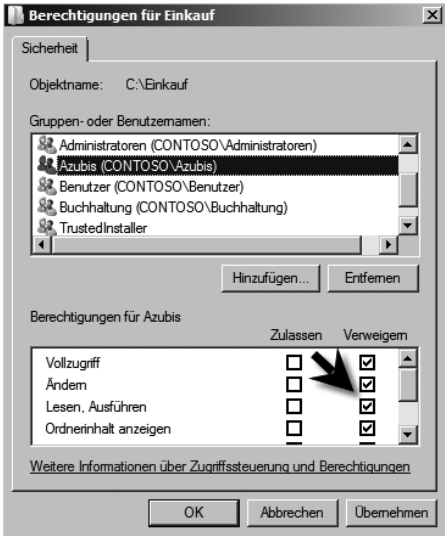
Abbildg. 6.3 Verwalten von Berechtigungen für Verzeichnisse und Dateien

Zusätzlich ist es möglich, einzelnen Benutzern oder Gruppen Berechtigungen zu verweigern, wobei die Verweigerung immer Vorrang hat.

Beispiel

Auf eine Datei sollen alle Mitarbeiter der Buchhaltung (mit der Mitgliedschaft in der gleich benannten Gruppe) Zugriff erhalten. Eine Ausnahme machen dabei allerdings die Auszubildenden, die ebenfalls Mitglied der Gruppe *Buchhaltung* sind. Wenn der Gruppe *Buchhaltung* der Zugriff auf diese Datei erlaubt wird, erhalten auch die Auszubildenden Zugriff, da sie Mitglied der Gruppe sind. Anschließend können Sie der Gruppe *Auszubildende* den Zugriff verweigern. So erhalten die Auszubildenden zwar den Zugriff durch die Mitgliedschaft in der Gruppe *Buchhaltung*, der ihnen aber durch die Mitgliedschaft in der Gruppe *Auszubildende* verweigert wird.

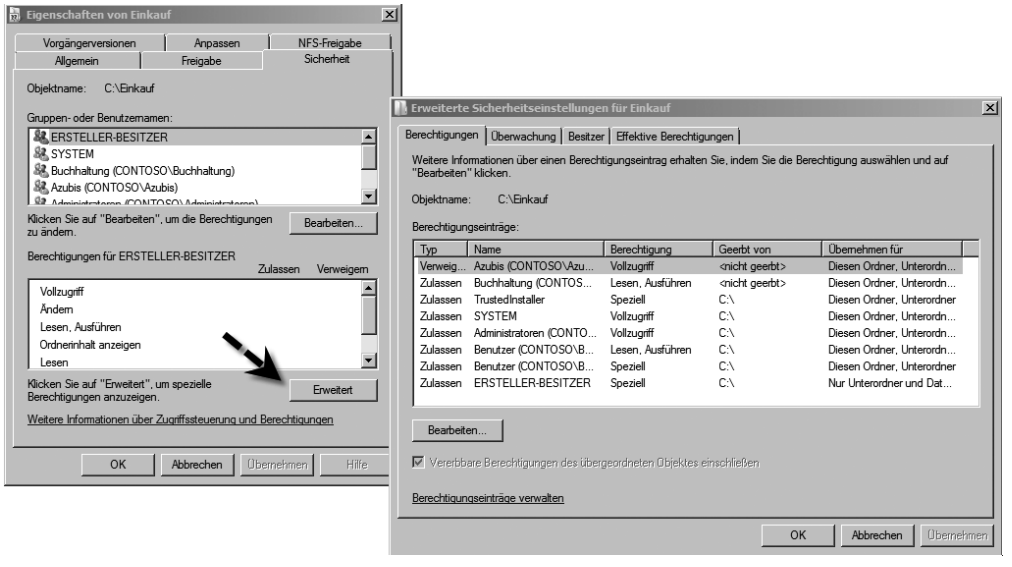
Abbildg. 6.4 Verweigern von Berechtigungen für bestimmte Gruppen



Erweiterte Berechtigungen auf Verzeichnisse

Um spezielle Berechtigungen zu setzen und weitere Einstellungen vorzunehmen, wählen Sie auf der Registerkarte *Sicherheit* die Schaltfläche *Erweitert* (Abbildung 6.5). Um die erweiterten Berechtigungen zu konfigurieren, klicken Sie im neuen Fenster auf *Bearbeiten*. Als Nächstes können Sie entweder bestehende Einträge bearbeiten oder neue Benutzerkonten hinzufügen, denen Sie dann spezielle Berechtigungen zuweisen können.

Abbildg. 6.5 Bearbeiten der erweiterten Berechtigungen für Verzeichnisse



Damit Sie für das Verzeichnis erweiterte Berechtigungen zuweisen können, müssen Sie entscheiden, wie weit sich diese Berechtigungen auswirken. Dazu wählen Sie aus der Liste *Übernehmen für* in den Eigenschaften eines Eintrags aus, in welchem Bereich sich die speziellen Berechtigungen auswirken sollen (Abbildung 6.6).

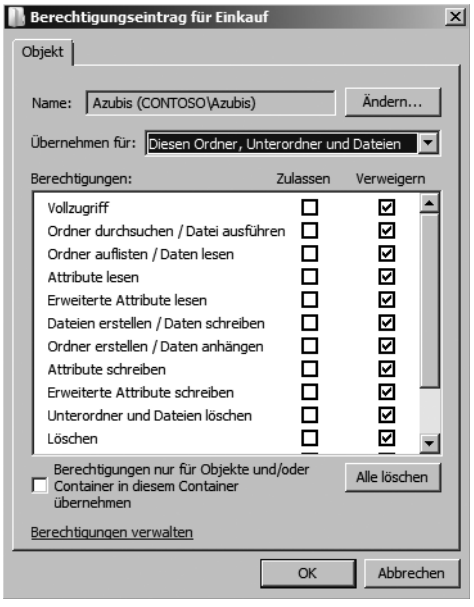
- **Nur diesen Ordner** Die Berechtigungen werden nur für diesen Ordner gesetzt und gelten nicht für darin enthaltene Unterordner oder Dateien.
- **Diesen Ordner, Unterordner und Dateien** Die Berechtigungen werden auf die komplette Verzeichnisstruktur angewendet und gelten für alle Verzeichnisse und Dateien unterhalb dieses Verzeichnisses.
- **Diesen Ordner, Unterordner** Die Berechtigungen werden nur auf dieses Verzeichnis und alle Unterverzeichnisse gesetzt, Berechtigungen auf Dateien werden nicht gesetzt.
- **Diesen Ordner, Dateien** Die Berechtigungen gelten nur für dieses Verzeichnis und die darin enthaltenen Dateien.
- **Nur Unterordner und Dateien** Dieses Verzeichnis wird von der Vergabe der Berechtigungen ausgenommen, sondern auf darin enthaltene Dateien und andere Verzeichnisse gesetzt.
- **Nur Unterordner** Dieses Verzeichnis wird von der Vergabe der Berechtigungen ausgenommen und nur auf darin enthaltene Verzeichnisse gesetzt.
- **Nur Dateien** Dieses Verzeichnis wird von der Vergabe der Berechtigungen ausgenommen und nur auf darin enthaltene Dateien gesetzt.

Setzen Sie nach der Auswahl die erweiterten Berechtigungen. Über die Schaltfläche *Alle löschen* können Sie die Liste der gesetzten Berechtigungen wieder löschen. Auch bei Dateien gibt es eine Unterteilung in Standard- und erweiterte Berechtigungen.

Besitzer für ein Objekt festlegen

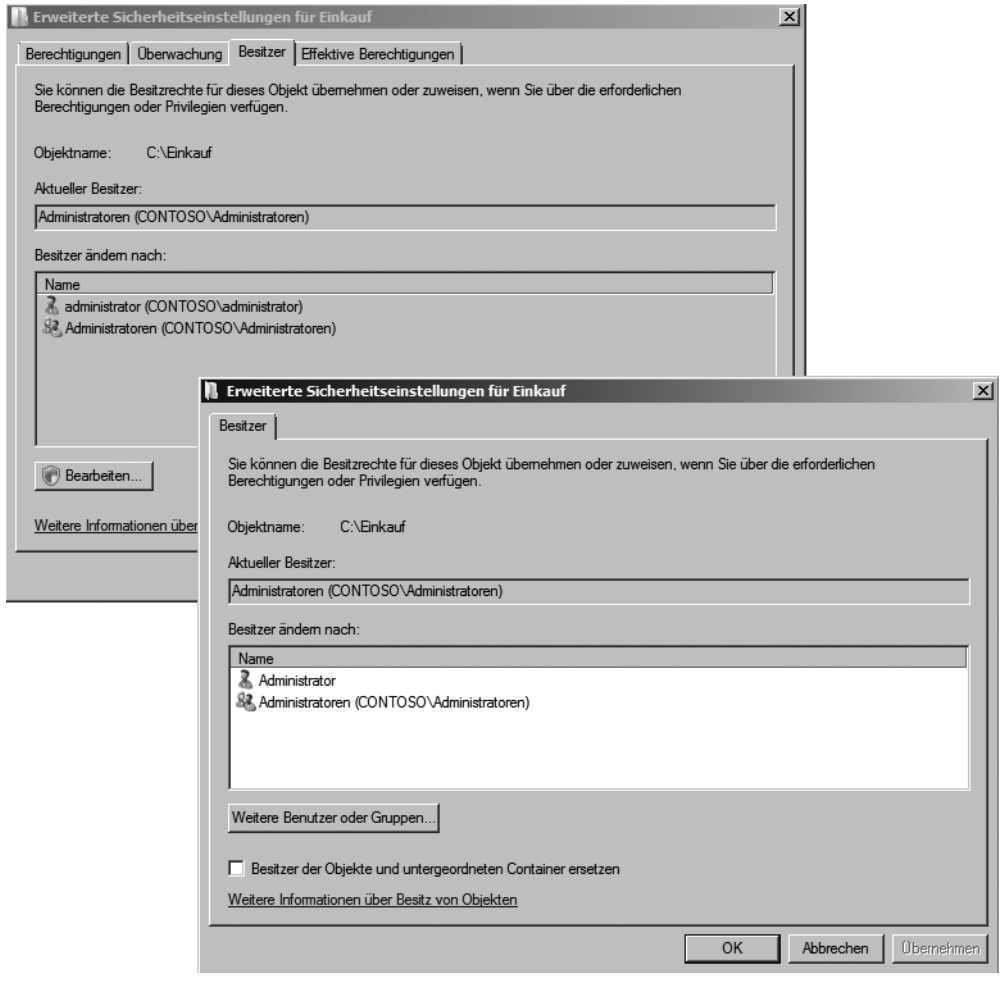
Neben den Berechtigungen im Dateisystem gibt es noch den Objektbesitzer. Der Objektbesitzer darf festlegen, wer weitere Berechtigungen auf die Datei erhält. Objektbesitzer ist standardmäßig der Anwender, der eine Datei erstellt. Die Information über den Besitzer einer Datei wird verwendet, wenn Sie Kontingente zur Begrenzung des von Anwendern verwendeten Speicherplatzes eingerichtet haben. Über diese Eigenschaft der Datei wird der von einem Anwender bereits genutzte Speicherplatz ermittelt.

Abbildg. 6.6 Bearbeiten der erweiterten Berechtigungen für ein Verzeichnis



Um den Besitzer einer Datei festzustellen oder zu ändern, öffnen sie zunächst die Eigenschaften des Objekts, wählen dort die Registerkarte *Sicherheit* und anschließend die Schaltfläche *Erweitert*. Auf der Registerkarte *Besitzer* sehen Sie unter *Aktueller Besitzer* den Besitzer dieses Objekts. Es gibt zwei Möglichkeiten, den Besitzer zu ändern: Administratoren haben die Berechtigung, den Besitz selbst zu übernehmen oder auf einen anderen Benutzer zu übertragen, wogegen alle Anwender lediglich anderen Anwendern die spezielle Berechtigung *Besitzrechte übernehmen* zuweisen können, woraufhin diese anschließend den Besitz übernehmen. Um den Besitz zu übernehmen, wählen Sie Ihr Konto aus der Liste *Besitzer ändern nach* aus. Wenn Sie den Besitz einem anderen Anwender übertragen wollen, der nicht in der Liste aufgeführt ist, können Sie dieses Konto über *Weitere Benutzer oder Gruppen* hinzufügen. Wollen Sie den Besitzer nicht nur für dieses Verzeichnis, sondern auch für alle Unterordner und darin enthaltenen Dateien ersetzen, aktivieren Sie das Kontrollkästchen *Besitzer der Objekte und untergeordneten Container ersetzen*.

Abbildg. 6.7 Bearbeiten des Besitzers eines Objektes im NTFS

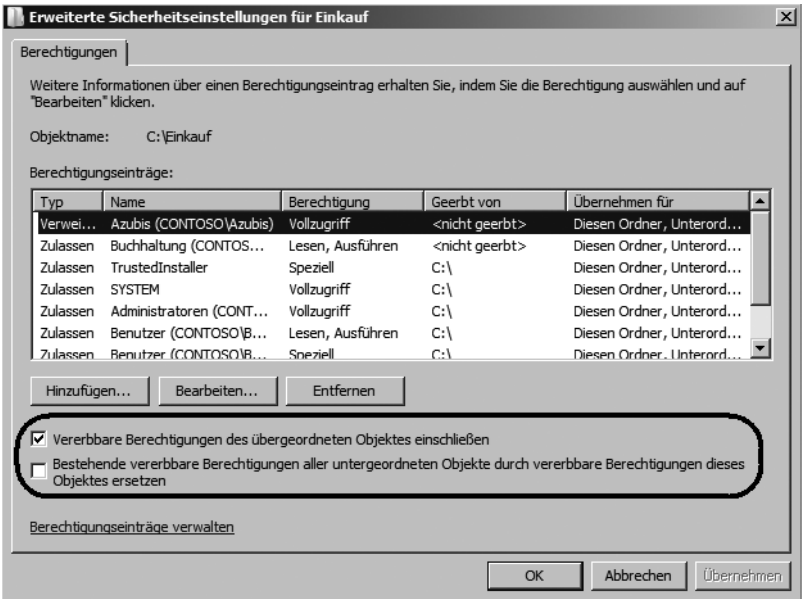


Vererbung von Berechtigungen

Grundsätzlich gilt bei Verzeichnisstrukturen das Prinzip der Vererbung. Das heißt, eine Berechtigung, die ein Benutzer auf ein Verzeichnis erhält, erhält er auch auf die darin enthaltenen Verzeichnisse und Dateien. Geben Sie einem Benutzerkonto die Berechtigung *Ändern* auf ein Verzeichnis, sehen Sie in den untergeordneten Verzeichnissen, dass der Benutzer die gleichen Berechtigungen hat. Allerdings sind die entsprechenden Felder grau unterlegt. Damit wird angezeigt, dass die Berechtigung nicht explizit in diesem Verzeichnis zugewiesen wird, sondern vom übergeordneten Ordner vererbt wurde. Da bei vererbten Berechtigungen nicht ohne weiteres eine Berechtigung herausgenommen werden kann, können Sie für Unterordner einzelne Rechte verweigern. Wählen Sie auf der Registerkarte *Sicherheit* die Schaltfläche *Erweitert*. Wichtig ist in diesem Dialogfeld das Kontrollkästchen *Vererbbare Berechtigungen des übergeordneten Objektes einschließen,* nachdem auf die

Schaltfläche *Bearbeiten* geklickt wurde Durch dessen Auswahl werden Berechtigungen von übergeordneten Verzeichnissen im Verzeichnisbaum übernommen.

Abbildg. 6.8 Konfigurieren der Vererbung für ein Verzeichnis



Wenn dieses Kontrollkästchen nicht aktiviert ist, werden auf das Verzeichnis nur die definierten Berechtigungen angewendet. Eine Vererbung von Zugriffsrechten kann damit gezielt auf der Ebene von Unterverzeichnissen unterbrochen werden. Darüber hinaus kann mit dem Kontrollkästchen *Bestehende vererbbare Berechtigungen aller untergeordneten Objekte…* konfiguriert werden, dass die für dieses Verzeichnis definierten Berechtigungen auf alle untergeordneten Dateien und Verzeichnisse kopiert werden. Dort werden alle bereits konfigurierten Berechtigungen zurückgesetzt. In der Liste der Berechtigungen wird der Vererbungsstatus von Berechtigungen in der Spalte *Geerbt von* angegeben.

Herstellen der Standardberechtigungen für die Vererbung

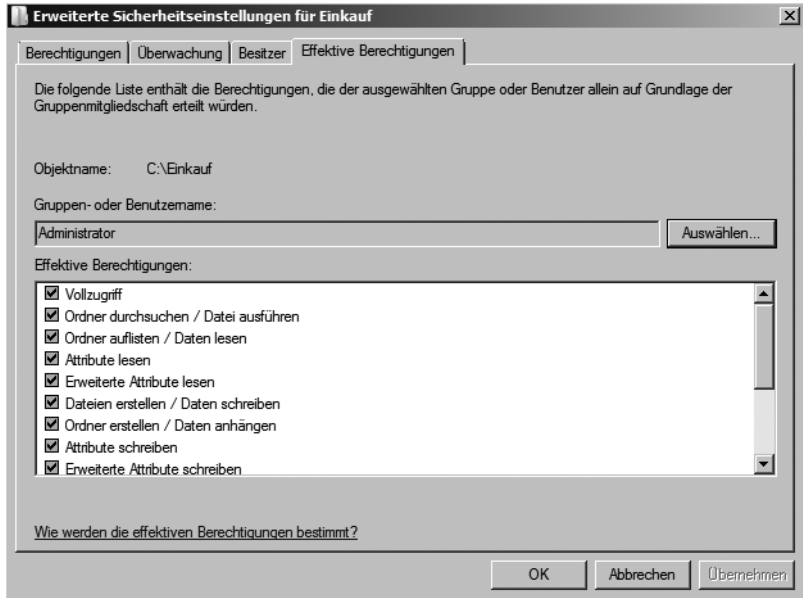
Um den Ausgangszustand wiederherzustellen, öffnen Sie den Ordner, dessen Berechtigungen wieder auf die Unterordner übertragen werden sollen. Wählen Sie anschließend auf der Registerkarte *Sicherheit* die Schaltfläche *Erweitert*. Aktivieren Sie das Kontrollkästchen *Bestehende vererbbare Berechtigungen aller untergeordneten Objekte …*, nachdem Sie auf Bearbeiten geklickt haben. Anschließend werden die Berechtigungen an alle Unterordner weitergegeben.

Effektive Berechtigungen

Um die effektiven Berechtigungen anzuzeigen, öffnen Sie in den Eigenschaften des Verzeichnisses die Registerkarte *Sicherheit* und dann die erweiterten Einstellungen. Wählen Sie die Registerkarte *Effektive Berechtigungen* aus. Sie sehen alle speziellen Berechtigungen, die der Benutzer hat. Um die

Berechtigungen für einen anderen Benutzer anzuzeigen, wählen Sie über *Auswählen* ein anderes Konto aus.

Abbildg. 6.9 Anzeigen der effektiven Berechtigungen für ein Verzeichnis



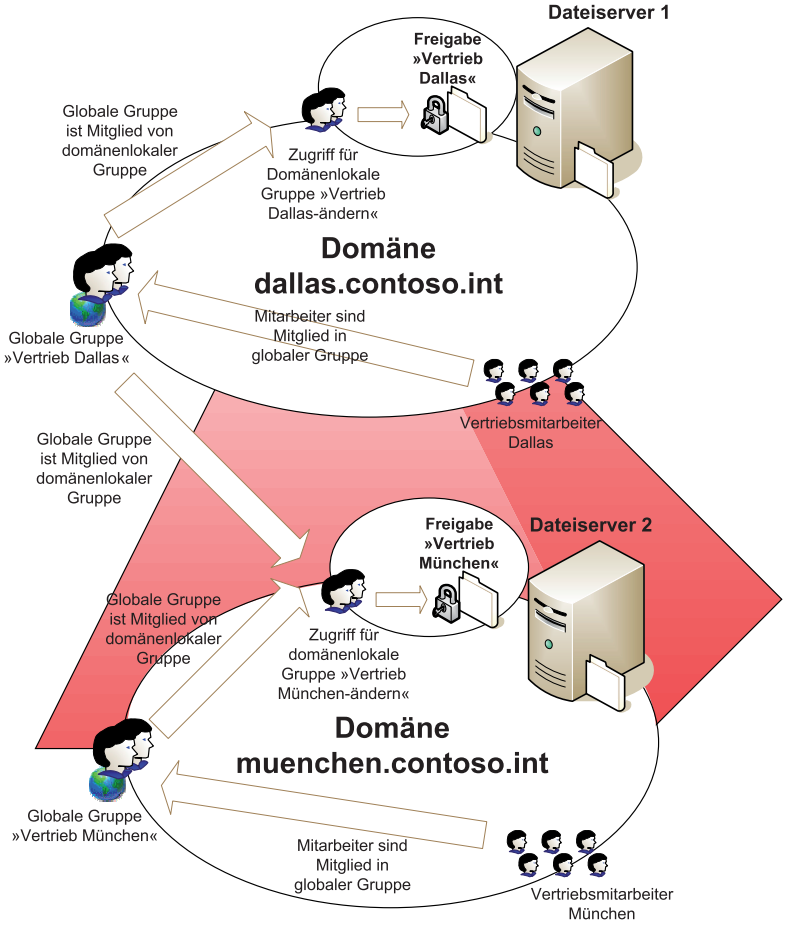
Berechtigungen für Benutzer und Gruppen verwalten

Die Vergabe von Zugriffsberechtigungen sollte immer an Gruppen erfolgen, da damit der geringste administrative Aufwand entsteht. Wenn ein weiterer Benutzer diese Berechtigung erhalten soll, muss er nur der Gruppe zugeordnet werden. Die Berechtigungen müssen nicht verändert werden. Ebenso lassen sich die Zugriffsberechtigungen einzelnen Benutzern entziehen, indem diese einfach aus der Gruppe entfernt werden. Zugriffsberechtigungen sollten nach Möglichkeit über ein Skript und nicht über die grafische Oberfläche vergeben werden, damit eine Dokumentation der Berechtigungen möglich ist. Dies ist wichtig, wenn beispielsweise Daten auf einen externen Datenträger (CD oder DVD) ausgelagert werden, der keine Zugriffsrechte unterstützt. Bei der Planung von Berechtigungen sollten Sie sehr effizient planen, welche Ordnerstrukturen Sie anlegen und welche Gruppen Sie aufnehmen. Microsoft empfiehlt folgende Berechtigungsstruktur:

- Domänenlokale Gruppe erhält Berechtigung auf Ordner und Freigabe
- Globale Gruppe(n) wird in lokale Gruppe aufgenommen
- Benutzerkonten der Anwender sind Mitglieder der einzelnen globalen Gruppen
- Auf Verzeichnisse im Dateisystem sollten die Administratoren Vollzugriff erhalten. Zusätzlich sollten Sie eine domänenlokale Gruppe anlegen, die Berechtigung auf der Verzeichnisebene und auf Freigabeebenen erhält.

Der Sinn dieses Konzepts liegt darin, dass Sie einerseits nicht ständig Berechtigungen für den freigegebenen Ordner ändern müssen, da nur die domänenlokale Gruppe Zugriff erhält. Da die Anwender in globalen Gruppen aufgenommen werden, können die Gruppen auch in andere domänenlokale Gruppen in anderen Domänen von Active Directory aufgenommen werden. Das hat in großen Organisationen den Vorteil, dass Freigaben sehr effizient überall bereitgestellt werden können.

Abbildg. 6.10 Aufbau einer Berechtigungsstruktur basierend auf Gruppen



Mitgliedschaften und Änderungen sollten deshalb auf ein Minimum reduziert werden. Es sollten keine einzelnen Benutzer zu den Berechtigungen auf Freigabe- oder Dateiebene hinzugefügt werden. Zugriffsberechtigungen werden im Regelfall pro Verzeichnis einheitlich vergeben. Eine Anpassung von Berechtigungen für einzelne Dateien ist nur in Ausnahmen sinnvoll und lässt sich oft dadurch umgehen, dass mit eigenen Verzeichnissen für die Dateien, bei denen abweichende Berechtigungen konfiguriert werden müssten, gearbeitet wird. Spezielle Zugriffsberechtigungen für einzelne Dateien stellen immer ein Problem dar, wenn Zugriffsberechtigungen für alle Dateien verändert werden sollen, weil

neue Benutzergruppen hinzugefügt werden. Hier müssen die abweichenden Berechtigungen neu definiert werden. Im Beispiel von Abbildung 6.10 sehen Sie den Sinn dieses Konzepts:

- Domänenlokale Gruppen können zwar globale Gruppen aus der kompletten Gesamtstruktur aufnehmen, aber selbst nicht in anderen Domänen verwendet werden.
- Globale Gruppen können nur Mitglieder aus der eigenen Domäne aufnehmen, haben aber dafür die Möglichkeit, dass sie überall im Active Directory verwendet werden können.

Die Vertriebsmitarbeiter in Dallas können durch dieses Konzept sowohl auf die Freigabe in Dallas als auch auf die Freigabe in München zugreifen. Wenn neue Mitarbeiter Zugriff erhalten müssen, kann dies durch Aufnahme in die entsprechende globale Gruppe recht schnell erledigt werden. Zugriffsberechtigungen sollten nie ad hoc, sondern immer nur nach genau definierten Konzepten vergeben werden. Nur so lässt sich sicherstellen, dass mit einem durchdachten und damit sicheren Verfahren gearbeitet wird.

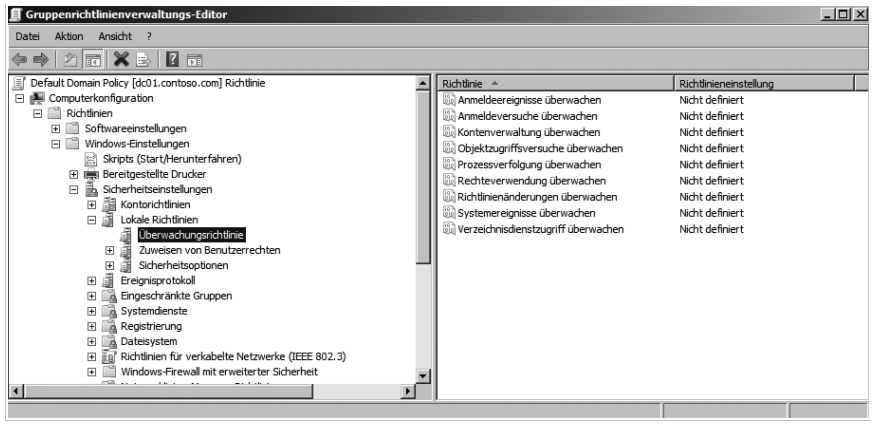
Überwachen von Dateien und Verzeichnissen

In den meisten Fällen kann eine Überwachung der Zugriffe auf Verzeichnisse nützlich sein, bei der festgehalten wird, wer erfolgreich oder auch erfolglos versucht hat, bestimmte Operationen auf Dateien und Verzeichnisse auszuführen. Damit die Überwachung durchgeführt werden kann, müssen sie diese zunächst aktivieren. Dies geschieht entweder über eine lokale Richtlinie oder über Gruppenrichtlinien.

Aktivieren der Überwachung von Dateisystemzugriffen

Öffnen Sie die lokale oder Gruppenrichtlinie für den Computer und navigieren Sie anschließend zu *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Überwachungsrichtlinien*. Die Verwendung von Gruppenrichtlinien wird im Kapitel 9 ausführlich besprochen. Die Verwaltung der lokalen Richtlinien wird durch Eingabe des Befehls gpedit.msc gestartet. Die Überwachung der Zugriffe auf das Dateisystem aktivieren Sie über *Objektzugriffsversuche überwachen*. Neben Dateizugriffen überwachen Sie mit dieser Einstellung auch Zugriffe auf Drucker. In der Standardeinstellung ist die Überwachung zunächst nicht aktiviert. Nach der Aktivierung müssen Sie noch auswählen, ob erfolgreiche und/oder fehlgeschlagene Zugriffsversuche protokolliert werden sollen.

Abbildg. 6.11 Konfiguration der Überwachungsrichtlinie

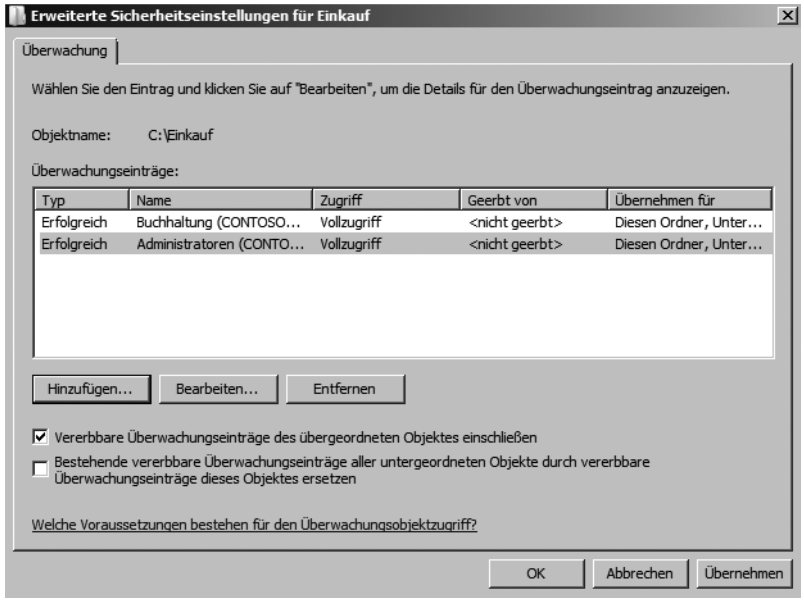


Nachdem Sie die Überwachung aktiviert haben, müssen Sie die eigentliche Überwachung für die entsprechenden zu überwachenden Dateien und Verzeichnisse aktivieren. Öffnen Sie dazu die Eigenschaften des Objekts und wählen Sie auf der Registerkarte *Sicherheit* die Schaltfläche *Erweitert*. Auf der Registerkarte *Überwachung* sehen Sie, welche Operationen protokolliert werden. Damit Sie die bei der Überwachung anfallenden Protokolldaten sinnvoll bearbeiten können, sollten Sie von diesen Einschränkungsmöglichkeiten Gebrauch machen und nur das Nötigste protokollieren. Über *Hinzufügen* legen Sie die Überwachung fest. Wie bei den NTFS-Berechtigungen gilt auch hier das Prinzip der Vererbung, das Sie bei Bedarf ausschalten können. Nachdem Sie *Hinzufügen* gewählt haben, können Sie über *Ändern* den zu überwachenden Benutzer auswählen. Wie schon bei der Vergabe spezieller NTFS-Berechtigungen können Sie wieder angeben, inwieweit sich diese Einstellungen auf untergeordnete Objekte und Verzeichnisse auswirken. Wählen Sie anschließend im Feld *Zugriff* aus, welche Zugriffe protokolliert werden sollen, und ob Sie erfolgreiche oder fehlgeschlagene Zugriffe protokollieren wollen.

Anzeige des Überwachungsprotokolls

Die Protokollierung der Überwachung erfolgt in der Ereignisanzeige. Starten Sie die Verwaltungskonsole über *Start/Ausführen/eventvwr.msc* oder über den Server-Manager. In der Ereignisanzeige finden Sie die protokollierten Zugriffsversuche im Sicherheitsprotokoll. Die mit einem Schlüssel gekennzeichneten Einträge stehen für erfolgreiche Zugriffe, wogegen ein Schloss für fehlgeschlagene Zugriffe steht. Genauere Informationen zu einem Eintrag bekommen Sie, wenn Sie ihn öffnen. Ein einzelner Zugriff erzeugt eine ganze Reihe von Einträgen im Sicherheitsprotokoll.

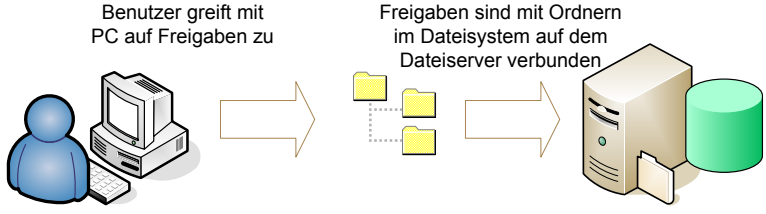
Abbildg. 6.12 Konfigurieren der Überwachung für Verzeichnisse



Freigeben von Verzeichnissen

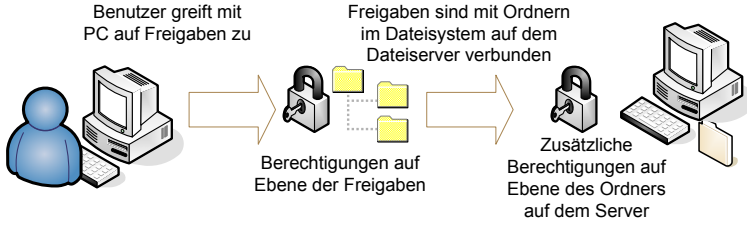
Die Verbindung der Clients erfolgt zunächst zu einem Server. Auf diesem Server wird auf eine Freigabe zugegriffen. Eine Freigabe definiert, auf welche Verzeichnisse auf welchen Datenträgern zugegriffen werden kann. Der Client sieht nicht die physischen Festplatten auf den Servern und die dort definierten Verzeichnisstrukturen. Vielmehr stellt ihm eine Freigabe einen Eintrittspunkt zum Server bereit, von dem aus er die dort definierten Verzeichnisstrukturen durchsuchen kann (Abbildung 6.13).

Abbildg. 6.13 Dateiserver mit Windows Server 2008



Der Benutzer muss nicht wissen, welche Festplatten es auf den Servern gibt und wie diese strukturiert sind, sondern soll nur die Bereiche sehen, die für ihn relevant sind. Für Freigaben können Zugriffsberechtigungen definiert werden. Damit können Freigaben als weitere Ebene der Sicherheit eingesetzt werden, zusätzlich zu den Sicherheitsmechanismen auf der Ebene und zu den Zugriffsberechtigungen auf der Ebene des Dateisystems (Abbildung 6.14). Freigaben lassen sich ganz einfach erstellen. Dazu wird im Windows-Explorer das Verzeichnis ausgewählt, für das eine Freigabe erstellt werden soll. Im Kontextmenü findet sich der Befehl *Freigabe*.

Abbildg. 6.14 Arbeiten mit Berechtigungen auf Freigabe- und Verzeichnisebene



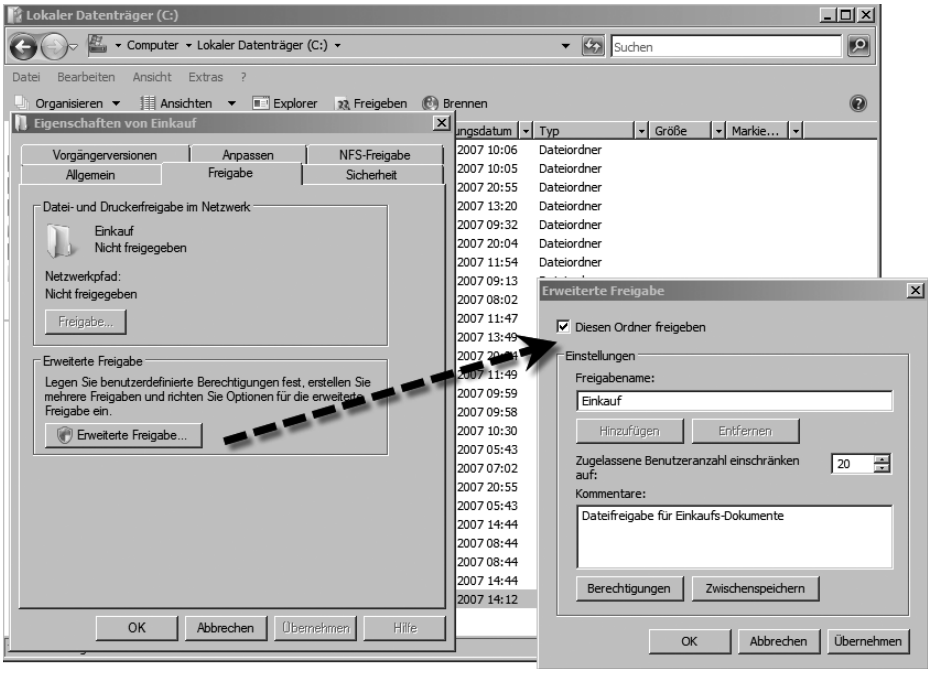
Im angezeigten Dialogfeld wird automatisch die Registerkarte *Freigabe* geöffnet (Abbildung 6.15). Öffnet sich nicht diese Registerkarte sondern ein Assistent, ist noch der Freigabe-Assistent aktiviert und sollte deaktiviert werden:

1. Öffnen Sie über *Start/Computer* ein Explorer-Fenster.
2. Wählen Sie aus dem Dropdown-Menü *Organisieren* die Option *Ordner- und Suchoptionen* aus.
3. Wechseln Sie zur Registerkarte *Ansicht*.
4. Deaktivieren Sie die Einstellung *Freigabe-Assistent verwenden*.
5. Melden Sie sich mit dem gleichen Benutzernamen und Kennwort an, oder authentifizieren Sie sich entsprechend.

Klicken Sie als Nächstes auf die Schaltfläche *Erweiterte Freigabe*, da Sie so mehr Einstellungen vornehmen können. Mit der Option *Diesen Ordner freigeben*, können Sie dieses Verzeichnis im Netzwerk zur Verfügung stellen. Sie können einen Freigabenamen und einen Kommentar zur Freigabe eingeben. Für die Definition von Freigabenamen sollten bereits klare Namensregeln bestehen, um diese einheitlich und sinnvoll zu bezeichnen.

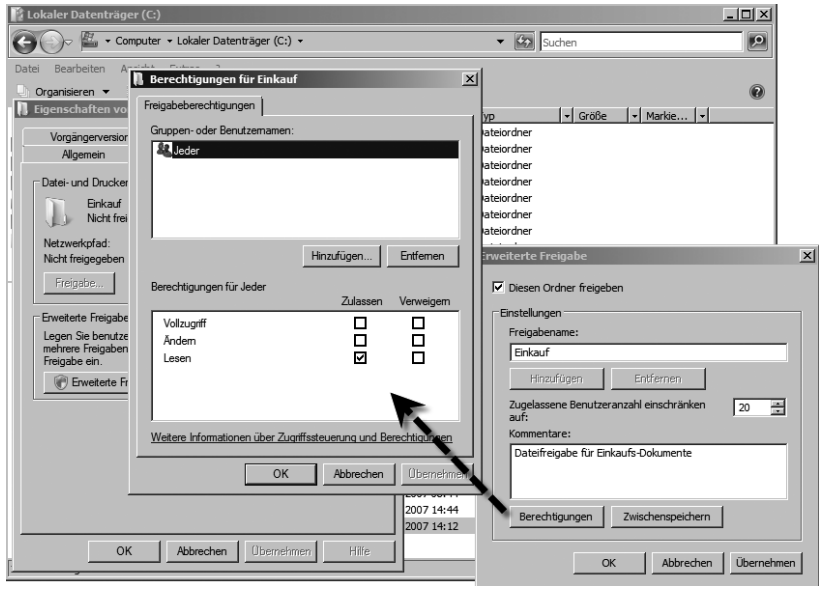
HINWEIS Administratoren können auf die komplette Festplatte über das Netzwerk zugreifen, indem die Freigabe *C$* bzw. *<Laufwerksbuchstabe>$* verwendet werden. Allerdings haben in diesem Fall sämtliche Netzwerkteilnehmer das Recht, auf die komplette Festplatte zuzugreifen und beliebige Daten zu löschen oder zu verändern. Diese Freigaben werden Admin-Freigaben genannt. Nur Administratoren haben Zugriff darauf.

Abbildg. 6.15 Konfigurieren einer Freigabe unter Windows Server 2008



Über die Schaltfläche *Berechtigungen* können Zugriffsrechte für die Freigabe konfiguriert werden. Aus diesen Berechtigungen und den Rechten für Dateien und Verzeichnisse, die im NTFS definiert wurden, wird die Schnittmenge gebildet. Es gelten grundsätzlich die engsten Einschränkungen der Zugriffsberechtigungen. Wenn ein Benutzer *Vollzugriff* auf die Freigabe hat und ein Verzeichnis im NTFS nur lesen darf, darf er es auch tatsächlich nur lesen. Hat er andersherum im NTFS Vollzugriff und wurde auf die Freigabe nur das Leserecht vergeben, darf er auf das Verzeichnis über das Netzwerk nur lesend zugreifen. Er kann allerdings lokal auf dem Server oder über andere, überlappende Freigaben, die diese Einschränkung nicht haben, mit mehr Rechten zugreifen. Die Gruppe *Jeder* hat in Windows Server 2008 nur lesenden Zugriff für neu erstellte Freigaben. Benutzer, Computer und Gruppen, die Zugriffsberechtigungen erhalten sollen, können über die Schaltfläche *Hinzufügen* ausgewählt werden.

Abbildg. 6.16 Hinzufügen und Verwalten von Berechtigungen für eine Freigabe



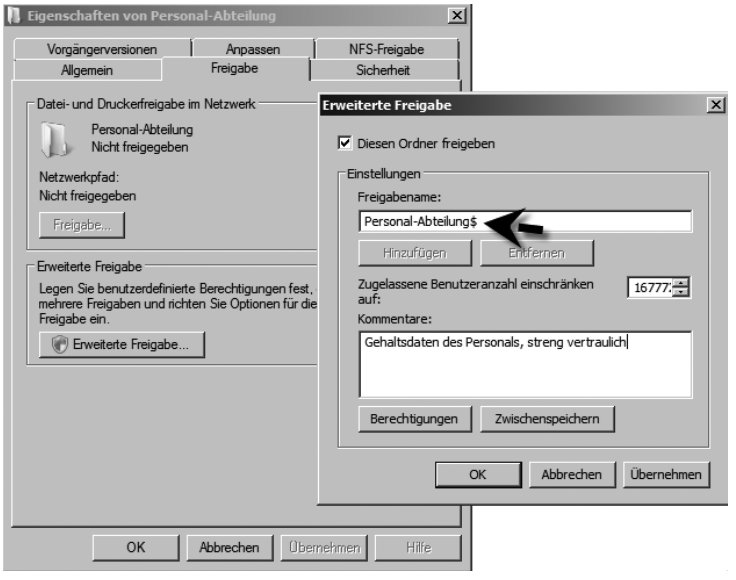
Im ersten angezeigten Dialogfeld können Sie die Benutzernamen oder Gruppen angeben. Alternativ können Sie den Befehl *Erweitert* verwenden, um auf ein weiteres Dialogfeld zuzugreifen und dort die Benutzer und Gruppen detaillierter auszuwählen. Gruppen, Benutzern und Computern, die hinzugefügt werden, wird zunächst das Recht *Lesen* vergeben. Andere Berechtigungen können selektiv in dem Dialogfeld *Berechtigungen* ausgewählt oder verweigert werden. Wenn für ein Verzeichnis eine Freigabe konfiguriert wurde, ist das im Windows-Explorer am Freigabe-Symbol zu erkennen, welches zusätzlich zum Ordnersymbol angezeigt wird.

HINWEIS Die effektiven Berechtigungen bei einem Zugriff über eine Freigabe werden folgendermaßen ermittelt: Unabhängig voneinander wird erst die Berechtigung für den Zugriff über die Freigabe aus den zugewiesenen Berechtigungen sowie den Berechtigungen für Gruppen, in denen der Anwender Mitglied ist, ermittelt und anschließend die effektiven NTFS-Berechtigungen. Beim Vergleich der Berechtigungen erhält der Anwender jetzt die am stärksten einschränkende Berechtigung.

Versteckte Freigaben

Auch wenn es möglich ist, die Zugriffsberechtigungen auf eine Freigabe so einzustellen, dass einem unbefugten Anwender der Zugriff auf die Dateien und Verzeichnisse der Freigabe verwehrt werden, wird die Freigabe selbst aber immer angezeigt, unabhängig von den zugewiesenen Berechtigungen. Spezielle Freigaben können aber vor Anwendern versteckt werden, sodass diese nicht als Freigaben auftauchen, unabhängig von den jeweiligen Berechtigungen. Um zu verhindern, dass Anwender eine Freigabe sehen, verstecken Sie die Freigabe, indem Sie dem Freigabenamen ein Dollarzeichen anhängen (Abbildung 6.16). Sie können sich mit dieser Freigabe jetzt nur noch durch direkte Eingabe des Freigabenamens (inklusive Dollarzeichen) verbinden. In der Netzwerkumgebung wird die Freigabe nicht mehr angezeigt.

Abbildg. 6.17 Erstellen von versteckten Freigaben



Für die Verwaltung der Windows-Computer werden direkt bei der Installation des Computers einige Standardfreigaben erstellt. Dabei handelt es sich ausnahmslos um versteckte Freigaben, die ausschließlich für die Verwendung durch den Administrator gedacht sind. Die Berechtigungen für diese Freigaben können nicht verändert werden. Alle Festplattenlaufwerke werden für den Zugriff durch den Administrator komplett freigegeben. Dies gilt nicht für CD- oder DVD-Laufwerke. Da Sie bei der Installation eines Windows-Computers frei angeben können, in welches Verzeichnis die Windows-Dateien installiert werden, gelangen Sie über die Freigabe *Admin$* zum Windows-Verzeichnis. Über die Freigabe *Print$* werden bei der Verknüpfung mit einem Netzwerkdrucker die benötigten Druckertreiber geladen.

Abbildg. 6.18 Konfigurieren von Berechtigungen für eine Freigabe

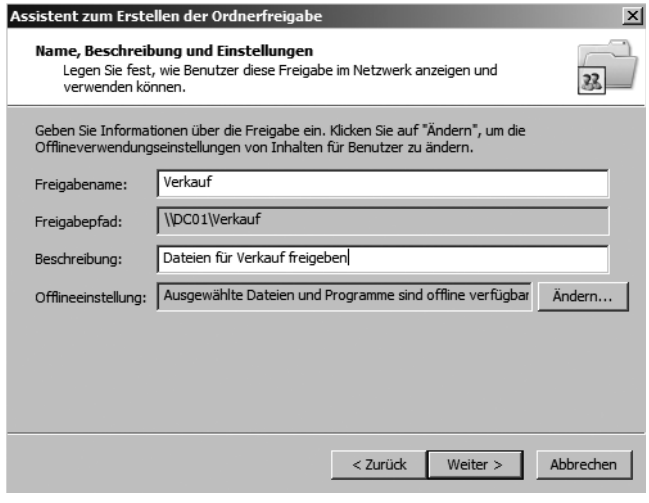
Sie sollten auf der Ebene der Freigaben die gleichen Gruppen berechtigen, wie auf NTFS-Ebene. Die Festlegung auf NTFS-Ebene erfolgt über die Eigenschaften eines Ordners auf der Registerkarte *Sicherheit*. Über die Schaltfläche *Hinzufügen* können neue Objekte, denen Berechtigungen gewährt werden sollen, ausgewählt werden. Als Standardberechtigungen sind definiert:

- **Vollzugriff** Erlaubt den vollen Zugriff auf das Verzeichnis oder die Datei. Bei Verzeichnissen bedeutet das, dass Dateien hinzugefügt und gelöscht werden können. Bei Dateien stehen alle Funktionen zur Verfügung. Dazu gehört auch die Veränderung von Zugriffsberechtigungen.
- **Ändern** Die Berechtigungen sind im Vergleich mit dem Vollzugriff auf das Schreiben, Lesen, Ändern und Löschen beschränkt. Es können keine Berechtigungen erteilt werden.
- **Lesen, Ausführen** Für Programmdateien relevant, da diese ausgeführt werden dürfen.
- **Ordnerinhalt auflisten** (nur bei Verzeichnissen) Der Inhalt des Verzeichnisses kann angezeigt werden. Die Inhalte der Dateien im Verzeichnis können nicht angezeigt werden.
- **Lesen** Definiert, dass eine Datei gelesen, aber nicht ausgeführt werden darf.
- **Schreiben** Die Datei darf verändert, jedoch nicht gelöscht werden.

Der Assistent zum Erstellen von Freigaben

Über *Start/Ausführen/shrpubw* können Sie den Assistenten zur Erstellung von Freigaben starten (Abbildung 6.19). Auf dem nächsten Fenster des Assistenten können Sie den Ordner auswählen, den Sie im Netzwerk zur Verfügung stellen wollen. Auf der nächsten Seite legen Sie den Freigabenamen sowie die Offlineverfügbarkeit der Freigabe fest. Wenn eine Freigabe offline verfügbar ist, kann diese zum Beispiel mit Hilfe von Offlinedateien synchronisiert werden. Auf der letzten Seite des Assistenten legen Sie schließlich fest, welche Berechtigungen Anwender über das Netzwerk auf die Freigabe bekommen sollen. Über die Schaltfläche *Fertig stellen* wird die Freigabe schließlich erstellt.

Abbildg. 6.19 Erstellen einer Freigabe mit dem Assistenten für die Ordnerfreigabe

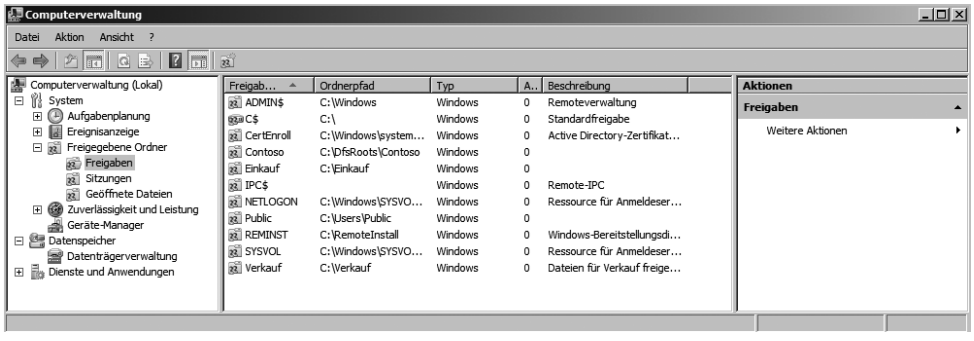


Anzeigen aller Freigaben

Sie können in der Computerverwaltung alle Freigaben Ihres Servers verwalten. Sie finden die Verwaltung der Freigaben über *Start/Verwaltung/Computerverwaltung*. Alternativ können Sie die Computerverwaltung über *Start/Ausführen/compmgmt.msc* starten. In der Computerverwaltung können Sie sich auch mit anderen Servern verbinden, zum Beispiel Core-Server, die lokal nicht über dieses Snap-In verfügen. Sie können die explizite Verwaltung der Freigaben eines Servers auch über *Start/Ausführen/fsmgmt.msc* öffnen. Im Bereich *Freigegebene Ordner* stehen Ihnen an dieser Stelle drei verschiedene Einträge zur Verfügung, über die Sie Freigaben verwalten und überprüfen können:

- **Freigaben** Wenn Sie auf diesen Eintrag klicken, werden Ihnen alle Freigaben angezeigt, die derzeit auf dem Computer verfügbar sind. Über das Kontextmenü zu diesem Eintrag können Sie neue Freigaben erstellen und über das Kontextmenü der einzelnen Freigaben lassen sich die Einstellungen der jeweiligen Freigabe konfigurieren.
- **Sitzungen** Über diesen Eintrag werden Ihnen alle aktuell über das Netzwerk verbundenen Benutzer angezeigt. Sie können die Benutzer per Klick mit der rechten Maustaste vom Server trennen
- **Geöffnete Dateien** Hier werden alle Dateien angezeigt, die derzeit von verbundenen Benutzern über Freigaben auf dem Server geöffnet sind. Hier können Sie die Dateien auch schließen.

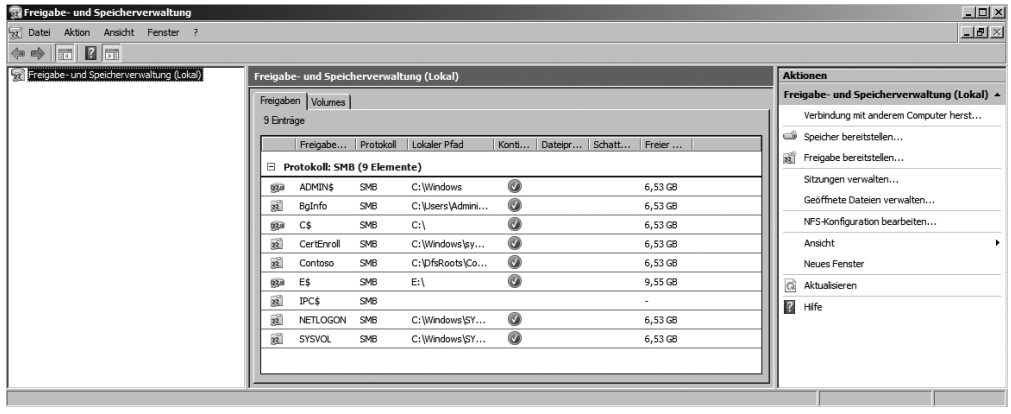
Abbildg. 6.20 Verwalten der Freigaben eines Servers



TIPP Eine Auflistung aller Freigaben erhalten Sie ebenfalls, wenn Sie den Kommandozeilenbefehl *net share* ausführen.

Ein weiteres wertvolles Werkzeug für die Verwaltung von Freigaben und deren zugrunde liegenden Laufwerke ist das neue Snap-In *Freigabe- und Speicherverwaltung*, mit dem Sie neben dem lokalen Server auch auf andere Server wie zum Beispiel Core-Server zugreifen können. Sie rufen die neue Verwaltungskonsole über *Start/Verwaltung/Freigabe- und Speicherverwaltung* auf oder indem Sie im Suchfeld des Startmenüs den Befehl *StorageMgmt.msc* eingeben.

Abbildg. 6.21 Verwalten von Freigaben und Laufwerken mit der *Freigabe- und Speicherverwaltung*



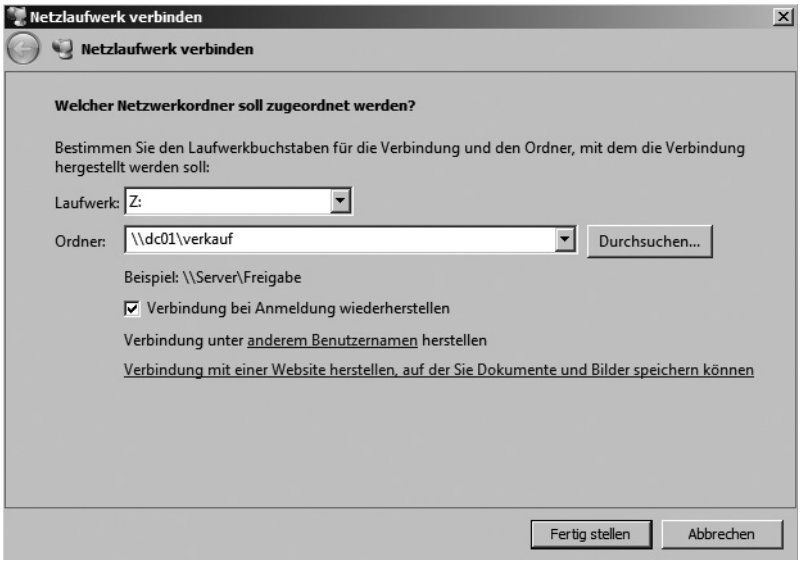
Auf Freigaben über das Netzwerk zugreifen

Damit die freigegebenen Dateien genutzt werden können, muss eine Verbindung zur Freigabe hergestellt werden. Dies kann direkt über die Angabe des UNC-Pfads (Universal Naming Convention) geschehen. Dieser Zugriff erfolgt zum Beispiel auf das Verzeichnis über \\<*Servername*>\<*Freigabe*>. Für Anwender wird in der Regel eine Verknüpfung mit einem Laufwerkbuchstaben hergestellt, sodass diese in der gewohnten Umgebung arbeiten können. Wenn Sie eine Freigabe eines Servers im Netzwerk als Laufwerk auf Ihrem PC verbinden wollen, gehen Sie am besten über die Startschaltfläche und klicken mit der rechten Maustaste auf *Netzwerk*. Wählen Sie im Kontextmenü den Eintrag *Netzlaufwerk zuordnen* aus. Geben Sie als Nächstes den Freigabenamen im Feld *Ordner* ein. Die Syntax dazu lautet \\<*Servername oder IP-Adresse*>\<*Name der Freigabe*>. Sie können zum Beispiel folgende Bezeichnung eingeben *dc01\einkauf* (Abbildung 6.22). Die Freigabe *c$* ist auf jedem Server oder PC vorhanden. Sie können diese Freigabe von einem anderen PC aus aber nur mit Administratorberechtigungen öffnen, daher heißt diese Freigabe auch Admin-Share (Admin-Freigabe). Wenn Sie auf *Fertig stellen* klicken, öffnet sich ein Anmeldefenster, in dem Sie die Authentifizierungsdaten eingeben müssen.

Ist der Server Mitglied einer Domäne, werden die Anmeldedaten des angemeldeten Benutzers verwendet. Wenn Sie sich am PC mit dem gleichen Benutzernamen und Kennwort anmelden, wie auf dem PC oder Server, auf dem Sie die Freigabe öffnen, müssen Sie keine Authentifizierung eingeben, auch dann nicht, wenn beide PCs in der gleichen Active Directory-Gesamtstruktur sind. Hier erkennt Windows Server 2008 automatisch, dass es sich um den entsprechenden Benutzer handelt. Wenn Sie allerdings von einem anderen Server im Netzwerk die *c$*-Freigabe öffnen wollen, erhalten Sie häufig ein Authentifizierungsfenster angezeigt, obwohl Sie an beiden Servern mit dem gleichen Benutzernamen und Kennwort angemeldet sind, beide Benutzer in der jeweiligen Administratorengruppe Mitglied sind und die Freigaben im Netzwerk- und Freigabecenter aktiviert wurden. Dieses Problem tritt aber nur zwischen Servern in verschiedenen Gesamtstrukturen auf, oder die nicht Mitglied einer Domäne sind. Ursache dafür ist, dass noch der Freigabe-Assistent aktiviert ist, der einen solchen Zugriff nicht gestattet. Um den Zugriff auf eine Freigabe über das Netzwerk, zum Beispiel *c$*, zu ermöglichen, deaktivieren Sie am besten diesen Assistenten. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie über *Start/Computer* ein Explorer-Fenster.
2. Wählen Sie aus dem Dropdown-Menü *Organisieren* die Option *Ordner- und Suchoptionen* aus.
3. Wechseln Sie zur Registerkarte *Ansicht*.
4. Deaktivieren Sie die Einstellung *Freigabe-Assistent verwenden*. Unter Windows Vista ist dieser standardmäßig aktiviert, unter Windows Server 2008 deaktiviert.
5. Melden Sie sich mit dem gleichen Benutzernamen und Kennwort an, oder authentifizieren Sie sich entsprechend.

Abbildg. 6.22 Verbinden eines Netzlaufwerkes



TIPP Geben Sie im Suchfeld des Startmenüs \\<*Servername*> ein, werden Ihnen alle Freigaben sowie die freigegebenen Drucker des Servers angezeigt. Dadurch können Sie per Doppelklick oder über das Kontextmenü sehr schnell den Inhalt von Netzwerkordnern anzeigen lassen.

Verwenden von *net use*

Eine weitere Möglichkeit, Netzlaufwerke zu verbinden, steht Ihnen über die Eingabeaufforderung mit dem Befehl *net use* zur Verfügung. Eine Befehlszeile öffnen Sie entweder über *Start/Ausführen/cmd* oder über die Tastenkombination Ä+R und Eingabe von *cmd*. Alternativ verwenden Sie die Verknüpfung im Startmenü. Dazu werden am häufigsten die folgenden Befehle verwendet:

- *net use* Zeigt alle derzeit verbundenen Netzlaufwerk an
- *net use <Laufwerksbuchstabe>: /del /yes* Trennt das angegebene Netzlaufwerk, zum Beispiel *net use z: /del /yes*. Durch Eingabe von */yes* muss nicht erst nochmals die Trennung bestätigt werden, was sinnvoll bei Anmeldeskripts ist. Wenn als Platzhalter das * verwendet wird, werden alle Netzlaufwerke auf einmal getrennt.

- *net use <Laufwerksbuchstabe>: \\<Server>\<Freigabename>* Durch Eingabe dieses Pfades wird das angegebene Netzlaufwerk verbunden, zum Beispiel *net use z: \\dc01\verkauf*. Wenn als Platzhalter * verwendet wird, wird der nächste freie Buchstabe als Laufwerksbuchstabe eingesetzt.
- Sie können den Befehl auch mit der Syntax *net use <Laufwerksbuchstabe>: \\<Server>\<Freigabename> <Benutzername> <Kennwort>* angeben, um ein Laufwerk mit Hilfe eines anderen Benutzers als dem derzeitig angemeldeten zu verbinden.

Robocopy – Robust File Copy Utility

Robocopy ist ein Kommandozeilen-Programm, welches ähnlich wie Xcopy funktioniert, aber deutlich mehr Möglichkeiten bietet. Das Tool gehörte bei Windows Server 2003 noch zu den Ressource Kit Tools, ist aber in Windows Server 2008 fest integriert. Mit Robocopy sind sehr komplexe Dateireplizierungsaufgaben möglich. Zum Beispiel können Sie mit Robocopy vollständig gespiegelte Duplikate von zwei Dateistrukturen einschließlich aller Unterverzeichnisse und Dateien anlegen, ohne dass dabei unnötige Dateien kopiert werden müssten. Nur neue und aktualisierte Dateien am Quellspeicherort werden kopiert. Robocopy unterstützt außerdem alle verbundenen Dateiinformationen, einschließlich der Datums- und Zeitstempel, Sicherheitszugriffssteuerungslisten (Access Control Lists, ACL) und vieles mehr.

In diesem Abschnitt wird Ihnen auch das Tool *CopyRite XP* erläutert, welches eine kostenlose grafische Oberfläche für *robocopy.exe* bereitstellt. Vor allem für kleinere Unternehmen kann die Datensicherung per Skript über *robocopy.exe* sehr effizient sein und wird auch schon bei vielen Unternehmen praktiziert. Mit dem Tool lassen sich ohne großen Aufwand sehr effiziente Backupstrategien erstellen. Robocopy unterstützt das Logging in Protokolldateien, kann allerdings nicht auf Bandlaufwerke zugreifen, sondern ist hauptsächlich für die Datensicherung auf externe Festplatten oder Netzlaufwerke gedacht. Robocopy kann auch Windows-Berechtigungen kopieren und Dateien verschieben, nicht nur kopieren. Robocopy verfügt über eine Vielzahl von Optionen und kann zum Beispiel per Skript ein Verzeichnis mit einem anderen abgleichen. Es ist auch möglich, nur veränderte Dateien zu kopieren und gelöschte Dateien des einen Verzeichnisses auf dem anderen zu löschen.

Mit diesen Möglichkeiten können kleinere oder auch mittlere Unternehmen ihren Dateiserver schnell und leicht spiegeln, und so Datenverlust vorbeugen, unabhängig von einem Datensicherungskonzept. Robocopy kann Verzeichnisse mit Unterverzeichnissen kopieren und dabei einzelne Dateien ausschließen. Robocopy kann Zeitstempel der Dateien auslesen und so auf Basis des Erstellungs- oder Änderungsdatums Dateien kopieren oder auch löschen. Wenn Sie häufig ein Verzeichnis über das Netzwerk spiegeln wollen, lässt sich mit Robocopy deutlich Zeit sparen, da Sie zum Beispiel nur veränderte Dateien kopieren müssen und bereits vorhandene einfach übergehen können.

Befehlszeilen-Referenz von Robocopy

Wenn Sie mit Robocopy arbeiten, müssen Sie die Datei *Robocopy.exe* auf den Server oder die Arbeitsstation kopieren, auf der Sie den Job erstellen wollen oder die Batchdatei liegt, welche Robocopy verwendet. In Windows Server 2008 und Windows Vista ist das Programm nach der Installation bereits vorhanden. Es werden keine weiteren Dateien benötigt. Die Befehlszeile von Robocopy sieht folgendermaßen aus:

Robocopy <Quelle> <Ziel>< Datei(en)>/< Option>

Platzhalter sind erlaubt. Wenn keine Dateien oder Platzhalter eingegeben werden, verwendet Robocopy standardmäßig (*.*), kopiert also alle Dateien. Quelle und Ziel können ein Verzeichnis, ein Laufwerk oder auch ein UNC-Pfad sein *(\\<SERVER>\<FREIGABE>)*. Die Optionen werden hinter dem Befehl angehängt. Sie können beliebig viele Optionen miteinander kombinieren:

Tabelle 6.1 Aufrufoptionen von Robocopy

Option	Funktion
/S	Kopiert Unterverzeichnisse (außer leere Verzeichnisse)
/E	Kopiert Unterverzeichnisse (auch leere Verzeichnisse)
/LEV:n	Kopiert nur bis zu einer Verzeichnistiefe von *n*. Die restlichen Verzeichnisse werden nicht kopiert.
/Z	Wenn der Kopiervorgang unterbrochen wird, können Sie mit dieser Option an der Stelle weitermachen, an der abgebrochen wurde. Es können aber nicht alle Dateien kopiert werden.
/B	Dateien werden im Backup-Modus kopiert. Es werden also alle Dateien kopiert, auch diejenigen mit denen die Option */Z* Probleme hat.
/ZB	Es wird zunächst die Option */Z* probiert. Schlägt das bei einer Datei fehl, verwendet Robocopy die Option */M*.
/COPY:copyflags	Kopiert nur die Dateiattribute, die definiert werden. Dazu muss das Dateisystem auf dem Quell- und dem Zielverzeichnis im NTFS-Format formatiert sein. D – Daten S – Sicherheit (NTFS ACLs) A – Attribute O – Besitzer-Informationen T – Zeitstempel U – Informationen zur Überwachung Standardmäßig kopiert Robocopy nur mit der Option /COPY:DAT. Überwachung, Sicherheit und Datenbesitzer werden standardmäßig nicht kopiert.
/COPYALL	Kopiert alles, also wie */COPY:DATSOU* (s.o.)
/NOCOPY	Es wird nichts kopiert (nur sinnvoll für Spiegelung, wenn gelöscht werden soll)
/SEC	Entspricht dem Schalter */COPY:DATS*. Sicherheitsinformationen und ACLs werden kopiert.
/MOV	Löscht nach dem Kopieren die Quelldatei
/MOVE	Verschiebt Dateien und Verzeichnisse
/PURGE	Löscht Dateien und Verzeichnisse im Ziel-Verzeichnis, die auf dem Quell-Verzeichnis nicht mehr vorhanden sind
/MIR	Spiegelt ein komplettes Verzeichnis. Löscht also auch Dateien im Ziel, die in der Quelle nicht mehr vorhanden sind.
/A+:{R|A|S|H|N|T}	Ändert die Dateiattribute beim Kopieren: R – Read only S – System N – Not content indexed A – Archive H – Hidden T – Temporary

Tabelle 6.1 Aufrufoptionen von Robocopy *(Fortsetzung)*

Option	Funktion
/A-:{R|A|S|H|N|T}	Löscht die definierten Attribute beim Kopieren: R – Read only S – System N – Not content indexed A – Archive H – Hidden T – Temporary
/CREATE	Erstellt leere Verzeichnisse, wenn in der Quelle auch vorhanden
/FAT	Ändert die Dateinamen ab, damit sie dem 8.3-Format entsprechen, also maximal acht Zeichen vor und drei nach dem Punkt
/FFT	Kopiert auf Systeme, die nur kompatibel zu NTFS sind, aber eigentlich nur das FAT-Dateisystem beherrschen (wird eher selten benötigt)
/MON:n	Zählt die Änderungen von Dateien im Quell-Verzeichnis mit und startet nach *n* Änderungen den Kopiervorgang nach dem Zeitraum, der mit /MOT (s.u.) definiert wird
/MOT:n	Führt den Kopiervorgang nach *n* Minuten wieder aus. In Kombination mit */MON* möglich.
/RH:hhmm-hhmm	Definiert, innerhalb welcher Zeit kopiert werden darf. Die Werte sind in 24 Stunden angegeben und müssen im Format 0000 bis 2359 eingegeben werden.
/PF	Die Option ist optimal, wenn ein laufender Kopiervorgang über den mit */RH* definierten Zeitraum hinausgeht. Der Kopiervorgang kann so schneller abgeschlossen werden.
/IPG:n	Mit dieser Option wird nach 64 KB *n* Millisekunden gewartet, bevor weiterkopiert wird. Vor allem für Kopiervorgänge zwischen Niederlassungen kann so die Bandbreite eingespart werden.
/IA:{R|A|S|H|C|N|E|T|O}	Kopiert nur Dateien mit den definierten Attributen: R – Read only A – Archive S – System H – Hidden C – Compressed N – Not content indexed E – Encrypted T – Temporary O – Offline
/XA:{R|A|S|H|C|N|E|T|O}	Kopiert keine Dateien mit den definierten Attributen: R – Read only A – Archive S – System H – Hidden C – Compressed N – Not content indexed E – Encrypted T – Temporary O – Offline
/A	Kopiert nur Dateien, in denen die Eigenschaft *Archiv* gesetzt wurde (kann man über die Eigenschaften einer Datei durchführen)
/M	Wie */A*, allerdings wird das Archiv-Attribut in der Quell-Datei zurückgesetzt
/XF file [file]	Kopiert diese Dateien nicht. Sie können mehrere hintereinander schreiben
/XD dir [dir]	Kopiert diese Verzeichnisse nicht
/XC	Schließt Dateien aus, die im Quell-Verzeichnis als »geändert« markiert sind
/XN	Kopiert keine Dateien, die im Quell-Verzeichnis als neuer deklariert sind
/XO	Wie */XN*, nur werden Dateien nicht kopiert, die im Quell-Verzeichnis als älter definiert sind
/MAX:n	Dateien, die größer als *n* Bytes sind, werden nicht kopiert (Achtung, nicht Kilobytes)

Tabelle 6.1 Aufrufoptionen von Robocopy *(Fortsetzung)*

Option	Funktion
/MIN:n	Kopiert keine Dateien, die kleiner als *n* Bytes sind
/MAXAGE:n	Kopiert keine Dateien, die älter als *n* Tage sind. Sie können *n* auch als Datum in der Form von YYYYMMDD angeben.
/MINAGE:n	Kopiert keine Dateien, die neuer sind. Syntax wie oben.
/MAXLAD:n	Kopiert keine Dateien, auf die vor *n* Tagen nicht zugegriffen wurde (Syntax s.o.)
/MINLAD:n	Wie */MAXLAD*, nur nach *n* Tagen, also neuere Dateien
/R:n	Definiert die maximalen Fehler, die beim Kopieren übergangen werden (standardmäßig 1 Mio.)
/W:n	Definiert die Sekunden, die gewartet wird, wenn ein Kopiervorgang nicht erfolgreich war, um es erneut zu versuchen
/REG	Speichert */R* und */W* in der Registry als Standardwert für weitere Robocopy-Jobs
/L	Gibt nur eine Liste der Dateien aus, führt aber keinen Kopiervorgang durch
/TS	Zeigt den Zeitstempel der Quell-Dateien im Logfile an
/FP	Zeigt den vollen Pfadnamen in der Logdatei
/NS	Zeigt nicht Datei- und Verzeichnisgröße in der Logdatei an
/NFL	Loggt keinen Kopiervorgang außer Fehler
/NP	Zeigt den Fortschritt des Kopiervorgangs bei großen und kleinen Dateien nicht an (%-Angabe)
/ETA	Zeigt die Dauer der Kopiervorgänge an
/LOG:file	Speichert das Log in der definierten Datei
/LOG+:file	Hängt das Log an einer bereits bestehenden Logdatei an
/TEE	Zeigt die Vorgänger auch in der Kommandozeile an, nicht nur im Log
/JOB:job	Liest die Parameter von einer Job-Datei aus
/SAVE:job	Speichert die Parameter in einer Job-Datei
/QUIT	Führt nichts aus. Zeigt in Verbindung mit dem Job-Schalter den Inhalt der Job-Datei an.

Anmerkungen zum Umgang mit Robocopy

Wenn der Kopiervorgang einer Datei aus irgendwelchen Gründen fehlschlägt (beispielsweise ist die Datei in Benutzung oder der Zugriff wurde verweigert), führt Robocopy innerhalb eines definierten Zeitraums einige weitere Versuche durch, um den Kopiervorgang noch erfolgreich abzuschließen. Robocopy wartet standardmäßig 30 Sekunden und 1 Mio. Versuche, um den Kopiervorgang durchzuführen. Diese beiden Werte lassen sich mit den Optionen */W* und */R* steuern, sowie mit */REG* als Standard in der Registry festlegen. Bei jedem Vorgang werden die Optionen */W* und */R* zunächst verwendet, bevor der Standard aktiv wird. Sind in der Befehlszeile */R* und */W* nicht gesetzt, greifen die Standardwerte.

Wenn Sie Datei- oder Verzeichnisnamen kopieren wollen, die ein Leerzeichen beinhalten, geben Sie den Pfad in Anführungszeichen an, zum Beispiel *Robocopy "\fs01\einkauf\lieferanten 2007" \fs01\archiv\einkauf*. Alle Optionen werden von links nach rechts gelesen und ausgeführt. Experimentieren Sie zunächst ein bisschen mit den Optionen in einer Testumgebung oder zumindest mit einem Testverzeichnis, um das für Sie optimale Ergebnis herauszuholen. Nach meiner Erfahrung verwenden die meisten Administratoren die Option */MIR*, weil so schnell und einfach ein Spiegel eines File-Servers, oder eines wichtigen Verzeichnisses angelegt wird. So kommen Sie schnell an fehlerhaft gelöschte oder veränderte Dateien, und müssen nicht zuerst mit Ihrem Datensicherungsgerät Bänder einlesen und komplizierte Wiederherstellungsvorgänge starten.

TIPP Um die Daten in einer Freigabe auf einen anderen Rechner zu spiegeln, schreiben Sie am besten ein Skript mit dem Befehl *robocopy <Quell-Verzeichnis <Sicherungs-Laufwerk>:\ <Sicherungs-Verzeichnis> /mir*. Mit dem *Befehl robocopy c:\users\thomas\documents y:\backup /mir* werden die Verzeichnisse und Dateien aus einem Dokumenten-Verzeichnis auf das Laufwerk *Y:* in das Verzeichnis *backup* kopiert.

Die Option */mir* von Robocopy kopiert nur geänderte Dateien. Das heißt, der erste Kopiervorgang dauert recht lange, da erst alle Dateien kopiert werden müssen. Der zweite geht aber deutlich schneller, da nur geänderte Dateien kopiert werden. Löschen Sie im Quell-Verzeichnis eine Datei, wird diese auch im Backup-Verzeichnis gelöscht. So erhalten Sie immer eine 1:1-Kopie Ihrer wichtigsten Daten. Sie können ohne weiteres auch mehrere Verzeichnisse sichern. Verwenden Sie in diesem Fall einfach öfters den Befehl nacheinander in der Datei.

Auch wenn die Oberfläche von Robocopy nicht so schick aussieht, wie von vielen Datensicherungsprogrammen oder Synchronisierungstools, haben Sie den Vorteil, dass über diesen Befehl die Sicherung deutlich schneller abläuft wie mit jedem anderen Tool. Anstatt mit Laufwerksbuchstaben können Sie auch mit Freigabenamen arbeiten.

Grafische Oberflächen für Robocopy – CopyRite XP und Robocopy GUI

Da die Bedienung von Robocopy durch die vielen möglichen Optionen nicht sehr trivial ist, bietet das kostenlos erhältliche Tool *CopyRite XP* eine enorme Hilfe. Bei *CopyRite XP* handelt es sich um eine grafische Oberfläche für Robocopy. Sie können die ältere Version 1.1 kostenlos aus dem Internet herunterladen. Geben Sie dazu in Google einfach die Bezeichnung *CopyRite* ein. Die aktuelle Version des Programms kostet in etwa 10 US-Dollar und kann von der Internetseite *http://www.wintotal.de/softw/index.php?rb=43&id=2339* bezogen werden. Das Tool enthält allerdings nicht die notwendige Datei *robocopy.exe*. Diese muss in das Installationsverzeichnis von *CopyRite XP* manuell kopiert werden.

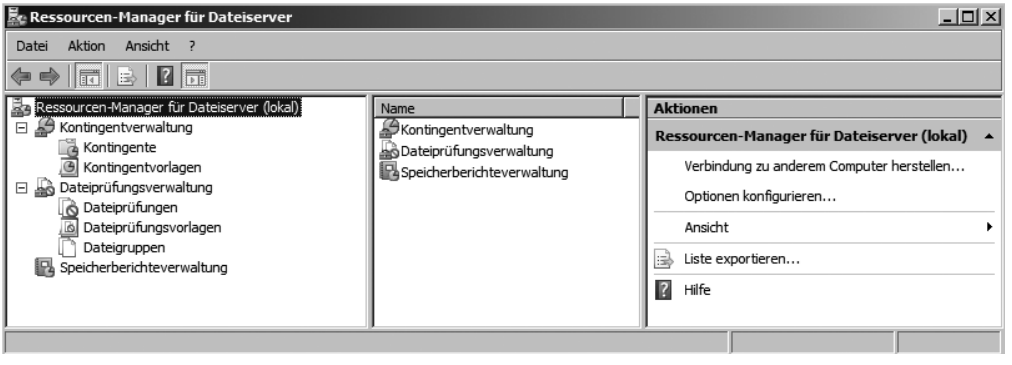
Ein weiteres Tool, welches eine grafische Oberfläche für Robocopy liefert, ist Robocopy GUI, welches Microsoft kostenlos auf der Internetseite *http://download.microsoft.com/download/f/d/0/fd05def7-68a1-4f71-8546-25c359cc0842/UtilitySpotlight2006_11.exe* zur Verfügung stellt. In dem Tool können die Quell- und Zielpfade sowie alle gewünschten benutzerdefinierten Optionen oder Filter angegeben werden. Robocopy GUI erweitert außerdem die Funktionalität des klassischen Robocopy. Durch die Multithreading-Fähigkeit können Sie ein Robocopy-Skript erstellen und ausführen. Parallel können Sie mit der Entwicklung eines anderen Skripts beginnen, während das erste Skript immer noch läuft. Sie können Skripts auch speichern. Die wichtigste Funktion besteht darin, dass Sie mit der Robocopy GUI die eigenen Standardeinstellungen abspeichern können. Robocopy

GUI beinhaltet darüber hinaus eine eigene Hilfedatei sowie eine integrierte Kopie des vollständigen Robocopy-Referenzhandbuchs. Diese Referenz enthält einen vollständigen Index aller Robocopy-Befehle und der gesamten Syntax.

Ressourcen-Manager für Dateiserver

Eine weitere Neuerung in Windows Server 2003 R2, die für Windows Server 2008 weiterentwickelt wurde, ist der neue *Ressourcen-Manager für Dateiserver (Fileserver Resource Manager, FSRM)*. Mit diesem Tool lassen sich an zentraler Stelle alle Dateiserver eines Unternehmens konfigurieren und Datenträger-Kontingente (Quotas) steuern. Sie können Anwender daran hindern, unerwünschte Dateien auf den Servern abzulegen, zum Beispiel MP3-Dateien oder Bilder. Mit dem FSRM können Sie detaillierte Berichte und Vorlagen für Quotas erstellen. Starten können Sie den Ressourcen-Manager für Dateiserver über die Programmgruppe *Verwaltung* oder *Start/Ausführen/fsrm.msc*.

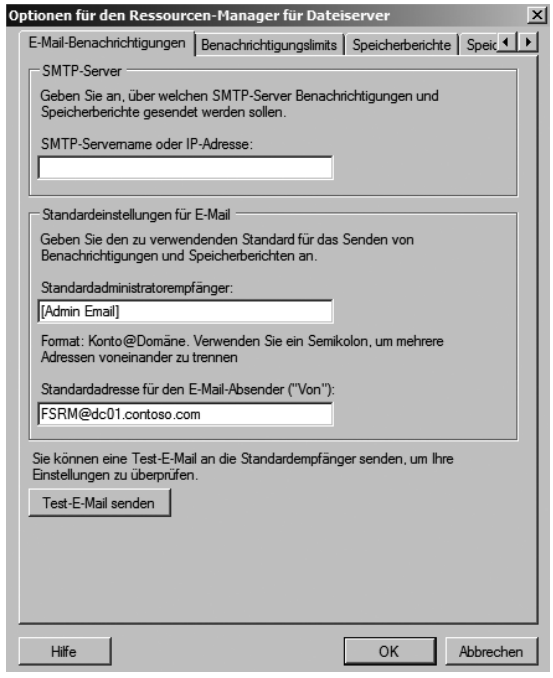
Abbildg. 6.23 Verwalten von Dateiservern mit dem neuen Ressourcen-Manager für Dateiserver



Nachdem Sie das Programm gestartet haben, können Sie mit dem Befehl *Optionen konfigurieren* im Kontextmenü des Eintrags *Ressourcen-Manager für Dateiserver* detaillierte Benachrichtigungen und Berichte erstellen lassen. Vor allem die E-Mail-Adressen der Administratoren sollten konfiguriert werden, damit die später konfigurierten Berichte und Warnungen auch zugestellt werden können. Wenn Sie die Administratoren eingetragen haben, sollten Sie zunächst mit der Schaltfläche *Test-E-Mail senden* überprüfen, ob die E-Mail beim gewünschten Empfänger ankommt.

HINWEIS Wenn ein Benutzer mehrmals versucht, eine blockierte Datei oder eine Datei, die die Kontingentgrenze überschreitet, zu speichern, und wenn für dieses Dateiprüfungs- bzw. Kontingentereignis eine E-Mail-Benachrichtigung konfiguriert ist, dann wird für einen Zeitraum von 60 Minuten nur eine einzige E-Mail an den Administrator gesendet. Auf diese Weise wird verhindert, dass das E-Mail-Konto des Administrators mit Nachrichten überschwemmt wird.

Abbildg. 6.24 Verwalten der Benachrichtigungsoptionen für den Ressourcen-Manager für Dateiserver



Kontingentverwaltung mit dem FSRM

Mit einem Kontingent können Sie beispielsweise festlegen, dass ein Benutzer nur maximal 100 MB auf seinem Home-Laufwerk speichern kann. Sie können mit Hilfe des FSRMs eine automatische E-Mail an Administratoren und den Benutzer senden, damit dieser rechtzeitig Daten auf seinem Laufwerk löschen kann. Sie können auch Benachrichtigungen konfigurieren, ohne dass ein Kontingent gesetzt wird. Wenn Sie den Konsoleneintrag *Kontingentverwaltung* erweitern, stehen Ihnen die Konfiguration von Kontingenten und von Kontingentvorlagen zur Verfügung. An dieser Stelle können Sie für einzelne Freigaben oder ganze Datenträger Kontingente festlegen, also Speichergrenzen, die von den Anwendern nicht überschritten werden dürfen.

Beispiele:

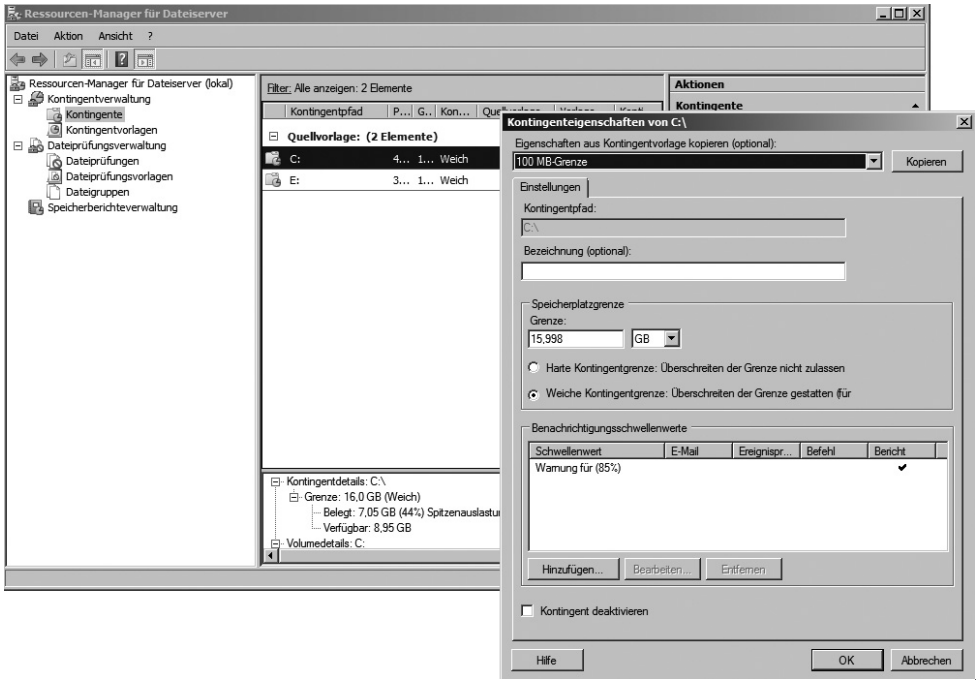
- Sie können eine Grenze von 200 MB für den persönlichen Ordner eines Benutzers auf einem Server festlegen und bestimmen, dass Sie und der Benutzer benachrichtigt werden, wenn 180 MB Speicherplatz überschritten wurden.
- Für den gemeinsam verwendeten Ordner einer Gruppe kann ein flexibles Kontingent von 500 MB festgelegt werden. Wird diese Speicherbeschränkung erreicht, werden alle Benutzer in der Gruppe per E-Mail benachrichtigt, dass das Speicherkontingent temporär auf 520 MB erweitert wurde.
- Sie können festlegen, dass Sie eine Benachrichtigung erhalten, wenn die Auslastung eines Ordners 2 GB erreicht, ohne jedoch das Kontingent dieses Ordners zu beschränken, da dieses erforderlich ist, um einen Dienst auf dem Server auszuführen.

Erstellen von Kontingenten und Kontingentvorlagen

Kontingente können aus einer Vorlage oder individuell erstellt werden. Wenn Sie Kontingente aus Vorlagen erstellen, können Sie die Kontingente zentral verwalten, indem Sie statt der einzelnen Kontingente die Vorlagen konfigurieren. Sie können Änderungen auf alle Kontingente anwenden:

- Um ein neues Kontingent zu erstellen, klicken Sie im Knoten *Kontingentverwaltung* mit der rechten Maustaste auf den Eintrag *Kontingente* und wählen im Kontextmenü den Befehl *Kontingent erstellen* aus.
- Wählen Sie unter *Kontingentpfad* den Pfad zu dem Ordner aus, für den das Kontingent gelten soll, oder geben Sie den Pfad ein. Die Erstellung von Kontingentvorlagen läuft genauso ab, wie die Erstellung eines Kontingents. *Kontingentvorlagen* können als Vorlagen für verschiedene Kontingente verwendet werden. Um ein Kontingent basierend auf einer Vorlage zu erstellen, wählen Sie unter *Kontingentvorlagen* die Vorlage aus, auf der das neue Kontingent basieren soll. Klicken Sie dann mit der rechten Maustaste auf die Vorlage und wählen Sie im Kontextmenü den Befehl *Kontingent mithilfe einer Vorlage erstellen*.
- Um eine Kontingentvorlage als Basis für das Kontingent zu verwenden, wählen Sie im Dialogfeld *Kontingent erstellen* die Option *Eigenschaften aus dieser Kontingentvorlage übernehmen* aus und legen dann über das zugehörige Listenfeld die Vorlage aus. Alle Vorlageneigenschaften werden unter *Zusammenfassung der Kontingenteigenschaften* angezeigt.

Abbildg. 6.25 Erstellen eines Kontingents basierend auf einer Vorlage



- Klicken Sie anschließend auf *Erstellen*.

Nach der Erstellung wird das Kontingent im FSRM angezeigt, wenn Sie auf der linken Seite auf den Eintrag *Kontingente* klicken. Wenn Sie ein neues Kontingent erstellen, können Sie bei der Erstellung die Option *Vorlage autom. anwenden, Kontingente in Unterordnern erstellen* aktivieren. Sobald in dem konfigurierten Ordner ein neuer Unterordner erstellt wird, zum Beispiel wenn Sie mit servergespeicherten Profilen arbeiten, wird dieses Kontingent diesem Unterordner automatisch zugewiesen.

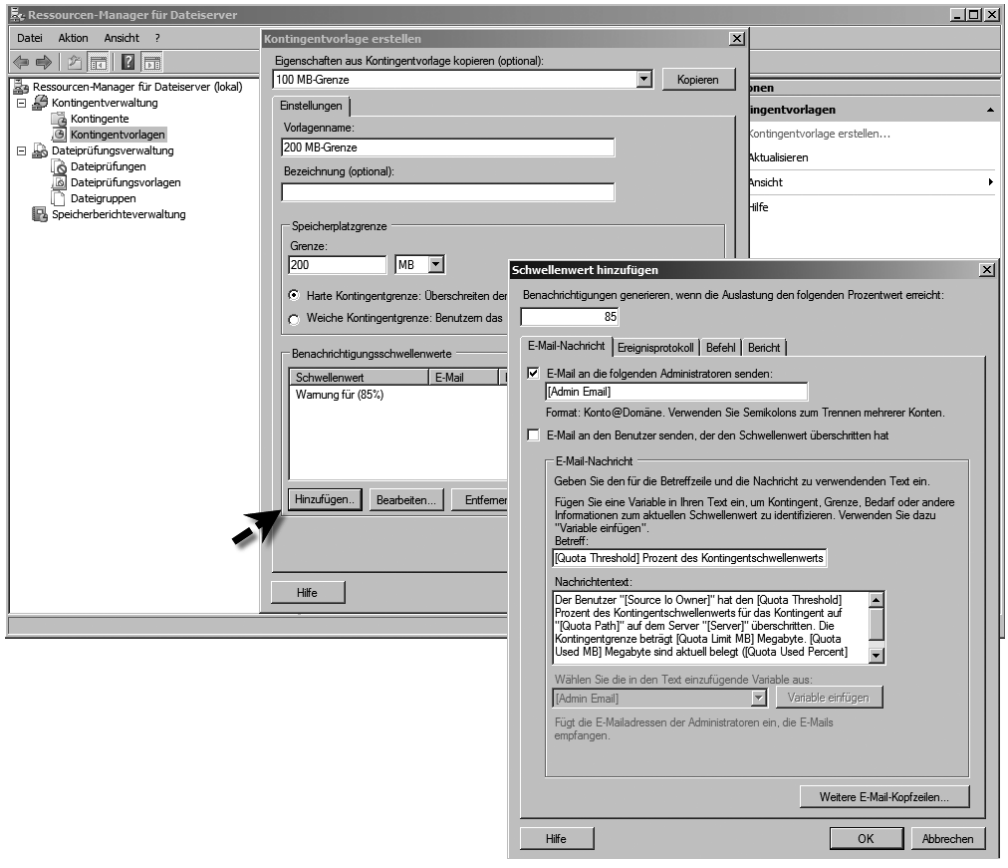
Sie können einer Vorlage durch Klicken auf die Schaltfläche *Hinzufügen* verschiedene Schwellenwerte und damit verbundene Aktionen, wie die Ereignisprotokollierung oder das Senden von E-Mails zuweisen. Sie können an dieser Stelle den Text der E-Mails konfigurieren, die vorhandenen Vorlagen bearbeiten oder neue Vorlagen erstellen (Abbildung 6.26). Bei der Erstellung von Kontingentvorlagen können Sie harte oder weiche Grenzen festlegen. Bei harten Grenzen werden beim Überschreiten der Grenze die Schreibrechte des Anwenders aufgehoben, sodass er keine weiteren Dateien mehr in diesem Verzeichnis speichern kann. Bei einer weichen Grenze ist das Speichern weiterhin möglich, es werden aber Benachrichtigungsaktionen ausgelöst. Benachrichtigungsschwellenwerte bestimmen, was passiert, wenn die Kontingentgrenze erreicht wird. Sie können E-Mail-Benachrichtigungen senden, ein Ereignis protokollieren, einen Befehl oder ein Skript ausführen oder Berichte generieren. Standardmäßig werden keine Benachrichtigungen generiert. Um Benachrichtigungen zu konfigurieren, die bei Erreichen der Kontingentgrenze generiert werden, markieren Sie in der Liste *Benachrichtigungsschwellenwerte* den Schwellenwert und klicken auf *Bearbeiten*. Um E-Mail-Benachrichtigungen zu konfigurieren, legen Sie auf der Registerkarte *E-Mail-Nachricht* die folgenden Optionen fest:

- Aktivieren Sie das Kontrollkästchen *E-Mail an die folgenden Administratoren senden*, und geben Sie die E-Mail-Adressen der Administratorkonten ein, die Benachrichtigungen erhalten sollen. Trennen Sie mehrere Konten durch Semikolons voneinander.
- Um den Anwender selbst zu kontaktieren, aktivieren Sie das Kontrollkästchen *E-Mail an den Benutzer versenden, der den Schwellenwert überschritten hat*.
- Der Text in eckigen Klammern fügt Variableninformationen zu dem Kontingentereignis ein, das die Benachrichtigung verursacht hat. Die Variable *[Source Io Owner]* fügt beispielsweise den Namen des Benutzers oder der Anwendung ein, von dem die Datei auf den Datenträger geschrieben wurde. Klicken Sie auf die Schaltfläche *Variable einfügen*, um weitere Variablen in den Text einzufügen.

Um einen Eintrag im Ereignisprotokoll zu protokollieren, aktivieren Sie auf der Registerkarte *Ereignisprotokoll* das Kontrollkästchen *Warnung an Ereignisprotokoll senden*. Wollen Sie einen Befehl oder ein Skript auszuführen, aktivieren Sie auf der Registerkarte *Befehl* das Kontrollkästchen *Diesen Befehl oder dieses Skript ausführen*, und geben Sie den Befehl ein. Wollen Sie die automatische Generierung von Speicherberichten festlegen, aktivieren Sie auf der Registerkarte *Bericht* das Kontrollkästchen *Berichte generieren*, und wählen Sie aus, welche Berichte generiert werden sollen. Nachdem Sie die Benachrichtigungstypen konfiguriert haben, die generiert werden sollen, klicken Sie auf *OK*, um den Schwellenwert zu speichern. Um weitere Benachrichtigungsschwellenwerte zu konfigurieren, klicken Sie im Bereich *Benachrichtigungsschwellenwerte* auf *Hinzufügen*. Geben Sie oben im Dialogfeld *Schwellenwert hinzufügen* den Prozentsatz der Kontingentgrenze ein, bei dem Benachrichtigungen generiert werden sollen. Der Standardschwellenwert für die erste Benachrichtigung liegt bei 85 Prozent.

HINWEIS Um E-Mail-Benachrichtigungen zu senden und die Speicherberichte zu konfigurieren, müssen Sie zunächst die allgemeinen Optionen des Ressourcen-Managers für Dateiserver konfigurieren, wie zu Beginn des Abschnittes besprochen.

Abbildg. 6.26 Erstellen einer Kontingentvorlage



Anpassen von Kontingentvorlagen

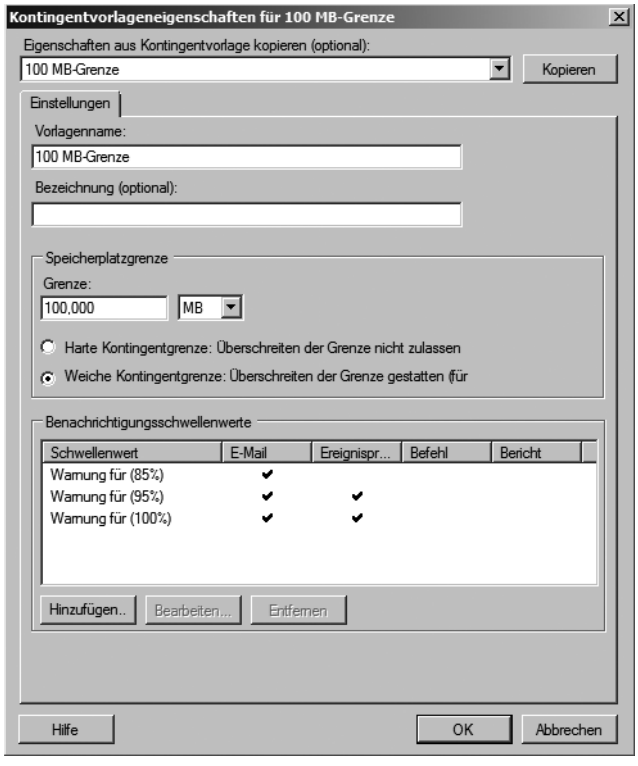
Sie können die Eigenschaften der vorhandenen oder von Ihnen erstellten Kontingentvorlagen jederzeit bearbeiten, wenn Sie auf der entsprechenden Vorlage einen Doppelklick ausführen. Wenn Sie eine Vorlage ändern und die Änderung abspeichern, erscheint ein neues Fenster mit verschiedenen Optionen:

- **Vorlage nur auf abgeleitete Kontingente anwenden** Mit dieser Option werden alle Kontingente mit den neuen Einstellungen der Vorlage überschrieben, wenn die Kontingente noch den Einstellungen der Originalvorlage entsprechen, also nicht nachträglich verändert wurden.
- **Vorlage auf alle abgeleiteten Kontingente anwenden** Mit dieser Option werden alle Änderungen der Vorlage auf die Kontingente übertragen, die mit der Vorlage erstellt wurden, unabhängig davon, ob in den einzelnen Kontingenten nach der Erstellung Einstellungen geändert wurden. Wenn Sie auswählen, die Änderungen an allen Kontingenten vorzunehmen, die von der Originalvorlage abgeleitet sind, werden alle von Ihnen erstellten benutzerdefinierten Kontingenteigenschaften überschrieben.

- **Vorlage nicht auf abgeleitete Kontingente anwenden** Wenn Sie diese Option wählen, werden die Änderungen der Vorlage nicht auf die bereits erstellten Kontingente übertragen, sondern nur auf neue Kontingente angewendet, die Sie mit der Vorlage erstellen.

Die gleichen Optionen stehen Ihnen zur Verfügung, wenn Sie ein automatisch erstelltes Kontingent bearbeiten.

Abbildg. 6.27 Bearbeiten einer Kontingentvorlage



HINWEIS Entsprechen die Werte *Verwendet* und *Verfügbar* für einige erstellte Kontingente nicht der tatsächlichen Einstellung für *Grenze*, könnte die Ursache ein verschachteltes Kontingent sein. Dabei handelt es sich bei dem Kontingent, das für einen Ordner gilt, um ein restriktiveres Kontingent, das von einem seiner übergeordneten Ordner abgeleitet ist. Wechseln Sie in diesem Fall im Knoten *Kontingentverwaltung* zu *Kontingente*, und wählen Sie dann den Kontingenteintrag mit dem Problem aus. Klicken Sie im Aktionsbereich auf *Kontingente anzeigen, die sich auf Ordner auswirken*, und suchen Sie nach Kontingenten, die auf übergeordnete Ordner angewendet sind. So können Sie identifizieren, welche Kontingente restriktive Einstellungen für das ausgewählte Kontingent haben.

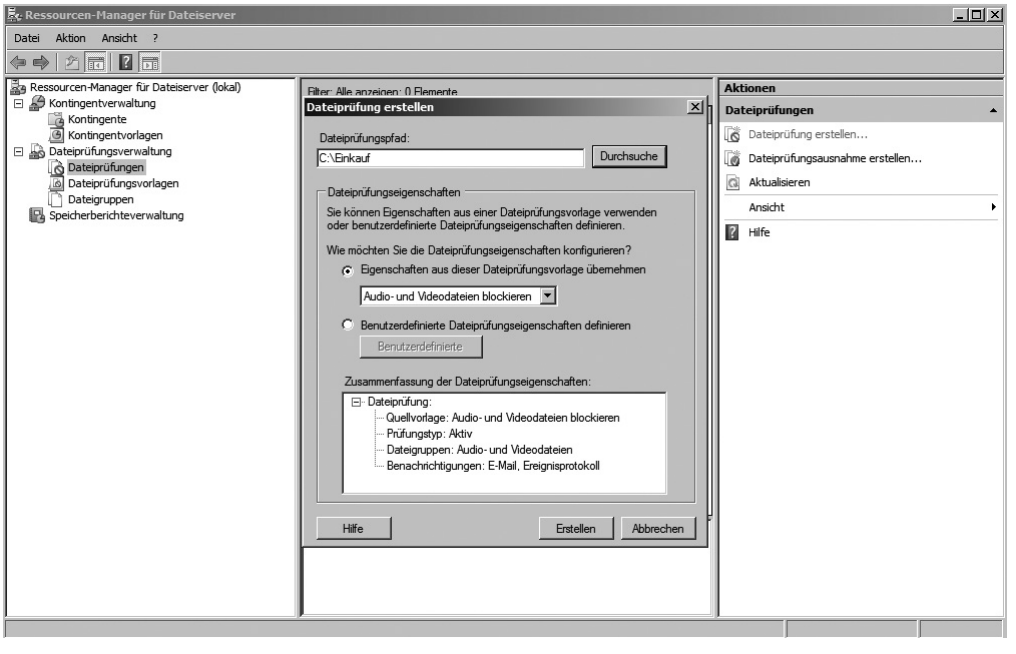
Dateiprüfungsverwaltung im FSRM

Über den Konsoleneintrag *Dateiprüfungsverwaltung* im Ressourcen-Manager für Dateiserver können Sie Dateiprüfungen erstellen, um zu steuern, welche Dateitypen von Benutzern gespeichert werden können, und um Benachrichtigungen zu senden, wenn Benutzer versuchen, blockierte Dateien zu speichern. Sie können zum Beispiel sicherstellen, dass keine Musikdateien, Bilder oder Videos in persönlichen Ordnern auf einem Server gespeichert werden, können jedoch die Speicherung bestimmter Arten von Mediendateien zulassen, die die Rechteverwaltung unterstützen oder den Unternehmensrichtlinien entsprechen. Speziellen Anwendern im Unternehmen können dagegen besondere Privilegien zum Speichern beliebiger Dateien in seinem persönlichen Ordner gewährt werden. Mit diesem Feature des FSRM können Sie also Ihren Anwendern das Speichern von bestimmten Dateianhängen wie zum Beispiel **.mp3*, **.mpeg* oder **.wmv* untersagen. Versucht ein Anwender, eine solche Datei zu speichern, können Sie Benachrichtigungen konfigurieren, die automatisch verschickt werden.

Erstellen einer Dateiprüfung

Wenn Sie im FSRM den Eintrag *Dateiprüfungen* mit der rechten Maustaste anklicken, können Sie eine neue Dateiprüfung erstellen. Ähnlich wie bei den Kontingenten müssen Sie einen Pfad festlegen, auf dem die Dateiprüfung aktiviert ist. Sie können die Prüfung anhand einer Vorlage erstellen oder eine benutzerdefinierte Prüfung erstellen. In beiden Fällen können Sie konfigurieren, dass die Anwender daran gehindert werden, die Dateien zu speichern (aktive Prüfung). Sie können den Anwendern allerdings auch das Speichern erlauben, aber dennoch eine Aktion zur Überwachung konfigurieren (passive Prüfung).

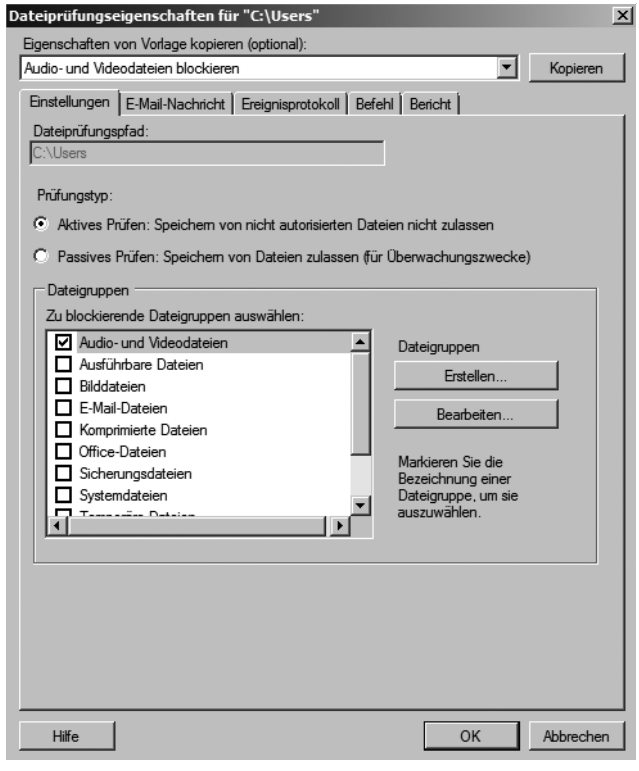
Abbildg. 6.28 Erstellen einer Dateiprüfung für Dateiserver



HINWEIS Wenn im geprüften Pfad einer Dateiprüfung bereits Dateien gespeichert sind, die blockiert werden sollen, hindert die Dateiprüfung Anwender nicht am Zugriff. Erst das Speichern nach der aktivierten Dateiprüfung wird verhindert und überwacht.

Wie bei den Kontingenten können Sie auch für die Dateiprüfungen eigene Vorlagen erstellen oder die bereits erstellten Vorlagen bearbeiten. Sie können die Einstellungen einer bereits erstellten Vorlage in eine neue kopieren und so die Einstellungen einer Vorlage für andere verwenden. Wenn Sie eine Vorlage bearbeiten und speichern, werden Sie (wie bei den Vorlagen für Kontingente) gefragt, ob die Änderungen an die Dateiprüfungen übergeben werden sollen, die mit Hilfe dieser Vorlage erstellt wurden. Wählen Sie unter *Wie möchten Sie die Dateiprüfungseigenschaften konfigurieren?* die Option *Benutzerdefinierte Dateiprüfungseigenschaften definieren* aus, und klicken Sie dann auf die Schaltfläche *Benutzerdefinierte Eigenschaften*. Möchten Sie Eigenschaften aus einer vorhandenen Vorlage kopieren, wählen Sie die zu verwendende Vorlage aus, und klicken Sie auf *Kopieren*.

Abbildg. 6.29 Konfigurieren einer neuen Dateiprüfung



Wählen Sie unter *Prüfungstyp* den Prüfungstyp aus, der angewendet werden soll:

- **Aktives Prüfen** verhindert, dass Benutzer Dateien speichern, die zu blockierten Dateigruppen gehören, und generiert Benachrichtigungen, wenn Benutzer versuchen, blockierte Dateien zu speichern. Wenn ein Benutzer versucht, eine verbotene Datei zu speichern, erhält er eine entsprechende Zugriff-verweigert-Fehlermeldung.

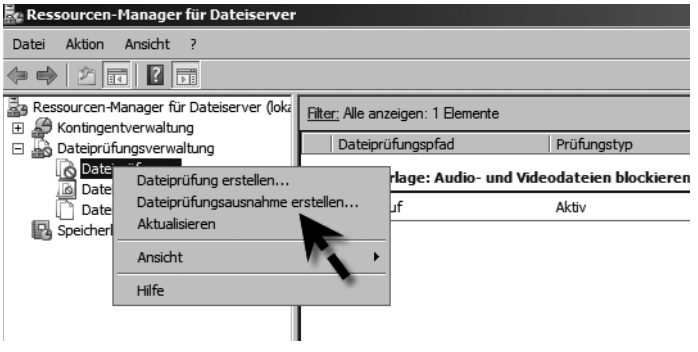
- **Passives Prüfen** sendet Benachrichtigungen, hindert Benutzer jedoch nicht daran, blockierte Dateien zu speichern.

Wählen Sie unter *Dateigruppen* die Dateien aus, die einbezogen werden sollen. Um E-Mail-Benachrichtigungen für die Dateiprüfung zu konfigurieren, legen Sie auf der Registerkarte *E-Mail-Nachricht* die Optionen fest, analog zur Erstellung von Kontingenten. Klicken Sie auf *Erstellen*, um die Dateiprüfung zu speichern. Sie werden gefragt, ob Sie eine Dateiprüfungsvorlage auf der Grundlage der Dateiprüfungseigenschaften speichern möchten, die Sie gerade definiert haben. Wenn Sie die aktuellen Einstellungen in anderen Dateiprüfungen verwenden möchten, sollten Sie eine Vorlage speichern. Die Vorlage wird auf die neue Dateiprüfung angewendet.

Dateiprüfungsausnahmen

Um Dateien zuzulassen, die von anderen Dateiprüfungen blockiert werden, erstellen Sie eine *Dateiprüfungsausnahme*. Eine Dateiprüfungsausnahme ist eine besondere Art der Dateiprüfung, die Dateiprüfungen in einem bestimmten Ausnahmepfad außer Kraft setzt. Das heißt, dass eine Ausnahme für alle Regeln erstellt wird, die von einem übergeordneten Ordner abgeleitet sind. Sie können keine Dateiprüfungsausnahme für einen Ordner erstellen, für den bereits eine Dateiprüfung besteht. Sie müssen die Ausnahme einem Unterordner zuweisen oder Änderungen an der vorhandenen Dateiprüfung vornehmen. Klicken Sie mit der rechten Maustaste auf *Dateiprüfungen*, und rufen Sie im zugehörigen Kontextmenü den Befehl *Dateiprüfungsausnahme erstellen* auf. Wählen Sie unter *Ausnahmepfad* den Pfad aus, für den die Ausnahme gelten soll. Die Ausnahme wird auf den Ordner und alle seine Unterordner angewendet. Um festzulegen, welche Dateien von der Dateiprüfung ausgenommen werden sollen, wählen Sie unter *Dateigruppen* jede Dateigruppe aus, die in der Dateiprüfungsausnahme enthalten sein soll.

Abbildg. 6.30 Erstellen einer Dateiprüfungsausnahme



HINWEIS Ändern Anwender die Endungen der Dateien ab, können diese weiterhin gespeichert werden.

Dateigruppen für die Dateiprüfung

Eine Dateigruppe wird verwendet, um einen Namensraum für eine Dateiprüfung, eine Dateiprüfungsausnahme oder einen Speicherbericht zu definieren. Sie werden in *Einzuschließende Dateien* (Dateien, die zur Gruppe gehören) und *Auszuschließende Dateien* (Dateien, die nicht zur Gruppe gehören) unterschieden. Standardmäßig werden bereits ausreichend Dateigruppen angelegt, die Sie

beliebig bearbeiten können. Um eine neue Dateigruppe zu erstellen, klicken Sie in der Konsolenstruktur des FSRM mit der rechten Maustaste auf *Dateigruppen* und wählen im zugehörigen Kontextmenü den Eintrag *Dateigruppe erstellen* aus. Bei Eingabe von **.exe* werden zum Beispiel alle ausführbaren Dateien ausgewählt.

Speicherberichteverwaltung im FSRM

Der letzte Eintrag in der Konsolenstruktur des FSRM ist *Speicherberichteverwaltung*. Wenn Sie diesen mit der rechten Maustaste anklicken, stehen Ihnen verschiedene Optionen zum Erstellen der Berichte zur Verfügung. Sie können einen Zeitplan erstellen, nach dem ein Bericht regelmäßig erstellt werden soll, oder Sie können einen manuellen Bericht anfertigen. Dazu stehen Ihnen verschiedene Berichtsdaten und Formate zur Verfügung.

Abbildg. 6.31 Anzeigen von Berichten als HTML-Datei

Beispiele

Ein Bericht kann jederzeit ausgeführt werden, um alle doppelt vorhandenen Dateien auf einem Laufwerk oder auf einem Server zu identifizieren. So lässt sich Speicherplatz schnell freigeben, ohne dass Daten verloren gehen. Sie können einen Bericht für Dateien nach Dateigruppe ausführen, um zu identifizieren, wie Speicherressourcen zwischen verschiedenen Dateigruppen aufgeteilt sind,

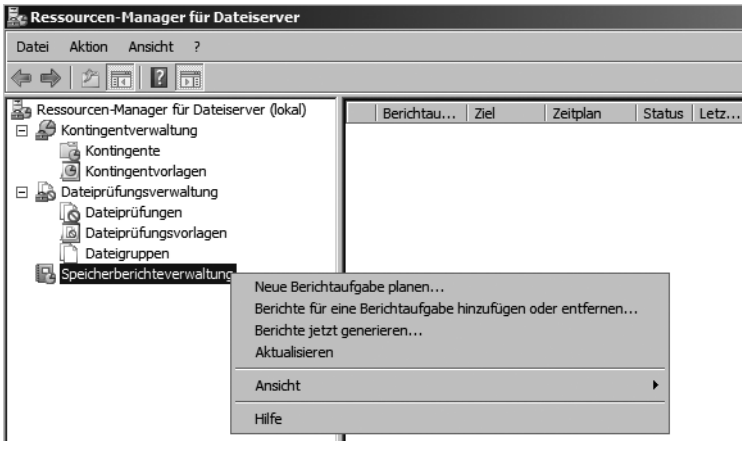
oder einen Bericht für Dateien nach Besitzer, um zu analysieren, wie einzelne Benutzer die gemeinsamen Speicherressourcen verwenden.

Jeder Bericht kann ein eigenes Format haben. Sie können zum Beispiel regelmäßige HTML-Berichte und Abteilungsberichte erstellen, die den Abteilungsleitern einen Überblick über den aktuellen Speicherbedarf der Dateien verschafft. Durch die Speicherberichte können Sie sich bequem per E-Mail regelmäßig einen Überblick über den aktuellen Stand Ihrer Dateiserver verschaffen. Die Vorgehensweise bei der Erstellung der Berichte ist sehr simpel. Auf der Registerkarte *Zustellung* können Sie eine E-Mail-Adresse festlegen, zu der die einzelnen Berichte gesendet werden.

Erstellen eines Berichts

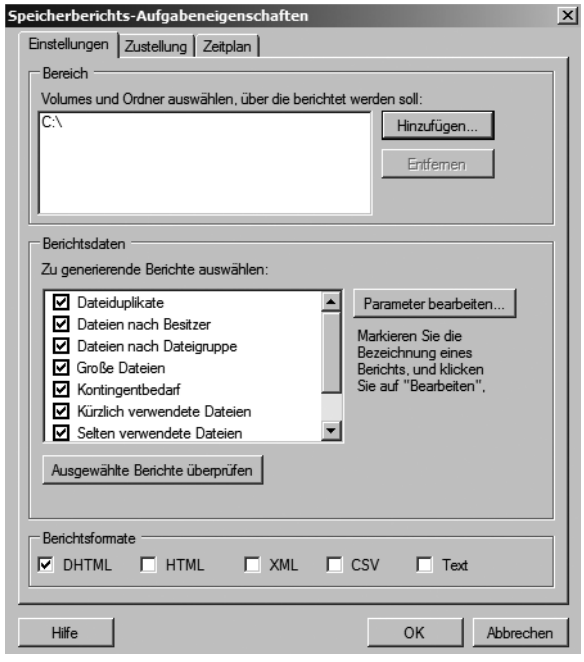
Die Erstellung von Berichten wurden im FSRM sehr intuitiv gelöst. Wollen Sie einen Speicherbericht erstellen, gehen Sie folgendermaßen vor (Abbildung 6.32):

Abbildg. 6.32 Erstellen einer neuen Berichtaufgabe



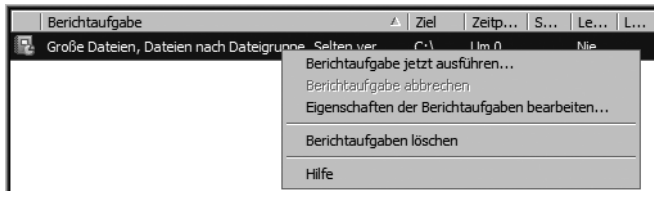
1. Klicken Sie mit der rechten Maustaste auf *Speicherberichteverwaltung* und dann auf *Neue Berichtaufgabe planen*.
2. Klicken Sie im daraufhin geöffneten Dialogfeld im Abschnitt *Bereich* auf die Schaltfläche *Hinzufügen*.
3. Wählen Sie die Volumes und/oder Ordner aus, für die Berichte generiert werden sollen, und klicken Sie auf *OK*.
4. Wählen Sie im Abschnitt *Berichtsdaten* per Klick auf das jeweilige Kontrollkästchen die Berichte aus, die Sie generieren möchten.
5. Möchten Sie die Einstellungen eines Berichts anpassen, markieren Sie diesen, und klicken Sie auf die Schaltfläche *Parameter bearbeiten*.

Abbildg. 6.33 Konfigurieren eines Speicherberichts



6. Bearbeiten Sie die Parameter nach Bedarf, und klicken Sie auf *OK*.
7. Möchten Sie Administratoren per E-Mail Kopien der Berichte zustellen, aktivieren Sie auf der Registerkarte *Zustellung* das Kontrollkästchen *Bericht an die folgenden Administratoren senden*, und geben Sie die E-Mail-Konten ein.
8. Um die Berichte zu planen, klicken Sie auf der Registerkarte *Zeitplan* auf die Schaltfläche *Zeitplan erstellen*. Klicken Sie dann im Dialogfeld *Zeitplan* auf *Neu*. Der Standardzeitplan ist auf täglich 9:00 Uhr festgelegt und beginnt am nächsten Tag. Sie können tägliche, wöchentliche oder monatliche Berichte planen, oder die Berichte nur einmalig generieren.
9. Um die Berichtaufgabe zu speichern, klicken Sie auf *OK*. Die Berichtaufgabe wird anschließend angezeigt.

Abbildg. 6.34 Anzeigen, Starten oder Bearbeiten einer Berichtaufgabe



Sie können erstellte Berichtaufgaben über deren Kontextmenü bearbeiten oder sofort einen Bericht erstellen lassen.

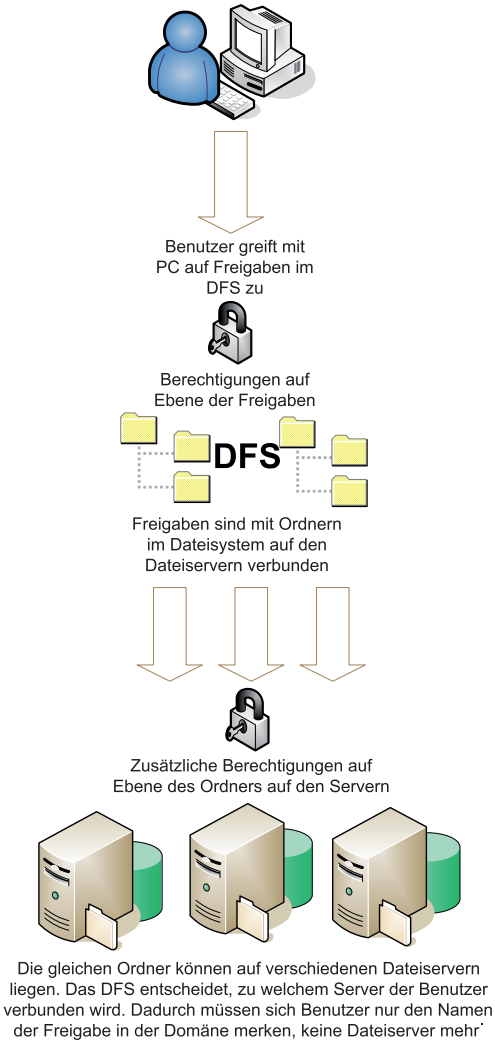
Organisieren und Replizieren von Freigaben über DFS

In größeren Netzwerken sind die Freigaben oft über viele Server verteilt, sodass es schwierig wird, eine gesuchte Freigabe auf Anhieb auf dem richtigen Server zu finden. Gelegentlich wird auch gewünscht, dass die Freigaben für einzelne Abteilungen oder Projektgruppen in irgendeiner Form logisch zusammengefasst werden können. Letzteres würde bedeuten, dass die Freigaben auf einen Server kopiert werden. Sobald aber mehrere Projektgruppen auf eine Freigabe zugreifen sollen, ist diese Methode nicht mehr praktikabel. Eine Funktion, die dieses Problem lösen soll, ist das *verteilte Dateisystem (Distributed File System, DFS)*. Windows Server 2008 enthält im Grunde genommen alle Änderungen von DFS, die bereits in Windows Server 2003 R2 enthalten sind. Im Vergleich zu Windows Server 2003 ergeben sich jedoch zahlreiche Neuerungen, die wir im nächsten Abschnitt näher beleuchten.

Einführung und wichtige Informationen beim Einsatz von DFS

In DFS wird eine logische Struktur über physische Verzeichnisse entwickelt, die auf einem oder mehreren Servern liegen können. Windows Server 2008 unterstützt zwei Varianten des DFS. Der Domänen-DFS-Stamm verwendet das Active Directory, um die Struktur- und Konfigurationsinformationen für das DFS zu speichern. Einfach ausgedrückt bietet DFS die Möglichkeit, Freigaben zu definieren, die auf unterschiedlichen Dateiservern liegen. Anwender müssen nicht mehr wissen, auf welchem Dateiserver die Dateien liegen, sondern kennen nur noch den Freigabenamen. Diese Form von verteilten Dateisystemen kann fehlertolerant aufgebaut werden. So wird die automatische Replikation von Daten zwischen verschiedenen Servern unterstützt. Der eigenständige DFS-Stamm wird pro Server konfiguriert. Die Informationen werden nur auf diesem einen Server abgelegt und nicht repliziert. Der eigenständige DFS-Stamm ist nur sinnvoll, wenn entweder nicht mit Active Directory gearbeitet wird oder wenn DFS bei der Migration eines Windows NT-Servers übernommen wurde. Das Domänen-DFS bietet wesentlich mehr Funktionen und ist damit im Regelfall erste Wahl.

Abbildg. 6.35 DFS unter Windows Server 2008



Für ein Domänen-DFS muss der Server, auf dem der Konsolenstamm bereitgestellt wird, ein Domänencontroller oder ein Mitgliedsserver einer Active Directory-Domäne sein. Wichtig bei Windows Server 2008 ist, dass bei Domänen-DFS mehrere DFS-Stämme auf einem Server gehostet werden können. Damit wird eine der gravierendsten Einschränkungen des DFS, die es bei Windows 2000 Server gab, aufgehoben: Dort konnte nur ein DFS-Stamm pro Server verwaltet werden. Es ließen sich nicht mehrere DFS-Stämme anlegen. Daher musste gegebenenfalls ein gemeinsamer Einstiegspunkt definiert werden, von dem aus auf verschiedene Verzeichnisbäume für unterschiedliche Benutzergruppen verzweigt werden konnte. Das ist nicht mehr der Fall, jede logisch sinnvolle Struktur kann angelegt werden. Über das DFS selbst werden keine Zugriffsberechtigungen gesteuert. Die Rechte von Benutzern werden vielmehr über die Dateisysteme, die in ein DFS integriert werden, definiert. DFS-Verknüpfungen sind Verzeichnisse im DFS-Baum, die auf eine Freigabe verweisen. Wenn eine DFS-

Verknüpfung *Excel-Dateien* angelegt wird, kann diese auf die Freigabe *Budgets* des Servers *file01* verweisen. Der Benutzer sieht bei der Verbindung zum DFS einen Ordner *Excel-Dateien*. Wenn er auf diesen Ordner zugreift, wird er mit dem Server *file01* verbunden und kann dort auf die Dateien und Unterverzeichnisse des Ordners *Budgets* zugreifen. Bei der Erstellung einer DFS-Verknüpfung wird der Name angegeben, unter dem die Freigabe im DFS erscheinen soll. Mit dieser Freigabe wird ein freigegebener Ordner verbunden. Vor allem bei mehreren Dateiservern, auch über Niederlassungen verteilt, können Freigaben mit dem DFS wesentlich effizienter gesteuert werden. Der DFS-Stamm vermittelt den Anwendern einen Überblick über alle verfügbaren Freigaben.

DFS-Namespaces und DFS-Replikation

DFS besteht hauptsächlich aus den beiden Technologien DFS-Namespaces und DFS-Replikation. Diese bieten zusammen eingesetzt einen vereinfachten, fehlertoleranten Dateizugriff, Nutzlastverteilung und WAN-kompatible Replikation. Die DFS-Replikation ist ein Multimasterreplikationsmodul, das die Replikationszeitplanung und Bandbreiteneinschränkung unterstützt. Die DFS-Replikation verwendet ein als RDC (Remote Differential Compression) bezeichnetes neues Komprimierungsprotokoll, mit dem Dateien über ein Netzwerk mit eingeschränkter Bandbreite effizient aktualisiert werden können. RDC erkennt, wenn Daten in Dateien eingefügt oder anders angeordnet oder aus Dateien entfernt wurden. Dadurch ist es möglich, mit der DFS-Replikation nur die beim Aktualisieren von Dateien auftretenden Änderungen zu replizieren.

Mit DFS-Namespaces, früher als verteiltes Dateisystem bezeichnet, können Administratoren freigegebene Ordner, die sich auf unterschiedlichen Servern befinden, zusammenfassen und den Benutzern als virtuelle Ordnerstruktur, den so genannten *Namespace*, zur Verfügung stellen. Sobald ein Benutzer versucht, auf einen Ordner im Namespace zuzugreifen, stellt der Clientcomputer eine Verbindung mit einem Namespaceserver her. Der Namespaceserver sendet dem Clientcomputer einen Verweis mit einer Liste von Servern, auf denen der freigegebene Ordner gespeichert ist. Der Clientcomputer speichert den Verweis im Cache und stellt einen Kontakt mit dem ersten Server im Verweis her. Normalerweise ist das ein Server am Standort des Clients. Wenn einer der Server nicht mehr zur Verfügung steht, findet ein Failover des Clientcomputers auf den verbleibenden Server statt.

Wichtige Planungspunkte beim Einsatz von DFS

Wollen Sie DFS im Unternehmen einsetzen, sollten Sie vor der Einrichtung einige wichtige Planungspunkte beachten, die wir im folgenden Abschnitt zusammengestellt haben:

- DFS unterstützt zwar keinen Cluster, aber dafür die Schattenkopien, sodass gelöschte Dateien wiederhergestellt werden können.
- Sie können DFS nicht dafür verwenden, um Exchange-Datenbanken oder Postfächer abzusichern. Wollen Sie Exchange ausfallsicher installieren, müssen Sie einen Cluster einsetzen.
- Offlinedateien können ebenfalls in einem DFS eingesetzt werden (siehe weiter hinten in diesem Kapitel im Abschnitt »Offlinedateien für den mobilen Einsatz unter Windows Vista«). Achten Sie aber darauf, dass in Szenarios, in denen mehrere Mitarbeiter auf die gleiche Datei schreibend zugreifen, Probleme entstehen können, da durch die Offlinesynchronisierung in Verbindung mit der DFS-Replikation durchaus Dateien synchronisiert werden, die von mehreren Mitarbeitern bearbeitet wurden und so unter manchen Umständen Informationen verloren gehen können.
- Da durch das Scannen von Dateien mit Virenscannern unter Umständen der Dateistempel verändert und dadurch die Replikation im DFS aktiviert wird, sollten Sie auch den Einsatz eines

Virenscanners planen. Stellen Sie sicher, dass Ihr Virenscanner nicht unnötigen Replikationsverkehr verursacht und kompatibel zu DFS ist. Microsoft stellt dazu wichtige Informationen zur Verfügung, die Sie auf der Internetseite *http://go.microsoft.com/fwlink/?LinkId=73990* abrufen können.

- In diesem Kapitel zeigen wir Ihnen auch den Einsatz des *verschlüsselndes Dateisystems (Encrypting File System, EFS)*. Lassen Sie Dateien verschlüsseln, werden diese von der DFS-Replikation ausgenommen und nur auf dem Quell-Server belassen. Die DFS-Replikation löscht alle Replikate der verschlüsselten Dateien, die nicht verschlüsselt sind. Sie sollten daher bei der parallelen Einrichtung von EFS und DFS sehr umsichtig planen, welche Verzeichnisse und Freigaben von DFS repliziert werden und welche Dateien Sie verschlüsseln.
- DFS kann nur auf NTFS-Volumes eingesetzt werden, FAT wird nicht unterstützt.
- Die beteiligten Server in der DFS-Infrastruktur müssen nicht Mitglied der gleichen Domäne oder Struktur sein, aber zwingend in der gleichen Gesamtstruktur.
- DFS-Replikation sollte möglichst nicht in Umgebungen eingesetzt werden, in denen mehrere Mitarbeiter auf unterschiedlichen Servern mit denselben Dateien arbeiten. Durch die DFS-Replikation können so sehr schnell Änderungen von Mitarbeitern verloren gehen.
- Sie sollten die DFS-Replikation regelmäßig überwachen. Microsoft stellt dazu das Tool *Dfsradmin.exe* zur Verfügung. Hierbei handelt es sich um ein Befehlszeilenprogramm, das Sie als Aufgabe in einem Skript regelmäßig verwenden sollten, um Berichte über die DFS-Replikation zu erstellen. Geben Sie in einer Befehlszeile *dfsradmin.exe* ein, erhalten Sie ausführliche Informationen über die Syntax. Auf der Seite *http://go.microsoft.com/fwlink/?LinkId=74010* finden Sie hierzu weitere Informationen, wie die DFS-Replikation optimal überwacht werden kann.
- Die DFS-Replikation repliziert auch die NTFS-Berechtigungen auf Dateien. Achten Sie aber darauf, dass die Änderung der Berechtigung von zahlreichen Dateien großen Replikationsverkehr verursacht, da diese Änderungen repliziert werden müssen. Sie sollte daher die Dateiberechtigungen bereits vor der Einrichtung von DFS konfigurieren und abschließen.
- Der DFS-Replikationsverkehr zwischen Servern wird verschlüsselt und kann daher nicht abgehört werden.
- Die DFS-Replikation unterstützt die Replikationszeitplanung und Bandbreiteneinschränkung in 15-minütigen Schritten innerhalb eines Zeitraums von sieben Tagen. Administratoren wählen beim Angeben eines Replikationsintervalls die Start- und die Stoppzeit sowie die zu verwendende Bandbreite in diesem Intervall aus. Die Einstellungen für die Bandbreitenauslastung liegen im Bereich zwischen 16 Kbit/s und 256 Mbit/s oder voller, unbeschränkter Bandbreite. Sie können eine sofortige Replikation mit dem Befehl *Dfsrdiag SyncNow* starten.
- Die globalen Konfigurationseinstellungen für die DFS-Replikation, wie zum Beispiel die Topologie und der Replikationszeitplan, werden in Active Directory gespeichert. Die Einstellungen werden außerdem auf jedem Mitgliedsserver in einer lokalen XML-Datei gespeichert. Diese Datei kann von der DFS-Replikation mit den in Active Directory gespeicherten Einstellungen neu erstellt werden, wenn die Datei beschädigt oder der Server nach einem Ausfall wiederhergestellt wird.
- Bevor Sie einer Replikationsgruppe einen neuen Server hinzufügen, können Sie ein Pre-Staging der replizierten Ordner auf den Zielservern ausführen. Dazu können Sie die Daten auf die Server kopieren, eine Sicherung wiederherstellen oder Dateien von einem Band, einer DVD oder einer Wechselfestplatte kopieren. Auf diese Weise entsteht bei der anfänglichen Synchronisierung nur minimaler WAN-Datenverkehr. Falls die Dateien auf dem Zielserver veraltet sind, repliziert die

DFS-Replikation mithilfe der Remote Differential Compression (RDC) nur die Änderungen, die seit dem Pre-Staging der Daten aufgetreten sind.

- Die DFS-Replikation wird für die SYSVOL-Replikation in Windows Server 2008 nicht unterstützt. Verwenden Sie weiterhin den Dateireplikationsdienst (File Replication Service, FRS) für die Replikation von SYSVOL auf Domänencontrollern.

Dateiprüfungen oder Kontingente in DFS

Sie können in einer DFS-Infrastruktur auch die Dateiprüfungen des Ressourcen-Managers für Dateiserver verwenden, die ebenfalls in diesem Kapitel besprochen werden. Zusätzlich zu dieser Dateiprüfung, können Sie in der DFS-Replikation konfigurieren, dass manche Dateitypen von der Replikation ausgeschlossen werden. Wollen Sie in einer DFS-Infrastruktur Kontingente oder Dateiprüfungen einsetzen, sollten Sie darauf achten, dass vor der Einrichtung der Dateiprüfung keine Dateitypen gespeichert wurden, die später gefiltert werden. Die Dateiprüfung entdeckt nur, wenn neue Dateien abgelegt werden, bereits vorhandene Dateien werden nicht blockiert. Natürlich sollten Sie sicherstellen, dass kein Verzeichnis bereits sein Kontingent überschreitet, wenn Sie DFS oder die Kontingentverwaltung einrichten. Sie sollten bei der Einrichtung von harten Kontingenten, bei denen Anwender nach Überschreitung nicht mehr speichern dürfen, vorsichtig sein. Unter manchen Umständen, wenn ein Verzeichnis zum Beispiel kurz vor dem Erreichen der Grenze ist, kann es passieren, dass durch die DFS-Replikation diese Grenze überschritten wird. Arbeiten Sie in einer DFS-Infrastruktur daher besser mit weichen Grenzen, bei denen die Anwender noch schreiben dürfen, aber Meldungen generiert werden.

Voraussetzungen für DFS

Damit Sie DFS sinnvoll verwenden können, müssen in Ihrem Unternehmen einige Voraussetzungen geschaffen werden. Zunächst benötigen Sie ein Active Directory, da nur unter dem Betrieb eines DFS-Stamms im Active Directory die Struktur sinnvoll ist. Des Weiteren benötigen Sie idealerweise Dateiserver unter Windows Server 2008. Auch die Clients müssen DFS unterstützen, dies kann jede Windows-Version ab Windows NT 4.0 sein. Sie können das DFS auch so einrichten, dass mehrere Dateiserver ihre Daten miteinander replizieren. Dazu verwendet das DFS einen ähnlichen Mechanismus wie beim Replizieren der Anmeldeskripts zwischen den Domänencontrollern, den Dateireplikationsdienst (File Replication Service, FRS). Die Replikation der DFS-Daten wird aber nicht durch den FRS des Servers durchgeführt, sondern durch die DFS-Replikation. Die DFS-Replikation kommuniziert nicht mit dem FRS, sondern läuft eigenständig. Dadurch ist es möglich, eine Freigabe auf mehrere Ziele zu verweisen. Sie können diese Konfiguration leicht über den Assistenten zur Einrichtung von DFS durchführen. Durch diese Replikation können Sie auch Niederlassungen anbinden. Dies hat den Vorteil, dass Mitarbeiter auch in den Niederlassungen mit den gleichen Dateien arbeiten und das DFS dafür sorgt, dass die Daten von und zu den Niederlassungen repliziert werden. Vor allem Windows Server 2008 weist hier einige deutliche Verbesserungen auf. Außer dem bereits beschriebenen Vorteil des einfachen Zugriffs lassen sich durch die Möglichkeit, gleiche Daten auf unterschiedliche Server replizieren zu lassen, durchaus weitere Vorteile erkennen. Wenn einer der DFS-Server ausfällt, fällt das den Anwendern nicht auf, denn ohne dass sie es merken, verbindet der DFS-Stamm sie auf den zweiten Server. Sie sollten aus diesen Gründen einen DFS-Stamm auf den Domänencontrollern konfigurieren. Wenn Sie für die Ausfallsicherheit der Domänencontroller sorgen, zum Beispiel durch den Einsatz mehrerer Domänencontroller, finden die Clients immer einen DFS-Stamm-Server.

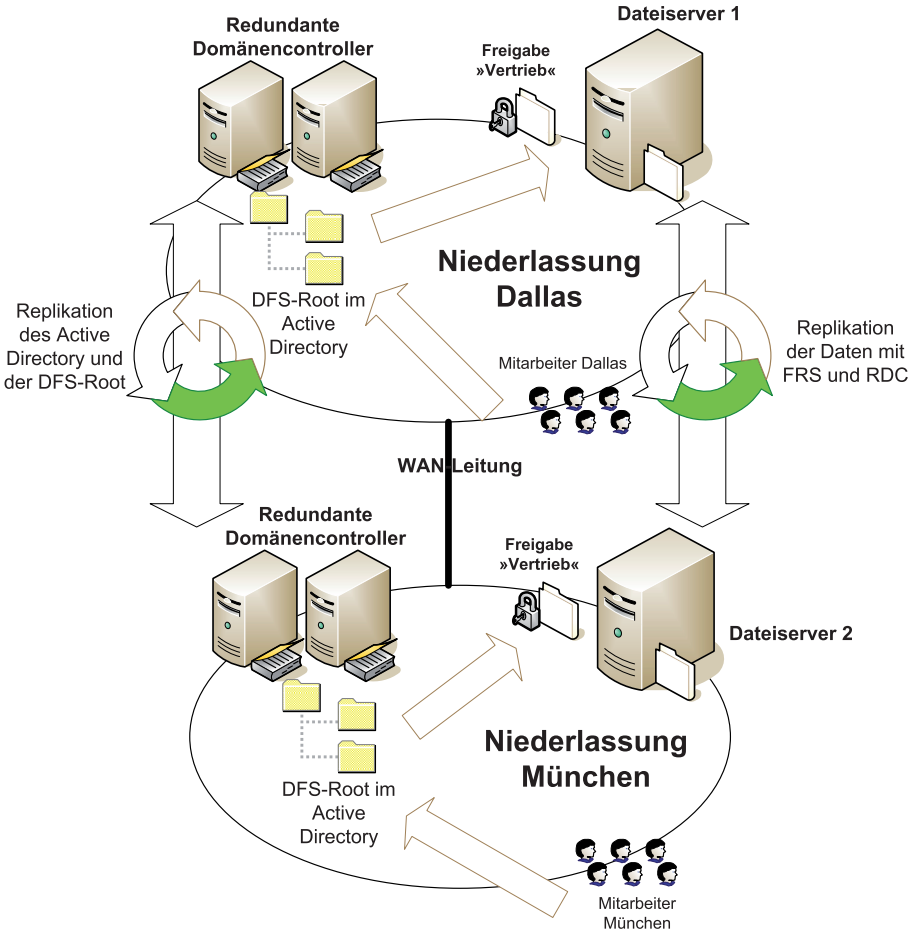
Remote Differential Compression (RDC)

Eines der wesentlichsten, neuen Merkmale ist die Remote Differential Compression (RDC), die es bereits seit Windows Server 2003 R2 gibt. Mit diesem neuen Kompressionsverfahren werden Dateien über WAN-Leitungen wesentlicher effizienter zwischen den DFS-Servern repliziert als bisher. Die Replikation des DFS nutzt dazu eine verbesserte Kompression. RDC ist vor allem für schmalbandige Verbindungen entwickelt worden, also gerade VPN-Verbindungen zu Niederlassungen. Bei RDC werden bei Änderungen in Dateien nicht mehr die ganzen Dateien repliziert, sondern nur noch die geänderten Daten. Daher spart diese Replikationsmethode deutlich an Bandbreite ein. Dadurch ist es möglich auch größere Dateien, die bereits repliziert wurden, schneller zu aktualisieren, da nur noch Deltas kopiert werden müssen. Wenn ein Benutzer in einer Niederlassung eine 10 Mbyte große PowerPoint-Folie verändert, aber nur kleinere Änderungen vornimmt, werden statt 10 Mbyte nur diese wenigen bytegroßen Änderungen repliziert. Das Beispiel in Abbildung 6.36 zeigt, wie wichtig es ist, auch bei der Anbindung von Niederlassungen ein genaues Konzept zu erstellen. Jede Niederlassung mit einem oder mehreren Domänencontrollern sollte im Active Directory als eigenes Subnetz und eigener Standort geführt werden, damit die DFS-Stamm die Anwender zum richtigen Dateiserver in ihrer Niederlassung verbindet. RDC beansprucht allerdings auch die CPU eines Servers, da Dateien vor der Replikation komprimiert werden müssen. Es ist daher möglich für Verbindungen zwischen Standorten, die über ein LAN verbunden sind, RDC auszuschalten. Dadurch wird zwar die replizierte Datenmenge erhöht, was in einem LAN aber selten eine Rolle spielt. Auf der anderen Seite wird dadurch die Belastung der CPU verringert. RDC wird nicht für Dateien verwendet, die kleiner als 64 KB sind. Auch für Hochgeschwindigkeits-LANs, in denen die Netzwerkbandbreite nicht stark beansprucht wird, bringt RDC keinen Vorteil. RDC kann für einzelne Verbindungen mithilfe des DFS-Verwaltungs-Snap-Ins deaktiviert werden.

Zusätzlich können Sie für jede DFS-Verknüpfung, also jede Freigabe, die im DFS hinterlegt wird, zwei Ziele angeben, zwischen denen die Daten zur Ausfallsicherheit repliziert werden. Zusätzlich kann dieser Mechanismus zur Anbindung von Niederlassungen verwendet werden. Wenn der Dateiserver in der Zentrale steht, müssen die Niederlassungen über langsame WAN-Leitungen zugreifen. Mit DFS kann in der Niederlassung ein kleiner Dateiserver aufgestellt werden, auf den die Daten repliziert werden. Die Mitarbeiter der Außenstelle können dadurch genauso effizient und schnell auf die Freigaben und notwendige Dateien zugreifen wie die Mitarbeiter in der Zentrale.

HINWEIS Das FRS kann auch innerhalb eines DFS keine Dateien zusammenführen. Wenn die gleiche Datei von zwei verschiedenen Benutzern geöffnet wird, repliziert der FRS immer die jüngere Datei. Die Änderungen des zweiten Mitarbeiters können dadurch verloren gehen. Es ist daher sehr wichtig, eine genaue Berechtigungsstruktur zu planen, wer auf welche Dateien nur lesen, schreibend oder auch löschend zugreifen darf.

Abbildg. 6.36 Optimale Replikation bei der Verwendung von DFS einrichten



Installation und Einrichtung von DFS

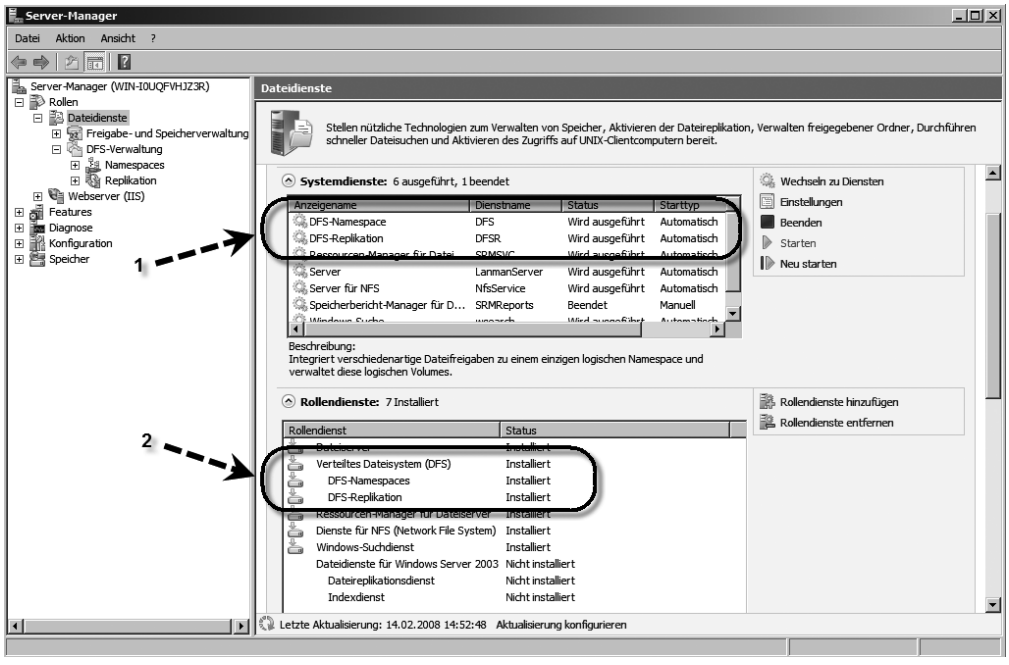
Wollen Sie im Unternehmen DFS einsetzen, müssen Sie das Schema Ihrer Gesamtstruktur auf Windows Server 2008 aktualisieren. In Kapitel 8 gehen wir näher auf diese Thematik ein. Die Schemaerweiterung auf Windows Server 2008 fügt die notwendigen Klassen und Objekte hinzu, die für die Einrichtung von DFS unter Windows Server 2008 verwendet werden.

TIPP Das Tool *Adprep.exe* zur Aktualisierung des Schemas einer Windows Server 2003-Gesamtstruktur führen Sie mit der Option *adprep.exe /forestprep* durch. *Adprep.exe* finden Sie auf dem Windows Server 2008-Installationsmedium im Verzeichnis *Windows\sources\adprep*.

Installation von DFS

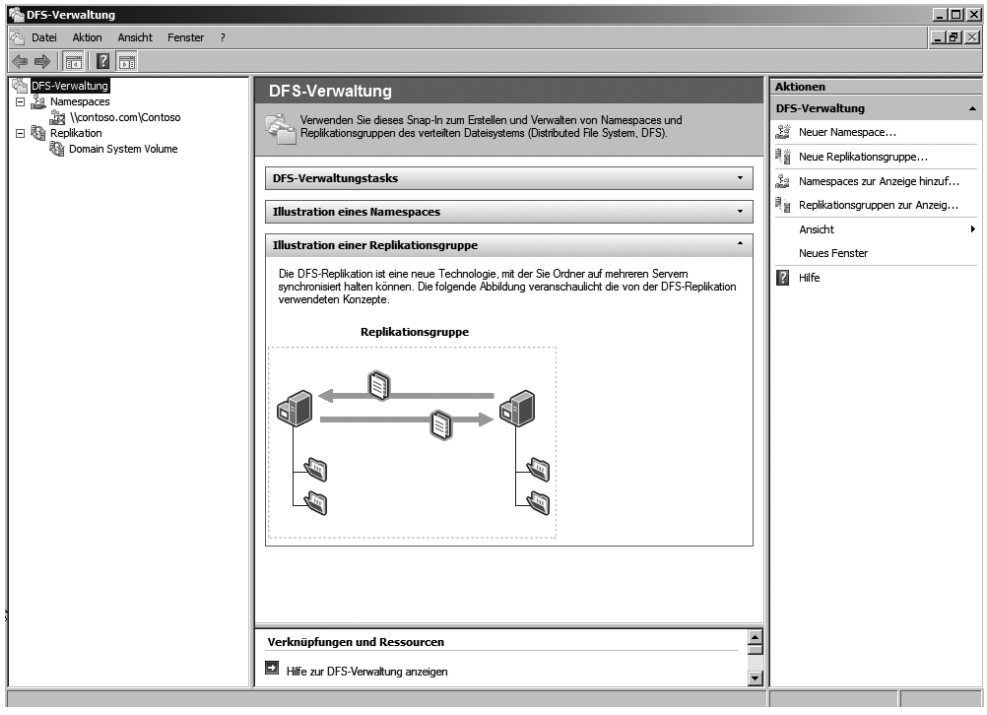
DFS installieren Sie am besten über den Server-Manager und die Rolle *Dateidienste*. Stellen Sie sicher, dass die Rollendienste *Verteiltes Dateisystem, DFS-Namespace* und *DFS-Replikation* installiert sind (siehe Punkt 2 in Abbildung 6.37). Überprüfen Sie außerdem, ob die Systemdienste *DFS-Replikation* und *DFS-Namespace* auf *Automatisch* stehen und gestartet worden sind (siehe Punkt 1 in Abbildung 6.37).

Abbildg. 6.37 Installieren von DFS auf einem Server



Nachdem Sie die notwendigen Rollendienste installiert haben, können Sie das Snap-In *DFS-Verwaltung* über *Start/Verwaltung* starten (Abbildung 6.38). Alternativ starten Sie die Verwaltungsoberfläche über *Start/Ausführen/dfsmgmt.msc*. Die Verwaltungsoberfläche dient zur Konfiguration und Verwaltung sowohl des DFS-Namespaces als auch der DFS-Replikation.

Abbildg. 6.38 Konfigurieren von DFS mit der DFS-Verwaltung



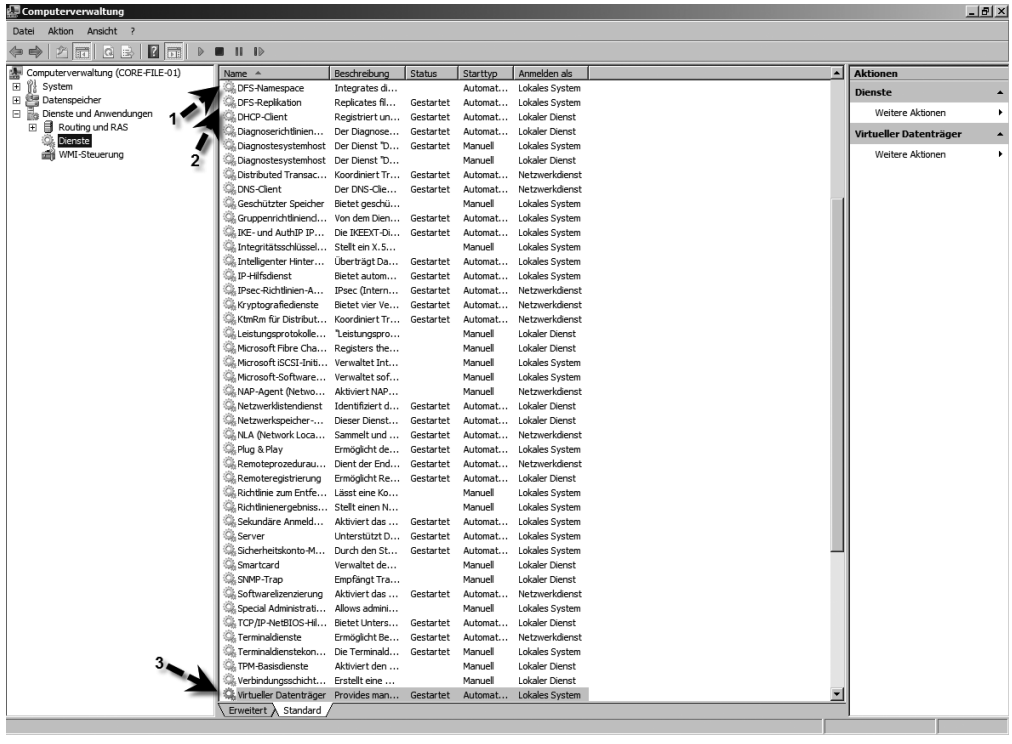
DFS auf einem Core-Server installieren

Die DFS-Installation auf einem Core-Server gestaltet sich etwas komplizierter als über den Server-Manager. Gehen Sie zur Installation und Einrichtung folgendermaßen vor:

1. Wollen Sie das verteilte Dateisystem (Distributed File System, DFS) auf einem Core-Server installieren, geben Sie in der Befehlszeile des Servers den Befehl *start /w ocsetup DFSN-Server* ein. Sie erhalten keine Rückmeldung der Installation. Nachdem Sie den Installationsvorgang abgeschlossen haben, können Sie überprüfen, ob auf dem Server der Dienst *DFS-Replication* installiert wurde und gestartet ist.
2. Die DFS-Replikation (Distributed File System Replication), installieren Sie mit dem Befehl *start /w ocsetup DFSR-Infrastructure-ServerEdition*.
3. Wollen Sie die Datenträgerverwaltung eines Core-Servers über das entsprechende MMC-Snap-In von einem anderen Server aus durchführen, müssen Sie auf dem Core-Server den Dienst *Virtueller Datenträger (Virtual Disk)* starten. Geben Sie dazu auf dem Core-Server den Befehl *net start vds* ein.
4. Zusätzlich müssen Sie in der Windows-Firewall die Regel für das Remotemanagement freischalten. Verwenden Sie dazu den Befehl *netsh advfirewall set allprofiles settings remotemanagement enable*. Den kompletten Netzwerkverkehr auf einem Core-Server können Sie über *netsh advfirewall set allprofiles firewallpolicy allowinbound,allowoutbound* freischalten. Um die Firewallregeln für Core-Server zu steuern, bietet es sich an, dass Sie den Core-Server in eine eigene OU legen, auf die Sie eine Gruppenrichtlinie verknüpfen. In dieser Richtlinie können Sie die Regeln für die Firewall hinterlegen, damit die Kommunikation funktioniert.

Haben Sie die notwendigen Dienste installiert und die Remoteverwaltung über das Netzwerk freigeschaltet, können Sie sich über die Computerverwaltung von einem anderen Server auf den Core-Server verbinden und überprüfen ob die notwendigen Dienste (*DFS-Replikation*, *DFS-Namespace* und *Virtueller Datenträger*) gestartet worden sind (Abbildung 6.39).

Abbildg. 6.39 Überprüfen der notwendigen Systemdienste auf einem DFS-Server

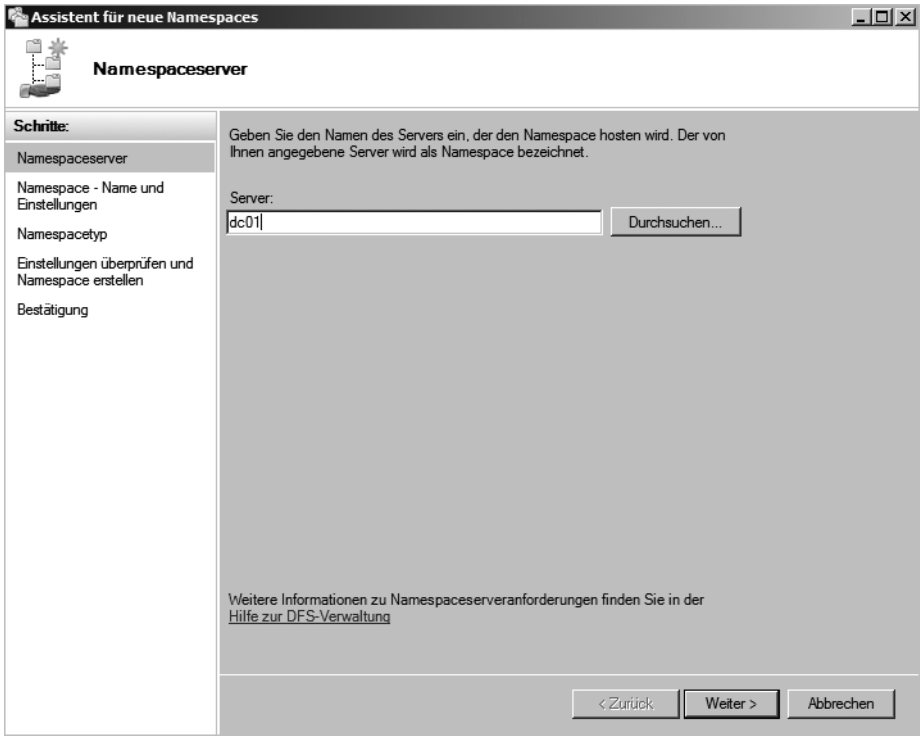


Einrichtung eines DFS-Namespace

Die Einrichtung eines DFS-Namespace nehmen Sie am besten in der DFS-Verwaltung vor, nicht unbedingt auf einem Core-Server, da die Verwaltungsoberfläche wesentlich bequemer ist. Ein DFS-Namespace verbindet mehrere physische Freigaben auf verschiedenen Servern zu einer virtuellen DFS-Freigabe, auf die Anwender zugreifen können. Wenn Sie einen Namespace erstellen, wählen Sie aus, welche freigegebenen Ordner dem Namespace hinzugefügt werden sollen, entwerfen die Hierarchie, in der die Ordner angezeigt werden, und legen die Namen für die freigegebenen Ordner im Namespace fest. Wenn der Namespace von einem Benutzer angezeigt wird, werden die Ordner so auf dem Bildschirm angezeigt, als seien sie auf einer einzelnen Festplatte gespeichert. Benutzer können im Namespace navigieren, ohne die Namen der Server oder der freigegebenen Ordner kennen zu müssen, die der jeweilige Host für die Daten sind. Um einen neuen Namespace einzurichten, gehen Sie folgendermaßen vor:

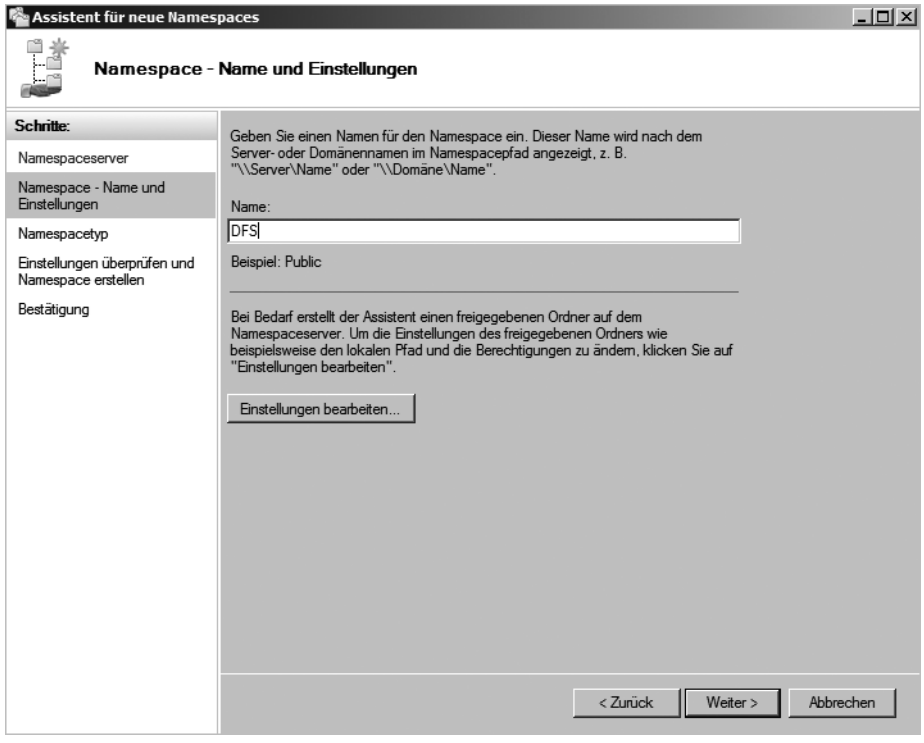
1. Klicken Sie in der DFS-Verwaltung mit der rechten Maustaste auf *Namespaces* und wählen im Kontextmenü den Eintrag *Neuer Namespace* aus.
2. Im ersten Fenster des Assistenten wird der Namespaceserver festgelegt. Dabei handelt es sich nicht gezwungenermaßen um einen Server, auf dem auch die Freigaben liegen, sondern es kann sich auch um einen Domänencontroller oder einen anderen Mitgliedsserver handeln (Abbildung 6.40).

Abbildg. 6.40 Auswählen des Namespaceservers für die Einrichtung eines DFS-Namespaces



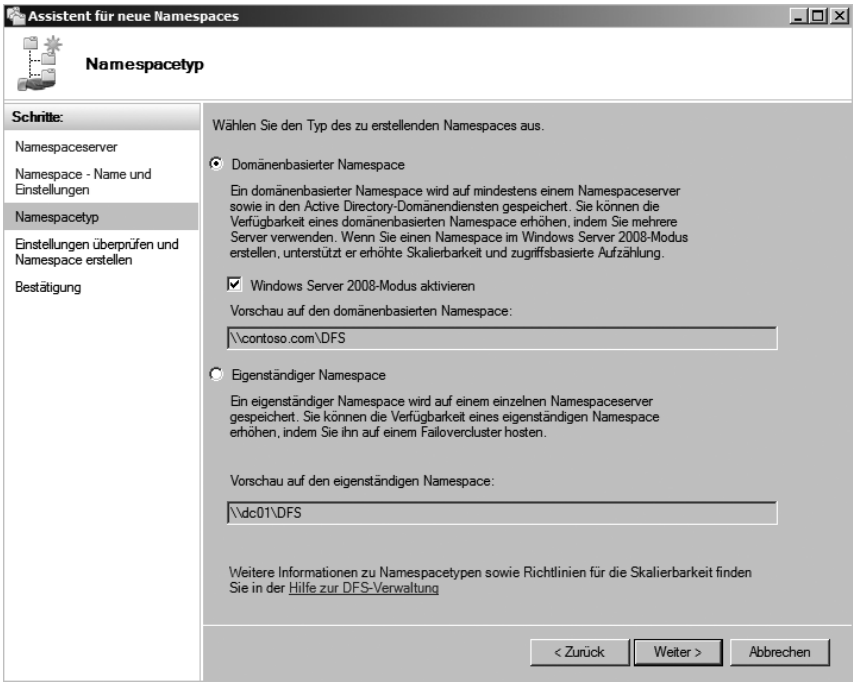
3. Im nächsten Dialogfeld wählen Sie den Namen für den neuen Namespace aus. Für eine Testumgebung können Sie den Namen auf *DFS* setzen. Der Namespacestamm ist der Ausgangspunkt des Namespaces. In diesem Beispiel lautet der Name des Stamms *Public*, und der Namespacepfad lautet *Contoso**DFS*. Neben dem Namespace gibt es noch *Ordner*. Ordner dienen dem Aufbau der Namespacehierarchie. Ordner können optional *Ordnerziele* haben. Wenn Benutzer einen Ordner mit Zielen im Namespace durchsuchen, empfängt der Clientcomputer einen Verweis, der ihn an eines der Ordnerziele umleitet. Ein *Ordnerziel* ist ein UNC-Pfad eines freigegebenen Ordners oder ein anderer Namespace. Ein Ordner kann mehrere Ordnerziele haben, die auf physische Freigaben auf Servern verweisen.

Abbildg. 6.41 Festlegen des Namens des DFS-Namespaces

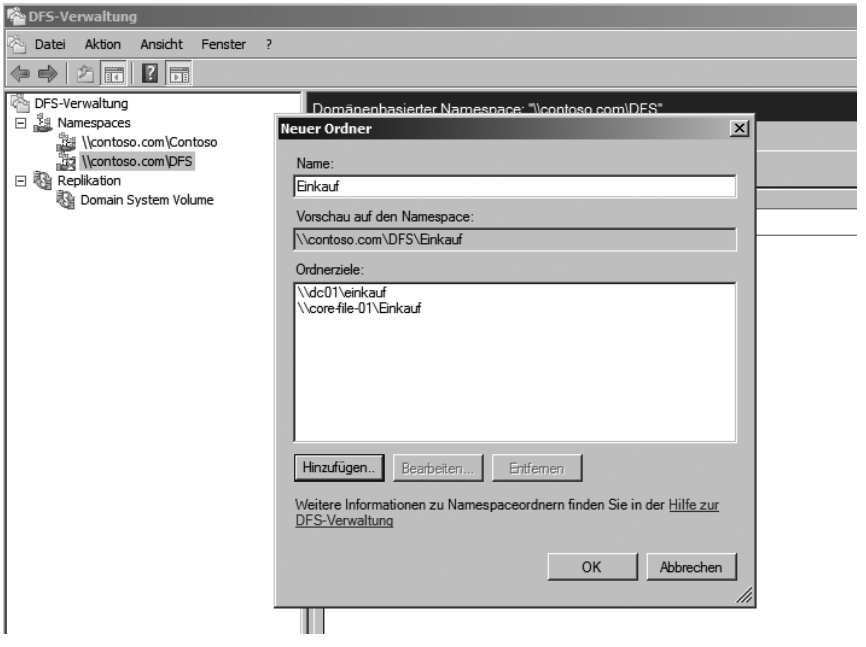


4. Auf der nächsten Seite des Assistenten legen Sie den Namespacetyp fest. Dieser Namespacetyp wird als *Domänenbasierter Namespace* bezeichnet, da er mit einem Domänennamen beginnt und seine Metadaten in Active Directory gespeichert werden. Ein domänenbasierter Namespace kann auf mehreren Namespaceservern gehostet werden.
5. Nachdem Sie die Daten eingegeben haben, können Sie den Namespace erstellen lassen. Er wird anschließend in der DFS-Verwaltung angezeigt. Sie können zur Ausfallsicherheit jederzeit dem Namespace weitere Namespaceserver hinzufügen. Stellen Sie in diesem Fall aber sicher, dass die zusätzlichen Namespaceserver erreicht werden können. Weitere Namespaceserver können nur hinzugefügt werden, wenn Sie einen domänenbasierten Namespace erstellt haben. Klicken Sie zum Hinzufügen mit der rechten Maustaste auf den erstellten Namespace.
6. Klicken Sie anschließend mit der rechten Maustaste auf den neuen Namespace und wählen Sie *Neuer Ordner* aus. Anschließend können Sie einen neuen Ordner erstellen, auf den die Anwender zugreifen können. Im Assistenten zum Erstellen eines neuen Ordner, können Sie jetzt auch ein oder mehrere Ordnerziele hinzufügen. Ordnerziele verweisen auf physische Freigaben auf Servern (Abbildung 6.43). Sie können beliebig viele Ordner mit dazugehörigen Ordnerzielen erstellen. Die Anwender greifen von ihren Clients zwar physisch auf die Ordnerziele zu, allerdings verwenden sie als Namen die Bezeichnung, die Sie im DFS festlegen. Bestätigen Sie die Erstellung. Sie werden noch gefragt, ob Sie gleich eine Replikationsgruppe erstellen wollen. Dies müssen Sie an dieser Stelle nicht tun. Replikationsgruppen werden in einem späteren Abschnitt noch ausführlicher besprochen.

Abbildg. 6.42 Auswählen des Namespacetyps



Abbildg. 6.43 Erstellen von neuen Ordnern mit Ordnerzielen

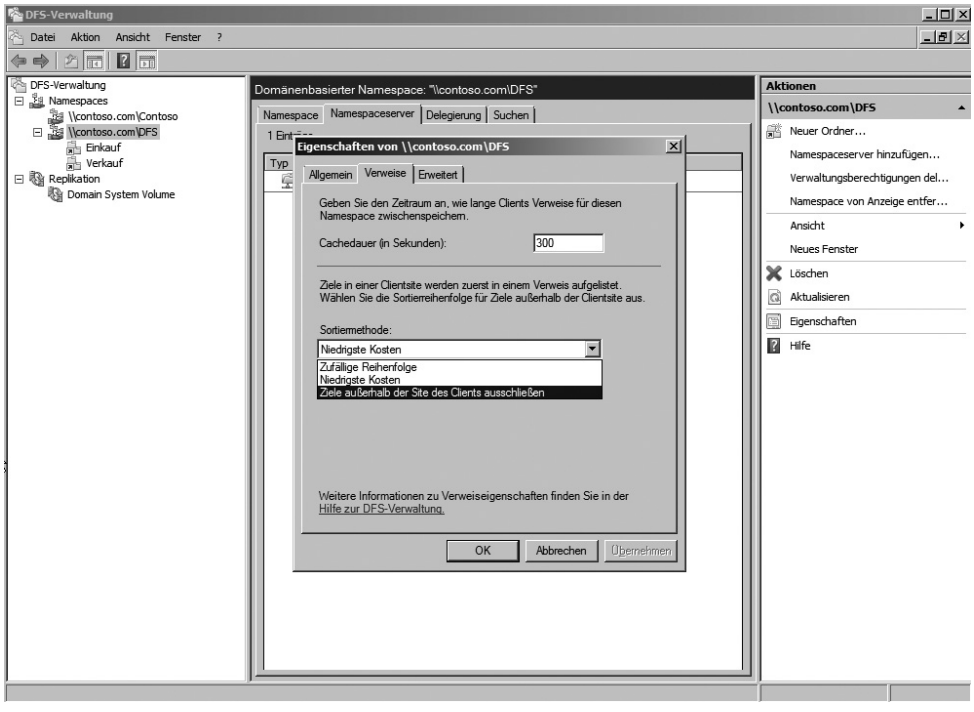


Konfigurieren von Verweisen

Ein Verweis ist eine sortierte Zielliste, die ein Clientcomputer von einem Domänencontroller oder Namespaceserver empfängt, wenn der Benutzer auf einen Namespacestamm oder Ordner mit Zielen im Namespace zugreift. Durch die Verweisliste weiß der Client, auf welchen Servern das zugehörige Ordnerziel gespeichert ist. Fordert ein Client einen Verweis an, berücksichtigt der DFS-Dienst den Standort des Clients und den Standort des Ziels und stellt einen Verweis mit Zielen bereit, die entsprechend der aktuellen Verweisreihenfolge geordnet sind. Standardmäßig werden in einem Verweis zunächst Ziele am Standort eines Clients in zufälliger Reihenfolge aufgelistet, dann folgt eine Liste der Ziele, die außerhalb des Clientstandorts liegen, sortiert nach den niedrigsten Kosten. Um die Reihenfolge anzupassen, können Sie die Sortiermethode für einen ganzen Namespace oder für einzelne Ordner ändern:

1. Klicken Sie in der DFS-Verwaltung mit der rechten Maustaste auf den Namespace und dann auf *Eigenschaften*.
2. Überprüfen Sie auf der Registerkarte *Verweise* unter *Sortiermethode*, dass *Niedrigste Kosten* ausgewählt ist (Abbildung 6.44). Bei der Sortiermethode für die niedrigsten Kosten werden Ziele in einem Verweis sortiert. Ziele im gleichen Standort wie der Client werden in zufälliger Reihenfolge ganz oben im Verweis aufgelistet. Ziele außerhalb des Standorts des Clients werden in der Reihenfolge von den niedrigsten zu den höchsten Kosten aufgelistet. Verweise mit gleichen Kosten werden zusammen gruppiert, und innerhalb der einzelnen Gruppen werden die Ziele in zufälliger Reihenfolge aufgelistet. Wenn Sie nicht möchten, dass Clients auf Ordnerziele außerhalb ihres Standorts zugreifen, können Sie die Sortiermethode für einzelne Ordner ändern. Klicken Sie dann auf *Ziele außerhalb der Site des Clients ausschließen*.

Abbildg. 6.44 Konfigurieren der Verweise für DFS-Namespaces

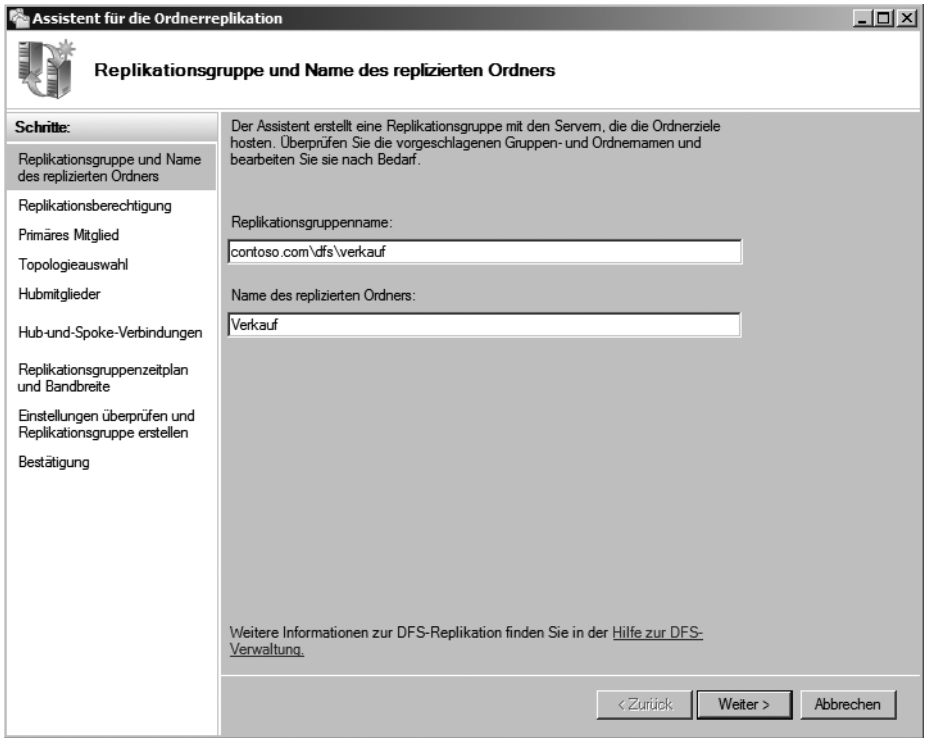


Einrichten der DFS-Replikation

Wollen Sie den Inhalt von Freigaben replizieren, können Sie diese Funktion für einzelne Ordner im Namespace aktivieren. Standardmäßig ist die Replikation nicht aktiviert. Um diese zu aktivieren, klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie im Kontextmenü den Eintrag *Ordner replizieren* aus. Anschließend startet der Assistent, mit dem Sie die Replikation konfigurieren können:

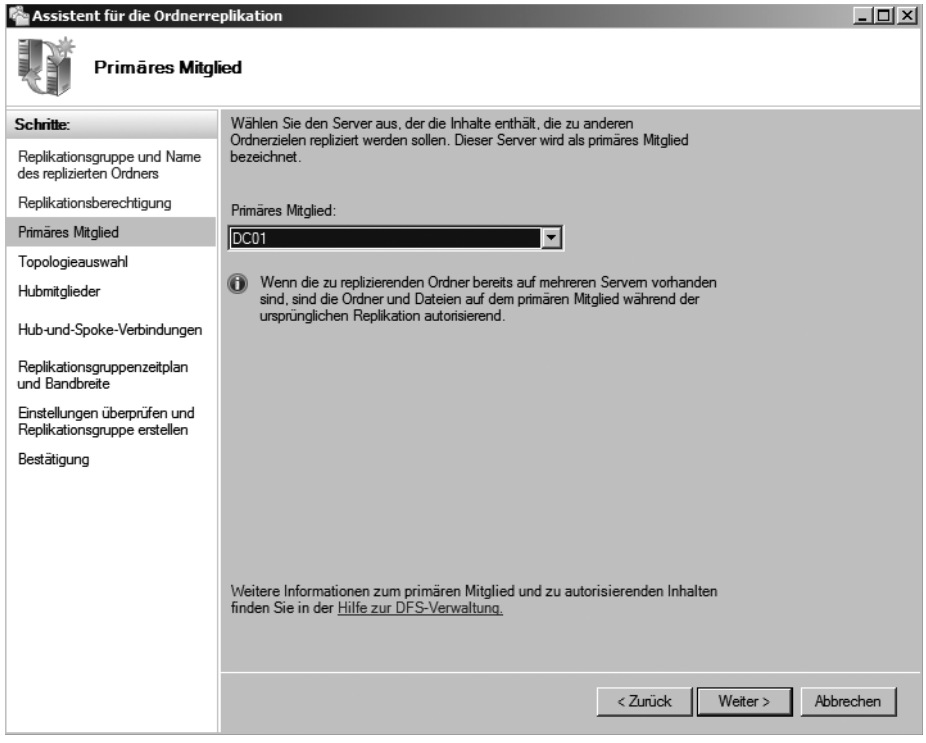
1. Auf der ersten Seite des Assistenten wird Ihnen noch mal der Namen des Ordners angezeigt. Hier legen Sie auch den Namen der Replikationsgruppe fest (Abbildung 6.45). Eine Replikationsgruppe besteht aus einer Reihe von Servern, die an der Replikation eines replizierten Ordners beteiligt sind. Ein replizierter Ordner ist ein Ordner, der auf den einzelnen Mitgliedern synchron gehalten wird. Der Name der Replikationsgruppe stimmt mit dem Namespacepfad überein und der Name des replizierten Ordners mit dem Ordnernamen in der DFS-Verwaltungs-Konsole.

Abbildg. 6.45 Festlegen des Replikationsgruppennamens und des Namens des replizierten Ordners



2. Auf der nächsten Seite werden die Freigaben und die dazugehörigen Server angezeigt, deren Freigaben repliziert werden.
3. Auf der nächsten Seite wählen Sie das primäre Mitglied der Replikationsgruppe aus. Wählen Sie hier den Server aus, der den aktuellsten Inhalt enthält (Abbildung 6.46).

Abbildg. 6.46 Auswählen des primären Mitglieds der Replikationsgruppe

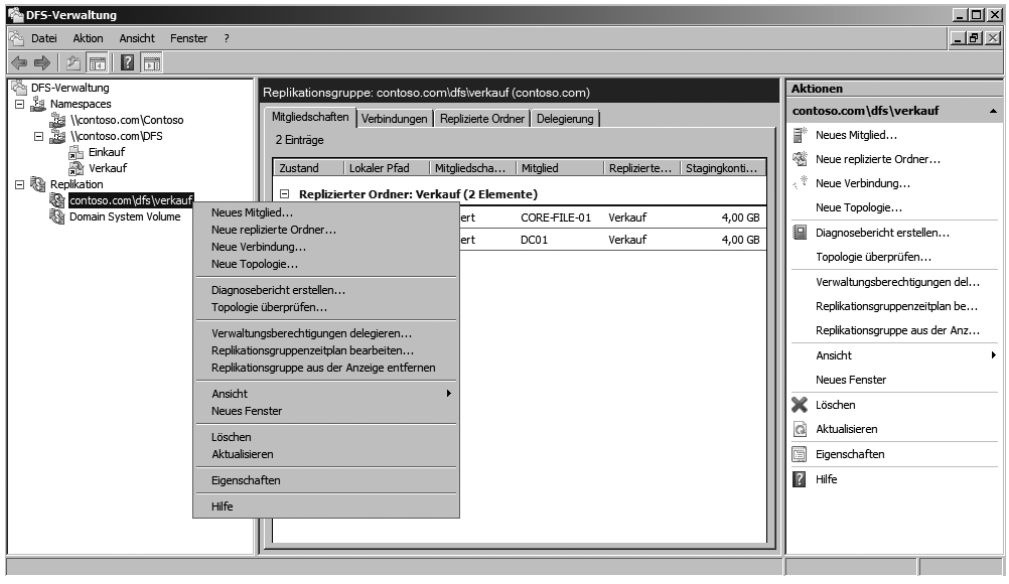


4. Auf der nächsten Seite wählen Sie aus, welche Replikationstopologie Sie verwenden wollen. Die Definitionen der Replikationstopologien sind selbsterklärend. Sie sollten möglichst die Option *Full-Mesh* verwenden.
5. Auf der nächsten Seite legen Sie die Bandbreite oder den Zeitplan für die Replikation fest.
6. Anschließend wird die Replikation erstellt. Nachdem diese erstellt wurde, wird die Replikation in der DFS-Verwaltung unter dem Knoten *Replikation* angezeigt. Sie können die Eigenschaften der Replikation jederzeit über das Kontextmenü anpassen (Abbildung 6.47).

HINWEIS Die erste Replikation beginnt nicht sofort. Die Topologie- und DFS-Replikationseinstellungen müssen zu allen Domänencontrollern repliziert werden, und jedes Mitglied der Replikationsgruppe muss seinen nächstgelegenen Domänencontroller abfragen, um diese Einstellungen zu erhalten. Die erste Replikation tritt zunächst zwischen dem primären Mitglied und den empfangenden Replikationspartnern des primären Mitglieds auf. Wenn ein Mitglied alle Dateien vom primären Mitglied empfangen hat, repliziert dieses Mitglied Dateien ebenfalls zu seinen empfangenden Partnern. Beim Empfang von Dateien des primären Mitgliedsservers während der ersten Replikation, verschieben die empfangenden Mitgliedsserver Dateien, die auf dem primären Server nicht vorhanden sind, in den Ordner *DfsrPrivate\PreExisting*. Wenn eine Datei mit einer Datei auf dem primären Mitglied identisch ist, wird die Datei nicht repliziert. Wenn sich die Version einer Datei auf dem empfangenden Mitglied von der Version des primären Mitglieds unterscheidet, wird die Version des empfangenden Mitglieds in den Konfliktordner für gelöschte Dateien verschoben. Nach der Initialisierung des replizierten Ordners wird die Bezeichnung *Primäres Mitglied* entfernt.

Die Initialisierung findet statt, wenn alle Dateien, die vor der Übernahme der Konfiguration durch die DFS-Replikation vorhanden waren, der DFS-Replikationsdatenbank hinzugefügt wurden. Das Mitglied, das zuvor primäres Mitglied war, wird dann wie jedes andere Mitglied behandelt, und seine Dateien werden nicht länger als autorisierend im Vergleich zu denen der anderen Mitglieder angesehen. Alle Mitglieder, die die erste Replikation abgeschlossen haben, werden gegenüber Mitgliedern ohne abgeschlossene erste Replikation als autorisierend betrachtet.

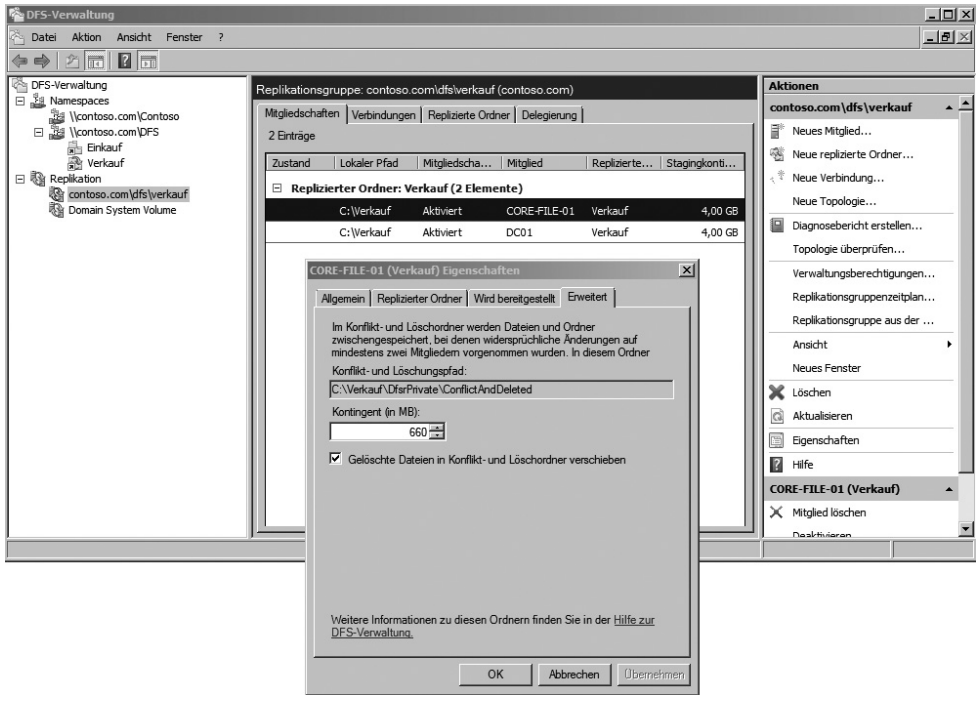
Abbildg. 6.47 Nachträgliche Kontrolle der Replikationsverbindung



Klicken Sie auf die Replikationsverbindung, können Sie auf vier Registerkarten die Einstellungen der Replikationsgruppe überprüfen. Auf diesen Registerkarten werden unterschiedliche Details zur ausgewählten Replikationsgruppe, ihren Mitgliedern und ihren replizierten Ordnern angezeigt:

- **Registerkarte *Mitgliedschaften*** Hier sind die Einträge nach repliziertem Ordner sortiert. Doppelklicken Sie auf ein Mitglied, um die Eigenschaften pro Mitglied und pro repliziertem Ordner auf den Registerkarten anzuzeigen. Auf der Registerkarte *Erweitert* können Sie Speicherort und Größe des Stagingordners und des Konfliktordners für gelöschte Dateien auf dem ausgewählten Mitglied anzeigen (Abbildung 6.48).

Abbildg. 6.48 Konfigurieren der Mitgliedschaften einer Replikationsgruppe



- **Registerkarte *Verbindungen*** Jede Verbindung ist ein einseitiger Replikationspfad, sodass für die Replikation zwischen zwei Mitgliedern zwei Verbindungen erforderlich sind, die Daten in der jeweiligen Gegenrichtung replizieren. Jede Verbindung verfügt über einen Zeitplan und andere Einstellungen, zum Beispiel zum Aktivieren oder Deaktivieren der Remotedifferenzialkomprimierung (Remote Differential Compression, RDC). Doppelklicken Sie auf eine Verbindung, um deren Einstellungen anzuzeigen.

Erstellen eines Diagnoseberichts

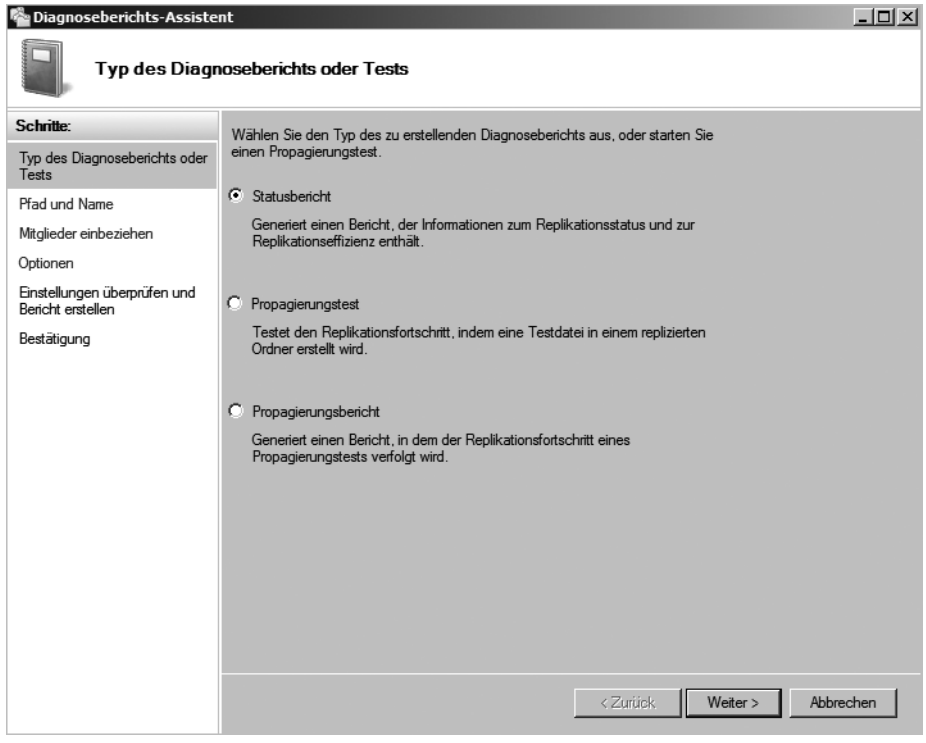
Über das Aktionsmenü der DFS-Verwaltung können Sie einen Assistenten starten, über den Sie einen Diagnosebericht erstellen lassen können. Der Bericht wird als HTML-Datei erstellt (Abbildung 6.49). Mit dem Assistenten lassen sich sehr schnell und einfach Berichte über die Replikation erstellen.

Abbildg. 6.49 Anzeigen eines Berichts der DFS-Replikation

TIPP Wollen Sie regelmäßig automatisch Diagnoseberichte erstellen, bietet sich auch das Befehlszeilen-Tool *Dfsradmin.exe* an. Sie können ein Skript erstellen, das Sie als Aufgabe hinterlegen und mit dem Sie automatisch Berichte erstellen lassen. Ein Beispielskript für diese Aufgabe finden Sie auf der Internetseite *https://blogs.technet.com/filecab/articles/437214.aspx*.

Auf Basis dieser Berichte lässt sich schnell ein Überblick gewinnen, ob die Replikation innerhalb der DFS-Infrastruktur funktioniert. Der Assistent führt durch die zahlreichen Optionen, die bei der Erstellung des Berichts konfiguriert werden können.

Abbildg. 6.50 Erstellen eines Diagnoseberichts für das DFS



Encrypting File System (EFS)

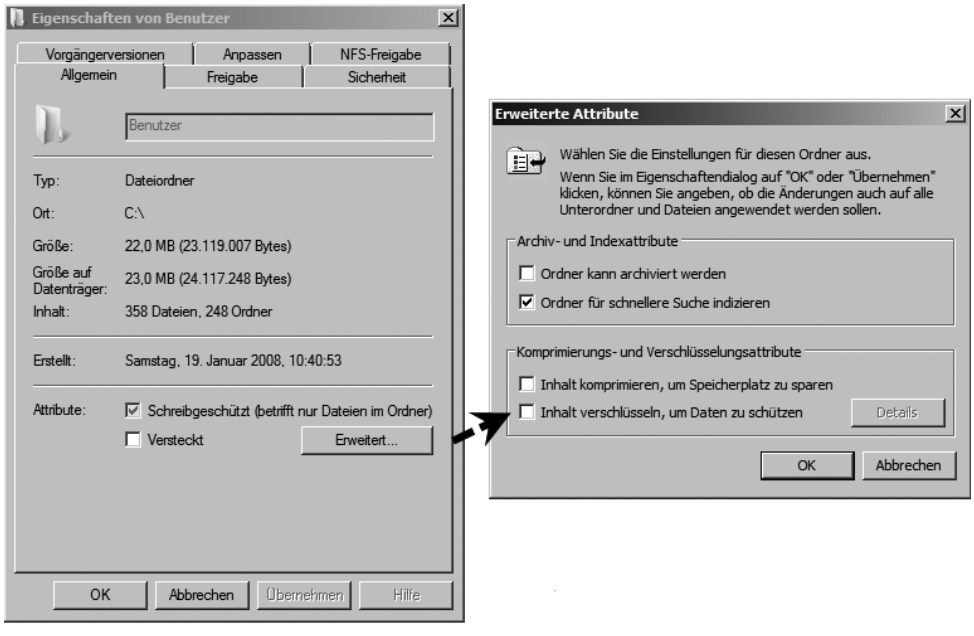
Das verschlüsselnde Dateisystem (Encrypting File System, EFS) erlaubt die Verschlüsselung von Informationen auf der lokalen Festplatte. Das EFS kann lokal eingesetzt werden. In diesem Fall reicht es aus, wenn der Benutzer definiert, dass Dateien verschlüsselt werden sollen. Das EFS kann aber auch in verteilten Umgebungen eingesetzt werden. In diesem Fall muss mit einer Zertifikatstelle (siehe Kapitel 17) gearbeitet werden, da die Verschlüsselung über digitale Zertifikate gesteuert wird. Um Dateien lokal zu verschlüsseln, wird der Befehl *Eigenschaften* im Kontextmenü der Datei oder des Verzeichnisses, das verschlüsselt werden soll, gewählt. Dort kann die Schaltfläche *Erweitert* ausgewählt werden. Im angezeigten Dialogfeld findet sich das Kontrollkästchen *Inhalt verschlüsseln, um Dateien zu schützen*. Durch Auswahl dieses Kontrollkästchens wird das EFS genutzt. Die Verschlüsselung und der Zugriff auf diese Informationen erfolgen transparent für die Anwender. Falls ein Verzeichnis für die Verschlüsselung ausgewählt wurde, fragt das System, ob die Einstellungen für untergeordnete Verzeichnisse übernommen werden sollen. Beachten Sie, dass die Ver- und Entschlüsselung auch vom Clientbetriebssystem unterstützt werden muss. Sie benötigen mindestens Windows 2000 Professional, um verschlüsselte Dateien auf dem Server oder auf lokalen Festplatten ablegen zu können. Eine gemeinsame Nutzung verschlüsselter Dateien ist sogar erst ab Windows XP Professional möglich. EFS verschlüsselt die Daten auf der Festplatte und entschlüsselt die Daten nur, wenn die zur Verschlüsselung verwendeten Anmeldeinformationen eingegeben werden. Wenn Verschlüsselung für einen Ordner festgelegt wird, verschlüsselt EFS automatisch Folgendes:

- Alle neu im Ordner erstellten Dateien
- Alle Textdateien, die in den Ordner kopiert oder verschoben werden
- Optional die meisten vorhandenen Dateien und Unterordner, mit der ausdrücklichen Ausnahme von Windows-Systemdateien und Benutzerprofilen

EFS verwendet einen öffentlichen Schlüssel zum Verschlüsseln von Dateien. Daher sind für die Verschlüsselung ein Paar aus öffentlichem und privatem Schlüssel, und ein öffentliches Schlüsselzertifikat erforderlich. Zur Verwendung von EFS müssen die Benutzer im Besitz von EFS-Zertifikaten sein, für die die beiden folgenden Optionen verfügbar sind:

- **Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure, PKI)** Es kann eine Public Key Infrastructure (PKI) bereitgestellt werden.
- **Selbstsignierte Zertifikate** Selbstsignierte Zertifikate werden automatisch vom Betriebssystem generiert.

Abbildg. 6.51 Verschlüsseln von Dateien mit EFS



Die Funktionsweise von EFS

Windows XP und Windows Vista generieren EFS-Zertifikate automatisch. Die Benutzer erhalten ein Zertifikat, indem sie eine Datei verschlüsseln. Jeder Benutzer, der sich beim Computer anmeldet, kann Dateien verschlüsseln. EFS generiert ein eindeutiges Zertifikat und ein Schlüsselpaar für jeden Benutzer. Sofern ein Benutzer die verschlüsselten Dateien nicht für andere freigibt, kann kein Benutzer auf Dateien zugreifen, die einem anderen Benutzer gehören. EFS nutzt das EFS-Zertifikat eines Benutzers, um den Inhalt einer Datei zu verschlüsseln. Der private Schlüssel wird in verschlüsselter Form mit in der Datei abgelegt und kann zur Wiederherstellung der Datei genutzt werden. EFS arbeitet mit dem symmetrischen DESX-Algorithmus zur Dateiverschlüsselung und dem RSA-

Algorithmus zur Verschlüsselung der privaten Schlüssel. Durch eine mögliche Wiederherstellung des privaten Schlüssels ist eine Entschlüsselung von Dateien durch so genannte Wiederherstellungs-Agenten möglich. Falls keine Zertifikatdienste verfügbar sind, beispielsweise in einer Arbeitsgruppe, generiert EFS automatisch im lokalen System ein selbst signiertes Zertifikat für den aktuellen Benutzer und verwendet dieses Zertifikat für die Verschlüsselung. Beachten Sie, dass andere Benutzer die Datei immer noch umbenennen oder löschen können, wenn Sie dies nicht in den Dateisicherheitseinstellungen (ACLs) verhindern. Der Dateiinhalt ist lediglich vor dem Auslesen durch unberechtigte Personen geschützt. Alternativ zur grafischen Oberfläche können Sie auch den Befehl *Cipher* in der Befehlszeile einsetzen, um Dateien zu ver- und entschlüsseln oder sich den Status anzeigen zu lassen. Der Befehl:

- **cipher /e /s:c:\vertraulich** verschlüsselt das Verzeichnis *c:\vertraulich* und alle darunter liegenden Verzeichnisse und Dateien
- **cipher /d /s:c:\vertraulich** entschlüsselt die Daten im Verzeichnis *c:\vertraulich* und allen darunter liegenden Verzeichnisse

Verschlüsselung für mehrere Personen nutzen

Häufig ist es sinnvoll, vertrauliche Daten mit einer anderen Person zu teilen, beispielsweise zwischen zwei Geschäftsführern, oder Chef und Sekretärin. Wenn Sie auch anderen Personen Zugriff auf Ihre EFS-verschlüsselten Dateien gewähren wollen, müssen diese explizit berechtigt werden:

1. Verschlüsseln Sie zuerst die Datei wie oben beschrieben.
2. Rufen Sie nochmals die *Eigenschaften* der Datei auf, klicken Sie auf *Erweitert* und danach auf *Details*.
3. Sie erhalten eine Übersicht darüber, welche Benutzer auf die Datei zugreifen können (obere Liste) und welche Benutzer die Datei wiederherstellen und dabei die Verschlüsselung aufheben können (untere Liste).
4. Klicken Sie auf *Hinzufügen*, um nacheinander alle Benutzer einzutragen, die auf Ihre verschlüsselte Datei Zugriff erhalten sollen.

Sie können an dieser Stelle nur Benutzer eintragen, keine Gruppen. Die Benutzer benötigen außerdem jeweils ein EFS-Zertifikat. Sie können deshalb die Verschlüsselung nur innerhalb einer Active Directory-Domäne mit installierten Zertifikatdiensten, und manuell oder automatisch zugeordneten Benutzerzertifikaten für Basic EFS sinnvoll einsetzen. Am Ende des Vorgangs können Sie in den Dateieigenschaften die Liste aller zugelassenen Benutzer überprüfen. Alle diese Benutzer können auf die verschlüsselte Datei zugreifen.

Wann sollte EFS nicht genutzt werden

Einige Hindernisse können Ihnen bei der Nutzung von EFS im Wege stehen oder sogar eine erfolgreiche Wiederherstellung der Daten verhindern. Als Administrator sollten Sie diese Klippen kennen, damit Sie nicht erst im Fehlerfall bemerken, dass eine Datei nicht mehr zugänglich ist.

- Sie können eine Datei nicht gleichzeitig verschlüsseln und komprimieren. Wenn Sie eine bereits verschlüsselte Datei komprimieren und die erforderlichen Zertifikate besitzen, wird die Datei automatisch entschlüsselt.

- Wenn Sie keine NTFS-Laufwerke, sondern FAT16 oder FAT32 einsetzen, können Sie die Verschlüsselung nicht nutzen. Dies bedeutet, dass es unmöglich ist, eine verschlüsselte Datei auf CD zu brennen oder auf Diskette zu kopieren, ohne die Verschlüsselung zu verlieren.
- Wenn Sie eine verschlüsselte Datei kopieren, wird diese während des Kopierens im Hauptspeicher des PCs entschlüsselt. Am Zielort wird die Datei nur dann wieder verschlüsselt, wenn der Zielordner ebenfalls das Attribut *Verschlüsselt* besitzt. Wenn Sie also eine lokal verschlüsselte Datei auf den Server kopieren, verliert diese ihre Verschlüsselung, falls Sie im Serververzeichnis nicht vorher ebenfalls die Verschlüsselung aktivieren.
- Systemdateien können nicht verschlüsselt werden.
- Offlinedateien können erst ab Windows XP Professional verschlüsselt werden.
- Wenn Sie nicht in einer Domäne arbeiten, hat nur der lokale Administrator die Möglichkeit der Datenwiederherstellung. Sollte also die lokale Benutzerdatenbank einmal kaputt gehen oder das Administratorkennwort unauffindbar verschwinden, ist eine Wiederherstellung der verschlüsselten Dateien dieses PCs unmöglich. Achten Sie in diesem Fall darauf, dass Sie von jedem Einzelsystem eine Systemstatussicherung besitzen. Hier ist die Benutzerdatenbank enthalten.
- Einige Anwendungen zerstören die Zertifikate der zusätzlichen Benutzer beim Schreiben in die Datei. Nur speziell angepasste Programme, beispielsweise Office 2007, behalten die EFS-Zertifikate aller Benutzer bei der Dateibearbeitung bei.

Wiederherstellung von verschlüsselten Dateien

Wichtig ist nicht nur das Verschlüsseln, sondern auch die Wiederherstellung von Dateien für den Fall, dass ein Benutzer nicht mehr im System verfügbar oder sein Kennwort nicht bekannt ist. Das Sichern eines Wiederherstellungsschlüssels hilft sicherzustellen, dass die verschlüsselten Daten für den Fall wiederhergestellt werden können, dass der Benutzer, der das EFS-Verschlüsselungszertifikat besitzt, die Daten nicht entschlüsseln kann. Die Sicherung für den Wiederherstellungsschlüssel muss mithilfe des Kontos des Wiederherstellungs-Agenten erfolgen, das über das Dateiwiederherstellungs-Zertifikat und den privaten Schlüssel in seinem privaten Informationsspeicher verfügt. Der standardmäßige Wiederherstellungs-Agent ist der Domänenadministrator.

Damit ein Konto mithilfe von EFS verschlüsselte Daten lesen oder wiederherstellen kann, richten Sie das Konto als Wiederherstellungs-Agent ein. In einer Domänenumgebung ist es ratsam, für diesen Zweck Domänenkonten zu verwenden. Ein Wiederherstellungs-Agent kann für jeden Standort, Domäne oder Organisationseinheit in einer Active Directory-Gesamtstruktur erstellt werden. Standardmäßig ist das eingebaute Administratorkonto für eine Domäne ein Wiederherstellungs-Agent. Zum Entschlüsseln von EFS-Dateien genügt es nicht unbedingt, lokale Administratorrechte auf dem betreffenden System zu haben, sondern Sie müssen als *Wiederherstellungs-Agent* in der Datei eingetragen sein, um diese wieder in Klartext zu verwandeln. Wer zum Wiederherstellungs-Agenten wird und damit automatisch entsperrenden Zugriff auf verschlüsselte Dateien hat, muss mithilfe so genannter *Wiederherstellungsrichtlinien* bereits vor der Verschlüsselung der ersten Dateien festgelegt werden. Wenn Sie die Wiederherstellungs-Agenten in einem laufenden System ändern, wirkt sich dies nicht immer auf alle verschlüsselten Dateien aus. Speziell lokal auf den Arbeitsstationen verschlüsselte Dateien bleiben an den alten Wiederherstellungs-Agenten gebunden, auch wenn Sie Richtlinien in der Domäne verändern.

Sie können für jede verschlüsselte Datei in den Eigenschaften unter *Erweitert/Details* überprüfen, welche Benutzer die Datei wiederherstellen und dabei die Verschlüsselung aufheben können. Wenn Sie nichts weiter konfiguriert haben, gibt es zwei Standardfälle für die Wiederherstellung von Dateien:

- Auf einem lokalen System (Arbeitsgruppe) wird automatisch der lokale Administrator als Wiederherstellungs-Agent eingetragen.
- Innerhalb einer Domäne gibt es ein Wiederherstellungszertifikat, das standardmäßig der Gruppe *Administratoren* in der Domäne zugewiesen wurde. Diese Zuweisung können Sie jedoch mithilfe von Richtlinien verändern und somit das Recht zur Dateiwiederherstellung an jeden beliebigen Domänenbenutzer übertragen.

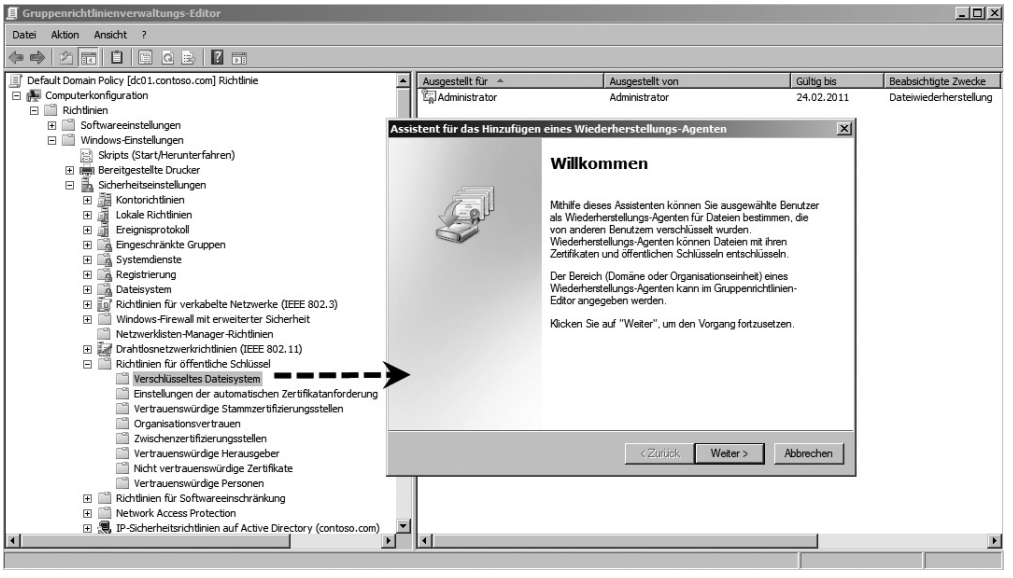
Ein Datensicherungsprogramm, dessen Dienstekonto der Gruppe *Backup-Operatoren* angehört, kann den verschlüsselten Inhalt der Dateien auch ohne Wiederherstellungsfunktion auslesen. Der Inhalt bleibt dabei jedoch verschlüsselt und wird nicht im Klartext auf das Sicherungsmedium übertragen. Geben Sie dem Dienstekonto, das Sie für das Backup einsetzen, nicht die Funktion des Wiederherstellungs-Agenten, sonst werden Ihre Dateien während des Backups entschlüsselt und im Klartext auf das Band geschrieben.

Eigene Wiederherstellungs-Agenten einrichten

Um die Wiederherstellung von Dateien durch andere Benutzer als den Domänenadministrator zu ermöglichen, können Sie eigene Wiederherstellungs-Agenten einrichten. Diese Personen können dann – auch ohne Administratorrechte – auf alle Dateien zugreifen. So können Sie beispielsweise der Revision Zugriff auf alle Dateien gewähren oder der Datensicherungssoftware ein Restore des Dateiinhalts im unverschlüsselten Zustand ermöglichen. Der Wiederherstellungs-Agent sollte das Datenwiederherstellungszertifikat und den privaten Schlüssel auf einen Datenträger exportieren, diesen an einem sicheren Ort verwahren und den privaten Schlüssel aus dem System löschen. Auf diese Weise kann nur die Person Daten für das System wiederherstellen, der der Aufbewahrungsort des privaten Schlüssels bekannt ist. Die Anzahl der Wiederherstellungs-Agenten sollte auf ein Minimum beschränkt werden. Wenn Sie Zertifikatdienste konfigurieren und eine benutzerdefinierte Zertifikatvorlage zum Ausstellen von EFS-Zertifikaten verwenden, aktivieren Sie nicht die Option *Benutzer zur Eingabe während der Registrierung auffordern* und *Benutzereingabe beim Verwenden eines privaten Schlüssels anfordern*. Diese Option verhindert, dass EFS den privaten Schlüssel für die Ver- oder Entschlüsselung verwendet.

Um einen Benutzer als Wiederherstellungs-Agenten auf einem lokalen System einzusetzen, rufen Sie die lokale Sicherheitsrichtlinie auf und wählen den entsprechenden Unterpunkt in diesem Menü aus. Klicken Sie auf *Sicherheitseinstellungen/Richtlinien öffentlicher Schlüssel/global verschlüsselndes Dateisystem*. Falls der Benutzer bereits ein EFS-Wiederherstellungszertifikat besitzt, wählen Sie im Kontextmenü den Befehl *Wiederherstellungs-Agenten* aus. In diese Liste muss der Wiederherstellungs-Agent eingetragen werden. Klicken Sie nun auf *Verzeichnis durchsuchen*, um einen Wiederherstellungs-Agenten auszuwählen. Möglicherweise erhalten Sie bei der Auswahl eines Benutzers eine Fehlermeldung. In diesem Fall müssen Sie erst ein EFS-Wiederherstellungszertifikat für den Benutzer erstellen. Klicken Sie dazu auf *Abbrechen* und wählen Sie im Kontextmenü der Gruppenrichtlinie *global verschlüsselndes Dateisystem* den Eintrag *Dateiwiederherstellungs-Agenten erstellen* aus. Sie werden von einem Assistenten durch die Erstellung des passenden Zertifikats geführt.

Abbildg. 6.52 Auswählen eines Wiederherstellungs-Agenten



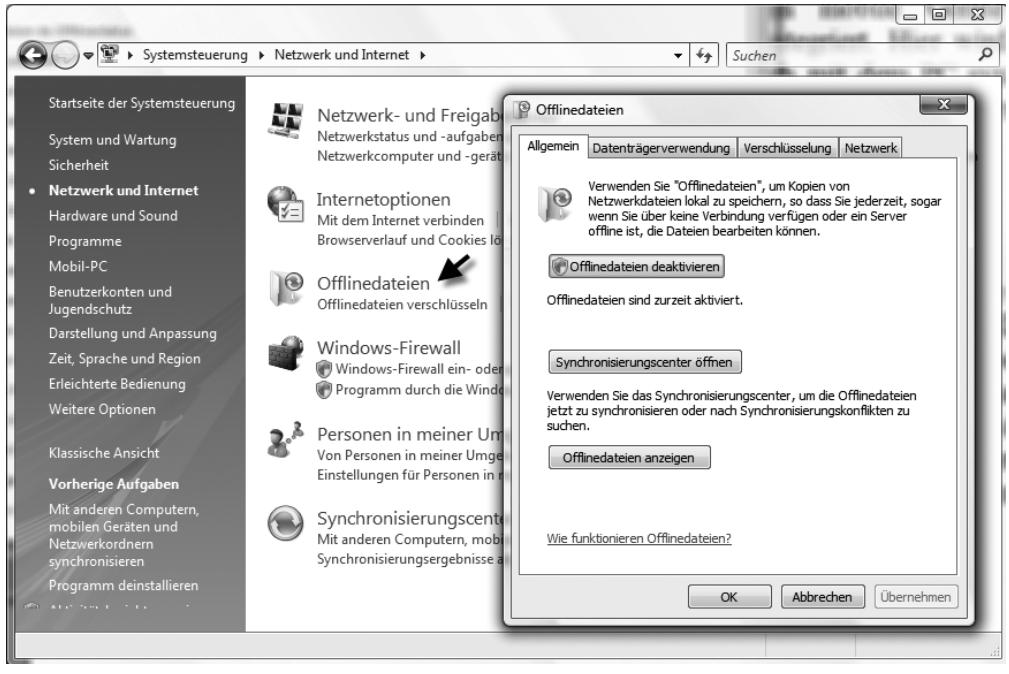
Achten Sie darauf, dass Sie nur ein EFS-Wiederherstellungszertifikat pro Benutzer erstellen, da das Management von mehreren Zertifikaten des gleichen Typs pro Benutzer sehr umständlich ist; Sie können dann nicht mehr die Automatikfunktionen des Betriebssystems verwenden. Um einen anderen Benutzer als Wiederherstellungs-Agenten in der gesamten Domäne einzusetzen, rufen Sie die Sicherheitsrichtlinien für Domänencontroller auf. Da die Entschlüsselung von Dateien ein sensibles Thema ist und in größeren Unternehmen nicht immer der Vollzugriff auf alle Daten gewünscht wird, können durch den Einsatz verschiedener Gruppenrichtlinien auch unterschiedliche Wiederherstellungs-Agenten für die Container, in denen sich die Computer befinden, konfiguriert werden.

Offlinedateien für den mobilen Einsatz unter Windows Vista

Mit den Offlinedateien haben Sie die Möglichkeit, Dateien aus dem Netzwerk, zum Beispiel von einem Dateiserver, auch dann verfügbar zu machen, wenn Sie mit einem Notebook unterwegs sind. Dazu wird auf dem Notebook eine Kopie der entsprechenden Datei erstellt, sodass diese auch ohne Netzwerkverbindung zur Verfügung steht. Sie können die entsprechenden Dateien auf dem Notebook bearbeiten, wenn Sie nicht mit dem Netzwerk verbunden sind. Bei der nächsten Verbindung werden die Dateien mit dem Server synchronisiert, sodass die Dateien auf dem Server und dem Notebook wieder übereinstimmen. Die Verwaltung der Offlinedateien unter Windows Vista findet über *Start/Systemsteuerung/Netzwerk* und *Internet/Offlinedateien* statt (Abbildung 6.53). Über die Schaltfläche *Offlinedateien aktivieren* bzw. *Offlinedateien deaktivieren* können Sie diese Funktion ein- oder ausschalten. In Zusammenarbeit mit Windows Vista wurde diese Funktion insoweit verbessert, dass der Zugriff auf die konfigurierten Offlinedateien im Onlinemodus, also wenn sich ein mobiler Anwender mit dem Netzwerk verbindet, deutlich schneller abgewickelt wird. Die generelle

Umschaltung zwischen Offline- und Onlinemodus wurde extrem beschleunigt. Vor allem bei der Zusammenarbeit mit der verbesserten Synchronisierung in Windows Vista sind Offlinedateien jetzt wesentlich effizienter als unter Windows Server/Windows XP.

Abbildg. 6.53 Offlinedateien unter Windows Vista zusammen mit einem Dateiserver einsetzen



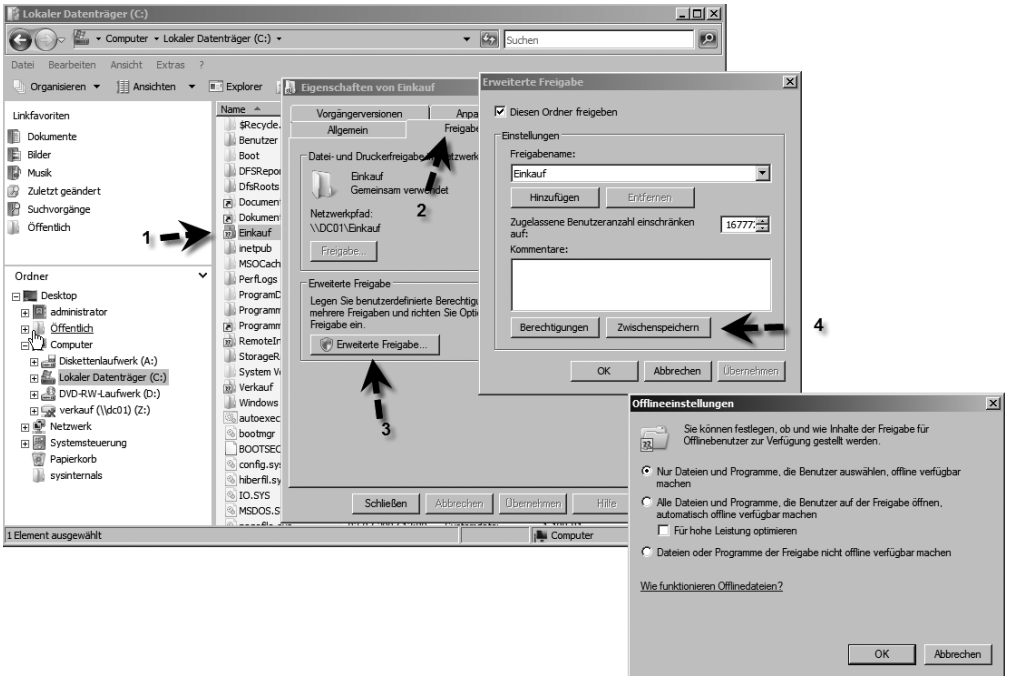
Konnte unter Windows Server 2003 auf eine einzige Datei in einem offline verfügbaren Verzeichnis nicht zugegriffen werden, wurde der komplette Ordner als Offline gekennzeichnet, was nicht sehr effizient war. In Windows Server 2008 werden nur die Dateien, die nicht online verfügbar sind, offline verwendet, alle anderen Dateien im Verzeichnis bleiben weiterhin online verfügbar. In den Eigenschaften jeder Offlinedatei können spezielle Einstellungen für Offlinedateien vorgenommen werden.

Nachdem das System für den Offlinebetrieb aktiviert ist, können Sie Ordner und Dateien von Servern für den Offlinebetrieb verfügbar machen. Hier gibt es Steuerungsmöglichkeiten sowohl vom Client als auch vom Server aus. Vom Client aus verwenden Sie den Befehl *Immer Offline verfügbar machen*, der sich im Kontextmenü findet, wenn Sie eine Freigabe, eine Datei oder ein Verzeichnis auf einem Server markiert haben, die oder das für den Offlinezugriff freigegeben ist. Sie können auf diese Weise einzelne Dateien, ganze Verzeichnisse oder ein komplettes Netzlaufwerk offline verfügbar machen. Achten Sie aber darauf, dass es sich bei Offlinedateien um Kopien von Dateien aus dem Netzwerk handelt und der Speicherplatz mit der Anzahl der Offlinedateien zunimmt. Sie sollten daher möglichst nur Dateien offline verwenden, die Sie auch tatsächlich benötigen, nicht gleich alle auf einmal.

Vom Server aus kann die Nutzung von Offlinedateien über die Freigabe gesteuert werden. Beim Erstellen von Freigaben findet sich die Option *Zwischenspeichern*. Wenn diese ausgewählt wird, kann gesteuert werden, ob das Zwischenspeichern von Dateien in dem freigegebenen Ordner zuge-

lassen wird oder nicht. Standardmäßig wird das manuelle Zwischenspeichern von Dateien zugelassen (Abbildung 6.54).

Abbildg. 6.54 Konfigurieren von Offlinedateien unter Windows Server 2008



Wenn die Option *Dateien oder Programme der Freigabe nicht offline verfügbar machen* aktiviert ist, erscheint der Befehl *Offline verfügbar machen* auf dem Client nicht. Es werden drei Varianten für das Zwischenspeichern von Dokumenten unterschieden:

- Mit *Nur Dateien und Programme, die Benutzer auswählen, offline verfügbar machen* wird definiert, dass über den Befehl *Offline verfügbar machen* auf dem Client Dateien lokal in den Cache genommen werden können.
- *Alle Dateien und Programme, die Benutzer auf der Freigabe öffnen, automatisch offline verfügbar machen* bewirkt, dass alle Dokumente und ausführbaren Dateien in dieser Freigabe lokal gecacht werden, auf die irgendwann zugegriffen wird. In diesem Fall muss sich der Benutzer nicht mehr darum kümmern, die Dokumente offline verfügbar zu machen.
- Über das Kontrollkästchen *Für hohe Leistung optimieren* kann festgelegt werden, dass ausführbare Dateien aus dieser Freigabe auf dem Client verfügbar bleiben, wenn sie einmal genutzt wurden. In diesem Fall sollten die Zugriffsberechtigungen für die Freigabe auf *Lesen* gesetzt werden, um zu verhindern, dass veränderte Programme zurückgespeichert werden. Generell ist es empfehlenswert, Programme nicht auf diesem Weg, sondern über die Softwareverteilungsmechanismen der Gruppenrichtlinien zu verteilen.

Sie können die Einstellungen der Synchronisierungseigenschaften von Offlinedateien im *Synchronisierungscenter* von Windows Vista anpassen. Das Synchronisierungscenter finden Sie über *Start/Systemsteuerung/Mobil-PC/Synchronisierungscenter*. Bei der Synchronisation kann es zu Konflikten

kommen. Dies ist immer dann der Fall, wenn eine Datei im Offlinebetrieb verändert wurde und wenn sie vor der Synchronisation auf dem Server verändert wurde. Der Client erkennt dies über einen Vergleich der Speicherungsdaten dieser Dateien und zeigt bei der Synchronisation Meldungen an. Bei einem Konflikt kann entweder die eigene Version der Datei übernommen oder die eigene Datei unter einem anderen Namen abgespeichert werden. Es gibt keine Funktion, mit der die Inhalte von Dateien synchronisiert werden könnten. Allerdings gibt es Anwendungsprogramme wie Microsoft Word, die entsprechende Funktionen bereitstellen und zwei parallel geänderte Dateien zusammenführen können.

Abbildg. 6.55 Konfigurieren der Synchronisierung von Offlinedateien über das Synchronisierungscenter in Windows Vista

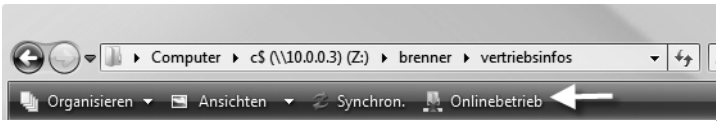
Arbeiten mit Offlinedateien

Als Bestätigung, dass eine Datei oder der Ordner offline verfügbar ist, klicken Sie erneut mit der rechten Maustaste auf die Datei oder den Ordner. Überprüfen Sie, ob ein Häkchen neben *Immer offline verfügbar* angezeigt wird. Eine Kopie der Datei auf der Festplatte wird mit der Netzwerkkopie synchronisiert, sobald die Netzwerkverbindung wieder hergestellt wird. Wenn Sie eine Datei als Offlinedatei markieren, erhält diese ein neues Dateisymbol, dass die Datei als Offlinedatei kennzeichnet (Abbildung 6.56).

Abbildg. 6.56 Dateisymbol einer Offlinedatei

Wenn Sie einen ganzen Ordner als offline verfügbar markieren, erhält auch dieser ein spezielles Symbol. Um eine Datei offline zu bearbeiten, auch wenn Sie mit dem Netzwerk verbunden sind, öffnen Sie den Netzwerkordner und klicken in der Symbolleiste auf *Offlinebetrieb*. Diese Schaltfläche wird nur angezeigt, wenn Sie diesen Ordner bereits offline verfügbar gemacht haben. Sie können den Offlinebetrieb auch aktivieren, wenn Sie mit dem Netzwerk verbunden sind. So können Sie sicherstellen, dass Sie auf jeden Fall die Offlinekopie der Datei bearbeiten, nicht die Quelldatei im Netzwerk. Wenn Sie die Bearbeitung der Offlinedateien abgeschlossen haben und wieder die Dateien im Netzwerkordner bearbeiten möchten, klicken Sie in der Symbolleiste auf *Onlinebetrieb* (Abbildung 6.57).

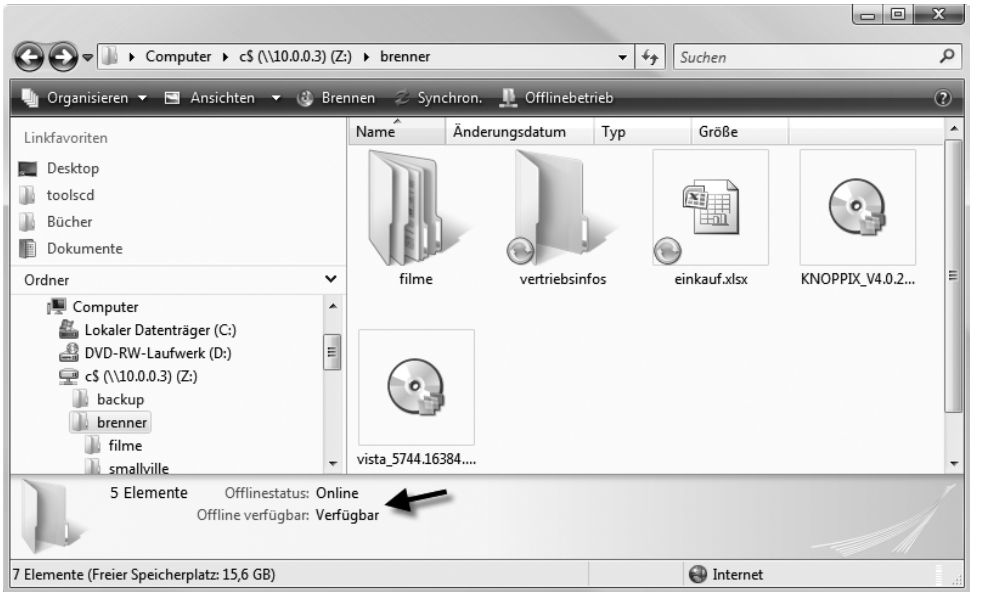
Abbildg. 6.57 Aktivieren des Offline- und des Onlinebetriebs für Offlinedateien



Durch Aktivierung des Onlinebetriebs werden alle offline vorgenommenen Änderungen mit den Dateien im Netzwerk synchronisiert. Um festzustellen, ob Sie offline arbeiten, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Netzwerkordner mit der zu bearbeitenden Datei.
2. Überprüfen Sie den Status unten im Detailfenster. Wenn der Status *Offline* lautet, arbeiten Sie an einer Offlinekopie der Datei auf dem Computer. Lautet der Status *Online*, arbeiten Sie an der Datei im Netzwerk (Abbildung 6.58).

Abbildg. 6.58 Anzeigen des Onlinestatus einer Offlinedatei



Wenn Sie mit Offlinedateien in verschiedenen Ordnern arbeiten, können Sie alle Dateien anzeigen, ohne jeden Ordner einzeln öffnen zu müssen:

1. Öffnen Sie wie beschrieben die Verwaltung der Offlinedateien in Windows.
2. Holen Sie die Registerkarte *Allgemein* in den Vordergrund und klicken Sie darin auf *Offlinedateien anzeigen*.

TIPP Sie können das Verwaltungsprogramm für die Offlinedateien auch über *Start/Ausführen/control.exe cscui.dll* aufrufen.

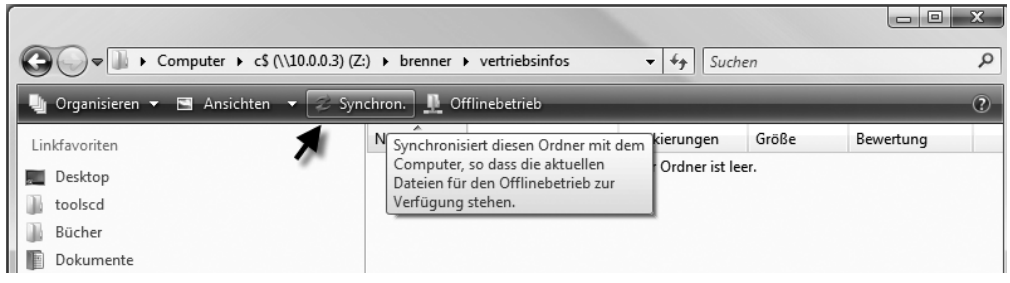
Synchronisieren der Offlinedateien mit dem Server

Windows synchronisiert die Offlinedateien automatisch, jedoch nicht kontinuierlich. Manchmal empfiehlt es sich, die Offlinedateien sofort zu synchronisieren, beispielsweise dann, wenn die Verbindung zum Netzwerk demnächst getrennt wird und sichergestellt sein muss, dass die neuesten Dateiversionen im Netzwerk gespeichert sind. Wenn Sie erstmalig Offlinedateien einrichten, wird im Infobereich der Taskleiste neben der Uhr ein neues Symbol integriert, welches das Synchronisierungscenter darstellt. Wenn Sie mit der rechten Maustaste auf das Symbol klicken, können Sie auf die wichtigsten Funktionen zugreifen, zum Beispiel *Alle synchronisieren*. Neben dieser Möglichkeit können Sie die Synchronisierung auch auf einem anderen Weg erreichen:

1. Öffnen Sie das *Synchronisierungscenter.*
2. Klicken Sie auf die Synchronisierungspartnerschaft *Offlinedateien* und dann auf der Symbolleiste auf *Alle synchronisieren.*

Wenn Sie nur den Inhalt eines bestimmten Ordners synchronisieren möchten, öffnen Sie den Ordner und klicken Sie dann auf der Symbolleiste auf *Synchronisieren* (Abbildung 6.59). Zum Synchronisieren einer einzelnen Datei klicken Sie mit der rechten Maustaste auf die Datei und anschließend auf Synchronisieren. Nachdem Sie Offlinedateien aktiviert und eingerichtet haben, werden diese als eine Synchronisierungspartnerschaft im Synchronisierungscenter angezeigt. Hierüber können Sie auch eventuelle Konflikte erkennen, sowie weitere Einstellungen vornehmen.

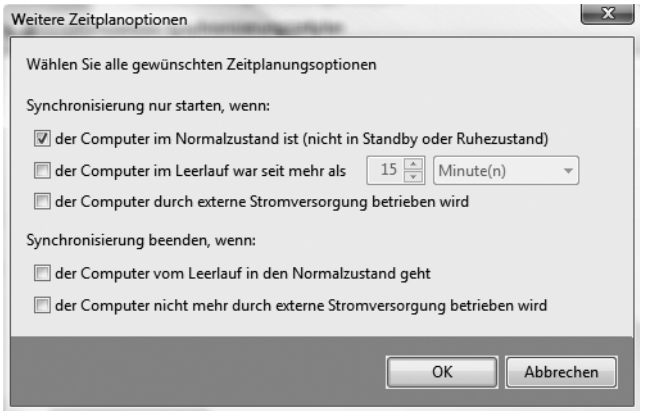
Abbildg. 6.59 Synchronisieren eines Offlineordners



Zusätzlich können Sie in den Eigenschaften eines offline verfügbaren Ordners auf der Registerkarte *Offlinedateien* den aktuellen Stand des Ordners einsehen. Hier können Sie auch die Offline-Verfügbarkeit des Ordners steuern und die Synchronisierung aktivieren. Wenn Sie im Synchronisierungscenter die Synchronisierungspartnerschaft der Offlinedateien öffnen, können Sie über die Schaltflä-

che *Zeitplan* genau einstellen, wann die Offlinedateien synchronisiert werden sollen. Auf der ersten Seite des Assistenten können Sie zunächst festlegen, für welche übergeordneten Netzlaufwerke Sie den Zeitplan für die Synchronisierung steuern wollen. Auf der nächsten Seite legen Sie fest, ob die Synchronisierung zeitabhängig erfolgen soll, oder nach einer bestimmten Aktion, zum Beispiel der Anmeldung am PC. Wählen Sie zur Synchronisierung die Option *Nach Zeitplan* aus, können Sie auf der nächsten Seite festlegen, zu welchem Zeitpunkt die Synchronisierung stattfinden soll. Hier können Sie auch einstellen, wie oft die Synchronisierung stattfinden soll und in welchen Abständen sie wiederholt wird. Über die Schaltfläche *Weitere Optionen* lässt sich detailliert einstellen, wann die Synchronisierung starten soll und wann nicht. Hier können vor allem für Notebooks Einstellungen vorgenommen werden, die eine Synchronisierung verhindern, um die Akkulaufzeit zu erhöhen.

Abbildg. 6.60 Festlegen des Zeitplans für die Synchronisierung

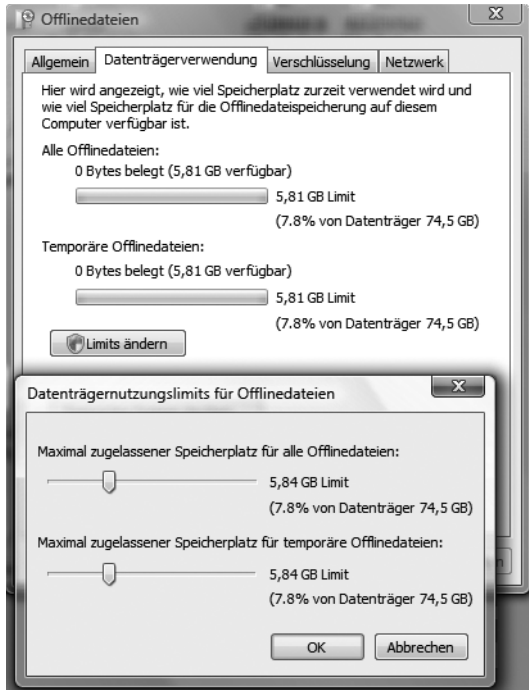


Wollen Sie als Synchronisierungsoption keine Zeiten konfigurieren, sondern spezielle Ereignisse, wie zum Beispiel die Anmeldung oder das Sperren des PCs, wählen Sie die Option *Über ein Ereignis oder einen Vorgang* auf der Startseite des Assistenten. Im Anschluss stellt Ihnen Windows Vista die Ereignisse zur Verfügung, die eine Synchronisierung auslösen. Über die Schaltfläche *Weitere Optionen* erreichen Sie die gleichen Detaileinstellungen, wie bei der Synchronisierung nach Zeitplan.

Konfigurieren der Speicherplatzverwendung von Offlinedateien

Die Größe und Anzahl der Offlinedateien bestimmen den Umfang des verwendeten Speicherplatzes auf der Festplatte, den die Offlinedateien belegen. Um festzustellen, wieviel Speicherplatz die Offlinedateien belegen, öffnen Sie die Verwaltung der Offlinedateien in der Systemsteuerung und wechseln zur Registerkarte *Datenträgerverwendung*. Hier sehen Sie, wie viel Speicherplatz von den Offlinedateien belegt wird (Abbildung 6.61).

Abbildg. 6.61 Konfigurieren des Speicherplatzes für Offlinedateien

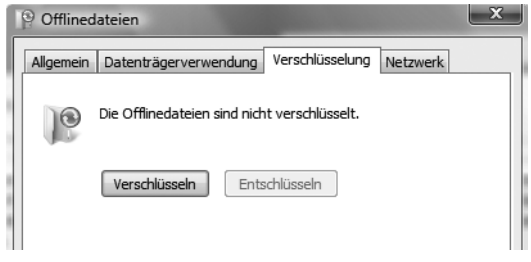


Über die Schaltfläche *Limits ändern* können Sie den Speicherplatz steuern, der auf dem Notebook für Offlinedateien zur Verfügung steht.

Verschlüsseln von Offlinedateien

Offlinedateien werden nur dann verschlüsselt, wenn Sie dies entsprechend auswählen. Sie können über die Registerkarte *Verschlüsselung* das Verschlüsseln von Offlinedateien aktivieren. Beim Verschlüsseln der Offlinedateien verschlüsseln Sie nur die auf dem Computer gespeicherten Offlinedateien, nicht die Netzwerkversionen der Dateien. Unter Windows-Versionen ohne EFS (Encrypting File System, verschlüsselndes Dateisystem) wird die Registerkarte *Verschlüsselung* nicht angezeigt.

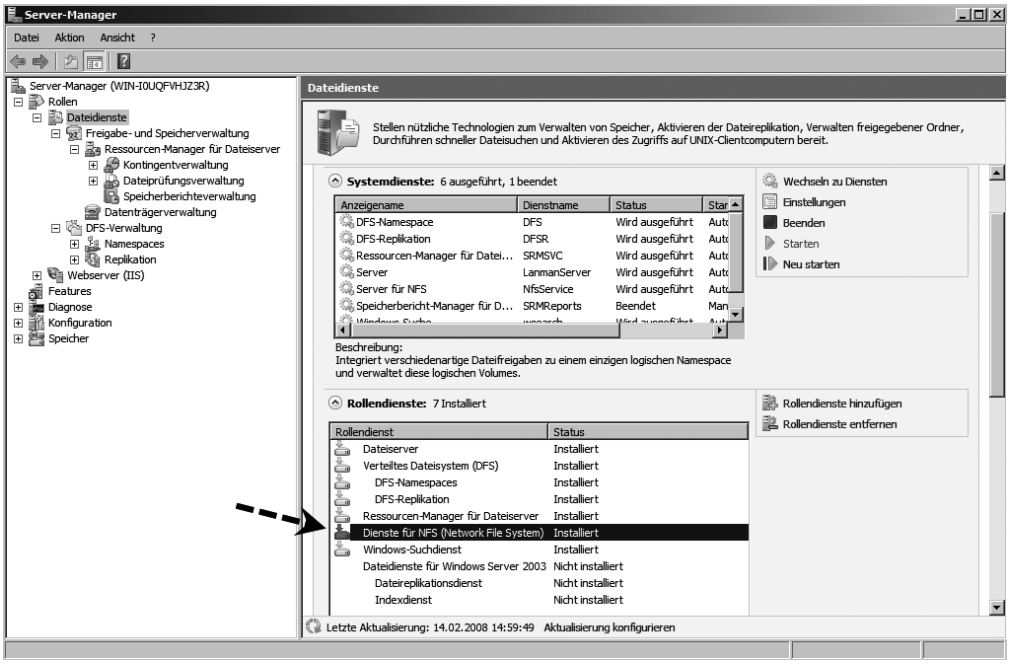
Abbildg. 6.62 Offlinedateien verschlüsseln



Network File System (NFS)

Das NFS ermöglicht Unternehmen, die Windows Server 2008 und UNIX-Systeme einsetzen, den Datenaustausch zwischen den beiden Systemen. Beim NFS handelt es sich um eine Aktualisierung der *Windows Services for UNIX 3.5*. NFS gehört zum Bestandteil von Windows Server 2008 Standard, Enterprise und Datacenter-Edition. Wollen Sie NFS nutzen, können Sie diese Funktion im Server-Manager als Rollendienst für die Rolle *Dateidienste* installieren (Abbildung 6.63). Für den Zugriff auf Dateien auf NFS-Servern benötigt jeder Windows-Benutzer eine Identität im UNIX-Format. Neu ist unter anderem, dass Active Directory-Objekte jetzt direkt für NFS genutzt werden können, es müssen keine zwei Identitäten angelegt werden. NFS in Windows Server 2008 unterstützt jetzt auch 64 Bit und weist daher eine deutlich höhere Leistung auf.

Abbildg. 6.63 Installieren von NFS als Rollendienst über den Server-Manager



Microsoft hat in NFS im Vergleich zu den Windows Services for UNIX 3.5 einige Neuerungen integriert:

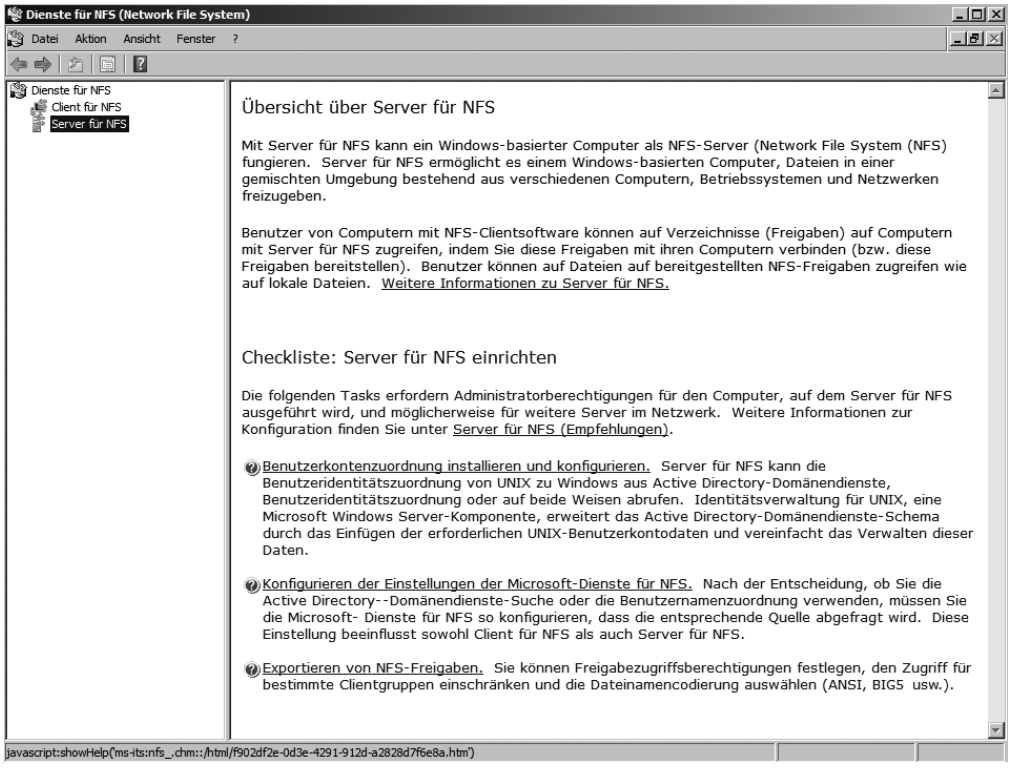
- Active Directory Lookup – Die UNIX Identity Management Active Directory Schema Extension, enthält UNIX User Identifier (UID) und Group Identifier (GID)-Felder, welche es den NFS-Clients ermöglichen, UNIX-Identitätsinformationen direkt in Active Directory abzufragen.
- NFS kann auch auf den 64-Bit-Editionen von Windows Server 2008 installiert werden.
- Die Performance und der Zugriff wurden erheblich verbessert.
- Mknod-Geräte unter UNIX werden jetzt auch von NFS unterstützt.

NFS besteht hauptsächlich aus drei Komponenten, um UNIX-Systeme mit Windows Server 2008 zu verbinden:

- **Identitätsverwaltung für UNIX (User Name Mapping)** Mit dieser Funktion können Benutzerkonten zwischen Windows- und UNIX-Domänen assoziiert werden. Dadurch müssen sich Benutzer nicht mehr separat an den Windows-Systemen und an UNIX anmelden, sondern es reicht entweder die Anmeldung an Windows oder die an UNIX.
- **Server für NFS** Mit dieser Funktion können UNIX-Clients auf Freigaben von Windows-Servern zugreifen.
- **Client für NFS** Mit dieser Funktion wiederum können Windows-Clients auf Freigaben von UNIX-Servern zugreifen.

Für die Verwaltung von NFS steht sowohl die Verwaltungskonsole *Dienste für NFS* zur Verfügung, die Sie über *Start/Verwaltung* starten können, sowie verschiedene Befehle für die Befehlszeile.

Abbildg. 6.64 Verwalten von NFS über das Snap-In *Dienste für NFS*



Befehlszeilen-Tools zur Verwaltung von NFS

Die einzelnen Befehlszeilenprogramme zur Verwaltung bieten auch eine ausführliche Hilfe über deren Syntax, die Sie über *<Toolname>/?* aufrufen können. Die wichtigsten Befehlszeilen-Tools für NFS sind:

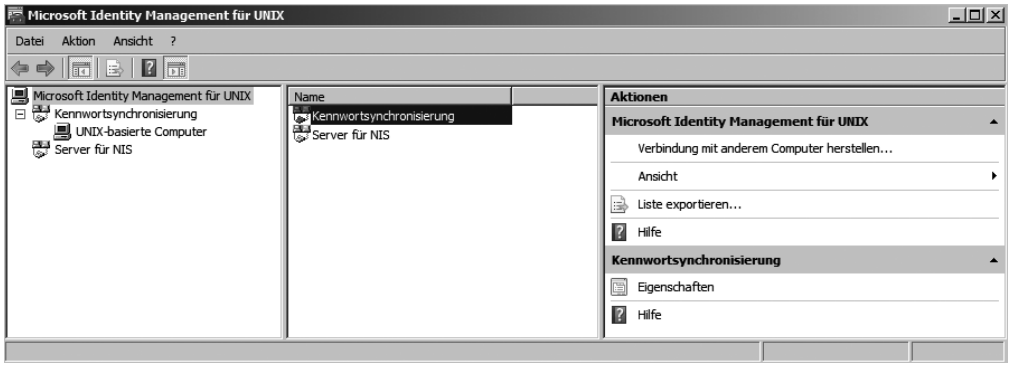
- **Mapadmin** Mit diesem Tool können Sie die Identitätsverwaltung für UNIX (User-Mapping) konfigurieren, falls diese installiert ist (siehe den folgenden Abschnitt).
- **Mount** Mit diesem Befehl werden NFS-Netzlaufwerke bereitgestellt.
- **Nfsadmin** Mit diesem Tool verwalten Sie den Client und den Server für NFS.
- **Nfsshare** Dieses Tool dient zur Verwaltung der NFS-Freigaben.
- **Nfsstat** Dieses Tool zeigt die Anzahl der Zugriff auf den NFS-Server an oder setzt die Anzeige zurück.
- **Showmount** Dieses Tool zeigt die bereitgestellten Systeme an, die durch den Server für NFS exportiert wurden.
- **Unmount** Mit diesem Tool werden die Bereitstellungen der über NFS bereitgestellten Laufwerke aufgehoben.

Identitätsverwaltung für UNIX

Die Identitätsverwaltung für UNIX wird nicht durch die Installation der NFS-Dienste für den Rollendienst *Dateidienste* installiert, sondern als zusätzlicher Rollendienst der *Active Directory-Domänendienste*. Wollen Sie Kennwörter und Benutzerdaten zwischen Ihrer Windows- und UNIX-Infrastruktur replizieren, sollten Sie daher diesen Rollendienst nachträglich installieren.

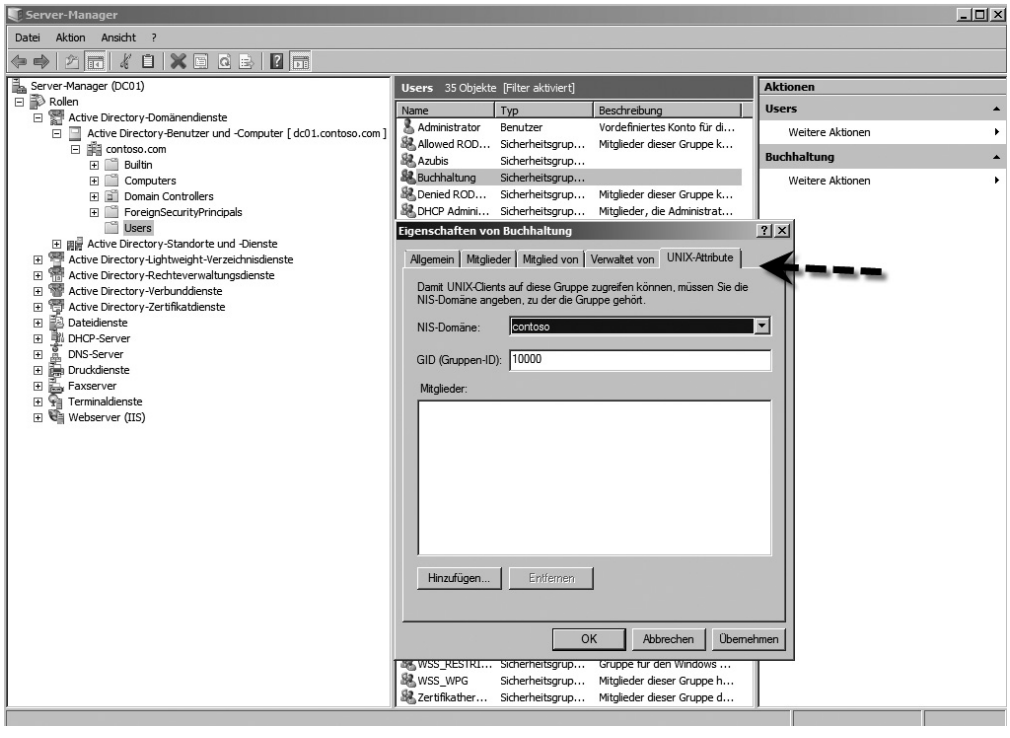
Nachdem Sie den Rollendienst installiert haben, müssen Sie den Domänencontroller neu starten. Zur Verwaltung der Identitätsverwaltung für UNIX steht in der Programmgruppe *Verwaltung* das neue Snap-In *Microsoft Identity Management für UNIX* zur Verfügung (Abbildung 6.65). Rufen Sie die Eigenschaften der Identitätsverwaltung für UNIX auf, um die Benutzerdaten des UNIX-Systems zu konfigurieren, mit dem Sie Ihre Daten replizieren wollen. Um die Server zu autorisieren, die auf den Dienst zugreifen, stellt dieser eine Textdatei mit der Bezeichnung **.maphosts* zur Verfügung. Diese Datei befindet sich im Verzeichnis *C:\Windows\msnfs* und listet die Namen aller Systeme auf, die berechtigt sind, diesen Dienst abzufragen. Hier müssen Sie alle Server eintragen, die entweder als NFS-Server oder als NFS-Client fungieren. Starten Sie die Konsole, erscheint zunächst eine Fehlermeldung. Diese wird dadurch verursacht, dass der Systemdienst *NIS-Server* deaktiviert wurde. Setzen Sie diesen Dienst auf *Automatisch* und starten Sie diesen, bevor Sie die Verwaltungskonsole starten. Der mitgelieferte *Server für NIS* ermöglicht es dem Server, im Netz als so genannter *Master-Server für NIS* zu arbeiten. NIS (Network Information Service), das von Sun Microsystems im Jahr 1985 auf den Markt gebracht wurde, war einer der ersten verteilten Namensdienste auf UNIX-Basis. NIS ist ein Verzeichnisdienst zur Verteilung von Konfigurationsdaten wie Benutzernamen oder Rechnernamen in einem Netzwerk. Als Teil der Installationsroutine wird das Active-Directory-Schema so erweitert, dass Anwender- und Gruppendaten von NIS in Active Directory gespeichert werden können. Damit steht dem Administrator ein gemeinsames Tool zur Verwaltung von Windows- und UNIX-Authentifizierungen und -Anmeldungen zur Verfügung.

Abbildg. 6.65 Konfigurieren der Identitätsverwaltung für UNIX



Nach der Installation der Identitätsverwaltung für UNIX können Sie in den Eigenschaften von Benutzern und Gruppen über die Registerkarte *UNIX-Attribute* Daten eintragen, die von UNIX-Servern und -Clients abgefragt werden können (Abbildung 6.66).

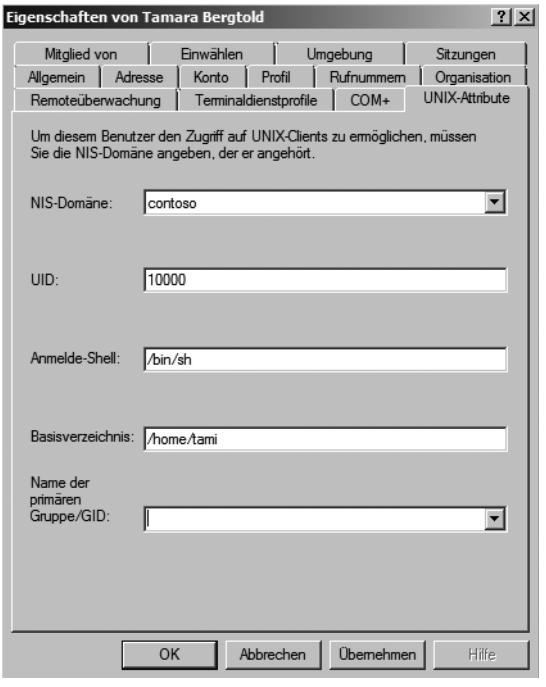
Abbildg. 6.66 Konfigurieren von UNIX-Attributen für Gruppen



Durch diese Konfiguration können Gruppen sowohl in Active Directory als auch auf den UNIX-Computern verwendet werden. In den Eigenschaften der Benutzerkonten können Sie ebenfalls

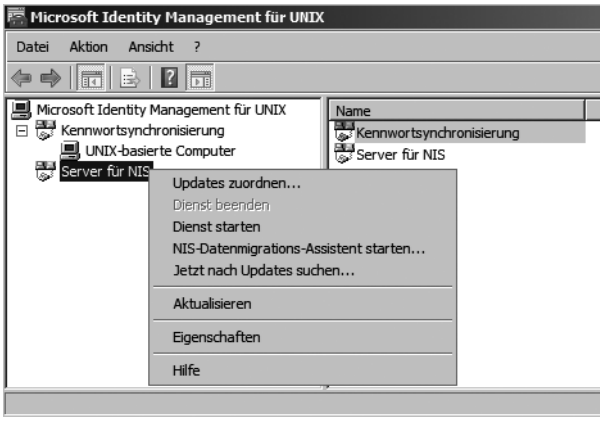
UNIX-Attribute pflegen. Dadurch können diese Benutzerkonten für die Anmeldung an einen Windows-PC sowie über UNIX verwendet werden (Abbildung 6.67).

Abbildg. 6.67 Konfigurieren von UNIX-Attributen für Benutzerkonten in Active Directory



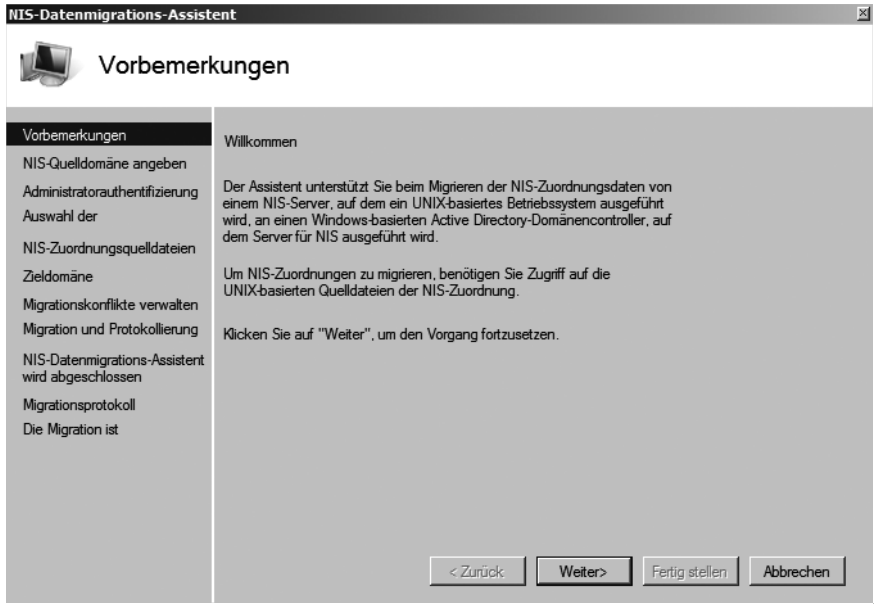
Klicken Sie mit der rechten Maustaste im Snap-In *Microsoft Identity Management für UNIX* auf den Eintrag *Server für NIS*, können Sie den Migrationsassistenten starten, über den Sie Daten zwischen UNIX und Windows replizieren können (Abbildung 6.68).

Abbildg. 6.68 Starten des Assistenten für die Migration von Benutzerdaten zwischen Windows und UNIX



Über den Assistenten können Sie bequem die Daten auswählen, die zwischen UNIX und Windows repliziert werden sollen (Abbildung 6.69).

Abbildg. 6.69 Replizieren von UNIX-Daten und Windows-Daten



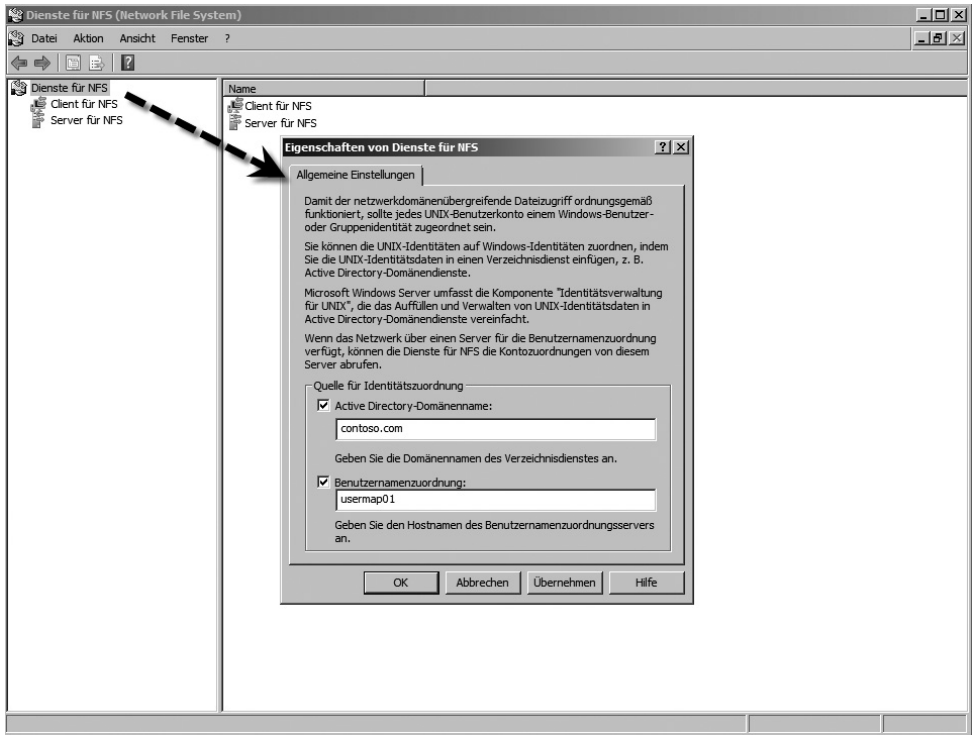
Für die Replikation benötigen Sie ebenfalls Replikationsdateien, die Sie vorher auf den Domänencontroller kopieren sollten. Der Assistent kann auf diese Daten zugreifen, um die Replikation vorzunehmen.

Server/Client für UNIX

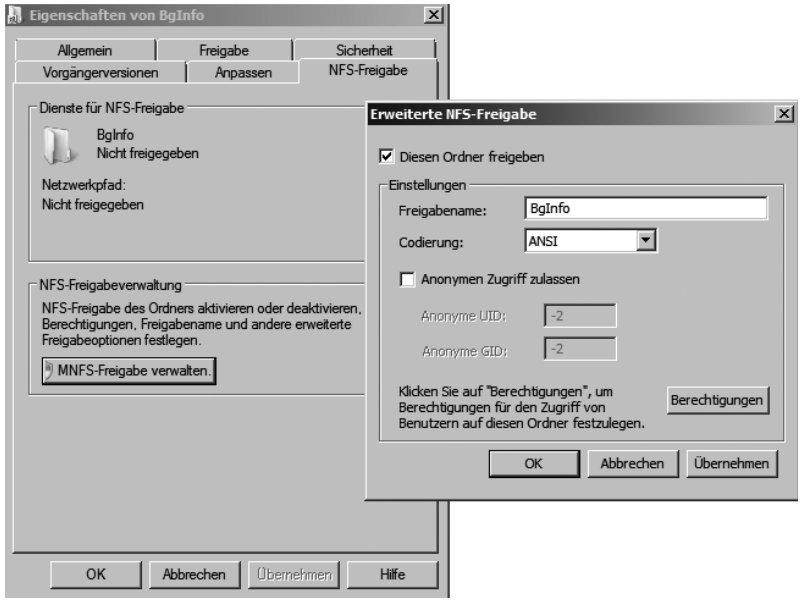
Um diese Funktion nutzen zu können, müssen Sie in der Verwaltungskonsole für das NFS die Eigenschaften des Menüs *Dienste für NFS* aufrufen. Hier können Sie die Benutzerdaten hinterlegen, die zum Datenausgleich zwischen dem Active Directory und der UNIX-Umgebung verwendet werden (Abbildung 6.70). Hier können Sie auch einen Server angeben, der die Benutzerdaten von UNIX bereits synchronisiert.

Generell ist die Erstellung von NFS-Freigaben nach der Installation von NFS recht einfach. Geben Sie ein Verzeichnis frei, erscheint eine neue Registerkarte mit der Bezeichnung *NFS-Freigabe*. Über diese Registerkarte steuern Sie, wie NFS-Clients auf die Freigabe zugreifen dürfen (Abbildung 6.71).

Abbildg. 6.70 Konfigurieren des User-Mappings für NFS



Abbildg. 6.71 Erstellen einer NFS-Freigabe

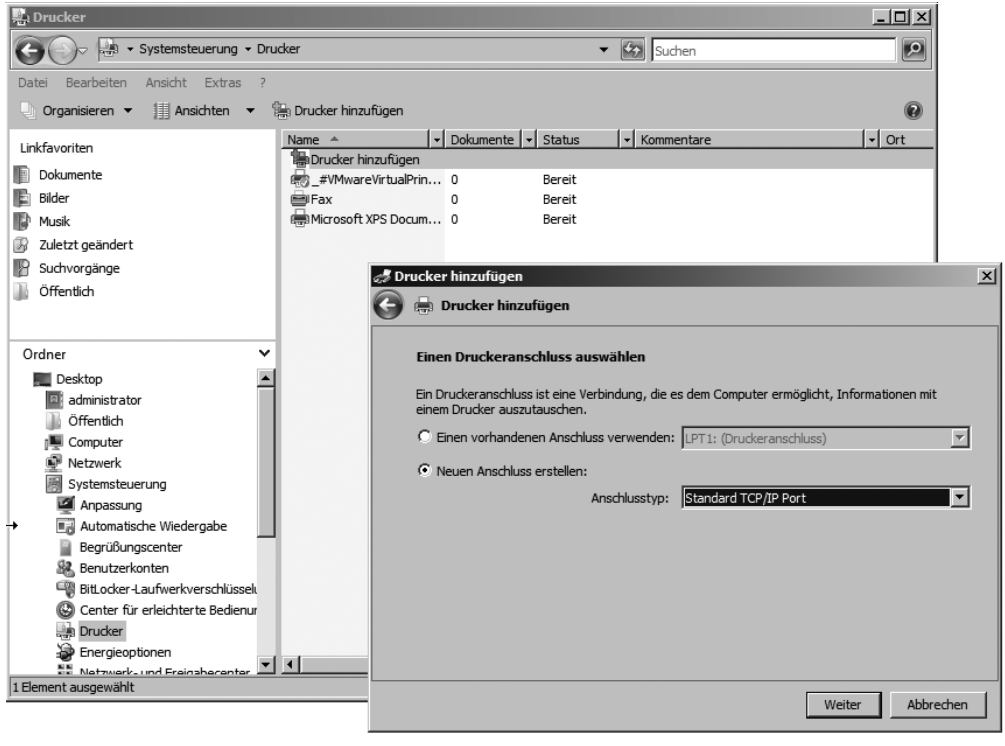


Zur Freigabe von Verzeichnissen über NFS, müssen Sie zusätzlich auch die Benutzernamenzuordnung konfigurieren. Hierbei werden die UNIX-Benutzer in Active Directory verfügbar gemacht. Die Zuordnung von Benutzernamen findet ebenfalls über das Snap-In *Dienste für NFS* statt.

Druckserver einrichten und verwalten

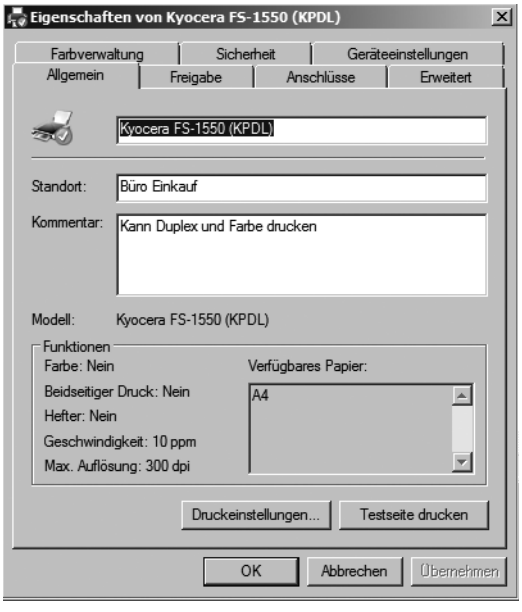
Wollen Sie einen Windows Server 2008 auch als Druckserver einsetzen, sollten Sie die Serverrolle *Druckdienste* über den Server-Manager installieren. In diesem Fall werden die notwendigen Verwaltungsprogramme installiert und in der Windows-Firewall die Ausnahmen für freigegebene Drucker eingetragen. Windows Server 2008 wird mit Druckertreibern geliefert, die mit Windows Server 2003, Windows 2000, Windows XP und Windows Vista einsetzbar sind. Damit ein Drucker im Netzwerk zur Verfügung gestellt wird, müssen Sie diesen zunächst auf dem Druckserver installieren. Die Installation erfolgt dabei genauso wie die Installation eines lokalen Druckers auf einer Arbeitsstation. Wenn Sie einen lokalen Drucker installieren, müssen Sie einen Druckeranschluss auswählen. Sie können hier einen der standardmäßigen lokalen Anschlüsse verwenden oder auch alternativ bei *Neuen Anschluss erstellen* einen TCP/IP-Port konfigurieren (Abbildung 6.72). Damit können Sie auf einen Netzwerkdrucker zugreifen. Den Drucker müssen Sie dazu direkt an das Netzwerk anschließen und ihm eine IP-Adresse zuweisen. Genau diese IP-Adresse verwenden Sie für den TCP/IP-Port.

Abbildg. 6.72 Erstellen eines neuen Druckeranschlusses für die Installation eines Netzwerkdruckers



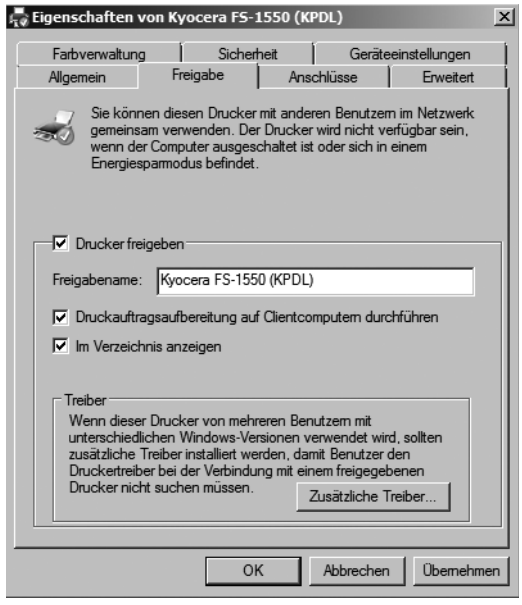
Als Freigabename wird eine Kurzform des Druckernamens gewählt. Sie können aber auch längere Freigabenamen verwenden. Die Beschränkung auf acht Zeichen spielt nur bei älteren Client-Versionen eine Rolle. Wenn Sie dagegen nur mit Windows 2000- und Windows Vista/XP-Clients arbeiten, können Sie auch längere Bezeichnungen angeben. Dies ist auch empfehlenswert, damit Benutzer die Drucker einfacher identifizieren können. Im darauf folgenden Dialogfeld können Sie den Standort des Druckers und einen Kommentar zu diesem angeben. Nachdem Sie die Informationen zu dem Drucker eingegeben haben, können Sie eine Testseite ausdrucken. Damit ist die Installation des Druckers zunächst abgeschlossen. Bei installierten Druckern können Sie dessen Eigenschaften öffnen, um weitere Einstellungen vorzunehmen. Im zugehörigen Dialogfeld können Sie über eine Reihe von Registerkarten die Detailkonfiguration des Druckers durchführen (Abbildung 6.73).

Abbildg. 6.73 Eigenschaften eines Druckers verwalten



Über die Registerkarte *Freigabe* wird die Freigabe von Druckern konfiguriert. Mit der Option *Im Verzeichnis anzeigen* wird definiert, dass dieser Drucker in Active Directory sichtbar und verfügbar sein soll. Damit können Benutzer nach diesem Drucker suchen und einfach eine Verbindung zu ihm herstellen. Über die Schaltfläche *Zusätzliche Treiber* können Druckertreiber für andere Windows-Versionen installiert werden. Diese Druckertreiber werden auf dem Server bereitgehalten. Wenn sich ein Benutzer einer älteren Arbeitsstation mit dem Drucker verbindet, wird der Druckertreiber automatisch vom Server geladen.

Abbildg. 6.74 Konfigurieren der Freigabe eines Druckers



Über die Registerkarte *Sicherheit* lassen sich die Zugriffsberechtigungen für Drucker konfigurieren. Hier gibt es drei Berechtigungen, die standardmäßig zugeordnet werden können:

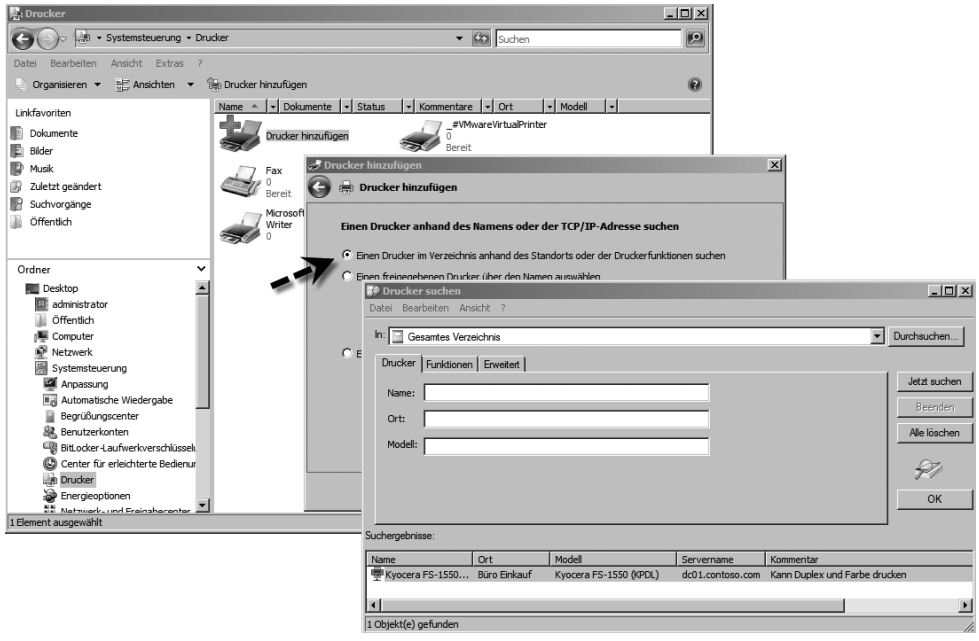
- **Drucken** Erlaubt die Ausgabe von Dokumenten auf dem Drucker
- **Drucker verwalten** Ermöglicht die Veränderung von Druckereinstellungen, wie bei den auf den vorangegangenen Seiten beschriebenen Festlegungen
- **Dokumente verwalten** Erlaubt die Verwaltung von Warteschlangen und damit beispielsweise das Löschen von Dokumenten aus solchen Warteschlangen

Der Zugriff auf freigegebene Drucker

Um auf einen freigegebenen Drucker im Netzwerk zuzugreifen, wird, wie schon beim Erstellen von Druckern, der Assistent für die Druckerinstallation verwendet, der über *Drucker hinzufügen* aufgerufen werden kann. Der Drucker kann auch im Verzeichnis gesucht werden (Abbildung 6.75).

Alternativ kann aber auch der Druckername direkt in der Form \\<*Servername*>\<*Freigabename*> eingegeben werden. Auch wenn Sie über das Startmenü diesen Befehl eingeben, wird der Drucker verbunden.

Abbildg. 6.75 Freigegebenen Drucker im Active Directory suchen



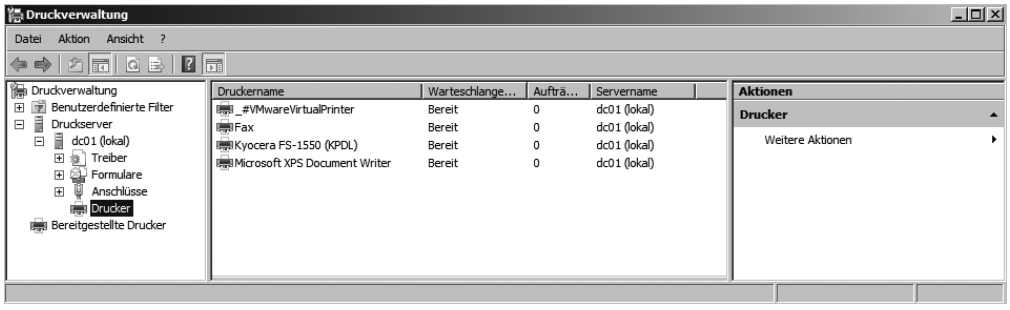
Verwaltung von Druckjobs

Zunächst muss der Drucker ausgewählt werden, auf dem Druckjobs verwaltet werden sollen. Klicken Sie in der Druckersteuerung dazu doppelt auf den entsprechenden Drucker. Damit wird die Druckerwarteschlange geöffnet. In dieser sind alle Dokumente zu finden, die aktuell im Druck sind beziehungsweise auf ihren Ausdruck warten. Über die Befehle in den Menüs *Drucker* und *Dokument* lassen sich die anstehenden Druckjobs verwalten (Abbildung 6.76). Die dort verfügbaren Befehle sind weitgehend selbsterklärend. Wenn sich fehlerhafte Druckjobs in der Verwaltung des Druckers nicht löschen lassen, beenden Sie die *Druckwarteschlange* auf dem Server. Sie können diesen Vorgang entweder über die Dienstesteuerung vornehmen oder in der Befehlszeile *net stop spooler* eingeben und anschließend den Dienst wieder mit *net start spooler* starten lassen. Alle Druckaufträge sollten jetzt gelöscht sein oder sich zumindest ohne weitere Fehler löschen lassen.

Druckverwaltungs-Konsole – Die Zentrale für Druckserver

Die Druckverwaltung ist eine zentrale Verwaltungsoberfläche für Drucker in Ihrem Unternehmen. Sie können mit dieser Konsole alle Druckserver Ihres Unternehmens an zentraler Stelle verwalten und neue Drucker hinzufügen oder entfernen. Mit der Druckverwaltung ist die Verwaltung von zahlreichen Druckservern im Unternehmen extrem effizient geworden. Wenn ein Server offline geschaltet wird, ändert sich das Druckerserversymbol. Sie können die Treiber, Formulare, Ports und Drucker erst verwalten, wenn der Server wieder online geschaltet ist. Dadurch erkennen Sie auch sehr schnell, ob ein Druckserver heruntergefahren wurde oder eventuell abgestürzt ist.

Abbildg. 6.76 Druckserver mit der Druckverwaltung überwachen und konfigurieren

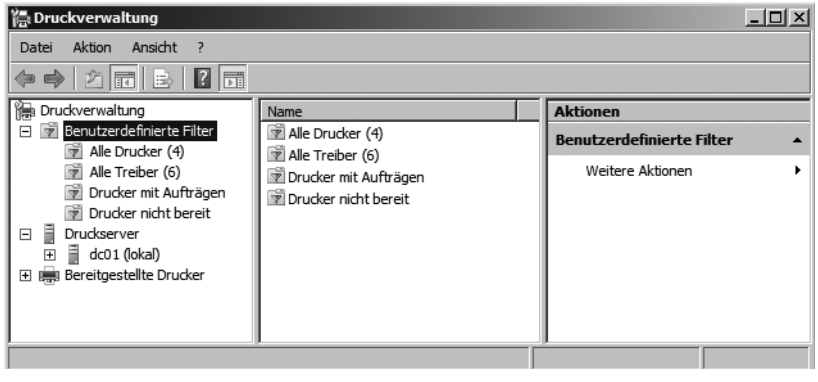


Klicken Sie mit der rechten Maustaste auf der Konsolenstruktur auf den Eintrag *Druckserver*, können Sie weitere Server der Verwaltungskonsole hinzufügen, die Sie zukünftig über diese zentrale Stelle verwalten können. Die Drucker der verbundenen Druckserver werden in der Druckverwaltung an drei Orten gespeichert: *Benutzerdefinierte Druckerfilter*, *Druckserver* und *Bereitgestellte Drucker*.

Erstellen von benutzerdefinierten Filteransichten

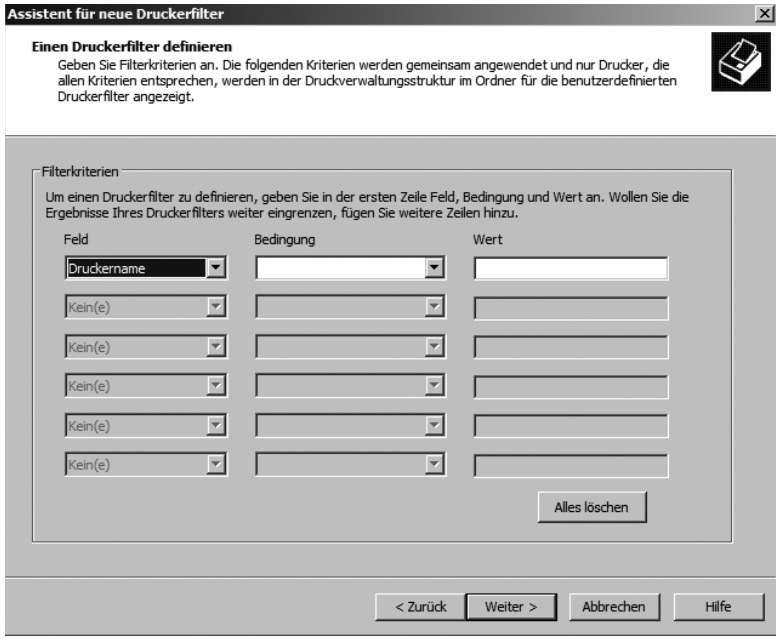
Der Eintrag *Benutzerdefinierte Druckerfilter* in der Druckverwaltung enthält verschiedene Filter, über die Sie auf einen Blick alle notwendigen Informationen zu den installierten Druckern im Unternehmen anzeigen können (Abbildung 6.77).

Abbildg. 6.77 Anzeigen der Drucker im Unternehmen



Sie können erkennen, welche Drucker derzeit nicht bereit sind, und zwar von allen Druckservern, die Sie verbunden haben. Außerdem werden Ihnen an dieser Stelle alle Drucker zentral angezeigt, sowie alle installierten Druckertreiber. Ebenso lassen sich alle Druckaufträge in der Konsole filtern. Neben dem bereits standardmäßig angelegten Filter können Sie durch einen Klick mit der rechten Maustaste auf den Knoten *Benutzerdefinierter Filter* weitere Filter erstellen, zum Beispiel Farbdrucker, Duplexdrucker oder welche Kategorien auch immer Sie benötigen. Der Assistent zum Erstellen eines neuen benutzerdefinierten Filters lässt viele Auswahlmöglichkeiten zu (Abbildung 6.78).

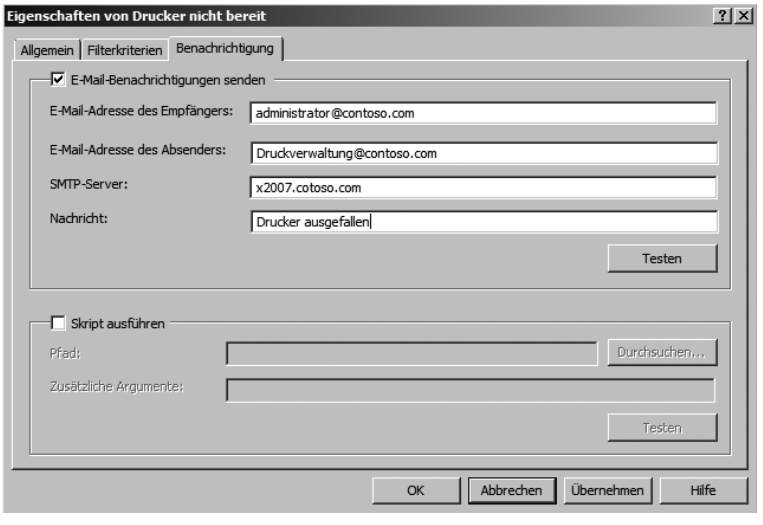
Abbildg. 6.78 Erstellen eigener Druckerfilter für die Verwaltung in der Druckverwaltungs-Konsole



Konfigurieren von E-Mail-Benachrichtigungen

In den Eigenschaften der einzelnen Druckerfilter können Sie auf der Registerkarte *Benachrichtigung* eine automatische E-Mail-Benachrichtigung hinterlegen (Abbildung 6.79). So können Sie sich darüber informieren lassen, wenn einzelne Drucker nicht mehr bereit sind oder neue Drucker auf angeschlossenen Druckservern installiert werden.

Abbildg. 6.79 Konfigurieren von Benachrichtigungen bei ausgefallenen Druckern



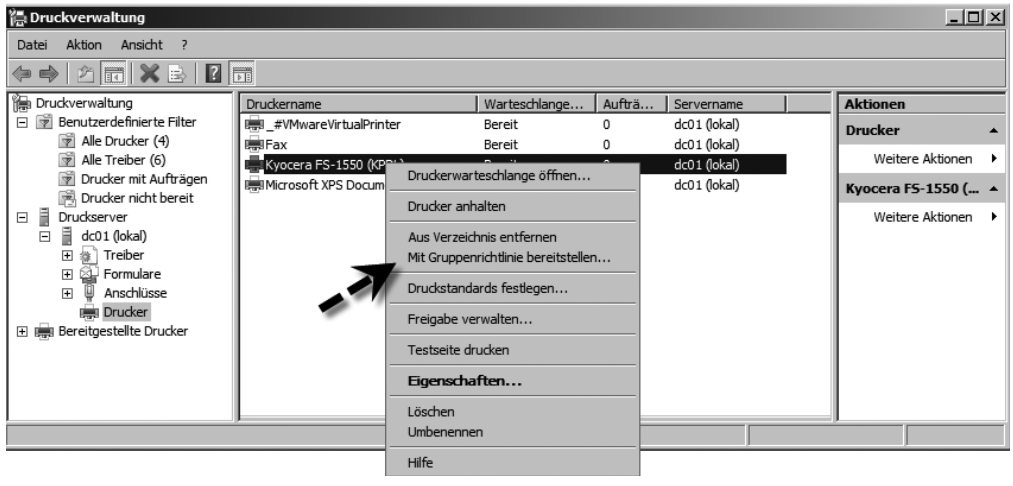
Exportieren und Importieren von Druckern

Klicken Sie mit der rechten Maustaste auf einen der verbundenen Druckserver, können Sie verschiedene Aufgaben durchführen. Unter anderem können Sie alle Druckertreiber auf einen Schlag exportieren. Die Exportdatei können Sie auf einem anderen Druckserver wieder importieren. Durch das Exportieren erhalten Sie außerdem eine Datensicherung der Druckkonfiguration und können beim Einsatz zahlreicher Drucker auf dem Server sehr schnell eine Wiederherstellung durchführen, da Sie nur die Exportdatei benötigen. Über das Kontextmenü können Sie auch neue Drucker hinzufügen. Im Gegensatz zum normalen Installationsassistenten für Drucker, können Sie über den Assistenten in der Druckverwaltung auch automatisch nach verfügbaren Druckern im gleichen Subnetz suchen lassen.

Drucker verwalten und über Gruppenrichtlinien verteilen lassen

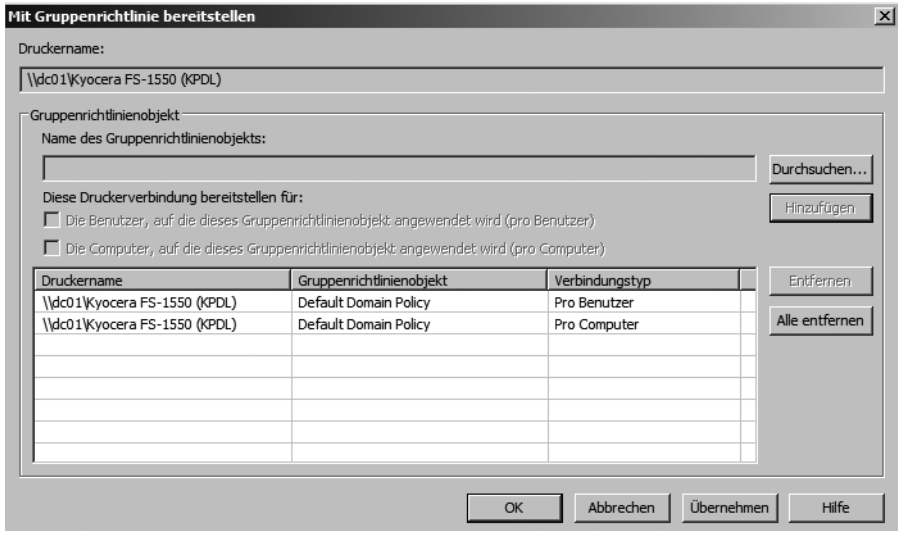
Klicken Sie mit der rechten Maustaste auf einen Drucker, können Sie über das Kontextmenü verschiedene Aufgaben durchführen (Abbildung 6.80).

Abbildg. 6.80 Verwalten von Druckereinstellungen in der Druckverwaltung



So können Sie zum Beispiel mit dem Befehl *Mit Gruppenrichtlinie bereitstellen* eine Gruppenrichtlinie auswählen, in die Sie den Drucker integrieren. Alle Benutzer und alle Computer, für die diese Richtlinie angewendet wird, werden automatisch mit dem hinterlegten Drucker verbunden.

Abbildg. 6.81 Verteilen von Druckern über Gruppenrichtlinien

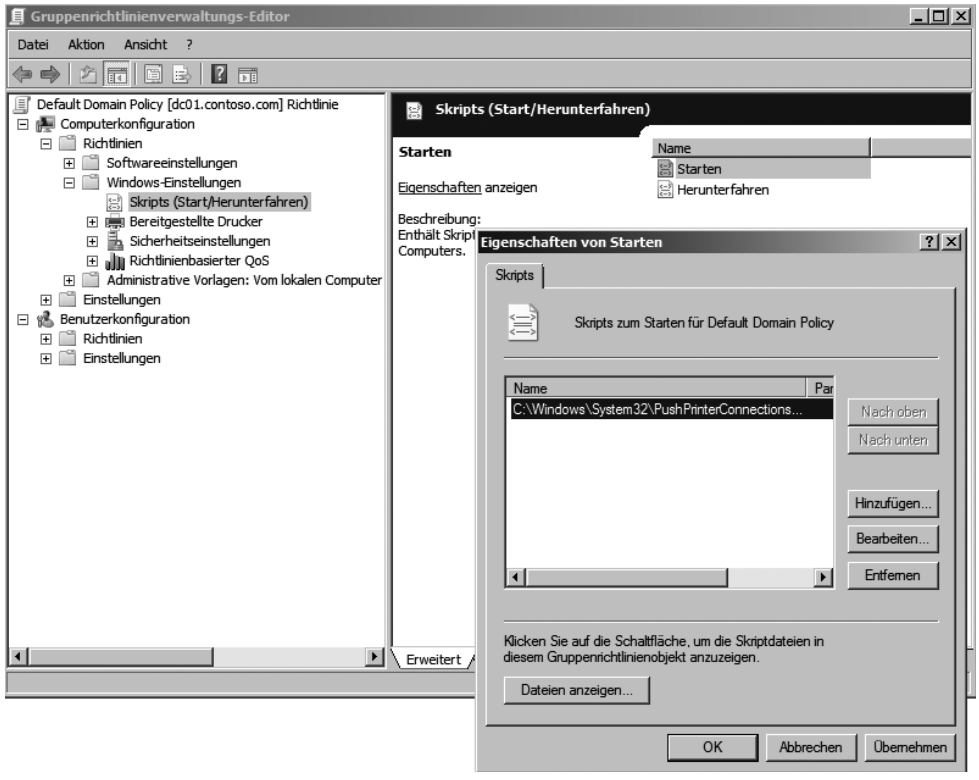


Wenn die Verarbeitung der Gruppenrichtlinie auf Clientcomputern ausgeführt wird, werden die Druckerverbindungseinstellungen auf die dem Gruppenrichtlinienobjekt zugeordneten Benutzer oder Computer angewendet. Über diese Methode bereitgestellte Drucker werden im Knoten *Bereitgestellte Drucker* in der Druckverwaltung angezeigt. Ein Drucker, der so installiert wurde, kann von jedem Benutzer dieses Computers verwendet werden. Zusätzlich sollten Sie bei der Verwendung dieser Funktion auf Arbeitsstationen mit Windows XP das Tool *PushPrinterConnections.exe* verwenden, welches zum Lieferumfang von Windows Server 2008 gehört. Das Tool liest die vom Gruppenrichtlinienobjekt vorgenommenen Einstellungen, in dem die Druckereinstellung enthalten ist, und fügt die Druckerverbindung hinzu. Bevor Sie Drucker mithilfe der Gruppenrichtlinie installieren können, muss für die Druckerverbindungseinstellungen ein Gruppenrichtlinienobjekt vorhanden sein, das den entsprechenden Benutzern und Computern zugewiesen wurde:

1. Klicken Sie in der Gruppenrichtlinienkonsole mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, das die Druckerverbindungseinstellungen enthält, und klicken Sie dann auf *Bearbeiten*.
2. Wenn die Druckerverbindungen pro Computer bereitgestellt werden, navigieren Sie zu *Computerkonfiguration/Windows-Einstellungen/Skripts (Starten/Herunterfahren)*.
3. Wenn die Druckerverbindungen pro Benutzer bereitgestellt werden, navigieren Sie zu *Benutzerkonfiguration/Windows-Einstellungen/Skripts (Anmelden/Abmelden)*.
4. Klicken Sie mit der rechten Maustaste auf *Start* oder *Anmeldung*, und wählen Sie im Kontextmenü den Eintrag *Eigenschaften* aus.
5. Klicken Sie im Dialogfeld auf die Schaltfläche *Dateien anzeigen*.
6. Kopieren Sie die Datei *PushPrinterConnections.exe* an diesen Speicherort, und schließen Sie dann das Dialogfeld. Die Datei befindet sich im Verzeichnis *C:\Windows\System32*.
7. Klicken Sie auf *Hinzufügen*.
8. Geben Sie *PushPrinterConnections.exe* in das Feld *Skriptname* ein.

9. Wenn Sie die Protokollierung aktivieren möchten, geben Sie *–log* in das Feld *Skriptparameter* ein. Protokolldateien werden auf dem Computer, auf den die Richtlinie angewendet wird, in die Datei *%windir%\temp\ppcMachine.log* oder *%temp%\ppcUser.log* geschrieben.
10. Klicken Sie auf *OK*.
11. Wenn Sie die Druckerverbindungseinstellungen aus dem Gruppenrichtlinienobjekt entfernen, entfernt das Dienstprogramm *PushPrinterConnections.exe* die entsprechenden Drucker beim nächsten Neustart oder bei der nächsten Benutzeranmeldung vom Clientcomputer.

Abbildg. 6.82 Konfigurieren von Gruppenrichtlinien für die Verteilung von Druckern



Zusammenfassung

Wie Sie in diesem Kapitel erfahren haben, bietet Windows Server 2008 zahlreiche Möglichkeiten, um Dateien im Netzwerk effizient zur Verfügung zu stellen. Davon profitieren kleinere Unternehmen, aber auch größere Unternehmen mit den DFS-Funktionen von Windows Server 2008. Damit Daten aber überhaupt im Netzwerk zur Verfügung gestellt werden können, muss der Server auch an das Netzwerk angebunden werden. Hier hat sich im Vergleich zu Windows Server 2003 einiges geändert. In nächsten Kapitel gehen wir ausführlich darauf ein, wie Sie Windows Server 2008 in ein Netzwerk einbinden.

Kapitel 7

Netzwerke mit Windows Server 2008

In diesem Kapitel:

Microsoft hat im Bereich der Konfiguration der Netzwerkschnittstellen einige Verbesserungen vorgenommen, um die Anbindung von Windows Server 2008 an ein Netzwerk effizienter zu gestalten. Die wichtigste Neuerung ist, dass sowohl in Windows Server 2008 als auch in Windows Vista standardmäßig IPv6 installiert und aktiviert ist. Windows Server 2008 und Windows Vista versuchen untereinander möglichst immer mit IPv6 zu kommunizieren. Gelingt dies nicht, wird für die Kommunikation IPv4 verwendet. Für Anwender und Administratoren ändert sich dabei nichts, diese Kommunikation läuft transparent ab. Windows Server 2008 beinhaltet eine aktualisierte Implementierung des TCP/IP-Stacks mit signifikanten Verbesserungen, die sich speziell an mehrere wichtige Netzwerkprobleme richten, und Verbesserungen bei Leistung und Durchsatz, eine allgemeine Wi-Fi-Achitektur und APIs zur Inspizierung von Netzwerkpaketen bieten. Die Maximierung der Netzwerkauslastung erfordert eine komplexe Optimierung der TCP/IP-Konfigurationseinstellungen. In Windows Server 2008 müssen Sie dies nicht mehr manuell erledigen, indem Sie die Netzwerkbedingungen erkennen und die Leistung automatisch optimieren. Wenn Windows Server 2008 auf den Domänencontroller über das Netzwerk zugreifen kann, wechselt es automatisch in das Domänenprofil.

Dank Netzwerk-Awareness können Anwendungen, wie die Windows-Firewall, mit erweiterter Sicherheit unterschiedliche Konfigurationen auf Grundlage des Netzwerktyps haben, mit dem gegenwärtig eine Verbindung besteht, und automatisch zwischen den Konfigurationen wechseln, wenn sich der Netzwerktyp ändert (siehe Kapitel 14). In Windows Server 2008 kann auch die Gruppenrichtlinie das Netzwerk erkennen: Sie erkennt automatisch, wenn sich der Computer am Domänennetzwerk befindet und beginnt mit der Verarbeitung aller neuen Gruppenrichtlinieneinstellungen, ohne auf den nächsten Aktualisierungszyklus zu warten. Das bedeutet, Windows Server 2008 überprüft automatisch, ob neue Einstellungen der Gruppenrichtlinie vorliegen, wenn es eine Verbindung mit dem Domänennetzwerk aufnimmt. Administratoren sind dadurch in der Lage, Sicherheitseinstellungen schneller bereitzustellen. Windows Server 2008, verwendet auch Server Message Block (SMB) in der Version 2.0. Die Kommunikation zwischen Windows Server 2008- und Windows Vista-Computern wird dadurch extrem beschleunigt, wenn auf Daten zugegriffen wird. Microsoft plant Aktualisierungen, damit auch die Kommunikation mit Windows Server 2003 und Windows XP beschleunigt wird. Derzeit ist allerdings die Geschwindigkeit zwischen den neuen und den alten Windows-Versionen noch langsamer als zwischen Windows Server 2008 und Windows Vista.

Neue Netzwerkfeatures in Windows Server 2008 und Windows Vista

Windows Server 2008 und Windows Vista bringen zahlreiche neue Netzwerkfeatures mit, die in den einzelnen Kapiteln dieses Buches noch ausführlicher besprochen werden. Die wichtigsten Neuerungen im Kern der Netzwerkkommunikation sind zusammenfassend folgende Punkte:

- **TCP/IP-Stack der nächsten Generation** Der TCP/IP-Stack der nächsten Generation ist sowohl für IPv4 als auch für IPv6 eine vollständige Neuentwicklung. Durch einen besseren Durchsatz wird die Nutzung der Netzwerkbandbreite verbessert. Bei der Unerreichbarkeitserkennung handelt es sich um ein Feature von IPv6, bei dem der Server verfolgt, ob ein benachbarter Knoten erreichbar ist. Dies ermöglicht eine bessere Fehlererkennung und Korrektur. Diese Erkennung wird in Windows Server 2008 auch für das IPv4-Protokoll genutzt, sodass ausgefallene Netzwerkknoten schneller erkannt werden können. Der TCP/IP-Stack unterstützt eine Architektur mit einer doppelten IP-Schicht, in der die IPv4- und IPv6-Implementierungen gemeinsame

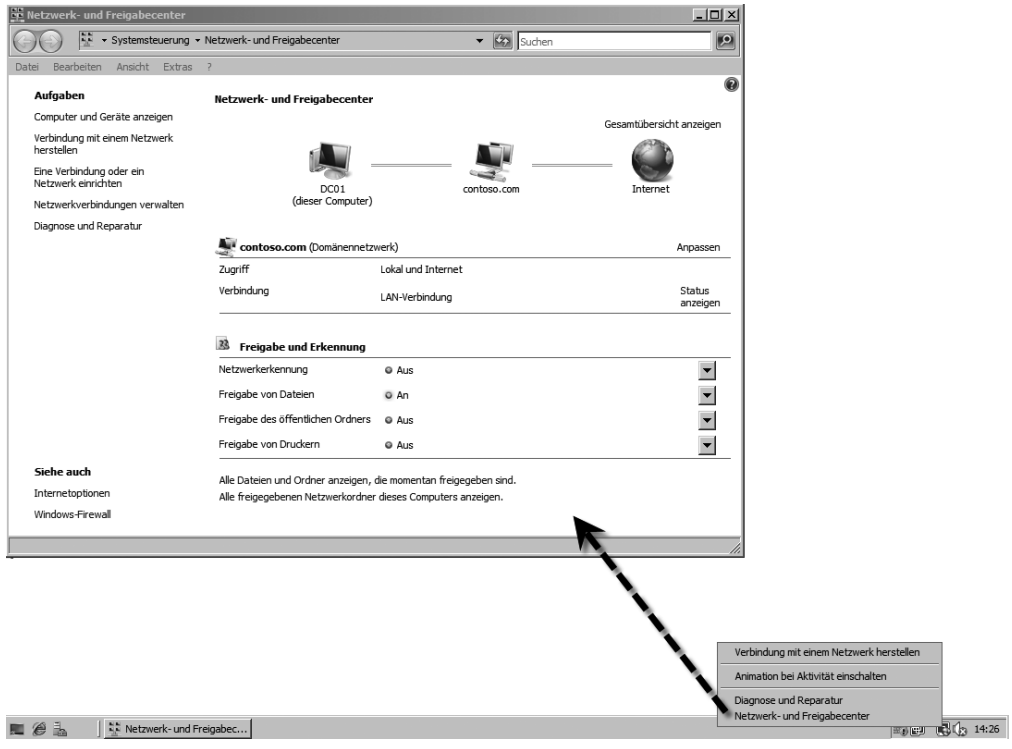
Transportebenen verwenden. In der Standardeinstellung ist sowohl IPv4 als auch IPv6 aktiviert. Für eine IPv6-Unterstützung muss keine separate Komponente installiert werden. IPv6 kann für Verbindungen deaktiviert werden. IPv6 kann über die grafische Oberfläche und in der Befehlszeile mit *netsh interface ipv6* konfiguriert werden. Windows Server 2008 und Windows Vista beinhalten einen DHCPv6-fähigen DHCP-Client, der einen DHCPv6-Server unterstützt. Windows Server 2008 beinhaltet einen DHCPv6-fähigen DHCP-Serverdienst.

- **QoS (Quality of Service)** Windows Server 2008 und Windows Vista verfügen über neue Möglichkeiten für die Verwaltung des Netzwerkverkehrs. Die QoS-Richtlinien ermöglichen es, die Senderate für ausgehenden Netzwerkverkehr zu priorisieren oder zu verwalten. Die QoS-Richtlinieneinstellungen sind Teil der Gruppenrichtlinien.
- ***Http.sys*-Erweiterungen** Bei Http.sys handelt es sich um neue Funktionen für die neuen IIS 7.0 von Windows Server 2008. Diese Neuerungen werden ausführlich im Kapitel 13 besprochen.
- **WinInet-Erweiterungen** Bei diesen Erweiterungen handelt es sich zum größten Teil ebenfalls um Funktionen für die Webkomponente von Windows Server 2008. Zu den Erweiterungen der WinInet-API in Windows Server 2008 gehören hauptsächlich Unterstützung für IPv6-Literale und Bereichs-IDs, Unterstützung für HTTP-Dekomprimierung, Unterstützung für internationalisierte Domänennamen, Unterstützung für die ETW-Ablaufverfolgung, IPv6-Unterstützung in Web Proxy Auto-Discovery-Skripts. So kann durch IPv6-literale IDs ein Benutzer mit einem WinInet-basierten Webbrowser (zum Beispiel dem Internet Explorer 7) die Adresse *http://[3ffe:ffff:100:2a5f::1]* eingeben, um eine Verbindung mit dem Webserver unter der IPv6-Adresse *3ffe:ffff:100:2a5f::1* herzustellen. WinInet beinhaltet eine integrierte Unterstützung für Codierungsschemas zur gzip- und deflate-Komprimierung.
- **Windows Sockets-Erweiterungen** Windows Server 2008 beinhaltet die neue Schnittstelle *Winsock Kernel (WSK)*. WSK erleichtert Softwareherstellern die Entwicklung von Protokolltreibern in Windows. WSK beinhaltet eine neue Socket-API im Kernel-Modus.
- **NDIS 6.0** Network Driver Interface Specification (NDIS) 6.0 legt eine Standardschnittstelle zwischen Netzwerktreibern im Kernel-Modus und dem Betriebssystem fest. Windows Server 2003 und XP verwenden NDIS 5.1, welches aber vollständig kompatibel zu NDIS 6.0 von Windows Vista und Windows Server 2008 ist. NDIS 6.0 bietet vor allem eine deutlich erhöhte Geschwindigkeit im Vergleich zu NDIS 5.1
- **Windows Peer-zu-Peer-Netzwerkumgebungserweiterungen** Hierbei handelt es sich einfach gesagt um Funktionen, die andere Windows Server 2008- oder Windows Vista-Computer im Netzwerk erkennen und entsprechend reagieren können. Auf diese Funktionen baut zum Beispiel Windows-Teamarbeit auf, sowie die Vista-Funktion *Personen in meiner Umgebung*.
- **Windows-Firewall-Erweiterungen** Diese neuen Funktionen werden vor allem in Kapitel 14 besprochen.
- **IPsec-Verbesserungen** IPSec wurde deutlich erweitert. Wir widmen uns ausführlich in Kapitel 14 diesem Thema.

Das Netzwerk- und Freigabecenter

Die Konfiguration der Netzwerkeinstellungen von Windows Server 2008 nehmen Sie im neuen Netzwerk- und Freigabecenter vor. Wenn Sie mit der rechten Maustaste auf das Netzwerksymbol im Infobereich der Taskleiste klicken, öffnet sich ein Kontextmenü, und Sie können das *Netzwerk- und Freigabecenter* öffnen (Abbildung 7.1).

Abbildg. 7.1 Öffnen des Netzwerk- und Freigabecenters



Unter Windows Server 2008 erkennen Sie bereits an diesem Symbol die Netzwerkverbindung:

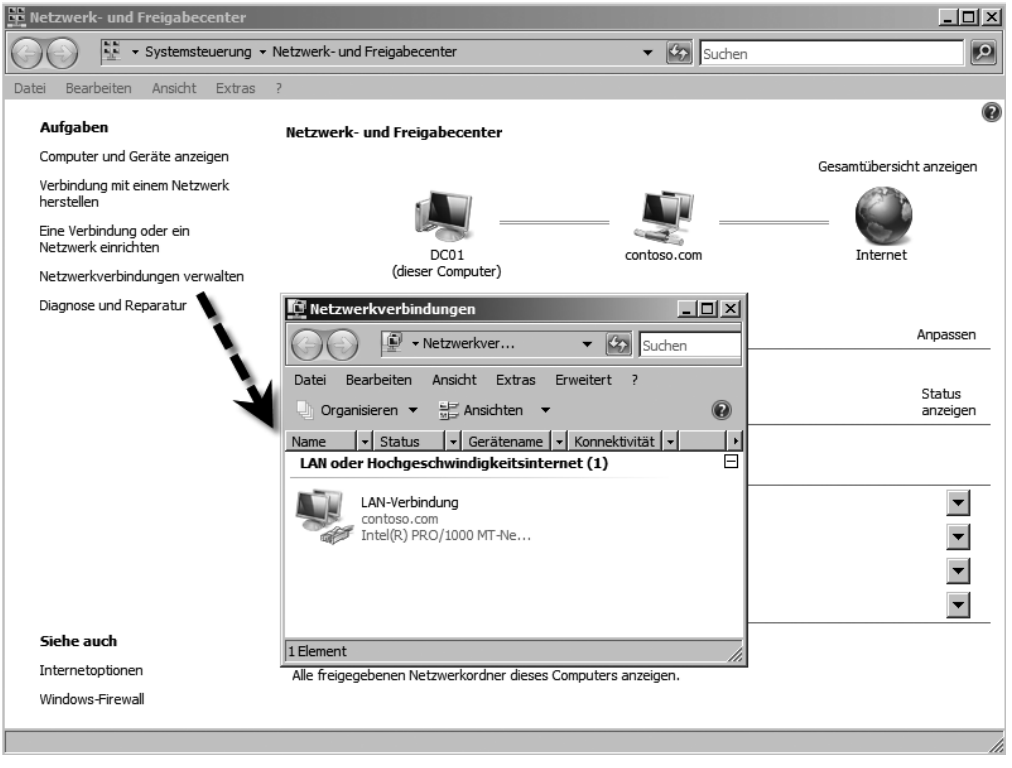
- Werden zwei Computer angezeigt, ist das ein Zeichen, dass der Server mit dem Netzwerk verbunden ist und eine IP-Adresse erhalten hat.
- Wird ein Computer mit einem roten Kreuz angezeigt, wurde der Server physisch nicht mit dem Netzwerk verbunden.
- Wird ein Computer mit einem Ausrufezeichen angezeigt, ist der Computer zwar mit dem Netzwerk verbunden, hat aber noch keine IP-Adresse vom DHCP-Server erhalten.
- Werden zwei Computer mit einer Weltkugel angezeigt, ist der Computer mit dem Netzwerk und dem Internet verbunden.

Verwalten der Netzwerkverbindungen

Haben Sie das Netzwerk- und Freigabecenter geöffnet, sehen Sie bereits die Netzwerkverbindung des Servers oder müssen feststellen, dass diese nicht hergestellt werden konnte. Sie müssen zunächst die Netzwerkverbindung richtig konfigurieren. Klicken Sie dazu links im Fenster im Bereich *Aufgaben* auf den Link *Netzwerkverbindungen verwalten* und rufen dann im neuen Fenster mit der rechten Maustaste die Eigenschaften Ihrer *LAN-Verbindung* auf (Abbildung 7.2). Es öffnet sich ein neues Fenster, in dem Sie die Eigenschaften der Netzwerkverbindung konfigurieren können. Die Konfiguration an dieser Stelle ist wiederum nahezu identisch mit Windows Server 2003.

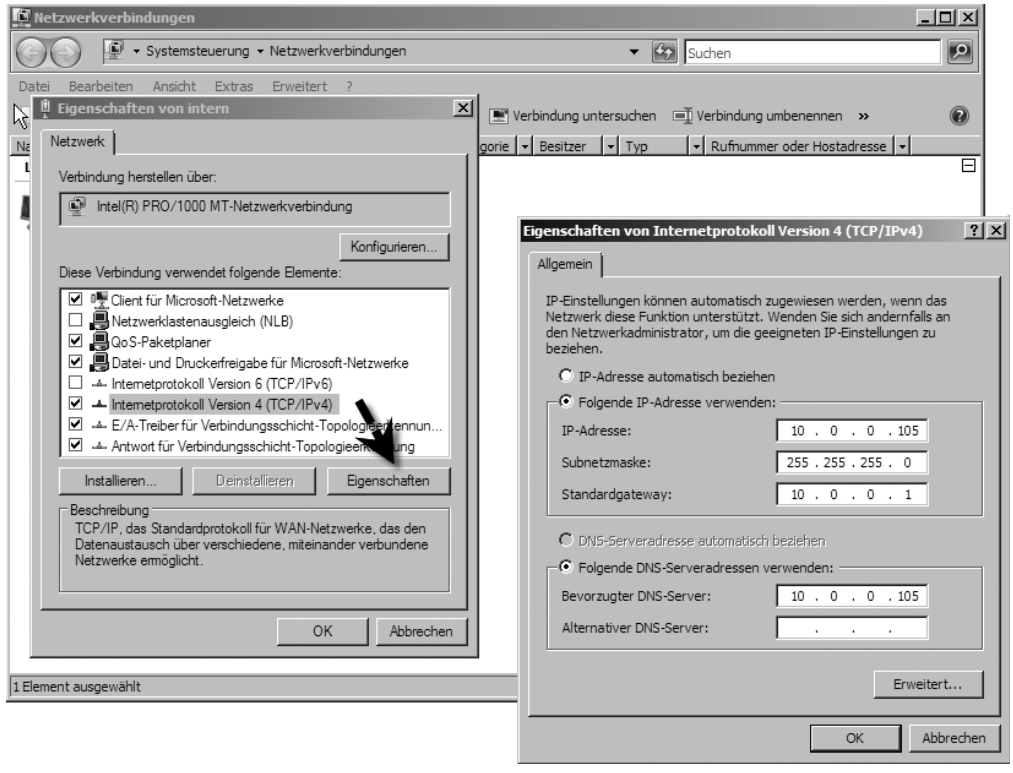
HINWEIS Sie können die Verwaltung der Netzwerkverbindungen auch über *Start/Ausführen/ncpa.cpl* starten.

Abbildg. 7.2 Konfigurieren der Netzwerkverbindungen in Windows Server 2008



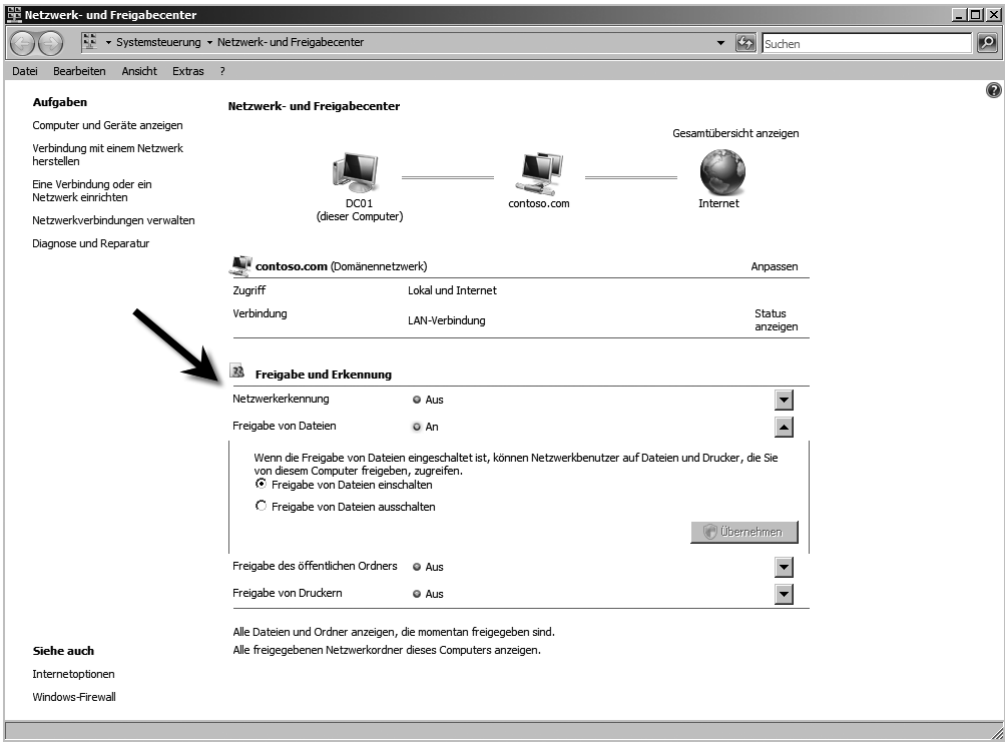
Markieren Sie als Nächstes den Eintrag *Internetprotokoll Version 4 (TCP/IPv4)*, und klicken Sie auf die Schaltfläche *Eigenschaften* (Abbildung 7.3). Hier können Sie jetzt eine ordnungsgemäße IP-Adresse vergeben. Wenn Sie die IP-Adresse manuell vergeben, setzen Sie die Markierung auf die Option *Folgende IP-Adresse verwenden* sowie die Option *Folgende DNS-Serveradressen verwenden* und tragen die notwendigen Daten ein. In diesem Beispiel hat der DNS-Server die IP-Adresse 10.0.0.105.

Abbildg. 7.3 Konfigurieren der IP-Einstellungen für einen Computer unter Windows Server 2008



Im Anschluss öffnet sich meistens ein neues Fenster für den Netzwerkstandort, und Sie müssen auswählen, wo Sie den Server betreiben. Wählen Sie die entsprechende Option aus, und schließen Sie dieses Fenster. In Unternehmen wählen Sie entweder die Option *zu Hause* oder *Arbeitsplatz* aus. Wird der Server in eine Domäne aufgenommen, wird der Netzwerkplatz automatisch auf den Domänenbetrieb umgestellt. Abhängig von diesen Einstellungen, können Daten auf dem Server im Netzwerk freigegeben werden. Wollen Sie auf dem Server Freigaben erstellen, müssen Sie diese noch im Bereich *Freigabe von Dateien* aktivieren (Abbildung 7.4). Erst dann ist der Zugriff über das Netzwerk möglich. Der Assistent aktiviert dazu in den Ausnahmen der Windows-Firewall den Zugriff auf den Server über Dateifreigaben. Diese Einstellungen werden auch vorgenommen, wenn Sie die Rolle eines Dateiservers installieren.

Abbildg. 7.4 Aktivieren der Dateifreigabe unter Windows Server 2008

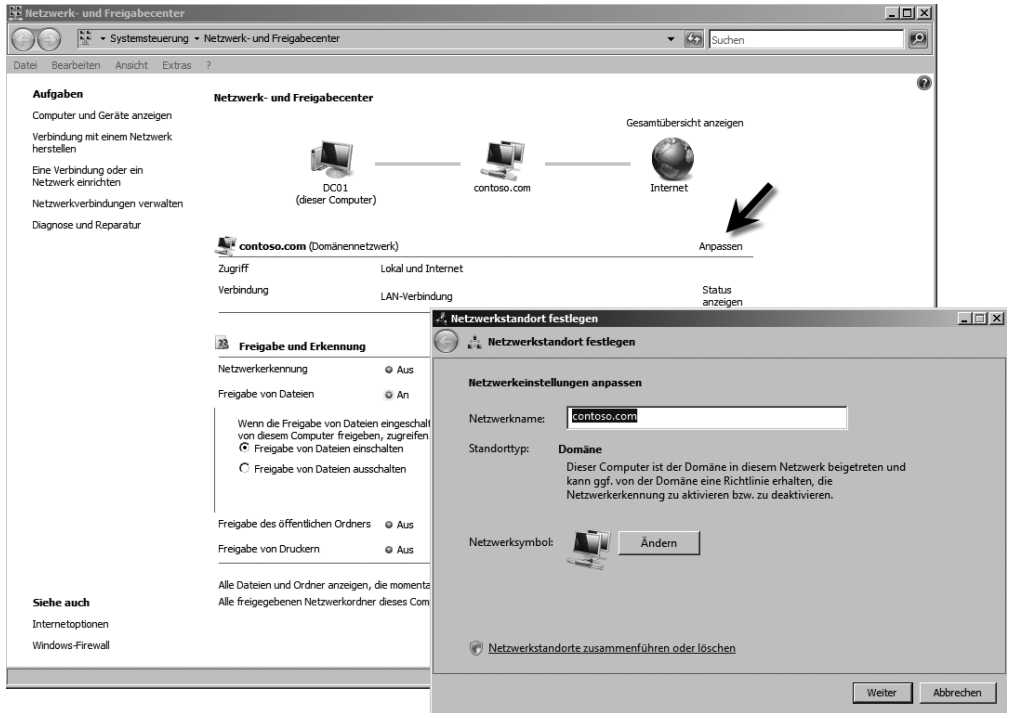


Neben Dateien können auch Drucker im Netzwerk freigegeben werden (siehe Kapitel 6). Normalerweise ist ein Drucker meistens direkt mit einem Server im Netzwerk verbunden. Damit andere Benutzer auf diesen Drucker zugreifen können, muss dieser auf dem Server freigegeben werden. Dazu schließen Sie den Drucker zunächst an einem Rechner an und installieren den Treiber. Stellen Sie sicher, dass der Drucker lokal drucken kann. Im nächsten Schritt können Sie diesen Drucker im Netzwerk freigeben. Auch die Freigabe von Druckern müssen Sie im Netzwerk- und Freigabecenter erst aktivieren. Diese Einstellungen werden vorgenommen, wenn Sie die Rolle eines *Druckservers* installieren.

Verwalten der Netzwerkstandorte

Bei der Einrichtung der Netzwerkverbindung haben Sie festgelegt, mit welcher Art von Netzwerk sich Ihr Server verbunden hat. Sie konnten festlegen, ob es sich um ein privates Netzwerk oder ein öffentliches Netzwerk handelt. Diese Einstellungen können nachträglich angepasst werden. Über den Link *Anpassen* im Bereich der Netzwerkstandorte lässt sich festlegen, um welches Netzwerk es sich handelt (Abbildung 7.5). Ist der Server Mitglied einer Domäne, müssen Sie in diesem Bereich keine Anpassungen vornehmen, da der Netzwerkstandort automatisch für eine Windows-Domäne konfiguriert wird.

Abbildg. 7.5 Anpassen und überprüfen des Netzwerkstandortes

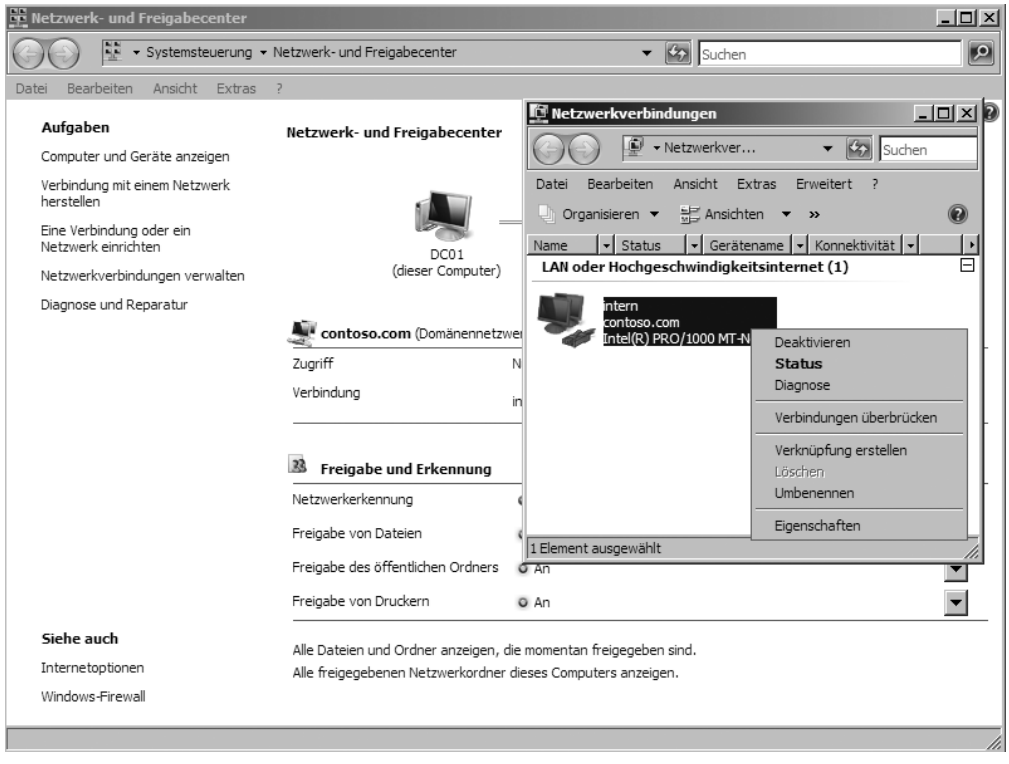


Über den Link *Gesamtübersicht anzeigen* öffnet sich ein neues Fenster, in dem alle Server und Netzwerkgeräte angezeigt werden, sofern Ihr Server diese im Netzwerk findet. Dieser Bereich ist extrem hilfreich, wenn Sie auf einem Server Netzwerk- oder Verbindungsprobleme untersuchen wollen. Allerdings können Sie sich nur dann eine Gesamtansicht anzeigen lassen, wenn die Netzwerkerkennung im Netzwerk- und Freigabecenter aktiviert worden ist. Solche Einstellungen werden in Domänen üblicherweise in den Gruppenrichtlinien vorgenommen. Die dazu notwendigen Einstellungen finden sich unter *Computerkonfiguration/Administrative Vorlagen/Netzwerk/Verbindungsschicht-Topologieerkennung*. Die Einstellungen sind selbsterklärend. Auf Seite *http://www.windowsnetworking.com/articles_tutorials/Enabling-Network-Mapping-Windows-Vista.html* finden Sie weitere Hinweise über die Aktivierung dieser Funktion. Über den Link *Diagnose und Reparatur* können Sie eventuell vorhandene Fehler von Windows überprüfen lassen und erhalten Hilfestellung, oder Vorschläge zur Behebung von Fehlern. Über den Link *Computer und Geräte anzeigen* im linken Bereich des Netzwerk- und Freigabecenters werden Ihnen alle Server und PCs angezeigt, die im Netzwerk gefunden werden können. Wenn Sie auf einen Server doppelt klicken, werden die Freigaben auf dem Server angezeigt und können geöffnet werden. Klicken Sie im Netzwerk- und Freigabecenter auf die einzelnen Symbole, welche die Verbindungen in Ihrem Netzwerk darstellen, können Sie direkt die notwendigen Programme starten, um den Teil des Netzwerkes zu durchsuchen. Klicken Sie zum Beispiel auf das Symbol *Internet*, öffnet sich der Internet Explorer mit der Startseite. So können Sie schnell überprüfen, ob die Verbindung zum Internet tatsächlich hergestellt werden kann. Ein Klick auf das Computer-Symbol öffnet den Windows-Explorer, ein Klick auf das Netzwerk-Symbol öffnet die Netzwerkumgebung.

Erweiterte Verwaltung der Netzwerkverbindungen

Wenn eine Netzwerkverbindung aktiviert ist, aber keine Netzwerkverbindung herstellen kann, wird die entsprechende Verbindung mit einem roten X angezeigt. Sie sollten beim Einsatz mehrerer Netzwerkverbindungen diese entsprechend benennen, da Windows die Bezeichnung nur durchnummeriert. Der Name einer Netzwerkverbindung beeinflusst nicht deren Konnektivität, sondern lediglich deren Bezeichnung und Überblick in Windows. Sie können die Bezeichnung von Netzwerkverbindungen über das Kontextmenü ändern. Klicken Sie eine Netzwerkverbindung mit der rechten Maustaste an, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Grundsätzlich gibt es an dieser Stelle acht verschiedene Möglichkeiten (Abbildung 7.6):

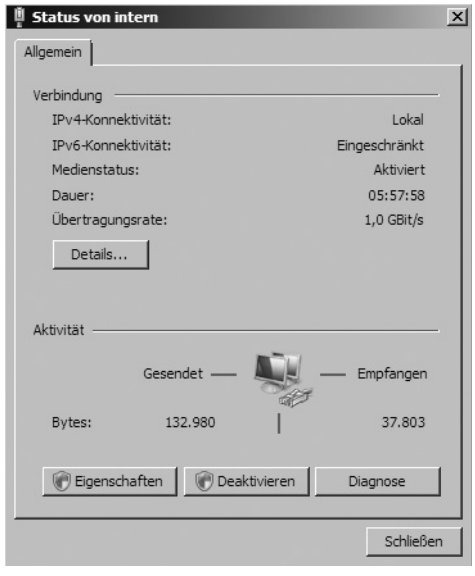
Abbildg. 7.6 Netzwerkverbindungen über das Kontextmenü verwalten



- **Deaktivieren** Wählen Sie diese Option aus, wird die Verbindung vom Netzwerk getrennt, auch wenn sie konfiguriert wurde und Verbindung hat. Die Verbindung verursacht keinerlei Fehlermeldungen mehr und die entsprechende Netzwerkkarte wird im Geräte-Manager deaktiviert. Die Karte verhält sich so, als ob sie nicht installiert ist.

- **Status** Wenn Sie diesen Menüpunkt auswählen, werden Ihnen ausführliche Informationen über die Konfiguration der Netzwerkverbindung angezeigt, sowie die Datenpakete, die über das Netzwerk gesendet wurden (Abbildung 7.7). Wollen Sie eine Netzwerkverbindung ausführlicher überprüfen, bietet sich dieser Menüpunkt an. Es öffnet sich ein neues Fenster, über das Sie zahlreiche Informationen erhalten und Konfigurationen vornehmen können. Sie erkennen zunächst, mit welcher Geschwindigkeit die Verbindung aufgebaut worden ist, wie lange die Netzwerkverbindung besteht und wie viele Datenpakete empfangen und gesendet wurden.

Abbildg. 7.7 Status von Netzwerkverbindungen anzeigen

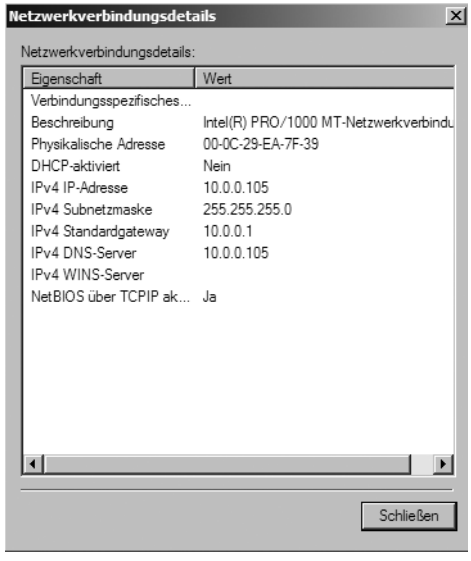


Klicken Sie auf die Schaltfläche *Details*, werden Ihnen ausführlichere Informationen über die Konfiguration der Netzwerkverbindung angezeigt (Abbildung 7.8). Sie erkennen die IP-Adresse, die physische (MAC)-Adresse sowie eine Vielzahl weiterer Informationen, die vor allem bei der Fehlersuche hilfreich sein können. Neben dieser Schaltfläche stehen Ihnen noch drei weitere Schaltflächen zur Verfügung, über die Sie die Netzwerkverbindung konfigurieren können:

- Eigenschaften
- Deaktivieren
- Diagnose

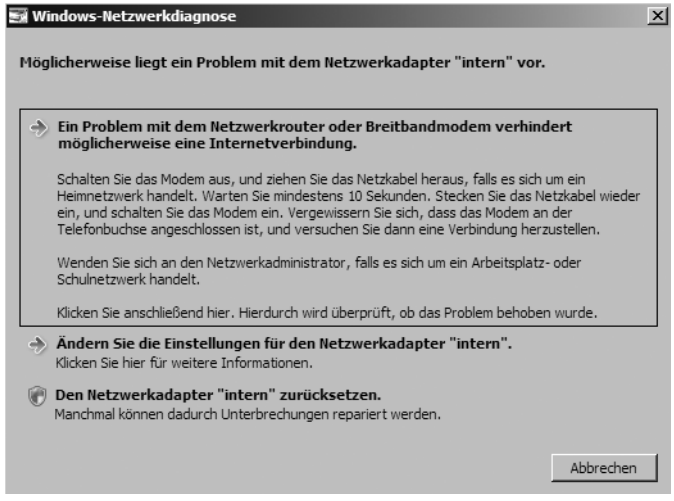
Die beiden Schaltflächen *Eigenschaften* und *Deaktivieren* erfordern administrative Berechtigungen, was durch das Windows-Schutzschild auf den Schaltflächen symbolisiert wird. Zu den Eigenschaften der Netzwerkverbindung gelangen Sie auch über das Kontextmenü. Die Schaltfläche *Deaktivieren* hat die gleiche Auswirkung wie die Auswahl der entsprechenden Option aus dem Kontextmenü.

Abbildg. 7.8 Anzeigen der Details einer Netzwerkverbindung



Klicken Sie im *Status*-Dialogfeld auf die Schaltfläche *Diagnose*, versucht Windows Server 2008 festzustellen, warum eine bestimmte Netzwerkverbindung nicht funktioniert. Auch diese Option ist über das Kontextmenü der Verbindung zu erreichen. Sobald Sie die Diagnose gestartet haben, schlägt Windows eine Fehlerbehebungsmaßnahme vor. Lesen Sie sich die Meldung durch, bevor Sie eine andere Maßnahme durchführen, und überprüfen Sie, ob der entsprechende Fehler bereits durch die Hinweise gelöst werden kann. Sie können auf die einzelnen Optionen der Diagnose klicken, um die vorgeschlagene Option automatisch durchführen zu lassen. Im Anschluss versucht Windows Server 2008 automatisch den Fehler zu beheben und die Netzwerkverbindung wiederherzustellen. Oft liegt beim Einsatz von DHCP lediglich ein Fehler in dessen Konfiguration vor.

Abbildg. 7.9 Durchführen einer automatischen Diagnose für Netzwerkverbindungen

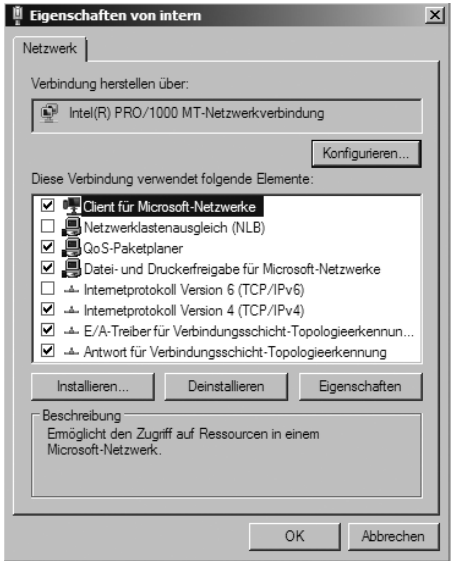


Wenn Sie im Kontextmenü einer Netzwerkverbindung die Option *Verbindungen überbrücken* auswählen, können Sie den Windows Server 2008-Computer als Verbindung zwischen zwei Netzwerken einsetzen. Dazu wird eine Netzwerkkarte mit dem einen Netzwerk verbunden und eine zweite Netzwerkkarte mit einem anderen Netzwerk. Die beiden Netzwerkverbindungen müssen IP-Adressen in unterschiedlichen Subnetzen haben. Um eine Netzwerkbrücke aufzubauen, also zwei verschiedene Netzwerke physisch miteinander zu verbinden, müssen Sie zunächst die erste Verbindung auswählen, dann die Strg-Taste drücken und anschließend die zweite Verbindung auswählen. Mit Aufruf des Kontextmenübefehls *Verbindungen überbrücken* startet Windows den Assistent zum Aufbau einer Netzwerkbrücke. Die Netzwerkbrücke bietet eine einfache und kostengünstige Möglichkeit zur Verbindung von LAN-Segmenten. Eine Konfiguration ist nicht erforderlich, und Sie müssen auch keine zusätzliche Hardware wie Router oder Brücken erwerben. Die Netzwerkbrücke automatisiert die Konfiguration, die für die Weiterleitung von Datenverkehr zwischen Netzwerken erforderlich ist. Die Netzwerkbrücke kann den Datenverkehr von einem LAN-Segment zu einem anderen LAN-Segment weiterleiten und ermöglicht so, dass alle Computer miteinander kommunizieren können

Eigenschaften von Netzwerkverbindungen

Wenn Sie aus dem Kontextmenü einer Netzwerkverbindung die *Eigenschaften* aufrufen, oder über den Status einer Netzwerkverbindung zur gleichen Konfiguration gelangen, können Sie das Verhalten der Netzwerkverbindung ausführlich konfigurieren (Abbildung 7.10).

Abbildg. 7.10 Verwalten der Eigenschaften einer Netzwerkverbindung

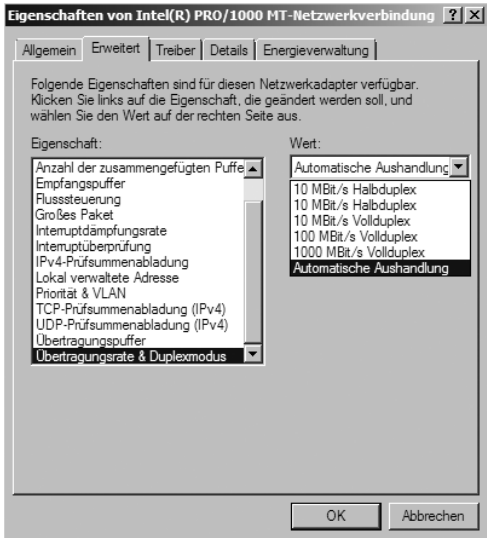


Über die Schaltfläche *Konfigurieren* können Sie die Einstellungen der Netzwerkkarte anpassen. Diese Einstellungen haben zunächst nichts mit den Netzwerkprotokollen zu tun, sondern ausschließlich mit dem Verhalten der Netzwerkkarte im Netzwerk. Normalerweise müssen an dieser Stelle keine Einstellungen vorgenommen werden. Wenn Sie Anpassungen vornehmen, sollten Sie genau wissen, was Sie tun, da Experimente an dieser Stelle schnell zu einem Ausfall der Netzwerkverbindung füh-

ren können. Sie stellen hier zum Beispiel ein, wie hoch die Netzwerkgeschwindigkeit in Ihrem Netzwerk ist. Nachdem Sie auf die Schaltfläche *Konfigurieren* geklickt haben, erscheint ein neues Fenster mit mehreren Registerkarten (Abbildung 7.11):

- Die Registerkarte *Allgemein* ist zunächst weniger interessant, da hier nur ein paar Informationen zur Netzwerkkarte angezeigt werden.
- Auf der Registerkarte *Erweitert* werden die Einstellungen angezeigt, die der Treiber der Netzwerkkarte unterstützt. Die angezeigten Optionen und Einstellungsmöglichkeiten sind je nach installierter Netzwerkkarte und zugehörigem Treiber unterschiedlich. Die wichtigste Einstellung auf dieser Registerkarte sind die Optionen des Duplexmodus und der Geschwindigkeit des Netzwerkes. Die Bezeichnung der Menüs und die einstellbaren Werte sehen bei den verschiedenen Treibern der Netzwerkkarte unterschiedlich aus, aber Sie können immer zwischen Standardwerten auswählen. Standardmäßig steht die Erkennung der Netzwerkgeschwindigkeit auf *Automatisch*. Wenn Sie hier Einstellungen ändern, mit denen andere Netzwerkgeräte nicht funktionieren, kann der Server keine Verbindung mehr zum Netzwerk herstellen. Wenn Sie daher Verbindungsprobleme bei einem Computer haben, und die IP-Konfiguration korrekt ist, sollten Sie überprüfen, welche Netzwerkgeschwindigkeit für die Karte eingestellt ist. Die wichtigste Einstellung in diesem Bereich ist der Duplexmodus. Dieser legt fest, wie die Daten im Netzwerk von diesem PC aus empfangen und gesendet werden können.

Abbildg. 7.11 Konfigurieren des Duplexmodus für Netzwerkkarten



Grundsätzlich können Netzwerkkarten in zwei verschiedenen Modi betrieben werden:

- **Vollduplex** Bei diesem Modus kann der Computer gleichzeitig Daten aus dem Netzwerk empfangen und Daten an das Netzwerk senden. Diese Übertragungsvariante ist die schnellste, wird aber nicht von allen Netzwerkgeräten, vor allem älteren, unterstützt.
- **Halbduplex** Bei diesem Modus können keine Daten gleichzeitig empfangen und gesendet werden, sondern immer nur jeweils in eine Richtung. Da die Daten zwar auch in beide Richtungen fließen können, aber nicht gleichzeitig, ist die Geschwindigkeit etwas geringer.

Auf der Registerkarte *Energieverwaltung* können Sie konfigurieren, ob Windows Server 2008 das Gerät zeitweise deaktivieren kann, wenn es nicht benötigt wird. Standardmäßig darf Windows Geräte ausschalten um Energie zu sparen, zum Beispiel auch, um in den Energiesparmodus zu wechseln. Ansonsten sind bei der Konfiguration von Netzwerkkarten keine weiteren Einstellungen zu beachten. Interessanter sind hier die Einstellungen der einzelnen Netzwerkprotokolle und -dienste, die für eine Netzwerkverbindung standardmäßig bereits aktiviert sind.

HINWEIS An dieser Stelle sollten Sie keine Dienste oder Protokolle deinstallieren, ohne zu wissen, wofür diese benötigt werden. Teilweise werden auch Dienste und Protokolle in den anderen Netzwerkverbindungen deinstalliert, wenn Sie diese für eine bestimmte Netzwerkverbindung deinstallieren. Wenn Sie Computer untereinander vernetzen und Dateien oder Drucker freigeben, werden die beiden Dienste *Client für Microsoft-Netzwerke* und *Datei- und Druckerfreigabe für Microsoft-Netzwerke* dringend benötigt und sollten keinesfalls deinstalliert werden.

Sie können neben der Deinstallation von Diensten oder Protokollen auch einen Dienst für eine einzelne Netzwerkkarte deaktivieren. In diesem Fall müssen Sie in den Eigenschaften der Netzwerkverbindung nur das Häkchen bei dem Dienst entfernen. Der Dienst *QoS-Paketplaner* (Quality Of Service) ist dafür zuständig, dass der Computer immer genügend Ressourcen zur Verfügung stellt, um auf Netzwerkpakete zu antworten. Wenn Sie zum Beispiel viele Downloads gleichzeitig aus dem Internet durchführen und parallel eine große Datenmenge auf andere Computer im Netzwerk verteilen, sorgt der QoS-Paketplaner dafür, dass eine Mindestgröße an Bandbreite zur Verfügung bleibt. Manche Experten raten dazu, diesen Dienst zu deinstallieren, da er eine gewisse Bandbreite selbst verbraucht. Allerdings benötigen die wenigsten Unternehmen heutzutage wirklich jede kleine Menge Bandbreite, sondern profitieren besser davon, dass die Verbindung stabil bleibt. Wenn Sie das Gefühl haben, Ihr Computer ist im Netzwerk zu langsam, wird die Geschwindigkeit sicherlich nicht dadurch steigen, indem Sie diesen Dienst deaktivieren oder deinstallieren. Sie können dies aber ohne Probleme selbst testen und bei Leitungsproblemen den QoS-Paketplaner testweise deaktivieren.

Eigenschaften von TCP/IP und DHCP

Das wichtigste Protokoll für die Verbindung in Netzwerke stellt TCP/IP dar. Sie können entweder eine manuelle Konfiguration durchführen, also eine so genannte statische IP-Adresse zuweisen, oder mit einem DHCP-Server arbeiten (siehe Kapitel 11). DHCP ist ein TCP/IP-Standard für die vereinfachte Verwaltung der IP-Konfiguration und -Zuweisung in einem Netzwerk. DHCP verwendet einen DHCP-Server zum dynamischen Zuweisen von IP-Adressen. DHCP-Server enthalten eine Datenbank mit IP-Adressen, die Hosts im Netzwerk zugewiesen werden können. Um DHCP in einem Netzwerk zu verwenden, muss für die Hosts in diesem Netzwerk DHCP aktiviert sein. Zum Aktivieren von DHCP müssen Sie das Kontrollkästchen *IP-Adresse automatisch beziehen* aktivieren. Über Protokolle wie BOOTP oder DHCP können IP-Adressen beim Hochfahren des Rechners über einen entsprechenden Server zugewiesen werden. Auf dem Server wird dazu vom Administrator ein Bereich von IP-Adressen definiert, aus dem sich weitere Rechner beim Hochfahren eine Adresse entnehmen können. Diese Adresse wird an den Rechner geleast, also für eine bestimmte Zeit vergeben. Rechner, die feste Adressen benötigen, können im Ethernet-Netzwerk über ihre MAC-Adresse (physische Adresse) identifiziert werden und eine dauerhafte Adresse erhalten. Vorteil hierbei ist die zentrale Verwaltung der Adressen. Mit DHCP kann einem Computer, der auch als DHCP-Client bezeichnet wird, aus einer dem Subnetz zugewiesenen Adressdatenbank automatisch eine IP-Adresse zugewiesen werden. Wenn ein Computer für einen bestimmten Zeitraum offline ist, kann DHCP dessen IP-Adresse anderweitig vergeben.

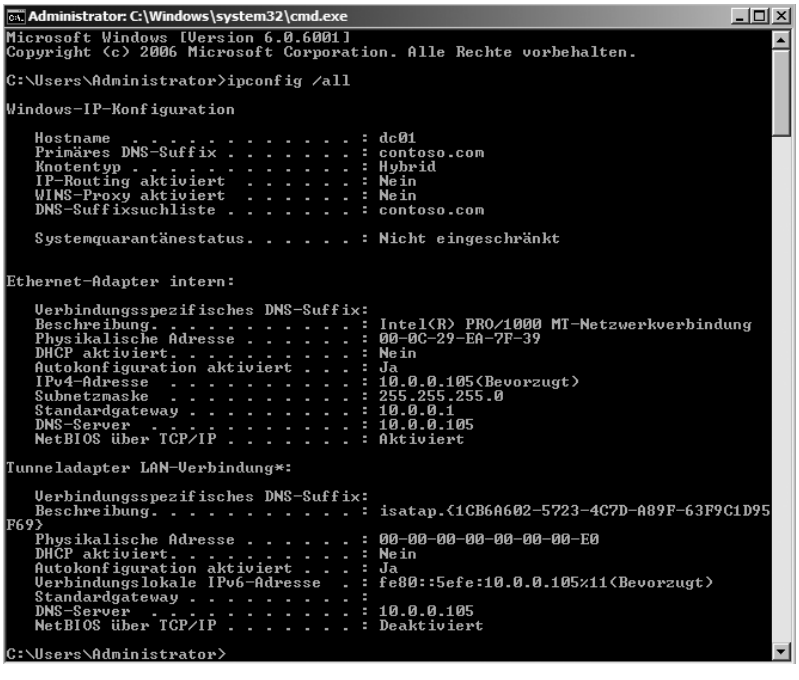
APIPA (Automatic Private IP Addressing)

Für den Fall, dass kein DHCP-Server für das automatische Zuweisen einer IP-Adresse erreicht werden kann, bestimmt Windows Server 2008 eine Adresse in der für Microsoft reservierten IP-Adressierungsklasse, die von 169.254.0.1 bis 169.254.255.254 reicht. Diese Adresse wird verwendet, bis ein DHCP-Server gefunden wird. Diese Methode des Beziehens einer IP-Adresse wird als automatische IP-Adressierung (APIPA) bezeichnet. Bei dieser Methode wird kein DNS, WINS oder Standardgateway zugewiesen, da diese Methode nur für ein kleines Netzwerk mit einem einzigen Netzwerksegment entworfen wurde. Dafür können alle Computer in einem Netzwerk, die eine APIPA-Adresse verwenden, miteinander kommunizieren.

Anzeigen der IP-Adresse

Es können Situationen auftreten, in denen Sie die IP-Adressinformationen für einen bestimmten Computer anzeigen müssen. Dies ist der Fall, wenn Ihr Computer beispielsweise nicht mit anderen Computern im Netzwerk kommuniziert oder wenn andere Computer nicht mit Ihrem Computer kommunizieren können. In solchen Situationen müssen Sie die IP-Adresse der anderen Computer kennen, um die Ursache des Problems bestimmen zu können. Im Dialogfeld *Eigenschaften von Internetprotokoll (TCP/IP)* können Sie statische TCP/IP-Informationen anzeigen. Windows Server 2008 enthält ein Befehlszeilendienstprogramm mit der Bezeichnung *Ipconfig*, um TCP/IP-Informationen anzuzeigen. Mit dem Dienstprogramm *Ipconfig* werden die TCP/IP-Konfigurationsoptionen auf einem Host überprüft, aber nicht festgelegt. Zu diesen Optionen zählen die IP-Adresse, die Subnetzmaske und das Standardgateway. Starten Sie das Programm am besten über eine Befehlszeile. Ausführlichere Informationen erhalten Sie, wenn Sie die Option */all* mit angeben. Geben Sie an der Eingabeaufforderung *ipconfig /all* ein. Auf dem Bildschirm werden die Informationen zu allen TCP/IP-Konfigurationsoptionen angezeigt. Nun sehen Sie, ob DHCP aktiviert ist.

Abbildg. 7.12 Anzeige ausführlicher IP-Informationen in der Befehlszeile



Zusätzlich lassen sich beim Aufruf von *ipconfig* noch die beiden Optionen */renew* und */release* angeben:

- **ipconfig /release** Entfernt die IP-Adresse vom Client und fordert keine neue an. Wenn ein Client Probleme hat, eine Verbindung mit einem DHCP-Server herzustellen, sollten Sie immer zuerst die IP-Adresse beim Client zurücksetzen.
- **ipconfig /renew** Fordert vom DHCP-Server eine erneute Verlängerung des Lease oder eine neue IP-Adresse an. Sollte der Befehl nicht funktionieren, geben Sie zunächst *ipconfig /release* ein.

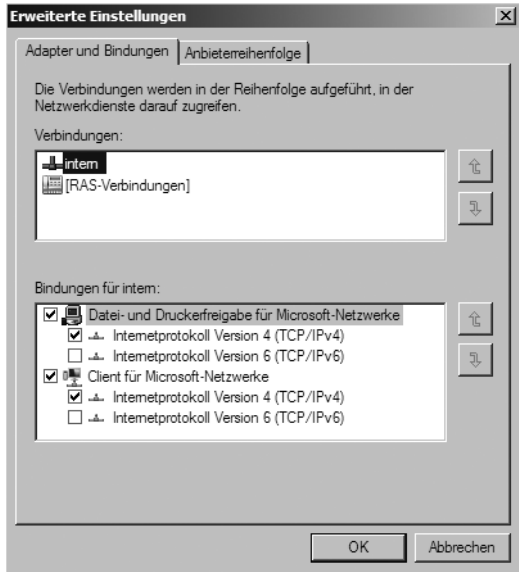
Bindungsreihenfolge der Netzwerkverbindungen konfigurieren

Wenn Sie mehrere Netzwerkkarten in Ihrem Computer eingebaut haben, werden Netzwerkpakete nicht immer an alle Netzwerkkarten gleichzeitig verschickt, sondern immer in einer bestimmten Reihenfolge. Damit die Antwortzeiten im Netzwerk optimiert werden, bietet es sich natürlich an, wenn Sie die Reihenfolge so konfigurieren, dass Ihre produktive Netzwerkkarte (meistens wird sowieso nur eine verwendet) in der Reihenfolge ganz oben steht. Damit Sie diese Reihenfolge festlegen können, gehen Sie folgendermaßen vor:

1. Klicken Sie zunächst im Netzwerk- und Freigabecenter auf den Link *Netzwerkverbindungen verwalten*.
2. Aktivieren Sie anschließend über *Organisieren/Layout* die Menüleiste. Alternativ können Sie temporär die Menüleiste über die Alt-Taste einblenden.
3. Rufen Sie den Menübefehl *Erweitert/Erweiterte Einstellungen* auf.

Es öffnet sich ein neues Fenster, über das Sie unter anderem die Bindungsreihenfolge der Netzwerkkarten einstellen können. Klicken Sie dazu auf der Registerkarte *Adapter und Bindungen* im Bereich *Verbindungen* auf die ausgewählte LAN-Verbindung und dann auf die Schaltflächen mit den Pfeilen, damit die gewünschte Verbindung ganz nach oben gesetzt wird.

Abbildg. 7.13 Konfigurieren der Bindungsreihenfolge der Netzwerkverbindungen



IP-Routing – Erstellen von manuellen Routen

Sie können in den IP-Eigenschaften von Netzwerkkarten immer nur ein Standardgateway festlegen. Wenn IP-Pakete zu Hosts geschickt werden sollen, die außerhalb des konfigurierten Subnetzes liegen, werden diese von Windows immer an das konfigurierte Standardgateway geschickt. Auch wenn in einen Computer mehrere Netzwerkkarten eingebaut sind, kann immer nur ein Standardgateway festgelegt werden. Wenn Sie aber Pakete zu unterschiedlichen Netzwerken schicken wollen, können Sie in Windows manuelle Routen erstellen. Diese Routen werden mit dem Befehl *route* in der Befehlszeile erstellt. Für IPv6 müssen Sie den Befehl *netsh interface ipv6 add route* verwenden, um manuelle Routen zu erstellen. Das Standardgateway können Sie entweder über DHCP mitgeben, oder auf einer der eingebauten Netzwerkkarten manuell festlegen. Alle Netzwerkpakete, die nicht an das interne Netzwerk gesendet werden können und für die keine manuelle Route hinterlegt ist, werden zum Standardgateway geschickt. Das Standardgateway muss sich im gleichen Subnetz befinden, wie die IP-Adresse des Computers. Die zweite Schnittstelle des Standardgateways bzw. weitere Schnittstellen befinden sich in anderen Subnetzen. Um manuelle Routen zu erstellen, wird der Befehl *Route.exe* in der folgenden Syntax verwendet:

route –p add <ziel> MASK <netzmaske> <gateway> METRIC <metrik> IF <schnittstelle>.

Die einzelnen Parameter haben folgende Funktionen:

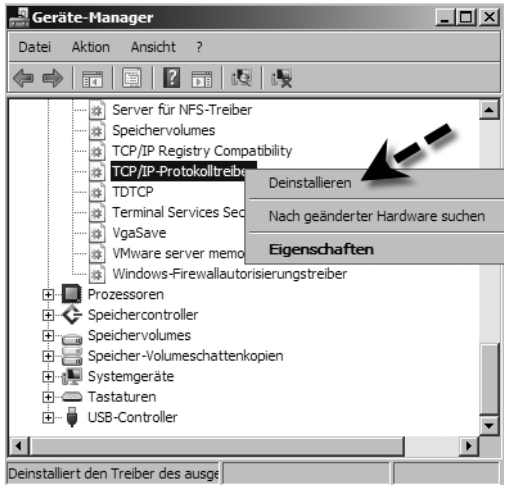
- Mit der Option *–p* wird festgelegt, dass die Route auch nach dem Booten des PCs noch vorhanden ist. Standardmäßig werden die Routen beim Neustart wieder gelöscht.
- Die Option *add* fügt eine Route hinzu, mit *del* kann eine Route gelöscht werden.
- **ziel** Das Ziel kann entweder eine IP-Adresse oder ein Subnetzpräfix, eine IP-Adresse für eine Hostroute oder 0.0.0.0 für die Standardroute sein.
- **MASK** Die Subnetzmaske kann entweder die korrekte Subnetzmaske für eine IP-Adresse oder ein Subnetzpräfix, 255.255.255.255 für eine Hostroute oder 0.0.0.0 für die Standardroute sein. Wenn keine Angabe gemacht wird, wird die Subnetzmaske 255.255.255.255 verwendet.
- **gateway** Gibt die Weiterleitungs-IP-Adresse oder die IP-Adresse des nächsten Hops an, über die die durch das Netzwerkziel und die Subnetzmaske definierten Adressen erreichbar sind. Bei Remoterouten, die über mindestens einen Router erreichbar sind, ist die Gatewayadresse die direkt erreichbare IP-Adresse eines angrenzenden Routers.
- **metrik** Gibt eine ganzzahlige Kostenmetrik (im Bereich von 1 bis 9.999) für die Route an. Sie wird verwendet, wenn mehrere Routen in der Routingtabelle zur Wahl stehen, die der Zieladresse eines weitergeleiteten Pakets entsprechen. Es wird die Route mit der niedrigsten Metrik ausgewählt. Die Metrik kann die Anzahl der Hops, die Geschwindigkeit und Zuverlässigkeit des Pfads, den Pfaddurchsatz oder administrative Eigenschaften widerspiegeln.
- **IF** Gibt den Schnittstellenindex der Schnittstelle an, über die das Ziel erreichbar ist. Eine Liste der Schnittstellen und ihrer Schnittstellenindizes können Sie mit dem Befehl *route print* anzeigen. Sie können für den Schnittstellenindex sowohl Dezimal- als auch Hexadezimalwerte verwenden. Stellen Sie Hexadezimalwerten 0x voran. Wenn Sie den *IF*-Parameter nicht angeben, wird die Schnittstelle anhand der Gatewayadresse ermittelt.

Neuinstallation von TCP/IPv4

Unter manchen Umständen kann es sinnvoll sein, das TCP/IP-Protokoll neu installieren zu lassen, zum Beispiel wenn Änderungen vorgenommen worden sind, die nicht mehr nachvollziehbar sind, das Protokoll beschädigt ist, oder Sie alle anderen Möglichkeiten ausgetestet haben. Microsoft empfiehlt die Deinstallation von TCP/IP nicht. Wenn Sie das Protokoll dennoch deinstallieren wollen, besteht die Gefahr, dass der Computer oder einzelne Netzwerkanwendungen nicht mehr funktionsfähig sind. Sie sollten den Weg der Deinstallation von TCP/IPv4 daher nur dann wählen, wenn auf einem Server alle anderen Möglichkeiten zur Fehlerbehebung ausgeschöpft worden sind. Wenn Sie in den Eigenschaften der Netzwerkverbindung das TCP/IP-Protokoll anklicken, wird die Schaltfläche zur Deinstallation inaktiv. Sie müssen daher einen anderen Weg wählen als die Standard-Deinstallation:

1. Um das Protokoll zu deinstallieren, müssen Sie zunächst den Geräte-Manager aufrufen. Der schnellste Weg geht über *Start/Ausführen/devmgmt.msc*.
2. Im Anschluss müssen Sie die ausgeblendeten Geräte anzeigen lassen. Hierüber versteckt Windows Server 2008 Geräte, die zum Systemkern gehören und eigentlich nicht deinstalliert werden sollen. Sie können die Anzeige der ausgeblendeten Geräte über den Menübefehl *Ansicht/Ausgeblendete Geräte anzeigen* aktivieren.
3. Nachdem Sie die Ansicht der ausgeblendeten Geräte aktiviert haben, suchen Sie als Nächstes nach der Gerätegruppe *Nicht-PnP-Treiber*.
4. Öffnen Sie den Knoten *Nicht-PnP-Treiber* und suchen Sie nach dem Gerät *TCP/IP-Protokolltreiber*.
5. Klicken Sie dieses Gerät mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Deinstallieren*.

Abbildg. 7.14 Deinstallieren des TCP/IP-Protokolltreibers zur Reparatur von IPv4 auf einem Server



6. Nachdem Sie die Deinstallation ausgewählt haben, erscheint ein Fenster, über das Sie die Deinstallation bestätigen müssen. Wenn Sie die Deinstallation bestätigt haben, wird das Protokoll vom Computer ohne weitere Meldung entfernt.

7. Nachdem das Protokoll entfernt wurde, müssen Sie den Computer neu starten. Während des Startvorgangs wird das Protokoll automatisch wieder installiert und die alten Einstellungen werden aus der Registry übernommen.

Wollen Sie die Einstellungen der TCP/IP-Konfiguration ebenfalls zurücksetzen, geben Sie in der Befehlszeile die folgenden Befehle ein und bestätigen Sie diese jeweils mit der ↵-Taste:

Netsh

Int

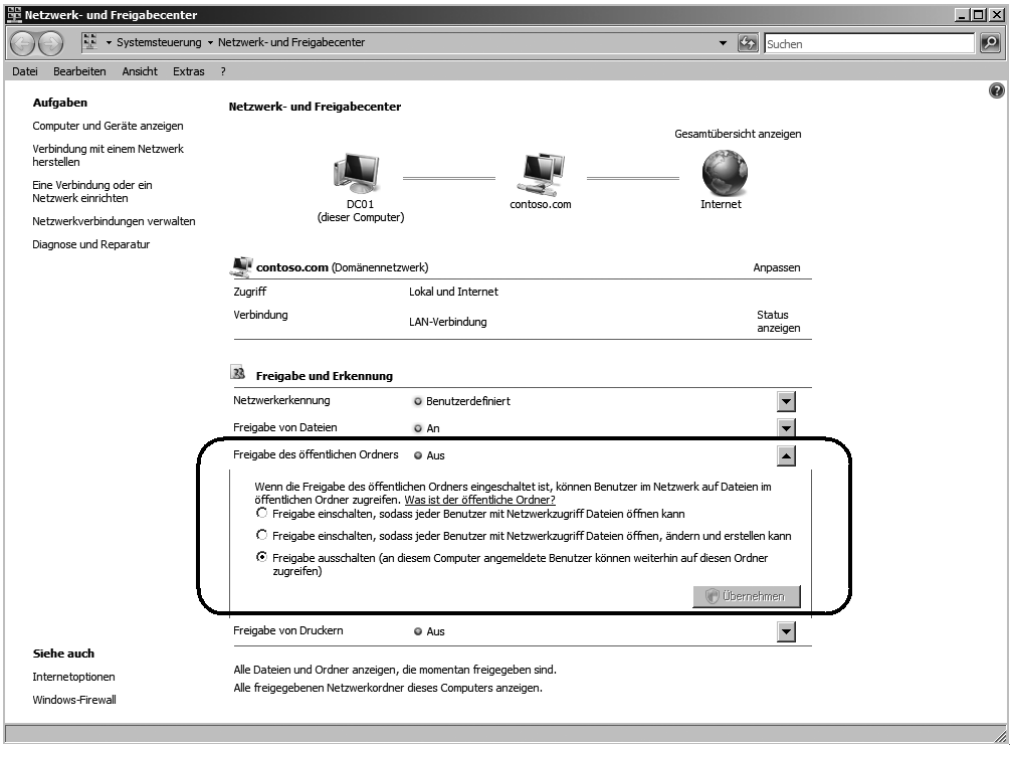
Tcp

Reset

Der öffentliche Ordner

Der öffentliche Ordner ist eine neue Funktion in Windows Vista und Windows Server 2008 und dient dem unkomplizierten Informationsaustausch der Benutzer des lokalen PCs oder Servers und den Benutzern im Netzwerk. Alle Ordner und Dateien im öffentlichen Ordner stehen sofort allen Anwendern des Computers und im Netzwerk zur Verfügung. Der Zugriff auf den öffentlichen Ordner muss im Netzwerk- und Freigabecenter ebenfalls erst konfiguriert und gestattet werden (Abbildung 7.15).

Abbildg. 7.15 Konfigurieren des öffentlichen Ordners in Windows Server 2008



Der Ordner steht jedem Anwender des Servers oder PCs über *Start/Computer/Öffentlich* zur Verfügung (auf der linken Seite). Dadurch können Anwender auf Vista-PCs schnell und unkompliziert Daten untereinander und im Netzwerk austauschen. Der Ordner *Öffentlich* befindet sich im Verzeichnis *C:\Benutzer*. Hier können auch nachträglich Anpassungen an den Berechtigungen und der Freigabe vorgenommen werden. Wenn andere Anwender die Freigabe als Netzlaufwerk anbinden, oder direkt auf die Freigabe zugreifen wollen, können diese den Pfad \\<*Servername-Name*>*public* verwenden. Sie können sich den öffentlichen Ordner über das Netzwerk auch als festen Laufwerksbuchstaben verbinden. Klicken Sie dazu mit der rechten Maustaste auf den Eintrag *Netzwerk* im Startmenü und wählen Sie im daraufhin geöffneten Kontextmenü den Befehl *Netzlaufwerk zuordnen*. Es öffnet sich ein neues Fenster, in dem Sie den Freigabenamen eingeben sowie den Laufwerksbuchstaben definieren, unter dem das Laufwerk im Windows-Explorer angezeigt wird. Anschließend wird das Verzeichnis über das Netzwerk geöffnet und Sie können zukünftig über den Windows-Explorer auf das Laufwerk zugreifen.

Windows Server 2008 und Active Directory-Domänen

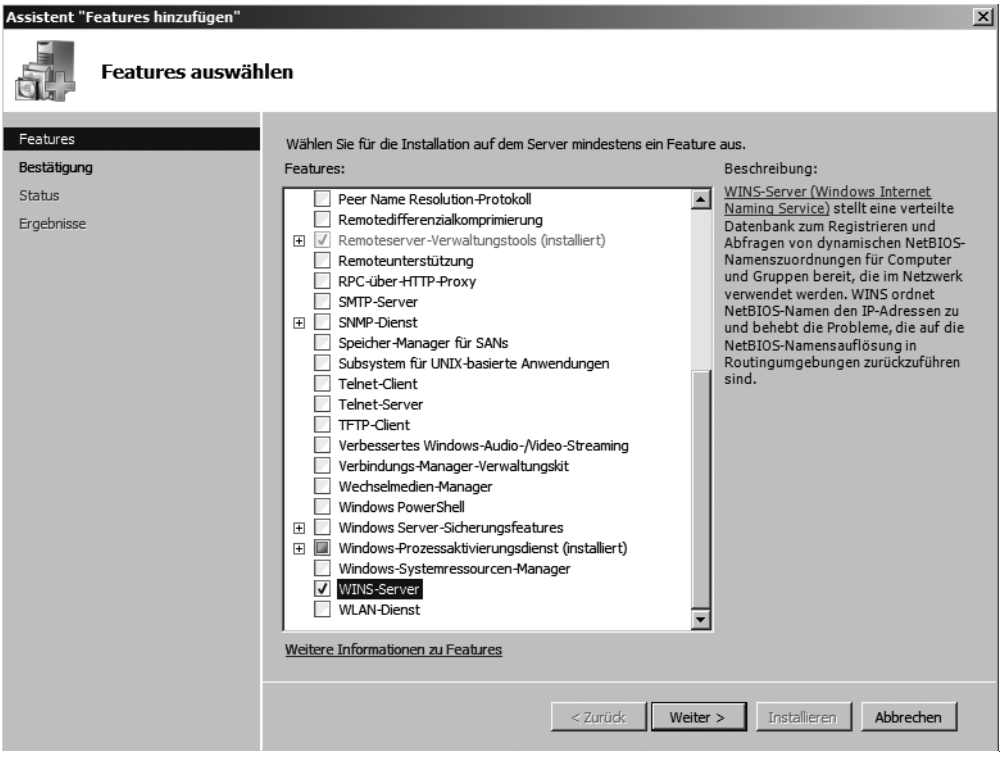
Die meisten Unternehmen werden Windows Server 2008 in einer Windows-Domäne aufnehmen oder als Domänencontroller betreiben (siehe Kapitel 8). In einem Unternehmensnetzwerk können die Hauptvorteile der Microsoft-Betriebssysteme, sei es auf Ebene der Server oder der Clients, erst sinnvoll ausgespielt werden, wenn eine Active Directory-Domäne gebildet wird. Der erste Schritt, einen Windows Server 2008 in eine Windows-Domäne als Mitgliedsserver aufzunehmen, ist, den Server mit dem Netzwerk zu verbinden und zu überprüfen, ob ein Domänencontroller mit dem Ping-Befehl, ganz ohne Namensauflösung erreicht werden kann. Erst wenn sichergestellt ist, dass der Domänencontroller auf Netzwerkebene erreicht werden kann, sollten Sie weitere Schritte durchführen. Dieser Test ist vor allem in Verbindung mit der Windows-Firewall sinnvoll. Der nächste wichtige Schritt ist das Eintragen eines DNS-Servers in den IP-Einstellungen eines Windows Server 2008-Servers. Erst wenn ein DNS-Server eingetragen wurde, der die DNS-Zone der Active Directory-Domäne auflösen kann, ist eine Aufnahme in eine Windows-Domäne möglich. Diese Einstellung erfolgt in den Netzwerkeinstellungen der LAN-Verbindung. Sie finden diese, indem Sie das Netzwerk- und Freigabecenter aufrufen.

Windows Internet Name Service (WINS)

Zu jeder Active Directory-Domäne gehört ein WINS-Server (siehe auch Kapitel 11). WINS steht für *Windows Internet Name Service* und ist der Vorgänger der dynamischen DNS-Aktualisierung. Während DNS für die Namensauflösung mit vollqualifizierten Domänennamen zuständig ist, werden mit WINS NetBIOS-Namen aufgelöst. Die Namensauflösung in einem Active Directory ist überaus wichtig. Sie können auf den Domänencontrollern neben DNS auch ohne weiteres den WINS-Dienst installieren, da dieser so gut wie keine Auswirkungen auf das System hat. DNS kann darüber hinaus eng mit WINS zusammenarbeiten. Seit Windows Server 2003 SP1 wurden Erweiterungen eingebaut, welche die Namensauflösung zur Replikation von Active Directory über WINS abwickeln können, falls DNS Probleme hat. Auch Windows Server 2008 unterstützt noch WINS. Damit sich die Server und Servers beim WINS registrieren und Daten aus WINS abfragen können, müssen Sie in den IP-Einstellungen die WINS-Server eintragen. Auf den Arbeitsstationen können Sie diese Ein-

stellungen auch mit Hilfe eines DHCP-Servers verteilen. WINS kann als Feature über den Server-Manager installiert werden (siehe Abbildung 7.16 und Kapitel 11). Die Verwaltung der Funktion ist nahezu identisch mit Windows Server 2003. Auch die Replikation zwischen WINS-Servern unter Windows Server 2003 und Windows Server 2008 ist möglich.

Abbildg. 7.16 WINS steht auch noch in Windows Server 2008 als Feature zur Verfügung

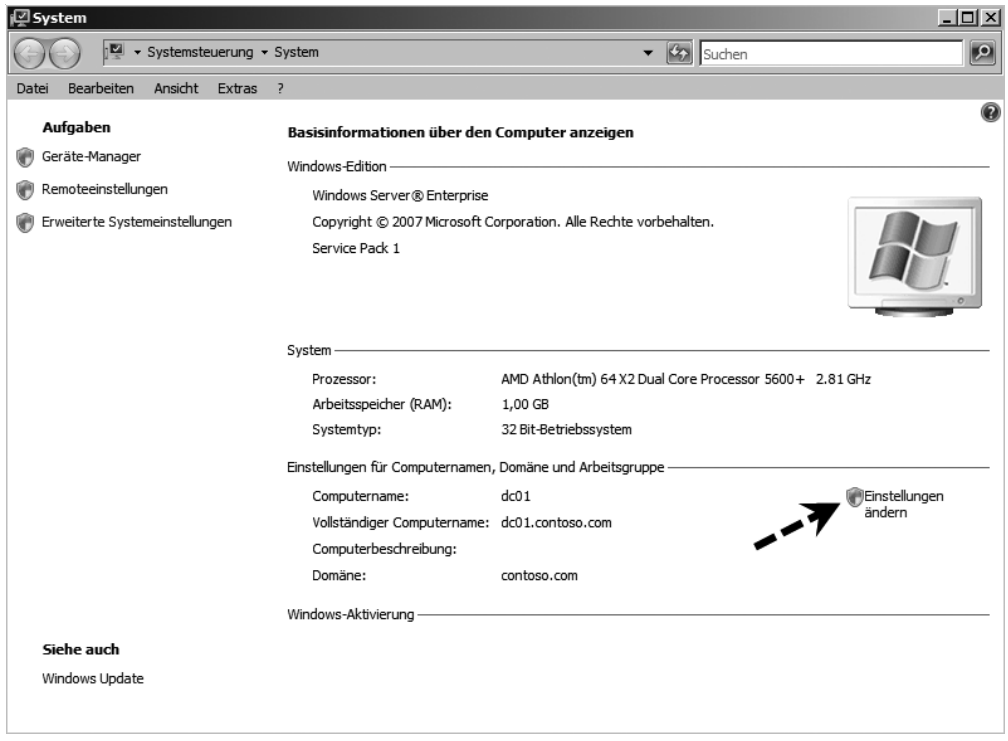


Erstellen eines Computerkontos für den Server in der Domäne

Nachdem Sie die IP-Einstellungen korrekt vorgenommen haben, besteht der nächste Schritt darin, dass Sie für den Server in der Windows-Domäne ein Domänenkonto erstellen. Dieses Konto kann ohne weiteres auch direkt auf dem Windows Server 2008 erstellt werden, es ist dazu lediglich eine Authentifizierung eines Benutzerkontos notwendig, welches berechtigt ist, Computerkonten in der Domäne zu erstellen. Um einen Windows Server 2008-Server in eine Windows-Domäne aufzunehmen, öffnen Sie am besten zunächst das Startmenü, klicken mit der rechten Maustaste auf den Eintrag *Computer* und wählen im daraufhin geöffneten Kontextmenü den Befehl *Eigenschaften* aus. Es öffnet sich ein neues Fenster, über das Sie die Domänenmitgliedschaft des Servers anpassen können. Klicken Sie dazu im Bereich *Einstellungen für Computernamen, Domäne und Arbeitsgruppe* auf den Link *Einstellungen ändern*. Wie Sie sehen, wird neben dieser Einstellung das bekannte Schild in den Windows-Farben anzeigt. Dieses Symbol wird immer angezeigt, wenn für die Ausführung der besagten Aufgabe administrative Berechtigungen benötigt werden. Nachdem Sie diese Meldung

bestätigt haben, werden die Eigenschaften des Computers angezeigt und die Anzeige wechselt automatisch zur Registerkarte *Computername*.

Abbildg. 7.17 Ändern der Domänenmitgliedschaft



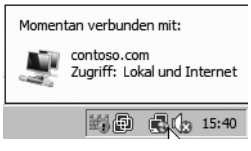
Auf der Registerkarte *Computername* können Sie eine Beschreibung des Servers eintragen, die auch in den Verwaltungswerkzeugen von Active Directory angezeigt wird. Über die Schaltfläche *Ändern* können Sie am effizientesten einer Domäne beitreten oder den Namen des Servers ändern. Wichtig ist an dieser Stelle, dass Sie den Namen der Domäne eingeben, in die der Server aufgenommen wird. Im Anschluss versucht der Server eine Verbindung zu der Domäne aufzubauen. Gelingt dies nicht, erscheint eine Fehlermeldung, die Sie detailliert darüber informiert, warum eine Domänenaufnahme nicht möglich ist. Meistens liegt ein solcher Fehler darin begründet, dass der DNS-Server in den IP-Einstellungen nicht stimmt, oder der Server keine Verbindung zum Domänencontroller herstellen kann, weil der Netzwerkverkehr blockiert wird, oder die IP-Adresse des Servers nicht stimmt. Überprüfen Sie daher an dieser Stelle diese Einträge. Nachdem Ihr Server neu gestartet wurde, erhalten Sie die Meldung, dass Sie die Tastenkombination Strg+Alt+Entf auf der Tastatur drücken müssen, damit das Anmeldefenster erscheint. Erst wenn Sie diese Tastenkombination auf der Tastatur gedrückt haben, erscheint das bekannte Anmeldefenster von Windows Server 2008. Im Anschluss authentifiziert sich der Server an der Domäne und ein ganz neues Benutzerprofil wird erstellt. Wenn Sie sich das nächste Mal am Server anmelden, hat sich der Server die Anmeldung an der Domäne gemerkt und zeigt diese auch in der Anmeldemaske an. An dieser Stelle reicht jetzt die Angabe des Kennwortes, und Sie werden an der Domäne angemeldet. Wenn Sie sich an Ihrem Server lokal anmelden wollen, wählen Sie einfach wieder die Anmeldung am lokalen Server aus.

Abbildg. 7.18 Anmeldemaske von Windows Server 2008

Erste Schritte in der Windows-Domäne

Haben Sie sich an der Domäne angemeldet, können Sie über den bereits beschriebenen Weg die Eigenschaften des Computerkontos aufrufen. Sie erkennen am Server-Namen, dass dieser automatisch mit dem primären DNS-Suffix der Active Directory-Domäne ergänzt wurde. Außerdem sehen Sie auf der Registerkarte *Computername* zusätzlich, welcher Domäne Ihr Server beigetreten ist. Sie können die Domänenmitgliedschaft jederzeit wieder rückgängig machen und aus der Domäne austreten. Dazu können Sie den gleichen Weg verwenden, den Sie bereits zur Aufnahme in die Domäne durchgeführt haben. Im Anschluss daran, können Sie überprüfen ob die Domänen-Benutzergruppen in die lokalen Gruppen des Servers aufgenommen worden sind. Wird ein Server in eine Domäne aufgenommen, wird automatisch die Gruppe *Domänen-Admins* in die lokale Gruppe *Administratoren* aufgenommen. Die Domänen-Benutzergruppe *Domänen-Benutzer* wird in die lokale Gruppe *Benutzer* aufgenommen. Sie können die lokale Benutzerverwaltung über *Start/Ausführen/lusrmgr.msc* aufrufen. Durch die Aufnahme dieser beiden Gruppen wird sichergestellt, dass zum einen die Administratoren der Domäne über administrative Berechtigungen in der Domäne verfügen und die Benutzerkonten der Domäne die Möglichkeit erhalten sich an den einzelnen Arbeitsstationen der Domäne zu authentifizieren. Fahren Sie mit der linken Maustaste über das Netzwerksymbol in der Informationsleiste, wird Ihnen angezeigt, an welcher Domäne der Server angeschlossen ist (Abbildung 7.19).

Abbildg. 7.19 Anzeigen der Netzwerkverbindung in Windows Server 2008

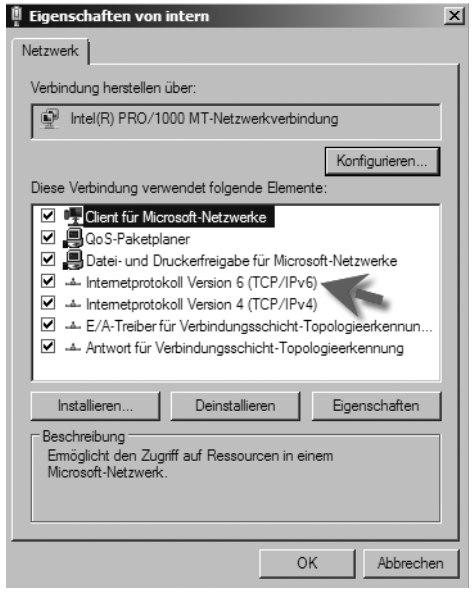


Hier wird Ihnen der DNS-Name der Domäne angezeigt. Wenn Sie das Netzwerk- und Freigabecenter öffnen, wird zum einen die Verbindung zur Domäne angezeigt und zum anderen die Netzwerkverbindung zum Domänennetzwerk erklärt. Rufen Sie auf dem Domänencontroller im Snap-In *Active Directory-Benutzer und -Computer* die Eigenschaften eines Windows Server 2008-Servers auf, können Sie sich auf der Registerkarte *Betriebssystem* auch die Edition anzeigen lassen. Sie können dieses Snap-In auf dem Domänencontroller über *Start/Ausführen/dsa.msc* aufrufen.

Internetprotokoll Version 6 – IPv6

IPv6, das Internet Protocol Version 6, (auch IPnG, Internet Protocol Next Generation) ist der Nachfolger des gegenwärtig im Internet noch überwiegend verwendeten Internet Protocol in der Version 4. Beide Protokolle sind Standards für die Netzwerkschicht des OSI-Modells und regeln die Adressierung und das Routing von Datenpaketen durch ein Netzwerk. Das alte IPv4 bietet einen Adressraum von etwas über 4,3 Milliarden IP-Adressen (2^{32}), mit denen Computer und andere Geräte angesprochen werden können. In den Anfangstagen des Internet, als es nur wenige Rechner gab, die eine IP-Adresse brauchten, galt dies weit mehr als ausreichend. Daher wurde mit den Adressen extrem freizügig umgegangen. So bekam etwa die University of California in Berkeley (UCB) rund 16,8 Millionen IP-Adressen zugewiesen. Viele IPv4-Adressen liegen daher ungenutzt in Datenbanken, können aber durch den immensen Aufwand nicht umstrukturiert werden. Nach neuesten Schätzungen werden spätestens 2012 die IPv4-Adressen vollständig zugewiesen sein. Spätestens zu diesem Zeitpunkt, wahrscheinlich weit vorher, wird sich IPv6 im Markt durchgesetzt haben. Windows Vista und Windows Server 2008 können zwar weiterhin über IPv4 kommunizieren, verwenden als primäres Protokoll aber möglichst IPv6. Die neue Version des IP-Protokolls ist bereits seit 1995 in Entwicklung, als klar wurde, dass die IPv4-Adressen irgendwann ausgehen würden.

Abbildg. 7.20 Windows Server 2008 unterstützt bereits standardmäßig IPv6



Für den Einsatz im internen LAN sind die meisten Switches schon ausgelegt, sodass keine besonderen Vorkehrungen getroffen werden müssen, um die neue Kommunikation zu nutzen. Lediglich zur Kommunikation zwischen Netzwerken müssen Router entsprechend konfiguriert sein.

Vorteile von IPv6 gegenüber IPv4

Eine IPv6-Adresse ist 128 Bit lang (IPv4: 32 Bit). Damit gibt es etwa $3{,}4^{128}$ (340,28 Sextillionen) IPv6-Adressen. IPv6 bietet aber neben der riesigen Anzahl zusätzlicher IP-Adressen auch weitere Vorteile, wie eine deutlich bessere Auto-IP-Konfiguration, die auf Basis der MAC-Adresse durchgeführt wird. In einem IPv6-Netzwerk wird nicht mehr gezwungenermaßen ein DHCPv6-Server benötigt, auch wenn in Windows Server 2008 diese Funktion integriert ist. Weitere Vorteile von IPv6 sind die deutlich erweiterte Paketgröße von bis zu 4 Gigabyte, schnelleres Routing und bessere Unterstützung von IPSec.

Aufbau und Grundlagen von IPv6

IPv6 wurde so entworfen, dass es einfacher als IPv4 zu konfigurieren ist. IPv6-Adressen werden in hexadezimaler Notation mit Doppelpunkten geschrieben, die die Adresse in acht Blöcke mit einer Länge von jeweils 16 Bit unterteilen. Als Trennzeichen dient der Doppelpunkt. Beispiel einer IPv6-Adresse: Die ersten vier Blöcke (64 Bit) werden für das Routing genutzt und bilden das Netz-Präfix. Die weiteren 64 Bit (die letzten vier Blöcke) dienen der Adressierung des Hosts. IPv6 kann sich automatisch selbst konfigurieren, auch ohne DHCPv6 (Dynamic Host Configuration Protocol for IPv6). Nachfolgend einige Beispiele dazu:

fe80::490a:1dba:f2d1:2a65%13

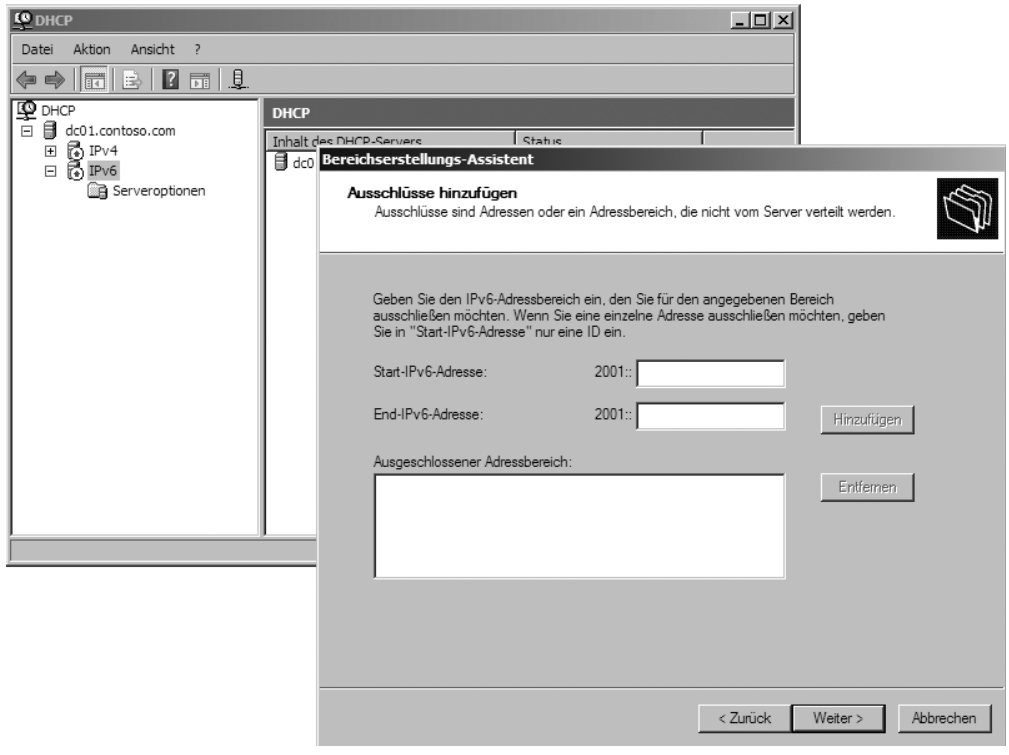
Nullen müssen nicht zwingend dargestellt werden und können durch Doppelpunkte abgekürzt werden. Eine oder mehrere 16-Bit-Gruppen mit dem Wert *0000* können durch zwei aufeinander folgende Doppelpunkte ersetzt werden. So wird über *::1* der lokale Host dargestellt, dessen Adresse richtiger Weise *0000:0000:0000:000:1* heißen müsste. Die entsprechende IPv4-Variante wäre *127.0.0.1*. Werden IPv6-Adressen als URL im Internet Explorer verwendet, kollidieren die Doppelpunkte mit der Bezeichnung des Ports. Aus diesem Grund werden IPv6-Adressen in einem Browser in eckige Klammer gesetzt:

http://[fe80::490a:1dba:f2d1:2a65%13]:80/

Die resultierende Adresse darf höchstens einmal zwei aufeinander folgende Doppelpunkte enthalten. *2001:0db8::1428:57ab* ist gleichbedeutend mit *2001:0db8:0000:0000:0000:0000:1428:57ab* aber *2001::25de::cade* ist nicht korrekt, da nicht nachvollzogen werden kann, wie viele 16-Bit-Gruppen durch die zwei Doppelpunkte jeweils ersetzt wurden. Führende Nullen einer 16-Bit-Gruppe dürfen ausgelassen werden, *2001:db8::28:b* ist gleichbedeutend mit *2001:0db8::0028:000b*. Beim Starten weist sich jede Netzwerkverbindung, die IPv6 unterstützt, eine so genannte Link-lokale Adresse zu, mit der auch eine Kommunikation im Netzwerk stattfinden kann. Diese Adresse beginnt immer mit *fe80::*. Die nächsten drei Blöcke bestehen aus Nullen, sodass diese Link-lokale Adresse richtigerweise *fe80:0000:0000:000* heißen würde, daher die beiden Doppelpunkte am Ende von *fe80*. Diese Adressen können nur zur Kommunikation mit benachbarten Knoten verwendet werden. Sie werden nicht im DNS registriert. Für die zweiten 64 Bit wird die MAC-Adresse des Netzwerk-Interfaces in das Nummerierungssystem EUI-64 (Extended Unique Identifier) des IEEE umgewandelt. Ein Beispiel für diese Adresse ist dann: **fe80::490a:1dba:f2d1:2a65%13.** Bevor ein Client eine IP-Adresse verwen-

det, überprüft er, ob im Netzwerk bereits eine solche vorhanden ist. Diese Möglichkeit ist aber extrem unwahrscheinlich, da durch die Einbeziehung der einzigartigen MAC-Adresse in die IPv6-Adresse schon ein Alleinstellungsmerkmal erreicht wird. Die automatische Konfiguration kann aber keine DNS-Server zuweisen. Sollen diese auch automatisch zugewiesen werden, wird ein DHCPv6-Server benötigt, wie er in Windows Server 2008 integriert ist (Abbildung 7.21).

Abbildg. 7.21 Konfigurieren eines IPv6-Bereiches unter Windows Server 2008



Windows Server 2008 und Windows Vista nutzen IPv6

Windows Server 2008 und Windows Vista nutzen beide den Next Generation TCP/IP-Stack. Hierbei handelt es sich um einen neu überarbeiteten TCP/IP-Protokollstack, in den sowohl IPv4 (Internet Protocol version 4) als auch IPv6 (Internet Protocol version 6) integriert sind. Wenn eine DNS-Abfrage beispielsweise eine IPv6- und IPv4-Adresse zurückgibt, dann versucht der Stack zuerst, über IPv6 zu kommunizieren. Die Bevorzugung von IPv6 gegenüber IPv4 bietet IPv6-fähigen Anwendungen eine bessere Netzwerkkonnektivität. IPv6-Verbindungen sind in der Lage, IPv6-Technologien wie Teredo zu nutzen. Teredo ist eine IPv6-Technologie, die durch ein oder mehrere NATs voneinander getrennte IPv6/IPv4-Knoten eine End-To-End-Kommunikation mit globalen IPv6-Adressen ermöglicht. IPv6-Netzwerkverkehr auf Basis von Teredo kann ein NAT ohne eine Neukonfiguration oder eine Änderung der Anwendungsprotokolle passieren. Teredo ist in Windows XP Service Pack 2 und Windows Server 2003 ab Service Pack 1 enthalten. Teredo ist auf Domänen-

computern aktiviert. Bei Teredo-Netzwerkverkehr handelt es sich um IPv6-Pakete, die in IPv4-UDP-Nachrichten gekapselt wurden. Die standardmäßige Aktivierung von IPv6 und die Bevorzugung von IPv6 haben keine negativen Auswirkungen auf die IPv4-Konnektivität. In Netzwerken, in denen keine IPv6-DNS-Einträge zur Verfügung stehen, wird beispielsweise nicht über IPv6-Adressen kommuniziert. Um die Vorteile einer IPv6-Konnektivität zu nutzen, müssen Netzwerkanwendungen aktualisiert werden. Windows Server 2008 unterstützt bereits nach der Installation das neue IP-Protokoll Version 6 (IPv6). Wenn Sie die Eigenschaften der Netzwerkverbindung anzeigen lassen, sehen Sie das IPv6 automatisch mit den Netzwerkverbindungen verknüpft wird. Wenn Sie einen Server mit Windows Server 2008 für IPv6 konfigurieren, sind folgende automatische Einstellungen möglich:

- Ein IPv6-Host sendet eine Multicast-Nachricht und empfängt eine oder mehrere Router-Nachrichten. In diesen Router-Nachrichten finden sich Subnet-Prefixe (diese nutzt der IPv6-Host zum Festlegen weiterer IPv6-Adressen und zum Hinzufügen von Routen zur IPv6-Routingtabelle) und weitere Konfigurationsparameter (zum Beispiel das Standardgateway).
- Über DHCPv6 erhält der IPv6-Host Subnet-Prefixe und andere Konfigurationsparameter. Oft wird DHCPv6 bei IPv6-Hosts unter Windows zum Beispiel dazu genutzt, die IPv6-Adressen der DNS-Server zu konfigurieren, was über die Routererkennung nicht möglich ist.

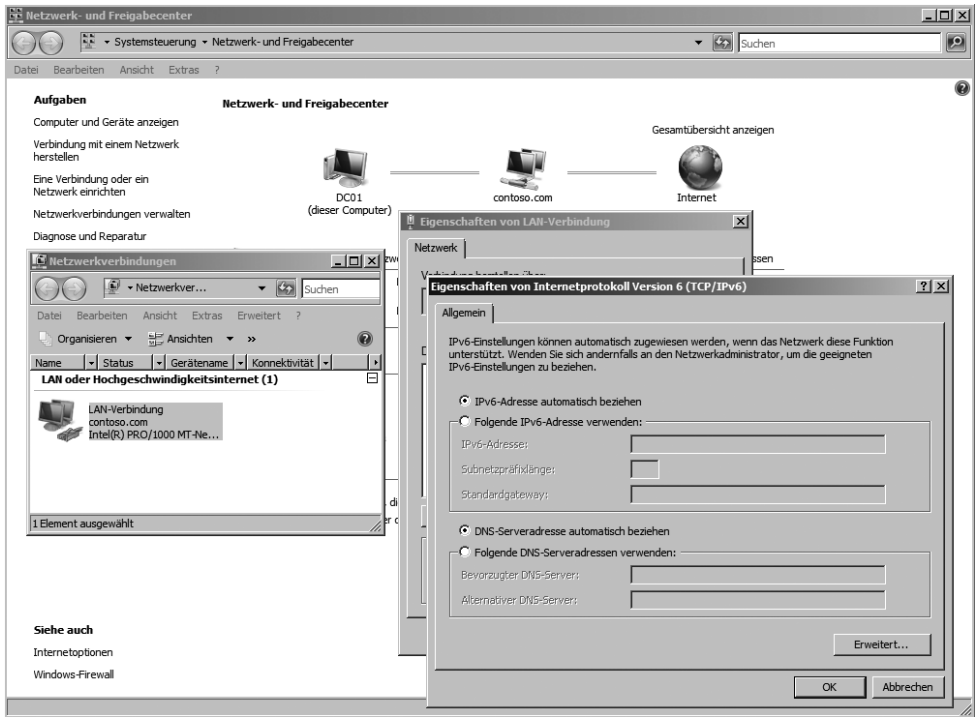
Konfigurieren von IPv6

Neben der automatischen Konfiguration ist auch eine manuelle Konfiguration von IPv6 möglich. Windows Server 2008 stellt dazu eine grafische Oberfläche bereit, unterstützt aber auch die Konfiguration in der Befehlszeile über den Befehl *netsh*. Wenn Sie in den Eigenschaften der Netzwerkverbindung die Eigenschaften von IPv6 aufrufen, können Sie verschiedene Einstellungen vornehmen.

Bei Verwendung einer zufällig abgeleiteten Schnittstellen-ID ist die Chance einer Duplizierung der Link-Local-Adresse äußerst gering. Computer, auf denen Windows Vista oder Windows Server 2008 ausgeführt wird, generieren standardmäßig zufällige Schnittstellen-IDs für nichttemporäre, automatisch konfigurierte IPv6-Adressen. Eine öffentliche IPv6-Adresse ist eine globale Adresse, die im DNS registriert ist und in der Regel von Serveranwendungen für eingehende Verbindungen, beispielsweise einen Webserver, verwendet wird. Sie können dieses Standardverhalten mit dem Befehl *netsh interface ipv6 set global randomizeidentifiers=disabled* deaktivieren. Bei Deaktivierung verwendet IPv6 EUI-64-basierte Schnittstellen-IDs.

- **IPv6-Adresse automatisch beziehen** Hier wird konfiguriert, dass die IPv6-Adressen für diese Verbindung oder diesen Adapter automatisch festgelegt werden.
- **Folgende IPv6-Adresse verwenden** IPv6-Adresse und das Standardgateway für diese Verbindung oder diesen Adapter manuell festlegen.
- **IPv6-Adresse** Hier können Sie eine IPv6-Unicastadresse angeben.
- **Subnetzprefixlänge** Hier können Sie die Länge des Subnetzprefix für die IPv6-Adresse festlegen. Bei IPv6-Unicastadressen sollte dies 64 sein (der Standardwert).
- **Standardgateway** Hier können Sie die IPv6-Unicastadresse des Standardgateways angeben.
- **DNS-Serveradresse automatisch beziehen** Hier wird konfiguriert, dass die IPv6-Adresse des DNS-Servers im Netzwerk über DHCPv6 bezogen wird.

Abbildg. 7.22 Konfiguration von IPv6 in Windows Server 2008



- **Folgende DNS-Serveradressen verwenden** Hier können Sie die Adressen des primären und sekundären DNS-Servers manuell festlegen.

Über die Schaltfläche *Erweitert* kommen Sie, wie bei IPv4, zu weiteren Einstellmöglichkeiten für IPv6. Auf der Registerkarte *IP-Einstellungen* können Sie die IPv6-Adressierung des Servers detaillierter spezifizieren:

- Für jede IPv6-Unicastadresse müssen Sie eine IPv6-Adresse und eine Subnetzprefixlänge angeben. Die Schaltfläche *Hinzufügen* steht nur dann zur Verfügung, wenn die Option *Folgende IPv6-Adresse verwenden* bei den Einstellungen für die IPv6-Adresse gesetzt ist.
- Für jedes Standardgateway müssen Sie eine IPv6-Adresse angeben. Außerdem müssen Sie angeben ob die Metrik für dieses Gateway über die Verbindungsgeschwindigkeit beziehungsweise über die Geschwindigkeit des Adapters ermittelt werden soll oder ob Sie die Metrik selbst festlegen möchten. Die Schaltfläche *Hinzufügen* steht nur dann zur Verfügung, wenn die Option *Folgende IPv6-Adresse verwenden* aktiviert wurde.
- Sie können festlegen, ob eine bestimmte Metrik für die IPv6-Adressen oder die Standardgateways verwendet werden soll oder ob diese über die Verbindungsgeschwindigkeit oder die Geschwindigkeit des Adapters ermittelt werden soll. Die Metrik wird verwendet, wenn mehrere Routen in der Routingtabelle zur Wahl stehen, die der Zieladresse eines weitergeleiteten Pakets entsprechen. Es wird die Route mit der niedrigsten Metrik ausgewählt. Die Metrik kann die Anzahl der Hops, die Geschwindigkeit und Zuverlässigkeit des Pfads, den Pfaddurchsatz oder administrative Eigenschaften widerspiegeln.

- Auf der Registerkarte *DNS* können im Grunde genommen die gleichen Einstellungen vorgenommen werden, wie auf der entsprechenden Karte für IPv4.

Konfigurieren von IPv6 in der Befehlszeile mit *netsh.exe*

Neben der Möglichkeit IPv6 in der grafischen Oberfläche zu konfigurieren, besteht zusätzlich die Möglichkeit die Konfiguration über die Befehlszeile durchzuführen. Für diese Konfiguration wird *netsh.exe* verwendet. Installieren Sie zum Beispiel einen Core-Server, steht die grafische Oberfläche nicht zur Verfügung und Sie können ausschließlich *netsh.exe* verwenden.

Mit dem Befehl *netsh interface ipv6 add address* können Sie IPv6-Adressen konfigurieren. Hierbei gilt die folgende Syntax:

netsh interface ipv6 add address interface=<Schnittstellenname_oder_Index> address=<IPv6_Adresse>/<Länge_Prefix> type=<unicast>|anycast validlifetime=<Zeit>|infinite preferredlifetime=<Zeit>|infinite store=active|persistent

Die einzelnen Optionen haben folgende Bedeutung:

- **interface** Der Name der Verbindung oder des Adapters oder der Index der Schnittstelle
- **address** IPv6-Adresse (optional gefolgt von der Länge des Subnet-Prefix – standardmäßig 64)
- **type** Type der IPv6-Adresse – Unicast (Standard) oder Anycast
- **validlifetime** Die Lebensdauer, für die die Adresse gültig ist. Dieser Zeitraum kann in Tagen, Stunden, Minuten und Sekunden angegeben werden (zum Beispiel 1d2h3m4s). Standardmäßig ist die Lebensdauer unbegrenzt.
- **preferredlifetime** Der Zeitraum, über den die Adresse bevorzugt wird. Er kann in Tagen, Stunden, Minuten und Sekunden angegeben werden (zum Beispiel 1d2h3m4s). Standardwert für diese Einstellung ist *unbegrenzt*.
- **store** Wie die IPv6-Adresse gespeichert werden soll – entweder aktiv (die Adresse wird beim System-Neustart entfernt) oder persistent (die Adresse bleibt beim System-Neustart erhalten, was auch die Standardeinstellung ist)

Mit dem folgenden Befehl können Sie zum Beispiel die IPv6-Unicastadresse *1002:db6::281d:1283::1* für die Schnittstelle *LAN* persistent und mit unbegrenzter Lebensdauer konfigurieren:

netsh interface ipv6 add address "LAN" 1002:db6::281d:1283::1

Mit dem Befehl *netsh interface ipv6 add route* können Sie ein Standardgateway konfigurieren und eine Standardroute (::/0) hinzufügen. Die Syntax dieses Befehls finden Sie im Abschnitt *Erstellen von manuellen Routen für IPv6*. Auch die DNS-Server können für eine IPv6-Verbindung manuell festgelegt werden. Um DNS-Server hinzuzufügen, nutzen Sie den Befehl *netsh interface ipv6 add dnsserver*. Dabei verwenden Sie folgende Syntax: *netsh interface ipv6 add dnsserver interface=<Schnittstellenname> address=<IPv6-Adresse> index=<Reihenfolge>*. Standardmäßig wird der DNS-Server an das Ende der Liste gesetzt. Wenn Sie jedoch hier einen Wert angeben, wird der DNS-Server an die entsprechende Position der Liste gesetzt. Um zum Beispiel einen DNS-Server mit der Adresse *1002:db6::281d:1283::1* und der Schnittstelle LAN hinzuzufügen, verwenden Sie den folgenden Befehl: *netsh interface ipv6 add dnsserver "LAN" 1002:db6::281d:1283::1*

Wie für IPv4 können auch für IPv6 manuelle Routen erstellt werden. Allerdings wird beim Erstellen von manuellen Routen für IPv4 der Befehl *route.exe* verwendet, während für IPv6 der Befehl *netsh* verwendet wird. Der Syntax zur Erstellung einer manuellen Route für IPv6 ist:

netsh interface ipv6 add route prefix=<IPv6-Adresse>/<ganze Zahl> interface=<Zeichenfolge> nexthop=<IPv6-Adresse> siteprefixlength=<ganze Zahl> metric=<ganze Zahl> publish=<Wert> validlifetime=<ganze Zahl>|infinite preferredlifetime=<ganze Zahl> store=<Wert>

Die einzelnen Optionen dieses Befehls haben folgende Funktion:

- **prefix** Adresse oder Subnetzpräfix, für die oder das eine Route hinzugefügt wird
- **interface** Schnittstellenname oder -index
- **nexthop** Gatewayadresse, wenn das Präfix nicht auf Verbindung ist
- **siteprefixlength** Präfixlänge für die ganze Website, falls sie auf Verbindung ist
- **metric** Metrische Route
- **publish** Stellt einen der folgenden Werte dar. Wenn *publish* auf *age* festgelegt wird, enthält die Routenankündigung die verbleibende Gültigkeitsdauer bis zum Löschen. Wenn *publish* auf *yes* festgelegt wird, wird die Route niemals gelöscht, unabhängig vom Wert der Gültigkeitsdauer, und jede Routenankündigung enthält dieselbe angegebene Gültigkeitsdauer. Wenn *publish* auf *no* oder *age* festgelegt wird, wird die Route nach Ablauf der Gültigkeitsdauer gelöscht.
  - **no** Nicht in Routenankündigungen angekündigt (Standard)
  - **age** In Routenankündigungen angekündigt mit sinkender Gültigkeitsdauer
  - **yes** In Routenankündigungen angekündigt mit unveränderter Gültigkeitsdauer
- **validlifetime** Die Gültigkeitsdauer einer Route in Tagen, Stunden, Minuten und Sekunden (zum Beispiel *1d2h3m4s*). Der Standardwert ist *infinite*.
- **preferredlifetime** Die bevorzugte Gültigkeitsdauer der Route. Standardmäßig entspricht dieser Wert der Gültigkeitsdauer.
- **store** Stellt einen der folgenden Werte dar:
  - **active** Änderung wird nur bis zum nächsten Starten beibehalten
  - **persistent** Änderung ist dauerhaft (Standard)

Deaktivieren von IPv6

Unter Windows Server 2008 ist es nicht möglich, IPv6 zu deinstallieren. Sie können IPv6 jedoch deaktivieren:

- Sie können in den Eigenschaften der Netzwerkverbindung das Häkchen bei IPv6 entfernen, um IPv6 zu deaktivieren.
- Alternativ können Sie in der Registry einen neuen DWORD-Wert mit der Bezeichnung *DisabledComponents* und dem Wert *0xFF* erstellen. Erstellen Sie diesen Wert im folgenden Schlüssel: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters*. Durch diese Aktion wird IPv6 für alle LAN-Schnittstellen, deaktiviert.
- Um IPv6 für eine Schnittstelle zu deaktivieren, können Sie auch den Befehl *netsh netio add bindingfilter framing ipv6 fl68 block persistent* verwenden. Um IPv6 wieder zu aktivieren, verwenden Sie den Befehl *netsh netio delete bindingfilter framing ipv6 fl68 persistent*.

Netzwerkdiagnoseframework (NDF)

Um Netzwerkprobleme optimaler untersuchen zu können, bringt Windows Server 2008 das *Netzwerkdiagnoseframework (Network Diagnostics Framework, NDF)* mit. Mit dem NDF lassen sich Probleme innerhalb der Anwendung untersuchen, die gerade im Einsatz war, als das Problem auftrat. Als Teil der übergeordneten *Windows-Diagnoseinfrastruktur (Windows Diagnostics Infrastructure, WDI)* sorgt es dafür, dass die Ursachen für Netzwerkprobleme schneller und zielgenauer beseitigt werden können. Während der Diagnose analysiert das NDF, warum die Aufgabe fehlgeschlagen ist, und zeigt eine Lösung oder mögliche Ursachen für das Problem an. Die Problemlösung kann möglicherweise automatisch ausgeführt werden. Es kann jedoch auch sein, dass der Benutzer eine von mehreren möglichen Lösungen auswählen oder bestimmte Schritte selbst durchführen muss. Bei TCP/IP-basierter Kommunikation fordert das Netzwerkdiagnose-Framework den Benutzer über verschiedene Optionen auf, mögliche Ursachen zu entfernen, bis die zu Grunde liegende Ursache des Problems identifiziert oder sämtliche möglichen Ursachen ausgeräumt sind. Folgende Probleme im Zusammenhang mit TCP/IP können vom Netzwerkdiagnose-Framework diagnostiziert werden:

- Falsche IP-Adressen
- Standardgateway (Router) ist nicht verfügbar
- Falscher Standardgateway
- Namensauflösungsfehler bei NetBIOS (Network Basic Input/Output System) über TCP/IP (NetBT)
- Falsche DNS-Einstellungen
- Lokaler Port wird bereits verwendet
- DHCP-Clientdienst wird nicht ausgeführt
- Kein Remotelistener
- Medium ist nicht verbunden
- Der lokale Port ist gesperrt
- Unzureichender Speicher

Zusammenfassung

Nachdem wir Ihnen gezeigt haben, wie Windows Server 2008 im Netzwerk betrieben wird und mit welchen Tricks Sie den Server optimal im Netzwerk betreiben, gehen wir im nächsten Kapitel ausführlich darauf ein, wie Sie mit Windows Server 2008 ein Active Directory betreiben. Gerade in diesem Bereich stecken viele neue Funktionen, die wir im folgenden Kapitel 8 ausführlich erläutern werden.

Kapitel 8

Active Directory im Praxiseinsatz

In diesem Kapitel:

Ein wichtiger Bestandteil von Windows Server 2008 sind die Active Directory-Funktionen. Microsoft hat in diesem Bereich zwar einiges geändert, aber viele bekannte Funktionen sind noch identisch mit Windows Server 2003. In diesem Kapitel gehen wir auf die neuen AD-Funktionen im Praxiseinsatz mit Windows Server 2008 ein. Die Funktion eines Domänencontrollers wird in Windows Server 2008 durch die neuen *Active Directory-Domänendienste* dargestellt. Zusätzlich empfehlen wir Ihnen das Buch *Active Directory – Das Praxisbuch für Windows Server 2008*. In diesem Buch gehen wir ausführlicher auf die einzelnen Bereiche von Active Directory in Windows Server 2008 ein.

Neuerungen in Active Directory

Windows Server 2008 bringt einige Änderungen in der Verwaltung eines Active Directory mit. Die generelle Verwaltung und Funktionen von Active Directory sind noch weitgehend identisch mit Windows Server 2003. Die Funktionen wurden integriert, die im folgenden Abschnitt besprochen werden.

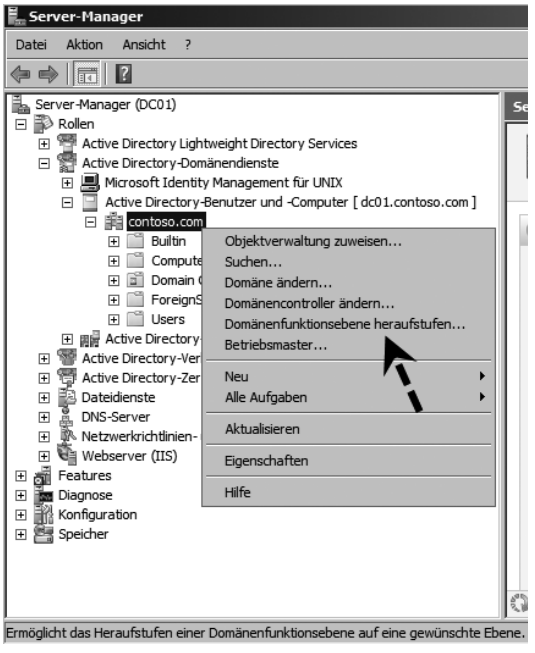
Richtlinien für Kennwörter

Unter Windows Server 2003 konnte in einer Domäne nur eine einzige Richtlinie für Kennwörter existieren, die als Gruppenrichtlinie direkt dem Domänenobjekt zugewiesen werden musste. Unter Windows Server 2008 können jetzt mehrere Richtlinien für Kennwörter definiert werden, sodass sich besonders sensiblen Bereichen des Unternehmens komplexere Kennwörter zuweisen lassen als anderen. Diese Funktion steht aber nur zur Verfügung, wenn Sie die Domäne in den Funktionsmodus *Windows Server 2008* versetzen. Die Domänenfunktionsebene können Sie über den Server-Manager heraufsetzen, indem Sie die Domäne im Snap-In *Active Directory-Benutzer und -Computer* mit der rechten Maustaste anklicken (Abbildung 8.1). Haben Sie während der Installation für die Gesamtstruktur die Funktionsebene *Windows Server 2008* ausgewählt, sind die Domänen ebenfalls automatisch in diesem Modus. Kennwortrichtlinien können Sie jetzt einzelnen OUs zuweisen. Microsoft hat für diese Funktion zwei neue Objekt-Klassen in das Schema von Active Directory eingeführt:

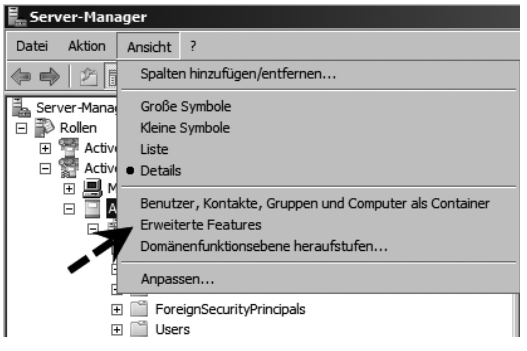
- Password Settings Container
- Password Settings

Ebenfalls wichtig für diese neue Funktion ist die OU *Passwort Setting Container*, der unterhalb der OU *System* im Snap-In *Active Directory-Benutzer und -Computer* angezeigt wird (Abbildung 8.3). Damit diese Objekte angezeigt werden, müssen Sie für das Snap-In zunächst die Ansicht der erweiterten Funktionen aktivieren. Klicken Sie dazu im Server-Manager auf das Snap-In *Active Directory-Benutzer und -Computer*, und rufen Sie den Menübefehl *Ansicht/Erweiterte Features* auf (Abbildung 8.2).

Abbildg. 8.1 Konfigurieren der Domänenfunktionsebene



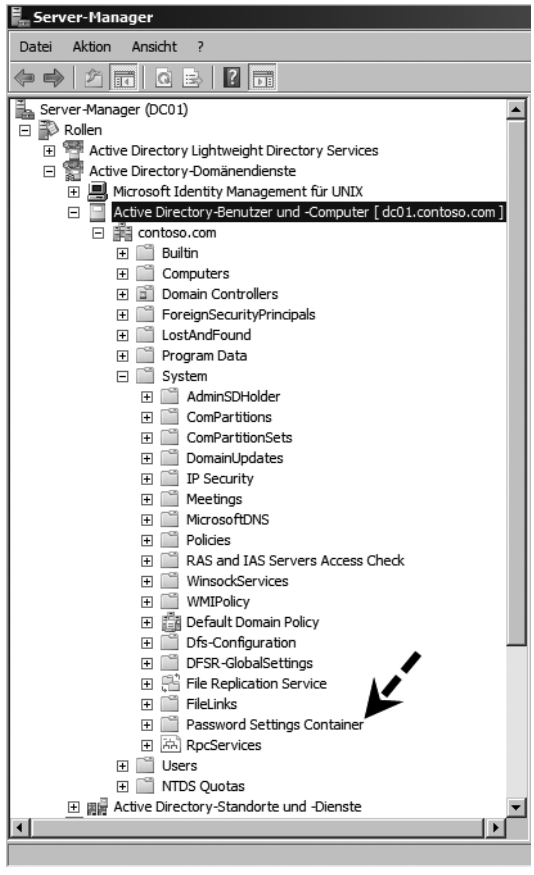
Abbildg. 8.2 Aktivieren der erweiterten Features für das Snap-In *Active Directory-Benutzer und -Computer*



Nachdem Sie die erweiterten Funktionen aktiviert haben, werden im Snap-In *Active Directory-Benutzer und -Computer* deutlich mehr OUs angezeigt, die standardmäßig ausgeblendet werden, darunter auch der Container *Passwort Settings Container*. In dieser OU werden nach Erstellung die *Passwort Settings Objects (PSO)* gespeichert. Eine PSO enthält alle notwendigen Einstellungen zur Konfiguration von Kennwortrichtlinien.

TIPP Eine sehr gute grafische Oberfläche für die Verwaltung von Kennwortrichtlinien finden Sie auf der Seite *http://www.specopssoft.com*. Das Freeware-Tool *Specops Password Policy BASIC* ermöglicht die effizientere Verwaltung mehrerer Kennwortrichtlinien. Auf der Seite gibt es darüber hinaus noch weitere, allerdings kostenpflichtige Tools.

Abbildg. 8.3 Anzeigen der OU *Password Settings Container*



Schreibgeschützte Domänencontroller

Eine weitere Neuerung sind die schreibgeschützten Domänencontroller (Read-Only Domain Controller, RODC). Diese Domänencontroller erhalten die replizierten Informationen von den normalen Domänencontrollern und nehmen selbst keine Änderungen entgegen. Durch diese neue Funktion können auch Domänencontroller in kleineren Niederlassungen betrieben werden, ohne dass das Sicherheitskonzept eines Unternehmens beeinträchtigt wird, weil die Domänencontroller in den Niederlassungen nicht so geschützt sind wie die in der Zentrale und dadurch sehr leicht kompromittiert werden können. Ein RODC schützt ein Active Directory davor, dass Kennwörter ausspioniert werden können. Ein RODC kennt zwar alle Objekte im Active Directory, speichert aber nur die Kennwörter der Benutzer, die Sie explizit festlegen. Wird ein solcher Domänencontroller gestohlen und versucht ein Angreifer die Kennwörter aus der Datenbank des Controllers auszulesen, sind die Konten der restlichen Domäne geschützt.

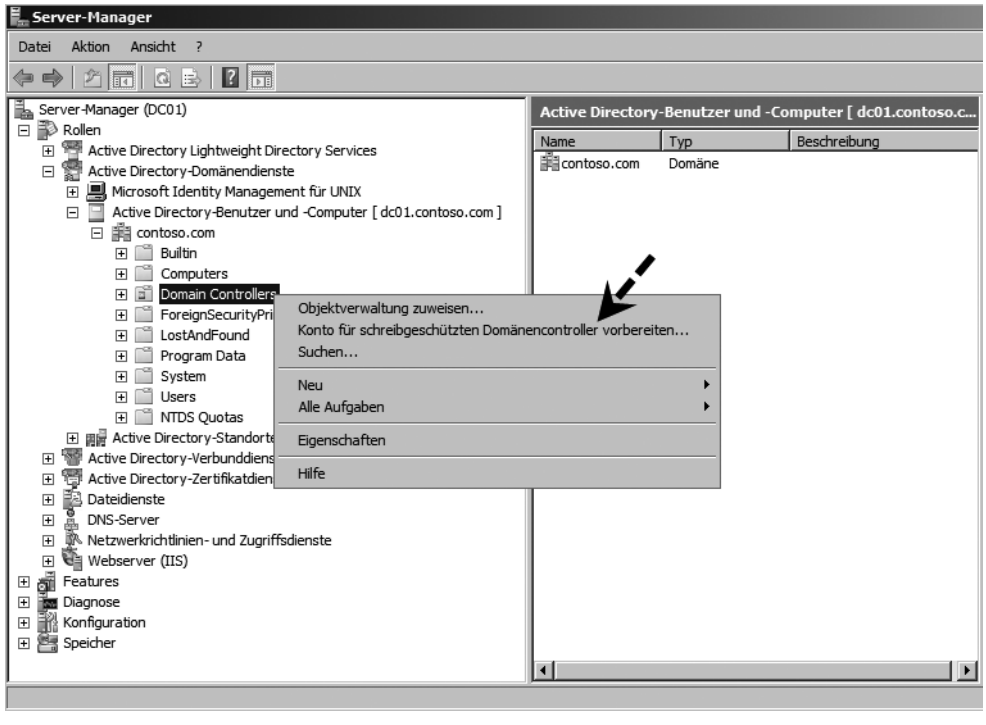
Während der Heraufstufung eines Domänencontrollers können Sie diesen zum RODC deklarieren. In diesem Fall repliziert sich der Domänencontroller von anderen Domänencontrollern, gibt aber selbst keine Änderungen weiter. Damit Sie diese Funktion nutzen können, muss der PDC-Emulator

der Domäne auf einem Windows Server 2008 installiert sein. Ein RODC nimmt keinerlei Änderungen an der Datenbank von Active Directory an. Lesender Zugriff wird allerdings gestattet. Schreibende Domänencontroller richten keine Replikationsverbindung zu RODCs ein, da eine Replikation nur von normalen DCs zu RODCs erfolgen kann. RODCs richten Replikationsverbindungen zu den schreibenden Domänencontrollern ein, die Sie bei der Heraufstufung angeben.

HINWEIS Verwenden Sie schreibgeschützte Domänencontroller (Read-Only Domain Controller, RODC), sollten Sie den Befehl *adprep /rodcprep* auf dem Schema-Master der Gesamtstruktur ausführen. Vor allem wenn Sie in der Gesamtstruktur noch Windows Server 2003-DCs ausführen, ist dieser Befehl notwendig. Außerdem muss sich die Gesamtstruktur mindestens im Windows Server 2003-Modus befinden. Sie finden *adprep* auf der Windows Server 2008-DVD im Verzeichnis *\sources\adprep*.

Die Replikation zwischen Windows Server 2003-DCs und RODCs ist allerdings weniger zuverlässig und funktional, wie die Replikation zwischen Windows Server 2008-DCs und RODCs. Aus diesem Grund sollte die Replikation zu einem RODC am besten immer über einen Windows Server 2008-DC abgewickelt werden. Nur so ist sichergestellt, dass die Domänen-Partition repliziert werden kann. In jedem Fall muss es in der Gesamtstruktur mindestens einen vollwertigen Windows Server 2008-DC geben.

Abbildg. 8.4 Vorbereiten eines Computerkontos für einen neuen RODC



Klicken Sie im Snap-In *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf die OU *Domain Controllers*, können Sie die Option *Konto für schreibgeschützten Domänencontroller vorbereiten* auswählen. In diesem Fall führen Sie in der Zentrale den Assistent zum Erstellen eines

neuen Domänencontrollers aus und weisen diesem ein Computerkonto zu. In der Niederlassung kann anschließend ein Administrator diesen Server installieren. Der Server bekommt automatisch die Funktion des RODCs zugewiesen. Auch wenn diese Rolle ähnliche Funktionen hat, wie ein Backup-Domänencontroller (BDC) unter Windows NT 4.0, hat diese nichts mit dieser alten Funktion gemeinsam, sondern ist eine komplette Neuentwicklung.

Bei einem BDC unter Windows NT 4.0 wurden die Benutzernamen und Kennwörter zusätzlich gespeichert, um Anmeldungen zu ermöglichen. Ein RODC bietet ein vollständiges Active Directory, allerdings ohne gespeicherte Kennwörter. Dieses Verzeichnis auf dem RODC ist, wie der Name schon sagt, Read-Only, also nur lesbar. Zwar kann auch ein RODC Kennwörter speichern, aber nur genau diejenigen, die ein Administrator angibt. Bei der Verwendung von RODCs werden folgende Abläufe beim Anmelden eines Benutzers abgewickelt:

1. Ein Anwender meldet sich am Standort des RODC an.
2. Der RODC überprüft, ob das Kennwort des Anwenders auf den Server repliziert wurde. Wenn ja, wird der Anwender angemeldet.
3. Ist das Kennwort nicht auf dem RODC verfügbar, wird die Anmeldeanfrage an einen vollwertigen DC weitergeleitet.
4. Wird die Anmeldung erfolgreich durchgeführt, wird dem RODC ein Kerberosticket zugewiesen.
5. Der RODC stellt dem Anwender jetzt noch ein eigenes Kerberosticket aus, mit dem dieser Anwender arbeitet. Gruppenmitgliedschaften und Gruppenrichtlinien werden übrigens nicht über die WAN-Leitung gesendet. Diese Informationen werden auf dem RODC gespeichert.
6. Als Nächstes versucht der RODC das Kennwort dieses Anwenders in seine Datenbank von einem vollwertigen DC zu replizieren. Ob das gelingt oder nicht, hängt von der jeweiligen Gruppenmitgliedschaft ab, die wir noch ausführlich in diesem Kapitel beschreiben.
7. Bei der nächsten Anmeldung dieses Anwenders beginnt dieser Prozess von vorne.

HINWEIS Die Kennwörter von Administratorkonten in Active Directory werden in keinem Fall auf einem schreibgeschützten Domänencontroller gespeichert. Diese Kennwörter sind durch ihre Wichtigkeit von der möglichen Replikation zum schreibgeschützten Domänencontroller ausgeschlossen. Geht die WAN-Verbindung in der Niederlassung mit dem RODC zu einem normalen DC verloren, findet keine Anmeldung mehr an der Domäne statt. Der RODC verhält sich dann wie ein normaler Mitgliedsserver, es ist nur die lokale Anmeldung am Server möglich.

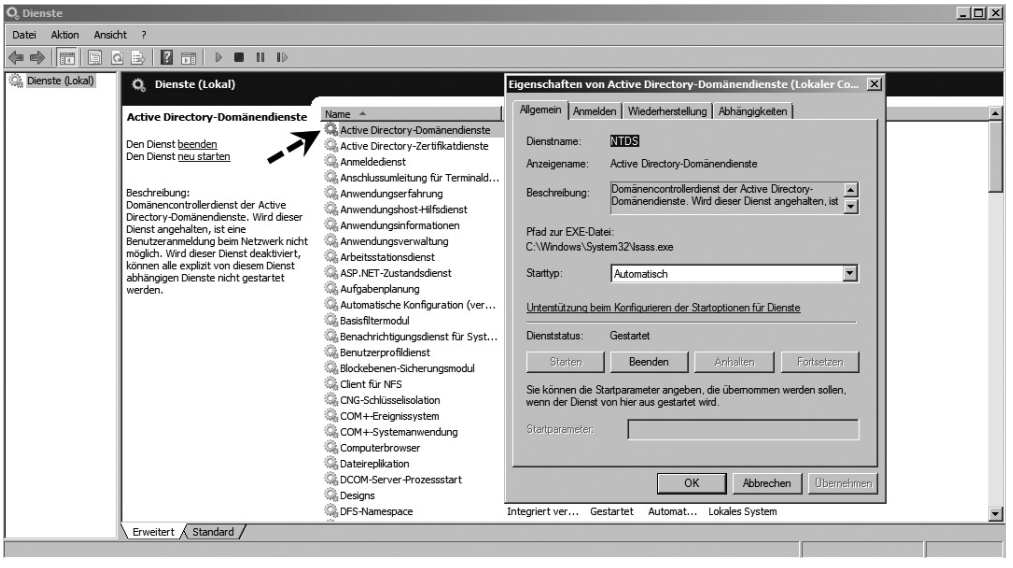
Read-Only DNS

Installieren Sie auf einem RODC den DNS-Dienst, wird dieser Server zum Read-Only DNS-Server. Hier gelten die gleichen Einschränkungen für einen RODC. Ein Read-Only DNS nimmt nur Änderungen von normalen DNS-Servern entgegen und akzeptiert selbst keine Änderungen. Ein Read-Only DNS steht für Benutzer als normaler DNS-Server für Abfragen zur Verfügung, unterstützt aber keine dynamische DNS-Registrierung. Versucht sich ein Client zu registrieren, erhält er vom DNS-Server eine Rückinfo, dass keine Aktualisierung akzeptiert wird. Im Hintergrund kann der Client versuchen, sich an einem normalen DNS-Server zu registrieren, der die Änderungen dann wieder zum Read-Only DNS-Server repliziert.

Active Directory-Dienst manuell starten und stoppen

Unter Windows Server 2008 ist es jetzt möglich, den Dienst für Active Directory im laufenden Betrieb zu stoppen und wieder zu starten. Unter Windows Server 2003 war das noch nicht möglich, sondern der Server musste explizit heruntergefahren werden. Durch diese Funktion kann das Active Directory auf einem Server auch neu gestartet werden, während die anderen Dienste des Servers weiter funktionieren. Dies kann zum Beispiel für die Offlinedefragmentation der Active Directory-Datenbank sinnvoll sein oder für die Installation von Updates. Sie finden den dazugehörigen Systemdienst *Active Directory-Domänendienste* in der Dienstesteuerung. Diese können Sie ausführen, wenn Sie *services.msc* im Suchfeld des Startmenüs eingeben. Der Dienst kann auch, wie alle anderen Dienste, über die Befehlszeile mit *net stop* gestoppt und mit *net start* wieder gestartet werden.

Abbildg. 8.5 Manuelles Starten und Beenden des Systemdienstes für das Active Directory



Active Directory Snapshot-Viewer

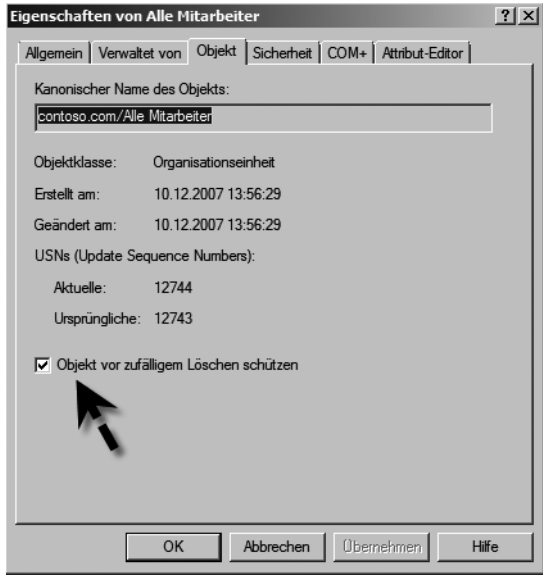
Mit dem neuen Active Directory Snapshot-Viewer können versehentlich gelöschte Objekte der Domäne angezeigt werden. Sie können mit dieser Funktion zwar keine Objekte wiederherstellen, erkennen aber, welche Objekte versehentlich gelöscht worden sind. Dazu kann unter Windows Server 2008 ein Snapshot von Active Directory durchgeführt und mit dem Snapshot-Viewer dieses auf gelöschte Objekte untersucht werden. Um diese Funktion nutzen zu können, gehen Sie folgendermaßen vor:

1. Sie erstellen eine Aufgabe, die mit Hilfe von *ntdsutil.exe* regelmäßig Snapshots des ADs erstellt.
2. Über *ntdsutil.exe* können Sie sich alle Snapshots anzeigen lassen.
3. Mit dem Befehl *dsamain.exe* können Sie ein Snapshot als LDAP-Server bereitstellen.
4. Jetzt können Sie mit *ldp.exe* den Snapshot genauso untersuchen, wie einen normalen Online-Domänencontroller.

Versehentliches Löschen von Objekten in Active Directory verhindern

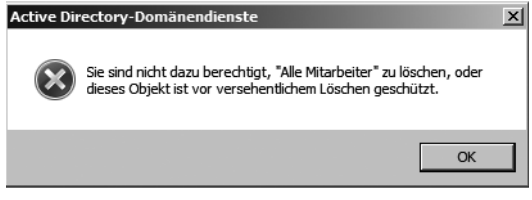
In Windows Server 2008 sind Active Directory-Objekte davor geschützt, versehentlich gelöscht zu werden. Dieser Schutz ist standardmäßig aktiviert. Nachdem die erweiterte Ansicht im Menü *Ansicht* aktiviert wurde, finden Sie auf der Registerkarte *Objekt* das Kontrollkästchen *Objekt vor zufälligem Löschen schützen* (Abbildung 8.6).

Abbildg. 8.6 In Windows Server 2008 sind Active Directory-Objekte vor dem versehentlichen Löschen geschützt



Durch diese Option werden die Berechtigungen auf der Registerkarte *Sicherheit* gesteuert. Der Gruppe *Jeder* wird der Eintrag *Löschen* verweigert. Das äußert sich darin, dass ein Administrator vor dem Löschen eines solchen geschützten Objektes das Kontrollkästchen zunächst deaktivieren muss, bevor das Objekt gelöscht werden kann. Bleibt das Kontrollkästchen aktiviert, erhalten auch Administratoren eine Fehlermeldung, dass der Zugriff verweigert wird (Abbildung 8.7).

Abbildg. 8.7 Geschützte Objekte in Active Directory können auch durch Administratoren nicht gelöscht werden



Kompatibilität mit Windows 2000/2003/XP

Ein Windows Server 2008-Computer kann Mitglied einer Windows 2000- oder einer Windows Server 2003-Domäne werden. Windows Server 2003- und Windows 2000 Server-Computer können Mitglied einer Windows Server 2008-Domäne werden. In diesem Bereich ist daher die Kompatibilität sichergestellt.

TIPP Windows Server 2003-Domänencontroller können direkt auf Windows Server 2008 aktualisiert werden. In diesem Fall kann es unter Umständen passieren, dass der Systemdienst *Netlogon* nicht mehr startet. Um diesen Fehler zu beheben, geben Sie die beiden folgenden Befehle ein:

1. *sc config netlogon depend= lanmanworkstation/lanmanserver*
2. *net start netlogon*

Windows XP- und Windows 2000 Professional-Arbeitsstationen können problemlos Mitglied einer Domäne mit Windows Server 2008 sein. Empfohlen wird allerdings, möglichst auf Windows Vista umzusteigen, da erst im Zusammenspiel Windows Server 2008/Windows Vista alle Funktionen voll genutzt werden können (siehe auch die Kapitel 1, 15 und 24). Windows Server 2008 kann auch als Domänencontroller in einer Windows 2000- oder Windows Server 2003-Domäne dienen. Die neuen Funktionen von Windows Server 2008 können allerdings nur dann genutzt werden, wenn alle Domänencontroller unter Windows Server 2008 laufen. Ein Beispiel hierfür ist der Read-Only Domänencontroller. Damit diese Funktion unterstützt wird, muss der PDC-Emulator auf einen Domänencontroller unter Windows Server 2008 verlegt werden. Windows Server 2008 unterstützt zwar prinzipiell noch Windows NT 4.0-Mitgliedsserver, es werden aber keine NT 4.0-BDCs unterstützt. Wollen Sie einen Windows Server 2008-Domänencontroller in ein Windows Server 2003-Active Directory integrieren, müssen Sie dieses Active Directory zunächst auf Windows Server 2008 vorbereiten. Gehen Sie dazu folgendermaßen vor:

1. Melden Sie sich mit einem Benutzerkonto an, das Mitglied der Gruppen *Organisations-Administratoren, Schema-Admins* und *Domänen-Admins* der Stammdomäne ist.
2. Kopieren Sie den Inhalt des Verzeichnisses *\sources\adprep* von der Windows Server 2008-DVD auf den Domänencontroller, der die Rolle des Schemamasters verwaltet.
3. Öffnen Sie auf dem Server eine Befehlszeile und navigieren Sie in das Verzeichnis, in das Sie *adprep* kopiert haben. Geben Sie den Befehl *adprep /forestprep* ein.
4. Wollen Sie auch schreibgeschützte Domänencontroller (Read-Only Domain Controller, RODC) installieren, geben Sie noch den Befehl *adprep /rodcprep* ein.

Im Anschluss müssen Sie auch die Domänen vorbereiten, in denen Sie Domänencontroller unter Windows Server 2008 installieren wollen. Kopieren Sie dazu wieder den Inhalt des Verzeichnisses *sources\adprep*, aber dieses Mal auf den Domänencontroller mit der Infrastrukturmaster-Rolle.

1. Öffnen Sie auf dem Server eine Befehlszeile, navigieren Sie zum Verzeichnis, in das Sie *adprep* kopiert haben, und geben Sie den Befehl *adprep /domainprep /gpprep* ein.
2. Stellen Sie sicher, dass sich die Domänencontroller replizieren.

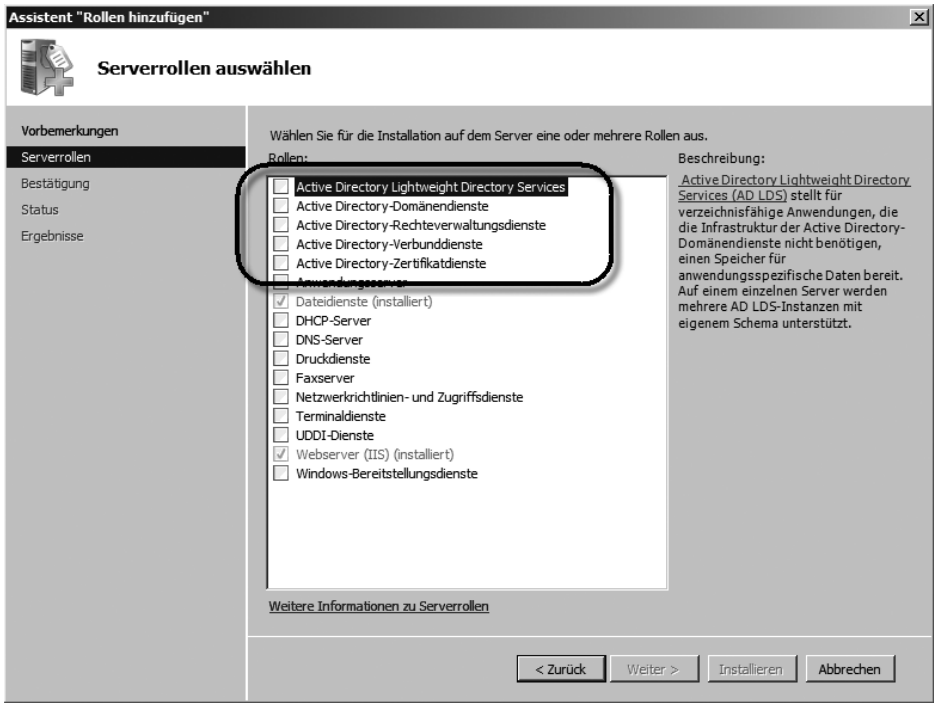
HINWEIS Ausführliche Informationen über das Tool *adprep* finden Sie auf der Internetseite *http://go.microsoft.com/fwlink/?LinkID=50439*.

Verschiedene Rollen für Active Directory

Im Kapitel 3 haben wir Ihnen gezeigt, welche Rollen und Features Sie unter Windows Server 2008 aktivieren können. Bezüglich von Active Directory, kann ein Windows Server 2008 verschiedene Rollen einnehmen, die Sie im Server-Manager anzeigen können (Abbildung 8.8).

- **Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS)** Diese Rolle ersetzt die Zertifikatdienste unter Windows Server 2003. Sie können mit dieser Rolle eine Public Key Infrastructure (PKI) aufbauen (siehe Kapitel 17).
- **Active Directory-Domänendienste (Active Directory Domain Services, AD DS)** Hierbei handelt es sich um die Rolle eines Domänencontrollers für das Active Directory. Bevor Sie einen Server zum Domänencontroller für das Active Directory heraufstufen können, muss diese Rolle installiert sein.
- **Active Directory-Verbunddienste (Active Directory Federation Services, AD FS)** Mit den AD FS können Sie eine webbasierte Single Sign-On (SSO)-Infrastruktur aufbauen (siehe Kapitel 17).
- **Active Directory Lightweight Directory Services (AD LDS)** Mit diesen Diensten können Applikationen, welche Informationen in einem Verzeichnis speichern, arbeiten. Im Gegensatz zu den Active Directory Domain Services, wird das Verzeichnis nicht als Dienst ausgeführt. Diese Dienste benötigen keinen reinen Domänencontroller. Auf einem Server können mehrere Instanzen laufen. Bei den AD LDS handelt es sich sozusagen um ein Mini-Active Directory ohne große Verwaltungsfunktionen. Unter Windows Server 2003 wurden diese Dienste noch Active Directory Application Mode (ADAM) genannt (siehe Kapitel 17).

Abbildg. 8.8 Active Directory-Rollen unter Windows Server 2008



- **Active Directory-Rechteverwaltungsdienste (Active Directory Rights Management Services, AD RMS)** Mit dieser Technologie werden Daten mit digitalen Signaturen versehen, um sie vor einem unerwünschten Zugriff zu sichern. Besitzer von Dateien können basierend auf Benutzerinformationen exakt festlegen, was andere Benutzer mit den Dateien machen dürfen. Dokumente können zum Beispiel als »Nur Lesen« konfiguriert werden (siehe Kapitel 17).

Aufbau und Grundlagen von Active Directory

Wenn Sie mit Active Directory arbeiten, ist das Wissen über einzelne wichtige Begriffe und die Grundstruktur unerlässlich. Im folgenden Abschnitt gehen wir daher kurz auf die Theorie hinter Active Directory ein. Dieses theoretische Wissen wird sowohl für den Aufbau als auch für die Verwaltung oder die Fehlerbehebung benötigt.

Protokolle für Active Directory

Alle Verzeichnisdienste, auch das Active Directory, arbeiten nach Standards. Innerhalb dieser Standards wurden Protokolle und technische Begriffe definiert, die auch zur Planung eines Active Directory notwendig sind.

X.500

Außer dem Begriff *Verzeichnis* sollten Sie auch die beiden Begriffe *X.500* und *LDAP* kennen. Wenn Sie ein Active Directory planen oder administrieren, werden Sie ständig auf diese beiden Begriffe stoßen. X.500 beschreibt einen Standard, wie Verzeichnisse aufgebaut sein müssen. Damit ein Verzeichnis, oft auch *Verzeichnisdienst* genannt, funktioniert und global Zugriffe erfolgen können, ist es extrem wichtig, einen gemeinsamen Standard zu verwenden, der den Aufbau des Verzeichnisdienstes vorgibt. Das Active Directory arbeitet nach dem X.500-Standard. Hierüber finden Sie genauere Informationen unter *http://verzeichnisdienst.de*. X.500 gibt vor, wie das Verzeichnis aufgebaut sein muss. Alle Verzeichnisse, die sich nach dem X.500-Standard richten, sind in etwa gleich aufgebaut, und zwar hierarchisch in einer Baumstruktur. Aus diesem Grund werden die einzelnen Komponenten eines solchen Verzeichnisses oft mit Bezeichnungen belegt, die mit Bäumen zu tun haben. Man liest von der bereits erwähnten Baumstruktur, welche die Verästelung der Datenbank verdeutlichen soll. Es gibt Äste und es gibt Blätter. Auch Microsoft verwendet im Active Directory Begriffe wie *Forest (Gesamtstruktur)* und *Tree* (*Struktur*). Auch der Begriff *Stamm* (im Englischen *Root* genannt) wird verwendet. Die Root ist die Grundlage, die Basis eines Verzeichnisses. Wenn Sie im Zusammenhang mit Active Directory von einer Root-Domäne lesen, ist damit die Ursprungsdomäne von Active Directory gemeint. Hierbei handelt es sich um die erste installierte Domäne in einem Active Directory. Ein Verzeichnis wird meistens durch mehrere Server verwaltet. Diese Verwaltung übernehmen im Active Directory die Domänencontroller. Da das Active Directory recht kompliziert aufgebaut sein kann, können einzelne Domänencontroller für verschiedene Bereiche von Active Directory zuständig sein. Diese untergliederten Bereiche in Verzeichnisdiensten wie dem Active Directory werden *Partitionen* genannt. Ein Active Directory kann aus mehreren Domänen bestehen. Jede dieser Domänen hat eigene Domänencontroller und ist eine eigene Partition.

Lightweight Directory Access Protocol (LDAP)

Außer einem Standard, wie der Verzeichnisdienst aufgebaut sein muss, muss es auch Netzwerkprotokolle geben, die definieren, wie auf ein solches Verzeichnis zugegriffen werden kann. LDAP regelt die Abfrage von Verzeichnisdiensten. Auch Active Directory arbeitet mit LDAP. Der Zugriff auf Verzeichnisdienste ist ebenfalls im X.500-Standard definiert.

Das Schema eines Verzeichnisdienstes

Die Struktur eines Verzeichnisses wird *Schema* genannt. In einem Schema ist genau definiert, welche Informationen auf welche Art gespeichert werden sollen. Jede relationale Datenbank hat ein solches Schema. Da ein Verzeichnisdienst wie Active Directory möglichst viele Informationen speichern soll, ist es unerlässlich, dass definiert wird, welche Informationen wo im Verzeichnis gespeichert werden können. Es muss festgelegt werden, ob manche Informationen zwingend eingegeben werden müssen und ob andere Informationen nur optional sind. Sie können sich Active Directory als große leere Lagerhalle vorstellen. Damit diese gefüllt werden kann, muss es Regale (Regeln) und Anweisungen (Definitionen) geben, wo Waren gelagert werden sollen und wie die Arbeitsprozesse für diese Lagerung definiert sind. Das Active Directory speichert die Daten, das Schema definiert, wie sie gespeichert werden. Der Aufbau des Schemas ist recht einfach. Es gibt *Objekte* und es gibt *Attribute*. Die *Attribute* sind *Objekten* zugeordnet. Jeder Verzeichniseintrag ist ein *Objekt*. Am Beispiel von Active Directorys sind Objekte also *Benutzer, Computer, Freigaben* oder *Drucker*. Das Active Directory verfügt über ein erweiterbares Schema. Dieses gibt die Möglichkeit, flexibel zusätzliche Informationen im Verzeichnis zu speichern. Dadurch können neue Anwendungen wie zum Beispiel der Exchange Server ihre speziellen Informationen im Verzeichnis ablegen. Jeder Benutzer, jeder Computer und Drucker ist ein Objekt. Die Informationen, die für einzelne Benutzer hinterlegt werden können, zum Beispiel Vornamen, Nachnamen, Anmeldenamen, Telefonnummer usw., werden als *Attribute* bezeichnet. Das Schema definiert genau, welche Objekte mit welchen Attributen im Active Directory angelegt werden können.

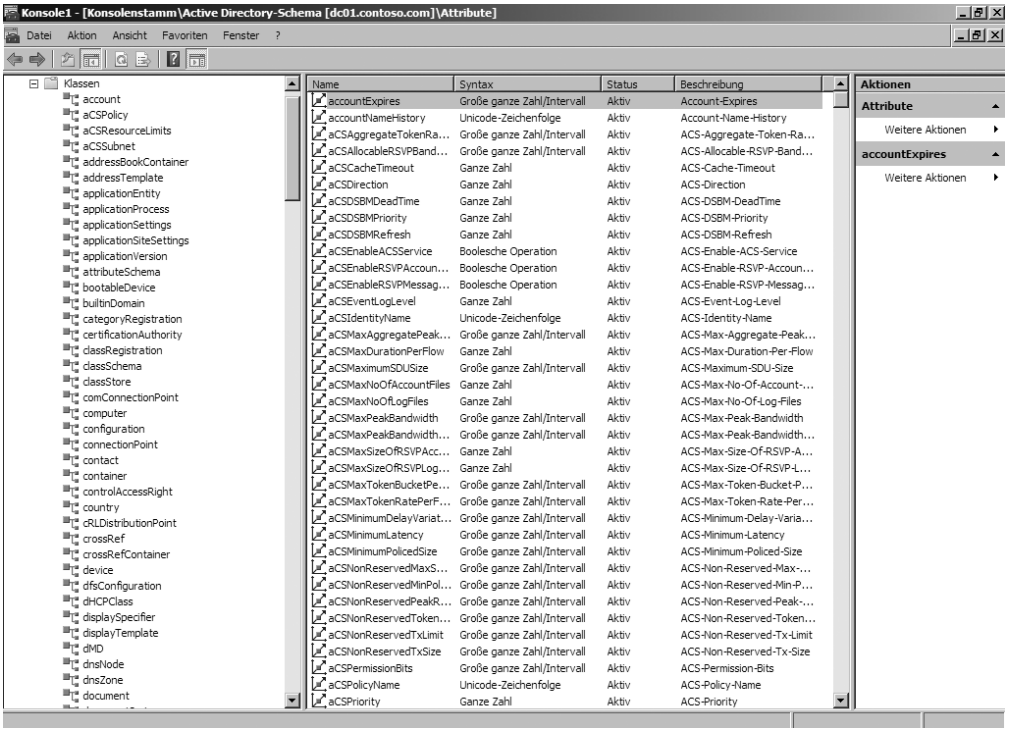
Ohne das Schema wäre ein Active Directory ein wilder Haufen von Informationen, die unmöglich abgefragt werden könnten. Durch das erweiterbare Schema lassen sich jederzeit zusätzliche Objekteigenschaften hinzufügen. Diese Funktion wird beispielsweise von Exchange Server genutzt. Alle notwendigen Informationen zu einem E-Mail-Postfach werden im Active Directory abgelegt. Bei der Installation von Exchange wird das Active Directory-Schema um die notwendigen Attribute und Klassen erweitert. Active Directory kennt schon Hunderte von Objektklassen und Attributtypen. Zu den wichtigsten gehören:

- **Das Objekt *User*** Dieses Objekt definiert einen bestimmten Benutzer in einer Domäne. Zu den Attributen, die für das Objekt definiert werden können, gehören beispielsweise der Benutzername, der Vor- und Nachname des Benutzers, seine Adresse und Telefonnummer, ein Bild des Benutzers.
- **Das Objekt *Computer*** Dieses Objekt identifiziert Systeme, die zu einer Domäne gehören. Zu den Attributen gehören Betriebssystem und installierte Service Packs, DNS-Name und die Rolle des Systems in der Domäne.

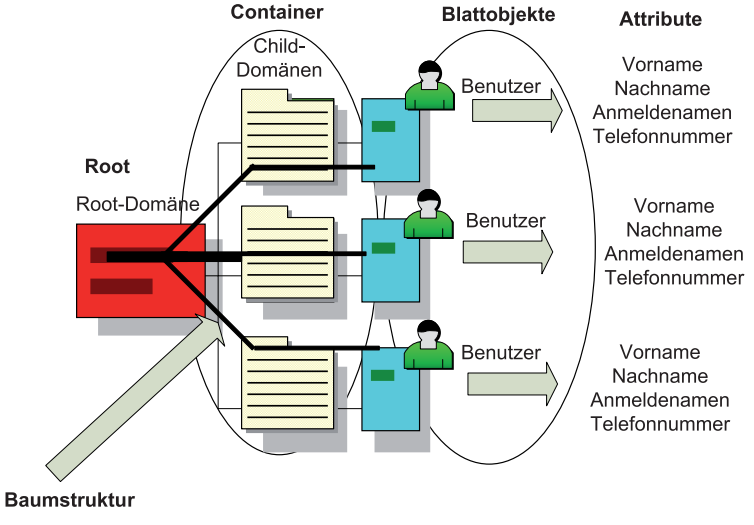
Für jedes Objekt, das im Active Directory gespeichert ist, gibt es eine *Zugriffsteuerungsliste (Access Control List, ACL)*, mit der differenziert angegeben werden kann, wer in welcher Form mit diesem Objekt umgehen darf. Es werden genaue Berechtigungen definiert, die vorgeben, wer ein Objekt verändern, löschen oder neu anlegen darf. Objekte werden in Klassen unterschieden. Ein Objekt kann durchaus mehreren Klassen zugeordnet werden, muss aber mindestens einer Klasse zugehörig sein. In allen Verzeichnisdiensten, auch dem Active Directory, gibt es Objekte, die andere Objekte beinhalten können. Diese Objekte werden *Container* genannt. Im Active Directory sind Container

zum Beispiel Domänen oder *Organisationseinheiten (Organizational Units, OUs)*. Objekte, die ausschließlich aus Informationen, den Attributen, bestehen, wie zum Beispiel Benutzer oder Computer, werden auch als Blattobjekte bezeichnet.

Abbildg. 8.9 Anzeige des Schemas von Active Directory mit der Microsoft Management Console (MMC)



Abbildg. 8.10 Aufbau eines LDAP-Verzeichnisses und der dazugehörigen Baumstruktur



Ein LDAP-Verzeichnis kann aus mehreren Containern hierarchisch angeordnet werden, bis am Ende der Äste die Blattobjekte, in diesem Beispiel die Benutzer, kommen.

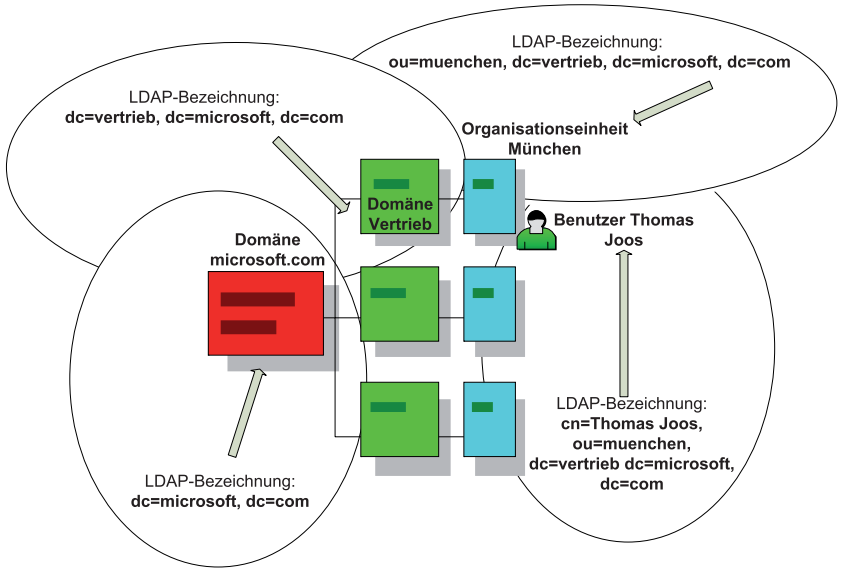
Adressierung in Verzeichnisdiensten

Damit die Objekte innerhalb eines Verzeichnisdienstes nicht nur korrekt gespeichert, sondern auch gefunden werden können, gibt es Protokolle wie das bereits beschriebene LDAP-Protokoll. Damit LDAP die Daten im Verzeichnis finden kann, muss ein Standard zur Adressierung dieser Objekte verfügbar sein. Jedes Objekt in einem Verzeichnis erhält eine eindeutige Adressierung. Diese Adressierung wird *Distinguished Name (DN)* genannt. Die Adressierung gibt nicht nur die Bezeichnung eines Objektes im Verzeichnis wieder, sondern auch dessen Speicherort. Ein Beispiel für einen solchen Distinguished Name im Active Directory ist folgender:

cn=Thomas Joos, ou=muenchen, dc=vertrieb, dc=microsoft, dc=com

Die Bezeichnung eines Objektes, in diesem Fall im Active Directory, wird immer vom Ursprungsort, der Root, bis zur eigentlichen Bezeichnung fortgeführt. Domänen werden dazu als *dc* abgekürzt, Organisationseinheiten als *ou* und die Blattobjekte schließlich als *cn* für *common name*.

Abbildg. 8.11 Beispiel von Distinguished Names in einem Verzeichnis

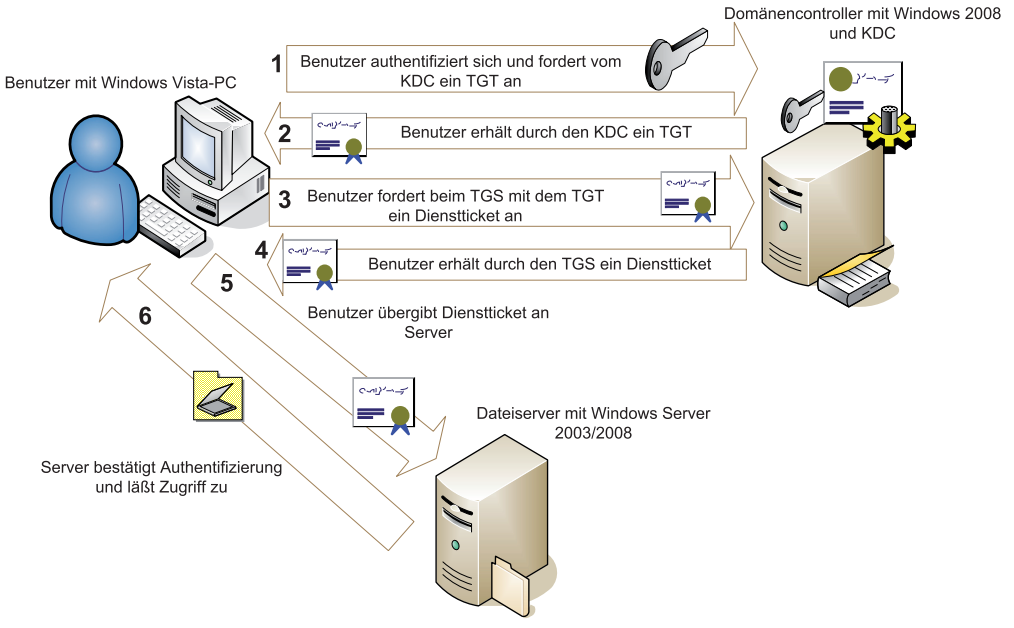


Jedes Objekt im Active Directory hat einen solchen eindeutigen Namen, der durch entsprechende LDAP-kompatible Programme gesucht werden kann.

Die Funktionsweise von Kerberos

Bei Kerberos wird die Identität des Benutzers und die Identität des authentifizierenden Servers festgestellt. Kerberos arbeitet mit einem so genannten Ticket-System, um Benutzer zu authentifizieren. Kennwörter werden in einem Active Directory niemals über das Netzwerk übertragen.

Abbildg. 8.12 Kerberos in Active Directory



Damit sich ein Benutzer an einem Server authentifizieren kann, um zum Beispiel auf sein Postfach auf dem Exchange-Server zuzugreifen, wird ausschließlich mit verschlüsselten Tickets gearbeitet. Ein wesentlicher Bestandteil der Kerberos-Authentifizierung ist das Schlüsselverteilungscenter (Key Distribution Center, KDC). Dieser Dienst wird auf allen Windows Server 2008-Domänencontrollern ausgeführt und ist für die Ausstellung der Authentifizierungstickets zuständig. Der zuständige Kerberos-Client läuft auf allen Windows 2000, XP und Vista-Arbeitsstationen, sowie auch unter Windows Server 2003 und Windows Server 2008.

Meldet sich ein Benutzer an einer Arbeitsstation im Active Directory an, muss er sich zunächst an einem Domänencontroller und dem dazugehörigen KDC authentifizieren. Im nächsten Schritt erhält der Client ein Ticket-genehmigendes Ticket (TGT) vom KDC ausgestellt. Hat der Client dieses TGT erhalten, fordert er beim KDC mithilfe dieses TGT ein Ticket für den Zugriff auf den Dateiserver an. Diese Authentifizierung führt der Ticket-genehmigende Dienst (Ticket Granting Service, TGS) auf dem KDC aus. Nach der erfolgreichen Authentifizierung des TGT durch den TGS stellt dieser ein Dienstticket aus und übergibt dieses Ticket an den Client. Dieses Dienstticket gibt der Client an den Server weiter, auf den er zugreifen will, in diesem Beispiel den Mailbox-Server.

Durch dieses Ticket kann der Server sicher sein, dass sich kein gefälschter Benutzer mit einem gefälschten Benutzernamen anmeldet. Durch das Dienstticket wird sowohl der authentifizierende Domänencontroller als auch der Benutzer authentifiziert. Der genaue Ablauf dieses Verfahrens ist in der Abbildung 8.12 skizziert. Sollten Probleme mit dem Schlüsselverteilungscenter oder Kerberos im Allgemeinen auftreten, besteht unter Umständen noch ein Problem bei der Kerberosauthentifizierung. In diesem Fall wird normalerweise allerdings eine entsprechende Fehlermeldung bei *Dcdiag.exe* angezeigt, die auf Probleme mit LDAP oder Kerberos hinweisen. Kerberos ist für die Anmeldung in Active Directory von existenzieller Wichtigkeit.

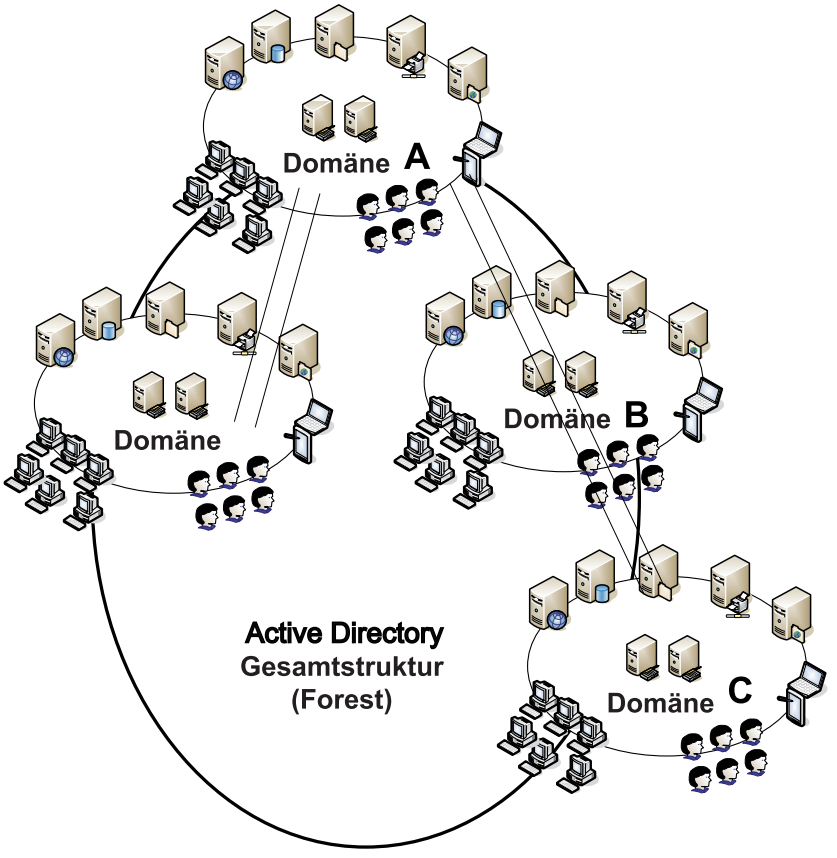
Aufbau von Active Directory

Zwei Begriffe aus dem klassischen Domänenmodell finden sich im Active Directory wieder: Es gibt Active Directory-Domänen und Domänencontroller. Die Domäne ist weiterhin die grundlegende Strukturierungseinheit. Allerdings kann sie in eine komplexere Struktur eingebunden werden. Domänencontroller finden sich ebenfalls im Active Directory. Die Domänencontroller übernehmen die Verwaltung der Verzeichnisinformationen innerhalb einer Domäne. Die Benutzer-, Computer-, Freigaben- und Druckerinformationen werden in einer Datenbank gespeichert. Diese Datenbank ist eine *JET-Datenbank (Joint-Engine-Technologie)*, die Microsoft auch bei Exchange einsetzt. Das Active Directory arbeitet mit den Technologien, die weiter vorne in diesem Kapitel beschrieben sind. Das Active Directory hat im Gegensatz zum alten Windows NT-Domänenmodell einige Änderungen erfahren. Bei Windows NT wurden alle Benutzer- und Computerinformationen nicht in einer Datenbank, sondern in der Registry der Domänencontroller gespeichert. Die Daten einer Domäne wurden auf dem primären Domänencontroller, dem PDC, im so genannten *Security Account Manager (SAM)* gespeichert. Dieser SAM enthielt alle Informationen über den Benutzer und die Computer einer Windows-Domäne. Wenn ein Administrator Änderungen durchführt, zum Beispiel das Anlegen eines neuen Benutzers, wird er immer zum PDC verbunden. Damit eine NT-Domäne ausfallsicher gestaltet werden kann, gab es noch Backup-Domänencontroller (BDC). Die Änderungen werden in regelmäßigen Abständen auf die BDCs repliziert. Eine Änderung auf den BDC ist nicht möglich, da diese nur Replikate der Änderungen erhalten, aber selbst keine weitergeben können. Auch wenn die Funktion der neuen Read-Only-Domänencontroller (RODC) ähnlich zu BDCs sind, sollten Sie diese nicht mit dieser alten Funktion gleichsetzen. Ein RODC bietet deutlich mehr Sicherheitsoptionen, zum Beispiel die genaue Steuerung, welche Objekte repliziert werden sollen. Weitere Untergliederungen oder Container gab es nicht. Es war möglich, Vertrauensstellungen zwischen Domänen herzustellen. Beide Domänen hatten danach aber immer noch getrennte Benutzerdatenbanken. Der einzige Vorteil war, dass durch Vertrauensstellungen Berechtigungen zwischen verschiedenen Domänen verteilt werden. Wenn der PDC ausfällt, können keinerlei Änderungen in der Windows-Domäne mehr vorgenommen werden und die Domäne steht auch den Benutzern nicht mehr zur Verfügung.

Active Directory-Gesamtstruktur (Forest)

Im Active Directory werden die Benutzerdaten und Computerinformationen nicht mehr in der Registry des PDC durch den SAM gespeichert, sondern in der Datenbank von Active Directory. Eine Active Directory-Umgebung kann im Gegensatz zu Windows NT mehrere Domänen zu einer Einheit zusammenfassen. Das Domänenmodell ist immer noch vorhanden, wird aber extrem erweitert. Ein Active Directory kann aus mehreren selbstständigen Domänen bestehen, die dennoch zu einer großen gemeinsamen Organisation gehören. Alle verbundenen Domänen eines Active Directory teilen sich eine Datenbank und ein Schema. Diese Domänen bilden eine *Gesamtstruktur*, im Englischen auch Forest genannt (Abbildung 8.13). Ein Forest ist die Grenze des Verzeichnisdienstes eines Unternehmens, in dem einheitliche Berechtigungen vergeben und delegiert werden können.

Abbildg. 8.13 Aufbau einer Active Directory-Gesamtstruktur

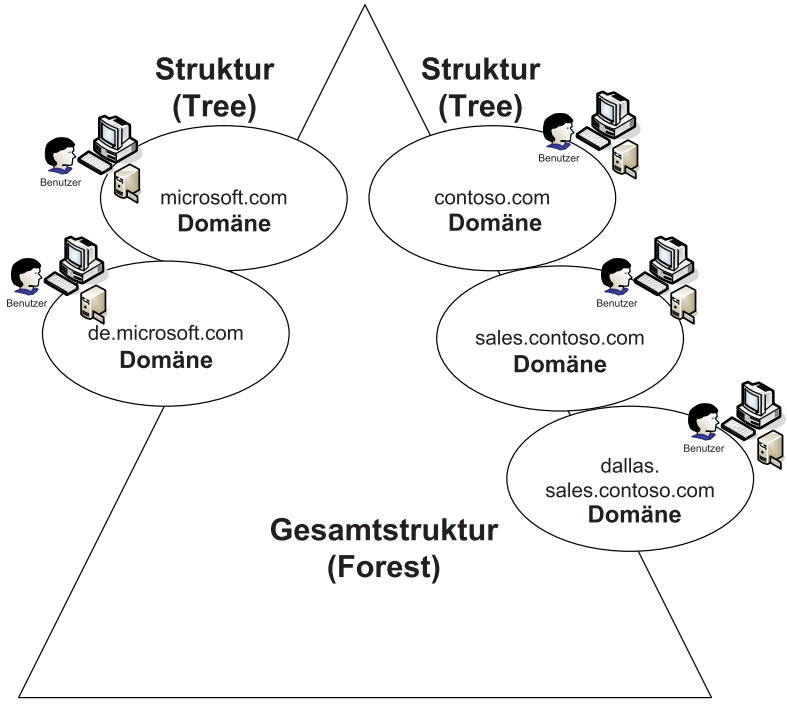


In den einzelnen Domänen eines Active Directory existieren Domänencontroller und Domänen-Administratoren. Für Anwender ändert sich beim Umgang mit der Domäne so gut wie nichts. Sie können mehrere Domänen in einer Gesamtstruktur hierarchisch aufbauen. Jede Domäne in einem Active Directory ist eine eigene Partition im Verzeichnis, die automatisch angelegt wird. Jede Partition wird von unterschiedlichen Domänencontrollern verwaltet. Diese Partitionierung erfolgt automatisch. Zusätzlich gibt es die Möglichkeit, mit Zusatztools wie *Ldp.exe*, das zum Lieferumfang von Windows Server 2008 gehört, zusätzliche Partitionen zu erstellen.

Active Directory-Struktur (Tree)

Das Namensmodell von Active Directory orientiert sich stark am DNS. Domänen werden im Active Directory zu Strukturen (Trees) zusammengefasst. Eine Struktur muss über einen einheitlichen Namensraum verfügen. Hier wird mit DNS-Namen gearbeitet. Wenn eine Struktur beispielsweise *contoso.com* heißt, kann es innerhalb dieser Struktur weitere Einheiten geben, die beispielsweise *sales.contoso.com*, *marketing.contoso.com* und *dallas.marketing.contoso.com* heißen.

Abbildg. 8.14 Domänenstrukturen in Active Directory



In einer *Struktur (Tree)* werden gegenseitige Vertrauensstellungen zwischen den beteiligten Domänen automatisch erzeugt. Darüber hinaus kann in einer Struktur eine Suche über mehrere Domänen hinweg erfolgen. Ein Globaler Katalog-Server enthält die Informationen der Gesamtstruktur und kann Anfragen an die verantwortlichen Domänencontroller der jeweiligen Domäne weiterleiten. Eine Active Directory-*Gesamtstruktur (Forest)* kann aus mehreren *Strukturen (Trees)* zusammengesetzt sein, oftmals besteht sie allerdings aus nur einer Struktur. Jedes Active Directory muss aus mindestens einer Struktur bestehen. Der ersten Domäne eines Active Directory kommt eine besondere Bedeutung zu. Da sie die erste Domäne ist, bildet sie zugleich die erste *Struktur* von Active Directory und ist gleichzeitig die *Root-Domäne* der Gesamtstruktur.

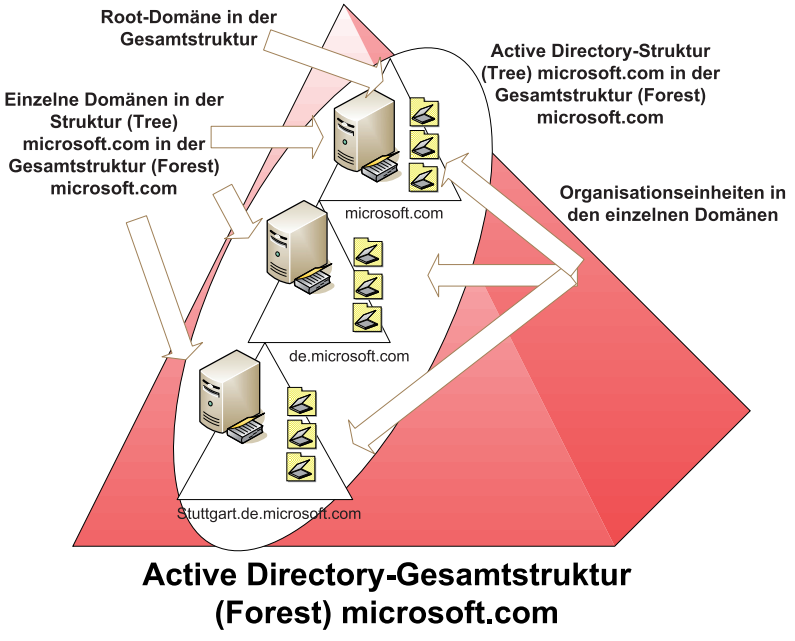
Wenn Sie ein Active Directory mit nur einer Domäne planen, bildet diese Domäne die Gesamtstruktur, die erste und einzige Struktur und die Root-Domäne von Active Directory. Die Domänen einer Struktur (Tree) teilen sich einen so genannten Namensraum. Unter Windows NT hatten Domänen lediglich einen NetBIOS-Namen mit bis zu 15 Zeichen. In Active Directory gibt es diese NetBIOS-Namen auch noch. Wichtiger sind jedoch die DNS-Namen, die jede Domäne eindeutig einem DNS-Namensraum zuweist. Als Struktur wird ein Namensraum bezeichnet, der vollkommen eigenständig ist. In Abbildung 8.15 sind zum Beispiel die Domänen *microsoft.com* und *de.microsoft.com* eine eigene Struktur (Tree). Auch die Domänen *contoso.com*, *sales.contoso.com* und *dallas.sales.com* bilden eine eigene Struktur. Im Beispiel von Abbildung 8.15 sind die beiden Strukturen *contoso.com* und *microsoft.com* trotz ihrer vollständig eigenständigen Namensräume Teil einer gemeinsamen Active Directory-Gesamtstruktur. Jede Domäne kann beliebige untergeordnete Domänen (Child-Domänen genannt) haben, die wiederum wieder Child-Domänen beinhalten können. Alle Domä-

nen eines Namensraums werden als eigenständige Struktur bezeichnet. Child-Domänen sind wie die übergeordneten Domänen vollkommen eigenständig, teilen sich jedoch einen Namensraum und eine Active Directory-Gesamtstruktur. Sie bilden jeweils eigene Partitionen im Active Directory, die durch getrennte Domänencontroller verwaltet werden.

Organisationseinheiten (Organizational Units, OUs)

Jede Domäne kann unterschiedliche Organisationseinheiten beinhalten. Organisationseinheiten können Sie sich wie Ordner im Windows-Explorer, in denen Dateien liegen, vorstellen. Durch Organisationseinheiten können Sie Objekte innerhalb von Domänen ordnen. Organisationseinheiten sind Container, in denen Objekte von Active Directory liegen können. Innerhalb von Organisationseinheiten können Berechtigungen delegiert und Richtlinien definiert werden, die für alle Objekte eines solchen Containers Gültigkeit haben. Diese Richtlinien, auch Gruppenrichtlinien, werden in Kapitel 9 näher behandelt. Organisationseinheiten sind die kleinsten Container in Active Directory. Eine Organisationseinheit kann mehrere Unterorganisationseinheiten beinhalten.

Abbildg. 8.15 Organisationseinheiten in Active Directory



Die Container von Active Directory im Vergleich

Wie Sie bereits zu Beginn des Kapitels gelesen haben, werden Objekte in einem Verzeichnis, die andere Objekte beinhalten können, als *Container* bezeichnet. Der Begriff *Container* kann durchaus wörtlich verstanden werden. In einem Container lassen sich Objekte lagern. Dabei kann es sich um Informationen über Benutzer, über Computer oder Drucker handeln. Außerdem können in einen großen Container kleine Container eingelagert werden. Im Active Directory gibt es durch diese Definition vier verschiedene Container:

- **Gesamtstruktur (Forest)** Dieser Container kann *Strukturen (Trees)* beinhalten.
- **Struktur (Tree)** Dieser Container beinhaltet die einzelnen Domänen eines Active Directory.
- **Domänen** Dieser Containertyp beinhaltet *Organisationseinheiten*.
- **Organisationseinheiten (Organizational Units, OUs)** Dieser Container beinhaltet Benutzer- und Computerkonten, kann aber auch weitere OUs beinhalten. Vor allem die Organisationseinheiten, welche dafür zuständig sind, die einzelnen Objekte der Domäne zu ordnen, sollten frühzeitig geplant werden. Auch wenn jederzeit weitere OUs erstellt werden können, sollten sie bereits bei der Planung von Active Directory berücksichtigt werden.

Der wichtigste Container im Active Directory ist die Domäne. Sie ist die logische Struktur, in der das Unternehmen abgebildet wird. Gleichzeitig hat eine Domäne Auswirkung auf die physische Speicherung von Informationen: Die Domäne stellt die Grenze dar, innerhalb der Informationen gemeinsam verwaltet werden. Der erste Schritt in der Planung von Active Directory ist daher die Gestaltung von Domänen. Domänen dienen zur Gruppierung gleichartiger Systeme. Sie müssen bei der Implementierung von Active Directory vor allem unter logischen Gesichtspunkten betrachtet werden. Im Grunde genommen kann jede Domäne Organisationseinheiten darstellen, in denen die einzelnen Computer und Benutzer, die Mitglied der Domäne sind, geordnet werden. Genau an dieser Stelle liegt der Kernpunkt einer ordentlichen Active Directory-Planung. Wie viele Gesamtstrukturen, Strukturen, Domänen mit Child-Domänen, Organisationseinheiten mit Unterorganisationseinheiten in Ihrem Active Directory angelegt werden, muss genau geplant werden. Es gibt keinen Königsweg, der vorgibt, welche Planung die effizienteste ist.

Installieren von Active Directory

In diesem Abschnitt erfahren Sie, wie Sie Active Directory auf Windows Server 2008 installieren. Active Directory und DNS sind eng miteinander verbunden. Aus diesem Grund werden in diesem Abschnitt sowohl die notwendigen Themen um DNS als auch das Zusammenspiel mit Active Directory ausführlich behandelt. Ohne stabiles DNS ist Active Directory nicht funktionsfähig.

HINWEIS Während der Installation des DNS-Dienstes, beziehungsweise bei der Heraufstufung eines Servers zu einem Domänencontroller, erhalten Sie unter Umständen die Meldung, dass noch DHCP aktiviert ist, auch wenn Sie eine statische IPv4-Adresse festgelegt haben. Dieser Fehler wird durch die IPv6-Verbindung von Windows Server 2008 verursacht und kann ignoriert werden. Deaktivieren Sie in den Netzwerkverbindungen IPv6, erscheint diese Meldung nicht mehr, allerdings verlieren Sie auch die Vorteile der effizienteren Kommunikation zwischen Windows Server 2008- und Windows Vista-Computern.

Einführung in DNS unter Windows Server 2008

Die hauptsächliche Aufgabe von DNS (Domain Name System) ist die Auflösung von Computernamen zu IP-Adressen, auch *Forward-Lookup* genannt. Eine weitere Aufgabe ist das Auflösen von IP-Adressen zu Computernamen, auch *Reverse-Lookup* genannt. Computernamen im DNS bestehen nicht nur aus einem NetBIOS-Namen, wie zum Beispiel *dc01*, sondern zusätzlich aus einem so genannten Domänennamen, wie zum Beispiel *contoso.com*. Einen vollständigen Rechnernamen bezeichnet man auch als *vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN)*. Der FQDN eines Servers *dc01* in der Domäne *contoso.com* ist *dc01.contoso.com*. Die beiden Rechner

dc01.contoso.com und *dc01.contoso.int* sind zwei vollkommen unterschiedliche Systeme. Um eine Verbindung mit einem dieser Systeme aufzubauen, reicht es nicht aus, nur den Namen *dc01* auflösen zu können. Es ist wichtig, dass die beteiligten Computer, die die Verbindung zu den beiden Servern aufnehmen sollen, beide Domänennamen auflösen können. DNS-Domänen, wie in diesem Beispiel *contoso.com* und *contoso.int*, werden auf DNS-Servern in so genannten *Zonen* verwaltet. Eine *Zone* kann mehrere Subdomänen einer Domäne verwalten, zum Beispiel *de.contoso.com* oder *fr.contoso.com*. Allerdings kann eine Zone auf einem DNS-Server nicht verschiedene Namensräume verwalten, wie zum Beispiel *contoso.com* und *contoso.int*. In diesem Fall müssten für diese beiden DNS-Domänen zwei getrennte Zonen angelegt werden.

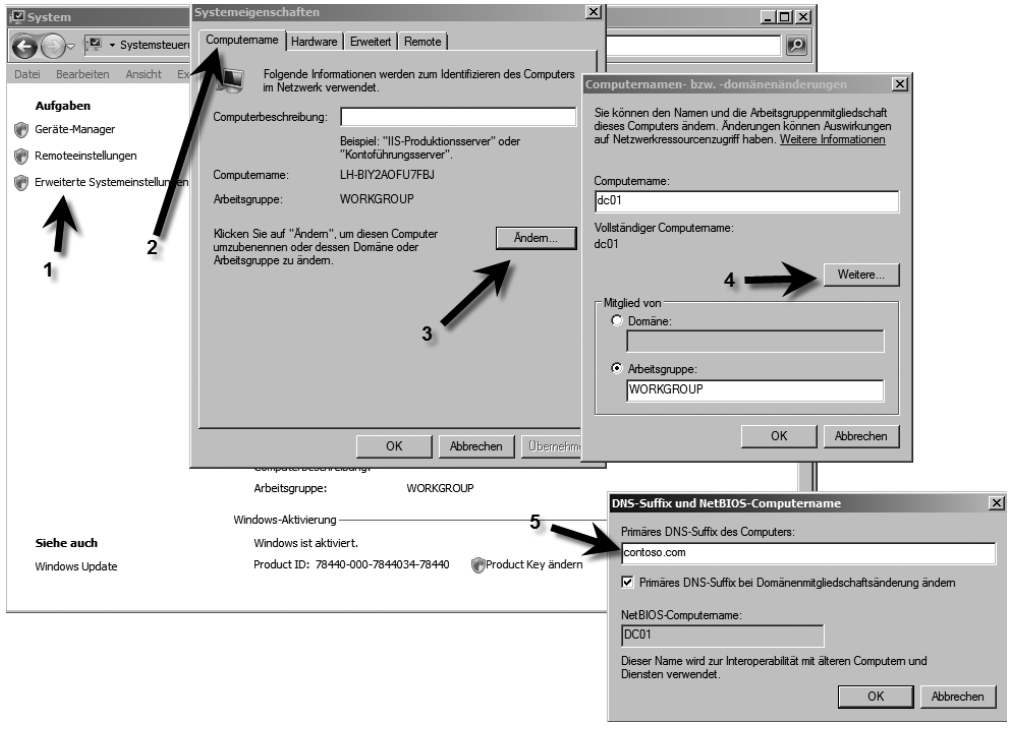
Eine weitere wichtige Aufgabe von DNS ist das Auflösen von *SRV-Records* (Service-Records). In SRV-Records werden spezielle Serverdienste abgelegt, die in DNS veröffentlicht werden. Ein Beispiel wäre der bekannte SRV-Record MX (Mailexchanger), der festlegt, welche E-Mail-Server es in einer Domäne gibt und wie die IP-Adresse dieses Servers lautet. Die Aufgabe des DNS-Servers besteht in diesem Bereich darin, dass Computer den DNS-Server befragen können, welcher Server im Netzwerk einen bestimmten Netzwerkdienst verwaltet. Es gibt zahlreiche SRV-Records im DNS, die durch Active Directory angelegt werden. Wollen Computer spezielle Dienste in Active Directory erreichen, zum Beispiel einen globalen Katalogserver, können die DNS-Server befragt werden, die alle SRV-Records der globalen Katalogserver kennen.

Vorbereitungen für Active Directory

Der nächste Schritt bei der Installation von Active Directory besteht darin, den NetBIOS-Namen und das DNS-Suffix des ersten Domänencontrollers so zu wählen, wie später die Active Directory-Domäne benannt werden soll. Konfigurieren Sie daher zunächst über *Systemsteuerung/System/Erweiterte Systemeinstellungen*, Registerkarte *Computername*, Schaltfläche *Ändern* den NetBIOS-Namen des neuen Domänencontrollers, zum Beispiel *dc01*. Klicken Sie dann in diesem Fenster auf die Schaltfläche *Weitere* und geben Sie das DNS-Suffix des Servers an. Geben Sie an dieser Stelle exakt den DNS-Namen an, den Ihre Active Directory-Domäne später erhalten soll, zum Beispiel *contoso.com* (Abbildung 8.16).

Der vollständige Name des Servers (FQDN) setzt sich aus dem Computernamen und dem primären DNS-Suffix zusammen. Der vollständige Computername des Domänencontrollers lautet *dc01.contoso.com*. Haben Sie die Änderungen vorgenommen, müssen Sie den Server neu starten.

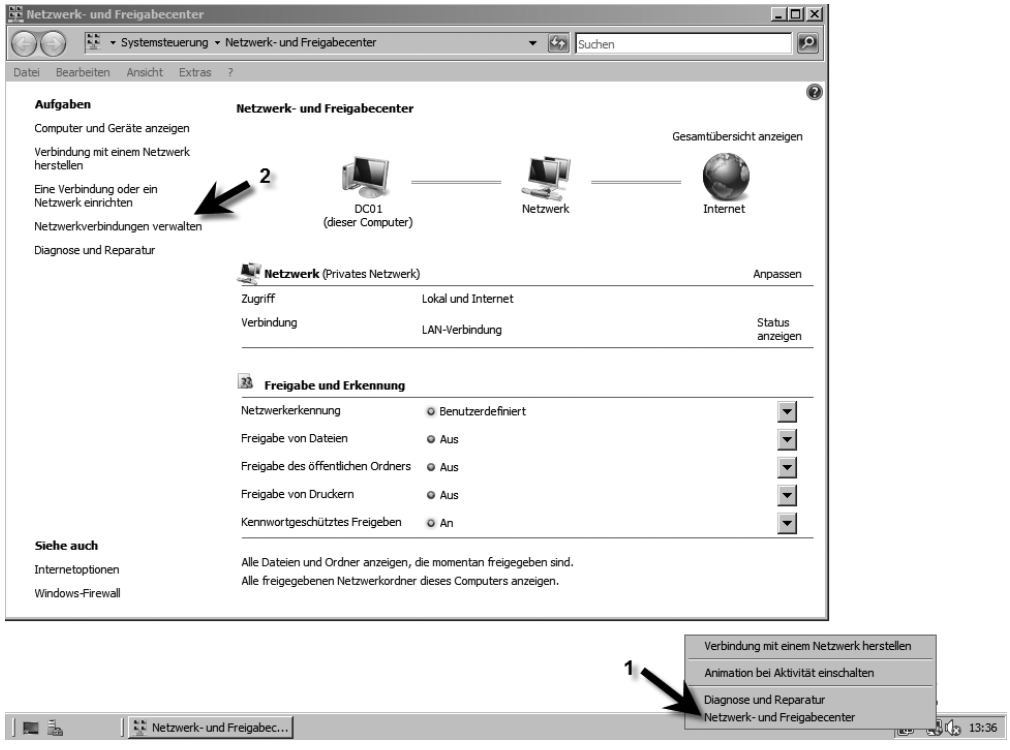
Abbildg. 8.16 Definieren des Computernamens und des DNS-Suffix eines Domänencontrollers



Konfigurieren der IP-Einstellungen des Servers

Haben Sie den vollständigen Computernamen festgelegt, sollten Sie als Nächstes die IP-Einstellungen des Servers anpassen. Wichtig ist an dieser Stelle, dass Sie die lokale IP-Adresse des Servers als primären DNS-Server festlegen. Da dieser Server der erste Domänencontroller des neuen Active Directory werden soll, wird er auch der erste DNS-Server. Tragen Sie in den Eigenschaften des IP-Protokolls die IP-Adresse des Servers als bevorzugten Server ein (Abbildung 8.17). Der nächste Schritt besteht darin, den DNS-Server für das Active Directory vorzubereiten. An dieser Stelle müssen Sie noch keinen alternativen DNS-Server eintragen. Der alternative DNS-Server wird erst von einem Client befragt, wenn der bevorzugte DNS-Server nicht mehr antwortet. Die IP-Einstellungen für Netzwerkverbindungen erreichen Sie über den Link *Netzwerkverbindungen verwalten* im Netzwerk- und Freigabecenter. Am schnellsten gelangen Sie an diese Konfiguration über *Start/Ausführen/ncpa.cpl*.

Abbildg. 8.17 Verwalten der Netzwerkverbindungen über das Netzwerk- und Freigabecenter



Rufen Sie die Eigenschaften des IPv4-Protokolls auf, um die IP-Einstellungen für die Domäne vorzunehmen. Tragen Sie in den Eigenschaften des IP-Protokolls die IP-Adresse des Servers als bevorzugten Server ein (Abbildung 8.18). An dieser Stelle müssen Sie noch keinen alternativen DNS-Server eintragen. Der alternative DNS-Server wird erst von einem Client befragt, wenn der bevorzugte DNS-Server nicht mehr antwortet.

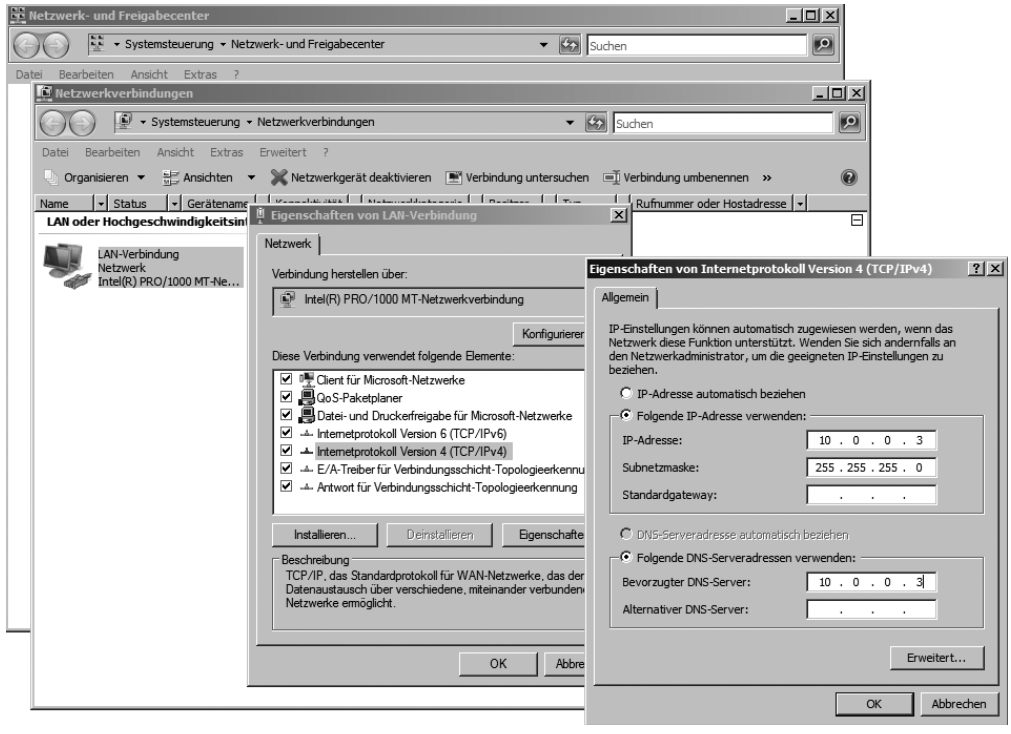
Erweiterte Netzwerkeinstellungen für die Domänenaufnahme

Über die Schaltfläche *Erweitert* erreichen Sie weitere Einstellungen, um die Namensauflösung per DNS oder WINS im Netzwerk optimaler einzustellen. Normalerweise werden Sie hier keine Einstellungen vornehmen müssen, da bereits die Standardeinstellungen ausreichen. Für manche Netzwerke kann jedoch eine Nachjustierung sinnvoll sein. Ob das für Sie notwendig ist, erfahren Sie auf den folgenden Seiten. Passen Sie die erweiterten Einstellungen an, sollten Sie darauf achten die Standardeinstellungen zu notieren, da diese später nicht einfach nachzuvollziehen sind, wenn Sie erneut Änderungen vornehmen müssen.

Windows Internet Name Service (WINS)

Auf der Registerkarte *WINS* können Sie einen WINS-Server eintragen, sofern Sie einen solchen im Netzwerk betreiben. Zu jeder Active Directory-Domäne gehört ein WINS-Server. *WINS* steht für *Windows Internet Name Service* und ist der Vorgänger der dynamischen DNS-Aktualisierung. Während DNS für die Namensauflösung mit vollqualifizierten Domänennamen zuständig ist, werden mit WINS NetBIOS-Namen aufgelöst. Auf den Arbeitsstationen können Sie diese Einstellungen auch mit Hilfe eines DHCP-Servers verteilen.

Abbildg. 8.18 IP-Einstellungen unter Windows Server 2008 für die Erstellung einer Active Directory-Domäne

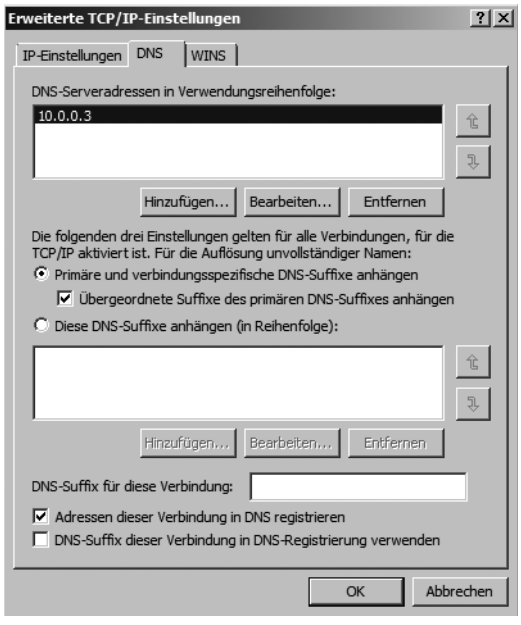


Erweiterte DNS-Einstellungen in Windows Vista und Windows Server 2008

Auf der Registerkarte *DNS* werden schließlich notwendige Einstellungen vorgenommen, um Windows Server 2008 besser in eine Windows-Domäne einzubinden. Für eine generelle Aufnahme von Windows Vista oder Windows Server 2008 in eine Domäne sind hier keine Änderungen vorzunehmen. Auf den folgenden Seiten erfahren Sie jedoch an Hand von Beispielen, wann hier Änderungen sinnvoll sein können. Zunächst sind standardmäßig immer nur die folgenden Optionen bzw. Kontrollkästchen aktiviert (Abbildung 8.19):

- Primäre und verbindungsspezifische DNS-Suffixe anhängen
- Übergeordnete Suffixe des primären DNS-Suffixes anhängen
- Adressen dieser Verbindung in DNS registrieren

Abbildg. 8.19 Erweiterte DNS-Einstellungen für Windows Server 2008



Die einzelnen Optionen spielen bei der Namensauflösung in einer DNS-Infrastruktur eine erhebliche Rolle:

- **Primäre und verbindungsspezifische DNS-Suffixe anhängen** Durch die Aktivierung dieser Option wird festgelegt, dass der Rechner versucht, bei der Auflösung von Rechnernamen immer automatisch das konfigurierte primäre DNS-Suffix des eigenen Computernamens anzuhängen. Wollen Sie zum Beispiel einen Rechnernamen mit der Bezeichnung *dc01* auflösen, versucht der Rechner eine Namensauflösung nach *dc01.contoso.com*, wenn das primäre DNS-Suffix des Servers *contoso.com* ist.
- **Übergeordnete Suffixe des primären DNS-Suffixes anhängen** Diese Option bedeutet, dass auch die Namen von übergeordneten Domänen bei der Namensauflösung verwendet werden. Wenn Sie zum Beispiel in einer untergeordneten Domäne mit der Bezeichnung *muenchen.de.contoso.com* einen Servernamen *dc05* auflösen wollen, versucht der Rechner zunächst die Auflösung über *dc05.muenchen.de.contoso.com*, falls dies das primäre DNS-Suffix des PCs oder Servers ist. Im Anschluss wird versucht, den Namen über *dc05.de.contoso.com* und dann über *dc05.contoso.com* aufzulösen, da diese Domänen der Domäne *muenchen.de.contoso.com* übergeordnet sind.
- **DNS-Suffix für diese Verbindung** Zusätzlich haben Sie noch die Möglichkeit, in diesem Bereich ein weiteres beliebiges DNS-Suffix einzutragen. Wenn der Rechner den eingegebenen Namen bei seinem konfigurierten DNS-Server nicht über sein eigenes primäres DNS-Suffix finden kann, versucht er es mit dem DNS-Suffix in diesem Feld. Wollen Sie zum Beispiel den Servernamen *dc06* auflösen, versucht der PC oder Server zunächst die Auflösung in *dc06.contoso.com*, sofern das sein primäres DNS-Suffix ist. Tragen Sie im Feld *DNS-Suffix für diese Verbindung* noch ein Suffix in der Form *muenchen.de.microsoft.com* ein, versucht der PC auch den Namen nach *dc06.muenchen.de.microsoft.com* aufzulösen.

- **Adressen dieser Verbindung in DNS registrieren** Auch diese Option ist bereits standardmäßig aktiviert. Ein DNS-Server unter Windows Server 2008 hat die Möglichkeit, Einträge dynamisch zu registrieren. Durch dieses dynamische DNS müssen Hosteinträge nicht mehr manuell durchgeführt werden. Sobald sich ein Rechner im Netzwerk anmeldet, versucht er seinen FQDN beim konfigurierten DNS-Server automatisch einzutragen, sofern diese Option nicht deaktiviert wurde. Dieser Punkt ist für die interne Namensauflösung in einem Active Directory-Netzwerk von sehr großer Bedeutung.

Außer den standardmäßig aktivierten Optionen gibt es noch weitere Möglichkeiten, die Sie in diesem Fenster konfigurieren können:

- **Diese DNS-Suffixe anhängen** Wenn Sie diese Option aktivieren, können Sie DNS-Suffixe konfigurieren, nach denen unvollständige Rechnernamen aufgelöst werden. Aktivieren Sie diese Option, wird weder das primäre DNS-Suffix des Servers noch die DNS-Suffixe dieser Verbindung verwendet. Es werden die DNS-Suffixe in der Reihenfolge angehängt, die im Feld *Diese DNS-Suffixe anhängen (in Reihenfolge)* konfiguriert sind. Achten Sie bei der Konfiguration darauf, dass möglichst das DNS-Suffix der Windows-Domäne, in der dieser Server Mitglied ist oder werden soll, als Erstes in dieser Liste eingetragen ist. Diese Option wird häufig verwendet, um die Namensauflösung in Gesamtstrukturen mit mehreren Strukturen zu lösen. Dazu werden in der Reihenfolge alle Strukturen der Gesamtstruktur eingetragen, um eine Namensauflösung innerhalb von Active Directory zu gewährleisten. Vor allem beim Einsatz von Exchange Servern ist diese Option sehr nützlich, wenn die Exchange-Server über mehrere Strukturen und Domänen verteilt sind. Standardmäßig ist diese Option nicht aktiviert.
- **DNS-Suffix dieser Verbindung in DNS-Registrierung verwenden** Wenn Sie dieses Kontrollkästchen aktivieren, wird der Server im DNS mit seinem Computernamen und seinem primären DNS-Suffix registriert, also seinem FQDN (Fully Qualified Domain Name). Zusätzlich wird der Name mit dem DNS-Suffix auch beim DNS-Server registriert, das im Bereich *DNS-Suffix für diese Verbindung konfiguriert* ist. Diese Option ist ebenfalls nicht standardmäßig aktiviert.

Wenn Sie schnell und effizient Server-Namen in verschiedenen DNS-Zonen auflösen wollen, aktivieren Sie auf den PCs oder Servern in den IP-Einstellungen über die Schaltfläche *Erweitert* auf der Registerkarte *DNS* die Option *Diese DNS-Suffixe anhängen (in Reihenfolge)*. Tragen Sie als Nächstes zuerst den Namensraum der eigenen Struktur ein und hängen Sie danach die Namensräume der anderen Strukturen an. Der Sinn dieser Konfiguration ist die schnelle Auflösung von Servern in den anderen Strukturen. Wenn Sie zum Beispiel den Domänencontroller *dc1* in der Struktur *contoso.com* auflösen wollen, müssen Sie immer *dc1.contoso.com* eingeben, wenn Ihr Server nicht Mitglied dieser Struktur ist. Diese Einstellung ist nur optional, erleichtert aber die Stabilität der Namensauflösung in Ihrem Active Directory. Sie sollten diese Einstellung auf jedem Domänencontroller sowie auf jedem Exchange-Server in Ihrer Gesamtstruktur durchführen sowie auf PCs von Administratoren oder Powerusern, die ständig Verbindung zu anderen Domänen aufbauen müssen. Zuerst sollte immer die eigene Domäne und der eigene Namensraum eingetragen werden, bevor andere Namensräume abgefragt werden. Haben Sie diese Maßnahme durchgeführt, können Sie mit *Nslookup* den Effekt überprüfen, allerdings erst dann, wenn das Active Directory installiert wurde. Sie können an dieser Stelle lediglich *dc1* eingeben. Der Server befragt seinen bevorzugten DNS-Server, ob ein Server mit dem Namen *dc1.microsoft.com* gefunden wird, wenn es sich hier um Ihr primäres DNS-Suffix handelt. Da dieser Server unter Umständen in dieser Domäne nicht vorhanden ist, wird der nächste Namensraum abgefragt. Das ist in diesem Beispiel *contoso.com*.

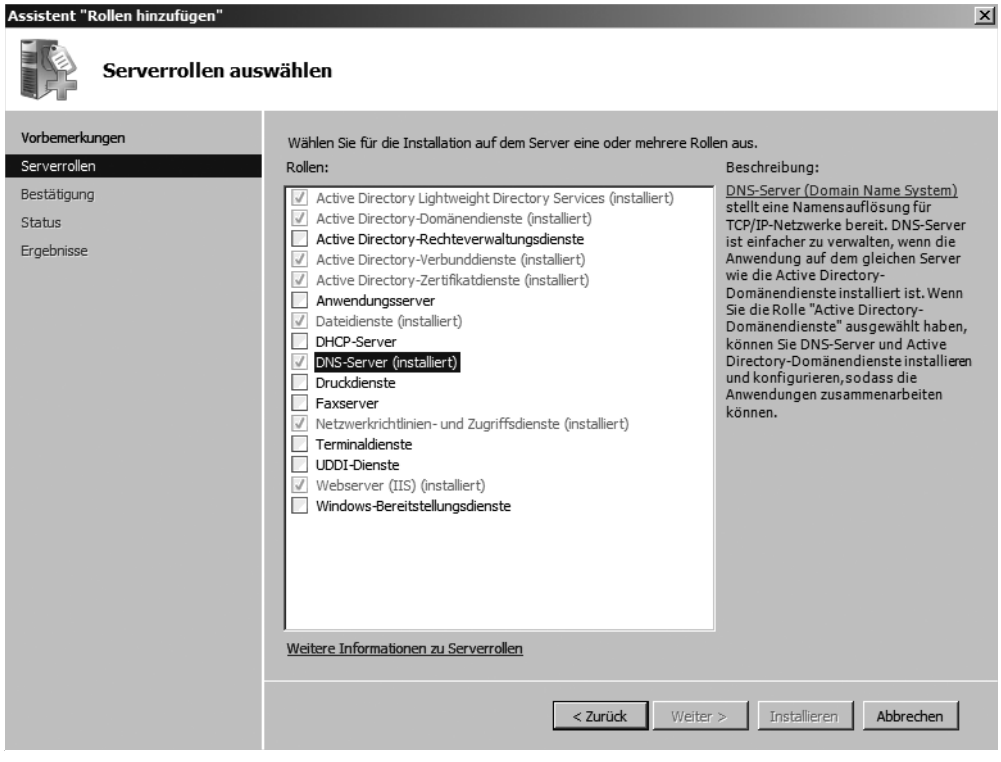
Viele Administratoren tragen auf ihrem DNS-Server einfach einen neuen statischen Hosteintrag ein, der auf die IP-Adresse des Servers des anderen Namensraumes zeigt. Diese Vorgehensweise ist aber

nicht richtig, auch wenn sie grundsätzlich funktioniert. Es wird in diesem Fall nämlich nicht der korrekte DNS-Name des entsprechenden Servers zurückgegeben, sondern der Servername mit der Zone des DNS-Servers, in die der Server als Host eingetragen wurde. Vor allem in größeren Active Directorys sollten Administratoren darauf achten, die Konfigurationen so vorzunehmen, dass sie auch formal korrekt sind. Das hilft oft, unbedachte Probleme zu vermeiden. Wenn Sie zum Beispiel in der Zone *microsoft.com* einen neuen Eintrag *dc1* für den Domänencontroller *dc1.contoso.com* erstellen, der auf die IP-Adresse des Servers verweist, wird der Name als *dc1.microsoft.com* aufgelöst, obwohl der eigentliche Name des Servers *dc1.contoso.com* ist. Dadurch funktioniert zwar die Auflösung, aber es wird ein falscher Name zurückgegeben.

DNS in Windows Server 2008 installieren

Der Assistent für die Installation von Active Directory kann zwar auch im Rahmen der Einrichtung die DNS-Funktionalität installieren und einrichten, allerdings ist diese Vorgehensweise nicht optimal.

Abbildg. 8.20 DNS-Server für das Active Directory installieren



Zunächst legt der Assistent für DNS-Zone und Active Directory-Daten zwei Zonen an. Außerdem wird keine Reverse-Lookupzone erstellt. Auch aus Gründen des Wissensaufbaus gilt für Windows Server 2008 aus unserer Sicht das Gleiche wie für Windows Server 2003: Legen Sie die DNS-Zonen selbst an. Um DNS auf einem Windows Server 2008 zu installieren, starten Sie den Server-Manager und klicken auf *Rollen*. Klicken Sie anschließend auf den Link *Rollen hinzufügen* und wählen Sie die

Rolle *DNS-Server* aus. Klicken Sie diese Option an und lassen Sie die notwendigen Komponenten installieren. Nach der Installation müssen Sie den Server nicht neu starten. Wollen Sie ein neues Active Directory erstellen, besteht der erste Schritt darin, auf dem ersten geplanten Domänencontroller nach der Installation des Windows Server 2008 zunächst die DNS-Erweiterung zu installieren. Unter Windows Server 2008 wird DNS automatisch installiert und eingerichtet, wenn das Active Directory auf einem Server installiert wird. Dennoch ist die korrekte Vorbereitung einer DNS-Infrastruktur immer noch der bessere Weg. Nach der Installation finden Sie das Verwaltungsprogramm für den DNS-Server unter *Start/Verwaltung/DNS*. Starten Sie die Verwaltung, sehen Sie zunächst die Einträge, die Sie an dieser Stelle zur Verwaltung verwenden (Abbildung 8.21):

- Globale Protokolle und die DNS-Ereignisanzeige
- Forward-Lookupzonen
- Reverse-Lookupzonen
- Bedingte Weiterleitungen

Abbildg. 8.21 Verwaltungskonsole eines DNS-Servers nach der Installation

Standardmäßig werden Sie mit dem lokal installierten DNS-Server verbunden. Erstellen Sie später eine einheitliche Managementkonsole (MMC), können Sie die Verwaltung mehrerer DNS-Server in Ihrem Unternehmen an einer Stelle verbinden. Klicken Sie mit der rechten Maustaste in der Konsole auf den Eintrag *DNS*, können Sie sich mit zusätzlichen DNS-Servern verbinden. Für die Testumgebung werden diese Schritte nicht benötigt. Mit den Knoten *Forward-Lookupzonen* und *Reverse-Lookupzonen* werden die Zonen angelegt, die das Active Directory für seinen Betrieb benötigt. Im Knoten *Globale Protokolle* finden Sie das gleiche Protokoll wie in der Ereignisanzeige des Servers. Über *Bedingte Weiterleitungen* können Sie Anfragen zu bestimmten DNS-Zonen an fest definierte DNS-Server weiterleiten. Unter Windows Server 2003 war diese Einstellung noch in den Eigenschaften des DNS-Servers verfügbar.

Erstellen der notwendigen DNS-Zonen für das Active Directory

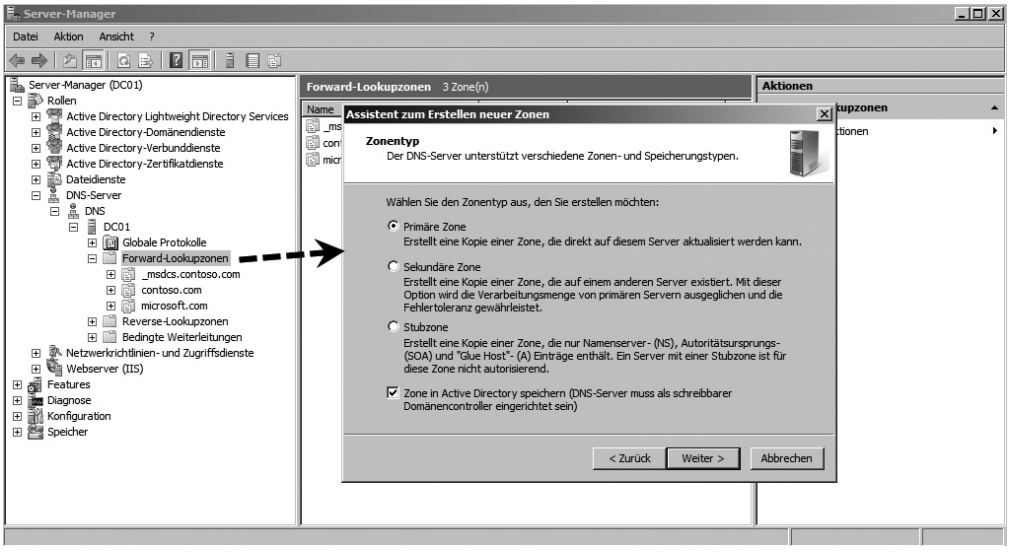
Der nächste Schritt zur Erstellung eines Active Directory besteht in der Erstellung der neuen Zonen, welche die DNS-Domänen von Active Directory verwalten. Starten Sie die DNS-Verwaltung.

Erstellen einer Forward-Lookupzone

Die erste und wichtigste Zone, die Sie auf einem DNS-Server erstellen, ist die *Forward-Lookupzone* der ersten Domäne von Active Directory. Klicken Sie dazu in der MMC mit der rechten Maustaste auf den

Eintrag *Forward-Lookupzonen* und wählen Sie im Kontextmenü den Befehl *Neue Zone* aus. Es startet der Assistent zum Erstellen von neuen Zonen. Im nächsten Fenster können Sie festlegen, welche Art von Zonen Sie erstellen wollen. Wählen Sie die Option *Primäre Zone* aus. Beim Erstellen neuer Domänen im Active Directory werden ausschließlich primäre Domänen benötigt (Abbildung 8.22).

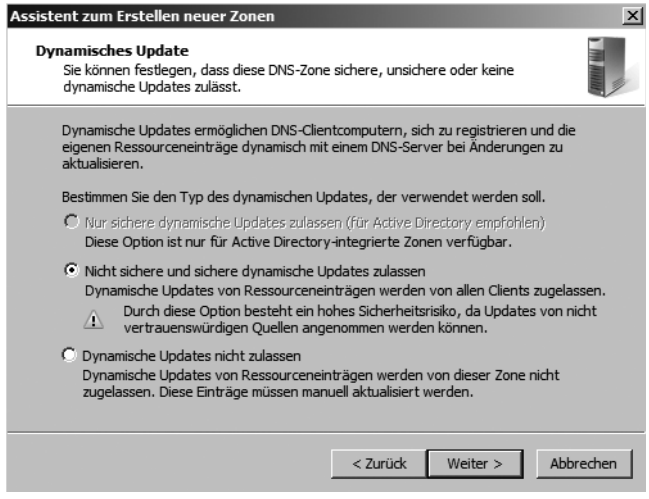
Abbildg. 8.22 Erstellen einer primären Forward-Lookupzone



Auf der nächsten Seite des Assistenten legen Sie den Namen der neuen Zone fest. Wird bereits ein Active Directory betrieben, kann auf einer vorhergehenden Registerkarte eingestellt werden, auf welche Server die Daten der neuen Zone repliziert werden sollen. Hier ist es extrem wichtig, dass Sie als Zonennamen exakt den Namen wählen, den Sie zuvor als DNS-Suffix des Servers eingetragen haben. Das DNS-Suffix des Domänencontrollers wird später in dieser Zone integriert und die erste Active Directory-Domäne speichert ihre SRV-Records ebenfalls in dieser Domäne. In diesem Beispiel lautet die Zone *contoso.com*. Im Anschluss erscheint das Fenster, in dem Sie die Erstellung einer neuen Datei für die Zone bestätigen müssen. Sie könnten an dieser Stelle den Namen der Datei zwar ändern, sollten ihn aber möglichst immer so belassen, wie er festgelegt wurde.

Im nächsten Fenster müssen Sie die dynamischen Updates der DNS-Zone festlegen. DNS-Server unter Windows Server 2008 arbeiten mit dynamischen Updates. Das heißt, alle Servernamen und IP-Adressen sowie die SRV-Records von Active Directory werden automatisch in diese Zone eingetragen. Ohne dynamische Updates können Sie in einer Zone kein Active Directory integrieren. Der Installationsassistent von Active Directory muss in einer Zone dutzende Einträge automatisch durchführen können. Aktivieren Sie daher im Fenster die Option *Nicht sichere und sichere dynamische Updates* zulassen (Abbildung 8.23). Sichere Updates können Sie nach der Erstellung von Active Directory konfigurieren. Vor der Installation ist diese Einstellung deaktiviert.

Abbildg. 8.23 Aktivieren der dynamischen Updates für eine Zone

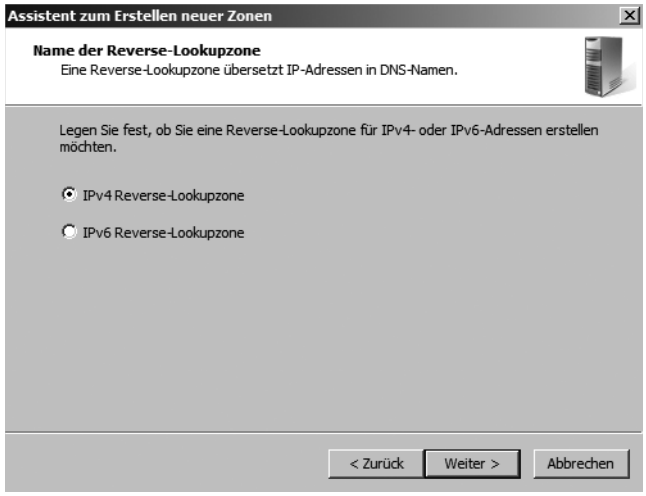


Im Anschluss erhalten Sie nochmals eine Zusammenfassung Ihrer Angaben. Danach wird die Zone erstellt und in der MMC angezeigt. Innerhalb der Zone sollte bereits der lokale Server als *Host (A)* mit seiner IP-Adresse registriert sein. Diese Registrierung findet nur statt, wenn das primäre DNS-Suffix des Servers mit der erstellten Zone übereinstimmt und die dynamische Aktualisierung zugelassen wurde. In den IP-Einstellungen des Servers muss außerdem der DNS-Server eingetragen sein, der die Zone verwaltet.

Erstellen einer Reverse-Lookupzone

Im Anschluss an die *Forward-Lookupzone* sollten Sie eine *Reverse-Lookupzone* erstellen. Diese Zone ist dafür zuständig, IP-Adressen in Rechnernamen zu übersetzen. Diese Zonen werden zwar für den stabilen Betrieb eines Active Directory nicht zwingend benötigt, gehören aber dennoch zu einer ordentlichen Namensauflösung im Netzwerk. Klicken Sie mit der rechten Maustaste auf den Knoten *Reverse-Lookupzone* und wählen Sie im Kontextmenü den Befehl *Neue Zone* aus. Auf der ersten Seite des Assistenten wählen Sie wieder die Option *Primäre Zone*. Auf der nächsten Seite können Sie festlegen, ob Sie eine IPv4- oder eine IPv6-Reverse-Lookupzone anlegen wollen. Da Windows Server 2008 neben IPv4 auch IPv6 unterstützt, wird dieses neue Dialogfeld eingeblendet. In den meisten Netzwerken wird derzeit noch mit IPv4 gearbeitet. Aus diesem Grund sollten Sie bei einer Testumgebung auch eine IPv4-Reverse-Lookupzone anlegen. Legen Sie auf der nächsten Seite des Assistenten den IP-Bereich fest, der durch diese Zone verwaltet werden soll. Tragen Sie zur Definition des IP-Bereiches unter *Netzwerkkennung* den IP-Bereich ein, den Sie verwalten wollen. Für jeden eigenständigen IP-Bereich müssen Sie eine eigene Zone anlegen. Verwalten Sie ein B-Klasse-Netz (255.255.0.0), können Sie auch einfach die letzte Stelle leer lassen. Hat sich bei einer Zone, die Sie für die Netzwerkkennung *10.0.* konfiguriert haben, ein Server mit der IP-Adresse *10.0.1.20* registriert, legt der DNS-Server automatisch einen Ordner *1* unter der Zone *10.0* an. In diesem Ordner wird der Hosteintrag des Servers registriert. Alle weiteren IP-Adressen, wie zum Beispiel *10.0.2.20*, werden ebenfalls automatisch als neuer Ordner angelegt. Sie müssen daher bei einem B-Klasse-Netzwerk nicht manuell für jedes Unternetz eine eigene Zone anlegen. Nur wenn sich der IP-Bereich vollständig unterscheidet, zum Beispiel *192.168.* und *10.1.*, müssen Sie zwei getrennte Zonen anlegen.

Abbildg. 8.24 Windows Server 2008 ermöglicht das Anlegen von IPv6-Reverse-Lookupzonen



Auf der nächsten Seite des Assistenten legen Sie den Zonennamen fest. Danach müssen Sie die dynamischen Updates zulassen und die Zusammenfassung bestätigen. Als Nächstes wird die neue Zone erstellt. Hat sich der Server noch nicht automatisch registriert, können Sie über die Eingabe des Befehls *ipconfig /registerdns* in der Befehlszeile die dynamische Registrierung anstoßen. Danach sollte die IP-Adresse des Servers in der Zone registriert sein.

Überprüfung und Fehlerbehebung der DNS-Einstellungen

Bevor Sie Active Directory auf dem Server installieren, sollten Sie sicherstellen, dass alle DNS-Einstellungen korrekt vorgenommen wurden. Überprüfen Sie, ob sich der Server sowohl in der Forward- als auch in der Reverse-Lookupzone korrekt eingetragen hat. Öffnen Sie danach eine Befehlszeile und geben Sie den Befehl *nslookup* ein. Die Eingabe des Befehls darf keinerlei Fehlermeldungen verursachen. Es muss der richtige FQDN des DNS-Servers und seine IP-Adresse angezeigt werden. Sollte das nicht der Fall sein, gehen Sie Schritt für Schritt vor, um den Fehler einzugrenzen:

1. Sollte ein Fehler erscheinen, versuchen Sie es einmal mit dem Befehl *ipconfig /registerdns* in der Befehlszeile.
2. Sollte der Fehler weiterhin auftreten, überprüfen Sie, ob das primäre DNS-Suffix auf dem Server mit dem Zonennamen übereinstimmt.
3. Stellen Sie als Nächstes fest, ob die IP-Adresse des Servers stimmt und der Eintrag des bevorzugten DNS-Servers auf die IP-Adresse des Servers zeigt.
4. Überprüfen Sie in den Eigenschaften der Zone, ob die dynamische Aktualisierung zugelassen wird und ändern Sie gegebenenfalls die Einstellung, damit die Aktualisierung stattfinden kann. Die Eigenschaften der Zonen erreichen Sie, wenn Sie mit der rechten Maustaste auf die Zone klicken und die *Eigenschaften* auswählen.
5. Treten keine Fehler auf, können Sie mit der Erstellung von Active Directory auf diesem Server beginnen.

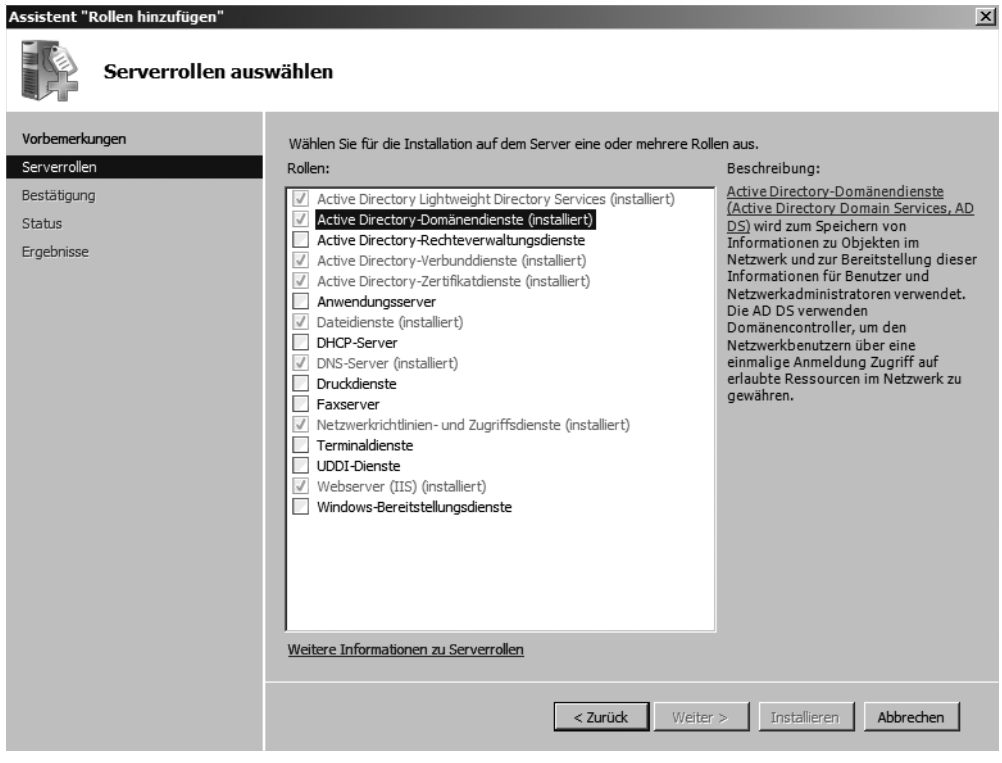
Installieren der Active Directory-Domänendienste-Rolle

Nachdem Sie diese Vorbereitungen getroffen haben, können Sie das Active Directory auf dem Server installieren. Dazu stehen Ihnen zwei Möglichkeiten zur Verfügung.

Installieren von Active Directory über den Server-Manager

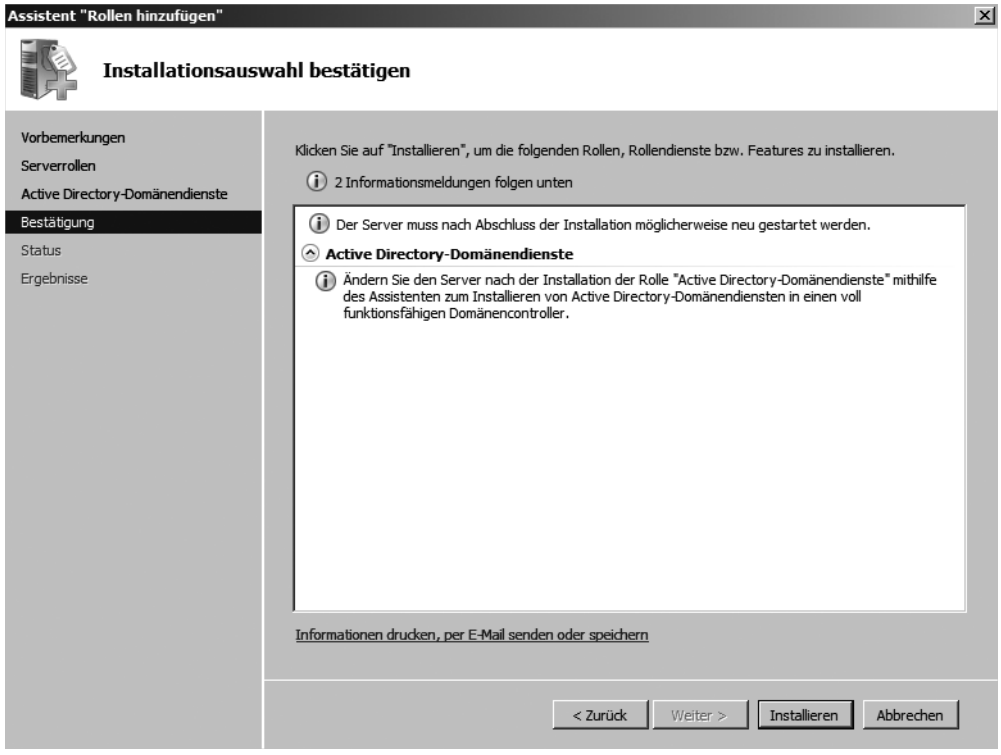
Starten Sie den Server-Manager, klicken Sie in der Konsolenstruktur auf *Rollen* und dann im rechten Fensterbereich auf den Link *Rollen hinzufügen*. Im Anschluss startet der Assistent zum Hinzufügen von neuen Rollen. Bestätigen Sie das Startfenster des Assistenten. Auf der nächsten Seite wählen Sie die Rolle *Active Directory-Domänendienste* aus (Abbildung 8.25). Diese Maßnahme entspricht dem Befehl *dcpromo*, der bereits unter Windows Server 2003 genutzt wurde und auch noch unter Windows Server 2008 unterstützt wird. Wir kommen bei der Installation eines zusätzlichen Domänencontrollers noch auf diese Möglichkeit zurück.

Abbildg. 8.25 Auswählen und installieren der Rolle *Active Directory-Domänendienste*



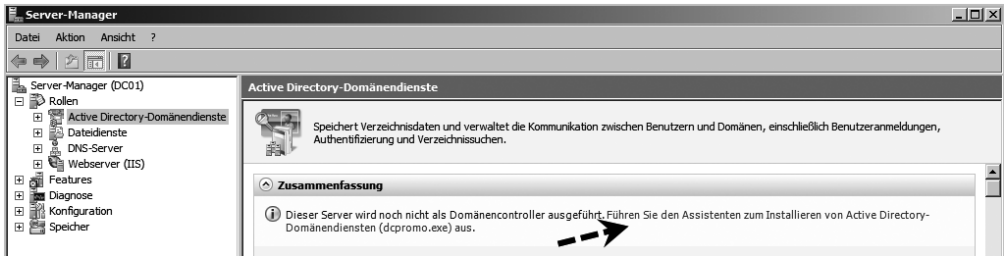
Klicken Sie zur Installation der Rolle auf *Weiter*. Es erscheint ein neues Fenster mit Hinweisen zu Active Directory, welches Sie ebenfalls mit *Weiter* bestätigen können. Auf der nächsten Seite des Assistenten starten Sie über die Schaltfläche *Installieren* die Installation der Rolle auf dem Server (Abbildung 8.26).

Abbildg. 8.26 Starten der Active Directory-Installation auf dem Domänencontroller



Nach kurzer Zeit wird die Installation der Rolle abgeschlossen. Anschließend startet normalerweise der Assistent zur Einrichtung des Domänencontrollers. An dieser Stelle sind noch keine Konfigurationen für die Domäne durchgeführt worden, sondern Sie haben lediglich die notwendigen Dateien zur Erstellung eines Active Directory auf dem Server installiert. Startet der Assistent zur Einrichtung der Domäne nicht automatisch, klicken Sie im Server-Manager unter *Rollen/Active Directory-Domänendienste* in der Mitte der Konsole auf den Link *Führen Sie den Assistenten zum Installieren von Active Directory-Domänendiensten (dcpromo.exe) aus* (Abbildung 8.27). Dieser Link startet den gleichen Assistenten, den Sie auch, wie unter Windows Server 2003, über *dcpromo* starten können. Erst durch die Ausführung dieses Assistenten wird der Server zum Domänencontroller heraufgestuft. Unter Windows Server 2008 kann dieser Assistent noch immer verwendet werden. Beim Aufrufen wird die Rolle *Active Directory-Domänendienste* automatisch nachinstalliert, wenn sich die entsprechenden Dateien noch nicht auf dem Server befinden.

Abbildg. 8.27 Starten des Assistenten für die Installation von Active Directory



Installieren Sie das Active Directory über den bekannten Weg in der Befehlszeile mit *dcpromo*, ist der Ablauf für die Einrichtung von Active Directory, der nachfolgend beschrieben wird, identisch mit der Einrichtung über den Server-Manager. Fortgeschrittene Benutzer werden den Weg über *dcpromo* bevorzugen. Starten Sie die Einrichtung von Active Directory über *dcpromo*, überprüft der Assistent, ob die notwendigen Daten für das Active Directory installiert wurden und installiert diese gegebenenfalls nach. Nach der Installation der Rolle *Active Directory-Domänendienste* wird diese auch über diesen Weg im Server-Manager nach der Einrichtung angezeigt. Es ist also nicht zwingend notwendig, vor der Ausführung von *dcpromo* die Rolle *Active Directory-Domänendienste* zu installieren. Aktivieren Sie das Kontrollkästchen *Installation im erweiterten Modus verwenden*, damit Sie auch alle notwendigen Einstellungen für Ihre Domäne konfigurieren können (Abbildung 8.28).

Abbildg. 8.28 Beim Starten des Assistenten für die Erstellung von Active Directory kann der erweiterte Modus aktiviert werden

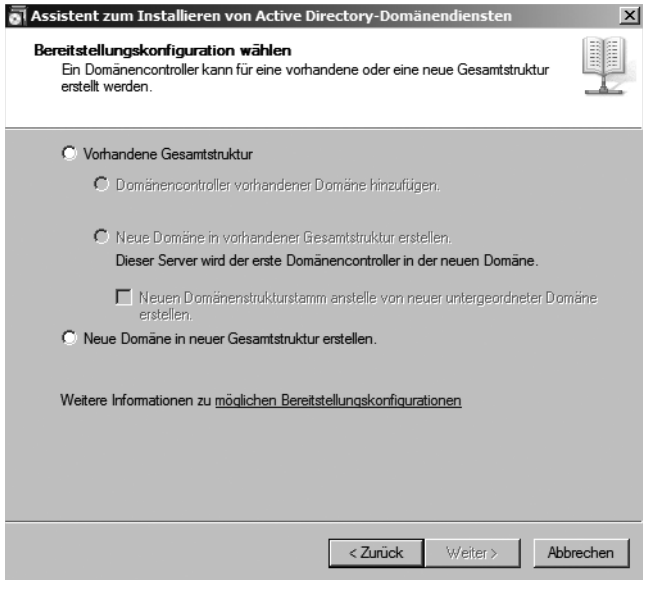
TIPP Wird *dcpromo* über die Befehlszeile gestartet, kann mit der Option *dcpromo /adv* gleich in den erweiterten Modus gewechselt werden.

Durch die Aktivierung des erweiterten Modus können Sie mit dem Assistenten noch folgende Funktionen einstellen:

- Erstellen von neuen Domänenstrukturen
- Verwenden eines Sicherungsmediums für die Replikation von Active Directory, um Netzwerkverkehr im WAN zu sparen
- Auswählen des Quell-Domänencontrollers für die Installation
- Anpassen des NetBIOS-Namens der Domäne
- Konfiguration der Richtlinien für die Kennwortreplikation für RODCs

Auf der nächsten Seite des Assistenten legen Sie fest, wie das Active Directory installiert werden soll. Da Sie die erste Domäne für Ihre Gesamtstruktur erstellen, wählen Sie die Option *Neue Domäne in neuer Gesamtstruktur* aus. Sie erstellen durch diese Auswahl eine neue Domäne und auch die dazugehörige Gesamtstruktur. Insgesamt gibt es im Active Directory die drei Container *Gesamtstruktur*, *Struktur* und *Domäne*.

Abbildg. 8.29 Installation von Active Directory unter Windows Server 2008



Active Directory-Gesamtstruktur (Forest)

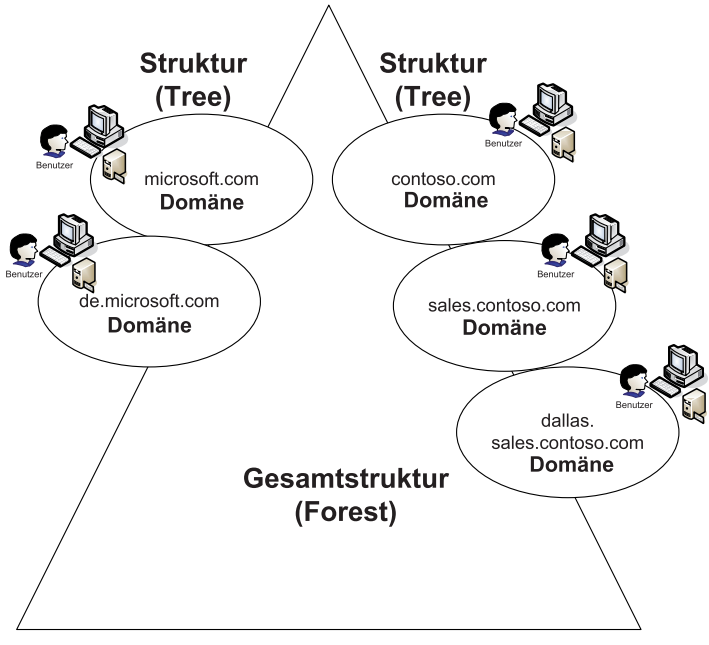
Ein Active Directory kann aus mehreren selbstständigen Domänen bestehen, die dennoch zu einer großen gemeinsamen Organisation, auch Gesamtstruktur genannt, gehören. Alle verbundenen Domänen einer Gesamtstruktur teilen sich eine Datenbank. Eine Gesamtstruktur (Forest) ist die Grenze des Verzeichnisdienstes eines Unternehmens, in dem einheitliche Berechtigungen vergeben und delegiert werden können. Für Anwender ändert sich beim Umgang mit der Domäne so gut wie

nichts. Sie können mehrere Domänen in einer Gesamtstruktur hierarchisch aufbauen. Jede Domäne in einem Active Directory ist eine eigene Partition im Verzeichnis. Jede Partition wird von unterschiedlichen Domänencontrollern verwaltet. Diese Partitionierung erfolgt automatisch.

Domänenstrukturstamm (Tree)

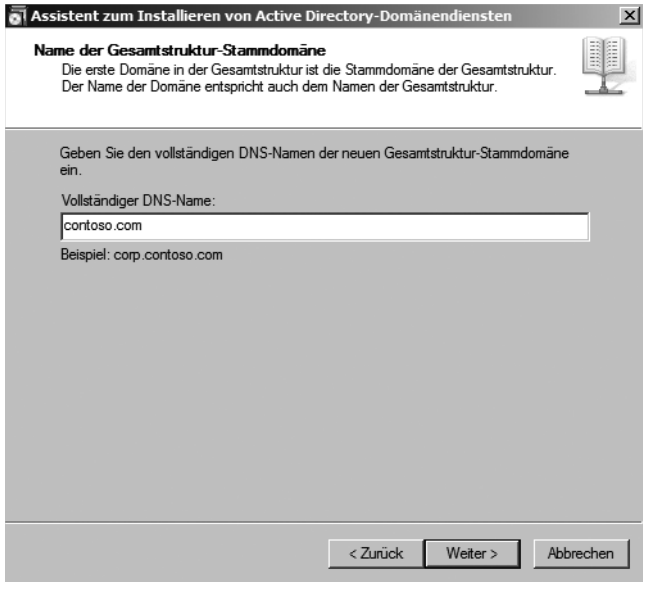
Domänen werden im Active Directory zu Strukturen (Trees) zusammengefasst. Eine Struktur muss über einen einheitlichen Namensraum verfügen. Heißt eine Struktur beispielsweise *contoso.com*, kann es innerhalb dieser Struktur weitere Einheiten geben, wie beispielsweise *sales.contoso.com*, *marketing.contoso.com* und *dallas.marketing.contoso.com*. In einer Struktur (Tree) werden automatisch gegenseitige Vertrauensstellungen zwischen den beteiligten Domänen erzeugt. Darüber hinaus kann in einer Struktur eine Suche über mehrere Domänen hinweg erfolgen. Eine Active Directory-Gesamtstruktur (Forest), kann aus mehreren Strukturen (Trees) zusammengesetzt sein. Jede Gesamtstruktur besteht aus mindestens einer Struktur. Der ersten Domäne eines Active Directory kommt eine besondere Bedeutung zu. Da sie die erste Domäne ist, bildet sie die erste Struktur von Active Directory und ist gleichzeitig die Stamm-(Root)-Domäne der Gesamtstruktur. Planen Sie ein Active Directory mit nur einer Domäne, bildet diese Domäne die Gesamtstruktur, die erste und einzige Struktur und die Stamm-(Root)-Domäne von Active Directory. Die Domänen einer Struktur (Tree) teilen sich einen so genannten Namensraum. Unter Windows NT hatten Domänen lediglich einen NetBIOS-Namen mit bis zu 15 Zeichen. Im Active Directory gibt es diese NetBIOS-Namen auch. Wichtiger sind jedoch die DNS-Namen, die jede Domäne einem DNS-Namensraum eindeutig zuweisen. Als Struktur wird ein Namensraum bezeichnet, der vollkommen eigenständig ist. In der Abbildung 8.30 bilden zum Beispiel die Domänen *microsoft.com* und *de.microsoft.com* jeweils eine eigenständige Domäne innerhalb derselben Struktur (Tree). Auch die Domänen *contoso.com*, *sales.contoso.com* und *dallas.sales.contoso.com* sind eine eigene Struktur. Die beiden Strukturen *contoso.com* und *microsoft.com* sind trotz ihrer vollständig eigenständigen Namensräume Teil einer gemeinsamen Active Directory-Gesamtstruktur.

Abbildg. 8.30 Aufbau einer Gesamtstruktur mit mehreren Strukturen, Domänen und untergeordneten Domänen



Jede Domäne kann beliebige untergeordnete Domänen (Child-Domänen genannt) haben, denen ebenfalls weitere Domänen untergeordnet werden. Alle Domänen eines Namensraums werden als eigenständige Struktur (neuer Begriff auch Domänenstrukturstamm) bezeichnet. Child-Domänen sind wie die übergeordneten Domänen vollkommen eigenständig, teilen sich jedoch einen Namensraum und eine Active Directory-Gesamtstruktur. Sie bilden jeweils eigene Partitionen im Active Directory, die durch getrennte Domänencontroller verwaltet werden. Auf der nächsten Seite des Assistenten legen Sie den DNS-Namen der neuen Domäne fest. Tragen Sie hier genau den gleichen Namen ein, den Sie bereits bei dem primären DNS-Suffix des Domänencontrollers verwendet haben, in diesem Beispiel *contoso.com* (Abbildung 8.31).

Abbildg. 8.31 Festlegen des DNS-Namens der Domäne



Im nächsten Fenster müssen Sie den NetBIOS-Namen der neuen Domäne festlegen (Abbildung 8.32). Dieser Name wird zum Beispiel in den Anmeldemasken und den meisten Authentifizierungsfenstern verwendet. Sie sollten möglichst einen NetBIOS-Namen wählen, der auch zum DNS-Namen passt, am besten den DNS-Namen ohne die letzte Endung, in diesem Beispiel also *CONTOSO*.

Abbildg. 8.32 Festlegen des NetBIOS-Namens einer neuen Domäne

Auf der nächsten Seite des Assistenten legen Sie die Funktionsebene der Gesamtstruktur fest. Ein Active Directory kann unter verschiedenen Betriebsmodi betrieben werden:

- Betriebsmodus der einzelnen Domänen in der Gesamtstruktur
- Betriebsmodus der Gesamtstruktur

Während die Funktionsebene der Gesamtstruktur nur einmal verändert werden muss, müssen Sie für jede Domäne der Gesamtstruktur deren eigene Funktionsebene anpassen. Diese beiden Ebenen können unabhängig voneinander jeweils drei verschiedene Betriebsmodi annehmen. Diese drei Betriebsmodi haben keine Kompatibilitätsunterschiede für Mitgliedsserver oder -PCs. Wichtig ist der Modus nur für die integrierten Domänencontroller.

- **Windows 2000** In diesem Modus können nur noch Windows 2000-, Windows Server 2003- und Windows Server 2008-Domänencontroller die Domäne verwalten. Es dürfen aber weiterhin Windows NT 4.0-Server als Mitglied betrieben werden. Ab diesem Modus können universelle Gruppen erstellt werden und die SID-History wird unterstützt. Bei der SID-History können den Benutzerkonten mehrere SIDs aus anderen Domänen zugeordnet werden. Sicherheitsgruppen können in diesem Modus zu Verteilergruppen umfunktioniert werden. Ab diesem Modus kann auch Exchange Server 2007 in der Domäne installiert werden.
- **Windows Server 2003** Ab diesem Modus können Domänen in der Gesamtstruktur umbenannt und umstrukturiert werden. Es können Gesamtstruktur-übergreifende Vertrauensstellungen erstellt werden. Sofern in einer Gesamtstruktur keine Windows 2000-Domänencontroller unterstützt werden müssen, sollten Sie so schnell wie möglich die Funktionsebene der Domänen und der Gesamtstruktur auf den Windows Server 2003-Modus hochsetzen. Sie erhalten dadurch keinerlei Nachteile, eröffnen sich aber erst dann die vollständigen Möglichkeiten von Active Directory. In diesem Modus werden schreibgeschützte Domänencontroller (RODC) unterstützt,

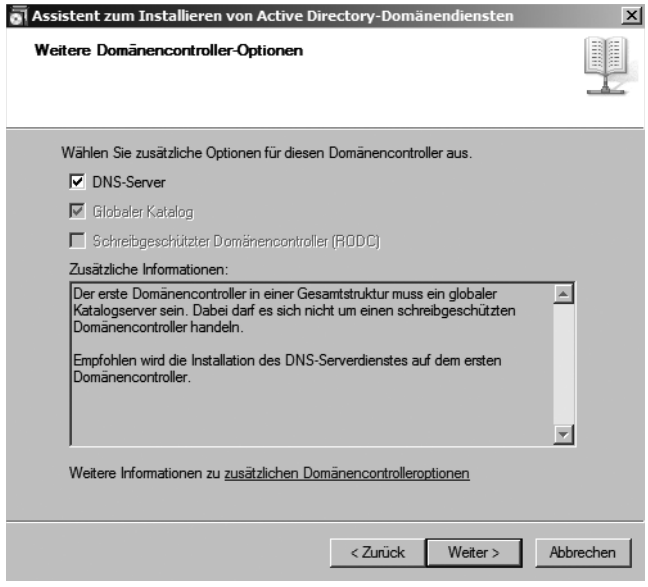
sofern sich der PDC-Emulator auf einem Domänencontroller unter Windows Server 2008 befindet.

- **Windows Server 2008** Dieser Modus hat funktional keine großen Unterschiede zum Windows Server 2003-Modus. Allerdings wird durch Auswahl dieses Modus sichergestellt, dass alle Domänen der Gesamtstruktur im Windows Server 2008-Modus betrieben werden. In diesem Modus werden Kennwortrichtlinien für mehrere OUs unterstützt. Außerdem wird in diesem Modus zu Replikation des Sysvol-Verzeichnisses DFS genutzt, was wesentlich performanter und stabiler funktioniert. In diesem Modus kann der Kerberosverkehr mit AES 128 oder 256 verschlüsselt werden.

Abbildg. 8.33 Festlegen der Funktionsebene der Gesamtstruktur

Auf der nächsten Seite des Assistenten konfigurieren Sie, dass der Domänencontroller auch zum DNS-Server konfiguriert wird. Der erste Domänencontroller in der Gesamtstruktur sollte möglichst auch immer DNS-Server sein. Der neue Domänencontroller wird darüber hinaus auch zwingend der erste globale Katalog Server (siehe den Abschnitt »Verwalten der Betriebsmasterrollen von Domänencontrollern« weiter hinten in diesem Kapitel). Auf dieser Seite können Sie auch festlegen, ob ein Domänencontroller zum Read-Only Domänencontroller (RODC) werden soll. Hierbei wird auf dem Domänencontroller ein Replikat der Active Directory-Datenbank gespeichert, die keinerlei Änderungen akzeptiert. Außerdem lässt sich die Berechtigung zur RODC-Verwaltung an einen beliebigen Domänenbenutzer delegieren, um beispielsweise Aktualisierungen von Gerätetreibern vor Ort rasch durchführen zu können. Der erste Domänencontroller einer Gesamtstruktur kann nicht zum RODC konfiguriert werden, aus diesem Grund ist diese Option, genau wie die Auswahl zum globalen Katalog, deaktiviert. Wir kommen bei der Integration eines zusätzlichen Domänencontrollers noch auf dieses Thema zurück.

Abbildg. 8.34 Konfigurieren der Optionen für einen Domänencontroller



Nachdem Sie die Installation des DNS-Servers ausgewählt haben, erscheint eine weitere Warnmeldung, die etwas verwirrend ist. Obwohl dem Server eine statische IP-Adresse zugewiesen wurde, erscheint die Meldung, dass eine dynamische IP-Adresse verwendet wird. Das liegt daran, dass für die IPv6-Verbindung meistens dynamische Einstellungen verwendet werden (siehe Kapitel 7). Solange Sie der IPv4-Verbindung eine statische Adresse zugewiesen haben, können Sie die Meldung mit *Ja* bestätigen.

Als Nächstes erscheint eine Meldung, dass DNS bereits installiert ist und der Assistent möchte eine Delegierung für die DNS-Zone erstellen. Diese Meldung erscheint allerdings nur dann, wenn Sie nicht, wie zuvor beschrieben, vor der Installation von Active Directory, die Rolle *DNS-Server* installiert haben und die Zonen eingerichtet wurden. Diese Meldung besagt in aller Kürze, dass der DNS-Server, den Sie in den IP-Einstellungen konfiguriert haben, nicht in der Lage ist, die DNS-Zone der neuen Active Directory-Domäne aufzulösen. Da Sie derzeit den ersten DNS-Server und Domänencontroller installieren, wird diese Zone natürlich erst erstellt. Aus diesem Grund erscheint die Meldung, die Sie mit *Nein* bestätigen. In diesem Fall übernimmt der Assistent nicht die Einrichtung des DNS-Servers, sondern integriert die Daten für das Active Directory direkt in die Zone, die zuvor angelegt wurde.

Abbildg. 8.35 Erstellen einer delegierten DNS-Zone für Active Directory

Diese Meldung hat ihren Ursprung bei der Erweiterung eines bestehenden Active Directory um zusätzliche Domänen. Wenn Sie eine untergeordnete Domäne erstellen wollen, zum Beispiel die Domäne *de* unterhalb der Domäne *contoso.com*, haben Sie zwei Möglichkeiten, die Namensauflösung und das DNS-Konzept zu erstellen. Sie können auf den primären DNS-Servern der Zone *contoso.com* eine Unterdomäne *de* erstellen. In diesem Fall wird die neue Domäne unterhalb der Domäne *contoso.com* angezeigt. Alle DNS-Server, welche die Zone *contoso.com* verwalten, sind auch für die Domäne *de.contoso.com* zuständig. Haben Sie die neue Domäne erstellt, müssen Sie als Nächstes auf dem ersten Domänencontroller der neuen untergeordneten Domäne in den IP-Einstellungen den DNS-Server der Hauptzone eintragen. Wenn sich die Domäne in einer anderen Niederlassung befindet, können Sie nach der Erstellung der neuen untergeordneten Domäne die Einstellungen auf den lokalen DNS-Server umstellen. Da bei den meisten Active Directorys die DNS-Zonen im Active Directory integriert sind, können Sie vor dem Heraufstufen eines Domänencontrollers diesen noch nicht zum DNS-Server innerhalb eines Active Directory konfigurieren. Erstellen Sie eine neue untergeordnete Domäne und ist in den IP-Einstellungen des neuen Domänencontrollers der DNS-Server der Hauptzone eingetragen, können Sie nach der Heraufstufung die komplette Zone zum DNS-Server in der untergeordneten Domäne replizieren lassen.

Vor allem bei größeren Unternehmen kann die Erstellung von untergeordneten DNS-Domänen Probleme bereiten. Wenn zum Beispiel in der Zentrale in Dallas die Root-Domäne *contoso.com* verwaltet werden soll, aber die Administratoren in der deutschen Domäne *de* diese Zone aus Sicherheitsgründen nicht verwalten sollen, sondern nur ihre eigene, können Sie nicht einfach eine Unterdomäne anlegen, da sonst jeder Administrator eines DNS-Servers Änderungen in der ganzen Zone vornehmen kann. Durch fehlerhafte Änderungen kann dadurch ein weltweites Active Directory schnell außer Funktion gesetzt werden. Aus diesem Grund hat Microsoft in seinen DNS-Servern die Delegation von Domänen integriert. Gehen Sie dazu folgendermaßen vor:

Auf dem DNS-Server der neuen untergeordneten Domäne wird eine eigene Zone *de.contoso.com* angelegt und konfiguriert. Zukünftig verwalten die Administratoren der Domäne *de* ihre eigene Zone *de.contoso.com*.

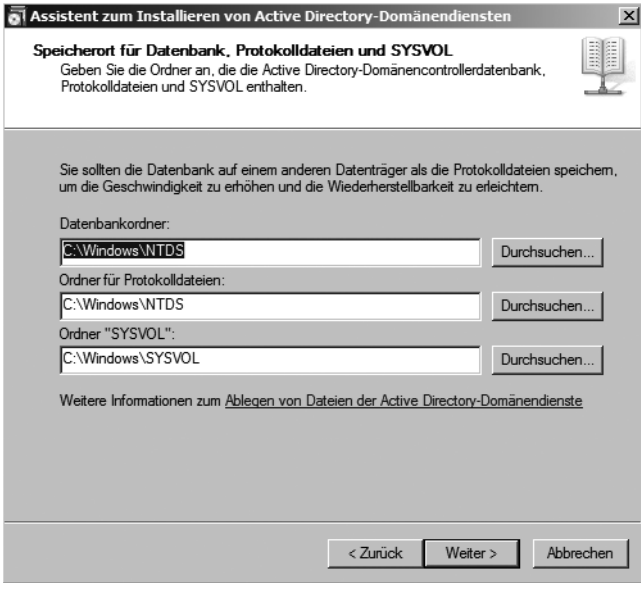
Damit die DNS-Server und Domänencontroller der restlichen Niederlassungen ebenfalls Verbindung zu der Zone *de.contoso.com* aufbauen können, wird in der Hauptzone *contoso.com* eine so genannte *Delegation* eingerichtet, in der festgelegt wird, dass nicht die DNS-Server der Zone *contoso.com* für die Domäne *de.contoso.com* zuständig sind, sondern die DNS-Server der Niederlassung in Deutschland. Durch diese Konfiguration können weiterhin alle Namen aufgelöst werden, aber die Administratoren der Niederlassungen können nur ihre eigenen Zonen verwalten, nicht die Zonen der anderen Niederlassungen. Nachdem Sie die Delegation eingerichtet haben, wird die Zone unterhalb der Hauptzone als delegiert angezeigt. Dieser DNS-Server ist nicht mehr für diese Zone verantwortlich, kann aber Namen in der Domäne durch die Delegation auflösen, indem er Anfragen an die DNS-Server weiterleitet, die in der Delegation angegeben sind.

Auf Dauer kann allerdings diese Konfiguration auch kompliziert werden. Einfacher ist es, innerhalb eines Namensraums möglichst alle neuen Domänen als Unterdomänen anzulegen. Stellen Sie bei der Replikation der Hauptzone ein, dass diese Zone auf alle DNS-Server von Active Directory repliziert wird. Dadurch ist sichergestellt, dass in jeder Niederlassung alle notwendigen Server aufgelöst werden können. Sie ersparen sich dadurch komplizierte Verwaltungsvorgänge. Wenn jedoch in den Niederlassungen Administratoren sitzen, die Ihre eigenen Domänen verwalten sollen, arbeiten Sie mit der Delegation. Geben Sie die delegierte Domäne ein, müssen Sie nur die neue Zone eingeben, also in diesem Fall *de*. Den restlichen Domänennamen, also hier *contoso.com*, wird durch den Assistenten automatisch eingerichtet. Geben Sie auf der letzten Seite des Assistenten die IP-Adresse des DNS-Servers ein, der zukünftig diese Zone verwalten soll. Sie können jederzeit in den Zoneneinstellungen zusätzliche DNS-Server für die Zone eintragen.

Nachdem die Delegation erstellt wurde, können alle PCs und Server, die den DNS-Server der Hauptzone abfragen, auch die Namen der Server in den untergeordneten Zonen auflösen. Sobald der DNS-Server der Zone *contoso.com* eine Anfrage für die Domäne *de.contoso.com* erhält, gibt er diese Abfrage an die DNS-Server weiter, die in der Delegation hinterlegt sind. Die Zone *de.contoso.com* wird auf den DNS-Servern, welche die Zone verwalten, genau so verwaltet wie die Zone *contoso.com* auf dem Haupt-DNS-Server. Die Zone sollte in das Active Directory integriert und zu den anderen Domänencontrollern der Niederlassung repliziert werden. Die Delegation auf den DNS-Servern der Zone *contoso.com* hat keinerlei Auswirkungen auf die Verwaltung der Zone *de.contoso.com*. Die Delegation ist quasi nur eine Verknüpfung zu den DNS-Servern in der Zone *de.contoso.com*. In der Ansicht der DNS-Verwaltung auf den DNS-Servern von *contoso.com* werden die Delegationen grau angezeigt. Delegationen können jederzeit gelöscht und wieder angelegt werden, da Sie keinerlei Auswirkungen auf die Zone haben, zu der sie delegiert sind.

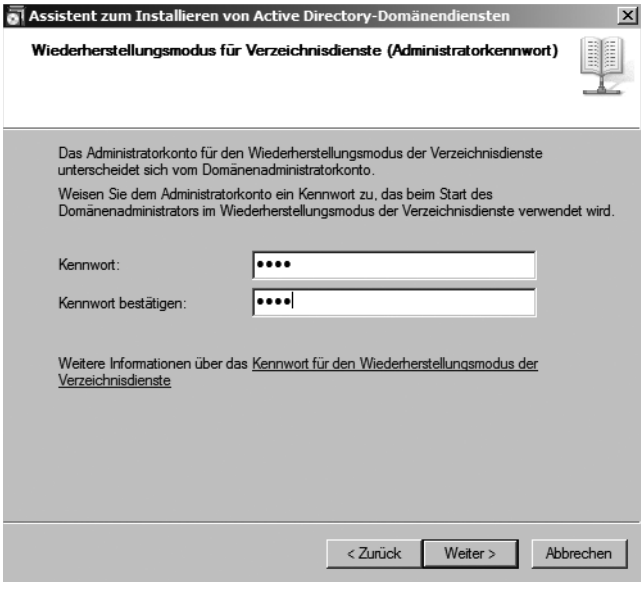
In diesem Fenster werden Sie also gefragt, ob in der übergeordneten DNS-Zone eine Delegation zur aktuellen Domäne durchgeführt werden soll. Dies spielt nur bei der Installation von untergeordneten Domänen eine Rolle. Da Sie die erste Domäne in der Gesamtstruktur erstellen, können Sie an dieser Stelle die Option *Nein, keine DNS-Delegierung erstellen* auswählen. In diesem Fall erstellt der Assistent die notwendigen Daten in der Zone, die Sie erstellt haben. Im nächsten Fenster legen Sie den Speicherort der Datenbank und der Protokolle fest, die das Active Directory zum Speichern der Informationen benötigt (Abbildung 8.36). Sie sollten hier den Ordner an der Stelle belassen, die vorgeschlagen wird. Im Anschluss müssen Sie noch den Ordner festlegen, der als *netlogon*- und *sysvol*-Freigabe verwendet wird. In diesem Ordner werden die Anmeldeskripts und später die Gruppenrichtlinien gespeichert. Belassen Sie auch an dieser Stelle den Standardpfad, da eine Änderung keinen Sinn ergeben würde.

Abbildg. 8.36 Festlegen des Speicherortes für die Active Directory-Datenbank und das *SYSVOL*-Verzeichnis



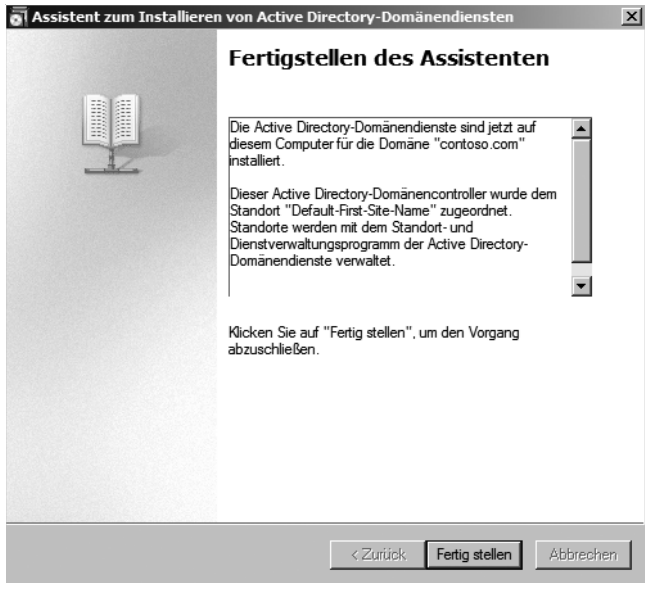
Im nächsten Fenster legen Sie das Kennwort für den Verzeichnisdienstwiederherstellungsmodus fest (Abbildung 8.37). In diesem Modus können Sie einzelne Objekte aus dem Active Directory oder auch ein ganzes Active Directory wiederherstellen.

Abbildg. 8.37 Festlegen des Kennwortes für die Verzeichnisdienst-Wiederherstellung



Anschließend erhalten Sie eine Zusammenfassung angezeigt und der Assistent beginnt mit seiner Arbeit. Sie können den Server automatisch neu starten lassen, nachdem die Installation durchgeführt wurde, oder Sie können die Installation manuell durchführen. Nachdem Sie die Installation abgeschlossen haben, können Sie den Server neu starten. Unter Umständen erhalten Sie noch eine Fehlermeldung angezeigt, in welcher der Assistent Ihnen mitteilt, dass keine DNS-Zone erstellt werden kann, da Sie bereits eine Zone mit der gleichen Bezeichnung erstellt haben. Bestätigen Sie diese Meldung. Der Assistent integriert in diesem Fall die notwendigen Daten von Active Directory in Ihre bereits erstellte Zone.

Abbildg. 8.38 Abschließen der Installation



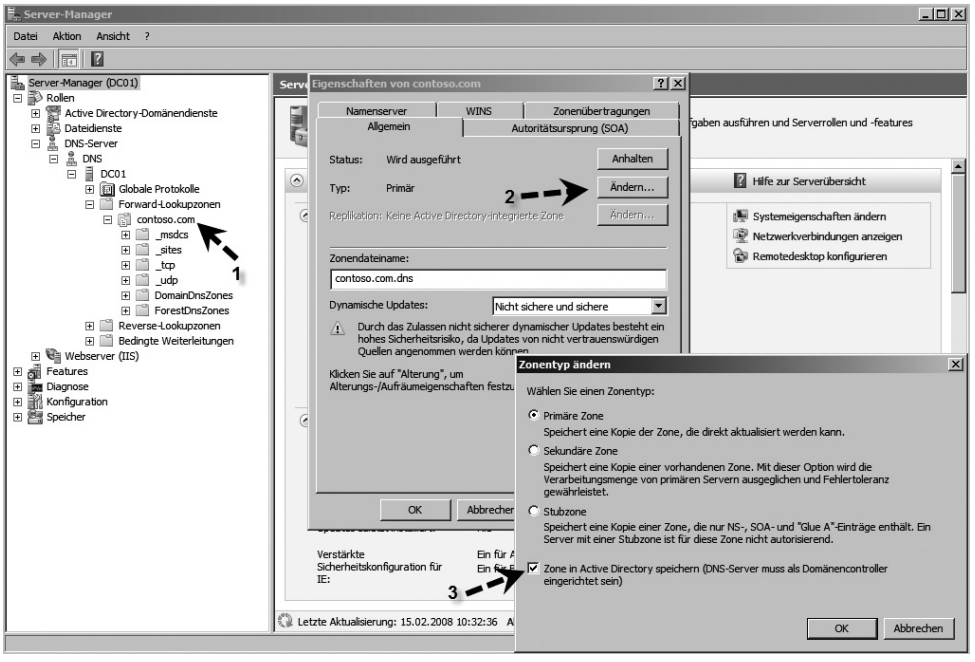
DNS in das Active Directory integrieren und sichere Updates konfigurieren

Die erste Maßnahme, die Sie nach der Installation von Active Directory durchführen sollten, ist die Integration der DNS-Zonen in das Active Directory. Durch diese Integration werden die kompletten Daten der DNS-Zonen über die Active Directory-Replikation verteilt. Haben Sie die Installation des DNS-Servers nicht manuell vorgenommen, sondern durch den Assistenten für das Active Directory, sind die Zonen bereits automatisch in das Active Directory integriert. Um die DNS-Zonen-Daten manuell in das Active Directory zu integrieren, rufen Sie zunächst das DNS-Snap-In auf. Erweitern Sie die Zone, sehen Sie die Erweiterungen, die das Active Directory hinzugefügt hat (Abbildung 8.39). In den einzelnen Unterdomänen der Zone finden Sie die verschiedenen SRV-Records.

1. Klicken Sie mit der rechten Maustaste auf die Zone und wählen Sie *Eigenschaften*.
2. Auf der Registerkarte *Allgemein* können Sie durch Klicken auf die Schaltfläche *Ändern* im Bereich *Typ* die Zone in das Active Directory integrieren lassen.
3. Aktivieren Sie im Fenster *Zonentyp ändern* das Kontrollkästchen *Zone in Active Directory speichern*.

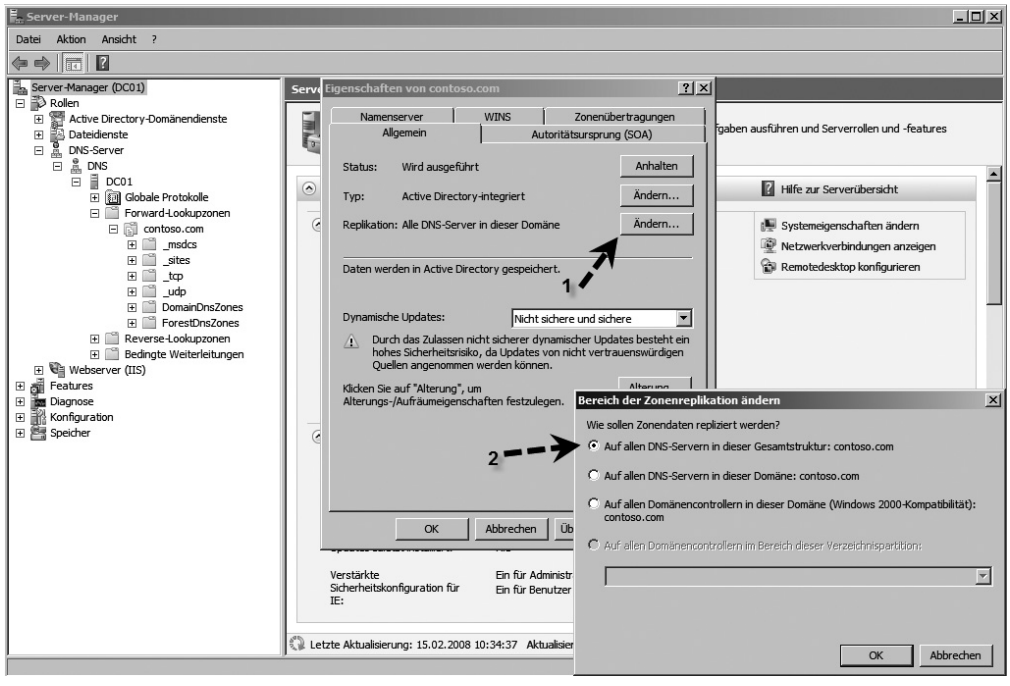
4. Haben Sie diese Einstellung vorgenommen, können Sie noch im Bereich *Dynamische Updates* die Option *Nur sichere* aktivieren.

Abbildg. 8.39 Integration der DNS-Daten in Active Directory



Bei dieser Einstellung können sich nur Computer, die sich erfolgreich im Active Directory authentifizieren, dynamisch in DNS registrieren. Eine Stubzone ist die Kopie einer Zone, die nur die für diese Zone erforderlichen Ressourceneinträge zum Identifizieren der autorisierenden DNS-Server enthält. Diese wird in dieser Testumgebung nicht benötigt, taucht aber im Fenster zur Konfiguration des Zonentyps auf. Haben Sie die Zone in das Active Directory integriert, können Sie auch die Replikation der DNS-Daten anpassen: Klicken Sie in den Eigenschaften einer Zone im Bereich *Replikation* auf *Ändern*, können Sie konfigurieren, auf welche Server die DNS-Daten repliziert werden sollen (Abbildung 8.40). Standardmäßig werden die Daten einer DNS-Zone nur auf den Domänencontrollern der Windows-Domäne repliziert. Die Replikation kann jedoch ohne weiteres auf weitere Server ausgedehnt werden. Sie können die Zone auf alle DNS-Server der Gesamtstruktur, auf alle DNS-Server der aktuellen Domäne oder auf alle Domänencontroller der aktuellen Domäne replizieren.

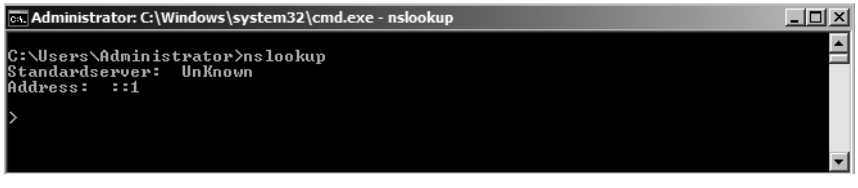
Abbildg. 8.40 Konfiguration der DNS-Daten-Replikation



DNS-IP-Einstellungen anpassen

Windows Server 2008 hat die Eigenart, die Konfiguration Ihrer Netzwerkverbindungen automatisch abzuändern, sodass die Einstellungen für manche Administratoren verwirrend sein können. Im folgenden Abschnitt erfahren Sie, wie Sie die Einstellungen wieder an Ihre Bedürfnisse anpassen. Geben Sie nach der Fertigstellung der Installation von Active Directory auf dem Domänencontroller in der Befehlszeile *nslookup* ein, erhalten Sie unter Umständen eine etwas verwirrende Ausgabe (Abbildung 8.41).

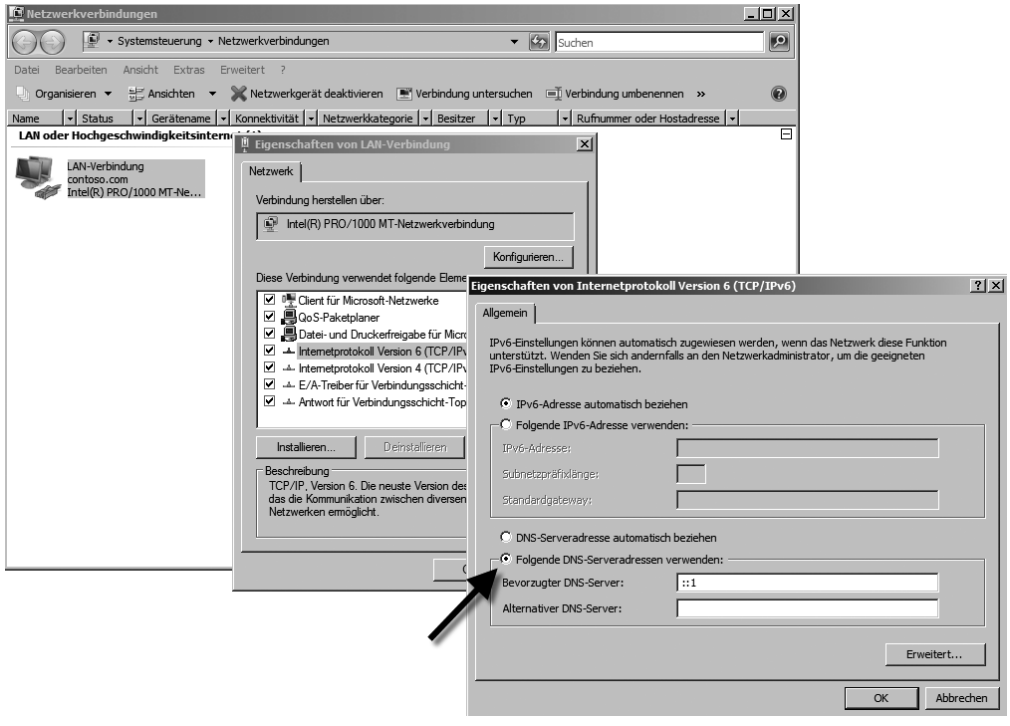
Abbildg. 8.41 Ausgabe von *nslookup* nach der Installation von Active Directory



Der Fehler wird durch eine Konfiguration der Netzwerkverbindungen verursacht. Rufen Sie zunächst die Verwaltung Ihrer Netzwerkverbindungen auf. Der schnellste Weg ist, wenn Sie *ncpa.cpl* in das Suchfeld des Startmenüs eingeben. Rufen Sie zunächst die Eigenschaften des IPv6-Protokolls auf (Abbildung 8.42). Wie Sie sehen hat Windows Server 2008 die Option *Folgende DNS-Serveradressen verwenden aktiviert* und den Eintrag *::1* hinterlegt. Dies entspricht bei IPv6 dem Eintrag 127.0.0.1 (*localhost*) bei IPv4. Durch diesen Eintrag fragt der DNS-Server bei Reverse-Abfragen per

IPv6 den lokalen DNS-Server. Haben Sie keine IPv6-Reverse-Lookupzone erstellt, weil Sie im Unternehmen noch kein IPv6 einsetzen, wird durch diese Konfiguration ein Fehler verursacht. Legen Sie entweder eine IPv6-Reverse-Lookupzone an und stellen Sie sicher, dass ein Zeiger zur IPv6-Adresse des Servers eingetragen wird. In den meisten Fällen ist diese Konfiguration allerdings nicht notwendig, vor allem dann nicht, wenn im Unternehmen nicht mit IPv6 gearbeitet wird. Aktivieren Sie in diesem Fall die Option *DNS-Serveradresse automatisch beziehen*. Durch diese Konfiguration vermeiden Sie die irreführende Meldung in *nslookup*.

Abbildg. 8.42 Konfiguration des DNS-Servers für IPv6-Abfragen



Rufen Sie als Nächstes die Eigenschaften für das IPv4-Protokoll auf. Auch hier hat der Assistent als bevorzugten DNS-Server die Adresse des lokalen Hosts hinterlegt (127.0.0.1). In diesem Fall funktionieren zwar Abfragen per DNS, aber diese Konfiguration ist nicht sauber und resultiert in einer fehlerhaften Ausgabe bei *nslookup*. Tragen Sie auch hier die richtige IPv4-Adresse des Servers ein. Anschließend sollte die Eingabe von *nslookup* in der Befehlszeile keine Fehler mehr ausgeben.

Active Directory von Installationsmedium installieren

Soll ein Domänencontroller nach der Installation seine Replikationsdaten nicht über das Netzwerk beziehen, sondern lokale Dateien verwenden, müssen zuvor einige Vorbereitungen getroffen werden. Für die Installation eines Domänencontrollers in Niederlassungen oder bereits ausgelasteten

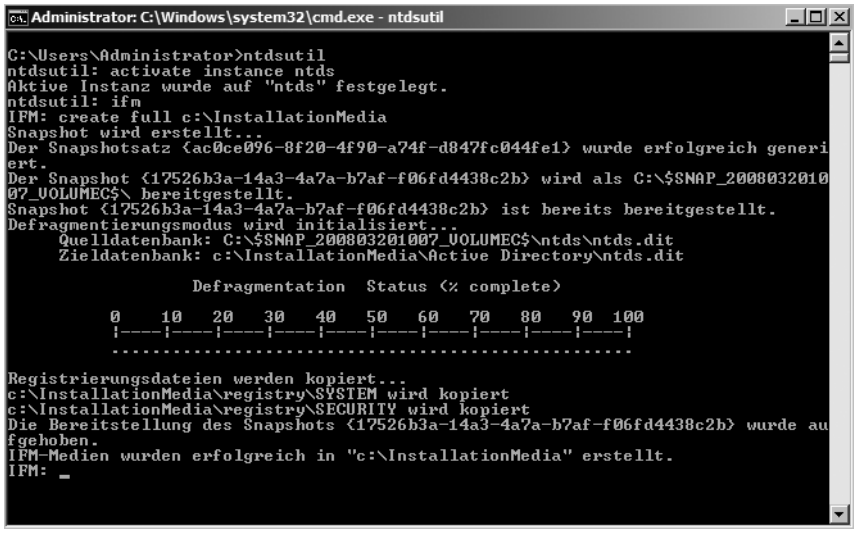
Netzwerken bietet es sich an, auf einem Quell-Domänencontroller zunächst Daten aus dem Active Directory zu exportieren, auf einen Datenträger zu kopieren und per Post zur Niederlassung zu senden. Bei der Heraufstufung eines Domänencontrollers kann dieses Medium verwendet werden. So muss der Domänencontroller in der Niederlassung nur noch das Delta zwischen Medium und aktuellen Daten mit seinen Replikationspartnern synchronisieren, was deutlich Netzwerklast spart. Auf den folgenden Seiten zeigen wir Ihnen, wie Sie dazu am besten vorgehen.

Vorbereiten von Active Directory-Installationsmediums

Um ein Installationsmedium vorzubereiten, müssen Sie sich an einem Domänencontroller mit Admin-Rechten anmelden. Gehen Sie im Anschluss folgendermaßen vor (Abbildung 8.43):

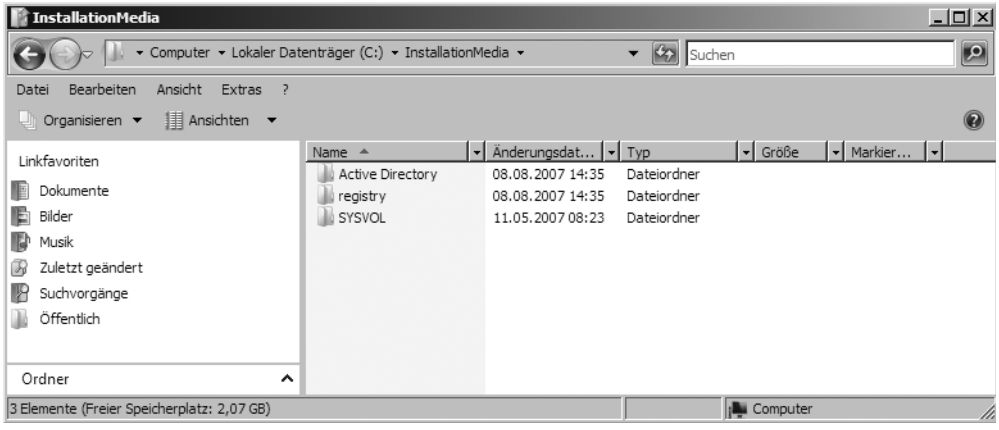
1. Öffnen Sie eine Befehlszeile und geben Sie *ntdsutil* ein.
2. Geben Sie als Nächstes *activate instance ntds* ein und bestätigen Sie.
3. Geben Sie *ifm* ein und bestätigen Sie.

Abbildg. 8.43 Erstellen eines Installationsmediums für die Installation von Active Directory



4. Geben Sie *create rodc C:\InstallationMedia* ein, um ein Installationsmedium für einen RODC zu erstellen. Um einen vollwertigen DC mit dem Installationsmedium zu erstellen, geben Sie *create full C:\InstallationMedia* ein. Soll das *sysvol*-Verzeichnis nicht mit eingeschlossen werden, verwenden Sie einen der beiden Befehle *create nosysvol rodc C:\InstallationMedia* oder *create nosysvol full C:\InstallationMedia*. Das Verzeichnis können Sie natürlich beliebig ändern.
5. Verlassen Sie *ntdsutil* mit der wiederholten Eingabe von *Quit*.
6. Überprüfen Sie, ob das Verzeichnis erstellt wurde und die Daten enthalten sind (Abbildung 8.44).

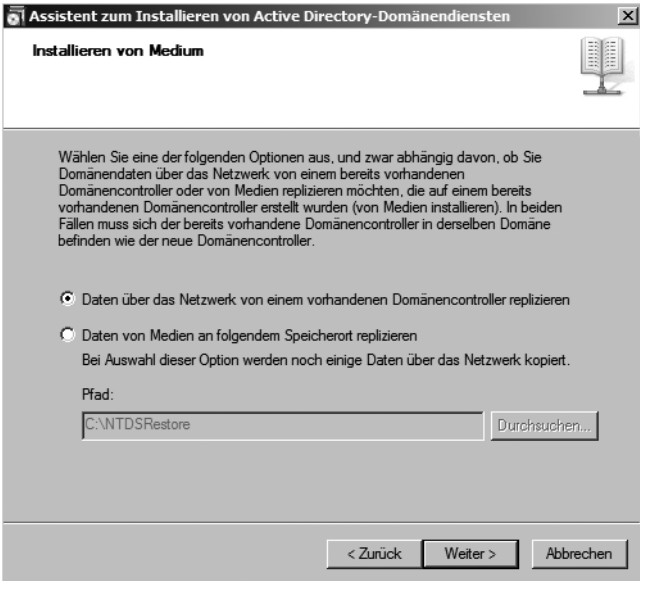
Abbildg. 8.44 Überprüfen des Verzeichnisses mit den Installationsdaten für Active Directory



Domänencontroller mit Medium installieren

Kopieren Sie die Daten auf ein Medium und legen dieses in den Server ein, den Sie mit diesem Medium installieren wollen. Soll die Installation unbeaufsichtigt erfolgen (siehe »Durchführung der Installation von Active Directory mit einer Antwortdatei« weiter hinten in diesem Kapitel), verwenden Sie die Variable */ReplicationSourcePath*. Verwenden Sie den Assistenten in der grafischen Oberfläche, aktivieren Sie auf der Seite *Installieren von Medium* die Option *Daten von Medien an folgendem Speicherort replizieren* und wählen Sie das lokale Verzeichnis aus, in dem die Daten abgelegt wurden (Abbildung 8.45).

Abbildg. 8.45 Erste Replikation eines Domänencontrollers von Installationsmedium ausführen



Active Directory-Diagnose und Fehlerbehebung

Nachdem Sie das Active Directory auf dem Server installiert haben, sind noch einige Nacharbeiten notwendig, in deren Rahmen Sie auch einige erste Schritte mit dem Umgang von Active Directory erlernen. Treten in Ihrem Active Directory Probleme auf, können Sie oft leicht bereits mit Bordmitteln eine Diagnose durchführen und die Lösung für das Problem finden. Auch beim Installieren von neuen Domänencontrollern oder wenn Sie sich einen Überblick über die Replikation der Domänencontroller verschaffen wollen, helfen Bordmittel. Vor allem nach der Installation eines Domänencontrollers ist eine Diagnose sinnvoll, um die Stabilität zu gewährleisten.

Verwenden der Domänencontroller-Diagnose (*dcdiag.exe*)

Das wichtigste Tool für die Diagnose von Domänencontrollern ist *dcdiag.exe*. Sie können das Tool in der Befehlszeile aufrufen, indem Sie *dcdiag* eingeben. Unter Windows Server 2003 mussten Sie dieses Tool noch nachträglich installieren. Eine ausführliche Diagnose erhalten Sie durch *dcdiag /v*. Wollen Sie eine ausführlichere Diagnose durchführen, sollten Sie die Ausgabe jedoch in eine Datei umleiten, da Sie dadurch das Ergebnis besser durchlesen und eventuell auch an einen Spezialisten versenden können. Die Befehlszeile könnte dann zum Beispiel *dcdiag/v >c:\dcdiag.txt* lauten. Für die erste Überprüfung reicht die normale Diagnose mit *dcdiag* jedoch vollkommen aus. Im Folgenden gehen wir die wichtigsten Informationen durch, die bei der Diagnose mit *dcdiag* eine Rolle spielen.

Listing 8.1 Diagnose von Domänencontrollern mit *dcdiag*

```
         *** Warning: could not confirm the identity of this server in the
         directory versus the names returned by DNS servers. If there are
         problems accessing this directory server then you may need to check
         that this server is correctly registered with DNS.
         ..... DC01 passed test Connectivity <- Diese Fehlermeldung
erscheint, wenn in der DNS-Zone keine IPv6-Namensauflösung stattfinden kann. Verwenden Sie
im internen Netz noch kein IPv6 können Sie diesen Fehler ignorieren. Die Verbindung zum
Active Directory ist vorhanden. Hier muss auf jeden Fall Passed stehen. Mit diesem Test
wird überprüft, ob der Domänencontroller im DNS registriert ist. Zusätzlich wird überprüft
ob der Server per Ping, RPC und LDAP erreichbar ist. Die IPv6-Verbindung ist keine
zwingende Voraussetzung für das Bestehen des Tests wie Sie sehen.
Doing primary tests
   Testing server: Default-First-Site-Name\DC01
      Starting test: Advertising
         ..... DC01 passed test Advertising <- Verbindung zum Active
Directory ist mit Anmeldung möglich, daher muss auf jeden Fall auch hier Passed stehen. So
ist sichergestellt, dass sich der DC im Active Directory als Domänencontroller angemeldet
hat.
Starting test: FrsEvent
         ..... DC01 passed test FrsEvent
      Starting test: FrsSysVol
```

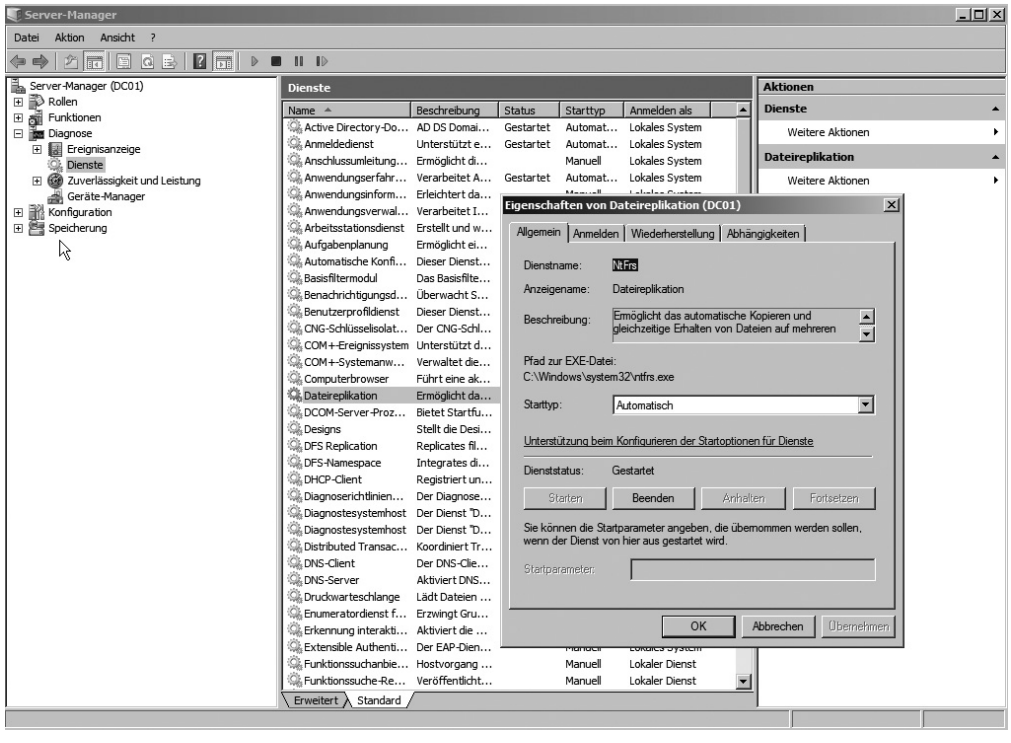
Listing 8.1 Diagnose von Domänencontrollern mit *dcdiag* *(Fortsetzung)*

```
        ..... DC01 passed test FrsSysVol <- Diese beiden Tests sind
nicht ganz so wichtig, sollten aber auch bestanden werden. FRS (File Replication Service)
ist dafür zuständig, dass Anmeldeskripts im Sysvol-Verzeichnis zwischen den verschiedenen
DCs repliziert werden. Hier kann durchaus auch mal Failed stehen, die Replikation
funktioniert meistens trotzdem, überprüfen Sie das aber an Hand des Inhalts. Schauen Sie
auch im Server-Manager unter Rollen/Dateidienste in der Mitte des Bildschirms, ob der
Systemdienst Dateireplikation gestartet ist und auf Automatisch steht. Wenn nicht, starten
Sie den Dienst und führen Sie dcdiag nochmals aus. Der Test sollte jetzt bestanden werden.

Starting test: kccevent      Starting test: KccEvent
..... DC01 passed test KccEvent <- Der Knowledge Consistency Checker
stellt fest, dass der DC alle anderen DCs finden kann, um Replikationsverbindungen
herzustellen. Der Test muss bestanden werden.
```

Neben *dcdiag.exe* kann auch *netdiag.exe* zur Diagnose herangezogen werden. Auch hier erzeugt das System aussagekräftige Fehlermeldungen. Im Gegensatz zu *dcdiag.exe* kann *netdiag.exe* auch auf Mitgliedsservern zur Diagnose verwendet werden.

Abbildg. 8.46 Start und Konfiguration der Dateireplikation auf einem Domänencontroller



Erscheinen bei *Dcdiag* Fehler bezüglich der Replikation des Sysvol-Verzeichnisses, sollte, wie im *Listing 8.1* beschrieben, ein Blick auf den Systemdienst *Dateireplikation* geworfen werden. Dieser Dienst verbindet die Domänencontroller der verschiedenen Standorte und erstellt automatisch eine Replikationstopologie auf Basis der definierten Zeitpläne und Standortverknüpfungen. Der KCC ist

ein automatischer Mechanismus im Active Directory. Dieser läuft auf jedem Domänencontroller und erstellt und pflegt die Topologie des Netzwerks, um die optimalen Replikationspartner zu finden. Er erstellt automatisch Standortverknüpfungsbrücken, wenn zwei Standorte nicht miteinander verbunden sind, sondern nur über einen dritten erreicht werden können. Er versucht mit Erfahrungswerten über die Performance der Replikation die optimale Struktur aufzubauen. Dieser Ansatz ist deshalb empfehlenswert, weil die Struktur durch den KCC alle 15 Minuten überprüft wird und damit ausgefallene Verbindungen erkannt werden. Der Zeitraum für die Überprüfung kann verlängert werden. Innerhalb eines Standortes spielt der Netzwerkverkehr keine große Rolle. Die Replikationsdaten innerhalb eines Standortes werden daher, im Gegensatz zur Replikation zwischen Standorten, nicht komprimiert. Der KCC versucht automatisch innerhalb eines Standortes eine Ringtopologie zu erstellen und maximal drei Hops zwischen zwei Domänencontrollern durchzuführen. Das heißt, dass nicht unbedingt jeder Domänencontroller mit jedem Daten replizieren muss, aber dass auch maximal drei Schritte zwischen zwei Domänencontrollern liegen dürfen.

Je mehr Standorte im Active Directory definiert sind, desto mehr muss der KCC die Routingtopologie dauerhaft überwachen. Aus diesen Gründen müssen Domänencontroller über mehr Performance verfügen, als in Umgebungen mit nur einem oder wenigen Standorten. Wenn in den Standorten mehr als nur ein Domänencontroller zur Verfügung gestellt wird, werden zwischen den Standorten nicht alle Domänencontroller repliziert. In jedem Standort gibt es so genannte *Bridgehead-Server*, welche die Informationen ihres Standortes an die Bridgeheadserver der anderen Standorte weitergeben. Dadurch wird der Verkehr über die WAN-Leitung minimiert, da nicht mehr alle Domänencontroller Daten nach extern versenden. Der *Intersite Topology Generator (ISTG)* wählt automatisch für jeden Standort automatisch die am besten geeigneten Bridgehead-Server aus. Microsoft empfiehlt, die Bridgeheadserver nicht manuell zu konfigurieren, sondern den ISTG zu verwenden. Wenn Sie Bridgeheadserver manuell auswählen und einzelne Server zu bevorzugten Bridgeheadservern konfigurieren, kann der KCC nur zwischen diesen Servern auswählen, nicht zwischen allen Domänencontrollern eines Standortes. Außerdem besteht darüber hinaus noch die Gefahr, dass bei Ausfall von allen bevorzugten Bridgeheadservern keine Replikationen zu und von diesem Standort durchgeführt werden können.

Listing 8.2 Überprüfen eines Windows Server 2008-Domänencontrollers mit *dcdiag.exe*

```
Starting test: systemlog                Starting test: KnowsOfRoleHolders
         ..... DC01 passed test KnowsOfRoleHolders <- Der DC kann alle
notwendigen FSMO-Rollen im Active Directory finden (PDC-Emulator, RID-Master, Infrastruktur
Master,  Schemamaster, Domänennamenmaster. Hier muss Passed stehen. Werden einzelne Rollen
nicht gefunden, liegt nicht zwingend ein Problem mit dem lokalen Domänencontroller vor,
sondern vielleicht mit dem Rolleninhaber.

      Starting test: MachineAccount
        ..... DC01 passed test MachineAccount <- Das Computerkonto für
den DC im Active Directory ist in Ordnung. Hier muss auf jeden Fall Passed stehen. Hier wird
geprüft, ob das Computerkonto im Active Directory in Ordnung ist und ob das Computerkonto
sich richtig registriert hat. Sie können über die Option dcdiag /RecreateMachineAccount
eine Fehlerbehebung versuchen, wenn der Test fehlschlägt. Über dcdiag /FixMachineAccount
können Sie ebenfalls eine Fehlerbehebung versuchen. Eine weitere Option, die Fehler in
diesem Bereich behebt, ist dcdiag /fix.

 MachineAccount      Starting test: NCSecDesc
         ..... DC01 passed test NCSecDesc
Starting test: NetLogons
```

Listing 8.2 Überprüfen eines Windows Server 2008-Domänencontrollers mit *dcdiag.exe* *(Fortsetzung)*

```
         ..... DC01 passed test NetLogons <- Die Anmeldung am Active
Directory ist möglich, auch hier muss auf jeden Fall Passed stehen.
      Starting test: ObjectsReplicated
         ..... DC01 passed test ObjectsReplicated <- Der DC hat alle
Objekte von Active Directory mit anderen DCs repliziert. Dieser Test muss bestanden werden,
da hier die Replikation überprüft wird.
      Starting test: Replications
         ..... DC01 passed test Replications
      Starting test: RidManager
         ..... DC01 passed test RidManager
      Starting test: Services
        ..... DC01 passed test Services <- Mit diesem Test wird
überprüft, ob die notwendigen Systemdienste auf dem Domänencontroller gestartet wurden.
Auch dieser Test muss erfolgreich bestanden werden.
Starting test: SystemLog
         ..... DC01 passed test SystemLog <- Bei diesem Test werden
Fehler aus der Ereignisanzeige abgeprüft. Genauere Erkenntnisse erlangen Sie, wenn Sie
selbst im Systemprotokoll der Ereignisanzeige nachschauen. Schlägt dieser Test fehl, ist
das nicht weiter schlimm, da er nur besagt, dass es Fehler in der Ereignisanzeige gibt. Sie
sollten diese aber dennoch überprüfen und abstellen.
      Starting test: VerifyReferences
         ..... DC01 passed test VerifyReferences
   Running partition tests on : ForestDnsZones
      Starting test: CheckSDRefDom
         ..... ForestDnsZones passed test CheckSDRefDom
      Starting test: CrossRefValidation
         ..... ForestDnsZones passed test
         CrossRefValidation
   Running partition tests on : DomainDnsZones
      Starting test: CheckSDRefDom
         ..... DomainDnsZones passed test CheckSDRefDom
      Starting test: CrossRefValidation
         ..... DomainDnsZones passed test
         CrossRefValidation
   Running partition tests on : Schema
      Starting test: CheckSDRefDom
         ..... Schema passed test CheckSDRefDom
      Starting test: CrossRefValidation
         ..... Schema passed test CrossRefValidation
   Running partition tests on : Configuration
      Starting test: CheckSDRefDom
         ..... Configuration passed test CheckSDRefDom
      Starting test: CrossRefValidation
         ..... Configuration passed test CrossRefValidation
   Running partition tests on : contoso
      Starting test: CheckSDRefDom
         ..... contoso passed test CheckSDRefDom
      Starting test: CrossRefValidation
         ..... contoso passed test CrossRefValidation
   Running enterprise tests on : contoso.com
      Starting test: FsmoCheck
         ..... contoso.com passed test FsmoCheck
```

Listing 8.2 Überprüfen eines Windows Server 2008-Domänencontrollers mit *dcdiag.exe* *(Fortsetzung)*

```
      Starting test: Intersite
        ......................... contoso.com passed test Intersite <- Alle Tests seit dem
letzten Kommentar sollten auf jeden Fall auf Passed stehen. Hier werden wichtige Elemente
von DNS und Active Directory getestet. Tauchen an dieser Stelle Fehler auf, geben Sie den
Namen des Tests und das Ergebnis Failed in einer Suchmaschine ein. Sie erhalten dadurch
gezielt Hinweise, wo das Problem liegen könnte. Sie sollten keinesfalls einzelne Fehler
ignorieren. Die Tests überprüfen verschiedene Querverweise der einzelnen Domänen und
Anwendungspartitionen im Active Directory.
```

Mit *dcdiag /a* überprüfen Sie alle Domänencontroller am gleichen Active Directory-Standort, über *dcdiag /e* werden alle Server in der Gesamtstruktur getestet. Um sich nur die Fehler und keine Informationen anzeigen zu lassen, verwenden Sie *dcdiag /q*. Die Option *dcdiag /s:<Domänencontroller>* ermöglicht den Test eines Servers über das Netzwerk.

Testen der Namensauflösung mit *nslookup.exe*

Ein weiterer wichtiger Test besteht darin, dass Sie in der Befehlszeile *nslookup* aufrufen. An dieser Stelle sollte kein Fehler auftreten:

Listing 8.3 Fehlerfreie Ausgabe von *nslookup*

```
C:\Users\Administrator>nslookup
Standardserver:  DC1.contoso.com
Address:  10.1.1.20
```

Erscheint ein Fehler, lesen Sie den Abschnitt »DNS-IP-Einstellungen anpassen« weiter vorne in diesem Kapitel. Dieser Test zeigt, dass der bevorzugte DNS-Server erreicht werden kann und sein Computername sowie seine IP-Adresse im DNS registriert sind. Erhalten Sie hier bereits eine Fehlermeldung angezeigt, sollten Sie überprüfen, ob die IP-Adresse des DNS-Servers in der *Reverse-Lookupzone* registriert ist. Sollte der Server noch nicht registriert sein, versuchen Sie mit *ipconfig /registerdns* in der Befehlszeile eine erneute automatische Registrierung beim DNS-Server. Das ist eine häufige Fehlerquelle. Danach sollten Sie durch die Eingabe des vollständigen Computernamens aller restlichen Domänencontroller feststellen, dass alle notwendigen Domänencontroller per DNS erreicht werden können.

Standard-OUs per *Active Directory-Benutzer und -Computer* überprüfen

Nach einer Neuinstallation sollten Sie überprüfen, ob sich das Snap-In *Active Directory-Benutzer und -Computer* im Server-Manager fehlerfrei öffnen lässt und die fünf wichtigsten OUs angezeigt werden. Diese OUs sind in jeder Domäne identisch und müssen vorhanden sein (Abbildung 8.47):

- **Builtin** Im Container *Builtin* befinden sich vom System vordefinierte Gruppen.
- **Computers** Der Container *Computers* enthält Computerkonten für alle Computer, die in die Domäne aufgenommen wurden. Jeder Computer wird mit einem eigenen Konto im Active Directory verwaltet.

- **Users** Im Container *Users* befinden sich die Benutzer und Gruppen, die von Windows Server 2008 automatisch angelegt werden.
- **ForeignSecurityPrincipals** Der Container *ForeignSecurityPrincipals* enthält Informationen über SIDs, die mit Objekten aus entfernten, vertrauten Domänen verbunden sind.
- **Domain Controllers** Im Container *Domain Controllers* befinden sich Computerkonten für alle Domänencontroller der Domäne.

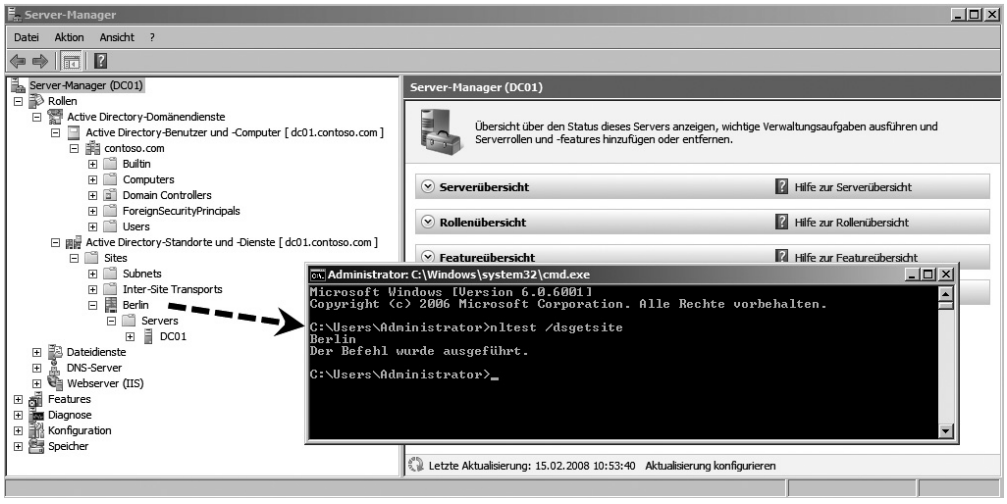
Sie müssen nicht den Inhalt der Container überprüfen, sondern lediglich testen, ob diese tatsächlich angelegt wurden. Achten Sie darauf, im Snap-In den Befehl *Erweiterte Features* im Menü *Ansicht* zu aktivieren.

Abbildg. 8.47 Anzeigen der Standard-OUs nach der Installation von Active Directory

Überprüfen der Active Directory-Standorte

Sie sollten bei Problemen oder nach Installationen von Domänencontrollern überprüfen, ob die Domänencontroller dem jeweils richtigen Standort zugewiesen sind und ob an jedem Standort ein Server zum globalen Katalog konfiguriert wurde. Haben Sie bereits mehrere Domänencontroller installiert, sollten Sie überprüfen, ob bei allen Domänencontrollern automatisch konfigurierte Replikationsverbindungen eingerichtet wurden und ob diese auch funktionieren. Alle installierten Domänencontroller sollten angezeigt werden und sich ohne Fehler mit ihren Replikationspartnern replizieren lassen. Installieren Sie einen neuen Domänencontroller oder auch einen Mitgliedsserver, sollten Sie vor allem dann, wenn dieser auch Exchange-Server werden soll, in der Befehlszeile testen, ob dieser Server seinen Standort auflösen kann und richtig konfiguriert ist. Geben Sie dazu den Befehl *nltest /dsgetsite* ein. Es darf kein Fehler auftreten, sondern der Server muss seinen richtigen Standort ausgeben. Erscheinen an dieser Stelle Fehler, sollten Sie die IP-Einstellungen des Servers und die DNS-Konfiguration des bevorzugten DNS-Servers überprüfen. Auch die IP-Subnetze und deren korrekte Zuordnung zu den richtigen Standorten sollte hier überprüft werden. Den Standardnamen des ersten Standortes passen Sie am besten im Server-Manager über *Rollen/Active Directory-Domänendienste/Active Directory-Standorte und -Dienste an* (Abbildung 8.48). Klicken Sie dazu den Standort mit der rechten Maustaste an und wählen Sie *Umbenennen*.

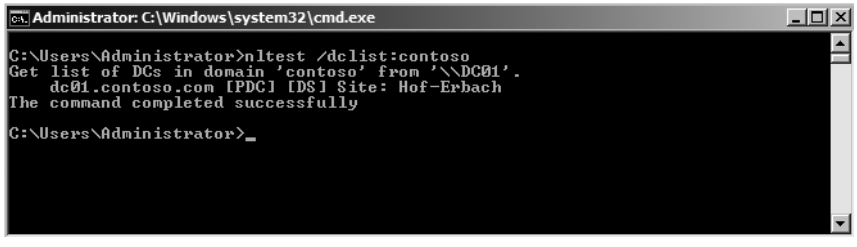
Abbildg. 8.48 Anzeigen des zugeordneten Active Directory-Standortes in der Befehlszeile



Überprüfen der Domänencontroller-Liste

Geben Sie in der Befehlszeile den Befehl *nltest /dclist:<NetBIOS-DOMÄNENNAME>* ein, zum Beispiel *nltest /dclist:contoso*. Alle Domänencontroller sollten mit ihren vollständigen Domänennamen ausgegeben werden. Werden einzelne Domänencontroller nur mit ihrem NetBIOS-Namen angezeigt, überprüfen Sie deren DNS-Registrierung auf den DNS-Servern.

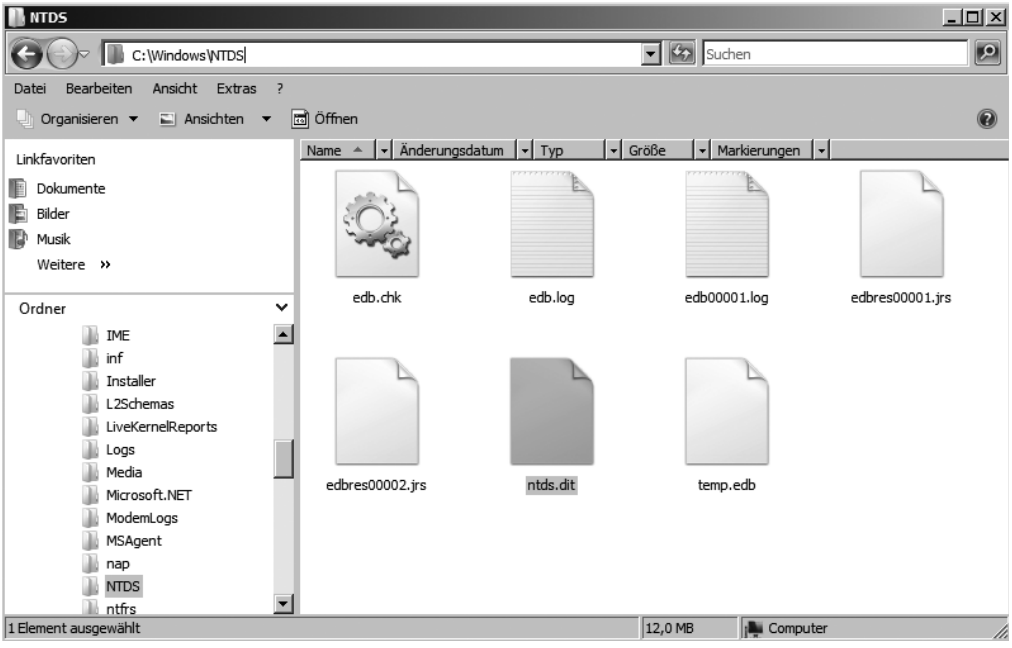
Abbildg. 8.49 Anzeigen der vollständigen Domänencontroller-Liste in der Befehlszeile



Überprüfen der Active Directory-Dateien

Die Active Directory-Daten werden in einer Datenbank gespeichert. Diese Datenbank ist eine Datei im Dateisystem auf den Domänencontrollern. Die Active Directory-Datenbank wird in der Datei *ntds.dit* in dem Verzeichnis gespeichert, das Sie bei der Heraufstufung zum Domänencontroller festgelegt haben. Standardmäßig wird die Active Directory-Datenbank im Verzeichnis *c:\windows\ntds* abgelegt. Überprüfen Sie, ob die Dateien auf dem Domänencontroller vorhanden sind und ob noch genügend Festplattenplatz frei ist, damit die Datenbank wachsen kann. Sie können die Größe der Active Directory-Datenbank jederzeit feststellen, indem Sie die Größe dieser Datei überprüfen.

Abbildg. 8.50 Anzeigen der Systemdateien von Active Directory

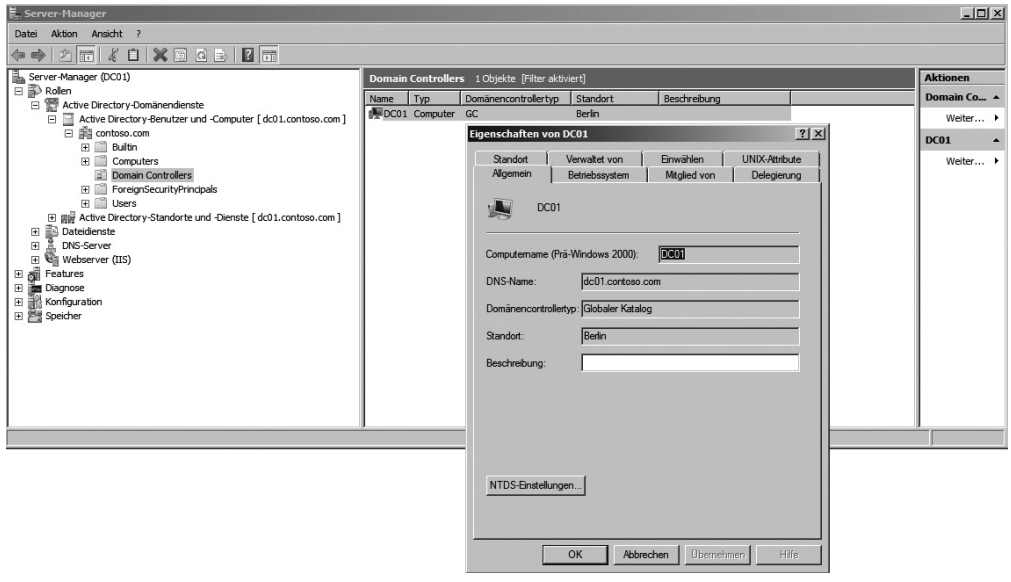


Bei den **.jrs*-Dateien handelt es sich um die Transaktionsprotokolle der Datenbank. Die Datei *edb.chk* ist die Checkpoint-Datei. Diese Datei enthält die Informationen, welche Transaktionsprotokolle bereits in die Datenbank geschrieben wurden.

Domänenkonto der Domänencontroller überprüfen

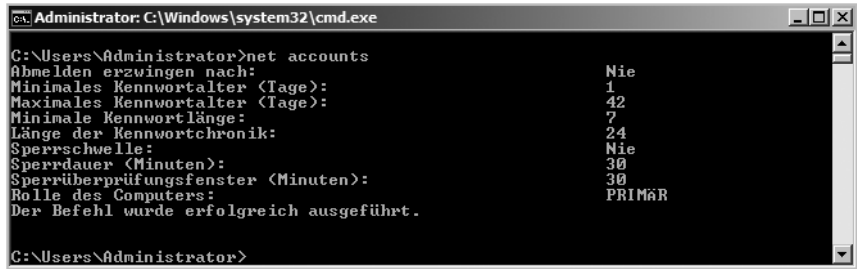
Die Domänencontroller sollten im Snap-In *Active Directory-Benutzer und -Computer* in der OU *Domain Controllers* angezeigt werden (Abbildung 8.51). Von diesem Konto sollten Sie fehlerfrei die Eigenschaften aufrufen können. Die Informationen auf den einzelnen Registerkarten sollten fehlerfrei dargestellt werden und die korrekten Daten enthalten.

Abbildg. 8.51 Anzeigen der Eigenschaften des Computerkontos eines Domänencontrollers



Außerdem können Sie mit dem Befehl *net accounts* in der Befehlszeile den Status des Domänenkontos eines Domänencontrollers überprüfen. Innerhalb der Ausgabe von *net accounts* sollte die Rolle des Computers *Primär* sein, wenn es sich um den PDC-Emulator handelt. Bei allen anderen Domänencontrollern wird an dieser Stelle die Rolle *Sicherung* angezeigt.

Abbildg. 8.52 Anzeigen der Eigenschaften des Domänencontroller-Computerkontos in der Befehlszeile



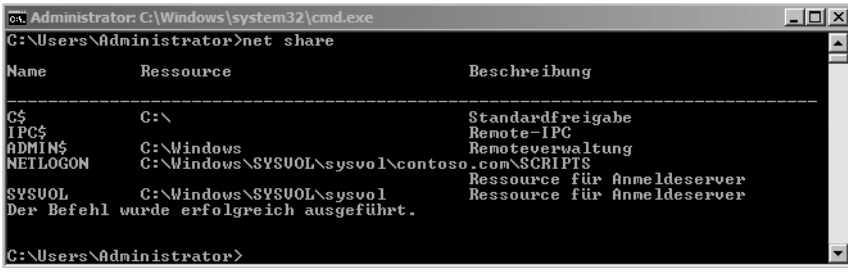
Überprüfen der administrativen Freigaben

Vor allem die beiden Freigaben *netlogon* und *sysvol* sollten fehlerfrei dargestellt werden. Überprüfen Sie die Freigaben mit Hilfe des Befehlszeilenprogrammes *net share*. Standardmäßig werden die beiden Verzeichnisse ...

- *C:\Windows\sysvol\sysvol\<Domäne>\Scripts* als Freigabe *netlogon*
- *C:\Windows\sysvol\sysvol* als Freigabe *SYSVOL*

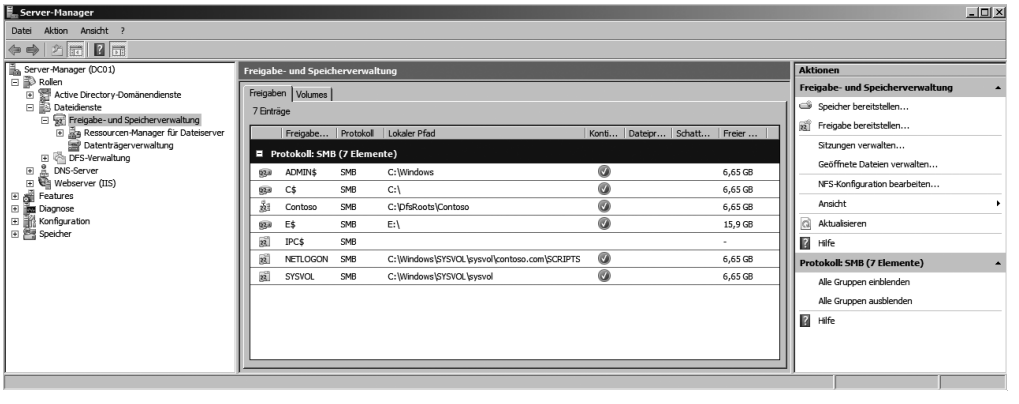
... freigegeben. Beide Freigaben werden durch *net share* in der Befehlszeile angezeigt.

Abbildg. 8.53 Anzeigen der administrativen Freigaben in der Befehlszeile



Alternativ überprüfen Sie die administrativen Freigaben im Server-Manager über *Rollen\Dateidienste\Freigabe- und Speicherverwaltung* (Abbildung 8.54). Auch hier werden die Freigaben angezeigt.

Abbildg. 8.54 Anzeigen der administrativen Freigabe über den Server-Manager



Überprüfen der Gruppenrichtlinien

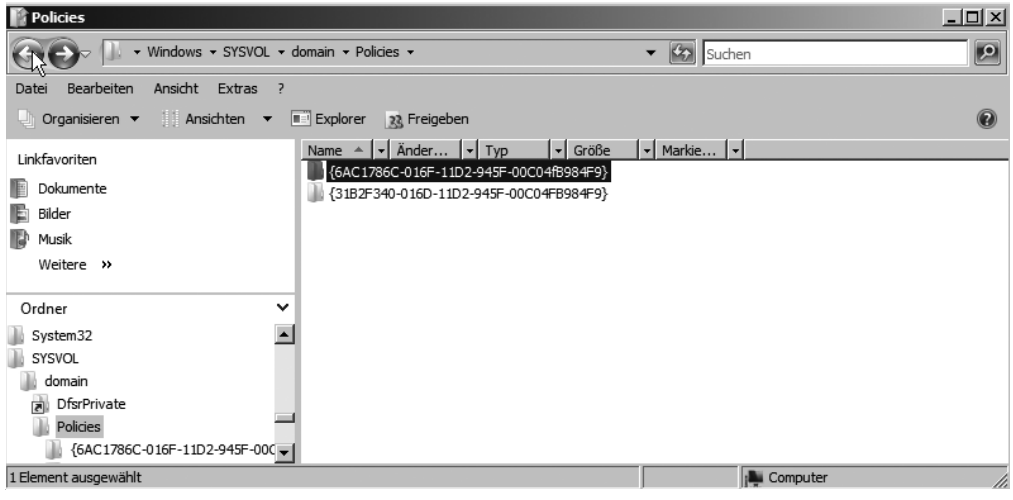
Automatisch werden nach der Installation durch das Active Directory die beiden Gruppenrichtlinien ...

- Default Domain Controller Policy
- Default Domain Policy

... angelegt. Die Einstellungen der beiden Gruppenrichtlinien werden im Dateisystem auf den Domänencontrollern gespeichert. Für beide Richtlinien gibt es im Verzeichnis *C:\Windows\SYSVOL\domain\policies* jeweils einen Unterordner, der durch eine eindeutige GUID dargestellt wird. Überprüfen Sie, ob diese beiden Unterordner vorhanden sind und fehlerfrei geöffnet werden können:

- **{31B2F340-016D-11D2-945F-00C04FB984F9}** Default Domain Policy
- **{6AC1786C-016F-11D2-945F-00C04fB984F9}** Default Domain Controller Policy

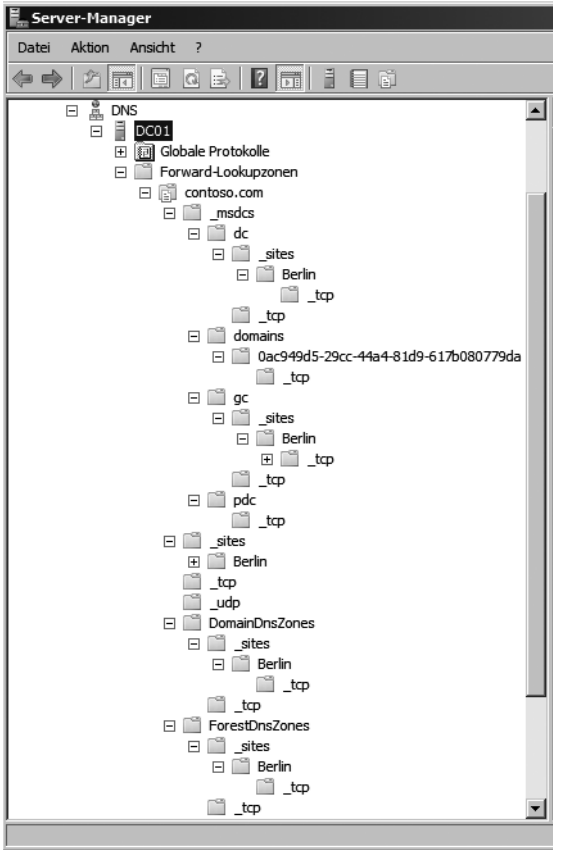
Abbildg. 8.55 Anzeigen der Verzeichnisse für die beiden standardmäßigen Gruppenrichtlinien



DNS-Einträge von Active Directory überprüfen

Nach der Installation von Active Directory werden in der Forward-Lookupzone der entsprechenden Domäne zahlreiche Einstellungen vorgenommen. Überprüfen Sie in der DNS-Verwaltung, ob die Einträge von Active Directory fehlerfrei vorgenommen worden sind. Sie brauchen nicht alle Einträge zu überprüfen, können aber schon an der Übersicht alleine erkennen, ob überhaupt Einträge erstellt wurden. Alle notwendigen Dienste von Active Directory werden als SRV-Record im DNS gespeichert.

Abbildg. 8.56 Überprüfen der DNS-Daten von Active Directory im Server-Manager



Testen der Betriebsmaster

Als Nächstes sollten Sie auf einem neuen Domänencontroller testen, ob dieser alle FSMO-Rolleninhaber (Flexible Single Master Operations) kennt. Geben Sie in der Befehlszeile den Befehl *netdom query fsmo* ein (Abbildung 8.57). Dann gibt der Domänencontroller alle FSMO-Rollen aus, die er kennt. Dieser Test baut keine Verbindung zu den FSMO-Rolleninhabern auf, sodass nicht sichergestellt wird, dass diese auch funktionieren. Allerdings wird durch diesen schnell durchführbaren Test überprüft, ob die Rolleninhaber bekannt sind.

Abbildg. 8.57 Anzeigen der Betriebsmaster-Rollen in einem Active Directory

Freeware-Tools für die Verwaltung von Netzwerken und Active Directory

In diesem Abschnitt stellen wir Ihnen die Sysinternal-Tools vor, die für die Verwaltung und Fehlersuche in Netzwerken und Active Directory dienen. Tools wie *AdRestore* oder der *AD Explorer* bieten für jeden Administrator eine wertvolle Ergänzung zu seiner eigenen Tool-Sammlung. Auf einfachem Weg lassen sich mit den Tools von Sysinternals Active Directory-Objekte wiederherstellen oder die Datenbank bearbeiten. Die Tools können auf der Internetseite *www.sysinternals.com* heruntergeladen werden.

Objekte aus dem Active Directory wiederherstellen mit AdRestore

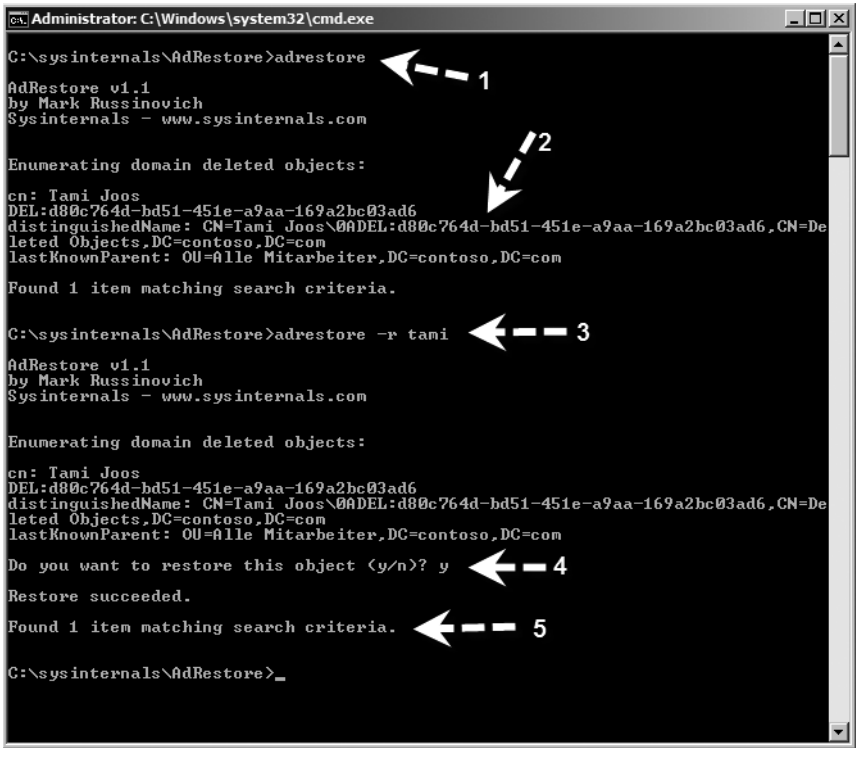
Das Löschen von Konten im Active Directory ist schnell passiert und kann unangenehme Auswirkungen haben. Die Wiederherstellung mit Bordmitteln, die autorisierte Wiederherstellung, ist aufwändig und zeitintensiv. Vor allem ungeübte Administratoren können mit solchen Vorgängen sehr schnell mehrere Stunden oder einen ganzen Tag verbringen. Für genau solche Fälle gibt es das Tool AdRestore von Sysinternals. Mit dem Tool werden gelöschte Objekte ohne die Verwendung der Active Directory-Sicherung oder das Booten von Domänencontroller wiederhergestellt. Das Tool macht sich dazu eine automatische Sicherungsfunktion im Active Directory zu Nutze: Ein gelöschtes Objekt kann im Active Directory innerhalb eines gewissen Zeitraums wiederhergestellt werden. Es befindet sich sozusagen im Papierkorb der Active Directory-Datenbank, aus dem es wiederhergestellt werden kann. Wenn dieser Zeitraum allerdings einmal abgelaufen ist, kann das Objekt nicht mehr ohne weiteres wiederhergestellt werden. Dieser Zeitraum wird im Active Directory als Tombstone Lifetime bezeichnet. Wurde mit Windows Server 2003 eine Gesamtstruktur erstellt, beträgt die Tombstone Lifetime 60 Tage. Wurde die Gesamtstruktur mit einem Datenträger erstellt, der das Service Pack 1 oder das Service Pack 2 für Windows Server 2003 bereits enthält, beträgt die Tombstone Lifetime 180 Tage, das gilt auch für Windows Server 2008.

Der Tombstone wird zur Replikation gelöschter Objekte genutzt und enthält einige Rumpfdaten wie den Objektnamen und vor allem die Sicherheitskennung (Security ID, SID). Windows Server 2003/2008 enthält eine Schnittstelle, über den sich ein Tombstone wiederbeleben lässt. Durch diesen Vorgang können gelöschte Objekte, die sich noch innerhalb der Tombstone Lifetime befinden, sehr einfach und leicht wiederhergestellt werden. Das Tool reanimiert nur den Tombstone selbst, stellt aber keine weiteren Daten wieder her. Dadurch fehlen die erweiterten Namensfelder, die Adressinformationen und Organisationsdaten und vor allem die Gruppenmitgliedschaften. Es ist also Handarbeit angesagt, die fehlenden Einträge wiederherzustellen. Die wichtigsten Daten und vor allem die SID

sind nach der Wiederherstellung aber wieder verfügbar. Ausführliche Hinweise finden sich auch im Knowledge Base-Artikel 840001: »How to restore deleted user accounts and their group memberships in Active Directory«.

Die Wiederherstellung der Objekte durch AdRestore erfolgt über die Befehlszeile. Wenn das Tool ohne weitere Optionen aufgerufen wird, werden die gelöschten Objekte angezeigt, die das Tool wiederherstellen kann. Anschließend werden mit der Option *–r* Objekte wiederhergestellt. Dabei ist die Syntax recht einfach: *adrestore –r <Name oder Teil des Namens>*. Wird ein Objekt bei den gelöschten Objekten gefunden, kann es nach einer Bestätigung wiederhergestellt werden. Das Objekt befindet sich anschließend wieder auf dem Domänencontroller, auf dem die Wiederherstellung durchgeführt wurde. Damit das Objekt auch im kompletten Active Directory wieder verfügbar ist, muss eine Replikation angestoßen werden. Nach der Replikation wird das Objekt auf allen Domänencontrollern wieder angezeigt. Das Gute an dieser Lösung ist, dass die SID des ursprünglichen Objektes meistens erhalten bleibt, sodass Berechtigungen nicht neu gesetzt werden müssen.

Abbildg. 8.58 Mit AdRestore können gelöschte Objekte im Active Directory sehr einfach und schnell wiederhergestellt werden

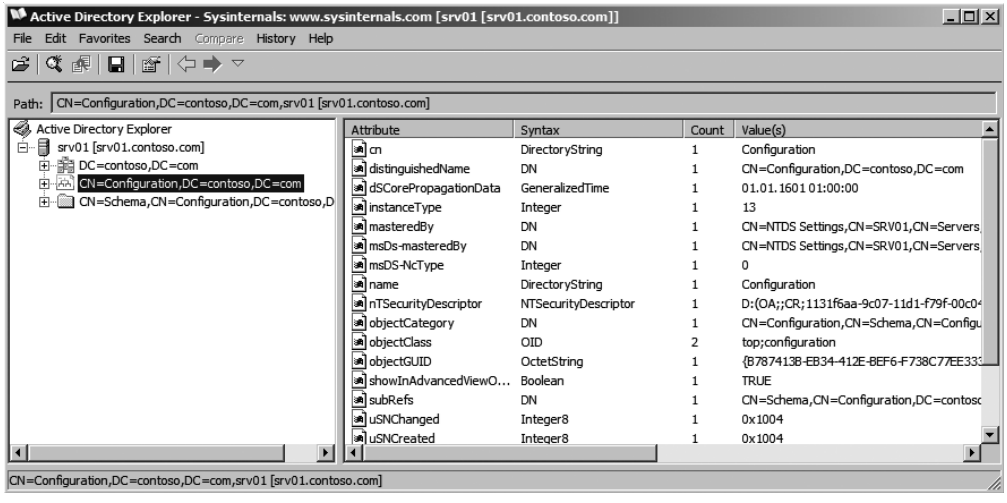


Active Directory Explorer (AD Explorer)

Der AD Explorer ist ein sehr mächtiges Werkzeug, um Einstellungen in der Active Directory-Datenbank zu überprüfen und zu bearbeiten. Das Programm bietet eine grafische Oberfläche und ist wesentlich effizienter und leichter zu bedienen als das Windows-Tool ADSI-Edit. Wie alle Sysinternal-Tools muss das Programm nicht installiert werden, sondern lässt sich direkt nach dem Ent-

packen einsetzen. Somit stellt es ein optimales Zusatztool für USB-Sticks dar, da sich die Anmeldung an der Domäne beim Starten des Programms mitgeben lässt. Das Tool bietet eine Windows-Explorer ähnliche Oberfläche. Mit dem Tool lassen sich Snapshots der Active Directory-Datenbank erstellen, die zu Analysezwecken auch offline bearbeitet und untersucht werden können. Zu diesem Zweck steht der Menübefehl *File/Create Snapshot* zur Verfügung. Achten Sie aber darauf, dass bei der Erstellung eines Snapshots die CPU-Auslastung des Servers sehr schnell über mehrere Minuten 100 % erreichen kann, abhängig von der Größe der Active Directory-Datenbank. Die Navigation in den Snapshots erfolgt absolut identisch zur Bearbeitung und Überprüfung einer produktiven AD-Datenbank. Werden mehrere Snapshots angefertigt, lassen sich Änderungen in diesen Snapshots mit dem Tool vergleichen. Dadurch können Sie die Änderungen von Software-Installationen, die das Active Directory betreffen, sehr leicht nachvollziehen und überprüfen.

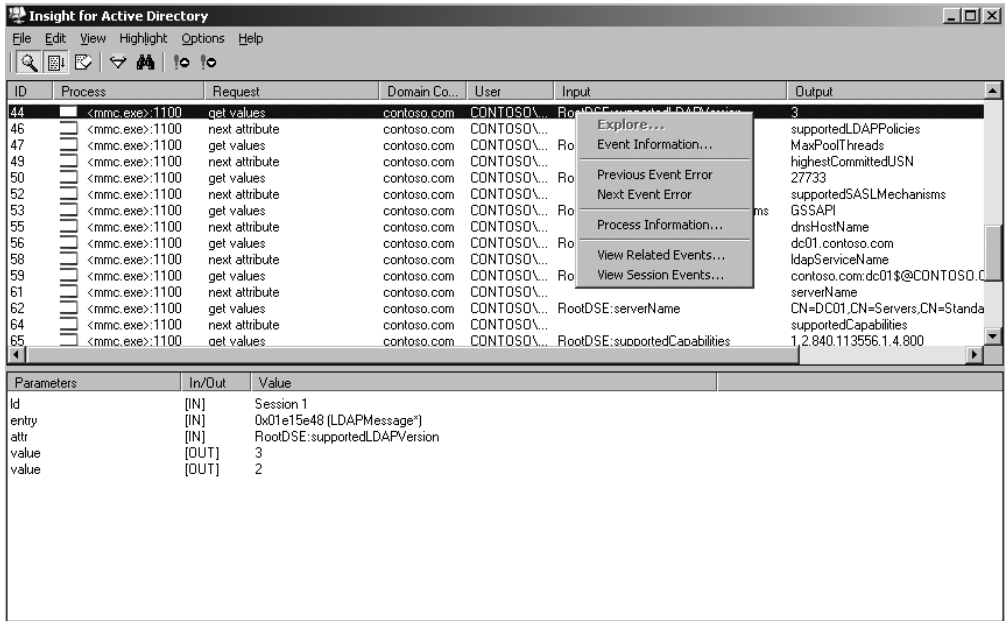
Abbildg. 8.59 Mit dem AD Explorer von Sysinternals lässt sich das Active Directory durchsuchen und Snapshots der Datenbank für die Analyse anfertigen



Insight for Active Directory (AdInsight)

Mit dem Tool AdInsight werden die LDAP-Verbindungen eines Domänencontrollers in Echtzeit mit einer grafischen Oberfläche analysiert. Dazu untersucht das Tool alle Aufrufe der Datei *Wldap32.dll*. Diese DLL wird von den meisten Programmen verwendet, wenn auf das Active Directory per LDAP zugegriffen wird. Das Tool zeigt alle Anfragen an, auch diese, die blockiert werden. Auf diesem Weg können Authentifizierungsprobleme von Active Directory-abhängigen Programmen wie zum Beispiel Exchange behoben werden. Alle Anfragen an den Domänencontroller werden protokolliert und können zur Fehlersuche auch als HTML-Bericht oder als Textdatei gespeichert werden. Wird das Programm als Administrator ausgeführt, werden auch die Zugriffe der Systemdienste angezeigt. Bestandteil des Tools ist eine englischsprachige Hilfedatei, die bei den ausführlichen Analysemöglichkeiten unterstützen kann. Nach dem Start werden zunächst keine Daten angezeigt, wenn auf den Domänencontroller nicht per LDAP zugegriffen wird. Sobald aber Programme wie Exchange oder ADSI-Edit auf den Domänencontroller zugreifen, füllt sich das Fenster mit Informationen. Per Klick mit der rechten Maustaste können weitere Informationen über die einzelnen Einträge angezeigt werden. Die Anzeige lässt sich über das Menü auch filtern.

Abbildg. 8.60 Mit AdInsight lassen sich LDAP-Zugriffe auf Domänencontroller diagnostizieren

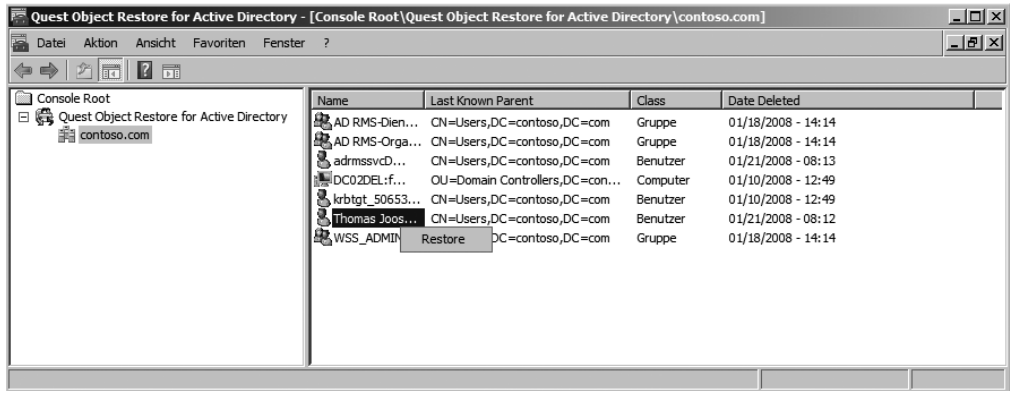


Object Restore for Active Directory

Mit diesem Freeware-Tool von Quest (*www.quest.com/object-restore-for-active-directory/*) werden einzelne, versehentlich gelöschte Objekte einfacher als mit der Windows-Datensicherung wiederhergestellt. Das Tool stellt eine grafische Oberfläche zur Verfügung und benötigt zur Wiederherstellung keinen Neustart des Domänencontrollers. Im Grunde genommen arbeitet das Programm auf dem gleichen Weg wie AdRestore von Sysinternals, aber mit grafischer Benutzeroberfläche. Die Software ist nach der Installation sechs Monate lauffähig und muss dann deinstalliert und anschließend neu installiert werden. Kosten fallen dabei keine an. Offiziell wird zwar nur Windows Server 2003 unterstützt, bei unseren Tests hat Object Restore for Active Directory aber seine Dienste problemlos auch in einer Windows Server 2008-Domäne verrichtet. Nach der Installation des Tools wird dieses über ein eigenes Snap-In einer Managementkonsole hinzugefügt oder über seine Programmgruppe gestartet. Anschließend werden die Domänen, von denen gelöschte Objekte eingelesen werden sollen, per Rechtsklick auf den Eintrag *Quest Object Restore for Active Directory* und Auswahl von *Connect To* im Kontextmenü hinzugefügt. Wird eine Domäne angeklickt, werden die gelöschten Objekte im Fenster angezeigt. Über das Kontextmenü eines gelöschten Objektes wird dieses mit dem Befehl *Restore* wiederhergestellt. Als weitere Informationen werden im Fenster das Datum der Löschung angezeigt, sowie in welcher OU das Objekt gespeichert war. Da die Löschung von Objekten noch nicht unbedingt auf alle Domänencontroller repliziert wurde, lässt sich über das Menü *Aktion* bestimmen, mit welchem Domänencontroller sich das Tool verbinden soll, um gelöschte Objekte anzuzeigen. Da es sich bei dem Programm um ein vollwertiges Snap-In für die MMC handelt, lassen sich auch spezielle Aufgabenblockansichten anpassen, über die zum Beispiel Support-Mitarbeitern eine angepasste Oberfläche mit bestimmten Domänen und Domänencontrollern zur Verfügung gestellt wird. Mit dem neuen Tool AdInsight können die LDAP-Verbindungen eines Domänencontrollers in Echtzeit analysiert werden. Auf diesem Weg können Authentifizierungsprobleme von

Active Directory-abhängigen Programmen wie zum Beispiel Exchange behoben werden. Alle Anfragen an den Domänencontroller werden protokolliert und können zur Fehlersuche auch als HTML-Bericht oder als Textdatei gespeichert werden.

Abbildg. 8.61 Mit *Object Restore for Active Directory* lassen sich auf einfache Weise gelöschte Objekte wiederherstellen



Anzeigen der geöffneten Ports mit TCPView

Mit TCPView aus der Sysinternals Suite können in einer grafischen Oberfläche alle TCP und UDP-Endpunkte eines Computers angezeigt werden. Zusätzlich wird angezeigt, welche Prozesse auf die Endpunkte und Ports zugreifen. Das Tool enthält noch das Programm *Tcpvcon.exe*, welches die gleichen Informationen wie *TCPView* in der Befehlszeile anzeigt, zum Beispiel zur Verwendung in Skripts. Nach dem Start zeigt das Tool alle Verbindungen des Computers an und löst wenn möglich die IP-Adressen noch in DNS-Namen auf, damit die Anzeige der Informationen übersichtlicher wird. Einzelne Verbindungen können durch Rechtsklick beendet und damit geschlossen werden. Das Tool eignet sich hervorragend zur Überwachung von Netzwerkverbindungen auf Computern, oder wenn Verdacht auf die Verseuchung durch einen Trojaner besteht. Das Tool verwendet als Grundlage das Windows-Bordmittel-Tool *Netstat*, ist aber wesentlich komfortabler zu bedienen und bietet schneller ausführlichere Informationen. Netstat ist beispielsweise nur in der Lage offene Ports anzuzeigen, nicht den Prozess, der den Port geöffnet hat. Das ist ein sehr großer Vorteil von TCP-View, da eine grundlegende Analyse nur durch die Kombination beider Informationen erreicht wird. Zu den Prozessen lassen sich weitere Informationen anzeigen. Wertvolle Hilfe bietet das Tool dabei nicht nur bei Verbindungen in Netzwerken, sondern auch für Verbindungen zum Internet. Die angezeigten Ports werden in Echtzeit aktualisiert und können auch farblich hervorgehoben werden, um diese besser nachverfolgen zu können.

Zusätzlichen Domänencontroller installieren (RODC)

Haben Sie eine neue Domäne installiert, sollten Sie immer so schnell wie möglich einen zusätzlichen Domänencontroller installieren. In einer Testumgebung wird das zwar nicht unbedingt notwendig sein, aber durch mehrere Domänencontroller können Sie das Verhalten von Active Directory besser testen, vor allem bezüglich der Replikation. Die Installation ist schnell durchgeführt und Sie können damit sichergehen, dass die Daten der Active Directory-Domäne bei Ausfall des ersten Servers nicht verloren gehen können. Wir zeigen Ihnen im folgenden Abschnitt, wie zusätzliche Domänencontroller in einer Domäne installiert werden. Dabei muss es sich nicht gezwungenermaßen um einen schreibgeschützten Domänencontroller handeln, wir gehen aber in diesem Beispiel davon aus.

HINWEIS Wollen Sie einen schreibgeschützten Domänencontroller installieren, achten Sie darauf, dass der PDC-Emulator auf einem Windows Server 2008-DC positioniert sein muss. Außerdem muss sich die Gesamtstruktur mindestens im Windows Server 2003-Betriebsmodus befinden.

Vorbereitungen für die Integration eines zusätzlichen Domänencontrollers in eine Domäne

Der erste Schritt bei der Integration eines zusätzlichen Domänencontrollers in eine Domäne besteht aus der Installation des Betriebssystems. Achten Sie darauf, dass Sie den Server mit dem gleichen Stand des Betriebssystems installieren, damit Sie eine homogene Umgebung erhalten.

Computername und primäres DNS-Suffix

Geben Sie dem zusätzlichen Domänencontroller zunächst einen passenden Namen, zum Beispiel *dc02*, und konfigurieren Sie das primäre DNS-Suffix auf dem Server. Gehen Sie bei diesem Schritt so vor wie bei der Erstellung des ersten Domänencontrollers.

DNS-Erweiterung installieren

Installieren Sie auf dem Rechner nach dem Neustart des Servers, wie beim ersten Server, ebenfalls die DNS-Erweiterung. Wurde der Server als Domänencontroller in das Active Directory mit aufgenommen, steht er ebenfalls als DNS-Server für die Mitgliedsserver und Arbeitsstationen zur Verfügung.

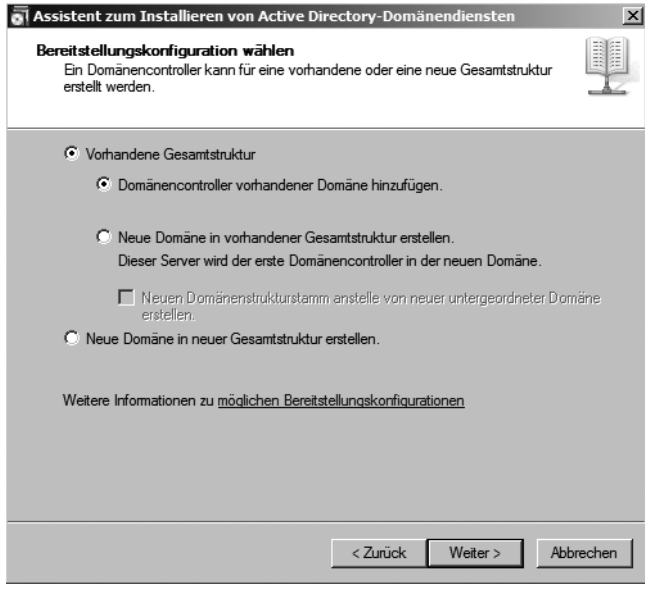
Konfigurieren der IP-Einstellungen

Weisen Sie dem zusätzlichen Domänencontroller zunächst den ersten Domänencontroller, den Sie installiert haben, als bevorzugten DNS-Server zu. Später kann diese Einstellung noch abgeändert werden, aber für das Beitreten der Domäne muss der Server einen DNS-Server in der Domäne erreichen können.

Integrieren eines neuen Domänencontrollers

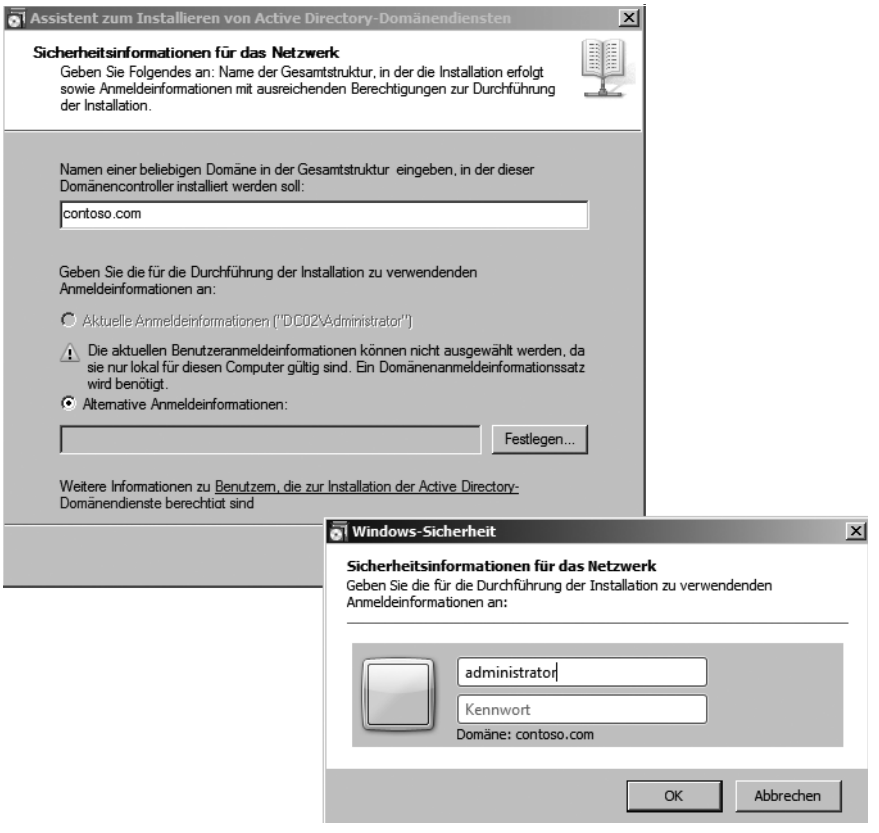
Rufen Sie im Anschluss über *Start/Ausführen/dcpromo* den Installationsassistenten von Active Directory auf dem neuen Domänencontroller auf. Aktivieren Sie auch in diesem Fall wieder die erweiterte Konfiguration. Auf dem ersten Fenster wählen Sie die Option *Vorhandene Gesamtstruktur* und dann *Domänencontroller vorhandener Domäne* hinzufügen. (Abbildung 8.62).

Abbildg. 8.62 Hinzufügen eines Domänencontrollers zu einer bestehenden Domäne



Auf der nächsten Seite des Assistenten ist automatisch die Option *Alternative Anmeldeinformationen* aktiviert. Über die Schaltfläche *Festlegen* müssen Sie das Konto eines Administrators festlegen, der über die Rechte verfügt, Domänencontroller zu einer Domäne hinzuzufügen (Abbildung 8.63). Außerdem müssen Sie auf dieser Seite den DNS-Namen der Domäne angeben, der Sie einen Domänencontroller hinzufügen wollen. Sie können zwar auch mit dem NetBIOS-Namen der Domäne arbeiten, aber die Auflösung per DNS geht schneller und ist zuverlässiger. Wichtig ist an dieser Stelle nicht, dass Sie dieser hier angegebenen Domäne einen zusätzlichen Domänencontroller hinzufügen, sondern dass Sie sich an der Gesamtstruktur authentifizieren. Damit Sie sicherstellen, dass die Authentifizierung und die Verbindung auch zur Domäne passen, der Sie einen Domänencontroller hinzufügen wollen, ist hier die Angabe dieser Domäne der beste Weg.

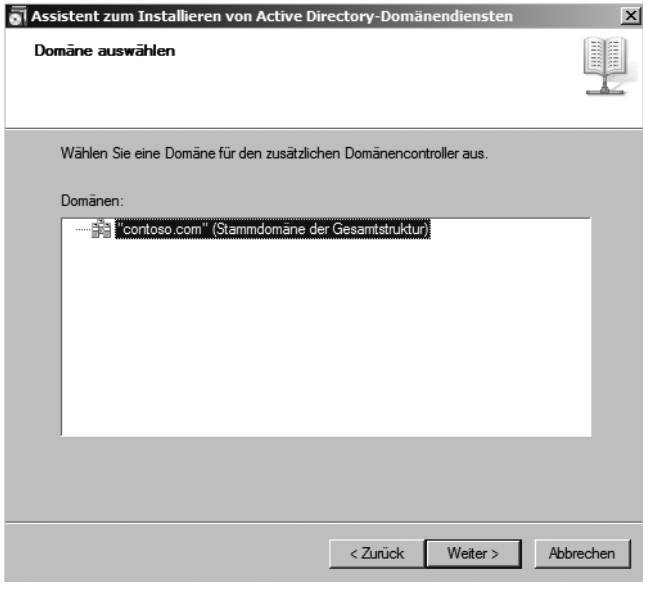
Abbildg. 8.63 Festlegen der Domäne, in der Sie einen zusätzlichen Domänencontroller hinzufügen wollen



Auf dem nächsten Fenster wählen Sie schließlich exakt die Domäne in der verbundenen Gesamtstruktur aus, der Sie einen zusätzlichen Domänencontroller hinzufügen wollen (Abbildung 8.64).

Als Nächstes wählen Sie den physischen Standort aus, in welcher der Domänencontroller positioniert wird. Diese Möglichkeit ist neu in Windows Server 2008. Bei Windows Server 2003 wurde die Zuweisung nur automatisiert durchgeführt, eine manuelle Zuweisung während dem Heraufstufen war nicht möglich.

Abbildg. 8.64 Auswählen der Domäne für den zusätzlichen Domänencontroller

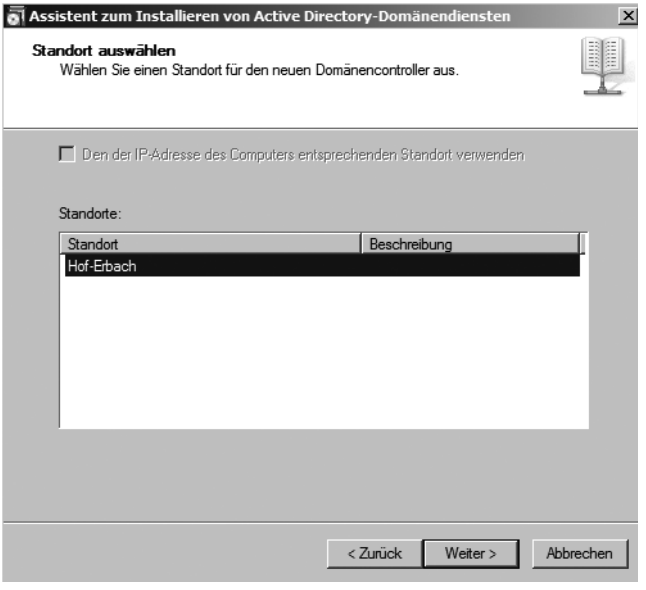


Das Active Directory bietet die Möglichkeit, eine Gesamtstruktur in mehrere Standorte zu unterteilen, die durch verschiedene IP-Subnetze voneinander getrennt sind. Durch diese physische Trennung der Standorte ist es nicht notwendig, für jede Niederlassung eine eigene Domäne zu erstellen. An jedem Standort müssen zwar weiterhin Domänencontroller installiert werden, allerdings kann die Domäne von einem zentralen Standort aus verwaltet werden, von dem die Änderungen auf die einzelnen Standorte repliziert werden können. Die Replikation zwischen verschiedenen Standorten im Active Directory läuft weitgehend automatisiert ab. Damit die Replikation aber stattfinden kann, müssen Sie zunächst die notwendige Routingtopologie erstellen. Bei der Erstellung der Routingtopologie fallen hauptsächlich folgende Aufgaben an:

- Erstellen von Standorten in der Active Directory-Verwaltung
- Erstellen von IP-Subnetzen und Zuweisen an die Standorte
- Erstellen von Standortverknüpfungen für die Replikation von Active Directory
- Konfiguration von Zeitplänen und Kosten für die optimale Standort-Replikation

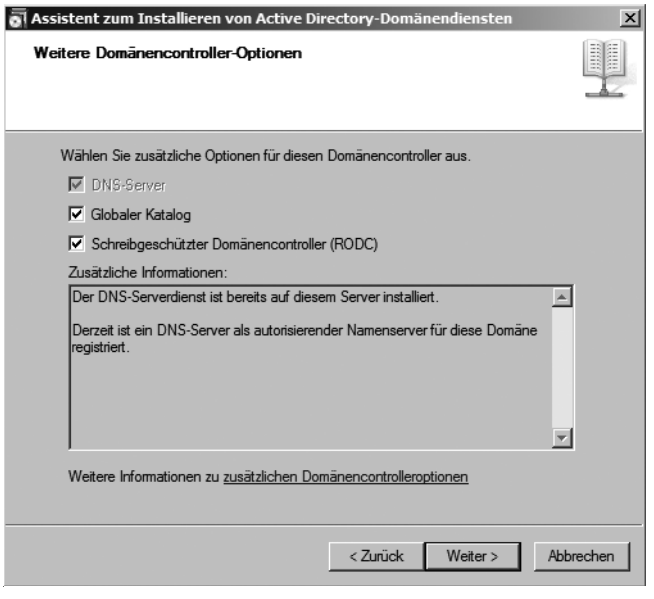
Damit Sie die standortübergreifende Replikation von Active Directory verwenden können, sollten Sie in jedem Standort, an dem später ein Domänencontroller angeschlossen wird, ein unabhängiges IP-Subnetz verwenden. Dieses IP-Subnetz wird in der Active Directory-Verwaltung hinterlegt und dient künftig zur Unterscheidung der Standorte im Active Directory. Das wichtigste Verwaltungswerkzeug, um Standorte im Active Directory zu verwalten, ist das Snap-In *Active Directory-Standorte und -Dienste*, das auch über den Server-Manager zur Verfügung gestellt wird.

Abbildg. 8.65 Auswählen des physischen Standortes



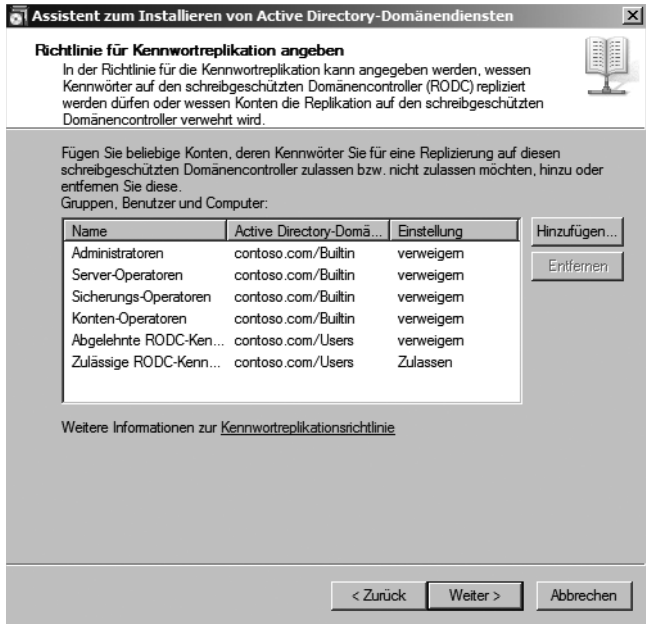
Auf der nächsten Seite des Assistenten legen Sie fest, ob der neue Domänencontroller zum globalen Katalog konfiguriert werden soll. Außerdem können Sie an dieser Stelle festlegen, dass der Domänencontroller nur als schreibgeschützter Domänencontroller verwendet wird, also dieser Server keine Änderungen entgegennimmt, außer als Replikation von seinem übergeordneten Domänencontroller (Abbildung 8.66).

Abbildg. 8.66 Konfiguration des zusätzlichen Domänencontrollers als schreibgeschützter Domänencontroller (RODC)



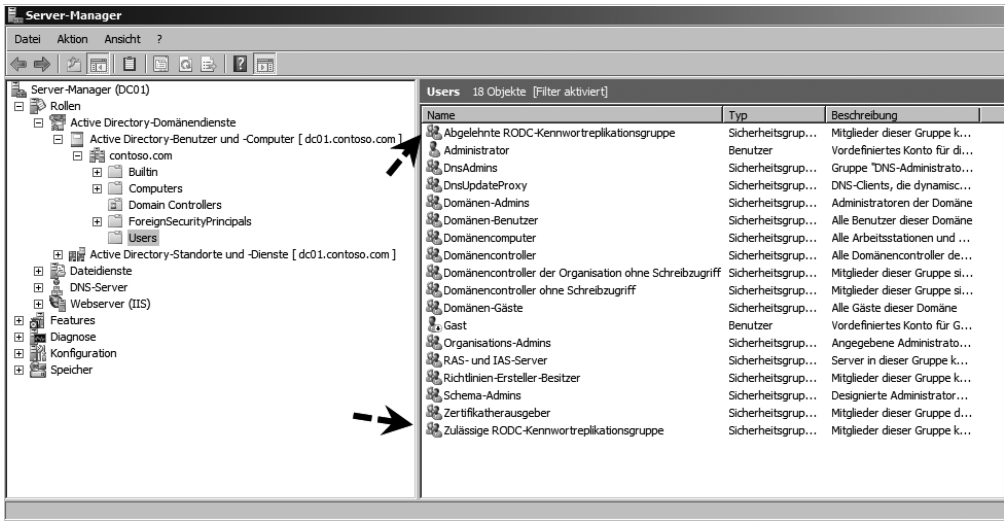
Auf der nächsten Seite wählen Sie die Benutzergruppen oder direkt die Benutzer aus, deren Kennwörter auf den RODC repliziert werden dürfen. Wird für eine Gruppe die Replikation des Kennwortes verweigert, steht den Mitgliedern dieser Gruppe der RODC nicht als Anmeldeserver zur Verfügung, da er die Kennwörter nicht verifizieren kann. Durch diese Konfiguration können Sie recht leicht festlegen, welche Benutzer sich an diesem DC anmelden dürfen und welche nicht (Abbildung 8.67). Diese Richtlinien spielen für die Authentifizierung von Benutzern an einem Domänencontroller eine wichtige Rolle. Authentifiziert sich ein Benutzer an einem RODC, kontaktiert dieser einen normalen DC, um die Anmeldeinformationen zu kopieren. Der DC erkennt, dass die Anforderung von einem RODC kommt und überprüft auf Basis der Richtlinien für die Kennwortreplikation, ob diese Daten zu dem jeweiligen RODC übertragen werden dürfen. Wird die Replikation durch die Richtlinie gestattet, werden die Anmeldeinformationen vom DC zum RODC übertragen und dort zwischengespeichert, sodass weitere Anmeldungen deutlich schneller ablaufen.

Abbildg. 8.67 Festlegen der Benutzerkonten und Gruppen, deren Kennwörter auf den RODC repliziert werden sollen



In der OU *Users* gibt es bereits die standardmäßigen Benutzergruppen *Zulässige RODC-Kennwortreplikationsgruppe* und *Abgelehnte RODC-Replikationsgruppe* (Abbildung 8.68). Benutzerkonten, die Sie diesen Benutzergruppen zuordnen, können sich an diesem Domänencontroller anmelden, da die Kennwörter repliziert wurden (*Zulässige RODC-Kennwortreplikationsgruppe*), oder Sie können sich nicht anmelden, da die Kennwörter nicht zur Verfügung stehen (*Abgelehnte RODC-Replikationsgruppe*). Sie können die Einstellungen, die Sie auf diesem Fenster vornehmen, jederzeit über die Eigenschaften des Computerkontos im Server-Manager wieder anpassen, nachdem der Server zum Domänencontroller heraufgestuft worden ist.

Abbildg. 8.68 Neue Standardgruppen im Active Directory, über die Sie die Replikation der Kennwörter auf schreibgeschützte Domänencontroller konfigurieren können

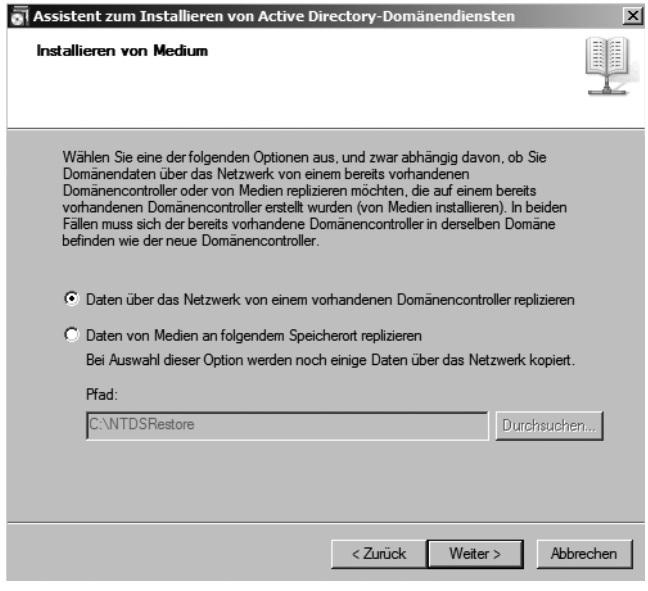


Auf der nächsten Seite des Assistenten geben Sie eine Benutzergruppe an, welche die Berechtigung erhält den Domänencontroller zu verwalten. Mitglieder der angegebenen Gruppe dürfen den Server verwalten beziehungsweise Änderungen auf dem Server vornehmen. Die Gruppe oder Benutzer, die Sie hier angeben, erhalten lokale Administratorberechtigungen auf dem Controller, verfügen aber über keinerlei Rechte in der Active Directory-Domäne.

Abbildg. 8.69 Auswählen der Benutzergruppen für den Zugriff und die Installation auf den schreibgeschützten Domänencontroller

Im nächsten Fenster legen Sie fest, ob der Domänencontroller die Daten von Active Directory über das Netzwerk oder die WAN-Leitung erhalten soll oder ob Sie die Datensicherung Ihres Active Directory verwenden (Abbildung 8.70). Diese Option ist vor allem sinnvoll, wenn Sie einen neuen Domänencontroller für eine kleine Niederlassung installieren. Ist diese Niederlassung nur über eine schmalbandige WAN-Leitung angebunden, kann die Replikation der Active Directory-Daten sehr lange dauern und vor allem die Leitung blockieren. Sie können an dieser Stelle auch auf einem Domänencontroller in der Zentrale eine Datensicherung des Servers vornehmen, diese auf CD brennen und mit der Post verschicken und dann erst auf dem Server einlesen.

Abbildg. 8.70 Festlegen des Quellmediums für die Active Directory-Replikation

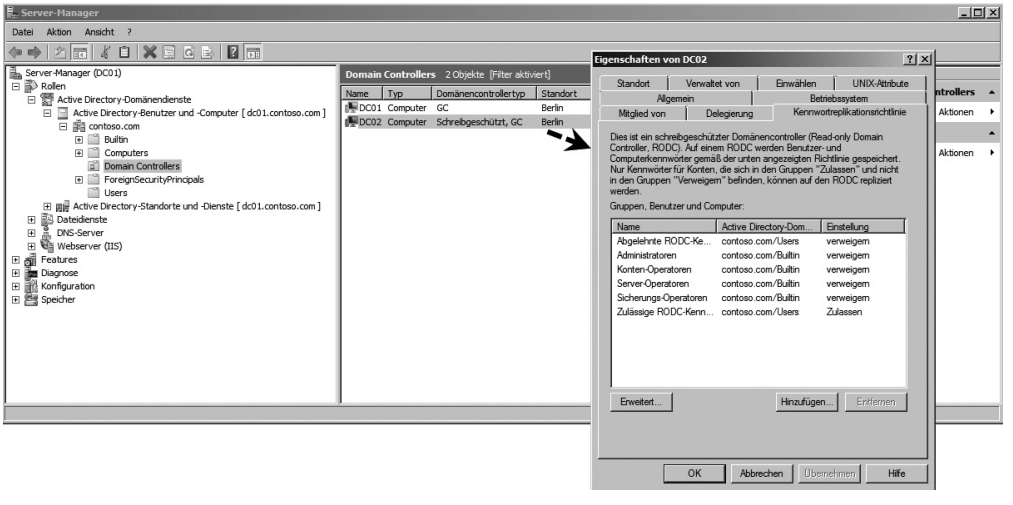


Auf der nächsten Seite des Assistenten wählen Sie aus, von welchem Domänencontroller Sie die Replikation zum neuen Domänencontroller für die Installation ausführen wollen (Abbildung 8.71). Alle weiteren Fenster sind identisch mit der Installation des ersten Domänencontrollers.

Abbildg. 8.71 Auswählen des Replikationspartners für den neuen Domänencontroller

Im Anschluss beginnt der Assistent mit der Installation von Active Directory auf dem Domänencontroller und repliziert die Daten auf den lokalen Domänencontroller. Hat der Assistent seine Arbeit beendet, können Sie den Server neu starten und sich in der Domäne anmelden. Die Installation des zusätzlichen Domänencontrollers ist damit abgeschlossen. Das Konto des neuen Domänencontrollers wird im Server-Manager angezeigt, auch dessen Typ (Abbildung 8.72).

Abbildg. 8.72 Verwalten der Computerkonten und der Kennwortreplikationsrichtlinie der Domänencontroller im Server-Manager



ACHTUNG **Einschränkungen für schreibgeschützte Domänencontroller**

Beim Einsatz von RODCs müssen einige Einschränkungen beachtet werden:

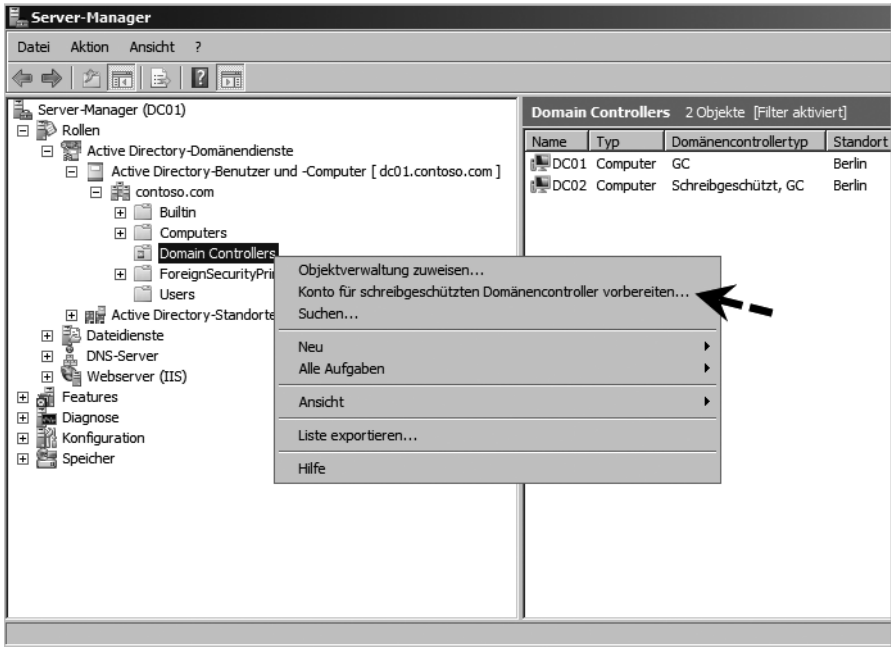
- An jedem Active Directory-Standort wird pro Windows-Domäne nur ein einzelner schreibgeschützter Domänencontroller (RODC) unterstützt.
- Zwischen RODCs kann keine Replikation durchgeführt werden.
- Wird am Active Directory-Standort ein Exchange-Server betrieben, muss an diesem Standort auch ein normaler Domänencontroller positioniert werden. Exchange Server 2003/2007 unterstützen keine RODCs für den Zugriff auf den globalen Katalog. Diese Einschränkung soll mit Windows Server 2008 R2 wegfallen.

Delegierung der RODC-Installation

Da es sich bei RODC meistens um Server in Niederlassungen handelt, besteht auch die Möglichkeit, die Installation des Servers zu delegieren. Dazu wird vorher ein neues Computerkonto für den RODC in der Domäne erstellt und der Administrator vor Ort darf den Server dann installieren und zum RODC der Domäne heraufstufen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Snap-In *Active Directory-Benutzer und -Computer*.
2. Klicken Sie in der OU *Domain Controllers* für die Domäne, in der Sie den RODC installieren wollen, mit der rechten Maustaste.
3. Wählen Sie im Kontextmenü den Eintrag *Konto für schreibgeschützten Domänencontroller vorbereiten* (Abbildung 8.73).

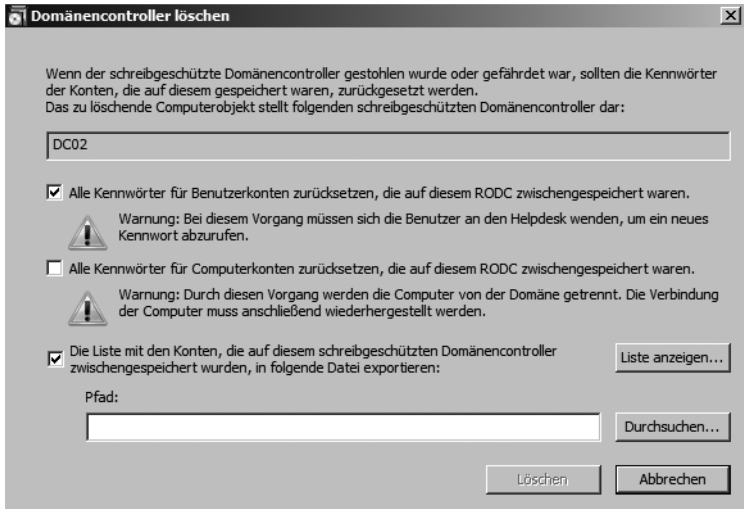
Abbildg. 8.73 Vorbereiten eines Kontos für einen RODC



4. Anschließend startet der Assistent.
5. Geben Sie den Namen des RODCs ein. Der Administrator vor Ort muss anschließend den Server exakt so benennen.
6. Anschließend können alle Optionen genauso vorgegeben werden wie bei der normalen Installation eines RODC.
7. Der Administrator kann auf dem RODC vor Ort anschließend den Assistenten über *dcpromo / UseExistingAccount:Attach* aufrufen.

HINWEIS Wird ein schreibgeschützter Domänencontroller gestohlen, enthält dieser ausschließlich nur die Daten der Benutzerkonten, die zur Replikation auf den Server explizit ausgewählt wurden. Alle anderen Daten von Active Directory sind auf dem Server nicht verfügbar und können daher auch nicht ausgelesen werden. Entfernt ein Administrator das Computerkonto des gestohlenen Domänencontrollers, erhält er ein Auswahlfenster angezeigt, auf dem die Kennwörter der Benutzer und Computer, die auf den RODC repliziert wurden, zurückgesetzt werden können. Selbst wenn es einem Dieb gelingen sollte, diese Daten vom RODC auszulesen, sind diese wertlos, weil sie zurückgesetzt wurden. Bei diesem Vorgang werden nicht die Benutzer- und Computerkonten selbst gelöscht, sondern ausschließlich nur die Kennwörter, welche von den Anwendern neu festgelegt werden können (Abbildung 8.74). Diese Daten können außerdem nicht nur zurückgesetzt werden, sondern über den Assistenten besteht auch eine Export-Möglichkeit der Konten, sodass auch manuell vorgegangen werden kann.

Abbildg. 8.74 Beim Löschen des Computerkontos eines schreibgeschützten Domänencontrollers können die Kennwörter der zwischengespeicherten Benutzerkonten zurückgesetzt werden



Notwendige Nacharbeiten nach der Integration eines zusätzlichen Domänencontrollers

Haben Sie den Domänencontroller in die Domäne aufgenommen, sollten Sie zunächst noch einige Nacharbeiten durchführen, um den Domänencontroller optimal einzubinden. Zunächst sollten Sie auf dem neuen Domänencontroller das Snap-In der DNS-Verwaltung starten. Überprüfen Sie, ob die Daten der DNS-Zonen auf den Domänencontroller repliziert wurden. Ist sichergestellt, dass die DNS-Daten repliziert wurden, ist die DNS-Funktionalität auf dem zusätzlichen Domänencontroller vorhanden. Die Replikation kann allerdings durchaus einige Minuten dauern.

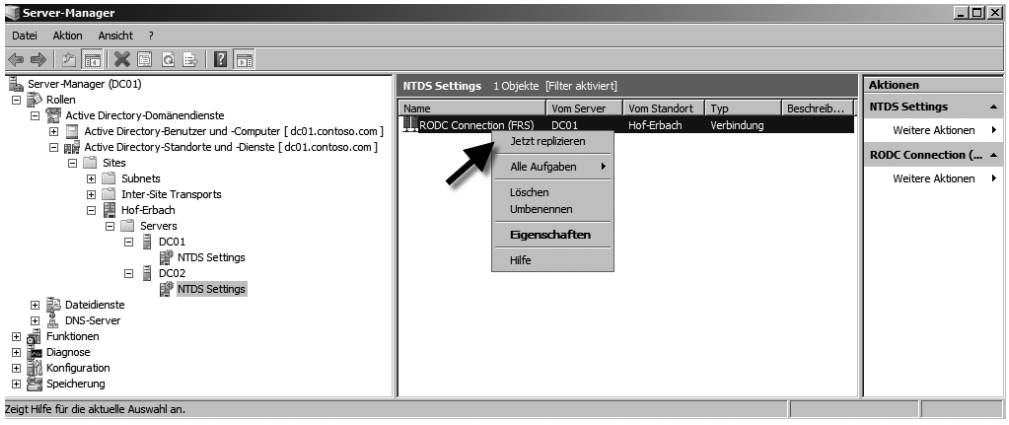
Optimierung der IP-Einstellungen auf den Domänencontrollern

Im nächsten Schritt sollten Sie die IP-Einstellungen auf den Domänencontrollern optimieren. Tragen Sie in den IP-Einstellungen jeweils den anderen Domänencontroller als bevorzugten Server und als alternativen Domänencontroller den Controller selbst ein, zumindest dann, wenn sich beide am selben Standort befinden. Durch diese Konfiguration ist sichergestellt, dass die beiden Domänencontroller über Kreuz die Namen auflösen können. Wird ein Domänencontroller neu gestartet, besteht die Möglichkeit, dass der DNS-Dienst vor dem Active Directory beendet wird und das Herunterfahren unnötig lange dauert. In diesem Fall werden darüber hinaus noch Fehlermeldungen in der Ereignisanzeige protokolliert. Aus Gründen der Ausfallsicherheit ist es daher immer am besten, wenn ein Domänencontroller jeweils einen anderen Domänencontroller als bevorzugten DNS-Server verwendet, und nur wenn dieser bevorzugte Server nicht zur Verfügung steht, seine eigenen Daten verwendet. Haben Sie diese Einstellungen vorgenommen, können Sie mit *nslookup* in der Befehlszeile überprüfen, ob die Namensauflösung auf den Domänencontrollern noch fehlerfrei funktioniert. Öffnen Sie dazu eine Befehlszeile und geben Sie *nslookup* ein. Geben Sie danach einmal die Bezeichnung des ersten und dann die des zweiten Domänencontrollers ein, also in diesem Beispiel *dc01.contoso.com* und *dc02.contoso.com*. Auf dem anderen Domänencontroller sollten Sie diese Aufgaben ebenfalls durchführen. Es sollte kein Fehler angezeigt werden, damit sichergestellt ist, dass die Namensauflösung funktioniert.

Replikation der beiden Domänencontroller überprüfen

Nach einigen Minuten sollten Sie die Replikation der beiden Domänencontroller überprüfen. Starten Sie dazu das Snap-In *Active Directory-Standorte und -Dienste* (Abbildung 8.75). Navigieren Sie zum Menü des Namens des Standortes und öffnen Sie das Menü *Servers*. An dieser Stelle sollten beide Domänencontroller angezeigt werden. Klicken Sie bei den Servern auf das Pluszeichen, sehen Sie darunter einen weiteren Menüpunkt mit der Bezeichnung *NTDS-Settings*. Klicken Sie auf diesen Menüpunkt, wird auf der rechten Seite jeder Replikationspartner des Domänencontrollers angezeigt. Klicken Sie auf diese automatisch erstellten Verbindungen mit der rechten Maustaste, können Sie aus dem Menü die Option *Jetzt replizieren* auswählen. Im Anschluss daran erscheint ein Fenster, das Sie über die erfolgreiche Replikation informiert.

Abbildg. 8.75 Überprüfen der Replikationsverbindung von neuen Domänencontrollern



Führen Sie diese Replikation für beide Domänencontroller durch, damit sichergestellt ist, dass die Active Directory-Replikation zwischen den beiden Domänencontrollern funktioniert. Damit ist die Erstellung des zusätzlichen Domänencontrollers abgeschlossen und Sie haben alle notwendigen Maßnahmen zur Überprüfung durchgeführt.

Verwalten der Betriebsmasterrollen von Domänencontrollern

In einem Active Directory sind alle Domänencontroller gleichberechtigt. Auf jedem Domänencontroller können Änderungen vorgenommen werden, die daraufhin zu den anderen Domänencontrollern repliziert werden. Allerdings gibt es fünf unterschiedliche Rollen, die ein Domänencontroller annehmen kann:

1. PDC-Emulator
2. Infrastrukturmaster
3. RID-Master
4. Schemamaster
5. Domänennamenmaster

Die verschiedenen Rollen, also PDC-Emulator, Infrastrukturmaster, RID-Master, Schemamaster und Domänennamenmaster, werden als *Flexible Single Master Operations (FSMOs)* bezeichnet. Jede dieser Rollen ist entweder einmalig pro Domäne (PDC-Emulator, Infrastrukturmaster, RID-Master) oder sogar einmalig pro Gesamtstruktur (Schemamaster, Domänennamenmaster). Fällt eine dieser Rollen aus, gibt es im Active Directory Fehlfunktionen, die schnell behoben werden müssen, da durch diese Fehlfunktionen der produktive Betrieb beeinflusst wird. Schon aus der Bezeichnung *Flexible* geht hervor, dass diese Rollen zwar einzelnen Domänencontrollern zugewiesen werden, aber auch recht flexibel verschoben werden können.

PDC-Emulator

Die Rolle des PDC-Emulators gibt es in jeder Domäne von Active Directory einmal. Der erste installierte Domänencontroller einer Active Directory-Domäne bekommt diese Rolle automatisch zugewiesen.

- Er ist für die Anwendung und Verwaltung der Gruppenrichtlinien zuständig. Steht der Domänencontroller, der diese Rolle hat, nicht mehr zur Verfügung, werden Gruppenrichtlinien fehlerhaft angewendet und können so gut wie nicht mehr verwaltet werden, da spezielle Verwaltungskonsolen, wie die Gruppenrichtlinienverwaltungskonsole (Group Policy Management Console, GPMC), gezielt die Verbindung zum PDC-Emulator aufbauen.
- Der PDC-Emulator ist darüber hinaus für Kennwortänderungen bei Benutzern verantwortlich.
- Er steuert auch die externen Vertrauensstellungen einer Domäne.
- Außerdem ist der PDC-Emulator der Zeitserver einer Domäne.

Alle hier beschriebenen Funktionen sind gestört, wenn der PDC-Emulator nicht mehr zur Verfügung steht.

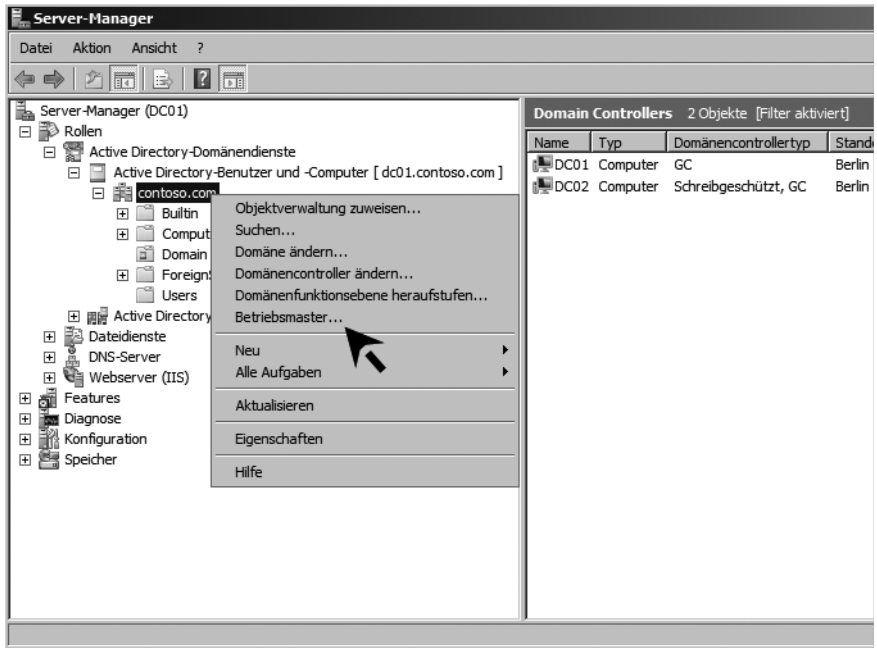
Zeitserver – W32Time

In einem Active Directory synchronisieren alle Arbeitsstationen und Mitgliedsserver ihre Zeit mit den Domänencontrollern. Alle Domänencontroller einer Domäne synchronisieren ihre Zeit mit dem PDC-Emulator. Setzen Sie mehrere Strukturen und untergeordnete Domänen ein, dann synchronisieren die PDC-Emulatoren der einzelnen Domänen ihre Zeit mit dem PDC-Emulator der jeweils übergeordneten Domäne. Der oberste Zeitserver in einer Gesamtstruktur ist der PDC-Emulator der Stamm-(Root)-Domäne, mit dem die einzelnen PDC-Emulatoren der anderen Strukturen die Zeit synchronisieren. Die Zeitsynchronisation in einem Active Directory ist sehr wichtig für die Kommunikation und die Sicherheit, auch für Exchange Server 2007. In einem Active Directory wird hauptsächlich mit dem Kerberos-Protokoll für die Authentifizierung gearbeitet. Dieses Protokoll ist extrem davon abhängig, dass die Uhren auf den Mitgliedsrechnern und Domänencontrollern synchron laufen. Sobald die Uhren mehr als fünf Minuten voneinander abweichen, kann es zu Problemen bei der Authentifizierung kommen. Aus diesem Grund ist die Rolle des PDC-Emulators wichtig, wenn nicht sogar die wichtigste. Windows Server 2008 verwendet für die Synchronisation der Uhren das NTP-Protokoll (Network Time Protocol). Dieses Protokoll kommuniziert mittels des UDP-Ports 123.

Anzeigen des PDC-Emulators

Wollen Sie überprüfen, welcher Domänencontroller die Rolle des PDC-Emulators in Ihrer Domäne verwaltet, öffnen Sie das Snap-In *Active Directory-Benutzer und -Computer* im Server-Manager oder über *Start/Ausführen/dsa.msc*. Klicken Sie mit der rechten Maustaste auf die Domäne im Snap-In und wählen Sie im Kontextmenü den Eintrag *Betriebsmaster* aus (Abbildung 8.76). Es öffnet sich ein neues Fenster. Holen Sie die Registerkarte *PDC* in den Vordergrund. Hier wird Ihnen der aktuelle PDC-Emulator der Domäne angezeigt.

Abbildg. 8.76 Anzeigen der Betriebsmaster einer Domäne



Sie können sich den aktuellen PDC-Emulator auch mit Hilfe des Befehls *dsquery server –hasfsmo pdc* in der Befehlszeile anzeigen lassen.

RID-Master

Auch die Rolle des RID-Masters erhält der erste installierte Domänencontroller einer Domäne automatisch. Den RID-Master gibt es einmal in jeder Domäne einer Gesamtstruktur. Die Aufgabe des RID-Masters ist es, den anderen Domänencontrollern einer Domäne *Relative Identifiers (RIDs)* zuzuweisen. Wird ein neues Objekt in der Domäne erstellt, also ein Computerkonto, ein Benutzer oder eine Gruppe, wird diesem Objekt eine eindeutige Sicherheits-ID (SID) zugewiesen. Diese SID erstellt der Domänencontroller aus einer domänenspezifischen SID in Verbindung mit einer RID aus seinem RID-Pool. Ist der RID-Pool eines Domänencontrollers aufgebraucht ist, werden ihm vom RID-Master neue RIDs zugewiesen. Steht der RID-Master nicht mehr zur Verfügung und bekommen die Domänencontroller damit keine RIDs mehr, können keine neuen Objekte mehr in dieser Domäne erstellt werden, bis der RID-Master wieder einem Domänencontroller zur Verfügung gestellt wird. Jeder Domänencontroller erhält zunächst einen Pool von 500 RIDs. Stehen nur noch 100 RIDs zur Verfügung, fordert er neue RIDs vom RID-Master an. Steht der RID-Master nicht mehr zur Verfügung, können also pro Domänencontroller der Domäne immerhin noch bis zu 100 neue Objekte erstellt werden, was für die meisten Organisationen ausreichen wird. Um den Domänencontroller anzuzeigen, der die Rolle des RID-Masters verwaltet, öffnen Sie wieder das Snap-In Active *Directory-Benutzer und -Computer*, klicken mit der rechten Maustaste auf die Domäne und wählen im Kontextmenü den Eintrag *Betriebsmaster* aus. Wechseln Sie auf die Regis-

terkarte *RID*. Dort wird Ihnen der RID-Master dieser Domäne angezeigt. Sie können sich den RID-Master auch mit dem Befehl *dsquery server –hasfsmo rid* in der Befehlszeile anzeigen lassen.

Abbildg. 8.77 Die Betriebsmaster einer Domäne können ebenfalls im Server-Manager angezeigt werden

Außerdem können Sie sich die erfolgreiche Verbindung und den Status des RID-Pools anzeigen lassen. Geben Sie in der Befehlszeile den Befehl *dcdiag /v /test:ridmanager* ein. Suchen Sie dann den Bereich *Starting test: RidManager* (siehe Listing 8.4). Hier sehen Sie, ob der Domänencontroller fehlerfrei eine Verbindung zum RID-Master aufbauen kann.

Listing 8.4 Testen des RID-Master mit *dcdiag*

```
      Starting test: RidManager
         * Available RID Pool for the Domain is 1600 to 1073741823
         * dc01.contoso.com is the RID Master
         * DsBind with RID Master was successful
         * rIDAllocationPool is 1100 to 1599
         * rIDPreviousAllocationPool is 1100 to 1599
         * rIDNextRID: 1102
         ..................... DC01 passed test RidManager
```

Tritt an dieser Stelle ein Fehler auf, sollten Sie am besten den RID-Master auf einen anderen Server transferieren oder verschieben.

Infrastrukturmaster

Auch den Infrastrukturmaster gibt es in jeder Domäne einer Gesamtstruktur einmal. Diese Rolle erhält ebenfalls wieder der erste installierte Domänencontroller einer Active Directory-Domäne. In einer Gesamtstruktur mit nur einer Domäne spielt dieser Betriebsmaster keine Rolle. Seine Bedeutung steigt jedoch beim Einsatz mehrerer Domänen oder Strukturen. Er hat in einer Domäne die

Aufgabe, die Berechtigungen für die Benutzer zu steuern, die aus unterschiedlichen Domänen kommen. Da die Berechtigungsanfragen sonst sehr lange dauern würden, wenn zum Beispiel in den Berechtigungen einer Ressource Benutzerkonten oder Gruppen aus unterschiedlichen Domänen gesetzt sind, dient der Infrastrukturmaster einer Domäne sozusagen als Cache für diese Zugriffe, um die Abfrage der Berechtigungen zu beschleunigen. Er wird außerdem für die Auflösung von Verteilergruppen verwendet, wenn Sie Exchange einsetzen, da auch an dieser Stelle eine Gruppe Mitglieder aus verschiedenen Domänen der Gesamtstruktur enthalten kann. Um sich den Infrastrukturmaster anzeigen zu lassen, öffnen Sie das Snap-In *Active Directory-Benutzer und -Computer*. Klicken Sie mit der rechten Maustaste auf die Domäne und wählen Sie die Option *Betriebsmaster* aus. Wechseln Sie auf die Registerkarte *Infrastruktur*. Auch den Infrastrukturmaster können Sie sich in der Befehlszeile anzeigen lassen. Verwenden Sie dazu den Befehl *dsquery server –hasfsmo infr*.

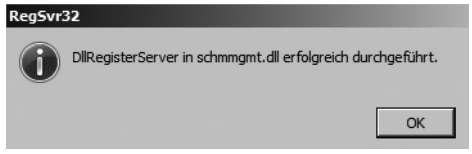
Schemamaster

Die Struktur eines Verzeichnisses, wie das Active Directory eines ist, wird *Schema* genannt. Im Schema ist genau definiert, welche Informationen auf welche Art gespeichert werden sollen. Das Active Directory speichert die Daten, das Schema definiert, wie sie gespeichert werden. Der Aufbau des Schemas ist recht einfach. Es gibt *Objekte* und es gibt *Attribute*. Die Attribute sind Objekten zugeordnet. Jeder Verzeichniseintrag ist ein Objekt. Beim Active Directory sind Objekte also Benutzer, Computer, Freigaben oder Drucker. Das Active Directory verfügt über ein erweiterbares Schema. Dieses gibt die Möglichkeit, zusätzliche Informationen im Verzeichnis flexibel zu speichern. Durch das erweiterbare Schema lassen sich jederzeit zusätzliche Objekteigenschaften hinzufügen. Diese Funktion wird beispielsweise von Exchange Server 2000/2003/2007 genutzt. Alle notwendigen Informationen zu einem E-Mail-Postfach werden im Active Directory abgelegt. Bei der Installation von Exchange 2007 wird das Schema von Active Directory um die notwendigen Attribute und Klassen erweitert. Damit das Schema erweitert werden kann, wird der *Schemamaster* benötigt. In jeder Gesamtstruktur gibt es nur einen Schemamaster. Nur auf diesem Schemamaster können Änderungen am Schema vorgenommen werden. Steht der Schemamaster nicht mehr zur Verfügung, können auch keine Erweiterungen des Schemas stattfinden und die Installation von Exchange Server 2007 schlägt fehl. Der erste installierte Domänencontroller der ersten Domäne und Struktur einer Gesamtstruktur erhält die Rolle des Schemamasters. Alle Änderungen des Schemas werden ausschließlich auf dem Schemamaster durchgeführt. Der Schemamaster hat ansonsten keine Auswirkungen auf den laufenden Betrieb. Solange das Schema nicht durch eine spezielle Applikation wie zum Beispiel die Installation von Exchange 2007 erweitert wird, spielt dieser Betriebsmaster keine Rolle.

Schemamaster anzeigen

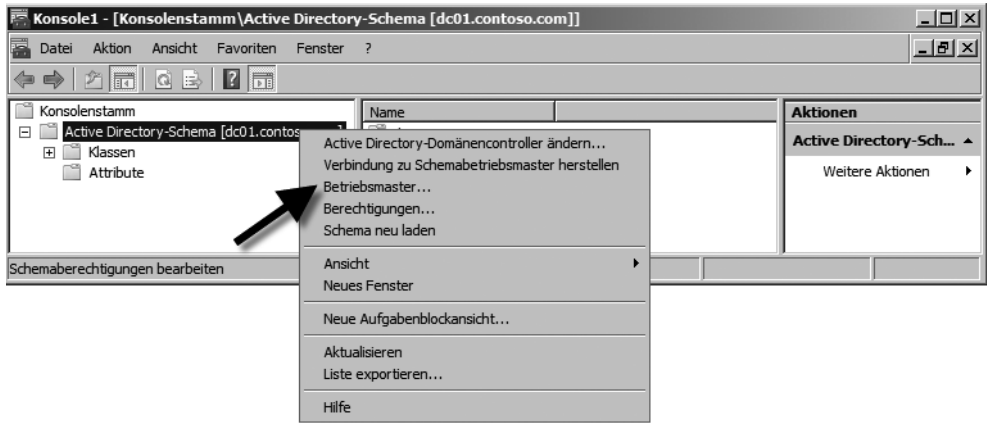
Damit der Schemamaster angezeigt werden kann, müssen Sie zunächst das Snap-In registrieren, welches das Schema anzeigt. Aus Sicherheitsgründen wird dieses Snap-In zwar installiert, jedoch nicht angezeigt. Geben Sie über *Start/Ausführen* den Befehl *regsvr32 schmmgmt.dll* ein. Sie erhalten daraufhin die Information, dass die *dll* im System erfolgreich registriert wurde (Abbildung 8.78).

Abbildg. 8.78 Registrieren der notwendigen DLL-Datei für die Anzeige der Schemaverwaltung



Im Anschluss können Sie das Snap-In *Active Directory-Schema* in eine MMC über den Menübefehl *Datei/Snap-In hinzufügen/entfernen* integrieren. Wurde dieses Snap-In integriert, können Sie das Schema verwalten und sich auch den Betriebsmaster anzeigen lassen. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Eintrag *Active Directory-Schema* und wählen Sie im Kontextmenü den Befehl *Betriebsmaster* aus (Abbildung 8.79).

Abbildg. 8.79 Anzeigen des Schemamasters



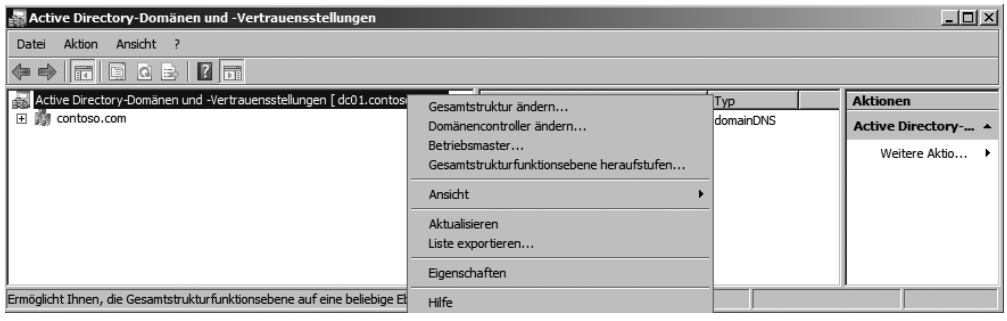
Anschließend öffnet sich ein neues Fenster, in dem der Betriebsmaster angezeigt wird. Sie können mit Hilfe dieses Fensters später den Betriebsmaster auch auf einen anderen Domänencontroller verschieben. Auch den Schemamaster können Sie sich in der Befehlszeile anzeigen lassen. Geben Sie dazu den Befehl *dsquery server –hasfsmo schema* ein.

Domänennamenmaster

Der Domänennamenmaster ist für die Erweiterung der Gesamtstruktur um neue Domänen oder Strukturen verantwortlich. In jeder Gesamtstruktur gibt es einen Domänennamenmaster. Diese Rolle wird automatisch dem ersten installierten Domänencontroller einer neuen Gesamtstruktur zugewiesen. Immer wenn ein Server zum Domänencontroller hochgestuft wird und eine neue Domäne erstellt werden soll, wird eine Verbindung zum Domänennamenmaster aufgebaut. Steht der Master nicht zur Verfügung oder kann keine Verbindung aufgebaut werden, besteht auch nicht die Möglichkeit, eine neue Domäne zur Gesamtstruktur hinzuzufügen. Der Domänennamenmaster hat im produktiven Betrieb einer Domäne oder der Gesamtstruktur keine Aufgabe. Er wird nur benötigt, wenn eine neue Domäne in der Gesamtstruktur erstellt werden soll. Um sich den Domänennamenmaster anzeigen zu lassen, benötigen Sie das Snap-In *Active Directory-Domänen und*

-*Vertrauensstellungen*. Klicken Sie mit der rechten Maustaste direkt auf das Snap-In und wählen Sie die Option *Betriebsmaster.* Danach öffnet sich ein neues Fenster, in dem der Domänennamenmaster dieser Gesamtstruktur angezeigt wird. Auch den Schemamaster können Sie sich in der Befehlszeile anzeigen lassen. Geben Sie dazu den Befehl *dsquery server –hasfsmo name* ein.

Abbildg. 8.80 Anzeigen des Domänennamenmasters im Active Directory



Verwalten und Verteilen der Betriebsmaster

Die Stabilität und Performance der Betriebsmaster spielt für die Stabilität der Gesamtstruktur eine nicht unerhebliche Rolle. Aus diesem Grund sollten die Rollen auch möglichst optimal verteilt und verwaltet werden.

Empfohlene Verteilung der FSMO-Rollen

Standardmäßig besitzt der erste installierte Domänencontroller einer Gesamtstruktur alle fünf FSMO-Rollen seiner Domäne und der Gesamtstruktur. Jeder erste Domänencontroller weiterer Domänen verwaltet die drei Betriebsmasterrollen seiner Domäne (PDC-Emulator, RID-Master, Infrastrukturmaster). Vor allem in größeren Active Directorys empfiehlt Microsoft jedoch die Verteilung der Rollen auf verschiedenen Domänencontrollern. Zur optimalen Verteilung der FSMO-Rollen gibt es folgende Empfehlungen:

- Der Infrastrukturmaster sollte nicht auf einem globalen Katalog liegen, da ansonsten Probleme bei der Auflösung von Gruppen, die Mitglieder aus verschiedenen Domänen haben, auftreten können. Bei Unternehmen mit nur einer Domäne müssen Sie diese Richtlinie nicht beachten. Installieren Sie einen zusätzlichen Domänencontroller in der Domäne, überprüft der Assistent für das Active Directory, ob sich der Infrastrukturmaster auf einem globalen Katalog befindet. Ist das der Fall, schlägt der Assistent das Verschieben der Rolle auf den neuen Domänencontroller vor.
- Domänennamenmaster und Schemamaster sollten auf einem gemeinsamen Domänencontroller liegen, der auch globaler Katalog ist.
- PDC-Emulator und RID-Master kommunizieren viel miteinander und sollten daher auf einem gemeinsamen Domänencontroller liegen, der auch globaler Katalog ist.

Anzeigen aller FSMO-Rollen

Um sich einen Überblick über alle Betriebsmaster einer Gesamtstruktur zu verschaffen, können Sie den Befehl *netdom query fsmo* in der Befehlszeile eingeben. Dadurch werden Ihnen alle Rollen dieser Domäne und der Gesamtstruktur angezeigt. So können Sie recht schnell überprüfen, ob die Verteilung der Rollen so vorgenommen wurde, wie sie von Microsoft empfohlen wird.

Übertragen eines Betriebsmasters

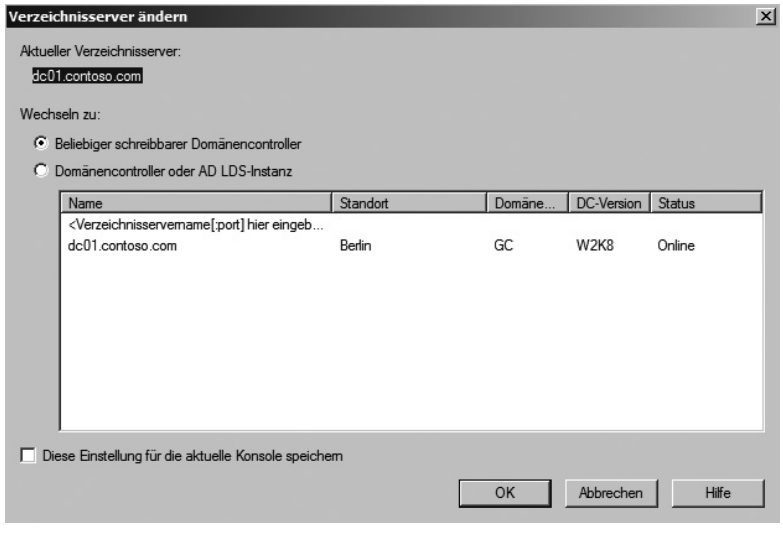
Auf Basis dieser Empfehlungen sollten Sie daher nach der Installation die Betriebsmaster entsprechend auf die einzelnen Domänencontroller der Domänen bzw. der Gesamtstruktur aufteilen. Betriebsmasterrollen können ohne weiteres im laufenden Betrieb von einem auf den anderen Domänencontroller übertragen werden. Sie sollten bei diesen Vorgängen allerdings vorsichtig sein, da bei größeren Active Directorys die Replikation etwas dauern kann und die Übertragung daher nicht sofort auf alle Domänencontroller durchgeführt wird. In diesem Fall besteht die Gefahr, dass für einzelne Anwender die übertragenen Betriebsmaster zeitweilig nicht mehr zur Verfügung stehen, was die beschriebenen Konsequenzen nach sich zieht. Am besten übertragen Sie daher diese Rollen zu einer Zeit, in der die Anwender nicht im Netzwerk arbeiten.

Übertragen des PDC-Emulators, RID-Masters und Infrastrukturmasters

Wie Sie gesehen haben, werden die drei Betriebsmaster einer Domäne auf verschiedenen Registerkarten an der gleichen Stelle angezeigt. An dieser Stelle werden die einzelnen FSMO-Rollen auch übertragen. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste im Snap-In *Active Directory-Benutzer und -Computer* auf die Domäne und wählen Sie im Kontextmenü den Eintrag *Domänencontroller ändern* aus.
2. Wählen Sie im nächsten Fenster den Domänencontroller aus, auf den Sie die Rolle übertragen wollen, und bestätigen Sie die Eingabe (Abbildung 8.81).
3. Klicken Sie dann wieder mit der rechten Maustaste auf die Domäne und wählen Sie dieses Mal *Betriebsmaster* aus.

Abbildg. 8.81 Ändern des Domänencontrollers zum Übertragen von FSMO-Rollen



4. Auf den drei Registerkarten *RID, PDC* und *Infrastruktur* wird der aktuelle Betriebsmaster und im unteren Feld der Domänencontroller, mit dem Sie sich verbunden haben, angezeigt.
5. Klicken Sie auf der Registerkarte, deren Betriebsmaster Sie verschieben wollen, auf die Schaltfläche *Ändern*. Sie können hier auch mehrere Betriebsmaster verschieben.
6. Es erscheint eine Warnung, die Sie bestätigen müssen.
7. Nach dieser Warnung erscheint die Meldung, dass der Betriebsmaster erfolgreich übertragen wurde.

Auf dieselbe Weise gehen Sie bei der Übertragung der Betriebsmaster *Schemamaster* und *Domänennamenmaster* vor. Diese beiden Betriebsmaster werden in der bekannten jeweiligen Verwaltungskonsole übertragen.

Besitzübernahme eines Betriebsmasters

Wenn der bisherige Rolleninhaber nicht mehr zur Verfügung steht, weil er zum Beispiel ausgefallen ist, besteht auch die Möglichkeit, einem anderen Domänencontroller die FSMO-Rolle fest zuzuweisen. In diesem Fall darf der ursprüngliche Rolleninhaber jedoch nicht mehr in das Active Directory integriert werden, da dieser vom Rollentausch nichts mitbekommen hat und dann zwei gleiche Betriebsmaster in einer Gesamtstruktur betrieben würden. Für die Besitzübernahme eines Betriebsmasters wird das Befehlszeilenprogramm *Ntdsutil.exe* benötigt.

Voraussetzungen für die Besitzübernahme einer FSMO-Rolle

Wenn Sie eine FSMO-Rolle auf einen anderen Domänenkontroller verschieben wollen, ohne dass der bisherige Rolleninhaber das mitbekommt, sollten Sie zwei Voraussetzungen berücksichtigen:

- Die erste Voraussetzung ist, dass der bisherige Rolleninhaber nicht mehr ins Netzwerk integriert wird. Sie können den bisherigen Rolleninhaber neu installieren und nach der Besitzübernahme sogar mit gleichem Namen wieder in das Netzwerk integrieren. Zunächst sollten Sie jedoch die Active Directory-Replikation für den Verschiebevorgang abwarten.
- Verschieben Sie den Domänennamenmaster und den Schemamaster am besten wieder auf einen anderen Domänencontroller der Root-Domäne in der Gesamtstruktur, der auch die Rolle eines globalen Katalogs hat.

Durchführen der Besitzübernahme in der Befehlszeile

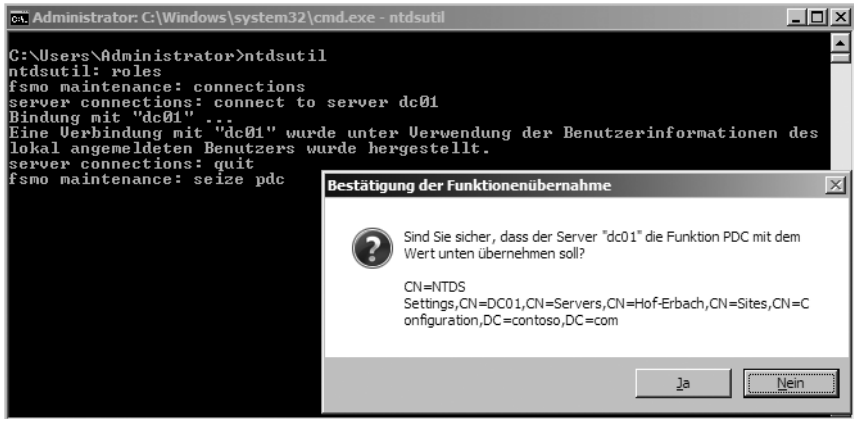
Um die Betriebsmasterrolle auf einen anderen Domänencontroller zu verschieben, öffnen Sie eine Befehlszeile und starten Sie *Ntdsutil*. Gehen Sie danach in folgender Reihenfolge vor (Abbildung 8.82):

1. Nach dem Start von *ntdsutil.exe* geben Sie den Befehl *roles* ein.
2. Geben Sie dann *connections* ein.
3. Danach geben Sie *connect to server <Servername>* ein. Tragen Sie als Name des Servers den zukünftigen Rolleninhaber ein.
4. Überprüfen Sie, ob die Verbindung hergestellt wurde und keine Fehlermeldung angezeigt wird.
5. Wenn die Verbindung erfolgreich hergestellt wurde, geben Sie den Befehl *quit* ein, damit Sie wieder im vorherigen Menü *fsmo maintenance* ankommen.
6. Geben Sie den Befehl *seize <FSMO-Rolle>* ein. Der Rollenname ist entweder *pdc* (PDC-Emulator), *rid master* (RID-Master), *schema master* (Schemamaster), *infrastructure master* (Infrastruk-

turmaster) oder *naming master* (Domänennamenmaster). In diesem Beispiel wird der Schemamaster verschoben. Der Befehl lautet also *seize schema master*.

7. Daraufhin erscheint ein Warnfenster, in dem Sie den Vorgang bestätigen müssen.
8. Nachdem Sie das Fenster bestätigt haben, versucht der Assistent zunächst, ob er den ursprünglichen Rolleninhaber erreicht und die Rolle damit normal übertragen werden kann.
9. Nach der erwarteten erfolglosen Kontaktaufnahme mit dem ursprünglichen Rolleninhaber wird die Rolle ohne weitere Zwischenfrage auf den neuen Server verschoben.

Abbildg. 8.82 Verschieben von FSMO-Rollen mit *ntdsutil.exe*



Sie können Rollen mit *ntdsutil* auch wie in der grafischen Oberfläche übertragen, wenn der ursprüngliche Betriebsmaster also noch normal funktioniert. Geben Sie in diesem Fall statt des Befehls *seize <FSMO-Rolle>* den Befehl *transfer <FSMO-Rolle>* ein. Die sonstige Syntax des Befehls ist identisch. Um die einzelnen Rollen zu übertragen, können Sie in *Ntdsutil* folgende Befehle verwenden:

- **PDC Emulator** *transfer pdc*
- **RID-Master** *transfer rid master*
- **Schemamaster** *transfer schema master*
- **Infrastrukturmaster** *transfer infrastructure master*
- **Domänennamenmaster** *transfer naming master*

Der globale Katalog

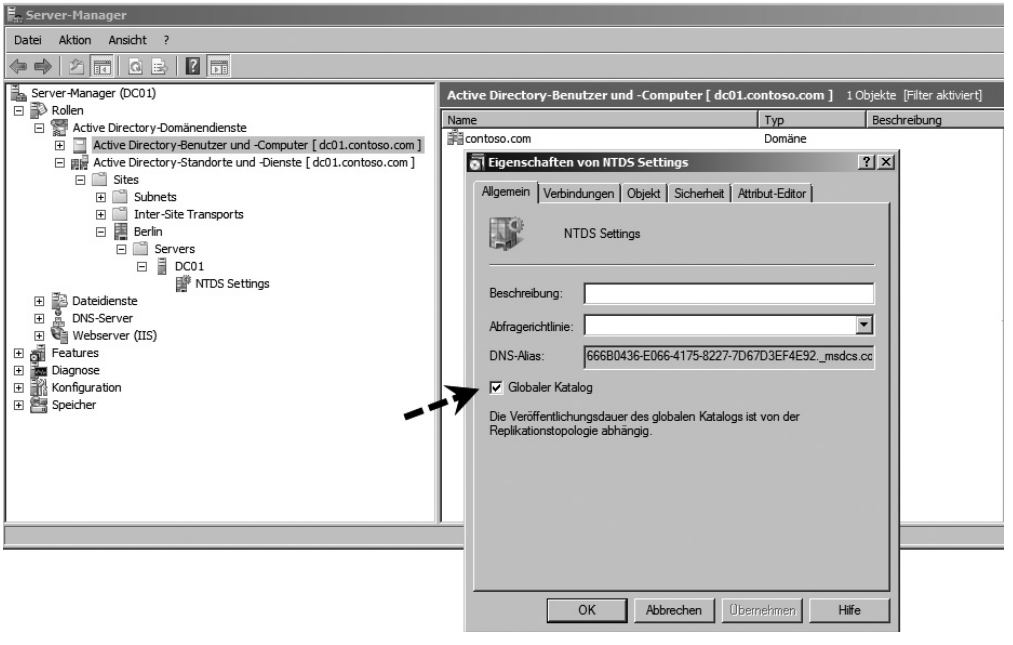
An jedem Standort im Active Directory sollte ein globaler Katalog-Server installiert sein. Der globale Katalog ist eine weitere Rolle, die ein Domänencontroller einnehmen kann. Im Gegensatz zu den beschriebenen FSMO-Rollen kann (und sollte auch) die Funktion des globalen Katalogs mehreren Domänencontrollern zugewiesen werden. Dem globalen Katalog kommt in einer Active Directory-Domäne eine besondere Bedeutung zu. Er enthält einen Index aller Domänen einer Gesamtstruktur. Aus diesem Grund wird er von Serverdiensten wie Exchange Server 2007 und Suchanfragen verwendet, wenn Objekte aus anderen Domänen Zugriff auf eine Ressource der lokalen Domäne enthalten.

Der globale Katalog spielt darüber hinaus eine wesentliche Rolle bei der Anmeldung von Benutzern. Steht der globale Katalog in einer Domäne nicht mehr zur Verfügung, können sich keine Benutzer mehr anmelden, wenn keine speziellen Vorbereitungen getroffen worden sind. Ein Domänencontroller mit der Funktion des globalen Katalogs repliziert sich nicht nur mit den Domänencontrollern seiner Domäne, sondern enthält eine Teilmenge aller Domänen in der Gesamtstruktur. Der erste installierte Domänencontroller einer Gesamtstruktur ist automatisch ein globaler Katalog. Alle weiteren globalen Kataloge müssen hingegen manuell hinzugefügt werden. Der globale Katalog dient auch zur Auflösung von universalen Gruppen. Sie sollten aber nicht alle Domänencontroller zu globalen Katalogen machen, da dadurch der Replikationsverkehr zu diesen Domänencontrollern stark zunimmt. An jedem Standort sollten zwei bis drei Domänencontroller diese Aufgabe übernehmen. Während der Heraufstufung zum Domänencontroller können Sie diese Auswahl bereits treffen. Aber auch nachträglich können Sie einen Domänencontroller zum globalen Katalog konfigurieren:

1. Um einen Domänencontroller als globalen Katalog zu konfigurieren, benötigen Sie das Snap-In *Active Directory-Standorte und -Dienste* aus dem Server-Manager.
2. Öffnen Sie dieses Snap-In und rufen Sie die Eigenschaften der Option *NTDS Settings* über *Sites/<Name des Standortes>/Servers/<Servername>* auf.
3. Auf der Registerkarte *Allgemein* aktivieren Sie das Kontrollkästchen *Globaler Katalog*.

Haben Sie diese Konfiguration vorgenommen, repliziert sich der Server zukünftig mit weiteren Domänencontrollern und enthält nicht nur Informationen seiner Domäne, sondern einen Index der Gesamtstruktur.

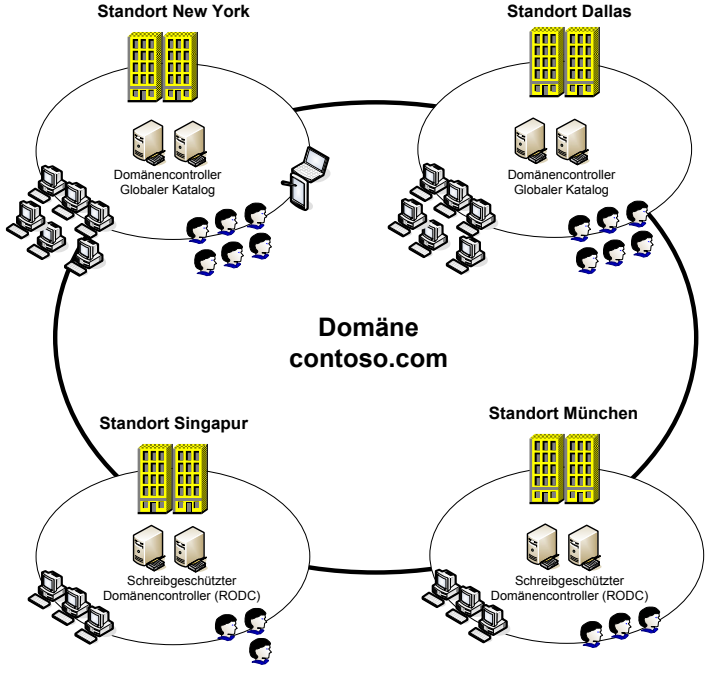
Abbildg. 8.83 Festlegen eines globalen Katalogs



Active Directory-Replikation und -Standorte

Ein weiterer wichtiger Bereich in der Verwaltung und Erstellung von Active Directorys ist die Replikation der Domänencontroller, vor allem über mehrere Standorte hinweg. Active Directory-Domänen lassen sich über mehrere physische Standorte verteilen. Das Active Directory bietet die Möglichkeit, eine Gesamtstruktur in mehrere Standorte zu unterteilen, die durch verschiedene IP-Subnetze voneinander getrennt sind (Abbildung 8.84).

Abbildg. 8.84 Standorte in Active Directory



Durch diese physische Trennung der Standorte ist es nicht mehr notwendig, für jede Niederlassung eine eigene Domäne zu erstellen. An jedem Standort müssen zwar weiterhin Domänencontroller installiert werden, allerdings kann die Domäne von einem zentralen Standort aus verwaltet werden, von dem die Änderungen auf die einzelnen Standorte repliziert werden können.

Konfiguration der Routingtopologie im Active Directory

Die Replikation zwischen verschiedenen Standorten im Active Directory läuft weitgehend automatisiert ab. Damit die Replikation aber stattfinden kann, müssen Sie zunächst die notwendige Routingtopologie erstellen. Bei der Erstellung der Routingtopologie fallen hauptsächlich folgende Aufgaben an, die auf den nächsten Seiten ausführlicher behandelt werden:

- Erstellen von Standorten in der Active Directory-Verwaltung

- Erstellen von IP-Subnetzen und Zuweisen an die Standorte
- Erstellen von Standortverknüpfungen für die Replikation von Active Directory
- Konfiguration von Zeitplänen und Kosten für die optimale Standort-Replikation

Damit Sie die standortübergreifende Replikation von Active Directory verwenden können, sollten Sie in jedem Standort, an dem später ein Domänencontroller angeschlossen wird, ein unabhängiges IP-Subnetz verwenden. Dieses IP-Subnetz wird in der Active Directory-Verwaltung hinterlegt und dient fortan zur Unterscheidung der Standorte im Active Directory. Das wichtigste Verwaltungswerkzeug, um Standorte im Active Directory zu verwalten, ist das Snap-In *Active Directory-Standorte und -Dienste*.

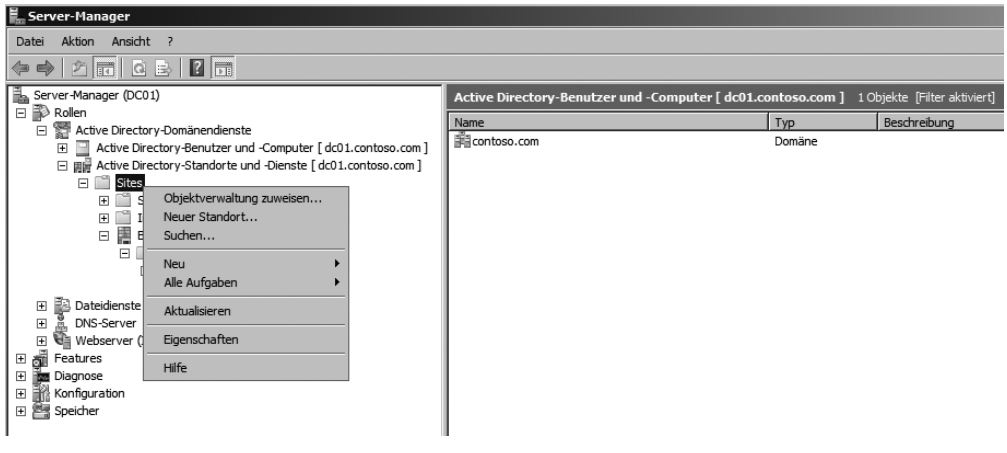
Voraussetzungen für eine Routingtopologie

Die Standorte müssen mit WAN-Leitungen angebunden werden. Dazu ist es nicht unbedingt notwendig, dass jeder Standort mit der Zentrale durch eine Sterntopologie angebunden ist. Die Replikation im Active Directory ermöglicht auch die Anbindung von Standorten, die zwar mit anderen Standorten verbunden sind, aber nicht mit der Zentrale. In jedem Standort sollten darüber hinaus ein oder mehrere unabhängige IP-Subnetze verwendet werden. Das Active Directory unterscheidet auf Basis dieser IP-Subnetze, ob Domänencontroller zum gleichen oder zu unterschiedlichen Standorten gehören.

Erstellen von neuen Standorten in *Active Directory-Standorte und -Dienste*

Sobald die Voraussetzungen für die Routingtopologie vorhanden sind, sollten Sie die einzelnen physischen Standorte im Snap-In *Active Directory-Standorte und -Dienste* erstellen. Wenn Sie das Snap-In öffnen, wird unterhalb des Menüpunktes *Sites* der erste Standort als *Standardname-des-ersten-Standortes* bezeichnet. Im ersten Schritt sollten Sie für diesen Standardnamen den richtigen Namen eingeben, indem Sie ihn mit der rechten Maustaste anklicken und *Umbenennen* wählen. Sie müssen die Domänencontroller im Anschluss nicht neu starten, der Name wird sofort aktiv. Als Nächstes können Sie alle notwendigen Standorte erstellen, an denen Sie Domänencontroller installieren wollen. Klicken Sie dazu mit der rechten Maustaste im Snap-In in der Konsolenstruktur auf den Eintrag *Sites* und wählen Sie im Kontextmenü den Befehl *Neuer Standort* aus. Sie finden das Snap-In am schnellsten über den Server-Manager.

Abbildg. 8.85 Erstellen eines neuen Standorts in Active Directory

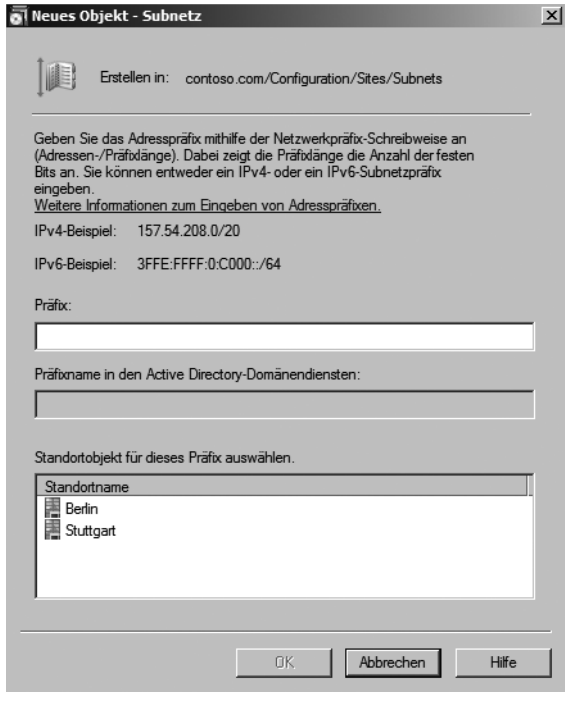


Es öffnet sich ein neues Fenster, in dem Sie den Namen des Standortes sowie die Standortverknüpfung, die diesem Standort zugewiesen werden soll, auswählen können. Standardmäßig gibt es bereits die Verknüpfung *DEFAULTIPSITELINK*. Verwenden Sie bei der Erstellung eines neuen Standortes zunächst diese Standortverknüpfung. Bestätigen Sie die Erstellung mit *OK*, erhalten Sie eine Mitteilung, welche Aufgaben nach der Erstellung noch notwendig sind. Bestätigen Sie diese Meldung, damit der Standort erstellt wird. Anschließend erscheint der neue Standort im Snap-In. Legen Sie auf die gleiche Weise alle Standorte in Ihrer Gesamtstruktur an. Nur Mitglieder der Gruppe Organisations-Admins dürfen neue Standorte im Active Directory erstellen.

Erstellen und zuweisen von IP-Subnetzen

Nachdem Sie die Standorte erstellt haben, an denen Domänencontroller installiert werden sollen, müssen Sie IP-Subnetze anlegen und diese dem jeweiligen Standort zuweisen. Um ein neues Subnetz zu erstellen, klicken Sie mit der rechten Maustaste im Snap-In *Active Directory-Standorte und -Dienste* in der Konsolenstruktur auf den Eintrag *Subnets* und wählen Sie im Kontextmenü den Befehl *Neues Subnetz* aus. Es öffnet sich ein neues Fenster, in dem Sie das IP-Subnetz definieren und dem jeweiligen Standort zuweisen können (Abbildung 8.86).

Abbildg. 8.86 Erstellen von Subnetzen in Windows Server 2008



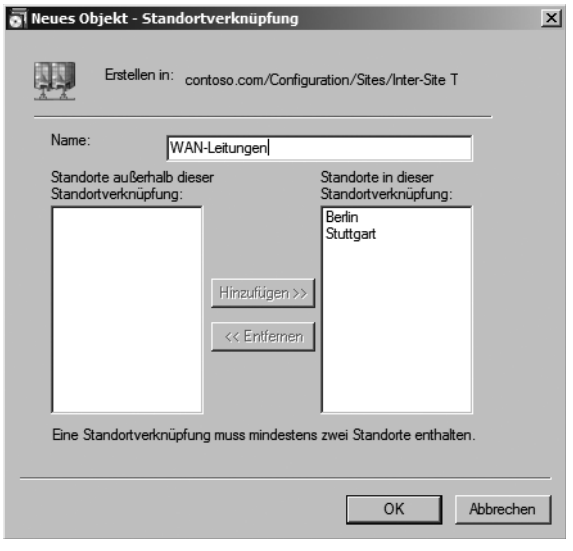
In Windows Server 2008 können Sie auch Subnetze auf IPv6-Basis erstellen. Nachdem Sie das Subnetz erstellt haben und die Erstellung mit *OK* bestätigen, wird es unterhalb des Menüs *Subnets* angezeigt. Wiederholen Sie diesen Vorgang für jedes Subnetz in Ihrem Unternehmen. Auch IP-Subnetze, in denen keine Domänencontroller installiert sind, in denen aber unter Umständen Mitgliedsrechner liegen, die sich bei dem Domänencontroller anmelden, sollten Sie an dieser Stelle anlegen und

dem entsprechenden Standort zuweisen. Wenn Sie den Konsoleneintrag *Subnets* anklicken, werden Ihnen auf der rechten Seite alle IP-Subnetze und die ihnen zugewiesenen Standorte angezeigt. Die Zuweisung des Subnetzes zu einem bestimmten Standort kann jederzeit über dessen Eigenschaften geändert werden. Sie können auch nachträglich Standorte erstellen und neue Subnetze vorhandenen Standorten zuweisen.

Erstellen von Standortverknüpfungen und Standortverknüpfungsbrücken

Nachdem Sie Standorte und die in den Standorten vorhandenen IP-Subnetze erstellt haben, können Sie neue *Standortverknüpfungen* anlegen. Bei der Installation von Active Directory wird bereits automatisch die Standortverknüpfung *DEFAULTIPSITELINK* angelegt. Für viele Unternehmen reicht diese Verknüpfung bereits aus. Wenn Sie in Ihrem Unternehmen verschiedene Bandbreiten der WAN-Leitungen einsetzen, macht es Sinn, auch verschiedene Standortverknüpfungen zu erstellen. Sie können auf Basis jeder Standortverknüpfung einen Zeitplan festlegen, wann die Replikation möglich ist. Standortverknüpfungen können auf Basis von *IP* oder *SMTP* erstellt werden. SMTP hat starke Einschränkungen bei der Replikation und wird nur selten verwendet. Sie sollten daher auf das IP-Protokoll setzen, über das von Active Directory alle Daten repliziert werden können. Um eine neue Standortverknüpfung zu erstellen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Eintrag *IP* unterhalb des Knotens *Inter-Site Transports*. Wählen Sie im zugehörigen Kontextmenü den Befehl *Neue Standortverknüpfung* aus.

Abbildg. 8.87 Erstellen von Standortverknüpfungen zur Anbindung von Niederlassungen

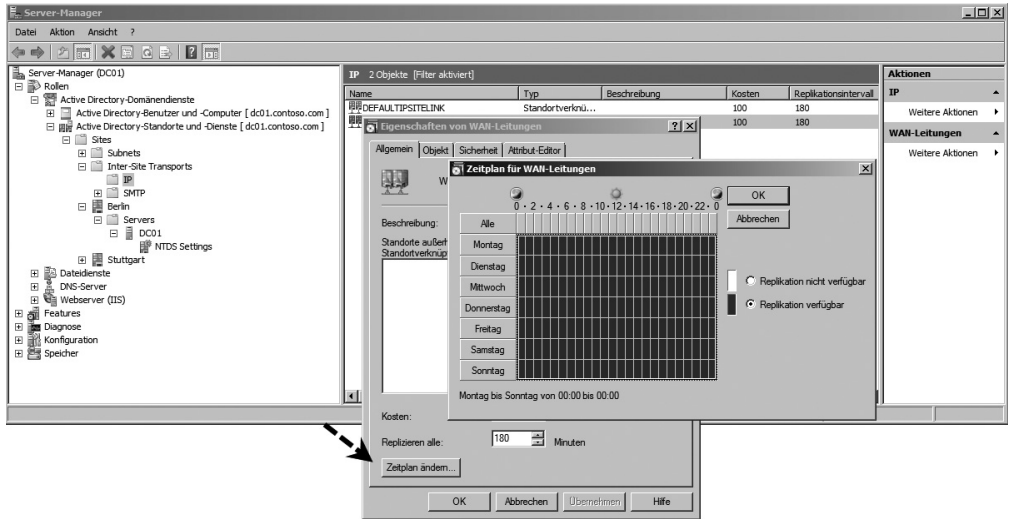


Nachdem Sie die Erstellung einer neuen Standortverknüpfung gewählt haben, erscheint das Fenster, in dem Sie die Bezeichnung der Standortverknüpfung sowie die Standorte eingeben (Abbildung 8.87). Wählen Sie den Namen der Standortverknüpfung so, dass bereits durch die Bezeichnung der Standortverknüpfung darauf geschlossen werden kann, welche Standorte miteinander verbunden sind, zum Beispiel *Berlin <> Stuttgart* oder auch die Art der Verbindung zwischen den verschiedenen Niederlassungen. In diesem Fenster können Sie auswählen, welche Standorte mit dieser Standortverknüpfung verbunden werden. Ein Standort kann Mitglied mehrerer Standortverknüpfungen

sein. Die Replikation findet immer über die Standortverknüpfungen statt, deren Kosten am geringsten sind. Wenn Sie den Namen der neuen Standortverknüpfung und deren Mitglieder festgelegt haben, können Sie mit *OK* die Erstellung abschließen. Klicken Sie das Protokoll *IP* an, werden auf der rechten Seite alle erstellten Standortverknüpfungen angezeigt.

Nachdem Sie die Standortverknüpfung erstellt haben, können Sie die Eigenschaften der Verknüpfung im Snap-In *Active Directory-Standorte und -Dienste* anpassen. Auf der Registerkarte *Allgemein* können Sie zunächst festlegen, in welchem Intervall die Informationen zwischen den Standorten repliziert werden sollen. Standardmäßig ist die Replikation auf alle drei Stunden sowie die Kosten auf 100 eingestellt. Die Active Directory-Replikation verwendet immer die Standortverknüpfungen, deren Kosten bei der Verbindung am günstigsten sind. Wenn Sie auf die Schaltfläche *Zeitplan ändern* klicken, können Sie festlegen, zu welchen Zeiten die Replikation über diese Standortverknüpfung möglich ist. Sie können zum Beispiel für Niederlassungen mit schmalbandiger Verbindung die Replikation nur außerhalb der Geschäftszeiten oder am Wochenende zulassen. Die Replikationsdaten von Active Directory werden zwischen verschiedenen Standorten komprimiert.

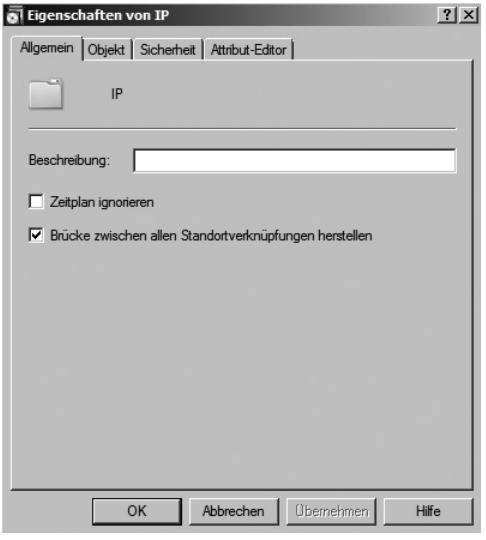
Abbildg. 8.88 Konfigurieren der Replikation von verschiedenen Standorten



Standortverknüpfungsbrücken

Den Kontextmenübefehl *Neue Standortverknüpfungsbrücke* benötigen Sie an dieser Stelle nicht. *Standortverknüpfungsbrücken* werden verwendet, wenn zwischen zwei Standorten keine physische Verbindung besteht, aber beide über einen dritten Standort angebunden sind. Standortverknüpfungsbrücken werden automatisch erstellt. Sie müssen diese nur dann manuell erstellen, wenn Sie den Automatismus deaktivieren. Diese automatische Erstellung können Sie deaktivieren, wenn Sie die Eigenschaften des Eintrags *IP* unterhalb des Knotens *Inter-Site Transports* aufrufen und das Kontrollkästchen *Brücke zwischen allen Standortverknüpfungen herstellen* deaktivieren (Abbildung 8.89).

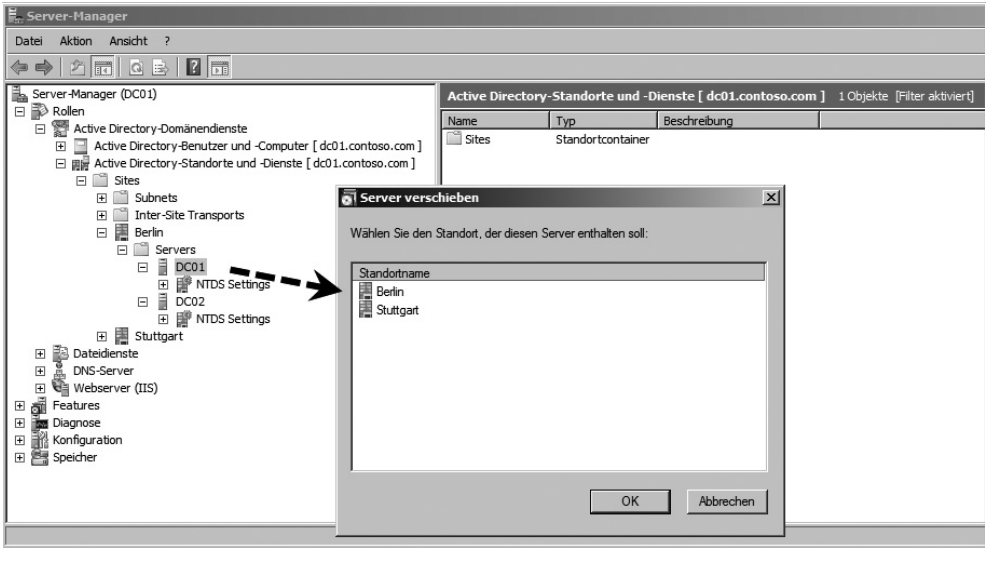
Abbildg. 8.89 Konfigurieren von Standortverknüpfungsbrücken



Zuweisen der Domänencontroller zu den Standorten

Nachdem Sie die Routingtopologie erstellt haben, werden neu installierte Domänencontroller durch ihre IP-Adresse automatisch dem richtigen Standort zugewiesen. Bereits installierte Domänencontroller müssen Sie jedoch manuell an den richtigen Standort verschieben. Klicken Sie dazu den Server im Snap-In *Active Directory-Standorte und -Dienste* mit der rechten Maustaste an und wählen Sie im Kontextmenü den Befehl *Verschieben* aus. Dann werden Ihnen alle Standorte angezeigt und Sie können den neuen Standort des Domänencontrollers auswählen (Abbildung 8.90).

Abbildg. 8.90 Verschieben von Domänencontrollern zwischen Standorten

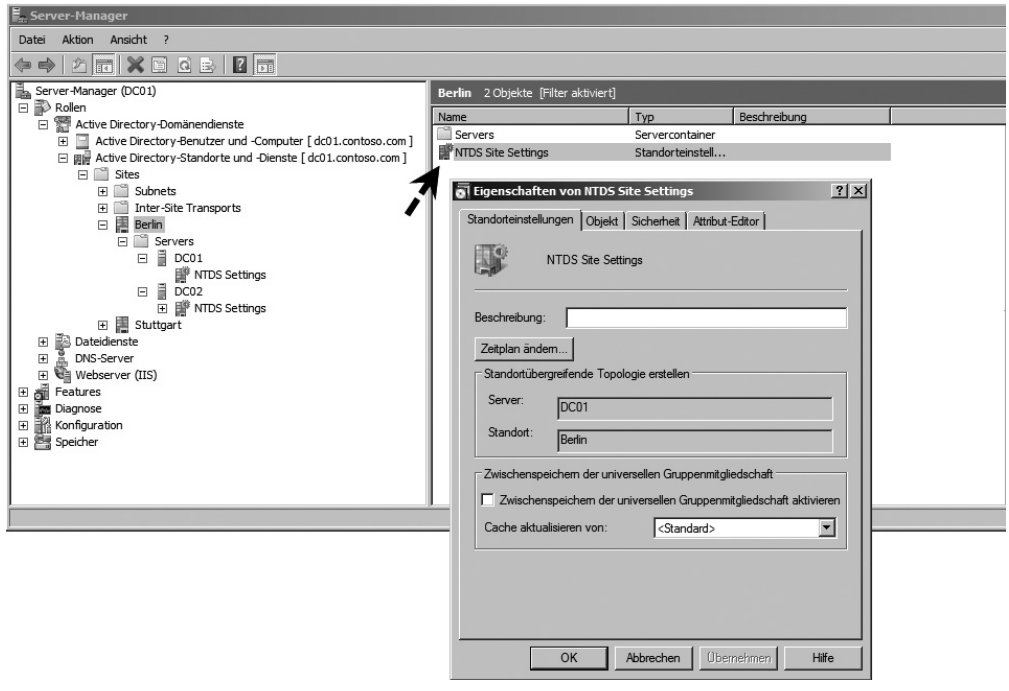


Nachdem Sie den Domänencontroller an einen anderen Standort verschoben haben, sollten Sie den Server neu starten. Sie können einen Domänencontroller auch mit Drag & Drop an einen anderen Standort verschieben. Achten Sie vor dem Verschieben des Domänencontrollers darauf, dass die IP-Einstellungen des Servers zu den zugewiesenen IP-Subnetzen des neuen Standortes passen.

Der Knowledge Consistency Checker (KCC)

Wenn Sie die Routingtopologie wie beschrieben erstellt haben, kann der KCC die Verbindung der Domänencontroller automatisch herstellen. Der KCC konfiguriert auf Basis der konfigurierten Standorte, der Standortverknüpfungen und deren Zeitplänen und Kosten sowie den enthaltenen Domänencontrollern automatisch die Active Directory-Replikation. Der KCC läuft vollkommen automatisch auf jedem Domänencontroller der Gesamtstruktur. Sind zwei Standorte nicht durch Standortverknüpfungen verbunden, erstellt er automatisch Standortverknüpfungsbrücken, wenn eine Verbindung über einen dritten Standort hergestellt werden kann. Der KCC verbindet nicht jeden Domänencontroller mit jedem anderen, sondern erstellt eine intelligente Topologie. Er überprüft die vorhandenen Verbindungen alle 15 Minuten auf ihre Funktionalität und ändert bei Bedarf automatisch die Replikationstopologie.

Abbildg. 8.91 Anzeigen des ISTG eines Standorts



Innerhalb eines Standortes erstellt der KCC möglichst eine Ringtopologie, wobei zwischen zwei unterschiedlichen Domänencontrollern maximal drei andere Domänencontroller stehen sollten. Zwischen verschiedenen Standorten werden die Active Directory-Daten nicht von allen Domänencontrollern auf die anderen Domänencontroller der Standorte übertragen, sondern immer jeweils nur von einem Domänencontroller. Dieser Domänencontroller, auch *Brückenkopfserver (Bridge-*

headserver) genannt, repliziert sich mit den Bridgeheadservern der anderen Standorte automatisch. Der KCC legt automatisch fest, welche Domänencontroller in einer Niederlassung zum Bridgeheadserver konfiguriert werden, Sie müssen keine Eingaben oder Maßnahmen vornehmen. Die Auswahl der Bridgeheadserver in einem Standort übernimmt der *Intersite Topology Generator (ISTG)*, ein Dienst, der zum KCC gehört. Der KCC wiederum legt für jedem Standort fest, welcher Domänencontroller der ISTG sein soll. Wenn Sie einen Standort im Snap-In *Active Directory-Standorte und -Dienste* anklicken, wird auf der rechten Seite der Eintrag *NTDS Site Settings* angezeigt. Rufen Sie die Eigenschaften dieses Menüpunktes auf, wird Ihnen im Bereich *Standortübergreifende Topologie erstellen* der derzeitige ISTG angezeigt (Abbildung 8.91).

Zwischenspeichern der universellen Gruppenmitgliedschaft

An dieser Stelle können Sie auch das Kontrollkästchen *Zwischenspeichern der universellen Gruppenmitgliedschaft aktivieren* einschalten. Diese Option wirkt sich dann aus, wenn Sie am Standort keinen globalen Katalog betreiben, der die Mitgliedschaften der universellen Gruppen zwischenspeichert. Da universelle Gruppen Mitglieder aus mehreren Domänen und Standorten enthalten können, ist die Information, welche Benutzerkonten Mitglied sind, bei der Anmeldung eines Benutzers oder dem Zugreifen auf Ressourcen sehr wichtig. Haben Sie an einem Standort keinen globalen Katalog installiert, sollten Sie auf mindestens einem Domänencontroller diese Option aktivieren. Wenn Sie das Zwischenspeichern der universellen Gruppenmitgliedschaft aktivieren, ergeben sich die folgenden Vorteile:

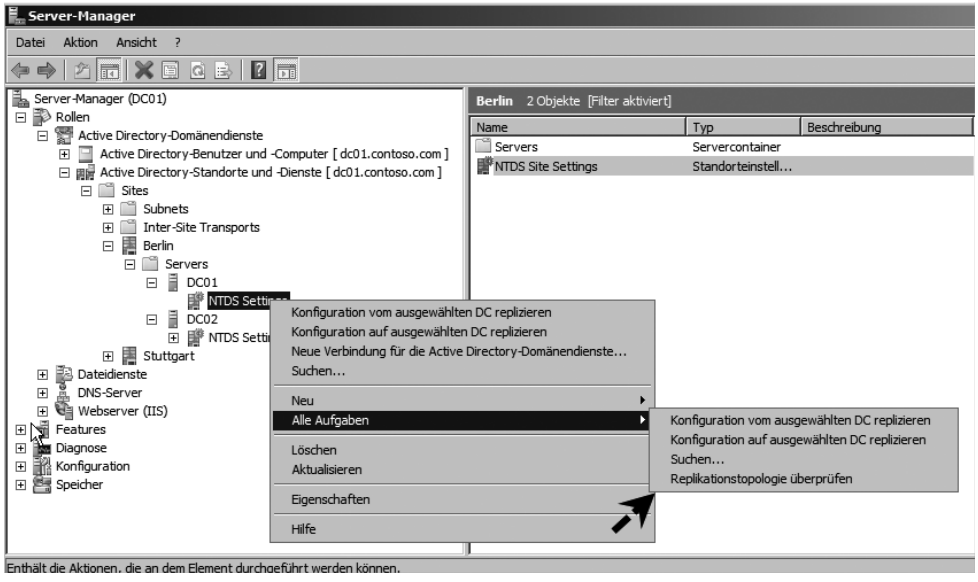
- Es ist kein globaler Katalogserver an jedem Standort in der Domäne erforderlich.
- Die Anmeldezeiten werden verringert, weil die authentifizierenden Domänencontroller nicht mehr auf einen globalen Katalog zugreifen müssen, um universelle Gruppenmitgliedschaftsinformationen abzurufen.
- Die Auslastung der Netzwerkbandbreite wird minimiert, weil ein Domänencontroller nicht alle Objekte replizieren muss, die sich in der Gesamtstruktur befinden.

Standardmäßig überprüft der KCC automatisch alle 15 Minuten die Funktionalität der Routingtopologie. Wenn Sie Änderungen an der Routingtopologie durchgeführt haben, besteht die Möglichkeit, die Routingtopologie sofort erstellen zu lassen. Am besten kann die Routingtopologie vom derzeitigen ISTG-Rolleninhaber aus überprüft werden. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Snap-In *Active Directory-Standorte und -Dienste*.
2. Navigieren Sie zu dem Standort, von dem aus Sie die Überprüfung starten wollen.
3. Klicken Sie auf das Pluszeichen des derzeitigen ISTG-Rolleninhabers des Standortes.
4. Klicken Sie mit der rechten Maustaste auf den Eintrag *NTDS Settings* und wählen Sie im Kontextmenü den Befehl *Alle Aufgaben/Replikationstopologie überprüfen* aus (Abbildung 8.92).

Die Überprüfung dauert einige Zeit, abhängig von der Anzahl der Standorte und Domänencontroller. Alle Verbindungen werden überprüft und gegebenenfalls neu erstellt. Sie erhalten eine entsprechende Meldung.

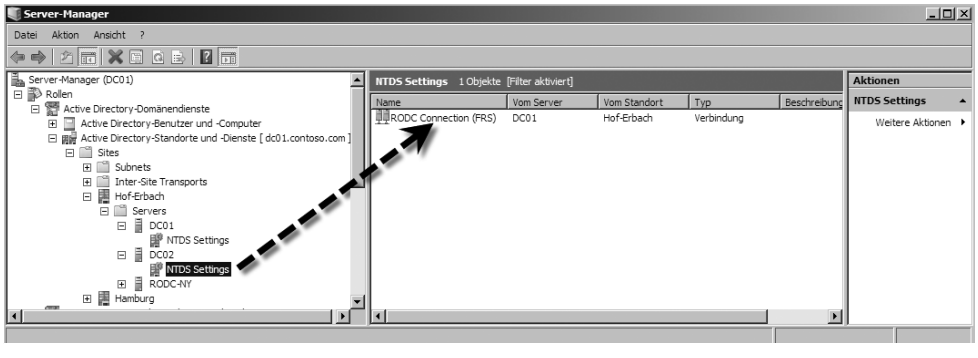
Abbildg. 8.92 Manuelles Starten der Routingtopologieüberprüfung



Starten der manuellen Replikation

Sie können die Replikation zwischen zwei Domänencontrollern jederzeit manuell starten. Die Verbindungen, die der KCC erstellt hat, werden automatisch angezeigt (Abbildung 8.93). Wenn Sie eine solche Verbindung mit der rechten Maustaste anklicken, können Sie die Replikation zu diesem Server mit der Option *Jetzt replizieren* sofort ausführen. Starten Sie die Replikation zu einem Domänencontroller, der in einem anderen Standort sitzt, wird die Replikation allerdings nicht sofort durchgeführt, sondern erst zum nächsten Zeitpunkt, den der Zeitplan zulässt. Bevor die Daten repliziert werden, stellt der Domänencontroller zunächst sicher, ob er eine Verbindung zu dem Domänencontroller herstellen kann, zu dem die Daten repliziert werden. Wenn mit dem Replikationspartner erfolgreich kommuniziert werden kann, erhalten Sie eine entsprechende Erfolgsmeldung. Kann der Replikationspartner nicht erreicht werden, erhalten Sie eine Fehlermeldung angezeigt.

Abbildg. 8.93 Anzeigen der Replikationsverbindung zwischen Domänencontrollern



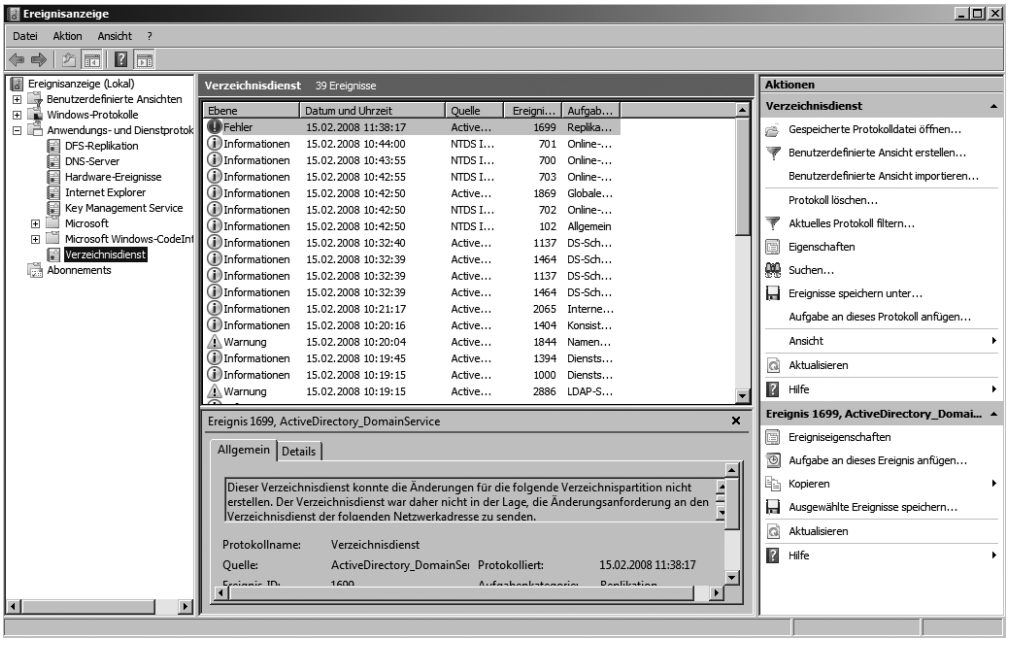
Fehler bei der Active Directory-Replikation beheben

Häufige Fehlerursache ist in einem Active Directory mit vielen Niederlassungen und zahlreichen Domänencontrollern die Replikation zwischen diesen Standorten. Beim Einsatz eines einzelnen Standortes werden nur selten Probleme auftreten. Bei der Fehlersuche bezüglich der Replikation sollten Sie zunächst die beteiligten Domänencontroller überprüfen und testen, ob diese innerhalb ihres Standortes funktionieren. Der nächste Schritt sollte der Blick in die Ereignisanzeige und das Protokoll Verzeichnisdienst sein. Achten Sie vor allem auf Fehler von *NTDS KCC*, *NTDS Replication* oder *NTDS General*. Bereits mit Hilfe dieser Fehlermeldungen können Sie auf den genannten Internetseiten eine Lösung für das Problem finden:

- www.eventid.net
- www.experts-exchange.com
- http://support.microsoft.com

Bei Problemen mit der Active Directory-Replikation sollte immer eine vollständige Diagnose der Domänencontroller vorausgehen, die auf den vorigen Seiten bereits beschrieben wurde. Fertigen Sie eine einfach Skizze der Replikationsverbindungen der Domänencontroller an und halten Sie genau fest, welche Domänencontroller sich nicht mehr mit welchen anderen Domänencontrollern replizieren können. Wenn Sie mit Hilfe dieser Skizze die Probleme verdeutlichen, werden Sie schnell erkennen, welcher Domänencontroller die Hauptursache für das Problem ist.

Abbildg. 8.94 Die Ereignisanzeige in Windows Server 2008 enthält mehr und ausführlichere Informationen, wenn Fehler auftreten



Replikationsprobleme mit *repadmin* finden

Treten Replikationsprobleme auf, sollten Sie mit Hilfe des Befehlszeilentools *repadmin.exe* die einzelnen Replikationsvorgänge analysieren. Geben Sie in der Befehlszeile den Befehl *repadmin /showreps* ein, um sich alle Replikationsvorgänge des Domänencontrollers anzeigen zu lassen. Im Anschluss finden Sie eine mögliche Ausgabe von *repadmin* und Hinweise auf eventuelle Probleme.

Listing 8.5 Replikationsprobleme mit *repadmin.exe* beheben

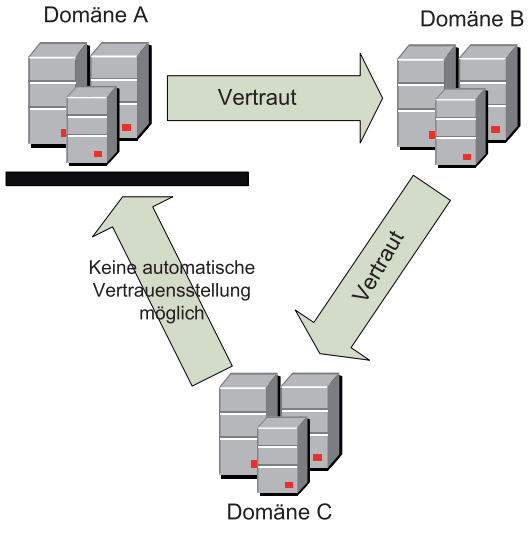
```
Berlin\DC01
DC Options: IS_GC  Site Options: (none)
DC object GUID: b533518a-5f8c-426e-b819-c5348dacca66
DC invocationID: b533518a-5f8c-426e-b819-c5348dacca66
INBOUND NEIGHBORS ====================================
DC=contoso,DC=com     Berlin\DC04 via RPC         DC object GUID: b138e402-751f-4266-9413-
1c0546b873e2        Last attempt @ 2007-08-14 10:46:47 was successful. <- Hier sehen Sie,
dass die interne Replikation im gleichen Standort zum Domänencontroller DC04 ohne Probleme
funktioniert hat. Stellen Sie sicher, dass die Replikation nur einige Minuten zurückliegt,
damit Sie interne Replikationsprobleme der Domänencontroller ausschließen können.
-CN=Configuration,DC=contoso,DC=com     Berlin\DC02 via RPC         DC object GUID:
c9fcc8e7-0bda-44a7-963e-cbb36437c083         Last attempt @ 2007-04-14 10:45:58 failed,
result 8524 (0x214c):              Ein DSA-Vorgang kann aufgrund eines DNS-Aufruffehlers
nicht fortgesetzt werden.         15 consecutive failure(s).         Last success @ 2007-04-
11 17:13:38. <- Hier sehen Sie, dass der Domänencontroller DC02 nicht replizieren kann. Die
Fehlermeldung können Sie zum Beispiel in Google oder der Microsoft Knowledge Base verwenden.
Da sich der lokale Domänencontroller mit dem DC04 replizieren kann, liegt vermutlich ein
Problem auf dem DC02 vor. Untersuchen Sie auf dem DC02, ob dieser auch mit dem DC04
replizieren kann. Wenn nicht, liegt sicherlich ein Problem mit dem DC02 vor. Ist es das auch
nicht, liegt ein Leitungsproblem zwischen DC02 und DC01 vor.
Berlin\DC03 via RPC         DC object GUID: df705a6c-1078-4803-8786-7e607a618557         Last
attempt @ 2007-04-14 10:46:19 failed, result 1722 (0x6ba):              Der RPC-Server ist
nicht verfügbar.          7 consecutive failure(s). Last success @ 2007-04-13 15:54:38
Beheben
```

Mit Hilfe dieser Diagnose können Sie auf den verschiedenen beteiligten Domänencontrollern genau erkennen, wann welche Replikation stattfinden oder nicht stattfinden kann. Geben Sie die angezeigten Fehlermeldungen in einer Internetsuchmaschine ein, da durch diese speziellen Tests die möglichen Suchergebnisse bereits deutlich eingegrenzt werden.

Vertrauensstellungen in Active Directorys

In Active Directory spielen Vertrauensstellungen eine noch wichtigere Rolle als unter Windows NT 4.0. In einer Gesamtstruktur werden bei der Erstellung von Domänen automatisch Vertrauensstellungen eingerichtet. Diese Vertrauensstellungen sind im Gegensatz zu Windows NT 4.0 transitiv. Bei Windows NT 4.0 konnten zwar auch Vertrauensstellungen eingerichtet werden (Abbildung 8.95), allerdings waren diese nicht transitiv. Wenn unter Windows NT 4.0 eine Vertrauensstellung zwischen den Domänen A und B sowie zwischen B und C eingerichtet wurde, dann hat nicht automatisch auch Domäne A der Domäne C oder umgekehrt die Domäne C der Domäne A vertraut. Diese Verbindung musste ebenfalls manuell erstellt werden.

Abbildg. 8.95 Nicht transitive Vertrauensstellungen unter Windows NT 4.0



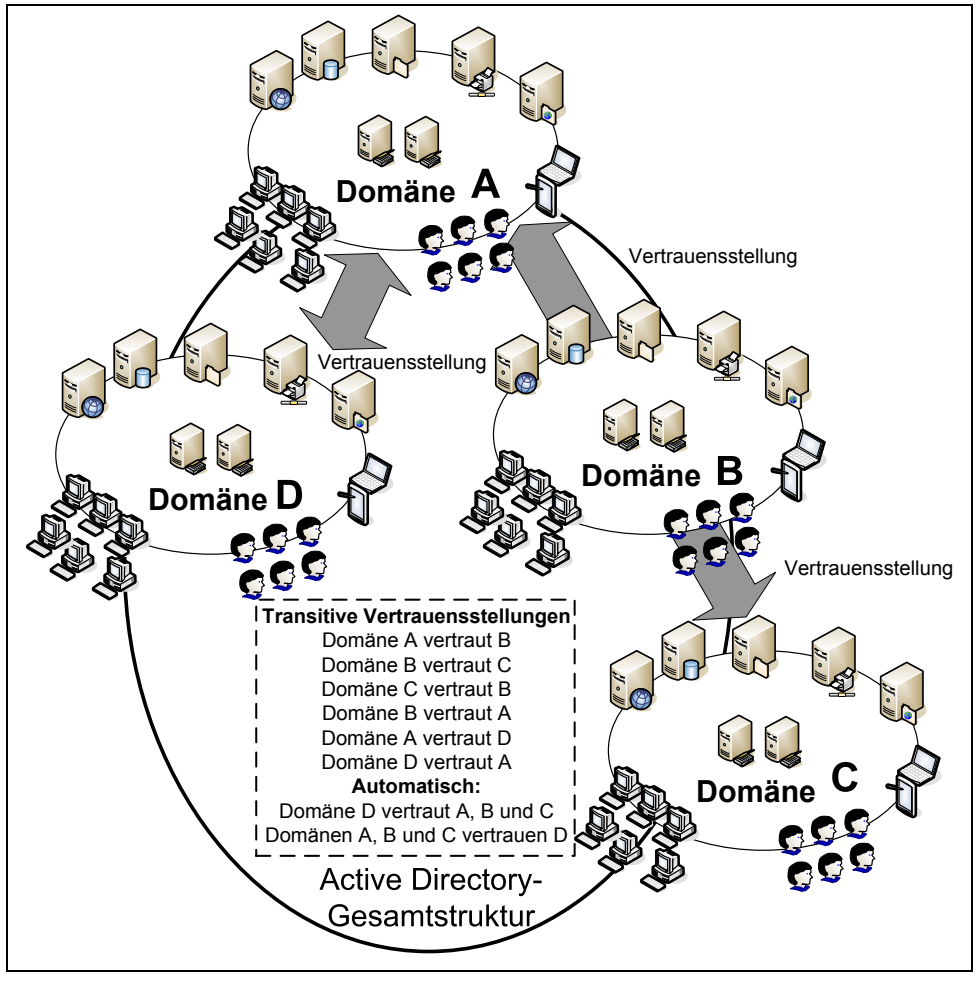
Wichtige Grundlagen der Vertrauensstellungen im Active Directory

Durch Domänen, untergeordnete Domänen und Strukturen gibt es die Möglichkeit, fast unbegrenzt Domänen anbinden zu können, die sich automatisch untereinander vertrauen. In einem Active Directory vertraut jede Domäne jeder anderen Domäne, die Bestandteil der gleichen Gesamtstruktur ist. Es ist nicht mehr notwendig, zahlreiche manuelle Vertrauensstellungen einzurichten (Abbildung 8.96).

Auch wenn die Vertrauensstellungen in einer Gesamtstruktur auf den ersten Blick komplex erscheinen, sind sie einfacher als unter Windows NT 4.0, weil diese Vertrauensstellungen automatisch eingerichtet werden. Administratoren müssen keinerlei Maßnahmen vornehmen, damit sich Domänen in einer Gesamtstruktur untereinander vertrauen. Durch diese automatische Verbindung wird die Effizienz von verschiedenen Domänen und Strukturen innerhalb einer Gesamtstruktur deutlich erhöht. In einer Gesamtstruktur werden jedoch nicht automatisch Vertrauensstellungen zwischen allen Domänen eingerichtet, sondern es wird ein gewisses Schema beibehalten:

- Vertrauensstellungen zwischen übergeordneten und untergeordneten Domänen werden immer automatisch eingerichtet. Dieser Typ wird *Untergeordnete Vertrauensstellung* genannt.
- Zusätzlich werden noch Vertrauensstellungen zwischen den Rootdomänen der einzelnen Strukturen eingerichtet. Es gibt jedoch keine Vertrauensstellungen zwischen den Domänen verschiedener Strukturen. Diese vertrauen sich auf Basis der transitiven Vertrauensstellungen. Der Zugriff auf die Ressourcen wird zwischen Domänen durch transitive Vertrauensstellungen ermöglicht, nicht durch die direkte Verbindung zwischen den Domänen. Die Vertrauensstellungen zwischen den Rootdomänen der verschiedenen Strukturen werden *Strukturstamm-Vertrauensstellungen* genannt.

Abbildg. 8.96 Transitive Vertrauensstellungen unter Windows Server 2008 in Active Directory

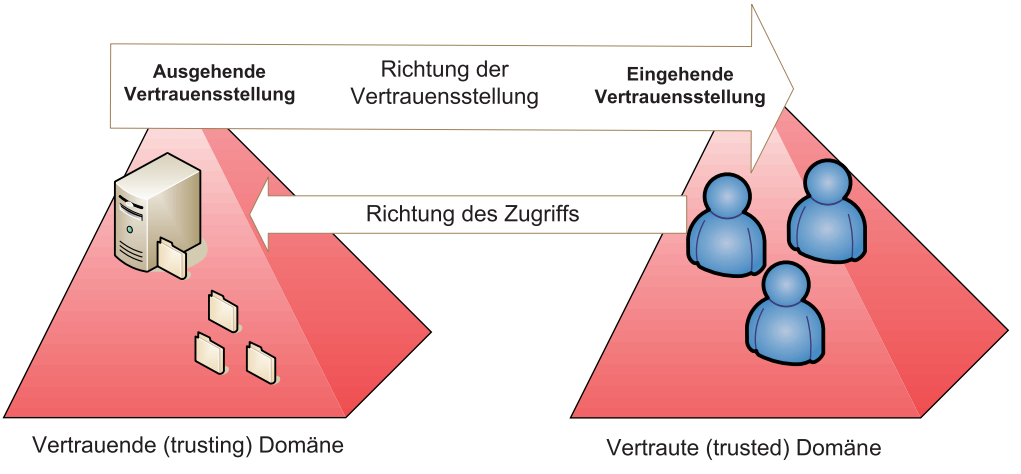


Die Verwaltung der Vertrauensstellungen findet mit Hilfe des Snap-Ins *Active Directory-Domänen und -Vertrauensstellungen* statt. Wenn Sie in diesem Snap-In die Eigenschaften einer Domäne aufrufen, finden Sie auf der Registerkarte *Vertrauensstellungen* alle Vertrauensstellungen dieser Domäne und die dazugehörigen Informationen (Abbildung 8.97).

Abbildg. 8.97 Anzeigen und verwalten der Vertrauensstellung einer Domäne

Außer den automatisch eingerichteten Vertrauensstellungen können Sie natürlich noch zusätzliche manuelle Vertrauensstellungen einrichten. Für viele Administratoren ist die Richtung der Vertrauensstellungen noch immer gewöhnungsbedürftig, da die einzelnen Begriffe teilweise etwas verwirrend sind. Generell gibt es im Active Directory zunächst zwei verschiedene Arten von Vertrauensstellungen, *unidirektionale* und *bidirektionale*. Bei *unidirektionalen* Vertrauensstellungen vertraut eine Domäne der anderen, aber nicht umgekehrt. Das heißt, die Benutzer der Domäne 1 können zwar auf Ressourcen der Domäne 2 zugreifen, aber die Benutzer in der Domäne 2 nicht auf Ressourcen in der Domäne 1. Dieser Vorgang ist natürlich auch umgekehrt denkbar (Abbildung 8.98).

Abbildg. 8.98 Vertrauensstellungen in Active Directory verstehen



Weitere Unterscheidungen der Vertrauensstellungen im Active Directory sind *ausgehende* und *eingehende* Vertrauensstellungen. Bei ausgehenden Vertrauensstellungen vertraut die Domäne 1 der Domäne 2. Das heißt, Anwender der Domäne 2 dürfen auf Ressourcen der Domäne 1 zugreifen. Bei diesem Vorgang ist die Domäne, von der die Vertrauensstellung ausgeht, die *vertrauende (trusting)* Domäne. Bei der Domäne mit der eingehenden Vertrauensstellung handelt es sich um die *vertraute (trusted)* Domäne, in der die Benutzerkonten angelegt sind, die Berechtigungen in der vertrauenden Domäne haben.

HINWEIS Bevor eine Vertrauensstellung erstellt wird, prüft der Server die Eindeutigkeit in folgender Reihenfolge:

- Den NetBIOS-Namen der Domäne
- Den Fully Qualified Domain Name (FQDN) der Domäne
- Die Security Identifier (SID) der Domäne

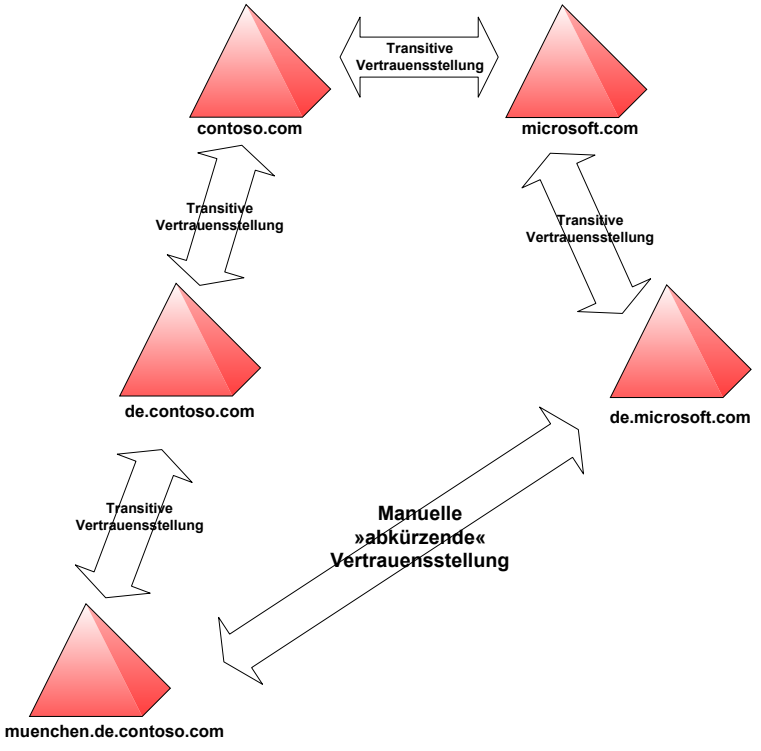
Diese drei Punkte müssen eindeutig sein, da ansonsten keine Vertrauensstellung erstellt werden kann. Wenn die Domänen-SID gleich lautet, muss eine von beiden Domänen erneut installiert werden. Dieser Fall kann eintreten, wenn eine Domäne von einer anderen geklont wurde oder nach dem Installieren des Betriebssystems auf einem Server dieser geklont wurde und anschließend SYSPREP nicht ordnungsgemäß ausgeführt worden ist. Meistens erhalten Sie in diesem Fall eine Fehlermeldung in der Art *Dieser Vorgang kann nicht auf der aktuellen Domäne ausgeführt werden.*

Varianten der Vertrauensstellungen im Active Directory

Neben den beschriebenen Vertrauensstellungen im Active Directory gibt es verschiedene Möglichkeiten, nachträglich manuelle Vertrauensstellungen einzurichten:

- Externe Vertrauensstellungen, zum Beispiel zu Windows NT 4.0-Domänen oder einzelnen Domänen einer anderen Gesamtstruktur
- *Gesamtstruktur-übergreifende Vertrauensstellungen* (neu seit Windows Server 2003), um die Rootdomänen von zwei unterschiedlichen Gesamtstrukturen zu verbinden. Alle Domänen der beiden Vertrauensstellungen vertrauen sich anschließend automatisch transitiv.
- Vertrauensstellungen zu einem Nicht-Windows-Kerberossystem
- Vertrauensstellungen zwischen untergeordneten Domänen verschiedener Strukturen, so genannte S*hortcut Trusts* oder *abkürzende Vertrauensstellungen*, sind ebenfalls möglich. Diese Art der Vertrauensstellung wird häufig verwendet, um den Zugriff auf Ressourcen zwischen Domänen zu beschleunigen. In einem Active Directory vertrauen sich alle Domänen innerhalb einer Struktur untereinander. Diese transitiven Vertrauensstellungen werden automatisch eingerichtet. Es werden allerdings keine Vertrauensstellungen zwischen untergeordneten Domänen verschiedener Strukturen eingerichtet, sondern nur zwischen den Rootdomänen der einzelnen Strukturen. Wenn Anwender auf Daten verschiedener untergeordneter Domänen zugreifen wollen, muss die Authentifizierung daher immer den Weg bis zur Root-Domäne der eigenen Struktur gehen, dann zur Root-Domäne der anderen Struktur und schließlich zur entsprechenden untergeordneten Domäne. Diese Authentifizierung kann durchaus einige Zeit dauern.

Abbildg. 8.99 Pfad der Vertrauensstellungen mit mehreren Domänenstrukturen in einer Gesamtstruktur



TIPP Weitere Informationen zu Vertrauensstellungen finden Sie auf folgenden Internetseiten. Die Ausführungen für Windows Server 2003 haben auch unter Windows Server 2008 Relevanz:

- **Wie sollte WINS konfiguriert werden?** *http://www.faq-o-matic.net/2004/10/23/wie-sollte-wins-konfiguriert-werden/*
- **Access control in Active Directory** *http://technet2.microsoft.com/WindowsServer/en/library/2f98f5b2-5e7e-4ff3-83a9-c32cf23329211033.mspx?mfr=true*
- **Support WebCast: Microsoft Windows Server 2003: Implementing an Active Directory Domain Rename Operation** *http://support.microsoft.com/kb/819145/en-us*
- **Error message when you create the trusted side of a trust between Windows Server 2003-based domains: "The parameter is incorrect"** *http://support.microsoft.com/kb/930218/en-us*
- **MS02-001: Forged SID could result in elevated privileges in Windows 2000** *http://support.microsoft.com/kb/289243/en-us*
- **Sind Vertrauensstellungen ohne NetBIOS-Namensauflösung möglich?** *http://www.faq-o-matic.net/2006/07/01/sind-vertrauensstellungen-ohne-netbios-namensaufloesung-moeglich/*
- **Windows Server 2003 Trust Enhancements** *http://www.microsoft.com/technet/community/columns/profwin/pw0303.mspx*

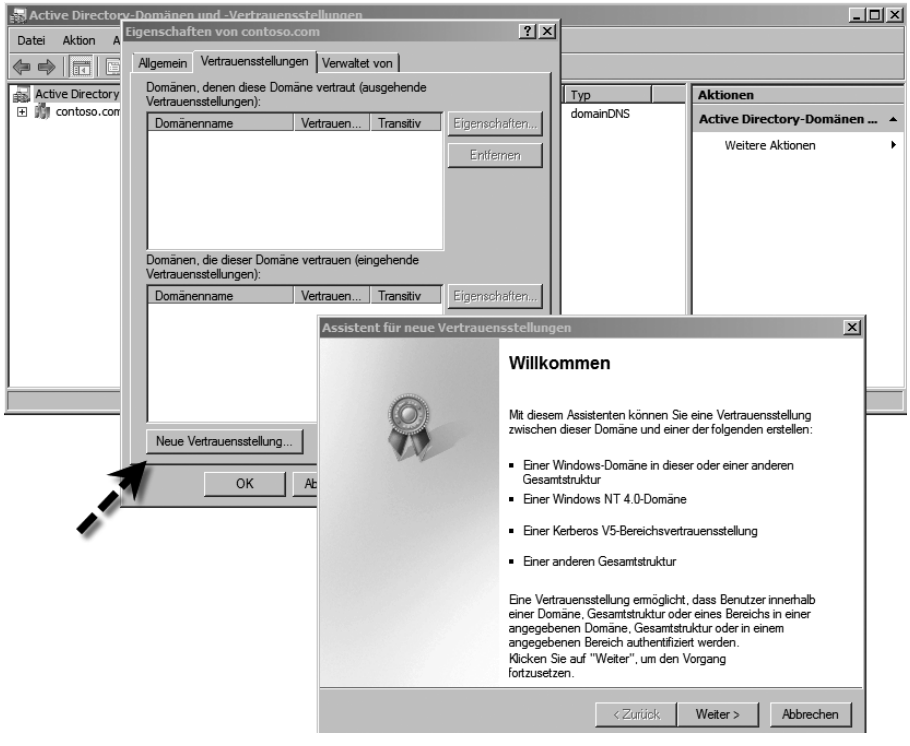
Einrichtung einer Vertrauensstellung

Wenn Sie eine Vertrauensstellung zu einer externen Domäne erstellen wollen, sollten Sie zunächst sicherstellen, dass die Namensauflösung zwischen den Domänen fehlerfrei funktioniert. Erst wenn die Namensauflösung stabil und zuverlässig funktioniert, sollten Sie die Vertrauensstellung einrichten. Hilfreich ist auch hier wieder eine WINS-Server-Infrastruktur. Richten Sie eine Vertrauensstellung zu einer Windows NT 4.0-Domäne ein, sollten Sie auf jeden Fall einen WINS-Server einsetzen. Ohne WINS ist die Verbindung zwischen einer Windows NT 4.0-Domäne und einer Active Directory-Domäne zwar grundsätzlich möglich, aber auf Dauer sehr unstabil.

TIPP Um eine externe bidirektionale Vertrauensstellung in der Befehlszeile einzurichten, können Sie auch den Befehl *Netdom Trust <vertrauende Domäne> /d:<vertraute Domäne> /Add /Twoway* verwenden.

1. Um eine Vertrauensstellung einzurichten, rufen Sie im Snap-In *Active Directory-Domänen und -Vertrauensstellungen* die Eigenschaften der Domäne auf, von der die Vertrauensstellung ausgehen soll.
2. Wechseln Sie in den Eigenschaften zur Registerkarte *Vertrauensstellungen*.
3. Klicken Sie auf die Schaltfläche *Neue Vertrauensstellung*. Es erscheint der Assistent zur Einrichtung neuer Vertrauensstellungen (Abbildung 8.100). Bestätigen Sie das Fenster und geben Sie auf der zweiten Seite den Namen der Domäne an, zu der Sie eine Vertrauensstellung einrichten wollen (Abbildung 8.101).

Abbildg. 8.100 Starten des Assistenten zum Erstellen einer neuen Gesamtstruktur

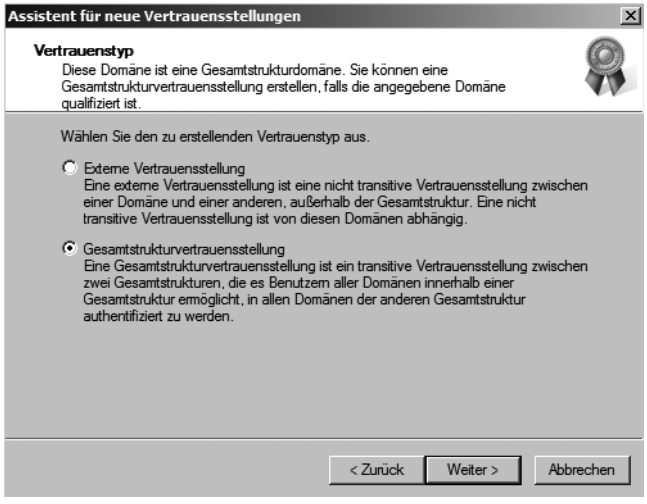


Wenn Sie eine Vertrauensstellung zu einer Active Directory-Domäne aufbauen wollen, verwenden Sie am besten den DNS-Namen, beim Verbindungsaufbau zu einer Windows NT 4.0-Domäne den NetBIOS-Namen.

Abbildg. 8.101 Festlegen des Namens der Domäne, zu der Sie eine Vertrauensstellung aufbauen wollen

4. Klicken Sie auf *Weiter*, überprüft der Assistent, ob er eine Verbindung zur Domäne aufbauen kann. Wollen Sie eine Vertrauensstellung mit einer anderen Gesamtstruktur aufbauen, können Sie auf dem nächsten Fenster diese Option auswählen. Bei einer externen Vertrauensstellung kann eine uni- oder bidirektionale Vertrauensstellung zu einer einzelnen Domäne (in einer separaten Gesamtstruktur) eingerichtet werden. Diese Art einer Vertrauensstellung ist nie transitiv. Eine externe Vertrauensstellung kann notwendig sein, wenn Benutzer Zugriff auf Ressourcen einer anderen Domäne in einer anderen Gesamtstruktur brauchen und keine Gesamtstrukturvertrauensstellung besteht. Dadurch wird eine explizite Vertrauensstellung nur zu dieser einen Domäne erstellt. Wenn diese Domäne weiteren Domänen vertraut, bleibt der Zugriff auf die weiteren Domänen verwehrt. Gesamtstrukturvertrauensstellungen haben den Vorteil, dass diese vollständige Kerberos-Integration zwischen Gesamtstrukturen bieten, und zwar bidirektional und transitiv.

Abbildg. 8.102 Erstellen einer neuen Gesamtstrukturvertrauensstellung



Voraussetzungen für Gesamtstruktur-übergreifende Vertrauensstellungen

Für die Gesamtstruktur-übergreifende Vertrauensstellungen müssen einige Voraussetzungen geschaffen werden:

- Gesamtstruktur-übergreifende Vertrauensstellungen werden nur in Windows Server 2003/2008-Gesamtstrukturen unterstützt.
- Stellen Sie sicher, dass sich die Domänenfunktionsebene und die Gesamtstrukturfunktionsebene im Windows Server 2003-Modus, besser im Windows Server 2008-Modus befindet.
- Stellen Sie sicher, dass die Namensauflösung zwischen den Gesamtstrukturen funktioniert. Stellen Sie domänenspezifische Weiterleitungen her und überprüfen Sie, ob sich die Domänencontroller der beiden Gesamtstrukturen untereinander per DNS auflösen können. Alternativ können Sie einen DNS-Server erstellen, der für die Zonen beider Gesamtstrukturen zuständig ist.
- Bei Gesamtstruktur-übergreifenden Vertrauensstellungen müssen Sie nur die beiden Rootdomänen der Gesamtstrukturen durch eine Vertrauensstellung verbinden. Dann vertrauen sich die Domänen der beiden Gesamtstrukturen transitiv, sodass Sie durch eine Vertrauensstellung mehrere Domänen miteinander verbinden können.

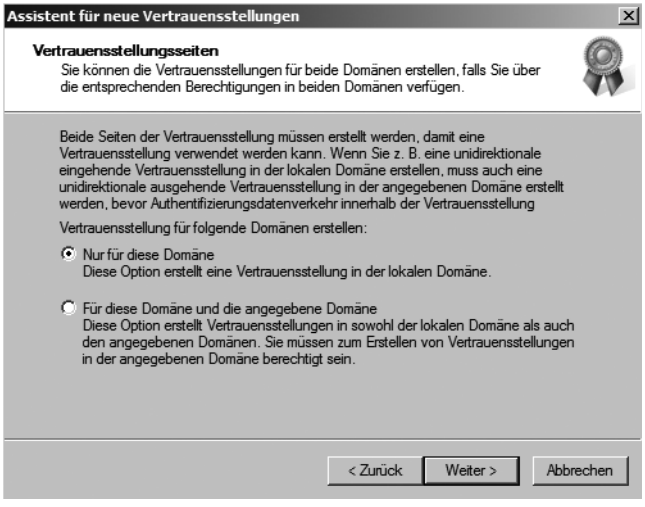
Nach der Auswahl der Art der Vertrauensstellung können Sie festlegen, ob Sie eine unidirektionale oder bidirektionale Vertrauensstellung aufbauen wollen (Abbildung 8.103).

- **Bidirektional** In diesem Fall können sich die Anwender beider Domänen in der jeweils anderen Domäne authentifizieren.
- **Unidirektional:eingehend** Bei dieser Variante legen Sie fest, dass es sich bei dieser Domäne um die vertraute Domäne der Vertrauensstellung handelt. In diesem Fall können sich die Benutzer dieser Domäne bei der anderen Domäne authentifizieren.
- **Unidirektional:ausgehend** Bei dieser Vertrauensstellung konfigurieren Sie, dass sich ausschließlich die Anwender der anderen Domäne bei dieser Domäne anmelden dürfen. Die Benutzer dieser Domäne können sich hingegen nicht bei der anderen Domäne anmelden.

Abbildg. 8.103 Festlegen der Richtung von Vertrauensstellungen

Im nächsten Fenster können Sie bei Gesamtstrukturvertrauensstellungen auswählen, ob Sie auch gleich die Vertrauensstellung in der anderen Domäne der anderen Gesamtstruktur erstellen wollen. Diese Option ist selten sinnvoll. Erstellen Sie am besten erst die Vertrauensstellung in der Stammdomäne der einen, dann in der anderen Gesamtstruktur (Abbildung 8.104).

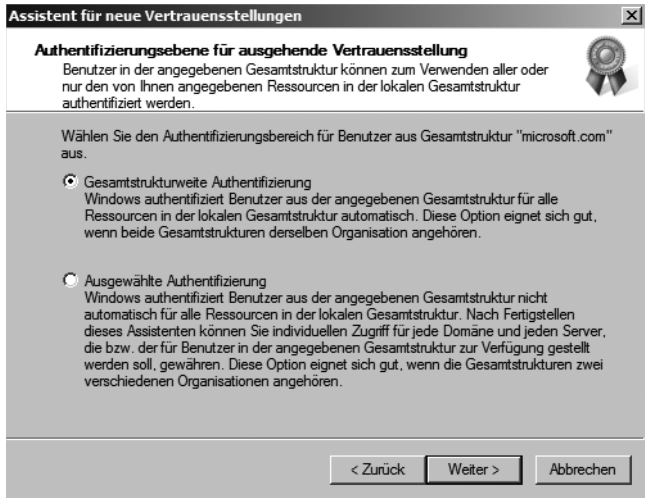
Abbildg. 8.104 Auswählen, ob die Gesamtstrukturvertrauensstellung in beiden Domänen eingerichtet werden soll



Im nächsten Fenster legen Sie den Bereich der Authentifizierung der Vertrauensstellung fest (Abbildung 8.105). Die meisten Administratoren verwenden hier die Option *Domänenweite Authentifizierung*, bzw. bei einer Gesamtstrukturvertrauensstellung die Option *Gesamtstrukturweite Authentifizierung*. Dabei können die Anwender der anderen Domäne durch Gruppenmitgliedschaften oder direkte Berechtigungen Zugriff auf die Ressourcen dieser Domäne nehmen. Wenn Sie die Variante

Ausgewählte Authentifizierung auswählen, müssen Sie für jeden Server auf den die Anwender der anderen Domäne zugreifen dürfen, in den Sicherheitseinstellungen die Option *Darf Authentifizieren* aktivieren. Durch diese Einstellung erhöhen Sie zwar die Sicherheit auf der anderen Seite, aber auch den Verwaltungsaufwand für die Berechtigungsstruktur. Wenn Sie diese Option aktivieren, wird der Zugriff auf die einzelnen Server im Unternehmen für die Benutzer der anderen Domäne verweigert. Erst muss diese Verweigerung für jeden Server mit Aktivierung der Option *Darf Authentifizieren* einzeln zurückgenommen werden.

Abbildg. 8.105 Auswählen der Authentifizierungsebene für eine neue Vertrauensstellung

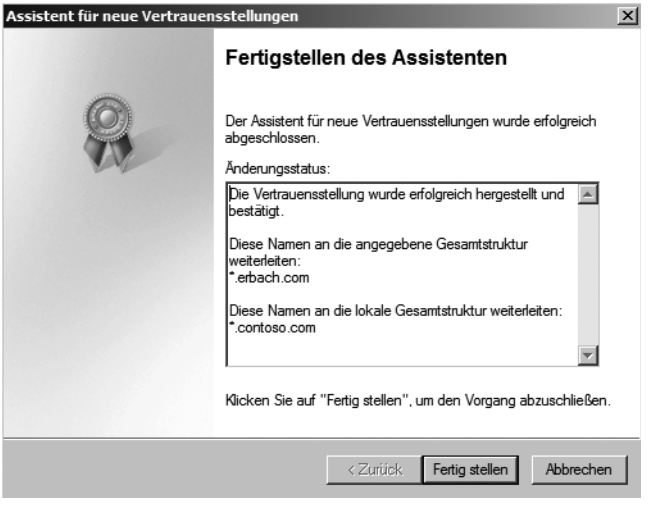


Im nächsten Fenster müssen Sie ein Kennwort für die Vertrauensstellung festlegen. Merken Sie sich dieses Kennwort, da Sie es unter Umständen später wieder für die Verifizierung verwenden müssen.

HINWEIS Verbinden Sie zwei Gesamtstrukturen durch eine Gesamtstruktur-übergreifende Vertrauensstellung, sollten Sie sicherstellen, dass möglichst alle Domänennamen eindeutig sind. Sobald in den Gesamtstrukturen doppelte DNS- oder NetBIOS-Namen auftreten, können diese Domänen nicht auf Ressourcen der jeweils anderen Gesamtstruktur zugreifen.

Wählen Sie im nächsten Fenster aus, ob Sie die Vertrauensstellung überprüfen wollen. Wenn Sie eine Vertrauensstellung zu einer Windows NT 4.0-Domäne einrichten, sollten Sie zunächst die Vertrauensstellung auf der Seite der Windows NT 4.0-Domäne einrichten, bevor Sie in den Eigenschaften der Vertrauensstellung in der Active Directory-Domäne die Überprüfung starten. Erst wenn eine Vertrauensstellung als aktiv verifiziert wurde, können Sie auch sicher sein, dass Anwender auf die Ressourcen zugreifen können. Wenn die Erstellung einer Vertrauensstellung nicht funktioniert, liegt es fast immer an Problemen mit der Namensauflösung oder entsprechenden Berechtigungen. Unter Umständen müssen Sie sich bei der Überprüfung der Vertrauensstellung noch mal in der anderen Domäne authentifizieren. Nach der erfolgreichen Überprüfung erhalten Sie eine Meldung, dass die Vertrauensstellung aktiv ist.

Abbildg. 8.106 Abschließen des Assistenten zur Einrichtung von Vertrauensstellungen



Wenn in Ihrer Gesamtstruktur mehrere Strukturen eingesetzt werden, können Sie in der Gesamtstruktur-übergreifenden Vertrauensstellung festlegen, welche Namensräume bzw. Strukturen diese Vertrauensstellung nutzen kann. Sie können einzelne Namensräume aus dem Routing entfernen oder später über die Eigenschaften der Vertrauensstellung hinzufügen. Für die Verwaltung dieser verschiedenen Strukturen können Sie in den Eigenschaften der Vertrauensstellung die Registerkarte *Namenssuffixrouting* verwenden.

Abbildg. 8.107 Konfigurieren des Namenssuffixroutings für eine Gesamtstrukturvertrauensstellung

Automatisch aktivierte SID-Filterung

Wenn Sie die Erstellung der Vertrauensstellung abgeschlossen haben, erhalten Sie einen Hinweis, dass der SID-Filter für diese externe Vertrauensstellung aktiviert wurde. Der SID-Filter wird automatisch aktiviert, wenn eine Vertrauensstellung zu einer externen Domäne von einem Windows Server 2003/2008-Domänencontroller oder einem Domänencontroller unter Windows 2000 Server mit SP4 eingerichtet wird. Mit der SID-Filterung werden ausgehende Vertrauensstellungen gesichert. Mit der SID-Filterung soll verhindert werden, dass Administratoren in der vertrauten (trusted) Domäne unberechtigt Berechtigungen innerhalb der vertrauenden (trusting) Domäne vergeben. Der SID-Filter stellt sicher, dass sich in der vertrauenden Domäne ausschließlich Benutzer aus der vertrauten Domäne authentifizieren dürfen, deren SID die Domänen-SID der vertrauten Domäne enthalten. Wenn die SID-Filterung deaktiviert wird, könnte ein außen stehender Benutzer, der Administrator-Rechte in der vertrauten Domäne besitzt, den Netzwerkverkehr der vertrauenden Domäne abhören und die SID eines Administrators auslesen. Im Anschluss kann er diese SID seiner eigenen SID-History anhängen.

Durch diesen Vorgang würde also ein Administrator der vertrauten Domäne zu Administrator-Rechten in der vertrauenden Domäne gelangen. Durch die Aktivierung der SID-Filterung ist es allerdings auch möglich, dass die SID-History der Anwender ignoriert wird, die diese unter Umständen aus anderen Domänen durch eine Migration erhalten haben. In diesem Fall könnten Probleme bei der Authentifizierung bei Ressourcen auftreten. Der SID-Filter kann daher nicht immer eingesetzt werden. Verwenden Sie den SID-Filter für die Absicherung von Windows NT 4.0-Vertrauensstellungen, sind selten Probleme zu erwarten. Schwierig wird es dagegen, wenn Sie eine externe Vertrauensstellung zu einer Domäne in einem Active Directory einrichten. Wenn Sie für Ressourcen in der vertrauenden Domäne Berechtigungen für eine universale Gruppe aus dem Active Directory der vertrauten Domäne vergeben, müssen Sie zuvor sicherstellen, dass diese universale Gruppe auch in der vertrauten Domäne erstellt wurde und nicht in einer anderen Domäne von Active Directory. Wurde die universale Gruppe nicht in der vertrauten Domäne erstellt, enthält sie auch nicht die SID dieser Domäne und darf durch die SID-Filterung nicht auf die Ressourcen in der vertrauenden Domäne zugreifen. Aus den genannten Gründen, vor allem bei Migrationen oder Vertrauensstellungen zu Domänen eines anderen Active Directory, kann es sinnvoll sein, die SID-Filterung zu deaktivieren.

Die Deaktivierung der SID-Filterung erfolgt über das Befehlszeilenprogramm *netdom.exe*. Um die SID-Filterung zu deaktivieren, geben Sie in der Befehlszeile den Befehl *netdom trust <VertrauendeDomäne> /domain:<VertrauteDomäne> /quarantine:no /userD:<Domänenadministrator> /passwordD:<PasswordDesDomänenAdministrators>* ein. Sie können die SID-Filterung wieder ganz einfach aktivieren, indem Sie die Option */quarantine* auf *:yes* setzen, also mit dem Befehl *netdom trust <VertrauendeDomäne> /domain:<VertrauteDomäne> /quarantine:yes /userD:<Domänenadministrator> /passwordD: <PasswordDesDomänenAdministrators>*.

Namensauflösung für Vertrauensstellungen zu Windows NT 4.0-Domänen

In manchen Fällen kann es beim Einrichten der Vertrauensstellungen zu Problemen kommen. Daran sind oft fehlerhafte Namensauflösungen, abgesicherte Router zwischen verschiedenen Subnets oder Fehler auf den WINS-Servern verantwortlich. Sie können zwar unter Umständen von einem Server den jeweils anderen Server auch mit Namen anpingen, wenn Sie die Vertrauensstel-

lung einrichten wollen, erscheint dennoch die Meldung, dass der Domänencontroller der Domäne nicht gefunden werden kann. Können Sie keine Vertrauensstellung zwischen zwei Domänencontrollern der verschiedenen Domänen einrichten, sollten Sie auf beiden Servern eine LMHOSTS-Datei anlegen und bearbeiten. Diese Datei finden Sie im Verzeichnis *System32\drivers\etc*. Achten Sie darauf, dass Sie sich die Dateiendungen anzeigen lassen, da in diesem Verzeichnis auch eine Datei *lmhosts.sam* liegt, wobei die Endung **.sam* eventuell unterdrückt wird. Damit die Namensauflösung funktioniert, muss die Datei *lmhosts* ohne irgendeine Endung benannt werden. In dieser Datei sollten Sie die Auflösung der Domänen konfigurieren, damit der WINS-Server für diese Auflösung übergangen wird. Schreiben Sie folgende Zeilen in die Datei *lmhosts*, ändern Sie dabei die Werte auf Ihre Konfiguration ab:

10.0.0.1 PDCNAME #pre #dom:Domäne

10.0.0.1 Domäne \0x1b #pre

Achten Sie auf Groß- und Kleinschreibung. Die IP-Adresse muss mit der Adresse Ihres PDCs übereinstimmen. Zwischen den Anführungszeichen in der zweiten Zeile müssen zwingend 20 Zeichen stehen, sonst funktioniert die Auflösung nicht. Gleich nach dem ersten Anführungszeichen muss der NetBIOS-Name der Windows-Domäne stehen, zu der die Vertrauensstellung aufgebaut werden soll. Der NetBIOS-Name darf per Definition nur 15 Zeichen lang sein. Wenn der Name der Domäne, die aufgelöst werden soll, kürzer ist, müssen Sie den Namen mit Leerzeichen bis auf 15 Zeichen auffüllen. Nach dem 15. Zeichen muss die Zeichenfolge *0x1b* und dann gleich das abschließende Anführungszeichen folgen. Der Backslash muss zwingend auf Position 16 stehen. Nachdem Sie diese Änderungen vorgenommen haben, müssen Sie den Server entweder neu starten oder den NetBIOS-Cache durch den Befehl *nbtstat –r* neu laden. Das Laden des Cache sollte Ihnen auch mit einer entsprechenden Meldung angezeigt werden. Mit dem Befehl *nbtstat –c* können Sie sich den Cache anzeigen lassen. Bei der Anzeige des Cache muss die Domäne als *Typ 1B* vermerkt sein, dann ist alles korrekt. Wird die Domäne nicht angezeigt, sollten Sie den Server neu starten oder Ihre Eingaben überprüfen. Wenn Sie die Vertrauensstellung neu einrichten, sollte kein Fehler mehr erscheinen. Sie können die Datei *lmhosts* auch für alle Windows NT 4.0-Rechner verwenden, die Probleme haben, einen Active Directory-Domänencontroller zu finden. Diese Konfiguration ist allerdings recht komplex, der Einsatz eines oder mehrerer WINS-Server ist im Vergleich deutlich effizienter.

Bereinigung von Active Directory und Entfernen von Domänencontrollern

In manchen Fällen ist der Aufwand einer Fehlerbehebung viel größer, als einfach den betroffenen Domänencontroller neu zu installieren und wieder in das Active Directory zu integrieren. Wenn Sie einen Domänencontroller aus dem Active Directory entfernen müssen, gibt es grundsätzlich drei Möglichkeiten:

1. Der Domänencontroller soll zu einem Mitgliedsserver heruntergestuft werden, wenn zum Beispiel auf einem Server Exchange und Domänencontroller zusammen Probleme bereiten, aber der Server noch Verbindung zum Active Directory hat.
2. Der Domänencontroller läuft zwar noch und verwaltet installierte Applikationen, hat aber seine Verbindung zum Active Directory verloren. Er soll heruntergestuft werden, ohne Verbindung mit dem Active Directory zu haben oder neu installiert zu werden. Das Active Directory muss dazu nachträglich bereinigt werden.

3. Der Domänencontroller ist vollkommen ausgefallen und funktioniert nicht mehr. Dem Active Directory muss mitgeteilt werden, dass der Domänencontroller nicht mehr verfügbar ist.

Auf den folgenden Seiten sind die Abläufe der einzelnen Möglichkeiten beschrieben, um einen Domänencontroller aus dem Active Directory zu entfernen.

Vorbereitungen beim Entfernen eines Domänencontrollers

Wird ein Domänencontroller aus dem Active Directory entfernt, sollten Sie einige Vorbereitungen treffen, damit die Anwender durch seinen Ausfall nicht betroffen sind:

- Sie sollten sicherstellen, dass der Domänencontroller nicht als bevorzugter oder alternativer DNS-Server von einem anderen Rechner der Domäne verwendet wird (auch nicht als DNS-Weiterleitungsserver).
- Wenn möglich, sollten Sie vor der Herabstufung das DNS von diesem Domänencontroller entfernen. Haben Sie das DNS entfernt, überprüfen Sie auf einem anderen DNS-Server in den Eigenschaften der DNS-Zone, dass der Server auf der Registerkarte *Namensserver* nicht mehr aufgeführt wird (Abbildung 8.108). Entfernen Sie aber nicht den Hosteintrag des Servers, da dieser für die Herabstufung noch benötigt wird.

Abbildg. 8.108 Überprüfen der Active Directory-DNS-Zone nach verwaisten Namensservern

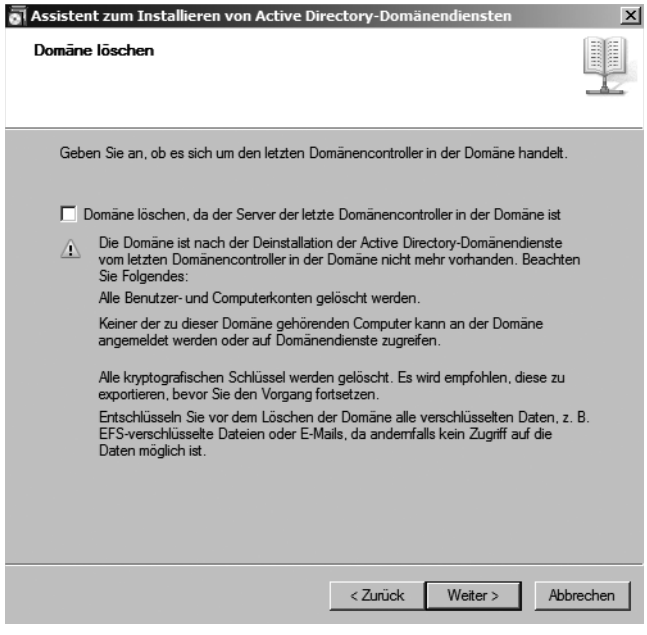
- Stellen Sie sicher, dass der Domänencontroller nicht an irgendeiner Stelle als Domänencontroller explizit eingetragen ist, zum Beispiel auf einem Linux-Server oder einem Exchange-Server.

- Entfernen Sie alle Active Directory-abhängigen Dienste, wie VPN, Zertifikatstelle oder andere Programme, die nach der Herabstufung nicht mehr funktionieren werden.
- Verschieben Sie vor der Herabstufung zuerst alle FSMO-Rollen auf andere Server.
- Wenn es sich bei diesem Server um einen globalen Katalog handelt, konfigurieren Sie einen anderen Server als globalen Katalog und entfernen Sie im Snap-In *Active Directory-Standorte und -Dienste* unter *Sites/<Standort des Servers>/<Servername>/Eigenschaften der NTDS-Settings* den Haken bei *Globaler Katalog*.

Herabstufen eines Domänencontrollers

Starten Sie als nächsten Schritt auf dem Server den Assistenten zum Entfernen von Active Directory über *Start/Ausführen/dcpromo*, um den Server zu einem Mitgliedsserver der Domäne herabzustufen. Wenn es sich bei dem Domänencontroller, den Sie herabstufen wollen, um einen globalen Katalog handelt, werden Sie darüber mit einer Meldung informiert. Handelt es sich um einen globalen Katalog, können Sie auf der nächsten Seite auswählen, ob es sich bei diesem Domänencontroller um den letzten seiner Domäne handelt. In diesem Fall würde nicht nur der Domänencontroller aus der Gesamtstruktur entfernt, sondern die ganze Domäne. Haben Sie Ihre Auswahl getroffen, beginnt der Assistent mit der Herabstufung des Domänencontrollers. Sobald das Active Directory vom Server entfernt wurde, können Sie diesen neu starten. Nach der Herabstufung eines Domänencontrollers wird dieser als Mitgliedsserver in die Domäne aufgenommen. Wenn auf dem Server Applikationen installiert waren, zum Beispiel Exchange, stehen diese nach dem Neustart weiterhin zur Verfügung.

Abbildg. 8.109 Auswählen, ob beim Entfernen eines Domänencontrollers die ganze Domäne ebenfalls entfernt werden soll



Erzwungene Herabstufung eines Domänencontrollers

Wenn Sie einen Domänencontroller, der die Verbindung mit dem Active Directory verloren hat, nicht neu installieren wollen, können Sie das Active Directory trotz fehlender Verbindung entfernen. Starten Sie dazu den Assistenten zum Entfernen von Active Directory über *Start/Ausführen/dcpromo* mit der Option */forceremoval*. Der Assistent startet und meldet, dass das Entfernen von Active Directory von diesem Server erzwungen wird (Abbildung 8.110). Verwaltet der Server FSMO-Rollen oder ist der DNS-Dienst installiert, erscheinen Fehlermeldungen. Starten Sie den Assistenten mit der Option */demotefsmo:yes* werden diese Meldungen unterdrückt. Diese Einstellungen lassen sich auch in einer Antwortdatei konfigurieren (siehe den Abschnitt »Herabstufung eines Domänencontrollers« am Ende dieses Kapitels) Nach der gezwungenen Entfernung von Active Directory ist der Domänencontroller allerdings kein Mitgliedsserver, sondern ein allein stehender Server. Sie können sich daher an diesem Server nicht mehr bei der Domäne anmelden. Als lokales Kennwort für den Administrator wird das Kennwort verwendet, das Sie auf diesem Server für den Verzeichnisdienstwiederherstellungsmodus beim Erstellen von Active Directory verwendet haben. Nachdem das Active Directory von dem Server entfernt wurde, wird in der Ereignisanzeige eine entsprechende Meldung protokolliert. Der Server wird bei diesem Vorgang allerdings nicht aus dem Active Directory entfernt. Sie müssen nachträglich die Active Directory-Metadaten bereinigen (wie im nächsten Abschnitt ausführlich beschrieben).

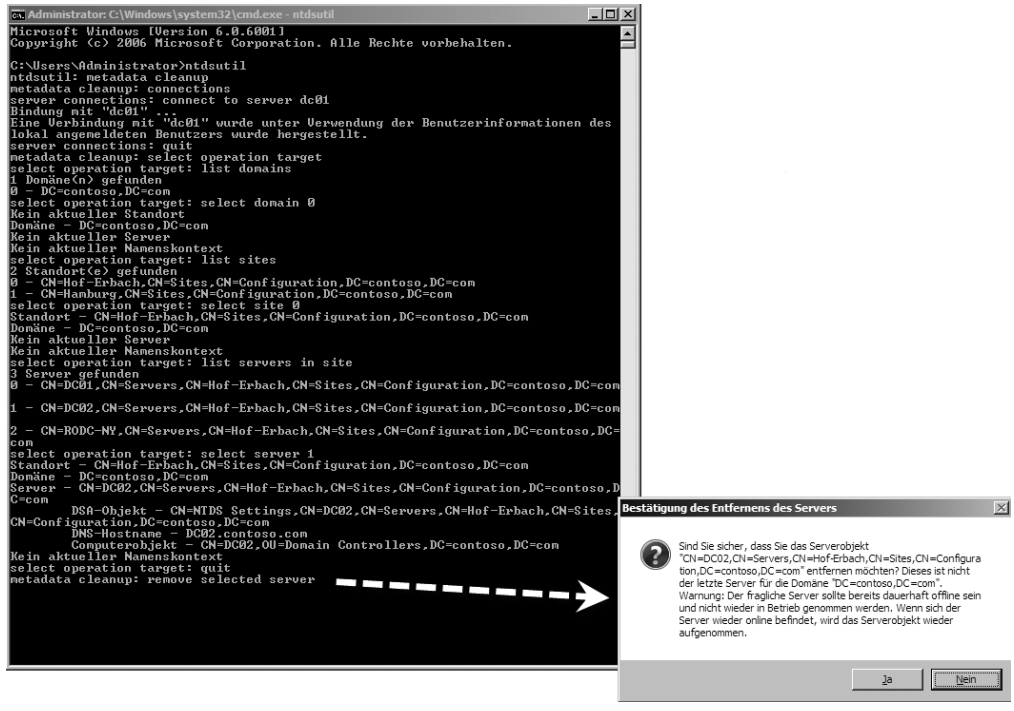
Abbildg. 8.110 Erzwungene Entfernung von Active Directory

Bereinigen der Metadaten von Active Directory

Die Metadaten von Active Directory enthalten alle Einträge und Servernamen, die zum Active Directory gehören. Wenn ein Domänencontroller ausfällt oder erzwungen aus dem Active Directory entfernt wird, sollten diese Metadaten nachträglich bereinigt werden. Für diese Bereinigung benötigen Sie das Befehlszeilenprogramm *ntdsutil.exe*, das Sie bereits beim Verschieben der FSMO-Rollen kennen gelernt haben. Um die Metadaten von Active Directory zu bereinigen, starten Sie zunächst *ntdsutil.exe* in der Befehlszeile. Gehen Sie wie in den folgenden Schritten beschrieben vor (Abbildung 8.111):

1. Geben Sie nach dem Start von *ntdsutil* den Befehl *metadata cleanup* ein.
2. Geben Sie im Anschluss daran *connections* ein.
3. Geben Sie den Befehl *connect to server <Domänencontroller>* ein. Verwenden Sie am besten einen globalen Katalog und führen Sie diese Maßnahmen in einer Terminalsitzung auf dem Server aus.
4. Geben Sie dann einmal den Befehl *quit* ein, damit Sie wieder im Menü *metadata cleanup* sind.
5. Als Nächstes müssen Sie *select operaton target* eingeben.
6. Es folgt der Befehl *list domains*. Damit werden alle Domänen der Gesamtstruktur angezeigt.
7. Geben Sie danach den Befehl *select domain <Nummer der Domäne>* ein. Wählen Sie als Nummer die Domäne aus, von der Sie den Domänencontroller entfernen wollen.
8. Geben Sie als Nächstes *list sites* ein. Daraufhin werden alle Standorte der Gesamtstruktur angezeigt.
9. Wählen Sie den Standort aus, von dem Sie einen Domänencontroller entfernen wollen. Verwenden Sie dazu den Befehl *select site <Nummer des Standortes>*.
10. Nachdem Sie den Standort ausgewählt haben, geben Sie den Befehl *list servers in site* ein. Es werden alle Server in diesem Standort angezeigt.
11. Dann müssen Sie mit *select server <Nummer des Servers>* den Server angeben, den Sie aus dem Active Directory entfernen wollen.
12. Wenn Sie den Server ausgewählt haben, geben Sie *quit* ein, damit Sie wieder in das Menü *metadata cleanup* gelangen.
13. Wenn Sie wieder im Menü *metadata cleanup* angelangt sind, geben Sie den Befehl *remove selected server* ein. Es folgt eine Warnmeldung, in der Sie das Entfernen des Servers bestätigen müssen. Bestätigen Sie diese Meldung, wird der Server aus dem Active Directory entfernt.
14. In *ntdsutil* werden die einzelnen Vorgänge beim Entfernen des Servers angezeigt.
15. Im Anschluss können Sie *ntdsutil* mit *quit* beenden. Die Active Directory-Metadaten sind bereinigt.

Abbildg. 8.111 Entfernen eines verwaisten Domänencontrollers aus der Active Directory-Datenbank



Nacharbeiten der Bereinigung

Nachdem die Metadaten von Active Directory bereinigt wurden, sollten Sie noch die Einträge im DNS bereinigen. Entfernen Sie alle SRV-Records, in denen noch der alte Server steht, aus der DNS-Zone der Domäne. Gehen Sie bei der Entfernung vorsichtig vor und löschen Sie keine Daten von anderen Domänencontrollern. Entfernen Sie auch alle Hosteinträge des Servers. In allen Einstellungen und Einträgen auf dem DNS-Server und in der DNS-Zone sollte der Server entfernt sein. Wenn Sie alle DNS-Einträge aus der Zone entfernt haben, können Sie das Computerkonto des Servers löschen, falls dies noch nicht geschehen ist. Löschen Sie das Konto aus der OU *Domain Controllers* im Snap-In *Active Directory-Benutzer und -Computer.*

Active Directory mit Antwortdatei installieren – Core-Server als Domänencontroller

Auch Core-Server können als Domänencontroller verwendet werden. Das Active Directory kann allerdings nicht wie andere Rollen auf einem Core-Server installiert werden (siehe die Kapitel 3 und 4). Soll daher ein Core-Server als Domänencontroller dienen, muss das Active Directory mit einer Antwortdatei installiert werden. Der bekannte Assistent *dcpromo* funktioniert auf Core-Servern nicht, sondern kann nur in der Befehlszeile eine Antwortdatei auslesen. Soll daher auf einem Core-

Server das Active Directory installiert werden, muss eine Antwortdatei erstellt und diese bei der Heraufstufung verwendet werden. Auf den nächsten Seiten gehen wir auf dieses Thema ein. Die unbeaufsichtigte Installation von Active Directory kann auch auf herkömmlichen Servern durchgeführt werden, zum Beispiel als Skript, um Server in Niederlassungen zu Domänencontrollern heraufzustufen.

Variablen der Antwortdateien für die unbeaufsichtigte Installation

Um das Active Directory unbeaufsichtigt zu installieren, wird in der Befehlszeile *dcpromo /answer:<Antwortdatei>* oder *dcpromo /unattend:<Antwortdatei>*eingegeben. Die Kunst dabei ist, diese Antwortdatei korrekt zu erstellen und die Informationen aufzunehmen, die für die Installation benötigt werden. Die Antwortdatei ist eine normale Textdatei. Diese besteht zunächst aus dem Kopf *[DCInstall]*. Mit diesem Kopf wird dem Server mitgeteilt, dass anschließend Anweisungen für die unbeaufsichtigte Installation von Active Directory erfolgen. Die Antwortdatei muss dazu nicht nur aus den Antworten für die Installation eines Domänencontrollers enthalten, sondern kann auch Antworten für die unbeaufsichtigte Installation von Windows Server 2008 enthalten. In diesem Abschnitt gehen wir jedoch vor allem auf die unbeaufsichtigte Installation von Active Directory ein. Nach dem Kopf können verschiedene Variablen verwendet werden und hinter einem Gleichheitszeichen ein Wert für diese Variable. So kann zum Beispiel mit *AutoConfigDNS = Yes* konfiguriert werden, dass der Assistent die DNS-Einstellungen für eine neue Domäne automatisch vornimmt. Zwischen Variable und Wert kann noch ein Leerzeichen eingefügt werden, nach der Syntax *<Variable>_ =_ <Wert>*. Dies dient aber nur der besseren Übersicht und wird nicht vorgeschrieben. In der Tabelle 8.1 haben wir für Sie die meisten möglichen Variablen und deren Möglichkeiten aufgelistet.

Tabelle 8.1 Mögliche Variablen zum Erstellen einer Antwortdatei für die unbeaufsichtigte Installation von Active Directory, zum Beispiel auf einem Core-Server

Variable	Beschreibung
AdministratorPassword	Mit diesem Wert wird das lokale Administratorkennwort des Servers festgelegt, das während der Herabstufung vom Domänencontroller zum Mitgliedsserver verwendet wird. Bei der Heraufstufung wird diese Option nicht benötigt. Das Kennwort wird nach dem Gleichheitszeichen in Klartext eingetragen. Wird dieser Wert nicht angegeben, verwendet der Assistent ein leeres Kennwort. Nach der Herabstufung wird der Wert aus der Antwortdatei gelöscht, sodass das Kennwort nicht nachvollzogen werden kann.
AutoConfigDNS	Durch diese Option kann die DNS-Konfiguration für die Domäne automatisch durch den Assistenten durchgeführt werden, wenn festgestellt wird, dass kein DNS-Server für die neue Domäne vorhanden ist. Die möglichen Antworten sind = *Yes* oder = *No*. Wird dieser Wert nicht angegeben, geht der Assistent von der Standardantwort *Yes* aus.

Tabelle 8.1 Mögliche Variablen zum Erstellen einer Antwortdatei für die unbeaufsichtigte Installation von Active Directory, zum Beispiel auf einem Core-Server *(Fortsetzung)*

Variable	Beschreibung
ChildName	Durch diese Variable wird festgelegt, wie der untergeordnete Name der Domäne ist, wenn die Domäne als Childdomäne für eine übergeordnete Domäne installiert wird. Ein Beispielwert ist *ChildName = berlin.* Hier muss nicht der komplette DNS-Name (FQDN) der neuen Childdomäne mitgegeben werden, sondern nur der Name, der an die übergeordnete Domäne angehängt wird. Wird eine untergeordnete Domäne erstellt, ist dieser Wert zwingend, es gibt keine Standardantwort. Natürlich darf die hier angegebene Domäne noch nicht existieren und es muss ein DNS-Server verfügbar sein, der die Domäne verwendet oder auf dem diese automatisch durch den Assistent erstellt werden kann. Der Wert ist eng mit der Variable *TreeOrChild* verbunden.
ConfirmGc	Durch diese Option wird der neue Domänencontroller auch zum globalen Katalog. Die möglichen Antworten sind = *Yes* oder = *No*. Wird dieser Wert nicht angegeben, geht der Assistent von der Standardantwort *Yes* aus. Diese Option spielt eine Rolle, wenn der Wert *ReplicationSourcePath* verwendet wird. Handelt es sich bei den Dateien, von denen repliziert werden soll, um eine Datensicherung eines globalen Katalogs, kann der neue Server ebenfalls seine globalen Katalogdaten aus diesen Dateien ziehen. Die Option kann aber auch ohne den Wert *ReplicationSourcePath* verwendet werden.
CreateOrJoin	Mit dieser Option wird festgelegt, ob eine neue Gesamtstruktur oder eine Struktur innerhalb einer bestehenden Gesamtstruktur erstellt werden soll. Die möglichen Antworten sind = *Create* oder = *Join*. Durch *Create* wird eine neue Gesamtstruktur erstellt, mit *Join* eine neue Struktur innerhalb der Gesamtstruktur. Der Standardwert ist *Join*. Dieser Wert wird hauptsächlich für die Abwärtskompatibilität zu Windows 2000 verwendet. Für Windows Server 2008 kann, wie für Windows Server 2003, die Option *NewDomain* verwendet werden.
CriticalReplicationOnly	Hier wird festgelegt, dass während der Heraufstufung nur die wichtigsten Daten repliziert werden und die komplette Replikation der Active Directory-Daten erst nach der Heraufstufung durchgeführt wird. Die möglichen Antworten sind = *Yes* oder = *No*. Nach der Heraufstufung und dem Neustart des Servers werden die restlichen Daten im Hintergrund repliziert.
DatabasePath	Hiermit wird der Pfad zu der Active Directory-Datenbank festgelegt. Standardmäßig wird das Verzeichnis *\Windows\ntds* verwendet. Enthält der Pfad Leerzeichen, muss dieser in Anführungszeichen gesetzt werden.
DisableCancelForDnsInstall	Mit dieser Option kann die *Abbrechen*-Schaltfläche während der DNS-Konfiguration ausgeblendet werden. Die möglichen Antworten sind = *Yes* oder = *No*. Wird dieser Wert nicht angegeben, geht der Assistent von der Standardantwort *No* aus. Die *Abbrechen*-Schaltfläche wird also angezeigt.
DNSOnNetwork	Mit dieser Option wird festgelegt, ob die IP-Adresse des DNS-Servers automatisch aus dem Netzwerk bezogen werden soll. Die möglichen Antworten sind = *Yes* oder = *No*. Wird dieser Wert nicht angegeben, geht der Assistent von der Standardantwort *Yes* aus. Bei *No* wird der DNS-Dienst installiert, eine funktionsfähige DNS-Infrastruktur erstellt und eine Zone für die neue Domäne erstellt. Der Wert wird verwendet, wenn eine neue Domäne in einer neuen Gesamtstruktur erstellt wird und die DNS-Konfiguration keinen funktionsfähigen DNS-Server für die neue Domäne enthält. Ohne diese Option wird in diesem Fall die Installation mit Fehlermeldungen abgebrochen, da ohne funktionsfähiges DNS kein Active Directory installiert werden kann.

Tabelle 8.1 Mögliche Variablen zum Erstellen einer Antwortdatei für die unbeaufsichtigte Installation von Active Directory, zum Beispiel auf einem Core-Server *(Fortsetzung)*

Variable	Beschreibung
DomainNetBiosName	Wird eine neue Domäne erstellt, kann mit dieser Option der NetBIOS-Name dieser Domäne konfiguriert werden. Wird eine neue Domäne erstellt, ist diese Option zwingend vorgeschrieben.
IsLastDCInDomain	Wird mit dem Assistenten das Active Directory von einem Server unbeaufsichtigt entfernt, kann mit dieser Option festgelegt werden, dass es sich bei dem Domänencontroller um den letzten der Domäne handelt. In diesem Fall wird auch die Domäne aus der Struktur entfernt. Die möglichen Antworten sind = *Yes* oder = *No*. Wird dieser Wert nicht angegeben, geht der Assistent von der Standardantwort *No* aus.
LogPath	Diese Option legt den Pfad zu den Protokolldateien zum Active Directory fest. Existiert das Verzeichnis nicht, wird es automatisch angelegt. Ohne diesen Pfad erfolgt die Ablage im gleichen Verzeichnis wie die Datenbank, was in den meisten Fällen in Ordnung ist, außer bei sehr großen Umgebungen.
NewDomain	Diese Option legt fest, ob mit dem Domänencontroller eine komplett neue Domäne erstellt werden soll. Diese Option ist extrem wichtig. Es wird festgelegt, ob es sich um eine neue Struktur (= *Tree*), eine untergeordnete Domäne (= *Child*) oder eine neue Gesamtstruktur (= *Forest*) handelt. Der Standardwert ist = *Forest*.
NewDomainDNSName	Dieser Wert legt den Namen einer neuen Struktur einer neuen Gesamtstruktur fest, wenn zum Beispiel auch eine neue Gesamtstruktur installiert wird. Hier muss der FQDN, also der vollständige DNS-Name der neuen Struktur oder Gesamtstruktur angegeben werden.
ParentDomainDNSName	Mit dieser Option wird der DNS-Name einer existierenden Domäne mitgegeben, wenn zum Beispiel eine untergeordnete Domäne installiert werden soll. Hier wird der FQDN der übergeordneten Domäne der untergeordneten Domäne angegeben. Hierbei ist es wichtig, dass die Anmeldedaten für diese Domäne korrekt in der Antwortdatei hinterlegt sind und dass die aktuelle DNS-Konfiguration den Namen auch auflösen kann. Hierbei muss der Name einer bereits existierenden Domäne angegeben werden, nicht der Namen einer neu zu installierenden.
Password	Hiermit wird das Kennwort für den Benutzer mitgegeben, über den der Domänencontroller heraufgestuft wird. Nach der Heraufstufung wird das Kennwort aus der Datei entfernt.
RebootOnSuccess	Legt fest, dass der Server nach erfolgreicher Heraufstufung neu gestartet wird. Die möglichen Antworten sind = *Yes* oder = *No* oder =*NoAndNoPromptEither*. Bei *No* erfolgt kein Neustart, aber der Administrator erhält ein Popup-Fenster, in dem zum Neustart aufgefordert wird. Bei = *NoAndNoPromptEither* wird nicht neu gestartet und es erscheint auch kein Meldefenster. Bei = *Yes* wird der Server ohne Rückfrage gestartet, was bei der Installation von Active Directory auf einem Server auch notwendig ist.
RemoveApplicationPartitions	Legt fest, dass bei der Herabstufung eines Domänencontrollers auch eventuell vorhandene Anwendungsverzeichnispartitionen gelöscht werden. Die möglichen Antworten sind = *Yes* oder = *No*. Wird dieser Wert nicht angegeben, geht der Assistent von der Standardantwort *No* aus. Setzen Sie die Option *IsLastDCInDomain* auf =*Yes*, muss dieser Wert gesetzt sein.
ReplicaDomainDNSName	Legt den Namen der DNS-Domäne fest, die repliziert werden soll. Hierbei muss es sich um eine Domäne in der bestehenden Gesamtstruktur handeln, mit der sich der Server verbinden kann, um Daten zu replizieren.

Tabelle 8.1 Mögliche Variablen zum Erstellen einer Antwortdatei für die unbeaufsichtigte Installation von Active Directory, zum Beispiel auf einem Core-Server *(Fortsetzung)*

Variable	Beschreibung
ReplicaOrNewDomain	Dieser Wert legt fest, ob der Server als zusätzlicher Domänencontroller in einer existierenden Domäne aufgenommen werden soll oder ob eine neue Domäne erstellt wird. Die möglichen Antworten sind = *Replica* oder = *Domain*. Bei = *Replica* wird der Server als zusätzlicher Domänencontroller einer existierenden Domäne installiert. Bei = *Domain* wird eine neue Domäne innerhalb einer neuen Domäne installiert. Dieser Wert muss zusammen mit *TreeOrChild* verwendet werden. Der Standardwert ist = *Replica*.
ReplicationSourceDC	Mit dieser Option wird ein existierender Domänencontroller mitgegeben, von dem der neue DC seine Daten replizieren kann
ReplicationSourcePath	Hiermit wird der Pfad zu den Systemdateien konfiguriert, mit deren Hilfe der neue Domänencontroller heraufgestuft wird. Hierbei handelt es sich üblicherweise um eine Datensicherung eines existierenden Domänencontrollers, von der dieser neuer Domänencontroller die Active Directory-Daten replizieren kann. So müssen die Daten nicht aus dem Active Directory über das Netzwerk repliziert werden, sondern können auch lokal kopiert und dann integriert werden. Natürlich können nicht alle Daten von Dateien repliziert werden, sondern nach der ersten erfolgreichen Replikation muss eine Replikation mit einem existierenden Domänencontroller erfolgen. Hierzu wird dann zusätzlich noch die Option *ReplicationSourceDC* verwendet. Ohne diesen Wert findet die Replikation über das Netzwerk statt.
SafeModeAdminPassword	Hier wird das Kennwort für den Verzeichnisdienstwiederherstellungsmodus mitgeteilt. Alternativ kann noch der Wert = *None* mitgegeben werden, das ist auch die Standardantwort. In diesem Fall wird für diesen Modus kein Kennwort festgelegt.
SetForestVersion	Hiermit wird der Betriebsmodus der neuen Gesamtstruktur festgelegt. Die möglichen Antworten sind = *Yes* oder = *No*. Bei = *Yes* wird der Windows Server 2003-Betriebsmodus aktiviert, bei = *N*o der Kompatibilitätsmodus zu Windows 2000. Der Standardwert ist = *No*.
SiteName	Durch diese Option wird der Standortname im Active Directory festgelegt. Wird dieser Wert nicht angegeben, weist das Setup den Standort auf Basis der IP-Adresse automatisch zu.
Syskey	Mit dieser Option wird festgelegt, dass der Benutzer den Systemschlüssel bereithalten muss. Diese Option wird nur benötigt, wenn die Variable *ReplicationSourcePath* gesetzt ist, also die erste Replikation aus geschützten Systemdateien erfolgt. Der Key wird während der Erstellung dieser Dateien konfiguriert.
SysVolPath	Hiermit wird das Sysvol-Verzeichnis festgelegt. Der Wert muss nicht angegebenen werden. Standardmäßig werden in diesem Verzeichnis Anmeldeskripts und Gruppenrichtlinien angelegt. Es liegt im Verzeichnis *C:\Windows*.
TreeOrChild	Hier wird festgelegt, ob die Domäne eine neue Stammdomäne für eine neue Domänenstruktur wird oder eine untergeordnete Domäne innerhalb einer bereits existierenden Domäne. Die möglichen Antworten sind = *Tree* oder = *Child*. Bei = *Tree* wird eine neue Domäne für eine neue Struktur innerhalb einer bestehenden Gesamtstruktur erstellt. Dazu muss *CreateOrJoin* oder *NewDomain* korrekt gesetzt sein. Bei = *Child* wird eine untergeordnete Domäne erstellt. Die Standardantwort ist = *Child*.
UserDomain	Mit dieser Option wird die Domäne mitgegeben, in der sich der Benutzername findet, mit dem die Heraufstufung stattfindet

Tabelle 8.1 Mögliche Variablen zum Erstellen einer Antwortdatei für die unbeaufsichtigte Installation von Active Directory, zum Beispiel auf einem Core-Server *(Fortsetzung)*

Variable	Beschreibung
UserName	Diese Option legt den Benutzernamen fest, mit dem die Heraufstufung erfolgen soll

Die in Tabelle 8.1 gezeigten Optionen zur unbeaufsichtigten Installation von Active Directory funktionieren auch für Windows Server 2003. Zusätzlich wurden mit Windows Server 2008 weitere Optionen hinzugefügt, die in Tabelle 8.2 besprochen werden. Die neuen Variablen können auf exakt dem gleichen Weg zu einer Antwortdatei hinzugefügt werden wie die bereits bekannten Variablen.

Tabelle 8.2 Neue Variablen für die unbeaufsichtigte Installation von Windows Server 2008

Neue Variablen für Windows Server 2008	Beschreibung der neuen Variablen
/AllowDomainReinstall	Mit diesem Wert kann eine Domäne neu installiert werden, auch wenn diese bereits vorhanden ist. Die möglichen Antworten sind = *Yes* oder = *No*. Wird dieser Wert nicht angegeben, geht der Assistent von der Standardantwort *Yes* aus.
/installDNS	Dieser Wert ersetzt den Wert *AutoConfigDNS*, der aber auch noch immer funktioniert. Die möglichen Antworten sind = *Yes* oder = *No*. Wird dieser Wert nicht angegeben, geht der Assistent von der Standardantwort *Yes* aus.
/DNSDelegation	Mit dieser Option kann für Active Directory-integrierte DNS-Zonen eine Delegation auf den neuen DNS-Server eingerichtet werden (siehe Kapitel 11). Die möglichen Antworten sind = *Yes* oder = *No*.
/DNSDelegationUserName	Mit diesem Wert wird das Benutzerkonto angegeben, dass berechtigt ist, auf den existierenden DNS-Servern eine Delegation einzurichten
/DNSDelegationPassword	Mit diesem Wert wird das Kennwort für den Benutzernamen hinterlegt, mit dem die Delegation für DNS eingerichtet wird
/DomainLevel	Mit diesem Wert wird die Funktionsebene der Domäne festgelegt. Verwendet werden können *0* (Windows 2000 kompatibel), *2* (Windows Server 2003-Modus) und *3* (Windows Server 2008-Modus).
/ForestLevel	Dieser Wert setzt den Wert *SetForestVersion*. Hiermit kann die Funktionsebene der Gesamtstruktur festgelegt werden. Verwendet werden können *0* (Windows 2000 kompatibel), *2* (Windows Server 2003-Modus) und *3* (Windows Server 2008-Modus). Der Standardwert ist *0*.
/OnDemandAllowed	Mit dieser Option können die Benutzer- und Computerkonten festgelegt werden, die auf schreibgeschützte Domänencontroller (RODC) repliziert werden
/OnDemandDenied	Diese Option legt die Computer- und Benutzerkonten fest, die nicht auf den RODC repliziert werden dürfen
/ReplicaOrNewDomain	Dieser Wert legt fest, ob der Domänencontroller als zusätzlicher, normaler, Domänencontroller (=*replica*), als schreibgeschützter Domänencontroller (=*ReadOnlyReplica*) oder als neuer Domänencontroller (=*domain*) einer neuen Domäne installiert werden soll. Der Standardwert ist *replica*.
/ServerAdmin	Mit diesem Wert kann der Benutzername festgelegt werden, der über Admin-Rechte auf einem RODC verfügen soll

Tabelle 8.2 Neue Variablen für die unbeaufsichtigte Installation von Windows Server 2008 *(Fortsetzung)*

Neue Variablen für Windows Server 2008	Beschreibung der neuen Variablen
/DemoteFSMO	Wird ein Domänencontroller herabgestuft, kann mit dieser Option festgelegt werden, dass die gezwungene Herabstufung auch dann fortgesetzt wird, wenn der Domänencontroller eine FSMO-Rolle verwaltet. Die möglichen Antworten sind *=yes* und *=no*, die Standardantwort ist *no*.
/IgnoreIsLastDcInDomainMismatch	Wird der Wert *IsLastDCInDomain* gesetzt und liefert die Option einen Fehler zurück, weil doch noch Domänencontroller in der Domäne gefunden werden, kann mit dieser Option die Herabstufung erzwungen werden. Die möglichen Antworten sind *=yes* und *=no*, die Standardantwort ist *no*.
/RebootOnCompletion	Diese Variable ist ähnlich zu *RebootOnSuccess* mit dem Unterschied dass auch gebootet wird, wenn die Heraufstufung nicht erfolgreich war. Auch hier stehen als Antwort wieder *yes* und *no* zur Verfügung.

Praxisbeispiele für den Einsatz einer Antwortdatei

Im folgenden Abschnitt zeigen wir Ihnen, welche Variablen auf jeden Fall gesetzt werden sollen, abhängig von der Rolle, die dem Domänencontroller zugewiesen werden soll. In diesem Abschnitt werden die möglichen Optionen verwendet, die auch kompatibel zu Windows Server 2003 sind, da für Migrationen eine solche Vorgehensweise zur Installation oder Deinstallation von Active Directory optimal sind. Die auf den folgenden Seiten beschriebenen Werte können natürlich beliebig mit den Werten aus Tabelle 8.2 ergänzt werden. Viele Befehle sind auch neu in Windows Server 2008 eigeführt worden. Verwenden Sie Befehle, die bereits in Windows Server 2003 unterstützt wurden, erscheint eine Warnung sowie ein Vorschlag, welcher neue Befehl verwendet werden kann.

Erstellen einer neuen Gesamtstruktur

Soll eine neue Struktur innerhalb einer neuen Gesamtstruktur erstellt werden, sind folgende Variablen notwendig:

[DCINSTALL]

ReplicaOrNewDomain=Domain

TreeOrChild=Tree

CreateOrJoin=Create

NewDomainDNSName=<FQDN der neuen Struktur, zum Beispiel corp.com >

DNSOnNetwork=yes

DomainNetbiosName=<NetBIOS-Domänennamen>

AutoConfigDNS=yes

SiteName=<Optionaler Standortname>

AllowAnonymousAccess=no

DatabasePath=%SystemRoot%\ntds

LogPath=%SystemRoot%\ntds

SYSVOLPath=%SystemRoot%\sysvol

SafeModeAdminPassword=<Kennwort>

CriticalReplicationOnly=No

RebootOnSuccess=yes

Installation einer neuen, untergeordneten Domäne (Childdomäne)

Soll eine neue, untergeordnete Domäne in einer existierenden Struktur installiert werden, sind folgende Variablen empfohlen:

[DCINSTALL]

UserName=<Benutzername mit Rechten neue Domänen in der Gesamtstruktur zu erstellen>

Password=<Kennwort für den Benutzernamen>

UserDomain=<Domäne in der das angegebene Konto liegt>

DatabasePath=%SystemRoot%\ntds

LogPath=%SystemRoot%\ntds

SYSVOLPath=%SystemRoot%\sysvol

SafeModeAdminPassword=<Kennwort>

CriticalReplicationOnly=no

ReplicaOrNewDomain=Domain

TreeOrChild=Child

ParentDomainDNSName=<FQDN der übergeordneten Domäne>

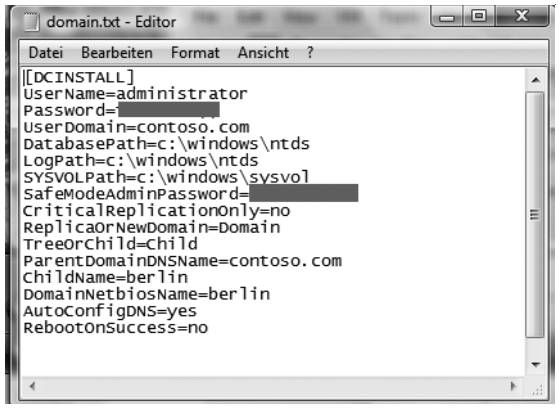
ChildName=<FQDN der neuen Domäne>

DomainNetbiosName=<NetBios-Name der Domäne>

AutoConfigDNS=yes (Abhängig von der Infrastruktur des Unternehmens)

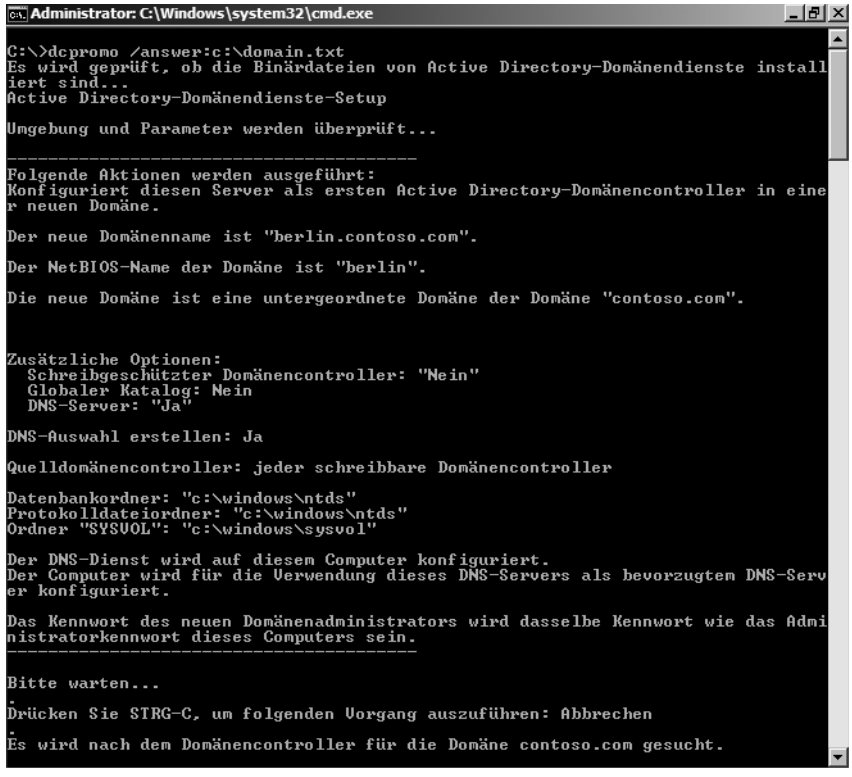
RebootOnSuccess=yes

Abbildg. 8.112 Beispiel einer Antwortdatei für die unbeaufsichtigte Installation von Active Directory



Nachdem Sie die Installation über *dcpromo /answer:<Antwortdatei>* oder *dcpromo /unattend:<Antwortdatei>*gestartet haben, wird die Installation durchgeführt. Über die Befehlszeile erhalten Sie Rückinfos über die einzelnen Maßnahmen, die vorgenommen werden (Abbildung 8.113).

Abbildg. 8.113 Installieren von Active Directory über eine Antwortdatei



Installation einer neuen Struktur innerhalb einer bestehenden Gesamtstruktur

Für eine neue Struktur in einer bereits bestehenden Gesamtstruktur verwenden Sie am besten folgende Optionen:

[DCINSTALL]

UserName=<Benutzername mit Rechten, neue Domänen in der Gesamtstruktur zu erstellen>

Password=<Kennwort für den Benutzernamen>

UserDomain=<Domäne, in der das angegebene Konto liegt>

DatabasePath=%SystemRoot%\ntds

LogPath=%SystemRoot%\ntds

SYSVOLPath=%SystemRoot%\sysvol

SafeModeAdminPassword=<Kennwort>

SiteName=<Optionaler Standortname>

CriticalReplicationOnly=no

ReplicaOrNewDomain=Domain

TreeOrChild=Tree

NewDomainDNSName=<FQDN der neuen Struktur, zum Beispiel corp.com >

DomainNetbiosName=<NetBIOS-Domänennamen>

AutoConfigDNS=yes (Abhängig von der Infrastruktur des Unternehmens)

RebootOnSuccess=yes

Neuer Domänencontroller in existierender Domäne

Soll ein neuer Domänencontroller in einer bereits existierenden Domäne als zusätzlicher DC installiert werden, verwenden Sie am besten die folgenden Variablen:

[DCINSTALL]

UserName=<Benutzername mit Rechten, neue Domänen in der Gesamtstruktur zu erstellen>

Password=<Kennwort für den Benutzernamen>

UserDomain=<Domäne, in der das angegebene Konto liegt>

DatabasePath=%SystemRoot%\ntds

LogPath=%SystemRoot%\ntds

SYSVOLPath=%SystemRoot%\sysvol

CriticalReplicationOnly=no

ReplicaOrNewDomain=Replica

ReplicaDomainDNSName=<FQDN der Domäne>

ReplicationSourceDC=<FQDN eines existierenden DCs innerhalb der Domäne>

RebootOnSuccess=yes

Herabstufung eines Domänencontrollers

Soll ein Domänencontroller zu einem normalen Mitgliedsserver über eine Antwortdatei herabgestuft werden, sind folgende Variablen zu empfehlen:

[DCINSTALL]

UserName=<Benutzername mit Rechten, neue Domänen in der Gesamtstruktur zu erstellen>

Password=<Kennwort für den Benutzernamen>

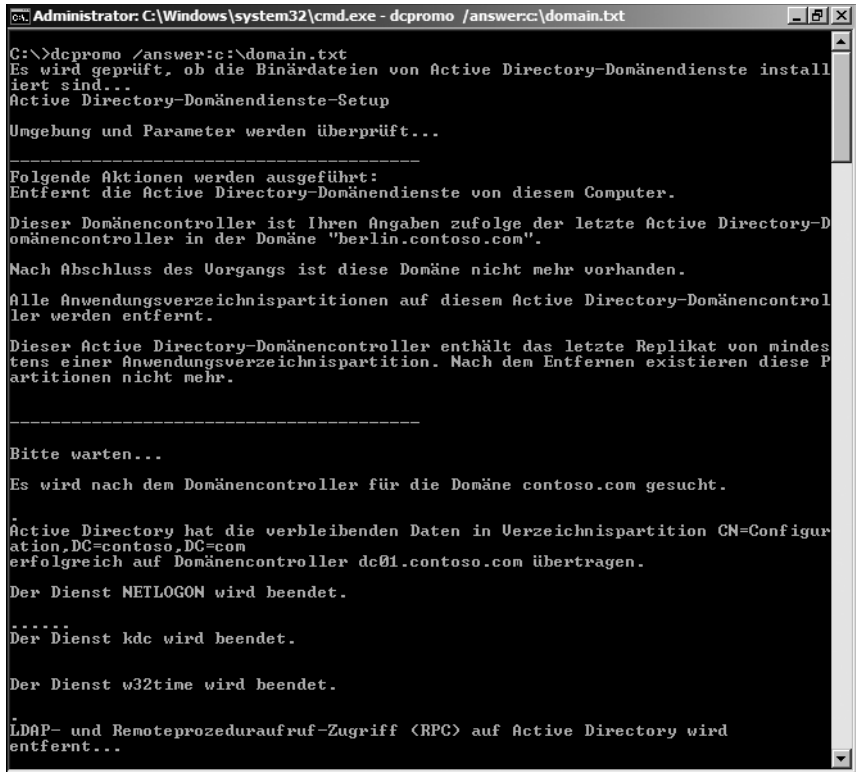
UserDomain=<Domäne, in der das angegebene Konto liegt>

AdministratorPassword=<Kennwort des neuen lokalen Administrators>

IsLastDCInDomain=< Ja oder Nein, siehe Tabelle 8.1>

RebootOnSuccess=yes

Abbildg. 8.114 Entfernen von Active Directory über eine Antwortdatei von einem Core-Server



Durchführung der Installation von Active Directory mit einer Antwortdatei

Wollen Sie die Installation mit einer Antwortdatei durchführen, müssen Sie folgende Vorbereitungen treffen, die bereits in diesem Kapitel besprochen wurde. Auch in Kapitel 4 und 11 werden die entsprechenden Vorbereitungen getroffen:

- Installieren Sie den Server als Core-Server, falls Sie die Installation auf einem solchen Server durchführen wollen (siehe Kapitel 2).
- Richten Sie den Server im Netzwerk ein. Sie sollten IP-Adresse, den richtigen Namen und die Partitionen erstellen, wie gewünscht (siehe die Kapitel 2, 3, 4 und 7).
- Aktivieren Sie den Server (siehe die Kapitel 2 und 3).
- Wollen Sie neue Strukturen, Gesamtstrukturen oder untergeordnete Domänen installieren, bereiten Sie die DNS-Konfiguration vor, wie in diesem Kapitel und in Kapitel 11 besprochen wurde.
- Erstellen Sie die Antwortdatei als Textdatei und kopieren Sie diese lokal auf den Server.
- Wollen Sie die erste Replikation von Systemdateien durchführen, müssen Sie diese zunächst erstellen und lokal auf den neuen Server kopieren.

Haben Sie diese Vorbereitungen getroffen, kann das Active Directory auf dem Server installiert werden. Rufen Sie dazu das Installationsprogramm von Active Directory über die Option *dcpromo /answer:<Antwortdatei>* oder *dcpromo /unattend:<Antwortdatei>* auf. Entsprechende Meldungen der Installation werden in der Befehlszeile angezeigt, das gilt auch für Fehler. Achten Sie darauf, dass auch bei Abbrüchen die Kennwörter aus der Antwortdatei entfernt werden und vor dem neuen Starten eingetragen werden müssen. Nach der Installation wird der Server neu gestartet und das Active Directory ist installiert.

HINWEIS Achten Sie darauf, vorher das Remotemanagement in der Firewall freizuschalten. Verwenden Sie dazu den Befehl *netsh advfirewall set allprofiles settings remotemanagement enable*. Den kompletten Netzwerkverkehr auf einem Core-Server können Sie über *netsh advfirewall set allprofiles firewallpolicy allowinbound,allowoutbound* freischalten. Anschließend können Sie über die einzelnen MMCs, zum Beispiel auch direkt über die Computerverwaltung, auf die Funktionen des Core-Servers zugreifen und diesen verwalten.

Zusammenfassung

Auch wenn vieles gleich geblieben ist, haben Sie in diesem Kapitel gelesen, dass Microsoft im Bereich Active Directory viele Verbesserungen integriert hat. Mit dem schreibgeschützten Domänencontroller, dem verbesserten Rollenmodell und den überarbeiteten Assistenten und Möglichkeiten zur automatisierten Installation profitieren Unternehmen deutlich von der Einführung des neuen Servers als Domänencontroller. Im nächsten Kapitel zeigen wir Ihnen, wie Sie die neuen Funktionen zu den Gruppenrichtlinien produktiv einsetzen. Auch hier hat Microsoft vieles geändert, vor allem im Detail. Im nächsten Kapitel erfahren Sie, wie Sie in einer Domäne Gruppenrichtlinie einsetzen und verwalten.

Kapitel 9

Gruppenrichtlinien einsetzen

In diesem Kapitel:

Eine wichtige Aufgabe bei der Administration eines Servers ist die Verwaltung von Benutzer- und Computereinstellungen. Damit sind nicht nur Desktop-Einstellungen gemeint, sondern auch sicherheitsrelevante Einstellungen und die Konfiguration von Programmen wie Internet Explorer, Windows-Explorer oder Office-Programmen. Für diese Verwaltungsarbeiten stehen die lokalen Sicherheitsrichtlinien und in Domänen die Gruppenrichtlinien zur Verfügung. Mit diesen lassen sich zahlreiche Einstellungen auf einem Server oder PC automatisch vorgeben. So lässt sich beispielsweise das Verhalten des Internet Explorer oder die Konfiguration der Kennwörter definieren. Lokale Sicherheitsrichtlinien arbeiten auch unter Windows Server 2008 mit speziellen Registry-Schlüsseln, die zu keinen permanenten Änderungen der Registry führen. Die Informationen werden so lange in diesen Schlüsseln gehalten, wie die Einstellung in der lokalen Sicherheitsrichtlinie gültig ist. Microsoft hat im Bereich der Gruppenrichtlinien unter Windows Server 2008 und Windows Vista wichtige Änderungen vorgenommen, die in diesem Kapitel besprochen werden.

Lokale Sicherheitsrichtlinien

Lokale Sicherheitsrichtlinien bieten die Möglichkeit, Einstellungen des Servers entweder auf Benutzerebene oder für den ganzen Server in einer zentralen Oberfläche zu konfigurieren, die ansonsten nicht zur Verfügung stehen. Die Aufgaben der lokalen Sicherheitsrichtlinien dienen hauptsächlich, wie der Name schon sagt, der Konfiguration der Sicherheit. In Unternehmen werden diese Einstellungen zentral vorgegeben und automatisch an alle Server verteilt. Diese Richtlinien werden dann Gruppenrichtlinien bezeichnet. Die lokalen Sicherheitsrichtlinien können Sie am besten über den Gruppenrichtlinienverwaltungs-Editor konfigurieren. Diesen können Sie über *Start/Ausführen/gpedit.msc* aufrufen (Abbildung 9.1). Der Gruppenrichtlinienverwaltungs-Editor besteht aus zwei Hälften. Auf der linken Seite (die so genannte Konsolenstruktur) können Sie auswählen, für welchen Bereich Sie Einstellungen vornehmen wollen:

- Die Einstellungen unter *Computerkonfiguration* werden auf Server und PCs angewendet, wenn diese gestartet werden. Hier hat sich in der Bedienung wenig geändert.
- Die Einstellungen unter *Benutzerkonfiguration* werden auf die Profile der einzelnen Anwender angewendet, wenn sich diese beim Server anmelden. Auch hier gibt es zwar neue Einstellungen, aber die generelle Bedienung ist noch identisch.

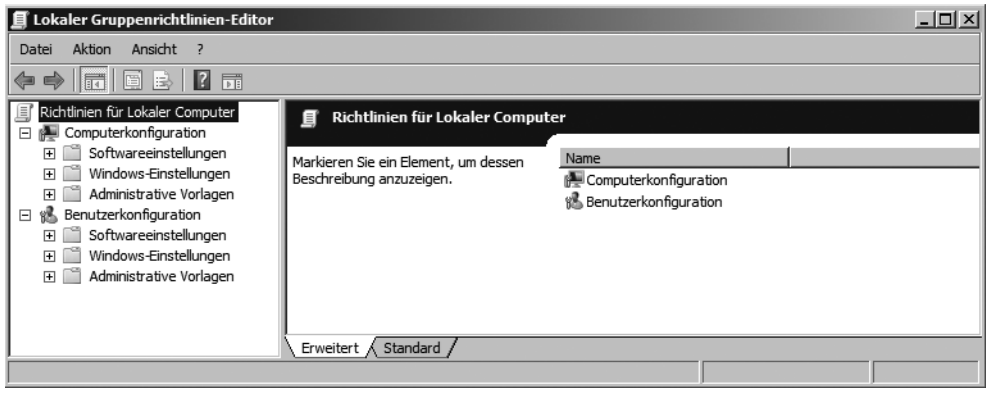
Die Einstellungen sind jeweils in drei weitere Einträge unterteilt:

- **Softwareeinstellungen** Über diesen Eintrag können Sie Applikationen automatisch verteilen lassen.
- **Windows-Einstellungen** In diesem Bereich befinden sich die meisten Einstellungen, die Sie vornehmen können, und zwar hauptsächlich Skripts, die durch diese Gruppenrichtlinien beim Starten eines Servers oder Anmelden eines Anwenders ausgeführt werden, und die Sicherheitseinstellungen.
- **Administrative Vorlagen** Hier finden sich einige Möglichkeiten zur Einstellung und Automatisierung von Windows Server 2008 und Windows Vista. Sie können Einstellungen im Windows-Explorer, dem Desktop und vielen anderen Funktionen in Windows vornehmen.

Klicken Sie sich durch die Einträge der Konsolenstruktur, werden auf der rechten Seite die Einstellungen angezeigt, die in diesem Bereich verfügbar sind.

Öffnen Sie die Einstellungen per Doppelklick, können Sie Konfigurationen vornehmen, die an die Benutzer bei der *Benutzerkonfiguration* oder die Server bei der *Computerkonfiguration* weitergegeben werden.

Abbildg. 9.1 Neue lokale Richtlinien in Windows Server 2008



Neue lokale Richtlinien

Vor Windows Server 2008 wurde nur ein lokales Gruppenrichtlinienobjekt unterstützt. Wenn an der Eingabeaufforderung *gpedit.msc* eingegeben und einige Änderungen an den Einstellungen vorgenommen wurden, dann wirkten sich die Änderungen auf alle Benutzer und Administratoren aus, die diesen Computer verwendeten. Die neuen Funktionen zur Unterstützung mehrerer lokaler Gruppenrichtlinienobjekte haben mehrere Gruppenrichtlinienobjektschichten. Diese Fähigkeit wird wahrscheinlich hauptsächlich auf Systemen eingesetzt, die nicht in einer Active Directory-Domäne zusammengefasst sind. Die neuen Funktionen zur Unterstützung mehrerer lokaler Gruppenrichtlinienobjekte, die auf Schichten basieren, können ein wenig kompliziert werden. Es gibt immer noch ein lokales Standardgruppenrichtlinienobjekt, das für den Kontext des lokalen Computersystems gilt und alle Benutzer auf dem System betrifft. Dieses Gruppenrichtlinienobjekt definiert sowohl die Computereinstellungen als auch die Benutzereinstellungen. Die zweite Schicht betrifft entweder die Mitglieder der lokalen Administratorgruppe oder die Gruppe der Benutzer auf dem lokalen System, bei denen es sich nicht um Administratoren handelt. Per Definition kann sich ein Benutzerkonto nicht in beiden Gruppen befinden. Die Schicht ermittelt, ob es sich beim Benutzer um einen lokalen Systemadministrator oder einen regulären Benutzer handelt. Anschließend wird das entsprechende Gruppenrichtlinienobjekt (entweder Administratoren oder Nicht-Administratoren) angewendet. Die dritte Schicht betrifft das lokale Systembenutzerkonto mit einem bestimmten Namen. Das bedeutet, es gibt drei potenzielle lokale Gruppenrichtlinienobjekte, die einen bestimmten Benutzer betreffen können, der am Computer sitzt. Sie können zum Beispiel drei Schichten verwenden, um für alle Benutzer, die an einem bestimmten Computer arbeiten, Einstellungen festzulegen, um mehr Einstellungen für die Nicht-Administratoren an diesem Computer und schließlich um Einstellungen festzulegen, die nur einen einzelnen Benutzer betreffen, der diesen Computer verwendet. Wenn das System jedoch an einer Active Directory-Domäne teilnimmt, haben die Active Directory-Gruppenrichtlinienobjekte Priorität vor den lokalen Richtlinien. Sie sollten außerdem beachten, dass Domänenadministratoren die gesamte Verarbeitung der lokalen Gruppenrichtlinienobjekte für Windows Server 2008 und auch Windows Vista ausschalten können. Die Bearbeitung

dieser Einstellungen läuft dabei fast immer identisch ab: Auf der Registerkarte *Sicherheitseinstellung* beziehungsweise Einstellung können Sie entweder direkt Einstellungen weitergeben oder die Einstellung lediglich aktivieren bzw. deaktivieren, wenn keine weiteren Eingaben vorgegeben werden müssen. Eine Einstellung kann verschiedene Zustände annehmen:

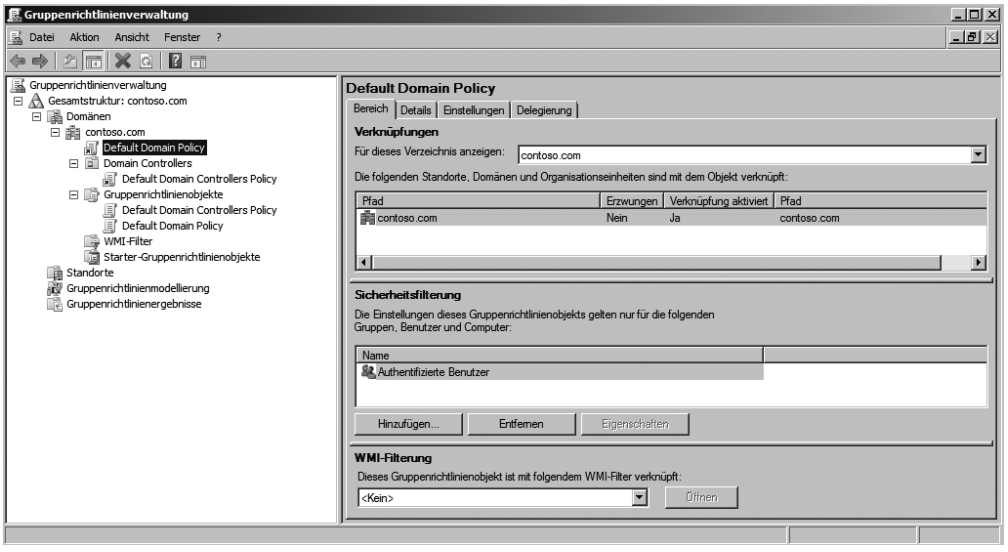
- **Aktiviert** Bei dieser Einstellung wird die Konfiguration auf das Zielobjekt angewendet und weitergegeben.
- **Deaktiviert** Bei dieser Einstellung wird die Konfiguration der Gruppenrichtlinie auf dem Server auf den Standard zurückgesetzt.
- **Nicht konfiguriert** Bei dieser Einstellung wird die lokale Einstellung des Clients beibehalten und durch die Gruppenrichtlinie nicht geändert.

Auf der Registerkarte *Erklärung* finden Sie eine ausführliche Hilfe zu der Einstellung und ihren Auswirkungen. Bevor Sie eine Einstellung aktivieren, sollten Sie sich möglichst immer die Erklärung genau durchlesen.

Gruppenrichtlinien verwalten

Eine wichtige Aufgabe bei der Administration von Netzwerken ist die Verwaltung von Benutzer- und Computereinstellungen. Damit sind nicht nur Desktop-Einstellungen oder IP-Adressen gemeint, sondern auch sicherheitsrelevante Einstellungen und die Konfiguration von Programmen, wie Internet Explorer, Windows-Explorer oder Office-Programme. Für diese Verwaltungsarbeiten stehen die Gruppenrichtlinien (Group Policies), oft auch als Gruppenrichtlinienobjekte (Group Policy Object, GPO) bezeichnet, zur Verfügung. Mit Gruppenrichtlinien lassen sich zahlreiche Einstellungen in einem Active Directory automatisch vorgeben. Sie können zum Beispiel das Verhalten des Internet Explorers oder die Konfiguration der Kennwörter in Ihrem Netzwerk per Gruppenrichtlinie definieren. Die Gruppenrichtlinien sind das primäre Werkzeug für die automatische Verwaltung von Konfigurationen im Netzwerk, auch für neu hinzugefügte Systeme. Die Verwaltung von Gruppenrichtlinien über die Gruppenrichtlinienverwaltungskonsole ist nahezu identisch zu Windows Server 2003. Die Gruppenrichtlinienverwaltungskonsole (GPMC) muss unter Windows Server 2008 nicht mehr heruntergeladen werden. Sie können diese als Funktion über den Server-Manager hinzufügen. Klicken Sie dazu auf *Features* und dann auf *Features hinzufügen*. Wählen Sie aus dem Fenster zur Auswahl der zu installierenden Funktionen die *Gruppenrichtlinienverwaltung* aus. Auf Domänencontrollern wird dieses Feature standardmäßig bereits automatisch installiert. Nach kurzer Zeit ist die Installation abgeschlossen und die Gruppenrichtlinienverwaltung steht über die Programmgruppe *Verwaltung* zur Verfügung (Abbildung 9.2). Der Umgang und die Verwaltung der Konsole hat sich nicht grundlegend geändert.

Abbildg. 9.2 Die Gruppenrichtlinienverwaltung unter Windows Server 2008



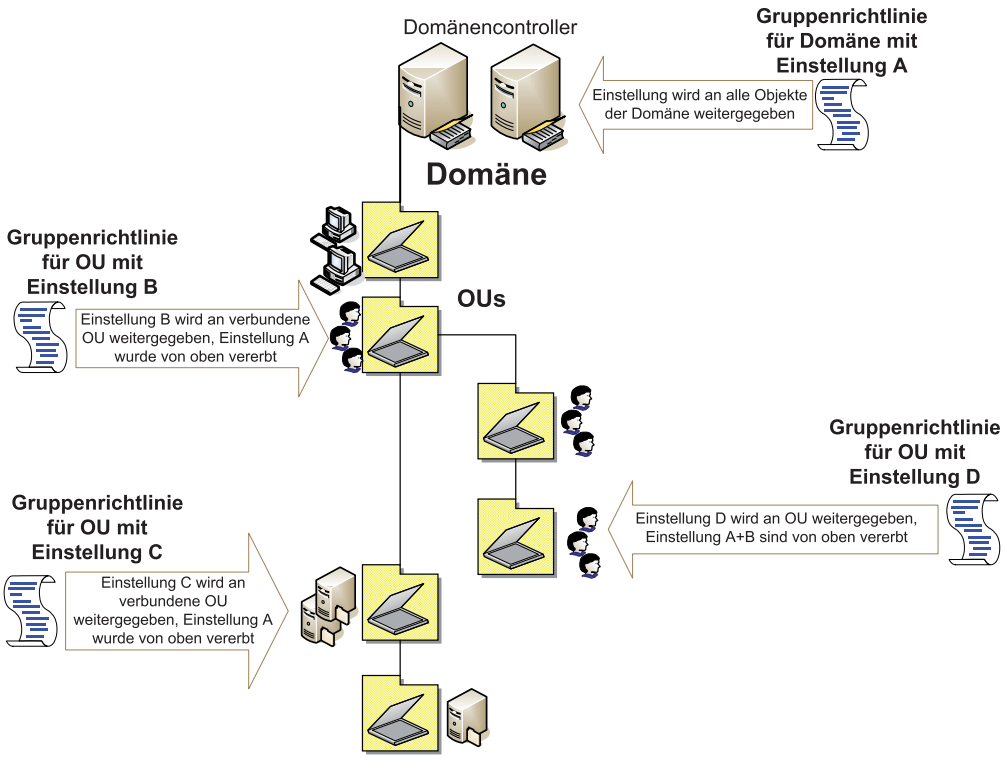
Grundlagen und Überblick der Gruppenrichtlinien

Wenn Sie mit der Verwaltung von Gruppenrichtlinien beginnen, sollten Sie zunächst zwei Definitionen verstehen, die oft verwechselt werden:

- Gruppenrichtlinienobjekte (Group Policies Objects, GPOs)
- Gruppenrichtlinienverknüpfungen

Allgemein wird oft von Gruppenrichtlinien gesprochen. Damit sind meistens die GPOs gemeint. Ein GPO ist eine Gruppenrichtlinie, in der Einstellungen vorgenommen und gespeichert wurden. Diese Einstellungen legen für Benutzer-PCs oder Benutzerkonten fest, wie sich die Systeme verhalten, zum Beispiel die automatische Konfiguration des Internet Explorers. Diese Einstellungen werden innerhalb eines Containers, der GPO, gespeichert. Damit diese Einstellungen jedoch auch angewendet werden, muss die GPO mit Organisationseinheiten oder einer ganzen Domäne verknüpft werden. Erst wenn eine GPO mit einer Organisationseinheit verknüpft ist, werden die Einstellungen innerhalb der GPO auf die entsprechende OU angewendet. In diesem Fall spricht man von Gruppenrichtlinienverknüpfungen. Die Einstellungen, die in einer Gruppenrichtlinie durchgeführt werden, können auch lokal gesetzt werden. Das entsprechende Programm rufen Sie über *Start/Ausführen/gpedit.msc* auf. Ein GPO kann nicht nur mit einer OU verknüpft werden, sondern mit mehreren. Wenn Einstellungen in einem GPO verändert werden, dann werden diese Änderungen auf alle verknüpften OUs übertragen. Werden Einstellungen in einem GPO verändert, das noch nicht mit einer OU verknüpft ist, werden keinerlei Änderungen durchgeführt. Diese erfolgen erst dann, wenn das GPO verknüpft ist.

Abbildg. 9.3 Die Einstellungen in den Gruppenrichtlinien werden nach unten vererbt



Neuerungen in den Gruppenrichtlinien

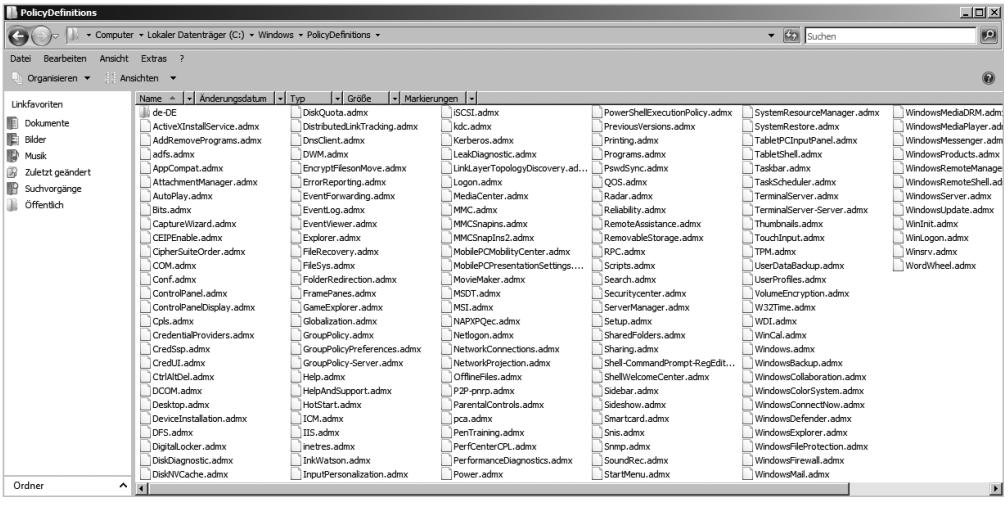
Windows Server 2008 bietet zahlreiche Neuerungen in den Gruppenrichtlinien, die natürlich ihre gesamte Funktionsbreite erst durch Einsatz von Windows Server 2008 und Windows Vista darlegen. Windows Server 2008 unterstützt als Neuerung zum Beispiel die Konfiguration der Energiesparoptionen für Windows Vista. Dadurch besteht die Möglichkeit, an zentraler Stelle die Energiesparoptionen der Notebooks und PCs festzulegen. Anwender, die ihren PC über Nacht anlassen, können so sicherstellen, dass sich ihr Monitor und Festplatte ausschalten, was bei größeren Unternehmen eine deutliche Kostenreduktion bedeuten kann, da auch für normale Desktop-PCs Energiesparmaßnahmen konfiguriert werden können. Auch der Zugriff auf USB-Sticks kann in Windows Server 2008, zusammen mit Windows Vista, konfiguriert werden. Viele Änderungen hat Microsoft bezüglich der Einstellmöglichkeiten des Internet Explorers integriert. Auch die Steuerung von Druckerinstallationen und der Druckerverwaltung in Windows wurde erneuert.

Neue administrative Vorlagen

Unter Windows XP und Windows Server 2003 gab es für unterschiedliche Sprachversionen von Windows unterschiedliche Versionen der Vorlagendateien (**.adm*-Dateien). Da dies vor allem für internationale Unternehmen nicht sehr effizient ist, hat Microsoft das Design der Vorlagendateien

angepasst. Änderungen in Gruppenrichtlinien müssen dadurch nicht in jeder Sprachversion eingestellt werden, sondern nur noch einmal zentral im Unternehmen. Die alten Vorlagen-Dateien (**.adm*) können unter Windows Server 2008 weiterhin verwendet werden. Windows Server 2008 verwendet für seine neuen Vorlagendateien sprachneutrale **.admx*-Dateien. Diese bauen auf XML auf. Diese **.admx*-Dateien werden nicht mehr für jede einzelne Gruppenrichtlinie hinterlegt, sondern zentral im *Policy*-Ordner. Dadurch wird deutlich Bandbreite gespart, da nur noch die Einstellungen in den Gruppenrichtlinien repliziert werden müssen, nicht mehr alle **.adm*-Dateien bei jeder Replikation. Unter Windows Server 2003 wurden in allen Gruppenrichtlinienobjekten immer alle verwendeten **.adm*-Dateien gespeichert, was zu einem unnötigen Datenverkehr bei der Replikation und unnötigen Speicherplatzverbrauch führt. **.adm*-Dateien haben auch Schwierigkeiten beim Einsatz von unterschiedlichen Windows-Versionen im Netzwerk und dadurch resultierenden unterschiedlichen **.adm*-Dateien. Die Gruppenrichtlinientools – der Gruppenrichtlinienverwaltungs-Editor und die Gruppenrichtlinienverwaltung (GPMC) – bleiben weitestgehend unverändert. In den meisten Situationen werden Sie nicht einmal bemerken, dass es nur **.admx*-Dateien gibt. Die Vorlagendateien von Windows Server 2008 (**.admx*) liegen im Verzeichnis *C:\Windows\PolicyDefinitions* (Abbildung 9.4).

Abbildg. 9.4 Die neuen Gruppenrichtlinienvorlagen von Windows Server 2008



Wenn Sie eine **.admx*-Datei mit dem Editor öffnen, sehen Sie den XML-typischen Aufbau der neuen Gruppenrichtliniendateien (siehe Listing 9.1).

Listing 9.1 Aufbau einer **.admx*-Datei in Windows Server 2008

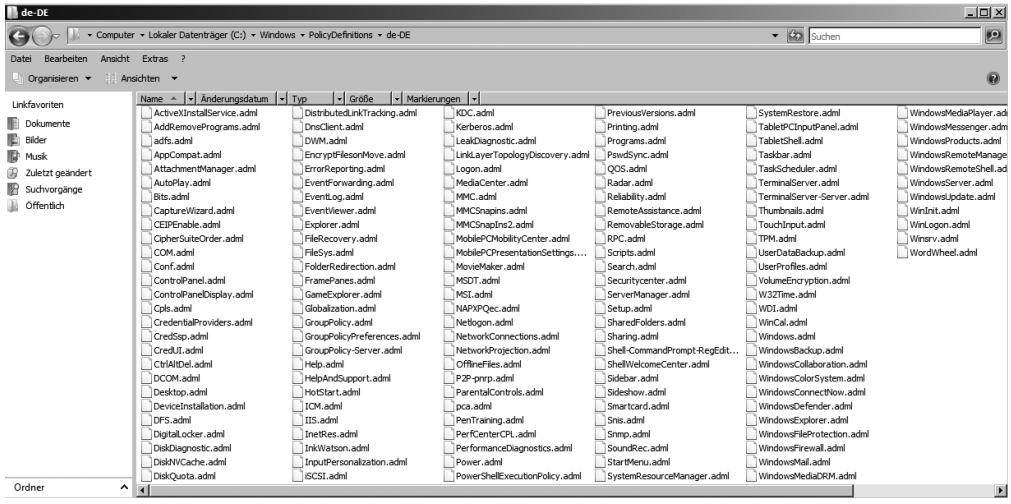
```
<?xml version="1.0" encoding="utf-8"?>
<!--  (c) 2006 Microsoft Corporation  -->
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
  <policyNamespaces>
    <target prefix="bits" namespace="Microsoft.Policies.BITS" />
    <using prefix="windows" namespace="Microsoft.Policies.Windows" />
```

Listing 9.1 Aufbau einer **.admx*-Datei in Windows Server 2008 *(Fortsetzung)*

```
  </policyNamespaces>
  <resources minRequiredRevision="1.0" />
  <supportedOn>
    <definitions>
      <definition name="SUPPORTED_WindowsXPWindowsNETorBITS15"
displayName="$(string.SUPPORTED_WindowsXPWindowsNETorBITS15)" />
      <definition name="SUPPORTED_WindowsXPSP2WindowsNETSP1orBITS20"
displayName="$(string.SUPPORTED_WindowsXPSP2WindowsNETSP1orBITS20)" />
    </definitions>
  </supportedOn>
  <categories>
    <category name="BITS" displayName="$(string.BITS)">
      <parentCategory ref="windows:Network" />
    </category>
  </categories>
  <policies>
    <policy name="BITS_EnablePeercaching" class="Machine"
displayName="$(string.BITS_EnablePeercaching)"
explainText="$(string.BITS_EnablePeercachingText)"
key="Software\Policies\Microsoft\Windows\BITS" valueName="EnablePeercaching">
        <parentCategory ref="BITS" />
        <supportedOn ref="windows:SUPPORTED_WindowsVista" />
        <enabledValue>
            <decimal value="1" />
        </enabledValue>
        <disabledValue>
            <decimal value="0" />
        </disabledValue>
    </policy>
    <policy name="BITS_Job_Timeout" class="Machine"
displayName="$(string.BITS_Job_Timeout)" explainText="$(string.BITS_Job_Timeout_Help)"
presentation="$(presentation.BITS_Job_Timeout)"
key="Software\Policies\Microsoft\Windows\BITS">
      <parentCategory ref="BITS" />
      <supportedOn ref="SUPPORTED_WindowsXPWindowsNETorBITS15" />
      <elements>
        <decimal id="BITS_Job_Timeout_Time" valueName="JobInactivityTimeout" minValue="1"
maxValue="999" />
      </elements>
    </policy>
```

Im Verzeichnis der Gruppenrichtlinienvorlagen sehen Sie auch die installierten Sprachversionen von Windows Server 2008. Für jede installierte Sprache wird ein eigener Ordner angelegt. In diesem Ordner liegen die Dateien in Form von **.adml*-Dateien, da diese an die entsprechende Sprache angepasst sind. Für jede installierte Sprache auf einem Server gibt es einen entsprechenden Ordner. Jeder dieser Ordner enthält die sprachspezifischen **.adml*-Dateien, die auf die entsprechende sprachneutrale **.admx*-Datei referenziert. Beim Einsatz von Windows Server 2008 ohne Active Directory-Domäne werden die **.admx*-, und **.adml*-Dateien lokal im bereits beschriebenen Ordner gespeichert. Unter Windows Server 2008 werden die **.admx*-Dateien nicht vom Gruppenrichtlinienverwaltungs-Editor und von der Gruppenrichtlinienverwaltungskonsole in das gerade bearbeitete GPO kopiert. Stattdessen werden die Dateien von einem zentralen Speicherort im SYSVOL-Ordner eines Domänencontrollers gelesen (dieser Speicherort ist nicht anpassbar). Wenn dieser zentrale Speicherort nicht verfügbar ist, werden die lokal gespeicherten Dateien verwendet.

Abbildg. 9.5 Angepasste Sprachdateien für Gruppenrichtlinien unter Windows Server 2008



Kompatibilität zwischen ADM- und ADMX-Dateien

Ihre eigenen ADM-Dateien werden weiterhin von den Gruppenrichtlinientools angezeigt – die durch ADMX-Dateien ersetzten ADM-Dateien jedoch nicht. Bei den ersetzten Dateien handelt es sich um:

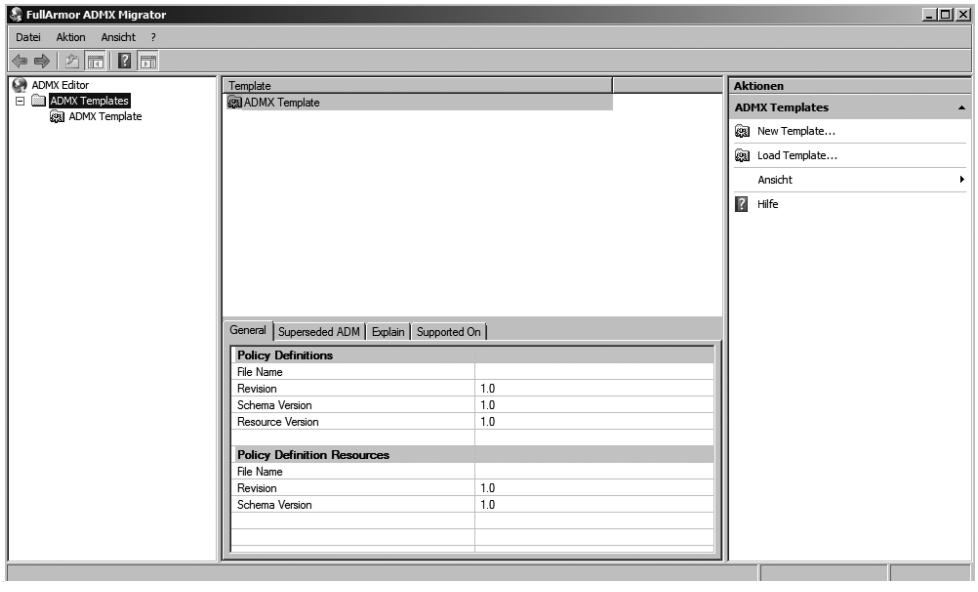
- System.adm
- Inetres.adm
- Conf.adm
- Wmplayer.adm
- Wuau.adm

Wenn Sie eine dieser Dateien angepasst haben, werden die angepassten Einstellungen unter Windows Server 2008 daher nicht mehr angezeigt. Zusätzlich sollten Sie beim Einsatz der neuen Werkzeuge und Einstellungen für die Gruppenrichtlinien unter Windows Server 2008 noch folgende Fakten kennen:

1. Der Gruppenrichtlinienverwaltungs-Editor zeigt die Einstellungen aus den ADMX-Dateien automatisch an. Sie können auch weiterhin eigene ADM-Dateien hinzufügen oder entfernen. Alle derzeit über die ADM-Dateien von Windows Server 2003, Windows XP und Windows 2000 umgesetzten Einstellungen werden auch über die ADMX-Dateien von Windows Server 2008 und Windows Server 2008 zur Verfügung stehen.
2. Die neuen Richtlinieneinstellungen für Windows Server 2008 können nur über Computer unter Windows Server 2008 oder Windows Vista und deren Gruppenrichtlinienverwaltungs-Editor oder die Gruppenrichtlinienverwaltung angezeigt oder bearbeitet werden. Diese Einstellungen werden nur über ADMX-Dateien definiert. Sie sind daher unter Windows Server 2003, Windows XP oder Windows 2000 nicht zu sehen.

3. Die Berichtsfunktion der Gruppenrichtlinienverwaltung unter Windows Server 2003 und Microsoft Windows XP zeigt die neuen Windows Server 2008-Einstellungen unter dem Eintrag *Administrative Vorlagen* als eigene Registrierungseinstellungen an.
4. Die Windows Server 2008- und Windows Vista-Versionen des Gruppenrichtlinienverwaltungs-Editors und der Gruppenrichtlinienverwaltung können zur Verwaltung aller Betriebssysteme verwendet werden, die Gruppenrichtlinien unterstützen (Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP und Windows 2000).
5. In ADM-Dateien vorhandene Einstellungen unter dem Knoten *Administrative Vorlagen* aus Windows Server 2003, Windows XP und Windows 2000 können über jedes Betriebssystem konfiguriert werden, das Gruppenrichtlinien unterstützt (Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP und Windows 2000).
6. Der Gruppenrichtlinienverwaltungs-Editor und die Gruppenrichtlinienverwaltung von Windows Server 2008 und Windows Vista arbeiten mit den entsprechenden Versionen unter Windows Server 2003 und Windows XP zusammen. Angepasste ADM-Dateien, die in GPOs gespeichert sind, werden zum Beispiel unter Windows Server 2008, Windows Vista, Windows Server 2003 und Windows XP angezeigt.
7. Der Gruppenrichtlinienverwaltungs-Editor von Windows Server 2008 und Windows Vista arbeitet mit dem Gruppenrichtlinienverwaltungs-Editor von Windows Server 2003 zusammen. Angepasste ADM-Dateien, die in GPOs gespeichert sind, werden zum Beispiel unter Windows Server 2008, Windows Vista, Windows Server 2003 und Windows 2000 angezeigt (die Konsole der Gruppenrichtlinienverwaltung gibt es unter Windows 2000 nicht).

Abbildg. 9.6 Migrieren und bearbeiten von Gruppenrichtlinienvorlagen-Dateien mit dem kostenlosen *ADMX Migrator*



TIPP Zur Migration bisheriger ADM-Vorlagen, aber auch für das Erstellen neuer Vorlagen, gibt es jetzt ein Snap-In für die Managementkonsole, den *ADMX Migrator*. Das Tool kann über das Microsoft Download-Center heruntergeladen werden (*http://www.microsoft.com/downloads/details.aspx?FamilyId=0F1EEC3D-10C4-4B5F-9625-97C2F731090C&displaylang=en*). Das Tool kann bestehende **.adm*-Dateien in **.admx* umwandeln oder neue ADMX-Vorlagen erstellen (Abbildung 9.6).

Voraussetzungen für die Bearbeitung von GPOs

Die Bearbeitung von lokalen GPOs muss über einen Computer unter Windows Server 2008 oder Windows Vista erfolgen. Um domänenbasierte GPOs bearbeiten und erstellen zu können, benötigen Sie die folgenden Konfigurationen:

- Eine Domäne unter Windows Server 2008, Windows Server 2003 oder Windows 2000 mit funktionierender DNS-Namensauflösung über einen DNS-Server
- Einen Computer unter Windows Server 2008 oder Windows Vista, um die Richtlinieneinstellungen aus den ADMX-Dateien anzeigen zu können

Der Gruppenrichtlinienverwaltungs-Editor erkennt ADM-Dateien, wenn diese in Ihrer Umgebung vorhanden sind. ADM-Dateien, die durch ADMX-Dateien ersetzt wurden, werden jedoch ignoriert (diese sind, wie bereits beschrieben, *System.adm, Inetres.adm, Conf.adm, Wmplayer.adm* und *Wuau.adm*).

Administration von domänenbasierten GPOs mit ADMX-Dateien

Zentral gespeicherte ADMX-Dateien ermöglichen es den Administratoren, domänenbasierte GPOs mit den gleichen ADMX-Dateien zu bearbeiten. Wenn Sie die ADMX-Dateien nicht zentral speichern, funktioniert das Bearbeiten der GPOs genauso wie im vorherigen Abschnitt bei der Bearbeitung der administrativen Vorlagen. Nachdem Sie einen zentralen Speicherort eingerichtet haben, nutzen Gruppenrichtlinientools nur noch diese zentral gespeicherten ADMX-Dateien und ignorieren die lokalen Versionen. Die Ordnerstruktur für die zentrale Speicherung befindet sich im SYSVOL-Verzeichnis auf den Domänencontrollern. Sie müssen diesen nur einmal pro Domäne erstellen. Der Dateireplikationsdienst repliziert ihn dann auf alle anderen Domänencontroller der jeweiligen Domäne. Es wird empfohlen, die Ordnerstruktur auf dem PDC-Emulator der Domäne zu erstellen. Da sie sich standardmäßig mit dem PDC-Emulator verbinden, können die Gruppenrichtlinientools so schneller auf die ADMX-Dateien zugreifen. Der zentrale Speicherort setzt sich folgendermaßen zusammen:

- Ein Stammordner, in dem alle sprachneutralen ADMX-Dateien enthalten sind
- Unterordner mit den sprachspezifischen ADMX-Dateien

Zum Erstellen eines zentralen Speicherortes für ADMX-Dateien gehen Sie folgendermaßen vor:

1. Erstellen Sie auf Ihrem Domänencontroller einen Stammordner: *%SystemRoot%\SYSVOL\domain\Policies\PolicyDefinitions*.

2. Erstellen Sie unter *%SystemRoot%\SYSVOL\domain\Policies\PolicyDefinitions* einen Unterordner für jede Sprache, die von Ihren Gruppenrichtlinienadministratoren verwendet wird. Jeder Unterordner sollte entsprechend der passenden ISO-Abkürzung benannt werden. Eine Liste der ISO-Kürzel finden Sie auf der Webseite *http://msdn2.microsoft.com/en-us/library/ms693062.aspx*. Der Unterordner für *Englisch/USA* sieht zum Beispiel so aus: *%SystemRoot%\SYSVOL\domain\Policies\PolicyDefinitions\EN-US,* bei deutschen Servern wird *DE-DE* verwendet.

Um diese Schritte durchführen zu können, müssen Sie Mitglied der Active Directory-Gruppe *Domänen-Admins* sein.

Speichern der ADMX-Dateien am zentralen Speicherort

Nach der Erstellung des zentralen Speicherortes müssen Sie die ADMX-Dateien, deren Einstellungen Sie zentral verwalten wollen, in den zentralen Speicherort kopieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie eine Befehlszeile.
2. Kopieren Sie alle sprachneutralen Dateien (**.admx*) in den zentralen Ordner *\PolicyDefinitions*.
3. Kopieren Sie alle sprachspezifischen Dateien (**.adml*) in die entsprechenden Unterordner.

Bearbeiten von Richtlinieneinstellungen unter dem Knoten *Administrative Vorlagen* in domänenbasierten GPOs

Die folgenden Schritte müssen Sie auf einem Windows Vista oder Windows Server 2008-Computer ausführen – anderenfalls werden die Einstellungen aus den ADMX-Dateien nicht angezeigt:

1. Öffnen Sie den Gruppenrichtlinien-Editor.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Gruppenrichtlinienobjekte* und wählen Sie im Kontextmenü den Befehl *Neu* aus.
3. Geben Sie einen Namen für das neue GPO ein, und klicken Sie auf *OK*.
4. Erweitern Sie den Knoten *Gruppenrichtlinienobjekte*.
5. Klicken Sie mit der rechten Maustaste auf das neue GPO und wählen Sie im Kontextmenü den Befehl *Bearbeiten* aus.
6. Der Gruppenrichtlinienverwaltungs-Editor liest automatisch die zentral gespeicherten ADMX-Dateien ein. ADMX-Dateien, die zentral gespeichert sind, werden aus der Domäne gelesen, für die das GPO erstellt wurde. Sie können ADM-Dateien weiterhin mit der Option *Vorlagen hinzufügen/entfernen* hinzufügen oder entfernen.

Beschreibung der wichtigsten neuen Gruppenrichtlinien-Einstellungen

In diesem Abschnitt werden die wichtigsten neuen Einstellungen in den Gruppenrichtlinien von Windows Server 2008 erläutert (siehe Tabelle 9.1). Da fast alle Einstellungen auch über eine eigene Registerkarte *Erklärung* verfügen, können Sie auch durch Erforschen der einzelnen Bereiche optimal feststellen, welche Einstellungen benötigt werden und welche nicht.

Tabelle 9.1 Neue Gruppenrichtlinieneinstellungen in Windows Vista und Windows Server 2008

Kategorie	Beschreibung	Speicherort der Einstellung im Gruppenrichtlinienverwaltungs-Editor
Antivirus	Verwaltet das Verhalten bei der Bewertung von Anlagen mit hohem Risiko	*Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Anlagen-Manager*
Intelligenter Hintergrundübertragungsdienst (BITS – Background Intelligent Transfer Service)	Konfiguriert das neue Feature *BITS Neighbor Casting* zur Durchführung von Peer-to-Peer-Dateiübertragungen innerhalb einer Domäne. Das neue Feature wird von Windows Vista und Windows Server 2008 unterstützt.	*Computerkonfiguration/Administrative Vorlagen/Netzwerk/Intelligenter Hintergrundübertragungsdienst*
Bereitgestellte Druckerverbindungen	Stellt eine Druckerverbindung für einen Computer bereit. Dies ist hilfreich, wenn der Computer in einer gesperrten Umgebung freigegeben ist, z.B. einer Schule, oder wenn ein Benutzer an einen anderen Standort wechselt und der Drucker automatisch angeschlossen werden soll.	*Computerkonfiguration/Windows-Einstellungen/Bereitgestellte Drucker* *Benutzerkonfiguration/Windows-Einstellungen/Bereitgestellte Drucker*
Geräteinstallation	Lässt die Installation eines Geräts zu oder verweigert sie, abhängig von der Geräteklasse oder -ID	*Computerkonfiguration/Administrative Vorlagen/System/Geräteinstallation*
Datenträgerfehlerdiagnose	Steuert die Stufe des Informationsgehalts bei der Anzeige der Datenträgerfehlerdiagnose	*Computerkonfiguration/Administrative Vorlagen/System/Fehlerbehebung und Diagnose/Datenträgerdiagnose*
Brennen von Video-DVDs	Passt die Einstellungen zum Erstellen von Video-CDs oder -DVDs an	*Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Video importieren*
Quality of Service (QoS) in Unternehmen	Vermindert eine Überlastung des Netzwerks durch Aktivieren der zentralen Verwaltung von Windows Vista-Netzwerkverkehr. Ohne dass Änderungen in Anwendungen erforderlich wären, können Sie flexible Richtlinien zur Priorisierung von Differentiated Services Code Point (DSCP)-Markierungen und Begrenzungsraten definieren.	*Computerkonfiguration/Windows-Einstellungen/Richtlinienbasierte QoS*
Hybridfestplatte	Konfiguriert die Eigenschaften der Hybridfestplatte (mit nicht flüchtigem Cache), über die Sie Folgendes verwalten können: – Verwendung des nicht flüchtigen Cache – Start- und Fortsetzungsoptimierungen – Solid-State-Modus – Energiesparmodus	*Computerkonfiguration/Administrative Vorlagen/System/Nicht flüchtiger Festplattencache*
Internet Explorer 7	Ersetzt und erweitert die aktuellen Einstellungen in der Erweiterung *Internet Explorer-Wartung*, sodass Administratoren die aktuellen Einstellungen anzeigen können, ohne die Werte zu ändern	*Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Internet Explorer* *Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Internet Explorer*

Tabelle 9.1 Neue Gruppenrichtlinieneinstellungen in Windows Vista und Windows Server 2008 *(Fortsetzung)*

Kategorie	Beschreibung	Speicherort der Einstellung im Gruppenrichtlinienverwaltungs-Editor
Netzwerk: Quarantäne	Verwaltet drei Komponenten: – Health Registration Authority (HRA) – Internet Authentication Service (IAS) – Network Access Protection (NAP)	*Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Network Access Protection*
Netzwerk: Verdrahtet oder drahtlos	Verwaltet Netzwerkeinstellungen	*Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Richtlinien für verdrahtete Netzwerke (IEEE 802.11)* *Computerkonfiguration/Windows-Einstellungen/Richtlinien für drahtlose Netzwerke (IEEE 802.11)*
Energieverwaltung	Konfiguriert aktuelle Energieverwaltungsoptionen in der Systemsteuerung	*Computerkonfiguration/Administrative Vorlagen/System/Energieverwaltung*
Wechselspeichermedien	Ermöglicht Administratoren den Schutz von Unternehmensdaten durch Einschränken der Daten, die von Wechselspeichermedien gelesen und auf sie geschrieben werden können. Administratoren können Einschränkungen auf bestimmten Computern oder für bestimmte Benutzer erzwingen, ohne auf Drittanbieterprodukte zurückzugreifen oder die Busse zu deaktivieren.	*Computerkonfiguration/Softwareeinstellungen/Richtlinien/Microsoft/Windows/Wechselspeichermedien* *Benutzerkonfiguration/Softwareeinstellungen/Richtlinien/Microsoft/Windows/(Wechselspeichermedien)*
Sicherheit	Kombiniert die Verwaltung der Windows-Firewall und der IPsec-Technologien, um die Möglichkeit zu verringern, dass widersprüchliche Regeln erstellt werden. Administratoren können angeben, welche Anwendungen oder Ports geöffnet werden und ob Verbindungen zu diesen Ressourcen sicher sein müssen.	*Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Windows-Firewall*
Shell-Anwendungsverwaltung	Verwaltet den Zugriff auf Symbolleiste, Taskleiste, Startmenü und die Anzeige von Symbolen	*Benutzerkonfiguration/Administrative Vorlagen/Startmenü und Taskleiste*
Shell-Erfahrung, Anmeldung und Berechtigungen	Konfiguriert die Anmeldung mit erweiterten Gruppenrichtlinieneinstellungen für: – Roaming-Benutzerprofile – Umgeleitete Ordner – Anmeldefenster	*Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten*
Gemeinsame Nutzung der Shell, Synchronisierung und Roaming	Zur Anpassung folgender Bereiche: – Autorun für verschiedene Geräte und Medien – Erstellen und Entfernen von Partnerschaften – Synchronisierungszeitplan und -verhalten – Erstellen von Arbeitsbereichen und Zugriff auf dieselben	*Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten/*

Tabelle 9.1 Neue Gruppenrichtlinieneinstellungen in Windows Vista und Windows Server 2008 *(Fortsetzung)*

Kategorie	Beschreibung	Speicherort der Einstellung im Gruppenrichtlinienverwaltungs-Editor
Shell-Steuerelemente	Konfiguriert die Desktopanzeige bezüglich: – Aero-Anzeige – Neues Verhalten des Bildschirmschoners – Suchen und Ansichten	*Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten*
Tablet PC	Konfiguriert Tablet PCs für Folgendes: – Tablet Ink Watson und Personalisierungsfeatures – Tablet PC-Desktopfeatures – Features des Eingabebereichs – Tablet PC-Fingereingabe	*Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten* *Eingabepersonalisierung* *Stifttraining* *Tablet PC-Eingabebereich* *Fingereingabe* *Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten* *Eingabepersonalisierung* *Stifttraining* *TabletPC/Tablet PC-Eingabebereich* *TabletPC/Fingereingabe*
Terminaldienste	Konfiguriert folgende Features zur Verbesserung der Sicherheit, Benutzerfreundlichkeit und Verwaltbarkeit von Terminaldienst-Remoteverbindungen. Sie können: – Die Umleitung zusätzlicher unterstützter Geräte auf den Remotecomputer in einer Terminaldienstesitzung erlauben oder verweigern – Die Verwendung von Transport Layer Security (TLS) 1.0 oder systemeigener Remote Desktop Protocol (RDP)-Verschlüsselung erfordern oder eine Sicherheitsmethode aushandeln – Die Verwendung einer bestimmten Verschlüsselungsstufe (entsprechend FIPS, hoch, nach Clientstandard oder gering) erfordern	*Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Terminaldienste* *Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Terminaldienste*
Fehlerbehebung und Diagnose	Steuert die Diagnosestufe von der automatischen Erkennung und Behebung von Problemen bis zur Anzeige, dass eine unterstützte Lösung für die folgenden Bereiche verfügbar ist: – Anwendungsprobleme – Erkennung von Lecks – Ressourcenzuweisung	*Computerkonfiguration/Administrative Vorlagen/System/Fehlerbehebung und Diagnose/Datenträgerdiagnose*

Tabelle 9.1 Neue Gruppenrichtlinieneinstellungen in Windows Vista und Windows Server 2008 *(Fortsetzung)*

Kategorie	Beschreibung	Speicherort der Einstellung im Gruppenrichtlinienverwaltungs-Editor
Schutz der Benutzerkonten	Konfiguriert die Eigenschaften von Benutzerkonten für folgende Zwecke: – Festlegen der Aufforderung für erweiterten Zugriff – Gewähren von Zugriffsberechtigungen bei Anwendungsinstallationen – Erkennen der Benutzerkonten mit den geringsten Berechtigungen – Virtualisieren von Datei- und Registrierungsschreibfehlern an benutzerspezifischen Speicherorten	*Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Sicherheitsoptionen*
Windows-Fehlerberichterstattung	Deaktiviert Windows-Feedback nur für Windows oder für alle Komponenten. Standardmäßig ist Windows-Feedback für alle Windows-Komponenten aktiviert.	*Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Windows-Fehlerberichterstattung* *Benutzerkonfiguration/Windows-Komponenten/Administrative Vorlagen/Windows-Fehlerberichterstattung*

Steuerung der Anbindung von USB-Sticks über Gruppenrichtlinien

Durch die Unterstützung von USB-Sticks in den Gruppenrichtlinien ist es nicht mehr notwendig, den gesamten USB-Port eines Servers oder PCs zu sperren, damit keine USB-Sticks mehr angeschlossen werden können. Windows Server 2008 und Windows Vista verwendet so genannte Geräte, *Identifikations-Strings* und *Geräte-Setup-Klassen*, um die angeschlossene Hardware am Server zu identifizieren. Dadurch besteht die Möglichkeit, auf Basis dieser Geräte Einstellungen für diese Geräte selbst vorzunehmen, nicht mehr nur für den Port, an dem diese angeschlossen sind. USB-Sticks kann dadurch das Lesen gewährt, aber das Schreiben untersagt werden. Wenn ein USB-Stick an einem PC angeschlossen wird, identifiziert Windows dieses Gerät und installiert einen Treiber, um das Gerät anzusprechen. Die neuen Gruppenrichtlinien verwenden genau diese Technologie, um die angeschlossenen Geräte zu konfigurieren. Auf dieser Basis lassen sich Digitalkameras und USB-Sticks genehmigen, während USB-Festplatten ab einer gewissen Größe komplett ausgesperrt werden können. Beim Anschluss eines USB-Gerätes werden ausführliche generische Informationen übertragen, mit denen Windows Server 2008 und Windows Vista auch zusätzliche Funktionen identifizieren kann. Dies ermöglicht einem Unternehmen zum Beispiel, firmeneigene USB-Sticks zuzulassen, aber private Sticks zu sperren. So kann vermieden werden, dass Mitarbeiter Daten aus dem Unternehmen schmuggeln können oder private Daten in das Netzwerk kopieren.

ACHTUNG Achten Sie aber darauf, dass das Sperren von USB-Sticks keine Garantie dafür ist, dass Mitarbeiter Daten vom oder ins Unternehmen transportieren können. Mittlerweile besteht auch die Möglichkeit, über freien Speicherplatz im Internet Daten transportieren zu können. Eine sichere Netzwerkumgebung können Sie nur dann erreichen, wenn Sie alle Facetten des Datentransports, auch über das Internet, berücksichtigen.

Grundsätzlich können in Windows folgende Einstellungen über Richtlinien vorgenommen werden:

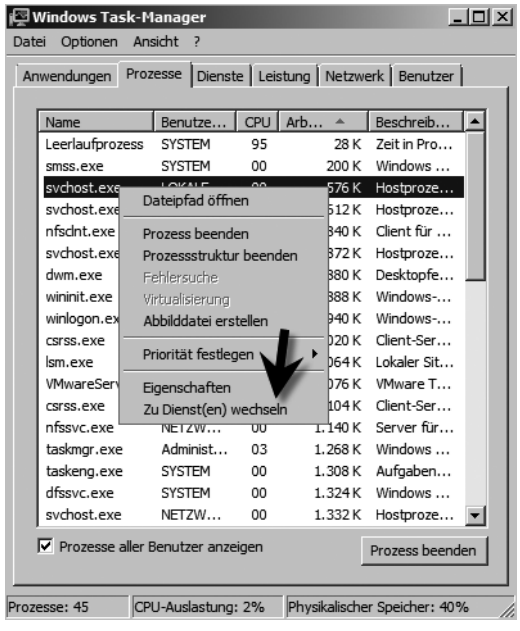
- Es kann die Geräteinstallation verhindert werden, wenn die Installation des Gerätes nicht den Richtlinien des Unternehmens entspricht
- Administratoren können gesetzte Richtlinien überschreiben
- Die Installation von Geräten kann auch auf Basis der Device-ID oder der Device-Klasse erlaubt oder verboten werden. So können Sie selbst entscheiden, ob eine Positiv- oder Negativliste für Sie einfacher zu implementieren ist.

Aktualisierte Gruppenrichtlinien und weitere Neuerungen

Unter Windows XP oder Windows Server 2003 wurde häufig das Internet Explorer Administration Kit (IEAK) zur Steuerung des Internet Explorers zu verwendet. Auch der Internet Explorer 7 unterstützt das IEAK. Dieses IEAK verwendet allerdings hauptsächlich die Gruppenrichtlinien. Die Funktionen des IEAK sind jetzt in den Gruppenrichtlinien integriert. Ebenfalls neu ist die Möglichkeit, über Gruppenrichtlinien QoS-Richtlinien festzulegen. Mit diesen Richtlinien kann eine Priorisierung des Netzwerkverkehrs durchgeführt werden. Die Basis dieser Richtlinien können Quell-IPs (IPv4 und IPv6) sein, Ziel-IPs, Protokolle oder Ports. Es können einzelnen Protokollen mehr oder weniger Bandbreite zugewiesen werden. So können Sie Instant-Messaging-Clients minimale Bandbreite zuweisen, oder wichtigen Servern eine höhere, zum Beispiel SAP-Server. Die Infrastruktur im Unternehmen muss jedoch diese Priorisierung unterstützen. Der Gruppenrichtlinien-Client in Windows Server 2008 und Windows Vista verwendet nicht mehr das ICMP-Protokoll zur Anbindung an den Domänencontroller. ICMP hat vor allem bei VPN-Verbindungen das Problem, dass die Verbindung nicht zuverlässig gemessen werden kann. Die Gruppenrichtlinien werden nicht durch die Anmeldung gestartet, sondern nur durch einen eigenen Dienst. Dadurch werden weniger Neustarts benötigt und die Gruppenrichtlinien benötigen weniger Performance. Einstellungen werden dadurch sehr schnell auf die Ziel-PCs implementiert. Dieser neue Gruppenrichtliniendienst läuft unter der *svchost.exe*. Diese Datei taucht als Prozess auf jedem Rechner einige Male im Task-Manager in der Liste der laufenden Prozesse auf. Die *svchost.exe* gibt es seit Windows 2000. Sie liegt im *System32*-Verzeichnis und wird beim Systemstart von Windows automatisch als allgemeiner Prozess gestartet. Der Prozess durchsucht beim Systemstart die Registry nach Diensten, die beim Systemstart geladen werden müssen. Dienste, die nicht eigenständig lauffähig sind, sondern über Dynamic Link Library (DLL)-Dateien geladen werden, werden mit Hilfe der *svchost.exe* geladen. Auch wenn Windows läuft, kommt die *svchost.exe* immer dann ins Spiel, wenn Dienste über DLL-Dateien geladen werden müssen. Das Betriebssystem startet SVCHOST-Sessions, sobald solche benötigt werden, und beendet sich auch wieder, sobald sie nicht mehr gebraucht werden. Da unter Windows die unterschiedlichsten Dienste parallel laufen, können auch mehrere Instanzen der *svchost.exe* gleichzeitig in der Prozessliste auftauchen. Über den Befehl *tasklist /svc* in der Befehlszeile können Sie sich anzeigen lassen, welche Anwendungen auf die *svchost.exe* zurückgreifen. Alternativ können Sie die mit der *svchost.exe* verbundenen Dienste auch im Task-Manager anzeigen lassen. Gehen Sie dazu folgendermaßen vor:

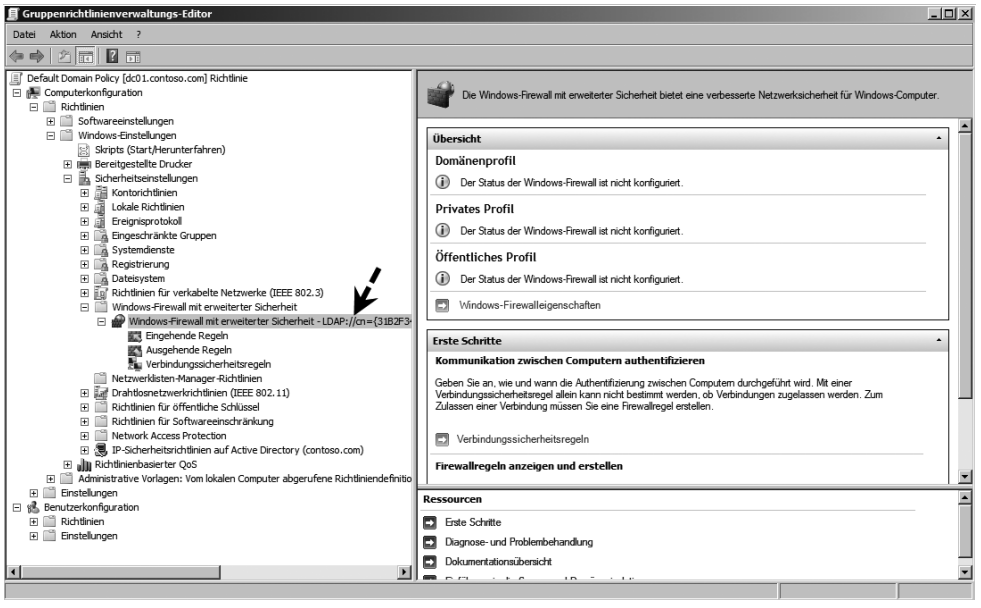
1. Öffnen Sie den Task-Manager per Klick mit der rechten Maustaste auf die Taskleiste und Auswahl des Befehls *Task-Manager* im Kontextmenü.
2. Klicken Sie auf die Registerkarte *Prozesse*.
3. Klicken Sie mit der rechten Maustaste auf eine Instanz von *svchost.exe*, und klicken Sie im zugehörigen Kontextmenü auf *Zu Dienst(en) wechseln* (Abbildung 9.7). Die dem betreffenden Prozess zugeordneten Dienste werden auf der Registerkarte *Dienste* hervorgehoben.

Abbildg. 9.7 Anzeigen der Dienste, die mit *svchost.exe* gestartet wurden



Neue Einstellungen in Gruppenrichtlinien werden nicht erst bei Neustart oder einer erneuten Anmeldung weitergegeben, sondern im laufenden Betrieb. Sie können jetzt auch Drucker über Gruppenrichtlinien freigeben und einzelnen Anwendern zuweisen. Durch diese Möglichkeit können Anwendern auch auf Basis deren Standorts (zum Beispiel für mobile Benutzer für jeden Standort) andere Drucker zugewiesen werden. Die Drucker werden dazu einfach in der Gruppenrichtlinie mit ihrem Freigabenamen hinterlegt. Die neue Windows-Firewall kann jetzt ebenfalls innerhalb von Gruppenrichtlinien gesteuert werden. Dabei lässt sich die Firewall nicht nur ein- oder ausschalten, sondern es können auch einzelne Regeln für die Windows-Firewall hinterlegt werden (Abbildung 9.8). Auf diesem Weg sind auch IPSec-Sicherheitsrichtlinien über die Firewallregeln, genauso wie lokal, konfigurierbar.

Abbildg. 9.8 Konfiguration der Windows-Firewall für Windows Vista und Windows Server 2008 über Gruppenrichtlinien



In den Windows-Komponenten der Gruppenrichtlinien sind zahlreiche Einstellungen hinzugekommen. Dadurch können zahlreiche, selbsterklärende Informationen direkt in den Gruppenrichtlinien eingestellt werden. Sie können im Internet Explorer zum Beispiel den Popup-Blocker konfigurieren und alle Einstellungen vornehmen, die bisher nur mit dem IEAK möglich waren. Wenn Clients unter Windows XP den Internet Explorer 7 einsetzen, werden die Einstellungen der Gruppenrichtlinien teilweise auch übernommen. Der Internet Explorer 6 kann über die Gruppenrichtlinien nicht effizient gesteuert werden, hier sollten Sie das entsprechende **.adm*-File verwenden oder das IEAK. Natürlich sind die Funktionen, die im Internet Explorer 6 ähnlich zum Internet Explorer 7 sind, auch über die Gruppenrichtlinien zu steuern.

Standardgruppenrichtlinien

Nach der Erstellung eines Active Directorys gibt es bereits zwei Gruppenrichtlinienobjekte. Diese Richtlinien sollten möglichst nicht verändert werden. Wenn Sie neue Einstellungen vornehmen wollen, sollten Sie möglichst eigene Gruppenrichtlinien definieren und die Einstellungen der Standardrichtlinien so belassen wie sie sind.

- **Default Domain Controllers Policy** Diese GPO ist mit dem Container *Domain Controllers* verknüpft. In dieser Richtlinie werden spezielle Einstellungen vorgegeben, die für Domänencontroller notwendig sind. Aus diesem Grund sollten Sie auch keine Domänencontroller aus dem Container *Domain Controllers* in eine andere OU verschieben.
- **Default Domain Policy** In dieser Richtlinie werden spezielle Einstellungen für die ganze Domäne gesetzt. Diese Richtlinie ist mit dem Domänenobjekt verknüpft und hat daher für alle OUs in der Domäne Gültigkeit.

Gruppenrichtlinien mit der Gruppenrichtlinienverwaltung konfigurieren und verwalten

Nach dem Start verbindet sich die Konsole *Gruppenrichtlinienverwaltung* (Group Policy Management Console, GPMC) automatisch mit der Gesamtstruktur und der Domäne, in der sich der Rechner befindet, auf dem Sie die Software installiert haben.

Konfiguration der GPMC

Nach der Installation sollten Sie zunächst die Gruppenrichtlinienverwaltung (GPMC) an Ihre Bedürfnisse anpassen und die Einstellungen vornehmen, die zur Konfiguration von Gruppenrichtlinien notwendig sind.

Domänen zur GPMC hinzufügen

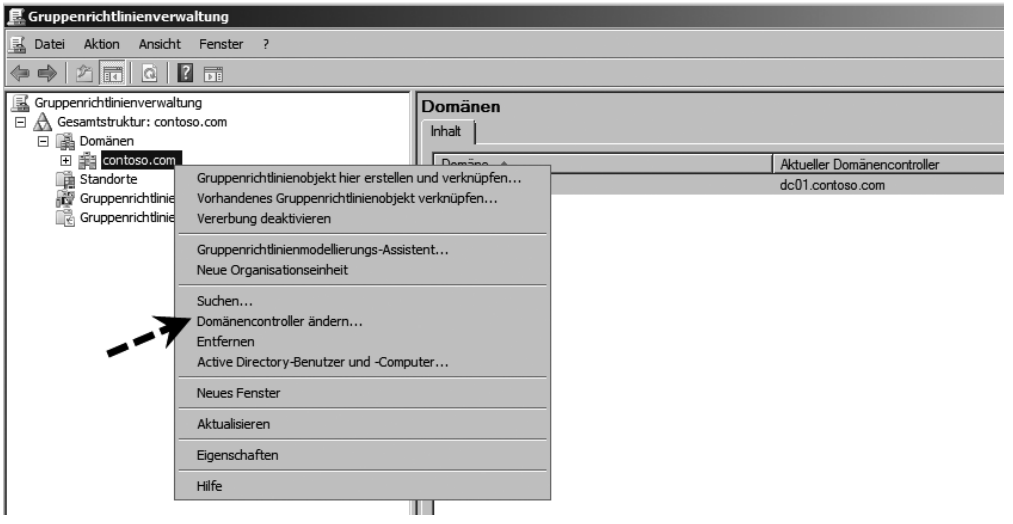
Wenn Sie über genügend Berechtigungen verfügen, können Sie mit einer zentralen GPMC die Gruppenrichtlinien mehrerer Domänen und sogar Gesamtstrukturen verwalten. Standardmäßig werden Sie bereits mit der lokalen Domäne, dem PDC-Emulator dieser Domäne und damit mit Ihrer Gesamtstruktur verbunden. Wenn Sie weitere Domänen Ihrer Gesamtstruktur anzeigen lassen wollen, klicken Sie in der GPMC mit der rechten Maustaste auf den Knoten *Domänen* und wählen Sie im Kontextmenü den Befehl *Domänen anzeigen* aus. Danach können Sie alle Domänen aktivieren, die in Ihrer Gesamtstruktur vorhanden sind.

Abbildg. 9.9 Hinzufügen von zusätzlichen Domänen zur Gruppenrichtlinienverwaltung

Ändern des Domänencontrollers

Standardmäßig verbindet sich die GPMC automatisch mit dem PDC-Emulator der Domäne, da dieser für die Verwaltung der Gruppenrichtlinien zuständig ist. Wollen Sie jedoch einen anderen Domänencontroller auswählen (beispielsweise weil der Zugriff auf den PDC-Emulator zum Beispiel zu langsam ist, wenn Sie in einer Niederlassung Gruppenrichtlinien verwalten), klicken Sie in der GPMC mit der rechten Maustaste auf die Domäne und wählen im Kontextmenü die Option *Domänencontroller ändern* (Abbildung 9.10).

Abbildg. 9.10 Verbinden mit einem anderen Domänencontroller als dem PDC-Emulator



Innerhalb der GPMC werden alle Organisationseinheiten angezeigt, die es auch in Ihrem Active Directory gibt. Unterhalb jeder Organisationseinheit werden die Gruppenrichtlinien angezeigt, die mit der OU verknüpft wurden.

Neue Gruppenrichtlinie – Internet Explorer-Einstellungen verteilen

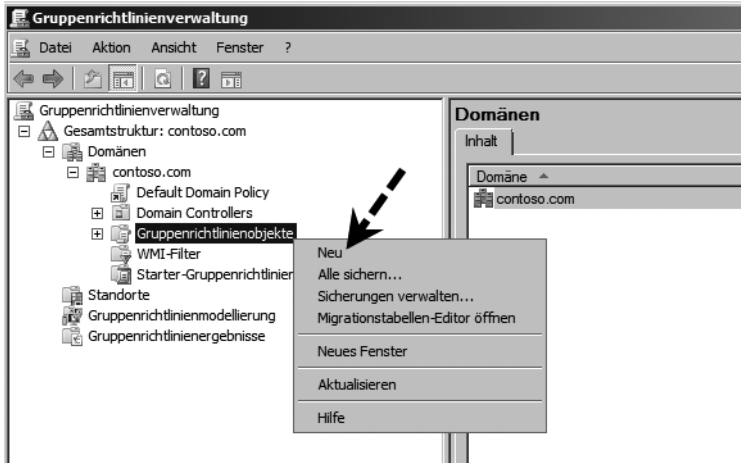
In den folgenden Abschnitten zeigen wir Ihnen die typischen Aufgaben, die in der GPMC durchgeführt werden, an Hand praktischer Beispiele. Um Einstellungen per Gruppenrichtlinie an die PCs, Server oder Benutzerkonten in Ihrem Netzwerk weiterzugeben, ist es am besten, immer nach der gleichen Vorgehensweise zu verfahren:

1. Planen der Einstellungen für die Richtlinie
2. Festlegen der OUs, auf die die Richtlinie angewendet werden soll
3. Erstellen des GPOs
4. Konfiguration der Einstellungen des GPOs
5. Verlinken (verknüpfen) des GPOs mit den gewünschten OUs
6. Testen der Einstellungen
7. Fehlerbehebung, wenn etwas nicht funktioniert

Erstellen eines neuen GPOs

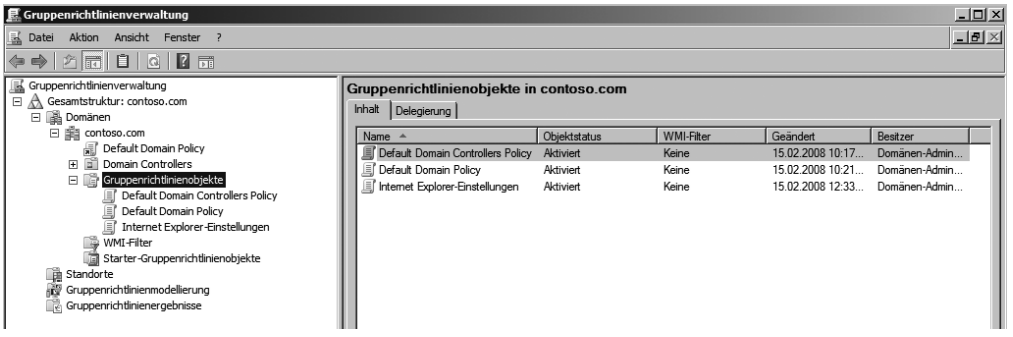
Die erste Aufgabe bei der automatischen Weitergabe einer Einstellung durch eine Gruppenrichtlinie besteht darin, das GPO zu planen und die Organisationseinheiten festzulegen. Nach Abschluss der Planung erfolgt die Erstellung und die Verknüpfung des GPOs mit Organisationseinheiten oder der ganzen Domäne. Um ein neues GPO zu erstellen, klicken Sie in der GPMC auf den Knoten *Gruppenrichtlinienobjekte* und wählen im Kontextmenü den Befehl *Neu* aus. Geben Sie danach dem GPO einen passenden Namen, der wiedergibt, welche Einstellungen mit diesem GPO verteilt werden. In diesem Beispiel erläutern wir Ihnen die Verteilung der Internet Explorer-Einstellungen und die Anpassungen an einen ISA-Server.

Abbildg. 9.11 Erstellen einer neuen Gruppenrichtlinie



Geben Sie daher am besten dem GPO die Bezeichnung *Internet Explorer-Einstellungen* oder einen ähnlichen Namen. Das GPO wird dann unter dem Menüpunkt *Gruppenrichtlinienobjekte* angezeigt. Hier finden Sie in der GPMC alle GPOs, die Sie erstellt haben (Abbildung 9.12). Auch wenn Sie Einstellungen im GPO vornehmen, werden diese erst dann angewendet, wenn Sie das GPO mit einer oder mehreren OUs verknüpfen. Neu in Windows Server 2008 sind an dieser Stelle auch die *Starter-Gruppenrichtlinienobjekte*, die als eine Art Vorlage dienen können. Wird eine neue Richtlinie erstellt, kann eine Starter-Richtlinie ausgewählt werden und deren schon vorhandene Einstellungen in die neue Richtlinie übernommen werden. Für die Erstellung in diesem Workshop benötigen Sie zunächst keine Starter-Gruppenrichtlinie.

Abbildg. 9.12 Anzeigen der GPOs einer Domäne in der GPMC



Bearbeiten der Gruppenrichtlinie – Anbindung der Arbeitsstationen an den ISA-Server

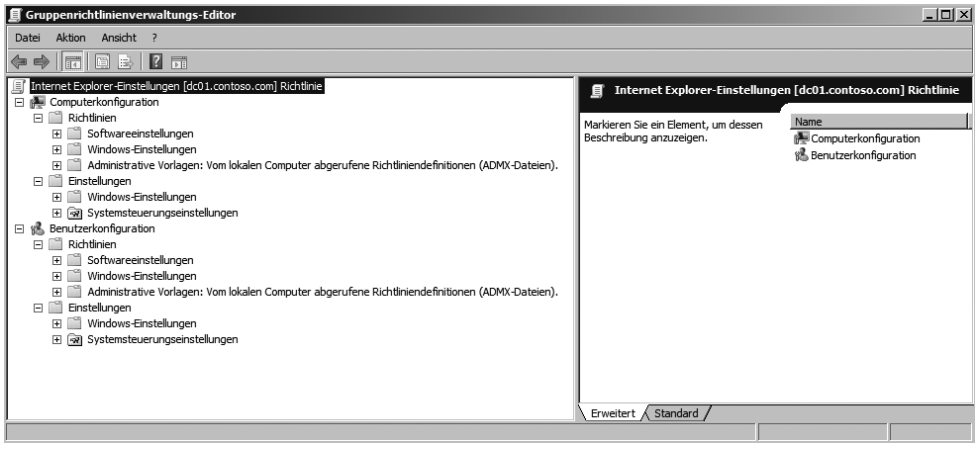
Nach der Erstellung des Gruppenrichtlinienobjekts (GPO) ist dieses in der Domäne vorhanden. Allerdings werden keine Einstellungen weitergegeben, da das GPO noch nicht verknüpft ist und keinerlei Einstellungen enthält. Der nächste Schritt besteht daher darin, die Gruppenrichtlinie zu bearbeiten und die Einstellungen vorzunehmen, die Sie an die Arbeitsstationen verteilen wollen. In diesem Beispiel zeigen wir Ihnen die notwendigen Einstellungen dafür, dass automatisch auf allen Rechnern im Netzwerk der Proxyserver eingetragen wird und weitere Einstellungen im Internet Explorer vorgenommen werden. Klicken Sie im Menü *Gruppenrichtlinienobjekte* mit der rechten Maustaste auf das neu erstellte GPO und wählen Sie im Kontextmenü die Option *Bearbeiten* aus. Damit öffnet sich der Gruppenrichtlinienverwaltungs-Editor, mit dessen Hilfe Sie die Einstellungen innerhalb des GPOs vornehmen, die automatisch verteilt werden sollen. Der Gruppenrichtlinienverwaltungs-Editor besteht aus zwei Hälften. Auf der linken Seite können Sie auswählen, für welchen Bereich Sie Einstellungen vornehmen wollen (Abbildung 9.13). Gruppenrichtlinieneinstellungen werden über den Knoten *Richtlinien* vorgenommen.

- Die Einstellungen unter *Computerkonfiguration* werden auf PCs angewendet, wenn diese gestartet werden.
- Die Einstellungen unter *Benutzerkonfiguration* werden auf die Profile der einzelnen Anwender angewendet, wenn sich diese beim PC anmelden.

Die Einstellungen sind jeweils in drei weitere Knoten unterteilt:

- **Softwareeinstellungen** Über diesen Knoten können Sie Applikationen automatisch verteilen lassen. Zu diesem Punkt kommen wir am Ende dieses Kapitels zurück.
- **Windows-Einstellungen** In diesem Knoten befinden sich die meisten Einstellungen, die Sie vornehmen können, und zwar hauptsächlich Skripts, die durch diese Gruppenrichtlinien beim Starten eines PCs oder Anmelden eines Anwenders ausgeführt werden, und die Sicherheitseinstellungen.
- **Administrative Vorlagen** Hier finden sich einige Möglichkeiten zur Einstellung und Automatisierung von Windows. Sie können Einstellungen im Windows-Explorer, dem Desktop und vielen anderen Funktionen in Windows vornehmen.

Abbildg. 9.13 Aufbau des Gruppenrichtlinien-Editors



Wenn Sie sich durch die Knoten auf der linken Seite klicken, werden auf der rechten Seite die Einstellungen angezeigt, die in diesem Bereich verfügbar sind. Öffnen Sie die Einstellungen einer Gruppenrichtlinie per Doppelklick, können Sie Konfigurationen vornehmen, die an die Benutzer bei der Benutzerkonfiguration oder die PCs bei der Computerkonfiguration weitergegeben werden. Die Bearbeitung dieser Einstellungen läuft dabei fast immer identisch ab. Auf der Registerkarte *Einstellung* können Sie entweder direkt Einstellungen weitergeben oder die Einstellung lediglich aktivieren bzw. deaktivieren, wenn keine weiteren Eingaben vorgegeben werden müssen. Eine Einstellung kann drei verschiedene Zustände annehmen:

- **Nicht konfiguriert** Bei dieser Einstellung wird an dem Zielobjekt in der Registry keine Änderung vorgenommen. Alles bleibt so, wie es auf dem PC eingestellt ist.
- **Aktiviert** Bei dieser Einstellung wird die Konfiguration auf das Zielobjekt angewendet und weitergegeben.
- **Deaktiviert** Bei dieser Einstellung wird die Konfiguration der Gruppenrichtlinie auf dem PC auf den Standard zurückgesetzt. Wenn in einer übergeordneten Gruppenrichtlinie die Einstellung aktiviert wurde, wird sie durch diese Einstellung wieder deaktiviert. Das gilt auch, wenn die entsprechende Einstellung in den lokalen Richtlinien geändert wurde.

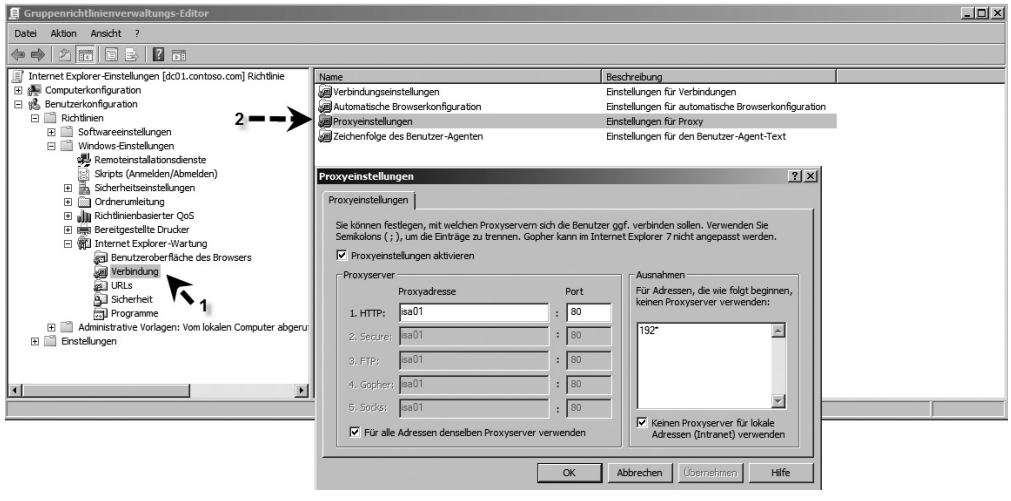
Auf der Registerkarte *Erklärung* finden Sie eine ausführliche Hilfe zu der Einstellung und ihren Auswirkungen. Bevor Sie eine Einstellung aktivieren, sollten Sie sich möglichst immer die Erklärung genau durchlesen.

Konfiguration der Proxyeinstellungen

Eine der vielen möglichen Einstellungen einer Gruppenrichtlinie ist die automatische Konfiguration der Proxyanbindung der Rechner in der Domäne. Sie finden diese Einstellung in der Konsolenstruktur unter *Benutzerkonfiguration/Windows-Einstellungen/Internet Explorer-Wartung/Verbindung*. Klicken Sie diesen Eintrag an, können Sie auf der rechten Seite wichtige Einstellungen vornehmen, um die Clients zu konfigurieren. Öffnen Sie die Einstellungen für die Option *Proxyeinstellungen* (Abbildung 9.14). In diesem Dialogfeld können Sie einstellen, welchen Proxyserver die PCs und Server im Netzwerk verwenden sollen. Durch die automatische Weitergabe dieser Einstellungen ist keine manuelle Konfiguration mehr nötig. Tragen Sie als Proxyadresse entweder den Netzwerknamen des

ISA-Servers oder seine interne IP-Adresse ein. Konfigurieren Sie den Port, unter dem der ISA-Server auf Anfragen antwortet. Standardmäßig hört der ISA-Server auf den Port 8080. Damit die Einstellungen auf alle Protokolle angewendet werden, deaktivieren Sie die Einstellung *Für alle Adressen denselben Proxyserver verwenden* und aktivieren Sie die Einstellung gleich wieder. Tragen Sie im Feld *Ausnahmen* alle Webserver ein, zum Beispiel die Intranetserver, die durch den Internet Explorer direkt angesprochen werden sollen und die nicht an den ISA-Server geschickt werden. Sie können an dieser Stelle mit dem Platzhalter * arbeiten. Die verschiedenen Einträge werden durch das Semikolon (;) getrennt. Wenn Sie die Einstellungen vorgenommen haben, können Sie diese mit *OK* bestätigen.

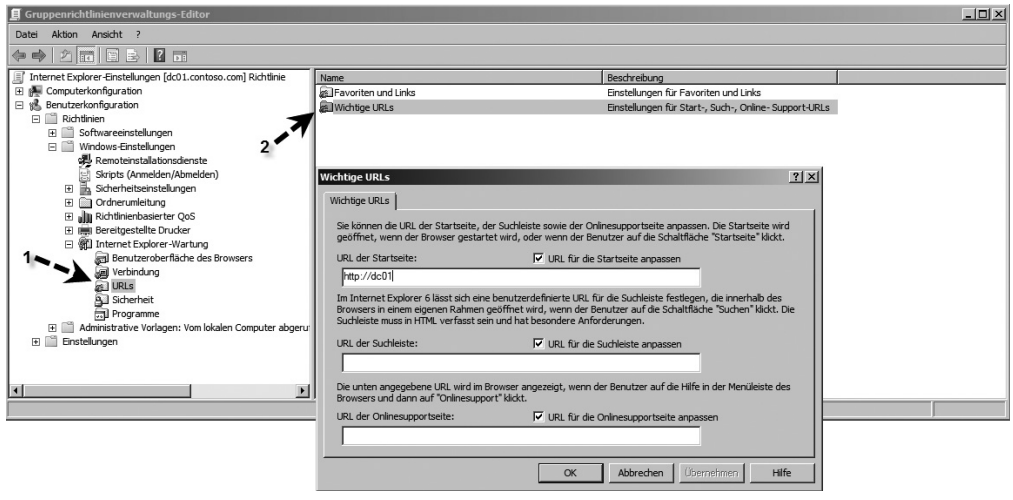
Abbildg. 9.14 Konfigurieren der Proxyeinstellungen über Gruppenrichtlinien



Konfiguration der Startseite und der Favoriten

Eine weitere wichtige Einstellung ist die automatische Konfiguration der Startseite und unter Umständen der Suchseite des Internet Explorers. Diese Einstellung finden Sie in der Konsolenstruktur unter *Benutzerkonfiguration/Windows-Einstellungen/Internet Explorer-Wartung/URLs/Wichtige URLs*. Hier können Sie die Startseite und die automatische Suchseite konfigurieren. So können Sie zum Beispiel konfigurieren, dass nach dem Start des Webbrowsers automatisch die SharePoint-Seite des Servers geöffnet wird. Sie müssen bei den Adressen die vollständige Adresse hinterlegen, also auch das *http://*. Mit Hilfe der Richtlinie *Favoriten und Links* können Sie allen PCs im Netzwerk automatisch verschiedene Favoriten zuweisen, von denen Sie der Meinung sind, dass jeder Benutzer sie braucht. Alternativ wären hier die Pflege der Startseite einer bestimmten Seite im Intranet und die wichtigsten Links Ihrer Firma im Intranet abzulegen.

Abbildg. 9.15 Konfigurieren der Startseite des Internet Explorers über Gruppenrichtlinien



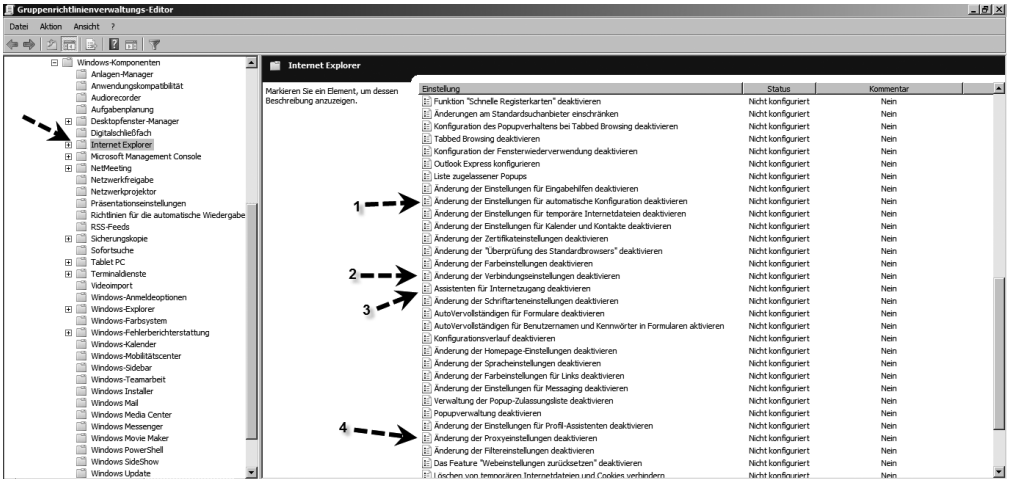
Automatische Verteilung von Sicherheitseinstellungen

Wenn Sie Einstellungen automatisch vorgeben, heißt das noch nicht, dass die Anwender diese Einstellungen nicht verändern können. Wollen Sie die Möglichkeit deaktivieren, Änderungen im Internet Explorer vorzunehmen, erledigen Sie das am besten über den Knoten *Benutzerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Internet Explorer* in der Konsolenstruktur. An dieser Stelle finden Sie dutzende Einstellmöglichkeiten für den Internet Explorer. Wichtig ist hier, die vier folgenden Einstellungen zu aktivieren (Abbildung 9.16):

- Assistenten für Internetzugang deaktivieren
- Änderung der Verbindungseinstellungen deaktivieren
- Änderung der Proxyeinstellungen deaktivieren
- Änderung der Einstellungen für automatische Konfiguration deaktivieren

Setzen Sie die Einstellung einer Gruppenrichtlinie auf *Aktiviert*, bedeutet das die Aktivierung dieser Einstellung. Wenn in dieser Einstellung eine Windows-Funktion deaktiviert wird, wird die Funktion direkt auf dem PC deaktiviert. Durch die Aktivierung einer Einstellung im GPO bewirken Sie also eine Deaktivierung der entsprechenden Funktion in Windows. Die hier beschriebenen Einstellungen sind die am häufigsten verwendeten. Sie können auch noch weitere Einstellungen vornehmen. Achten Sie aber darauf, nicht zu viele Funktionen im Internet Explorer zu deaktivieren, die unter Umständen noch benötigt werden. Wenn Sie alle Einstellungen vorgenommen haben, können Sie den Gruppenrichtlinienverwaltungs-Editor schließen, da die Bearbeitung der Gruppenrichtlinienobjekte an dieser Stelle abgeschlossen ist.

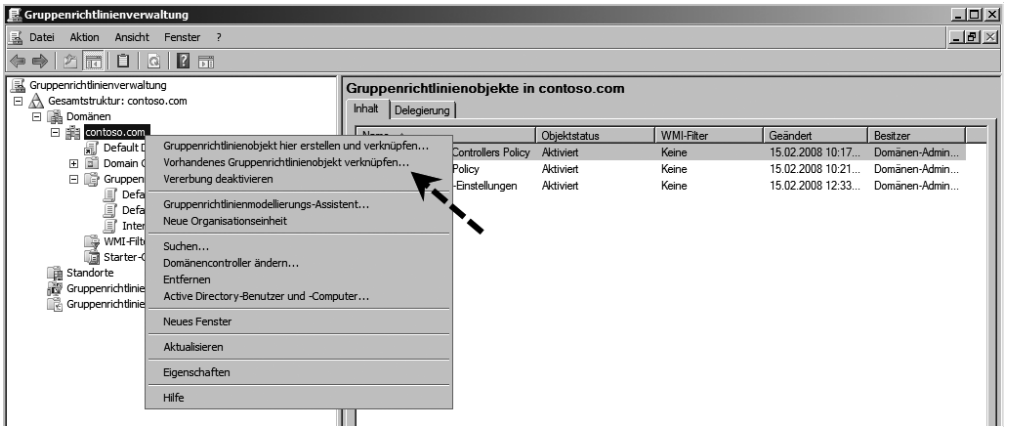
Abbildg. 9.16 Deaktivieren von Einstellungsoptionen im Internet Explorer über Gruppenrichtlinien



Verknüpfen eines GPOs mit einem Container

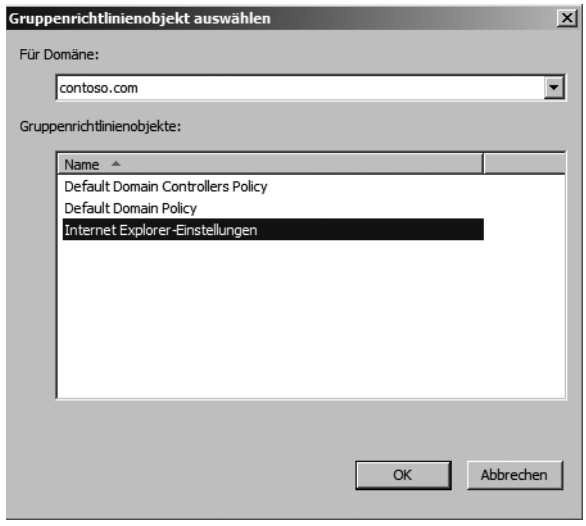
Damit die Einstellungen in der Gruppenrichtlinie angewendet werden, müssen Sie diese mit einer OU oder der ganzen Domäne verknüpfen. Da die Einstellungen des Internet Explorers am besten für alle Objekte in einer Domäne durchgeführt werden, bietet es sich an, diese auch mit der ganzen Domäne zu verknüpfen. Klicken Sie dazu in der Gruppenrichtlinienverwaltung mit der rechten Maustaste entweder auf die OU, mit der Sie dieses GPO verknüpfen wollen, oder auf die Domäne. Wählen Sie aus dem Kontextmenü die Option *Vorhandenes Gruppenrichtlinienobjekt verknüpfen* aus (Abbildung 9.17).

Abbildg. 9.17 Verknüpfen einer GPO mit einem Container im Active Directory



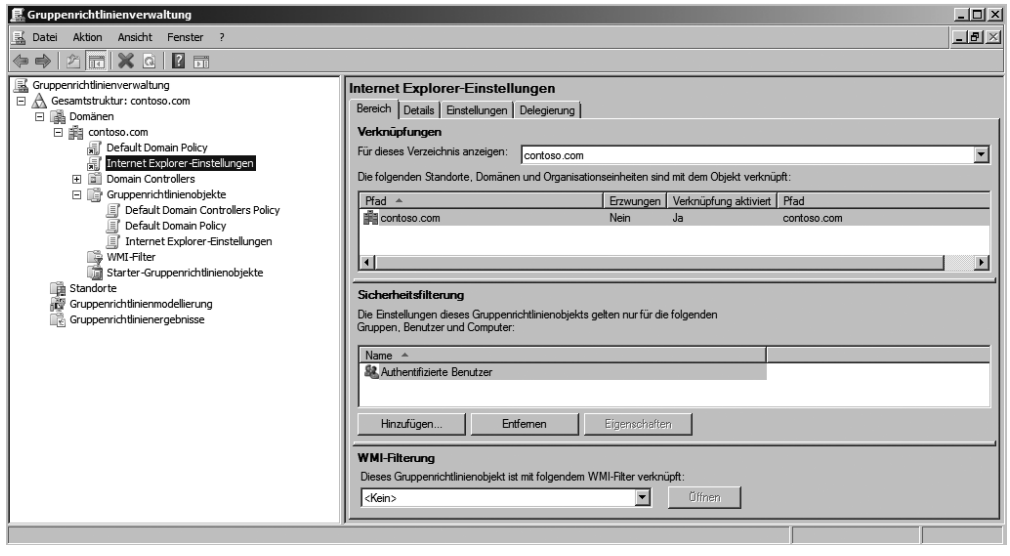
Es öffnet sich ein Fenster, in dem Ihnen alle Gruppenrichtlinien angezeigt werden, die in der Domäne bereits konfiguriert sind. Wählen Sie in dem Fenster das GPO aus und bestätigen Sie mit *OK* (Abbildung 9.18).

Abbildg. 9.18 Auswählen einer erstellten GPO für die Verknüpfung mit einem Container



Nach der erfolgreichen Auswahl wird die Verknüpfung des GPOs unterhalb der Domäne angezeigt. Sie können das GPO auch nur mit einzelnen OUs verknüpfen und so viele OUs verknüpfen, wie Sie wollen. Wenn Sie später eine Änderung an dem GPO vornehmen, wird diese Änderung automatisch an alle verknüpften OUs weitergegeben. In der Gruppenrichtlinienverwaltugn erkennen Sie durch die übersichtliche Baumstruktur unter jedem Container, welche Gruppenrichtlinien verknüpft worden sind und daher angewendet werden (Abbildung 9.19). Ab diesem Moment ist das GPO aktiv, da Einstellungen innerhalb des GPOs vorgenommen wurden und das GPO verknüpft ist. Als Nächstes können Sie testen, ob die Einstellungen auch übernommen wurden.

Abbildg. 9.19 Anzeigen einer verknüpften GPO



Testen der Einstellungen einer GPO

Starten Sie einen PC, der Mitglied der Domäne ist, und melden Sie sich an. Sie sehen bereits beim Starten des Internet Explorers, dass das GPO angewendet wird, da sich bereits die konfigurierte Startseite öffnet. Unter manchen Umständen dauert es ein bisschen, bis eine Gruppenrichtlinie auf alle Domänencontroller repliziert wurde. Starten Sie daher einen manuellen Replikationsvorgang oder warten Sie einige Minuten auf die Replikation. Beim ersten Start eines Internet Explorers wird unter Umständen nicht sofort die Startseite übernommen. Schließen Sie in einem solchen Fall den Internet Explorer wieder und öffnen Sie ihn erneut. Die Einstellungen sollten jetzt übernommen sein. Öffnen Sie im Internet Explorer mit *Extras/Internetoptionen/Verbindungen* die Registerkarte für die Verbindungen zum Internet. Wenn alle Einstellungen übernommen wurden, sollten die einzelnen Schaltflächen deaktiviert sein, die Benutzer können keine Veränderungen vornehmen. Die Bearbeitung und der Test sind damit abgeschlossen.

Gruppenrichtlinien erzwingen und Priorität erhöhen – Kennwortkonfiguration für die Anwender

In diesem Abschnitt erfahren Sie am Beispiel einer weiteren neuen Gruppenrichtlinie, wie Sie das GPO priorisieren und eine Überschreibung durch untergeordnete Richtlinien verhindern können. Eine oft verwendete Gruppenrichtlinie ist die Vorgabe von sicheren Kennwörtern für die Anwender und die Steuerung der Kennwortstruktur. In vielen Unternehmen werden die Server zwar extrem vor Sicherheitsgefahren geschützt, allerdings werden oft die Kennwörter der Benutzer bei der Absicherung übersehen. Anwender verwenden meistens einfache Kennwörter, wie Familiennamen, Namen der Kinder, Tastenfolgen (»qwert«) oder andere einfach zu erratende Kennwörter. Manchmal werden Kennwörter von den Nutzern auch auf Zetteln an den Monitor oder unter die Tastatur geklebt. Windows Server 2008 bietet für die Steuerung der Kennwörter einige Optionen an. Wenn diese Optionen aktiviert sind und Ihre Anwender im Umgang mit Kennwörtern geschult werden, lässt sich die Sicherheitsgefahr von unsicheren Kennwörtern relativ schnell beheben. Damit Gruppenrichtlinien für Kennwörter funktionieren, musste die entsprechend hinterlegte Gruppenrichtlinie unter Windows Server 2003 immer mit der kompletten Domäne verknüpft werden, nicht mit einzelnen Organisationseinheiten. Dieser Sachverhalt wurde in Windows Server 2008 behoben, wie wir Ihnen bereits zu Beginn des Kapitels gezeigt haben. Dennoch bietet es sich aus Übersichtlichkeitsgründen an, am besten nur eine einzelne Gruppenrichtlinie für Kennwörter zu erstellen und diese direkt mit der Domäne zu verbinden. Wenn Sie eine Gruppenrichtlinie für die Steuerung von Kennwörtern mit einer einzelnen OU verknüpfen, wird diese unter Windows Server 2003 nicht angewendet, unter Windows Server 2008 allerdings schon. Eine Active Directory-Domäne kann unter Windows Server 2003 immer nur eine Kennwortrichtlinie verwenden. Auch bei Windows Server 2008 sollten mehrere Richtlinien nur in Ausnahmen konfiguriert werden. Am besten erstellen Sie für die Kennwortrichtlinie eine neue Richtlinie und verknüpfen diese direkt mit der Domäne. Die *Default Domain Policy* sollten Sie möglichst nicht verändern.

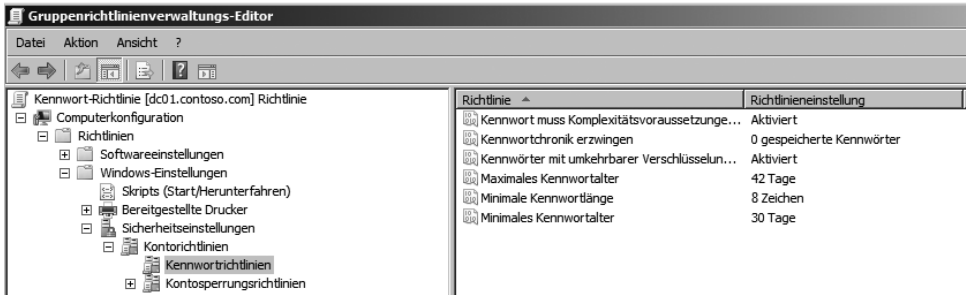
Erstellen einer neuen Gruppenrichtlinie für sichere Kennwörter

Um eine neue Gruppenrichtlinie für sichere Kennwörter zu erstellen, sollten Sie zunächst die Konsole *Gruppenrichtlinienverwaltung* (GPMC) aktivieren.

1. Erstellen Sie, wie bereits zuvor beschrieben, in der Konsolenstruktur unter dem Knoten *Gruppenrichtlinienobjekte* ein neues GPO und geben Sie diesem die Bezeichnung *Kennwort-Richtlinie*.
2. Klicken Sie dann mit der rechten Maustaste auf den Eintrag *Kennwort-Richtlinie* und wählen Sie im Kontextmenü die Option *Bearbeiten* aus.
3. Navigieren Sie zu den Einstellungen der Kennwörter unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Kontorichtlinien/Kennwortrichtlinien* (Abbildung 9.20).
4. Geben Sie für diese Einstellungen jeweils die Option *Diese Richtlinieneinstellung definieren* und die empfohlenen Werte für sichere Kennwörter ein. In Windows Server 2008 gibt es sechs Einstellungen, die Sie zur Konfiguration von sicheren Kennwörtern verwenden können:

- **Kennwort muss Komplexitätsvoraussetzungen entsprechen** Bei dieser Option muss das Kennwort mindestens sechs Zeichen lang sein. Microsoft empfiehlt, diese Einstellung zu aktivieren. Wenn Sie die Komplexitätsvoraussetzungen für Kennwörter aktivieren, sollten Sie vorher am besten eine E-Mail an alle Mitarbeiter schicken und diese darüber informieren, wie zukünftig die Kennwörter aufgebaut werden sollen. Dieser Hinweis kann im Intranet hinterlegt werden. Das Kennwort darf maximal zwei Zeichen enthalten, die auch in der Zeichenfolge des Benutzernamens vorkommen. Außerdem müssen drei der fünf Kriterien von komplexen Kennwörtern erfüllt sein:
  - Großbuchstaben (A bis Z)
  - Kleingeschriebene Buchstaben (a bis z)
  - Ziffern (0 bis 9)
  - Sonderzeichen (zum Beispiel !, &, /, %)
  - Unicodezeichen (_, @, ®)
- **Kennwortchronik erzwingen** Hier können Sie festlegen, wie viele Kennwörter im Active Directory gespeichert werden sollen, die bisher bereits durch einen Anwender verwendet wurden. Wenn Sie diese Option wie empfohlen auf 24 setzen, darf sich ein Kennwort erst nach 24 Änderungen wiederholen.
- **Kennwörter mit umkehrbarer Verschlüsselung speichern** Bei dieser Option werden die Kennwörter so gespeichert, dass die Administratoren sie auslesen können. Diese Option sollte nur verwendet werden, wenn bestimmte Applikationen für Single Sign-On das benötigen. Ansonsten sollten Sie diese Option deaktivieren. Dazu müssen Sie die Richtlinieneinstellung definieren und diese auf *Deaktiviert* setzen.
- **Maximales Kennwortalter** Hier legen Sie fest, wie lange ein Kennwort gültig bleibt, bis der Anwender es selbst ändern muss. Microsoft empfiehlt, Kennwörter für 42 Tage zu verwenden und erst danach eine Änderung durchzuführen.
- **Minimale Kennwortlänge** Hier wird festgelegt, wie viele Zeichen ein Kennwort mindestens enthalten muss. Dafür wird ein Wert von acht Zeichen empfohlen.
- **Minimales Kennwortalter** Hier wird festgelegt, wann ein Kennwort frühestens geändert werden darf, also wie lange es mindestens aktuell sein muss. Diese Option ist zusammen mit der Kennwortchronik sinnvoll, damit die Anwender das Kennwort nicht so oft ändern, dass sie wieder ihr altes verwenden können. Microsoft empfiehlt an dieser Stelle einen Wert von 2.

Abbildg. 9.20 Konfigurieren einer Kennwortrichtlinie für sichere Kennwörter

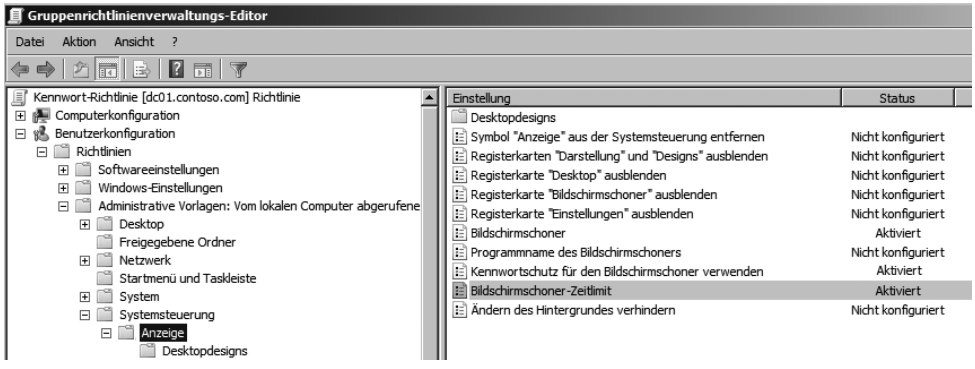


Aktivieren von Bildschirmschonern mit Kennwortschutz

Sie sollten auch die Einstellung aktivieren, dass nach gewisser Zeit der Bildschirmschoner aktiviert wird und Anwender ein Kennwort eingeben müssen, wenn der Bildschirm entsperrt werden soll. Das ist vor allem dann sinnvoll, wenn Anwender ihren Platz verlassen. Wenn der Bildschirm nicht gesperrt wird, können ungehindert andere Anwender unter dem Namen des angemeldeten Benutzers Aktionen durchführen. Sie finden die Einstellungen für Bildschirmschoner unter *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Systemsteuerung/Anzeige* (Abbildung 9.21). Konfigurieren Sie die folgenden Einstellungen:

- *Bildschirmschoner* auf *Aktiviert*
- *Kennwortschutz für den Bildschirmschoner verwenden* auch auf *Aktiviert*
- *Bildschirmschoner-Zeitlimit* auf *Aktiviert* und als Einstellung *600* Sekunden bis zur Aktivierung

Abbildg. 9.21 Konfigurieren des Bildschirmschoners über Gruppenrichtlinien

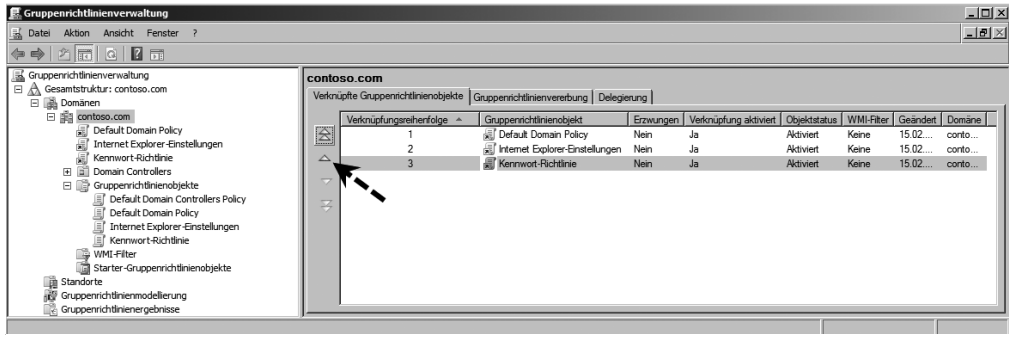


Wenn Sie Eintragungen vorgenommen haben, können Sie den Gruppenrichtlinienverwaltungs-Editor wieder schließen. Verknüpfen Sie die erstellte Richtlinie wieder mit der Domäne und gehen Sie dabei genauso vor, wie bei der Verknüpfung der Internet Explorer-Einstellungen.

Priorisierung einer Gruppenrichtlinienverknüpfung anpassen

Wenn Sie die Richtlinie erstellt und verknüpft haben, klicken Sie die Domäne in der Gruppenrichtlinienverwaltung an. Auf der rechten Seite werden Ihnen alle Gruppenrichtlinien angezeigt, die direkt mit der Domäne verknüpft sind. Die neu erstellte Kennwort-Richtlinie sollte die erste Verknüpfung sein, die angewendet wird, da sie ansonsten übergangen wird. Markieren Sie die Verknüpfung der Kennwort-Richtlinie auf der rechten Seite der Gruppenrichtlinienverwaltung und klicken Sie auf die Pfeile, bis die Verknüpfung ganz oben angeordnet ist (Abbildung 9.22). Dadurch ist sichergestellt, dass diese Verknüpfung und die Einstellungen des verknüpften GPOs zuerst angewendet werden.

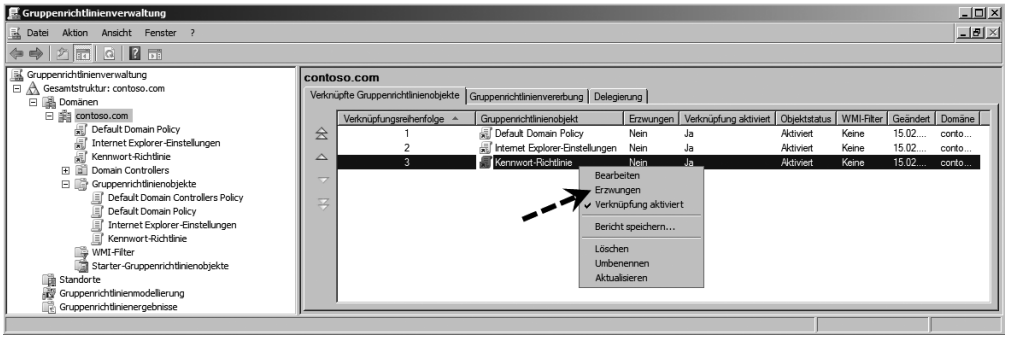
Abbildg. 9.22 Änderung der Priorisierung einer Gruppenrichtlinie



Erzwingen einer Richtlinie

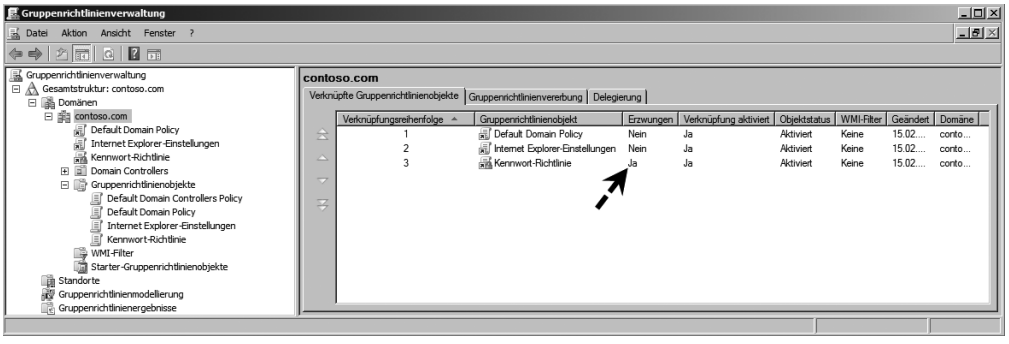
Durch die Vererbung von Gruppenrichtlinien besteht die Möglichkeit, dass die Einstellung einer Gruppenrichtlinie durch eine andere Gruppenrichtlinie, die in einer untergeordneten OU definiert ist, überschrieben wird. Wenn Sie zum Beispiel eine Richtlinie, in der die Komplexität der Kennwörter mitgegeben wird, mit der ganzen Domäne verknüpfen, dann wird diese Einstellung an alle Organisationseinheiten und die darin enthaltenen Benutzer weitergegeben. Ist jetzt aber mit einer untergeordneten Organisationseinheit eine weitere Gruppenrichtlinie verknüpft, die in der Anwendungsreihenfolge nach der Richtlinie für die Domäne angewendet wird, besteht die Möglichkeit, dass die Einstellungen der vererbten Richtlinie der Domäne überschrieben werden. Für Benutzer innerhalb eines Containers gilt immer die zuletzt angewendete Richtlinie. Wenn also in der Domänenrichtlinie eine Einstellung gesetzt wird, die in der OU des Benutzers zurückgenommen wird, dann gilt das auch für den Benutzer. Wenn Domänenadministratoren sicherstellen wollen, dass gewisse Gruppenrichtlinien nicht überschrieben werden können, besteht die Möglichkeit, die Einstellungen dieser Richtlinie zu erzwingen. In diesem Fall kann von untergeordneten Organisationseinheiten die Durchsetzung dieser Gruppenrichtlinie nicht verhindert werden. Sie können eine Gruppenrichtlinie erzwingen lassen, indem Sie auf der rechten Seite der Gruppenrichtlinienverwaltung auf der Registerkarte *Verknüpfte Gruppenrichtlinienobjekte* die Verknüpfung mit der rechten Maustaste anklicken. Wählen Sie im daraufhin geöffneten Kontextmenü die Option *Erzwungen* aus (Abbildung 9.23).

Abbildg. 9.23 Erzwingen einer Gruppenrichtlinie in der Gruppenrichtlinienverwaltung



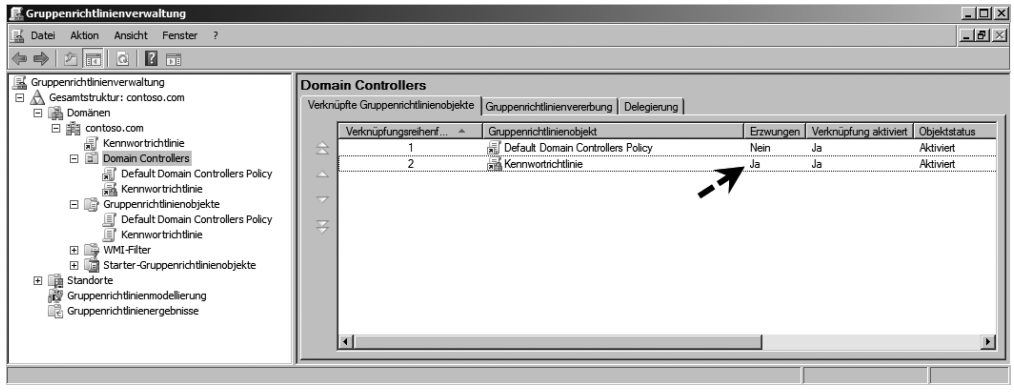
Nach der Auswahl erscheint eine Meldung, in der Sie das *Erzwingen* der Richtlinie bestätigen müssen. Nach der Bestätigung wird die Richtlinie als *Erzwungen* angezeigt (Abbildung 9.24).

Abbildg. 9.24 Erzwingen einer Gruppenrichtlinie in der GPMC anzeigen



Dadurch stellen Sie sicher, dass diese Einstellungen für alle Benutzer der Domäne Gültigkeit haben und in keiner OU aufgehoben werden können. Wenn Sie anschließend in der GPMC eine untergeordnete OU aktivieren, sehen Sie auf der rechten Seite auf der Registerkarte *Gruppenrichtlinienvererbung*, dass die Richtlinie auch hier als *Erzwungen* angezeigt wird (Abbildung 9.25). Das heißt, die Anwendung dieser Richtlinie kann nicht verhindert werden.

Abbildg. 9.25 Anzeige von erzwungenen Richtlinien in der Gruppenrichtlinienvererbung



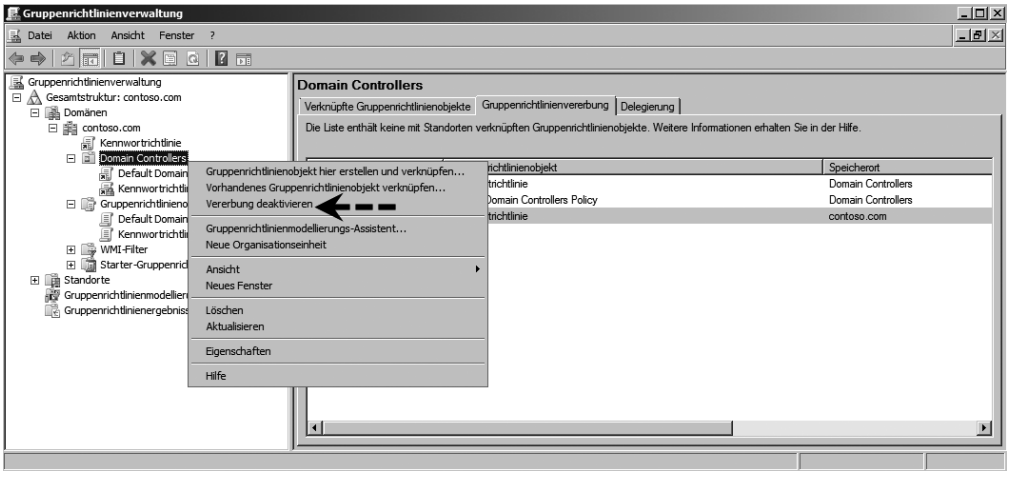
Testen der Gruppenrichtlinie

Im Anschluss daran können Sie die Gruppenrichtlinie auf einer Windows-Arbeitsstation mit *gpupdate /force* in der Befehlszeile übertragen. Alternativ können Sie auch die Arbeitsstation neu starten. Wenn Sie die Einstellungen korrekt vorgenommen haben, können Sie in den Eigenschaften des Bildschirmschoners feststellen, dass der Benutzer zwar aussuchen darf, welchen Bildschirmschoner er verwendet, aber die Optionen *Wartezeit* und *Kennworteingabe bei Reaktivierung* aktiviert sind und durch den Benutzer nicht geändert werden dürfen. Sie können auch den Bildschirmschoner in der Gruppenrichtlinie einstellen, dann dürfen die Anwender auch diesen nicht mehr verändern.

Vererbung für Gruppenrichtlinien deaktivieren

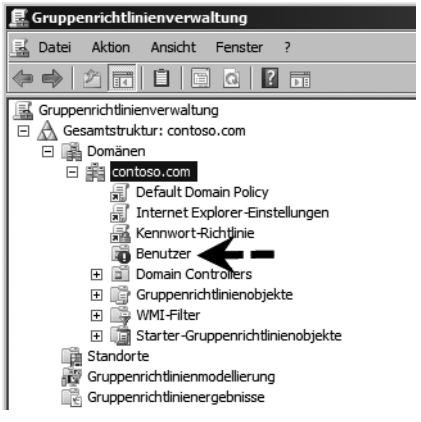
Für manche Gruppenrichtlinien ist es unter Umständen sinnvoll, die standardmäßige Vererbung zu deaktivieren. Wenn Sie zum Beispiel in allen OUs einer Domäne die Internet Explorer-Einstellungen wie beschrieben weitergeben wollen, in einer OU aber nicht, dann können Sie in dieser OU die Verwendung der Richtlinie deaktivieren, auch wenn diese mit der ganzen Domäne verknüpft ist. Haben Sie zum Beispiel einige Mitarbeiter, die einen eigenen Proxyserver verwenden, zum Beispiel die Entwicklungsabteilung oder die IT-Abteilung, können Sie eine eigene Gruppenrichtlinie für diese OU erstellen und sie mit dieser OU verknüpfen. Die Vererbung der übergeordneten Richtlinie können Sie für diese OU deaktivieren. Wenn Sie die entsprechende OU in der Gruppenrichtlinienverwaltung anklicken, können Sie auf der rechten Seite der Konsole auf der Registerkarte *Gruppenrichtlinienvererbung* erkennen, welche Verknüpfungen von übergeordneten OUs auf diese OU übernommen – also vererbt – werden (Abbildung 9.26). Sie können allerdings nicht die Vererbung einzelner Gruppenrichtlinien deaktivieren, sondern nur die Vererbung als Ganzes. Klicken Sie dazu in der Gruppenrichtlinienverwaltung mit der rechten Maustaste auf die OU, für die Sie die Vererbung deaktivieren wollen, und wählen Sie im Kontextmenü den Befehl *Vererbung deaktivieren* aus.

Abbildg. 9.26 Vererbung für eine OU deaktivieren



Nachdem Sie die Vererbung von Gruppenrichtlinien für eine OU deaktiviert haben, wird diese OU in der Gruppenrichtlinienverwaltung mit einem blauen Kreis und einem weißen Ausrufezeichen angezeigt (Abbildung 9.27). Auf die gleiche Weise können Sie die Vererbung auch wieder aktivieren. Auf der Registerkarte *Gruppenrichtlinienvererbung* werden jetzt nur noch die Gruppenrichtlinien angezeigt, die erzwungen werden.

Abbildg. 9.27 Anzeigen von OUs mit deaktivierter Vererbung für Gruppenrichtlinien



HINWEIS Erzwungene Gruppenrichtlinien lassen sich auch durch die Deaktivierung der Vererbung nicht deaktivieren.

Datensicherung von Gruppenrichtlinien

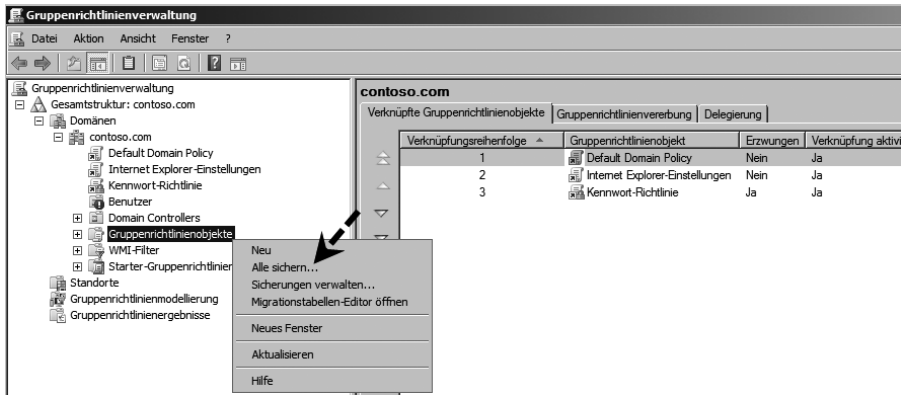
Beim Einsatz von Gruppenrichtlinien sollten diese in regelmäßigen Abständen gesichert werden. Zu einer richtigen Backup-Strategie gehört in einem Unternehmen auch die Sicherung der Gruppenrichtlinien, nachdem diese geändert wurden. Vor allem beim Einsatz vieler Richtlinien sollten Sie bei Änderungen ein Backup der Richtlinie im Netzwerk ablegen und unter Umständen auch mit der Bandsicherung sichern. Sichern Sie am besten die Gruppenrichtlinie immer in ein spezielles Verzeichnis auf der lokalen Festplatte und kopieren Sie danach dieses Verzeichnis auf einen Datenträger im Netzwerk, damit auch bei Ausfall einer lokalen Festplatte die Sicherung noch zur Verfügung steht. Mit der Gruppenrichtlinienverwaltung (GPMC) können Sie einzelne Gruppenrichtlinien sichern und wiederherstellen, ohne eine Datensicherung von Active Directory verwenden zu müssen. Da die Datensicherung von Gruppenrichtlinien in Dateien gespeichert wird, können Sie die Sicherung auch zum Erstellen neuer Gruppenrichtlinien verwenden, indem Sie gesicherte Gruppenrichtlinien in neu erstellte importieren.

Sicherung von Gruppenrichtlinien in der GPMC

Um eine Datensicherung einzelner oder aller Gruppenrichtlinien durchzuführen, klicken Sie in der GPMC auf den Knoten *Gruppenrichtlinienobjekte*. Dieser Knoten enthält alle Gruppenrichtlinien, die in dieser Domäne erstellt wurden. Klicken Sie mit der rechten Maustaste auf eine Gruppenrichtlinie und wählen Sie im Kontextmenü den Befehl *Sichern* aus. Bei der Sicherung von Gruppenrichtlinien werden die Einstellungen in eine Datei exportiert. Diese Datei kann zur Wiederherstellung importiert werden. Sie können auch direkt auf den Knoten *Gruppenrichtlinienobjekte* klicken und im Kontextmenü den Befehl *Alle sichern* auswählen, um sämtliche Gruppenrichtlinien einer Domäne auf einmal zu sichern (Abbildung 9.28). Bei der Sicherung eines GPOs werden folgende Informationen gesichert:

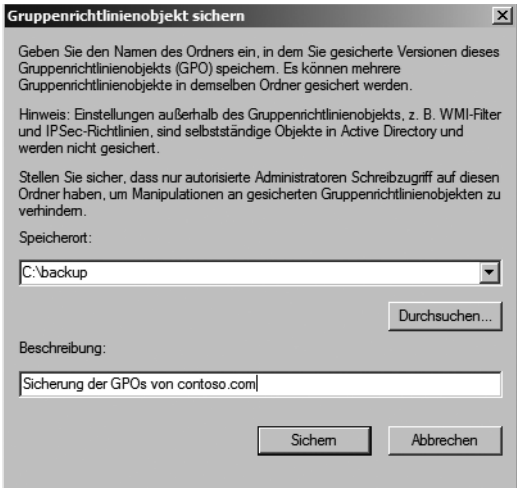
- Einstellungen des GPOs als XML-Datei
- Der Globally Unique Identifier (GUID) des GPOs
- Die Berechtigungen des GPOs
- WMI-Filter und deren Verlinkung
- Zeitstempel der Datensicherung
- Benutzerdefinierte Information zum gesicherten GPO

Abbildg. 9.28 Starten der Datensicherung von Gruppenrichtlinien



Danach erscheint ein Fenster, in dem Sie ein Verzeichnis auf der Festplatte auswählen und eine Beschreibung der Sicherung hinterlegen können. Wenn Sie die Eingaben bestätigen, beginnt der Sicherungsassistent mit der Datensicherung der Gruppenrichtlinie und speichert diese im ausgewählten Verzeichnis der Festplatte (Abbildung 9.29).

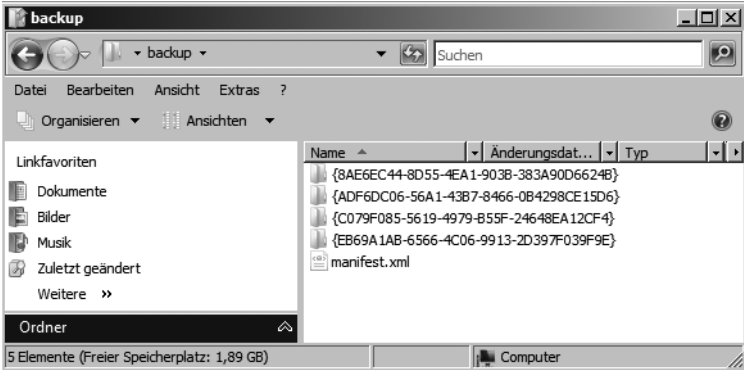
Abbildg. 9.29 Durchführung der Datensicherung für Gruppenrichtlinien



Verwalten der Datensicherung von Gruppenrichtlinien

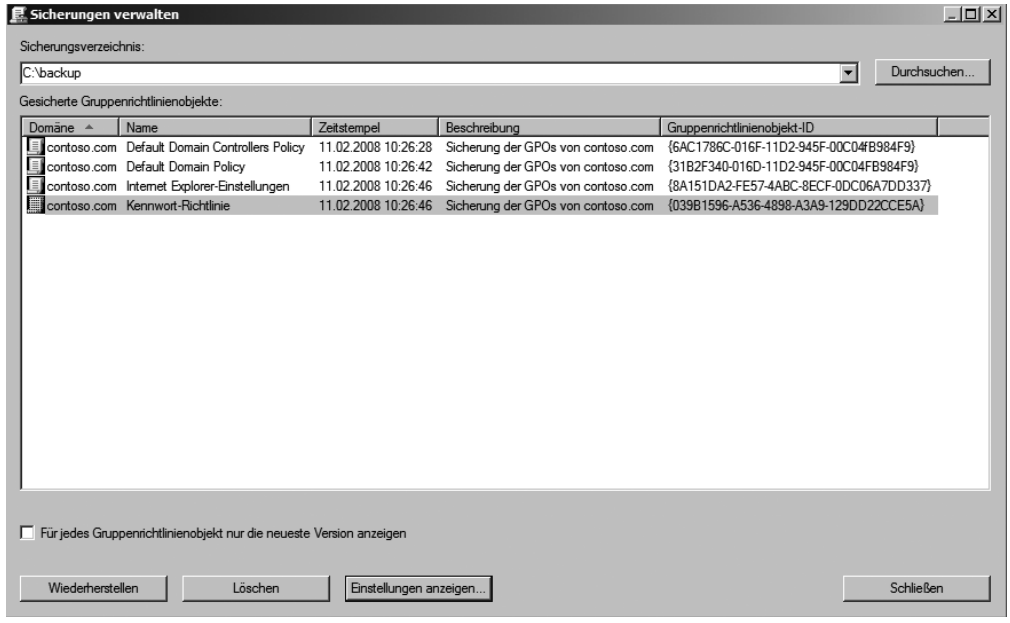
Jede Datensicherung wird auf der Festplatte mit einer eindeutigen GUID im ausgewählten Verzeichnis abgelegt (Abbildung 9.30). Die Verwaltung der gesicherten Gruppenrichtlinien findet allerdings nicht über das Dateisystem statt, sondern ebenfalls mit der GPMC.

Abbildg. 9.30 Anzeigen der GPO-Datensicherung im Windows-Explorer



Sie können in der GPMC mit der rechten Maustaste auf den Knoten *Gruppenrichtlinienobjekte* klicken. Wählen Sie im daraufhin geöffneten Kontextmenü den Befehl *Sicherungen verwalten* aus. Mit diesem Kontextmenübefehl können Sie alle Datensicherungen der Gruppenrichtlinien an zentraler Stelle verwalten. Wenn Sie mehrere Sicherungen vorgenommen haben und zahlreiche Gruppenrichtlinien verwalten müssen, können Sie in diesem Fenster auch das Kontrollkästchen *Für jedes Gruppenrichtlinienobjekt nur die neueste Version anzeigen* aktivieren. In diesem Fall werden aus dem Fenster alle Datensicherungen ausgeblendet, die vor der aktuellsten Sicherung des einzelnen GPOs angelegt wurden. Sie können die einzelnen Sicherungen markieren und sich über die Schaltfläche *Einstellungen anzeigen* die Einstellungen in der Richtlinie anzeigen lassen, die Sie zum Zeitpunkt der Sicherung gesetzt hatten. Die Einstellungen werden Ihnen als HTML-Datei angezeigt.

Abbildg. 9.31 Verwalten der GPO-Datensicherungen in der GPMC



Wiederherstellen von Gruppenrichtlinien

Bei der Wiederherstellung einer Gruppenrichtlinie werden die Daten der exportierten Datei wieder in die produktive Richtlinie importiert. Sie können eine Wiederherstellung durchführen, wenn die Gruppenrichtlinie versehentlich gelöscht wurde oder wenn Sie einen älteren Versionsstand der Einstellungen der Gruppenrichtlinie wiederherstellen wollen. Bei der Wiederherstellung einer Gruppenrichtlinie werden, neben den Einstellungen der Richtlinien, auch die Berechtigungen für das Gruppenrichtlinienobjekt sowie, falls vorhanden, die Verknüpfungen der WMI-Filter wiederhergestellt. Um eine Gruppenrichtlinie wiederherzustellen, klicken Sie in der Verwaltung der Sicherungen auf die Schaltfläche *Wiederherstellen*. Nachdem Sie Ihre Eingabe bestätigt haben, wird die Sicherung wiederhergestellt.

Kopieren von Gruppenrichtlinien

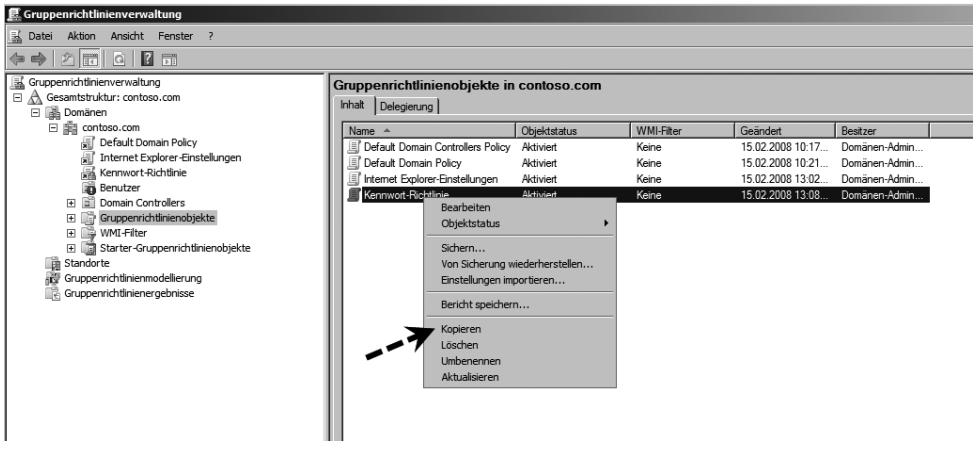
Bei einem Kopiervorgang wird eine komplett neue Gruppenrichtlinie mit neuer GUID erstellt und die Einstellungen der Quellrichtlinie werden importiert. Nach diesem Vorgang sind die beiden Gruppenrichtlinien vollkommen unabhängig voneinander, haben aber identische Einstellungen. Das Kopieren von Gruppenrichtlinien ermöglicht es Ihnen, auch Einstellungen von Gruppenrichtlinien zunächst in einer Testumgebung zu testen und danach in die produktive Umgebung zu importieren. Dazu müssen Sie die Richtlinie in der produktiven Umgebung nicht neu erstellen, sondern können sie aus der Testumgebung in die produktive Umgebung kopieren. Gruppenrichtlinien können mit der GPMC zwischen Domänen, Strukturen und Gesamtstrukturen kopiert werden. Sie müssen für einen Kopiervorgang zwischen Domänen, Strukturen oder Gesamtstrukturen allerdings bidirektionale Vertrauensstellungen einrichten, damit die Gruppenrichtlinien an zentraler Stelle von einer GPMC erstellt, kopiert, gesichert und wiederhergestellt werden können (siehe Kapitel 8).

Kopieren eines GPOs in der GPMC

Um Gruppenrichtlinien zu kopieren, klicken Sie in der GPMC auf den Knoten *Gruppenrichtlinienobjekte* in der Domäne, aus der Sie die Richtlinie kopieren wollen.

1. Klicken Sie mit der rechten Maustaste auf die entsprechende Gruppenrichtlinie und wählen Sie im Kontextmenü den Befehl *Kopieren* aus (Abbildung 9.32). Es erscheint keine weitere Meldung, wenn Sie die Gruppenrichtlinie kopiert haben.

Abbildg. 9.32 Kopieren von Gruppenrichtlinien in der GPMC

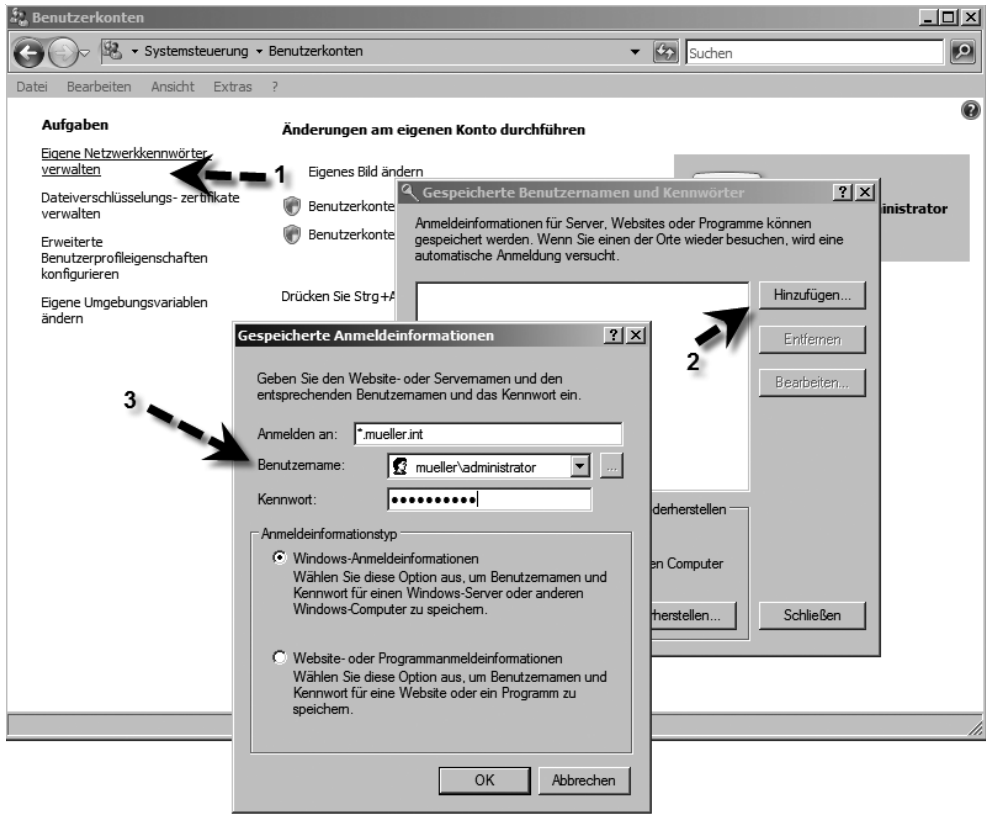


2. Klicken Sie als Nächstes in der GPMC auf den Knoten *Gruppenrichtlinienobjekte* in der Domäne, in der Sie die Gruppenrichtlinie einfügen wollen.
3. Klicken Sie mit der rechten Maustaste auf den Knoten *Gruppenrichtlinienobjekte* und wählen Sie im Kontextmenü den Befehl *Einfügen* aus. Alternativ können Sie die entsprechende Richtlinie auch per Drag & Drop auf den Gruppenrichtlinienobjekt-Container der anderen Gesamtstruktur ziehen.

HINWEIS Wenn Sie die Gruppenrichtlinienverwaltung gestartet haben, können Sie mit einem Klick der rechten Maustaste auf den Eintrag *Gruppenrichtlinienverwaltung* in der Konsolenstruktur im Kontextmenü den Befehl *Gesamtstruktur hinzufügen* auswählen. Standardmäßig werden Sie mit der Gesamtstruktur und Domäne verbunden, in der die Gruppenrichtlinienverwaltung gestartet wird. Sie können einmal hinzugefügte Gesamtstrukturen wieder aus der Konsole entfernen, wenn Sie diese mit der rechten Maustaste anklicken und im Kontextmenü den Befehl *Entfernen* auswählen. Wenn Sie externe Domänen oder andere Gesamtstrukturen hinzufügen wollen, müssen zu diesen Domänen bidirektionale Vertrauensstellungen vorhanden sein (siehe Kapitel 8). Falls Sie explizite Rechte in einzelnen externen Domänen vergeben haben, um diese mit der GPMC zu verwalten, können Sie die Überprüfung der bidirektionalen Vertrauensstellungen nach Aufruf des Menübefehls *Ansicht/Option* auf der Registerkarte *Allgemein* über das Kontrollkästchen *Vertrauensprüfung aktivieren* ausschalten.

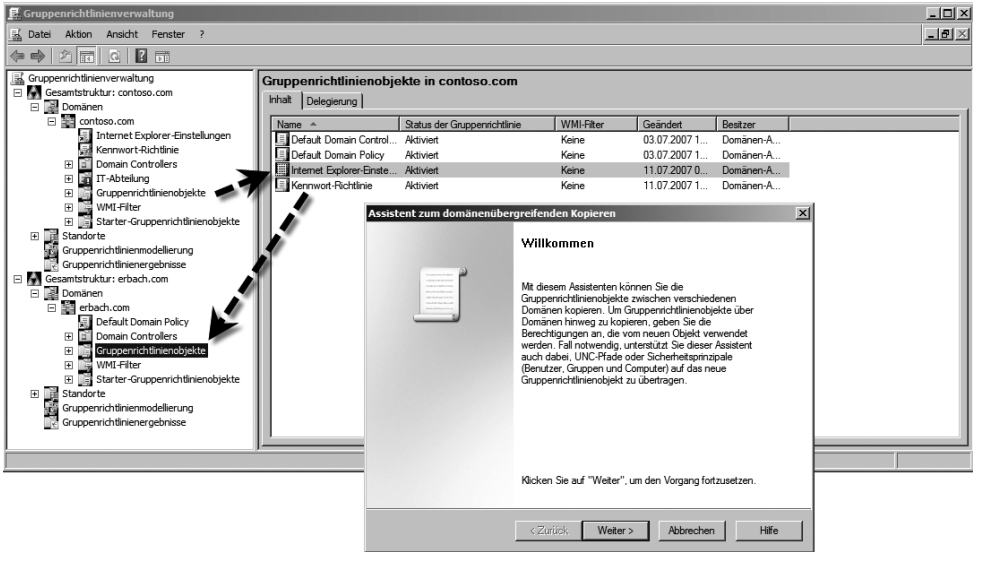
Wollen Sie für die Verwaltung der Gruppenrichtlinien in der GPMC von externen Gesamtstrukturen nicht gleich eine Vertrauensstellung einrichten, können Sie die bereits beschriebene Überprüfung für Vertrauensstellung deaktivieren. In diesem Fall müssen Sie in der Systemsteuerung mit Hilfe des von *Benutzerkonten/Eigene Netzwerkkennwörter verwalten* für die Gesamtstruktur ein Benutzerkonto mit Kennwort hinterlegen, welches Sie zur Administration der Gruppenrichtlinien berechtigt. Hinterlegen Sie als Servernamen die Bezeichnung **.<DNS-Name der Gesamtstruktur>*, zum Beispiel **.contoso.com*.

Abbildg. 9.33 Hinterlegen von Anmeldedaten für nicht vertraute Domänen in der Systemsteuerung



Anschließend erscheint der Assistent zum domänenübergreifenden Kopieren von Gruppenrichtlinien (Abbildung 9.34).

Abbildg. 9.34 Gruppenrichtlinien zwischen verschiedenen Domänen oder Gesamtstrukturen kopieren



4. Im nächsten Fenster müssen Sie entscheiden, ob in der neuen Domäne die Standardberechtigungen gesetzt werden oder ob Sie die ursprünglichen Berechtigungen des GPOs übernehmen bzw. migrieren.
5. Als Nächstes werden die Berechtigungen der Gruppenrichtlinie überprüft. Wenn Sie die Berechtigungen der ursprünglichen Gruppenrichtlinie nicht übernehmen wollen, werden die Berechtigungen der neuen Gruppenrichtlinie auf die Standardberechtigungen gesetzt.
6. Danach erhalten Sie noch ein Informationsfenster und der Assistent beginnt mit dem Import der Gruppenrichtlinie.

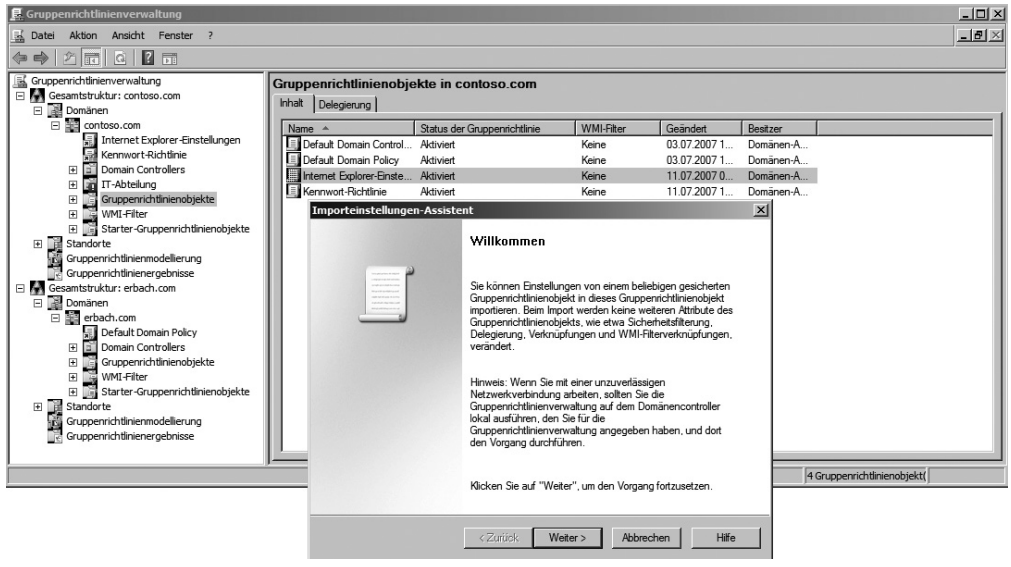
HINWEIS Wenn Sie eine Gruppenrichtlinie kopieren, wird diese nicht automatisch mit Containern verknüpft. Sie müssen eine kopierte Gruppenrichtlinie zunächst mit den gewünschten Containern verknüpfen, ansonsten werden die Einstellungen der Richtlinie nicht angewendet.

Importieren von Gruppenrichtlinien in eine neue Gruppenrichtlinie

Neben dem kompletten Kopieren von Gruppenrichtlinien können Sie auch nur die Einstellungen einer Gruppenrichtlinie in eine bereits vorhandene andere übernehmen. Beim Importieren einer Gruppenrichtlinie werden die Einstellungen aus der Datensicherung der Gruppenrichtlinie verwendet. Beim Importvorgang werden alle Einstellungen der Ziel-Richtlinie gelöscht und danach die Einstellungen der Quell-Richtlinie übernommen. Dieser Vorgang funktioniert auch zwischen Richtlinien aus verschiedenen Gesamtstrukturen und auch innerhalb der gleichen Domäne. Um

Einstellungen aus der Datensicherung von Gruppenrichtlinien in eine neue Richtlinie zu übernehmen, klicken Sie mit der rechten Maustaste auf die Gruppenrichtlinie im Knoten *Gruppenrichtlinienobjekte* und wählen im Kontextmenü den Befehl *Einstellungen importieren* aus. Es erscheint der Importeinstellungen-Assistent (Abbildung 9.35).

Abbildg. 9.35 Importieren von Einstellungen aus der Datensicherung in eine Gruppenrichtlinie

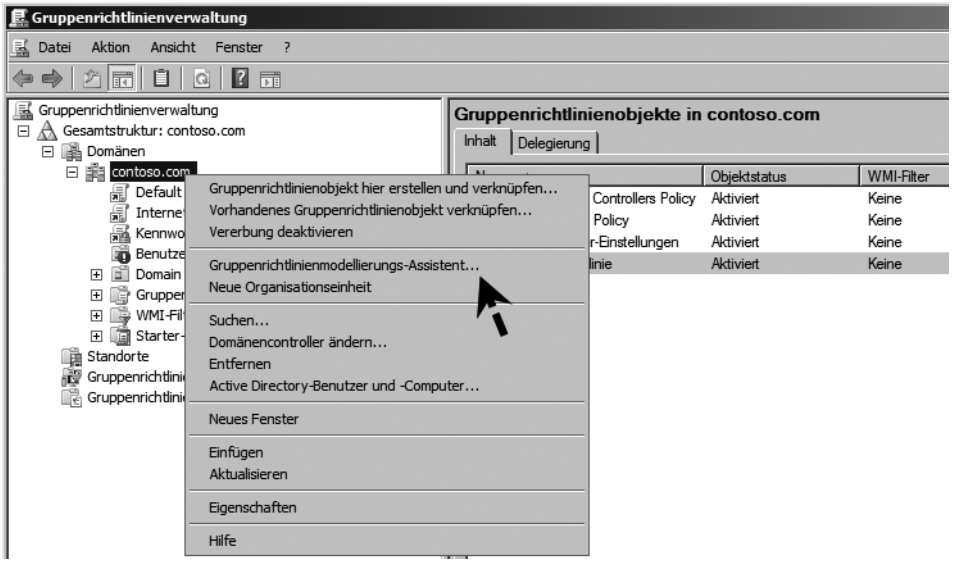


Beim Importieren der Einstellungen gehen alle Einstellungen der Ziel-Richtlinie verloren. Aus diesem Grund schlägt Ihnen der Assistent zunächst die Sicherung des Ziel-GPOs vor. Im nächsten Fenster müssen Sie zunächst das Sicherungsverzeichnis der Gruppenrichtlinien auswählen. Danach können Sie die Quell-Richtlinie auswählen, aus der Sie die Einstellungen in die Ziel-Richtlinie übernehmen wollen. An dieser Stelle können Sie die Einstellungen mit der Schaltfläche *Einstellungen anzeigen* noch einmal überprüfen. Im nächsten Fenster wird die Sicherung nochmals überprüft. Danach erhalten Sie eine Zusammenfassung, nach der die Einstellungen schließlich von der Quell- in die Ziel-Richtlinie übernommen werden.

Gruppenrichtlinienmodellierung

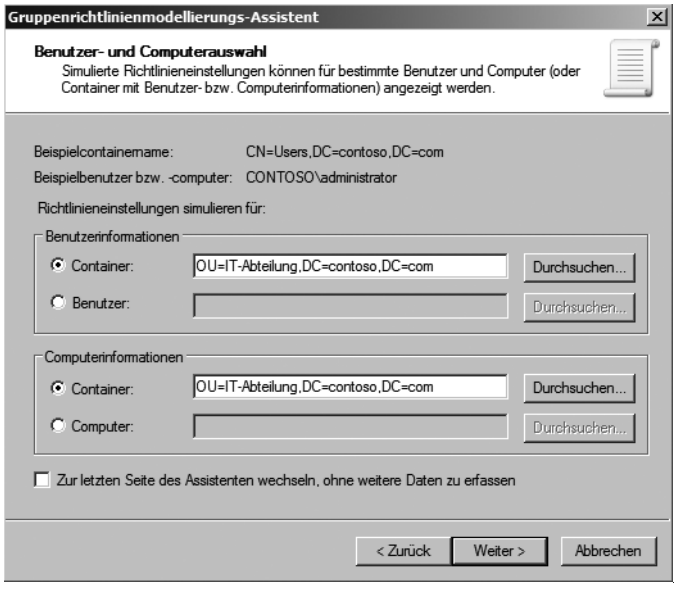
Mit der Gruppenrichtlinienmodellierung aus der GPMC lassen sich die Auswirkungen von Gruppenrichtlinien simulieren. Durch diese Funktion können Sie die Einstellungen vor der eigentlichen Inbetriebnahme einer Gruppenrichtlinie ausführlich testen. Die Gruppenrichtlinienmodellierung wird nur auf Domänencontrollern unter Windows Server 2003/2008 unterstützt. Um eine Simulation für eine bestimmte Domäne oder OU zu simulieren, klicken Sie mit der rechten Maustaste auf den Knoten und wählen im Kontextmenü den Befehl *Gruppenrichtlinienmodellierungs-Assistent* aus (Abbildung 9.36). Es erscheint das Startfenster des Assistenten.

Abbildg. 9.36 Gruppenrichtlinien planen mit dem Gruppenrichtlinienmodellierungs-Assistent



1. Im nächsten Fenster können Sie den Domänencontroller auswählen, mit dem sich die Gruppenrichtlinienmodellierung verbinden soll.
2. Danach müssen Sie den Container auswählen, in dem sich die Benutzer und Computer befinden, für die Sie die Simulation durchführen wollen (Abbildung 9.37).

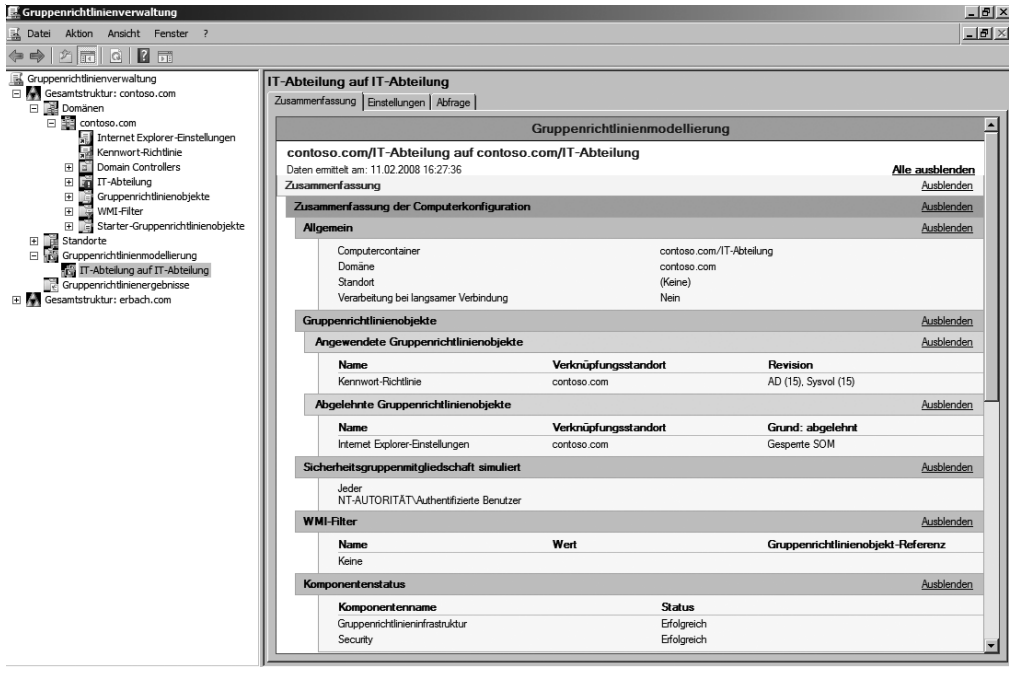
Abbildg. 9.37 Auswählen des zu untersuchenden Containers für die Gruppenrichtlinienmodellierung



3. Im nächsten Fenster können Sie Optionen bezüglich des Standortes und der Netzwerkverbindung auswählen. Normalerweise können Sie die vorgegebenen Einstellungen übernehmen.
4. Auf einer weiteren Seite können Sie simulieren, was passieren würde, wenn die getesteten Benutzer nicht mehr in ihren entsprechenden Sicherheitsgruppen Mitglied wären.
5. Danach können Sie die gleichen Einstellungen für die Computerkonten auswählen.
6. Als Nächstes können Sie noch einzelne Einstellungen der WMI-Filter auswählen, bevor Sie am Ende noch einmal eine Zusammenfassung aller Eingaben erhalten.
7. Normalerweise reichen für Tests die Standardeinstellungen aus und müssen nicht verändert werden. Nachdem Sie die Zusammenfassung bestätigt haben, beginnt bereits die Simulation. Abhängig von der Anzahl Ihrer Benutzer und Computer kann die Simulation bei mehreren Gruppenrichtlinien durchaus eine Weile dauern.
8. Im Anschluss daran erhalten Sie einen detaillierten HTML-Bericht über die Auswirkungen der simulierten Gruppenrichtlinien für den konfigurierten Container.

Auf die gleiche Weise lassen sich auch für den Knoten *Gruppenrichtlinienergebnisse* Abfragen generieren, die exakt aufzeigen, welche Operationen der einzelnen Gruppenrichtlinien angewendet werden und was diese verursachen. Diese Diagnose lässt sich zum Beispiel auch für die Fehlersuche nutzen.

Abbildg. 9.38 Anzeigen des Berichts der Gruppenrichtlinienmodellierung



Anmelde- und Abmeldeskripts für Benutzer und Computer

Es gibt fünf Arten von Skripts, die Anwendern oder Computern zugewiesen werden können. Es spricht nichts dagegen, eine Mischform zu betreiben und mehrere Möglichkeiten der Anmeldeskripts zu nutzen. Folgende Skripts stehen zur Verfügung:

- Das klassische Anmeldeskript, das in den Eigenschaften des Profils eingetragen wird
- Anmeldeskripts in den Gruppenrichtlinien für Benutzer
- Abmeldeskripts in den Gruppenrichtlinien für Benutzer
- Skripts in den Gruppenrichtlinien beim Hochfahren eines Computers, unabhängig vom Benutzer
- Skripts in den Gruppenrichtlinien beim Herunterfahren eines Computers, unabhängig vom Benutzer

Die klassischen Anmeldeskripts werden auf der Registerkarte *Profil* bei den Benutzern hinterlegt. Diese Skripts können problemlos weiter in einem Windows Server 2008-Active Directory verwendet werden.

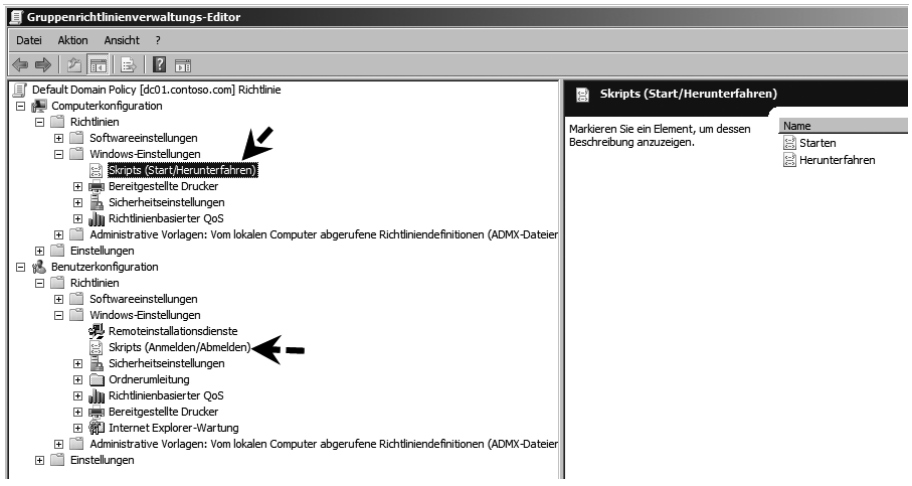
HINWEIS Damit die Skripts beim Anmelden auch gestartet werden, müssen die Dateien in der Freigabe *netlogon* auf den Domänencontrollern liegen. Das gilt auch für Programme oder andere Skripts, die wiederum von den Anmeldeskripts gestartet werden. Wenn Sie ein Skript in die *netlogon*-Freigabe kopieren, wird es durch den Dateireplikationsdienst (File Replication Service, FRS) automatisch auf die anderen Domänencontroller repliziert. Der lokale Speicherort der *netlogon*-Freigabe auf einem Windows Server 2008 ist das Verzeichnis *\Windows\SYSVOL\sysvol\<Domänennamen>\scripts*.

Die Skripts können entweder einfache Batchdateien, spezielle Varianten mit KiXtart (*http://www.kixtart.org*) oder AutoIT (*http://www.hiddensoft.com/autoit*), aber auch VBScript-Dateien sein.

Klassische Anmeldeskripts laufen sichtbar ab, wenn sich ein Anwender bei seinem Computer anmeldet. Mit klassischen Anmeldeskripts ist es nicht möglich, Skripts zu schreiben, die bereits beim Starten des Computers abgearbeitet werden. In einem Active Directory können neben den klassischen Skripts auch Skripts beim Anmelden und Abmelden sowie beim Starten und Herunterfahren eines Computers eingesetzt werden. Die Skripts werden in den Gruppenrichtlinien an folgender Stelle hinterlegt:

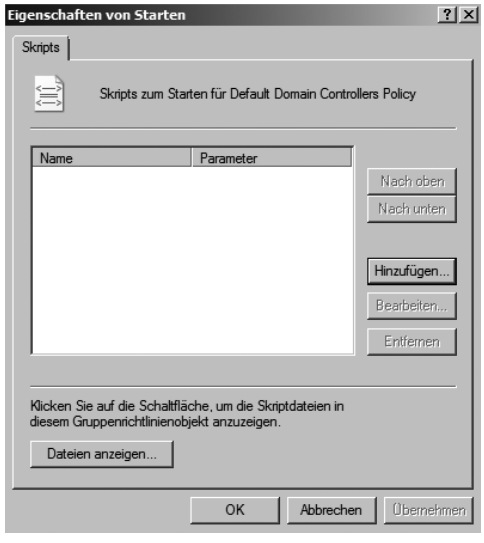
- Skripts für Computer zum Starten und Herunterfahren werden über *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Skripts* gesteuert.
- Skripts für Anwender beim An- oder Abmelden werden über *Benutzerkonfiguration/Richtlinien/Windows-Einstellungen/Skripts* gesteuert.

Abbildg. 9.39 Verwenden von Skripts für das An-, Abmelden von Benutzern oder das Starten und Herunterfahren von PCs



1. Die Skripts in den Gruppenrichtlinien werden nicht sichtbar, sondern im Hintergrund durchgeführt. Um Skripts in den Gruppenrichtlinien zu verwenden, sollten Sie schrittweise vorgehen.
2. Legen Sie die entsprechende Gruppenrichtlinie an und navigieren Sie zu dem Bereich, für den Sie das Skript hinterlegen wollen, also *Computerkonfiguration* oder *Benutzerkonfiguration*.
3. Klicken Sie doppelt auf den jeweiligen Eintrag des *Skripts*, also *Anmelden*, *Abmelden*, *Starten* oder *Herunterfahren*.
4. Klicken Sie auf die Schaltfläche *Dateien anzeigen* (Abbildung 9.40). Es öffnet sich ein Explorer-Fenster.
5. Kopieren Sie anschließend Ihre Skriptdatei in dieses geöffnete Verzeichnis.

Abbildg. 9.40 Hinterlegen von Anmeldeskripts in Gruppenrichtlinien



6. Klicken Sie anschließend auf die Schaltfläche *Hinzufügen* und wählen Sie das Skript aus. Das Skript wird danach im Fenster angezeigt. Sie können auch mehrere Skripts hintereinander ausführen lassen.

Auch die Kombination von klassischen Skripts und Skripts über Gruppenrichtlinien ist möglich. Es ist auch kein Problem, wenn die Skripts in den Gruppenrichtlinien von übergeordneten OUs nach unten vererbt werden und in den untergeordneten OUs weitere Skripts gestartet werden. Sie können alle möglichen Formen miteinander kombinieren. Wenn Sie mit klassischen und Gruppenrichtlinienskripts arbeiten, werden beide parallel abgearbeitet. Diesen Sachverhalt sollten Sie in den Skripts beachten, wenn zum Beispiel Abhängigkeiten existieren. Nach unserer Erfahrung werden die Skripts in den Gruppenrichtlinien meistens vor den klassischen Anmeldeskripts ausgeführt.

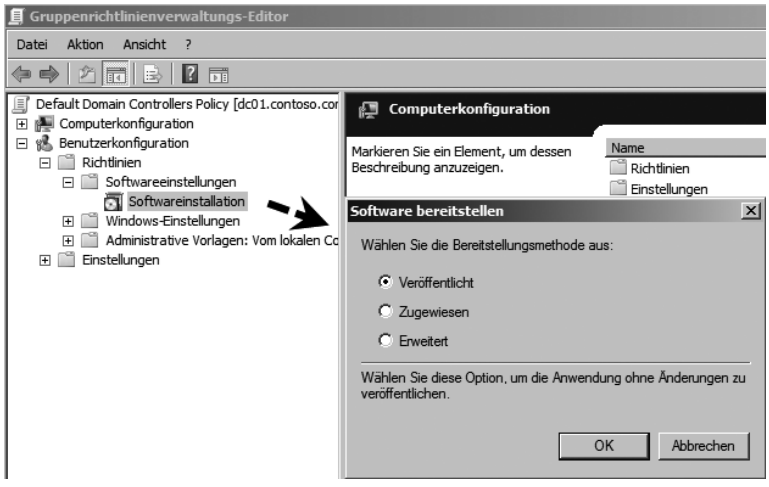
Außer speziellen Skripts können Sie in den Gruppenrichtlinien auch diverse Einstellungen hinterlegen, die den Ablauf der Skripts steuern. Sie finden diese Einstellungen an folgenden Stellen:

- *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Skripts*
- *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Anmeldung*
- *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Gruppenrichtlinien*
- *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Skripts*
- *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Anmeldung*

Softwareverteilung über Gruppenrichtlinien

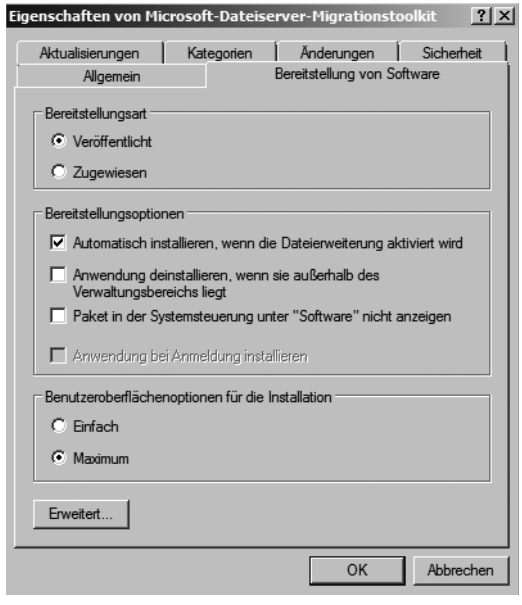
Die Konfiguration der Softwareverteilung bei Windows Server 2008 erfolgt über die Gruppenrichtlinien. Dort können MSI-Pakete für die Installation auf Client-Systemen zugeordnet werden. Die Softwareverteilung erfolgt über die in diesem Kapitel ausführlich behandelten Gruppenrichtlinien. Da diese auf der Ebene von Standorten, Domänen und Organisationseinheiten zugeordnet werden können, lässt sich flexibel steuern, welche Softwarepakete verteilt werden. Die Konfiguration der Softwareverteilung in Gruppenrichtlinien erfolgt über den Bereich *Computerkonfiguration/Richtlinien/Softwareeinstellungen* beziehungsweise *Benutzerkonfiguration/Richtlinien/Softwareeinstellungen*. Dort findet sich jeweils der Eintrag *Softwareinstallation*. Über den Befehl *Paket* im Untermenü *Neu* des Kontextmenüs dieses Eintrags kann die Bereitstellung eines MSI-Pakets durchgeführt werden. Es muss im ersten Schritt das MSI-Paket ausgewählt werden. Dieses Paket muss zunächst auf eine Freigabe im Netzwerk kopiert werden. Ansonsten wird eine Fehlermeldung angezeigt, da die Installation nur von einer Lokation im Netzwerk aus erfolgen kann, auf die Netzwerk-Clients zugreifen können.

Abbildg. 9.41 Automatische Installation von Anwendungen über Gruppenrichtlinien



Nach der Auswahl des Pakets kann die Bereitstellungsmethode ausgewählt werden. Falls es sich um ein Paket handelt, das für Computer bereitgestellt wird, steht die Option *Veröffentlicht* nicht zur Verfügung. Wenn die Option *Veröffentlicht* gewählt wird, wird das Paket automatisch in die Liste der Softwarepakete aufgenommen. Alle erforderlichen Einstellungen werden automatisch gesetzt. Durch einen Doppelklick auf das Paket können die Eigenschaften bearbeitet werden. Wird die Option *Zugewiesen* gewählt, wird ebenfalls automatisch ein Eintrag erstellt. Dieser kann später durch einen Doppelklick angepasst werden. Eine konkrete Steuerung der Optionen ist nur möglich, wenn die Option *Erweitert* ausgewählt wird. In diesem Fall wird gleich das Eigenschaften-Dialogfeld aufgerufen.

Abbildg. 9.42 Bearbeiten eines Softwarepaketes zur automatischen Installation



Über die Registerkarte *Bereitstellung von Software* kann zwischen *Veröffentlicht* und *Zugewiesen* gewählt werden. Darunter können die Bereitstellungsoptionen konfiguriert werden. Es stehen vier wichtige Optionen zur Auswahl:

- Die Option *Automatisch installieren, wenn die Dateierweiterung aktiviert wird* bewirkt, dass die Anwendung beim Öffnen einer Datei, deren Dateityp für diese Anwendung registriert wurde, automatisch installiert wird. Diese Option ist im Regelfall gesetzt und sollte so belassen werden, da dies das sinnvolle Standardverhalten ist.
- Mit *Anwendung deinstallieren, wenn sie außerhalb des Verwaltungsbereichs liegt* wird konfiguriert, dass das System eine Anwendung automatisch von den Client-Systemen entfernt, wenn die Gruppenrichtlinien, über die sie eingerichtet wurde, keine Gültigkeit mehr für diesen Benutzer oder Computer hat. Das macht bei Anwendungen Sinn, die Zugriff auf kritische Informationen im Unternehmen gewähren.
- Mit *Paket in der Systemsteuerung unter "Software" nicht anzeigen* wird festgelegt, dass das Paket zwar über die Gruppenrichtlinie verteilt wird, in der Systemsteuerung aber nicht erscheint. Das kann hilfreich sein, um zu verhindern, dass Anwender dieses Paket deinstallieren. Das Installationsprogramm kann über Skripts oder durch Zugriff auf die Freigabe gesteuert werden.
- Sie können mit *Anwendung bei Anmeldung installieren* definieren, dass die Anwendung bei der Anmeldung eines Benutzers installiert wird. Diese Option ist nur bei Paketen verfügbar, die in den Computerrichtlinien konfiguriert sind, da sie bei den Benutzerrichtlinien redundant wäre.

Über die Einstellungen für die *Benutzeroberflächenoptionen* kann konfiguriert werden, ob dem Benutzer alle Installationsmeldungen präsentiert werden oder ob sich das System darauf beschränkt, nur den Installationsfortschritt anzuzeigen. Auf der Registerkarte *Aktualisierungen* werden die Informationen über die Zusammenhänge zwischen verschiedenen MSI-Paketen aufgeführt. Im oberen Bereich können über die Schaltfläche *Hinzufügen* Pakete aus dieser oder anderen Gruppenrichtlinien angegeben werden, die durch das aktuell bearbeitete Paket aktualisiert werden. Im unteren Bereich sind Pakete aufgeführt, die dem bearbeiteten Paket übergeordnet sind. Über die Registerkarte *Kategorien* können Kategorien angegeben werden, unter denen diese Anwendung im Bereich *Software* der Systemsteuerung aufgeführt werden soll. Bei Änderungen können MST-Pakete angegeben werden, die für dieses Paket eingesetzt werden sollen. Mit der Registerkarte *Sicherheit* lassen sich die Zugriffsberechtigungen für die Nutzung der Installationspakete konfigurieren. Über die Registerkarte *Änderungen* lassen sich Transformationsdateien (**.mst*) für MSI-Dateien hinterlegen, welche die Installation der Software beeinflussen.

Fehlerbehebung und Tools für den Einsatz von Gruppenrichtlinien

Sie sollten bei der Einführung von Richtlinien immer eigene Gruppenrichtlinien anlegen und bereits vorhandene Standardrichtlinien nicht bearbeiten. Das hat den Vorteil, dass bei einem Problem auf jeden Fall der Weg frei bleibt, die eigenen Richtlinien zu deaktivieren. Wenn Gruppenrichtlinien nicht funktionieren, können die Ursachen sehr unterschiedlich sein. Sie sollten Schritt für Schritt untersuchen, wo das Problem liegen könnte. Legen Sie am besten für die unterschiedlichen Einstellungen verschiedene Gruppenrichtlinien an und verknüpfen Sie diese mit der entsprechenden OU oder der ganzen Domäne.

- Stellen Sie sicher, dass die Clients den DNS-Server verwenden, auf dem die SRV-Records von Active Directory liegen.
- Überprüfen Sie mit *nslookup* in der Befehlszeile, ob auf den Clients der Domänencontroller aufgelöst werden kann.
- Überprüfen Sie die Ereignisanzeige auf Fehler.
- Ist der Benutzer/Computer in der richtigen OU, auf der die Richtlinie angewendet wird?
- Versuchen Sie die Richtlinie auf eine Sicherheitsgruppe anzuwenden? Das ist nämlich nicht ohne weiteres möglich.
- Bei Windows XP/Vista hat sich der Bootvorgang im Vergleich zu Windows 2000 geändert. Der Explorer wird vor dem Netzwerk geladen. Desktopspezifische Einstellungen können daher noch nicht heruntergeladen werden. Lösung: *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Anmelden/Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten*.
- Stimmt die Vererbung? In welcher Reihenfolge werden die Gruppenrichtlinien angewendet?
- Wurde an der standardmäßigen Vererbung der Richtlinie etwas verändert?
- Haben Sie irgendwo *Erzwungen* oder *Vererbung deaktivieren* aktiviert?
- Geben Sie auf dem PC in der Befehlszeile als angemeldeter Benutzer *gpresult > gp.txt* ein, um sich das Ergebnis der Richtlinie anzeigen zulassen.
- Das Windows-Snap-In *Richtlinienergebnissatz* bietet eine grafische Oberfläche und wertet die angewendeten Richtlinien aus. Sie können sich den Richtlinienergebnissatz auf einer Windows XP oder Vista-Arbeitsstation über *Start/Ausführen/MMC/Datei/Snap-In hinzufügen/Richtlinienergebnissatz* anzeigen lassen. Mit dem Assistenten können Sie die Gruppenrichtlinien übertragen lassen und sich in der grafischen Oberfläche alle angewendeten Gruppenrichtlinien anzeigen lassen. Sie starten die Überprüfung über das Menü *Aktion*.
- Überprüfen Sie, ob sich Ihre Domänencontroller fehlerfrei replizieren.

TIPP Auf der Internetseite *www.gruppenrichtlinien.de* finden Sie weiterführende Informationen und Tipps rund um den Einsatz von Gruppenrichtlinien. Schauen Sie sich auf dieser Seite um, wenn Sie planen Gruppenrichtlinien einzusetzen. Auch auf der englischsprachigen Seite *http://www.gpoguy.com* finden Sie ausführliche Informationen und Tools für Gruppenrichtlinien.

Geräteinstallation mit Gruppenrichtlinien konfigurieren

In diesem Abschnitt werden die Möglichkeiten besprochen, wie Sie Anwendern die Installation von Geräten auf Ihrem Server zuweisen oder verweigern können. In diesen Bereich fällt auch die Konfiguration von USB-Sticks. Generell können Sie mit Windows Server 2008 oder Windows Vista verschiedene Aufgaben durchführen, welche die Geräteinstallation von Benutzern betreffen:

- Sie können verhindern, dass Anwender irgendwelche Geräte installieren.
- Sie können konfigurieren, dass Anwender nur Geräte, also auch USB-Sticks, installieren, die auf einer Liste der genehmigten Geräte stehen.

- Umgekehrt können Sie Anwendern untersagen, Geräte zu installieren, die auf einer bestimmten Liste stehen. Alle anderen Geräte können in diesem Fall von den Anwendern installiert werden.
- Sie können den Schreib- und Lesezugriff auf USB-Sticks konfigurieren. Das gilt aber nicht nur für USB-Sticks, sondern auch für CD-, DVD-Brenner, Disketten, externe Festplatten und Pocket-Servers.

Hauptsächlich werden diese neuen Funktionen zur Steuerung der Geräteinstallation zur Konfiguration der Anbindung von USB-Sticks verwendet.

Geräte Identifikations String und Geräte Setup Klasse

Wie bereits erwähnt untersucht Windows bei der Anbindung eines neuen Gerätes zwei Informationen die vom angeschlossenen Gerät übermittelt werden. Auf Basis dieser Informationen kann Windows entscheiden, ob ein eigener Treiber installiert werden kann, oder ob der Treiber des Drittherstellers verwendet werden soll. Auch zusätzliche Funktionen der Endgeräte können dadurch aktiviert werden. Diese beiden Informationen zur Installation von Gerätetreibern sind die *Geräte Identifikations Strings* und die *Geräte Setup Klasse*.

Geräte Identifikations String

Ein Gerät verfügt normalerweise über mehrere *Geräte Identifikations Strings*, die der Hersteller festlegt. Dieser String wird auch in der **.inf*-Datei des Treibers mitgegeben. Auf dieser Basis entscheidet Windows, welchen Treiber es installieren soll. Es gibt zwei Arten von Geräte Identifikations Strings:

- **Hardware IDs** Diese Strings liefern eine detaillierte und spezifische Information über ein bestimmtes Gerät. Hier wird der genaue Name, das Modell und die Version des Gerätes als so genannte Geräte ID festgelegt. Teilweise werden nicht alle Informationen, zum Beispiel die Version, mitgeliefert. In diesem Fall kann Windows selbst entscheiden, welche Version des Treibers installiert wird.
- **Kompatible IDs** Diese IDs werden verwendet, wenn Windows keinen passenden Treiber zum Gerät finden kann. Diese Informationen sind allerdings optional und sind sehr generisch. Wenn diese ID zur Treiberinstallation verwendet wird, können zumindest die Grundfunktionen des Geräts verwendet werden.

Windows weist Treiberpaketen einen gewissen Rang zu. Je niedriger der Rang, umso besser passt der Treiber zum Gerät. Der beste Rang für einen Treiber ist *0*. Je höher der Rang, umso schlechter passt der Treiber. Mehr Infos zu dieser Technologie finden Sie in TechNet-Artikeln auf den Seiten:

- *http://go.microsoft.com/fwlink/?LinkId=54881*
- *http://go.microsoft.com/fwlink/?linkid=52665*
- *http://go.microsoft.com/fwlink/?linkid=52662*

Das Neue an Windows Server 2008 und auch Windows Vista ist, dass diese beiden Informationen nicht nur zur Identifikation des Gerätetreibers verwendet werden können, sondern auch zur Zuweisung von Richtlinien, über welche die Funktionen und Berechtigungen des Geräts verwaltet werden können.

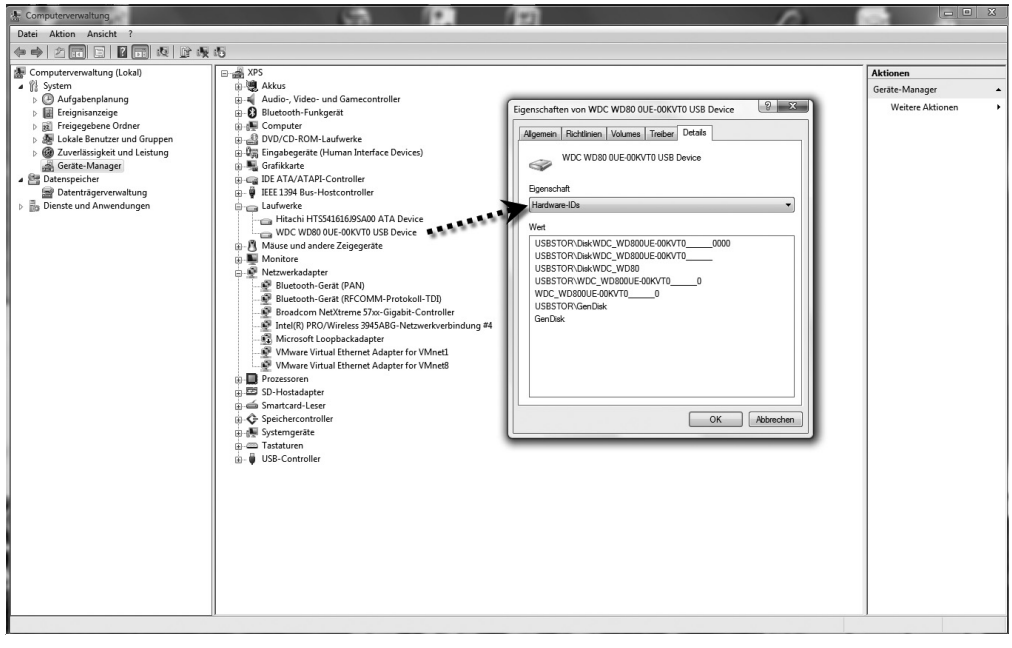
Geräte Setup Klasse

Die *Geräte Setup Klassen* sind eigene Arten von Identifikations Strings. Auch auf diesen Strings wird im Treiberpaket verwiesen. Alle Geräte, die sich in einer gemeinsamen Klasse befinden, werden auf die gleiche Weise installiert, unabhängig von ihrer eindeutigen Hardware ID. Das heißt, alle DVD-Laufwerke werden auf exakt die gleiche Weise installiert. Die Geräte Setup Klasse wird durch einen Globally Unique Identifier (GUID) angegeben.

Hardware-ID und Geräte Setup Klassen ermitteln

Um die *Hardware-ID* oder die *Geräte Setup Klasse* eines Gerätes zu ermitteln, verbinden Sie dieses am besten zunächst mit einem Windows-PC und lassen Sie den Treiber installieren. Im Anschluss rufen Sie den Geräte-Manager auf. Rufen Sie im Anschluss die Eigenschaften des Gerätes auf und wechseln Sie auf die Registerkarte *Details*. Über die Auswahl der Option *Hardware-IDs* im Dropdown-Menü *Eigenschaften* können Sie sich die alle Hardware-IDs eines Gerätes anzeigen lassen (Abbildung 9.43). Diese Informationen können Sie später in der Richtlinie hinterlegen (siehe den folgenden Abschnitt). Über dieses Menü können Sie auch weitere Informationen über die Eigenschaften des Geräts anzeigen lassen, unter anderem auch die Geräteklasse. Sie können die Werte markieren und über die Tastenkombination Strg + C in die Zwischenablage kopieren und bei Bedarf wieder in die Gruppenrichtlinien einfügen.

Abbildg. 9.43 Anzeigen der Hardware-IDs eines Gerätes, zum Beispiel einer externen USB-Festplatte

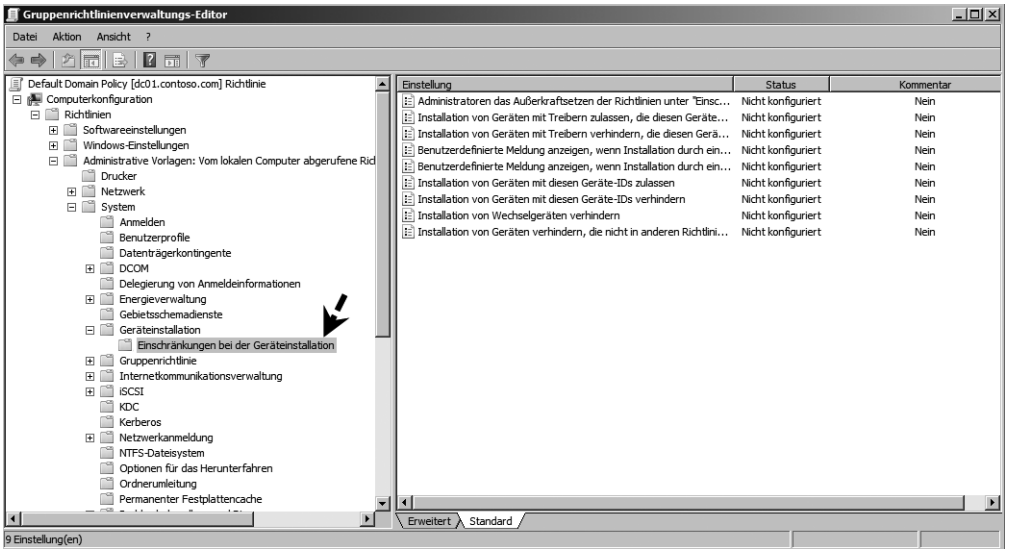


Zusätzlich können Sie diese Informationen mit Hilfe des Befehlszeilentools *DevCon* anzeigen lassen. Sie können sich dieses Tool über die Internetseite *http://go.microsoft.com/fwlink/?linkid=56391* kostenlos herunterladen.

Gruppenrichtlinien-Einstellungen für die Geräteinstallation

Die Einstellungen für die Geräteinstallationen können unter Windows Server 2008 und Windows Vista entweder lokal auf den jeweiligen PC vorgenommen werden oder über Gruppenrichtlinien. Die vorgenommenen Einstellungen gelten immer für den gesamten Computer, an den sie zugewiesen worden sind. Die Einstellungen können nicht auf einzelne Benutzer oder Gruppen zugewiesen werden, mit Ausnahme der Möglichkeit, dass Administratoren die Einstellungen für ihr eigenes Benutzerkonto überschreiben können. Diese Richtlinie finden Sie über *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Geräteinstallation/Einschränkungen bei der Geräteinstallation* (Abbildung 9.44). Aktivieren Sie an dieser Stelle die Richtlinie *Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallation" erlauben*, können Administratoren auf PCs mit aktivierter eingeschränkter Geräteinstallation über den Assistent zum Hinzufügen von Hardware Treiber installieren.

Abbildg. 9.44 Konfiguration von Gruppenrichtlinien für die Steuerungen von USB-Sticks an Anwender-PCs

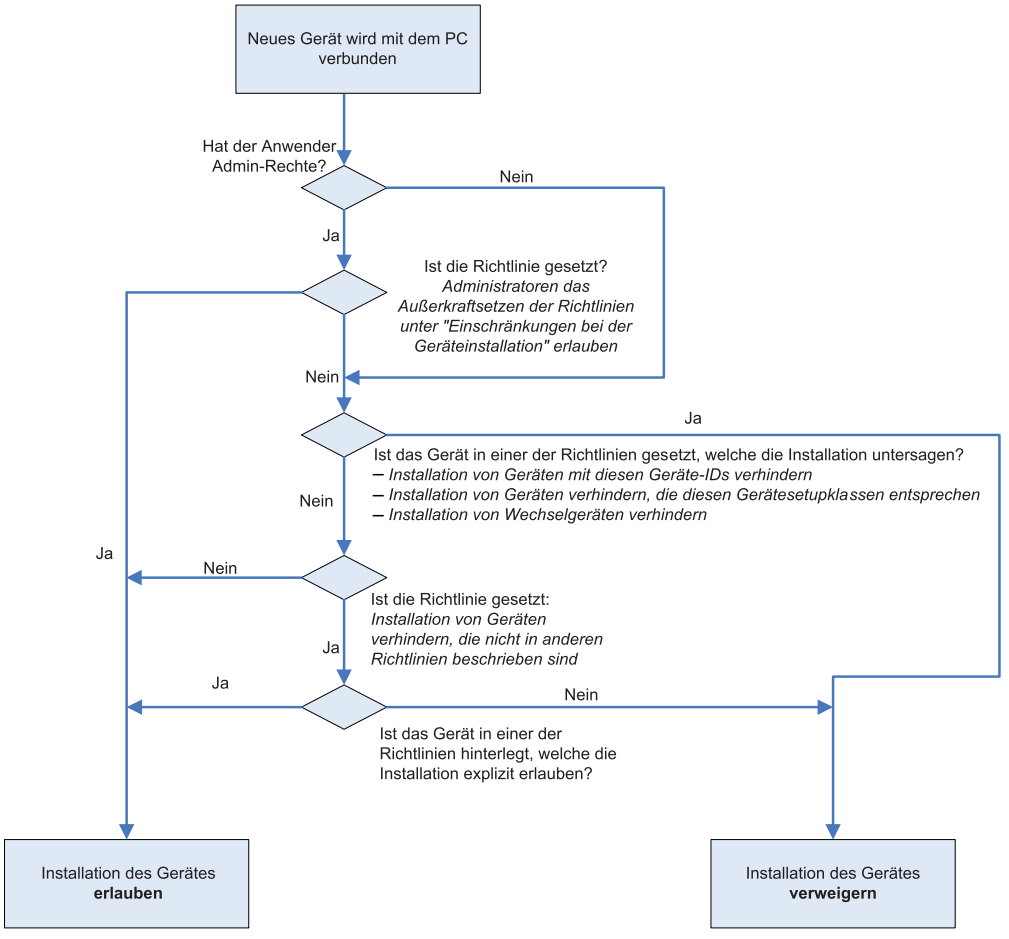


- **Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind** Aktivieren Sie diese Einstellung, können Anwender keine Geräte installieren, bis diese Geräte in der Einstellung *Installation von Geräten mit diesen Geräte-IDs zulassen* oder *Installation von Geräten zulassen, die diesen Gerätesetupklassen entsprechen* definiert wurden.

- Wenn Sie die Richtlinie *Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind* nicht konfigurieren oder aktivieren, können Anwender alle Geräte installieren mit Ausnahme der Geräte, die in den Einstellungen *Installation von Geräten mit diesen Geräte-IDs verhindern* oder *Installation von Geräten verhindern, die diesen Gerätesetupklassen entsprechen* oder *Installation von Wechselgeräten verhindern* definiert wurden.
- **Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallation" erlauben** Bei dieser Einstellung können die Mitglieder der lokalen Administratoren-Gruppe jede Art von Treiber installieren, unabhängig von den Gruppenrichtlinieneinstellungen. Dazu muss allerdings der Assistent zum Hinzufügen von neuer Hardware verwendet werden. Wenn diese Einstellung nicht gesetzt wird, werden auf den betroffenen Maschinen auch die Administratoren an der Installation gehindert.
- **Installation von Geräten mit diesen Geräte-IDs verhindern** Hier können Sie eine Liste festlegen, in der Sie alle Hardware-IDs und Compatible-IDs der Geräte hinterlegen, deren Installation Sie verhindern wollen. Diese Richtlinie hat immer Vorrang vor allen anderen Richtlinien, in denen die Installation von Geräten erlaubt wird.
- **Installation von Geräten mit Treibern verhindern, die diesen Gerätesetupklassen entsprechen** Bei dieser Richtlinie wird für die Anwender die Installation kompletter Geräteklassen verhindert. Diese Einstellung hat Vorrang vor allen anderen Einstellungen und Richtlinien, welche die Installation von Geräten erlauben.
- **Installation von Geräten mit diesen Geräte-IDs zulassen** Hier können Sie eine Liste aller Geräte auf Basis der Hardware-ID oder der Compatible-ID hinterlegen, welche die Anwender installieren dürfen. Diese Richtlinie macht aber nur in Verbindung mit der Richtlinie *Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind* Sinn, da dadurch die Anwender davon abgehalten werden, andere Geräte als die hinterlegten zu installieren. Diese Richtlinie kann durch die Richtlinien *Installation von Geräten mit Treibern verhindern, die diesen Gerätesetupklassen entsprechen, Installation von Geräten mit diesen Geräte-IDs verhindern, Installation von Wechselgeräten verhindern* überschrieben werden.
- **Installation von Geräten mit Treibern zulassen, die diesen Gerätesetupklassen entsprechen** Hier können Sie, analog zur Richtlinie mit den Geräte-IDs, festlegen, welche Geräte-Klassen die Anwender installieren dürfen.

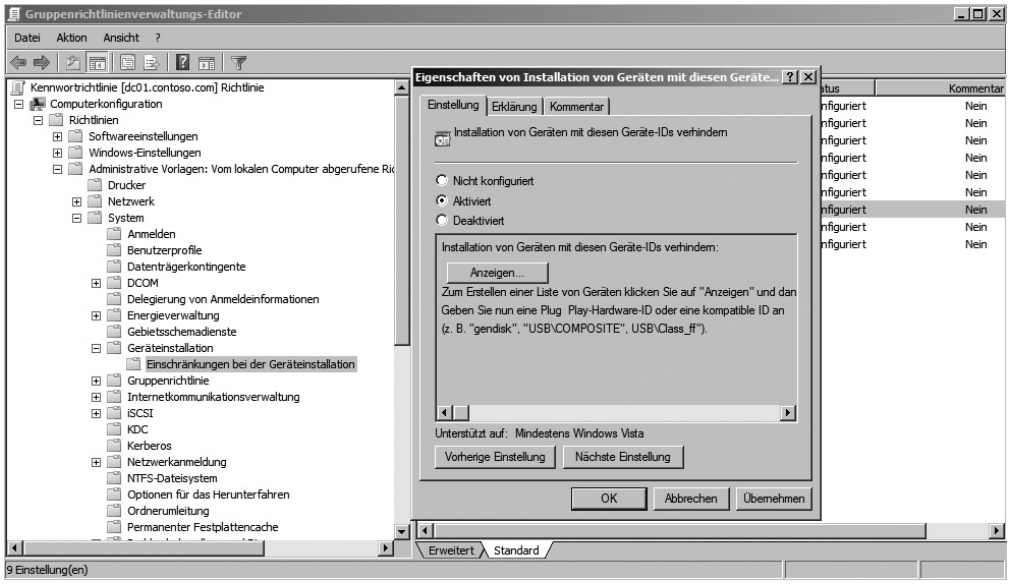
In der Abbildung 9.45 sehen Sie, wie die Richtlinien bei der Anbindung von neuen Geräten an den Server angewendet werden:

Abbildg. 9.45 Wie funktioniert die Steuerungen in Geräteinstallationen über Gruppenrichtlinien



Um in den Richtlinien für die Zulassung oder Verhinderung der Installation von Geräten Hardware-IDs aufzunehmen, rufen Sie die Eigenschaften dieser Einstellung auf und aktivieren Sie diese. Klicken Sie im Anschluss auf die Schaltfläche *Anzeigen* und dann auf Schaltfläche *Hinzufügen*. Hier können Sie die Hardware-ID einfügen, die Sie zuvor in den Eigenschaften des Gerätes im Geräte-Manager in die Zwischenablage kopiert haben (Abbildung 9.46).

Abbildg. 9.46 Konfiguration der Gruppenrichtlinie zur Unterbindung der Treiberinstallation

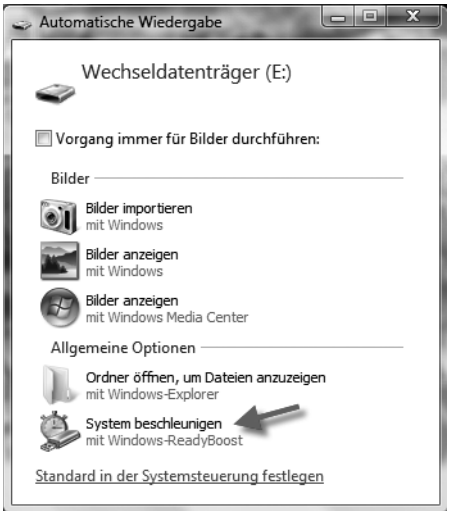


Wird die Installation eines Gerätes untersagt, erhält ein Anwender entsprechende Fehlermeldungen, die darauf hinweist, dass die Installation auf Basis einer Richtlinie untersagt wird.

Konfigurieren von Gruppenrichtlinien für den Zugriff auf Wechselmedien

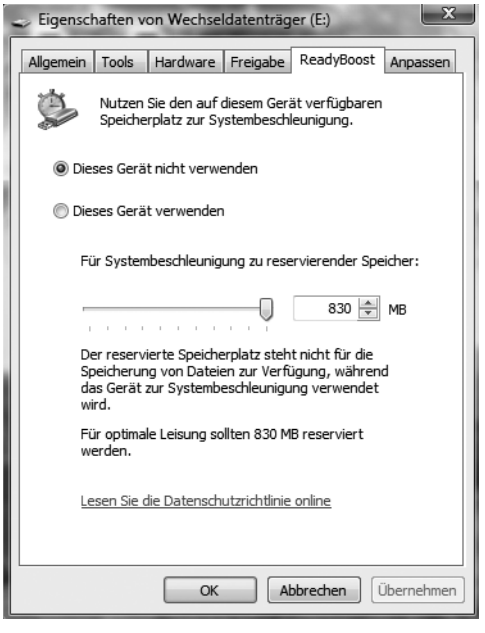
Zusätzlich zu der Möglichkeit, die Installation von Geräten zu steuern, können in Windows Server 2008 und Windows Vista Gruppenrichtlinien erstellt werden, welche den schreibenden und lesenden Zugriff auf Wechselmedien steuern. Diese Einstellungen können auch in der lokalen Richtlinie einzelner PCs gesetzt werden und haben so Wirkung für alle Anwender, die sich an diesem PC anmelden. Alternativ können diese Einstellungen auch auf Benutzerebene für einzelne Benutzerkonten getroffen werden. Die Richtlinien für den Schreib- oder Lesezugriff auf Wechselmedien haben keinerlei Einfluss auf die *ReadyBoost*-Funktion von Windows Vista. Diese neue Funktion unterstützt die Integration von externem Speicher, wie zum Beispiel USB-Sticks. Die Auslagerungsdatei kann auf solche Flashspeicher angelegt werden und steht so deutlich performanter zur Verfügung als auf der Festplatte. Die dabei angelegten Informationen werden verschlüsselt abgelegt, sodass auch beim Abtrennen dieses Speichers vom System kein Sicherheitsproblem entsteht. Der externe Datenträger kann jederzeit wieder entfernt werden, dann steht allerdings diese Performancesteigerung nicht mehr zur Verfügung. Sobald ein USB-Stick mit dem Computer verbunden wird, erscheint das Autostartmenü, über das Sie die Performance verbessern können (Abbildung 9.47). Sie können die Konfiguration von ReadyBoost jederzeit über das Eigenschaftenmenü des Datenträgers vornehmen, dazu steht die Registerkarte *ReadyBoost* zur Verfügung.

Abbildg. 9.47 Aktivieren von ReadyBoost unter Windows Vista



Vista überprüft bei der Auswahl der Option, ob das Gerät genutzt werden kann und schlägt nur dann die Einbindung in das System vor, wenn sich tatsächlich eine Performancesteigerung erreichen lässt. Sie können selbst entscheiden, ob Sie die Funktion für das Laufwerk nutzen wollen und wie viel Speicherplatz Sie zur Verfügung stellen möchten (Abbildung 9.48). Nicht unterstützte Geräte können nicht eingebunden werden.

Abbildg. 9.48 Anpassen des Speicherplatzes, der auf dem USB-Speicher für ReadyBoost zur Verfügung steht



Die Richtlinie zur Steuerung von Wechselmedien kann sowohl unter der Computerkonfiguration als auch in der Benutzerkonfiguration durchgeführt werden. Sie finden die Einstellungen für den Zugriff auf Wechselmedien unter

- Computerkonfiguration/Administrative Vorlagen/System/Wechselmedienzugriff
- Benutzerkonfiguration/Administrative Vorlagen/System/Wechselmedienzugriff

Die Einstellungen dieser Richtlinie sind selbsterklärend. Wenn Sie eine Richtlinie aufrufen, finden Sie auf der Registerkarte *Erklärung* eine ausführliche Information über die Auswirkungen der Richtlinien. Nicht jedes Brennprogramm von Drittherstellern hält sich an die Einstellungen in der Richtlinie für den schreibenden Zugriff auf CDs oder DVDs. Wenn Sie sicherstellen wollen, dass keine CDs oder DVDs gebrannt werden können, sollten Sie die Installation von DVD- oder CD-Brennern über die entsprechende Richtlinie einstellen. WPD-Geräte sind Windows Portable Devices wie Media Player, Handy oder andere Windows Mobile-Geräte wie Pocket-PCs.

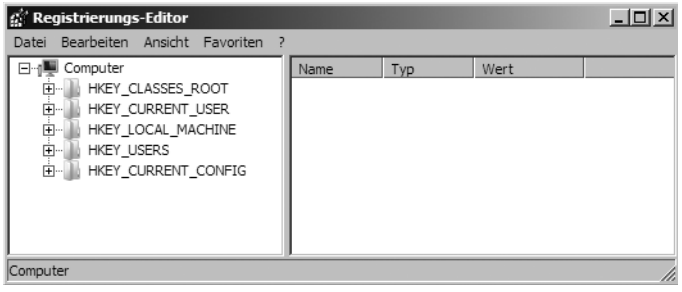
Die Registrierungsdatenbank

Die Registrierungsdatenbank, die auch kurz als Registrierung oder mit dem englischen Begriff Registry bezeichnet wird, beinhaltet sämtliche Konfigurationseinstellungen für Windows. Die Einträge in der Registry können wie die Inhalte jeder anderen Datenbank betrachtet und modifiziert werden. Bedenken Sie jedoch immer, dass Sie durch unbedachte Änderungen Schäden am Betriebssystem verursachen können, sodass Windows nicht mehr in der Lage ist, zu starten oder stabil zu funktionieren. In diesem Fall bringt Ihnen auch eine Sicherung der Registry keine Hilfe mehr, da diese nur in ein laufendes Windows zurückgespielt werden kann. Sie müssen stattdessen an eine Wiederherstellung des Systems gehen.

Der Aufbau der Registry

Die Registry bildet eine feste Struktur aus *Werten* und *Schlüsseln*, die wiederum Unterschlüssel enthalten können. Jedem Schlüssel ist ein Wert zugewiesen. Dabei gibt es unterschiedliche Werte der Typen *String*, *Binary* usw. Es kann sich jedoch auch um einen leeren Wert handeln. Jeder Wert besteht unabhängig von seinem Typ aus einem Namen und einem Wert. Wenn Sie die Registry mit dem Registrierungs-Editor betrachten, erinnert diese zunächst in gewisser Weise an den Windows-Explorer. Auf oberster Hierarchieebene finden Sie den Arbeitsplatz, darunter die verschiedenen Schlüssel und Unterschlüssel, die mit dem Ordnersymbol versehen sind, sowie die Werte, die Sie sich wie Dateien vorstellen können. Die Werte können analog zu Dateien verschiedenen Typs sein. Um die Registry zu öffnen und später auch zu modifizieren, verwenden Sie das Programm *regedit.exe*. Geben Sie unter *Start/Ausführen* den Befehl *regedit* ein, um das Fenster des Registrierungs-Editors zu öffnen. Mit Hilfe dieses Editors können Sie Schlüssel und Werte hinzufügen, bearbeiten und löschen (Abbildung 9.49).

Abbildg. 9.49 Bearbeiten der Registry mit dem Registrierungs-Editor



HINWEIS Die Registrierung in den 64-Bit-Versionen von Windows ist in 32-Bit- und 64-Bit-Schlüssel unterteilt. Des Registrierungs-Editor in den 64-Bit-Versionen zeigt sowohl die 32-Bit-Schlüssel als auch die 64-Bit-Schlüssel an. Sie können 64-Bit- und 32-Bit-Registrierungsschlüssel und -Werte mit der standardmäßigen 64-Bit-Version des Registrierungs-Editors einsehen und bearbeiten.

Änderungen an der Registry können über den Registrierungs-Editor nicht wieder rückgängig gemacht werden. Unter früheren Windows-Versionen konnten Sie die Registry auch über das Programm *regedt32.exe* öffnen. Dieses Programm steht unter Windows Vista und Windows Server 2008 nicht mehr zur Verfügung. Sofern Sie den Befehl eingeben, öffnet sich dasselbe Fenster wie nach dem Aufruf von *regedit*. Die Registry besteht grundsätzlich aus fünf *Hauptschlüsseln*. Die Anzahl und Art der Unterschlüssel ist auf jedem System unterschiedlich und richtet sich nach dessen Hardware- und Softwarekonfiguration. Diese fünf Schlüssel können nicht gelöscht werden.

- **HKEY_CLASSES_ROOT (HKCR)** Hier befinden sich die auf dem System registrierten Dateitypen sowie Konfigurationsdaten zu COM-Komponenten wie ActiveX oder OLE-Handler. Der Schlüssel ist ein Unterschlüssel des Schlüssels *HKEY_LOCAL_MACHINE\SOFTWARE*. Die hier gespeicherten Informationen stellen sicher, dass das richtige Programm gestartet wird, wenn Sie eine Datei öffnen. Der Schlüssel *HKEY_LOCAL_MACHINE\SOFTWARE\Classes* beinhaltet die Standardeinstellungen, die auf alle Benutzer des lokalen Computers angewendet werden können. Im Schlüssel *HKEY_CURRENT_USER\Software\Classes* sind Einstellungen gespeichert, die Standardeinstellungen überschreiben und nur für den aktuellen Benutzer gelten. Der Schlüssel *HKEY_CLASSES_ROOT* bietet eine Ansicht der Registrierung, in der die Informationen aus diesen zwei Quellen zusammengefasst sind. Die Datentypen der Dateierweiterungen sind mit jeweils einem eigenen Schlüssel unter *HKCR* gespeichert. Zusätzlich besitzt dort jeder Schlüssel noch einen Unterschlüssel mit den Eigenschaften des Dateityps. Zu den Eigenschaften gehören beispielsweise das Symbol oder die im Kontextmenü angezeigten Befehle für die Datei. Alle Dateitypen, die unter *HKCR* registriert sind, können per Doppelklick vom Benutzer geöffnet werden.
- **HKEY_CURRENT_USER (HKCU)** Sobald sich ein Benutzer anmeldet, wird dieser Schlüssel erstellt. Dabei werden die Informationen für den aktuellen Benutzer aus dem Schlüssel *HKEY_USERS* bezogen. *HKCU* beinhaltet sämtliche benutzerbezogenen Einträge wie installierte Programme oder Einstellungen an seinem *GUI*. Sobald sich ein Benutzer anmeldet, wird aus dem Schlüssel *HKEY_USERS* der Unterschlüssel für sein Benutzerkonto mit seinen aktuellen Einstellungen für Desktop, Startmenü usw. in diesen Schlüssel kopiert. Nimmt er Änderungen

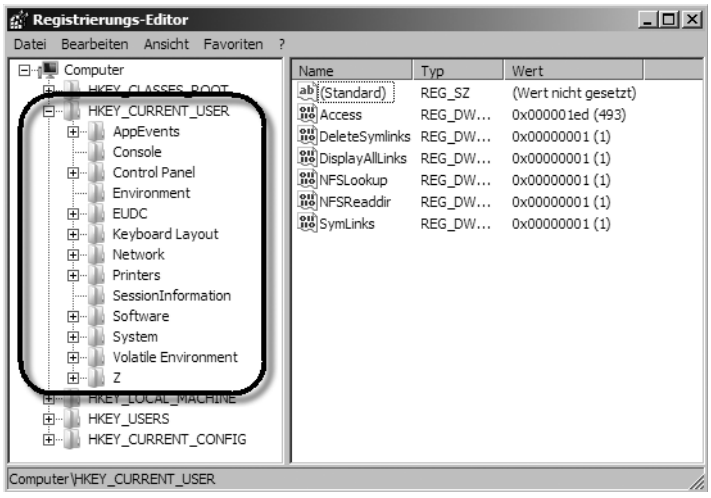
an diesen Einstellungen vor, werden diese unter *HKCU* und zugleich auch im jeweiligen Schlüssel unter *HKEY_USERS* gespeichert.

TIPP Registrierungseinstellungen in *HKEY_CURRENT_USER* werden manchmal nicht bei der Installation, sondern beim ersten Ausführen eines Programms erstellt. Wenn Sie das Programm nicht ausführen, während der Installationsmodus noch aktiv ist, werden die *HKEY_CURRENT_USER*-Einstellungen nicht in *HKEY_LOCAL_MACHINE* kopiert. Wenn ein Benutzer das Programm erstmals ausführt, wird *HKEY_CURRENT_USER* mit den Standardeinstellungen geladen. Wenn diese Standardeinstellungen nicht ausreichen, müssen sie für jeden Benutzer individuell angepasst werden. Um dieses Problem auf Terminalservern zu vermeiden, führen Sie das Programm einmal aus, bevor Sie in der Software auf *Fertig stellen* klicken. Wenn Sie den Installationsmodus auf einem Terminalserver ohne Programmausführung verlassen haben, wechseln Sie mit *change user /install* erneut in den Installationsmodus und führen dann das Programm aus. Wenn Sie das Programm bereits im Ausführungsmodus ausgeführt haben, erstellen Sie ein neues Administratorkonto und melden sich mit diesem Konto an. Geben Sie den Befehl *change user /install* ein, führen Sie anschließend das Programm aus, und geben Sie dann *change user /execute* ein, um den Installationsmodus zu verlassen.

Der Schlüssel *HKCU* enthält folgende Unterschlüssel (Abbildung 9.50):

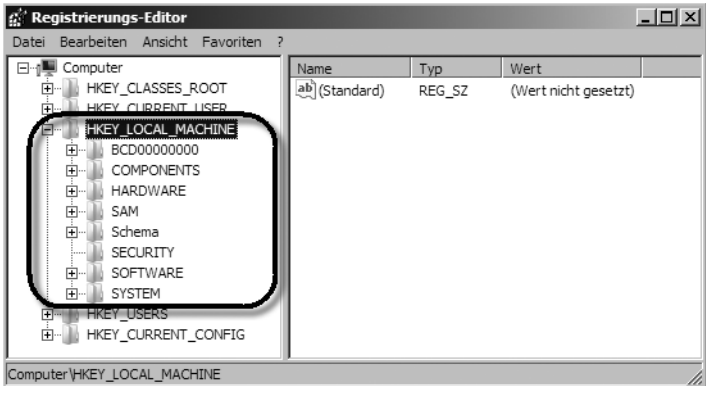
- **AppEvents** Pfade zu den Windows-Sound-Dateien, die bei Windows-Ereignissen wie Fehlermeldungen abgespielt werden
- **Console** Einstellungen der Konsole wie Schriftart oder Puffergröße
- **Control Panel** Einträge, die sich über die Systemsteuerung modifizieren lassen
- **Environment** Die Umgebungsvariablen auf dem System, zum Beispiel zum Ordner *\TEMP* des Benutzerkontos
- **EUDC** Hierbei handelt es sich um die Steuerschlüssel für die Systemfonts *eudc.tte* (End User Defined Character). Hierüber können Sie eigene Schriftzeichen erstellen oder importieren.
- **Identities** Angaben zur Benutzeridentifizierung wie ursprüngliche und aktuelle User-ID
- **Keyboard Layout** Gibt das Tastatur-Layout (Schema sowie zugehörige **.dll*-Dateien) an
- **Network** Auflistung der Netzwerkpfade des Benutzers unter Angabe von Zielcomputer und Anmeldename
- **Printers** Auflistung der zur Verfügung stehenden Drucker sowie seiner persönlichen Einstellungen daran
- **SessionInformation** Hier finden Sie den Wer *ProgramCount*. Dieser gibt an, wie viele Anwendungen in der Taskliste sichtbar sind. Es werden nicht alle laufenden Programme gezählt, sondern nur diejenigen, die sichtbar sind. Außerdem werden Programme mit doppelter Instanz nur einmal gezählt.
- **Software** Benutzerdefinierte Softwareeinstellungen, wie die zuletzt geöffneten Dateien
- **System** Hierbei handelt es sich um benutzerspezifische Einstellungen für Systemgeräte, die nur für diesen Benutzer gelten
- **Volatile Environment** Angaben zum Anmeldeserver und Pfadangaben zu *\BENUTZER*
- **Z** Hier werden die Einstellungen des Network File Systems für den Anwender gespeichert, sowie dessen verknüpfte Anmeldenamen unter Unix

Abbildg. 9.50 Anzeigen der Unterschlüssel des Hauptschlüssels *HKCU*



- **HKEY_USERS (HKU)** Hier sind die Konfigurationseinstellungen für sämtliche auf dem System hinterlegten Benutzer gespeichert. Für jeden auf dem System hinterlegten Benutzer ist ein eigener Schlüssel abgelegt. Der Schlüssel trägt als Namen die *SID* des jeweiligen Benutzers. Darin werden sämtliche Einstellungen gespeichert, die der aktuell angemeldete Benutzer beispielsweise am Desktop oder am Startmenü vornimmt. Die Standardeinstellungen sind im Unterschlüssel *\.Default* hinterlegt. Sobald sich ein neuer Benutzer das erste Mal am System anmeldet, werden die Inhalte dieses Schlüssels komplett in einen neuen Unterzweig von *HKEY_USERS* kopiert. Als Name wird die *SID* des Benutzerkontos gesetzt.
- **HKEY_LOCAL_MACHINE (HKLM)** In diesem Schlüssel sind die Konfigurationen für den Computer hinterlegt. Dabei handelt es sich sowohl um die Hardware- als auch um die Softwareeinstellungen der Programme, die für alle Benutzer des Computers installiert sind. Diese Informationen gelten immer, unabhängig davon, welcher Benutzer aktuell angemeldet ist (Abbildung 9.51).

Abbildg. 9.51 Konfigurieren des Hauptschlüssels *HKEY_LOCAL_MACHINE*



- **BCD00000000** Dieser Eintrag enthält die Informationen des neuen *Boot Configuration Datastores* (BCD) von Windows Server 2008 und Windows Vista (siehe Kapitel 2). Änderungen können aber nicht an dieser Stelle vorgenommen werden, sondern nur über das Tool *bcdedit.exe* oder Zusatztools.
- **COMPONENTS** Hier werden einige Informationen, hauptsächlich Versionsstände zu den installierbaren Funktionen und Serverrollen gespeichert.
- **HARDWARE** Hier sind alle auf dem Computer installierten Hardware-Komponenten sowie deren Einstellungen hinterlegt.
- **SAM** Benutzerkennungen und Gruppen wurden in Windows NT 4.0 und werden noch auf Servern ohne Active Directory-Anbindung in der so genannten *Security Account Manager (SAM)* -Datenbank gespeichert. Die SAM Datenbank ist wiederum ein Teil der Registry. Dieser Schlüssel dient hauptsächlich noch der Kompatibilität mit älteren Betriebssystemen.
- **Schema** Hier werden verschiedene Metadaten des Systems gespeichert, die unter anderem mit Gruppenrichtlinien angepasst werden können.
- **SECURITY** Hier werden zum Beispiel Informationen zu lokalen Sicherheitsrichtlinien gespeichert oder Sicherheitseinstellungen, die innerhalb von Systemkomponenten wie einigen Snap-Ins für die MMC gelten.
- **SOFTWARE** Speicherort für die globalen Softwareeinstellungen der auf dem Computer installierten Programme
- **SYSTEM** Hier sind sämtliche Dateien für den Windows-Start enthalten. Dazu zählen beispielsweise Computereinstellungen oder zu startende Dienste.

- **HKEY_CURRENT_CONFIG (HKCC)** In diesem Schlüssel befinden sich die aktuellen Konfigurations- und Hardware-Einstellungen des Computers. So finden Sie hier beispielsweise die aktuelle Auflösung und Farbtiefe der Grafikkarte oder den Verbindungsstatus des Druckers. Verwechseln Sie diese Einträge nicht mit der Beschreibung der Computerhardware unter *HKLM*. Im Unterschlüssel *\Software* sind Informationen zu den Bildschirmschriften oder der Internetverbindung zu finden.

Neuerungen im Registry-Aufbau von Windows Server 2008

Bei Windows XP und Windows Server 2003 (vor allem auf Terminalservern) scheiterte das Arbeiten ohne administrative Berechtigungen oft daran, dass Softwareinstallationen fehlerhaft durchgeführt wurden oder die entsprechenden Rechte zur Ausführung gefehlt haben. Die Probleme lagen meist darin begründet, dass die entsprechenden Programme in den Windows-Ordner schreiben wollten, was die Sicherheitseinstellungen nicht genehmigt haben. Diese Konfiguration ist zwar sicher, aber nicht ganz stabil, da die Anwendungen nun mal nicht laufen. Um dieses Problem zu umgehen, haben sich einfach die meisten Benutzer als Administrator angemeldet. In Windows Server 2008 und Windows Vista wird diese Technik angepasst. Windows legt für jeden Benutzer einen virtuellen Ordner an, auf den er Schreibrechte hat. Während der Arbeit wird dieser virtuelle Ordner über den Windows-Ordner gelegt, sodass es für Programme erscheint, als ob die Dateien im echten Windows-Ordner liegen. Diese Vorgehensweise wird auch für einzelne Bereiche der Registry durchgeführt.

Unter Windows Server 2008 und Windows Vista können viele ältere Anwendungen, die nicht für die Nutzung von Standardbenutzerkonten entworfen wurden, ohne Änderungen weiterhin eingesetzt werden – und zwar dank der Virtualisierung von Dateisystem und Registrierung. Dieses Feature stellt jeder Anwendung seine eigene virtuelle Version einer Ressource, in die geschrieben werden soll, zur Verfügung. Wenn eine Anwendung zum Beispiel versucht, in eine Datei im Ordner *Programme* zu schreiben, dann stellt Windows dieser Anwendung seine eigene private Kopie der entsprechenden Datei zur Verfügung. Durch die Virtualisierung besteht außerdem standardmäßig die Möglichkeit einer Protokollierung beim Zugriff auf geschützte Bereiche.

Viele Anwendungen, die auf Windows XP oder Windows Server 2003 nicht als Standardbenutzer ausgeführt werden können, können aufgrund der Funktion für Datei- und Registrierungsvirtualisierung ohne Änderungen auf Windows Server 2008 und Windows Vista ausgeführt werden. In Windows XP und Windows Server 2003 werden die meisten Anwendungen unterbrochen, wenn sie versuchen, in geschützte Bereiche des Dateisystems oder der Registrierung zu schreiben, für die der Standardbenutzer keine Zugriffsberechtigung besitzt. Windows Server 2008 und Windows Vista verbessern die Kompatibilität, indem Schreibzugriffe (und nachfolgende Lesezugriffe auf Dateien und Registrierungen) an einen speziellen Speicherort innerhalb dieses Benutzerprofils umgeleitet werden. Wenn zum Beispiel eine Anwendung versucht, in die unter *C:\Program Files\contoso\settings.ini* gespeicherte Datei zu schreiben, und der Benutzer hierfür keinen Schreibzugriff besitzt, wird dieser in das Verzeichnis *C:\Users\<Benutzername>\AppData\Local\VirtualStore\Programme\contoso\settings.ini* umgeleitet. Wenn eine Anwendung versucht, in den Registrierungsschlüssel *HKLM\SOFTWARE\Contoso* zu schreiben, wird diese Aktion automatisch an *HKCU\Software\Classes\VirtualStore\MACHINE\Software\Contoso* umgeleitet. Darüber hinaus ist es für das Logo-Programm *Certified for Windows Vista Software* erforderlich, dass eine Anwendung als Standardbenutzer ohne Virtualisierung ausgeführt wird. Andernfalls erhält die Anwendung nicht das Logo.

HINWEIS Die Virtualisierung des Dateisystems und der Registry macht in manchen Umständen etwas Probleme. Auf der Internetseite *http://support.microsoft.com/kb/927387/de-de* finden Sie einige Hinweise, um diese Probleme zu umgehen.

Tools zur Verwaltung der Registry

Neben dem herkömmlichen Tool zur Verwaltung der Registry bieten Windows Server 2008 und Windows Vista weitere Bordmittel, um die Registry zu bearbeiten. Sie finden die ausführliche Hilfe dieser Tools, wenn Sie in der Befehlszeile den Toolnamen mit der Bezeichnung */?* aufrufen. Meistens werden in Unternehmen folgende Befehle verwendet:

Reg.exe – Registry in der Befehlszeile und in Skripts bearbeiten

Hierbei handelt es sich um ein Tool für die Befehlszeile, welches Sie auch in Skripts verwenden können. Das kleine Programm bietet in vielerlei Hinsicht interessantere Fähigkeiten als der grafische Registrierungs-Editor *Regedit*. Mit *Reg.exe* lassen sich zum Beispiel einzelne Schlüsselstrukturen kopieren oder vergleichen. Zudem können Sie auch die Registry eines Rechners im Netzwerk damit anpassen, wenn Sie auf diesem über Administratorrechte verfügen. Sie wollen zum Beispiel auf einem PC für mehrere Benutzer alle Registry-Einstellungen ändern. Dann öffnen Sie zunächst die versteckte Registry-Datei *Ntuser.DAT* des jeweiligen Benutzers. Die Datei finden Sie in dessen Profil-Verzeichnis bei Windows Server 2008 und Windows Vista unter *C:\Users\<Benutzer>*. Geben Sie für

jeden Benutzer einzeln den Befehl *reg load HKU\<Benutzer> <Benutzerordner>\ntuser.dat* ein. Im zweiten Schritt vergleichen Sie alle Einträge eines Schlüssels mit denen Ihres eigenen Profils, indem Sie ebenfalls für jeden Benutzer einzeln die Zeile *reg compare HKU\<Benutzer>\<Schlüssel> HKCU\<Schlüssel> > c:\<Benutzer>.txt* eingeben. Die Unterschiede der beiden Registry-Schlüssel finden Sie anschließend in der Datei *C:\<Benutzer>.txt*. Sie können die einzelnen Dateien einsehen, mit *fc.exe* vergleichen und einzelne Werte in der Registry anpassen, indem Sie die Werte neu setzen. Diese Option führen Sie mit *reg add <Schlüssel> /v <Eintrag> /t <Datentyp> /d <Wert>* durch. Im letzten Schritt entfernen Sie die mit *reg load* hinzugefügten Bereiche wieder aus Ihrer Registrierung, indem Sie für jeden Benutzer einzeln *reg unload HKU\<Benutzer>* eingeben. Der letzte Schritt ist sehr wichtig. Denn wenn Sie ihn vergessen, können die anderen Benutzer sich nicht mehr anmelden, da der Zugriff auf die Registry für sie gesperrt ist.

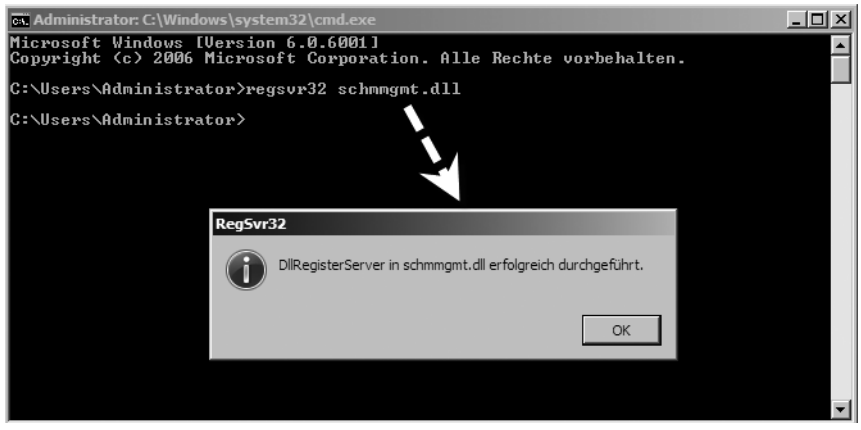
Regini.exe – Berechtigungen der Registry in Skripts setzen

Mit diesem Befehlszeilentool können Sie Berechtigungen für einzelne Werte und Schlüssel steuern. Dieses Tool wird häufig in Skripts verwendet, die Applikationen automatisiert installieren, um sicherzustellen, dass normale Benutzerkonten über die notwendigen Rechte verfügen, die Applikation zu starten. Das Tool dient im Gegensatz von *Reg.exe* nicht dazu die Registry zu bearbeiten, sondern hauptsächlich die Berechtigungen gezielt anpassen zu können. Aber auch wenn Sie Registry-Änderungen auf PCs im Netzwerk verteilen wollen, ist das Tool geeignet. Im Vergleich zu **.reg*-Dateien bietet *Regini* mehr Funktionen, die auch das Löschen von Teilschlüsseln und Datenelementen sowie das Festlegen von Berechtigungen für Registrierungsschlüssel ermöglichen. *Regini* arbeitet mit der Syntax *regini <SkriptDateiName>*. Dabei ist *SkriptDateiName* der Pfad zu einer Skriptdatei, die zur Durchführung einer bestimmten Registrierungsänderung geschrieben wurde. Wenn sich das Skript in einem freigegebenen Netzwerkverzeichnis befindet, kann die UNC (Namenskonvention, Uniform Naming Convention) in der Pfadangabe verwendet werden. Zur Verteilung von Registrierungsänderungen, die mit Hilfe von *Regini* ausgeführt werden, muss das Programm jedem Zielcomputer zugänglich sein (unter Windows Server 2008 und Windows Vista gehört das Tool zu den Bordmitteln).

Regsvr32.exe – DLLs in der Registry anmelden

Regsvr32.exe ist ein Programm zum Registrieren von DLLs (Dynamic Links Libraries) und ActiveX-Steuerelementen (früher als benutzerdefinierte OLE-Steuerelemente bezeichnet) in der Registrierung. Damit zum Beispiel der Schemamaster eines Active Directorys angezeigt werden kann, müssen Sie zunächst das Snap-In registrieren, welches das Schema anzeigt. Aus Sicherheitsgründen wird dieses Snap-In zwar installiert, jedoch nicht angezeigt. Geben Sie über *Start/Ausführen* den Befehl *regsvr32 schmmgmt.dll* ein. Sie erhalten daraufhin die Information, dass die DLL-Datei im System erfolgreich registriert wurde (Abbildung 9.52).

Abbildg. 9.52 Registrieren von neuen DLLs in der Registry von Windows Server 2008



Im Anschluss können Sie das Snap-In *Active Directory-Schema* in eine MMC über *Datei/Snap-In hinzufügen* integrieren. In einigen Fällen kann es vorkommen, dass die Registrierung von einzelnen DLL-Dateien nicht stattfindet oder die eingetragenen Informationen aus der Registry gelöscht wurden. Wenn Ihnen die dafür benötigte DLL bekannt ist, können Sie diese neu in Ihrem System registrieren lassen.

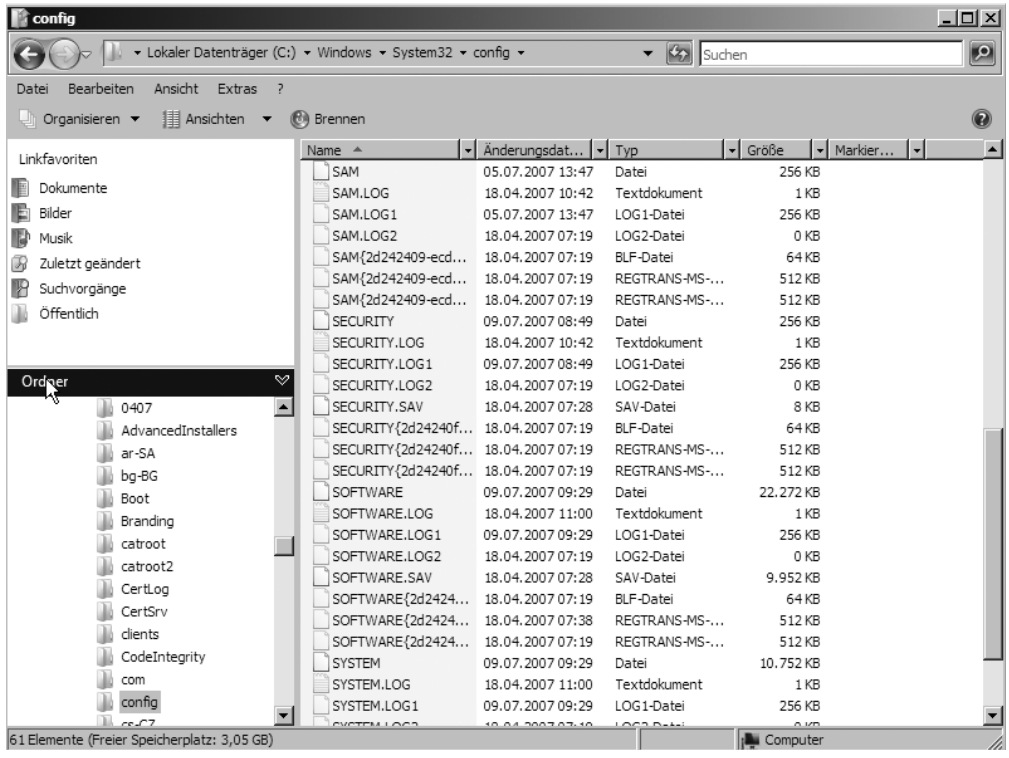
Zusammenspiel zwischen Registry und Systemdateien

Die Einstellungen der Registry sind in verschiedenen Windows-Dateien abgelegt. Diese verschiedenen Dateien haben die folgenden Funktionen:

- **System.dat** Systemkonfiguration
- **User.dat** Benutzerprofil
- **Classes.dat** Dateierweiterungen, Dateitypen und COM-Komponenten
- **Default** Benutzerprofil mit Standardeinstellungen
- **Sam** Security Account Manager (Benutzerkontendatenbank) für die Steuerung der Zugriffs- und Systemberechtigungen
- **Software** Allgemeine Informationen zur Software
- **Usrclass.dat** Benutzerspezifische Softwareeinstellungen
- **Ntuser.dat** Konfigurationseinstellungen des Benutzerprofils

Im Ordner *C:\Windows\System32\config* finden Sie verschiedene Windows-Konfigurationsdateien. Dabei handelt es sich unter anderem um die Dateien *Default*, *Sam*, *Security*, *Software* sowie *System*. Diese Dateien bestimmen die jeweilige Struktur in der Registry. Sie tragen teilweise keine Dateierweiterung. Jedoch gehört zu jeder Datei auch eine gleichnamige **.log*-Datei, zum Beispiel *System* und *System.log*. Diese Dateien spiegeln die Inhalte der jeweiligen Registry-Schlüssel wider.

Abbildg. 9.53 Systemdateien der Registry im *System32*-Verzeichnis der Windows-Installation



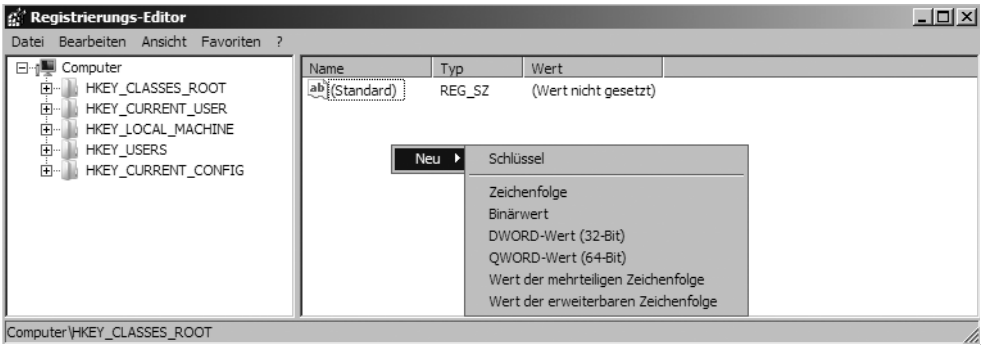
Benutzerinformationen speichert Windows in der Datei *ntuser.dat* unter *C:\Users\<Benutzername>*. In diesem Benutzerordner befindet sich unter *\Appdata\Local\Microsoft\Windows* die Datei *usrclass.dat*. Hier werden die benutzerspezifischen Softwareeinstellungen gespeichert. Diese Einstellungen sind relevant, wenn ein Benutzer Änderungen am Desktop oder am Startmenü vornimmt oder eine bestimmte Applikation nicht für alle Benutzer installiert ist. Den verschiedenen Registry-Schlüsseln sind die einzelnen Dateien direkt zugeordnet und Änderungen, die im Registrierungs-Editor durchgeführt werden, speichert das System in den Dateien:

- **HKEY_LOCAL_MACHINE\SAM** *Sam* und *Sam.log*
- **HKEY_LOCAL_MACHINE\SECURITY** *Security* und *Security.log*
- **HKEY_LOCAL_MACHINE\SOFTWARE** *Software* und *Software.log*
- **HKEY_LOCAL_MACHINE\SYSTEM** *System* und *System.log*
- **HKEY_CURRENT_CONFIG** *System* und *System.log*
- **HKEY_CURRENT_USER** *Ntuser.dat* und *Ntuser.dat.log*
- **HKEY_USERS\.DEFAULT** *Default* und *Default.log*

Die Werte in der Registry

Die Datenwerte in der Registry können verschiedene Typen haben. Klicken Sie im Registrierungs-Editor mit der rechten Maustaste auf einen Schlüssel, können Sie selbst solche Wert erzeugen (Abbildung 9.54).

Abbildg. 9.54 Erstellen von neuen Werten in der Registry



Die hier aufgelisteten Typen können Sie auch zur Erstellung neuer Werte benutzen:

- **Zeichenfolge (REG_SZ)** Dieser Typ beinhaltet Zeichenfolgen (Strings), die entweder Texte oder Zahlenwerte enthalten können. Die Werte dieses Typs müssen grundsätzlich von Anführungszeichen umschlossen sein.
- **Binärwert (REG_BINARY)** Die Länge des Binärwerts ist nach oben hin nicht begrenzt. Die Binärwerte werden beispielsweise von der Systemsteuerung eingepflegt. Die Binärcodierung kann voneinander abweichen. Ändern Sie diese Einträge deshalb besser nicht manuell. Die meisten Informationen zu Hardwarekomponenten sind als binäre Daten gespeichert und werden im Hexadezimalformat angezeigt.
- **DWORD-Wert (32-Bit) (REG_DWORD)** Die Länge dieses Werts darf maximal 32 Bit betragen. Es muss sich dabei um eine Zahl handeln, die in dezimaler oder hexadezimaler Form dargestellt werden kann. Viele Parameter für Gerätetreiber und Dienste haben diesen Typ. Sie können im Binär-, Hexadezimal- oder Dezimalformat angezeigt werden.
- **QWORD-Wert (64-Bit) (REG_QWORD)** Daten, die durch 64 Bit repräsentiert werden. Diese Daten werden als Binärdaten im Registrierungs-Editor angezeigt und seit Windows 2000 verwendet.
- **Wert der mehrteiligen Zeichenfolge (REG_MULTI_SZ)** In einem solchen Wert können mehrere Teilstrings gespeichert werden. Werte, die Listen oder verschiedene Werte in für Benutzer lesbarem Format enthalten, werden oft in dieser Form gespeichert. Einträge werden durch Leerzeichen, Kommas oder andere Trennzeichen voneinander getrennt.
- **Wert der erweiterbaren Zeichenfolge (REG_EXPAND_SZ)** Unter diesem Typ können erweiterbare Daten aufgenommen werden. In aller Regel handelt es sich dabei um Umgebungsvariablen in der Form *%SystemRoot%,* die zur Laufzeit in den aktuellen Pfad erweitert oder aufgelöst werden.

- **REG_FULL_RESOURCE_DESCRIPTOR** Dieser Typ enthält Hardware-Informationen wie IRQ-Angaben oder DMA-Einträge. Die Werte werden standardmäßig in hexadezimaler Form angegeben, können aber auch in anderen Formaten ausgegeben werden.

Der Registrierungs-Editor

Um die Registry einsehen und bearbeiten zu können, verwenden Sie den Registrierungs-Editor. Dieses Programm wird über die Datei *regedit.exe* aufgerufen. Der Registrierungs-Editor hat eine große Ähnlichkeit mit dem Windows-Explorer. Auch seine Handhabung bezüglich Öffnen und Auswahl der Einträge ist identisch. Betrachten Sie die Schlüssel quasi als Ordner und die Werte als Dateien. Jeder *Schlüssel* besteht aus mindestens einem *Wert*. Besitzt ein Schlüssel mehrere Werte, so ist ein Wert als *(Standard)* gekennzeichnet. Für diesen muss jedoch nicht zwangsläufig ein Wert gesetzt sein. Ist dies nicht der Fall, finden Sie in der Spalte *Wert* den Eintrag *(Wert nicht gesetzt)*. Ein Schlüssel kann über mehrere Werte verschiedener Typen verfügen.

Abbildg. 9.55 Anzeigen des Standardwertes eines Registry-Schlüssels

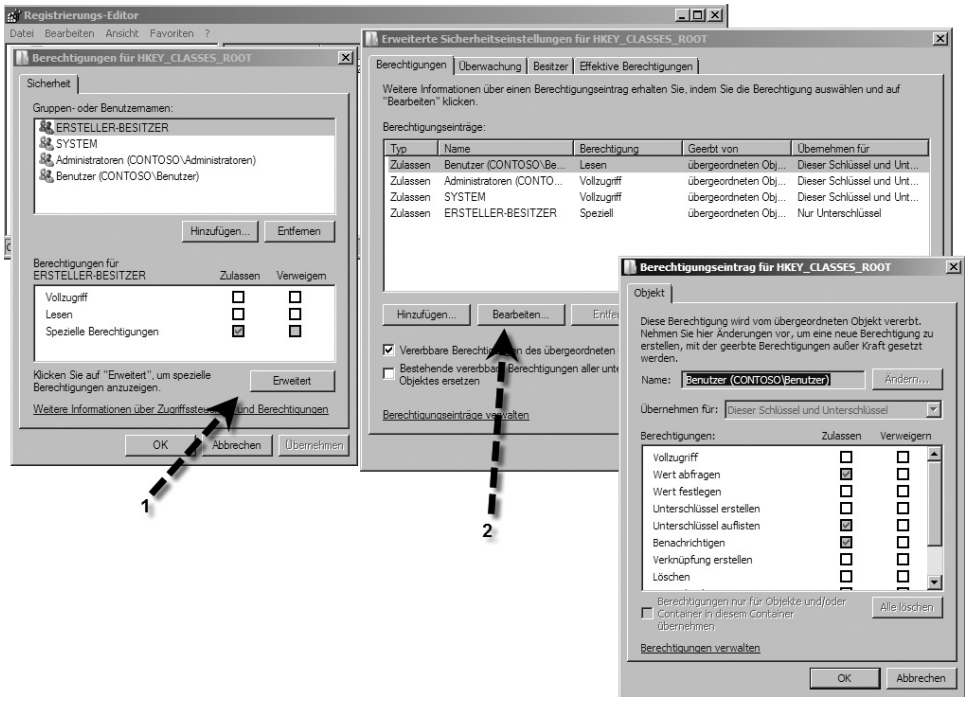
Berechtigungen für die Registry

Im Registrierungs-Editor haben Sie die Möglichkeit, für jeden Schlüssel und Unterschlüssel separat die Berechtigungen für die Benutzer festzulegen. Um für einen Schlüssel die Berechtigungen zu ändern, markieren Sie diesen und wählen entweder den Menübefehl *Bearbeiten/Berechtigungen* oder aus dem Kontextmenü den Eintrag *Berechtigungen*. Dieses Fenster gleicht dem Fenster einer *Zugriffssteuerungsliste (Access Control List, ACL)* für eine herkömmliche Datei oder einen Ordner. Klicken Sie auf die Schaltfläche *Erweitert* und danach auf *Bearbeiten*, können Sie spezielle Berechtigungen für einen Benutzer konfigurieren (Abbildung 9.56). Beim Bearbeiten können Sie eine Reihe spezifischer Berechtigungen festlegen:

- **Vollzugriff** Beinhaltet sämtliche Berechtigungen, einschließlich der Möglichkeit, selbst Berechtigungen zu erteilen
- **Wert abfragen** Werte können ausgelesen werden
- **Wert festlegen** Neue Werte können erstellt werden
- **Unterschlüssel erstellen** Unterschlüssel können erstellt werden
- **Unterschlüssel auflisten** Unterschlüssel können angezeigt werden

- **Benachrichtigungen** Benachrichtigungen von einem Registry-Schlüssel aktivieren oder deaktivieren
- **Verknüpfung erstellen** Erstellen von Verknüpfungen in einem Schlüssel
- **Löschen** Der Schlüssel und/oder Wert kann gelöscht werden
- **DAC schreiben** Für den Schlüssel darf die DACL (Discretionary Access Control List) geschrieben werden. Die DACL ist ein Teil der Zugriffssteuerungsliste (ACL).
- **Besitzer festlegen** Der Besitzer des gewählten Schlüssels darf geändert werden
- **Lesekontrolle** Öffnen der DACL für einen Schlüssel

Abbildg. 9.56 Bearbeiten der Registry-Berechtigungen für Benutzer



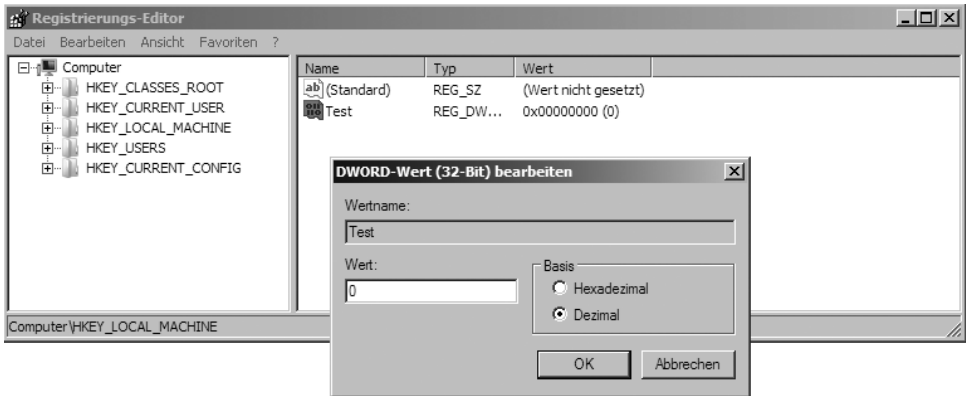
Änderungen an Schlüsseln und Werten vornehmen

Um einen Wert zu ändern, klicken Sie den zum Wert gehörenden Schlüssel in der Baumstruktur doppelt an. Danach können Sie den Wert entweder über das Kontextmenü *Ändern*, das Menü *Bearbeiten/Ändern* oder per Doppelklick öffnen. Achten Sie darauf, dass Sie den alten Wert im Bearbeitungsfenster markieren, bevor Sie ihn ändern. Andernfalls werden die neuen Werte hinzugefügt, was höchstwahrscheinlich zu einer Fehlfunktion des Systems führen wird. Das sich dann öffnende Bearbeitungsfenster variiert je nach gewähltem Wert:

- ***REG_EXPAND_SZ* bearbeiten** Sie können hier den Wert in Form von Umgebungsvariablen angeben, zum Beispiel *%SystemRoot%*. Geben Sie hingegen einen Wert als Text ein, so muss dieser in Anführungszeichen gesetzt werden, z.B. *"C:\Windows"*. Um den Wert zu übernehmen, klicken Sie auf *OK*.

- ***REG_MULTI_SZ* bearbeiten** Hier können mehrere Werte enthalten sein. Jede Zeile stellt einen Teilstring des Wertes dar. Um einen neuen Teilstring einzufügen, geben Sie diesen in eine neue Zeile ein. Bestehende Zeilen werden zum Bearbeiten markiert. Die Trennung der verschiedenen Teilstrings erfolgt automatisch per *Nullbyte*. Bestätigen Sie die Änderungen mit *OK*.
- ***REG_BINARY* bearbeiten** Ein Binärwert kann aus mehreren Bytes bestehen. Die Maximalgröße sollte jedoch 64 KB nicht übersteigen, sodass dieser Typ zum Speichern großer Dateneinträge verwendet wird. Die Darstellung im Registrierungs-Editor erfolgt als Hexbyte/ASCII.
- ***REG_DWORD* bearbeiten** Ein solcher Wert kann maximal eine Größe von 32 Bit haben. Der Wert kann in hexadezimaler und in dezimaler Form angegeben werden. Achten Sie beim Ändern des REG_DWORD-Wertes darauf, dass Sie unter *Basis* die Auswahl *Dezimal* treffen, wenn Sie den Wert in dieser Form eingeben möchten, da standardmäßig die Option *Hexadezimal* ausgewählt ist.

Abbildg. 9.57 Bearbeiten eines DWORD-Wertes im Registrierungs-Editor



Beachten Sie, dass Sie den Typ eines vorhandenen Wertes nicht ändern können. Bei bereits vorhandenen Werten ist dies ohnehin nicht sinnvoll, weil Windows die Werte festgelegt hat. Haben Sie hingegen selbst einen neuen Wert angelegt und diesem einen falschen Typ zugeordnet, so müssen Sie diesen Wert komplett löschen und danach korrekt neu erstellen.

Neue Schlüssel und Werte einfügen

Für einen bestehenden Wert können Sie zusätzliche Unterschlüssel oder Werte hinzufügen. Um einen neuen Schlüssel anzulegen, wählen Sie aus dem Kontextmenü oder dem Menü *Bearbeiten* den Eintrag *Neu/Schlüssel*. Dieser trägt zunächst den Namen *Neuer Schlüssel #1*. Geben Sie den neuen Namen ein. Der Schlüssel besteht zuerst nur aus einem Wert vom Typ *REG_SZ* namens *(Standard)* und einem nicht gesetztem Wert. Um einen neuen Wert hinzuzufügen, wählen Sie aus dem Kontextmenü *Neu* oder dem Menü *Bearbeiten/Neu* einen der beschriebenen Einträge. Bestehende Werte und Schlüssel können auch umbenannt werden. Verwenden Sie dazu entweder den Kontextmenüeintrag *Umbenennen* oder das Menü *Bearbeiten/Umbenennen*. Danach können Sie einen neuen Namen eingeben.

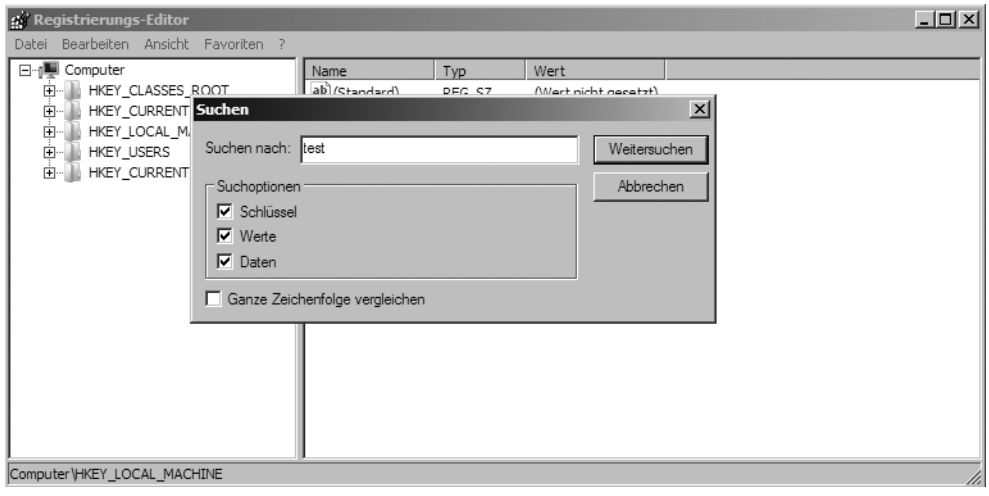
Löschen von Schlüsseln und Werten

Zum Löschen eines Schlüssels oder Werts markieren Sie diesen und wählen entweder den Kontextmenüeintrag *Löschen* bzw. den Menübefehl *Bearbeiten/Löschen* oder drücken die Entf-Taste. In dem folgenden Fenster müssen Sie den Löschvorgang mit einem Klick auf die Schaltfläche *Ja* bestätigen. Handelt es sich beim Löschen um einen Schlüssel, der noch weitere Unterschlüssel umfasst, werden diese ebenfalls alle gelöscht.

Durchsuchen der Registry

Da das Durchsuchen der Registry nach einem bestimmten Wert oder Schlüssel sehr zeitaufwendig werden kann, wenn Sie manuell in der Baumstruktur suchen, bietet die Registry eine eigene Suchfunktion. Um die Registry zu durchsuchen, rufen Sie entweder den Menübefehl *Bearbeiten/Suchen* auf oder drücken die Tastenkombination Strg+F. Es erscheint ein neues Fenster (Abbildung 9.58).

Abbildg. 9.58 Registry im Registrierungs-Editor durchsuchen

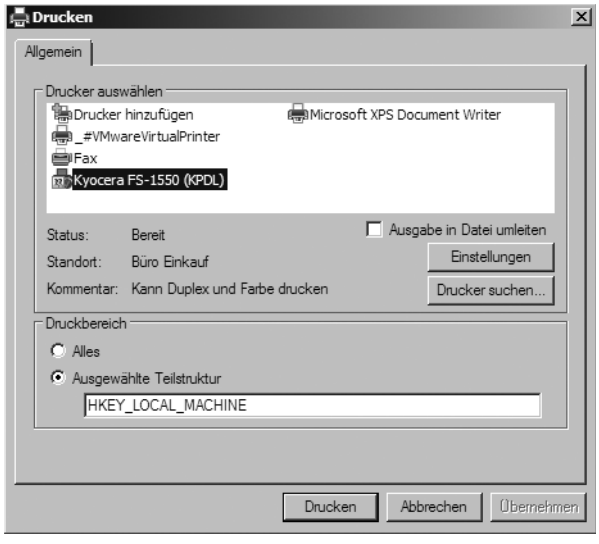


In das Feld *Suchen nach* tragen Sie den Begriff oder einen Teilbegriff ein. Das Zeichen * als Platzhalter ist für die Suche möglich. Weiterhin wählen Sie aus, welche der Optionen *Schlüssel, Werte* oder *Daten* durchsucht werden soll. Verwenden Sie in der Suche nur Teilbegriffe, dürfen Sie das Kontrollkästchen *Ganze Zeichenfolge vergleichen* nicht markieren. Wird ein gesuchter Eintrag gefunden, öffnet der Registrierungs-Editor die Registry an der entsprechenden Stelle und hebt den Eintrag dabei hervor. Sofern mehrere Suchergebnisse gefunden wurden, können Sie die Suche über den Menübefehl *Bearbeiten/Weitersuchen* oder die Taste F3 fortsetzen. Wurde die Registry vollständig durchsucht, erhalten Sie eine Information darüber.

Die Druckfunktion des Registrierungs-Editors

Der Registrierungs-Editor stellt Ihnen die Möglichkeit bereit, die komplette Registry oder einzelne Zweige daraus auszudrucken. Dies kann beispielsweise im Zuge einer Dokumentation sehr hilfreich sein. Markieren Sie im Registrierungs-Editor den gewünschten Schlüssel und rufen Sie den Menübefehl *Datei/Drucken* auf. Sie können die Druckfunktion auch über die Tastenkombination Strg+P aufrufen (Abbildung 9.59). Unter *Druckbereich* ist standardmäßig der Schlüssel eingetragen, den Sie ausgewählt haben. Sie können jedoch auch über die Option *Alles* den kompletten Inhalt der Registry ausdrucken. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf *Drucken*.

Abbildg. 9.59 Teile der Registry über die Druckfunktion ausdrucken



Die Favoritenfunktion des Registrierungs-Editors

Um die Suche nach bereits besuchten Schlüsseln zu erleichtern, stellt der Registrierungs-Editor ähnlich wie der Internet Explorer eine Favoritenfunktion zur Verfügung. Sobald Sie einen Schlüssel markiert haben, auf den Sie häufiger zugreifen müssen, rufen Sie den Menübefehl *Favoriten/Zu Favoriten hinzufügen* auf. Sie werden aufgefordert, einen Namen festzulegen. Standardmäßig ist der Name des Schlüssels eingetragen. Um auf einen Favoriten zuzugreifen, öffnen Sie das Menü *Favoriten* und wählen den gewünschten Eintrag aus. Zum Löschen eines Eintrags klicken Sie auf *Favoriten entfernen*. Wählen Sie dort die gewünschten Einträge aus und klicken auf *OK*.

HINWEIS Die Favoriteneinträge werden in der Registry in dem Schlüssel *HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\Favorites* abgelegt. Auch dort können Sie die Einträge löschen.

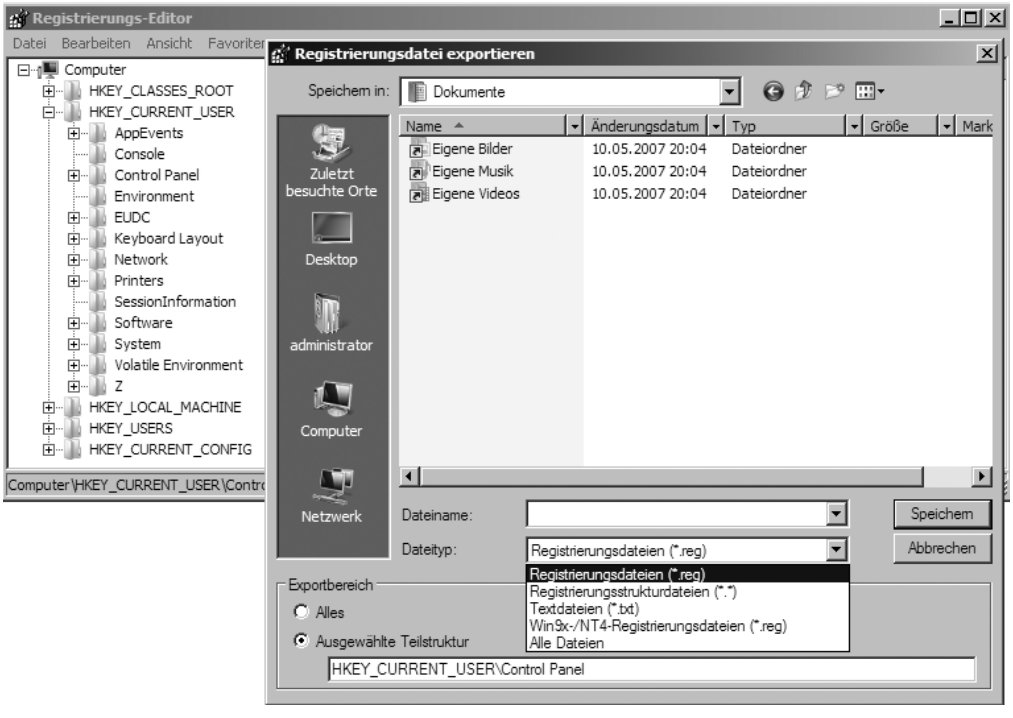
Import und Export von Registry-Schlüsseln

Ein wichtiger Punkt ist auch der Import und Export von Registry-Schlüsseln. Ein Export ist sinnvoll, wenn Sie bestimmte Einträge für spätere Aufgaben, beispielsweise auf einem anderen Computer, nutzen möchten. Zum Einspielen des Exports wird der *Importieren*-Befehl verwendet.

Die Exportfunktion

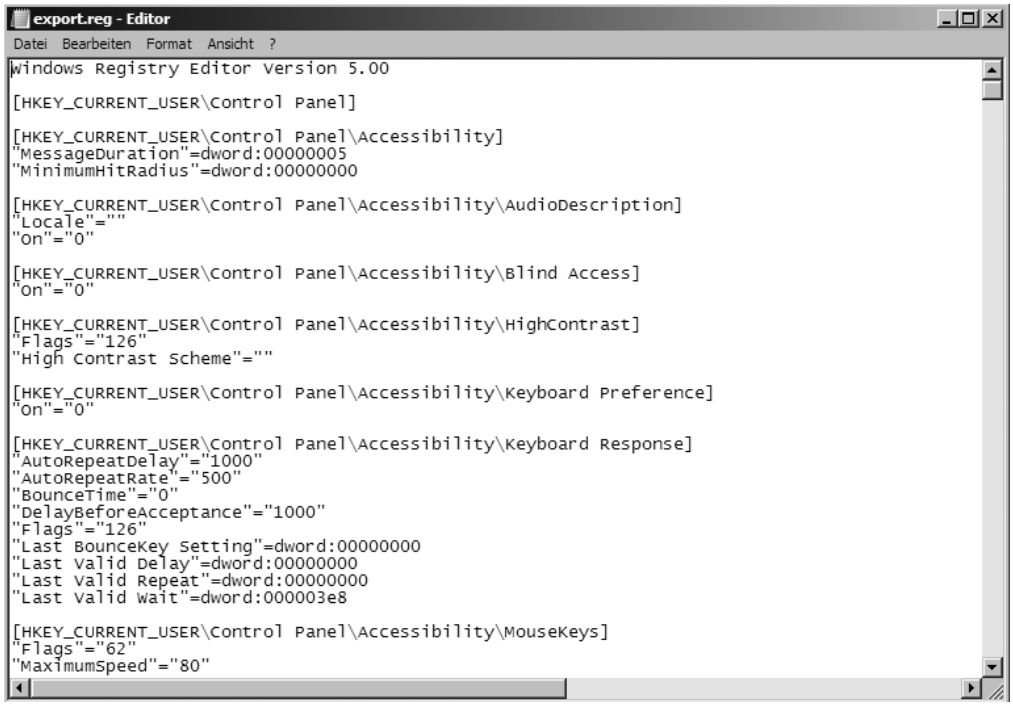
Um einen Schlüssel aus der Registry zu exportieren, markieren Sie diesen und rufen den Menübefehl *Datei*/*Exportieren* auf. Wie beim Speichern einer beliebigen Datei müssen Sie auch hier einen Dateinamen und den Speicherort festlegen. Die Datei wird mit der Dateiendung **.reg* versehen (Abbildung 9.60). Diese Datei können Sie mit jedem beliebigen Texteditor betrachten. Die Datei kann auch als Text- oder Hive-Datei gespeichert werden. Wählen Sie im zweiten Fall den Eintrag *Registrierungsstrukturdateien* aus der Auswahlliste. Dabei handelt es sich um die Binärform der Datei.

Abbildg. 9.60 Exportieren von Teilen der Registry



Führen Sie zum Betrachten einer **.reg*-Datei keinen Doppelklick darauf aus. Ein Doppelklick bewirkt (nach vorheriger Nachfrage) die Installation der Registry-Daten. Wählen Sie stattdessen im Kontextmenü zur Datei den Eintrag *Bearbeiten* aus.

Abbildg. 9.61 Anzeigen und Bearbeiten einer Registry-Exportdatei im Editor von Windows Server 2008



Die Importfunktion

Für den Import von **.reg*-Dateien gibt es verschiedene Möglichkeiten: Sie können entweder im Registrierungs-Editor den Menübefehl *Datei/Importieren* aufrufen und die gewünschte Datei auswählen, auf eine **.reg*-Datei doppelklicken oder im Kontextmenü zur **.reg*-Datei den Eintrag *Zusammenführen* wählen. In den beiden letzten Fällen müssen Sie nur noch die Sicherheitsabfrage bestätigen. Für den Import müssen Sie nicht zwangsläufig vor dem Import einen Export durchgeführt haben. Sie können eine **.reg*-Datei auch direkt erstellen. Dies macht Sinn, wenn Sie selbst bestimmte Schlüssel oder Werte zur Registry hinzufügen möchten, aber Ihnen der Einsatz des Registrierungs-Editors nicht zusagt. Mit Hilfe einer **.reg*-Datei können Sie sämtliche beschriebenen Modifikationen an der Registry vornehmen. Ist beim Import der zu importierende Schlüssel bereits vorhanden, werden die vorhandenen Daten überschrieben. Sind Schlüssel oder Werte noch nicht vorhanden, werden diese der Registry hinzugefügt.

Manuelles Anlegen von **.reg*-Dateien

Um die Struktur zum Anlegen einer eigenen **.reg*-Datei zu verdeutlichen, sehen Sie in Abbildung 9.61 zunächst ein Beispiel. Die oberste Zeile gibt die Version des Registrierungs-Editors an. *5.00* ist die Version unter Windows Server 2008, Windows Vista und Windows XP. Es ist auch möglich, **.reg*-Dateien früherer Versionen zu importieren. Wenn Sie selbst eine **.reg*-Datei schreiben, müssen Sie diese Zeile immer angeben. Ansonsten kann der Import nicht ordnungsgemäß durchgeführt werden. Jeder Schlüssel wird in eine eckige Klammer gesetzt. Unterhalb des Schlüssels finden Sie alle seine zugehörigen Werte. Der Name des Werts wird in Anführungszeichen gesetzt. Hinter dem Gleichheitszeichen werden die Daten des Werts genannt. Die Textstrings der Werte werden dabei wie der Wertname in Anführungszeichen gesetzt. Wird ein spezieller Typ angegeben, erfolgt dies in dem Format *=dword:*.

Sind diese Werte bereits vorhanden, werden sie ersetzt, andernfalls hinzugefügt. Möchten Sie einen bestehenden Schlüssel löschen, benutzen Sie die folgende Syntax:

```
Windows Registry Editor Version 5.00
[-HKEY_LOCAL_MACHINE\SOFTWARE\Neu]
```

Um den Schlüssel mit allen Unterschlüsseln zu löschen, fügen Sie zwischen die eckige Klammer und den Namen des Schlüssels ein Minuszeichen ein. Ist der hier angegebene Schlüssel jedoch nicht vorhanden, so wird er stattdessen neu angelegt. Auf diese Weise können Sie zwar Unterschlüssel löschen, nicht jedoch die Hauptschlüssel der Registry. Möchten Sie einen bestimmten Wert aus einem Schlüssel löschen, verwenden Sie die folgende Syntax:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Neu]
"Wert"=-
```

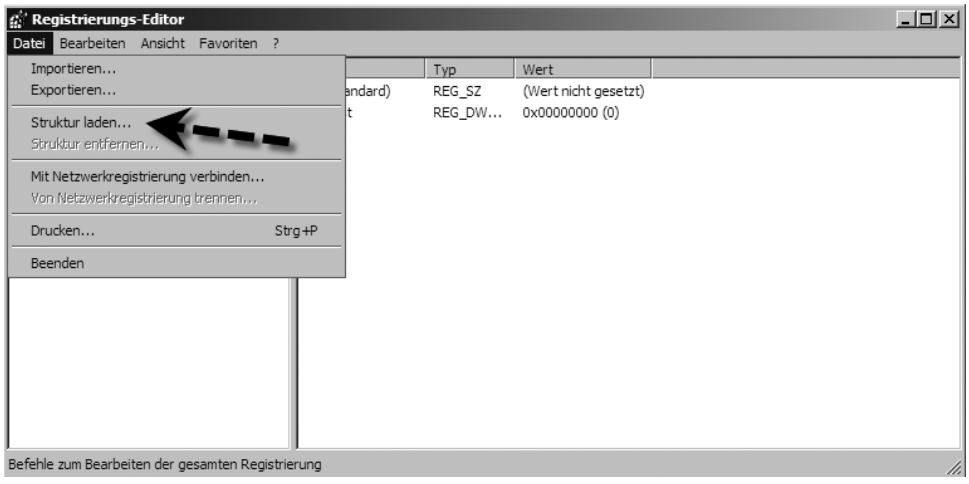
Zum Löschen von Werten geben Sie den Namen des Werts wie gewohnt an. Hinter dem Gleichheitszeichen muss jedoch ein Minuszeichen stehen.

Registry-Strukturen laden

Sie haben die Möglichkeit, über den Registrierungs-Editor Strukturen zu laden oder besser gesagt zu verknüpfen und auch wieder zu entfernen. Das Bearbeiten einer Strukturdatei kann im Registrierungs-Editor durchgeführt werden:

1. Markieren Sie im Registrierungs-Editor zunächst den Schlüssel *HKEY_LOCAL_MACHINE* oder *HKEY_USERS*. Da die Strukturdateien nur auf diese beiden Schlüssel wirken, können Sie für die übrigen Hauptschlüssel keine Struktur laden. Rufen Sie dann den Menübefehl *Datei*/*Struktur laden* auf (Abbildung 9.62).

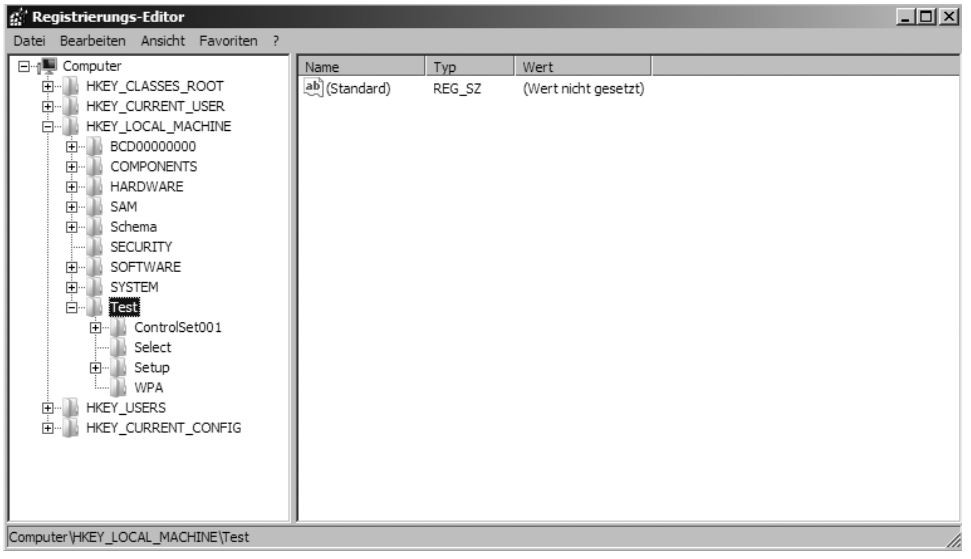
Abbildg. 9.62 Laden von Registry-Strukturen in *regedit.exe*



2. Wählen Sie nun die Strukturdatei aus, die Sie zum Bearbeiten in die Registry laden möchten. Haben Sie den Schlüssel *HKEY_LOCAL_MACHINE* ausgewählt, selektieren Sie nun eine der Strukturdateien, die Sie im Verzeichnis *C:\Windows\System32\Config* finden. Die Wahl der folgenden Dateien ist möglich:
   - **System.dat** Systemkonfiguration
   - **Default** Benutzerprofil mit Standardeinstellungen
   - **Sam** Security Account Manager (Benutzerkontendatenbank) für die Steuerung der Zugriffs- und Systemberechtigungen
   - **Software** allgemeine Informationen zur Software

   Haben Sie hingegen den Schlüssel *HKEY_USERS* gewählt, suchen Sie eine Strukturdatei aus dem Benutzerverzeichnis. Im Ordner *C:\Users\<Benutzername>* befindet sich die Datei *Ntuser.dat* mit den Konfigurationseinstellungen des Benutzerprofils und in diesem Verzeichnis unter *\AppData\Local\Microsoft\Windows* die Datei *usrclass.dat*. In dieser Datei sind die benutzerspezifischen Softwareeinstellungen gespeichert. Da es sich um Dateien handelt, können Sie diese auch von einem anderen Computer im Netzwerk laden und auf dem lokalen Computer bearbeiten.
3. Nachdem Sie eine Strukturdatei ausgewählt haben, erhalten Sie das Fenster *Struktur laden* angezeigt. Geben Sie hier einen Namen ein (beispielsweise *Test*), unter dem die Datei als Schlüssel in der Registry angezeigt werden soll, und klicken auf *OK*. Ist die Datei durch einen anderen Prozess in Benutzung, so kann sie nicht geladen werden und Sie erhalten eine entsprechende Fehlermeldung.

Abbildg. 9.63 Anzeigen der geladenen Registry-Struktur im Registrierungs-Editor



4. Der Inhalt der Strukturdatei wird nun als Schlüssel in der Registry angezeigt. Dort ist der geladene Schlüssel *Test* neben den übrigen Schlüsseln präsent.
5. Nachdem die Struktur geladen worden ist, können Sie diese wie jeden anderen Registry-Schlüssel auch bearbeiten. Die Änderungen werden in die jeweilige Strukturdatei übernommen.
6. Haben Sie die Bearbeitung des Schlüssels abgeschlossen, sollten Sie diesen wieder entfernen. Rufen Sie dazu den Menübefehl *Datei/Struktur entfernen* auf. Achten Sie darauf, dass Sie dabei den korrekten Schlüssel markiert haben, und bestätigen die Sicherheitsabfrage mit *Ja*.

Registry-Bearbeitung im Netzwerk

Die bislang beschriebenen Einstellungen an der Registry wurden lediglich an dem lokalen Computer vorgenommen. Sie haben jedoch auch die Möglichkeit, auf die Registry eines anderen Computers im Netzwerk zuzugreifen und diese zu bearbeiten. Verwenden Sie dazu im Registrierungs-Editor den Menübefehl *Datei/Mit Netzwerkregistrierung verbinden*. Zunächst müssen Sie über die Suchmaske den Zielcomputer auswählen. Nachdem Sie den Computer ausgewählt haben, müssen Sie sich gegebenenfalls an diesem mit einem Benutzernamen und einem Kennwort authentifizieren. Dieses Benutzerkonto muss auf dem Netzwerkcomputer über Administratorberechtigungen verfügen. Danach können Sie auf diesem Computer die Registry bearbeiten.

TIPP Damit der Zugriff auf die Registry eines Computers über das Netzwerk gelingt, muss auf dem Computer, auf den Sie zugreifen wollen, der Systemdienst *Remoteregistrierung* gestartet sein.

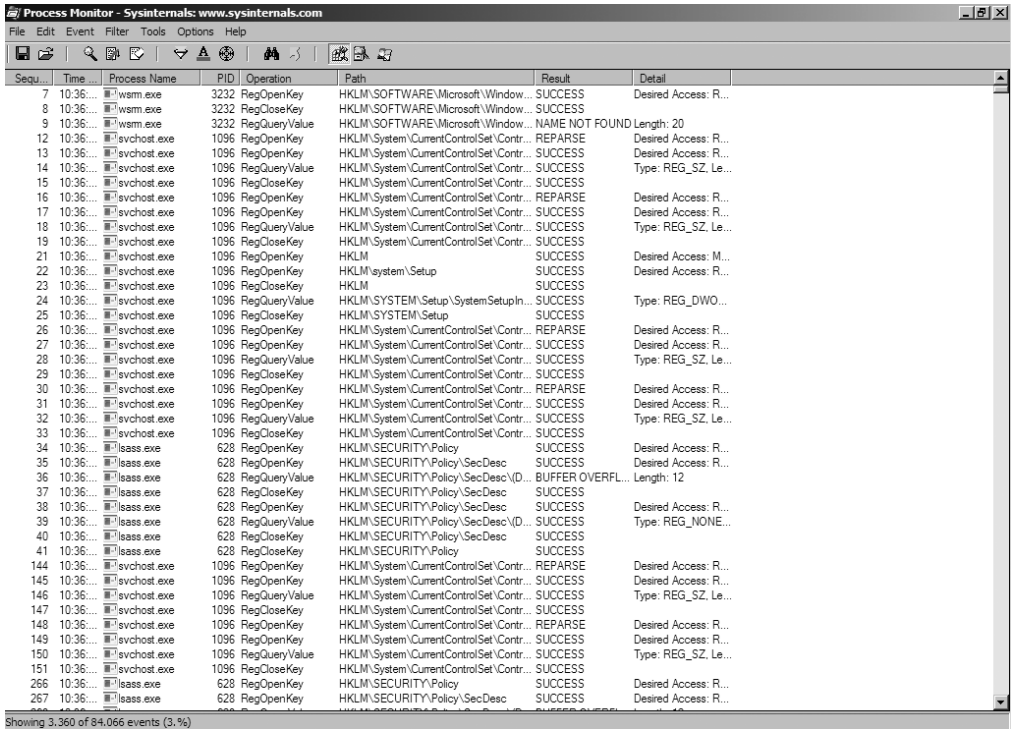
Haben Sie die Arbeiten an der Registry auf dem Netzwerkcomputer abgeschlossen, klicken Sie auf das Menü *Datei/Von Netzwerkregistrierung trennen*. Damit wird verhindert, dass am Netzwerkrechner weitere Registry-Änderungen vorgenommen werden, die sich eigentlich wieder auf den lokalen Rechner beziehen sollten.

RegMon und der Process Monitor

RegMon ist ein kostenloses Überwachungsprogramm für die Registry von Sysinternals (*http://technet.microsoft.com/en-us/sysinternals/bb896652.aspx*). Es arbeitet ähnlich wie *Filemon* – überwacht aber die Registry, keine Dateien. Unter Windows Server 2008 können Sie *Regmon* nicht mehr einsetzen, sondern müssen den *Process Monitor* verwenden, der allerdings identische Funktionen hat. Bei der Bedienung von Windows und Anwendungen erfährt man gewöhnlich nichts von den Aktivitäten der Registry, die im Hintergrund ablaufen. Welches Programm wie oft, auf welche Weise und wann auf die Registry zugreift, kann allerdings sehr informativ sein, wenn man auf die Suche nach Fehlern geht. *RegMon* und der *Process Monitor* helfen dabei, Fehlerquellen in Zusammenhang mit der Registrierdatenbank ausfindig zu machen. Das Tool zeichnet alle Zugriffe auf die Registry auf und zeigt diese in Echtzeit an. Der Anwender erfährt, welches Programm bei welcher Aktion welchen Key der Registry anspricht. Für spätere Arbeiten mit dem Registrierungs-Editor *Regedit* geben die Tools auch über den Pfad des jeweiligen Keys Auskunft. Eine Volltextsuche durch die Aufzeichnungen vervollständigt das Werkzeug. Bei tückischen Fehlermeldungen, die sich auf die Registry zurückführen lassen, ist das Programm dank seiner ausführlichen Aufzeichnungen eine nützliche Hilfe.

Der *Process Monitor* gehört zu den mächtigsten Sysinternal-Tools (*http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx*). Sie können mit diesem Programm und seiner sehr effizienten grafischen Oberfläche ausführlich in Echtzeit alle Aktivitäten im Dateisystem, der Registry und der Prozesse/Threads anzeigen lassen. Das Tool vereint zwei Standardprogramme von Sysinternals *FileMon* und *RegMon*. Sie können Filter erstellen und so nach SID oder Benutzernamen filtern lassen. Mit dem Programm können Sie zum einen optimal Fehler auf Servern beheben, aber auch Malware und Viren auf PCs finden. Das Programm läuft unter Windows 2000/XP/2003 und Windows Server 2008 sowie Windows Vista, auch auf allen 64-Bit-Versionen dieser Betriebssysteme. Schauen Sie sich das Tool an und beschäftigen Sie sich damit. Im Forum auf der Sysinternal-Seite und in der Hilfe des Programms erhalten Sie zahlreiche weiterführende Informationen. Sie können zum Beispiel über die drei Schaltflächen auf dem Startfenster die einzelnen Überwachungsfunktionen durch einen Klick aktivieren oder deaktivieren.

Abbildg. 9.64 Überwachen der Registry mit dem Process Monitor von Sysinternals



Sequ...	Time ...	Process Name	PID	Operation	Path	Result	Detail
7	10:36:...	wsrm.exe	3232	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
8	10:36:...	wsrm.exe	3232	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
9	10:36:...	wsrm.exe	3232	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 20
12	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
13	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
14	10:36:...	svchost.exe	1096	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
15	10:36:...	svchost.exe	1096	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
17	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
18	10:36:...	svchost.exe	1096	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
19	10:36:...	svchost.exe	1096	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
21	10:36:...	svchost.exe	1096	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
22	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\system\Setup	SUCCESS	Desired Access: R...
23	10:36:...	svchost.exe	1096	RegCloseKey	HKLM	SUCCESS	
24	10:36:...	svchost.exe	1096	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWO...
25	10:36:...	svchost.exe	1096	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	
26	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
27	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
28	10:36:...	svchost.exe	1096	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
29	10:36:...	svchost.exe	1096	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
30	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
31	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
32	10:36:...	svchost.exe	1096	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
33	10:36:...	svchost.exe	1096	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
34	10:36:...	lsass.exe	628	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: R...
35	10:36:...	lsass.exe	628	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
36	10:36:...	lsass.exe	628	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	BUFFER OVERFL...	Length: 12
37	10:36:...	lsass.exe	628	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
38	10:36:...	lsass.exe	628	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
39	10:36:...	lsass.exe	628	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	SUCCESS	Type: REG_NONE...
40	10:36:...	lsass.exe	628	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
41	10:36:...	lsass.exe	628	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
144	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
145	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
146	10:36:...	svchost.exe	1096	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
147	10:36:...	svchost.exe	1096	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
148	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
149	10:36:...	svchost.exe	1096	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
150	10:36:...	svchost.exe	1096	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
151	10:36:...	svchost.exe	1096	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
266	10:36:...	lsass.exe	628	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: R...
267	10:36:...	lsass.exe	628	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...

Zusammenfassung

Mit den neuen Gruppenrichtlinien sowie deren Möglichkeiten, die Installation von USB-Sticks zu verhindern, profitieren Unternehmen von verbesserten Leistungen der Arbeitsstationen und einer erhöhten Sicherheit. Es ist ohne zusätzliche Werkzeuge möglich, im Unternehmen den Datendiebstahl per USB-Stick zu verhindern. Größere Unternehmen profitieren von den neuen Dateiformaten der Gruppenrichtlinien und deren verbesserter Replikation. Im nächsten Kapitel zeigen wir Ihnen, wie Sie Benutzer in Windows Server 2008-Netzwerken verwalten und welche Änderungen es im Bereich der Benutzerprofile und der Ordnerumleitungen mit Gruppenrichtlinien gibt.

Kapitel 10

Benutzerverwaltung

In diesem Kapitel:

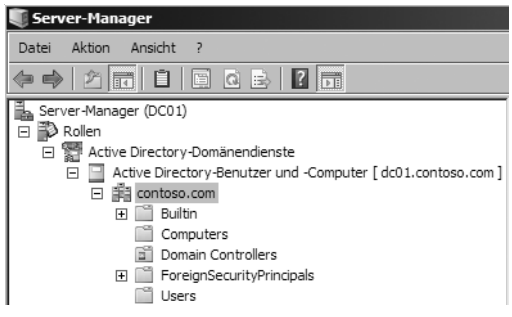
Die Benutzerverwaltung in Windows Server 2008 ist im Vergleich zu Windows Server 2003 etwas komplexer geworden. In den einzelnen Verzeichnissen von Benutzerprofilen gibt es jetzt deutlich mehr Unterscheidungen und es gibt mehr Möglichkeiten, Ordner auf Freigaben im Netzwerk umzuleiten. Die grundsätzliche Verwaltung von Benutzern ist allerdings noch recht ähnlich zu Windows Server 2003. Die Verwaltung von Benutzern ist für allein stehende Server ebenso wichtig wie für Mitgliedsserver in einer Active Directory-Domäne. Die Verwaltung von Benutzern einer Domäne findet mit dem Snap-In *Active Directory-Benutzer und -Computer* statt. Lokale Benutzerkonten verwalten Sie über den lokalen Benutzermanager, den Sie über *Start/Ausführen/lusrmgr.msc* starten.

Die Standard-Container im Active Directory

Im Active Directory findet sich eine Reihe von vordefinierten Containern. Die nachfolgende Betrachtung konzentriert sich auf die fünf Standardcontainer. Ein Container ist eine Gliederungseinheit. Domänen sind ebenso wie Organisationseinheiten Container, in denen andere Objekte wie Benutzer oder Gruppen enthalten sein können. Die Standardcontainer im Active Directory sind nicht als Organisationseinheiten definiert, weshalb bestimmte Funktionen wie die Zuordnung von Gruppenrichtlinien dafür nicht zur Verfügung stehen. Bei einer intensiveren Beschäftigung mit dem Active Directory ist zudem wichtig, dass die LDAP-Namen dieser Container **cn**=*users,dc=contoso,dc=com* und nicht **ou**=*users,dc=contoso,dc=com* lauten, weil es eben keine Organisationseinheiten sind. Das zu wissen, kann, wenn Sie einmal LDAP-Namen eingeben müssen, einiges an Sucharbeit und Ärger ersparen. Die Container haben folgende Funktionen:

- Im Container *Builtin* finden sich vom System vordefinierte Gruppen.
- Der Container *Computers* enthält Objekte für alle Computer, die in die Domäne aufgenommen worden sind. Jeder Computer wird mit einem eigenen Objekt im Active Directory verwaltet. Computer können zu Gruppen zusammengefasst werden.
- Im Container *Domain Controllers* finden sich Objekte für alle Domänencontroller der Domäne. Für diesen Container gibt es eine eigene Gruppenrichtlinie, die besondere Sicherheitseinstellungen für die Domänencontroller konfiguriert. Daher wurden diese von den übrigen Computern getrennt.

Abbildg. 10.1 Die Standard-Container in der Active Directory-Verwaltung verstehen



- Der Container *ForeignSecurityPrincipals* enthält Informationen über SIDs, die mit Objekten aus entfernten, vertrauten Domänen verbunden sind.

- Im Container *Users* stehen die Benutzer und Gruppen, die vom Windows Server 2008 automatisch angelegt werden. Es können weitere Benutzer und Gruppen eingerichtet werden. Der wichtigste Container von Active Directory für die Administration ist zunächst der Ordner *Users*. Allerdings muss gut überlegt werden, in welchem Maß Sie dort neue Benutzer und Gruppen anlegen oder stattdessen von Beginn an mit Organisationseinheiten arbeiten, um die Informationen sauber zu strukturieren.

Die Gruppen im Container *Builtin*

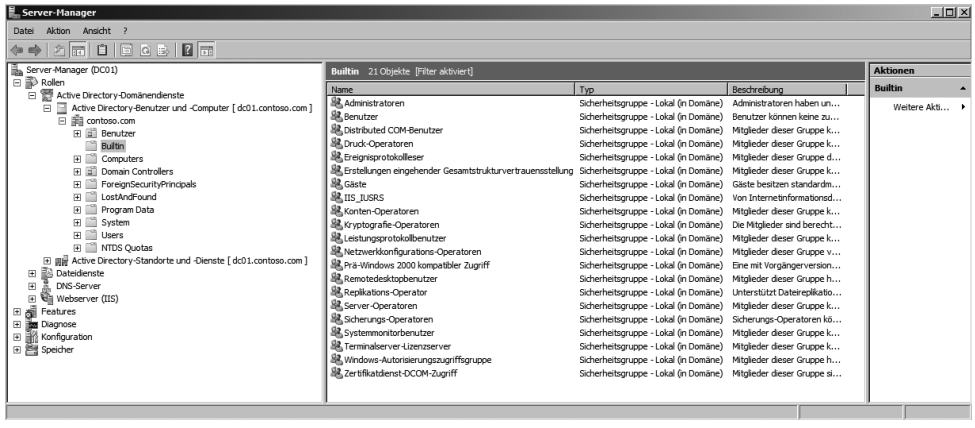
Im Gegensatz zu anderen Gruppen können die vordefinierten Gruppen im Container *Builtin* weder gelöscht noch umbenannt werden. Es können die Zuordnungen von Benutzern und Gruppen angepasst werden. Folgende Gruppen werden in diesem Bereich definiert:

- **Administratoren** Diese Gruppe hat Vollzugriff auf den Computer beziehungsweise auf die Domäne. Es handelt sich um die lokale Gruppe der Administratoren. Wie weit sich deren Rechte erstrecken, ist davon abhängig, ob es sich um einen Domänencontroller oder um einen Mitglieds- beziehungsweise allein stehenden Server handelt. Im ersten Fall haben die Mitglieder Vollzugriff auf die Domäne – nicht andere Domänen in der Struktur –, im zweiten Fall dagegen nur Vollzugriff auf das lokale System. Wird ein Server in eine Domäne aufgenommen, wird während dieses Prozesses die Gruppe *Domänen-Admins* in die Gruppe der lokalen *Administratoren* aufgenommen.
- **Benutzer** Die Mitglieder dieser Gruppe haben Benutzerrechte im System. Sie können mit dem System arbeiten und Dokumente speichern. Sie können aber keine Programme installieren oder kritische Anpassungen an Einstellungen des Systems vornehmen. Bei Servern haben die Mitglieder dieser Gruppe allerdings im Regelfall nur das Recht, über das Netzwerk zuzugreifen. Sie dürfen sich dagegen nicht lokal anmelden. Wird ein Server in eine Domäne aufgenommen, wird während dieses Prozesses die Gruppe *Domänen-Benutzer* in die Gruppe der lokalen *Benutzer* aufgenommen.
- **Distributed COM-Benutzer** Mitglieder dieser Gruppe dürfen die Komponentendienste verwalten und Komponenten für diese Verwaltung hinzufügen und verwalten. Diese Dienste werden hauptsächlich für interaktive Webanwendungen benötigt.
- **Druck-Operatoren** Die Mitglieder dieser Gruppe können Drucker verwalten und installieren.
- **Ereignisprotokollleser** Mitglieder dieser Gruppe haben das Recht, das lokale Ereignisprotokoll zu lesen.
- **Erstellungen eingehender Gesamtstrukturvertrauensstellung** Mitglieder dieser Gruppe dürfen Vertrauensstellungen zwischen verschiedenen Gesamtstrukturen erstellen.
- **Gäste** Mitglieder dieser Gruppe können mit dem Computer arbeiten und Dokumente speichern. Die Gruppe sollte allerdings aus Gründen der Sicherheit nicht verwendet werden. Das zugehörige Benutzerkonto *Gast* ist deaktiviert.
- **IIS_IUSRS** Diese Gruppe wird durch IIS zur Authentifizierung verwendet. Das neue anonyme Konto *IIS_IUSR* ist direkt integriert, was bedeutet, dass sich das Ablaufen der Kennwörter nicht auf das Konto auswirkt und dass auch keine Kennwortsynchronisierung zwischen Computern erforderlich ist. Die neue Gruppe *IIS_IUSRS* ersetzt die Gruppe *IIS_WPG* und ist automatisch in die Identität des Arbeitsprozesses integriert. Durch *IIS_IUSR* und *IIS_USRS* lassen sich Anwendungsinhalte, in denen Zugriffssteuerungslisten (ACLs) für das anonyme IIS-Konto und die

anonyme IIS-Gruppe definiert werden, schnell und einfach auf einen anderen IIS-Server kopieren, ohne dass zusätzliche Schritte zur Beibehaltung der Sicherheitseinstellungen notwendig wären.

- **Konten-Operatoren** Die Mitglieder dieser Gruppe können Benutzer und Benutzergruppen in der Domäne sowie Computerkonten verwalten.
- **Kryptografie-Operatoren** Mitglieder dieser Gruppe verfügen über administrative Berechtigungen für Zertifikate und deren Ausstellung der lokalen Zertifizierungsstelle.
- **Leistungsprotokollbenutzer** Die Mitglieder dieser Gruppe verfügen über Remotezugriffsrechte, um die Protokollierung von Leistungsindikatoren auf dem lokalen System planen zu können.
- **Netzwerkkonfigurations-Operatoren** Dieser Gruppe sind verschiedene Administrationsrechte zur Verwaltung von Netzwerkfunktionen zugeordnet. Sie können damit wichtige Bereiche der Netzwerkkonfiguration wie Protokolleinstellungen anpassen, ohne allerdings umfassendere Berechtigungen im System zu erhalten.

Abbildg. 10.2 Die Standardgruppen im Active Directory



- **Prä-Windows 2000 kompatibler Zugriff** Wie der Name der Gruppe bereits sagt, handelt es sich um eine Gruppe, die speziell für die Kompatibilität mit Vorgängerversionen erstellt wurde. Sie erlaubt einen Zugriff, der kompatibel mit Windows NT 3.x und Windows NT 4.0 ist und den dortigen Zugriffsberechtigungen für die Gruppe *Benutzer* exakt entspricht. Hintergrund ist, dass einige Sicherheitseinstellungen ab Windows 2000 deutlich enger definiert wurden. Das führt dazu, dass Zugriffe von älteren Clients in verschiedenen Situationen nicht mehr funktionieren würden. Da die Delegation von Berechtigungen bei Windows NT 4.0 nicht in der Form wie im Active Directory zur Verfügung steht, wurde diese Gruppe entwickelt. Sobald sich ein älterer Client anmeldet, wird seine SID in dieser Gruppe eingefügt. Über die Gruppe können Zugriffsprobleme für ältere Clients gelöst werden, indem erforderliche Berechtigungen an die Gruppe delegiert werden.
- **Remotedesktopbenutzer** Mitglieder dieser Gruppe haben die Berechtigung, über den Remotedesktop – die administrative Variante der Terminaldienste – auf den Computer zuzugreifen und entsprechend ihrer lokalen Berechtigungen darauf zu arbeiten und Anpassungen an der Systemkonfiguration vorzunehmen. Die Mitgliedschaft in dieser Gruppe berechtigt nur zum Zugriff, ohne weitergehende Berechtigungen für die Systemadministration zu geben. Diese werden wei-

terhin durch Berechtigungen im Dateisystem, im Active Directory und anderen Bereichen des Systems gesteuert.

- **Replikations-Operator** Die Mitglieder dieser Gruppe können die Dateireplikation zwischen Servern steuern.
- **Server-Operatoren** Die Mitglieder dieser Gruppe können Domänencontroller verwalten.
- **Sicherungs-Operatoren** Die Sicherungs-Operatoren können Dateien mit Hilfe von Backup-Programmen sichern.
- **Systemmonitorbenutzer** Die Mitglieder dieser Gruppe dürfen den Systemmonitor benutzen und die Leistungsüberwachung auf dem lokalen System konfigurieren.
- **Terminalserver-Lizenzserver** Diese spezielle Gruppe wird für den Betrieb des Terminalserver-Lizenzservers benötigt, um diesem Zugriffsberechtigungen auf dem lokalen System einzuräumen.
- **Windows-Autorisierungszugriffsgruppe** Hinter diesem Begriff verbirgt sich eine Gruppe, mit der Benutzer die berechneten Gruppenzugehörigkeiten von anderen Benutzern erfragen können. Das wird teilweise von Anwendungen im Bereich der Autorisierung benötigt. Mitglieder sind spezielle Konten, in deren Kontext um Dienste ausgeführt werden.
- **Zertifikatdienst-DCOM-Zugriff** Mitglieder dieser Gruppe dürfen die Zertifikatsdienste verwalten und Verbindung aufbauen.

Die Objekte in den Containern *Computers* und *Domain Controllers*

Die beiden Container *Computers* und *Domain Controllers* werden verwendet, um die Objekte, mit denen Computer im Active Directory abgebildet werden, zu speichern. Hintergrund ist, dass erst die Gruppenrichtlinien angewendet werden können, für deren Steuerung die Computerobjekte unter anderem wichtig sind. Während der Container *Domain Controllers* unverändert belassen werden sollte, kann der Container *Computers* durchaus angepasst werden. Es macht wenig Sinn, in einer größeren Domäne womöglich Tausende von Computerobjekten in einem einzigen Container zu verwalten.

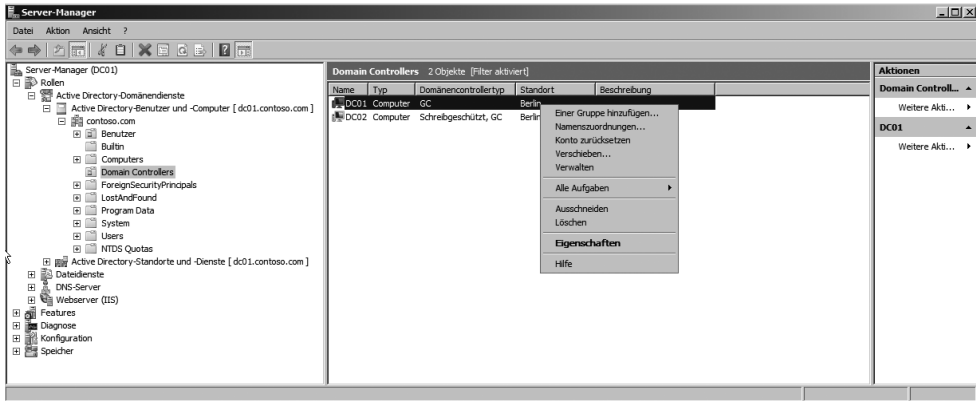
Der Container *Domain Controllers*

Windows Server 2008 unterscheidet bei den Computer-Objekten zwischen Domänencontrollern und anderen Computern. Andere Computer können sowohl Windows Server 2008, Windows Server 2003, Windows 2000 Server sowie Windows NT 4.0 als Clients, die Mitglied einer Domäne sind, sein. Als Clients werden sowohl Windows XP, Windows 2000 Professional, Windows NT 4.0 und Windows Vista unterstützt. Alle Plattformen benötigen Computer-Objekte. Die Unterscheidung zwischen normalen Computern und Domänencontrollern in unterschiedlichen Containern ist sinnvoll, weil dadurch unterschiedliche Sicherheitsrichtlinien auf diese Systeme angewendet werden können. Domänencontroller sollten in der Regel nicht von einschränkenden Richtlinien, die für die Arbeitsstationen von Endanwendern definiert werden, betroffen sein. Das wird durch die Verwaltung der Domänencontroller in einer eigenen organisatorischen Einheit und die Definition spezieller Gruppenrichtlinien für diese Systeme erreicht. Für die Objekte in der Gruppe *Domain Controllers* können eine Reihe von Befehlen ausgeführt werden. Die wichtigsten sind (Abbildung 10.3):

- Mit dem Befehl *Verschieben* können Objekte in einen Container der gleichen Domäne verschoben werden

- Mit *Verwalten* kann das Programm *Computerverwaltung* für das ausgewählte Objekt aufgerufen werden.
- Der Befehl *Eigenschaften* zeigt die Detailinformationen zu einem Objekt an.
- Der Befehl *Konto zurücksetzen* wird zwar im Kontextmenü dieser Objekte angeboten, kann aber nicht genutzt werden, da die Verwaltung von Kennwörtern bei Domänencontrollern durch das System erfolgt. Das Zurücksetzen von Kennwörtern für Domänencontroller erfolgt durch das Befehlszeilen-Tool *netdom* und dem Befehl *netdom resetpwd /server:<Ein Domänencontroller der Domäne der noch funktioniert> /userd:<Administratorkonto der Domäne> /passwordd:<Kennwort des Administrators>*.

Abbildg. 10.3 Kontextmenü von Domänencontrollern anzeigen



Die wichtigsten Administratorkonten im Active Directory

In Active Directory gibt es verschiedene Administratorengruppen, die über unterschiedliche Berechtigungen verfügen. Nur wenn ein Konto in allen wichtigen Administratorgruppen Mitglied ist, verfügt es über umfassende Rechte im Active Directory. Diese Gruppen befinden sich im Container *Users* des Snap-Ins *Active Directory-Benutzer und -Computer* (Abbildung 10.4). Im folgenden Abschnitt besprechen wir diese Gruppen ausführlicher, damit Sie die Auswirkungen verstehen, wenn Sie einen Anwender als Mitglied einer dieser Gruppen aufnehmen.

- **Domänen-Admins** enthalten die Administratoren, welche die lokale Domäne verwalten und umfassende Rechte in dieser Domäne haben. Ein Administrator ist jeweils nur für eine Domäne zuständig. Wenn Sie mehrere Domänen in einer Gesamtstruktur anlegen, gibt es mehrere Benutzerkonten Administrator, die jeweils zu einer Domäne gehören und nur in dieser einen Domäne volle administrative Berechtigungen besitzen. Domänen-Admins haben in einer Domäne umfassendere Rechte als Organisations-Admins.
- **Organisations-Admins** sind eine spezielle Gruppe von Administratoren, die Berechtigungen für alle Domänen im Active Directory besitzen. Sie haben auf Ebene der Gesamtstruktur die meisten Rechte, aber in einzelnen Domänen haben die Domänen-Admins mehr Rechte. Organisations-Admins gibt es nur in der Root-Domäne.

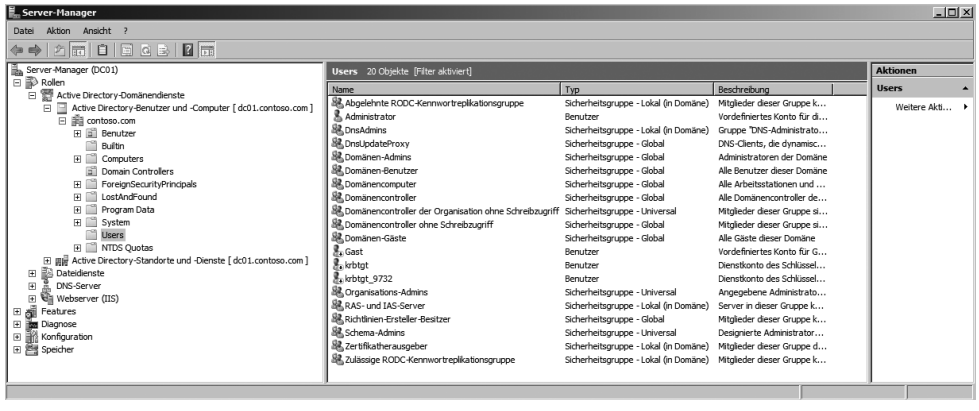
- **Schema-Admins** sind eine der kritischsten Gruppen überhaupt. Mitglieder dieser Gruppe dürfen Veränderungen am Schema von Active Directory vornehmen. Produkte, die das Schema von Active Directory erweitern, wie zum Beispiel Exchange Server 2007, können nur installiert werden, wenn der installierende Administrator in dieser Gruppe Mitglied ist.

HINWEIS Das Konto *Administrator* in der ersten installierten Domäne einer Gesamtstruktur ist das wichtigste und kritischste Konto im gesamten System. Es erlaubt den administrativen Zugriff auf alle wichtigen Systemfunktionen und ist Mitglied aller beschriebenen Administratorengruppen. Einige der Gruppen sind nur in der ersten Domäne, die in der Gesamtstruktur eingerichtet wurde, definiert. Andere Gruppen werden erst nach der Installation bestimmter Dienste, wie DNS und DHCP, auf Domänencontrollern erstellt. Sie werden nicht erstellt, wenn DNS und DHCP auf allein stehenden Servern installiert werden.

Vor allem in Gesamtstrukturen sind diese Standardgruppen in der Root-Domäne besonders wichtig:

- *DHCP-Administratoren* dürfen DHCP-Server in der Domäne verwalten. Die Gruppe wird nach der Installation des ersten DHCP-Servers auf einem Domänencontroller der Domäne erstellt.
- *DHCP-Benutzer* enthält Benutzerkonten, die lesend auf die Informationen des DHCP-Dienstes zugreifen, aber keine Änderungen vornehmen dürfen. Diese Gruppe ist nur für Administratoren und Operatoren, nicht für normale Benutzer oder Computer relevant. Computer, die DHCP-Adressen anfordern, müssen darin nicht aufgenommen werden.

Abbildg. 10.4 Die wichtigsten Standardkonten in Active Directory werden in der OU Users zusammengefasst



- Die Gruppe *DnsAdmins* enthält die Administratoren für DNS-Server. Dieser Gruppe sind keine Benutzer zugeordnet. Sie kann verwendet werden, um die Administration von DNS-Servern zu delegieren. Das ist vor allem dann von Bedeutung, wenn die DNS-Infrastruktur eines Unternehmens von Administratoren verwaltet wird, die nicht für die Active Directory-Umgebung zuständig sind. Diese Gruppe wird erst angelegt, wenn ein DNS-Server auf einem Domänencontroller erstellt wurde, der seine Informationen im Active Directory verwaltet.
- In der Gruppe *DnsUpdateProxy* befinden sich Computer, die als Proxy für die dynamische Aktualisierung von DNS-Einträgen fungieren können. Diese Gruppe steht nur zur Verfügung, wenn

ein Domänencontroller angelegt wird. In diese Gruppe können Sie zum Beispiel DHCP-Server aufnehmen, die dynamische DNS-Einträge für die Clients auf den DNS-Servern erstellen sollen.

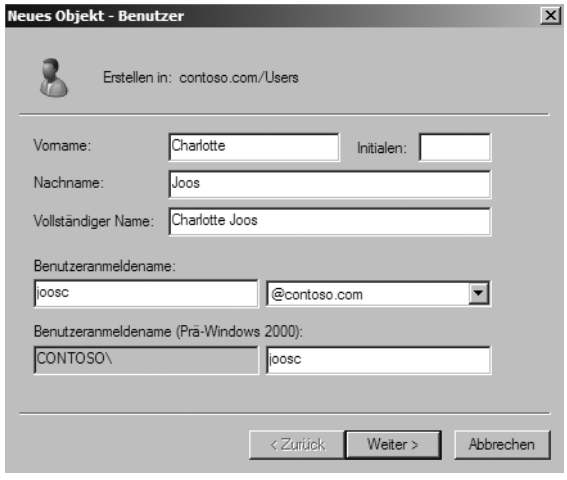
- Die Gruppe *Richtlinien-Ersteller-Besitzer* umfasst die Anwender, die Gruppenrichtlinien für die Domäne erstellen dürfen. Das können Administratoren sein, die sich nur um diese Aufgabe in der Gesamtstruktur kümmern.
- Die Gruppe *WINS Users* wird angelegt, wenn es einen WINS-Server auf einem der Domänencontroller gibt. In ihr befinden sich die Benutzer, die nur Leserechte auf die WINS-Datenbank haben.
- Neben der Konfiguration auf den Terminalservern können Sie auch über Gruppenrichtlinien steuern, welche Anwendungen über *TS Web Access* zur Verfügung gestellt werden. Diese Möglichkeit macht vor allem bei größeren Unternehmen Sinn, die zahlreiche Terminalserver einsetzen. Wollen Sie diese Konfiguration nicht über das Active Directory und die Gruppenrichtlinien abwickeln, können Sie die notwendigen Einstellungen auch direkt auf den Terminalservern durchführen. Sie können auch über TS Web Access einige Einstellungen an der Oberfläche vornehmen, allerdings wird die Verwaltungsoberfläche erst dann eingeblendet, wenn Sie das Konto des Administrators in die lokale Gruppe *TS Web Access Administrators* auf dem TS Web Access Server hinzufügen.
- *WSS_ADMIN_WPG* Mitglieder dieser Gruppe verfügen über Administratorberechtigungen für die SharePoint Services.

Die Gruppen *DnsUpdateProxy, Organisations-Admins, Schema-Admins* und *DnsAdmins* werden in der ersten Domäne, die in einer Gesamtstruktur eingerichtet wird, definiert. Das ist gleichzeitig die oberste Domäne der ersten Struktur der Gesamtstruktur. Einer Gruppe können Benutzer und Benutzergruppen aus unterschiedlichen Domänen der Struktur hinzugefügt werden.

Active Directory-Benutzerverwaltung

Um einen Benutzer anzulegen, wählen Sie im ersten Schritt die *Organisationseinheit (Organizational Unit, OU)* aus, in der dieser Benutzer definiert werden soll. Im Kontextmenü dieses Containers können Sie im Untermenü *Neu* den Befehl *Benutzer* auswählen, um einen Assistenten zu starten, der Sie durch die Einrichtung des Benutzers führt (Abbildung 10.5). Im ersten Dialogfeld werden die Namensinformationen für diesen Benutzer festgelegt. Hier können der Vorname, ein oder mehrere Mittelinitialen und der Nachname angegeben werden. Windows Server 2008 bildet daraus automatisch den vollständigen Namen, der bearbeitet werden kann. Der Benutzeranmeldename ist der Name, mit dem sich der Benutzer im System anmeldet. Der Benutzeranmeldename kann als DNS-Name für Windows Server 2008 und als NetBIOS-kompatibler Name gebildet werden. Normalerweise melden sich die Benutzer über den NetBIOS-Namen an. Der NetBIOS-Name darf eine Länge von bis zu 20 Zeichen haben und muss innerhalb der Domäne eindeutig sein. Es kann mehrere Benutzer mit dem gleichen Benutzernamen in unterschiedlichen Domänen der Gesamtstruktur geben.

Abbildg. 10.5 Erstellen eines neuen Benutzerkontos unter Windows Server 2008



Durch Auswahl der Schaltfläche *Weiter* wechseln Sie zur zweiten Seite des Assistenten. Dort können Sie die Einstellungen für das Kennwort konfigurieren. Darunter finden Sie vier Kontrollkästchen (Abbildung 10.6):

- Wenn das Kontrollkästchen *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* aktiviert ist, muss der Benutzer bei der ersten Anmeldung ein neues Kennwort eingeben. Er erhält dazu eine entsprechende Aufforderung.
- Das zweite Kontrollkästchen *Benutzer kann Kennwort nicht ändern* ist selbsterklärend und wird meistens für Dienstkonten verwendet.
- Aktivieren Sie das Kontrollkästchen *Kennwort läuft nie ab*, muss der Anwender das Kennwort nicht ändern, auch wenn in den Gruppenrichtlinien eine entsprechende Änderung vorgeschrieben ist.

Abbildg. 10.6 Festlegen des Kennworts für ein neues Benutzerkonto

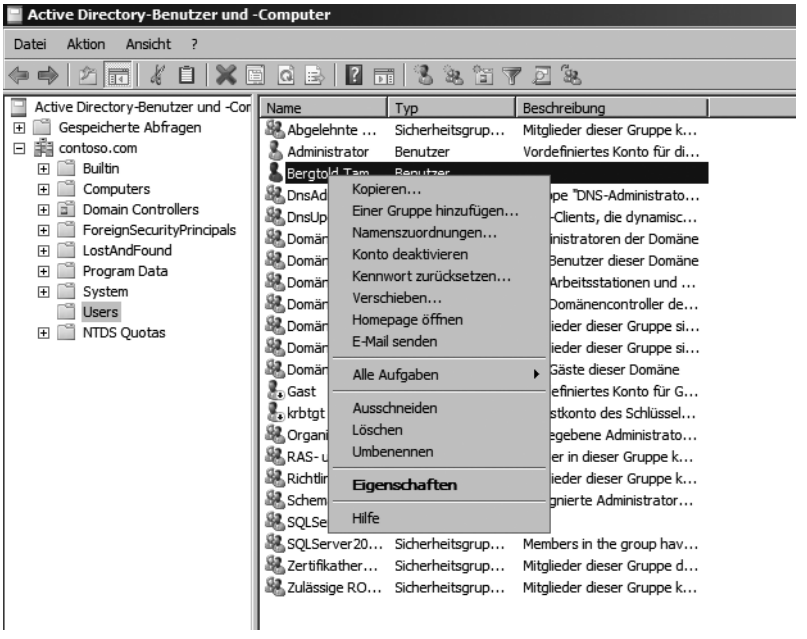
- Durch das Kontrollkästchen *Konto ist deaktiviert* wird das Konto zwar erstellt, steht aber nicht zur Anmeldung bereit, bis ein Administrator das Konto aktiviert. Diese Option ist von Bedeutung, wenn ein Benutzer für eine längere Zeit abwesend ist und verhindert werden soll, dass trotzdem mit seinem Konto gearbeitet wird. Beispiele dafür sind Mutterschutz, längerer Urlaub und andere Situationen. Sie dürfen einen Benutzer in dieser Situation nicht löschen, da die Zugriffsrechte jeweils über die eindeutige Sicherheits-ID (SID) vergeben werden. Wenn Sie den Benutzer löschen und neu definieren, erhält dieser eine neue SID, die sich definitiv von seiner früheren unterscheidet. Damit müssen Sie ihm alle Zugriffsrechte neu zuweisen.

Verwalten von Benutzerkonten

Im Kontextmenü eines angelegten Benutzers steht Ihnen eine Reihe von Möglichkeiten zur Verfügung (Abbildung 10.7):

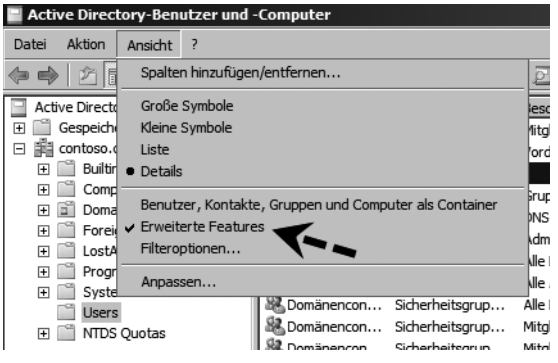
- Mit dem Befehl *Kopieren* können Sie die meisten Einstellungen dieses Benutzerkontos in ein neues Konto übernehmen. Die Einstellungen für Benutzername und Kennwort müssen erneut eingegeben werden. Dazu wird der beschriebene Assistent aufgerufen. Beim Kopieren werden die Gruppenmitgliedschaften übernommen.
- Durch Auswahl von *Einer Gruppe hinzufügen* können Sie den Benutzer zu Gruppen Ihrer Domäne oder Gesamtstruktur hinzufügen. Durch Auswahl von *Mitglieder einer Gruppe hinzufügen* können Sie den Benutzer zu Gruppen Ihrer Domäne hinzufügen. Dieses Dialogfeld hat sich im Vergleich zu Windows 2000 verändert. Sie können entweder Objektnamen eingeben oder alternativ auf *Erweitert* klicken, um nach Gruppen zu suchen. Dort können Sie Teile von Namen eingeben oder sich alle Gruppen auflisten lassen. Die Änderung wurde durchgeführt, um in großen Umgebungen effizienter suchen zu können.
- Der Befehl *Konto deaktivieren* kann verwendet werden, um die zeitweilige Deaktivierung eines Kontos durchzuführen. Das Konto bleibt mit allen Einstellungen erhalten, kann aber nicht zur Anmeldung genutzt werden. Deaktivierte Konten werden durch ein besonderes Symbol in der Anzeige des Snap-Ins *Active Directory-Benutzer und -Computer* gekennzeichnet. Ein deaktiviertes Konto können Sie über den gleichen Weg wieder aktivieren.
- Mit *Kennwort zurücksetzen* können Sie einem Benutzer ein neues Kennwort zuweisen.
- Mit dem Befehl *Verschieben* kann ein Dialogfeld geöffnet werden, über das der Benutzer in eine andere OU der Domäne, in der er angelegt wurde, verschoben werden kann. Damit können auf einfache Weise Reorganisationen durchgeführt werden.
- Zusätzlich gibt es die beiden Befehle *Löschen* und *Umbenennen*. Mit diesen Befehlen kann ein Benutzerkonto gelöscht oder der vollständige Name des Benutzers verändert werden. Beim Löschen ist darauf zu achten, dass es sich um eine nicht widerrufbare Aktion handelt, weil damit die SID des Benutzers gelöscht wird. Durch das Anlegen eines Benutzers mit gleichem Namen wird nicht das gleiche Benutzerkonto erzeugt, da sich die SID ändert. Die Gruppenmitgliedschaften und Zuordnungen von Benutzerrechten müssen in diesem Fall manuell wiederhergestellt werden.

Abbildg. 10.7 Kontextmenü von Benutzerkonten



Die meisten Informationen liefert der Befehl *Eigenschaften* im Kontextmenü. Damit kann auf ein Dialogfeld zugegriffen werden, in dem über eine Vielzahl von Registerkarten die Eigenschaften von Benutzern angepasst werden können. Rufen Sie zuvor den Menübefehl *Ansicht*/*Erweiterte Features* auf, damit alle Registerkarten angezeigt werden (Abbildung 10.8).

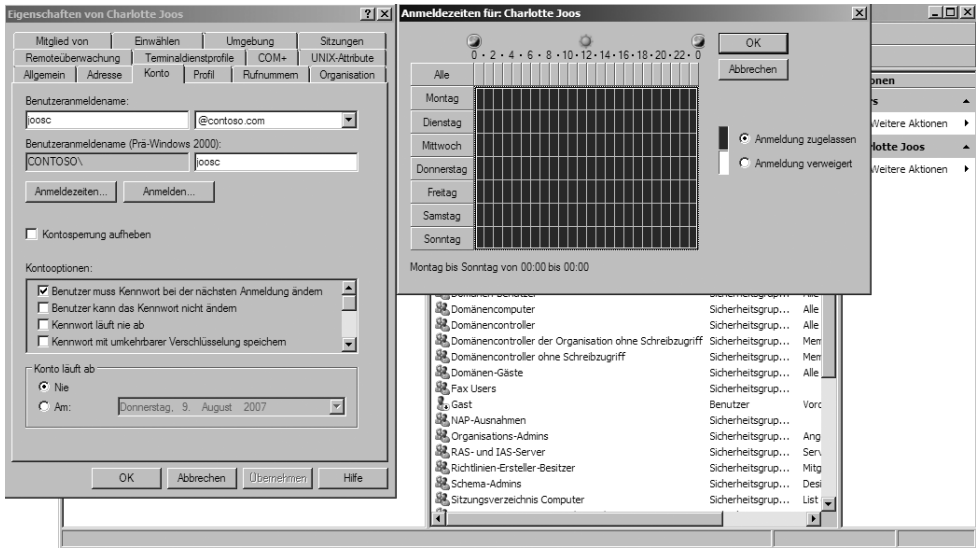
Abbildg. 10.8 Aktivieren der erweiterten Funktion in der Ansicht des Snap-Ins *Active Directory-Benutzer und -Computer*



- Auf der Registerkarte *Allgemein* befinden sich unter anderem die Informationen zum vollständigen Namen des Benutzers, die beim Anlegen des Benutzerkontos eingegeben wurden.
- Auf der Registerkarte *Konto* werden die Einstellungen für Kennwörter und Anmeldenamen verwaltet.

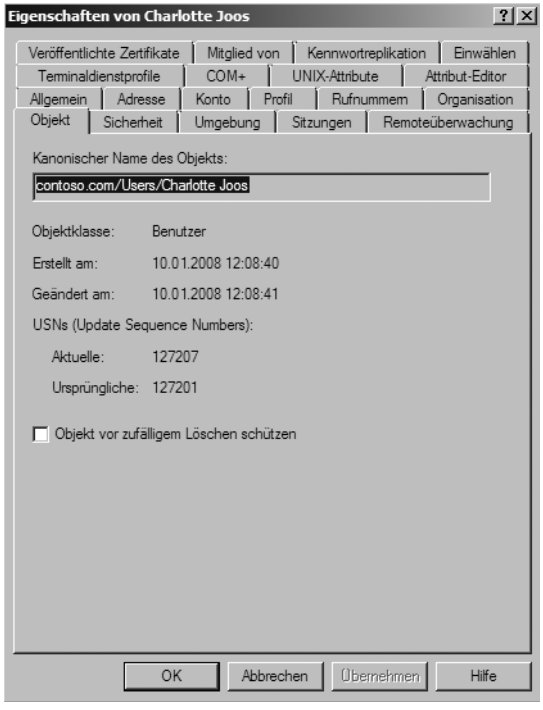
- Mit der Schaltfläche *Anmeldezeiten* kann ein Dialogfeld geöffnet werden, in dem die Zeiten festgelegt werden können, zu denen sich ein Benutzer anmelden darf.
- Über die Schaltfläche *Anmelden an* können Computer ausgewählt werden, auf denen eine Anwendung erfolgen darf.
- Das Kontrollkästchen *Kontosperrung aufheben* kann nur ausgewählt werden, nachdem ein Konto gesperrt wurde. An dieser Stelle können Sie die automatische Sperrung auch wieder aufheben. Die Situationen, in denen ein Konto gesperrt werden soll, können in den Gruppenrichtlinien von Windows Server 2008 konfiguriert werden (siehe Kapitel 9).
- *Benutzer kann das Kennwort nicht ändern* setzt ein Kennwort auf eine feste Vorgabe, die nur von entsprechend autorisierten Operatoren und von Administratoren verändert werden kann.
- *Kennwort läuft nie ab* definiert, dass für dieses Konto keine Änderungen nach in den Richtlinien definierten Zeiträumen erforderlich werden. Diese Option sollte für Dienstkonten gesetzt werden, wenn das dort zwingend erforderlich ist.
- *Kennwort mit umkehrbarer Verschlüsselung speichern* führt dazu, dass das Kennwort von Benutzern mit einer umkehrbaren Verschlüsselung gespeichert wird, die von Administratoren gelesen werden kann.
- *Konto ist deaktiviert* führt dazu, dass das Konto nicht mehr für eine Anmeldung genutzt werden kann, aber mit allen Eigenschaften verfügbar bleibt.
- *Benutzer muss sich mit einer Smartcard anmelden* hat die Folge, dass sich ein Benutzer in jedem Fall unter Verwendung einer Smartcard authentifizieren muss. Er kann sich nicht mehr mit einer Kombination von Benutzername und Kennwort anmelden. Mit Smartcard-basierenden Authentifizierungsmechanismen können weitere Sicherheitsfunktionen wie biometrische IDs für die Aktivierung der Smartcard verbunden werden.
- *Konto ist vertraulich und kann nicht delegiert werden* verhindert die Delegation eines Kontos an andere Benutzer, es kann nur von Administratoren verwaltet werden.
- *Kerberos-DES-Verschlüsselungstypen für dieses Konto* legt fest, welche Verschlüsselungsverfahren für das Konto eingesetzt werden. Das ist für das Deployment von Clients im internationalen Umfeld mit unterschiedlichen rechtlichen Rahmenbedingungen für die Verschlüsselung von Bedeutung.
- *Keine Kerberos-Präauthentifizierung erforderlich* Laut dem Kerberos-Standard ist die TGT-Anforderung des Clients ein unverschlüsseltes Paket, da es keine sicherheitssensiblen Daten enthält (siehe Kapitel 8). Bei Verwendung der Kerberos-Präauthentifizierung wird dieses Paket bereits mit dem privaten Schlüssel des Benutzers/Anforderers verschlüsselt. Für die Interoperabilität mit anderen Kerberos-Implementierungen kann diese Präauthentifizierung deaktiviert werden.
- Zusätzlich kann unten in diesem Dialogfeld ein Ablaufdatum für das Konto gesetzt werden. Ein Datum sollte immer definiert werden, wenn das Benutzerkonto, zum Beispiel bei Praktikanten, nur für einen begrenzten Zeitraum Gültigkeit besitzt.

Abbildg. 10.9 Konfigurieren der Kontoeigenschaften für ein Benutzerkonto



- Die Registerkarte *Mitglied von* zeigt eine Liste der Gruppen an, in denen der Benutzer Mitglied ist. Hier können weitere Gruppenzugehörigkeiten hergestellt werden. Außerdem kann auch die primäre Gruppe für einen Benutzer definiert werden.
- Über die Registerkarte *Einwählen* können die RAS-Berechtigungen für diesen Benutzer konfiguriert werden. Grundsätzlich dürfen sich Benutzer nur einwählen, wenn ihnen explizit diese Berechtigung erteilt wurde.
- Eine weitere Registerkarte bei den Eigenschaften eines Benutzers ist *Objekt (*Abbildung 10.10*)*. Diese wird nur angezeigt, wenn Sie im Menü *Ansicht* die erweiterten Features aktiviert haben. Auf dieser Registerkarte werden einige systeminterne Informationen angezeigt. Dazu gehört der vollqualifizierte Domänenname des Objekts, die Objektklasse – die Klasse, auf der dieses Objekt basiert – sowie Erstellungs- bzw. Änderungsdaten und die *USN (Update Sequence Number)*. Die *USN* wird fortlaufend vergeben und zeigt an, um die wievielte Änderung im Active Directory es sich handelt. Sie bildet die Basis für die Replikation, da anhand ihrer überprüft werden kann, ob die Einträge auf zwei unterschiedlichen Domänencontrollern den gleichen Status haben.

Abbildg. 10.10 Anzeige der USN eines Benutzerkontos



Auf dieser Registerkarte kann auch konfiguriert werden, dass das Objekt nicht gelöscht werden kann. Zu den weiteren Registerkarten kommen wir noch im Laufe dieses Kapitels.

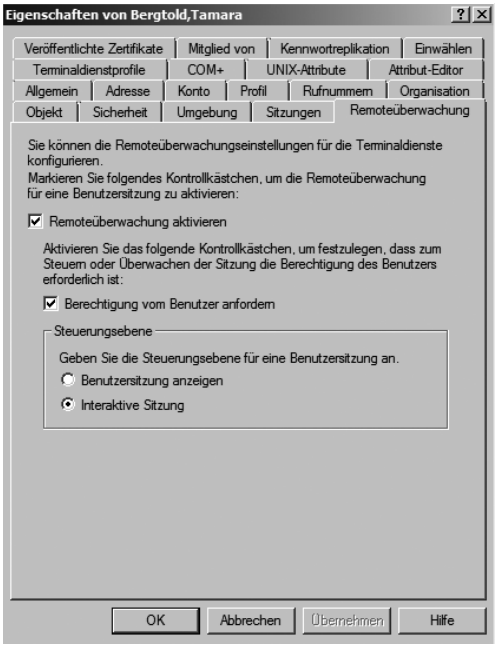
Benutzerverwaltung für Terminalserverbenutzer

In den Eigenschaften eines Benutzers stehen Ihnen vier Registerkarten zur Verfügung, auf denen Sie die Eigenschaften des Benutzerkontos für die Anmeldung auf Terminalservern (siehe auch Kapitel 12) speziell anpassen können:

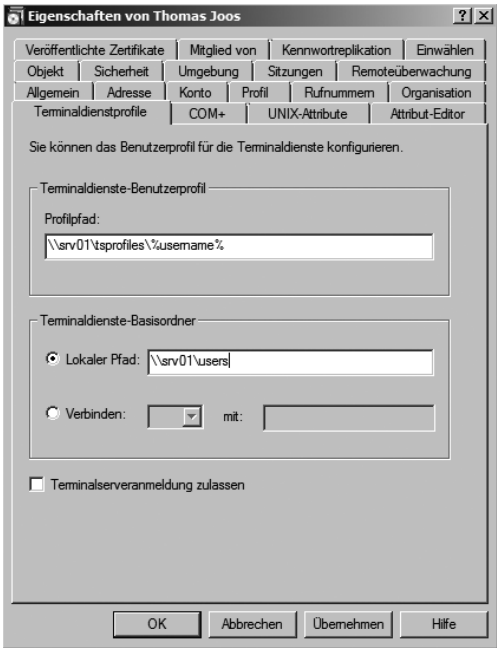
- Umgebung
- Sitzungen
- Remoteüberwachung
- Terminaldiensteprofil

Auf der Registerkarte *Remoteüberwachung* legen Sie fest, ob dieser Benutzer von Administratoren gespiegelt werden kann und mit welchen Optionen. Hier legen Sie auch fest, ob sich Administratoren ohne Bestätigung durch den Benutzer auf die Sitzung spiegeln können. Diese Einstellungen entsprechen den in Kapitel 12 besprochenen Einstellungen in der Terminaldienstekonfiguration. Die Einstellungen in den Benutzerkonten haben nur für diesen Benutzer Gültigkeit.

Abbildg. 10.11 Konfigurieren der Remoteüberwachung für ein Benutzerkonto



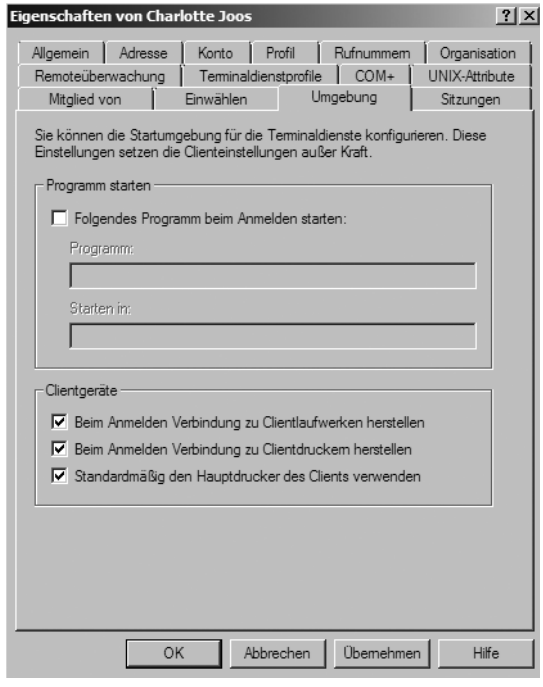
Abbildg. 10.12 Konfigurieren der Terminalserver-Berechtigungen eines Benutzers



Auf der Registerkarte *Terminaldienstprofile* können Sie das servergespeicherte Profil festlegen, das ausschließlich für die Terminalsitzungen dieses Benutzers verwendet wird. Zusätzlich können Sie auf dieser Registerkarte festlegen, ob mit dem Benutzer ein bestimmtes Netzlaufwerk verbunden werden soll. Auch diese Konfiguration hat nur bei der Anmeldung auf einem Terminalserver Gültigkeit. Hier legen Sie auch fest, ob sich ein Benutzer überhaupt auf einem Terminalserver anmelden darf. Zu den servergespeicherten Profilen kommen wird noch in den nächsten Abschnitten zurück.

Die Registerkarten *Umgebung* und *Sitzungen* entsprechen den entsprechenden Einstellungen für das RDP-Protokoll in der Terminaldienstekonfiguration. Wenn der Terminalserver nur verwendet wird, um eine einzige Anwendung zur Verfügung zu stellen oder alle anderen Anwendungen über eine Startapplikation gestartet werden sollen, können Sie dem Anwender über die Registerkarte *Umgebung* statt des Windows-Desktops auch nur diese Applikation zur Verfügung stellen. Aktivieren Sie dazu das Kontrollkästchen *Folgendes Programm beim Anmelden starten* und geben Sie anschließend das zu startende Programm mit dem kompletten Pfad an. Durch diesen Schritt müssen die Anwender beim Starten der Verbindung nicht noch ein Programm starten und können darüber hinaus keine Einstellungen auf dem Terminalserver verändern.

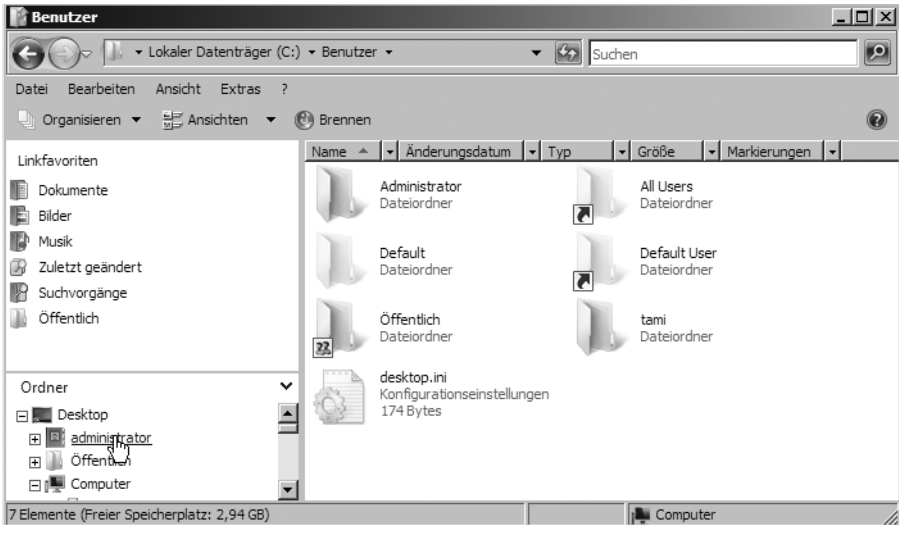
Abbildg. 10.13 Konfigurieren der Terminalserver-Umgebung für ein Benutzerkonto



Verwalten von Benutzerprofilen

Alle persönlichen Einstellungen der einzelnen Benutzer auf einem Computer werden in einem so genannten Benutzerprofil gespeichert. Dieses Profil ist ein Verzeichnis mit dem Namen des Benutzeranmeldenamens des jeweiligen Anwenders im Verzeichnis *C:\Benutzer* beziehungsweise *C:\Users*. Dieses Verzeichnis ist neu in Windows Vista und Windows Server 2008. Unter Windows XP hat dieses Verzeichnis noch die Bezeichnung *C:\Dokumente und Einstellungen* getragen. Oft kann Festplattenplatz auf einem PC durch das Löschen nicht mehr benötigter Profile wieder freigegeben werden. Wenn Sie ein Profil löschen, wird dieses neu erstellt, sobald sich der Benutzer erneut am PC anmeldet. Alle Einstellungen des Benutzers werden beim Löschen zurückgesetzt, das Profil ist also vollkommen leer und wird neu erstellt. Beachten Sie aber, dass beim Löschen eines Profils alle Daten des entsprechenden Benutzers verloren gehen. Sie sollten diese daher vorher möglichst sichern.

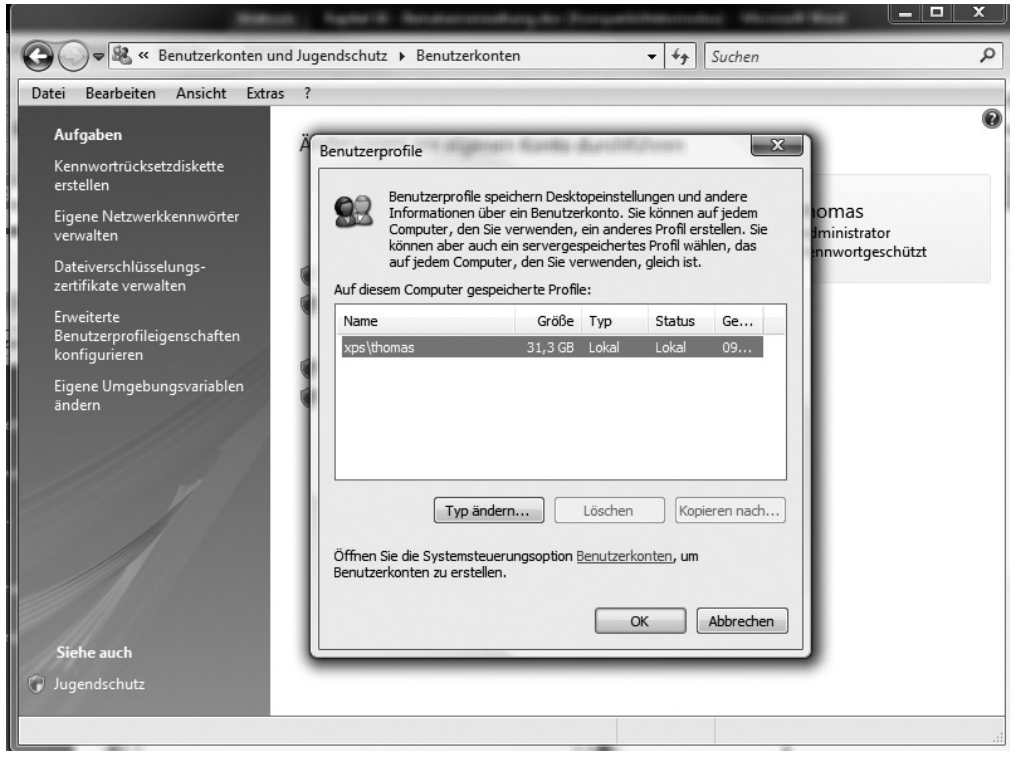
Abbildg. 10.14 Anzeigen der Benutzerprofile unter Windows Server 2008 oder Windows Vista



Über den Link *Erweiterte Benutzerprofileigenschaften konfigurieren* im Fenster *Benutzerkonten* der Systemsteuerung können Sie sich alle Benutzerprofile auf einem PC unter Windows Vista anzeigen lassen und diese anschließend löschen (Abbildung 10.15). Sie sehen an dieser Stelle auch die Größe des jeweiligen Profils. Im Verzeichnis werden mehrere Unterordner angezeigt. Die persönlichen Daten jedes Benutzers liegen in seinem eigenen Verzeichnis, auf das nur er selbst sowie die Administratoren Zugriff haben.

Die Benutzerprofile werden zunächst als Kopie des Standardprofils, des *Default User*, erzeugt. Zusätzlich gibt es einen Ordner *All Users*, der ebenfalls für Benutzerprofile verwendet wird. Während der Ordner *Default User* die Einstellungen für neu zu erstellende Benutzerprofile für alle Benutzer enthält, finden sich in *All Users* die Einstellungen für die bereits erstellten Profile, die für alle Nutzer der Arbeitsstation gelten. Damit diese beiden Verzeichnisse angezeigt werden, müssen Sie die versteckten Dateien und die Systemdateien einblenden lassen.

Abbildg. 10.15 Verwalten der Benutzerprofile unter Windows Vista

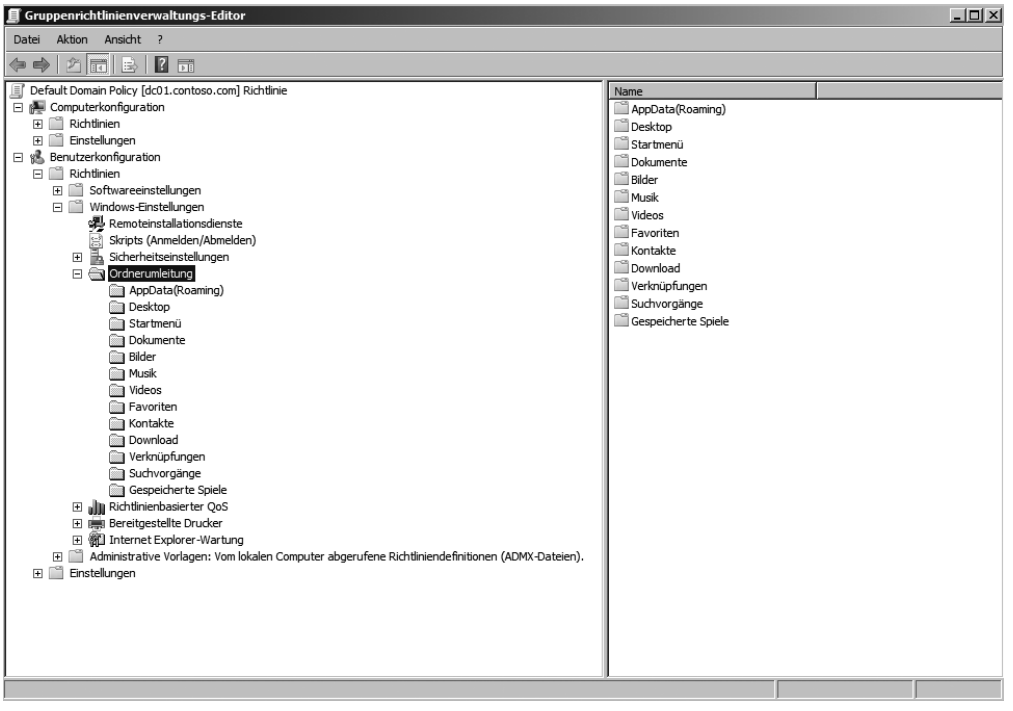


Allgemeines zu Ordnerumleitungen und servergespeicherten Profilen

Auch unter Windows Vista besteht die Möglichkeit, Profile serverbasiert zu konfigurieren und Ordner umzuleiten. Da der Aufbau der Profile geändert wurde, müssen hier teilweise neue Wege gegangen werden. Die Synchronisation von Clients und Server für servergespeicherte Profile wurde in Windows Vista stark verbessert, sodass längere Anmeldezeiten oder zu große Profile der Vergangenheit angehören. Insgesamt bietet Windows Vista die Möglichkeit, an bis zu zehn Ordner innerhalb des Profils auf ein Serverlaufwerk umzuleiten. Bei der Ordnerumleitung werden Pfade zum Dokumenten-Verzeichnis oder dem Startmenü auf einen Server umgeleitet. Dadurch ist sichergestellt, dass die Daten der Anwender sicher auf einem Server gespeichert werden, aber dennoch transparent zugreifbar sind, wenn ein Anwender zum Beispiel seinen Dokumenten-Ordner öffnet. Durch die Ordnerumleitung können wichtige Benutzerdaten aus dem servergespeicherten Profil herausgenommen werden und stehen auch auf mehreren Arbeitsstationen in Echtzeit zur Verfügung, wenn alle Arbeitsstationen Zugriff auf den gleichen Server haben. Die Größe der Profile wird reduziert,

die Anmeldezeit verkürzt. Außerdem hat Microsoft einen neuen Bereich für die Umleitung von Ordnern aus dem Benutzerprofil entwickelt, mit dessen Hilfe die Ordnerumleitung per Gruppenrichtlinien deutlich effizienter durchgeführt werden können (Abbildung 10.16). Sie finden die Ordnerumleitungen im Gruppenrichtlinienverwaltungs-Editor unter *Benutzerkonfiguration/Richtlinien/Windows-Einstellungen/Ordnerumleitungen*.

Abbildg. 10.16 Ordnerumleitung mit Windows Vista und Windows Server 2008



Mit diesem neuen Snap-In können auch die Ordnerumleitungen für Windows XP und Windows 2000 konfiguriert werden. Die effizienteste Möglichkeit, um Ordner umzuleiten, ist über eine Gruppenrichtlinie in einer Active Directory-Domäne. Windows Server 2008 bietet dazu auch die Möglichkeit, Ordner abhängig von einer Sicherheitsgruppe umzuleiten, sodass für unterschiedliche Abteilungen im Unternehmen unterschiedliche Ordner im Netzwerk als Umleitung verwendet werden können. Bei der Umleitung können Sie die Ordner in vordefinierte Verzeichnisse auf den Servern umleiten lassen oder für jeden Anwender in einem spezifischen Ordner automatisch ein Verzeichnis für die Ordnerumleitung anlegen lassen. Die Einstellungen in den Richtlinien für die Ordnerumleitung sind selbsterklärend (Abbildung 10.17).

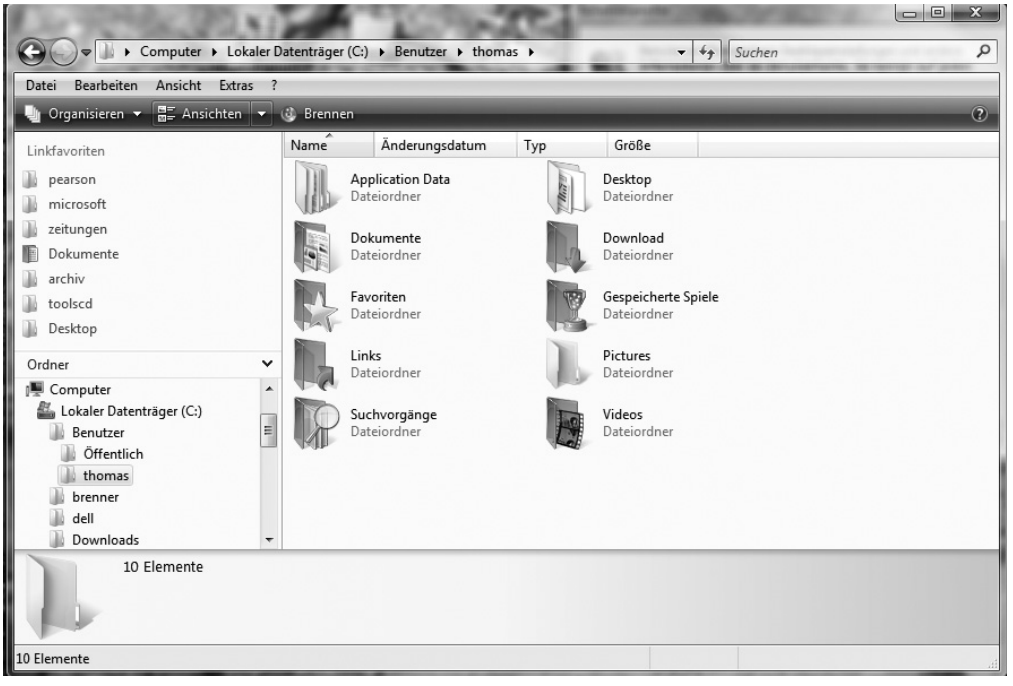
Abbildg. 10.17 Ordnerumleitung in einer Windows Server 2008-Gruppenrichtlinie konfigurieren

Änderungen in den Benutzerprofilen

Wie bereits erwähnt, werden Benutzerprofile in Windows Vista und Windows Server 2008 im Ordner *C:\Users\<Benutzername>* gespeichert. Die Tiefe der Ordnerstruktur innerhalb des Profils hat Microsoft wesentlich reduziert, auch die Bezeichnung der Ordner ist jetzt wesentlich selbsterklärender und es ist leichter, innerhalb der Ordnerstuktur eines Profils die wesentlichen Verzeichnisse zu finden. Zur Abwärtskompatibilität hat Microsoft noch einige Verknüpfungen eingefügt, die in den vorangegangen Windows-Versionen noch verwendet wurden oder die direkt auf ein anderes Verzeichnis verweisen, wie zum Beispiel das Startmenü. Folgende Verzeichnisse spielen dabei eine wesentliche Rolle. Achten Sie aber darauf, dass einige Ordner standardmäßig im Explorer ausgeblendet werden. Erst muss die Anzeige der Systemdateien und der versteckten Dateien aktiviert werden.

- **Kontakte** Enthält die angelegten Kontakte des Benutzers
- **Desktop** Symbole und Einstellungen des Benutzerdesktops
- **Dokumente** Standardmäßiger Speicherort aller persönlicher Dateien eines Benutzers. Unter Vista gibt es eine Verknüpfung *Eigene Dateien,* die auf den Ordner *Dokumente* zeigt.
- **Download** Speicherort aller Downloads
- **Favoriten** Favoriten des Internet Explorers
- **Musik** Ablageort von Musikdateien
- **Videos** Ablageort für gespeicherte Filmdateien
- **Bilder** Ablageort für Bilddateien und Grafiken
- **Suchvorgänge** Ablageort für abgespeicherte Suchen
- **AppData** Ablageort für benutzerspezifische Daten und Systemdateien von Applikationen
- **Gespeicherte Spiele** Zentraler Ablageort für Spielstände von kompatiblen Windows-Spielen

Abbildg. 10.18 Neue Verzeichnisse in den Profilen von Benutzern unter Windows Server 2008 und Windows Vista



In Windows Vista und Windows Server 2008 wurden ebenfalls Änderungen vorgenommen, wie die Daten von Applikationen gespeichert werden. Unter Windows XP war es nicht einfach möglich festzustellen, welche Daten von Applikationen maschinenbezogen waren und welche benutzerspezifisch sind. Zu dem Zweck der Vereinheitlichung von anwendungsspezifischen Daten hat Microsoft den Ordner *AppData* im Benutzerprofil eingeführt. Dieser Ordner enthält die drei Unterordner:

- Local
- LocalLow
- Roaming

In den beiden Verzeichnissen *Local* und *LocalLow* werden Daten von Anwendungen gespeichert, die nicht mit dem Benutzer bei der Verwendung von verschiedenen Arbeitsstationen mit wandern. Hier handelt es sich vor allem um maschinenbezogene Daten oder um Daten, die ein Benutzerprofil unnötig aufblähen würden. Das Verzeichnis *Local* ist im Endeffekt identisch mit dem Verzeichnis *C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Anwendungsdaten* in Windows XP. Der Ordner *Roaming* enthält die Daten, welche benutzerspezifisch sind und für servergespeicherte Profile verwendet werden können. Diese Daten können mit dem Benutzer auf verschiedene Arbeitsstationen mit wandern. Dieser Ordner entspricht dem Ordner *C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten* in Windows XP.

Sie sollten diese Zusammenhänge verstehen, bevor Sie in einem Unternehmen servergespeicherte Profile in Verbindung von Windows Vista- und Windows XP-Arbeitsstationen unter Windows Server 2008 verwenden. In Tabelle 10.1 sind die einzelnen wichtigen Verzeichnisse im Profil eines Benutzers von Windows Vista im Vergleich zum entsprechenden Ordner unter Windows XP aufgelistet.

Tabelle 10.1 Verzeichnisse in den Benutzerprofilen von Windows Vista im Vergleich zu Windows XP

Ordner	Beschreibung	Name unter Windows XP	Speicherort unter Windows XP
Kontakte	Enthält die angelegten Kontakte des Benutzers	Nicht verfügbar	Nicht verfügbar
Desktop	Symbole und Einstellungen des Benutzerdesktops	*Desktop*	*C:\Dokumente und Einstellungen\<Benutzername>\Desktop*
Dokumente	Standardmäßiger Speicherort aller persönlicher Dateien eines Benutzers	*Eigene Dateien*	*C:\Dokumente und Einstellungen\<Benutzername>\Eigene Dateien* Unter Vista gibt es daher eine Verknüpfung *Eigene Dateien*, die auf den Ordner *Dokumente* zeigt
Download	Speicherort aller Downloads	Nicht verfügbar	Nicht verfügbar
Favoriten	Favoriten des Internet Explorers	*Favoriten*	*C:\Dokumente und Einstellungen\<Benutzername>\Favoriten*
Musik	Ablageort von Musikdateien	*Eigene Musik*	*C:\Dokumente und Einstellungen\<Benutzername>\Eigene Dateien\Eigene Musik*
Videos	Ablageort für gespeicherte Filmdateien	Nicht verfügbar	Nicht verfügbar
Bilder	Ablageort für Bilddateien und Grafiken	*Eigene Bilder*	*C:\Dokumente und Einstellungen\<Benutzername>\Eigene Dateien\Eigene Bilder*
Suchvorgänge	Ablageort für abgespeicherte Suchen	Nicht verfügbar	Nicht verfügbar
AppData	Ablageort für Benutzerspezifische Daten und Systemdateien von Applikationen	Nicht verfügbar (vergleichbar mit *Anwendungsdaten*)	Nicht verfügbar Vergleichbar mit dem Ordner *Anwendungsdaten* im Profil
Gespeicherte Spiele	Zentraler Ablageort für Spielstände von kompatiblen Windows-Spielen	Nicht verfügbar	Nicht verfügbar

Das *All Users*-Profil

Unter den Vorgängerversionen von Windows Vista hat das Verzeichnis *All Users* die Inhalte zur Verfügung gestellt, die für alle Anwender auf dem PC gegolten haben. So war es möglich, durch Bearbeitung eines einzelnen Verzeichnisses die Einstellungen aller Benutzer anzupassen. Beispiel für den Einsatz von *All Users* ist zum Beispiel das Startmenü oder den Inhalt des Desktops, der sich immer aus dem eigenen Benutzerprofil und dem Inhalt des Ordners *All Users* zusammensetzt. Wenn zum Beispiel eine Verknüpfung in das Verzeichnis *\All Users\Startmenü* kopiert wurde, wurde diese bei allen Benutzern des PCs im Startmenü angezeigt. In Windows Vista ist das Verzeichnis *C:\Users\All Users* nur noch als Verknüpfung vorhanden, die auf den Ordner *C:\ProgramData* verweist. Hier wird wiederum auf das Profil *Öffentlich* unter *C:\Users* verlinkt.

Papierkorb in Windows Vista

Der Papierkorb ist jetzt in Windows Vista Bestandteil des Profils. Unter Windows XP war der Papierkorb noch nicht benutzerspezifischer Teil des Profils. Der Papierkorb wird in Windows Vista als versteckte Datei im Hauptverzeichnis des Profils gespeichert.

Verbindungspunkte (Junction Points)

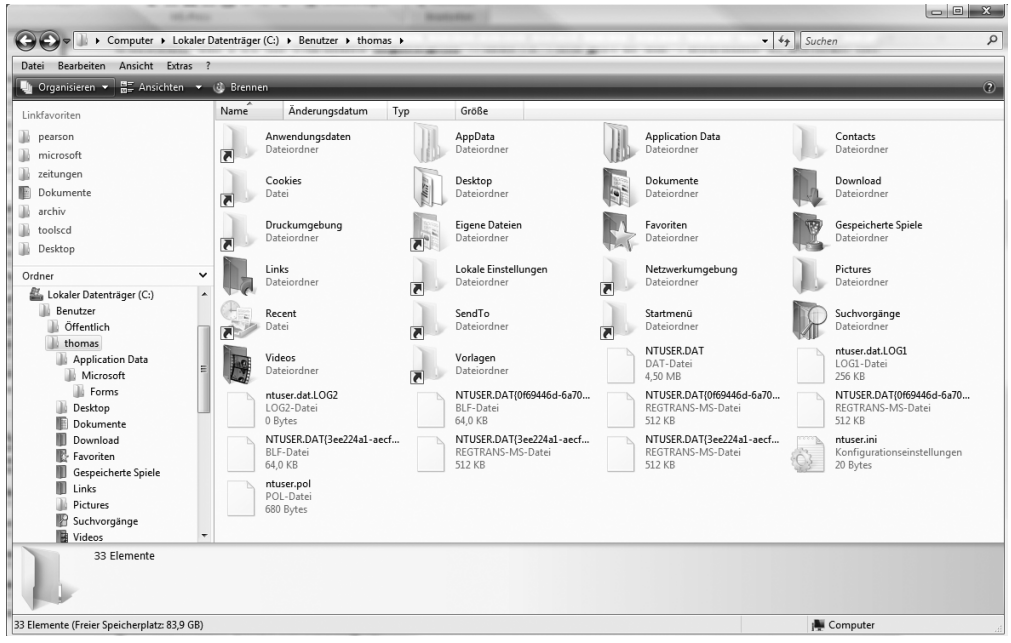
Die meisten Anwendungen sind bereits standardmäßig kompatibel zu den neuen Verzeichnissen des Profils in Windows Vista. Meistens sind daher keinerlei Änderungen notwendig. In Windows Vista wurde dazu die Unterstützung von älteren Dateipfaden integriert. Alle Pfade sind auch für ältere Anwendungen vollkommen transparent. Manche Anwendungen haben unter Umständen dennoch Probleme mit den neuen Verzeichnisstrukturen. Microsoft hat für die Unterstützung solcher Anwendungen auf dem Dateisystem *Verbindungspunkte* eingerichtet. Ein solcher Verbindungspunkt verweist ähnlich wie eine Verknüpfung auf einen anderen Pfad auf dem PC, in dem schließlich die gesuchten Daten liegen. Für alle notwendigen Systemverzeichnisse unter Windows XP hat Microsoft in Windows Vista Verbindungspunkte eingerichtet.

Beispiel

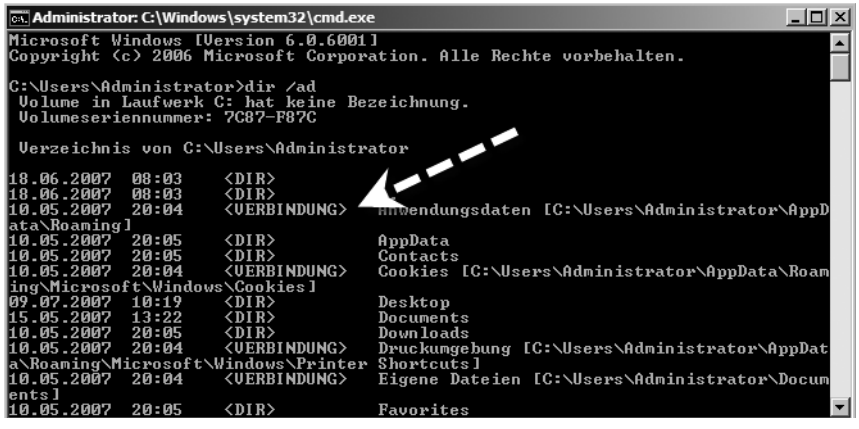
Das Verzeichnis *C:\Users\<Benutzername>\Dokumente* in Windows Vista stellt das neue Verzeichnis für *C:\Dokumente und Einstellungen\<Benutzername>\Eigene Dateien* in Windows XP dar. Damit auch ältere Applikationen, die zum Beispiel Zugriff auf den Ordner *Eigene Dateien* haben müssen, weiterhin funktionieren, hat Microsoft einen Verbindungspunkt *Eigene Dateien* im Profil unter Windows Vista eingerichtet. Solche Verbindungspunkte gibt es massenweise in Windows Vista an verschiedener Stelle. Im Windows-Explorer werden diese durch einen Verknüpfungspfeil gekennzeichnet (Abbildung 10.19).

Sie können sich in der Befehlszeile die Verbindungspunkte und deren Zielverzeichnisse anzeigen lassen. Wechseln Sie dazu in das entsprechende Verzeichnis und geben Sie den Befehl *dir /ad* ein. Sie erhalten eine Auflistung über den Inhalt des Verzeichnisses und Verbindungspunkte werden als *VERBINDUNG* angezeigt. Wenn Sie im Windows-Explorer per Doppelklick auf einen solchen Verbindungspunkt klicken, erhalten Sie oft die Meldung, dass der Zugriff verweigert wird, das gilt aber nur für den manuellen Zugriff über den Verbindungspunkt, nicht für Applikationen und nicht für das Zielverzeichnis an sich. Verbindungspunkte (Junction Points) sind eine Funktion im NTFS-Dateisystem und haben nichts mit Ordnerumleitung oder Verknüpfungen zu tun, sondern sind eine eigenständige Funktion.

Abbildg. 10.19 Anzeigen der verschiedenen Verbindungspunkte unter Windows Vista



Abbildg. 10.20 Anzeige von Verbindungspunkten über die Befehlszeile



Kompatibilität mit Profilen von älteren Windows-Versionen

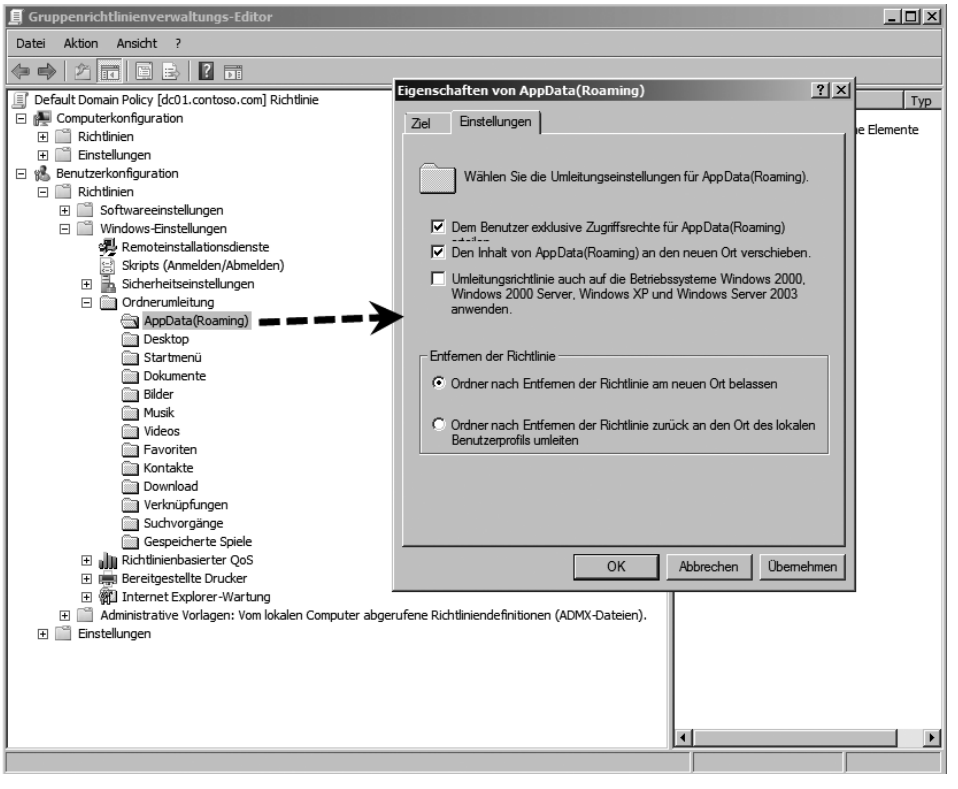
Die Pfade in den Benutzerprofilen von Windows XP sind identisch mit Windows 2000. Windows Vista lädt standardmäßig keine servergespeicherten Profile von älteren Windows-Versionen wie XP oder 2000. Durch die Pfadunterschiede laden PCs mit Windows XP oder 2000 auch keine Windows Vista-Profile. Servergespeicherte Profile von einem Windows Vista-PC erhalten bei der Speicherung

auf einem Server ein *v2* als Zusatz, welches kenntlich macht, dass es sich bei diesem Profil um ein servergespeichertes Profil eines Windows Vista-PCs handelt. Wenn Sie servergespeicherte Profile für Windows Vista-PCs einsetzen wollen, muss auf mindestens einem Domänencontroller Windows Server 2003 mit SP1 oder R2 installiert sein. Am besten werden die servergespeicherten Benutzerprofile von Windows Server 2008 unterstützt. Wenn Sie im Unternehmen Windows Vista-PCs und Windows XP-PCs einsetzen und sich Anwender mit servergespeicherten Profilen an beiden Windows-Versionen anmelden können, müssen Sie einige Punkte beachten. Sie können bei der Ordnerumleitung zum Beispiel den Inhalt der einzelnen Ordner in die gleichen Verzeichnisse freigeben, dadurch können die Gruppenrichtlinien sicherstellen, dass der Inhalt sowohl bei der Anmeldung unter Windows XP als auch unter Windows Vista funktionieren. Durch diese Art und Weise lassen sich zum Beispiel auch die Favoriten und die Eigenen Dateien (unter Windows Vista *Dokumente* genannt) in einen gemeinsamen Ordner umleiten.

Umleiten der Verzeichnisse *AppData* und *Desktop*

Das Verzeichnis *AppData* spielt bei der Ordnerumleitung eine wichtige Rolle, da hier die maßgeblichen Unterschiede zur Verzeichnisstruktur eines Profils zwischen Windows XP und Vista bestehen. Um die Ordnerumleitung für Windows Vista durchzuführen, lassen Sie über den beschriebenen Weg der Gruppenrichtlinien zunächst den Ordner *AppData* in ein Verzeichnis im Netzwerk, zum Beispiel \\<*Servername*>\<*Freigabe*>*%username%**AppData,* umleiten. Deaktivieren Sie die Option in der Richtlinie, dass die Umleitung auch für Windows 2000, 2003 oder XP Gültigkeit hat (Abbildung 10.21).

Abbildg. 10.21 Konfigurieren der Ordnerumleitung für das Verzeichnis *AppData* unter Windows Server 2008



Gehen Sie bei der Umleitung für den Desktop analog vor. Hier können Sie jedoch die Option aktivieren, dass die Umleitung auch für PCs mit Windows 2000, 2003 und XP Gültigkeit hat.

Umleiten der Ordner *Eigene Dateien/Dokumente* und des Startmenüs

Der Ordner *Dokumente* in einem Profil in Windows Vista entspricht dem Ordner *Eigene Dateien* unter Windows XP. Bei der Umleitung dieses Ordners sollten Sie sicherstellen, dass der Pfad außerhalb des Benutzerprofils auf einem Server liegt. Hier können Sie auch die Option aktivieren, dass die Umleitung auch für PCs mit Windows 2000, 2003 und XP Gültigkeit hat. Wenn Sie das Startmenü auf einen Server auslagern wollen, können Sie das ebenfalls in dieser Richtlinie tun und zusätzlich auch die Richtlinie für Windows XP, 2000 und 2003-Rechner aktivieren.

Anlegen von neuen servergespeicherten Profilen

Wie bei den Vorgängerversionen legt Windows Vista automatisch ein neues Profil an, wenn sich ein Benutzer das erste Mal am PC anmeldet. Das neue Profil wird im Verzeichnis *C:\Users\<Benutzername>* abgespeichert. Dabei wird das Profil aus dem Default-Profil erstellt, wie bei Windows XP oder auch Windows 2000 und NT 4.0. Wenn für den Anwender ein servergespeichertes Profil vorliegt, wird dieses verwendet. Wenn das Default-Profil im Netzwerk gespeichert wurde, wird dieses von der Netlogon-Freigabe eines Domänencontrollers auf den PC kopiert.

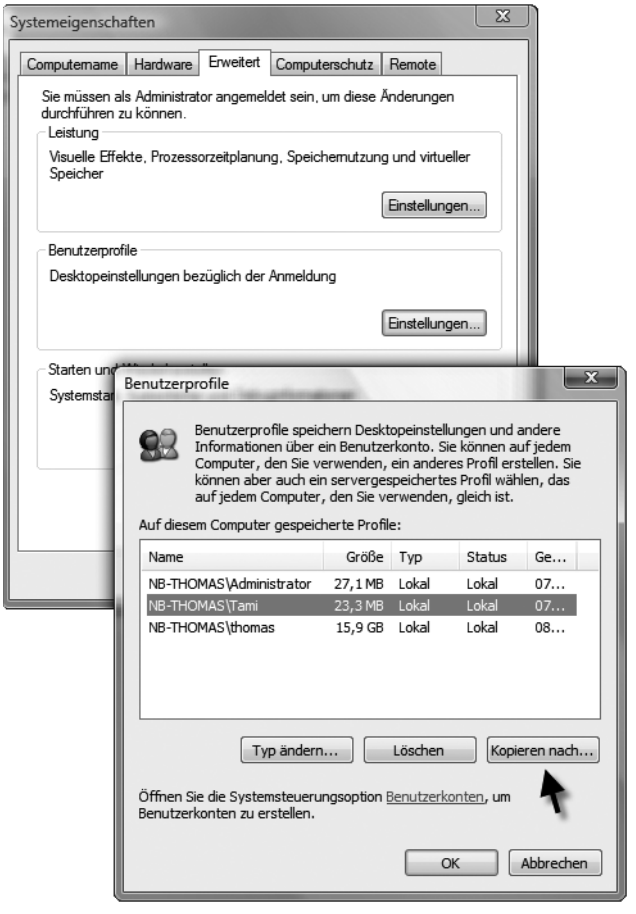
Erstellen eines Default-Netzwerk-Benutzerprofils

Wenn Sie für alle PCs im Unternehmen das gleiche standardmäßige Profil bei der ersten Anmeldung erstellen wollen, können Sie dieses am besten auf einem Domänencontroller ablegen. Achten Sie in diesem Fall aber darauf, dass bei jeder ersten Anmeldung eines Anwenders an einem PC Daten über das Netzwerk kopiert werden, was bei entsprechender Benutzerlast eine ganze Menge sein kann. Um ein solches standardmäßiges Default-Profil anzulegen, gehen Sie folgendermaßen vor:

1. Melden Sie sich an einem PC mit Windows Vista mit dem Benutzerkonto an der Domäne an, welches Sie als Standardprofil definieren wollen.
2. Führen Sie alle Einstellungen aus, zum Beispiel Bildschirmschoner, Hintergrundbild und so weiter, welche Sie für das Profil festlegen wollen.
3. Melden Sie sich nach der Fertigstellung der Einstellungen ab.
4. Melden Sie sich am gleichen PC mit einem Domänenadmin-Konto an.
5. Erstellen Sie in der Netlogon-Freigabe auf einem Domänencontroller das neue Verzeichnis *Default User.v2*. Das *v2* definiert das Profil, welches nur für Windows Vista-PCs verwendet wird.
6. Klicken Sie auf dem PC mit der rechten Maustaste auf *Computer* im Startmenü und rufen Sie im Kontextmenü den Befehl *Eigenschaften* auf.
7. Klicken Sie links im Fenster auf den Link *Erweiterte Systemeinstellungen*.
8. Klicken Sie im Bereich *Benutzerprofile* auf *Einstellungen*.

9. Markieren Sie den Benutzer, dessen Profil Sie als Standard definieren wollen, und klicken Sie auf *Kopieren nach*.
10. Geben Sie den Pfad zum Default User-Verzeichnis in der Netlogon-Freigabe an, welches Sie zuvor angelegt haben, zum *Beispiel \\dc01\NETLOGON\Default User.v2*.

Abbildg. 10.22 Kopieren eines Profils als Vorlage für servergespeicherte Profile



11. Klicken Sie im Bereich *Benutzer* auf *Ändern*.
12. Geben Sie im Benutzerfeld *Jeder* ein und klicken Sie auf *Namen überprüfen*.
13. Klicken Sie anschließend auf *OK*.
14. Bestätigen Sie im Anschluss alle noch offenen Fenster mit *OK*, damit das Profil kopiert werden kann. Das servergespeicherte Profil ist jetzt vorbereitet.

Abbildg. 10.23 Festlegen der Berechtigungen für ein neues servergespeichertes Profil

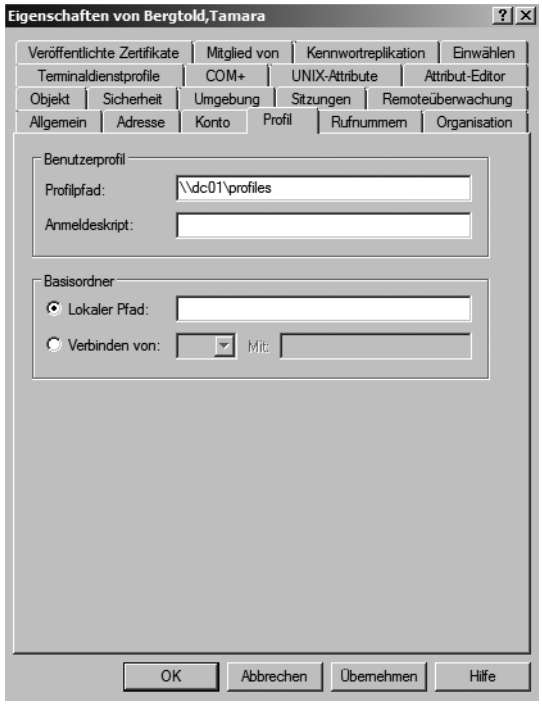
Sie können darüber hinaus im unteren Bereich des Dialogfeldes den Eintrag für Benutzer ändern, wenn Sie das Profil in den Ordner eines anderen Anwenders kopieren möchten. Über die Schaltfläche *Typ ändern* können Sie festlegen, ob bei der Anmeldung das lokal zwischengespeicherte Profil verwendet werden soll oder ob mit dem serverbasierenden Profil gearbeitet werden soll. Bei der Erstellung von Benutzerprofilen sind einige Besonderheiten zu beachten. Sie sollten immer daran denken, dass die Benutzer, wenn sie sich an unterschiedlichen Arbeitsstationen anmelden, immer mit unterschiedlichen Bildschirmauflösungen konfrontiert sind. Sie sollten bei der Definition immer den typischen Arbeitsplatz des Benutzers, für den das Profil vordefiniert wird, beachten. Das gilt vor allem für verbindliche Profile. Ein weiterer Punkt ist, dass das in *Default User* gespeicherte Profil, das zum Einsatz kommt, wenn Sie keine zentralen Profile für alle Benutzer vorgeben, auf jedem einzelnen Computer definiert ist.

Festlegen von servergespeicherten Profilen für Benutzer im Active Directory

Wenn Sie ein Standardprofil festgelegt haben, müssen Sie in der Active Directory-Domäne zunächst servergespeicherte Profile für die Anwender konfigurieren. Auf der Registerkarte *Profil* eines Benutzerkontos können die notwendigen Angaben durchgeführt werden (Fehler! Verweisquelle konnte nicht gefunden werden.). Bei *Profilpfad* wird das Verzeichnis angegeben, in dem das Benutzerprofil des Anwenders abgelegt wird. Bei Verwendung eines serverbasierenden Benutzerprofils steht dieses Profil an allen Arbeitsstationen im Netzwerk zur Verfügung. Durch die Angabe dieses Pfads wird

automatisch ein leerer Ordner für diesen Benutzer erstellt. Die Angabe des Profilpfads erfolgt in der Form \\<*Servername*>\<*Freigabename*>*%username%*.

Abbildg. 10.24 Konfigurieren eines servergespeicherten Profils



Der Profilpfad verweist auf den Ordner, in dem das Benutzerprofil des Anwenders abgelegt wird. Ist kein Pfad angegeben, wird nur mit lokalen Benutzerprofilen gearbeitet. Wenn sich ein Benutzer anmeldet, überprüft Windows Server 2008, ob für diesen Benutzer ein Profilpfad angegeben ist und damit ein serverbasierendes Profil definiert wurde. Ist dies der Fall, wird verglichen, ob das serverbasierende oder das lokale Profil aktueller ist. Ist das serverbasierende Profil aktueller, werden die geänderten Dateien aus diesem Profil auf das lokale System kopiert. Bei der Abmeldung wird das serverbasierende Profil durch die lokal veränderten Dateien aktualisiert. Bei der ersten Anmeldung eines Benutzers nach der Definition eines Profilpfads wird entweder ein vordefiniertes Profil vom Server geladen oder, wenn dieses leer ist, bei der Abmeldung das bisherige lokale Profil des Benutzers auf den Server kopiert. Die zweite Einstellung bezieht sich auf das Anmeldeskript. Hier kann angegeben werden, dass ein Programm ausgeführt werden soll, wenn sich ein Benutzer anmeldet. In den meisten Fällen handelt es sich um eine Batchdatei oder ein VB-Skript. Dieser Einstellung ist in aller Regel nicht mehr erforderlich, da Skripts für die An- und Abmeldung von Benutzern über die Gruppenrichtlinien konfiguriert werden können. Das Basisverzeichnis gibt an, welches Netzwerklaufwerk für den Benutzer automatisch verbunden werden soll. So kann ein lokaler Pfad auf der Arbeitsstation des Benutzers angegeben werden. Die Angabe der Pfadnamen erfolgt in der Regel unter Verwendung des Parameters *%username%*. Dadurch werden die Basisverzeichnisse automatisch nach dem Benutzernamen bezeichnet. Neben den Ordnern, mit denen die Inhalte der Arbeitsoberfläche und der Taskleiste inklusive des Startmenüs beschrieben werden, findet sich im

Profilpfad die Datei *Ntuser.dat*. Diese enthält die Einstellungen der Registry, die sich dort unter *HKEY_CURRENT_USER* finden. Die gesamten benutzerspezifischen Einstellungen sind hier enthalten. Die Benutzerprofile werden zunächst als Kopie des Standardprofils des *Default User* erzeugt.

Benutzerprofile für Terminalserver

Auf der Registerkarte *Terminaldienstprofile* können Sie angeben, ob ein Benutzer auf einem Terminalserver ein zusätzliches Profil bekommt. Die Einstellung des Profilpfads erlaubt die Verwendung eines zweiten Benutzerprofils für die Nutzung mit dem Terminalserver. Für die Anwender muss die Umgebung auf einem Terminalserver transparent sein, sie dürfen also keinen Unterschied bemerken, egal, auf welchem Server sie gerade arbeiten. Dazu muss aber auch gewährleistet sein, dass die Einstellungen, die ein Benutzer auf einem Server vornimmt, nach der Anmeldung auf dem anderen Server ebenfalls vorhanden sind. Dies ist nur möglich, wenn das Profil, das der Anwender auf dem Terminalserver verwendet, nach der Abmeldung zentral gespeichert und bei der Anmeldung auf einem beliebigen Terminalserver von dort wieder geladen wird. Beim Verwenden von gleichen Profilen auf den Arbeitsstationen und dem Terminalserver können sich Konflikte ergeben, wenn für die Terminalserver nicht ein eigenes Profil verwendet wird. Im Folgenden erfahren Sie an einem Beispiel, was bei der gemeinsamen Verwendung von Profilen auf Arbeitsstationen und Terminalservern passieren könnte:

1. Der Anwender meldet sich an seiner lokalen Arbeitsstation an und sein Profil wird vom Server geladen.
2. Während der Anwender an seiner Workstation angemeldet ist, startet er eine Sitzung auf einem der Terminalserver (zum Beispiel für die Arbeit mit SAP). Daraufhin wird auch hier das Profil vom Server geladen.
3. Der Anwender hat Änderungen an seinem Profil vorgenommen und meldet sich nun wieder vom Terminalserver ab. Daraufhin wird sein Profil auf den Server zurückgeschrieben.
4. Nachdem der Anwender seine Arbeit an seiner Arbeitsstation beendet hat, meldet er sich auch hier ab. Sein Profil wird nun erneut auf den Server zurückgeschrieben, überschreibt jetzt aber die Einstellungen, die er zuvor auf dem Terminalserver vorgenommen hat. Bei einer erneuten Anmeldung am Terminalserver sind die Einstellungen, die der Anwender während der letzten Sitzung vorgenommen hat, wieder verschwunden.

Sie sehen, es ist sinnvoll, ein zweites Profil für die Verwendung auf dem Terminalserver zu definieren, das an einer anderen Stelle gespeichert wird. Ebenso kann ein anderer Basisordner für die Verwendung am Terminalserver angegeben werden, falls zum Beispiel der Terminalserver an einem anderen Standort steht. In diesem Fall würde der Zugriff auf das Heimlaufwerk über ein langsames Netzwerk erfolgen. Um die Geschwindigkeit des Systems nicht unnötig auszubremsen, wird nun ein Verzeichnis auf einem Server angegeben, das sich im selben Standort befindet wie der Terminalserver selbst, und somit erfolgen die Zugriffe wieder lokal.

Verbindliche Profile (Mandatory Profiles)

Es wird zwischen *persönlichen* und *verbindlichen* Profilen unterschieden. Ein persönliches Profil kann nur einem Benutzer zugeordnet werden und dient diesem als Ausgangsposition. Die Anpassungen, die er vornimmt, werden in diesem Profil abgespeichert. Ein Benutzer, dem ein *verbindliches* Profil zugeordnet wurde, kann daran zwar Änderungen vornehmen, aber diese werden nicht

gespeichert. Bei Beginn jeder Arbeitssitzung hat er damit die gleichen Einstellungen für seine Arbeitsumgebung. Die Umwandlung eines normalen Profils in ein verbindliches Profil erfolgt durch die Umbenennung von *Ntuser.dat* in *Ntuser.man*. Verbindliche Profile können von mehreren Anwendern gemeinsam verwendet werden. Dazu wird für alle Anwender der gleiche Benutzerprofilpfad angegeben. Sie müssen nur einen Ordner auf dem Server erstellen, in dem das Profil gespeichert werden kann. Wenn ein Benutzer sich das erste Mal anmeldet, wird das Profil vom Server geladen. Wenn der Ordner leer ist, kann nichts geladen werden und das bisherige persönliche Profil des Benutzers wird verwendet. Ansonsten werden entweder das vordefinierte persönliche Profil oder das verbindliche Profil vom Server geladen und die bisherigen lokalen Einstellungen überschrieben. Wenn sich ein Benutzer abmeldet, wird das Profil auf dem Server aktualisiert. Die einzige Ausnahme ist die Verwendung eines verbindlichen Profils. In diesem Fall erfolgt keine Aktualisierung des serverbasierenden Profils. Eine Kopie des Profils wird lokal gespeichert.

Bei der nächsten Anmeldung werden die Daten für das lokale Profil und für das auf dem Server gespeicherte Profil verglichen. Das aktuellere der beiden Profile wird geladen. Gegebenenfalls wird das auf dem Server gespeicherte Profil aktualisiert. Ein verbindliches Profil wird bei jeder Anmeldung geladen. Falls der Server, auf dem das Profil gespeichert ist, nicht verfügbar ist, wird mit der lokal zwischengespeicherten Kopie dieses Profils gearbeitet. Durch die zentrale Speicherung auf dem Server wird aus dem Profil automatisch ein wanderndes Profil. Wenn sich ein Benutzer an einer anderen Arbeitsstation anmeldet, wird bei der Anmeldung über den Eintrag für den Benutzerprofilpfad bei den Eigenschaften des Benutzers in *Active Directory-Benutzer und -Computer* erkannt, dass dieser Benutzer ein Benutzerprofil hat. Es wird geladen, weil bei der ersten Anmeldung auf einer neuen Arbeitsstation dort kein lokal zwischengespeichertes Profil vorhanden sein kann, sodass der Benutzer auf jeder Arbeitsstation mit dem gleichen Profil arbeiten kann.

Super verbindliche Profile (Super Mandatory Profiles)

Eine weitere Steigerung von verbindlichen Profilen sind *Super verbindliche Profile*. Bei einem solchen Profil kann sich der Anwender nur dann am PC anmelden, wenn das verbindliche Profil auf dem Server zur Verfügung steht. Wenn der Windows Vista-PC keine Verbindung zum Server aufbauen kann, wird die Anmeldung verweigert. Um ein solches verbindliches Profil zu erstellen, gehen Sie zunächst genauso vor wie beim Anlegen eines verbindlichen Profils:

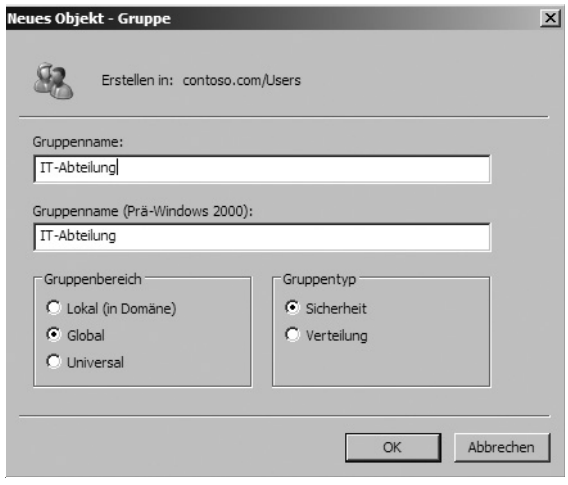
1. Als Nächstes ändern Sie den Namen des Benutzerprofil-Verzeichnisses so ab, dass dieser Ordner der Syntax *<Profilname>.man.v2* entspricht.
2. Als Nächstes fügen Sie auf der Registerkarte *Profil* im Active Directory hinter den Pfad des Benutzerprofils noch die Endung *.man* hinzu, diesmal ohne das *v2*.
3. Durch diese Aktion wurde aus dem verbindlichen Profil mit der Datei *ntuser.man* ein Super verbindliches Profil, bei dem auch der Ordner des Profils die Endung *.man.v2* hat.

Gruppen verwalten

Nicht weniger wichtig als die Verwaltung von Benutzern ist die Verwaltung von Gruppen in Active Directory. Gruppen werden ebenfalls im Snap-In *Active Directory-Benutzer und -Computer* erstellt und verwaltet. Wählen Sie im Menü *Neu* die Option *Gruppe* aus. In Active Directory werden die folgenden vier Gruppentypen unterschieden:

- Lokal
- Domänenlokal
- Global
- Universal

Abbildg. 10.25 Erstellen einer neuen Gruppe



Bei der Unterscheidung und Verwendung dieser Gruppen können folgende Bereiche beachtet werden:

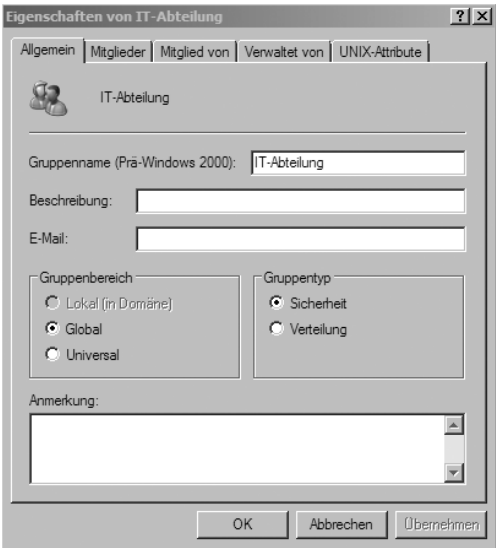
- *Lokale Gruppen* werden für die Zusammenfassung von globalen Gruppen oder in Ausnahmefällen Benutzern eingesetzt, denen Zugriffsberechtigungen erteilt werden. Aus lokalen Gruppen werden beim Wechsel in den einheitlichen Modus von Active Directory automatisch domänenlokale Gruppen. Der Unterschied besteht darin, dass diese Gruppen einheitlich auf allen Windows 2000-, Windows Server 2003- und Windows Server 2008-Mitgliedssystemen sowie Windows NT-Maschinen der Domäne zu sehen sind. Der Vorteil ist, dass damit eine lokale Gruppe im einheitlichen Modus nur einmal pro Domäne definiert werden muss.
- *Globale Gruppen* sind überall in der Gesamtstruktur sichtbar, können aber nur Mitglieder aus der eigenen Domäne enthalten. Globale Gruppen können Mitglied von lokalen und universellen Gruppen werden. Im einheitlichen Modus können globale Gruppen zudem verschachtelt werden.
- Ein weiterer Gruppentyp sind die *universellen Gruppen*. Alle Informationen über Zugehörigkeiten zu universellen Gruppen werden auf den globalen Katalogservern gespeichert.

Neben den verschiedenen Gruppenbereichen können zwei unterschiedliche Gruppentypen erstellt werden.

- **Sicherheit** definiert, dass es sich um eine Gruppe handelt, über die Zugriffsberechtigungen zugeordnet werden sollen. Diese Gruppe kann zusätzlich als E-Mail-Verteilerliste verwendet werden.
- **Verteilung** gibt an, dass die Gruppe nur für Verteiler in E-Mail-Programmen verwendet werden kann. Sie kann nicht für die Zuordnung von Zugriffsberechtigungen eingesetzt werden.

Die Eigenschaften von Gruppen können genauso bearbeitet werden wie die Eigenschaften von Benutzerkonten. Es stehen allerdings weniger Optionen zur Verfügung.

Abbildg. 10.26 Verwalten von Gruppen in Windows Server 2008



- Neben dem Gruppennamen kann eine Beschreibung für die Gruppe eingegeben werden, die in den Listen des Verwaltungsprogramms *Active Directory-Benutzer und -Computer* angezeigt wird.
- Auf der Registerkarte *Mitglieder* können über die Schaltflächen *Hinzufügen* und *Entfernen* neue Benutzer in Gruppen aufgenommen beziehungsweise aus diesen gelöscht werden.
- Auf der Registerkarte *Mitglied von* werden die Gruppen angezeigt, in denen diese Gruppe Mitglied ist.
- Über die Registerkarte *Verwaltet von* kann der Benutzer, der für eine Gruppe zuständig ist, konfiguriert werden. Dazu wird über die Schaltfläche *Ändern* eine Liste der Benutzer und Gruppen geöffnet, aus der der entsprechende Benutzer ausgewählt werden kann.

Computerkonten in Active Directory

Für jeden Rechner im Netzwerk wird ein Computerkonto im Active Directory benötigt. Ein Computerkonto wird automatisch angelegt, wenn Sie einen PC oder Server zur Domäne hinzufügen. Domänencontroller werden im Ordner *Domain Controllers* abgelegt, während normale Systeme im Container *Computers* landen. Bei der Installation kann nur die Domäne angegeben werden, keine Organisationseinheit. Nach der Installation kann ein neues Computerobjekt in die entsprechende OU verschoben werden. Computerkonten können aber durch Administratoren auch vor der Domäneaufnahme in der Domäne selbst erstellt werden. Dadurch können die Computer nämlich gleich gezielt in den Container aufgenommen werden, für den sie vorgesehen sind. Bei der Installation kann dagegen nur die Domäne angegeben werden, keine Organisationseinheit. Beim Anlegen eines Computerobjekts muss ein Computername definiert werden (Abbildung 10.27).

Abbildg. 10.27 Erstellen eines Computerkontos in der Domäne

Über den Assistenten kann der Benutzer oder – besser – die Gruppe angegeben werden, die diesen Computer installieren darf. Hier kann auch eine Operatoren-Gruppe ausgewählt werden, die für die Installation neuer Systeme zuständig ist. Hier kann auch die Option *Dieses Computerkonto als einen Prä-Windows 2000-Computer zuweisen* konfiguriert werden, sodass Downlevel-Clients über dieses Computerkonto in eine Domäne aufgenommen werden können. Eine weitere Einstellung ist *Verwalteter Computer*. Diese können Sie im nächsten Dialogfeld vornehmen. Sie müssen die vollständige GUID – eine ziemlich lange Zeichenfolge – des Systems eingeben. Damit wird festgelegt, dass dieses Computerkonto für eine genau definierte Maschine verwendet wird, die eine eindeutige GUID besitzt. Diese wird vom Hersteller definiert.

Abbildg. 10.28 Computerkonten in Active Directory verwalten

In den Eigenschaften können eine Reihe weiterer Einstellungen festgelegt werden. Dazu gehört neben der obligatorischen Eingabe einer Beschreibung die Option *Computer für Delegierungszwecke vertrauen* auf der Registerkarte *Delegierung*. Diese Option ist sicherheitssensibel. Damit können lokal ausgeführte Dienste auf diesem System Dienste von anderen Systemen anfordern. Grundsätzlich ist dies kein Problem, wenn aber durch irgendeinen Angriff die lokale Sicherheit des Systems kompromittiert ist, wird dadurch ein illegaler Zugriff auf andere Serverdienste möglich, soweit diese einen Zugriff des Computers von sich aus erlauben. Daher sollte diese Option nur gewählt werden, wenn es für Anwendungen zwingend erforderlich ist. Bei den Eigenschaften stehen darüber hinaus noch mehrere Registerkarten zur Auswahl:

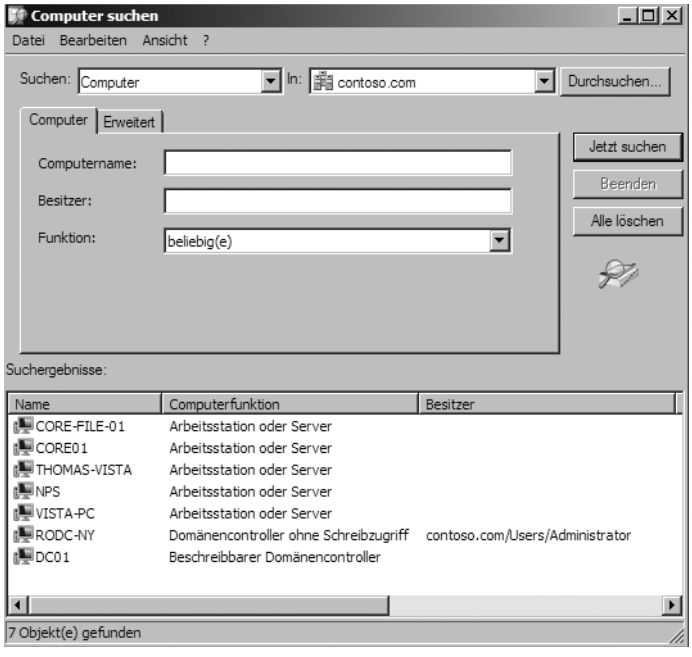
- Auf der Registerkarte *Allgemein* finden sich Informationen über den NetBIOS- und DNS-Namen sowie die Funktion des Systems. Die Einstellungen in diesem Dialogfeld können nicht verändert werden. Der NetBIOS-Name wird als *Prä-Windows 2000* bezeichnet. In den Eigenschaften für Domänencontroller kann auf dieser Registerkarte festgelegt werden, ob der DC als *Globaler Katalog* fungieren soll. Dazu wird die Schaltfläche *NTDS-Einstellungen* verwendet.
- Die Registerkarte *Betriebssystem* hat informativen Charakter. Hier werden der Name des Betriebssystems, die Version und gegebenenfalls die Version des zuletzt eingespielten Service Packs angegeben.
- Über die Registerkarte *Mitglied von* kann die Gruppenzugehörigkeit des Systems konfiguriert werden.
- Auf der Registerkarte *Standort* wird der Standort des Systems angegeben. Dieser kann bei Domänencontrollern nur verändert werden, wenn Sie als Administrator in der gleichen Domäne angemeldet ist, in der der Domänencontroller steht oder über eine Gruppenzugehörigkeit in dieser Domäne administrative Berechtigungen besitzt.
- Die Registerkarte *Verwaltet von* enthält Informationen zu dem Benutzer, der für die Administration des Domänencontrollers zuständig ist. Diese Informationen können nicht verändert werden.
- Auf der Registerkarte *Einwählen* sind RAS-Berechtigungen für diesen Computer definiert, falls dieser eine automatische Einwahl durchführt.
- Die Registerkarte *UNIX-Attribute* dient bei installiertem NFS zur Anbindung des Computers an eine Unix-Domäne.

Bei Computer-Objekten gibt es im Kontextmenü im Wesentlichen die gleichen Befehle wie bei Domänencontrollern. Im Unterschied zu Domänencontrollern findet sich im Kontextmenü der Befehl *Konto deaktivieren*, mit dem ein Computerkonto gesperrt werden kann. Die Konsequenz daraus ist, dass von diesem Computer aus keine Anmeldung in der Domäne mehr erfolgen kann. Ansonsten gibt es keine funktionalen Unterschiede. Allerdings können Computerobjekte sehr viel flexibler verwaltet werden.

Suchen nach Informationen im Active Directory

In *Active Directory-Benutzer und -Computer* steht im Kontextmenü der Container jeweils der Befehl *Suchen* zur Verfügung. Über diesen Befehl kann eine Suche im Active Directory durchgeführt werden. Das ist vor allem bei sehr großen Verzeichnissen hilfreich, wenn Objekte nicht auf Anhieb in der definierten Struktur gefunden werden. Allerdings sollte ein Verzeichnis im Idealfall so strukturiert sein, dass die Suchfunktion nicht erforderlich ist, weil immer klar ist, in welchem Container sich welches Objekt befindet.

Abbildg. 10.29 Nach Objekten im Active Directory suchen



Im angezeigten Dialogfeld kann oben im Auswahlfeld *Suchen* zunächst definiert werden, wonach gesucht werden soll. Hier können die Optionen ausgewählt werden:

- Benutzer, Kontakte und Gruppen
- Computer
- Drucker
- Freigegebene Ordner
- Organisationseinheiten

- Benutzerdefinierte Suche
- Remoteinstallationsserver
- Allgemeine Abfragen
- Remoteinstallationsclients
- Message Queuing-Warteschlangen

Im Feld *In* kann der Bereich der Suche konfiguriert werden. Sie können einzelne Container, Teile der Domänenstruktur oder das gesamte Verzeichnis auswählen. Je nachdem, was gesucht wird, können im unteren Bereich unterschiedliche Suchkriterien festgelegt werden. Hier können die allgemeinen Kriterien auf der ersten der beiden Registerkarten konfiguriert werden. Über die Registerkarte *Erweitert* lassen sich alle Feldnamen (Attribute) für die Suche auswählen. Wenn die *Benutzerdefinierte Suche* gewählt wird, kann eine LDAP-Suchabfrage manuell eingegeben werden. Damit wird die optimale Flexibilität bei der Gestaltung der Suche geboten. Da nach jedem Attribut gesucht werden kann, lassen sich mit dieser Suchfunktion sehr flexible Abfragen gestalten. So können schnell alle Benutzer mit konfiguriertem RAS-Zugang ermittelt werden, indem einfach nach dem entsprechenden Feld abgefragt wird. In sehr großen Verzeichnissen lassen sich damit alle Informationen schnell finden.

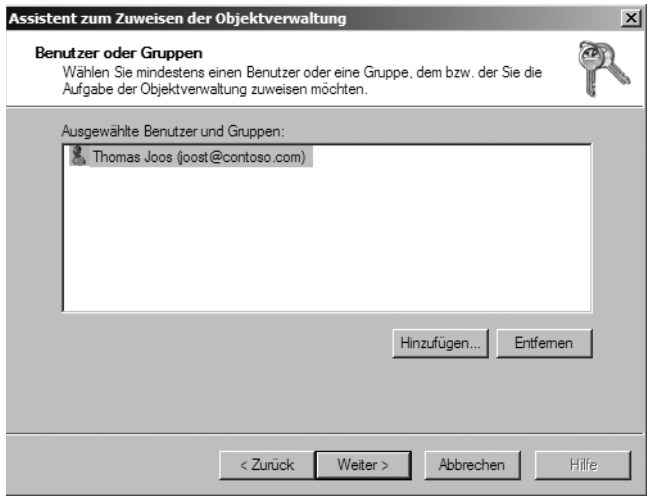
Delegieren von Administrationsaufgaben

Mit Hilfe eines Assistenten können Berechtigungen in einfacher Weise delegiert werden. Dadurch lassen sich einzelne Administrationsaufgaben durch die Aufteilung der OUs verteilen. Dieser Abschnitt geht etwas genauer auf die Delegierung von Administrationsaufgaben im Bereich Active Directory ein. Klicken Sie mit der rechten Maustaste auf eine Organisationseinheit oder eine Domäne, können Sie mit Hilfe des Befehls *Objektverwaltung zuweisen* im Kontextmenü einzelne Aufgaben an verschiedene Benutzergruppen delegieren (Abbildung 10.31). Die Delegierung von Berechtigungen im Active Directory kann auf verschiedenen Ebenen erfolgen:

- Sie kann auf der Ebene der Domäne mit Gültigkeit für die gesamte Domäne vorgenommen werden. Es können allerdings für untergeordnete Organisationseinheiten Abweichungen davon eingerichtet werden.
- Sie kann auf der Ebene von Organisationseinheiten durchgeführt werden.
- Sie kann auch über die Zugriffsberechtigungen für Objekte vorgenommen werden. So kann über die Sicherheitseinstellungen einer Gruppe festgelegt werden, dass diese nur von bestimmten Operatoren verwaltet werden darf. Allerdings kann die Delegierung nicht über den Assistenten für die Delegierung von administrativen Berechtigungen erfolgen, da dieser nur eine Delegierung auf der Ebene von Domänen und Organisationseinheiten unterstützt, sondern muss über die konkrete Konfiguration der Sicherheitseinstellungen des Objekts durchgeführt werden.

Das wichtigste Werkzeug für die Delegierung von Berechtigungen ist ein Assistent, der über das Kontextmenü von Domänen und Organisationseinheiten aufgerufen werden kann. Er wird mit dem Befehl *Objektverwaltung zuweisen* gestartet. Der Assistent führt schrittweise durch die Konfiguration der Berechtigungen.

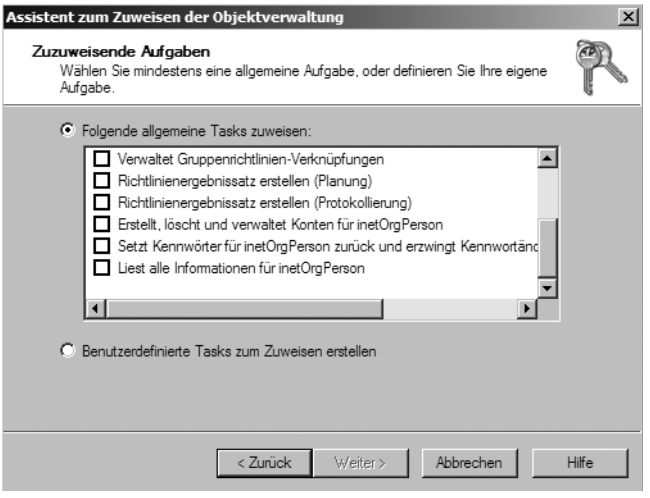
Abbildg. 10.30 Delegierung von Administrationsberechtigungen im Active Directory



Der erste Schritt bei der Delegierung von Berechtigungen ist die Auswahl der Benutzer oder Gruppen, denen Sie eine administrative Aufgabe zuweisen wollen. Durch Anklicken der Schaltfläche *Hinzufügen* können Sie aus einem weiteren Dialogfeld die Benutzer oder Benutzergruppen auswählen Der nächste Schritt ist die Auswahl der zuzuweisenden Aufgaben:

- Mit *Fügt einen Computer einer Domäne hinzu* kann delegiert werden, welche Benutzer neue Systeme in eine Domäne aufnehmen dürfen.
- Die Aufgabe *Verwaltet Gruppenrichtlinien-Verknüpfungen* gibt die Möglichkeit, vorhandene Gruppenrichtlinien zu Objekten zuzuordnen.
- Die Auswahl *von Erstellt, entfernt und verwaltet Benutzerkonten* delegiert die Berechtigung für das Anlegen von Benutzern in einer Organisationseinheit.
- Mit *Setzt Benutzerkennwörter zurück* kann selektiv die Berechtigung vergeben werden, dass ein Benutzer Kennwörter anderer Benutzer ändern darf. Damit kann der operative Aufwand vom Helpdesk in die Fachabteilungen verlegt werden, indem dort ausgewählte Benutzer Kennwörter zurücksetzen können, wenn andere Benutzer ihr Kennwort vergessen haben.
- Die Option *Liest alle Benutzerinformationen* ermöglicht den vollen Zugriff auf alle Informationen zu Benutzerkonten.
- Mit *Ändert die Mitgliedschaft einer Gruppe* können keine neuen Gruppen erstellt, aber Gruppenzugehörigkeiten von Benutzern und Gruppen angepasst werden.
- Weitere Möglichkeiten sind die Erstellung eines Richtlinienergebnissatzes für die Planung von Gruppenrichtlinien und die Verwaltung des Benutzertyps *InetOrgPerson*.

Abbildg. 10.31 Delegieren von Administrationsaufgaben

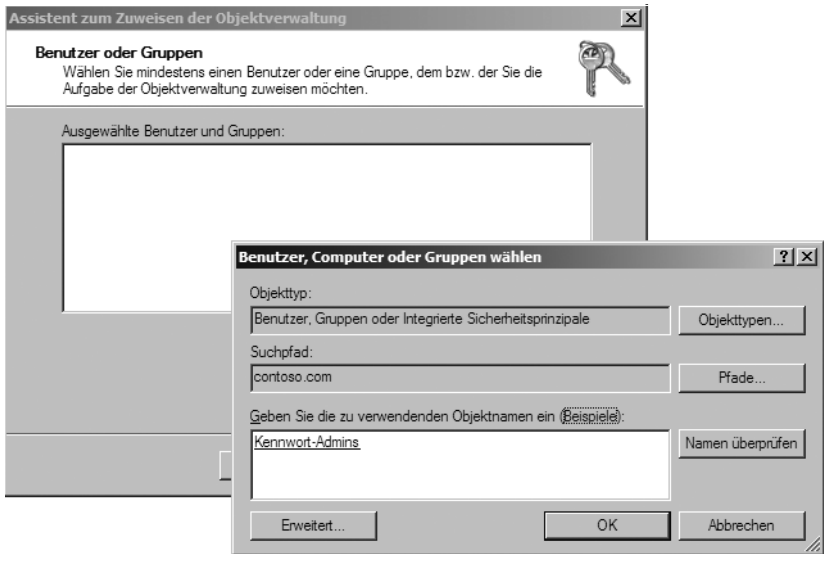


Szenario: Delegierung zum administrativen Verwalten einer Organisationseinheit

Ein gutes Praxisbeispiel für die Delegierung von Benutzerrechten im Active Directory ist das Zurücksetzen von Kennwörtern. Wenn Anwender ihr Kennwort vergessen oder ein neues Kennwort zugewiesen bekommen, sollte das nicht die Aufgabe der Systemadministratoren sein. In diesem Fall könnte zum Beispiel der Abteilungsleiter oder ein Poweruser diese Aufgaben übernehmen. Es besteht außerdem die Möglichkeit, an einen Benutzer genau diese Rechte für seine OU zu delegieren und ihm im Anschluss ein speziell angepasstes Administrationsprogramm zur Verfügung zu stellen, mit dem er diese Aufgabe durchführen kann. Bei der Delegierung in diesem Beispiel wird dem entsprechenden Anwender nicht nur die Berechtigung zum Zurücksetzen der Kennwörter, sondern auch die komplette Verwaltung der Benutzer seiner OU zugewiesen. In Ihrem Unternehmen können Sie dazu bei der Objektverwaltung statt des Vollzugriffs einfach nur das Recht zum *Zurücksetzen von Kennwörtern* delegieren. Gehen Sie dazu folgendermaßen vor:

1. Legen Sie zunächst eine globale Benutzergruppe an, welche die Rechte der Delegierung enthält. Auch wenn die Gruppe zunächst nur einen Benutzer enthält, sollten Sie in den Berechtigungen von Active Directory niemals nur einzelne Konten eintragen. Wenn Sie Änderungen durchführen wollen, zum Beispiel noch eine Urlaubsvertretung berechtigen oder einen anderen Benutzer dazu berechtigen wollen, müssen Sie den entsprechenden Benutzer nur in die Gruppe aufnehmen, ohne Änderungen in den Berechtigungen von Active Directory durchführen zu müssen.
2. Klicken Sie mit der rechten Maustaste auf die OU, in der die Benutzerkonten abgelegt sind, deren Verwaltung Sie delegieren wollen. Wählen Sie im Kontextmenü den Befehl *Objektverwaltung zuweisen* aus.
3. Fügen Sie im Assistenten die angelegte Gruppe hinzu, der Sie das Recht zur Verwaltung der OU geben wollen.

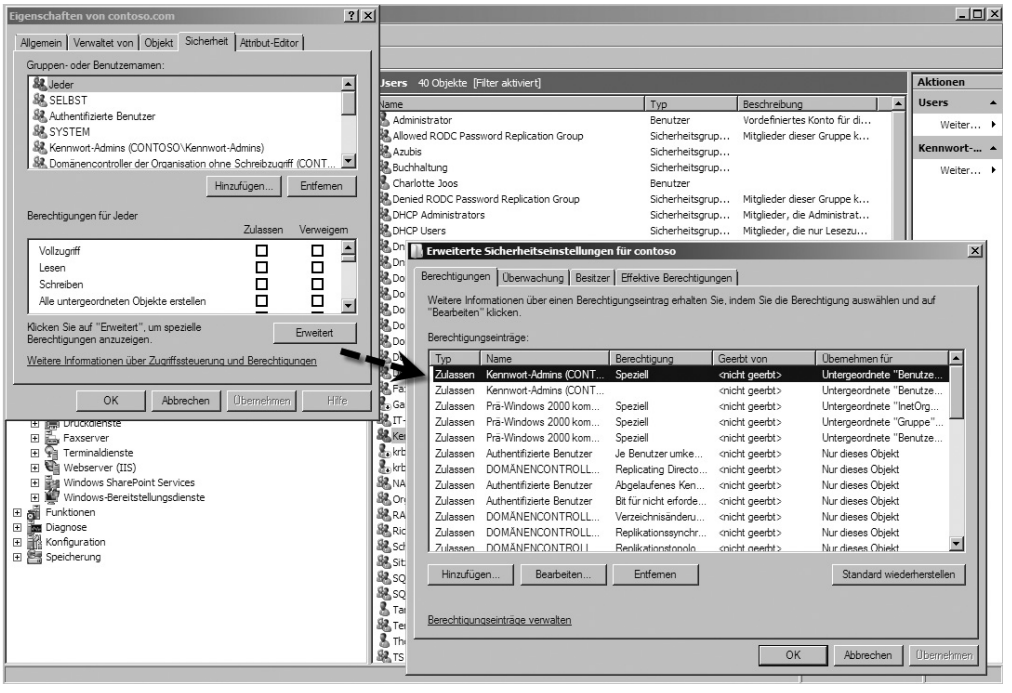
Abbildg. 10.32 Delegieren von Kennwortberechtigungen und auswählen einer entsprechenden Gruppe für diese Aufgabe



4. Aktivieren Sie im nächsten Fenster als zuzuweisende Aufgabe das Kontrollkästchen *Erstellt, entfernt und verwaltet Benutzerkonten*. Wenn Sie den entsprechenden Nutzern nur das Recht zum Ändern der Kennwörter geben wollen, können Sie hier auch die Option *Setzt Benutzerkennwörter zurück und erzwingt Kennwortänderung bei der nächsten Anmeldung* verwenden.
5. Beenden Sie den Assistenten, um die Delegierung abzuschließen.

Die entsprechenden Rechte für diese Gruppe finden Sie, indem Sie zunächst im Snap-In *Active Directory-Benutzer und -Computer* über den Menübefehl *Ansicht/Erweiterte Features* die erweiterten Ansichtsfunktionen aktivieren. Wenn Sie danach die Eigenschaften der OU oder der Domäne aufrufen, wird die Registerkarte *Sicherheit* angezeigt (Abbildung 10.33). Klicken Sie hier auf *Erweitert*, finden Sie im folgenden Fenster auf der Registerkarte *Berechtigungen* die genauen Rechte der Gruppe aufgelistet. Wenn Sie die Delegierung wieder rückgängig machen wollen, müssen Sie einfach an dieser Stelle die Rechte der Gruppe wieder entfernen.

Abbildg. 10.33 Anzeigen der delegierten Berechtigungen auf der Registerkarte *Sicherheit* des delegierten Containers



Installation der Verwaltungsprogramme für die delegierten Aufgaben

Nachdem die Gruppe die entsprechenden Rechte zur Verwaltung dieser OU bekommen hat und Sie die Benutzer in die Gruppe aufgenommen haben, sollten Sie den entsprechenden Benutzern noch ein Administrationsprogramm zur Verfügung stellen, über dass sie die OU verwalten können. Entweder arbeiten die Anwender dazu über den Remote Desktop auf einem Server, oder Sie müssen die *Remote Server Administration Tools (RSAT)* auf einem Windows Vista PC installieren.

Zusammenfassung

Auch wenn die Verwaltung der Benutzer und die Delegation von Rechten noch sehr ähnlich zu Windows Server 2003 ist, haben Sie in diesem Kapitel erfahren, dass vor allem im Bereich der Benutzerprofile und der Verwendung von servergespeicherten Profilen Änderungen integriert wurden, welche die Möglichkeiten im Netzwerk deutlich verbessern. Im nächsten Kapitel zeigen wir Ihnen am Beispiel der wichtigen Infrastrukturdienste WINS, DNS und DHCP, wie Arbeitsstationen der Anwender optimal im Netzwerk betrieben werden können.

Kapitel 11

Infrastrukturdienste – DNS, DHCP und WINS

In diesem Kapitel:

In diesem Kapitel beschäftigen wir uns mit den wichtigen Infrastrukturdiensten von Windows Server 2008. Über diese Dienste werden Funktionen im Netzwerk bereitgestellt, die von anderen Servern, aber auch Arbeitsstationen genutzt werden. Die wichtigen Infrastrukturdienste DNS, DHCP und WINS sind auch bereits unter den Vorgängerversionen von Windows Server 2008 genutzt worden. In der neuen Version unterstützen diese allerdings den neuen TCP/IP-Stack sowie ein paar neue Funktionen.

WINS einsetzen

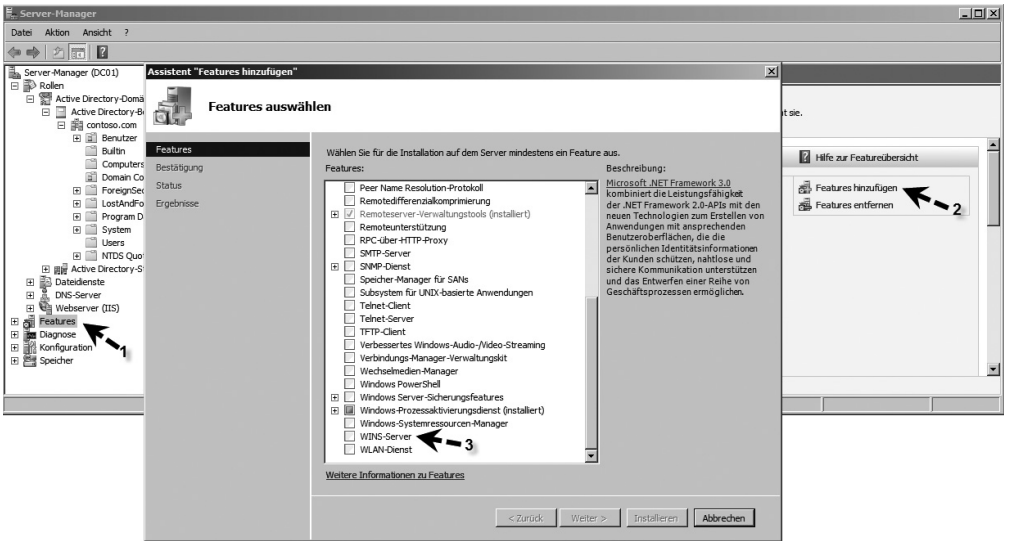
WINS steht für Windows Internet Name Service und ist der Vorgänger der dynamischen DNS-Aktualisierung. Vor allem in Umgebungen mit mehreren Domänen kann daher eine WINS-Auflösung eine wertvolle Ergänzung zu DNS sein. Die Namensauflösung in einem Netzwerk ist von existentieller Bedeutung, daher schadet es sicher nicht, parallel zu einer vernünftigen DNS-Struktur auch auf WINS zu setzen. Vor allem wenn noch ältere Clients im Netzwerk betrieben werden, oder bei einem Ausfall der DNS-Infrastruktur, kann ein WINS-Server wertvolle Hilfe sein. Während DNS für die Namensauflösung mit vollqualifizierten Domänennamen zuständig ist, werden mit WINS NetBIOS-Namen aufgelöst. Die Namensauflösung in einem Active Directory ist überaus wichtig. Aus diesen Gründen gehört zur Erstellung eines Active Directory auch die Integration von WINS dazu. Sie können auf den Domänencontrollern neben DNS auch ohne weiteres den WINS-Dienst installieren, da dieser so gut wie keine Auswirkungen auf das System hat. DNS kann darüber hinaus eng mit WINS zusammenarbeiten.

HINWEIS Seit Windows Server 2003 SP1 wurden Erweiterungen in das Betriebssystem integriert, welche die Namensauflösung zur Replikation von Active Directory über WINS abwickeln können, falls DNS Probleme hat. Diese Verbesserungen sind auch in Windows Server 2008 übernommen worden.

Installation eines WINS-Servers

WINS ist eine Serverfunktion, keine Rolle unter Windows Server 2008. Um den WINS-Dienst zu installieren, rufen Sie im Server-Manager über *Features/Features hinzufügen* den Assistenten zur Installation von neuen Serverfeatures auf. Die vorletzte Funktion im Fenster ist *WINS-Server*. Wählen Sie zur Installation dieses Feature aus (Abbildung 11.1). Es müssen keine weiteren Eingaben gemacht werden, damit der Dienst installiert wird. Nach der Installation steht WINS sofort zu Verfügung. Es müssen keine Zonen erstellt und auch keine dynamischen Updates aktiviert werden. WINS funktioniert sofort nach der Installation uneingeschränkt.

Abbildg. 11.1 Installieren von WINS unter Windows Server 2008



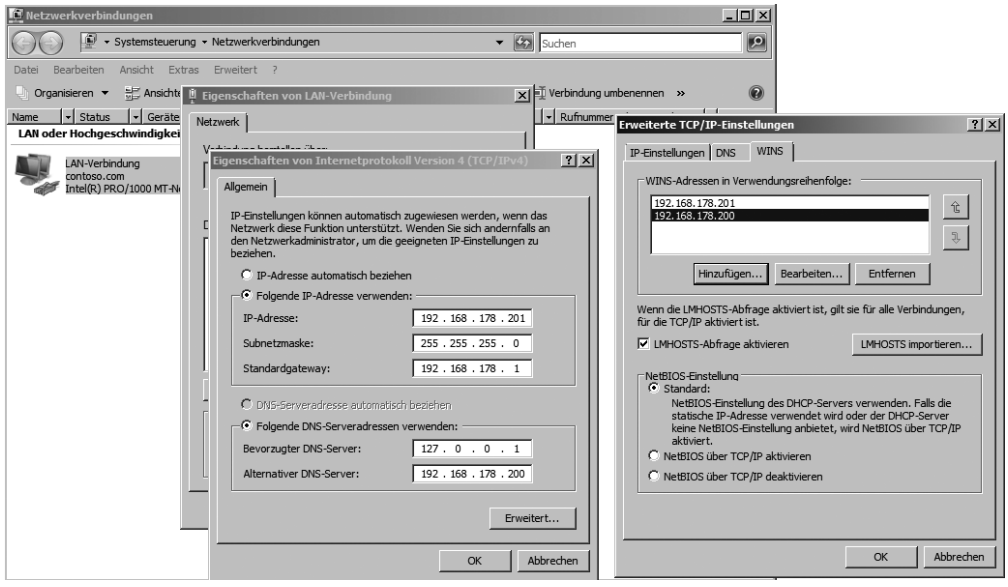
Konfiguration der IP-Einstellungen für WINS

Damit sich die Server und Arbeitsstationen beim WINS registrieren und Daten aus WINS abfragen können, müssen Sie in den IP-Einstellungen der Server die WINS-Server eintragen. Sie müssen nicht auf allen Domänencontrollern einer Domäne WINS installieren, zwei WINS-Server pro Standort reichen durchaus aus. Wenn Sie auf den beiden Domänencontrollern in diesem Workshop WINS installiert haben, können Sie in den *IP-Einstellungen* der Computer unter *Erweitert* auf der Registerkarte *WINS* die beiden WINS-Server hinzufügen (Abbildung 11.2). Diese IP-Einstellungen sollten Sie auf allen Mitgliedsservern und Arbeitsstationen einrichten, damit die Namensauflösung im Netzwerk optimal funktioniert. Auf den Arbeitsstationen können Sie diese Einstellungen auch mit Hilfe eines DHCP-Servers verteilen.

Neben der Namensauflösung über WINS kann auch eine lokal gespeicherte Textdatei *LMHosts* verwendet werden. Dies ist allerdings sehr aufwändig, da diese Datei auf alle Computer im Netzwerk verteilt werden muss. Die NetBIOS-Namensauflösung funktioniert generell auch ohne den Einsatz eines WINS-Servers, wobei die gesuchte IP-Adresse über Broadcasts ins Netzwerk ermittelt wird. Ob ein Computer diese Broadcasts und/oder einen WINS-Server verwendet, ist über den NetBIOS-Knotentyp festgelegt. Hier gibt es vier verschiedene Knotentypen:

- **P (Peer)** Es wird lediglich die WINS-Abfrage durchgeführt. Bleibt diese ohne Ergebnis, wird keine weitere Abfrage durchgeführt.
- **H (Hybrid)** Zunächst wird die WINS-Abfrage durchgeführt. Bleibt diese ohne Ergebnis, wird die Namensauflösung über Broadcast durchgeführt.
- **M (Mixed)** Zunächst wird die Namensauflösung über Broadcast durchgeführt. Bleibt diese ohne Ergebnis, wird die WINS-Abfrage durchgeführt.
- **B (Broadcast)** Es wird lediglich die Namensauflösung über Broadcast durchgeführt. Bleibt diese ohne Ergebnis, wird keine weitere Abfrage durchgeführt.

Abbildg. 11.2 Konfiguration der Computer für die Verwendung von WINS

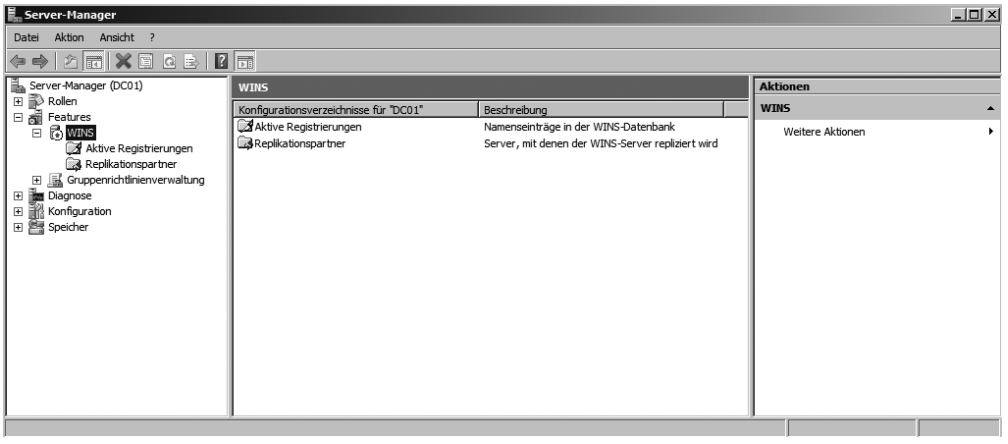


Bei einer durchgehenden Verwendung von WINS sollten Sie den Knotentyp auf P-Knoten einstellen, da ein Broadcast auch nicht zu einem Ergebnis führen wird, weil alle Computer beim WINS-Server registriert sind. Alternativ kann der Knotentyp auch über den DHCP-Server gesetzt werden. Sobald Sie die Unterstützung für NetBIOS-Namen nicht mehr benötigen, können Sie diese abschalten. Wann und ob das möglich ist, hängt von der verwendeten Software ab. Der Vorteil einer deaktivierten NetBIOS-Unterstützung liegt in der verminderten Netzlast, die unter anderem durch den Wegfall der Registrierung des Computers beim so genannten Suchdienst und die Beschränkung der Namensauflösung auf DNS zustande kommt. Wenn Sie die Einstellung direkt am Computer vornehmen wollen, wählen Sie auf der Registerkarte *WINS* die Option *NetBIOS über TCP/IP deaktivieren*. Alternativ können Sie diese Einstellung auch über einen DHCP-Server vornehmen.

Einrichten der WINS-Replikation

Nachdem WINS installiert und eingerichtet sowie die IP-Einstellungen auf den Servern angepasst wurden, sollte die Replikation der WINS-Server eingerichtet werden, damit sich die Datenbanken untereinander abgleichen. Für die Verwaltung von WINS wird das Snap-In *WINS* verwendet, das Sie auf die gleiche Weise wie andere Snap-Ins einer MMC hinzugefügt werden können. Die Verwaltung kann auch über den Server-Manager durchgeführt werden. Nach der Installation dieser Funktion erscheint das Verwaltungsprogramm unterhalb des Eintrags *Features* (Abbildung 11.3).

Abbildg. 11.3 Verwalten von WINS über den Server-Manager

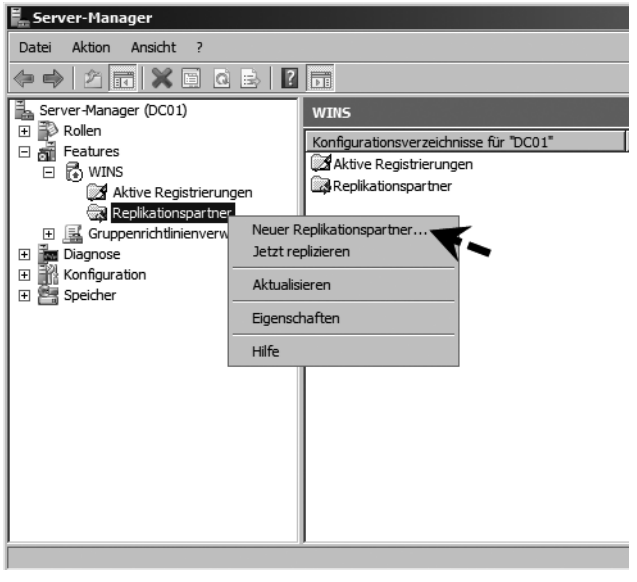


Nach der Installation sollte der WINS-Dienst als aktiv und verbunden angezeigt werden (Abbildung 11.3).

WINS hat eine eigene Datenbank und kann seine Daten nicht wie DNS in Active Directory speichern. Aus diesem Grund muss auf WINS-Servern die Replikation manuell und getrennt von Active Directory eingerichtet werden:

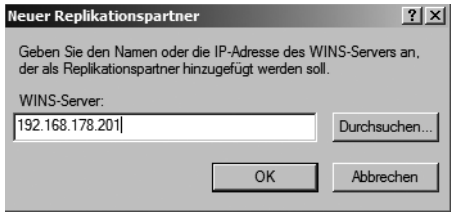
1. Klicken Sie zunächst mit der rechten Maustaste im Knoten *WINS* auf den Eintrag *Replikationspartner* und wählen im Kontextmenü den Befehl *Neuer Replikationspartner* aus (Abbildung 11.4).

Abbildg. 11.4 Hinzufügen von Replikationspartnern zu WINS-Servern



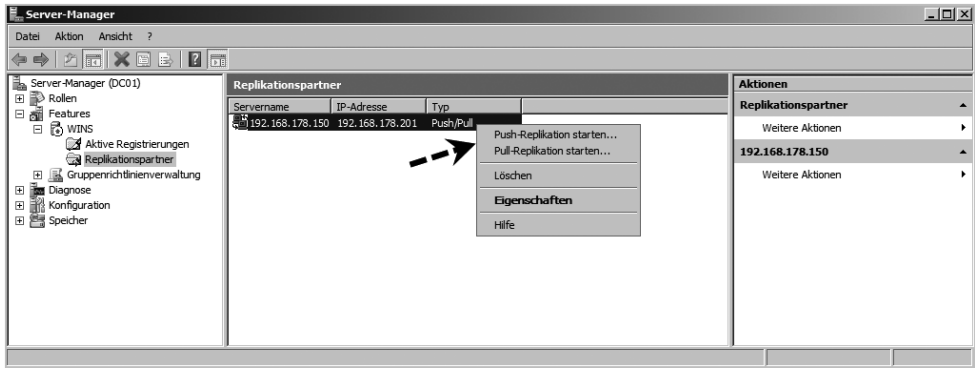
2. Tragen Sie die IP-Adresse des anderen Servers ein. Sie können an dieser Stelle die Datenbank auch durchsuchen, aber das manuelle Eintragen der IP-Adresse geht oft schneller, vor allem wenn die WINS-Datenbank noch keine Einträge enthält.

Abbildg. 11.5 Auswählen eines Replikationspartners für WINS



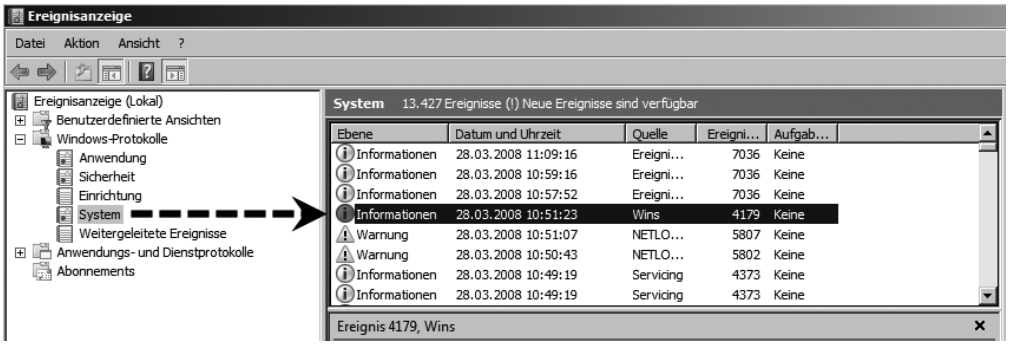
3. Wenn Sie die Replikationspartner auf allen WINS-Servern eingetragen haben, können Sie mit der rechten Maustaste auf die Replikationsverbindung klicken und im Kontextmenü zunächst den Befehl *Push-Replikation starten* und dann den Befehl *Pull-Replikation starten* auswählen (Abbildung 11.6).

Abbildg. 11.6 Starten der WINS-Replikation auf einem WINS-Server



Im Anschluss müssen Sie noch vorgeben, ob die Replikation an alle oder nur an den ausgewählten Replikationspartner übermittelt werden soll. Nachdem die Replikation angestoßen wurde, erscheint keine weitere Meldung und die Replikation beginnt. Überprüfen Sie in der Ereignisanzeige, ob Fehler angezeigt werden. Kurz nach der Einrichtung besteht durchaus die Möglichkeit, dass noch Fehler angezeigt werden. Diese sollten aber nach einiger Zeit nicht mehr auftauchen, wenn die Replikation gestartet wird. WINS-Meldungen finden Sie in der Ereignisanzeige unter *Windows-Protokolle/System* (Abbildung 11.7).

Abbildg. 11.7 WINS-Meldungen werden in der Ereignisanzeige festgehalten

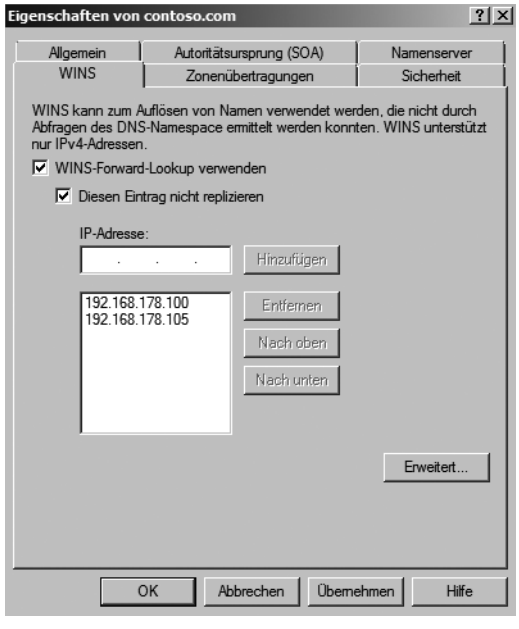


Die Einrichtung ist abgeschlossen, wenn die Replikation fehlerfrei stattfindet.

Integration von WINS in DNS

Um WINS in DNS zu integrieren, müssen Sie die Eigenschaften der einzelnen Zonen im DNS öffnen. Dort kann auf der Registerkarte *WINS* die Option *WINS-Forward-Lookup verwenden* ausgewählt und die IP-Adresse eines WINS-Servers angegeben werden. Richtet ein Client eine Anfrage an den DNS-Server, versucht dieser zunächst diese Anfrage über die lokalen Informationen in der DNS-Datenbank zu beantworten. Wenn ihm das nicht gelingt, sendet er den Hostnamen an den WINS-Server. Dieser versucht, die Anfrage zu beantworten, und liefert gegebenenfalls das Ergebnis an den DNS-Server zurück. Die Konfiguration muss für jede DNS-Domäne erfolgen (Abbildung 11.8).

Abbildg. 11.8 WINS-Forward-Lookup verwenden, um die Namensauflösung zu optimieren

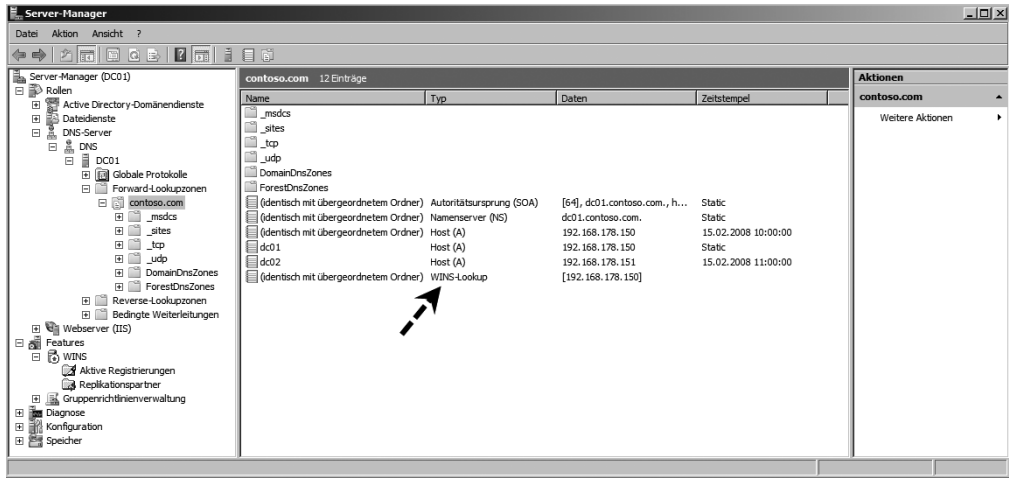


Sie können in den einzelnen DNS-Zonen alle WINS-Server einrichten, um auch an dieser Stelle eine Ausfallsicherheit zu erreichen. Die Einstellungen müssen nicht für jeden DNS-Server, sondern für jede Zone auf den Servern eingetragen und konfiguriert werden. DNS speichert außerdem die WINS-Antwort in seinem Cache. Über die Schaltfläche *Erweitert* definieren Sie unter *Cachezeitlimit*, wie lange ein Eintrag, der von einem WINS-Server geliefert wurde, im DNS-Cache verbleibt (Standard 15 Minuten) und wie lange der DNS-Server auf die Antwort eines WINS-Servers wartet, bevor er zum nächsten Server in der Liste übergeht (Standard 2 Sekunden, siehe Abbildung 11.9).

Abbildg. 11.9 Erweiterte Einstellungen für WINS-Forward-Lookup

In der Standardeinstellung wird nach der Aktivierung des WINS-Lookup ein DNS-Eintrag generiert, über den sekundäre DNS-Server erfahren, dass ein WINS-Server zur erweiterten Abfrage bereitsteht. Durch diese Koppelung von WINS und DNS wird die Stabilität der Namensauflösung in einem Active Directory erheblich verbessert, wobei vor allem Unternehmen mit Exchange-Servern profitieren.

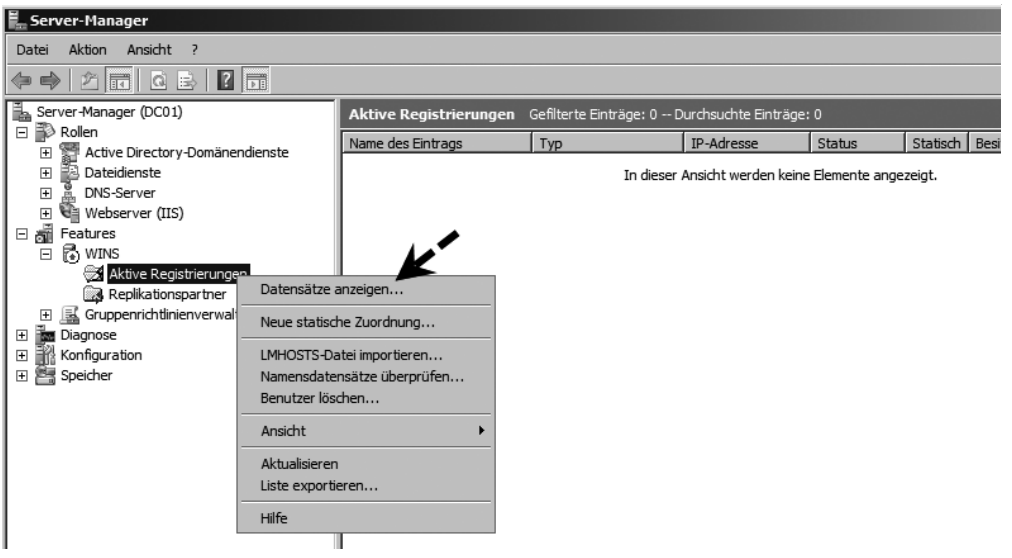
Abbildg. 11.10 Die Aktivierung von WINS-Forward-Lookup wird in der DNS-Zone als eigener Eintrag gespeichert



Die WINS-Datenbank verwalten

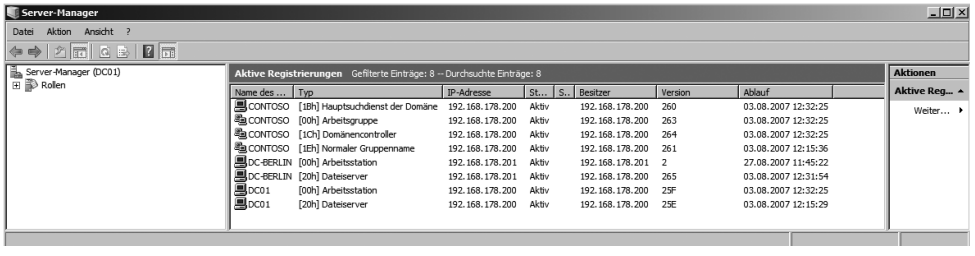
Für die Anzeige der in der WINS-Datenbank eingetragenen Systeme können eine Vielzahl von Filtern definiert werden. Auf der Registerkarte *Eintragszuordnung* können Sie die Filterung zunächst nach IP-Adressen und Computernamen vornehmen. Um die Inhalt der WINS-Datenbank anzuzeigen, klicken Sie mit der rechten Maustaste auf den Eintrag *Aktive Registrierungen* und wählen im Kontextmenü den Befehl *Datensätze anzeigen* aus (Abbildung 11.11).

Abbildg. 11.11 Anzeigen des Inhalts der WINS-Datenbank



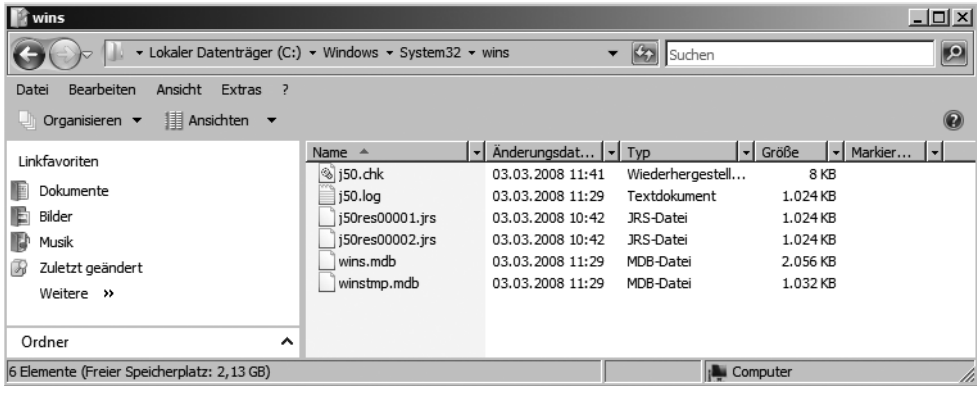
- **Computernamen** Namen, Namensteile oder * als Platzhalter erlauben die Einschränkung.
- **IP-Adressen** Eine Einschränkung nach Teilnetzen ist durch die Angabe einer Netzwerkadresse und der zugehörigen Subnetzmaske möglich.
- **Eintragsbesitzer** Der Besitzer eines Eintrags ist immer der WINS-Server, bei dem der Eintrag erfolgte. Da die Einträge zwischen den WINS-Servern repliziert werden können, ist hiermit eine Ansicht nach den einzelnen WINS-Servern möglich.

Abbildg. 11.12 Anzeigen des Inhaltes der WINS-Datenbank



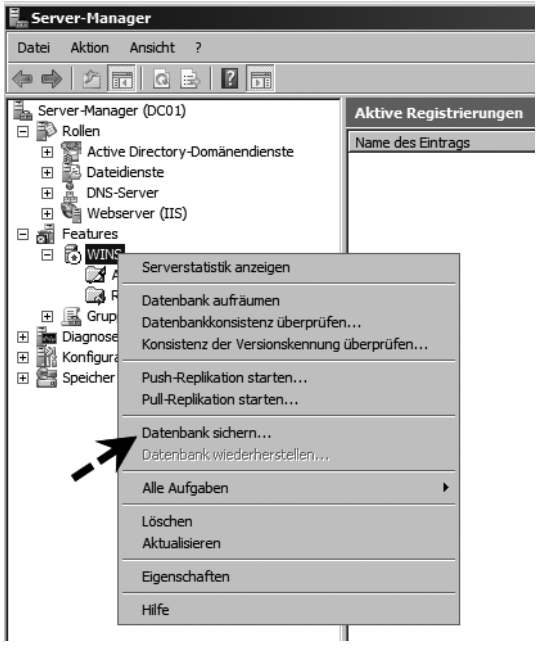
Um die WINS-Datenbank im Falle einer Beschädigung nicht komplett wieder aufbauen zu müssen, können Sie die Datenbank beim Herunterfahren des Servers sichern, das heißt, es wird eine Kopie der Datenbank in das von Ihnen vorgegebene Verzeichnis geschrieben. Diese Kopie können Sie bei Bedarf in das Verzeichnis *%Windir%\System32\wins* zurückkopieren (Abbildung 11.13).

Abbildg. 11.13 Anzeigen der WINS-Datenbank als Systemdatei



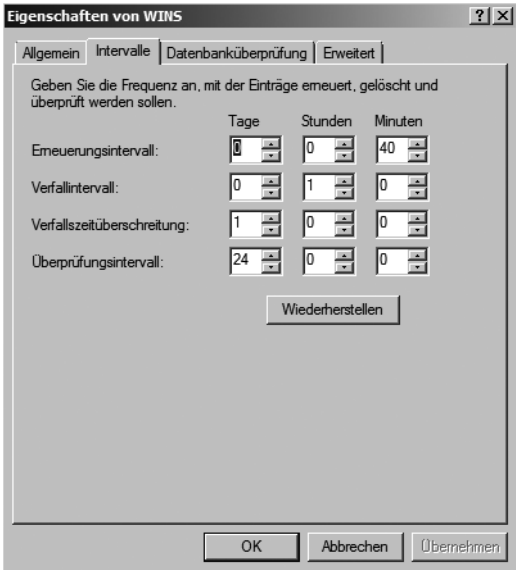
Die Sicherung und Wiederherstellung der WINS-Datenbank kann über das Kontextmenü des Knotens *WINS* durchgeführt werden (Abbildung 11.14).

Abbildg. 11.14 Sichern und Wiederherstellen der WINS-Datenbank



Damit die Einträge in den WINS-Datenbanken immer möglichst aktuell bleiben, werden die Registrierungen immer nur für eine bestimmte Zeit aufgenommen. Wenn der Client den Eintrag nicht innerhalb des angegebenen Erneuerungsintervalls bestätigt, wird dieser wieder freigegeben. Ein freigegebener Eintrag wird nach Ablauf der unter *Verfallintervall* angegebenen Zeit als verfallen angesehen und zur Löschung vorbereitet. Dazu wird in der Datenbank zu diesem Objekt ein Tombstone (Grabstein) gesetzt. Die Einstellung kann auf der Registerkarte *Intervalle* in den Eigenschaften eines WINS-Servers vorgenommen werden (Abbildung 11.15). Nachdem der Tombstone länger als die unter *Verfallszeitüberschreitung* angegebene Zeit gesetzt war, wird das Objekt endgültig aus der Datenbank gelöscht. Eine direkte Löschung des Objekts ist deshalb nicht möglich, weil ohne das Objekt den anderen WINS-Servern nichts mehr über die erfolgte Löschung mitgeteilt werden kann. So wird für das Objekt die neue Eigenschaft (Tombstone gesetzt) an alle anderen Server weitergegeben, die dann nach Ablauf der entsprechenden Frist das Objekt endgültig aus ihren Datenbanken löschen.

Abbildg. 11.15 Konfiguration der Aktualisierungsintervalle einer WINS-Datenbank



Um den Verlust von Informationen durch Dienstabstürze oder Verbindungsprobleme zu verhindern, kann in regelmäßigen Abständen eine Überprüfung der Datenbankkonsistenz durchgeführt werden. Dabei wird die lokale Datenbank mit der eines anderen WINS-Servers abgeglichen und bei Bedarf eine Übertragung der fehlenden Datensätze durchgeführt. Die Überprüfung kann dabei gegen einen zufällig gewählten Partner durchgeführt werden, oder aber die Einträge werden mit dem Besitzerserver, also dem Server, bei dem ein Computer registriert wurde. Da dieser Prozess stark zu Lasten des Servers und des Netzwerks gehen kann, sollten Sie diesen Abgleich stets außerhalb der regulären Betriebszeiten durchführen lassen.

WINS in der Befehlszeile verwalten

Über den Befehl *Netsh.exe* lässt sich auch der WINS-Dienst von Windows Server 2008 in der Befehlszeile verwalten. Öffnen Sie zunächst eine Befehlszeile und geben Sie *netsh* ein. Geben Sie als Nächstes *wins* ein, um zur WINS-Konsole von *Netsh* zu gelangen. Die wichtigsten Befehle zur Verwaltung von WINS über *Netsh* sind nachfolgend aufgelistet. Eine ausführliche Übersicht erhalten Sie in der Konsole jeweils über den Befehl *help*:

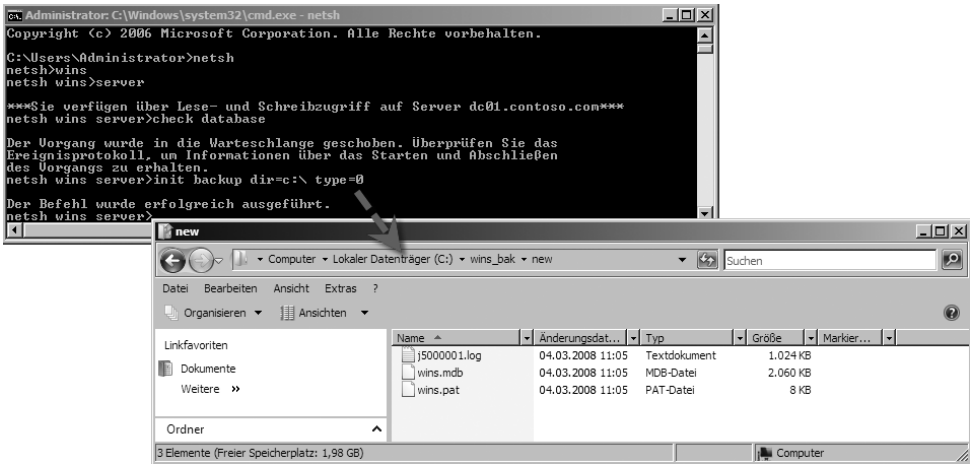
- **server** Wechselt zum angegebenen Server. Wenn dieser Befehl ohne Parameter verwendet wird, wird standardmäßig der lokale WINS-Server verwendet.
- **add name** Fügt einen Namenseintrag zur Datenbank auf dem angegebenen WINS-Server hinzu
- **add partner** Fügt einen Replikationspartner auf dem angegebenen WINS-Server hinzu
- *check database* Überprüft die Konsistenz der WINS-Datenbank. Ohne Parameter wird für alle Replikate, deren Überprüfungsintervall abgelaufen ist, eine Konsistenzprüfung durchgeführt. Die Konsistenzprüfung wird nicht sofort durchgeführt, falls das System überlastet ist, jedoch nach Ablauf des konfigurierten Überprüfungsintervalls (Abbildung 11.16).

Abbildg. 11.16 Überprüfen der WINS-Datenbank mit *netsh.exe*

- **check name** Vergleicht eine Liste mit Namenseinträgen mit einem angegebenen Satz von WINS-Servern
- **check version** Überprüft die Konsistenz von Versionskennungsnummern für WINS-Eintragsbesitzer in der WINS-Datenbank
- **delete name** Löscht einen registrierten Namen aus der WINS-Serverdatenbank
- **delete owners** Mit diesem Befehl wird eine Liste von Besitzern und deren Einträge aus der Datenbank auf dem angegebenen WINS-Server gelöscht oder in der Datenbank auf dem angegebenen WINS-Server als veraltet markiert
- **delete partner** Löscht alle oder einen bestimmten Replikationspartner aus der Liste der Replikationspartner auf dem angegebenen WINS-Server. Ohne Parameter werden alle Replikationspartner ohne Bestätigungsaufforderung aus den Pull- und Push-Partnerlisten gelöscht.
- **delete records** Löscht alle Einträge oder eine Gruppe von Einträgen auf dem aktuellen WINS-Server oder markiert Einträge als veraltet

- **init backup** Startet die Sicherung der WINS-Datenbank im angegebenen Verzeichnis. Ohne Parameter stellt dieser Befehl eine vollständige Sicherung im derzeit festgelegten Standardsicherungspfad bereit. Die WINS-Sicherung kann nur für die lokale Sicherung auf demselben Server verwendet werden. Die Sicherung von Remote-WINS-Servern wird nicht unterstützt. Sicherungsdateien werden automatisch im Unterverzeichnis *wins_bak* des mit *dir=* angegebenen Verzeichnisses erstellt, zum Beispiel *init backup dir=c:\ type=0* (Abbildung 11.17).

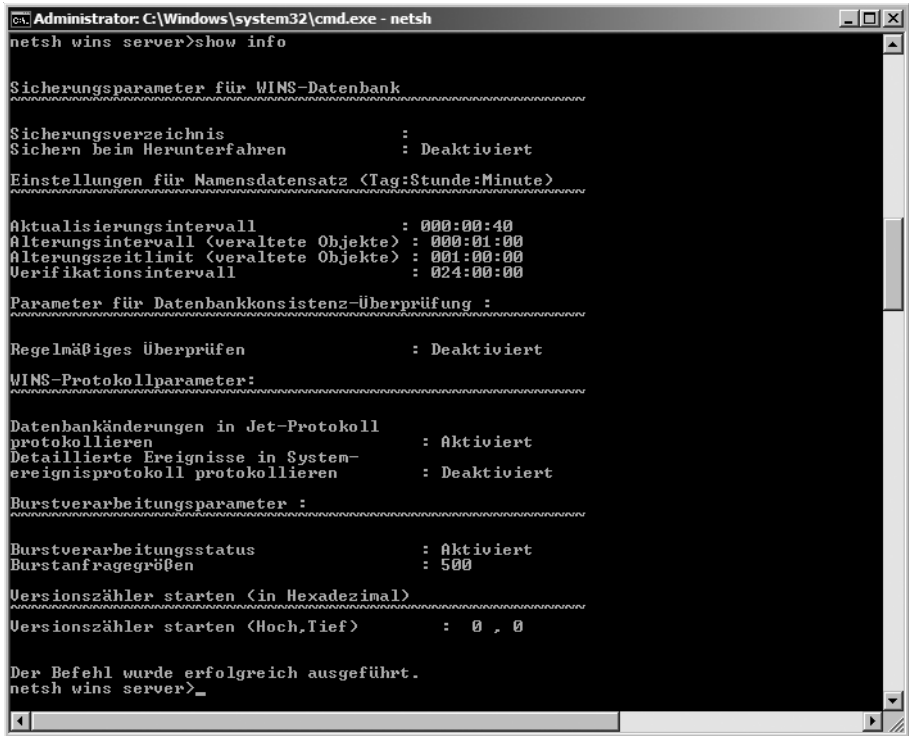
Abbildg. 11.17 Durchführen der WINS-Datensicherung über die Befehlszeile



- **init import** Initiiert das Importieren statischer Zuordnungen aus einer *Lmhosts*-Datei
- **init pull** Initiiert einen Pull-Trigger und sendet ihn an einen anderen WINS-Server
- **init push** Initiiert einen Push-Trigger und sendet ihn an einen anderen WINS-Server
- **init replicate** Initiiert und erzwingt das sofortige Replizieren der Datenbank mit Replikationspartnern
- **init restore** Initiiert die Wiederherstellung der WINS-Datenbank von einem Verzeichnis und einer Datei auf dem angegebenen WINS-Server. WINS-Sicherungen können nur lokal auf demselben Server wiederhergestellt werden. Es ist nicht möglich, die WINS-Datenbank von einem Remotecomputer wiederherzustellen. *Dir=* sollte das Unterverzeichnis *wins_bak* zum Aufnehmen der Datenbankdatei enthalten. Dieses Unterverzeichnis sollte jedoch nicht im Parameter *dir=* enthalten sein. Beispiel *init restore dir=C:\WINSfiles.*
- **init scavenge** Initiiert das Aufräumen der WINS-Datenbank für den angegebenen WINS-Server
- **init search** Initiiert eine Suche nach dem angegebenen Eintragsnamen in der WINS-Datenbank
- **reset statistics** Setzt die Statistiken für den lokalen WINS-Server zurück
- **set backuppath** Legt die Sicherungsparameter für den angegebenen WINS-Server fest
- **set defaultparam** Legt die Standardparameter für die WINS-Serverkonfiguration fest. Dieser Befehl legt alle Konfigurationsparameter für den WINS-Server auf die Standardwerte fest. Es wird empfohlen, diesen Befehl nach der Installation des WINS-Dienstes auszuführen, um für den Server Standardparametereinstellungen zu konfigurieren.

- **set periodicdbchecking** Legt die Parameter für die periodische Überprüfung der Datenbankkonsistenz für den angegebenen WINS-Server fest
- **set pullparam** Legt die standardmäßigen Pull-Parameter für den angegebenen WINS-Server fest
- **set pullpartnerconfig** Legt die Konfigurationsparameter für den angegebenen Pull-Partner fest
- **set pushparam** Legt die Standardparameter für die Push-Partner des angegebenen WINS-Servers fest
- **set pushpartnerconfig** Legt die Konfigurationsparameter für den angegebenen Push-Partner fest
- **show browser** Zeigt alle aktiven Suchdiensteinträge des Domänenmasters [1Bh] für den angegebenen WINS-Server an
- **show database** Zeigt die Datenbank und die Einträge für alle Besitzerserver oder einen Teil davon an
- **show info** Zeigt Konfigurationsinformationen für den angegebenen WINS-Server an (Abbildung 11.18)

Abbildg. 11.18 Anzeigen der WINS-Konfiguration in der Befehlszeile



- **show name** Ruft detaillierte Informationen für einen angegebenen Eintrag in der aktuellen WINS-Serverdatenbank ab und zeigt sie an

- **show partner** Zeigt alle Pull-Partner, Push-Partner oder Pull- und Push-Partner für den angegebenen WINS-Server an. Ohne Parameter zeigt dieser Befehl alle Push-Partner, Pull-Partner oder Push/Pull-Partner für den angegebenen WINS-Server an.
- **show partnerproperties** Zeigt Standardinformationen zur Partnerkonfiguration für den angegebenen
- **show pullpartnerconfig** Zeigt die Konfigurationsinformationen für einen Pull-Partner an
- **show pushpartnerconfig** Zeigt die Konfigurationsinformationen für einen Push-Partner an
- **show reccount** Zeigt die Anzahl der Datensätze an, die einem bestimmten WINS-Server gehören
- **show server** Zeigt Informationen für den angegebenen WINS-Server an
- **show statistics** Zeigt Statistiken für den angegebenen WINS-Server an (Abbildung 11.19)

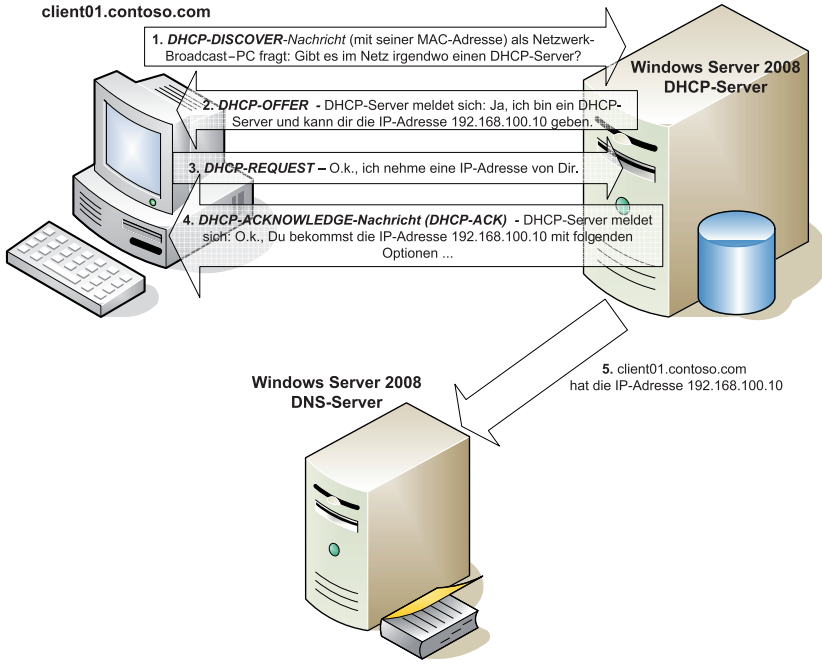
Abbildg. 11.19 Anzeigen der Server-Statistik in der Befehlszeile

- **show versionmap** Zeigt die Tabelle mit den Zuordnungen der Besitzerkennungen zum maximalen Wert für den Versionszähler des angegebenen WINS-Servers an

Windows Server 2008 als DHCP-Server einsetzen

DHCP steht für Dynamic Host Configuration Protocol. Mit diesem Serverdienst können Arbeitsstationen von einer zentralen Stelle aus automatisch mit IP-Adressen versorgt werden. Einer der zentralen Bereiche von DHCP bei Windows Server 2008 ist die Integration in DNS. Die Zielsetzung der DHCP-DNS-Integration ist eine automatische Registrierung von Computernamen und IP-Adressen bei DNS-Servern durch den DHCP-Server. Windows Server 2008 unterstützt neben DHCPv4 auch DHCPv6, also die automatische IP-Adressenvergabe von IPv6-Adressen. In Abbildung 11.20 sehen Sie, wie die automatische IP-Adressenvergabe funktioniert.

Abbildg. 11.20 Zuweisen von IP-Adressen über DHCP

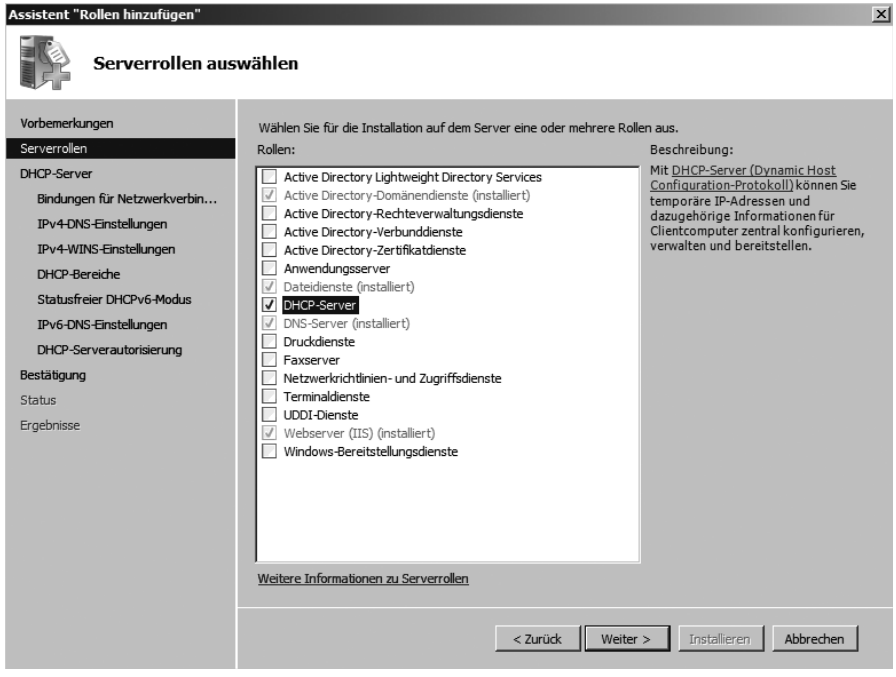


Installation eines DHCP-Servers

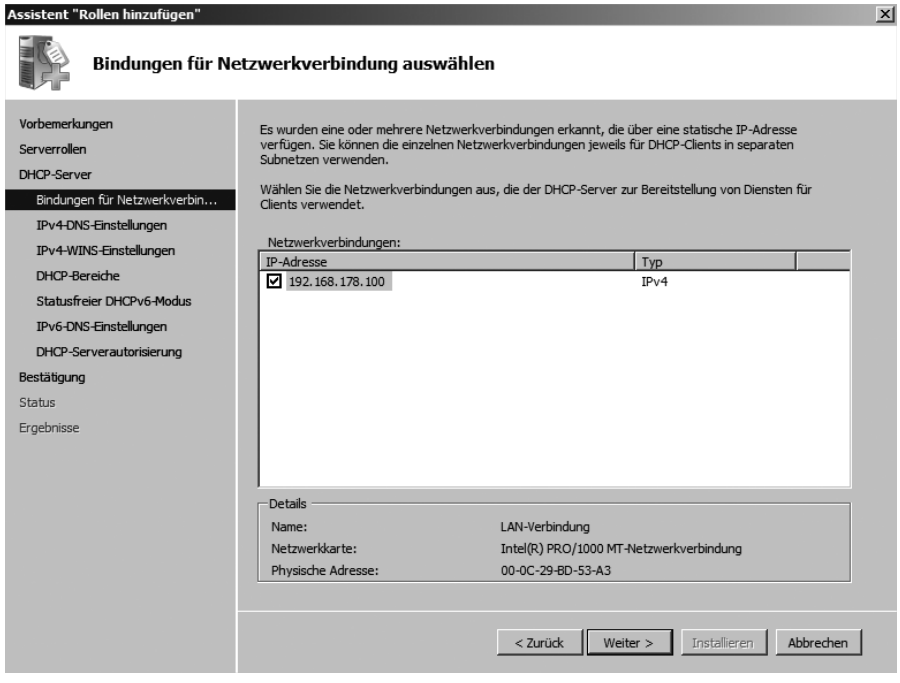
Der DHCP-Server-Dienst wird über den Server-Manager installiert. Im Gegensatz zu WINS handelt es sich bei DHCP um eine Serverrolle. Um diese einem Server hinzuzufügen, klicken Sie im Server-Manager in der Konsolenstruktur auf den Knoten *Rollen* und dann im rechten Bereich auf den Link *Rollen hinzufügen*. Anschließend kann die Rolle *DHCP-Server* ausgewählt werden. Neu bei Windows Server 2008 ist die mögliche Einrichtung eines DHCP-Servers bereits bei der Installation, nicht erst später bei der Verwaltung (Abbildung 11.21).

Auf der ersten Seite des Installationsassistenten legen Sie fest, auf welchen Netzwerkschnittstellen und welcher IP-Adresse der DHCP-Server auf Anfragen hören soll. Hier wird auch der Typ des IP-Netzes angezeigt. In den meisten Netzwerken wird derzeit noch IPv4 verwendet. Aus diesem Grund wird bei den meisten DHCP-Servern zunächst die IPv4-Adresse als Bindung angezeigt. Sind in einem Server mehrere Netzwerkkarten eingebaut, besteht auch die Möglichkeit, den Server auf mehrere dieser Schnittstellen hören zu lassen. Die Einstellung, die Sie hier vornehmen, kann aber auch jederzeit wieder rückgängig gemacht werden. Hierbei handelt es sich um keine Einbahnstraße.

Abbildg. 11.21 Hinzufügen der DHCP-Serverrolle

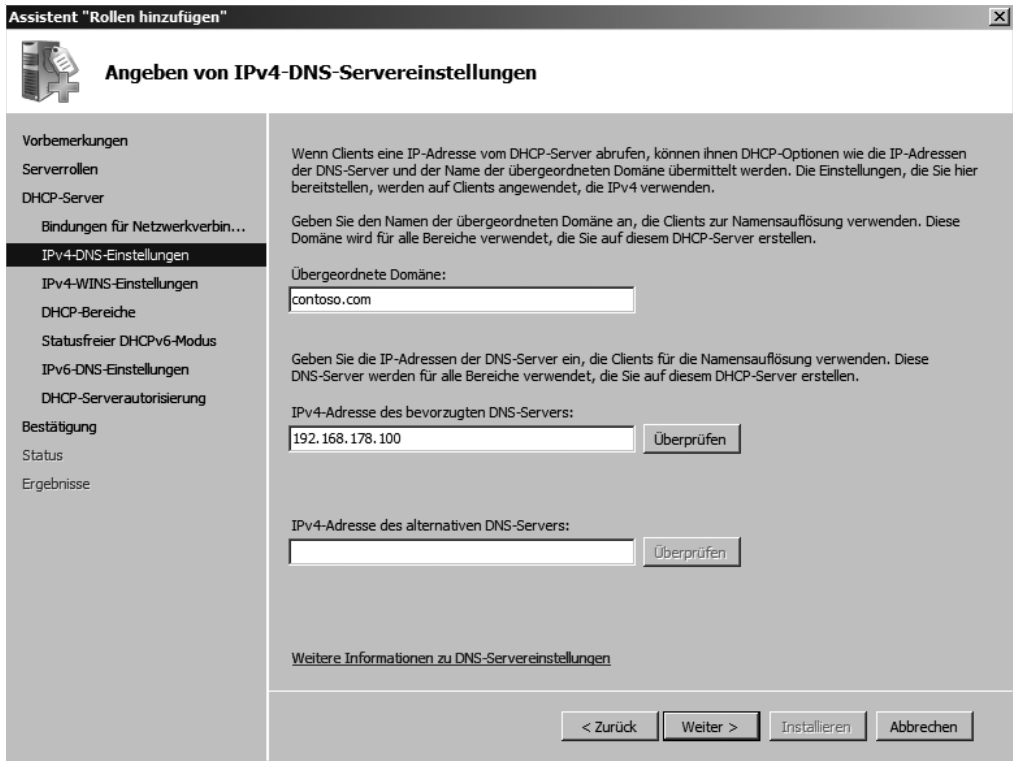


Abbildg. 11.22 Festlegen der Bindungen eines DHCP-Servers



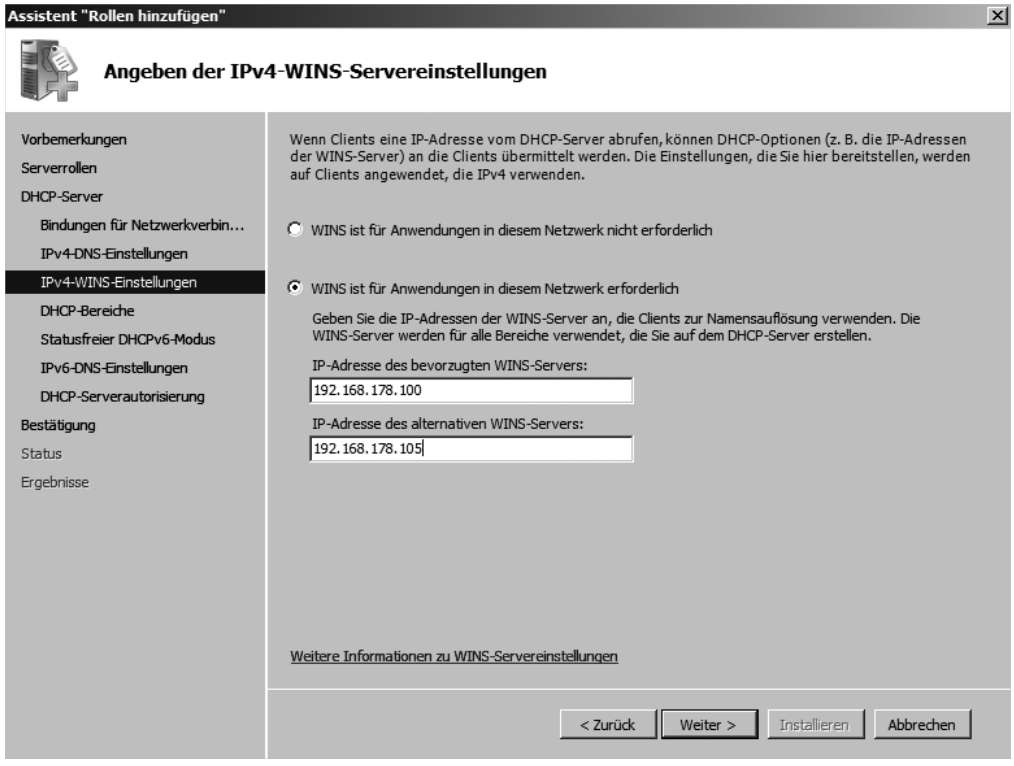
Auf der nächsten Seite des Assistenten legen Sie die DNS-Einstellungen fest, die an die Clients verteilt werden sollen (Abbildung 11.23). An dieser Stelle können neben einem bevorzugten und alternativen DNS-Server auch die DNS-Domäne mitgegeben werden, die den DHCP-Clients zugewiesen werden sollen. Computer, die bereits Mitglied der Domäne sind, erhalten den DNS-Namen ohnehin statisch bereits bei der Domänenmitgliedschaft zugewiesen. Alleinstehende Computer, ohne DNS-Konfiguration können durch diese Funktion jedoch ebenfalls die DNS-Domäne des Unternehmens auflösen. Es schadet nicht, wenn Sie hier die Domäne eintragen. Arbeiten Sie im Unternehmen mit mehreren DNS-Domänen innerhalb eines IP-Bereichs, besteht auch die Möglichkeit den Eintrag an dieser Stelle leer zu lassen. Haben Sie die IP-Adresse der DNS-Server eingetragen, kann über die Schaltfläche *Überprüfen* sichergestellt werden, dass die IP-Adresse des Servers stimmt und der Server auch erreicht werden kann.

Abbildg. 11.23 Konfigurieren der DNS-Einstellungen für DHCP-Clients



Auf der nächsten Seite legen Sie die WINS-Server fest, die den Clients zugewiesen werden sollen (Abbildung 11.24). Auch wenn in Active Directory WINS nicht so eine wichtige Rolle spielt wie DNS, schadet der Einsatz des Systems nicht, wie wir Ihnen in diesem Kapitel noch zeigen. WINS sorgt parallel zu DNS zu einer Namensauflösung im Netzwerk ohne eine zu große Serverlast zu verursachen. Durch den parallelen Einsatz von WINS und DNS wird außerdem eine gewisse Ausfallsicherheit der Namensauflösung im Netzwerk erreicht. WINS kann zwar eine DNS-Struktur nicht vollkommen ersetzen, einzelne fehlende DNS-Einträge oder ausgefallene DNS-Server aber schon, zumindest kurzzeitig.

Abbildg. 11.24 Festlegen der WINS-Server für DHCP-Clients



Auf der nächsten Seite des Assistenten legen Sie den IP-Bereich fest, aus dem den Clients IP-Adressen zugewiesen werden sollen. Hier bietet es sich an einen unabhängigen Bereich innerhalb des Subnetzes des Unternehmens zu wählen. Über die Schaltfläche *Hinzufügen* können detaillierte Informationen konfiguriert werden, welche IP-Adressen den Clients zugewiesen werden sollen. Neben einem frei wählbaren Namen für den Bereich werden an dieser Stelle die Start- und End-IP-Adresse aus dem Bereich festgelegt. Hier kann auch konfiguriert werden, ob den Clients ein Standardgateway zugewiesen werden soll, was innerhalb von gerouteten Netzwerken sinnvoll ist. Sie sollten bei der automatischen Vergabe des Standardgateways aber Vorsicht walten lassen. Wenn die Arbeitsstationen zum Beispiel den ISA Server als Standardgateway erhalten, werden diese bei der Adressversorgung durch den DHCP automatisch zu SecureNAT-Clients. Diese Konfiguration ist vollkommen unnötig. Achten Sie daher darauf, dass Sie nur ein Standardgateway mitgeben, wenn Sie interne Router einsetzen. Für die Verbindung zum Internet sollten Sie möglichst mit einem Proxyserver arbeiten. Über dieses Fenster kann der Bereich auch gleich aktiviert werden, sodass der DHCP-Server Adressen verteilen kann. Die Aktivierung des Bereiches kann aber auch jederzeit später über die Verwaltungskonsole erfolgen.

Festlegen der Leasedauer

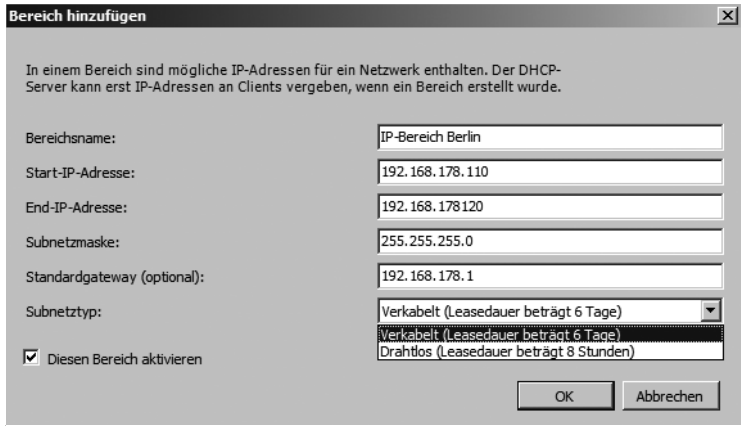
Weist ein DHCP-Server einem Client eine IP-Adresse zu, dann ist diese Zuweisung immer auf einen gewissen Zeitraum beschränkt, die so genannte *Leasedauer*, die in der Standardeinstellung 6 Tage beträgt. Windows Server 2008 unterscheidet an dieser Stelle zwischen stationären (verkabelten)

Computern, die erfahrungsgemäß länger mit dem Netzwerk verbunden sind und mobilen (drahtlosen) Computern, also Notebooks von mobilen Mitarbeitern. Je länger die Leasedauer, um so länger wird eine IP-Adresse für einen Client reserviert. Abhängig von dieser Zeit durchläuft der DHCP-Client drei Phasen:

1. Nachdem die Leasedauer zur Hälfte abgelaufen ist, wendet sich der Client an den Server, um die erhaltene IP-Adresse erneut zu bestätigen. Ist der DHCP-Server betriebsbereit, wird die Leasedauer wieder auf ihren ursprünglichen Wert zurückgesetzt, also verlängert. Antwortet der Server nicht, wird der Client in regelmäßigen Abständen einen neuen Versuch unternehmen.
2. Steht nach Ablauf der Zeit der ursprüngliche DHCP-Server nicht mehr zur Verlängerung zur Verfügung, versucht der DHCP-Client nach $^{7}/_{8}$ der Leasedauer, irgendeinen DHCP-Server zu erreichen, der ihm eine neue IP-Adresse zuweisen kann. Auch diesen Versuch wiederholt er in regelmäßigen Abständen.
3. Nach Ablauf der Leasedauer muss der Client seine IP-Adresse freigeben und versucht nun weiter, einen DHCP-Server zu erreichen, der ihm eine neue IP-Adresse zuweist.

Bei ausreichend verfügbaren IP-Adressen sollte die Leasedauer möglichst hoch gesetzt werden, damit die Clients keine unnötige Netzwerklast erzeugen. Nur wenn die Anzahl der verfügbaren Adressen kleiner als die Gesamtzahl der Computer ist, sollte der Wert so niedrig gewählt werden (unter Umständen sogar im Stundenbereich), dass der DHCP-Server nicht mehr benötigte Adressen schnell wieder aus der Datenbank löschen und anderen Clients zuweisen kann. Nach der Installation des DHCP-Servers kann die Leasedauer noch genauer konfiguriert werden.

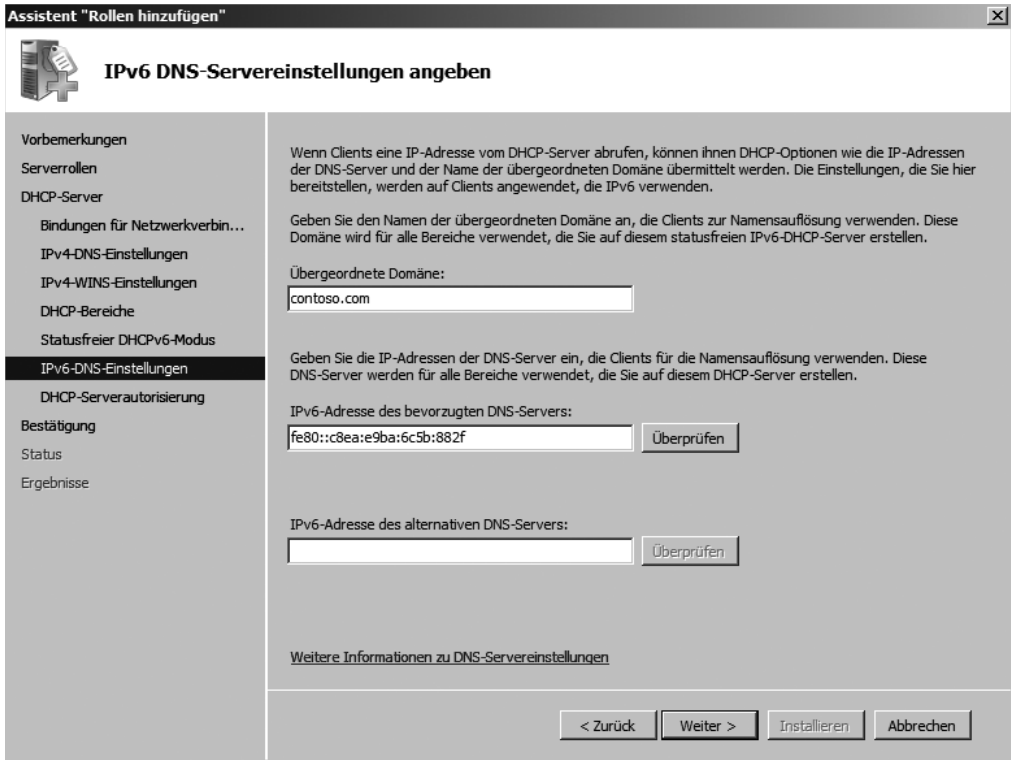
Abbildg. 11.25 Konfigurieren eines IP-Adressbereiches für den DHCP-Server



Nachdem Sie den oder die IP-Bereiche festgelegt haben, kann auf der nächsten Seite die IPv6-Konfiguration des DHCP-Servers aktiviert werden. Werden im Unternehmen keine IPv6-fähigen Netzwerkgeräte eingesetzt, können Sie sich diese Konfiguration sparen. Windows Vista und Windows Server 2008 unterstützen bereits standardmäßig nach der Installation IPv6, allerdings müssen auch die Switches und Router im Unternehmen dieses neue Protokoll unterstützen. Bei einem IPv6-Netzwerk wird DHCP eigentlich nicht zum Konfigurieren von Adressen benötigt, es können jedoch gute Gründe für seine Verwendung sprechen, zum Beispiel wenn Sie nicht den Computern selbst die Konfiguration deren IPv6-Adressen überlassen wollen. Wollen Sie neben den IPv4-Einstellungen auf die IPv6-Einstellungen für den Server vornehmen, aktivieren Sie die entsprechende Option.

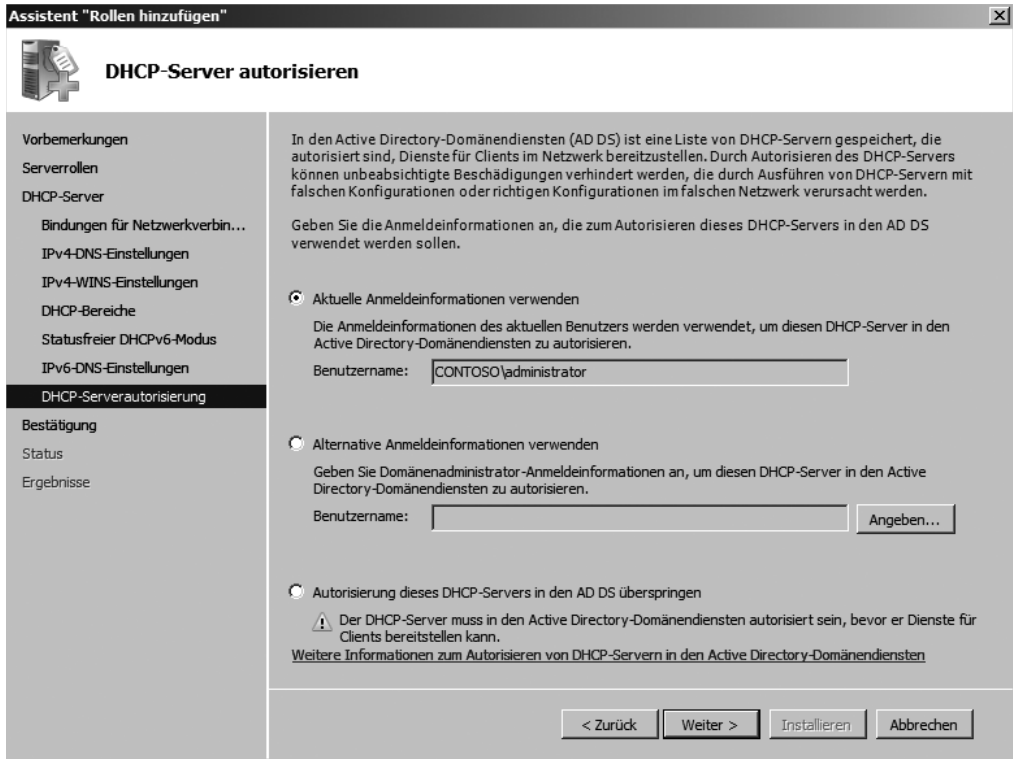
Haben Sie die IPv6-Konfiguration aktiviert, können Sie auf der nächsten Seite die IPv6-Adressen der DNS-Server im Netzwerk konfigurieren (Abbildung 11.26). Auch hier kann die Konfiguration wieder über die Schaltfläche *Überprüfen* getestet werden.

Abbildg. 11.26 Festlegen der IPv6-DNS-Server für den DHCP-Server



Auf der nächsten Seite des Assistenten wird der DHCP-Server in Active Directory autorisiert. Dazu können Sie entweder die aktuellen Anmeldeinformationen oder neue Anmeldedaten eingeben. Erst wenn der Server berechtigt ist, IP-Adressen zu vergeben, startet er mit seiner Arbeit. Anschließend erhalten Sie noch eine Zusammenfassung über die Konfiguration angezeigt, und der DHCP-Server-Dienst wird installiert und aktiviert.

Abbildg. 11.27 Autorisieren eines DHCP-Servers in Active Directory



Grundkonfiguration eines DHCP-Servers

Nach der Installation des DHCP-Dienstes können Sie die Grundkonfiguration des Servers vornehmen. Alle Einstellungen, die bei der Installation vorgenommen wurden, können nachträglich über das Verwaltungsprogramm angepasst werden. Starten Sie dazu das Verwaltungsprogramm über *Start/Verwaltung/DHCP*. Die Verwaltung der Ereignisse von DHCP kann auch über den Server-Manager und den Eintrag *Rollen/DHCP-Server* in der Konsolenstruktur vorgenommen werden.

HINWEIS **APIPA (Automatic Private IP Addressing)**

Für den Fall, dass kein DHCP-Server für das automatische Zuweisen einer IP-Adresse erreicht werden kann, bestimmt Windows Vista eine Adresse in der für Microsoft reservierten IP-Adressierungsklasse, die von *169.254.0.1* bis *169.254.255.254* reicht. Diese Adresse wird verwendet, bis ein DHCP-Server gefunden wird. Diese Methode des Beziehens einer IP-Adresse wird als automatische IP-Adressierung bezeichnet (APIPA). Bei dieser Methode wird kein DNS, WINS oder Standardgateway zugewiesen, da diese Methode nur für ein kleines Netzwerk mit einem einzigen Netzwerksegment entworfen wurde. Um die APIPA-Funktion zu deaktivieren, müssen Sie in der Registrierung unter *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters* einen Schlüssel namens *IPAutoconfigurationEnabled* anlegen und ihm den Wert *0* zuweisen. Diese Konfiguration kann derzeit noch nicht über Gruppenrichtlinien verteilt werden. Generell wird empfohlen werden, die Einstellungen auf den Standardwerten zu belassen.

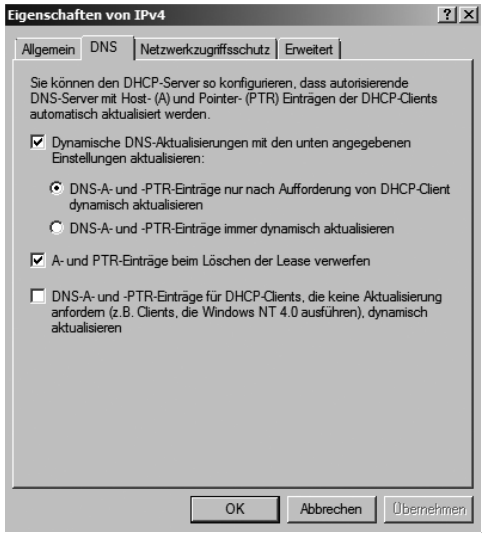
DHCP-Server autorisieren

Sobald der DHCP-Server Mitglied in einer Active Directory-Domäne ist, muss der Server im Active Directory autorisiert werden, falls diese Aktion nicht bereits während der Installation durchgeführt wurde. Nur Mitglieder der Gruppe *Organisations-Admins* können standardmäßig DHCP-Server autorisieren. Erst dadurch ist sichergestellt, dass er IP-Adressen automatisch an die Clients verteilen kann. Nach der Installation wird ein DHCP-Server zunächst als *Nicht autorisiert* angezeigt, was Sie am roten Pfeil erkennen, der nach unten gerichtet ist, wenn Sie die Verwaltung des DHCP-Servers öffnen. Klicken Sie in der DHCP-Verwaltung mit der rechten Maustaste auf den Servernamen und wählen Sie im Kontextmenü den Befehl *Autorisieren* aus. An dieser Stelle kann diese auch wieder aufgehoben werden, wenn ein DHCP-Server keine Adressen mehr verteilen soll. Nach kurzer Zeit wird der DHCP-Server als autorisiert angezeigt. Wenn der DHCP-Serverdienst von Windows Server 2008 gestartet wird, fragt er zunächst das Active Directory ab, um festzustellen, ob er sich in der Liste der autorisierten DHCP-Server befindet. Ist dies der Fall, sendet er eine *DHCPinform*-Nachricht in das Netzwerk, um festzustellen, ob es andere Verzeichnisdienste gibt und er bei diesen gültig ist. Falls der DHCP-Server dagegen keinen Eintrag im Active Directory vorfindet oder keinen Active Directory-Server finden kann, geht er davon aus, dass er nicht autorisiert ist, und beantwortet keine Clientanfragen. Dieser Mechanismus funktioniert allerdings nur dann optimal, wenn mit dem Active Directory gearbeitet wird. Bei alleinstehenden Servern mit Windows Server 2008 und DHCP-Dienst kann der DHCP-Serverdienst nur genutzt werden, solange keine Domäne von Active Directory im Netzwerk gefunden wird. Der Schutz von Active Directory greift natürlich nicht, wenn auch andere, nicht auf Windows Server 2008 basierende DHCP-Server im Netzwerk sind, beispielsweise in einem Router.

Dynamische DNS-Updates konfigurieren

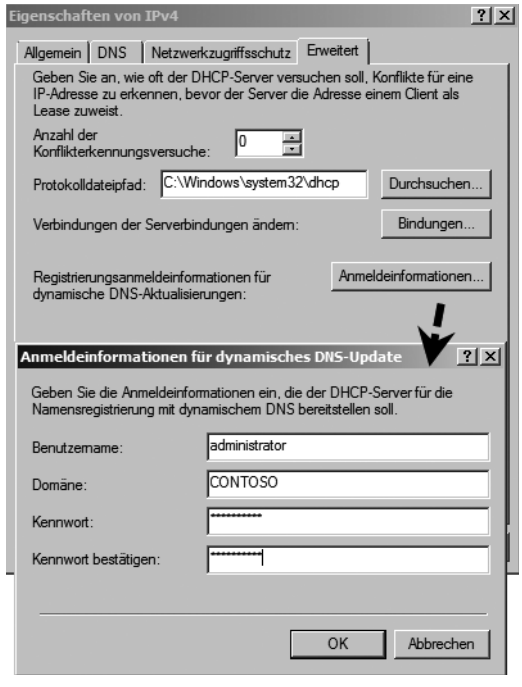
Damit der DHCP-Server für die Clients eine automatische DNS-Registrierung auf den DNS-Servern durchführen kann, müssen Sie ihn erst dafür konfigurieren. Wenn Sie die Eigenschaften von IPv4 oder IPv6 des DHCP-Servers aufrufen, können Sie auf der Registerkarte *DNS* konfigurieren, welche Einträge der DHCP-Server auf den DNS-Servern erstellen soll (Abbildung 11.28).

Abbildg. 11.28 Konfiguration der DNS-Anbindung eines DNS-Servers



Setzen Sie noch Clients ein, die kein dynamisches DNS unterstützen, also alles was älter ist als Windows 2000, sollten Sie in den Eigenschaften des DHCP-Servers auf der Registerkarte *DNS* die Option *DNS-A- und -PTR-Einträge für DHCP-Clients, die keine Aktualisierungen anfordern …* sowie zusätzlich die Option *DNS-A- und -PTR-Einträge immer dynamisch aktualisieren* aktivieren. Ein Computer, dessen Leasedauer für die IP-Adresse abgelaufen ist, muss seine Adresse abgeben. Daher löscht der DHCP-Server in der Standardeinstellung auch die zugehörigen DNS-Einträge. Falls Sie die Einträge trotzdem behalten wollen, deaktivieren Sie das Kontrollkästchen *A- und PTR-Einträge beim Löschen der Lease verwerfen*. Bevor ein Windows Server 2008-DHCP-Server Clients dynamisch im DNS eintragen kann, müssen Sie in den Eigenschaften des Servers auf der Registerkarte *Erweitert* mit Hilfe der Schaltfläche *Anmeldeinformationen* die Benutzerdaten eines DNS-Administrators hinterlegen, der die Aktualisierung vornehmen kann. Ohne diese Konfiguration kann der DHCP keine dynamische Registrierung durchführen (Abbildung 11.29).

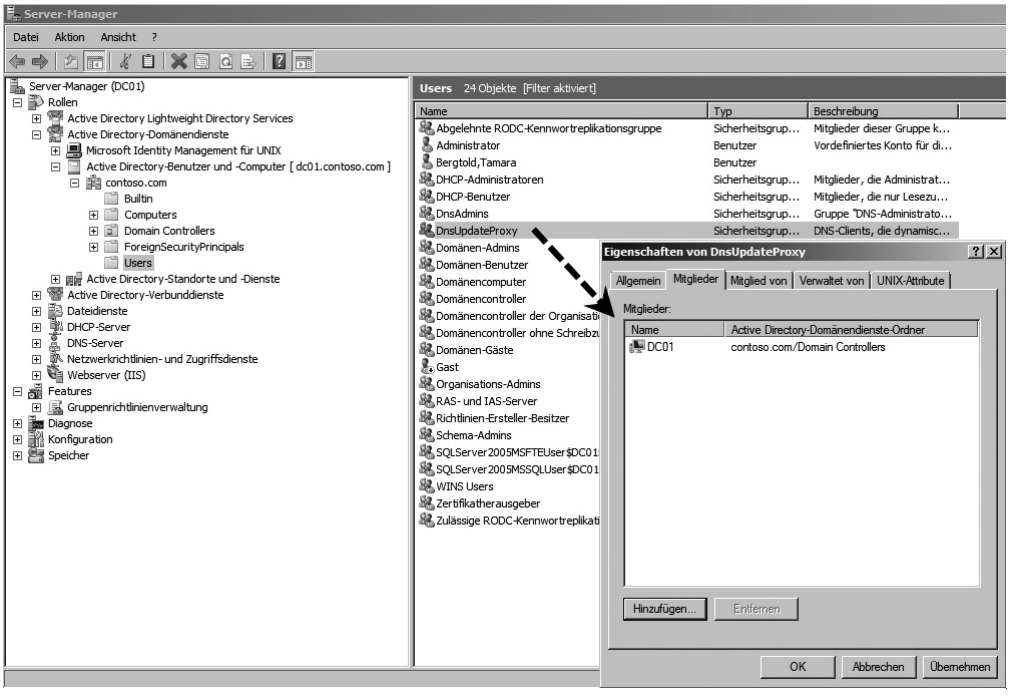
Abbildg. 11.29 Festlegen der Anmeldedaten für den DHCP-Server am DNS-Dienst



Es besteht auch die Möglichkeit, das Computerkonto des DHCP-Servers in die entsprechende Sicherheitsgruppe der Domäne aufzunehmen. In diesem Fall besteht nicht die Notwendigkeit, die Benutzerdaten eines Administrators auf dem DHCP zu hinterlegen. Die Gruppe *DnsAdmins* enthält die Administratoren für DNS-Server. Dieser Gruppe sind standardmäßig noch keine Benutzer zugeordnet. Sie kann verwendet werden, um die Administration von DNS-Servern zu delegieren. In der Gruppe *DnsUpdateProxy* befinden sich Computer, die als Proxy für die dynamische Aktualisierung von DNS-Einträgen fungieren können. DHCP-Server werden in diese Gruppen nicht automatisch aufgenommen. Wollen Sie keine Anmeldedaten hinterlegen, aber dem DHCP-Server dennoch

gestatten, dynamische Einträge in den DNS-Zonen vorzunehmen, sollten Sie die Computerkonten der DHCP-Server in die Gruppe *DnsUpdateProxy* aufnehmen.

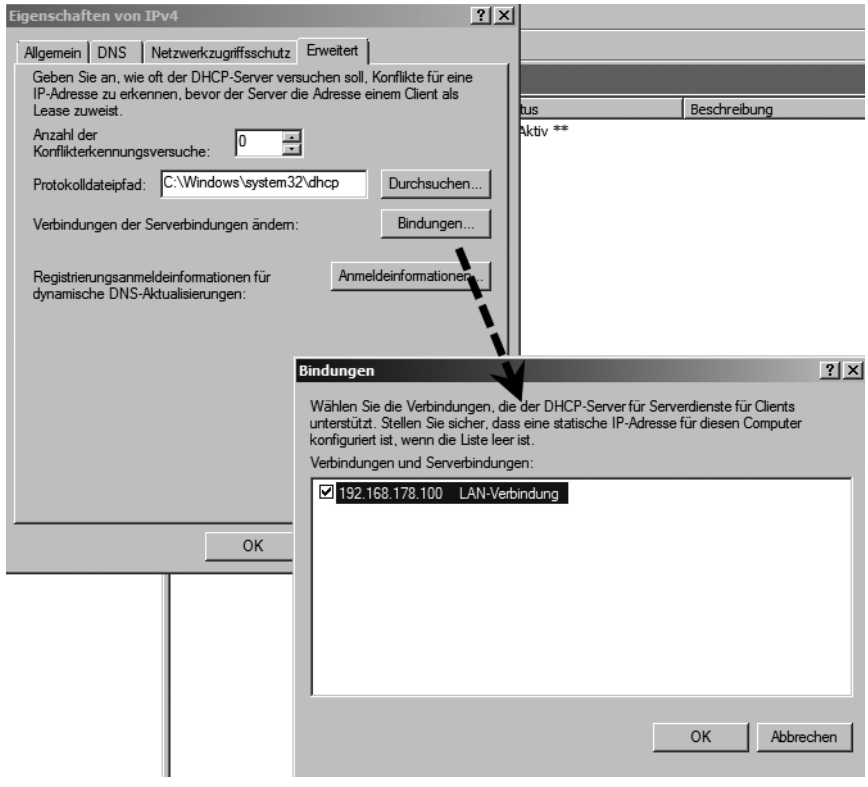
Abbildg. 11.30 Aufnehmen von DHCP-Servern in die Gruppe *DnsUpdateProxy*



Konfiguration der Netzwerkverbindung

Auf der Registerkarte *Erweitert* in den Eigenschaften von IPv4 oder IPv6 legen Sie zudem fest, wo die vom DHCP-Server erstellten Dateien abgelegt werden. Wenn Sie den DHCP-Server mit mehreren IP-Adressen konfiguriert haben, können Sie über die Schaltfläche *Bindungen* definieren, auf welchen dieser Adressen er auf Anfragen reagiert (Abbildung 11.31).

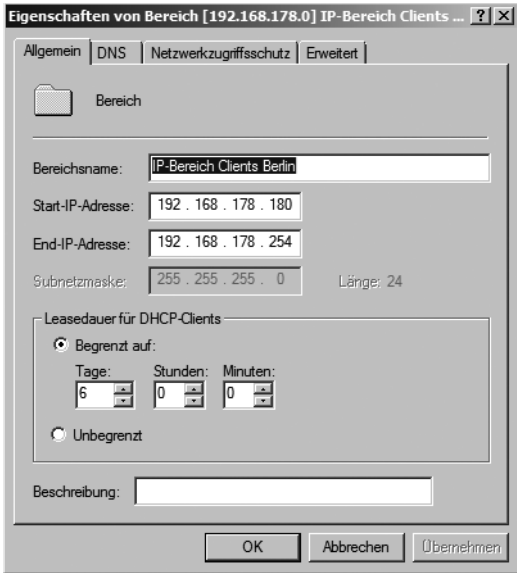
Abbildg. 11.31 Konfiguration der Netzwerkbindungen eines DHCP-Servers



Verwalten von DHCP-Bereichen

Nach der Installation der DHCP-Rolle kann über die Eigenschaften eines DHCP-Bereichs in der Verwaltungskonsole genauer festgelegt werden, wie der Server reagieren soll. Auf der Registerkarte *Allgemein* können bei Bedarf der Name und die Beschreibung des Bereichs sowie die Start-IP-Adresse, die End-IP-Adresse und die Leasedauer verändert werden. Unter *Adresspool* ist der Adressbereich mit den ein- und ausgeschlossenen Adressen zu sehen. Unter *Adressleases* werden die derzeit vergebenen IP-Adressen, auch Leases genannt, im definierten Bereich angezeigt. Die Reservierungen beinhalten die IP-Adressen, die einer MAC-Adresse fest zugeordnet worden sind.

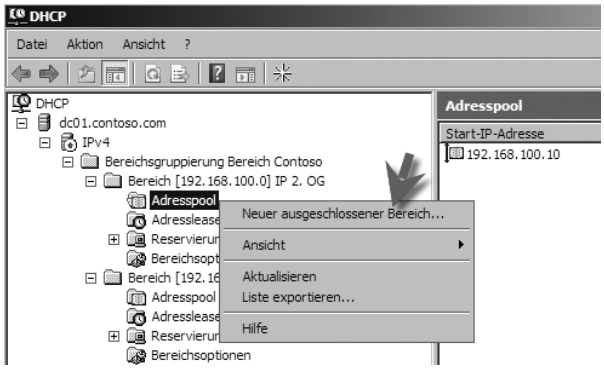
Abbildg. 11.32 Verwalten von IP-Bereichen auf einem DHCP-Server



Zusätzlich zu den Einstellungen bei der Erstellung des Bereichs kann die Leasedauer auf *Unbegrenzt* gesetzt werden. Diese Einstellung wird jedoch nicht empfohlen. Die Registerkarte *DNS* entspricht exakt der Registerkarte *DNS* der Servereigenschaften, wobei die Bereichseinstellungen Vorrang vor den Servereinstellungen haben. Wenn sich 400 mobile Benutzer mit einem Netzwerk verbinden können, in dem nur rund 240 freie Adressen verfügbar sind, führt das dazu, dass faktisch 160 IP-Adressen mehr als erforderlich benötigt würden. Wenn davon maximal 100 Benutzer gleichzeitig verbunden sind, lässt sich dieser Engpass durch eine sinnvolle Festlegung der Leasedauer umgehen. Die Leasedauer sollte sich in etwa an der durchschnittlichen Verweildauer der Benutzer im lokalen Netzwerk orientieren. Auch in einigen Servicebereichen, in denen immer neue Systeme an ein Netzwerk angeschlossen werden müssen und die ihre IP-Adressen über DHCP erhalten, sind sehr kurze Leasedauern sinnvoll. In der Praxis haben sich Leasedauern zwischen 21 und 30 Tagen bewährt. Die unbegrenzte Leasedauer sollte keinesfalls verwendet werden. Sie führt dazu, dass IP-Konfigurationen nicht mehr automatisch freigegeben werden. Dadurch werden irgendwann die Adressen knapp. Erstellte Bereiche können entweder bei der Installation von DHCP aktiviert werden, oder später. Aktivierte Bereiche lassen sich auch wieder deaktivieren.

TIPP Wenn ein Bereich aktiviert wurde, sollte er aber erst dann deaktiviert werden, wenn die enthaltenen IP-Adressen nicht weiter im Netzwerk verwendet werden sollen. Nach dem Deaktivieren eines Bereichs akzeptiert der DHCP-Server diese Adressen nicht mehr als gültig. Wenn Adressen nur zeitweise deaktiviert werden sollen, kann durch Bearbeiten oder Ändern von Ausschlussbereichen in einem aktiven Bereich das gewünschte Resultat ohne ungewollte Nebeneffekte erzielt werden. Ausgeschlossene Bereiche lassen sich über das Kontextmenü des Eintrags *Adresspool* erzeugen (Abbildung 11.33).

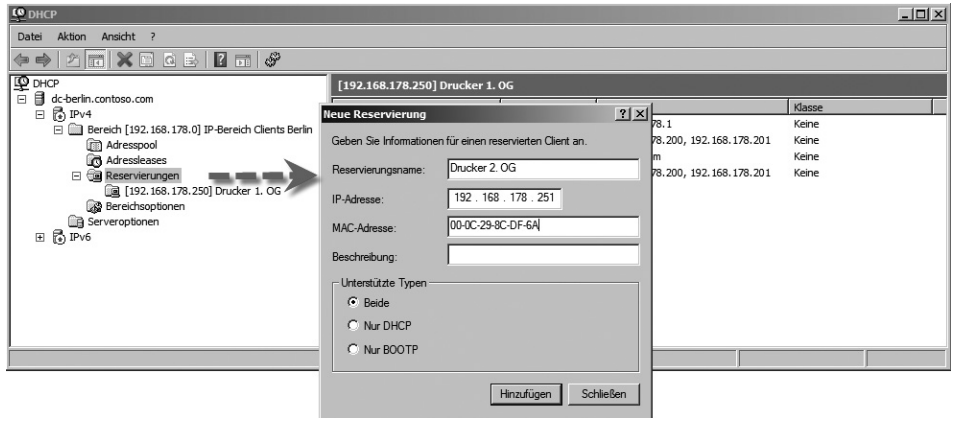
Abbildg. 11.33 Erstellen von ausgeschlossenen IP-Adressen innerhalb eines Bereichs



Statische IP-Adressen reservieren

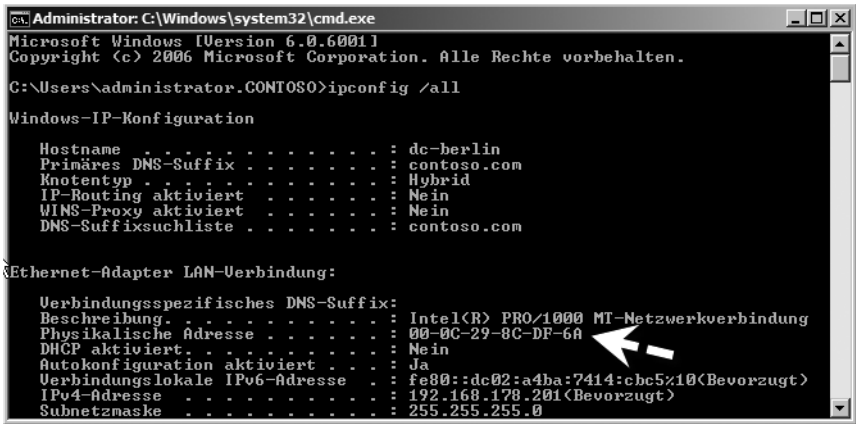
Einige Geräte, zum Beispiel Netzwerkdrucker, können nur sehr umständlich auf eine feste IP-Adresse konfiguriert werden, manche nutzen sogar nur DHCP. Damit sich aber die Anwender nicht täglich auf neue IP-Adressen der Drucker einstellen müssen, sollen die Adressen dennoch statisch sein. Da ein DHCP-Server aber immer auf eine Anfrage irgendeine Adresse aus seinem konfigurierten Bereich vergeben kann, muss diese nicht mit der dem Gerät zuletzt zugewiesenen übereinstimmen. In einem solchen Fall bietet sich eine Reservierung an, bei der die Hardware- oder MAC-Adresse des Druckers oder sonstigen Netzwerkgeräts mit einer bestimmten IP-Adresse verknüpft wird. Fordert dieses Gerät nun eine IP-Adresse an, vergleicht der DHCP-Server die MAC-Adresse mit seiner Datenbank und weist ihm daraufhin, zwar dynamisch, aber doch immer wieder dieselbe Adresse zu. Dieser Vorgang wird *Reservierung* genannt. Um eine Reservierung zu erstellen, klicken Sie unterhalb des Bereichs mit der rechten Maustaste auf den Eintrag *Reservierungen* und wählen im Kontextmenü den Befehl *Neue Reservierung* aus. Geben Sie als Nächstes den Namen der Reservierung ein. Anschließend muss die IP-Adresse, die diesem Gerät immer zugewiesen wird, sowie die MAC-Adresse angegeben werden. Bei Druckservern finden Sie diese in der Regel auf einem Gehäuseaufkleber. Auf Netzwerkkarten finden Sie diesen Aufkleber häufig auch vor, nur leider in den seltensten Fällen an der Außenblende.

Abbildg. 11.34 Erstellen von Reservierungen auf einem DHCP-Server



Damit Sie nicht alle PCs aufschrauben müssen, können Sie die MAC-Adresse auch über die Eingabeaufforderung mit dem Kommando *ipconfig /all* ermitteln. Die MAC-Adresse wird in der Zeile *Physikalische Adresse* angezeigt (Abbildung 11.35).

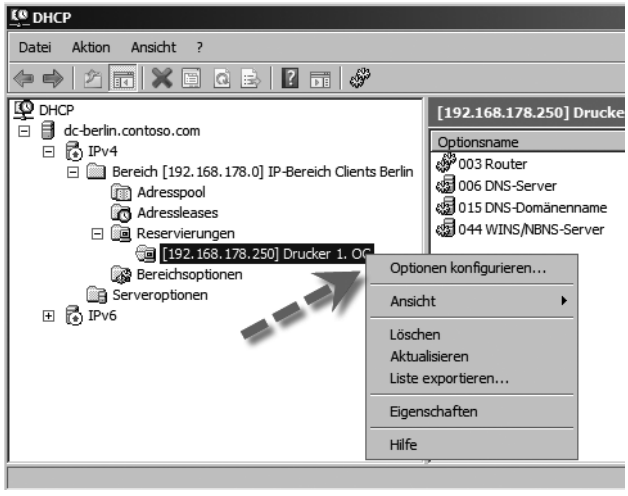
Abbildg. 11.35 Anzeigen der MAC-Adresse eines Computers



TIPP Unter Umständen kann es sehr hilfreich sein, sich an einer zentralen Stelle alle MAC-Adressen in Ihrem Netzwerk anzeigen zu lassen. Mit der Batchdatei *getmac.bat*, die Sie auf der Seite *http://www.wintotal.de/Software/index.php?id=2574* im Internet herunterladen können, werden alle MAC-Adressen in einem Netzwerk in der Befehlszeile ausgelesen. Geben Sie dazu den Befehl *getmac <Subnetz> <Startadresse> <Endadresse>* ein. So werden zum Beispiel mit *getmac 10.0.0 1 20* die MAC-Adressen aller Rechner im Subnetz *10.0.0* von der IP-Adresse *10.0.0.1* bis zur Adresse *10.0.0.20* ausgelesen. Danach werden die Ergebnisse in der Textdatei *used_ips.txt* ausgegeben, die im gleichen Verzeichnis angelegt wird, aus dem Sie *getmac.bat* starten. Mit diesem kostenlosen Tool erhalten Sie schnell alle verfügbaren MAC-Adressen in einem IP-Bereich.

Wenn Sie nach dem Erstellen einer Reservierung die Eigenschaften des neuen Objekts öffnen, können Sie alle Einstellungen bis auf die zuzuweisende IP-Adresse wieder ändern. Die zusätzliche Registerkarte *DNS* erlaubt es Ihnen, für dieses eine Gerät zu bestimmen, ob der DHCP-Server die dynamische Registrierung beim DNS-Server übernimmt. Diese Registerkarte entspricht exakt der Registerkarte *DNS* in den Eigenschaften des DHCP-Servers. Im Kontextmenü der Reservierung finden Sie außerdem den Befehl *Optionen konfigurieren*. Neben den Möglichkeiten für den Server bzw. für den Bereich können zusätzlich zur IP-Adresse und zum Subnetz noch weitere Einstellungen übergeben werden.

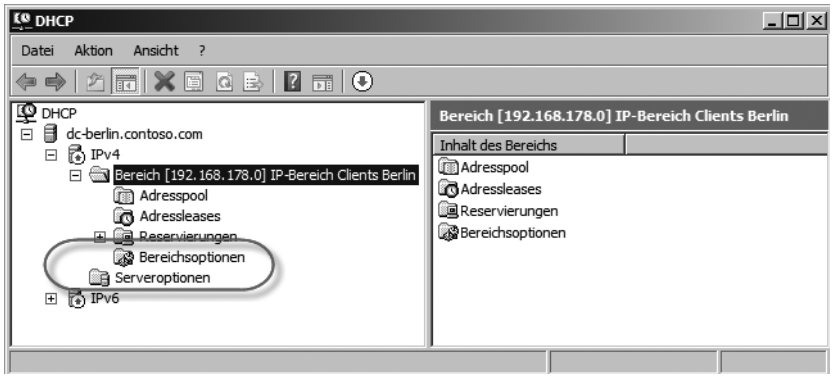
Abbildg. 11.36 Konfigurieren der DHCP-Optionen für Reservierungen



Zusätzliche DHCP-Einstellungen vornehmen

Zur Konfiguration der Optionen öffnen Sie entweder die *Eigenschaften* der Serveroptionen oder der jeweiligen Bereichsoptionen. Serveroptionen haben für alle erstellten Bereiche Gültigkeit, während Bereichsoptionen nur für den Bereich gelten, für den sie konfiguriert wurden.

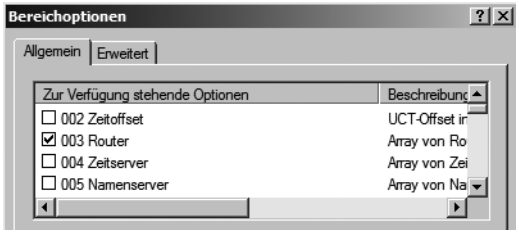
Abbildg. 11.37 Bearbeiten der Server- oder Bereichsoptionen für einen DHCP-Server



Um die Optionen zu bearbeiten, wählen Sie im Kontextmenü den Befehl *Optionen konfigurieren* aus. Aktivieren Sie nun das Kontrollfeld für die gewünschte Option und tragen Sie anschließend im Feld *Dateneingabe* jeweils die entsprechenden IP-Adressen, Namen oder Ähnliches ein. Die wichtigsten Optionen dabei sind:

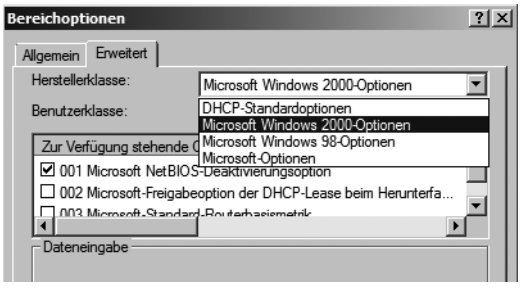
- 003 Router (Standardgateway)
- 006 DNS-Server
- 015 DNS-Domänenname
- 044 WINS/NBNS-Server
- 046 WINS/NBT-Knotentyp

Abbildg. 11.38 Konfigurieren von Optionen für Bereiche



Wenn Sie das komplette Netzwerk so weit umgestellt haben, dass Sie keine NetBIOS-Unterstützung mehr benötigen und dies über DHCP einstellen wollen, müssen Sie zur Registerkarte *Erweitert* wechseln. Dort wählen Sie unter *Herstellerklasse* den Eintrag *Microsoft Windows 2000-Optionen* und aktivieren die Option *001 Microsoft NetBIOS-Deaktivierungsoption*.

Abbildg. 11.39 Bearbeiten der Optionen zur Deaktivierung von NetBIOS im Netzwerk



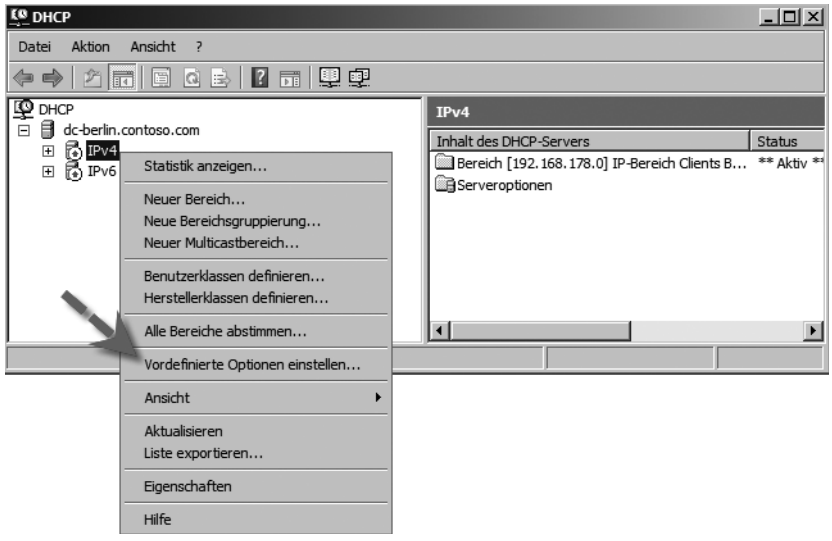
Der DHCP-Server ist nur mit einer beschränkten Anzahl an Optionen vorkonfiguriert. Es können jederzeit weitere Optionen hinzugefügt werden.

WPAD (Web Proxy Auto Detection)

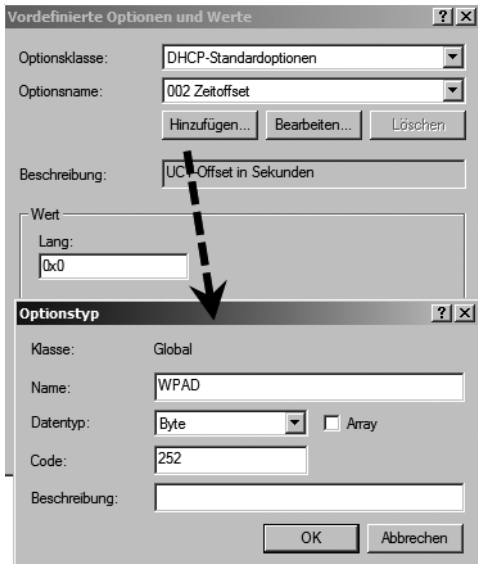
Als Beispiel soll über DHCP an die Clients übermittelt werden, bei welchem Proxyserver die Daten für die Internet Explorer-Autokonfiguration abgelegt sind. Diese Option wird als *WPAD (Web Proxy Auto Detection)* bezeichnet:

1. Wählen Sie im Kontextmenü des DHCP-Servers über IPv4 oder IPv6 den Eintrag *Vordefinierte Optionen einstellen*. Über *Hinzufügen* erstellen Sie nun eine neue Option.
2. Geben Sie als Namen für die neue Option *WPAD* ein und wählen Sie als Datentyp den Eintrag *Zeichenfolge* aus. Als Code für die Option geben Sie anschließend *252* an. Bestätigen Sie die Eingabe.

Abbildg. 11.40 Erstellen von neuen DHCP-Optionen für die Verwendung von WPAD



Abbildg. 11.41 Erstellen einer neuen DHCP-Option für den Einsatz von WPAD

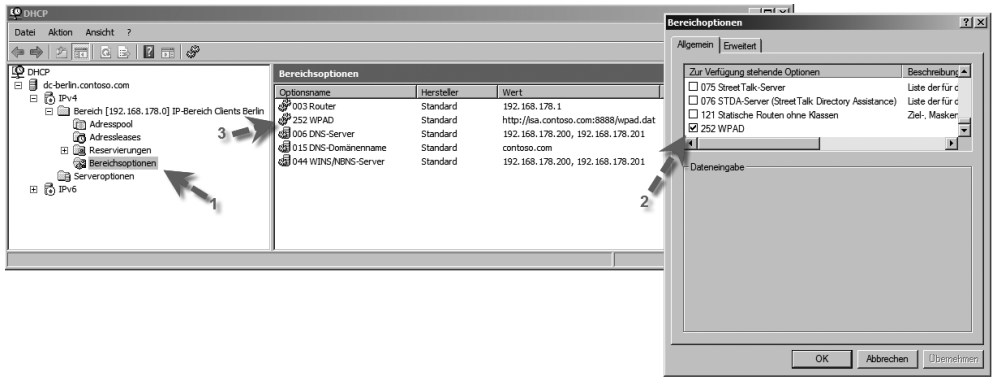


3. Stellen Sie jetzt sicher, dass unter *Optionsname* die neue Option *252 WPAD* ausgewählt ist und geben Sie im Feld *Zeichenfolge* anschließend den URL des Proxyservers an – dazu den Port, auf dem die Anfrage für die Autokonfiguration durchgeführt wird, und anschließend den Namen der Konfigurationsdatei, *Wpad.dat* (Abbildung 11.42). Auf der Internetseite *http://www.msisa-faq.de/anleitungen/2004/Konfiguration/wpad.htm* finden Sie dazu eine ausführliche Anleitung zur Verwendung von WPAD mit einem ISA-Server.

Abbildg. 11.42 Festlegen der URL für den WPAD-Eintrag

Wechseln Sie danach in die Bereichs- bzw. Serveroptionen und aktivieren Sie die Option *252 WPAD*. Bekommt ein Client jetzt per DHCP eine IP-Adresse zugewiesen, wird die neue Option ebenfalls übertragen, die anschließend vom Browser übernommen und ausgewertet werden kann.

Abbildg. 11.43 Aktivieren der WPAD-Option auf dem DHCP-Server

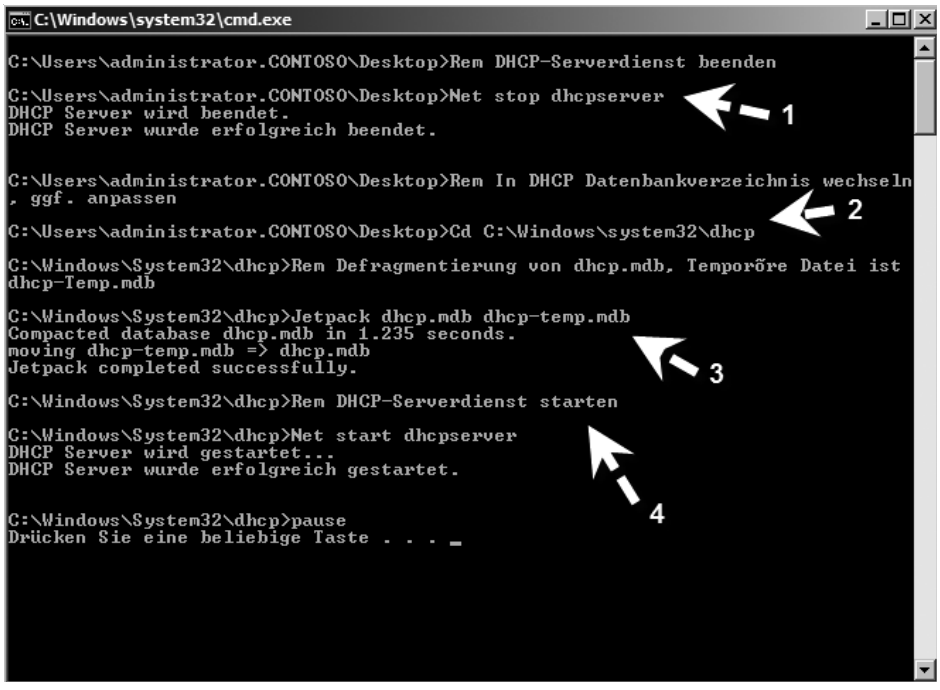


Verwalten und optimieren der DHCP-Datenbank

Durch die ständige Vergabe und Löschung von Leases wächst die Datenbank des DHCP-Servers im Laufe der Zeit und die Daten in der Datenbank werden immer weiter verteilt. Um die Performance des Systems zu erhöhen, sollten Sie daher gelegentlich mit dem Dienstprogramm *Jetpack* eine Defragmentierung der Datenbank durchführen. Da dazu aber der DHCP-Server gestoppt werden muss, kann dies nur außerhalb der regulären Betriebszeiten geschehen. Mit der folgenden Batchdatei lässt sich dieser Prozess automatisieren:

```
Rem DHCP-Serverdienst beenden
Net stop dhcpserver
Rem In DHCP Datenbankverzeichnis wechseln, ggf. anpassen
Cd %windir%\system32\dhcp
Rem Defragmentierung von dhcp.mdb, Temporäre Datei ist dhcp-Temp.mdb
Jetpack dhcp.mdb dhcp-temp.mdb
Rem DHCP-Serverdienst starten
Net start dhcpserver
```

Abbildg. 11.44 Defragmentieren der DHCP-Datenbank über eine Batchdatei in der Befehlszeile



Konsistenz der DHCP-Datenbank überprüfen

Ebenfalls wichtig ist die Überprüfung der Konsistenz der Active Directory-Datenbank. Klicken Sie dazu mit der rechten Maustaste auf den Knoten *IPv4* oder *IPv6* und wählen dann im Kontextmenü den Befehl *Alle Bereiche abstimmen* aus. Der Server überprüft darauf hin, ob die Inhalt der Bereiche und der Datenbank konsistent sind und keine Überschneidungen auftreten (Abbildung 11.45).

Abbildg. 11.45 Konsistenzüberprüfung der DHCP-Datenbank vornehmen

Verschieben einer DHCP-Datenbank auf einen anderen Server

Unter manchen Umständen muss die DHCP-Datenbank und deren Inhalt auf einen neuen Server verschoben werden. Es können nur DHCP-Datenbanken derselben Sprachversion wiederhergestellt werden. Gehen Sie dazu folgendermaßen vor. Damit Sie diese Schritte ausführen können, müssen Sie auf dem DHCP-Quell- und Zielserver Mitglied der Gruppe *Administratoren* oder der Gruppe *DHCP-Administratoren* sein:

1. Sichern Sie die DHCP-Datenbank auf dem Quell-Server über das Kontextmenü des Servers in der Verwaltungskonsole. Der DHCP-Dienst erstellt während des normalen Betriebs auch eine automatische Sicherungskopie der DHCP-Datenbank. Standardmäßig wird diese Kopie der Datenbanksicherung im Verzeichnis *Windows\System32\Dhcp\Backup* gespeichert.
2. Beenden Sie den DHCP-Server. Dadurch wird verhindert, dass der Server nach dem Sichern der Datenbank neue Adressleases an Clients zuweist.
3. Deaktivieren Sie den DHCP-Serverdienst.
4. Kopieren Sie den Ordner mit der DHCP-Sicherungsdatenbank auf den DHCP-Zielserver.
5. Öffnen Sie auf dem Ziel-Server die DHCP-Verwaltungskonsole
6. Klicken Sie im Kontextmenü auf *Wiederherstellen*.
7. Wählen Sie den Ordner mit der DHCP-Sicherungsdatenbank aus, und klicken Sie dann auf *OK*.

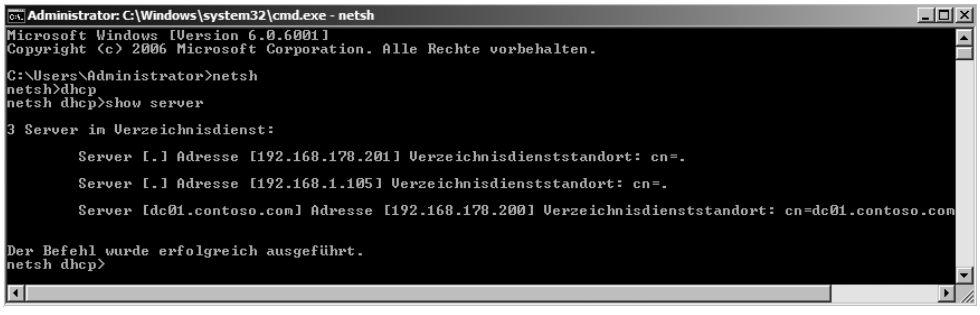
Core-Server – DHCP mit *netsh.exe* über die Befehlszeile verwalten

Der DHCP-Dienst von Windows Server 2008 lässt sich mit dem Befehl *netsh* auch über die Befehlszeile verwalten. Vor allem auf Core-Servern ist dieses Tool der beste Weg zur Verwaltung, wenn nicht die DHCP-Konsole von einem anderen Server verwendet werden soll. Geben Sie dazu in der Befehlszeile zunächst *netsh* ein und bestätigen Sie. Anschließend geben Sie *dhcp* ein und bestätigen Sie. Jetzt können die spezifischen DHCP-Befehle in der Befehlszeile verwendet werden. Die folgen-

den Befehle stehen zur Verfügung. Innerhalb der Konsole können weitere Befehle über *list* angezeigt werden:

- **add server** Fügt einen DHCP-Server zur Liste der autorisierten Server in Active Directory hinzu. Syntax: *add server <Server-DNS> <Server-IP>*. Der Parameter *<Server-DNS>* gibt den DHCP-Server an, der hinzugefügt werden soll. Der Server wird durch die IP-Adresse identifiziert, daher sind beide Optionen wichtig.
- **delete server** Löscht einen DHCP-Server aus der Liste der autorisierten Server in Active Directory. Syntax: *delete server <Server-DNS> <Server-IP>*. Der Parameter *<Server-DNS>* gibt den DHCP-Server an, der hinzugefügt werden soll. Der Server wird durch die IP-Adresse identifiziert, daher sind beide Optionen wichtig.
- **server** Wechselt vom aktuellen Netsh-DHCP-Befehlszeilenkontext zu dem eines anderen DHCP-Servers. Werden keine Parameter verwendet, wechselt *server* vom aktuellen Befehlszeilenkontext zum Kontext des lokalen Computers.
- **show server** Zeigt eine Liste der autorisierten Server in Active Directory an (Abbildung 11.46)

Abbildg. 11.46 Anzeigen der autorisierten DHCP-Server über die Befehlszeile



Neben den Standardbefehlen stehen noch zahlreiche andere Befehle zur Verfügung, die über *help* angezeigt werden können. Auch die entsprechende Syntax der Befehle kann über die Hilfe in der Befehlszeile angezeigt werden. Es würde den Umfang dieses Buches sprengen alle Befehle zu besprechen. Auf der Internetseite *http://technet2.microsoft.com/windowsserver/de/library/61427fbd-de1f-4c8a-b613-321f7a3cca6a1031.mspx?mfr=true* finden Sie die Optionen, die neben Windows Server 2003 auch für Windows Server 2008 gelten.

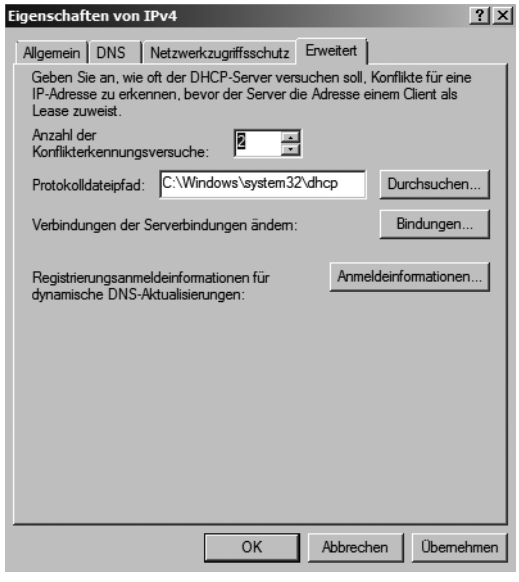
Ausfallsicherheit bei DHCP-Servern herstellen

Die Ausfallsicherheit bei DHCP-Servern herzustellen, gestaltet sich leider etwas schwieriger, als dies zum Beispiel beim DNS der Fall ist. Aufgrund der laufenden und schnellen Änderungen an der DHCP-Datenbank ist eine Replikation zwischen zwei DHCP-Servern nicht möglich, da während des Replikationsvorgangs bereits ein weiterer Client eine IP-Adresse anfordern könnte, die der andere DHCP-Server soeben vergeben hat. Die Folge wäre ein IP-Adresskonflikt. Den Adressbereich in zwei getrennte Bereiche aufzuteilen, die jeweils von einem Server exklusiv verwaltet werden, ist auch nur dann sinnvoll, wenn ein Server allein alle Computer mit den verbleibenden IP-Adressen versorgen könnte. Setzen Sie aber 150 Computer ein und verwenden ein Klasse-C-Netz mit nur 254 IP-Adressen schlägt diese Aufteilung fehl.

Ausfallsicherheit durch Konflikterkennung

Als praktisch hat sich die Funktion der Konflikterkennung erwiesen, bei der ein DHCP-Server zunächst versucht, einen Verbindungsaufbau mit der IP-Adresse zu bewerkstelligen, die er als Nächstes vergeben will. Bekommt er darauf keine Antwort, ist die Adresse unbenutzt und kann vergeben werden, andernfalls wird sie übergangen und der DHCP-Server verwendet die nächste verfügbare IP-Adresse. Wenn Sie nun auf beiden DHCP-Servern die Anzahl der Konflikterkennungsversuche in den Servereigenschaften von IPv4 oder IPv6 auf der Registerkarte *Erweitert* auf den Wert 1 oder 2 setzen, können Sie auf beiden Servern den gleichen Bereich definieren, ohne dass es zu doppelten Adressvergaben kommt (Abbildung 11.47). Sie müssen dabei lediglich bedenken, dass sich die Adressvergabe etwas verlangsamt.

Abbildg. 11.47 Arbeiten mit den Konflikterkennungsversuchen eines DHCP-Servers



Erkennt der DHCP-Client einen Konflikt, sendet er eine DHCP-Ablehnungsmeldung (*DHCPDECLINE*) an den Server. Für jeden zusätzlichen Konflikterkennungsversuch des DHCP-Dienstes werden der für die Aushandlung von Leases für DHCP-Clients benötigten Zeit zusätzliche Sekunden hinzugefügt. Beim Verwenden der Konflikterkennung sollten Sie die Anzahl der Konflikterkennungsversuche des Servers auf maximal zwei Versuche festlegen.

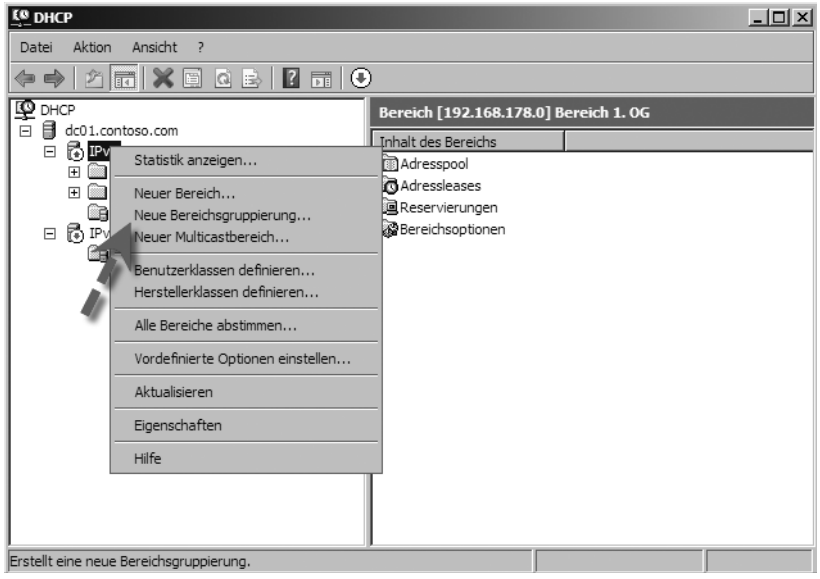
Ausfallsicherheit mit 80/20-Regel

Eine weitere Möglichkeit und Strategie der Ausfallsicherheit für DHCP-Server, ist die 80/20-Regel. Bei dieser Regel verwaltet ein DHCP-Server 80 % der Adressen eines Bereiches, und einer zweiter DHCP-Server 20 % des Bereiches. Die IP-Adressen dürfen sich nicht überlappen. Fällt ein Server aus, kann der zweite Server zumindest teilweise übernehmen.

Bereichsgruppierung (Superscopes)

Bereich werden im englischen als Scope bezeichnet. Unter Windows Server 2008 können mehrere Bereiche eines DHCP-Servers zu einer Bereichsgruppierung, auf englischen Servern auch Superscope genannt, zusammengefasst werden. Clients die IP-Adressen anfragen, erhalten dadurch IP-Adressen aus allen der zusammengefassten Bereichen. Bereichsgruppierungen können über das Kontextmenü des DHCP-Servers über IPv4 oder IPv6 erstellt werden (Abbildung 11.48).

Abbildg. 11.48 Gruppieren von IP-Bereichen



Durch den Einsatz von Bereichsgruppen erhalten Sie mehrere Vorteile:

- Sind die IP-Adressen eines Bereichs erschöpft erhalten Clients IP-Adressen aus einem anderen Bereich.
- Netzwerke können logisch voneinander getrennt werden.
- Beim Starten überträgt jeder DHCP-Client eine DHCP-Ermittlungsnachricht (DHCPDISCOVER) an das lokale Subnetz auf der Suche nach einem DHCP-Server. Da DHCP-Clients beim ersten Starten Broadcasts verwenden, kann nicht vorhergesagt werden, welcher Server auf die DHCP-Ermittlungsanforderung eines Clients antwortet, wenn mehrere DHCP-Server innerhalb eines Subnetzes aktiv sind. Dieses Probleme kann mithilfe einer Bereichsgruppierung, die auf allen Servern gleich konfiguriert ist, vermieden werden. Zur Bereichsgruppierung sollten alle gültigen Bereiche für das Subnetz als Mitgliedsbereiche gehören. Für die Konfiguration von Mitgliedsbereichen auf den einzelnen Server genügt es, IP-Adressen nur auf einem der DHCP-Server im Subnetz zur Verfügung zu stellen. Für alle anderen Server im Subnetz sollten Ausschlussbereiche für dieselben Bereichsadressen beim Konfigurieren der entsprechenden Bereiche verwendet werden.

TIPP Wenn Sie mit DHCP arbeiten, benötigen Sie das Befehlszeilenprogramm *ipconfig*. Hauptsächlich benötigen Sie das Tool mit folgenden Optionen:

- **Ipconfig** Gibt die IP-Adresse, Standardgateway und Subnetzmaske des Clients aus
- **Ipconfig /all** Gibt detaillierte Informationen, auch über den konfigurierten DNS und WINS-Server, aus
- **Ipconfig /release** Entfernt die IP-Adresse vom Client und fordert keine neue an. Wenn ein Client Probleme hat, eine Verbindung mit einem DHCP-Server herzustellen, sollten Sie immer zuerst die IP-Adresse beim Client zurücksetzen.
- **Ipconfig /renew** Fordert vom DHCP-Server eine erneute Verlängerung des Leases oder eine neue IP-Adresse an
- **Ipconfig /registerdns** Erneuert die Registrierung des Clients am konfigurierten DNS-Server, wenn für die DNS-Zone die dynamischen Updates aktiviert sind
- **Ipconfig /flushdns** Löscht den lokalen DNS-Cache

DNS in Windows Server 2008

DNS ist einer der zentralen Mechanismen des Internet und von allen TCP/IP-basierenden Netzwerken. In diesem Abschnitt wird auf die Grundkonzepte von DNS eingegangen. In den vorangegangenen Kapiteln sind wir bereits bei der Einrichtung von Active Directory auf DNS eingegangen. Allerdings bietet der DNS-Server unter Windows Server 2008 noch wesentlich mehr Funktionen, als für einzelne Active Directory-Domänen die Namensauflösung zur Verfügung zu stellen. DNS wird unter Windows Server 2008 als Serverrolle installiert und konfiguriert. Für die Einrichtung von Active Directory muss diese Rolle nicht zwingend installiert werden, da der Server-Manager in diesem Fall DNS automatisch mit installiert. Unabhängig davon, ob ein DNS-Server Active Directory-Zonen verwaltet, kann er beliebig weitere DNS-Domänen in verschiedenster Ausprägung verwalten. Die Verwaltung von DNS findet mit einem eigenen Snap-In statt, das entweder über den Server-Manager oder über *Start/Verwaltung* gestartet werden kann.

Grundkonzepte von DNS

DNS steht für *Domain Name System*. DNS ist einer der zentralen Mechanismen des Internet. Die zentrale Aufgabe des Protokolls und der dahinter stehenden Dienste ist die Auflösung (Umsetzung) von Computernamen in IP-Adressen. Wenn ein Benutzer auf *www.microsoft.com* zugreift, wird aus diesem Computernamen eine IP-Adresse gebildet. Beim Senden einer E-Mail an *test@microsoft.com* wird DNS verwendet. In diesem Fall wird der zuständige Mailserver für *microsoft.com* ermittelt. DNS kann eine Zuordnung in umgekehrter Richtung vornehmen und feststellen, welcher Name zu einer IP-Adresse gehört. Das ist im Bereich der Sicherheit und des Spamschnutzes wichtig, es kann damit überprüft werden, ob ein Server, der sich als *dns.microsoft.com* ausgibt, *dns.microsoft.com* ist oder ob sich hinter der von diesem Server gelieferten IP-Adresse nicht tatsächlich ein ganz anderes System verbirgt. Diese Zugriffe von der IP-Adresse auf Namen werden als *Reverse-Lookups* bezeichnet. Bei DNS spielen zwei Begriffe eine besonders wichtige Rolle:

- Es gibt den Begriff der *Domäne*. Diese Domäne ist nicht mit den Domänen in Active Directory zu verwechseln. Domänen werden verwendet, um Netzwerke zu strukturieren. Es gibt für das gesamte Internet eine zentralistische Struktur für die Vergabe von Domänennamen. Domänen können in Subdomänen aufgegliedert werden. So könnte unterhalb einer Domäne *contoso.com* eine Domäne *de.contoso.com* und darunter eine Domäne *berlin.de.contoso.com* geschaffen werden. Die untergeordneten Domänen werden als *Subdomänen* bezeichnet.
- Der zweite wichtige Begriff ist die *Zone*. Eine Zone bezeichnet eine physische Verwaltungseinheit bei DNS. Eine Zone kann eine Domänen und untergeordnete Subdomänen umfassen. Es können nur hierarchisch verbundene Domänen in einer gemeinsamen Zone verwaltet werden. So kann eine Domäne nicht über mehrere Zonen aufgesplittet werden. Für jede Zone gibt es eine Zonendatei, die auf andere DNS-Server kopiert werden kann.

Für jede Zone gibt es einen *primären Namensserver*. Auf diesem werden alle Änderungen durchgeführt. Er kann seine Änderungen auf andere, *sekundäre Namensserver* replizieren. Dadurch kann ein DNS-Server durchaus als *primärer Namensserver* für eine Zone und als *sekundärer Namensserver* für eine andere Zone fungieren. Im Normalfall arbeitet DNS mit einem Single Master-Konzept. Änderungen können nur auf dem primären Namensserver vorgenommen werden. Diese werden anschließend verteilt. Anders stellt sich das bei Windows Server 2008 dar. Bei dem DNS-Server von Windows Server 2008 werden die DNS-Informationen im Active Directory abgelegt und über die Replikationsmechanismen von Active Directory verteilt. Das hat mehrere Vorteile:

- Durch diesen Ansatz wird ein Konzept ermöglicht, das nicht mehr die Single Master-Problematik hat. Änderungen können über mehrere DNS-Server erfolgen.
- Die Integration von Active Directory und DNS wird dadurch erleichtert, da eine Reihe von Informationen von Active Directory als DNS-Informationen abgelegt werden muss.
- Die Replikation zwischen DNS-Servern erfolgt als Active Directory-Replikation. Es werden nur die Änderungen an der DNS-Datenbank in sicherer Weise verteilt, während im Regelfall die komplette Zonendatei über das Netzwerk kopiert wird. Es wird ein normaler Kopiervorgang verwendet, bei dem weder die Fehlerfreiheit sichergestellt ist noch ein zusätzlicher Schutz der kopierten Daten erfolgt.
- Der Administrator muss nur eine Replikationstopologie verwalten anstatt zwei. Das hilft Kosten zu sparen, da die Replikation von Active Directory ohnehin konfiguriert und verwaltet werden muss.

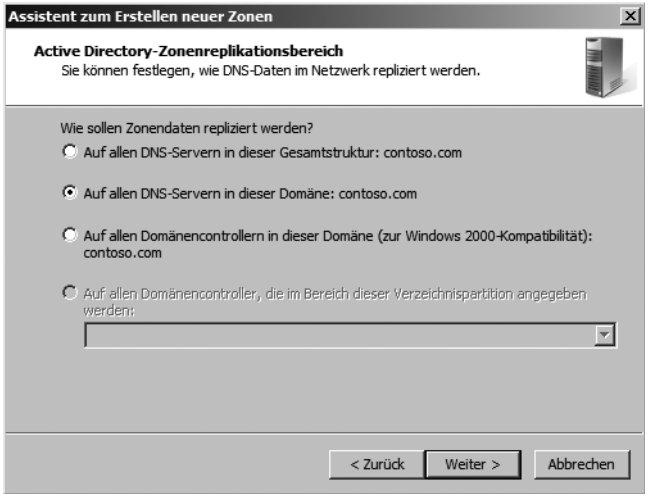
Erstellen von Zonen und Domänen

Über das Menü zur Verwaltung von DNS können Sie verschiedene Zonen erstellen. *Forward-Lookupzonen* übersetzen DNS-Namen in IP-Adressen. Eine *Reverse-Lookupzone* übersetzt dagegen IP-Adressen in DNS-Namen. Nur auf Domänencontrollern kann mit den Active Directory-integrierten Zonen gearbeitet werden. Unterschieden wird weiterhin zwischen *primären* und *sekundären* Zonen sowie so genannten *Stubzonen*, die nur auf andere DNS-Server verweisen. Bei der Einrichtung des ersten DNS-Servers müssen Sie eine primäre Zone erstellen. Grundsätzlich gilt, dass Sie in Active Directory-Umgebungen wegen mit Active Directory-integrierten Zonen arbeiten sollten. Das bedeutet in der Konsequenz allerdings, dass die DNS-Serverdienste immer auf Domänencontrollern installiert werden müssen.

Abbildg. 11.49 Festlegen des Zonentyps

Wird eine Zone in Active Directory gespeichert, kann festgelegt werden, auf welche DNS-Server in der Gesamtstruktur diese Zone repliziert werden soll. Dieses Fenster erscheint aber nur, wenn eine Zone in Active Directory gespeichert wird. Die Reihenfolge der folgenden Fenster kann variieren abhängig davon, welche Einstellungen ausgewählt werden.

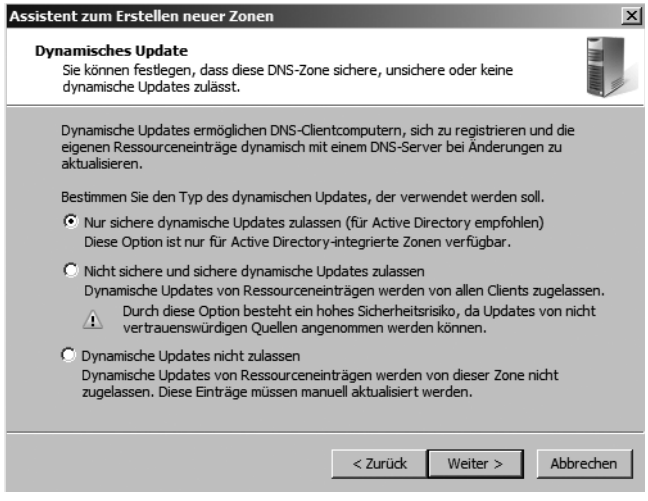
Abbildg. 11.50 Festlegen des Replikationsbereiches für eine DNS-Zone



Der nächste Schritt ist die Festlegung des Zonennamens. Hier wird festgelegt, wie die Zone tatsächlich heißt und welche Domäne von dieser Zone verwaltet wird. Als Nächstes kann festgelegt werden, ob die Zone dynamische DNS-Einträge erlaubt und welche Bedingungen dafür zutreffen müssen (Abbil-

dung 11.51). Dynamische Updates aktualisieren die Informationen zu einem Server oder Client. Damit müssen die Einträge in der DNS-Datenbank nicht mehr, wie es früher üblich war, manuell gepflegt werden. Die Einträge können von Clients oder über DHCP-Server aktualisiert werden.

Abbildg. 11.51 Festlegen der dynamischen Updates für eine DNS-Zone



Danach müssen Sie die Zonendatei benennen, aber nur wenn die Zone nicht in Active Directory gespeichert wird. Die Datei erhält die Bezeichnung *<Zonenname>.dns*. In der Regel sollten Sie diese nicht umbenennen, da sie durch den gewählten Namen eindeutig bezeichnet ist. Sie können an dieser Stelle allerdings eine bereits vorhandene Datei importieren. Falls Sie eine neue Datei angeben, wird diese automatisch in dem Verzeichnis erstellt (Abbildung 11.52).

Abbildg. 11.52 Festlegen des Dateinamens für die Zone bei nicht Active Directory-integrierten DNS-Zonen

Bei den Einstellungen für die Reverse-Lookupzone müssen Sie die Netzwerkkennung eingeben. Diese wird automatisch in den Namen der Reverse-Lookupzone umgesetzt. Diese Art von Zonen hat vorgegebene Namen. Falls mehrere IP-Subnetze zu der von Ihnen verwendeten Forward-Lookupzone gehören, müssen Sie mehrere Reverse-Lookupzonen erstellen. Analog zur Vorgehensweise bei der Konfiguration einer Forward-Lookupzone müssen Sie den Namen der Datei angeben, in der die Konfigurationsinformationen gespeichert werden sollen. Dieser wird ebenfalls vorgegeben und muss in der Regel nicht angepasst werden.

Erstellen von statischen Einträgen in der DNS-Datenbank

Die Administration der DNS-Server erfolgt entweder über *Verwaltung/DNS* im Startmenü oder über den Server-Manager. Es kann Situationen geben, in denen Sie Hostnamen manuell hinzufügen müssen und die dynamischen Einträge alleine nicht ausreichen. In diesem Fall verwenden Sie den Befehl *Neuer Host* im Kontextmenü der Zone, zu der der Eintrag hinzugefügt werden soll. Sie können dort den Hostnamen – ohne den Namen der Zone – und die IP-Adresse angeben. Sie können gleich einen als *PTR-Eintrag (Pointer)* bezeichneten Eintrag in der Reverse-Lookupzone vornehmen.

Abbildg. 11.53 Erstellen von neuen statischen Host-Einträgen

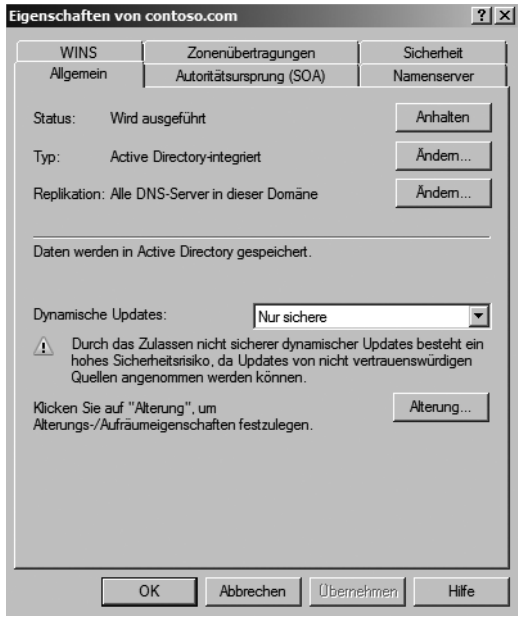
Einstellungen und verwalten von Zonen

Wenn Sie die Eigenschaften einer Zone aufrufen, stehen Ihnen verschiedene Registerkarten zur Verfügung, auf denen Sie die Konfiguration der Zone anpassen können. Die Registerkarte *WINS* ist ausführlich im Abschnitt »Integration von WINS in DNS« weiter vorne in diesem Kapitel besprochen. Die Registerkarte *Sicherheit* dient zur Konfiguration der Sicherheitseinstellungen und der Berechtigungen für die Verwaltung der Zone. Hier können Einstellungen vorgenommen werden, um die Berechtigungsstruktur anzupassen, damit einige Benutzergruppen oder Administratoren zwar Informationen der Zone lesen, aber keine Informationen schreiben dürfen.

Registerkarte *Allgemein*

Auf der Registerkarte *Allgemein* können Sie festlegen, dass die Zone in Active Directory integriert wird und welche Systeme sich dynamisch aktualisieren dürfen. In kleineren Netzwerken kann es durchaus Sinn machen, wenn Sie neben den sicheren auch unsichere Aktualisierungen zulassen. Die Namensauflösung in Microsoftnetzwerken ist sehr wichtig. Der parallele und stabile Betrieb einer WINS- und einer DNS-Infrastruktur ist daher sehr wichtig. Auch in größeren Netzwerken mit vielen DNS-Zonen spielt die Replikation der DNS-Daten keine große Rolle beim Datenverkehr. Gehen Sie daher immer auf Nummer sicher und lassen Sie möglichst alle Zonen in das Active Directory integrieren.

Abbildg. 11.54 Verwalten einer Zone über deren Eigenschaften



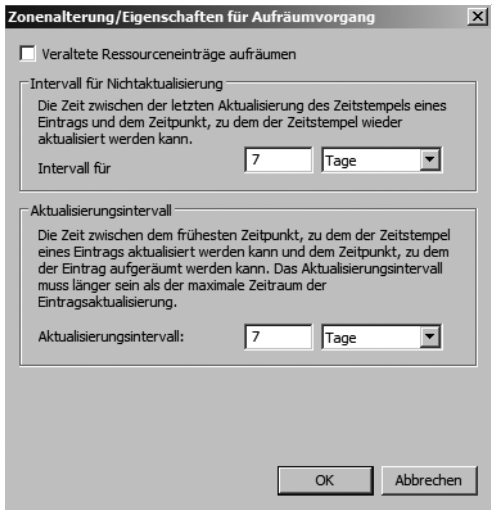
Konfiguration des Entfernens alter Einträge aus der Zone

So bequem die dynamische Aktualisierung der DNS-Einträge für den Administrator auch sein mag, sie birgt auch die Gefahr, dass sich im Laufe der Zeit eine Menge veraltete Einträge ansammeln, zum Beispiel Maschinen, die irgendwann mal in Betrieb waren, sich dynamisch registriert haben und irgendwann wieder außer Betrieb genommen wurden. Die zugehörigen DNS-Einträge verbleiben allerdings in der Datenbank und erhöhen natürlich den Platzbedarf, die Zeit für Suchen in der Datenbank sowie die Übertragungszeiten bei der Replikation zu anderen DNS-Servern. Um diesem Wachstum Einhalt zu gebieten, sollten Sie die Alterung der dynamischen Einträge konfigurieren. Dies kann auf der Registerkarte *Allgemein* über die Schaltfläche *Alterung* vorgenommen werden. In der Standardeinstellung bleiben alle Einträge so lange erhalten, bis sie vom Administrator manuell gelöscht werden. Aktivieren Sie das Kontrollkästchen *Veraltete Ressourceneinträge aufräumen*, um die Einträge mit Zusatzinformationen über den Zeitpunkt der letzten Aktualisierung, den so genannten Zeitstempel, zu versehen und sie anschließend aufgrund dieser Informationen als veraltet erkennen und löschen zu können. Da jede Änderung des Zeitstempels immer dazu führt, dass

sekundäre DNS-Server eine Replikation der DNS-Daten anfordern, wird eine Mindestzeit vorgegeben, nach der der Zeitstempel wieder neu gesetzt werden kann. Registriert sich ein System während dieser Zeit erneut beim DNS-Server, erfolgt keine Veränderung an diesem Eintrag. Erst nach Ablauf der Zeit wird der Zeitstempel neu gesetzt. Diesen Wert legen Sie im Abschnitt *Intervall für Nichtaktualisierung* fest.

Die eigentliche Verweildauer eines Eintrags in der Datenbank legen Sie im zweiten Abschnitt *Aktualisierungsintervall* fest. Nach Ablauf dieser Zeitspanne wird ein System als inaktiv erkannt und der zugehörige Eintrag aus der Zone gelöscht. Der hier angegebene Wert muss größer sein als das minimale Intervall zwischen zwei Aktualisierungen des Zeitstempels, da sonst auch aktive Einträge gelöscht würden, die lediglich noch nicht aktualisiert werden konnten.

Abbildg. 11.55 Konfigurieren der Zonenalterung für DNS-Zonen

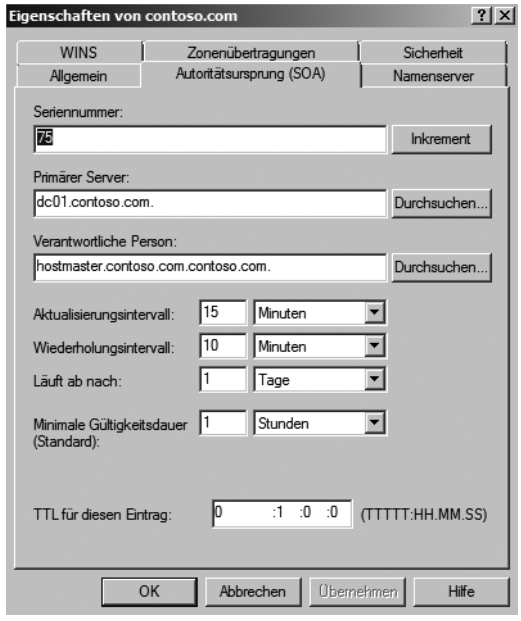


Sie können den Prozess auch manuell starten, indem Sie im Kontextmenü des DNS-Servers den Befehl *Veraltete Ressourceneinträge aufräumen* aufrufen und die anschließende Sicherheitsabfrage bestätigen.

Registerkarte *Autoritätsursprung (SOA)*

Auf der Registerkarte *Autoritätsursprung (SOA)* werden Informationen abgelegt, die für die Replikation der Zone zu anderen Servern sowie die Zwischenspeicherung abgefragter DNS-Einträge wichtig sind. Damit sekundäre DNS-Server erkennen können, ob sich an den Daten des primären DNS-Servers etwas geändert hat und damit eine Replikation notwendig geworden ist, wird für jede Zone eine Serien- oder Versionsnummer gepflegt. Diese Seriennummer wird mit jeder Veränderung an der Datenbank um 1 erhöht. Fragt ein sekundärer DNS-Server die Seriennummer des primären DNS-Servers ab, so stellt er einen Versionsunterschied fest und fordert eine Übertragung der Zonendaten an (man spricht hier auch von einem Zonentransfer). Diesen Wert können Sie nun selbst erhöhen, auch ohne dass neue Einträge in der Datenbank vorhanden sind. Dies ist zum Beispiel dann sinnvoll, wenn Sie eine Beschädigung in der DNS-Datenbank festgestellt und die Datenbank anschließend repariert oder von einer Sicherung wieder eingespielt haben. Damit alle sekundären DNS-Server diese Datenbank erhalten, müssen Sie ihnen signalisieren, dass es eine Änderung gegeben hat.

Abbildg. 11.56 Verwalten der Einstellungen zum Übertragen von Informationen an sekundäre DNS-Server



Der im Feld *Primärer Server* angegebene Eintrag definiert den Server, der im SOA-Eintrag im DNS eingesetzt wird. Während an dieser Stelle logisch ist, welcher Server hier einzutragen ist, nämlich der primäre DNS-Server, wird diese Option dann relevant, sobald die Zone ins Active Directory integriert wird. Alle Server, bei denen diese Änderung vorgenommen wurde, werden gleich gestellt, und es gibt in diesem Sinne keinen ersten DNS-Server mehr. Da aber noch andere Server als klassische sekundäre DNS-Server eingesetzt werden können, muss diesen klar ein primärer DNS-Server vorgegeben werden. Wählen Sie den gewünschten Server jeweils über *Durchsuchen* aus. Im folgenden Feld geben Sie an, wer die verantwortliche Person für die Verwaltung der Zone ist. Dabei handelt es sich um die E-Mail-Adresse des DNS-Administrators, sodass andere Administratoren Kontakt zu ihm aufnehmen können, falls sie Probleme feststellen. Da das Zeichen <@> im DNS nicht erlaubt ist, wird es durch einen Punkt ersetzt, der oben abgebildete Eintrag steht also für *hostmaster@contoso.com*. Über das *Aktualisierungsintervall* teilt der primäre DNS-Server den sekundären Servern mit, wie oft sie überprüfen sollen, ob es Änderungen in der Zone gibt. Je kleiner die Abstände sind, desto aktueller sind natürlich auch die Kopien auf den sekundären Servern. Dafür steigt allerdings auch die bei der Übertragung anfallende Datenmenge, da je nach Anzahl der Änderungen und verwendeter Software beim sekundären Server eine Übertragung der kompletten Zonendaten notwendig sein kann. Zu große Intervalle dagegen führen unter Umständen zu falschen Informationen.

Kann die Aktualisierung der Daten nicht durchgeführt werden, zum Beispiel wegen eines Ausfalls des Servers oder der Netzwerkverbindung zwischen primärem und sekundären Servern, wird nach Ablauf des Wiederholungsintervalls der Versuch wiederholt. Kann die Replikation länger als unter *Läuft ab* nicht durchgeführt werden, so werden die kompletten Informationen der Zone auf dem sekundären Server als ungültig markiert und nicht mehr weiter verwendet. Sie sollten diesen Wert daher nicht zu niedrig setzen. So könnte der Ausfall des primären DNS-Servers an einem Freitag Nachmittag dazu führen, dass das komplette Netzwerk montags nicht mehr verwendet werden kann, da zwar für die Ausfallsicherheit sekundäre DNS-Server installiert wurden, diese ihre Daten

aber länger als einen Tag nicht mit dem primären DNS-Server abgleichen konnten und ihre Zoneneinträge damit als ungültig markiert haben. Eine Einstellung von drei Tagen dagegen hätte die Daten bis Montag Nachmittag gültig sein lassen. Um die bei DNS-Abfragen entstehende Datenmenge zu reduzieren, werden die Ergebnisse auf Clients wie auf DNS-Servern in einem Cache zwischengespeichert. Wie lange sie gespeichert werden, wird über die *TTL (Time to Live)* angegeben. Bei dieser TTL handelt es sich um eine absolute Zeit. Kann ein DNS-Server eine Anfrage aus seinem Cache beantworten, dann gibt er als TTL nicht wieder den Startwert (hier 1 Stunde) weiter, sondern nur noch die verbleibende TTL von zum Beispiel 15 Minuten. Nach Ablauf der Zeit wird der Eintrag auf allen Systemen aus dem Cache gelöscht. Diese TTL kann für jeden Eintrag in der Zone separat gesetzt werden, der Wert gibt lediglich die Standardeinstellung vor. Die TTL für diesen Eintrag entspricht in der Standardeinstellung diesem Wert.

Registerkarte *Namenserver*

Damit in der Zone nicht nur die Adresse des primären DNS-Servers im SOA-Eintrag aufgeführt wird, sondern auch die aller sekundären DNS-Server in den NS-Einträgen, müssen Sie diese zunächst in der Registerkarte *Namenserver* einfügen. Nachdem Sie über *Hinzufügen* einen neuen Eintrag erstellt haben, wird auch ein neuer NS-Eintrag in der Zone erstellt. Falls es Änderungen beim Namen bzw. an den IP-Adressen der DNS-Server gibt, können Sie diese über *Bearbeiten* ändern. Bevor ein DNS-Server abgeschaltet wird, sollten Sie ihn über *Entfernen* aus der Liste nehmen, damit kein Client mehr versucht, von diesem System noch Informationen zu erhalten.

Abbildg. 11.57 Konfigurieren der Namensserver für eine DNS-Zone

Wenn Sie einen neuen Namenserver hinzufügen, geben Sie zunächst den vollständigen Hostnamen an. Alternativ können Sie auch über *Durchsuchen* einen bereits bestehenden DNS-Eintrag auswählen. Sofern Sie einen bereits eingetragenen Servernamen ausgewählt haben, brauchen Sie die zugehörigen IP-Adressen nicht von Hand einzutragen, sondern können sie über *Auflösen* direkt aus dem

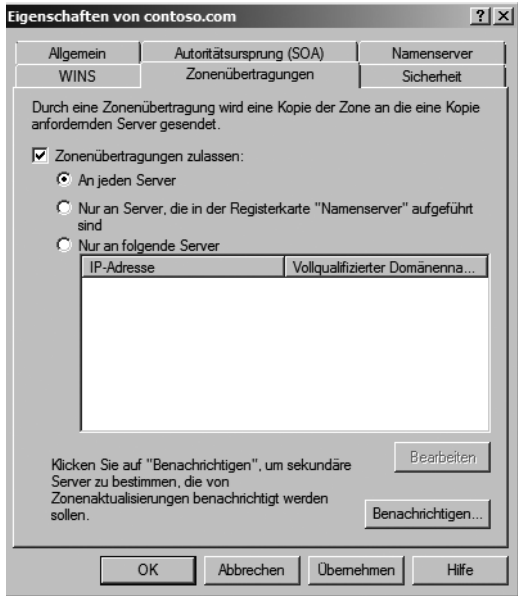
DNS-Server auslesen. Eine manuelle Überarbeitung der IP-Adressen ist im Anschluss auch über die Schaltflächen *Hinzufügen* und *Entfernen* möglich. In einigen Fällen sind DNS-Server auch mit mehreren IP-Adressen ausgestattet. Sofern beide Schnittstellen für Clients und andere DNS-Server erreichbar sind, spielt die Reihenfolge keine große Rolle. Wird zwischen den beiden Karten aber nicht geroutet, dann sollten Sie über die Schaltflächen *Nach oben* und *Nach unten* die IP-Adresse an die erste Stelle setzen, die von den anderen Systemen erreicht werden kann, um Verzögerungen bei der Abfrage zu reduzieren. Wenn Sie noch weitere Namenserver hinzufügen wollen, müssen Sie diesen Eintrag erst mit *OK* bestätigen und anschließend einen weiteren Eintrag erstellen.

Registerkarte *Zonenübertragungen*

Auf der einen Seite ist es natürlich gut, dass eine Replikation der Zonendaten auf sekundäre DNS-Server möglich ist, da dies die Verfügbarkeit und die Leistung erhöht. Andererseits drohen hier allerdings auch Gefahren. Ein Angreifer könnte so zum Beispiel eine Replikation der Daten anfordern, die er anschließend lokal modifiziert und schließlich DNS-Anfragen auf seinen modifizierten Server umleitet.

Die Registerkarte *Zonenübertragungen* erlaubt eine gezielte Einschränkung dieses Zonentransfers. In der Standardeinstellung ist diese Funktion deaktiviert und erlaubt sekundären DNS-Servern keine Durchführung des Zonentransfers. Wenn Sie das Kontrollkästchen *Zonenübertragungen zulassen* deaktiviert lassen, ist diese Funktion nicht verfügbar. In diesem Fall können nur noch Active Directory-integrierte Zonen zu anderen DNS-Servern repliziert werden, da hier die internen Replikationsmechanismen von Active Directory verwendet werden und nicht die des DNS.

Abbildg. 11.58 Konfigurieren der DNS-Zonenübertragungen an andere DNS-Server



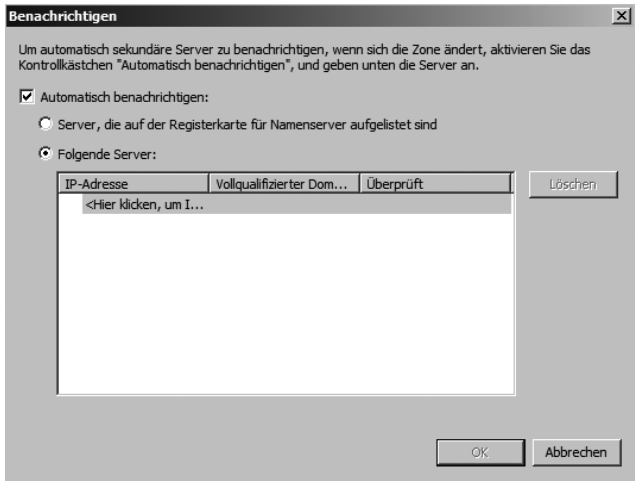
Sofern Sie die Zonenübertragung erlauben, können Sie nun noch feiner abstufen, zu welchen Servern eine solche Zonenübertragung überhaupt nur durchgeführt werden darf:

- **An jeden Server** Diese Variante ist die einfachste, da keine weitere Konfiguration mehr erfolgen muss. Dafür kann jeder DNS-Server jetzt den Zonentransfer anfordern, was eine entsprechende potenzielle Sicherheitslücke bedeutet.
- **Nur an Server, die in der Registerkarte "Namenserver" aufgeführt sind** Da Sie im Vorfeld auf der Registerkarte *Namenserver* bereits die sekundären Namenserver eingepflegt haben, ist diese Einstellung auch mit wenig administrativem Aufwand verbunden. Server, die nicht auf dieser Registerkarte geführt sind, werden bei einer Anforderung des Zonentransfers abgewiesen.
- **Nur an folgende Server** Hier definieren Sie explizit über die Schaltflächen *Hinzufügen* und *Entfernen* die IP-Adressen der DNS-Servers, die einen Zonentransfer anfordern dürfen. Da hier natürlich auch die sekundären DNS-Server eingepflegt werden müssen, die Sie bereits auf der Registerkarte *Namenserver* eingetragen haben, entsteht hier eine gewisse Redundanz und es besteht die Gefahr, dass IP-Adressen falsch eingetragen werden.

Der klassische Replikationsprozess sieht vor, dass ein sekundärer DNS-Server zunächst das Replikationsintervall aus dem SOA-Eintrag der Zone ausliest und dann in diesem Intervall den primären DNS-Server nach der aktuellen Versionsnummer der Zonendatenbank fragt. Diese Methode birgt allerdings zwei Risiken:

- Die Daten der sekundären DNS-Server sind nicht aktuell. Außerdem kann eine Funktion, mit der Bandbreite bei der Zonenübertragung gespart werden soll, der inkrementelle Zonentransfer, nur dann verwendet werden, wenn eine bestimmte Menge an neuen Einträgen nicht überschritten wird. Bei Überschreitung dieser Menge muss wieder ein Transfer der kompletten Zone erfolgen.
- Die sekundären DNS-Server fragen den primären DNS-Server zu häufig ab und erzeugen dabei unnötige Last auf dem Server sowie im Netzwerk, auch wenn es keine neuen Einträge gibt. Die Lösung ist eine Erweiterung vom bisher verwendeten Pull-Verfahren, bei dem der sekundäre Server vom primären Server aufgefordert wird, eine Überprüfung der Versionsnummer durchzuführen. Somit führen die sekundären Server nur dann eine Abfrage durch, wenn auch tatsächlich Änderungen an der Zone vorgenommen wurden. Dabei handelt es sich wieder um eine standardisierte Funktion, die auch andere DNS-Server verwenden können. Über die Schaltfläche *Benachrichtigungen* gelangen Sie zu der entsprechenden Konfigurationsseite.

Abbildg. 11.59 Konfigurieren der automatischen Benachrichtigung der sekundären DNS-Server durch den primären DNS-Server



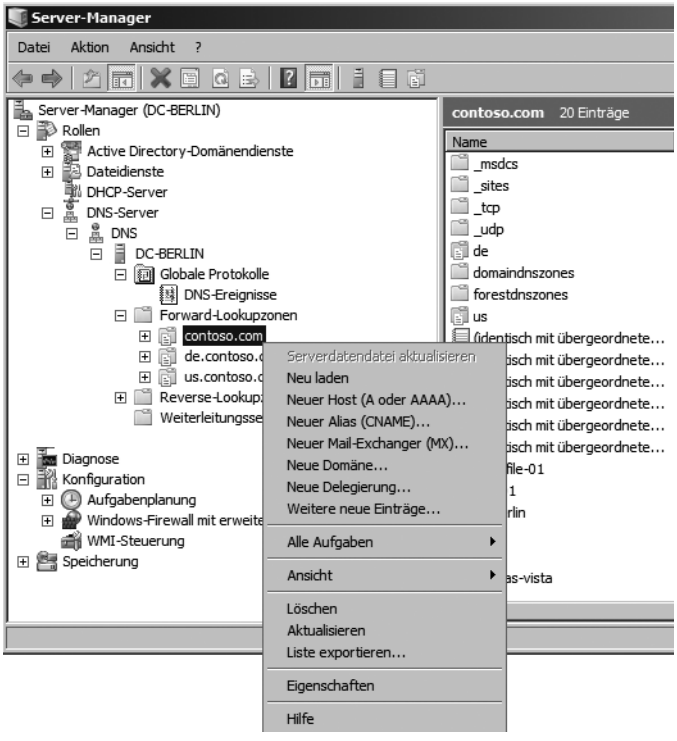
Da alle Microsoft-DNS-Server die Benachrichtigungen bereits unterstützen, ist das Kontrollkästchen *Automatisch benachrichtigen* in der Standardeinstellung bereits aktiviert und sollte nur für die Server abgeschaltet werden, bei denen es zu Kompatibilitätsproblemen kommt. Auch hier werden automatisch die Server benachrichtigt, die auf der Registerkarte für *Namenserver* aufgelistet sind. Alternativ können Sie auch hier wieder unter *Folgende Server* eine eigene Liste definieren.

Verwaltungsmöglichkeiten im Kontextmenü einer Zone

Wenn Sie mit der rechten Maustaste auf eine Zone klicken, stehen Ihnen verschiedene Möglichkeiten zur Verfügung, diese Zone zu verwalten:

- **Neu laden** Mit diesem Befehl können Sie die Einstellungen und die Ansicht der Zone im Snap-In neu laden lassen. Diesen Befehl benötigen Sie selten. Die Zone wird aus dem Active Directory noch mal in die Ansicht übertragen.
- **Neuer Host (A oder AAAA)** Mit diesem Befehl fügen Sie einen neuen statischen Eintrag in die DNS-Datenbank ein, wie weiter vorne beschrieben. Neu ist in Windows Server 2008 der AAAA-Eintrag. Dieser enthält eine IPv6-Adresse, ein Host A-Eintrag enthält eine IPv4-Adresse.
- **Neuer Alias (CNAME)** Dieser Menüpunkt dient zum Hinzufügen eines neuen Eintrags der Form »canonical name«. Dazu wird zu einem bereits vorhandenen Eintrag eines Servers ein weiterer Eintrag zu derselben IP-Adresse hinzugefügt. Dieser zusätzliche Eintrag wird auch Alias genannt. Wenn ein Client versucht diesen Alias aufzulösen, wird bei der Ausgabe des Namens parallel zum Alias auch der richtige Eintrag ausgegeben.
- **Neuer Mail-Exchanger (MX)** Mit dieser Option können Sie einen neuen SRV-Record mit der Bezeichnung *MX* erstellen. In einer normalen Umgebung werden Sie einen solchen MX-Record nicht benötigen. Er dient dazu, aus einer Zone den verantwortlichen SMTP-Server zu erfragen, zu dem E-Mails zugestellt werden sollen. Der MX-Record ermöglicht es, unter einer Domain mehrere Mailserver zu betreiben. Außerdem gibt er anderen Mailservern eine Priorisierung vor, in welcher Reihenfolge diese die Mailserver einer bestimmten Domain kontaktieren sollen. Internetprovider verwenden diese Priorisierung, um zu steuern, wohin E-Mails zuerst zugestellt werden sollen. Der MX10-Eintrag definiert, dass E-Mails vor der Zustellung zum MX20 zunächst zum Server zugestellt werden sollen, der als MX10 hinterlegt ist. Antwortet dieser Server nicht auf Anfragen, wird automatisch eine Zustellung zum MX20 versucht. Sie können auch einen MX30 definieren.
- **Neue Domäne** Mit diesem Eintrag erstellen Sie unterhalb dieser Zone eine neue Domäne. Diese Unterdomäne, zum Beispiel *sales.contoso.com,* wird von diesem DNS-Server und dieser Zone verwaltet, ohne dass zusätzliche Zonen angelegt werden müssen. Wenn Sie eine neue Unterdomäne eines Active Directory erstellen wollen, können Sie unterhalb der bereits erstellten Root-Domäne eine Unterdomäne erstellen, oder eine eigene Zone, die allerdings getrennt verwaltet werden muss.

Abbildg. 11.60 Verwaltungsmöglichkeiten einer DNS-Zone



- **Neue Delegierung** Mit diesem Menübefehl können Sie eine erstellte Zone an einen anderen DNS-Server delegieren. Zukünftig ist für diese Zone der DNS-Server zuständig, den Sie hier definiert haben. Die delegierte Zone wird im ursprünglichen DNS-Server als delegiert angezeigt. Wird dieser DNS-Server nach einem Eintrag aus einer delegierten Zone gefragt, weist er die Anfrage an den verantwortlichen DNS-Server weiter. Eine solche Delegation macht Sinn, wenn Sie eine Unterdomäne erstellten wollen, aber ein anderer DNS-Server in einer anderen Niederlassung für diese Zone zuständig sein soll. Wir kommen zu diesem Thema noch ausführlicher in diesem Kapitel.

HINWEIS Wird der erste Domänencontroller einer neuen untergeordneten Domäne erstellt, richtet der Assistent unter Windows Server 2008 automatisch eine Delegation auf dem übergeordneten DNS-Server ein.

- **Weitere neue Einträge** Zusätzlich zum MX-Record können Sie weitere Service-Records eintragen. Diese werden aber nur in Ausnahmefällen benötigt und nicht für den Betrieb von Active Directory.

Abbildg. 11.61 Erstellen von neuen Einträgen in der Zone

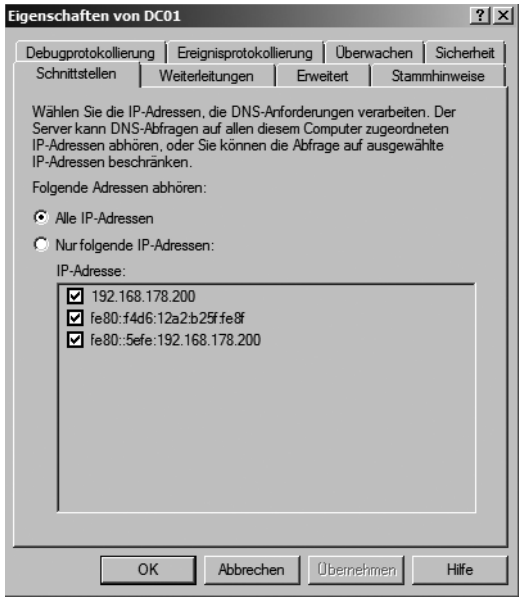
Verwalten der Eigenschaften eines DNS-Servers

Neben den Eigenschaften der einzelnen Zonen, die Sie über das Kontextmenü aufrufen können, stehen auch in den Eigenschaften des DNS-Servers selbst einige Möglichkeiten zur Konfiguration zur Verfügung. Wir gehen im folgenden Abschnitt ausführlicher auf die einzelnen Registerkarten in den Eigenschaften eines DNS-Servers ein.

Registerkarte *Schnittstellen*

Auf der Registerkarte *Schnittstellen* definieren Sie, auf welchen IP-Adressen der DNS-Server bei Anfragen reagiert. Dies ist zum Beispiel in solchen Fällen sinnvoll, in denen der DNS-Server mit mehreren Netzwerkkarten ausgestattet ist. Teilnetze, die zum Teil öffentlich zugänglich sind, können so von Anfragen an den Server ausgeschlossen werden, wodurch die Sicherheit des Systems erhöht wird. Wenn Sie die Standardeinstellung, in der der DNS-Server Anfragen auf allen IP-Adressen entgegennimmt, ändern wollen, ändern Sie die Konfiguration von *Alle IP-Adressen* auf *Nur folgende IP-Adressen* und wählen anschließend im Feld *IP-Adresse* jeweils eine gewünschte Adresse an.

Abbildg. 11.62 Auswählen der Netzwerkschnittstellen eines DNS-Servers

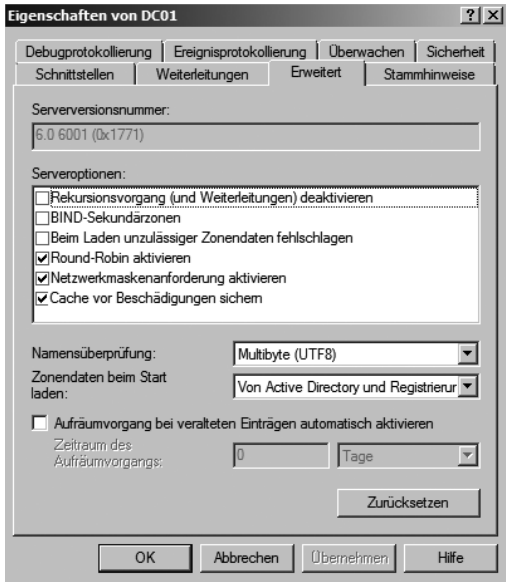


Registerkarte *Erweitert*

Über die Registerkarte *Erweitert* können einige Serveroptionen konfiguriert werden:

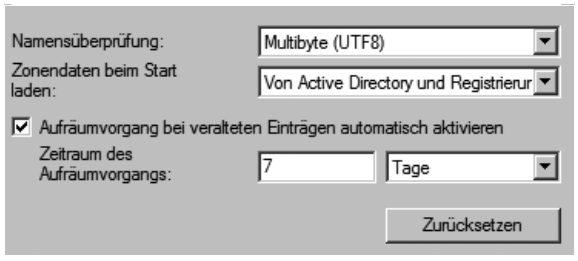
- **Rekursionsvorgang (und Weiterleitungen) deaktivieren** Unabhängig von den Weiterleitungen (siehe nächsten Abschnitt) können Sie den DNS-Server auch lokal isolieren, indem Sie dieses Kontrollkästchen aktivieren. Damit greift der DNS-Server nur noch auf seine eigene Datenbank zu, es werden keine Anfragen mehr an weitere DNS-Server weitergeleitet.
- **BIND-Sekundärzonen** Mit der Aktivierung dieses Kontrollkästchens können Sie die Kompatibilität des Servers zum System herstellen, deren Funktionsumfang nicht bis zu BIND 4.9.4 heranreicht. Dazu wird die Komprimierung der Daten beim Zonentransfer ausgeschaltet. Aus Performancegründen ist diese Funktion standardmäßig deaktiviert, die schnelle Übermittlung damit also aktiviert.
- **Beim Laden unzulässiger Zonendaten fehlschlagen** Der DNS-Server liest in der Standardeinstellung alle Zonendaten komplett ein und protokolliert fehlerhafte Einträge lediglich im Ereignisprotokoll. Damit kann der DNS-Server allerdings auch Hostnamen in seine Datenbanken aufnehmen, die nicht den offiziellen Spezifikationen aus den RFCs entsprechen, was wiederum bedeutet, dass es Systeme geben kann, die mit diesen Namen nicht arbeiten können. Sobald dieses Kontrollkästchen aktiviert ist, wird das Laden der kompletten Zone abgebrochen. Wie strikt die Überprüfung erfolgt, stellen Sie über die Option *Namensüberprüfung* ein. Dabei gibt es folgende Stufen:
  - **Ausschließlich RFC (ANSI)** Nur Namen, die der offiziellen Spezifikation entsprechen
  - **Kein RFC (ANSI)** Alle Namen, die sich aus dem ANSI-Zeichensatz zusammensetzen
  - **Multibyte (UTF8)** Alle Namen, deren Zeichen über das Unicode Transformation Format (UTF-8) abgebildet werden können (zum Beispiel arabische oder asiatische Zeichensätze)
  - **Alle Namen** Keine Einschränkung der verwendeten Zeichen

Abbildg. 11.63 Erweiterte DNS-Einstellungen für DNS-Server



- **Round-Robin aktivieren** Die einfachste Form der Lastverteilung auf mehrere Computer wird als *DNS-Round-Robin* bezeichnet. Dabei wird ein Hostname mehrfach mit jeweils einer anderen IP-Adresse eingetragen. Erreicht den DNS-Server eine Anfrage des Clients, liefert er die Liste aller gefundenen IP-Adressen zurück, wobei er die Reihenfolge der Einträge jeweils um den Wert 1 verschiebt. Damit wird im Mittel jeder Eintrag gleich häufig an erster Stelle dem Client zurückgeliefert. Diese Funktion muss zum Beispiel dann deaktiviert werden, wenn Sie zwar mehrere Server unter demselben Namen nutzen wollen, die weiteren Systeme aber leistungsschwächer oder weiter entfernt sind und nur zur Ausfallsicherheit dienen sollen. Wenn Sie die Funktion lediglich für bestimmte Typen deaktivieren möchten, so kann dies nur über die Registry erfolgen. Fügen Sie dazu unter *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters* einen REG_SZ-Wert mit dem Namen *DoNotRoundRobinTypes* hinzu und tragen Sie als Werte die Recordtypen ein, zum Beispiel *a ns srv*.
- **Netzwerkmaskenanforderung aktivieren** Um dem Client möglichst einen Server direkt in seiner Nähe zu nennen – im TCP/IP bedeutet das innerhalb desselben IP-Subnetzes – wird bei Hostnamen mit mehreren zugeordneten IP-Adressen vor der Umsortierung durch Round-Robin zunächst ermittelt, ob es einen Eintrag gibt, der dem Subnetz des Clients zuzuordnen ist. Dieser wird anschließend an die erste Stelle der zurückgegebenen Liste gesetzt. Nur wenn kein passender eindeutiger Eintrag gefunden wird, kommt Round-Robin zur Lastverteilung zum Einsatz.
- **Cache vor Beschädigungen sichern** Diese Option ist von ihrer Bezeichnung her etwas irreführend, da es sich hier eher um einen Schutz vor zweifelhaften Einträgen im Cache handelt, die im Original als *Pollution (Verschmutzung)* bezeichnet werden. Dies sind Einträge, die nicht aus erster Hand gewonnen, sondern durch Weiterleitungen von anderen DNS-Servern ermittelt wurden. Hierbei besteht natürlich eine gewisse Gefahr, dass es sich dabei um gefälschte Einträge handelt. Daher werden diese Ergebnisse zwar an den Client weitergeleitet, aber nicht in den Cache eingetragen. Wenn Sie diese Funktion deaktivieren, nimmt der DNS-Server alle Anfragen in seinen Cache auf, wodurch sich die Systemgeschwindigkeit etwas erhöhen kann.

Abbildg. 11.64 Konfigurieren der Namensüberprüfungen, Zonendaten und des Aufräumvorgangs in den erweiterten Einstellungen



Zonendaten beim Start des DNS-Servers einlesen

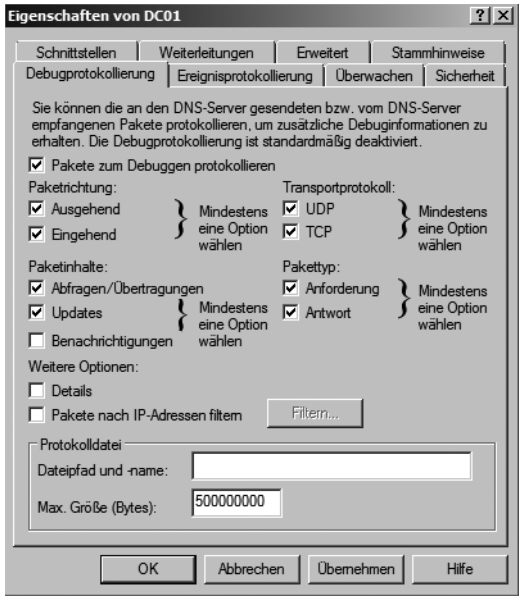
Welche Zonendaten der DNS-Server bei seinem Start einliest, erfährt er in der Regel aus dem Active Directory und der Registry. Wenn kein Active Directory verwendet wird, können Sie die Einstellung auch auf *Von der Registrierung* ändern. Die letzte Option *Von Datei* ist dann sinnvoll, wenn Sie eine Übernahme der Funktion von einem BIND-Server vorgenommen haben, der seine Konfiguration ebenfalls aus einer Konfigurationsdatei (*named.boot*) bezieht. Die Datei *boot* muss im Verzeichnis *%Windir%\Sytem32\Dns* abgelegt sein. Nachdem Sie das Kontrollkästchen *Aufräumvorgang bei veralteten Einträgen automatisch aktivieren* aktiviert haben, geben Sie den Zeitraum des Aufräumvorgangs an, der angibt, nach welcher Zeit ein dynamisch (also manuell nicht vom Administrator) erstellter DNS-Eintrag als veraltet betrachtet und aus der Datenbank entfernt wird. Über die Schaltfläche *Zurücksetzen* können Sie die Standardeinstellung bei Bedarf wiederherstellen.

Registerkarte *Debugprotokollierung*

Damit die Fehlersuche bei der Namensauflösung vereinfacht werden kann, ist es möglich, die komplette Kommunikation des DNS-Servers mit Clients und anderen Servern in einer Textdatei zu protokollieren. Wenn Sie den Dateipfad und -namen auf der Registerkarte *Debugprotokollierung* nicht angeben, wird die Datei als *%Windir%\System32\Dns\Dns.log* abgespeichert. Um zu vermeiden, dass diese Datei die komplette Festplatte füllt, ist immer eine maximale Größe anzugeben. Sobald dieses Limit erreicht ist, werden die ältesten Einträge überschrieben. Nachdem Sie die Protokollierung durch Aktivierung des Kontrollkästchens *Pakete zum Debuggen protokollieren* eingeschaltet haben, können Sie noch genauer angeben, welche Daten überhaupt in die Datei aufgenommen werden, damit Sie bei geringerer Datenmenge schneller suchen können:

- **Paketrichtung** Mit dieser Einstellung legen Sie fest, ob Sie Pakete protokollieren, die vom DNS-Server stammen (*Ausgehend*) oder an den DNS-Server gerichtet sind (*Eingehend*).
- **Transportprotokoll** DNS-Daten können über die beiden IP-Protokolle TCP und UDP übertragen werden. Die Protokollierung eines der Protokolle zu deaktivieren, ist dort nützlich, wo Sie Kommunikationsprobleme aufgrund von Paketfiltern vermuten. So können Sie leicht vergleichen, welche Pakete auf beiden Seiten gesendet bzw. empfangen wurden und anhand der Differenz feststellen, dass unter Umständen zum Beispiel eine Firewall nicht korrekt konfiguriert ist.

Abbildg. 11.65 Konfigurieren der Debugprotokollierung

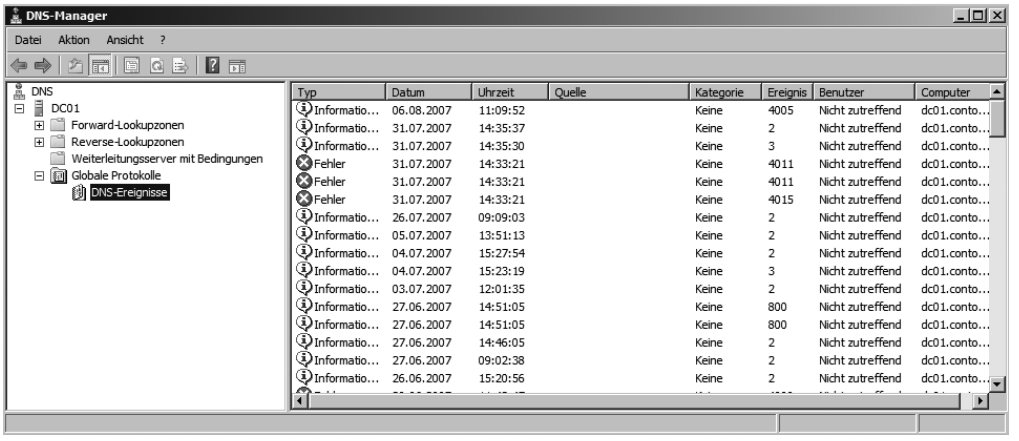


- **Paketinhalte** Die übertragenen Daten sind generell in drei Gruppen unterteilt. Unter *Abfragen/Übertragungen* finden Sie alle DNS-Anfragen sowie die zugehörigen Antworten und die Daten für die Replikation von DNS-Servern. *Updates* steht für die Pakete, die bei der dynamischen Registrierung von Hosts beim DNS-Server gesendet werden und *Benachrichtigungen* für die Pakete, mit denen ein DNS-Server einem anderen signalisiert, dass Änderungen an seiner Datenbank vorgenommen wurden, die der andere replizieren muss.
- **Pakettyp** Nachdem Sie den Paketinhalt bereits eingeschränkt haben, legen Sie hier nun noch die Richtung fest, aus der die Übertragung gestartet wurde, wobei Anforderung für Anfragen vom Client oder Server stehen. Bei den Einstellungen für Paketrichtung, Paketinhalt, Pakettyp und Transportprotokoll müssen Sie jeweils mindestens eine Option aktivieren.
- **Weitere Optionen** Um die Datenmenge zu beschränken, wird nicht der komplette Paketinhalt protokolliert, sondern nur die wichtigsten Daten. Falls Sie alle verfügbaren Informationen aufnehmen wollen, aktivieren Sie das Kontrollkästchen *Details*. Wenn Sie die Daten der Kommunikation mit einem bestimmten Computer aufnehmen wollen, können Sie auch Pakete nach IP-Adressen filtern. Hier ist aber nur die Angabe einzelner Adressen möglich, die Filterung für ganze Netzwerke über die Eingabe einer Subnetzmaske ist leider nicht möglich.

Registerkarte *Ereignisprotokollierung*

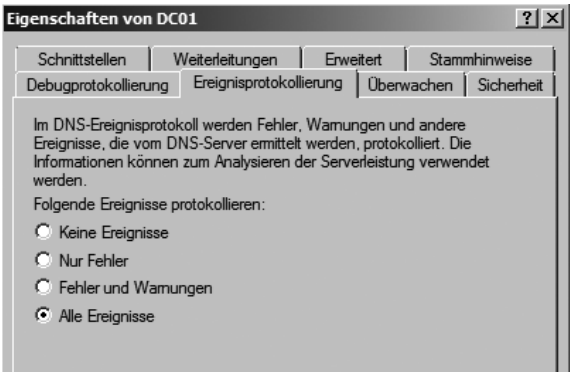
Wie Sie in der Standardanzeige der Verwaltungskonsole bereits sehen, verfügt der DNS-Server über einen eigenen Abschnitt im Ereignisprotokoll (Abbildung 11.66).

Abbildg. 11.66 Überprüfen der DNS-Ereignisse in der DNS-Verwaltung



Über die Registerkarte *Ereignisprotokollierung* definieren Sie, welche Ereignisse tatsächlich in dieses Protokoll geschrieben werden (Abbildung 11.67).

Abbildg. 11.67 Welche Ereignisse in der Ereignisanzeige protokolliert werden, kann in den Eigenschaften eines DNS-Servers festgelegt werden



Wählen Sie unter *Folgende Ereignisse protokollieren* die gewünschte Option.

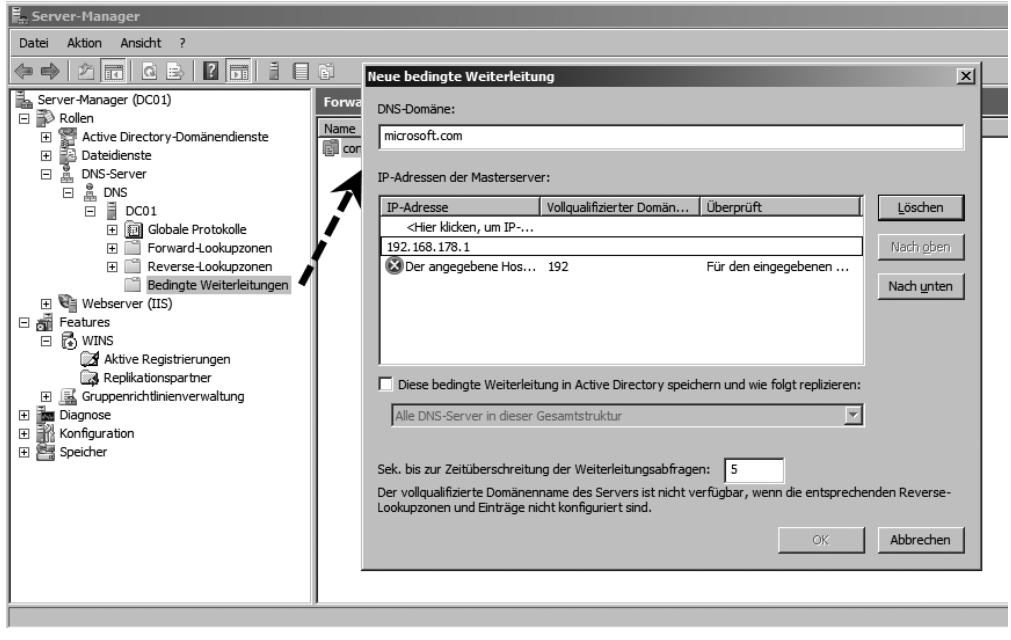
- **Keine Ereignisse** Es erfolgt keine Protokollierung der Ereignisse. Dadurch sparen Sie zwar etwas Speicherplatz und Rechenzeit, haben dafür aber überhaupt keine Möglichkeit zur Fehlersuche, weshalb diese Einstellung nicht zu empfehlen ist.
- **Nur Fehler** Auf dieser Stufe werden zumindest Fehler protokolliert. Dies können Probleme beim Start des Dienstes, beim Laden der Datenbanken oder der Übernahme von Einträgen sein. Eine vollständige Fehlersuche ist jedoch auch hier noch nicht möglich.
- **Fehler und Warnungen** Diese Einstellung erlaubt die Anzeige aller Fehler und Warnungen, die beim Start und Betrieb des DNS-Servers auftreten können. Damit haben Sie die komplette Datenmenge zusammen, die in den meisten Fällen für das Troubleshooting ausreicht.

- **Alle Ereignisse** In einigen Fällen ist eine Fehlersuche nur dann möglich, wenn Sie auch sehen, welche Operationen erfolgreich ausgeführt wurden. Dies ist auch die Standardeinstellung für die Protokollierung. Allerdings laufen Sie hier auch Gefahr, dass Sie in der Menge der Informationen die Warnungen oder Fehler übersehen. Ferner können je nach Konfiguration der Ereignisanzeige durch zu viele Einträge auch Informationen verloren gehen.

DNS-Weiterleitungen

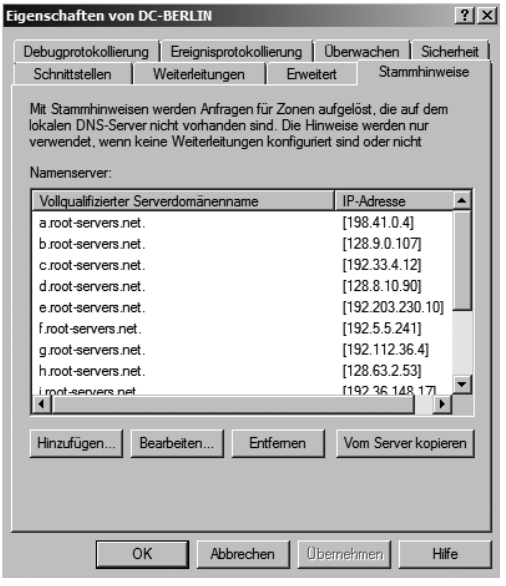
Ihr DNS-Server kann nur Anfragen der Clients beantworten, für die Zonen hinterlegt wurden. Wenn Sie auch andere Zonen auflösen wollen, müssen Sie im DNS konfigurieren, welche Server gefragt werden sollen. Der DNS-Server überprüft zunächst, ob er für die Domäne zuständig ist. Wenn er keine Zone finden kann, und auch keine Delegation, werden die DNS-Server gefragt, die über den Eintrag *Bedingte Weiterleitungen* in der Konsolenstruktur hinterlegt sind (Abbildung 11.68). Bei Windows Server 2008 kann konfiguriert werden, dass der Server generell alle Anfragen an bestimmte Server weiterleiten soll oder nur bestimmte Domänen zu bestimmten DNS-Servern.

Abbildg. 11.68 Festlegen von Weiterleitungsservern, zu denen ein DNS-Server Einträge weiterleiten kann



Wenn keine Weiterleitungen konfiguriert sind, werden automatisch die DNS-Server befragt, die auf der Registerkarte *Stammhinweise* in den Eigenschaften des DNS-Servers hinterlegt sind. Wenn diese Server nicht erreicht werden, erhält der fragende Client eine Fehlermeldung zurück.

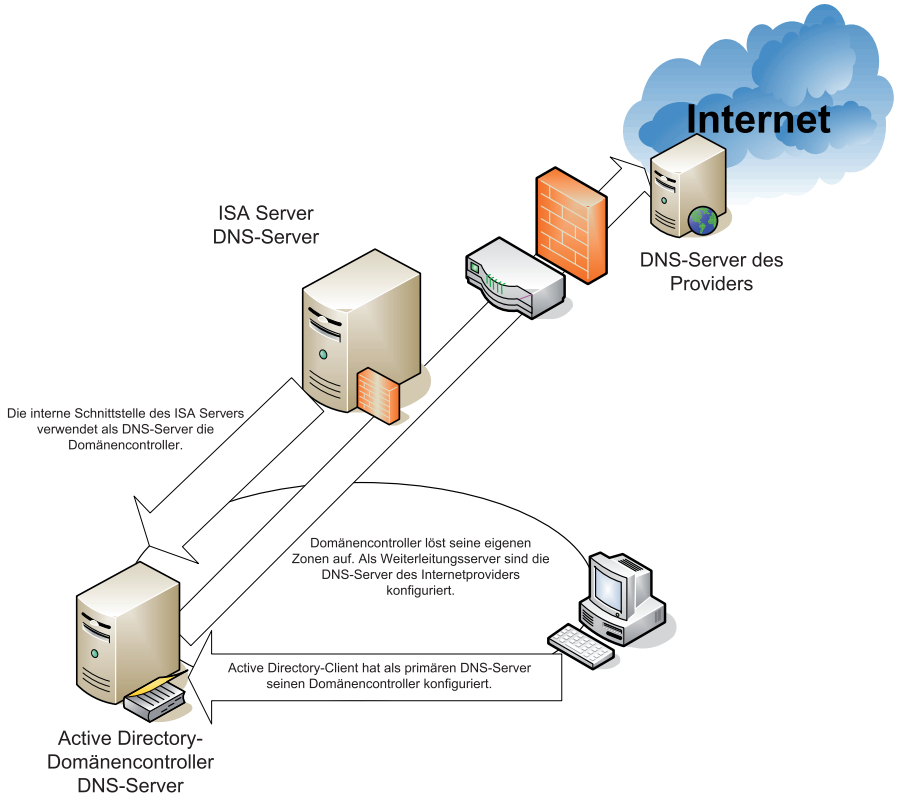
Abbildg. 11.69 Registerkarte *Stammhinweise* in den Eigenschaften eines DNS-Servers



Damit die Benutzer und Server Verbindung ins Internet aufbauen können, müssen Sie dafür sorgen, dass die Domänen-Namen im Internet aufgelöst werden können. Auch zu diesem Zweck wird DNS eingesetzt. Die DNS-Server von Active Directory können nicht nur die internen Zonen auflösen, sondern können auch als Weiterleitungsserver die DNS-Server Ihres Providers verwenden oder alternativ die Stammhinweise, also die Root-DNS-Server des Internets. Dadurch ist sichergestellt, dass die DNS-Server des Unternehmens zuverlässig interne und externe DNS-Namen auflösen können. Setzen Sie zum Beispiel einen ISA-Server oder einen anderen Proxy für die Internetanbindung ein, können Sie diesen auch als Server für die Namensauflösung verwenden. Die interne Netzwerkkarte des ISA-Servers verwendet als DNS-Server die Domänencontroller von Active Directory. Durch diese empfohlene Vorgehensweise, die Sie in Abbildung 11.70 sehen, ist immer sichergestellt, dass die Namen der Internetseiten aufgelöst werden können. In den Eigenschaften der PCs und Mitgliedsserver der Domäne, auch auf dem ISA-Server, stehen die DNS-Server von Active Directory, also die Domänencontroller. Dadurch ist sichergestellt, dass auch der ISA-Server interne DNS-Namen auflösen kann.

Die Active Directory-DCs fragen die DNS-Server Ihres Internetproviders nach DNS-Zonen, für die sie nicht selbst zuständig sind oder verwendet automatisch die Stammhinweise, wenn keine Weiterleitungsserver konfiguriert wurden. Damit die Domänencontroller die DNS-Namen bei den DNS-Servern im Internet abfragen können, müssen natürlich auf dem ISA-Server entsprechende Regeln definiert werden. Sie sollten auf den DNS-Servern als Weiterleitungsserver nicht nur einen externen DNS-Server verwenden, sondern am besten mehrere oder gleich die Stammhinweise verwenden. Dadurch ist sichergestellt, dass der Internetverkehr auch noch funktioniert, wenn ein DNS-Server des Providers nicht mehr zur Verfügung stehen sollte. Sie müssen für die Namensauflösung natürlich nicht diesen Weg wählen, sondern können für die Auflösung von DNS-Namen im Internet auf dem ISA-Server einen DNS-Server konfigurieren, der wiederum die DNS-Server im Internet als Weiterleitungsserver verwendet. Die Möglichkeit, die DNS-Server von Active Directory zu verwenden, ist aber nach unserer Erfahrung vor allem für mittelständische Unternehmen die beste.

Abbildg. 11.70 Optimaler Aufbau einer DNS-Infrastruktur für das Internet



Komplexere DNS-Struktur für verzweigte Active Directory-Domänen erstellen

Vor allem wenn ein Active Directory aus mehreren Domänen aufgebaut ist, wird die DNS-Struktur etwas komplizierter. Auf den folgenden Seiten gehen wir ausführlicher auf die mögliche Aufteilung von DNS-Zonen und -Domänen ein. Im nächsten Abschnitt wird die Erweiterung von Active Directory um weitere Domänen und Strukturen sowie die damit verbundene komplexere Verwaltung von DNS besprochen.

Erstellen einer neuen untergeordneten Domäne

Eine sehr häufige Aufgabe ist in einer Active Directory-Gesamtstruktur die Erstellung einer untergeordneten Domäne. Wenn Sie eine Active Directory-Gesamtstruktur durch die Erstellung der ersten Domäne, also dem Heraufstufen des ersten Domänencontrollers, definieren, ist diese Domäne die Root-Domäne der Gesamtstruktur. Viele Unternehmen binden an diese Domäne weitere Domänen, die als untergeordnete Domänen bezeichnet werden. Ein Beispiel hierfür ist die Domäne *contoso.com* als erste Domäne in einer Active Directory-Gesamtstruktur. Sie können an diese Domäne

beliebig weitere untergeordnete Domänen anbinden, zum Beispiel die Domäne *de.contoso.com*. Die beiden Domänen agieren vollkommen unabhängig voneinander, teilen sich aber den gleichen Namensraum. Bei der Erstellung der Domäne wird automatisch eine Vertrauensstellung zwischen *contoso.com* und *de.contoso.com* eingerichtet. Auf diese Weise werden in vielen Gesamtstrukturen Niederlassungen angebunden, die eine eigene IT-Abteilung haben. In der Zentrale des Unternehmens wird eine Root-Domäne (oft auch als Stammdomäne bezeichnet) erstellt und die einzelnen Niederlassungen werden als untergeordnete Domänen angebunden. Auch wenn die Root-Domäne nicht erreichbar ist, können alle Anwender in den untergeordneten Domänen problemlos weiterarbeiten. Eine dauerhafte Verbindung ist nicht zwingend notwendig.

Anpassen der DNS-Infrastruktur an untergeordnete Domänen

Bei der Erstellung von untergeordneten Domänen werden durch die enge Verzahnung von Active Directory und DNS auch die Anforderungen an die DNS-Infrastruktur komplizierter. Bevor Sie eine neue untergeordnete Domäne erstellen können, müssen Sie zunächst die passende DNS-Infrastruktur dafür erstellen. Wenn Sie untergeordnete Domänen erstellen, haben Sie für die Namensauflösung grundsätzlich zwei Möglichkeiten:

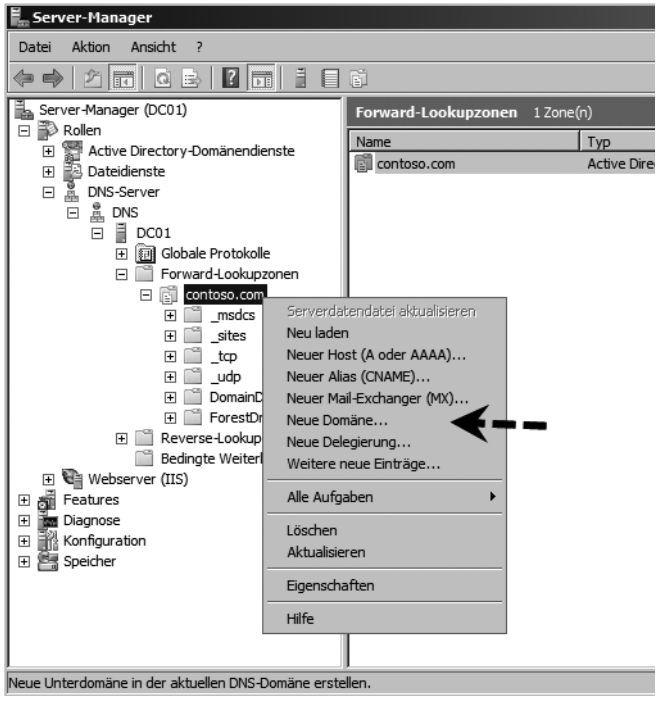
1. Die DNS-Server der Root-Domäne verwalten auch die DNS-Domänen der untergeordneten Domänen.
2. Die untergeordneten Domänen verwalten jeweils ihre eigene DNS-Domäne.

Erstellen Sie eine neue untergeordnete Domäne, sollten Sie zunächst genau planen, wie die DNS-Infrastruktur dafür erstellt wird. Wenn die DNS-Server der Root-Domäne auch für die Namensauflösung in der untergeordneten Domäne zuständig sind, sollten Sie die Replikationseinstellungen für die Zone so ändern, dass sie auf alle DNS-Server und Domänencontroller repliziert wird. Da untergeordnete Domänen oft auch physisch durch eine WAN-Leitung von der Root-Domäne getrennt sind, besteht die Notwendigkeit die DNS-Daten der untergeordneten Domäne in die Niederlassung zu replizieren. In diesem Fall müssen jedoch ganz genaue Berechtigungskonzepte erstellt werden, da ansonsten Administratoren der untergeordneten Domäne Änderungen an der DNS-Infrastruktur der übergeordneten Domäne durchführen können. In vielen Unternehmen wird dieses Sicherheitsproblem dadurch gelöst, dass die untergeordnete Domäne als eigenständige Zone ausschließlich von den Administratoren der untergeordneten Domäne verwaltet wird. Dadurch ist sichergestellt, dass jede Domäne ihre eigene DNS-Zone verwaltet, damit die Administratoren der einzelnen untergeordneten Domänen sich nicht gegenseitig beeinträchtigen können. Wir zeigen Ihnen im Anschluss die Erstellung beider Varianten. Anhand dieser Fakten können Sie dann selbst entscheiden, welche Möglichkeiten Sie für die einzelnen untergeordneten Domänen einsetzen.

Erstellen einer DNS-Domäne für eine neue untergeordnete Domäne

Die erste Möglichkeit der Namensauflösung ist die Erstellung einer neuen DNS-Domäne unterhalb der Root-Domäne auf den Root-Domänencontrollern. Diese Domäne befindet sich auf dem DNS-Server in der gleichen Zone wie die DNS-Domäne der Root-Domäne. Um eine neue Domäne unterhalb einer DNS-Domäne zu erstellen, müssen Sie zunächst das Snap-In zur Verwaltung von DNS starten. Klicken Sie dann mit der rechten Maustaste auf die Zone, unter der Sie die neue DNS-Domäne erstellen wollen. Wählen Sie im Kontextmenü den Befehl *Neue Domäne* aus. Im nächsten Fenster müssen Sie die Bezeichnung der neuen Domäne eingeben.

Abbildg. 11.71 Erstellen von neuen untergeordneten Domänen

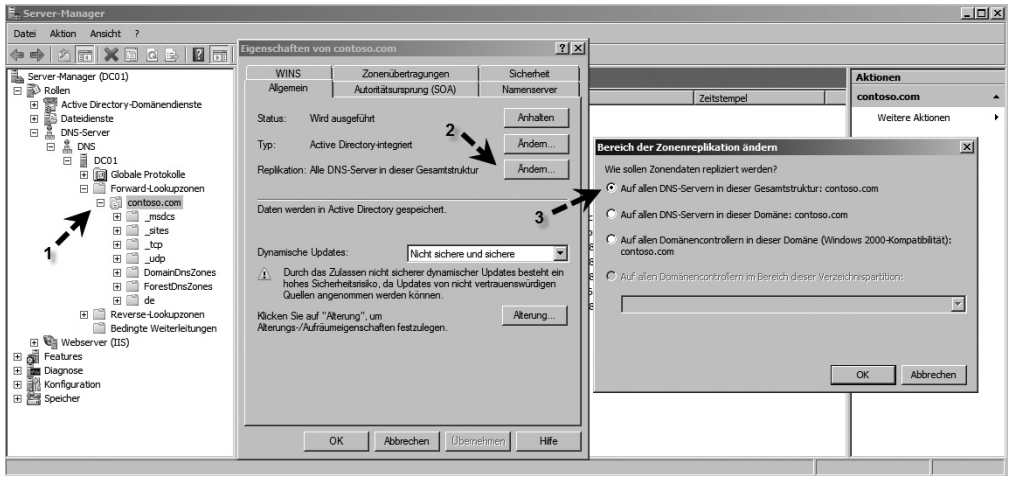


Da die neue Domäne unterhalb einer bereits existierenden DNS-Domäne angelegt wird, müssen Sie nur die Bezeichnung der Domäne ohne die Endung der Root-Domäne angeben. In diesem Beispiel lautet die Bezeichnung *de* unterhalb der Zone *contoso.com*. Nachdem Sie die Erstellung bestätigt haben, wird die neue Domäne unterhalb der Zone angezeigt (Abbildung 11.72). Sie müssen keinerlei zusätzliche Angaben machen, da die Einstellungen für die Replikation der dynamischen Updates und Berechtigungen durch die übergeordnete Zone an die untergeordnete Domäne weitergegeben werden.

Abbildg. 11.72 Neue untergeordnete Domänen können schnell angelegt werden

Damit Sie auf dem Domänencontroller der untergeordneten Domäne das Active Directory installieren können, müssen Sie in den IP-Einstellungen des neuen Domänencontrollers einen DNS-Server der übergeordneten Domäne als bevorzugt eintragen. Zum Erstellen einer untergeordneten Domäne ist eine Kontaktaufnahme zu der übergeordneten Domäne notwendig. Dieser Kontakt wird über DNS hergestellt und kann nur zustande kommen, wenn der neue Domänencontroller eine Verbindung aufbauen kann und die Namen der Domänencontroller der Root-Domäne kennt. Nach der Heraufstufung des neuen Domänencontrollers der untergeordneten Domäne sollten Sie auf diesem zunächst die DNS-Erweiterung installieren, damit er die DNS-Daten seiner Zone empfangen kann. Zusätzlich müssen Sie in den Eigenschaften der DNS-Zone die Replikation so anpassen, dass die DNS-Daten nicht nur auf die DNS-Server der gleichen Domäne repliziert werden, sondern auf alle DNS-Server der Gesamtstruktur (Abbildung 11.73). Da die DNS-Server der neuen untergeordneten Domäne nicht zur gleichen Domäne gehören, ist diese Maßnahme notwendig. Nachdem die DNS-Daten auf den untergeordneten Domänencontrollern angezeigt werden, können Sie in den IP-Einstellungen der Server die DNS-Server der untergeordneten Domäne als bevorzugte und die der übergeordneten Domäne als alternative DNS-Server konfigurieren. Dadurch ist sichergestellt, dass die Namensauflösung funktioniert, auch wenn unter Umständen die DNS-Server der untergeordneten Domäne nicht zur Verfügung stehen. Da diese Aufgabe erst durchgeführt werden kann, wenn das Active Directory auf den neuen Domänencontrollern installiert wurde, müssen Sie zunächst die Heraufstufung der untergeordneten Domänencontroller vornehmen.

Abbildg. 11.73 Festlegen der Konfiguration für DNS-Zonen



Delegierung von DNS-Zonen

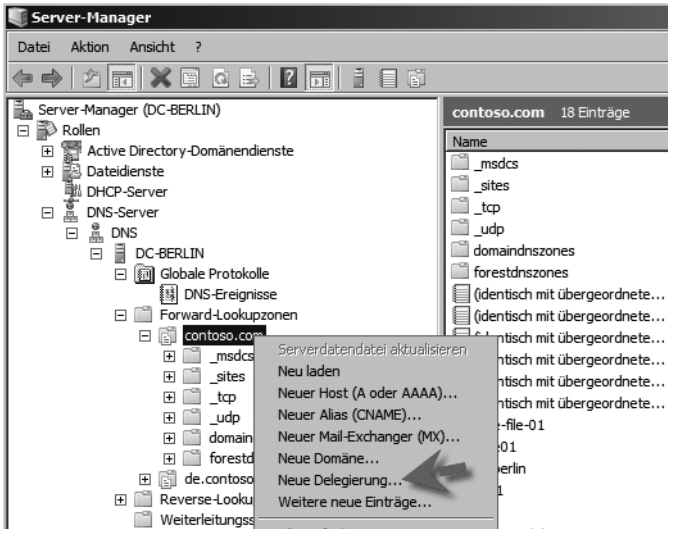
Die zweite Variante der Namensauflösung einer neuen untergeordneten Domäne ist die so genannte *Delegierung*. Installieren Sie zunächst auf dem neuen Domänencontroller die DNS-Erweiterung. Nachdem die DNS-Erweiterung installiert wurde, erstellen Sie auf dem neuen DNS-Server eine neue Zone. Die neue Zone erhält dieselbe Bezeichnung wie die neue untergeordnete Domäne. In diesem Beispiel wird der Domänencontroller *dc-berlin* der erste Domänencontroller der untergeordneten Domäne *de.contoso.com* unterhalb der Domäne *contoso.com*. Gehen Sie dazu folgendermaßen vor:

1. Legen Sie zunächst den Computernamen fest. Auch das primäre DNS-Suffix des neuen Domänencontrollers kann an dieser Stelle bereits eingegeben werden. Der Computername ist in diesem Beispiel *dc-berlin*, das primäre DNS-Suffix *de.contoso.com*.
2. Konfigurieren Sie in den IP-Einstellungen des Domänencontrollers seine eigene IP-Adresse als bevorzugten DNS-Server.
3. Erstellen Sie in der DNS-Verwaltung eine neue Zone mit der Bezeichnung der neuen untergeordneten Domäne, in diesem Beispiel *de.contoso.com*. Gehen Sie bei der Erstellung so vor, wie bereits in Kapitel 8 beschrieben. An dieser Stelle spielt die bereits vorhandene DNS-Domäne der Root-Domäne noch keinerlei Rolle. Achten Sie auf die dynamischen Updates der Zone.

Abbildg. 11.74 Erstellen einer neuen DNS-Zone für eine neue untergeordnete Domäne

4. Nachdem die Zone erstellt wurde, wird sie in der DNS-Verwaltung wie die DNS-Zone der Root-Domäne auf den Root-Domänencontrollern angezeigt.
5. Im nächsten Schritt müssen Sie dafür sorgen, dass sich beide DNS-Server gegenseitig auflösen können. Es muss in der untergeordneten Domäne möglich sein, Servernamen der übergeordneten Domäne aufzulösen, und in der übergeordneten Domäne muss es möglich sein, Servernamen der untergeordneten Domäne per DNS aufzulösen. Dazu wird die DNS-Zone der Root-Domäne so konfiguriert, dass alle Abfragen an die untergeordnete Domäne an deren Domänencontroller weitergeleitet werden. Die DNS-Server der übergeordneten Domäne kümmern sich fortan nicht mehr um die Verwaltung der untergeordneten Domäne, sondern haben diese Aufgabe an die Domänencontroller der untergeordneten Domäne delegiert. Für diesen Vorgang müssen Sie die *Delegierung* zunächst auf den DNS-Servern der übergeordneten Domäne einrichten. Klicken Sie dazu mit der rechten Maustaste auf die DNS-Zone der übergeordneten Domäne und wählen Sie aus dem Menü *Neue Delegierung*.

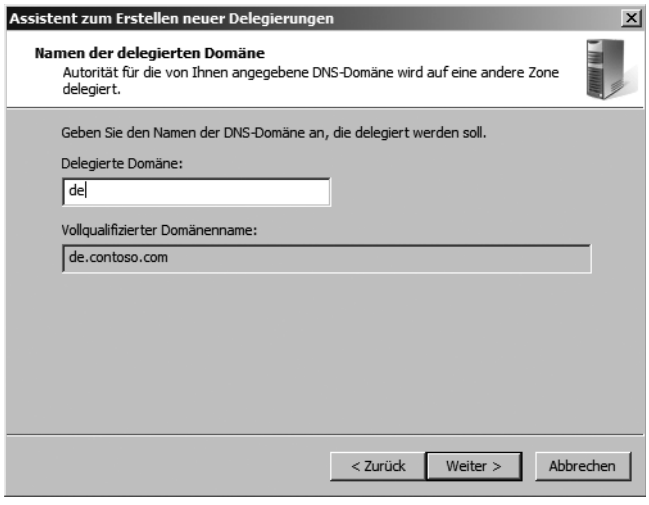
Abbildg. 11.75 Erstellen einer neuen Delegierung innerhalb der übergeordneten Domäne



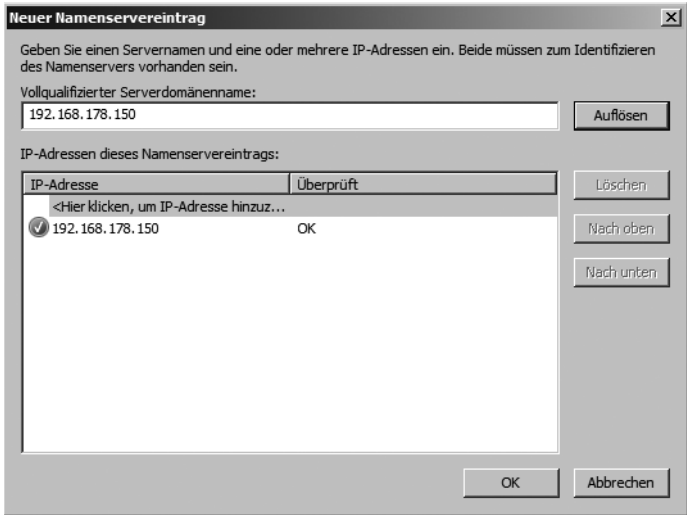
Es erscheint das Startfenster des Delegierungs-Assistenten. Im nächsten Fenster tragen Sie den Namen der neuen delegierten Domäne ein (Abbildung 11.76). Auch hier müssen Sie nur den Namen der untergeordneten Domäne eintragen, in diesem Beispiel *de*. Der Assistent vervollständigt automatisch den Namen zum FQDN. Dieser Vorgang ist vollkommen unabhängig von der Erstellung der neuen Zone in der untergeordneten Domäne. Die Namensauflösung von der übergeordneten Domäne zu Servern der untergeordneten Domäne funktioniert allerdings erst dann, wenn die Zone in der untergeordneten Domäne erstellt wurde und die Delegierung in der übergeordneten Domäne eingerichtet wurde. Wenn ein Client oder ein Server einen DNS-Server der übergeordneten Domäne als bevorzugten DNS-Server eingetragen hat und einen Namen der untergeordneten Domäne auflösen will (zum Beispiel ein zweiter Domänencontroller für die Replikation von Active Directoryvon Active Directory), kann nach der erfolgreichen Einrichtung der Delegierung der übergeordnete DNS-Server die Anfrage an den untergeordneten DNS-Server weiterleiten, der die Antwort an den übergeordneten DNS-Server weitergibt. Dieser DNS-Server gibt die entsprechende Antwort an den Client zurück.

6. Auf der nächsten Seite des Assistenten müssen Sie den Namensserver angeben, der für die Auflösung der delegierten Domäne zuständig ist. Da an dieser Stelle die Namensauflösung noch nicht funktioniert, weil Sie diese gerade erst konfigurieren, müssen Sie die einzelnen Eingaben manuell durchführen. Zunächst müssen Sie auf die Schaltfläche *Hinzufügen* klicken. Tragen Sie dann im Bereich *Vollqualifizierter Serverdomänenname* den Namen des Servers ein. Die Auflösung oder das Durchsuchen der Zone funktioniert an dieser Stelle noch nicht. Geben Sie danach im Bereich *IP-Adresse* die IP-Adresse des oben eingetragenen DNS-Servers der untergeordneten Domäne ein und klicken auf *OK*. Nach dieser Aktion wird dieser DNS-Server als Namensserver für die Delegierung verwendet. Sie können später noch Änderungen vornehmen oder weitere Server hinzufügen, wenn zum Beispiel in der untergeordneten Domäne ein weiterer Domänencontroller hinzugefügt wird. Durch das Eintragen von zwei Servern in der delegierten Domäne erhalten Sie eine Ausfallsicherheit bei der Namensauflösung von der übergeordneten zur untergeordneten Domäne.

Abbildg. 11.76 Konfigurieren der delegierten Domäne

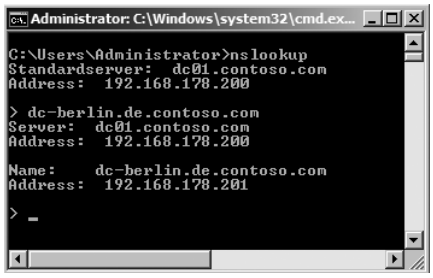


Abbildg. 11.77 Eintragen eines DNS-Servers, an den die Auflösung einer Domäne delegiert wird



7. Im Anschluss daran wird die delegierte Domäne grau in der DNS-Domäne angezeigt.
8. Überprüfen Sie jetzt mit *nslookup*, ob die Auflösung fehlerfrei funktioniert. Gehen Sie dazu in die Befehlszeile und geben Sie auf dem DNS-Server der Root-Domäne (oder einem Client, der diesen als bevorzugten DNS-Server konfiguriert hat) *nslookup* ein. Überprüfen Sie den FQDN des DNS-Servers der untergeordneten Domäne, in diesem Beispiel also *dc-berlin.de.contoso.com* (Abbildung 11.78). Die IP-Adresse des Servers muss fehlerfrei zurückgegeben werden.

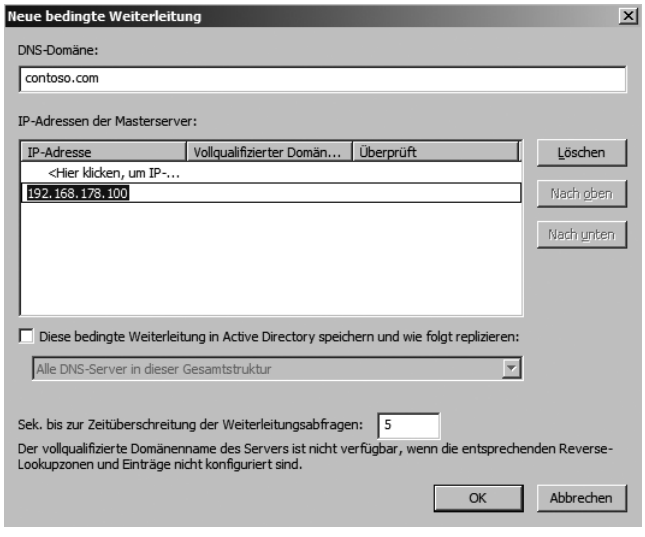
Abbildg. 11.78 Überprüfen der Namensauflösung von der übergeordneten zur untergeordneten Domäne



An dieser Stelle ist die Namensauflösung von der übergeordneten zur untergeordneten Domäne hergestellt. Sie müssen noch die Namensauflösung von der untergeordneten zur übergeordneten Domäne herstellen. Die beste Variante hierzu ist die bereits besprochene Weiterleitung:

1. Klicken Sie dazu mit der rechten Maustaste im Snap-In der DNS-Verwaltung auf den Eintrag *Bedingte Weiterleitungen.*
2. Wählen Sie im Kontextmenü den Befehl *Neue bedingte Weiterleitung* aus und tragen Sie die übergeordnete DNS-Domäne ein.
3. Tragen Sie die IP-Adresse eines DNS-Servers der übergeordneten Domäne ein. Wenn in der übergeordneten Domäne mehrere DNS-Server für die Namensauflösung zuständig sind, tragen Sie alle DNS-Server ein (Abbildung 11.79).
4. Diesen Vorgang müssen Sie nicht auf jedem DNS-Server der untergeordneten Domäne durchführen, wenn Sie die Einträge auf die DNS-Server der untergeordneten Domäne replizieren lassen. Das funktioniert allerdings erst, dann wenn die untergeordnete Domäne erstellt worden ist. Diese Möglichkeit ist neu in Windows Server 2008, genauso wie der Menüpunkt zur Weiterleitung. Unter Windows Server 2003 werden diese Maßnahmen in den Eigenschaften des DNS-Servers vorgenommen und können nicht repliziert werden.

Abbildg. 11.79 Konfigurieren eines Weiterleitungsservers in der untergeordneten Domäne



5. Nachdem Sie diese Konfiguration vorgenommen haben, öffnen Sie wieder eine Befehlszeile und geben *nslookup* ein. Überprüfen Sie, ob von der untergeordneten Domäne die Domänencontroller der übergeordneten Domäne aufgelöst werden können. Auch hier sollten keine Fehler mehr auftreten. In diesem Beispiel ist *dc-berlin.de.contoso.com* ein untergeordneter Domänencontroller und *dc01.contoso.com* sind Domänencontroller der übergeordneten Domäne *contoso.com*.

Achten Sie darauf, dass beim Einsatz von mehreren untergeordneten Domänen auch die Namensauflösung zwischen den untergeordneten Domänen untereinander funktioniert. Nur durch eine lückenlos konfigurierte Namensauflösung ist die Replikation im Active Directory sichergestellt. Damit haben Sie die Konfiguration der DNS-Einstellungen abgeschlossen. Die Namensauflösung sollte sowohl innerhalb der Domänen als auch zwischen den Domänen reibungslos funktionieren.

Einführen einer neuen Domänenstruktur in einer Gesamtstruktur

Neben der möglichen Einführung untergeordneter Domänen können in einer Gesamtstruktur auch neue Domänenstrukturen hinzugefügt werden. Eine Struktur innerhalb einer Gesamtstruktur teilt sich mit allen ihren untergeordneten Domänen einen Namensraum. In diesem Beispiel wäre das die Struktur *contoso.com* mit der untergeordneten Domäne *de.contoso.com*. In manchen Unternehmen kann es jedoch sinnvoll sein, unabhängige Namensräume zu erstellen, die zwar Bestandteil der Gesamtstruktur sind, aber vom Namen her von den anderen Domänen unabhängig sind. Ein Beispiel wäre die neue Struktur *microsoft.com* in der Gesamtstruktur *contoso.com*. Neue Strukturen werden vor allem dann geschaffen, wenn Teile des Unternehmens, zum Beispiel durch eine Akquisition, vom Namen her unabhängig erscheinen wollen. Im Grunde genommen ist eine neue Domänenstruktur zunächst nichts anderes als eine neue untergeordnete Domäne der Root-Domäne der Gesamtstruktur, mit dem Unterschied, dass sie einen eigenen Namensraum hat. Bevor Sie eine neue Struktur einführen können, müssen Sie auch hier erst die passende DNS-Infrastruktur erstellen.

Bei der Erstellung einer neuen Struktur gibt es die Möglichkeit, eine neue Delegierung zu erstellen nicht, da der Namensraum von der bisherigen Struktur komplett unabhängig ist. Auch wenn eine neue Struktur vom Namen her mit der ersten erstellten Struktur einer Gesamtstruktur gleichwertig ist, ist die zweite Struktur immer untergeordnet. Die Gesamtstruktur trägt im Active Directory immer die Bezeichnung der ersten installierten Struktur. In der ersten Struktur und der in ihr erstellten ersten Domäne befinden sich auch die beiden Betriebsmasterrollen *Domänennamenmaster* und *Schemamaster* (siehe Kapitel 8). Ein wichtiger Punkt bei der Erstellung von mehreren Strukturen innerhalb einer Gesamtstruktur ist auch der Pfad der Vertrauensstellungen. In einem Active Directory vertrauen sich alle Domänen innerhalb einer Struktur untereinander. Diese transitiven Vertrauensstellungen werden automatisch eingerichtet. Es werden allerdings keine Vertrauensstellungen zwischen untergeordneten Domänen verschiedener Strukturen eingerichtet, sondern nur zwischen den Root-Domänen der einzelnen Strukturen. Wenn Anwender auf Daten verschiedener untergeordneter Domänen zugreifen wollen, muss die Authentifizierung daher immer den Weg bis zur Root-Domäne der eigenen Struktur gehen, dann zur Root-Domäne der anderen Struktur und schließlich zur entsprechenden untergeordneten Domäne. Diese Authentifizierung kann durchaus einige Zeit dauern. Es gibt allerdings Möglichkeiten, diese Aufgabe zu beschleunigen. Dazu müssen Sie manuelle Vertrauensstellungen direkt zwischen den untergeordneten Domänen der verschiedenen Strukturen innerhalb der Gesamtstruktur erstellen.

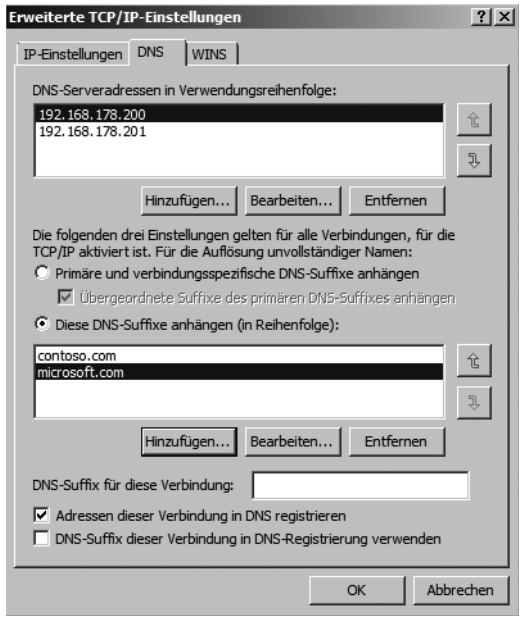
Erstellen der DNS-Infrastruktur für eine neue Domänenstruktur

Um eine neue Struktur innerhalb einer Gesamtstruktur zu erstellen, müssen Sie zunächst wieder eine passende DNS-Infrastruktur schaffen. Sie können dazu entweder wieder auf den DNS-Servern einer bereits vorhandenen Struktur eine neue DNS-Zone mit der Bezeichnung der neuen Struktur oder auf den neuen Domänencontrollern der neuen Struktur eine eigenständige neue Zone erstellen. Gehen Sie dazu genauso vor wie bei der Erstellung der ersten Struktur. Wenn Sie die neue Zone erstellt haben, sollten Sie auf den DNS-Servern der neuen Struktur in den Weiterleitungen eine entsprechende Weiterleitung zur anderen Struktur einrichten, wie sie bereits bei der Delegierung von DNS-Domänen weiter vorne beschrieben wurde. Auf allen DNS-Servern aller Strukturen sollten Weiterleitungen eingerichtet werden, die entsprechende Anfragen an die DNS-Server der jeweiligen Struktur weiterleiten können. Überprüfen Sie die Namensauflösung wieder mit *nslookup*, damit sichergestellt ist, dass die Auflösung zwischen den verschiedenen Strukturen auch funktioniert. Erst wenn die Namensauflösung zwischen der neuen und der bereits vorhandenen DNS-Domäne funktioniert, können Sie die neue Struktur im Active Directory erstellen. Wenn Sie eine neue Struktur innerhalb einer Gesamtstruktur erstellen, müssen Sie sich bei der Gesamtstruktur authentifizieren und der neue Domänencontroller muss eine Verbindung zum Domänennamenmaster aufbauen können. Tragen Sie in den IP-Einstellungen des ersten Domänencontrollers der neuen Struktur seine eigene IP-Adresse als bevorzugten DNS-Server ein. In den Eigenschaften des DNS-Servers tragen Sie die Weiterleitungen zu den DNS-Servern der Root-Domäne ein, in der sich der Domänennamenmaster befindet.

Optimieren der IP-Einstellungen beim Einsatz von mehreren Domänen

Installieren Sie einen zusätzlichen Domänencontroller für eine Domäne, müssen Sie sicherstellen, dass der bevorzugte DNS-Server in den IP-Einstellungen den Namen der Zone auflösen kann, welche die Domäne verwaltet. Sie können in den IP-Einstellungen eines Servers mehrere DNS-Server eintragen. Es wird immer zunächst der bevorzugte DNS-Server verwendet. Die alternativen DNS-Server werden erst eingesetzt, wenn der bevorzugte DNS-Server nicht mehr zur Verfügung steht, weil er zum Beispiel gerade neu gestartet wird. Ein Server verwendet nicht alle konfigurierten DNS-Server parallel oder hintereinander, um Namen aufzulösen. Wollen Sie einen DNS-Namen auflösen und der bevorzugte DNS-Server kann den Namen nicht auflösen und meldet das dem Client zurück, wird nicht der alternative Server eingesetzt. Auch das Zurückgeben einer nicht erfolgten Namensauflösung wird als erfolgreiche Antwort akzeptiert. Über die Schaltfläche *Erweitert* in den IP-Einstellungen eines Rechners können Sie weitere Einstellungen vornehmen, um die Zusammenarbeit mit DNS zu konfigurieren (siehe Kapitel 8). Sie können auf der Registerkarte *DNS* der erweiterten Einstellungen weitere alternative DNS-Server eintragen. Aktivieren Sie auf den Domänencontrollern in den IP-Einstellungen über die Schaltfläche *Erweitert* auf der Registerkarte *DNS* die Option *Diese DNS-Suffixe anhängen (in Reihenfolge)* (Abbildung 11.80). Tragen Sie als Nächstes zuerst den Namensraum der eigenen Struktur ein und hängen Sie danach die Namensräume der anderen Strukturen an.

Abbildg. 11.80 Optimieren der Namensauflösung über neue DNS-Suffixe



Der Sinn dieser Konfiguration ist die schnelle Auflösung von Servern in den anderen Strukturen. Wenn Sie zum Beispiel den Domänencontroller *dc01* in der Struktur *contoso.com* auflösen wollen, müssen Sie immer *dc01.contoso.com* eingeben. Diese Einstellung ist nur optional, erleichtert aber die Stabilität der Namensauflösung in Ihrem Active Directory. Sie sollten diese Einstellung auf jedem Domänencontroller sowie auf jedem Exchange-Server in Ihrer Gesamtstruktur durchführen. Zuerst sollte immer die eigene Domäne und der eigene Namensraum eingetragen werden, bevor andere Namensräume abgefragt werden. Wenn Sie diese Maßnahme durchgeführt haben, können Sie mit *nslookup* den Effekt überprüfen. Sie können an dieser Stelle lediglich *dc01* eingeben. Der Server befragt seinen bevorzugten DNS-Server, ob ein Server mit dem Namen *dc01.microsoft.com* gefunden wird. Da dieser Server nicht vorhanden ist (sonst würde dieser Trick nicht funktionieren), wird der nächste Namensraum abgefragt. Das ist in diesem Beispiel *contoso.com*. Da die Zone *contoso.com* als Weiterleitung in den DNS-Servern definiert ist, fragt der DNS-Server jetzt beim DNS-Server dieser Zone nach und löst den Namen richtig auf. Viele Administratoren tragen auf ihrem DNS-Server einfach einen neuen statischen Hosteintrag ein, der auf die IP-Adresse des Servers des anderen Namensraumes zeigt.

Diese Vorgehensweise ist aber nicht richtig, auch wenn sie grundsätzlich funktioniert. Es wird in diesem Fall nämlich nicht der richtige DNS-Name des entsprechenden Servers zurückgegeben, sondern der Servername mit der Zone des DNS-Servers, in die der Server als Host eingetragen wurde. Vor allem in größeren Active Directorys sollten Administratoren darauf achten, die Konfigurationen so vorzunehmen, dass sie auch formal korrekt sind. Das hilft oft, unbedachte Probleme zu vermeiden. Wenn Sie zum Beispiel in der Zone *microsoft.com* einen neuen Eintrag *dc01* für den Domänencontroller *dc01.contoso.com* erstellen, der auf die IP-Adresse des Servers verweist, wird der Name als *dc01.microsoft.com* aufgelöst, obwohl der eigentliche Name des Servers *dc01.contoso.com* ist. Dadurch funktioniert zwar die Auflösung, aber es wird ein falscher Name zurückgegeben.

Konfiguration sekundärer DNS-Server

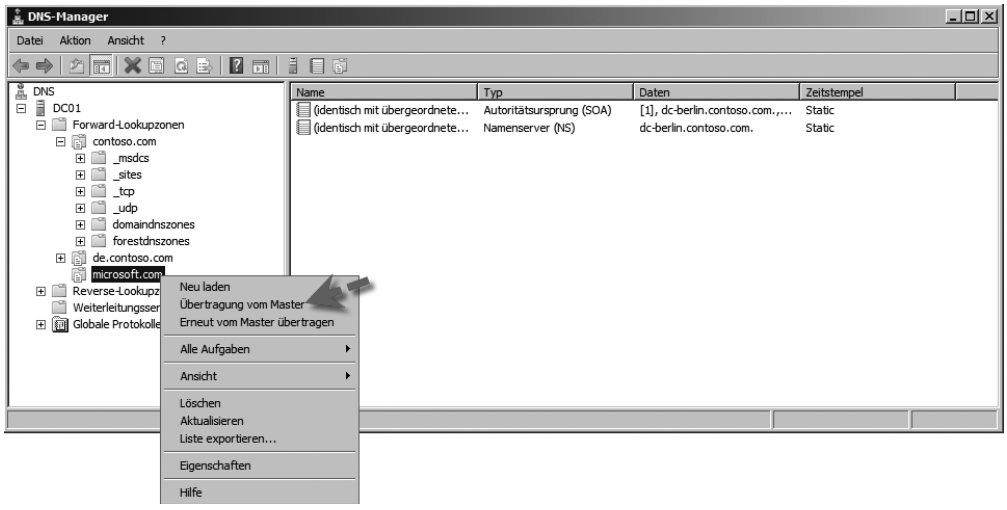
Das Erstellen einer sekundären Zone unterscheidet sich nur unwesentlich vom Erstellen einer primären Zone, weshalb wir uns hier nur mit den Unterschieden eingehender befassen werden:

1. Sie starten den Vorgang, indem Sie in der Verwaltungskonsole im Kontextmenü des Eintrags *Forward-Lookupzonen* den Befehl *Neue Zone* und im zweiten Schritt des Assistenten die Option *Sekundäre Zone* wählen.
2. Geben Sie jetzt im Feld *Zonenname* den Namen der existierenden Domäne ein. Der Name der Zonendatei kann hier nicht mehr ausgewählt werden, er wird automatisch generiert und kann erst später in den Eigenschaften der neu erstellen Zone verändert werden.
3. Da Sie an dieser Stelle unter Umständen noch nicht mit der vorhandenen DNS-Struktur verbunden sind, müssen Sie jetzt die IP-Adresse mindestens eines DNS-Servers angeben, der eine Kopie der Zone gespeichert hat. Dabei muss es sich nicht unbedingt um den primären DNS-Server handeln, falls dieser zum Beispiel nur über eine langsame, unzuverlässige oder teure Netzwerkverbindung zu erreichen ist. In diesem Fall wählen Sie einfach einen der bereits vorhandenen sekundären DNS-Server aus. Die Liste wird anschließend mit dem obersten Eintrag beginnend abgearbeitet, bis ein Server auf die Anfrage zum Zonentransfer antwortet. Alle weiteren Server in der Liste werden dann nicht mehr berücksichtigt. Die Replikation findet also immer nur mit einem Server statt, nicht mit allen in der Liste aufgeführten Servern.

Abbildg. 11.81 Festlegen eines Master-DNS-Servers, von dem die Zone auf den sekundären Server übertragen wird

Der DNS-Server wird nun die in der Liste angegebenen DNS-Server abfragen und einen Zonentransfer anfordern. Falls Sie den Transfer von Hand (außerhalb des regulären Intervalls) starten wollen, wählen Sie im Kontextmenü der Zone den Eintrag *Übertragung vom Master* (Abbildung 11.82). Danach wird ermittelt, ob es neue Einträge gibt, die anschließend angefordert werden. Der Eintrag *Erneut vom Master übertragen* sorgt dafür, dass die bisher empfangenen Daten komplett verworfen werden und eine erneute Anforderung der kompletten Zone erfolgt, was zum Beispiel bei einer Beschädigung der lokalen DNS-Datei nach einem Systemabsturz der Fall sein kann.

Abbildg. 11.82 Übertragen einer DNS-Zone vom Master-DNS-Server auf den sekundären DNS-Server



Befehlszeilen-Tools für DNS

Wenn Probleme im Active Directory auftreten, liegt meistens ein Fehler in der DNS-Konfiguration vor. Aus diesem Grund sollten Sie sich bereits frühzeitig mit den möglichen Fehlerquellen und der DNS-Infrastruktur vertraut machen.

Nslookup zur Fehlerdiagnose einsetzen

Treten im Active Directory Fehler auf, sollten Sie immer zunächst überprüfen, ob sich die beteiligten Server im DNS auflösen können. Verwenden Sie dazu das Befehlszeilenprogramm *Nslookup*. Neben *Nslookup* besprechen wir im nächsten Abschnitt noch weitere Tools, die für die Fehlersuche und Verwaltung von DNS unter Windows Server 2008 eine besondere Rolle spielen. *Nslookup* gehört zu den Bordmitteln von Windows Server 2008. Wenn ein Servername mit *Nslookup* nicht aufgelöst werden kann, sollten Sie überprüfen, wo das Problem liegt:

1. Ist in den IP-Einstellungen des Servers der richtige DNS-Server als bevorzugt eingetragen?
2. Verwaltet der bevorzugte DNS-Server die Zone, in der Sie eine Namensauflösung durchführen wollen?
3. Wenn der Server diese Zone nicht verwaltet, ist dann auf der Registerkarte *Weiterleitungen* in den Eigenschaften des Servers ein Server eingetragen, der die Zone auflösen kann?
4. Wenn eine Weiterleitung eingetragen ist, kann dann der Server, zu dem weitergeleitet wird, die Zone auflösen?
5. Wenn dieser Server nicht für die Zone verantwortlich ist, leitet er dann wiederum die Anfrage weiter?

An irgendeiner Stelle der Weiterleitungskette muss ein Server stehen, der die Anfrage schließlich auflösen kann, sonst kann der Client keine Verbindung aufbauen und die Abfrage des Namens wird nicht erfolgreich sein. Gehen Sie strikt nach dieser Vorgehensweise vor, werden Sie bereits recht schnell den Fehler in der Namensauflösung finden. Sollte bei Ihnen ein Fehler auftauchen, müssen Sie in der Reverse- und der Forward-Zone überprüfen, ob sich der Server dynamisch in das DNS integriert hat. In Ausnahmefällen kann es vorkommen, dass die Aktualisierung der Reverse-Lookupzone nicht funktioniert hat. In diesem Fall können Sie einfach den Eintrag des Servers manuell ergänzen. Dazu müssen Sie lediglich einen neuen Zeiger (engl.: Pointer) erstellen. Ein Zeiger oder Pointer ist ein Verweis von einer IP-Adresse zu einem Hostnamen. Kurz nach der Installation kann dieser Befehl durchaus noch Fehler melden. Versuchen Sie die IP-Adresse des Domänencontrollers erneut mit *Ipconfig /registerdns* zu registrieren. Nach einigen Sekunden sollte der Name fehlerfrei aufgelöst werden. Sobald Sie Nslookup aufgerufen haben, können Sie beliebig Servernamen auflösen. Wenn Sie keinen FQDN eingeben, sondern nur den Computernamen eingeben, ergänzt der lokale Rechner automatisch den Namen durch das primäre DNS-Suffix des Computers, bzw. durch die in den IP-Einstellungen konfigurierten DNS-Suffixe. Sie sollten *auf* kritischen Servern, bzw. auf Servern, bei denen die Namensauflösung nicht funktioniert, mit nslookup überprüfen, an welcher Stelle Probleme auftauchen.

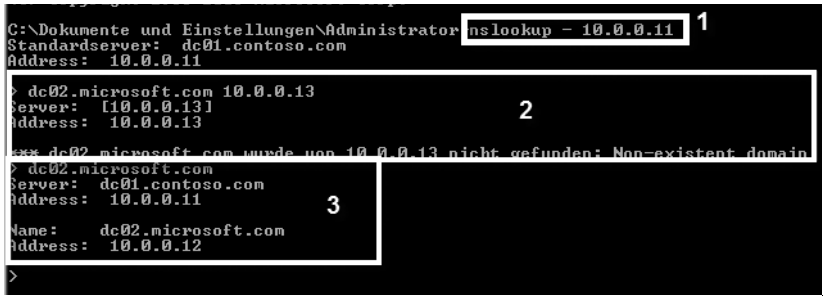
Wenn Sie *Nslookup* aufrufen, um Servernamen aufzulösen, wird als DNS-Server immer der Server befragt, der in den IP-Einstellungen des lokalen Rechners hinterlegt ist. Sie können von dem lokalen Rechner aus aber auch andere DNS Server mit der Auflösung befragen. Geben Sie dazu die Befehlszeile *nslookup <host> <server>*, zum Beispiel *nslookup dc02.microsoft.com dc01.contoso.com*, ein. Bei diesem Beispiel versucht *Nslookup* den Host *dc02.microsoft.com* mit Hilfe des Servers *dc01.contoso.com* aufzulösen. Anstatt den zweiten Eintrag, also den DNS-Server mit seinem FQDN anzusprechen, können Sie auch die IP-Adresse angeben. Wenn Sie als Servereintrag bei dieser Befehlszeile einen DNS-Server mit seinem FQDN eingeben, setzt das voraus, dass der DNS-Server, den der lokale Rechner verwendet, zwar nicht den Host *dc02.microsoft.com* auflösen kann, aber dafür den Server *dc01.contoso.com*. Der DNS-Server *dc01.contoso.com* wiederum muss dann den Host *dc02.microsoft.com* auflösen können, damit keine Fehlermeldung ausgegeben wird. Sie können also mit *nslookup* sehr detailliert die Schwachstellen Ihrer DNS-Auflösung testen. Wenn Sie mehrere Hosts hintereinander abfragen wollen, müssen Sie nicht jedes Mal den Befehl *nslookup <host><server>* verwenden, sondern können Nslookup mit dem Befehl *nslookup –<server>* starten, wobei der Eintrag *server* der Namen oder die IP-Adresse des DNS-Servers ist, den Sie befragen wollen, zum Beispiel *nslookup –10.0.0.11*.

Diagnose der Namensauflösung über DNS mit *Nslookup* an einem Beispiel für fortgeschrittene Benutzer

Sie können die beiden Optionen auch kombinieren. In Abbildung 11.83 ist ein solcher Ablauf dargestellt:

- Wenn Sie zum Beispiel *Nslookup* so starten, dass nicht der lokal konfigurierte DNS-Server zur Namensauflösung herangezogen wird, sondern der Remoteserver *10.0.0.11*, können Sie innerhalb der *Nslookup*-Befehlszeile durch Eingabe von *<host> <server>* wieder einen weiteren DNS-Server befragen.

Abbildg. 11.83 Diagnose von DNS-Problemen mit *Nslookup*

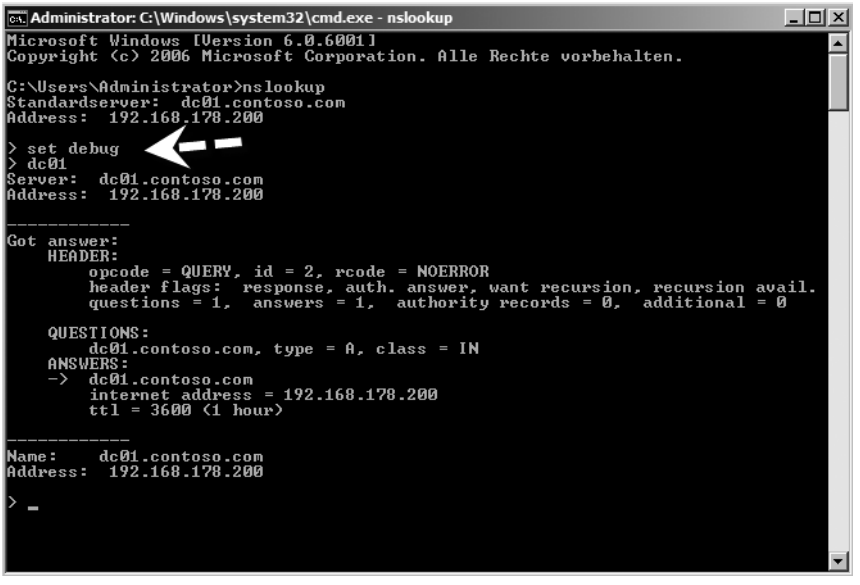


- *Nslookup* wird in der Befehlszeile gestartet und so konfiguriert, dass der DNS-Server *10.0.0.11* zur Namensauflösung herangezogen wird.
- *Nslookup* überprüft, ob der lokal konfigurierte DNS-Server in seiner Reverse-Lookupzone die IP-Adresse *10.0.0.11 zu* einem Servernamen auflösen kann. Da das funktioniert, wird als Standardserver für diese *Nslookup*-Befehlszeile der DNS-Server *10.0.0.11* mit seinem FQDN *dc01.contoso.com* verwendet. Wäre an dieser Stelle eine Fehlermeldung erschienen, dass der Servername für *10.0.0.11* nicht bekannt ist, würde das bedeuten, dass der DNS-Server, der in den IP-Einstellungen des lokalen Rechners konfiguriert ist, in seiner Reverse-Lookupzone den Servernamen nicht auflösen kann. In diesem Fall sollten Sie die Konfiguration der Reverse-Lookupzone überprüfen und sicherstellen, dass alle Zeiger (Pointer) korrekt eingetragen sind. Zu einer konsistenten Namensauflösung per DNS gehört nicht nur die Auflösung von Servername zu IP (Forward), sondern auch von IP zu Servernamen (Reverse).
- In der nächsten Zeile (Punkt 2, Abbildung 11.83) soll der Rechnername *dc02.microsoft.com* vom Server *10.0.0.13* aufgelöst werden. Der Server *10.0.0.13* kann jedoch den Servernamen *dc02.microsoft.com* nicht auflösen. In diesem Fall liegt ein Problem auf dem Server *10.0.0.13* vor, der die Zone *microsoft.com* nicht auflösen kann. Sie sollten daher auf dem Server *10.0.0.13* entweder in den Eigenschaften des DNS-Servers auf der Registerkarte *Weiterleitungen* überprüfen, ob eine Weiterleitung zu *microsoft.com* eingetragen werden muss, oder eine sekundäre Zone für *microsoft.com* auf dem Server *10.0.0.13* anlegen, wenn dieser Rechnernamen für die Zone *microsoft.com* auflösen können soll.
- Als Nächstes wird versucht den gleichen Servernamen *dc02.microsoft.com* über den Standardserver dieser Nslookup-Befehlszeile aufzulösen (siehe Punkt 3, Abbildung 11.83). Der Standardserver kann den Servernamen problemlos auflösen, was zeigt, dass diese Konfiguration in Ordnung ist.

Nslookup.exe zur Auflösung von Internetdomänen verwenden

Bei entsprechend konfigurierter Weiterleitung auf dem DNS-Server muss ein lokaler Rechner auch Internetdomänen auflösen können. Die Antwort kann zwar etwas dauern, da der interne DNS-Server zunächst durch die konfigurierte Weiterleitung einen DNS-Server im Internet befragen muss, aber wenn Sie eine Antwort erhalten, können Sie sicher sein, dass die Namensauflösung ins Internet ebenfalls funktioniert. Sie können über *Nslookup* auch ausführlichere Informationen über eine DNS-Zone oder einen DNS-Server abfragen. Starten Sie dazu *Nslookup* in der Befehlszeile und geben Sie den Befehl *set debug* ein. Im Anschluss erhalten Sie deutlich ausführlichere Informationen über die Hostnamen, DNS-Server und DNS-Zonen, die Sie an dieser Stelle überprüfen.

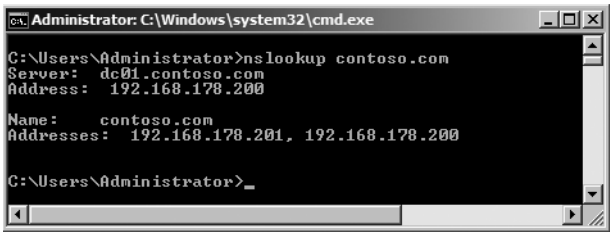
Abbildg. 11.84 Debuginformationen über einen DNS-Server mit *Nslookup* abrufen



Nslookup zur Auflösung von ganzen Domänen verwenden

Wenn Sie *Nslookup* aufrufen, können Sie durch die Eingabe *nslookup contoso.com* überprüfen, welche Namensserver für die DNS-Domäne *contoso.com* zuständig sind (Abbildung 11.85). Im Beispiel in Abbildung 11.83 wird angezeigt, dass der Standardserver *dc01.contoso.com* alle Namensserver auflösen kann. Sie können daher auch auf einem Remoteserver feststellen, welche Namensserver für eine Domäne konfiguriert sind, ohne in das Snap-In *DNS* wechseln zu müssen.

Abbildg. 11.85 Überprüfen der Namensserver für eine Domäne

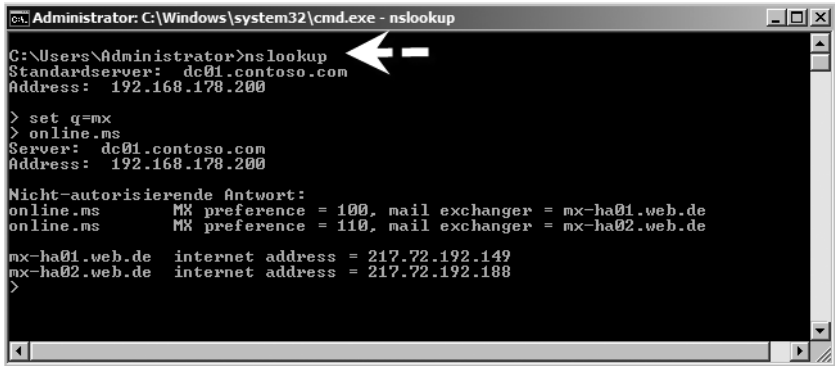


Mit *Nslookup* SRV-Records oder MX-Records anzeigen

Eine der wichtigsten Abfragen, um zum Beispiel Exchange SMTP-Connectoren einzurichten, ist die Abfrage auf SRV-Records. Wenn Sie die bereits besprochene Internetverbindung der DNS-Server sichergestellt haben, können Sie mit nslookup auch die MX-Einträge von Domänen im Internet abfragen. Dadurch können Sie zum Beispiel sicherstellen, dass zu Ihnen geschickte E-Mails auch über diese MX-Server geschickt wurden. Die Abfrage von SRV-Records über *Nslookup* wird hauptsächlich für die Mailexchanger (MX)-Einträge verwendet. Um SRV-Records einer Domäne abzufragen, starten Sie in der Befehlszeile ganz normal *nslookup*. Geben Sie als Nächstes den Befehl *set*

q=mx ein, damit für abgefragte Domänen explizit nur der MX-Eintrag zurückgegeben wird. Sie können durch diese Diagnose auch zum Beispiel Ihren eigenen MX-Eintrag im Internet auf Korrektheit überprüfen.

Abbildg. 11.86 Überprüfen der MX-Einträge für bestimmte Domänen (auch über das Internet)



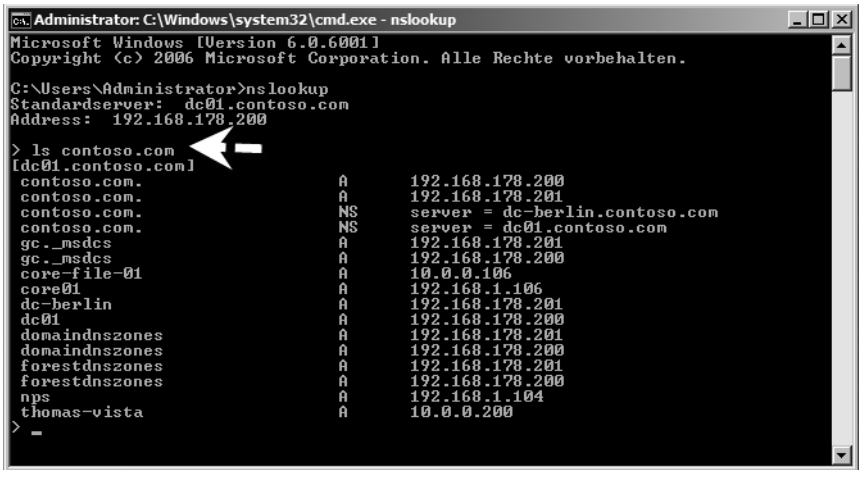
Komplette Zonen mit *Nslookup* übertragen

Zusätzlich können Sie alle Einträge einer Zone in *nslookup* anzeigen lassen. Starten Sie dazu in der Befehlszeile *Nslookup*. Geben Sie als Nächstes den Befehl *ls <Domäne>* ein, zum Beispiel *ls contoso.com*. *Nslookup* baut eine Verbindung zum Namensserver dieser Zone auf und überträgt den Inhalt der kompletten Zone auf den lokalen Rechner, um diesen anzuzeigen. Die Option *–a* liefert Aliasnamen und kanonische Namen (CNAMEs), *–d* liefert alle Daten, und *–t* filtert nach Typ. Durch diese Option können Sie sich alle Informationen über eine Zone anzeigen lassen. Da es sich bei dieser Abfrage um ein klares Sicherheitsproblem handelt, da ein Angreifer auf diese Weise sehr schnell an alle Informationen und Servernamen einer DNS-Zone gelangt, verweigert ein DNS-Server unter Windows Server 2008 standardmäßig diese Abfrage (Abbildung 11.87).

Abbildg. 11.87 Fehlermeldung beim Abrufen von Zoneninformationen über *Nslookup*

Sie können diese Sicherheitseinstellungen für jede einzelne Zone auf einem DNS-Server jedoch anpassen. Rufen Sie dazu die Eigenschaften der Zone auf und wechseln Sie auf die Registerkarte *Zonenübertragung* (Abbildung 11.88). An dieser Stelle können Sie die Übertragung auf einzelne Server zulassen oder verweigern.

Abbildg. 11.88 Anzeigen aller Zonendaten mit *Nslookup*



Mit *Nslookup* die SRV-Records von Active Directory überprüfen

Zusätzlich können mit *Nslookup* auch die SRV-Records von Active Directory überprüft werden. Mit SRV-Records werden spezielle Netzwerkdienste wie zum Beispiel Mailexchanger (MX) oder auch LDAP und Kerberos im DNS veröffentlicht. Clients können im DNS nachfragen, welcher Host im Netzwerk für die einzelnen Serverdienste verantwortlich ist. Das Active Directory baut stark auf diese SRV-Records auf. Aus diesem Grund ist eine Diagnose dieser Einträge mit *Nslookup* durchaus sinnvoll. Alle SRV-Records in Active Directory befinden sich parallel in der Datei *\Windows\system32\config\netlogon.dns.*

IPconfig für DNS-Diagnose verwenden

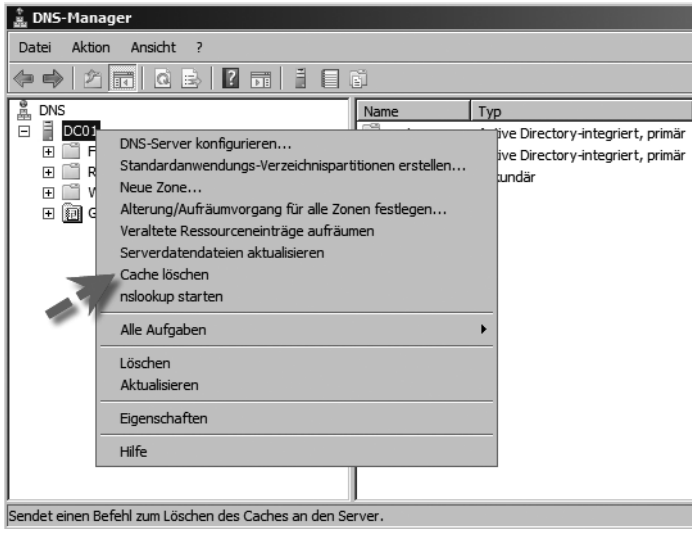
Ein weiteres wichtiges Tool ist *IPconfig.exe*, welches ebenfalls zum Lieferumfang von Windows Server 2008, Windows Server 2003, Windows 2000, Windows XP und Windows Vista gehört. Vor allem die beiden Optionen */registerdns* und */flushdns* sollten jedem Administrator bekannt sein, der einen DNS-Server verwaltet.

IPconfig /flushdns zum Löschen des lokalen DNS-Caches

Wenn Sie eine DNS-Diagnose durchführen und Fehlerbehebungsmaßnahmen daraus ableiten, müssen Sie aufpassen, dass Ihnen der lokale DNS-Cache keinen Strich durch die Rechnung macht. Wenn Sie mit *Nslookup* Namen auf dem DNS-Sever überprüfen, versucht der Client zunächst den Namen aus seinem lokalen DNS-Cache zu lesen. Wenn Sie einen eventuell vorhandenen Fehler behoben haben, kann dennoch der lokale DNS-Cache fehlerhafte Einträge enthalten. Löschen Sie daher immer vor der erneuten Abfrage den lokalen DNS-Cache in der Befehlszeile mit *IPconfig /flushdns*. Auch der DNS-Server verwendet einen eigenen Cache, der bei einer Fehlerdiagnose störend sein kann. Wenn ein Client in seinem DNS-Cache keinen Eintrag finden kann, gibt er die Abfrage an den DNS-Server weiter. Bevor der Server in seinen Zonen überprüft, ob er die Anfrage beantworten kann, bzw. die Anfrage weitergeleitet wird, sucht er in seinem eigenen Server-Cache. Sie sollten daher bei einer Feh-

lerbehebung diesen Cache ebenfalls löschen lassen. Sie finden diese Möglichkeit im Kontextmenü des DNS-Servers im Snap-In *DNS* (Abbildung 11.89).

Abbildg. 11.89 Löschen des DNS-Server-Cache in der DNS-Verwaltung



IPconfig /registerdns

Wenn ein Client gestartet wird, registriert er sich automatisch am DNS, wenn die lokalen Dienste *Anmeldedienst* und *DNS-Client* gestartet werden. Da Sie bei einer Fehlerbehebung nicht jedes Mal die beiden Dienste neu starten oder den ganzen Server durchbooten wollen, können Sie in der Befehlszeile mit dem Befehl *ipconfig/registerdns* eine manuelle Aktualisierung der Einträge auf dem DNS durchführen. Nach der Eingabe des Befehls sollten die Einträge recht schnell auf dem DNS aktualisiert worden sein. Sollte das dynamische Aktualisieren noch immer nicht funktionieren, überprüfen Sie in den Eigenschaften der Zone, ob die dynamische Aktualisierung aktiviert ist. Wenn sich an der Zone auch Arbeitsstationen und Server dynamisch registrieren sollen, die nicht Mitglied der Gesamtstruktur sind, können Sie auch die Option *Nicht sichere und sichere* aktivieren.

DNScmd.exe zur Verwaltung eines DNS-Servers in der Befehlszeile

Ein weiteres wichtiges Befehlszeilenprogramm ist *DNScmd.exe*, mit dem Sie einen DNS-Server in der Kommandozeile verwalten können. Mit *DNScmd.exe* können sowohl Informationen über einen DNS-Server abgerufen als auch Informationen in Textdateien exportiert werden. Mit dem Tool lässt sich ein DNS-Server komplett über die Befehlszeile verwalten, zum Beispiel über Skripts. Über *dnscmd /?* erhalten Sie eine ausführliche Hilfe. Auf der Internetseite *http://technet2.microsoft.com/windowsserver/en/library/5c497b2e-3387-4ecf-adf5-562045620a961033.mspx?mfr=true* finden Sie die ausführliche Befehlszeilensyntax. Unter manchen Umständen, zum Beispiel für die Diagnose von DNS-Problemen, kann es durchaus sinnvoll sein, eine komplette Zone aus dem DNS in eine Textdatei zu importieren. Wenn die Zonen nicht im Active Directory integriert sind, sondern es sich um

normale primäre oder sekundäre DNS-Zonen handelt, ist ein Export mit *Dnscmd* unnötig. Sie können in diesem Fall die Zonendateien mit der Endung **.dns* aus dem Verzeichnis *\Windows\System32\dns* kopieren. Active Directory integrierte Zonen werden nicht in **.dns*-Dateien gespeichert, sondern direkt in die Active Directory-Datenbank integriert. Um mit *Dnscmd* eine Active Directory-integrierte DNS-Zone in eine Testdatei zu kopieren, öffnen Sie eine Befehlszeile und geben zum Beispiel den Befehl *dnscmd dc01.contoso.com /zonexport contoso.com contoso.txt* ein. Die Zonendatei wird in das Verzeichnis *\Windows\System32\dns* kopiert. Die Optionen von *Dnscmd* und deren Aufgaben sind:

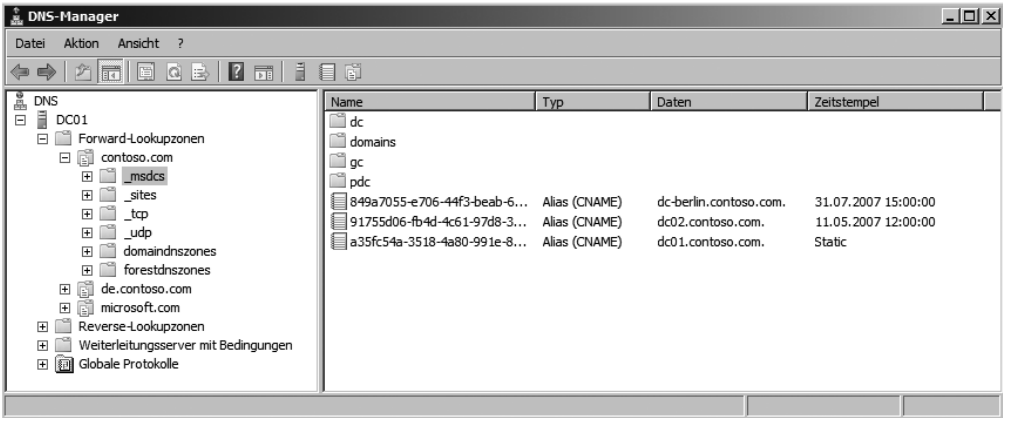
- **Dnscmd ageallrecords** Verändert die Zeitstempel von Einträgen innerhalb einer bestimmten Zone, zum Beispiel *dnscmd reskit.com /ageallrecords test.reskit.com*
- **Dnscmd clearcache** Löscht den Cache des Servers aus der Befehlszeile
- **Dnscmd config** Mit dieser Option können verschiedene Einstellungen der Zonen und des kompletten Servers vorgenommen werden
- **Dnscmd createbuiltindirectorypartitions** Mit dieser Option können DNS-Anwendungspartitionen auf Gesamtstruktur- oder Domänenebene erstellt werden. Der Befehl dient hauptsächlich zur Wiederherstellung der Standard-Anwendungspartitionen.
- **Dnscmd createdirectorypartition** Mit dieser Option können neben den Standard-Partitionen weitere Anwendungspartitionen erstellt werden, um die DNS-Replikation detaillierter steuern zu können
- **Dnscmd deletedirectorypartition** Löscht erstellte DNS-Anwendungsverzeichnispartitionen
- **Dnscmd directorypartitioninfo** Zeigt Informationen über eine spezifische DNS-Anwendungsverzeichnispartition an
- **Dnscmd enlistdirectorypartition** Fügt DNS-Server zu der Replikationsliste einer Anwendungsverzeichnispartition hinzu
- **Dnscmd enumdirectorypartitions** Zeigt alle DNS-Anwendungsverzeichnispartitionen eines bestimmten Servers an
- **Dnscmd enumrecords** Zeigt die Ressourcen eines bestimmten Knotens innerhalb einer DNS-Zone an
- **Dnscmd enumzones** Zeigt die Zonen eines bestimmten Servers an, zum Beispiel *dnscmd reskit.com /enumzones* oder *dnscmd reskit.com /enumzones /auto-created /reverse*
- **Dnscmd info** Zeigt bestimmte Einstellungen für den DNS-Server an, die auch im Registrykey *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters* gespeichert sind. Beispiele hierfür sind *dnscmd reskit.com /info isslave* oder *dnscmd reskit.com /info recursiontimeout.*
- **Dnscmd nodedelete** Löscht alle Einträge eines bestimmten Hosts, zum Beispiel *dnscmd reskit.com /nodedelete test.reskit.com node /tree* oder *dnscmd reskit.com /NodeDelete test.reskit.com host /F*
- **Dnscmd recordadd** Fügt einen neuen Eintrag auf einem bestimmten DNS-Server und einer bestimmten DNS-Zone hinzu
- **Dnscmd recorddelete** Löscht einen Eintrag auf einem bestimmten DNS-Server und einer bestimmten DNS-Zone
- **Dnscmd resetforwarders** Löscht die Liste der Weiterleitungsserver eines bestimmten DNS-Servers

- **Dnscmd resetlistenaddresses** Legt die Schnittstelle fest, auf die der DNS-Server auf Clientanfragen hört
- **Dnscmd startscavenging** Veranlasst einen bestimmten DNS-Server nach abgelaufenen Einträgen zu suchen
- **Dnscmd statistics** Zeigt Informationen für einen bestimmten DNS-Server an oder löscht diese, zum Beispiel *dnscmd reskit.com /statistics 00000001* oder *DNSCmd reskit.com /Statistics 00200000*
- **Dnscmd unenlistdirectorypartition** Löscht einen DNS-Server von der Replikationsliste einer bestimmten Zone, wenn eine eigene DNS-Anwendungsverzeichnispartition erstellt wurde
- **Dnscmd writebackfiles** Überprüft, ob im Arbeitsspeicher des DNS-Servers noch Änderungen stehen, die nicht auf die Platte geschrieben wurden und speichert diese dann auf der Platte
- **Dnscmd zoneadd** Fügt einem Server eine neue Zone hinzu
- **Dnscmd zonechangedirectorypartition** Verschiebt eine Zone in eine bestimmte DNS-Anwendungsverzeichnispartition, um die Replikation der Zone besser zu steuern
- **Dnscmd zonedelete** Löscht eine bestimmte Zone von einem Server, zum Beispiel *dnscmd reskit.com /zonedelete test.reskit.com*
- **Dnscmd zoneexport** Exportiert eine Zone in eine Textdatei
- **Dnscmd zoneinfo** Zeigt Informationen einer bestimmten Zone an, die auch in der Registry im Key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\Zones\<Zonen-Namen>* gespeichert sind, zum Beispiel *dnscmd reskit.com /zoneinfo test.reskit.com refreshinterval* oder *dnscmd reskit.com /zoneinfo test.reskit.com aging*
- **Dnscmd zonepause** Pausiert eine Zone. Client-Anfragen an diese Zone werden nicht beantwortet.
- **Dnscmd zoneprint** Zeigt alle Einträge einer Zone an
- **Dnscmd zoneresettype** Ändert den Typ einer Zone
- **Dnscmd zonerefresh** Zwingt einen sekundären DNS-Server zum Abgleich der Zone mit seinem Master
- **Dnscmd zonereload** Lässt eine Zone aus dem Active Directory oder deren Textdatei aus dem Verzeichnis *\Windows\System32\dns* neu laden
- **Dnscmd zoneresetmasters** Setzt die IP-Adresse des Master-DNS-Server auf sekundären DNS-Server zurück
- **Dnscmd zoneresetscavengeservers** Konfiguriert die IP-Adressen, die eine bestimmte Zone bereinigen dürfen
- **Dnscmd zoneresetsecondaries** Legt auf einem DNS-Master-Server die IP-Adressen der sekundären DNS-Server fest, die Zonendaten abrufen dürfen
- **Dnscmd zoneresume** Startet eine pausierte Zone wieder
- **Dnscmd zoneupdatefromds** Aktualisiert eine Active Directory-integrierte Zone aus dem Active Directory
- **Dnscmd zonewriteback** Überprüft, ob im Arbeitsspeicher für eine bestimmte Zone noch Einträge stehen und schreibt diese auf die Platte

Probleme bei der Replikation durch fehlerhafte DNS-Konfiguration – *DNSLint.exe*

Die häufigsten Fehler aller Art innerhalb von Active Directory sind Fehler im DNS. Jeder Domänencontroller in Active Directory hat neben seinem Host A-Namen, zum Beispiel *dc01.contoso.com*, noch einen zugehörigen CNAME, der das so genannte DSA (Directory System Agent)-Objekt seiner NTDS-Settings darstellt. Dieses DSA-Objekt ist als SRV-Record im DNS unterhalb der Zone der Domäne unter dem Eintrag *_msdcs* zu finden (Abbildung 11.90).

Abbildg. 11.90 Anzeigen der DNS-DSA-Objekte von Domänencontrollern



Der CNAME ist die GUID dieses DSA-Objektes. Domänencontroller versuchen ihren Replikationspartner nicht mit dem herkömmlichen Host A-Eintrag aufzulösen, sondern mit dem hinterlegten CNAME. Auf Windows 2000 Servern und Windows Server 2003 ohne installiertes SP1 ist die Namensauflösung im DNS für die Replikation deutlich fehleranfälliger gewesen. Wenn ein Domänencontroller mit diesen älteren Betriebssystemständen versucht einen Replikationspartner mit diesem CNAME über DNS aufzulösen und dies misslingt, bricht die Replikation mit einem Fehler ab. Ein Windows Server 2003-Domänencontroller mit installiertem SP1 oder Windows Server 2008-Domänencontroller versuchen nach der erfolglosen Namensauflösung des CNAME eines Domänencontrollers, einen HOST A-Eintrag zu finden. Schlägt auch das fehl, versucht der Domänencontroller den Namen mit NetBIOS aufzulösen, entweder über Broadcast oder einen WINS-Server. Jeder Domänencontroller braucht einen eindeutigen CNAME, der wiederum auf seinen Host A-Eintrag verweist. Überprüfen Sie bei Replikationsproblemen, ob diese Einträge vorhanden sind. Sollte die Namensauflösung mit DNS noch immer nicht funktionieren, steht Ihnen noch das Tool *Dnslint.exe* zur Verfügung, mit denen die SRV-Records im Active Directory überprüft werden können. Sie können sich das Tool bei Microsoft auf der Seite *http://download.microsoft.com/download/2/7/2/27252452-e530-4455-846a-dd68fc020e16/dnslint.v204.exe* herunterladen. Entpacken Sie das Tool nach dem Herunterladen in ein Verzeichnis. Für das Tool gibt es insgesamt drei verschiedene Funktionen, die jeweils DNS überprüfen und einen entsprechenden HTML-Bericht generieren. Diese drei Funktionen sind:

- **dnslint /d** Diese Funktion diagnostiziert mögliche Ursachen einer langsamen Delegierung
- **dnslint /ql** Diese Funktion überprüft benutzerdefinierte DNS-Datensätze auf mehreren DNS-Servern
- **dnslint /ad** Diese Funktion überprüft DNS-Datensätze, die speziell für die Active Directory-Replikation verwendet werden

Die Syntax lautet:

dnslint /d <Domänenname> | /ad [<LDAP_IP_Adresse>] | /ql <Input_Datei> [/c [smtp,pop,imap]] [/no_open] [/r <Report_Name>] [/t] [/test_tcp] [/s <DNS_IP_Adresse>] [/v] [/y]

Bei der Ausführung von DNSLint müssen Sie eine der Befehlszeilenoptionen */d*, */ad* oder */ql* verwenden. Mit *Dnslint.exe /ad* können Sie überprüfen, ob Ihre Domänencontroller die DNS-Einträge im Active Directory zur Replikation abrufen können. Geben Sie zur Überprüfung den Befehl *dnslint /ad <IP-Adresse des ersten DCs> /s <IP-Adresse des zweiten DCs>* ein. Das Tool benötigt einige Sekunden und überprüft, ob im Active Directory die notwendigen *_msdcs*-Einträge vorhanden sind. Geben Sie an dieser Stelle nicht den DNS-Namen der beiden Server an, die Replikationsprobleme haben, sondern die IP-Adressen. Die Option */ad* dient zur Angabe eines Domänencontrollers, der die notwenigen GUIDs im DNS auflösen können muss. Jeder Domänencontroller muss in der Lage sein, die Namen dieser GUIDs per DNS aufzulösen.

Abbildg. 11.91 Ausführen von *DNSLint* zur Diagnose von Active Directory

Testen Sie daher auf jedem Server mit DNSLint, ob die einzelnen Server Probleme bei der Auflösung dieser GUIDs haben. Wenn in diesem Bereich Fehler auftreten, liegen die Replikationsprobleme eindeutig zunächst an diesen fehlenden GUIDs. Die Option */s* dient dazu dem Befehl einen DNS-Server mitzuteilen, der die Zone *_msdcs* von Active Directory verwaltet. Der Server hinter der Option */ad* dient daher zum Verbindungsaufbau per LDAP, während der Server hinter */s* zum Auflösen per DNS dient. Sie müssen nicht unbedingt zwei unterschiedliche Server angeben, sondern können auch zweimal die gleiche IP-Adresse verwenden. Nachdem der Befehl abgeschlossen ist, wird Ihnen ein detaillierter HTML-Bericht angezeigt, mit dessen Hilfe Sie die Probleme der GUID-Auflösung mit DNS nachvollziehen können. Der Bericht zeigt die Auflösung der einzelnen GUIDs der Domänencontroller und die vorhandenen Fehler sehr ausführlich an. Beim Starten des Befehls verbindet sich DNSLint zunächst mit dem Domänencontroller, um alle GUIDs der Gesamtstruktur abzufragen. Die Abfrage erfolgt mit LDAP. Aus diesem Grund müssen Sie vor der Ausführung sicherstellen, dass Sie den Befehl unter einem Benutzerkonto starten, das über genügend Rechte verfügt. Sobald die GUID-Liste vom LDAP-Server zurückgegeben wird, versucht DNSLint über den mit der Option */s* konfigurierten DNS-Server, diese GUIDs zu ihrer IP-Adresse aufzulösen. Durch DNSLint erhalten Sie daher ausführlich Informationen über die korrekte DNS-Konfiguration Ihrer Gesamtstruktur. Mit der Befehlszeilenoption */d* fordern Sie Domänennamentests an. Diese Befehlszeilenoption ist für die Behandlung von Problemen in Bezug auf eine langsame Delegierung nützlich. Sie müssen den zu testenden Domänennamen angeben. Sie können die Befehlszeilenoption */d* nicht in Verbindung mit der Option */ad* verwenden. Mit der Befehlszeilenoption */ad* rufen Sie einen Active Directory-Test auf. Mit der Befehlszeilenoption */ql* fordern Sie DNS-Abfragetests von einer Liste ab. Die Befehlszeilenoption */ql* versendet die DNS-Abfragen, die in einer Texteingabedatei angegeben wurden. Sie müssen den Namen und den Pfad der Eingabedatei angeben. Die Befehlszeilenoption */ql* unterstützt A-, PTR-, CNAME-, SRV- und MX-Datensatzabfragen. Sie können eine Beispieleingabedatei erstellen, indem Sie den folgenden Befehl ausführen: *dnslint /ql autocreate*. Sie können die Befehlszeilenoption */ql* nicht in Verbindung mit der Option */d, /ad* oder */c* verwenden.

Optionale Befehlszeilenoptionen:

- Mit */c* veranlassen Sie Konnektivitätstests auf E-Mail-Servern. Die Befehlszeilenoption */c* testet dazu SMTP-, POP- und IMAP-Ports auf den gefundenen E-Mail-Servern. Es werden standardmäßig alle drei Ports (SMTP, POP und IMAP) getestet. Sie können nur einen Port oder eine Kombination aus mehreren Ports festlegen. Verwenden Sie hierzu eine kommagetrennte Liste, zum Beispiel: */c pop,imap,smtp*.
- Mit der Befehlszeilenoption */no_open* verhindern Sie, dass Berichte automatisch geöffnet werden. Die Befehlszeilenoption */no_open* ist besonders in Skripts nützlich.
- Mit der Befehlszeilenoption */r* können Sie den Namen der erzeugten Berichtsdatei festlegen. Dem Berichtsnamen wird automatisch die Dateinamenerweiterung **.htm* angehängt. Der Bericht wird also im HTML-Format erstellt. Der Standardname des Berichts lautet *Dnslint.htm*.
- Verwenden Sie die Befehlszeilenoption */s*, um einen WHOIS-Lookup zu umgehen. Sie können hier IP-Adressen von DNS-Servern angeben, statt diese bei *InterNIC* abzufragen. Die Befehlszeilenoption */s* startet die Überprüfung von DNS-Datensätzen unter Verwendung der angegebenen IP-Adresse. Es werden nur gültige IP-Adressen akzeptiert. Namen werden nicht akzeptiert. Verwenden Sie diese Option zur Überprüfung von Domänennamen, die von InterNIC nicht unterstützt werden. Wenn Sie */ad* verwenden, müssen Sie die Option */s* verwenden, um einen DNS-Server anzugeben, der für die *_msdcs*-Unterdomäne in der Stammdomäne der Active Directory-Struktur autorisierend ist. Wenn Sie die Option */ad* verwenden, können Sie den Befehl */s local-*

host ausführen, um festzustellen, ob das lokale System die Datensätze auflösen kann, die bei den Active Directory-Tests gefunden werden.

- Verwenden Sie */t*, um die Ausgabe in eine Textdatei anzufordern. Die Textdatei hat denselben Namen wie der HTM-Bericht, der Textdatei wird jedoch die Dateinamenerweiterung **.txt* angehängt. Die Textdatei wird in demselben Verzeichnis gespeichert wie die HTM-Berichtsdatei.
- Verwenden Sie */test_tcp*, um anzufordern, dass der TCP-Port 53 getestet wird. Standardmäßig wird nur der UDP-Port 53 getestet. Die Option */test_tcp* überprüft, ob TCP-Port 53 auf Abfragen reagiert. Diese Option kann nicht in Verbindung mit der Option */ql* verwendet werden.
- Mit */v* bewirken Sie eine ausführliche Ausgabe auf dem Bildschirm. Bei dieser Option zeigt das Tool auf dem Bildschirm an, welche Schritte es ausführt, um Daten zu sammeln.
- Verwenden Sie */y*, um eine vorhandene Berichtsdatei zu überschreiben, ohne dass der Benutzer den Überschreibvorgang bestätigen muss.
- Verwenden Sie die Befehlszeilenoption */d* (Domänennamentest) zum Testen eines bestimmten DNS-Domänennamens. Diese Option hilft bei der Diagnose möglicher Ursachen einer langsamen Delegierung sowie weiterer einschlägiger DNS-Probleme. Der Domänenname, den Sie testen, kann ein Name sein, der für die Verwendung im Internet registriert ist, oder es kann sich um einen Namen handeln, der in einem privaten Namespace verwendet wird. Wenn Sie Domänennamen in einem privaten Netzwerk oder im Internet registrierte Domänennamen mit einer Tiefe von mehr als zwei Ebenen testen, müssen Sie die Option */s* verwenden.
- Bei der Verwendung der Befehlszeilenoption */c* versucht DNSLint standardmäßig, auf jedem gefundenen E-Mail-Server Verbindungen zu allen drei Ports herzustellen, das heißt zu TCP-Port 25 für SMTP, zu TCP-Port 110 für POP und zu TCP-Port 143 für IMAP. Das Tool zeigt für jeden Port den jeweiligen Status an: »Listening« (Horcht), »Not Listening« (Horcht nicht) oder »No Response« (Keine Antwort). Stellt DNSLint fest, dass der Port horcht, meldet es auch eine etwaige Antwort des Ports. Wenn zum Beispiel ein SMTP-Port horcht, gibt er typischerweise eine Antwort zurück, die der SMTP-Protokollspezifikation entspricht. Der Befehl *dnslint /y /v /c /d microsoft.com* erzeugt beispielsweise einen Bericht mit dem Namen *Dnslint.htm*, der einen bereits vorhandenen Bericht mit demselben Namen überschreibt, ohne dass der Benutzer das Überschreiben bestätigen muss. Da die Option */c* angegeben wurde, wird an das Ende des DNSLint-Standardberichts ein zusätzlicher Abschnitt angehängt. Wenn ein Ziel-E-Mail-Server auf einen Verbindungsversuch über einen seiner E-Mail-Ports nicht reagiert, versucht DNSLint insgesamt drei Mal, die Verbindung herzustellen.

Zusammenfassung

Im Bereich DNS, WINS und DHCP hat sich im Vergleich zu Windows Server 2003 wenig geändert. Dennoch gibt es Detailverbesserungen sowie die Unterstützung des Netzwerkzugriffschutzes beim DHCP-Server in Windows Server 2008. Auch IPv6 wird jetzt in diesen Bereichen unterstützt. Im Kapitel 15 gehen wir ausführlicher auf die Möglichkeiten ein, einen DHCP-Server zusammen mit dem neuen Netzwerkzugriffschutz zu betreiben. Im nächsten Kapitel zeigen wir Ihnen zunächst die zahlreichen Neuerungen im Bereich der Terminaldienste.

Kapitel 12

Terminalserver

In diesem Kapitel:

Mit den Windows-Terminaldiensten ist es möglich, Windows-Anwendungen auf allen Arten von Geräten, unabhängig vom Betriebssystem, zu starten. Dabei läuft die eigentliche Anwendung auf dem Terminalserver, während der Benutzer mit einem Client Verbindung zu einer Sitzung auf einem Terminalserver aufbaut. Auf dem Client werden nur die Bildschirmänderungen angezeigt. Durch einen Terminalserver lassen sich Anwendungen schnell in der Firma verteilen, da diese nur auf einem oder mehreren Terminalservern installiert werden müssen und Clients eine Verbindung zu diesem Server aufbauen können. Ein Terminalserver zeigt seine Stärken bei der schnellen Verteilung von Windows-basierten Anwendungen auf die Rechner eines Unternehmens, speziell auch von Anwendungen, die häufig aktualisiert werden, oder schwer zu verwalten sind. Windows Server 2008 kann als Terminalserver installiert werden und stellt zentral Anwendungen zur Verfügung, die von den Benutzern ausgeführt werden. Beim Einsatz eines Terminalservers müssen nicht alle Anwendungen auf dem Server installiert werden. Es ist daher ohne weiteres möglich, dass einigen Anwendern einzelne Applikationen auf ihrem PC installiert werden. Wenn Benutzer mit einem PC arbeiten, werden ihre Tastatur- und Mauseingaben lokal wiedergegeben. Auch die Ausgabe des PC erfolgt direkt auf dem Bildschirm und alle Daten werden lokal verarbeitet. Die Geschwindigkeit einer Anwendung ist von der Performance des PCs abhängig. Arbeiten Benutzer über einen Terminalserver, werden die Tastatur- und Mauseingaben über ein Netzwerkprotokoll an einen Terminalserver übermittelt, der auch die Daten verwaltet. Die Bildschirmausgabe wird über das Netzwerk wieder an den Client übermittelt. Durch diese Arbeitsweise wird die Last der Datenverarbeitung auf einen Server ausgelagert und der Client-PC muss nur noch die Änderungen des Bildschirms anzeigen.

Grundlegende Neuerungen der Terminaldienste

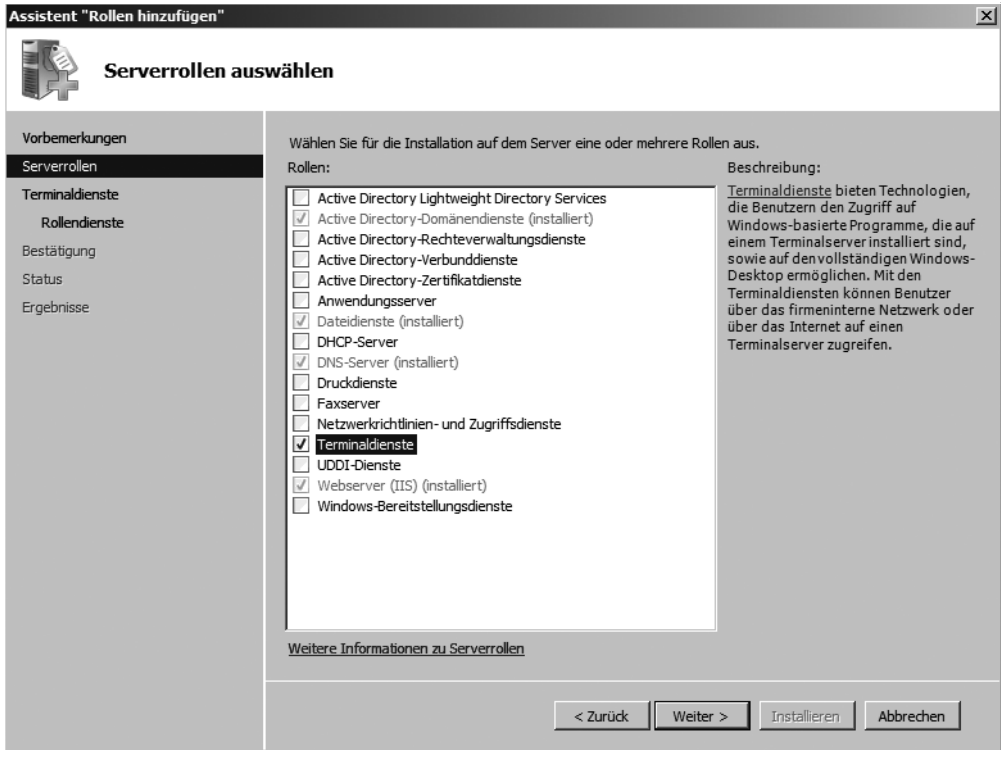
In Kapitel 1 sind wir bereits auf viele Neuerungen der Terminaldienste eingegangen. In diesem Abschnitt zeigen wir Ihnen die grundlegenden Neuerungen und Vorteile der neuen Version. Das Netzwerkprotokoll, mit dem die Terminaldienste Daten mit den Clients austauschen, wird *RDP (Remote Desktop Protocol)* genannt, das in Windows Server 2008 mittlerweile in der Version 6 vorliegt. Die vom Benutzer auf dem Terminalserver ausgeführten Anwendungen laufen in einer eigenen isolierten Umgebung. Die vom Server zur Verfügung gestellte Arbeitsumgebung wird als *Terminalserversitzung* bezeichnet. Ein Anwender kann eine Sitzung starten und anschließend die Verbindung beenden, ohne die Sitzung selbst zu schließen. Seine Arbeitsumgebung bleibt damit auf dem Server erhalten und der Anwender kann sich später wieder mit der Sitzung verbinden. Ein Terminalserver sollte grundsätzlich dediziert eingesetzt werden, das heißt, er wird ausschließlich für diese Funktion eingesetzt. Im Bereich der Terminalserver-Rolle hat Microsoft einige neue Funktionen eingeführt. In diesem Kapitel gehen wir auf die neuen Funktionen und Möglichkeiten ein, die ein Terminalserver unter Windows Server 2008 bietet. Mit der neuen *RemoteApp*-Funktion können Anwendern Applikationen so zur Verfügung gestellt werden, dass nicht mehr ersichtlich ist, ob die Anwendung lokal oder auf einem Terminalserver läuft. Die Anwendung wird dazu auf dem Terminalserver gestartet, sieht beim Anwender aber aus, als ob sie lokal läuft. Unter Windows Server 2003 konnte diese Funktionalität nur durch den Einsatz von Citrix Presentation Server ermöglicht werden. Weitere Neuerungen sind das Terminaldienste-Webzugriff und das Terminaldienstegateway, welche für den Zugriff über das Internet zuständig sind. Neu ist auch die Windows Vista-Oberfläche für Clients sowie die Unterstützung des neuen RDP 6.0-Protokolls. Auch im Bereich des Loadbalancing hat Microsoft einige Änderungen eingeführt, die wir Ihnen im Laufe dieses Kapitels zeigen werden. Die Terminaldienste unter Windows Server 2008 unterstützen sehr effizient 64-Bit-Server, also die Unterstützung von

mehr Arbeitsspeichern. Da die Terminaldienste sehr serverlastig und Arbeitsspeicherhungrig sind, wird durch mehr Arbeitsspeicher auch deutlich mehr Leistung unterstützt. Die Authentifizierung am Server findet jetzt nicht mehr über eine Anmeldemaske auf dem Server statt, sondern zunächst am RDP-Client auf dem Client-Computer. Dadurch wird die Last des Servers und des Netzwerks erheblich vermindert. Mit der neuen Technik findet erst die Authentifizierung statt, bevor der Desktop geladen wird. Lokale Geräte wie Digitalkameras können jetzt vom RDP-Client aus auf den Terminalserver umgeleitet werden, was deutlich besser funktioniert als unter Windows Server 2003. Geräte können auch im laufenden Betrieb einer Terminalserversitzung umgeleitet werden. Die weiteren Neuerungen zeigen wir Ihnen nach der Beschreibung der Installation. Die meisten neuen Funktion lassen sich besser verstehen, wenn diese in einer Testumgebung betrachtet werden.

Installieren eines Terminalservers

Die Installation eines Terminalservers findet über den Server-Manager statt, indem Sie über den Server-Manager die Rolle *Terminaldienste* installieren (Abbildung 12.1).

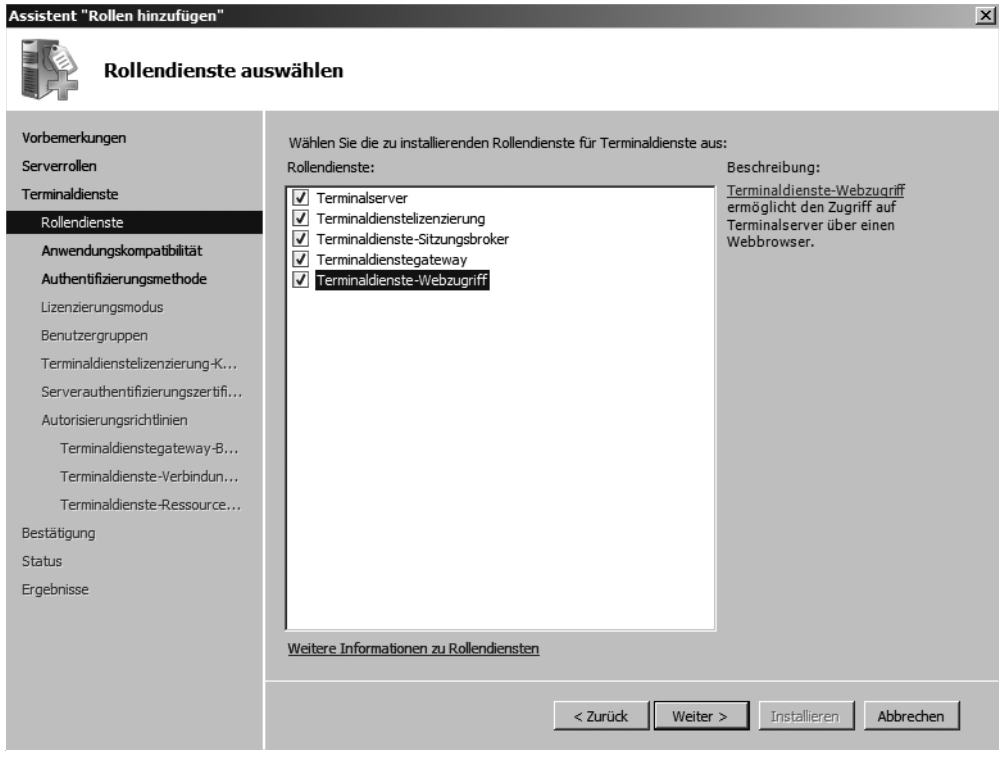
Abbildg. 12.1 Installieren eines Terminalservers



Haben Sie die Rolle ausgewählt, startet der Assistent, über den Sie die verschiedenen neuen Funktionen installieren können. Abhängig von den bereits installierten Rollen sowie den Funktionen, die Sie auswählen, erscheinen im Laufe der Installation mehr oder weniger Fenster. Die folgenden Seiten gehen ausführlicher auf die Installation ein. Auf der nächsten Seite des Assistenten wählen Sie

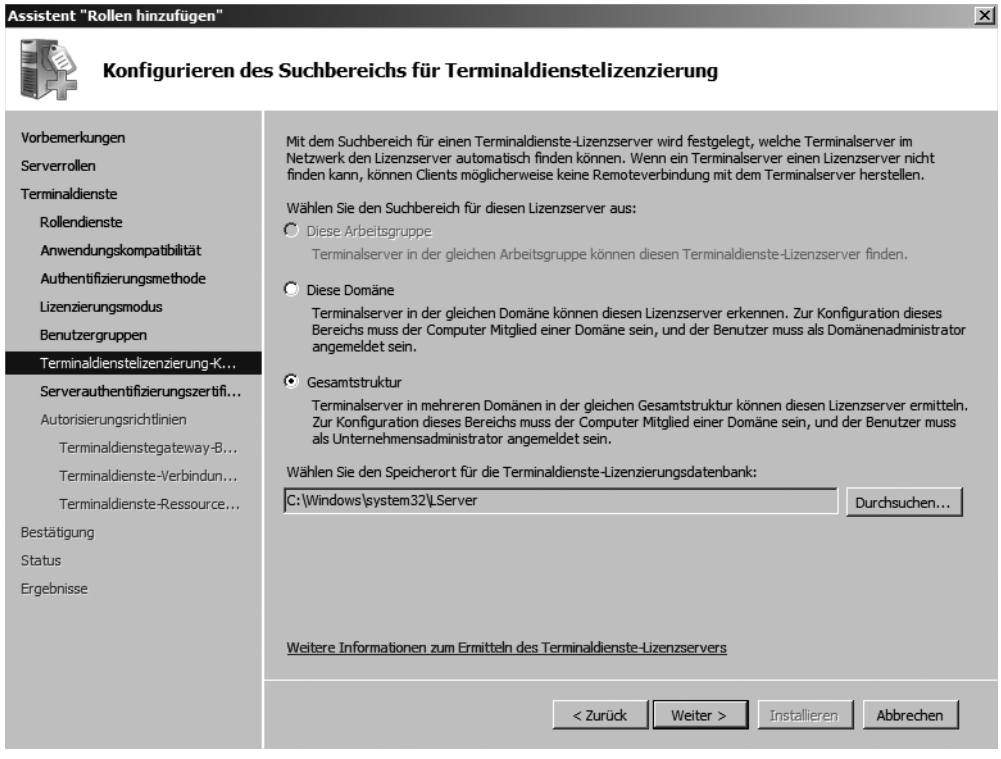
aus, welche zusätzlichen Terminalserver-Funktionen Sie installieren wollen. Abhängig von Ihrer Auswahl schlägt der Assistent die Installation weiterer Rollen und Funktionen vor, sofern Abhängigkeiten bestehen (Abbildung 12.2).

Abbildg. 12.2 Auswählen der Rollendienste für die Terminalserver-Installation



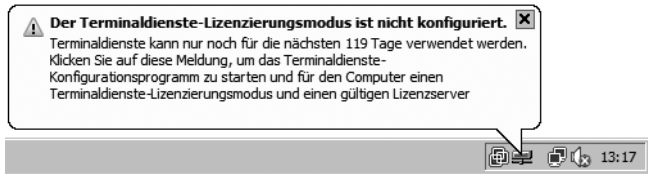
Das nächste Fenster, auf dem Sie eine Auswahl treffen können, dient der Konfiguration der Authentifizierung. Hier können Sie auswählen, ob nur Clients mit dem neuen RDP 6.0-Client-Programm Verbindung aufbauen können (unter Windows Vista standardmäßig installiert) oder auch ältere Versionen (muss unter Windows XP SP2 manuell nachinstalliert werden). Anschließend konfigurieren Sie die Lizenzierung der Clients. Auf dem nächsten Fenster können Sie die Benutzergruppen auswählen, die sich auf den Terminalserver verbinden können. Standardmäßig dürfen sich nur Administratoren auf einem Server anmelden. Damit sich Benutzer auf einem Terminalserver anmelden können, müssen Sie diese auf dem Terminalserver in die lokale Benutzergruppe *Remotedesktopbenutzer* aufnehmen. Legen Sie am besten in der Domäne eine globale Gruppe *Terminalserver-Benutzer* an. Diese Gruppe fügen Sie den lokalen Gruppen *Remotedesktopbenutzer* auf den Terminalservern hinzu. Wenn Sie einem Benutzer das Anmelden auf einem Terminalserver gestatten wollen, müssen Sie ihn nur noch in die globale Domänengruppe aufnehmen. Will sich ein Benutzer mit einem Terminalserverprogramm verbinden und hat keine Anmeldeberechtigung auf dem Terminalserver, erhält er eine entsprechende Fehlermeldung bei der Anmeldung. Installieren Sie auf dem Server auch noch einen Terminallizenzserver, können Sie auf dem nächsten Fenster auswählen, in welchem Bereich der Lizenzserver Lizenzen ausstellen darf (Abbildung 12.3).

Abbildg. 12.3 Bereich der Terminaldienstelizenzierung konfigurieren



Das Terminaldienstegateway verwendet SSL zum Verbindungsaufbau. Aus diesem Grund können Sie auf der nächsten Seite festlegen, ob Sie ein bestehendes Zertifikat verwenden wollen oder ein neues Zertifikat ausstellen möchten. Zu Testzwecken können Sie auch ein selbstsigniertes Zertifikat verwenden, das der Installationsassistent der Terminaldienste integriert. Auf den nächsten Fenstern können Sie verschiedene Einstellungen vornehmen, die davon abhängig sind, welche Funktionen Sie auf dem Server installiert haben. Wir gehen in den einzelnen Abschnitten dieses Kapitel ausführlicher auf die Konfiguration der einzelnen Funktionen ein. Am Ende des Assistenten können Sie die Installation über die Schaltfläche *Installieren* starten. Nach der Installation erhalten Sie unter Umständen eine Meldung, dass Sie den Lizenzserver aktivieren müssen (Abbildung 12.4). Ohne aktivierten Lizenzserver kann ein Terminalserver nur 120 Tage betrieben werden. Nach dieser Zeit lässt der Server keine Verbindungen zu.

Abbildg. 12.4 Meldung der Terminaldienstelizenzierung nach der Installation



Terminalserverlizenzierung

Sie benötigen für jeden Terminalserver eine Windows Server-Lizenz. Zusätzlich benötigen Sie für jeden Benutzer, wie bei normalen Serverzugriffen auf File- oder Printserver, eine entsprechende Clientzugriffslizenz (Client Access License, CAL). Diese CALs sind bei keinem Betriebssystem integriert, sondern müssen immer gesondert erworben werden. Bei einem Terminalserver benötigen Sie zusätzlich für jeden Client, der sich mit dem Terminalserver verbindet, eine spezielle Terminalserver-Zugriffslizenz (TS-CAL). Diese Lizenz wird pro PC oder pro Benutzer vergeben und gilt nicht pro gleichzeitigem Zugriff. Das heißt, Sie müssen nicht so viele Lizenzen kaufen, wie gleichzeitig Benutzer mit dem Terminalserver arbeiten, sondern so viele Lizenzen, wie Benutzer überhaupt mit dem Terminalserver innerhalb eines Zeitraums arbeiten. Microsoft bietet für die Lizenzierung der TS-CALs die gleichen Lizenzierungsmöglichkeiten wie bei den normalen CALs. Es gibt TS-Geräte-CALs und TS-Benutzer-CALs. Befindet sich der Terminalserver in einem Active Directory, sollten Sie die Terminaldienstelizenzierung auf einem Domänencontroller installieren. Haben Sie in Ihrer Umgebung nur einen Terminalserver, können Sie auch auf diesem die Terminaldienstelizenzierung installieren. Unter Windows Server 2008 haben Sie, wie bei Windows Server 2003, 120 Tage Zeit, bevor Sie den Lizenzierungsdienst auf einem Server installieren und aktivieren müssen. Ein Windows Server 2008-Terminalserver findet in einem Active Directory Lizenzserver automatisch. Der Ablauf bei der Lizenzierung ist folgender:

1. Ein Client verbindet sich mit einem Terminalserver.
2. Der Terminalserver ruft von einem Terminallizenzserver eine Lizenz ab. Hierbei muss es sich nicht um den lokalen Terminalserver handeln. Ein Lizenzserver kann Lizenzen für mehrere Terminalserver zur Verfügung stellen.
3. Der Terminalserver stellt dem Client die Lizenz zur Verfügung.

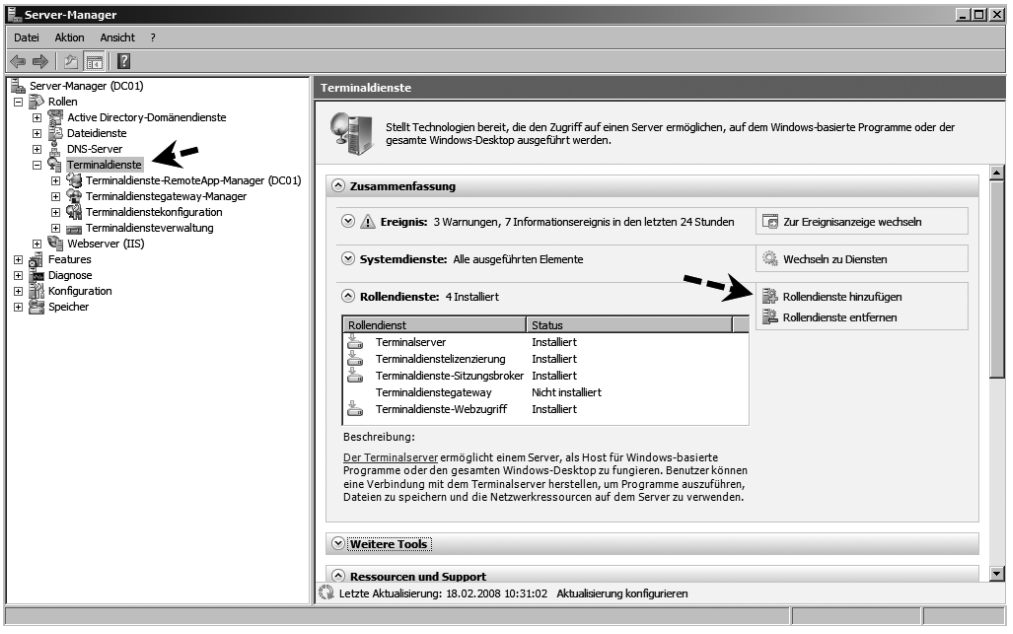
HINWEIS Ein Terminaldienstelizenz-Server unter Windows Server 2008 unterstützt auch die Lizenzierung von Terminalservern unter Windows 2000 Server, Windows Server 2003 und Windows Server 2003 R2. Allerdings unterstützen Terminalserver unter Windows Server 2008 ausschließlich Windows Server 2008-Terminaldienstelizenz-Server.

Installation der Terminaldienstelizenzierung

Um die Terminaldienstelizenzierung unter Windows Server 2008 zu installieren, wählen Sie diese Funktion entweder bereits bei der Installation des Terminalservers aus, oder auch nachträglich. Die Installation führen Sie über das Hinzufügen der Rolle *Terminaldienste* im Server-Manager durch. Haben Sie bereits Terminaldienste installiert und wollen Sie zusätzliche Rollendienste, wie zum Beispiel die Lizenzierung hinzufügen, klicken Sie im Server-Manager auf die Rolle *Terminaldienste* und dann in der Mitte auf *Rollendienste hinzufügen*. Haben Sie bereits alle Rollendienste installiert, ist diese Funktion deaktiviert.

HINWEIS Die Rolle der Terminaldienstelizenzierung benötigt nur sehr geringe Systemressourcen und kann daher ohne weiteres auch direkt auf einem Terminalserver installiert werden. CPU-Last wird so gut wie keine verursacht und der Dienst benötigt maximal 10 MB Arbeitsspeicher. Die Datenbank für die Lizenzen hat pro 6.000 Lizenzen in etwa eine Größe von 5 MB. Der Dienst wird nur aktiv, wenn ein Terminalserver eine Lizenz für einen Client anfordert.

Abbildg. 12.5 Hinzufügen von zusätzlichen Rollendiensten



Die Terminaldienstelizenz-Verwaltung starten Sie über *Start/Verwaltung/Terminaldienste/Terminaldienstelizenzierungs-Manager* (Abbildung 12.6). Haben Sie das Programm gestartet, durchsucht das Programm das Netzwerk und zeigt die gefundenen Lizenzserver an. Nicht aktivierte Lizenzserver werden entsprechend hervorgehoben.

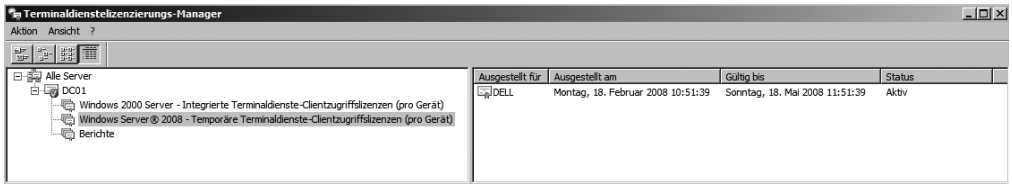
Abbildg. 12.6 Verwalten der Terminaldienstelizenzierung

Um einen Lizenzserver zu aktivieren, klicken Sie mit der rechten Maustaste auf den Servernamen und wählen im Kontextmenü den Befehl *Server aktivieren*. Anschließend können Sie den Server entweder direkt über die Konsole aktivieren, wenn Ihr Lizenzserver an das Internet angebunden ist, oder Sie führen die Aktivierung per Telefon durch. Nachdem ein Lizenzserver aktiviert worden ist, stellt er temporäre Lizenzen aus, die 120 Tage gültig sind. Nach diesem Testzeitraum müssen Ihre Clients allerdings mit permanenten Lizenzen versorgt werden, die Sie im Lizenzserver einspielen müssen. Diese Aktivierung ist kostenlos, nur die TS-CALs, die Sie später brauchen, kosten Geld.

Abbildg. 12.7 Aktivieren der Terminaldienstelizenzierung

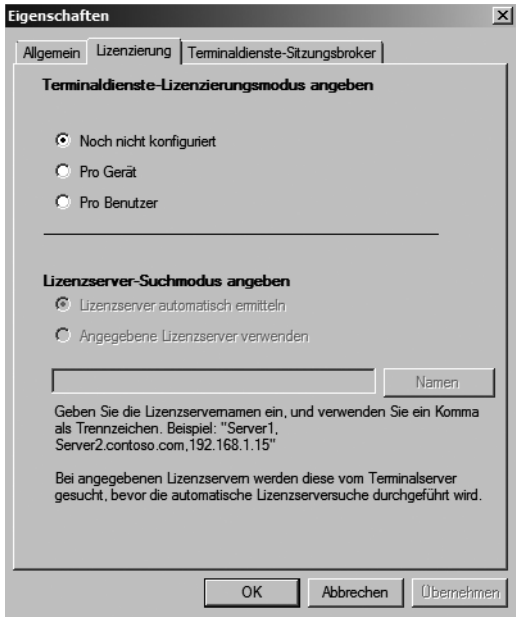
Nach der erfolgreichen Aktivierung wird der Lizenzserver als fehlerfrei dargestellt. Die ausgestellten Lizenzen werden angezeigt, wenn Sie auf die Terminalserverversion klicken, die Sie einsetzen (Abbildung 12.8). Hier sehen Sie auch, wie lange die temporären Lizenzen ihre Gültigkeit verlieren. Neben der Aktivierung muss bei der Installation des Lizenzservers auch der Lizenzmodus festgelegt werden. Diese Vorgänge werden über die Terminaldienstekonfiguration vorgenommen, die wir im nächsten Abschnitt besprechen.

Abbildg. 12.8 Ausgestellte Lizenzen für Terminalserver anzeigen



Ist der Testzeitraum abgeschlossen, können sich Clients solange nicht verbinden, bis Sie TS-CALs einspielen. Hierbei hat sich im Vergleich zu Windows Server 2003 nichts verändert. Im Terminaldienstelizenzierungs-Manager können Sie auch Berichte erstellen, um die Nutzung der Lizenzen zu bestimmten Zeiträumen anzuzeigen. Ausführliche Informationen werden allerdings nur dann angezeigt, wenn sich der Terminalserver und die Arbeitsstationen in einer Active Directory-Domäne befinden. Weitere Optionen der Lizenzierung, wie den Suchmodus für den Lizenzserver oder den Lizenzierungsmodus, können Sie in der *Terminaldienstekonfiguration* über *Start/Ausführen/tsconfig.msc* im Bereich *Lizenzierung* konfigurieren (Abbildung 12.9).

Abbildg. 12.9 Konfiguration der Terminalserverlizenzierung in der Terminaldienstekonfiguration

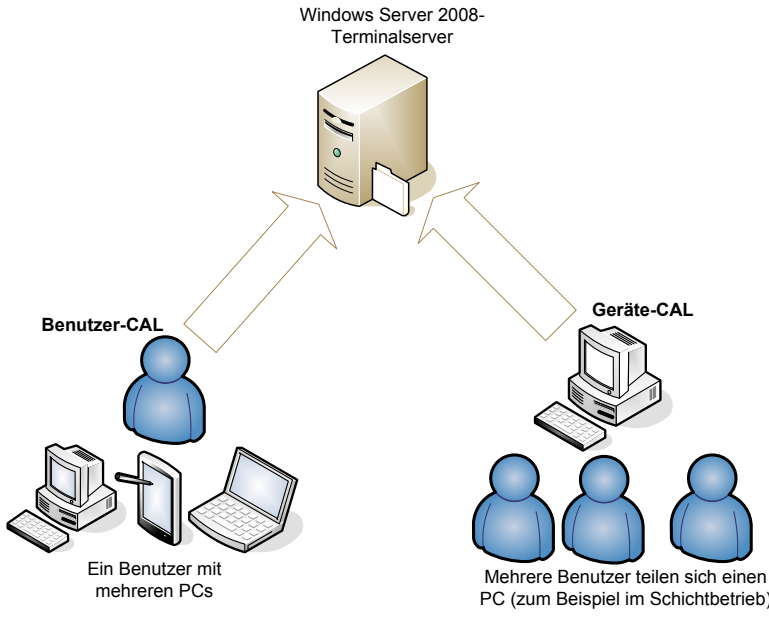


Geräte-Lizenzen (Device-CALs) oder Benutzer-Lizenzen (User-CALs)

Microsoft bietet die beiden Lizenzvarianten *Geräte-Lizenzen* und *Benutzer-Lizenzen* an. Die beiden Lizenzen unterscheiden sich nicht preislich voneinander. Sie müssen bereits bei der Bestellung Ihrer Lizenzen im Voraus planen, welchen Lizenztyp Sie einsetzen wollen. Wenn Sie mit Geräte-CALs lizenzieren, müssen Sie für jeden PC, der auf diesen Server zugreift, eine Lizenz kaufen, unabhängig davon, wie viele Benutzer an diesem PC arbeiten. Wenn Sie PCs betreiben, zum Beispiel im Schichtbetrieb, an denen zu unterschiedlichen Zeiten unterschiedliche Benutzer arbeiten, benötigen Sie für diese PCs nur jeweils eine Geräte-CAL. Im umgekehrten Fall, wenn also ein Benutzer mit mehreren PCs, Notebook oder Smartphones auf den Server zugreift, benötigen Sie für diesen Benutzer mehrere Geräte-CALs, da dieser Benutzer mit mehreren PCs auf den Server zugreift. Auch PCs, auf denen Sie per Terminaldienste-Wegzugriff auf den Server zugreifen, müssen lizenziert werden. Alternativ können Sie auch eine Benutzer-CAL kaufen. Jeder Benutzer mit einer Benutzer-CAL kann an beliebig vielen PCs eine Verbindung mit einem Server aufbauen.

Die CALs müssen eindeutig zugewiesen werden. Sie können daher nicht nur so viele CALs kaufen, wie gleichzeitig Benutzer mit dem Terminalserver arbeiten, sondern müssen die Gesamtzahl Ihrer Arbeitsstationen, Pocket-PCs und sonstiger Geräte lizenzieren, wenn Sie Geräte-Lizenzen kaufen, die mit dem Server eine Verbindung herstellen sollen. Bei Benutzer-Lizenzen müssen diese genau der Anzahl der Benutzer zugewiesen werden, die insgesamt mit dem Terminalserver arbeiten.

Abbildg. 12.10 Lizenzierung mit Benutzer-CALs oder Geräte-CALs



Beispiel-Einsatzszenarien für Lizenzen

Szenario: Lizenzen bei weniger PCs als Mitarbeiter

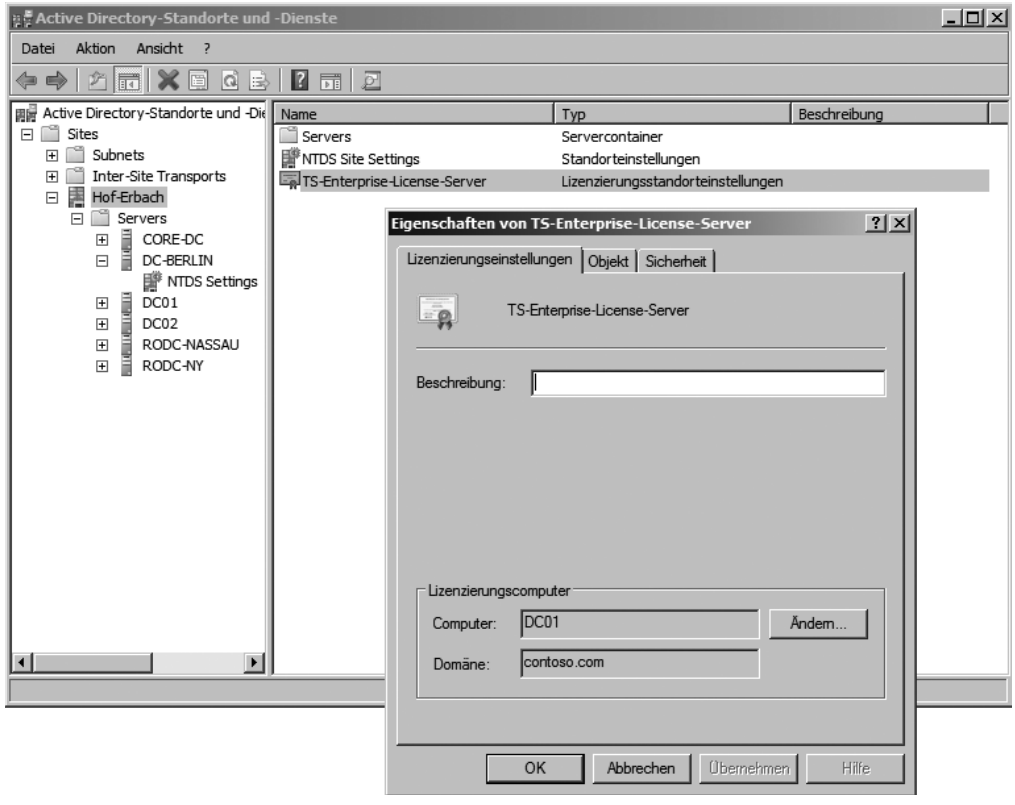
In Ihrem Unternehmen sind beispielsweise 100 Mitarbeiter beschäftigt, von denen jedoch lediglich 63 mit PCs am Terminalserver arbeiten. Wenn Sie Geräte-CALs kaufen, wird jede gekaufte Lizenz einem bestimmten PC zugeordnet. Mit diesen PCs können sich jetzt beliebig viele Mitarbeiter mit dem Terminalserver verbinden, wenn sich diese zum Beispiel PCs im Schichtbetrieb teilen. Wenn neue PCs hinzukommen, müssen Sie für diese PCs weitere Geräte-Lizenzen kaufen.

Szenario: Lizenzen bei mehr PCs als Mitarbeiter

Das nächste Beispiel geht von einer IT-Firma aus, in der 90 Mitarbeiter beschäftigt sind. Von diesen 40 Mitarbeitern arbeiten 25 mit der Windows-Domäne und dem Terminalserver. Jeder dieser Mitarbeiter hat einen PC und ein Notebook, mit denen er am Terminalserver arbeitet, um Dateien auszutauschen oder auf sein Postfach zurückzugreifen. Obwohl in diesem Unternehmen nur 40 Mitarbeiter beschäftigt sind, verbinden sich 50 PCs mit dem Terminalserver. Es müssen in diesem Beispiel daher 50 Geräte-Lizenzen erworben werden. Wenn das Unternehmen seine Lizenzen jedoch als Benutzer-Lizenz erwirbt, werden lediglich 25 Lizenzen benötigt, da nur 25 Benutzer mit dem Terminalserver arbeiten.

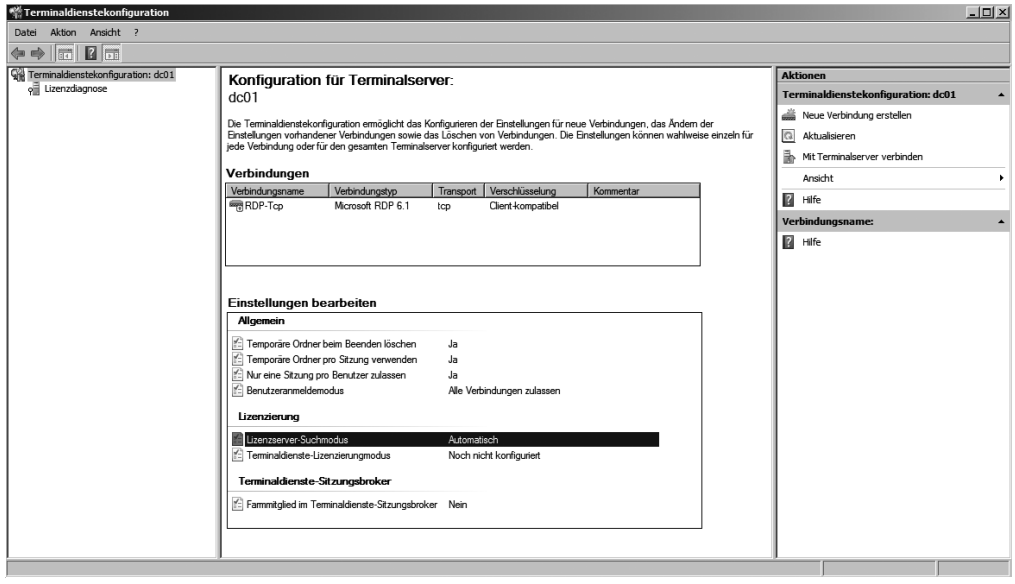
Die Installation der Terminaldienste fügt dem jeweiligen Standort im Active Directory eine neue Lizenzierungsoption hinzu (Abbildung 12.11). Stellen Sie sicher, dass bei der Option *TS-Enterprise-License-Server* ein gültiger Lizenzierungsserver hinterlegt ist. Sie finden diese Einstellungen, wenn Sie im Snap-In *Active Directory-Standorte und -Dienste* den Standort anklicken, auf der rechten Seite des Fensters.

Abbildg. 12.11 Anzeigen des Lizenzservers für Terminalserver



Wenn sich ein Benutzer mit einem Terminalserver verbindet, überprüft der Terminalserver, ob der Client bereits über eine ausgestellte Lizenz verfügt. Hat der Client noch keine Lizenz, baut der Terminalserver eine Verbindung zum Lizenzierungsserver auf, ruft eine Lizenz ab und gibt diese an den Client weiter. Auf dem Terminalserver sollte im Verwaltungsprogramm *Terminaldienstekonfiguration* unter *Einstellungen bearbeiten* zum Eintrag *Lizenzserver-Suchmodus* die Option *Automatisch* angezeigt werden (Abbildung 12.12). Hier kann aber auch manuell ein Lizenzserver hinterlegt werden.

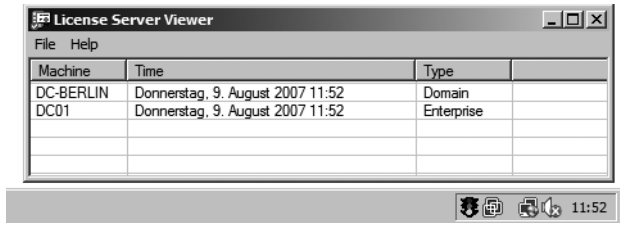
Abbildg. 12.12 Konfigurieren eines Lizenzservers für einen bestimmten Terminalserver



License Server Viewer

Eine weitere Möglichkeit ist der *License Server Viewer* (*Lsview.exe*) aus dem Windows Server 2003 Ressource Kit. Das Tool funktioniert ebenfalls unter Windows Server 2008 und wird auch Bestandteil des neuen Windows Server 2008 Resource Kit sein. Mit diesem Programm können Sie feststellen, ob der Terminalserver eine Verbindung zu einem Lizenzierungsserver aufbauen kann. Sie können sich dieses Tool auf der Seite *http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en* kostenlos aus dem Internet herunterladen.

Abbildg. 12.13 Anzeigen der Terminalserverlizenz-Server im Unternehmen

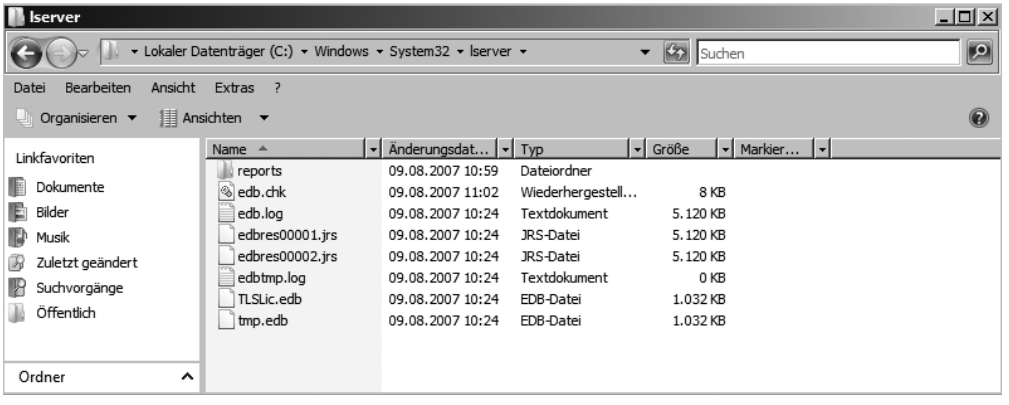


Rufen Sie nach der Installation des Resource Kits das Tool über *Start/Ausführen/lsview* auf. In der grafischen Oberfläche werden die Lizenzserver angezeigt, die durch das Tool gefunden werden. Wenn an dieser Stelle kein Lizenzierungsserver angezeigt wird, wurde auch keine Verbindung aufgebaut und der Terminalserver kann keinen Lizenzserver finden. Unter Umständen hilft in diesem Fall ein Neustart des Lizenzierungsservers und des Terminalservers. Sie können auf dem Terminalserver in der Terminaldienstekonfiguration auch einen Server manuell eintragen. Der License Server Viewer zeigt darüber hinaus in der Taskleiste neben der Uhr mit einer Ampel an, ob eine fehlerfreie Verbindung zum Lizenzserver aufgebaut werden kann.

Backup eines Lizenzservers

Sie sollten in regelmäßigen Abständen eine Sicherung des Lizenzservers durchführen, damit bei einem Serverausfall die Datenbank mit den ausgestellten Lizenzen möglichst nicht verloren geht. Um einen Lizenzserver zu sichern, können Sie die Windows-Datensicherung verwenden. Standardmäßig befindet sich der Pfad im Verzeichnis *\Windows\System32\lserver*.

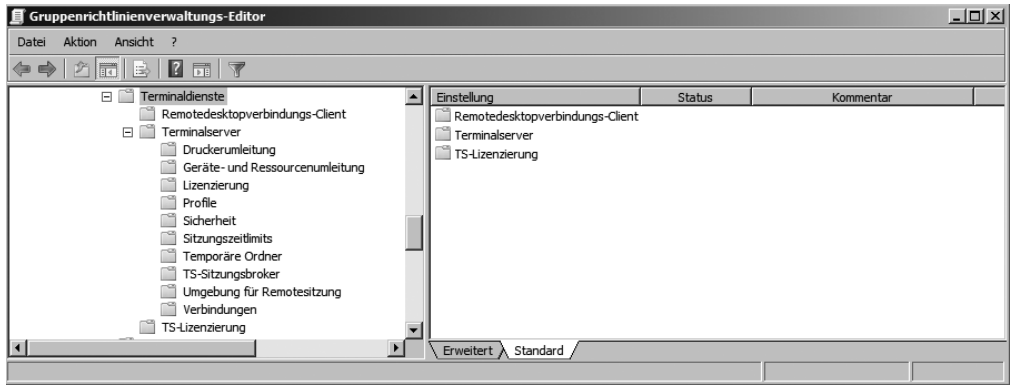
Abbildg. 12.14 Anzeigen und sichern der Terminalserverlizenz-Server-Datenbank



Gruppenrichtlinien für die Terminalserverlizenzierung

Sie können die Arbeitsweise des Lizenzservers mit Gruppenrichtlinien steuern. Wenn Sie eine Gruppenrichtlinie aufrufen, finden Sie die Richtlinien für die Terminalserverlizenzierung in der Konsolenstruktur unter *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Terminaldienste/Terminalserver/Lizenzierung* sowie unter *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Terminaldienste/TS-Lizenzierung* (Abbildung 12.15). Sie können hier zum Beispiel steuern, welche Terminalserver eine Lizenz durch den Lizenzserver erhalten dürfen. Standardmäßig stellt ein Terminalserverlizenz-Server jedem Terminalserver eine Lizenz aus, der eine anfordert.

Abbildg. 12.15 Die Terminalserverlizenzierung lässt sich auch über Gruppenrichtlinien steuern

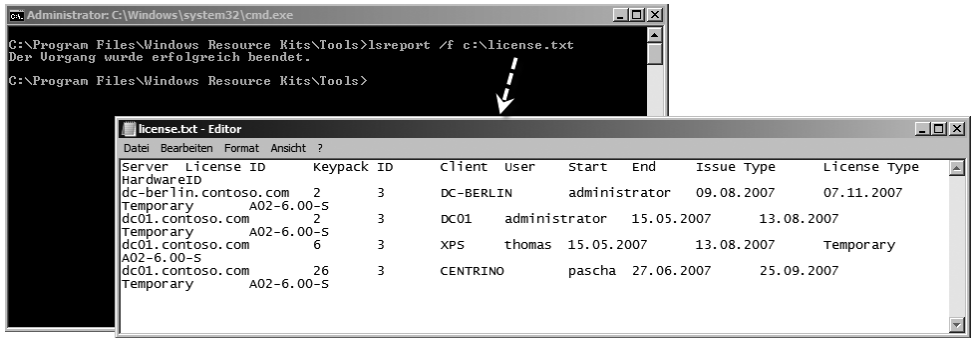


Terminal Server License Tool

Das Terminal Server License Tool (*lsreport.exe*) ist ebenfalls Bestandteil des Windows Server 2003 Resource Kits und funktioniert auch uneingeschränkt unter Windows Server 2008. Mit diesem Tool können Sie die Lizenzdatenbank überprüfen, analysieren und exportieren. Das Tool basiert auf der Befehlszeile und hat verschiedene Optionen, mit denen Sie arbeiten können:

- **/f <Dateiname>** Mit dieser Option können Sie die Ausgabe von *lsreport* in eine Datei umleiten lassen

Abbildg. 12.16 Exportieren der Lizenzdatenbank in eine Textdatei



- **/D start {end}** Diese Option ruft nur Lizenzen auf, die innerhalb eines bestimmten Zeitraums ausgestellt wurden. Wenn Sie *end* weglassen, erfolgt die Ausgabe bis zum aktuellen Datum.
- **/T** Diese Option erfasst nur ausgestellte temporäre Lizenzen
- **/W** Diese Option gibt die Hardware-ID des Clients mit an
- **Serverlist** Mit dieser Option können Sie angeben, welche Lizenzserver abgefragt werden. Standardmäßig werden alle erreichbaren Server abgefragt.

Nacharbeiten zur Installation

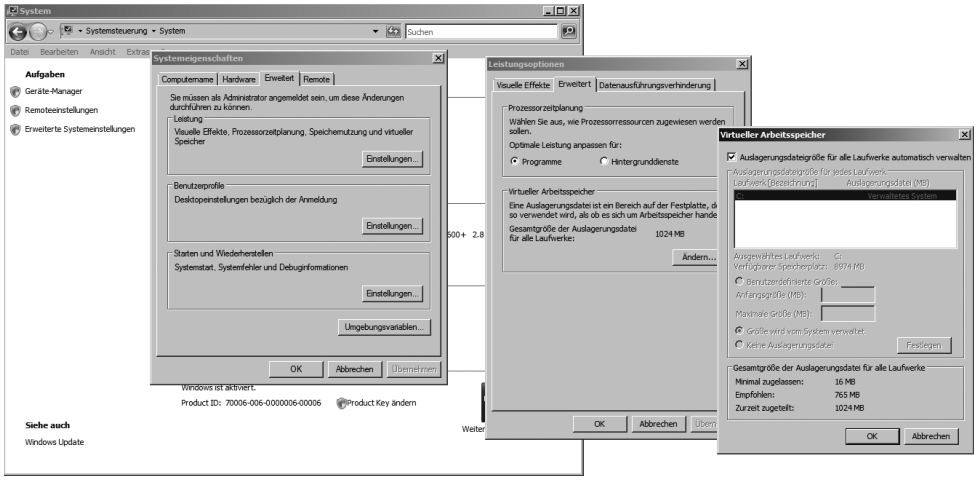
Haben Sie auf einem Server die Terminaldienste installiert, sollten Sie einige empfohlene Nacharbeiten durchführen, die wir im folgenden Abschnitt ausführlicher besprechen.

Auslagerungsdatei auf einem Terminalserver optimieren

Zunächst sollten Sie die Auslagerungsdatei auf eine andere physische Festplatte des Servers verschieben, damit Schreibzugriffe auf die Auslagerungsdatei nicht von Schreibzugriffen auf der Festplatte ausgebremst werden. Wenn keine zweite physische Festplatte zur Verfügung steht, macht ein Verschieben keinen Sinn, da die Auslagerung auf eine Partition, die auf derselben Platte liegt, keine positiven Auswirkungen hat. Zusätzlich sollten Sie die Größe der Auslagerungsdatei auf das 2,5-fache des tatsächlichen Arbeitsspeichers legen. Damit wird die Fragmentierung der Datei minimiert:

1. Die Einstellungen für die Auslagerungsdatei finden Sie über *Start/Systemsteuerung/System/Erweiterte Systemeinstellungen/Leistung/Einstellungen/Erweitert/Virtueller Arbeitsspeicher/Ändern* (Abbildung 12.18).
2. Deaktivieren Sie das Kontrollkästchen *Auslagerungsdateigröße für alle Laufwerke automatisch verwalten*.
3. Aktivieren Sie die Option *Benutzerdefinierte Größe*.
4. Setzen Sie bei *Anfangsgröße* und bei *Maximale Größe* in etwa das 2,5-fache Ihres Arbeitsspeichers ein. Dadurch ist sichergestellt, dass die Datei nicht fragmentiert wird, da sie immer die gleiche Größe hat. Setzen Sie die Größe der Auslagerungsdatei für Laufwerk C: auf 0.
5. Klicken Sie auf *Festlegen*.
6. Schließen Sie alle Fenster und starten Sie den Server neu.

Abbildg. 12.17 Konfiguration der Auslagerungsdatei auf einem Terminalserver

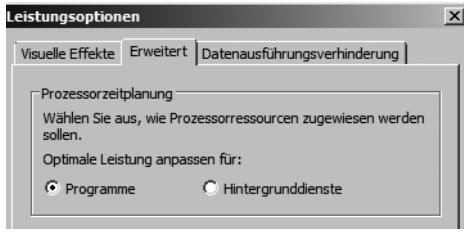


Prozessorzeitplanung anpassen

Standardmäßig ist Windows Server 2008 darauf optimiert, Hintergrunddienste zu beschleunigen. Wenn Sie auf einem Server die Terminaldienste installieren, sollten Sie aber die Optimierung auf

Anwendungen einstellen, damit Benutzer möglichst performant arbeiten können. Diese Einstellung sowie die Konfiguration der Auslagerungsdatei finden Sie an der gleichen Stelle wie die Konfiguration des virtuellen Arbeitsspeichers. Wählen Sie für die Prozessorzeitplanung die Option *Programme* aus (Abbildung 12.18).

Abbildg. 12.18 Optimieren der Prozessorzeitplanung für Terminalserver



Aktualisierung der Treiber

Überprüfen Sie nach der Installation, ob alle Geräte im Geräte-Manager korrekt erkannt worden sind. Vor allem der Treiber der Grafikkarte ermöglicht den Benutzern die Wahl der Farbtiefe, mit der die Sitzung aufgebaut wird. Installieren Sie daher möglichst aktuelle Treiber und stellen Sie sicher, dass jedes Gerät erkannt und mit einem passenden Treiber in das System integriert wurde.

Berechtigungen für Terminalserveranmeldung setzen

Standardmäßig dürfen sich nur Administratoren auf einem Windows Server 2008-Server anmelden. Damit sich Benutzer auf einem Terminalserver anmelden können, müssen Sie diese auf dem Terminalserver in die lokale Benutzergruppe *Remotedesktopbenutzer* aufnehmen. Legen Sie am besten in der Domäne eine globale Gruppe *Terminalserver-Benutzer* an. Diese Gruppe fügen Sie den lokalen Gruppen *Remotedesktopbenutzer* auf den Terminalservern hinzu. Wenn Sie einem Benutzer das Anmelden auf einem Terminalserver gestatten wollen, müssen Sie ihn nur noch in die globale Domänengruppe aufnehmen. Wenn sich ein Benutzer mit einem Terminalserverprogramm verbinden will und keine Anmeldeberechtigung auf dem Terminalserver hat, erhält er eine entsprechende Fehlermeldung bei der Anmeldung.

Terminal Services Easy Print Driver

Das Thema Drucken in den Terminaldiensten ist schon seit Windows NT 4.0 Terminalserver Edition ein heißes Thema und wird auch unter Windows Server 2008 wieder viele Administratoren beschäftigen. Microsoft hat seit Windows NT 4.0 Terminalserver Edition die Einbindung von Druckern in eine Terminalserver-Umgebung immer wieder verbessert. Auch in Windows Server 2008 wurden wieder viele Verbesserungen eingeführt. Eine der Neuerungen ist der *Terminal Services Easy Print Driver*, der die Druckaufträge verschiedener Drucker an den Client umleiten kann. Auch in den Gruppenrichtlinien wurden viele Einstellungen für die Konfiguration von Druckern integriert. Damit Sie den neuen Terminal Services Easy Print Driver verwenden können, müssen Sie den RDP Client 6.1, also Windows Vista SP1, verwenden. Zusätzlich muss dazu .NET Framework 3.0 Service Pack 1 installiert werden. Mit diesem neuen Druckertreiber wird die Verfügbarkeit für Drucker in Terminalserverumgebungen deutlich verbessert. Der Druckertreiber unterstützt eine Vielzahl neue-

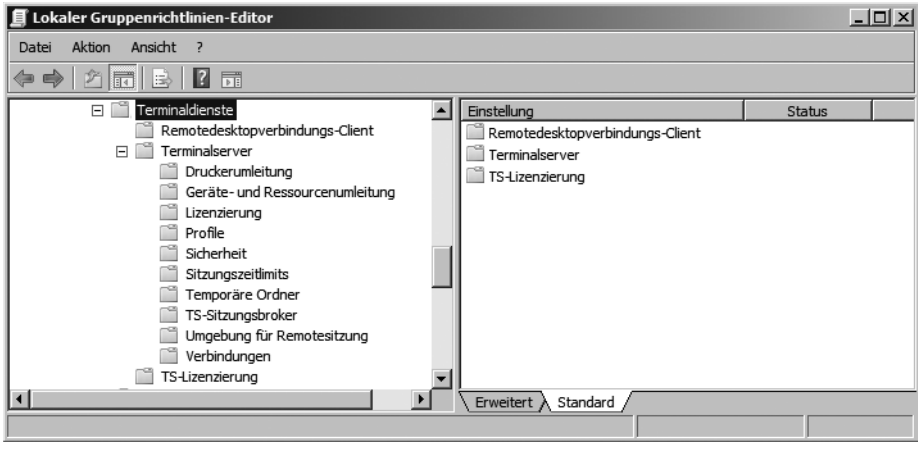
rer und älterer Drucker, sodass auf einem Terminalserver nicht unbedingt zahlreiche Druckertreiber installiert werden müssen. Der Treiber unterstützt für die kompatiblen Drucker alle Features, nicht nur die grundlegenden Funktionen. Auch die Performance bei der Übertragung des Druckauftrages wird durch den Treiber verbessert. Unterstützen Clients diesen universalen Druckertreiber nicht, muss auf dem Terminalserver weiterhin ein aktueller Treiber der Drucker installiert werden. Auf dem Server wird dazu ein Abbild des Druckertreiber des Clients angezeigt, aber nicht installiert. Wird in der Sitzung gedruckt, wird der Druck in eine XPS-Datei umgeleitet und zum Client geschickt, auf dem der Druck schließlich auf dem Drucker ausgegeben wird. Damit der neue Terminal Services Easy Print Driver genutzt werden kann, muss nichts auf dem Server installiert werden. Die auf dem Client verfügbaren Drucker werden auf den Server übernommen, sofern diese kompatibel sind. Auch die spezifischen Einstellungen des Druckers werden auf dem Server angezeigt und beim Abrufen wieder auf den Client zurückgeleitet. Ob Drucker umgeleitet werden, muss im RDP-Client eingestellt werden. Auf der Registerkarte *Lokale Ressourcen* auf dem Client muss dies zunächst aktiviert werden.

TIPP Unterstützen Ihre Unternehmensdrucker den neuen Terminal Services Easy Print Driver nicht, können Sie auch unter Windows Server 2008 den Weg einer Druckermapping-Datei gehen. Diese Möglichkeit gibt es bereits seit Windows 2000 Server. Dabei kann über eine spezielle Datei mehreren Druckern der gleiche Treiber zugeordnet werden. Sehen Sie sich dazu den Microsoft Knowledge Base-Artikel *http://support.microsoft.com/kb/239088/en-us* oder *http://support.microsoft.com/kb/239088/de-de* an.

Neue Gruppenrichtlinien für die Steuerung von Druckern

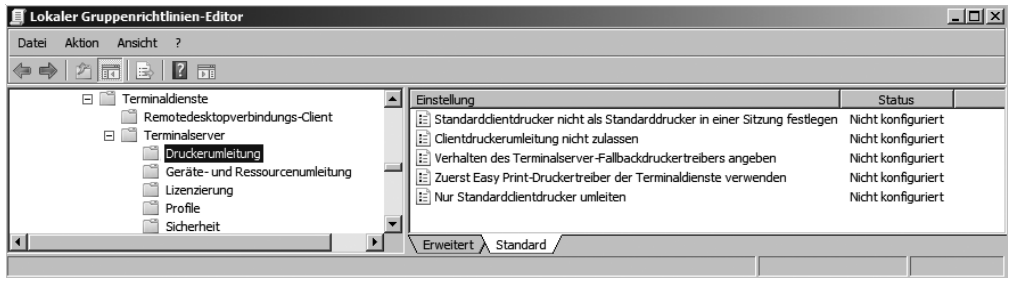
In Windows Server 2008 gibt es auch neue Möglichkeiten, die Anbindung von Druckern über Gruppenrichtlinien zu steuern. Die meisten Einstellungen für Gruppenrichtlinien werden im Gruppenrichtlinien-Editor unter *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Terminaldienste* vorgenommen (Abbildung 12.19).

Abbildg. 12.19 Die Terminaldienste in Windows Server 2008 können jetzt effizient mit Gruppenrichtlinien gesteuert werden



Die Verwaltung von Druckern findet über den Untereintrag *Terminalserver/Druckerumleitung* statt. Hier können auch Einstellungen des Easy Print Drivers angepasst werden (Abbildung 12.20).

Abbildg. 12.20 Die Umleitung von Druckern kann ebenfalls über Gruppenrichtlinien gesteuert werden



HINWEIS Wird die Richtlinie *Zuerst Easy Print-Druckertreiber der Terminaldienste verwenden* aktiviert, versucht ein Terminalserver zuerst diesen Treiber zu verwenden, bevor ein anderer Treiber installiert wird. Auch wenn diese Richtlinie nicht konfiguriert wird, verwendet der Terminalserver standardmäßig zuerst den Easy Print Driver. Unterstützt der Drucker diesen Treiber nicht, sucht der Terminalserver als Nächstes lokal nach einem passenden Treiber. Findet der Server keinen Treiber, kann der Drucker in der Terminalsitzung nicht verwendet werden. Standardmäßig ist diese Richtlinie nicht konfiguriert.

Wird diese Einstellung deaktiviert, versucht der Server zunächst einen Druckertreiber zu finden, der kompatibel für den Drucker ist, und verwendet dann erst den Easy Print Driver.

Installation von Applikationen

Wollen Sie auf einem Terminalserver Software für die Benutzer installieren, sollten Sie darauf achten, dass die entsprechende Software auch mit der Installation auf einem Terminalserver kompatibel ist. Die aktuellen Microsoft-Programme aus dem Office-Paket sind standardmäßig kompatibel mit der Installation auf einem Terminalserver. Allerdings können OEM- oder MSDN-Versionen von Office 2007 nicht auf Terminalservern installiert werden.

Installations- und Ausführungsmodus konfigurieren

Installieren Sie eine Applikation auf einem Terminalserver, sollten Sie den Server in den Installationsmodus versetzen. Sie können dazu den Befehl *change user* in der Befehlszeile verwenden. Mit *change user /install* wird der Terminalserver in den Installationsmodus versetzt. Sie können diesen Befehl eingeben und danach die Software wie auf jedem anderen Computer installieren. Durch den Befehl werden im Systemverzeichnis INI-Dateien für die Anwendung erstellt. Diese Dateien werden als Masterkopien für benutzerspezifische INI-Dateien verwendet. Wenn die Anwendung das erste Mal ausgeführt wird, durchsucht sie das Basisverzeichnis nach ihren INI-Dateien. Wenn sich die INI-Dateien nicht im Basisverzeichnis, sondern im Systemverzeichnis befinden, werden sie von den Terminaldiensten in das Basisverzeichnis kopiert. So wird gewährleistet, dass jeder Benutzer über

eine eindeutige Kopie der INI-Dateien der Anwendung verfügt. Neue INI-Dateien werden im Basisverzeichnis erstellt. Jeder Benutzer muss über eine eindeutige Kopie der INI-Dateien für eine Anwendung verfügen. Dadurch wird verhindert, dass verschiedene Benutzer über inkompatible Anwendungskonfigurationen verfügen. Wenn sich das System im Installationsmodus befindet, finden mehrere Aktionen statt:

- Von allen erstellten Registrierungseinträgen werden unter *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install* Schattenkopien erstellt.
- Zu *HKEY_CURRENT_USER* hinzugefügte Schlüssel werden in den Schlüssel *\Software* kopiert.
- Zu *HKEY_LOCAL_MACHINE* hinzugefügte Schlüssel werden in den Schlüssel *\Machine* kopiert.
- Wenn das Windows-Verzeichnis von der Anwendung durch Systemaufrufe abgefragt wird, gibt der Terminalserver das Verzeichnis *Systemroot* zurück.
- Werden Einträge in der INI-Datei mithilfe von Systemaufrufen hinzugefügt, werden sie zu den INI-Dateien im Verzeichnis *Systemroot* hinzugefügt.

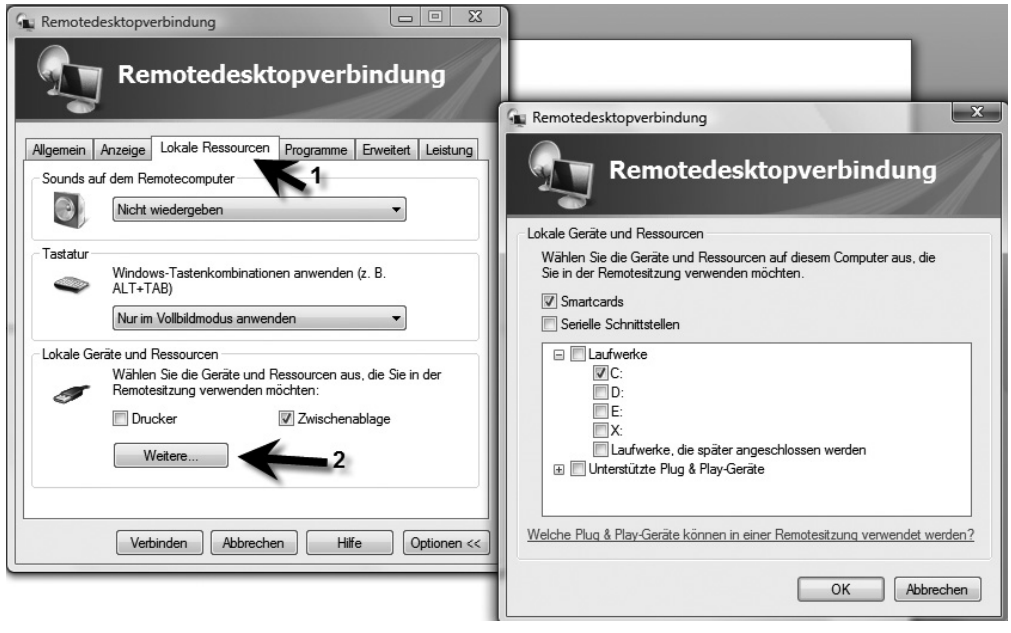
Kehrt das System mit *change user /execute* in den Ausführungsmodus zurück und versucht die Anwendung einen nicht vorhandenen Registrierungseintrag unter *HKEY_CURRENT_USER* zu lesen, wird von den Terminaldiensten überprüft, ob eine Kopie des Schlüssels im Registry-Schlüssel *\Terminal Server\Install* vorhanden ist. Ist dies der Fall, werden die Schlüssel an den entsprechenden Speicherort unter *HKEY_CURRENT_USER* kopiert. Versucht die Anwendung eine nicht vorhandene INI-Datei zu lesen, wird diese INI-Datei von den Terminaldiensten im Systemstamm gesucht. Befindet sich die INI-Datei im Systemstamm, wird sie in das Unterverzeichnis *\Windows* des Basisverzeichnisses des Benutzers kopiert. Fragt die Anwendung das Verzeichnis *Windows* ab, gibt der Terminalserver das Unterverzeichnis *\Windows* des Basisverzeichnisses des Benutzers zurück. Melden sich Benutzer an, wird von den Terminaldiensten überprüft, ob die eigenen INI-Dateien des Systems aktueller sind als die INI-Dateien auf dem Computer. Ist die Version des Systems aktueller, wird die INI-Datei entweder ersetzt oder mit der aktuelleren Version zusammengeführt. Sind die Systemregistrierungswerte im Schlüssel *\Terminal Server\Install* aktueller sind als die Version unter *HKEY_CURRENT_USER*, wird die Version der Schlüssel gelöscht und durch die neuen Schlüssel aus *\Terminal Server\Install* ersetzt. Registrierungseinstellungen in *HKEY_CURRENT_USER* werden manchmal nicht bei der Installation, sondern beim ersten Ausführen eines Programms erstellt. Wird das Programm nicht ausgeführt, während der Installationsmodus noch aktiv ist, werden die *HKEY_CURRENT_USER*-Einstellungen nicht in *HKEY_LOCAL_MACHINE* kopiert. Führt ein Benutzer das Programm erstmals aus, wird *HKEY_CURRENT_USER* mit den Standardeinstellungen geladen. Reichen diese Standardeinstellungen nicht aus, müssen für jeden Benutzer individuelle Anpassungen vorgenommen werden. Um dieses Problem auf Terminalservern zu vermeiden, sollte das Programm einmal ausgeführt werden, bevor der Installationsmodus auf einem Terminalserver verlassen wird. Mit *change user /execute* wird der Terminalserver wieder in den Ausführungsmodus versetzt. Wenn Sie den Terminalserver durchstarten, befindet er sich immer im ausführenden Modus, auch wenn der heruntergefahren wurde, weil zuvor die Option */install* ausgeführt wurde. Mit *change user /query* fragen Sie den aktuellen Status des Servers ab. Unabhängig davon, wie Sie eine Applikation auf dem Terminalserver installieren, sollten Sie nach der Installation in einer Terminalserversitzung überprüfen, ob die Applikation auf dem Terminalserver funktioniert. Um einen zuverlässigen Test durchzuführen, sollten Sie die Applikation möglichst in zwei gleichzeitig laufenden Sitzungen starten, da erst in diesem Fall die Terminalserverkompatibilität sichergestellt ist.

HINWEIS Installieren Sie eine Anwendung über eine **.msi*-Datei, müssen Sie diesen Befehl nicht verwenden, sondern können die Installation wie auf einem normalen PC ohne weitere Eingaben durchführen. In MSI-Dateien sind die entsprechenden Optionen für die Installation auf Terminalservern bereits gesetzt.

Remote Desktop Client (RDP) 6.1

Terminalserver unter Windows Server 2008 können in den Terminalsitzungen deutlich mehr Geräte des angeschlossenen Clients verwenden. So werden in Terminalsitzungen jetzt auch Digitalkameras und Media Player unterstützt, die an den Terminalserver-Client angeschlossen sind. Auch das Plug&Play für diese Geräte wird unterstützt. Mit Windows Vista und Windows Server 2008 wird der neue Client für RDP 6.0 ausgeliefert. Wollen Sie die Weiterleitung von an den Client angeschlossenen Plug&Play-Geräten in die Terminalserver-Sitzung erlauben, können Sie im RDP-Client über *Optionen/Lokale Ressourcen/Weitere* die Einstellungen sehr spezifisch vornehmen (Abbildung 12.21).

Abbildg. 12.21 Konfiguration der Weiterleitung von lokalen Ressourcen im neuen RDP-Client



Microsoft stellt auf der Internetseite *http://go.microsoft.com/fwlink/?LinkId=79373* die Software für Windows Server 2003 und Windows XP zur Verfügung. Die Terminaldienste unterstützen jetzt auch höhere Auflösungen, zum Beispiel 1.680 × 1.050 oder 1.900 × 1.200. Auch der Einsatz von Mehrmonitor-Lösungen wird unterstützt. Durch die neue *Monitor-Spanning* genannte Funktion können Terminalserversitzungen jetzt über mehrere Monitore gestreckt werden. Die maximale Auflösung ist 4.096 × 2.048. Neben den herkömmlichen Auflösungen im 4:3-Format unterstützt Windows Server 2008 auch Auflösungen im 16:9- und 16:10-Format. Damit alle neuen Funktionen der Terminal-

dienste in Windows Server 2008 verwendet werden können, empfiehlt Microsoft den Einsatz des neuen Remote Desktop 6.0, der Bestandteil in Windows Vista und Windows Server 2008 ist.

TIPP Sie finden den Client für den Remotedesktop über *Start/Alle Programme/Zubehör/Remotedesktopverbindung*. Schneller können Sie den Client aufrufen, wenn Sie im Suchfeld des Startmenüs den Befehl *mstsc.exe* eingeben:

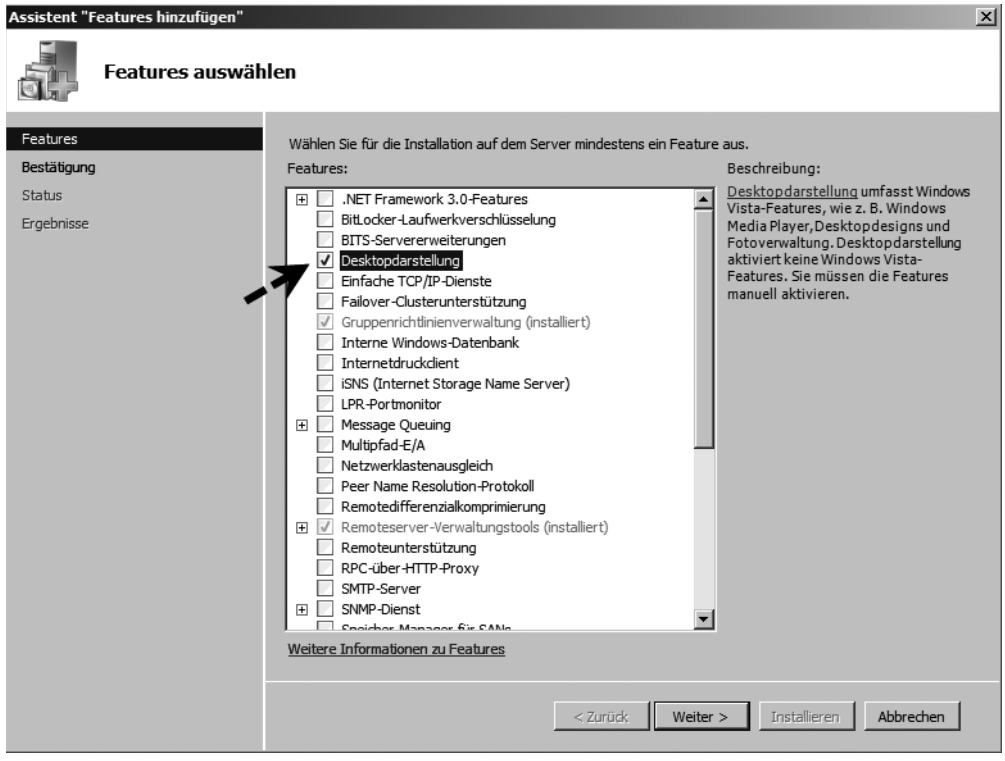
- Über den Befehl *mstsc /w:<Auflösung> /h:<Auflösung>* können Sie beim Starten des Clients die Auflösung angeben.
- Geben Sie *mstsc /span* ein, kann die Terminalserversitzung in einer Mehrmonitor-Umgebung genutzt werden. Damit die Erweiterung auf mehrere Monitore funktioniert, müssen alle mit der gleichen Auflösung betrieben werden. Die Monitore müssen nebeneinander und können nicht übereinander angeordnet werden. Die maximale Auflösung über alle Monitore verteilt kann 4.096 x 2.048 nicht übersteigen. Über die Option *span:i:1* wird die Erweiterung in einer **.rdp*-Datei hinterlegt.

Erweiterte Desktopdarstellung (Desktop Experience)

Installieren Sie auf einem Terminalserver über den Server-Manager das Feature *Desktopdarstellung*, erhalten die Anwender in einer Terminalserversitzung die gleiche Oberfläche wie bei Windows Vista. Ohne diese Funktion sieht die Oberfläche in den Terminalsitzungen weniger modern aus. Windows Server 2008 unterstützt für die Darstellung in Terminalserversitzungen auch die Aero-Funktionen von Windows Vista. Allerdings muss dazu die Hardware auf dem Client die Aero-Darstellung unterstützen. Die Hardware im Terminalserver selbst muss Aero nicht unterstützen. Nach der Installation der Desktopdarstellung müssen Sie den Server neu starten. Neben Aero wird auch die Windows-Fotogalerie und der Windows Media Player 11 installiert. Auch Desktopdesigns können aktiviert werden.

Damit Sie die Aero-Funktionen in einer Terminalserversitzung nutzen können, müssen Sie das Thema zunächst konfigurieren. Der erste Schritt dazu ist, dass Sie den Dienst *Designs* im Dienstemanager auf dem Terminalserver auf *Automatisch* stellen und starten. Anschließend können Sie den Desktop und die grafische Darstellung anpassen. Eine weitere interessantere Funktion ist die Schriftartglättung im RDP Client 6.0. Mit dieser Funktion werden ClearType-Schriftarten in einer Terminalserversitzung besser dargestellt. Sie können die Funktion *Schriftartglättung* in den Optionen des RDP-Clients über die Registerkarte *Erweitert* aktivieren (Abbildung 12.23). ClearType dient dazu, Computerschriftarten klar und mit geglätteten Kanten anzuzeigen. Bildschirmtext kann mithilfe von ClearType detaillierter dargestellt werden und ist daher über einen längeren Zeitraum besser zu lesen, da die Augen nicht belastet werden. Jedes Pixel in einer Schriftart besteht aus drei Teilen: Rot, Blau und Grün. ClearType verbessert die Auflösung, indem die einzelnen Farben im Pixel aktiviert und deaktiviert werden. Ohne ClearType muss das gesamte Pixel aktiviert oder deaktiviert werden. Durch diese genauere Steuerung der Rot-, Bau- und Grünanteile eines Pixels kann die Deutlichkeit auf einem LCD-Monitor deutlich verbessert werden. Sie können aber auch herkömmliche Monitore (CRT) verwenden.

Abbildg. 12.22 Installation des Features *Desktopdarstellung* für Terminalserversitzungen



Optimalere Ergebnisse erreicht man aber beim Einsatz von LCD-Monitoren, da ClearType für LCD entwickelt und optimiert wurde. ClearType nutzt die Besonderheit der LCD-Technologie, bei der Pixel sich an einer festen Position befinden, indem Teile des Pixels aktiviert und deaktiviert werden. ClearType funktioniert auf einem CRT-Monitor nicht auf die gleiche Weise, da in einem CRT-Monitor ein Elektronenstrahl verwendet wird, um Pixel anzuregen oder zu bewegen, anstatt die Pixel an festen Positionen zu belassen. Dennoch kann der Einsatz von ClearType die Deutlichkeit auf CRT-Monitoren verbessern, da die gezackten Kanten der einzelnen Buchstaben durch ClearType geglättet werden. Dies wird als *Antialiasing* bezeichnet. Die ClearType-Technologie funktioniert daher besonders gut bei LCD-Geräten, einschließlich Flachbildschirmen und Notebooks.

HINWEIS Standardmäßig verwendet der RDP-Client 6.0 eine Farbtiefe von 32 Bit. Dieser Modus ist der effizienteste im Kompromiss zwischen Darstellung und Netzwerkverkehr. Eine Herabstufung auf 24 oder 16 Bit bringt keinerlei Geschwindigkeitsvorteile, schränkt aber die Anzeige ein.

Abbildg. 12.23 Aktivierung der Schriftartglättung in RDP 6.0

Befehlszeilenparameter für den Remotedesktop-Client

Der RDP-Client von Windows Server 2008 und Windows Vista hat einige neue Optionen für die Befehlszeile:

mstsc [<Verbindungsdatei>] [/v:<server[:port]>][/console] [/f[ullscreen]] [/w:<width>] [/h:<height>] [/public] | [/span] [/edit "Verbindungsdatei"] [/migrate] [/?] /v:<Server[:Port]>

- **/console** Ermöglicht eine Verbindung mit der Konsolensitzung älterer Versionen von Windows. Diese Einstellung funktioniert unter Windows Vista oder Windows Server 2008 nicht.
- **/f** Startet die Remotedesktopverbindung im Vollbildmodus
- **/w:<Breite>** Gibt die Breite des Fensters *Remotedesktopverbindung* an
- **/h:<Höhe>** Gibt die Höhe des Fensters *Remotedesktopverbindung* an
- **/public** Führt die Remotedesktopverbindung im öffentlichen Modus aus. Im öffentlichen Modus erfolgt durch den RDP-Client keine Zwischenspeicherung der Daten im lokalen System. Verwenden Sie den öffentlichen Modus, wenn Sie zum Beispiel eine Verbindung von einem System in einem Konferenzzentrum zu einem Geschäftsserver herstellen.
- **/span** Stimmt die Remotedesktopbreite und -höhe mit dem lokalen virtuellen Desktop ab und verteilt dies bei Bedarf monitorübergreifend. Beachten Sie, dass die Monitore alle die gleiche Höhe haben und parallel ausgerichtet sein müssen.

- **/edit** Öffnet die angegebene RDP-Verbindungsdatei zum Bearbeiten. RDP-Dateien werden verwendet, um die Verbindungsinformationen für ein bestimmtes Remotesystem zu speichern.
- **/migrate** Wandelt ältere Verbindungsdateien, die mit dem Clientverbindungsmanager erstellt wurden, in neue RDP-Verbindungsdateien um

TIPP Auf der Internetseite *http://support.microsoft.com/?kbid=885187* erhalten Sie ausführliche Informationen, wie Sie gespeicherte **.rdp*-Dateien nachträglich mit einem Texteditor bearbeiten. Die Einstellungen gelten für Windows Server 2003/2008 und für Windows XP/Vista.

Display-Daten-Priorisierung

Die Terminaldienste in Windows Server 2008 reservieren 70% der verfügbaren Bandbreite für die Übertragung des Grafik-, Maus- und Tastaturverkehrs. Drucker, Zwischenablage und die anderen Funktionen erhalten nur 30 % der verfügbaren Bandbreite. Sie können die Einstellungen über die Registry an Ihre Bedürfnisse anpassen. Die jeweiligen Einstellungen finden Sie im Registryschlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD*. Die folgenden Werte werden als *DWORD-Wert (32-Bit)* erstellt. Ändern Sie die Werte ab, müssen Sie den Terminalserver neu starten, damit die Änderungen eingelesen werden.

- **FlowControlDisable** Weisen Sie diesem Wert den Wert 1 zu, wird die Display-Daten-Priorisierung deaktiviert. In diesem Fall wird der Netzwerkverkehr nach dem Prinzip First-In/First-Out behandelt. Der Standardwert dieses Wertes ist 0.
- **FlowControlDisplayBandwidth** Mit Hilfe dieses Wertes setzen Sie die Bandbreitenverteilung auf Basis der relativen Gewichtung fest. Der Standardwert ist 70, der Maximalwert 255.
- **FlowControlChannelBandwidth** Dieser Wert ist für die Steuerung der restlichen Kanäle im Netzwerkverkehr. Diese sind zum Beispiel Druckverkehr, Zwischenablage oder Dateiübertragungen. Der Standardwert ist 30, der Maximalwert 255.
- **FlowControlChargePostCompression** Hier legen Sie fest, ob die Bandbreite auf Basis des Netzwerkverkehrs vor der Komprimierung oder nach der Komprimierung berechnet werden soll. Standardmäßig findet die Berechnung durch den Wert 0 nach der Komprimierung statt.

Existieren diese Unterschlüssel bei Ihnen nicht, können Sie diese nachträglich auch manuell erstellen.

Umleitung von Digitalkameras und Mediaplayer

Ebenfalls neu ist die Möglichkeit, dass Plug&Play-Geräte wie Digitalkameras und Mediaplayer auf den Terminalserver umgeleitet werden können. Dazu muss auf dem RDP-Client auf die Registerkarte *Lokale Ressourcen* gewechselt werden. Über die Schaltfläche *Weitere* kann die Umleitung von Plug&Play-Geräten aktiviert werden. Diese Umleitung funktioniert auch, wenn das Gerät nach dem Verbindungsaufbau mit dem Terminalserver verbunden wird.

Abbildg. 12.24 Auch lokale Plug&Play-fähige Geräte können mit dem RDP-Client auf den Terminalserver umgeleitet werden

HINWEIS Der Remote Desktop Client 6 unterstützt für Terminalserver unter Windows Server 2008, auch die Umleitung für Geräte, welche die Funktion *Microsoft Point of Service* nutzen, also zum Beispiel Kassen oder Inventurgeräte (*http://www.microsoft.com/windows/embedded/de-de/wepos/default.mspx*). Dazu muss auf dem Terminalserver noch die Erweiterung *Microsoft Point of Service for .NET 1.11* von der Internetseite *http://go.microsoft.com/fwlink/?linkid=66169* installiert werden.

Verwalten eines Terminalservers

In den folgenden Abschnitten gehen wir auf die Verwaltung der neuen Funktionen ein und beleuchten zunächst ausführlich die Konfiguration und Verwaltung der Standardfunktionen eines Terminalservers. Bevor Sie sich mit speziellen Funktionen wie dem Gateway oder Webzugriff auseinandersetzen, sollten Sie zunächst die Standardverwaltung eines Servers verstehen. Sie finden die Programme zur Verwaltung eines Terminalservers in der Programmgruppe *Verwaltung/Terminaldienste* im Startmenü.

Terminaldienstekonfiguration

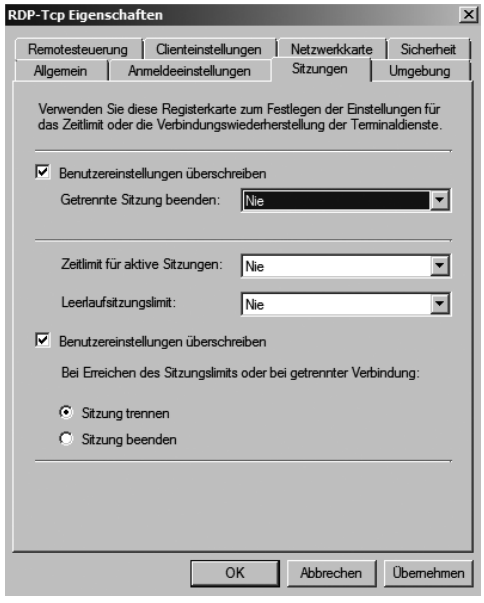
Mit dem Tool *Terminaldienstekonfiguration* werden die maßgeblichen Verbindungseinstellungen für einen Terminalserver konfiguriert. Sie können das Programm auch über *tsconfig.msc* starten. Im Bereich Verbindungen finden Sie die aktuelle RDP-Tcp-Verbindung des Terminalservers, über den die Anwender ihre Sitzungen öffnen. Wenn Sie die Eigenschaften der RDP-Verbindung öffnen, stehen Ihnen verschiedene Registerkarten zur Verfügung, mit denen Sie das RDP-Protokoll an Ihre Bedürfnisse anpassen können (Abbildung 12.25).

Abbildg. 12.25 Konfigurieren des RDP-Protokolls auf einem Terminalserver

Wenn Sie die Eigenschaften der RDP-Verbindung aufrufen, stehen Ihnen folgende Registerkarten zur Verfügung:

- Auf der Registerkarte *Allgemein* legen Sie die Verschlüsselungsstufe fest, mit der Clients über diese RDP-Verbindung Sitzungen aufbauen. Beachten Sie, dass die Geschwindigkeit der einzelnen Sitzungen abnimmt, je höher Sie die Verschlüsselung einstellen.
- Auf der Registerkarte *Anmeldeeinstellungen* können Sie festlegen, dass alle Benutzer, die über diese RDP-Verbindung eine Sitzung aufbauen, mit dem gleichen Benutzerkonto angemeldet werden. Wahlweise können Sie das Kennwort offen lassen, damit die Benutzer das Kennwort eingeben müssen. Eine solche Konfiguration wäre zum Beispiel für ein Internetcafé oder einen Informationsschalter sinnvoll.
- Auf der Registerkarte *Sitzungen* bestimmen Sie, wie sich die Terminalserversitzungen der Benutzer bei den verschiedenen Zuständen verhalten sollen (Abbildung 12.26). Diese Einstellungen gelten für alle Benutzer, die sich mit dem Terminalserver verbinden.

Abbildg. 12.26 Konfigurieren der Sitzungen auf einem Terminalserver



Für einzelne Benutzer können identische Einstellungen in den Eigenschaften des Benutzerkontos auf der Registerkarte *Sitzungen* durchgeführt werden. Benutzersitzungen können folgende Zustände annehmen:

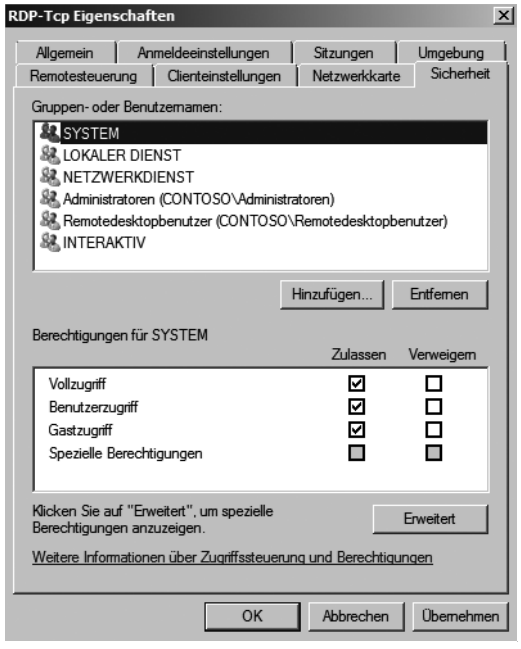
- **Aktiv** Der Benutzer ist mit der Sitzung verbunden und arbeitet. Es werden Daten zwischen Client und Server übermittelt.
- **Leerlauf** Der Benutzer ist verbunden, es findet allerdings zwischen Server und Client kein Datenverkehr statt.
- **Getrennt** Der Benutzer hat seinen Client von der Sitzung getrennt, sich aber nicht abgemeldet. Die Sitzung bleibt auf dem Terminalserver bestehen und alle Programme laufen weiter. Der Benutzer kann sich erneut mit dem Terminalserver verbinden und wird automatisch wieder mit seiner laufenden Sitzung verbunden.
- **Zurückgesetzt** Die Sitzung ist nicht mehr vorhanden, alle Programme werden beendet. Dieser Status ähnelt dem Abmelden von einem Computer.

  Sie können einstellen, dass eine Sitzung nach einer bestimmten Zeit getrennt wird oder getrennte Sitzungen zurückgesetzt werden. Sie definieren hier Grenzwerte für spätere Sitzungen. Diese Einstellungen sind für alle Benutzer bindend.

TIPP Sie sollten die Option *Getrennte Sitzungen beenden* aktivieren. Dadurch ist sichergestellt, dass getrennte Sitzungen nach einer gewissen Zeit, beispielsweise zwei Stunden, beendet werden und den Server nicht mehr belasten. Wenn ein Benutzer durch Netzwerkprobleme getrennt wird, besteht die Möglichkeit, dass er sich innerhalb dieser zwei Stunden wieder auf dem Terminalserver anmeldet und mit seiner Sitzung verbunden wird. Aktive Sitzungen oder Sitzungen mit Leerlauf sollten Sie nur in Ausnahmefällen automatisch beenden lassen, damit die Benutzer keine Datenverluste erleiden.

- Auf der Registerkarte *Umgebung* können Sie festlegen, dass automatisch ein Programm gestartet wird, wenn sich ein Benutzer über RDP mit dem Terminalserver verbindet. Diese Option wäre sinnvoll, wenn auf einem Terminalserver nur eine Applikation, zum Beispiel ein ERP-Client, installiert wird. Die Benutzer können dann nur auf diese eine Applikation zugreifen, nicht auf den gesamten Server.
- Auf der Registerkarte *Netzwerkkarte* legen Sie fest, welcher Netzwerkkarte diese Verbindung zugeordnet ist und wie viele Verbindungen gleichzeitig aufgebaut werden können. Hier brauchen Sie keine Einstellungen vorzunehmen, außer Sie wollen definieren, dass sich nur eine bestimmte Anzahl von Benutzern mit dem Server verbinden darf.
- Die Registerkarte *Sicherheit* dient zur Verwaltung von Berechtigungen innerhalb der RDP-Sitzungen. Auf dieser Karte können Sie Berechtigungen vergeben, die für Sitzungen über diese Verbindung hinaus Gültigkeit haben. Hier können Sie bestimmen, welche Benutzer auf die Sitzungen anderer Benutzer Einfluss nehmen, diese zurücksetzen oder Einstellungen verändern können. Normalerweise müssen Sie hier keine Änderungen vornehmen (Abbildung 12.27).

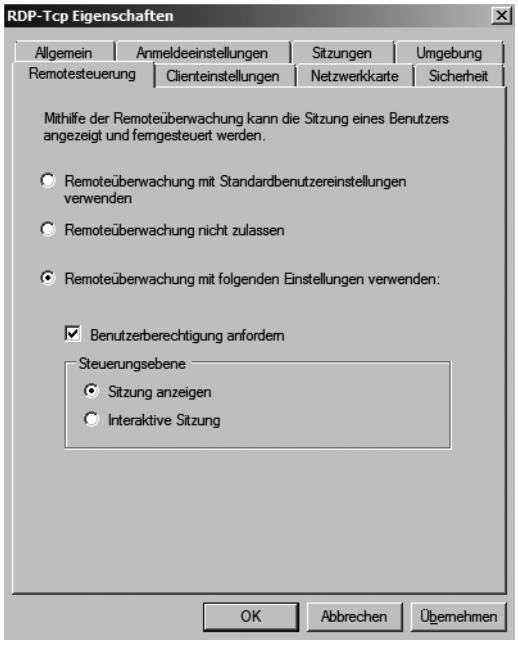
Abbildg. 12.27 Konfigurieren der Sicherheitseinstellungen von Terminalserververbindungen



- Die Registerkarte *Remotesteuerung* steuert den Zugriff anderer Benutzer auf einzelne Sitzungen (Abbildung 12.28). Mit den Terminaldiensten haben Sie die Möglichkeit, sich auf die Sitzung anderer zu spiegeln. So können mehrere Benutzer sich mit der gleichen Sitzung verbinden und Support-Mitarbeiter schnell bei Problemen helfen. Diese Funktion ist wie eine Fernwartung für Terminalserversitzungen. Sie sollten an dieser Stelle die Einstellungen für die Remoteüberwachung auf allen Terminalservern vorgeben, indem Sie die Option *Remoteüberwachung mit folgenden Einstellungen verwenden* aktivieren. Wenn Sie das Kontrollkästchen *Benutzerberechtigung anfordern* aktivieren, muss der entsprechende Benutzer der Spiegelung zuerst zustimmen, bevor Sie den Bildschirminhalt sehen können. Unter *Steuerungsebene* können Sie entweder die Option

Sitzung anzeigen aktivieren oder die Option *Interaktive Sitzung*. Bei der interaktiven Sitzung dürfen der Remotebenutzer und der Administrator, der die Sitzung spiegelt, Maus und Tastatur nutzen, bei der Option *Sitzung anzeigen* kann der Administrator nur zusehen. Die Spiegelung wird über das Verwaltungsprogramm *Terminaldiensteverwaltung* durchgeführt, das später in diesem Abschnitt noch besprochen wird.

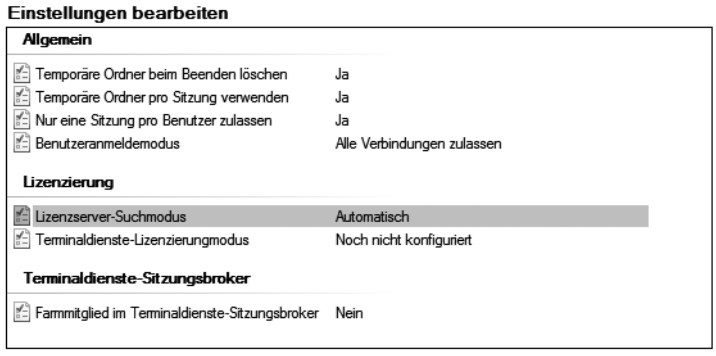
Abbildg. 12.28 Konfiguration der Remotesteuerung von Terminalsitzungen



- Auf der Registerkarte *Clienteinstellungen* stellen Sie verschiedene Verbindungsoptionen der Benutzer ein. Sie können festlegen, dass zum Beispiel die Zwischenablage des Clients dem Server zur Verfügung gestellt wird. An dieser Stelle können Sie auch zentral vorgeben, ob die lokalen Laufwerke auf den Clients in der Terminalserversitzung verfügbar sind. Auch die Drucker der Clients können in einer Terminalserversitzung genutzt werden. Sie sollten die Option *Standardmäßig den Hauptdrucker des Clients verwenden* deaktivieren, da durch diese Einstellung häufig auch andere Terminalserversitzungen negativ beeinflusst werden. Oft passiert es, dass der letzte Benutzer, der sich anmeldet, seinen Drucker an die anderen Sitzungen propagiert. Testen Sie, ob Sie bei sich ein solches Phänomen beobachten und deaktivieren Sie in diesem Fall diese Option. Die Farbtiefe sollten Sie möglichst nicht vorgeben, damit die Clients selbst bestimmen können, welche Farbtiefe verwendet wird.

Außer den Eigenschaften für verschiedene RDP-Verbindungen können Sie im Dienstprogramm *Terminaldienstekonfiguration* auch verschiedene Servereinstellungen definieren. Diese Einstellungen erreichen Sie über den Bereich *Einstellungen bearbeiten* (Abbildung 12.29).

Abbildg. 12.29 Bearbeiten der Terminalservereinstellungen in der Terminaldienstekonfiguration



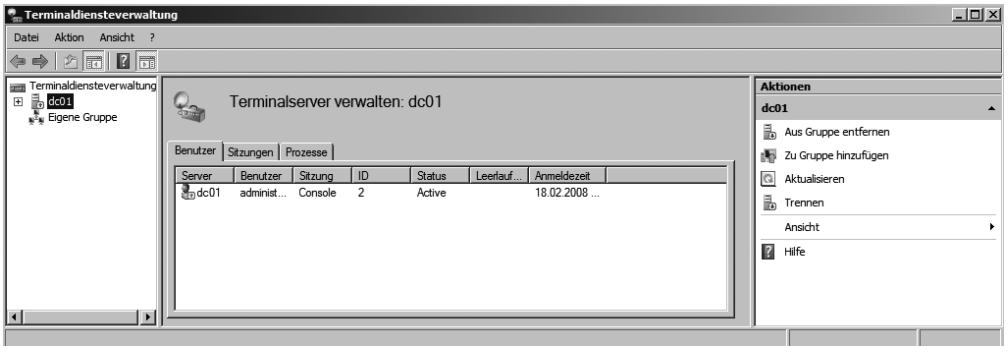
Sie können festlegen, ob für jede Anmeldung temporäre Ordner erstellt werden sollen und diese nach der Abmeldung des Benutzers wieder gelöscht werden. In diesem Menü können Sie die Sicherheitseinstellungen nachträglich ändern, die Sie bei der Installation der Terminaldienste festgelegt haben. Neu ist seit Windows Server 2003 die Möglichkeit, die Lizenzierung abzuändern. Microsoft hat unter Windows Server 2003 eine neue Lizenzierung eingeführt, die Benutzerlizenzierung (User-CALs). Diese Lizenzierung wird auch unter Windows Server 2008 fortgeführt. Eine Gerätelizenzierung (Device-CAL) erlaubt einer beliebigen Anzahl von Benutzern den Zugriff auf die lizenzierte Serversoftware von einem bestimmten Gerät aus. Eine User-CAL erlaubt einem bestimmten Benutzer den Zugriff auf die lizenzierte Serversoftware von einer beliebigen Anzahl von Geräten. Eine User-CAL sichert einem bestimmten Benutzer den Zugriff auf die Serversoftware über die PCs und Laptops im Büro, aber auch über PCs zu Hause, PDAs, in Internet-Cafes und mit anderen Geräten. Die Device-CAL wäre sinnvoll für mehrere Benutzer, die von einem gemeinsam genutzten Gerät auf die Serversoftware zugreifen.

TIPP In manchen Umgebungen macht es Probleme, wenn den Anwendern nur erlaubt wird, eine Sitzung auf dem Terminalserver zu öffnen. Vor allem bei der Anmeldung von Administratoren kann diese Einstellung Probleme bereiten. Stellen Sie in diesem Fall die Option *Nur eine Sitzung pro Benutzer zulassen* auf *Nein* ein.

Terminaldiensteverwaltung

Die *Terminaldiensteverwaltung* finden Sie im gleichen Menü wie die *Terminaldienstekonfiguration*. Mit Hilfe dieses Programms können Sie in Echtzeit sehen, welche Benutzer mit einem Server verbunden sind, und verschiedene Einstellungen vornehmen (Abbildung 12.30). Außerdem können Sie die bereits beschriebene Remoteüberwachung eines Benutzers durchführen. In diesem Programm können Sie Benutzersitzungen trennen und getrennte Sitzungen zurücksetzen. Hier können Sie beliebige Terminalserver verwalten. Sie können sehen, welche Prozesse von welchem Benutzer ausgeführt werden und einzelne Prozesse beenden, wenn diese zum Beispiel den Terminalserver zu stark belasten.

Abbildg. 12.30 Verwalten eines Terminalservers mit der Terminaldiensteverwaltung

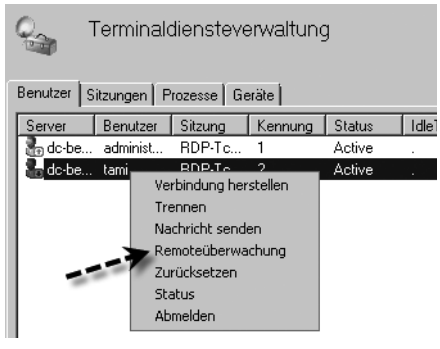


Klicken Sie eine Sitzung mit der rechten Maustaste an, können Sie diese Sitzung im Kontextmenü über die Option *Zurücksetzen* wieder freigeben (Abbildung 12.31). In diesem Fall ist die Lizenz sofort wieder frei. Sie können sich auch mit dem Verwaltungsprogramm *Terminaldiensteverwaltung* von einem Server mit einen anderen Server verbinden lassen und dort Sitzungen freigeben. Klicken Sie dazu mit der rechten Maustaste auf den Menüpunkt *Terminaldiensteverwaltung* und wählen Sie die Option *Verbindung mit Computer herstellen*. Wenn Sie über genügend Rechte auf dem anderen Server verfügen, können Sie auf diese Weise die Sitzungen auf mehreren Servern wieder freigeben.

Spiegelung – Remoteüberwachung

Wie bereits weiter vorne erwähnt, haben Administratoren oder Benutzer mit den entsprechenden Rechten die Möglichkeit, sich mit beliebigen Sitzungen anderer Benutzer zu verbinden. Diese Möglichkeit wird *Remoteüberwachung* bzw. *Spiegeln* genannt. Um eine Benutzersitzung zu spiegeln, klicken Sie diese mit der rechten Maustaste in der *Terminaldiensteverwaltung* an und wählen *Remoteüberwachung* (Abbildung 12.31).

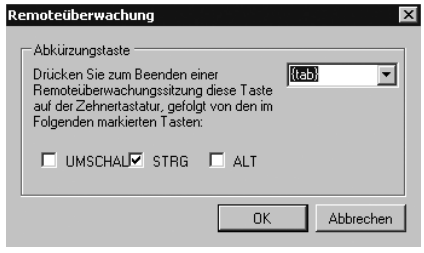
Abbildg. 12.31 Starten der Remoteüberwachung einer Terminalserversitzung



HINWEIS Spiegelungen können nur von Terminalserversitzung zu Terminalserversitzung durchgeführt werden. Sie können keine Benutzer spiegeln, wenn Sie an der Konsole arbeiten. Wenn Sie daher eine Sitzung spiegeln wollen, müssen Sie sich zuvor mit dem Terminalserver verbinden und in dieser Sitzung die Terminaldiensteverwaltung aufrufen. Es ist auch nicht möglich, auf einem Server eine Terminalserversitzung zum lokalen Server aufzubauen.

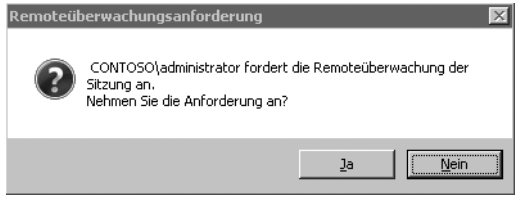
Nachdem Sie die Spiegelung gestartet haben, müssen Sie zunächst festlegen, mit welchem Tastaturkürzel Sie die gespiegelte Sitzung wieder verlassen (Abbildung 12.32).

Abbildg. 12.32 Festlegen des Tastaturkürzels für das Verlassen einer gespiegelten Sitzung



Danach erhält der Benutzer, den Sie spiegeln wollen, einen entsprechenden Hinweis auf dem Bildschirm, mit dem er der Spiegelung zustimmen muss (Abbildung 12.33). Lehnt er die Spiegelung ab oder bestätigt er eine gewisse Zeit nicht das Fenster, wird die Spiegelung abgebrochen.

Abbildg. 12.33 Damit die Sitzung eines Anwenders gespiegelt werden kann, muss dieser zustimmen



Sie können das Verhalten der Spiegelung im Verwaltungsprogramm *Terminaldienstekonfiguration* in den Eigenschaften der RDP-Verbindung auf der Registerkarte *Remotesteuerung* genauer konfigurieren. Nur wenn der Anwender auf die Schaltfläche *Ja* klickt, kann die Sitzung gespiegelt werden, wenn das Einverständnis des Anwenders eingeholt werden muss. Bei der Ablehnung erhält der Administrator eine Fehlermeldung. Stimmt der Benutzer der Spiegelung zu, dann verwandelt sich die Terminalsitzung des Administrators zur Sitzung des Anwenders und seine eigene wird in den Hintergrund verschoben. Wenn der Administrator die Spiegelung durch Eingabe der Tastenkombination beendet, landet er wieder in seiner eigenen Sitzung.

Weitere Möglichkeiten in der Terminaldiensteverwaltung

Wenn Sie einen verbundenen Benutzer mit der rechten Maustaste anklicken, können Sie darüber hinaus weitere Maßnahmen vornehmen. Sie können Benutzersitzungen trennen, getrennte Sitzungen zurücksetzen, eine Nachricht an den Benutzer schicken oder getrennte Sitzungen neu mit dem Clientgerät verbinden. Bei Windows Server 2008 können im Remoteverwaltungsmodus nur zwei

Terminalsitzungen pro Server aufgebaut werden. Wenn ein Administrator seine Sitzung nur trennt und nicht beendet, darf sich nur noch ein weiterer Administrator verbinden. Gibt es auf einem solchen Terminalserver im Remoteverwaltungsmodus zwei dieser getrennten Sitzungen, können sich Administratoren nicht mehr verbinden.

Single Sign-On (SSO) für Terminalserver

Unter Windows Server 2008 können Sie SSO-Szenarien erstellen, damit sich Anwender nur noch einmal authentifizieren müssen, zum Beispiel an ihrer Arbeitsstation, und auf weitere Server im Netzwerk zugreifen können, ohne sich noch einmal authentifizieren zu müssen. Damit Sie diese Funktionalität nutzen können, müssen Sie Windows Vista zusammen mit Windows Server 2008 einsetzen. Außerdem müssen sich beide Systeme im gleichen Active Directory befinden. Damit Sie SSO nutzen können, müssen Sie zum einen auf dem Terminalserver die Authentifizierung entsprechend konfigurieren. Gehen Sie dazu folgendermaßen vor:

1. Starten Sie über *Start/Ausführen/tsconfig.msc*.
2. Rufen Sie im Bereich *Verbindungen* die Eigenschaften der RDP-Verbindung auf.
3. Auf der Registerkarte *Allgemein* sollte bei der Sicherheitsstufe entweder *Verhandeln* oder *SSL* ausgewählt sein (Abbildung 12.34).

Abbildg. 12.34 Konfiguration der Authentifizierung für die RDP-Verbindung

4. Auf den Arbeitsstationen unter Windows Vista können Sie entweder die lokale Richtlinie bearbeiten oder Sie erstellen eine Gruppenrichtlinie. Navigieren Sie zum Bereich *Computerkonfiguration/Administrative Vorlagen/System/Delegierung von Anmeldeinformationen*.
5. Öffnen Sie die Richtlinie *Delegierung von Standardanmeldeinformationen zulassen*.

6. Aktivieren Sie diese Richtlinie.
7. Tragen Sie in der Serverliste den Eintrag *termsrv/<Servername>* ein. Wichtig an dieser Stelle ist, dass Sie vor dem Eintrag des Servernamens noch den Eintrag *termsrv* vornehmen.

Terminaldienste-RemoteApp

Dieser Rollendienst ist komplett neu in Windows Server 2008. Mit dieser Funktion können Anwendungen über eine Terminalserver-Sitzung zur Verfügung gestellt werden, ohne dass dazu eine Desktop-Verbindung zur Verfügung gestellt werden muss. Unter Citrix ist diese Funktion als Veröffentlichung von Anwendungen bekannt. Anwender können nur auf die veröffentlichte Anwendung zugreifen. Für den Anwender ist diese Technik transparent, er kann nicht feststellen ob diese Anwendung lokal oder in einer Terminalserversitzung läuft. Durch diese Funktion wird auch die Sicherheit erhöht, da die Anwender keinen Zugriff mehr auf den Desktop des Servers haben, sondern nur mit den Anwendungen Verbindung aufbauen. Sie können die Funktion nur dann nutzen, wenn Sie mit dem RDP-Client 6.1 arbeiten, der in Windows Vista und Windows Server 2008 integriert ist. Sie können den Client auch für Windows XP SP2 von der Internetseite *http://go.microsoft.com/fwlink/?LinkId=79373* herunterladen. Die Bedienung des Programms ist identisch mit der Bedienung eines lokalen Programms. Anwender können die Größe des Fensters anpassen oder das Fenster minimieren. Die Anwendung wird in den Desktop des Anwenders integriert. Auch Symbole, welche die Anwendung in der Informationsleiste anzeigen, werden auf dem Desktop des Anwenders angezeigt. Die Funktion unterstützt alle Anwendungen, die auf einem Terminalserver installiert werden können, Sie müssen dazu keine besonderen Versionen kaufen. Anwender können natürlich mit ihrem Desktop parallel zu den serverbasierten RemoteApp-Anwendungen auch lokale Anwendungen starten, ein Mischbetrieb ist daher ohne weiteres möglich. So können Anwender zum Beispiel mit Ihren Anwendungen arbeiten und Sie können den SAP-Client über einen Terminalserver zur Verfügung stellen. Die RemoteApp-Programme können Sie entweder über eine Weboberfläche zur Verfügung stellen, als **.rdp*-Protokolldatei, oder indem Sie auf eine Datei doppelklicken, die mit der Anwendung verknüpft ist. Die Verknüpfungen lassen sich auch durch die Software-Verteilung in den Gruppenrichtlinien in die Startmenüs oder Desktops auf den Clients pushen.

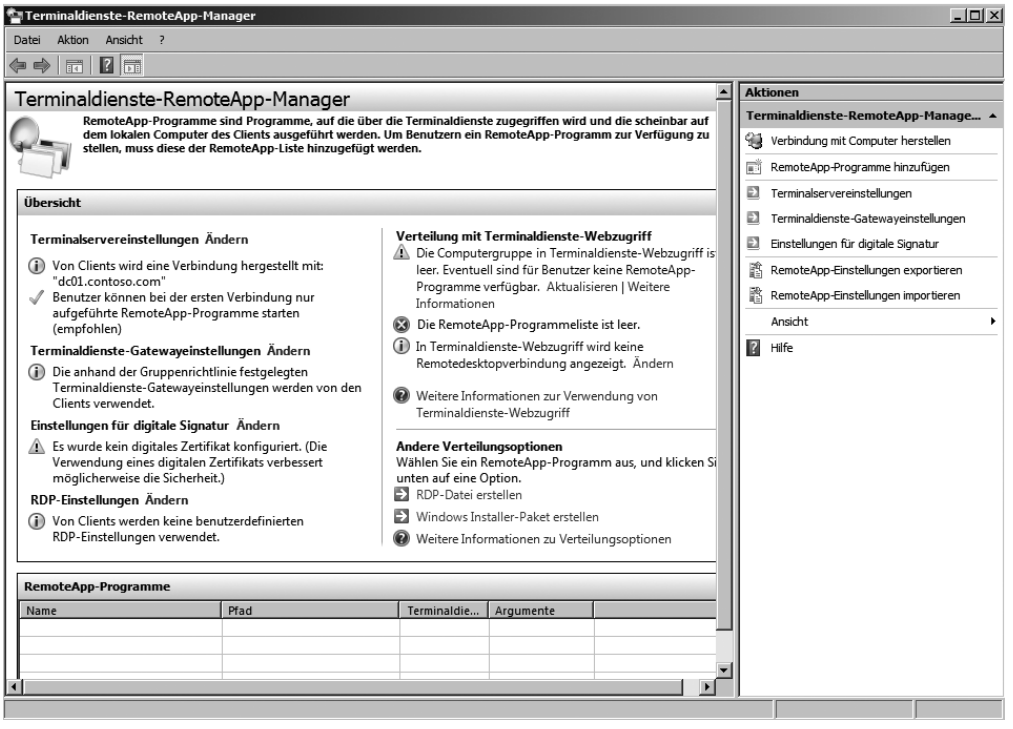
HINWEIS In Windows Server 2008 ist der RDP-Client 6.1 integriert. Windows Vista wird mit dem RDP-Client 6.0 ausgeliefert. Das Service Pack 1 für Windows Vista aktualisiert den Client auf Version 6.1.

Konfiguration von Terminaldienste-RemoteApp

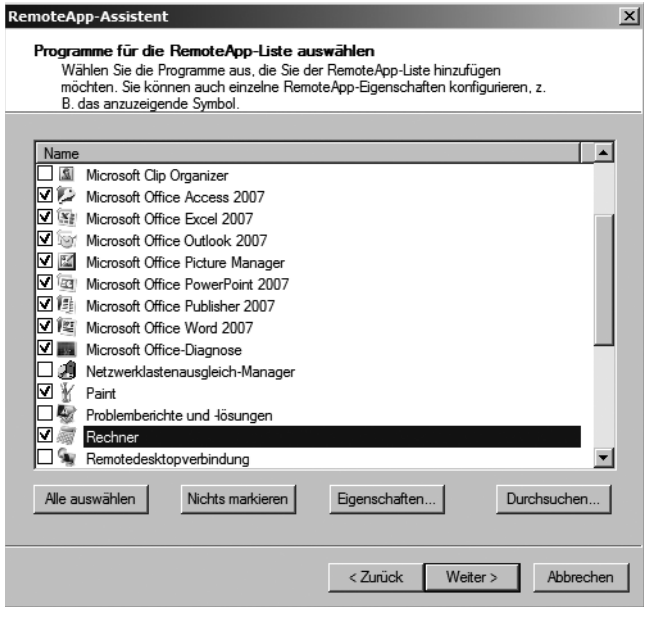
Um eine Anwendung als RemoteApp zur Verfügung zu stellen, müssen Sie zunächst den Terminalserver regulär installieren. Auch die Anwendungen werden auf normalen Weg installiert. Nachdem Sie den Server vorbereitet haben, können Sie die Funktion *RemoteApp* über *Start/Verwaltung/Terminaldienste/Terminaldienste-RemoteApp-Manager* verwalten (Abbildung 12.35).

Über dieses Verwaltungsprogramm können Sie zusätzliche Anwendungen hinzufügen und die Anwendungsliste verwalten. Um eine Anwendung der Liste hinzuzufügen, klicken Sie in der Spalte *Aktionen* auf den Link *RemoteApp-Programme hinzufügen*. Im Anschluss startet der *RemoteApp-Assistent*, über den Sie die Anwendungen der Liste hinzufügen können (Abbildung 12.36). Wählen Sie entweder das Programm aus der Liste aus oder klicken Sie auf *Durchsuchen*, um die Startdatei der Anwendung hinzuzufügen.

Abbildg. 12.35 Verwaltung von RemoteApps im Terminaldienste-RemoteApp-Manager



Abbildg. 12.36 Auswählen der Remoteanwendungen

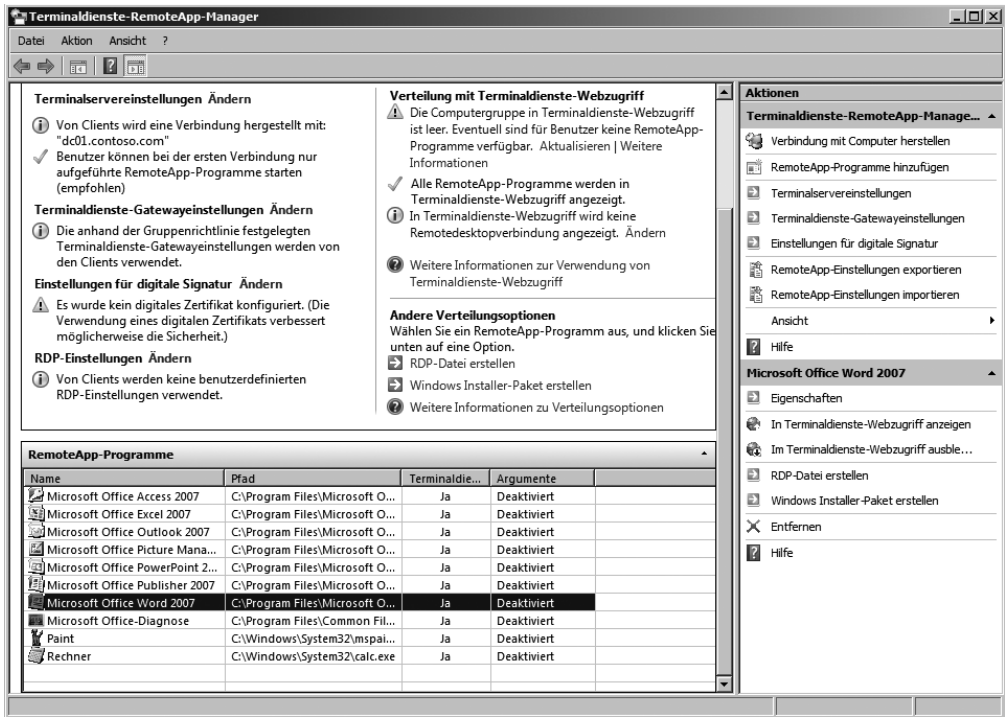


Sie können an dieser Stelle mehrere Anwendungen auswählen. Nachdem Sie die Anwendungen ausgewählt haben, werden diese in der Anwendungsliste angezeigt (Abbildung 12.37). Sie können die Eigenschaften der Applikationen jederzeit anpassen. Sie können in den Eigenschaften der Anwendung den Anzeigenamen ändern sowie die Syntax für den Startbefehl der Anwendung. An dieser Stelle können Sie auch konfigurieren, ob die Anwendung über Terminaldienste-Webzugriff zur Verfügung gestellt wird.

Anpassen der Terminalserver-Infrastruktur für RemoteApp

Neben der Konfiguration der RemoteApp-Liste sollten Sie auch die globalen Einstellungen für die Terminalserver konfigurieren. Die globalen Einstellungen haben die Aufgabe die Terminalserver so zu steuern, dass nur authentifizierte und berechtigte Benutzer auf die Remoteanwendungen zugreifen können.

Abbildg. 12.37 Bearbeiten der Applikationen in der Liste der RemoteApp-Programme



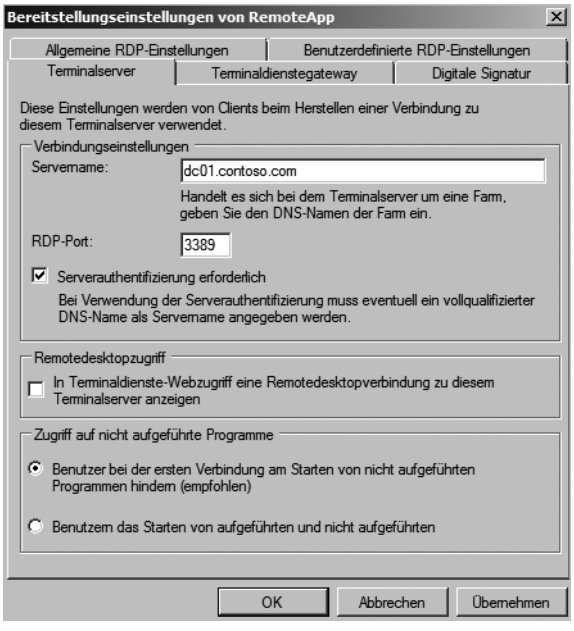
Die notwendigen Einstellungen für die Terminaldienste erreichen Sie ebenfalls über den *Terminaldienste-RemoteApp-Manager*. Klicken Sie dazu auf den Link *Terminalservereinstellungen* im Aktionsbereich. Es startet ein neues Fenster mit mehreren Registerkarten, auf denen Sie die globale Einstellungen für RemoteApps vornehmen können. Auf der Registerkarte *Terminalserver* konfigurieren Sie den Servernamen, beziehungsweise den DNS-Namen der Serverfarm. Zusätzlich steuern Sie hier

den Port der Verbindung, die Authentifizierung und den Zugriff der Anwender auf die Applikationen (Abbildung 12.38).

HINWEIS Greifen auf die Anwendungen Benutzer mit Windows XP SP2-PCs zu, müssen Sie für die Authentifizierung ein SSL-Zertifikat auf dem Terminalserver hinterlegen, zum Beispiel über die interne Zertifizierungsstelle (siehe Kapitel 17). Setzen Sie nur Windows Vista ein, können Sie auch mit dem selbstsignierten Zertifikat von Windows Server 2008 arbeiten.

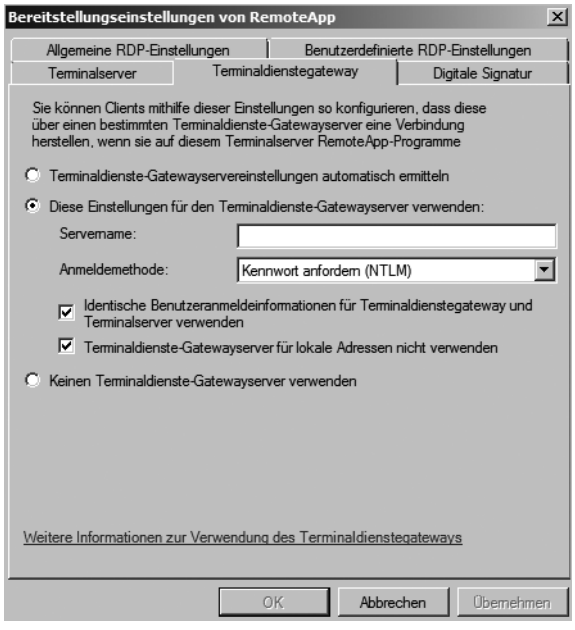
Auf der Registerkarte *Terminalserver* können Sie auch einstellen, dass über Terminaldienste-Webzugriff der Desktop des Servers zur Verfügung gestellt wird, wenn Sie zum Beispiel nicht nur mit Remoteanwendungen arbeiten.

Abbildg. 12.38 Konfigurieren der allgemeinen Einstellungen für Remoteanwendungen



Über die Registerkarte *Terminaldienstegateway* können Sie die Zusammenarbeit zwischen Remoteanwendungen und dem Terminaldienstegateway konfigurieren (siehe auch Abschnitt Terminal Services Gateway). Hauptsächlich legen Sie auf dieser Registerkarte fest, ob die Einstellungen des Gateways automatisch bezogen werden sollen (Standard), oder Sie können die Einstellungen manuell vorgeben. Bei der automatischen Einstellung erhalten die Clients die Informationen über die Gruppenrichtlinien zugeteilt. Geben Sie den Servernamen manuell an, müssen Sie darauf achten, dass dieser mit der Bezeichnung des Zertifikats übereinstimmt. Auf der Registerkarte *Digitale Signatur* können Sie festlegen, ob die **.rdp*-Datei der Remoteanwendungen digital signiert werden soll, um Fälschungen auszuschließen. Sie können für digitale Signaturen das gleiche Zertifikat verwenden wie für das Terminaldienstegateway. Die Registerkarte *Benutzerdefinierte RDP-Einstellungen* dient zur optionalen Konfiguration der **.rdp*-Datei der Remoteanwendungen. Sie können hier zum Beispiel die Einstellungen einer **.rdp*-Datei einfügen, die Sie vorher mit dem Editor kopiert haben.

Abbildg. 12.39 Konfiguration der Unterstützung des Terminaldienstegateways für Remoteanwendungen



Nachdem Sie die Anwendungen in die Remoteanwendungsliste hinzugefügt haben, können Sie diese entweder über eine **.rdp*-Datei oder über Terminaldienste-Webzugriff zur Verfügung stellen. Sie können die **.rdp*-Datei über den Link *RDP-Datei erstellen* anlegen lassen. Die Datei können Sie nach der Erstellung noch beliebig bearbeiten. Anwender können per Doppelklick auf diese Datei eine Verbindung zum Server aufbauen (Abbildung 12.40). So können Sie in einer Testumgebung einen schnellen Überblick über die veröffentlichten Anwendungen erhalten.

HINWEIS Auf der Registerkarte *Digitale Signatur* in den TS-Gateway-Einstellungen können die einzelnen RDP-Dateien der Remoteanwendungen mit einem Zertifikat signiert werden. So können die Clients im Netzwerk sicherstellen, dass der Anwendung vertraut werden kann. Allerdings muss in diesem Fall auf dem Client der RDP-Client 6.1 installiert werden, der nur in Windows Server 2008 und Windows Vista SP1 enthalten ist. Standardmäßig wird Windows Vista mit dem RDP-Client 6.0 ausgeliefert, der keine digitalen Signaturen unterstützt.

Zwischen lokalen Anwendungen und RemoteApps auf dem Server können auch Daten ausgetauscht werden. So besteht beispielsweise die Möglichkeit, über eine ERP-Anwendung, die Remote auf dem Terminalserver ausgeführt wird, Daten über die Zwischenablage in ein lokales Excel zu übernehmen. Die Abläufe dabei sind für den Anwender komplett transparent, da er bei der Bedienung der Software keinerlei Unterschiede zwischen der lokalen Anwendung und der Anwendung auf dem Server feststellen kann.

Abbildg. 12.40 Verbindungsaufbau über eine **.rdp*-Datei zu einer RemoteApp

Terminaldienste-Webzugriff

Windows Server 2008 bietet jetzt auch einen Webzugriff für die Terminaldienste an. Der Funktionsumfang ist ähnlich zu Outlook Web Access von Exchange. Über den Terminaldienste-Webzugriff (Terminal Services Web Access) können Sie zum Beispiel einen Terminalserver im Internet zur Verfügung stellen oder Ihre RemoteApps veröffentlichen. Standardmäßig werden die Applikationen, die Sie in der Remoteanwendungsliste zur Verfügung stellen, über den Terminaldienste-Webzugriff zur Verfügung gestellt.

HINWEIS Wird der Remoteanwendungsliste eine neue Anwendung hinzugefügt, wird diese automatisch im Terminaldienste-Webzugriff angezeigt; es sind keine weiteren Maßnahmen zur Konfiguration notwendig. Dabei ist es unerheblich, ob die Liste lokal auf dem entsprechenden Terminalserver oder über Gruppenrichtlinien erstellt wird.

Der Terminaldienste-Webzugriff ist ein Rollendienst der Terminaldienste, den Sie entweder bereits bei der Installation oder auch nachträglich installieren können. Wählen Sie zur Installation den Rollendienst *Terminaldienste-Webzugriff* aus. Nach der Installation steht Ihnen über *http://<Servername>/ts* der Webzugriff zur Verfügung (Abbildung 12.41). Natürlich können Sie den Zugriff mit SSL verschlüsseln.

Abbildg. 12.41 Anzeigen der veröffentlichten Anwendungen über den Terminaldienste-Webzugriff

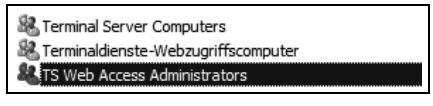
Die Rolle muss zwingend auf einem Windows Server 2008 mit installiertem IIS 7.0 durchgeführt werden. Beim TS Web Access-Server muss es sich aber nicht unbedingt um einen Terminalserver handeln. Greifen Anwender über das Webportal auf den Terminalserver zu, müssen diese nicht zuvor auch den RDP-Client gestartet haben. Anwendungen, die als RemoteApp konfiguriert sind, stehen standardmäßig automatisch auch über den Terminaldienste-Webzugriff zur Verfügung.

HINWEIS Handelt es sich beim TS Web Access-Server um einen anderen Server als den Terminalserver, über den Sie die Applikationen zur Verfügung stellen, müssen Sie auf dem Terminalserver mit den Remoteanwendungen das Computerkonto des TS Web Access-Servers in die Sicherheitsgruppe *TS Web Access Computers* hinzufügen.

Veröffentlichen der RemoteApps über Terminalserver oder Active Directory

Neben der Konfiguration auf den Terminalservern können Sie auch über Gruppenrichtlinien steuern, welche Anwendungen über Terminaldienste-Webzugriff zur Verfügung gestellt werden. Diese Möglichkeit macht vor allem bei größeren Unternehmen Sinn, die zahlreiche Terminalserver einsetzen. Wollen Sie diese Konfiguration nicht über das Active Directory und die Gruppenrichtlinien abwickeln, können Sie die notwendigen Einstellungen auch direkt auf den Terminalservern durchführen. Sie können auch über TS Web Access einige Einstellungen an der Oberfläche vornehmen, allerdings wird die Verwaltungsoberfläche erst dann eingeblendet, wenn Sie das Konto des Administrators in die lokale Gruppe *TS Web Access Administrators* auf dem TS Web Access Server hinzufügen (Abbildung 12.42).

Abbildg. 12.42 Sicherheitsgruppe für den TS Web Access-Zugriff und die weiteren Sicherheitsgruppen für die Terminaldienste



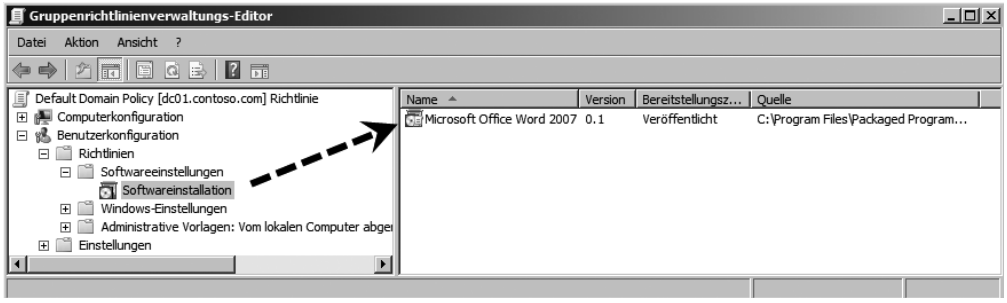
Haben Sie sich am TS Web Access als Administrator authentifiziert, der Mitglied der Gruppe *TS Web Access Administrators* ist, können Sie TS Web Access und die veröffentlichten RemoteApp-Programme verwalten. Dazu wird im Browser die neue Schaltfläche *Konfiguration* eingeblendet. Klicken Sie auf diese Schaltfläche, können Sie festlegen, ob das Webpart für den Zugriff auf die RemoteApp-Programme entweder über den Terminalserver steuert oder über das Active Directory (Abbildung 12.43).

Abbildg. 12.43 Verwalten der RemoteApp-Programme über einen Terminalserver oder über das Active Directory

Aktivieren Sie die Zusammenstellung der veröffentlichten Anwendungen über das Active Directory, müssen Sie folgendermaßen vorgehen:

1. Erstellen Sie für die RemoteApps ein **.msi*-Paket. Ein solches Paket erstellen Sie ähnlich wie eine **.rdp*-Datei. Im Verwaltungsprogramm *Terminaldienste-RemoteApp-Manager* markieren Sie die Anwendung und klicken auf den Link *Windows Installer-Paket erstellen*. In der erstellten **.msi*-Datei werden die notwendigen Informationen zu den Symbolen und der Verbindung zum Terminalserver hinterlegt. Führt ein Anwender eine solche **.msi*-Datei aus, wird nicht die Anwendung installiert, sondern nur für die Verbindung notwendige Daten auf dem Client. Aus diesem Grund können Sie diese Pakete auch über Gruppenrichtlinien auf den Clients installieren lassen.
2. Achten Sie darauf, dass die Datei die Endung **.rap.msi* hat, damit diese im Webpart in TS Web Access angezeigt wird. Soll die Anwendung als RemoteApp aber nicht über TS Web Access zur Verfügung gestellt werden, wird eine **.rdp.msi*-Datei erstellt. Sie können die Endungen der Dateien aber ohne weiteres auch nachträglich abändern, der Inhalt ist identisch.
3. Speichern Sie die **.rap.msi*-Dateien auf einer Freigabe, auf die auch der TS Web Access Server oder die Benutzer selbst, wenn Sie diese Dateien ausführen sollen, zugreifen dürfen. Damit der TS Web Access Server auf die Freigabe zugreifen kann, müssen Sie das Computerkonto des Servers für die Freigabe berechtigen.
4. Sie können anschließend für dieses Paket über Gruppenrichtlinien im Bereich *Benutzerkonfiguration/Softwareeinstellungen* ein neues Paket erstellen. Als Ziel für dieses Paket nehmen Sie die **.rap.msi*-Datei aus der Freigabe.

Abbildg. 12.44 Erstellen von Softwarepaketen für Remoteanwendungen

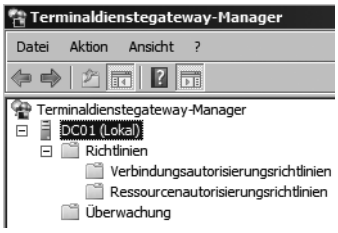


5. Wählen Sie *Veröffentlicht* als Option aus.
6. Achten Sie darauf, dass in der OU, für die Sie diese Richtlinie erstellen, sowohl die Benutzerkonten der Anwender enthalten sind, welche die Anwendung bekommen sollen, als auch das Computerkonto des TS Web Access-Servers, der die Anwendungen bereitstellen soll. Dadurch ist sichergestellt, dass das Webpart des TS Web Access-Servers die Anwendungen anzeigt, für die Sie über die **.rap.msi*-Dateien Pakete erstellt haben. Befindet sich das Computerkonto des TS Web Access Servers in einer anderen OU als die Benutzerkonten, können Sie die GPO auch auf die OU des TS Web Access Servers verknüpfen. Stellen Sie sicher, dass sowohl die Benutzer als auch das Computerkonto des TS Web Access Servers die GPO lesen und anwenden darf.

Terminaldienstegateway

Eine weitere neue Funktion in den Terminaldiensten von Windows Server 2008 ist das Terminaldienstegateway (Terminal Services Gateway). Auch diese Funktion kann als Rollendienst hinzugefügt werden, wenn Sie die Terminaldienste auf einem Server installieren. Die Aufgabe des Terminaldienstegateway besteht darin, Anwendern, die sich über das Internet mit dem Unternehmen verbinden, Zugriff auf die internen Terminalserver zu gestatten. Ein Terminaldienstegateway verbindet das RPD- mit dem HTTPS-Protokoll, um eine gesicherte Verbindung zu allen möglichen Terminalservern auch über RemoteApps zu ermöglichen. Es ist nicht notwendig, dass sich diese Anwender zusätzlich über ein VPN oder RAS einwählen. Die Verbindung erfolgt über HTTPs und kann ohne weitere Maßnahmen RDP-Sitzungen im internen Netzwerk aufbauen. TS Gateways können so konfiguriert werden, dass Administratoren genau festlegen können, auf welche internen Server oder auch RDP-aktivierte PCs die Anwender über das Internet zugreifen können. TS Gateways ermöglichen den Zugriff auf RDP-Sitzungen über Firewalls oder Network Address Translation (NAT) hinweg. Die Verbindung zwischen Client und TS Gateway erfolgt über den Port 443 (SSL). Nur die Verbindung zwischen TS Gateway und Terminalserver erfolgt über den RDP-Port (3389).

Abbildg. 12.45 Verwaltungsoberfläche für das Terminaldienstegateway



Bisher konnten Anwender über das Internet nicht auf Terminalserver zugreifen, wenn der Port 3389 blockiert wird, was meistens der Fall sein wird und auch sinnvoll ist. Nachdem Sie die Rolle installiert haben, können Sie die entsprechenden Richtlinien über *Start/Verwaltung/Terminaldienste/Terminaldienstegateway-Manager* erstellen und konfigurieren (Abbildung 12.45).

HINWEIS Sie können mit einem TS Gateway-Server unter Windows Server 2008 den Zugriff auf Terminalserver gewähren, die unter Windows Server 2003, Windows 2000 Server und sogar Windows NT 4.0 Terminalserver Edition installiert worden sind. Auch der Zugriff auf den Remotedesktop von Windows XP oder Windows Vista wird unterstützt. Die Clients müssen allerdings den RDP-Client 6.0 von Windows Vista verwenden. Für Windows XP SP2 steht der Client ebenfalls kostenlos zum Download zur Verfügung. Sie finden diesen auf der Internetseite *http://go.microsoft.com/fwlink/?LinkId=79373*.

Abbildg. 12.46 Konfigurieren eines Terminaldienstegateway

Über diese Richtlinien können Sie festlegen, wer sich über das Internet auf die Terminalserver verbinden darf und auf welche Server sich die Anwender verbinden können. Auch die Umleitung der lokalen Ressourcen wie Drucker, Zwischenablage und Laufwerke können Sie über diese Richtlinien steuern. Neben der herkömmlichen Authentifizierung werden auch Smartcards unterstützt. TS Gateways können auch die neue Netzwerkzugriffsschutz (Network Access Protection, NAP)-Funktion von Windows Server 2008 und Windows Vista nutzen, um den Zugriff zu steuern (siehe Kapitel 15). Über NAP können auch Arbeitsstationen unter Windows XP SP3 mit Richtlinien abgeprüft werden. Der optimalste Weg, ein TS Gateway zur Verfügung zu stellen, ist als Veröffentlichung über einen ISA Server 2004/2006, ähnlich zur RPC-über-HTTP-Funktion von Exchange Server 2003/2007. Dadurch wird die SSL-Verbindung zwischen dem Client im Internet und dem ISA-Server aufgebaut und zwischen ISA und TS Gateway eine neue SSL- oder eine HTTP-Verbindung. Verwenden Sie als Zertifikatestelle am besten eine interne Zertifizierungsstelle, genauso wie bei einer Veröffentlichung von Outlook Web Access (siehe Kapitel 17). Achten Sie auch hier darauf, dass der Name des Zertifikates mit dem DNS-Namen des TS Gateways übereinstimmt, mit dem sich die Anwender über das Internet verbinden. Stimmen die Namen nicht überein, erhalten die Anwender eine Zertifikate-Fehlermeldung und der Zugriff wird blockiert. Natürlich muss der Client der Zertifizierungsstelle des Unternehmens vertrauen. Sie müssen dazu unter Umständen das Zertifikat der Stammzertifizierungsstelle im Zertifikatespeicher des TS Gateways, des ISA-Servers und des Clients integrieren. Befinden sich TS Gateway und ISA-Server in einer Active Directory-Domäne, wird die Zertifizierungsstelle automatisch als vertrauenswürdig integriert.

HINWEIS Damit Sie ein TS Gateway einsetzen können, müssen Sie auf dem TS Gateway-Server die RPC-über-HTTP-Proxy-Funktion installieren, da über dieser der RDP-HTTP-Verkehr abgewickelt wird. Außerdem muss auf dem TS Gateways Server IIS 7.0 installiert und aktiviert werden. Dies geschieht bei der Auswahl der Rolle *Terminaldienstegateway* automatisch. Auch die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* muss auf dem Server installiert sein. Alternativ können Sie den TS Gateway Server auch an einen anderen Server mit der Rolle *Netzwerkrichtlinien- und Zugriffsdienste* (ehemals RAS) verbinden.

Der Verkehr zwischen TS Gateway und dem Client im Internet wird über einen HTTPS-Tunnel abgewickelt. Zwischen TS Gateway und Terminalserver findet die Verbindung über RDP (Port 3389) statt.

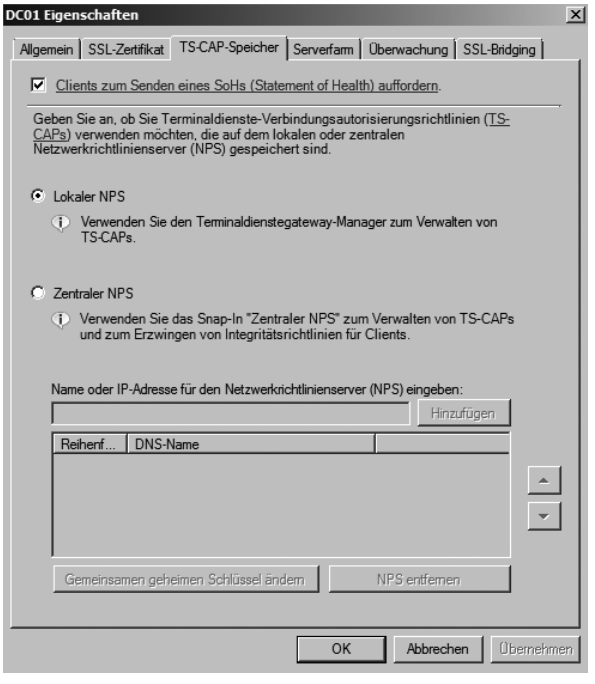
HINWEIS Der Verbindungsaufbau der Clients zu den Terminalservern findet über die bereits erwähnten Richtlinien auf dem TS Gateway statt. Diese werden auch als *Terminal Server Client Access Policies* (TS-CAPs) bezeichnet. Außerdem gibt es noch die *Terminal Services Resource Authorization Policies* (TS-RAPs). Diese steuern, auf welche Server die Clients zugreifen dürfen, die Sie in mindestens einer TS-CAP festgelegt haben. Bevor der Zugriff über das Internet auf ein TS Gateway und die Terminalserver funktioniert, müssen Sie mindestens eine TS-CAP und eine TS-RAP konfiguriert haben.

Terminaldienstegateway und ISA Server 2004/2006

Veröffentlichen Sie ein Terminaldienstegateway über einen ISA Server 2004/2006, müssen Sie beachten, dass der HTTPS-Verkehr vom Client aus dem Internet am ISA Server beendet wird. Sie können den Datenverkehr zwischen ISA und TS Gateways über HTTP laufen lassen. In diesem Fall müssen

Sie die Eigenschaften des TS Gateway-Servers im Terminaldienstegateway-Manager aufrufen und auf die Registerkarte *SSL-Bridging* wechseln (Abbildung 12.47). Aktivieren Sie die Option *Verwenden Sie HTTPS-HTTP-Bridging*. In diesem Fall wird die HTTPS-Sitzung am ISA Server terminiert und zwischen ISA Server und TS Gateway eine neue Verbindung aufgebaut, die auf HTTP basiert.

Abbildg. 12.47 Verwalten der Eigenschaften eines TS Gateway-Servers



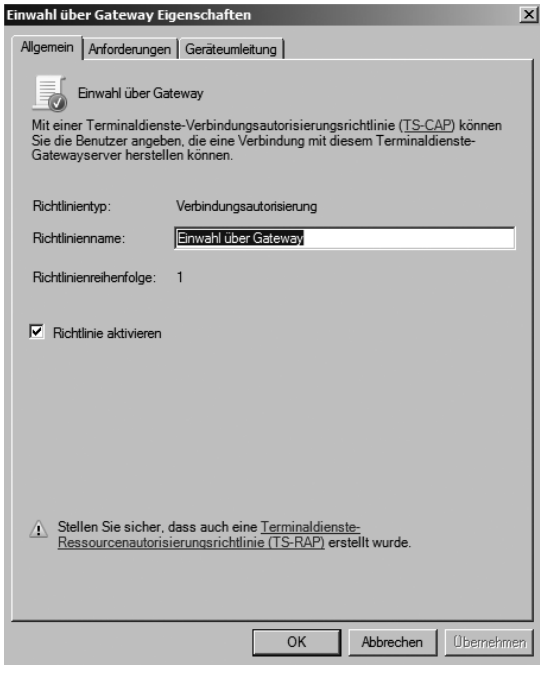
Einrichtung und Konfiguration eines TS Gateway

Um ein TS Gateway zu installieren, wählen Sie im Server-Manager den Rollendienst *Terminaldienstegateway* aus. Während der Installation können Sie bereits das Zertifikat für die SSL-Verbindung auswählen. Für Testzwecke können Sie auch das selbstsignierte Zertifikat der Terminaldienste verwenden. In einer produktiven Umgebung sollten Sie jedoch möglichst eine eigene Zertifizierungsstelle verwenden oder ein Zertifikat von einer öffentlichen Zertifizierungsstelle, der die beteiligten Server und Arbeitsstationen vertrauen müssen. Sie können das Zertifikat auch in den Eigenschaften des Terminaldienstegateway-Managers auf der Registerkarte *SSL-Zertifikat* anpassen (Abbildung 12.48).

Sie können auch bereits während der Installation der Rolle die entsprechenden Richtlinien (TS-CAP und TS-RAP) konfigurieren. Natürlich können Sie diese Einstellungen auch jederzeit über den Terminaldienstegateway-Manager anpassen. Über den Eintrag *Richtlinien/Verbindungsautorisierungsrichtlinie* in der Konsolenstruktur sehen Sie die standardmäßig angelegte erste TS-CAP. Sie können im Terminaldienstegateway-Manager die Eigenschaften dieser Richtlinie öffnen und die Einstellungen ändern. An dieser Stelle können Sie konfigurieren, in welcher Gruppe sich die Anwender im Active Directory befinden müssen, damit die Einwahl funktioniert. Sie können die Umleitung der Ressourcen auf den Clients konfigurieren und die Art der Anmeldung (Abbildung 12.49).

Abbildg. 12.48 Verwalten des Zertifikats für das Terminaldienstegateway

Abbildg. 12.49 Anpassen der TS-CAP



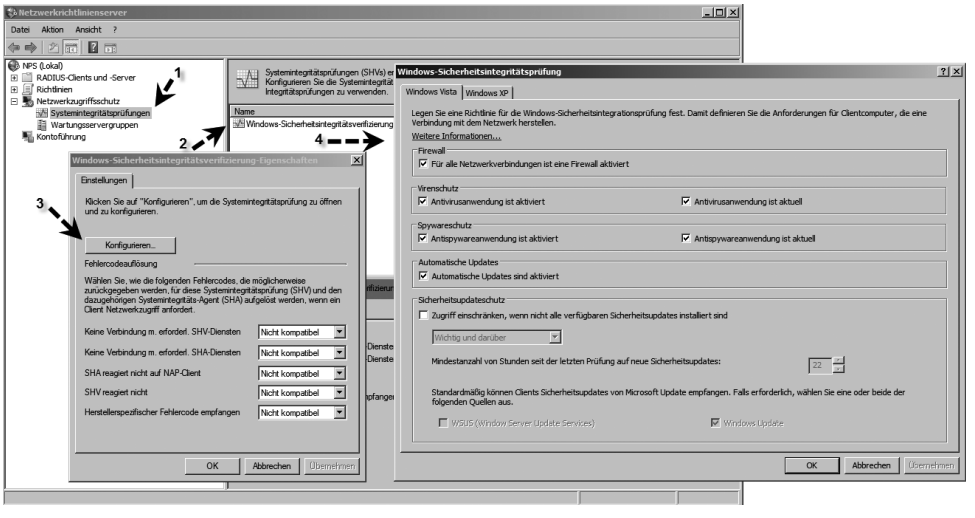
Terminaldienstegateway und Network Access Protection (NAP)

Auf der Registerkarte *TS CAP-Speicher* konfigurieren Sie, ob die Clients, die sich über das TS Gateway authentifizieren, auch über eine NAP-Richtlinie berechtigen müssen. Aktivieren Sie in diesem Fall auf dieser Registerkarte die Option *Clients zum Senden eines SoH (Statement of Health) auffordern*. Nach Bestätigung dieser Auswahl erscheint eine Meldung, dass Sie die TS CAPs für NAP konfigurieren müssen. Bestätigen Sie diese Meldung.

Damit ein TS Gateway NAP unterstützt, müssen Sie anschließend eine entsprechende Richtlinie auf dem Netzwerkrichtlinienserver konfigurieren:

1. Diese Einstellungen nehmen Sie über *Start/Verwaltung/Netzwerkrichtlinienserver* vor (Abbildung 12.50).
2. Öffnen Sie in den Konsolenstruktur den Knoten *Netzwerkzugriffschutz.*
3. Klicken Sie auf *Systemintegritätsprüfungen*.
4. Rufen Sie die Eigenschaften der Option *Windows-Sicherheitsintegritätsprüfung* auf.
5. Klicken Sie im Dialogfeld auf die Schaltfläche *Konfigurieren*.
6. Hier können Sie jetzt einstellen, welche Voraussetzungen ein Client erfüllen muss, um auf das Netzwerk zugreifen zu können.

Abbildg. 12.50 Konfigurieren der Integritätsüberprüfung von Computern im Netzwerk

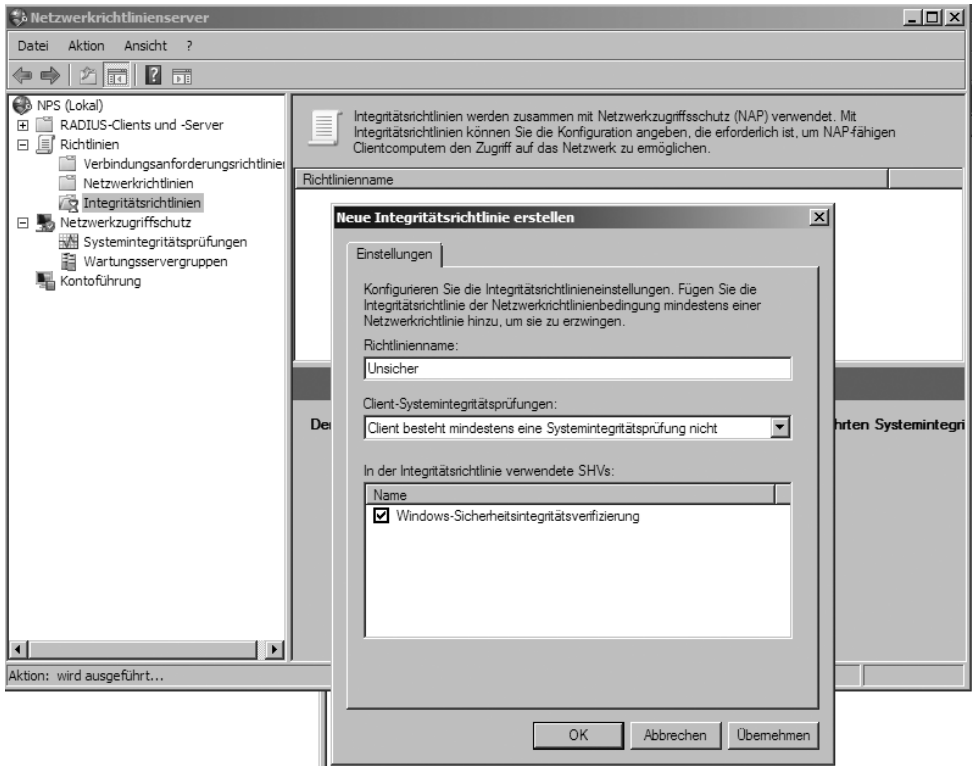


Um eine neue Richtlinie zu konfigurieren, die Clients den Zugriff verweigert, wenn diese nicht den Bedingungen entsprechen, gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten *Richtlinien*.
2. Klicken Sie mit der rechten Maustaste auf *Integritätsrichtlinien* und wählen Sie im Kontextmenü den Befehl *Neu*.
3. Geben Sie der Richtlinie einen Namen, zum Beispiel *Unsicher-Verbindung nicht erlaubt*.

4. Im Listenfeld *Client-Systemintegritätsprüfungen* wählen Sie den Eintrag *Client besteht mindestens eine Systemintegritätsüberprüfung nicht* aus.
5. Aktivieren Sie das Kontrollkästchen *Windows-Sicherheitsintegritätsüberprüfung*.
6. Erstellen Sie eine weitere Richtlinie, in der Sie konfigurieren, dass dem Client der Zugriff gestattet wird, wenn der PC die Richtlinien erfüllt. Die Erstellung ist analog zur ersten Richtlinie.

Abbildg. 12.51 Erstellen einer neuen Integritätsrichtlinie

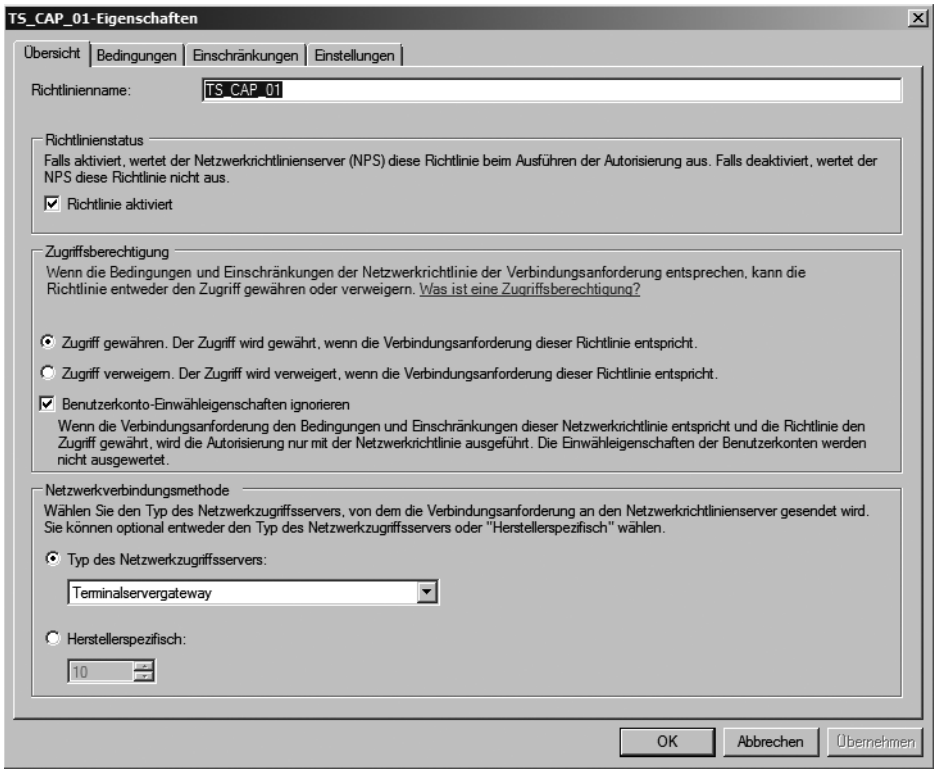


Durch Konfiguration dieser beiden Richtlinien wird allerdings noch kein Zugriff gestattet oder verweigert. Sie müssen dazu im nächsten Schritt zunächst eine Netzwerkrichtlinie bearbeiten oder erstellen, welche den Zugriff basierend auf Ihren konfigurierten Integritätsprüfungen erfüllt oder nicht erfüllt:

1. Klicken Sie dazu in der Verwaltungskonsole *Netzwerkrichtlinienserver* auf *Richtlinien/Netzwerkrichtlinien*.
2. Rufen Sie die Eigenschaften der TS-CAP in der Mitte der Konsole auf.
3. Sinnvollerweise bearbeiten Sie die erste standardmäßige Richtlinie so, dass Sie den Zugriff auf das TS Gateway verweigern, wenn der zugreifende PC nicht sicher ist. Als Basis für diese Richtlinie dient die erstellte Integritätsüberprüfungs-Richtlinie, die Sie zuvor erstellt haben.
4. Ändern Sie daher den Namen der Richtlinie auf *TS_CAP_01_FAILED* ab.

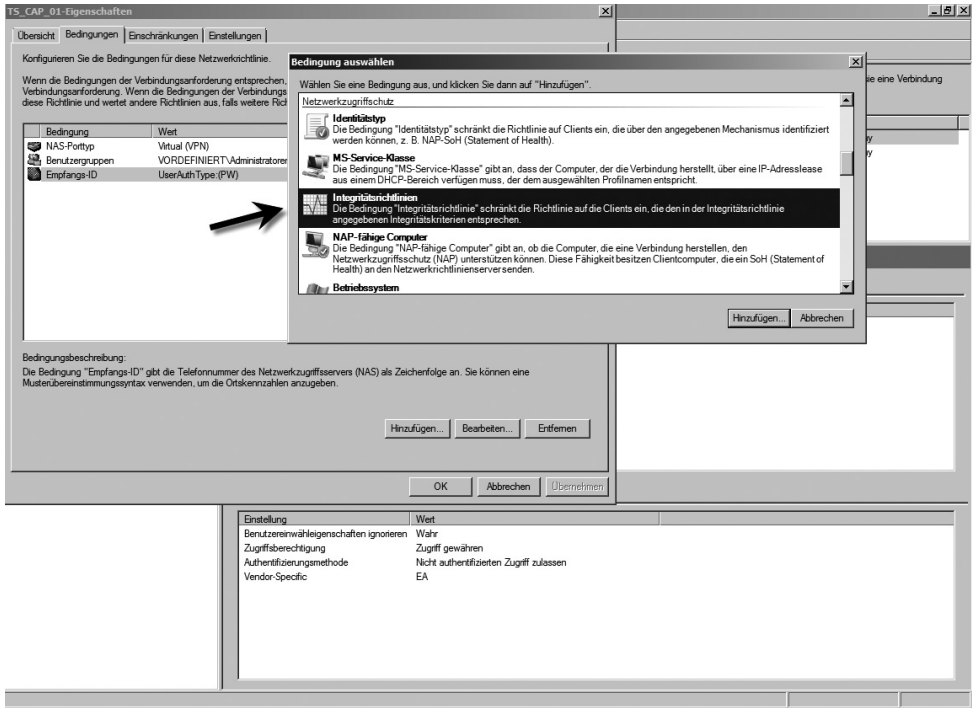
5. Stellen Sie sicher, dass die Richtlinie aktiviert ist.
6. Aktivieren Sie die Option *Zugriff gewähren*.
7. Stellen Sie sicher, dass die Option *Terminalservergateway* bei *Typ des Netzwerkzugriffsservers* aktiviert ist (Abbildung 12.52).
8. Wechseln Sie auf die Registerkarte *Bedingungen*.

Abbildg. 12.52 Konfiguration einer NAP-Richtlinie für den Zugriff auf das TS Gateway



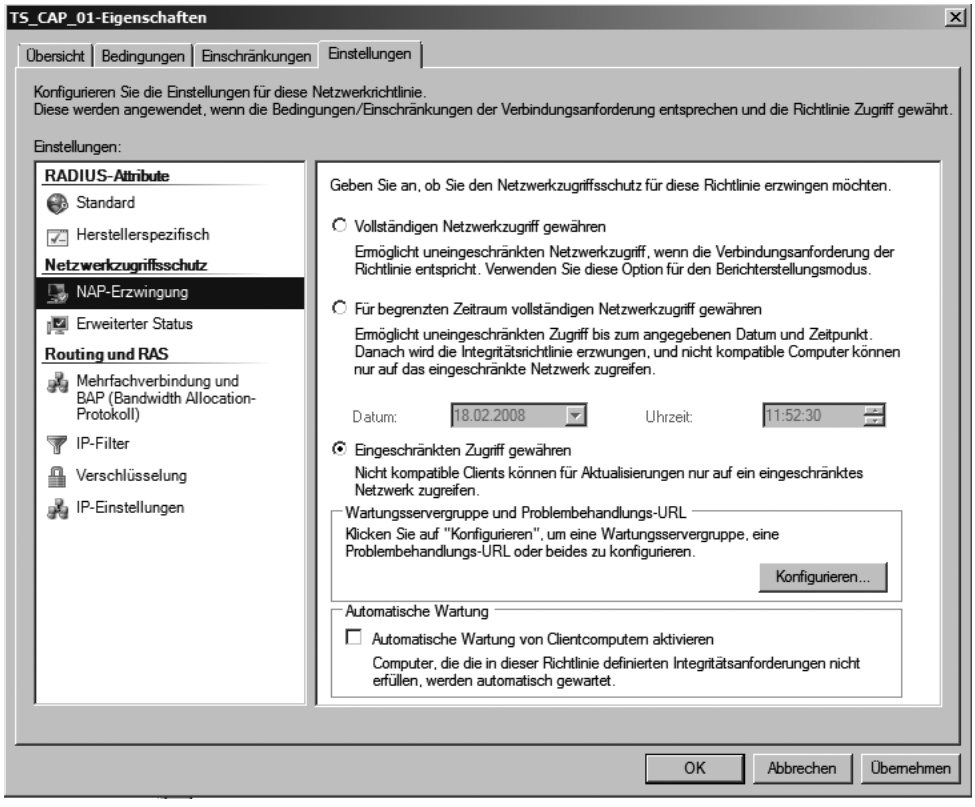
9. Klicken Sie auf *Hinzufügen*.
10. Markieren Sie *Integritätsrichtlinien*.
11. Klicken Sie auf *Hinzufügen* (Abbildung 12.53).

Abbildg. 12.53 Hinzufügen von Integritätsrichtlinien zu einer Netzwerkrichtlinie



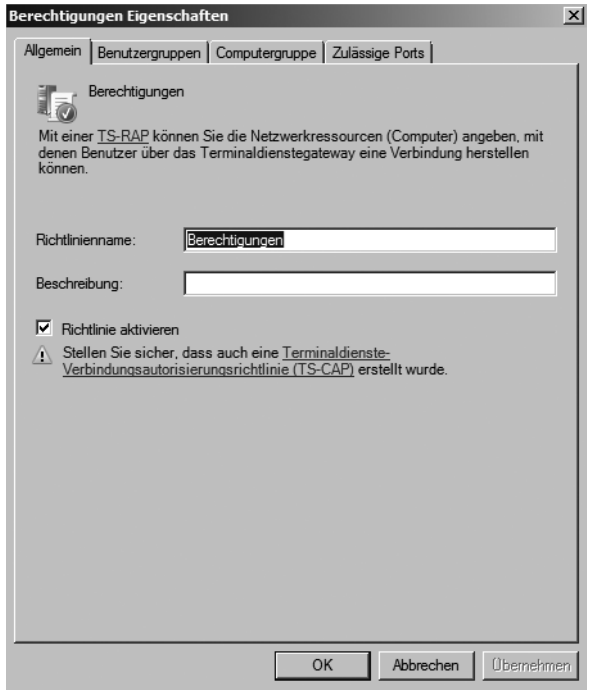
12. Wählen Sie die Richtlinie *Unsicher-Verbindung verweigert* aus.
13. Aktivieren Sie auf der Registerkarte *Einschränkungen* die Option *Clients gestatten ohne Aushandlung einer Authentifizierungsmethode eine Verbindung herzustellen*.
14. Wechseln Sie auf die Registerkarte *Einstellungen*.
15. Klicken Sie auf die Option *NAP-Erzwingung*.
16. Stellen Sie sicher, dass die Option *Eingeschränkten Zugriff gewähren* aktiviert ist (Abbildung 12.54).
17. Erstellen Sie eine zweite Richtlinie, zum Beispiel mit der Bezeichnung *TS_CAP_02_PASS*.
18. Gehen Sie bei dieser Richtlinie analog vor und verwenden Sie als Integritätsrichtlinie die Zugriffsrichtlinie, wenn der PC NAP-Bedingungen erfüllt und gewähren Sie diesem Client vollen Zugriff.
19. Optional können Sie eine weitere Richtlinie erstellen, die Sie für Clients konfigurieren, die kein NAP beherrschen (alle Windows-Versionen vor Windows XP SP2).

Abbildg. 12.54 Konfigurieren der NAP-Erzwingung



Die Konfiguration der Richtlinie, in der definiert wird, auf welche Terminalserver die Anwender zugreifen können (TS-RAP), finden Sie über den Knoten *Ressourcenautorisierungsrichtlinien*. Stellen Sie hier nach der Installation sicher, ob in der entsprechenden Richtlinie die Terminalserver entweder als einzelnes Computerkonto oder besser als Gruppe hinterlegt sind (Abbildung 12.54). Sie müssen an dieser Stelle sicher sein, dass Ihre Auswahl konsistent ist. Das heißt, dass für die Gruppen, die Sie in der TS-CAP definieren, eine TS-RAP existieren muss, die auf die entsprechende Gruppe im Active Directory verweist, in der sich die Computerkonten der Terminalserver befinden.

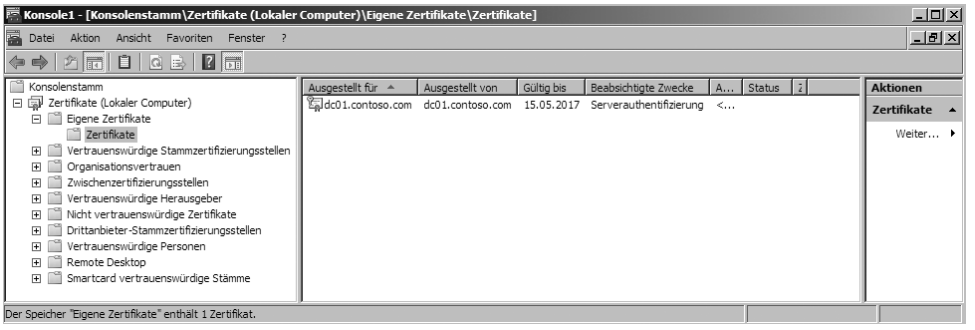
Abbildg. 12.55 Konfiguration der TS-RAP



Damit das Terminaldienstegateway funktioniert, müssen Sie darüber hinaus sicherstellen, dass der Systemdienst *Terminaldienstegateway* gestartet ist. Ohne diesen Dienst ist keine Verbindung möglich. Auch die Standardwebseite in der IIS 7.0-Verwaltung muss gestartet sein, damit der Zugriff funktioniert. Stellen Sie sicher, dass das Zertifikat für den TS Gateway-Server installiert ist. Sie können in den Eigenschaften des Servers auf der Registerkarte *SSL-Zertifikat* entweder das bei der Installation erstellte Zertifikat verifizieren oder ein neues Zertifikat ausstellen. Stellen Sie sicher, dass das Zertifikat auf dem Server installiert ist. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie über *Start/Ausführen/mmc* eine neue Managementkonsole und fügen Sie das Snap-In *Zertifikate* hinzu.
2. Wählen Sie im anschließend geöffneten Dialogfeld die Option *Computerkonto* aus und klicken Sie auf *Weiter*.
3. Wählen Sie im nächsten Dialogfeld die Option *Lokalen Computer* aus, klicken Sie auf *Fertig stellen* und anschließend auf *OK*.
4. Klicken Sie in der Konsolenstruktur auf *Zertifikate/Eigene Zertifikate/Zertifikate*. Hier sollte das Serverzertifikat hinterlegt sein. Ist dies nicht der Fall, können Sie an dieser Stelle ein Zertifikat aus einer Datei importieren.

Abbildg. 12.56 Anzeigen des Serverzertifikats für das TS Gateway

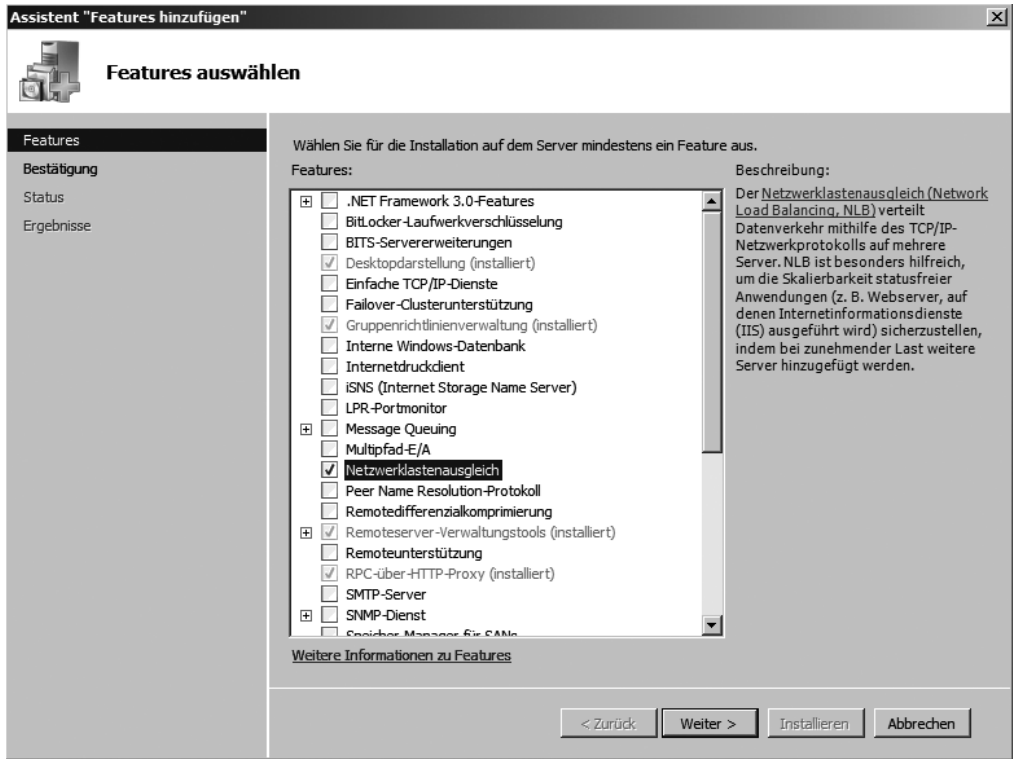


Terminaldienste-Sitzungsbroker (Terminal Service Session Broker)

Der neue Terminaldienste-Sitzungsbroker (TS Session Broker) hat die Aufgabe, Benutzer wieder mit ihren getrennten Sitzungen zu verbinden, wenn Sie die Terminaldienste in einer Farm einsetzen. Vor allem beim Einsatz von Loadbalancing speichert diese Funktion den Benutzernamen, die Session-ID und den Terminalserver, auf dem der Anwender verbunden war. Damit die Benutzer wieder mit der entsprechenden Sitzung auf ihrem Terminalserver verbunden werden, müssen allerdings alle Server in der Loadbalancing-Farm unter Windows Server 2008 laufen. Eine gemischte Umgebung mit Windows Server 2003 wird für diese Funktion nicht unterstützt. Der Netzwerklastenausgleich unterstützt die Lastverteilung auf der Ebene des TCP/IP-Protokolls und findet sich daher bei den Einstellungen für die Netzwerkverbindungen. Bei NLB werden mehrerer Systeme zu einem Cluster zusammengeschlossen. Der NLB sorgt dafür, dass die eingehenden TCP/IP-Anforderungen optimal auf die verschiedenen Server verteilt werden. Diese Art des Clustering ist vor allem für Webserver sowie für Terminaldienste gedacht.

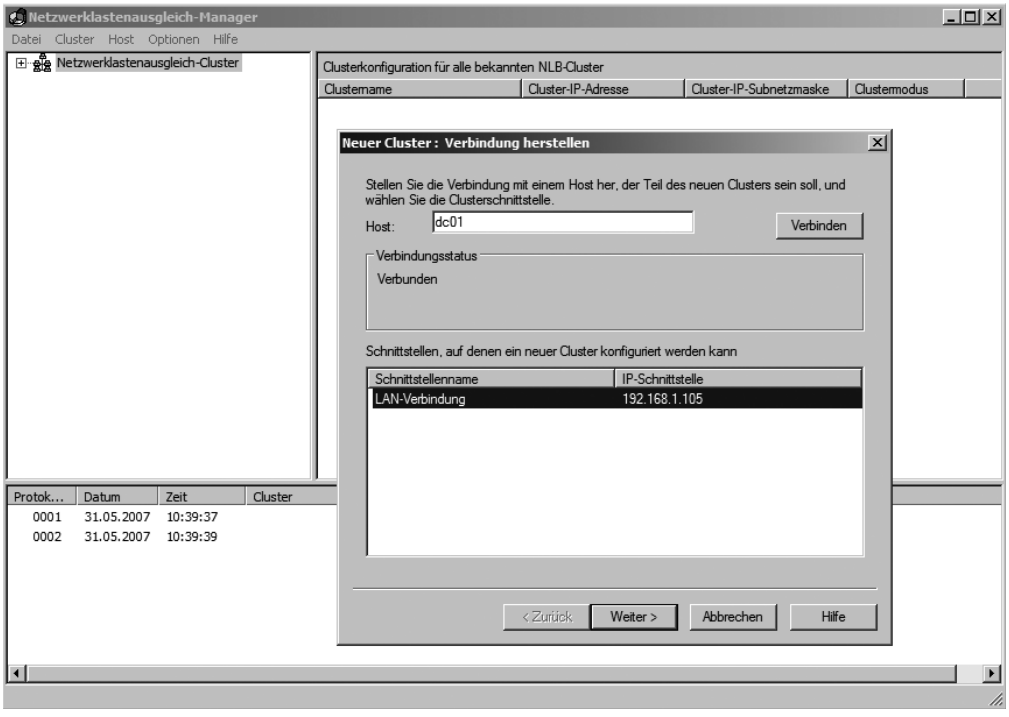
HINWEIS Der Terminaldienste-Sitzungsbroker sollte nicht auf einem Terminalserver installiert werden. Auch der Remotedesktop sollte auf diesem Server nicht aktiviert werden. Da der Terminaldienste-Sitzungsbroker auf die Network Loadbalancing (NLB)-Funktion von Windows Server 2008 aufsetzt, sollte auch diese Funktion eingerichtet werden. Der Sitzungsbroker speichert seine Informationen in einer Datenbank. Alle Server, die in einem NLB-Verbund beteiligt sind, sollten sich im gleichen Subnetz befinden. Sie müssen für alle beteiligten Server im NLB-Verbund den gleichen Farmnamen verwenden, da über diese Konfiguration der Sitzungsbroker die Benutzeranmeldungen verteilt. NLB können Sie über den Server-Manager als neues Feature hinzufügen. Alternativ können Sie NLB auch über die Befehlszeile mit dem Befehl *servermanagercmd.exe –install nlb* installieren. Falls Sie für die Installation die grafische Oberfläche verwenden, wählen Sie die Funktion *Netzwerklastenausgleich* aus (siehe Abbildung 12.57 und Kapitel 19).

Abbildg. 12.57 Installieren des Netzwerklastenausgleichs auf einem Terminalserver



Nach der Installation des Features können Sie über das Verwaltungsprogramm des Netzwerklastenausgleichs einen neuen NLB-Cluster erstellen (siehe hierzu Kapitel 19). In diesem Bereich hat sich im Vergleich zu Windows Server 2003, außer einigen Änderungen in der Oberfläche, nichts Größeres verändert. Wie alle Netzwerkdienste in Windows Server 2008, zum Beispiel DNS oder DHCP, unterstützt der Netzwerklastenausgleich jetzt auch IPv6 für die Kommunikation zwischen den Clusterknoten. Auch die Zusammenarbeit mit einem ISA-Server wurde im Netzwerklastenausgleich verbessert. Es können mehrere IP-Adressen für die Clusterknoten konfiguriert werden, was für Clients, die IPv4- und IPv6-Verkehr verwenden, sinnvoll ist. Zur Verwaltung eines NLB-Clusters dient der *Netzwerklastenausgleich-Manager*, den Sie über *Start/Verwaltung* aufrufen können (Abbildung 12.58).

Abbildg. 12.58 Erstellen eines neuen NLB-Clusters mit dem Netzwerklastenausgleich-Manager

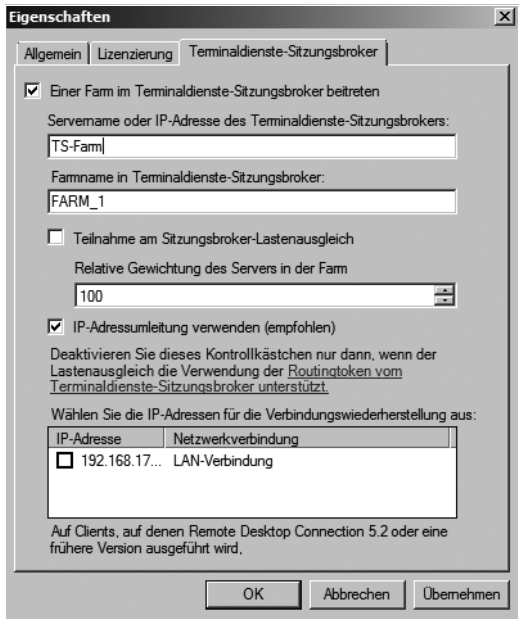


Der Sitzungsbroker kann nur innerhalb eines Loadbalancing-Verbundes verwendet werden. Außerdem müssen alle Server Mitglied einer Active Directory-Domäne sein. Ebenfalls neu ist die Möglichkeit, dass Sie die Performance einzelner Server gewichten können. So können Sie zum Beispiel leistungsfähigeren Servern mehr Benutzer zuteilen als weniger leistungsfähigen Servern. Diese Einstellung können Sie in der Terminaldienstekonfiguration in den Eigenschaften für den Terminaldienste-Sitzungsbroker konfigurieren. Alternativ können diese Einstellungen auch über Gruppenrichtlinien vorgenommen werden. Die entsprechenden Einstellungen finden Sie unter *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Terminaldienste/Terminalserver.* Für den Sitzungsbroker gibt es an dieser Stelle einen eigenen Unterpunkt.

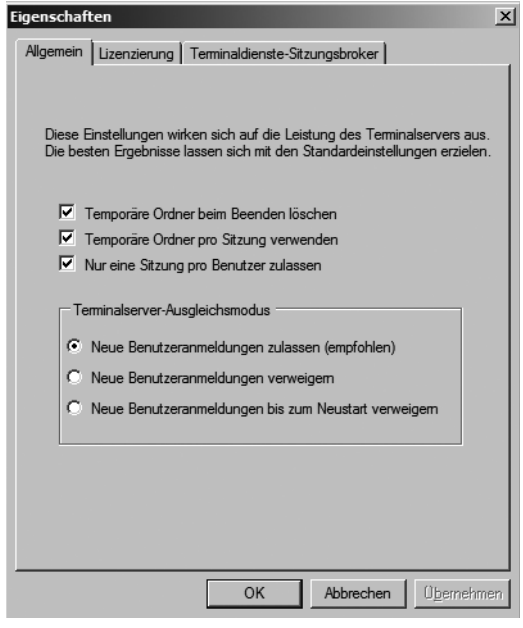
Auf der Registerkarte *Allgemein* können Sie neue Benutzeranmeldungen des Servers deaktivieren, wenn Sie einen Server in einer Farm zum Beispiel warten müssen. Die Anwender werden in diesem Fall auf andere Server in der Farm verteilt und bekommen von dieser Konfiguration nichts mit. Will sich ein Benutzer über den Terminaldienste-Sitzungsbroker wieder mit seiner getrennten Sitzung verbinden, aber der Server steht nicht zur Verfügung, wird er automatisch auf einen anderen Server verbunden. Auf diesem neuen Server wird in diesem Fall auch eine neue Sitzung erstellt, da die getrennte Sitzung auf dem Ursprungsserver nicht zur Verfügung steht.

ACHTUNG Verwenden Sie bei allen Einstellungen auf allen Servern, auch in den Gruppenrichtlinieneinstellungen, immer den gleichen Farm-Namen. Nur dann ist sichergestellt, dass alle Einstellungen auch auf allen Servern in der Farm angewendet werden.

Abbildg. 12.59 Konfigurieren des Terminaldienste-Sitzungsbrokers auf einem Terminalserver und die relative Gewichtung des Servers in der Farm



Abbildg. 12.60 Konfiguration der Anmeldung auf einem Terminalserver für das Loadbalancing



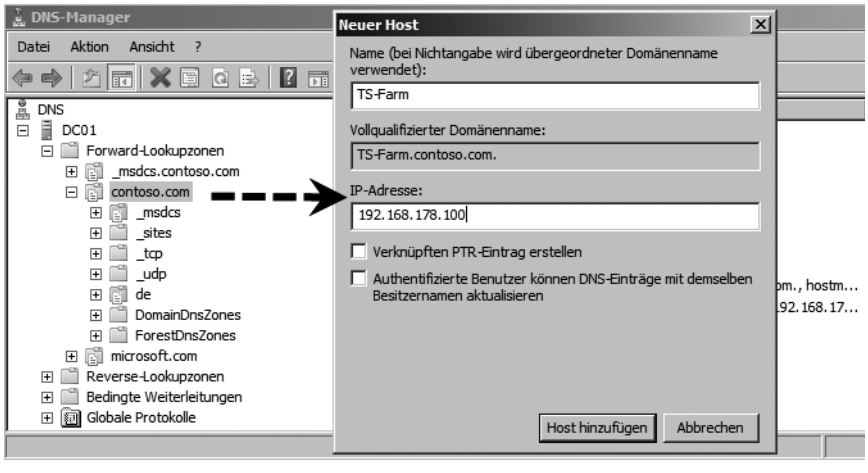
ACHTUNG Auf dem Server, auf dem Sie den Terminaldienste-Sitzungsbroker installiert haben, wird eine lokale Gruppe mit der Bezeichnung *Sitzungsverzeichnis-Computer* (Session Directory Computers) erstellt. Die lokale Benutzerverwaltung rufen Sie am besten über *Start/Ausführen/lusrmgr.msc* auf. Jedes Terminalserver-Computer-Konto, das Mitglied der Farm werden soll, muss in diese Gruppe auf dem TS-Broker-Server aufgenommen werden.

Konfigurieren von Round Robin

Erstellen Sie eine Serverfarm für den TS-Sitzungsbroker, müssen Sie auch Konfigurationen im DNS vornehmen. Diese Konfiguration wird als *Round Robin* bezeichnet. Das ist ein einfacher Mechanismus, mit dem DNS-Server die Last auf Netzwerkressourcen verteilen. Round Robin wird verwendet, um die Reihenfolge der zurückgegebenen Ressourceneinträge in der Antwort auf eine Abfrage zyklisch zu ändern, wenn es für den verlangten DNS-Domänennamen mehrere Einträge desselben Typs gibt. Diese einfachste Form der Lastverteilung auf mehrere Computer wird als DNS-Round-Robin bezeichnet (siehe auch Kapitel 11). Dabei wird ein Hostname mehrfach, mit jeweils anderer IP-Adresse eingetragen. Erreicht den DNS-Server jetzt eine Anfrage des Clients, liefert er die Liste aller gefundenen IP-Adressen zurück, wobei er die Reihenfolge der Einträge jeweils um eins verschiebt. Damit wird im Mittel jeder Eintrag gleich häufig an erster Stelle dem Client zurückgeliefert. Um dem Client möglichst einen Server direkt in seiner Nähe zu nennen – im TCP/IP bedeutet das, innerhalb desselben IP-Subnetzes – wird bei Hostnamen mit mehreren zugeordneten IP-Adressen vor der Umsortierung durch Round Robin zunächst ermittelt, ob es einen Eintrag gibt, der dem Subnetz des Clients zuzuordnen ist. Dieser wird anschließend an die erste Stelle der zurückgegebenen Liste gesetzt. Nur wenn kein passender eindeutiger Eintrag gefunden wird, kommt Round Robin zur Lastverteilung zum Einsatz. Um einen Round Robin-Eintrag für die Farm zu erstellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Verwaltung Ihres DNS-Servers.
2. Erstellen Sie in der Zone von Active Directory einen neuen Forward-Lookup-Eintrag mit der Bezeichnung der Farm. Verwenden Sie als Farmnamen keinesfalls den Namen eines Servers innerhalb der Farm, sondern einen eigenständigen Namen.

Abbildg. 12.61 Erstellen von neuen HOST A-Einträgen für die Unterstützung von Round Robin



3. Tragen Sie als IP-Adresse die Adresse eines Servers in der Farm ein und bestätigen Sie die Erstellung des Eintrags.
4. Erstellen Sie jetzt für jeden weiteren Server der Farm einen identischen Eintrag, der jeweils zur IP-Adresse des Servers zeigt.
5. Abschließend haben Sie für jeden Server in der TS-Farm einen Eintrag mit gleichem Namen und jeweils einer IP-Adresse für einen Server in der Farm.

Terminaldienste und der Windows System Resource Manager

Durch die Integration von Windows-Systemressourcen-Manager (Windows System Resource Managers, WSRM) direkt in das Betriebssystem können Sie CPU und Arbeitsspeicher direkt einzelnen Applikationen, Diensten oder Prozessen zuweisen. So können Sie verhindern, dass unwichtige Applikationen auf einem Server andere, wichtigere Applikationen ausbremsen.

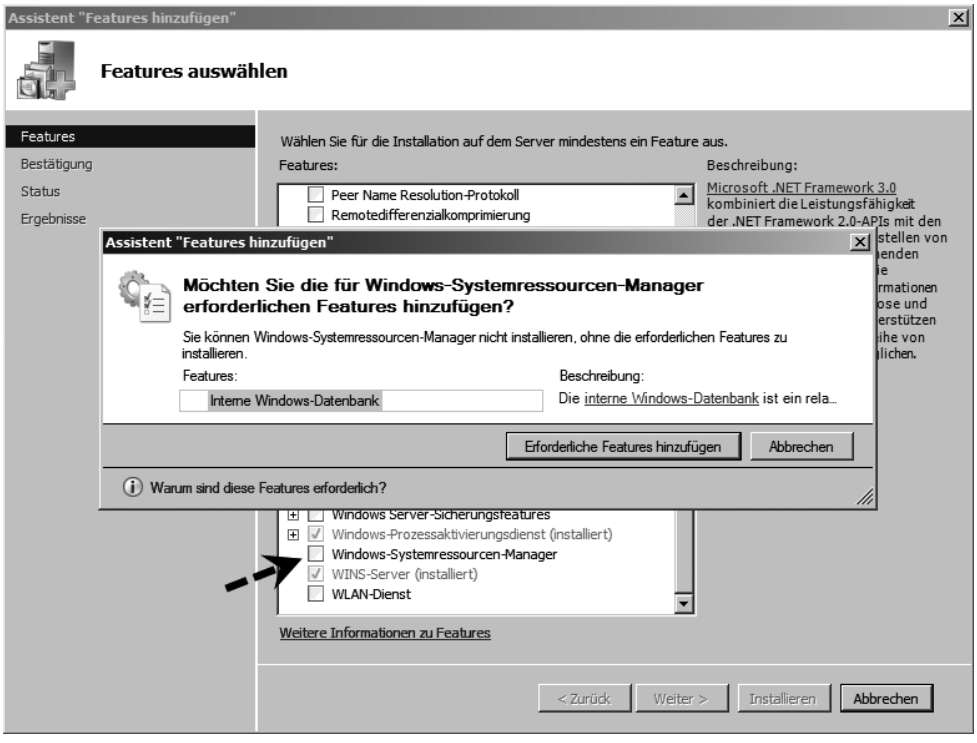
TIPP Wollen Sie den WSRM zusammen mit den Terminaldiensten einsetzen, sollten Sie vor der Installation des WSRM zunächst die Terminaldienste installieren.

Installieren von WSRM

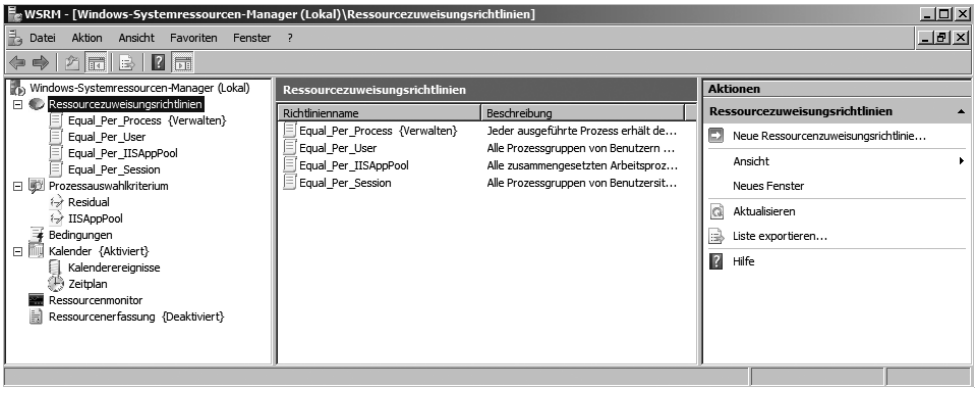
Um den WSRM auf einem Terminalserver zu installieren, gehen Sie folgendermaßen vor (Abbildung 12.62):

1. Starten Sie den Server-Manager und klicken Sie auf *Features/Features hinzufügen*.
2. Wählen Sie die Funktion *Windows-Systemressourcen-Manager* aus.
3. Bestätigen Sie die Meldung *Erforderliche Funktionen hinzufügen* und schließen Sie die Installation ab.
4. Stellen Sie sicher, dass der Systemdienst *Windows-Systemressource-Manager* gestartet ist und auf *Automatisch* steht. Die Dienste finden Sie am schnellsten, wenn Sie im Suchfeld des Startmenüs *services.msc* eingeben.
5. Nachdem Sie den WSRM installiert und den dazugehörigen Systemdienst gestartet haben, können Sie die Verwaltung der Funktion über *Start/Verwaltung/Windows-Systemressourcen-Manager* starten (Abbildung 12.63).
6. Lassen Sie sich mit dem lokalen Computer verbinden.

Abbildg. 12.62 Installation des WSRM auf einem Server



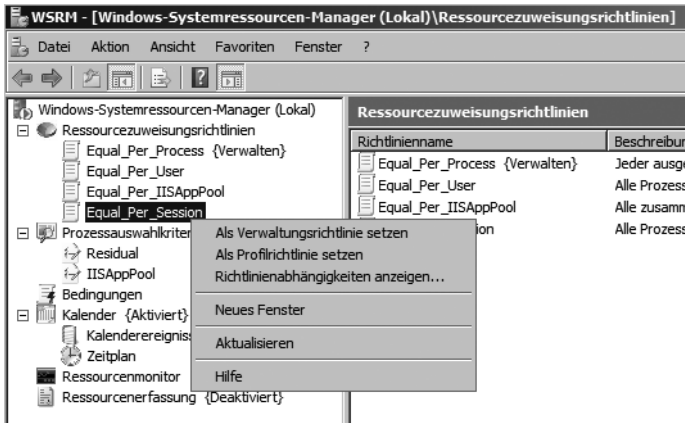
Abbildg. 12.63 Verwalten des Windows-Systemressourcen-Managers



Um die Ressourcen auf einem Terminalserver zu verwalten, dienen hauptsächlich die beiden Ressourcezuweisungsrichtlinien *Equal_Per_User* und *Equal_Per_Session*. Die Richtlinie *Equal_Per_Session* ist neu in Windows Server 2008. Idealerweise setzen Sie diese Richtlinie ein, um die Ressourcen auf einem Terminalserver zu steuern. In diesem Fall erhalten die Anwender und deren gestartete Prozesse gleichmäßig CPU und Speicher zugeteilt. Um diese Richtlinie als Basis für die Verteilung zu

verwenden, klicken Sie diese mit der rechten Maustaste an und wählen Sie die Option *Als Verwaltungsrichtlinie setzen* (Abbildung 12.64).

Abbildg. 12.64 Zuweisen von Systemressourcen mit den WSRM



Tools für Terminalserver

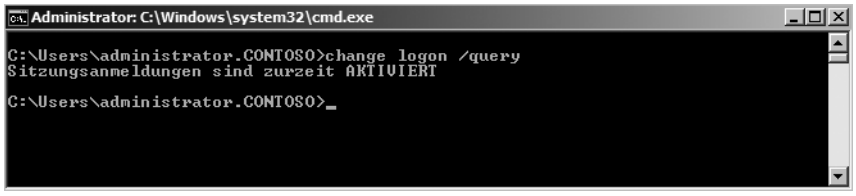
Für die bessere Verwaltung von Terminalservern bringt Windows Server 2008 bereits einige Bordmittel mit, welche einzelne Aufgaben deutlich erleichtern. Im folgenden Abschnitt gehen wir auf die wichtigsten Befehlszeilen-Tools für die Verwaltung von Terminalservern ein sowie auf Zusatztools, welche die Arbeit enorm erleichtern.

Change Logon – Anmeldungen aktiveren oder deaktivieren

Mit diesem Befehlszeilenprogramm können Sie die Anmeldung auf einem Terminalserver aktivieren oder deaktivieren. Wenn Sie zum Beispiel einen Terminalserver warten und nicht wollen, dass sich Benutzer mit dem Server verbinden, können Sie *Change Logon* verwenden. Dazu stehen Ihnen verschiedene Optionen zur Verfügung (Abbildung 12.65):

- **change logon /enable** Aktiviert die Anmeldung auf einem Terminalserver
- **change logon /disable** Deaktiviert die Anmeldung. Es darf sich kein Benutzer mehr auf dem Terminalserver anmelden.
- **change logon /drain** Durch diese Option werden neue Anmeldungen verhindert, aber getrennte Sitzungen auf dem Server können wieder neu aufgebaut werden
- **change logon /query** Mit dieser Abfrage können Sie den aktuellen Status der Anmeldung abfragen

Abbildg. 12.65 Steuerung der Benutzeranmeldung mit *change logon*

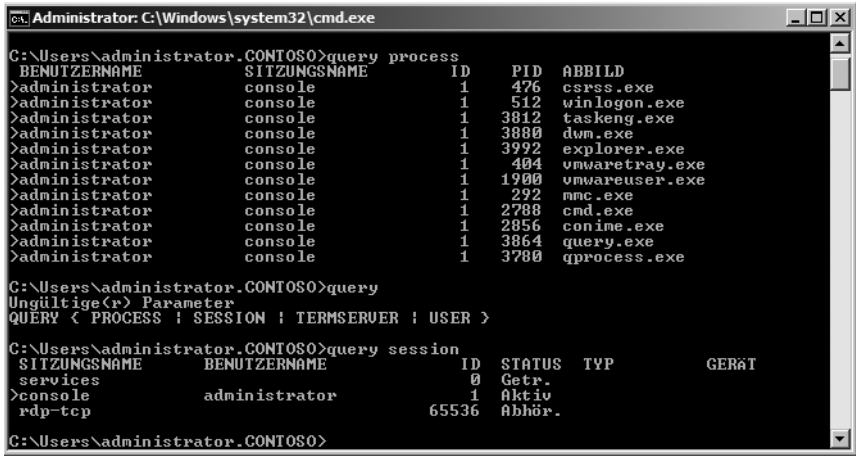


Query – Prozessinformationen auf Terminalservern

Mit diesem Befehl können Sie verschiedene Abfragen in der Befehlszeile starten, um sich einen Überblick zu verschaffen, welche Prozesse zurzeit laufen und welche Benutzer angemeldet sind. Sie können sich alle Terminalserver des Standorts anzeigen lassen. Grundsätzlich gibt es vier wichtige Optionen, die Sie mit Query abfragen können (Abbildung 12.66):

- **query process** Dieser Befehl zeigt alle laufenden Prozesse auf dem Terminalserver.
- **query session** Mit diesem Befehl werden alle laufenden Terminalsitzungen angezeigt.
- **query termserver** Alle Terminalserver im Subnetz werden angezeigt.
- **query user** Alle auf dem Terminalserver angemeldeten Benutzer werden angezeigt.

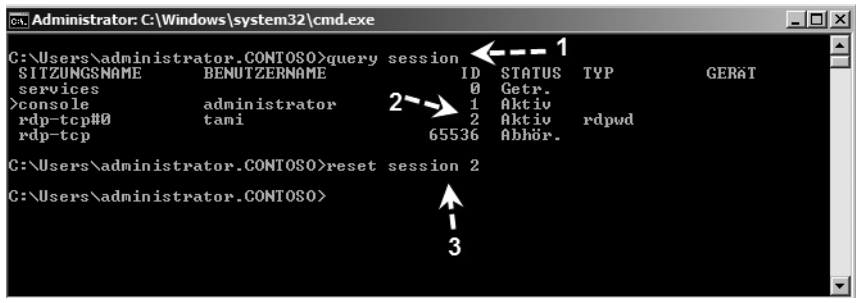
Abbildg. 12.66 Abfragen des Status eines Terminalservers mit dem Befehlszeilentool *query*



Reset – Terminalsitzungen zurücksetzen

Mit diesem Befehl können Sie anhand Ihrer ID Sitzungen auf dem Terminalserver zurücksetzen. Sie können zum Beispiel mit dem Befehl *query session* alle Sitzungen mit deren ID anzeigen lassen. Im Anschluss können Sie mit *reset session <Nummer der Session>* eine bestimmte Sitzung zurücksetzen. Dieser Vorgang geht oft schneller als in der Terminalserververwaltung (Abbildung 12.67).

Abbildg. 12.67 Terminalserver-Sitzungen mit *reset* beenden



TSCON und TSDISCON – Abmelden und Anmelden von Terminalsitzungen

Mit diesen beiden Befehlen können Terminalsitzungen verbunden oder abgemeldet werden. Diese Funktion hat die gleiche Bedeutung wie in der Terminalserververwaltung, wenn eine getrennte Sitzung wieder mit einem Client verbunden werden soll. Bei diesen Befehlen werden die Benutzer nicht zurückgesetzt und deren Sitzung gelöscht, sondern nur getrennt oder erneut verbunden.

TSCON

Tscon {<Sitzungskennung> | <Sitzungsname>} [/dest:<Sitzungsname>] [/password:<Kennwort>] [/v]

Wenn Sie den optionalen Parameter */dest:<Sitzungsname>* verwenden, ist dieser die Kennung der Sitzung, mit der eine Verbindung hergestellt werden soll. Dieser gibt den Namen der aktuellen Sitzung an. Diese Sitzung wird getrennt, wenn eine Verbindung mit der neuen Sitzung hergestellt wird. Sie müssen über die Zugriffsberechtigung für den Vollzugriff oder über die beschränkte Zugriffsberechtigung für den Verbindungsaufbau verfügen, um eine Verbindung mit einer anderen Sitzung herstellen zu können. Mit dem Parameter */dest:<Sitzungsname>* können Sie die Sitzung eines anderen Benutzers mit einer anderen Sitzung verbinden. Geben Sie im Parameter *Kennwort* kein Kennwort an und gehört die Zielsitzung einem anderen Benutzer als dem aktuellen, schlägt die Ausführung von *tscon* fehl. Mit der Konsolensitzung kann keine Verbindung hergestellt werden.

Beispiele:

- Geben Sie *tscon 12* ein, um eine Verbindung mit Sitzung *12* auf dem aktuellen Terminalserver herzustellen und um die aktuelle Sitzung zu trennen.
- Geben Sie *tscon 23 /password:<meinkennwort>* ein, um eine Verbindung mit Sitzung *23* auf dem aktuellen Terminalserver unter Verwendung des Kennworts *meinkennwort* herzustellen und um die aktuelle Sitzung zu trennen.
- Geben Sie *tscon TERM03 /v /dest:TERM05* ein, um eine Verbindung zwischen der Sitzung *TERM03* und der Sitzung *TERM05* herzustellen und dann die noch verbundene Sitzung *TERM05* zu trennen.

TSDISCON

Tsdiscon [{Sitzungskennung | Sitzungsname}] [/server:Servername] [/v]

Zum Trennen eines anderen Benutzers von einer Sitzung müssen Sie über die Berechtigung zum Vollzugriff verfügen. Wird keine Sitzungskennung oder kein Sitzungsname angegeben, trennt *tsdiscon* die aktuelle Sitzung. Alle Anwendungen, die beim Trennen der Sitzung ausgeführt wurden, werden beim erneuten Verbinden mit dieser Sitzung automatisch und ohne Datenverlust wieder ausgeführt. Verwenden Sie den Befehl *reset session*, um die aktiven Anwendungen der getrennten Sitzung zu beenden. Dies kann jedoch bei der betreffenden Sitzung zum Verlust von Daten führen. Der Parameter */server* ist nur erforderlich, wenn Sie *tsdiscon* von einem Remoteserver aus verwenden. Die Konsolensitzung kann nicht getrennt werden.

Beispiele:

Geben Sie *tsdiscon* zum Trennen der aktuellen Sitzung ein.

Geben Sie *tsdiscon 10* zum Trennen von Sitzung 10 ein.

Geben Sie *tsdiscon TERM04* zum Trennen der Sitzung mit dem Namen *TERM04* ein.

TSKILL – Prozesse auf Terminalservern beenden

Mit diesem Befehl können Sie einzelne Prozesse auf einem Terminalserver beenden. Sie können sich zum Beispiel mit *query process* alle laufenden Prozesse anzeigen lassen und im Anschluss mit *tskill <PID des Prozesses>* den Prozess beenden.

Syntax: *Tskill {<Prozesskennung> | <Prozessname>} [/server:<Servername>] [{/id:<Sitzungskennung> | /a}] [/v]*

- **Prozesskennung** Die Kennung des zu beendenden Prozesses (PID)
- **Prozessname** Der Name des zu beendenden Prozesses. Sie können bei der Eingabe dieses Parameters Platzhalterzeichen verwenden.
- **/server:<Servername>** Gibt den Terminalserver an, auf dem sich der zu beendende Prozess befindet. Erfolgt keine Angabe, wird der aktuelle Terminalserver verwendet.
- **/id:<Sitzungskennung>** Beendet den in der angegebenen Sitzung ausgeführten Prozess
- **/a** Beendet den in allen Sitzungen ausgeführten Prozess
- **/v** Zeigt Informationen zu den Aktionen an, die gerade ausgeführt werden

Wenn Sie kein Administrator sind, können Sie den Befehl *tskill* nur zum Beenden der Prozesse verwenden, die Sie besitzen. Administratoren haben Vollzugriff auf alle Funktionen von *tskill* und können Prozesse in Sitzungen anderer Benutzer beenden. Werden alle in einer Sitzung ausgeführten Prozesse beendet, wird die Sitzung ebenfalls beendet.

Beispiele:

- Um den Prozess *6543* zu beenden, geben Sie *tskill 6543* ein.
- Um den in Sitzung 5 ausgeführten Prozess *explorer* zu beenden, geben Sie *tskill explorer /id:5* ein.

Zusammenfassung

Mit den neuen Funktionen in den Terminaldiensten wie RemoteApp, das Terminaldienstegateway, den Terminaldienste-Webzugriff sowie den neuen RDP-Client stellen die Terminaldienste in Windows Server 2008 ein mächtiges Werkzeug zur Anwendungsvirtualisierung dar. Wir haben Ihnen in diesem Kapitel ausführlich gezeigt, wie Sie einen Terminalserver unter Windows Server 2008 installieren und betreiben. Im nächsten Kapitel erläutern wir Ihnen, wie Sie die neuen Webserver-Funktionen von Windows Server 2008 konfigurieren, also die Internetinformationsdienste (IIS) 7.0.

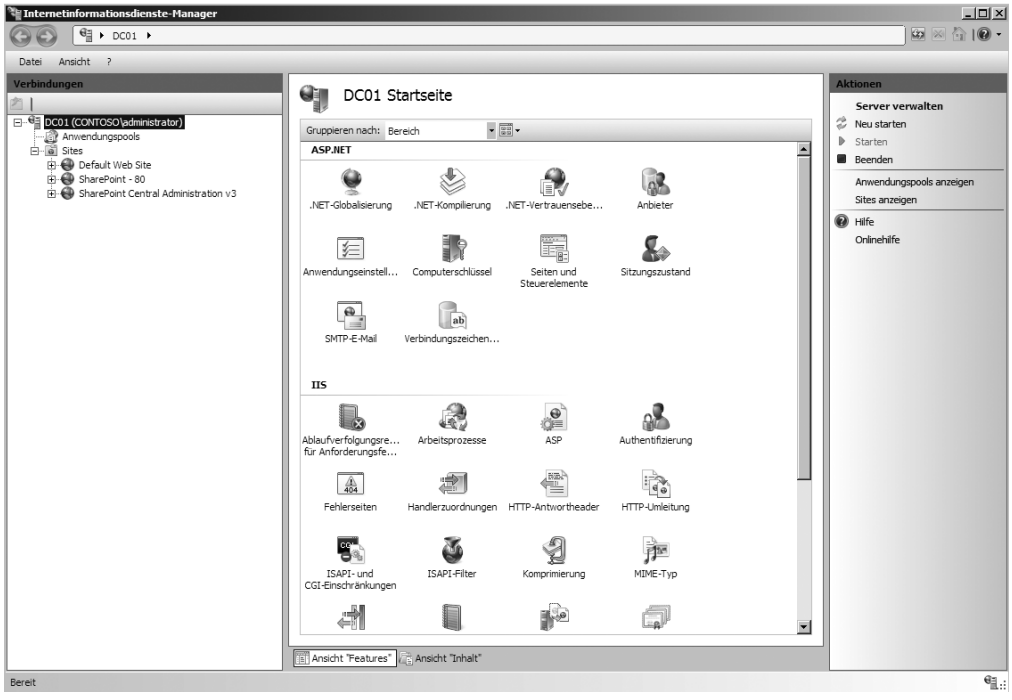
Kapitel 13

Webserver – IIS 7.0

In diesem Kapitel:

Wie Sie bereits in Kapitel 1 gesehen haben, hat Microsoft auch die Internetinformationsdienste (Internet Information Services, IIS) komplett überarbeitet. Während in Windows Server 2003 noch IIS 6.0 ihre Dienste verrichten, wird Windows Server 2008 mit den neuen IIS 7.0 ausgeliefert, die einige Neuerungen mitbringen. In Kapitel 1 wurde bereits auf die wichtigsten Neuerungen eingegangen. Diese werden in diesem Kapitel noch weiter vertieft. Das erste, was Administratoren auffällt, ist die neue Verwaltungsoberfläche von IIS, die deutlich überarbeitet wurde (Abbildung 13.1).

Abbildg. 13.1 Die überarbeitete Oberfläche des Internetinformationsdienste-Managers



Für die Remoteverwaltung von Webservern wird unter Windows Server 2008 nicht mehr das RPC-Protokoll verwendet, sondern HTTP oder HTTPS. Die einzelnen Komponenten zur Verwaltung sind in der neuen Oberfläche schneller zu finden und leichter zu bedienen.

Neuerungen in IIS 7.0

Neben den bereits erwähnten Neuerungen wurde in IIS 7.0 auch einiges in der internen Struktur geändert. *Http.sys*, der Kernelmodus-Treiber für Hypertext Transfer Protocol-(HTTP-)Verkehr, wurde in Windows Server 2008 und Windows Vista für folgende Elemente erweitert:

- **HTTP-Server-API 2.0** Bei der HTTP-Server-API handelt es sich um einen HTTP-Protokolltreiber im Kernelmodus, für den über *Httpapi.dll* APIs im Benutzermodus verfügbar sind. Die HTTP-Server-APIs ermöglichen einer Serveranwendung die Registrierung von HTTP-URLs sowie das Empfangen von Anfragen und von Dienstantworten. HTTP-Server-APIs beinhalten benutzerfreundliche HTTP-Listener-Funktionalität für Windows sowohl für systemeigene als

auch für verwaltete Windows .NET-Anwendungen. Anwendungen können die HTTP-Server-API verwenden, um TCP-Ports gemeinsam mit Internet Information Services (IIS) 6.0 zu verwenden. Dadurch können viel genutzte TCP-Ports (z. B. 80 und 443) gleichzeitig sowohl von HTTP-Server-API-basierten als auch von IIS 6.0-Anwendungen verwendet werden, sofern diese verschiedene Teile des URL-Namespace bedienen.

- **Serverseitige Authentifizierung** *Http.sys* führt nun eine serverseitige Authentifizierung durch. Bislang führten die Serveranwendungen eigene Authentifizierungen durch. Serveranwendungen können jetzt unter geringer privilegierten Konten ausgeführt werden. Es können verschiedene Konten verwendet werden, da *Http.sys* nun die Service Principle Name-(SPN-)Authentifizierung für Anwendungen übernimmt.
- **Protokollierung** *Http.sys* bietet eine zentralisierte W3C-Protokollierung, wobei alle Einträge für sämtliche Sites einer Serveranwendung in einer einzigen Protokolldatei gespeichert werden. Innerhalb der zentralisierten Protokolldatei identifizieren ID-Felder die Site, zu der die Protokolleinträge gehören.
- **Ereignisablaufverfolgung in Windows für HTTP-Ereignisse** Bei der Ereignisablaufverfolgung für Windows (Event Tracing for Windows, ETW) handelt es sich um eine Möglichkeit, in Windows Informationen zu Komponenten und Ereignissen abzurufen, die in der Regel in Protokolldateien geschrieben werden. Mithilfe von ETW-Protokolldateien wird die Problembehebung deutlich erleichtert.
- ***Netsh*-Befehle** Sie können die Konfigurationseinstellungen verwalten und die Diagnose für *Http.sys* über verschiedene Befehle im *Netsh*-HTTP-Kontext steuern. *Netsh* ist ein Befehlszeilentool. Mithilfe dieser neuen Unterstützung können Sie an einer Windows-Eingabeaufforderung zahlreiche Aufgaben durchführen: Konfigurieren von SSL-Zertifikatbindungen, URL-Reservierungen, IP-Überwachungslisten oder globalen Zeitüberschreitungen ist möglich. Auch das Löschen oder Leeren des HTTP-Zwischenspeichers oder das Protokollieren von Puffern. Das Anzeigen des Status des *Http.sys*-Dienstes oder des Zwischenspeichers kann in der Befehlszeile durchgeführt werden.
- **Leistungsindikatoren** *Http.sys* verfügt über neue Leistungsdatenindikatoren, die bei der Überwachung, Diagnose und Kapazitätsplanung von Webservern helfen sollen:
  - Leistungsindikatoren für HTTP-Dienste
  - Anzahl an URLs im Zwischenspeicher, hinzugefügt seit dem Start, gelöscht seit dem Start und Anzahl an Zwischenspeicherleerungen
  - Cachetreffer/Sekunde und Cachefehlversuche/Sekunde
  - HTTP-Dienst-URL-Gruppen
  - Datensenderate, Datenempfangsrate, übertragene Bytes (gesendet und empfangen)
  - Maximale Anzahl an Verbindungen, Verbindungsversuchsrate, Rate für GET- und HEAD-Anfragen und Gesamtanzahl an Anfragen
  - Anfragenwarteschlangen des HTTP-Dienstes
  - Anzahl der Anfragen in der Warteschlange, Alter der ältesten Anfrage in der Warteschlange
  - Rate der Anfrageeingänge in der Warteschlange, Ablehnungsrate, Gesamtzahl der abgelehnten Anfragen und Rate der Cachetreffer

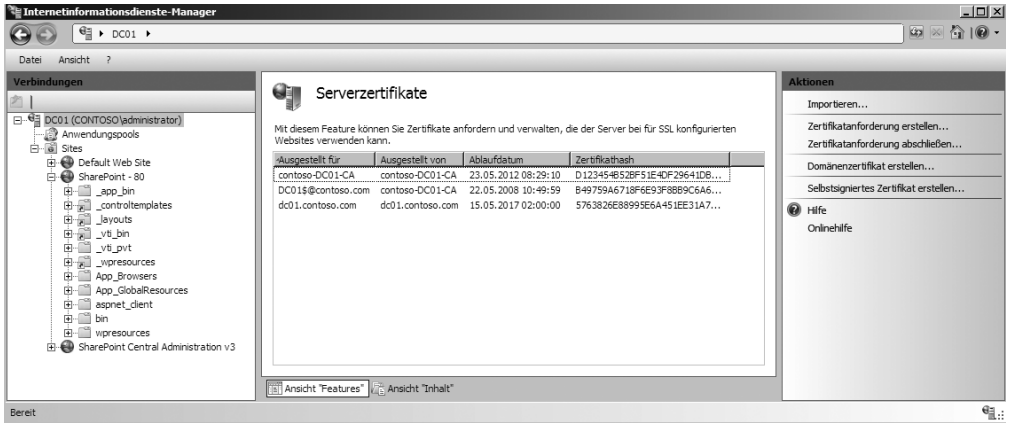
Anders als der Vorgänger IIS 6.0 bieten IIS 7.0 um einen kleinen Webserverkern (Web Core Server) herum die Auswahl unter mehr als 40 IIS-Modulen für Netzwerkprotokolle, Protokollierung, Konfiguration, Authentifizierungsverfahren und Diagnose. Neben den Anwendungsentwicklungsframe-

works wie ASP, ASP.NET, CGI und ISAPI können IIS 7.0 auch in den Bereichen HTTP-Features, Diagnose, Sicherheit und Verwaltungswerkzeuge selektieren. Im Bereich Sicherheit sind verschiedene Authentifizierungsverfahren (Basic, Windows, Digest, Zertifikate) wählbar. Bei den Management-Diensten steht zur Wahl, ob eine Fernverwaltung von IIS über einen Management Service erlaubt sein soll. Im Hinblick auf Sicherheit reduziert dies die Angriffsfläche und erhöht die Sicherheit des Webservers. IIS 7.0 verwendet das .NET-basierte Konfigurationssystem. Alle Einstellungen einer Web-Anwendung, sowohl die von ASP.NET als auch die von IIS, werden in **.config*-Dateien gespeichert. *Web.config*-Dateien bieten gegenüber dem bisherigen Metabase-basierten Konfigurationsmodell einige Vorteile:

- Die Konfigurationsdateien können mit einfachen Werkzeugen (Text- oder XML-Editoren) bearbeitet werden
- Die Konfigurationsdateien können einfacher (per Dateikopie und auch per FTP) übertragen werden
- Geänderte Konfigurationsdateien führen sofort zur Verhaltensänderung
- Die Konfigurationsdateien liegen lokal in dem jeweiligen Webprojekt. Die Delegation von administrativen Aufgaben wird dadurch einfacher.
- In jedem Unterverzeichnis können Konfigurationsdateien existieren, wobei untergeordnete Konfigurationsdateien übergeordnete Einstellung überschreiben

Zentrale Einstellungen, die für den ganzen Webserver gelten, befinden sich in der Datei *applicationHost.config* im Verzeichnis *systemroot\System32\inetsrv*. Die Datei erbt die Einstellungen von der *Machine.config* in .NET Framework. Unterhalb der *applicationHost.config* steht die globale *Web.config-Datei* aus dem Verzeichnis *systemroot\Microsoft.NET\Framework\Versionnummer\CONFIG*. Zur automatisierten Administration bietet IIS 7.0 ein neues Befehlszeilenwerkzeug *AppCMD.exe*. Die Verwaltung der Zertifikate findet jetzt direkt über den Server im Internetinformationsdienste-Manager statt. An dieser Stelle können Sie Zertifikate hinzufügen und die Zertifikate des Servers verwalten.

Abbildg. 13.2 Verwalten der Serverzertifikate in IIS 7.0

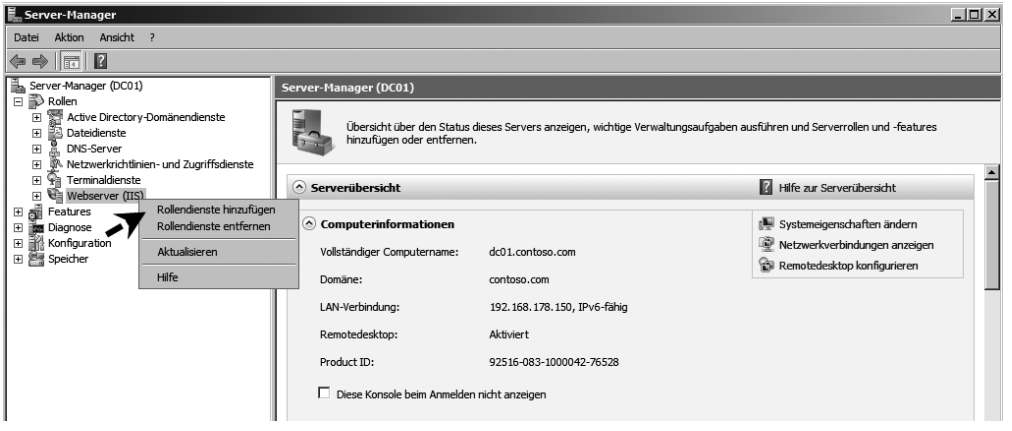


TIPP Auf der Internetseite *www.iis.net* werden vom IIS-Entwicklungsteam ausführliche Informationen zu den Services zur Verfügung stellt.

Authentifizierung in IIS 7.0

Im Bereich der Authentifizierung und Berechtigungen hat Microsoft einige Anpassungen im Vergleich zu IIS 6.0 von Windows Server 2003 vorgenommen. Unterstützte Authentifizierungsverfahren sind vor allem NTLM, Kerberos, Standardauthentifizierung, Formulare und Zertifikate. Auch RSA und Herstellermethoden von Drittanbietern können integriert werden. Die einzelnen Authentifizierungsprotokolle können einzeln installiert werden. Diese Funktion ist neu unter Windows Server 2008. Klicken Sie dazu den Eintrag *Webserver (IIS)* in der Konsolenstruktur des Server-Managers mit der rechten Maustaste an und wählen Sie im Kontextmenü den Befehl *Rollendienste hinzufügen* aus (Abbildung 13.3). Auf diesem Weg können Sie auch Rollendienste entfernen, zum Beispiel Authentifizierungsmaßnahmen, die Sie nicht auf Ihrem Webserver unterstützen wollen.

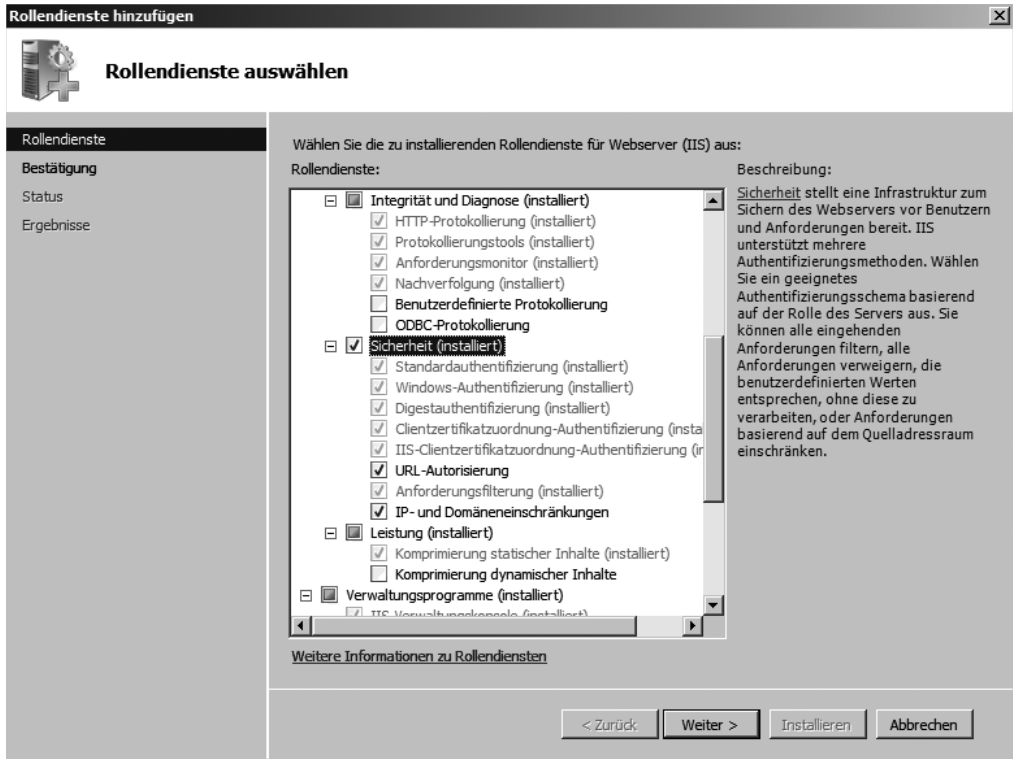
Abbildg. 13.3 Die Authentifizierungsprotokolle können bei IIS 7.0 einzeln über das Hinzufügen oder Entfernen von Rollendiensten installiert oder deinstalliert werden



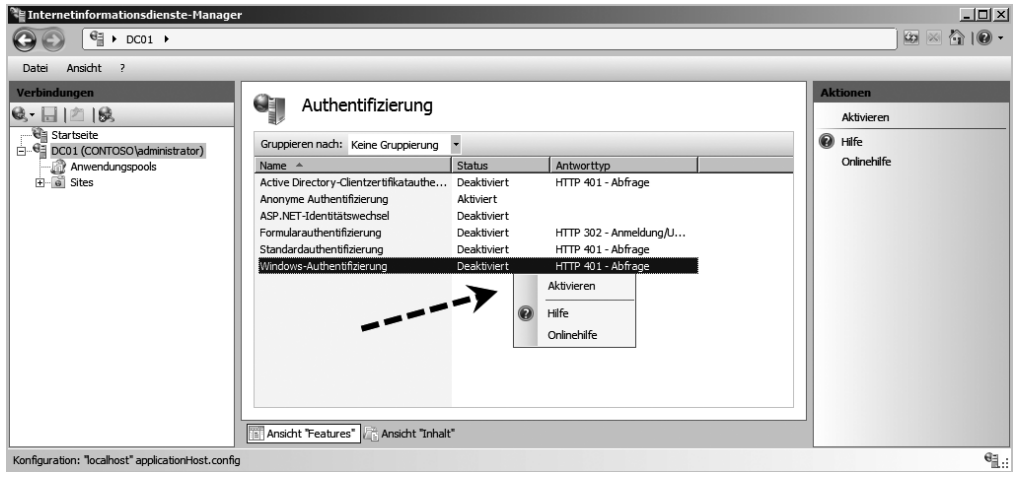
Die Authentifizierungsprotokolle finden Sie unter *Sicherheit* (Abbildung 13.4). Hier können einzelne Protokolle aus- oder abgewählt werden.

Im Internetinformationsdienste-Manager können über *Authentifizierung* die einzelnen Authentifizierungsprotokolle für den kompletten Server aktiviert oder deaktiviert werden. Der erste Schritt nach der Einrichtung des Servers besteht daher darin, zunächst die unterstützten Authentifizierungsmaßnahmen auf dem Server zu konfigurieren (Abbildung 13.5). Über den Menüpunkt *.NET-Benutzer* können neue Benutzer angelegt werden, die unabhängig von Domänenbenutzerkonten zur Authentifizierung für den Webserver verwendet werden können. Ein Administrator kann sehr einfach über dieses Menü neue Benutzer anlegen und auf deren Basis Berechtigungen vergeben.

Abbildg. 13.4 Auswählen der Authentifizierungsprotokolle für IIS

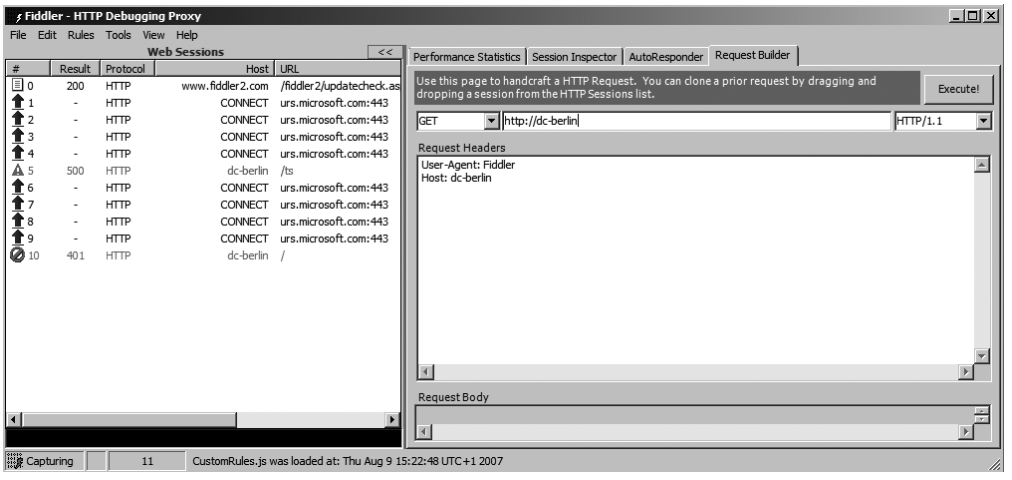


Abbildg. 13.5 Konfigurieren der Authentifizierung in IIS 7.0



TIPP Entwickler und Administratoren, die Authentifizierungsprobleme lösen müssen, sollten Sie von der Internetseite *www.fiddlertool.com* das Tool des Herstellers kostenlos herunterladen. Das Tool bindet sich als Proxy zwischen Browser und IIS und liefert umfangreiche Debuginformationen für Webentwickler und Administratoren (Abbildung 13.6).

Abbildg. 13.6 Analysieren von Authentifizierungsproblemen mit dem kostenlosen Fiddler-Tool



Neue *IIS_WPG*-Gruppe

Die *IIS_WPG*-Gruppe von IIS 6.0 gibt es in dieser Form in IIS 7.0 nicht mehr. Stattdessen gibt es die Gruppe *IIS_IUSRS*, mit der Berechtigungen erteilt werden können. Diese Gruppen sind nicht mehr speziell maschinenbezogen, sondern unterstützen auch das Übertragen und Klonen der IIS-Metabase sowie das Kopieren von Berechtigungen (ACLs) über Xcopy. Diese Gruppe ist daher auf jedem IIS-Server bekannt, sodass gesetzte Berechtigungen übernommen werden können. Da die Berechtigungen nicht durch Benutzernamen, sondern durch SIDs gesetzt werden, können auch diese Daten zwischen IIS 7.0-Servern per Xcopy übernommen werden. Dadurch besteht die Möglichkeit, über die Mitgliedschaft der Gruppe *IIS_IUSRS* auf einem Server auch auf Daten anderer Server im Netzwerk zuzugreifen, sofern dies konfiguriert und erwünscht ist. Auf Basis dieser Gruppenmitgliedschaften dürfen Anwendungspools gestartet und verwaltet werden. Entwickler, die eigene Benutzerkonten für die Verwaltung Ihrer Anwendungspools erstellen, müssen dieses Benutzerkonto nicht mehr manuell der Gruppe *IIS_WPG* hinzufügen, wie noch unter Windows Server 2003. Entsprechende Benutzerkonten werden automatisch in die Gruppe *IIS_IUSRS* aufgenommen.

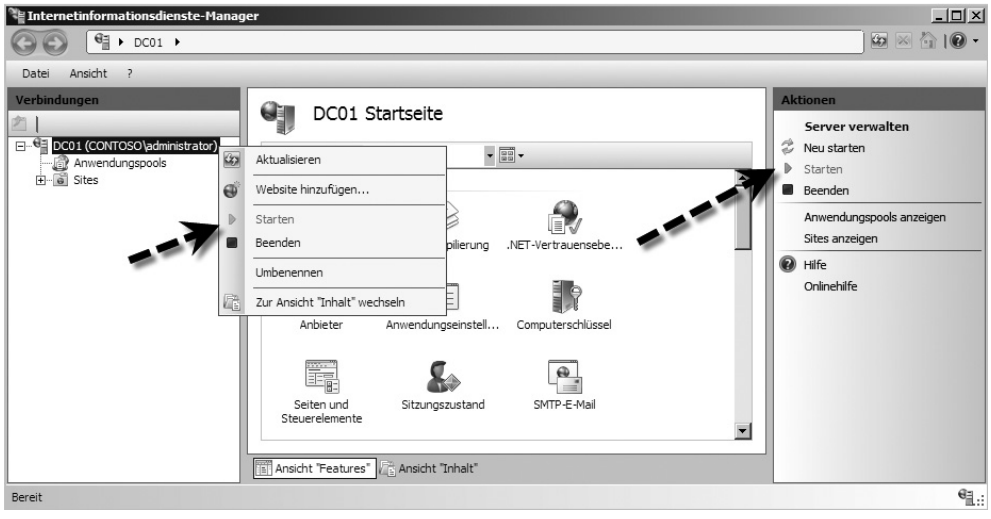
Installieren, konfigurieren und erste Schritte

IIS 7.0 kann als Rolle über den Server-Manager hinzugefügt werden. Nach der Auswahl der zu installierenden Rollendienste können Sie die Verwaltung über den Internetinformationsdienste-Manager starten. Die Oberfläche des Verwaltungstools sieht im Vergleich zu seinem Pendant in Windows Server 2003 deutlich verändert aus. Das Verwaltungstool kann auch über *Start/Ausführen/inetmgr* gestartet werden.

Starten und beenden des Webservers

Beim Installieren von Patches oder der Änderung von wichtigen Systemeinstellungen ist es oft nötig, den Webserver neu zu starten. Dazu muss nicht der ganze Server gebootet werden, sondern die Dienste von IIS können einzeln beendet und wieder gestartet werden. An dieser Vorgehensweise hat sich im Vergleich zu IIS 6.0 von Windows Server 2003 nichts geändert. Das Beenden und der Start von IIS kann über die Verwaltungskonsole durchgeführt werden, indem Sie die entsprechenden Punkte aus dem Kontextmenü des Servers oder im Aktionsbereich auswählen (Abbildung 13.7).

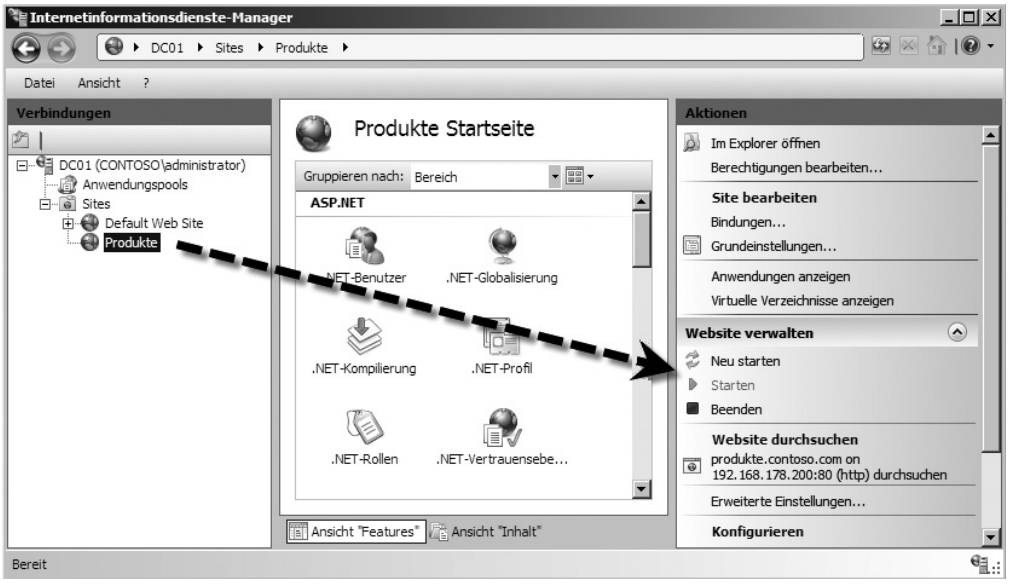
Abbildg. 13.7 Starten und beenden des Webservers in IIS 7.0



Alternativ können Sie in der Befehlszeile auch den Befehl *net stop w3svc* zum Beenden und *net start w3svc* zum Starten des Dienstes eingeben. Neben dem Starten und Stoppen des kompletten Servers können Sie auch einzelne Webseiten zeitweise deaktivieren. Alle anderen Webseiten des Servers bleiben davon unbeeinflusst. Klicken Sie dazu im Internetinformationsdienste-Manager auf die Website, die neu gestartet oder beendet werden soll. Im Aktionsbereich der Konsole wird im Abschnitt *Website verwalten* die Befehle zum Neustart und zum Beenden angezeigt (Abbildung 13.8).

Neben dem Starten und Beenden können auf diesem Weg auch die anderen Einstellungen der Webseite angepasst werden. Über die Befehlszeile kann mit dem Tool *AppCMD.exe* (siehe den folgenden Abschnitt) ebenfalls ein Neustart oder das Beenden erzwungen werden. Zum Beenden beispielsweise der Webseite *Contoso* geben Sie den Befehl *appcmd stop site /site.name:contoso* ein, mit *appcmd start site /site.name:contoso* wird die Seite wieder gestartet.

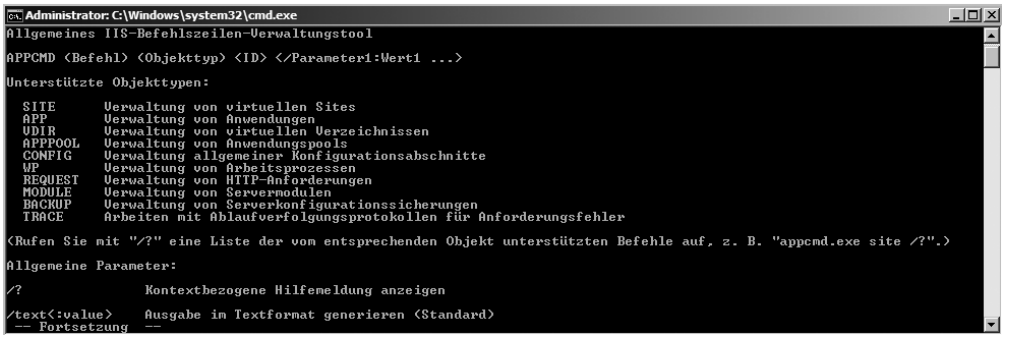
Abbildg. 13.8 Starten und beenden einzelner Webseiten in IIS



IIS in der Befehlszeile verwalten – *AppCMD.exe*

Neben der Verwaltung in der grafischen Oberfläche bietet IIS 7.0 auch ein neues Befehlszeilentool für die Verwaltung mit der Bezeichnung *appcmd.exe* an. Für die Verwaltung von IIS werden nicht mehr verschiedene Tools und Skripts benötigt, wie noch für IIS 6.0, sondern alle Verwaltungsaufgaben werden jetzt in einem Befehlszeilen-Tool zusammengefasst. Das Tool befindet sich allerdings nicht direkt im Pfad der Befehlszeile, kann also nicht direkt aufgerufen werden. Sie müssen zuvor in das Verzeichnis *\Windows\System32\inetsrv* wechseln. Das Tool muss mit Adminrechten gestartet werden. Eine ausführliche Hilfe erhalten Sie über *appcmd /?*. Da die Hilfe kontextsensitiv ist, können Sie auch für einzelne Befehle, wie zum Beispiel *appcmd site /?*, die entsprechende Hilfe aufrufen. Wir zeigen Ihnen in den entsprechenden Abschnitten in diesem Kapitel auch die zu *AppCMD.exe* gehörigen Befehle.

Abbildg. 13.9 Befehlszeilenverwaltungstool für IIS



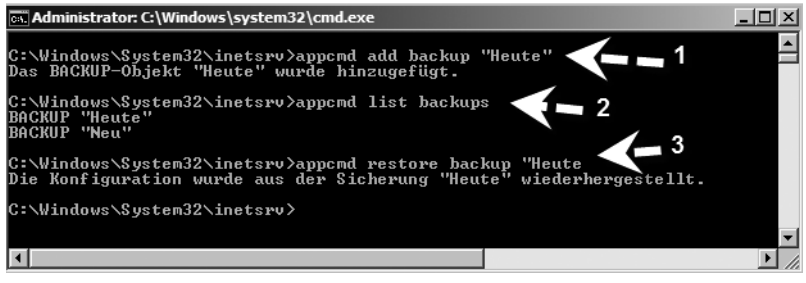
Mit *AppCMD.exe* können Einstellungen des Servers, einzelner Webseiten und von *Web.config*-Dateien angepasst werden. Für die Systemverwaltung von IIS und einzelner Seiten spielen hauptsächlich die drei Dateien *Machine.config*, *Web.config* und *applicationHost.config* eine wesentliche Rolle. In diesen drei Dateien werden die wichtigsten Systemeinstellungen von IIS vorgenommen. Standardmäßig liest und schreibt das Tool Änderungen in die Datei *applicationHost.config*. Soll der Fokus auf die Datei *Machine.config* oder der obersten *Web.config* gesetzt werden, muss zusätzlich noch die Option *commit* verwendet werden. Die zusätzliche Option *MACHINE* für *commit* setzt den Fokus auf *Machine.config*, die Option *WEBROOT* aktiviert oder liest Änderungen aus der obersten *Web.config*. Soll zum Beispiel der Bereich *machineKey* aus der obersten *Web.config* gelesen werden, verwenden Sie den Befehl *appcmd list config /section:machineKey /commit:WEBROOT*. Sollen Einstellungen in der *Web.config* einzelner Seiten vorgenommen werden, muss die Bezeichnung der Seite in den Befehl integriert werden, zum Beispiel über *appcmd set config "Contoso" /section:defaultDocument /enabled:false*. Bei diesem Beispiel werden die Änderungen in der Datei *Web.config* für alle Webseiten unterhalb der Seite *Contoso* vorgenommen. Sollen Änderungen nur in einzelnen Unterwebseiten oder virtuellen Verzeichnissen durchgeführt werden, muss auch dieser Pfad im Befehl mit angegeben werden, zum Beispiel über *appcmd set config "Contoso/Produkte" /section:defaultDocument /enabled:true*.

Beispiele:

Neben den Möglichkeiten, die wir auf den folgenden Seiten vorstellen, können mit *AppCMD.exe* zum Beispiel auch die aktuellen Anfragen an einen Webserver angezeigt werden. Dazu wird der Befehl *appcmd list request* verwendet.

TIPP Die aktuellen Einstellungen eines Servers lassen sich darüber hinaus mit *AppCMD* auch sichern. Mit dem Befehl *appcmd add backup <Name>* kann ein Backup erstellt werden, zum Beispiel bevor Systemänderungen vorgenommen werden. Die erstellten Sicherungen lassen sich über *appcmd list backups* anzeigen und über *appcmd restore backup <Name>* wiederherstellen (Abbildung 13.10).

Abbildg. 13.10 Mit *AppCMD* die Einstellungen von IIS sichern, auflisten und wiederherstellen

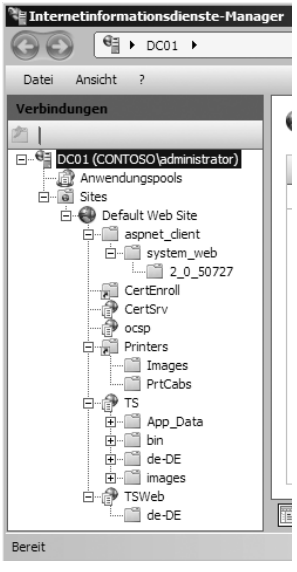


Auch mit der PowerShell können Administrationsaufgaben für IIS durchgeführt werden (siehe Kapitel 24).

Anzeigen der Webseiten in IIS

Die Webseiten, die ein IIS-Server verwaltet, können in der grafischen Verwaltungsoberfläche oder über die Befehlszeile angezeigt werden. In der grafischen Oberfläche werden die Webseiten und deren virtuelle Verzeichnisse in einer Baumstruktur wie im Explorer angezeigt (Abbildung 13.11).

Abbildg. 13.11 Anzeigen der Webseiten eines IIS-Servers



Neben der grafischen Oberfläche können die Webseiten auch in der Befehlszeile über den Befehl *appcmd list site* angezeigt werden. Mit diesem Befehl werden aber nur die Webseiten, nicht die enthaltenen virtuellen Verzeichnisse angezeigt. Auch der Status der einzelnen Seiten wird in der Befehlszeile angezeigt (Abbildung 13.12).

Abbildg. 13.12 Anzeigen von Webseiten und deren Status in der Befehlszeile

Hinzufügen und verwalten von Webseiten

Das Hinzufügen von Webseiten übernehmen viele Applikationen selbst, wie zum Beispiel Exchange, die Terminaldienste, SharePoint usw. In vielen Unternehmen wird IIS aber auch zur Anzeige selbst entwickelter Webseiten und Applikationen für das Internet oder Intranet verwendet. In IIS 7.0 ist das Hinzufügen und Verwalten von Webseiten ähnlich einfach gehalten wie unter IIS 6.0. Allerdings sind verschiedene neue Funktionen hinzugekommen, welche die Sicherheit erhöhen. Standardmäßig werden nicht mehr alle Funktionen automatisch aktiviert, sondern Administratoren und Webentwickler können einzelne Funktionen und Einstellungen detaillierter als unter IIS 6.0 verwalten.

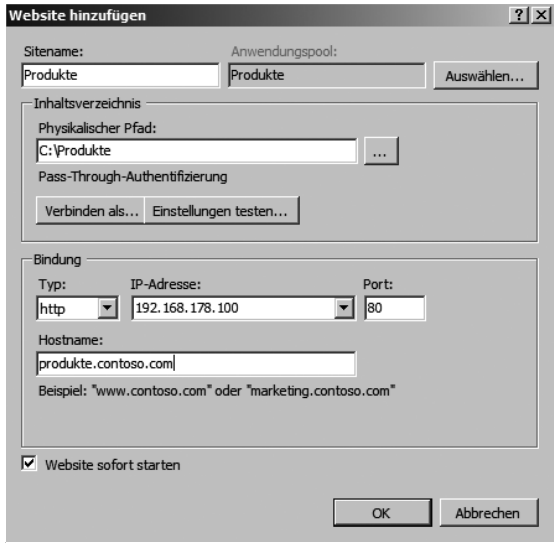
Erstellen einer neuen Webseite

Um eine neue Webseite manuell hinzuzufügen, klicken Sie mit der rechten Maustaste auf den Eintrag *Sites* und wählen im Kontextmenü den Befehl *Webseite hinzufügen* aus (Abbildung 13.13). Dieser Menübefehl steht auch im Aktionsbereich der MMC zur Verfügung.

Abbildg. 13.13 Hinzufügen von neuen Webseiten zu IIS 7.0

Auf dem neuen Fenster können jetzt die Daten für die neue Webseite eingetragen werden. Hier kann auch der Applikationspool ausgewählt sowie der physische Pfad zu der Datei ausgewählt werden. Beim Erstellen einer neuen Webseite wird in IIS 7.0 automatisch auch ein eigener Anwendungspool für diese Webseite erstellt. Ist das nicht gewünscht, kann beim Erstellen auch ohne weiteres ein anderer Anwendungspool verwendet werden. Zusätzlich kann beim Erstellen ausgewählt werden, mit welchem Benutzerkonto sich das System in dem physischen Verzeichnis anmelden darf, um auf die Daten des Servers zuzugreifen. Im Bereich Bindung kann ausgewählt werden, mit welchem Protokoll auf die Webseite zugegriffen wird, auf welche IP-Adresse gehört wird und welcher Port für den Zugriff aktiviert werden soll (Abbildung 13.14).

Abbildg. 13.14 Erstellen und konfigurieren einer neuen Webseite in IIS 7.0



Neben der grafischen Oberfläche können neue Webseiten auch über die Befehlszeile erstellt werden, was die skriptbasierte oder automatisierte Installation von Webservern deutlich erleichtert. Die Syntax sieht in diesem Fall folgendermaßen aus: *appcmd add site /name:<Name> /id:<ID> /physicalPath:<Pfad> /bindings:<URL>*. Als *ID* können Sie eine normale Zahl zur Identifikation der Seite verwenden. Die Option *bindings* ist eine Kombination aus Protokoll, IP-Adresse, Port und Header der Seite. So aktiviert die Option *http/*:88*, dass die neue Seite auf alle Anfragen zu allen Domänen auf den Port 88 antwortet. Durch die Option *http/*:88:shop.contoso.com* hört die Seite auf den Port 88 aller IP-Adressen zur Domäne *shop.contoso.com*.

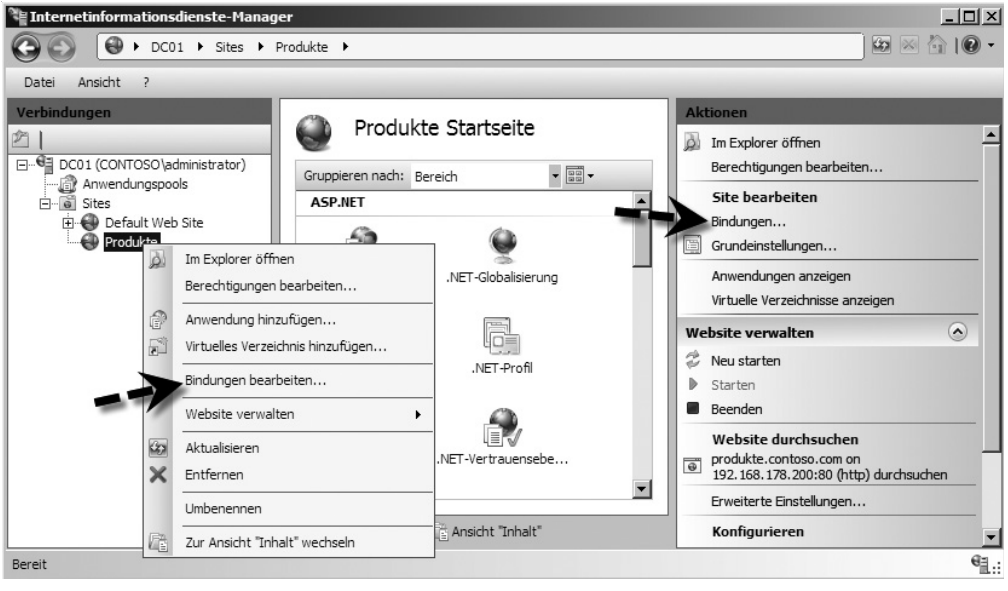
Beispiel

Um eine Seite mit der ID 2 aus dem physikalischen Verzeichnis *c:\contoso*, die auf HTTP-Anfragen zum Port 88 auf alle IP-Adressen und der Domäne *shop.contoso.com* hört, zu aktivieren, verwenden Sie den Befehl *appcmd add site /name:contoso /id:2 /physicalPath:c:\contoso /bindings:http/*:88:shop.contoso.com*.

Bindungen einer Seite nachträglich bearbeiten

Haben Sie eine Webseite erstellt, können die Bindungen, also das Protokoll, die IP-Adresse und der Port jederzeit über das Kontextmenü oder den Aktionsbereich der Seite erweitert werden (Abbildung 13.15). Über das Bindungs-Menü können auch Hostnamen von Webseiten nachträglich bearbeitet und hinzugefügt werden.

Abbildg. 13.15 Die Bindungen von Webseiten können nachträglich angepasst werden



Grundeinstellungen von Webseiten bearbeiten

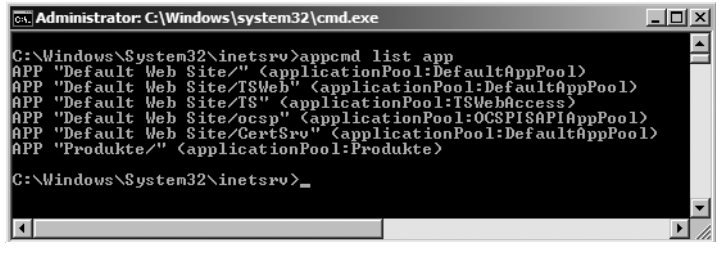
Über den Link *Grundeinstellungen* im Aktionsbereich der Verwaltungskonsole kann der physische Pfad und der Anwendungspool einer Webseite nachträglich angepasst werden (Abbildung 13.16).

Abbildg. 13.16 Bearbeiten der Grundeinstellungen einer Webseite

Verwalten der Webanwendungen und virtuellen Verzeichnisse einer Webseite

Eine einzelne Webseite kann aus mehreren virtuellen Verzeichnissen oder Anwendungen bestehen, die jeweils über eine eigene URL verfügen, aber unter einem gemeinsamen Dach, der Webseite, agieren. Die Anwendungen werden im Internetinformationsdienste-Manager als untergeordnete Objekte der Webseite angezeigt. In der Befehlszeile können Sie die Anwendungen eines Webservers mit dem Befehl *appcmd list app* angezeigt werden (Abbildung 13.17).

Abbildg. 13.17 Anzeigen der Webanwendungen einer Webseite



Sollen nur die Anwendung einer einzelnen Webseite angezeigt werden, verwenden Sie den Befehl *appcmd list app /site.name:<Name>*.

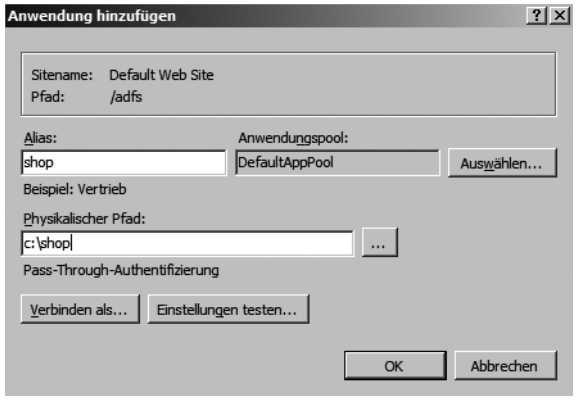
Erstellen einer neuen Webanwendung oder eines virtuellen Verzeichnisses

Um eine neue Webanwendung zu erstellen, klicken Sie mit der rechten Maustaste auf die Webseite, unter der Sie die neue Anwendung erstellen wollen, und wählen im Kontextmenü den Befehl *Anwendung hinzufügen* aus (Abbildung 13.18). Soll ein virtuelles Verzeichnis hinzugefügt werden, benutzen Sie im Kontextmenü die Option *Virtuelles Verzeichnis hinzufügen*.

Abbildg. 13.18 Hinzufügen von neuen Anwendungen zu einer Webseite

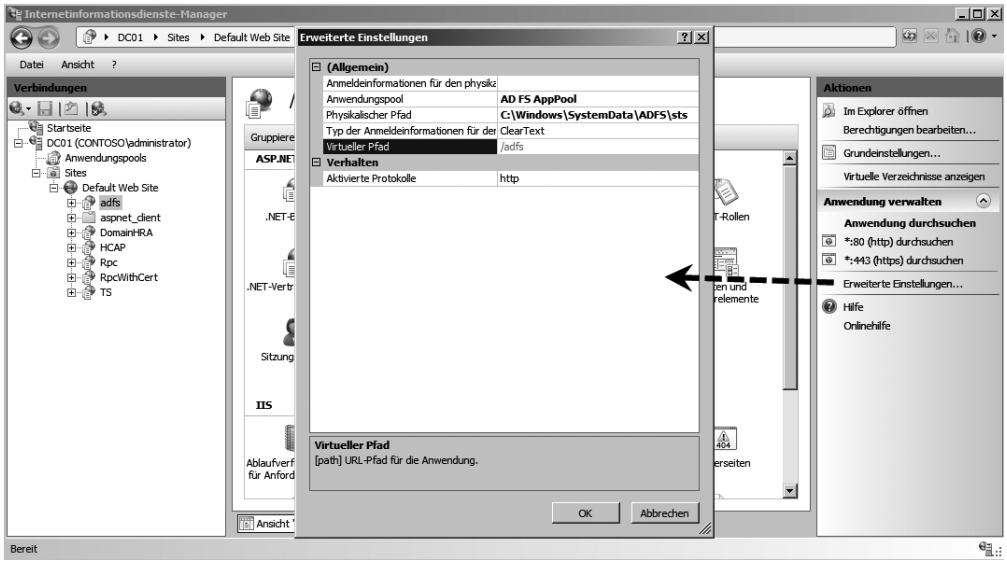
Es öffnet sich ein neues Fenster, über das Sie die Daten für die neue Anwendung konfigurieren können (Abbildung 13.19). Hier kann der Alias, der Anwendungspool, der physische Pfad und der Benutzer konfiguriert werden, mit dem der Dienst auf den Pfad zugreifen soll. Nachdem die Anwendung erstellt wurde, wird diese als untergeordnetes Objekt der Webseite angezeigt. Über die Befehlszeile verwenden Sie den Befehl *appcmd add app /site.name:<Name der Webseite> /path:/<Alias der Anwendung> /physicalPath:<Pfad auf der Platte>*. Die Einstellungen lassen sich ebenfalls wieder über den Aktionsbereich der Konsole bearbeiten.

Abbildg. 13.19 Konfiguration der neuen Anwendung



Die erweiterten Einstellungen einer Webanwendung oder der kompletten Seite lassen sich durch den Link *Erweiterte Einstellungen* im Aktionsbereich oder im Kontextmenü mit dem Befehl *Anwendung verwalten* beziehungsweise *Website verwalten* aufrufen. In diesem Fenster können detaillierte Änderungen vorgenommen werden, als in den jeweiligen Grundeinstellungen.

Abbildg. 13.20 Konfigurieren der erweiterten Einstellungen für eine Webseite oder eine Webanwendung

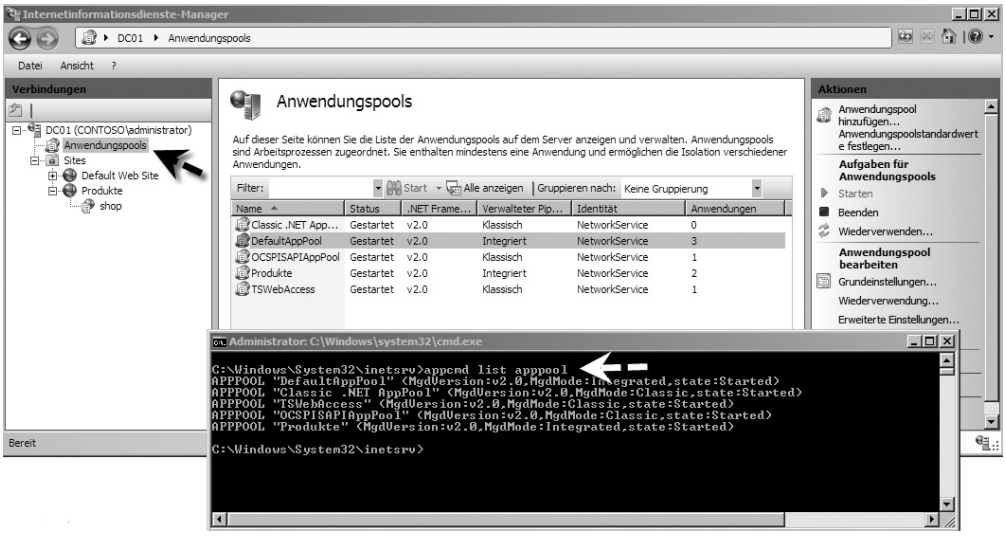


Verwalten von Anwendungspools

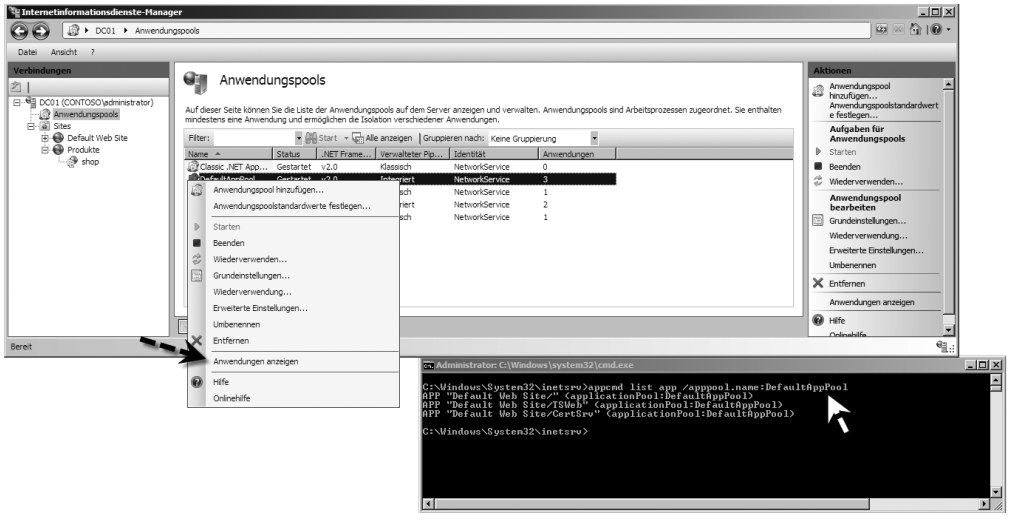
Webseiten und Webanwendungen können unter Windows Server 2008, wie bereits unter Windows Server 2003, in eigenen Anwendungspools und daher Speicherbereichen laufen. Der Absturz einer einzelnen Anwendung führt dabei nicht unweigerlich zum Absturz anderer Anwendungen oder des kompletten Servers. Bei der Erstellung einer neuen Webseite schlägt der Assistent automatisch auch das Erstellen eines eigenen Anwendungspools für die Seite vor. Alle Anwendungspools werden im Internetinformationsdienste-Manager über den Eintrag *Anwendungspools* in der Konsolenstruktur angezeigt und konfiguriert. Über die Befehlszeile können Sie die Anwendungspools über *appcmd list apppool* anzeigen lassen (Abbildung 13.21).

Über den Befehl *Anwendungen anzeigen* im Kontextmenü oder Aktionsbereich des Anwendungspools werden die Webseiten und Anwendungen angezeigt, die sich diesen Anwendungspool teilen. Über die *Zurück*-Schaltfläche in der Oberfläche kommen Sie im Fenster wieder zur Hauptansicht zurück. In der Befehlszeile werden die Anwendung eines Anwendungspools über *appcmd list app /apppool.name:<Name>* angezeigt (Abbildung 13.22).

Abbildg. 13.21 Verwalten und anzeigen der Anwendungspools in IIS 7.0



Abbildg. 13.22 Anzeigen der Anwendungen eines Anwendungspools



Erstellen und verwalten von Anwendungspools

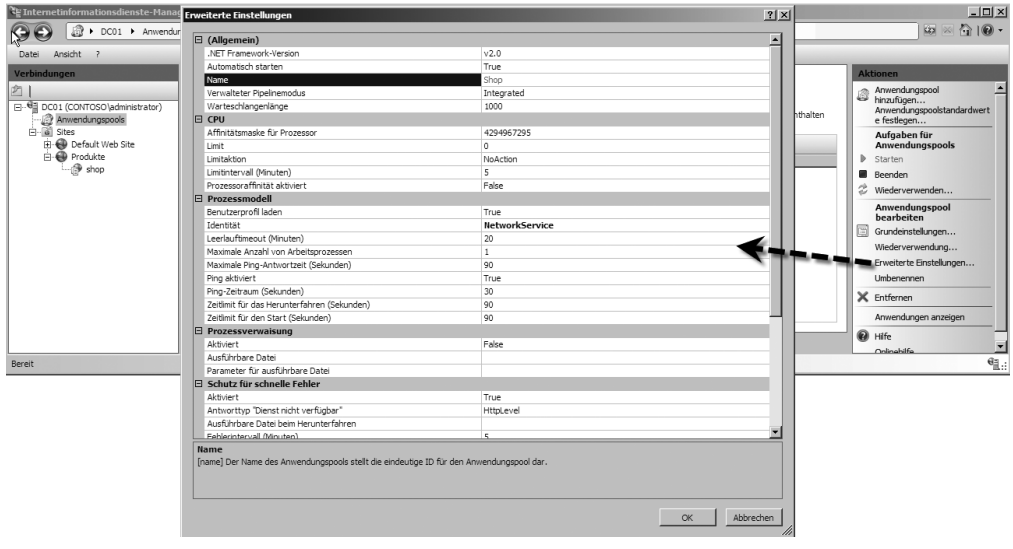
Beim Erstellen einer neuen Webseite kann auf dem entsprechenden Fenster gleich ein neuer Anwendungspool erstellt werden. Über den Eintrag *Anwendungspools* in der Konsolenstruktur des Internetinformationsdienste-Managers kann ebenfalls ein neuer Anwendungspool über das Kontextmenü oder den Aktionsbereich erstellt werden. Beim Erstellen können auf dem Standardfenster zunächst der Name, die Version der unterstützten .NET-Version und der verwaltete Pipelinemodus konfiguriert werden. Dieser steht normalerweise auf *Integriert*. Dadurch werden Anfragen direkt über IIS

und der ASP.NET Pipeline abgebildet. Ältere Anwendungen haben mit dieser Funktion unter Umständen Schwierigkeiten. In diesem Fall können Sie den Modus auf *Klassisch* stellen.

Abbildg. 13.23 Erstellen eines neuen Anwendungspools in IIS 7.0

Im Gegensatz zu IIS 6.0 werden bei der Erstellung von neuen Anwendungspools in IIS 7.0 keine weiteren Einstellungen benötigt. Wollen Sie die Identität des Anwendungspools oder erweiterte Einstellungen anpassen, müssen Sie nach der Erstellung den Befehl *Erweiterte Einstellungen* oder *Anwendungspoolstandardwerte festlegen* im Kontextmenü oder dem Aktionsbereich aufrufen. In dem neuen Fenster können dann die Grundeinstellungen, aber auch die erweiterten Einstellungen wie zum Beispiel die Identität angepasst werden (Abbildung 13.24).

Abbildg. 13.24 Verwalten der erweiterten Einstellungen für Anwendungspools

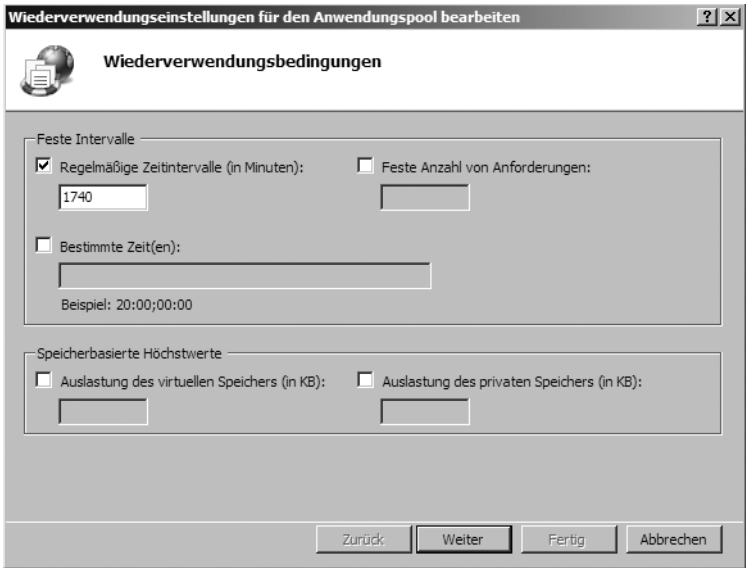


Der Windows Process Activation Services (WAS) überprüft in regelmäßigen Abständen, ob ein Anwendungspool noch funktioniert. Dabei wird, wie beim Pingen, das ICMP-Protokoll verwendet. In den erweiterten Einstellungen kann dieser Ping deaktiviert werden, indem die entsprechende Einstellung von *True* auf *False* gesetzt wird.

Zurücksetzen von Arbeitsprozessen in Anwendungspools

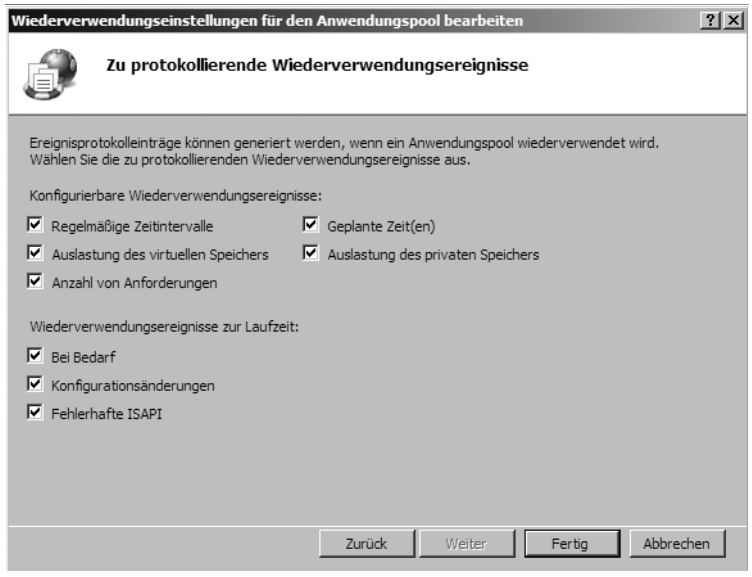
Manche Anwendungen werden im Laufe der Zeit instabiler, da zu viele Anfragen vorliegen oder die Speicherlast zu stark ansteigt. Anwendungspools können in regelmäßigen Abständen die Arbeitsprozesse von Anwendungen zurücksetzen und damit neu starten. Diese Funktion ist ähnlich zum Neustart eines Servers. Dieses Zurücksetzen wird auf englischen Servern *Recyceln*, auf deutschen *Wiederverwenden* genannt. Das Zurücksetzen von Arbeitsprozessen bereinigt laufende Anwendungen und kann diese nach dem Neustart extrem beschleunigen. Dieses Wiederverwenden kann über das Kontextmenü konfiguriert werden. Dabei besteht die Möglichkeit in regelmäßigen Zeitabständen ein Zurücksetzen zu konfigurieren, nach einer bestimmten Anzahl Anfragen oder zu einer bestimmten Zeit. Weitere Möglichkeiten sind das Zurücksetzen bei der starken Auslastung des Arbeitsspeichers oder des virtuellen Speichers.

Abbildg. 13.25 Zurücksetzen von Anwendungen nach bestimmten Kriterien



Das Zurücksetzen von Arbeitsprozessen für Webanwendungen kann Ereignisse in der Ereignisanzeige generieren. Auf der zweiten Seite des Assistenten zur Konfiguration dieses Vorgangs kann ausgewählt werden, welche Ereignisse protokolliert werden sollen (Abbildung 13.26).

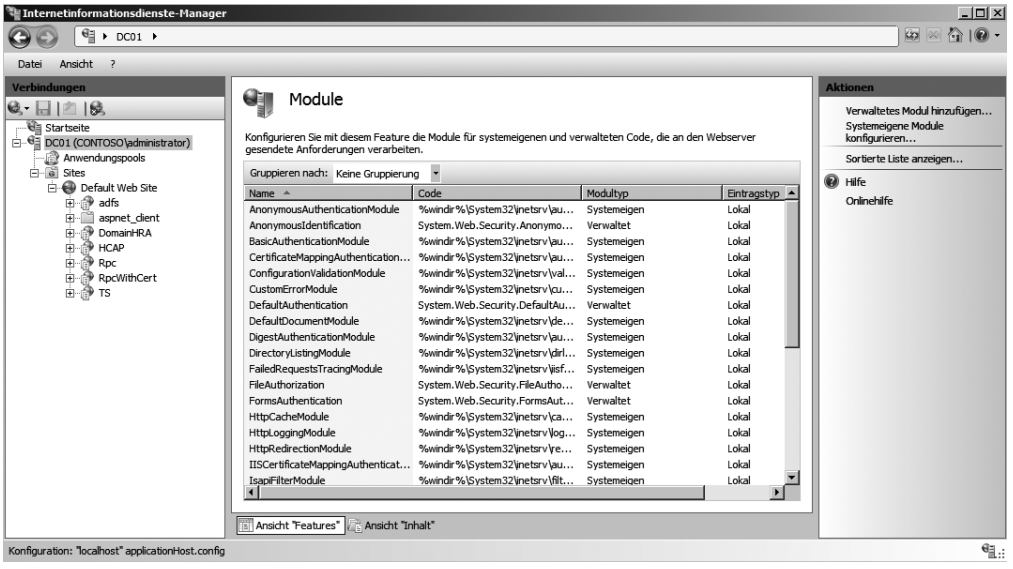
Abbildg. 13.26 Die Ereignisse, die beim Starten eines Wiederherstellungsvorgangs anfallen, können protokolliert werden



Verwalten von Modulen in IIS 7.0

IIS 7.0 unterscheidet im Betrieb zwischen systemeigenen (nativen) Modulen, die nicht von .NET-Funktionen wie ASP.NET erstellt werden und verwalteten (managed) Modulen, die durch .NET-Prozesse erstellt werden. Bei den systemeigenen Modulen handelt es sich meistens um **.dll*-Dateien, die im Webserver integriert werden müssen. Es würde den Rahmen dieses Buches sprengen, dieses Thema ausführlich zu behandeln, vor allem weil es in diesem Bereich eher um das Thema Entwicklung geht. Administratoren und Consultants sollten diese Funktion dennoch etwas verstehen, da IIS 7.0 mit Anwendungen und Webseiten basierend auf diesen beiden Modultypen umgeht. Module werden über *Module* auf der Hauptseite des Internetinformationsdienste-Managers verwaltet und konfiguriert (Abbildung 13.27).

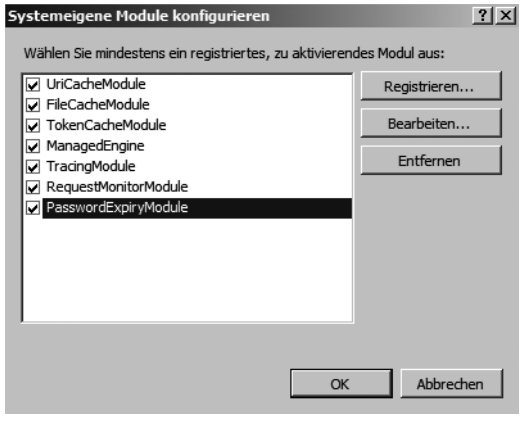
Abbildg. 13.27 Verwalten der Module in IIS 7.0



Hinzufügen und verwalten von Modulen

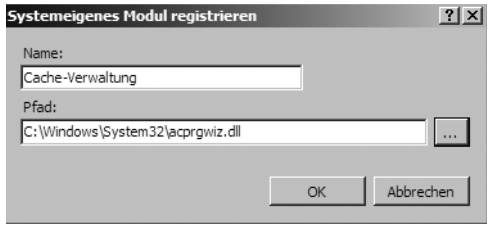
Native Module werden geladen, wenn der Arbeiterprozess (Worker Process) einer Anwendung gestartet und initialisiert wird. Native Module werden immer auf Server-Basis hinzugefügt, können für einzelne Webseiten oder Anwendungen aber deaktiviert werden. Um ein systemeigenes Modul hinzuzufügen, wählen Sie in der Module-Verwaltung aus dem Kontextmenü oder dem Aktionsbereich die Option *Verwaltetes Modul hinzufügen* oder *Systemeigene Module konfigurieren* aus. Anschließend kann das entsprechende Modul aktiviert und über die Schaltfläche *Registrieren* dem Server hinzugefügt werden (Abbildung 13.28).

Abbildg. 13.28 Hinzufügen eines systemeigenen Moduls zu IIS



Nachdem Sie auf die Schaltfläche *Registrieren* geklickt haben, können Sie einen Namen für das Modul festlegen sowie die entsprechende **.dll* für das native Modul auswählen (Abbildung 13.29).

Abbildg. 13.29 Konfigurieren eines systemeigenen Moduls



Nachdem die Daten eingegeben wurden, kann das Modul aktiviert und bearbeitet werden. Auf dem gleichen Weg kann ein Modul wieder deinstalliert werden, wenn dieses nicht mehr benötigt wird.

Delegierung der IIS-Verwaltung

Mit IIS 7.0 kann die Verwaltung von einzelnen Webseiten oder des kompletten Servers wesentlich besser delegiert und konfiguriert werden, als bei IIS 6.0. Administratoren für Webseiten oder Anwendungen müssen nicht gezwungenermaßen auch Administratoren des kompletten Servers sein. Es besteht die Möglichkeit die Verwaltung einzelner Funktionen und Webseiten an verschiedene Administratoren zu verteilen. Da die meisten IIS-Einstellungen in *Web.config*-Dateien liegen, können Berechtigungen und Einstellungen auch im Rahmen der Synchronisierung von Webseiten zwischen verschiedenen Servern kopiert werden.

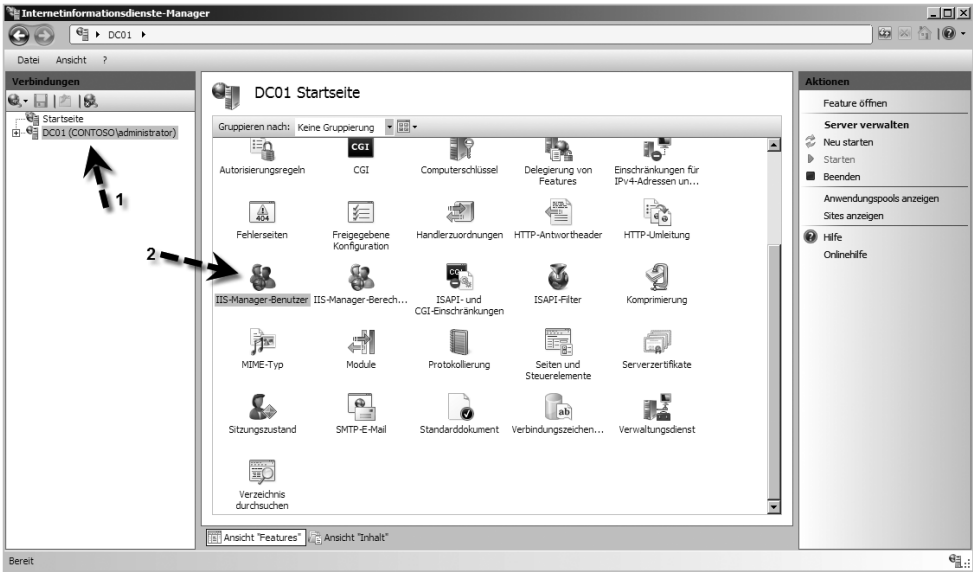
Vorgehensweise bei der Delegierung von Berechtigungen

Um Benutzern das Recht der Verwaltung für einzelne Webseiten oder Anwendungen zu erteilen, können entweder Windows-Benutzerkonten oder spezielle IIS-Konten verwendet werden. Die IIS-Konten können ausschließlich nur innerhalb des Webservers für die Delegierung von Rechten verwendet werden. Im nächsten Schritt können auf Basis der angelegten Benutzerkonten Rechte speziell für einzelne Webseiten oder Webanwendungen gewährt werden. Damit die Webadministratoren ihre Webseiten auch verwalten können, muss der Verwaltungsdienst auf dem Webserver so konfiguriert werden, dass der Zugriff gestattet wird.

Verwalten von IIS-Manager-Benutzern

Damit Benutzerkonten speziell im IIS verwaltet werden können, starten Sie den *Internetinformationsdienste-Manager* in der Programmgruppe *Verwaltung*. Sie können das Tool auch über *Start/Ausführen/inetmgr* starten. Die Benutzerverwaltung wird über den Menüpunkt *IIS-Manager-Benutzer* durchgeführt (Abbildung 13.30). Klicken Sie auf diesen Menüpunkt, werden im Fenster alle bereits angelegten Benutzer im IIS angezeigt. Über dieses Fenster können weitere Benutzer angelegt, die Kennwörter geändert oder Benutzer gelöscht werden.

Abbildg. 13.30 Starten der Benutzerverwaltung von IIS

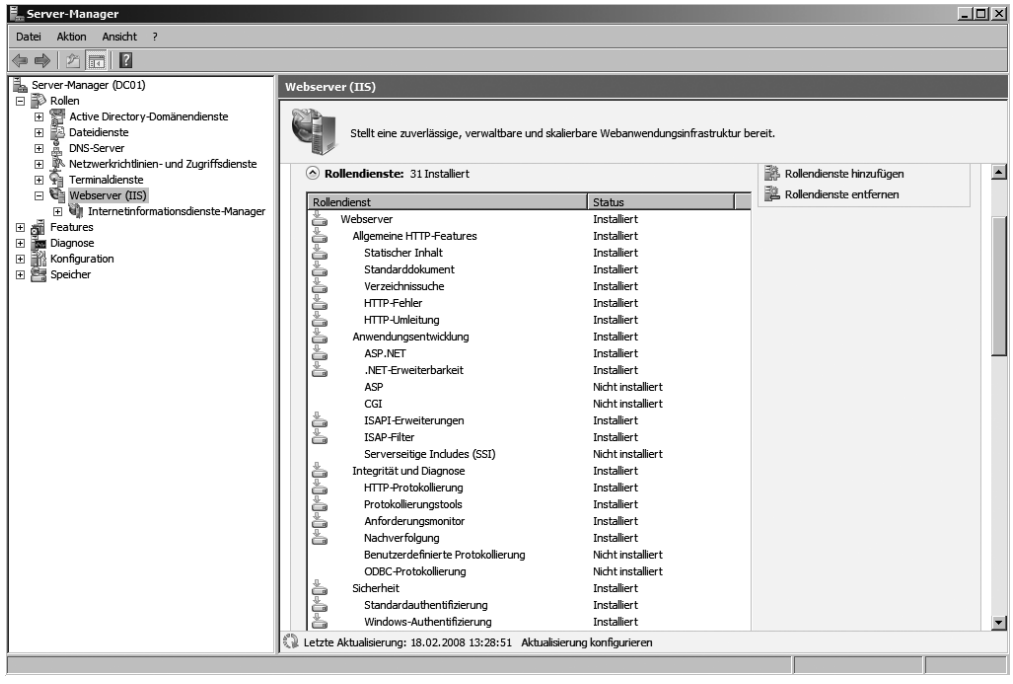


Dieses Feature wird allerdings nur dann angezeigt, wenn der Rollendienst *Verwaltungsdienst* unterhalb der *Verwaltungsprogramme* für den Webserver installiert wurde. Über das Kontextmenü eines IIS-Manager-Benutzers können verschiedene Verwaltungsaufgaben durchgeführt werden (Abbildung 13.31). So besteht zum Beispiel auch die Möglichkeit, solche Benutzer zu deaktivieren. In diesem Fall kann der Benutzer bis zu seiner Aktivierung nicht mehr auf die Verwaltungsoberfläche zugreifen, muss dafür aber auch nicht wieder neu angelegt werden, wenn dieser erneut benötigt wird.

Abbildg. 13.31 Über das Kontextmenü können die Manager-Benutzer innerhalb von IIS verwaltet werden

HINWEIS Die installierten Rollendienste des Webservers werden angezeigt, wenn Sie im Server-Manager auf *Webserver* klicken. Die installierten Rollendienste werden im Bereich *Rollendienste* angezeigt (Abbildung 13.32). Über *Rollendienste hinzufügen*, beziehungsweise *Rollendienste entfernen*, werden diese Funktionen dem Server hinzugefügt oder entfernt. Von den installierten Rollendiensten hängen auch die angezeigten Verwaltungsmöglichkeiten von IIS ab. Sollen lokale IIS-Konten verwaltet werden, benötigen Sie den Rollendienst *Verwaltungsdienst*.

Abbildg. 13.32 Die installierten Rollendienste von IIS werden über den Server-Manager verwaltet

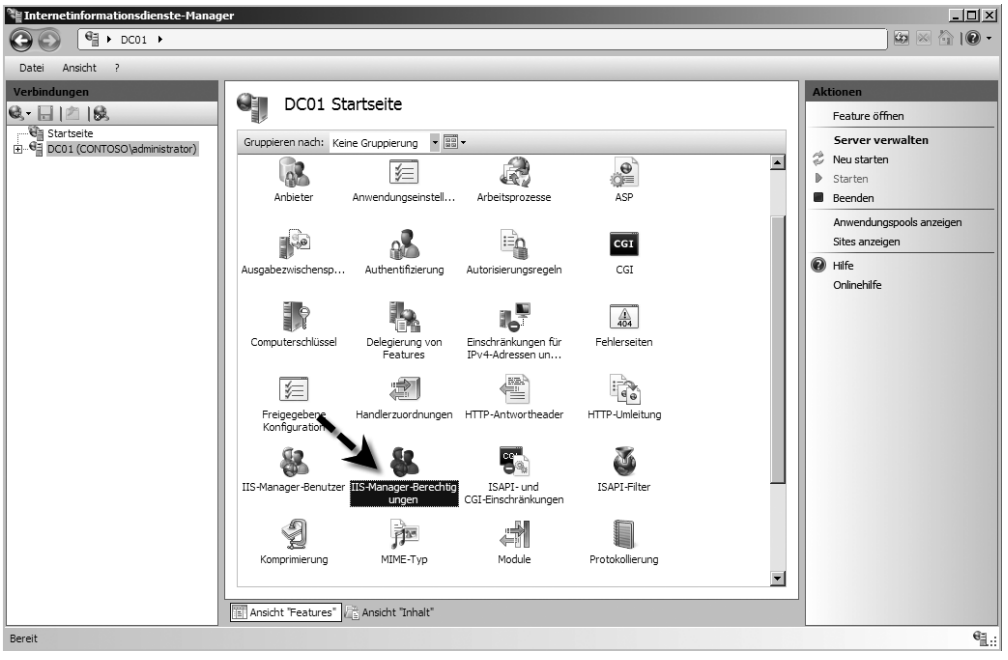


Berechtigungen der IIS-Manager-Benutzer verwalten

Nachdem die Benutzerkonten im IIS für die Delegierung angelegt wurden, können die Rechte für diese Benutzer über den Menüpunkt *IIS-Manager-Berechtigungen* verwaltet werden (Abbildung 13.33).

Dazu verwenden Sie aber nicht das Symbol in der Serverkonfiguration, sondern klicken auf die Webseite, für die Sie den IIS-Manager delegieren wollen und wählen den Menüpunkt aus. Anschließend klicken Sie auf Benutzer zulassen (Abbildung 13.34). Es öffnet sich ein neues Fenster, über das Sie auswählen können, welche Benutzer zugelassen werden.

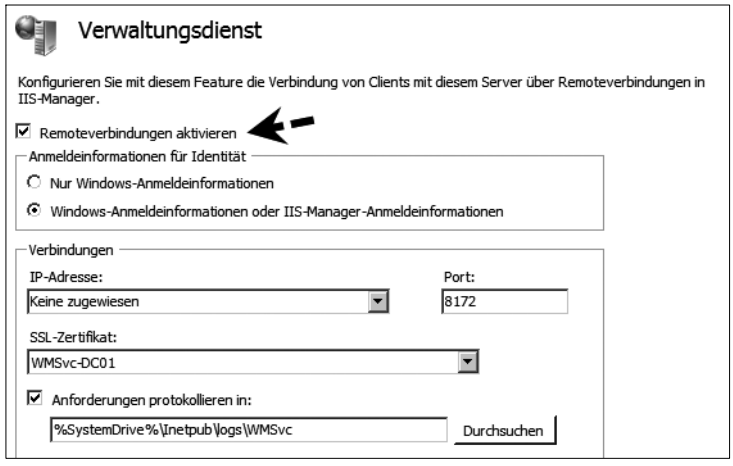
Abbildg. 13.33 Verwalten der Berechtigungen für IIS-Manager-Benutzer



Abbildg. 13.34 Benutzer als Administratoren für eine bestimmte Webseite festlegen

HINWEIS Standardmäßig ist die Möglichkeit, IIS-Manager für eine Webseite zu delegieren, deaktiviert, da der Server nur Windows-Benutzerkonten zulässt. Damit auch die angelegten IIS-Manager-Benutzer verwendet werden können, muss auf Serverebene über das Feature *Verwaltungsdienst* die Option *Windows-Anmeldeinformationen oder IIS-Manager-Anmeldeinformationen* aktiviert und bestätigt sein. Der Dienst muss anschließend gestartet werden (Abbildung 13.35). Erst dann kann in den IIS-Manager-Berechtigungen auch ein IIS-Manager ausgewählt werden.

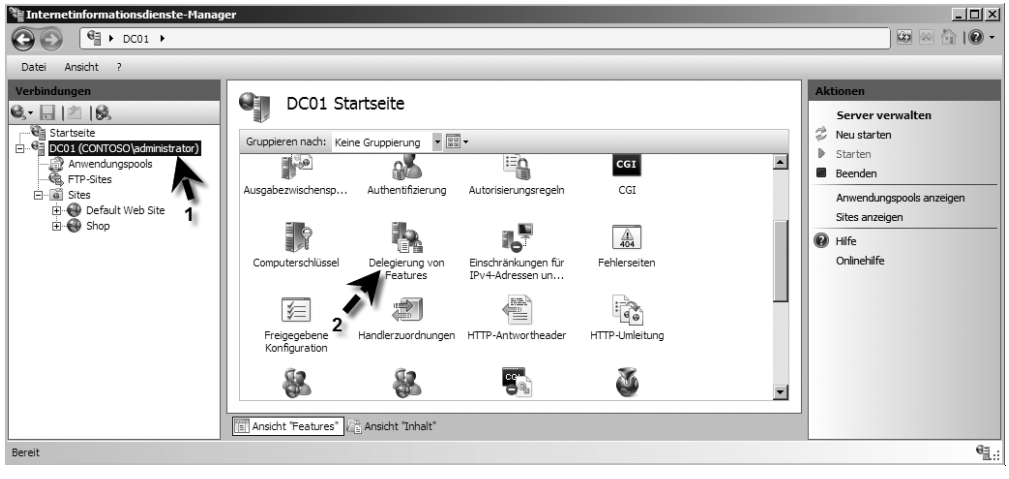
Abbildg. 13.35 Aktivieren der IIS-Manager-Anmeldeinformationen für einen Webserver



Verwalten der Delegierung

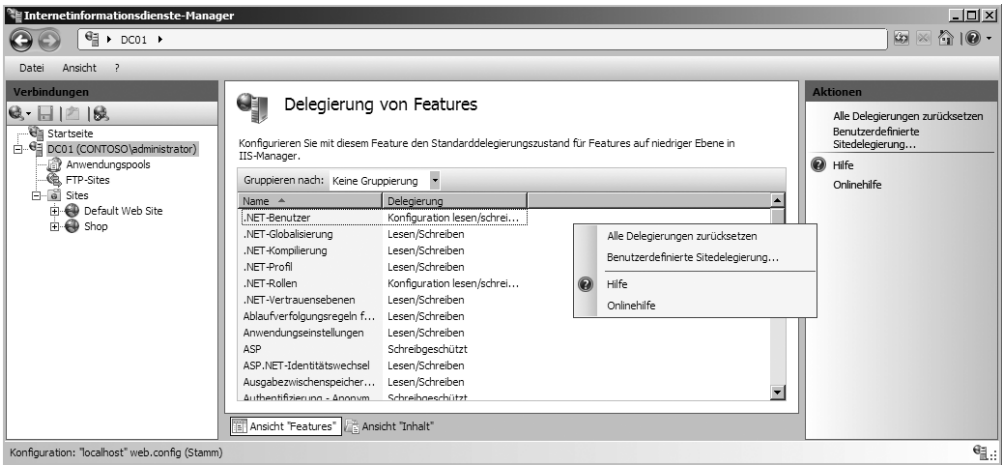
Nachdem den entsprechenden IIS-Manager-Benutzern und/oder Windows-Benutzern das Recht zur Anmeldung für spezielle Webseiten gewährt wurde, kann generell festgelegt werden, welche Rechte überhaupt für Webseiten auf dem Server delegiert werden können. Da die Delegations-Einstellungen automatisch nach unten vererbt werden, lässt sich gezielt einstellen, welche Rechte auf welcher Ebene und Webseite die einzelnen Manager-Benutzer erhalten sollen. Diese Einstellungen finden entweder in oberster Ebene über den Server statt, oder indem Sie auf eine übergeordnete Website im Internetinformationsdienste-Manager klicken (Abbildung 13.36). Die Verwaltung der Delegation findet dann über das Feature *Delegierung von Features* statt.

Abbildg. 13.36 Festlegen der Delegierung der einzelnen Funktionen



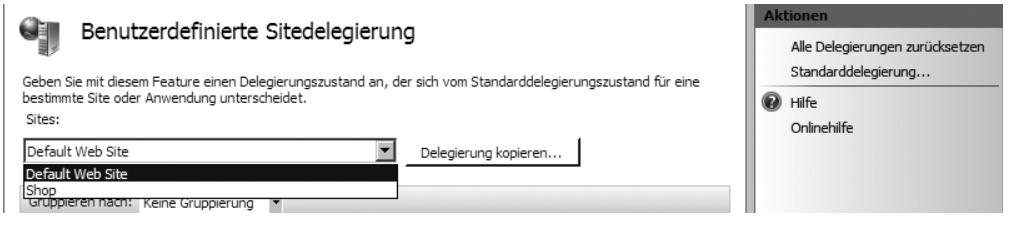
In diesem Bereich kann jetzt sehr detailliert festgelegt werden, welche Rechte die einzelnen Manager-Benutzer erhalten sollen (Abbildung 13.37). Über das Kontextmenü oder den *Aktionen*-Bereich der Konsole können bereits gesetzte Delegierungen wieder zurückgesetzt oder benutzerdefinierte Delegierungen konfiguriert werden.

Abbildg. 13.37 Festlegen der einzelnen Delegierungsfeatures für den Server oder einzelne Webseiten



Durch die benutzerdefinierte Delegierung können Aufgaben speziell für einzelne untergeordnete Sites festgelegt werden. Auch hier werden die Rechte wieder an die untergeordneten Webseiten vererbt. Die benutzerdefinierten Delegationen können aber ebenfalls jederzeit entweder wieder auf den Standard oder auf Vererbung von oben zurückgesetzt werden.

Abbildg. 13.38 Auswählen einer Webseite für eine benutzerdefinierte Siteregelung

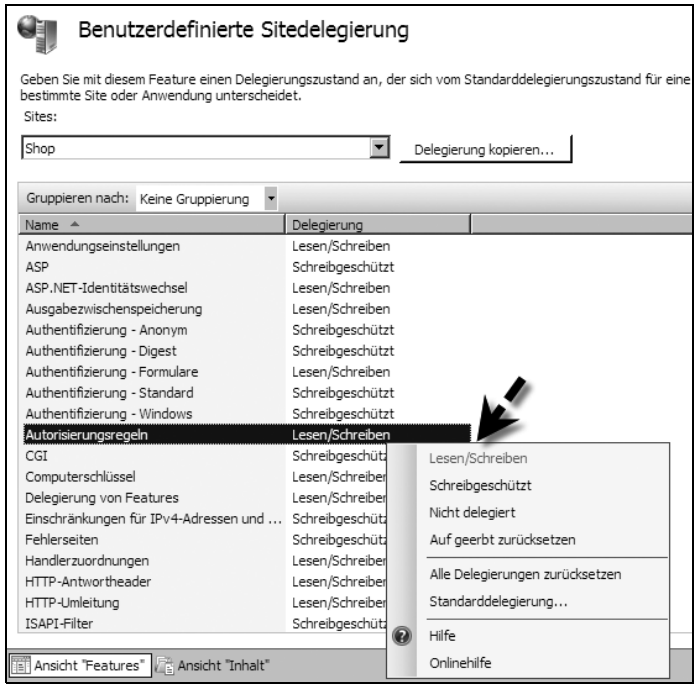


Festlegen der Rechte zur Delegierung

Für die einzelnen Features, die delegiert werden können, besteht die Möglichkeit, unterschiedliche Rechte festzulegen (Abbildung 13.39).

- **Lesen/Schreiben** Bei diesem Recht darf das entsprechende Feature angezeigt und angepasst werden.
- **Schreibgeschützt** Wird für ein Feature diese Option ausgewählt, kann der IIS-Manager, der sich an der Seite anmelden darf, die entsprechenden Einstellungen in der IIS-Verwaltung zwar anzeigen, aber nicht bearbeiten.

Abbildg. 13.39 Festlegen der Rechte für einzelne Features



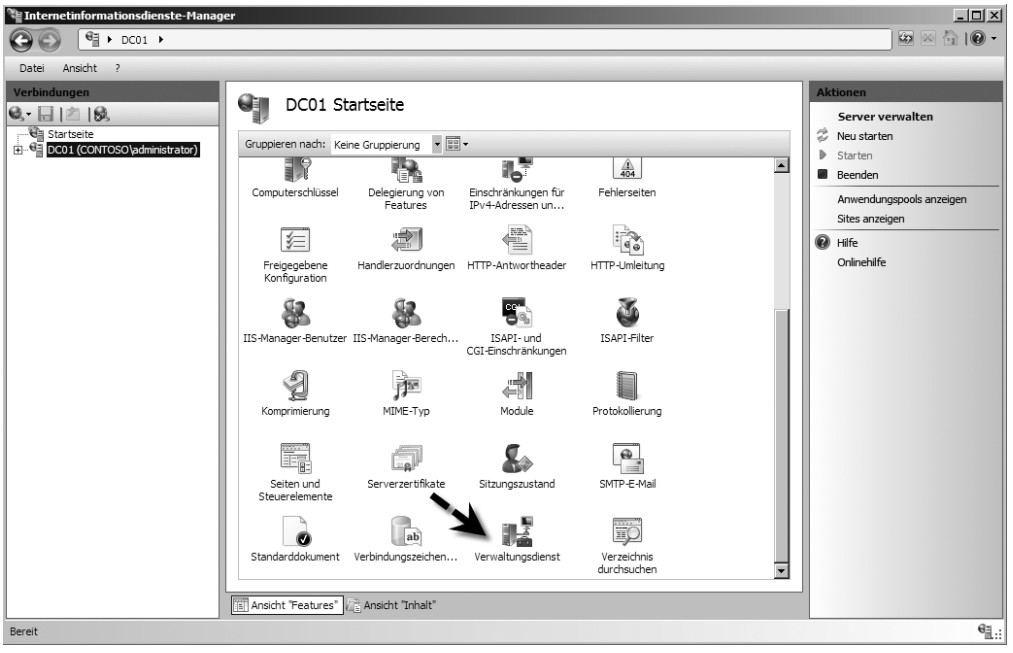
- **Nicht delegiert** Bei diesem Recht wird das entsprechende Feature in der IIS-Verwaltung nicht angezeigt. So können die Administratoren der Webseite die Einstellung der jeweiligen Funktion nicht mal lesen.
- **Auf geerbt zurücksetzen** Durch das Aktivieren diese Option wird die benutzerdefinierte Einstellung des jeweiligen Features wieder auf den Standard zurückgestellt und das Recht wird vom jeweils übergeordneten Objekt vererbt. Das übergeordnete Objekt kann jeweils der Server oder eine Webseite sein.
- **Alle Delegierungen zurücksetzen** Durch diese Option werden alle benutzerspezifischen Einstellungen der Features wieder auf den Standard zurückgesetzt.

Aktivieren der Remoteverwaltung

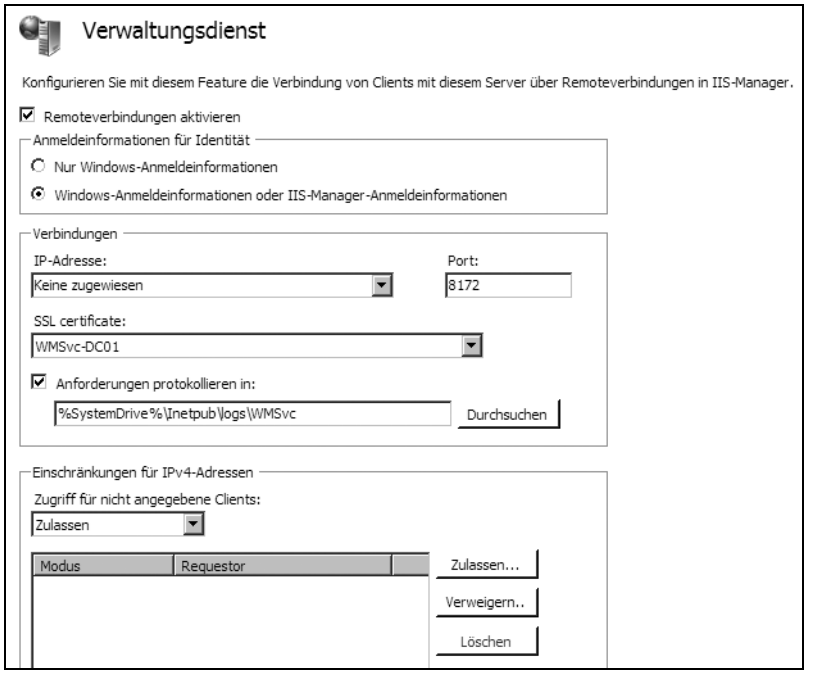
Damit die Delegationen verwendet werden können, muss auf einem Server die Remoteverwaltung konfiguriert und aktiviert werden. Diese Option findet auf Serverebene über den Menüpunkt *Verwaltungsdienst* statt (Abbildung 13.40).

Damit die Einstellungen angepasst werden können, muss ein gestarteter Verwaltungsdienst zunächst beendet werden. Erst dann können Einstellungen vorgenommen werden. Neben der allgemeinen Aktivierung und der Möglichkeit, neben Windows-Benutzern auch IIS-Manager-Benutzer zu berechtigen, können in diesem Bereich der Konsole weitere Einstellungen zur Remoteverwaltung eines Servers vorgenommen werden (Abbildung 13.41).

Abbildg. 13.40 Konfigurieren des Verwaltungsdienstes auf einem Webserver



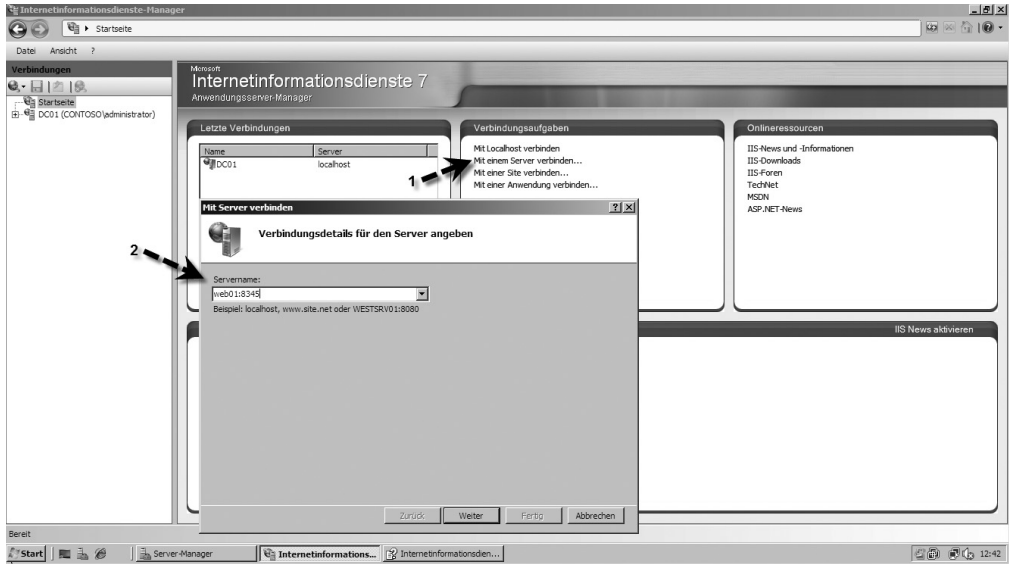
Abbildg. 13.41 Konfigurieren des Verwaltungsdienstes für einen Webserver



- Über das Listenfeld *IP-Adresse* wird die Netzwerkschnittstelle festgelegt, mit der sich Administratoren über das Netzwerk verbinden können. Dadurch besteht die Möglichkeit, in größeren Serverfarmen spezielle Netzwerkverbindungen nur für die Verwaltung zu definieren.
- Im Feld *Port* wird der Standard-Port festgelegt, über den sich die Benutzer verbinden.

HINWEIS Der Verwaltungsdienst verwendet für die Remoteverbindung von Clients standardmäßig den Port 8172. Ändern Sie den Port ab, muss im Internetinformationsdienste-Manager des Clients ebenfalls der neue Port beim Verbindungsaufbau festgelegt werden. Dazu wird dieser mit einem Doppelpunkt nach dem Servernamen angegeben (Abbildung 13.42)

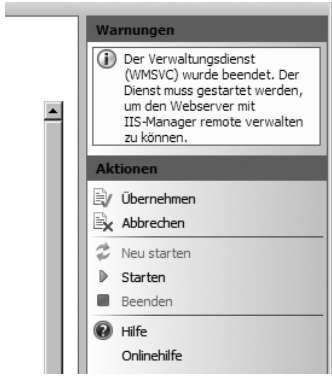
Abbildg. 13.42 Verbindungsaufbau zu einem Server über einen angepassten Port



- Über *SSL-Zertifikat* legen Sie fest, welches SSL-Zertifikat für die Verbindung verwendet werden soll. Hier werden die Zertifikate angezeigt, die als Serverzertifikat dem Server zugewiesen wurden. Über die SSL-Verbindung wird der Datenverkehr zwischen Client und Server verschlüsselt.
- Im Verzeichnis unterhalb des Kontrollkästchens *Anforderungen protokollieren in* werden die Protokolldateien festgelegt, in denen die Verbindungen der Administratoren über das Netzwerk festgehalten werden.
- Über den Bereich *Einschränkungen für IPv4-Adresse* können Sie entweder eine Liste pflegen, welchen Clients der Zugriff gestattet wird, oder eine Liste führen, welchen Clients der Zugriff generell untersagt wird. Hier wird auch festgelegt, ob nicht angegebenen Clients der Zugriff generell erlaubt wird (Standardeinstellung) oder nicht.

Auf der rechten Seite der Konsole werden die Einstellungen schließlich bestätigt und der Verwaltungsdienst gestartet oder beendet (Abbildung 13.43). Änderungen können nur vorgenommen werden, wenn der Dienst beendet wurde.

Abbildg. 13.43 Übernehmen der Änderungen und starten oder beenden des Verwaltungsdienstes



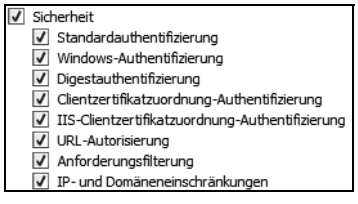
Sicherheit in IIS 7.0 konfigurieren

In diesem Abschnitt beschäftigen wir uns maßgeblich mit der Sicherheit und der Authentifizierung in IIS 7.0. Da sich vor allem in diesem Bereich einiges geändert hat, sollten Sie sich mit den Sicherheits- und Authentifizierungsoptionen gründlich auseinandersetzen.

Authentifizierung in IIS 7.0

Die Konfiguration der Authentifizierung ist eine der wichtigsten Konfigurationsmaßnahmen auf einem Webserver. In diesem Bereich hat sich im Vergleich zu IIS 6.0 von Windows Server 2003 einiges geändert, vor allem die einzelnen Stellschrauben, um die Authentifizierung zu konfigurieren. Bei Windows Server 2008 können die verschiedenen Authentifizierungsoptionen nachträglich installiert oder einzeln deinstalliert werden. Auf dem Server stehen nur die Authentifizierungsoptionen zur Verfügung, die auch bei der Installation als Rollendienst ausgewählt wurden. Über den Server-Manager können einzelne Rollendienste und auch Authentifizierungsoptionen deinstalliert werden (Abbildung 13.44).

Abbildg. 13.44 Die einzelnen Authentifizierungsoptionen und Sicherheitsfunktionen in IIS 7.0 können modular installiert und deinstalliert werden

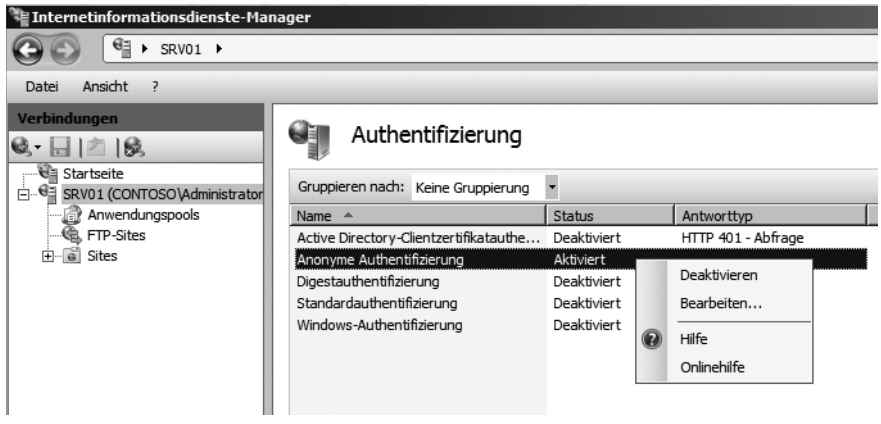


Konfiguration der anonymen Authentifizierung

Häufig wird auf Webservern ein Zugriff benötigt, bei dem keinerlei Authentifizierung stattfindet. In IIS 7.0 ist diese anonyme Authentifizierung standardmäßig bereits aktiviert. Soll daher den Anwendern der Zugriff auf einige Verzeichnisse verwehrt werden, können Sie mit NTFS-Berechtigungen

den Zugriff entziehen. Soll für eine Webseite immer eine Authentifizierung stattfinden, muss der anonyme Zugriff zunächst deaktiviert und eine Authentifizierungsvariante ausgewählt werden. Dabei stehen in IIS 7.0 einige Möglichkeiten zur Verfügung. Bei der Standardauthentifizierung erscheint ein Anmeldefenster und Anwender müssen sich mit Benutzernamen und Kennwort authentifizieren. Die Daten werden dabei in Klartext übertragen, können also durch spezielle Programme wie dem Netzwerk-Monitor angezeigt werden. Um die anonyme Authentifizierung generell auf dem Server zu aktivieren oder zu deaktivieren, öffnen Sie den Internetinformationsdienste-Manager und doppelklicken auf das Feature *Authentifizierung*. Über das Kontextmenü der Option *Anonyme Authentifizierung* aktivieren oder deaktivieren Sie diese (Abbildung 13.45).

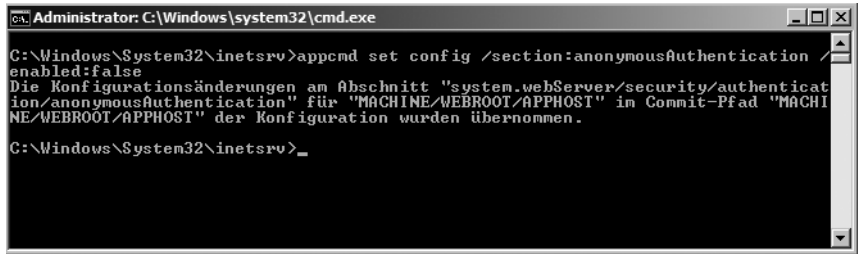
Abbildg. 13.45 Die anonyme Authentifizierung kann über den Internetinformationsdienste-Manager für den kompletten Server gesteuert werden



An dieser Stelle aktivieren oder deaktivieren Sie auch die anderen Authentifizierungs-Optionen, die auf dem Server verfügbar sein sollen.

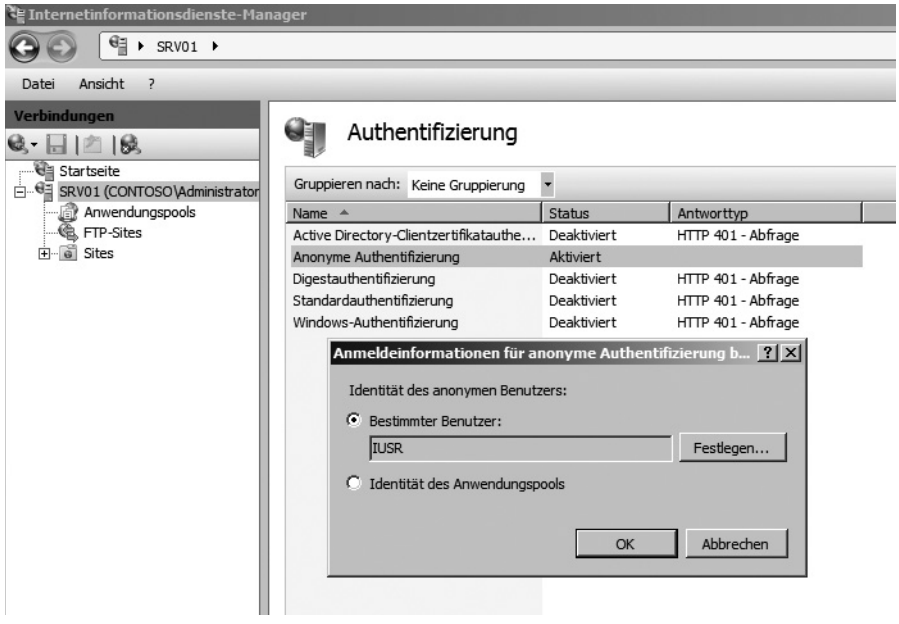
Über die Befehlszeile deaktivieren Sie die anonyme Authentifizierung mit dem Befehl *appcmd set config /section:anonymousAuthentication /enabled:false*. Mit dem Befehl *appcmd set config /section:anonymousAuthentication /enabled:true* wird die anonyme Authentifizierung wieder aktiviert. Achten Sie darauf, dass das Verzeichnis *C:\Windows\System32\Inetsrv*, in dem sich das Befehlszeilen-Tool *appcmd.exe* von IIS 7.0 befindet, nicht im Standard-Pfad des Servers enthalten ist. Sie müssen daher entweder den Pfad hinzufügen oder in der Befehlszeile zunächst in das Verzeichnis wechseln. Die erfolgreiche Aktivierung oder Deaktivierung wird in der Befehlszeile gemeldet und im IIS-Manager auch angezeigt.

Abbildg. 13.46 Die anonyme Authentifizierung kann auch in der Befehlszeile deaktiviert werden



Ist die anonyme Authentifizierung aktiviert, verwendet IIS das Benutzerkonto *IUSR_<Servername>*, das bei der Installation von IIS angelegt wird, für den anonymen Zugriff. Über das Kontextmenü der anonymen Authentifizierung kann neben der Deaktivierung auch die Bearbeitung der Funktion durchgeführt werden. In diesem Fall wird das Konto und das Kennwort, das für den anonymen Zugriff verwendet wird, konfiguriert. Dabei kann entweder ein spezielles Benutzerkonto ausgewählt werden oder es wird das Benutzerkonto verwendet, mit dem der Anwendungspool gestartet wird, in welcher die Anwendung, die den anonymen Zugriff verwendet, gespeichert ist (Abbildung 13.47).

Abbildg. 13.47 Die Identität des Benutzers für den anonymen Zugriff kann im IIS-Manager angepasst werden



Achten Sie aber darauf, dass Anwendungspools standardmäßig mit dem Benutzerkonto *Netzwerkdienst* gestartet werden. Das Konto kann in den erweiterten Einstellungen des Anwendungspools konfiguriert werden.

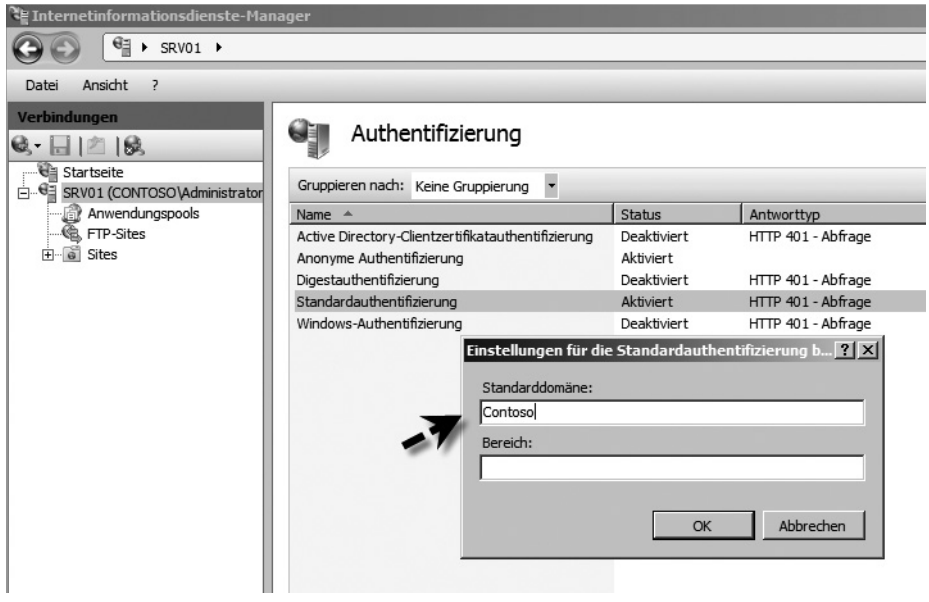
Auch diese Einstellungen können in der Befehlszeile durchgeführt werden. Dazu wird der Befehl *appcmd set config /section:anonymousAuthentication /userName:<Name> /password:<Kennwort>* verwendet.

Konfiguration der Standardauthentifizierung

Bei der Standardauthentifizierung müssen sich Anwender über ein Windows-typisches Fenster zuerst am Server authentifizieren, dabei wird allerdings Benutzername und Kennwort in Klartext übertragen. Die Standardauthentifizierung macht daher nur für Webseiten Sinn, bei denen SSL aktiviert ist. Hier wird der komplette Datenverkehr, auch die Standardauthentifizierung verschlüsselt. Die Standardauthentifizierung ist standardmäßig nach der Installation deaktiviert. Um diese zu aktivieren oder zu deaktivieren, rufen Sie im Internetinformationsdienste-Manager den Punkt *Authentifizierung* auf. Über das Kontextmenü der Option *Standardauthentifizierung* kann diese akti-

viert oder deaktiviert werden. Über Bearbeiten legen Sie zum Beispiel die Standarddomäne fest. Gibt ein Besucher einen Benutzer ein, wird das Konto erst in der hier angegebenen Domäne gesucht (Abbildung 13.48).

Abbildg. 13.48 Konfigurieren und aktivieren der Standardauthentifizierung in IIS 7.0



Über die Befehlszeile deaktivieren Sie die Standardauthentifizierung mit dem Befehl *appcmd set config /section:basicAuthentication /enabled:false*. Mit dem Befehl *appcmd set config /section:basicAuthentication /enabled:true* wird die Standardauthentifizierung aktiviert. Achten Sie darauf, dass das Verzeichnis *C:\Windows\System32\Inetsrv*, in dem sich das Befehlszeilen-Tool *appcmd.exe* von IIS 7.0 befindet, nicht im Standard-Pfad des Servers enthalten ist. Sie müssen daher entweder den Pfad hinzufügen oder in der Befehlszeile zunächst in das Verzeichnis wechseln. Die erfolgreiche Aktivierung oder Deaktivierung wird in der Befehlszeile gemeldet und im IIS-Manager auch angezeigt.

Konfiguration der Windows-Authentifizierung

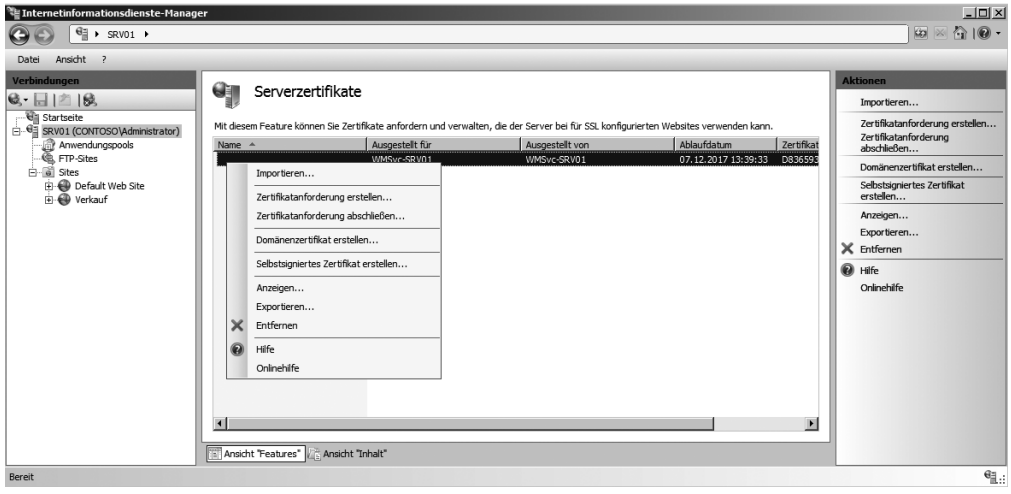
Auch die Windows-Authentifizierung kann getrennt installiert werden und ist wie die Standardinstallation zunächst deaktiviert. Im Internetinformationsdienste-Manager über den Punkt *Authentifizierung* kann auch diese Authentifizierungsmethode konfiguriert werden. Über das Kontextmenü der Option *Windows-Authentifizierung* kann diese aktiviert oder deaktiviert werden.

Über die Befehlszeile deaktivieren Sie die Windows-Authentifizierung mit dem Befehl *appcmd set config /section:windowsAuthentication /enabled:false*. Mit dem Befehl *appcmd set config /section:windowscAuthentication /enabled:true* wird die Windows-Authentifizierung aktiviert.

Serverzertifikate verwalten

Für die Verwendung von SSL und auch für die sichere Authentifizierung werden Serverzertifikate eingesetzt. IIS 7.0 bietet nach der Installation bereits standardmäßig ein selbstsigniertes Zertifikat an. Es ist allerdings sicherer und auch professioneller, entweder ein Zertifikat im Internet zu erwerben oder eine eigene Zertifizierungsstelle zum Beispiel mit Windows Server 2008 zu verwenden. Die Serverzertifikate werden über das Feature *Serverzertifikate* im Internetinformationsdienste-Manager verwaltet. Hier werden alle ausgestellten Zertifikate angezeigt. Außerdem können neue Zertifikate ausgestellt werden.

Abbildg. 13.49 Verwalten der Serverzertifikate in IIS 7.0



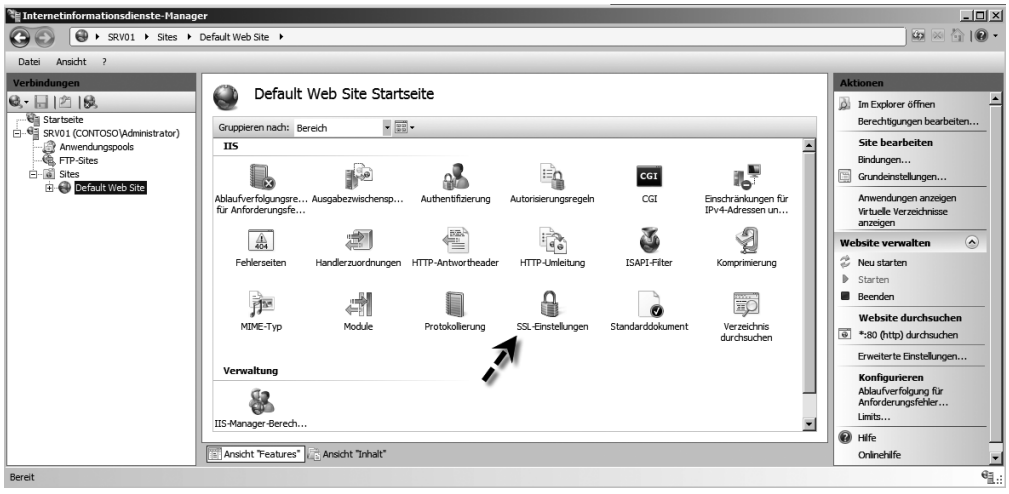
Über das Kontextmenü oder den Aktionsbereich können bereits hinterlegte Zertifikate exportiert, neue importiert oder neue Anforderungen erstellt werden. Hier kann auch ein selbstsigniertes Zertifikat ausgestellt werden, um die Installation einer eigenen Zertifizierungsstelle zu vermeiden. Per Doppelklick auf ein Zertifikat werden die Informationen sowie die Zertifizierungsstelle und die Gültigkeit des Zertifikats angezeigt.

Secure Sockets Layer (SSL) konfigurieren

Um Internetseiten sicher zur Verfügung zu stellen, ist die SSL-Verschlüsselung der einfachste und gebräuchlichste Weg. SSL kann für einzelne Webseiten, Anwendungen, Verzeichnisse und URLs konfiguriert werden. Die Konfiguration von SSL wird im Internetinformationsdienste-Manager über das Feature *SSL-Einstellungen* vorgenommen (Abbildung 13.50).

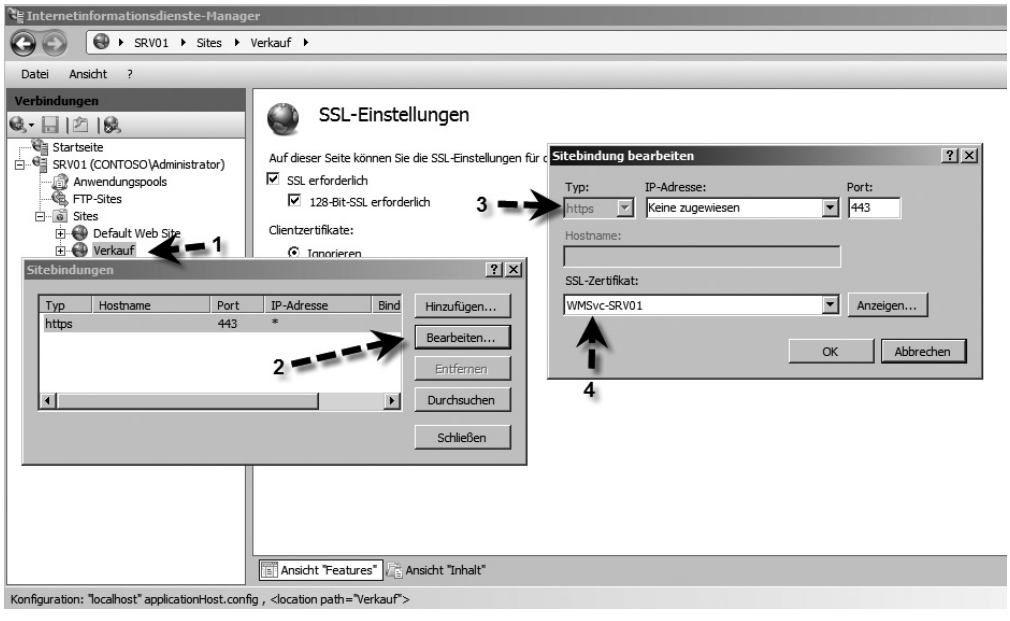
HINWEIS In IIS 7.0 können SSL-Einstellungen nicht auf Serverebene durchgeführt werden. Damit das Feature *SSL-Einstellungen* angezeigt wird, muss daher zunächst eine Webseite wie beispielsweise die Standardwebseite markiert werden.

Abbildg. 13.50 SSL-Einstellungen werden am besten auf Ebene der Webseiten durchgeführt



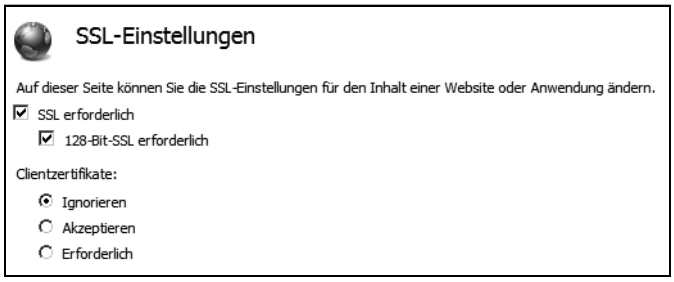
In den SSL-Einstellungen kann die Verwendung von SSL vorgeschrieben werden, sowie eine 128-Bit-Verschlüsselung aktiviert werden. Allerdings stehen diese Optionen nur dann zur Verfügung, wenn für eine Webseite eine HTTPS-Bindung konfiguriert und ein Zertifikat zugewiesen wurde (Abbildung 13.51).

Abbildg. 13.51 Für Webseiten können HTTPS-Bindungen und Zertifikate zugewiesen werden



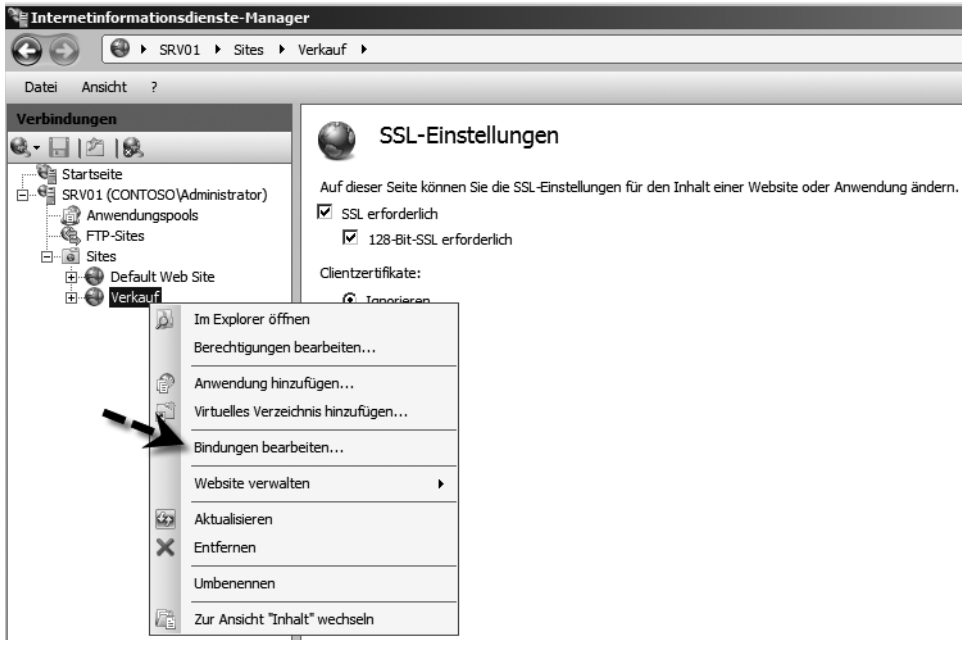
Bei HTTPS-aktivierten Webseiten kann über die SSL-Einstellungen die Konfiguration aktiviert und eingestellt werden (Abbildung 13.52).

Abbildg. 13.52 Die SSL-Einstellungen werden für einzelne Webseiten im Internetinformationsdienste-Manager vorgenommen



Bereits bei der Erstellung von Webseite kann eine HTTPS-Verbindung vorgegeben und ein Zertifikat hinterlegt werden. Diese Einstellungen lassen sich aber auch über den Befehl *Bindungen bearbeiten* im Kontextmenü auch nachträglich vornehmen (Abbildung 13.53).

Abbildg. 13.53 Die Bindungen von Webseiten lassen sich auch nachträglich bearbeiten

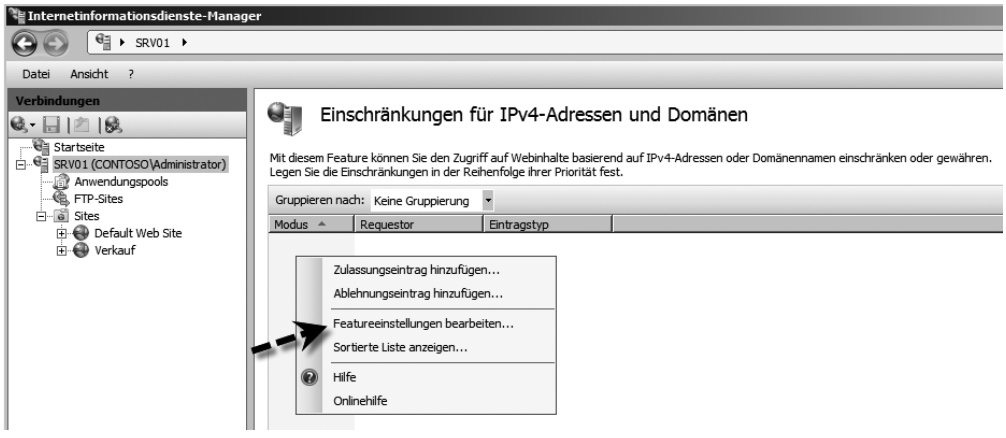


Einschränkungen für IPv4-Adressen und Domänen

Über das Feature *Einschränkungen für IPv4-Adressen und Domänen* gelangen Sie zur Steuerung der Zugriffsregeln für den Webserver. Über das Kontextmenü oder das Aktionsmenü können bestimmte Zulassungs- oder Verweigerungsregeln für einzelne IP-Adressen oder komplette Bereiche erstellt werden. Regeln für IPv4-Adressen können einfach erstellt werden. Damit aber auch Domänen ausgeschlossen werden können, muss die DNS-Infrastruktur im Unternehmen Reverse-DNS unterstützen, damit im Internet die IP-Adressen der zugreifenden Clients zu einer Domäne aufgelöst werden

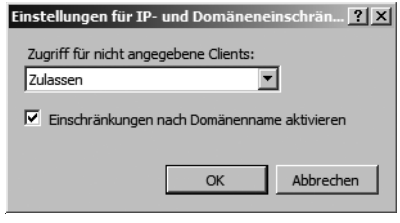
können. Die Einschränkungen für Domänenfilterung müssen darüber hinaus zunächst aktiviert werden. Klicken Sie dazu im Bereich *Einschränkungen für IPv4-Adressen und Domänen* mit der rechten Maustaste und wählen Sie die Option *Featureeinstellungen bearbeiten* aus (Abbildung 13.54).

Abbildg. 13.54 Die Einstellungen der Einschränkungen für IPv4-Adressen und Domänen müssen erst konfiguriert werden



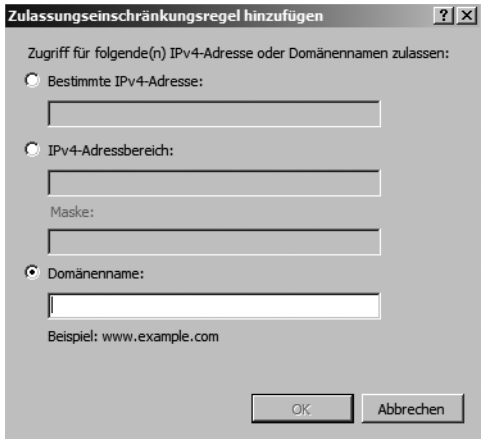
Anschließend öffnet sich ein neues Fenster. Hier legen Sie zunächst fest, was mit Clients passieren soll, für die keine Regeln hinterlegt wurden. Standardmäßig dürfen alle Clients zugreifen, außer die, für die Sie Ablehnungseinträge konfigurieren. Aktivieren Sie an dieser Stelle aber die Option *Verweigern*, dürfen nur die Clients Verbindung zu diesem Webserver aufbauen, für die Sie einen Zulassungseintrag konfiguriert haben.

Abbildg. 13.55 Konfigurieren der Standardeinstellungen für die Einschränkung von IPv4-Adressen oder Domänen



Schalten Sie das Kontrollkästchen *Einschränkungen nach Domänenname aktivieren* ein, können auch Zulassungs- beziehungsweise Ablehnungseinträge konfiguriert werden, die als Basis einen bestimmten Domänennamen haben. Nach Aktivierung erhalten Sie noch eine Warnung, dass Reverse-DNS-Einträge den Server belasten. Das ist allerdings auch abhängig von den Zugriffen.

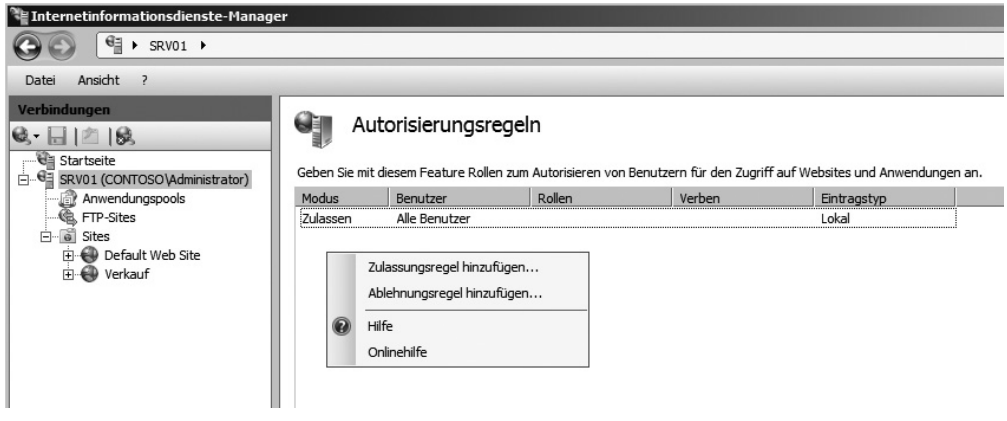
Abbildg. 13.56 Erstellen einer Zulassungs- oder Ablehnungsregel



Konfigurieren und verwalten von Autorisierungsregeln

Autorisierungsregeln steuern, welche Benutzer auf den Server zugreifen dürfen. Die Regeln werden im Internetinformationsdienste-Manager über das Feature *Autorisierungsregeln* verwaltet. Über das Kontextmenü oder den Aktionsbereich können neue Regeln erstellt und vorhandene bearbeitet werden (Abbildung 13.57). Standardmäßig dürfen zunächst alle Besucher auf einen Server zugreifen.

Abbildg. 13.57 Verwalten der Autorisierungsregeln in IIS 7.0



Beim Erstellen von Zulassungs- oder Ablehnungsregeln können verschiedene Einstellungen vorgenommen werden:

- **Alle Benutzer** Wird diese Option aktiviert, gilt die Regel sowohl für anonyme als auch für authentifizierte Benutzer
- **Alle anonymen Benutzer** Bei Aktivierung dieser Option sind nur die anonymen, also nicht authentifizierten Benutzer betroffen

- **Bestimmte Rollen oder Benutzergruppen** Durch Aktivierung dieser Option können bestimmte Serverrollen oder Benutzergruppen ausgewählt werden, für welche die Regel gilt
- **Bestimmte Benutzer** Hier werden speziell einzelne Benutzer angegeben, für welche die Regel gilt
- **Diese Regel auf bestimmte Verben anwenden** Hierüber können Regeln speziell für einzelne Befehle im Zugriff konfiguriert werden

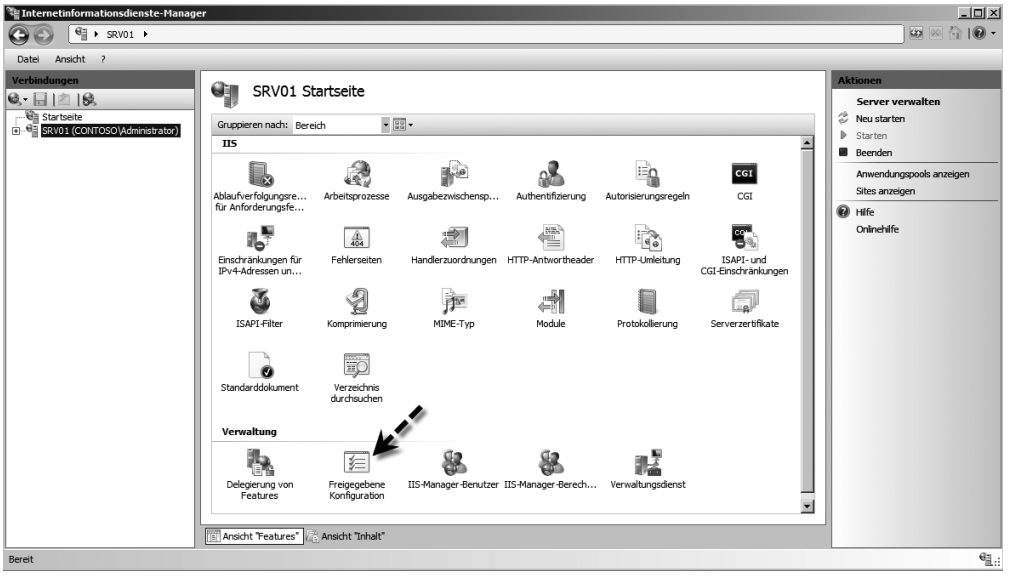
Abbildg. 13.58 Konfigurieren von Regeln für den Webserverzugriff

HINWEIS Regeln können nachträglich bearbeitet werden. Eine Zulassungsregel kann aber nicht in eine Ablehnungsregel umkonfiguriert werden. Dies gilt auch umgekehrt.

Freigegebene Konfiguration

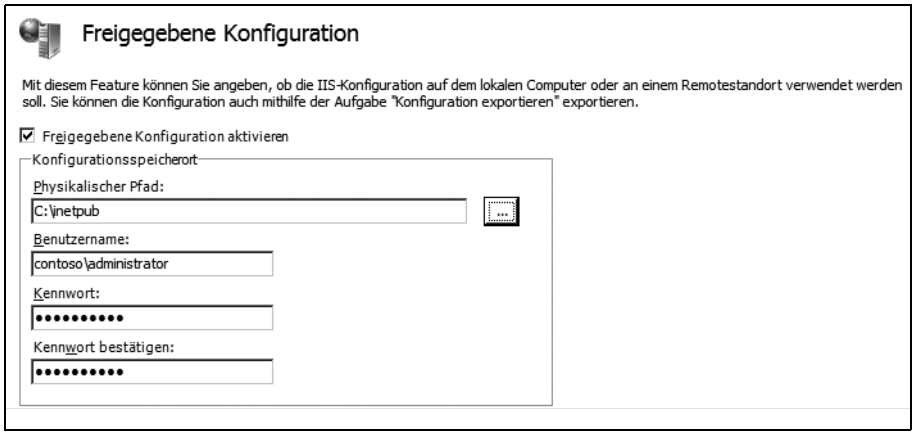
Mit IIS 7.0 ist es möglich, die Konfiguration des Webservers an einer zentralen Stelle im Netzwerk freizugeben, sodass mehrere Webserver von einer zentralen Stelle aus verwaltet werden können. Die Konfiguration dieser Funktion erfolgt im Internetinformationsdienste-Manager im Abschnitt *Verwaltung* über das Feature *Freigegebene Konfiguration* (Abbildung 13.59).

Abbildg. 13.59 In IIS 7.0 kann eine Konfiguration für mehrere Webserver konfiguriert werden



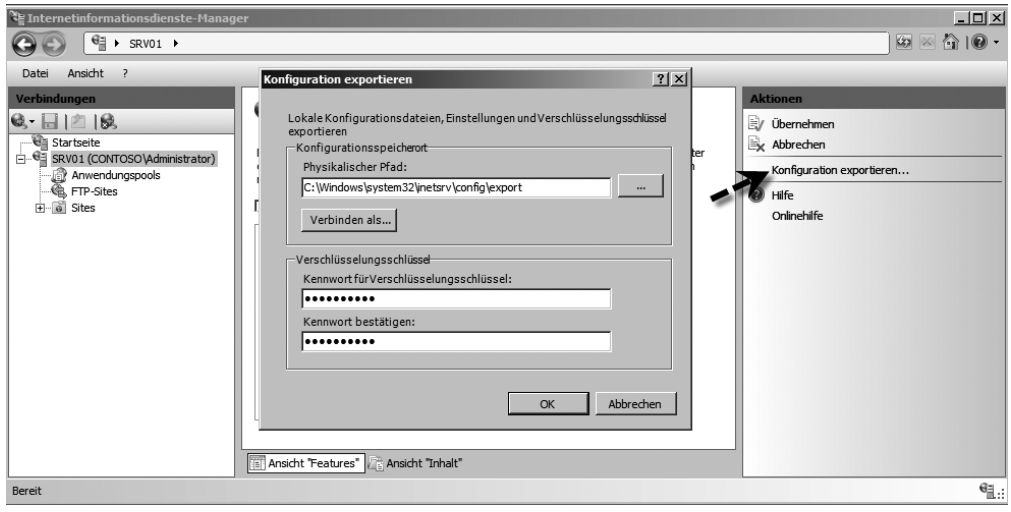
Im angegebenen Verzeichnis müssen sich alle Konfigurationsdateien von IIS befinden. Erst dann lässt sich die Konfiguration durchführen.

Abbildg. 13.60 Festlegen des Speicherplatzes für eine gemeinsame Konfiguration



Aus diesem Grund bietet es sich vor der Konfiguration der freigegebenen Konfiguration an, zunächst Einstellungen auf einem Webserver vorzunehmen und dann über den Link *Konfiguration exportieren* in den Einstellungen für die freigegebene Konfiguration die notwendigen Installationsdateien in eine Netzwerkfreigabe zu exportieren (Abbildung 13.61).

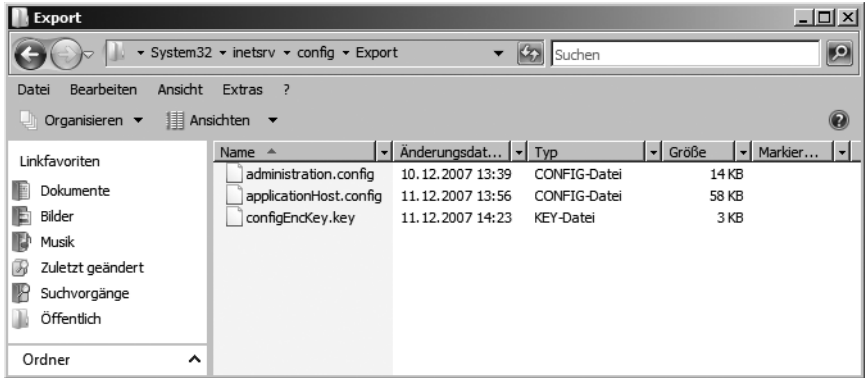
Abbildg. 13.61 Exportieren der Konfiguration eines Webservers für die gemeinsame Konfiguration



Die Konfigurationsdaten lassen sich auch verschlüsseln, damit keine unbefugten Anwender Zugriff auf die Einstellungen der Webserver nehmen können. Beim Exportieren werden folgende Daten berücksichtigt:

- **administration.config** Diese Datei enthält die Servereinstellungen für den Internetinformationsdienste-Manager
- **applicationHost.config** Diese Datei enthält die Einstellungen auf Serverebene
- **configEncKey.key** Diese Datei enthält den Verschlüsselungsschlüssel für den Zugriff auf die freigegebene Konfiguration. Alle Computer, welche die gemeinsame Konfiguration nutzen, importieren diesen Schlüssel und speichern ihn lokal.

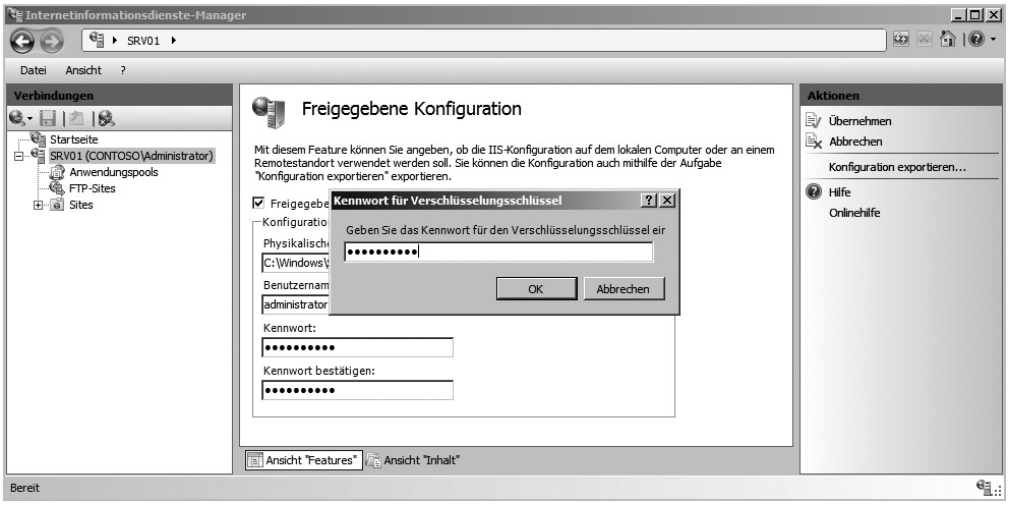
Abbildg. 13.62 Beim Exportieren der Konfiguration werden drei Dateien kopiert



Wird die freigegebene Konfiguration auf einem Server aktiviert, muss das Kennwort angegeben werden, dass beim Exportieren konfiguriert wurde. Erst dann wird diese Konfiguration übernommen.

Nachdem die gemeinsame Konfiguration aktiviert wurde, sollten Sie den Internetinformationsdienste-Manager schließen und den Dienst *IIS-Verwaltungsdienst* neu starten

Abbildg. 13.63 Beim Aktivieren der gemeinsamen Konfiguration muss das Kennwort für den Verschlüsselungsschlüssel eingegeben werden



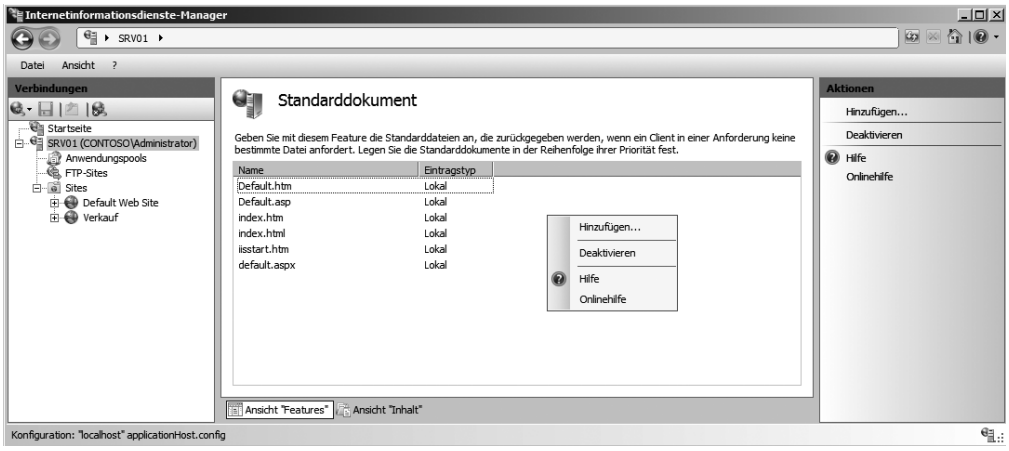
Konfigurieren der Webseiten, Dokumente und HTTP-Verbindungen

Greifen Anwender auf einen Server über eine Domäne zu, zum Beispiel *http://www.contoso.com*, wird das Standarddokument der Seite angezeigt. Anwender müssen nicht *http://www.contoso.com/default.hmtl* eingeben, sondern die Seite *default.html* kann in IIS bereits hinterlegt werden. Es kann aber nicht nur ein Dokument angegeben werden, sondern eine komplette Liste, die der Server nach und nach abarbeitet. Wird kein Standarddokument hinterlegt oder kann das entsprechende Verzeichnis nicht durchsucht werden, erhält der Anwender eine typische *404 – Datei nicht gefunden*-Meldung.

Festlegen des Standarddokuments

Damit ein Standarddokument angezeigt wird, muss diese Funktion erst aktiviert und entsprechende Standarddokumente hinterlegt werden. Die Konfiguration des Standarddokumentes eines Servers findet über das Feature *Standarddokument* im Internetinformationsdienste-Manager statt. Die Funktion ist standardmäßig bereits aktiviert und es sind einige Dokumente hinterlegt (Abbildung 13.64). Über das Kontextmenü kann die Funktion deaktiviert werden, zum Beispiel, wenn Sie die Funktion *Verzeichnis durchsuchen* im nächsten Abschnitt konfigurieren. Auch neue Dokumente können an dieser Stelle hinterlegt werden. Bereits vorhandene Dokumente lassen sich über deren Kontextmenü aus der Liste entfernen. Hierüber kann auch die Reihenfolge, in welcher der Server nach einem Dokument sucht, konfiguriert werden. Standarddokumente können auf Ebene des Servers, aber auch für einzelne Webseiten und Anwendungen hinterlegt werden.

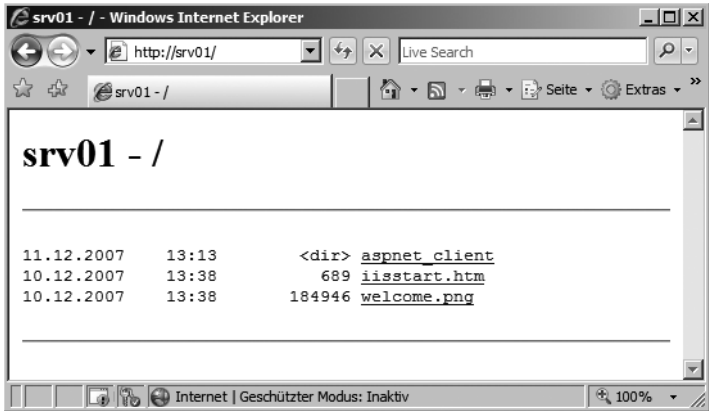
Abbildg. 13.64 Konfigurieren von Standarddokumenten in IIS



Das Feature *Verzeichnis durchsuchen* aktivieren und verwalten

Wird im Internetinformationsdienste-Manager das Feature *Verzeichnis durchsuchen* aktiviert und konfiguriert, wird Anwendern der komplette Inhalt des hinterlegten Verzeichnisses angezeigt, wenn in der URL nicht ein spezifisches Dokument direkt angegeben wurde. Auch wenn kein Standarddokument hinterlegt worden ist oder das Feature *Standarddokument* deaktiviert wurde, wird in diesem Fall das ganze Verzeichnis angezeigt, keine spezielle Webseite (Abbildung 13.65). Standardmäßig ist dieses Feature deaktiviert und muss zuerst aktiviert werden. Da die Verzeichnisse nicht angezeigt werden, wird die Sicherheit des Servers erhöht.

Abbildg. 13.65 Anzeigen des Verzeichnisinhalts statt einer HTML-Seite



Durch diese Funktion können schnell verschiedene Dateien zur Verfügung gestellt werden, zum Beispiel ohne eine HTML-Seite zu konfigurieren.

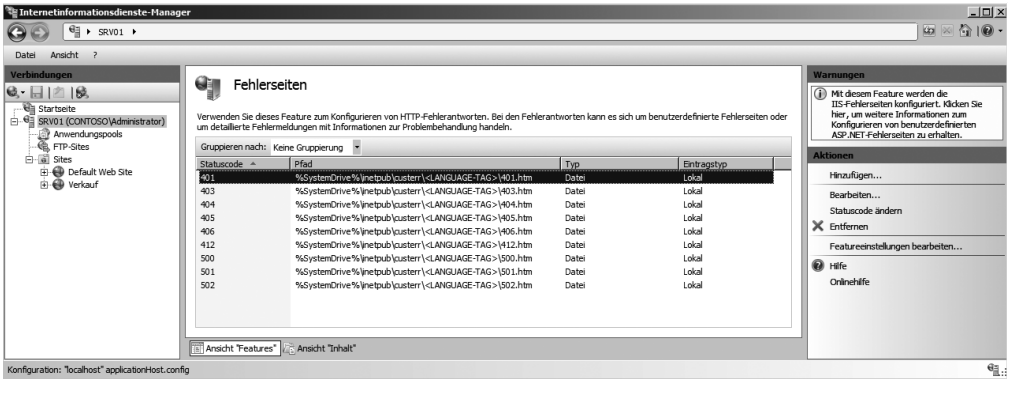
Abbildg. 13.66 Damit das Verzeichnis einer Webseite durchsucht wird, muss die Funktion erst aktiviert werden

Diese Funktion kann auf Ebene des Servers, also der Standardwebseite, oder für einzelne Webseiten und Anwendungen aktiviert werden. Sollen nicht alle Verzeichnisse oder Dateien angezeigt werden, kann auch mit NTFS-Berechtigungen gearbeitet werden.

Konfigurieren der HTTP-Fehlermeldungen

Auf Ebene des Servers oder der einzelnen Webseiten können die Fehlermeldungen, die den Anwendern angezeigt werden, ebenfalls bearbeitet und konfiguriert werden. Über das Feature *Fehlerseiten* im Internetinformationsdienste-Manager können Sie sich eine Liste aller hinterlegten Fehlermeldungen anzeigen lassen (Abbildung 13.67). Über das Kontextmenü können entweder andere HTML-Seiten hinterlegt oder neue Fehlermeldungen konfiguriert und angezeigt werden.

Abbildg. 13.67 Die Fehlerseiten in IIS können modular bearbeitet werden



Neben den Standardfehlermeldungen besteht natürlich die Möglichkeit, die angezeigten Meldungen anzupassen. Für die Fehlermeldungen 400, 403.9, 411, 414, 500, 500.11, 500.14, 500.15, 501, 503 und 505 können allerdings keine angepassten Fehlermeldungen erstellt werden.

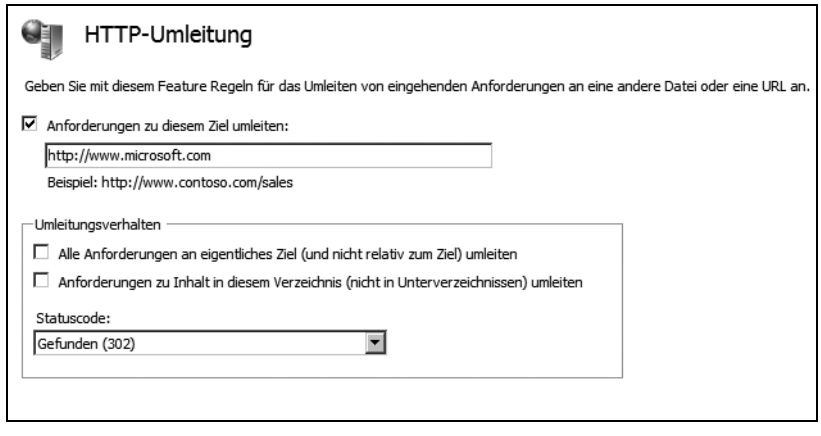
Um angepasste Fehlermeldungen anzuzeigen, öffnen Sie die Verwaltung der Fehlerseiten im Internetinformationsdienste-Manager. Klicken Sie im Aktionenbereich auf den Link *Hinzufügen*. Anschließend öffnet sich ein Dialogfeld, über das Sie die verschiedenen Daten der Fehlermeldung konfigurieren können.

Konfigurieren von HTTP-Umleitungen

Bei einer HTTP-Umleitung werden alle Zugriffe auf eine bestimmte URL zu einer anderen URL automatisch umgeleitet. So können Sie zum Beispiel Ihre Seite umleiten lassen, wenn Teile davon bearbeitet werden. Beispielsweise können Sie alle Anfragen zu *http://www.contoso.com/marketing/default.aspx* zur Seite *http://www.contoso.com/sales/default.aspx* umleiten lassen. Die Konfiguration der Umleitungen können auf Serverebene oder auf Ebene der Webseiten über das Feature *HTTP-Umleitung* durchgeführt werden.

Neben der Umleitung kann an dieser Stelle auch das Verhalten dieser Konfiguration festgelegt werden. Aktivieren Sie das Kontrollkästchen *Alle Anforderungen an eigentliches Ziel (und nicht relativ zum Ziel) umleiten*, werden Anfragen immer exakt zu der Adresse umgeleitet, die in der Umleitung konfiguriert wurde. Das gilt auch dann, wenn Anfragen an Unterverzeichnisse gestellt werden. Wird das Kontrollkästchen *Anforderungen zu Inhalt in diesem Verzeichnis (nicht in Unterverzeichnissen) umleiten* aktiviert, werden Anfragen, die an Unterverzeichnisse des umgeleiteten Verzeichnisses gerichtet sind, direkt an das Weiterleitungsziel geleitet, ohne die Unterverzeichnisse zu berücksichtigen. Beachten Sie, dass diese Konfiguration noch in der Konsole bestätigt werden muss.

Abbildg. 13.68 Konfigurieren der HTTP-Umleitung



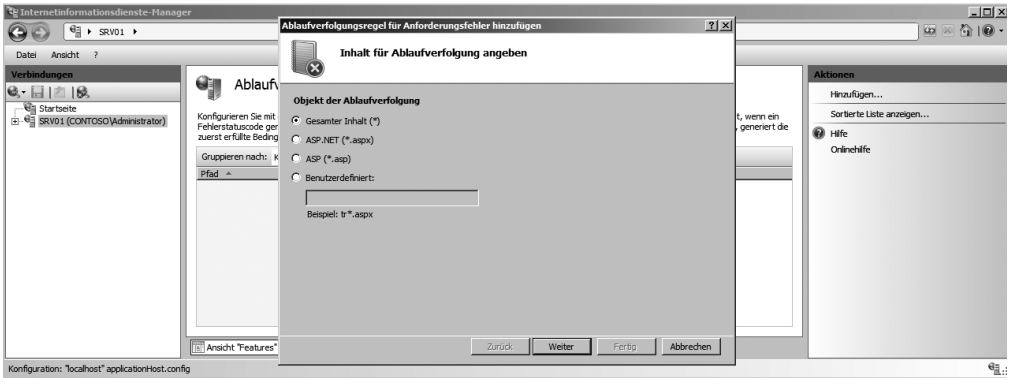
IIS 7.0 überwachen und Logdateien konfigurieren

In diesem Abschnitt gehen wir auf die Überwachung der IIS-Zugriffe ein. Vor allem zur Fehlersuche beim Zugriff sind die verschiedenen Möglichkeiten der Überwachung ein wichtiger Punkt bei der Verwaltung von IIS. Die Überwachung kann auf Ebene des Servers, der Webseiten, von Applikation und physischen wie virtuellen Verzeichnissen abgewickelt werden.

Ablaufverfolgungsregeln für Anforderungsfehler

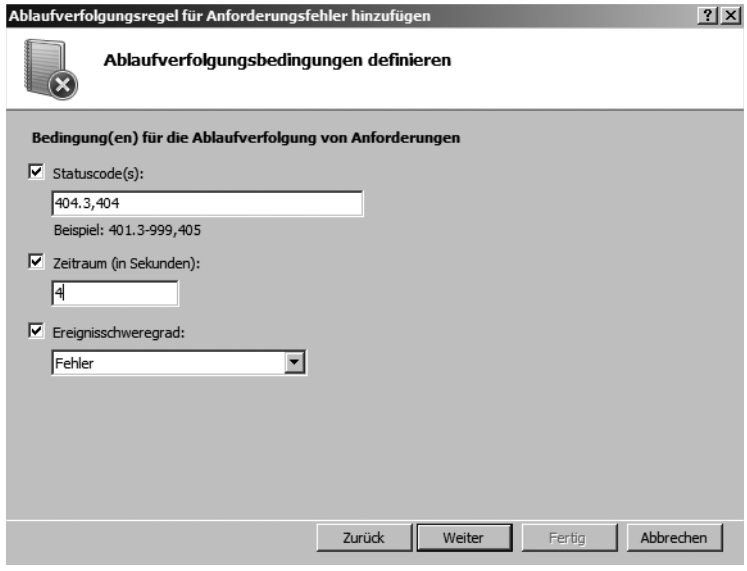
Doppelklicken Sie im Internetinformationsdienste-Manager auf das Feature *Ablaufverfolgungsregeln für Anforderungsfehler*, können Regeln erstellt und bearbeitet werden, mit denen die fehlerhaften Zugriffe auf den Server überwacht werden können (Abbildung 13.69). Neue Regeln lassen sich über das Kontextmenü oder den Aktionsbereich erstellen.

Abbildg. 13.69 Erstellen und verwalten von Regeln für die Ablaufverfolgung



Über den Assistenten kann auf verschiedenen Seiten festgelegt werden, was der Server überwachen soll. Auf der nächsten Seite des Assistenten legen Sie fest, welche Fehler protokolliert werden sollen. Dadurch erhalten Sie ein Protokoll und müssen den Fehler nicht erst nachstellen. Sobald eine der hinterlegten Bedingungen auftritt, wird der Fehler protokolliert. Auf der Seite der Bedingungen können auch mehrere Statuscodes hinterlegt werden, die jeweils durch Komma voneinander getrennt werden (Abbildung 13.70). Im Feld *Zeitraum (in Sekunden)* geben Sie an, wie lange der Zeitraum ist, welche die Anforderung verbrauchen darf, bevor der Fehler protokolliert wird.

Abbildg. 13.70 Festlegen der Bedingungen, bei denen die Ablaufverfolgung einen Fehler protokolliert

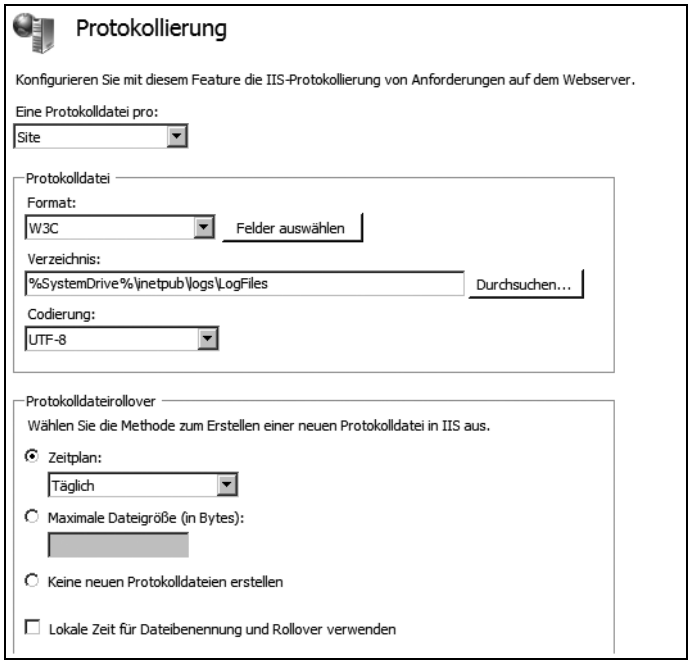


Auf der nächsten Seite des Assistenten legen Sie schließlich fest, welche der Anbieter überwacht werden sollen, und sofern möglich, auch welche Module der Anbieter. Über das Listenfeld *Ausführlichkeitsgrad* legen Sie fest, wie viele Daten protokolliert werden sollen. Hier kann für die jeweiligen Anbieter ein unterschiedlicher Protokollierungsgrad ausgewählt werden. Nach der Erstellung der Regel wird diese im Fenster angezeigt. Es können weitere Regeln erstellt und vorhandene Regeln können nachträglich über deren Kontextmenü bearbeitet werden. Die Logdateien werden standardmäßig im Verzeichnis *\inetpub\logs\FailedReqLogFiles* gespeichert.

Allgemeine Protokollierung aktivieren und konfigurieren

Neben der Ablaufverfolgung für fehlerhafte Anforderungen kann auch der normale Betrieb von IIS protokolliert werden. Dazu steht der Punkt Protokollierung auf der Startseite des Internetinformationsdienste-Managers zur Verfügung. Die Protokollierung kann für einzelne Seiten und Anwendungen getrennt aktiviert oder deaktiviert werden. Auch dazu steht das Feature *Protokollierung* zur Verfügung, wenn Sie die entsprechende Seite oder Anwendung im IIS-Manager anklicken (Abbildung 13.71). Standardmäßig ist die Protokollierung für den Server an sich und für Webseiten aktiviert. Über den Aktionsbereich der Konsole kann diese für einzelne Bereiche gezielt deaktiviert werden. Die Protokolldateien können in einem beliebigen Verzeichnis abgelegt werden und befinden sich standardmäßig im Verzeichnis *\inetpub\logs\LogFiles*.

Abbildg. 13.71 Konfiguration der Protokollierung für IIS



Im ersten Auswahlfeld wird über ein Listenfeld ausgewählt, ob für jede Webseite eine Protokolldatei erstellt werden soll oder eine Datei für den kompletten Server. Als Format stehen für die Protokolldatei verschiedene Möglichkeiten zur Verfügung. Die Codierung der Protokollierung sollte bei UTF-8 belassen werden:

- **W3C** Dies ist die Standardauswahl. Diese Protokolldateien werden textbasiert gespeichert und über die Schaltfläche *Felder auswählen* wird festgelegt, was in der Datei protokolliert werden soll. Die einzelnen Felder werden durch Leerzeichen getrennt.
- **IIS** Bei dieser Auswahl werden die Protokolldateien ebenfalls im Textformat gespeichert. Die einzelnen Felder sind allerdings fest vorgegeben und können daher nicht angepasst werden. Die einzelnen Felder werden durch Kommas getrennt.
- **Binär** Bei dieser Auswahl wird eine Protokolldatei für alle Webseiten auf dem Server erstellt, daher steht diese nur dann zur Verfügung, wenn die Protokollierung pro Server eingestellt wird, nicht pro Datei. Die Daten werden in binärer Form gespeichert. Der Vorteil bei dieser Auswahl ist, dass der Server extrem wenig belastet wird, da nur wenige Daten protokolliert werden. Vor allem Server mit hohem Besucheraufkommen sollten dieses Format verwenden. Im Gegensatz zu den anderen Formaten können diese Dateien nicht mit einem Texteditor gelesen werden. Hier bietet sich das kostenlose Zusatztool Logparser an, das Microsoft ebenfalls zur Verfügung stellt. Mithilfe des Protokollparsers können Einträge gefiltert, Protokolldateien in andere Formate konvertiert und Datenfilterung durchgeführt werden. Das Tool unterstützt unterschiedliche Eingabeformate einschließlich sämtlicher IIS-Protokolldateiformate. Protokollparser unterstützt gleichermaßen mehrere Ausgabeformate, wie beispielsweise Textdateien und Datenbanktabellen.

- **NCSA** Bei NCSA handelt es sich um die National Center For Supercomputing Applications. Auch hier werden die Felder fest vorgegeben und es werden weniger Informationen protokolliert als bei den anderen Protokollmethoden.

Ebenfalls in diesem Fenster legen Sie fest, wann neue Protokolldatei erstellt werden sollen, also nach einem bestimmten Zeitplan (Stündlich, Täglich, Wöchentlich oder Monatlich), nach einer bestimmten Größe oder überhaupt nicht. Die Auswahl hängt unter anderem von der Besucheranzahl des Servers ab. Aktivieren Sie nicht die Option *Lokale Zeit für Dateibenennung und Rollover verwenden*, wird standardmäßig die UTC-Zeit (Universelle Weltzeit) verwendet (*http://de.wikipedia.org/wiki/Koordinierte_Weltzeit*).

Überprüfen der Arbeitsprozesse der Anwendungspools

Über das Feature *Arbeitsprozesse* auf der Startseite des Internetinformationsdienste-Managers werden die laufenden Prozesse sowie deren Ressourcenverbrauch angezeigt. Anwendungspools können dabei auch mehrere Arbeitsprozesse, oft auch als Worker Processes bezeichnet, starten. Die eigentlichen Websites, sei es in Form von simplen statischen Websites oder als komplexe webbasierende Anwendungen, werden über diese Worker Processes abgewickelt, die eine Art von Mini-Webservern sind. Diese Arbeitsprozesse nutzen die Dienste der zentralen Komponenten, agieren also aus Sicht der Anwendungen als Webserver. Die Verwaltungskomponente überwacht den Status der Arbeitsprozesse, löscht sie, wenn sie nicht mehr erforderlich sind und kann sie neu starten, wenn Fehler in diesen Prozessen auftreten.

Optimieren der Serverleistung

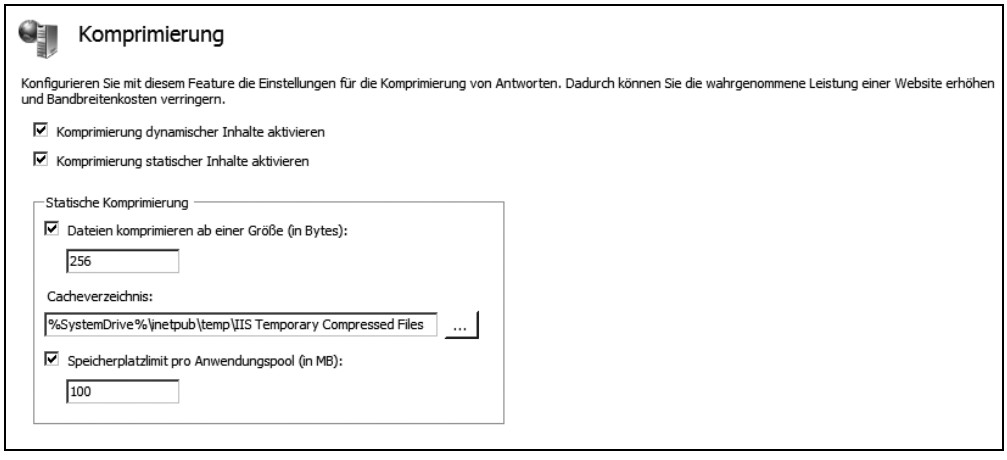
Die Optimierung der Serverleistung ist kein einfaches Unterfangen. Damit ein Server schnell und performant zur Verfügung steht, sind nicht nur Konfigurationen in IIS notwendig, sondern auch die Serverleistung an sich muss passen. Im folgenden Abschnitt gehen wir auf Möglichkeiten ein, Anfragen an IIS mit den Bordmitteln des Internetinformationsdienste-Managers zu verbessern.

Komprimierung aktivieren

Mit der Komprimierung werden die Antwortzeiten eines Servers verbessert und Bandbreite bei der Übertragung von Webseiten kann gespart werden. Die Komprimierung wird über das Feature *Komprimierung* im Internetinformationsdienste-Manager gesteuert. Manche Einstellungen stehen nur auf Serverebene zur Verfügung. Viele Einstellungen können aber auch auf Ebene der Websites und Anwendungen vorgenommen werden, sodass jede Anwendung eigene Einstellungen für die Kom-

primierung verwenden kann. Wird die Komprimierung aktiviert, belastet das zwar die Serverhardware, aber die Netzwerkleistung wird erhöht. Ob durch diese Maßnahmen mehr Leistung erzielt wird, hängt davon ab, ob der Server oder die Leitung der Flaschenhals ist. Da meist eher die Leitung schuld an einer langsamen Übertragung ist, wird bei IIS 7.0 die Komprimierung von statischen Inhalten standardmäßig bereits aktiviert (Abbildung 13.72). Wurde ein statischer Inhalt, zum Beispiel eine Seite oder eine Datei, bereits komprimiert, belastet das den Server nicht erneut, da diese Datei bei der nächsten Anfrage einfach wieder aus dem Komprimierungscache zur Verfügung gestellt wird. Aktivieren Sie auch die Komprimierung für dynamische Inhalte, muss jede Übertragung immer wieder erneut komprimiert werden, was zwar Bandbreite spart, aber CPU-Leistung kostet.

Abbildg. 13.72 Konfigurieren der Komprimierung für IIS 7.0

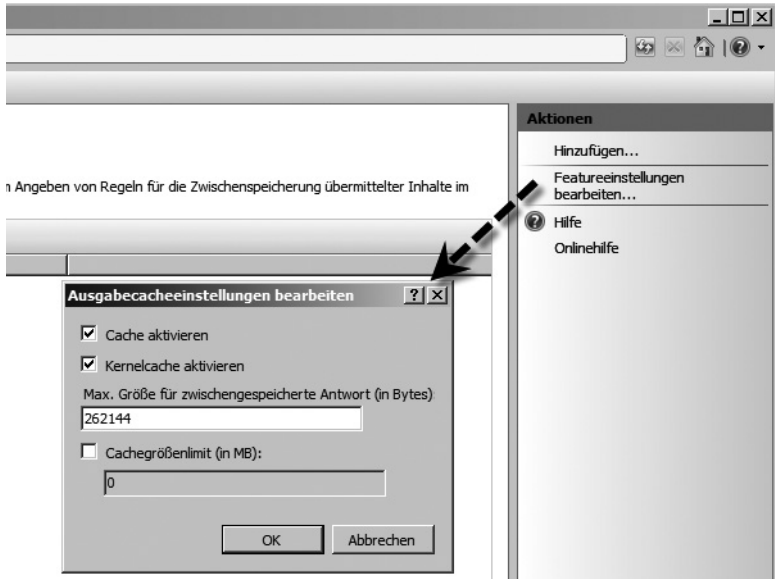


Sie können hier auch festlegen, ab welcher Größe Dateien komprimiert werden sollen und wie viel Speicherplatz jedem Anwendungspool und den darin enthaltenen Webseiten und Anwendungen zur Verfügung steht. Auch der Speicherplatz des Caches wird an dieser Stelle festgelegt.

Ausgabezwischenspeicherung verwenden

Im Cache des Webservers können Teile der Webseiten zur Verfügung gestellt werden, sodass die Abrufe dieser Teile den Server nicht belasten. Anfragen an diese Seiten können durch diese Funktion wesentlich beschleunigt werden. Über das Feature *Ausgabezwischenspeicherung* im Internetinformationsdienste-Manager erreichen Sie die Verwaltung dieser Funktion. Die allgemeinen Einstellungen werden über den Befehl *Featureeinstellungen bearbeiten* über das Kontextmenü oder den Aktionsbereich vorgenommen (Abbildung 13.73).

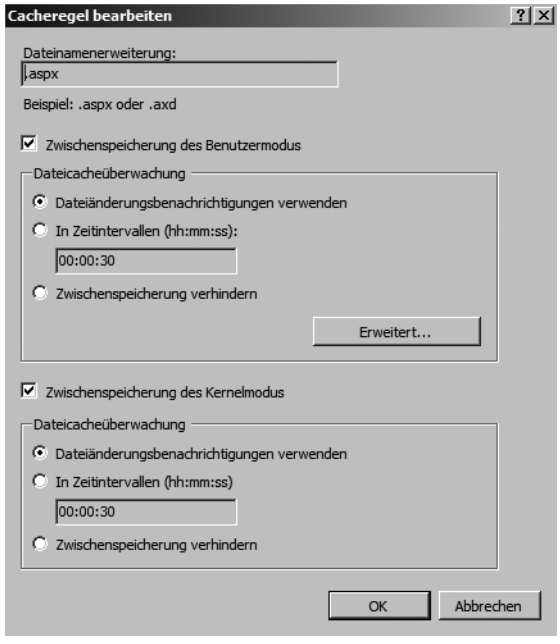
Abbildg. 13.73 Konfigurieren der Ausgabezwischenspeicherung



Der Cache ist standardmäßig aktiviert und die Größe ist nicht beschränkt. In den Einstellungen können die Funktion aktiviert sowie ein Limit festgelegt werden. Der Cache wird allerdings erst dann produktiv genutzt, wenn Regeln festgelegt werden, die bestimmen, welche Daten zwischengespeichert werden sollen. Auch das Kernelcaching ist bereits aktiviert. Bei dieser Funktion werden Anfragen an den Cache nicht im Benutzermodus des Servers durchgeführt, sondern im Kernel selbst. Die Anwendungen werden durch diese Funktion also nicht belastet. Das Cachegrößenlimit sollte möglichst nicht bearbeitet werden. IIS entscheidet selbst, wie viel Speicher er zur Verfügung stellt. Nur wenn Sie feststellen, dass Ihr Server noch nicht vollständig ausgelastet ist, können Sie das Limit erhöhen, sollten dabei aber sehr vorsichtig vorgehen, da schnell ein gegenteiliger Effekt erreicht wird.

Über das Kontextmenü werden neue Regeln für den Cache erstellt. Es öffnet sich ein neues Fenster, über das Einstellungen vorgenommen werden, wie Inhalte für den Benutzermodus und den Kernelmodus zwischengespeichert werden sollen. Zunächst wird im Fenster festgelegt, welche Dateien zwischengespeichert werden können. Als Nächstes wird festgelegt, wie lange die Daten im Zwischenspeicher verbleiben sollen. Es kann entweder eine Zwischenspeicherung bis zur Änderung der Datei oder ein Zeitintervall festgelegt werden. Auch das generelle Verhindern der Zwischenspeicherung für einige Dateitypen kann an dieser Stelle konfiguriert werden. Es können beliebig viele Cacheregeln erstellt werden. Die Regeln können nach der Erstellung jederzeit bearbeitet werden.

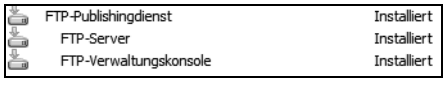
Abbildg. 13.74 Bearbeiten einer Cacheregel



FTP-Server betreiben

Mit IIS 7.0 lässt sich auch ein FTP-Server betreiben, um zum Beispiel performant Dateien für den Download zur Verfügung zu stellen. Bei der FTP-Komponente handelt es sich um einen eigenen Rollendienst, der nachträglich oder bereits bei der Installation der Internetinformationsdienste installiert werden kann. Damit IIS auch als FTP-Server verwendet werden kann, benötigen Sie den Rollendienst *FTP-Publishingdienst*, der jederzeit installiert werden kann.

Abbildg. 13.75 IIS 7.0 kann auch als FTP-Server verwendet werden



Nach der Installation des Rollendienstes ist der FTP-Server allerdings noch nicht gestartet. Rufen Sie die Verwaltung der Dienste auf, zum Beispiel über *services.msc,* und setzen Sie den Dienst *FTP-Publishingdienst* auf *Automatisch* und starten Sie diesen. Der Server kann anschließend über die Verwaltungskonsole konfiguriert werden. Über einen Webbrowser greifen Sie mit der Adresse *ftp://<Servername>* zu. Sie können im Verzeichnis normale Ordner anlegen und mit NTFS-Berechtigungen arbeiten.

Abbildg. 13.76 Auf den FTP-Server zugreifen

Die Verwaltung des FTP-Servers findet teilweise noch über den IIS 6.0-Internetinformationsdienste-Manager statt, der aber über den IIS 7.0-Internetinformationsdienste-Manager gestartet werden kann.

FTP in der Befehlszeile verwenden

Wenn Sie gelegentlich Daten zu einem FTP-Server hochladen müssen, können Sie das auch in der Befehlszeile durchführen. Für Anwender, die häufiger FTP verwenden, bietet es sich an, ein Tool zu erwerben und zu installieren, welches in einer grafischen Oberfläche die FTP-Übertragung zulässt. Hinzu kommt, dass die FTP-Übertragung per Befehlszeile in Windows nicht verschlüsselt stattfindet. Als Notlösung, oder wenn Sie nur selten Dateien per FTP hochladen müssen, eignet sich die Befehlszeile jedoch durchaus. Damit das Hochladen per FTP in der Befehlszeile funktioniert, müssen Sie zunächst eine Textdatei vorbereiten, welche die notwendigen Konfigurationsschritte enthält. In dieser Konfigurationsdatei werden auch die einzelnen Dateien angegeben sowie der FTP-Server, zu dem Sie diese Dateien hochladen wollen. Wenn Sie eine neue Textdatei für die FTP-Konfiguration erstellen und konfigurieren wollen, können Sie diese zum Beispiel *login.txt* nennen. Die Datei sollte folgenden Inhalt haben:

Listing 13.1 Konfigurationsdatei für den Upload von FTP-Dateien

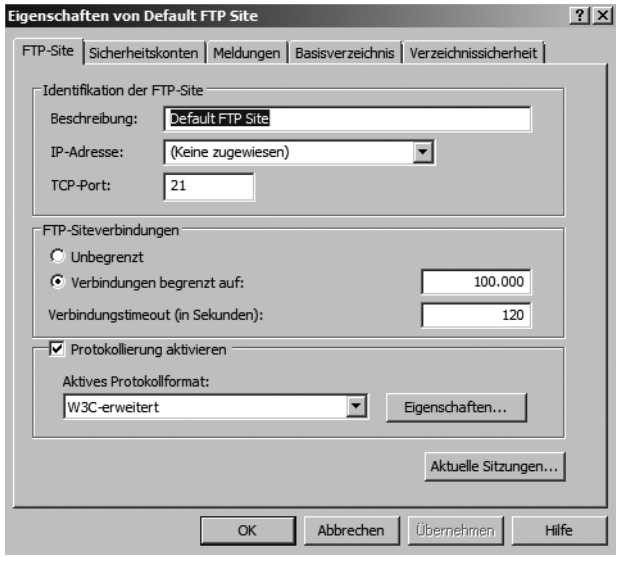
```
Open <DNS-Name oder IP-Adresse des FTP-Servers>
<Benutzername>
<Kennwort>
lc
cd <Verzeichnis, in das hochgeladen werden soll>
ascii
send <Dateiname>
send <Weitere Dateien>
```

Mit dem Befehl *send <Dateiname>* können Sie beliebig viele Dateien zum angegebenen FTP-Server hochladen. Möchten Sie nun die Übertragung starten, müssen Sie in der Befehlszeile den Befehl *ftp –s:C:\login.txt* ausführen.

Konfiguration des FTP-Servers

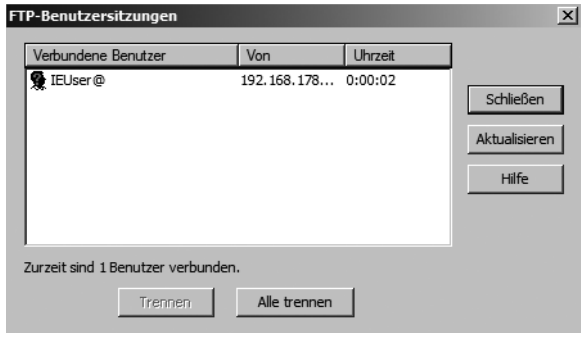
Der FTP-Dienst bietet nicht so viele Konfigurationsparameter wie die Webseiten. Einige davon sind zudem relativ ähnlich zu denen, die sich bei WWW-Dienst finden. Nach der Installation müssen Sie den IIS-Manager neu starten. Erst dann werden die FTP-Einstellungen angezeigt. Über die Registerkarte *FTP-Site* können die Festlegungen zur Identifikation, zu den maximalen Verbindungen sowie zur Protokollierung konfiguriert werden. Über die Registerkarte *Sicherheitskonten* kann definiert werden, ob anonyme Verbindungen zugelassen und über welches Benutzerkonto diese abgewickelt werden sollen. Wie für die anderen virtuellen Server auch, lassen sich die verwendete IP-Adresse sowie der TCP-Port angeben. Im Gegensatz zu anderen Protokollen kann für FTP allerdings nur eine Adresse und ein Port angegeben werden. Die Anzahl eingehender Verbindungen ist in der Standardeinstellung auf 100.000 gesetzt, was faktisch keiner Begrenzung entspricht, weshalb Sie in diesem Fall auch *Unbegrenzt* wählen können.

Abbildg. 13.77 Die Eigenschaften des FTP-Servers werden über den IIS-Manager konfiguriert



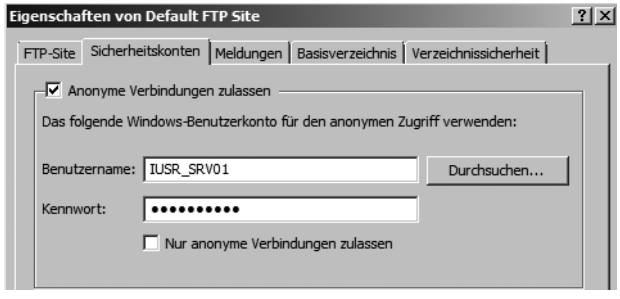
Die Auswahl der verschiedenen Formate der Protokolldateien ist bei FTP auf *W3-erweitert*, *ODBC* und *Microsoft IIS* beschränkt, ansonsten ist die Konfiguration der Protokollierung identisch mit dem bereits beschriebenen Webserver. Die aktuell mit dem virtuellen FTP-Server verbundenen Benutzer können Sie jederzeit über die Schaltfläche *Aktuelle Sitzungen* anzeigen lassen. Neben dem Benutzernamen, mit dem sich ein Anwender am FTP-Server angemeldet hat, sehen Sie zusätzlich, von welcher IP-Adresse aus der Zugriff erfolgt ist. Die Dauer der Verbindung wird ebenfalls angezeigt. Falls die Verbindung nicht mehr benötigt wird oder Sie vermuten, dass es sich bei dem Benutzer um einen unbefugten Eindringling handelt, wählen Sie den entsprechenden Benutzer aus und beenden die Verbindung über *Trennen*.

Abbildg. 13.78 Anzeigen und trennen der verbundenen Benutzer



Über *Durchsuchen* wählen Sie aus der Liste das Konto aus, mit dem die automatische Anmeldung erfolgen soll. Geben Sie danach das Kennwort für das Konto ein. Falls Sie den virtuellen FTP-Server in einer gesicherten Umgebung einsetzen wollen, in der nur autorisierte Benutzer Zugriff auf die Dateien haben sollen, deaktivieren Sie das Kontrollfeld *Anonyme Verbindungen zulassen*. Umgekehrt können Sie über *Nur anonyme Verbindungen zulassen* auch ausschließen, dass Anwender ihre Anmeldekennung verwenden, über die sie unter Umständen erweiterte Berechtigungen hätten.

Abbildg. 13.79 Verwalten der Berechtigungen für FTP-Benutzer

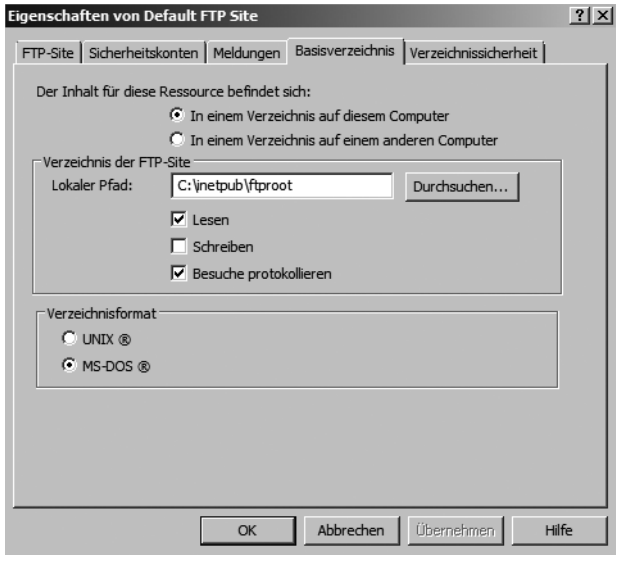


HINWEIS FTP arbeitet mit unverschlüsselten Kennwörtern. Aus diesem Grund sollte gut überlegt werden, ob bei FTP überhaupt mit einer Authentifizierung gearbeitet wird. Falls diese genutzt wird, sollte das idealerweise nur mit getrennten Benutzerkonten, die nur für FTP eingesetzt werden, oder über eine durch IPsec gesicherte Verbindung erfolgen.

Sie haben über die Registerkarte *Meldungen* die Möglichkeit, einen langen Banner-Text anzugeben, der dem Anwender beim Aufbau der Verbindung angezeigt wird, sowie einen Willkommen-Text, der nach der Anmeldung erscheint. Ein kurzer Beenden-Text erlaubt eine Nachricht zum Ende der Verbindung. Sobald das auf der Registerkarte *FTP-Site* angegebene Verbindungslimit erreicht ist, nimmt der Server keine neuen Verbindungen mehr an, kann dem Anwender aber eine Meldung anzeigen, die ihn darauf hinweist, dass das System derzeit ausgelastet ist. Diesen Text können Sie im Feld *Maximale Verbindungen* angeben. Über den FTP-Server ist der Zugriff auf die lokalen Laufwerke des Servers möglich, es können aber auch Freigaben auf anderen Servern zugänglich gemacht werden. So genügt ein einziger FTP-Server, um auf alle Ressourcen im gesamten Netzwerk zuzugrei-

fen. Über die virtuellen Verzeichnisse, mit denen wir uns im Anschluss beschäftigen, wird ein solcher Zugriff eingerichtet. In der Standardeinstellung *In einem Verzeichnis auf diesem Computer* wird ein lokales Verzeichnis verwendet. Wählen Sie *In einem Verzeichnis auf einem anderen Computer* für den Zugriff auf die Freigabe eines anderen Servers. Anschließend geben Sie unter *Verzeichnis der FTP-Site* den lokalen Pfad bzw. die Freigabe an.

Abbildg. 13.80 Verwalten des Speicherorts der FTP-Dateien



Wie bei Standardfreigaben können an dieser Stelle auch generell Berechtigungen für den Zugriff über FTP gesetzt werden. Zur Verfügung steht allerdings nur die Berechtigung *Lesen*, die standardmäßig gesetzt ist. Schreibzugriffe sowie das Löschen von Dateien sind erst dann möglich, wenn die Berechtigung *Schreiben* gegeben wird. Zusätzlich können die einzelnen Dateien und Verzeichnisse auch noch lokal über NTFS-Berechtigungen einzeln mit Berechtigungen versehen werden. Falls Sie auf der Registerkarte *FTP-Site* die Protokollierung eingeschaltet haben, aktivieren Sie das Kontrollkästchen *Besuche protokollieren*, um die Zugriffe in diesem Verzeichnis zu protokollieren. Um die Anzeige der Dateien an die Gewohnheiten der Anwender anpassen zu können, haben Sie unter Verzeichnisformat noch die Möglichkeit, zwischen den Formaten UNIX und MS-DOS zu wählen.

Neben der Zugriffssicherung über die Anmeldung kann zusätzlich noch anhand von Adressen eine Einschränkung des Zugriffs durchgeführt werden. Das ist besonders dann wichtig, wenn Anwender von sicheren wie unsicheren Netzwerken aus auf den FTP-Server zugreifen können. Sofern die Gefahr besteht, dass ein Angreifer die unverschlüsselte Anmeldung protokolliert und somit in den Besitz der Benutzernamen und Passwörter gelangt, sollten Sie den Zugriff über die Registerkarte *Verzeichnissicherheit* einschränken. Dabei können Sie entweder mit einer Positiv- oder Negativliste arbeiten. In der Standardeinstellung wird mit einer leeren Negativliste gearbeitet, es wird also allen Systemen der Zugriff gestattet. Fügen Sie die Systeme der Liste hinzu, denen Sie explizit den Zugriff verweigern wollen. Andererseits können Sie über *Zugriff verweigert* auch zunächst allen Systemen den Zugriff verweigern und anschließend den gewünschten Systemen explizit erlauben.

Abbildg. 13.81 Verwalten der Berechtigungen für einen FTP-Server

Erstellen virtueller Verzeichnisse

Über den virtuellen FTP-Server ist zunächst einmal nur der Zugriff auf die lokale Festplatte des Servers bzw. eine Freigabe im Netzwerk möglich. Ein Anwender, der Daten von mehreren Servern haben möchte, müsste sich daher mit allen Servern verbinden und jeweils die benötigten Daten übertragen. Über virtuelle Verzeichnisse können allerdings andere Laufwerke oder Computer unter einem einzigen FTP-Server zusammengefasst werden, die dann nach außen für den Anwender wie ein einziges System erscheinen, in dessen Verzeichnissen er irgendwo die benötigten Dateien findet. Sie erstellen ein virtuelles Verzeichnis aus dem Kontextmenü des jeweiligen virtuellen FTP-Servers heraus über *Neu/Virtuelles Verzeichnis*. Eine Verschachtelung virtueller Verzeichnisse ist ebenfalls möglich – wählen Sie dann den gleichen Menüpunkt, allerdings in diesem Fall aus dem Kontextmenü eines bereits angelegten virtuellen Verzeichnisses.

Geben Sie anschließend den Alias an, also den Namen, mit dem der Anwender in das virtuelle Verzeichnis wechselt und den Pfad, in dem die Daten des virtuellen Verzeichnisses tatsächlich liegen. Als Nächstes definieren Sie die Zugriffsrechte der Anwender, wobei die Berechtigung *Lesen* bereits gesetzt ist. Gewähren Sie über *Schreiben* bei Bedarf auch Schreibrechte.

Weitere virtuelle FTP-Server erstellen Sie, indem Sie im Kontextmenü des Knotens *FTP-Sites* die Option *Neu/FTP-Site* auswählen. Weisen Sie anschließend dem neuen virtuellen FTP-Server einen Namen zu und wählen Sie dann aus, über welche IP-Adresse und welchen TCP-Port der Server angesprochen werden soll. Achten Sie dabei darauf, dass sich entweder die IP-Adresse oder der TCP-Port oder beides von den Einstellungen bereits existierender virtueller Server unterscheiden, da es sonst zu Kommunikationsproblemen kommt. Danach geben Sie an, welches lokale Verzeichnis bzw. welche Freigabe über den virtuellen FTP-Server zur Verfügung gestellt werden soll und ob der Anwender Lese- und/oder Schreibrechte bekommen soll. Anschließend steht der neue virtuelle FTP-Server bereits zur Verfügung.

Zusammenfassung

Wie Sie gelesen haben, hat Microsoft in IIS zahlreiche Änderungen und viele Verbesserungen vorgenommen. Die Verwaltung wurde überarbeitet und mit den neuen Befehlszeilentools kann ein Webserver jetzt auch über Skripts konfiguriert werden. Erfahren Sie im nächsten Kapitel, welche Sicherheitsfunktionen es in Windows Server 2008 gibt und wie Sie mit der Festplattenverschlüsselung *BitLocker* Server auch in kleinen Niederlassungen optimal schützen.

Kapitel 14

Neue Sicherheitsfunktionen

In diesem Kapitel:

Microsoft hat vor allem im Bereich Sicherheit einiges in Windows Server 2008 optimiert. Wir sind in den einzelnen Kapiteln dieses Buches genauer auf die einzelnen Sicherheitsfunktionen von Windows Server 2008 eingegangen, sofern diese direkt mit einzelnen Serverkomponenten verknüpft sind. In diesem Kapitel zeigen wir Ihnen die neuen Sicherheitsfunktionen von Windows Server 2008, die für alle Serverdienste zur Verfügung stehen und die Sicherheit des Servers im Allgemeinen erhöhen. Außerdem erläutern wir Ihnen in diesem Kapitel, wie die Festplatten von Servern sicher mit BitLocker vor einem möglichen Datendiebstahl geschützt werden.

Neuerungen im Betriebssystem-Kern

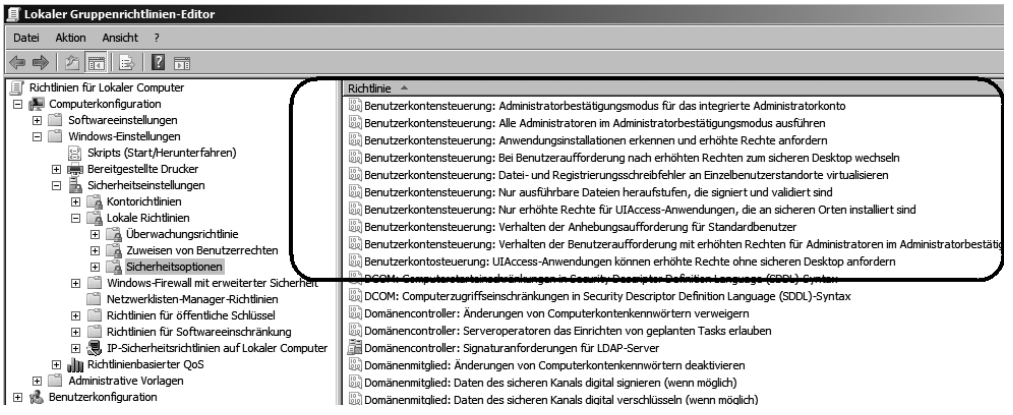
Der Kernel des Betriebssystem wird unter Windows Server 2008 besser geschützt. Die Anzahl der Komponenten, die im Kernelmodus betrieben werden, sind deutlich reduziert worden. Durch diese Reduzierung werden Kernelabstürze, die auch im Absturz des Servers resultieren, verhindert. Die meisten Dienste laufen jetzt im Kontext des Benutzers, sodass Abstürze das System nicht mehr gefährden können. Die Berechtigungsstufen der Dienste wurde im Vergleich zu Windows Server 2003 deutlich eingeschränkt. Dienste laufen jetzt nicht mehr mit maximaler Berechtigung, sondern nur mit minimalen Berechtigungen. Dienste werden auch durch die Windows-Firewall geschützt und eingeschränkt. Durch diese Einschränkungen werden Dienste daran gehindert Manipulationen am Dateisystem und der Registry durchzuführen. Wird ein Dienst kompromittiert, kann ein Dienst mit zu vielen Rechten nicht ein ganzes System oder gar Netzwerk angreifen. DLLs und Dienste werden beim Starten ebenfalls validiert. Dazu erstellt Windows Server 2008 einen Hashwert, der durch ein X.509-Zertifikat geschützt wird. Stellt der Server beim Starten fest, dass der Hashwert nicht mit den tatsächlichen Daten des Dienstes oder der DLL übereinstimmt, wird die Funktion blockiert. Wie unter Windows Vista kann auch unter Windows Server 2008 die Installation neuer Hardware über Gruppenrichtlinien verhindert werden (siehe Kapitel 9).

Benutzerkontensteuerung

Die neue Funktion der Benutzerkontensteuerung (User Account Control, UAC) dient hauptsächlich dazu, die Arbeitsstationen vor ungewollten Änderungen zu schützen und kann auch für Server per Richtlinie aktiviert werden. Wird im Unternehmen Windows Vista eingesetzt, kann die Benutzerkontensteuerung auf zentraler Ebene durch Gruppenrichtlinien konfiguriert werden. Wenn ein Benutzer angemeldet ist und eine Tätigkeit durchführen will, die administrative Rechte benötigt, erscheint das Warnfenster der Benutzerkontensteuerung und der Anwender muss die Authentifizierungsdaten eines Administratorkontos eingeben. Wenn der Anwender jedoch bereits über Administratorberechtigungen verfügt, erscheint ein Warnfenster, das zuerst bestätigt werden muss, bevor die Aktion durchgeführt wird. Dadurch sind jetzt erstmalig in Windows auch Administratorkonten davor geschützt, ungewollte Änderungen am System durchzuführen. Hauptziel der Benutzerkontensteuerung ist die Reduzierung der Angriffsfläche des Betriebssystems. Hierzu arbeiten alle Benutzer als Standardbenutzer. Der administrative Zugriff ist auf autorisierte Prozesse eingeschränkt. Diese Einschränkung minimiert die Möglichkeiten der Benutzer, Änderungen vorzunehmen, die sich auf die Stabilität des Computers auswirken können oder den Computer versehentlich für Malware oder Viren anfällig machen. Mit der Benutzerkontensteuerung können Administratoren die meisten Anwendungen, Komponenten und Prozesse mit eingeschränkten Privilegien ausführen – sie haben aber gleichzeitig die Möglichkeit, bestimmte Aufgaben oder Anwendungen mit administrativen Rechten auszuführen. Wenn ein Benutzer einen Task ausführt, für den administrative Rechte not-

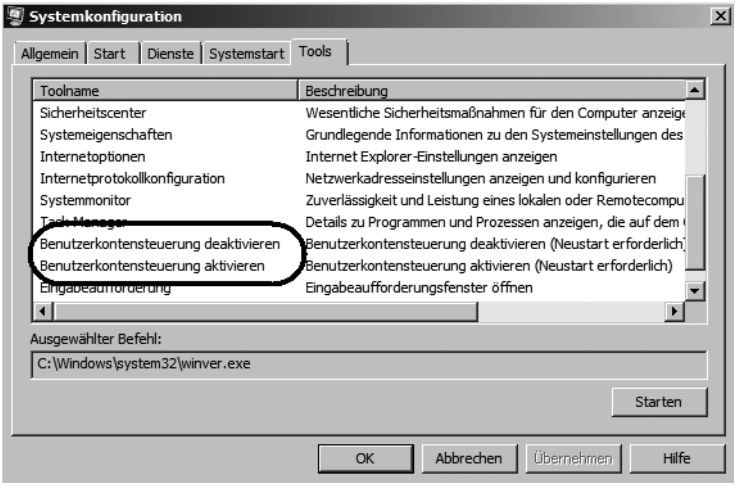
wendig sind (zum Beispiel die Installation einer Anwendung), benachrichtigt Windows Server 2008 beziehungsweise Windows Vista den Benutzer und fragt entsprechende Anmeldeinformationen ab. Die dazu notwendigen Einstellungen finden Sie über *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Sicherheitsoptionen* (Abbildung 14.1). Auf Servern, die nicht Bestandteil einer Domäne sind, kann der Gruppenrichtlinien-Editor für lokale Einstellungen auch über *Start/Ausführen/gpedit.msc* aufgerufen werden.

Abbildg. 14.1 Verwalten der Benutzerkontensteuerung in Windows Server 2008



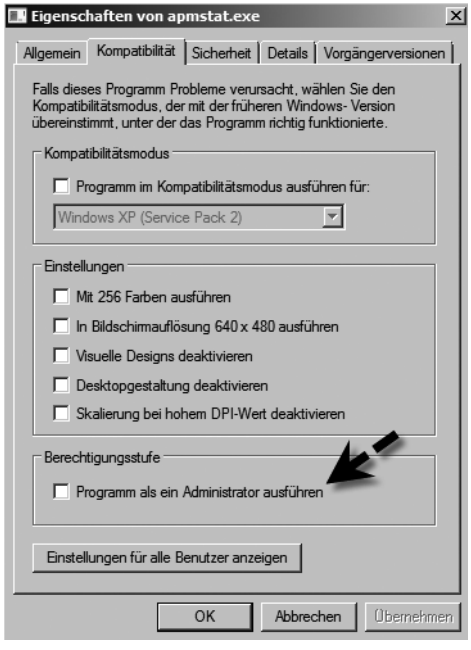
Sie können die Benutzerkontensteuerung über *Start/Ausführen/msconfig* auf der Registerkarte *Tools* deaktivieren (Abbildung 14.2). Markieren Sie die Option zur Deaktivierung der Benutzerkontensteuerung und klicken Sie auf *Starten*. Im Anschluss erscheint eine Befehlszeile, welche die erfolgreiche Ausführung bestätigt. Im Gegensatz zu Windows Vista erscheinen bei Windows Server 2008 keine Meldefenster, die bestätigt werden müssen. Über die Richtlinien können diese Meldungen aber nachträglich genau so aktiviert werden, wie sie bei Windows Vista deaktiviert werden.

Abbildg. 14.2 Deaktivieren der Benutzerkontensteuerung über *msconfig.exe*



Wenn Sie wollen, dass eine Applikation immer im Administratormodus gestartet wird, weil diese zum Beispiel zu dem neuen Windows Server 2008-Modell nicht kompatibel ist, können Sie die auszuführende Datei mit der rechten Maustaste anklicken und die Eigenschaften dieser Datei aufrufen. Wechseln Sie auf die Registerkarte *Kompatibilität*, und aktivieren Sie das Kontrollkästchen *Programm als ein Administrator ausführen*. Steht diese Option nicht zur Verfügung, benötigt dieses Programm zur Funktion keine administrativen Berechtigungen, oder Sie sind nicht als ein Administrator angemeldet und dürfen die Option nicht setzen. Einmalig können Sie diese Aufgabe auch über das Kontextmenü der Verknüpfung oder der Startdatei des Programms durchführen.

Abbildg. 14.3 Starten eines Programms im Administratormodus

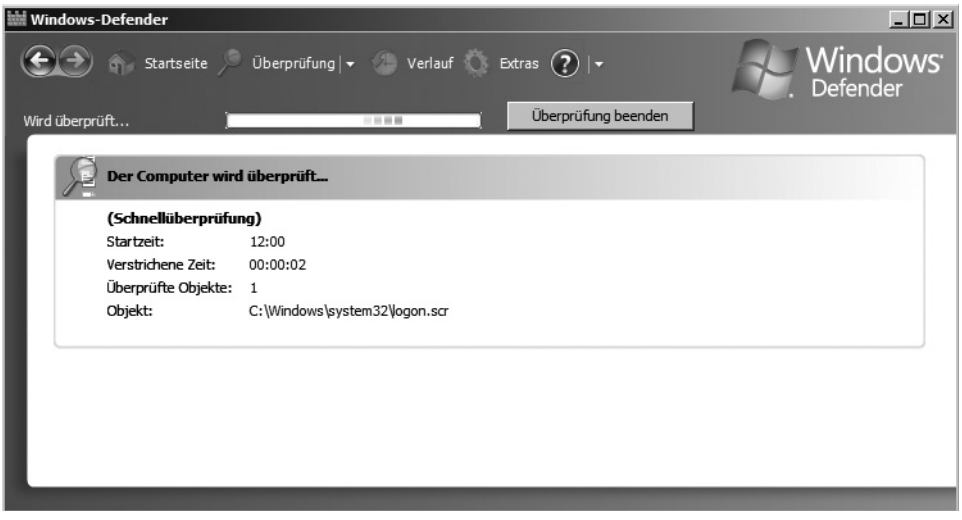


Windows-Defender

Der Spyware-Killer Windows-Defender von Microsoft gehört zum Standardinstallationsumfang von Windows Server 2008 und Windows Vista und kann das System auch im laufenden Betrieb überwachen sowie automatisch scannen. Damit der Defender aber unter Windows Server 2008 zur Verfügung steht, muss das Feature *Desktopdarstellung* installiert werden. Auch wenn Windows-Defender eine zusätzliche Möglichkeit darstellt, um Windows Server 2008 abzusichern, ersetzt das Programm keinesfalls einen Virenscanner. Nach dem Aufruf von Windows-Defender über das Startmenü oder der Systemsteuerung sehen Sie auf der Startseite, wann das System zuletzt gescannt wurde und wann die letzte Aktualisierung stattgefunden hat bzw. wie der Status von Windows-Defender derzeit ist. Auf der Startseite können keine Einstellungen vorgenommen werden. Haben Sie noch keine Definitionen heruntergeladen, erhalten Sie einen entsprechenden Warnhinweis und können über die Schaltfläche *Jetzt nach Updates suchen* aktuelle Definitionsdateien herunterladen. Klicken Sie oben im Fenster auf den Link *Überprüfung*, beginnt Windows-Defender die vorhandenen Festplatten mit einer vollständigen Überprüfung nach Schädlingen zu durchsuchen (Abbil-

dung 14.4). Dadurch können Sie durch wenige Mausklicks überprüfen, ob auf dem System Schädlinge erkannt wurden und diese entfernen. Während des Scanvorgangs können Sie in Windows-Defender keine weiteren Einstellungen vornehmen, da alle Schaltflächen blockiert sind.

Abbildg. 14.4 Überprüfen von Windows Server 2008 mit dem Windows-Defender



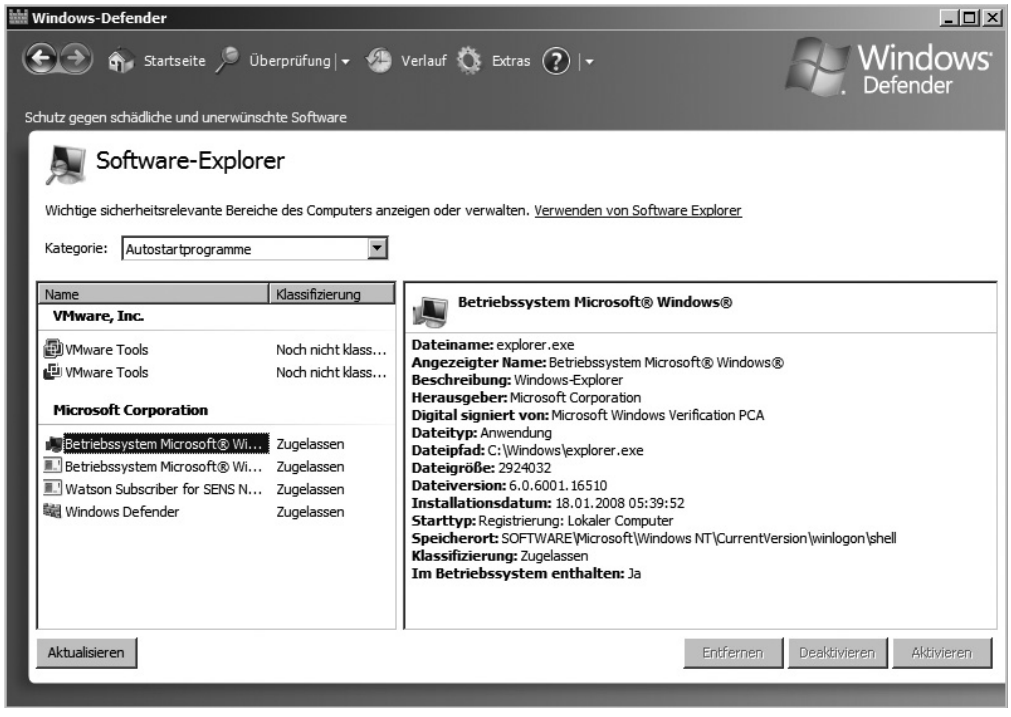
Wenn Sie auf das kleine Dreieck neben dem Link *Überprüfung* klicken, können Sie entweder eine vollständige Systemüberprüfung durchführen, die wesentlich sicherer ist, aber auch länger dauert, oder einen benutzerdefinierten Scanvorgang starten, bei dem Sie die Einstellungen selbst vornehmen können. Über den Link *Verlauf* können Sie sich die aktuellen Aktionen von Windows-Defender anzeigen lassen und welche Applikationen blockiert wurden. Sie sollten den Verlauf in regelmäßigen Abständen löschen, damit Sie den Überblick behalten, welche Anwendungen blockiert wurden und welche Schädlinge Windows-Defender erkannt hat.

Der Software-Explorer von Windows-Defender

Über den Link *Software-Explorer* im Fenster *Einstellungen und Extras*, das Sie über den Menüpunkt *Extras* nach dem Start von Windows-Defender erreichen, können mit dem Windows-Defender erstmalig in Windows mit Bordmitteln laufende Applikationen und Autostart-Programme an einer zentralen Stelle mit detaillierten Informationen angezeigt werden. Sie benötigen dazu kein Zusatzprogramm mehr. Wenn ein Server nicht mehr stabil läuft, liegt es höchstwahrscheinlich an irgendeinem Programm, das automatisch gestartet wird. Wenn Sie in den Software-Explorer wechseln, können Sie über das Listenfeld *Kategorie* detailliert auswählen, welche Applikationen angezeigt werden sollen, zum Beispiel die *Autostartprogramme* (Abbildung 14.5). Sie können das entsprechende Programm anklicken und sehen auf der rechten Seite detaillierte Informationen, unter anderem den Speicherort, also über welche Option das Programm automatisch gestartet wird. Die wenigsten Applikationen verwenden den Autostart-Ordner in Windows, sondern meist den Registrypfad *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* oder auch andere Stellen der Registry. Sie können störende Programme direkt vom Windows-Defender aus über den Software-Explorer aus diesem Registrierungsschlüssel löschen lassen oder manuell über *Start/Aus-*

führen/regedit. Neben den Autostartprogrammen können Sie hier auch die aktuell ausgeführten Programme, über das Netzwerk verbundene Programme und Winsock-Dienstanbieter anzeigen lassen. Winsock-Dienstanbieter sind Programme, die unter Windows laufen und auf eine Verbindung warten, da sie einen Dienst bereitstellen, zum Beispiel Bluetooth. Wenn ein Programm auf dem Server mit dem Netzwerk kommunizieren will, gibt es die Anforderung an den entsprechenden Winsock-Dienst weiter. Hier sollten nur geübte Benutzer Löschvorgänge ausführen oder Dienste deaktivieren.

Abbildg. 14.5 Überprüfen der Autostart-Programme in Windows-Defender



Windows-Firewall und IPSec

Die neue Windows-Firewall kann jeglichen eingehenden Netzwerkverkehr ablehnen, der nicht als Antwort auf eine Anfrage von Ihrem Computer eingeht oder für den keine Ausnahme konfiguriert wurde (unverlangt eingehender Netzwerkverkehr). Dies ist bei einer Firewall die wichtigste Funktion. Sie sorgt dafür, dass der Computer nicht durch Viren und Würmer infiziert wird. Die neue Windows-Firewall kann jedoch auch den ausgehenden Netzwerkverkehr überwachen. Ein Netzwerkadministrator kann zum Beispiel Ausnahmen konfigurieren, die alle an bestimmte Ports gesendeten Pakete blockieren. Standardmäßig blockiert die Firewall von Windows Server 2008 jeglichen eingehenden Netzwerkverkehr – es sei denn, er erfolgt aufgrund von Anfragen oder es wurde eine Ausnahme konfiguriert. Die meisten Serverrollen und Funktionen tragen ihre eigenen Ausnahmen automatisch ein. Die Regeln der Windows-Firewall wurden intelligenter gemacht. Es kann genau festgelegt werden, welche Komponenten und Dienste nach extern kommunizieren dürfen. Unter

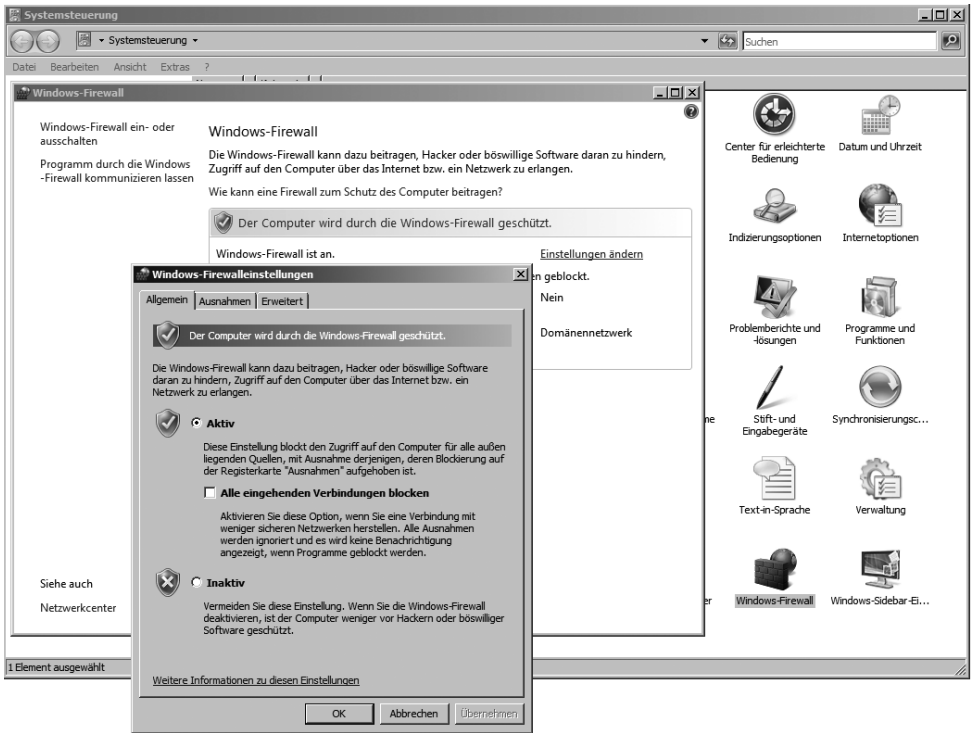
Windows Server 2008 können auch komplexe Regeln erstellt werden. Regeln können mit Authentifizierung arbeiten und die Verschlüsselung für bestimmte Kommunikationsarten vorschreiben. Regeln können auch auf Basis von Active Directory-Gruppen oder -Benutzer erstellt werden.

HINWEIS Die Firewall in Windows Server 2008 ist im Gegensatz zu Windows Server 2003 automatisch aktiviert.

Die Firewall lässt ausgehenden Netzwerkverkehr automatisch zu, solange darauf keine konfigurierte Ausnahme zutrifft. Zusammenfassend lässt sich festhalten, dass die neue Windows-Firewall in Windows Server 2008 gegenüber den Vorgängerversionen von Windows Server 2003 einige deutliche Weiterentwicklungen erfahren hat:

- Sie unterstützt eingehenden und ausgehenden Netzwerkverkehr. Die Firewall von Windows Server 2003 blockiert nur eingehenden Netzwerkverkehr.
- Es gibt ein neues Snap-In für die Microsoft Management Console (*wf.msc*).
- Es wurden Einstellungen für die Firewall-Filterung und für IPsec (Internet Protocol Security) integriert. Für die Steuerung der IP-Sicherheit wird daher kein zusätzliches Programm benötigt.
- Ausnahmen können jetzt für Active Directory-Konten und -Gruppen, für Quell- und Ziel-IP-Adressen, für IP-Protokollnummern, für Quell- und Ziel-TCP- und UDP-Ports, für alle oder bestimmte TCP- und UDP-Ports, für bestimmte Schnittstellen, für bestimmte Dienste und für ICMP- und ICMPv6-Netzwerkverkehr konfiguriert werden.

Abbildg. 14.6 Einfache Steuerung der Windows-Firewall in Windows Server 2008

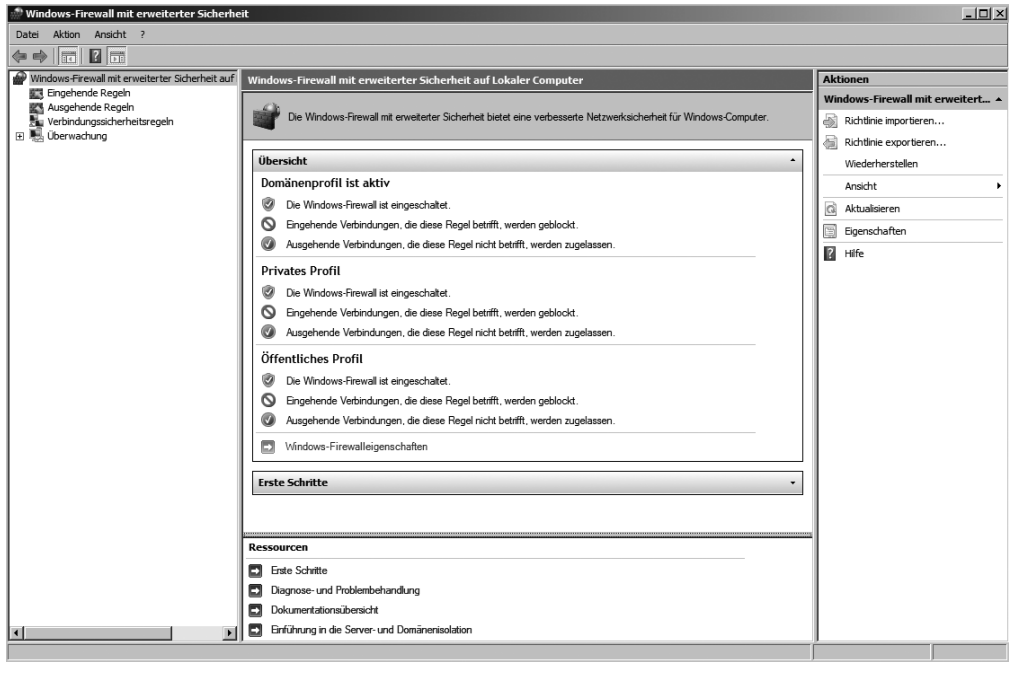


Die Standardkonfiguration der Windows-Firewall erreichen Sie über *Start/Systemsteuerung/Windows-Firewall* (Abbildung 14.6). Sie können die detaillierte Konfiguration der Firewall über die entsprechende Managementkonsole aufrufen (*wf.msc*). Nur an dieser Stelle können detailliert konfigurierte Regeln erstellt werden. Innerhalb dieser Konsole können neben den Einstellungen für die Firewall auch Funktionen im Bereich IPSec konfiguriert werden. Durch diese Kombination der beiden Technologien erhalten Unternehmen einige Vorteile:

- Die Konflikte und der Aufwand für die Koordination zwischen beiden Technologien werden verringert
- Die Firewallregeln werden intelligenter
- Integration in Active Directory (Benutzer- Computergruppen)
- Filterung des ausgehenden Datenverkehrs
- Konzipiert für den Einsatz in Unternehmensnetzwerken
- Vereinfachte Richtlinien für den Schutz des Systems reduzieren den Aufwand für die Verwaltung

Die Konsole starten Sie am schnellsten über *Start/Ausführen/wf.msc*. Auf der linken Seite können die entsprechenden Regeln zur Konfiguration ausgewählt werden. Hier gibt es folgende Möglichkeiten (Abbildung 14.7):

Abbildg. 14.7 Verwalten der Windows-Firewall mit dem MMC-Snap-In *Windows-Firewall mit erweiterter Sicherheit*



- **Eingehende Regeln** Hier werden die konfigurierten Ausnahmen für den eingehenden Netzwerkverkehr angezeigt

- **Ausgehende Regeln** Hier werden die konfigurierten Ausnahmen für den ausgehenden Netzwerkverkehr angezeigt
- **Verbindungssicherheitsregeln** Hier werden die Regeln für den geschützten Netzwerkverkehr angezeigt
- **Überwachung** Hier werden Informationen zu den aktuellen Ausnahmen, den Sicherheitsregeln der Verbindungen und den Sicherheitszuordnungen angezeigt. Innerhalb des Gruppenrichtlinien-Editors wird dieser Unterpunkt nicht angezeigt.

In der Mitte der Konsole wird eine Zusammenfassung des Status der Firewall angezeigt, sodass Administratoren einen schnellen Überblick erhalten. Die Firewall kann direkt über diese Konsole überwacht und die entsprechenden Protokolle angezeigt werden. Alle Regeln lassen sich effizient und einfach anzeigen. Bereits standardmäßig wird die Firewall mit einer Reihe von Regeln installiert und aktiviert. Die internen Betriebssystemdienste von Windows Server 2008 installieren automatisch ihre Regeln bei der Installation des Dienstes.

Konfiguration der Firewall mit der Konsole

Die Konfiguration der Windows Firewall setzt sich aus den folgenden Elementen zusammen:

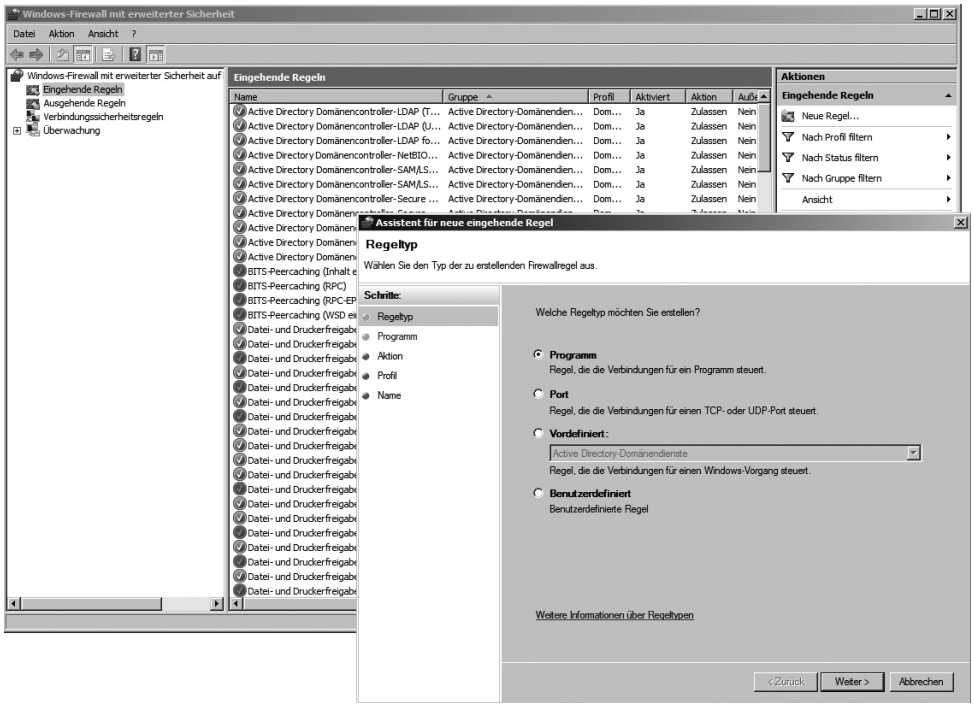
- Ausnahmen für eingehenden Netzwerkverkehr
- Ausnahmen für ausgehenden Netzwerkverkehr
- Sicherheitsregel
- Festlegen, für welches Profil die Regeln gelten (Domäne, öffentlich oder Privat)

Markieren Sie zunächst auf der linken Seite den Eintrag *Eingehende Regeln* oder den Eintrag *Ausgehende Regeln*. Klicken Sie anschließend mit der rechten Maustaste auf den jeweiligen Eintrag und wählen Sie im Kontextmenü den Befehl *Neue Regel* aus. Alternativ dazu können Sie auch den gewünschten Eintrag auf der linken Seite markieren und auf der rechten Seite des Fensters im Bereich Aktionen auf *Neue Regel* klicken. Es startet ein Assistent zum Erstellen von neuen Regeln (Abbildung 14.8).

Sie können über den Assistenten mehrere Bedingungen für die Regel festlegen. Folgende Konfigurationen lassen sich vornehmen:

- **Programm** Eine Ausnahme für eingehenden Netzwerkverkehr auf Basis eines Programmnamens. Sie müssen zusätzlich eine Aktion (zulassen, blockieren oder schützen), das Profil, auf das die Ausnahme angewendet wird (Standard, Domäne oder beide), und einen Namen für die Ausnahme angeben.
- **Port** Eine Ausnahme auf Basis von TCP- oder UDP-Ports. Auch hier müssen Sie zusätzlich eine Aktion (zulassen, blockieren oder schützen), das Profil, auf das die Ausnahme angewendet wird (Standard, Domäne oder beide), und einen Namen für die Ausnahme angeben.
- **Vordefiniert** Eine Ausnahme für einen vordefinierten Dienst. Hierzu gehören zum Beispiel Remoteunterstützung, Datei- und Druckerfreigabe, Remotedesktop, Universal Plug and Play (UPnP) Framework und ICMP-Echo-Requests (v4). Auch hier muss ein Name für die Ausnahme festgelegt werden.
- **Benutzerdefiniert** Eine Ausnahme, die sich nicht auf ein Programm, einen Port oder einen vordefinierten Dienst bezieht. Mit dieser Option können Sie alle Konfigurationseinstellungen selbst festlegen. Auch hier müssen Sie wieder einen Namen angeben.

Abbildg. 14.8 Erstellen einer neuen Firewallregel

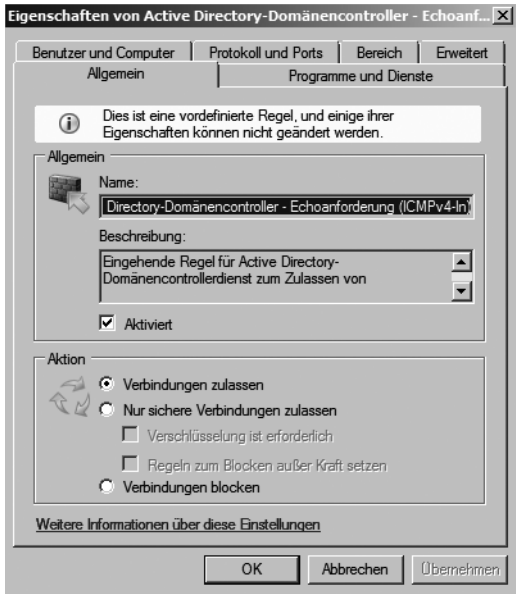


Nachdem Sie den Assistenten abgeschlossen haben, wird eine neue Regel im Detailbereich angezeigt. Wenn Sie die erweiterten Eigenschaften der Regel konfigurieren möchten, klicken Sie mit der rechten Maustaste auf die Regel und wählen anschließend im Kontextmenü den Eintrag *Eigenschaften* aus (Abbildung 14.9).

Hier gibt es mehrere Registerkarten:

- **Allgemein** Name der Regel, Programm, auf das sich die Ausnahme bezieht, und Aktion (zulassen, blocken oder nur sichere Verbindungen zulassen)
- **Benutzer und Computer** Wenn als Aktion *Nur sichere Verbindungen zulassen* definiert ist, werden hier die Computer- oder Benutzerkonten angezeigt, die geschützte Verbindungen aufbauen dürfen
- **Protokolle und Ports** IP-Protokoll, TPC- und UDP-Quellport und -Zielport sowie ICMP- oder ICMPv6-Einstellungen
- **Bereich** Quell- und Zieladressen für die Ausnahme
- **Erweitert** Profile, Schnittstellentypen und Dienste, für welche die Ausnahme gilt
- **Programme und Dienste** Hier können Sie definieren, welches Programm oder welcher Dienst mit der Regel verwaltet wird

Abbildg. 14.9 Verwalten einer Firewallregel



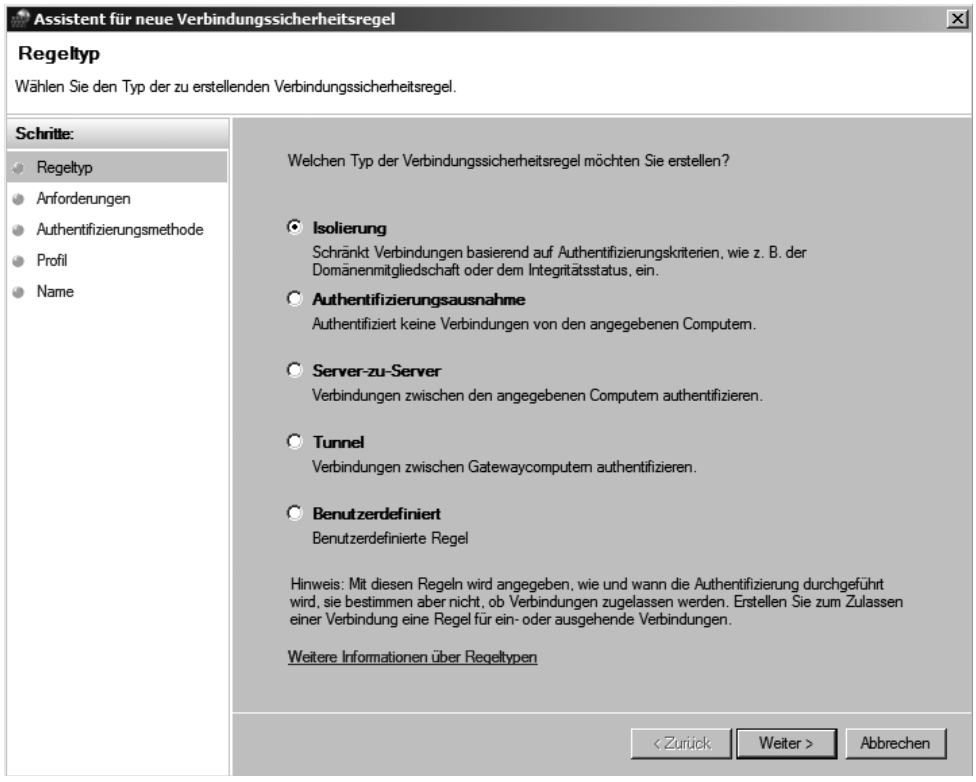
Konfigurieren von Verbindungssicherheitsregeln in der Konsole

Klicken Sie auf der linken Seite der MMC mit der rechten Maustaste auf *Verbindungssicherheitsregeln* und wählen Sie im Kontextmenü den Eintrag *Neue Regel* aus. Es startet ein Assistent zum Erstellen von neuen Regeln (Abbildung 14.10). Sie können über den Assistenten mehrere Bedingungen für die Regel festlegen.

Folgende Konfigurationen lassen sich vornehmen:

- **Isolierung** Legt anhand der Active Directory-Infrastruktur oder über den Status von Computern fest, welche Computer isoliert sind. Sie müssen angeben, wann eine Authentifizierung stattfinden soll (zum Beispiel bei eingehendem oder ausgehendem Netzwerkverkehr) und ob die Verbindung geschützt sein muss oder ob dies nur angefordert wird. Außerdem müssen Sie die Authentifizierungsmethode und einen Namen für die Regel festlegen. Die Isolation über den Status eines Computers nutzt die neue Network Access Protection-Plattform von Windows Server 2008 und Windows Vista. Auf diesem Weg kann der Zugriff auf sensible Server schon auf IP-Ebene kontrolliert und abgesichert werden.
- **Authentifizierungsausnahme** Legt anhand Ihrer IP-Adresse die Computer fest, die sich nicht authentifizieren müssen oder keine geschützte Verbindung benötigen
- **Server zu Server** Legt fest, wie die Verbindung zwischen Computern geschützt wird. Sie müssen Endpunkte (IP-Adressen) festlegen und angeben, wann die Authentifizierung stattfinden soll. Außerdem müssen die Authentifizierungsmethode und ein Name für die Regel festgelegt werden.

Abbildg. 14.10 Erstellen einer Verbindungssicherheitsregel mit der neuen Windows-Firewall



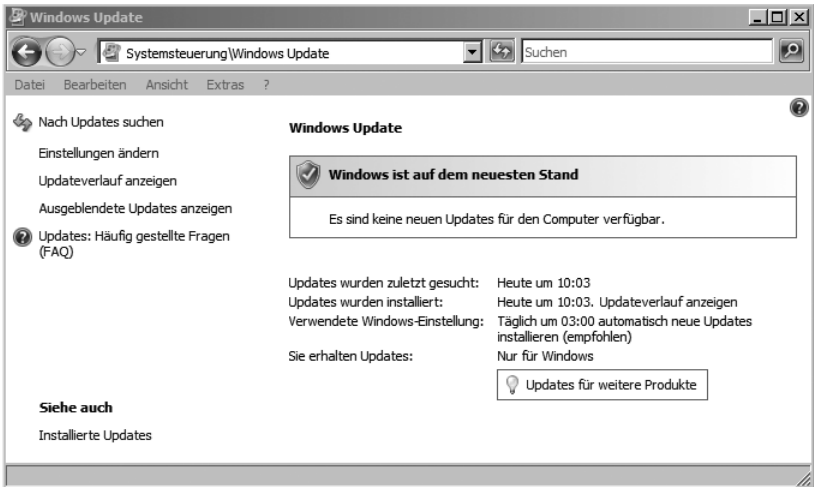
- **Tunnel** Legt eine durch einen Tunnel geschützte Verbindung fest (zum Beispiel bei Verbindungen über das Internet). Sie müssen die Tunnel-Endpunkte über deren IP-Adressen angeben; außerdem natürlich die Authentifizierungsmethode und einen Namen für die Regel.
- **Benutzerdefiniert** Erstellt eine frei konfigurierbare Regel

Wenn Sie die erweiterten Eigenschaften der Regel konfigurieren möchten, klicken Sie mit der rechten Maustaste auf die Regel und wählen dann im Kontextmenü den Eintrag *Eigenschaften* aus. Hier gibt es wieder mehrere Registerkarten. Erstellen Sie eine Ausnahme oder öffnen einen Port in der Firewall, erlauben Sie einem bestimmten Programm, Daten über die Firewall von oder zu Ihrem Computer zu senden. Wenn Sie einem Programm die Kommunikation über die Firewall erlauben (wenn Sie seine Blockierung aufheben), öffnen Sie dadurch förmlich eine winzige Tür in der Firewall. Jedes Mal, wenn Sie eine Ausnahme zulassen oder einen Port öffnen, damit ein Programm über die Firewall kommunizieren kann, wird Ihr Computer etwas weniger sicher. Je mehr Ausnahmen oder offene Ports Ihre Firewall hat, umso mehr Gelegenheiten haben Hacker und schädliche Software, eine dieser Öffnungen zu verwenden, um einen Wurm zu verbreiten, auf Ihre Dateien zuzugreifen oder mithilfe Ihres Computers schädliche Software an andere zu verteilen. Erstellen Sie Ausnahmen und öffnen Sie Ports nur dann, wenn Sie sie wirklich benötigen. Wenn sie nicht mehr erforderlich sind, sollten Sie Ausnahmen entfernen und Ports schließen. Erstellen Sie keine Ausnahmen und öffnen Sie keinen Port für ein Programm, das Sie nicht erkennen.

Automatische Windows-Updates

Die Funktion der automatischen Aktualisierung wurde bereits in Windows Server 2003 eingeführt, aber in Windows Server 2008 weiter verbessert. Auch versierten Administratoren ist es heutzutage nicht mehr zumutbar, ständig nach Produktupdates zu schauen und diese zu installieren. Die Konfiguration der automatischen Updates kann in der Systemsteuerung über *Windows Update* durchgeführt werden. Hier steht ein eigenes Menü zur Verfügung, mit dessen Hilfe die installierten Updates angezeigt werden können, manuell nach neuen Updates gesucht werden kann und die Konfiguration dieser Funktion angepasst werden kann (Abbildung 14.11). Zusätzlich besteht die Möglichkeit, nicht nur Windows aktuell zu halten, sondern auch andere Produkte, die auf dem Server installiert sind und Windows Update unterstützen. Um die Aktualisierung für weitere Microsoft-Produkte zu aktivieren, gibt es im Konfigurationsfenster von Windows Updates den Link *Updates für weitere Produkte*, über den zusätzliche Produkte eingebunden werden können. Microsoft hat dazu seinen Internetdienst Windows Updates an die neue Version 6 angepasst, mit der auch Aktualisierungen von anderen Produkten möglich werden. Nachdem Sie die Funktion einmalig aktiviert haben, wird der Server zukünftig auch automatisch mit Updates versorgt. Besser ist in diesem Fall natürlich die Anbindung an einen WSUS 3.0 (siehe Kapitel 23). Auf der linken Seite des Fensters können Sie weitere Informationen abrufen und die Einstellungen für automatische Updates anpassen. Hier können auch die bereits installierten Updates angezeigt oder ausgeblendete Updates überprüft werden.

Abbildg. 14.11 Verwalten der Windows Update-Funktion unter Windows Server 2008

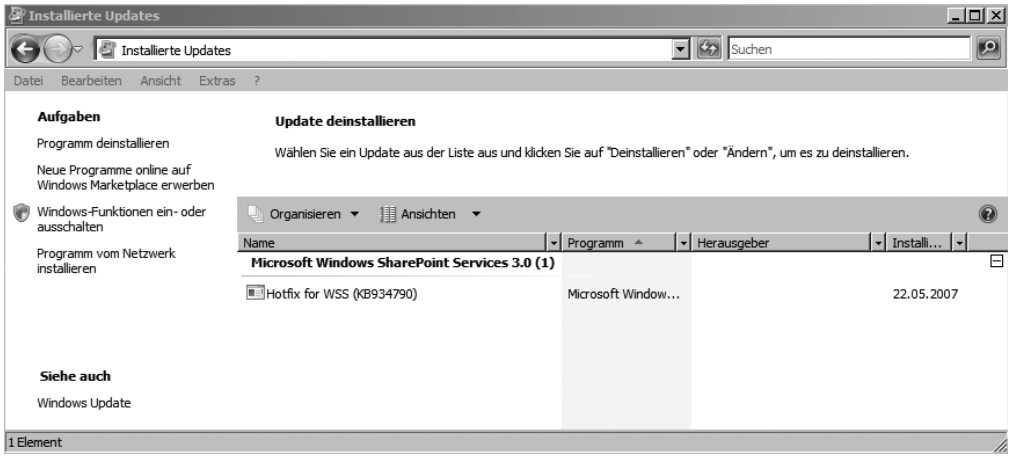


- Wenn Sie auf den Link *Nach Updates suchen* klicken, überprüft Windows Server 2008, ob aktuell Updates im Internet verfügbar sind.
- Über den Link *Updateverlauf anzeigen* im Update-Fenster oder auf der linken Seite des Fensters können Sie sich anzeigen lassen, welche Updates heruntergeladen und installiert worden sind.
- Über den Link *Einstellungen ändern* öffnet sich ein Konfigurationsfenster, in dem Sie einstellen können, wie und wann Updates installiert werden sollen. Grundsätzlich können Sie hier zunächst konfigurieren, ob Windows Server 2008 automatisch aktualisiert werden soll oder ob Sie die automatische Aktualisierung komplett deaktivieren möchten. Diese Einstellungen können auch über Gruppenrichtlinien vorgenommen werden (siehe die Kapitel 9 und 23).

Wenn Sie Windows Server 2008 so konfigurieren, dass die Aktualisierung automatisch erfolgen soll, können Sie eine Uhrzeit einstellen, zu welcher die Aktualisierung durchgeführt wird. Wenn der Server zu diesem Zeitpunkt keine Internetverbindung herstellen kann oder nicht gestartet ist, wird der Aktualisierungsvorgang automatisch im Hintergrund beim nächsten Start durchgeführt. Hier können Sie auch festlegen, ob die Updates automatisch installiert werden sollen oder ob Sie die Installation manuell bestätigen wollen. Um sich viel Arbeit mit den Windows-Updates zu ersparen, sollten Sie die automatische Aktualisierung aktivieren.

Über den Link *Installierte Updates* links unten im Hauptfenster von Windows Update können Sie sich alle installierten Updates auf dem Server anzeigen lassen und bei Bedarf einzelne Updates deinstallieren. Hier können Sie auch sehen, wann diese Updates eingespielt worden sind (Abbildung 14.12). Sie finden diese Informationen auch über *Start/Systemsteuerung/Programme und Funktionen/Installierte Updates anzeigen* einsehen.

Abbildg. 14.12 Anzeigen von installierten Updates unter Windows Server 2008



Über den Link *Ausgeblendete Updates anzeigen* können Sie sich die Patches anzeigen lassen, die nicht in den installierten Updates angezeigt, sondern von Windows Server 2008 automatisch ausgeblendet werden.

TIPP Sie können sich die installierten Patches in der Befehlszeile mit dem Befehl *wmic qfe* anzeigen lassen. Idealerweise lassen Sie die Ausgabe des Befehls durch Eingabe von *wmic qfe >c:\patches.txt* in eine Textdatei umleiten, die Sie nach der Erstellung besser lesen können als die Auflistung in der Befehlszeile. Vor allem auf Core-Server ist dieser Befehl nützlich.

Verwalten von Patches auf Core-Server

Auf Core-Servern steht Ihnen die grafische Oberfläche zur Verwaltung von Windows-Updates nicht zur Verfügung. Hier müssen Sie alle Einstellungen über die Befehlszeile vorgeben oder als Gruppenrichtlinie steuern. Hauptsächlich verwenden Sie für die Verwaltung von Updates in der Befehlszeile die folgenden Befehle:

Installation eines Updates

Wusa <Update>.msu /quiet

Deinstallieren eines Updates

Wollen Sie ein installiertes Update deinstallieren, gehen Sie folgendermaßen vor:

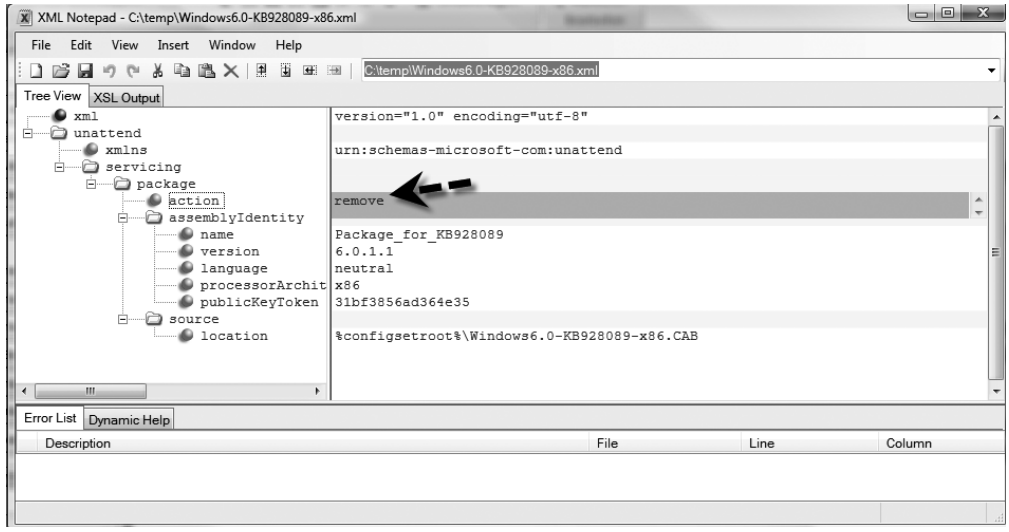
1. Kopieren Sie die Installationsdatei des Updates auf den Core-Server.
2. Geben Sie den Befehl *Expand /f:* <update>.msu c:\temp* ein, um das Archiv zu entpacken. Diesen Vorgang können Sie auch auf einer normalen Arbeitsstation durchführen.
3. Öffnen Sie in diesem Verzeichnis die **.xml*-Datei des Patches mit einem Editor oder XML Notepad 2007.
4. Ersetzen Sie den Befehl *Install* mit *Remove* und speichern Sie die Datei.
5. Geben Sie als Nächstes den Befehl *Pkgmgr /n:<Update>.xml* ein. Dazu müssen Sie aber den bearbeiteten Patch wieder auf den Core-Server kopieren und den Befehl lokal ausführen.

HINWEIS Mit dem kostenlosen *XML Notepad 2007* von Microsoft können XML-Dokumente durchsucht und editiert werden. XML (Extensible Markup Language) ist der übergeordnete Standard aller Web-Autoren-Sprachen. Dabei unterstützt Sie die Freeware bei der Eingabe der Daten und hilft Fehler zu vermeiden. XML-Dokumente werden in einer Baumstruktur dargestellt. Um das XML Notepad 2007 nutzen zu können, muss .NET Framework auf Ihrem Rechner installiert sein. Sie können das Tool von der Internetseite *http://www.microsoft.com/downloads/details.aspx?FamilyID=72D6AA49-787D-4118-BA5F-4F30FE913628&displaylang=en* herunterladen. Das Tool bietet in der neuen Version einige Vorteile:

- Inkrementelle Suche (Strg + I) in der Struktur- und der Textansicht, damit Sie während der Eingabe zu dem am besten passenden Knoten navigieren können
- Ausschneiden/Kopieren/Einfügen mit vollständiger Namespace-Unterstützung in einem einfachen, interoperablen XML-Format
- Drag & Drop-Unterstützung für die einfache Manipulation der Struktur auch über verschiedene Instanzen von XML-Notepad hinweg und aus dem Dateisystem heraus
- Unbegrenztes Rückgängig/Wiederholen für alle Bearbeitungsfunktionen
- Mehrzeilige Vor-Ort- und Popup-Bearbeitung großer Textknotenwerte basierend auf erwarteten Elementen und Attributen
- Konfigurierbare Schriftarten und Farben mithilfe des Optionsdialogfelds
- Umfassendes Dialogfeld *Suchen/Ersetzen* mit Unterstützung für RegEx- und XPath-Ausdrücke
- Gute Leistung bei großen XML-Dokumenten (ein Dokument mit 3 MB wird in ungefähr einer Sekunde geladen)
- Sofortige Validierung des XML-Schemas während der Bearbeitung, wobei Fehler und Warnungen im Aufgabenlistenfenster angezeigt werden
- Unterstützung benutzerdefinierter Editoren für die Datentypen *Datum*, *DatumZeit*, *Uhrzeit* und *Farbe*
- HTML-Anzeige für die Anzeige von XSLT-Transformationsergebnissen
- Integriertes XML-Vergleichs-Tool

Ausführliche Anleitungen für das Tool finden Sie auf der Internetseite *http://www.microsoft.com/germany/msdn/library/data/xml/DesignvonXMLNotepad2006.mspx?mfr=true*.

Abbildg. 14.13 Bearbeiten von XML-Dateien mit XML Notepad 2007



Konfigurieren der Windows Update-Funktion

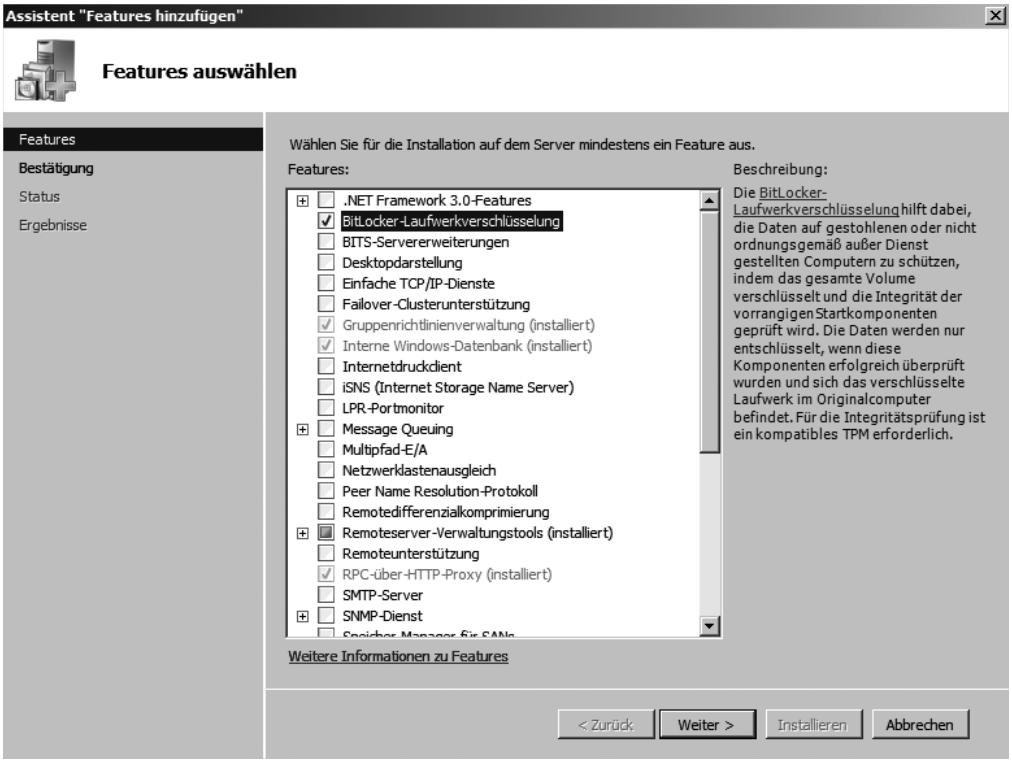
Die Konfiguration der Windows Update-Funktion auf einem Core-Server nehmen Sie mit dem Tool *scregedit.wsf* aus dem Verzeichnis *\Windows\System32* vor (siehe Kapitel 3). Ihnen stehen hierzu verschiedene Möglichkeiten zur Verfügung:

- **Überprüfen der aktuellen Einstellungen für Windows Update** Cscript scregedit.wsf /AU /v
- **Aktivieren der automatischen Update-Funktion** Cscript scregedit.wsf /AU 4
- **Deaktivieren der automatischen Update-Funktion** Cscript scregedit.wsf /AU 1

BitLocker – Laufwerksverschlüsselung

In Kapitel 3 wurde bereits auf die BitLocker-Laufwerksverschlüsselung eingegangen. Diese muss als Feature nachträglich über den Server-Manager installiert werden. BitLocker dient der kompletten Verschlüsselung von Partitionen. Die Funktion wird durch die Installation nur zugänglich gemacht, noch nicht aktiviert. Die Aktivierung von BitLocker ist ein längerer Prozess, den wir in diesem Abschnitt ausführlich besprechen. Die Hauptaufgabe von BitLocker ist das Verhindern, dass Daten im Unternehmen gestohlen werden. Selbst wenn ein Server gestohlen wird, zum Beispiel in einer kleineren Niederlassung, kann auf die Daten des Servers nicht zugegriffen werden, da diese zuverlässig verschlüsselt werden.

Abbildg. 14.14 Installieren von BitLocker unter Windows Server 2008



HINWEIS In Windows Vista ohne SP1 kann nur die Systempartition mit BitLocker verschlüsselt werden. Bei Windows Vista mit SP1 und Windows Server 2008 lassen sich alle Partitionen des Computers mit BitLocker verschlüsseln. In der Verwaltungskonsole von BitLocker werden alle Partitionen des Computers zur Verschlüsselung angezeigt.

Voraussetzungen für BitLocker

Damit BitLocker verwendet werden kann, sollte Ihr Server über einige Voraussetzungen verfügen:

- TPM-Chip (Trusted Platform Module, siehe auch *http://de.wikipedia.org/wiki/Trusted_Platform_Module*) der Spezifikation 1.2 sollte verbaut sein, muss es aber nicht
- TCG 1.2 (Trusted Computing Group, siehe auch *http://de.wikipedia.org/wiki/Trusted_Computing_Group*)-konformes BIOS ist hilfreich, aber nicht unbedingt notwendig
- USB-Support durch das BIOS in der Pre-Boot-Phase
- Eine unverschlüsselte Boot-Partition, die größer als 50 MB sein muss. Diese Partition wird durch das BIOS für den Windows-Ladevorgang benötigt.
- Einen USB-Stick für das Speichern des Wiederherstellungsschlüssels

- Auf dem Server müssen mindestens zwei Partitionen angelegt sein (es reichen auch verschiedene Partitionen auf einer physischen Festplatte, die Partitionen müssen nicht auf verschiedene physische Festplatten aufgeteilt sein). Eine Partition ist für das Betriebssystem vorbehalten (in der Regel Laufwerk C:) und wird von BitLocker verschlüsselt, während die andere Partition die aktive Partition ist, die unverschlüsselt bleiben muss, damit der Computer gestartet werden kann. Die Größe der aktiven Partition muss mindestens 50 GB betragen, besser etwas mehr

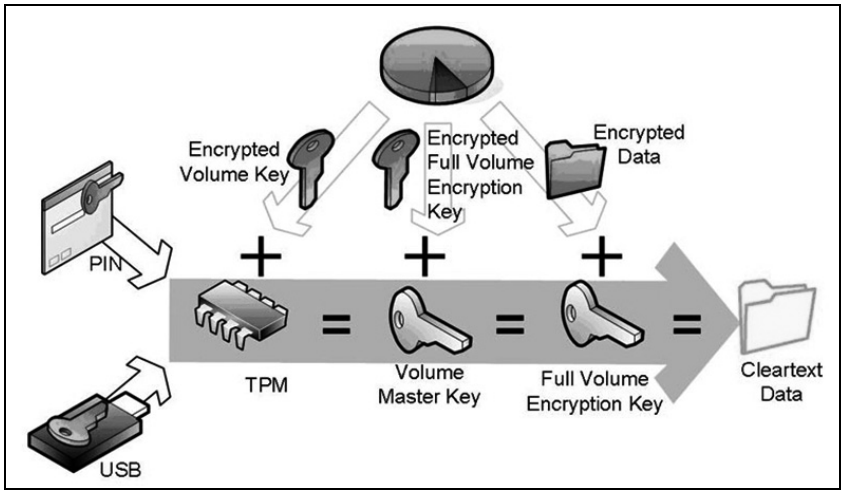
Damit BitLocker genutzt werden kann, muss die Festplattenkonfiguration stimmen. BitLocker benötigt eine unverschlüsselte Startpartition sinnvoller Weise ab 100 MB Größe, die am Anfang der Festplatte liegen sollte, damit das BIOS booten kann. Diese Partition muss in der Partitionstabelle als aktiv gekennzeichnet sein. Auf dieser Partition muss die Bootkonfigurationsdatenbank von Windows Server 2008 liegen sowie der eigentliche Bootmanager. Der Bootvorgang läuft dann so ab, dass zuerst diese Partition gestartet wird, der TPM entsperrt und der Schlüssel zum Entschlüsseln der Windows Server 2008-Partition gelesen wird. Danach startet Windows Server 2008 ganz normal. Die Entschlüsselung findet im laufenden Betrieb ab, wobei optimierte Verfahren dafür sorgen, dass hier kein signifikanter Performanceverlust eintritt. Die Windows Server 2008-Partition selbst bleibt die ganze Zeit über verschlüsselt.

Die Funktionsweise von BitLocker

BitLocker lässt sich abhängig von der Ausstattung des Servers und dem Sicherheitsbedürfnis des Unternehmens in fünf verschiedenen Versionen betreiben:

1. **Server ohne TPM-Chip** Wenn im Server kein TPM-Chip integriert ist, wird für die Entschlüsselung der Daten ein Schlüssel auf einem USB-Stick gespeichert. Dieser muss mit dem Server verbunden sein, damit BitLocker booten kann. Der USB-Stick funktioniert sozusagen als Dongle, darf aber nicht verloren gehen. Es können ganz normale USB-Sticks verwendet werden, die auch als Speicher verwendet werden. Nach dem Start des Servers kann der Schlüssel entfernt werden. Wird der Computer gestohlen, kann der Dieb den Server nicht starten und auch nicht auf die verschlüsselten Daten zugreifen.
2. **Server mit TPM-Chip** Hier werden die Daten mit der im TPM-Chip gespeicherten Prüfsumme entschlüsselt. Der Zugriff auf die Daten des Servers kann auch hier nur lokal erfolgen.
3. **TPM und PIN** Zusätzlich muss bei jedem Neustart des Servers eine vier- bis 20-stellige PIN eingetragen werden.
4. **TPM und Startschlüssel** Statt der PIN wird der Startschlüssel von einem USB-Stick bezogen, der mit dem Server bei jedem Startvorgang verbunden sein muss.
5. **Recovery-Schlüssel** Diese Funktion wird benötigt, wenn nach einem Angriff oder dem Einbau der Festplatte in ein neues Gerät weiterhin auf die Daten zugegriffen werden soll. Dieser kann als PIN eingegeben oder von einem USB-Stick gelesen werden.

Abbildg. 14.15 Funktionsweise von BitLocker



BitLocker mit TPM schützt den Computer, ohne dass der Benutzer etwas davon merkt. Das Entsperren des TPM, das Auslesen des Schlüssels und die Entschlüsselung gehen vollständig transparent ohne Benutzerinteraktion vonstatten. Solange ein Angreifer nicht die Anmeldedaten des Anwenders hat, kann er nicht auf die Daten zugreifen. Die zusätzlichen Sicherungsoptionen einer PIN-Eingabe beim Start oder die Nutzung eines zusätzlichen USB-Sticks als Securitytoken erhöhen den Schutz noch, haben aber auch einen Einfluss auf die Benutzbarkeit, da hier eine Aktion des Benutzers erforderlich ist. Beim Booten überprüft BitLocker den Hashwert im TPM, bevor der Server gestartet werden kann. Dadurch ist auch sichergestellt, dass Bootsektorviren oder Rootkits nicht einfach den Schutz aushebeln können. Da sich der Hashwert ändert, wenn eine maßgebliche Komponente des Server ausgetauscht wird, zum Beispiel die Hauptplatine, oder die Platte in einen anderen Server eingebaut wird, verweigert BitLocker den Zugriff auf den Datenträger. Erst wenn die Integrität sichergestellt ist, lässt BitLocker den Zugriff zu. Die Integritätsprüfung von BitLocker umfasst folgende Komponenten:

- BIOS
- Master Boot Record (MBR)
- Boot-Manager
- NTFS-Boot-Sektor
- NTFS-Boot-Block
- Core Root of Trust of Measurement (CRTM)

Die Verschlüsselung erfolgt sektorbasiert. Die Basis der BitLocker-Verschlüsselung stellt der Full Volume Encryption Key (FVEK) dar, der die Daten direkt auf der Festplatte verschlüsselt. BitLocker unterstützt derzeit Schlüssel mit 128 bis 512 Bit. Die Standardverschlüsselung verwendet einen 128-Bit-AES-Algorithmus. Um auch nach der Deaktivierung von BitLocker auf verschlüsselte Daten auf der Platte zugreifen zu können, existiert ein so genannter Clear Key. Dieser wird unverschlüsselt auf der Platte gespeichert und nutzt den Full Volume Encryption Key (FVEK), um trotz deaktiviertem BitLocker auf verschlüsselte Daten zuzugreifen. Auf den Clear Key kann nur zugegriffen werden, wenn BitLocker deaktiviert wurde. Nachdem BitLocker aktiviert ist, besteht kein Zugriff mehr auf

den Clear Key. Die beste Sicherheit erreichen Sie, indem Sie TPM 1.2 mit einem TCG-konformen BIOS und einem Startup-Key einsetzen. Ein Startup-Key stellt einen zusätzlichen Authentifizierungsfaktor dar, da entweder ein physischer Schlüssel (ein USB-Gerät) oder ein PIN erforderlich ist.

ACHTUNG Achten Sie bei der Verwendung von BitLocker darauf, dass die Aktualisierung des BIOS mit aktiviertem TPM erst dann erfolgen sollte, wenn BitLocker deaktiviert wird. Nach der Aktualisierung des BIOS kann BitLocker wieder aktiviert werden.

Einrichtung von BitLocker auf einem neuen Server

Damit Sie die BitLocker-Laufwerksverschlüsselung verwenden können, sollten Sie vor der Installation von Windows Server 2008 die Partitionen des Servers vorbereiten.

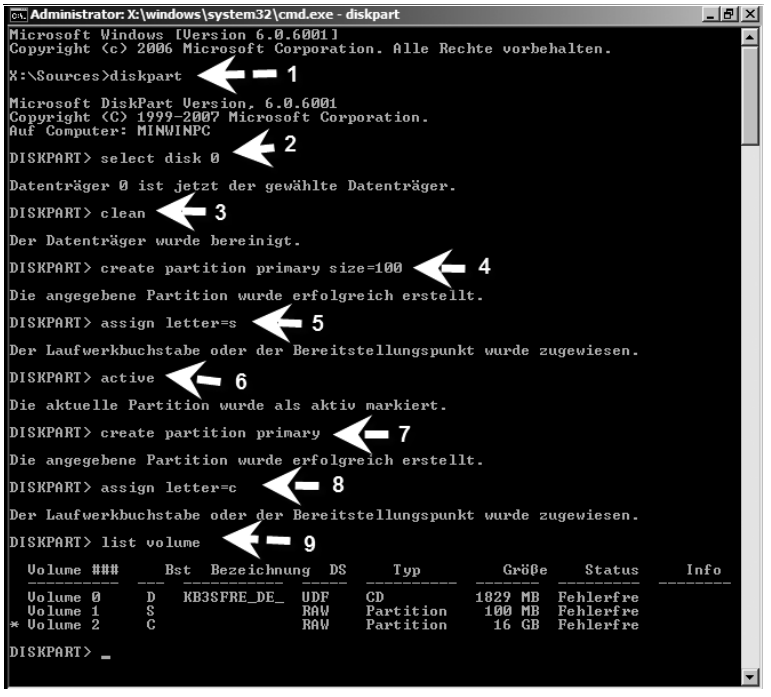
HINWEIS Damit BitLocker verwendet werden kann, wird die erste physische Festplatte in zwei Partitionen unterteilt. Microsoft unterscheidet hier in *Bootpartition* und eine *Windows-Partition*. Die *Bootpartition* wird auch als *Systempartition* bezeichnet, die *Windows-Partition* als *Startpartition*. Von der kleineren *Systempartition*, die auch als *aktive Partition* konfiguriert ist, wird gebootet, die Daten liegen auf der Windows-Partition. Die notwendige Partitionierung kann vor der Installation von Windows Server 2008 durchgeführt werden, aber auch nachträglich, wie wir in diesem Kapitel noch zeigen werden. Für eine Testumgebung reicht es die Systempartition für BitLocker 100 MB groß zu konfigurieren. Bei produktiven Maschinen empfiehlt Microsoft eine Größe von 1,5 GB für die Systempartition.

Gehen Sie zur Neueinrichtung folgendermaßen vor:

1. Booten Sie zunächst mit der Windows Server 2008-DVD.
2. Starten Sie die *Computerreparaturoptionen*, und gehen Sie in den *Systemwiederherstellungsoptionen* in die *Eingabeaufforderung*. Bestätigen Sie zuvor das Fenster zum Laden des Datenträgers. Wenn in Windows Server 2008 kein passender Treiber für den Datenträger integriert ist, können Sie diesen zuvor über die Schaltfläche *Treiber laden* integrieren lassen. Auf dem Server sollte möglichst noch kein Betriebssystem installiert sein. Wenn auf der Festplatte, die für BitLocker eingerichtet wird, ein Betriebssystem installiert ist, muss dieses neu installiert werden und Sie sollten vorher alle Daten sichern, da nach der hier durchgeführten Einrichtung das Betriebssystem entfernt wird.
3. Als Nächstes müssen Sie mit dem Befehl *diskpart* die Partition für BitLocker vorbereiten. Geben Sie dazu die Befehle in der Reihenfolge ein, wie in den nächsten Punkten beschrieben, und bestätigen Sie jeden Befehl mit der ↵-Taste (Abbildung 14.16). Bei dieser Einrichtung wird für eine Testumgebung eine neue Systempartition erstellt.

```
Diskpart
Select disk 0
Clean
Create partition primary size=100
Assign letter=S
Active
Create partition primary
Assign letter=C
List volume
Exit
```

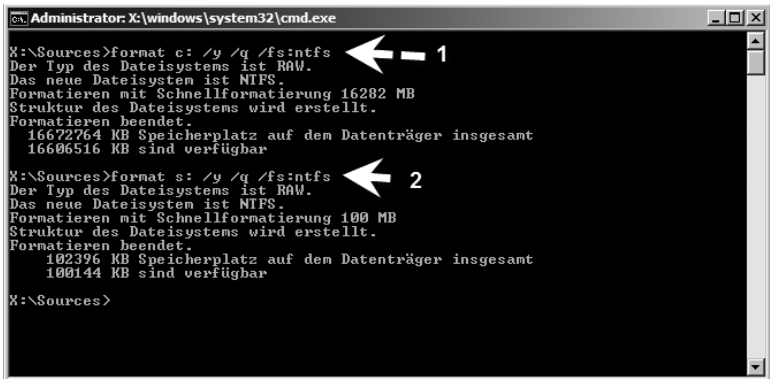
Abbildg. 14.16 Zur Einrichtung von BitLocker sollte der Server vor der Installation von Windows Server 2008 vorbereitet werden



4. Anschließend müssen die Partitionen noch formatiert werden. Geben Sie dazu die Befehle ein wie nachfolgend beschrieben.

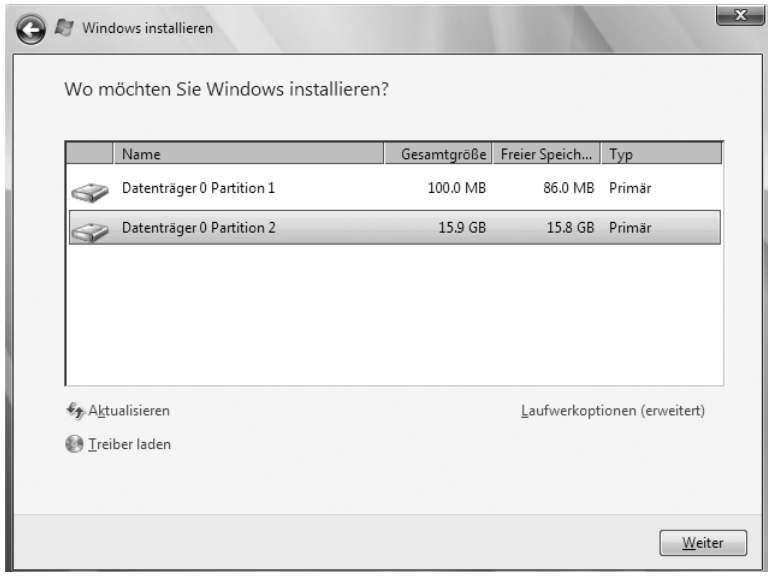
```
Format c: /y /q /fs:ntfs
Format s: /y /q /fs:ntfs
Exit
```

Abbildg. 14.17 Nach der Einrichtung der Partitionen müssen diese noch formatiert werden, bevor Windows Server 2008 installiert wird



5. Installieren Sie im Anschluss ganz normal auf Partition C Windows Server 2008. Klicken Sie dazu in den *Computerreparaturoptionen* auf *Neu starten* und booten Sie von der Windows Server 2008-DVD. Installieren Sie Windows Server 2008 auf Partition C. Dazu wird im Installationsfenster die größere Partition ausgewählt. Die kleinere Partition wird im Installationsfenster als Erste vorgeschlagen, da diese als aktiv markiert wurde, also der Bootmanager während der Installation auf dieser Partition abgelegt wird. Die verschlüsselten Systemdateien liegen auf der zweiten, größeren Partition.

Abbildg. 14.18 Nach der Einrichtung der Partitionen kann Windows Server 2008 installiert werden



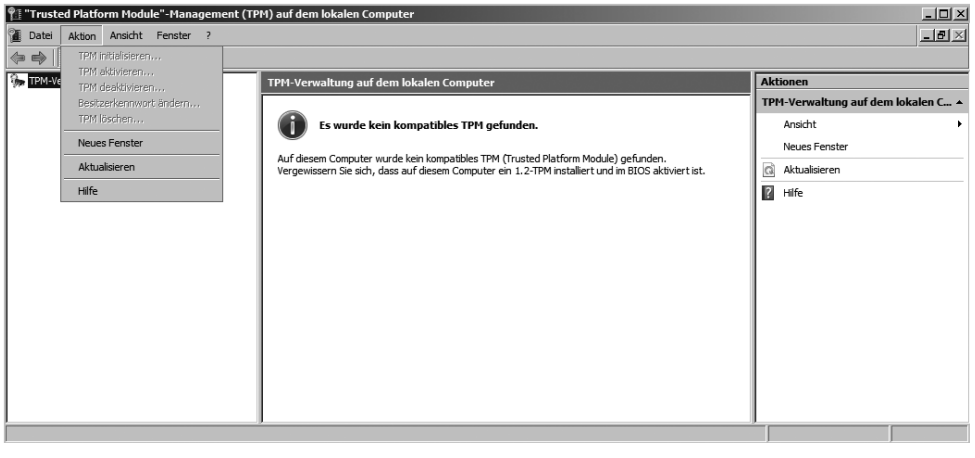
6. Wenn Sie ein kompatibles BIOS einsetzen, das auch einen TPM-Chipsatz hat, müssen Sie diesen nach der Installation aktivieren. Achten Sie bei der Bootreihenfolge darauf, dass von der Windows Server 2008-DVD gebootet wird, nicht von einer der neu erstellten und noch leeren Partitionen.
7. Aktivieren Sie danach in der Systemsteuerung *BitLocker*. Diesen Bereich zeigen wir Ihnen im nächsten Abschnitt. Verfügt der Computer über einen TPM-Chip und haben Sie diesen im BIOS aktiviert, muss dieser nach der Installation zunächst initialisiert werden. Diesen Vorgang zeigen wir Ihnen als Nächstes. Verfügt der Computer über keinen TPM-Chip, können diese Schritte übersprungen werden. In diesem Fall werden die notwendigen Daten direkt auf einem USB-Stick gespeichert.

Aktivieren und initialisieren von TPM in Windows Server 2008

Um das TPM auf Ihrem Server zu initialisieren, müssen Sie es einschalten und anschließend die TPM-Besitzrechte festlegen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie über *Start/Ausführen/tpm.msc* die TPM-Verwaltungskonsole.
2. Klicken Sie unter *Aktionen* auf *TPM initialisieren*, um den TPM-Initialisierungs-Assistenten zu starten.
3. Wenn das TPM ausgeschaltet ist, zeigt der TPM-Initialisierungs-Assistent das Dialogfeld *TPM-Sicherheitshardware einschalten* an. In diesem Dialogfeld werden Sie durch das Einschalten des TPM geführt. Um das TPM einzuschalten, müssen Sie das System neu starten.
4. Wenn das TPM bereits eingeschaltet ist, zeigt der TPM-Initialisierungs-Assistent das Dialogfeld *TPM-Besitzerkennwort erstellen* an.
5. Starten Sie den Server neu.
6. Nach dem Neustart wird eine Bestätigungsaufforderung angezeigt, um sicherzustellen, dass keine bösartige Software versucht, das TPM einzuschalten, sondern ein physisch anwesender Benutzer.
7. Bevor das TPM zum Schützen Ihres Computers verwendet werden kann, muss es einem Besitzer zugeordnet sein. Beim Festlegen des TPM-Besitzers weisen Sie ein Kennwort zu, sodass nur der autorisierte TPM-Besitzer auf das TPM zugreifen und es verwalten kann. Mit dem TPM-Kennwort können Sie das TPM ausschalten oder es löschen. Um die TPM-Besitzrechte festzulegen, müssen Sie als Administrator angemeldet sein.
8. Starten Sie erneut den TPM-Initialisierungs-Assistenten.
9. Wählen Sie im Dialogfeld *TPM-Besitzerkennwort erstellen* die Option *Kennwort automatisch erstellen (empfohlen)* aus.
10. Klicken Sie im Dialogfeld *TPM-Besitzerkennwort speichern* auf *Kennwort speichern*, und wählen Sie einen Speicherort für das Kennwort aus.
11. Klicken Sie nochmals *Speichern*. Die Kennwortdatei wird unter dem Namen *Computername.tpm* gespeichert.
12. Klicken Sie auf *Kennwort drucken*, wenn Sie das Kennwort drucken möchten.
13. Klicken Sie auf *Initialisieren*. Der Initialisierungsprozess kann einige Minuten dauern.

Abbildg. 14.19 Die Konsole zur Verwaltung des TPM-Chips erkennt, ob ein Chip verbaut und aktiviert wurde. Wird kein Chip gefunden, sind die Menübefehle zur Einrichtung deaktiviert.

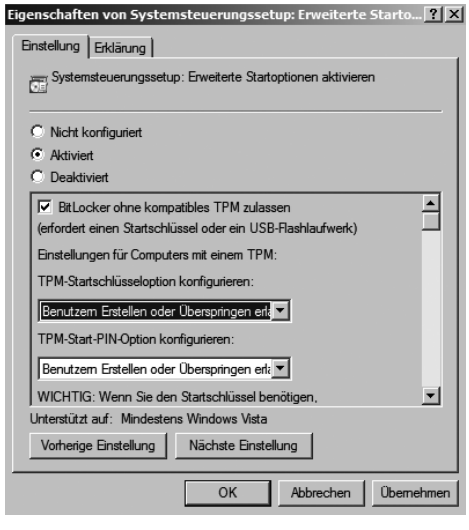


Aktivieren der BitLocker-Laufwerksverschlüsselung mit und ohne TPM

Bevor Sie BitLocker einschalten können, sollten Sie über ein eingeschaltetes und initialisiertes, kompatibles TPM verfügen, dessen Besitzrechte Sie übernommen haben. Sie müssen außerdem als Administrator angemeldet sein. Aber auch die Aktivierung ohne TPM ist möglich. In diesem Fall benötigen Sie einen USB-Stick, der mit dem Server verbunden wird. Die Fehlermeldung mit der Partitionierung lässt sich nicht ohne weiteres beheben. Wir zeigen Ihnen diese Vorgehensweise später noch in diesem Kapitel. Die Aktivierung von BitLocker ohne TPM lässt sicher allerdings recht einfach konfigurieren. Dazu ist es notwendig, in die lokale Sicherheitsrichtlinie des Computers zu wechseln. Alternativ können die folgenden Einstellungen auch über Gruppenrichtlinien in einem Active Directory vorgegeben werden. Gehen Sie zur Konfiguration der lokalen Sicherheitsrichtlinie folgendermaßen vor (Abbildung 14.20):

1. Starten Sie über *Start/Ausführen/gpedit.msc* die Verwaltungsoberfläche der lokalen Sicherheitsrichtlinie.
2. Wechseln Sie in der Konsolenstruktur zum Eintrag *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerksverschlüsselung*.
3. Doppelklicken Sie im rechten Bereich des Fensters auf die Richtlinie *Systemsteuerungssetup: Erweiterte Startoptionen aktivieren*.
4. Aktivieren Sie im Dialogfeld die Option *Aktiviert.*
5. Stellen Sie sicher, dass das Kontrollkästchen *BitLocker ohne kompatibles TPM zulassen* aktiviert ist.
6. Klicken Sie auf *OK*.
7. Die Richtlinie erhält darauf in der Statuszeile den Status *Aktiviert*.
8. Nachdem die lokale Sicherheitsrichtlinie konfiguriert wurde, ist die Einstellung aber noch nicht in das System übernommen worden. Dazu muss entweder der Computer neu gestartet werden oder Sie müssen in der Befehlszeile den Befehl *gpupdate /force* eingeben. Durch Eingabe dieses Befehls wird die konfigurierte Einstellung übernommen.

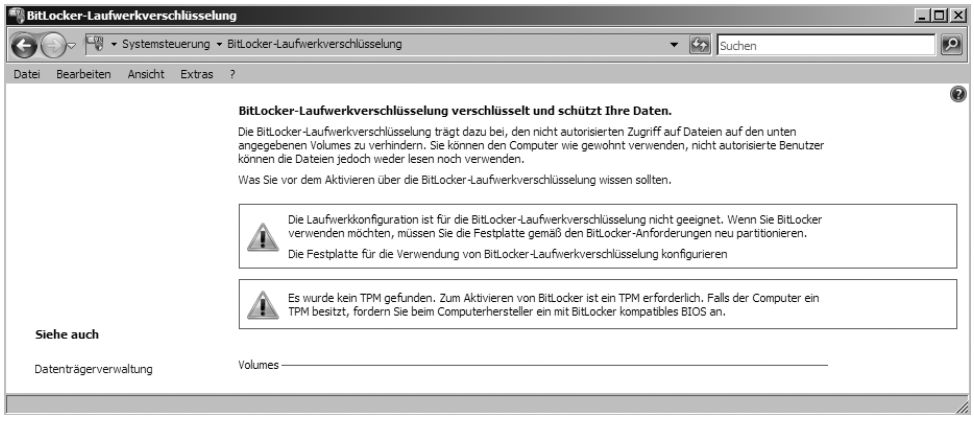
Abbildg. 14.20 Erst nach der Bearbeitung der lokalen Sicherheitsrichtlinien lässt sich BitLocker ohne TPM nutzen



Nachdem diese Aufgaben durchgeführt wurden, kann BitLocker aktiviert werden. Entspricht die Partitionierung der Festplatte den Vorgaben und wurde die lokale Sicherheitsrichtlinie entsprechend angepasst, wird kein Fehler mehr angezeigt und BitLocker kann aktiviert werden (Abbildung 14.21):

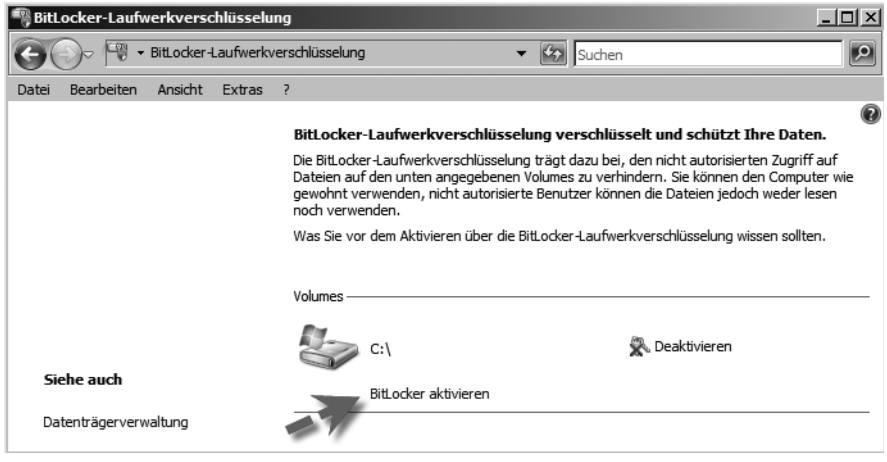
1. Starten Sie die Konfigurationsoberfläche von BitLocker über *Start/Systemsteuerung/BitLocker-Laufwerksverschlüsselung*.
2. Wenn die Partitionierung nicht den Vorgaben entspricht, erhalten Sie eine entsprechende Meldung.

Abbildg. 14.21 BitLocker meldet, wenn die Partitionierung nicht korrekt vorgenommen wurde, oder die Gruppenrichtlinie, um BitLocker ohne TPM zu verwenden, nicht aktiviert ist



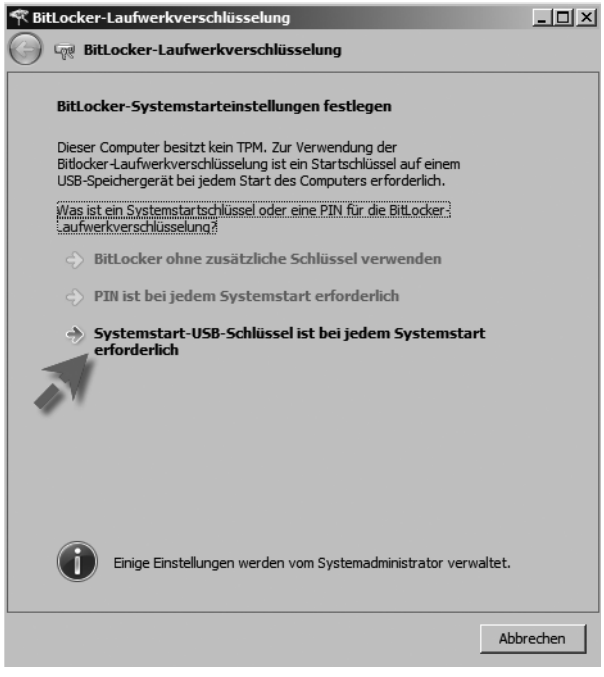
3. Klicken Sie auf dem Bildschirm auf *BitLocker aktivieren*. Diese Option wird nur angezeigt, wenn die Partitionen vorhanden, das TPM aktiviert oder die Einstellung gesetzt wurde, dass BitLocker auch ohne TPM eingesetzt werden kann.

Abbildg. 14.22 BitLocker-Laufwerksverschlüsselung in der Systemsteuerung aktivieren



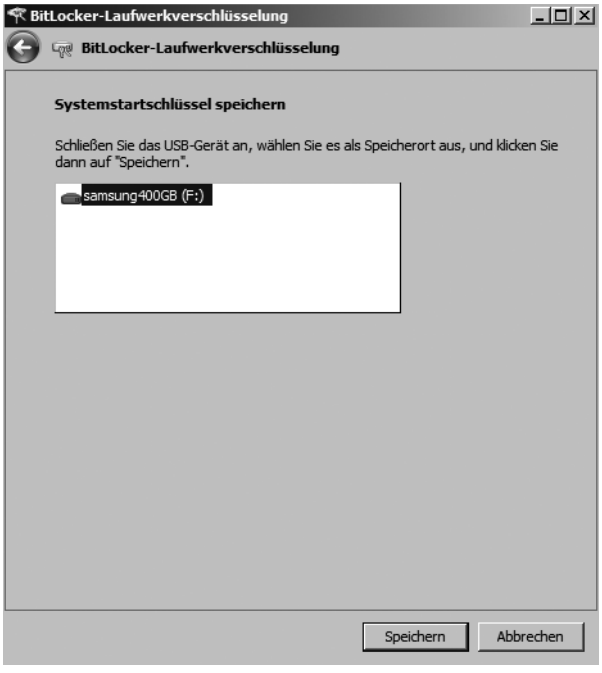
4. Klicken Sie auf *BitLocker ohne zusätzliche Schlüssel verwenden, PIN ist bei jedem Systemstart erforderlich*, oder *Systemstart-USB-Schlüssel ist bei jedem Systemstart erforderlich*. Wird BitLocker ohne TPM eingesetzt, kann bei der Einrichtung ohnehin nur die USB-Option verwendet werden. Klicken Sie daher auf *Systemstart-USB-Schlüssel ist bei jedem Systemstart erforderlich*. Bevor diese Meldung bestätigt wird, sollte der entsprechende USB-Stick mit dem Server verbunden werden.

Abbildg. 14.23 Nach der Aktivierung von BitLocker muss zunächst festgelegt werden, wo der Schlüssel gespeichert wird und ob zusätzliche Funktionen genutzt werden sollen



5. Wird BitLocker ohne TPM eingerichtet oder soll der Schlüssel zusätzlich auf einem USB-Stick gespeichert werden, muss als Nächstes der USB-Stick ausgewählt werden, auf dem der Schlüssel zum Starten des PCs gespeichert werden soll. Neben USB-Sticks können hier natürlich auch USB-Festplatten ausgewählt werden.

Abbildg. 14.24 Auswählen des USB-Speichers für die Ablage des Schlüssels



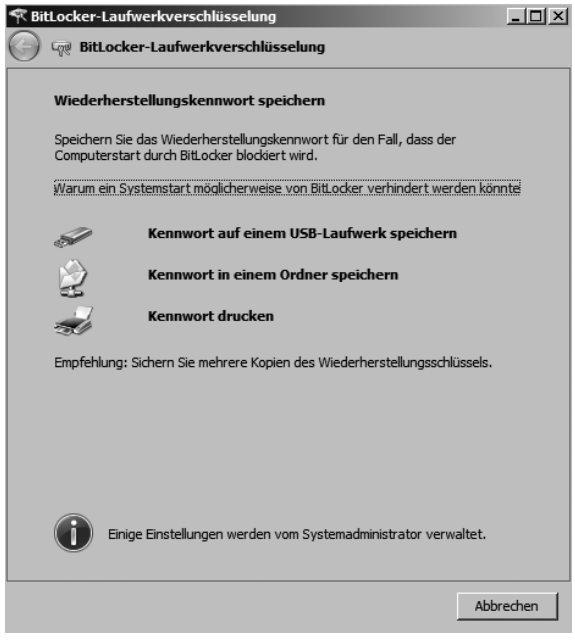
Im nächsten Dialogfeld *Wiederherstellungskennwort speichern* werden die folgenden Optionen angezeigt:

- Kennwort auf einem USB-Laufwerk speichern
- Kennwort in einem Ordner speichern
- Kennwort drucken

Das Kennwort für den Wiederherstellungsschlüssel ist erforderlich, um die verschlüsselten Daten des Volumes zu entsperren, wenn BitLocker in einen gesperrten Zustand wechselt. Sie können mit seiner Hilfe nicht die verschlüsselten Daten einer anderen BitLocker-Verschlüsselungssitzung wiederherstellen.

1. Wählen Sie die gewünschten Optionen aus, um das Wiederherstellungskennwort aufzubewahren. Wird die Speicherung des Systemstartschlüssels auf einem USB-Stick eingesetzt, können Sie das Wiederherstellungskennwort auf dem gleichen Stick speichern lassen. Wichtig ist an dieser Stelle jedoch, dass dieser Stick keinesfalls in fremde Hände gelangen darf, da sonst der komplette Schutz des Computers ausgehebelt wird. Nach der Speicherung des Schlüssels auf dem Stick kann zusätzlich die Speicherung auf einem anderen Laufwerk oder das Ausdrucken aktiviert werden.

Abbildg. 14.25 Speicherung des Wiederherstellungskennwortes von BitLocker



2. Nachdem das Kennwort gespeichert und gedruckt wurde, kann BitLocker aktiviert werden. Nach der BitLocker-Aktivierung erreichen Sie das Fenster für die Verwaltung des Kennwortes jederzeit über die Systemsteuerung. So lässt sich der Schlüssel auch nachträglich ausdrucken oder speichern. Zuvor muss die Aktivierung von BitLocker noch bestätigt werden. Zur Aktivierung und zur Überprüfung der Konfiguration wird der Computer daraufhin neu gestartet. Es müssen alle DVDs oder CDs aus den Laufwerken entfernt werden, damit sichergestellt ist, dass der Computer über die konfigurierte BitLocker-Infrastruktur gebootet wird. Beim nächsten Bootvorgang überprüft BitLocker, ob auf den gespeicherten Startschlüssel zugegriffen werden kann und verschlüsselt die Festplatte nach dem Start von Windows. Nach dieser Einrichtung ist die Verschlüsselung aktiv. Wenn nicht mehr auf das TPM zugegriffen werden kann, oder wenn jemand versucht, von einer Diskette/CD/DVD oder USB-Stick zu starten, um das Betriebssystem zu umgehen, wechselt der Computer in den gesperrten Modus, bis der Wiederherstellungsschlüssel bereitgestellt wird. Wurde der Computer neu gestartet, beginnt Windows Vista mit der Verschlüsselung der Daten. Abhängig von der Größe der Platte dauert dieser Vorgang mehrere Stunden. Der Computer steht zwar parallel zu Arbeit zur Verfügung, allerdings ist die Festplatte stark ausgelastet.

Abbildg. 14.26 Zur Fertigstellung der BitLocker-Einrichtung muss der PC neu gestartet werden

Nach der Einrichtung von BitLocker können auch weitere Partitionen und Festplatten auf dem Server verschlüsselt werden. Auch wenn nachträglich Festplatten eingebaut und Partitionen erstellt werden, kann über die BitLocker-Verwaltungsoberfläche die Verschlüsselung nachträglich für diese Laufwerke aktiviert werden.

HINWEIS Verwenden Sie TPM zusammen mit einer PIN, muss bei jedem Start des Servers eine PIN für den Start eingegeben werden. Unterstützt der Server kein TPM, muss beim Serverstart der USB-Stick mit dem Schlüssel mit dem Server verbunden werden.

Aktivieren von BitLocker bei bereits installiertem Windows Server 2008

Sollte bei der Installation von Windows die Voraussetzungen von BitLocker, also das Anlegen von zwei Partitionen, nicht durchgeführt worden sein, besteht auch die Möglichkeit, nachträglich eine zusätzliche Partition anzulegen. Dazu wird die Hauptpartition verkleinert, was mit Windows Server 2008 ohne weiteres möglich ist, und die zweite, notwendige Partition angelegt. Ist in dem Computer eine zweite Festplatte verfügbar, ist es nicht notwendig, die erste Partition zu verkleinern, da in diesem Fall die zweite Platte zur Ablage der Bootdateien verwendet wird. Wird die zweite Platte aber für andere Zwecke eingesetzt, sollte besser eine neue Partition mit der notwendigen Größe angelegt werden, um BitLocker einzurichten, was auch der empfohlene Weg ist. Wollen Sie BitLocker einrichten, nachdem Windows Server 2008 installiert wurde, gehen Sie folgendermaßen vor:

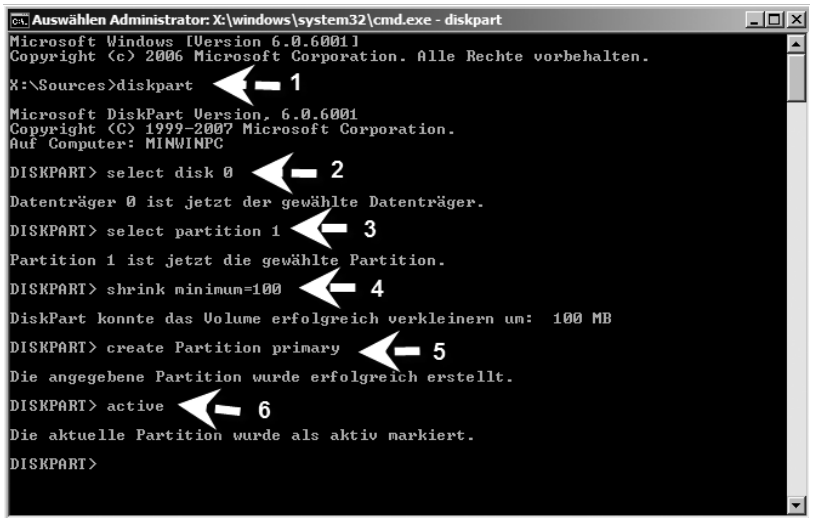
1. Booten Sie zunächst mit der Windows Server 2008-DVD.
2. Starten Sie die *Computerreparaturoptionen*, und gehen Sie in den *Systemwiederherstellungsoptionen* in die *Eingabeaufforderung*, wie wir bereits zu Beginn dieses Artikels beschrieben haben. Da sich bereits ein Betriebssystem auf dem Computer befindet, muss dieses zum Laden ausgewählt werden.
3. Nachdem Sie in der Eingabeaufforderung sind, muss mit dem Befehl *diskpart* die Partition für BitLocker vorbereitet werden. Bei der Neueinrichtung eines Computers kann dazu einfach eine neue Partition angelegt werden, wie wir zuvor beschrieben haben. Bei einer Einrichtung von BitLocker nach der Installation von Windows Server 2008, wird die erste Partition zunächst verkleinert. Mit dem verkleinerten Raum wird anschließend eine neue Partition angelegt, auf der BitLocker die Bootmanager-Daten ablegen kann. Dazu werden die folgenden Befehle verwendet. Nach jedem Befehl müssen Sie die Ausführung zunächst mit der ↵-Taste bestätigen:

```
Diskpart
Select disk 0
select partition 1
shrink minimum=100
create partition primary
active
```

4. Schließen Sie das Diskpart-Fenster noch nicht, da noch weitere Befehle eingeben werden müssen. Auch diese müssen wieder in der folgenden Reihenfolge eingegeben und anschließend bestätigt werden:

```
assign letter=S
format quick
exit
```

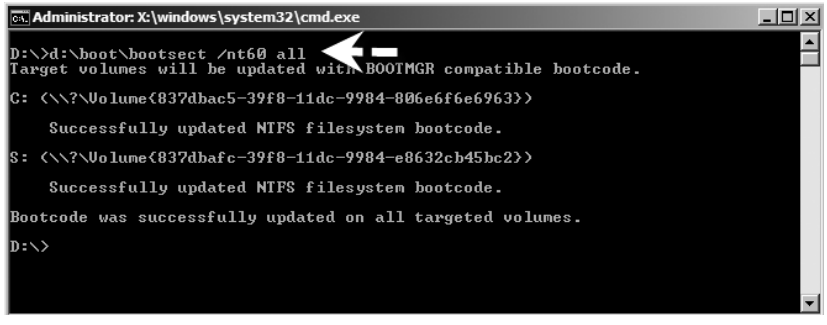
Abbildg. 14.27 Für die Einrichtung von BitLocker wird die bestehende Partition um 100 MB verkleinert, damit eine Partition für BitLocker erstellt werden kann



Nach der Eingabe dieser Befehle ist die Konfiguration mit *diskpart* abgeschlossen. Als Nächstes wird der Bootmanager von der Windows Server 2008-DVD verwendet, um die notwendigen Systemdateien von der C-Platte auf die neu erstellte S:-Partition zu transferieren. Lassen Sie dazu die Eingabeaufforderung geöffnet und gehen Sie folgendermaßen vor:

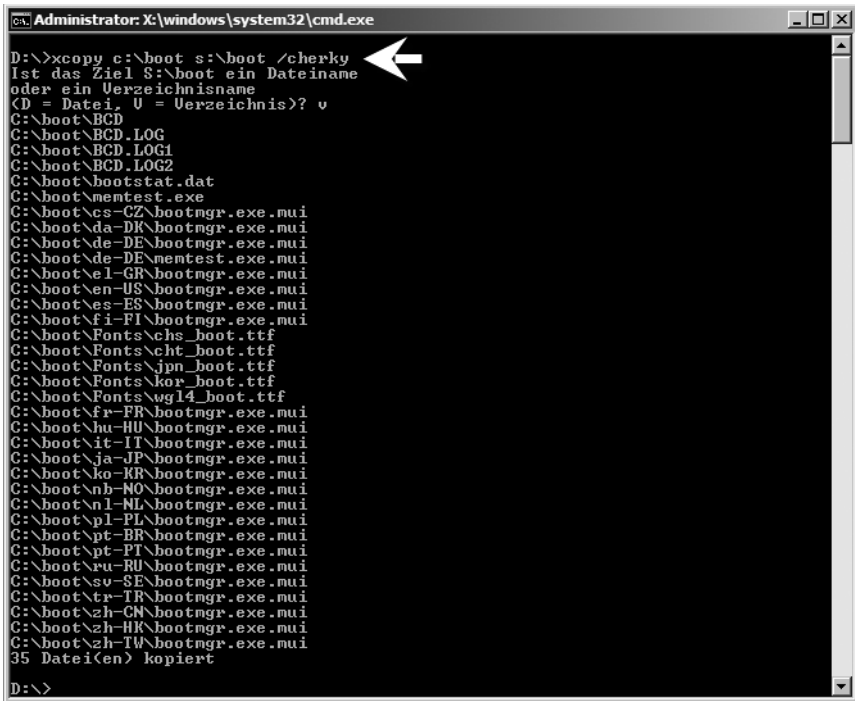
1. *D:\boot\bootsect /nt60 ALL* (installiert den Bootmanager, wobei D: das Laufwerk mit der Setup-DVD ist)

Abbildg. 14.28 Der Bootmanager wird von der DVD erneut auf C: und auf die neue S-Partition installiert



2. Kopieren Sie in der gleichen Befehlszeile die Bootdateien von der C:-Systempartition auf die aktivierte Startpartition, in diesem Beispiel das Laufwerk S:. Geben Sie bei der Frage, ob es sich bei den zu kopierenden Dateien um eine Datei oder ein Verzeichnis handelt, den Buchstaben *V* (für Verzeichnis) ein. Der Befehl in diesem Beispiel für diesen Vorgang lautet *xcopy c:\boot s:\boot\ /cherky*.

Abbildg. 14.29 Kopieren der Bootdateien von C: auf S:



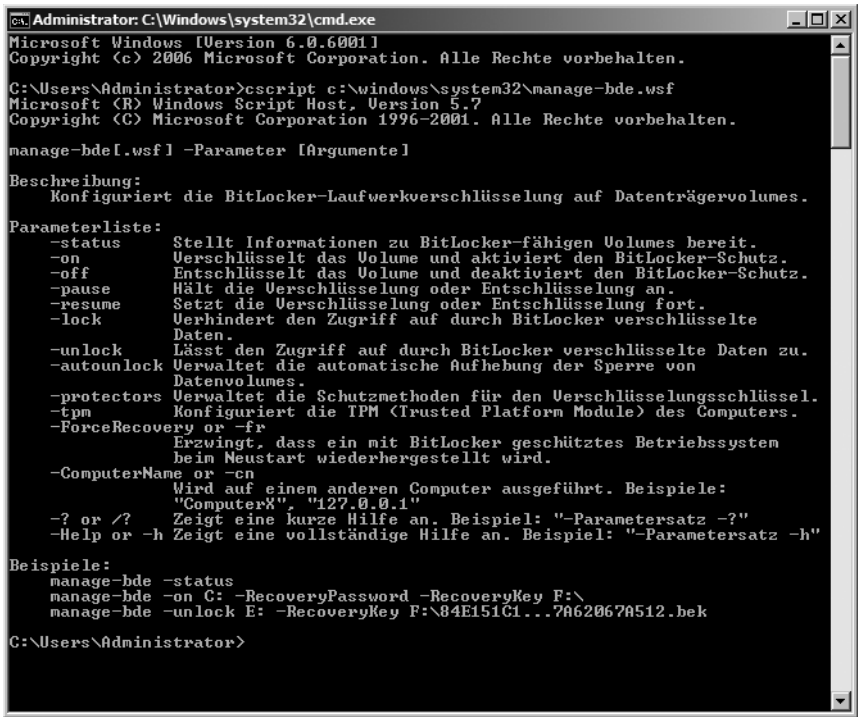
3. Anschließend werden in der gleichen Befehlszeile noch weitere Befehle eingegeben, durch die der Bootmanager in das neue Laufwerk übertragen und entsprechend konfiguriert wird. Hier werden auch die notwendigen Dateiattribute für beide Verzeichnisse neu gesetzt

```
attrib –r –s –h C:\bootmgr
xcopy C:\bootmgr S:\
attrib +r +h +s C:\bootmgr
attrib +r +h +s S:\bootmgr
attrib +r +h +s S:\boot
chkdsk /f C:
chkdsk /f S:
exit
```

Schließen Sie das Fenster und starten Sie den Computer neu. Anschließend sollte sich BitLocker, wie bereits beschrieben, einrichten lassen. Gehen Sie dazu genau so vor, wie bei der Einrichtung mit neu installiertem Windows Server 2008.

TIPP Zur Verwaltung von BitLocker über Skripts oder der Befehlszeile gibt es das Skript *manage-bde.wsf*, welches im Verzeichnis *C:\Windows\System32* zur Verfügung steht. Über *Cscript c:\windows\system32\manage-bde.wfs* erhalten Sie eine Auflistung der verschiedenen Optionen (Abbildung 14.30). Der aktuelle Status der Verschlüsselung lässt sich zum Beispiel mit dem Befehl *cscript c:\windows\system32\manage-bde.wfs –status* anzeigen.

Abbildg. 14.30 Für die Verwaltung von BitLocker gibt es auch ein Tool für die Befehlszeile



Rettungsmöglichkeiten zur Wiederherstellung

Wenn Daten verschlüsselt werden, trägt der Administrator immer das Risiko, dass er selbst nicht mehr an die Daten kommt, wenn er die entsprechenden Schlüssel verliert. Es besteht auch die Möglichkeit, dass der TPM defekt, der Startschlüssel zerstört ist oder Sie Ihren PIN vergessen haben. Damit bei solchen Vorfällen, auch bei der Erweiterung des Servers, die Daten noch zugänglich sind, gibt es die BitLocker-Recovery-Konsole. Wenn Sie BitLocker aktivieren, legen Sie sich auf jeden Fall ein Wiederherstellungskennwort an. Dieser generierte Code besteht aus sechs Blöcken mit je acht Ziffern. Sie können ihn ausdrucken oder als Textdatei auf einem USB-Stick speichern. Das stellt im Übrigen ein ziemliches Sicherheitsrisiko dar, da jeder, der diesen Schlüssel besitzt, auf die BitLocker-Partition zugreifen kann. Wenn Sie zum Beispiel eine mit BitLocker verschlüsselte Festplatte in einen anderen Server einbauen, benötigen Sie lediglich einen USB-Stick mit dem Wiederherstellungsschlüssel, um auf die Partition wieder zugreifen zu können. Die Partition ist gesperrt, wenn der Datenträgerverschlüsselungsschlüssel nicht automatisch neu erstellt werden kann. Dafür gibt es verschiedene Ursachen:

- Der Benutzer verliert oder vergisst die PIN, oder er verliert den Systemstartschlüssel.
- Ein Fehler in Bezug auf das TPM tritt auf.
- Eine der früher verwendeten Startdateien wird geändert.
- Der Computer wird bei versehentlich ausgeschaltetem TPM ausgeschaltet.
- Der Computer wird bei versehentlich gelöschtem TPM ausgeschaltet.

Ein gesperrter Computer kann nicht die normalen Zahlen einer Standardtastatur annehmen, deshalb müssen Sie das Kennwort für den Wiederherstellungsschlüssel mit den Funktionstasten eingeben. F1 bis F9 stellen die Ziffern *1* bis *9* dar, F10 die Ziffer *0*. Um die Datenwiederherstellung zu testen, gehen Sie folgendermaßen vor:

1. Öffnen Sie über *Start/Ausführen/tpm.msc* die TPM-Verwaltungskonsole.
2. Klicken Sie unter *Aktionen* auf *TPM ausschalten*.
3. Wenn die Meldung *Das TPM ist ausgeschaltet und der Besitz des TPM wurde übernommen* angezeigt wird, schließen Sie die Konsole.
4. Entfernen Sie das USB-Laufwerk mit dem gespeicherten Wiederherstellungsschlüssel vom Server.
5. Schalten Sie den Server aus.
6. Starten Sie den Computer erneut, werden Sie nach dem Kennwort für den Wiederherstellungsschlüssel gefragt, da die Startkonfiguration nach dem Verschlüsseln geändert wurde.
7. In der Wiederherstellungskonsole von BitLocker werden Sie aufgefordert, das USB-Laufwerk anzuschließen, auf dem sich der Systemstart- oder Wiederherstellungsschlüssel befindet.
8. Der Computer wird nach dem Anschluss neu gestartet. Sie müssen den Wiederherstellungsschlüssel nicht manuell eingeben.
9. In der Wiederherstellungskonsole von BitLocker werden Sie aufgefordert, das Kennwort für den Wiederherstellungsschlüssel einzugeben.

Ausschalten von BitLocker

Wenn Sie BitLocker ausschalten, können Sie sich entscheiden, ob Sie BitLocker temporär deaktivieren oder das Laufwerk entschlüsseln möchten. Wenn Sie BitLocker deaktivieren, können Sie TPM-Änderungen und Betriebssystemaktualisierungen durchführen. Durch das Entschlüsseln des Laufwerks wird das Volume wieder lesbar und der Wiederherstellungsschlüssel wird gelöscht. Wenn ein Volume entschlüsselt wurde, müssen Sie einen neuen Wiederherstellungsschlüssel generieren, indem Sie den Verschlüsselungsvorgang erneut durchlaufen. Klicken Sie auf *BitLocker ausschalten.* Klicken Sie im Dialogfeld *Welche Entschlüsselungsstufe möchten Sie anwenden* auf *BitLocker deaktivieren* oder *Volume entschlüsseln*.

BitLocker und Active Directory-Domänen

Das Wiederherstellungskennwort von BitLocker kann in einem Ordner oder auf einem oder mehreren USB-Geräten gespeichert oder einfach ausgedruckt werden. Ein Administrator kann außerdem eine Gruppenrichtlinie konfigurieren, um Wiederherstellungskennwörter automatisch zu generieren und diese in Active Directory zu sichern. Der effizienteste Weg in einer Unternehmensumgebung ist es, diese durch BitLocker in Active Directory sichern zu lassen. Dies kann über Gruppenrichtlinien oder via WMI erreicht werden. Der Zugriff auf die Wiederherstellungsschlüssel ist dann zum Beispiel über Skripts oder LDAP-Befehle möglich. Eine weitere Möglichkeit ist die Speicherung von Schlüsseln auf USB-Geräten. Active Directory kann sowohl zum Speichern von Wiederherstellungsinformationen für die Windows BitLocker-Laufwerkverschlüsselung als auch zum Speichern von TPM-Besitzerinformationen verwendet werden. Die BitLocker-Wiederherstellungsinformatio-

nen werden in einem untergeordneten Objekt eines Computerkontos in Active Directory gespeichert. Das bedeutet, das Computerobjekt ist der Container für das BitLocker-Wiederherstellungsobjekt. Für jedes Computerkonto können mehrere BitLocker-Wiederherstellungsobjekte vorhanden sein, da jedem BitLocker-aktivierten Volume mehrere Wiederherstellungskennwörter zugeordnet werden können. Jedes BitLocker-Wiederherstellungsobjekt auf einem BitLocker-aktiviertem Volume hat einen eindeutigen Namen und enthält eine GUID (Globally Unique Identifier) für das Wiederherstellungskennwort. Der Name des BitLocker-Wiederherstellungsobjekts ist aufgrund der Einschränkungen von Active Directory auf 64 Zeichen begrenzt. Dieser Name enthält die GUID des Wiederherstellungskennworts sowie Datums- und Uhrzeitinformationen.

Beispiel:

2006-09-30T151843-0610{064aADE1-122D-5173-A501-3554520B86D5}

Der allgemeine Name (Common Name, CN) von Active Directory für das BitLocker-Wiederherstellungsobjekt lautet *ms-FVE-RecoveryInformation* und enthält Attribute wie *ms-FVE-RecoveryPassword* und *ms-FVE-RecoveryGuid*. Pro Computer ist immer nur ein TPM-Besitzerkennwort möglich, der Hash des TPM-Besitzerkennworts wird in Active Directory als ein Attribut des Computerkontos gespeichert. Die Speicherung erfolgt in Unicode. Das Attribut hat den allgemeinen Namen (CN) *ms-TPM-OwnerInformation*. Damit BitLocker- und TPM-Informationen in Active Directory gespeichert werden können, muss auf allen Domänencontrollern Windows Server 2003 mit Service Pack 1 oder Windows Server 2008 installiert sein.

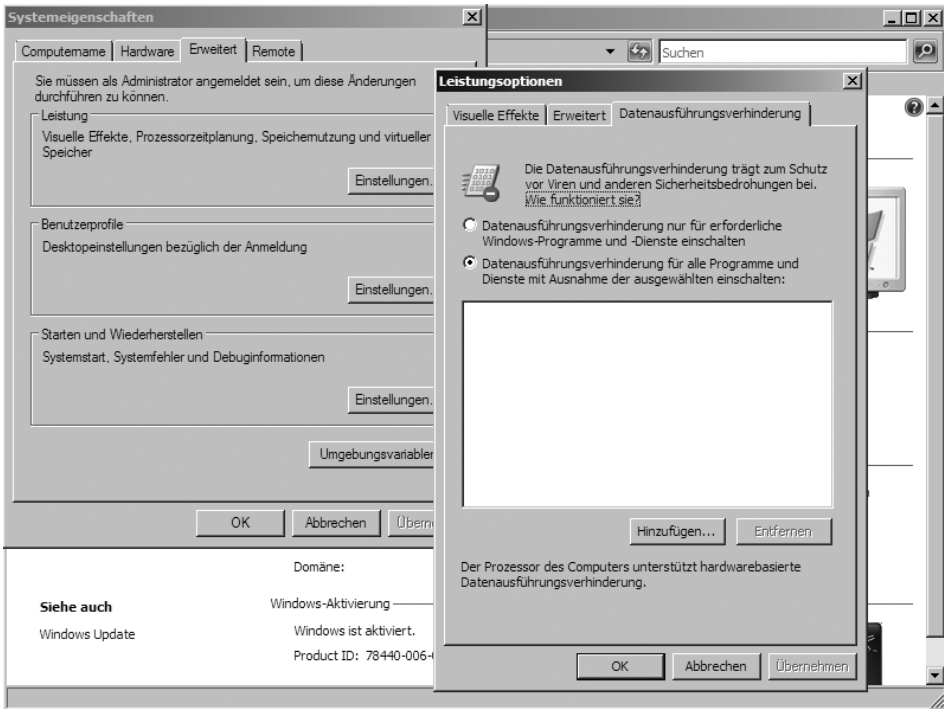
Setzen Sie im Unternehmen Windows Vista Ultimate Edition oder Enterprise Edition, kann über Gruppenrichtlinien der Einsatz der Gruppenrichtlinien konfiguriert werden. Die Einstellungen dafür erfolgen an der gleichen Stelle wie die Aktivierung von BitLocker ohne TPM.

Dateiausführungsverhinderung

Die Datenausführungsverhinderung ist ein Sicherheitsfeature, das den Computer vor Schäden durch Viren schützt. Diese Funktion wurde bereits mit Windows Server 2003 eingeführt, aber wenig genutzt. Hierbei werden Programme überwacht, um die sichere Verwendung des Systemspeichers durch die betreffenden Programme sicherzustellen. Wenn ein Programm versucht, Code aus dem Speicher auf unzulässige Weise auszuführen, wird das Programm durch die Datenausführungsverhinderung (Data Execution Prevention, DEP) geschlossen. Dadurch können Angriffe durch Viren und Trojaner frühzeitig entdeckt werden. Die Datenausführungsverhinderung überwacht automatisch die wichtigsten Windows-Programme und -Dienste. Sie können den Schutz verbessern, indem Sie alle Programme durch die Datenausführungsverhinderung überwachen lassen. Sollten Sie mit einer Applikation auf einem Server Probleme haben, die sich darin äußern, dass die Anwendung nicht startet, sollten Sie für diese Anwendung die DEP deaktivieren. Zur Konfiguration der gelangen Sie mit den folgenden Schritten:

1. Rufen Sie über die *Start*-Schaltfläche die *Systemsteuerung* auf.
2. Doppelklicken Sie zunächst auf *System* und anschließend per einfachem Klick im Bereich *Aufgaben* auf *Erweiterte Systemeinstellungen*.
3. Wählen Sie auf der nun geöffneten Registerkarte *Erweitert* im Bereich *Leistung* die Schaltfläche *Einstellungen*.
4. Aktivieren Sie im daraufhin geöffneten Dialogfeld *Leistungsoptionen* die Registerkarte *Datenausführungsverhinderung*.

Abbildg. 14.31 Verwalten der Dateiausführungsverhinderung unter Windows Server 2008



Normalerweise können Sie die Standardeinstellungen einfach übernehmen. Wenn Sie der Datenausführungsverhinderung bestimmte Programme hinzufügen wollen, können Sie dies auf der nun angezeigten Registerkarte durchführen. Wenn die Dateiausführungsverhinderung ein Programm immer wieder schließt, dem Sie vertrauen, können Sie die Datenausführungsverhinderung für das geschlossene Programm deaktivieren oder eine Version des Programms installieren, welches zur Dateiausführungsverhinderung kompatibel ist. Die Datenausführungsverhinderung ist ein softwarebasiertes Feature von Windows. Manche Computerprozessoren verfügen ebenfalls über eine hardwarebasierte Datenausführungsverhinderung. Diese Prozessoren verwenden Hardwaretechnologie, um zu verhindern, dass Programme Code in geschützten Speicherbereichen ausführen. Wenn Ihr Prozessor keine hardwarebasierte Datenausführungsverhinderung unterstützt, verwendet Windows die softwarebasierte Datenausführungsverhinderung zum Schutz des Computers.

TIPP Auf der Internetseite *http://support.microsoft.com/kb/875352/DE/* erhalten Sie weitergehende Informationen über die Dateiausführungsverhinderung.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, welche neuen Sicherheitsfunktionen es in Windows Server 2008 gibt und wie Sie diese produktiv im Netzwerk einsetzen. Im nächsten Kapitel vertiefen wir das Thema Sicherheit und widmen uns dem neuen Netzwerkzugriffschutz (NAP), mit dem ein Windows Server 2008-Netzwerk vor unsicheren Arbeitsstationen geschützt werden kann.

Kapitel 15

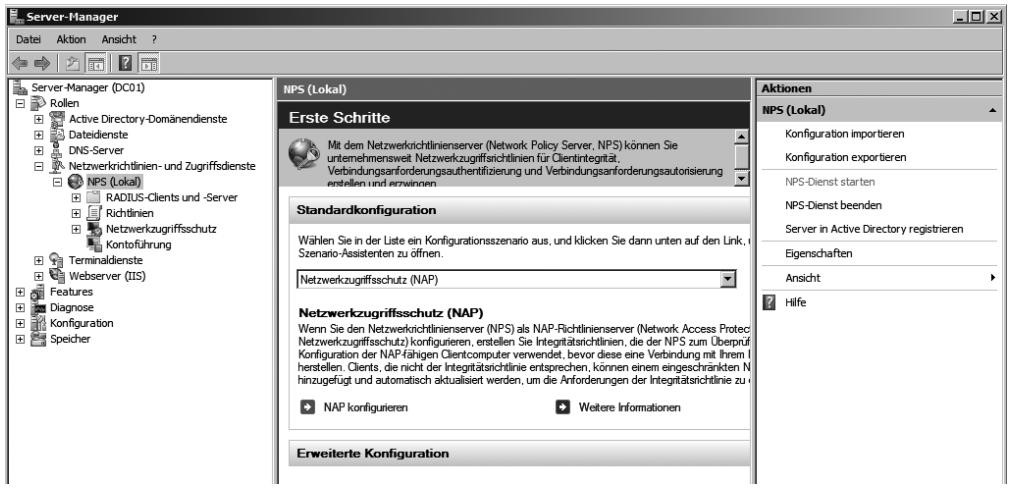
Netzwerkrichtlinien- und Zugriffsdienste verwalten

In diesem Kapitel:

Mit den neuen Netzwerkrichtlinien- und Zugriffsdiensten werden nicht nur die Remoteeinwahlen verwaltet, sondern auch die neue Netzwerkzugriffsschutz-Funktion (Network Access Protection, NAP) von Windows Server 2008, die auch in Windows Vista und Windows XP SP2 integriert ist. In Windows Vista in der Client bereits enthalten, für Windows XP und Windows Server 2003 muss er nachträglich installiert werden. Bei der Installation von Service Pack 3 wird der Client in Windows XP integriert.

TIPP Wollen Sie die IPSec- oder NAP-Konfiguration auf einem Core-Server überprüfen, verwenden Sie in der Befehlszeile die beiden Befehle *Netsh ipsec* und *Netsh nap*.

Abbildg. 15.1 Verwalten von NAP im Server-Manager

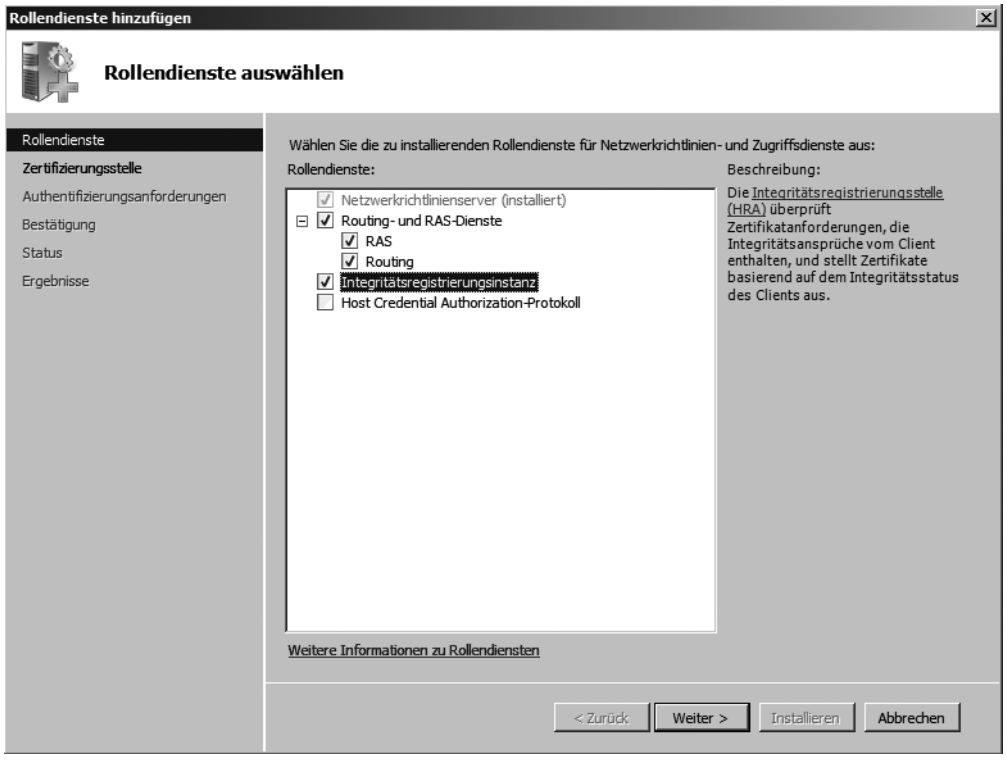


NAP kann nicht nur für Domänencomputer verwendet werden, sondern auch für Computer, die nicht Mitglied einer Domäne sind. Bei NAP können Sie Computern abhängig von deren Sicherheitseinstellungen, Patchstand und installierten Anwendungen den Netzwerkzugriff gestatten oder verweigern bzw. beschränken. In diesem Kapitel beschäftigen wir uns ausführlich mit dieser Funktion, die im Zusammenhang mit dem TS Gatewaydienst in Kapitel 12 ebenfalls bereits einleitend beschrieben worden sind. Neben der NAP-Funktionalität bietet ein Netzwerkrichtlinien- und Zugriffserver auch die Remoteeinwahl. Die Remote Authentication Dial-In User Service (RADIUS)-Funktion von Windows Server 2008 ersetzt den Internet Authentication Service (IAS) von Windows Server 2003. NAP können Sie auch in Windows Server 2003-Domänen nutzen, allerdings muss der Netzwerkrichtlinienserver (Network Policy Server, NPS) unter Windows Server 2008 laufen. Wir zeigen Ihnen in diesem Kapitel auf Basis verschiedener Workshops, wie Sie die Sicherheits- und Einwahlmethoden von Windows Server 2008 nutzen können. Durch diese praxisnahe Erläuterung ersparen wir Ihnen die Erläuterungen von einzelnen Optionen und Registerkarten, sondern zeigen direkt an der Praxis, welche Möglichkeiten Sie nutzen können. Im Rahmen dieser Workshops zeigen wir Ihnen neben den komplexeren Möglichkeiten des Netzwerkzugriffsschutzes auch die Einrichtung der Standardfunktionen wie Routing und RAS oder VPN.

Überblick über den Netzwerkzugriffsschutz (NAP)

Der Netzwerkzugriffsschutz (Network Access Protection, NAP) ist neu in Windows Server 2008. Als Client für diese neue Funktion wird Windows Vista, aber auch Windows XP mit installiertem SP2 unterstützt. Der Client für NAP wird mit dem Service Pack 3 für Windows XP installiert. Damit NAP im Netzwerk eingesetzt werden kann, wird ein Richtlinienserver benötigt, über den Sie die entsprechenden Richtlinien für NAP hinterlegen können. Diese Rolle können Sie über den Server-Manager hinzufügen und anschließend verwalten (Abbildung 15.2).

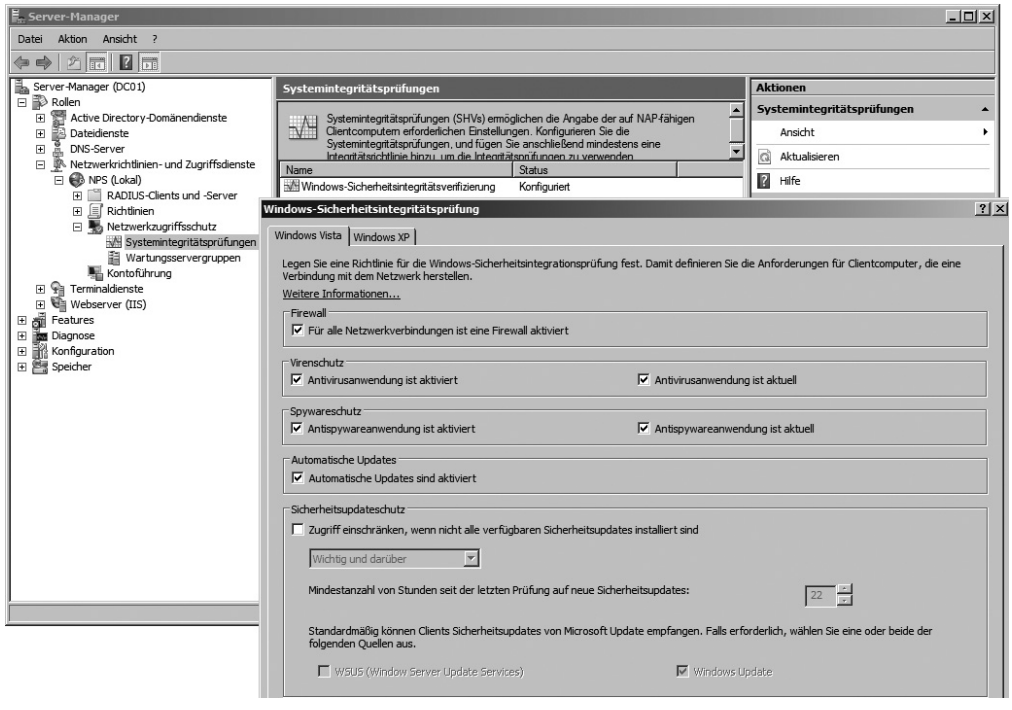
Abbildg. 15.2 Hinzufügen der Rolle *Netzwerkrichtlinien- und Zugriffsdienste*



Im Gegensatz zu Serverdiensten wie die kostenlos erhältlichen Windows Server Update Services (WSUS, siehe Kapitel 23) ist NAP nicht dafür zuständig, Patches zu installieren, sondern zu überprüfen, ob auf einem PC entsprechende Patches installiert sind. Entspricht ein Client nicht den Bedingungen für eine VPN-Einwahl, zum Beispiel durch einen installierten Virenscanner, installierte Patches oder sonstigen Sicherheitseinstellungen, wird diesem nur ein eingeschränkter Zugriff zum Netzwerk oder überhaupt kein Zugriff gewährt. Durch diese Funktion können vor allem Gefahren, die von Heim-PCs und Notebooks ausgehen, vermieden werden. Fremdsysteme, Internet-Cafés und unsichere Heimarbeitsplätze lassen sich so effizient vom Netzwerk ausschließen. NAP ist dafür zuständig, nur jenen PCs den Zugriff auf das Netzwerk zu gewähren, die den Sicherheits-

vorgaben des Unternehmens entsprechen. PCs unter Windows XP SP2 und Windows Vista können eine Windows-Sicherheitsintegritätsverifizierung durchführen, bei der Sie konfigurieren können, welche Bedingungen ein PC erfüllen muss (Abbildung 15.3). NAP ist sozusagen eine Weiterentwicklung der Network Access Quarantine von Windows Server 2003. Die Konfiguration und Einrichtung der Funktion wurde aber für Windows Server 2008 extrem vereinfacht und optimiert. Ein Vorteil der NAP ist, dass Sie nicht nur PCs berücksichtigen können, die sich über VPN einwählen, sondern auch PCs, die sich ins LAN einwählen. Ein Beispiel für diese Konfiguration sind zum Beispiel Notebooks, die auch zu Hause betrieben werden.

Abbildg. 15.3 Konfiguration der Windows-Sicherheitsintegritätsprüfung in Windows Server 2008



NAP stellt sicher, dass die Endpunkte in einem Netzwerk, also die PCs, einem fest definierten Sicherheitsstandard entsprechen. Sie benötigen für NAP einen Windows Server 2008 und als Clientkomponente Windows Vista und Windows XP. Es ist geplant, auch Windows Server 2003 NAP-fähig zu machen. Microsoft stellt eine API zur Verfügung, sodass auch Dritthersteller ihre Produkte in NAP integrieren können. So können Sie zum Beispiel auch Ihren Antiviren-Hersteller in die Plattform einbinden.

Funktionsweise von NAP im Netzwerk

Die NAP-Plattform baut auf verschiedenen Grundstrukturen auf:

- Computer werden auf Basis von zentralen Richtlinien und der Windows-Sicherheitsintegritätsverifizierung eingeordnet.

- Computer, die den Richtlinien entsprechen, können ungestört im Netzwerk kommunizieren.
- Computer, die nicht den Richtlinien entsprechen, können bei der Kommunikation eingeschränkt werden oder an der Kommunikation gehindert werden.
- Computern, die nicht den Richtlinien entsprechen, können darüber hinaus Mechanismen zur Verfügung gestellt werden, um die Richtlinien einzuhalten. So können zum Beispiel Patches über einen WSUS nachgezogen werden, sodass diese Computer zukünftig diesen Richtlinien entsprechen.
- Der Sicherheitszustand der Computer wird durch NAP dauerhaft und ständig sichergestellt.

Damit der Zugriff eines PCs überprüft werden kann, findet folgender Vorgang statt:

1. Ein Client will sich mit dem Netzwerk verbinden.
2. Als Nächstes generiert der Client ein *Statement of Health*. Der NAP-Client weiß, wie er das System untersuchen muss und kann einen Bericht erstellen, der an den Netzwerkrichtlinien-Server übergeben wird.
3. Dieser entscheidet auf Basis der zentralen Richtlinie, ob das Statement of Health gültig ist oder nicht.
4. Auf Basis dieses Ergebnisses wird eine Richtlinie verwendet, die den Zugriff gestattet oder nicht.

Sie können für die NAP-Infrastruktur ungeschützte Bereiche von DMZs und geschützten Bereichen unterscheiden. In den geschützten Bereichen stehen zum Beispiel Ihre Datei- oder Exchange-Server. In der DMZ könnte ein WSUS-Server oder der DHCP-Server stehen. Der ungeschützte Bereich ist von der NAP vollkommen unberücksichtigt. Wichtig ist in diesem Bereich die Art und Weise, wie der Zugriff zum Netzwerk stattfindet. Clients können sich per VPN einwählen, auf ein TS Gateway zugreifen (siehe Kapitel 12) oder sich mit dem Netzwerk verbindet. Findet die Verbindung über das Hausnetzwerk statt, benötigt ein Client zunächst eine IP-Adresse von einem DHCP-Server. Dieser Zugriff sollte also gestattet werden. Nicht konforme Clients können sogar vom Beziehen einer DHCP-Adresse gehindert werden. Auch der Zugriff per WLAN kann über NAP gesteuert werden. Ein Client, der nicht konform ist, sollte aber Gelegenheit haben, zumindest auf den WSUS-Server zuzugreifen, damit die notwendigen Patches installiert werden können.

Netzwerkrichtlinien (Network Policies) steuern den Netzwerkzugriff von Clients basierend auf Integritätsrichtlinien (Health Policies), die wiederum auf den Systemintegritätsprüfungen (System Health Validators, SHVs) aufbauen. Nachdem Sie die Systemintegritätsprüfungen konfiguriert haben, in denen konfiguriert ist, welche Bedingungen ein NAP-konformer Client erfüllen muss, wird mit den Integritätsrichtlinien festgelegt, ob ein Client NAP-konform noch Nicht-NAP-konform ist. Das bedeutet, ein Client muss erst bestimmte Bedingungen erfüllen, zum Beispiel die Installation aktueller Patches oder eines Virenschutzes. Meldet er diesen Zustand und erfüllt damit die Systemintegritätsrichtlinie, ist der NAP-Konform, darf also im Netzwerk kommunizieren. Erfüllt er die Bedingungen in den Systemintegritätsprüfungen nicht, ist er nicht NAP-Konform und darf entweder gar nicht oder nur eingeschränkt mit anderen Rechnern kommunizieren, bis die Systemintegritätsprüfungen erfüllt sind. Die Netzwerkrichtlinien steuern wiederum, was mit NAP-konformen bzw. Nicht-NAP-konformen Clients im Netzwerk passieren soll und welchen Zugriff diese erhalten dürfen. Die NAP-Infrastruktur basiert daher auf den drei Pfeilern:

- Systemintegritätsprüfungen (System Health Validators)
- Integritätsrichtlinien (Health Policies)
- Netzwerkrichtlinien (Network Policies)

TIPP Auf der Internetseite *http://blogs.technet.com/nap* erhalten Sie direkt von den NAP-Entwicklern interessante Infos aus erster Hand.

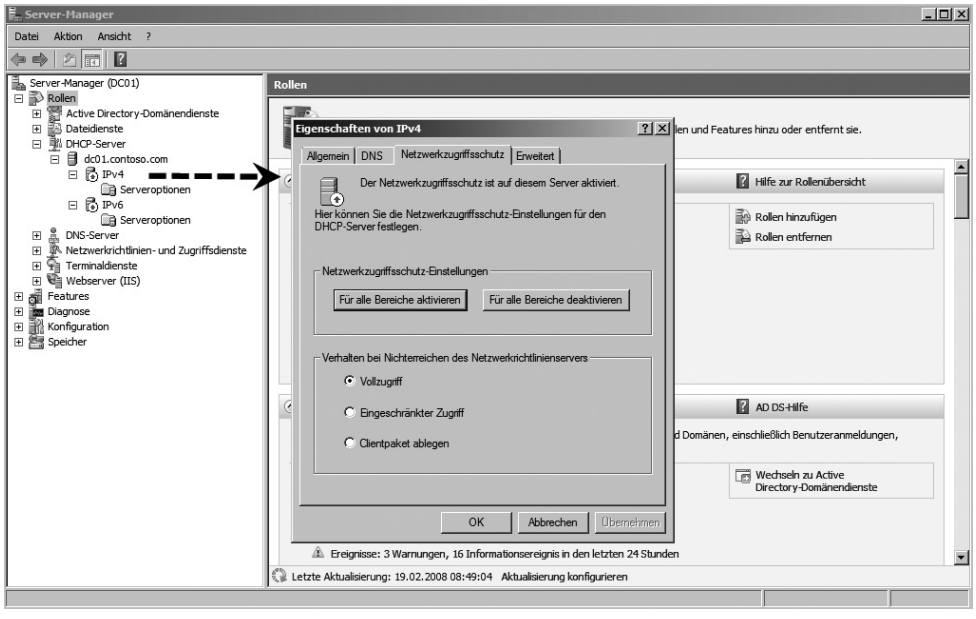
Komponenten der NAP

NAP unterstützt verschiedene Funktionsweisen und die damit verbundenen Komponenten, um das Netzwerk zu schützen. Folgende Verbindungsvarianten können von NAP geschützt werden. Diese Komponenten werden von Microsoft auch als *Enforcement Components* bezeichnet. Auch eine Kombination der Zugangsmethoden wird unterstützt:

- **IPSec-Kommunikation** Verwenden Sie IPSec, bekommen NAP-konforme Clients ein Zertifikat und können anschließend mit anderen IPSec-Computern kommunizieren. Entspricht ein Client nicht den Richtlinien, erhält er auch kein Zertifikat und kann mit anderen IPSec-geschützten Computern nicht kommunizieren. Für das Ausstellen dieser Zertifikate ist der NAP-Server zuständig. Für diese Funktion benötigen Sie nicht unbedingt eine eigene PKI (Public Key-Infrastruktur). Die Komponente in NAP, die dieses Zertifikat ausstellt, trägt die Bezeichnung *Health Registration Authority (HRA)*. Bei den Zertifikaten handelt es sich um standardmäßige X.509-Zertifikate. Bei der NAP-geschützten IPSec-Kommunikation findet folgende Kommunikation statt. Diese Kommunikation findet analog auch bei den anderen Enforcement Components statt:
  - **a.** Der Client sendet seine Anforderung an die IPSec Enforcement Component. Der Client verwendet dazu entweder HTTP oder HTTPS (kann auch über die Gruppenrichtlinien gesteuert werden).
  - **b.** Diese sendet den Statement of Health des Clients (SoH) an die HRA.
  - **c.** Die HRA sendet die Anfrage an den Netzwerkrichtlinienserver (Network Policy Server, NPS).
  - **d.** Der NPS gibt den Status an den HRA zurück, ob der Client konform ist oder nicht verweist den Client zusätzlich an die notwendigen Wartungsserver, zum Beispiel einen Server mit WSUS 3.0, von dem der Client aktuelle Patches ziehen kann.
  - **e.** Ist der Client NAP-konform, teilt die HRA ein Zertifikat zu.
  - **f.** Ist der Client nicht konform, erhält er kein Zertifikat, sondern die Anforderung sich mit dem Wartungsserver zu verbinden.
  - **g.** Der Client sendet eine Updateanforderung an den Wartungsserver, wenn er nicht NAP-konform ist.
  - **h.** Nach der Aktualisierung sendet der Client erneut seinen SoH an den HRA.
- **IEEE 802.1x Verbindungen** IEEE 802.1x ist ein Standard zur Authentifizierung in Netzwerken. Der Standard beschreibt die Zuordnung von zwei logischen Ports (*Controlled*, *Uncontrolled*) zu einem physischen Port. Der physische Port leitet die empfangenen Pakete an den *Uncontrolled* Port. Der *Controlled* Port kann nur nach erfolgreicher Authentifizierung erreicht werden. Nicht konforme Geräte werden durch das IEEE 802.1x-Gerät (zum Beispiel eine Switch) blockiert oder in ein spezielles virtuelles LAN (VLAN) verschoben.
- **RAS- oder VPN-Einwahl** Bei dieser Methode wählen sich PCs über das Internet oder per DFÜ ins Netzwerk ein und werden auf NAP-Konformität überprüft. Unter Windows Server 2003 haben Sie für diese Funktion noch die Quarantäne-Lösung verwendet. Diese wird in Windows Server 2008 durch NAP ersetzt und ist deutlich effizienter und leichter zu konfigurieren.

- **TS Gateway** Ein TS Gateway verbindet mehrere Terminalserver über HTTP/RDP-Kommunikation mit dem Internet. Diese Funktion ist neu in Windows Server 2008. Auch diese Verbindungen werden durch NAP geschützt (siehe Kapitel 12).
- **DHCP-Server** Nicht-konforme NAP-Clients können am Beziehen einer IP-Adresse durch einen DHCP-Server gehindert werden. Alternativ erhalten die Clients spezielle IP-Adresse und kein Standardgateway. DHCP-Server unter Windows Server 2008 haben bei der Konfiguration eines Bereiches für die Verwaltung von NAP eine zusätzliche Registerkarte, bei der Sie die NAP-Unterstützung aktivieren können. Sie können auf dieser Registerkarte auch Profile auf dem Bereich und den NPS miteinander verbinden. So lassen sich auf Basis unterschiedlicher Subnetze Profile auf dem NPS zuweisen.

Abbildg. 15.4 Aktivieren des Netzwerkzugriffsschutzes (NAP) für einen DHCP-Bereich



HINWEIS **Cisco und NAP**

Das Cisco-Pendant zu Microsoft Network Access Protection (NAP) mit der Bezeichnung Cisco Network Admission Control (NAC) arbeitet mit NAP zusammen. Es gibt gemeinsame Produkttest und die Entwicklung findet Hand in Hand statt. Sie können in NAP-Lösungen auch NAC-Komponenten von Cisco integrieren und umgekehrt. Der NAP-Client in Windows Vista unterstützt auch Cisco NAC. Für Cisco NAC muss daher kein zusätzlicher Client installiert werden. Auch die Cisco-EAP (Extensible Authentication Protocol)-Module werden durch Windows Update unterstützt. Neben Cisco arbeiten auch zahlreiche andere Unternehmen mit NAP zusammen (zum Beispiel Nortel, Juniper). Eine ausführliche Liste finden Sie auf der Internetseite *www.microsoft.com/nap*. Ausführliche Informationen zur NAP/NAC-Interoperatibilität finden Sie im Whitepaper *http://download.microsoft.com/download/c/1/2/c12b5d9b-b5c5-4ead-a335-d9a13692abbb/TNC_NAP_white_paper.pdf*. Die Interoperabilität sieht folgendermaßen aus:

1. Der Client sendet seinen Statement of Health (SoH) an den Cisco Secure Access Control Server (ACS).
2. Der ACS sendet den SoH an den Netzwerkrichtlinienserver (Network Policy Server, NPS) weiter. Dabei wird das Host Credential Authorization Protocol (HCAP) verwendet.
3. Auf Basis der Richtlinien des NPS wird der Zugriff des Clients gesteuert.

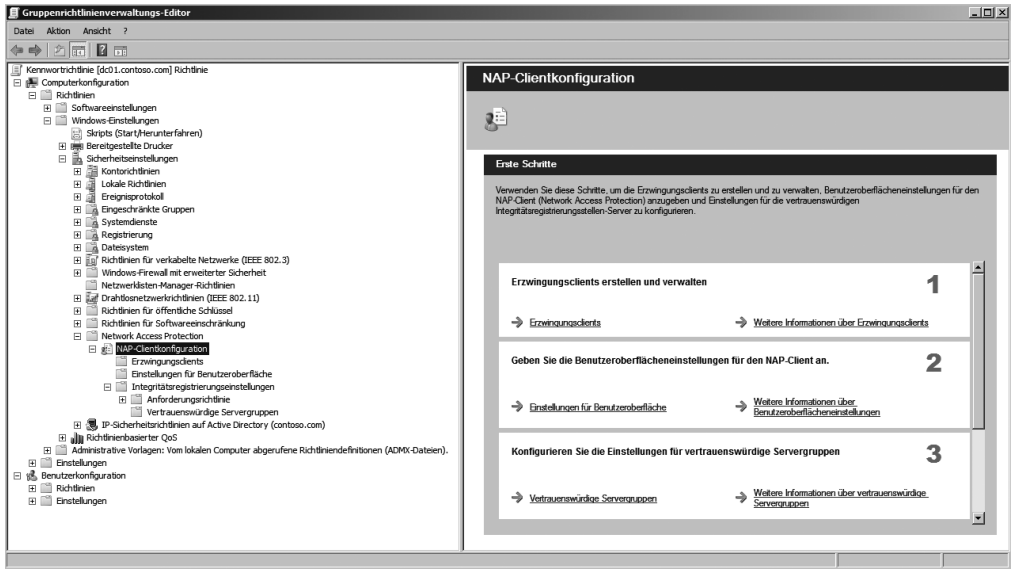
Erste Schritte mit NAP

In diesem Abschnitt werden die ersten Schritte im Umgang mit NAP erläutert. In den weiteren Abschnitten dieses Kapitels gehen wir dann ausführlicher auf die einzelnen Funktionen in NAP ein.

Verwaltung von Clients zur Unterstützung von NAP

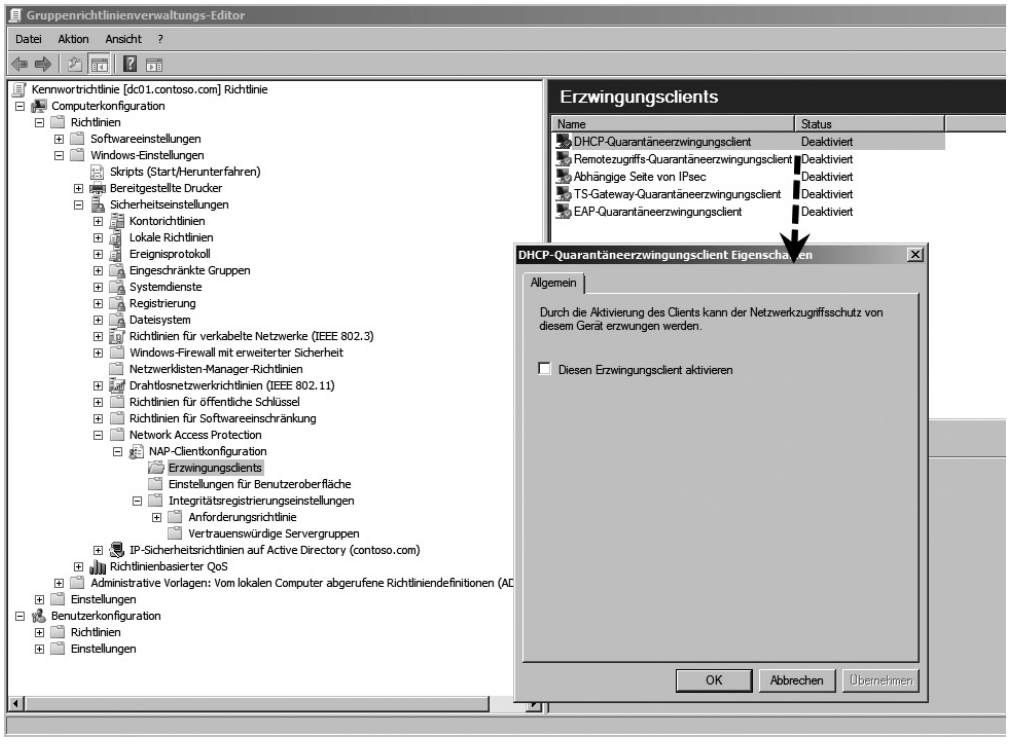
Standardmäßig unterstützen Windows Vista-Clients NAP. Für Windows XP und Windows Server 2003 gibt es einen Client, der gesondert installiert werden muss. Die clientseitige Konfiguration von NAP führen Sie am besten über Gruppenrichtlinien durch. Die Einstellungen hierfür finden Sie in der Gruppenrichtlinienverwaltung unter *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Network Access Protection* (Abbildung 15.5).

Abbildg. 15.5 Konfiguration der NAP-Clients über Gruppenrichtlinien



Über diese Einstellungen können Sie das Verhalten der Clientcomputer konfigurieren. Hier können Sie zum Beispiel die einzelnen Clients für NAP für die einzelnen Funktionen aktivieren oder deaktivieren.

Abbildg. 15.6 Aktivierung der NAP-Clients über Gruppenrichtlinien



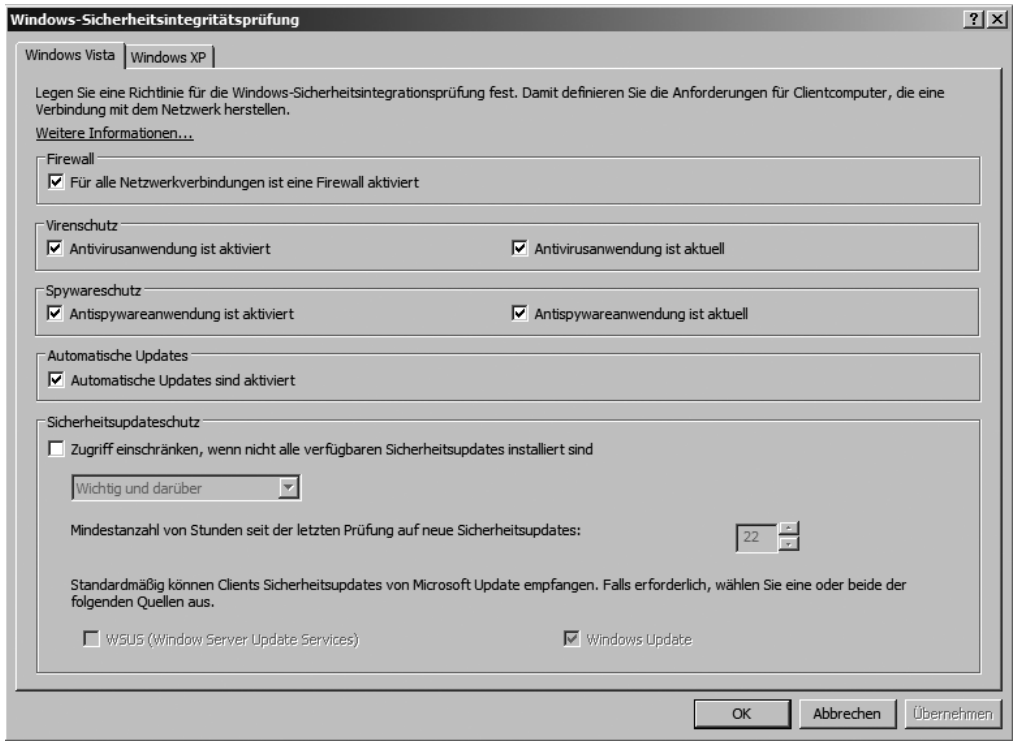
Verwalten der Serverkomponenten von NAP

Die Servereinstellungen von NAP führen Sie entweder über den Server-Manager durch. Sie finden die Konfiguration des Netzwerkrichtlinienservers über *Rollen/Netzwerkrichtlinien- und Zugriffsdienste*. Alternativ können Sie diese Konfiguration auch über *Start/Verwaltung/Netzwerkrichtlinienserver* aufrufen oder noch schneller über *Start/Ausführen/nps.msc*.

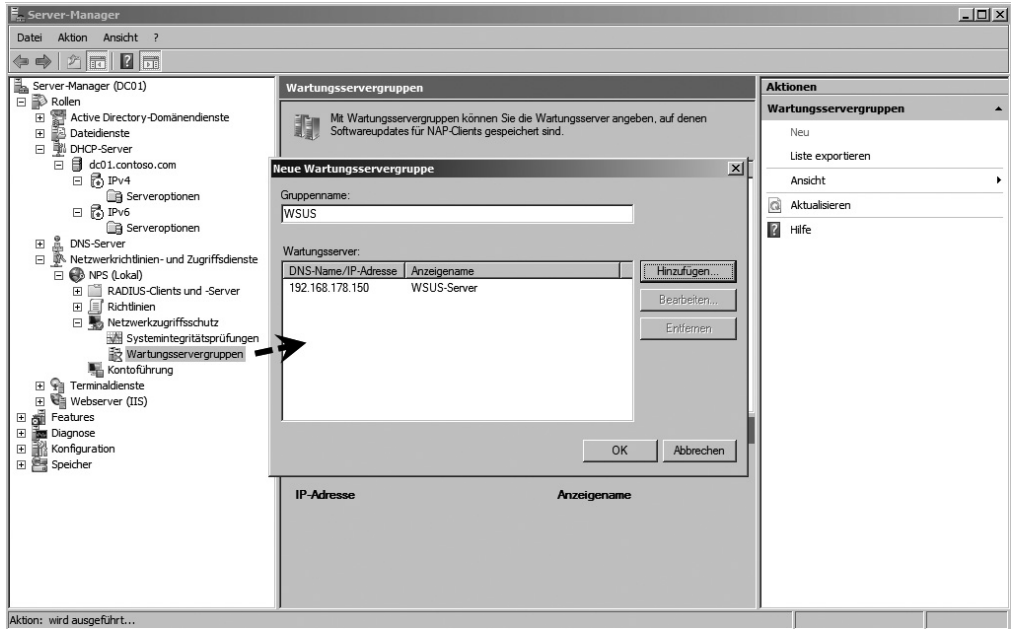
Festlegen der Systemintegritätsprüfung

Die Verwaltung baut zunächst auf die *Sicherheitsintegritätsprüfung* auf. Diese ruft von den Clients das *Statement of Health (SoH)* ab. Diese Einstellungen finden Sie in der Verwaltungskonsole über *NPS/Netzwerkzugriffsschutz/Systemintegritätsprüfungen*. Rufen Sie in der Mitte diese Eigenschaften der Verifizierungsmethode auf, zum Beispiel von der standardmäßigen vorhandenen *Windows-Sicherheitsintegritätsverifizierung*. Hier können Sie über die Schaltfläche *Konfigurieren* die Einstellungen festlegen, welche die Clients erfüllen müssen, um mit NAP in Ihrem Netzwerk konform zu sein. Diese Systemintegritätsprüfungen bezeichnet Microsoft auch als *Security Health Agents (SHA)*. Der SHA wird in Windows Vista durch den *Windows Security Health Validator (SHV)* verbunden. Hauptsächlich überprüfen diese SHAs den Zustand des Windows-Sicherheitscenters in Windows Vista und XP.

Abbildg. 15.7 Konfigurieren der Sicherheitsintegritätsverifizierung



Abbildg. 15.8 Festlegen von Wartungsservern für NAP

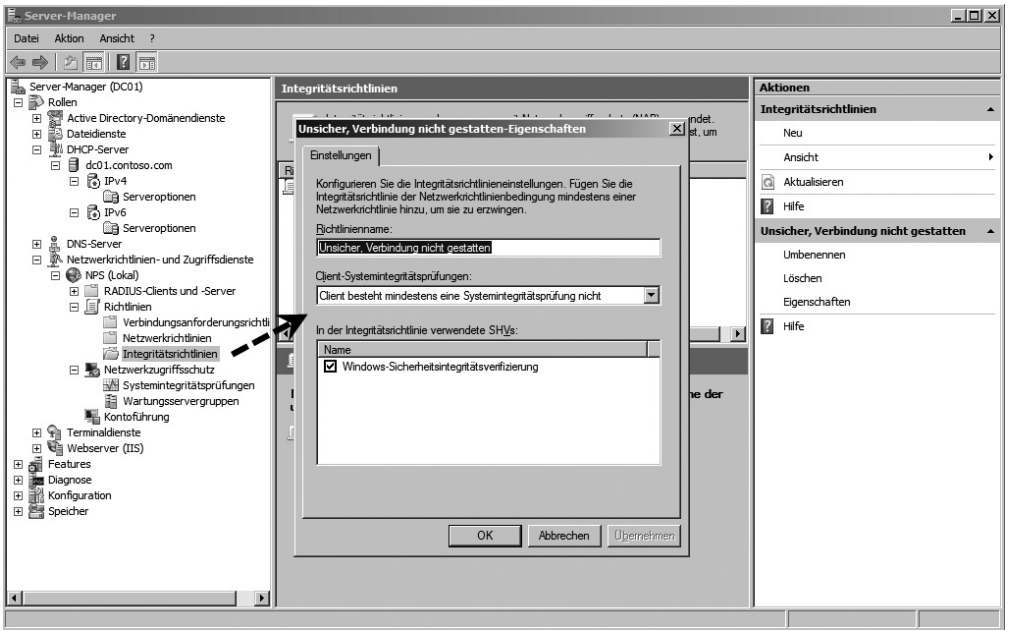


Über den Konsoleneintrag *Wartungsservergruppen* (Remediation Server) hinterlegen Sie die DNS-Namen oder IP-Adressen von Servern, über die nicht konforme Clients mit Updates versorgt werden können. Auf diese Server greifen nicht konforme Clients bei der Netzwerkverbindung zu und können sich mit den notwendigen Patches versorgen.

Verwalten der Integritätsrichtlinien

Über den Konsoleneintrag *NPS/Richtlinien/Integritätsrichtlinien* legen Sie schließlich Richtlinien fest, auf deren Basis bestimmt wird, was mit Clients passieren soll, die konform sind oder nicht. Hier legen Sie fest, wann die Richtlinie angewendet werden soll, also ob der Client eine vorher festgelegte Systemintegritätsüberprüfung besteht oder nicht. Zusätzlich legen Sie hier fest, welche Systemintegritätsprüfung Sie als Basis für die Integritätsrichtlinie verwenden. Sinn dieser Einstellung ist es, eine Richtlinie für konforme und eine Richtlinie für nicht konforme PCs festzulegen und auf welcher Basis diese Konformität überprüft werden soll.

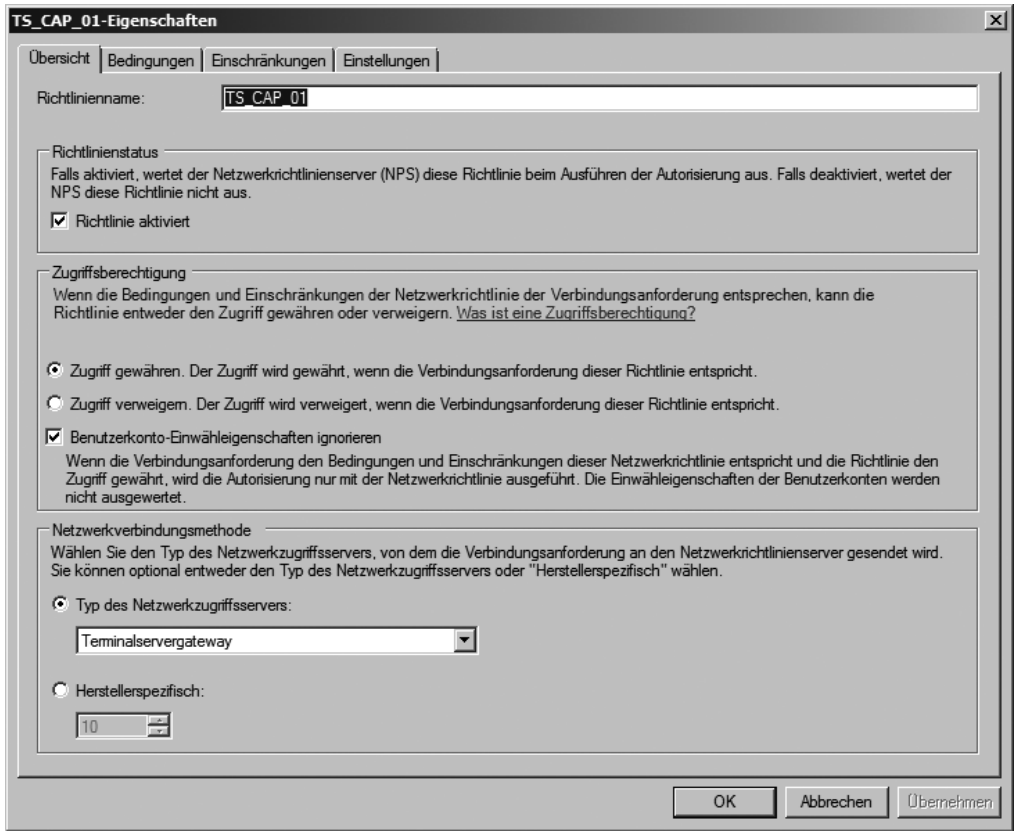
Abbildg. 15.9 Verwalten der Integritätsrichtlinien



Verwalten der Netzwerkrichtlinien

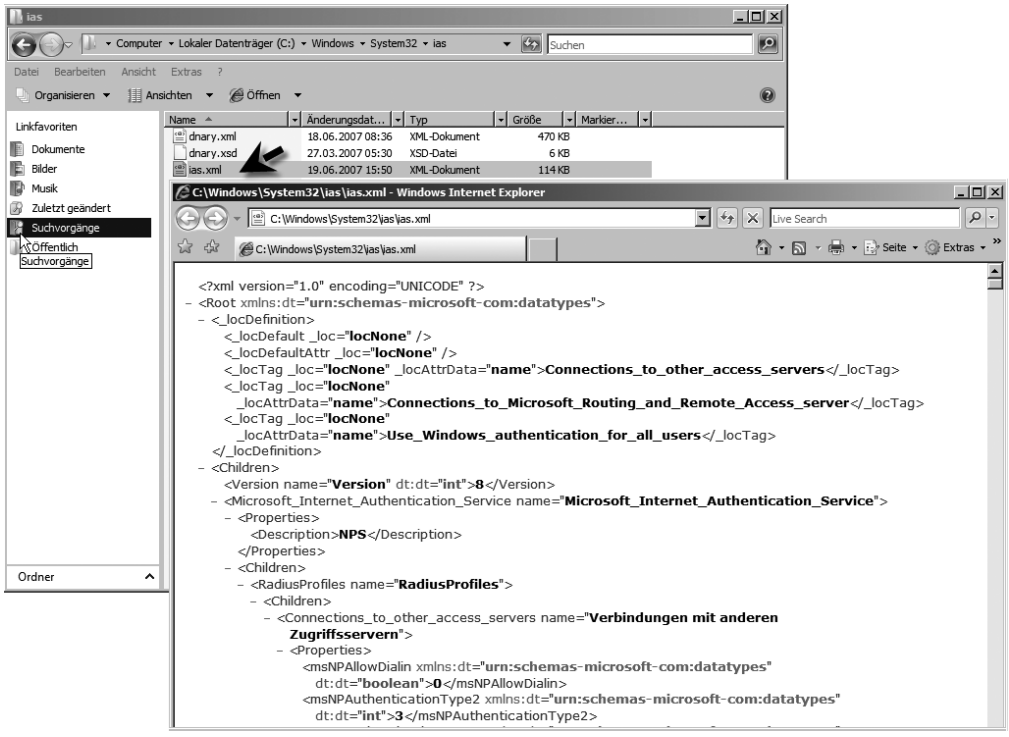
Nachdem Sie die Einstellungen in der jeweiligen Systemintegritätsprüfung definiert haben, die ein Computer erfolgreich übermitteln muss, legen Sie eine Integritätsrichtlinie fest, die entscheidet, auf welcher Systemintegritätsüberprüfung festgemacht wird, ob ein Client konform oder nicht konform ist. Clients werden also einer dieser Richtlinien zugewiesen. Zusätzlich macht es vor allem bei einer Übergangszeit Sinn, eine weitere Integritätsrichtlinie festzulegen, in der Clients aufgenommen werden, die NAP nicht unterstützen. Als Nächstes erstellen Sie eine Netzwerkrichtlinie, die auf Basis der Integritätsrichtlinie basiert. In der Netzwerkrichtlinie steuern Sie schließlich, was mit den konformen beziehungsweise nicht konformen Clients passieren soll (siehe hierzu auch Kapitel 12 und Abbildung 15.10).

Abbildg. 15.10 Konfigurieren der Netzwerkrichtlinie auf Basis der Integritätsrichtlinie



TIPP Die Konfiguration der Richtlinien wird als XML-Datei abgespeichert. Sie finden diese Konfiguration in der Datei *ias.xml* im Verzeichnis *\Windows\System32\ias* (Abbildung 15.11). Diese Datei können Sie im Fehlerfall zum Beispiel zu einem Microsoft-Experten schicken, der die Fehler dann effizienter auswerten kann. Die Logdateien für NAP-Clients finden Sie unter *\Windows\Tracing*.

Abbildg. 15.11 Anzeigen der Richtlinieninformationen des Netzwerkrichtlinienservers



Netzwerkzugriffsschutz (NAP) mit DHCP einsetzen

Microsoft empfiehlt den grundlegenden NAP-Schutz in einem Unternehmen über den DHCP-Server einzuführen. Über diese Möglichkeit erlangen Unternehmen den Vorteil der NAP ohne großartige Änderungen in der Infrastruktur. Der NAP-Schutz in DHCP ist zwar die unsicherste Variante des NAP-Schutzes (Clients könnten sich schließlich auch manuell eine IP-Adresse zuteilen), dafür aber auch die am schnellsten einführbare. In diesem Abschnitt zeigen wir Ihnen, wie Sie NAP zusammen mit DHCP einführen. Durch diesen Workshop vertiefen Sie auch die bisher erwähnten theoretischen Ausführungen zur NAP.

Vorbereitungen für den Einsatz von NAP mit DHCP

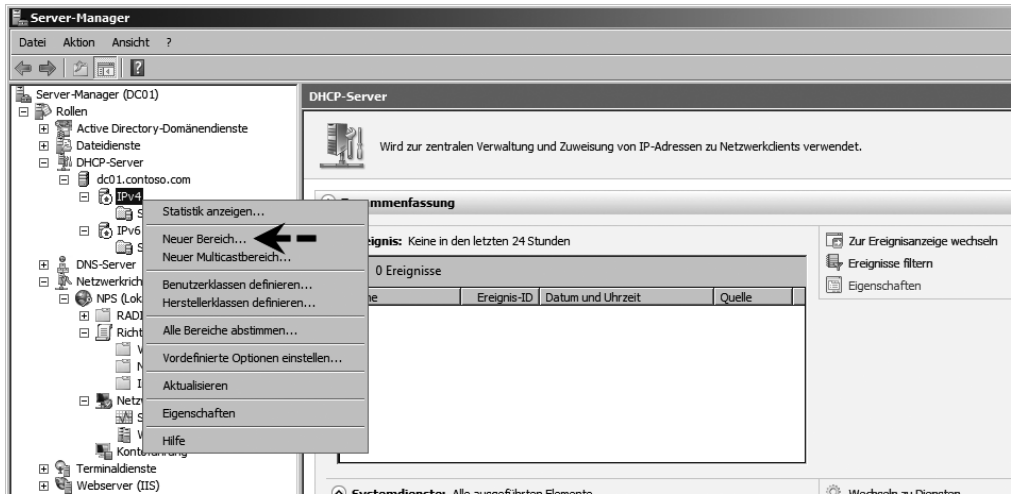
Damit Sie NAP mit DHCP einsetzen können, müssen Sie nicht unbedingt gleich die ganze Domäne auf Windows Server 2008 umstellen. Die Domänencontroller können ohne weiteres noch unter Windows Server 2003 laufen. Nur der DHCP- und der Netzwerkrichtlinienserver (NPS) muss unter Windows Server 2008 laufen. Installieren Sie auf dem Windows Server 2008 die DHCP- und die

Netzwerkrichtlinien und -Zugriffsdienste-Rolle. Als Client kommt derzeit nur Windows Vista in Frage. Der NAP-Client für Windows XP wird durch die Installation von Service Pack 3 für Windows XP integriert.

Konfiguration des DHCP-Bereiches für NAP-Unterstützung

Nachdem Sie DHCP auf dem Windows Server 2008 installiert haben, können Sie als Nächstes einen neuen Bereich erstellen. Geben Sie dem Bereich die Bezeichnung »NAP-Bereich« und weisen Sie diesem ein paar IP-Adressen zu. Einen neuen Bereich erstellen Sie, indem Sie das DHCP-Verwaltungsprogramm aufrufen (am besten über den Server-Manager). Klicken Sie mit der rechten Maustaste auf den DHCP-Server und wählen Sie im Kontextmenü den Befehl *Neuer Bereich* aus (Abbildung 15.12).

Abbildg. 15.12 Erstellen eines neuen DHCP-Bereiches für die Unterstützung von NAP über DHCP



Konfiguration des Netzwerkrichtlinienservers

Im nächsten Schritt werden die Einstellungen auf dem Netzwerkrichtlinienserver vorgenommen. Rufen Sie zur Verwaltung von NAP die dazugehörige Verwaltungskonsole auf. Am schnellsten starten Sie die Konsole über *Start/Ausführen/nps.msc*.

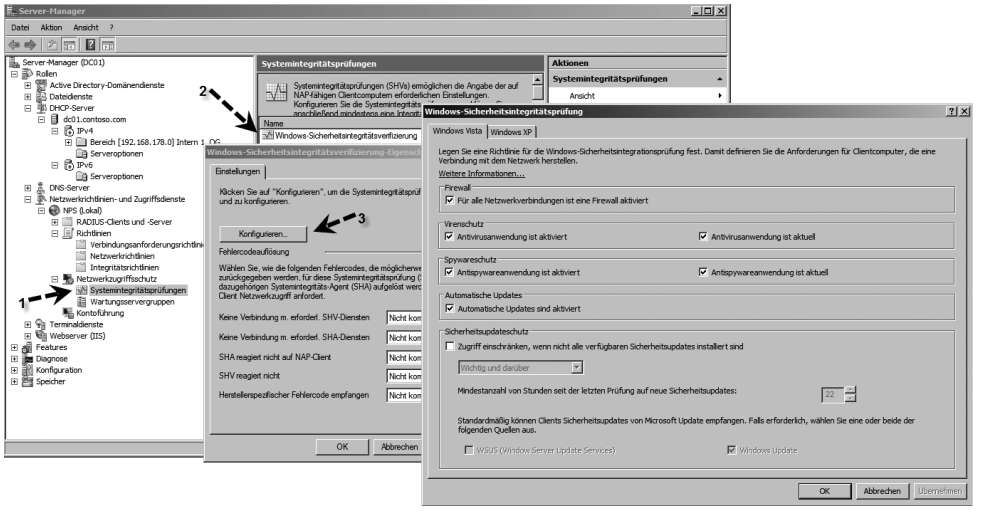
Verwalten der Systemintegritätsprüfungen

Der nächste Schritt besteht darin, dass Sie die Systemintegritätsprüfungen (System Health Validators, SHVs) konfigurieren:

1. Klicken Sie dazu in der NAP-Konsole auf *Netzwerkzugriffsschutz/Systemintegritätsprüfungen.*
2. Rufen Sie die Eigenschaften der *Windows-Sicherheitsintegritätsverifizierung* auf.

3. Klicken Sie im Fenster auf die Schaltfläche *Konfigurieren*. Jetzt können Sie festlegen, welche Bedingungen eine Arbeitsstation erfüllen muss, damit diese mit dem Netzwerk kommunizieren darf (Abbildung 15.13).
4. Deaktivieren Sie für diesen Test alle Kontrollkästchen außer *Für alle Netzwerkverbindungen ist eine Firewall aktiviert*.
5. Das Kontrollkästchen *Automatische Updates* können Sie ebenfalls aktiviert lassen. Hierüber wird konfiguriert, ob der Clients seine Patches von einem WSUS-Server erhält oder direkt aus dem Internet.

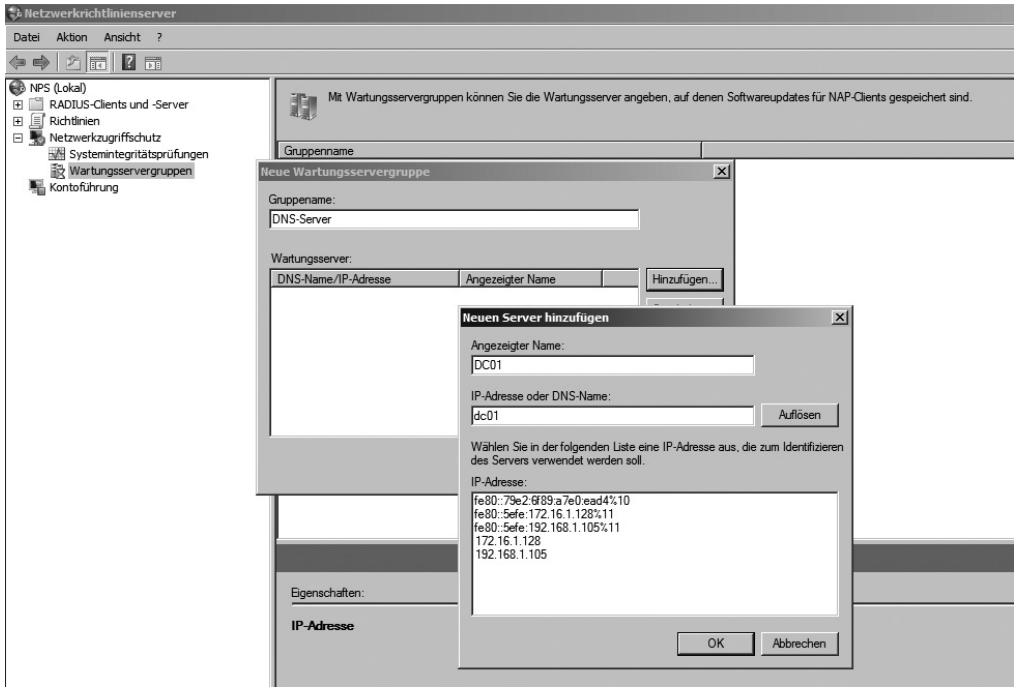
Abbildg. 15.13 Konfiguration der Windows-Sicherheitsintegritätsverifizierung



Konfiguration der Wartungsservergruppen

Wartungsserver (Remediation Server) sind Server, auf die Clients zugreifen können, wenn sie nicht NAP-konform sind. Hier tragen Sie die DNS-Namen oder IP-Adressen von Servern ein, mit denen nicht-konforme Clients kommunizieren dürfen. Das können entweder WSUS-Server oder ein FTP-Server sein, auf dem Sie Virensignaturen bereitstellen. In diesem Beispiel können Sie den Domänencontroller als Wartungsserver festlegen, damit nicht-konforme NAP-Clients Zugriff auf DNS haben. Sie können zu Testzwecken eine neue Gruppe erstellen und den Domänencontroller hinterlegen, der auch DNS bereitstellt. Klicken Sie dazu mit der rechten Maustaste auf den Konsoleneintrag *Wartungsservergruppen*, rufen Sie den Kontexmenübefehl *Neu* auf und hinterlegen Sie die Daten des DNS-Servers (Abbildung 15.14).

Abbildg. 15.14 Erstellen einer neuen Wartungsservergruppe



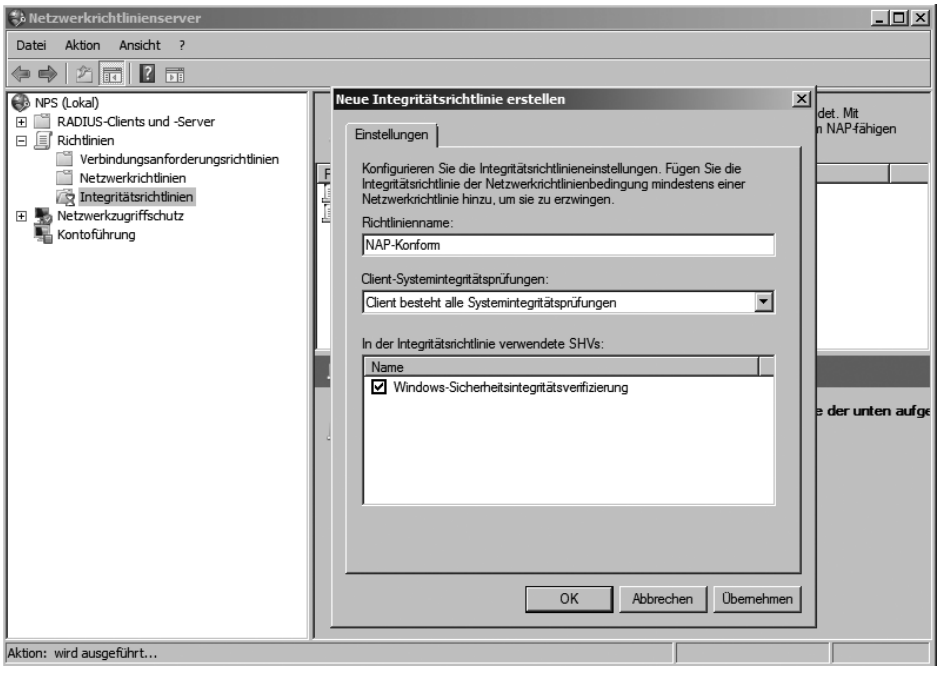
Erstellen der Integritätsrichtlinien

Der nächste Schritt besteht darin, dass Sie eine Integritätsrichtlinie (Health Policy) erstellen, die als Grundlage die Systemintegritätsprüfung (SHV) verwendet. Integritätsrichtlinien haben die Aufgabe, Clients in konforme und nicht-konforme NAP-Clients zu unterscheiden. Clients, welche die Systemintegritätsprüfung bestehen, sind konform, Clients, die diese Prüfung nicht bestehen, sind nicht konform. Aus diesem Grund werden meist zwei Integritätsrichtlinien erstellt:

- Eine Richtlinie, die den Client konform erklärt, wenn die Systemintegritätsprüfung bestanden wird
- Eine Richtlinie, die den Client als nicht-konform erklärt, wenn die Systemintegritätsprüfung nicht bestanden wird

1. Klicken Sie zur Erstellung einer Integritätsrichtlinie mit der rechten Maustaste auf *Richtlinien/Integritätsrichtlinien* und wählen Sie im Kontextmenü den Befehl *Neu*.
2. Geben Sie der Richtlinie die Bezeichnung *NAP-Konform*.
3. Stellen Sie sicher, dass im Listenfeld *Client-Systemintegritätsprüfen* der Eintrag *Client besteht alle Systemintegritätsprüfungen* ausgewählt ist.
4. Aktivieren Sie das Kontrollkästchen *Windows-Sicherheitsintegritätsverifizierung*.
5. Klicken Sie auf *OK*, damit die Richtlinie erstellt wird.

Abbildg. 15.15 Erstellen einer neuen Integritätsrichtlinie



6. Erstellen Sie eine weitere Integritätsrichtlinie.
7. Geben Sie dieser die Bezeichnung *Nicht-NAP-Konform*.
8. Wählen Sie im Listenfeld den Eintrag *Client besteht mindestens eine Systemintegritätsprüfung nicht* aus.
9. Aktivieren Sie wiederum das Kontrollkästchen *Windows-Sicherheitsintegritätsverifizierung*.

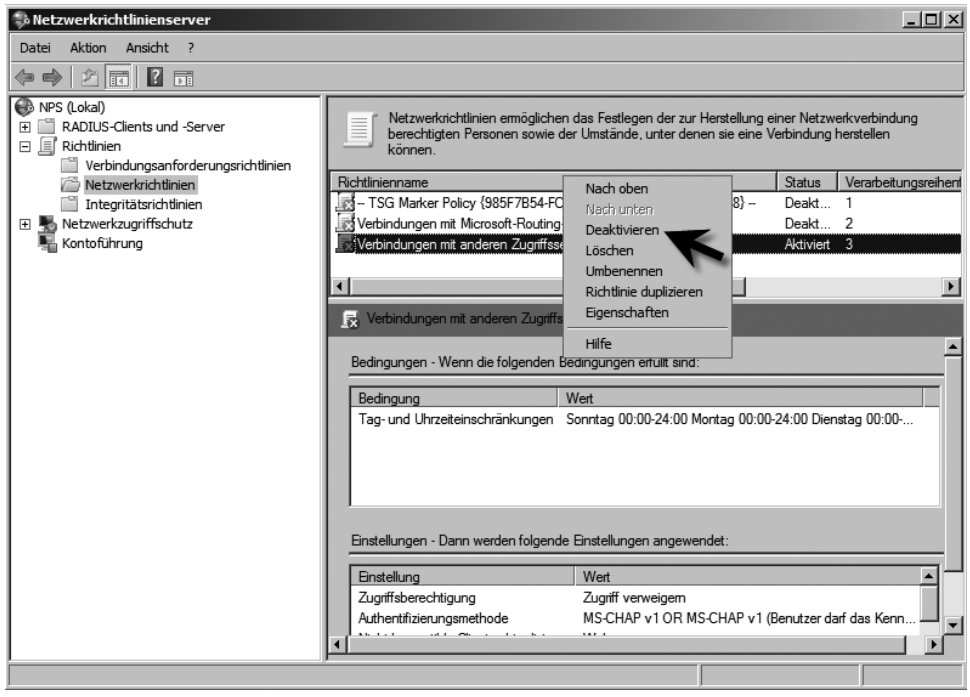
Erstellen der Netzwerkrichtlinien

Netzwerkrichtlinien (Network Policies) steuern den Netzwerkzugriff von Clients basierend auf Integritätsrichtlinien (Health Policies), die wiederum auf den Systemintegritätsprüfungen (System Health Validators, SHVs) aufbauen. Nachdem Sie die Systemintegritätsprüfung festgelegt haben, in denen konfiguriert ist, welche Bedingungen ein NAP-konformer-Client erfüllen muss, wird mit den Systemrichtlinien festgelegt, ob ein Client NAP-konform noch Nicht-NAP-konform ist. Die Netzwerkrichtlinien steuern wiederum, was mit NAP-konformen bzw. Nicht-NAP-konformen Clients im Netzwerk passieren soll und welchen Zugriff diese erhalten dürfen. Die NAP-Infrastruktur basiert daher auf den drei Pfeilern:

- Systemintegritätsprüfungen (System Health Validators)
- Integritätsrichtlinien (Health Policies)
- Netzwerkrichtlinien (Network Policies)

Bevor Sie neue Richtlinien erstellen, sollten Sie zunächst die standardmäßig angelegten Richtlinien deaktivieren. Klicken Sie diese dazu mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Deaktivieren* aus (Abbildung 15.16).

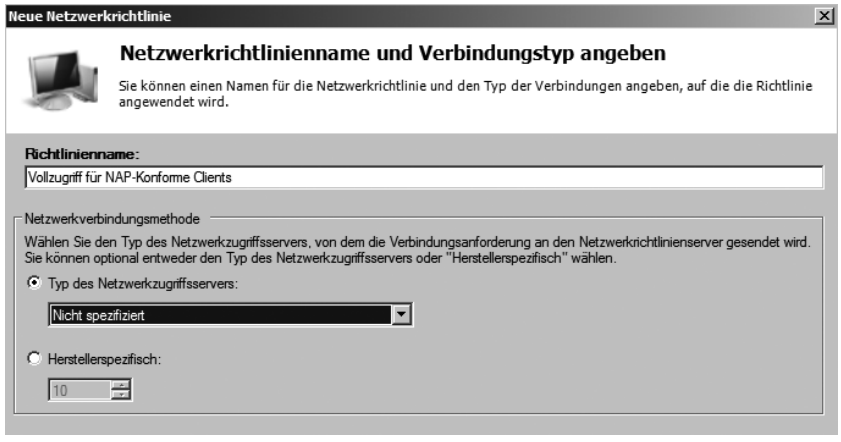
Abbildg. 15.16 Deaktivieren von Standard-Richtlinien



Erstellen der Netzwerkrichtlinie für konforme NAP-Clients

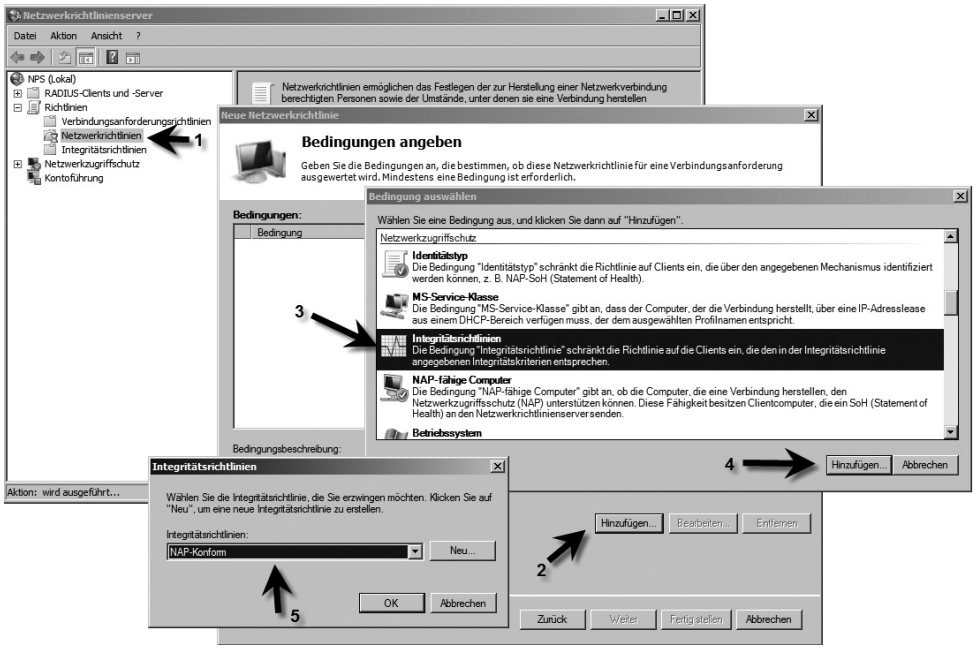
1. Im ersten Schritt erstellen Sie die Netzwerkrichtlinie für konforme Clients.
2. Klicken Sie dazu mit der rechten Maustaste auf den Konsoleneintrag *Richtlinien/Netzwerkrichtlinien* und wählen Sie im Kontextmenü den Befehl *Neu* aus.
3. Geben Sie der Richtlinie eine Bezeichnung in der Form *Vollzugriff für NAP-Konforme Clients* und klicken Sie auf *Weiter* (Abbildung 15.17).

Abbildg. 15.17 Erstellen einer neuen Netzwerkrichtlinie für NAP-konforme Clients



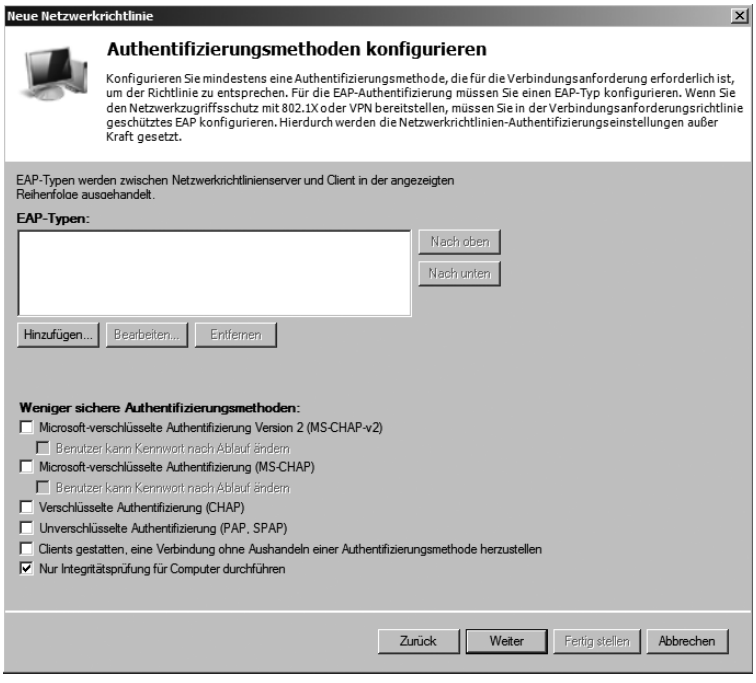
4. Klicken auf der nächsten Seite *Bedingungen angeben* auf *Hinzufügen*.
5. Wählen Sie als Option *Integritätsrichtlinien* aus (Abbildung 15.18).
6. Klicken Sie auf *Hinzufügen*.
7. Wählen Sie die Richtlinie *NAP-Konform* aus.

Abbildg. 15.18 Festlegen der erstellten Integritätsrichtlinie für die Netzwerkrichtlinie

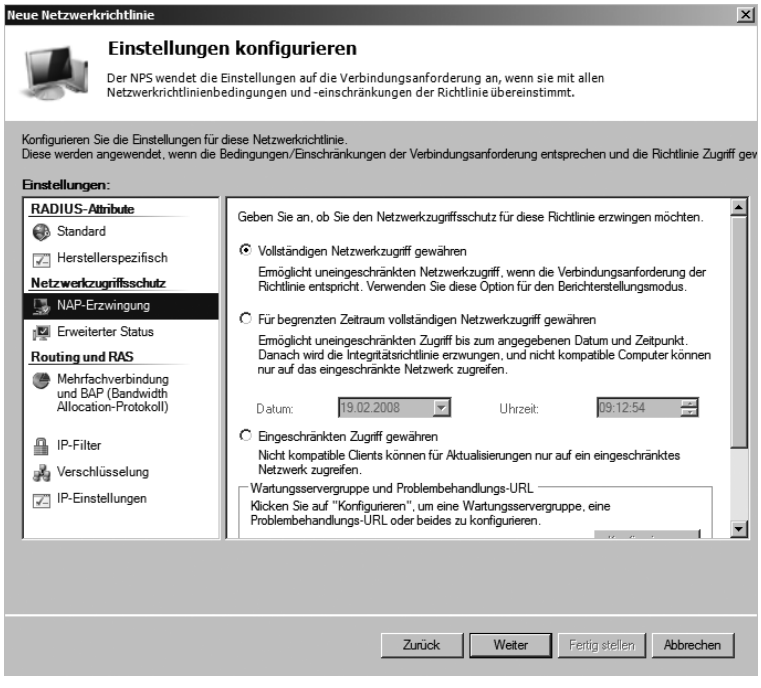


8. Auf der nächsten Seite des Fensters legen Sie den Netzwerkzugriff der Richtlinie fest. Wählen Sie hier *Zugriff gewährt* aus.
9. Klicken Sie auf *Weiter*, um zum Fenster *Authentifizierungsmethoden konfigurieren* zu gelangen (Abbildung 15.19).
10. Deaktivieren Sie die Standardeinstellungen und aktivieren Sie noch die Option *Nur Integritätsprüfung für Computer durchführen*.
11. Klicken Sie auf *Weiter* und belassen Sie im nächsten Fenster alle Einstellungen wie sie sind. Auf diesem Fenster legen Sie die Einschränkungen fest.
12. Klicken Sie im Fenster *Einschränkungen konfigurieren* ebenfalls auf *Weiter*. Sie gelangen auf das Fenster *Einstellungen konfigurieren*.
13. Klicken Sie hier auf *NAP-Erzwingung* und stellen Sie sicher, dass die Option *Vollständigen Netzwerkzugriff gewähren* aktiviert ist (Abbildung 15.20).
14. Klicken Sie nach der Einstellung auf *Weiter* und schließen Sie die Erstellung der Richtlinie ab.

Abbildg. 15.19 Festlegen der Authentifizierungsoptionen für die Netzwerkrichtlinie



Abbildg. 15.20 Konfigurieren der NAP-Erzwingung für Clients

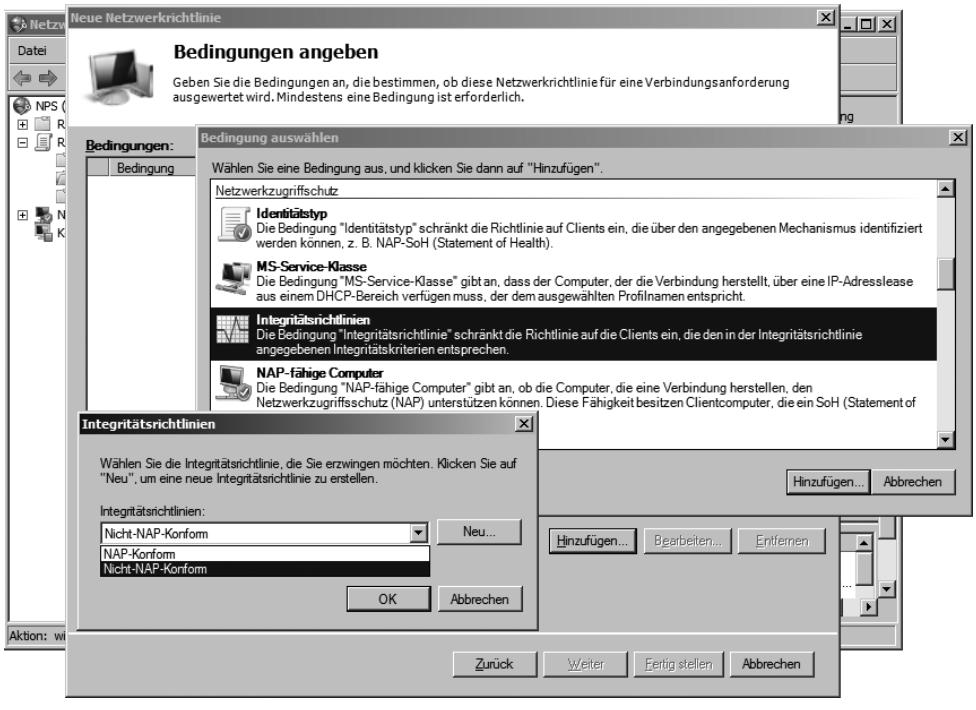


Erstellen der Netzwerkrichtlinie für Nicht-konforme NAP-Clients

Nachdem Sie die Richtlinie für konforme NAP-Clients erstellt haben, müssen Sie als Nächstes eine Netzwerkrichtlinie erstellen, die den Netzwerkzugriff für Nicht-konforme Clients steuert.

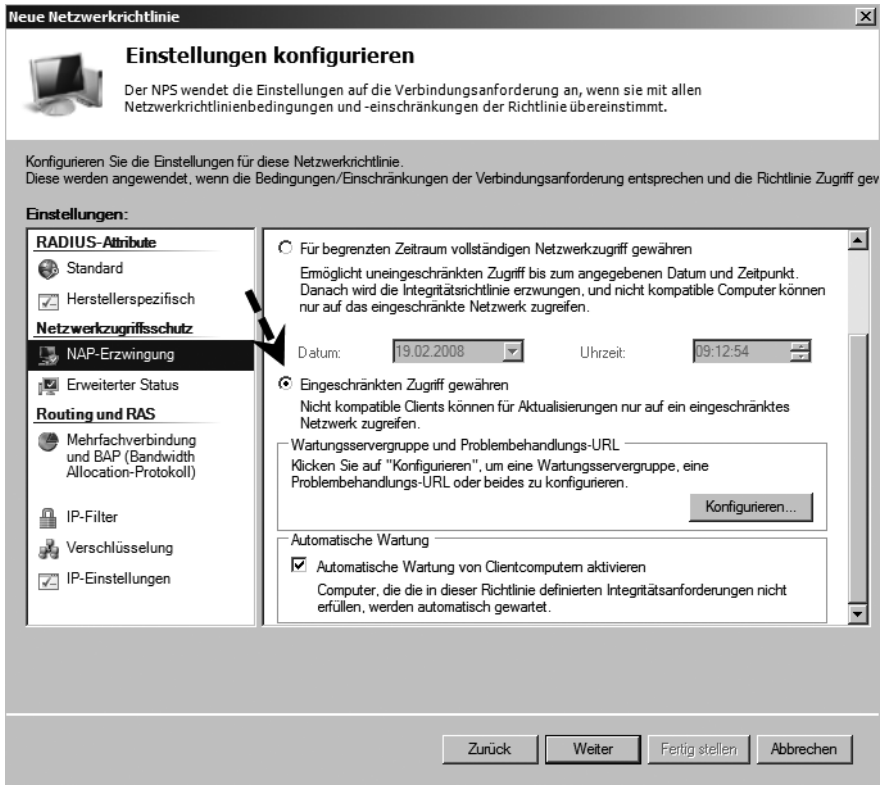
1. Gehen Sie zur Erstellung analog vor und weisen Sie der Richtlinie eine passende Bezeichnung zu.
2. Wählen Sie diesmal als Integritätsrichtlinie die Richtlinie *Nicht-NAP-Konform* aus (Abbildung 15.21).
3. Auf der Seite *Zugriffsberechtigungen angeben* wählen Sie auch hier *Zugriff gewähren*. Der Zugriff wird später noch eingeschränkt. Natürlich könnten Sie für sich auch die Option *Zugriff verweigert* auswählen, um den Clients die komplette Kommunikation zu untersagen. Allerdings sperren Sie in diesem Fall die Clients komplett aus dem Netzwerk aus.
4. Klicken Sie auf *Weiter*, um zum Fenster *Authentifizierungsmethoden konfigurieren* zu gelangen.
5. Deaktivieren Sie die Standardeinstellungen und aktivieren Sie noch das Kontrollkästchen *Nur Integritätsprüfung für Computer durchführen*.

Abbildg. 15.21 Hinterlegen der Integritätsrichtlinie für Nicht-konforme NAP-Clients



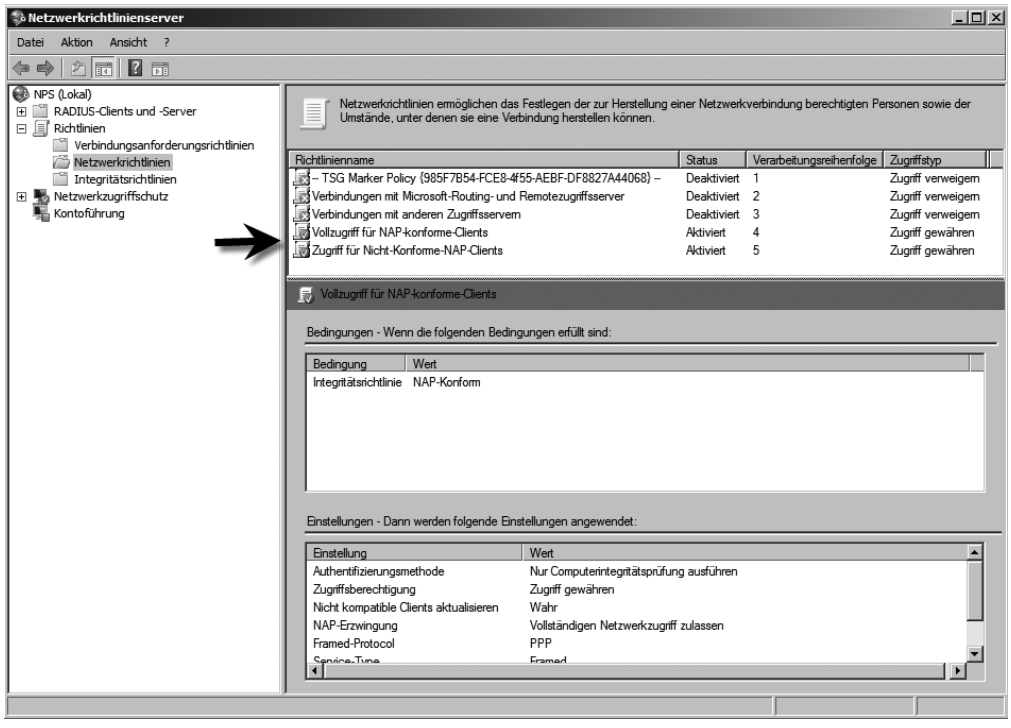
6. Klicken Sie auf *Weiter*, um zur Seite *Einschränkungen konfigurieren* zu gelangen. Klicken Sie auch hier auf *Weiter*, um zur Seite *Einstellungen konfigurieren* zu gelangen.
7. Klicken Sie auf *NAP-Erzwingung*.
8. Aktivieren Sie die Option *Eingeschränkten Zugriff gewähren*.
9. Aktivieren Sie das Kontrollkästchen *Automatische Wartung von Clientcomputern aktivieren* (Abbildung 15.22).

Abbildg. 15.22 Steuerung des Netzwerkzugriffs für Nicht-konforme NAP-Clients



Schließen Sie die Erstellung der Netzwerkrichtlinien ab. Diese werden nach der Erstellung in der NPS-Konsole angezeigt. Alle anderen Richtlinien sollten als deaktiviert angezeigt werden (Abbildung 15.23).

Abbildg. 15.23 Anzeigen der Netzwerkrichtlinien für das Netzwerk

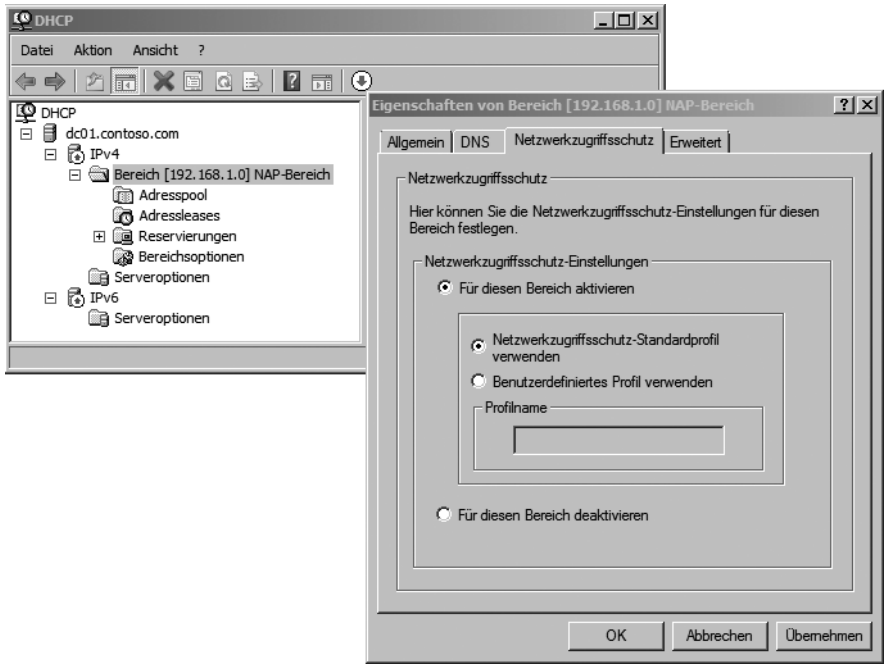


Konfigurieren des DHCP-Servers für NAP

Im nächsten Schritt müssen Sie den DHCP-Server unter Windows Server 2008 konfigurieren, damit dieser NAP nutzen kann. Rufen Sie die Verwaltungskonsole des DHCP-Servers auf. Sie finden die Konsole über *Start/Verwaltung/DHCP* oder im Server-Manager. Auch über *Start/Ausführen/dhcpmgmt.msc* können Sie die Konsole aufrufen. Um DHCP für NAP zu konfigurieren, gehen Sie folgendermaßen vor:

1. Rufen Sie die Eigenschaften des Bereiches auf, den Sie zuvor erstellt haben.
2. Wechseln Sie auf die Registerkarte *Netzwerkzugriffsschutz* (Abbildung 15.24).
3. Aktivieren Sie die Option *Für diesen Bereich aktivieren*.
4. Aktivieren Sie die Option *Netzwerkzugriffsschutz-Standardprofil verwenden*.

Abbildg. 15.24 Konfigurieren von NAP für einen DHCP-Bereich

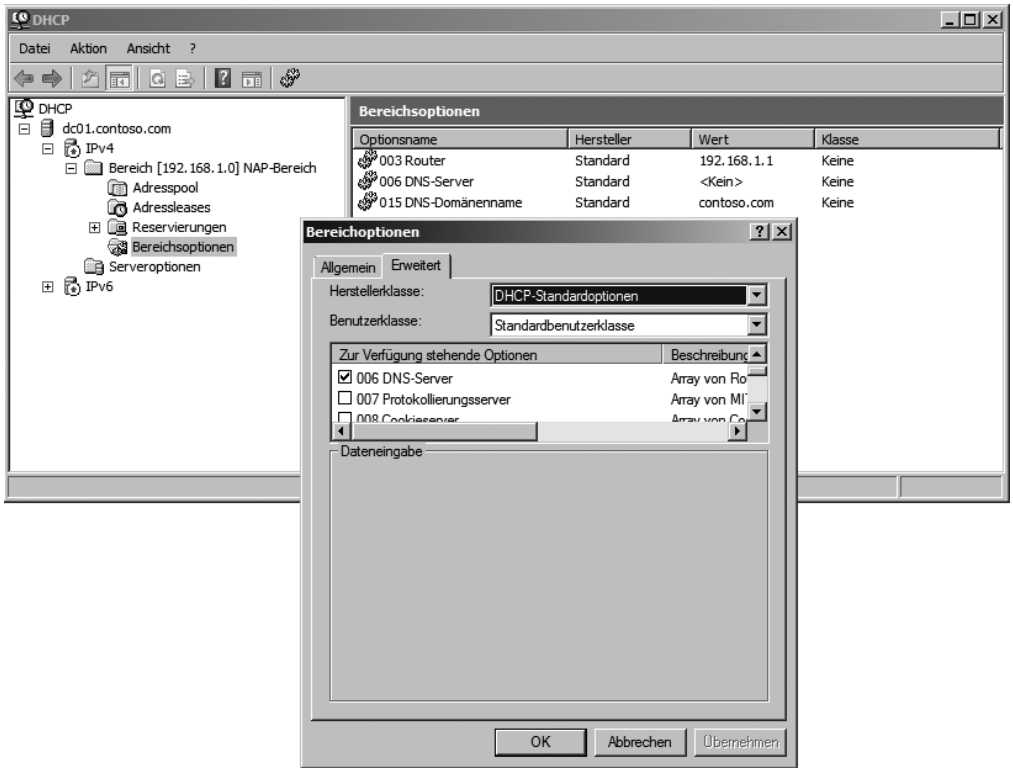


Konfigurieren des DHCP-Servers für konforme NAP-Clients

Im nächsten Schritt können Sie den DHCP-Server so konfigurieren, dass NAP-konforme Clients eine IP-Adresse vom Server erhalten. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf den Konsoleneintrag *Bereichsoptionen* unterhalb des von Ihnen erstellten Bereiches und wählen Sie *Optionen konfigurieren* aus.
2. Wechseln Sie auf die Registerkarte *Erweitert*.
3. Wählen Sie im Dropdownlistenfeld *Benutzerklasse* die Option *Standardbenutzerklasse* aus.
4. Jetzt können Sie die Optionen auswählen, die Ihren standardmäßigen NAP-konformen Clients zugewiesen werden sollen, zum Beispiel DNS-Server, WINS und DNS-Domäne.

Abbildg. 15.25 Konfigurieren der Bereichsoptionen für NAP-konforme Clients



Konfigurieren des DHCP-Servers für Nicht-konforme NAP-Clients

Im nächsten Schritt müssen Sie den DHCP-Server so konfigurieren, dass Nicht-konforme NAP-Clients entsprechende IP-Adressen erhalten, damit sich diese mit den Wartungsservern verbinden können bzw. nur teilweise mit dem Netzwerk kommunizieren können. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf den Konsoleneintrag *Bereichsoptionen* unterhalb des von Ihnen erstellten Bereiches und wählen Sie *Optionen konfigurieren* aus.
2. Wechseln Sie auf die Registerkarte *Erweitert*.
3. Wählen Sie im Dropdownlistenfeld *Benutzerklasse* die Option *Standardmäßige Netzwerkzugriffsschutz-Klasse* aus.
4. Wählen Sie die Option *006 DNS-Server* aus und hinterlegen Sie die IP-Adresse Ihres DNS-Servers.
5. Wählen Sie die Option *015 DNS-Domänenname* aus und hinterlegen Sie als Namen einen DNS-Namen, zum Beispiel *restricted.contoso.com*.
6. Durch diese Konfiguration haben Sie sichergestellt, dass die konformen NAP-Clients eine vollständige Anbindung an das Netzwerk erhalten und die nicht-konformen eingeschränkten Zugriff.

Konfiguration des NAP-Clients

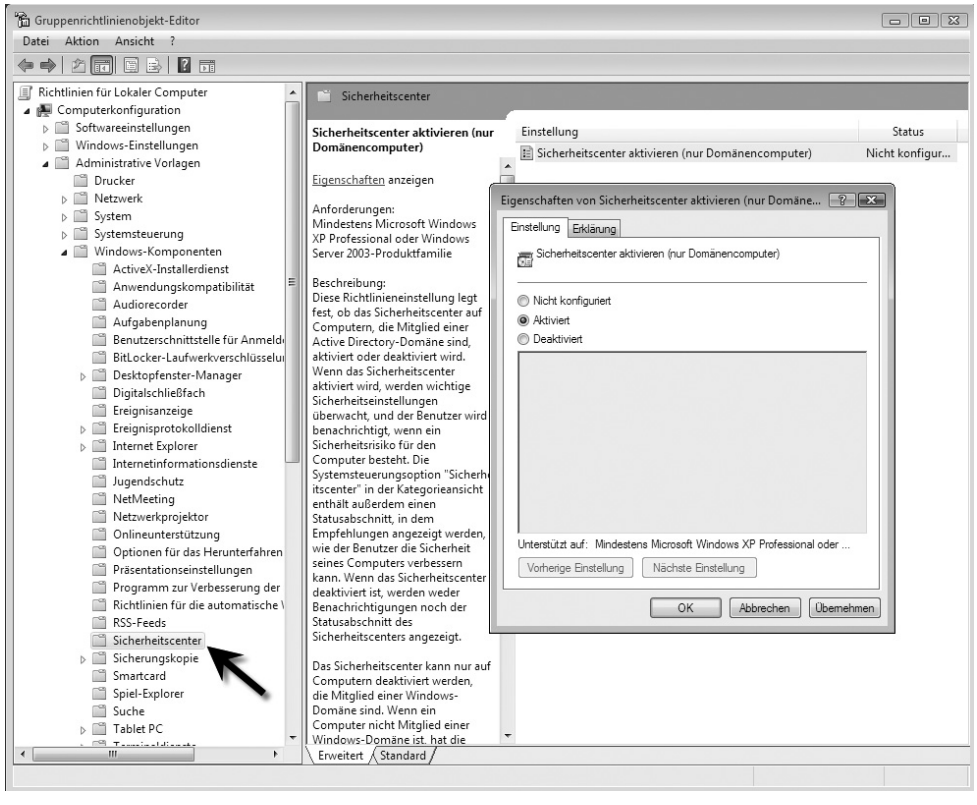
Damit die Windows-Sicherheitsintegritätsverifizierung unter Windows Server 2008 Daten empfangen kann, muss auf dem Windows Vista-PC das Sicherheitscenter aktiviert sein. Das Sicherheitscenter fragt die entsprechenden Daten auf dem PC ab und sendet diese zum NPS-Server.

Aktivieren des Sicherheitscenters auf Windows Vista-Domänen-PCs

Auf Windows Vista-PCs, die Mitglied einer Domäne sind, wird das Sicherheitscenter deaktiviert. Um NAP unter Windows Vista zu testen, müssen Sie dieses daher aktivieren. Der beste Weg dazu in einer Testumgebung ist die Aktivierung über lokale Richtlinien. Sie finden die Einstellung auch über Gruppenrichtlinien. Gehen Sie dazu folgendermaßen vor:

1. Geben Sie über *Start/Ausführen/gpedit.msc* ein.
2. Navigieren Sie zu *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Sicherheitscenter*.
3. Aktivieren Sie die Richtlinie *Sicherheitscenter aktivieren (nur Domänencomputer)* (Abbildung 15.26).

Abbildg. 15.26 Aktivieren des Sicherheitscenters in Windows Vista für die Unterstützung von NAP

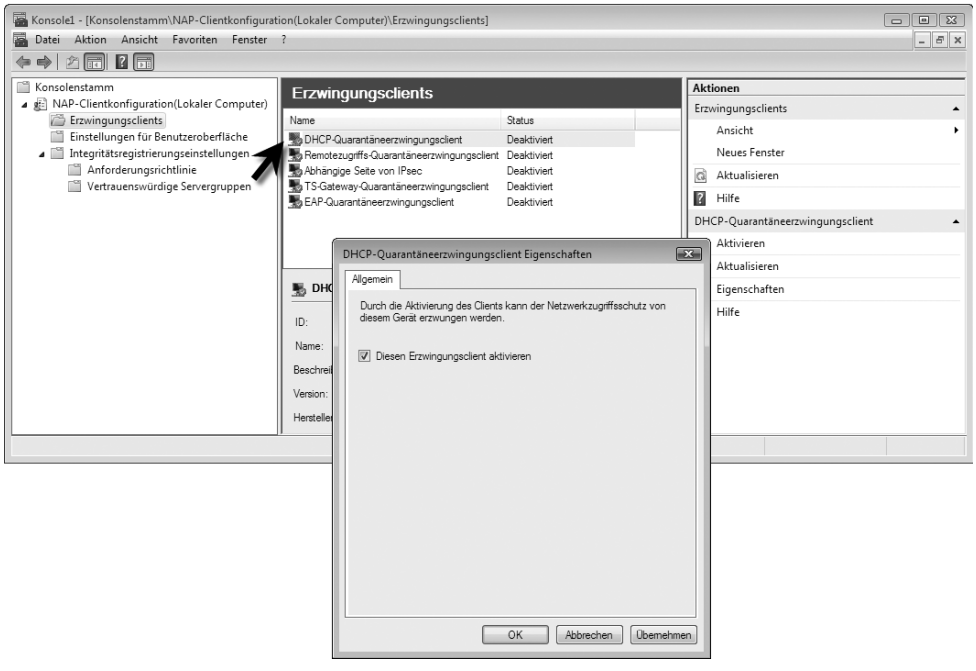


Aktivieren des DHCP-Quarantäneerzwingungsclients

Die nächste Aufgabe, die Sie durchführen müssen, ist die Aktivierung der DHCP-NAP-Unterstützung:

1. Starten Sie dazu auf dem Vista-PC über *Start/Ausführen/napclcfg.msc* die Verwaltungskonsole des NAP-Clients (Abbildung 15.27).
2. Klicken Sie in der Konsolenstruktur auf den Eintrag *Erzwingungsclients*.
3. Aktivieren Sie den *DHCP-Quarantäneerzwingungsclient*.

Abbildg. 15.27 Aktivieren des DHCP-Quarantäneerzwingungsclients unter Windows Vista



Alternativ können Sie Erzwingungsclients für den Netzwerkzugriffsschutz auch über Gruppenrichtlinien aktivieren. Diese Einstellung finden Sie unter *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Network Access Protection/NAP-Clientkonfiguration/Erzwingungsclients* (Abbildung 15.28).

Abbildg. 15.28 Aktivieren von Erzwingungsclients über Gruppenrichtlinien

NAP-Agent (Network Access Protection) aktivieren

Der nächste Schritt zur Anbindung von Windows Vista an eine NAP-Infrastruktur ist die Aktivierung des Systemdienstes *NAP-Agent (Network Access Protection)*. Setzen Sie nach Aufruf der *Dienste*-Konsole über *Services.msc* den Starttyp dieses Dienstes auf *Automatisch* und starten Sie diesen.

Windows Vista in Domäne aufnehmen

Nachdem Sie diese Konfigurationen vorgenommen haben, erhalten Sie durch den DHCP-Server eine IP-Adresse und können den Windows Vista-PC in die Domäne aufnehmen. In einem Unternehmensnetzwerk können die Hauptvorteile der Microsoft-Betriebssysteme, sei es auf Ebene der Server oder der Clients, erst sinnvoll ausgespielt werden, wenn eine Active Directory-Domäne gebildet wird.

HINWEIS Nur die Business-, Enterprise- und Ultimate-Edition von Windows Vista können Mitglied in Windows-Domänen werden, bei den anderen Editionen fehlt diese Unterstützung. Dies muss vor allem beim Erwerb von neuen Notebooks beachtet werden, die oft mit der Windows Vista Home Premium Edition verkauft werden. Diese Version ist nicht domänenfähig.

Notwendige Netzwerkeinstellungen für die Domänen-Aufnahme

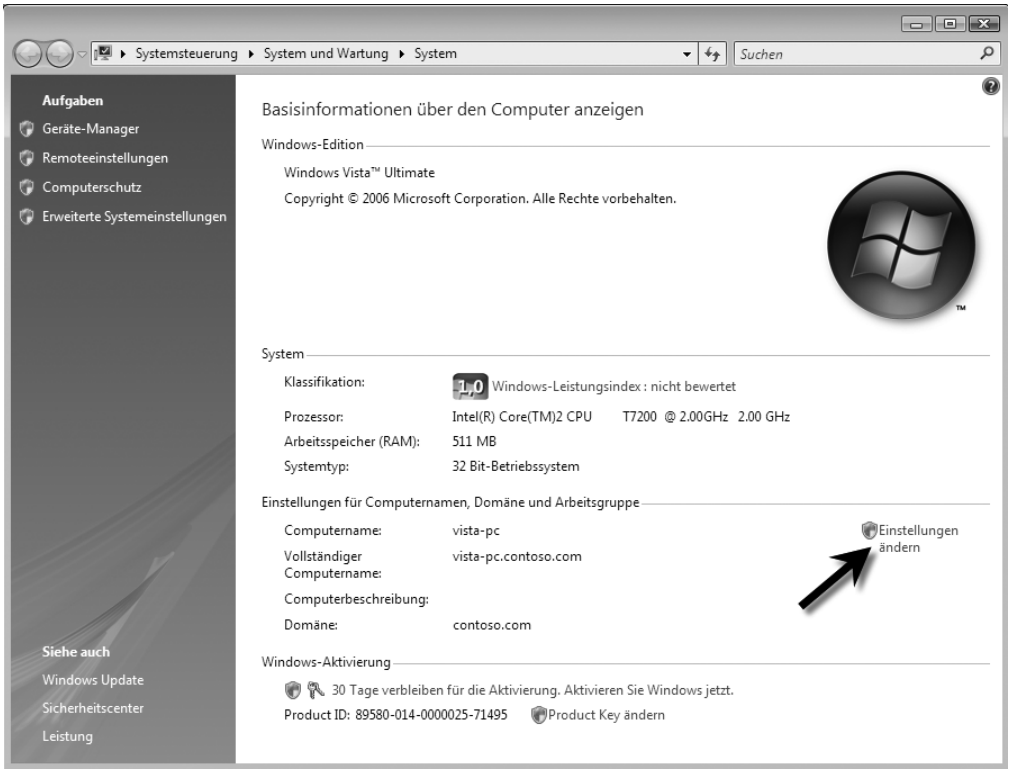
Grundsätzlich ist der Ablauf mit dem unter Windows XP nahezu identisch. Der erste Schritt, einen Windows Vista-PC in eine Windows-Domäne aufzunehmen, ist es, den PC erstmals mit dem Netzwerk zu verbinden und zu überprüfen, ob ein Domänencontroller mit dem Ping-Befehl, ganz ohne Namensauflösung erreicht werden kann. Der nächste wichtige Schritt ist das Eintragen eines DNS-Servers in den IP-Einstellungen eines Windows Vista-PCs. Erst wenn ein DNS-Server eingetragen

wurde, der die DNS-Zone der Active Directory-Domäne auflösen kann, ist eine Aufnahme in eine Windows-Domäne möglich. Bei der Verwendung von DHCP erhält der Windows Vista-PC die IPv4-Konfiguration durch den DHCP-Server.

Erstellen eines Computerkontos für den PC in der Domäne

Nachdem Sie die IP-Einstellungen korrekt vorgenommen haben, besteht der nächste Schritt darin, dass Sie für den PC in der Windows-Domäne ein Domänenkonto erstellen.

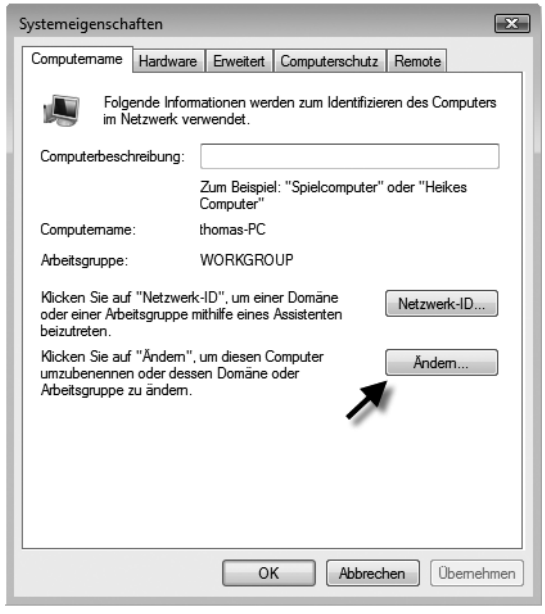
Abbildg. 15.29 Einstellungen zum Windows Vista-Computerkonto ändern



Dieses Konto kann ohne weiteres auch direkt auf dem Windows Vista-PC erstellt werden. Dazu ist lediglich eine Authentifizierung eines Benutzerkontos notwendig, welches berechtigt ist, Computerkonten in der Domäne zu erstellen. Um einen Windows Vista-PC in eine Windows-Domäne aufzunehmen, öffnen Sie am besten zunächst das Startmenü und klicken dann mit der rechten Maustaste auf den Menüpunkt *Computer* und wählen im zugehörigen Kontextmenü den Eintrag *Eigenschaften*. Es öffnet sich ein neues Fenster, über das Sie die Domänenmitgliedschaft des PCs anpassen können. Klicken Sie dazu im Abschnitt *Einstellungen für Computernamen, Domäne und Arbeitsgruppe* auf den Link *Einstellungen ändern*. Wie Sie sehen, wird neben dieser Einstellung das bekannte Schild in den Windows-Farben anzeigt. Dieses Symbol wird immer angezeigt, wenn für die Ausführung der besagten Aufgabe administrative Berechtigungen benötigt werden. Sobald Sie auf den Link *Einstellungen ändern* klicken, erscheint zunächst eine Meldung der Benutzerkontensteuerung (UAC), die

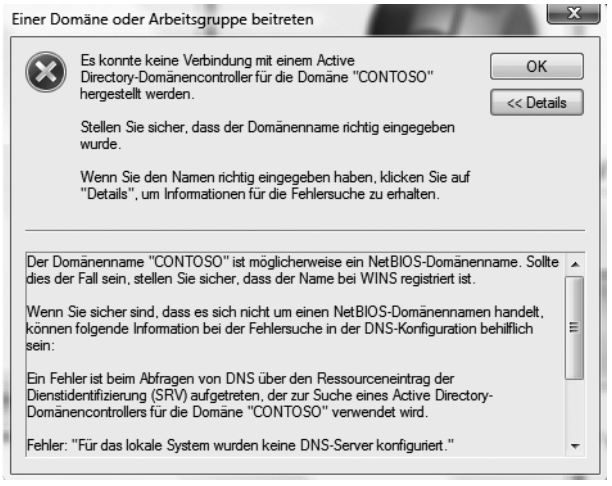
Sie bestätigen müssen. Nachdem Sie diese Meldung bestätigt haben, werden die Eigenschaften des Computers angezeigt und die Anzeige wechselt automatisch auf die Registerkarte *Computername*. Auf der Registerkarte *Computername* können Sie eine Beschreibung des PCs eintragen, die auch in den Verwaltungswerkzeugen von Active Directory angezeigt wird. Über die Schaltfläche *Ändern* können Sie am effizientesten einer Domäne beitreten oder den Namen des PC ändern.

Abbildg. 15.30 Aufnehmen eines Windows Vista-PC in eine Windows-Domäne



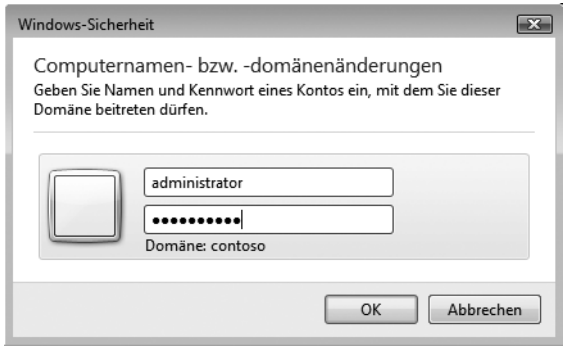
Über die Schaltfläche *Netzwerk-ID* wird ein Assistent gestartet, der Sie bei der Aufnahme unterstützt. Da die Domänenaufnahme keine allzu langwierige Aufgabe ist, benötigen Sie im Grunde genommen keinen Assistenten und können dadurch über die Schaltfläche *Ändern* schneller zum Ziel gelangen. Wichtig ist an dieser Stelle, dass Sie den Namen der Domäne eingeben, in die der PC aufgenommen wird. Das muss nicht immer genau die Domäne sein, in der sich auch Ihr Benutzerkonto befindet. Allerdings ist das unter Windows Server 2003 eigentlich immer so. Bei Domänen unter Windows NT 4.0 wurden Benutzerkonten und Ressourcen bzw. PCs in verschiedenen Domänen aufgenommen, was Sicherheitsgründe hatte, bzw. darin begründet lag, dass die maximale Anzahl von Objekten begrenzt war. Active Directory-Domänen haben in dieser Hinsicht keine Einschränkungen mehr, sodass Benutzerdomäne und Computerdomäne normalerweise immer identisch sind. Im Anschluss versucht der PC eine Verbindung zu der Domäne aufzubauen. Gelingt dies nicht, erscheint eine Fehlermeldung, die Sie detailliert darüber informiert, warum eine Domänenaufnahme nicht möglich ist.

Abbildg. 15.31 Fehlermeldung bei der Domänenaufnahme



Meistens liegt ein solcher Fehler darin begründet, dass der DNS-Server in den IP-Einstellungen nicht stimmt oder der PC keine Verbindung zum Domänencontroller herstellen kann, weil der Netzwerkverkehr blockiert wird oder die IP-Adresse des PCs nicht stimmt. Überprüfen Sie daher an dieser Stelle diese Einträge. Wenn Sie die beschriebenen Einstellungen ohne Assistent ändern wollen, klicken Sie auf die Schaltfläche *Ändern*. Es erscheint ein neues Fenster, in dem Sie den Namen Ihres PCs und die Domäne eintragen können, zu der Ihr PC eine Verbindung aufbauen soll. Tragen Sie an dieser Stelle am besten den NetBIOS-Namen der Domäne ein. Wenn Sie auf *OK* klicken, baut der PC Verbindung zur Domäne auf, und Sie müssen sich mit einem Benutzerkonto authentifizieren, welches Computerkonten in die Domäne aufnehmen darf. Sind alle Daten korrekt eingetragen worden, erhalten Sie eine Meldung, dass Sie der Domäne beigetreten sind. Nachdem Sie den erfolgreichen Beitritt zu der Windows-Domäne bestätigt haben, müssen Sie Ihren PC neu starten.

Abbildg. 15.32 Authentifizieren an der Windows-Domäne



Erste Anmeldung an der Windows-Domäne

Nachdem Ihr PC neu gestartet wurde, erhalten Sie die Meldung, dass Sie die Tastenkombination Strg+Alt+Entf auf der Tastatur drücken müssen, damit das Anmeldefenster erscheint. Diese Meldung wird aus Sicherheitsgründen angezeigt, damit auf PCs keine Trojaner oder Viren die Anmeldung der Domäne vortäuschen können, um an geheime Benutzerdaten zu gelangen. Erst wenn Sie diese Tastenkombination auf der Tastatur gedrückt haben, erscheint das bekannte Anmeldefenster von Windows Vista. Allerdings wird nicht unbedingt gleich die Anmeldung an der Domäne angezeigt. Nach der ersten Anmeldung am PC nach der Aufnahme in der Domäne wird unter Umständen noch der Anmeldename am lokalen PC angezeigt. Sie erkennen dies daran, dass Ihr Benutzernamen zusammen mit Ihrem PC-Namen angezeigt wird, was die lokale Anmeldung am PC symbolisiert. Sie können sich auch nach der Aufnahme in einer Domäne ohne weiteres lokal anmelden, erhalten dann aber ein anderes Benutzerprofil als mit dem Benutzerkonto in der Domäne. Klicken Sie auf die Schaltfläche *Benutzer wechseln* in der Anmeldemaske, erscheint eine neue Ansicht. Über die Auswahl der Option *Anderer Benutzer* können Sie ein Domänenkonto auswählen, mit dem Sie sich am PC anmelden können.

Abbildg. 15.33 Windows Vista an der Domäne anmelden

Geben Sie an dieser Stelle am besten im oberen Feld den Namen Ihrer Domäne gefolgt von einem Rückstrich (Backslash = \) und dann dem Benutzernamen und dem Kennwort des Domänenkontos an. Klicken Sie im Anschluss entweder auf das blaue Symbol mit dem Pfeil neben dem Kennwort oder auf der Tastatur auf *Return*, um die Anmeldung vorzunehmen. Im Anschluss authentifiziert sich der PC an der Domäne und ein ganz neues Benutzerprofil wird erstellt. Wenn Sie sich das nächste Mal am PC anmelden, hat sich der PC die Anmeldung an der Domäne gemerkt und zeigt diese auch in der Anmeldemaske an. An dieser Stelle reicht jetzt das Angeben des Kennwortes und Sie werden an der Domäne angemeldet. Wollen Sie sich an Ihrem PC lokal anmelden, wählen Sie einfach wieder die Schaltfläche *Benutzer wechseln* aus.

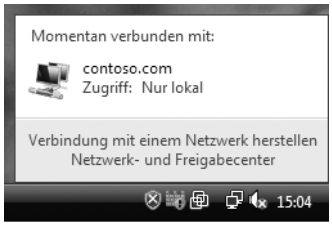
HINWEIS Das lokale Administratorkonto in Windows Vista wird deaktiviert. Einzige Ausnahme: Wenn Windows Vista während einem Upgrade von Windows XP erkennt, dass der Administrator das einzig aktive lokale Konto mit administrativen Berechtigungen ist, bleibt das Konto auch unter Vista aktiv. Solange auf Computern, die keiner Domäne angehören, weitere aktive administrative Konten existieren, kann der Administrator nicht im abgesicherten Modus genutzt werden. Stattdessen muss eines der normalen Konten zur Anmeldung verwendet werden. Wird allerdings das letzte lokale Konto mit administrativen Berechtigungen herabgestuft, gelöscht oder deaktiviert, kann der Administrator im abgesicherten Modus für ein Disaster Recovery genutzt werden.

Computer, die Mitglied einer Domäne sind, werden anders behandelt. Hier kann der standardmäßig deaktivierte lokale Administrator-Account nicht zur Anmeldung im abgesicherten Modus benutzt werden. Dadurch kann sich kein Standardbenutzer über diesen Weg lokal mehr Rechte verschaffen. Ein Mitglied der Gruppe der Domänen-Administratoren kann sich jedoch an jedem Domänenmitglieds-PC anmelden und dort lokale administrative Konten für die weitere Verwaltung erzeugen, falls keine existieren. Sollte sich kein Domänenadministrator angemeldet haben, muss der Computer im Falle eines Ausfalls im abgesicherten Modus mit Netzwerkzugriff gestartet werden, um darüber einen Domänenadministrator anmelden zu können. Dessen Anmeldung wird lokal nicht zwischengespeichert. Sollte der Computer allerdings aus der Domäne entfernt werden, tritt das Verhalten eines PCs wieder in Kraft, der nicht Mitglied einer Domäne ist.

Erste Schritte in der Windows-Domäne

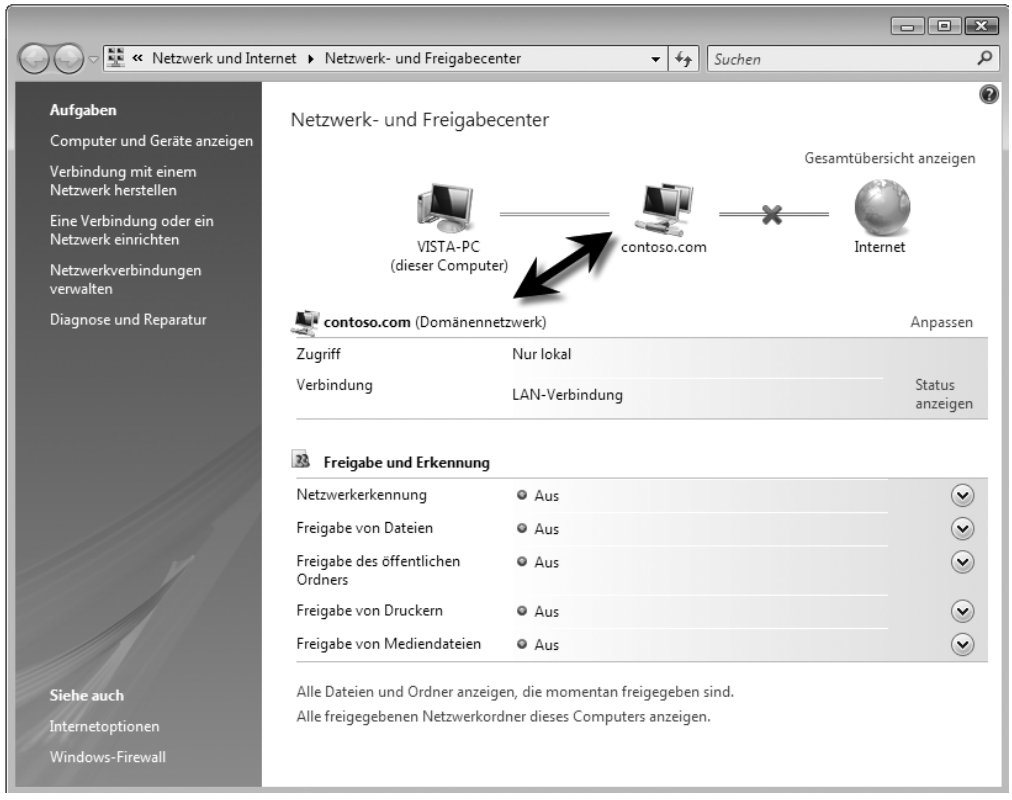
Wenn Sie sich an der Domäne angemeldet haben, können Sie über den bereits beschriebenen Weg die Eigenschaften des Computerkontos aufrufen. Sie erkennen am PC-Namen, dass dieser automatisch mit dem primären DNS-Suffix der Active Directory-Domäne ergänzt wurde. Außerdem sehen Sie auf der Registerkarte *Computername* zusätzlich, welcher Domäne Ihr PC beigetreten ist. Sie können die Domänenmitgliedschaft jederzeit wieder rückgängig machen und aus der Domäne austreten. Dazu können Sie den gleichen Weg verwenden, den Sie bereits zur Aufnahme in die Domäne durchgeführt haben. Anschließend können Sie überprüfen, ob die Domänen-Benutzergruppen in die lokalen Gruppen des PCs aufgenommen worden sind. Wenn ein PC in eine Domäne aufgenommen wird, wird automatisch die Gruppe *Domänen-Admins* in die lokale Gruppe *Administratoren* aufgenommen. Die Domänen-Benutzergruppe *Domänen-Benutzer* wird in die lokale Gruppe *Benutzer* aufgenommen. Sie können die lokale Benutzerverwaltung über *Start/Ausführen/lusrmgr.msc* aufrufen. Durch die Aufnahme dieser beiden Gruppen wird sichergestellt, dass zum einen die Administratoren der Domäne über administrative Berechtigungen auf dem PC verfügen und die Benutzerkonten der Domäne die Möglichkeit erhalten, sich an den einzelnen Arbeitsstationen der Domäne zu authentifizieren. Fahren Sie mit der linken Maustaste über das Netzwerksymbol im Infobereich der Taskleiste, wird Ihnen angezeigt, an welcher Domäne der PC angeschlossen ist (Abbildung 15.34).

Abbildg. 15.34 Anzeigen der Domänenmitgliedschaft eines PC



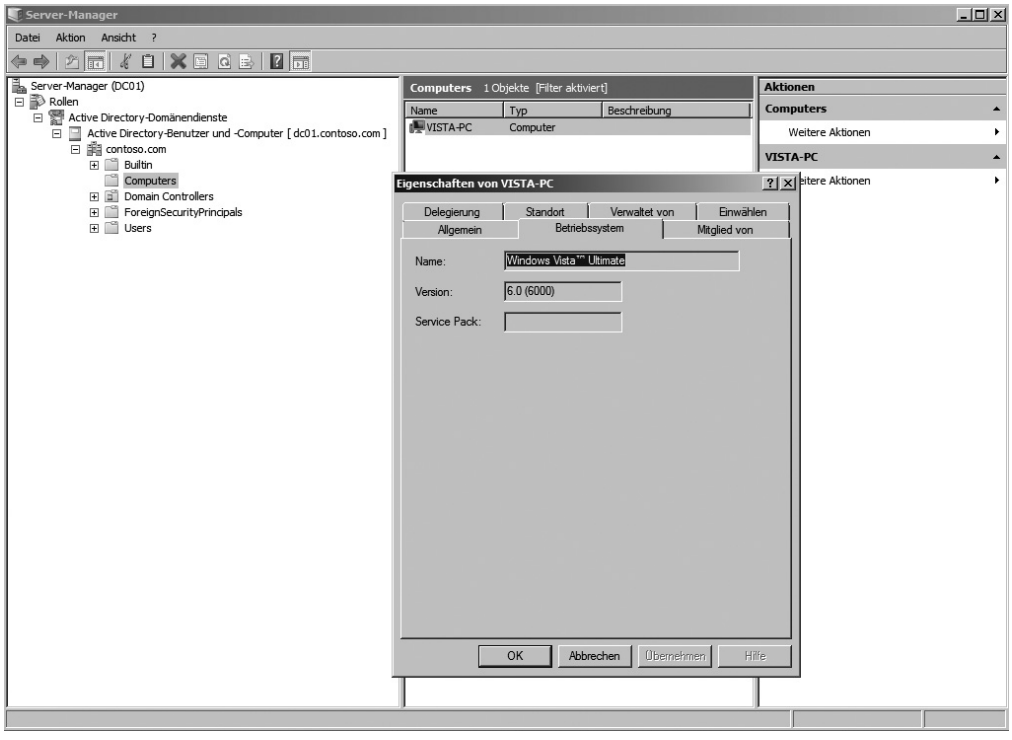
Hier wird Ihnen der DNS-Name der Domäne angezeigt. Öffnen Sie das Netzwerk- und Freigabecenter, wird die Verbindung zur Domäne angezeigt und zusätzlich die Netzwerkverbindung zum Domänennetzwerk erklärt (Abbildung 15.35). Innerhalb eines Domänennetzwerkes werden die automatischen Freigaben und die Erkennung der Freigaben für andere PCs zunächst standardmäßig deaktiviert.

Abbildg. 15.35 Überprüfen der Domänenmitgliedschaft eines Windows Vista-PCs



Rufen Sie auf dem Domänencontroller im Snap-In *Active Directory-Benutzer und -Computer* die Eigenschaften eines Windows Vista-PCs auf, können Sie sich auf der Registerkarte *Betriebssystem* auch die Edition anzeigen lassen, also ob es sich um die Business-, Enterprise- oder Ultimate-Edition handelt (Abbildung 15.36). Sie können dieses Snap-In auf dem Domänencontroller über den Server-Manager oder *Start/Ausführen/dsa.msc* aufrufen.

Abbildg. 15.36 Überprüfen der Computereigenschaften eines PCs



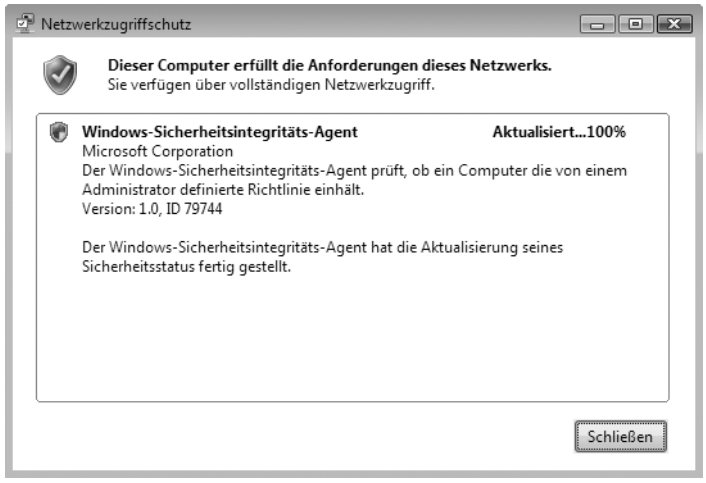
Überprüfung der NAP-Konfiguration

Durch die Einstellung in der Netzwerkrichtlinie, dass sich die angebundenen Windows Vista-PCs automatisch warten sollen, wenn diese nicht NAP-konform sind, wird die Windows-Firewall immer wieder in Echtzeit automatisch aktiviert, wenn Sie diese deaktivieren. Dadurch ist sichergestellt, dass auch auf PCs, an denen Benutzer mit Administratorrechten sitzen, die Firewall immer aktiv ist. In regelmäßigen Abständen, vor allem bei der Anmeldung, erscheint im Infobereich der Taskleiste ein Hinweis, ob der Client den Netzwerkrichtlinien entspricht (Abbildung 15.37).

Abbildg. 15.37 Meldung beim Erfüllen der Netzwerkanforderungen für NAP

Klicken Sie doppelt auf die Meldung oder das dazugehörige Symbol, erhalten Sie eine ausführliche Statusangabe anzeigt (Abbildung 15.38).

Abbildg. 15.38 Erfolgreiche Überprüfung des Netzwerkzugriffsschutzes

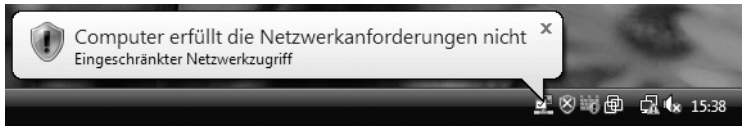


Da die Firewall immer wieder automatisch aktiviert wird, wenn Sie diese deaktivieren, müssen Sie einen anderen Weg gehen, um zu testen, ob auch die Konfiguration des DHCP-Servers funktioniert, der nicht-konformen Clients den Zugriff eingeschränkt zur Verfügung stellt. Der einfachste Weg dazu ist, dass Sie die Systemintegritätsüberprüfung so abändern, dass der Client die Prüfung nicht mehr besteht. Durch diese Änderung wird der Client durch die Integritätsrichtlinie zum nicht-konformen Client erklärt und durch die Netzwerkrichtlinie wird der Zugriff eingeschränkt. Der einfachste Weg ist, dass Sie die Windows-Sicherheitsintegritätsüberprüfung aufrufen und auf einem Test-PC noch den Virenschutz kontrollieren lassen. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie in der NAP-Konsole auf *Netzwerkzugriffsschutz/Systemintegritätsprüfungen*.
2. Rufen Sie die Eigenschaften der *Windows-Sicherheitsintegritätsverifizierung* auf.
3. Klicken Sie im Fenster auf die Schaltfläche *Konfigurieren*. Jetzt können Sie konfigurieren, welche Bedingungen eine Arbeitsstation erfüllen muss, damit diese mit dem Netzwerk kommunizieren darf.
4. Aktivieren Sie für diesen Test die Option *Antivirusanwendung ist aktiviert*.
5. Klicken Sie auf *OK*. Sie müssen keine weiteren Änderungen vornehmen. Die Einstellungen werden automatisch von den Integritätsrichtlinien und auch den Netzwerkrichtlinien übernommen.

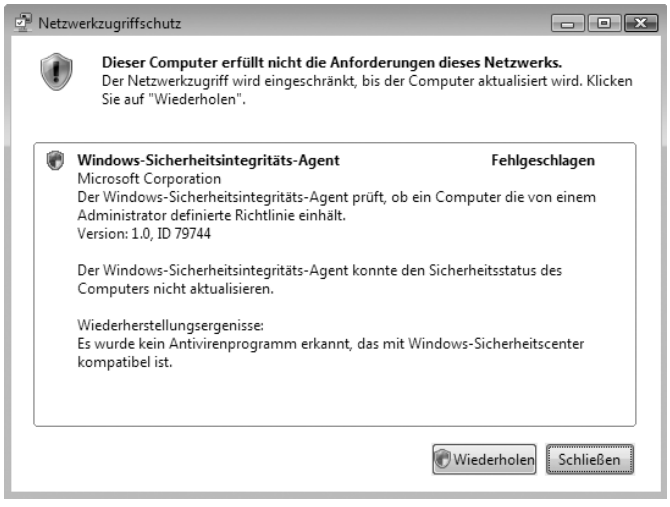
Da Sie auf Ihrer Test-Maschine noch keinen Virenscanner aktiviert haben, besteht diese den Konformitätstest nicht mehr. Sie müssen dazu aber vom DHCP-Server eine neue IP-Adresse beziehen. Geben Sie dazu in der Befehlszeile des PC den Befehl *ipconfig /release* ein. Nachdem die IP-Adresse entfernt wurde, rufen Sie den Befehl *ipconfig /renew* auf, um eine neue IP-Adresse zu erhalten. Sobald dem Client eine neue IP-Adresse durch den DHPC-Server erteilt wurde, erkennt NAP, dass dieser nicht mehr konform ist (Abbildung 15.39).

Abbildg. 15.39 Meldung eines PCs, wenn dieser zum nicht-konformen NAP erklärt wird



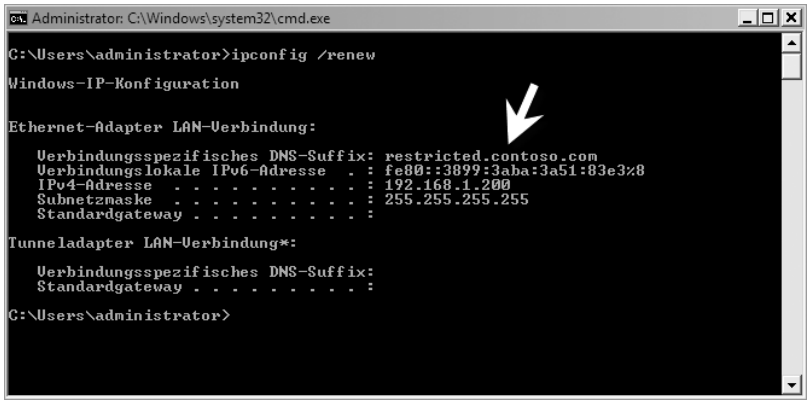
Klicken Sie auf die Meldung, erhalten Sie ausführliche Hinweise angezeigt, warum der Client nicht mehr die Netzwerkanforderungen erfüllt (Abbildung 15.40).

Abbildg. 15.40 Meldung des Netzwerkzugriffsschutzes, wenn der Client nicht mehr NAP-konform ist



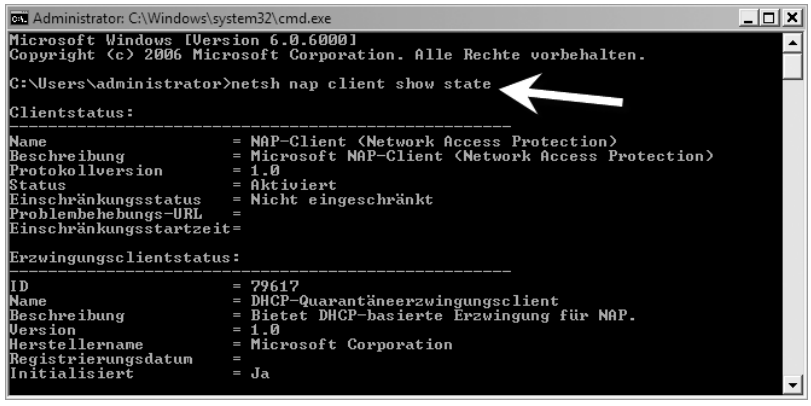
Außerdem erkennen Sie in der Befehlszeile, dass dem Client der DNS-Domänenname zugewiesen worden ist, den Sie für die NAP-Klasse auf dem DHCP-Server konfiguriert haben (Abbildung 15.41). Sie können an dieser Stelle also feststellen, dass die NAP-Überprüfung funktioniert. Sobald Sie diese Bedingung auf dem NPS wieder entfernen, besteht der Client sofort wieder die NAP-Prüfung und Sie erhalten eine entsprechende Meldung.

Abbildg. 15.41 Anzeigen der eingeschränkten DNS-Domänennamen in Windows Vista



TIPP Sie können den NAP-Status eines PC in der Befehlszeile über den Befehl *netsh nap client show state* anzeigen lassen (Abbildung 15.42). So können Sie schnell einen Bericht über die NAP-Konfiguration erstellen, den Sie zum Beispiel in Hilfeforen veröffentlichen können.

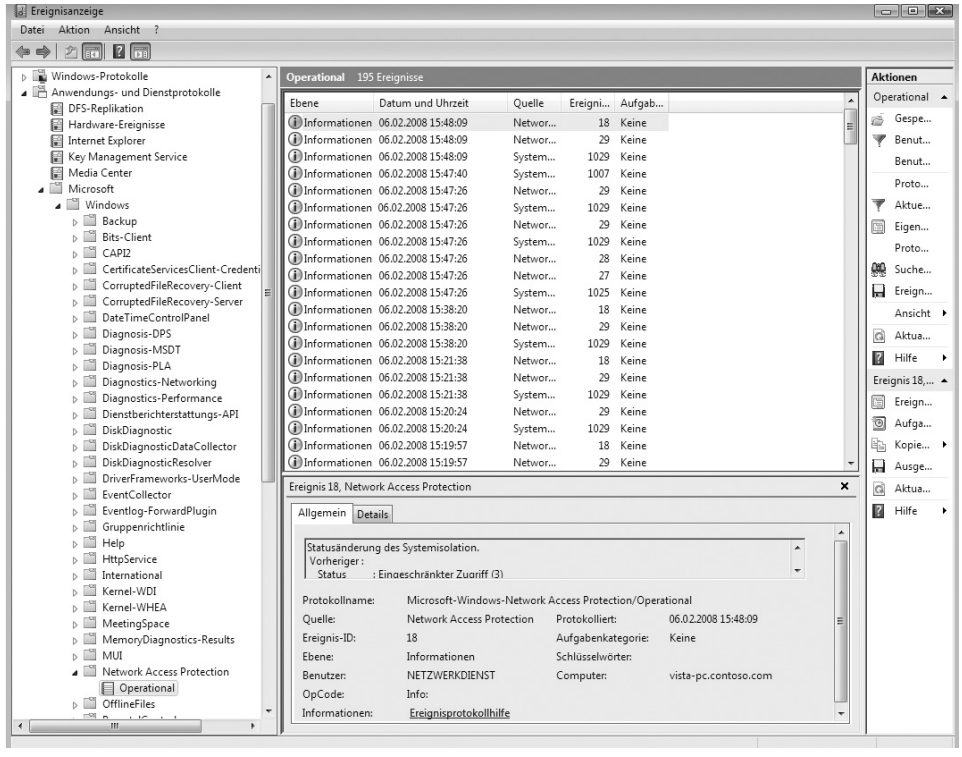
Abbildg. 15.42 Anzeigen des NAP-Status in der Befehlszeile



Fehlersuche der NAP-Konfiguration

Alle Ereignisse der NAP-Konfiguration finden Sie in der Ereignisanzeige. Die Ereignisse auf dem Client finden Sie in der Ereignisanzeige über *Anwendungs- und Dienstprotokolle/Microsoft/Windows/Network Access Protection/Operational* (Abbildung 15.43). Auf dem Server finden Sie die Fehler im Systemprotokoll.

Abbildg. 15.43 Überprüfen der Ereignisanzeige auf dem Vista-Client



Netzwerkzugriffsschutz (NAP) mit VPN

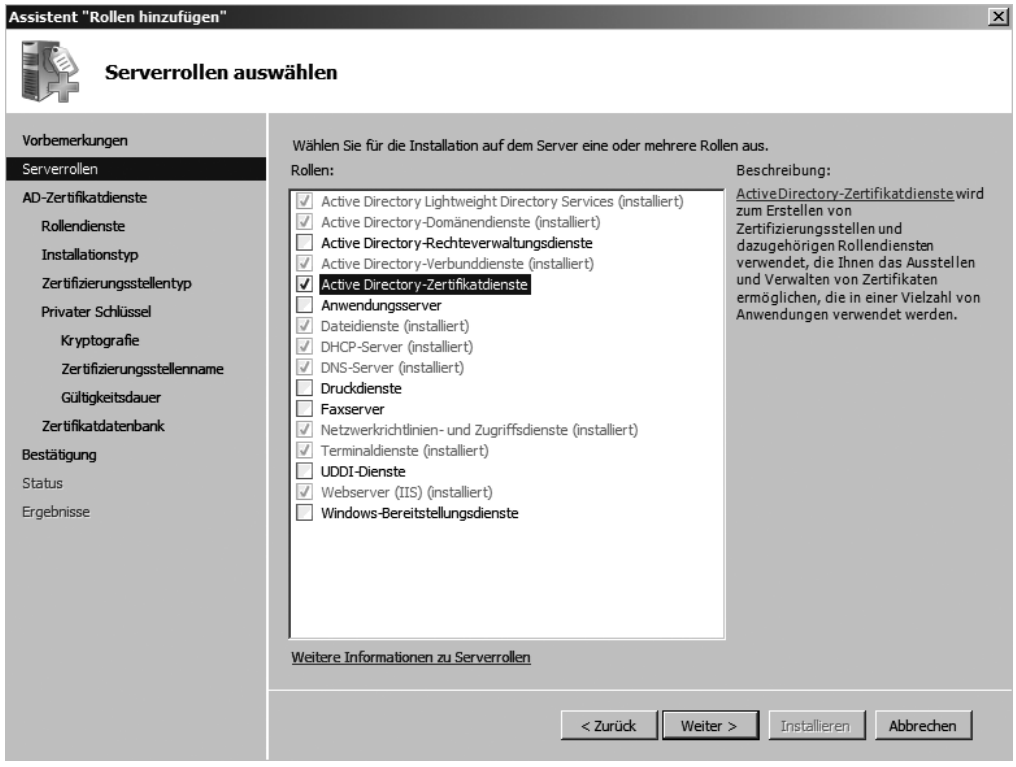
NAP macht vor allem für Clients Sinn, die sich per VPN einwählen. Bei diesen Clients können Administratoren standardmäßig nicht sicherstellen, ob ein Virenschutz installiert oder die Firewall aktiviert ist. Mit NAP können Sie gezielt verhindern, dass sich unsichere Clients aus dem Internet mit Ihrem sicheren internen Netzwerk verbinden. Ähnlich wie bei NAP über DHCP können Sie auch bei NAP über VPN einen Netzwerkrichtlinienserver einsetzen, um Ihr Netzwerk effizient zu schützen. Die Domänencontroller der Domäne können dabei noch unter Windows Server 2003 betrieben werden, nur der VPN und der Netzwerkrichtlinienserver müssen unter Windows Server 2008 laufen. Bei der Einwahl verbindet sich der Client aus dem Internet mit dem RAS-VPN-Server. Dieser fordert wie bei DHCP einen Statement of Health (SoH) vom Client und gibt diesen an den Netzwerkrichtlinienserver weiter. Auf diesem Server werden wieder die entsprechenden Regeln angewendet, die wir bereits im vorangegangenen Abschnitt zur Einbindung von NAP über DHCP besprochen haben.

Auf Basis dieser Richtlinien wird ein Client dann entweder zum konformen oder zum nicht-konformen NAP-Client erklärt und entsprechende Regeln werden angewendet. Wie auch bereits bei NAP über DHCP muss nicht jeder Server unter Windows Server 2008 laufen. Die Domänencontroller können dabei, wie bereits erwähnt, ohne weiteres noch mit Windows Server 2003 betrieben werden. Allerdings muss der RAS-VPN-Server und der Netzwerkrichtlinienserver mit Windows Server 2008 installiert werden, damit Sie diese Funktionen nutzen können. Auf dem Client sollte idealerweise Windows Vista oder mindestens Windows XP mit SP2, besser SP3 und installiertem NAP-Client installiert sein. Optimal wäre auch der Einsatz einer internen Windows-CA, die Sie entweder auf Basis von Windows Server 2003 oder auf Basis von Windows Server 2008 betreiben können (siehe auch Kapitel 17).

Installieren einer Zertifizierungsstelle (CA) unter Windows Server 2008

Die sichere Einwahl über VPN realisieren Sie am besten auch geschützt durch entsprechende Zertifikate, die Sie durch eine interne Windows-Zertifizierungsstelle (Certificated Authority, CA) ausstellen lassen können. Unter Windows Server 2008 werden die Active Directory-Zertifikatdienste über den Server-Manager als Rolle hinzugefügt (Abbildung 15.44).

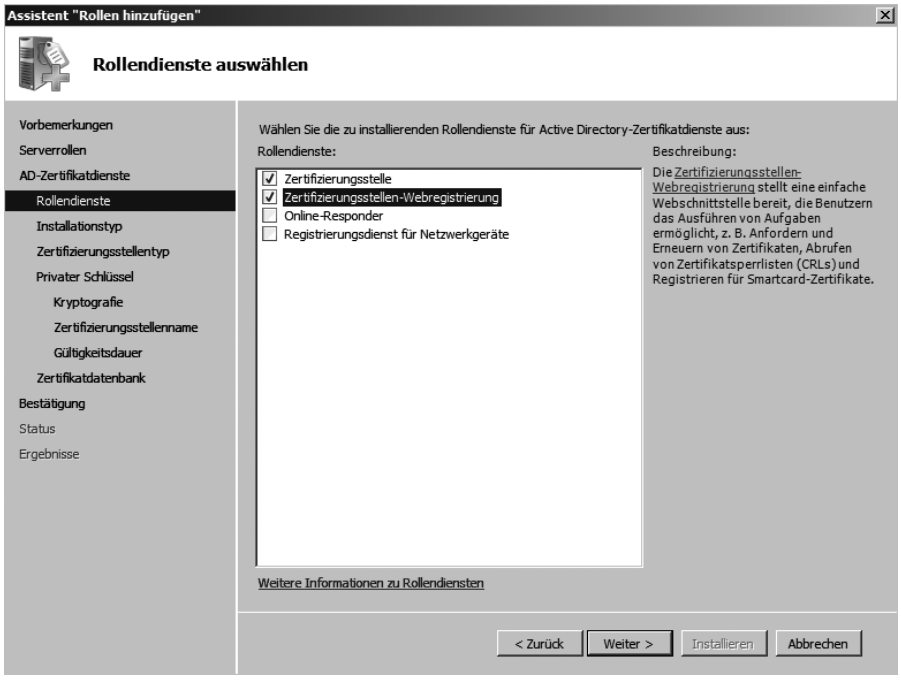
Abbildg. 15.44 Active Directory-Zertifkatdienste installieren



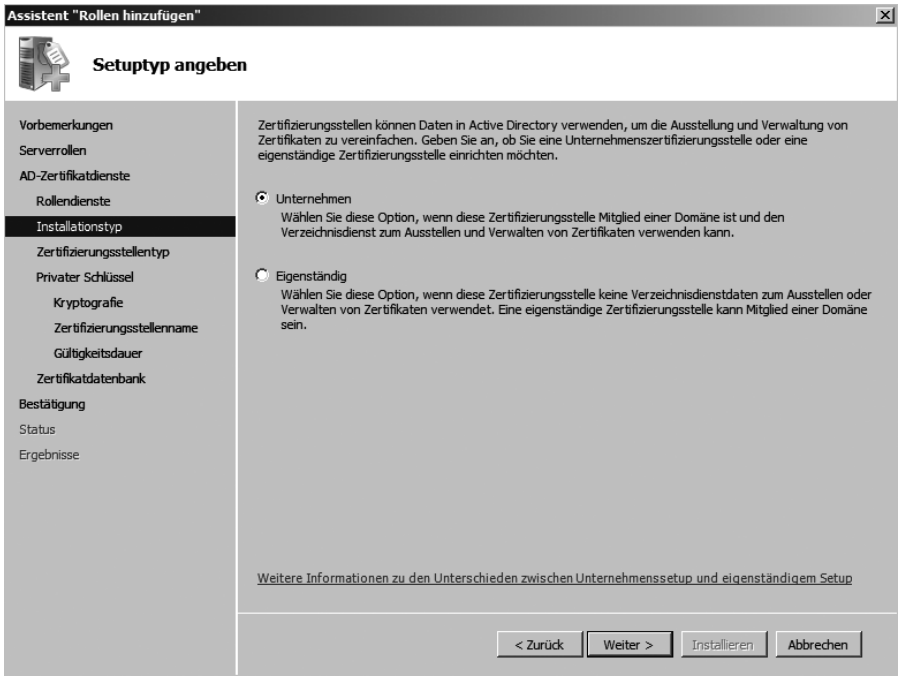
Wählen Sie diese Rolle aus, können Sie die Zertifikatdienste mit einem Assistenten installieren, über den Sie verschiedene Auswahlmöglichkeiten haben. Auf der nächsten Seite des Assistenten wählen Sie aus, welche Rollendienste Sie installieren wollen. Sie sollten auf jeden Fall die Rollendienste *Zertifizierungsstelle* und *Zertifizierungsstellen-Webregistrierung* auswählen (Abbildung 15.45). Der Rollendienst *Zertifizierungsstellen-Webregistrierung* stellt die Weboberfläche der Zertifizierungsdienste zur Verfügung, die Sie über *http://<Servername>/certsrv* aufrufen können, um Zertifikate anzufordern.

Auf der nächsten Seite wählen Sie den Setuptyp aus (Abbildung 15.46). Hier sollten Sie die Option *Unternehmen (empfohlen)* auswählen, da Sie bei der ersten CA eine Root-CA installieren. Bei dieser Auswahl wird auch die CA in Active Directory integriert.

Abbildg. 15.45 Auswählen der Rollendienste für die Active Directory-Zertifikatdienste

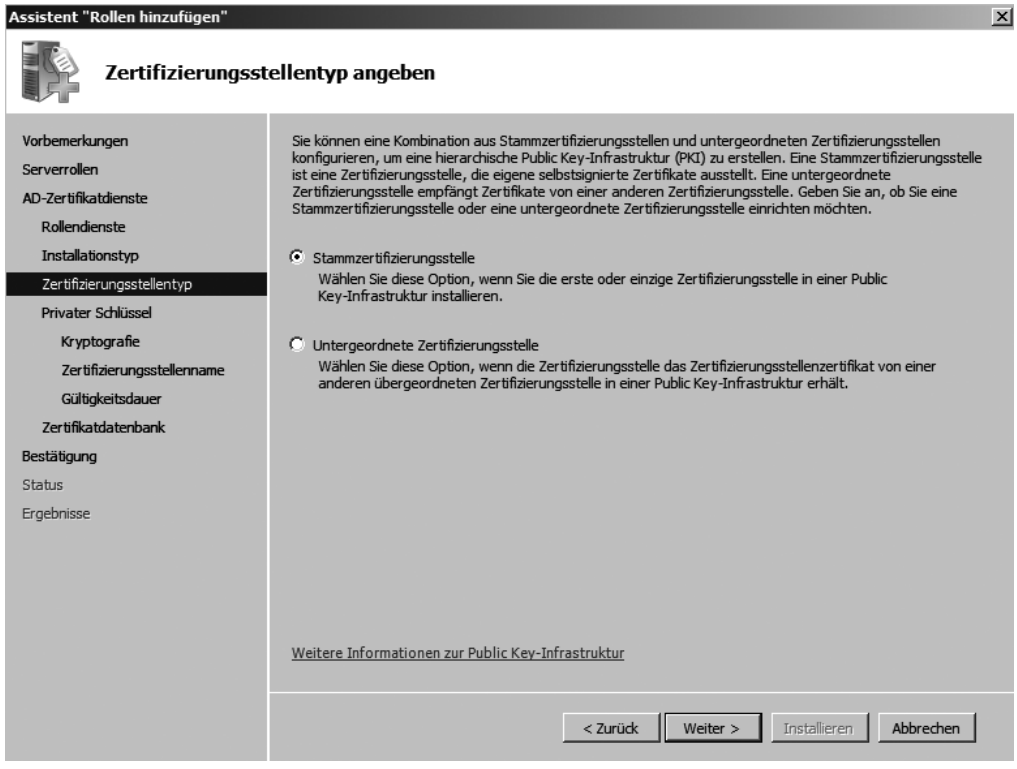


Abbildg. 15.46 Auswählen des Setuptyps



Auf der nächsten Seite des Assistenten legen Sie den Zertifizierungsstellentyp fest. Hier sollten Sie bei der ersten Installation möglichst eine *Stammzertifizierungsstelle (empfohlen)* auswählen (Abbildung 15.47).

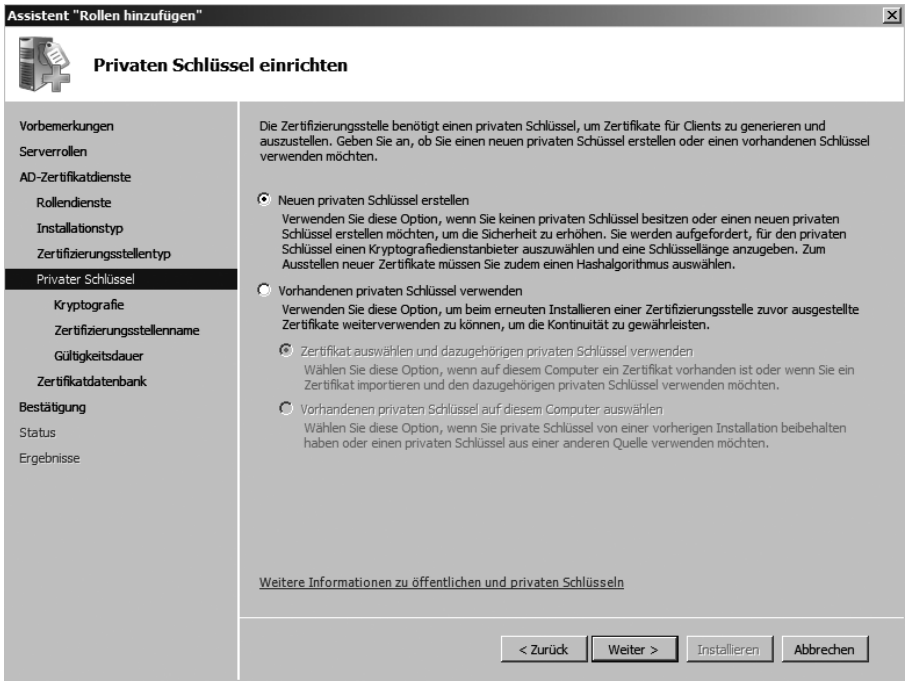
Abbildg. 15.47 Festlegen des Zertifizierungsstellentyps



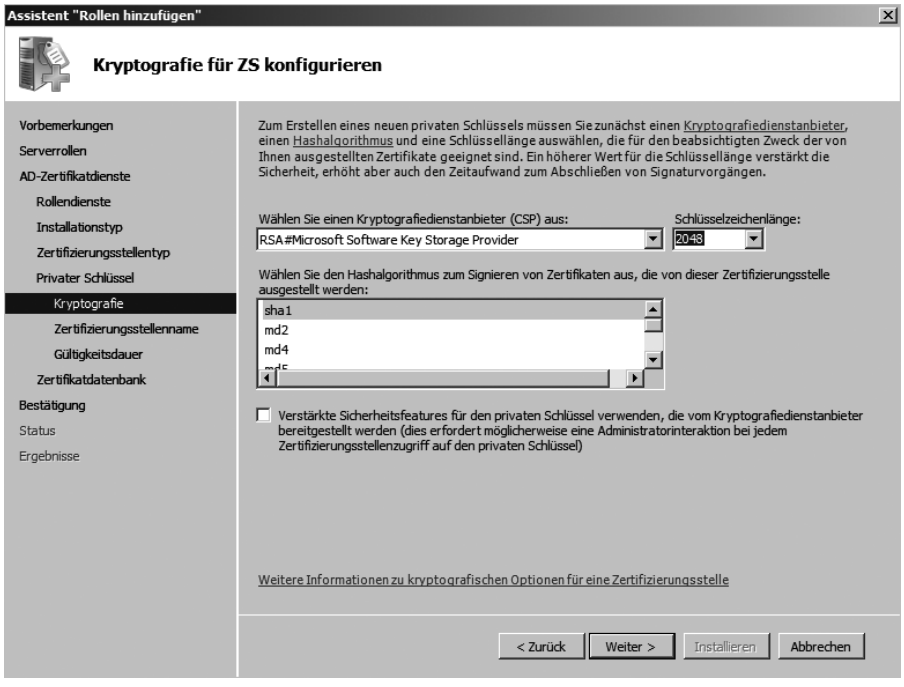
Bei der ersten Installation einer Zertifizierungsstelle wählen Sie aus, dass Sie einen neuen privaten Schlüssel erstellen wollen, da es für diese Zertifizierungsstelle noch keinen Schlüssel gibt (Abbildung 15.48).

Auf der nächsten Seite des Assistenten wählen Sie aus, mit welcher Verschlüsselung Sie Zertifikate ausstellen wollen. Hier sollten Sie möglichst den Standard belassen. Es gibt derzeit zahlreiche verschiedene Verschlüsselungstechniken. Die von R. Rivest für RSA Data Security entwickelten Hash-Algorithmen MD2, MD4 und MD5 sind für digitale Signatursysteme gedacht und bilden eine Nachricht beliebiger Länge auf ein Destillat fester Länge ab. Man spricht in diesem Zusammenhang auch vom digitalen Fingerabdruck einer Nachricht. MD2 gilt als sicher, ist aber langsam. MD4 hingegen hat bekannte Schwächen, weswegen von einer Verwendung abgesehen werden sollte. MD5 dagegen gilt als sicher und ist sehr weit verbreitet. Das nach seinen Entwicklern R. L. Rivest, A. Shamir und L. M. Adleman benannte Kryptosystem ist zur Zeit das bedeutendste asymmetrische Verschlüsselungsverfahren. Es basiert auf dem Faktorisierungsproblem und ist das am besten untersuchte asymmetrische Verfahren überhaupt. Der Algorithmus wurde in zahlreichen Anwendungen implementiert und gilt als sehr sicher. Das Patent wird von RSA Data Security gehalten und ist im Jahr 2000 abgelaufen.

Abbildg. 15.48 Erstellen des privaten Schlüssels

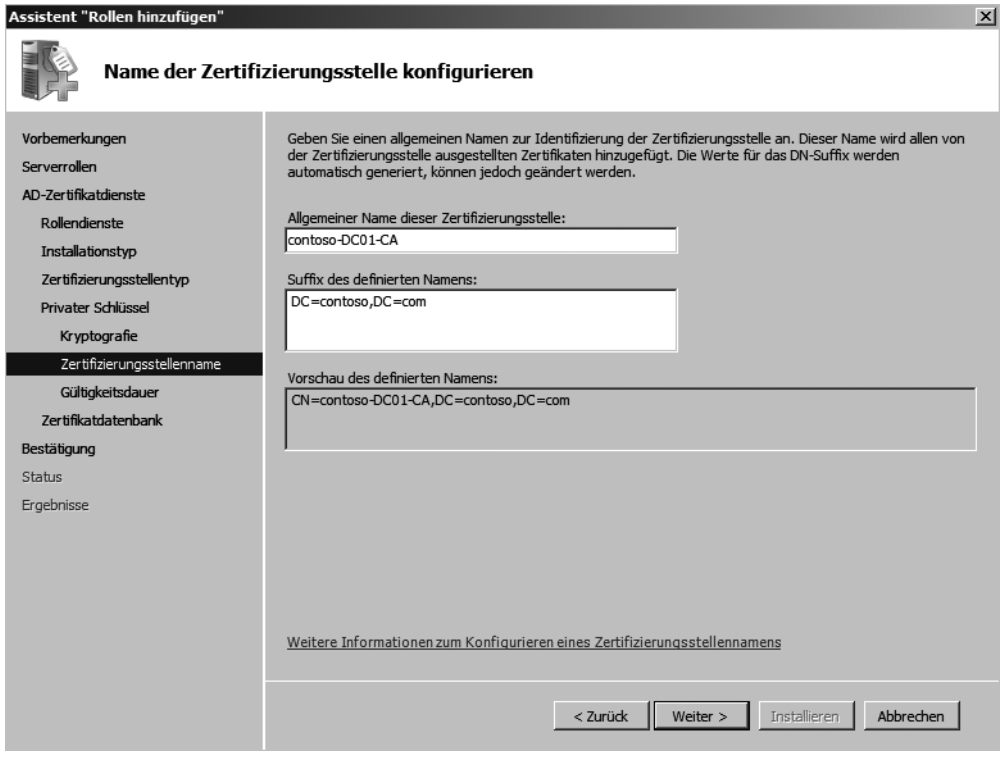


Abbildg. 15.49 Auswählen der Verschlüsselung für die Zertifizierungsstelle



Auf der nächsten Seite legen Sie den Namen für die neue Zertifizierungsstelle fest. Hier sollten sie bei der ersten Stammzertifizierungsstelle im Unternehmen einen passenden Namen wählen, zum Beispiel *Root*. Im Anschluss legen Sie die Gültigkeitsdauer für die Zertifikate fest und schließen die Konfiguration ab. Nach der Installation der Zertifikatsdienste stehen diese zur Verfügung.

Abbildg. 15.50 Festlegen des Namens der Zertifizierungsstelle

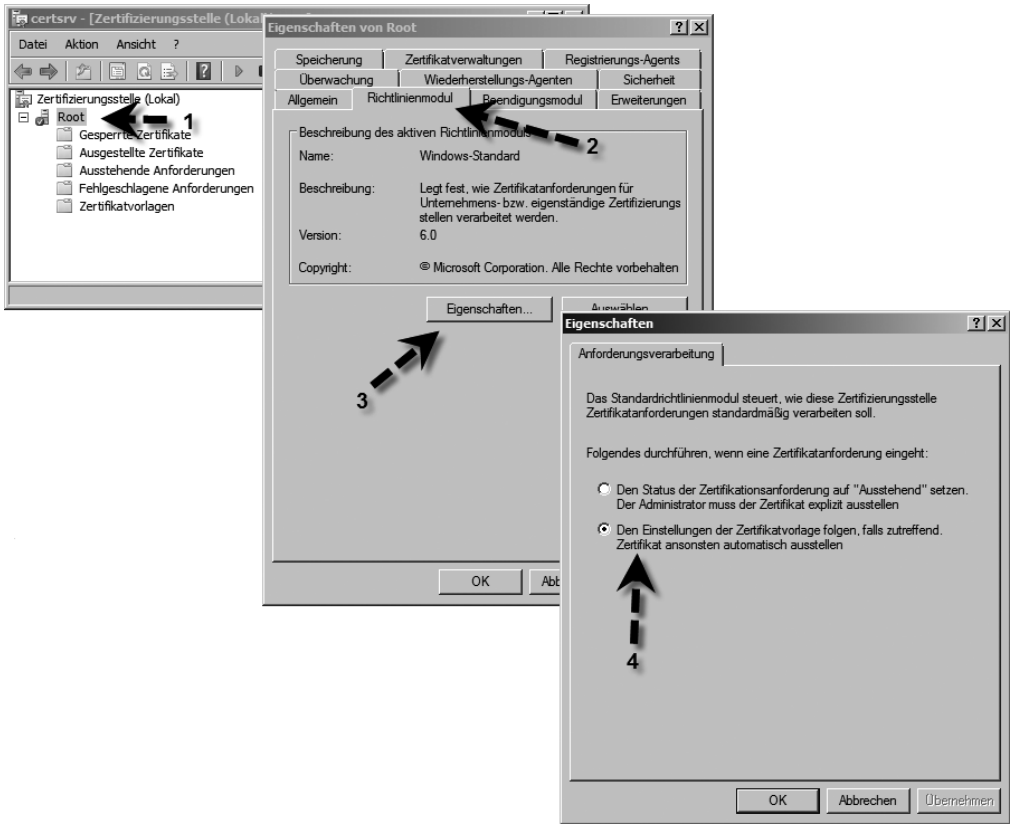


Testen und verifizieren der Zertifikatstelle

Nach der Installation können Sie über das Verwaltungsprogramm *Start/Verwaltung/Zertifizierungsstelle* überprüfen, ob die Installation erfolgreich war (Abbildung 15.51). Der Server sollte mit einem grünen Haken in der Verwaltungsoberfläche angezeigt werden. Zusätzlich sollten Sie überprüfen, dass Zertifikate von der Zertifizierungsstelle auch automatisch zugewiesen werden können. Gehen Sie dazu folgendermaßen vor:

1. Starten Sie die Verwaltungskonsole der Zertifizierungsstelle über *Start/Verwaltung/Zertifizierungsstelle*.
2. Klicken Sie mit der rechten Maustaste auf den Servernamen und rufen Sie die *Eigenschaften* auf.
3. Wechseln Sie auf die Registerkarte *Richtlinienmodul*.
4. Klicken Sie auf die Schaltfläche *Eigenschaften*.
5. Stellen Sie sicher, dass die Option *Den Einstellungen der Zertifikatvorlage folgen, falls zutreffend* aktiviert ist.

Abbildg. 15.51 Verifizieren der Zertifizierungsstelle und Konfiguration der automatischen Ausstellung von Zertifikaten



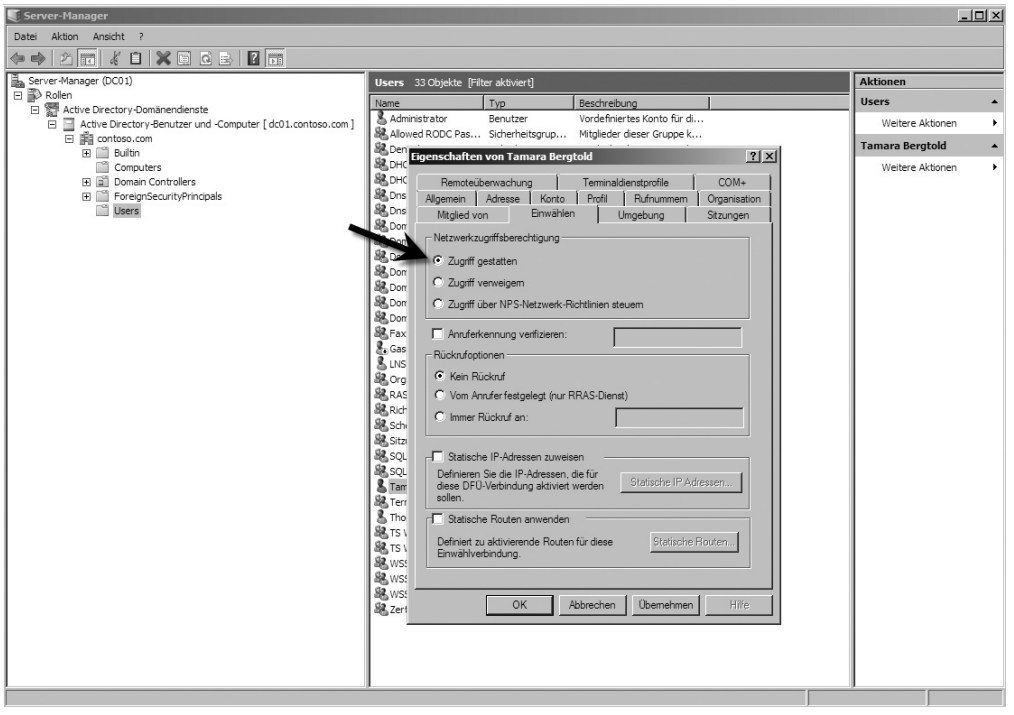
Haben Sie bei der Installation noch den Rollendienst *Zertifizierungsstellen-Webregistrierung* ausgewählt, steht zusätzlich noch die Weboberfläche der Zertifizierungsstelle über den Link *http://<Servername>/certsrv* zur Verfügung. Diese Webseite sollte sich nach erfolgter Authentifizierung fehlerfrei öffnen lassen (Abbildung 15.52). Mehr Optionen sind möglich, wenn die Seite per HTTPS geöffnet wird.

Abbildg. 15.52 Aufrufen der Webseite einer neu installierten Zertifizierungsstelle

Erstellen eines Benutzerkontos mit Einwahlberechtigungen

Für eine Testumgebung sollten Sie ein Beispielkonto anlegen und diesem Konto entsprechende Einwahlberechtigungen erteilen. Ein neues Konto erstellen Sie am besten auf dem Domänencontroller. Ist auf diesem Windows Server 2008 installiert, legen Sie ein neues Benutzerkonto über den Server-Manager an. Tragen Sie die entsprechenden Daten für das Konto ein. Aktivieren Sie auf der Registerkarte *Einwählen* im Bereich *Netzwerkzugriffsberechtigung* die Option *Zugriff gestatten* (Abbildung 15.53). In einer produktiven Umgebung können Sie auch die Option *Zugriff über NPS-Netzwerkrichtlinien steuern* wählen. In diesem Fall erstellen Sie eine Gruppe im Active Directory, zum Beispiel mit der Bezeichnung VPN-Zugriff und nehmen die Benutzerkonten in die Gruppe mit auf, denen Sie VPN-Zugriff gestatten wollen. Auf dem NPS-Server können Sie dann dieser Gruppe die Einwahl gestatten. Dies hat den Vorteil, dass Sie nicht die einzelnen Benutzerkonten konfigurieren müssen, sondern über Gruppenmitgliedschaft die Einwahl steuern. Nehmen Sie in dieser Testumgebung den Benutzer auch in die Domänen-Admin-Gruppe auf, damit die Einwahl funktioniert und entsprechende Konfigurationen durchgeführt werden können.

Abbildg. 15.53 Konfigurieren der Netzwerkzugriffsberechtigung für ein Benutzerkonto

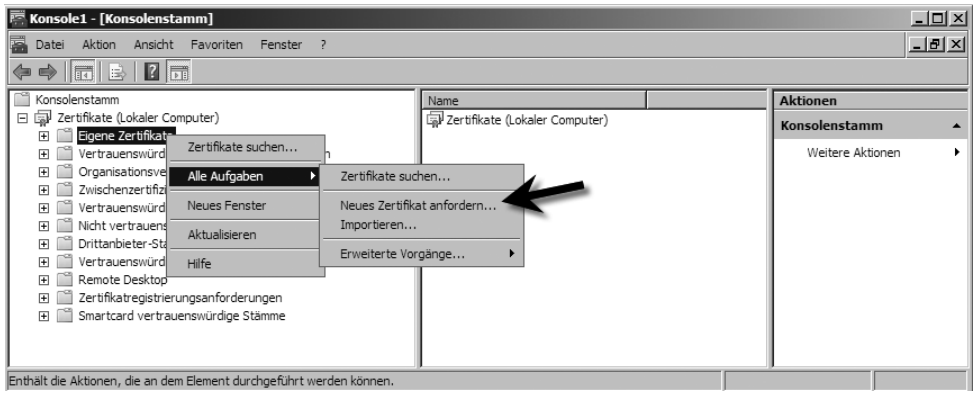


Zertifikat für den NPS-Server zuweisen

Im nächsten Schritt sollten Sie dem NPS-Server ein Zertifikat zuweisen. Gehen Sie dazu folgendermaßen vor:

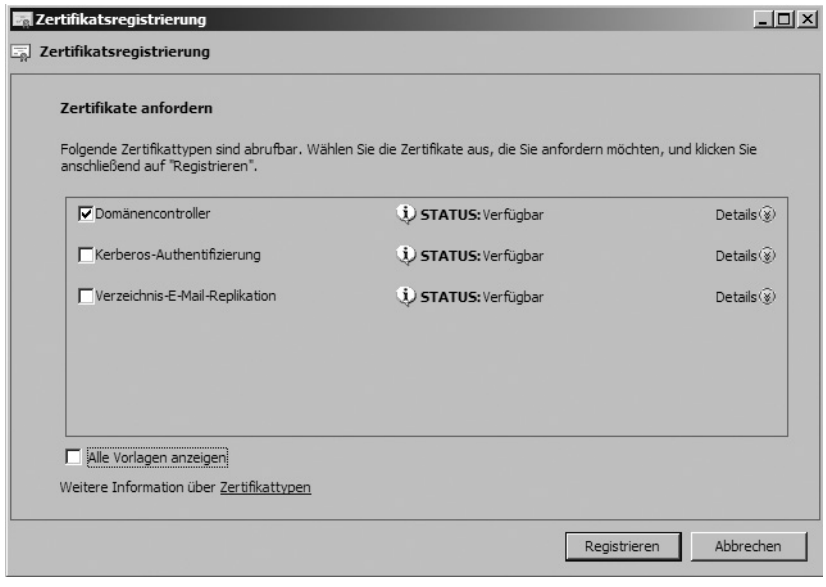
1. Öffnen Sie über *Start/Ausführen/mmc* eine neue Konsole.
2. Fügen Sie das Snap-In *Zertifikate* zu dieser Konsole hinzu.
3. Wählen Sie als Option für den Zertifikatespeicher das Snap-In *Computerkonto* aus.
4. Wählen Sie den lokalen Computer aus.
5. Klicken Sie im Snap-In mit der rechten Maustaste auf *Eigene Zertifikate* und wählen Sie im Kontextmenü den Eintrag *Alle Aufgaben/Neues Zertifikat anfordern* aus (Abbildung 15.54).

Abbildg. 15.54 Anfordern eines neuen Zertifikats für einen Server



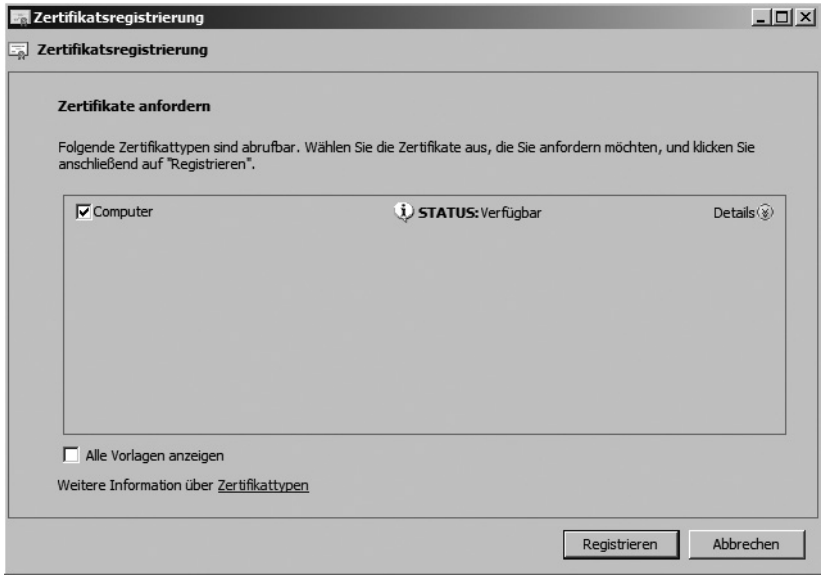
6. Wählen Sie als Zertifikattyp *Computer* aus. Haben Sie den NPS-Server auf einem Domänencontroller installiert, können Sie als Zertifikattyp auch *Domänencontroller* auswählen. Dieses Zertifikat verfügt über die gleichen Möglichkeiten, die ein Computer-Zertifikat beherrscht. Allerdings sollten Sie den NPS- und VPN-Server am besten auf einem getrennten Server installieren.

Abbildg. 15.55 Auswählen des Zertifikattyps für die Installation auf einem NPS-Server



7. Klicken Sie auf *Registrieren*, um das Zertifikat anzufordern. Nach wenigen Sekunden sollte das Zertifikat als erfolgreich ausgestellt angezeigt werden.

Abbildg. 15.56 Auswählen eines Computerzertifikats bei der Installation des VPN-Servers auf einem Mitgliedsserver



Konfiguration des NPS-Servers

Im Anschluss können Sie den NPS-Server konfigurieren. Starten Sie dazu die Verwaltungskonsole für die Netzwerkrichtlinien. Der schnellste Weg, diese Konsole zu starten, ist über *Start/Ausführen/nps.msc*. Als Nächstes konfigurieren Sie die Systemintegritätsprüfungen exakt so, wie sie im Abschnitt »Verwalten der Systemintegritätsprüfungen« weiter vorne in diesem Kapitel für NAP über DHCP konfiguriert worden sind. Im Anschluss erstellen Sie die Integritätsrichtlinien, genauso wie im Abschnitt »Erstellen der Integritätsrichtlinien« weiter vorne in diesem Kapitel für NAP über DHCP besprochen. Die Konfiguration der Systemintegritätsprüfungen und der Integritätsrichtlinien erfolgt komplett identisch. Wichtig an dieser Stelle ist die Konfiguration der *Windows-Sicherheitsintegritätsverifizierung* (Statement of Health, SoH). Diese wird vom Client durch das Vista-Sicherheitscenter an den Server übermittelt. Auf Basis dieser Verifizierung wird der Client einer Integritätsrichtlinie zugeordnet, also zum konformen oder Nicht-Konformen-Client erklärt.

Erstellen der Netzwerkrichtlinien

Netzwerkrichtlinien (Network Policies) steuern den Netzwerkzugriff von Clients basierend auf Integritätsrichtlinien (Health Policies), die wiederum auf den Systemintegritätsprüfungen (System Health Validators, SHVs) aufbauen. Nachdem Sie die Systemintegritätsprüfung festgelegt haben, in denen konfiguriert ist, welche Bedingungen ein NAP-konformer Client erfüllen muss, wird mit den Systemrichtlinien festgelegt, ob ein Client NAP-konform oder Nicht-NAP-konform ist. Die Netzwerkrichtlinien steuern wiederum, was mit NAP-konformen bzw. Nicht-NAP-konformen Clients im Netzwerk passieren soll und welchen Zugriff diese erhalten dürfen. Bevor Sie neue Richtlinien erstellen, sollten Sie die standardmäßig angelegten Richtlinien zunächst deaktivieren. Klicken Sie diese dazu mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Deaktivieren*

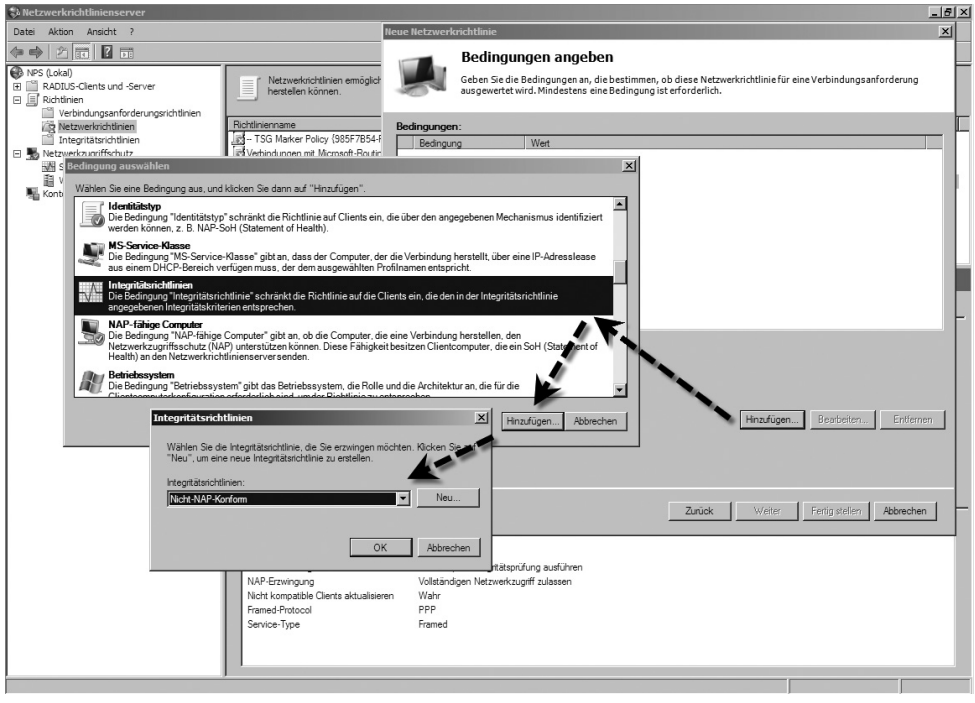
aus. Erstellen Sie die Netzwerkrichtlinie für konforme NAP-Clients genauso wie im Abschnitt »Erstellen der Netzwerkrichtlinien« weiter vorne in diesem Kapitel bereits beschrieben wurde.

Erstellen der Netzwerkrichtlinie für nicht-konforme NAP-Clients

Nachdem Sie die Richtlinie für konforme NAP-Clients erstellt haben, müssen Sie als Nächstes eine Netzwerkrichtlinie erstellen, die den Netzwerkzugriff für nicht-konforme Clients steuert. Diese Konfiguration unterscheidet sich etwas von der Netzwerkrichtlinie für nicht-konforme Clients im Bereich NAP über DHCP.

1. Gehen Sie zur Erstellung analog vor und geben Sie der Richtlinie eine passende Bezeichnung.
2. Wählen Sie als Integritätsrichtlinie dieses Mal die Richtlinie *Nicht-NAP-Konform* aus (Abbildung 15.57).

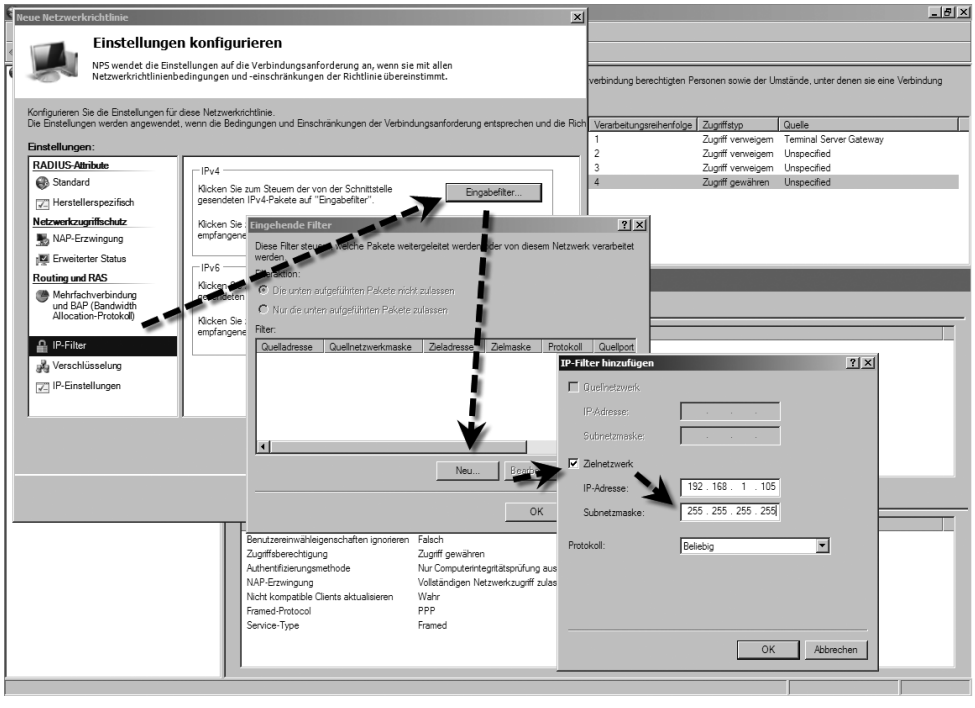
Abbildg. 15.57 Erstellen einer Richtlinie für Nicht-NAP-konforme Clients



3. Auf der Seite *Zugriffsberechtigung angeben* wählen Sie auch hier *Zugriff gewährt*. Der Zugriff wird später noch eingeschränkt. Natürlich könnten Sie bei sich auch die Option *Zugriff verweigert* auswählen, um den Clients die komplette Kommunikation zu untersagen. Allerdings sperren Sie in diesem Fall die Clients komplett aus dem Netzwerk aus.
4. Klicken Sie auf *Weiter*, um zum Fenster *Authentifizierungsmethoden konfigurieren* zu gelangen.
5. Übernehmen Sie die Standardeinstellungen
6. Klicken Sie auf *Weiter*, um zur Seite *Einschränkungen konfigurieren* zu gelangen. Klicken Sie auch hier auf *Weiter*, um zur Seite *Einstellungen konfigurieren* zu gelangen.
7. Klicken Sie auf *NAP-Erzwingung*.

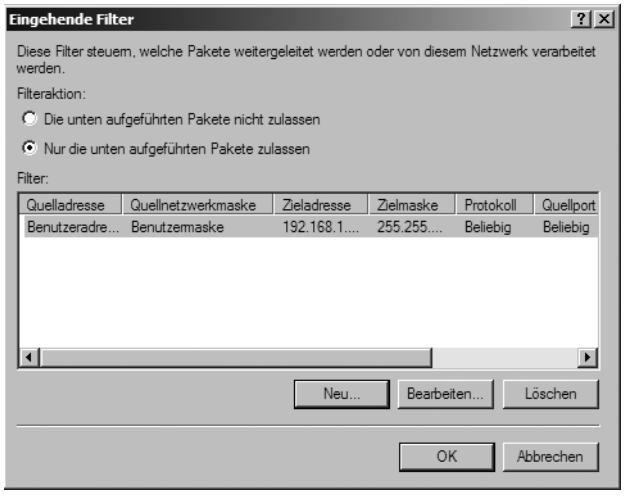
8. Aktivieren Sie die Option *Eingeschränkten Zugriff gewähren*.
9. Aktivieren Sie das Kontrollkästchen *Automatische Wartung von Clientcomputern aktivieren*.
10. Klicken Sie als Nächstes auf *IP-Filter*.
11. Klicken Sie im Bereich *IPv4* auf *Eingabefilter*.
12. Klicken Sie auf *Neu*.
13. Aktivieren Sie das Kontrollkästchen *Zielnetzwerk*.
14. Geben Sie die IP-Adresse des Domänencontrollers mit der Subnetzmaske *255.255.255.255* an. Dadurch ist sichergestellt, dass sich nicht-konforme NAP-Clients nur mit dem Domänencontroller verbinden können, um sich zu authentifizieren (Abbildung 15.58).
15. Bestätigen Sie die Eingabe mit *OK*.

Abbildg. 15.58 Erstellen eines IP-Filters für VPN-Clients



16. Aktivieren Sie dann im Fenster *Eingehende Filter* die Option *Nur die unten aufgeführten Netzwerkpakete zulassen*. Dadurch wird sichergestellt, dass der Client sich ausschließlich mit der festgelegten IP-Adresse verbinden darf, allerdings mit allen Protokollen (Abbildung 15.59).

Abbildg. 15.59 Festlegen der gültigen IP-Pakete für den Eingabefilter



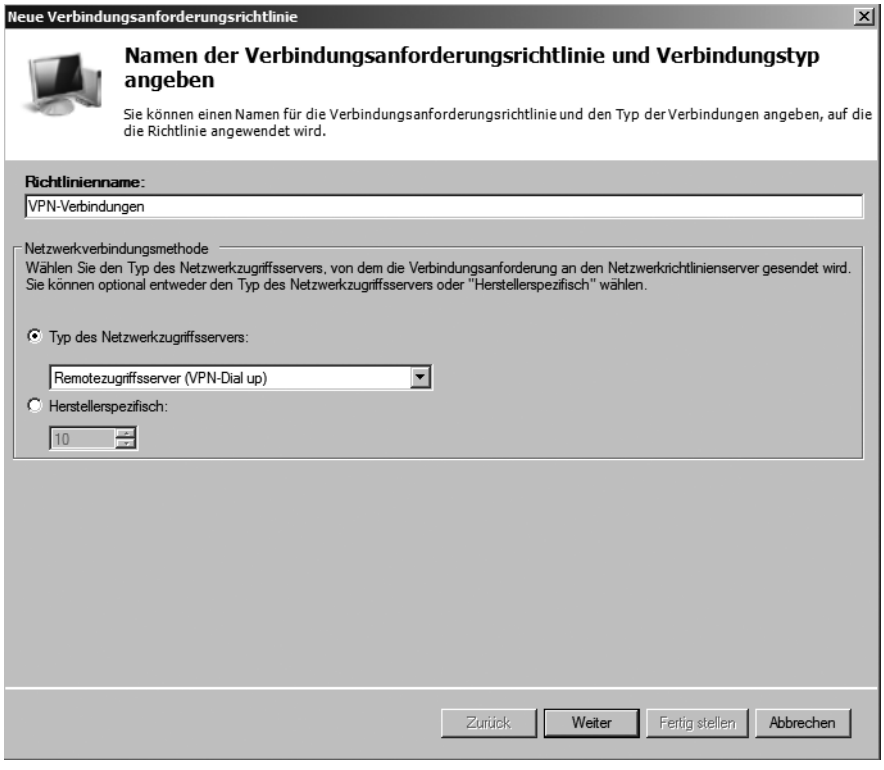
17. Klicken Sie auf *OK*, um das Fenster *Eingehende Filter* zu schließen und klicken Sie im Hauptfenster anschließend im Bereich *IPv4* auf *Ausgabefilter*.
18. Gehen Sie hier analog zur Konfiguration des Eingabefilters vor und hinterlegen Sie auch hier die IP-Adresse des Domänencontrollers mit der Subnetzmaske *255.255.255.255*. Dadurch ist sichergestellt, dass der Client nicht nur Datenpakete zum Domänencontroller senden kann, sondern auch nur vom Domänencontroller empfängt.
19. Schließen Sie die Erstellung der Netzwerkrichtlinien ab. Diese werden nach der Erstellung in der NPS-Konsole angezeigt. Alle anderen Richtlinien sollten als deaktiviert angezeigt werden.

Erstellen der Verbindungsanforderungsrichtlinie

Für die Einwahl von VPN-Clients werden noch *Verbindungsanforderungsrichtlinien* (Connection Request Policies, CRPs) benötigt. Diese konfigurieren Sie über die NPS-Konsole, indem Sie im Bereich Richtlinien auf den Menüpunkt *Verbindungsanforderungsrichtlinien* klicken. Gehen Sie zur Konfiguration einer CRP für die VPN-Einwahl wie folgt vor:

1. Deaktivieren Sie zunächst die Standardrichtlinien.
2. Erstellen Sie eine neue Richtlinie, indem Sie mit der rechten Maustaste auf *Verbindungsanforderungsrichtlinien* klicken und *Neu* wählen.
3. Geben Sie der Richtlinie einen passenden Namen, zum Beispiel *VPN-Verbindungen*.
4. Wählen Sie im Listenfeld zur Option *Typ des Netzwerkzugriffsservers* den Eintrag *Remotezugriffsserver (VPN-Dial up)* aus.
5. Klicken Sie auf *Weiter*.

Abbildg. 15.60 Erstellen einer Verbindungsanforderungsrichtlinie



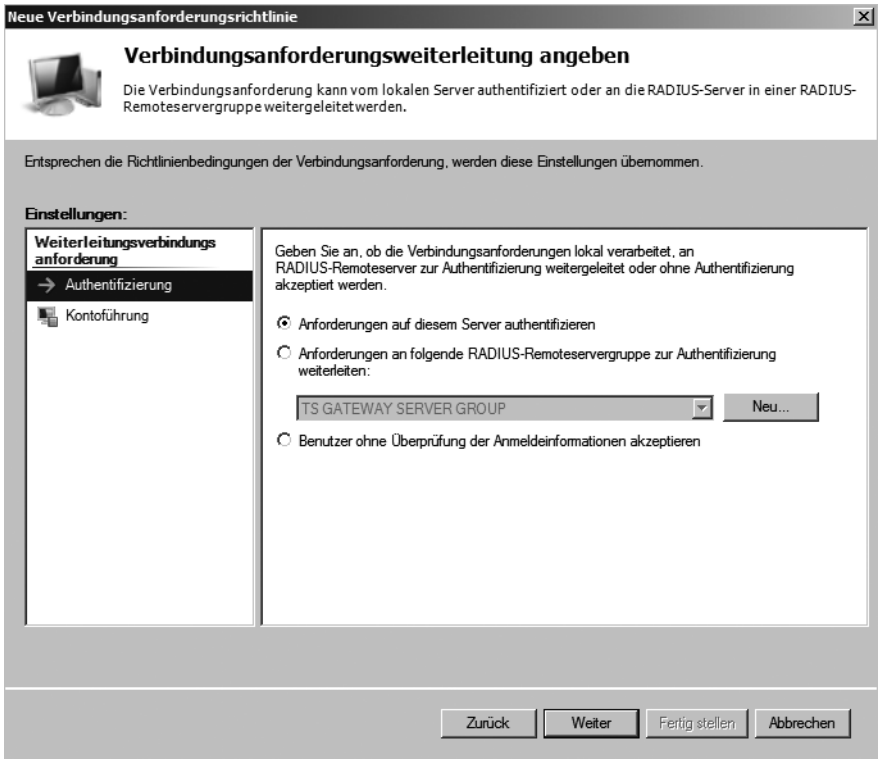
6. Klicken Sie im Fenster *Bedingungen eingeben* auf *Hinzufügen*.
7. Aktivieren Sie die Option *Client-IPv4-Adresse* und klicken Sie auf *Hinzufügen*.
8. Geben Sie die IP-Adresse des RADIUS-Servers ein, an dem sich die Benutzer über das Internet anmelden sollen (Abbildung 15.61). Hierbei handelt es sich üblicherweise um den NPS-Server, nicht um den Domänencontroller. Für die Authentifizierung von Benutzern an einem Einwählserver sind Protokolle erforderlich, die von Client und Server unterstützt werden. Grundsätzlich stellt eine Einwahl immer ein Sicherheitsrisiko dar. Um diesen Bereich zu sichern, gibt es eine Reihe unterschiedlicher Konzepte. Einmalkennwörter sind ein Beispiel, die Windows Server 2008-Authentifizierung des Remote Access Service (RAS) ein anderes. Diese Ansätze haben einen grundsätzlichen Nachteil: Sie sind an eine bestimmte Plattform gebunden und damit in einem heterogenen Umfeld sehr pflegeintensiv. Sicherheitskonzepte müssen mehrfach für unterschiedliche Plattformen implementiert werden. Eine offene, weil plattformunabhängige Lösung stellt das in RFC 2058 von der IETF definierte Client/Server-Protokoll RADIUS (Remote Authentication Dial-In User Service) dar, das ursprünglich von dem Unternehmen Livingston Enterprises entwickelt wurde. Bei diesem Modell wird ein RADIUS-Server eingesetzt, auf dem sich die Informationen über die Sicherheitseinstellungen für die Remotebenutzer befinden. Auf dem Einwählserver läuft ein RADIUS-Client, der die Benutzer bei RADIUS-Server authentifiziert. Für unterschiedliche Betriebssysteme und Einwählserver – die auch Hardware-Lösungen sein können – wird damit nur ein Authentifizierungssystem benötigt. Der RRAS von Windows Server 2008 stellt einen RADIUS-Client zur Verfügung, mit dem auf RADIUS-Server zugegriffen

werden kann. Windows Server 2008 kann damit voll in ein auf RADIUS basierendes Authentifizierungs-Konzept für Remote Access Server integriert werden und auch als RADIUS-Server agieren. Das ist vor allem von Bedeutung, wenn sich entweder unterschiedlichste Clients einwählen sollen oder wenn neben dem RRAS Hardware-Lösungen als Einwählserver verwendet werden. RADIUS stellt den kleinsten gemeinsamen Nenner dar.

Abbildg. 15.61 Festlegen des RADIUS-Servers für die Einwahl

9. Nachdem Sie die Eingaben vorgenommen haben, klicken Sie auf *Weiter*.
10. Aktivieren Sie im Fenster *Verbindungsanforderungsweiterleitung angeben* für den Bereich *Authentifizierung* die Option *Anforderungen auf diesem Server authentifizieren* (Abbildung 15.62).
11. Klicken Sie auf *Weiter*.

Abbildg. 15.62 Konfiguration der Authentifizierung für VPN-Clients

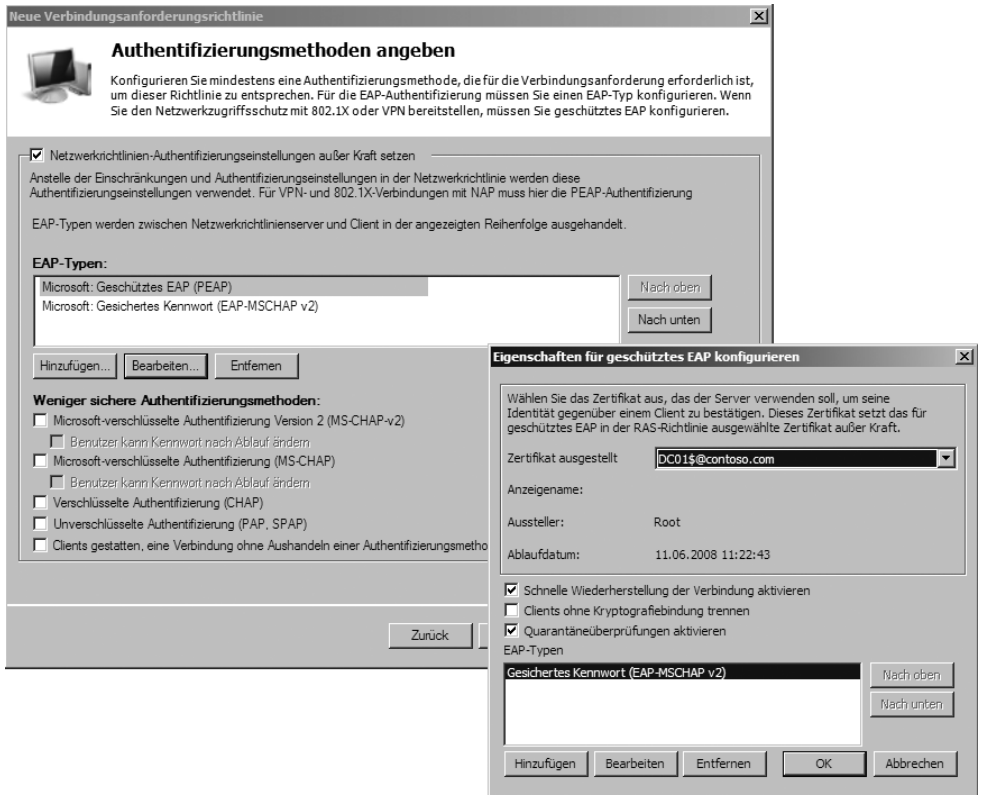


12. Aktivieren Sie auf dem Fenster *Authentifizierungsmethoden angeben* das Kontrollkästchen *Netzwerkrichtlinien-Authentifizierungseinstellungen außer Kraft setzen*. Durch diese Auswahl wird die Authentifizierung so verwendet, wie Sie diese in der Verbindungsanforderungsrichtlinie festlegen, unabhängig davon, wie die entsprechenden Netzwerkrichtlinien konfiguriert sind.
13. Klicken Sie im Bereich *EAP-Typen* auf *Hinzufügen*. Mit EAP können andere Authentifizierungsanbieter eingebunden werden, die Einmalkennwörter oder biometrische Verfahren unterstützen. Am sichersten sind die Microsoft-verschlüsselten Authentifizierungsmechanismen, wobei MS-CHAP v2 ein sehr hohes Maß an Sicherheit bietet. Allerdings wird dieser Standard von älteren Windows-Clients nicht unterstützt. Beim Extensible Authentication Protocol (EAP) handelt es sich um eine Erweiterung des Point-to-Point Protocols (PPP), das zufällige Authentifizierungsmethoden unter Verwendung des Austauschs von Anmeldeinformationen und Daten zufälliger Länge zulässt. Es handelt sich um einen herstellerübergreifenden Industriestandard, der mehrere unterschiedliche Authentifizierungsmethoden zulässt. So ist EAP vielseitig und mit unterschiedlicher Hardware einsetzbar, beispielsweise mit Tokenkarten, Einmal-Kennwörtern, Smartcards und anderweitigen zertifikatsbasierten Protokollen, wie sie im VPN (Virtual Private Network) eingesetzt werden. Im VPN werden unterschiedliche Authentifizierungsprotokolle wie PAP, CHAP, MSCHAP oder zertifikatsbasierte Protokolle unterstützt. Auch für die Datenverschlüsselung sind verschiedene Protokolle wie PPTP (Point To Point Tunnel Protocol) oder L2TP (Layer 2 Tunnel Protocol) verfügbar. Windows Server 2008 bietet von Haus aus Unterstützung für mehrere EAP-Typen.

14. Wählen Sie *Microsoft: Geschütztes EAP (PEAP)* aus. PEAP verwendet TLS (Transport Level Security), um einen verschlüsselten Kanal zwischen einem authentifizierten PEAP-Client und einem authentifizierenden PEAP-Server zu erstellen. PEAP gibt keine Authentifizierungsmethode an, bietet allerdings zusätzliche Sicherheit für andere EAP-Authentifizierungsprotokolle, z. B. EAP-MSCHAPv2, das den mit TLS verschlüsselten Kanal von PEAP verwenden kann. Zur Optimierung von EAP-Protokollen und Netzwerksicherheit bietet PEAP Schutz der Aushandlung der EAP-Methode, die zwischen Client und Server über einen TLS-Kanal stattfindet. Dies verhindert, dass ein Angreifer Pakete zwischen dem Client und dem Netzwerkzugriffsserver mit dem Ziel einfügt, dass eine nicht so sichere EAP-Methode ausgehandelt wird. Der verschlüsselte TLS-Kanal verhindert außerdem Denial-of-Service-Angriffe auf den Server. Der PEAP-Authentifizierungsvorgang zwischen dem PEAP-Client und dem Authentifizierungsserver besteht aus zwei Phasen. In der ersten Phase wird ein sicherer Kanal zwischen dem PEAP-Client und dem Authentifizierungsserver eingerichtet. In der zweiten Phase wird die EAP-Authentifizierung zwischen dem EAP-Client und dem Authentifizierungsserver durchgeführt.

15. Klicken Sie auf *OK* und noch mal auf *Hinzufügen*.

Abbildg. 15.63 Konfigurieren der Authentifizierungseinstellungen



16. Wählen Sie *Microsoft: Gesichertes Kennwort (EAP-MSCHAP v2)* aus. Das Protokoll bietet Funktionen für die gegenseitige Authentifizierung, leistungsfähigere Ausgangsschlüssel für die Datenverschlüsselung sowie unterschiedliche Schlüssel für die Verschlüsselung beim Senden und

Empfangen. Um das Risiko von Attacken auf Kennwörter während des Datenaustausches über MS-CHAP zu minimieren, unterstützt MS-CHAP v2 nicht mehr die Änderung des Kennwortes für MS-CHAP, und das verschlüsselte Kennwort wird nicht mehr übertragen.

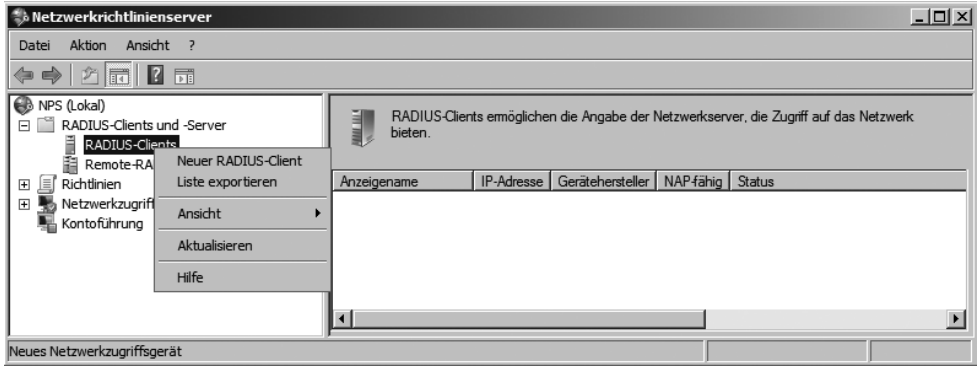
17. Markieren Sie als Nächstes die Option *Microsoft: Geschütztes EAP (PEAP)* und klicken Sie auf *Bearbeiten* (Abbildung 15.63).
18. Stellen Sie sicher, dass das Kontrollkästchen *Quarantäneüberprüfungen aktivieren* eingeschaltet ist.
19. Wählen Sie das Zertifikat aus, das Sie zuvor für den Server ausgestellt haben.
20. Bestätigen Sie auf den restlichen Fenstern die Standardeinstellungen und schließen Sie die Erstellung der Richtlinie ab.

Konfiguration des RADIUS-Clients

Der nächste Schritt bei der Einrichtung von NAP über VPN ist die Konfiguration des RADIUS-Clients. Dies ist vor allem dann sinnvoll, wenn es sich beim VPN-Einwahlserver und dem Netzwerkrichtlinienserver nicht um das gleiche Gerät handelt. Setzen Sie einen eigenständigen VPN-Server ein, müssen Sie diesen auf dem NPS-Server als RADIUS-Client konfigurieren, da es sich beim NPS-Server um den RADIUS-Server handelt. Sie verwenden dazu wieder die Verwaltungskonsole *Netzwerkrichtlinienserver*:

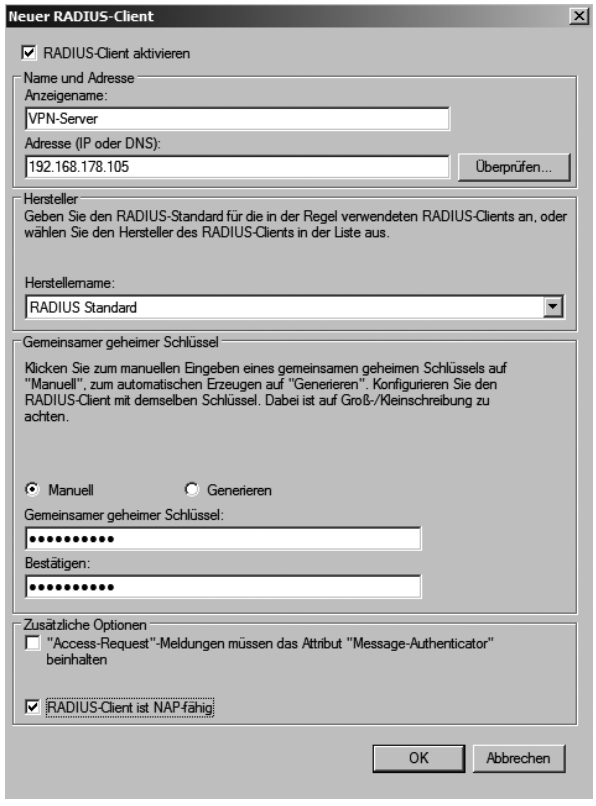
1. Öffnen Sie in der Konsolenstruktur den Knoten *RADIUS-Clients und -Server*, klicken Sie mit der rechten Maustaste auf *RADIUS-Clients* und wählen Sie aus dem Kontextmenü den Eintrag *Neuer RADIUS-Client* aus (Abbildung 15.64).

Abbildg. 15.64 Erstellen eines neuen RADIUS-Clients auf dem NPS-Server



2. Es öffnet sich ein neues Fenster, in dem Sie die Daten des RADIUS-Clients konfigurieren können. Tragen Sie den Anzeigenamen und die IP-Adresse oder den DNS-Namen des Servers in die entsprechenden Felder ein (Abbildung 15.65).
3. Aktivieren Sie noch das Kontrollkästchen *RADIUS-Client ist NAP-fähig*.
4. Hinterlegen Sie im Feld *Gemeinsamer geheimer Schlüssel* ein Kennwort und bestätigen Sie dieses.
5. Schließen Sie das Fenster mit *OK*.

Abbildg. 15.65 Konfigurieren des RADIUS-Clients auf dem NPS-Server

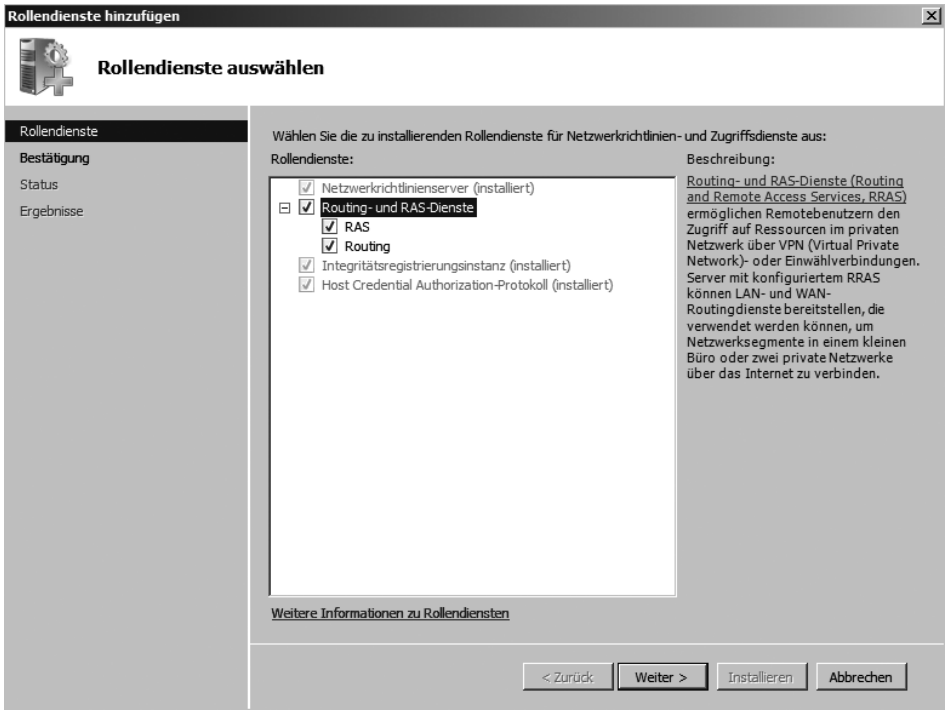


Konfigurieren des Routing- und RAS-Dienstes für die Remoteeinwahl

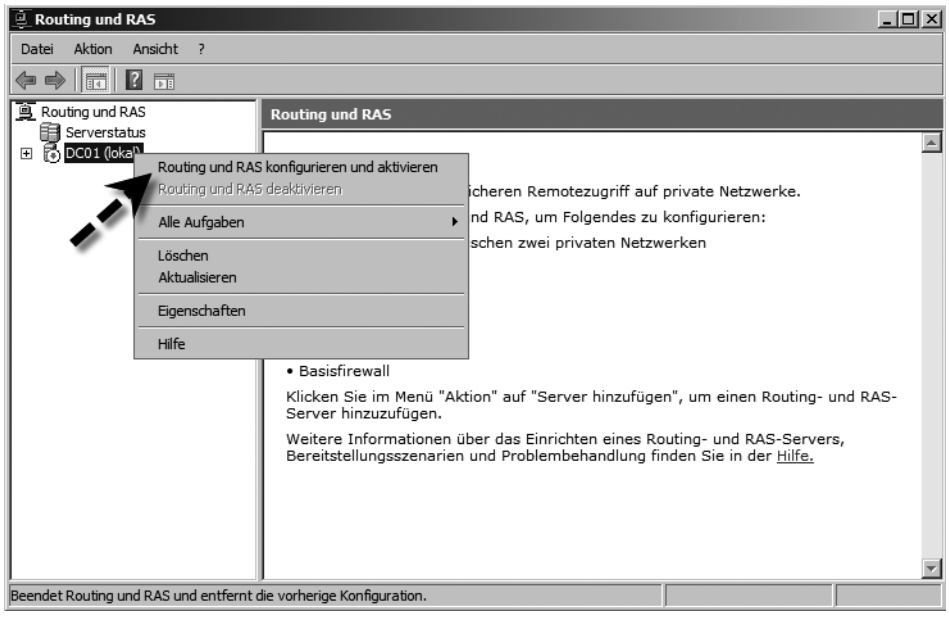
Der nächste Schritt bei der Einrichtung ist die Konfiguration des VPN-Servers, also des RADIUS-Clients an sich. Der VPN-Server sollte zwei Netzwerkkarten verwenden. Für die Remoteeinwahl müssen Sie auf dem VPN-Server die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* installieren. Zusätzlich müssen Sie noch den Rollendienst *Routing- und RAS-Dienste* auswählen. Haben Sie die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* bereits installiert, klicken Sie im Server-Manager auf *Rollen/Netzwerkrichtlinien- und Zugriffsdienste* und dann in der Mitte der Konsole auf *Rollendienste hinzufügen*. Wählen Sie an dieser Stelle den Rollendienst *Routing- und RAS-Dienste* aus (Abbildung 15.66). Schließen Sie die Installation des Rollendienstes ab, damit diese Funktion über den Server-Manager verwaltet werden darf.

Nach der Installation des Rollendienstes *Routing- und RAS-Dienste* starten Sie die Verwaltung über *Start/Ausführen/rrasmgmt.msc* oder über *Start/Verwalten/Routing und RAS* (Abbildung 15.67). Nachdem Sie die Konsole gestartet haben, klicken Sie mit der rechten Maustaste auf den Servernamen und wählen im Kontextmenü den Eintrag *Routing und RAS konfigurieren und aktivieren* aus. Daraufhin startet ein Assistent, mit dessen Hilfe Sie die Einwahlmöglichkeiten per VPN konfigurieren können.

Abbildg. 15.66 Installation der Routing- und RAS-Dienste

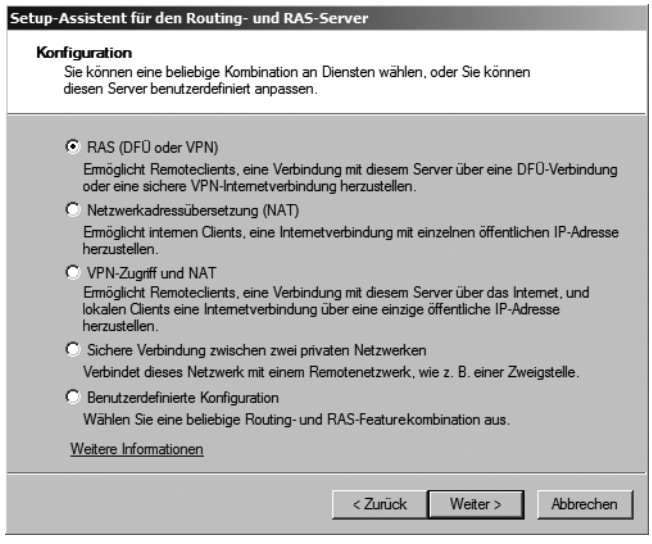


Abbildg. 15.67 Konfigurieren und aktivieren von Routing und RAS in Windows Server 2008



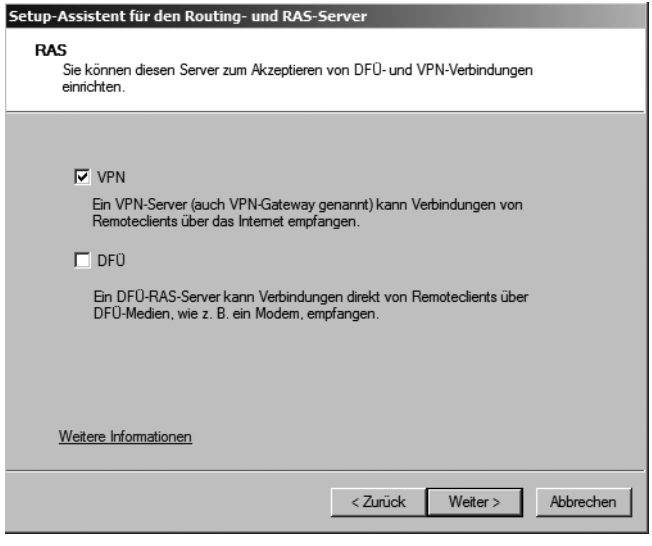
Nach dem Willkommensbildschirm konfigurieren Sie auf der nächsten Seite des Assistenten zunächst die Funktion des RAS-Servers. Für die Einwahlmöglichkeiten per DFÜ oder VPN wählen Sie die Option *RAS (DFÜ oder VPN)*.

Abbildg. 15.68 Erstellen der VPN-Einwahl



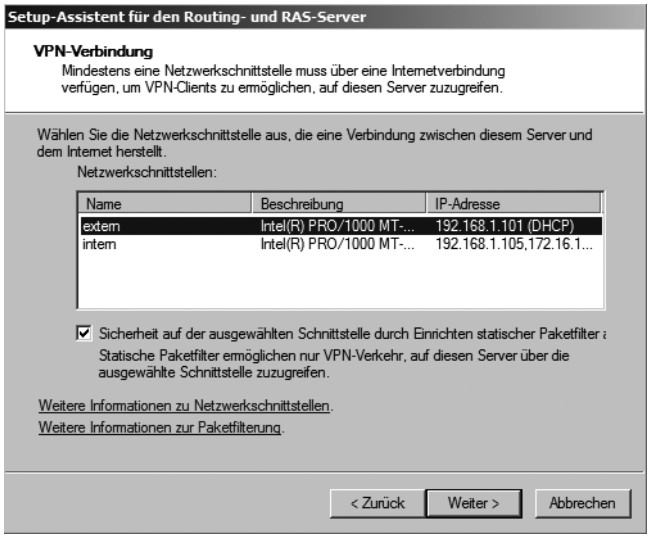
Auf der nächsten Seite des Assistenten aktivieren Sie das Kontrollkästchen *VPN*. Wollen Sie über diesen Server auch die Einwahl per Modem oder ISDN ermöglichen, können Sie auch das Kontrollkästchen *DFÜ* aktivieren, müssen den Server aber, am besten über eine aktive ISDN-Karte, mit dem Telefonnetz verbinden.

Abbildg. 15.69 Auswählen der RAS-Funktionalität des Servers



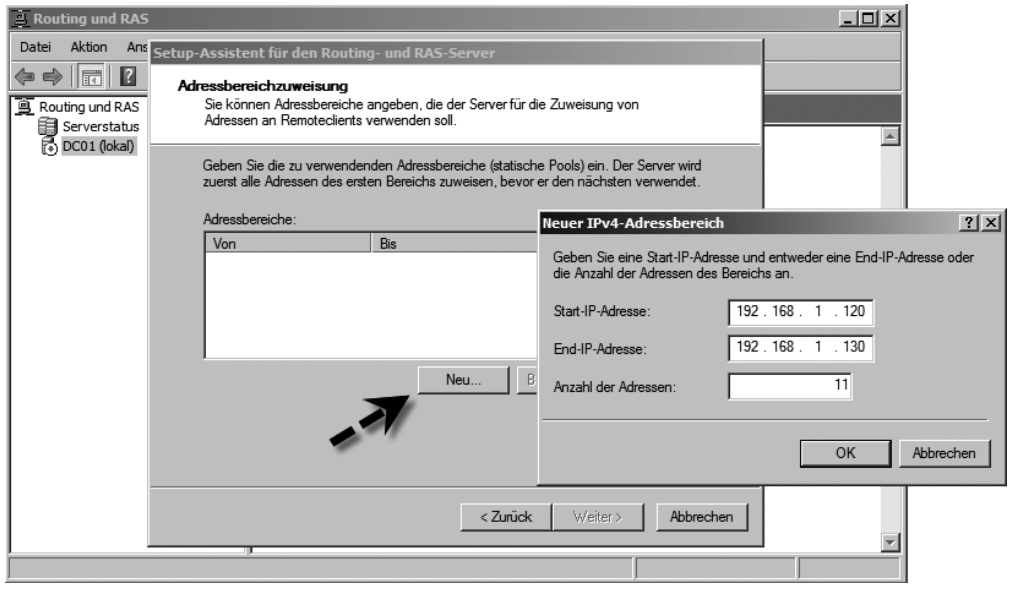
Auf der nächsten Seite des Assistenten legen Sie fest, an welcher Schnittstelle der Server auf Verbindungen warten soll. Hier verwenden Sie natürlich die Schnittstelle, die mit dem externen Netzwerk verbunden ist. Haben Sie im Server zwei Netzwerkkarten eingebaut, benennen Sie im Netzwerk- und Freigabecenter diese Verbindungen am besten in *intern* und *extern* um, damit Sie diese einfacher zuordnen können. Deaktivieren Sie zusätzlich noch die Option *Sicherheit auf der ausgewählten Schnittstelle durch Einrichten statischer Paketfilter.* Dadurch ist sichergestellt, dass die VPN-Clients Verbindung mit dem VPN-Server aufbauen können, um diesen zum Beispiel zu pingen, ohne dass eine Route gesetzt wird. Mithilfe dieser Option wird eine Basisfirewall konfiguriert, ein dynamischer Paketfilterdienst, mit dem Sie das private Netzwerk vor unerwünschtem Netzwerkverkehr schützen können.

Abbildg. 15.70 Festlegen der externen Schnittstelle für die VPN-Einwahl



Auf der nächsten Seite des Assistenten legen Sie fest, welche IP-Adresse die Clients bei der Einwahl erhalten sollen. Wählt sich ein Client per VPN in das Netzwerk ein, erhält er eine IP-Adresse im internen Netzwerk. Sie können entweder die IP-Adressen über einen DHCP-Server zuweisen lassen, in dem Sie die Option *Automatisch* auswählen, oder über die Option *Aus einen angegebenen Adressbereich* manuell die IP-Adressen im internen Netzwerk eingeben, die VPN-Clients zugewiesen werden. Wählen Sie in diesem Beispiel diese Option aus. So können Sie einen IP-Bereich festlegen, der VPN-Clients zugewiesen wird. Auf der nächsten Seite geben Sie den IP-Bereich ein, aus dem die VPN-Clients IP-Adressen zugeteilt bekommen (Abbildung 15.71).

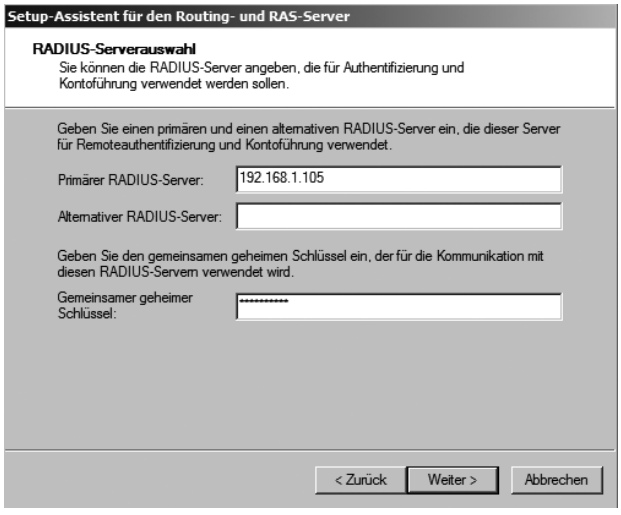
Abbildg. 15.71 Festlegen des IPv4-Adressbereiches für VPN-Clients



Auf der nächsten Seite aktivieren Sie die Option *Ja, diesen Server für die Verwendung eines RADIUS-Servers einrichten*. In diesem Fall wird die Authentifizierung der Clients nicht durch den einzelnen VPN-Server vorgenommen, sondern durch den RADIUS-Server. In der Testumgebung können Sie Netzwerkrichtlinienserver und VPN-Server auf einem gemeinsamen Server installieren. Dieser Server ist durch die Einrichtung bereits automatisch RADIUS-fähig und Sie können ihn selbst auch als RADIUS-Client konfigurieren. Natürlich können Sie auch VPN-Server und Netzwerkrichtlinienserver auf getrennte Maschinen installieren.

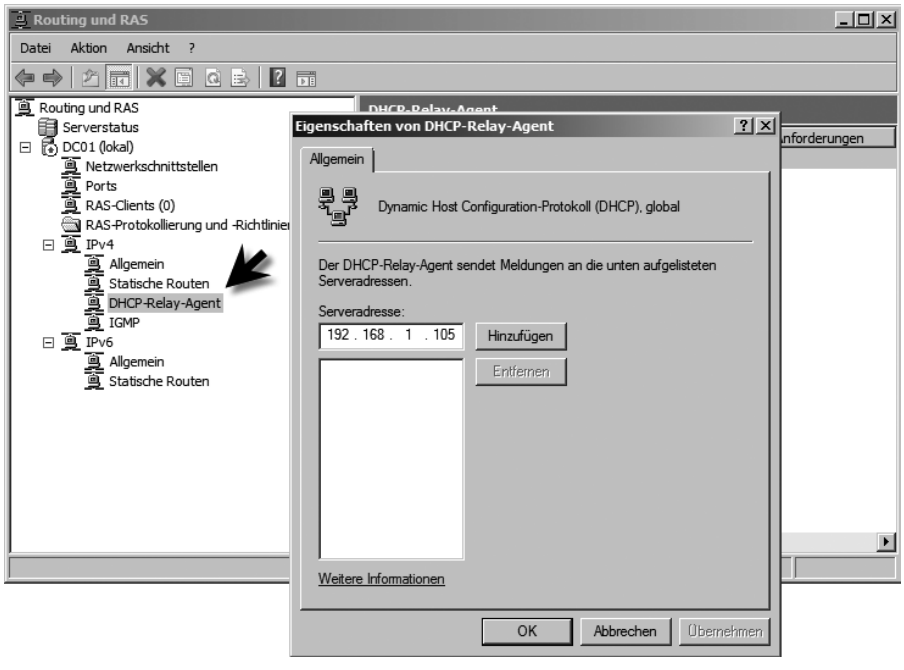
Auf der nächsten Seite des Assistenten legen Sie den RADIUS-Server fest sowie das Kennwort, das Sie zuvor konfiguriert haben (Abbildung 15.72). Das RADIUS-Protokoll ermöglicht es, die Berechtigung eines Benutzers für die Einwahl zu überprüfen, auch wenn der Benutzer nicht in der lokalen bzw. Domänenbenutzerdatenbank angelegt wurde, sondern auf einem fremden Server. Der RAS-Server reicht die Prüfung des Benutzernamens und des Passwortes an den angegebenen Server weiter, wenn sich ein Client einwählt. Klicken Sie auf *Fertig stellen*, um die Installation abzuschließen. Der Routing- und RAS-Dienst wird jetzt konfiguriert und gestartet. Nach der Auswahl schließen Sie den Assistenten ab. Anschließend wird durch den Assistenten *Routing und RAS* aktiviert. Sie erhalten anschließend noch verschiedene Meldungen, die Sie darauf hinweisen, dass Sie die Authentifizierungsoptionen festlegen müssen und den DHCP-Relay-Agenten konfigurieren müssen. Im DHCP-Relay-Agenten müssen Sie die IP-Adresse des DHCP-Servers hinterlegen. Der Relay-Agent antwortet auf die Anfragen von Clients und leitet diese an den DHCP-Server weiter. Dieser teilt eine IP-Adresse zu, die dann wiederum vom Relay-Agent dem Client mitgeteilt wird.

Abbildg. 15.72 Konfigurieren des RADIUS-Servers auf dem VPN-Server



Wenn Sie DHCP für VPN verwenden möchten, müssen Sie die IP-Adresse Ihres DHCP-Servers als Relay-Agent im RAS-Server eintragen, damit die Anfragen des RAS-Clients an den DHCP-Server weitergeleitet werden können. Sie erhalten beim ersten Start des Dienstes eine entsprechende Warnung. Klicken Sie dazu nach dem Starten des RAS-Dienstes auf *IPv4/DHCP-Relay-Agent* und rufen Sie die Eigenschaften auf. In den Eigenschaften tragen Sie die IP-Adresse Ihres DHCP-Servers ein.

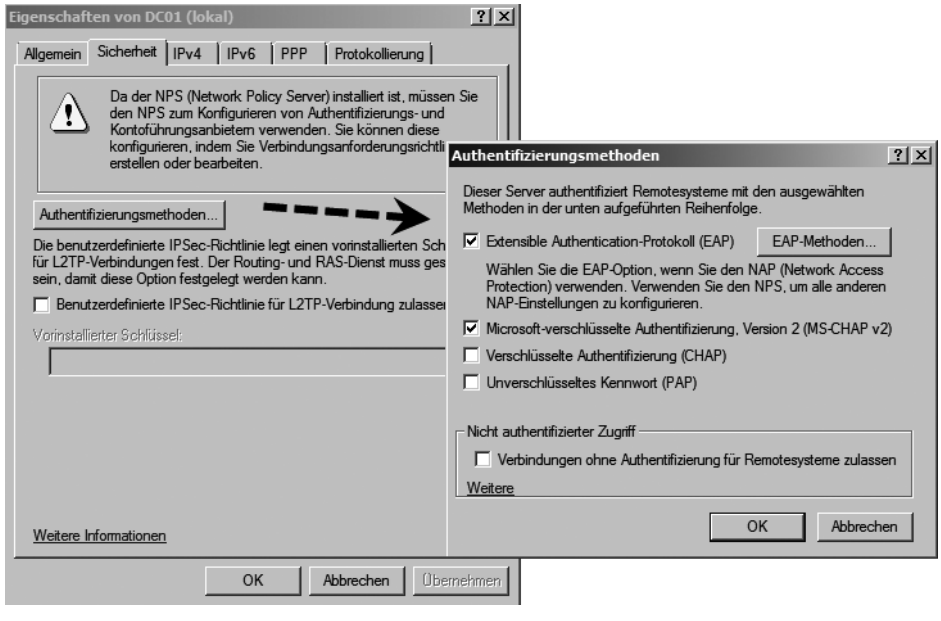
Abbildg. 15.73 Konfigurieren des DHCP-Relay-Agenten



Konfiguration der Authentifizierung für den VPN-Server

Der nächste Schritt besteht darin, dass Sie den VPN-Server noch konfigurieren. Sie müssen zum Beispiel noch die Authentifizierung für Clients festlegen. Starten Sie dazu die Verwaltungskonsole für Routing und RAS. Rufen Sie die Eigenschaften des VPN-Servers in der Konsole auf und wechseln Sie auf die Registerkarte *Sicherheit*. Klicken Sie anschließend auf *Authentifizierungsmethoden*. Das Extensible Authentication Protocoll (EAP) wurde bereits weiter vorne beschrieben. Stellen Sie sicher, dass *Extensible Authentication Protocol (EAP)* und *Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP v2)* ausgewählt sind. *PAP (Password Authentication Protocol)* verwendet Kennwörter mit Klartext und ist das einfachste Authentifizierungsprotokoll. Beim Aktivieren von PAP als Authentifizierungsprotokoll werden Benutzerkennwörter als Klartext gesendet. Durch das Abfangen von Paketen während des Authentifizierungsprozesses kann das Kennwort leicht entschlüsselt und für nicht autorisierten Intranetzugriff verwendet werden. Von der Verwendung von SPAP wird dringend abgeraten, besonders für VPN-Verbindungen. Wenn die PAP-Unterstützung auf dem RAS-Server deaktiviert ist, werden Klartextkennwörter vom DFÜ-Client nicht gesendet. Klicken Sie auf *EAP-Methoden* und überprüfen Sie, ob *Geschütztes (Protected) EAP (PEAP)* angezeigt wird (Abbildung 15.74).

Abbildg. 15.74 Konfiguration der VPN-Authentifizierungsmethoden

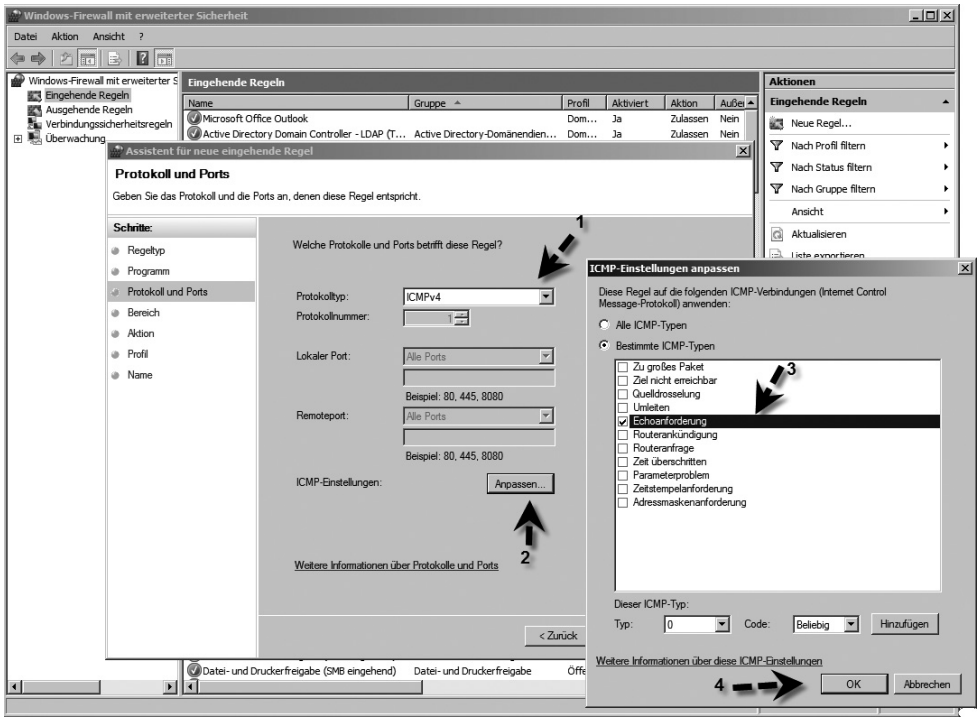


Erlauben von Ping zwischen VPN-Clients und VPN-Server

Zur Verifizierung der Verbindung zwischen dem VPN-Client im Internet und dem VPN-Server sollten Sie noch das ICMP-Protokoll in der Windows-Firewall freischalten. Ohne die Aktivierung dieses Protokolls wird ICMP und damit ein Ping blockiert. Das *Internet Control Message-Protokoll (ICMP)* ist dafür verantwortlich, Diagnosefunktionen bereitzustellen und Fehler aufgrund einer nicht erfolgreichen Datenübermittlung zu melden. Öffnen Sie dazu auf dem VPN-Server die erweiterte Verwaltungsoberfläche für die Windows-Firewall:

1. Der schnellste Weg hierzu führt über *Start/Ausführen/wf.msc*.
2. Klicken Sie mit der rechten Maustaste auf *Eingehende Regeln* und wählen Sie im Kontextmenü den Eintrag *Neue Regel* aus.
3. Wählen Sie im Konfigurationsfenster die Option *Benutzerdefiniert* aus.
4. Aktivieren Sie auf der nächsten Seite die Option *Alle Programme*.
5. Wählen Sie auf der nächsten Seite bei *Protokolltyp* die Option *ICMPv4* aus (Abbildung 15.75).
6. Klicken Sie auf *Anpassen*.
7. Aktivieren Sie die Option *Bestimmte ICMP-Typen*.
8. Aktivieren Sie das Kontrollkästchen *Echoanforderung*.
9. Klicken Sie auf *OK* und dann auf *Weiter*.
10. Klicken Sie auf *Weiter*, um die Standardeinstellungen für den DHCP-Bereich zu bestätigen.
11. Klicken Sie noch mal auf *Weiter* und stellen Sie sicher, dass die Option *Verbindung zulassen* aktiviert ist.

Abbildg. 15.75 Konfigurieren der Windows-Firewall für die Aktivierung von ICMP-Echoanforderungen



12. Im nächsten Fenster bestätigen Sie die Aktivierung der Regel für alle Netzwerk-Profile.
13. Weisen Sie der Regel einen entsprechenden Namen zu und schließen Sie die Erstellung der Regel ab.

Testen der Verbindung mit einem Client

Auf Windows Vista-PCs, die Mitglied einer Domäne sind, wird das Sicherheitscenter deaktiviert. Das Sicherheitscenter ist aber dafür zuständig die Sicherheitsverifizierungsprüfung (Statement of Health, SoH) an den NPS-Server zu übermitteln. Um NAP unter Windows Vista zu testen, müssen Sie dieses daher aktivieren, wenn der PC Mitglied der Domäne ist. Das kann zum Beispiel bei Firmennotebooks durchaus der Fall sein. Der beste Weg in einer Testumgebung dazu ist die Aktivierung über lokale Richtlinien. Sie finden die Einstellung auch über Gruppenrichtlinien. Gehen Sie dazu folgendermaßen vor:

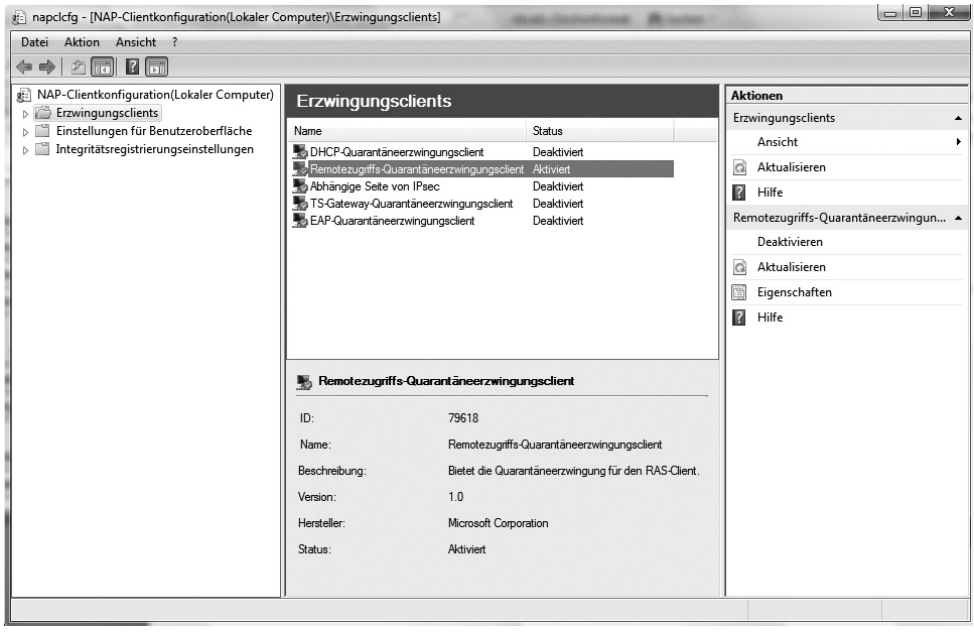
1. Rufen Sie über *Start/Ausführen/gpedit.msc* den Gruppenrichtlinien-Editor auf.
2. Navigieren Sie in der Konsolenstruktur zum Eintrag *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Sicherheitscenter.*
3. Aktivieren Sie die Richtlinie *Sicherheitscenter aktivieren (nur Domänencomputer).*

Aktivieren des DHCP-Quarantäneerzwingungsclients

Die nächste Aufgabe, die Sie durchführen müssen, ist die Aktivierung der RAS-Client-NAP-Unterstützung auf dem VPN-Client:

1. Starten Sie dazu auf dem Vista-PC die Verwaltungskonsole des NAP-Clients (Abbildung 15.76), indem Sie über die Tastenkombination Ä+R das Ausführen-Dialogfeld öffnen und darin den Befehl *napclcfg.msc* eintragen.
2. Klicken Sie auf den Konsoleneintrag *Erzwingungsclients*.
3. Aktivieren Sie den *Remotezugriffs-Quarantäneerzwingungsclient*.

Abbildg. 15.76 Den Remotezugriffs-Quarantäneerzwingungsclient aktivieren



NAP-Agent (Network Access Protection) aktivieren

Der nächste Schritt zur Anbindung von Windows Vista an eine NAP-Infrastruktur ist die Aktivierung des Systemdienstes *NAP-Agent (Network Access Protection)*. Setzen Sie den Starttyp dieses Dienstes auf *Automatisch* und starten Sie diesen. Testen Sie anschließend, ob Sie vom VPN-Client aus den VPN-Server über dessen IP-Adresse im Internet anpingen können. Da Sie ICMP für den VPN-Server aus dem Internet erlaubt haben, sollten Sie nach kurzer Zeit eine Antwort erhalten.

Erstellen und testen der VPN-Verbindung

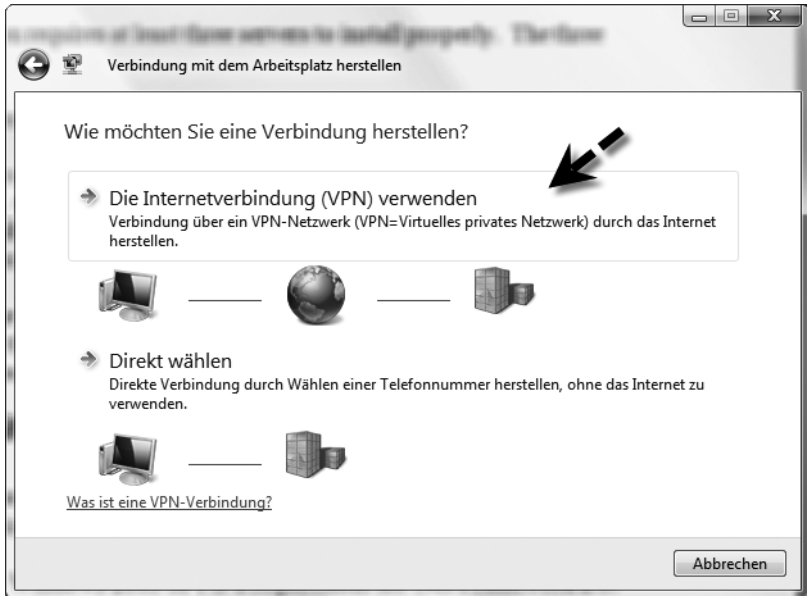
Der nächste Schritt in diesem Workshop besteht darin, dass Sie auf dem Client eine Wähl-VPN-Verbindung einrichten, über die Sie sich mit der externen IP-Adresse des VPN-Servers verbinden können. Gehen Sie dazu folgendermaßen vor:

1. Starten Sie auf dem Client das *Netzwerk- und Freigabecenter.*
2. Klicken Sie auf *Eine Verbindung oder ein Netzwerk einrichten*.
3. Wählen Sie auf dem neuen Fenster die Option *Verbindung mit dem Arbeitsplatz herstellen* (Abbildung 15.77).

Abbildg. 15.77 Erstellen einer VPN-Verbindung unter Windows Vista

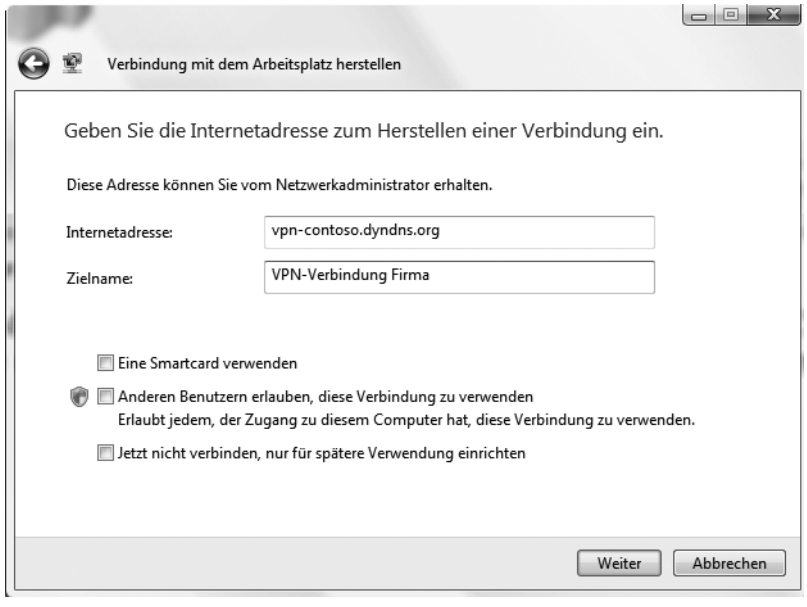
4. Klicken Sie auf *Weiter* und im nächsten Fenster auf *Die Internetverbindung (VPN) verwenden* (Abbildung 15.78).

Abbildg. 15.78 Erstellen einer VPN-Verbindung unter Windows Vista



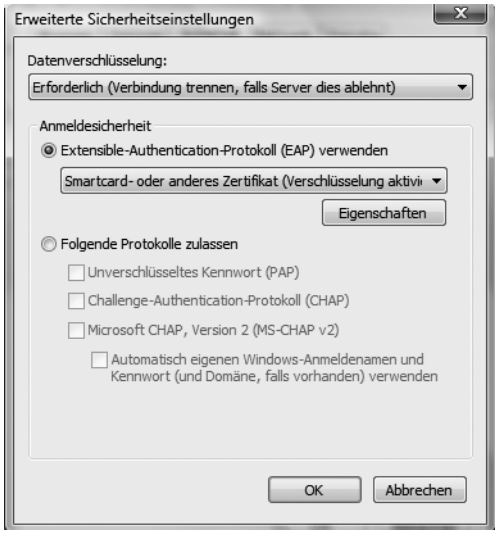
5. Auf dem nächsten Fenster legen Sie den DNS-Namen oder die IP-Adresse fest zu der sich der Client verbinden sollen. Hier tragen Sie die externe IP-Adresse oder den DNS-Namen des VPN-Servers ein (Abbildung 15.79).

Abbildg. 15.79 Eintragen des VPN-Servers unter Windows Vista



6. Tragen Sie anschließend den Benutzernamen, die Domäne und das Kennwort für die Anmeldung ein und lassen Sie sich mit dem Netzwerk verbinden.
7. Sollte die Verbindung nicht hergestellt werden (was wir an dieser Stelle erwarten), erhalten Sie eine entsprechende Meldung. Hier sollten Sie auf jeden Fall bestätigen, dass die Verbindung zwar nicht hergestellt werden kann, aber dass Sie diese trotzdem zur späteren Benutzung speichern wollen.
8. Im Anschluss wird die Verbindung noch konfiguriert. Klicken Sie dazu im Netzwerk- und Freigabecenter auf den Link *Netzwerkverbindungen verwalten*. Dieses Konfigurationsfenster, das auch für die Konfiguration der Netzwerkverbindungen im LAN verwendet wird, können Sie auch über die Tastenkombination Ä+R und Eingabe von *ncpa.cpl* starten (Abbildung 15.80).
9. Rufen Sie die Eigenschaften der VPN-Verbindung auf und wechseln Sie zur Registerkarte *Sicherheit*.
10. Aktivieren Sie die Option *Erweitert*.
11. Klicken Sie auf *Einstellungen*.
12. Aktivieren Sie die Option *Extensible-Authentication-Protokoll (EAP)* verwenden.
13. Wählen Sie aus dem Dropdown-Menü die Option *Geschütztes EAP (PEAP) (Verschlüsselung aktiviert)* aus.
14. Klicken Sie auf *Eigenschaften*.
15. Stellen Sie sicher, dass die Option *Serverzertifikat überprüfen* aktiviert ist.
16. Deaktivieren Sie die Option *Verbindung mit diesen Servern herstellen*.
17. Aktivieren Sie als Authentifizierungsmethode die Option *Geschütztes Kennwort (EAP-MSCHAP v2)*.
18. Deaktivieren Sie die Option *Schnelle Wiederherstellung der Verbindung aktivieren*.
19. Aktivieren Sie die Option *Quarantäneüberprüfungen aktivieren*.
20. Bestätigen Sie alle Fenster mit *OK*.

Abbildg. 15.80 Konfigurieren der VPN-Verbindung für die Unterstützung von NAP

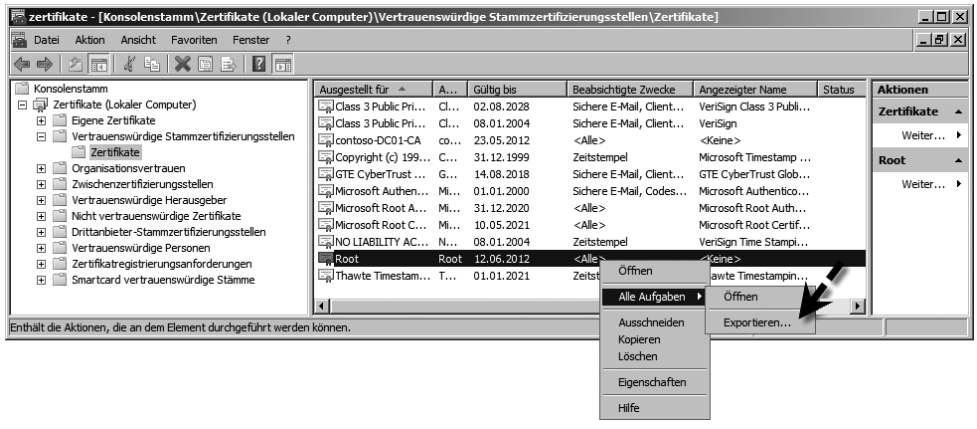


Hinterlegen des Stammzertifizierungsstellen-Zertifikats auf dem Client

Damit sich ein Client über die in diesem Workshop konfigurierte Sicherheitsoptionen einwählen kann, benötigt er ein Zertifikat. Dieses Zertifikat kann aber vom VPN-Server nur dann ausgestellt werden, wenn das Stammzertifikatsstellen-Zertifikat auf dem Client in die vertrauenswürdigen Stammzertifizierungsstellen integriert worden ist. Ist der Client Mitglied der Domäne, wurde diese bereits automatisch durchgeführt. Ist der Client kein Mitglied der Domäne, können Sie das Stammzertifikatsstellen-Zertifikat auf einem Mitgliedscomputer der Domäne in eine Datei exportieren und müssen dieses auf dem Client-PC importieren. Gehen Sie dazu folgendermaßen vor:

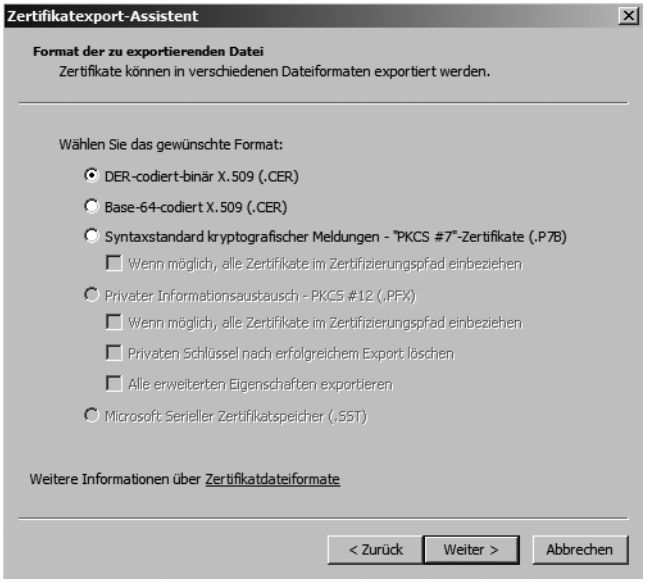
1. Öffnen Sie auf dem NPS-Server wie bereits beschrieben das Snap-In zur Verwaltung der lokalen Zertifikate.
2. Klicken Sie auf den Menüpunkt *Zertifikate/Vertrauenswürdige Stammzertifizierungsstellen/Zertifikate*.

Abbildg. 15.81 Exportieren des Zertifikats der Stammzertifizierungsstelle des Unternehmens



3. Klicken Sie mit der rechten Maustaste auf das Zertifikat Ihrer Stammzertifizierungsstelle und wählen Sie im Kontextmenü den Eintrag *Alle Aufgaben/Exportieren* aus.
4. Bestätigen Sie den Willkommensbildschirm des Zertifikatexport-Assistenten und aktivieren Sie im nächsten Fenster die Option *DER-codiert-binär X.509 (.CER)*.

Abbildg. 15.82 Auswählen des Formats für den Zertifikatexport

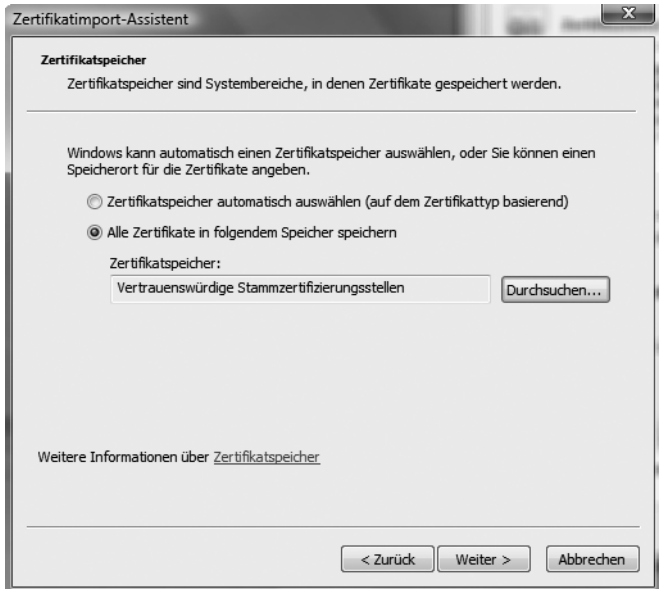


5. Im nächsten Fenster wählen Sie den Pfad aus, in dem das Zertifikat gespeichert werden soll.
6. Schließen Sie den Export des Zertifikats ab.

Abbildg. 15.83 Anzeigen des Zertifikats auf dem Client

7. Anschließend müssen Sie das Zertifikat per Mail oder Datenaustausch auf den Client kopieren, der sich per VPN einwählen soll.
8. Klicken Sie auf dem Client doppelt auf die Zertifikatedatei.
9. Es öffnet sich das Zertifikat und Sie erkennen auf einen Blick, dass dieses nicht als gültig klassifiziert wird, weil Windows die Zertifikatsstelle nicht erkennt (Abbildung 15.83).
10. Klicken Sie als Nächstes auf die Schaltfläche *Zertifikat installieren*.
11. Es öffnet sich der Assistent auf dem Client, mit dessen Hilfe Sie das Zertifikat in den lokalen Zertifikatsspeicher integrieren können.
12. Wählen Sie die Option *Alle Zertifikate in folgendem Speicher speichern*.
13. Klicken Sie auf *Durchsuchen*.
14. Wählen Sie den Speicher *Vertrauenswürdige Stammzertifizierungsstellen* aus.

Abbildg. 15.84 Auswählen des Zertifikatspeichers für das Zertifikat der Stammzertifizierungsstelle Ihres Unternehmens



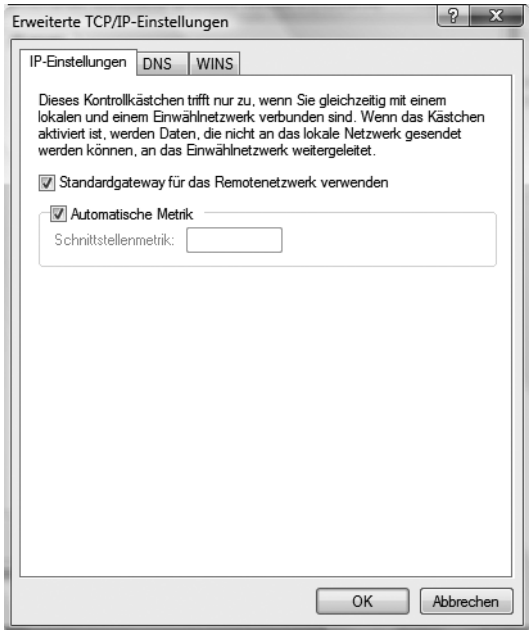
15. Bestätigen Sie die Sicherheitsmeldung und lassen Sie das Zertifikat installieren.
16. Klicken Sie anschließend nochmals doppelt auf die Zertifikatedatei, sehen Sie, dass jetzt die Zertifikatsstelle als vertrauenswürdig klassifiziert worden ist. Das Zertifikat wird anschließend auch in dem ausgewählten Zertifikatsspeicher auf dem Client angezeigt.

VPN-Clients und der Internetzugriff

Wenn sich ein Client über das VPN verbindet, wird der Verkehr seines PCs zum Internet blockiert. Das hat den Vorteil, dass keine Viren oder Trojaner aus dem Internet in Ihr Firmennetzwerk übertragen werden können. Vor allem wenn Sie bei der Erstellung der Firewallrichtlinie den gesamten Datenverkehr von den VPN-Clients zum internen Netzwerk zulassen, spielt dieser Punkt eine wichtige Rolle. Manchmal ist es jedoch nicht gewollt, dass der Internetverkehr auf dem Client-PC blockiert wird,

wenn sich der Client per VPN einwählt. Sie können diese Blockade deaktivieren. Navigieren Sie dazu auf dem Client-PC in den Eigenschaften der VPN-Verbindung über die Registerkarte *Netzwerk/Internetprotokoll (TCP/IP)/Eigenschaften/Erweitert* und deaktivieren Sie die Option *Standardgateway für das Remotenetzwerk verwenden*. Danach ist der Internetverkehr wieder möglich (Abbildung 15.85).

Abbildg. 15.85 Konfigurieren des Standardgateways bei der VPN-Einwahl



Fehlersuche und Behebung für die VPN-Einwahl mit NAP

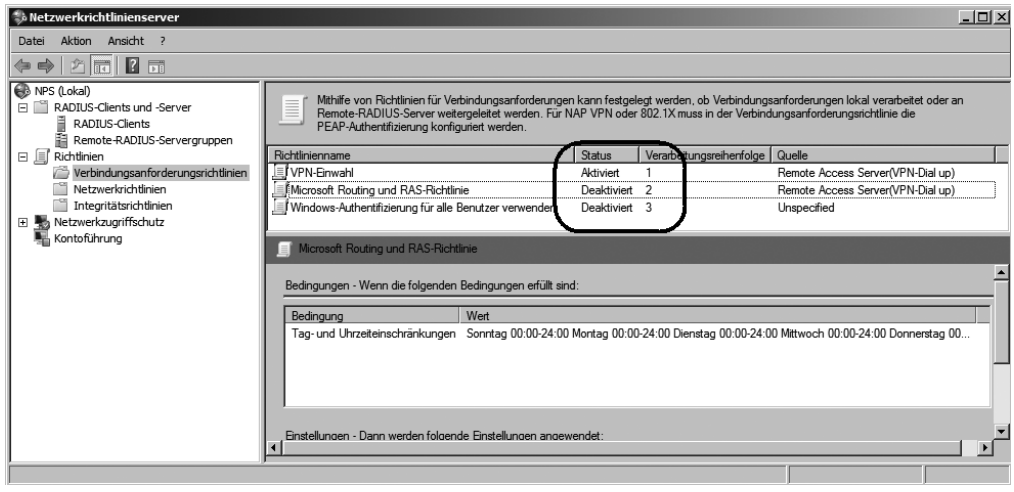
Haben Sie alle Eingaben vorgenommen, wie in den letzten Abschnitten besprochen, sollte die Einwahl funktionieren. Erhalten Sie eine Fehlermeldung angezeigt und ist die Einwahl nicht möglich, überprüfen Sie nochmals, ob Sie alle Einstellungen korrekt vorgenommen haben.

Überprüfen der Verbindungsanforderungsrichtlinien

Oft wird von Windows bei der Aktivierung von Routing und RAS eine neue Verbindungsanforderungsrichtlinie angelegt, die in der Hierarchie vor Ihrer manuell erstellten Richtlinie angeordnet wird.

Klicken Sie alle standardmäßig angelegten Verbindungsanforderungsrichtlinien mit der rechten Maustaste an und deaktivieren Sie diese. Stellen Sie sicher, dass sich Ihre Richtlinie ganz oben in der Hierarchie befindet und aktiviert ist.

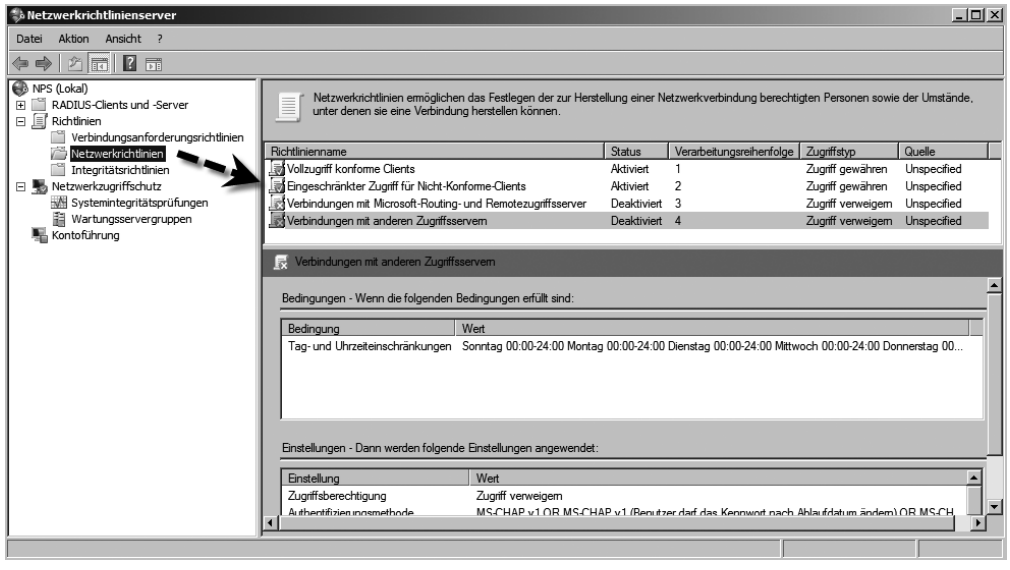
Abbildg. 15.86 Überprüfen der Verbindungsanforderungsrichtlinien in der Verwaltungskonsole des NPS



Überprüfen der Integritätsrichtlinien, Netzwerkrichtlinien und der Windows-Sicherheitsintegritätsverifizierung

Diese drei Funktionen sollten Sie als Nächstes überprüfen, da diese aufeinander aufbauen. Die Windows-Sicherheitsintegritätsverifizierung muss aktiviert und richtig konfiguriert sein, die Integritätsrichtlinien auf dieser aufbauen. Schließlich verwenden die Netzwerkrichtlinien die Integritätsrichtlinie zur Verwaltung der Clients (Abbildung 15.87). Alle standardmäßigen Netzwerkrichtlinien sollten deaktiviert sein. Nur Ihre manuell erstellten Richtlinie sollten aktiviert und sich in der Hierarchie ganz oben befinden.

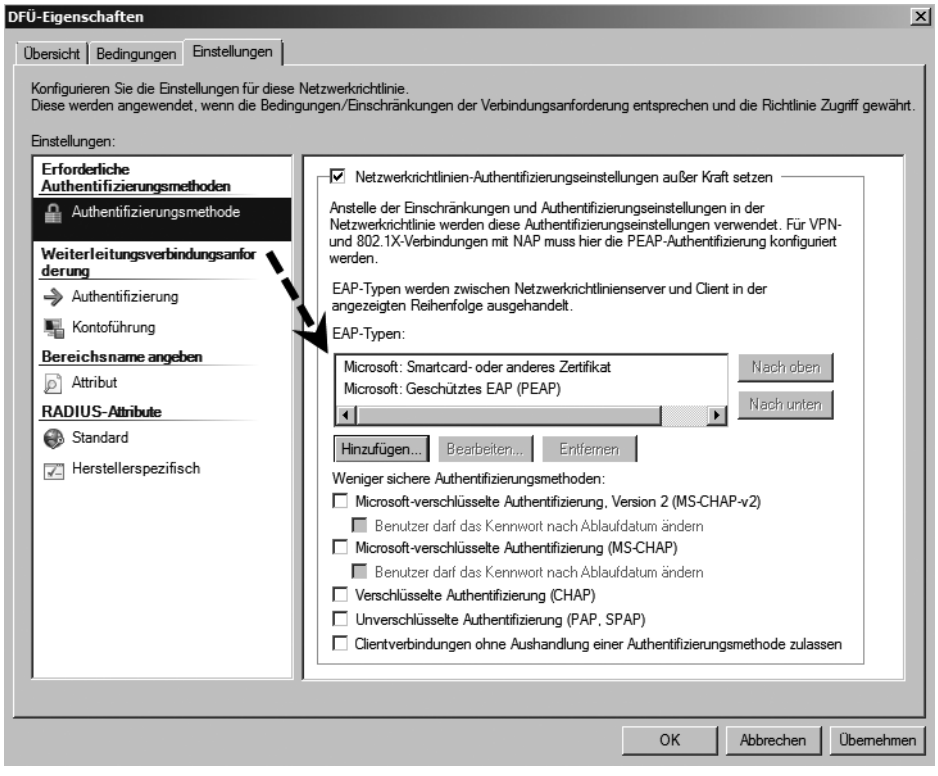
Abbildg. 15.87 Überprüfen der Netzwerkrichtlinien



Überprüfung der Client-Einstellungen

Als Nächstes sollten Sie überprüfen, dass auf dem Client der Erzwingungsclient aktiviert ist, der entsprechende Dienst gestartet wurde und die Authentifizierung auf dem VPN-Client identisch mit der Verbindungsanforderungsrichtlinie konfiguriert ist.

Abbildg. 15.88 Verifizieren der richtigen Authentifizierungseinstellungen zwischen Client und Server



Verwalten und konfigurieren der RAS-Benutzer und RAS-Ports

Die effizienteste Methode, um mit Windows Server 2008 ein VPN aufzubauen, ist der Einsatz von PPTP. Dieser Verbindungstyp ist zwar nicht so sicher wie L2TP oder IPSec, aber es gibt auch keinen dokumentierten Fall, wo ein VPN auf Basis von PPTP gehackt wurde.

Point to Point Tunnel Protocol (PPTP)

PPTP-basierter VPN-Datenverkehr besteht aus einer TCP-Verbindung zum TCP-Port 1723 auf dem VPN-Server, um den Tunnel zu verwalten, und aus GRE- (Generic Routing Encapsulation) gekapselten Paketen für die VPN-Daten. PPTP-Datenverkehr kann jedoch Probleme mit Firewalls, NATs und Webproxys haben. Um Probleme zu vermeiden, müssen Firewalls so konfiguriert werden, dass sie sowohl die TCP-Verbindung als auch GRE-gekapselte Daten ermöglichen. Viele Experten stufen

PPTP mittlerweile als sicher ein, auch wenn die Verschlüsselung nicht so stark ist wie die von L2TP. PPTP ermöglicht die verschlüsselte Einkapselung von verschiedenen Netzwerkprotokollen und unterstützt Schlüssellängen bis zu 128 Bit. Nachdem die Authentifizierung durchgeführt wurde, wird die Verbindung verschlüsselt. Die Verschlüsselung baut auf dem Kennwort der Authentifizierung auf. Je komplexer das Kennwort ist, umso besser ist die Verschlüsselung. Da die Verschlüsselung und der Transport der einzelnen IP-Pakete durch das GRE-Protokoll durchgeführt wird, müssen Sie darauf achten, dass die Hardwarefirewall bzw. der DSL-Router, den Sie vor dem ISA-Server im Internet platzieren, dieses Protokoll beherrscht. Viele preisgünstige Modelle beherrschen GRE nicht. In diesem Fall können Sie kein PPTP-VPN mit einem ISA Server 2004 aufbauen. Sie sollten daher bereits den Erwerb der Hardwarefirewall, die vor dem ISA-Server im Internet steht, in die Planung einbeziehen.

Layer 2 Tunnel Protocol (L2TP)

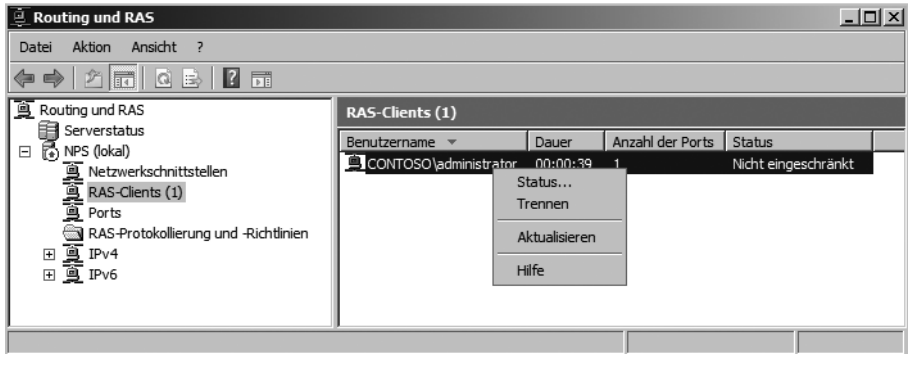
Die zweite Variante, ein VPN aufzubauen, ist das Layer 2 Tunnel Protocol (L2TP). Dieses Protokoll ist sicherer als PPTP, aber dafür auch komplexer in der Einrichtung. Auch bei diesem Protokoll werden die IP-Pakete in die Verschlüsselung eingekapselt. Das L2TP verwendet IPSec, um eine Verschlüsselung aufzubauen. Beim Aufbau eines VPN mit L2TP wird der Datenverkehr, im Gegensatz zu PPTP, bereits vor der Authentifizierung zuverlässig verschlüsselt. Da L2TP zur Verschlüsselung des Datenverkehrs IPSec verwendet, kann mit diesem VPN-Typ auch eine 3DES-Verschlüsselung durchgeführt werden. Der Einsatz eines VPN auf Basis von L2TP setzt eine Zertifizierungsstelleninfrastruktur voraus.

Vor allem mittelständische Unternehmen tun sich wesentlich leichter, wenn als VPN-Protokoll PPTP verwendet wird. Der Einsatz eines VPNs mit L2TP ist nur Experten zu empfehlen, die genau wissen, wie Zertifizierungsstellen eingerichtet werden und L2TP bzw. IPSec funktionieren. Für den schnellen, effizienten und sicheren Aufbau eines VPNs ist PPTP sicherlich die beste Wahl.

Verwaltung und Überwachung des VPNs

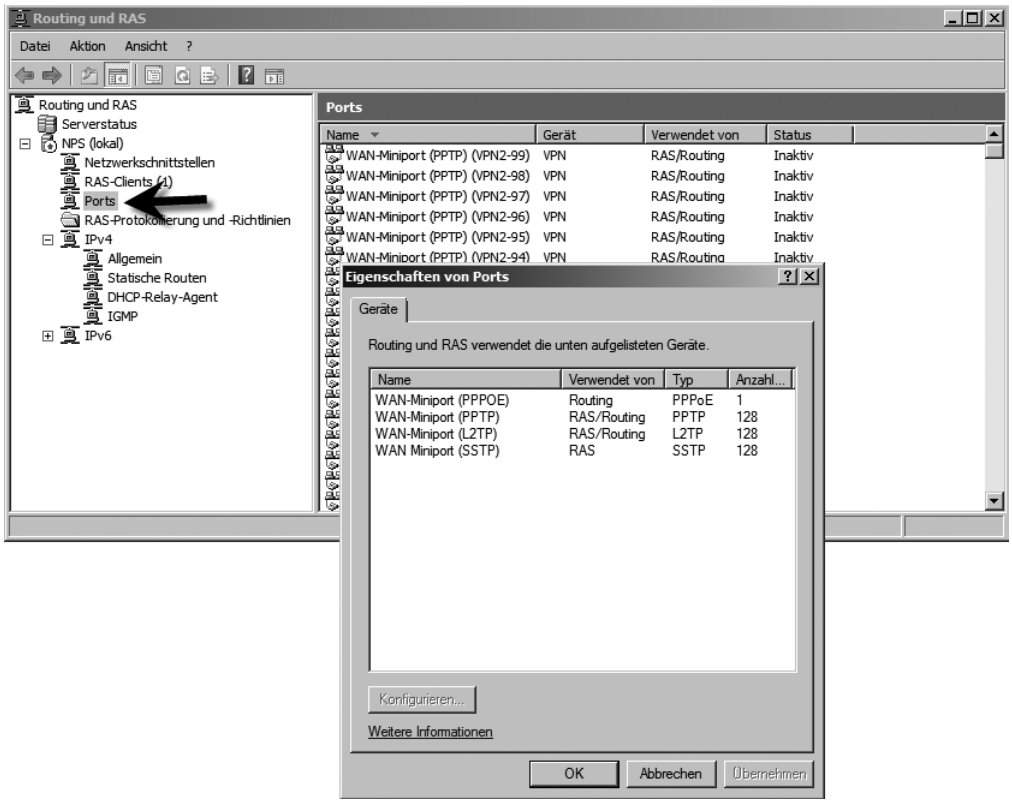
Sie können die Konfiguration über *Start/Verwaltung/Routing und RAS* überprüfen. Öffnen Sie dieses Snap-In, sehen Sie die Konfigurationen, die der Assistent auf dem Windows Server 2008 durchgeführt hat (Abbildung 15.89). Klicken Sie auf den Konsoleneintrag *RAS-Clients*, sehen Sie alle derzeit verbundenen VPN-Clients sowie deren aktuelle Verbindungsdauer. Klicken Sie mit der rechten Maustaste auf den Client, können Sie dessen Verbindung vom Server aus trennen.

Abbildg. 15.89 Verwalten der eingewählten RAS-Benutzer



Klicken Sie mit der rechten Maustaste auf den Eintrag *Ports*, können Sie die Anzahl der Ports definieren und damit der gleichzeitig möglichen Einwahlen (Abbildung 15.90). Verwenden Sie zum Beispiel nur PPTP und kein L2TP, können Sie die benötigen Ports für L2TP auf 0 setzen. Wollen Sie für die Einwahl für PPTP weniger Ports zur Verfügung stellen, können Sie auch diese Anzahl reduzieren.

Abbildg. 15.90 Konfiguration der Einwählports unter Windows Server 2008



HTTPS-VPN über Secure Socket Tunneling Protocol

Windows Server 2008 und Windows Vista SP1 unterstützen neben PPTP und L2TP auch das *Secure Socket Tunneling Protocol (SSTP)*. Mit diesem Protokoll wird ein VPN auf Basis von HTTPS aufgebaut, welches viel leichter durch Firewalls und NAT-Geräten geschleust werden kann. Meistens wird der Port 443 in Firewalls nicht geschlossen und auch eine Verbindung über Proxyserver ist möglich. SSTP verwendet eine HTTP-über-SSL-Sitzung zwischen VPN-Clients und -Servern, um gekapselte IPv4- oder IPv6-Pakete auszutauschen. Ein IPv4- oder IPv6-Paket wird zunächst zusammen mit einem PPP-Header und einem SSTP-Header gekapselt. Die Kombination aus dem IPv4- oder IPv6-Paket, dem PPP-Header und dem SSTP-Header wird durch die SSL-Sitzung verschlüsselt. Ein TCP-Header und ein IPv4-Header werden hinzugefügt, um das Paket zu vervollständigen. SSTP unterstützt allerdings keine authentifizierten Webproxykonfigurationen, in denen der Proxy während der

HTTPS-Verbindungsanforderung irgendeine Form von Authentifizierung verlangt. Sie brauchen auch nicht IIS installieren, da der Routing- und RAS-Dienst eingehende Verbindungen überwacht. Es können jedoch gleichzeitig sowohl Routing- und RAS-Dienst als auch IIS auf demselben Server vorhanden sein. Auf dem SSTP-Server muss ein Computerzertifikat mit der Serverauthentifizierung oder der Universaleigenschaft »Erweiterte Schlüsselverwendung« (Enhanced Key Usage, EKU) installiert sein. Dieses Computerzertifikat wird vom SSTP-Client verwendet, um den SSTP-Server zu authentifizieren, wenn die SSL-Sitzung eingerichtet wird. Der SSTP-Client überprüft das Computerzertifikat des SSTP-Servers. Um dem Computerzertifikat zu vertrauen, muss die Stammzertifizierungsstelle (CA) der CA, die das Computerzertifikat des SSTP-Servers ausgestellt hat, auf dem SSTP-Client installiert sein. Im Unterschied zu den PPTP- und L2TP/IPsec-Protokollen in Windows XP und Windows Server 2003 unterstützt SSTP keine Standort-zu-Standort-VPN-Verbindungen.

Ablauf beim Verbinden über SSTP

Wenn ein Benutzer auf einem Computer, der Windows Server 2008 oder Windows Vista mit Service Pack 1 ausführt, eine SSTP-basierte VPN-Verbindung initiiert, findet Folgendes statt:

1. Der SSTP-Client richtet eine TCP-Verbindung mit dem SSTP-Server zwischen einem dynamisch zugewiesenen TCP-Port auf dem Client und TCP-Port 443 auf dem Server ein.
2. Der SSTP-Client sendet eine SSL-Client-Begrüßungsnachricht, die anzeigt, dass der Client eine SSL-Sitzung mit dem SSTP-Server einrichten will.
3. Der SSTP-Server sendet dem SSTP-Client sein Computerzertifikat.
4. Der SSTP-Client überprüft das Computerzertifikat, bestimmt die Verschlüsselungsmethode für die SSL-Sitzung, generiert einen SSL-Sitzungsschlüssel und verschlüsselt diesen dann mit dem öffentlichen Schlüssel des Zertifikats des SSTP-Servers.
5. Der SSTP-Client sendet das verschlüsselte Formular des SSL-Sitzungsschlüssels zum SSTP-Server.
6. Der SSTP-Server entschlüsselt den verschlüsselten SSL-Sitzungsschlüssel mit dem privaten Schlüssel seines Computerzertifikats. Die gesamte zukünftige Kommunikation zwischen dem SSTP-Client und dem SSTP-Server wird mit der ausgehandelten Verschlüsselungsmethode und dem SSL-Sitzungsschlüssel verschlüsselt.
7. Der SSTP-Client sendet eine HTTP-über-SSL-Anforderungsnachricht zum SSTP-Server.
8. Der SSTP-Client handelt mit dem SSTP-Server einen SSTP-Tunnel aus.
9. Der SSTP-Client handelt mit dem SSTP-Server eine PPP-Verbindung aus. Zu dieser Aushandlung gehören die Authentifizierung der Anmeldeinformationen des Benutzers mit einer PPP-Authentifizierungsmethode und die Konfiguration der Einstellungen für den IPv4- oder IPv6-Datenverkehr. Verbindungen, die unter Verwendung von *PPP (Point-to-Point-Protokoll)* erstellt wurden, müssen den Standards entsprechen, die in PPP-RFCs festgelegt sind. Nachdem eine physische oder logische Verbindung mit einem PPP-basierten RAS-Server hergestellt ist, wird unter Verwendung der folgenden Aushandlungen eine PPP-Verbindung eingerichtet. PPP verwendet LCP (Link Control-Protokoll), um Verknüpfungsparameter wie die maximale PPP-Datenblockgröße, die Verwendung von Multilink und die Verwendung eines bestimmten PPP-Authentifizierungsprotokolls auszuhandeln. Link Control-Protokoll (LCP) konfiguriert die PPP-Datenblockerstellung. Die PPP-Datenblockerstellung bestimmt, auf welche Weise die Daten zu Datenblöcken zusammengefasst werden, bevor sie im WAN übertragen werden. Das standardmäßige PPP-Datenblockformat stellt sicher, dass RAS-Programme aller Hersteller miteinander

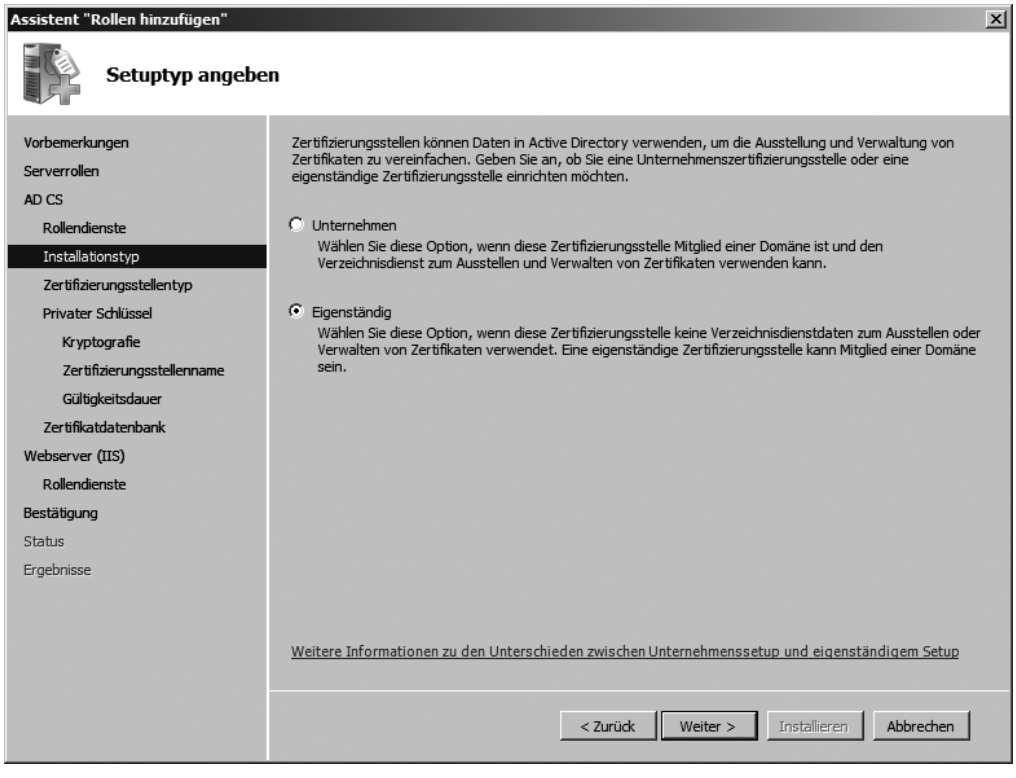
kommunizieren können und Datenpakete von jeder RAS-Software erkennen, die den PPP-Standards entspricht. Der RAS-Client und der RAS-Server tauschen Nachrichten entsprechend des ausgehandelten Authentifizierungsprotokolls aus. Wenn EAP (Extensible Authentication Protocol) verwendet wird, handeln der Client und der Server eine bestimmte EAP-Methode aus, die als EAP-Typ bekannt ist. Dann werden Nachrichten dieses EAP-Typs ausgetauscht. Die Nutzung von EAP ist die von Microsoft favorisierte Variante für Wählverbindungen und erlaubt eine einheitliche Authentisierung eines Nutzers über LAN, WLAN und WAN. Wenn für die DFÜ-Verbindung der Rückruf konfiguriert ist, wird die physische Verbindung beendet, und der RAS-Server ruft den RAS-Client zurück.

10. Der SSTP-Client beginnt, über die PPP-Verbindung IPv4- oder IPv6-Datenverkehr zu senden.

Installation von SSTP

Um SSTP in einer Active Directory-Domäne verwenden zu können, müssen nicht alle Server und die Domäne zu Windows Server 2008 migriert werden. Es reicht der Einsatz eines VPN-Servers mit Windows Server 2008. Auf den Clients muss Windows Vista SP1 installiert sein. Die Berechtigung für die Einwahl der Benutzer erfolgt identisch wie bei Berechtigungen über andere VPN-Methoden. Benutzern müssen nur die entsprechenden Rechte zugewiesen werden.

Abbildg. 15.91 Installieren einer eigenständigen Zertifizierungsstelle für die Unterstützung von SSTP



Vorbereiten der Installation von SSTP – Zertifizierungsstelle vorbereiten

Damit SSTP verwendet werden kann, muss der Rollendienst *Zertifizierungsstellen-Webregistrierung* der Rolle *Active Directory-Zertifikatsdienste* installiert sein. Der beste Weg ist, wenn Sie auf dem VPN-Server selbst eine Zertifizierungsstelle installieren und zwar als Typ *Eigenständig, keine Unternehmenszertifizierungsstelle* (Abbildung 15.91). Die Zertifizierungsstelle muss außerdem als Stammzertifizierungsstelle installiert werden. Alle weiteren Einstellungen wählen Sie so wie in Kapitel 17 erklärt. Für eine Testumgebung und auch für die meisten Produktivumgebungen verwenden Sie einfach die Standardeinstellungen.

Damit der Zugriff über SSTP funktioniert, benötigen Sie eine Zertifizierungsstelle mit den Active Directory-Zertifikatsdiensten (siehe Kapitel 17). Wollen Sie die Funktion in einer Testumgebung konfigurieren, benötigt der Server ebenfalls zwei Netzwerkkarten. Eine Karte ist mit dem internen Netzwerk, die andere mit dem Internet oder der Firewall verbunden. Der Server sollte Mitglied der Domäne sein.

Sicherheitseinstellungen im Internet Explorer auf dem VPN-Server konfigurieren

Nachdem die Zertifizierungsstelle auf dem Server installiert wurde, muss auf dem VPN-Server noch das Serverzertifikat installiert werden, über welches das SSTP-VPN ermöglicht wird. Da der Internet Explorer 7 von Windows Server 2008 sehr strenge Sicherheitseinstellungen aufweist, müssen zunächst in den Optionen des Internet Explorers Änderungen vorgenommen werden:

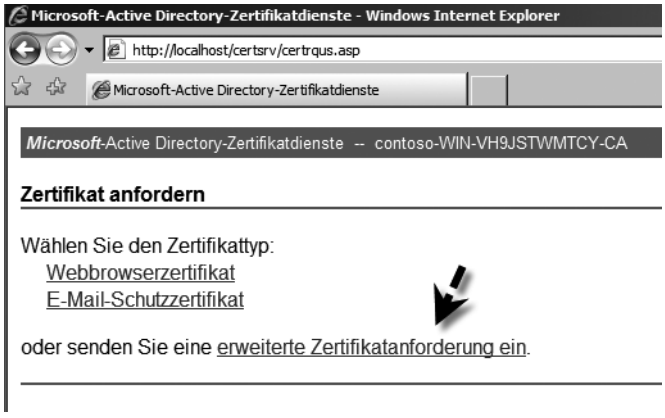
1. Starten Sie den Internet Explorer.
2. Stellen Sie über *Extras/Phishingfilter/Phishingfiltereinstellungen* sicher, dass der Phishingfilter deaktiviert ist.
3. Klicken Sie auf *Extras/Internetoptionen*.
4. Wechseln Sie zur Registerkarte *Sicherheit*.
5. Klicken Sie auf *Lokales Intranet* und stellen Sie sicher, dass die Sicherheitsstufe auf *Sehr niedrig* eingestellt ist. In einer produktiven Umgebung sollten über die Schaltfläche *Stufe anpassen* nur die ActiveX-Controls aktiviert werden. Den geschützten Modus des Internet Explorers unter Windows Vista können Sie aktiviert lassen, außer Sie stellen bei Ihrer Verbindung Probleme fest.

Serverzertifikat auf dem VPN-Server installieren

Der nächste Schritt, den VPN-Server vorzubereiten, besteht darin, ein Serverzertifikat von der Zertifizierungsstelle anzufordern und zu installieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie im Internet Explorer die Adresse *http://localhost/certsrv*.
2. Klicken Sie auf *Ein Zertifikat anfordern*.
3. Klicken Sie auf den Link *erweiterte Zertifikatanforderung* (Abbildung 15.92).

Abbildg. 15.92 Erstellen einer erweiterten Zertifikatanforderung für einen SSTP-VPN-Server



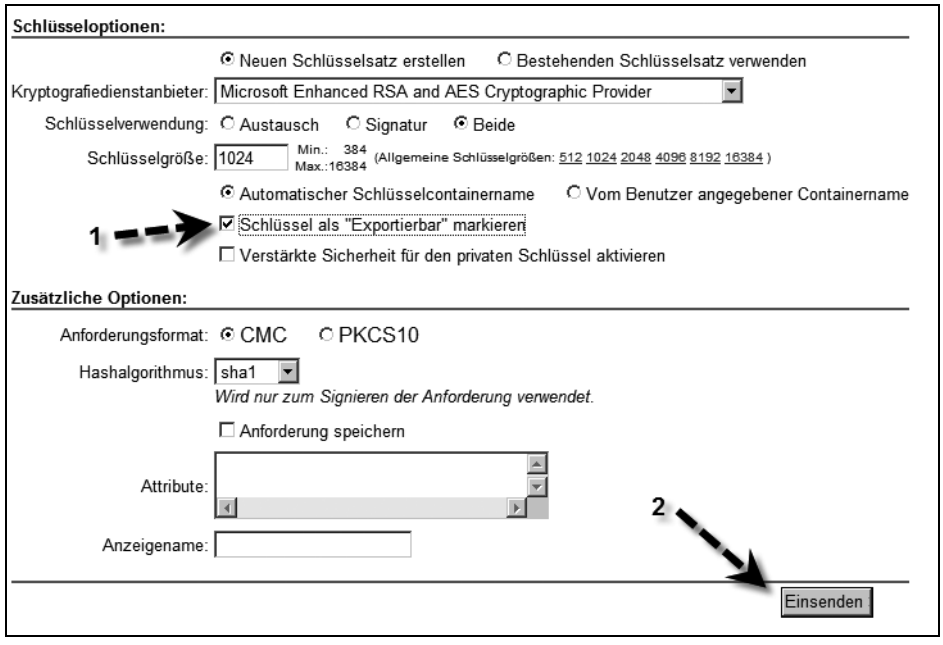
4. Klicken Sie auf *Eine Anforderung an diese Zertifizierungsstelle erstellen und einreichen*.
5. Bestätigen Sie die Zulassung für ActiveX-Controls für diese Seite.
6. Es öffnet sich ein neues Fenster, in dem die Daten des Zertifikats eingegeben werden. Tragen Sie unter *Name* den FQDN des Servers ein, mit dem über das Internet auf ihn zugegriffen wird. Es ist sehr wichtig, dass der Name und die VPN-Adresse übereinstimmen. Mehr zu diesem Thema finden Sie in Kapitel 17. Achten Sie bei der Ländereingabe darauf, zwei Buchstaben zu verwenden, am besten den jeweiligen ISO-Code des Landes.
7. Wählen Sie bei *Typ des erforderlichen Zertifikats* die Option *Serverauthentifizierungszertifikat* aus.

Abbildg. 15.93 Eintragen der Daten und auswählen des Zertifikattyps

8. Aktivieren Sie im Bereich *Schlüsseloptionen* noch das Kontrollkästchen *Schlüssel als "Exportierbar" markieren* und belassen Sie die anderen Einstellungen wie vorgegeben.
9. Klicken Sie auf *Einsenden*, um die Anfrage zu generieren.

10. Klicken Sie im Popup-Fenster auf *Ja*, damit die Anfrage gestartet wird. Die Anfrage wird jetzt eingereicht. Bei eigenständigen Zertifikatsstellen werden Anfragen nicht automatisch beantwortet, da keine direkte Verbindung zum Active Directory besteht. Hier muss ein Administrator das Zertifikat manuell genehmigen.

Abbildg. 15.94 Konfigurieren der Schlüsseloptionen und einsenden der Zertifikatsanfrage

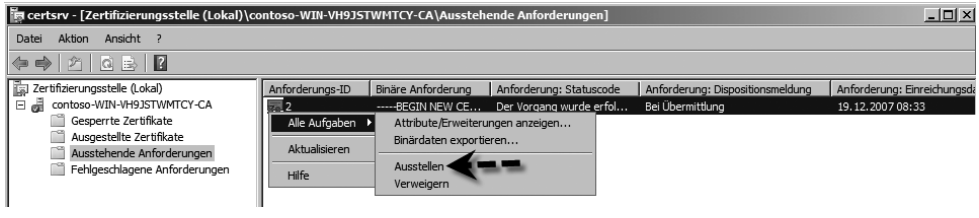


Zertifikat genehmigen

Um das Zertifikat zu genehmigen, gehen Sie folgendermaßen vor:

1. Öffnen Sie über *Start/Verwaltung* das Snap-In *Zertifizierungsstelle*.
2. Klicken Sie auf *Ausstehende Anforderungen*.
3. Klicken Sie mit der rechten Maustaste auf die Anfrage und wählen *Alle Aufgaben/Ausstellen*.

Abbildg. 15.95 Genehmigen einer Zertifikatsanfrage bei einer eigenständigen Zertifizierungsstelle



Zertifikat installieren

Nachdem das Zertifikat beantragt und genehmigt wurde, muss es noch installiert werden. Gehen Sie dazu folgendermaßen vor:

1. Starten Sie den Internet Explorer und öffnen Sie wieder die Seite *http://localhost/certsrv*.
2. Klicken Sie auf *Status ausstehender Zertifikate anzeigen*.
3. Klicken Sie auf das Serverzertifikat, das zur Installation vorgeschlagen wird.
4. Bestätigen Sie die ActiveX-Control-Meldung mit *Ja*.
5. Klicken Sie auf *Dieses Zertifikat installieren* und bestätigen Sie die Meldung zur Installation.

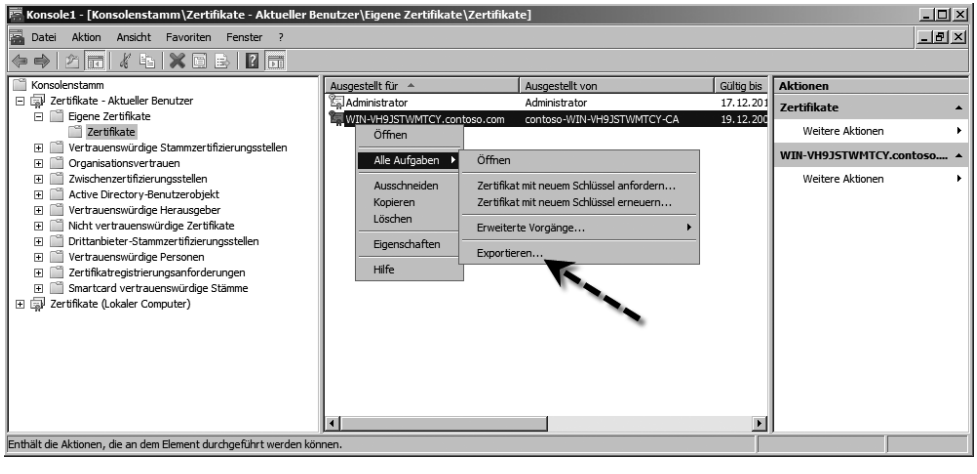
Abbildg. 15.96 Auswählen eines genehmigten Zertifikats zur Installation

Verschieben des Zertifikats in einen anderen Zertifikatspeicher

Nachdem das Zertifikat erfolgreich beantragt, genehmigt und installiert wurde, muss es noch in den richtigen Zertifikatspeicher verschoben werden. Gehen Sie dazu folgendermaßen vor:

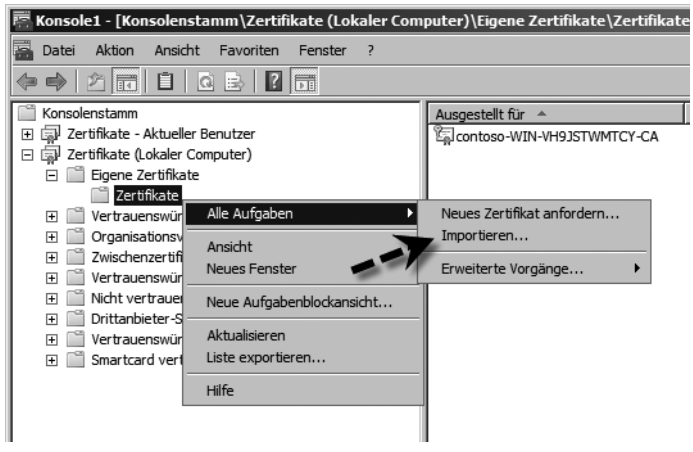
1. Öffnen Sie einen neue MMC-Konsole.
2. Fügen Sie das Snap-In *Zertifikate* hinzu.
3. Wählen Sie als Option *Eigenes Benutzerkonto* aus.
4. Fügen Sie ein weiteres Mal das Snap-In *Zertifikate* hinzu.
5. Legen Sie als Option *Computerkonto* fest und wählen den lokalen Computer aus.
6. Öffnen Sie das Objekt *Zertifikate – Aktueller Benutzer/Eigene Zertifikate/Zertifikate*.

Abbildg. 15.97 Exportieren eines installierten Zertifikats



7. Klicken Sie mit der rechten Maustaste auf das Zertifikat des VPN-Servers, das Sie gerade installiert haben.
8. Wählen Sie im Kontextmenü den Untermenüeintrag *Alle Aufgaben/Exportieren*.
9. Bestätigen Sie die Startseite des Assistenten.
10. Aktivieren Sie auf der nächsten Seite die Option *Ja, privaten Schlüssel exportieren*.
11. Übernehmen Sie auf der nächsten Seite die Standardeinstellungen für das gewünschte Format.
12. Geben Sie ein Kennwort ein. Dieses wird später beim Import wieder benötigt.
13. Legen Sie einen Namen und einen Speicherort für das Zertifikat fest und schließen Sie den Export ab.
14. Im nächsten Schritt wir das Zertifikat wieder importiert und zwar in den Zertifikatspeicher des lokalen Computers. Öffnen Sie dazu in der Konsolenstruktur den Eintrag *Zertifikate (Lokaler Computer)/Eigene Zertifikate/Zertifikate*.
15. Klicken Sie mit der rechten Maustaste auf *Zertifikate* und wählen Sie *Alle Aufgaben/Importieren*.

Abbildg. 15.98 Importieren eines Zertifikats ein den Zertifikatespeicher



16. Wählen Sie die Zertifikatedatei aus, die soeben exportiert wurde. Als Dateityp muss vorher die Option *Alle Dateien* ausgewählt werden, ansonsten wird die Datei nicht angezeigt.
17. Bestätigen Sie alle restlichen Fenster mit den Standardeinstellungen und schließen Sie den Import ab. Das Zertifikat muss jetzt im Zertifikatespeicher des lokalen Computers angezeigt werden.

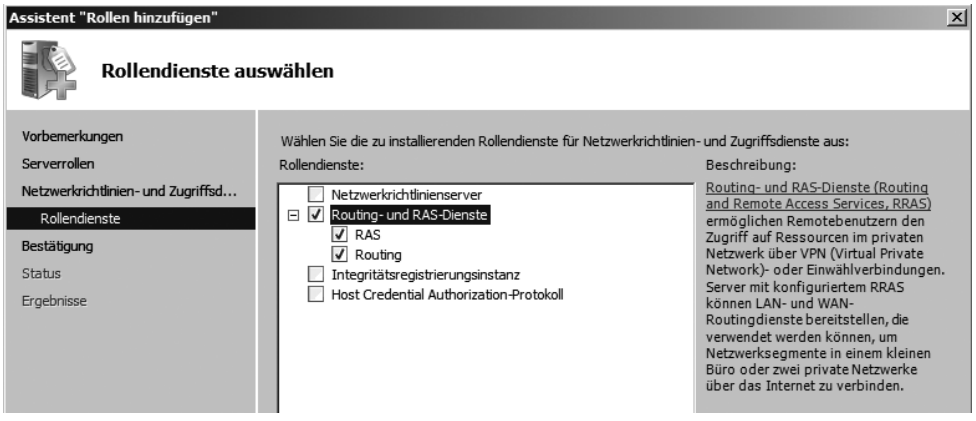
Routing und RAS-Dienste für SSTP-VPN installieren und konfigurieren

Der nächste Schritt der Einrichtung besteht darin, den Routing und RAS-Dienst zu installieren und einzurichten. Diese Installation ist mit der Installation weiter vorne recht identisch. Aus diesem Grund beschreiben wir die einzelnen Schritte weniger ausführlich, als in den vorangegangenen Abschnitten. Gehen Sie zur Installation folgendermaßen vor:

1. Starten Sie den Server-Manager, klicken Sie auf *Rollen* und dann auf *Rollen hinzufügen*.
2. Wählen Sie *Netzwerkrichtlinien- und Zugriffsdienste* aus.

3. Wählen Sie als Rollendienste für ein SSTP-VPN *Routing- und RAS-Dienste* mit den untergeordneten Diensten *RAS* und *Routing* aus. Schließen Sie die Installation der Rollendienste ab.

Abbildg. 15.99 Installieren von Routing- und RAS-Diensten für die Unterstützung von SSTP-VPN



Konfiguration der Routing- und RAS-Dienste

Nachdem Sie den Rollendienst installiert haben, muss dieser noch für SSTP-VPN konfiguriert werden. Starten Sie dazu über *Start/Verwaltung* die Verwaltungskonsole *Routing und RAS*. Um die Dienste auf dem VPN-Server zu aktivieren, klicken Sie diese mit der rechten Maustaste an und wählen die Option *Routing und RAS konfigurieren und aktivieren*, damit der Einrichtungsassistent gestartet wird. Zur weiteren Einrichtung gehen Sie folgendermaßen vor:

1. Wählen Sie auf der Konfigurations-Seite die Option *RAS (DFÜ oder VPN)* aus.
2. Aktivieren Sie auf der RAS-Seite nur die Option *VPN*.
3. Auf der nächsten Seite wird die Schnittstelle ausgewählt, auf die der VPN-Dienst hört. Damit die Konfiguration transparenter ist, macht es Sinn, die Netzwerkverbindungen auf dem Server an sich entsprechend *Intern* und *Extern* zu benennen. Die Verbindungen werden dann auf dem Server genauso angezeigt. Wählen Sie im Fenster *VPN-Verbindung* die Verbindung *extern* aus.
4. Deaktivieren Sie die Option *Sicherheit auf der ausgewählten Schnittstelle durch einrichten statischer Paketfilter.* Geübte Administratoren können in Produktivumgebungen diese Option auch aktiviert lassen, müssen dann aber die Paketfilter für das VPN entsprechend konfigurieren.
5. Auf der nächsten Seite wird festgelegt, ob Clients die IP-Adresse von einem DHCP-Server erhalten sollen, oder ob der RAS-Dienst die IP-Adressen selbst zuweisen soll. Die direkte Zuweisung durch den VPN-Server ist oft der einfachere Weg. Wählen Sie in diesem Fall die Option *Aus einem angegebenen Bereich* aus.
6. Auf der nächsten Seite legen Sie die IP-Adressen fest, die den Clients bei der VPN-Einwahl zugewiesen werden.
7. Auf der nächsten Seite wählen Sie die Option *Nein, Routing und RAS zum Authentifizieren von Verbindungsanforderungen verwenden* aus. Schließen Sie den Assistenten ab und bestätigen Sie die Meldung des DHCP-Relay-Agenten.

Der RAS-Dienst ist jetzt aktiviert. Die Einstellungen können jederzeit über die Eigenschaften des RAS-Servers geändert werden.

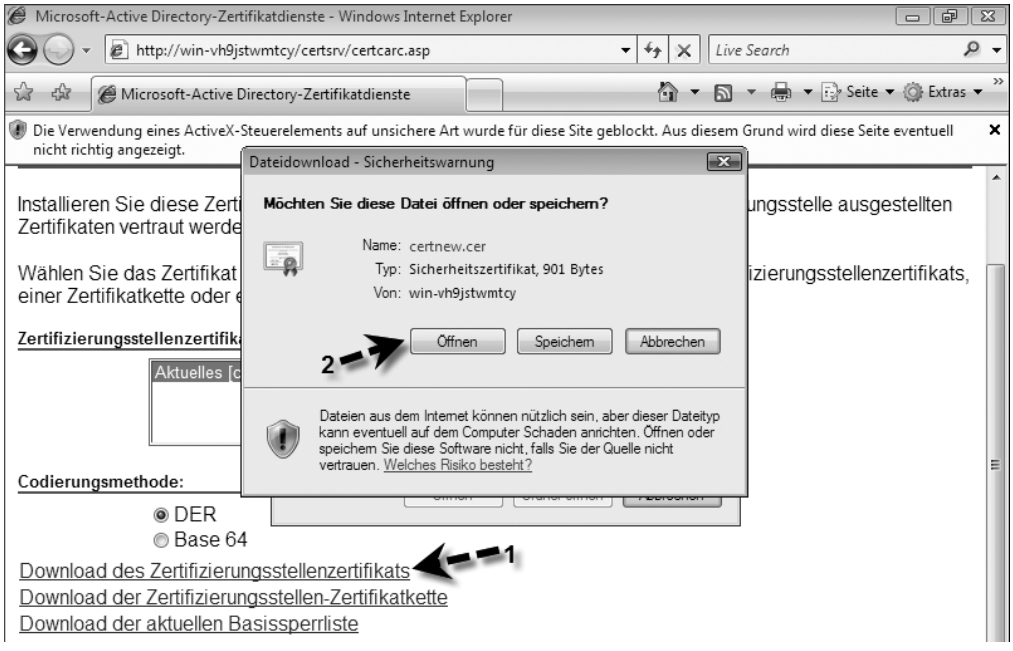
VPN-Client konfigurieren

Damit Sie ein VPN über HTTPS mit SSTP verwenden können, muss auf den Clients Windows Vista SP1 installiert sein. Ohne das SP1 kann Windows Vista kein SSTP-VPN aufbauen. Damit der VPN-Client sich verbinden kann, muss das Zertifikat der Stammzertifizierungsstelle auf dem Client installiert werden. Diese Vorgänge sind ausführlich in Kapitel 17 erläutert. Im folgenden Abschnitt gehen wir darauf ein, wie das Zertifikat der Zertifizierungsstelle über die Weboberfläche der Zertifizierungsstelle in Ihrem Unternehmen angefordert wird. Damit Clients über das Internet per HTTPS ein VPN aufbauen können, muss daher entweder vorher das Zertifikat im Unternehmen auf dem Rechner installiert werden oder Sie veröffentlichen die Zertifizierungsstelle über einen ISA-Server im Internet. Um das Zertifikat der Zertifizierungsstelle auf dem Computer zu installieren, rufen Sie zunächst im Internet Explorer des Clients die Webseite der Zertifizierungsstelle auf. Klicken Sie auf den Link *Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste* (Abbildung 15.100). Erscheint eine Sicherheitsmeldung im Internet Explorer, bestätigen Sie diese mit *Ja*.

Abbildg. 15.100 Herunterladen des Zertifizierungsstellen-Zertifikats

Klicken Sie in der nächsten Seite auf den Link *Download des Zertifizierungsstellenzertifikats* (Abbildung 15.101). Wählen Sie im Download-Fenster *Öffnen* aus. Klicken Sie im neuen Fenster auf *Zertifikat installieren*. Schließen Sie den Assistenten zur Installation des Assistenten mit den Standardeinstellungen ab.

Abbildg. 15.101 Herunterladen und öffnen eines Zertifizierungsstellen-Zertifikats



Anschließend muss das Zertifikat noch in den richtigen Zertifikatspeicher verschoben werden. Aktuell ist das Zertifikat im Speicher des Benutzers, muss aber in den Speicher des lokalen Computerkontos und zwar in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen (siehe auch Kapitel 17). Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie einen neue MMC-Konsole.
2. Fügen Sie das Snap-In *Zertifikate* hinzu.
3. Wählen Sie als Option *Eigenes Benutzerkonto* aus.
4. Fügen Sie noch mal das Snap-In *Zertifikate* hinzu.
5. Wählen Sie als Option *Computerkonto* aus und wählen den lokalen Computer aus.
6. Öffnen Sie den Konsoleneintrag *Zertifikate – Aktueller Benutzer/Zwischenzertifizierungsstellen/Zertifikate*.
7. Klicken Sie mit der rechten Maustaste auf das Zertifikat des VPN-Servers, das Sie gerade installiert haben, und wählen Sie im Kontextmenü den Eintrag *Kopieren* aus. Da das Zertifikat keinen privaten Schlüssel benötigt, muss es nicht exportiert werden wie auf dem VPN-Server.
8. Öffnen Sie den Konsoleneintrag *Zertifikate (Lokaler Computer)/Vertrauenswürdige Stammzertifizierungsstellen/Zertifikate* und fügen das Zertifikat per Klick mit der rechten Maustaste über den Kontextmenübefehl *Einfügen* ein.

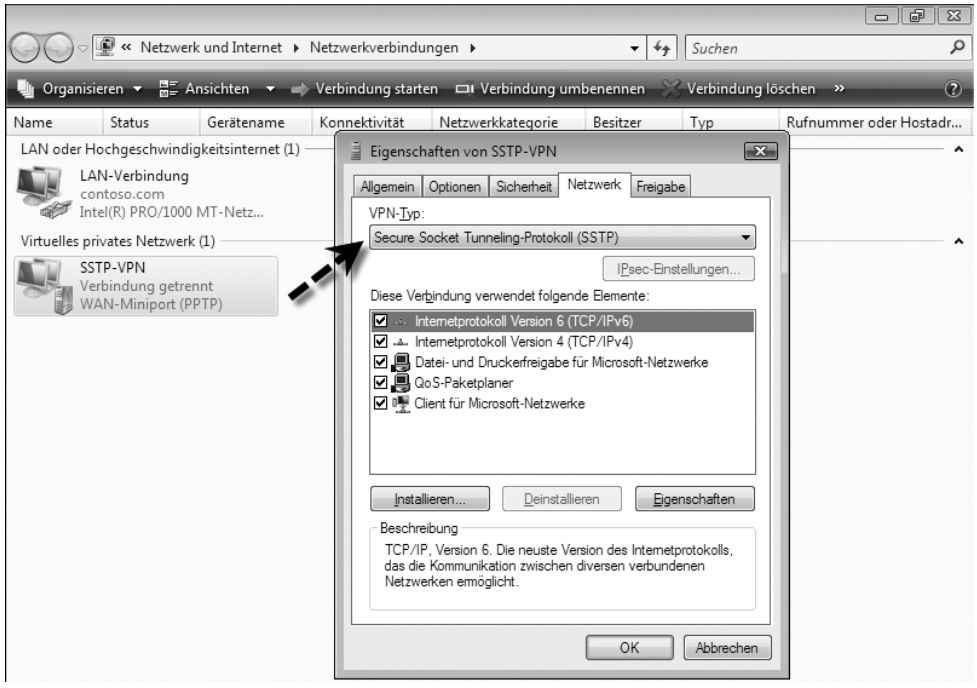
Konfigurieren einer SSTP-VPN-Verbindung

Der nächste Schritt besteht darin, eine VPN-Verbindung zu konfigurieren, die SSTP verwendet, nicht PPTP oder L2TP. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das *Netzwerk- und Freigabecenter* auf dem Computer.

2. Klicken Sie auf *Eine Verbindung oder ein Netzwerk einrichten*.
3. Wählen Sie *Verbindung mit dem Arbeitsplatz herstellen*.
4. Geben Sie die Daten der Verbindung ein, wie bei einer normalen VPN-Verbindung.
5. Rufen Sie in den Netzwerkverbindungen die Eigenschaften der neuen VPN-Verbindung auf.
6. Wechseln Sie zur Registerkarte *Netzwerk*.
7. Wählen Sie bei *VPN-Typ* die Option *Secure Socket Tunneling-Protokoll (SSTP)* aus. Genau dieser Punkt fehlt auf Computern ohne SP1 für Windows Vista.

Abbildg. 15.102 Aktivieren von SSTP für eine VPN-Verbindung



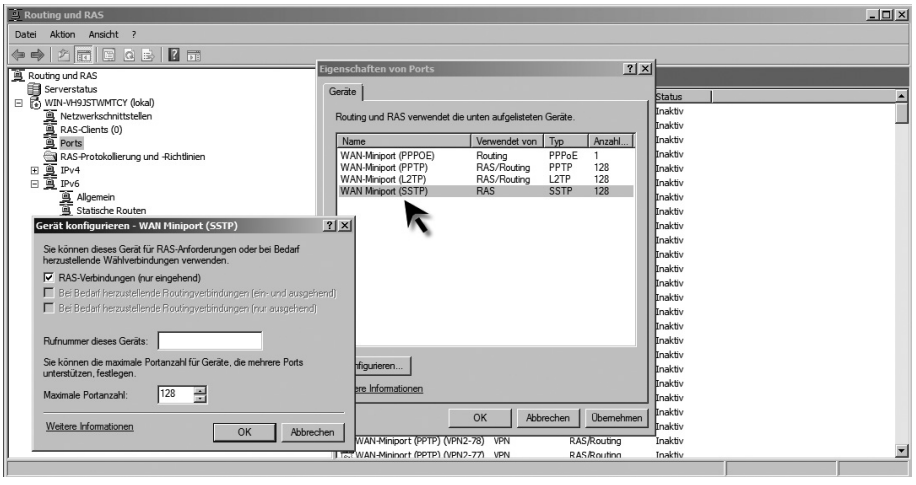
Fehlerbehebung bei SSTP-VPN

Wie bei allen Verbindungen werden auch Informationen zum SSTP-VPN in den Ereignisanzeigen des Servers gespeichert. Fehlermeldungen werden im Protokoll System gespeichert. Die Meldungen von SSTP haben die Quelle *RasSstp*. Sollten Verbindungsprobleme auftreten, liegt es fast immer an Problemen mit den Zertifikaten und dem Namen des Zertifikats.

Unter Eigenschaften in den Ports der RAS-Verwaltungskonsole können weitere Einstellungen bezüglich SSTP-VPN vorgenommen werden.

TIPP Im Routing und RAS-Blog der TechNet finden Sie oft Hinweise zur Einrichtung und zur Fehlerbehebung, auch für SSTP. Den Blog können Sie über die Adresse *http://go.microsoft.com/fwlink/?LinkId=82954* aufrufen.

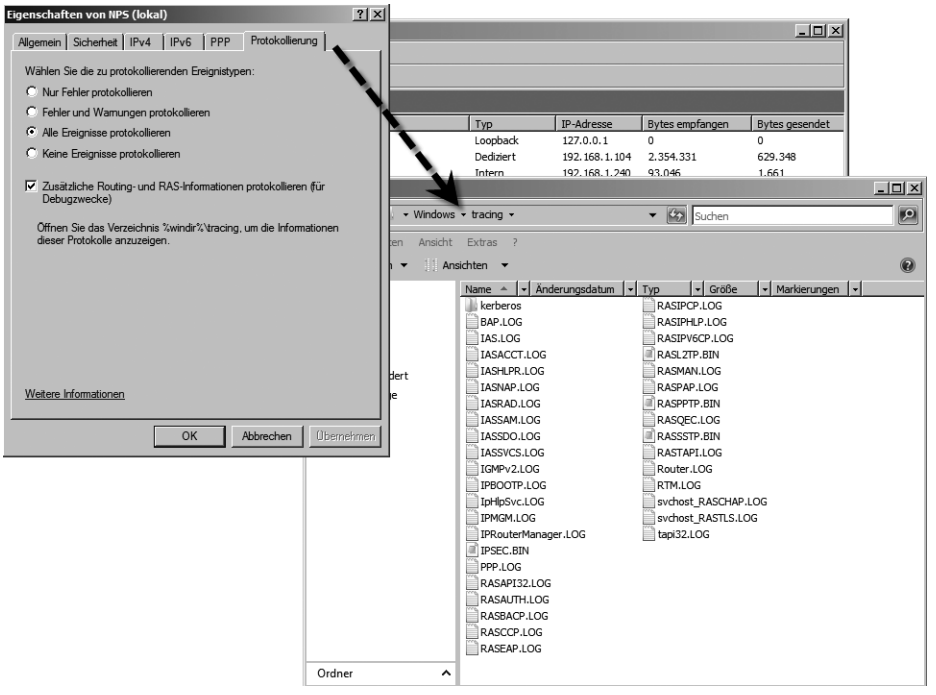
Abbildg. 15.103 Konfigurieren der SSTP-Ports für SSTP-VPN



Konfigurieren der RAS-Protokollierung

In der RAS-Verwaltungskonsole können Sie in den Eigenschaften für den Server auf der Registerkarte *Protokollierung* einstellen, welche Aktionen und Vorkommnisse protokolliert werden sollen. Das entsprechende Protokolle wird im Verzeichnis *\Windows\tracing* gespeichert (Abbildung 15.104).

Abbildg. 15.104 Anzeigen der RAS-Protokolle für die Fehlersuche



IPSec mit Netzwerkzugriffsschutz (NAP) einsetzen

Mit IPSec können Sie den Netzwerkverkehr zwischen verschiedenen Clients verschlüsseln lassen. Eines der größten Probleme in Netzwerken ist die sichere Kommunikation. Während der Zugang zu Serversystemen und zu Workstations über Kennwörter geschützt ist, laufen Informationen unverschlüsselt über das Netzwerk. IPsec ist ein von der IETF (Internet Engineering Task Force) definierter offener Standard, mit dem die Daten auf der Ebene des IP-Protokolls verschlüsselt werden. Das ist für alle darüber liegenden Kommunikationsprotokolle wie SMTP, HTTP und so weiter transparent. Die eigentliche Verschlüsselung bei IPsec erfolgt mit einem symmetrischen Verfahren, bei dem ein privater Schlüssel ausgetauscht werden muss. Solche Verfahren sind schneller als Public Key-Verfahren. Um den privaten Schlüssel zwischen Sender und Empfänger auszutauschen, verwendet Windows Server 2008 den ISAKMP/Oakley-Dienst, der als IKMP (Internet Key Management Protocol) bekannt ist. ISAKMP, das Internet Security Association and Key Management Protocol, wurde federführend von Cisco definiert und legt fest, wie zwei Knoten in einem Netzwerk Schlüssel austauschen und eine sichere Kommunikationsverbindung aufbauen. Oakley ist das Protokoll, um Verschlüsselungsverfahren und Schlüssel festzulegen. Für den Austausch der privaten Schlüssel können Public Key-Verfahren und Kerberos verwendet werden. Ob eine sichere Kommunikation erfolgen soll, wird bei Windows Server 2008 über Gruppenrichtlinien und die Konfiguration der neuen Windows-Firewall festgelegt. Es wird nicht pro Anwendung, sondern pro System und Verbindung mit bestimmten Rechnern im Netzwerk definiert, ob eine sichere Kommunikation erfolgen soll. Da IPsec ein offener Standard ist und IP als Transportprotokoll transparent in LAN und WAN eingesetzt werden kann, wird diese Form der sicheren Kommunikation im Intranet und im Internet verwendet. Damit Sie IPSec im Unternehmen einsetzen können, müssen Sie auf einem Server die Rolle *Active Directory-Zertifikatdienste* installieren. Die Installation erfolgt analog wie bereits bei der Verwendung von NAP mit DHCP beschrieben.

IPSec-Verbesserungen in Windows Server 2008

Unter Windows Server 2003 war die Konfiguration von IPSec noch eine relativ komplexe Angelegenheit. Durch die Integration der IPSec-Verwaltung in die Firewall-Konsole wird diese Konfiguration enorm vereinfacht. Die Verwaltungsoberfläche der neuen Firewall können Sie über *Start/Ausführen/wf.msc* starten. Die Firewall für erweiterte Sicherheit ersetzt die verschiedenen Verwaltungskonsolen für IPSec-Richtlinien.

Verwenden Sie mit Windows Server 2008 IPSec-Richtlinien, verhalten sich die Server wie folgt: Ein Server, für den IPSec aktiviert wurde, sendet Pakete über IPSec. Antwortet der empfangende Server ebenfalls mit IPSec, wird der Datenverkehr verschlüsselt. Unterstützt der empfangende Server kein IPSec, wird der Datenverkehr nicht verschlüsselt. Dieser Datenverkehr findet gleichzeitig statt. Unter Windows Server 2003 wurden erst IPSec-Pakete verschickt, dann drei Sekunden gewartet und dann erst die unverschlüsselten Pakete gesendet. So konnten oft starke Performance-Probleme auftreten, die durch das gleichseitige Versenden der Pakete in 2008 vermieden werden. Durch diese Funktion können Server IPSec-Verkehr unterstützen, aber nicht mehr zwingend voraussetzen, um eine möglichst sichere Verbindung zu erstellen.

Bisher hat IPSec unter Windows nur Internet Key Exchange (IKE) unterstützt. Windows Vista und Windows Server 2008 unterstützen eine neue Funktion, die Authenticated IP (AuthIP) genannt wird. Diese neue Funktion unterstützt weitere Authentifizierungsfunktionen als IKE, zum Beispiel

die Gültigkeit von Zertifikaten, die Bestandteil der neuen Network Access Protection (NAP) in Windows Server 2008 sind. Auch Kerberos- oder NTLMv2-Authentifizierung wird unterstützt. Zusätzlich wird die Authentifizierung mit mehreren Konten unterstützt. IPSec kann so konfiguriert werden, dass sowohl die Computerauthentifizierung als auch die Benutzerauthentifizierung unterstützt wird. Durch diese Möglichkeiten wird die Sicherheit im Netzwerk deutlich erhöht. Unter Windows Server 2008 und Windows Vista kann der Verkehr zwischen Domänenmitgliedern und Domänencontrollern IPSec-verschlüsselt stattfinden, während der Verkehr zwischen Domänenmitgliedern und Nicht-Domänenmitgliedern weiterhin unverschlüsselt erfolgen kann. Diese Funktion war unter Windows Server 2003 und Windows XP nicht möglich. Windows Vista und Windows Server 2008 unterstützen neue Algorithmen zur Verschlüsselung:

- Elliptic Curve Diffie-Hellman P-256 (256 Bit)
- Elliptic Curve Diffie-Hellman P-384 (384 Bit)
- AES mit cipher block chaining (CBC) und 128-bit key size (AES 128)
- AES mit CBC und 192-bit key size (AES 192)
- AES mit CBC und 256-bit key size (AES 256)

Weitere Informationen zu der neuen Windows-Firewall finden Sie auf folgenden Webseiten:

- Informationen zur neuen Windows-Firewall: *http://go.microsoft.com/fwlink/?LinkID=84639*
- Informationen zu IPSec: *http://go.microsoft.com/fwlink/?LinkID=84638* und *http://go.microsoft.com/fwlink/?LinkID=79430*
- Network Access Protection: *http://go.microsoft.com/fwlink/?LinkID=84637*

Windows Server 2008 und Windows Vista beinhalten außerdem folgende Verbesserungen der Internetprotokollsicherheit:

- IPSec-Schutz von Client zu Domänencontroller
- Verbesserter Lastausgleich und Unterstützung für Cluster
- Verbesserte IPSec-Authentifizierung
- Integration mit NAP (Network Access Protection)
- Integrierte IPv4- und IPv6-Unterstützung
- Erweiterte Ereignis- und Leistungsüberwachungsindikatoren
- Unterstützung für das Netzwerkdiagnose-Framework

Einrichtung einer IPSec-Umgebung

In den folgenden Abschnitten zeigen wir Ihnen, wie Sie eine NAP-gestützte IPSec-Infrastruktur aufbauen können. Oft gibt es Probleme, wenn Sie mehrere NAP-Konfigurationen, also zum Beispiel IPSec und DHCP, parallel auf einem Server konfigurieren, da Sie hier stark auf die Reihenfolge der Richtlinien achten müssen. Diese werden priorisierend angeordnet, ähnlich zu den Firewallrichtlinien im ISA Server.

Erstellen einer Ausnahmegruppe

Richten Sie eine IPSec-Infrastruktur ein, ist es sinnvoll, wenn Sie einigen PCs im Netzwerk die IPSec-Kommunikation gestatten, auch wenn diese nicht NAP-konform sind oder für die Sie keine NAP-Überprüfung vornehmen wollen, bevor die IPSec-Verbindung hergestellt wird. Mitglieder dieser Gruppe können auch dann mit anderen PCs kommunizieren, wenn diese eine Sicherheitsprü-

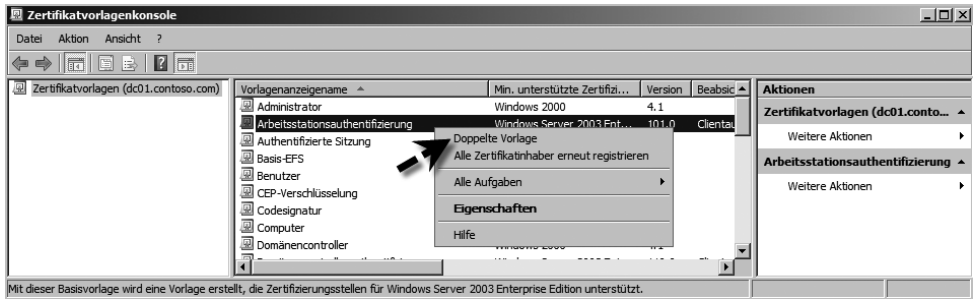
fung vorschreiben. Legen Sie dazu am besten eine eigene globale Sicherheitsgruppe in der Domäne an und wählen als Bezeichnung zum Beispiel *NAP-Ausnahmen*. In diese Gruppe nehmen Sie die Computerkonten auf, denen Sie die NAP-Überprüfung ersparen wollen.

Erstellen einer Zertifikatsvorlage

Wollen Sie die NAP-Überprüfung für manche Clients auf Basis der erwähnten Gruppe deaktivieren, sollten Sie für diese Clients auch eine eigene Zertifikatsvorlage erstellen. Zertifikatsvorlagen erstellen Sie am besten über die entsprechende Verwaltungskonsole auf dem Zertifikatsserver:

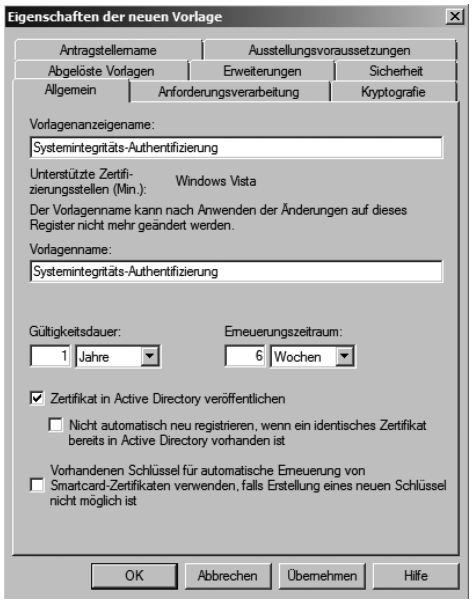
1. Diese Verwaltungskonsole rufen Sie über *Start/Ausführen/certtmpl.msc* auf.
2. Klicken Sie mit der rechten Maustaste auf die Vorlage *Arbeitsstationsauthentifizierung* und wählen Sie im Kontextmenü den Eintrag *Doppelte Vorlage* aus (Abbildung 15.105).

Abbildg. 15.105 Duplizieren einer vorhandenen Zertifikatvorlage



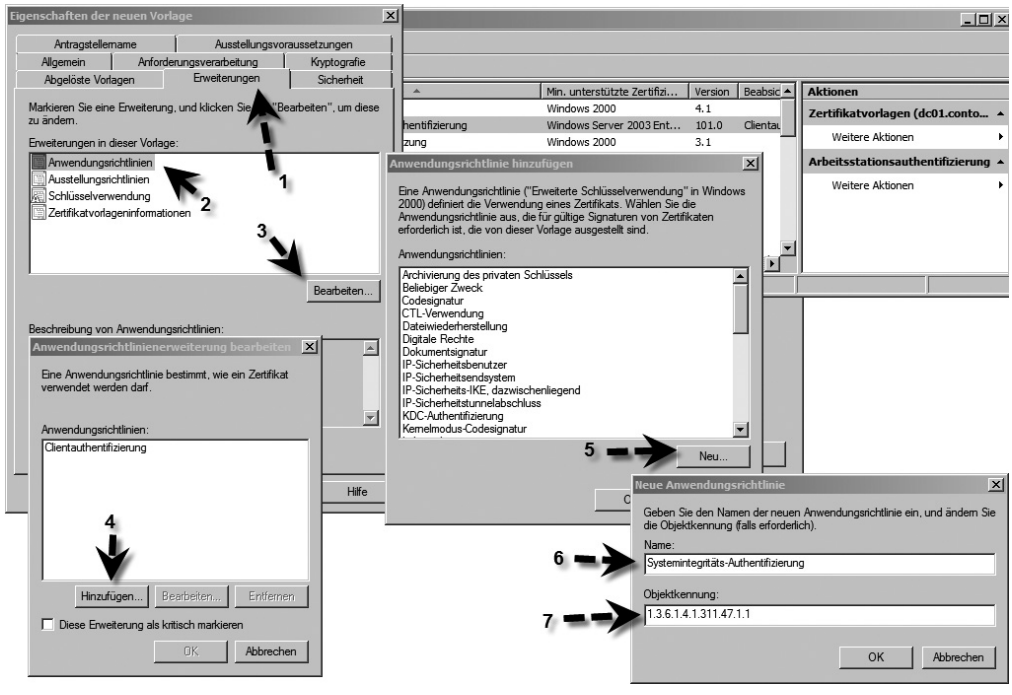
3. Wählen Sie aus, für welche Zertifizierungsstelle das Zertifikat kompatibel sein soll. Setzen Sie eine reine Windows Server 2008-CA ein, können Sie an dieser Stelle auch die Minimalvoraussetzung auf Windows Server 2008 setzen. Anschließend öffnet sich das Konfigurationsfenster für die neue Zertifikatsvorlage (Abbildung 15.106).
4. Geben Sie eine passende Bezeichnung für die neue Vorlage ein, zum Beispiel *Systemintegritäts-Authentifizierung*.
5. Aktivieren Sie das Kontrollkästchen *Zertifikat in Active Directory veröffentlichen*. Wenn ein Antragsteller ein Zertifikat erhält, das auf dieser Vorlage basiert, wird das ausgestellte Zertifikat zu dem Active Directory-Objekt dieses Antragstellers hinzugefügt.
6. Das Kontrollkästchen *Nicht automatisch erneut registrieren, wenn ein identisches Zertifikat bereits in Active Directory vorhanden ist* wird nicht aktiviert. Wenn der Antragsteller versucht, sich für ein auf dieser Vorlage basierendes Zertifikat zu registrieren, führen Computer unter Windows XP, Vista oder Windows Server 2003 und 2008 eine Überprüfung durch, um festzustellen, ob bereits ein identisches Zertifikat in Active Directory vorhanden ist. Ist dies der Fall, wird durch die automatische Registrierung keine erneute Registrierungsanforderung übermittelt. Hierdurch wird die Erneuerung von Zertifikaten ermöglicht und gleichzeitig verhindert, dass mehrere identische Zertifikate ausgestellt werden.
7. Holen Sie anschließend die Registerkarte *Erweiterungen* in den Vordergrund (Abbildung 15.107).
8. Klicken Sie auf *Anwendungsrichtlinien* und dann auf *Bearbeiten*.
9. Klicken Sie auf *Hinzufügen*.

Abbildg. 15.106 Konfigurieren einer neuen Zertifikatsvorlage



10. Klicken Sie auf *Neu*.

Abbildg. 15.107 Erstellen einer neuen Anwendungsrichtlinie für ein neues Zertifikat



11. Geben Sie im neuen Dialogfeld die Bezeichnung *Systemintegritäts-Authentifizierung* ein.
12. Weisen Sie der Richtlinie die Objektkennung *1.3.6.1.4.1.311.47.1.1* zu.
13. Bestätigen Sie die geöffneten Dialogfelder mit *OK*, bis nur noch das Dialogfeld *Eigenschaften der neuen Vorlage* geöffnet ist.
14. Wechseln Sie zur Registerkarte *Sicherheit*.
15. Nehmen Sie in diese Registerkarte die erstellte globale Gruppe *NAP-Ausnahmen* auf und aktivieren Sie bei der Option *Automatisch registrieren* das Kontrollkästchen *Zulassen*.
16. Klicken Sie auf *OK*, um die Eingaben abzuschließen.

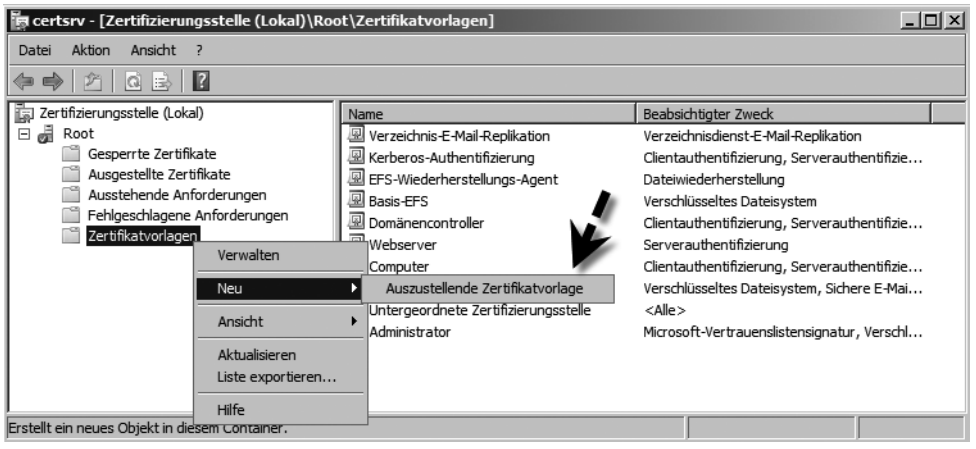
Abbildg. 15.108 Konfigurieren der NAP-Ausnahmen für einzelne Computer

Veröffentlichen der Zertifikatvorlage

Nachdem Sie die neue Vorlage für das Zertifikat erstellt haben, müssen Sie in den Zertifikatdiensten noch konfigurieren, dass diese Zertifikatsvorlage für neue Zertifikate verwendet werden darf. Gehen Sie dazu folgendermaßen vor:

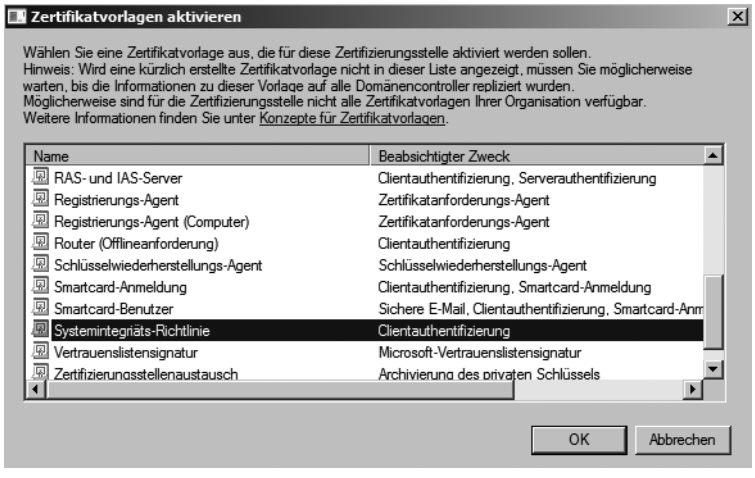
1. Starten Sie die Verwaltung der Zertifizierungsstelle entweder über die Programmgruppe *Verwaltung* oder über *Start/Ausführen/certsrv.msc* (Abbildung 15.109).
2. Erweitern Sie den Knoten Ihrer Zertifizierungsstelle und klicken Sie mit der rechten Maustaste auf *Zertifikatvorlagen*.
3. Wählen Sie *Neu* und dann *Auszustellende Zertifikatvorlage* aus.

Abbildg. 15.109 Veröffentlichen einer neu erstellten Zertifikatvorlage



4. Wählen Sie die erstellte Zertifikatvorlage *Systemintegritäts-Authentifizierung* aus und klicken Sie auf *OK*.
5. Im Anschluss sollte die Vorlage in der Zertifizierungsstelle angezeigt werden.

Abbildg. 15.110 Auswählen einer neuen Zertifikatvorlage für die Veröffentlichung

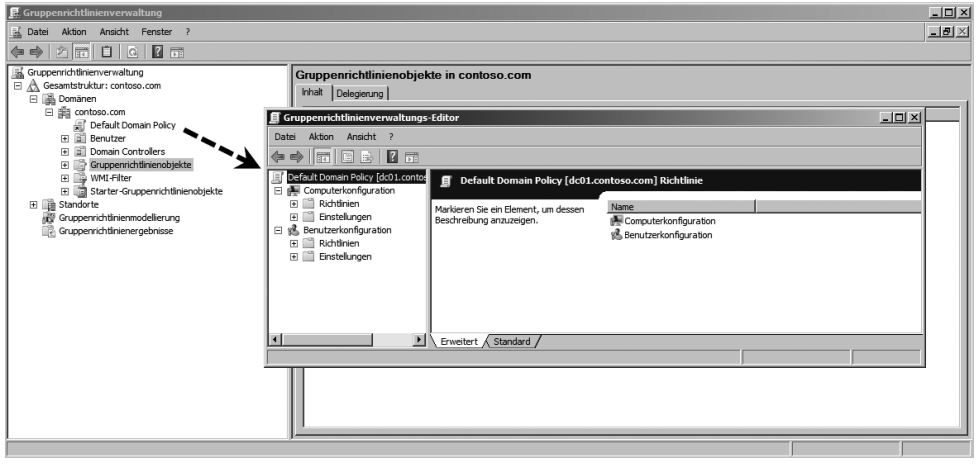


Konfiguration der automatischen Registrierung von Zertifikaten in Active Directory

Der nächste Schritt besteht darin, die Zertifizierungsstelle so zu konfigurieren, dass automatisch Zertifikate ausgestellt werden, wenn ein Domänencomputer eines anfordert. Auf Basis dieser Zertifikate wird später die IPSec-Kommunikation aufgebaut. Für die automatische Registrierung von Zertifikaten verwenden Sie am besten die Gruppenrichtlinien:

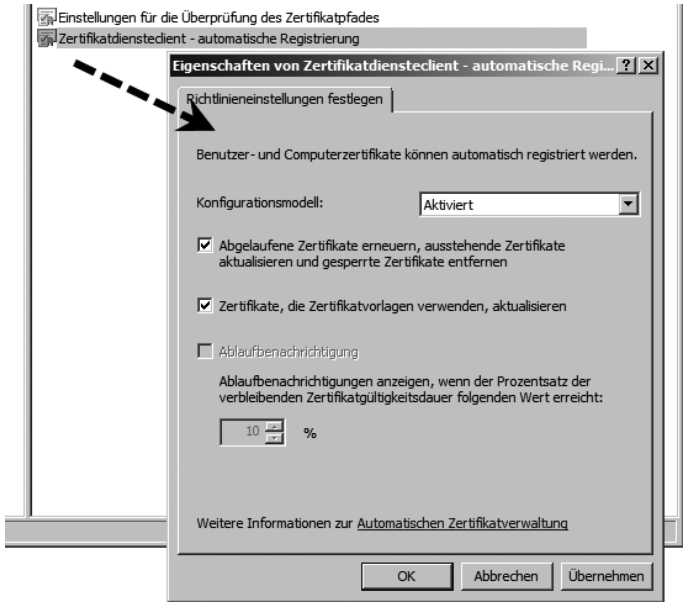
1. Starten Sie dazu die *Gruppenrichtlinienverwaltung*.
2. Öffnen Sie die Bearbeitung der *Default Domain Policy*.

Abbildg. 15.111 Bearbeiten der Default Domain Policy



3. Navigieren Sie zu *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Richtlinien für öffentliche Schlüssel*.
4. Klicken Sie auf der rechten Seite doppelt auf die Richtlinie *Zertifikatdiensteclient-automatische Registrierung*.
5. Setzen Sie die Richtlinie auf *Aktiviert*.
6. Aktivieren Sie zusätzlich noch die beiden Optionen *Abgelaufene Zertifikate erneuern…* und *Zertifikate, die Zertifikatvorlagen verwenden, aktualisieren*.
7. Bestätigen Sie alle Fenster und schließen Sie den Editor für die Gruppenrichtlinien wieder.

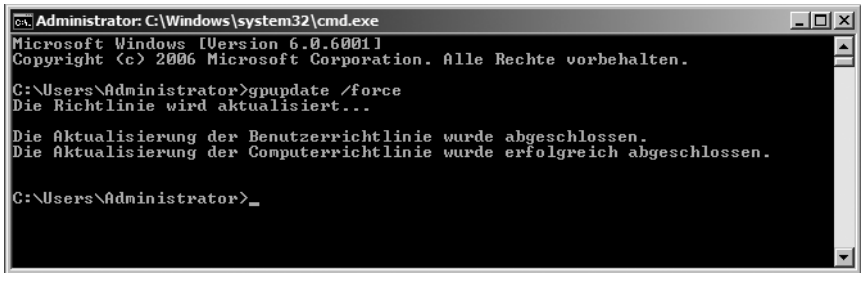
Abbildg. 15.112 Konfigurieren der automatischen Zertifikatregistrierung über Gruppenrichtlinien



Installation einer untergeordneten Zertifizierungsstelle und einer Integritätsregistrierungsinstanz

Als nächster Schritt wird der Netzwerkrichtlinienserver (Network Policy Server, NPS) konfiguriert. Sie sollten auf dem NPS Windows Server 2008 installieren, die Rolle eines Netzwerkrichtlinienservers. Nehmen Sie das Computerkonto des NPS in die Gruppe *NAP-Ausnahmen* auf, damit dieser Server immer uneingeschränkt mit allen PCs und Servern kommunizieren kann. Haben Sie den Server in die Gruppe aufgenommen, sollten Sie diesen entweder neu starten oder zumindest die Aktualisierung der Gruppenrichtlinien auf dem Server auslösen. Geben Sie dazu in der Befehlszeile oder über *Start/Ausführen* den Befehl *gpupdate /force* ein (Abbildung 15.113). Die Aktualisierung der Gruppenrichtlinie sollte für die Benutzerkonfiguration und die Computerkonfiguration erfolgreich abgeschlossen werden.

Abbildg. 15.113 Erfolgreiche Aktualisierung der Gruppenrichtlinie über *gpupdate /force*

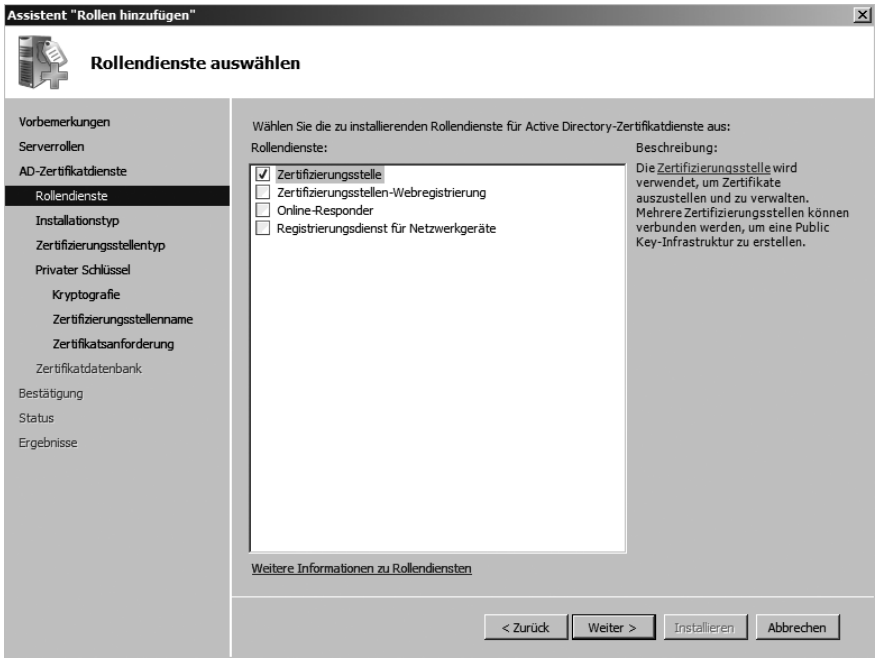


Installieren einer untergeordneten Zertifizierungsstelle auf dem Netzwerkrichtlinienserver

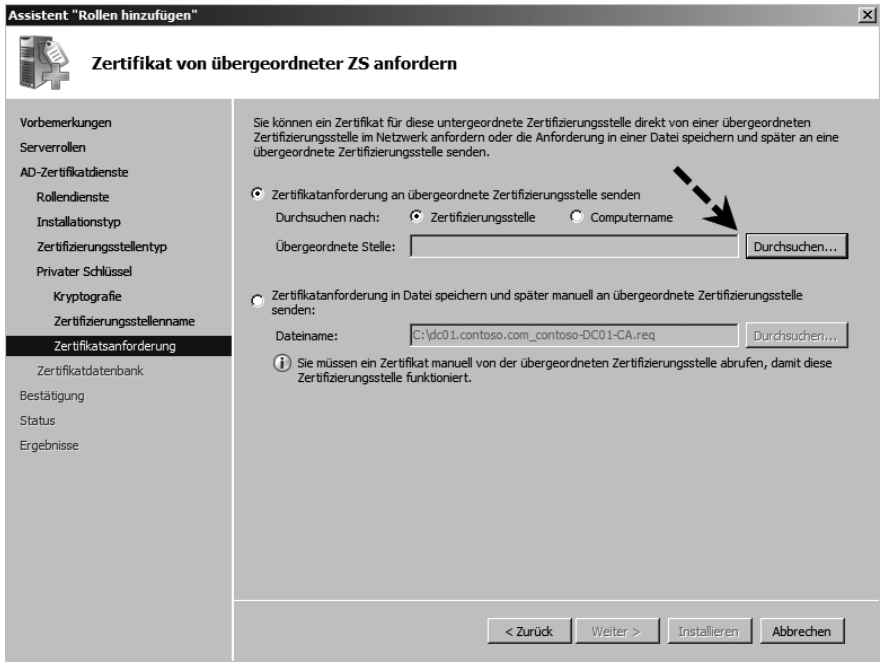
Zusätzlich wird auf dem NPS eine untergeordnete Zertifikatstelle installiert, die an die IPSec-Umgebung angepasst werden kann. Fügen Sie auf dem Server dazu neben der Rolle Netzwerkrichtlinien und -Zugriffsdienste auch die Rolle Active Directory-Zertifikatdienste hinzu. Haben Sie auf dem Server schon die Netzwerkrichtlinien installiert, müssen Sie nachträglich über den Menüpunkt *Rollen* im Server-Manager den Rollendienst *Integritätsregistrierungsinstanz* installieren. Installieren Sie vor diesem Rollendienst jedoch zunächst die Active Directory Zertifikatdienste auf dem Server:

1. Als Rollendienst für die Zertifizierungsdienste auf dem Server wählen Sie im entsprechenden Fenster nur *Zertifizierungsstelle* aus (Abbildung 15.114).
2. Im nächsten Fenster wählen Sie als Setuptyp *Eigenständig* aus.
3. Im nächsten Fenster wählen Sie *Untergeordnete Zertifizierungsstelle* aus.
4. Bestätigen Sie alle Fenster, bis Sie zum Fenster *Zertifikat von übergeordneter ZS anfordern* gelangen (Abbildung 15.115).
5. Aktivieren Sie in diesem Fenster die Option *Zertifikatanforderung an übergeordnete Zertifizierungsstelle senden* und klicken Sie auf *Durchsuchen*.
6. Wählen Sie die bereits installierte Root-CA aus.
7. Schließen Sie die Installation der CA ab.

Abbildg. 15.114 Installieren einer untergeordneten Zertifizierungsstelle auf dem Netzwerkrichtlinienserver



Abbildg. 15.115 Auswählen der übergeordneten Zertifizierungsstelle bei der Installation einer untergeordneten Zertifizierungsstelle



Installieren der Integritätsregistrierungsinstanz

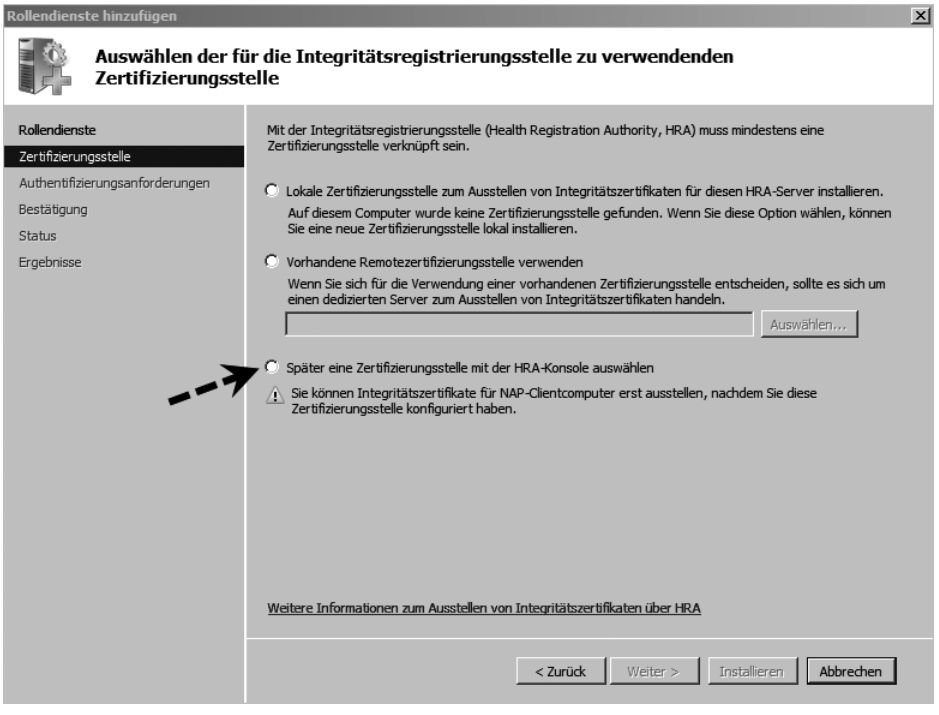
Fügen Sie nach der Installation der untergeordneten CA den Netzwerkrichtlinien-Rollendienst *Integritätsregistrierungsinstanz* über den Server-Manager hinzu (Abbildung 15.116):

1. Bestätigen Sie bei der Auswahl des Rollendienstes, dass notwendige zusätzliche Funktionen installiert werden. Die geläufigere Bezeichnung für Integritätsregistrierungsinstanz ist der englische Begriff *Health Registration Authority (HRA)*.

Abbildg. 15.116 Installieren der Integritätsregistrierungsinstanz auf dem Netzwerkrichtlinienserver

2. Wählen Sie im nächsten Fenster die Option *Später einen Zertifikateserver mit dem HRA-Snap-In auswählen* (Abbildung 15.117).

Abbildg. 15.117 Konfigurieren des Zertifikateservers für die Integritätsregistrierungsinstanz



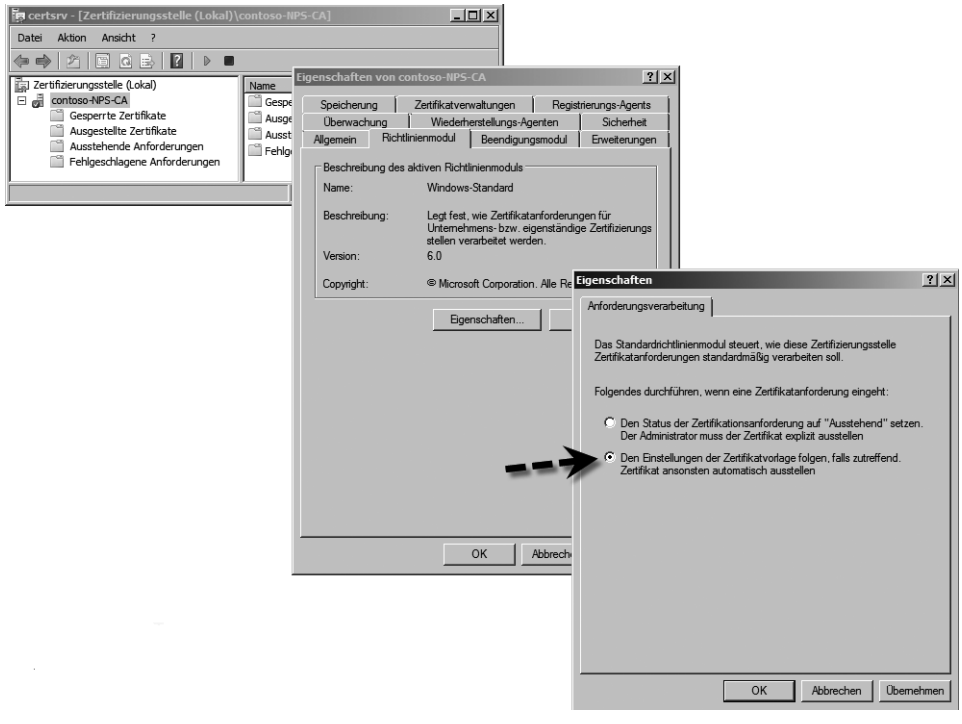
3. Im Fenster *Auswählen von Authentifizierungsanforderungen für die Integritätsregistrierungsstelle* aktivieren Sie die Option *Nein, anonyme Anforderungen von Integritätszertifikaten zulassen*.
4. Wählen Sie im nächsten Fenster *Serverauthentifizierungszertifikat für SSL-Verschlüsselung auswählen* die Option *Zertifikat zur späteren SSL-Verschlüsselung auswählen*, damit Sie das Zertifikat nach der Installation der HRA auswählen können. Microsoft empfiehlt zwar beim Einsatz einer HRA SSL zu verwenden, diese Konfiguration ist aber bei der Installation einer HRA nicht zwingend.
5. Bestätigen Sie alle restlichen Fenster und lassen Sie die Installation abschließen.

Konfiguration der untergeordneten Zertifizierungsstelle

Nachdem Sie die untergeordnete Zertifizierungsstelle und die Integritätsregistrierungsinstanz installiert haben, müssen Sie diese noch konfigurieren. Diese Konfiguration ist gleichzeitig eine Überprüfung der Installation:

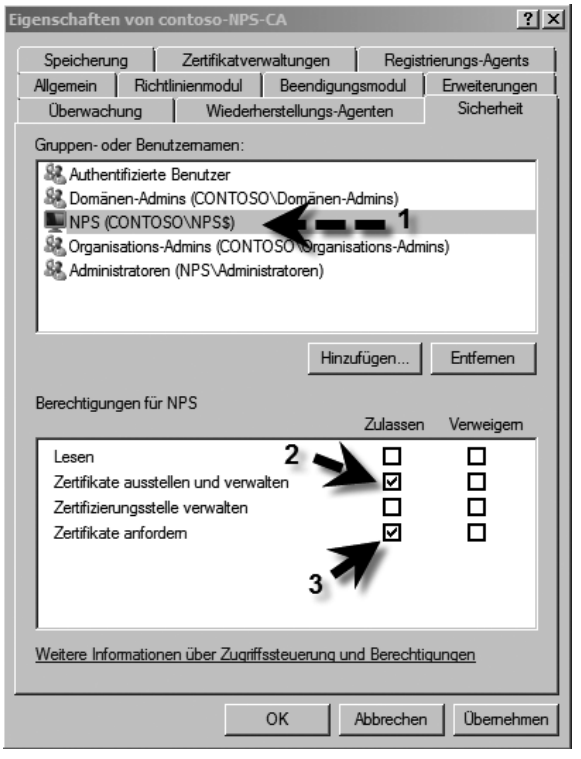
1. Starten Sie nach der Installation die Verwaltungskonsole der Zertifikatsdienste über *Start/Verwaltung* oder *Start/Ausführen/certsrv.msc*.
2. Klicken Sie die Zertifizierungsstelle mit der rechten Maustaste an und rufen Sie die Eigenschaften auf.
3. Aktivieren Sie die Registerkarte *Richtlinienmodul* und klicken Sie auf die Schaltfläche *Eigenschaften*.
4. Aktivieren Sie die Option *Den Einstellungen der Zertifikatvorlage folgen, falls zutreffend. Zertifikat ansonsten automatisch ausstellen*.

Abbildg. 15.118 Konfiguration der untergeordneten Zertifizierungsstelle für das automatische Ausstellen von Zertifikaten



5. Bestätigen Sie die Fenster und wechseln Sie anschließend zur Registerkarte *Sicherheit*.
6. Fügen Sie der Liste das Computerkonto des NPS-Servers hinzu und erteilen Sie diesem die Rechte *Zertifikate ausstellen und verwalten* und *Zertifikate anfordern*.

Abbildg. 15.119 Konfigurieren der Berechtigungen für die untergeordnete Zertifizierungsstelle

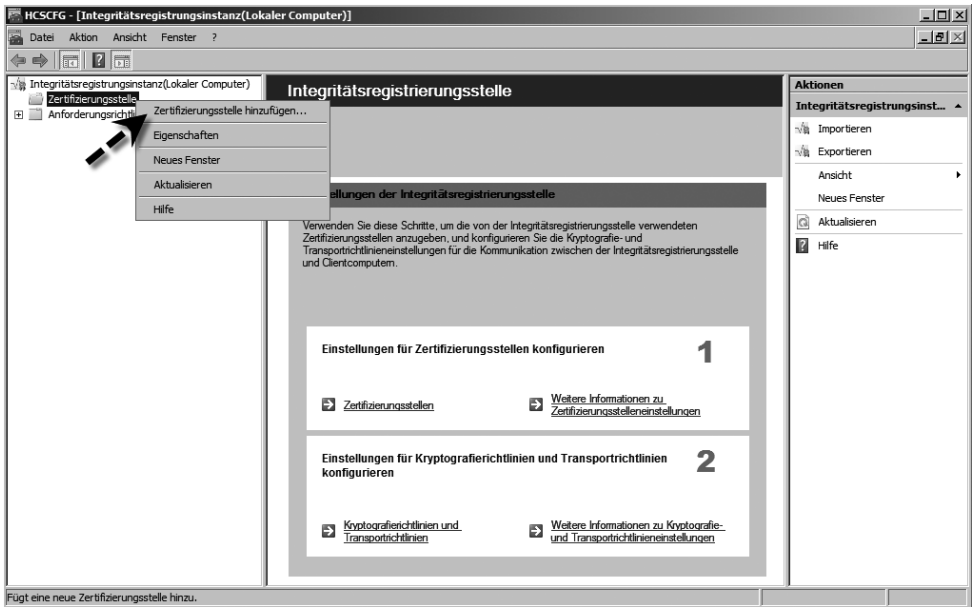


Konfigurieren der Integritätsregistrierungsinstanz

Nach diesen Konfigurationen müssen Sie als Nächstes die Integritätsregistrierungsinstanz über deren Verwaltungsoberfläche konfigurieren. Erstellen Sie dazu eine neue Management-Konsole mit dem Snap-In *Integritätsregistrierungsstelle*. Anschließend startet die Verwaltungsoberfläche der Integritätsregistrierungsinstanz (Abbildung 15.120).

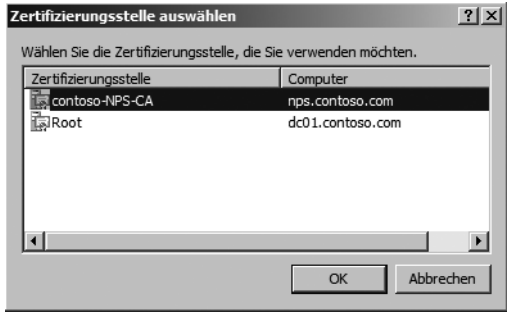
1. Klicken Sie mit der rechten Maustaste auf *Zertifizierungsstelle* und *Zertifizierungsstelle hinzufügen*.

Abbildg. 15.120 Hinzufügen einer Zertifizierungsstelle zur Integritätsregistrierungsinstanz



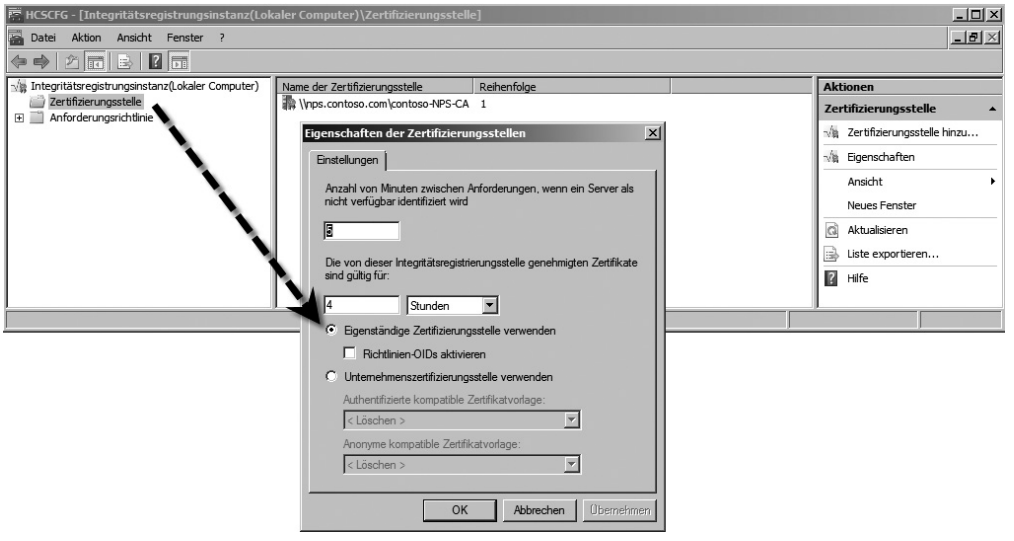
2. Klicken Sie auf *Durchsuchen* und wählen Sie die untergeordnete Zertifizierungsstelle aus, nicht die übergeordnete Root-CA (Abbildung 15.121).

Abbildg. 15.121 Auswählen der Zertifizierungsstelle für die Integritätsregistrierungsinstanz



3. Klicken Sie anschließend nochmals auf den Konsoleneintrag *Zertifizierungsstelle* und überprüfen Sie, ob die Option *Eigenständige Zertifizierungsstelle verwenden* aktiviert ist (Abbildung 15.122).

Abbildg. 15.122 Konfigurieren der Zertifizierungsstelle für die Integritätsregistrierungsinstanz



Konfigurieren des Netzwerkrichtlinienservers für die Verwendung des Netzwerkzugriffsschutzes (NAP)

Im Anschluss können Sie den Netzwerkrichtlinienserver so konfigurieren, dass der Netzwerkzugriffsschutz verwendet wird. So können Sie auf Basis der Windows-Sicherheitsintegritätsverifizierung sicherstellen, welche Clients eine sichere IPSec-Verbindung aufbauen können. Sie können diese Konfiguration mit dem Assistenten für den Netzwerkzugriffsschutz durchführen. Starten Sie dazu die Verwaltung des Netzwerkrichtlinienservers über *Start/Verwaltung* oder über *nps.msc*. Gehen Sie zur Konfiguration folgendermaßen vor:

1. Klicken Sie auf den obersten Eintrag der Konsole und dann in der Mitte der Konsole auf *NAP konfigurieren*, um den Assistenten zu starten (Abbildung 15.123).
2. Wählen Sie als Netzwerkverbindungsmethode die Option *IPSec mit Integritätsregistrierungsstelle (HRA)* aus.
3. Auf der nächsten Seite des Assistenten legen Sie den Netzwerkzugriffserver fest, auf dem die Integritätsregistrierungsinstanz (HRA) installiert ist.
4. Auf der nächsten Seite könnten Sie spezielle Gruppen festlegen, die Sie für NAP über IPSec konfigurieren wollen. In den meisten Umgebungen können Sie dieses Fenster ohne Eingaben bestätigen.
5. Im nächsten Fenster legen Sie die NAP-Integritätsrichtlinie fest. Hier sollten die beiden Optionen *Windows-Sicherheitsintegritätsverifizierung* und *Automatische Wartung von Clients aktivieren* aktiviert sein (Abbildung 15.124).
6. Bestätigen Sie die Optionen und schließen Sie den Assistenten ab.

TIPP Handelt es sich bei dem HRA-Server und dem NPS-Server nicht um den gleichen Server, müssen Sie den HRA-Server als RADIUS-Client auf dem NPS-Server hinterlegen.

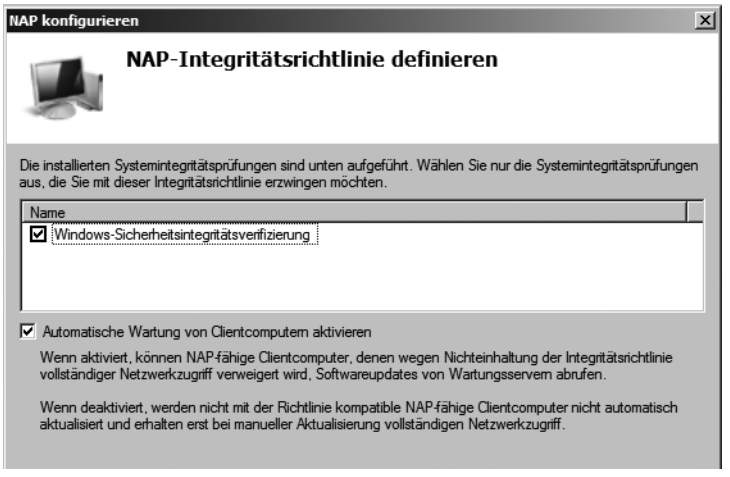
Abbildg. 15.123 Konfigurieren des Netzwerkzugriffsschutzes (NAP) über IPSec

Konfigurieren der Systemintegritätsprüfungen

Der nächste Schritt besteht darin, dass Sie die Windows-Sicherheitsintegritätsverifizierung konfigurieren:

1. Klicken Sie dazu in der NAP-Konsole auf *Netzwerkzugriffsschutz/Systemintegritätsprüfungen.*
2. Rufen Sie die Eigenschaften der *Windows-Sicherheitsintegritätsverifizierung* auf.
3. Klicken Sie im Fenster auf die Schaltfläche *Konfigurieren*. Jetzt können Sie konfigurieren, welche Bedingungen eine Arbeitsstation erfüllen muss, damit diese mit dem Netzwerk kommunizieren darf.
4. Deaktivieren Sie für diesen Test alle Kontrollkästchen außer *Für alle Netzwerkverbindungen ist eine Firewall aktiviert.*
5. Das Kontrollkästchen *Windows Update* können Sie aktiviert lassen. Hierüber wird konfiguriert, ob der Client seine Patches von einem WSUS-Server erhält oder direkt aus dem Internet.

Abbildg. 15.124 Auswählen der NAP-Integritätsrichtlinie für NAP über IPSec



Konfigurieren der Clients für die IPSec-Kommunikation

Im nächsten Schritt werden die Clients im Netzwerk so konfiguriert, dass die Kommunikation über die in diesem Workshop erstellte Infrastruktur per IPSec und NAP-geschützt stattfinden kann. Wollen Sie IPSec mit NAP im Unternehmen einsetzen, werden nur Arbeitstationen mit Windows Vista oder Arbeitsstationen mit Windows XP SP2 bei installiertem Client für den Netzwerkzugriffsschutz unterstützt.

Aktivieren des Sicherheitscenter auf Domänen-PCs

Die Verwaltung von IPsec und dem Netzwerkzugriffsschutz baut auf die Sicherheitsintegritätsprüfung, in diesem Fall die *Windows-Sicherheitsintegritätsverifizierung* auf. Diese ruft von den Clients das *Statement of Health (SoH)* ab. Diese Einstellungen finden Sie in der Verwaltungskonsole über *NPS/Netzwerkzugriffsschutz/Systemintegritätsprüfungen*. Diese Systemintegritätsprüfungen bezeichnet Microsoft auch als *Security Health Agents (SHA)*. Der SHA wird in Windows Vista durch den Windows *Security Health Validator (SHV)* verbunden. Hauptsächlich überprüfen diese SHAs den Zustand des Windows-Sicherheitscenters in Windows Vista und XP. Damit die Windows-Sicherheitsintegritätsverifizierung unter Windows Server 2008 Daten empfangen kann, muss auf dem Windows Vista-PC das Sicherheitscenter aktiviert sein. Das Sicherheitscenter fragt die entsprechenden Daten auf dem PC ab und sendet diese zum NPS-Server. Auf Windows Vista-PCs, die Mitglied einer Domäne sind, wird das Sicherheitscenter standardmäßig deaktiviert. Um NAP unter Windows Vista zu testen, müssen Sie dieses daher aktivieren. Sie finden die Einstellung auch über Gruppenrichtlinien. Gehen Sie dazu folgendermaßen vor:

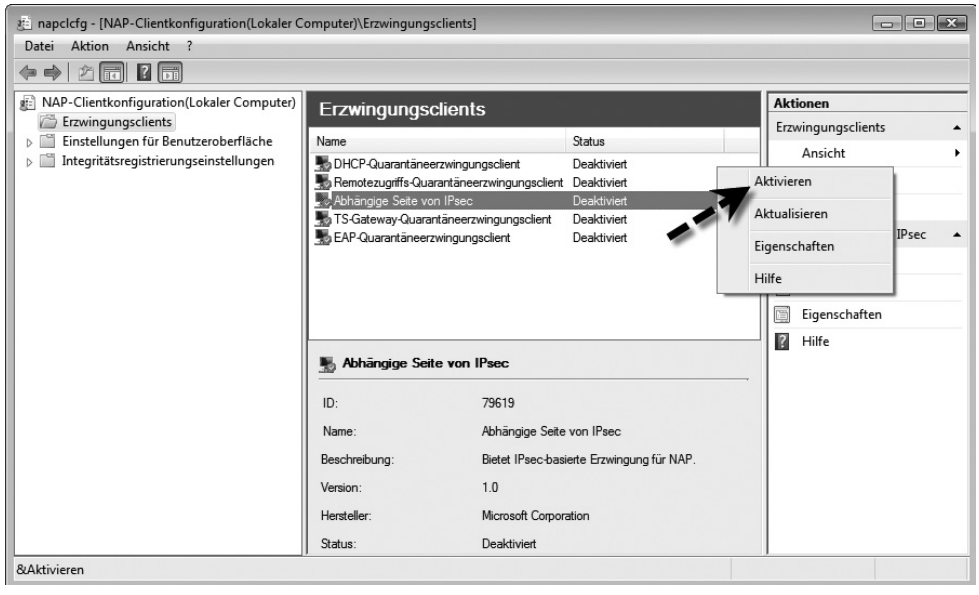
1. Navigieren Sie zu *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Sicherheitscenter.*
2. Aktivieren Sie die Richtlinie *Sicherheitscenter aktivieren (nur Domänencomputer)*.

Aktivieren des IPSec-Erzwingungsclients

Die nächste Aufgabe, die Sie durchführen müssen, ist die Aktivierung der NAP-Unterstützung auf dem Client:

1. Starten Sie dazu auf dem Vista-PC über *Start/Ausführen/napclcfg.msc* die Verwaltungskonsole des NAP-Clients (Abbildung 15.125).
2. Klicken Sie auf den Konsoleneintrag *Erzwingungsclients*.
3. Aktivieren Sie *Abhängige Seite von IPSec*.

Abbildg. 15.125 Aktivieren des IPSec-Erzwingungsclients unter Windows Vista



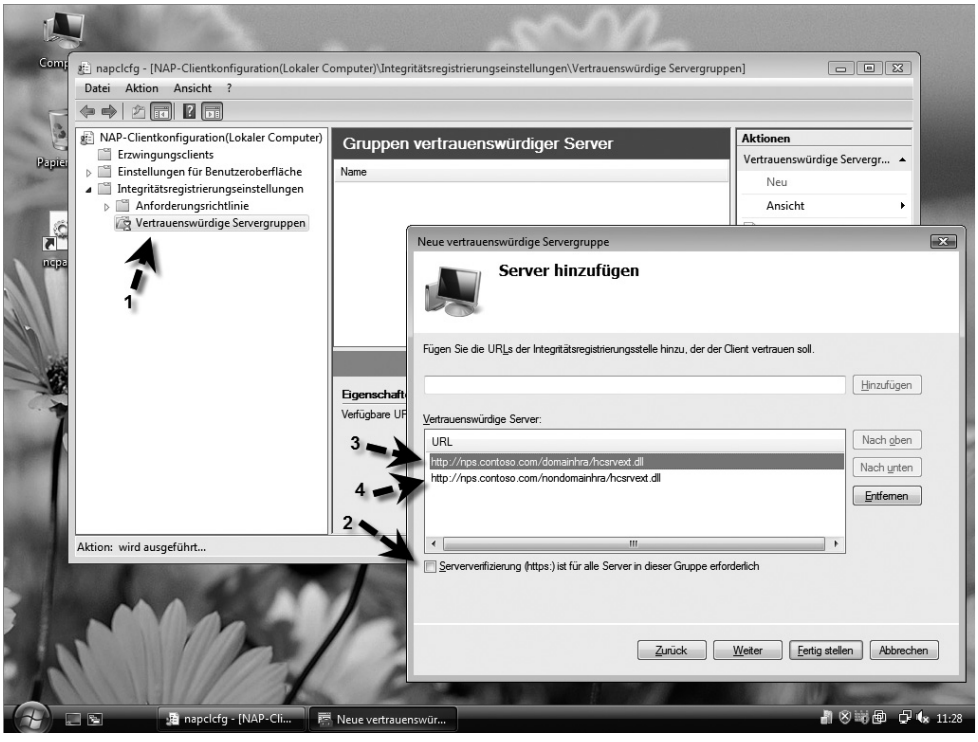
Alternativ können Sie Erzwingungsclients für den Netzwerkzugriffsschutz auch über Gruppenrichtlinien aktivieren. Diese Einstellung finden Sie unter *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Network Access Protection/NAP-Clientkonfiguration/Erzwingungsclients*.

Konfiguration Integritätsregistrierungseinstellungen

Für die Verwendung von NAP über IPSec müssen Sie in der NAP-Clientkonfiguration noch den Menüpunkt *Integritätsregistrierungseinstellungen* aufrufen:

1. Klicken Sie mit der rechten Maustaste auf die Gruppe *Vertrauenswürdige Servergruppen* und wählen *Neu*.
2. Geben Sie im nächsten Fenster der Gruppe eine Bezeichnung. Geben Sie zum Beispiel HRA-Server ein, da die Integritätsregistrierungsstellen-Server für diese Konfiguration verwendet werden.
3. Deaktivieren Sie für diesen Workshop das Kontrollkästchen *Serververifizierung (https:) ist für alle Server in dieser Gruppe erforderlich*.

Abbildg. 15.126 Konfigurieren der vertrauenswürdigen Servergruppen auf dem NAP-Client

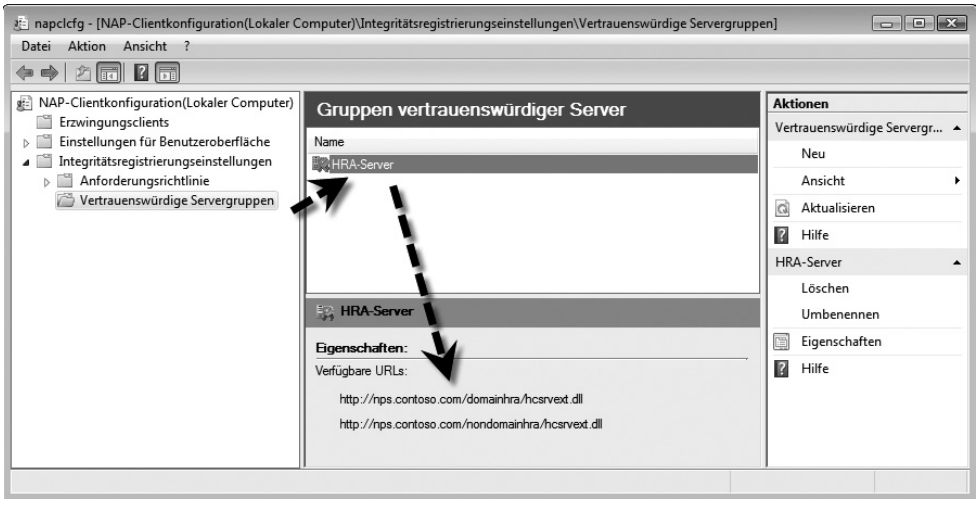


4. Fügen Sie im Fenster noch die URL *http://<NPS-Servername>/domainhra/hcsrvext.dll* als Health Registration Authority (HRA) hinzu. Dieser Server stellt Zertifikate für jene Computer aus, die sich in der Domäne authentifiziert haben.
5. Als Nächstes fügen Sie die URL *http://<NPS-Servername>/nondomainhra/hcsrvext.dll* ein. Diese URL wird nach der oberen URL angeordnet. Durch diese Konfiguration wird sichergestellt, dass sich Clients erst authentifizieren müssen, um ein Zertifikat zu erhalten. Gelingt das nicht, wird die zweite URL verwendet, welche ebenfalls einen anonymen Zugriff gestattet. Stellen Sie sicher, dass Sie beide URLs korrekt eintragen. Über diese URLs beantragen Clients automatisch Zertifikate, die automatisch von der Zertifizierungsstelle ausgestellt werden. Geben Sie eine fehlerhafte URL an, können Clients kein Zertifikat anfordern und die IPSec-Kommunikation schlägt fehl. Starten Sie auf dem NPS-Server den Internetinformationsdienste-Manager, können Sie diese beiden Webs anzeigen lassen (Abbildung 15.127).

Abbildg. 15.127 Anzeigen der Webseite für die Zertifikatsregistrierung von NAP-Clients

6. Schließen Sie die Konfiguration ab. Anschließend sollten die vertrauten Server und deren URL in der NAP-Client-Verwaltungskonsole angezeigt werden (Abbildung 15.128).

Abbildg. 15.128 Anzeigen der vertrauenswürdigen Servergruppen in der NAP-Client-Verwaltungskonsole



Alternativ können Sie diese Konfiguration für den Netzwerkzugriffsschutz auch über Gruppenrichtlinien aktivieren. Diese Einstellung finden Sie unter *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Network Access Protection/NAP-Clientkonfiguration*.

NAP-Agent (Network Access Protection) aktivieren

Der nächste Schritt zur Anbindung von Windows Vista an eine NAP-Infrastruktur ist die Aktivierung des Systemdienstes *NAP-Agent (Network Access Protection)*. Setzen Sie den Starttyp dieses Dienstes auf *Automatisch* und starten Sie diesen.

Erlauben von Ping zwischen den Clients

Zur Verifizierung der Verbindung zwischen den Clients sollten Sie noch das ICMP-Protokoll in der Windows-Firewall der Clients in der Testumgebung freischalten. Ohne die Aktivierung dieses Protokolls wird ICMP und damit ein Ping blockiert. Öffnen Sie dazu auf dem Client die erweiterte Verwaltungsoberfläche für die Windows-Firewall:

1. Der schnellste Weg hierzu ist über *Start/Ausführen/wf.msc*.
2. Klicken Sie mit der rechten Maustaste auf *Eingehende Regeln* und wählen Sie *Neue Regel* aus.
3. Wählen Sie im Konfigurationsfenster *Benutzerdefiniert* aus.
4. Aktivieren Sie auf der nächsten Seite *Alle Programme*.
5. Wählen Sie auf der nächsten Seite bei Protokolltyp die Option *IPv4* aus.
6. Klicken Sie auf *Anpassen*.
7. Aktivieren Sie die Option *Bestimmte ICMP-Typen*.
8. Aktivieren Sie die Option *Echoanforderung*.
9. Klicken Sie auf *OK* und dann auf *Weiter*.
10. Klicken Sie auf *Weiter*, um die Standardeinstellungen für den DHCP-Bereich zu bestätigen.
11. Klicken Sie noch mal auf *Weiter* und stellen Sie sicher, dass die Option *Verbindungen zulassen* aktiviert ist.
12. Im nächsten Fenster bestätigen Sie die Aktivierung der Regel für alle Netzwerk-Profile.
13. Weisen Sie der Regel einen entsprechenden Namen zu und schließen Sie die Erstellung der Regel ab.

Überprüfen der Zertifikate

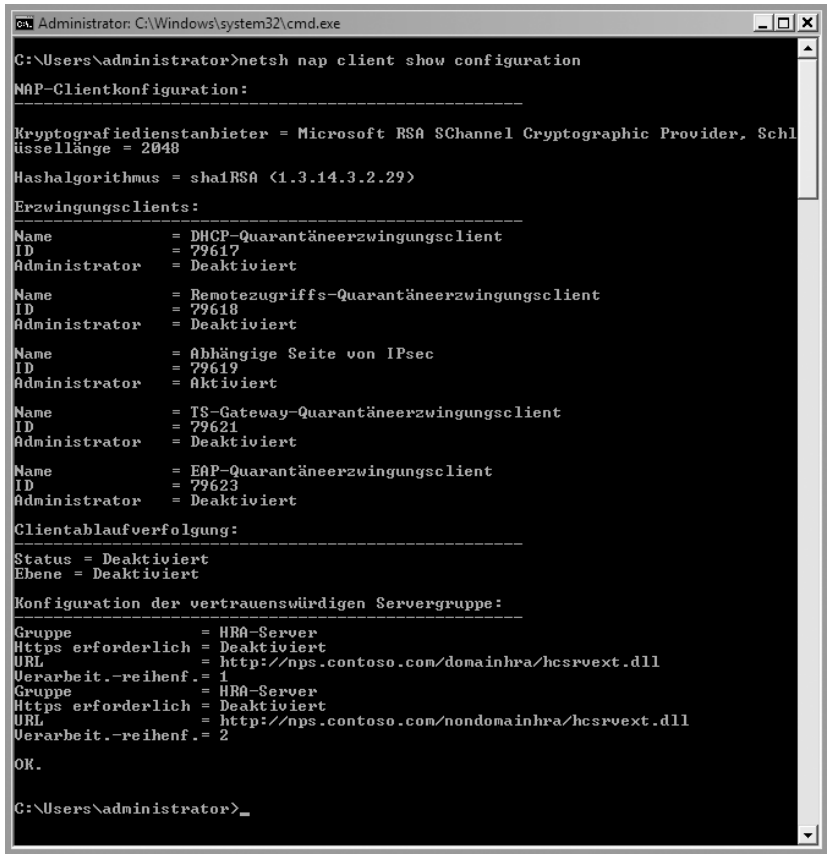
Starten Sie den Client neu und melden Sie sich an. Öffnen Sie anschließend die Verwaltungskonsole für lokale Zertifikate. Fügen Sie dazu in einer Verwaltungskonsole das Snap-In *Zertifikate* hinzu und öffnen Sie den lokalen Zertifikatespeicher. Hier sollte ein Zertifikat angezeigt werden, das durch die Zertifizierungsstelle ausgestellt worden ist.

Fehlersuche bei der Einrichtung von NAP über IPSec

Nachdem Sie die Konfiguration vorgenommen haben, wie in den vorangegangenen Abschnitten besprochen, können Sie überprüfen, ob dem Client ein Zertifikat ausgestellt worden ist. Sie finden die Zertifikate über das lokale Snap-In *Zertifikate*. Sollte sich kein Zertifikat in diesem Speicher finden, kann die Konfiguration nicht durchgeführt werden. Überprüfen Sie in diesem Fall, ob Sie die Konfiguration vorgenommen haben, wie wir auf den vorangegangenen Seiten beschrieben haben.

TIPP Sie können mit dem Befehl *netsh nap client show configuration* die Konfiguration des NAP-Clients in der Befehlszeile anzeigen lassen (Abbildung 15.129). Um ein neues Integritätszertifikat anzufordern, reicht es, wenn Sie den Systemdienst des NAP-Agents neu starten, Sie müssen nicht den ganzen PC booten.

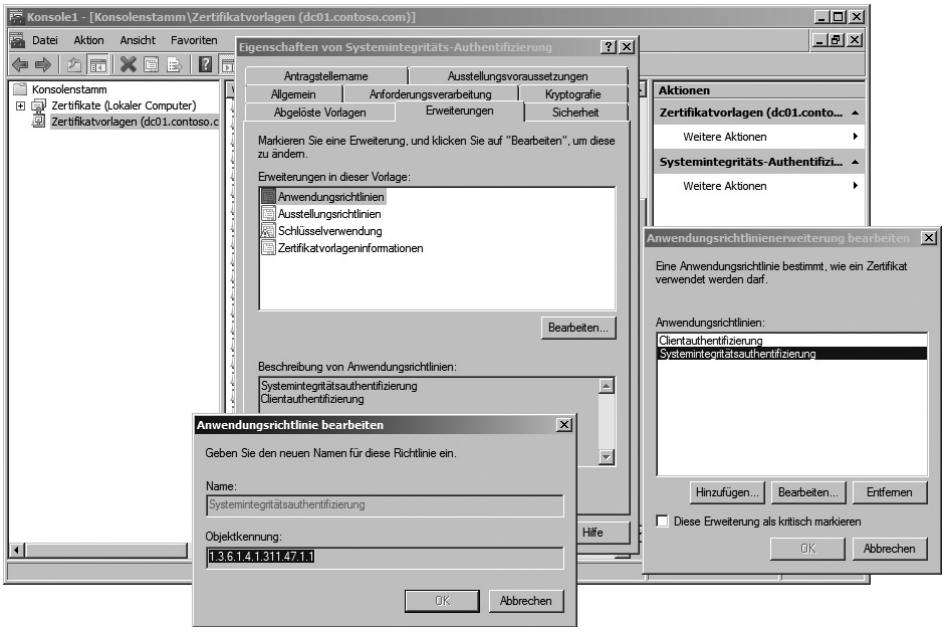
Abbildg. 15.129 Anzeigen der NAP-Client-Konfiguration in der Befehlszeile



Wichtig ist, dass der Erzwingungsclient für IPSec aktiviert worden ist, die URLs für die vertrauenswürdige Servergruppe stimmen, das Windows-Sicherheitscenter über die Systemsteuerung gestartet werden kann und der NAP-Client-Dienst gestartet ist. Die aktuelle Logdatei für den NPS finden Sie auf dem Server im Verzeichnis *C:\Windows\System32\LogFiles*. Hier finden Sie viele Infos, was die Arbeit des NPS transparenter macht. Sollten Sie hier Fehler finden, können Sie diese recht schnell eingrenzen. Auch in den Ereignisanzeigen des NPS-Servers werden viele Ereignisse festgehalten, wenn die NAP-Vorgänge ablaufen. Sie finden diese Fehler im Systemprotokoll auf dem Server. Auf dem Client finden Sie in der Ereignisanzeige über *Anwendungs- und Dienstprotokolle/Microsoft/Windows/Network Access Protection/Operational* zahlreiche Ereignisse, wenn Sie den NAP-Agent-Dienst neu starten. Diese Ereignisse haben die Quelle *Network Access Protection* und *SystemHealthState*. Zusätzlich sollten Sie noch folgende Funktionen überprüfen:

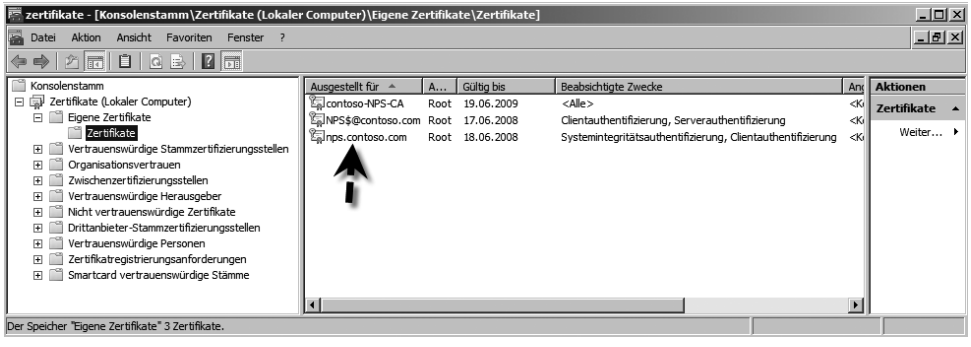
1. Stellen Sie sicher, dass das Computerkonto des NPS-Servers in den Eigenschaften der untergeordneten Zertifizierungsstelle auf der Registerkarte Sicherheit eingetragen ist und über die Rechte *Zertifikate ausstellen und verwalten* und *Zertifikate anfordern* verfügt.
2. Stellen Sie sicher, dass für die übergeordnete und untergeordnete Zertifizierungsstelle auf der Registerkarte *Richtlinienmodul* die automatische Registrierung aktiviert worden ist.
3. Stellen Sie sicher, dass die Objekterkennung der neuen Zertifikatvorlage in der Zertifikatvorlagen-Verwaltung auf der Registerkarte *Erweiterungen* über *Anwendungsrichtlinien/Bearbeiten/Systemintegritätsauthentifizierung/Bearbeiten* auf *1.3.6.1.4.1.311.47.1.1* gesetzt ist.

Abbildg. 15.130 Überprüfen der Objektkennung der Anwendungsrichtlinie



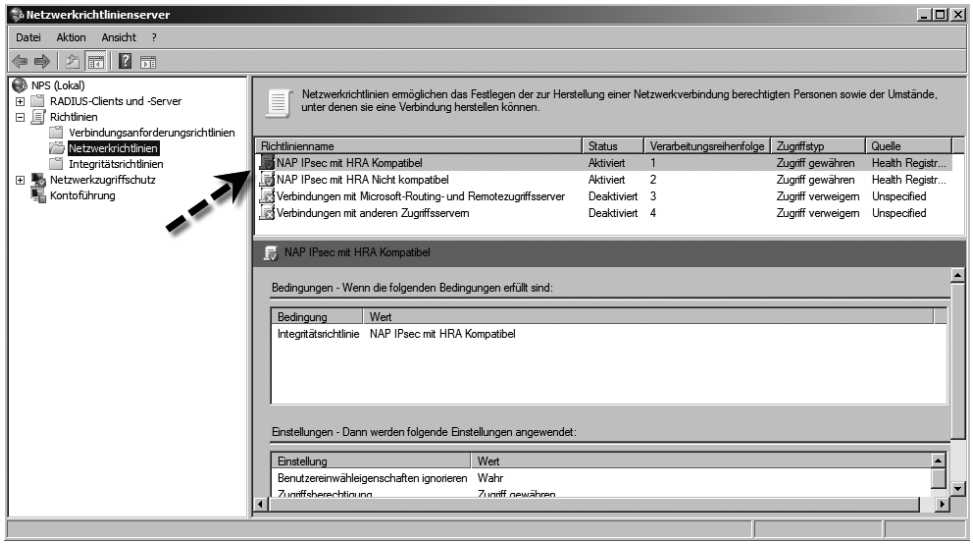
4. Stellen Sie sicher, dass dem NPS-Server, der auch als Health Registration Authority dient, ein Systemintegritätsauthentifizierungs-Zertifikat ausgestellt wurde (Abbildung 15.131).

Abbildg. 15.131 Überprüfen des Systemintegritätsauthentifizierungs-Zertifikats auf dem HRA-Server



5. Stellen Sie sicher, dass in der Netzwerkrichtlinienserver-Verwaltung (*Start/Ausführen/nps.msc*) unter dem Konsoleneintrag *Richtlinien/Netzwerkrichtlinien* die beiden Netzwerkrichtlinien für NAP in der Reihenfolge ganz oben angeordnet wurden. Diese Richtlinien sind bei der Durchführung des NAP-Assistenten weiter vorne in diesem Kapitel automatisch erstellt worden. Deaktivieren Sie im Idealfall alle anderen Netzwerkrichtlinien.

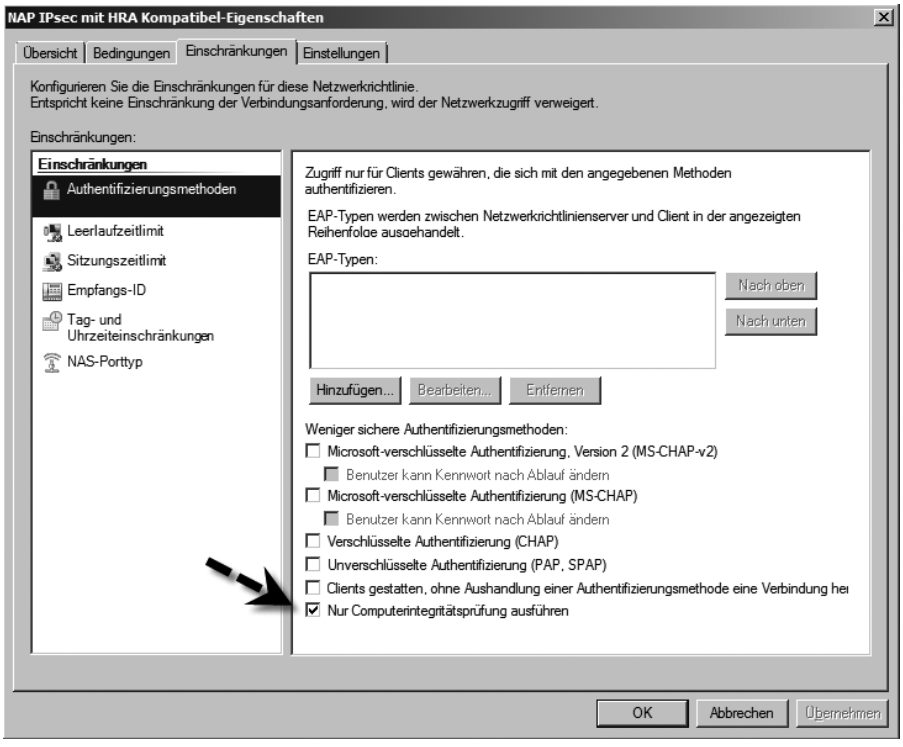
Abbildg. 15.132 Überprüfen der Netzwerkrichtlinien für die NAP-Unterstützung von IPSec



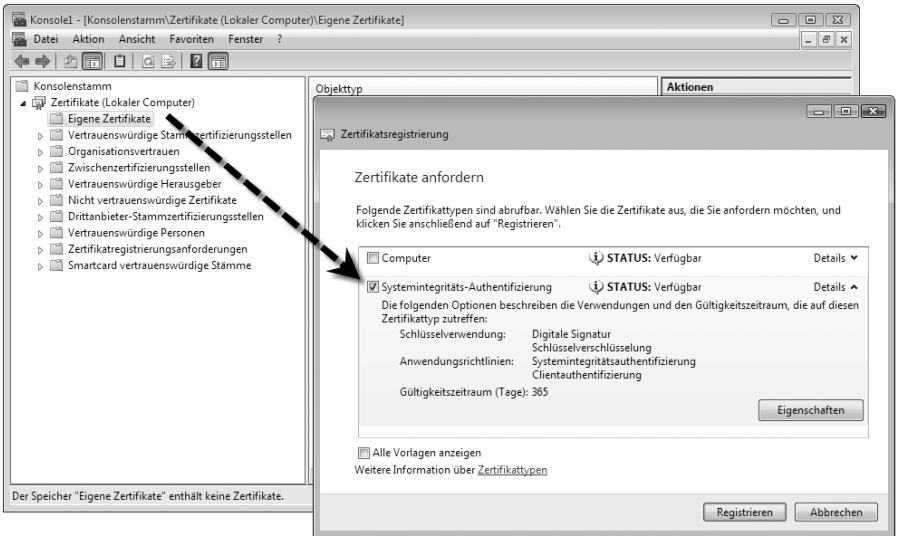
6. Rufen Sie zusätzlich die Eigenschaften der Richtlinie auf. Klicken Sie auf die Registerkarte *Einschränkungen*. Klicken Sie auf Authentifizierungsmethoden. Stellen Sie sicher, dass nur das Kontrollkästchen *Nur Computerintegritätsprüfung ausführen* aktiviert ist, keine anderen Authentifizierungsoptionen (Abbildung 15.133).

Sollten Sie immer noch kein Zertifikat erhalten, können Sie über die Zertifikateverwaltung des Clients durch Rechtsklick auf *Eigene Zertifikate/Alle Aufgaben/Neues Zertifikat anfordern* ein Zertifikat manuell ausstellen. Hier sollte auf jeden Fall das von Ihnen neu erstellte Zertifikat für die Systemintegritäts-Authentifizierung angezeigt werden. Um die IPSec-Einrichtung vornehmen zu können, besteht auch die Möglichkeit, dass Sie sich zunächst manuell ein Zertifikat ausstellen, die IPSec-Einrichtung durchführen und später überprüfen, warum das automatische Registrieren von Zertifikaten nicht funktioniert.

Abbildg. 15.133 Überprüfen der Clientauthentifizierung in den Netzwerkrichtlinien für NAP



Abbildg. 15.134 Manuelles Registrieren eines Zertifikats



Erstellen von IPSec-Richtlinien

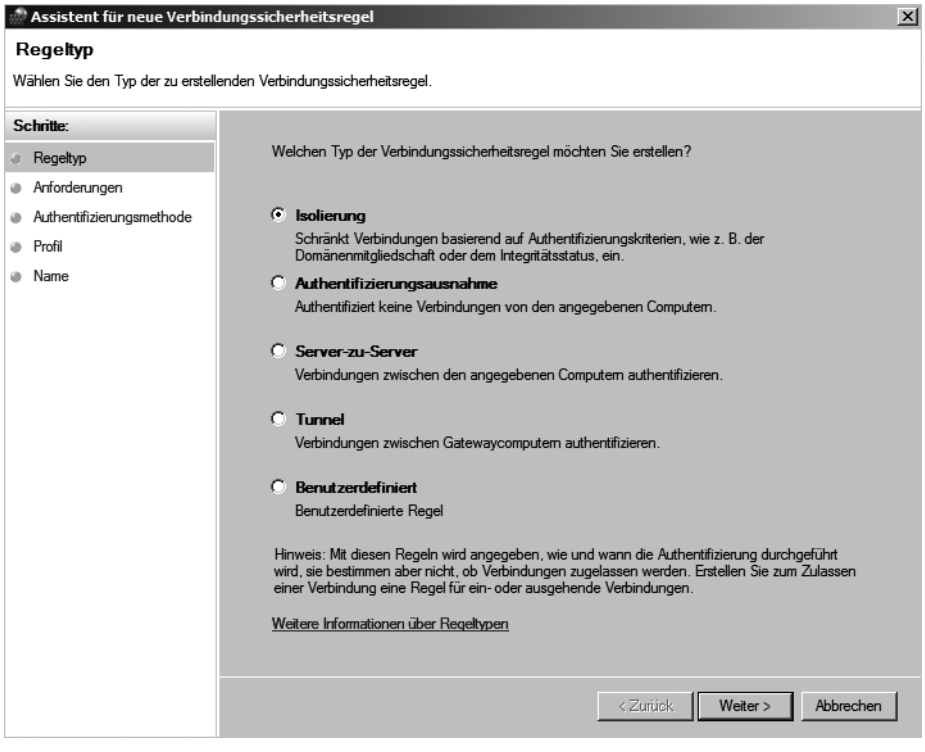
IPSec-Richtlinien können entweder zusammen mit dem Netzwerkzugriffsschutz (NAP) eingerichtet werden, oder, wie unter Windows Server 2003, ohne diese Funktion. Wollen Sie IPSec zusammen mit NAP einsetzen, sollten Sie zunächst die NAP-Einstellungen vornehmen, wie auf den vorderen Seiten beschrieben wurde. Solche Richtlinien erstellen Sie am besten über die Einstellungen der erweiterten Firewall über die Gruppenrichtlinien. Sie können dazu die Default Domain Policy verwenden oder für IPSec eine neue Gruppenrichtlinie erstellen, die Sie dann mit der OU verknüpfen, in der Sie die Computerkonten der Server und PCs aufnehmen, die per IPSec kommunizieren können sollen:

1. Sie finden die notwendigen Einstellungen für IPSec in der Gruppenrichtlinienverwaltung über *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Windows-Firewall mit erweiterter Sicherheit/Windows-Firewall mit erweiterter Sicherheit – LDAP* (Abbildung 15.135).
2. Rufen Sie über die rechte Maustaste die Eigenschaften von *Windows-Firewall mit erweiterter Sicherheit – LDAP* auf.
3. Anschließend stehen Ihnen verschiedene Registerkarten zur Verfügung, auf denen Sie Voreinstellungen treffen müssen. Hauptsächlich werden hier die Einstellungen für die verschiedenen Netzwerkprofile der PCs vorgenommen. Sie sollten für alle Netzwerkprofile identische Einstellungen vornehmen.
4. Setzen Sie den Firewallstatus auf *Ein (Empfohlen)*.
5. Setzen Sie die Option für *Eingehende Verbindungen* auf *Blocken (Standard)*.
6. Setzen Sie die Option auf *Ausgehende Verbindungen* auf *Zulassen (Standard)*.
7. Führen Sie diese Einstellungen für alle drei Netzwerkprofile durch.
8. Bestätigen Sie die Eingaben mit *OK*.

Abbildg. 15.135 Aktivieren der Windows-Firewall und sicherer Verbindungen über Gruppenrichtlinien

9. Klicken Sie anschließend auf *Verbindungssicherheitsregeln* und wählen Sie *Neue Regel* aus. Danach können Sie auswählen, welche Art von Regel Sie erstellen wollen. Dazu stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Für die Einrichtung von IPSec-Verbindungen eignet sich am besten die Option *Isolierung*, die Sie auch auswählen sollten. Eine Isolierungsregel schränkt Verbindungen auf der Grundlage der von Ihnen definierten Authentifizierungskriterien ein. So können Sie Computer Ihrer Domäne von Computern außerhalb der Domäne isolieren. Die *Authentifizierungsausnahme* kann verwendet werden, um Computer unabhängig von anderen Verbindungssicherheitsregeln von der Anforderung auszunehmen, sich selbst zu authentifizieren. Dieser Regeltyp wird gewöhnlich verwendet, um den Zugriff auf Infrastrukturcomputer (Active Directory-Domänencontroller, Zertifizierungsstellen oder DHCP-Server) zu gewährleisten, mit denen der betreffende Computer bereits kommunizieren muss, bevor eine Authentifizierung durchgeführt werden kann. Obwohl die Computer von der Authentifizierung ausgenommen sind, können sie nach wie vor von der Firewall blockiert werden, sofern keine Firewallregel die Verbindung zulässt. Mit dem Regeltyp *Server zu Server* wird die Kommunikation zwischen zwei Computern, zwischen zwei Subnetzen oder zwischen einem bestimmten Computer und einer Gruppe von Computern authentifiziert. Mit einem *Tunnel* wird die Kommunikation zweier Computer zwischen Tunnelendpunkten abgesichert, z.B. bei virtuellen privaten Netzwerken oder L2TP-Tunneln (IPsec Layer Two Tunneling Protocol).

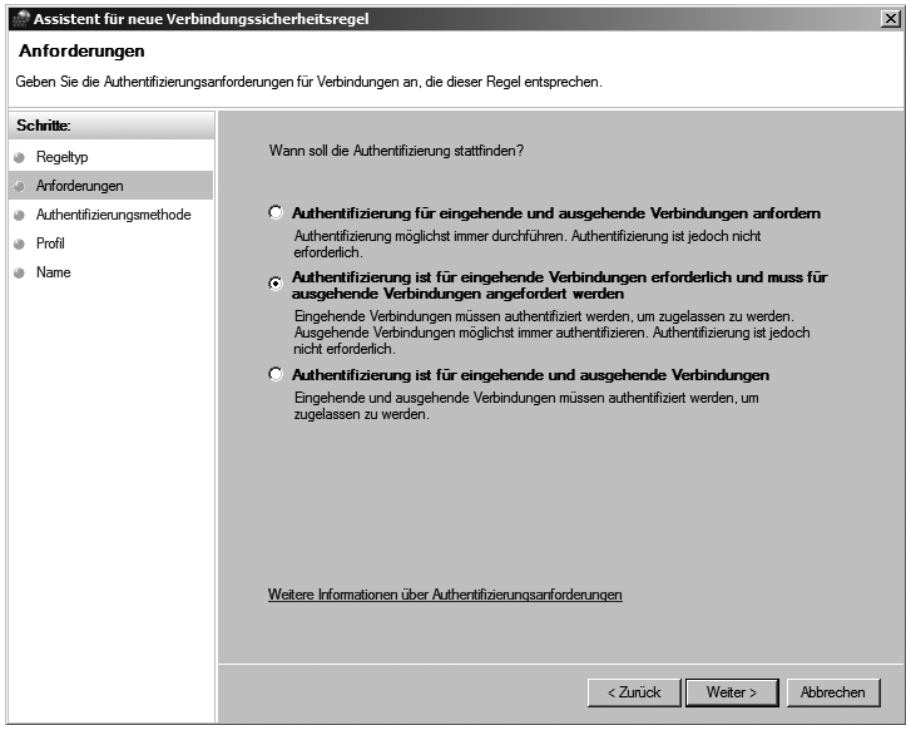
Abbildg. 15.136 Erstellen einer Isolierungs-Verbindungssicherheitsregel für IPSec



10. Auf der nächsten Seite des Assistenten legen Sie die Art der Authentifizierung fest. Wählen Sie hier die Option *Authentifizierung ist für eingehende Verbindungen erforderlich und muss für ausgehende*

Verbindungen angefordert werden aus. Mit dieser Option bestimmen Sie, dass der gesamte eingehende Datenverkehr authentifiziert oder anderenfalls blockiert wird. Der ausgehende Datenverkehr kann authentifiziert werden, ist aber auch bei fehlerhafter Authentifizierung zugelassen. Mit der Option *Authentifizierung für eingehende und ausgehende Verbindungen anfordern* legen Sie fest, dass der gesamte ein- und ausgehende Datenverkehr authentifiziert wird, lassen die Kommunikation jedoch auch bei fehlerhafter Authentifizierung zu. Wenn die Authentifizierung durchgeführt werden kann, wird der Datenverkehr authentifiziert. Die Option *Authentifizierung ist für eingehende und ausgehende Verbindungen erforderlich* legt fest, dass der gesamte ein- und ausgehende Datenverkehr authentifiziert oder anderenfalls blockiert wird.

Abbildg. 15.137 Festlegen der Authentifizierungs-Anforderungen für eine neue Verbindungssicherheitsregel

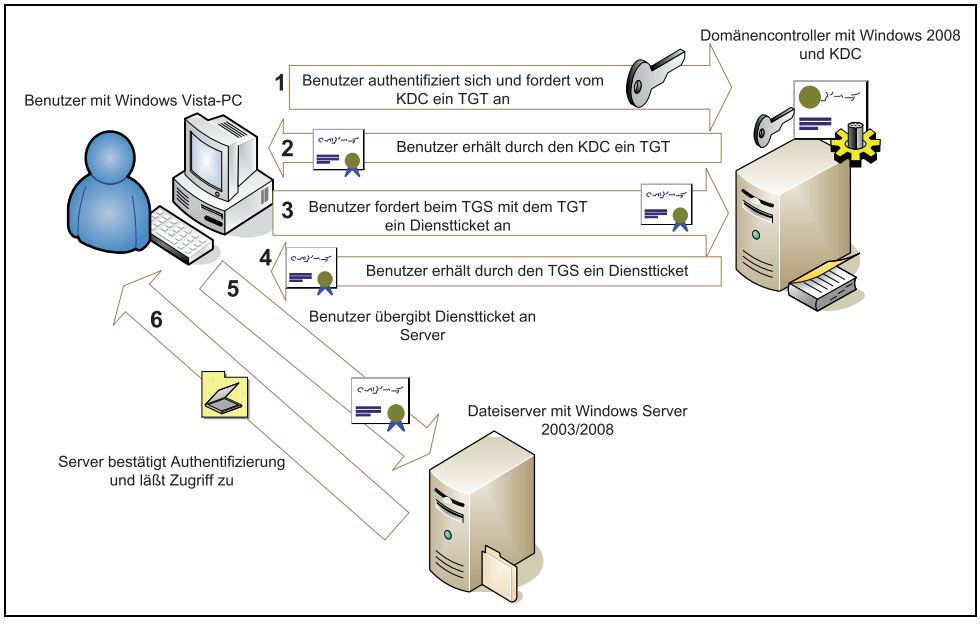


11. Auf der nächsten Seite legen Sie fest, auf welche Art die Authentifizierung hergestellt werden soll. Wählen Sie hier *Computerzertifikat* aus. Bei dieser Methode ist ein gültiges Integritätszertifikat zur Authentifizierung erforderlich oder wird angefordert. Die Option *Standard* legt die Authentifizierungsmethode gemäß der Konfiguration auf der Registerkarte *IPSec-Einstellungen* in den Eigenschaften der Windows-Firewall mit erweiterter Sicherheit fest. Bei *Computer und Benutzer (Kerberos V5)* wird sowohl die Computer- als auch die Benutzerauthentifizierung verwendet. Das bedeutet, dass sowohl die Benutzer- als auch die Computerauthentifizierung angefordert werden oder erforderlich sein können, bevor die Kommunikation fortgesetzt wird. Das Authentifizierungsprotokoll Kerberos Version 5 kann nur verwendet werden, wenn sowohl Computer als auch die Benutzer Mitglieder einer Domäne sind. Bei *Computer (Kerberos V5)* ist die Computerauthentifizierung über Kerberos Version 5 erforderlich oder wird angefordert. *Benutzer (Kerberos V5)* ist die Benutzerauthentifizierung mithilfe von Kerberos Version 5.

HINWEIS Bei Kerberos wird die Identität des Benutzers und die Identität des authentifizierenden Servers festgestellt. Kerberos arbeitet mit einem so genannten Ticket-System, um Benutzer zu authentifizieren. Kennwörter werden in einem Active Directory niemals über das Netzwerk übertragen. Damit sich ein Benutzer an einem Server authentifizieren kann, um zum Beispiel auf eine Freigabe eines Dateiservers zuzugreifen, wird ausschließlich mit verschlüsselten Tickets gearbeitet. Ein wesentlicher Bestandteil der Kerberos-Authentifizierung ist das Schlüsselverteilungscenter (Key Distribution Center, KDC). Dieser Dienst wird auf allen Windows Server 2008-Domänencontrollern ausgeführt und ist für die Ausstellung der Authentifizierungstickets zuständig. Der zuständige Kerberos-Client läuft auf allen Windows 2000, Windows Server 2003, 2008, XP und Vista-Computern. Wenn sich ein Benutzer an einer Arbeitsstation im Active Directory anmeldet, muss er sich zunächst an einem Domänencontroller und dem dazugehörigen KDC authentifizieren.

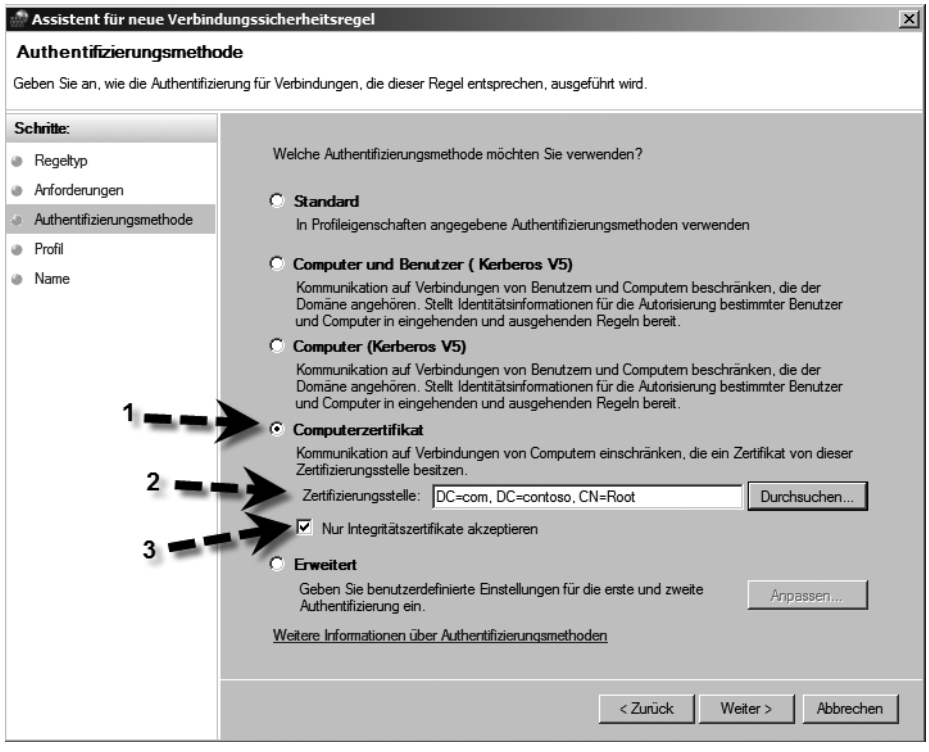
Im nächsten Schritt erhält der Client ein Ticket-genehmigendes Ticket (TGT) vom KDC ausgestellt. Nachdem der Client dieses TGT erhalten hat, fordert er beim KDC mithilfe dieses TGT ein Ticket für den Zugriff auf den Server an. Diese Authentifizierung führt der Ticket-genehmigende Dienst (Ticket Granting Service, TGS) auf dem KDC aus. Nach der erfolgreichen Authentifizierung des TGT durch den TGS, stellt dieser ein Dienstticket aus und übergibt dieses Ticket an den Client. Dieses Dienstticket gibt der Client an den Server weiter, auf den er zugreifen will, in diesem Beispiel der Dateiserver. Durch dieses Ticket kann der Dateiserver sicher sein, dass sich kein gefälschter Benutzer mit einem gefälschten Benutzernamen anmeldet. Durch das Dienstticket wird sowohl der authentifizierende Domänencontroller als auch der Benutzer authentifiziert. Der genaue Ablauf dieses Verfahrens ist in Abbildung 15.138 skizziert. Sollten Probleme mit dem Schlüsselverteilungscenter oder Kerberos im Allgemeinen auftreten, besteht unter Umständen noch ein Problem bei der Kerberosauthentifizierung. In diesem Fall wird allerdings in der Regel eine entsprechende Fehlermeldung bei *dcdiag.exe* angezeigt, die auf Probleme mit LDAP oder Kerberos hinweisen. Kerberos ist für die Anmeldung in Active Directory von existenzieller Wichtigkeit.

Abbildg. 15.138 Authentifizierung mit Kerberos in Active Directory



12. Aktivieren Sie die Option *Nur Integritätszertifikate akzeptieren*. Bei dieser Methode ist ein gültiges Integritätszertifikat zur Authentifizierung erforderlich oder wird angefordert.
13. Klicken Sie auf *Durchsuchen* und wählen Sie die erstellte Root-CA aus (Abbildung 15.139).

Abbildg. 15.139 Konfigurieren der Authentifizierung für eine IPSec-Verbindungssicherheitsregel



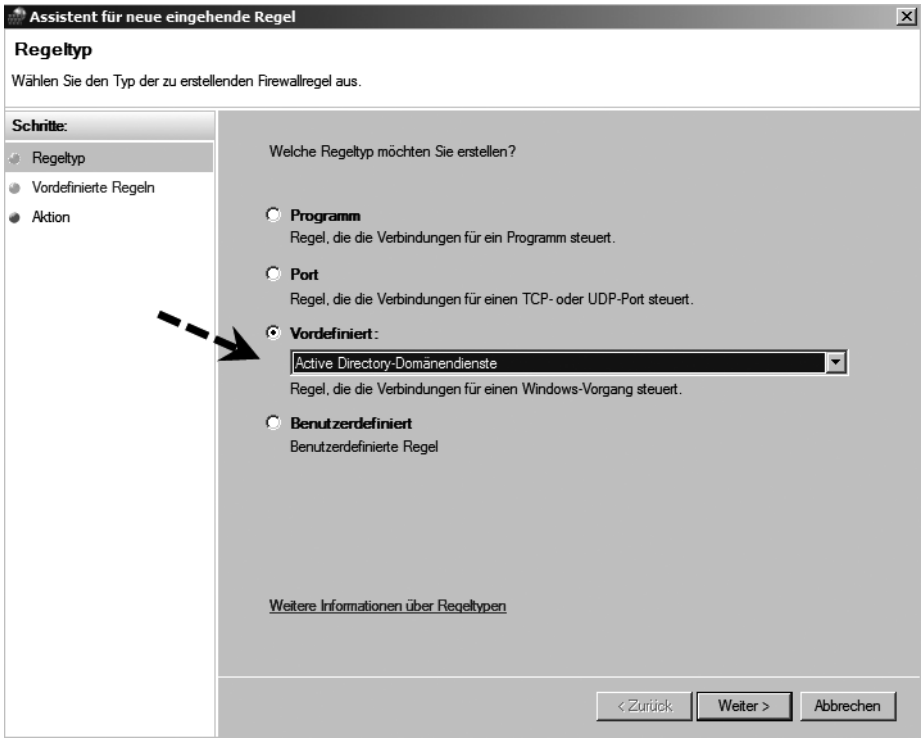
14. Aktivieren Sie auf der nächsten Seite die Regel für alle drei Netzwerkprofile.
15. Schließen Sie die Erstellung der Regel mit der Definition der Bezeichnung ab.
16. Die Regel wird anschließend in der Gruppenrichtlinie unter den Verbindungsregeln angezeigt.

Testen der Verbindung durch die Erstellung einer eingehenden Regel

Idealerweise testen Sie solche Verbindungsregeln zunächst in einer Testumgebung und legen die Gruppenrichtlinie, welche die Verbindungssicherheitsregeln festlegt, nur auf diese OU. Anschließend können Sie die Computerkonten der beteiligten PCs oder Server in diese OU verschieben, um die gesicherte Kommunikation zu verifizieren. Wählen Sie als Test-Clients eventuell zwei Windows Vista-PCs aus sowie einen Domänencontroller unter Windows Server 2008. Um den eingehenden Datenverkehr zu überprüfen, müssen Sie bei der Konfiguration dieses Workshops zunächst eine weitere Regel erstellen, welche die Kommunikation zulässt:

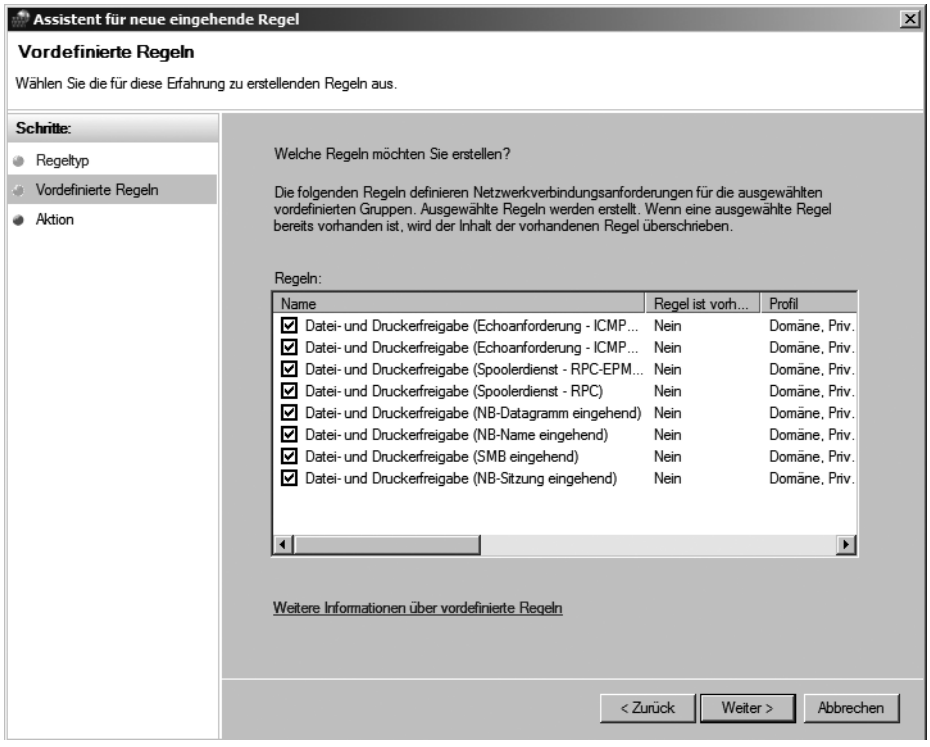
1. Klicken Sie dazu in der Gruppenrichtlinienverwaltung in der Verwaltung der Firewall mit erweiterter Sicherheit mit der rechten Maustaste auf *Eingehende Regeln* und wählen Sie *Neue Regel* aus.
2. Zum Testen der Verbindung von einzelnen Domänendiensten aktivieren Sie an dieser Stelle am besten die Option *Vordefiniert*.
3. Anschließend können Sie über das Auswahlmenü auf verschiedene Standardverbindungen in einem Netzwerk zugreifen. Für Testzwecke zwischen zwei Vista-Clients könnten Sie zum Beispiel die Datei- und Druckerfreigabe auswählen (Abbildung 15.140).

Abbildg. 15.140 Festlegen des Regeltyps für eingehende Firewallregeln



4. Auf der nächsten Seite des Assistenten können Sie Ihre Auswahl weiter spezifizieren. Hier können Sie ruhig alle Optionen ausgewählt lassen, damit der notwendige Datenverkehr für die Datei- und Druckerfreigabe zwischen sicheren Clients zugelassen wird (Abbildung 15.141).

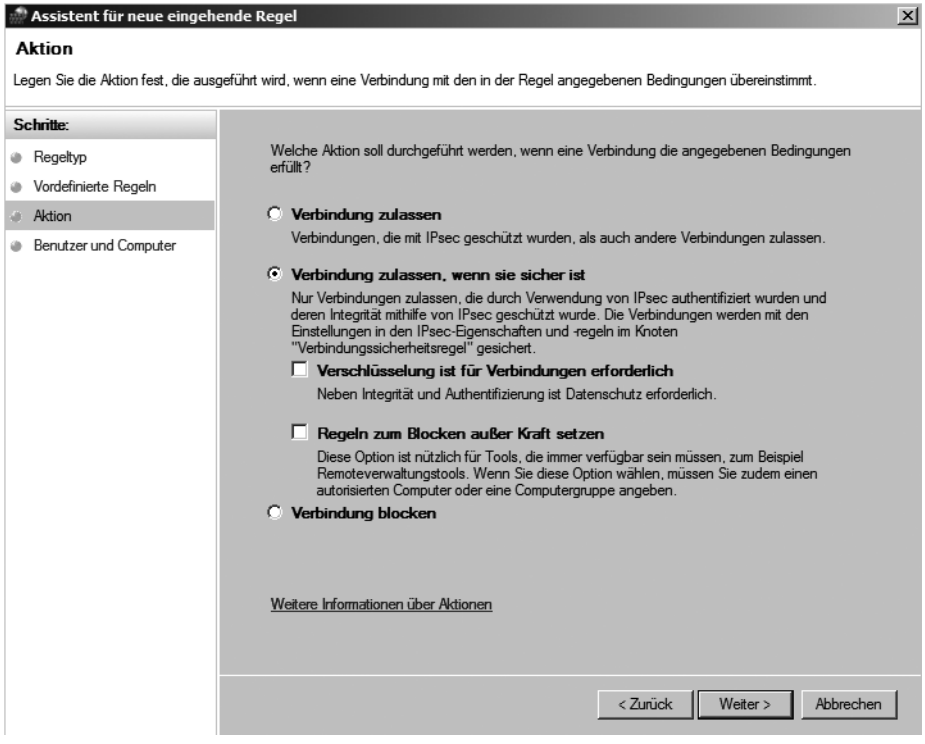
Abbildg. 15.141 Festlegen und auswählen von Standardregeln für die ausgewählte Funktion



5. Auf der nächsten Seite legen Sie fest, welche Aktion die Firewall durchführen soll, abhängig von der Authentifizierung des Clients, von dem die Anfrage kommt. Aktivieren Sie hier die Option *Verbindung zulassen, wenn sie sicher ist.* Dadurch legen Sie fest, dass nur durch IPSec geschützte Verbindungen zugelassen sind. Diese Einstellungen sind in der Verbindungssicherheitsregel definiert. Wählen Sie diese Option aus, wird dem Assistenten automatisch die Seite *Benutzer und Computer* hinzugefügt. Auf dieser Seite können Sie die Benutzer oder Computer angeben, denen Sie Zugriff gewähren möchten. Mit der Option *Verbindung zulassen* können Sie eine Verbindung zulassen, die alle angegebenen Kriterien erfüllt. Bei dieser Option werden Verbindungen ohne Rücksicht darauf zugelassen, ob sie gemäß einer Verbindungssicherheitsrichtlinie mithilfe von IPSec geschützt sind. Über das Kontrollkästchen *Verschlüsselung ist für Verbindungen erforderlich* legen Sie fest, dass die Kommunikation die Datenverschlüsselung gemäß der Definition in einer Verbindungssicherheitsregel verwenden muss. Mit dem Kontrollkästchen *Regeln zum Blocken außer Kraft setzen* lassen Sie alle Verbindungen zu, die mit dieser Firewallregel übereinstimmen, und überschreiben alle Firewallregeln, die sie blockieren würden. Verwenden Sie diese Option, wird die Verbindung auch dann zugelassen, wenn sie von einer anderen Regel blockiert wird. Wenn Sie *Eingehende Verbindungen* auf *Alle Verbindungen blocken* unter *Status* im Dialogfeld *Eigenschaften der Windows-Firewall mit erweiterter Sicherheit* festgelegt haben, werden die Verbindungen unabhängig von den Einstellungen dieser Option trotzdem blockiert.

Mit der Option *Verbindung blocken* blockieren Sie die Kommunikation. Das Blockieren hat Vorrang vor dem Zulassen, sofern Sie beim Erstellen der Firewallregel nicht die Option *Regeln zum Blocken außer Kraft setzen* aktivieren.

Abbildg. 15.142 Festlegen der Firewall-Aktion für die eingehende Verbindungsregel



Testen der Verbindung von NAP über IPSec

Nachdem Sie sichergestellt haben, dass die Computerkonten der Clients, mit denen Sie diese Einstellungen testen, in der OU liegen, für die Sie die Gruppenrichtlinie mit den Regeln definiert haben, können Sie versuchen, ob Sie eine Verbindung zu einer Freigabe auf den anderen Client erstellen können. Hierzu können Sie zum Beispiel *net use * \\<PC-Name\c$* verwenden. Entsprechen die Clients den Sicherheitseinstellungen und sind konform zur NAP-Richtlinie, sollte sich die Verbindung öffnen lassen.

Um die konfigurierte Sicherheitsinfrastruktur basierend auf NAP und IPsec weiter zu testen, können Sie in der Verwaltung des NAP-Servers zum Beispiel noch für die Windows-Sicherheitsintegritätsverifizierung sicherstellen, dass neben der aktivierten Firewall auch Windows-Updates installiert sein müssen. Aktivieren Sie diese Option, werden Clients, die keine automatischen Updates verwenden, zu nicht-konformen Clients erklärt.

Anschließend können Sie die Eigenschaften für die Netzwerkrichtlinie für nicht-konforme Clients öffnen. Hier haben Sie konfiguriert, dass Clients, die nicht den NAP-Richtlinien entsprechen, automatisch gewartet werden. In diesem Fall würden also bei diesen Clients sowohl die Windows-Firewall als auch die automatischen Updates aktiviert werden. Anschließend würde der NAP-Agent auf dem Client den neuen Status zum NAP-Server übermitteln, der dann wiederum den Client zum NAP-konformen Client erklären würde. Um das zu verhindern, wenn Sie zum Beispiel testen wollen was passiert, wenn ein Client nicht NAP-konform ist und auch nicht gewartet wird, können Sie die automatische Wartung in der Netzwerkrichtlinie für nicht-NAP-konforme Clients deaktivieren. Stellen Sie anschließend sicher, dass auf den Client die automatischen Updates in der Systemsteuerung deaktiviert werden. Die Verbindung zwischen den Clients wird dadurch unterbrochen.

802.1x und der Netzwerkzugriffsschutz (NAP)

Mithilfe der *802.1X-Erzwingung* weist ein Netzwerkrichtlinienserver (Network Policy Server, NPS) einen 802.1X-basierten Zugriffspunkt (ein Ethernet-Switch oder ein drahtloser Zugriffspunkt) an, für den 802.1X-Client so lange ein eingeschränktes Zugriffsprofil zu verwenden. Die 802.1X-Erzwingung bietet einen sicheren eingeschränkten Netzwerkzugriff für alle Computer, die auf das Netzwerk über eine 802.1X-Verbindung zugreifen. Unterstützen die Switches in Ihrem Netzwerk 802.1x, besteht die Möglichkeit, dass nicht-konforme NAP-Clients in spezielle VLANs verschobene werden, bevor diese Zugriff auf das Netzwerk erhalten. Damit Sie NAP in einer 802.1x-konformen Umgebung testen können, sollten Sie sicherstellen, dass Ihre Switch diese Umgebung unterstützt und das Anlegen von virtuellen LANs ermöglicht. Abhängig von den NAP-Richtlinien unter Windows Server 2008 weist ein 802.1x-kompatibler-Switch die Clients den entsprechenden VLANs zu. Um die Umgebung optimal testen zu können, sollten Sie mindestens drei VLANs einrichten. Ein VLAN sollte für die Clients im Netzwerk verwendet werden, für die Sie kein NAP verwenden wollen, ein VLAN sollte für NAP-konforme Clients verwendet werden und ein VLAN für nicht-konforme NAP-Clients. Zwischen den VLANs für NAP-konforme und nicht-NAP-konforme Clients sollte kein Routing eingerichtet werden, damit nicht-NAP-konforme Clients vom Netzwerk separiert werden.

HINWEIS Wollen Sie den Netzwerkzugriffsschutz in einer 802.1x-Umgebung einsetzen, müssen Sie sicherstellen, dass die Domänenfunktionsebene der beteiligten Clients auf Windows Server 2003, besser auf Windows Server 2008, gesetzt wird.

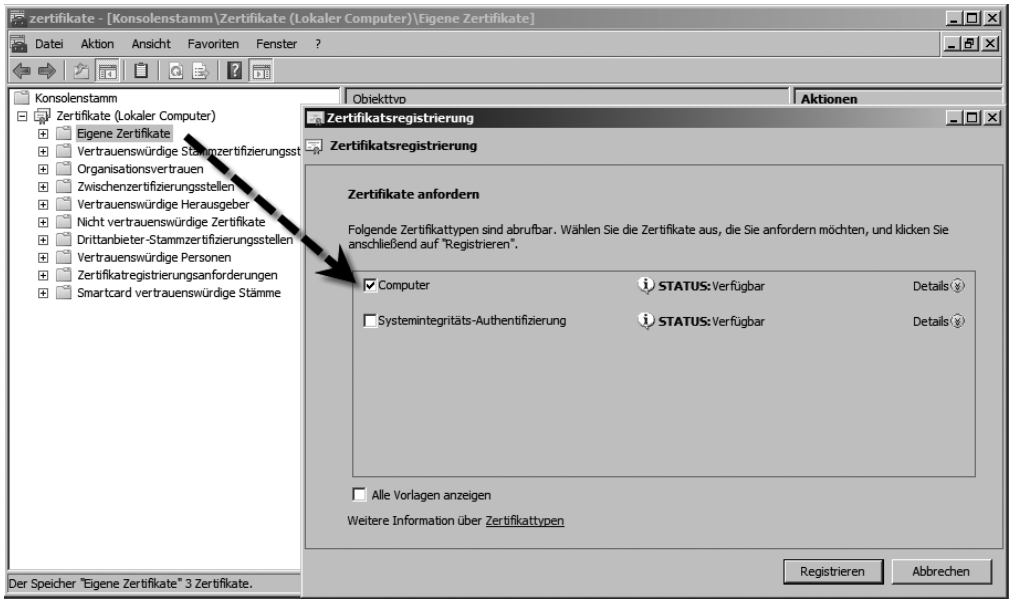
Vorbereitungen für einen 802.1x-Infrastruktur mit Netzwerkzugriffsschutz

Damit Sie diese Infrastruktur aufbauen können, muss sich in der Domäne wieder eine Zertifizierungsstelle befinden, deren Installation bereits beschrieben worden ist. Zusätzlich benötigen Sie einen Netzwerkrichtlinienserver, dem Sie auch ein Computerzertifikat zuweisen müssen:

1. Öffnen Sie über *Start/Ausführen/mmc* eine neue Konsole.
2. Fügen Sie das Snap-In *Zertifikate* zu dieser Konsole hinzu.
3. Wählen Sie als Option für den *Zertifikatespeicher* des Snap-Ins *Computerkonto* aus.
4. Wählen Sie den lokalen Computer aus.

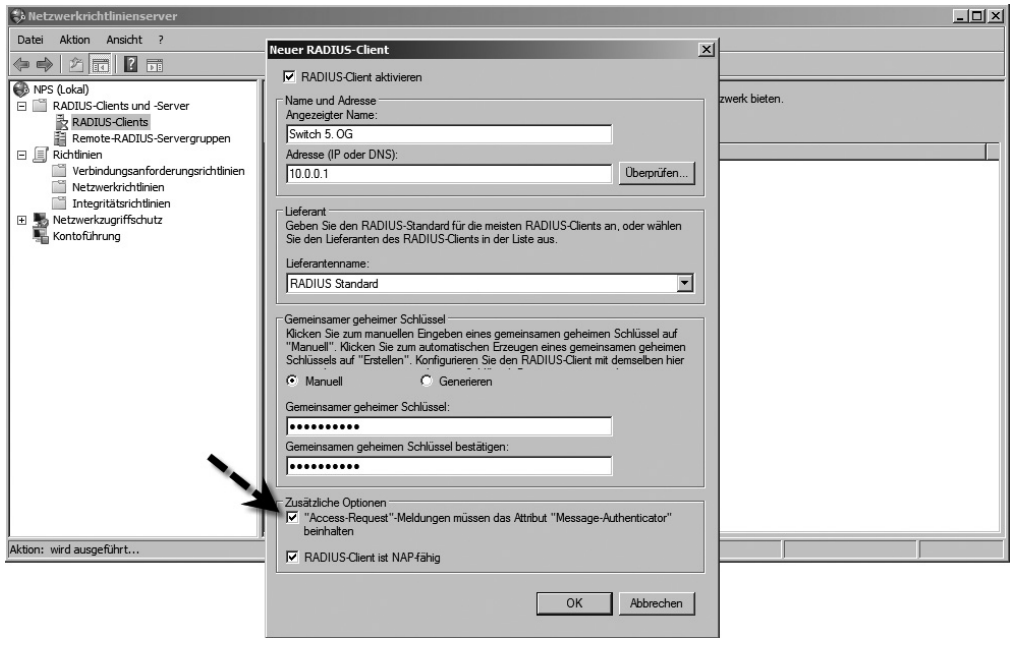
5. Klicken Sie im Snap-In mit der rechten Maustaste auf *Eigene Zertifikate* und wählen Sie im Kontextmenü den Eintrag *Alle Aufgaben/Neues Zertifikat anfordern* aus (Abbildung 15.143).
6. Wählen Sie ein Zertifikat mit der Bezeichnung *Computer* aus.

Abbildg. 15.143 Registrieren eines Computer-Zertifikats für den Netzwerkrichtlinienserver



HINWEIS Bauen Sie eine 802.1x-Infrastruktur für den Netzwerkzugriffsschutz auf, wird der 802.1x-kompatible Switch in der Verwaltungskonsole des Netzwerkrichtlinienservers als RADIUS-Client hinterlegt. Diese Konfiguration wurde bereits bei der Einrichtung von NAP über VPN weiter vorne in diesem Kapitel erläutert. Wichtig bei der Konfiguration eines 802.1x-Switches als RADIUS-Client ist, dass Sie die beiden Optionen *"Access-Request"-Meldungen müssen das Attribut "Message Authenticator" beinhalten* und *RADIUS-Client ist NAP-fähig* definieren. Falls eine eingehende Access-Request-RADIUS-Meldung nicht von mindestens einer der IP-Adressen von konfigurierten Clients stammt, verwirft der NPS die Meldung automatisch. Dadurch wird der Server geschützt. Als Schutz vor der Manipulation von Access-Request- und RADIUS-Meldungen kann jede RADIUS-Meldung zusätzlich mit dem *Message Authenticator-RADIUS-Attribut* geschützt werden. Das Attribut ist ein Message Digest 5 (MD5)-Hash der gesamten RADIUS-Meldung. Zum Verschlüsseln wird der gemeinsame geheime Schlüssel verwendet. Schlägt die Überprüfung fehl, wird die RADIUS-Meldung verworfen.

Abbildg. 15.144 Konfigurieren eines 802.1x-Switch als RADIUS-Client

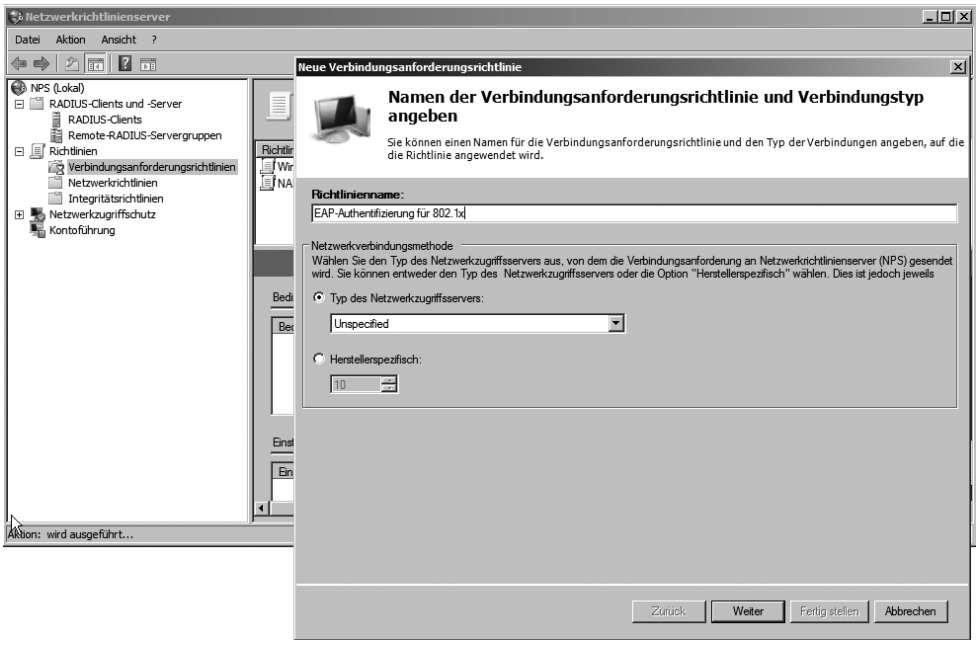


Erstellen der Verbindungsanforderungsrichtlinie

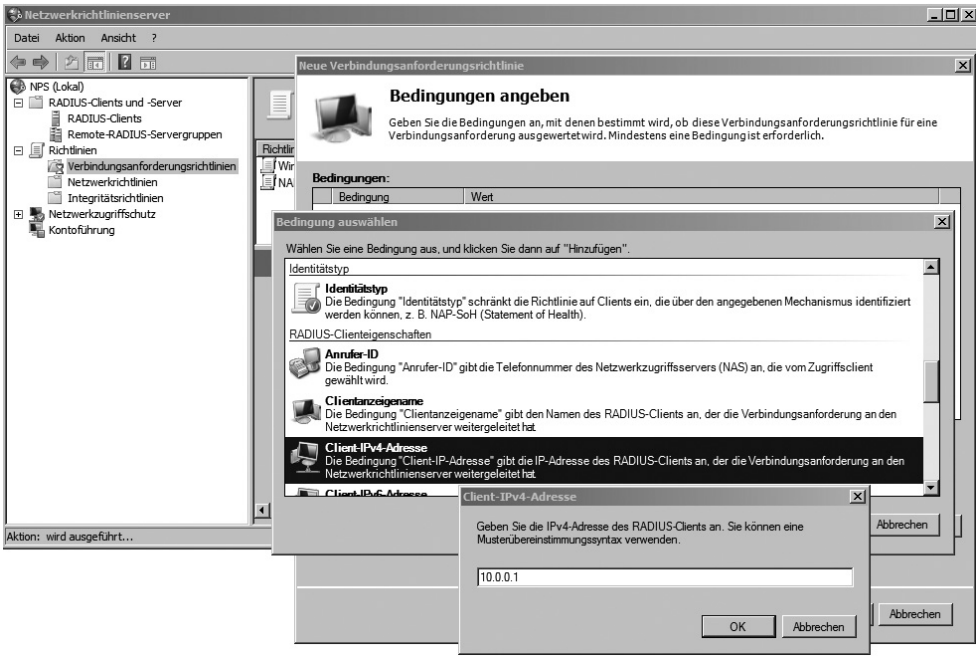
Für die Verwendung von NAP für 802.1x werden Verbindungsanforderungsrichtlinien (Connection Request Policies, CRPs) benötigt. Diese konfigurieren Sie über die NPS-Konsole, indem Sie im Bereich *Richtlinien* auf den Eintrag *Verbindungsanforderungsrichtlinien* klicken. Gehen Sie zur Konfiguration einer CRP wie folgt vor:

1. Deaktivieren Sie zunächst die Standardrichtlinien.
2. Erstellen Sie eine neue Richtlinie, indem Sie mit der rechten Maustaste auf *Verbindungsanforderungsrichtlinien* klicken und *Neu* wählen.
3. Geben Sie der Richtlinie einen passenden Namen, zum Beispiel *EAP-Authentifizierung für 802.1x*.
4. Klicken Sie auf *Weiter*.
5. Auf der nächsten Seite *Bedingungen* klicken Sie auf *Hinzufügen* und wählen die Option *Client-IPv4-Adresse* aus. Hinterlegen Sie als Wert die IP-Adresse des 802.1x-Netzwerkswitch. Diese Option bestimmt, von welchem RADIUS-Client die Anforderungen kommen. Da der RADIUS-Client bei dieser Konstellation 802.1x-Switch ist, müssen Sie diese IP-Adresse hinterlegen.
6. Auf der nächsten Seite des Assistenten stellen Sie sicher, dass die Option *Anforderungen auf diesem Server authentifizieren* ausgewählt ist.

Abbildg. 15.145 Erstellen einer neuen Verbindungsanforderungsrichtlinie für 802.1x

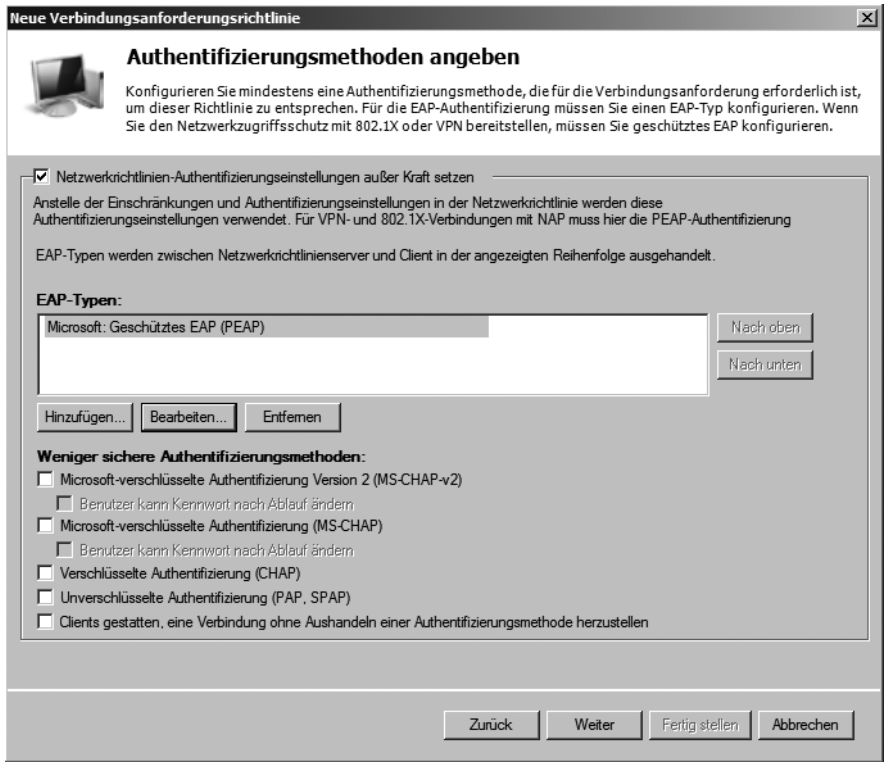


Abbildg. 15.146 Auswählen des 802.1x-Netzwerkswitch als RADIUS-Client



7. Aktivieren Sie auf dem Fenster *Authentifizierungsmethoden angeben* die Option *Netzwerkrichtlinien-Authentifizierungseinstellungen außer Kraft setzen*. Durch diese Auswahl wird die Authentifizierung so verwendet, wie Sie diese in der Verbindungsanforderungsrichtlinie festlegen, unabhängig davon, wie die entsprechenden Netzwerkrichtlinien konfiguriert sind.
8. Klicken Sie im Bereich *EAP-Typen* auf *Hinzufügen*. Wählen Sie *Microsoft: Geschütztes EAP (PEAP)* aus.
9. PEAP verwendet TLS (Transport Level Security), um einen verschlüsselten Kanal zwischen einem authentifizierten PEAP-Client und einem authentifizierenden PEAP-Server zu erstellen. PEAP gibt keine Authentifizierungsmethode an, bietet allerdings zusätzliche Sicherheit für andere EAP-Authentifizierungsprotokolle, z. B. EAP-MSCHAPv2, das den mit TLS verschlüsselten Kanal von PEAP verwenden kann. Zur Optimierung von EAP-Protokollen und Netzwerksicherheit bietet PEAP Schutz der Aushandlung der EAP-Methode, die zwischen Client und Server über einen TLS-Kanal stattfindet. Dies verhindert, dass ein Angreifer Pakete zwischen dem Client und dem Netzwerkzugriffsserver mit dem Ziel einfügt, dass eine nicht so sichere EAP-Methode ausgehandelt wird. Der verschlüsselte TLS-Kanal verhindert außerdem Denial-of-Service-Angriffe auf den Server. Der PEAP-Authentifizierungsvorgang zwischen dem PEAP-Client und dem Authentifizierungsserver besteht aus zwei Phasen. In der ersten Phase wird ein sicherer Kanal zwischen dem PEAP-Client und dem Authentifizierungsserver eingerichtet. In der zweiten Phase wird die EAP-Authentifizierung zwischen dem EAP-Client und dem Authentifizierungsserver durchgeführt.

Abbildg. 15.147 Auswählen und konfigurieren der Authentifizierungsmethode



10. Markieren Sie als Nächstes die Option *Microsoft: Geschütztes EAP (PEAP)* und klicken Sie auf *Bearbeiten*.
11. Stellen Sie sicher, dass die Option *Quarantäneüberprüfungen* aktiviert ist.
12. Wählen Sie das Zertifikat aus, das Sie zuvor für den Server ausgestellt haben.
13. Bestätigen Sie in den restlichen Fenstern die Standardeinstellungen und schließen Sie die Erstellung der Richtlinie ab.

Konfigurieren der Systemintegritätsprüfung und der Integritätsrichtlinien

Als Nächstes konfigurieren Sie in der Verwaltungskonsole für den Netzwerkrichtlinienserver die Systemintegritätsprüfung (System Health Validator, SHV). Die Verwaltung einer 802.1x-Infrastruktur baut auf die *Sicherheitsintegritätsprüfung* auf. Diese ruft von den Clients das *Statement of Health (SoH)* ab:

1. Diese Einstellungen finden Sie in der Verwaltungskonsole über *NPS/Netzwerkzugriffsschutz/Systemintegritätsprüfungen*.
2. Rufen Sie in der Mitte diese Eigenschaften der Verifizierungsmethode auf, zum Beispiel von der standardmäßigen vorhandenen *Windows-Sicherheitsintegritätsverifizierung*.
3. Hier können Sie über die Schaltfläche *Konfigurieren* die Einstellungen festlegen, welche die Clients erfüllen müssen, um mit NAP in Ihrem Netzwerk konform zu sein. Diese Systemintegritätsprüfungen bezeichnet Microsoft auch als *Security Health Agents (SHA)*. Der SHA wird in Windows Vista durch den *Windows Security Health Validator (SHV)* verbunden. Hauptsächlich überprüfen diese SHAs den Zustand des Windows-Sicherheitscenters in Windows Vista und XP.

Nachdem Sie diese Konfiguration vorgenommen haben, erstellen Sie wieder zwei Integritätsrichtlinien, wie bereits im Abschnitt zur Einrichtung von NAP über DHCP besprochen.

Erstellen der Netzwerkrichtlinien

Nachdem Sie die Integritätsrichtlinien erstellt haben, definieren Sie Netzwerkrichtlinien, auf deren Basis die Clients von der Switch in verschiedene VLANs zugeordnet werden, abhängig davon, ob diese NAP-konform sind oder nicht-NAP-konform.

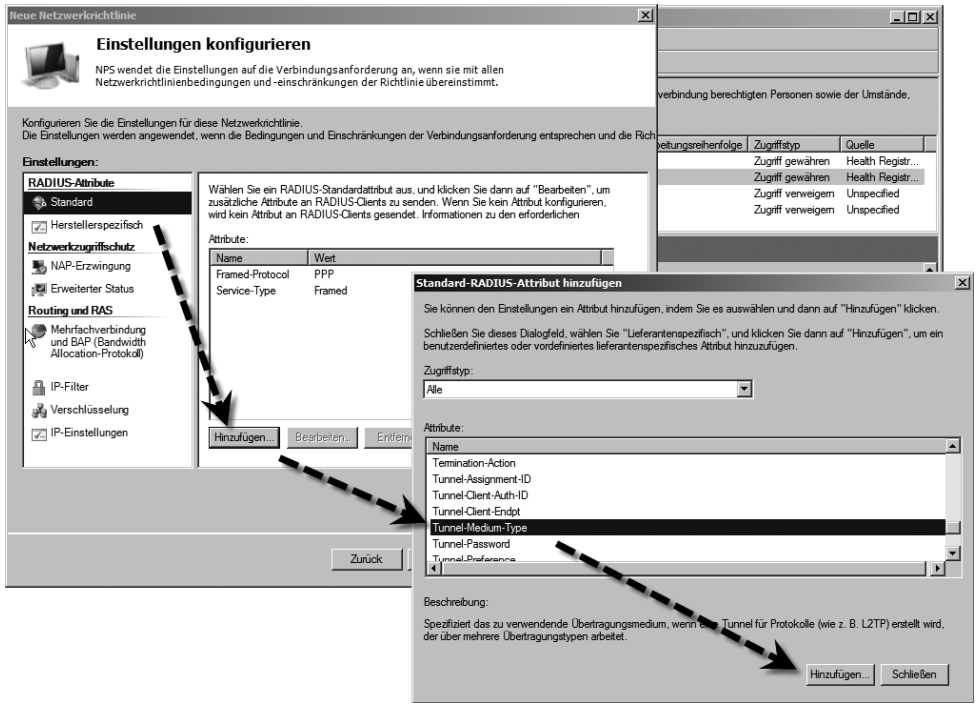
Erstellen der Netzwerkrichtlinie für nicht konforme und konforme NAP-Clients

Als Nächstes erstellen Sie eine Netzwerkrichtlinie, die den Netzwerkzugriff für nicht konforme Clients steuert:

1. Klicken Sie dazu mit der rechten Maustaste auf *Richtlinien/Netzwerkrichtlinien* und wählen Sie *Neu*.
2. Geben Sie der Richtlinie eine Bezeichnung in der Form »Zugriff für nicht konforme NAP-Clients« und klicken Sie auf *Weiter*.
3. Klicken auf der nächsten Seite *Bedingungen angeben* auf *Hinzufügen*.
4. Wählen Sie als Option *Integritätsrichtlinien* aus.

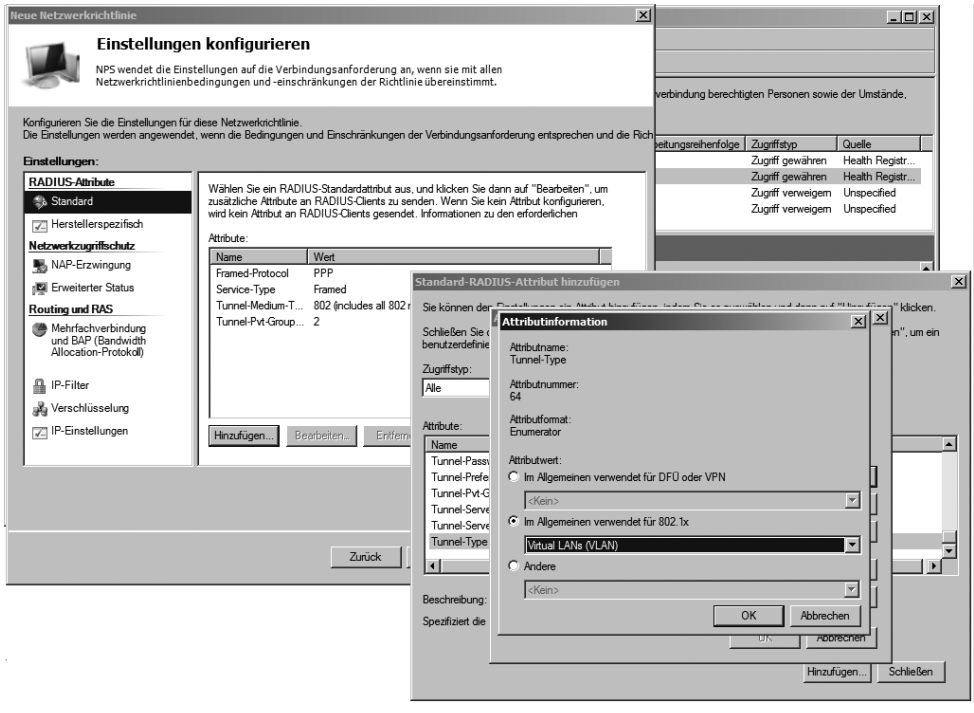
5. Klicken Sie auf *Hinzufügen*.
6. Wählen Sie die Richtlinie *Nicht-NAP-Konform* aus. Bei der Richtlinie für NAP-konforme Clients wählen Sie *NAP-Konform* aus.
7. Auf der nächsten Seite des Fensters legen Sie den Netzwerkzugriff der Richtlinie fest. Wählen Sie hier *Zugriff gewährt* aus.
8. Klicken Sie auf *Weiter*, um zum Fenster *Authentifizierungsmethoden* zu gelangen.
9. Klicken Sie auf *Weiter* und belassen Sie im nächsten Fenster alle Einstellungen wie sie sind. In diesem Fenster legen Sie die Einschränkungen fest.
10. Klicken Sie im Fenster *Einschränkungen* ebenfalls wieder auf *Weiter*. Sie gelangen auf das Fenster *Einstellungen konfigurieren*.
11. Klicken Sie hier auf *NAP-Erzwingung* und stellen Sie sicher, dass die Option *Eingeschränkten Zugriff gewähren* aktiviert ist. Bei NAP-konformen Clients gewähren Sie vollen Zugriff.
12. Aktivieren Sie die Option *Automatische Wartung von Clientcomputern aktivieren*.
13. Klicken Sie im Bereich *RADIUS-Einstellungen* (oben links auf dem Fenster) auf *Standard*.
14. Klicken Sie auf *Hinzufügen*.
15. Wählen Sie *Tunnel-Medium-Type* aus und klicken Sie auf *Hinzufügen*.
16. Klicken Sie auf *Hinzufügen* und im neu geöffneten Fenster *Attributinformationen* ebenfalls auf *Hinzufügen*. Wählen Sie *802 (includes all 802 media plus Ethernet canonical format)* aus.

Abbildg. 15.148 Hinzufügen eines neuen Tunnel-Medium-Typs



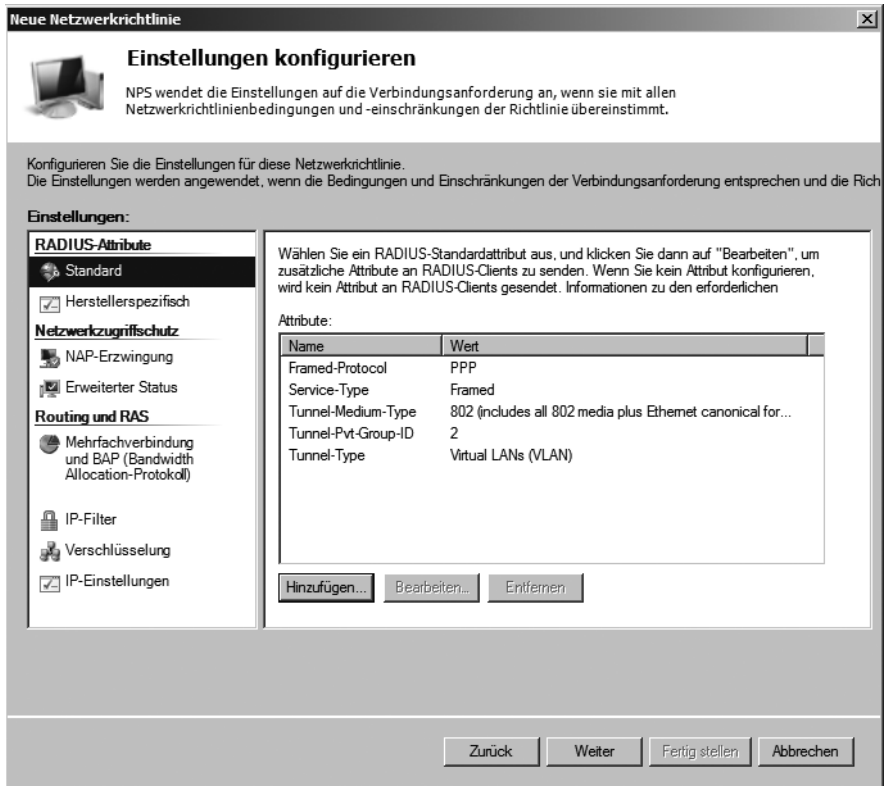
17. Fügen Sie als Nächstes die Option *Tunnel-Pvt-Group-ID* hinzu.
18. Fügen Sie dieses Mal das Attribut *2* hinzu. Bei diesem Attribut sollte es sich bei Ihnen um das Attribut des VLANs auf der Switch handeln, mit der die nicht konformen Clients verbunden werden. Für NAP-konforme Clients verwenden Sie die ID 3. Die ID 1 auf der Switch sollten Sie für Clients verwenden, die durch die NAP-Prüfung nicht betroffen sind.
19. Fügen Sie als Nächstes die Option *Tunnel-Type* hinzu.
20. Wählen Sie bei dieser Option die Attributinformation *Im Allgemeinen verwendet für 802.1x* aus und stellen Sie sicher, dass im Listenfeld der Eintrag *Virtual LANs (VLAN)* ausgewählt wurde.

Abbildg. 15.149 Konfigurieren von Attributinformationen für NAP über 802.1x



21. Nachdem Sie Eintragungen vorgenommen haben, sollten alle Attribute angezeigt werden.
22. Klicken Sie anschließend im Fenster auf die Option *Herstellerspezifisch*.
23. Wählen Sie das Attribut *Tunnel-Tag* aus und weisen Sie diesem den Wert *1* zu. Diese Einstellung kann aber für manche Switches unterschiedlich sein. Fragen Sie beim Hersteller Ihrer Switch nach, ob Sie einen anderen *Tunnel-Tag* eintragen müssen.
24. Schließen Sie die Erstellung der Netzwerkrichtlinie ab. Diese werden nach der Erstellung in der NPS-Konsole angezeigt. Alle anderen Richtlinien sollten als deaktiviert angezeigt werden.

Abbildg. 15.150 Abschließen der Konfiguration für die Netzwerkrichtlinie für Nicht-NAP-konforme Clients



Client für 802.1x konfigurieren

Auf dem Client sollten Sie Windows Vista oder Windows XP mit SP2 und installiertem NAP-Client installieren und den Client in die Domäne aufnehmen.

NAP-Agent und Automatische Konfiguration (verkabelt) aktivieren

Der nächste Schritt zur Anbindung von Windows Vista an eine NAP-Infrastruktur ist die Aktivierung des Systemdienstes *NAP-Agent (Network Access Protection)*. Setzen Sie den Starttyp dieses Dienstes auf *Automatisch* und starten Sie diesen. Anschließend führen Sie die gleiche Aktion noch für den Dienst *Automatische Konfiguration (verkabelt)* durch.

Aktivieren des Sicherheitscenters auf Windows Vista-Domänen-PCs

Auf Windows Vista-PCs, die Mitglied einer Domäne sind, wird das Sicherheitscenter deaktiviert. Um NAP unter Windows Vista zu testen, müssen Sie dieses daher aktivieren. Gehen Sie dazu folgendermaßen vor:

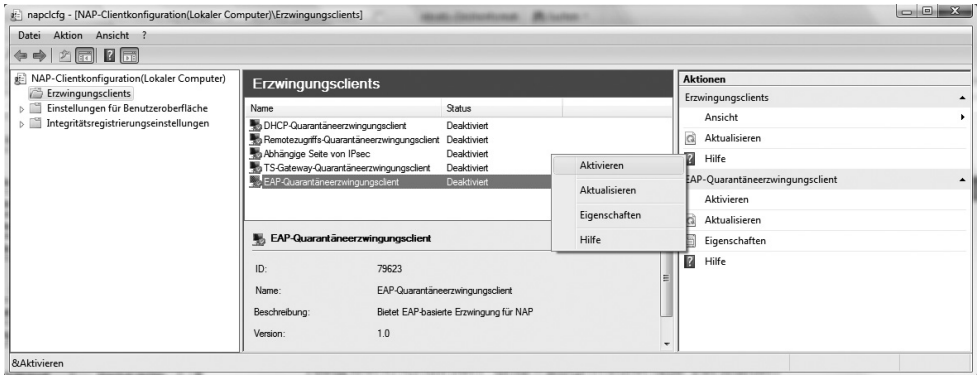
1. Geben Sie über *Start/Ausführen/gpedit.msc* ein.
2. Navigieren Sie zu *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Sicherheitscenter*.
3. Aktivieren Sie die Richtlinie *Sicherheitscenter aktivieren (nur Domänencomputer)*.

Aktivieren des EAP-Quarantäneerzwingungsclients

Die nächste Aufgabe, die Sie durchführen müssen, ist die Aktivierung der EAP-NAP-Unterstützung:

1. Starten Sie dazu auf dem Vista-PC über *Start/Ausführen/napclcfg.msc* die Verwaltungskonsole des NAP-Clients (Abbildung 15.151).
2. Klicken Sie auf *Erzwingungsclients*.
3. Aktivieren Sie den Eintrag *EAP-Quarantäneerzwingungsclient*.

Abbildg. 15.151 Aktivieren des EAP-Quarantäneerzwingungsclients unter Windows Vista



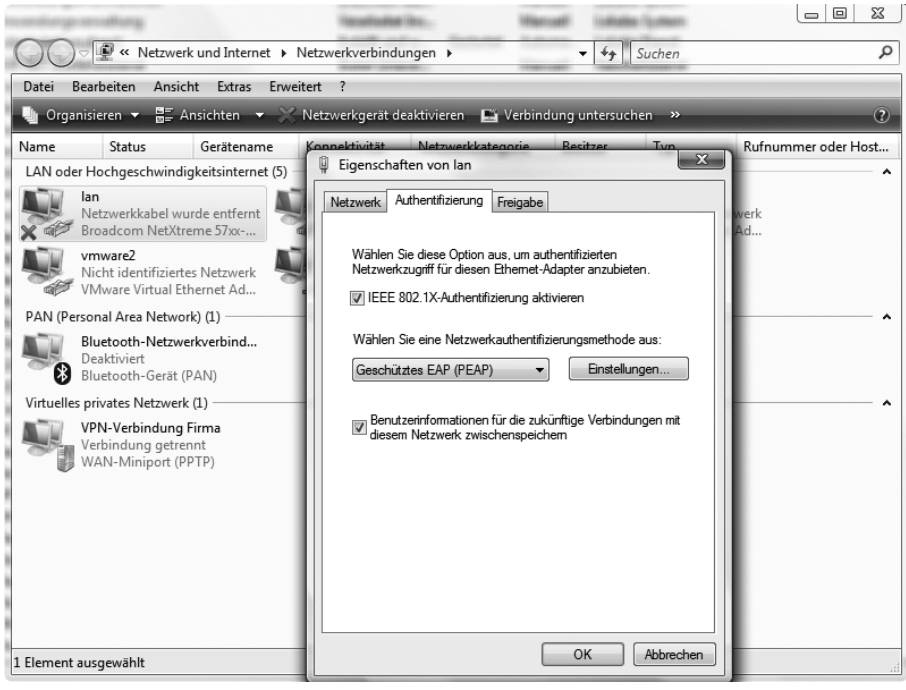
Alternativ können Sie Erzwingungsclients für den Netzwerkzugriffsschutz auch über Gruppenrichtlinien aktivieren. Diese Einstellung finden Sie unter *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Network Access Protection/NAP-Clientkonfiguration/Erzwingungsclients*.

Konfiguration der Authentifizierung

Als Nächstes rufen Sie die Eigenschaften der LAN-Verbindung auf und wechseln zur Registerkarte *Authentifizierung*.:

1. Schalten Sie das Kontrollkästchen *IEEE 802.1X-Authentifizierung aktivieren* ein.
2. Klicken Sie auf *Einstellungen* und stellen Sie sicher, dass auf dem Konfigurationsfenster die Option *Serverzertifikat überprüfen* aktiviert ist. Auch die Option *Quarantäneüberprüfungen aktivieren* sollten Sie einschalten.
3. Klicken Sie auf *Konfigurieren* und stellen Sie sicher, dass das Kontrollkästchen *Automatisch eigenen Windows-Anmeldenamen und Kennwort (…) verwenden* aktiviert ist.
4. Starten Sie anschließend den PC neu.

Abbildg. 15.152 Aktivieren der Authentifizierung für die LAN-Verbindung



Abbildg. 15.153 Sicherstellen der Authentifizierung für 802.1x

Anschließend können Sie die Konfiguration überprüfen, indem Sie testen, in welche VLANs die Clients von der Switch verschoben werden, abhängig davon, ob diese NAP-konform sind oder nicht.

Zusammenfassung

In diesem Kapitel haben Sie gelernt, wie Sie mit dem Netzwerkzugriffsschutz bereits mit einem einzelnen Windows Server 2008-Computer im Netzwerk Arbeitsstationen unter Windows XP und Windows Vista vor der Verbindung abprüfen können. Diese neue Sicherheitsfunktion ist vor allem für Unternehmen interessant, die Außendienstmitarbeiter über ein Terminaldienstegateway anbinden oder die eine hochsichere Umgebung zur Verfügung stellen wollen. Im nächsten Kapitel gehen wir darauf ein, wie Arbeitsstationen, aber auch die Server selbst, automatisiert und genormt mit kostenlosen Bordmitteln installiert werden.

Kapitel 16

Windows-Bereitstellungsdienste

In diesem Kapitel:

Mit der Fertigstellung von Windows Vista hat Microsoft auch zahlreiche Technologien zur Verfügung gestellt, wie das neue Betriebssystem in Unternehmen verteilt werden kann. Eine dieser Technologien, die Windows-Bereitstellungsdienste (Windows Deployment Services, WDS), stehen sowohl für Windows Server 2003 als auch für Windows Server 2008 zur Verfügung. Mit den WDS ist die Verteilung von Windows im Unternehmen einfach und effizient möglich. In diesem Kapitel zeigen wir Ihnen die mögliche Bereitstellung von Windows Vista in Unternehmen.

Grundlagen zur automatisierten Installation von Windows Vista und Windows Server 2008

Um Windows Vista und Windows Server 2008 in Unternehmen zu verteilen, unterstützt Microsoft Administratoren mit dem *Windows Automated Installation Kit (WAIK)*. WAIK ist optimiert für Windows Vista und Windows Server 2008 und enthält zahlreiche Tools, welche die Installation von Windows Vista und Windows Server 2008 deutlich optimieren. Mit dem WAIK sollen tausende Rechner automatisiert installiert werden können, der Aufwand der Verteilung ist daher deutlich reduziert worden. Neue Hotfixes können extrem einfach in bestehende Images integriert werden. Sie können das WAIK von der Internetseite *http://www.microsoft.com/downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=de* kostenlos herunterladen. Alternativ suchen Sie in einer Suchmaschine nach den Begriffen *WAIK* und *Download*. Die Dateigröße beträgt in etwa 1,2 GB. Ein weiteres Hilfsmittel zur automatisierten Installation ist das Business Desktop Deplyoment 2007 (BDD 2007). Das BDD 2007 können Sie von der Internetseite *http://www.microsoft.com/downloads/details.aspx?FamilyID=13f05be2-fd0e-4620-8ca6-1aad6fc54741&DisplayLang=en* ebenfalls kostenlos herunterladen. Der Download beträgt in etwa zwischen 30 und 50 MB. Wer zum großen Teil auf Windows Server 2008 und Windows Vista im Unternehmen setzt, kann den Nachfolger des BDD 2007 mit der Bezeichnung *Microsoft Deployment Toolkit (MDT) 2008* von der Seite *http://www.microsoft.com/downloads/details.aspx?familyid=3BD8561F-77AC-4400-A0C1-FE871C461A89&displaylang=en* herunterladen. Grundsätzlich gibt es zwei Möglichkeiten, Windows Vista automatisiert zu installieren:

Sie installieren Windows Vista über die DVD und die Datei *Setup.exe* auf der DVD, der Sie auch eine Antwortdatei auf XML-Basis mitgeben können. Die Installation von Windows Vista von DVD basiert ebenfalls auf einem WIM-Image.

Alternativ können Sie ein Image mit *ImageX*, einer installierten Windows Vista-Edition über die *Windows-Bereitstellungsdienste (Windows Deployment Services, WDS)* oder einer Netzwerkfreigabe auf PCs im Unternehmen verteilen. Die einzelnen Windows-Komponenten sind einzeln installierbar und beschreiben in XML-Dateien deren Installationsabläufe und Abhängigkeiten. Durch diese XML-basierte Steuerung der Installation wird die Verteilung deutlich flexibler gestaltet.

Es würde den Rahmen dieses Buches sprengen, eine komplette Rollout-Strategie darzustellen bzw. den allumfassenden Umgang mit den Werkzeugen zu erklären. Wir erläutern jedoch alle relevanten Werkzeuge und zeigen Ihnen die wichtigsten Möglichkeiten, wie sich die Installation von Windows Vista automatisieren lässt.

Abbildg. 16.1 Das Windows Automated Installation Kit kann auch für die automatisierte Installation von Windows Server 2008 verwendet werden

Notwendige Funktionen für die automatisierte Installation

In Windows Vista und Windows Server 2008 werden einige Tools, die auch unter Windows XP und Windows Server 2003 im Einsatz sind, weiterverwendet. Zusätzlich gibt es neue Tools und Funktionen, einige Funktionen sind jedoch weggefallen. Im folgenden Abschnitt gehen wir mit Ihnen eine Kurzbeschreibung der notwendigen Tools durch. Außerdem gehen wir auch kurz auf die Programme und Tools ein, die nicht mehr verwendet werden müssen. Alle benötigten Tools gehören entweder zu den Bordmitteln von Windows Vista und Windows Server 2008, zum WAIK, BDD 2007 oder zum MDT 2008.

HINWEIS Bei Windows XP und Windows Server 2003 verhinderten technische Einschränkungen die Erstellung eines einzigen Image, das auf allen Computern bereitgestellt werden konnte. Unterschiedliche HAL-Schichten (Hardware Abstraction Layer) bedeuteten, dass Sie mehrere Images pflegen mussten. In Windows Vista bestehen diese technischen Einschränkungen nicht mehr; das Betriebssystem ist in der Lage, die benötigte HAL festzustellen und sie automatisch zu installieren.

- **SYSPREP** Dies ist die aktualisierte, für Windows Vista und Windows Server 2008 abgeänderte Version
- **SETUP** Ein neues Installationsprogramm für Windows Vista Windows Server 2008, das WINNT und WINNT32 ersetzt
- **IMAGEX** Das neue Befehlszeilentool zur Erstellung von WIM-Images
- **Windows System Image Manager** Ein Tool zum Erstellen und Ändern von *unattend.xml*-Dateien

- **PEIMG** Das Tool zur Anpassung von Windows PE 2.0-Images
- **Windows Deployment Services** Die neue Version von RIS, mit der die Bereitstellung von Windows Vista Windows Server 2008 – und Windows XP-Images sowie Windows PE 2.0-Startimages ermöglicht wird
- **PNPUTIL** Mit diesem neuen Tool können Treiber dem Treiberspeicher von Windows Vista Windows Server 2008 hinzugefügt sowie daraus entfernt werden
- **PKGMGR** Dieses ebenfalls neue Windows Vista und Windows Server 2008 -Tool dient zur Wartung des Betriebssystems. Der Paket-Manager ist ein Befehlszeilen-Tool, mit dem Sie Windows-Pakete offline bearbeiten können.
- **OCSETUP** Dieses Hilfsprogramm ersetzt *SYSOCMGR* und dient zur Installation von Windows-Komponenten
- **BCDEDIT** Ein neues Tool von Windows Vista und Windows Server 2008 zum Bearbeiten von Startkonfigurationsdaten
- **Application Compatibility Toolkit 5.0** Mit diesem aktualisierten Tool können Sie feststellen, ob Ihre Anwendungen mit Windows Vista und Windows Server 2008 kompatibel sind
- **User State Migration Tool 3.01** Ein aktualisiertes Tool zum Erfassen und Wiederherstellen von Benutzereinstellungen, das in Windows XP und Windows Vista sowie allen Version von Office einschließlich Office 2007 eingesetzt werden kann

Nicht mehr verwendete Tools

Nachfolgend sind jene Tools aufgelistet, die für das Deployment von Windows Vista und Windows Server 2008 nicht mehr benötigt werden:

- **Remote Installation Services** RIS wurde durch die Windows Deployment Services (WDS) ersetzt, bietet unter Windows Server 2003 jedoch noch Legacy-Unterstützung; RIPREP und RISETUP können bei Windows Vista und Windows Server 2008 nicht verwendet werden
- **Setup Manager/Notepad** Verwenden Sie zum Bearbeiten der Konfigurationsdateien für die unbeaufsichtigte Installation stattdessen Windows System Image Manager
- **WINNT.EXE und WINNT32.EXE** Verwenden Sie stattdessen *Setup.exe*
- **SYSOCMGR** Ersetzt durch OCSETUP, PKGMGR
- **MS-DOS-Startdisketten** Nicht mehr nötig. Verwenden Sie Windows PE.

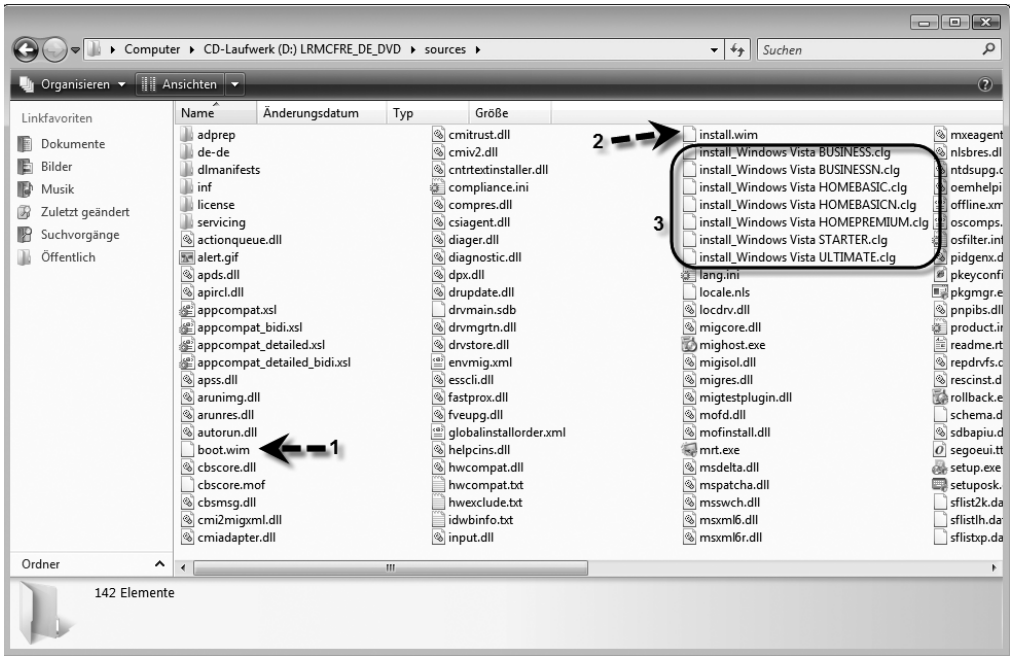
Windows Systemabbild-Manager, Antwortdateien und Kataloge

Windows Systemabbild-Manager (Windows System Image Manager, Windows-SIM) ist ein Tool, mit dem einfach Antwortdateien auf XML-Basis erstellt werden. Auch Netzwerkfreigaben können so konfiguriert werden, dass diese Konfigurationen zur Verteilung von Windows Vista und Windows Server 2008 enthalten. Mit Windows-SIM kann auf einem Computer eine Antwortdatei auf XML-Basis erstellt werden, auf deren Basis wiederum ein Installationsimage angefertigt werden kann. Dieses Image kann entweder über Netzwerkfreigaben auf Ziel-Computern installiert oder durch die Windows Deployment Services (WDS) im Unternehmen verteilt werden. Die Antwortdatei enthält das Grundgerüst, das für die einzelnen Konfigurationsphasen benötigt wird. Dadurch lassen sich

Eingaben wie PC-Namen, Seriennummer und weitere Eingaben in einer Datei vorgeben, sodass während der Installation keinerlei Eingaben mehr erfolgen müssen.

Die Katalogdatei eines Images *(*.clg)* enthält die Einstellungen und Pakete, die in einem Image auf WIM-Basis enthalten sind. Da auch die normale Installation von Windows Vista und Windows Server 2008 auf einem WIM-Image basieren, finden Sie auf der Vista- und Windows Server 2008-Installations-DVD im Verzeichnis *sources* die **.clg*-Dateien der verschiedenen Windows-Editionen (Abbildung 16.2). WIM-Images haben als Dateityp die Bezeichnung **.wim*. Im Verzeichnis befindet sich das Windows PE-Image, das für die Installation und die Computerreparaturoptionen verwendet wird (Punkt 1), das Standard-Image *install.wim* (Punkt 2) und die verschiedenen Katalogdateien (Punkt 3).

Abbildg. 16.2 Im Verzeichnis *sources* auf der Windows Vista- und Windows Server 2008-DVD finden sich alle Komponenten zur automatisierten Installation

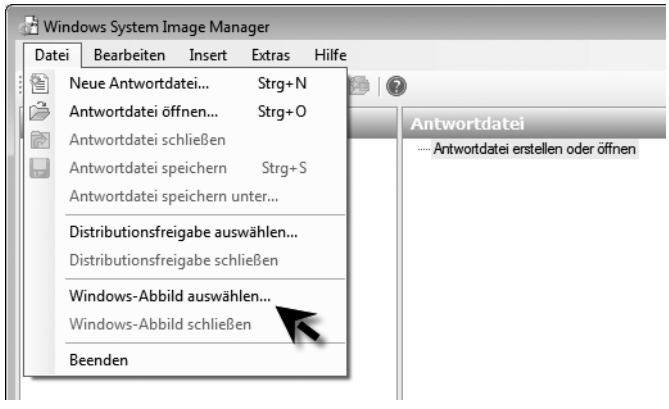


In diesen Dateien ist festgelegt, welche Komponenten von Windows Vista und Windows Server 2008 bei den einzelnen Vista-Editionen installiert werden. Um eine Antwortdatei zu erstellen, wird normalerweise folgendermaßen vorgegangen:

1. Um eine Antwortdatei zu erstellen, sollten Sie die folgenden Vorgänge idealerweise auf einem Admin-PC durchführen, auf dem Sie das Windows Automated Installation Kit (WAIK) installiert haben.
2. Kopieren Sie auf diesem Admin-PC die Datei *install.wim* von der Windows Vista- oder Windows Server 2008-DVD aus dem Verzeichnis *sources* in ein temporäres Verzeichnis auf der Festplatte, zum Beispiel *c:\unattend*. Auf Basis der Standardinstallation lassen sich am besten Antwortdateien erstellen. Diese Datei enthält das Windows Vista-Standardimage mit einer Größe von etwa 2,3 GB.

3. Starten Sie über *Start/Alle Programme/Microsoft Windows AIK* den *Windows Systemabbild-Manager*.
4. Zunächst wird mit Windows-SIM eine Antwortdatei auf XML-Basis erstellt. Öffnen Sie dazu im Image Manager über den Menübefehl *Datei/Windows-Abbild auswählen* die zuvor kopierte Datei *install.wim* (Abbildung 16.3).

Abbildg. 16.3 Öffnen eines Image mit dem Windows Systemabbild-Manager



5. Wählen Sie aus, welche Windows Vista- oder Windows Server 2008-Edition Sie innerhalb des Image verwenden wollen. Beachten Sie, dass Sie über entsprechende Lizenzen dieser Edition verfügen müssen.
6. Nach dem erfolgreiche Ladevorgang wird das Image im Image Manager angezeigt und Sie können sich durch die einzelnen Funktionen und Pakete klicken.
7. Anschließend starten Sie die Erstellung einer neuen Antwortdatei über *Datei/Neue Antwortdatei*.
8. Im Anschluss werden notwendige Komponenten hinzugefügt und bearbeitet. Dazu können Sie im Windows-SIM im Bereich des Images das hinzugefügte Image öffnen lassen und die Einstellungen vornehmen.

Speichern Sie Antwortdateien als *autounattend.xml*. Beim Starten der Installation durchsuchen Windows Vista und Windows Server 2008 standardmäßig das Stammverzeichnis auf eine Datei *autounattend.xml* und verwendet die hinterlegten Antworten zur Installation. Normalerweise werden Antwortdateien als *unattend.xml* gespeichert. Wenn Sie während der Installation auch die Datenträgerpartitionierung über die Antwortdatei automatisieren wollen, muss die Datei *autounattend.xml* genannt werden. Die Einstellungen, die in der Datei *autounattend.xml* vorgenommen wurden, werden während der Windows PE-Konfiguration durchgeführt, also vor dem Kopieren von Dateien auf den Datenträger.

Workshop: Erstellen einer Antwortdatei zur automatisierten Installation von Windows Vista

In diesem Abschnitt zeigen wir Ihnen in aller Kürze die einzelnen Schritte zum Aufbau einer typischen Antwortdatei mit dem Windows-Systemabbild-Manager:

1. Installieren Sie das WAIK auf einem Computer.
2. Kopieren Sie die Datei *install.wim* von der Windows Vista-DVD aus dem Verzeichnis *\sources* in ein temporäres Verzeichnis auf der Festplatte, zum Beispiel *c:\unattend*.
3. Starten Sie über *Start/Alle Programme/Microsoft Windows AIK* den *Windows Systemabbild-Manager*.
4. Öffnen Sie über den Menübefehl *Datei/Windows-Abbild auswählen* die zuvor kopierte Datei *install.wim*.
5. Wählen Sie aus, welche Windows Vista-Edition Sie installieren wollen.
6. Bestätigen Sie das Erstellen einer neuen Katalogdatei.
7. Das Paket wird jetzt eingelesen und im Windows System-Abbildmanager angezeigt.
8. Anschließend starten Sie die Erstellung einer neuen Antwortdatei über *Datei/Neue Antwortdatei*.
9. Die Antwortdatei wird mit ihren sieben verschiedenen Bereichen in der Mitte des Fensters angezeigt. Die Bereiche stellen die verschiedenen Phasen während der Installation da.
10. Im Bereich *Windows-Abbild* erweitern Sie *Components* und klicken unterhalb von *x86_Microsoft-Windows-International-Core-WinPE* mit der rechten Maustaste auf *SetupUILanguage* und wählen *Einstellungen zu Pass 1 windowsPE* hinzufügen.
11. Anschließend fügen Sie noch die Bereiche *x86_Microsoft-Windows-Setup\UserData* zum gleichen Bereich hinzu.
12. Die drei Bereiche *x86_Microsoft-Windows-Shell-Setup\OOBE* (zu Bereich 7), *x86_Microsoft-Windows-Shell-Setup\AutoLogon* (zu Bereich 7) und *x86_Microsoft-Windows-Shell-Setup* (zu Bereich 4) fügen Sie zum jeweilig vorgeschlagenen Pfad hinzu.
13. Im Bereich 4 bei der Antwortdatei kann über die rechte Maustaste alles unterhalb *x86_Microsoft-Windows-Shell-Setup_neutral* gelöscht werden.
14. Anschließend werden die verschiedenen Bereiche der Antwortdatei mit den Daten gefüllt, die für die Installation notwendig sind. Klicken Sie auf *x86_Microsoft-Windows-International-Core-WinPE.*
15. Hier werden die Spracheinstellungen unterhalb des Bereiches *Einstellungen* gesetzt. Dabei spielen die Werte *InputLocal* (Eingabe während der Installation), *SystemLocale (*Standardsprache der Programme), *UILanguage* (Standardsprache der Benutzeroberfläche) und *UserLocale* (Benutzereinstellung für Datum, Zeit, Währung und Zahlen) eine wichtige Rolle. Tragen Sie bei diesen Werten jeweils *de-DE* ein.
16. Klicken Sie dann im Bereich *Antwortdatei* auf den Wert *SetupUILanguage*.
17. Bei *UILanguage* (Sprache der Menüs während der Installation) tragen Sie ebenfalls *de-DE* ein. Bei *WillShowUI* (legt fest, wann ein Meldefenster erscheinen soll), tragen Sie *OnError* ein.
18. Klicken Sie als Nächstes bei Antwortdatei auf *UserData*.
19. Bei *AcceptEula* tragen Sie *true* ein. In diesem Fall werden die Lizenzbedingungen (EULA) automatisch bestätigt. Bei *Fullname* und *Organization* tragen Sie ein, für wen das Betriebssystem registriert ist.
20. Klicken Sie als Nächstes bei *Antwortdatei* auf *ProductKey*. In den Einstellungen kann der Produktschlüssel eingetragen werden und wieder *OnError* bei *WillShowUI*.
21. Klicken Sie als Nächstes auf *x86_Microsoft-Windows-Shell-Setup_neutral* im Bereich 4.
22. Bei *Computername* tragen Sie den Namen des Computers ein.
23. Klicken Sie als Nächstes auf *x86_Microsoft-Windows-Shell-Setup_neutral* im Bereich 7. Unter *TimeZone* tragen Sie *W. Europe Standard Time* ein.

24. Klicken Sie als Nächstes auf *AutoLogon* im Bereich 7.
25. Bei *Enabled* tragen Sie *true* ein. Bei *LogonCount* legen Sie den Wert mindestens auf 1 fest. Tragen Sie hier 2 ein, werden die ersten zwei Anmeldungen automatisch durchgeführt. Bei *Username* tragen Sie *Administrator* ein.
26. Klicken Sie dann im mittleren Bereich auf *Password* und geben dann im linken Bereich das Kennwort an.
27. Klicken Sie dann im mittleren Bereich auf *OOBE*. Diese Option steht für die *Out of the Box Experience*, das Verhalten des Betriebssystems direkt nach der Installation.
28. Anschließend werden die Werte für *OOBE* auf der rechten Seite gepflegt. *HideEULAPage* wird auf *true* gesetzt. *NetworkLocation* (Netzwerkstandort) ist entweder *Home* oder *Work* .
29. Bei *ProtectYourPC* wird das Sicherheitsverhalten festgelegt (1 = Empfohlene Einstellungen, 2 = Nur automatische Updates aktivieren, 3 =Schutz deaktivieren).
30. *SkipMaschineOOBE* legt fest, ob die Willkommensseite angezeigt wird. Mit *true* wird diese ausgeblendet. Der Wert *true* bei *SkipUserOOBE* blendet das Willkommenscenter aus.
31. Als Nächstes wird die Antwortdatei über *Extras/Antwortdatei überprüfen* auf eventuelle Fehler überprüft.
32. Im Bereich *Meldungen* dürfen keine Fehler erscheinen. Nur die Meldung, dass die Einstellung *SkipOOBE* veraltet ist, stellt kein Problem dar.
33. Speichern Sie die Antwortdatei über *Datei/Antwortdatei speichern* als *AutoUnattend.xml* ab. Die Erstellung der Datei ist damit abgeschlossen.
34. Speichern Sie die Datei auf einem USB-Stick und verbinden diesen mit dem Rechner, auf dem Windows Vista installiert wird. Booten Sie von der Windows Vista-DVD, wird jetzt die Antwortdatei zur automatisierten Installation verwendet. Die Installation über diese Antwortdatei ist allerdings noch nicht vollkommen automatisiert. Dazu muss auch die Festplattenkonfiguration automatisiert werden.

Workshop: Erweitern einer Antwortdatei zur automatisierten Partitionierung der Festplatten

Damit die Installation auch automatisiert die Festplatten konfiguriert, sind weitere Maßnahmen notwendig, die nachfolgend besprochen werden:

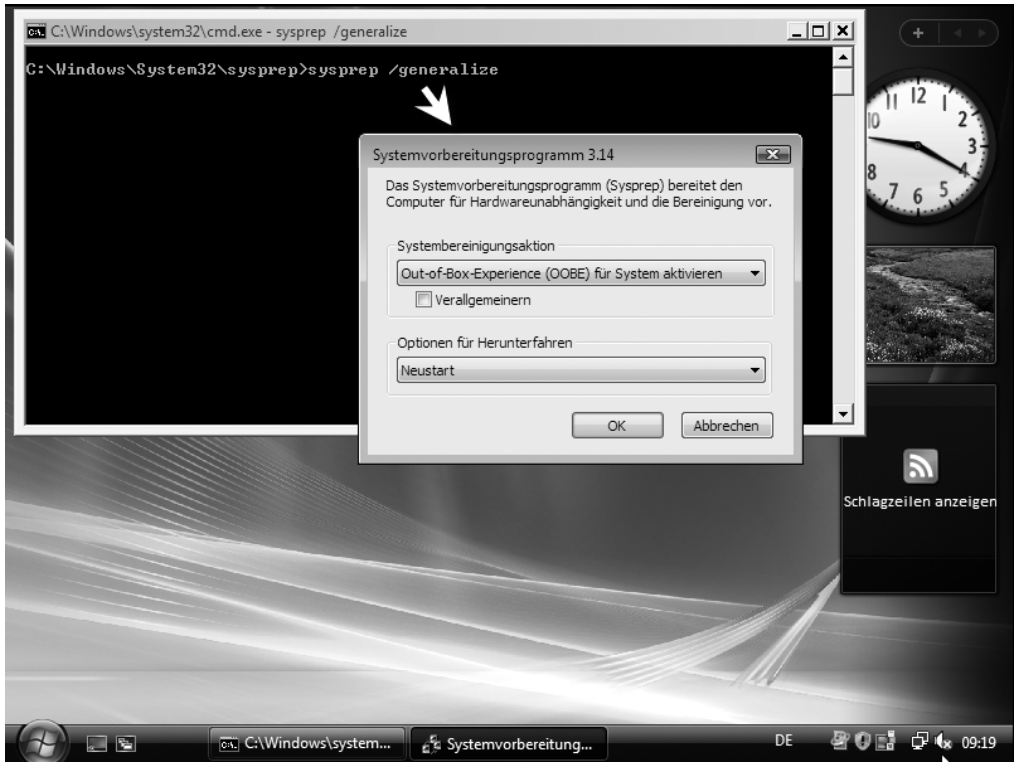
1. Öffnen Sie die erstellte Antwortdatei *autounattend.xml* im Windows-Systemabbild-Manager.
2. Erweitern Sie im Bereich *Windows-Abbild* die Komponente *x86_Microsoft-Windows-Setup_neutral* und dann *DiskConfiguration.*
3. Klicken Sie mit der rechten Maustaste auf *Disk* und fügen Sie diesen dem Bereich 1 hinzu.
4. Fügen Sie dann noch die Option *InstallTo* unter *x86_Microsoft-Windows-Setup_neutral/ImageInstall/OSImage* zum Bereich 1 hinzu.
5. Die hinzugefügten Werte werden jetzt wieder im Bereich *Antwortdatei* konfiguriert. Klicken Sie mit der rechten Maustaste auf *CreatePartitions* und wählen Sie *Neue CreatePartition einfügen* aus. Der Befehl kann so oft wiederholt werden, wie Partitionen automatisch erstellt werden sollen.
6. Klicken Sie mit der rechten Maustaste auf *ModifyPartitions* und wählen Sie *Neue ModifyPartition einfügen*. Der Befehl muss so oft wiederholt werden, wie es Partitionen auf dem Computer geben soll.

7. Klicken Sie dann auf *DiskConfiguration* und legen für den Wert *WillShowUI* wieder auf *OnError* fest.
8. Klicken Sie dann auf *Disk*. Beim Wert *DiskID* tragen Sie *0* ein. Windows wird daraufhin auf der ersten Platte im Computer installiert. Mit *true* bei *WillWipeDisk* wird vor der Installation der Inhalt der Platte gelöscht.
9. Klicken Sie im mittleren Bereich auf *CreatePartition* unterhalb von *CreatePartitions*. Mit dem Wert *Extend* wird bei *false* die Partiton nicht auf gesamte Festplattengröße erweitert. Bei *Size* wird der Wert in Megabyte eingegeben, wenn nicht die ganze Platte bei *Extend* verwendet wird. Mit *Type* wird die Art der Partition festgelegt, bei der ersten am besten *Primary*. Bei *Order* tragen Sie den Wert 1 ein.
10. Als Nächstes wird der Eintrag *ModifyPartition* unterhalb von *ModifyPartitions* angeklickt. Hier wird die erstellt Partition noch konfiguriert. Der Wert *Active* und *true* setzt die Partition auf Aktiv; nur so kann Windows Vista von der Partition starten. Mit *Extend* und *true* wird die gesamte Platte verwendet.
11. Die Option *Format* mit dem Wert *NTFS* legt das Dateisystem fest. Mit *Label* kann der Name des Laufwerks auf einen beliebigen Wert gesetzt werden. Mit *Letter* wird der Laufwerksbuchstabe konfiguriert, also am besten *C*. *Order* auf 1 gibt die Reihenfolge an, in der die Partition angepasst werden soll.
12. *PartitionID* mit dem Wert 1 legt die ID der Partition fest, welche modifiziert werden soll.
13. Als Nächstes klicken Sie im Bereich *Antwortdatei* auf *OSImage*.
14. *InstallToAvaiablePartition* wird mit *false* konfiguriert. Dadurch wird nicht die erste verfügbare Festplatte zur Installation des Betriebssystems verwendet, sondern die in der Antwortdatei konfigurierte Partition (siehe nächster Schritt). Bei *WillShowUI* wird wieder *OnError* aktiviert.
15. Klicken Sie dann im Bereich *Antwortdatei* auf *InstallTo*. Hier wird festgelegt, auf welcher Festplatte (daher bei *DiskID* der Wert 0) und welcher Partition Vista installiert werden soll. Tragen Sie bei *PartitionID* den Wert 1 ein, also die erste Partition auf der ersten Platte.
16. Als Nächstes wird die Antwortdatei erneut über *Extras* überprüft und anschließend wieder gespeichert.

Windows für die Erstellung von Images vorbereiten

Neben der Möglichkeit, Antwortdateien zu erstellen, kann auch ein Computer mit Windows Vista oder Windows Server 2008 installiert und als Image zur automatisierten Installation verwendet werden. Microsoft stellt dazu das Tool ImageX aus dem WAIK zur Verfügung. Bevor Sie ein Image eines Computers erstellen, sollten zunächst benutzerspezifische und spezielle maschinenbezogene Einstellungen zurückgesetzt werden. Microsoft stellt zur Vorbereitung eines Images das Tool *Sysprep* zur Verfügung.

Abbildg. 16.4 Vorbereiten eines Windows Vista-Image mit *Sysprep*



Wenn die Installation von Windows Vista oder Windows Server 2008 auf dem Mastercomputer abgeschlossen wurde, wird in der Befehlszeile *sysprep.exe /oobe /generalize /shutdown* ausgeführt. Das Tool befindet sich im Verzeichnis *\Windows\system32\sysprep*. Bei diesem Vorgang wird der Computer von den Benutzer- und Computereinstellungen bereinigt. Dieses Tool wurde bereits unter Windows XP und Windows Server 2003 eingesetzt. Die generelle Syntax von Sysprep ist folgende:

sysprep.exe [/oobe | /audit] [/generalize] {/reboot | /shutdown | /quit} [/quiet] [/unattend:answerfile]

- **/audit** Startet den Computer im Überwachungsmodus. Nach dem Start können zusätzliche Treiber oder Programme installiert werden.
- **/generalize** Diese Option sollte immer gesetzt werden, da dadurch Windows für die Erstellung des Images vorbereitet wird. Mit dieser Option werden alle einzigartigen Einstellungen vom Computer entfernt, die Security ID (SID) zurückgesetzt, Wiederherstellungspunkte gelöscht und die Ereignisanzeigen geleert.
- **/oobe** Mit dieser Option wird der Begrüßungsbildschirm beim nächsten Boot gestartet.
- **/reboot** Diese Option startet den Computer neu. Diese Option wird oft zusammen mit */audit* verwendet, um nach der Durchführung von *Sysprep* zu überprüfen, wie sich der Computer beim ersten Start verhält.

- **/shutdown** Diese Option fährt den Computer herunter, nachdem *Sysprep* durchgeführt worden ist.
- **/quiet** Mit dieser Option gibt *Sysprep* keine Meldungen aus. Diese Option wird normalerweise verwendet, wenn die Durchführung automatisiert wird.
- **/quit** Mit dieser Option wird *Sysprep* nach der Fertigstellung beendet.
- **/unattend: <Antwortdatei>** Mit dieser Option wird der Pfad und die Bezeichnung der Antwortdatei für die Windows-Installation gesetzt.

Einschränkungen von Sysprep

Nur die *Sysprep*-Version von Windows Vista und Windows Server 2008 kann zur Vorbereitung eines Windows Vista- beziehungsweise Windows Server 2008-Image verwendet werden. Die Zeitdauer, in der Windows nach der Installation aktiviert werden muss, kann durch *Sysprep* bis zu drei Mal zurückgesetzt werden. Nach der dritten Ausführung von *Sysprep* für einen Computer wird diese Zeitdauer nicht mehr zurückgesetzt. *Sysprep* kann nur auf Computern ausgeführt werden, die sich in einer Arbeitsgruppe befinden. Die Ausführung auf Computern, die Mitglied einer Domäne sind, wird nicht unterstützt. Wenn *Sysprep* auf einem PC mit verschlüsselten Dateien ausgeführt wird, sind diese Dateien nach der Ausführung unbrauchbar.

Windows Preinstallation Environment (Windows PE)

Bei Windows PE handelt es sich um eine Minimalversion von Windows Vista und Windows Server 2008, welches die Kernelfunktionen enthält. Auch die Basisinstallation von Windows Vista und Windows Server 2008 basiert auf Windows PE, es gibt keinen textorientierten Teil der Installation mehr. Windows PE gehört zum Lieferumfang von Windows Vista und Windows Server 2008 und muss nicht mehr gesondert heruntergeladen und installiert werden. Für Windows Vista und Windows Server 2008 gibt es daher keine DOS-Bootdisketten mehr; diese werden ersatzlos durch Windows PE ersetzt.

Trotz aller Funktionsvielfalt ist Windows PE kein normales Betriebssystem, sondern dient lediglich zur Installation oder Diagnose von Windows Vista und Windows Server 2008. Während der Installation von Windows Vista und Windows Server 2008 lädt die Installationsroutine die Windows PE-Version auf der DVD mit einer Größe von etwa 140 MB *(\Sources\boot.wim)*. Auf dieser Basis wird dann Windows Vista oder Windows Server 2008 installiert.

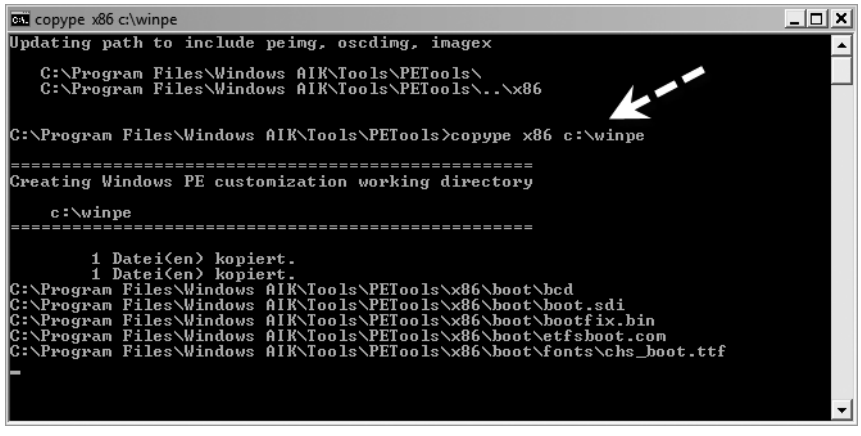
Auch die Computerreparaturoptionen von Windows Vista und Windows Server 2008 sind auf Basis von Windows PE aufgebaut. Mit Windows PE können Installationsvorbereitungen und Rollouts von Windows Vista und Windows Server 2008 durchgeführt werden. Nachdem eine Antwortdatei erstellt oder ein Master-PC installiert wurde, wird ein Image des Computers angelegt, auf dessen Basis die Installation im Netzwerk verteilt werden kann. Grundsätzlich läuft dies so ab: Im ersten Schritt wird eine CD erstellt, mit deren Hilfe Windows PE auf diesem Computer gestartet werden kann. Im Anschluss wird der Master-PC mit der Windows PE-CD gestartet und das Image erzeugt.

Erstellen einer Windows PE-CD

Um eine PE-CD zu erstellen, benötigen Sie das Windows Automated Installation Kit (WAIK). Gehen Sie dazu folgendermaßen vor:

1. Um eine solche CD zu erstellen, öffnen Sie eine Befehlszeile und gehen Sie in das Verzeichnis *C:\Program Files\Windows AIK\Tools\PETools*. Diese Eingabeaufforderung liegt bereits als Verknüpfung im Startmenü vor.
2. Führen Sie in der Befehlszeile den Befehl *copype.cmd <Systemvariante> <Verzeichnis>* aus. Als Systemvariante kann entweder *x86*, *amd64* oder *ia64* verwendet werdenn, abhängig davon, welches System eingesetzt wird. Als Verzeichnis geben Sie ein beliebiges Verzeichnis auf der Festplatte des Admin-PCs an, zum Beispiel *winpe*. Ein Beispiel für die Eingabe des Befehls ist *copype.cmd x86 c:\winped* (Abbildung 16.5). Das Verzeichnis muss vorher nicht erstellt werden. Der Assistent erstellt dieses automatisch und legt die Dateien im Anschluss in diesem Verzeichnis ab.

Abbildg. 16.5 Erstellen eines Windows PE-Image



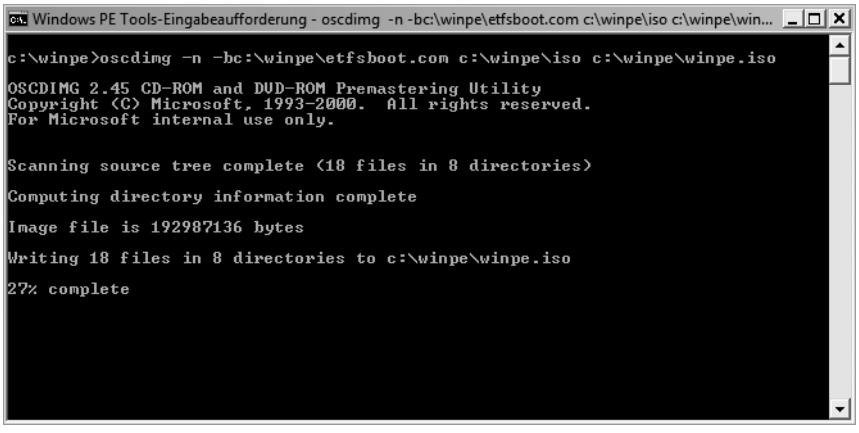
3. Anschließend sollten Sie zusätzliche Tools in dieses Verzeichnis kopieren, welches Sie beim Starten von Windows PE benötigen. Zumindest das Imaging-Programme *imagex.exe* sollten Sie in das Verzeichnis kopieren. Sie finden *Imagex.exe* unter *C:\Program files\Windows AIK\Tools\x86\Imagex.exe*. Kopieren Sie *Imagex.exe* in das Unterverzeichnis *ISO* im PE-Verzeichnis auf Ihrer Festplatte.
4. Anschließend können Sie für ImageX noch die Datei *wimscript.ini* erstellen. Diese Datei sollte die Einträge aus Listing 16.1 enthalten. Speichern Sie die Datei im gleichen Verzeichnis wie *ImageX.exe*. Diese Datei weist ImageX an, einige Dateien bei der Erstellung des Image zu überspringen. Beim Starten von ImageX verwendet dieses Tool automatisch die Datei *wimscript.ini*, wenn sich diese im gleichen Verzeichnis befindet.

Listing 16.1 Inhalt der Datei *wimscript.ini*

```
[ExclusionList]
ntfs.log
hiberfil.sys
pagefile.sys
"System Volume Information"
RECYCLER
Windows\CSC
[CompressionExclusionList]
*.mp3
*.zip
*.cab
```

5. Im nächsten Schritt wird die ISO-Datei erstellt, die schließlich die Windows PE-Installation enthält. Auch für diese Aufgabe gibt es im *Windows Automated Installation Kit* ein entsprechendes Tool mit der Bezeichnung *Oscdimg*. Um die ISO-Datei zu erstellen, wechseln Sie wieder in die Befehlszeile und gehen in das Verzeichnis *C:\Program Files\Windows AIK\Tools\PETools*. Geben Sie den Befehl *Oscdimg –n –bc:\winpe\etfsboot.com c:\winpe\ISO c:\winpe\winpe.iso* ein. Verwenden Sie als Verzeichnisnamen den Namen, den Sie bei sich verwendet haben und in dem sich die PE-Dateien befinden (Abbildung 16.6). Das Tool erstellt im Anschluss die ISO-Datei in der Befehlszeile.

Abbildg. 16.6 Erstellen einer ISO-Datei für das Windows PE-Image



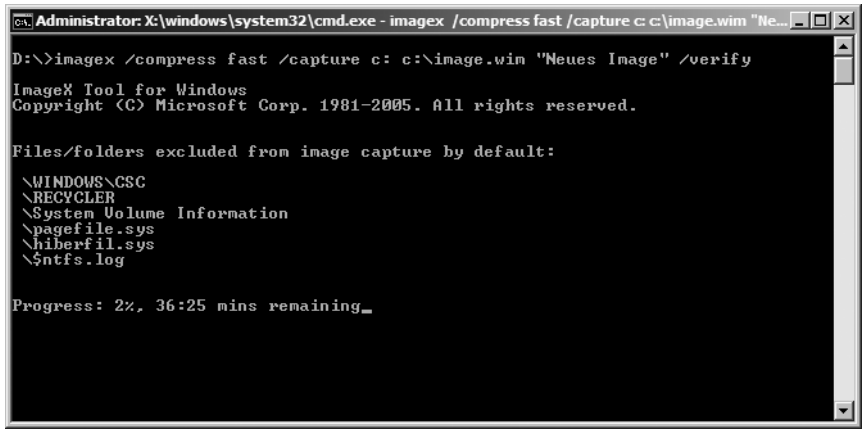
Brennen Sie im Anschluss diese ISO-Datei auf CD und booten Sie den Master-PC mit dieser CD. Wichtig an dieser Stelle ist, dass Sie in der Bootreihenfolge beachten, dass der Master-PC von dieser Windows PE-CD auch bootet. Im Anschluss wird Windows PE gestartet und es wird automatisch eine Befehlszeile geöffnet. Im Anschluss zeigen wir Ihnen, wie Sie mit ImageX und einem gestarteten Windows PE ein Image des Masterrechners erstellen können.

Images erstellen mit ImageX

Bei ImageX handelt es sich um ein Befehlszeilentool, welches im Windows Automated Deployment Kit (WAIK) enthalten ist. Mit WAIK lassen sich Images erstellen, bearbeiten und zuweisen. Dieses

Werkzeug basiert auf der Windows Imaginging-Technologie (WIM) und ist das wichtigste Tool beim Rollout von Windows Vista und Windows Server 2008. Idealerweise haben Sie das Tool auf die Windows PE-CD integriert. Für ImageX ist keine grafische Oberfläche geplant, allerdings hat das Tool eine eigene API, sodass Dritthersteller Anwendungen schreiben können, die ImageX verwenden. Nachdem auf dem Master-Computer Windows Vista oder Windows Server 2008 installiert und vorbereitet wurde, wird der Computer mit Windows PE gebootet. Anschließend wird in der Befehlszeile über den Befehl *imagex /compress fast /capture c: c:\mein-image.wim "<Beschreibung>" /verify* ein Image der Installation erstellt (Abbildung 16.7). Statt *mein-image.wim* kann eine beliebige Bezeichnung für das Image verwendet werden.

Abbildg. 16.7 Erstellen eines Image mit *ImageX* zur Verteilung mit den Windows-Bereitstellungsdiensten



Wird ein Windows Vista- oder Windows Server 2008-Computer mit Windows PE gebootet, werden drei Partitionen angelegt:

- **C** In dieser Partition befindet sich die installierte Windows Vista- oder Windows Server 2008-Version, von der ein Image erstellt werden soll.
- **D** Hierbei handelt es sich um die CD mit den Windows PE-Installations-Dateien. Hier finden Sie auch ImageX.
- **X** Dieser Laufwerksbuchstabe wird für die Laufzeitumgebung von Windows PE verwendet. Diese Partition wird im Arbeitsspeicher erstellt (RAM-Drive).

Nachdem die Erstellung des Image gestartet wird, beginnt ImageX die angegebene Partition zu scannen und das Image zu erstellen. Das Image kann dann über die Windows-Bereitstellungsdienste im Unternehmen verteilt werden.

Sie können das bereitgestellte Image auch bearbeiten – und zwar so wie jeden anderen Ordner. Sie können zum Beispiel ein Betriebssystemimage bereitstellen, Gerätetreiber hinzufügen und die Bereitstellung wieder aufheben. Für das Mounten eines Images wird zum Beispiel der Befehl *imagex /mountrw <Pfad zum Image und *.wim-Datei> <Pfad, in den das Image gemounten wird>* verwendet. Mit dem Befehl *peimg.exe /inf=<Pfad zur *.inf-Datei des Treibers> <Gemounteter Pfad>* werden Treiber in das Image kopiert. Über *imagex /unmount /commit <Gemounteter Pfad>* wird die Bereitstellung wieder aufgehoben. Das Image enthält jetzt den kopierten Treiber.

Um das erstellte Image wieder auf andere Computer zu installieren, werden Windows PE, ImageX oder am besten die Windows-Bereistellungsdienste verwendet.

Installation von Windows Vista über ein ImageX-Image

Wollen Sie ein Image nur auf einem einzelnen Computer, ohne die WDS installieren, booten Sie den Zielcomputer mit einem Windows PE-Datenträger und stellen sicher, dass der Datenträger korrekt konfiguriert ist. Sollte die Festplatte des Zielcomputers noch vollkommen leer sein, können Sie mit dem Befehl *diskpart* auf dem Zielcomputer eine ausreichend große aktive Partition erstellen. Geben Sie dazu die Befehle aus Listing 16.2 ein.

Listing 16.2 Erstellen einer Partition zur Installation von Windows Vista oder Windows Server 2008 über *ImageX*

```
diskpart
select disk 0
clean
create partition primary size=20000
select partition 1
active
format
exit
```

Im nächsten Schritt wird die Image-Datei von der Netzwerkfreigabe auf die lokale Festplatte des PCs kopiert. Im Anschluss wird das Image mit dem Befehl *imagex /apply c:\mein-image.wim c*: auf den Computer installiert.

Weitere Optionen von ImageX

Welche Optionen neben den beschriebenen ImageX noch kennt, können Sie der folgenden Tabelle entnehmen.

Tabelle 16.1 Befehlszeilenoptionen von ImageX

Option	Beschreibung
/append	Hängt ein Image an eine vorhandene WIM-Datei an
/apply	Stellt ein Image in einem bestimmten Laufwerk wieder her
/capture	Erstellt ein Image in einer neuen WIM-Datei
/commit	Übernimmt die Änderungen für eine WIM-Datei
/compress	Legt die Kompression auf »keine«, »schnell« oder »maximal« fest. Die genaue Syntax erfahren Sie durch *imagex /?*.
/config	Verwendet die in der angegebenen Datei festgelegten erweiterten Optionen
/delete	Löscht ein Image aus einer WIM-Datei mit mehreren Images
/dir	Zeigt eine Liste der Dateien und Ordner in einem Image an
/export	Überträgt ein Image von einer WIM-Datei zu einer anderen
/info	Gibt die XML-Beschreibungen für eine bestimmte WIM-Datei zurück
/ref	Legt die WIM-Referenzen für das Wiederherstellen fest

Tabelle 16.1 Befehlszeilenoptionen von ImageX *(Fortsetzung)*

Option	Beschreibung
/scroll	Gibt alle Ausgaben am Stück aus
/split	Unterteilt eine vorhandene WIM-Datei in mehrere schreibgeschützte Teile
/verify	Überprüft doppelte und extrahierte Dateien
/mount	Stellt ein Image schreibgeschützt in einem bestimmten Ordner bereit
/mountrw	Stellt ein Image mit Lese- und Schreibzugriff in einem bestimmten Ordner bereit. Durch diesen Befehl können Dateien ausgetauscht werden und Sie können auf den Inhalt des Image zugreifen.
/unmount	Hebt die Bereitstellung eines Image in einem bestimmten Ordner auf
/?	Gibt die möglichen Befehlszeilenparameter von ImageX aus

Einschränkungen von ImageX

Bei allen Vorteilen von ImageX sollten Sie auch die Einschränkungen des Tools berücksichtigen, wenn Sie Images von PCs erstellen:

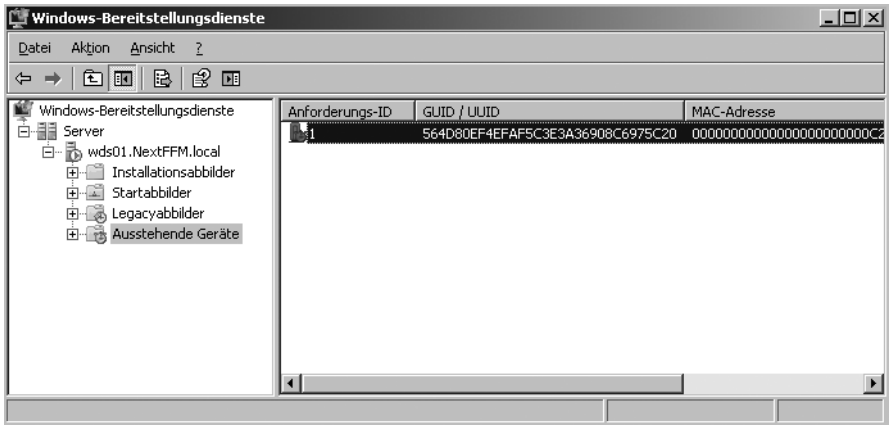
- Mit ImageX können ausschließlich nur Vollversionen der Betriebssysteme, keine Aktualisierungen verteilt werden.
- Mit ImageX lassen sich nur Images verwenden, die mit dem Windows Image-Format (WIM) erstellt wurden. Es werden keine Images von Drittherstellern unterstützt, die auf Sektorbasis erstellt wurden (Acronis, Norton Ghost usw.).
- Es können nur Images von Windows Vista, Windows Server 2008, Windows XP mit SP2 und Windows Server 2003 mit SP1 von ImageX gemountet werden. ImageX kann jedoch ohne weiteres Images von allen Versionen von Windows 2000, XP und 2003 erstellen und installieren, diese aber nicht zur direkten Bearbeitung mounten.
- Images können zum Anpassen und Konfigurieren nur auf NTFS-Partitionen gemountet werden. Wenn Images nur gelesen werden sollen, wird auch FAT, ISO und UDF unterstützt.
- Bevor ein Image auf einen anderen Datenträger zurückgespielt werden kann, muss dieser mit *diskpart* erstellt und konfiguriert werden.

Grundlagen der Windows-Bereitstellungsdienste

Die Windows-Bereitstellungsdienste sind der Nachfolger der Remote Installation Services (RIS) von Windows Server 2003. Windows Vista und Windows Server 2008 können nicht über die Remote Installation Service-Technologie installiert werden. Dies liegt daran, dass diese beiden Betriebssysteme über die Windows-Imaging (WIM)-Technologie installiert werden. WDS beherrschen im Gegensatz zu RIS die WIM-unterstützte Installation, doch dazu später mehr. Mit WDS können auch Windows Server 2003, XP und 2000 automatisiert installiert werden. Die Windows-Bereitstellungsdienste können kostenlos über das WAIK (Windows Automated Installation Kit) oder das Service Pack 2 auf einem Windows Server 2003 installiert werden. In Windows Server 2008 ist WDS bereits

integriert und kann ohne notwendiges Update aktiviert werden. WDS ist für den neuen Microsoft System Center Configuration Manager 2007, den Nachfolger des Systems Management Server 2003 optimiert.

Abbildg. 16.8 Nach der Installation der Windows-Bereitstellungsdienste steht ein neues Snap-In für die Management-Konsole zur Verfügung



WDS kann auch 64-Bit-Betriebssysteme verteilen, was durch die immer stärkere Verbreitung von 64-Bit-Computern und den geringen Aufpreis von Windows Vista x64 eine wertvolle Erweiterung darstellt. Der WDS-Server muss einer bestehenden Active Directory-Domäne angehören oder ein eigenständiger Domänencontroller sein. Natürlich wird auch eine DNS-Namensauflösung benötigt, diese sollte aber innerhalb von Active Directory ohnehin zur Verfügung stehen. Der WDS-Server muss außerdem Zugang zu einem aktiven DHCP-Server haben. Der Server benötigt eine separate Partition, die mit NTFS formatiert wurde. In dieser werden die Abbilder zur automatisierten Installation abgespeichert. In Abhängigkeit des Arbeitsmodus des Bereitstellungsdienstes benötigen Sie entweder Windows Server 2003 SP1 oder SP2, Windows Server 2003 R2 oder Windows Server 2008.

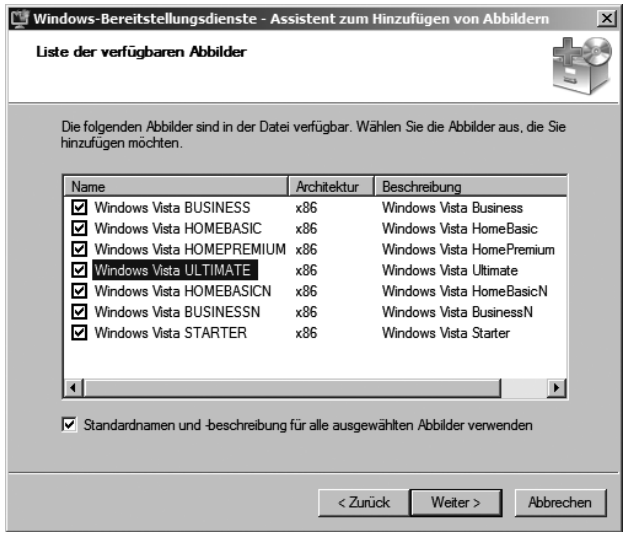
Der Betriebsmodus von WDS

Die Vorgehensweise der Installation richtet sich vor allem danach, welchen Modus Sie für den WDS-Server vorsehen: Legacy-Modus, Gemischter-Modus oder Einheitlicher-Modus. Der Legacy-Modus sowie der gemischte Modus unterstützen noch RIS-Abbilder, während der einheitliche Modus nur WDS-Abbilder unterstützt. Der einheitliche Modus kann sowohl unter Windows Server 2003 als auch unter Windows Server 2008 genutzt werden und ist die beste Möglichkeit, neue Abbilder im Unternehmen zu verteilen, vor allem dann, wenn keine RIS-Abbilder aus Kompatibilitätsgründen mehr benötigt werden. Die Konfiguration des WDS-Servers im Legacy Modus erfordert mindestens Windows Server 2003 SP1. Bei der Verwendung von Windows Server 2008 ist nur die Installation des einheitlichen Modus möglich. Eine Verwendung alter RIS-Abbilder ist nicht möglich. Über die Konsole der Windows Bereitstellungsdienste kann der WDS-Server konfiguriert werden. Klicken Sie mit der rechten Maustaste auf den Servernamen und wählen im Kontextmenü den Eintrag *Server konfigurieren*. Nach der ersten Einrichtung steht der Server für die Verteilung von Windows zur Verfügung.

Verwalten von Abbildern in WDS

Sobald der WDS-Server installiert und eingerichtet worden ist, können Abbilder hinzugefügt werden. Hier gibt es verschiedene Typen. Ein *Startabbild* kommt zum Einsatz, wenn auf dem Client Windows PE starten soll. *Installationsabbilder* dienen der Installation von Windows und erfordern eine Abbildgruppe. Eine *Abbildgruppe* ist ein Ordner, der sich unterhalb des Knotens *Installationsabbilder* befindet. Für alle Clientcomputer, die keine Unterstützung für PXE bieten, gibt es die Möglichkeit, ein Startabbild zu exportieren. Somit können auch diese Clientcomputer durch den WDS-Server bedient werden. Diese Abbilder werden *Suchstartabbilder* genannt und erhalten vor der Generierung die Information, welcher Bereitstellungsserver verwendet werden soll. Aufzeichnungsabbilder bieten eine Alternative zum Befehlszeilenprogramm *ImageX.exe*, wenn ein mit dem Dienstprogramm *Sysprep.exe* vorbereitetes Abbild aufgezeichnet wird. Beim Start eines Clients mit einem *Aufzeichnungsabbild* wird das Aufzeichnungsdienstprogramm der Windows-Bereitstellungsdienste aufgerufen. Es führt den Benutzer durch die erforderlichen Schritte zum Aufzeichnen und Hinzufügen eines neuen Abbilds. Das Aufzeichnungsabbild muss als Startabbild hinzugefügt werden.

Abbildg. 16.9 Mit Assistenten können auf einfachem Wege so genannte Installationsabbilder hinzugefügt werden



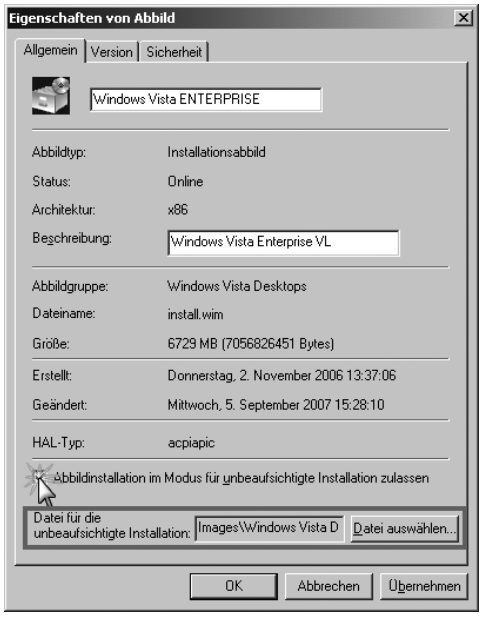
Für das Booten über das Netzwerk (PXE) stellen die Bereitstellungsdienste verschiedene *Network Bootstrap Programme (NBP)* zur Verfügung. Um diese auch effektiv nutzen zu können, sollten alle Clients im Active Directory bereits mit eindeutigen IDs ausgestattet sein. Nur durch diese Identifizierung anhand der GUID oder der MAC-Adresse kann das Bootverhalten der Clients durch die Zuweisung der NBP beeinflusst werden. Das Tool *PXEboot.com* erfordert, dass der Benutzer beim Starten des Computers die Taste F12 drücken muss, um einen Netzwerkboot durchzuführen. Wird *PXEboot.n12* genutzt, erfolgt der Boot über das Netzwerk ohne Drücken der Funktionstaste F12. *AbortPXE.com* legt fest, dass ein Computer direkt das nächst verfügbare Bootmedium nutzt. Es erfolgt kein Netzwerkboot. *Wdsnbp.com* stellt Funktionen bereit, die zur Erkennung der Architektur und zur Verwaltung von Anfragen der Bootberechtigung benötigt werden. Es wird noch vor *PXEboot.com* geladen. Steht in der Bootreihenfolge des Rechners das Booten über Netzwerk vor dem Booten von Festplatte und wird *PXEboot.n12* genutzt, wird der Client bei jedem Hochfahren in den

Netzwerkboot übergehen und nicht das eigentliche Betriebssystem laden. Dieses Verhalten lässt sich dadurch vermeiden, indem Sie *PXEboot.com* nutzen oder *AbortPXE.com* verwenden.

Windows-Imaging nutzen

Eine der wichtigsten Funktionen der Windows-Bereitstellungsdienste ist die Unterstützung von Windows-Imaging (WIM). Windows Vista und Windows Server 2008 werden ausschließlich über diese Technologie installiert. Diese Technik ist hardwareunabhängig. Das bedeutet, Sie brauchen nur ein Image für verschiedene Hardwarekonfigurationen. Mit WIM können mehrere Images in einer Datei gespeichert werden. Außerdem nutzt WIM eine Kompression und das Single-Instance-Verfahren. So wird die Größe von Imagedateien deutlich reduziert. Single-Instancing ist eine Technologie, bei der jede Datei nur einmal gespeichert wird. Wenn zum Beispiel Image 1, 2 und 3 alle die gleiche Datei A enthalten, dann sorgt Single-Instancing dafür, dass Datei A nur einmal tatsächlich gespeichert wird. WIM-Images ermöglichen die Offlinebearbeitung von Images. Sie können Betriebssystemkomponenten, Patches und Treiber hinzufügen oder löschen, ohne ein neues Image erstellen zu müssen. Windows Vista stellt eine Porgrammierschnittstelle (API) für das WIM-Imageformat zur Verfügung, die WIMGAPI. Diese kann von Entwicklern für die Arbeit mit WIM-Imagedateien genutzt werden. Mit WIM können auf dem Zielvolumen vorhandene Daten beibehalten werden. Das Einrichten eines Images löscht nicht zwingend alle vorhandenen Daten auf der Festplatte. In Kombination mit Windows PE 2.0 lassen sich diese Images auch erweitern oder ändern, ohne dass Windows dazu komplett gestartet sein muss. So ist es beispielsweise möglich, schnell einen Treiber auszutauschen, ohne dass das Image komplett neu geschrieben werden muss. Ein weiterer Vorteil des WIM-Formats ist das so genannte »non-destructive deployment«. Dies bedeutet, dass beim Einspielen des Images die Daten, die sich bereits auf der Festplatte befinden, nicht gelöscht oder überschrieben werden.

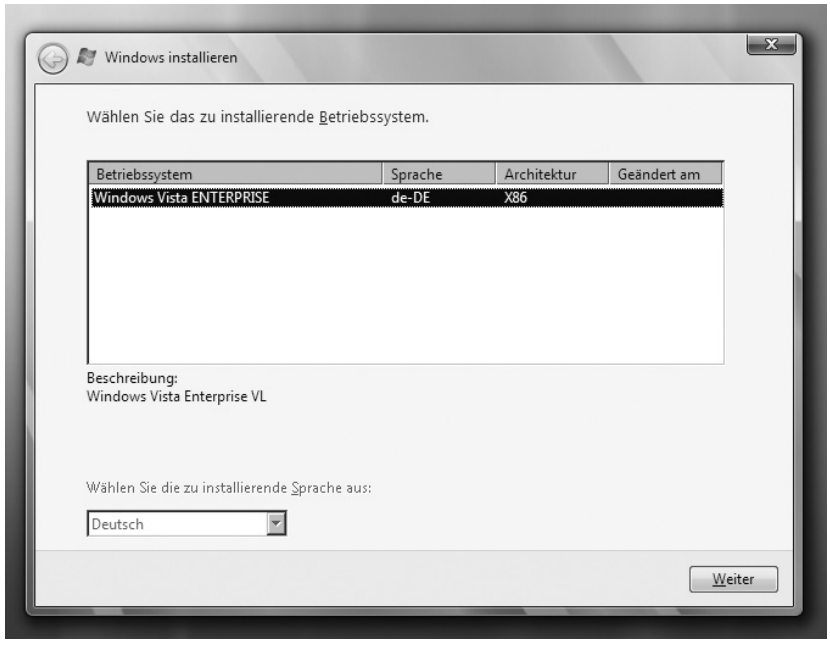
Abbildg. 16.10 Die Windows-Bereitstellungsdienste können WIM-Abbilder zur automatisierten Installation nutzen



Wie funktioniert die automatisierte Installation von Windows Vista über WDS?

Ein Clientcomputer wird mit PXE im Netzwerk gestartet. Nach dem Laden des BIOS sendet das PXE-ROM auf der Netzwerkkarte eine Netzwerk-Dienstanforderung an den nächstgelegenen DHCP-Server. Mit der Anforderung sendet der Client seine GUID (Globally Unique Identifier). Der DHCP-Server erteilt dem Client eine IP-Lease mit Optionen für DNS (006), Domäne (015) und PXE-Server (060). Als Nächstes startet das Bootimage mit Windows PE, das in das RAM geladen wird. Über einen Eintrag in der Antwortdatei wird die Festplatte angepasst. Das Setup führt die in der Antwortdatei enthaltene Anmeldung an den WDS-Server aus. Existiert dieser Eintrag nicht, wird um eine Authentifizierung gebeten. Soll eine unbeaufsichtigte Installation durchgeführt werden, darf immer nur ein Image in der Image-Gruppe existieren. Wurde die Antwortdatei mit Informationen wie Installations-Key, Sprachversion und Domänenkonto korrekt konfiguriert, läuft die Installation völlig automatisiert ab. Das Befehlszeilenprogramm *Wdsutil.exe* bietet eine erweiterte Funktionalität. Außerdem kann mit dem Tool auch ein bestehendes RIPREP-Image zu einem WIM-Image konvertiert werden.

Abbildg. 16.11 Bei der halbautomatisierten Installation von Windows Vista über WDS kann der Anwender das zu installierende Betriebssystem auswählen



Die Windows Deployment Services bieten eine effiziente Möglichkeit, Windows-Betriebssysteme ohne den Einsatz von Installationsmedien zu installieren. Durch den Einsatz von Antwortdateien lässt sich die Installation automatisieren. In Kombination mit der Lite Touch Installation (LTI) beziehungsweise der Zero Touch Installation (ZTI) von Business Desktop Deployment 2007 (BDD) oder Microsoft Deployment kann der Bereitstellungsdienste-Server, ohne viel Speicherplatz zu verbrauchen, als reines Transportmittel für die verwendeten Startabbilder verwendet werden.

HINWEIS Beachten Sie, dass bei der Verwendung von Windows Server 2008 nur noch die Installation des einheitlichen Modus möglich ist. Eine Verwendung alter RIS-Abbilder ist nicht möglich.

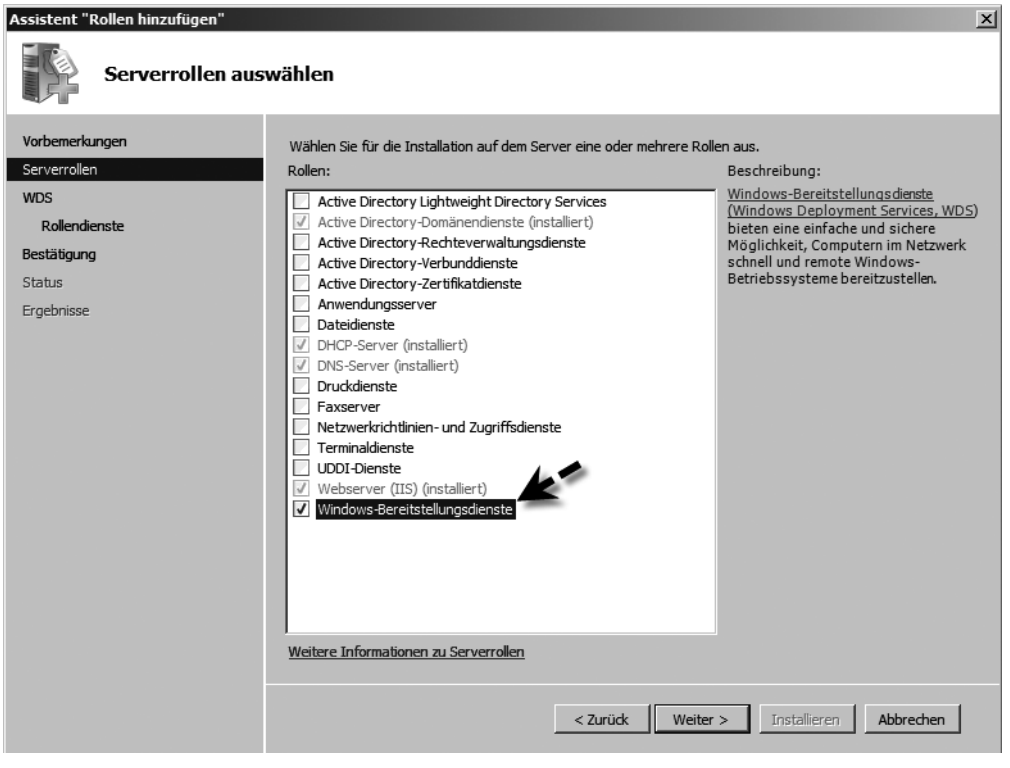
Installation der Windows-Bereitstellungsdienste

Um WDS auf einem Server zu installieren, sollten im Netzwerk zunächst die Voraussetzungen geschaffen werden. Es wird ein Active Directory, eine funktionsfähige DNS-Infrastruktur und ein DHCP-Server benötigt. Die Installation besteht aus der Installation der Serverrolle und der anschließenden Ersteinrichtung des Servers.

Serverrolle der Windows-Bereitstellungsdienste installieren

Als Erstes starten Sie den Server-Manager und installieren die Rolle *Windows-Bereitstellungsdienste* (Abbildung 16.12).

Abbildg. 16.12 Installieren der Serverrolle *Windows-Bereitstellungsdienste*

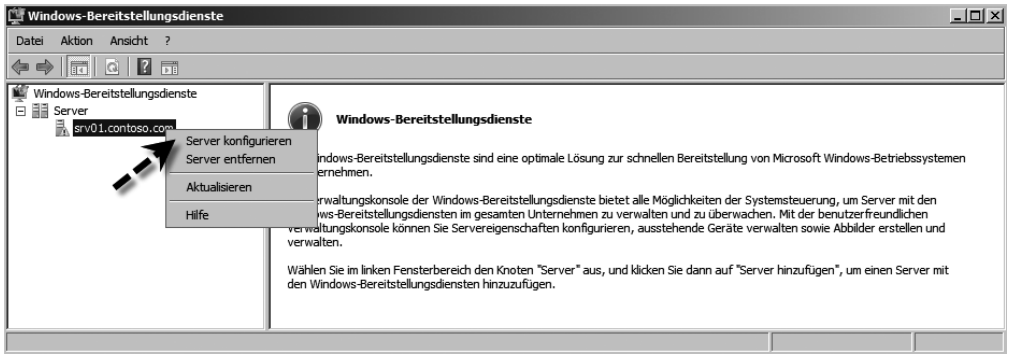


Auf der nächsten Seite des Assistenten erhalten Sie einige Informationen zur Installation, die Sie auf jeden Fall durchlesen sollten. Als Nächstes werden die Rollendienste für den Server ausgewählt. Standardmäßig wird sowohl der *Bereitstellungsserver* als auch der *Transportserver* installiert. Danach wird die Installation abgeschlossen. Der Serverdienst ist jetzt installiert, aber noch nicht eingerichtet. Zur Installation gehört eine Ersteinrichtung, auch Initialisierung genannt, die über die Verwaltungskonsole der Windows-Bereitstellungsdienste durchgeführt wird.

Ersteinrichtung der Windows-Bereitstellungsdienste

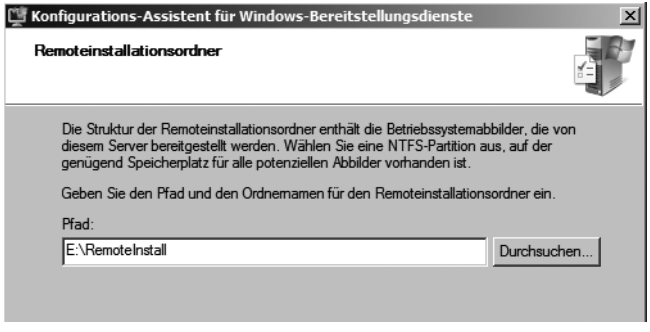
Öffnen Sie für die erste Einrichtung die Verwaltungskonsole der Windows-Bereitstellungsdienste über *Start/Verwaltung* oder durch Eingabe von *wdsmgmt.msc* in das Suchenfeld des Startmenüs. Der Server wird angezeigt, ist aber noch mit einem Warnzeichen versehen. Über das Kontextmenü wird der Befehl *Server konfigurieren* gestartet. Hierüber wird die Installation abgeschlossen.

Abbildg. 16.13 Starten der Ersteinrichtung nach der Installation der Windows-Bereitstellungsdienste



Es startet ein Assistent, über den der Server eingerichtet wird. Auf der ersten Seite nach dem Begrüßungsfenster legen Sie den Speicherort fest, in dem die Installationsabbilder gespeichert werden. Es bietet sich an, dafür eine eigene Partition zu wählen, damit die Daten übersichtlich gespeichert werden. Statt über den Assistenten kann dieser Vorgang auch über die Befehlszeile mit dem Befehl *wdsutil /initialize-server /reminst:<Verzeichnis>* durchgeführt werden.

Abbildg. 16.14 Auswählen des Verzeichnisses für die Images



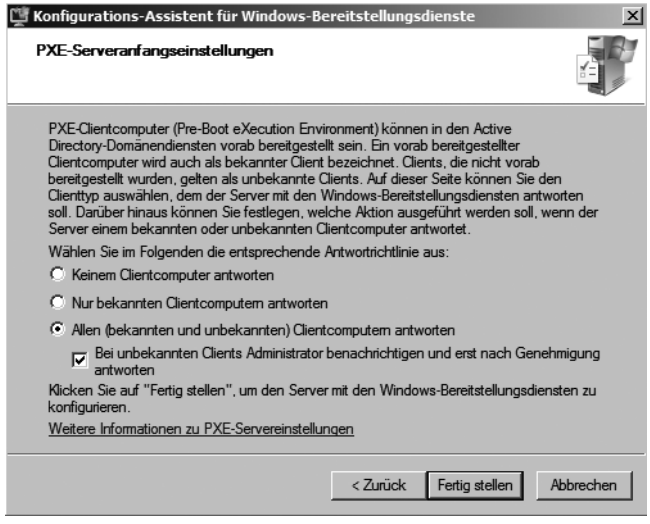
Auf der nächsten Seite werden die notwendigen Optionen für den DHCP-Server konfiguriert. Hier wird eingestellt, dass eine neue DHCP-Option 60 hinzugefügt wird und der Server nicht mehr den Port 67 abhört. Dies ist erforderlich, damit der DHCP-Server im Netzwerk von startenden Clients gefunden werden kann. In der Befehlszeile erreichen Sie diese Konfiguration über *wdsutil /Set-Server /UseDHCPPorts:no /DHCPoption60:yes*.

Abbildg. 16.15 Konfigurieren der DHCP-Optionen für den WDS

Auf der nächsten Seite des Assistenten legen Sie fest, auf welche Clients der PXE-Server antworten soll, wenn eine Bootabfrage an den Server gestellt wird. Aktivieren Sie die Option *Nur bekannten Clientcomputern antworten*, können nur Computer, für die in der Domäne ein Konto erstellt wurde, diesen Server verwenden. Damit der Server ordnungsgemäß Clients anbinden kann, sollten Sie am besten die Optionen *Allen (bekannten und unbekannten) Clientcomputern antworten* und, falls gewünscht, das Kontrollkästchen *Bei unbekannten Clients Administrator benachrichtigen und erst nach Genehmigung antworten* aktivieren. So ist sichergestellt, dass sich kein Unbefugter eine Vista-Installation unter den Nagel reißen kann. Diese Einstellung kann auch über die Befehlszeile mit dem Befehl *wdsutil /Set-Server /AnswerClients:all* durchgeführt werden. Nach der Installation kann diese Einstellung in der WDS-Konsole in den Eigenschaften des Servers auf der Registerkarte *PXE-Antworteinstellungen* konfiguriert werden.

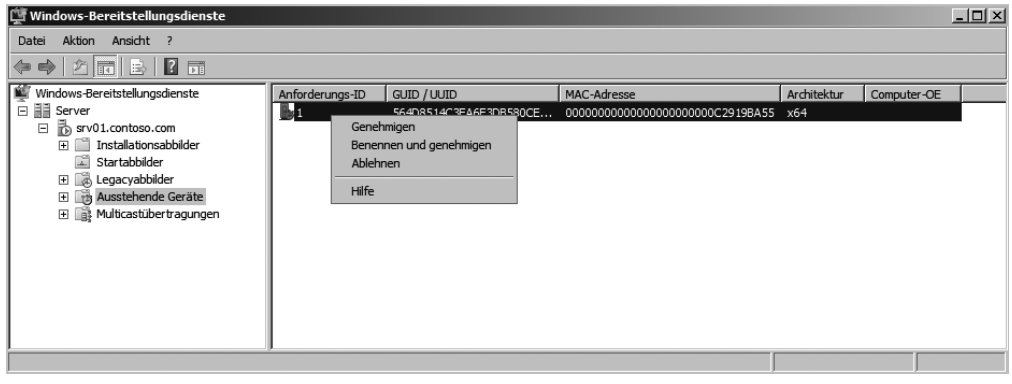
Anschließend wird die Ersteinrichtung über die Schaltfläche *Fertig stellen* abgeschlossen und der Server ist einsatzbereit für das Hinzufügen von Abbildern.

Abbildg. 16.16 Konfigurieren der PXE-Einstellungen des WDS



Sobald sich ein Client mit dem WDS-Server verbindet, kann die Genehmigung über *Ausstehende Geräte* durchgeführt werden (Abbildung 16.17).

Abbildg. 16.17 Genehmigen von Geräten für die Verbindung zum WDS



Für Testumgebungen, oder wenn diese Sicherheitsmaßnahme nicht gewünscht ist, kann die notwendige Genehmigung auch nachträglich deaktiviert werden.

TIPP Neben der Verwaltungskonsole bieten die Windows-Bereitstellungstools auch ein Befehlszeilenprogramm mit der Bezeichnung *Wdsutil.exe*. Viele Administrationsaufgaben, zum Beispiel das Verwalten von Abbildern, lassen sich neben der grafischen Oberfläche auch mit dem Tool durchführen. Eine ausführliche Hilfe über die Optionen erhalten Sie mit *wdsutil /?*. Bereits bei der Einrichtung des Servers kann über *Wdsutil.exe* einiges automatisiert oder über Skripts abgewickelt werden. Die einzelnen Befehle hierfür finden Sie im vorangegangenen Abschnitt des Kapitels.

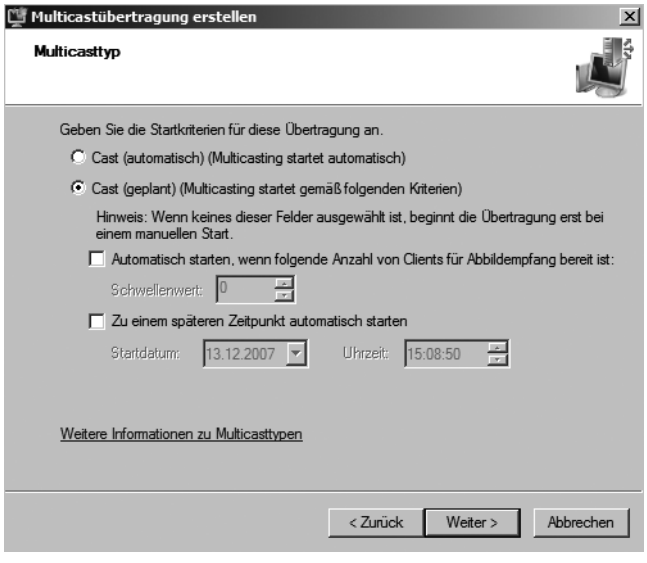
Multicast verwenden

Multicast wird dann verwendet, wenn sich nicht nur wenige Clients mit dem Bereitstellungsserver verbinden, sondern eine große Anzahl von Clients. Beim Erstellen einer Multicastübertragung für ein Abbild werden die Daten nur einmal über das Netzwerk gesendet, wodurch eine deutliche Verringerung der verwendeten Netzwerkbandbreite erreicht werden kann. Achten Sie aber darauf, dass diese Funktion von den Routern im Netzwerk unterstützt werden muss.

ACHTUNG Das Startabbild von Windows Vista kann nicht für die Multicastübertragung verwendet werden. Soll Multicast aktiviert werden, verwenden Sie die Datei *boot.wim* von der Windows Server 2008-DVD.

Verwenden Sie mehrere WDS-Server im Netzwerk, müssen Sie darauf achten, dass die Multicast-IP-Adressen nicht kollidieren. Ansonsten besteht die Gefahr eines übermäßigen Datenverkehrs. Um neue Multicastübertragungen zu aktivieren, klicken Sie mit der rechten Maustaste auf den Menüpunkt *Multicastübertragungen* und wählen im Kontextmenü den Befehl *Multicastübertragung erstellen* aus.

Abbildg. 16.18 Konfigurieren der Multicastübertragungen im Netzwerk



Anschließend geben Sie einen Namen der Übertragung ein und wählen das Installationsabbild aus, das verwendet werden soll. Interessant wird die Konfiguration auf der nächsten Seite des Assistenten, auf dem die Multicastübertragung ausführlicher konfiguriert wird.

Mit der Funktion *Cast (automatisch)* wird angegeben, dass eine Multicastübertragung des ausgewählten Abbilds beginnt, sobald von einem Client ein Installationsabbild angefordert wird. Wenn dasselbe Abbild noch von anderen Clients angefordert wird, werden auch diese in die bereits gestartete Sitzung eingebunden. Mit der Option *Cast (geplant)* werden die Startbedingungen für Multicast speziell festgelegt. Basis für diese Einstellung ist die Anzahl der Clients, die ein Abbild zu einer bestimmten Zeit anfordern. Daten werden nur dann über das Netzwerk übertragen, wenn diese von Clients angefordert werden.

Wenn die Übertragung als geplante Umwandlung konfiguriert wurde, mindestens ein Client verbunden ist und die Übertragung noch nicht gestartet wurde, können Sie mit der rechten Maustaste die Übertragung auswählen und auf *Starten* klicken. KlickenSie mit der rechten Maustaste auf die Übertragung, kann diese beendet werden. Die Clientinstallationen werden nicht dabei nicht gelöscht, sondern lediglich auf Unicast umgestellt. Deaktivieren Sie die Übertragung über das Kontextmenü, wird die bereits begonnene Installation von Clients fortgesetzt. Es werden jedoch keine neuen Clients in die Übertragung eingebunden. Die Übertragung wird anschließend gelöscht, nachdem die Installation aller aktuellen Clients abgeschlossen ist. Clientcomputer können auch mit dem Tool *Wdsmcast.exe*, ein Befehlszeilen-Tool des Windows AIK, an einer Übertragung teilnehmen.

In den Eigenschaften des Servers kann auf der Registerkarte *Netzwerkeinstellungen* das Verhalten des Servers bezüglich Multicast konfiguriert werden (Abbildung 16.19).

TIPP Werden im Unternehmen mehrere WDS-Server für Multicast konfiguriert, sollte in den Eigenschaften jedes Servers auf der Registerkarte *Netzwerkeinstelllungen* ein anderer IP-Bereich eingestellt werden, da sich sonst Datenpakete überlappen können und die Netzwerkbelastung stark ansteigt.

Abbildg. 16.19 Konfigurieren der Multicasteinstellungen für einen Server

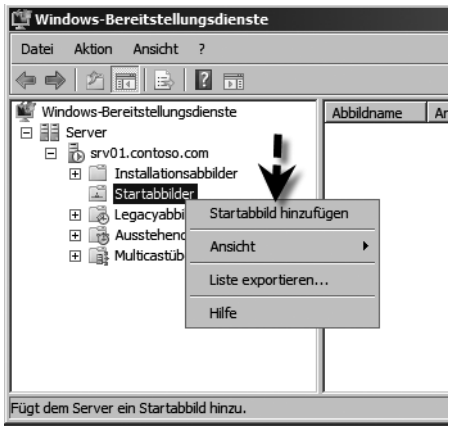
Verwalten und installieren von Abbildern

Die Installation von Clientcomputern über den WDS erfolgt über die bereits erwähnten Abbilder. Bei Startabbildern handelt es sich um Images, die lediglich Windows PE 2.0, also die Installationsumgebung des Servers laden. Installationsabbilder sind schließlich die Abbilder, über die zum Beispiel Windows Vista installiert werden kann.

Startabbilder verwalten

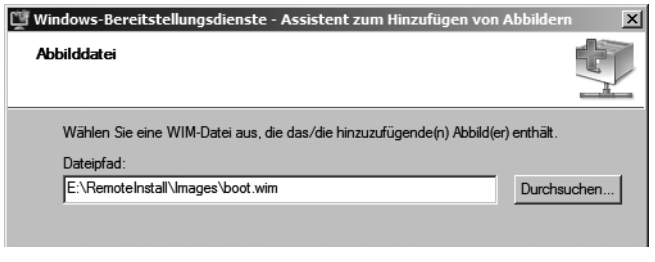
Startabbilder kommen dann zum Einsatz, wenn Sie eine automatisierte Vista-Installation über Antwortdateien durchführen wollen und das Business Desktop Deployment 2007 mit der Installationsmethode Lite Touch Installation (LTI) verwenden. Bei dieser Installationsmethode findet die Installation von Windows Vista oder Windows Server 2008 unabhängig von den Windows-Bereitstellungsdiensten über eine Antwortdatei statt. Der WDS startet dazu auf dem Client lediglich die Windows PE-Umgebung. Die weitere automatisierte Installation wird über das BDD oder einer Antwortdatei vorgenommen. Um ein Startabbild hinzuzufügen, wird zunächst die Verwaltungsoberfläche der WDS gestartet. Als Nächstes wird der Konsoleneintrag *Startabbilder* mit der rechten Maustaste angeklickt und über das Kontextmenü der Befehl *Startabbild hinzufügen* aufgerufen (Abbildung 16.20).

Abbildg. 16.20 Hinzufügen von Startabbildern zu den Windows-Bereitstellungsdiensten



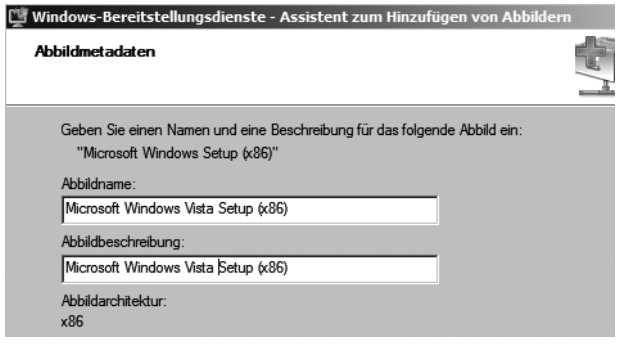
Im nächsten Fenster wird das Windows PE-Abbild ausgewählt, mit dem der Computer gestartet werden soll. Hier kann entweder ein eigenes Abbild erstellt und bearbeitet werden, wie bereits in diesem Kapitel besprochen, oder es wird das Standardabbild *boot.wim* aus dem Verzeichnis *sources* auf der Windows Vista oder Windows Server 2008-DVD verwendet. Dieses sollte vorher auf die Festplatte des Servers kopiert werden.

Abbildg. 16.21 Auswählen des Startabbildes



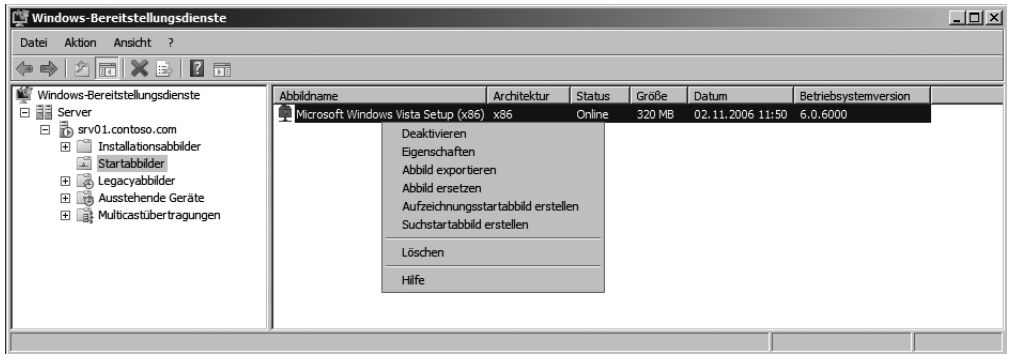
Auf der nächsten Seite wird der Name sowie die Beschreibung des Abbildes angezeigt und kann bearbeitet werden. Bestätigen Sie die restlichen Fenster, damit das Startabbild dem Server hinzugefügt wird.

Abbildg. 16.22 Konfigurieren der Daten für das Startabbild



Sobald das Startabbild dem Server hinzugefügt wurde, wird es in der Verwaltungskonsole als Online angezeigt. Über das Kontextmenü kann das Abbild bearbeitet oder andere Abbilder aus diesem Abbild erstellt werden (Abbildung 16.23).

Abbildg. 16.23 Anzeigen und verwalten der Startabbilder

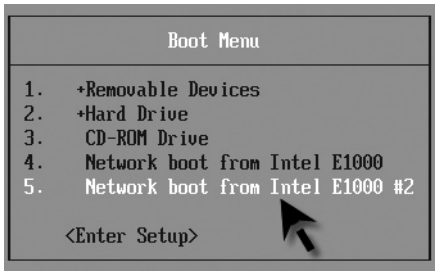


Startabbilder können auch über die Befehlszeile mit dem Befehl *wdsutil /Add-Image /ImageFile:<Pfad zur *.wim-Datei> /ImageType:boot* hinzugefügt werden.

Computer über WDS booten

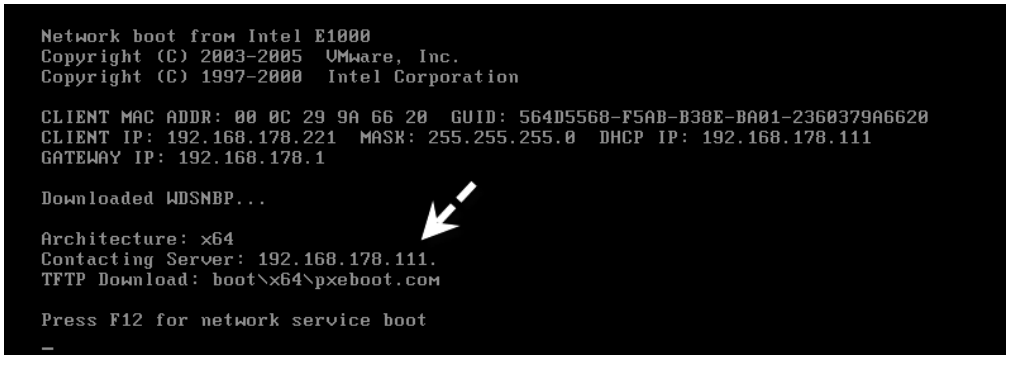
Sobald die Windows-Bereitstellungsdienste installiert und konfiguriert sind und ein Startabbild hinzugefügt wurde, können Computer über das Netzwerk gebootet werden. Achten Sie darauf, dass die Netzwerkkarte des Computers PXE beherrscht und der DHCP-Server korrekt mit der Option 60 konfiguriert wurde.

Abbildg. 16.24 Booten eines Computers über das Netzwerk



Sobald sich der Computer erfolgreich mit dem WDS-Server verbindet, erhält er eine IP-Adresse zugewiesen und Windows PE wird auf diesem Computer gestartet (Abbildung 16.25).

Abbildg. 16.25 Beim Booten über das Netzwerk wird zunächst der WDS-Server kontaktiert



Nach Bestätigung des Netzwerkboot-Vorganges startet der Computer mit dem Startabbild, das auf dem Computer hinterlegt worden ist (Abbildung 16.26).

Abbildg. 16.26 Booten von Windows über das Netzwerk auf dem WDS-Server

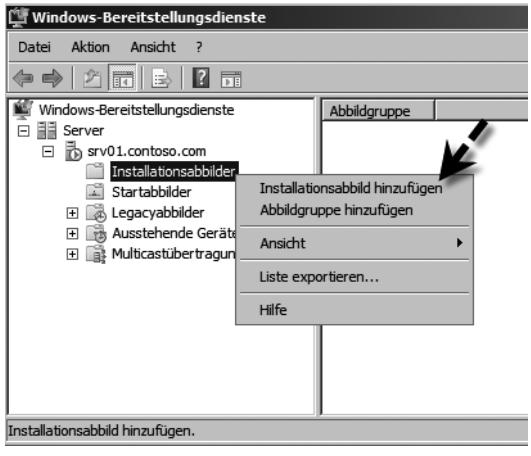
Windows PE wird anschließend gestartet. Ein nacktes Windows PE ohne angepasste Antwortdatei hat allerdings keinen Nutzen. Nur zusammen mit Mechanismen des Business Desktop Deployments 2007 macht die Verwendung von Startabbildern Sinn.

Installationsabbilder verwenden

Installationsabbilder sind Abbilder, über die Windows Vista oder Windows Server 2008 auf Basis eines Image installiert wird. Entweder erstellen Sie mit ImageX ein angepasstes Abbild, wie zu Beginn des Kapitels besprochen, oder verwenden zu Testzwecken das Standardabbild *install.wim* von Windows Vista oder Windows Server 2008 aus dem Verzeichnis *\Sources* auf der DVD. Installationsabbilder werden in Abbildgruppen zusammengefasst. Bei der Erstellung des ersten Installationsabbildes wird automatisch eine erste Abbildgruppe erstellt.

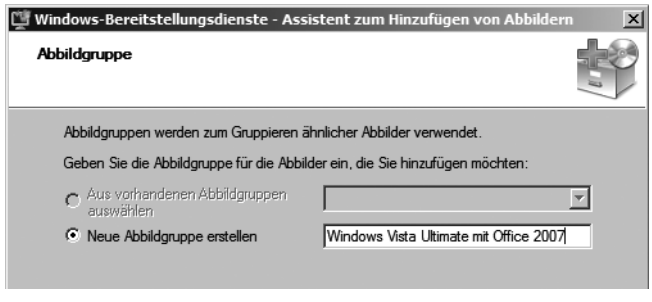
Um ein Installationsabbild zu integrieren, klicken Sie in der WDS-Verwaltungskonsole mit der rechten Maustaste auf *Installationsabbilder* und wählen im Kontextmenü den Befehl *Installationsabbild hinzufügen* aus (Abbildung 16.27).

Abbildg. 16.27 Hinzufügen eines Installationsabbilds zum WDS-Server



Im ersten Fenster kann die Abbildgruppe ausgewählt werden, in der das Installationsabbild integriert wird. Ist noch keine Abbildgruppe vorhanden, kann eine Abbildgruppe erstellt werden.

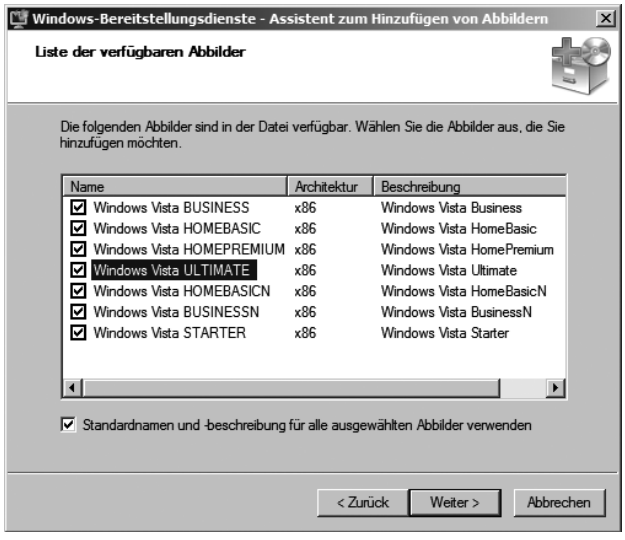
Abbildg. 16.28 Erstellen einer neuen Abbildgruppe für ein neues Installationsabbild



Im nächsten Fenster wird wieder die Image-Datei ausgewählt. Enthält ein Image mehrere Möglichkeiten und Windows-Editionen, wird im nächsten Fenster festgelegt, welche Edition installiert werden soll (Abbildung 16.29). Entfernen Sie das Häkchen bei denjenigen Editionen, die nicht verteilt werden

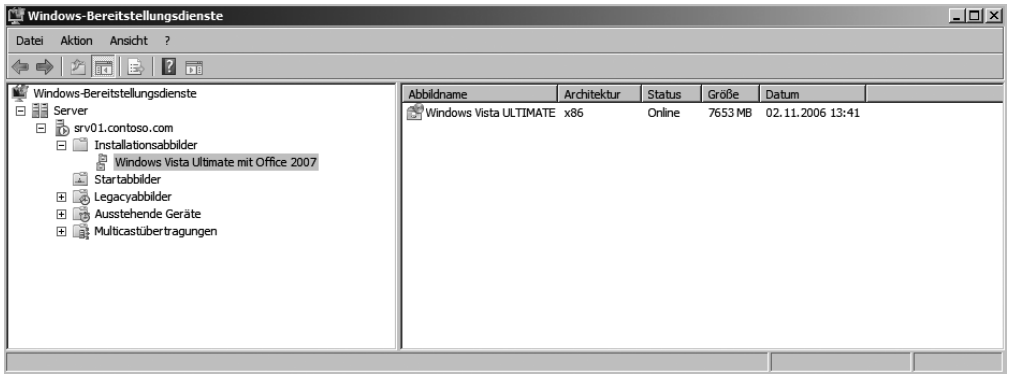
sollen. Deaktivieren Sie das Kontrollkästchen *Standardnamen und -beschreibung für alle ausgewählten Abbilder verwenden*, wenn Sie eigene Namen festlegen wollen. Auf der nächsten Seite erhalten Sie eine Zusammenfassung Ihrer Auswahl angezeigt und das Abbild wird anschließend hinzugefügt.

Abbildg. 16.29 Auswählen der Abbilder, die in der Image-Datei enthalten sind



Das Installationsabbild wird unterhalb seiner Gruppe angezeigt und kann nachträglich bearbeitet werden. Es lassen sich beliebige weitere Installationsabbilder hinzufügen, sodass bei der Betriebssystemauswahl auf dem Client weitere Optionen zur Verfügung stehen.

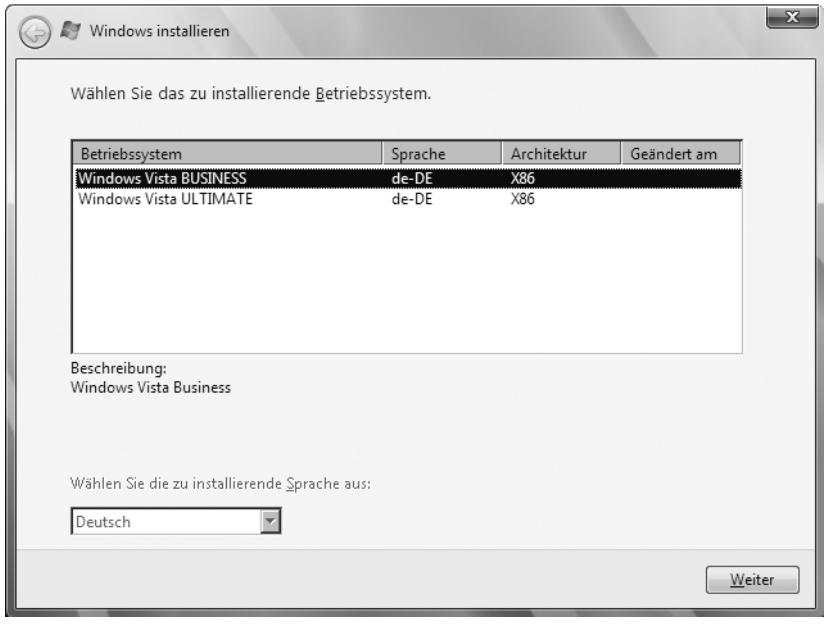
Abbildg. 16.30 Anzeigen der Installationsabbilder in der WDS-Verwaltungskonsole



Nach dem Hinzufügen können Sie einen Computer einrichten und das Image installieren lassen. Durch das konfigurierte Startabbild wird der Computer gebootet und durch die integrierten Installationsabbilder kann das zu installierende Betriebssystem auf dem Computer ausgewählt werden. Diese Installation kann auch vollkommen automatisiert durchgeführt werden. Darauf kommen wir später in diesem Kapitel noch ausführlicher zu sprechen.

Über die Befehlszeile wird ein Installationsabbild mit dem Befehl *wdsutil /add-image /ImageFile:<Pfad> /ImageType:install /ImageGroup:<Abbildgruppe>* hinzugefügt. Mit der zusätzlichen Option */SingleImage:<Bezeichnung>* kann nur ein einzelnes Image der WIM-Datei ausgewählt werden.

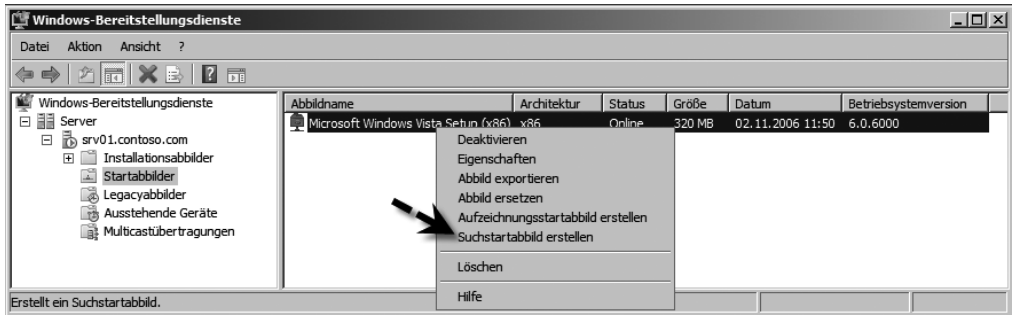
Abbildg. 16.31 Windows über WDS installieren



Suchstartabbilder verwenden

Suchstartabbilder sind Abbilder für Computer, die kein PXE-Boot über das Netzwerk beherrschen. Dazu wird ein Datenträger erstellt, mit dem der entsprechende Computer gebootet wird und sich mit dem WDS-Server verbinden kann. Suchstartabbilder werden über ein Startabbild erstellt. Klicken Sie dazu das Suchstartabbild mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Suchstartabbild erstellen* aus (Abbildung 16.32).

Abbildg. 16.32 Starten des Assistenten zum Erstellen eines Suchstartabbildes



Es öffnet sich ein neues Fenster, auf dem mehrere Eingaben für das Suchstartabbild vorgenommen werden können. Legen Sie die Beschreibung des Abbildes fest sowie den Namen und den Speicherort der zu erstellenden WIM-Datei. Auch der WDS-Server, der auf Anfragen dieses Clients antworten soll, wird hier festgelegt. Achten Sie darauf, dass für Suchstartabbilder immer nur ein WDS-Server konfiguriert werden kann.

Abbildg. 16.33 Konfigurieren eines Suchstartabbildes

Haben Sie alle Daten konfiguriert, wird das Abbild über *Weiter* erstellt. Das Abbild ist allerdings nicht als bootfähige ISO-Datei vorhanden, sondern wird als WIM-Image erstellt. Da sich aber der Client nicht mit dem WDS-Server verbinden kann, bringt das WIM-Image des Suchstartabbildes an dieser Stelle nicht viel und muss daher zunächst in eine ISO-Datei umgewandelt werden. Anschließend kann diese auf CD gebrannt und der Computer mit dieser CD gebootet werden. Um diese Datei in eine ISO-Datei umzuwandeln, verwenden wir den Weg, den wir bereits bei der Erstellung eines Windows PE-Datenträgers vorgeschlagen haben:

1. Kopieren Sie die Datei des Suchstartabbildes auf einen Computer, auf dem das WAIK installiert ist.
2. Öffnen Sie die Windows PE-Eingabeaufforderung.
3. Geben Sie den Befehl *copype x86 c:\WinPe* ein.
4. Löschen Sie jetzt die Datei *boot.wim* im Verzeichnis *C:\WinPe\ISO\sources*.
5. Kopieren Sie die WIM-Datei des Suchstartabbildes in dieses Verzeichnis und stellen Sie sicher, dass diese die Bezeichnung *boot.wim* hat.
6. Geben Sie den Befehl *oscdimg –n –bc:\winpe\etfsboot.com c:\winpe\ISO c:\winpe\winpe.iso* ein. Verwenden Sie als Verzeichnisnamen den Namen, den Sie bei sich verwendet haben und in dem sich die PE-Dateien befinden (Abbildung 16.34). Das Tool erstellt im Anschluss die ISO-Datei in der Befehlszeile.
7. Der Computer kann jetzt mit der CD gebootet werden und wird mit dem hinterlegten WDS-Server verbunden.

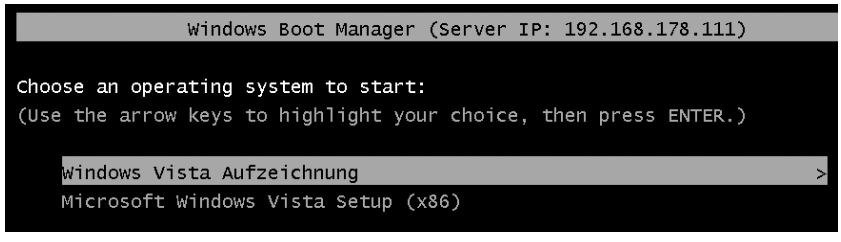
Aufzeichnungsstartabbilder verwenden

Aufzeichnungsabbilder sind eine Alternative zum beschriebenen Weg, über ImageX ein Abbild zu erstellen. Der Unterschied ist, dass mit diesem Aufzeichnungsstartabbild der Clientcomputer über PXE gebootet wird und ein Aufzeichnungsabbild auf dem WDS-Server erstellt wird. Aufzeichnungsabbilder werden wie Suchstartabbilder auf Basis von Startabbildern erstellt. Klicken Sie in der WDS-Konsole mit der rechten Maustaste auf das Startabbild, auf dessen Basis Sie das Aufzeichnungsstartabbild erstellen wollen, und wählen *Aufzeichnungsstartabbild erstellen* aus. Im folgenden Fenster muss wieder der Name des Abbildes sowie der Speicherort für die WIM-Datei des Abbildes ausgewählt werden.

Abbildg. 16.34 Erstellen eines Aufzeichnungsstartabbildes

Nachdem das Abbild erstellt wurde, muss dieses noch als zusätzliches Startabbild hinzugefügt werden. Gehen Sie dazu genauso vor wie beim Hinzufügen des ersten Startabbildes weiter vorne in diesem Kapitel. Sind mehrere Startabbilder konfiguriert, kann auf den Client-Computern standardmäßig ausgewählt werden, welches verwendet werden soll (Abbildung 16.35).

Abbildg. 16.35 Auswählen des Startabbildes, mit dem der Computer gestartet werden soll



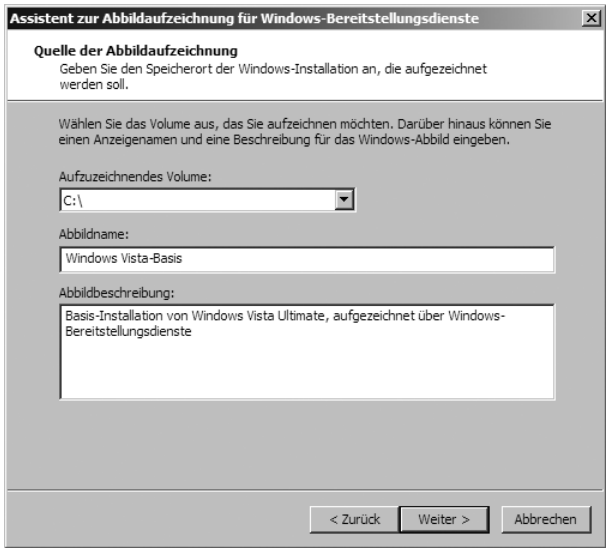
Wird ein Computer über ein Aufzeichnungsstartabbild gestartet, erscheint der Assistent, mit dem ein Image des Computers erstellt und über das Netzwerk auf dem WDS-Server gespeichert werden kann (Abbildung 16.36).

Abbildg. 16.36 Starten des Assistenten zum Aufzeichnen einer Windows Vista-Installation.

Auf der nächsten Seite des Assistenten wird die Partition ausgewählt, von der eine Aufzeichnung gemacht werden soll, sowie die Beschreibung des Images konfiguriert (Abbildung 16.37). Nachdem die Partition ausgewählt wurde, gelangen Sie mit *Weiter* zur nächsten Seite des Assistenten.

ACHTUNG Vom Assistenten zur Abbildaufzeichnung für die Windows-Bereitstellungsdienste werden nur die mithilfe von *Sysprep.exe* vorbereiteten Laufwerke angezeigt.

Abbildg. 16.37 Auswählen der Partition, die aufgezeichnet werden soll



Als Nächstes wird festgelegt, ob die Daten der Aufzeichnung über den Explorer auf einem normalen Verzeichnis oder dem WDS gespeichert werden sollen. Auch die jeweilige Abbildgruppe kann an dieser Stelle ausgewählt werden.

Abbildg. 16.38 Auswählen des Speicherortes der Abbildaufzeichnung

Automatische Namensgebung für Clients konfigurieren

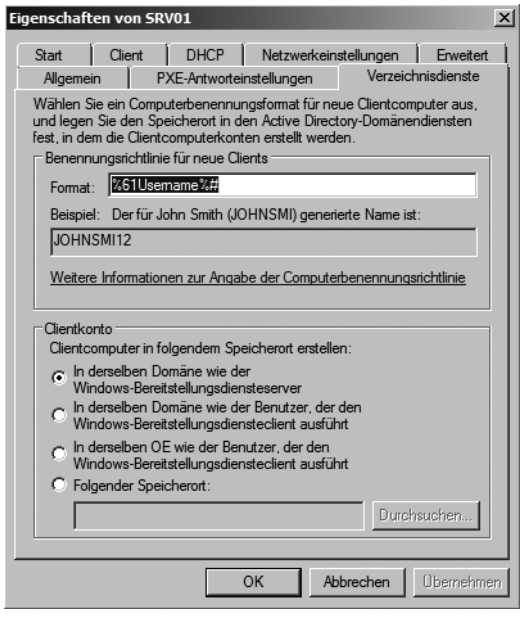
Clientcomputer werden bei der Installation über WDS automatisch an die Windows-Domäne angebunden und entsprechend benannt. In den Eigenschaften des Servers auf der Registerkarte *Verzeichnisdienste* kann diese Funktion konfiguriert werden.

Wird die Installation nicht über eine Antwortdatei gesteuert, in der auch die Namen der Computer angegeben werden, besteht die Möglichkeit an dieser Stelle in der WDS-Konsole eine Richtlinie zu konfigurieren. Die automatische Benennungsrichtlinie basiert auf dem Namen des Benutzers, der sich am WDS zur Installation anmeldet. Dabei wird eine inkrementelle Zahl hinzugefügt, um sicherstellen, dass der Computername eindeutig ist. Über Variablen kann der Name gesteuert werden:

- **%First** Der Vorname des Benutzers wird als Computername verwendet.
- **%Last** Der Nachname des Benutzers wird als Computername verwendet.
- **%Username** Der Benutzername wird als Computername verwendet.
- **%MAC** Die MAC-Adresse der Netzwerkkarte wird als Computername verwendet.
- **%[0][n]#** Wenn Sie die Zahl im Namen mit einer Null auffüllen möchten, geben Sie zusätzlich eine 0 an. Verwenden Sie zum Beispiel *%05#*, wird eine fünfstellige Zahl zwischen 00001 und 99999. verwendet.

Soll die Länge des Computernamens auf vier Zeichen des Nachnamens des Benutzers und einer angefügten dreistelligen Zahl begrenzt werden, geben Sie *%4Last%03#* ein. Soll der Computername aus den ersten drei Buchstaben des Vornamens des Benutzers und den ersten drei Buchstaben des Nachnamens des Benutzers und einer dreistelligen Zahl bestehen, geben Sie die Zeichenfolge *%3First%3Last%03#* ein.

Abbildg. 16.39 Konfigurieren der Benenennungsrichtlinie für Computer

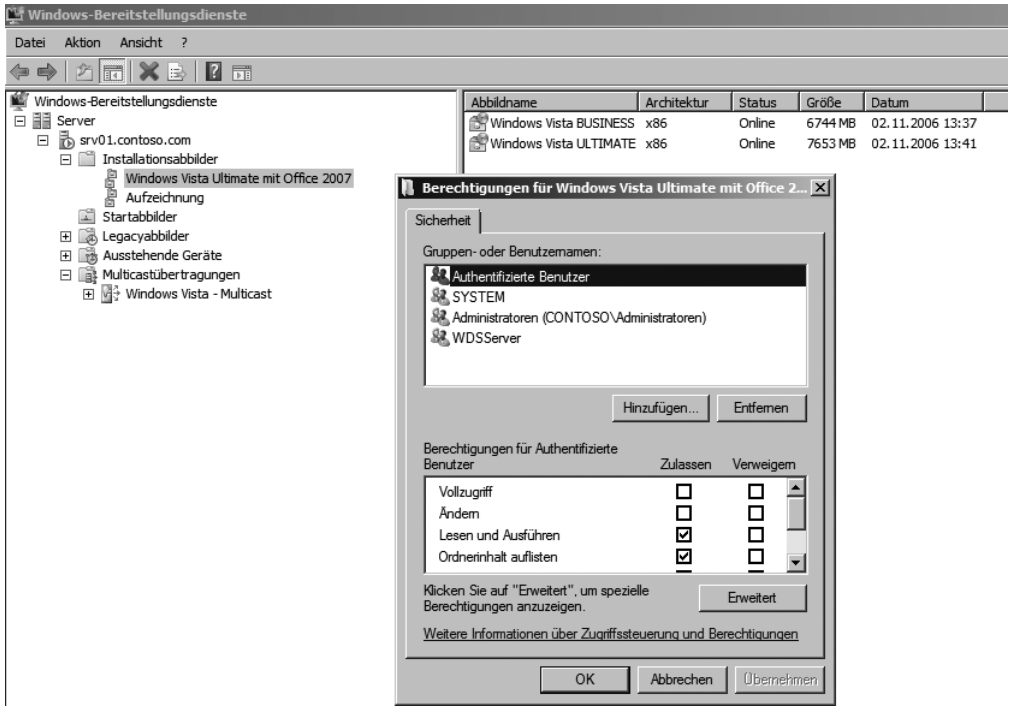


ACHTUNG Ein Computername darf aus maximal 15 Zeichen bestehen. Mit der Standardrichtlinie sind jedoch Namen mit einer Länge von bis zu 63 Zeichen möglich. Wenn ein Name mit einer Länge von mehr als 15 Zeichen generiert wird, werden alle Zeichen abgeschnitten, die auf die ersten 15 folgen, und der Computer kann der Domäne in diesem Fall nicht beitreten. Im Computernamen dürfen nur Standardzeichen enthalten sein. Die zugelassenen Zeichen sind: alle Großbuchstaben (A-Z), Kleinbuchstaben (a-z), Zahlen (0-9) und der Bindestrich (–).

Berechtigungen für Abbilder verwalten

Über das Kontextmenü der Abbildgruppe erreichen Sie mit dem Menüpunkt *Sicherheit* die Berechtigungsstruktur für die enthaltenen Abbilder. Wenn die Anwender im Unternehmen selbst das Abbild auswählen, achten Sie darauf, dass diese nur Leserechte für die Abbilder erhalten.

Abbildg. 16.40 Die Berechtigungen für Abbildgruppen lassen sich in der WDS-Konsole verwalten

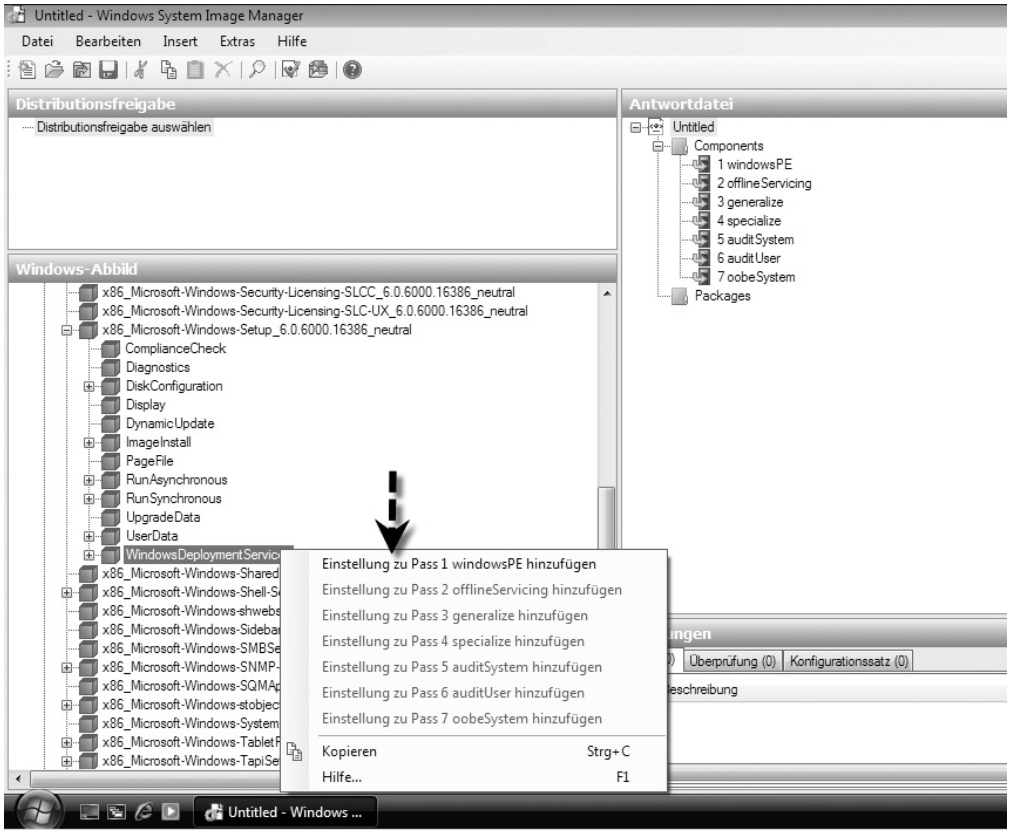


Unbeaufsichtigte Installation über die Windows-Bereitstellungsdienste

Erstellte Antwortdateien lassen sich für eine unbeaufsichtigte Installation von Windows Vista oder Windows Server 2008 auch in die Windows-Bereitstellungsdienste einbinden. Dazu muss die Antwortdatei allerdings so angepasst werden, dass die Anmeldedaten zum WDS-Server und das zu installierende Abbild angegeben werden:

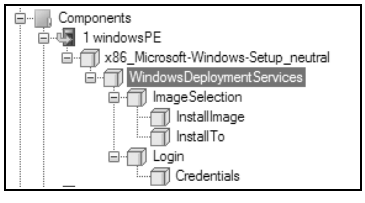
1. Öffnen Sie die Antwortdatei im Windows Systemabbild-Manager des WAIK.
2. Erweitern Sie im Bereich *Components* den Eintrag *x86_Microsoft-Windows-Setup_6.0.6000.16386_neutral*.
3. Klicken Sie den Eintrag *WindowsDeploymentServices* mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Einstellung zu Pass 1 windowsPE hinzufügen* aus. Damit kann dieser Eintrag für die Antwortdatei konfiguriert werden.

Abbildg. 16.41 Erweitern einer Antwortdatei zur Integration in die Windows-Bereitstellungsdienste



Nachdem der neue Zusatz der Antwortdatei hinzugefügt worden ist, kann dieser konfiguriert werden. Dazu stehen verschiedene Möglichkeiten zur Verfügung, die im mittleren Bereich des Fensters angezeigt werden.

Abbildg. 16.42 Bearbeiten der Antwortdatei zur Anpassung an den WDS



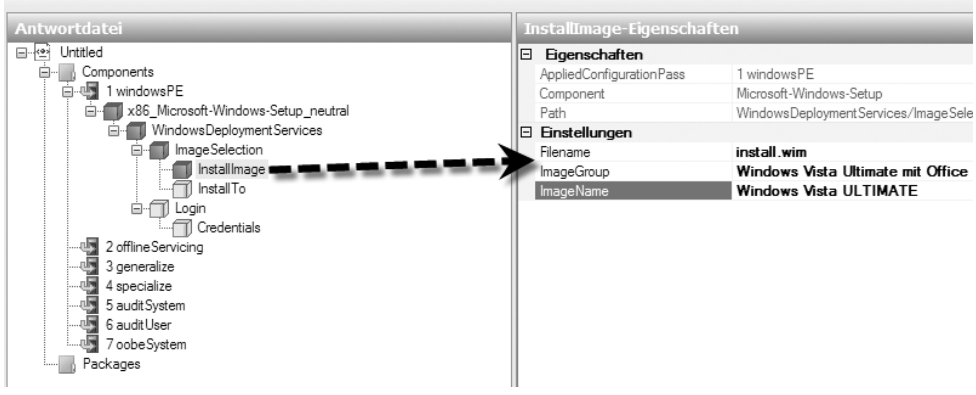
Um die Datei für WDS anzupassen, gehen Sie folgendermaßen vor:

1. Wählen Sie als Erstes den Eintrag *InstallImage* aus. Hier müssen verschiedene Eingaben erfolgen.
2. Unter *Filename* tragen Sie den Dateinamen des Installationsabbildes ein, das durch diese Antwortdatei über den WDS installiert werden soll. Hier wird nicht der Name des Abbildes, sondern der Name der entsprechenden WIM-Datei ausgewählt. Der Dateiname kann in den Eigen-

schaften des Installationsabbildes auf dem WDS auf der Registerkarte *Allgemein* angezeigt werden. Es genügt, den Namen der Datei anzugeben, der Pfad wird nicht benötigt.

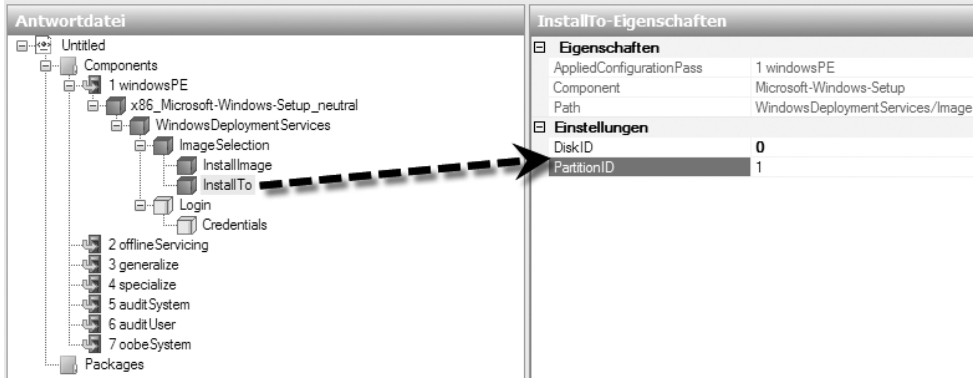
3. Bei *ImageGroup* wird der Name der Abbildgruppe eingegeben.
4. Bei *ImageName* geben Sie die Bezeichnung des Installationsabbildes auf dem WDS ein.

Abbildg. 16.43 Eintragen der notwendigen Daten für die WDS-Installation in den Eigenschaften der Antwortdatei



5. Als Nächstes wird der Punkt *Install To* in der Antwortdatei ausgewählt und die notwendigen Daten eingetragen.
6. Bei *DiskID* tragen Sie 0 ein, wenn die Installation auf der ersten Partition der ersten Festplatte durchgeführt werden soll. Hier wird die Festplatte ausgewählt.
7. Bei *PartitionID* tragen Sie 1 ein, wenn die Installation auf der ersten Partition der ersten Festplatte durchgeführt werden soll. Hier wird die Partition der ausgewählten Festplatte festgelegt.

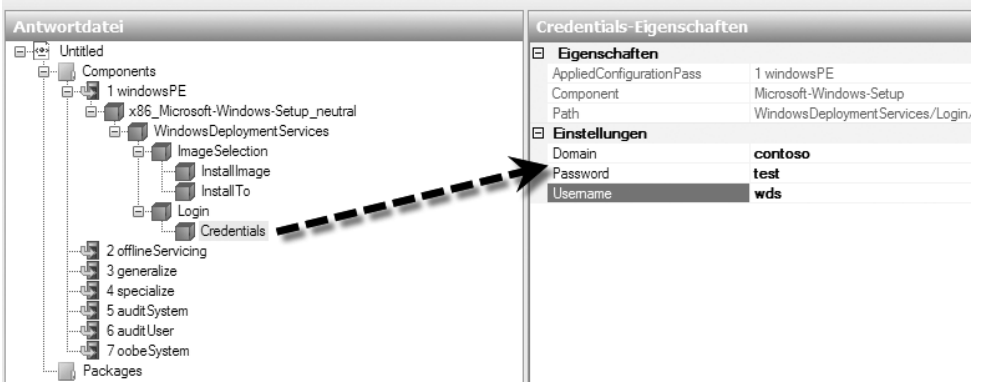
Abbildg. 16.44 Konfigurieren der Festplatte und Partition für die automatisierte Installation



8. Als Nächstes klicken Sie auf *Credentials*. Hier werden die Anmeldedaten für die Anbindung an den WDS hinterlegt. Die Anmeldedaten am WDS-Server werden in Klartext in der Antwortdatei abgelegt. Aus diesem Grund sollten Sie am besten einen Benutzernamen und ein Kennwort verwenden, das ausschließlich nur für die Installation über den WDS-Server verwendet wird.

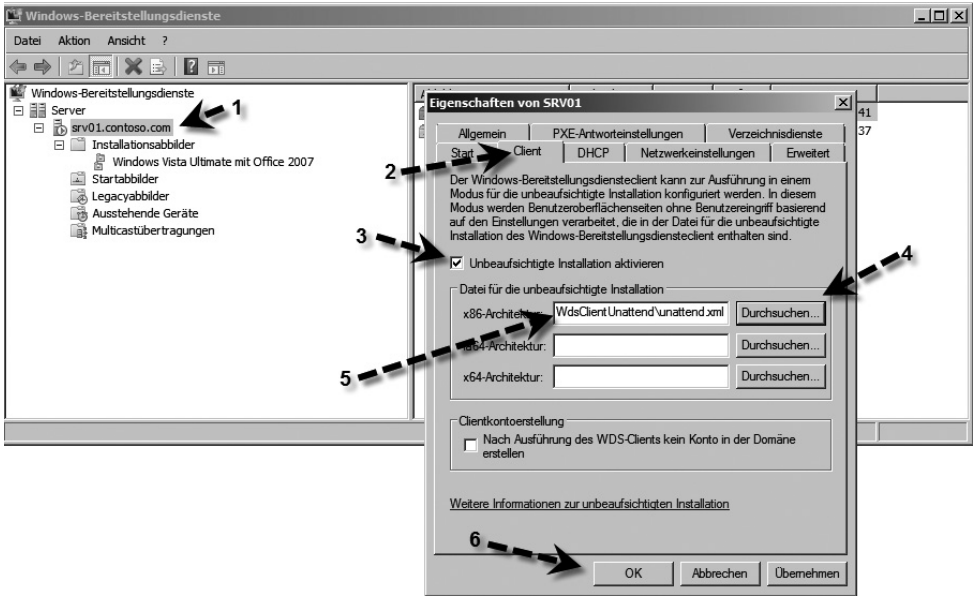
9. Unter *Domain* tragen Sie den Domänennamen der Domäne des Anwenders ein, der Zugriff auf den WDS-Server hat.
10. Unter *Password* legen Sie das Kennwort des Anwenders und unter *Username* den Benutzernamen fest.

Abbildg. 16.45 Konfigurieren der Anmeldedaten für die Anmeldung am WDS



Nachdem die Datei bearbeitet wurde, kopieren Sie diese in das Verzeichnis *WDSClientUnattend* in den Remoteinstallations-Ordner auf dem WDS-Server. Anschließend lässt sich die Antwortdatei in den Eigenschaften auf dem WDS-Server integrieren. Rufen Sie dazu in der WDS-Konsole die Eigenschaften des Servers auf und wechseln auf die Registerkarte *Client.* Aktivieren Sie die Option *Unbeaufsichtigte Installation aktivieren* und wählen Sie die gespeicherte Antwortdatei aus.

Abbildg. 16.46 Hinterlegen einer Antwortdatei für die automatisierte Installation



Beispiel einer Antwortdatei

Antwortdateien werden idealerweise über den Windows Systemabbild-Manager des WAIK verwaltet und erstellt. Die Antwortdateien stehen jetzt im XML-Format zur Verfügung und müssen nicht mehr unbedingt mit einem normalen Editor bearbeitet werden. Im folgenden Listing zeigen wir Ihnen eine typische Antwortdatei. Neben dem Windows Systemabbild-Manager können Sie zum Bearbeiten einer Antwortdatei auch einen beliebigen Editor verwenden, um zum Beispiel kleinere Änderungen durchzuführen.

Listing 16.3 Beispiel einer typischen Antwortdatei für die automatisierte Installation von Windows Vista oder Windows Server 2008

```
<?xml version="1.0" ?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
   <settings pass="windowsPE">
      <component name="Microsoft-Windows-Setup" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" processorArchitecture="x86">
         <WindowsDeploymentServices>
            <Login>
               <WillShowUI>OnError</WillShowUI>
               <Credentials>
                     <Username>username</Username>
                     <Domain>wds-dom</Domain>
                     <Password>my_password</Password>
                  </Credentials>
               </Login>
            <ImageSelection>
               <WillShowUI>OnError</WillShowUI>
               <InstallImage>
                  <ImageName>Windows Vista with Office</ImageName>
                  <ImageGroup>ImageGroup1</ImageGroup>
                  <Filename>Install.wim</Filename>
               </InstallImage>
                  <InstallTo>
                  <DiskID>0</DiskID>
                  <PartitionID>1</PartitionID>
               </InstallTo>
            </ImageSelection>
         </WindowsDeploymentServices>
         <DiskConfiguration>
            <WillShowUI>OnError</WillShowUI>
               <Disk>
                  <DiskID>0</DiskID>
                  <WillWipeDisk>false</WillWipeDisk>
                  <ModifyPartitions>
                     <ModifyPartition>
                        <Order>1</Order>
                        <PartitionID>1</PartitionID>
                        <Letter>C</Letter>
                        <Label>TestOS</Label>
                        <Format>NTFS</Format>
                        <Active>true</Active>
                        <Extend>false</Extend>
                     </ModifyPartition>
                  </ModifyPartitions>
            </Disk>
```

Listing 16.3 Beispiel einer typischen Antwortdatei für die automatisierte Installation von Windows Vista oder Windows Server 2008 *(Fortsetzung)*

```
         </DiskConfiguration>
      </component>
      <component name="Microsoft-Windows-International-Core-WinPE"
publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" processorArchitecture="x86">
         <SetupUILanguage>
            <WillShowUI>OnError</WillShowUI>
            <UILanguage>en-US</UILanguage>
         </SetupUILanguage>
         <UILanguage>en-US</UILanguage>
      </component>
   </settings>
</unattend>
```

Automatisieren der Installation über Abbilder

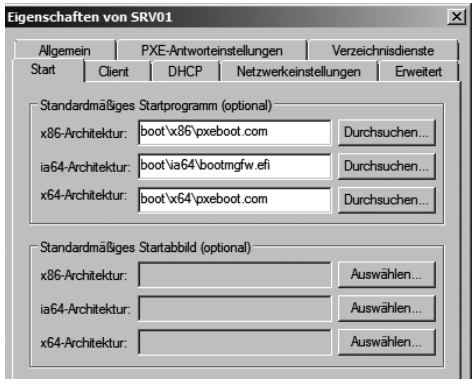
Die Automatisierung der Installation kann nicht nur in den Eigenschaften des WDS-Servers konfiguriert werden, sondern auch in den Eigenschaften des Abbildes. Auch hierzu müssen die Antwortdateien für die Abbilder angepasst und für WDS optimiert werden. In den Eigenschaften eines Installationsabbildes kann auf der Registerkarte *Allgemein* die Option *Abbildinstallation im Modus für unbeaufsichtigte Installation zulassen* aktiviert werden. Anschließend wählen Sie die entsprechende Antwortdatei aus (Abbildung 16.47). Die ausgewählte Datei wird automatisch in das Verzeichnis *\Images\<Abbildgruppe>\install\Unattend\ImageUnattend.XML* kopiert.

Abbildg. 16.47 Automatisieren der Installation über WDS auf Abbildebene

Automatisieren der Startabbilder

Die Installationsabbilder können zwar auf den beschriebenen Wegen automatisiert werden, allerdings sind die Vorgänge bis zur Auswahl der Installation noch nicht automatisiert. Anwender können auf dem PC in der Startabbildphase noch eingreifen, was häufig nicht erwünscht ist. Aus diesem Grund kann auch der komplette PXE-Bootvorgang automatisiert werden. WDS benutzt haupsächlich vier Netzwerk-Boot-Programme (NBP), um Clients an den Server anzubinden. Das standardmäßige Programm ist *Pxeboot.com*, das gestartet wird, wenn der Client auf seinem Computer den Netzwerkboot anfordert. Das Standardprogramm für den WDS-Server wird in den Eigenschaften des Servers in der WDS-Konsole auf der Registerkarte *Start* festgelegt (Abbildung 16.48). Das NBP *pxeboot.n12* bootet auch dann über das Netzwerk, wenn der Client nicht den Netzwerkboot anfordert. Über *Abortpxe.com* wird in keinem Fall über das Netzwerk gebootet, auch wenn der Client das anfordert. Das Programm *Wdsnbp.com* wiederum wird dazu verwendet, die Architektur des Computers sowie Anfragen, die genehmigt werden müssen, zu steuern.

Abbildg. 16.48 Festlegen des Standardstartprogrammes des WDS-Servers



Ebenfalls auf dieser Registerkarte legen Sie das Standardabbild fest, das beim Starten der Computer geladen werden soll. Für jede Architektur kann eine angepasste Auswahl der Architektur erfolgen. Wird an dieser Stelle das NBP *pxeboot.n12* hinterlegt, bootet der Rechner, auch ohne dass F12 gedrückt wird, im Netzwerkboot, zumindest wenn dies in der Reihenfolge so angegeben ist. Anschließend wird das Standardstartabbild geladen und der Computer beginnt mit der Installation.

Häufige Fehler und deren Behebung

In diesem Abschnitt gehen wir auf die häufigsten Probleme beim Einsatz mit den WDS sowie deren Lösungen ein.

64-Bit-Systeme können nicht installiert werden

Hierbei liegt häufig ein Problem bei der Datenübertragung oder dem BIOS des Clients vor. Der Computer meldet sich beim WDS-Server nicht als x64 und erhält daher auch kein x64-Abbild. Geben Sie auf dem Server den Befehl *wdsutil /set-server /architecturediscovery:yes* ein. In diesem Fall

wird der Server gezwungen, den Client zu überprüfen, was häufig funktioniert (Abbildung 16.49). Dieser Vorgang wird durch das bereits besprochene NBP *Wdsnbp.com* durchgeführt.

Abbildg. 16.49 Anzeigen der Architektur des Client-Computers für die automatisierte Installation

Alternativ zu dieser Lösung können Sie erzwingen, dass alle x64-basierten Clientcomputer x86-basierte Startdateien empfangen. Dazu konfigurieren Sie das Standardstartprogramm in den Einstellungen des Servers auf der Registerkarte *Start* so, dass das entsprechende Netzwerkstartprogramm (NBP) verwendet wird – beispielsweise *Pxeboot.com* unter *\RemoteInstall\boot\x86*.

Der Computer lädt das Startabbild, kann jedoch nicht auf ein Installationsabbild zugreifen

In diesem Fall liegt unter Umständen ein Netzwerkproblem vor, weil das Startabbild keinen Treiber für die Netzwerkkarte enthält. Öffnen Sie in diesem Fall mit der Tastenkombination ⇧+F10 eine Befehlszeile und geben dann *IPConfig* ein. Ist dem Client keine IP-Adresse zugewiesen, wurde der Treiber der Netzwerkkarte nicht installiert. Integrieren Sie über das WAIK einen passenden Treiber.

Aktivierung für Unternehmenskunden – Volume Activation (VA) 2.0

Für Windows Vista wird es keine Seriennummern geben, welche die notwendige Aktivierung von Windows Vista übergehen. Für Windows XP und Office 2003 hat Microsoft noch die Volume Activation 1.0 eingesetzt. Bei dieser Aktivierung haben Unternehmenskunden Seriennummern erhalten, die keine Aktivierung benötigten. Bei der neuen Volume Activation 2.0 gibt es solche Möglichkeiten nicht mehr. Alle Produkte, die unter die VA 2.0 fallen, müssen immer aktiviert werden. Microsoft stellt aber Tools und Funktionen wie das Volume Activation Management Tool (VAMT) oder den Schlüsselverwaltungsdienst (Key Management Service, KMS) zur Verfügung, über welche die Aktivierung automatisiert nach der Installation abgewickelt werden können.

HINWEIS Das Systemverhalten von Windows Server 2008 und Windows Vista sind nahezu identisch. Das heißt, alle Bereiche in den folgenden Abschnitten gelten sowohl für Windows Server 2008 als auch für Windows Vista.

Grundlegende Informationen zum Einsatz von Volume Activation (VA) 2.0

Alle Versionen von Windows Vista müssen immer auch aktiviert werden. Auch wenn Sie einen aktivierten Windows Vista-PC klonen wollen, müssen die installierten Klone erneut aktiviert werden. Zu diesem Zweck muss nach dem Klonen eines PCs mit *sysprep /generalize* unter anderem die Produktaktivierung zurückgesetzt werden. Bevor Sie einen PC klonen und *sysprep /generalize* ausführen, achten Sie darauf, dass der Registrywert *skiprearm*, den Sie im Schlüssel *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL* finden, auf *0* gesetzt ist. Hat dieser Eintrag einen anderen Wert, führen Sie *Sysprep* mit folgenden Optionen aus:

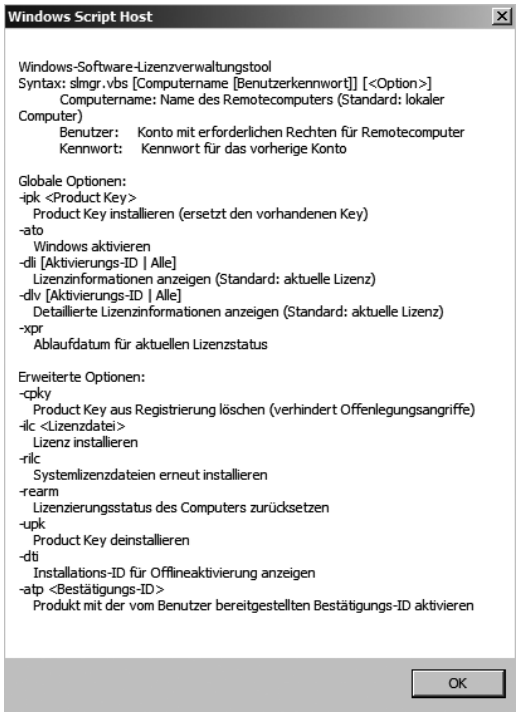
sysprep.exe /generalize /oobe /shutdown

Größeren Unternehmen stellt Microsoft für die Aktivierung eine neue Serverfunktionalität zur Verfügung, sodass die Aktivierung der Arbeitsstationen nicht über das Internet, sondern automatisiert über das Netzwerk abgewickelt werden kann. Dieser Dienst kann auch auf einem Windows Vista-PC installiert werden, setzt aber voraus, dass es im Netzwerk mindestens 25 PCs oder fünf Windows Server 2008-Computer gibt, wobei virtuelle Maschinen nicht mitgerechnet werden. Alternativ kann dieser Dienst unter Windows Server 2008 installiert werden. Die Lizenzschlüssel für Unternehmen laufen auch nach Aktivierung nicht mehr unbegrenzt, sie erlauben aber eine mehrfache Aktivierung. Mit Volume Activation 2.0 steht für Microsoft das Verhindern des Missbrauchs von Volumen-Lizenzschlüsseln im Vordergrund. Heute können sich Unternehmen nicht wirksam dagegen wehren, wenn ein Mitarbeiter, Dienstleister oder Dritte die eigenen Schlüssel weitergeben oder im Internet veröffentlichen. Zukünftig sind derartige Schlüssel wertlos, da nur der Originalinhaber die Verwendung der mit dem Schlüssel abgedeckten Lizenzen festlegen kann. Für Office 2007 gelten diese Einschränkungen nicht. Office 2007 fällt noch unter das Volume Activation 1.0. Hier erhalten Unternehmenskunden eine Seriennummer, die keine Aktivierung erfordert.

Volume Activation 2.0 unterstützt die zentrale Verwaltung der Volumen-Lizenzen über einen *Key Management Service (KMS)* oder über *Multiple Activation Keys (MAK)*. Der KMS-Dienst wird auf einem Computer mit einem eigenen Schlüssel aktiviert, welcher lediglich auf dem KMS-Host und nicht auf jedem einzelnen Computer zu finden ist. Der MAK wird auf den einzelnen Computern gespeichert, ist jedoch verschlüsselt und in einem vertrauenswürdigen Speicher aufbewahrt, so dass Benutzer diesen Schlüssel nie zu sehen bekommen und auch nicht nachträglich auslesen können. Als Schlüssel verwendet Microsoft *Cipher Block Chaining Message Authentication Code (CBC-MAC)* mit dem *Advanced Encryption Standard (AES)* als grundlegende Verschlüsselungstechnologie. Standardmäßig benötigen Windows Vista-Volumen-Lizenzversionen keine Eingabe eines Produktschlüssels während der Installation – der Computer muss lediglich innerhalb von 30 Tagen aktiviert werden. Volume Activation 2.0 erlaubt weiterhin Systemadministratoren die zentrale Verwaltung der eigenen Produktschlüssel. Dabei kann zwischen zwei verschiedenen Arten von Schlüsseln (MAK und KMS) und drei Aktivierungsmethoden (MAK Proxy Activation, MAK Independent Activation und KMS Activation ab 25 Windows Vista-Clients) gewählt werden.

Für die Verwaltung und die Abfrage von Lizenzinformationen auf Windows Vista- und Windows Server 2008-Computern stellt Microsoft das Skript *Slmgr.vbs* zur Verfügung, welches Sie über *Start/Ausführen* aufrufen (siehe auch die Kapitel 1 und 3). Nach dem Aufruf ohne eine bestimmte Option wird eine ausführliche Auflistung über alle möglichen Optionen angezeigt (Abbildung 16.50). Es werden allerdings nur die Optionen angezeigt, welche die Aktivierung basierend durch die eingegebene Seriennummer des Computers unterstützen, diese können daher differieren.

Abbildg. 16.50 Die Möglichkeiten der Lizenz-Verwaltung über das VBS-Skript *Slmgr.vbs*



Neben diesen Aktivierungsmethoden gibt es weiterhin die OEM Activation und Retail Activation:

- Bei der OEM Activation erfolgt eine Aktivierung vorab durch den OEM-Hersteller. Man kann an dem Computer beliebige Änderungen vornehmen. Lediglich das BIOS des Mainboards muss die OEM-spezifischen Informationen enthalten. Es wird nie eine Aktivierung erforderlich.
- Die Retail Activation kann ebenfalls durch den OEM erfolgen – in der Praxis führt diese aber der Endbenutzer durch. Er übermittelt während der Aktivierung die Product ID und einen Hardware-Hash von unterschiedlichen Teilen des PCs, die einzeln gewichtet werden. Im Gegensatz zu Windows XP ist bei Windows Vista keine Neuaktivierung erforderlich, solange die Festplatte nicht gewechselt wird.

Wenn ein Computer mit Windows Vista nach 30 Tagen nicht aktiviert wurde, wird dieser in den so genannten Reduced Functionality Mode (RFM) geschaltet. Bei diesem Modus kann mit dem PC nur eingeschränkt gearbeitet werden. Mit dem SP1 für Windows Vista ist dieser Modus etwas entschärft worden. Zum Beispiel besteht nur die Möglichkeit, per Internet Explorer auf die lokalen Daten der Festplatte zuzugreifen.

Multiple Activation Key (MAK)

Bei der MAK-Aktivierung findet ein ähnlicher Prozess statt wie bei MSDN- oder Action Pack-Versionen für Microsoft Partner. Jeder Produktschlüssel kann für eine bestimmt Anzahl an Computern verwendet werden, die dann auch aktiviert werden können. Die MAK-Aktivierung muss nur einmal durchgeführt werden und erlaubt beliebige Änderungen an der Hardware des Computers. Die MAK-Aktivierung kann über das Internet oder telefonisch durchgeführt werden. Vor allem bei mobilen Computern, die sich nicht ständig mit dem Netzwerk verbinden, ist die MAK-Aktivierung der bessere Weg, da keine ständige Verbindung zum KMS-Server benötigt wird und nur einmal aktiviert werden muss. Bei der Aktivierung über KMS müssen sich die Clients alle 180 Tage wieder mit dem Server verbinden können, der den KMS-Dienst zur Verfügung stellt. Wie viele Clients mit einem MAK aktiviert werden können, hängt vom individuellen Vertrag ab, den Ihr Unternehmen mit Microsoft geschlossen hat.

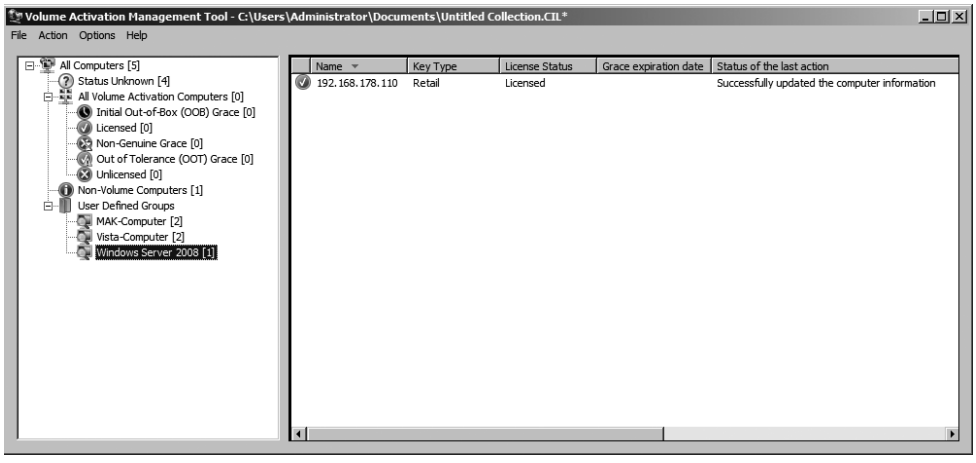
Wenn Sie die Aktivierung per MAK über das Internet durchführen und einen Proxyserver, zum Beispiel ISA Server 2004 oder 2006, einsetzen, sollten Sie nicht mit der Standardauthentifizierung arbeiten, da der Aktivierungsprozess keine Authentifizierungsinformationen übertragen kann. Wenn Sie Regeln auf dem ISA Server erstellen wollen, müssen Sie den Clients Zugriff auf die folgenden Internetseiten gewähren:

- http://go.microsoft.com/*
- https://sls.microsoft.com/*
- https://sls.microsoft.com:443
- http://crl.microsoft.com/pki/crl/products/MicrosoftRootAuthority.crl
- http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunications.crl
- http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureCommunications.crl
- http://crl.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl
- http://www.microsoft.com/pki/crl/products/MicrosoftProductSecureServer.crl

Es gibt zwei verschiedene Varianten der MAK-Aktivierung:

- **MAK Proxy Activation** Bei dieser Variante können mehrere Computer durch eine Verbindung bei Microsoft aktiviert werden. Microsoft stellt dazu das *Volume Activation Management Tool (VAMT)* zur Verfügung. Mit dem Tool steht eine grafische Oberfläche zur Verwaltung der Produktschlüssel zur Verfügung (Abbildung 16.51).
- **MAK Independent Activation** Bei dieser Variante muss jeder Computer durch eine eigene Verbindung bei Microsoft aktiviert werden.

Abbildg. 16.51 Mit dem Volume Activation Management Tool verwalten Sie effizient die Lizenzen der Client-Computer und Server im Netzwerk



Key Management Service (KMS)-Activation

Bei dieser Variante der Aktivierung können Sie die Aktivierung der eingesetzten Windows Vista- oder Windows Server 2008-Computer über einen lokalen Server durchführen. Eine Verbindung zu Microsoft ist nicht notwendig. Dazu muss auf einem Computer mit Windows Vista oder Windows Server 2008 der Schlüsselverwaltungsdienst (Key Management Service, KMS) installiert werden. Die Clients müssen sich nach Aktivierung alle 180 Tage erneut beim KMS-Server reaktivieren. Ab einem Netzwerk von 25 Computern kann dieser Dienst zur Aktivierung verwendet werden. Der Dienst lässt sich auch auf mehreren Domänencontrollern installieren, um die Ausfallsicherheit zu erhöhen. Beim Verbindungsaufbau versucht ein Client den ersten KMS-Host zu verwenden, der auf die Anfrage antwortet. Anschließend wird dieser KMS-Host in den Cache des Clients geschrieben. Bei der nächsten Aktivierung wird dann versucht, direkt diesen KMS-Host zu verwenden. Wenn ein KMS-Host nicht antwortet, versucht ein Client automatisch andere KMS-Hosts zu erreichen, für die SRV-Records zur Verfügung stehen. Wenn ein KMS-Host aus dem Netzwerk entfernt wird, muss dessen SRV-Record manuell gelöscht werden.Vista-Computer, die durch KMS-Aktivierung aktiviert worden sind, müssen sich alle 180 Tage neu bei dem KMS-Server melden und die Aktivierung erneuern.

Die Computer versuchen nach der Installation alle zwei Stunden eine Verbindung zum KMS-Server aufzubauen und müssen diesen innerhalb von 30 Tagen erreichen können. Die Computer können sich auf zwei verschiedene Varianten mit dem KMS-Server verbinden, dabei werden für jede Aktivierung ungefähr 250 Bytes übertragen:

Auto-discovery – Bei dieser Variante wird die Verbindung durch einen SRV-Record auf den DNS-Servern gelöst, was innerhalb von Active Directory der beste Weg ist. Für die Unterstützung der Funktion müssen die dynamischen Updates für die DNS-Zone aktiviert werden. Der Standardport für den Verbindungsaufbau zur Aktivierung ist 1688. Es wird eine RPC-over-TCP/IP-Verbindung aufgebaut. Der Port kann auch angepasst werden. Bei der Installation und Aktivierung des Key

Management Service für die Volumen Aktivierung 2.0 wird automatisch ein DNS-Eintrag erstellt, wenn die dynamische Aktualisierung der Zone aktiviert wurde. Sie können den SRV-Record für Autodiscovery auch manuell auf den DNS-Servern erstellen. Dazu sind folgende Daten zu verwenden:

Name=vlmcs._TCP

Type=SRV

Priority = 0

Weight = 0

Port = 1688

Hostname = <FQDN des KMS host>

Um die Funktionalität und den Verbindungsaufbau zu einem KMS-Host zu testen, können Sie mit *Nslookup* und der Syntax *nslookup –type=srv _vlmcs._tcp* die Namensauflösung testen. Der Client muss dann zum Beispiel folgende Antwort erhalten:

vlmcs._tcp.contoso.com SRV service location:

priority = 0

weight = 0

port = 1688

svr hostname = KMS1.contoso.com

Eine weitere Möglichkeit ist die manuelle Verbindung der Clients zum KMS-Host mit *Direct Connection*. Hier wird durch den Administrator ein spezieller KMS-Host und ein Port manuell festgelegt. Der Standardport für den Verbindungsaufbau zur Aktivierung ist auch hier 1688. Es wird eine RPC-over-TCP/IP-Verbindung aufgebaut. Mit Volumenlizenzschlüsseln ist es möglich, eine bestimmte Anzahl von Computern mit der gleichen Seriennummer zu installieren und anschließend zu aktivieren. Solche Lizenzschlüssel wird es nur für Windows Vista Business Edition und Windows Vista Enterprise Edition geben. Für Windows Vista Ultimate Edition sind derzeit keine Volumenlizenzschlüssel geplant.

Reduced Funtionality Mode (RFM)

Wenn ein Windows Vista- oder Windows Server 2008-Computer nach 30 Tagen nicht aktiviert wird, schaltet dieser in den Reduced Fuctionality Mode (RFM). Wenn sich ein Anwender bei diesem Modus anmeldet, erhält er mehrere Möglichkeiten, muss aber Vista (am besten mit SP1) oder Windows Server 2008 innerhalb einer Stunde aktivieren. Zum Ende der Frist erinnert der Computer in immer kürzeren Abständen daran, dass er noch aktiviert werden muss. Das gilt für Windows Vista und für Windows Server 2008. Mit dem Befehl *slmgr.vbs –rearm* kann die Testphase zusätzlich noch dreimal um weitere 30 Tage, also insgesamt auf 120 Tage verlängert werden. Wenn Sie die Computer mit KMS aktivieren, müssen sich diese nach 180 Tage automatisch neu aktivieren. Gelingt dies nicht, haben Sie weitere 30 Tage Zeit, bis diese Clients in den RFM gesetzt werden.

Multiple Activation Key (MAK) und Key Management Service (KMS)-Activation in der Praxis

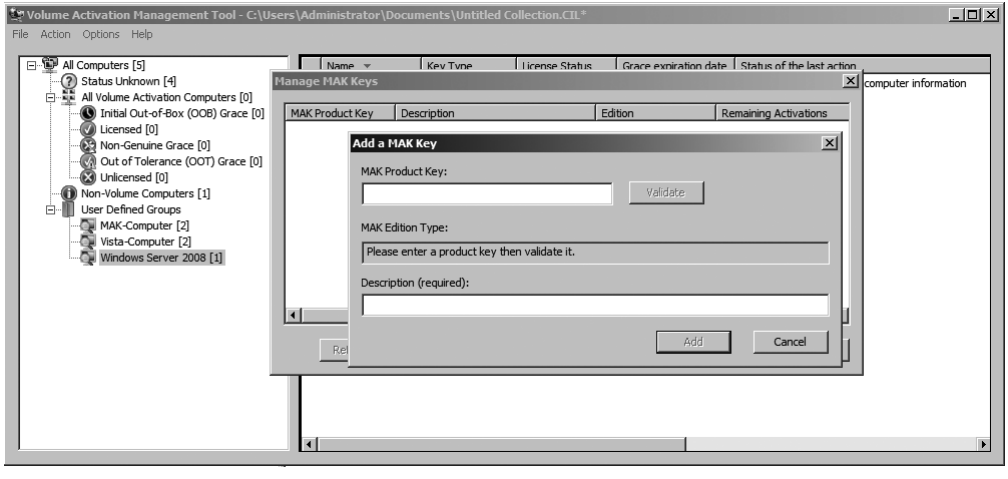
MAK unterstützt die Aktivierung über das Internet und per Telefon. Für Unternehmen ist die Aktivierung über das Internet wesentlich bequemer. Wenn Sie allerdings keine Möglichkeit haben oder aus Sicherheitsgründen auf den Internetzugang verzichten wollen, können Sie auch die telefonische Aktivierung verwenden. Möchten Sie die Aktivierung per Internet durchführen, müssen Sie lediglich dafür sorgen, dass sich die PCs mit dem Internet verbinden können. Auf welche Webseiten dazu ein Zugriff möglich sein muss, haben wir Ihnen bereits einige Seiten weiter vorne gezeigt.

Eine weitere Möglichkeit, mehrere Windows Vista- oder Windows Server 2008-Computer im Netzwerk zu aktivieren, ist das *Volume Activation Management Tool (VAMT)*, welches eine batchbasierte Aktivierung über das Internet unterstützt. Wollen Sie telefonisch aktivieren, benötigen Sie zunächst eine Identifikationsnummer, die über das Telefon eingegeben wird. Auf Basis dieser Nummer erhalten Sie über das Telefon dann die Aktivierungsnummer, die Sie wiederum im PC eingeben, um Windows zu aktivieren. Sie erhalten die notwendige Indentifikationsnummer zur telefonischen Aktivierung auch durch Eingabe des folgenden Befehls:

cscript \windows\system32\slmgr.vbs <Computer-Name> <Benutzer> <Kennwort> –dli

Mit Hilfe dieses Befehls können Sie die notwendigen Daten auch von Remotecomputern über das Netzwerk erhalten. Am besten verwalten Sie MAK-Produkt-Keys über das VAMT. Hier tragen Sie den zugewiesenen Lizenzschlüssel in das Tool ein. Verwenden Sie dazu den Menübefehl *Options/Manage MAK-Keys*. Anstatt die MAK-Keys auf den Clients einzutragen, werden diese direkt im Tool verwaltet. Der Rechner, auf dem das VAMT installiert ist, fungiert als MAK-Proxy.

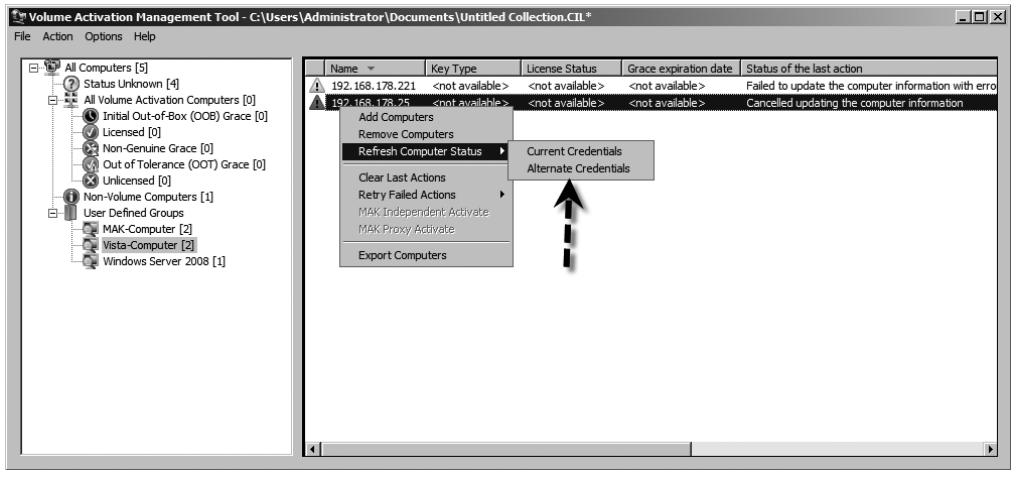
Abbildg. 16.52 Verwalten der MAK-Keys über das VAMT



Anschließend werden die Client-Computer über das Tool eingesammelt und nacheinander aktiviert. Dazu stellt das VAMT eine Verbindung zum Aktivierungsserver von Microsoft her und sendet die Aktivierungs-IDs zurück zu den Clients. Natürlich lassen sich MAK-Keys auch manuell auf den einzelnen Clients verwalten. Allerdings ist das wesentlich unkomfortabler. Außerdem wird der Sta-

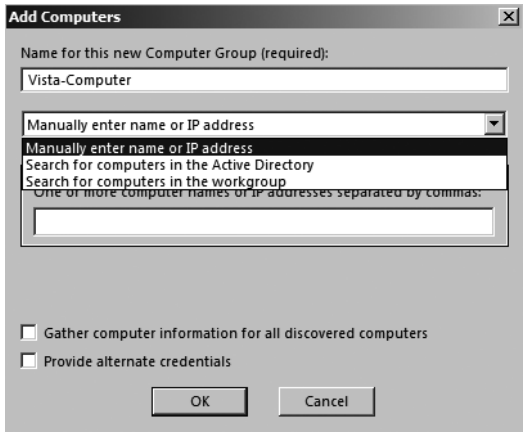
tus aller Clients im Tool angezeigt. Es muss für den Einsatz nicht immer eine Domäne vorhanden sein. In den Eigenschaften der einzelnen Computer können auch alternative Anmeldedaten verwendet werden (Abbildung 16.53).

Abbildg. 16.53 Verwenden von alternativen Anmeldedaten zur Verbindung mit den Clients



Die Computer können über den Menübefehl *Actions/Add Computers* hinzugefügt werden. Hier besteht die Möglichkeit, manuell Clients einzutragen, die Domäne zu durchsuchen oder eine Arbeitsgruppe zu verwenden (Abbildung 16.54).

Abbildg. 16.54 Hinzufügen von Clientcomputern zum VAMT



Haben Sie über das Telefon manuell die Indentifikationsnummer zur Aktivierung eingegeben, erhalten Sie durch den Telefoncomputer eine Confimation-ID (CID). Mit Hilfe dieser CID können Sie Windows aktivieren. Sie können dazu entweder den manuellen Weg wählen, der bereits weiter vorne in diesem Kapitel beschrieben wurde, oder Sie verwenden ein Skript zur Aktivierung:

cscript \windows\system32\slmgr.vbs <Computer-Name> <Benutzername> <Kennwort> –atp <Confirmation ID>

Mit diesem Skript können auch Windows Vista- und Windows Server 2008-Installationen über das Netzwerk aktiviert werden. Für die Aktivierung eines Computers mit der MAK ist die Anmeldung mit einem Benutzerkonto notwendig, welches über administrative Berechtigungen verfügt. Wenn Sie auch Benutzerkonten mit Standardberechtigungen die Aktivierung erlauben wollen, müssen Sie in der Registry im Schlüssel *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL* einen neuen DWORD-Registry-Wert mit der Bezeichnung *UserOperations* erstellen. Weisen Sie diesem den Wert 1 zu.

MAK über Windows verwenden

Wollen Sie MAK verwenden, können Sie die herkömmliche Oberfläche zur Aktivierung in Windows verwenden, wie bereits in diesem Kapitel beschrieben. Gehen Sie bei der Verwendung von MAK bei der Installation und Aktivierung folgendermaßen vor:

1. Installieren Sie Windows Vista oder Windows Server 2008 ohne die Eingabe eines Produktschlüssels.
2. Klicken Sie nach der Installation auf *Start* und dann mit der rechten Maustaste auf *Computer* und wählen Sie im Kontextmenü den Befehl *Eigenschaften* aus.
3. Im Bereich *Windows-Aktivierung* klicken Sie auf *Product Key ändern*.
4. Geben Sie im folgenden Fenster den MAK-fähigen Produktschlüssel ein und lassen Sie diesen über das Internet aktivieren, wenn eine Internetverbindung besteht. Wenn die Verbindung zur Aktivierung fehlschlägt, versucht der PC automatisch ständig eine Verbindung zum Aktivierungsserver bei Microsoft aufzubauen. Der angemeldete Benutzer muss dazu nicht über administrative Berechtigungen verfügen.

Wollen Sie diese automatischen Verbindungsversuche deaktivieren, müssen Sie den Wert *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\Activation\Manual* auf *1* setzen.

MAK über Skript verwenden

Sie können MAK auch über ein Skript verwenden, was bei der Bereitstellung von zahlreichen Clients sicherlich sinnvoller ist. Um MAK über ein Skript durchzuführen, gehen Sie folgendermaßen vor:

1. Installieren Sie Windows Vista oder Windows Server 2008 ohne die Eingabe eines Produktschlüssels.
2. Starten Sie den Computer und melden Sie sich mit einem Benutzerkonto an, das über administrative Rechte verfügt.
3. Starten Sie über *Start/Ausführen* den Befehl *cscript\windows\system32\slmgr.vbs –ipk <Multiple Activation Key>*.
4. Im Anschluss versucht Windows die Aktivierung über das Internet durchzuführen.

MAK über die Installationsroutine verwenden

Installieren Sie Windows Vista oder Windows Server 2008 unbeaufsichtigt, besteht auch die Möglichkeit, MAK bereits über die Installation des Betriebssystems durchzuführen. Zu diesem Zweck wird die MAK bereits in die *unattend.xml* eingebunden, über welche die automatisierte Installation per Windows Automated Installation Kit (WAIK) und den Windows-Bereitstellungsdiensten durch-

geführt wird. Die MAK wird zu diesem Zweck direkt in die *untattend.xml* integriert. Im folgenden Listing sehen Sie, wie die MAK integriert werden kann.

Listing 16.4 Beispiel einer *unattend.xml* mit MAK-Integration

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="windowsPE">
        <component name="Microsoft-Windows-Setup" processorArchitecture="x86"
publicKeyToken="3333333333333333" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
            <UserData>
                <AcceptEula>true</AcceptEula>
            </UserData>
</component>
    </settings>
    <settings pass="specialize">
        <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="x86"
publicKeyToken="3333333333333333" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
            <ProductKey>MAK Product Key</ProductKey>
        </component>
    </settings>
<cpi:offlineImage cpi:source="" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

HINWEIS Beachten Sie, dass bei der Integration der MAK in die *unattend.xml* der MAK-Schlüssel als Klartext in der Datei enthalten ist.

Aktivierung über den Key Management Service (KMS)

Der KMS kann unter Windows Vista, Windows Server 2008, aber auch unter Windows Server 2003 mit SP1 installiert werden. Windows Vista Business Edition und Windows Vista Enterprise Edition sind bereits standardmäßig auf eine Aktivierung per KMS ausgelegt, ohne dass eine Benutzereingabe erfolgen muss. Die Computer versuchen sich in einem Active Directory per SRV-Record mit einem KMS-Server zu verbinden und sich selbständig zu aktivieren. Ein KMS-Server aktiviert erst dann die Clients, wenn sich mindestens 25 Computer mit diesem verbunden haben. Die Clients versuchen sich nach der Installation alle zwei Stunden automatisch beim KMS zu aktivieren und müssen diese Aktivierung alle 180 Tage wiederholen. Auch virtuelle Maschinen können über KMS aktiviert werden, allerdings werden diese nicht zu der Liste der 25 benötigten Clients dazugezählt. Eine virtuelle Maschine kann auch als KMS-Host betrieben werden, zählt aber nicht zu den fünf physischen Servern dazu, ab der die Aktivierung erst unterstützt wird. Für diesen Vorgang wird auf dem entsprechenden Computer ein KMS-Schlüssel hinterlegt, der einmalig bei Microsoft aktiviert werden muss. Dieser Dienst verursacht keine größere Benutzerlast, sodass auch die Installation auf einem Server zusammen mit anderen Diensten in Frage kommt. Ein einzelner KMS kann hunderttausende Clients verwalten.

Bevor Sie die Aktivierung der Clients per KMS durchführen können, müssen einige Vorbereitungen getroffen werden:

- Sie müssen einen KMS-Host mit den zugewiesenen Clientlizenzen installieren und auch Windows Vista oder Windows Server 2008 mit diesen Produktschlüsseln installieren.
- Mit einem Windows Vista-Schlüssel für KMS können nur Windows Vista-Computer aktiviert werden. Mit einem Windows Server 2008-Schlüssel können nur Windows Server 2008-Computer aktiviert werden. Das heißt, auf dem KMS-Host muss jeweils ein Schlüssel für Windows Vista und für Windows Server 2008 integriert werden.
- Damit sich die Clients mit dem KMS-Host verbinden können, müssen Sie sicherstellen, dass diese Verbindung zu dem KMS-Host über den TCP-Port 1688 aufbauen können. Schalten Sie diesen Port auf den Firewalls und Routern im Unternehmen frei.
- Das Ereignisprotokoll auf dem KMS-Host wächst stark an, da viele Meldungen geschrieben werden. Erhöhen Sie daher die maximale Größe der Ereignisprotokolle oder stellen Sie die Überschreibung ein, damit die Ereignisse verarbeitet werden können. Um das notwendige Ereignisprotokoll zu konfigurieren, gehen Sie folgendermaßen vor:

1. Geben Sie den Befehl *eventvwr* über *Start/Ausführen* ein.
2. Öffnen Sie den Baum *Anwendungs- und Dienstprotokolle*.
3. Klicken Sie mit der rechten Maustaste auf *Key Management Service* und rufen Sie im Kontextmenü den Befehl *Eigenschaften* auf.
4. Setzen Sie den Wert bei *Maximale Protokollgröße* auf *10384* oder einen anderen höheren Wert.

Installation und Konfiguration eines KMS-Hosts

Der erste und wichtigste Schritt bei der Aktivierung per KMS ist der KMS-Host. Gehen Sie zur Installation eines KMS-Hosts folgendermaßen vor:

1. Installieren Sie zunächst das zugewiesene Volumenlizenzmedium auf dem KMS-Host.
2. Starten Sie den Computer neu und melden Sie sich mit einem Benutzerkonto an, welches über administrative Berechtigungen verfügt.
3. Im nächsten Schritt wird der notwendige KMS-Schlüssel auf dem KMS-Host hinterlegt. Dazu stellt Microsoft keine grafische Oberfläche zur Verfügung, Sie müssen den Schlüssel über ein Skript integrieren. Geben Sie dazu den Befehl *cscript c:\windows\system32\slmgr.vbs –ipk <Volume License Key>* ein.
4. Im Anschluss muss dieser Schlüssel bei Microsoft entweder telefonisch oder über das Internet aktiviert werden. Um den KMS-Schlüssel über das Internet zu aktivieren, geben Sie über *Start/Ausführen* den Befehl *cscript c:\windows\system32\slmgr.vbs –ato* ein. Zur telefonischen Aktivierung geben Sie über *Start/Ausführen* den Befehl *slui 4* ein und folgen Sie den Anweisungen.

Anpassung des KMS-Hosts

Nach der erfolgreichen Aktivierung können Sie auf dem KMS-Host noch notwendige Konfigurationsänderungen vornehmen. Auch für diese Konfigurationen verwenden Sie am besten wieder das bereits erwähnte Skript *slmgr.vbs*:

Ändern des Standardports Standardmäßig reagiert der KMS-Host auf Anfragen zum TCP-Port 1688. Wenn Sie den Standardpfad ändern wollen, geben Sie den Befehl *cscript c:\windows\system32\slmgr.vbs –sprt <port>*. Nachdem Sie die Änderung vorgenommen haben, sollten Sie den

KMS-Host neu starten. Alternativ können Sie in der Befehlszeile den KMS-Dienst über *net stop slsvc.exe* beenden und anschließend über *net start slsvc.exe* neu starten lassen. Clients, die sich über DNS automatisch verbinden, müssen dazu nicht konfiguriert werden.

Konfiguration der dynamischen DNS-Registrierung Bei der Installation und Aktivierung des KMS wird der entsprechende SRV-Record automatisch erstellt, wenn für die Active Directory-integrierte DNS-Zone die dynamische Registrierung aktiviert worden ist. Sie können die dynamische Registrierung über den Befehl *cscript C:\windows\system32\slmgr.vbs –cdns* deaktiveren. Der Befehl *cscript C:\windows\system32\slmgr.vbs –sdns* aktiviert die dynamische Registrierung wieder.

Anpassen des Aktivierungsintervalls Standardmäßig versuchen nicht aktivierte Clients alle 120 Minuten eine Verbindung zum KMS aufzubauen. Über den Befehl *cscript c:\windows\system32\slmgr.vbs –sai <Aktivierungsintervall>*, können Sie diesen Zeitraum an Ihre Bedürfnisse anpassen.

Standardmäßig registriert sich der KMS in der DNS-Zone, in der sich der Server selbst befindet. Wenn Sie wollen, dass sich der KMS in weiteren DNS-Zonen registriert, müssen Sie die Registry bearbeiten:

1. Navigieren Sie zum Schlüssel *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL*.
2. Erstellen Sie einen neuen REG_MULTI_SZ-Wert mit der Bezeichnung *DnsDomainPublishList*.
3. Tragen Sie als Wert jede DNS-Domäne in einer eigenen Zeile ein, in der sich der KMS registrieren soll.
4. Starten Sie den Lizenzdienst über die Befehle *net stop slsvc.exe* und anschließend über *net start slsvc.exe* neu.

MAK-Clients in KMS-Clients konvertieren

Wenn Sie im Unternehmen MAK-Clients einsetzen, können diese zu KMS-Clients konvertiert werden. Um einen MAK-Client zu konvertieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich am Client mit einem administrativen Benutzerkonto an.
2. Geben Sie in der Befehlszeile den Befehl *cscript \windows\system32\slmgr.vbs ipk <Produktschlüssel>* ein. Anschließend muss der Computer mit dem Befehl *cscript \windows\system32\slmgr.vbs –ato* erneut, diesmal über den KMS, aktiviert werden.

Standardmäßig ist in Windows Vista und Windows Server 2008 die Windows-Firewall bereits aktiviert. Wenn Sie mit dem bereits besprochenen Skript *Slmgr.vbs* über das Netzwerk remote PCs aktivieren wollen, müssen Sie sicherstellen, dass die Windows-Firewall auf den einzelnen PCs das Skript nicht blockieren. Um einen Client manuell zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Systemsteuerung, zum Beispiel über *Start/Systemsteuerung*.
2. Klicken Sie auf *Sicherheit*.
3. Klicken Sie auf *Windows-Firewall ein- oder ausschalten*.
4. Klicken Sie auf *Ausnahmen*.
5. Setzen Sie den Haken bei *Windows-Verwaltungsinstrumentation (WMI)*.

Alternativ können Sie diese Einstellung auch über Gruppenrichtlinien aktivieren. Wenn Sie mehrere Subnetze im Unternehmen einsetzen, reicht die vorangegangene Konfiguration allerdings nicht aus. In diesem Fall müssen Sie die erweiterte Konfiguration der Firewall starten:

1. Die erweiterte Konfiguration der Firewall rufen Sie über *Start/Ausführen/wf.msc* auf.
2. Klicken Sie im linken Bereich auf *Eingehende Regeln*.

Ganz unten finden Sie die folgenden drei Regeln. Für jede Regel gibt es eine Variante für das Profil *Domäne* und das Profil *Privat, Öffentlich*:

- Windows-Verwaltungsinstrumentation (ASync eingehend)
- Windows-Verwaltungsinstrumentation (DCOM eingehend)
- Windows-Verwaltungsinstrumentation (WMI eingehend)

Für alle dieser Einstellungen nehmen Sie für das entsprechende Netzwerkprofil (in Active Directory das Profil *Domäne*) die gleichen Einstellungen vor, wie nachfolgend beschrieben. Klicken Sie dazu doppelt auf die jeweilige Regel, um deren Eigenschaften aufzurufen:

- Auf der Registerkarte *Allgemein* aktivieren Sie die Option *Verbindungen zulassen*.
- Auf der Registerkarte *Bereich* geben Sie unten bei *Remote-IP-Adresse* die Subnetze ein, auf die von den Computer zugegriffen werden soll.
- Auf der Registerkarte *Erweitert* legen Sie fest, für welche Profile diese Einstellung Gültigkeit hat.

Zusammenfassung

Mit den Windows-Bereitstellungsdiensten und dem WAIK lassen sich Windows Vista-Arbeitsstationen und Windows Server 2008 hervorragend automatisiert installieren und im Netzwerk verteilen. Wir haben Ihnen in diesem Kapitel gezeigt, wie Sie den Dienst installieren sowie einrichten und wie Sie Antwortdateien zur automatischen Installation erstellen. Im nächsten Kapitel 17 vertiefen wir die Themen um die Active Directory-Zertifikatsdienste, die wir bereits im Kapitel 15 besprochen haben, und gehen zusätzlich auf die Active Directory-Rechteverwaltung und die Active Directory Lightweight Domain Services (AD LDS) ein.

Kapitel 17

Zusätzliche Active Directory-Rollen

In diesem Kapitel:

Microsoft hat in Windows Server 2008 auch die Bezeichnung der Komponenten angepasst, die zur Identitätsverwaltung verwendet werden. Alle diese Funktionen und Serverrollen, erhalten vor der eigentlichen Bezeichnung noch das Präfix *Active Directory* hinzu. So wird schnell ersichtlich, welche der Dienste direkt auf Active Directory aufbauen, oder mit Active Directory einen erweiterten Funktionsumfang erhalten: Die *Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS)* stellen die neue Version der Zertifikatdienste unter Windows Server 2003 dar. *Active Directory-Domänendienste (Active Directory Domain Services, AD DS)* ist die Serverrolle mit der ein Server zum Domänencontroller heraufgestuft werden kann, um entweder einer Gesamtstruktur beizutreten oder eine neue zu erstellen (siehe Kapitel 8). Die *Active Directory-Verbunddienste (Active Directory Federation Services, AD FS)* bieten eine webbasierte Single Sign-On (SSO)-Infrastruktur. Mit den *Active Directory-Rechteverwaltungsdiensten (Active Directory Rights Management Services, AD RMS)* werden Daten mit digitalen Signaturen versehen, um sie vor unerwünschtem Zugriff zu sichern. Besitzer von Dateien können basierend auf Benutzerinformationen exakt festlegen, was andere Benutzer mit den Dateien machen dürfen. Dokumente können zum Beispiel als »Nur Lesen« konfiguriert werden oder stehen nur bestimmten Anwendern zur Verfügung.

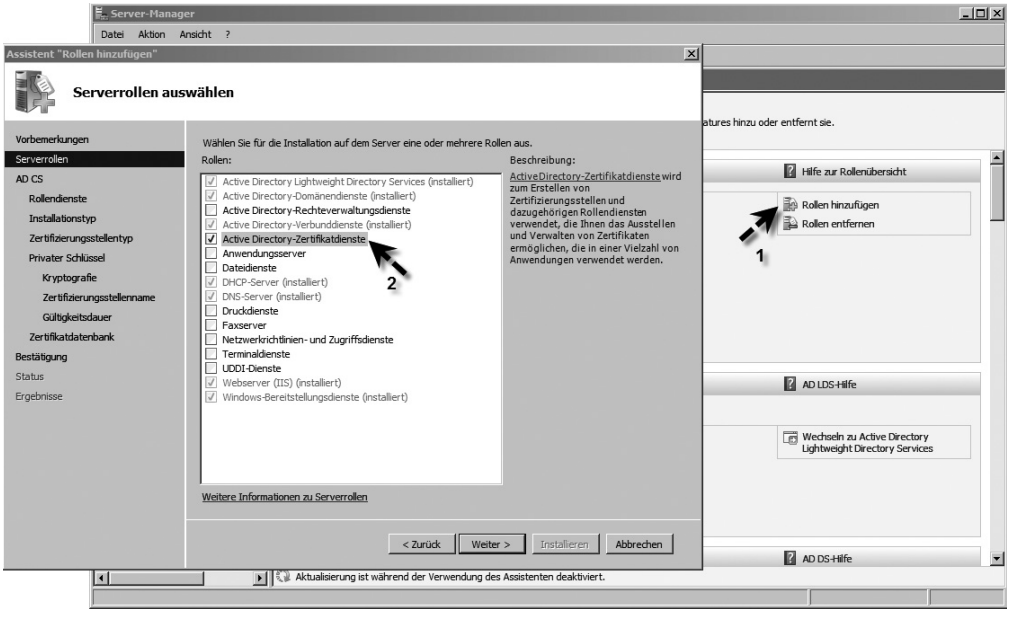
In diesem Kapitel gehen wir auf die wichtigsten Funktionen der zusätzlichen Active Directory-Rollen Active Directory-Zertifikatdienste, Active Directory-Rechteverwaltung, Active Directory Lightweight Services und Active Directory-Verbunddienste ein. Alle Funktionen sind in ähnlicher Form auch in Windows Server 2003 R2 vorhanden, wurden aber in Windows Server 2008 deutlich erweitert. Es würden den Umfang dieses Buches sprengen, diese Themen umfassend in einem Windows Server 2008-Handbuch zu besprechen. Wir gehen jedoch in diesem Buch auf die wichtigsten Themen ein. Ausführlichere Informationen und Praxistipps zu diesen Rollen, finden Sie im Buch *Active Directory – Das Praxisbuch für Windows Server 2008* (ISBN-10: 3866456301, ISBN-13: 978-3866456303). In diesem Buch widmen wir uns ausführlich den Active Directory-Funktionen von Windows Server 2008.

Active Directory-Zertifikatdienste

Der Betrieb einer eigenen Zertifizierungsstelle lohnt sich zum Beispiel beim Einsatz von SSL-gesicherten Webseiten, bei der Verwendung von Exchange Server 2007 im Netzwerk, oder generell bei der Absicherung des E-Mail-Verkehrs. Generell erfordert der Einsatz einer Zertifizierungsstelle keinen riesigen Verwaltungsaufwand. Bereits direkt nach der Installation steht eine Zertifizierungsstelle zur Verfügung und benötigt nur selten Verwaltungsaufwand. Wir zeigen Ihnen in diesem Kapitel auch ein paar Praxisbeispiele für den Einsatz einer Zertifizierungsstelle. In Kapitel 15 finden Sie weitere wichtige Anleitungen für Zertifizierungsstellen. Auch wenn viele Serverdienste, wie IIS oder Exchange Server 2007, ein eigenes Zertifikat mitbringen, empfiehlt Microsoft die Einbindung eines eigenes Zertifikats für verschiedene Sicherheitskonzepte. Das Exchange-eigene Zertifikat wird zum Beispiel als nicht-vertrauenswürdig eingestuft. Für die Veröffentlichung von Outlook Web Access, RPC über HTTP (Outlook Anywhere) und Exchange ActiveSync (EAS), kann ohne weiteres eine interne Zertifikatstelle verwendet werden. In Zusammenhang mit einem ISA-Server empfiehlt Microsoft sogar diese Vorgehensweise. Auch wenn die Netzwerkzugriffschutzdienste benötigt werden, empfiehlt Microsoft den Einsatz einer eigenen Zertifizierungsstelle.

HINWEIS Bei der Installation der Active Directory-Zertifikatdienste legen Sie auch einen Namen für die Zertifizierungsstelle fest. Es muss sich dabei nicht unbedingt um den Namen des Servers handeln, auch wenn dieser vorgeschlagen wird. Der Name darf maximal 64 Zeichen lang sein. Sonderzeichen sollten möglichst nicht verwendet werden, da manche Netzwerkgeräte Probleme damit haben. Der Name kann nach der Installation nicht mehr geändert werden.

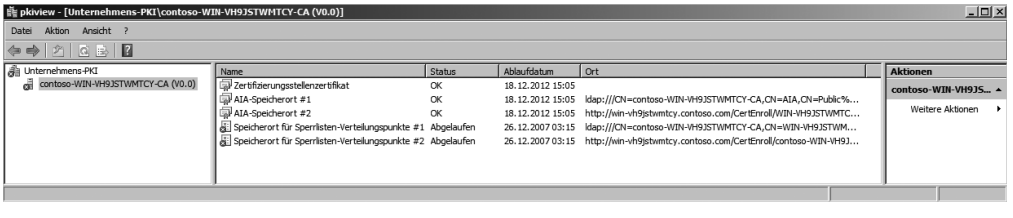
Abbildg. 17.1 Installieren der Active Directory-Zertifikatdienste als zusätzlicher Rollendienst



Neuerungen der Active Directory-Zertifikatdienste

Auch wenn viele Funktionen der Zertifikatdienste unter Windows Server 2008 ähnlich zu den Funktionen in Windows Server 2003 sind, gibt es einige interessante Neuerungen. Eine wichtige Neuerung ist die automatische Bereitstellung (Enrollment) von Zertifikaten für Arbeitsstationen und andere Geräte im Netzwerk. Diese Funktion wird Network Device Enrollment Service (NDES) genannt. Die Funktion unterstützt das *Simple Certificate Enrollment Protocol (SCEP)* von Cisco. Ebenfalls neu ist der Online Responder, der das *Online Certificate Status Protocol (OCSP)* implementiert. Dieser Dienst kann als Alternative zu *Certificate Revocations Lists (CLR)* eingesetzt werden, mit der Clients Informationen zum Status der Zertifikatsabfrage zur Verfügung gestellt werden (*http://de.wikipedia.org/wiki/Online_Certificate_Status_Protocol*). Ebenfalls neu ist die Cluster-Unterstützung und eine verbesserte Verschlüsselung. Zusätzlich gibt es das Zusatztool *PKIView.msc*, mit dem sehr schnell der allgemeine Zustand der Zertifizierungsstelle überprüft werden kann. Findet das Tool Fehler, werden diese in einer Konsole angezeigt (Abbildung 17.2).

Abbildg. 17.2 Überprüfen der internen PKI mit dem neuen Tool *PKIView*



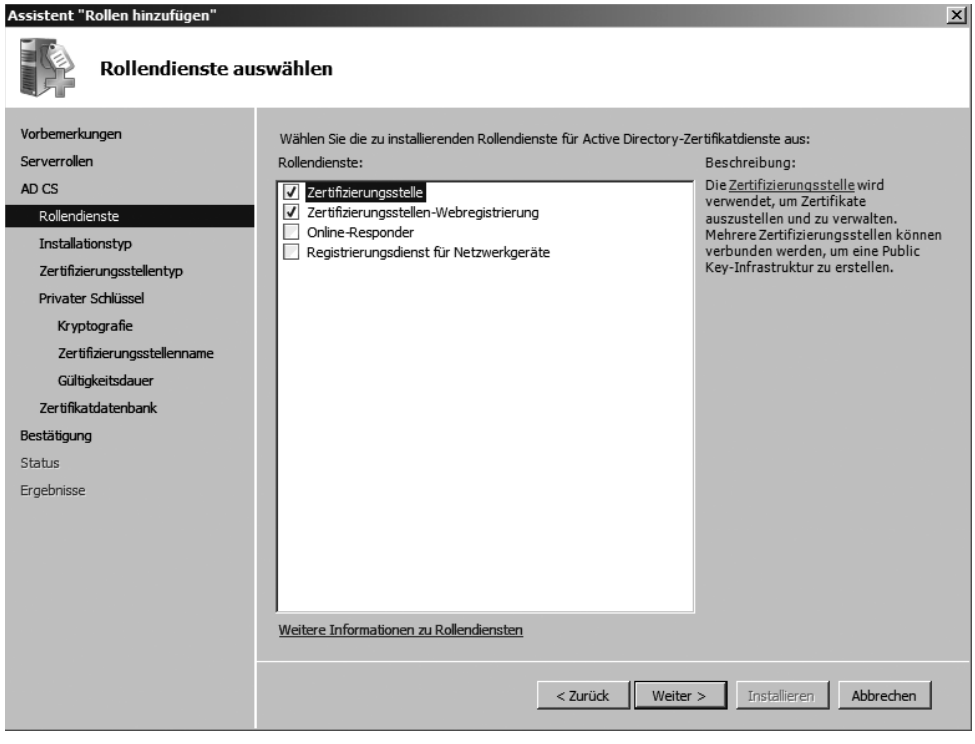
Die neue Webschnittstelle in den Zertifikatdiensten wurde für Windows Vista optimiert. Diese ist kompatibel zu Windows XP. Standardmäßig kann Windows Vista allerdings keine Zertifikate über die Webschnittstelle einer Windows Server 2003-CA abrufen. Hier besteht aber die Möglichkeit, die Webschnittstelle von Windows Server 2003 kompatibel mit Windows Vista zu machen. Ansonsten hat Windows Vista keinerlei Probleme mit einer Windows Server 2003-Zertifikatsstelle.

Installation einer Windows Server 2008-Zertifizierungsstelle

Die Installation einer eigenen Zertifizierungsstelle ist nicht sehr kompliziert, und Zertifikate können einfach und schnell angefordert werden. Installieren Sie die Zertifikatstelle entweder auf einem Domänencontroller oder einem anderen im Netzwerk befindlichen Server. Wird der Server, der die Zertifikatstelle verwaltet, aus der Domäne entfernt, verlieren die Zertifikate ihre Gültigkeit. Die Installation wird über das Hinzufügen der Rolle *Active Directory-Zertifikatdienste* im Server-Manager gestartet (Abbildung 17.1). Den genauen Ablauf der Installation haben wir Ihnen bereits in Kapitel 15 gezeigt. Lesen Sie sich daher in Kapitel 15 zunächst die Anleitung zur Installation durch. Insgesamt können bei der Installation vier Rollendienste ausgewählt werden:

- **Zertifizierungsstelle** Hierbei handelt es sich um den wichtigsten Rollendienst, der die Basis der Zertifikatdienste darstellt. Dieser Rollendienst wird für das Ausstellen und Verwalten der Zertifikate benötigt.

Abbildg. 17.3 Auswählen der Rollendienste der Active Directory-Zertifikatdienste



- **Zertifizierungsstellen-Webregistrierung** Wird dieser Rollendienst installiert, können auch Zertifikate über die Webadresse *http://<Servername>/certsrv* angefordert werden. Hierbei handelt es sich sozusagen um die Webschnittstelle der Zertifizierungsdienste. Der Rollendienst setzt die Installation von IIS 7.0 auf dem Server voraus.
- **Online-Responder** Dieser Rollendienst stellt die OCSP-Funktion zur Verfügung, über die den Clients erweiterte Informationen über den aktuellen Zustand der Zertifikatsabfrage gegeben werden. Der Dienst setzt die Installation von IIS 7.0 voraus, es wird ein neues Web mit der Adresse *http://<Servername>/ocsp* erstellt.
- **Registrierungsdienst für Netzwerkgeräte** Diese Funktion kann nur eigenständig installiert werden, nicht zusammen mit einer Zertifizierungsstelle. Mit diesem Rollendienst wird die bereits erwähnte Funktion zum automatischen Ausstellen von Zertifikaten an Netzwerkgeräte ermöglicht.

HINWEIS Die verschiedenen Editionen von Windows Server 2008 unterstützen nicht alle Funktionen einer Zertifizierungsstelle. Die Windows Server 2008 Web Edition unterstützt zum Beispiel die Installation einer Zertifizierungsstelle überhaupt nicht. Um Netzwerkgeräten automatisch ein Zertifikat zuweisen zu können, muss die Zertifizierungsstelle entweder auf der Windows Server 2008 Enterprise Edition oder Datacenter Edition installiert werden, die Standard Edition und Web Edition unterstützen diese Funktion nicht. Auch für die Schlüsselarchivierung, die Aufteilung der verschiedenen Rollendienste und der Einschränkungen in der Zertifikateverwaltung zur Delegierung wird entweder Windows Server 2008 Enterprise Edition oder Datacenter Edition benötigt.

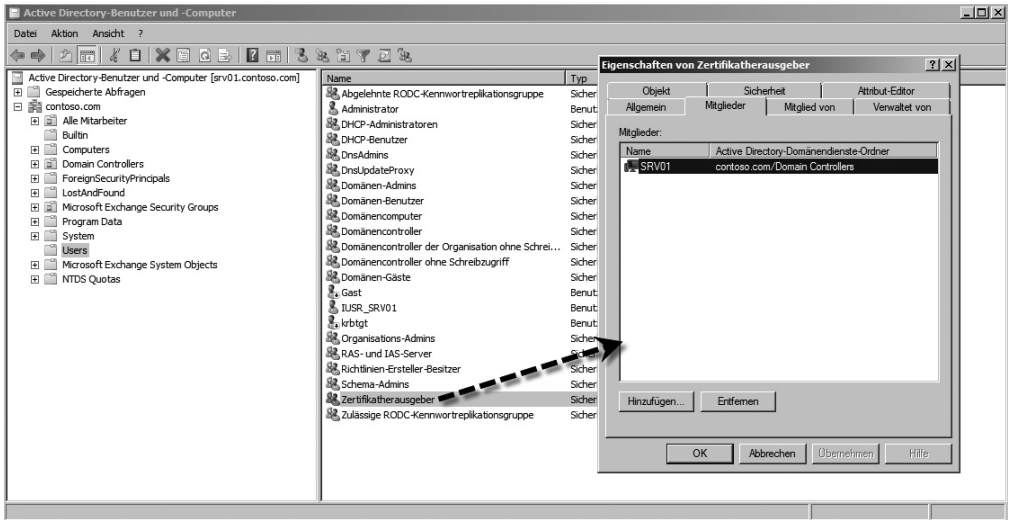
Die Zertifizierungsstellentypen und -Verwaltungskonsolen

Bei der Installation der Active Directory-Zertifikatdienste kann ausgewählt werden, ob der Typ *Unternehmen* oder *Eigenständig* installiert werden soll. Wird *Unternehmen* ausgewählt, werden die Zertifikatdienste in das Active Directory integriert. Außerdem verteilt eine Zertifizierungsstelle (Certificate Authority, CA) das Zertifikat für die vertrauenswürdigen Stammzertifizierungsstellen auf den Computern automatisch über eine Gruppenrichtlinie.

HINWEIS Alle Mitgliedcomputer einer Domäne vertrauen einer internen Stammzertifizierungsstelle mit dem Typ *Unternehmen* automatisch. Das Zertifikat dieser Zertifizierungsstelle wird dazu auf den Client-Computern und Mitgliedsservern in den Zertifikatespeicher der vertrauenswürdigen Stammzertifizierungsstellen integriert.

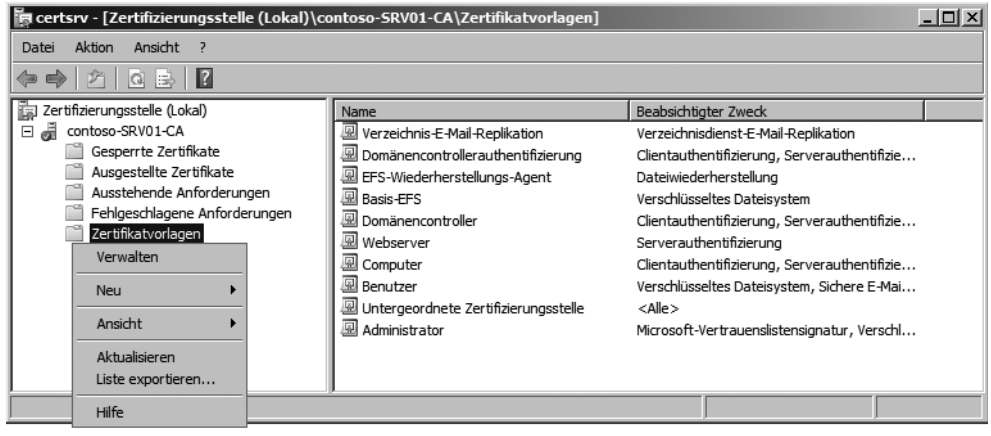
Damit der Server fehlerfrei Zertifikate ausstellen kann, muss er Mitglied der Gruppe *Zertifikateherausgeber* sein. Diese Gruppe befindet sich in der OU *Builtin*.

Abbildg. 17.4 Damit der Unternehmens-Zertifikateserver funktioniert, muss das Computerkonto Mitglied der Gruppe *Zertifikateherausgeber* sein



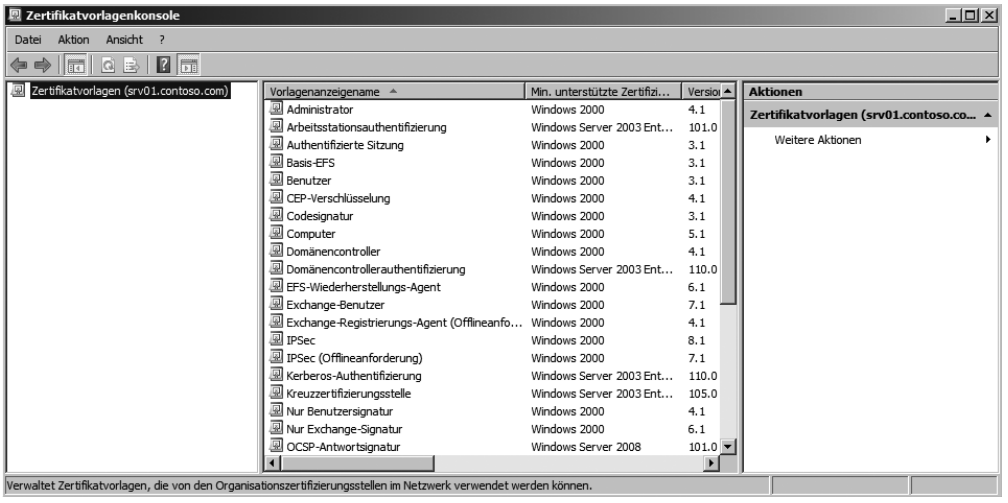
Innerhalb einer Unternehmenszertifizierungsstelle werden die Zertifikate auf Basis von Zertifikatvorlagen ausgestellt. In den Eigenschaften der Vorlagen kann eingestellt werden, wer Zertifikate auf der Basis der Vorlage anfordern oder verwalten darf (Abbildung 17.5). Die Zertifikatvorlagen werden mit dem Snap-In *Zertifikatvorlagen* verwaltet. Dieses wird gestartet, wenn in der Verwaltungskonsole *Zertifizierungsstelle* im Kontextmenü zum Konsoleneintrag *Zertifikatvorlagen* auf den Befehl *Verwalten* geklickt wird.

Abbildg. 17.5 Anzeigen und Verwalten der Zertifikatsvorlagen



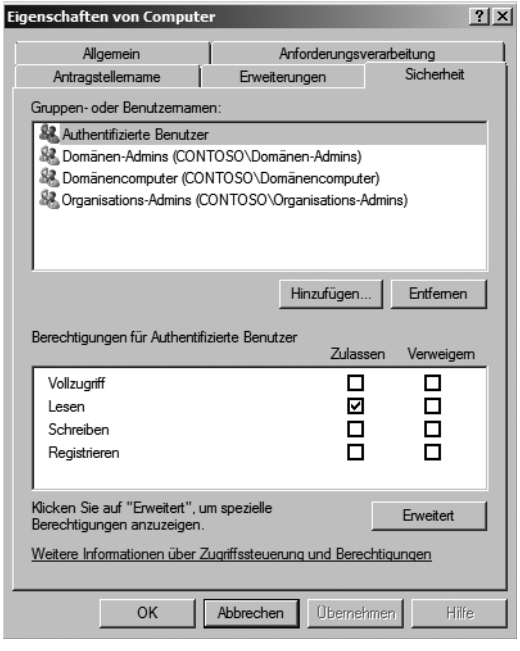
Neben den Standardvorlagen gibt es noch zahlreiche weitere, die über die Verwaltungskonsole konfiguriert und aktiviert werden können (Abbildung 17.6).

Abbildg. 17.6 Verwalten von Zertifikatsvorlagen auf Basis der Zertifikatvorlagenkonsole



Jede Zertifikatvorlage verfügt über eine eigene Sicherheitsverwaltung, die über das Kontextmenü in den Eigenschaften auf der Registerkarte *Sicherheit* aufgerufen wird (Abbildung 17.7). Werden Zertifikate auf Basis der Zertifikatvorlagen erstellt, können die Zertifikatdienste die Daten und den Namen des Antragstellers automatisch aus Active Directory auslesen.

Abbildg. 17.7 Verwalten der Sicherheitseinstellungen einer Zertifikatvorlage



Eigenständige Zertifizierungsstellen

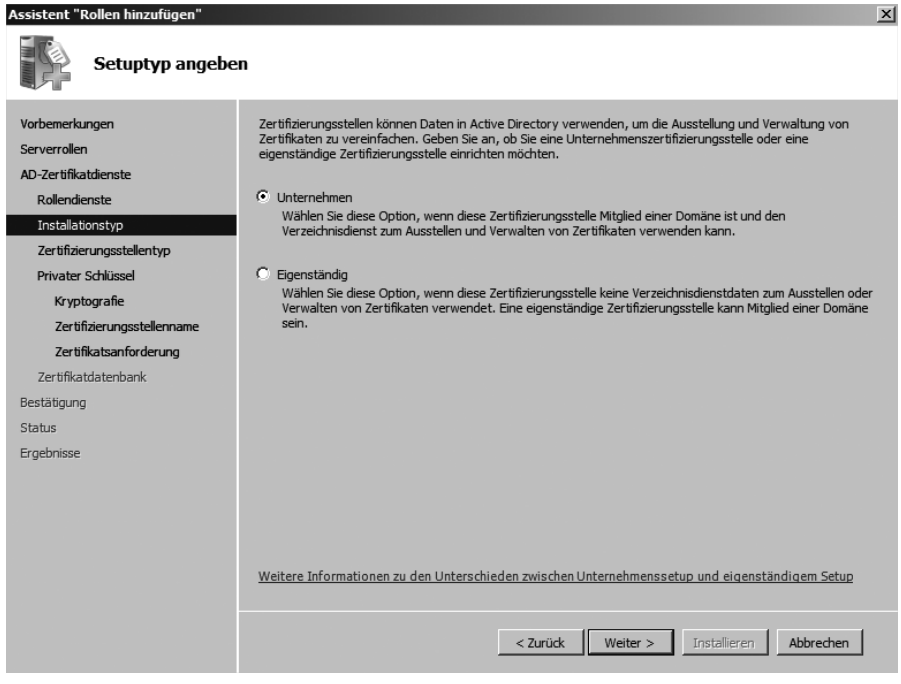
Eigenständige Zertifizierungsstellen werden dazu verwendet, S/MIME- oder SSL-Zertifikate auszustellen, wenn keine Active Directory-Unterstützung benötigt wird. Alle Vorteile der Unternehmenszertifizierungsstelle, die wir auf den vorherigen Seiten erläutert haben, gelten für eigenständige Zertifizierungsstellen nicht. Diese Art der Zertifizierungsstellen läuft vollkommen unabhängig von Active Directory. Eigenständige Zertifizierungsstellen verwenden auch keine Vorlagen und Anwender müssen beim Beantragen von Zertifikaten mehr Informationen angeben, da diese nicht aus dem Active Directory gelesen werden können. Administratoren müssen außerdem jede Anfrage manuell genehmigen.

TIPP Wird eine eigenständige Zertifizierungsstelle auf einem Domänencontroller installiert, erhalten wie bei der Unternehmenszertifzierungsstelle alle Mitglieds-Computer das Zertifikat der Zertifizierungsstelle. Das Zertifikat wird im Speicher der vertrauenswürdigen Stammzertifizierungsstellen abgelegt. Da keine Unterstützung für die Domäne integriert ist, werden alle Zertifikate ohne Benutzerüberprüfung ausgestellt, wenn die Funktion deaktiviert wird, dass der Administrator jedes Zertifikat genehmigen muss.

Installieren einer untergeordneten Zertifizierungsstelle

Während der Installation der Zertifikatdienste kann auch ausgewählt werden, ob eine untergeordnete Zertifizierungsstelle installiert werden soll. Clients verbinden sich in diesem Fall mit der untergeordneten Zertifizierungsstelle, und die Stammzertifizierungsstelle wird bei vielen Anfragen entlastet. Ansonsten sind die Installation und Verwaltung von untergeordneten Zertifizierungsstellen identisch zu übergeordneten.

Abbildg. 17.8 Während der Installation kann ausgewählt werden, ob eine Stammzertifizierungsstelle oder eine untergeordnete Zertifizierungsstelle installiert werden soll



Konfiguration des Online Certificate Status Protocol

Wird eine Zertifizierungsstelle (Certificate Authority, CA) im Unternehmen eingesetzt, lohnt es sich, häufig auch das *Online Certificate Statuts Protocol (OCSP)* zu konfigurieren, über das den Clients ausführlichere Informationen über den aktuellen Status der Zertifikatsanfrage zur Verfügung gestellt werden. Vor allem bei der automatischen Zuteilung von Zertifikaten zu Clients macht diese Konfiguration Sinn. Die Verwaltung des Online-Responders in Windows Server 2008 findet durch ein eigenes Snap-In mit der Bezeichnung *Online-Responderverwaltung* statt. Dieses kann über *Start/Verwaltung* gestartet werden. Alternativ starten Sie das Snap-In über *Start/Ausführen/ocsp.msc* (Abbildung 17.9).

Abbildg. 17.9 Verwalten des Online-Responders in Windows Server 2008

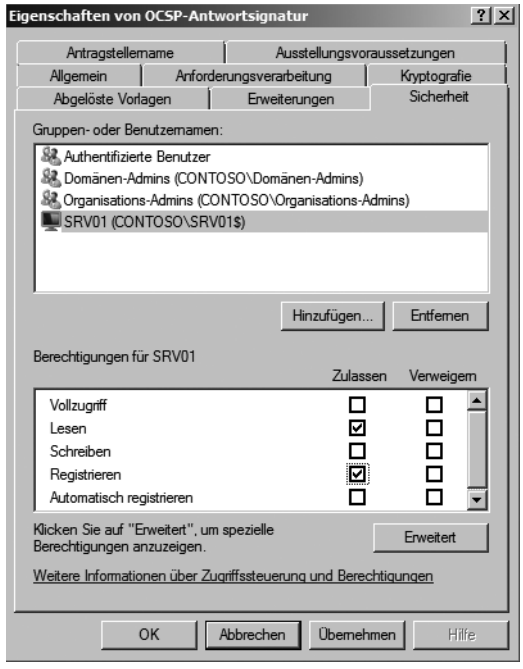
Mit dieser Konsole können die Responder für mehrere Zertifizierungsstellen verwaltet werden. Mit einem Online-Responder können Sperrinformationen über mehrere Zertifizierungsstellen und Zertifizierungsstellenzertifikate verfügbar gemacht werden. Für jede Zertifizierungsstelle und jedes Zertifizierungsstellenzertifikat ist eine *Sperrkonfiguration* erforderlich.

Über den Link *Respondereigenschaften* im Aktionsbereich legen Sie die Einstellungen für diesen Dienst fest. Hier wird zum Beispiel eingestellt, welche Administratoren den Dienst verwalten können. Die ausführliche Besprechung dieses komplexen Themas würde den Rahmen dieses Buches sprengen. In der Hilfe zum Online-Responder finden Sie zahlreiche Informationen, wie mit dieser Funktion umgegangen wird.

Wenn Sie den Rollendienst des Online-Responders installieren, müssen Sie zusätzlich noch die Zertifikatsvorlage *OCSP-Antwortsignatur* in der Zertifikatvorlagenkonsole bearbeiten:

1. Klicken Sie auf die Registerkarte *Sicherheit* und fügen Sie das Computerkonto des Servers hinzu, auf dem der Online-Responder installiert worden ist. Denken Sie daran, im Suchfeld den Objekttyp *Computer* hinzuzufügen.
2. Geben Sie dem Konto das Recht *Lesen* und das Recht *Registrieren*.

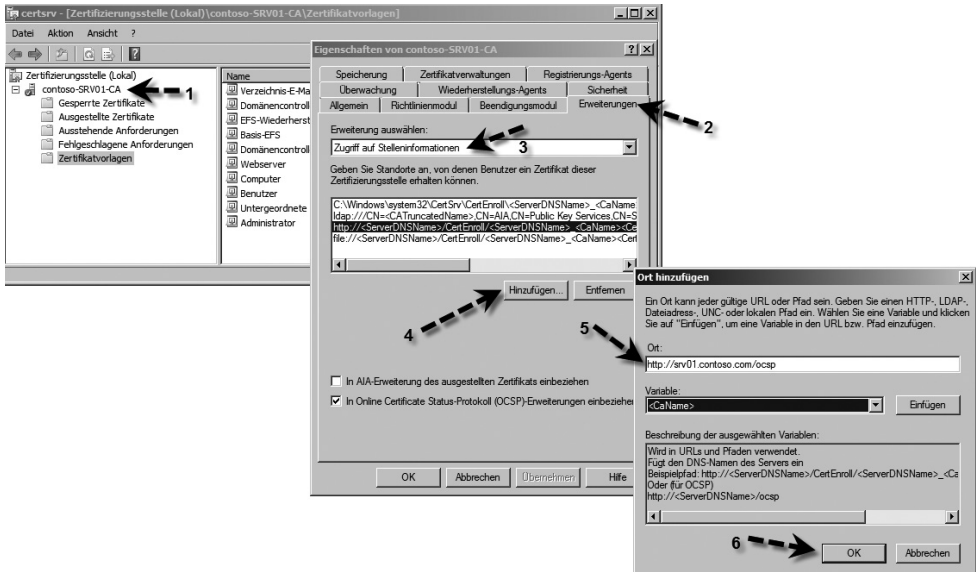
Abbildg. 17.10 Verwalten der Berechtigungen für den OCSP-Responder



Als Nächstes muss die Zertifizierungsstelle noch entsprechend konfiguriert werden:

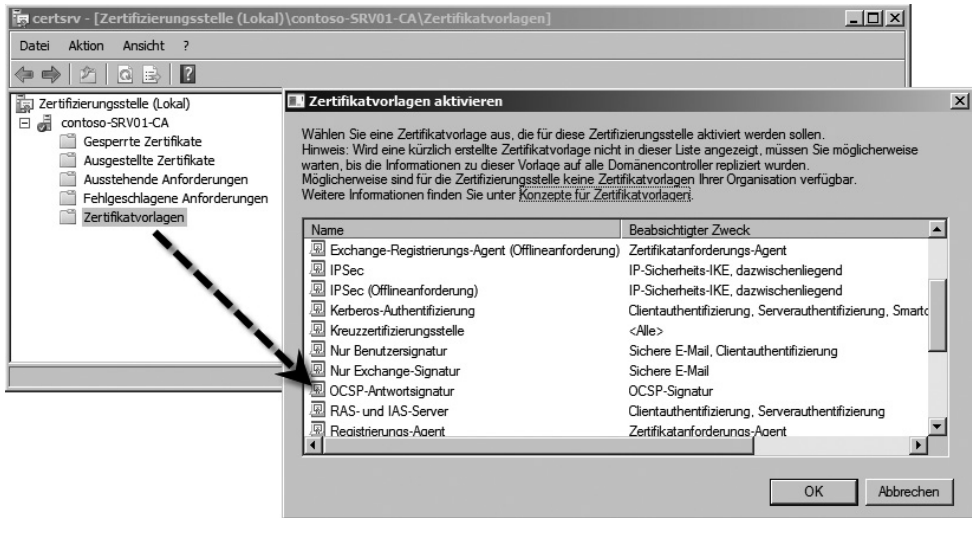
1. Öffnen Sie das Snap-In zur Verwaltung der Zertifizierungsstelle.
2. Rufen Sie die Eigenschaften der Zertifizierungsstelle in der Konsole auf.
3. Klicken Sie auf *Erweiterungen*.
4. Wählen Sie im Bereich *Erweiterung auswählen* die Option *Zugriff auf Stelleninformationen* aus.
5. Klicken Sie auf *Hinzufügen*.
6. Geben Sie bei *Ort* die OCSP-Adresse des Servers an, standardmäßig ist dies die Adresse *http://<Servername mit DNS>/ocsp*.
7. Bestätigen Sie das Dialogfeld *Ort hinzufügen* mit *OK*.
8. Aktivieren Sie im Eigenschaftenfenster das Kontrollkästchen *In Online Certificate Status-Protokoll (OCSP)-Erweiterungen einbeziehen* und bestätigen Sie mit *OK*.
9. Klicken Sie im Snap-In zur Verwaltung der Zertifizierungsstelle mit der rechten Maustaste auf *Zertifikatvorlagen* und wählen im Kontextmenü den Untermenübefehl *Neu/Auszustellende Zertifikatvorlage*.

Abbildg. 17.11 Festlegen des Speicherortes für den Online-Responder



10. Wählen Sie *OCSP-Antwortsignatur* aus und bestätigen Sie mit *OK* (Abbildung 17.12).

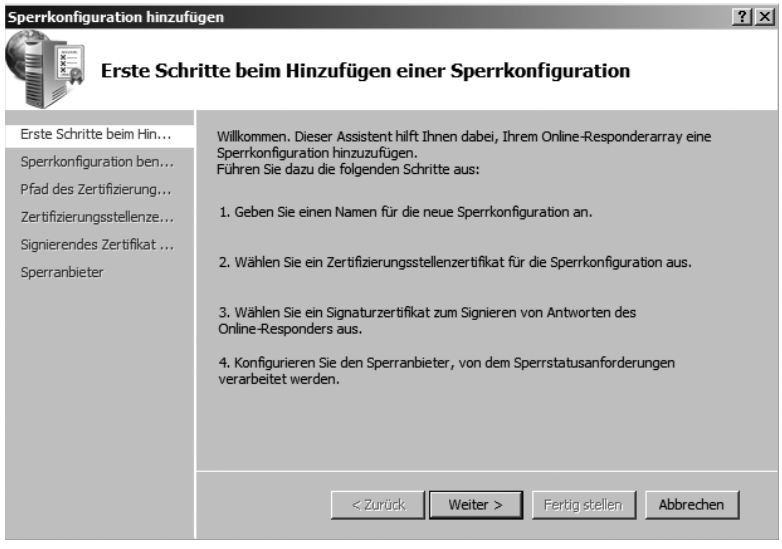
Abbildg. 17.12 Aktivieren einer neuen Zertifikatvorlage für OCSP



Eine Sperrkonfiguration enthält Einstellungen, die für die Beantwortung von Statusanforderungen bezüglich der Zertifikate erforderlich sind. In der Verwaltungskonsole des Online-Responders können dazu verschiedene Einstellungen vorgenommen werden (Abbildung 17.13). So erstellen Sie eine Sperrkonfiguration:

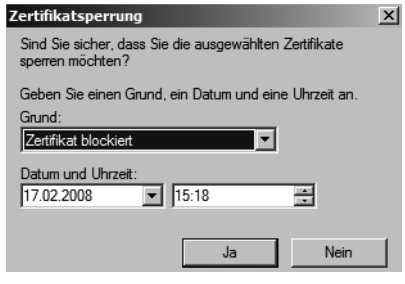
1. Öffnen Sie das Online-Responder-Snap-In.
2. Klicken Sie auf *Sperrkonfiguration*.
3. Klicken Sie im Bereich *Aktionen* auf *Sperrkonfiguration hinzufügen* und geben Sie die notwendigen Daten ein. Im zweiten Fenster klicken Sie auf *Zertifikat für eine vorhandene Unternehmenszertifizierungsstelle auswählen*.

Abbildg. 17.13 Erstellen einer neuen Sperrkonfiguration



Nach der Installation eines Online-Responders können Sie diesen testen, indem Sie versuchen, Zertifikate automatisch zu registrieren, Zertifikate zu sperren und Sperrdaten über den Online-Responder bereitzustellen. Zum Testen verwenden Sie das Snap-In *Zertifizierungsstelle*. Kicken Sie auf *Ausgestellte Zertifikate* und wählen das Zertifikat aus, das Sie sperren möchten. Wählen Sie im Kontextmenü den Untermenübefehl *Alle Aufgaben/Zertifikat sperren*. Geben Sie den Grund für die Zertifikatsperrung ein und bestätigen Sie die Sperrung (Abbildung 17.14).

Abbildg. 17.14 Sperren eines Zertifikats



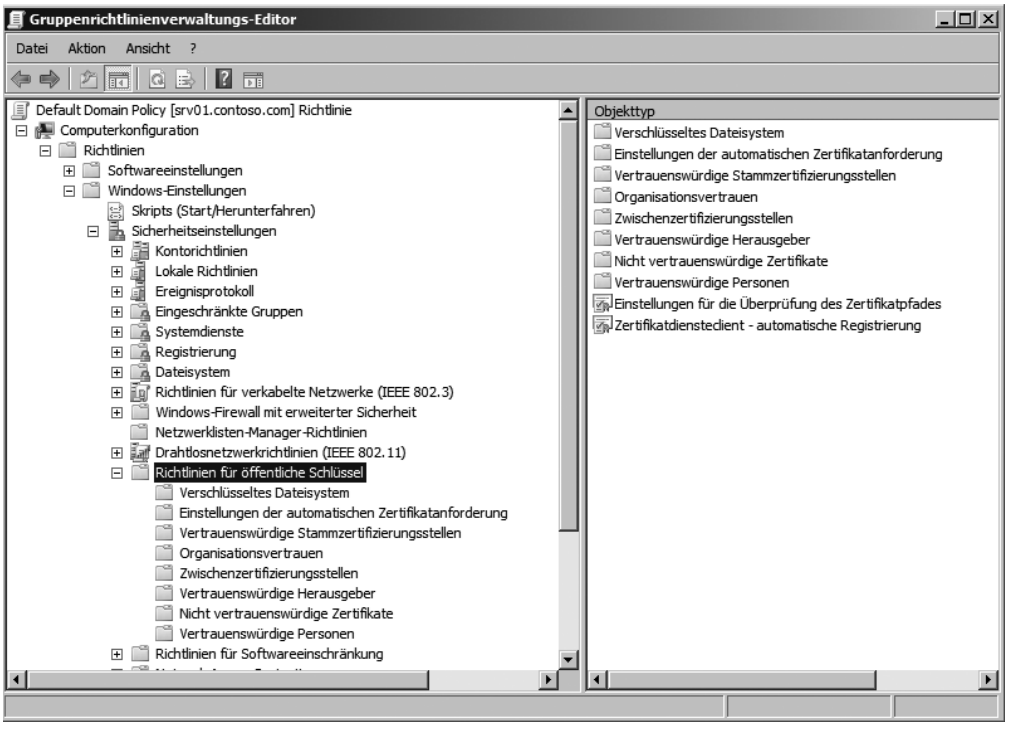
So veröffentlichen Sie über das Snap-In *Zertifizierungsstelle* eine neue Zertifikatsperrliste:

1. Klicken Sie mit der rechten Maustaste auf *Gesperrte Zertifikate*.
2. Wählen Sie im Kontextmenü den Untermenübefehl *Alle Aufgaben/Veröffentlichen*.

Verteilung der Zertifikatseinstellungen über Gruppenrichtlinien

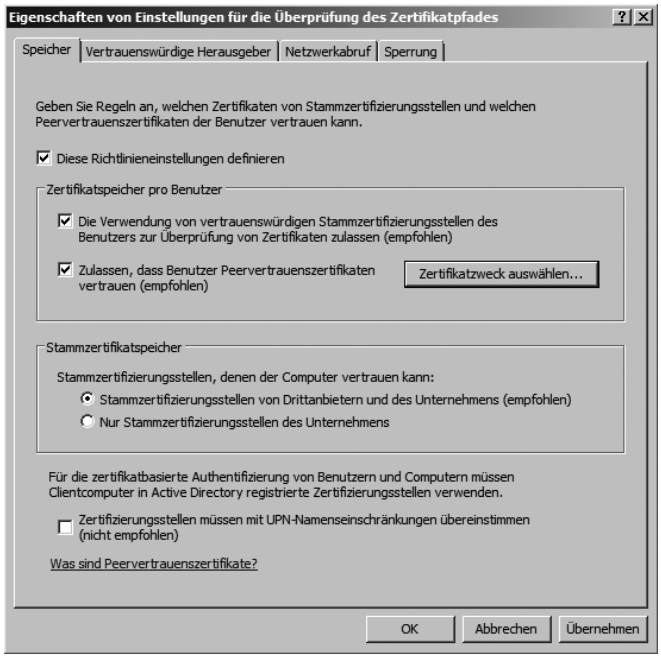
Der Einsatz einer CA macht vor allem in einem Active Directory Sinn. Vor allem, da die Einstellungen der Clients bezüglich des Verhaltens mit Zertifikaten über Gruppenrichtlinien eingestellt werden, haben davon insbesondere Unternehmen einige Vorteile. Neu in Windows Server 2008 ist die Möglichkeit, Zertifikate zu blockieren, die von der Sicherheitsrichtlinie als nicht vertrauenswürdig eingestuft werden. Die Einstellungen für Zertifikate finden Sie unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Richtlinien für öffentliche Schlüssel* (Abbildung 17.15). Über die Einstellungen an dieser Stelle werden zentral für alle Rechner einer Domäne Einstellungen vorgegeben. So kann zum Beispiel festgelegt werden, dass Anwender nur geprüfte und vertrauenswürdige Zertifikate herunterladen dürfen.

Abbildg. 17.15 Verwalten der Zertifikatseinstellungen einer Domäne über Gruppenrichtlinien

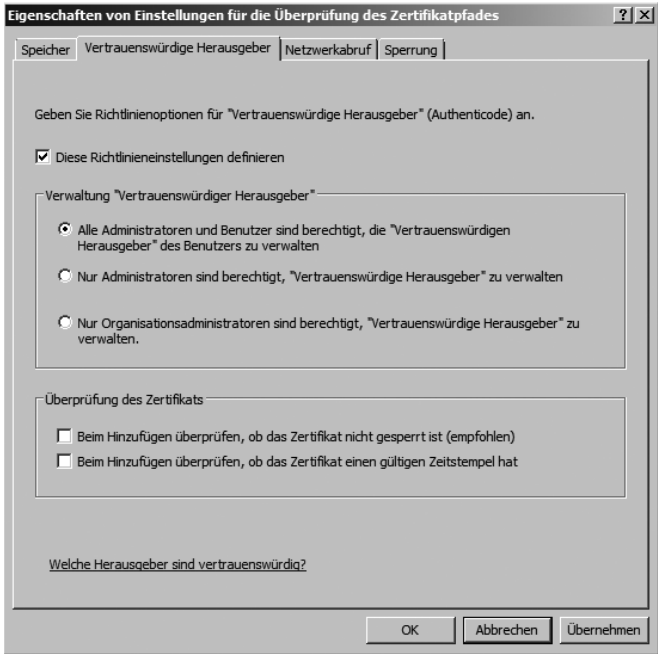


Die Einstellungen unter *Zwischenzertifizierungsstellen* und *Einstellungen für die Überprüfung des Zertifikatpfades* sind neu in Windows Server 2008. Vor allem die letztere Einstellung ist sehr wertvoll. Hier wird vorgegeben, welchen Zertifizierungsstellen die Computer in der Domäne vertrauen sollen. Per Doppelklick auf den Eintrag können Sie über mehrere Registerkarten Einstellungen vornehmen. Auf der Registerkarte *Speicher* wird die Richtlinie zunächst aktiviert (Abbildung 17.16). Anschließend kann definiert werden, dass die Anwender nur vertrauenswürdige Zertifikate verwenden dürfen, oder dass generell nur der Zertifizierungsstelle im Unternehmen vertraut werden soll.

Abbildg. 17.16 Verwalten der Zertifikatseinstellungen von Computern in einer Domäne



Abbildg. 17.17 Verwalten der Berechtigung zum Hinzufügen von neuen vertrauenswürdigen Zertifizierungsstellen auf Computern in der Domäne



Über die Registerkarte *Vertrauenswürdige Herausgeber* wird gesteuert, wer auf Computern die vertrauenswürdigen Zertifizierungsstellen verwalten darf. Das ist zum Beispiel wichtig beim Importieren von Zertifikaten in Heimarbeitsplätzen oder generell über den Internet Explorer. Wir kommen später noch ausführlicher zu diesem Thema zurück.

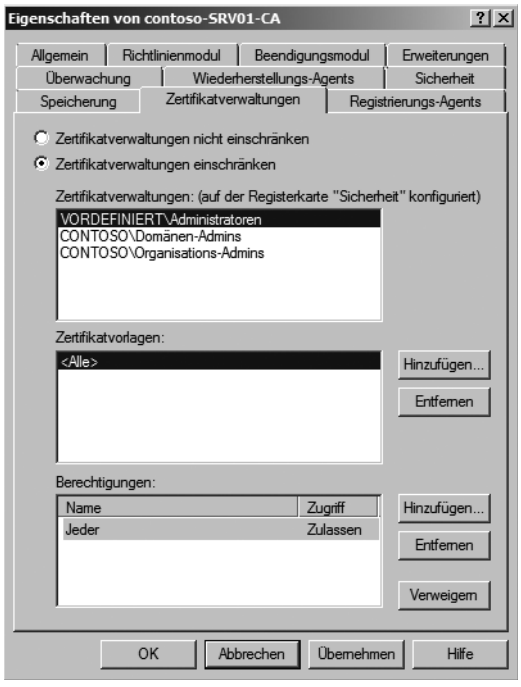
Sicherheit für Zertifizierungsstellen verwalten

Zum Betrieb einer Zertifizierungsstelle, gehört auch die Absicherung und die Steuerung der Berechtigungen für die CA. Die Active Directory-Zertifikatdienste sind vollständig in das Berechtigungsmodell von Active Directory integriert. Verwaltungsrollen können an verschiedene Personen in einer Organisation verteilt werden. Die rollenbasierte Verwaltung wird von Unternehmenszertifizierungsstellen und eigenständigen Zertifizierungsstellen unter Windows Server 2008 und Windows Server 2003 unterstützt. Folgende Rollen können zugewiesen werden. Als Basis dieser Rolle dienen die Berechtigungen auf der Registerkarte *Sicherheit* in den Eigenschaften der Zertifizierungsstelle. Jeder Zertifizierungsstellenrolle ist eine Liste mit Berechtigungen zugeordnet.

- **Zertifizierungsstellenadministrator** Diese Rolle hat umfassende Rechte zur Verwaltung der Zertifizierungsstelle. Außerdem dürfen mit dieser Rolle Rechte an andere Anwender delegiert werden. Für Unternehmenszertifizierungsstellen sind lokale Administratoren, Organisationsadministratoren und Domänenadministratoren standardmäßig Zertifizierungsstellenadministratoren. Bei einer eigenständigen Zertifizierungsstelle sind nur lokale Administratoren standardmäßig Zertifizierungsstellenadministratoren. Wenn eine eigenständige Zertifizierungsstelle auf einem Server installiert ist, der Mitglied einer Active Directory-Domäne ist, sind die Domänenadministratoren auch Zertifizierungsstellenadministratoren.
- **Zertifikatverwaltung** Mit dieser Rolle enthält ein Administrator das Recht zum Genehmigen von Zertifikatregistrierungs- und -sperrungsanforderungen.
- **Sicherungs-Operator** Mit dieser Rolle, kann eine Zertifizierungsstelle gesichert werden.
- **Auditor** Diese Rolle ist für das Verwalten von Überwachungs- und Sicherheitsprotokollen.
- **Registrieren** Registrierende sind Clients, die autorisiert sind, Zertifikate von einer Zertifizierungsstelle anzufordern.

Auf der Registerkarte *Zertifikatverwaltung* steuern Sie die Rechte der Gruppen. Rechte sollten nicht einzelnen Benutzern zugewiesen werden, sondern Gruppen. Anwender können dann durch die Mitgliedschaft in einer Gruppe entsprechend berechtigt werden. Klicken Sie auf der Registerkarte *Zertifikatverwaltungen* auf *Zertifikatverwaltungen einschränken* und überprüfen Sie, ob der Name der Gruppe oder des Benutzers angezeigt wird. Klicken Sie unter *Zertifikatvorlagen* auf *Hinzufügen* und wählen Sie die Vorlage für die Zertifikate aus, die von diesem Benutzer oder dieser Gruppe verwaltet werden sollen. Über *Berechtigungen* konfigurieren Sie die Rechte für die einzelnen Gruppen.

Abbildg. 17.18 Konfigurieren der Zertifikateverwaltung in den Eigenschaften der Zertifizierungsstelle

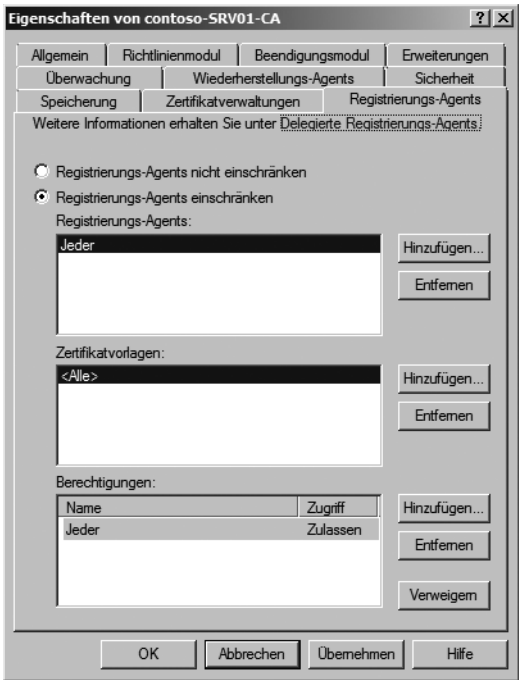


In Windows Server 2008 sind drei Zertifikatvorlagen enthalten, die unterschiedliche Registrierungs-Agenttypen aktivieren:

- **Registrierungs-Agent** Wird zum Anfordern von Zertifikaten im Namen eines anderen Antragstellers verwendet
- **Registrierungs-Agent (Computer)** Wird zum Anfordern von Zertifikaten im Namen eines anderen Computerantragstellers verwendet
- **Exchange-Registrierungs-Agent (Offlineanforderung)** Wird zum Anfordern von Zertifikaten im Namen eines anderen Antragstellers und zum Angeben des Antragstellernamens in der Anforderung verwendet. Diese Vorlage wird vom Registrierungsdienst für Netzwerkgeräte für dessen Registrierungs-Agent-Zertifikat verwendet.

Die Einstellungen für diese Agents werden auf der Registerkarte *Registrierungs-Agents* durchgeführt. Sie können Einschränkungen für Registrierungs-Agents nur auf Windows Server 2008-basierten Zertifizierungsstellen anwenden. Klicken Sie im Bereich *Registrierungs-Agents* auf *Hinzufügen* und geben Sie die Namen des Benutzers oder der Gruppen ein. Klicken Sie bei Zertifikatvorlagen auf *Hinzufügen* und wählen Sie die Vorlage für die Zertifikate aus, mit denen sich dieser Benutzer oder diese Gruppe registrieren kann.

Abbildg. 17.19 Konfigurieren der Registrierungs-Agenten



Auf der Registerkarte *Überwachung* werden die zu überwachenden Ereignisse ausgewählt. Die generellen Optionen der Überwachungsrichtlinie können in Gruppenrichtlinie unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien* eingestellt werden. Die Ereignisse werden im Überwachungsprotokoll der Ereignisanzeige festgehalten.

Sichern von Active Directory-Zertifikatdiensten

Die wichtigsten Daten der Active Directory-Zertifikatdienste lassen sich auch sichern. Wählen Sie im Kontextmenü der Zertifizierungsstelle in der Verwaltungskonsole die Option *Alle Aufgaben/Zertifizierungsstelle sichern*. Anschließend startet der Assistent, über den die Zertifizierungsstelle und deren Daten gesichert werden können.

Auf der nächsten Seite des Assistenten wählen Sie aus, welche Dateien gesichert werden sollen und in welcher Datei die Sicherung abgelegt wird. Anschließend vergeben Sie ein Kennwort für die Sicherung, damit niemand Zugriff auf die Daten erhält. Im Anschluss wird die Zertifizierungsstelle gesichert. Auf dem gleichen Weg lassen sich auch Daten wiederherstellen.

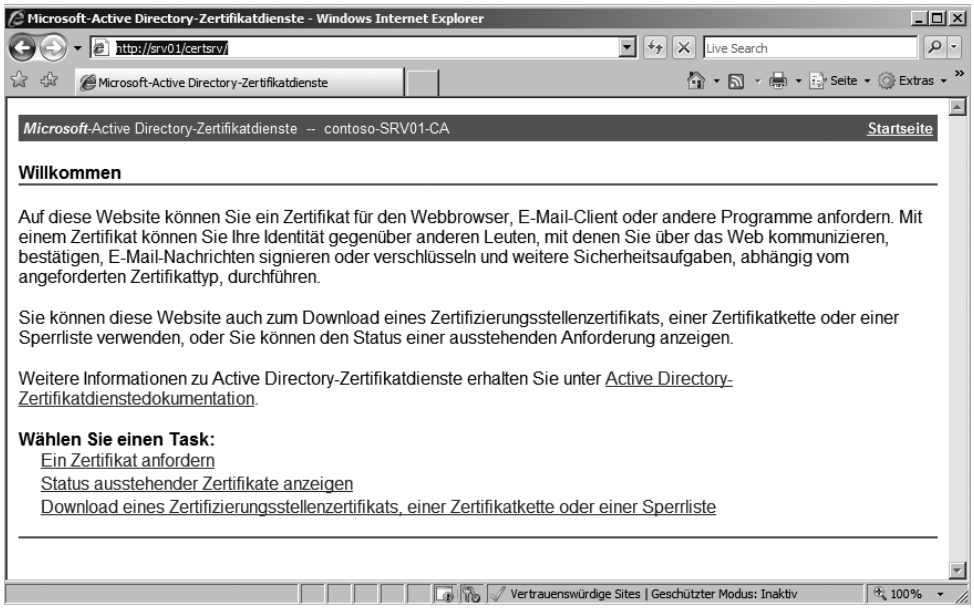
Abbildg. 17.20 Sichern einer Zertifizierungsstelle

Zuweisen und installieren eines Zertifikats zu einem Server am Beispiel von Exchange Server 2007 mit SP1

Mit dem Service Pack 1 für Exchange Server 2007 wird auch die Installation unter Windows Server 2008 unterstützt. Im folgenden Abschnitt zeigen wir Ihnen, wie Sie von einem Exchange Server 2007 SP1-Computer unter Windows Server 2008, ein Zertifikat von einer Zertifizierungsstelle unter Windows Server 2008 anfordern und installieren. Generell können Sie bei der Zuweisung eines Zertifikates auch den Weg über die lokale Verwaltung der Zertifikate gehen, wie in Kapitel 16 erläutert, aber die Zuweisung über die Weboberfläche funktioniert ebenso zuverlässig:

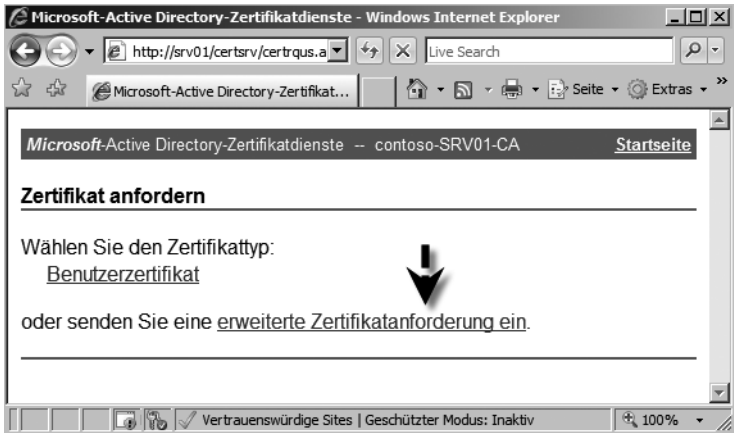
1. Um einem Server ein Zertifikat zuzuordnen, rufen Sie zunächst von diesem Server aus die Webseite der Zertifikatdienste mit der URL *https://<Server>/Certsrv* auf. Stellen Sie daher sicher, dass für die Zertifizierungsstellen-Webseite und den Webserver an sich SSL konfiguriert wurde. Der Verbindungsaufbau gelingt zwar auch ohne HTTPS, allerdings verlangt eine erweiterte Zertifikatsanforderung eine Verbindung per SSL und bricht die Anfrage sonst ab. Der Server baut nach Abfrage des Benutzernamens und des Kennworts eine Verbindung zu den Zertifikatdiensten auf:
2. Wählen Sie als Nächstes *Ein Zertifikat anfordern* aus, um ein Zertifikat vom Zertifikatserver anzufordern.
3. Auf der nächsten Seite wählen Sie aus, welches Zertifikat Sie anfordern wollen. Wählen Sie hier *Erweiterte Zertifikatanforderung* aus, wenn zum Beispiel ein neues Serverzertifikat für Exchange Server 2007 ausgestellt werden soll.

Abbildg. 17.21 Abrufen eines Zertifikats über die Weboberfläche der Zertifizierungsstelle



4. Haben Sie die Art des Zertifikats bestimmt, erscheint im nächsten Fenster eine Abfrage, welche Aktion Sie mit dem Zertifikat durchführen wollen. Wählen Sie hier *Eine Anforderung an diese Zertifizierungsstelle erstellen und einreichen*. In diesem Fall wird das Zertifikat sofort erstellt und kann auf dem Exchange-Server installiert werden.

Abbildg. 17.22 Erstellen einer erweiterten Zertifikatsanforderung



5. Auf der nächsten Seite geben Sie die Daten ein, die zur Ausstellung des Zertifikats benötigt werden. Zunächst müssen Sie auswählen, welches Zertifikat Sie anfordern wollen. Wählen Sie *Webserver* aus, da es sich bei Outlook Web Access um eine Erweiterung des lokalen IIS handelt. Geben Sie im Feld *Name* die Bezeichnung des Servers ein. Ohne die Eingabe eines Namens wird

das Zertifikat verweigert. Aktivieren Sie zusätzlich die Option *Zertifikat in lokalem Zertifikatspeicher aufbewahren*. Aktivieren Sie diese Option nicht, kann unter Umständen das Zertifikat später nicht in den Webserver eingelesen werden. Ansonsten können Sie alle Einstellungen so lassen, wie sie sind. Dieses Zertifikat kann später nicht nur für die SSL-Verschlüsselung von Outlook Web Access, sondern auch für RPC über HTTPS (Outlook Anywhere) und die Anbindung der Smartphones über Exchange ActiveSync (EAS), das ebenfalls über SSL abgesichert wird, verwendet werden.

TIPP Passen Sie im Feld *Name* die Bezeichnung des Zertifikats am besten gleich daran an, wie Sie später Outlook Web Access im Internet veröffentlichen. Veröffentlichen Sie zum Beispiel Outlook Web Access über einen ISA und verwenden den Namen *webmail.firma.com*, also nicht den internen FQDN des Servers, sollten Sie als Namen für das hier angeforderte Zertifikat auch den externen FQDN-Namen verwenden. Verbinden sich Benutzer über einen anderen Link, dann erhalten diese eine Meldung, die Sie bestätigen müssen, wenn der Zertifikatname und der Verbindungsname nicht übereinstimmen. Bei der Veröffentlichung über einen ISA ist die identische Bezeichnung von Veröffentlichung und Zertifikat zwingend.

6. Je nach Anforderung können Sie hier zudem die Verschlüsselungsstufe anpassen. Sie müssen an dieser Stelle aber keine weiteren Eingaben vornehmen. Die Voreinstellungen für ein Zertifikat sind vollkommen ausreichend für den Zugriff auf Outlook Web Access oder andere Webdienste. Eine intensivere Beschäftigung mit einzelnen Zertifikaten und deren Verschlüsselung würde allerdings den Rahmen des Kapitels und des Buches sprengen. Haben Sie alle Eingaben nach Ihren Vorstellungen durchgeführt, können Sie das Zertifikat von diesem Zertifikatserver mit *Einsenden* anfordern.

Wurde das Zertifikat erfolgreich angefordert, können Sie es auf dem Server installieren lassen. Es erscheint ein entsprechendes Fenster, in dem Sie die Installation durch einen Klick auf den entsprechenden Link durchführen können. Mit der Installation des Zertifikats ist die Konfiguration allerdings noch nicht abgeschlossen. Das Zertifikat muss noch in Outlook Web Access integriert werden.

Zuweisen eines Zertifikats einer Webseite am Beispiel von Outlook Web Access

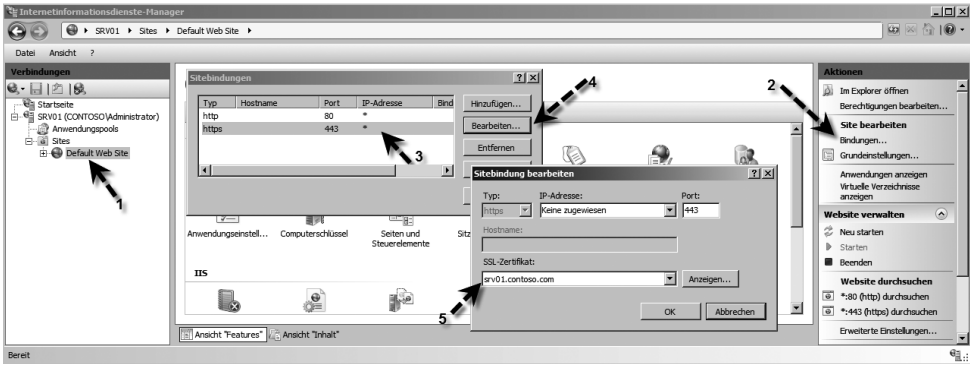
Um einer Webseite generell, oder Outlook Web Access speziell in diesem Beispiel, ein Zertifikat zuzuweisen und SSL zu verwenden, müssen Sie mit dem Snap-In zur Verwaltung von IIS arbeiten:

1. Starten Sie dazu den Internetinformationsdienste-Manager aus dem Menü *Verwaltung*. Nach dem Start klicken Sie auf der linken Seite auf den Servernamen. In der Mitte des Bildschirms wird per Doppelklick auf *Serverzertifikate* die Verwaltung der lokalen Serverzertifikate gestartet, die in IIS verwendet werden können. Hier wird das neue Zertifikat angezeigt, sowie das selbstsignierte Zertifikat von IIS und das selbstsignierte Zertifikat von Exchange Server 2007 (Abbildung 17.23). Über das *Aktionen*-Menü lassen sich ebenfalls neue Zertifikate anfordern.

Abbildg. 17.23 Verwalten der Serverzertifikate eines Webservers

2. Klicken Sie als Nächstes auf *Sites/Default Web Site*.
3. Klicken Sie im Aktionsbereich auf den Link *Bindungen*. Jetzt werden alle Ports, IP-Adressen und Protokolle angezeigt, auf welche die Webseite und alle untergeordneten Applikationen und Webseiten hören (Abbildung 17.24).
4. Markieren Sie den SSL-Eintrag und klicken Sie auf *Bearbeiten*. Jetzt kann das Webserverzertifikat ausgewählt werden, das von der *Default Web Site* und allen untergeordneten Webseiten verwendet wird. Das Zertifikat und dessen Daten kann in diesem Fenster auch angezeigt werden.

Abbildg. 17.24 Verwalten des Serverzertifikats einer Webseite

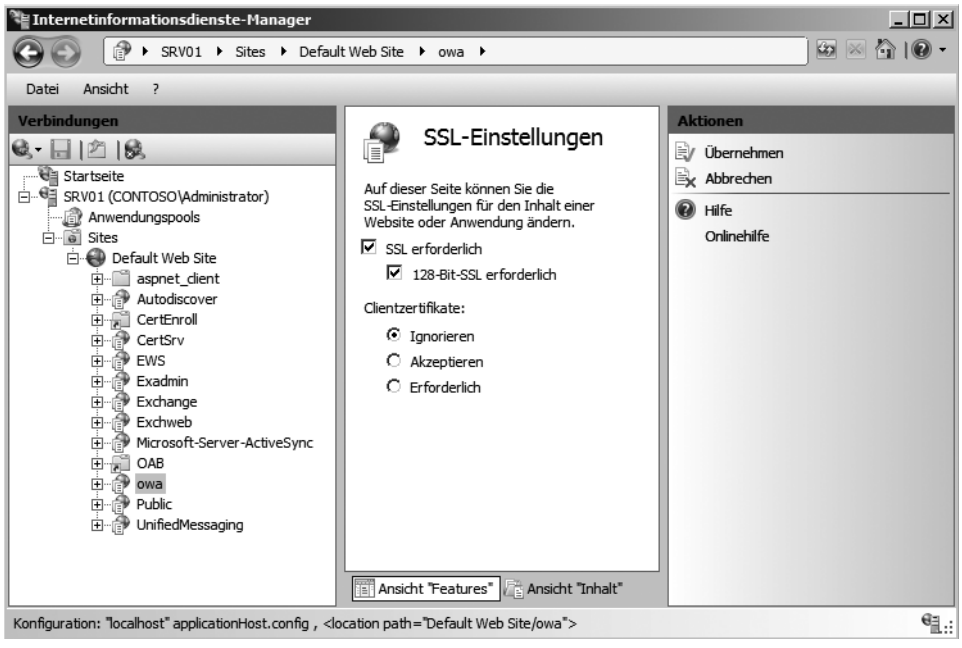


Aktivieren von SSL für Outlook Web Access

Um SSL für eine Webseite, in diesem Beispiel von Outlook Web Access zu aktivieren, navigieren Sie im Internetinformationsdienste-Manager zu den Unterordnern *OWA* (für Zugriff auf Exchange Server 2007-Mailbox-Server) und *Exchange* (für Zugriff auf Exchange-Server 2000/2003-Mailbox-Server) der Standardwebsite:

1. Klicken Sie auf *SSL-Einstellungen.*
2. Aktivieren Sie hier die beiden Optionen *SSL erforderlich* und *128-Bit-Verschlüsselung erforderlich*. Von nun an können sich Benutzer nicht mehr über HTTP mit Outlook Web Access verbinden, sondern nur noch mit HTTPS. Um eine Verbindung zu Outlook Web Access herzustellen, müssen die Anwender zukünftig *https://<Servername>/owa* in ihren Browser eingeben.

Abbildg. 17.25 Konfigurieren der SSL-Einstellungen für eine Webseite



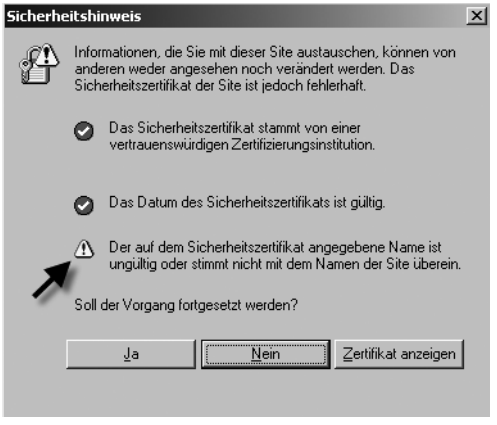
Stellen Benutzer eine Verbindung zum Server her, wird immer zuerst ein Zertifikat übertragen. Die Benutzer erhalten hierzu eine Meldung, die sie zunächst bestätigen müssen. Diese Meldung erscheint jedoch nicht, wenn der Servername und der Zertifikatname identisch sind. Haben Sie als Name für das Zertifikat den Namen verwendet, den Sie später im Internet verwenden, erhalten die internen Anwender eine Fehlermeldung, da sich dieser Name vom internen Namen unterscheidet. An der Fehlermeldung erkennen Sie die Problematik: Der Name des Zertifikats und die Adresse müssen übereinstimmen. Da es wichtiger ist, dass der Zugriff von extern funktioniert, ist die Verwendung des externen Namens auch effizienter. Versucht ein Benutzer, noch über HTTP eine Verbindung zu Outlook Web Access aufzubauen, erhält er eine Fehlermeldung angezeigt, in der er darauf hingewiesen wird, dass diese Webseite nur mit SSL zu erreichen ist. Wurde das Zertifikat erfolgreich übertragen, erscheint die neue Anmeldeseite von Outlook Web Access.

Wurde das Zertifikat übertragen, können Sie dieses im Internet Explorer per Klick auf das kleine Schlosssymbol in der Statusleiste des Internet Explorers anzeigen lassen.

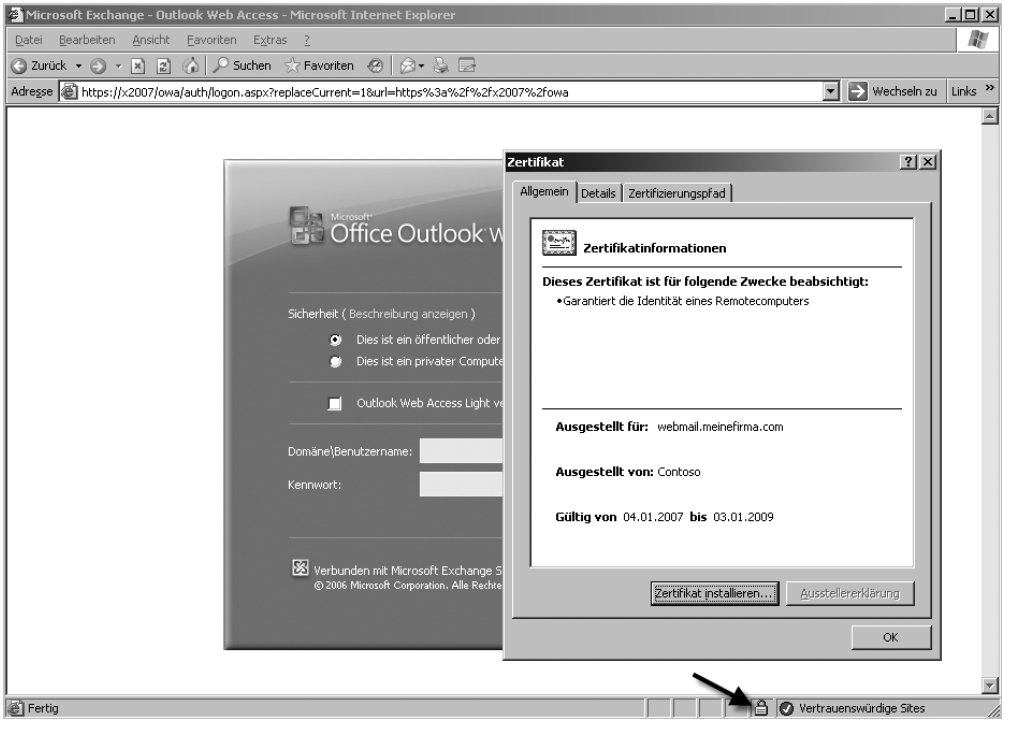
TIPP Testen Sie nach der Einrichtung die Verbindung per OWA über den Client-Access-Server von Exchange Server 2007 SP1 ohne die Verbindung über den ISA Server. Es müsste sich eine Verbindung aufbauen. Intern erhalten Sie unter Umständen die Zertifikatswarnung, da der Name der externen Verbindung hinterlegt ist, aber der interne Aufbau über den internen Namen durchgeführt wird. Ideal wäre es, wenn Sie zu Testzwecken auf den DNS-Servern in Active Directory eine neue Zone anlegen, welche die Bezeichnung Ihrer Internetdomäne trägt, unter der Sie später OWA veröffentlichen, zum Beispiel *meinefirma.de*. Tragen Sie in dieser Domäne einen statischen Eintrag *webmail* ein und weisen Sie dem Eintrag die interne IP-Adresse des Client-Access-Servers zu. Jetzt können Sie im Internet Explorer den Verbindungsaufbau zu *https://webmail.meinefirma.de/owa* testen. Es sollte sich eine Verbindung ohne Fehlermeldung des Zertifikats auf-

bauen lassen, da der FQDN des Zertifikats jetzt stimmt. Funktioniert der interne Verbindungsaufbau, ohne eine Zertifikatmeldung anzuzeigen, können Sie mit der Veröffentlichung auf dem ISA Server fortfahren.

Abbildg. 17.26 Warnmeldung eines Zertifikats bei einem ungültigen Namen



Abbildg. 17.27 Anzeigen eines Serverzertifikats im Internet Explorer 6

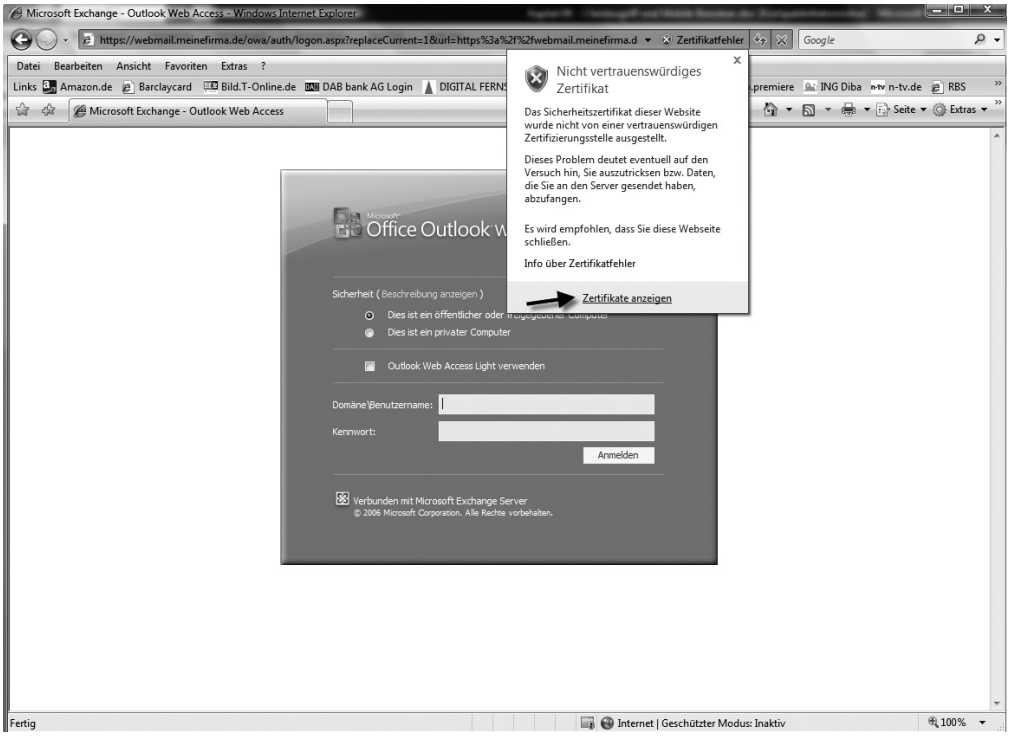


Bauen Sie mit Windows Vista und dem Internet Explorer 7 eine Verbindung mit Outlook Web Access auf, erhalten Sie eine Zertifikatswarnung und das Laden der Seite wird angehalten. Erst wenn Sie auf den Link klicken, um das Laden fortzusetzen, baut sich die Anmeldeseite von Outlook Web Access auf.

Abbildg. 17.28 Zertifikatfehler werden im IE 7 drastischer dargestellt als noch im IE 6

Wurde die Seite geladen, können Sie über den Zertifikatfehler oben in der Adressliste das Zertifikat anzeigen. Damit dieser Fehler nicht mehr angezeigt wird, muss das Zertifikat der Stammzertifizierungsstelle Ihres Unternehmens in die vertrauenswürdigen Stammzertifizierungsstellen auf dem Client-PC importiert werden. Für die stabile Arbeit mit Outlook Web Access wird das nicht benötigt, allerdings zwingend für Exchange ActiveSync und Outlook Anywhere. Ist ein Computer Mitglied der gleichen Domäne wie der Zertifikateserver, wird das Zertifikat der Stammzertifizierungsstelle automatisch importiert.

Abbildg. 17.29 Anzeigen eines Zertifikats im Internet Explorer 7 unter Windows Vista

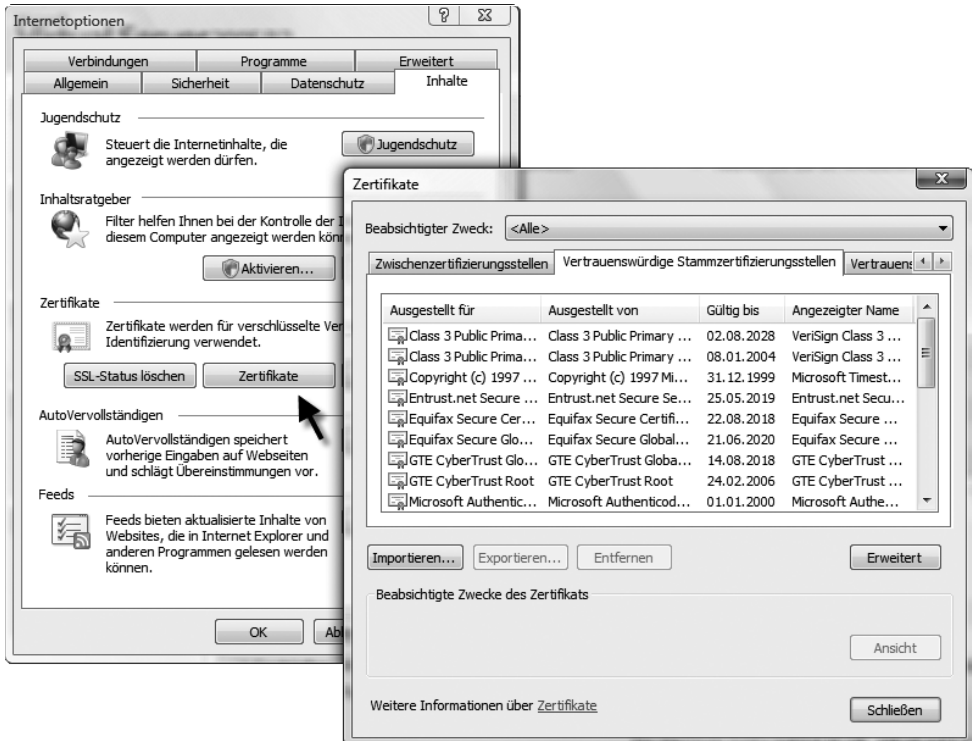


Importieren des Zertifikats auf einem Client-PC

Wurde auf dem Client-PC die Zertifizierungsstelle Ihres Unternehmens noch als nicht vertrauenswürdig eingestuft (was normal ist, wenn der PC nicht Mitglied der Domäne ist), sollten Sie vor dem Verbindungstest zunächst das Zertifikat der Zertifikatstelle auf den PC importieren. Dieses Zertifikat hat nichts mit dem Webserverzertifikat zu tun, dass Sie ausgestellt haben.

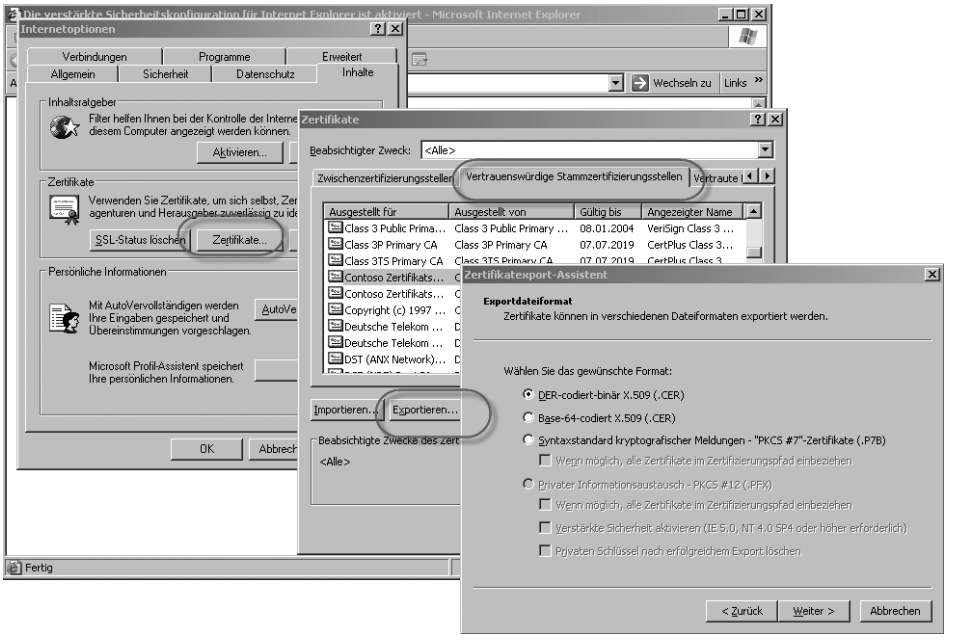
1. Die vertrauenswürdigen Zertifizierungsstellen finden Sie am besten über den Internet Explorer. Rufen Sie nach dem Start über *Extras/Internetoptionen* die Registerkarte *Inhalte* und dann per Klick auf die Schaltfläche *Zertifikate* und Auswahl der Registerkarte *Vertrauenswürdige Stammzertifizierungsstellen* die Auflistung der Zertifizierungsstellen auf dem PC auf.
2. Ist Ihre interne Zertifizierungsstelle Ihres Unternehmens hier nicht zu finden, erscheinen Zertifikatfehler, sobald auf interne Firmenwebseiten oder Outlook Web Access zugegriffen wird.

Abbildg. 17.30 Anzeigen und Verwalten der vertrauenswürdigen Stammzertifizierungsstellen auf einem Client-Computer



3. Rufen Sie auf dem Webserver, oder beim Einsatz von Exchange Server 2007 auf dem Client-Access-Server die gleiche Registerkarte auf. Hier sollte die Zertifizierungsstelle hinterlegt sein, da sich der Server in der Domäne befindet. Markieren Sie diese Zertifizierungsstelle und klicken Sie auf die Schaltfläche *Exportieren*. Unter Umständen tauchen an dieser Stelle mehrere Zertifikate Ihrer Stammzertifizierungsstelle auf. Erscheint beim Exportieren eine Abfrage des privaten Schlüssels des Zertifikats, haben Sie das falsche erwischt. Verwenden Sie dann einfach das andere Zertifikat.
4. Exportieren Sie auf dem Client-Access-Server das Zertifikat in eine CER-Datei. Diese Datei muss im Anschluss auf dem Client importiert werden. Klicken Sie doppelt auf das Zertifikat, wird es auf dem Client-PC angezeigt und Sie können es installieren. Klicken Sie auf die Schaltfläche *Zertifikat installieren*, damit das Zertifikat auf dem Client-PC installiert wird.

Abbildg. 17.31 Exportieren eines Zertifikats auf dem Exchange-Server



Lassen Sie das Stammzertifikat in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen importieren. Überprüfen Sie anschließend, ob das Zertifikat erfolgreich importiert wurde. Auf allen beteiligten Servern und Arbeitsstationen muss der Zertifizierungsstelle des Unternehmens auf dieser Registerkarte vertraut werden. Dies gilt auch für den ISA-Server.

Abbildg. 17.32 Importieren eines Zertifikats in die vertrauenswürdigen Stammzertifizierungsstellen eines PC

Importieren eines Zertifikats und Konfiguration der vertrauenswürdigen Stammzertifizierungsstelle

Eine weitere Möglichkeit das Zertifikat der Stammzertifizierungsstelle zu importieren, ist über Outlook Web Access. Dieser Weg funktioniert allerdings nicht immer, da meist nur das Webserver-Zertifikat übertragen wird, nicht zusätzlich noch das Zertifikat der Stammzertifizierungsstelle. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie eine Verbindung zu Outlook Web Access mit dem Internet Explorer. Bei diesem Vorgang wird das Zertifikat übertragen.
2. Klicken Sie anschließend auf das kleine Schloss-Symbol in der Statusleiste des Internet Explorers. Das Zertifikat der Seite wird angezeigt.
3. Öffnen Sie die Registerkarte *Zertifizierungspfad*.
4. Markieren Sie das oberste Zertifikat im Pfad, da dieses das Zertifikat der Zertifizierungsstelle darstellt. Uns geht es nicht darum, das Zertifikat zu importieren, sondern die Zertifizierungsstelle des Unternehmens als vertrauenswürdige Zertifizierungsstelle zu importieren. Wird hier kein weiteres Zertifikat angezeigt, funktioniert dieser Weg nicht. Das Zertifikat der Zertifizierungsstelle wird in diesem Fall nicht übertragen.
5. Klicken Sie nun auf *Zertifikat anzeigen*.
6. Holen Sie im neuen Fenster die Registerkarte *Details* in den Vordergrund und klicken Sie auf die Schaltfläche *In Datei kopieren*, um das Zertifikat in eine Datei zu exportieren.
7. Übernehmen Sie die Standardeinstellungen und exportieren Sie das Zertifikat in eine Datei, die Sie zum Beispiel auf dem Desktop ablegen.
8. Schließen Sie alle Fenster und klicken Sie doppelt auf die Zertifikatdatei, um so den Assistenten für den Import zu öffnen.
9. Klicken Sie auf die Schaltfläche *Zertifikat installieren*.
10. Wählen Sie im Fenster *Zertifikatspeicher* die Option *Alle Zertifikate in folgendem Speicher speichern* aus und klicken Sie auf *Durchsuchen*.
11. Wählen Sie die Option *Vertrauenswürdige Stammzertifizierungsstellen* aus und schließen Sie den Import ab.

Sicherheitszertifikate unter Windows Mobile

Arbeiten Sie mit Exchange ActiveSync, muss auch auf den mobilen Geräten das Zertifikat der Stammzertifizierungsstelle installiert werden. Sie finden die Zertifikate auf dem Pocket-PC über *Start/Einstellungen/System/Zertifikate/Stamm*. Es werden Ihnen alle Zertifizierungsstellen angezeigt, denen das Gerät vertraut. Wird hier Ihre Zertifizierungsstelle nicht angezeigt, kann die Synchronisierung nicht funktionieren. Damit Sie die Zertifizierungsstelle als vertrauenswürdig auf dem Pocket-PC hinterlegen können, benötigen Sie eine SD-Karte, auf der Sie eine Zertifikatdatei abspeichern können, oder eine Dockingstation. Diese Datei exportieren Sie am besten über einen Client, mit dem Sie per Outlook Web Access oder Outlook Anywhere Verbindung aufbauen können, oder direkt auf dem Server. Achten Sie beim Exportieren des Zertifikats der Stammzertifizierungsstelle darauf, dass Sie den privaten Schlüssel nicht mit exportieren müssen, es genügt der öffentliche Schlüssel.

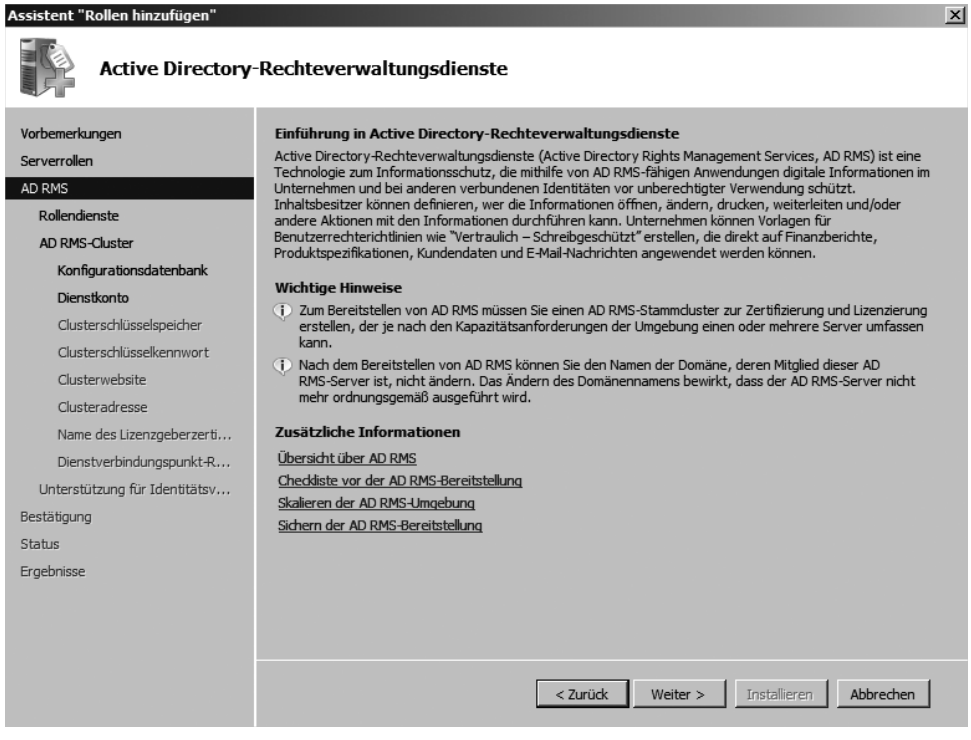
Exportieren Sie das Zertifikat in eine Datei. Diese Datei muss später per SD-Karte auf den Pocket-PC integriert werden. Alternativ können Sie die Datei auch über die ActiveSync-Funktion vom Arbeitsplatz auf das Gerät kopieren. Das Zertifikat muss auf jeden Fall zuerst auf dem Gerät zur Ver-

fügung stehen, bevor Sie per Exchange ActiveSync Daten übertragen können. Im Anschluss klicken Sie auf dem Pocket-PC auf die Zertifikatsdatei und lassen diese in die vertrauenswürdigen Stammzertifizierungsstellen importieren. Es reicht nicht aus, wenn das Zertifikat nur auf dem Pocket-PC installiert wird. Es ist wichtig, dass das Zertifikat bei den vertrauenswürdigen Stammzertifizierungsstellen hinterlegt wird. Lassen Sie die exportierte Zertifikatedatei per File Explorer (Datei Explorer) auf dem Endgerät anzeigen, reicht es aus, diese Datei anzuklicken, damit diese installiert werden kann. Haben Sie die Zertifikatedatei angeklickt, erkennt das Endgerät automatisch, dass es sich um ein Zertifikat handelt und schlägt die Installation vor. Vertraut der Pocket-PC der Stammzertifizierungsstelle des Unternehmens, kann die Synchronisierung durchgeführt werden.

Active Directory-Rechteverwaltung

Mit der Active Directory-Rechteverwaltung können Dateien, die mit kompatiblen Anwendungen erstellt wurden, mit digitalen Signaturen innerhalb und außerhalb des Unternehmens geschützt werden. Die internen Anwender im Unternehmen können auf diesem Weg zum Beispiel spezielle Benutzerrechte für einzelne Dokumente vergeben, wenn die Applikation AD RMS (Active Directory Rights Management Services) unterstützt. Um solche Dateien zur Verfügung zu stellen, gibt es zwei Möglichkeiten: Die Online-Veröffentlichung und die Offline-Veröffentlichung. Bei der ersten Verwendung von AD RMS erhalten interne Anwender automatisch ein Rights Account Certificate (RAC) und ein Client Licensor Certificate (CLC) ausgestellt. Anschließend können Anwender mit kompatiblen Applikationen Dateien erstellen und Benutzerrechte vergeben.

Abbildg. 17.33 AD RMS installieren



Die Domänencontroller in Active Directory kennen dazu den Standort und Servernamen der AD RMS-Server. Die Applikation erstellt daraufhin einen speziellen Inhaltsschlüssel, mit dem der Inhalt der Datei verschlüsselt wird. Der Anwender kann diese Datei jetzt online veröffentlichen oder offline. Bei der Online-Veröffentlichung wird der Inhaltsschlüssel mit dem öffentlichen Schlüssel des AD RMS-Servers verschlüsselt und zum AD RMS-Server geschickt. Der Server erstellt und signiert anschließend eine Publishing License (PL). Bei der Offline-Veröffentlichung, wird der Inhaltsschlüssel stattdessen mit dem öffentlichen Schlüssel des Client Licensor Certificates (CLC) verschlüsselt, sowie eine Kopie dieses Schlüssels mit dem öffentlichen Schlüssel des AD RMS-Servers. Die Publishing License (PL) wird in diesem Fall mit Hilfe des privaten Schlüssels des CLC signiert. Die PL wird anschließend an den verschlüsselten Inhalt der Datei angehängt. Die Daten des AD RMS-Servers, zum Beispiel die Daten der Zertifikate, die Schlüsselpaare und sonstigen Informationen, werden in einer sicheren SQL Server-Datenbank gespeichert.

In kleinen Umgebungen kann dazu der SQL Server auch auf dem AD RMS-Server betrieben werden. In größeren Infrastrukturen, die stark auf AD RMS setzen, sollte der SQL Server auf einem eigenen Server installiert werden. Dem Empfänger kann nach der Verschlüsselung die Datei zur Verfügung gestellt werden, auch per E-Mail. Der Empfänger öffnet die Datei über seinen Webbrowser, idealerweise den Internet Explorer oder einer AD RMS-kompatiblen Anwendung. Ist auf dem Client kein Zertifikat vorhanden, wird vom AD RMS-Server eines angefordert. Die URL zum AD RMS-Server ist in der Datei hinterlegt, der Server muss bei externem Zugriff über das Internet erreichbar sein. Die Datei sendet eine Benutzungsanfrage zum Server, der die Publishing License ausgestellt hat. Der Server stellt anschließend fest, ob der Empfänger berechtigt ist, die Datei zu öffnen, und stellt für den speziellen Anwender eine Benutzerlizenz aus. Anschließend wird der Inhalt der Datei mit dem privaten Schlüssel des Servers entschlüsselt und mit dem öffentlichen Schlüssel des Empfängers wieder verschlüsselt.

Auf diesem Weg kann ausschließlich der festgelegte Empfänger auf die Datei zugreifen. Die Benutzerlizenz wird auf den Computer des Empfängers übertragen. Nur wenn sowohl die Lizenz der Datei als auch die Benutzerlizenz in Ordnung sind, werden dem Empfänger die Rechte zugewiesen, die der Ersteller der Datei hinterlegt hat. Über die Active Directory Federation Services (AD FS) kann AD RMS auch für externe Anwender eingesetzt werden. Dazu werden die Authentifizierungsanfragen zum AD RMS-Server über AD FS gesteuert. Beide Komponenten gehören zum Lieferumfang von Windows Server 2008.

ACHTUNG Nur die Editionen Ultimate, Professional Plus und Enterprise von Microsoft Office 2007 unterstützen die Active Directory-Rechteverwaltungsdienste.

Aufbau einer Testumgebung für Active Directory-Rechteverwaltung

In diesem Abschnitt zeigen wir Ihnen am Beispiel einer Testumgebung den Aufbau einer Active Directory-Rechteverwaltungsstruktur. Idealerweise wird dazu eine Active Directory-Domäne, ein Datenbankserver mit SQL Server 2005 Standard Edition, ein Active Directory-Rechteverwaltung (AD RMS)-Client und schließlich der Server mit der Serverrolle AD RMS benötigt. Durch den Aufbau dieser Testumgebung lernen Sie die optimale Einführung und die Möglichkeiten von AD RMS im Unternehmen kennen. Auch für Windows Server 2003 gibt es eine Erweiterung für AD RMS. Die Möglichkeiten sind recht ähnlich, auch wenn AD RMS in Windows Server 2008 mehr Möglichkeiten bietet und direkt in Active Directory integriert ist. Ausführlichere Informationen über den Nut-

zen von AD RMS im Unternehmen erhalten Sie über die Webseiten *http://go.microsoft.com/fwlink/?LinkId=68637* und *http://technet2.microsoft.com/windowsserver2008/de/library/d5bf2071-43d3-4f47-a5ac-24a1ca2a17e11031.mspx?mfr=true*. Windows Server 2008-AD RMS kann auch in einer Windows Server 2003-Gesamtstruktur betrieben werden. Dazu wird der AD RMS-Server als Mitglied in einer Windows Server 2003-Domäne aufgenommen.

Vorbereitung der Testumgebung

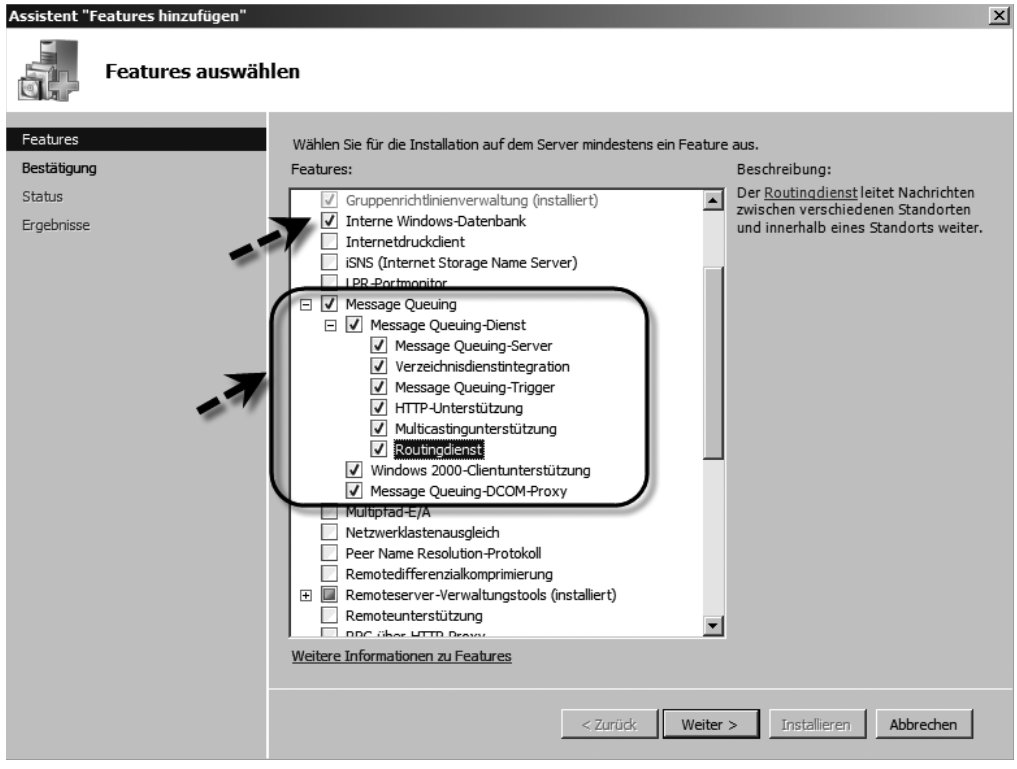
Um die Testumgebung vorzubereiten, benötigen Sie am besten einen Server mit Windows Server 2008, den Sie zum Domänencontroller heraufstufen. Legen Sie mehrere Benutzerkonten an, sowie einige universale Gruppen und verteilen die Test-Benutzerkonten in die universalen Gruppen, welche Abteilungen im Unternehmen widerspiegeln sollten. Außerdem benötigen Sie einen Mitgliedsserver mit einer installierten SQL Server-Instanz. Zusätzlich wird ein Windows Vista SP1-Computer mit installiertem Microsoft Office 2007 am besten in der Enterprise Edition benötigt. Auch eine Testinstallation von Exchange Server 2007 mit SP1 kann sinnvoll sein, um das Versenden von AD RMS geschützten Dokumenten in einem Unternehmen zu simulieren. Der Betriebsmodus der Domäne sollte möglichst Windows Server 2003 sein, da universale Gruppen für eine AD RMS-Struktur am besten geeignet sind. Auf dem Datenbankserver erstellen Sie eine Freigabe in der die Anwender Daten ablegen können.

Installation der Active Directory-Rechteverwaltungsdienste

Bevor Sie AD RMS auf einem Server installieren, sollten zunächst die Internetinformationsdienste in den Standardeinstellungen installiert werden. Außerdem wird noch das Feature *Interne Windows-Datenbank* benötigt. Auch diese Funktion ist neu in Windows Server 2008. Hierbei handelt es sich um eine kostenlose relationale Datenbank, die zum Beispiel für die SharePoint Services 3.0 verwendet wird. Die Datenbank kann allerdings nicht von Dritthersteller-Produkten verwendet werden, sondern nur von den Funktionen und Rollen in Windows Server 2008, also neben den SharePoint Services 3.0 noch WSUS, UDDI der Windows System Resource Manager und die Rechteverwaltung. Ein weiteres Feature, das für den AD RMS-Server benötigt wird, ist *Message Queuing*. Mit dieser Funktion können Nachrichten gesichert und überwacht zwischen Applikationen auf dem Server ausgetauscht werden. Nachrichten können priorisiert werden und es gibt eine Vielzahl an Möglichkeiten, um die Konfiguration anzupassen. Message Queuing (auch als MSMQ bezeichnet) ist sowohl eine Kommunikationsinfrastruktur als auch ein Entwicklungswerkzeug. Für Systemadministratoren als auch für Softwareentwickler bietet Message Queuing interessante Möglichkeiten (Installation und Verwaltung der Infrastruktur, Entwicklung von Nachrichtenanwendungen).

AD RMS kann auch in einem Cluster betrieben werden. Der erste AD RMS-Server in einer AD RMS-Infrastruktur wird als AD RMS Root-Cluster bezeichnet. Dieser Cluster besteht aus einem oder mehreren Servern, die in einer Loadbalancing-Umgebung zusammengefasst werden. In einer Testumgebung kann dieser Cluster auch aus einem einzelnen AD RMS-Server bestehen. Für die Installation von AD RMS, sollte das entsprechende Benutzerkonto in den Administrationsgruppen Organisations-Admins und Domänen-Admins der Domäne und Gesamtstruktur Mitglied sein. Nach der Installation kann das Benutzerkonto für den AD RMS in einer produktiven Umgebung aus der Gruppe der Organisations-Admins entfernt werden.

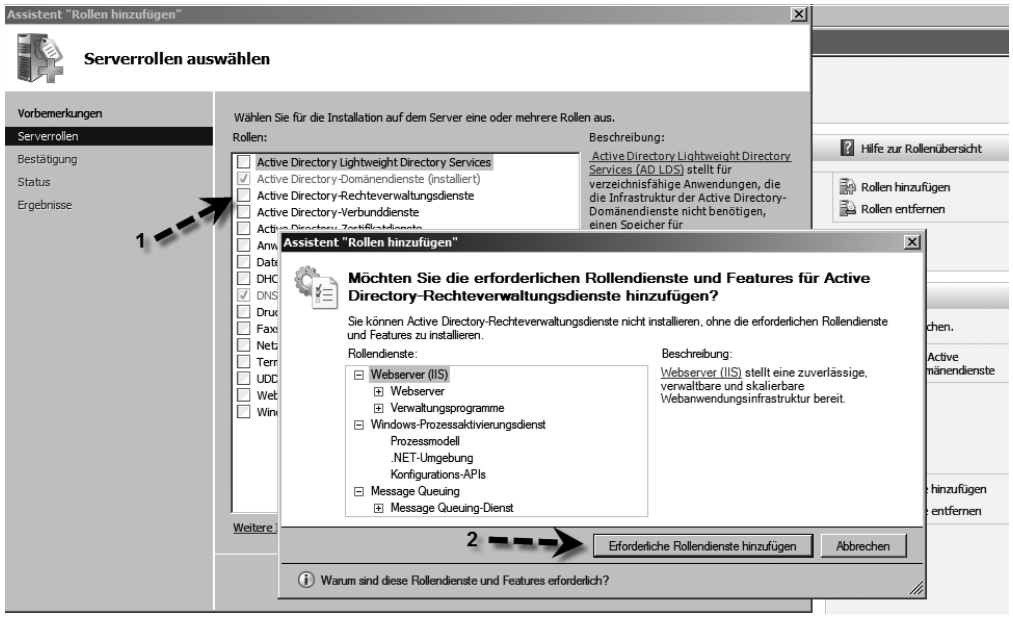
Abbildg. 17.34 Installieren der notwendigen Features für die Active Directory-Rechteverwaltung



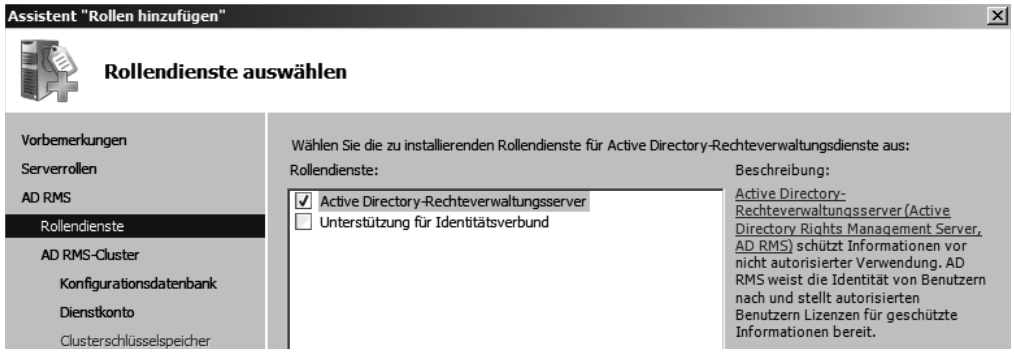
Installieren Sie die notwendigen Features sowie die abhängigen Features auf dem Server, bevor Sie die Rolle der Active Directory-Rechteverwaltung installieren. Nachdem diese Voraussetzungen getroffen wurden, wird über den Server-Manager die Installation der Rolle *Active Directory-Rechteverwaltungsdienste* gestartet (Abbildung 17.35). Fehlen bei der Installation noch Voraussetzungen, werden diese vom Assistenten automatisch zur Installation vorgeschlagen und mit den AD RMS installiert.

Wählen Sie auf der zweiten Seite des Assistenten die Installation *Active Directory-Rechteverwaltungsserver* aus. Durch die Installation der *Unterstützung für Identitätsverbund* kann AD RMS mit den Active Directory-Verbunddiensten zusammenarbeiten. So kann eine AD RMS-Infrastruktur über mehrere Gesamtstrukturen verteilt werden, die durch die Active Directory-Verbunddienste verbunden werden.

Abbildg. 17.35 Installieren der Serverrolle *Active Directory-Rechteverwaltungsdienste* und der erforderlichen Rollendienste



Abbildg. 17.36 Auswählen des Rollendienstes eines Active Directory-Rechteverwaltungsservers

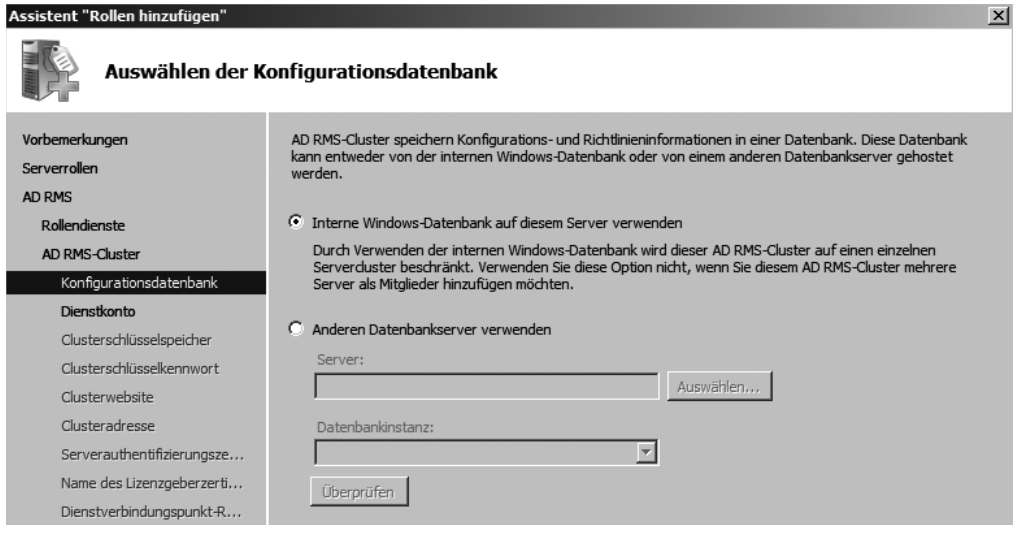


Auf der nächsten Seite des Assistenten lassen Sie einen neuen AD RMS-Cluster erstellen. Installieren Sie in der Domäne einen weiteren Server für AD RMS, kann dieser dem bestehenden Cluster beitreten.

Abbildg. 17.37 Erstellen eines neuen AD RMS-Clusters

Auf der nächsten Seite kann ausgewählt werden, ob die Daten des AD RMS-Servers in einer SQL Server-Datenbank gespeichert werden, oder in der internen Windows-Datenbank von Windows Server 2008. In einer Testumgebung kann durchaus auch die interne Windows-Datenbank verwendet werden. Allerdings können dann andere AD RMS-Server diesem Cluster nicht beitreten. Soll in der Testumgebung auch der Einsatz mehrerer AD RMS-Server in einem Cluster simuliert werden, muss vor der Fertigstellung der Rolleninstallation ein Server mit SQL Server zur Verfügung gestellt werden.

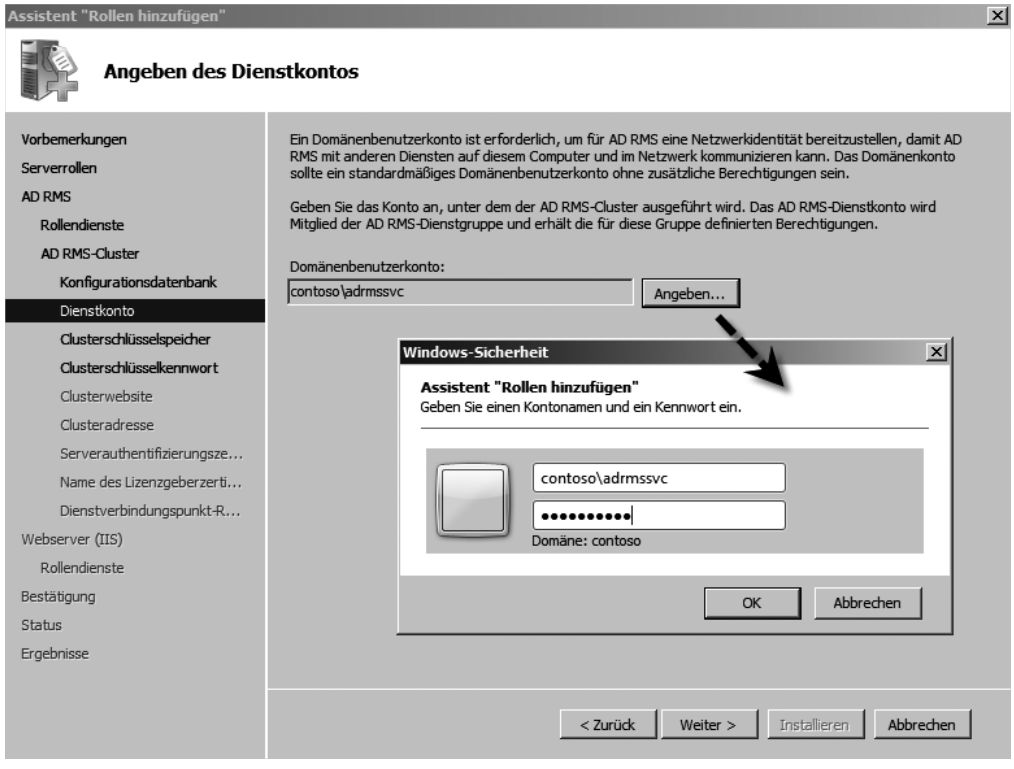
Abbildg. 17.38 Festlegen der Datenbank für den AD RMS-Dienst



Auf der nächsten Seite muss ein Dienstkonto für den AD RMS-Dienst angegeben werden. Dieses Konto darf nicht das gleiche sein, mit dem die Serverrolle installiert wird. Hierbei muss es sich um ein zusätzliches Benutzerkonto handeln. Das Konto muss in der Domäne keine besonderen Rechte

haben, aber lokaler Admin auf dem AD RMS-Server sein. Werden die Active Directory-Rechteverwaltungsdienste auf einem Domänencontroller installiert, erhält dieses Dienstkonto administrative Rechte in der Domäne. Darauf sollte bei der Planung geachtet werden. Wurde das Konto noch nicht angelegt, kann im Hintergrund zur Serverrollen-Installation die Verwaltungskonsole *Active Directory-Benutzer und -Computer* gestartet, der Benutzer angelegt und in die Gruppe der Administratoren aufgenommen werden. Diese Konsole starten Sie am schnellsten über *Start/Ausführen/dsa.msc*. Der Befehl kann natürlich auch in das Suchfeld des Startmenüs eingegeben werden.

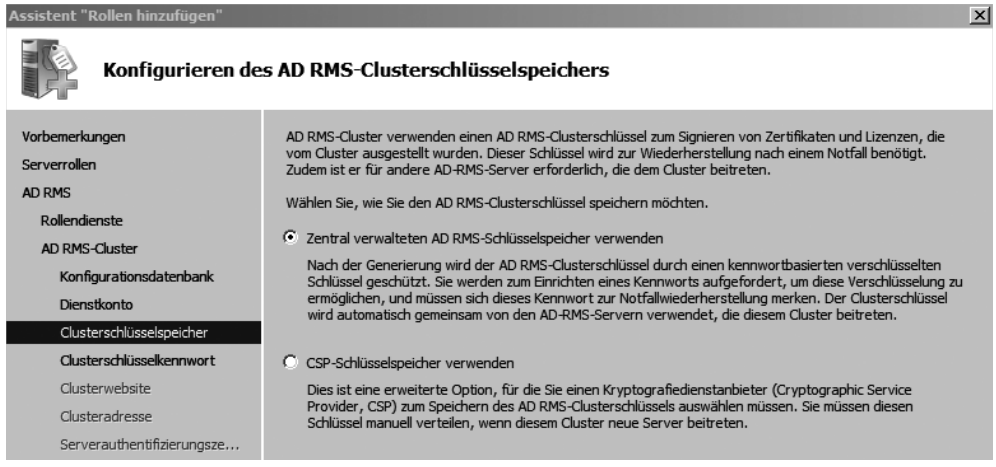
Abbildg. 17.39 Angeben des Dienstkontos für die Installation der Active Directory-Rechteverwaltungsdienste



Auf der nächsten Seite wird der AD RMS-Clusterschlüsselspeicher festgelegt. In diesem Speicher werden die Schlüssel abgelegt, mit denen Zertifikate und Lizenzen verschlüsselt werden. Der Schlüssel wird auch von anderen AD RMS-Servern benötigt, die diesem Cluster beitreten wollen. Hier kann normalerweise die Standardeinstellung *Zentral verwalteten AD RMS-Schlüsselspeicher verwenden* aktiviert werden.

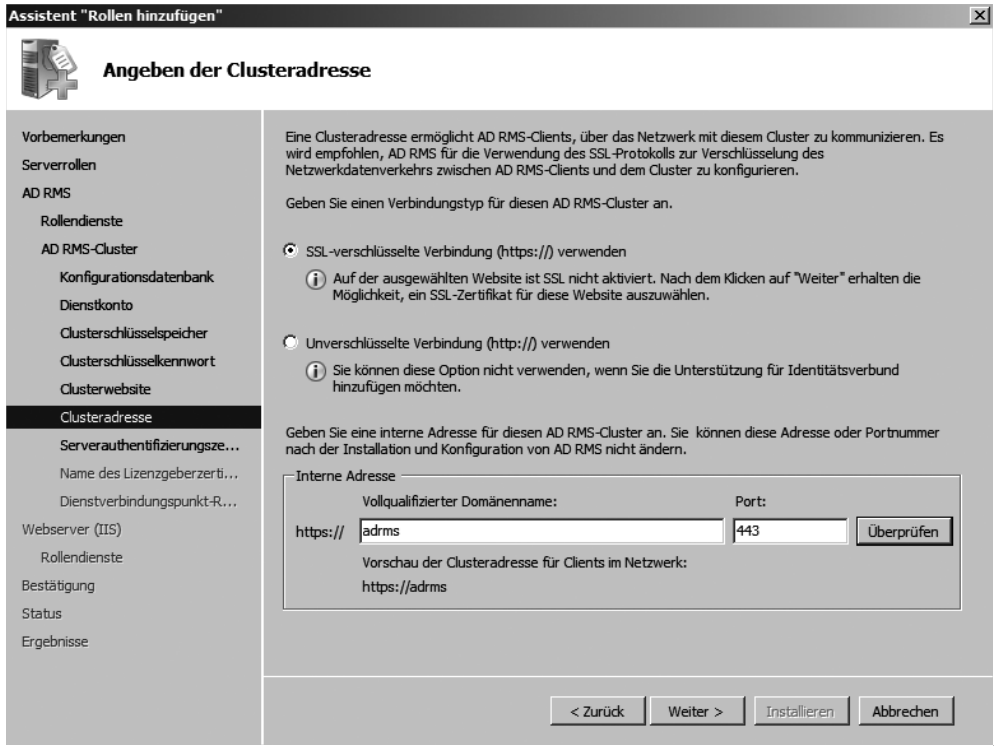
Auf der nächsten Seite wird das Kennwort für den Clusterschlüsselspeicher angegeben. Hierbei sollte es sich um ein sehr sicheres und langes Kennwort handeln, da mit diesem sehr sensible Daten entschlüsselt werden können.

Abbildg. 17.40 Konfigurieren des AD RMS-Clusterschlüsselspeichers



Auf der nächsten Seite wird festgelegt, unterhalb welcher Webseite die Clusterwebseite für den AD RMS-Server erstellt werden soll. Standardmäßig wird die *Default Web Site* vorgeschlagen. Diese kann problemlos ausgewählt werden.

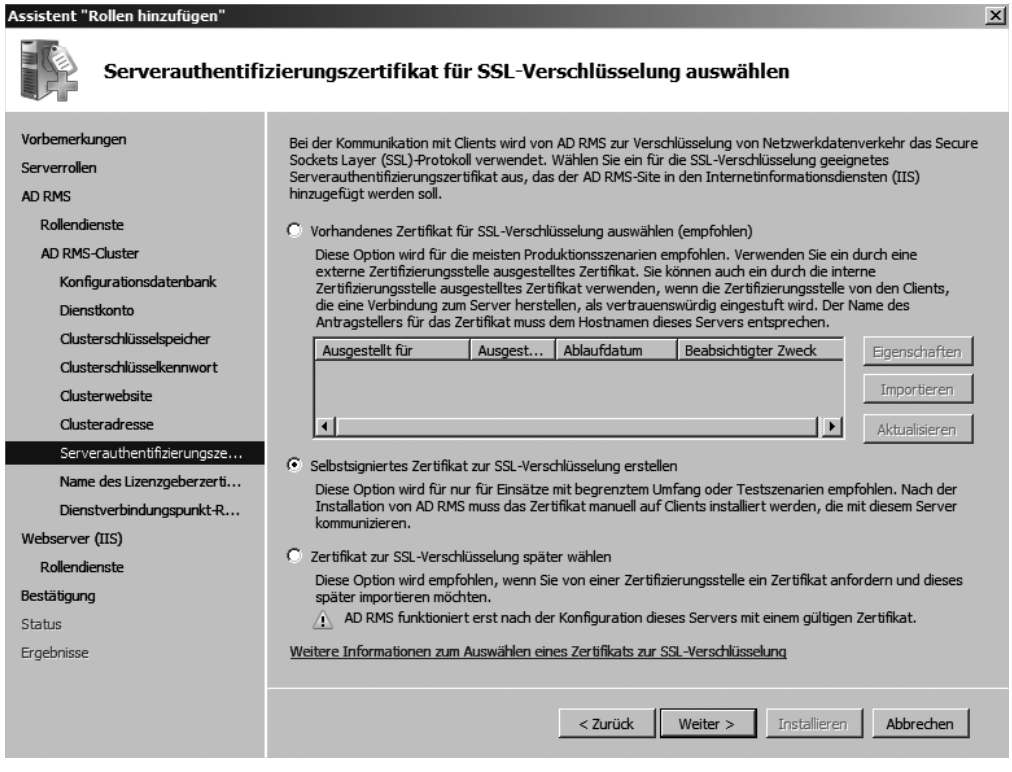
Abbildg. 17.41 Konfigurieren der Clusteradresse und URL zur Verbindung der Clients



Als Nächstes wird festgelegt, über welche Clusteradresse die Clients mit dem AD RMS-Cluster kommunizieren sollen. Hier sollte auf jeden Fall die SSL-Verschlüsselung verwendet werden, die vom Assistenten auch vorgeschlagen wird. Im unteren Bereich geben Sie die interne Adresse des Clusters ein. Am besten legen Sie vorher, oder auch parallel dazu, einen Alias-DNS-Eintrag in der Active Directory-Domäne fest, der zu diesem Cluster zeigt. Natürlich kann hier auch der interne Name des Servers an sich verwendet werden. Allerdings gibt es dann Schwierigkeiten, wenn einem Cluster mehrere Server beitreten wollen. Den Alias können Sie an dieser Stelle auch im Hintergrund anlegen. Starten Sie dazu über *Start/Ausführen/dnsmgmt.msc* die DNS-Verwaltung und legen den neuen Alias an. Zeigen Sie auf den Eintrag des aktuell zu installierenden Servers.

Auf der nächsten Seite des Assistenten wird das Zertifikat für die SSL-Verbindung ausgewählt. Entweder installieren Sie zuvor die Active Directory-Zertifikatdienste und stellen dem Server ein Zertifikat aus, oder wählen die Option *Selbstsigniertes Zertifikat zur SSL-Verschlüsselung erstellen*. Diese Option reicht für eine Testumgebung aus, aber nicht für eine produktive Umgebung. Bei selbstsignierten Zertifikaten erhalten die Clients immer eine Fehlermeldung.

Abbildg. 17.42 Auswählen des Serverzertifikats für die Active Directory-Rechteverwaltungsdienste

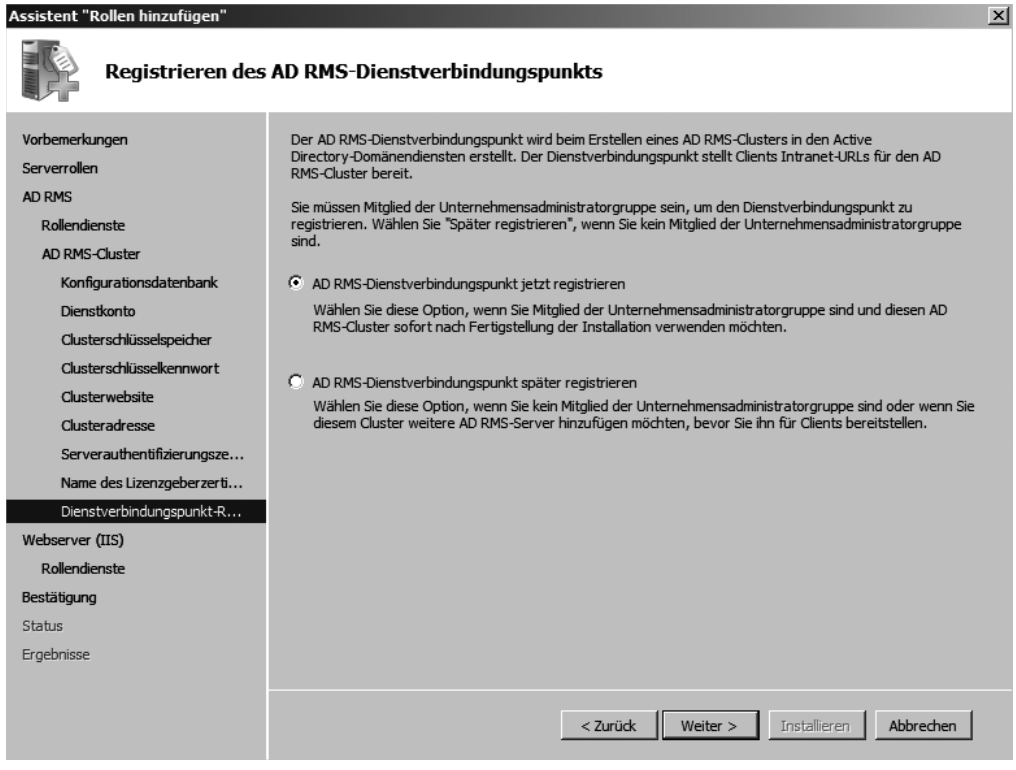


Auf der nächsten Seite geben Sie den Namen des Servers ein, der bei der Selbstsignierung verwendet wird. Verwenden Sie als Zugriff auf den Server einen DNS-Alias, tragen Sie diesen im Feld ein. Verwenden Sie den tatsächlichen Namen des Servers, dann tragen Sie diesen ein.

Auf der nächsten Seite des Assistenten wird festgelegt, ob sich der AD RMS-Server in Active Directory registrieren oder diese Registrierung später manuell durchgeführt werden soll. Hier wird die

Option *AD RMS-Dienstverbindungspunkt jetzt registrieren* aktiviert. So ist sichergestellt, dass nach der Installation der Server sofort funktionsfähig ist. Schließen Sie die Installation ab, damit der Assistent beginnt, den Rollendienst auf dem Server zu integrieren. Die Installation kann über eine Stunde dauern, abhängig von der Geschwindigkeit Ihres Servers. Nach Fertigstellung wird der Server neu gestartet.

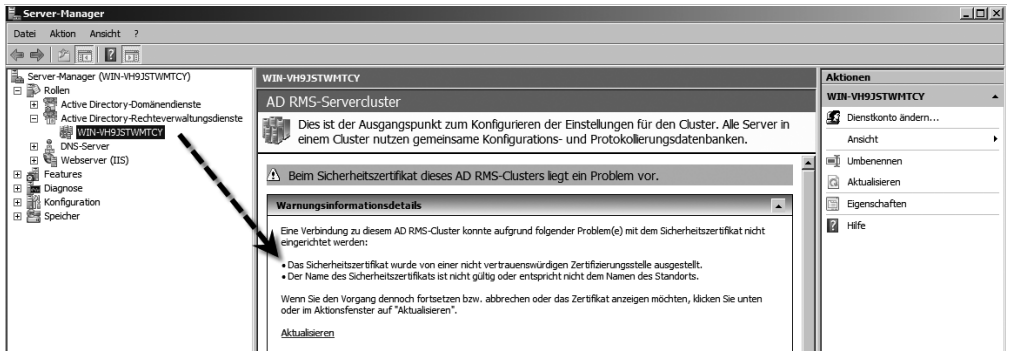
Abbildg. 17.43 Automatisches Registrieren des AD RMS-Dienstverbindungspunktes



Konfigurieren der Active Directory-Rechteverwaltung nach der Installation

Sobald die Installation abgeschlossen ist, und der Server neu gestartet wurde, werden noch einige Konfigurationsarbeiten durchgeführt. Wird zum Beispiel ein selbstsigniertes Zertifikat verwendet, muss dieses in einer Testumgebung noch in den Speicher für die vertrauenswürdigen Stammzertifizierungsstellen integriert werden. Diese Vorgehensweise ist aber nur innerhalb einer Testumgebung empfehlenswert. In einer produktiven Umgebung sollte entweder ein Zertifikat gekauft oder eine interne Zertifizierungsstelle erstellt werden. Wird das Zertifikat nicht in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen übernommen, ist der Server inaktiv und meldet dies als Fehler. Sie finden die Verwaltungskonsole der Active Directory-Rechteverwaltung am schnellsten über den Server-Manager (Abbildung 17.44).

Abbildg. 17.44 Die Verwaltungskonsole der Active Directory-Rechteverwaltung meldet einen Fehler, wenn das Zertifikat nicht vertrauenswürdig ist



Um das selbstsignierte Zertifikat in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen aufzunehmen, gehen Sie folgendermaßen vor:

1. Geben Sie *mmc* im Suchfeld des Startmenüs ein.
2. Fügen Sie das Snap-In *Zertifikate* hinzu.
3. Wählen Sie das lokale *Computerkonto* als Zertifikatspeicher aus.
4. Erweitern Sie den Knoten *Zertifikate (Lokaler Computer)*.
5. Erweitern Sie die beiden Knoten *Eigene Zertifikate* und *Vertrauenswürdige Stammzertifizierungsstellen*.
6. Klicken Sie bei *Eigene Zertifikate* auf *Zertifikate*.
7. Ziehen Sie das AD RMS-Zertifikat auf den Eintrag *Zertifikate* unter *Vertrauenswürdige Stammzertifizierungsstellen*.

Exportieren des Zertifikats für den Client

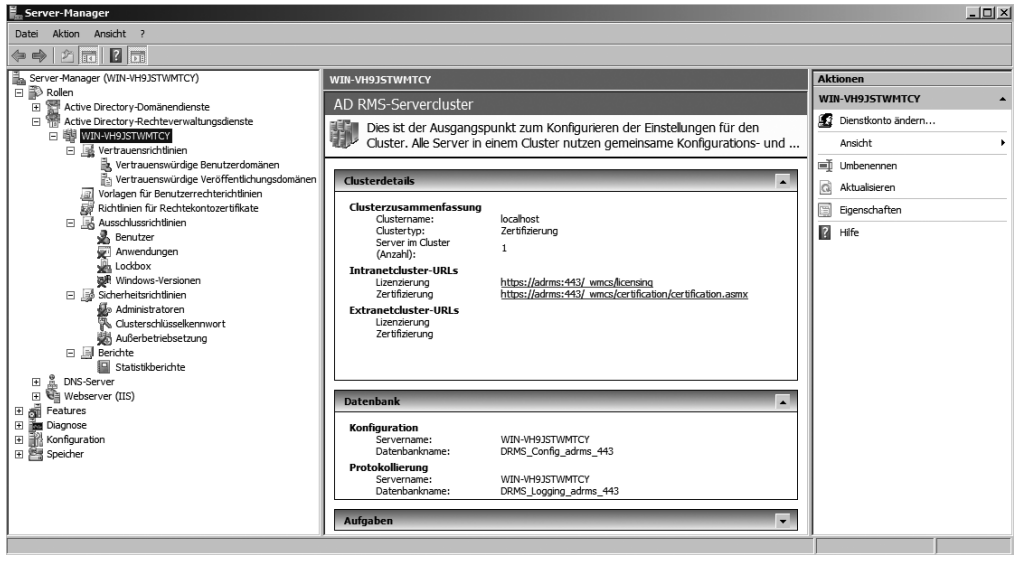
Auch auf dem Client wird dieses Zertifikat später benötigt. Aus diesem Grund bietet es sich an, dieses gleich an dieser Stelle zu exportieren. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie das Zertifikat mit der rechten Maustaste an und wählen Sie *Alle Aufgaben/Exportieren*.
2. Wählen Sie beim Exportieren die Option *Nein, privaten Schlüssel nicht exportieren*.
3. Wählen Sie die Einstellung *DER-codiert-binär…*
4. Speichern Sie die Datei direkt auf einer Freigabe des Servers oder in einem anderen Speicherort. Später wird diese Datei auf dem Client benötigt.
5. Schließen Sie den Export ab.

Testen der Installation der Active Directory-Rechteverwaltungsdienste

Unter Umständen erscheint noch eine Meldung, die besagt, dass der Name des Zertifikats und der AD RMS nicht übereinstimmt. Dies passiert, wenn Sie den Alias des Zertifikats nicht so benannt haben, wie den Alias der Webseite. Klicken Sie in diesem Fall einfach auf *Aktualisieren* und bestätigen Sie die Zertifikatemeldung. Anschließend wird die Verwaltungskonsole der Active Directory-Rechteverwaltung angezeigt (Abbildung 17.45).

Abbildg. 17.45 Anzeigen der Verwaltungskonsole für die Active Directory-Rechteverwaltung im Server-Manager



Vorbereiten des Windows Vista-Clients

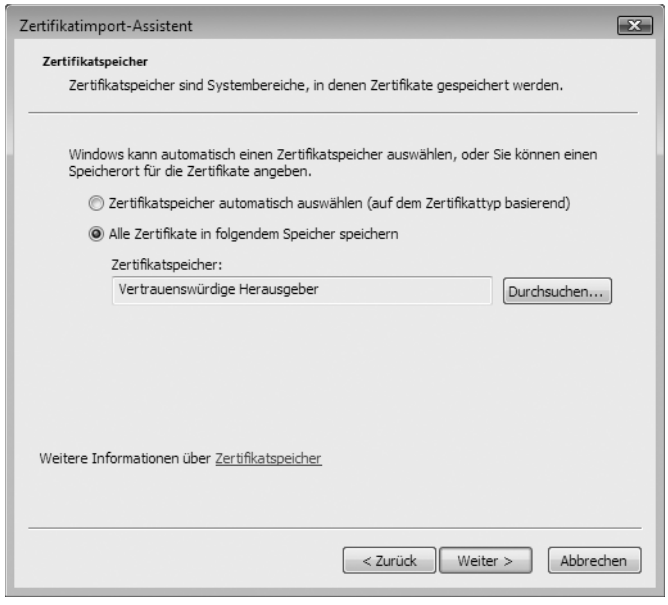
Nachdem der Server vorbereitet wurde, wird als Nächstes der Client konfiguriert. Am besten verwenden Sie einen Client mit Windows Vista SP1 und Office 2007 SP1, den Sie als Mitglied in die Domäne aufnehmen.

Exportiertes Zertifikat importieren

Der erste Schritt, den Client vorzubereiten, besteht darin, das auf dem AD RMS-Server exportierte Zertifikat in den Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* zu importieren:

1. Geben Sie *mmc* im Suchfeld des Startmenüs ein.
2. Fügen Sie das Snap-In *Zertifikate* hinzu.
3. Wählen Sie das lokale *Computerkonto* als Zertifikatespeicher aus.
4. Erweitern Sie den Knoten *Zertifikate (Lokaler Computer)*.
5. Erweitern Sie den Knoten *Vertrauenswürdige Stammzertifizierungsstellen.*
6. Klicken Sie mit der rechten Maustaste auf den Eintrag *Zertifikate* und wählen Sie *Alle Aufgaben/Importieren*.
7. Wählen Sie die Zertifikatedatei aus und schließen Sie den Import ab.

Abbildg. 17.46 Importieren des Zertifikats auf dem Client-PCs

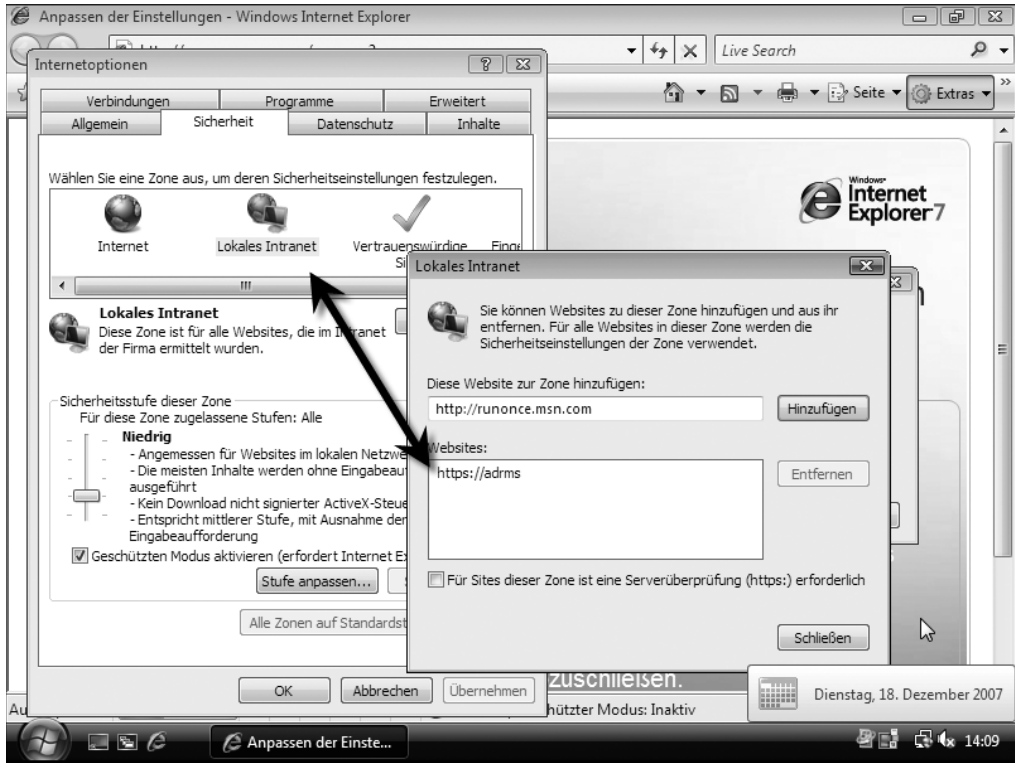


Clusteradresse zur lokalen Intranet-Sicherheitszone hinzufügen

Im nächsten Schritt muss die Adresse mit der Sie über den Internet Explorer auf den AD RMS-Cluster zugreifen in die Sicherheitszone *Lokales Intranet* aufgenommen werden. Gehen Sie dazu auf dem Windows Vista-Client folgendermaßen vor:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf *Extras/Internetoptionen*.
3. Holen Sie die Registerkarte *Sicherheit* in den Vordergrund.
4. Klicken Sie auf *Lokales Intranet* und dann auf *Sites*.
5. Klicken Sie auf *Erweitert*.
6. Geben Sie die URL der AD RMS-Adresse so an, wie Sie es bei der Installation von AD RMS eingegeben haben, und klicken Sie auf *Hinzufügen*.
7. Schließen Sie das Fenster.

Abbildg. 17.47 Hinzufügen der AD RMS-Seite zu den lokalen Intranetseiten



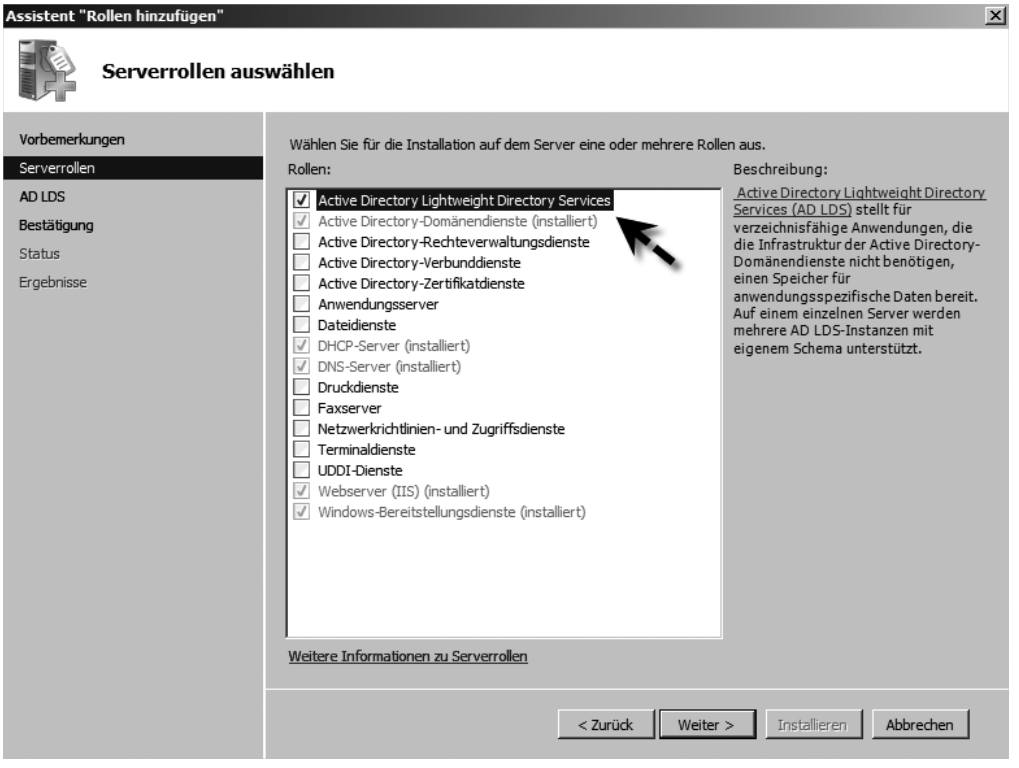
Test mit Word 2007 und AD RMS

Um AD RMS zu testen, öffnen Sie ein Word-Dokument. Über die *Office*-Schaltfläche erreichen Sie das Menü von Office. Wählen Sie über das Menü *Vorbereiten* den Menüpunkt aus, um Berechtigungen zu erteilen. Anschließend geben Sie in einem Feld Ihrer Wahl den UNC-Namen der Gruppe an, die das Recht erhalten soll, das Dokument entsprechend zu lesen oder zu bearbeiten. Ein Beispiel dafür wäre *einkauf@contoso.com*. Speichern Sie das Dokument entsprechend auf dem AD RMS-Server ab. Melden Sie sich am Testclient mit einem Benutzerkonto an, das in der Gruppe enthalten ist, die Sie für das Dokument berechtigt haben. Der Anwender sollte jetzt eine Meldung erhalten, dass der Zugriff eingeschränkt ist, wenn er das Dokument in der Freigabe auf dem AD RMS-Server öffnet. Am besten verwenden Sie hier auch wieder die *Office*-Schaltfläche. Auf diesem Weg können Sie noch über verschiedene andere Berechtigungen ein Gefühl für die Technik entwickeln. Weitere Informationen erhalten Sie in der Hilfe der Active Directory-Rechteverwaltungskonsole. Die Möglichkeiten des Dienstes sind sehr vielfältig, sodass sich alleine damit ein ganzes Buch füllen ließe.

Active Directory Lightweight Directory Services

Die Active Directory-Lightweight-Verzeichnisdienste (Active Directory Lightweight Directory Services, AD LDS) sind die Nachfolger von Active Directory Application Mode (ADAM). Vereinfacht ausgedrückt, können mit diesen Diensten Applikationen, welche Informationen in einem Verzeichnis speichern, arbeiten, um Informationen in einer eigenen Verzeichnisinstanz zu speichern.

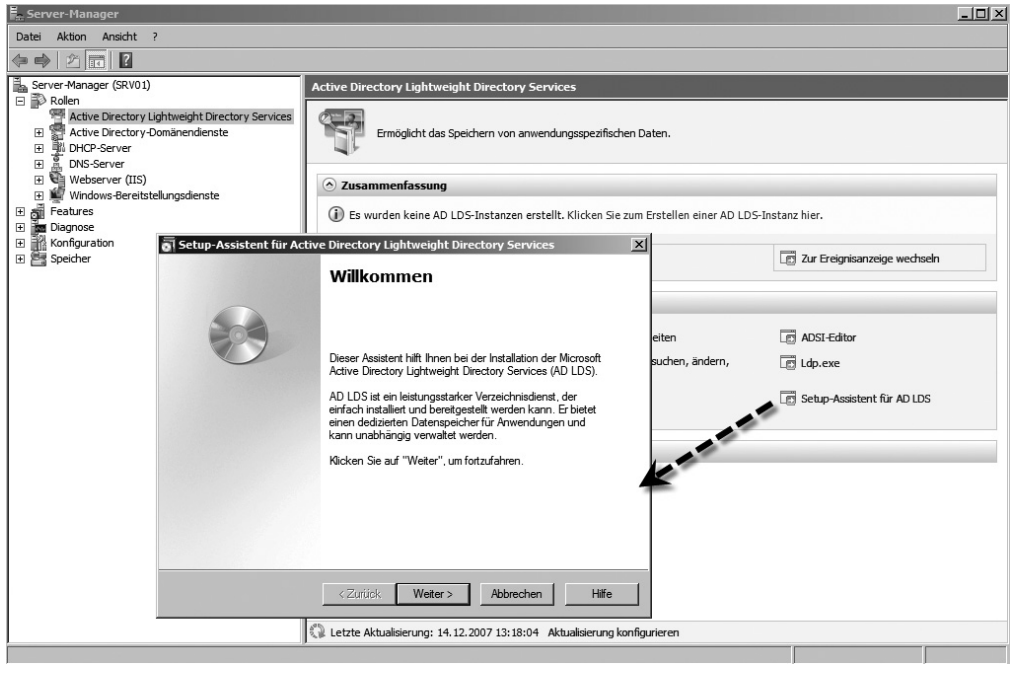
Abbildg. 17.48 Installieren der Active Directory Lightweight Directory Services



Diese Dienste benötigen keinen reinen Domänencontroller und kein Active Directory, sondern können vollkommen unabhängig betrieben werden. Auf einem Server können mehrere Instanzen von AD LDS parallel laufen. Bei den AD LDS handelt es sich sozusagen um ein kleines Active Directory. Mit AD LDS können unter anderem spezielle Anforderungen von Applikationen an einen Verzeichnisdienst abgebildet werden. Einer Applikation kann zum Beispiel ein eigenes Verzeichnis mit eigenem Schema zur Verfügung gestellt werden, ohne andere Anwendungen oder die Anmeldungen im Unternehmen zu beeinträchtigen. Die Verwaltung eines Extranets und die damit verbundene Identitätsverwaltung, können ebenfalls mit AD LDS verbessert werden. Sollen X.500/LDAP-Verzeichnisdienste migriert werden, bietet AD LDS eine optimale Schnittstelle zum Verzeichnis des Unternehmens. Auch zur Identitätsverwaltung in kleineren Niederlassungen oder in DMZs können die AD LDS wertvolle Dienste leisten. Die AD LDS verfügen dazu, genauso wie ein normales Active Direc-

tory, über eine eigene Benutzerverwaltung. Mit AD LDS können aber auch lokale Benutzerkonten und Gruppen, genauso verwendet werden, wie Benutzer und Gruppen aus dem Active Directory. Dazu wird die Authentifizierung mit diesen Objekten automatisch entweder zur lokalen Maschine oder einem Active Directory-Domänencontroller umgeleitet und anschließend der Zugriff auf die Daten innerhalb der AD LDS gestattet. Zur Verwaltung von AD LDS stellt Microsoft einige Tools zur Verfügung, die speziell für diese Serverrolle verwendet werden können. Nach der Installation der Rolle können die AD LDS über einen Assistenten im Server-Manager eingerichtet werden.

Abbildg. 17.49 Einrichten der AD LDS über einen Assistenten



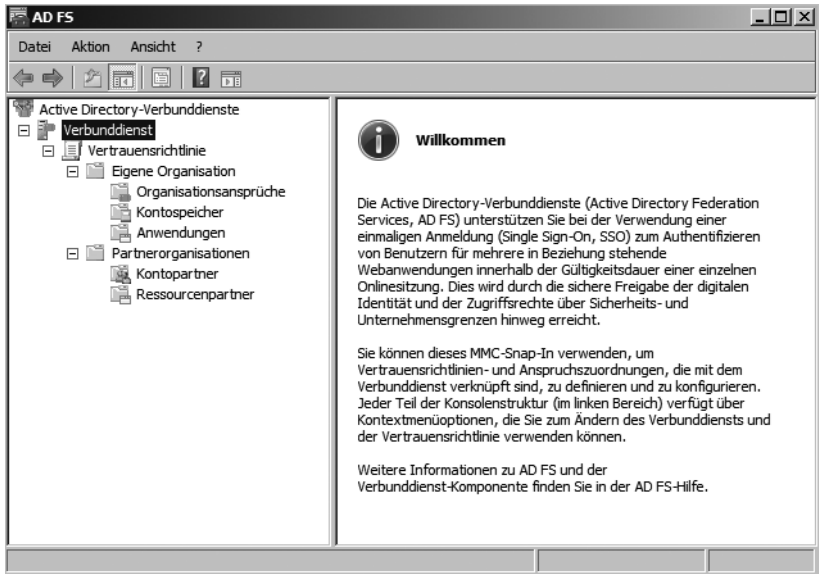
Mit dem *ADSchemaAnalyzer* kann das Schema einer Active Directory-Gesamtstruktur in eine AD LDS-Instanz übernommen werden. Auch die Migration des Schemas zwischen verschiedenen AD LDS-Instanzen oder anderen LDAP-kompatiblen Verzeichnisdiensten zu einer AD LDS-Instanz ist möglich. Mit dem *Active Directory to AD LDS Synchronizer* können Daten aus einem Active Directory in eine AD LDS-Instanz importiert werden, was für Testumgebungen oder der Verteilung von Anwendung sehr hilfreich sein kann. Der Snapshot Browser ermöglicht eine lesende Ansicht einer AD LDS-Datenbank, die zuvor über einen Volumenschattenkopiendienst (VSS)-Snapshot mit dem Tool *ntdsutil.exe* erstellt wurde.

Mit dem Snap-In *Active Directory-Standorte und -Dienste* kann die Replikation von AD LDS-Instanzen auch über mehrere Standorte verwaltet werden. Ebenfalls möglich ist die Installation einer Instanz über ein Datensicherungsmedium, ähnlich wie bei der Installation von Active Directory. Zwischen AD LDS-Instanzen können Daten über so genannte *Configuration Sets* repliziert werden, welches eine Gruppe von verschiedenen AD LDS-Instanzen zusammenfasst. Die Replikation zwischen den Instanzen ist vollkommen unabhängig von der Replikation im Active Directory.

Active Directory-Verbunddienste

Die Hauptaufgabe der AD FS (Active Directory Federation Services) besteht darin, Anwendern mit einer einzelnen Anmeldung während einer Online-Sitzung, Zugriff auf mehrere Web-Applikationen zu bieten (Single Sign-On, SSO). Die Installation erfolgt ebenfalls als Rollendienst.

Abbildg. 17.50 Die Active Directory-Verbunddienste, werden über ein eigenes Snap-In verwaltet



So kann zum Beispiel Anwendern im internen Netzwerk der Zugriff auf webbasierte Anwendungen in der DMZ gestattet werden. Dabei ist es unerheblich, ob der Zugriff von intern oder über das Internet durchgeführt wird. Die Authentifizierung findet dabei an der Gesamtstruktur statt, bevor der Zugriff genehmigt wird. Auch die Verbindung von zwei Gesamtstrukturen über einen solchen *Federation Trust* ist möglich. In diesem Fall können Anwender der einen Gesamtstruktur auf webbasierte Anwendungen in der anderen Gesamtstruktur zugreifen, was vor allem beim Zugriff über das Internet eine enorme Erleichterung sein kann. So können auf einem Federation Server die Gesamtstrukturen und Konten hinterlegt sein, die Zugriff auf ein Extranet haben sollen. Greift ein Anwender zu, kann der Federation Server den Zugriff genehmigen. Einmal authentifiziert darf der Anwender auf alle webbasierten Anwendungen zugreifen, für die er berechtigt wurde, ohne sich erneut authentifizieren zu müssen. Aber auch die Authentifizierung von externen Anwendern ohne Konto in einem Active Directory ist möglich, um eine Single Sign-On-Infrastruktur aufzubauen.

Zusammenfassung

Wir haben Ihnen in diesem Kapitel die grundlegenden Informationen zu den Zertifkatsdiensten sowie weiteren Active Directory-Diensten gezeigt. Mit den Zertifikatdiensten können zum Beispiel sichere Terminaldienste-Webzugriffserver, Webseiten mit IIS 7.0, aber auch Zertifikate für Outlook Web Access von Exchange Server 2003/2007 ausgestellt werden. Lesen Sie sich zusätzlich auch die Informationen in Kapitel 15 durch. Im nächsten Kapitel vertiefen wir die Möglichkeiten der Systemüberwachung und der Diagnosemöglichkeiten von Windows Server 2008. Auch hier hat Microsoft zahlreiche Verbesserungen in seine neue Server-Version integriert.

Kapitel 18

Systemüberwachung und Fehlerbehebung

In diesem Kapitel:

In diesem Kapitel werden die Funktionen von Windows Server 2008 erläutert, mit denen Sie das System überwachen und Fehler erkennen sowie beheben können. Darüber hinaus gehen wir in diesem Kapitel auf die Aufgabenplanung ein, über die Sie die verschiedenen Aufgaben der Systemüberwachung durchführen können, wenn diese automatisiert vorgenommen werden sollen. So können zum Beispiel direkt aus der Ereignisanzeige Aktionen an die Aufgabenplanung übergeben werden. Auch für die Systemüberwachung und Verwaltung von Windows Server 2008 bietet sich der Server-Manager als zentrale Schaltstelle an. Vor allem im Bereich der Systemüberwachung hat Microsoft einiges in Windows Server 2008 integriert.

Ereignisanzeige – Fehlerbehebung in Windows Server 2008

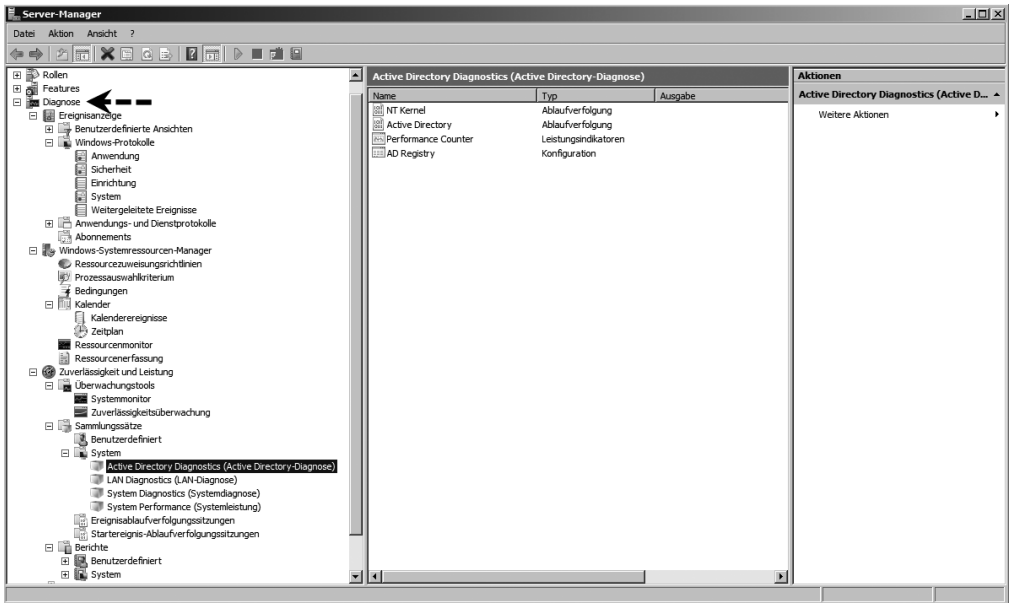
Alle Fehler und Aktionen von Windows werden in den Ereignisanzeigen festgehalten und stehen Administratoren zur Verfügung, um Fehler zu beheben oder den PC zu überwachen. Wie die Aufgabenplanung wurde von Microsoft auch die Ereignisanzeige komplett überarbeitet und stellt jetzt wesentlich mehr Informationen zur Verfügung. Windows Server 2008 verfügt über ein völlig neues Ereignisprotokollsystem. Das Gruppenrichtlinienmodul nutzt zum Beispiel ebenfalls das neue Windows Eventing 6.0-System und teilt Ereignisse in zwei besondere Protokolle auf. Das vertraute Systemprotokoll (das nun als ein administratives Protokoll bezeichnet wird) enthält die Probleme der Gruppenrichtlinie. Falls im Gruppenrichtlinienmodul ein Fehler auftritt, sollte er im Systemprotokoll erscheinen und als dessen Ursprung der Gruppenrichtliniendienst (nicht der *Userenv*-Prozess) angezeigt werden. Ein neues Protokoll für Anwendungen und Dienste wurde speziell für die Gruppenrichtlinien eingerichtet und speichert operative Ereignisse. Dieses Protokoll ersetzt im Wesentlichen die unhandliche Problembehandlungsdatei *userenv.log*, da jeder Schritt des Gruppenrichtlinienmoduls hier aufgeführt wird und leicht nachvollzogen werden kann.

Mithilfe dieser Protokolle ist es möglich, den allgemeinen Systemzustand zu überwachen. Anhand des Ereignisprotokolls können Sie nach Ereignissen suchen, die auf Probleme hinweisen. Darüber hinaus dienen diese Informationen zur Diagnose von Problemen. Sie können nach Programm- und Systemaktionen suchen, die zu einem Problem führen, und Details herausfinden, die Ihnen bei der Ermittlung der Grundursache behilflich sind. Zugleich lassen sich anhand dieser Informationen auch Leistungsprobleme beurteilen und beheben. Die neue Ereignisanzeige wurde vollständig umgeschrieben. Da sie in Microsoft Management Console (MMC) 3.0 integriert ist, hat sich ihr Erscheinungsbild ebenfalls geändert. Es gibt immer noch eine hierarchische Struktur und eine Ereignisliste. Unter dem Knoten *Windows-Protokolle* ist auch weiterhin der Zugriff auf die vertrauten Anwendungs-, System- und Sicherheitsprotokolle möglich (Abbildung 18.1).

Mit der Ereignisanzeige Fehler suchen

Die Ereignisanzeige wird unterhalb des Knotens *Diagnose* im Server-Manager angezeigt. Sie können diese auch über *Start/Ausführen/eventvwr.msc* starten.

Abbildg. 18.1 Die neuen Ereignisanzeigen in Windows Server 2008

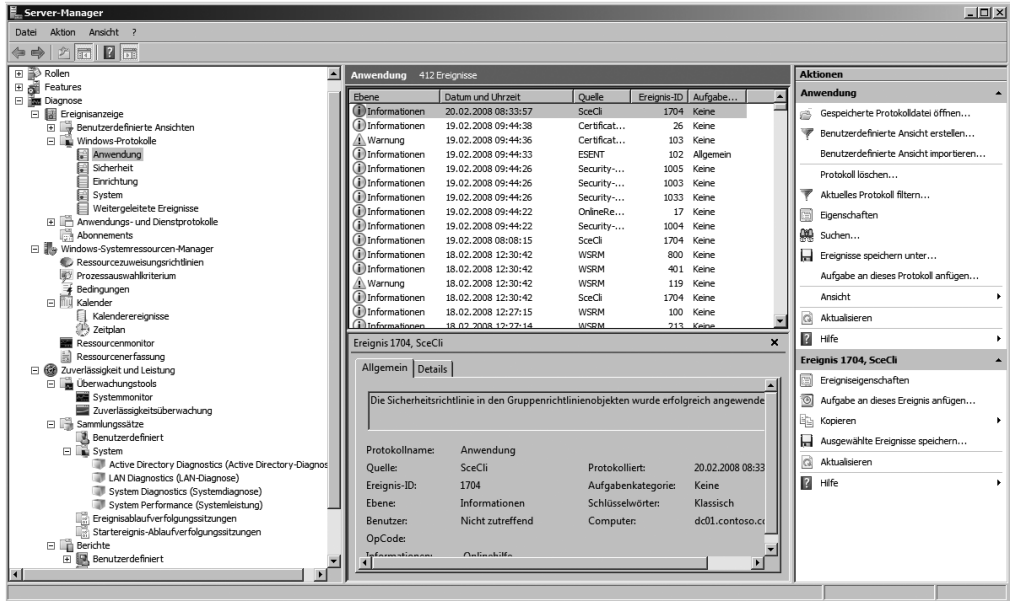


Zusätzlich wurden dem Stamm einige neue Knoten hinzugefügt. Unter dem Knoten *Windows-Protokolle* befindet sich jetzt das neue Protokoll *Weitergeleitete Ereignisse*. Auch das Protokoll *Einrichtung* ist neu. In diesem Protokoll werden Ereignisse während der Installation von Windows Server 2008- und Windows Vista-kompatiblen Applikationen gespeichert. Unterhalb des Knotens *Anwendungs- und Dienstprotokolle/Microsoft/Windows* findet sich für jeden Systemdienst ein eigenes Protokoll. Das auffälligste neue Feature ist der Vorschaubereich unterhalb der Ereignisliste. Er umfasst die Eigenschaften des aktuell ausgewählten Ereignisses. Das heißt, Sie müssen nicht mehr auf ein Ereignis doppelklicken, um dessen Eigenschaften anzuzeigen, und auch nicht mehr mit Fenstern jonglieren (Abbildung 18.2). Neben der Ereignisanzeige werden über den Knoten *Diagnose* weitere Hilfsmittel zur Verfügung gestellt, zum Beispiel eine Analyse von Active Directory oder Berichte über den Systemzustand.

HINWEIS Der Speicherort der Standardprotokolle ist *%SystemRoot%\System32\winevt\Logs*. Die Protokolldateien erhalten die Endung **.evtx*, da diese jetzt XML-basiert sind.

Unter dem Knoten *Benutzerdefinierte Ansichten* werden administrative Ereignisse angezeigt. Hier finden sich alle Fehler und Warnungen aus den verschiedenen Protokolldateien, die für Administratoren von Interesse sind. Windows Server 2008 bietet die Möglichkeit, weniger interessante Ereignisse hinauszufiltern, sodass Sie sich auf die Ereignisse konzentrieren können, die Ihnen wichtig sind. Hierzu wird eine protokollübergreifende Abfragesprache verwendet, die vom Ereignisprotokolldienst unterstützt wird. Damit dies funktionieren kann, müssen alle Ereignisse einer klar definierten Struktur folgen.

Abbildg. 18.2 Überarbeitete Anzeige der Ereignisprotokolle



Der Ereignisvorschaubereich umfasst die Registerkarte *Details*. Bei Auswahl dieser Registerkarte wird die XML-Darstellung des Ereignisses angezeigt (Abbildung 18.3). Jede Ereignisprotokolldatei wird als eine Abfolge solcher strukturierten Ereigniselemente behandelt. Auf diese Weise wird eine logische und überschaubare Ansicht von Ereignisprotokoll- und Ereignisarchivdateien geboten. Die Daten werden intern in einem binären Format gespeichert. Im Bereich *System* der XML-Daten wird der Zeitpunkt angegeben, an dem das Ereignis eingetreten ist, sowie die Prozess-ID, die Thread-ID, der Computername und die Sicherheitskennung (Security Identifier, SID) des Benutzers. Ein Ereignis wird durch die Kombination seiner EventID (eine Zwei-Byte-Zahl) und seiner Version (eine Ein-Byte-Zahl) eindeutig definiert. Alle Ereignisse vom gleichen Ereignisanbieter, die dieselbe EventID und Version aufweisen, haben eine identische Struktur.

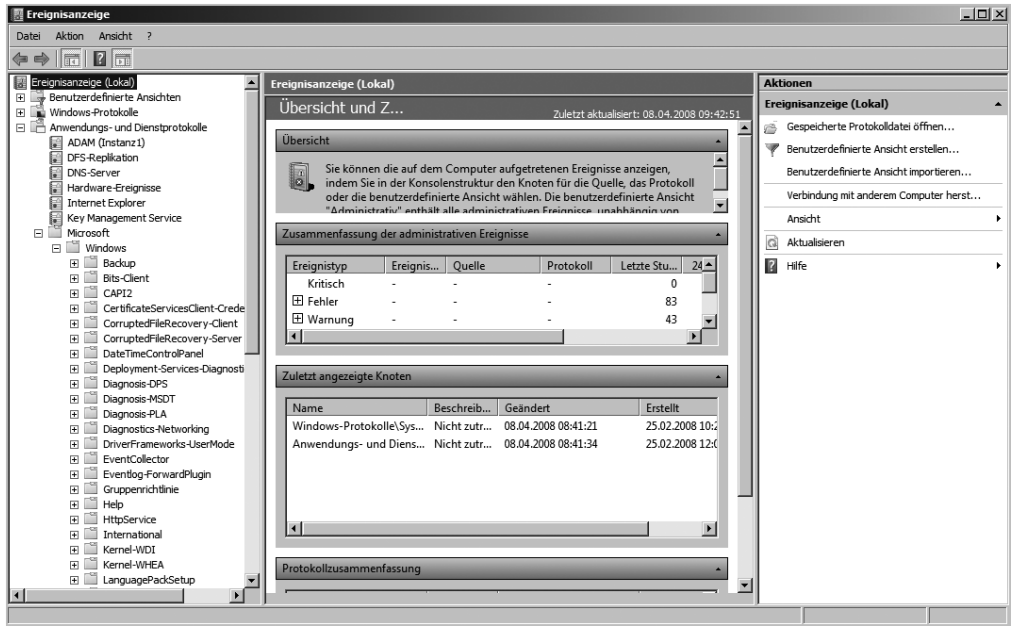
Der Wert *Level* gibt den Schweregrad bzw. den Ausführlichkeitsgrad eines Ereignisses an. Allgemein werden die vordefinierten Werte 1 (Kritisch), 2 (Fehler), 3 (Warnung), 4 (Information) und 5 (Ausführlich) verwendet, jedoch kann ein Anbieter seine eigenen Werte bis zu einem Höchstwert von 255 definieren. Je höher der Wert, desto ausführlicher das Ereignis. Mit der Eigenschaft *Task* wird in der Regel der allgemeine Funktionsbereich eines Ereignisses angegeben (z.B. Drucken, Netzwerk oder Benutzeroberfläche). Sie kann sich auch auf die Unterkomponente eines Programms beziehen. Diese Eigenschaften werden in hohem Maße von Sicherheitsüberwachungsereignissen eingesetzt. Jeder Ereignisherausgeber kann für diese Zwei-Byte-Zahl eine eigene Gruppe von Werten festlegen.

Abbildg. 18.3 XML-Ausgabe von Ereignissen

Mit dem Windows-Aufgabenplaner können Sie einer Abfrage eine Aufgabe anhängen. Jedes Mal, wenn ein Ereignis veröffentlicht wird, das der Abfrage entspricht, wird anschließend die entsprechende Aufgabe vom Aufgabenplaner gestartet. Abfragen können zum Archivieren ausgewählter Ereignisse eingesetzt werden. Vor allem in der Übersichtlichkeit der Anzeige hat Microsoft sehr viel beim Ereignisprotokoll geändert. Wenn Sie diese starten, erhalten Sie im mittleren Bereich des Fensters eine Zusammenfassung aller Einträge, deren detaillierte Informationen Sie anzeigen können, wenn Sie auf einzelne Meldungen doppelklicken. Es öffnet sich eine neue Ansicht der Ereignisanzeige, über die Ihnen die detaillierten Informationen einer bestimmten Meldung angezeigt werden (Abbildung 18.4).

Auf Basis dieser Fehlermeldung können Sie erkennen, welche Probleme Windows Server 2008 mit einzelnen Komponenten erkannt hat. Sie sollten durchaus regelmäßig die Ereignisanzeigen auf Fehler überprüfen, da Sie hier schnell Fehler erkennen können, bevor diese gravierendere Auswirkungen haben.

Abbildg. 18.4 Anzeigen der Zusammenfassung der Ereignisanzeigen



TIPP Haben Sie den Fehler genauer eingegrenzt und Fehlermeldungen in der Ereignisanzeige und der Diagnose festgestellt, suchen Sie auf der Internetseite *http://www.eventid.net* gezielt nach diesen Fehlern. Auf dieser Seite gibt es zu so gut wie jedem Eintrag der Ereignisanzeige Hinweise und mögliche Lösungsansätze. Geben Sie den Fehler in einer Suchmaschine oder speziellen Support-Seiten ein, wie zum Beispiel *http://www.experts-exchange.com*. Auch die Suche in der Microsoft Knowledge Base unter *http://support.microsoft.com* hilft oft weiter. Suchen Sie allerdings in der englischen Knowledge Base immer nur nach englischen Begriffen, da Sie hier mehr Antworten erhalten.

Neben der Zusammenfassung aller Ereignisanzeigen, können Sie auch die einzelnen Inhalte der Ereignisanzeigen anzeigen lassen, wenn Sie im linken Menü das Protokoll anklicken. Die Ansicht der Ereignisanzeige ändert sich und Sie sehen den kompletten Inhalt dieses Protokolls (Abbildung 18.5). Auch hier werden Ihnen alle Einträge angezeigt und unten im Fenster sehen Sie die detaillierten Informationen zum jeweiligen Eintrag. Sie können auch auf einzelne Einträge doppelklicken. In diesem Fall öffnet sich ein neues Fenster mit den Details zu dieser Meldung.

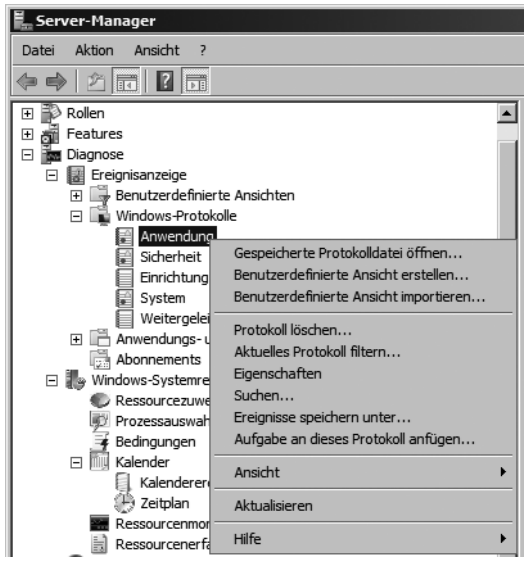
Abbildg. 18.5 Anzeigen von detaillierten Informationen in der Ereignisanzeige

Klicken Sie ein Protokoll mit der rechten Maustaste an, können Sie weitere Einstellungen vornehmen. Im Kontextmenü werden Ihnen zahlreiche Möglichkeiten angezeigt:

- **Gespeicherte Protokolldatei öffnen** Über diesen Menübefehl können Sie eine Protokolldatei öffnen, die Sie über die Option *Ereignisse speichern unter* abgespeichert haben. Dadurch können Sie Protokolle per E-Mail versenden und andere Benutzer können den Inhalt überprüfen.
- **Benutzerdefinierte Ansicht erstellen** Über diesen Menübefehl können Sie die Anzeige der Ereignisanzeigen anpassen und als benutzerdefinierten Filter ablegen. In diesem Fall werden Ihnen nur noch die Ereignisse in Ihrer gespeicherten Ansicht angezeigt.
- **Benutzerdefinierte Ansicht importieren** Mit dieser Optionen werden zuvor exportierte Ansichten auf einem Server wieder importiert und sind auf diese Weise schnell verfügbar.
- **Protokoll löschen** Wählen Sie diesen Menübefehl aus, wird nicht das Protokoll gelöscht, sondern der Inhalt des Protokolls. Sie erhalten zuvor noch eine Meldung, ob das Protokoll wirklich gelöscht werden soll und ob Sie das Protokoll vorher speichern wollen. Speichern Sie das Protokoll zuvor, entspricht das der Option *Ereignisse speichern unter*.
- **Aktuelles Protokoll filtern** Dieser Menübefehl wird verwendet, wenn Sie keine eigene Ansicht des Protokolls erstellen wollen, sondern nur die aktuelle Ansicht gefiltert werden soll. Dadurch können Sie zum Beispiel nach einem bestimmten Fehler suchen und überprüfen, wann dieser aufgetreten ist.
- **Eigenschaften** Über die Eigenschaften können Sie die Größe der einzelnen Protokolle festlegen bzw. bestimmen, wie sich Windows Server 2008 beim Erreichen der maximalen Ereignisprotokollgröße verhalten soll.

TIPP Überprüfen Sie in der Ereignisanzeige, ob Fehler gemeldet werden, die mit dem Problem in Zusammenhang stehen können, wenn Sie eine Fehlerbehebung durchführen. Überprüfen Sie auch, ob parallel zu diesem Fehler in anderen Protokollen der Ereignisanzeige Fehler auftreten, die zur gleichen Zeit gemeldet werden, also unter Umständen auf einen Zusammenhang schließen lassen. Überprüfen Sie, wann der Fehler in der Ereignisanzeige das erste Mal aufgetreten ist. Überlegen Sie genau, ob zu diesem Zeitpunkt irgendetwas verändert wurde, auch auf Basis der Ereignisprotokolle. Schauen Sie auch in anderen Protokollen der Ereignisanzeige nach, ob der Fehler mit anderen Ursachen zusammenhängt. Ein Fehler tritt selten ohne vorherige Änderung der Einstellung oder von defekter Hardware auf, sondern meist durch Änderungen am System oder der Installation von Applikationen und Tools. Durch die Filtermöglichkeiten der Ereignisanzeige in Windows Server 2008 können Fehler oft sehr genau eingegrenzt werden.

Abbildg. 18.6 Kontextmenü der einzelnen Protokolle in der Ereignisanzeige



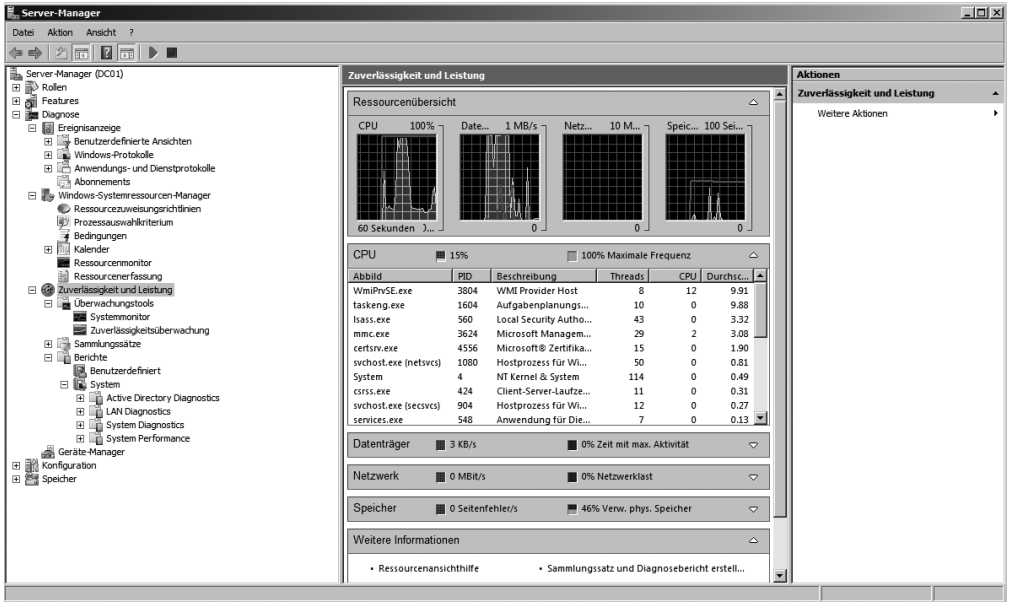
HINWEIS Neben der Ereignisanzeige, gibt es auch unter Windows Server 2008 noch verschiedene Protokolle auf Textbasis, zum Beispiel von IIS und Routing und RAS-Diensten. Die meisten Dateien tragen die Endung **.log*. Viele Logdateien befinden sich in den Verzeichnissen *%SystemRoot%\Debug*, *%SystemRoot%\System32\Config* und *%SystemRoot%\System32*. Die Logdateien von IIS finden Sie im *Inetpub*-Verzeichnis. Im *Debug*-Verzeichnis befinden sich zum Beispiel die Logdateien *dcpromo.log* und *dcpromoui.log*, die während der Heraufstufung zum Domänencontroller erzeugt werden.

Die Bedienung der Ereignisanzeige ist sehr intuitiv. Über den Kontextmenübefehl *Aufgabe an dieses Protokoll anfügen* können über die Aufgabenplanung spezielle Aktionen durchgeführt werden, sobald eine bestimmte Meldung auf dem Server auftaucht.

Überwachung der Systemleistung – Zuverlässigkeits- und Leistungsüberwachung

Über den Eintrag *Zuverlässigkeit und Leistung* in der Konsolenstruktur des Server-Managers können Sie sich die aktuelle Systemleistung Ihres Servers anzeigen lassen (Abbildung 18.7). Über den Knoten *Berichte* lassen sich auch auf Domänencontrollern sehr interessante Informationen über den Betrieb von Active Directory anzeigen.

Abbildg. 18.7 Überwachen der Serverleistung von Windows Server 2008



Die Gesamtleistung eines Systems wird durch verschiedene Faktoren begrenzt. Hierzu zählen etwa die Zugriffsgeschwindigkeit der physischen Datenträger, die Speichermenge, die für alle laufenden Prozesse zur Verfügung steht, die Prozessorgeschwindigkeit und der Datendurchsatz der Netzwerkschnittstellen. Nachdem die einschränkenden Faktoren auf der Hardwareseite identifiziert wurden, kann der Ressourcenverbrauch einzelner Anwendungen und Prozesse überprüft werden. Anhand einer umfassenden Leistungsanalyse, die sowohl die Auswirkungen von Anwendungen als auch die Gesamtkapazität berücksichtigt, können IT-Experten einen Bereitstellungsplan entwickeln und an die jeweiligen Anforderungen anpassen. Alternativ können Sie diese Funktion auch über *Start/Ausführen/perfmon.msc* starten. Durch Erweitern der *Ressourcenübersicht* können Sie zusätzliche Informationen anzeigen und überprüfen, welche Ressourcen von welchen Prozessen genutzt werden. Der Bereich mit der Ressourcenübersicht enthält vier animierte Diagramme, die die Auslastung der CPU-, Datenträger-, Netzwerk- und Speicherressourcen des lokalen Computers in Echtzeit anzeigen. Unter den Diagrammen befinden sich vier erweiterbare Bereiche, in denen Einzelheiten zur

jeweiligen Ressource angezeigt werden können. Klicken Sie zur Anzeige dieser Informationen auf den Abwärtspfeil rechts neben dem jeweiligen Balken.

CPU

In diesem Bereich wird die aktuelle Auslastung der CPU-Kapazität in Prozent angezeigt. Für die CPU stehen außerdem folgende Detailinformationen zur Verfügung:

- **Abbild** Die Anwendung, die die CPU-Ressourcen nutzt
- **PID** Die Prozess-ID der Anwendungsinstanz
- **Threads** Die Anzahl der Threads, die aktuell für die Anwendungsinstanz aktiv sind
- **CPU** Die CPU-Zyklen, die aktuell für die Anwendungsinstanz aktiv sind
- **Durchschnittliche CPU-Auslastung** Die von der Anwendungsinstanz verursachte durchschnittliche CPU-Auslastung. Angezeigt wird der prozentuale Anteil an der Gesamtkapazität der CPU.

Datenträger

In diesem Bereich wird die aktuelle Gesamtbelastung durch E-/A-Vorgänge angezeigt. Außerdem können folgende Detailinformation abgefragt werden:

- **Abbild** Die Anwendung, die die Datenträgerressourcen nutzt
- **PID** Die Prozess-ID der Anwendungsinstanz
- **Datei** Die Datei, die von der Anwendungsinstanz gelesen und/oder geschrieben wird
- **Lesen** Die aktuelle Geschwindigkeit (in Byte/min), mit der die Anwendungsinstanz Daten aus der Datei liest
- **Schreiben** Die aktuelle Geschwindigkeit (in Byte/min), mit der die Anwendungsinstanz Daten in die Datei schreibt

Netzwerk

In diesem Bereich wird der gesamte aktuelle Netzwerkverkehr (in Kbit/s) angezeigt. Für die Netzwerkauslastung stehen außerdem folgende Detailinformationen zur Verfügung:

- **Abbild** Die Anwendung, die die Netzwerkressourcen nutzt
- **PID** Die Prozess-ID der Anwendungsinstanz
- **Adresse** Die Netzwerkadresse, mit der der lokale Computer Informationen austauscht. Hier kann ein Computername (wenn sich der andere Computer im selben LAN befindet), eine IP-Adresse oder ein vollqualifizierter Domänenname angezeigt werden.
- **Senden** Die Datenmenge (in B/min), die die Anwendungsinstanz aktuell vom lokalen Computer an die Adresse sendet
- **Empfangen** Die Datenmenge (in B/min), die die Anwendungsinstanz aktuell von der Adresse empfängt
- **Total** Die gesamte Bandbreite (in B/min), die aktuell von der Anwendungsinstanz für das Senden und Empfangen genutzt wird

Speicher

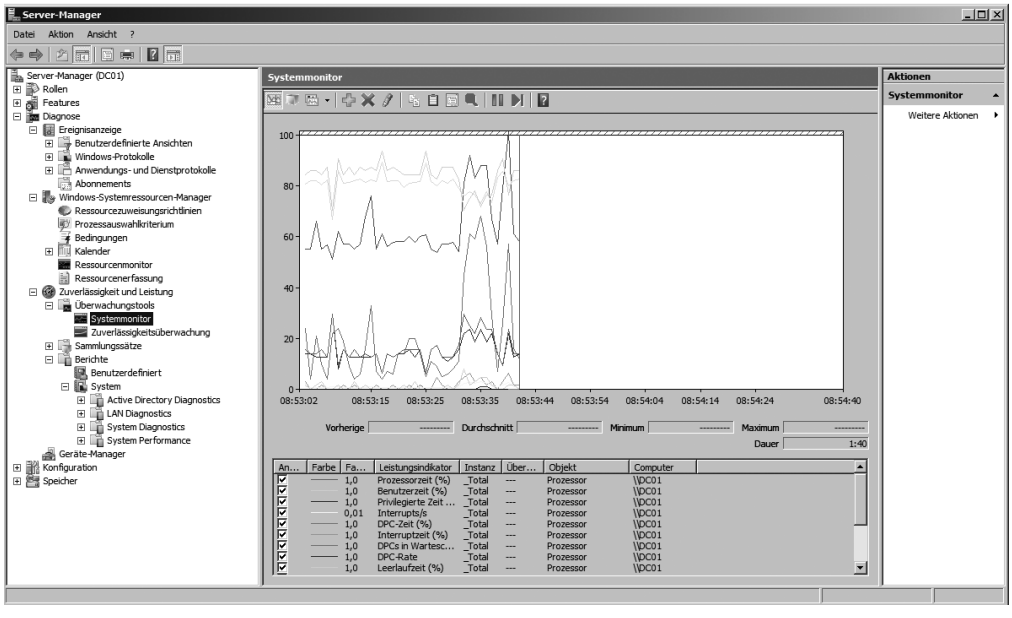
In diesem Bereich werden die aktuellen Seitenfehler pro Sekunde und der aktuell genutzte physische Speicher in Prozent angezeigt. Folgende Detailinformationen können für Speicherressourcen abgefragt werden:

- **Abbild** Die Anwendung, die die Speicherressourcen nutzt
- **PID** Die Prozess-ID der Anwendungsinstanz
- **Seitenfehler** Die Anzahl der Seitenfehler, die aktuell von der Anwendungsinstanz generiert werden

Der Systemmonitor

Klicken Sie in der Konsolenstruktur (die linke Fensterspalte) auf den Eintrag *Zuverlässigkeit und Leistung/Überwachungstools/Systemmonitor*, können Sie den Server noch genauer überwachen lassen (Abbildung 18.8).

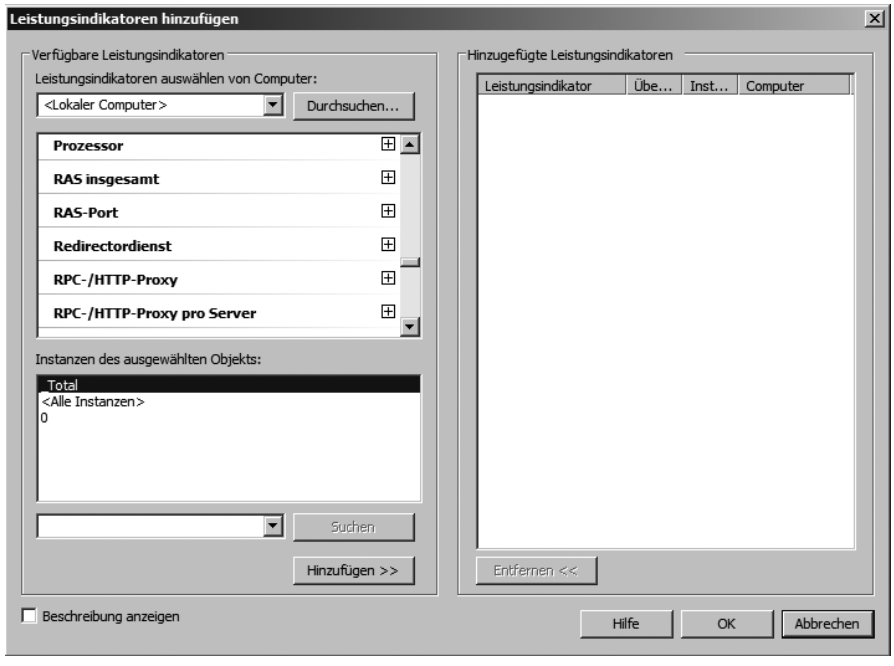
Abbildg. 18.8 Serverüberwachung mit dem Systemmonitor



Im Systemmonitor werden die integrierten Windows-Leistungsindikatoren grafisch dargestellt. Es können Daten in Echtzeit oder Verlaufsdaten angezeigt werden. Sie können im Systemmonitor Leistungsindikatoren entweder per Drag & Drop hinzufügen oder hierfür benutzerdefinierte Datensammlergruppen (Data Collector Sets, DCS) erstellen. Der Systemmonitor unterstützt verschiedene Ansichten für die visuelle Überprüfung der Daten in Leistungsprotokollen. Außerdem können benutzerdefinierte Ansichten in Form von Datensammlergruppen für die Verwendung in Leistungs- und Protokollfunktionen exportiert werden. Über das grüne Pluszeichen in der Symbolleiste können Sie weitere Leistungsindikatoren einblenden lassen. Wählen Sie zunächst den entsprechenden

Indikator aus und klicken Sie auf *Hinzufügen* (Abbildung 18.9). Sie können eine Beschreibung der Indikatorengruppe anzeigen, die aktuell in der Liste ausgewählt ist. Aktivieren Sie dazu das Kontrollkästchen *Beschreibung anzeigen* in der unteren linken Ecke des Bildschirms. Wenn Sie eine andere Gruppe auswählen, wird die zugehörige Beschreibung angezeigt. Sie können die verfügbaren Indikatoren einer Gruppe anzeigen, indem Sie auf den Abwärtspfeil rechts neben dem Gruppennamen klicken. Zum Hinzufügen einer Indikatorengruppe markieren Sie den Gruppennamen und klicken auf die Schaltfläche *Hinzufügen.*

Abbildg. 18.9 Hinzufügen von Leistungsindikatoren zum Systemmonitor



Nachdem Sie einen Gruppennamen markiert haben, können Sie die enthaltenen Leistungsindikatoren anzeigen. Markieren Sie einen Indikator in der Liste, bevor Sie auf *Hinzufügen* klicken, wird nur dieser Indikator hinzugefügt. Sie können einen einzelnen Indikator hinzufügen, indem Sie auf das Pluszeichen neben dem Gruppennamen klicken, den gewünschten Indikator markieren und danach auf *Hinzufügen* klicken. Möchten Sie mehrere Indikatoren einer Gruppe auswählen, klicken Sie bei gedrückter Strg-Taste auf die Namen in der Liste. Sobald alle gewünschten Indikatoren ausgewählt sind, klicken Sie auf *Hinzufügen*. Möchten Sie nur eine bestimmte Instanz eines Indikators hinzufügen, markieren Sie einen Gruppennamen in der Liste, wählen den gewünschten Prozess in der Liste im Bereich *Instanzen* des gewählten Objekts aus und klicken auf *Hinzufügen*. Derselbe Indikator kann von mehreren Prozessen generiert werden. Bei Auswahl einer Instanz werden nur diejenigen Indikatoren protokolliert, die vom gewählten Prozess erzeugt werden. Wenn Sie keine Instanz auswählen, werden alle Instanzen des Indikators protokolliert. Sie können nach Instanzen eines Indikators suchen, indem Sie die Indikatorengruppe markieren oder die Gruppe erweitern und den gewünschten Indikator markieren, den Prozessnamen in das Feld unterhalb der Instanzenliste für das gewählte Objekt eingeben und auf *Suchen* klicken. Der eingegebene Prozessname wird in der Dropdownliste für eine weitere Suche angeboten.

Beobachten der Indikatorendaten in Systemmonitor

Standardmäßig werden die Daten in Systemmonitor in Form eines Liniendiagramms angezeigt. Abgebildet werden Daten über einen Zeitraum von zwei Minuten. Die Abtastung erfolgt von links nach rechts. Die X-Achse ist beschriftet. Mithilfe des Diagramms lassen sich Änderungen an den Aktivitäten der einzelnen Indikatoren über einen kurzen Zeitraum beobachten. Sie können Details für einen bestimmten Indikator anzeigen, indem Sie im Diagramm mit der Maus auf die entsprechende Indikatorlinie zeigen. Mit dem Dropdownmenü auf der Symbolleiste können Sie die Anzeige für die aktuelle Datensammlergruppe ändern. In der Histogrammansicht werden Daten in Echtzeit angezeigt. In dieser Ansicht lassen sich Änderungen an den Aktivitäten der einzelnen Indikatoren beobachten. Die Berichtansicht enthält die Werte für den ausgewählten Indikator in Textform. Unter dem Ansichtsfenster befindet sich eine Legende mit Angaben zu den einzelnen Leistungsindikatoren. Über die Kontrollkästchen der einzelnen Zeilen können Sie steuern, welche Indikatoren in der Ansicht dargestellt werden. Ist eine Zeile in der Legende ausgewählt, können Sie die zugehörige Indikatorlinie optisch hervorheben, indem Sie auf der Symbolleiste auf die Schaltfläche *Markierung* klicken. Durch erneutes Klicken auf diese Schaltfläche wird die ursprüngliche Anzeige wiederhergestellt.

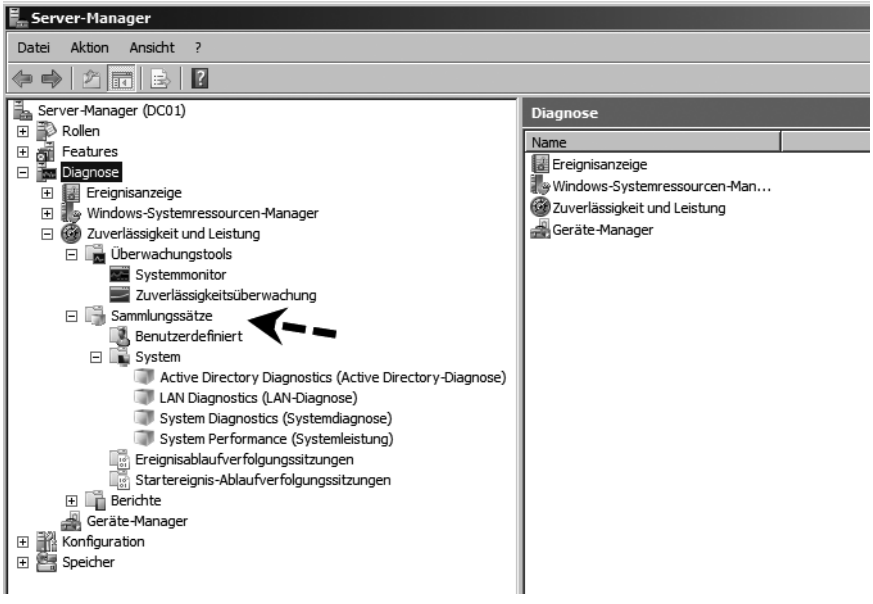
Sie können die Eigenschaften für die Anzeige eines Indikators ändern. Klicken Sie dazu mit der rechten Maustaste auf die entsprechende Zeile in der Legende, und wählen Sie *Eigenschaften*. Daraufhin wird das Dialogfeld *Eigenschaften* von Systemmonitor geöffnet. Die Registerkarte *Daten* ist aktiviert. Passen Sie die Eigenschaften mithilfe der Einträge in den Listenfeldern an. Mit der Schaltfläche *Anzeige fixieren* auf der Symbolleiste können Sie die Anzeige einfrieren, um die aktuelle Aktivität zu überprüfen. Wenn Sie die Anzeige wieder aktivieren möchten, klicken Sie auf die Schaltfläche *Fixierung der Anzeige aufheben*. Durch Klicken auf die Schaltfläche *Daten aktualisieren* kann die Anzeige schrittweise durchlaufen werden. Wird die Anzeige des Liniendiagramms angehalten und anschließend wieder gestartet, ändert sich der auf der X-Achse dargestellte Zeitraum. Der Systemmonitor arbeitet mit so genannten *Objekten*, die beobachtet werden können. Für jedes dieser Objekte wie zum Beispiel den Prozessor gibt es eine Reihe von Leistungsindikatoren wie *Prozessorzeit* oder *Interrupts/s*. Für einzelne Objekte gibt es zudem mehrere Instanzen. Dies ist zum Beispiel beim Prozessor der Fall, wenn mit einem Multiprozessor-System gearbeitet wird. Beim Objekt *Prozesse* wird eine Instanz für jeden aktiven Prozess definiert.

Sammlungssätze

Die Echtzeitanzeige ist nur eine Möglichkeit, den Systemmonitor zu nutzen. Nachdem Sie eine Kombination aus Datensammlern zusammengestellt haben, die nützliche Echtzeitinformationen über Ihr System liefern, können Sie diese als *Sammlungssätze* (Data Collector Set, DCS) speichern. Sammlungssätze bilden die Grundlage für die Leistungsüberwachung und Berichterstellung. Mit ihrer Hilfe lassen sich mehrere Datensammlungspunkte in einer Komponente zusammenfassen, die dann zum Überprüfen und Protokollieren genutzt werden kann. Um einen Sammlungssatz zu erstellen, beginnen Sie mit der Anzeige der Leistungsindikatoren. Erweitern Sie in der Konsole die Hierarchiestruktur, klicken Sie mit der rechten Maustaste auf *Systemmonitor* und rufen Sie im Kontextmenü den Untermenübefehl *Neu*/*Sammlungssatz* auf. Daraufhin wird der Assistent für die Erstellung einer neuen Datensammlergruppe gestartet. Die neue Datensammlergruppe enthält alle Informationen, die in der aktuellen Systemmonitoransicht ausgewählt sind. Alle von der Daten-

sammlergruppe zusammengestellten Informationen werden im Stammverzeichnis gespeichert. Sie können diese Vorgabe auch ändern und einen anderen Speicherort angeben. Möchten Sie nicht den Standardbenutzer verwenden, klicken Sie auf die Schaltfläche *Ändern* und geben den Namen und das Kennwort des gewünschten Benutzers ein. Der Sammlungssatz muss unter dem Konto eines Benutzers mit Administratorrechten ausgeführt werden.

Abbildg. 18.10 Erstellen eines Sammlungssatzes im Systemmonitor



Neben benutzerdefinierten Sammlungssätzen, werden automatisch bereits bei der Installation von Windows Server 2008 Sammlungssätze angelegt, die zur Diagnose verwendet werden können (Abbildung 18.10)

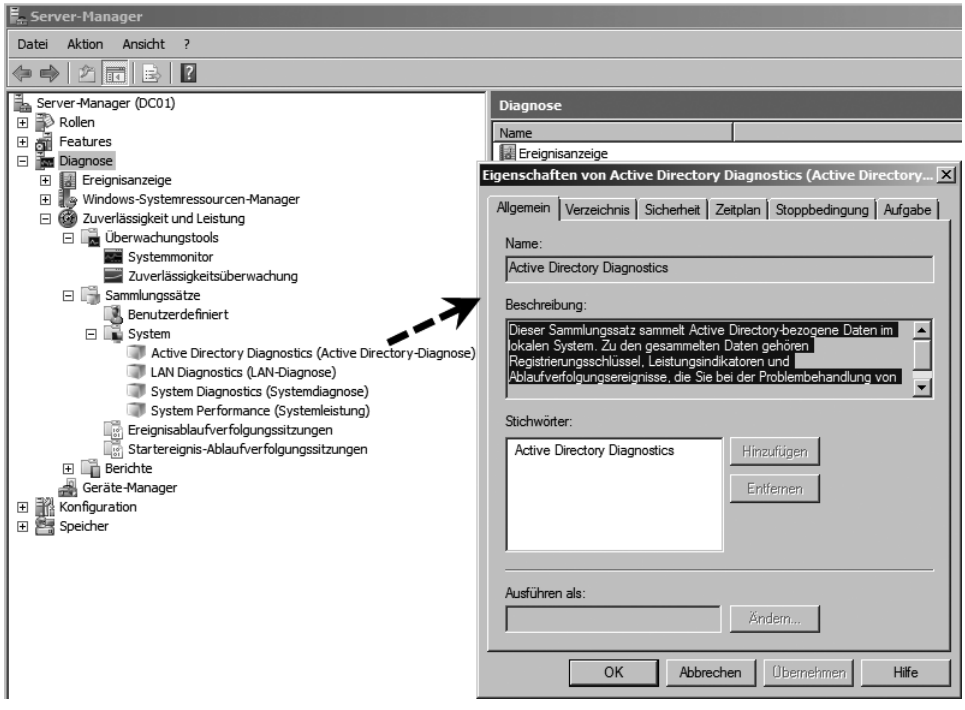
Protokolle aus einem Sammlungssatz erstellen

Ein Sammlungssatz erstellt eine Protokolldatei. Sie haben die Möglichkeit, für jeden Satz Speicheroptionen zu konfigurieren. Sie können beispielsweise bestimmen, dass der Dateiname Angaben zum Protokoll enthalten soll, und die Dateigröße für bestimmte Protokolle begrenzen. Außerdem können Sie entscheiden, ob Daten überschrieben oder angehängt werden sollen. Klicken Sie in der Liste des Fensters mit der rechten Maustaste auf den Namen des Sammlungssatzes, der konfiguriert werden soll, und wählen Sie *Eigenschaften*. Auf der Registerkarte *Allgemein* können Sie eine Beschreibung oder Schlüsselwörter für die Datensammlergruppe eingeben. Auf der Registerkarte *Verzeichnis* ist das Stammverzeichnis als Standardverzeichnis festgelegt, in dem alle Protokolldateien für die Datensammlergruppe gespeichert werden. Mit *Aktiver Bereich* geben Sie an, wann mit der Datensammlung begonnen wird. Mit den Optionen unter *Starten* legen Sie fest, wann ein neues Protokoll erstellt wird. Sie können einen Startzeitpunkt angeben und die Wochentage festlegen, an denen die Datensammlung erneut gestartet wird.

Auf der Registerkarte *Stoppbedingung* können Sie Kriterien für Bedingungen angeben, bei denen die Datensammlung angehalten wird. Wenn Sie das Kontrollkästchen *Maximale Dauer* aktivieren, können

Sie festlegen, wie lange Daten gesammelt werden sollen. Ist dieses Kontrollkästchen deaktiviert, erfolgt die Datensammlung zeitlich unbegrenzt. Im Bereich *Grenzen* können Sie durch Aktivieren des entsprechenden Kontrollkästchens einen Neustart der Datensammler vorsehen, wenn eine bestimmte Grenze erreicht ist. Auf diese Weise lassen sich segmentierte Protokolle erzeugen. Ist das Kontrollkästchen deaktiviert, erfolgt kein Neustart der Datensammlung, wenn eine der Grenzen erreicht ist. Wenn Sie auf der Registerkarte *Zeitplan* ein Ablaufdatum festgelegt haben, das nach einer auf der Registerkarte *Stoppbedingung* definierten Bedingung liegt, hat die Stoppbedingung Vorrang.

Abbildg. 18.11 Verwalten von Sammlungssätzen im Systemmonitor



Leistungsüberwachung für Fortgeschrittene

In diesem Abschnitt gehen wir etwas detaillierter darauf ein, wie Sie einzelne Engpässe in Windows Server 2008 entdecken können.

Speicherengpässe

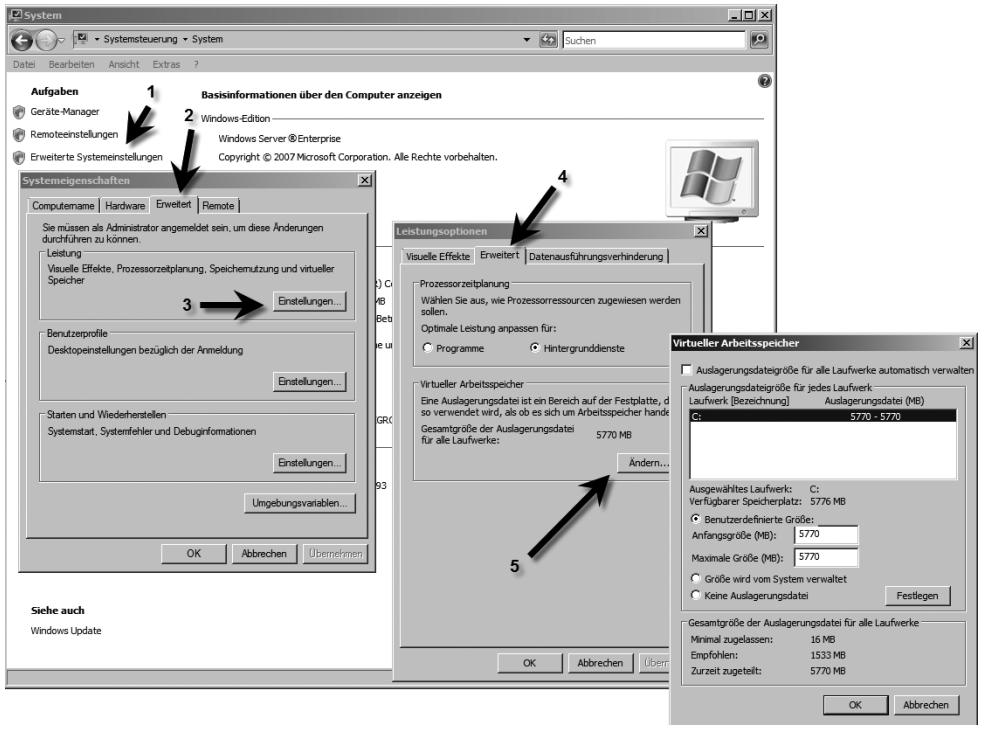
Performanceprobleme können eine Reihe unterschiedlicher Ursachen haben. Ein weiteres Problem bei der Performanceanalyse ist, dass die Beseitigung eines Engpasses oft zum nächsten Engpass führt. Dafür gibt es viele Beispiele. Wenn mehr Speicher bereitsteht, zeigt sich oft, dass auch die Prozessorauslastung bereits an der Kapazitätsgrenze ist. Es gibt nun einige grundsätzliche Regeln für den Einsatz von Hauptspeicher. Die erste Regel lautet: Viel hilft viel, sowohl beim Hauptspeicher als auch beim Cache. Das hat für Windows Server 2008 noch mehr Gültigkeit als unter Windows Server 2003. Die

zweite Regel besagt, dass die Auslagerungsdatei am besten auf einer anderen physischen Festplatte als der Systempartition aufgehoben ist. Der Preis dafür ist, dass dann keine Speicherdumps bei einem Systemfehler mehr durchgeführt werden können. Profis können Speicherdumps dazu nutzen, Fehler im Betriebssystem nachzuvollziehen. Allerdings werden diese Möglichkeiten heutzutage eher weniger genutzt, da zur Fehlerbehebung bessere Möglichkeiten und Tools zur Verfügung stehen. Die Auslagerungsdatei ist auch einer der Bereiche, die für die Speicherverwaltung die größte Bedeutung haben. Windows Server 2008 lagert Informationen aus dem physischen Hauptspeicher in die Auslagerungsdatei aus, wenn nicht genügend Hauptspeicher zur Verfügung steht. Der Server kann zwar, ausreichend freie Festplattenkapazität vorausgesetzt, fast beliebig viel Speicher auslagern. Es ist aber relativ schnell der Punkt erreicht, an dem diese Auslagerung zu langsam wird. Die Überwachung der Auslagerung spielt daher bei der Analyse eine wichtige Rolle.

Konfiguration der Auslagerungsdatei

Sie sollten die Auslagerungsdatei auf eine andere physische Festplatte des Servers verschieben, damit Schreibzugriffe auf die Auslagerungsdatei nicht von Schreibzugriffen auf der Festplatte ausgebremst werden. Wenn keine zweite physische Festplatte zur Verfügung steht, macht ein Verschieben keinen Sinn, da die Auslagerung auf eine Partition, die auf derselben Platte liegt, keine positiven Auswirkungen hat. Zusätzlich sollten Sie die Größe der Auslagerungsdatei auf das 2,5-fache des tatsächlichen Arbeitsspeichers legen. Damit wird die Fragmentierung der Datei minimiert. Die maximale Größe der Auslagerungsdatei von 4.095 MB, wurde unter Windows Server 2008 aufgehoben. Die Einstellungen für die Auslagerungsdatei finden Sie über *Start/Systemsteuerung/System/Erweiterte Systemeinstellungen/Erweitert/Einstellungen/Erweitert/Virtueller Arbeitsspeicher/Ändern* (Abbildung 18.12).

Abbildg. 18.12 Anpassen des Speicherortes der Auslagerungsdatei



1. Deaktivieren Sie das Kontrollkästchen *Auslagerungsdateigröße für alle Laufwerke automatisch verwalten*.
2. Aktivieren Sie die Option *Benutzerdefinierte Größe*.
3. Setzen Sie bei *Anfangsgröße* und bei *Maximale Größe* in etwa das 2,5-fache Ihres Arbeitsspeichers ein. Dadurch ist sichergestellt, dass die Datei nicht fragmentiert wird, da sie immer die gleiche Größe hat. Setzen Sie die Größe der Auslagerungsdatei für Laufwerk C: auf 0.
4. Klicken Sie auf *Festlegen*.
5. Schließen Sie alle Fenster und starten Sie den Server neu.

TIPP Auf einem Core-Server verschieben Sie die Auslagerungsdatei am besten mit dem Befehl *Wmic pagefileset where name="<Pfad>" set InitialSize=<Anfangsgröße>,MaximumSize=<Maximale Größe>*. Zuvor wird die automatische Konfiguration mit dem Befehl *wmic computersystem where name="<computername>" set AutomaticManagedPagefile=False* beendet. Interessante Hinweise zu diesem Vorgang finden Sie auch auf der Internetseite *http://forums.microsoft.com/TechNet/ShowPost.aspx?PostID=2599415&SiteID=17*.

Die nahe liegende Konsequenz bei Speicherengpässen heißt mehr RAM. Nur ist das keineswegs immer die sinnvollste Konsequenz. In jedem Fall sollte zunächst untersucht werden, welche Prozesse für die hohe Speicherauslastung verantwortlich sind. Dazu wird das Objekt *Prozess* in der Überwachung des Systemmonitors verwendet. Diesen finden Sie über den Menüpunkt *Systemmonitor*. Bei diesem werden die verschiedenen laufenden Prozesse angezeigt. Für die Analyse muss nun überlegt werden, welche Prozesse einen besonders hohen Speicherbedarf haben könnten.

Die Prozessorauslastung

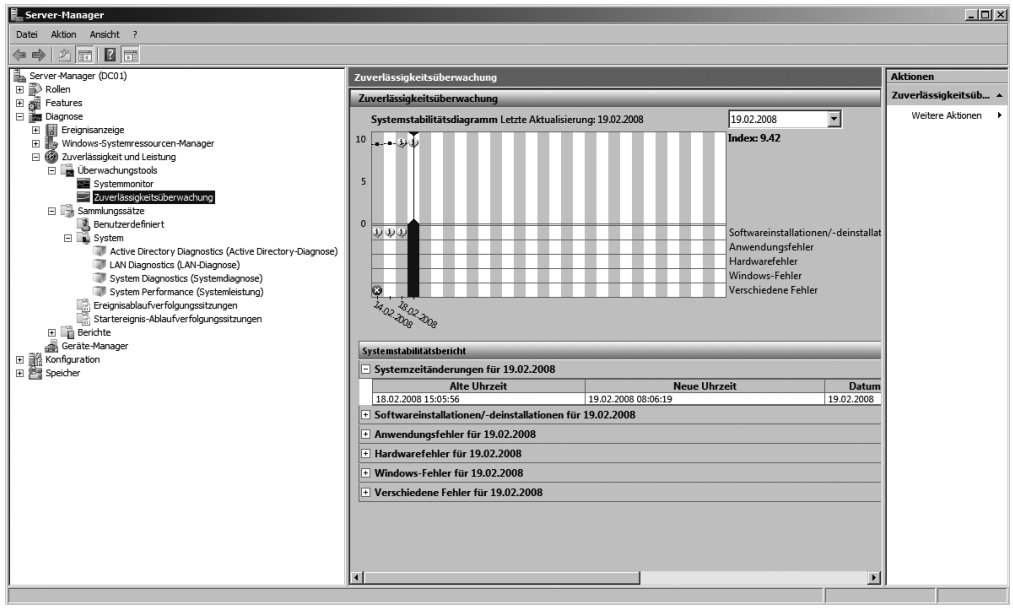
Auch die Prozessorleistung kann natürlich einen solchen Flaschenhals darstellen. Zu wenig Hauptspeicher kann die Konsequenz haben, dass auch der Prozessor sehr stark belastet wird. Denn die Auslagerung von Seiten und viele andere Vorgänge gehen natürlich nicht spurlos am Prozessor vorbei. Er hat an der Verwaltung des Arbeitsspeichers einen relativ hohen Anteil. Da Engpässe beim Hauptspeicher typischerweise deutlich kostengünstiger zu beheben sind als solche beim Prozessor, sollte diese Situation zunächst untersucht werden. Die Auslastung ist kein Problem, wenn sie kurzzeitig über 90 % liegt oder wenn das öfter einmal vorkommt. Zum Problem wird sie, wenn sie über längere Zeiträume in diesem Bereich liegt. Aber auch dann muss man mit der Analyse noch etwas vorsichtig sein. Bei Mehrprozessorsystemen gilt das Augenmerk natürlich vor allem den Leistungsindikatoren aus dem Objekt *System*. Dort werden Informationen von mehreren Systemkomponenten zusammengefasst. So kann dort beispielsweise die Gesamtbelastung aller Prozessoren ermittelt werden.

Der Leistungsindikator *Gesamtprozessorzeit* gibt Aufschluss darüber, wie stark die Prozessoren ausgelastet waren. Ergänzend sind aber auch hier die Leistungsindikatoren *Prozessorzeit* des Objekts *Prozessor* von Bedeutung. Wenn viele verschiedene Prozesse ausgeführt werden, ist eine einigermaßen gleichmäßige Lastverteilung fast sicher. Bei einem einzelnen Prozess ist dagegen die Aufteilung in einigermaßen gleichgewichtige Threads wichtig. Ein Thread ist eine Ausführungseinheit eines Prozesses. Wenn ein Prozess mehrere Threads verwendet, können diese auf unterschiedlichen Prozessoren ausgeführt werden. Die Verteilung erfolgt entsprechend der Auslastung der einzelnen Prozessoren durch das System. Eine hohe Zahl von Warteschlangen bedeutet, dass mehrere Threads rechenbereit sind, ihnen aber vom System noch keine Rechenzeit zugewiesen wurde. Die Faustregel für diesen Wert ist, dass er nicht allzu häufig über 2 liegen sollte. Wenn die Auslastung des Prozessors im Durchschnitt relativ gering ist, spielt dieser Wert nur eine untergeordnete Rolle.

Zuverlässigkeitsüberwachung

Die Zuverlässigkeitsüberwachung ist ein Snap-In für die Microsoft Management Console (MMC), das einen Überblick über die Systemstabilität sowie eine Trendanalyse mit Detailinformationen zu Ereignissen liefert, die sich auf die Stabilität des Gesamtsystems auswirken. Die Aufzeichnung entsprechender Daten beginnt mit der Systeminstallation (Abbildung 18.13). Sie finden die Zuverlässigkeitsüberwachung im Server-Manager über den Knoten *Diagnose/Zuverlässigkeit und Leistung/Zuverlässigkeitsüberwachung*. Bis Daten über einen Zeitraum von 28 Tagen zur Verfügung stehen, wird der Stabilitätsindex im Diagramm als gepunktete Linie dargestellt. Erst danach ist eine Messbasis für eine Berechnung vorhanden.

Abbildg. 18.13 Zuverlässigkeitsüberwachung in Windows Server 2008



In der oberen Hälfte der Zuverlässigkeitsüberwachung sehen Sie das Systemstabilitätsdiagramm und einen Kalender für die Auswahl eines Datums oder eines Datumsbereichs. Die Zuverlässigkeitsüberwachung speichert Verlaufsdaten für Systemstabilität und Zuverlässigkeitsereignisse über einen Zeitraum von einem Jahr. Im Systemstabilitätsdiagramm wird der fortlaufende Stabilitätsindex für das Betriebssystem angezeigt. In Windows Server 2008 deckt das Diagramm einen Zeitraum von einem Monat ab. Am unteren Rand des Systemstabilitätsdiagramms sehen Sie fünf Kategorien für Zuverlässigkeitsereignisse, die in die Stabilitätsberechnung für das System eingehen. Klicken Sie auf das Pluszeichen (+) neben einer Kategorie, werden die Ereignisse für das gewählte Datum bzw. den gewählten Datumsbereich angezeigt. Für jeden Ereignistyp sind folgende Daten verfügbar:

Softwareinstallationen/-deinstallationen

Diese Kategorie enthält Informationen zur Installation und Deinstallation von Software (Betriebssystem, Windows-Aktualisierungen, Treiber und Anwendungen).

- **Software** Betriebssystem, Name der Anwendung, Name der Windows-Aktualisierung oder Treibername
- **Version** Version des Betriebssystems, der Anwendung oder des Treibers (für Windows-Aktualisierungen steht dieses Feld nicht zur Verfügung)
- **Aktivität** Hier wird angezeigt, ob es sich um eine Installation oder Deinstallation handelt
- **Aktivitätsstatus** Hier wird angezeigt, ob die Aktion erfolgreich war oder fehlgeschlagen ist
- **Datum** Das Datum der Aktion

Anwendungsfehler

In dieser Kategorie werden Anwendungsabstürze protokolliert. Hierzu zählt auch das Beenden nicht mehr reagierender Anwendungen.

- **Anwendung** Der Name der ausführbaren Datei der Anwendung, die zum Stillstand gekommen oder abgestürzt ist
- **Version** Die Versionsnummer der Anwendung
- **Fehlertyp** Hier wird der Fehlertyp angezeigt (Stillstand oder Absturz)
- **Datum** Das Datum des Anwendungsfehlers

Hardwarefehler

Diese Kategorie enthält Informationen zu Datenträgerfehlern (DFD) und Speicherfehlern (WMD).

- **Komponententyp** Die Komponente (Festplattenlaufwerk oder Speicher), bei der der Fehler aufgetreten ist
- **Gerät** Das Gerät, bei dem der Fehler aufgetreten ist
- **Fehlertyp** Hier wird angezeigt, ob der Fehler durch ein defektes Laufwerk oder einen beschädigten Block (Laufwerksfehler) bzw. durch einen defekten Speicher (Speicherfehler) verursacht wurde
- **Datum** Das Datum des Hardwarefehlers

Windows-Fehler

In diese Kategorie fallen Betriebssystemabstürze, Startfehler und Ruhezustandsfehler.

- **Fehlertyp** Hier wird angezeigt, ob es sich um einen Startfehler, einen Absturz des Betriebssystems oder einen Fehler beim Wechsel in den Ruhezustand handelt
- **Version** Die Version des Betriebssystems und des Service Packs
- **Datum** Das Datum des Windows-Fehlers

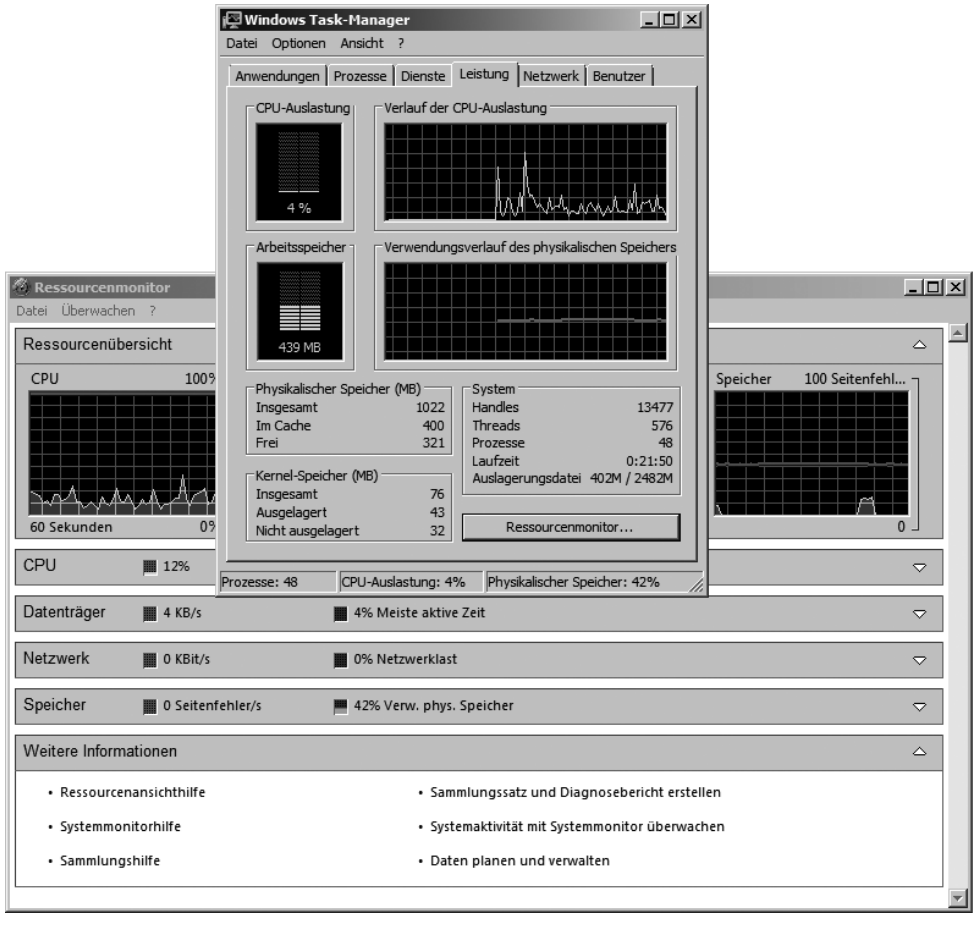
Der Task-Manager

Ein weiteres wichtiges Werkzeug für die Analyse der Performance ist der Windows Task-Manager. Dieser zeichnet sich dadurch aus, dass er mit sehr wenig Aufwand genutzt werden kann. Sie können den Task-Manager durch einen Klick mit der rechten Maus auf die Taskleiste über dessen Kontextmenü aufrufen. Alternativ können Sie den Task-Manager auch über das Menü aufrufen, das mit der Tastenkombination Strg+Alt+Entf erscheint, oder über *Start/Ausführen/taskmgr*. Direkt

lässt sich der Task-Manager über die Tastenkombination Strg+⇧+Esc starten. Der Task-Manager stellt sechs Registerkarten bereit (Abbildung 18.14):

- Auf der Registerkarte *Anwendungen* erhalten Sie einen Überblick über die aktuell laufenden Anwendungen. Angezeigt wird der Status dieser Anwendungen. Darüber hinaus können Sie über das Kontextmenü der Anwendungen steuern, wie diese Anwendungen angezeigt werden sollen. Außerdem können Sie hier laufende Anwendungen (Tasks) beenden, zu Anwendungen wechseln oder über die Schaltfläche *Neuer Task* auch neue Anwendungen starten. Diese zuletzt genannte Funktion entspricht dem Befehl *Ausführen* aus dem Startmenü.

Abbildg. 18.14 Systemüberwachung von Windows Server 2008 mit dem Task-Manager

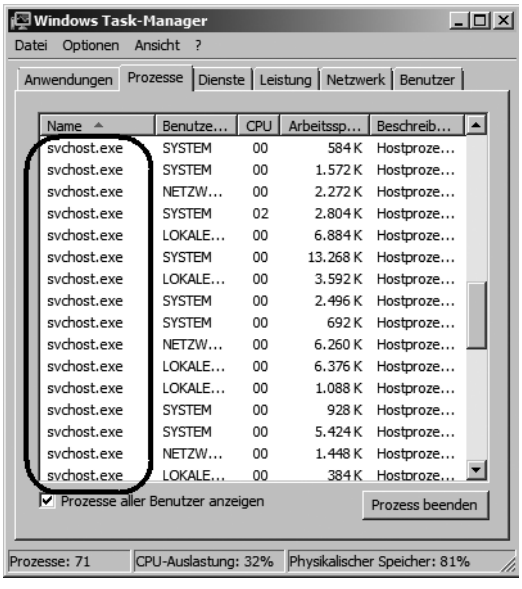


- Noch interessanter ist die Registerkarte *Prozesse*. Hier erhalten Sie einen Überblick über die derzeit aktiven Prozesse. Dabei handelt es sich nicht nur um Anwendungen, sondern auch um die gesamten Systemdienste, die im Hintergrund ausgeführt werden. Zu jedem dieser Prozesse werden Informationen über die Prozess-ID (PID), den aktuellen Anteil an der Nutzung der CPU, die insgesamt in dieser Arbeitssitzung konsumierte CPU-Zeit sowie die aktuelle Speichernutzung angezeigt. Gerade diese letzte Information ist von besonderem Interesse, da sie darüber

informiert, in welchem Umfang Anwendungen den Hauptspeicher tatsächlich nutzen – ohne dass man komplexe Parameter im Systemmonitor überwachen muss. Auch hier können Prozesse über die entsprechende Schaltfläche wieder beendet werden. Sie sollten damit allerdings sehr vorsichtig sein, da das Beenden eines Dienstes dazu führen kann, dass Ihr System nicht mehr korrekt ausgeführt wird.

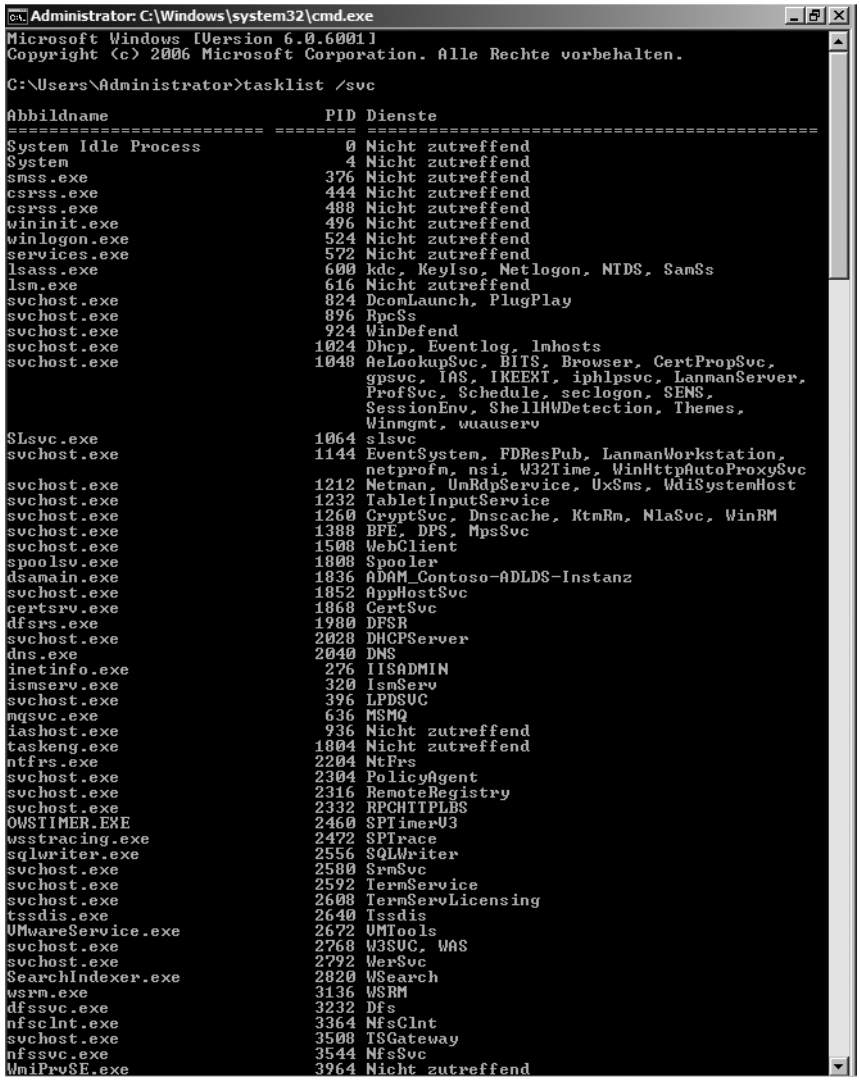
Bei den Prozessen fällt vor allem der Prozess *svchost.exe* auf. Die *svchost.exe* gibt es seit Windows 2000; sie liegt im *System32*-Verzeichnis und wird beim Systemstart von Windows automatisch als allgemeiner Prozess gestartet. Der Prozess durchsucht beim Systemstart die Registry nach Diensten, die beim Systemstart geladen werden müssen. Dienste, die nicht eigenständig lauffähig sind, sondern über Dynamic Link Library (DLL)-Dateien geladen werden, werden mit Hilfe der *svchost.exe* geladen. Auch wenn Windows läuft, kommt die *svchost.exe* immer dann ins Spiel, wenn Dienste über DLL-Dateien geladen werden müssen. Das Betriebssystem startet SVCHOST-Sessions, sobald solche benötigt werden und beendet sich auch wieder, sobald sie nicht mehr gebraucht werden. Da unter Windows die unterschiedlichsten Dienste parallel laufen, können auch mehrere Instanzen der *svchost.exe* gleichzeitig in der Prozessliste auftauchen (Abbildung 18.15).

Abbildg. 18.15 Anzeige der Prozesse, die durch den Dienst *svchost.exe* gestartet werden



Über den Befehl *tasklist /svc* in der Befehlszeile können Sie sich anzeigen lassen, welche Anwendungen auf die *svchost.exe* zurückgreifen (Abbildung 18.16).

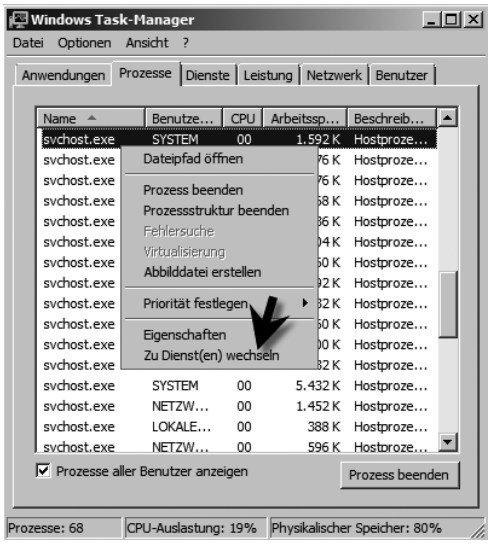
Abbildg. 18.16 Anzeige der Prozesse und der dazugehörigen Dienste in der Befehlszeile über *tasklist /svc*



TIPP Alternativ können Sie die mit *svchost.exe* verbundenen Dienste auch im Task-Manager anzeigen lassen. Gehen Sie dazu folgendermaßen vor:

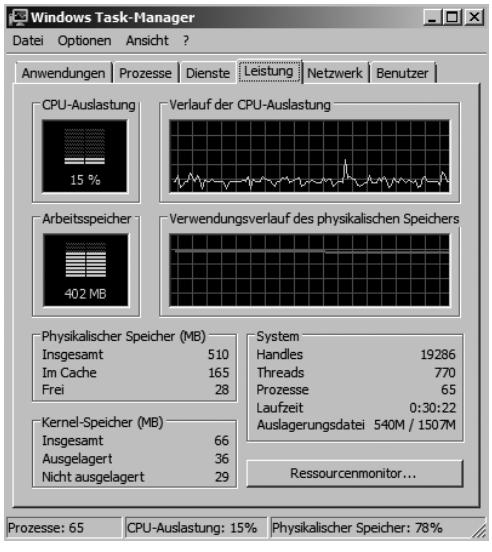
1. Öffnen Sie den Task-Manager
2. Aktivieren Sie die Registerkarte *Prozesse*.
3. Klicken Sie mit der rechten Maustaste auf eine Instanz von *svchost.exe*, und klicken Sie dann auf *Zu Dienst(en) wechseln* (Abbildung 18.17). Die dem betreffenden Prozess zugeordneten Dienste werden auf der Registerkarte *Dienste* hervorgehoben.

Abbildg. 18.17 Anzeige der zu Prozessen gehörigen Dienste



Eine weitere Option, die über den Befehl *Priorität festlegen* im Kontextmenü der verschiedenen Prozesse zur Verfügung steht, ist die Möglichkeit zur Prioritätssteuerung laufender Prozesse. Eine höhere Priorität führt dazu, dass ein Prozess mehr Rechenzeit zugewiesen erhält. Bei der Priorität *Echtzeit* erhält der Prozess die gesamte zuteilbare Rechenzeit. Die manuelle Zuordnung von Prioritäten sollte allerdings generell nur von Experten vorgenommen werden, da sie auch die gegenteilige Wirkung – nämlich ein deutlich langsameres System – haben kann, wenn hier falsche Einstellungen getroffen werden.

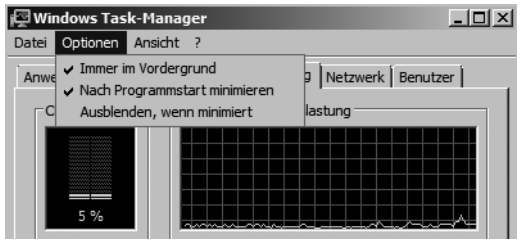
Abbildg. 18.18 Anzeige des Leistungsverbrauchs im Task-Manager



- Des Weiteren gibt es noch die Registerkarte *Leistung*. Dahinter verbirgt sich ein kleiner Systemmonitor, der die wichtigsten Informationen zur Systemauslastung in grafischer Form zur Verfügung stellt (Abbildung 18.18). In kleinen Fenstern wird die Auslastung der CPU und des Speichers zum aktuellen Zeitpunkt und im Zeitablauf dargestellt. Darunter findet sich eine Fülle von Informationen rund um die aktuelle Speichernutzung. Von besonderem Interesse ist dabei das Verhältnis von insgesamt zugesichertem virtuellen Speicher und dem physisch vorhandenen Hauptspeicher. Wenn mehr virtueller Speicher zugesichert ist, als im System vorhanden ist, muss auf jeden Fall ausgelagert werden. Eine optimale Systemgestaltung führt dazu, dass ausreichend physischer Hauptspeicher vorhanden ist beziehungsweise der Mittelwert des zugesicherten virtuellen Speichers zumindest nicht wesentlich über dem physischen Hauptspeicher liegt.
- Über die Registerkarte *Leistung* können Sie auch den *Ressourcenmonitor* starten, der auch im Server-Manager zur Verfügung steht.
- Die Registerkarten *Netzwerk* und *Benutzer* ergänzen die Registerkarte *Systemleistung* mit weiteren aktuellen Informationen zur Systemleistung.

Über die Befehle im Menü *Optionen* können Sie einige Einstellungen zum Verhalten des Task-Managers vornehmen (Abbildung 18.19).

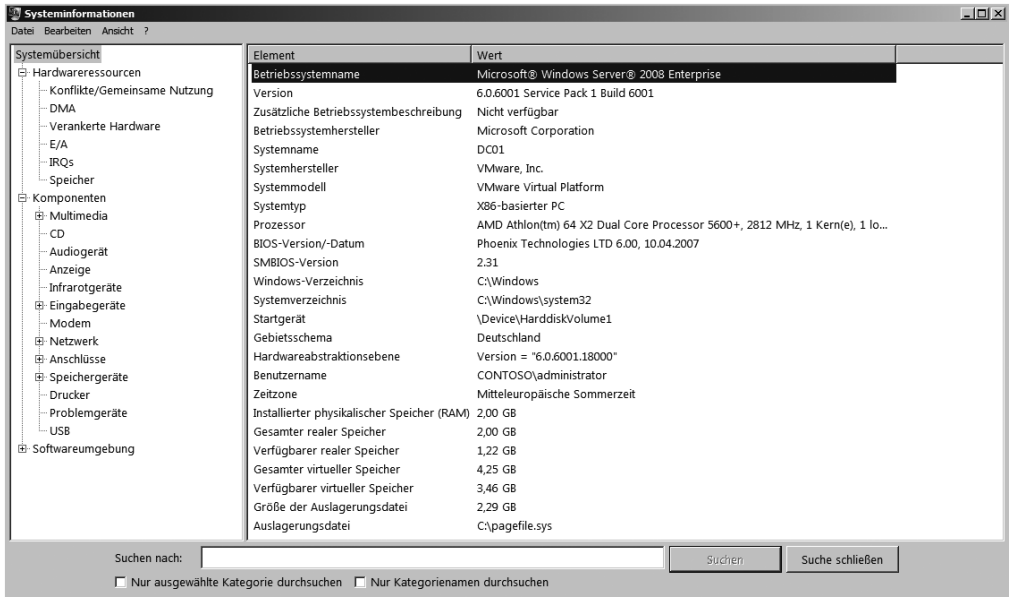
Abbildg. 18.19 Den Task-Manager konfigurieren



- **Immer im Vordergrund** Sorgt dafür, dass der Task-Manager immer im Vordergrund steht, wenn er ausgeführt wird. Dann kann allerdings nicht mehr besonders gut mit anderen Anwendungen gearbeitet werden. Diese Funktion hilft vor allem bei der Fehlersuche.
- **Nach Programmstart minimieren** Wenn diese Option gewählt ist, wird der Task-Manager nach dem Aufruf minimiert und lediglich im Infobereich der Taskleiste als kleines Symbol angezeigt.
- **Ausblenden, wenn minimiert** Mit dieser Option wird definiert, dass der Task-Manager nicht in der Taskleiste auftaucht, wenn er minimiert ist. Es findet sich dann nur noch im Infobereich der Taskleiste ein Symbol, das über die aktuelle Nutzung des Prozessors informiert.

TIPP Über *Start/Ausführen/msinfo32.exe* können Sie ebenfalls eine sehr ausführliche Übersicht über die eingebaute Hardware und die Ressourcen eines PCs abrufen (Abbildung 18.20).

Abbildg. 18.20 Aufrufen von Systeminformationen über *msinfo32.exe*



Beenden von Programmen über die Befehlszeile *Taskkill* und *Tasklist*

Mit *Tasklist* können Sie sich eine Liste der Anwendungen und Dienste mit der dazugehörigen PID (Prozess-ID) für alle Tasks anzeigen lassen. Der Befehl hat die Syntax *tasklist.exe /s <Computer>*. Mit dem Parameter */s <Computer>* geben Sie den Namen oder die IP-Adresse eines Remotecomputers an. Sie können diese Liste mit dem Befehl *tasklist > C:\tasks.txt* in eine Datei umleiten und bei Bedarf hinterher ausdrucken. Während Sie mit *tasklist.exe* eine Liste der Tasks ausgeben, können Sie mit *taskkill <PID>* einen Prozess beenden. Außerdem können Sie den Parameter */t* verwenden, um alle untergeordneten Prozesse zusammen mit dem übergeordneten Prozess abzubrechen.

Dienste in der Befehlszeile starten und beenden

Vor allem auf Core-Servern werden Sie Dienste und Tasks über die Befehlszeile steuern. Sie können sich die Dienste auf einem Core-Server zwar auch mit der Verwaltungskonsole Computerverwaltung von einem normalen Server anzeigen lassen (*Start/Ausführen/compmgmt.msc*), allerdings geht der schnelle Neustart oder das Beenden eines Dienstes auf einem Core-Server am schnellsten in der Befehlszeile, anstatt über die Remoteverwaltung. Um sich alle gestarteten Dienste anzeigen zu lassen, können Sie die beiden folgenden Befehle verwenden:

- Sc query
- Net start

Um einen Dienst zu starten, verwenden Sie einen der beiden Befehle:

- Sc start *<Dienst>*
- Net start *<Dienst>*

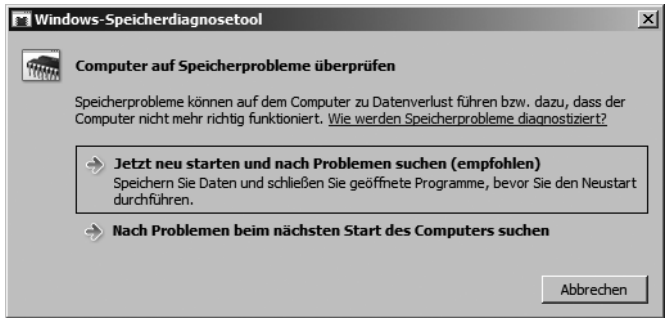
Um einen Dienst zu beenden, verwenden Sie einen der beiden Befehle:

- Sc stop *<Dienst>*
- Net stop *<Dienst>*

Diagnose des Arbeitsspeichers

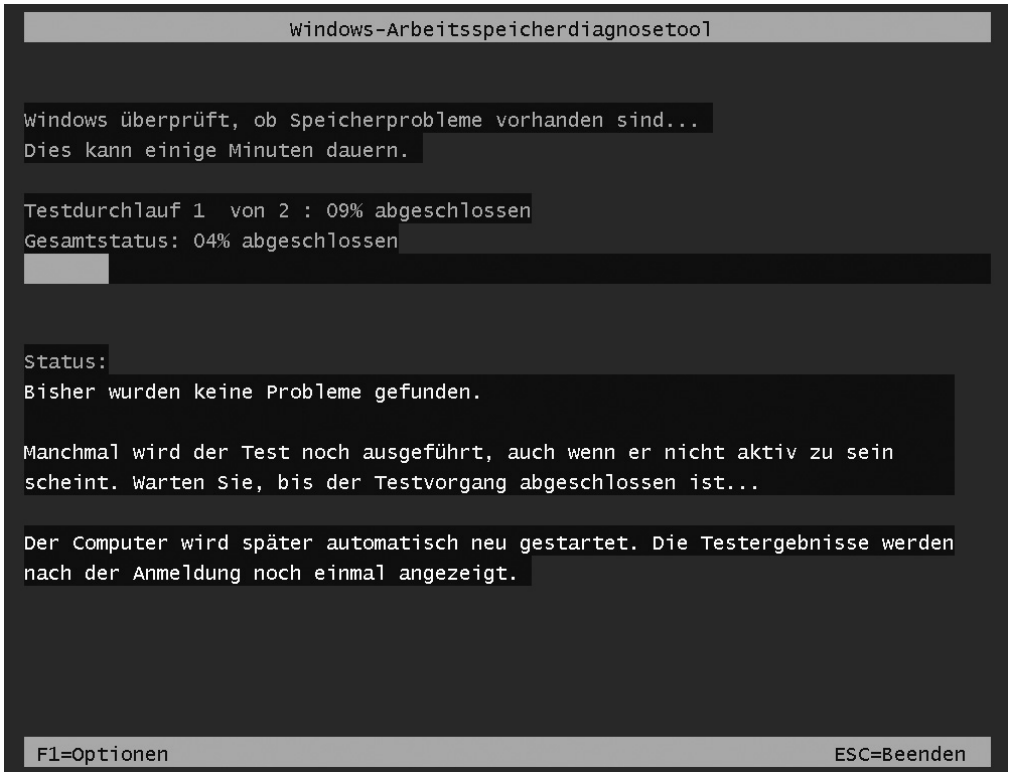
Häufig sind die Probleme auf einem PC auf defekten Arbeitsspeicher zurückzuführen. In Windows Server 2008 wurde daher ein spezielles Diagnoseprogramm integriert, welches den Arbeitsspeicher ausführlich auf Fehler überprüft. Sie können das Tool über *Start/Ausführen/mdsched* starten (Abbildung 18.21). Das Tool steht auch in der Programmgruppe *Verwaltung* zur Verfügung und – wenn Sie den Server mit der 2008-DVD starten – über die *Computerreparaturoptionen*.

Abbildg. 18.21 Diagnose des Arbeitsspeichers in Windows Vista



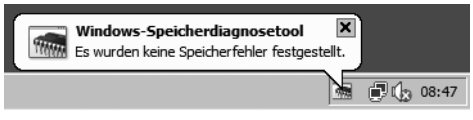
Sie können entweder den Server sofort neu starten und eine Diagnose durchführen, oder festlegen, dass die Diagnose erst beim nächsten Systemstart durchgeführt werden soll. Während der Speicherdiagnose prüft das Programm, ob der eingebaute Arbeitsspeicher Fehler aufweist, was eine häufige Ursache für ungeklärte Abstürze ist.

Abbildg. 18.22 Diagnose des Arbeitsspeichers in Windows Server 2008



Nachdem der Test abgeschlossen ist, startet der Server automatisch neu und meldet das Ergebnis über ein Symbol im Infobereich der Taskleiste (Abbildung 18.23). Sie müssen daher nicht warten, bis der Test abgeschlossen ist, damit der Server wieder zur Verfügung steht.

Abbildg. 18.23 Ausgabe des Ergebnisses der Speicherdiagnose in Windows Server 2008



Mehr zu dieser Diagnose und weitere Möglichkeiten finden Sie in Kapitel 21.

Die Systemkonfiguration

In der *Systemkonfiguration* können sie verschiedene Einstellungen am System vornehmen und überprüfen. Die Systemkonfiguration starten Sie am besten über *Start/Ausführen/msconfig* (Abbildung 18.24). Nach dem Start des Programms stehen Ihnen fünf Registerkarten zur Verfügung, über die Sie Systemeinstellungen vornehmen können:

Auf der Registerkarte *Allgemein* legen Sie fest, wie Windows Server 2008 standardmäßig starten soll. Hier können Sie festlegen, in welchem Modus das System geladen werden soll:

- **Normaler Systemstart** Startet Windows ganz normal
- **Diagnosesystemstart** Startet Windows nur mit den grundlegenden Diensten und Treibern
- **Benutzerdefinierter Systemstart** Startet Windows mit den grundlegenden Diensten und Treibern sowie anderen von Ihnen ausgewählten Diensten und Autostartprogrammen

Über die Registerkarte *Start* können Sie das Startverhalten der Windows Vista-Standardinstallation konfigurieren, zum Beispiel die Zeitdauer, in der das Bootmenü angezeigt wird.

Abbildg. 18.24 Die Systemkonfiguration in Windows Server 2008

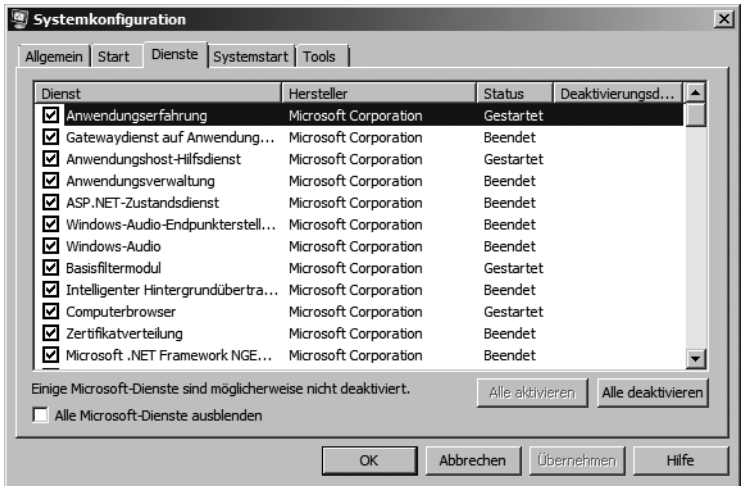
Hier legen Sie auch fest, welches Betriebssystem standardmäßig gestartet werden soll, wenn Sie den Starteintrag markieren und auf die Schaltfläche *Als Standard* klicken. Sie stellen hier auch die detaillierten Startoptionen des markierten Betriebssystems ein. Diese Optionen werden über den Bereich *Startoptionen* konfiguriert:

- **Abgesicherter Start: Minimal** Startet mit der grafischen Benutzeroberfläche von Windows im abgesicherten Modus, wobei nur die wichtigen Systemdienste ausgeführt werden. Das Netzwerk ist deaktiviert.
- **Abgesicherter Start: Alternative Shell** Startet mit der Windows-Eingabeaufforderung im abgesicherten Modus, wobei nur die wichtigen Systemdienste ausgeführt werden. Das Netzwerk und die grafische Benutzeroberfläche sind deaktiviert.
- **Abgesicherter Start: Active Directory-Reparatur** Startet mit der grafischen Benutzeroberfläche von Windows im abgesicherten Modus, wobei nur die wichtigen Systemdienste und das Active Directory ausgeführt werden.
- **Abgesicherter Start: Netzwerk** Startet mit der grafischen Benutzeroberfläche von Windows im abgesicherten Modus, wobei nur die wichtigen Systemdienste ausgeführt werden. Das Netzwerk ist aktiviert.

- **Kein GUI-Start** Beim Start wird kein Windows-Begrüßungsbildschirm angezeigt. Einige Programme oder Geräte zeigen beim Start Meldungen an, die sonst durch den Begrüßungsbildschirm verdeckt sind.
- **Startprotokollierung** Speichert alle Informationen über den Startvorgang in der Datei *%SystemRoot%Ntbtlog.txt*.
- **Basisvideo** Startet mit der grafischen Benutzeroberfläche von Windows im minimalen VGA-Modus. Dabei werden die standardmäßigen VGA-Treiber anstelle der spezifischen Grafiktreiber für die Grafikkarte des Computers geladen.
- **Betriebssystem-Startinformationen** Zeigt beim Laden der Treiber während des Startvorgangs die Treibernamen an.
- **Starteinstellungen sollen immer gelten** Wenn dieses Kontrollkästchen aktiviert ist, können Sie die Änderungen nicht durch die Auswahl von *Normaler Systemstart* auf der Registerkarte *Allgemein* rückgängig machen.

Auf der Registerkarte *Dienste* werden Ihnen alle installierten Systemdienste des Server angezeigt. Sie können hier einzelne Dienste markieren und diese auf einen Schlag deaktivieren. Hier können Sie auch die standardmäßigen Systemdienste von Microsoft ausblenden lassen, damit nur die zusätzlich installierten Dienste angezeigt werden. Wenn ein Server nicht mehr korrekt funktioniert, liegt es sehr häufig an fehlerhaft konfigurierten Systemdiensten. Sie können sich alle Dienste auch über *Start/Ausführen/services.msc* anzeigen lassen. Hier können Sie allerdings nicht nach Microsoft-Diensten filtern lassen, es werden immer alle Systemdienste angezeigt.

Abbildg. 18.25 Anzeigen und Verwalten der Systemdienste über die Systemkonfiguration



Auf der Registerkarte *Systemstart* werden Ihnen alle Programme angezeigt, die beim Starten von Windows automatisch gestartet werden. Sie können hier diese Programme auch deaktivieren. Haben Sie auf der Registerkarte *Allgemein* die Option *Benutzerdefinierter Systemstart* ausgewählt, müssen Sie entweder dort *Normaler Systemstart* auswählen oder das Kontrollkästchen des Systemstartelements aktivieren, um es beim Systemstart wieder zu starten.

Über die Registerkarte *Tools* können Sie verschiedene Aufgaben durchführen, die unterschiedliche Konfigurationsaufgaben haben. Sie können an dieser Stelle zum Beispiel die Benutzerkontensteuerung deaktivieren, die Windows-Version anzeigen lassen, usw. Die einzelnen Aufgaben sind gut erklärt. Um eine Maßnahme durchzuführen, markieren Sie diese und klicken dann auf die Schaltfläche *Starten*.

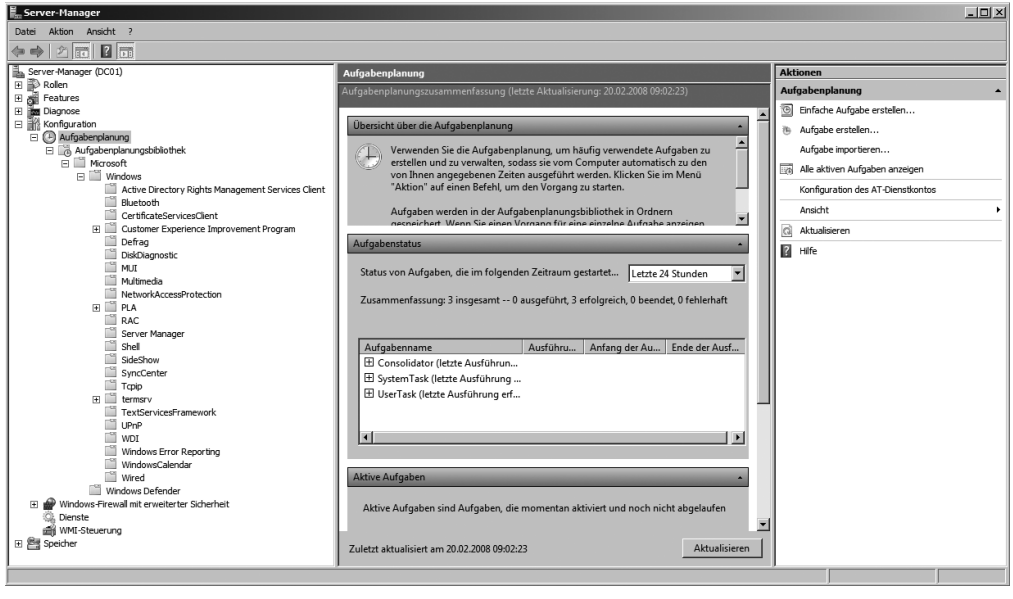
Systeminformation über die Befehlszeile *systeminfo.exe*

Mit dem Befehl *systeminfo* zeigen Sie alle Informationen Ihres Servers in der Befehlszeile an, darunter finden sich Infos über Hotfixes, Netzwerkkarten, Prozessor, Betriebssystem, Hersteller, usw. – sogar die aktuelle Systembetriebszeit (also wie lange der Rechner bereits läuft) und das ursprüngliche Installationsdatum lässt sich anzeigen. Hier empfiehlt sich die Umleitung in eine Textdatei, wobei Sie zusätzlich den Parameter */FO list* angeben sollten, um die Infos formatiert zu speichern. Um alle Infos in die Textdatei *C:\sysinfo.txt* zu speichern, müssen Sie den Befehl *systeminfo /FO list > C:\sysinfo.txt* verwenden

Neue Aufgabenplanung

Die Aufgabenplanung hatte in Windows Server 2003 noch die Bezeichnung *Geplante Tasks*. Mit Hilfe der Aufgabenplanung können Sie wiederkehrende Aufgaben, wie zum Beispiel die Datensicherung, Defragmentierung oder sonstige Tätigkeiten zu bestimmten Zeiten automatisch durchführen lassen. Die Aufgabenplanung wird durch einen eigenen Konsoleneintrag im Server-Manager über den Knoten *Konfiguration* verwaltet. Sie können die Aufgabenplanung auch über *Start/Verwaltung/Aufgabenplanung* starten, oder auch über *Start/Ausführen/taskschd.msc*. Das Hauptfenster der Aufgabenplanung ist in drei Bereiche untergliedert. Sie können die einzelnen Bereiche ausblenden, indem Sie mit der Maus auf den entsprechenden Balken klicken.

Abbildg. 18.26 Aufgabenplanung in Windows Server 2008

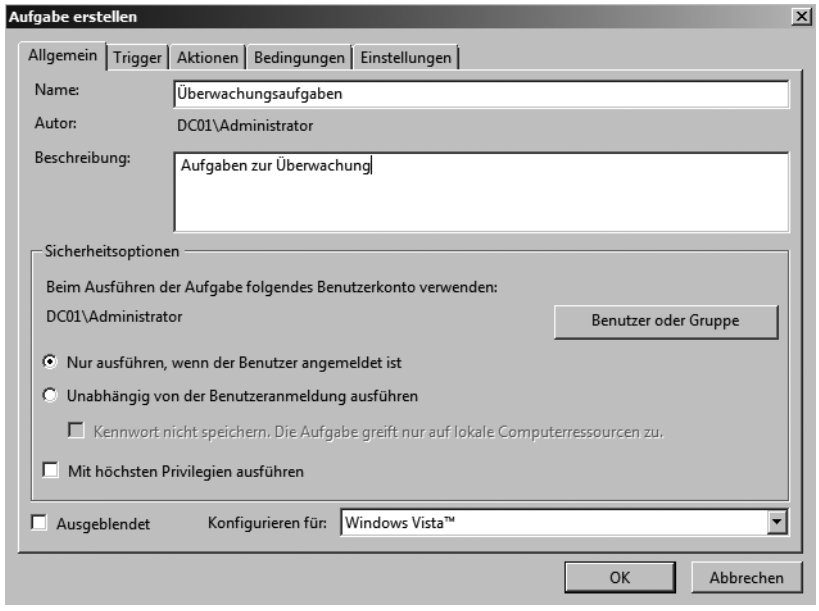


TIPP Über den *Aktionen*-Bereich kann nach einem Klick auf den Link *Konfiguration des AT-Dienstkontos* das Benutzerkonto ausgewählt werden, mit dem die Aufgaben durchgeführt werden sollen.

- **Übersicht über die Aufgabenplanung** Hier wird ein kurzer Hilfetext angezeigt, der die Möglichkeiten des Aufgabenplaners erläutert. Da dieser Text sich nicht dynamisch ändert, können Sie diesen Bereich normalerweise ausblenden.
- **Aufgabenstatus** Dieser Bereich zeigt alle Aufgaben an, die auch von Windows Server 2008 intern durchgeführt werden. Sie können einzelne Aufgaben anzeigen lassen und erkennen, wann diese ausgeführt wurden.
- **Aktive Aufgaben** Hier werden alle Aufgaben angezeigt, die zwar aktiv, aber noch nicht durchgeführt sind. Hier können Sie durch Doppelklick auf die einzelnen Aufgaben deren Konfiguration überprüfen und abändern. Hier werden auch einige Systemaufgaben angezeigt. Damit Sie die Einstellungen der Aufgabe ändern können, zum Beispiel den Zeitpunkt des Starts, können Sie im neuen Fenster, in dem die Konfiguration der Aufgabe angezeigt wird, doppelt auf die Aufgabe klicken. Es öffnet sich ein weiteres Fenster, über das Sie die Einstellungen anpassen können.

Die Einheit für Vorgänge in der Aufgabenplanung ist eine *Aufgabe*. Eine solche Aufgabe besteht aus verschiedenen Startbedingungen, einschließlich Triggern, Bedingungen und Einstellungen sowie eine oder mehrere Aktionen genannte Ausführungsvorgänge. *Trigger* sind Kriteriensätze, bei deren Erfüllung eine Aufgabe ausgeführt wird. Sie können zeit- oder ereignisabhängig sein, und es können Parameter wie Startzeitpunkte und Wiederholungskriterien angegeben werden. Mit *Bedingungen* können Sie Aufgaben so einschränken, dass sie nur ausgeführt werden, wenn sich der Computer in einem bestimmten Zustand befindet. Eine Aufgabe wird nur ausgeführt, wenn ein *Trigger* erfüllt ist und alle für die Aufgabe definierten *Bedingungen* wahr sind. Beispielsweise können Sie mithilfe von Bedingungen erreichen, dass ein Programm beim Eintreten eines Ereignisses nur gestartet wird, wenn das Netzwerk verfügbar ist, oder dass eine Aktion zu einem bestimmten Zeitpunkt nur gestartet wird, wenn der Computer im Leerlauf ist. Mit *Einstellungen* können Sie Ausführungsoptionen festlegen. Dadurch können Sie beispielsweise angeben, wie häufig eine fehlschlagende Aktion wiederholt werden soll. *Aktionen* sind die auszuführenden Befehle, wenn die *Trigger* und *Bedingungen* erfüllt sind. Mit einer *Aktion* können Sie beispielsweise ein Programm starten oder eine E-Mail senden. Haben Sie eine Aufgabe aufgerufen, sehen Sie auf der rechten Seite der Managementkonsole, welche speziellen Aufgaben Sie durchführen können (Abbildung 18.27). Sie können zum Beispiel eine Aufgabe exportieren, um diese auf einem anderen Windows Server 2008-Rechner zu importieren. Sie können Aufgaben deaktivieren, löschen oder sofort starten lassen.

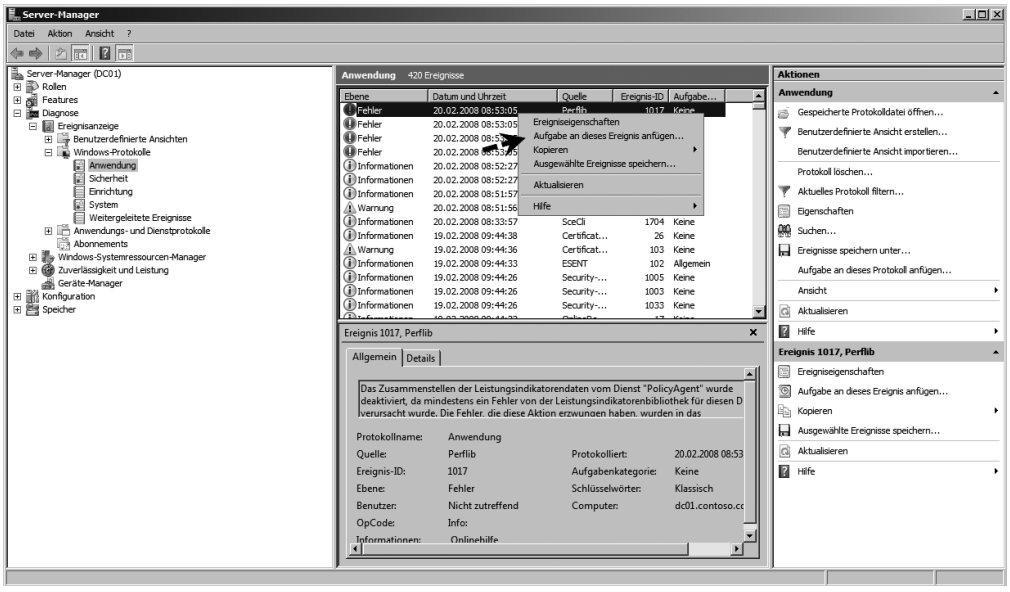
Abbildg. 18.27 Erstellen einer Aufgabe in Windows Server 2008



Neuerungen der Aufgabenplanung

Eine der leistungsstärksten neuen Funktionen der Aufgabenplanung bietet die Möglichkeit zum Auslösen einer Aufgabe durch ein beliebiges, im Ereignisprotokoll aufgezeichnetes Ereignis. Mithilfe dieser neuen Funktion können Administratoren beim Auftreten eines bestimmten Ereignisses automatisch eine E-Mail versenden oder ein Programm starten. In Windows Server 2008 können Sie Aufgaben, die abhängig vom Auftreten von Ereignissen gestartet werden sollen, sehr einfach mit dem neuen Aufgabenplanungs-Assistenten einrichten. Ein Administrator kann in der Ereignisanzeige einfach das als Trigger zu verwendende Ereignis auswählen und mit nur einem Klick den Aufgabenplanungs-Assistenten starten, um die Aufgabe einzurichten. Durch die nahtlose Integration der Aufgabenplanungs-Benutzeroberfläche in die Ereignisanzeige können Sie eine durch ein Ereignis ausgelöste Aufgabe mit nur fünf Mausklicks erstellen. Klicken Sie das Ereignis mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Aufgabe an dieses Ereignis anfügen* (Abbildung 18.28).

Abbildg. 18.28 Aufgaben basierend auf Ereignissen erstellen



Über Ereignisse hinaus unterstützt die Aufgabenplanung von Windows Server 2008 auch weitere neue Triggertypen, beispielsweise Trigger, die Aufgaben starten, wenn der Computer startet, sich ein Benutzer anmeldet oder sich der Computer im Leerlauf befindet. Mithilfe weiterer zusätzlicher Trigger können Administratoren Aufgaben einrichten, die abhängig vom Sitzungsstatus gestartet werden, zum Beispiel beim Herstellen oder Trennen einer Verbindung mit einem Terminalserver oder beim Sperren und Entsperren einer Arbeitsstation. Mit der Aufgabenplanung können Sie Aufgaben weiterhin abhängig von Datum und Uhrzeit auslösen. Er stellt eine einfache Verwaltung von geplanten regelmäßigen Aufgaben zur Verfügung. Es können Trigger genauer angepasst und so detaillierter festgelegt werden, wann Aufgaben gestartet und wie häufig sie ausgeführt werden sollen. Ein Administrator kann einem Trigger eine Verzögerung hinzufügen oder eine Aufgabe einrichten, die nach dem Auftreten des Triggers in regelmäßigen Intervallen wiederholt wird. Für jede Aufgabe können mehrere Bedingungen definiert werden. Durch Bedingungen können Sie Aufgaben so einschränken, dass sie nur ausgeführt werden, wenn sich der Computer in einem bestimmten Zustand befindet. Vor Windows Server 2008 wurde jede Aufgabe abhängig von einem einzelnen Trigger (normalerweise der Zeit) gestartet und eine bestimmte Aufgabe konnte nur aus einer Aktion bestehen. Die Aufgabenplanung von Windows Server 2008 ist beim Verknüpfen von Triggern und Aktionen wesentlich flexibler. In Windows Server 2008 können mit einer bestimmten Aufgabe mehrere Trigger verbunden werden. Beispielsweise gilt eine bestimmte Fehlerbedingung möglicherweise nur beim Auftreten von drei verschiedenen Ereignissen als erfüllt. Sie können einfach eine Aufgabe definieren, die nur dann gestartet wird, wenn alle drei Ereignisse auftreten. Für Aufgaben können nicht nur mehrere Trigger erforderlich sein, mit einer einzelnen Aufgabe können auch mehrere Aktionen gestartet werden.

Mit der neuen Aufgabenplanung müssen Sie beim aufeinander folgenden Ausführen von Aufgaben keine Vermutungen mehr anstellen. Sie müssen beispielsweise immer nachts um 1:00 Uhr einen bestimmten Batchprozess ausführen und nach dessen Abschluss die Ergebnisse des Prozesses drucken. Vor Windows Server 2008 waren zum Automatisieren dieses Prozesses zwei Aufgaben erfor-

derlich: eine um 1:00 Uhr gestartete Aufgabe zum Ausführen der Batchdatei und eine zweite Aufgabe zum Drucken der Ergebnisse. Sie mussten die Dauer zur Ausführung des Batchprozesses schätzen und die Druckaufgabe so einrichten, dass sie nach einem angemessenen Zeitraum gestartet wird. Wenn der Batchprozess beim Starten des Druckprozesses noch nicht abgeschlossen war (oder sogar fehlschlug) wurden die Ergebnisse nicht gedruckt.

Mit Windows Server 2008 ist dieses Szenario einfach zu verwalten. Eine einzelne Aufgabe kann definiert werden, mit dem der Batchprozess um 1:00 Uhr ausgeführt wird und nach dessen Abschluss die Ergebnisse gedruckt werden. Die Aufgabenplanung stellt die Ausführung von Aufgaben auch dann sicher, wenn sich ein Computer zum geplanten Zeitpunkt im Standbymodus befindet. Durch diese neue Funktionalität, durch die die Aufgabenplanung einen Computer zum Ausführen einer Aufgabe aus dem Standbymodus oder Ruhezustand reaktivieren kann, können Sie die Vorteile der verbesserten Stromsparmodi von Windows Server 2008 nutzen, ohne darauf achten zu müssen, ob wichtige Aufgaben pünktlich ausgeführt werden. Neben dem Reaktivieren eines Computers zum Ausführen einer Aufgabe können Sie nun durch eine Option festlegen, dass eine Aufgabe ausgeführt wird, sobald der Computer verfügbar ist. Aktivieren Sie diese Option und wurde der geplante Ausführungszeitpunkt einer Aufgabe nicht eingehalten, wird die Aufgabe beim nächsten Einschalten des Computers von der Aufgabenplanung ausgeführt.

Erstellen einer neuen Aufgabe

Um eine manuelle Aufgabe zu erstellen, stehen Ihnen drei Möglichkeiten zur Verfügung. Nachdem Sie die Aufgabenplanung gestartet haben, werden auf der rechten Seite die Aktionen angezeigt, die Sie durchführen können. Um eine neue Aufgabe zu erstellen, gibt es drei Möglichkeiten:

- **Einfache Aufgaben erstellen** Mit Hilfe dieser Aktion wird ein Assistent gestartet, der Sie bei der Erstellung einer neuen Aufgabe unterstützt.
- **Aufgabe erstellen** Wählen Sie diese Aktion aus, öffnet sich ein Aufgabenfenster, in dem Sie auf verschiedenen Registerkarten ohne Unterstützung von Assistenten die Aufgabe konfigurieren können.
- **Aufgabe importieren** Mit dieser Option können Sie Aufgaben importieren, die Sie vorher auf dem gleichen Server oder einem anderen Server exportiert haben.

Zusatztools für die Systemüberwachung

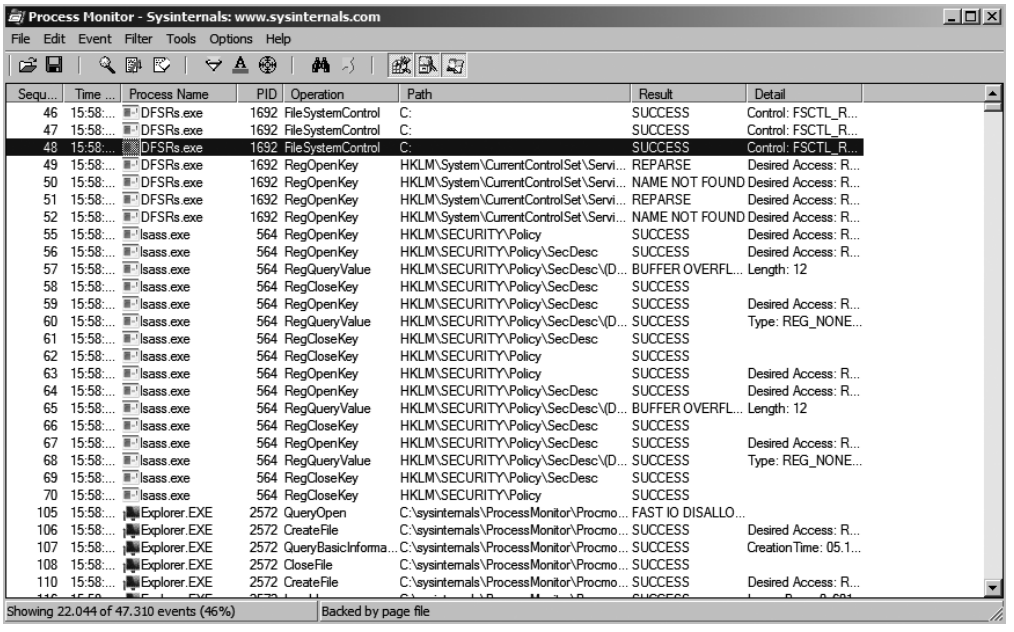
In diesem Abschnitt zeigen wir Ihnen Tools, die Ihnen dabei helfen, die laufenden Prozesse oder Dienste auf einem Server besser zu überwachen oder zu konfigurieren. Die Tools können Sie im Microsoft TechNet von der Sysinternals-Seite *www.sysinternals.com* herunterladen.

Process Monitor

Mit diesem Programm werden in einer grafischen Oberfläche, ausführlich in Echtzeit alle Aktivitäten im Dateisystem, der Registry und der Prozesse/Threads angezeigt. Das Tool vereint zwei Standardprogramme von Sysinternals *Filemon* und *Regmon*. Über Schaltflächen werden die einzelnen Überwachungsfunktionen durch einen Klick aktiviert und deaktiviert. Dadurch kann die Überwachung

der Registry-, und der Dateisystemzugriffe, sowie die Abfrage der Prozessaktivität gesteuert werden. Abhängig von den überwachten Aktivitäten, werden mehr oder weniger Informationen im Fenster angezeigt. Das Programm ist voll transportfähig (zum Beispiel auf USB-Sticks) und muss nicht installiert werden. Der Download ist wenige Kilobyte groß.

Abbildg. 18.29 Der Process Monitor bietet eine effiziente Überwachung der Registry- und Dateizugriffe eines Computers in Echtzeit an



Sequ...	Time ...	Process Name	PID	Operation	Path	Result	Detail
46	15:58:...	DFSRs.exe	1692	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
47	15:58:...	DFSRs.exe	1692	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
48	15:58:...	DFSRs.exe	1692	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
49	15:58:...	DFSRs.exe	1692	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	REPARSE	Desired Access: R...
50	15:58:...	DFSRs.exe	1692	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	NAME NOT FOUND	Desired Access: R...
51	15:58:...	DFSRs.exe	1692	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	REPARSE	Desired Access: R...
52	15:58:...	DFSRs.exe	1692	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	NAME NOT FOUND	Desired Access: R...
55	15:58:...	lsass.exe	564	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: R...
56	15:58:...	lsass.exe	564	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
57	15:58:...	lsass.exe	564	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	BUFFER OVERFL...	Length: 12
58	15:58:...	lsass.exe	564	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
59	15:58:...	lsass.exe	564	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
60	15:58:...	lsass.exe	564	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	SUCCESS	Type: REG_NONE...
61	15:58:...	lsass.exe	564	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
62	15:58:...	lsass.exe	564	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
63	15:58:...	lsass.exe	564	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: R...
64	15:58:...	lsass.exe	564	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
65	15:58:...	lsass.exe	564	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	BUFFER OVERFL...	Length: 12
66	15:58:...	lsass.exe	564	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
67	15:58:...	lsass.exe	564	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
68	15:58:...	lsass.exe	564	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	SUCCESS	Type: REG_NONE...
69	15:58:...	lsass.exe	564	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
70	15:58:...	lsass.exe	564	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
105	15:58:...	Explorer.EXE	2572	QueryOpen	C:\sysinternals\ProcessMonitor\Procmo...	FAST IO DISALLO...	
106	15:58:...	Explorer.EXE	2572	CreateFile	C:\sysinternals\ProcessMonitor\Procmo...	SUCCESS	Desired Access: R...
107	15:58:...	Explorer.EXE	2572	QueryBasicInforma...	C:\sysinternals\ProcessMonitor\Procmo...	SUCCESS	CreationTime: 05.1...
108	15:58:...	Explorer.EXE	2572	CloseFile	C:\sysinternals\ProcessMonitor\Procmo...	SUCCESS	
110	15:58:...	Explorer.EXE	2572	CreateFile	C:\sysinternals\ProcessMonitor\Procmo...	SUCCESS	Desired Access: R...

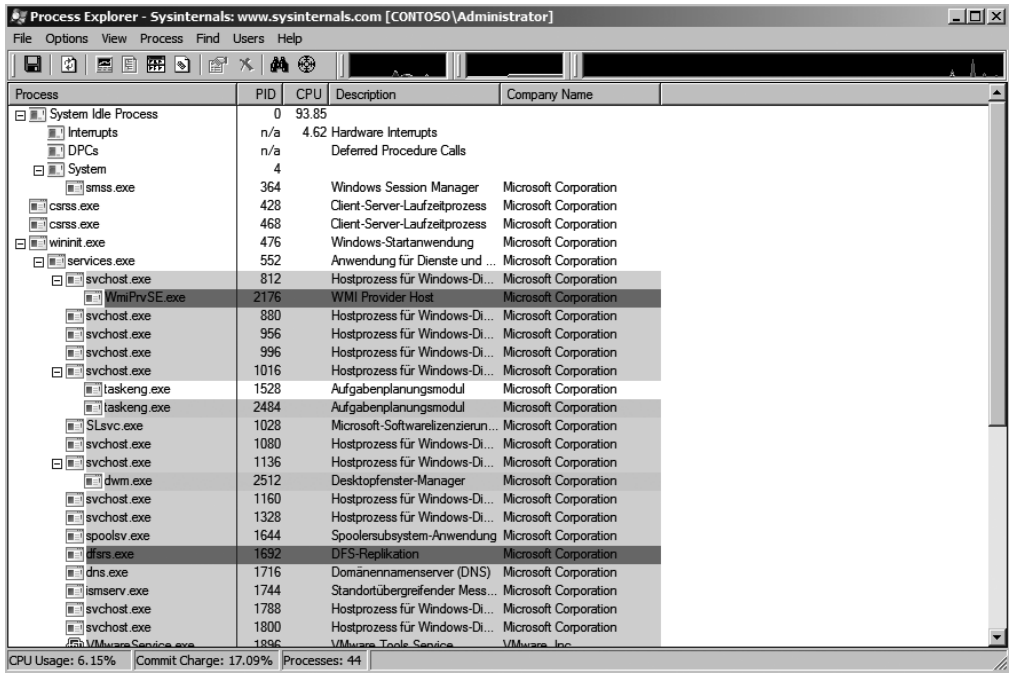
Den Systembremsen auf der Spur – Autoruns

Mit diesem Tool, welches zu den mächtigsten von Sysinternals gehört, um Viren und Trojaner zu finden, können in einer grafischen Oberfläche auf einen Blick alle Programme angezeigt werden, die automatisch auf dem Server mit Windows gestartet werden. Einträge können direkt aus dem Tool heraus gelöscht werden. In Windows gibt es zahlreiche Möglichkeiten, um Applikationen automatisiert zu starten. Mit dem Tool *Autoruns* steht Ihnen eine zentrale Verwaltungsstelle für diese Programme zur Verfügung. Auf mehreren Registerkarten wird angezeigt, welche Programme automatisch an welcher Stelle gestartet werden. Auf der Registerkarte *Everything* werden alle Autostart-Programme des Computers angezeigt. Vor allem erfahrene Benutzer können mit diesem Programm einen Server schnell säubern, ohne an verschiedenen Stellen im System manipulieren zu müssen. Neben der grafischen Oberfläche, die über *autoruns.exe* gestartet werden kann, bietet das Tool auch eine Befehlszeilenerweiterung, die über *autorunsc.exe* gestartet wird.

Der Super-Task Manager – Process Explorer

Der Process Explorer (ehemals HandleEX) zeigt sehr übersichtlich alle Prozesse in einem Fenster und darunter weitere Informationen zum aktuellen Prozess, wie zum Beispiel den aktuellen Zugriff auf Verzeichnisse. Im DLL-View-Mode werden die benutzten Librarys und deren Herkunft angegeben. Das *Process*-Menü beinhaltet den Eintrag *Restart*, der einen Prozess zunächst killt und danach neu startet. Individuelle Threads können zeitweilig außer Kraft gesetzt werden. Der Process Explorer ist im Prinzip ein aufgewerteter Windows Task-Manager. Er zeigt die laufenden Prozesse in einem Verzeichnisbaum, so dass Sie immer wissen, zu welcher Anwendung der Task gehört. Unterschiedliche Prozesse können in verschiedenen Farben markiert werden. Zusätzlich bindet sich der Process Explorer noch in die Taskleiste ein, sodass auf einen Blick die aktuelle CPU-Last und die Festplattennutzung angezeigt werden kann. Auch dieses Programm muss nicht installiert werden, sondern kann direkt über die **.exe*-Datei aufgerufen werden. Das Programm enthält eine ausführliche Hilfe zum Umgang mit dem Tool.

Abbildg. 18.30 Mit dem Process Explorer werden die laufenden Prozesse auf einem Server effizient überwacht.



Befehle über das Netzwerk ausführen *PSExec*

Dieses Tool ist Bestandteil der PSTools von Sysinternals. Auch hierbei handelt es sich um ein Befehlszeilen-Programm, welches ohne Installation verwendet werden kann. Das Tool ermöglicht es, auf dem eigenen Computer oder remote auf einem anderen Computer unter einem anderen Benutzerkonto ein Programm oder eine Routine zu starten. Die Syntax von *psexec.exe* mit den wichtigsten Parametern lautet:

psexec.exe \\<Remotecomputer> –u <Benutzername> –p <Kennwort> <Programm>.

Prozesse anzeigen und killen – *PSList* und *PSKill*

PSList arbeitet eng mit *PSKill* zusammen. Wird *PSList* ohne Optionen aufgerufen, werden viele Informationen über die aktiven Prozesse in der Befehlszeile anzeigt. Dabei werden standardmäßig neben der Prozess-ID (PID) von links nach rechts die Prioritätsklasse, die Anzahl der Threats, die Anzahl der Handles, der Menge der verbrauchten CPU-Zeit und die Zeit, die dieser Prozess schon aktiv ist, in der Konsole angezeigt. Dieses Programm braucht nicht unter einem Administratorkonto zu laufen, sondern kann auch ohne diese Berechtigung alle Informationen anzeigen. Soll es auf einem entfernten System zum Einsatz kommen, auf dem das aktuelle Konto nicht existiert, so ist es möglich, das Tool mittels der Optionen *–u* und *–p*, mit einer alternativen Benutzeranmeldung zu starten. Mit den drei Optionen *–m* , *–d* und *–x* kann das Programm veranlasst werden, differenzierte Ausgaben auf den Bildschirm zu bringen. Die Option *–m* dient dazu, weitergehende Informationen über den Umgang des Programms mit virtuellem und physischem Speicher zu erhalten.

Neben dem Gesamtverbrauch an virtuellem Speicher, den ein Prozess für sich reserviert, werden hierbei unter anderem auch Spitzen im Verbrauch angezeigt. Da Programme, die ein Memory Leak haben, grundsätzlich das Problem besitzen, dass sie *Private Virtual Memory* für sich reservieren aber anschließend nicht wieder freigeben, können sie erheblich dazu beitragen, ein System langsam zu machen. Solche Prozesse haben in der Regel einen stetig steigenden Bedarf an privatem virtuellen Speicher und der Spitzenwert solcher Prozesse entspricht in diesem Bereich dann auch fast immer dem augenblicklichen Wert. Der Task-Manager zeigt als Speicherverbrauch nur den physischen Speicher an, den ein Prozess verbraucht – nicht den virtuellen privaten Speicher. Auf diese Weise ist es ohne einem Hilfsprogramm wie *PsList* nur schwer möglich, einen solchen Prozess mit einem Memory Leak im System auszumachen.

Die Option *–d* zeigt Details über die Threats auf, die von einem Prozess verwendet werden. Mit der Option *–x* ist es möglich, die Detailinformationen zum Prozess, dem Speicherverbrauch und den Threats gemeinsam auszugeben. Eine weitere Option ist *–t*, der eine baumartige Prozess-Struktur ausgibt. Dabei sind alle Prozesse zu sehen, die von einem anderen Prozess gestartet wurden. Durch diese Ansicht ist es einfacher zu erkennen, welche Aufgaben ein Prozess im System hat. Wird nur *–s* ohne weitere Optionen verwendet, zeigt das Tool die Prozesse sortiert nach der verbrauchten CPU-Zeit an. Wollen Sie zum Beispiel nicht die Prozesse beobachten, sondern eine Aufstellung über den CPU-Gebrauch erhalten, geben Sie *–s* gefolgt vom Wert 2 ein. Dieser Wert gibt die Anzahl der Sekunden an, die das Tool läuft, bevor es abbricht. Ein beispielhafter Aufruf für ein Remotesystem könnte dann folgendermaßen aussehen: *pslist \<Computer> –s 2*. Die zwei Sekunden geben dem Tool genügend Zeit, um den CPU-Gebrauch zu berechnen.

Wie *PSExec* ist auch *PSKill* ein Befehlszeilenprogramm. Mit diesem Programm können Prozesse in der Befehlszeile auf dem lokalen Computer oder auf einem Computer im Netzwerk beendet werden. Die Syntax lautet:

pskill [–] [–t] [\\<Computer> [–u <Benutzername>] [–p <Kennwort]] <Prozessname oder PID>

Die Option *–t* killt den spezifizierten Prozess und alle von diesem Prozess abhängigen Prozesse. *PSKill* muss von einem Account benutzt werden, der Administratorrechte besitzt.

Systemdienste im Griff – *PSService*

Mit *PSService* können Systemdienste lokal oder auf Computern im Netzwerk angezeigt, beendet und gestartet werden. Die Syntax des Programms ist:

psservice [\\<Computer> [–u <Benutzername>] [–p <Kennwort>]] <Befehl> <Option>

- **query** Zeigt den Status eines Dienstes an
- **config** Zeigt die Einstellungen eines Dienstes an
- **setconfig** Setzt den Starttyp des Dienstes um
- **start** Startet einen Dienst
- **stop** Beendet einen Dienst
- **restart** Startet einen Dienst neu
- **pause** Hält einen Dienst an
- **cont** Führt einen Dienst weiter aus, nachdem er angehalten worden ist
- **depend** Zeigt die von diesem Dienst abhängigen Dienste an
- **security** Gibt die Sicherheitsinformationen für den Dienst aus
- **find** Unterstützt beim Suchen eines Dienstes

Sysinternals-Sicherheits-Tools

Die Sicherheit spielt in Unternehmen eine immer wichtigere Rolle. Um die Sicherheit von Servern und Arbeitsstationen sicherzustellen, bieten die Sysinternals-Tools zahlreiche Möglichkeiten. In diesem Abschnitt widmen wir uns den Sicherheits-Tools dieser Sammlung und geben Tipps für den Einsatz.

Anmeldungen in der Domäne überwachen *LogonSessions*

Mit diesem Befehlszeilenprogramm werden alle angemeldeten Sitzungen auf einem Computer angezeigt. Geben Sie den Befehl ohne Optionen ein, reicht unter Umständen der Puffer der Eingabeaufforderung nicht aus, da zu viele Informationen angezeigt werden. Verwenden Sie in diesem Fall die Option *logonsessions | more* oder vergrößern Sie den Puffer der Eingabeaufforderung in deren Eigenschaften. Alternativ lassen Sie die Ausgabe über die Option > *logon.txt* in eine Datei umleiten. Mit Hilfe dieses Programm erhalten Sie sehr schnell ausführliche Informationen, welche Sitzungen gerade auf dem Computer geöffnet sind. Verwenden Sie zusätzlich noch die Option *–p*, werden auch die geöffneten Prozesse der einzelnen Sitzungen und damit der angemeldeten Benutzer angezeigt. So kann effizient überwacht werden, wer auf einem Server, zum Beispiel Terminalserver, angemeldet ist und mit welchen Applikationen der Anwender arbeitet. Neben den angemeldeten Benutzern werden auch die Systemkonten angezeigt. Neben Terminalservern ist das Tool auch hervorragend in Active Directory-Umgebungen einsetzbar.

Neue SID erstellen – *NewSID*

Jedem Objekt in einer Active Directory-Domäne oder auch auf einem allein stehenden Computer wird ein Security Identifier (SID) zugeordnet. Wird ein System geklont, hat der geklonte Computer die gleiche SID wie das Quell-System, was in Domänen zu einigen Problemen führen kann. Vor allem bei der Bereitstellung von neuen Computern im Netzwerk kommt dieser Fall oft vor, wenn nicht korrekt vorgegangen wird. Das Tool *NewSID* erstellt neue SIDs bei diesen geklonten Systemen. Sie können das Tool so aufrufen, dass gleichzeitig eine neue SID zugewiesen und automatisch der Name des Computers geändert wird. Verwenden Sie dazu die Syntax *newsid /a <Neuer Name>*. Der Umgang mit dem Tool ist extrem einfach, eine Installation nicht notwendig. Das Tool kann auch hervorragend in Batchdateien eingesetzt werden, um geklonte Arbeitsstationen für die Bereitstel-

lung vorzubereiten. Wird ein Computer vor dem Klonvorgang aber mit dem Tool Sysprep vorbereitet, muss keine neue SID erstellt werden, da dies bei der Aufnahme in die Domäne automatisch erfolgt.

Lokale Anmeldungen überwachen *PsLoggedOn*

Wie *LogonSessions* dient *PSLoggedOn* der Überwachung von angemeldeten Benutzern. Dieses Tool ist Bestandteil der PSTools-Sammlung. Geben Sie den Befehl *PSLoggedOn* in der Befehlszeile ein, werden alle angemeldeten Benutzer mit den Anmeldezeiten am lokalen System angezeigt. Hier sehen Sie auch, welche Benutzer über eine Freigabe auf den Server zugreifen. Sie können das Tool auch so aufrufen, dass Sie einen Benutzernamen angeben. In diesem Fall untersucht das Tool alle Computer in der Netzwerkumgebung und zeigt an, wo der Benutzer angemeldet ist. Die Syntax lautet:

psloggedon [–] [–l] [–x] [\\<Computername> | <Benutzername>]. Die Option *–l* zeigt nur die lokal angemeldeten Benutzer, *–x* zeigt keine Anmeldezeiten an. Vor allem bei der Untersuchung von unberechtigten Zugriffen im Netzwerk wird dieses Tool oft verwendet, um festzustellen, auf welchen Computern ein bestimmter Benutzer angemeldet ist.

Ereignisanzeigen sammeln – *PSLoglist*

Mit *PSLoglist* aus der PSTools-Sammlung können über die Befehlszeile die Ereignisanzeigen verschiedener Computer eingesammelt, angezeigt und verglichen werden. Wenn Sie das Tool ohne Optionen aufrufen, werden alle Einträge des lokalen System-Ereignisprotokolls angezeigt. Das Programm hat darüber hinaus zahlreiche Optionen, welche beim Abfragen der Ereignisanzeigen viele verschiedene Vergleichsmöglichkeiten bieten:

psloglist [–] [\\<Computer>[,<Computer>[,...] | @<Datei> [–u <Benutzername>[–p <Kennwort>]]] [–s [–t delimiter]] [–m #|–n #|–h #|–d #|–w][–c][–x][–r][–a mm/dd/yy][–b mm/dd/yy][–f filter] [–i ID[,ID[,...] | –e ID[,ID[,...]]] [–o event source[,event source][,..]]] [–q event source[,event source][,..]]] [–l event log file] <eventlog>

- **@<Datei>** Führt den Befehl auf allen Computern aus, die in der Datei aufgelistet sind. Jeder Computer muss dazu in einer eigenen Spalte in der Textdatei stehen. Die entsprechenden Ereignisse der Computer werden hierüber also gesammelt.
- **–a** Zeigt die Einträge nach dem genannten Datum an. Als Format wird *dd/mm/yy* verwendet.
- **–b** Zeigt die Einträge vor dem genannten Datum an
- **–c** Löscht die entsprechenden Ereignisanzeigen nach der Anzeige über *PSLogList*. Dies ist zum Beispiel bei der Abfrage über eine Batchdatei sinnvoll.
- **–d** Zeigt nur die Einträge der letzten *n* Tage an. Dabei werden die letzten Tage als <*n*> hinter der Option mit angegeben.
- **–e** Filtert Einträge mit definierten IDs aus. Die Syntax entspricht der Option *–i* weiter unten.
- **–f** Filtert Ereignisse mit bestimmten Typen aus (*–f w* filtert Warnungen). Es können beliebige Buchstaben verwendet werden. Es werden nur Ereignisse, die mit den entsprechenden Buchstaben anfangen, angezeigt.
- **–h** Zeigt nur Einträge der letzten *n* Stunden. Die Syntax entspricht der Option *–d* weiter oben.
- **–i** Zeigt nur Einträge mit den definierten IDs. Es können auch mehrere IDs kommagetrennt angezeigt werden.
- **–l** Speichert Einträge der definierten Ereignisanzeige

- **–m** Zeigt nur Einträge der letzten *n* Minuten
- **–n** Zeigt nur die aktuellsten definierten Einträge an
- **–o** Zeigt nur die Einträge der spezifizierten Ereignisquelle (zum Beispiel *\–o cdrom*). Diese Option schließt in der Ausgabe also zusätzliche Informationen ein.
- **–p** Gibt das Kennwort für den konfigurierten Benutzer an. Geben Sie kein Kennwort ein, fragt das Tool notfalls nach. Dabei wird das Kennwort nicht in Klartext angezeigt oder über das Netzwerk geschickt.
- **–q** Zeigt die Einträge der spezifizierten Ereignisquelle nicht an (zum Beispiel *\–q cdrom\).* Benutzerdefinierte Einträge werden so von der Ausgabe ausgeschlossen. Sollen mehrere Quellen von der Ausgabe ausgeschlossen werden, müssen diese durch Komma voneinander getrennt werden.
- **–r** Speichert die Einträge aufsteigend ab
- **–s** Hier werden die Einträge kommabasiert angezeigt, um diese zum Beispiel in einer Excel-Tabelle oder SQL-Datenbank zu speichern. Nach der Auswertung kann zum Beispiel über den Befehl *start* die CSV-Datei sofort geöffnet und angezeigt werden.
- **–t** Definiert das Trennzeichen
- **–u** Legt den Benutzernamen fest, mit dem Sie auf die Server zugreifen
- **–w** Wartet auf neue Einträge und speichert diese, sobald diese in der Ereignisanzeige angezeigt werden. Das funktioniert aber nur für das lokale System.
- **–x** Speichert erweiterte Daten, die standardmäßig nicht angezeigt werden. Hierbei handelt es sich meistens um binäre Rohdaten.
- **Eventlog** Standardmäßig verwendet das Tool das System-Ereignisprotokoll. Sie können die Ereignisanzeige auswählen, wenn Sie die ersten Buchstaben oder die entsprechende Abkürzung angeben. Allerdings müssen auch auf deutschen Windows-Systemen die englischen Abkürzungen, also beispielsweise »sec« für »security«, eingegeben werden, wenn das Ereignisprotokoll »Sicherheit« geöffnet werden soll. Eine wichtige Funktion des Tools ist, dass das Programm in der Lage ist, direkt auf die Quell-DLLs auf den Remotesystemen zuzugreifen. Allerdings muss dazu auf dem entfernten System die administrative Freigabe (*Admin$*) aktiviert sein.

System Center Operations Manager 2007

Der neue Microsoft System Center Operations Manager (SCOM) 2007 ist der Nachfolger des Microsoft Operations Manager 2005. Mittlerweile steht auch das erste Service Pack der Server-Überwachungs-Lösung kurz vor der Fertigstellung. Das Produkt wird dadurch erweitert und die Stabilität erhöht. In diesem Abschnitt durchleuchten wir die Möglichkeiten von SCOM 2007. Dieser Server muss allerdings separat erworben werden und gehört nicht zum Lieferumfang von Windows Server 2008. Der kleine Bruder von SCOM 2007 sind die System Center Essentials (SCE) 2007, die aber nur maximal 30 Server überwachen können. SCOM 2007 ist mittlerweile nach dem MOM 2000 und 2005 das dritte Produkt in dieser Linie und wurde deutlich überarbeitet und erweitert. Mit SCOM 2007 werden jetzt auch die Arbeitsstationen im Unternehmen überwacht, um sicherzustellen, dass nicht nur die Server im Unternehmen funktionieren, sondern auch die Clientcomputer. Auch End-To-End-Überwachung, also die Erreichbarkeit spezieller Serverdienste wie Exchange-Postfach oder SQL-Datenbank auf dem Server für die Clients, ist jetzt möglich.

Aufgaben von System Center Operations Manager 2007

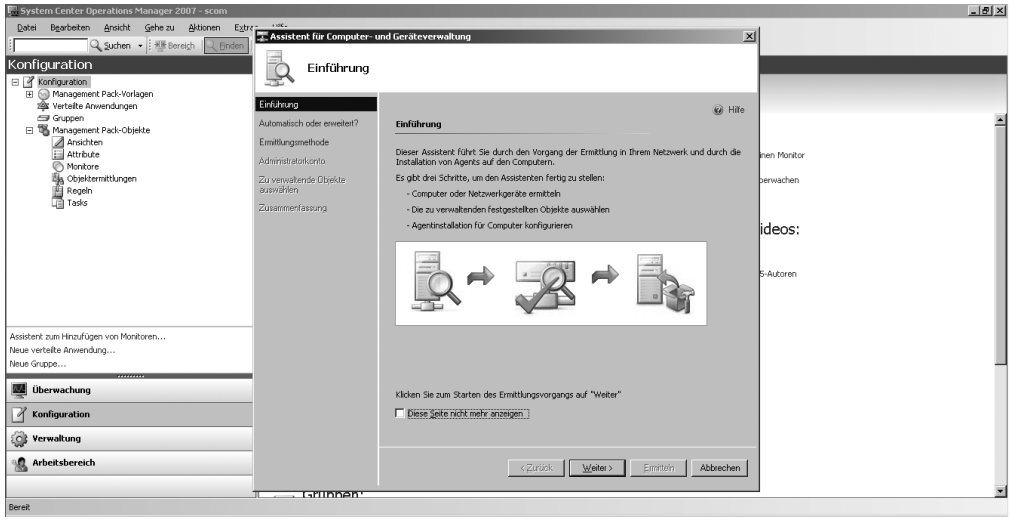
Das Produkt dient der Überwachung von Servern im Unternehmen. Die Administratoren bekommen auf einer grafischen Oberfläche den Status aller Server angezeigt und können sofort die Probleme lösen, wenn bestimmte Fehler auftauchen. Ohne eine automatisierte Überwachung fallen viele Fehler erst dann auf, wenn zum Beispiel die Benutzer keine Verbindung mehr mit einem Server aufbauen können. Die konsequente Überwachung ist einer der Bausteine, welche die Stabilität und Ausfallsicherheit eines Netzwerks gewährleisten und die Arbeitsfähigkeit der Anwender sicherstellt. SCOM verwaltet mit speziellen Agenten, die auf den zu überwachenden Servern installiert werden, die Funktionalität der einzelnen Serverdienste und stellt auch einen Überblick dar, wie diese angeordnet sind. So kann die aktuelle Exchange-Infrastruktur angezeigt und Fehler auf den einzelnen Servern sofort erkannt und behoben werden.

Im Gegensatz zur einfachen Überwachung der Netzwerkerreichbarkeit, CPU-Last und Arbeitsspeicherauslastung, geht SCOM deutlich weiter. Der Server überwacht bis ins Detail einzelne Serverdienste, deren Erreichbarkeit und die Funktionalität auch aus Sicht der Clients (End-To-End). Die Agenten auf den Servern sammeln die notwendigen Informationen und senden diese an den zentralen Management Server weiter. Hier werden diese Daten aufbereitet und den Administratoren zur Verfügung gestellt. Auch automatische Gegenmaßnahmen wie der Neustart eines Dienstes, oder das Versenden von E-Mails kann in Einzelfällen regelbasiert konfiguriert werden. Die Installation der Agenten sowie deren Konfiguration kann vollkommen automatisiert durchgeführt werden. Sobald ein neuer Server in das Netzwerk integriert wird, erkennt das der SCOM und installiert den Agenten automatisch auf dem Server. Für SCOM sind zahlreiche Management Packs erhältlich. Diese erweitern die Überwachungs-Funktion des Servers und der Agenten um weitere Aufgaben, zum Beispiel Exchange-spezifische Aufgaben, SQL-Datenbanken, DNS-Konfiguration oder die Überwachung der Hardware des Servers. Management Packs enthalten vordefinierte Regeln, Grenzwerte und Skripts, die speziell für ein Produkt entwickelt wurden. Die meisten Management Packs enthalten darüber hinaus noch Informationen und Tipps für die Fehlerbehebung einzelner Probleme, die automatisch angezeigt werden, wenn ein Fehler auftritt. Viele dieser Management Packs werden von den Hardware-Herstellern der Server und von Microsoft kostenlos zur Verfügung gestellt. Sofort nach der Installation eines Management Packs und der Integration in den Server findet die Überwachung der hinterlegten Komponenten statt. Da bereits zahlreiche Regeln automatisch hinterlegt sind, ist eine weitergehende Konfiguration nur zu Optimierungszwecken notwendig.

Für nahezu jedes Microsoft-Serverprodukt werden auf den Internetseiten von Microsoft kostenlose Management Packs zum Download angeboten. Da bei der Entwicklung dieser Management Packs auch das Know-how der Entwickler einfließt, stellen diese eine sehr effiziente Hilfe zur Überwachung von Microsoft-Servern dar, da genau die Komponenten überwacht werden, von denen die Entwickler der Meinung sind, das diese für die Stabilität eine Rolle spielen. Finden Administratoren für ein Problem, das auf einem Server aufgetaucht ist, selbst eine Lösung, kann diese in einer Datenbank auf dem SCOM-Server hinterlegt werden. Dazu wird das Problem wie als Ticket behandelt, vom Administrator geschlossen und die Fehlerbehebung in ein Textfeld eingetragen. Tritt dieses Problem noch einmal auf, weist der Server auf die mögliche Problemlösung hin. So müssen andere Administratoren nicht jedes Mal aufs Neue eine Fehlersuche beginnen. Dadurch werden der Zeitaufwand und auch die Kosten für die Verwaltung der IT reduziert. Fehler werden bereits erkannt, bevor diese gravierende Auswirkungen haben und Administratoren können agieren, anstatt beim Ausfall eines Servers nur zu reagieren.

Durch den Operations Manager wird nicht nur die Verfügbarkeit eines Servers geprüft, sondern auch die Stabilität und Erreichbarkeit einzelner Systemdienste und Serverkomponenten. Zum Beispiel sind im Management Pack für die Überwachung von Exchange-Servern die Regeln enthalten die auch im Exchange Best Practises Analyzer for Exchange enthalten sind. Diese Regeln werden aber nicht nur abgeprüft, wenn das Programm gestartet wird, sondern der Server überwacht ständig die Länge der Warteschlangen, die Systemdienste, Einstellungen und die Erreichbarkeit der einzelnen Dienste in Echtzeit. Sobald ein Problem auftritt, werden Maßnahmen gestartet, oft bevor das Problem gravierend wird. Auch die Infrastruktur der einzelnen Server wird entsprechend angezeigt. Die Exchange-Server werden im Überblick genauso dargestellt, wie ISA-Server oder die SQL-Server-Struktur. In der Übersicht werden Fehler auf den Servern angezeigt, sowie deren Auswirkung auf die anderen Server.

Abbildg. 18.31 Im Konfigurationsfenster der Konsole wird die Ersteinrichtung des Management-Servers durchgeführt und Clients werden an den Server angebunden



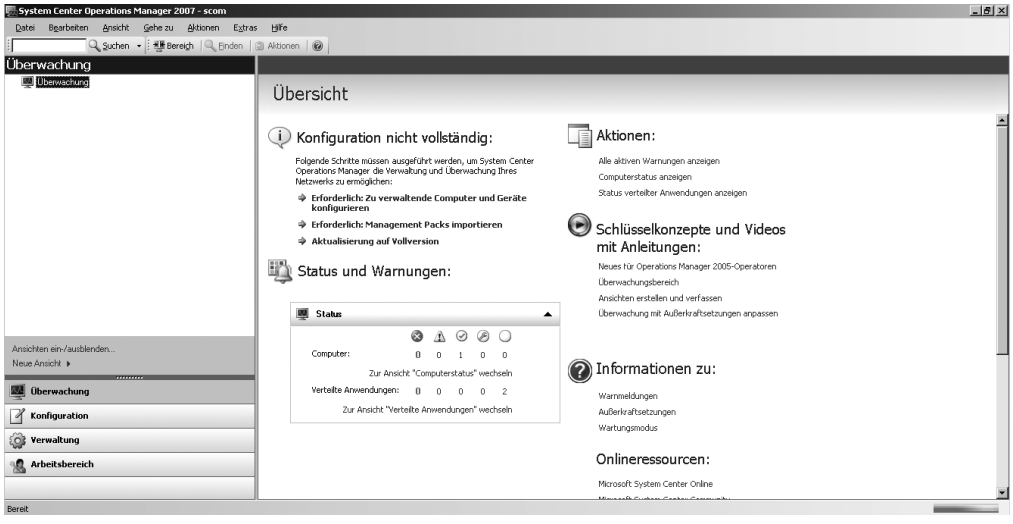
System Center Operations Manager 2007 im Überblick

Waren beim Microsoft Operations Manager 2005 noch die drei Konsolen Berichtskonsole, Operator-Konsole und Administrator-Konsole notwendig, gibt es bei SCOM 2007 nur noch die Operator-Konsole, über welche jetzt alle Aufgaben zentral durchgeführt werden. Die Konsole wurde dazu komplett überarbeitet, orientiert sich aber an der MOM 2005-Konsole, sodass ein Umlernen generell nicht notwendig ist. Wie bei den Vorgängern, kann die Konsole auch auf Arbeitsstationen installiert werden. Im Hauptfenster wird eine Zusammenfassung über das Netzwerk und alle vorhandenen Fehler angezeigt. Die generelle Bedienung ist aber noch immer sehr ähnlich zum Vorgänger, das heißt durch intuitives Klicken mit der Maus, kann die Infrastruktur bis zum einzelnen Server und Fehler »aufgefaltet« werden. Ebenfalls neu ist die Möglichkeit, Einträge aus den Sicherheitsprotokollen der Ereignisanzeigen aller überwachten Server zu sammeln und in der Datenbank abzulegen. Für diese Überwachung wird kein Agent benötigt. Auch andere Protokolle, lassen sich durch diese

neue Funktion überwachen. In die Leistungs- und Verfügbarkeitsüberwachung fließen daher jetzt nicht mehr nur die Ergebnisse der Management Packs und Agenten ein. Dadurch lassen sich auch sicherheitskritische Bereiche auf allen Servern effizient überwachen.

Viele Administratoren kennen diese Funktion noch als Audit Collection Services (ACS), die als Beta-Version von vielen Unternehmen genutzt wurden, um die Sicherheitsprotokolle, zum Beispiel aller Domänencontroller, zu sammeln und zentral auswerten zu können. Diese Technologie ist fester Bestandteil von SCOM 2007, eine eigene Infrastruktur für diese Technik wird nicht mehr benötigt. Fehler können per E-Mail an Administratoren geschickt werden. Dazu muss im Unternehmen ein SMTP-Server zur Verfügung stehen. Unterstützt wird neben Exchange, auch der interne SMTP-Dienst von Windows Server 2003/2008 oder auch andere SMTP-Server, zum Beispiel beim Internetprovider. Management Packs für SCOM 2007 gibt es nur noch in einer Version. Jedes Packet enthält alle Sprachen die SCOM unterstützt. Berichte und Regeln werden dann in der Sprache angezeigt, in welcher der Server installiert ist.

Abbildg. 18.32 Bei System Center Operations Manager 2007 gibt es nur noch eine Konsole, in der alle Aufgaben durchgeführt werden



Alle Komponenten können auch auf einem einzelnen Server installiert werden. Allerdings steigt dadurch die Last des Servers natürlich stark an und fällt dieser aus, ist keine Überwachung mehr verfügbar. In fehlertoleranten und größeren Umgebungen, sollte die Datenbank auf einem eigenen Server abgelegt, unter Umständen sogar geclustert werden. Außerdem sollten mehrere Management-Server installiert werden, welche die Informationen von den einzelnen Agenten auf den Servern erhalten. Mit dem neuen System Center Capacity Planner 2007 lässt sich eine Serverstruktur für SCOM 2007 optimal planen, da Zugriff und Verwaltung in komplexen Umgebungen simuliert werden können. Die Installation der Agenten auf den einzelnen Servern kann entweder automatisiert über die Softwareverteilung, aber auch skriptbasiert über die Windows PowerShell durchgeführt werden.

Mit dem neuen Gatewayserver lassen sich auch Computer in nicht vertrauten Domänen oder der DMZ überwachen. Dazu wird auf einem SCOM-Server diese neue Rolle zusätzlich installiert. Der Server dient dann zukünftig dazu, die SCOM-Infrastruktur mit unvertrauten Domänen oder der

DMZ zu verbinden. Die dazu notwendige Authentifizierung wird über entsprechende Zertifikate abgewickelt. Der Verbindungsaufbau zur Überwachung wird durch den Gatewayserver initiiert, sodass in den Firewalls, zum Beispiel zwischen Netzwerk und DMZ nur ein Server mit den entsprechenden Ports berechtigt werden muss. Auf diese Weise können aber keine Agenten auf den zu überwachenden Servern gepusht werden. Das liegt daran, dass der RPC-Verkehr zwischen vertrauten und nicht vertrauten Netzwerken oft blockiert wird. In diesem Fall sollte der Agent auf andere Weise installiert werden, also manuell oder per Skript. Alternativ muss dem Management Server der RPC-Zugriff auf die DMZ gestattet werden, die durch den Gatewayserver mit der SCOM-Infrastruktur überwacht wird.

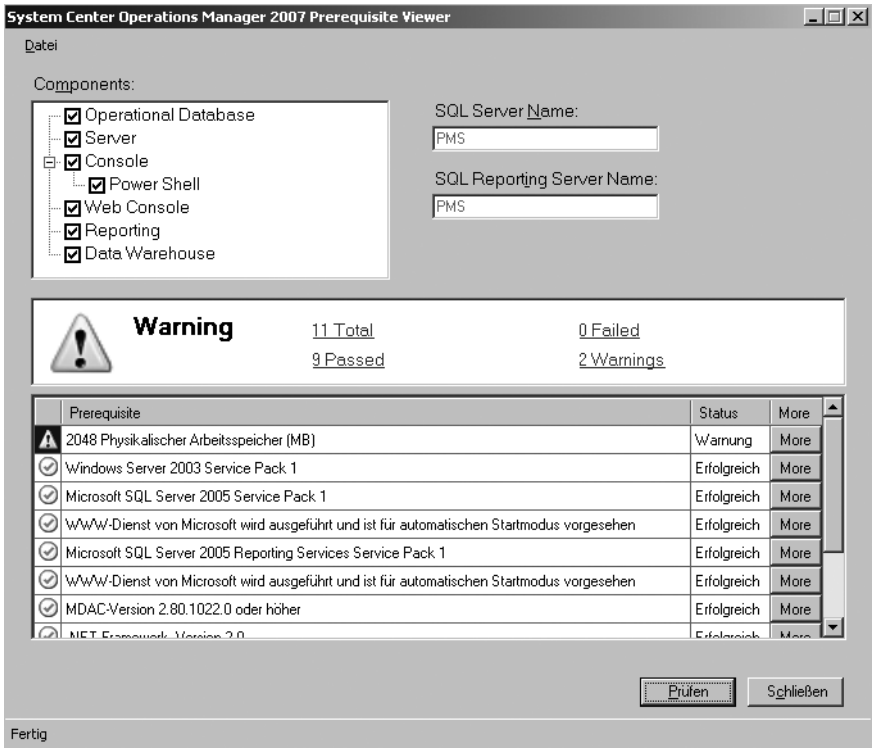
Soll von MOM 2005 zu SCOM 2007 migriert werden, empfiehlt Microsoft den parallelen Aufbau der neuen Umgebung. Auf den überwachten Servern wird dazu parallel zu den MOM 2005-Agenten der SCOM 2007-Agent installiert. Erst wenn die Überwachung auf SCOM 2007 gewechselt wurde, sollte die alte MOM 2005-Infrastruktur entfernt werden. Bestehende Regeln und Grenzwerte von MOM 2005-Management Packs können zu SCOM 2007 migriert werden. Der Import von MOM 2000-Regeln wird allerdings nicht unterstützt.

Viele Service Provider überwachen mit einer MOM-Infrastruktur den Serverzustand von Kunden, bei denen die Administratoren wiederum die Server mit den System Center Essentials (SCE) überwachen. Die SCE bauen auf SCOM 2007-Technologie auf und können bei der Überwachung durch einen zentralen Server auf den Service Provider-Modus umgeschaltet werden. SCE 2007 unterstützt die Überwachung von maximal 30 Servern. Müssen mehr überwacht werden, wird SCOM 2007 benötigt.

SCOM testen und installieren

Auf der Produktseite unter *http://www.microsoft.com/systemcenter/opsmgr/default.mspx* wird eine voll funktionsfähige 180 Tage-Testversion zur Verfügung gestellt. Lädt man die Testversion herunter, erhält man eine E-Mail in der zahlreiche weitere Links zu weiterführenden Informationen und Whitepapers vorgestellt werden. Vor der Installation lassen sich die notwendigen Systemvoraussetzungen prüfen und ein Bericht ausgeben, wo nachgearbeitet werden muss. Auf der Internetseite *http://technet.microsoft.com/en-us/opsmgr/bb986763.aspx* stellt Microsoft zahlreiche Lernvideos für den System Center Operation Manager 2007 zur Verfügung. Auch im Microsoft-TechNet gibt es zum Produkt zahlreiche Webcasts. Die Daten der Überwachung des Servers werden in einer Datenbank gespeichert. Dazu benötigt SCOM 2007 einen Server mit SQL Server 2005 SP1. Der SQL Server-Dienst sollte mit minimalsten Rechten gestartet werden, zumindest wenn kein anderer Dienst mehr Rechte benötigt. Ausreichend ist zum Beispiel der Benutzer »Netzwerkdienst«. Damit SCOM installiert werden kann, wird mindestens Windows Server 2003 mit SP1 besser SP2 benötigt. Außerdem muss auf dem Server die Windows PowerShell, sowie .NET Framework 3.0 installiert werden. Die Agenten unterstützen aber so gut wie alle Microsoft-Serverprodukte und auch Unix- oder Linux-Server. Auch Windows Vista und Windows Server 2008 werden unterstützt.

Abbildg. 18.33 Vor der Installation können die Systemvoraussetzungen an die Infrastruktur abgeprüft und angezeigt werden



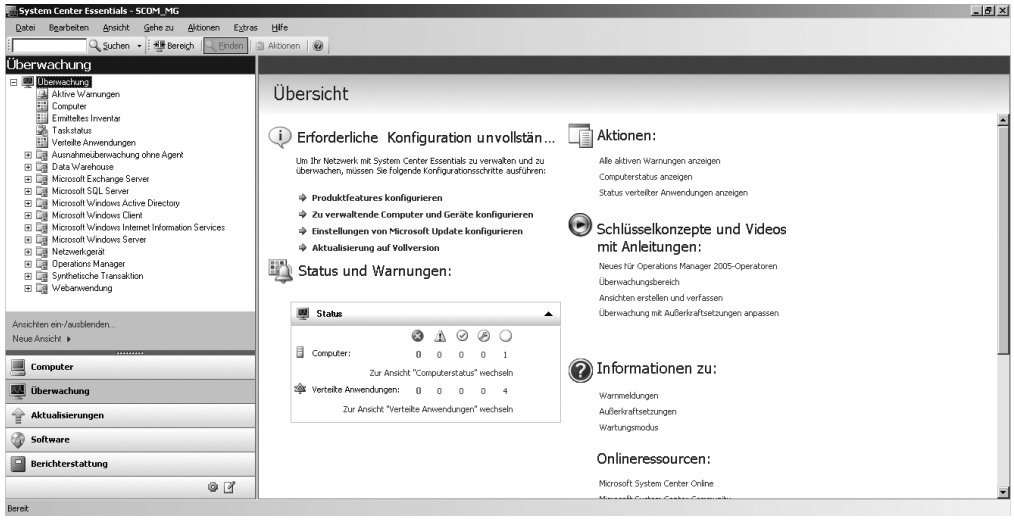
Microsoft System Center Essentials 2007

Die Microsoft System Center Essentials (SCE) 2007 richten sich an mittelständische Unternehmen bis maximal 30 Servern und 500 Arbeitsstationen. Bei dieser Serverlösung handelt es sich um eine Server-Technologie zur einfachen Verwaltung, Inventarisierung, Softwareverteilung und Betriebsüberwachung von Servern und Arbeitsstationen im Unternehmen. Vor allem die Überwachung der Server, die Diagnose von Fehlern, sowie die Inventarisierung und Softwareverteilung stehen dabei im Mittelpunkt. Das Produkt ist eine Neuentwicklung und basiert auf Technologien aus dem Microsoft System Center Operations Manager (SCOM) 2007, dem System Center Configuration Manager (SCCM) 2007 und den Windows Server Update Services 3.0. Dabei handelt es sich aber nicht nur um eine gemeinsame grafische Oberfläche für diese drei Produkte, sondern ein komplett neues Programm, in das diese Techniken integriert wurden. Da vor allem SCOM 2007 und SCCM 2007 sich eher an sehr große Unternehmen richten und teilweise sehr komplex in Einrichtung und Verwaltung sind, setzen mittelständische Unternehmen nur selten auf diese Produkte. Die System Center Essentials 2007 sollen das ändern und auch kleineren Unternehmen den Einstieg ermöglichen. Grundsätzlich handelt es sich bei den System Center Essentials 2007 um den Nachfolger des Microsoft Operations Manager 2005 Workgroup Edition, allerdings mit zahlreichen neuen Funktionen. Für den System Center Operations Manager 2007 wird es keine Workgroup Edition mehr geben.

Was bietet System Center Essentials 2007?

Durch die einheitliche Oberfläche, der Verwaltungskonsole, erhalten mittelständische Unternehmen eine zentrale Verwaltungslösung aus einem Guss. Es sind keine verschiedenen Technologien mit unterschiedlichen Verwaltungswerkzeugen notwendig. Sobald in der Konsole ein Fehler oder neuer Computer gemeldet wird, können über das Kontextmenü die dazu notwendigen Aufgaben angezeigt werden. Die Verwaltungskonsole kann natürlich auch auf einer Arbeitsstation installiert werden. Die Software unterstützt dabei mit einfach zu bedienenden Assistenten die Integration der einzelnen Technologien auch für Administratoren, die keine Spezialisten in diesem Bereich sind. Neben der Überwachung und Diagnose, erstellt SCE regelmäßig Berichte auf Basis der SQL Server 2005 Reporting Services. Wird im Unternehmen noch keine SQL Server 2005-Datenbank betrieben, installieren SCE 2007 automatisch die Express Edition von SQL Server 2005 und integrieren die Datenbank automatisch. Um das Produkt zu verwenden, ist keine Zusatzsoftware notwendig, keine monatelange Planung und kein komplexer Integrationsprozess. Schon nach der Installation sind die SCE sehr schnell einsatzbereit, die entsprechende Konfiguration erfolgt über Assistenten. Bestandteil der Berichte ist der aktuelle Status der Server und Arbeitsstationen im Gesamten. Ein Administrator erkennt so schon am Morgen ob die Server alle problemlos funktionieren, ob es neue Updates gibt, die installiert werden müssen und ob neue Computer im Netzwerk gefunden wurden. Auch die Inventarisierung, also eine Bestandsaufnahme aller Computer und Server im Netzwerk ist möglich. Software kann ebenfalls auf den einzelnen Arbeitsstationen einfach verteilt werden, doch dazu später mehr.

Abbildg. 18.34 Die System Center Essentials liefern eine einheitliche Oberfläche für Überwachung, Aktualisierung, Diagnose und Inventarisierung

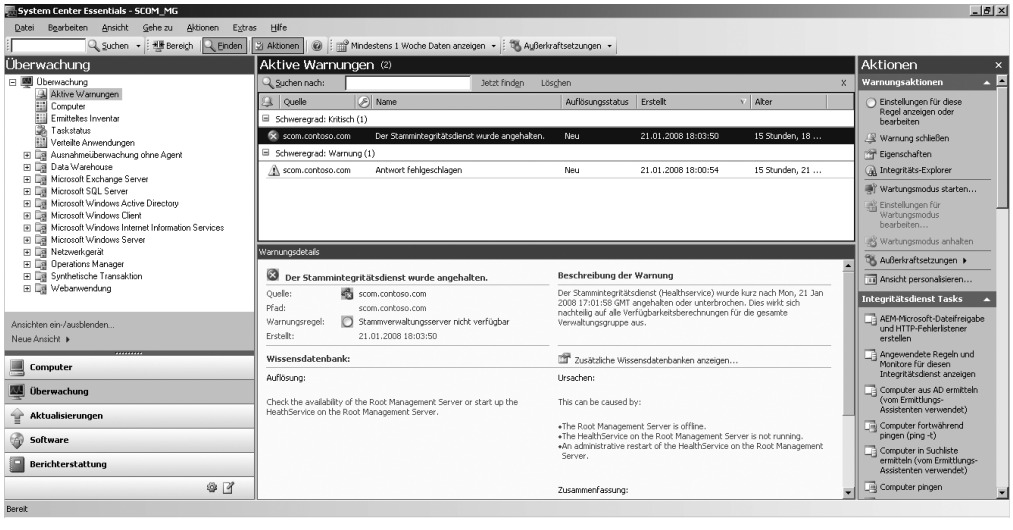


Die Überwachungsfunktion der SCE findet oft schon Fehler auf den Servern, bevor diese gravierende Auswirkungen haben. Weisen zum Beispiel erste Warnungen in den Ereignisanzeigen auf defekte Hardware hin, oder findet der installierte Agent auf dem Server einen Fehler, wird der Administrator darüber informiert und kann Maßnahmen einleiten. Alle Server im Netzwerk werden automatisch in Echtzeit überwacht, egal ob es sich dabei um physische oder virtuelle

Maschinen handelt. Serverdienste wie Exchange, Active Directory oder SQL werden mit speziellen Management Packs bis ins Detail überwacht. Es ist schwierig für einen Administrator sich mit allen Technologien im Netzwerk auszukennen und diese ständig zu überwachen. Da in den Management Packs Regeln zur Überwachung spezieller Bereiche des Servers, wie Warteschlangen, Verfügbarkeit der Postfächer bei Exchange und so weiter integriert sind und die Entwickler der Software selbst diese Regeln erstellt haben, ist sichergestellt, dass genau das überwacht wird, was wichtig ist. Administratoren müssen keine Spezialisten für SQL Server oder Exchange sein, um Probleme zu finden und zu lösen. SCE grenzt den Fehler ein und weißt auf Probleme und deren Lösung hin. Neben den Management Packs, die zum größten Teil von Microsoft und Serverherstellern kostenlos zur Verfügung gestellt werden, liest die Software auch Informationen per SNMP von Routern, Switches oder anderen Geräten aus, die diese Technologie unterstützen.

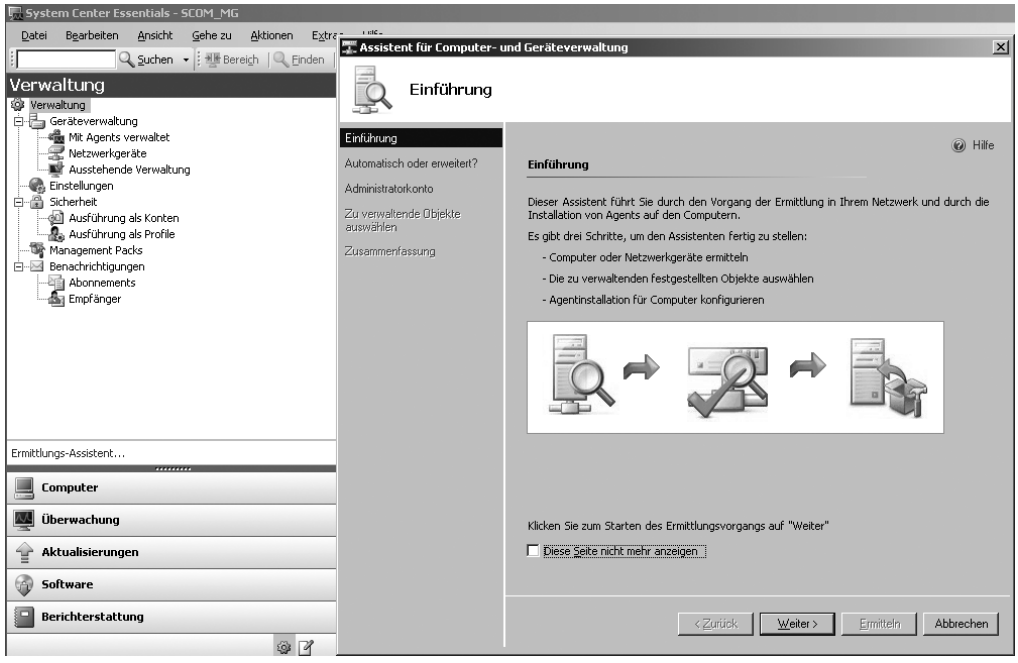
In der Konsole werden bereits über das Startfenster alle aktive Warnungen und Fehler im Netzwerk angezeigt. Wird eine Warnung oder ein Fehler angeklickt, wird automatisch die mögliche Ursache und Problemlösung im Fenster angezeigt. Über das Kontextmenü zum Fehler, schlagen die SCE weitere Diagnosemöglichkeiten und Werkzeuge vor um den Fehler einzugrenzen. Ist ein Fehler gelöst, kann dieser in der Konsole geschlossen werden. Dadurch wird die Konsole aufgeräumt und es werden nur die Fehler angezeigt, die tatsächlich aktuell im Netzwerk vorhanden sind. Für jeden Fehler kann eine eigene, firmenspezifische Lösung hinterlegt werden. Das hat den Vorteil, dass beim erneuten Auftauchen des gleichen Fehlers, der firmeninterne Lösungsvorschlag unterbreitet wird und nicht neu recherchiert werden muss. Auch diese Maßnahme wird wieder über das Kontextmenü zum Fehler durchgeführt, steht also intuitiv zur Verfügung.

Abbildg. 18.35 Alle Fehler auf den Servern werden an einer zentralen Stelle angezeigt und können bearbeitet werden. Auch Lösungsvorschläge werden unterbreitet.

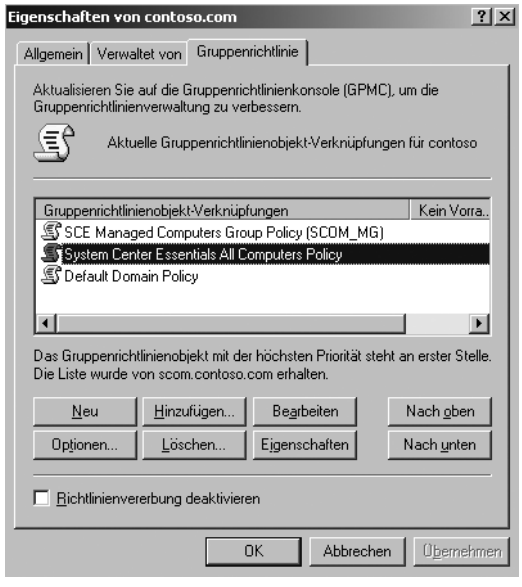


Die Konfiguration der einzelnen Funktionen erfolgt mit Assistenten. Die Einstellungen, die in den Assistenten durchgeführt werden, hinterlegen die SCE automatisch als Gruppenrichtlinien. Diese Richtlinien können mit den herkömmlichen Verwaltungswerkzeugen angezeigt und verwaltet werden. Das ist allerdings nicht notwendig, da die Einstellungen auch über die Verwaltungskonsole der System Center Essentials nachträglich angepasst werden können.

Abbildg. 18.36 Nach der Installation wird über einen Assistenten die Einrichtung durchgeführt, um die Server und Computer im Netzwerk anzubinden



Abbildg. 18.37 Der Konfigurationsassistent der SCE erstellt automatisch Gruppenrichtlinien, um die angebundenen Computer und Server zu konfigurieren



Die Verwaltungsoberfläche der SCE bieten auch die Möglichkeit, Updates im Netzwerk über WSUS 3.0 zu konfigurieren. Dazu wurde WSUS komplett in die Konsole integriert und ermöglicht daher eine zentrale Verwaltung aller Patches. Auch hier können wieder alle Computer automatisch ermittelt und integriert werden. Die Verwaltung der Patches wird dadurch sehr einfach und in die täglichen Berichte integriert. Neben der Überwachung der Server, werden auch die Arbeitsstationen überwacht. Teilt ein Anwender mit, dass sein Computer sehr langsam ist, kann direkt in der Konsole die aktuelle CPU-Last des Computers angezeigt und analysiert werden.

Automatische Bestandsverwaltung und Softwareverteilung

Eine der in SCE 2007 integrierten Technologien ist der System Center Configuration Manager 2007, der Nachfolger des System Management Servers (SMS) 2003. Dieser stellt neben automatischer Softwareverteilung auch eine vollständige und automatisierte Hard- und Softwareinventarisierung zur Verfügung, die in der gleichen Oberfläche verwaltet wird, wie die anderen Funktionen. Auch hier lassen sich wieder detaillierte und sehr professionelle Berichte auf Basis der SQL Server 2005 Reporting Services erstellen. Auch die Softwareverteilung ist ziemlich ausgereift. Neue Computer werden automatisch in die Überwachung und Inventarisierung integriert, da SCE täglich das Active Directory nach neuen Maschinen scannen kann. Um neue Software mit SCE zu verteilen, steht ein eigener Bereich in der Konsole zur Verfügung und mit Assistenten wird die Software als Packet in SCE integriert. Außerdem kann festgelegt werden, auf welche Computer die neue Software verteilt werden soll. Durch die einheitliche Oberfläche kann auch hier über das Kontextmenü von Computern festgelegt werden, welche Softwarepakete, die mit SCE bereitgestellt werden sollen, automatisch installiert werden.

Abbildg. 18.38 Über das Kontextmenü der Computer können auch die erstellten Softwarepakete zugewiesen werden

Über den Software-Bereich der Konsole kann wiederum angezeigt werden, auf wie vielen Computern die Anwendung installiert worden ist. Auch die Bezeichnung der Computer wird hier angezeigt, sodass in der Konsole ein schneller Überblick erlangt wird, welche Software auf welchen Computern tatsächlich installiert wurde. Alle dazu notwendigen Aufgaben und Informationen sind selbsterklärend über den jeweiligen Menüpunkt im Kontextmenü erreichbar. Tritt auf einem Rechner ein Fehler auf, erhält der Administrator sehr schnell eine Übersicht darüber, welche Hardware im Computer verbaut ist, welche Software installiert ist und wie die aktuelle Auslastung des Systems ist. Dazu

ist keine Turnschuh-Administration notwendig, sondern alle wichtigen Informationen können bequem über die Verwaltungskonsole der SCE abgerufen werden. Natürlich lässt sich auf dem gleichen Weg die Software auch wieder deinstallieren, wenn diese auf einem Computer nicht mehr benötigt wird, oder keine Lizenzen mehr frei sind.

System Center Essentials testen

Über die Microsoft-Webseite *http://www.microsoft.com/germany/systemcenter/sce* wird eine für 90 Tage lauffähige Testversion von SCE zur Verfügung gestellt, über die sehr leicht eine Testumgebung aufgebaut werden kann. Die Testversion kann später zur Vollversion aktualisiert werden, sodass beim produktiven Einsatz der Software keine Neuinstallation stattfinden muss. Auf der Webseite finden sich auch einige Links zu Webcasts und Whitepapern. Administratoren kommen aber auch durch das Ausprobieren zu den wichtigsten Bereichen der Software. Auf jeder Seite der Verwaltungskonsole werden ausführliche Hilfen und Lernvideos zur Verfügung gestellt, welche die Einrichtung und Verwaltung vereinfachen sollen.

Durch Microsoft System Center Essentials 2007 erhalten mittelständische Unternehmen die gleichen Technologien und damit verbundenen Vorteile, um vor allem Fehler auf Servern schnell zu erkennen und zu beheben. Durch die Software wird die Verwaltung erleichtert und der Überblick im Netzwerk geht nicht verloren. Da eine voll funktionsfähige Testversion zur Verfügung gestellt wird, die sehr einfach installiert und im Netzwerk integriert werden kann, sollten Unternehmen den Einsatz prüfen, wenn noch keine andere Überwachungssoftware eingesetzt wird. Natürlich macht die Software nur dann Sinn, wenn im Unternehmen hauptsächlich Microsoft-Server betrieben werden. Eine Überwachung von UNIX- und Linux-Computer ist generell zwar auch möglich, aber nicht im Fokus der Anwendung. Der wichtigste Bereich der SCE ist klar die Überwachung und Diagnose von Fehlern. Vor allem die proaktive Überwachung von wichtigen Serverdiensten kommt in mittelständischen Unternehmen oft zu kurz. Auch die automatische Softwareverteilung findet in vielen Unternehmen nur rudimentär oder gar nicht statt. Da die meisten Anwendungen ohnehin per MSI-Paket installiert werden, ist die automatische Verteilung per SCE ein netter Zusatznutzen, der die Administratoren im Unternehmen deutlich entlasten kann.

Zusammenfassung

In diesem Kapitel haben Sie erfahren, wie Sie Server mit Windows Server 2008 überwachen und Fehler finden können. Mit den Bordmitteln und den Werkzeugen, die Microsoft zum größten Teil kostenlos zur Verfügung stellt, können Windows Server 2008-Computer sehr effizient überwacht werden. Im nächsten Kapitel zeigen wir Ihnen, wie Sie die Verfügbarkeit von Windows Server 2008 auf hochverfügbar verbessern, wie Sie Cluster mit Windows Server 2008 installieren und wie Sie in einer virtuellen Testumgebung eine hochverfügbare iSCSI-Cluster-Testumgebung aufbauen.

Kapitel 19

Cluster und Hochverfügbarkeit

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen den Umgang und die generelle Planung eines Ausfallkonzeptes und die Einführung einer Hochverfügbarkeitslösung in Microsoft-Netzwerken. Weiterhin gehen wir in diesem Kapitel auch auf die Installation, Konfiguration und Verwaltung eines Clusters unter Windows Server 2008 ein. Vor allem bei der Installation und Verwaltung eines Clusters wurden einige Verbesserungen vorgenommen. In Kapitel 1 wurden Ihnen bereits einige Neuerungen vorgestellt. Die Installation eines Clusters wurde stark vereinfacht. Neben der Installation eines Clusters zeigen wir Ihnen in diesem Kapitel auch, wie Sie ein Microsoft-Netzwerk möglichst ausfallsicher gestalten können.

Ausfallkonzepte in Microsoft-Netzwerken

Ausfallkonzepte sollen verhindern, dass im Notfall, also beim Ausfall eines oder mehrerer Server, Mitarbeiter im Unternehmen nicht mehr arbeiten können. Ausfallkonzepte sind ein wichtiger Punkt bei der Konzeption eines Netzwerks, der leider viel zu oft vernachlässigt wird. Im Falle eines Serverausfalls sollte eine Dokumentation verfügbar sein, in der genaue Anleitungen stehen, welche Aufgaben erledigt werden müssen, damit die Funktion des Servers wiederhergestellt oder kompensiert werden kann. Ein Ausfallkonzept soll verhindern, dass Panikmaßnahmen und Schnellschüsse die Situation verschlimmern. Zu einem guten Microsoft-Netzwerk-Konzept gehört auch ein Ausfallkonzept für jeden einzelnen Server und eine ausführliche Dokumentation. Ein gutes Ausfallkonzept baut auf einer soliden Netzwerkplanung auf.

Grundlagen für ein Ausfallkonzept

Der erste Schritt eines Ausfallkonzepts besteht darin, bereits frühzeitig Einflüsse zu erkennen, die den Ausfall eines Servers begünstigen könnten. Der erste und wichtigste Schritt eines Ausfallkonzepts ist, einen Ausfall zu verhindern. Dazu gehört eine effiziente Planung des Netzwerks und der einzelnen Server. Ein solches Konzept beinhaltet aber auch eine vernünftige Sicherheits- und Berechtigungsstruktur. Natürlich enthält es auch die Planung und konsequente Umsetzung eines optimalen Serverraums sowie der Stromversorgung. Die letzte notwendige Voraussetzung für ein effizientes Ausfallkonzept ist eine gut geplante Datensicherung mit allen Möglichkeiten, um Dateien schnell und effizient wiederherzustellen. Erst wenn alle Voraussetzungen erfüllt sind, wird als letztes ein Ausfallkonzept erstellt. Wenn Sie in einem Unternehmen alles unternommen haben, damit die Server möglichst nicht ausfallen, dass Daten schnell wiederhergestellt werden können und dass niemand unberechtigt Einfluss auf die Daten nehmen kann, dann können Sie sich an die Erstellung eines Ausfallkonzepts machen. Ein Ausfallkonzept soll Ihnen helfen, falls unvorhergesehene Ausfälle passieren. Eine gute Netzwerkplanung soll vorhersehbare Ausfälle verhindern. Wenn Sie sich bereits Gedanken über einen Serverausfall machen, der noch gar nicht eingetreten ist, bleibt Ihnen genügend Zeit, notwendige Gegenmaßnahmen zu planen, ohne unter Zeitdruck zu stehen. Wenn einer oder mehrere Server ihre Funktion eingestellt haben, können keine Gegenmaßnahmen getroffen werden, sondern es wird nur reagiert und mit allen möglichen Mitteln versucht, den Server wieder ans Laufen zu bringen.

Dokumentationen für das Ausfallkonzept

Der Aufbau eines Ausfallskonzepts muss sehr strukturiert durchgeführt werden. Sehr wichtig dabei ist die Berücksichtigung wirklich jedes erdenklichen Problemfalls. Ein Ausfallkonzept macht keinen Sinn, wenn Sie sich zu einem großen Teil darauf verlassen, dass schon nichts schief gehen wird. Das Ausfallkonzept jedes Servers wird in einem Ordner aufbewahrt, der alle notwendigen Informationen enthält. Dieser Ordner muss an bekannter Stelle gelagert werden, damit er für den notwendigen Personenkreis zum Zugriff bereitsteht.

Dokumentation der Server

Eine gute Dokumentation gehört eigentlich nicht speziell zu einem Ausfallkonzept, sondern ist eine Selbstverständlichkeit für ein Netzwerkprojekt. Eine Dokumentation kann durchaus in elektronischer Form vorliegen. Im Falle eines Netzwerkausfalls werden Sie allerdings an eine elektronische Dokumentation möglicherweise nicht mehr herankommen. Daher sollten Sie parallel alle Dokumente für den Ausdruck optimieren, ausdrucken und in Ordner ablegen. Für jeden Server sollte eine Dokumentation angefertigt werden, die alle notwendigen Informationen über ihn enthält. Folgende Informationen gehören zum Beispiel in die Dokumentation eines Servers:

- Dokumentation des Standorts des Servers, zum Beispiel in welchem Serverraum und an welcher Stelle des Racks er eingebaut wurde.
- Genaue Dokumentation der eingebauten Hardware in verständlichen Worten und schnell überschaubar (am besten Kopie des Angebots oder der Rechnung, falls alles draufsteht).
- Telefonnummern der Ansprechpartner im Notfall, also Support und Techniker, notfalls IT-Administratoren.
- Soweit vorhanden, Servicenummer, Kundennummer und Kaufdatum, die Sie angeben müssen, wenn Sie den Herstellersupport verständigen. Er ist sehr ärgerlich, wenn die entsprechenden Daten bei einem Ausfall erst gesucht werden müssen.
- Dokumentation des Betriebssystems und der installierten Treiber. Bei Aktualisierungen muss auch dieser Teil der Dokumentation ständig aktuell gehalten werden.
- Dokumentation der installierten Software mit genauem Softwarestand. Ideal in diesem Fall sind Screenshots und die genaue Beschreibung der Installation jeder einzelnen Anwendung. Sie müssen nicht jedes Fenster dokumentieren. Aber zum Beispiel bei der Installation von Oracle-Datenbanken oder ERP-Systemen, die nicht jeden Tag durchgeführt werden, kann bei einer späteren Wiederherstellung eine lückenlose Dokumentation sehr wichtig sein.
- Dokumentation der Besonderheiten wie Partitionierung, spezielle RAID-Einstellungen oder aller Maßnahmen, die bei der Installation vorgenommen wurden und sich von der Norm unterscheiden.
- Dokumentation der Systemeinstellungen wie IP-Adresse, Domänennamen, Servername, angelegte lokale Benutzer und Kennwörter (nur unter Verschluss).
- Dokumentation, welche Abteilungen und Mitarbeiter im Unternehmen bei Ausfall des Servers nicht mehr arbeiten können, damit diese informiert werden können.
- Aufkleber auf dem Server, der die wichtigsten Informationen enthält (Servername, IP-Adresse, Servicenummer, die meistens auf der Rückseite steht).

- Gegenseitige Abhängigkeiten des Servers von anderen Servern oder Serverdiensten. Zum Beispiel kann ein ERP-Server ohne einen Oracle-Datenbankserver nicht mehr funktionieren.
- Dokumentation der Dienste des Servers (lässt sich in der Kommandozeile mit *net start >c:\dienste.txt* in eine Textdatei dokumentieren).

Sicherlich werden Ihnen noch einige weitere Punkte einfallen, die für Ihre Dokumentation notwendig sind. Auch wenn es oft lästig erscheint, Softwareinstallationen genau zu dokumentieren, sollten Sie an dieser Stelle so exakt wie möglich vorgehen. In dem Moment, in dem Sie eine Änderung vornehmen, wissen Sie, warum Sie dies getan haben. Wenn Sie später im Notfall den Server neu installieren oder wiederherstellen müssen, vor allem noch unter Zeitdruck, werden Sie dankbar dafür sein, wenn Sie nicht nachgrübeln müssen, sondern anhand der Anleitung nachvollziehen können, was bei der Installation durchgeführt wurde.

Empfehlungen für die Dokumentation

In eine Dokumentation sollten Sie so genau wie möglich vom Standard abweichende Informationen aufnehmen. Irrelevante Informationen wie etwa die Bestätigung von Standardfenstern verwirren nur und lenken von den wirklich wichtigen Dingen ab. Solche standardmäßigen Vorgänge müssen nicht dokumentiert werden. Eine Dokumentation sollte hinsichtlich spezieller Installationen und Einstellungen präzise sein und alle notwendigen Informationen enthalten. Sobald Sie etwas an einem Server ändern, sollten Sie diese Änderung in die Dokumentation aufnehmen und erläutern, was genau geändert oder installiert wurde, wann und von wem. Auch eine Beschreibung über den Grund der Änderung oder Installation kann sehr hilfreich sein. Eine Dokumentation ist nur brauchbar, wenn sie aktuell gehalten wird. Eine veraltete Dokumentation bringt im Notfall überhaupt nichts.

Archivierung der notwendigen Software

Der nächste Schritt sollte darin bestehen, dass Sie jede Software und jeden Treiber, den Sie auf dem Server installieren, in einem eigenen Verzeichnis im Netzwerk aufbewahren. Wenn sich ein Treiber oder eine Software ändert oder hinzugefügt wird, sollten Sie auch diese Änderung in dem Verzeichnis aufnehmen und die alte Version löschen. In einem solchen Verzeichnis sollten sich darüber hinaus auch alle Seriennummern und notwendigen Informationen befinden, die Sie zur Installation benötigt haben. Auch die Dokumentation des Servers in elektronischer Form sollte hier, zumindest in Kopie, abgelegt werden. Kopieren Sie den Inhalt dieses Verzeichnisses auf mindestens zwei CDs oder DVDs und bewahren Sie diese zwei Datenträger in einer Plastikhülle im Dokumentationsordner auf – zwei Datenträger aus dem Grund, weil dann die notwendige Software wirklich immer verfügbar ist. Nach Murphys Gesetz geht schief, was schief gehen kann. Folglich wird die CD in der Dokumentation sicher defekt sein, wenn Sie diese brauchen, daher machen zwei Kopien durchaus Sinn.

Im Dokumentationsordner befindet sich daher nicht nur die ausführliche Dokumentation, sondern er enthält auch zwei Datenträger mit allen Treibern und die Dokumentation in elektronischer Form. Halten Sie diesen Stand immer aktuell, auch wenn es lästig erscheint. Beim Ausfall des Servers werden Sie dankbar sein, nicht erst Software zusammensuchen oder herunterladen zu müssen. Sie sollten zusätzlich jede Software, die Sie auf einem Server installieren, lokal auf den Server kopieren. Das hat den Vorteil, dass Sie diese Software sofort verfügbar haben, wenn Sie diese auf dem Server nachinstallieren müssen oder auf einem anderen, neuen Server der gleichen Art benötigen. Vor allem eine Kopie der Windows Server 2008-DVD auf dem Server erspart Administratoren den Gang zum

Serverraum und den CD/DVD-Wechsel. Bei den Kapazitäten der heutigen Festplatten fallen diese paar Gigabyte kaum ins Gewicht. Wenn der Festplattenplatz trotzdem knapp werden sollte, müssen Sie die Datenträger ohnehin erweitern und bei Bedarf können Sie dieses Verzeichnis immer noch löschen. Ich kopiere vor jeder Installation einer Applikation die Software erst auf den Server, zum Beispiel in das Verzeichnis *c:\install*, und installiere dann die Applikationen aus diesem lokalen Verzeichnis.

Dokumentation der Netzwerkinfrastruktur

Mindestens genauso wichtig wie die Dokumentation der Server ist die Dokumentation der Netzwerkinfrastruktur. Diese sollte am besten mit Microsoft Visio oder einem anderen Grafikprogramm angefertigt werden. Die Dokumentation sollte visuell den Serverraum mit allen Servern sowie deren Namen und IP-Adressen enthalten. Auch die angeschlossenen USVs und Switches sowie die Anbindung der Niederlassungen mit Routern und Firewalls sollten lückenlos aufgezeichnet und die IP-Adressen der Routingtabellen genau dokumentiert werden. Am besten lassen Sie sich diese Zeichnung auf DIN A0 ausplotten oder drucken und hängen sie an die Wand. Je mehr Niederlassungen und physische Netzwerke ein Unternehmen hat, umso wichtiger ist die ausführliche Dokumentation der Leitungen und Wege, welche die IP-Pakete durchlaufen müssen. Die Dokumentation der einzelnen Netzwerkgeräte und deren Konfiguration sollte ebenfalls in schriftlicher Form vorliegen.

Die Dokumentation der Netzwerkinfrastruktur sollte daher grafisch erfolgen, aber auch schriftlich, was die Konfigurationen der einzelnen Geräte betrifft. Wenn Sie einen ISA Server einsetzen, sind auch die Erstellung der Regeln und Einstellungen genau zu dokumentieren und am besten bereits während der Einstellung mit Screenshots nachzuverfolgen. Die Informationen über die Netzwerkinfrastruktur sollten möglichst lückenlos sein. Auch auf Switches, Router und Hardware-Firewalls sollten Aufkleber mit IP-Adressen und Servicenummern vorne am Gerät angebracht sein. Auf diese Weise sind die wichtigsten Informationen sofort greifbar. Der entsprechende Ordner zur Dokumentation der Netzwerkinfrastruktur sollte ebenfalls die Notrufnummern des Supports beinhalten und genauso ausführlich sein wie die Dokumentation der Installation der Server. Zwar enthalten die meisten Netzwerkgeräte kein installiertes Betriebssystem mit Treibern und Software, aber dafür ist die Konfiguration, vor allem bei Routern, deutlich komplexer. Da die meisten Router eine Konfiguration in Form einer Textdatei bieten, sollten Sie diese im Netzwerk abspeichern, gegebenenfalls auch zeitlich gestaffelt in mehreren Versionen, um später noch einen Überblick über erfolgte Änderungen zu haben.

Workflow für Änderungen auf den Servern

Damit Sie sicher sein können, dass die Dokumentationen Ihrer Server immer so aktuell wie möglich sind, sollten Sie für Änderungen auf den Servern und den damit einhergehenden Änderungen der Dokumentation und archivierten Software einen Workflow definieren, den Sie zum Beispiel in den SharePoint Services ablegen können. In diesem Workflow wird definiert, was genau bei Änderungen an den Servern durchgeführt werden muss. Administratoren und Supportmitarbeiter müssen sich an diesen Workflow halten. Dieser hält in einfachen Schritten fest, in welcher Reihenfolge die einzelnen Aufgaben der Aktualisierung durchgeführt werden müssen. Viele Unternehmen setzen für solche Workflows ITIL (IT Infrastructure Library) ein. Ich gehe auf dieses Konzept kurz im nächsten Abschnitt ein. Ein Workflow sollte mindestens folgende Informationen enthalten:

- Vor der Installation beim Anbieter der bereits installierten Software nach der Kompatibilität erkundigen (sehr wichtig vor der Installation von Service Packs auf Warenwirtschaftsservern).

- Genehmigung einholen, wenn es ein Change Management im Unternehmen gibt (also beim Einsatz von ITIL). Auch ohne Change Management muss trotzdem ein Verantwortlicher über die Installation und deren möglichen Folgen informiert werden. Einfach etwas zu installieren und damit einen Ausfall zu provozieren hat schon manchen Administrator den Arbeitsplatz gekostet. Jede Installation ist ein potentielles Risiko, das genau abgewogen und genehmigt werden muss. Es muss begründet werden, warum eine Aktualisierung stattfinden soll, und erläutert, was im schlimmsten Fall passieren kann. Eventuell Zeitrahmen für die Installation mit den betroffenen Mitarbeitern abstimmen.
- Vor der Änderung eine Datensicherung des Servers durchführen, am besten sogar ein Image.
- Vor der Installation sicherstellen, dass das Ausfallkonzept auf dem aktuellen Stand ist (ein guter Administrator ist immer paranoid und geht vom Schlimmsten aus).
- Die notwendige Software auf den Server und das Archivierungsverzeichnis der installierten Software ins Netzwerk kopieren.
- Installation auf dem Server durchführen und lückenlos dokumentieren.
- Dokumentation aktualisieren, dazu kann zum Beispiel in den SharePoint Services ein Formular hinterlegt werden, in die nur noch alle wichtigen Informationen eingetragen werden müssen. Falls ein solches Formular vorhanden ist, können Sie davon ausgehen dass bei der Aktualisierung der Dokumentation alle notwendigen Informationen erfasst werden und einzelne Punkte nicht vergessen werden können.
- Dokumentation ausdrucken und im entsprechenden Ordner ablegen, überholte Dokumentation entfernen oder als ungültig kennzeichnen.
- Datenträger für das Softwarearchiv in der Dokumentation aktualisieren, alte Datenträger archivieren oder vernichten.
- Nach zwei bis drei Wochen veralteten Treiber oder Software aus dem Archivierungsverzeichnis im Netzwerk löschen, wenn sichergestellt ist, dass die neue Version funktioniert.

Dieser Ablauf ist natürlich nur sehr grob gehalten, zeigt aber nichtsdestotrotz, wie wichtig es ist, strukturiert bei Veränderungen vorzugehen. In Zeiten, in denen die IT für ein Unternehmen lebensnotwendig geworden ist und ein Ausfall zur Insolvenz führen kann, ist es nicht mehr angebracht, mal eben ein Service Pack zu installieren und zu hoffen, dass danach alles wie gehabt funktioniert. Wenn nie Probleme auftauchen, funktioniert dieses Vorgehen natürlich. Allerdings reicht oft ein einziges Problem nach einer Softwareinstallation, damit ein Unternehmen unnötig Daten verliert oder Mitarbeiter längere Zeit nicht mehr arbeiten können. Definieren Sie den Workflow, wie es für Ihr Unternehmen notwendig erscheint, und lassen Sie sich diese Vorgehensweise von der Geschäftsleitung oder den Verantwortlichen genehmigen bzw. ergänzen.

Welche Ausfälle kann es geben?

Der nächste Schritt eines Ausfallkonzepts besteht darin, genau zu überlegen, was alles passieren kann. Hier sollten Sie so detailliert wie möglich vorgehen. Wenn Sie auch hier auf Murphys Gesetz vertrauen, wird nämlich genau das schief gehen, was Sie nicht beachtet und berücksichtigt haben. Setzen Sie sich mit allen Kollegen in der IT zusammen und führen Sie ein Brainstorming durch. Lassen Sie Ihrer Fantasie freien Lauf und schreiben Sie alle Probleme auf, die auftreten können. Dieser Vorgang bildet die Basis eines Ausfallkonzepts. Wenn Sie an dieser Stelle etwas vergessen, fehlt später genau für diesen Bereich das entsprechende Ausfallkonzept. Bei dieser Auflistung sollten Sie

zunächst zwischen physischen Ausfällen der Netzwerkinfrastruktur und Ausfällen der Software oder der Server selbst unterscheiden.

Ausfall der Netzwerkinfrastruktur

Die erste Überlegung bezieht sich auf den Ausfall der Infrastruktur. Hier gilt es zu berücksichtigen, was alles ausfallen kann – ohne die Server einzubeziehen. Erfahrungsgemäß sollten bei diesen Punkten folgende Sachverhalte berücksichtigt werden:

- Der Strom kann ausfallen (Stichwort USV).
- Ein Einbrecher kann in den Serverraum eindringen und den Raum beschädigen.
- Ein Switch kann ausfallen.
- Eine oder alle Leitungen zu den Niederlassungen können ausfallen.
- In den Niederlassungen kann ein Switch ausfallen oder ein Einbrecher die Netzwerkgeräte oder Server entwenden.
- Die Router zu den Niederlassungen können ausfallen.
- Bei Funknetzwerken können einzelne oder alle Access Points ausfallen.
- Ein Brand kann im Unternehmen ausbrechen.
- Ein oder mehrere Netzwerkdrucker können ausfallen (zwar nicht lebensnotwendig, aber im Rechnungslauf der Buchhaltung sicherlich problematisch).
- Ein Bandgerät zur Datensicherung kann ausfallen.
- Durch Umbauarbeiten werden die Netzwerkkabel in einem Stockwerk beschädigt.

Sie können sich noch weitere mögliche Probleme ausdenken. Was die Netzwerkinfrastruktur betrifft, haben sicherlich die Netzwerkkabel und die Switches das größte Gefahrenpotential. Sie können das beste Ausfallkonzept für die Server erstellen, wenn aber die Netzwerkswitches nicht mehr funktionieren, kann niemand mehr arbeiten. Erfassen Sie alle möglichen Ausfälle und welche Probleme sich aus ihnen ergeben können. Ein Beispiel ist der Einbrecher im Serverraum, der die Switches und Router entwendet (Server werden erst später berücksichtigt).

Ausfall einzelner Server einplanen

Neben der Netzwerkinfrastruktur sollten Sie für jeden Einzelnen Ihrer Server erfassen, was alles passieren kann. Beispiele können sein:

- Das Netzteil eines Servers funktioniert nicht mehr.
- Die Hauptplatine oder Arbeitsspeicher eines Servers kann defekt sein.
- Ein oder mehrere Datenträger können beschädigt sein.
- Die Internetverbindung kann getrennt werden.
- Eine Software oder ein Dienst kann nicht mehr starten (zum Beispiel nach Absturz oder Installation eines Updates).
- Die Exchange-Datenbank kann zerstört sein.
- Der Server fällt aus unbekannten Gründen komplett aus.
- Eine Netzwerkkarte funktioniert nicht mehr.

- Das Betriebssystem startet nicht mehr (Bluescreen).
- Ein RAID-Controller wird defekt.
- Ein SAN kann Probleme beim Zugriff bereiten.
- Ein Server wird zerstört oder gestohlen.
- Alle Server oder mehrere fallen auf einmal aus, zum Beispiel durch Wasserschaden oder einen Brand.
- Ein Server in den Niederlassungen startet nicht mehr.
- Ein oder mehrere Server müssen abgeschaltet werden, um die thermische Belastung zu verringern (extremer Hochsommer oder Ausfall der Klimaanlage).

Auch diese Liste lässt sich fortsetzen. Denken Sie genau nach, welcher einzelne Server bzw. welche Komponenten des Servers bei Ihnen ausfallen können. Gehen Sie so lückenlos wie möglich vor und fassen Sie potentielle Probleme zusammen. Im Anschluss daran liegt ihnen eine schriftliche Dokumentation aller möglichen Ausfälle vor, die als Basis für das Ausfallkonzept dient.

Folgen für das Unternehmen abschätzen

Im nächsten Schritt erfassen Sie, welche Probleme die Ausfälle im Einzelnen bewirken und welche Abteilungen betroffen sind.

Auswirkungen auf die einzelnen Abteilungen

Angenommen, der Server, auf dem die Buchhaltungssoftware installiert ist, fällt aus. Das heißt, die Buchhaltung kann nicht mehr arbeiten. Setzen Sie sich mit der Buchhaltung zusammen und halten Sie genau fest, was der Ausfall für diese Abteilung bedeutet und welche Arbeitsprozesse des Unternehmens gestört werden. Im Fall der Buchhaltung können das Lohnzahlungen, Rechnungszahlungen, Monatsabschlüsse etc. sein. Sie müssen davon ausgehen, dass der Ausfall immer zum schlechtesten Zeitpunkt eintritt, ein weiteres Gesetz von Murphy. Diese Schritte müssen Sie für jeden Server durchführen. Wenn zum Beispiel der Exchange Server nicht mehr funktioniert, kann niemand im Unternehmen mit E-Mail arbeiten. Aber was heißt das für die einzelnen Fachabteilungen? Für jede Abteilung muss dokumentiert werden, welche Prozesse gestört werden. Es geht hier noch nicht darum, eine Lösung zu finden, sondern nur darum, sämtliche Auswirkungen der einzelnen Ausfälle festzustellen.

Maximale Ausfalldauer festlegen

Beim nächsten Schritt geht es darum, mit sämtlichen Abteilungsleitern festzulegen, für welchen Zeitraum diese Prozesse maximal unterbrochen sein dürfen. Hierbei gilt es realistisch festzulegen, welchen maximalen Ausfall das Unternehmen verkraften kann. Wenn zum Beispiel der Einkauf nicht mehr funktionsfähig ist und keine Ware bestellen kann, könnte unter Umständen auch der Verkauf die Kunden nicht mehr beliefern. Jede Abteilung hat solche Prozesse, die teilweise von einem oder mehreren Servern abhängen. Sie werden recht schnell erkennen, wie abhängig ein Unternehmen von der IT ist und wie fahrlässig es ist, kein Ausfallkonzept zu haben. Nachdem Sie diese maximale Ausfalldauer festgehalten haben, ist es sehr wichtig, mit Verantwortlichen im Unternehmen, im Mittelstand normalerweise der Geschäftsführer, bei Aktiengesellschaften der CIO

(Chief Information Officer), eine definitive Aussage und Entscheidung herbeizuführen, wie lange ein Ausfall genehmigt werden kann. Natürlich werden auch an dieser Stelle oft Forderungen nach 100-prozentiger Verfügbarkeit laut, die aber nach ersten Kostenschätzungen für gespiegelte Rechenzentren, SANs und Cluster schnell wieder zurückgenommen werden. Wichtig an dieser Stelle ist, dass der Verantwortliche im Unternehmen die Gefahren, die Sie erfasst haben, und die Auswirkungen auf die Prozesse kennt. Es ist die Aufgabe des Geschäftsführers, eine schriftliche Anweisung zu geben, welche der genannten Prozesse für einen fest definierten Zeitraum ausfallen können. Auch der maximal mögliche Datenverlust der einzelnen Server muss festgelegt werden. Erst nachdem ein Verantwortlicher im Unternehmen genau vorgegeben hat, was er akzeptiert und was nicht, natürlich schriftlich, kann ein seriöses Ausfallkonzept erstellt werden.

Dem Geschäftsführer muss klar sein, dass an dieser Stelle investiert werden muss. Aus diesem Grund kann es hilfreich sein, wenn Sie vor dem Gespräch mit dem Geschäftsführer aufgrund der Informationen der Abteilungen und der Abteilungsleiter ganz grob Preise schätzen und Maßnahmen erarbeiten, die durchgeführt werden können. Nach Festlegung der Ausfallzeiten durch den Geschäftsführer muss ein Konzept mit einem genauen Budgetplan erstellt werden, auf dem das Ausfallkonzept beruht. Diese maximalen Ausfallzeiten müssen von den Abteilungsleitern ebenfalls gegengezeichnet werden, damit bei einem Ausfall sichergestellt ist, dass der Abteilungsleiter mit dem Ausfall eines Prozesses für zum Beispiel zwei Tage auch einverstanden war. Oft legt der Abteilungsleiter für einen Prozess eine kürzere maximale Ausfallzeit fest als der Geschäftsführer. Der Abteilungsleiter muss daher über die Entscheidung des Geschäftsführers informiert werden. Natürlich kann eine Besprechung der IT-Abteilung, der Abteilungsleiter und des Geschäftsführers sinnvoll sein. Dabei kann gemeinsam eine Entscheidung getroffen und anschließend ein Ergebnisprotokoll an alle Teilnehmer verschickt werden. Ein IT-Leiter oder Berater sollte niemals selbständig solche Entscheidungen treffen, sondern immer den Verantwortlichen des Unternehmens in die Pflicht nehmen. Nur dadurch ist im Notfall sichergestellt, dass die Abteilungsleiter oder der Geschäftsführer genau informiert sind, welche Maßnahmen zu ergreifen sind.

Erstellen eines Ausfallkonzepts

Inzwischen haben Sie ein stabiles Fundament, auf dem Sie Ihr Ausfallkonzept aufbauen können. Sie haben alle möglichen Ausfallszenarien mit den IT-Spezialisten des Unternehmens definiert. Sie haben mit den Fachabteilungen die Folgen und die möglichen Auswirkungen auf die Abteilung und das Unternehmen besprochen. Schließlich hat ein Entscheider im Unternehmen festgelegt, welche maximalen Ausfallzeiten und Datenverluste akzeptiert werden. Erst dann und mit diesem Fundament können Sie beginnen, ein seriöses Ausfallkonzept zu erarbeiten.

Festlegen der Ausfallzeiten für einzelne Komponenten und Server

Der nächste Schritt besteht darin, dass Sie die Definition der maximalen Ausfallzeiten für die einzelnen Prozesse im Unternehmen bis auf die beteiligten Server und die Infrastruktur herunterbrechen.

Beispiel: Wenn in der Planung des Ausfalls der Geschäftsführer festlegt, dass der Rechnungszahlungslauf in der Buchhaltung maximal um drei Tage verzögert werden darf, müssen Sie alle Komponenten, die diesen Prozess betreffen, so absichern können, dass eine maximale Ausfallzeit von drei Tagen zusammenkommt. Das können zum Beispiel für diesen Server folgende Komponenten sein:

- Ausfall eines Switch
- Ausfall des Netzwerkdruckers, der die Rechnungen ausdruckt

- Ausfall der Software oder des ganzen Servers der Buchhaltung
- Ausfall der Domänencontroller, sodass sich niemand mehr anmelden kann
- Stromausfall im Unternehmen
- Totalzerstörung des Buchhaltungsservers

Das sind nur einige Beispiele, die Sie für diesen Prozess berücksichtigen müssen. Von den Netzwerkswitches hängen natürlich noch weitere Prozesse ab. Wenn zum Beispiel einer dieser Prozesse nur für einen Tag ausfallen darf, müssen Sie die Switches innerhalb eines Tages wieder ans Laufen bringen. Durch diese konsequente Analyse der einzelnen Prozesse und damit verbundenen Geräte haben Sie am Ende eine Auflistung darüber, welche Geräte, welcher Server und welche Software für welchen Zeitraum ausfallen darf. Anhand dieser Informationen müssen Sie für jeden einzelnen Server, jedes Netzwerkgerät, jeden Drucker, eben für alles, was einen Ausfall dieses Prozesses bewirken kann, einen Ausfallplan entwickeln. Wenn zum Beispiel ein Server nur halbe Tage ausfallen darf, macht ein Servicevertrag, bei dem ein Techniker erst am nächsten Arbeitstag kommt, keinen Sinn. In diesem Fall benötigen Sie einen Techniker nach maximal vier Stunden, besser früher. Daher muss auf dieser Basis eine exakte Aufgabenliste erstellt werden. Nachdem die Aufgaben genau definiert sind, welches Gerät in welchem Zeitraum wiederhergestellt werden muss, geht es an die Konzeptionierung der Ausfallsicherheit. Sie sollten die Geräte physisch nur so weit herunterbrechen, wie es möglich ist.

Beispiel: Beim Server eines Markenherstellers müssen Sie nicht den Ausfall jeder einzelnen Komponente berücksichtigen und Ersatzteile kaufen, da dieser Service durch den Technikersupport abgedeckt wird. Sie sollten sich aber bei den Komponenten, auf die Sie Einfluss haben, frühzeitig absichern. Bei Servern sind das:

- Doppelte Netzteile
- Doppelte Netzwerkkarten
- Mehrfache RAID-Controller
- RAID-Datenträger

Dem Ausfall des Arbeitsspeichers und der Hauptplatine können Sie nicht entgegenwirken. Vor allem bei der Planung einer Ersatzteilliste für Ihre Infrastruktur sollten Sie beim Hersteller Ihres Servers nachfragen, in welchem Zeitraum eine neue Hauptplatine oder ein neuer Arbeitsspeicher geliefert werden kann. Wenn Sie einen Supportvertrag mit vier Stunden Reaktionszeit abschließen, heißt das nur, dass nach vier Stunden eine Reaktion erfolgt, aber nicht automatisch eine Problemlösung. Die Servicetechniker haben oft auch keine Ersatzteile dabei, sondern müssen Hauptplatinen oder RAID-Controller erst bestellen. Wenn dieser Bestellvorgang länger als die maximale Ausfalldauer ist, müssen Sie den Ausfall des Servers zusätzlich absichern.

Sobald Sie eine vollständige Liste haben, welche Komponenten bei Ihnen ausfallen dürfen, können Sie auf dieser Grundlage für eine Notfallkonzeption sorgen. Zunächst benötigen Sie jedoch die Aufstellung dieser einzelnen Komponenten.

Erstellen des Ausfallkonzepts für die einzelnen Komponenten

Im Anschluss daran legen Sie fest, wie Sie die einzelnen Komponenten innerhalb des definierten Zeitraums wieder zum Laufen bringen. Hierbei können Sie nach vier Gesichtspunkten vorgehen:

- Ausfall einzelner Geräte der Netzwerkinfrastruktur oder sonstiger Hardware
- Ausfall eines kompletten Servers

- Ausfall von Software
- Mehrere Ausfälle infolge von Katastrophen wie Wasserschaden, Brand, Einbruch oder Vandalismus

Ein Ausfallkonzept baut immer auf diesen vier Punkten auf. Sie sollten daher Ihre Maßnahmenliste entsprechend aktualisieren und genau aufteilen.

Beispiel: Wenn es sich bei Ihrem Buchhaltungsserver um einen Server mit nur einem Netzteil, einer Netzwerkkarte, ohne RAID und Service handelt, müssen Sie für entsprechende Ersatzteile, neue Serviceverträge oder einen neuen Server sorgen. Bei Katastrophen, bei denen der ganze Serverraum betroffen ist, hilft nur die Auslagerung der Server, ein gespiegeltes Rechenzentrum oder ein SAN. Wenn eine Software auf einem Server nicht mehr läuft, helfen keine Ersatzteile, sondern die Software muss so schnell wie möglich wieder zum Laufen gebracht werden. Genau um diese Aufteilung geht es hier. Sie müssen entscheiden, welche Probleme Sie durch Lagerung von Ersatzteilen lösen, für welche Sie größere Investitionen vornehmen müssen (Spiegelung eines Rechenzentrums zum Beispiel) und welche durch Ausfallserver, Datensicherung oder Schulung abgefangen werden können.

Ausfall einzelner Geräte abfangen

Alle physischen Ausfälle können Sie leicht beeinflussen. Wenn ein Switch in Ihrem Unternehmen ausfällt und Sie nicht genügend Steckplätze auf den anderen Switches freihaben, vielleicht sogar nur einen einsetzen, dann sollten Sie schleunigst einen zusätzlichen Switch planen, der zur Ausfallsicherheit dient. Idealerweise verteilen Sie die Anschlüsse auf die beiden Switches, damit Sie auch sicher sein können, dass beide Switches im Notfall funktionieren. Beim Ausfall eines Switch müssen Sie nur die gesteckten Anschlüsse in den anderen Switch stecken und alle können wieder arbeiten. Genau nach dieser Vorgehensweise müssen Sie überprüfen, welche Ausfälle Sie auf einfache Art abfangen können. Switches können so geplant werden, dass der Ausfall eines Switch durch die anderen abgefangen werden kann. Auch beim Ausfall einer USV kann so verfahren werden, indem die Server auf mehrere USVs verteilt werden. Selbst gebaute Server erfordern entsprechende Ersatzteile der Komponenten am Lager. Aus diesem Grund sind Markenserver mit Supportverträgen bei Ausfallkonzepten längerfristig sehr viel sicherer und günstiger. Überlegen Sie genau, welche Hardware Sie einfach doppelt kaufen können, um dadurch einen Ausfall zu verhindern. Auch der Ausfall einer Klimaanlage im Serverraum gehört zu einem Ausfallkonzept. Statt einer großen Klimaanlage sollten Sie besser zwei mittlere installieren. Fällt eine aus, wird zwar die Temperatur nicht mehr so niedrig sein wie vorher, aber auf jeden Fall deutlich niedriger als ohne. Auch Rauchmelder sollten immer doppelt vorhanden sein. Ihnen fallen sicherlich noch weitere Geräte ein, die Sie in Ihre Vorsorgemaßnahmen einbeziehen können. Fällt erst einmal ein Gerät aus und Sie bekommen in angemessener Zeit kein neues, ist der Ärger vorprogrammiert. Daher lieber in die Zukunft investieren und die Kosten kalkulierbar halten.

Ausfall von Servern

Dieser Part ist im Grunde genommen der wichtigste von allen. Sie müssen genau festlegen, was zu tun ist, wenn ein einzelner Server komplett ausfällt. Der erste und wichtigste Schritt in dieser Situation ist, dass Sie die Supportverträge überprüfen und abklären, in welchem Zeitraum ein Techniker vor Ort ist und wie lange die Bestellung von Ersatzteilen dauert. Wenn Sie nicht hundertprozentig sicher sein können, dass die Hardware nach entsprechender Zeit wieder lauffähig ist, müssen Sie das in Ihre Planung mit einbeziehen. Beachten Sie, dass bei einem Server nicht nur ein Teil der Hardware ausfallen kann, sondern er unter Umständen neu installiert werden muss und alle Daten der

Datensicherung zurückgespielt werden müssen. Aus diesem Grund ist auch die genaue Festlegung des maximalen Datenverlustes wichtig. Wenn Sie zum Beispiel nachts um 22:00 Uhr die Daten auf verschiedenste Weise sichern und dabei ein ideales Datensicherungskonzept verwenden, ist so weit alles in Ordnung. Aber was ist, wenn der Server um 21:00 Uhr komplett ausfällt? Im schlimmsten Fall müssen Sie den Server neu installieren und die Datensicherung zurückspielen. Allerdings geht in diesem Beispiel die Arbeit eines ganzen Tages vollständig verloren, da Sie nur die Datensicherung des Vortages zurückspielen können. Wenn die Geschäftsführung sagt, das sei kein Problem, und Ihnen das schriftlich gibt, ist von Seiten der IT alles in Ordnung. Wenn allerdings festgelegt wird, dass maximal ein halber Tag verloren gehen darf, müssen Sie in Ihr Datensicherungskonzept eine Sicherung des Datenbankservers um die Mittagszeit einplanen. Diese Sicherung wird zwar das System ausbremsen, aber mittags werden sicherlich nicht viele Mitarbeiter arbeiten. Wenn die Sicherung nur wenige Minuten dauert, wäre es eventuell auch sinnvoll, die Dienste für diese Datensicherung währenddessen nicht zur Verfügung zu stellen. Aber auch das muss ein Geschäftsführer erst genehmigen. Wenn überhaupt keine Daten verloren gehen dürfen, hilft nur der Einsatz eines gespiegelten Datenspeichers in Echtzeit und ein gespiegeltes Rechenzentrum mit verteiltem Cluster oder eine sonstige Hochverfügbarkeitslösung. Da im Fall eines Ausfallkonzepts für Server oft ein zusätzlicher Server gekauft werden muss oder sonstige Investitionen vorgenommen werden müssen, sollten Sie innerhalb des Konzepts immer drei Möglichkeiten anbieten:

- Günstige Variante, die sehr wenig oder gar nichts kostet, dafür aber längere Ausfallzeiten und höhere Datenverluste nicht abfangen kann. Allerdings ist eine solche Lösung immer noch besser als gar keine.
- Mittlere Variante, bei der Ausfallzeiten und Datenverlust kalkulierbar bleiben und die Kosten nicht so hoch sind. Bei einem Warenwirtschaftsserver könnte das ein zweiter Server sein.
- Hochverfügbarkeitslösung, bei der die geforderte Sicherheitsstufe maximal eingehalten werden kann, zum Beispiel ein gespiegeltes Rechenzentrum oder ein SAN. Auch bei einer hochverfügbaren Lösung sollten Sie sich keine unnötige Arbeit machen und Vorschläge ausarbeiten, von denen Sie bereits bei der Erstellung wissen, dass sie nicht genehmigt werden. Sie sollten festlegen, was Sie als Unternehmer maximal ausgeben würden und was sich die Firma überhaupt leisten kann. Ein Mittelstandsunternehmen mit 200 Mitarbeitern wird nur selten ein gespiegeltes Rechenzentrum in einem atombombensicheren Keller aufbauen können.

Am Ende muss wieder der Geschäftsführer entscheiden, für welche Server er welches Ausfallkonzept genehmigt. Generell lässt sich sagen, dass der beste und bezahlbarste Ausfallschutz für Server einfach eine Verdoppelung ist. Wenn Sie nur einen Exchange Server haben, sollten Sie zwei einsetzen. Bei diesem Szenario können bei Ausfall eines Servers zumindest noch 50 % der Mitarbeiter arbeiten. Setzen Sie drei ein, sind es schon 66,66 %. Genau in diesem Rahmen sollten Sie in Bezug auf alle Server denken. Cluster können Sie auch für andere Zwecke einsetzen. Allerdings ist der pure Einsatz eines Clusters noch lange kein Garant dafür, dass der Server nicht ausfällt. Einen hundertprozentigen Schutz erreichen Sie durch einen Cluster auch nicht.

Ausfall von Software auf den Servern

Ein Server muss nicht unbedingt komplett ausfallen, sondern es ist auch möglich, dass nur einzelne Serversoftware beeinträchtigt ist. Im Fall von Exchange kann es durchaus passieren, dass der Server noch läuft, aber die Exchange-Dienste nicht mehr starten, weil die Datenbank defekt ist. Auch für diesen Fall muss festgelegt werden, wie lange Exchange als Funktion und wie lange die Datenbank mit den E-Mails und den Kalendereinträgen oder öffentlichen Ordnern nicht zur Verfügung stehen darf. Vor allem der Ausfall eines Exchange Servers kommt recht oft vor. In diesem speziellen Fall

kann die Reparatur der Datenbank durchaus unkalkulierbar lange dauern. Als Ausfallsicherheit kann an dieser Stelle nur helfen, die Benutzer auf möglichst viele Datenbanken und möglichst viele Server zu verteilen. Vor einer korrupten Datenbank hilft auch kein Cluster. Es muss in der Ausfallkonzeption festgelegt werden, wie hoch der Datenverlust auf dem Exchange Server sein darf. Hier gilt die gleiche Problematik wie bei dem bereits beschriebenen Ausfall des Datenbankservers, mit dem Unterschied, dass es für Exchange keine Exportskripts gibt. Zwischen dem Zeitpunkt der Datensicherung und dem Ausfall können E-Mails verloren gehen, zum Beispiel von Kunden oder Lieferanten. Daher sollte bereits frühzeitig an eine Ausfallsicherheit von Exchange gedacht werden. Ausfall einzelner Serversoftware kann auch dadurch abgefangen werden, dass die Images zurückgespielt werden, die dank des Workflows für Serveraktualisierungen vor einer Softwareaktualisierung angelegt wurden.

Meist fällt Serversoftware nur dann aus, wenn etwas am Server verändert wird. Aus diesen Gründen ist die Erstellung eines vorherigen Images sehr wertvoll. Auch der Einsatz eines zweiten Servers, auf dem die Software parallel installiert wurde, kann einem solchen Ausfall entgegenwirken. Vor allem beim Einsatz von ERP-Servern kann es sinnvoll sein, einen zweiten Ausfallserver zu betreiben, auf dem die Software parallel zur Verfügung gestellt wird. Dieser Server kann zum einen als Testserver für neue Softwarestände dienen und zum anderen als Ausfallserver, mit dem die Mitarbeiter beim Ausfall des Hauptservers arbeiten können. Auf dem Ausfallserver muss dazu lediglich die Datensicherung zurückgespielt werden, und es geht maximal ein halber Tag verloren. Diese Beispiele lassen sich unendlich fortsetzen. Sie sehen, worauf es hinaus läuft. Überlegen Sie in allen Einzelheiten, wie Sie für jeden einzelnen Serverdienst und Server einen Ausfall in angemessener Zeit kompensieren können.

Katastrophenfälle absichern

Die Absicherung von Katastrophenfällen können sich meistens nur sehr große Unternehmen leisten, da die Kosten leicht in die Höhe schnellen. Um den kompletten Ausfall eines ganzen Serverraums durch Brand, Wasserschaden, Einbruch oder Vandalismus zu verhindern, können alle Server auf zwei verschiedene Rechenzentren in verschiedenen Gebäuden aufgeteilt werden. Für jeden Server muss es einen oder mehrere Ausfallserver geben, die im jeweils anderen Rechenzentrum stehen. Auch die Daten werden mithilfe von gespiegelten SANs zwischen den Rechenzentren verteilt. Ideal ist in einem solchen Fall auch der Einsatz eines Clusters, bei dem die Knoten ebenfalls im gespiegelten Rechenzentrum verteilt werden. Kleinere Katastrophen können dadurch abgesichert werden, dass der Serverraum so gut es geht vor diesen Gefahren geschützt wird und der Server für die Datensicherung im Keller in einem speziellen Datentresor steht.

Genehmigung und Umsetzung des Konzepts

Nachdem Sie für alle Komponenten Ausfallkonzepte erstellt haben, müssen die Verbesserungen von entsprechender Stelle genehmigt werden. Sie sollten sich hier die Mühe machen und eine Präsentation erstellen, damit auch Geschäftsführer ohne starken IT-Bezug verstehen, warum Sie welche Vorschläge unterbreiten. Sie sollten Ihre Meinung äußern, welches Konzept Sie warum für das beste halten. Im Anschluss daran werden die Konzepte genehmigt und Sie können sich nach und nach an deren Umsetzung machen. Nach der Fertigstellung sollten Sie eine zweite Präsentation für die Abteilungsleiter und Geschäftsführer erstellen. Auf diese Weise werden alle darüber unterrichtet, wie die einzelnen Prozesse im Unternehmen durch die IT geschützt werden und wie die einzelnen Ausfallzeiten aussehen. Ein gut gemachtes Ausfallkonzept in einer schönen Präsentation professionell dargestellt, überzeugt Geschäftsführer und später die Banken davon, dass ein Unternehmen alles unter-

nimmt, um seine IT so sicher und stabil wie möglich zu machen. Zu einem guten Ausfallkonzept gehören eine effiziente Datensicherung und Sicherheitsstrategie des Unternehmens. Sehr wichtig ist hier, dass Sie nochmals ausführlich dokumentieren, für welche Prozesse welche maximalen Ausfallzeiten angestrebt sind. Auch den maximalen Datenverlust bei einem Ausfall sollten Sie in der Präsentation festhalten und noch einmal mit den Abteilungen und Geschäftsführern abschließend besprechen. Ganz ohne Datenverlust wird der komplette Ausfall eines Servers oder einer Exchange-Datenbank selten ausgehen. Allerdings lässt sich eine solche Problematik bereits frühzeitig planen und durch geeignete Maßnahmen umgehen. Vor allem die regelmäßige Datensicherung, stabile Server mit gut dokumentierten Änderungen, eine ganzheitliche Sicherheitsstrategie, ein guter Virenschutz mit sicherer Internetanbindung und ein durchdachtes Notfallkonzept helfen Unternehmen, Probleme in der IT möglichst effizient zu bewältigen.

IT-Sicherheit mit ITIL

Innerhalb von zahlreichen Unternehmen gehört der Einsatz von ITIL (IT-Infrastructure Library) schon fast zum Alltag. Es liegt stark im Trend die Abläufe in der IT-Abteilung im Unternehmen auf Basis von ITIL zu optimieren. ITIL ist ein Rahmenkonzept, eine Sammlung verschiedener Best-Practice-Richtlinien und Leitfäden, um das Zusammenwirken von Mitarbeitern, Prozessen und Technologie zu optimieren. ITIL steuert hauptsächlich zwei zentrale Bereiche des Service-Managements, den Service-Support (Incident-, Problem-, Configuration-, Change- und Release-Management) und Service Delivery (Service Level-, Availability-, Financial-, IT Service Continuity- und Capacity-Management). Entwickelt wurde ITIL in den späten 80er in Großbritannien und spielt mittlerweile in zahlreiche IT-Abteilungen weltweit eine sehr wichtige Rolle. Der Vorteil von ITIL ist die vollkommene Unabhängigkeit von Technologien oder Anbietern, es trägt Erfahrungen zahlreicher Experten zusammen und koordiniert diese. Das Hauptziel von ITIL ist die hauptsächlich technologieorientierte IT-Infrastruktur in eine prozess-, service- und kundenorientierte Richtung zu lenken, um das Zusammenspiel von Mitarbeitern und IT im Unternehmen optimal auszuschöpfen. Allerdings arbeiten derzeit die meisten IT-Sicherheitsexperten noch keineswegs mit dieser Standardisierung. Auch innerhalb von Unternehmen die ITIL verwenden, wird im Bereich der Sicherheit noch häufig ohne Standardisierung gearbeitet, obwohl die IT-Sicherheit grundsätzlich in ITIL berücksichtigt wird (Service Continuity Management, ISO 17799). Hauptsächlich werden die Optimierungen der IT-Sicherheit durch ITIL in der britischen Norm BS7799 erfasst. Es werden zwar keine Anleitungen für die Umsetzung geliefert, aber der Aufbau eines optimalen IT-Sicherheitsmanagements wird erläutert. Das Bundesamt für Sicherheit in der Informationstechnik gibt mit seinem IT-Grundschutzhandbuch detaillierte Vorgehensweisen vor, wie das IT-Sicherheitsmanagement zusammen mit ITIL optimiert werden kann. Sicherheitsaspekte sind in der heutigen Zeit für alle Unternehmen ein unverzichtbarer Bestandteil für einen effizienten und stabilen Betrieb der IT-Infrastruktur.

Bei der optimalen Umsetzung von Empfehlungen aus ITIL ergeben sich zahlreiche Vorteile, um auch die Sicherheits-Infrastruktur im Unternehmen zu optimieren. Es ist daher mehr als sinnvoll bereits frühzeitig das Sicherheitsmanagement in die Implementierung von IT-Service-Prozessen einzubinden. ITIL bietet die Grundlage, Verbindungen zwischen Geschäfts- und IT-Prozessen auch bezüglich von Sicherheitsfragen optimal zu gestalten. Dazu müssen allerdings alle Sicherheitsmaßnahmen auf klar definierte Prozesse und Service-Anforderungen bezogen werden. So können zum Beispiel der Service-Support und das Sicherheitsmanagement zusammen arbeiten. Das von ITIL empfohlene Service Desk für das Service Support Management kann gleichzeitig auch als Anlauf-

stelle für die Unterstützung der Anwender, zum Beispiel als Security Front Office, dienen. Alle Sicherheitsvorfälle, Störungen, die Dokumentation und die Benachrichtigung der Verantwortlichen könnte von einer solchen Gruppe verwaltet werden. Da der Service Desk ohnehin die zentrale Anlaufstelle für jeden Anwender ist, sollte hier die Verwaltung der IT-Sicherheit keineswegs ausgeklammert werden. Dadurch wird auch für das Sicherheitsmanagement im Unternehmen eine hohe Erreichbarkeit gewährleistet. Ein weiteres Beispiel sind Intrusion-Detection-Systeme (IDS) oder andere Technologien zur Beobachtung des Netzwerks, die oft ohne eine prozessuale oder organisatorische Einbindung implementiert werden. So besteht die Gefahr, dass Probleme für den IT-Betrieb entweder nicht erkannt werden oder falsch reagiert wird. Da beim Einsatz von ITIL Störungen zentral gemeldet und erfasst werden, können diese automatisch bearbeitet und überwacht werden. Warum soll das nicht auch für die IT-Sicherheits-Infrastruktur gelten? ITIL unterscheidet zwischen Störungs- und Problemmanagement. Hierzu gehören die Auditierung von Systemen, um zum Beispiel Sicherheitslücken aufzudecken, aber auch die Problemanalyse und exakte Lösungsvorschläge. Wenn das Service-Management auf Basis von ITIL durchgeführt wird, kann das Sicherheits-Management unterstützt werden, seine Verfahren zur Problemanalyse, -behebung und -vermeidung ebenfalls prozessorientiert zu gestalten. Durch diese Vorgehensweise werden sicherheitstechnische Anforderungen transparenter gestaltet und können frühzeitiger in die Entscheidungsprozesse eingebunden werden. Sicherheit wird dadurch zum Service definiert. Es können die Service Level Agreements (SLAs) um sicherheitstechnische Anforderungen erweitert werden.

Auch im Bereich des Change Management bietet sich die Integration von ITIL in die Verwaltung der Sicherheit an. Änderungen werden durch das Fachpersonal nicht mehr einfach durchgeführt, sondern zukünftig zunächst beantragt. Da auch für die IT-Infrastruktur bestimmte Verantwortungsbereiche vorliegen, kann die Verwaltung der einzelnen Prozesse genauso durch das Änderungsmanagement berücksichtigt werden, wie alle anderen IT-Technologien auch. Das kann auch umgekehrt gelten: Wenn Änderungen an der IT-Infrastruktur im Unternehmen Bereiche der Sicherheit betreffen, zum Beispiel das Anschaffen eines Funknetzwerkes oder das Patchmanagement etc., sollten auch die Verantwortlichen des Sicherheitsmanagements eingebunden werden und Änderungen planen oder freigeben. Natürlich muss hierzu festgelegt werden, welche Änderungen relevant für die Sicherheit im Unternehmen sind. Auch Bereiche die zunächst nicht mit dem Sicherheitsmanagement zu tun haben, sollten nach der Änderung auf eventuelle Sicherheitslücken überprüft werden, um kategorisch Schwachstellen in der IT-Sicherheit vermeiden zu können. Diese Synergieeffekte entstehen, wenn in das Change Management des Unternehmens auch Personen aus dem Sicherheitsmanagement einbezogen werden. Auch im Prozess der Versionsänderungen kann das Sicherheitsmanagement mitarbeiten. Neue Versionen von Applikationen oder anderen Technologien sollten bei der Einführung von neuen Varianten auf Sicherheitslücken überprüft werden. Neue Technologien der Sicherheits-Infrastruktur können in der Versionsplanung ebenfalls berücksichtigt werden. Auch hier sind deutliche Synergieeffekte zu verzeichnen. Zum einen profitiert die Sicherheit des Unternehmens davon, dass neue Versionen auf sicherheitstechnische Belange überprüft werden, zum Anderen werden neue Technologien in der Sicherheits-Infrastruktur ebenfalls durch das Versions-Management erfasst. Das Sicherheitsmanagement kann Testverfahren für Sicherheit, Stabilität und Vertraulichkeit erstellen, auf deren Basis neue Versionen getestet werden. Vor allem das Patchmanagement sollte in dieser Hinsicht optimiert werden, damit die ständigen Änderungen der Betriebssysteme und Applikationen im Unternehmen organisatorisch erfasst werden. Ein weiterer Bereich ist das Konfigurationsmanagement. Die damit verbundene Datenbank, die in den ITIL-Richtlinien empfohlen wird, kann um sicherheitstechnische Aspekte ergänzt und erweitert werden. Diese Datenbank kann wiederum für die Konfiguration der einzelnen Technologien im Sicherheitsmanagement eingesetzt werden, damit auch die Implementationen von neuen Techniken im Bereich

der Sicherheit universell abgebildet werden können. Bereits frühzeitig sollten die Anforderungen des Sicherheitsmanagements in der Datenbank des Konfigurationsmanagements einfließen. Im Bereich des Service-Delivery spielen die Sicherheitsmerkmale aller IT-Services eine erhebliche Rolle. Es müssen detaillierte Definitionen der Sicherheitsanforderungen an die IT-Prozesse dokumentiert und eingehalten werden. Dabei kann auch geregelt werden, wie die Zusammenarbeit der Nutzer dieser Services im Bereich der Sicherheit geregelt wird und wie diese bezüglich der Anforderungen an die Sicherheit Ihres Services mitarbeiten sollen. Eine der Hauptaufgaben einer konsistenten Planung der Sicherheit mit oder ohne ITIL ist die Sicherstellung der Verfügbarkeit von IT-Services. Aus diesem Grund ist es mehr als unabdingbar, dass im Bereich des Availability Managements auch Themen der Sicherheit berücksichtigt werden müssen. Hier können nicht nur die Verfügbarkeit und die Wartung von Prozessen bewertet werden, sondern auch die Risiken, Zuverlässigkeit und Vertraulichkeit, vor allem im Bereich der Auslagerung. Beim Availability Management trägt das Sicherheitsmanagement eine tragende Rolle, vor allem bei der Bewertung der Auswirkungen von Ausfällen.

Im Bereich der Hochverfügbarkeit spielt die Konzeptionierung der Sicherheit eine erhebliche Rolle. Eine Hochverfügbarkeitslösung kann noch so gut geplant sein, bei größeren Sicherheitslücken ist die Stabilität des Systems in extremer Gefahr. Aus diesem Grund können hier auch frühzeitig Maßnahmen der Prävention durch das Sicherheitsmanagement getroffen werden, um zum Beispiel Viren- oder Hackerattacken ausschließen zu können. Beim Capacitiy Management sollte das Sicherheitsmanagement dann Beachtung finden, wenn die Leistung eines Systems direkten Einfluss auf die Sicherheit hat, zum Beispiel der zentrale Server für den Virenschutz, Proxyserver, usw. Auch können Abweichungen in der Leistung eines Systems direkt von Angriffen herrühren, die frühzeitig erkannt, bzw. schon im Vorfeld vermieden werden sollten. Das Sicherheitsmanagement kann Methoden zur Verfügung stellen, mit denen Leistungseinbussen auf Grund von Attacken erkannt werden können. Das Service Continuity Management ist die hauptsächliche Beziehung von Sicherheitsmanagement und ITIL. In diesem Bereich muss eine detaillierte Rollenverteilung zwischen IT, IT-Sicherheit und dem Risikomanagement geschaffen werden, damit ein Gesamtkonzept geschaffen werden kann. Es kann eine Analyse durchgeführt werden, bei der die Sicherheitsvorgaben berücksichtigt und festgeschrieben werden. Beim Financial Management können die einzelnen Maßnahmen für die IT-Sicherheitsstruktur auf Wirtschaftlichkeit analysiert werden.

Auch die IT-Infrastruktur muss bereits unter Berücksichtigung der Sicherheitsanforderungen budgetiert werden. »Sicherheit kostet nur Geld« ist in diesem Segment oft zu hören, allerdings kostet keine Sicherheit oft mehr Geld. Natürlich ist der Return on Invest (ROI) für einzelne Techniken in der Sicherheit extrem schwer zu ermitteln, hier muss das Sicherheitsmanagement überprüfen, welche Ausgaben sinnvoll erscheinen und welche Investitionen vermieden werden können. Eine Zusammenarbeit zwischen Finanzmanagement und Sicherheitsmanagement bietet hier gute Möglichkeiten nur sinnvolle Investitionen zu tätigen. Zusammenfassend lässt sich sagen, dass die Verbindung von ITIL und Sicherheitsmanagement, wirtschaftlich und sicherheitstechnisch mehr als sinnvoll ist. Im Grunde genommen müssen dazu keine neuen Richtlinien geschaffen, sondern »nur« das Sicherheitsmanagement in die ITIL-Struktur des Unternehmens eingebettet werden.

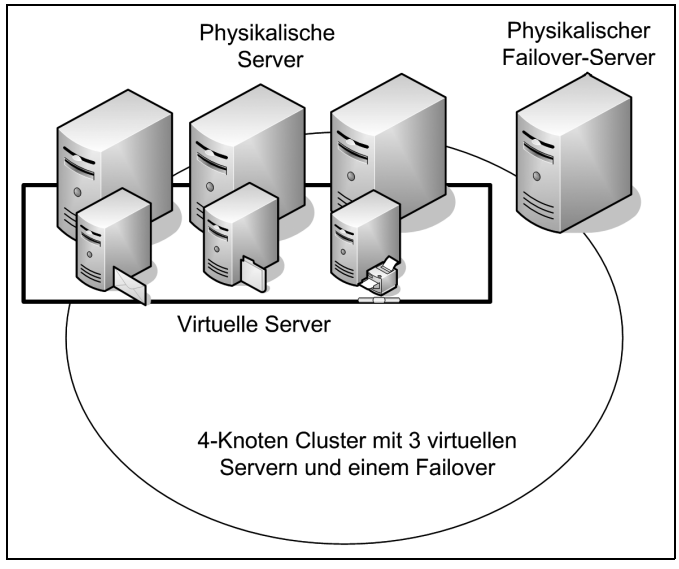
Einführung in die Hochverfügbarkeit mit Windows Server 2008

Ein Cluster ist eine Gruppe unabhängiger Computer, die jeweils die gleichen Anwendungen ausführen und beim Zugriff durch einen Client als ein einziges System dargestellt werden. Die Computer sind physisch durch Kabel und Clustersoftware miteinander verbunden. Durch das Vorhandensein dieser Verbindungen können im Cluster Probleme für den zugreifenden Client transparent behoben werden, zum Beispiel durch die Umverteilung von Aufgaben bei Ausfall eines Knotens auf einen anderen (Failover in Serverclustern) oder eine Verteilung aller zu bearbeitenden Aufgaben über einen Lastenausgleich in Netzwerklastenausgleich-Clustern, auch NLB-Cluster genannt. Durch diese Trennung unterscheiden sich Clustersysteme grundlegend von Multiprozessorsystemen, bei denen sich mehrere Prozessoren eine gemeinsame Computerperipherie teilen. Netzwerklastenausgleich (NLB) ist eine Clustertechnologie, die von Microsoft als Teil der Windows Server 2008 Enterprise und Datacenter Edition angeboten wird. NLB benutzt einen verteilten Algorithmus für den Lastenausgleich von IP-Datenverkehr über mehrere Hosts. Das führt zu einer besseren Skalierbarkeit und Verfügbarkeit unternehmenskritischer IP-basierter Dienste. Beispiele hierfür sind Webdienste, virtuelle private Netzwerke, Terminaldienste, Proxydienste und viele andere mehr. NLB kann Ausfälle von Servern automatisch erkennen und den Datenverkehr an andere Hosts umleiten. Dadurch wird eine Hochverfügbarkeit des NLB-Clusters erreicht.

Viele Firmen setzen für die Arbeit mit Exchange einen Cluster ein. Dies geschieht vor allem aus dem Grund, dass mittlerweile auch das E-Mail-System eines Unternehmens nicht ausfallen darf und so ausfallsicher wie möglich sein soll. Bei einem Cluster laufen mehrere Knoten zusammen. Dies hat den Vorteil, dass bei Ausfall eines Servers die Funktionalitäten des Clusters nicht beeinträchtigt werden, da die anderen Server dessen Dienste auffangen. Allerdings ist die Konfiguration eines Clusters alles andere als einfach. Mit einem Cluster ergibt sich der Nachteil, dass viele Konfigurationen, die bei einem Standalone-Server möglich sind, auf einem Cluster nur sehr schwer durchzuführen sind. Da auch der Clusterdienst eine Windows-Komponente ist, haben Sie bei einem Cluster zusätzlich einen weiteren Dienst zu verwalten, der dazu noch ungeheuer komplex ist.

Bevor Sie einen Cluster produktiv in Betrieb nehmen, sollten Sie sich ausführlich mit dessen Konfiguration befassen. Bei Exchange 2003/2007 empfiehlt Microsoft den Einsatz eines Aktiv/Passiv-Clusters. Das heißt im Klartext, dass bei einem Exchange-Cluster ein Server (Knoten) online die Exchange-Dienste zur Verfügung stellt und der zweite Knoten nur als Standby dient, wenn der Hauptknoten ausfallen sollte. Um einen Exchange-Cluster aufzubauen, benötigen Sie Windows Server 2008 Enterprise Edition oder Datacenter Edition als Betriebssystem und Exchange 2007 Enterprise Edition. Die beiden Standardserver dieser Produkte unterstützen kein Clustering. Windows Server 2008 Enterprise Edition unterstützt bis zu acht Knoten gleichzeitig in einem Aktiv/Passiv-Cluster. Unter Windows 2000 Advanced Server wurden dagegen nur zwei Knoten unterstützt. Die Ausfallsicherheit wurde deutlich erhöht. Wollen Sie einen Cluster einsetzen, sollten Sie sich zuvor bei Microsoft oder Ihrem Lieferanten vergewissern, dass die Hardware in der Microsoft Hardware Compatibility List (HCL) für Cluster aufgeführt ist.

Abbildg. 19.1 Cluster können als Hochverfügbarkeitslösung eingesetzt werden



Wenn Sie Hardware einsetzen, die nicht auf der HCL für Cluster steht, erhalten Sie keinerlei Support von Microsoft, und eine stabile Funktion kann nicht garantiert werden. Ein Cluster unter Windows Server 2008 wird in das Active Directory integriert. Bei der Erstellung eines Clusters werden die virtuellen Server als Computerobjekt in das Active Directory aufgenommen und können von Benutzern wie ein normaler Server angesprochen werden. Dadurch werden zwar keine Gruppenrichtlinien für die virtuellen Server unterstützt. Benutzer können aber mit Kerberos und Sitzungsschlüsseln deutlich sicherer arbeiten. Diese Form der Authentifizierung erlaubt es Benutzern, sich gegenüber einem Server ohne ein Kennwort zu authentifizieren. An Stelle eines Kennworts weisen Sie sich über ein Ticket aus, das Ihnen den Zugriff auf den Server erlaubt. Dies steht im Gegensatz zur NTLM-Authentifizierung, wie sie für den Clusterdienst unter Windows 2000 Server genutzt wird, der einen über das Passwort des Benutzers gebildeten Hashwert über das Netzwerk sendet. Auch wenn der Clusterdienst von Windows Server 2008 in das Active Directory integriert ist, findet keine Erweiterung des Schemas statt.

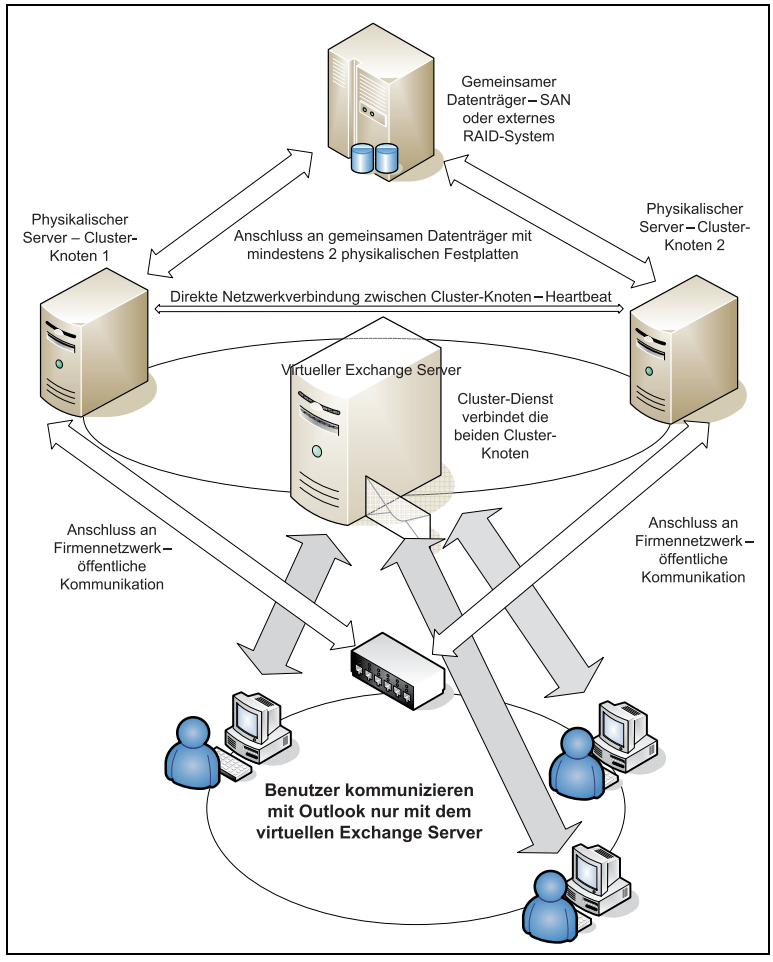
HINWEIS Die Terminologie der Clusterdienste hat sich in Windows Server 2008 noch mal geändert. Erstmalig wurde der Clusterdienst für Windows NT 4.0 entwickelt. Dieser trug als Betaversion die Bezeichnung »Wolfpack« und in der finalen Version *Microsoft Cluster Service (MSCS)*. Unter Windows 2000 Server und Windows Server 2003 hat sich die Bezeichnung zu *Server Clustering* geändert. Bei Windows Server 2008 lautet die Bezeichnung *Windows Server Failover-Clustering (WSFC)*. Diese Bezeichnungen werden auch in den verschiedenen Dokumentationen von Microsoft so geführt.

Nutzwert eines Clusters am Beispiel von Exchange Server 2007

Bevor Sie einen Cluster produktiv in Betrieb nehmen, sollten Sie sich ausführlich mit dessen Konfiguration befassen. Unter Exchange 2000 hat Microsoft noch einen Aktiv/Aktiv-Cluster empfohlen. Da diese Konfiguration aber nicht sehr populär war und auch nicht gut funktioniert hat, ist Microsoft bei Exchange 2003 umgeschwenkt und empfiehlt Aktiv/Passiv-Clustering. Das heißt im Klartext, dass bei einem Exchange 2003-Cluster ein Server (Knoten) online die Exchange-Dienste zur Verfügung stellt und der zweite Knoten nur als Standby dient, wenn der Hauptknoten ausfallen sollte. Unter Exchange Server 2007 sind nur die Server mit der Mailbox-Server-Rolle clusterfähig. Es wird auch nur noch ein Aktiv/Passiv-Cluster unterstützt. Sie können in einem Cluster ohne weiteres mehrere aktive Knoten betreiben, es muss aber mindestens ein passiver Knoten enthalten sein. Diese Rolle dient ausschließlich dem Speichern von Postfächern und öffentlichen Ordnern. Diese Rolle kann auch auf einem einzelnen Exchange-Server zusammen mit der Hub-Transport-, Client-Access- und Unified Messaging-Rolle installiert werden. Allerdings ist diese Rolle als einzige clusterfähig, alle anderen Rollen müssen durch Loadbalancing oder andere Absicherungsmethoden vor Ausfall geschützt werden. Exchange Server 2007 unterstützt mit der Single Copy Cluster (SCC)-Funktion einen Cluster für Postfachspeicher in einer Aktiv/Passiv-Clusterumgebung auf die gleiche Weise wie bereits die Vorgänger. Mit der Cluster Continuous Replication (CCR)-Funktion wird die bereits hochverfügbare Lösung Local Continuous Replication auf Cluster angepasst.

In diesem Kapitel gehen wir daher auch ausführlich auf den Aufbau eines Exchange-Clusters mit Windows Server 2008 ein. Auf Basis dieses Clusters können Sie anschließend die Installation und Verwaltung eines Single Copy Clusters (SCC), sowie der Cluster Continuous Replication (CCR) von Exchange Server 2007 testen. Um einen Exchange-Cluster aufzubauen, benötigen Sie Windows Server 2008 Enterprise Edition als Betriebssystem und Exchange Server 2007 Enterprise Edition als Exchange-Version SP1. Ohne das Service Pack 1 unterstützt Exchange Server 2007 keine Installation unter Windows Server 2008. Die Cluster-Unterstützung ist auch in Exchange Server 2007 ausschließlich der Enterprise Edition vorbehalten, Exchange Server 2007 Standard Edition unterstützt keine Clusterkonfiguration. Innerhalb eines Clusters können Sie die Funktion der fortlaufenden Datensicherung von Exchange Server 2007 dazu verwenden, einen Cluster zu installieren, der über keinen gemeinsamen Datenspeicher verfügt. Sie können zum Beispiel die Replikats-Datenbank auf den passiven Knoten des Clusters in Echtzeit replizieren lassen. Fällt der aktive Knoten aus, kann der passive Knoten gestartet werden und stellt die replizierte Datenbank nahezu in Echtzeit und ohne Datenverlust zur Verfügung. Dadurch wird die Datensicherung deutlich ausgeweitet und die Kosten für Hochverfügbarkeit werden reduziert.

Abbildg. 19.2 Darstellung eines Clusters am Beispiel von Exchange Server 2007



Neuerungen von Clustern unter Windows Server 2008

In Kapitel 1 sind wir bereits auf die Neuerungen in der Clusterfunktion von Windows Server 2008 eingegangen. In diesem Kapitel vertiefen wir das notwendige Wissen, um einen Windows Server 2008-Cluster aufzubauen und zu verwalten. Die neue Verwaltungsoberfläche der Clusterverwaltung basiert auf der neuen Microsoft Management Console (MMC) 3.0, die mit Windows Server 2003 R2 eingeführt und in Windows Server 2008 weiter verbessert wurde. Clusterverwalter können mit diesem leicht zu bedienenden und intuitiven Programm jetzt effizienter einen Cluster überwachen und verwalten. Microsoft hat bei der Konsole den Fokus auf die Verwaltung der Clusterapplikationen gesetzt, nicht in die Verwaltung des Clusters selbst. Dadurch können viele Administratoren Clusterapplikationen, wie zum Beispiel Exchange Server 2007 oder SQL Server 2005/2008 verwalten, ohne tief in die Clusterverwaltung vordringen zu müssen. In der Konsole können Ereignisse, die den

Cluster betreffen, gezielt überwacht werden, die Konfiguration wird eindeutig und leicht verständlich angezeigt, ohne durch viele Untermenüs klicken zu müssen.

Auch die Hardware des Clusters kann effizient überwacht werden. Diese neue Cluster Management Console bietet Clusterverwaltern eine neue Erfahrung. Verbessert wurden auch die Funktionen, um einen Cluster in der Befehlszeile zu verwalten, sowie die Unterstützung für WMI. Die Clusterkonfiguration kann mit dem Schattenkopie-Dienst gesichert und wiederhergestellt werden. Ebenfalls neu im Windows Server 2008-Failover-Clustering sind die Verbesserungen in der Netzwerkschicht. Ein Cluster unter Windows Server 2008 profitiert vom neuen TCP/IP-Stack und der vollen IPv6-Unterstützung. Die Kommunikation zwischen den Clusterknoten (Heartbeat) findet jetzt mit IPv6 statt. Es gibt keine Abhängigkeiten mehr von NetBIOS, sodass auch Umgebungen ohne WINS-Server oder NetBIOS-Paketen von der standardisierten Namensauflösung per DNS profitieren. Es werden keine Broadcasts mehr benötigt, was den Transport des SMB-Verkehrs deutlich verbessert.

Mit dem *Cluster-Migrationassistenten* können bestehende Windows Server 2003-Cluster leicht und effizient zu Windows Server 2008-Clustern migriert werden, sodass nicht zwingend Neuinstallationen notwendig sind. Es ist allerdings nicht möglich, dass in einem Cluster Windows Server 2003-Knoten und Windows Server 2008-Knoten betrieben werden. Es wird lediglich ein einheitlicher Betriebssystemstand unterstützt. Ebenfalls neu sind Verbesserungen in der Sicherheit eines Clusters. Der Clusterdienst läuft unter Windows Server 2008 im Kontext des LocalSystem-Kontos. Es ist nicht mehr zwingend ein eigenes Domänenkonto mit erweiterten Berechtigungen notwendig. Auch innerhalb der Clusterstrukturen hat Microsoft viele Verbesserungen in der Sicherheit eingeführt. So arbeiten Applikationen und DLLs des Clusters mit so wenigen Rechten wie möglich und haben keine Berechtigungen, mehr uneingeschränkt mit dem Netzwerk zu kommunizieren. Angriffe auf Cluster, um Berechtigungen im Netzwerk zu erhalten, werden dadurch eingeschränkt.

HINWEIS Das Quorum-Modell ist in Windows Server 2008 eine Mischung der besten Eigenschaften des bisherigen Shared Disks und des Majority Node Sets (MNS). Durch dieses neue Majority Quorum-Modell wird die Stabilität eines Clusters erhöht. Die beiden Vorgängermodelle werden durch den neuen Quorum-Typ vollkommen ersetzt, es gibt keinen Single Point of Failure mehr. Ein Cluster überlebt ohne weiteres, auch wenn er sein Quorum verliert. Dazu hält jeder Clusterknoten eine replizierte Offlinekopie des Quorums vor, mit der die Zeit ohne das Quorum überbrückt werden kann. Der MNS kann weiter verwendet werden, profitiert aber auch von den Neuerungen. Durch diese neuen Funktionen profitieren vor allem auch Cluster für Exchange Server 2007, welcher verschiedene Clusterunterstützungen mitbringt, die teilweise auf MNS aufbauen, wie zum Beispiel die Cluster Continuous Replication.

Durch die Verbesserungen in der Netzwerkschicht eines Clusters können die Knoten ein- und desselben Clusters auch sehr weit auseinander liegen. Durch dieses Geo-Clustering ist es möglich, dass sich ein Cluster über mehrere Niederlassungen erstreckt, was die Ausfallsicherheit auch bei größeren Katastrophen deutlich erhöht. Unternehmen mit einer echten Desaster-Recovery-Planung profitieren daher extrem von den neuen Funktionen. Clusterknoten müssen sich nicht mehr in einem gemeinsamen Subnetz befinden und können jetzt auch über Router zwischen verschiedenen Netzen kommunizieren. Aus diesem Grund ist es auch nicht mehr notwendig, Clusterknoten mit virtuellen LANs (VLANs) miteinander zu verbinden, was die Kosten für einen Cluster unter Windows Server 2008 weiter reduziert und die Einbindung in Desaster Recovery-Szenarien mit Geo-Clustern erhöht. Der Heartbeat-Timeout kann konfiguriert werden, sodass Clusterknoten auch über schmalbandige WAN-Anbindungen konsistent miteinander kommunizieren können. Clusterknoten können durch diese neue Möglichkeit weiter voneinander entfernt positioniert werden. Cluster, die sich in einem

gemeinsamen LAN befinden, profitieren von der Möglichkeit, den Timeout zu reduzieren, sodass der Ausfall eines Knotens noch schneller festgestellt werden kann und Wiederherstellungsaktionen in kürzerer Zeit durchgeführt werden können. Cluster mit gemeinsamen Datenträgern profitieren von der besseren Anbindung an SAN-Strukturen. Cluster unter Windows Server 2008 unterstützen serielles SCSI (SAS), iSCSI und Fibre Channel für die Anbindung von Datenträgern. Paralleles SCSI wird für gemeinsame Datenträger nicht mehr unterstützt. Es werden keine SCSI-Bus-Resets mehr verwendet, was bei Clustern mit gemeinsamen Datenträgern auf SANs viele Probleme bereitet hat.

Die generelle Verwaltung des gemeinsamen Datenträgers wurde überarbeitet und optimiert. Cluster unter Windows Server 2008 unterstützen jetzt auch GPT-Datenträger. Das Datenträger-Partitionsformat MBR (Master Boot Record) unterstützt Volumes mit einer Größe von bis zu zwei Terabyte und bis zu vier Primärpartitionen pro Datenträger (oder drei Primärpartitionen, eine erweiterte Partition und eine unbegrenzte Anzahl logischer Laufwerke). Im Vergleich dazu unterstützt das Partitionsformat GPT (GUID-Partitionstabelle) Volumes mit einer Größe von bis zu 18 Exabyte und bis zu 128 Partitionen pro Datenträger. Anders als bei Datenträgern mit dem MBR-Partitionsformat werden Daten, die für den Betrieb der Plattform zwingend erforderlich sind, in Partitionen abgelegt und nicht in Sektoren ohne Partition oder in versteckten Sektoren. Außerdem besitzen Datenträger mit dem GPT-Partitionsformat redundante Primär- und Sicherungspartitionstabellen, wodurch die Integrität der Partitionsdatenstruktur verbessert wird. Auf GPT-Datenträgern können Sie dieselben Aufgaben wie auf MBR-Datenträger durchführen.

Zusätzlicher Speicherplatz kann Clusterapplikationen zugewiesen werden, ohne dass diese offline gesetzt werden müssen. Die Eigenschaften von Ressourcen können bearbeitet werden, während diese online sind, sodass die Verfügbarkeit des Clusters deutlich erhöht wird, da Applikationen auch während der Wartung des Clusters zur Verfügung stehen. Abhängigkeiten des Cluster-Netzwerknamens können für mehrere virtuelle IP-Adressen gesetzt werden und können mit ODER-Verbindungen verknüpft werden. Microsoft bietet den Download einer Testversion von Windows Server 2008 an, mit der Partner Testumgebungen mit Clustern aufbauen können. Das Feedback dieser Tester wird in die finale Version von Windows Server 2008 integriert, sodass diese so stabil wie nur möglich ist.

Voraussetzungen für einen Cluster

Damit ein Cluster betrieben werden kann, wird eine gewisse Grundausstattung benötigt. Im folgenden Abschnitt gehen wir kurz auf die wichtigsten Punkte ein.

Clustertaugliche Hardware

Dazu gehört zunächst die Beschaffung von passender Hardware für Ihren Cluster. Diese Hardware sollte Bestandteil der Hardware Compatibilty List (HCL) für Cluster und Windows Server 2008 sein. Das System sollte mindestens folgende Komponenten beinhalten:

- Jeder der Knoten benötigt einen eigenen Controller für die Datenträger des Betriebssystems, am besten mit RAID 1 zur Absicherung der lokalen Servereinstellungen.
- Jeder Knoten benötigt einen clusterfähigen Adapter, der an den gemeinsamen Datenträger angeschlossen ist, auf den alle Knoten gleichzeitig zugreifen können, zumindest dann wenn Sie einen Cluster mit gemeinsamem Datenträger aufbauen wollen und nicht Cluster Continuous Replication (CCR) von Exchange Server 2007 verwenden, um Transaktionsprotokolle zwischen Clusterknoten zu replizieren.

- Sie benötigen für einen Cluster einen gemeinsamen Datenträger, ein SAN oder einen iSCSI-Festplattenturm, an den beide Knoten angeschlossen werden können, sowie passende Kabel für den Anschluss. An diesen gemeinsamen Datenträger muss jeder Knoten angeschlossen werden. Windows Server 2008 unterstützt keinen gemeinsamen SCSI-Bus mehr. Nur iSCSI und SANs werden unterstützt.
- In jedem Knoten sollten zwei Netzwerkkarten eingebaut werden. Eine Karte dient zur Kommunikation der Knoten untereinander (Heartbeat), die zweite dient zur Kommunikation mit den Benutzern. Idealerweise sollten die Knoten noch eine dritte Netzwerkkarte haben, die für die Kommunikation der Knoten untereinander und die Kommunikation der Benutzer zur Ausfallsicherheit dient. So ist sichergestellt, dass der Cluster auch dann weiter funktioniert, wenn eine Netzwerkkarte ausfällt. Die Netzwerkkarten auf allen Knoten sollten identisch sein.

Clustertaugliche Software

Zusätzlich zu der Hardware benötigen Sie noch die passende Software für den Aufbau des Clusters:

- Windows Server 2008 Enterprise Edition
- Exchange Server 2007 Enterprise Edition oder eine clusterfähige Edition der Software, die zusätzlich auf dem Cluster installiert werden muss
- Clusterfähige Produkte für Datensicherung und Virenschutz

Planung eines Clusters

Außer diesen Vorbereitungen müssen Sie einige Einstellungen in Ihrem Netzwerk und dem Active Directory vornehmen. Sie benötigen zum Beispiel mehrere Servernamen für den Cluster und mehrere IP-Adressen in verschiedenen Subnets:

- Legen Sie zunächst einen Namen für den Cluster als Ganzes fest. Dieser Name erhält kein Computerkonto, wird aber für die Administration des Clusters verwendet. Sie sollten einen Namen wählen, aus dem schnell deutlich wird, um was es sich handelt, zum Beispiel *EXCLUSTER*.
- Jeder physische Knoten des Clusters erhält ein Computerkonto in derselben Domäne. Daher benötigt jeder physische Knoten einen entsprechenden Rechnernamen, zum Beispiel *VCN1* und *VCN2*. Die beiden Server werden später als Mitgliedsserver in die Domäne aufgenommen.
- Des Weiteren benötigen die virtuellen Exchange-Server, die auf dem Cluster laufen, ebenfalls einen Namen. Erstellen Sie nur einen virtuellen Server, benötigen Sie natürlich nur einen Namen für den virtuellen Server. Diese virtuellen Server erhalten kein Computerkonto, sind in der Exchange-Konfiguration aber unter dem Namen zu finden, den Sie bei der Installation auswählen. Aus dem Namen sollte schnell ersichtlich sein, dass es sich um virtuelle Exchange-Server handelt. Wählen Sie zum Beispiel *EXV1*. Anwender verwenden auch diesen Namen für den Zugriff auf Exchange.
- Sie benötigen für den Cluster mehrere IP-Adressen. Jeder physische Knoten benötigt je eine IP-Adresse, der Cluster als Ganzes erhält eine IP-Adresse, jeder virtuelle Exchange-Server und die Netzwerkkarten für die private Kommunikation des Clusters erhalten je eine in einem getrennten Subnetz (wichtig!).
- Legen Sie für die Konfiguration des Clusters und von Exchange am besten ein neues Benutzerkonto in der Domäne an. Für die Installation des Clusters sollte dieses Konto Mitglied in der Gruppe der Domänen-Admins sein.

Gemeinsamer Datenträger eines Clusters

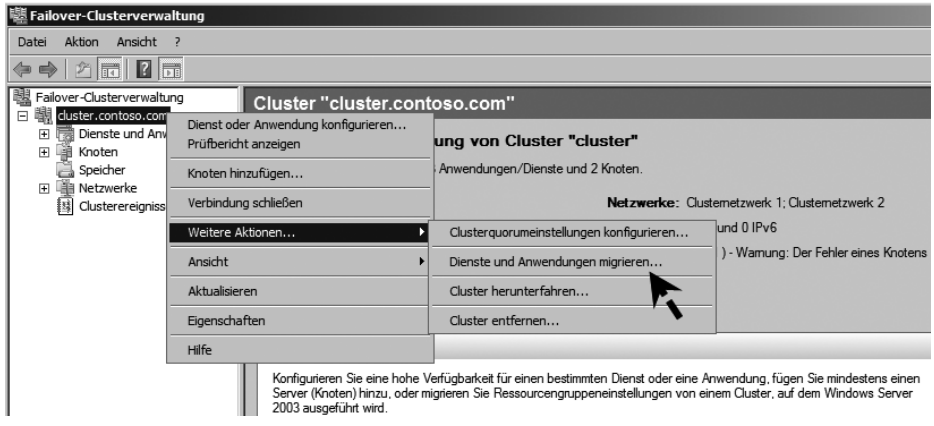
Der gemeinsame Datenträger ist später das Herz des Clusters, da auf ihm sowohl die Daten aller Benutzer als auch die Konfiguration des Clusters im Quorum gespeichert ist. Alle gemeinsamen Datenträger müssen an alle Knoten angeschlossen sein und auch von ihnen erreicht werden können, wenn Sie einen Cluster aufbauen und nicht Cluster Continuous Replication (CCR) verwenden, um Transaktionsprotokolle zwischen Clusterknoten zu replizieren.

Windows Server 2003-Cluster migrieren

Cluster, die mit Windows Server 2003 betrieben werden, können relativ leicht auf Windows Server 2008 migriert werden. Dabei empfiehlt Microsoft folgende Vorgehensweise:

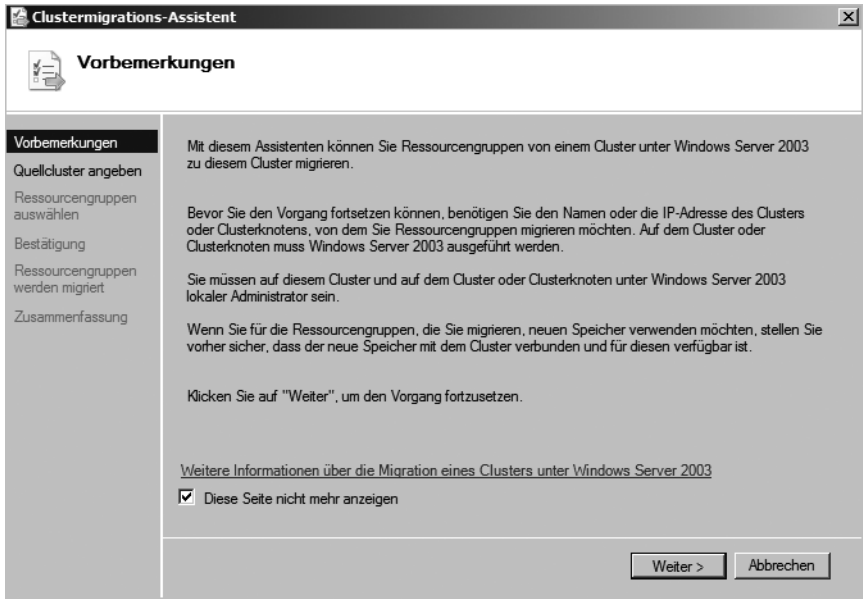
1. Verschieben Sie alle Gruppen vom zweiten Clusterknoten, damit dieser im Cluster keine Rolle mehr spielt.
2. Entfernen Sie den Knoten vom Cluster. Gehen Sie dazu folgendermaßen vor: Öffnen Sie die Clusterverwaltung auf dem aktiven Knoten. Klicken Sie mit der rechten Maustaste auf den passiven Knoten und wählen Sie *Clusterdienst beenden*. Nach kurzer Zeit wird der Clusterdienst als beendet angezeigt. Klicken Sie noch einmal auf den passiven Knoten mit der rechten Maustaste und wählen Sie dieses Mal im Kontextmenü den Eintrag *Knoten entfernen*. Es erscheint eine Warnmeldung und der Knoten wird aus dem Cluster entfernt. Haben Sie einen Clusterknoten von einem Cluster entfernt und wollen diesen Knoten erneut einem Cluster hinzufügen, funktioniert unter Umständen der Clusterdienst nicht mehr richtig. Geben Sie in diesem Fall in der Befehlszeile den Befehl *sc create clussvc* ein. Mit diesem Befehl werden die Registrierungsdaten des Clusters wiederhergestellt. Die physische Verbindung zum SAN, also dem gemeinsamen Datenträger bleibt erhalten.
3. Installieren Sie auf dem Server Windows Server 2008 neu. Erstellen Sie dann mit dem Server einen neuen Cluster mit einem neuen Clusternamen, wie in diesem Artikel beschrieben. Eine Aktualisierung von Windows Server 2003 zu Windows Server 2008 ist zwar prinzipiell möglich, allerdings rät Microsoft dringend davon ab und empfiehlt eine komplette Neuinstallation.
4. Starten Sie die Clusterverwaltung auf dem Windows Server 2008-Cluster. Klicken Sie mit der rechten Maustaste auf den Cluster und wählen Sie im Kontextmenü den Untermenübefehl *Weitere Aktionen/Dienste und Anwendungen migrieren* (Abbildung 19.3).

Abbildg. 19.3 Migrieren von Clusterdiensten zu Windows Server 2008



5. Anschließend startet der Assistent zur Migration von Clusterdiensten. Hier werden auf mehreren Seiten der Quellcluster und die dazugehörigen Gruppen ausgewählt, die migriert werden sollen (Abbildung 19.4). Mit dem Assistenten kann Gruppe für Gruppe zum neuen Cluster migriert werden. Ob die Migration funktioniert, hängt von den Ressourcen ab. Windows-interne Ressourcen wie DHCP, DNS, Datei- und Druckdienste werden problemlos übernommen. SQL Server oder Exchange kann nur übernommen werden, wenn vor der Migration die entsprechende Software auf dem zweiten Knoten installiert wurde. Da die Ressourcen auf dem ersten Knoten ohnehin erhalten bleiben und nur kopiert, nicht verschoben werden, kann die erfolgreiche Übernahme auch getestet werden. Nach der Migration sind die Ressourcen auf dem Windows Server 2008-Knoten online und müssen erst offline geschaltet werden.

Abbildg. 19.4 Cluster mit dem Clustermigrations-Assistenten migrieren



6. Nehmen Sie die Gruppen auf dem alten Cluster offline und auf dem neuen Cluster online.
7. Installieren Sie den anderen Clusterknoten ebenfalls neu und fügen Sie diesem den Windows Server 2008-Cluster hinzu. Die Migration ist an dieser Stelle abgeschlossen.

ACHTUNG Der Assistent für die Clustermigration kann nur von Windows Server 2003 zu Windows Server 2008 migrieren. Eine Migration zurück zu Windows Server 2003 kann nicht automatisiert werden.

Installation eines Clusters mit iSCSI – Testumgebung

Auf den folgenden Seiten zeigen wir Ihnen den Aufbau eines Clusters mit Windows Server 2008 am Beispiel einer Testumgebung mit Virtual PC 2007. Die Installation eines Clusters läuft in einer produktiven Umgebung so ab, wie in einer virtuellen Umgebung. Durch die Testumgebung haben Sie aber Gelegenheit, das Thema vorab testweise nachzuvollziehen.

Vorbereitungen für die Cluster-Installation

Um einen Cluster zu installieren, in diesem Fall in einer virtuellen Testumgebung, müssen mehrere Vorbereitungen getroffen werden. Für die Testumgebung werden drei virtuelle Server benötigt, die Sie am besten mit Virtual PC 2007 erstellen. Ein virtueller Server wird mit Windows Server 2003 installiert. Für eine virtuelle Umgebung reichen 256 MB Arbeitsspeicher für den virtuellen Domänencontroller, der auch als iSCSI-Target konfiguriert wird. Aus diesem Server machen Sie einen Domänencontroller, damit für den Cluster eine Domäne in der Testumgebung zur Verfügung steht. In einer produktiven Umgebung benötigen Sie für einen Cluster natürlich keine eigene Domäne. Hier werden die Clusterknoten als Mitgliedsserver zur bereits vorhandenen Domäne installiert. Auf den anderen beiden virtuellen Servern installieren Sie Windows Server 2008 Enterprise Edition und nehmen diese in die Domäne des virtuellen Domänencontrollers auf.

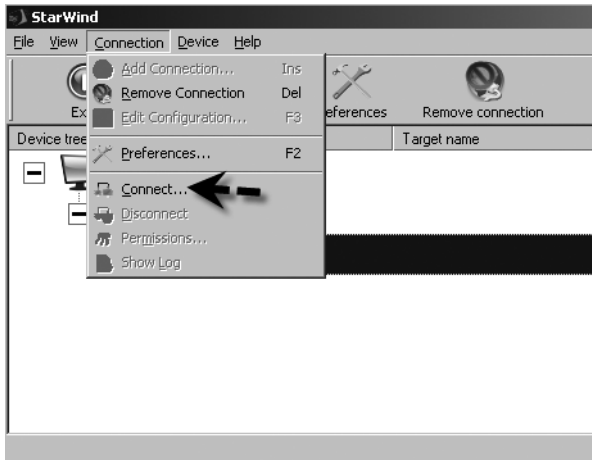
iSCSI installieren

Im Gegensatz zu Windows Server 2003 unterstützt ein Cluster mit Windows Server 2008 keinen gemeinsamen SCSI-Bus mehr. Als gemeinsamer Datenträger für den Cluster kann also kein SCSI-Speicher mehr verwendet werden. Das gilt auch für die diversen Möglichkeiten einer virtuellen Testumgebung. Hier kann für Windows Server 2003-Cluster zum Beispiel mit Virtual Server 2005 R2 ein virtueller gemeinsamer SCSI-Bus für den gemeinsamen Datenträger verwendet werden. Um einen gemeinsamen Datenträger für einen Cluster mit Windows Server 2008 zu erstellen, wird daher ein SAN (Storage Aera Network) oder ein iSCSI-Gerät benötigt. Für eine virtuelle Testumgebung ist ein virtuelles iSCSI-Laufwerk der beste Weg, auch für dieses Beispiel. iSCSI wird hauptsächlich bei NAS-Systemen eingesetzt. NAS steht für *Network Attached Storage*. Hierbei handelt es sich um Massenspeichergeräte, die direkt an das Netzwerk angeschlossen werden und mit einem eigenen Betriebssystem ausgestattet sind. Viele Betriebssysteme von NAS-Systemen sind webbasierend und im Gegensatz zu normalen Betriebssystemen deutlich eingeschränkt sowie ausschließlich auf den Einsatz als Dateiserverbetriebssystem optimiert. Ein großer Nachteil von NAS-Systemen ist die Problematik, dass die Anbindung über das LAN erfolgt. Durch diesen Umstand muss zwar keine eigene Speicherinfrastruktur aufgebaut werden, die zum Beispiel ein SAN benötigt, die Geschwindigkeit ist aber leider oft auch nicht optimal.

Manche Anwendungen haben allerdings Probleme damit, wenn der Datenspeicher im Netzwerk bereitgestellt wird und mittels IP auf die Daten zugegriffen wird, anstatt den blockbasierten Weg über SCSI oder Fibre Channel zu gehen. Zu diesem Zweck gibt es die iSCSI-Technologie. iSCSI ermöglicht den Zugriff auf NAS-Systeme mit dem bei lokalen Datenträgern üblichen Weg als normales lokales Laufwerk. Die Nachteile der IP-Kommunikation werden kompensiert. iSCSI verpackt dazu die SCSI-Daten in TCP/IP-Pakete. Für den empfangenden Server verhält sich so ein NAS in einem schnellen Gigabit-Netzwerk wie ein lokales Festplattensystem.

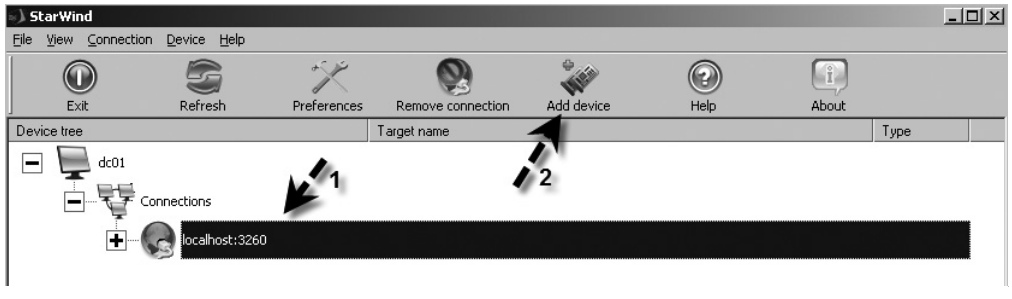
Um eine Testumgebung mit einem Windows Server 2008-Cluster aufzubauen, wird daher ein solches iSCSI-Gerät benötigt. Laden Sie sich dazu die 30-Tage-Testversion von StarWind von der Internetseite *www.rocketdivision.com* herunter. Ab der Version 3.5 unterstützt diese Software auch Windows Server 2008. Nachdem Sie die etwa 5 MB große Software heruntergeladen haben, installieren Sie diese auf dem Windows Server 2003-Domänencontroller in der Testumgebung. Nach der Installation werden über die Software drei virtuelle Laufwerke erstellt, die im Cluster als gemeinsame Datenträger und Quorum verwendet werden. Die über diese Software zur Verfügung gestellten virtuellen Datenträger sind voll clusterfähig. Um einen solchen Datenträger zu installieren, starten Sie die Software auf dem Testserver, klicken auf *Localhost* im Fenster und verbinden sich über den Menübefehl *Connection/Connect* mit dem lokalen Server (Abbildung 19.5). Als Benutzernamen verwenden Sie *test*, als Kennwort auch. Nach der Verbindung können virtuelle iSCSI-Laufwerke erstellt werden.

Abbildg. 19.5 Verbinden mit dem virtuellen iSCSI-Gerät



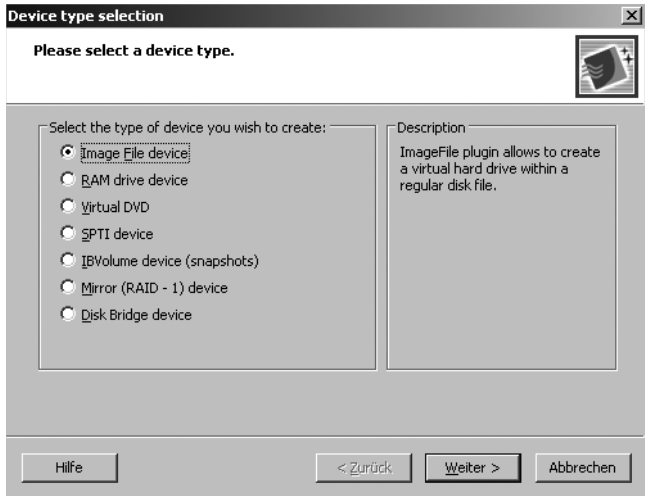
Nach der erfolgreichen Verbindung klicken Sie in der Symbolleiste auf *Add device*. Es startet der Assistent, mit dem virtuelle iSCSI-Laufwerke erstellt werden.

Abbildg. 19.6 Erstellen von virtuellen iSCSI-Laufwerken mit StarWind



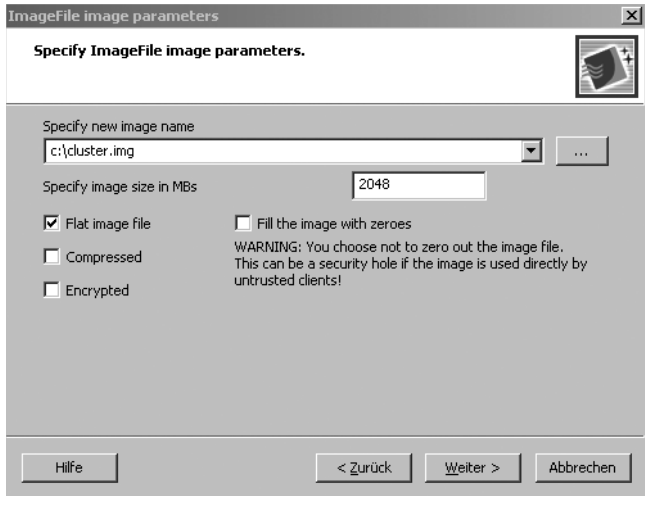
Auf der ersten Seite des Assistenten wählen Sie die Option *Image File device* aus (Abbildung 19.7). Auf der nächsten Seite starten Sie die Erstellung des Laufwerks über *Create new image*.

Abbildg. 19.7 Auswählen des virtuellen Laufwerkstyps für das iSCSI-Laufwerk



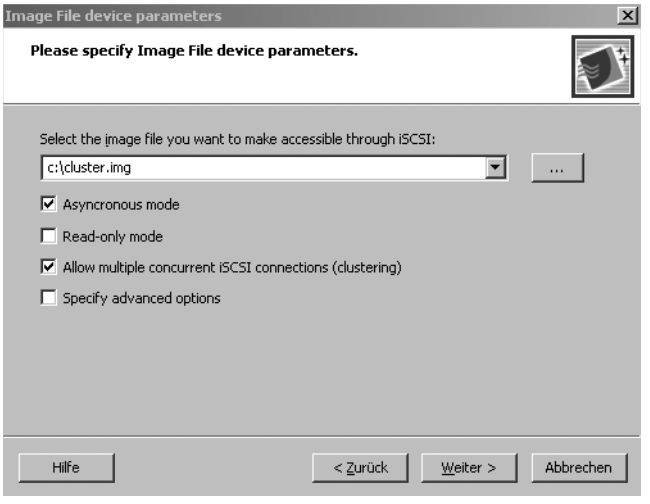
Als Nächstes müssen die Daten und der Pfad des neuen virtuellen Laufwerks angegeben werden. Als Größe für eine Testumgebung reichen 2.048 MB pro Laufwerk, als Pfad geben Sie den Pfad auf dem lokalen Server und den Namen der Cluster-Datei an. Aktivieren Sie noch das Kontrollkästchen *Flat image file* (Abbildung 19.8). Achten Sie darauf, der Datei die richtige Endung **.img* zuzuweisen und dass auf dem virtuellen Laufwerk des virtuellen Servers auch genügend Platz frei ist. Ansonsten wird bei der Erstellung des Laufwerks eine Fehlermeldung angezeigt. Am besten fügen Sie dem virtuellen Domänencontroller unter Windows Server 2003 eine zusätzliche virtuelle Festplatte mit ausreichender Größe hinzu, so etwa 16 GB.

Abbildg. 19.8 Konfigurieren der Daten für das virtuelle Cluster-Laufwerk



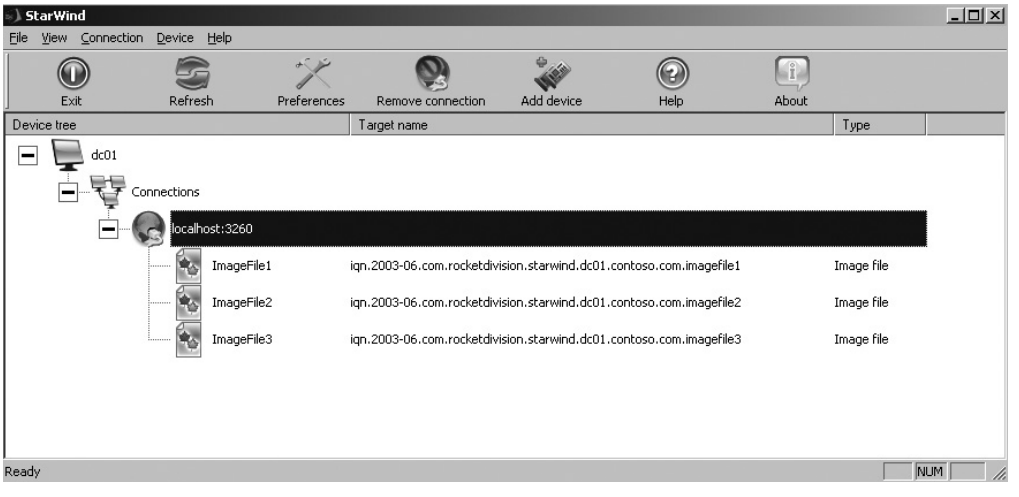
Auf der nächsten Seite des Assistenten aktivieren Sie die beiden Kontrollkästchen *Asyncronous mode* und vor allem *Allow multiple connections concurrent iSCSI connections (clustering)*. Lassen Sie das Laufwerk anschließend erstellen.

Abbildg. 19.9 Konfigurieren eines iSCSI-Laufwerks für die Cluster-Unterstützung



Für den Cluster werden drei solche virtuellen Laufwerke erstellt, alle auf dem beschriebenen Weg. Ein Laufwerk wird als Quorum verwendet, die beiden anderen als gemeinsame Clusterlaufwerke. Nach der Erstellung werden die Laufwerke in der Verwaltungskonsole von StarWind angezeigt.

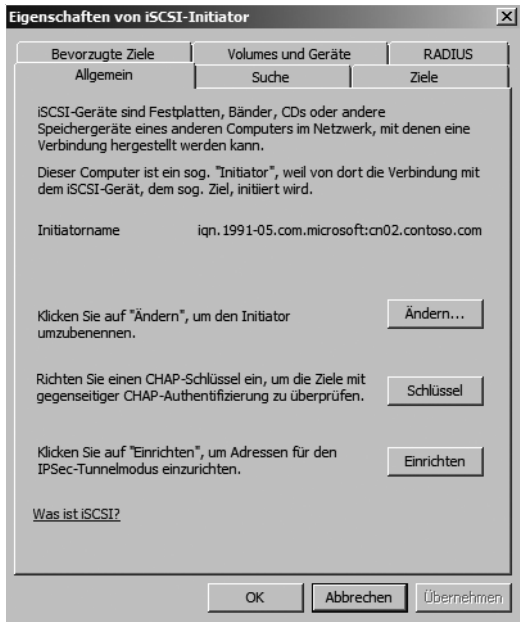
Abbildg. 19.10 Anzeigen der virtuellen iSCSI-Laufwerke für den Testcluster



Installation der Clusterknoten und des iSCSI-Initiators

Nachdem der virtuelle Domänencontroller unter Windows Server 2003 installiert wurde, der auch als iSCSI-Target dient, installieren Sie noch zwei virtuelle Windows Server 2008-Computer und nehmen diese in die Umgebung mit auf. Für einen Cluster werden mindestens zwei Server benötigt. Jeder physische Server, der an einem Cluster teilnimmt, wird als *Cluster-Knoten* bezeichnet. Zunächst müssen Sie die notwendige Hardware miteinander verkabeln. In einer virtuellen Umgebung reicht der Betrieb in einem gemeinsamen virtuellen Netzwerk (Standard bei Virtual PC 2007) und einem gemeinsamen Subnetz. Als Nächstes wird erst auf dem einen dann dem zweiten Clusterknoten eine Verbindung zu den iSCSI-Laufwerken auf dem Domänencontroller hergestellt. Dazu wird der *iSCSI-Initiator* verwendet, der zu den Bordmitteln von Windows Server 2008 gehört und über *Start/Verwaltung* gestartet wird. Beim ersten Start dieser Software muss der Start des entsprechenden Dienstes erst bestätigt und die Blockierung aufgehoben werden. Anschließend kann der Dienst über mehrere Registerkarten konfiguriert werden (Abbildung 19.11).

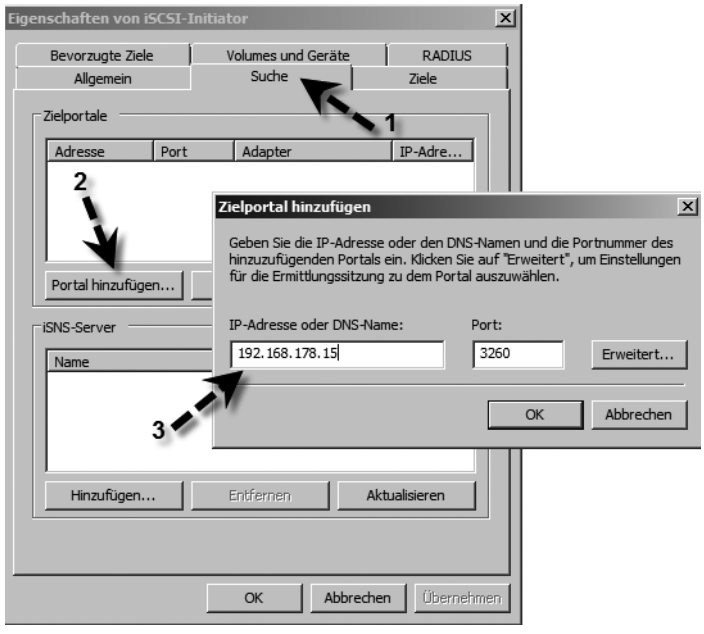
Abbildg. 19.11 Konfigurieren des iSCSI-Initiators unter Windows Server 2008



Gehen Sie zur Anbindung der Laufwerke folgendermaßen vor:

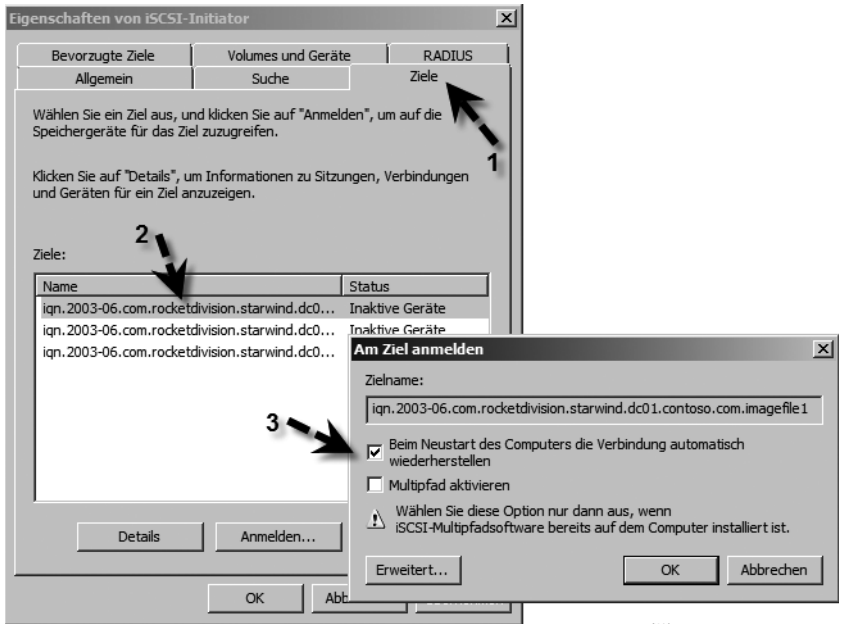
1. Wechseln Sie auf die Registerkarte *Suche*.
2. Klicken Sie auf die Schaltfläche *Portal hinzufügen*.
3. Geben Sie die IP-Adresse des Servers ein, auf dem StarWind installiert und konfiguriert wurde.

Abbildg. 19.12 Anbindung von Windows Server 2008 über den iSCSI-Initiator an ein iSCSI-Target

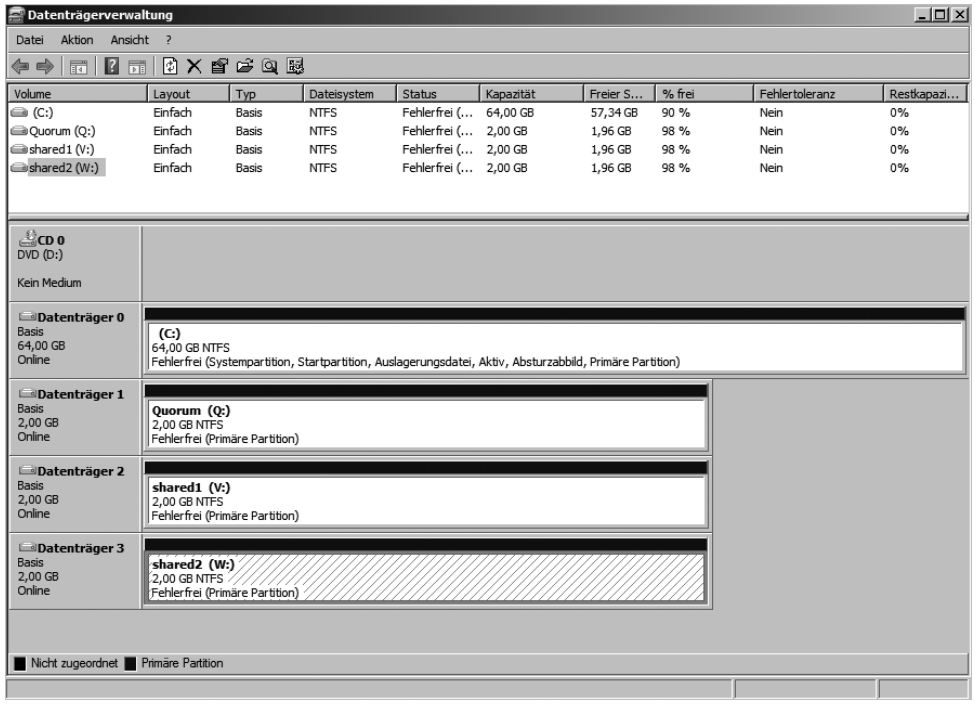


4. Wechseln Sie auf die Registerkarte *Ziele*. Hier werden jetzt die drei unter StarWind erstellten Laufwerke angezeigt (Abbildung 19.13).
5. Klicken Sie auf die Schaltfläche *Anmelden*. Damit wird eine Verbindung mit dem Gerät hergestellt. Bisher ist das Gerät nur verfügbar, aber noch nicht mit dem Computer verbunden.
6. Aktivieren Sie das Kontrollkästchen *Beim Neustart des Computers die Verbindung automatisch wiederherstellen*. Diese Option muss für alle drei Laufwerke separat eingestellt werden. Wenn der Clusterknoten neu gestartet wird, muss dieser natürlich auf die notwendigen Freigaben zugreifen können. Diese Einstellung muss auch in einer produktiven Umgebung so konfiguriert werden.
7. Nachdem die Laufwerke mit dem ersten Serverknoten verbunden wurden, müssen diese über die Festplattenverwaltung online geschaltet, initialisiert, partitioniert und formatiert werden. Wenn Sie nicht wissen, wie das geht, finden Sie die entsprechenden Hinweise in Kapitel 5. Weisen Sie den drei Laufwerken Buchstaben am Ende des Alphabets zu, also zum Beispiel *Q* für das Quorum und für die beiden gemeinsamen Datenträger *V* und *W*. Belassen Sie die Datenträger als *Basis*, eine Umwandlung in dynamische Datenträger wird für den Einsatz im Cluster nicht empfohlen (Abbildung 19.14). GPT wird an dieser Stelle nicht benötigt, da die Datenträger kleiner als 2 Terabyte sind (siehe auch Kapitel 5).
8. Gehen Sie auf dem zweiten Clusterknoten genauso vor, wie beim ersten und beginnen Sie bei Schritt 1. Da die Datenträger aber bereits auf dem ersten Knoten initialisiert und formatiert wurden, müssen Sie diesen Schritt auf dem zweiten nicht wiederholen. Auf dem zweiten Knoten reicht das Online-Schalten und das Ändern der Laufwerksbuchstaben, die mit dem ersten Knoten übereinstimmen müssen.

Abbildg. 19.13 Verbindungsaufbau zu den iSCSI-Laufwerken



Abbildg. 19.14 Konfigurieren der Datenträger für den Einsatz im Cluster



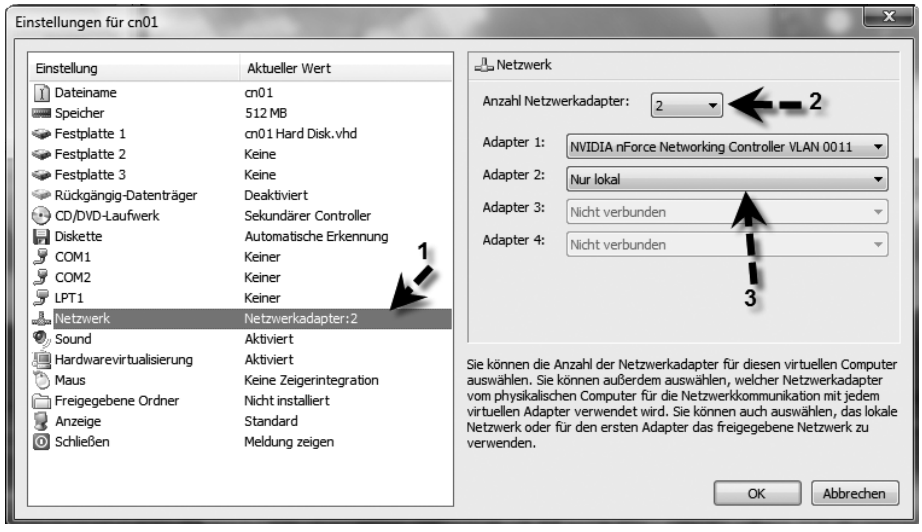
Konfiguration des Netzwerks auf den Clusterknoten

Haben Sie das Betriebssystem auf dem Server installiert und die iSCSI-Laufwerke verbunden, sollten Sie die IP-Einstellungen für die beiden Knoten vornehmen. Eine Netzwerkkarte dient dabei zur Kommunikation der Server mit dem normalen Netzwerk und sollte deshalb von den Arbeitsstationen und den Servern in Ihrem Netzwerk erreichbar sein. Hier verwenden Sie eine IP-Adresse, die sich im gleichen Subnetz wie der andere Knoten und der virtuelle Domänencontroller befindet. Diese Einstellung haben Sie bereits vorgenommen, da alle drei Server im gleichen Netzwerk betrieben werden.

Die andere Netzwerkkarte dient nur zur Kommunikation der Knoten untereinander. Clusterknoten unterhalten sich über diese private Schnittstelle und stellen fest, ob der jeweils andere Knoten noch online ist. Diese Überprüfung wird im Allgemeinen als Heartbeat bezeichnet. Benennen Sie nach der Konfiguration der Netzwerkkarte die Verbindungen um, so dass sofort ersichtlich ist, um welche es sich handelt. Empfohlen werden oft die beiden Bezeichnungen *private* und *public*. Sie sollten für die beiden Karten zudem die Option aktivieren, dass die Verbindung in der Taskleiste angezeigt wird. Dadurch haben Sie bei der Administration des Clusters immer schnell einen Überblick über die Netzwerkverbindungen. Haben Sie auf beiden Knoten die Netzwerkkarten konfiguriert, sollten Sie die Verbindung zwischen den Knoten, und die Verbindung zwischen den Knoten und Ihrem Firmennetzwerk testen. Bei der Testumgebung fahren Sie die beiden virtuellen Clusterknoten herunter und gehen in die Einstellungen der virtuellen Maschinen. Erhöhen Sie die Anzahl der Netzwerkadapter auf 2 und konfigurieren Sie die zweite Verbindung als *Nur lokal*.

Fahren Sie dann beide Clusterknoten wieder hoch, benennen Sie die Netzwerkverbindungen entsprechend um und weisen Sie der neuen, privaten Verbindung eine IP-Adresse zu, die sich in einem anderen Subnetz befindet, wie das öffentliche Netzwerk, aber im gleichen Subnetz wie die Private Verbindung zum zweiten Knoten. Testen Sie anschließend die private Verbindung zwischen den Knoten. Im nächsten Abschnitt beschreiben wir Ihnen die wichtigsten Schritte für die Kommunikation. Diese Maßnahmen müssen auch auf produktiven Clustern durchgeführt werden und gelten nicht nur für die virtuelle Testumgebung.

Abbildg. 19.15 Konfigurieren des privaten Netzwerks des Test-Clusters unter Virtual PC 2007



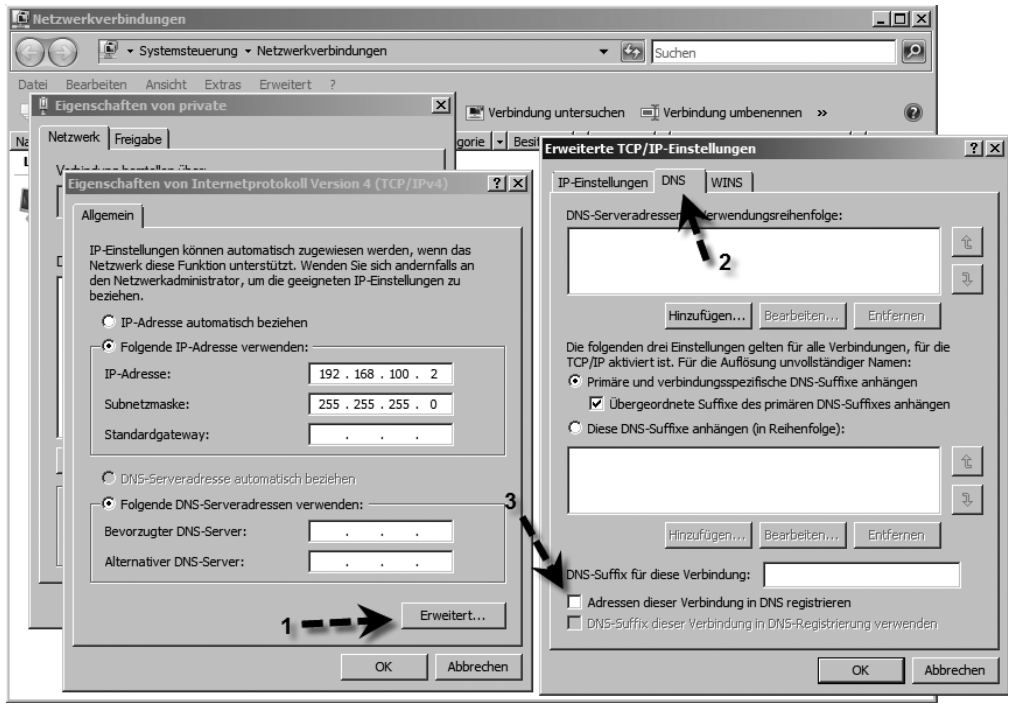
Haben Sie die virtuelle Hardware der Clusterknoten konfiguriert, führen Sie als Nächstes Konfigurationen unter Windows durch:

Starten Sie den ersten Clusterknoten *cn01* und melden Sie sich mit einem Domänenadmin-Konto an. Gehen Sie in die Verwaltung der Netzwerkverbindungen (*Start/Ausführen/ncpa.cpl*). Da Sie eine neue Netzwerkkarte hinzugefügt haben, wird in der Netzwerkverbindung diese neue LAN-Verbindung angezeigt. Die neue LAN-Verbindung 2 dient zur privaten Kommunikation der beiden Clusterknoten, dem Heartbeat. Benennen Sie daher am besten die LAN-Verbindung mit dem öffentlichen Netz in *public* um, die neu erstellte in *private*. Diese Vorgehensweise ist der Standard bei Clusterinstallationen. Dadurch können Sie bei der späteren Kommunikation oder Fehlersuche sofort erkennen um welches Netzwerk es sich handelt.

Konfigurieren Sie die Netzwerkeigenschaften der privaten Verbindung. Geben Sie dieser Verbindung zum Beispiel die IP-Adresse *192.168.100.1* und eine Subnetzmaske in einem vom öffentlichen Netzwerk getrennten Bereich. Das private Netzwerk eines Clusters sollte möglichst immer in einem eigenen Subnetz liegen, um störende Einflüsse anderer Teilnehmer am Netzwerk auszuschließen. Lassen Sie das Feld *Standardgateway* und *DNS Server* leer. Diese beiden Optionen werden beim Heartbeat auch bei der produktiven Umgebung nicht benötigt. Wichtig ist an dieser Stelle nur, dass die privaten Netzwerkkarten der beiden Clusterknoten sich untereinander auf IP-Basis unterhalten können.

Klicken Sie danach auf *Erweitert*. Gehen Sie auf die Registerkarte *DNS* und stellen Sie sicher, dass die beiden Kontrollkästchen ganz unten *Adressen dieser Verbindung in DNS registrieren* und *DNS-Suffix dieser Verbindung in DNS-Registrierung verwenden* deaktiviert sind, da DNS-Auflösungen für ein Heartbeat-Netzwerk eher stören, als die Funktionssicherheit zu erhöhen.

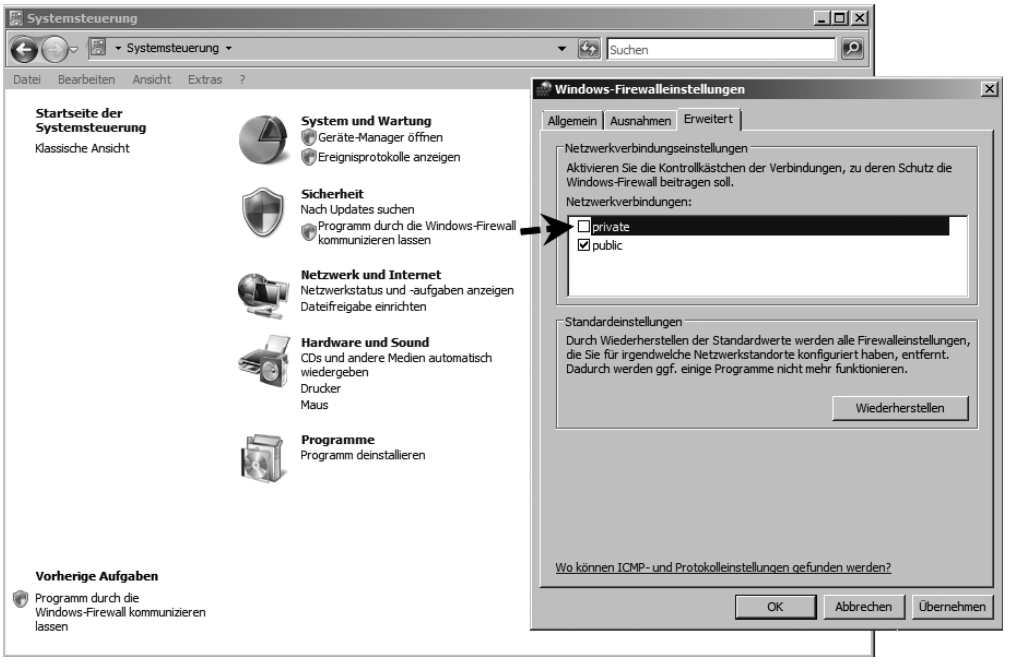
Abbildg. 19.16 Erweiterte DNS-Einstellungen für das private Cluster-Netzwerk konfigurieren



Gehen Sie danach auf die Registerkarte *WINS*. Aktivieren Sie die Option *NetBIOS über TCP/IP deaktivieren*, da NetBIOS die interne Kommunikation eines Clusters stören kann. Im Anschluss wechseln Sie innerhalb der Eigenschaften der Netzwerkumgebung mit der Schaltfläche *Erweitert* zu den erweiterten Einstellungen (Abbildung 19.16). Hier können Sie die Bindungsreihenfolge festlegen. Diese legt fest, in welcher Reihenfolge Netzwerkpakete über das Netzwerk geschickt werden und welche Verbindung zuerst verwendet wird. Ändern Sie die Reihenfolge so ab, dass die *public*-Verbindung ganz oben ist, damit die Kommunikation zu den Clients priorisiert wird. Diese Einstellung wird dringend empfohlen.

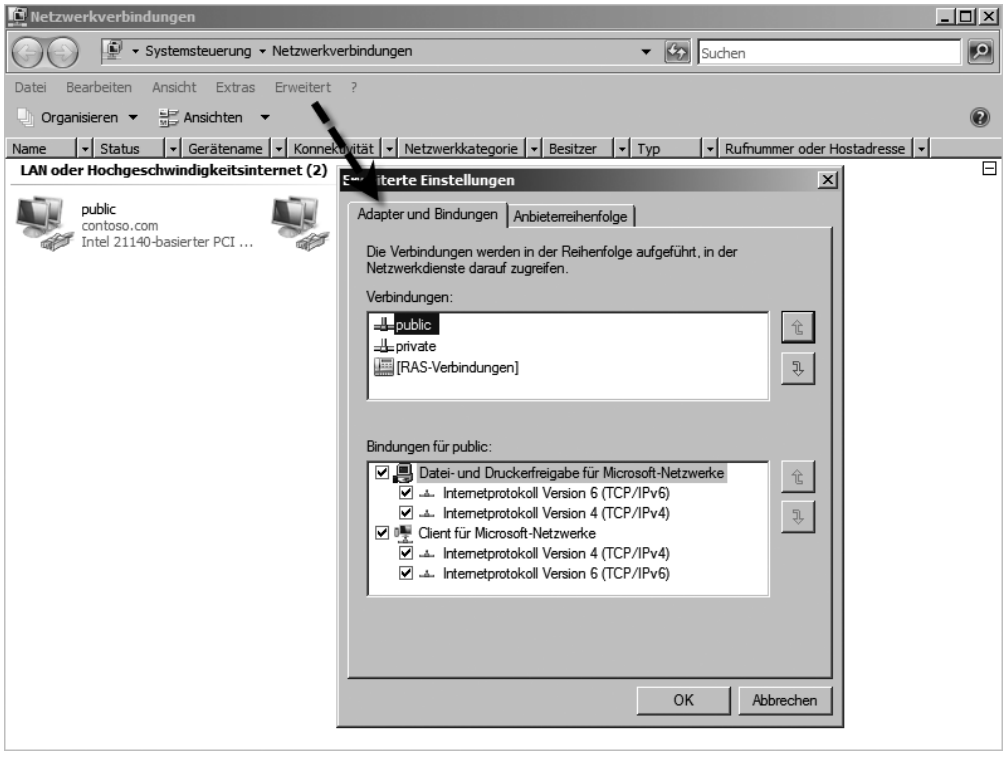
TIPP In den erweiterten Eigenschaften der Windows-Firewall, die über die Systemsteuerung gestartet werden, sollten auf der Registerkarte *Erweitert* die Firewall für das private Clusternetz und, falls vorhanden, für das Netzwerk zum iSCSI-Gerät deaktiviert werden. Für diese beiden Verbindungen stört die Firewall nur. Für das normale, öffentliche Netzwerk, kann die Firewall weiterhin aktiv bleiben (Abbildung 19.17).

Abbildg. 19.17 Windows-Firewall für das interne Clusternetzwerk deaktivieren



Führen Sie auf dem zweiten Clusterknoten genau die gleichen Aktionen durch. Weisen Sie der privaten Verbindung die IP-Adresse *192.168.100.2* zu und stellen Sie die Bindungsreihenfolge und die anderen Optionen genau identisch zum ersten Knoten ein.

Abbildg. 19.18 Einstellen der Bindungsreihenfolge auf den Clusterknoten

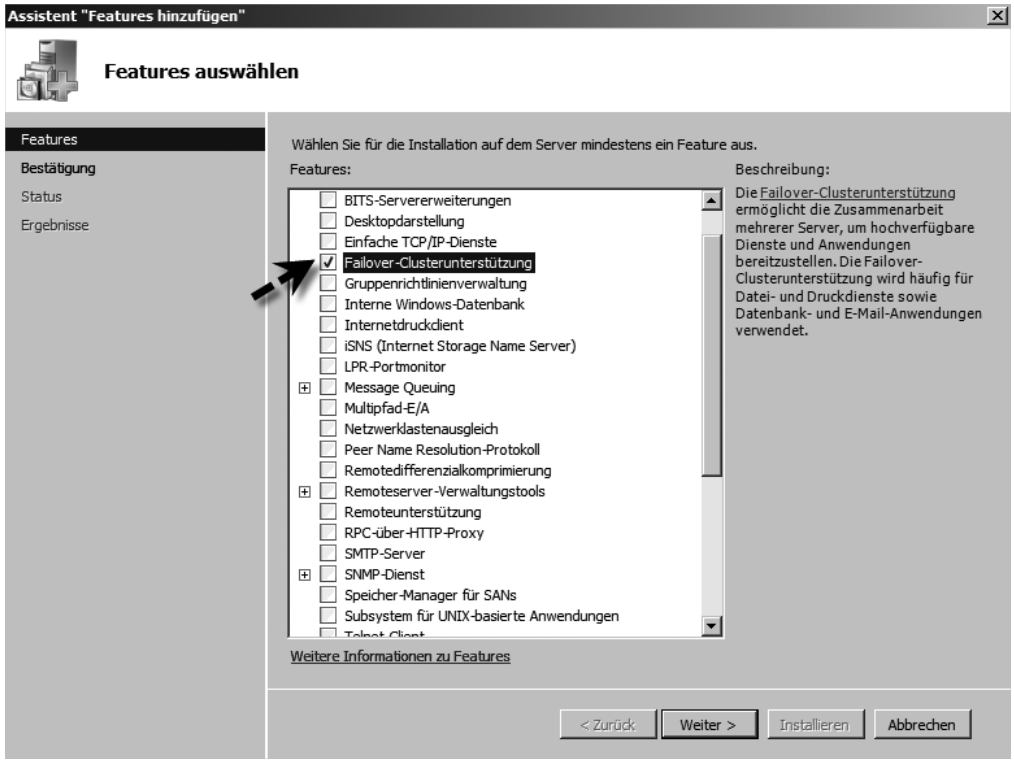


TIPP Verwenden Sie als gemeinsamen Datenträger iSCSI, kann IPv6 deaktiviert werden, wenn das Speichergerät IPv6 nicht unterstützt. Nur wenn alle beteiligten Komponenten eines Clusters IPv6 unterstützen, sollte IPv6 in den Eigenschaften der Netzwerkkarte aktiviert bleiben. In einer Testumgebung kann IPv6 generell deaktiviert werden.

Clustering installieren und konfigurieren

Nachdem die notwendigen Einstellungen vorgenommen wurden, kann der Cluster über den ersten Knoten erstellt werden. Clustering wird unter Windows Server 2008 als Feature installiert. Starten Sie daher den Servermanager und klicken Sie auf *Features* und dann *Features hinzufügen*. Wählen Sie das Feature *Failover-Clusterunterstützung* zur Installation aus (Abbildung 19.19). Während der Installation dieses Features werden noch keinerlei Einstellungen vorgenommen, sondern nur die notwendigen Systemdateien und die Clusterverwaltung installiert. Installieren Sie das Feature auf beiden Clusterknoten.

Abbildg. 19.19 Failover-Clusterunterstützung als Feature unter Windows Server 2008 installieren

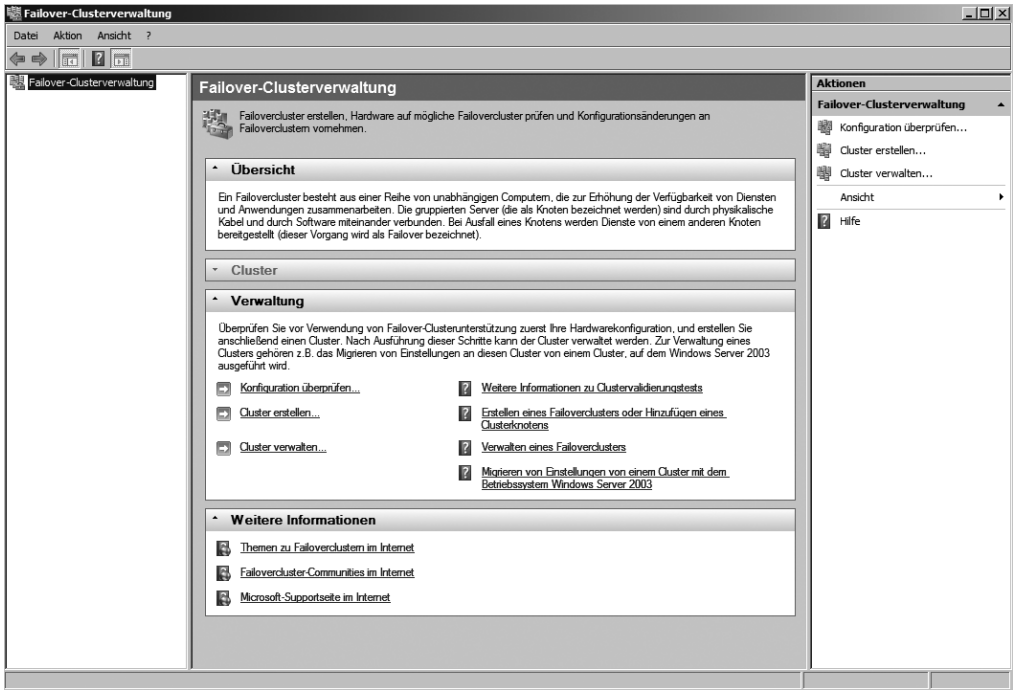


Cluster erstellen und konfigurieren

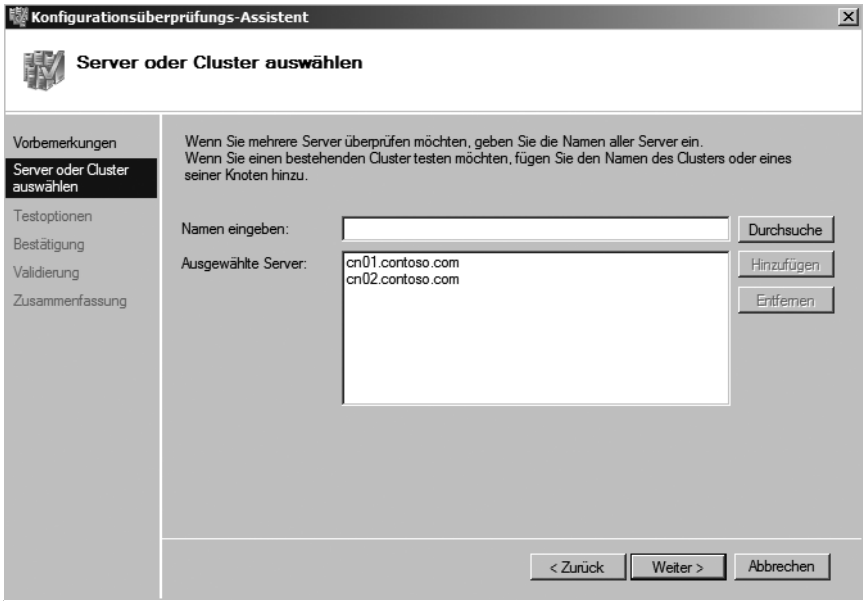
Nach der Installation des Features *Failover-Clusterunterstützung* auf beiden Clusterknoten gehen wir dazu über, den Cluster zu konfigurieren. Starten Sie auf dem ersten Knoten die *Failover-Clusterverwaltung* über *Start/Verwaltung*. Der erste Schritt, um einen Cluster unter Windows Server 2008 zu erstellen, besteht darin, die Clusterknotenkonfiguration zu überprüfen. Klicken Sie dazu auf den Link *Konfiguration überprüfen* im Aktionenbereich (Abbildung 19.20). Diese Konfiguration muss aber nicht zwingend auf dem ersten Knoten, sondern kann unter Windows Server 2008 auch auf dem zweiten Knoten durchgeführt werden. Bei der Erstellung eines Clusters unter Windows Server 2008 können bereits bei der Erstellung des Clusters alle beteiligten Knoten auf einmal angegeben werden.

Bestätigen Sie die Startseite des Assistenten. Auf der nächsten Seite geben Sie den Namen der beiden Clusterknoten ein (Abbildung 19.21). Auf der nächsten Seite des Assistenten wird ausgewählt, welche Tests der Assistent durchführen soll. Hier sollte möglichst immer die Option *Alle Tests ausführen (empfohlen)* gewählt werden. Anschließend erhalten Sie eine Zusammenfassung, was alles getestet wird, und der Assistent beginnt mit seinen Tests. Hier sollten möglichst alle Tests bestanden werden. Der Assistent testet beide Clusterknoten.

Abbildg. 19.20 Starten der Clusterverwaltung und Überprüfen der Konfiguration der Clusterknoten



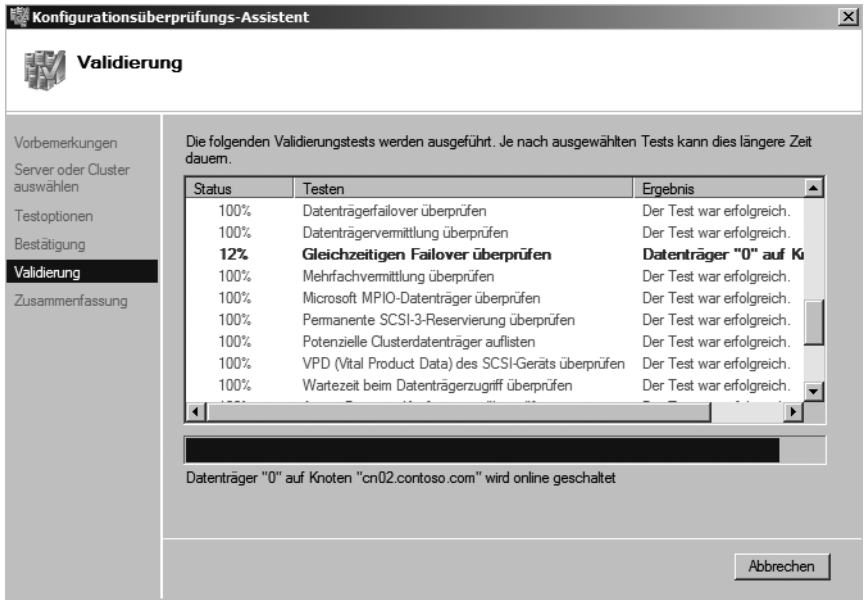
Abbildg. 19.21 Angeben der Clusterknoten, aus denen der Cluster erstellt werden soll



Nachdem der Assistent alle wichtigen Punkte getestet hat, erhalten Sie nach Abschluss einen ausführlichen Bericht über die Konfiguration. Eventuell vorhandene Fehler sollten vor der Installation des Clusters behoben werden und anschließend sollte erneut getestet werden. Erst wenn die Clusterüberprüfung keine Fehler meldet, wird empfohlen, den Cluster zu erstellen. Bei dem Test werden extrem viele Bereiche der Server getestet, sodass sichergestellt ist, dass der Cluster später auch fehlerfrei installiert werden kann. Überzeugen Sie sich selbst in der Testumgebung, welche Bereiche getestet werden. Der Test überprüft alle Clusterknoten, die im vorherigen Fenster hinzugefügt wurden.

HINWEIS Einer der Validierungstests der Clusterinstallation überprüft, ob sich der gemeinsame Datenträger wie ein SCSI 3-Datenträger verhält. Die beiden Standards SCSI 1 und SCSI 2 sind zu langsam und schmalbandig für einen Cluster unter Windows Server 2008.

Abbildg. 19.22 Der Konfigurationsüberprüfungs-Assistent testet die Voraussetzungen für den Failover-Cluster

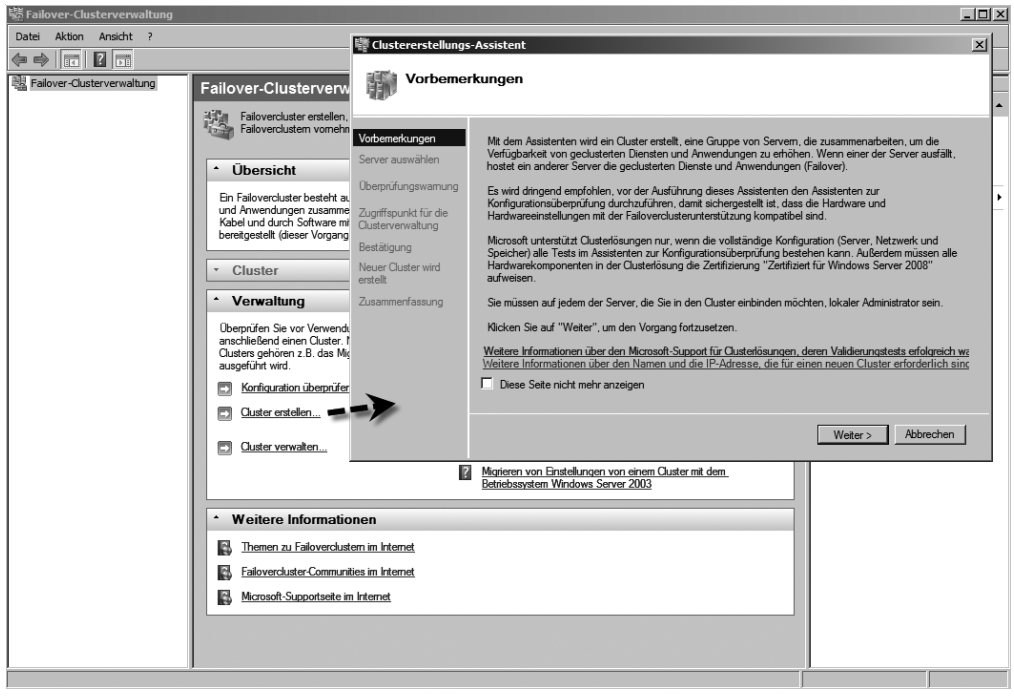


Der Bericht wird als MHT-Datei erstellt und im Internet Explorer angezeigt. Per Klick auf die einzelnen Tests werden ausführliche Informationen angezeigt. Wird ein Fehler gefunden, weist der Assistent darauf hin. In einer Testumgebung unter Virtual PC 2007 kann es durchaus sein, dass ein Fehler in der IP-Konfiguration gemeldet wird. Handelt es sich um keinen Fehler bei den Cluster-Netzwerkkarten, kann dieser ignoriert werden. Dieser ist darauf zurückzuführen, dass die beiden Clusterknoten auf dem gleichen physischen Computer betrieben werden.

Nachdem der Cluster überprüft wurde, kann die Erstellung in der Verwaltungskonsole über *Cluster erstellen* gestartet werden (Abbildung 19.24). Es startet der Assistent zum Erstellen des Clusters. Eine der Neuerungen in Windows Server 2008 ist, dass der Cluster zentral auf einem Knoten erstellt wird und keine Konfiguration auf beiden Knoten stattfinden muss.

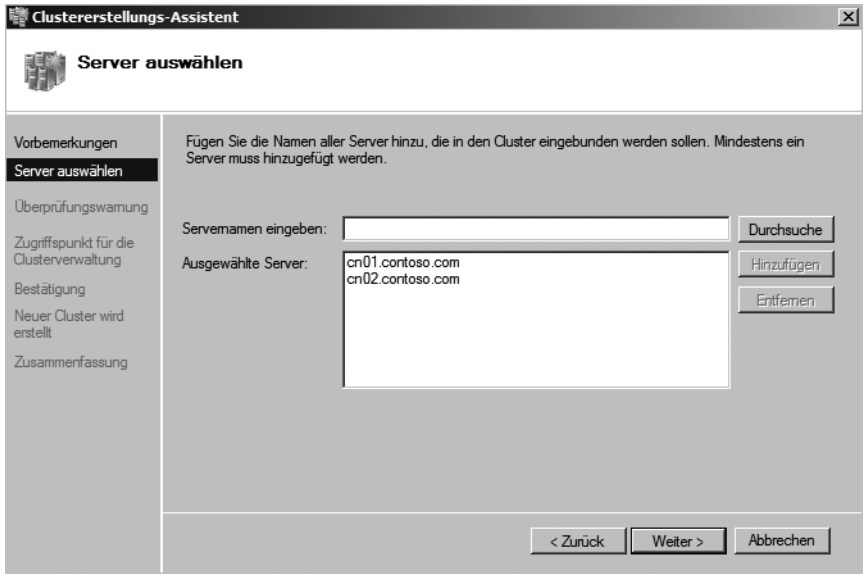
Abbildg. 19.23 Anzeigen des Validierungsberichts der Clusterüberprüfung

Abbildg. 19.24 Erstellen eines Clusters nach der Überprüfung



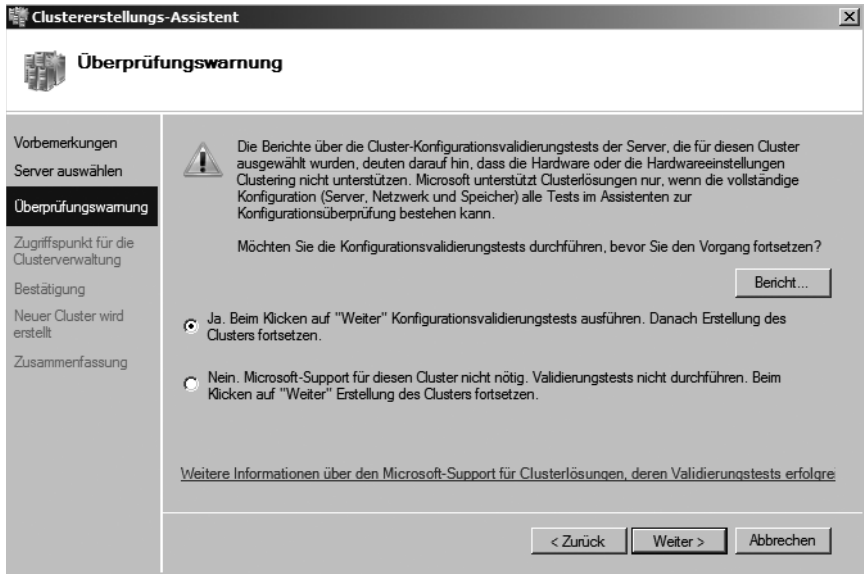
Auf der nächsten Seite des Assistenten werden die Clusterknoten hinzugefügt, mit denen der Cluster erstellt werden soll (Abbildung 19.25). Der Assistent versucht den Servernamen per DNS aufzulösen und fügen die Server hinzu.

Abbildg. 19.25 Hinzufügen der Clusterknoten



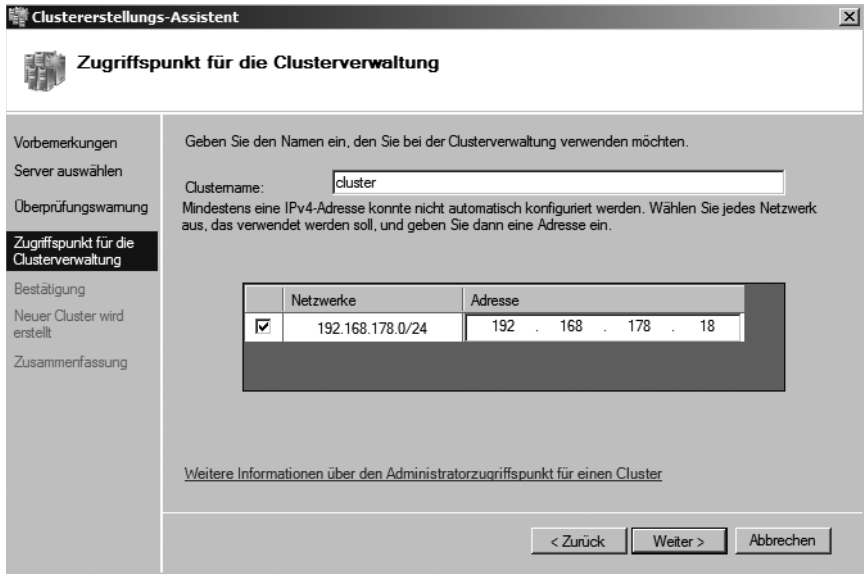
Auf der nächsten Seite erscheinen Meldungen, wenn die Clusterüberprüfung einen Fehler gefunden hat. Hier kann über die Schaltfläche *Bericht* der bereits angezeigte Bericht der Clusterüberprüfung geöffnet werden. Standardmäßig ist die Option aktiviert, dass der Cluster zunächst erneut überprüft und dann erst erstellt wird. Vor der Erstellung des Clusters sollte ohnehin immer zunächst eine fehlerfreie Überprüfung durchgeführt werden. Hier besteht aber noch mal die Möglichkeit, den Assistenten zur Überprüfung zu starten. Wird die Option *Nein, Microsoft-Support für diesen Cluster nicht nötig* aktiviert, fährt der Assistent mit der Installation des Clusters fort. In produktiven Umgebungen sollte das niemals so durchgeführt werden. Hier muss sichergestellt sein, dass der Cluster ohne den kleinsten Fehler installiert wird. In einer Testumgebung spielen kleinere Fehler, die natürlich im Bericht erst überprüft werden sollten, keine Rolle. Hier kann mit der Erstellung des Clusters fortgefahren werden.

Abbildg. 19.26 Anzeigen der Cluster-Überprüfungswarnung



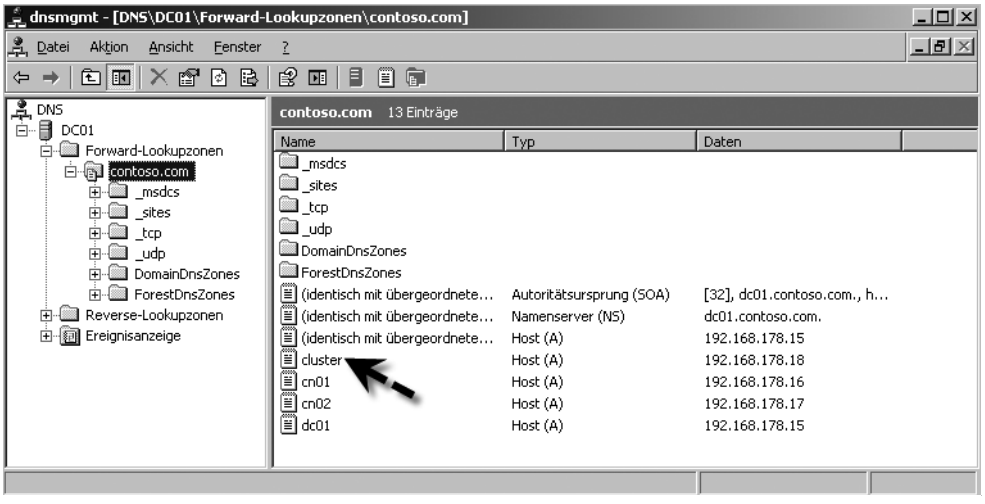
Auf der nächsten Seite legen Sie den Namen des Clusters als Ganzes fest. Über diesen Namen wird mit der Clusterverwaltung auf den Cluster zugegriffen. Hier wählen Sie auch eine IP-Adresse aus, mit welcher der Cluster an sich angesprochen wird. Die IP-Adresse muss natürlich einzigartig im Netzwerk sein und von den Clients und Administratoren erreicht werden können.

Abbildg. 19.27 Festlegen des Namens und der IP-Adresse des Clusters



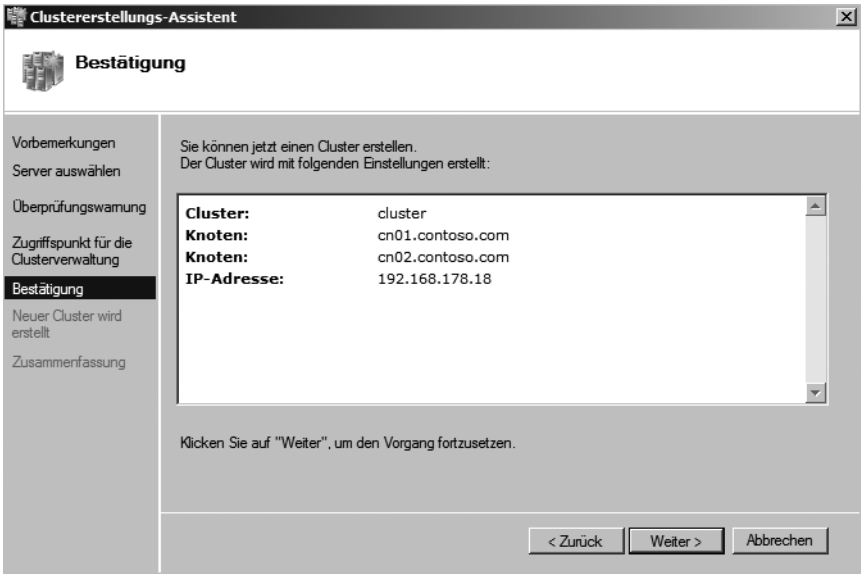
Legen Sie in diesem Fenster den Namen und die IP-Adresse des Clusters fest. Der Name wird mit der IP-Adresse genauso wie die physischen Knoten in der DNS-Zone der Domäne registriert (Abbildung 19.28).

Abbildg. 19.28 Der Cluster wird in der DNS-Zone der Domäne als Host-Eintrag registriert



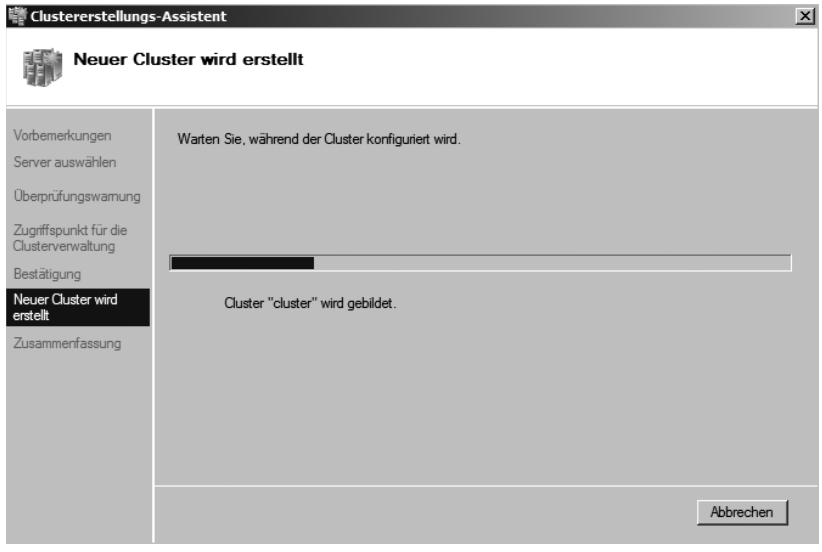
Auf der nächsten Seite des Assistenten erhalten Sie eine Zusammenfassung angezeigt, wie der Cluster erstellt wird. Hier wird der Name und die IP-Adresse des Clusters sowie die Knoten, mit denen dieser erstellt wird, angezeigt.

Abbildg. 19.29 Anzeigen der Daten des neuen Clusters



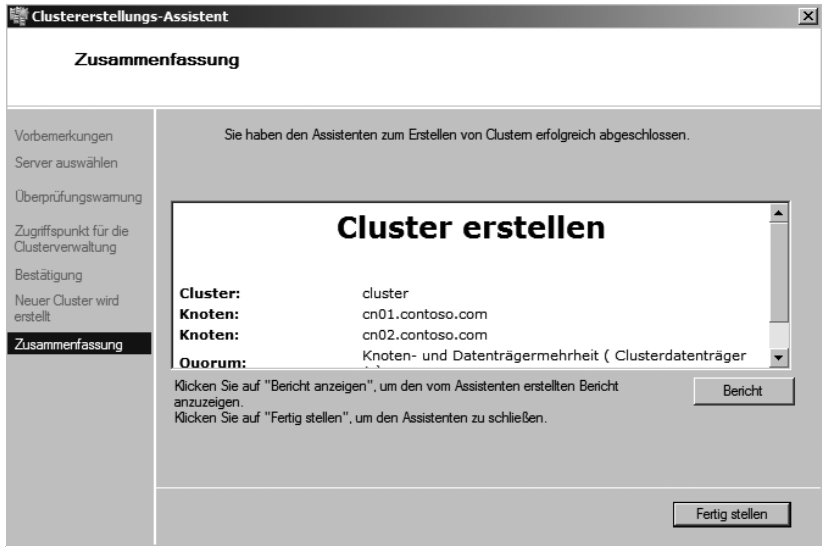
Schließlich wird der Cluster erstellt und die Verbindung zwischen den Knoten aufgebaut. Abhängig von der Geschwindigkeit der beteiligten Server und des gemeinsamen Datenträgers kann dieser Vorgang etwas dauern.

Abbildg. 19.30 Erstellen des Clusters



Nachdem der Cluster erfolgreich erstellt wurde, wird eine Zusammenfassung angezeigt (Abbildung 19.31). Hier sehen Sie, ob das Erstellen erfolgreich war und der Cluster ordnungsgemäß installiert worden ist.

Abbildg. 19.31 Anzeigen einer Zusammenfassung nach dem Erstellen des Clusters

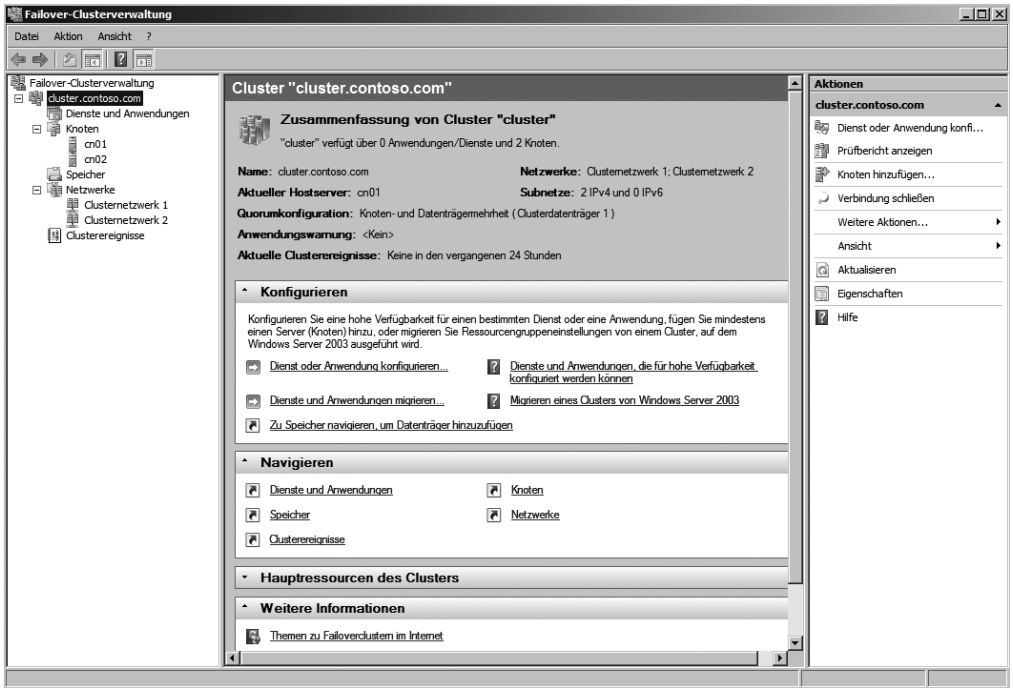


Über die Schaltfläche *Bericht* wird ein ausführlicher Bericht angezeigt, welche Maßnahmen der Assistent bei der Erstellung des Clusters durchgeführt hat. Der Bericht wird im Internet Explorer angezeigt und kann auch gespeichert werden.

Abbildg. 19.32 Anzeige eines Berichts über die Clustererstellung

Nach erfolgreicher Erstellung des Clusters wird dieser in der Clusterkonfiguration angezeigt und kann verwaltet werden. Die Erstellung ist an dieser Stelle abgeschlossen, und Sie können sich mit dem Cluster beschäftigen.

Abbildg. 19.33 Anzeige der Clusterkonfiguration nach der Erstellung



TIPP Das Befehlszeilenprogramm *Cluster.exe* ermöglicht die Verwaltung von Clustern in der Eingabeaufforderung oder über Skripts. Eine ausführliche Hilfe über die Optionen erhalten Sie mit dem Befehl *cluster /?*

Nacharbeiten: Überprüfung des Clusters und erste Schritte mit der Clusterverwaltung

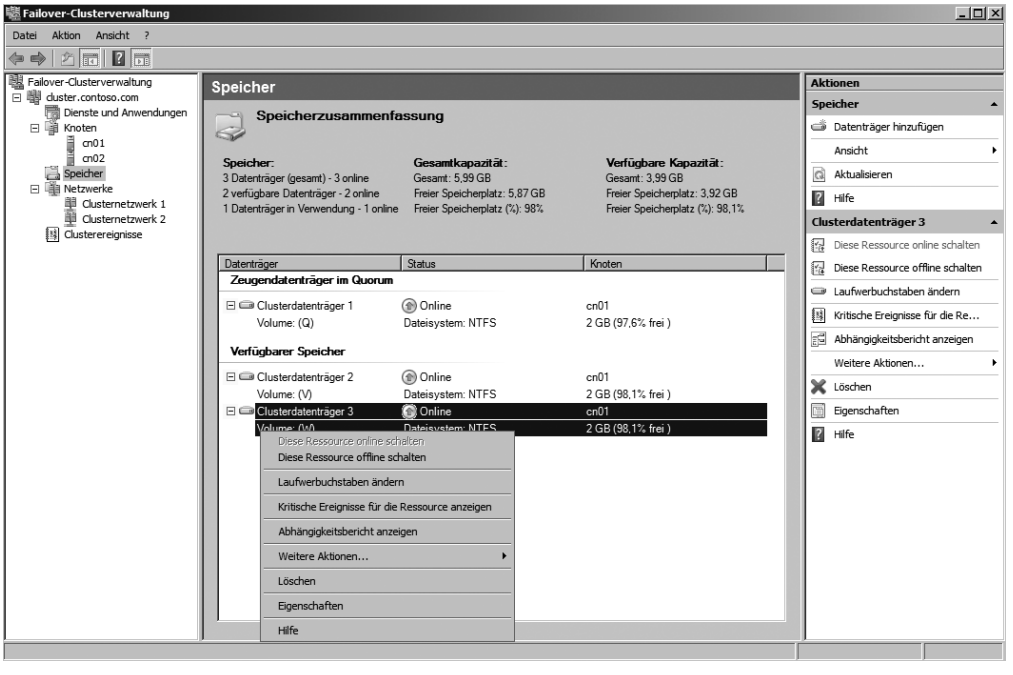
Im nächsten Schritt sollten Sie sich etwas vertraut darin machen, mit einem Cluster umzugehen. Die zentrale Verwaltungsstelle eines Clusters ist die *Failover-Clusterverwaltung*, mit der Sie neue Cluster erstellen, neue Knoten hinzufügen und den Cluster verwalten. Starten Sie die Clusterverwaltung, darf keine Fehlermeldung erscheinen. Kann der Clusteradministrator fehlerfrei eine Verbindung zum Cluster aufbauen, sehen Sie im Menü einige Optionen, die Ihnen zur Verwaltung des Clusters zur Verfügung stehen. Klicken Sie den Namen des Clusters in der Clusterverwaltung mit der rechten Maustaste an, können Sie die Eigenschaften des Clusters überprüfen und anpassen (Abbildung 19.34). Ebenso bietet das Kontextmenü zahlreiche Verwaltungsmöglichkeiten an.

Abbildg. 19.34 Verwalten der Eigenschaften eines Clusters

Auf der Registerkarte *Allgemein* wird der Name des Clusters angepasst. Ändern Sie diesen ab, wird auch der Clustername in der Clusterverwaltung, sowie der dazugehörige Eintrag in der DNS-Zone angepasst. Auf den Registerkarten *Ressourcentypen* wird definiert, welche Windows-Ressourcen dem Cluster hinzugefügt werden können, auf der Registerkarte *Clusterberechtigungen* steuern Sie den administrativen Zugriff der Administratoren auf den Cluster.

Über den Konsoleneintrag *Speicher* in der Clusterverwaltung werden die gemeinsamen Datenträger und das Quorum verwaltet und überprüft (Abbildung 19.35). Hier wird auch der derzeitig aktuelle Knoten angezeigt, der den Cluster aktiv verwaltet. Der zweite Knoten steht offline zur Verfügung. Hierüber werden neue Datenträger dem Cluster hinzugefügt oder vorhandene Ressourcen offline geschaltet.

Abbildg. 19.35 Verwalten der Datenträger des Clusters



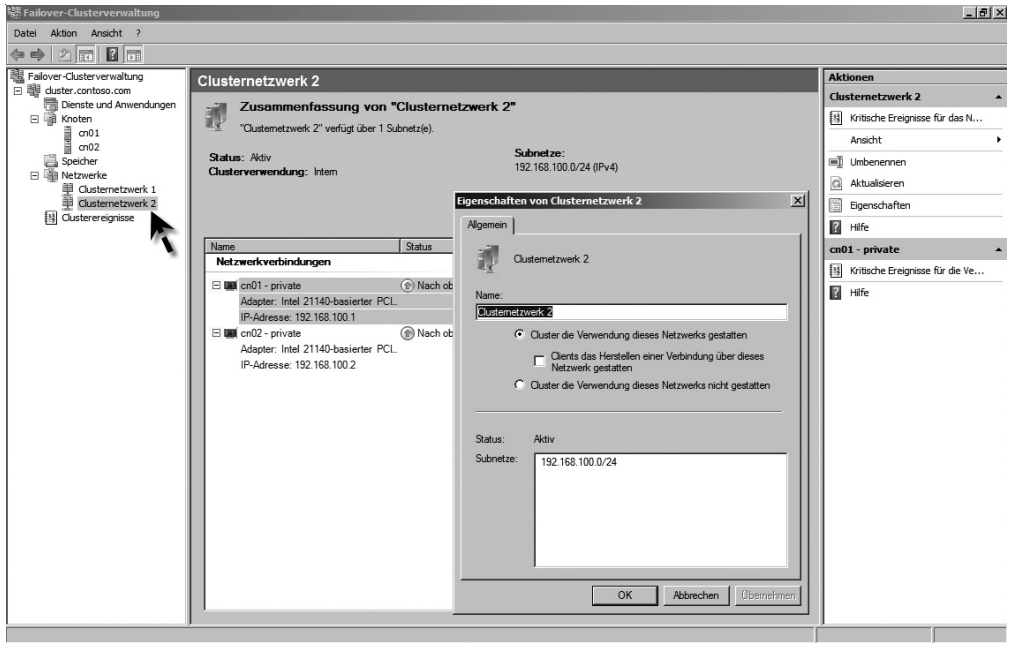
Konfiguration der Netzwerkpriorität im Cluster

In einer Produktivumgebung sollten Sie auf jeden Fall den Konsoleneintrag *Netzwerke* aufrufen. Hier werden die öffentlichen und privaten Verbindungen des Clusters verwaltet. In den Eigenschaften der Verbindungen wird eingestellt, ob diese den Clients zum Verbindungsaufbau, nur für den Heartbeat oder für beides zur Verfügung stehen. Über die private Verbindung soll das Heartbeat des Clusters laufen. Markieren Sie dazu erst die *private*-, dann die *public*-Verbindung und rufen Sie die Eigenschaften auf. Stellen Sie sicher, dass bei der privaten Verbindung nur die Option *Cluster die Verwendung dieses Netzwerks gestatten* aktiviert ist und damit nur die interne Clusterkommunikation aktiviert wird (Abbildung 19.36). Dadurch ist sichergestellt, dass dem Heartbeat ein privater Kanal im Netzwerk zur Verfügung steht und er nicht durch Benutzeranfragen beeinträchtigt wird.

Bei den Eigenschaften der *public*-Verbindung, sollten Sie die Option *Cluster die Verwendung dieses Netzwerks gestatten* und das Kontrollkästchen *Clients das Herstellen einer Verbindung über dieses Netzwerk gestatten* aktivieren, damit sichergestellt ist, dass die Clusterverbindung intern auf jeden Fall funktioniert, auch wenn eine private Netzwerkkarte ausfällt.

Bei einer fast perfekten Ausfallsicherheitskonfiguration verfügt jeder Clusterknoten über drei Netzwerkkarten. Eine Karte dient der internen Kommunikation, eine ausschließlich der privaten und die dritte dient zur Ausfallsicherheit und ist für den gemischten Modus aktiviert. Nur dadurch erhalten Sie eine optimale Ausfallsicherheit.

Abbildg. 19.36 Konfigurieren eines Cluster-Netzwerkes

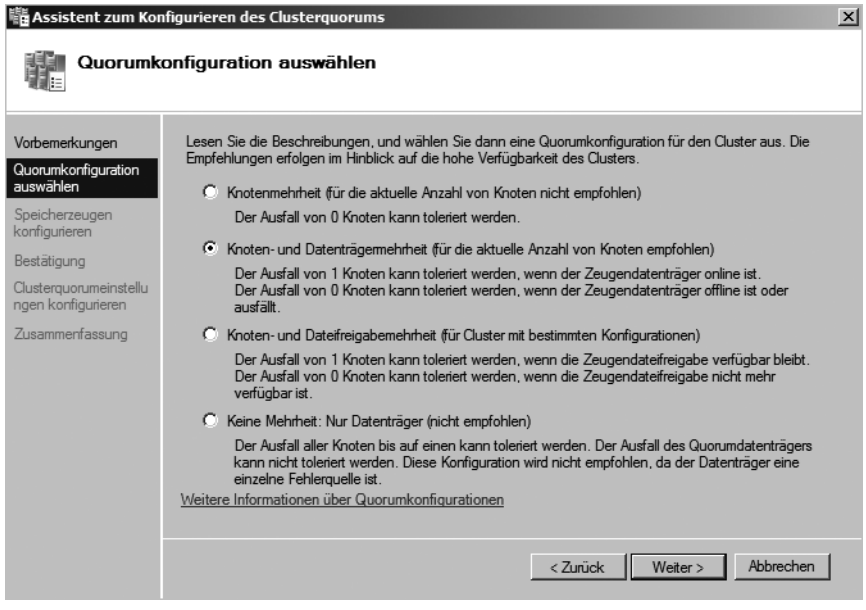


Der Cluster ist installiert und kann getestet werden. In den nächsten Abschnitten in diesem Kapitel zeigen wir Ihnen, welche Beispielanwendungen es für einen Cluster gibt und wie diese installiert werden.

Clusterquorum konfigurieren

Durch einen Klick mit der rechten Maustaste auf den Cluster kann über *Weitere Aktionen/Clusterquorumeinstellungen konfigurieren* das Quorum nachträglich an die gewünschte Option angepasst werden (Abbildung 19.37). Hier stehen zahlreiche Möglichkeiten zur Verfügung.

Abbildg. 19.37 Konfigurieren des Clusterquorums



Der Cluster Continuous Replication von Exchange Server 2007 nutzt eine Funktion des Clusterdienstes mit dem Namen *Hauptknotensatz (Majority Node Set, MNS)*. Dabei handelt es sich um eine besondere Clusterart, die generell ohne ein gemeinsames Clusterquorum auskommt. Jeder Cluster-Knoten hat sein eigenes Quorum, und ein Witness (Zeuge) genannter Rechner übernimmt die Steuerung und Kommunikation der Clusterverwaltung. Dieser Server wird nicht Bestandteil des Clusters, sondern ist außerhalb des Clusters angeordnet. Microsoft empfiehlt, einen Hub-Transport-Server am gleichen Active Directory-Standort zu verwenden, der von allen Clusterknoten über das Netzwerk erreicht werden kann. Mit Hilfe der Cluster Continuous Replication (CCR) können geografisch verteilte Cluster eingerichtet werden, ohne spezielle Applikationen und Hardware einsetzen zu müssen. Die Synchronisation der Clusterknoten erfolgt über die Replikation von Exchange-Transaktionsprotokolldateien. Diese Clustervariante ist natürlich auch für andere Cluster sinnvoll. Im Gegensatz zu einem Single Copy Cluster empfiehlt Microsoft beim Einsatz der Cluster Continuous Replication diese Einbindung eines weiteren Servers für die Bereitstellung einer Freigabe. Diese Freigabe wird offiziell als *File Share Witness (Dateifreigabenzeuge)* bezeichnet und zur Absicherung des Datenflusses zwischen den beiden Knoten eingesetzt. Hauptsächlich wird diese Erweiterung in Zwei-Knoten-Clustern eingesetzt. Dies hat den Grund, dass ein MNS-Cluster davon ausgeht, dass drei Knoten sich gegenseitig überwachen. Sind nur zwei Knoten verfügbar, muss ein dritter, außenstehender Server dafür sorgen, dass beide Clusterknoten immer einwandfrei funktionieren.

Erstellen der Freigabe für das File Share Witness

Haben Sie den Cluster mit beiden Knoten erstellt, bevor Sie CCR einrichten, sollten Sie die Freigabe für File Share Witness konfigurieren. Sie können diese Freigabe auf jedem Windows Server-System erstellen, optimal ist natürlich die Installation auf einem Windows Server 2008 mit installiertem Exchange Server 2007 und der Hub-Transport-Funktion, zumindest wenn der Cluster mit CCR betrieben werden soll. Der Server sollte sich am gleichen Active Directory-Standort befinden, wie der Cluster, auf dem Sie die CCR einrichten wollen. Gehen Sie dazu folgendermaßen vor:

1. Melden Sie sich an dem Server, auf dem Sie die Freigabe für *File Share Witness* erstellen wollen, mit einem Domänenadmin-Konto an.
2. Erstellen Sie ein neues Verzeichnis und weisen Sie diesem eine entsprechende Bezeichnung zu, zum Beispiel *<Name des virtuellen Exchange-Servers>-MNS-Cluster*.
3. Geben Sie das Verzeichnis frei und erteilen Sie dem Clusterkonto volle Zugriffsrechte auf Freigabe- und NTFS-Ebene.
4. Melden Sie sich an beiden Clusterknoten an und überprüfen Sie, ob Sie auf die Freigabe zugreifen können.

Konfiguration des MNS-Quorums für die Verwendung der File Share Witness

Haben Sie die Freigabe erstellt und können Sie von den Clusterknoten fehlerfrei auf diese zugreifen, müssen Sie das Quorum des Clusters noch für die MNS-Unterstützung anpassen. Gehen Sie folgendermaßen vor:

1. Melden Sie sich am aktiven Clusterknoten an.
2. Öffnen Sie eine Befehlszeile.
3. Geben Sie den Befehl *Cluster <Cluster-Name> res Hauptknotensatz/priv MNSFileShare=<Pfad zur Freigabe>* ein. Bei englischen Servern verwenden Sie statt *Hauptknotensatz* den Befehl *Cluster <Cluster-Name> res Majority Node Set/priv MNSFileShare=<Pfad zur Freigabe>*
4. Haben Sie den Befehl korrekt eingetragen, erhalten Sie die Meldung, dass die Änderungen zwar gespeichert wurden, aber erst beim nächsten Online-Schalten der Ressource verwendet werden.
5. Erhalten Sie die Fehlermeldung, dass die Ressource nicht gefunden werden kann, haben Sie vermutlich einen falschen Ressourcennamen für das Quorum verwendet. Die korrekte Bezeichnung der Ressource erhalten Sie, wenn Sie in der Befehlszeile den Befehl *cluster /quorum* eingeben. Auf der linken Seite wird die korrekte Bezeichnung der Hauptknotensatz-Ressource angezeigt.
6. Wurden die Änderungen gespeichert, müssen Sie dafür sorgen, dass die Ressource neu gestartet wird. Erst dann wird die konfigurierte Freigabe verwendet. Um die Gruppe neu zu starten, verschieben Sie diese am besten auf den zweiten Knoten.
7. Bei diesem Vorgang wird die Gruppe automatisch auf den passiven Knoten verschoben und dann online geschaltet. Verschieben Sie im Anschluss die Gruppe auf dem gleichen Weg wieder zurück auf den ersten Knoten. Alternativ können Sie das Verschieben von Clustergruppen auch in der Befehlszeile mit dem Befehl *cluster* ausführen.
8. Als Nächstes sollten Sie überprüfen, ob der konfigurierte Wert für die MNS-Freigabe angenommen und abgespeichert worden ist. Verwenden Sie dazu in der Befehlszeile den Befehl *cluster <Clustername> res Hauptknotensatz /priv*. Im Anschluss sollte der korrekte Wert angezeigt werden.
9. Zusätzlich können Sie sich nach der Erstellung des Clusters und der Konfiguration des Hauptknotensatzes, den Inhalt der Freigabe anzeigen lassen. Dieser enthält einen Unterordner mit einer GUID, der wiederum die Daten des Quorums enthält. Im dem Verzeichnis werden keine Exchange-Transaktionsprotokolle gespeichert, sondern lediglich Informationen zum CCR-Cluster.

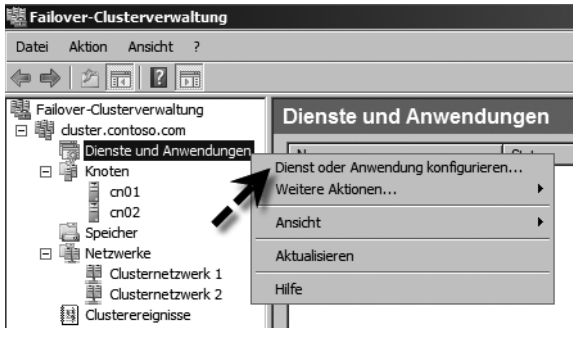
Dateiserver im Cluster betreiben

Nach der Installation eines Clusters, wie im vorangegangenen Abschnitt besprochen, sind noch keinerlei Dienste auf dem Server aktiviert. Es gibt nur den Cluster, der aber an sich keinen produktiven Nutzen hat. Ein verbreiteter Nutzen ist ein ausfallsicherer Dateiserver. Dazu werden die Freigaben im Cluster konfiguriert und die Clients verbinden sich mit dem Cluster. Fällt ein physischer Knoten aus, übernimmt der zweite Knoten alle Ressourcen und die Anwender können ungestört nach wenigen Sekunden weiterarbeiten.

Installieren eines Dateiserver-Clusters

Um einen Dateiserver-Cluster zu erstellen, muss zunächst ein ganz normaler Cluster installiert und betrieben werden, wie weiter vorne bereits beschrieben. Anschließend kann über die Failover-Clusterverwaltung ein ausfallsicherer Dateiserver-Cluster erstellt werden. Diese Vorgänge können auch in der Testumgebung vorgenommen werden, die wir in diesem Kapitel beschrieben haben. Klicken Sie anschließend mit der rechten Maustaste auf den Konsoleneintrag *Dienste und Anwendungen* und wählen Sie im Kontextmenü den Befehl *Dienst oder Anwendung konfigurieren* aus (Abbildung 19.38).

Abbildg. 19.38 Erstellen einer neuen Anwendung im Cluster

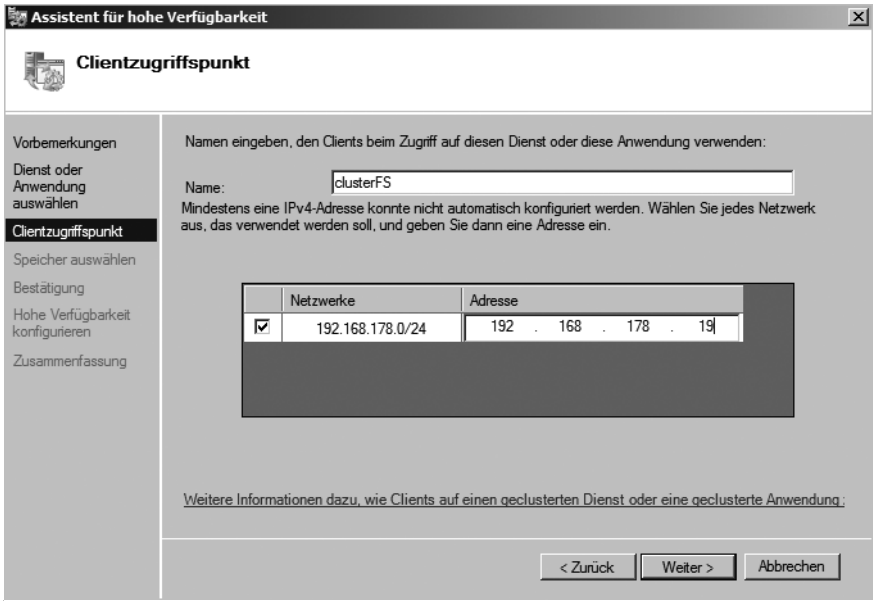


Anschließend startet der Assistent zur Erstellung von neuen Anwendungen in einem Cluster. Die erste Seite des Assistenten können Sie mit *Weiter* bestätigen. Auf der nächsten Seite wird ausgewählt, welche Anwendung auf dem Cluster installiert werden soll (Abbildung 19.39).

Um einen ausfallsicheren Dateiserver zu installieren, wählen Sie an dieser Stelle *Dateiserver* aus. Anschließend müssen noch die Cluster-Daten für den Dateiserver konfiguriert werden. Wie der Cluster selbst erhält der Dateiserver einen eigenen Namen und eine eigene IP-Adresse, über die er von den Clients angesprochen wird. Da diese beiden Ressourcen virtuell sind, werden diese vom zweiten Clusterknoten übernommen, wenn der erste Knoten ausfallen sollte.

Abbildg. 19.39 Auswählen des Dienstes, der im Cluster installiert werden soll

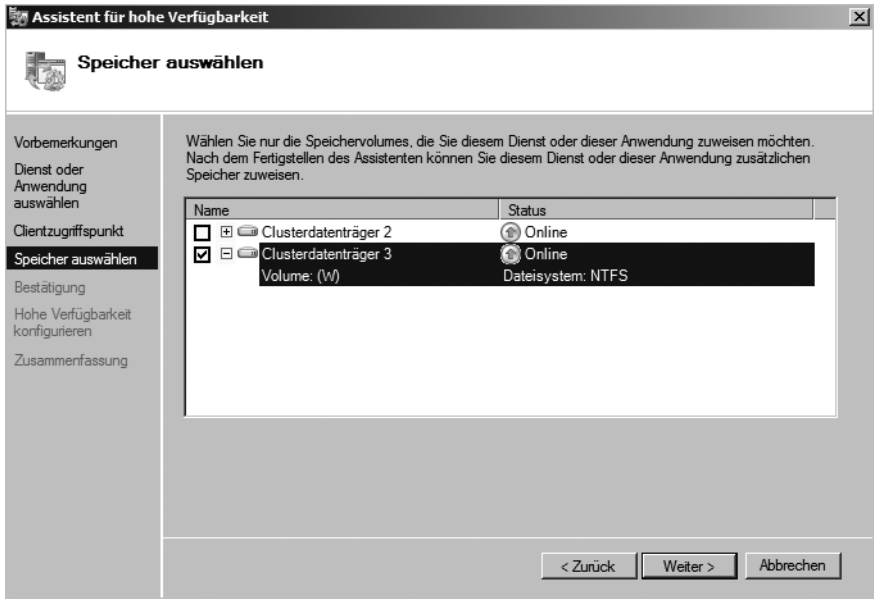
Abbildg. 19.40 Festlegen des Dateiservernamens und dessen IP-Adresse



Auf der nächsten Seite des Assistenten wird der gemeinsame Datenträger ausgewählt, der mit dem Dateiserver-Cluster verbunden werden soll. Freigaben auf diesem gemeinsamen Datenträger werden mit der IP-Adresse und dem Namen des Servers verschoben, sobald der aktive Knoten ausfällt.

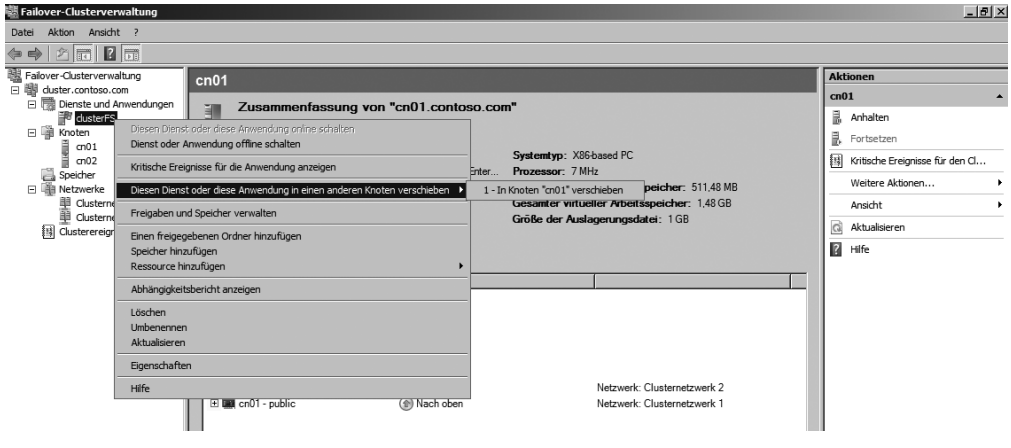
Wählen Sie den Datenträger aus. Der Datenträger mit dem Quorum gehört zum System des Clusters und wird nicht für die Ablage von Benutzerdateien vorgeschlagen. Anschließend erhalten Sie noch eine Zusammenfassung und die Anwendung wird im Cluster erstellt und zur Verfügung gestellt.

Abbildg. 19.41 Auswählen des gemeinsamen Datenträgers für den ausfallsicheren Dateiserver



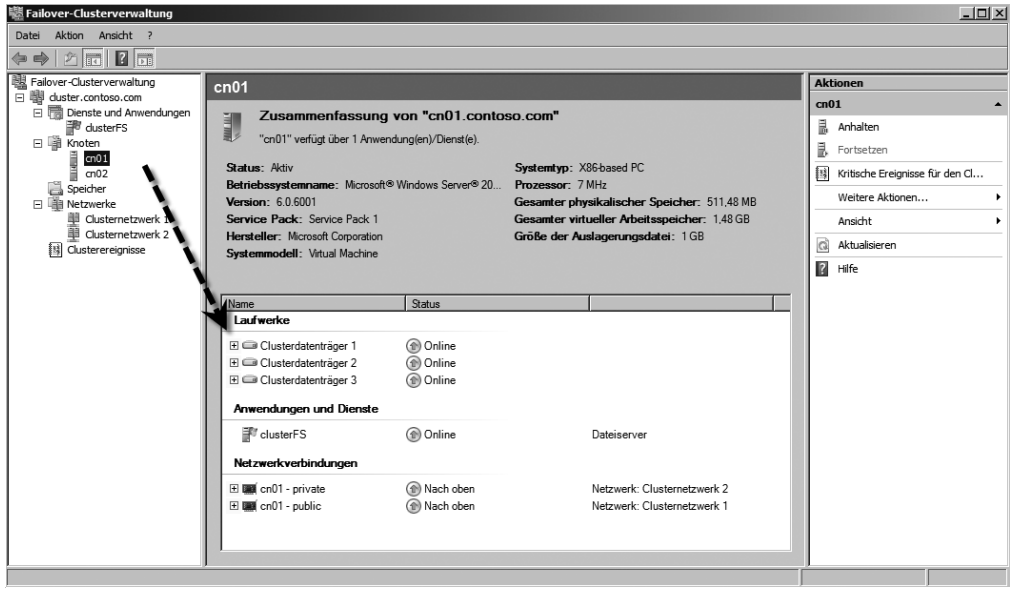
Nach Erstellung wird der neue Dienst unterhalb von *Dienste und Anwendungen* angezeigt. Auch der Name dieses Servers wird in der DNS-Zone der Domäne eingetragen, genauso wie der Name des Clusters selbst. Über das Kontextmenü können die Einstellungen für den Clusterdienst aufgerufen sowie weitere Verwaltungsaufgaben gestartet werden.

Abbildg. 19.42 Verwalten eines Dateiserver-Clusters



Über den Kontextmenübefehl *Diesen Dienst oder diese Anwendung in einen anderen Knoten verschieben* kann der Server mit allen Ressourcen auf den anderen Knoten verschoben werden. Dabei wird der Dienst kurz offline geschaltet, auf den anderen Knoten verschoben, und dann wieder online geschaltet. Nach Aufrufen dieser Option muss das Verschieben noch bestätigt werden. Der aktuelle Knoten des Dienstes wird angezeigt, wenn Sie auf den Dienst klicken. Auch über das Informationsfenster des jeweiligen Knotens wird angezeigt, welche Clusterdienste sich aktuell auf ihm befinden (Abbildung 19.43).

Abbildg. 19.43 Anzeigen der aktiven Dienste eines Knotens

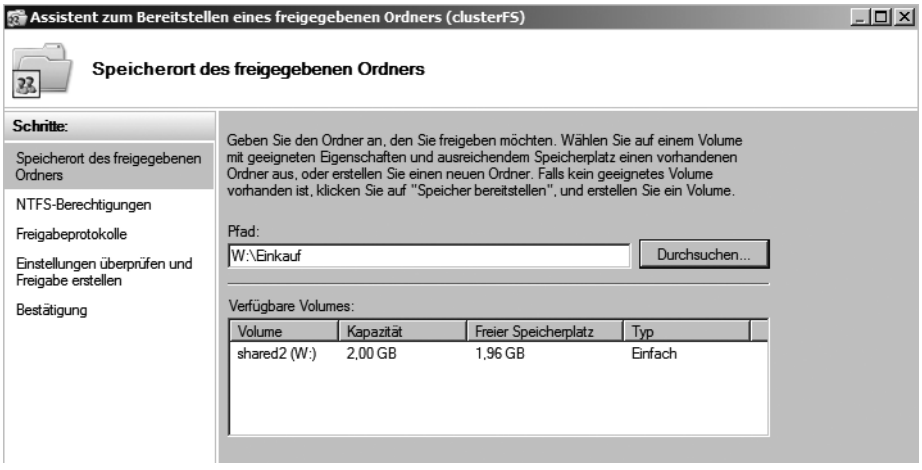


Erstellen von Freigaben für einen Dateiserver-Cluster

Auch die Freigaben auf einem Dateiserver-Cluster werden über die Clusterverwaltung erstellt und als Cluster-Ressource verwaltet. Nur so ist sichergestellt, dass beim Ausfall eines Knotens alle notwendigen Ressourcen auf den anderen Knoten verschoben werden können. Um neue Freigaben zu erstellen, klicken Sie mit der rechten Maustaste auf den Dateiserver in der Clusterverwaltung und wählen im Kontextmenü den Befehl *Einen freigegebenen Ordner hinzufügen* aus. Im ersten Fenster wird zunächst der Pfad ausgewählt der freigegeben werden soll (Abbildung 19.44). Anschließend können die NTFS-Berechtigungen über den Assistenten angepasst werden. Da die Rechte mit dem Verzeichnis gespeichert werden und sich dieses Verzeichnis auf dem ausgewählten gemeinsamen Datenträger befindet, können diese Einstellungen auch, wie bei normalen Servern, über den Windows-Explorer abgewickelt werden. Auf der nächsten Seite wird ausgewählt, welches Protokoll für die Freigabe verwendet werden soll. Unterstützt der Server auch NFS, kann dieses aktiviert werden. Standardmäßig wird aber nur das Windows-Protokoll SMB verwendet. Die Server Message Blocks (SMB) sind eines der wesentlichen, gemeinsamen Elemente der meisten Netzwerkbetriebssysteme. Es handelt sich um ein Protokoll, das einen Satz von Befehlen für den Austausch von Informationen

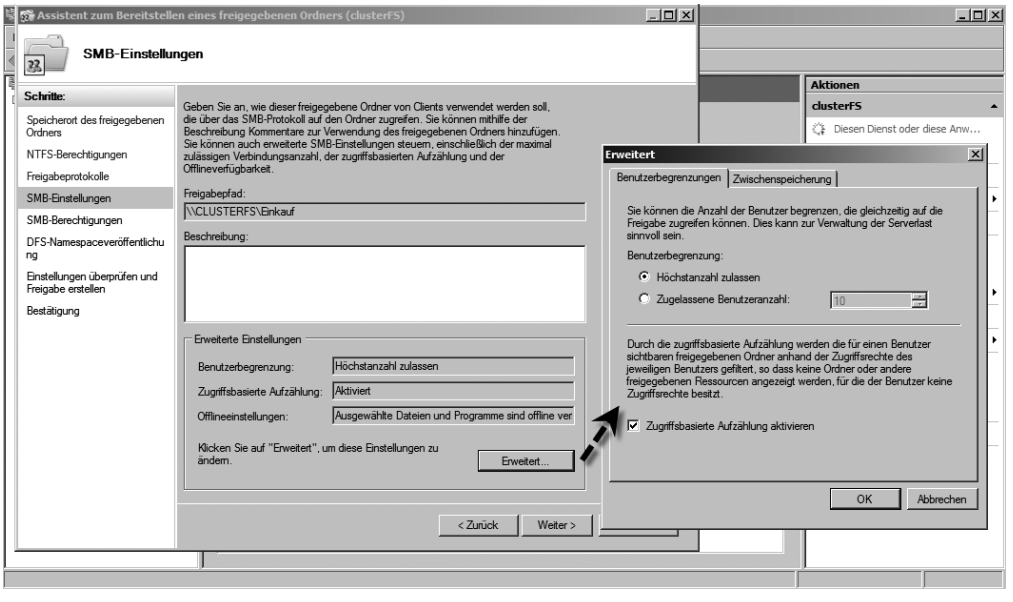
zwischen miteinander vernetzten Computern bereitstellt. Über SMBs kann ein Client eine Datei von einem Server anfordern.

Abbildg. 19.44 Auswählen des Pfades für die neue Freigabe im Cluster



Auf der nächsten Seite des Assistenten werden die Einstellungen für die Freigabe konfiguriert. Wichtige Einstellungen erreichen Sie über die Schaltfläche *Erweitert*. Die Möglichkeiten an dieser Stelle sind mit den Freigaben auf normalen Dateiservern identisch und wurden in Kapitel 6 besprochen.

Abbildg. 19.45 Konfigurieren der Einstellungen für die neue Freigabe

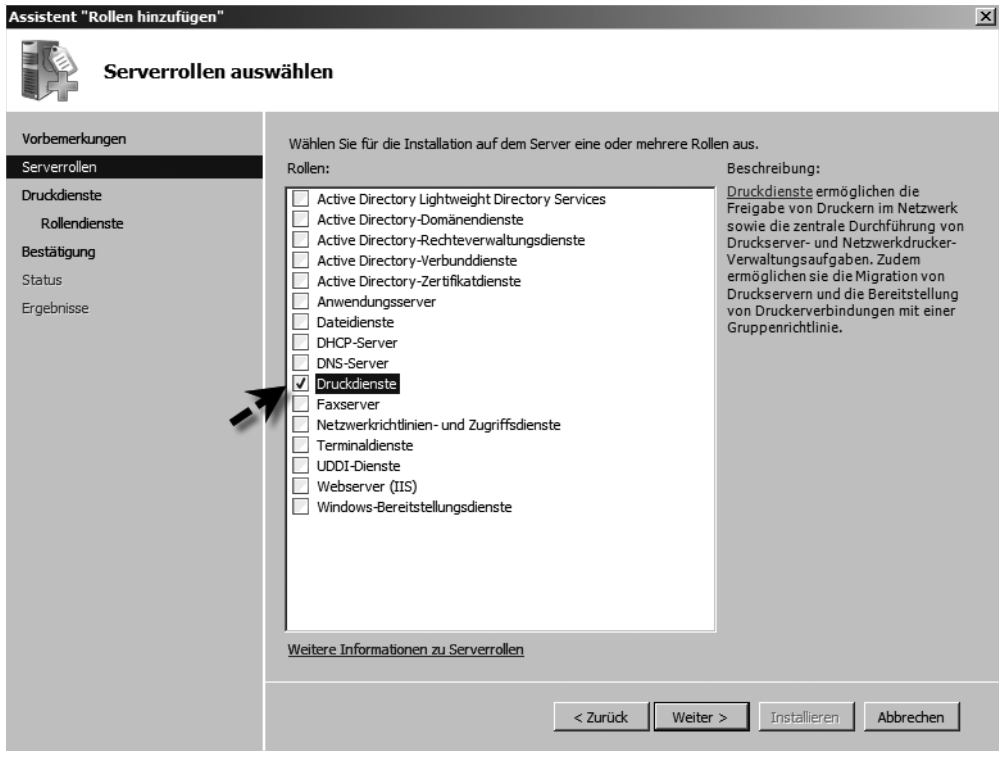


Auf der nächsten Seite werden schließlich die Freigabeberechtigungen konfiguriert. Auch diese Konfiguration ist identisch mit der herkömmlichen Erstellung von Freigaben. Hier können entweder vorgeschlagene Standardberechtigungen oder benutzerspezifische Einstellungen vorgenommen werden. Wollen Sie die Freigabe über einen DFS-Stamm zur Verfügung stellen, steht Ihnen die nächste Seite des Assistenten zur Verfügung. Auch diese Einstellungen sind ähnlich zu den Möglichkeiten von herkömmlichen Freigaben, die in Kapitel 6 besprochen sind. Anschließend wird die Freigabe erstellt und steht den Anwendern zur Verfügung. Sie wird im Informationsfenster des Dateiservers angezeigt. Über das Kontextmenü der Freigaben lassen sich die Einstellungen nachträglich anpassen. Anwender greifen auf die Freigabe mit dem virtuellen Namen \\<*Cluster-Dateiserver*>\<*Freigabe*> zu. Für Anwender ist diese Vorgehensweise transparent. Es gibt keinen Unterschied zu herkömmlichen Freigaben.

Druckserver im Cluster betreiben

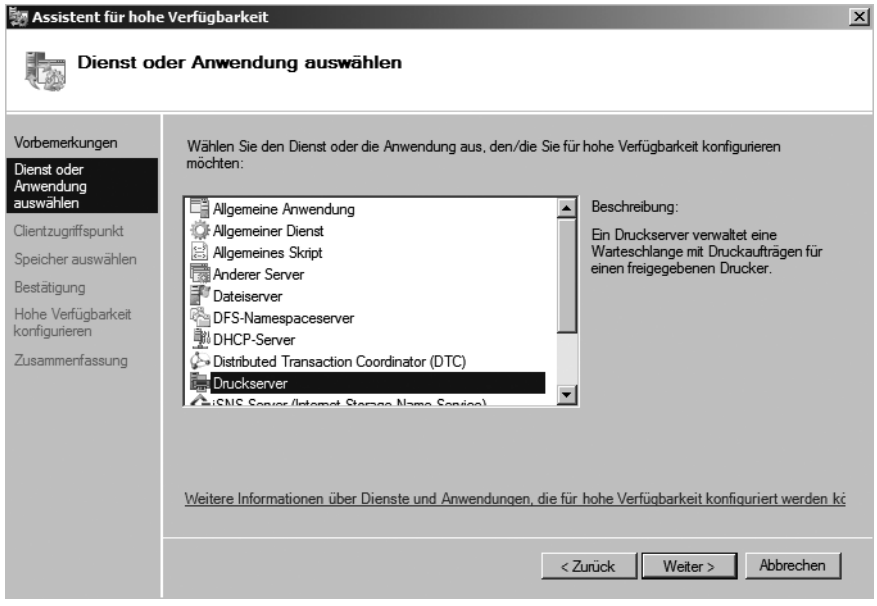
Die Installation eines Druckservers im Cluster läuft ähnlich ab, wie die Installation eines Dateiservers. Bevor Sie den Dienst eines Druckservers hinzufügen, muss zunächst der Cluster installiert werden. Außerdem muss auf den Clusterknoten noch die Rolle *Druckdienste* installiert werden. Bevor diese Rolle auf einem Clusterknoten nicht installiert ist, kann auch kein Druckserver im Cluster installiert werden.

Abbildg. 19.46 Installieren der Rolle *Druckdienste* für den Betrieb eines Druckservers im Cluster



Nachdem die Rolle auf beiden Knoten installiert wurde, starten Sie in der Clusterverwaltung die Erstellung einer neuen Anwendung genauso wie bei einem Dateiserver. Wählen Sie als Dienst für den Cluster aber *Druckserver* aus (Abbildung 19.47). Bereits bei der Auswahl dieses Dienstes überprüft der Cluster, ob dieser fehlerfrei integriert werden kann. Erst nach erfolgreicher Überprüfung wird der Assistent fortgesetzt und der Dienst kann installiert werden. Die weiteren Einstellungen sind mit der Erstellung eines Dateiservers im Cluster identisch. Auch dieser Dienst erhält einen eigenen Servernamen und eine eigene IP-Adresse.

Abbildg. 19.47 Installieren eines Druckservers im Cluster



Damit der Druckserver genutzt werden kann, müssen über das Kontextmenü noch freigegebene Drucker hinzugefügt werden. Drucker und neue Treiber werden über den Kontextmenübefehl *Drucker verwalten* dem Server hinzugefügt und freigegeben. Der Treiber des Druckers sollte zuvor auf beiden Knoten installiert werden, damit dieser in der Konsole hinzugefügt und freigegeben werden kann.

Single Copy Cluster mit Exchange Server 2007 SP1

Im Bereich *Hochverfügbarkeit* bietet Exchange Server 2007 einige Verbesserungen im Vergleich zu Exchange 2000/2003. Bereits mit der fortlaufenden lokalen Replikation (Local Continuous Replication, LCR) bietet Exchange Server 2007 bereits ohne einen Cluster eine Echtzeitreplikation der Exchange-Datenbank an. In diesem Fall sind Sie zwar nicht vor dem Ausfall eines Servers geschützt, aber vor dem Ausfall und der Zerstörung der Exchange-Datenbank. Die herkömmlichste Herstellung einer Hochverfügbarkeitslösung ist aber ein Single Copy Cluster. Im Verlauf dieses Kapitels wurde Ihnen bereits gezeigt, wie Sie einen Cluster auf Basis von Windows Server 2008 aufbauen. Installieren Sie

Exchange clusterfähig, baut die Installation von Exchange Server 2007 SP1 auf einem solchen Cluster auf. Der Single Copy Cluster dient dazu, einen Exchange Server 2007 mit der Mailbox-Server-Rolle auf einem Cluster mit gemeinsamen Datenträgern zu installieren.

Diese Funktion ist grundsätzlich identisch mit der Installation von Exchange 2000/2003 in einem Cluster. Wie bereits bei Exchange Server 2003 empfiehlt Microsoft auch bei Exchange Server 2007 den Einsatz eines Aktiv/Passiv-Clusters. Es wird also ein virtueller Exchange-Server erstellt, der auf einem Knoten aktiv geschaltet wird, während der passive Knoten auf den Ausfall des aktiven Knotens wartet und die Clustergruppe mit dem virtuellen Exchange-Server übernimmt. Bei dieser Installation sind Sie zwar vor Ausfall eines Exchange-Servers geschützt, eine defekte Datenbank können Sie mit dieser Funktion nicht abfangen. Da bei einem Cluster mit dieser Installationsmethode die Exchange-Datenbank auf dem gemeinsamen Datenträger des Clusters liegt und von mehreren Servern verwaltet werden kann, wird der Cluster jetzt auch Einzelkopiecluster (Single Copy Cluster, SCC) genannt, da die Datenbank als einzelne Kopie auf dem gemeinsamen Datenträger vorliegt.

Wichtig ist bei dieser Architektur, dass allerdings immer nur ein Server (der aktive Knoten) auf die Datenbank zugreifen kann und erst bei Ausfall dieses Servers andere Server (die passiven Knoten) Zugriff erhalten. Damit Sie diese Funktion nutzen können, müssen Sie zunächst mit Windows Server 2008 Enterprise Edition den Windows-Clusterdienst konfigurieren und einen Failover-Cluster einrichten. Installieren Sie Exchange Server 2007 auf einem Clusterknoten, wird automatisch die clusterfähige Installation durchgeführt. Zur Installation muss das SP1 für Exchange Server 2007 verwendet werden. Diese steht bei Microsoft zum Download zur Verfügung und kann ohne die Eingabe einer Seriennummer zu Testzwecken installiert werden.

Voraussetzungen für einen Single Copy Cluster unter Exchange Server 2007

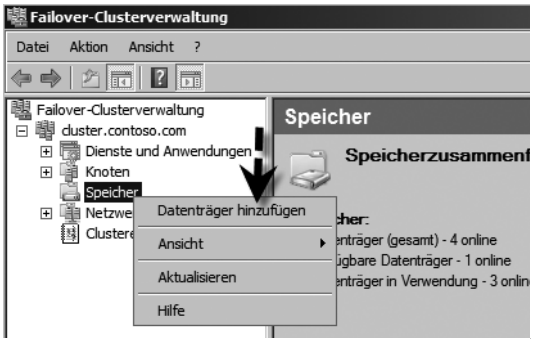
Bevor Sie einen Exchange Server 2007 als Single Copy Cluster installieren können, müssen mehrere Voraussetzungen geschaffen werden:

- Sie müssen einen Aktiv/Passiv-Cluster mit Windows Server 2008 Enterprise Edition installieren, wie bereits in diesem Kapitel ausführlich besprochen. Sie können auch Cluster mit mehreren Knoten erstellen, allerdings muss jeder Cluster über mindestens einen passiven Knoten verfügen.
- Auf dem Cluster darf nur die Mailbox-Server-Rolle installiert werden, alle anderen Serverrollen (Hub-Transport, Edge-Transport, Client- Access, Unified Messaging) unterstützen keine Installation in einem Failover-Cluster. Installieren Sie also einen Mailbox-Server-Cluster, stellen Sie sicher, dass Sie zusätzliche Exchange-Server für die anderen Rollen außerhalb des Clusters installieren müssen. Diese Rollen können auch nach der Installation des Clusters installiert werden.
- Sie benötigen Exchange Server 2007 Enterprise Edition mit SP1, da Exchange Server 2007 Standard Edition kein Clustering unterstützt.
- Ihre DNS-Server müssen für dynamische Aktualisierung eingerichtet sein, da während der Installation eines Clusters automatisch DNS-Einträge erstellt werden.
- Alle Knoten des Clusters müssen Mitglieder der gleichen Domäne sein.
- Die Knoten dürfen nur Mitgliedsserver sein, die Installation eines Single Copy Clusters auf Domänencontrollern wird nicht unterstützt.

- Ein Single Copy Cluster darf nur Exchange-Server mit Exchange Server 2007 enthalten. Ein gemeinsamer Cluster mit Exchange Server 2000/2003 wird nicht unterstützt.
- Auf dem Cluster dürfen keine zusätzlichen Clusterfunktionen wie zum Beispiel SQL Server laufen, der Cluster muss explizit für Exchange Server 2007 zur Verfügung stehen.
- Sie müssen auf allen Knoten die gleiche Version von Exchange Server 2007 und Windows Server 2008 und exakt in den gleichen Verzeichnissen installieren. Die Datenbank wird automatisch auf den gemeinsamen Datenträger verschoben.
- Microsoft empfiehlt die Transaktionsprotokolle, Datenbankdateien und das Quroum auf verschiedenen LUNs in einem SAN abzulegen. Es spricht aber auch nichts gegen eine gemeinsame Ablage von Transaktionsprotokollen und Datenbankdateien. Das Quorum sollte dagegen immer in einem getrennten Laufwerk liegen. Nur bei einer Testumgebung können Sie hier eine Ausnahme machen und alle Daten auf dem gleichen Datenträger ablegen.
- Alle beteiligten Datenträger müssen selbstverständlich mit NTFS formatiert sein.

HINWEIS Unter Umständen reichen die 2 GB-Laufwerke in der Cluster-Testumgebung unter Virtual PC 2007 nicht aus. In diesem Fall erstellen Sie einfach mit StarWind ein neues, größeres Laufwerk und binden dieses über den iSCSI-Initiator auf beiden Clusterknoten genauso ein, wie die anderen Laufwerke. Initialisieren und formatieren Sie dann den Datenträger in der Datenträgerverwaltung des ersten Knotens. Nach der Initialisierung kann der neue gemeinsame Datenträger über den Konsoleneintrag *Speicher* in der Failover-Clusterverwaltung in den Cluster integriert werden (Abbildung 19.48).

Abbildg. 19.48 Hinzufügen eines weiteren gemeinsamen Datenträgers zum Failover-Cluster



Installation eines Single Copy Clusters mit Exchange Server 2007

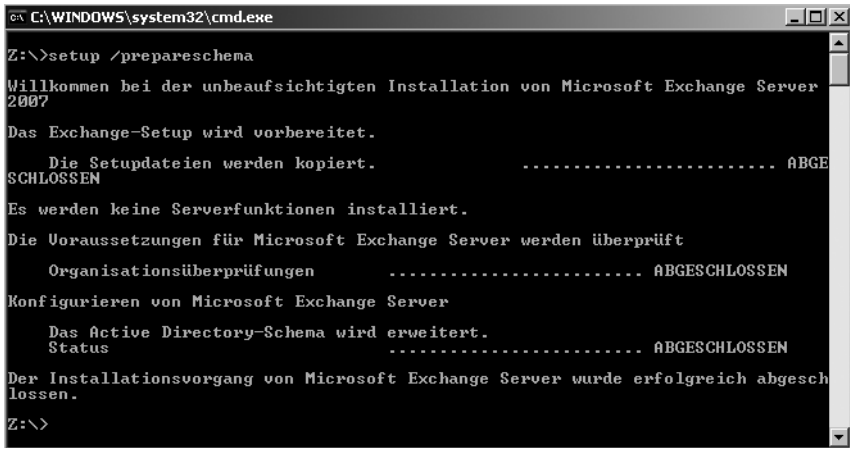
Bevor Sie Exchange Server 2007 in einem Cluster als Single Copy Cluster installieren, müssen Sie zunächst den Cluster unter Windows Server 2008 erstellen und konfigurieren. Erst wenn der Cluster fehlerfrei funktioniert, sollten Sie mit der Installation von Exchange Server 2007 SP1 fortfahren. Im folgenden Abschnitt gehen wird davon aus, dass die vorangegangenen Voraussetzungen erfüllt sind und der Cluster bereits funktioniert.

Vorbereiten des Schemas, der Gesamtstruktur und der Domäne

Bevor Exchange Server 2007 im Cluster installiert werden kann, muss das Schema und die Domäne auf Exchange vorbereitet werden. Auch in der Testumgebung sollten auf dem Domänencontroller vor der Installation des Exchange-Clusters, entsprechende Vorbereitungen vorgenommen werden. Bevor Sie einen Exchange Server 2007 in einem Active Directory installieren können, muss dieses Active Directory um zahlreiche Klassen und Attribute erweitert werden. Einige dieser Attribute sind zum Beispiel die Exchange-Eigenschaften der Benutzer. Haben Sie jedoch mehrere Domänen an mehreren Standorten installiert, sollten Sie die Schemavorbereitung vor der Installation eines Exchange-Servers durchführen. Da die Schemaerweiterungen erst noch auf alle Domänencontroller repliziert werden müssen, kann dieser Vorgang etwas länger dauern. In einer Domäne, auf deren Domänencontrollern diese Erweiterungen noch nicht repliziert wurden, kann Exchange Server 2007 nicht installiert werden, bis die Replikation erfolgreich durchgeführt wurde.

Um das Schema vorzubereiten, starten Sie das Exchange-Setupprogramm auf dem Domänencontroller mit der Option *setup /PrepareSchema*. Nach der Eingabe des Befehls verbindet sich das Installationsprogramm mit dem Schemamaster der Gesamtstruktur und importiert die entsprechenden Daten in das Schema Ihrer Gesamtstruktur. Um diesen Befehl ausführen zu können, muss sich das Konto, mit dem Sie sich angemeldet haben, in den Gruppen *Schema-Admins* und *Organisations-Admins* befinden. Sie müssen den Befehl *setup /PrepareSchema* immer auf einem Server durchführen, der sich in der gleichen Domäne und im gleichen Active Directory-Standort befindet, wie der Schemamaster der Gesamtstruktur. Haben Sie bei der Installation von Exchange Server 2007 in eine Exchange 2000/2003-Organisation vor der Ausführung von *setup /PrepareSchema* nicht die Domänen mit *setup /PrepareLegacyExchangePermissions* vorbereitet, wird dieser Befehl nachträglich automatisch gestartet. In diesem Fall muss der Server, auf dem Sie *setup /PrepareSchema* starten, eine Verbindung zu allen Domänen in der Gesamtstruktur herstellen können.

Abbildg. 19.49 Active Directory-Schema für die Installation von Exchange Server 2007 vorbereiten



HINWEIS Damit das Installationsprogramm von Exchange Server 2007 SP1 zur Erweiterung von Active Directory-Schemas gestartet werden kann, müssen auf dem Server das .NET Framework 2.0 sowie die PowerShell installiert werden. Wird das Schema mit Exchange Server 2007 SP1 auf einem Windows Server 2003-Domänencontroller aktualisiert, muss das SP1 für .NET Frame-

work 2.0 installiert werden. Dieses wird ebenfalls von Microsoft auf der Seite *http://www.microsoft.com/downloads/details.aspx?familyid=0C1B0A88-59E2-4EBA-A70E-4CD851C5FCC4&displaylang=de* zur Verfügung gestellt.

Probleme bei der Schemaerweiterung

Bei der Erweiterung des Schemas besteht unter Umständen die Möglichkeit, dass die Erweiterung in der Registry auf dem Schemamaster deaktiviert ist. Sollte das bei Ihnen der Fall sein, bricht die Schemaerweiterung ab. In diesem Fall sollten Sie auf dem Schemamaster zu folgendem Registrykey wechseln:

HKLM/System/CurrentControlSet/Services/NTDS/Parameters

Weisen Sie den beiden DWORD-Werten *Schema Update Allowed* und *Schema Delete Allowed* den Wert *1* zu. Warten Sie nach den Änderungen 10 bis 15 Minuten, bevor Sie die Schemaerweiterung erneut ausführen. Sie müssen dazu den Server nicht neu starten.

Nach der Vorbereitung des Schemas müssen Sie noch den Befehl *setup /PrepareAD* ausführen, damit in der Gesamtstruktur Objekte für Exchange Server 2007 angelegt werden. Ist in der Organisation noch keine Exchange-Organisation angelegt, wird der Befehl *setup /PrepareAD /organizationname:<Name>* verwendet. Dieser Befehl legt zum Beispiel die notwendigen Sicherheitsgruppen für Exchange Server 2007 in der Stammdomäne (Root) der Gesamtstruktur an. Um diesen Befehl ausführen zu können, müssen Sie sich mit einem Benutzerkonto anmelden, dass Mitglied in der Gruppe *Organisations-Admins* ist. Setzen Sie in der Organisation Exchange 2000 oder 2003-Server ein, müssen Sie noch Mitglied der Exchange-Administratoren dieser Organisation sein. Sie müssen den Befehl auf einem Server durchführen, der sich in der gleichen Domäne und dem gleichen Active Directory-Standort befindet, wie der Schemamaster der Gesamtstruktur.

Abbildg. 19.50 Vorbereiten der Gesamtstruktur für Exchange Server 2007

Haben Sie bei der Ausführung von *setup / PrepareAD* noch nicht *setup /PrepareSchema* ausgeführt, wird auch dieser Befehl nachträglich automatisch gestartet. Sie können die erfolgreiche Durchführung des Befehls überprüfen, indem Sie das Snap-In *Active Directory-Benutzer und -Computer* starten. Unterhalb der Domäne wurde automatisch eine neue OU mit der Bezeichnung *Microsoft Exchange Security Groups* angelegt, in der sich die notwendigen universellen Sicherheitsgruppen

befinden, die Exchange Server 2007 benötigt. Folgende universellen Sicherheitsgruppen sollten sich in der OU befinden:

- Exchange Organization Administrators
- Exchange Recipient Administrators
- Exchange View-Only Administrators
- Exchange Servers
- ExchangeLegacyInterop

Während der Installation von Exchange Server 2007 auf einem Server wird die Gruppe *Exchange Organization Administrators* automatisch in die lokale Administratorengruppe des Servers aufgenommen. Da die lokale Administrator-Gruppe auf Domänencontrollern fast umfassende Berechtigungen in der Domäne hat, erhalten dadurch unter Umständen Exchange-Administratoren mehr Rechte, als diese haben sollen, beachten Sie daher diesen Punkt bei der Planung und Installation.

Als Nächstes müssen noch die einzelnen Domänen in der Gesamtstruktur für die Installation von Exchange Server 2007 vorbereitet werden. Führen Sie das Exchange Server 2007-Setupprogramm mit einer der folgenden Optionen aus:

- **setup /PrepareDomain** Führen Sie diesen Befehl aus, wird nur die Domäne vorbereitet, in der sich der Server befindet auf dem Sie den Befehl starten. Sie müssen diesen Befehl nicht in jeder Domäne ausführen, in der Sie auch *setup / PrepareAD* durchgeführt haben, da hier die Domäne schon vorbereitet wurde.
- **setup /PrepareDomain: <FQDN der Domäne>** Mit diesem Befehl können Sie remote einzelne Domänen vorbereiten.
- **setup /PrepareAllDomains** Bereitet alle Domänen in der Gesamtstruktur für Exchange Server 2007 vor. Führen Sie diesen Befehl aus, erhalten Sie unter Umständen eine Fehlermeldung bei Domänen, die sich an anderen Active Directory-Standorten befinden, wenn zum Beispiel die Replikation noch nicht abgeschlossen worden ist. Führen Sie in diesem Fall eine manuelle Replikation durch oder warten Sie, bis die Replikation abgeschlossen worden ist. Starten Sie den Befehl dann noch einmal.

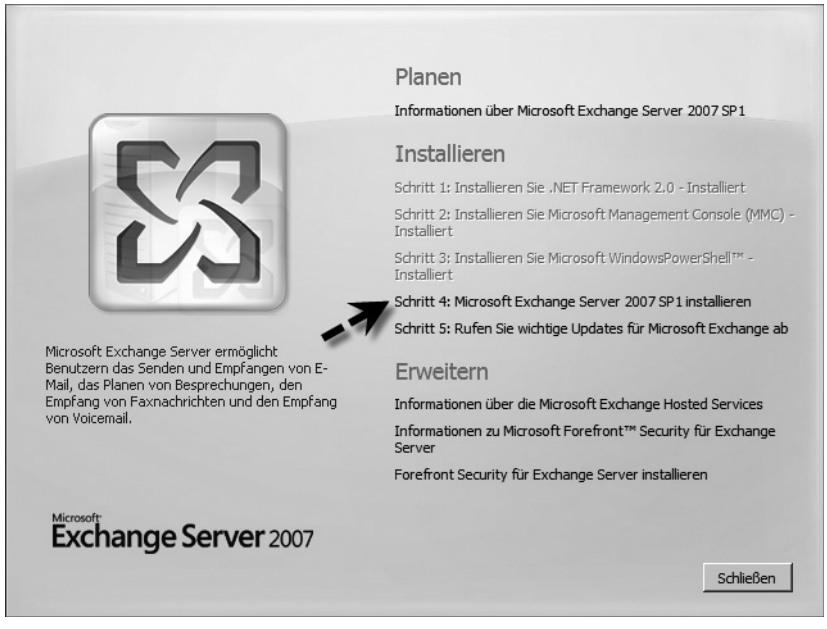
Abbildg. 19.51 Vorbereiten der Active Directory-Domänen für Exchange Server 2007

Damit Sie diese Befehle ausführen können, müssen Sie Mitglied der Gruppe *Organisations-Admins* sein, sowie Mitglied der Gruppe *Domänen-Admins* in jeder Domäne, die Sie vorbereiten. Sie können die Ausführung dieses Befehls überprüfen, in dem Sie im Snap-In *Active Directory-Benutzer und -Computer (Start/Ausführen/dsa.msc)* in der OU *Microsoft Exchange System Objects* eine neue globale Sicherheitsgruppe *Exchange Install Domain Servers* finden. Die OU *Microsoft Exchange System Objects* wird aber nur angezeigt, wenn Sie über das Menü *Ansicht* die erweiterten Funktionen aktiviert haben. Diese Gruppe wird benötigt, wenn Sie Exchange Server 2007 an einem anderen Active Directory-Standort installieren, an dem sich die Stammdomäne der Gesamtstruktur befindet. Durch diese Gruppe werden Fehlermeldungen während der Installation vermieden, die durch langsame Replikation erscheinen können. Die Gruppe *Exchange Install Domain Servers* ist Mitglied der Gruppe *Exchange Servers* in der Stammdomäne der Gesamtstruktur.

Installation der Mailbox-Server-Rolle auf dem aktiven Knoten

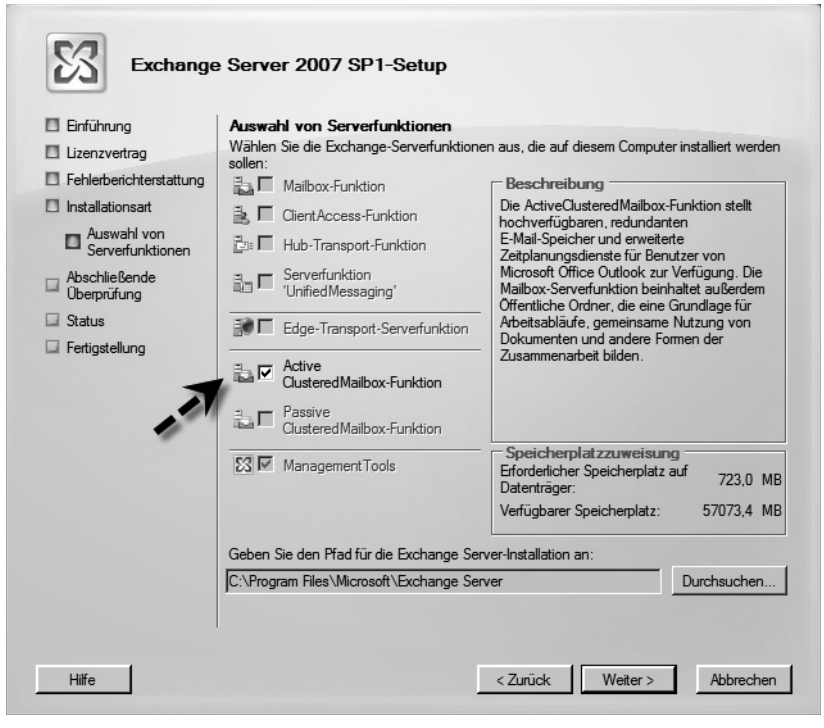
Haben Sie den Cluster, wie bereits beschrieben, installiert und konfiguriert, installieren Sie Exchange Server 2007 zunächst auf dem aktiven Knoten. Sie können die Installation auf dem aktiven Knoten entweder über die Befehlszeile oder die grafische Oberfläche durchführen. Stellen Sie sicher, dass alle Voraussetzungen für die normale Exchange-Installation getroffen worden sind. Unter Windows Server 2008 bedeutet das die Installation der Serverrolle *Webserver* mit den zusätzlichen Rollendiensten *Verwaltungsdienst*, *IIS 6.0-Verwaltungskompatibilität* mit allen Unterdiensten, und des Features *Windows PowerShell* auf allen beteiligten Knoten. Klicken Sie dann im Anschluss auf die Installation von Exchange Server 2007 SP1. Im ersten Fenster erhalten Sie eine kurze Einführung, welche der Installation auf einem normalen Server entspricht. Klicken Sie auf *Weiter*.

Abbildg. 19.52 Installieren von Exchange Server 2007 auf einem Windows Server 2008-Cluster



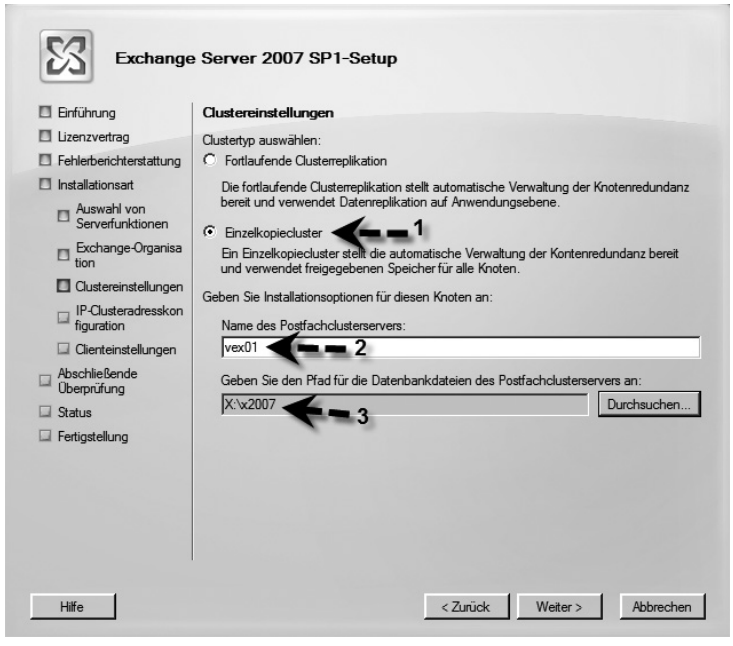
Auf der nächsten Seite bestätigen Sie den Lizenzvertrag, wie auch bei einer normalen Installation. Klicken Sie danach auf *Weiter*. Auf der Seite mit der Fehlerberichterstattung deaktivieren Sie am besten diese Funktion wieder. Auch dieser Installationsschritt entspricht der normalen Installation. Als Nächstes wird die Installationsart von Exchange Server 2007 bestimmt. Wählen Sie hier *Benutzerdefinierte Installation von Microsoft Exchange-Server* aus, da nur die Mailbox-Rolle installiert werden darf. Auf der nächsten Seite können Sie die Serverfunktionen auswählen. Aktivieren Sie hier die Option *ActiveClusteredMailbox-Funktion*. Die Verwaltungs-Tools werden dabei automatisch mit ausgewählt (Abbildung 19.53).

Abbildg. 19.53 Installieren des aktiven Knotens eines Clusters



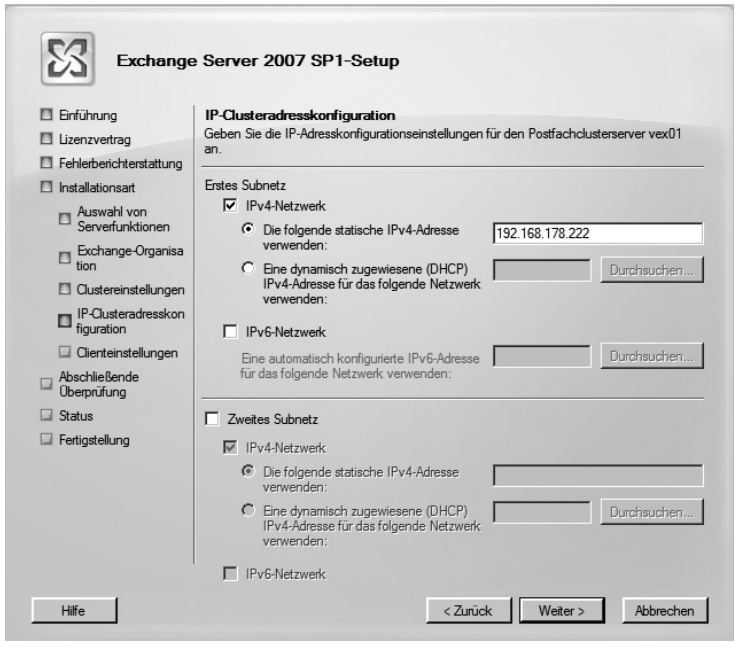
Auf der nächsten Seite des Assistenten wählen Sie die Clusterinstallation aus, die Sie durchführen möchten. Aktivieren Sie hier die Funktion *Einzelkopiecluster* (Abbildung 19.54). Zusätzlich müssen Sie auf dieser Seite die Bezeichnung des Exchange-Servers eingeben. Der Server erhält die Bezeichnung, die Sie hier eingeben, nicht die Bezeichnung eines der Knoten oder des Clusters selbst. Der hier gewählte Namen ist von allen anderen vollkommen unabhängig und wird von den Anwendern für den Zugriff auf ihre Postfächer verwendet. Zusätzlich tragen Sie auf dieser Seite auch die IP-Adresse dieses neuen virtuellen Mailbox-Servers ein. Auch diese IP-Adresse muss sich von den anderen IP-Adressen des Clusters unterscheiden und darf nicht identisch mit der IP-Adresse des Clusters selbst sein. Die IP-Adresse muss von den Clients und anderen Servern im Netzwerk erreichbar sein. Außerdem wählen Sie in diesem Fenster auch den Speicherplatz der Datenbankdateien und Transaktionsprotokolle auf dem gemeinsamen Datenträger aus. Achten Sie darauf, dass sich diese Dateien niemals in der Root eines Laufwerkes befinden dürfen, sondern immer in einem Unterverzeichnis. Legen Sie notfalls ein solches Verzeichnis an.

Abbildg. 19.54 Auswählen der Clustereinstellungen für Exchange Server 2007



Als Nächstes legen Sie die IP-Adresse des virtuellen Exchange-Servers fest. Auch diese muss einzigartig sein, wie die beim Einsatz eines Datei- oder Druckservers im Cluster.

Abbildg. 19.55 Konfigurieren der IP-Adresse des Exchange-Servers



Auf der nächsten Seite findet eine Überprüfung statt und Sie erhalten die notwendigen Ergebnisse dieser Überprüfung. Sind die Voraussetzungen erfolgreich durchgeführt worden, können Sie über die Schaltfläche *Installieren* die Installation des aktiven Clusterknotens beginnen (Abbildung 19.56). Kann die Installation nicht fortgeführt werden, erhalten Sie entsprechende Informationen. Beseitigen Sie zuerst alle Fehler, bevor Sie die Installation fortsetzen. Treten Fehler auf, beheben Sie diese und starten Sie die Installation erneut. Gehen Sie genauso vor, wie zuvor beschrieben. Erst wenn die Überprüfung der Installationsvoraussetzungen für einen aktiven Clusterknoten durchgeführt wurden, können Sie die Installation abschließen. Der Assistent unterscheidet bei der Überprüfung zwischen Warnungen und Fehlern. Treten Fehler auf, kann die Installation nicht fortgesetzt werden, bei Warnungen können Sie selbst entscheiden, ob Sie die Installation fortsetzen möchten oder nicht. Nachdem Sie auf die Schaltfläche *Installieren* geklickt haben, beginnt der Assistent mit der Installation von Exchange Server 2007 auf dem aktiven Clusterknoten. Ist die Installation abgeschlossen, erhalten Sie entsprechende Meldungen und können das Fenster schließen. Mit diesem Schritt ist die Installation auf dem aktiven Knoten abgeschlossen und Sie können mit der Installation auf dem passiven Knoten fortfahren. Klicken Sie auf *Fertig stellen*, wird die Installation von Exchange Server 2007 abgeschlossen. Standardmäßig ist die Option *Installation mithilfe der Exchange Verwaltungskonsole abschließen* ausgewählt. Bleibt die Option aktiviert, wird automatisch nach der Installation die Exchange-Verwaltungskonsole gestartet.

Installation der Mailbox-Server-Rolle auf dem passiven Knoten des Clusters

Haben Sie die Installation auf dem aktiven Knoten abgeschlossen, können Sie Exchange Server 2007 auf dem passiven Knoten installieren. Achten Sie darauf, dass Sie vor der Installation von Exchange Server 2007 zunächst die Voraussetzungen und die notwendigen Komponenten und Patches installieren. Der aktive Knoten muss bei der Installation des passiven Knotens ebenfalls gestartet sein. Um Exchange Server 2007 auf dem passiven Knoten zu installieren, gehen Sie folgendermaßen vor:

1. Installieren Sie zunächst wie beschrieben den aktiven Knoten.
2. Installieren Sie auf dem zweiten Knoten ebenfalls die Rolle *Webserver* und die notwendigen Rollendienste und Features.
3. Starten Sie das Installationsprogramm für Exchange-Server auf dem passiven Knoten.
4. Stellen Sie sicher, dass alle Voraussetzungen für die normale Exchange-Installation erfüllt sind. Führen Sie anschließend die Installation von Exchange Server 2007 durch (Schritt 4 im Menü).
5. Auf dem ersten Fenster erhalten Sie eine kurze Einführung, welche der Installation auf einem normalen Server entspricht. Klicken Sie auf *Weiter*.
6. Auf der nächsten Seite bestätigen Sie den Lizenzvertrag, wie auch bei einer normalen Installation. Klicken Sie danach auf *Weiter*.
7. Auf der Seite mit der Fehlerberichterstattung deaktivieren Sie diese Funktion am besten wieder. Auch dieser Installationsschritt entspricht der normalen Installation.
8. Auf der nächsten Seite des Assistenten können Sie die Installationsart bestimmen. Wählen Sie hier *Benutzerdefinierte Installation von Microsoft Exchange-Server* aus.
9. Auf der nächsten Seite können Sie die Serverfunktionen auswählen. Aktivieren Sie hier die Option *Passive ClusteredMailbox-Funktion*. Die Management-Tools werden dabei automatisch mit ausgewählt.
10. Haben Sie die Funktion ausgewählt, überprüft der Installationsassistent, ob alle Voraussetzungen erfüllt sind. Werden keine Fehler protokolliert, können Sie die Installation abschließen.

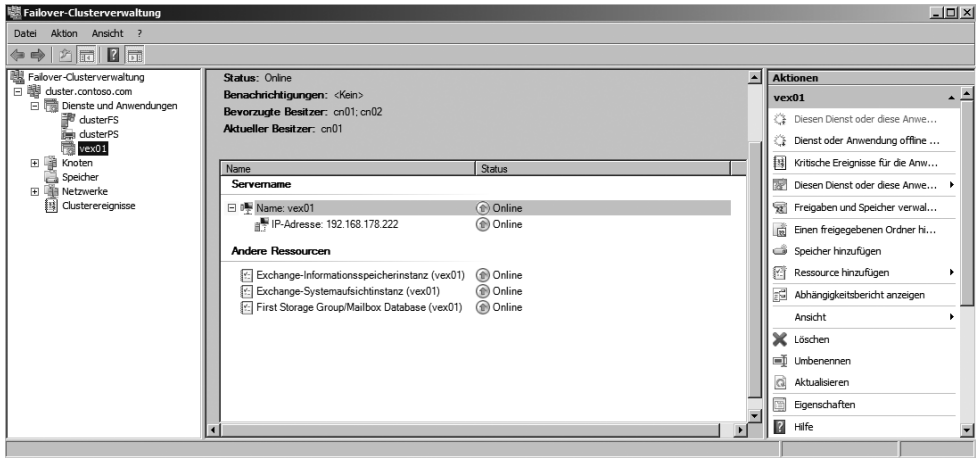
11. Nach einigen Minuten wird die Installation abgeschlossen und Sie erhalten eine Zusammenfassung angezeigt. Schließen Sie das Fenster mit der Zusammenfassung, wird die Installation abgeschlossen.
12. Die Installation sollte zu keinen Fehlermeldungen führen und alle Funktionen sollten erfolgreich abgeschlossen werden. Sie können sich den Inhalt des Fensters in eine Textdatei mit der Tastenkombination Strg + C kopieren. Ist die Installation erfolgreich abgeschlossen, können Sie das Fenster mit der Schaltfläche *Fertig stellen* schließen.

Überprüfen des passiven Clusterknotens

Die Installation eines passiven Clusterknotens ist wesentlich weniger umfangreich als die Installation eines aktiven Clusterknotens. Nach der Installation ist auch eine Diagnose des passiven Clusterknotens angebracht:

- Nach der Installation sollten Sie zunächst in der Ereignisanzeige überprüfen, ob irgendwelche Fehler protokolliert werden.
- Als Nächstes sollten Sie die Clusterverwaltung öffnen und überprüfen, ob die Verbindung zum Cluster fehlerfrei hergestellt werden kann.
- Der nächste Schritt besteht darin, die Clustergruppe des Exchange-Servers auf den passiven Knoten zu verschieben und diesen damit zum aktiven Knoten machen. Der bisherige aktive Knoten wird danach zum passiven Knoten. Dieser Vorgang wird von Microsoft als Handoff bezeichnet. Dieser Vorgang sollte in kurzer Zeit abgeschlossen sein und keinerlei Fehlermeldungen verursachen. Exchange Server 2007 wird im Cluster unter dem Namen des virtuellen Servers angezeigt, den Sie bei der Installation vorgegeben haben. Das Verschieben wird über das Kontextmenü durchgeführt, wie weiter vorne bereits besprochen wurde.

Abbildg. 19.56 Anzeige des virtuellen Exchange-Servers im Cluster



TIPP Neben der Möglichkeit, die Clustergruppen über die Clusterverwaltung von einem Knoten auf den anderen zu verschieben, können Sie auch einfach den aktiven Knoten herunterfahren. Durch den Heartbeat sollte dies der passive Knoten nach kurzer Zeit bemerken und alle Clustergruppen automatisch übernehmen.

Anhalten und Starten eines virtuellen Exchange-Servers

Müssen Sie Wartungsarbeiten am Server durchführen, können Sie den virtuellen Server für Anwender deaktivieren. Der Cluster selbst bleibt aktiviert, aber die Anwender können keine Verbindung mehr zum Server aufbauen. Sie können für diesen Weg entweder die Clusterverwaltung, oder die Exchange-Verwaltungsshell verwenden. Um eine Clustergruppe in der Clusterverwaltung zu deaktivieren, klicken Sie diese mit der rechten Maustaste an und rufen im Kontextmenü den Befehl *Dienst oder Anwendung offline schalten* auf. Im Anschluss fährt der Cluster alle Ressourcen des Servers herunter. Der Cluster selbst bleibt dabei aktiviert, nur die Exchange-Dienste und der Zugriff für die Clients wird deaktiviert. Auf dem gleichen Weg können Sie die Gruppe wieder online schalten.

Loadbalancing-Cluster (NLB) einsetzen

Die Aufgabe eines Failover-Clusters besteht darin, einen oder mehrere Serverdienste vor eventuellen Ausfällen zu schützen. Loadbalancing-Cluster haben die Aufgabe, die Last eines Servers auf mehrere zu verteilen, damit die Auslastung einzelner Server gesenkt und die Performance verbessert wird.

Loadbalancing vs. Failover-Cluster

Bei Loadbalancing werden bis zu 32 Server zu einem Loadbalancing-Cluster zusammengefügt, der von außen über eine gemeinsame virtuelle IP-Adresse angesprochen wird und somit wie ein einziger Computer erscheint. Vor allem Web- oder Proxyserver werden durch diese Technologie abgesichert. Auf allen beteiligten Servern liegen parallel alle notwendigen Daten und Programme. Beim Zugriff werden die Anwender durch den Lastenausgleich auf die Server verteilt. Dabei kann das Lastenausgleichsgewicht der einzelnen Hosts im Cluster für jeden einzelnen Server konfiguriert werden. Fällt ein Host des Clusters aus, übernehmen die anderen Server im Cluster die Zugriffe der Anwender. Daten werden allerdings nicht ausgetauscht oder mit einem gemeinsamen Datenträger zur Verfügung gestellt. Das ist Sache eines Failover-Clusters. Serverdienste wie Proxyserver können mit dem Dienst aber vor Ausfall geschützt werden, da diese keine Daten speichern müssen, die auf einem gemeinsamen Datenträger abgelegt werden. Der Zugriff der Clients erfolgt zwar über die virtuelle IP-Adresse des NLB-Clusters, aber schließlich auf die physischen Server in diesem Cluster. Bei einem Failover-Cluster mit Exchange Server 2007 SP1 zum Beispiel findet der Zugriff über den virtuellen Server statt, der auf den Knoten bereitgestellt ist, der aber auch über einen gemeinsamen Datenträger verfügt.

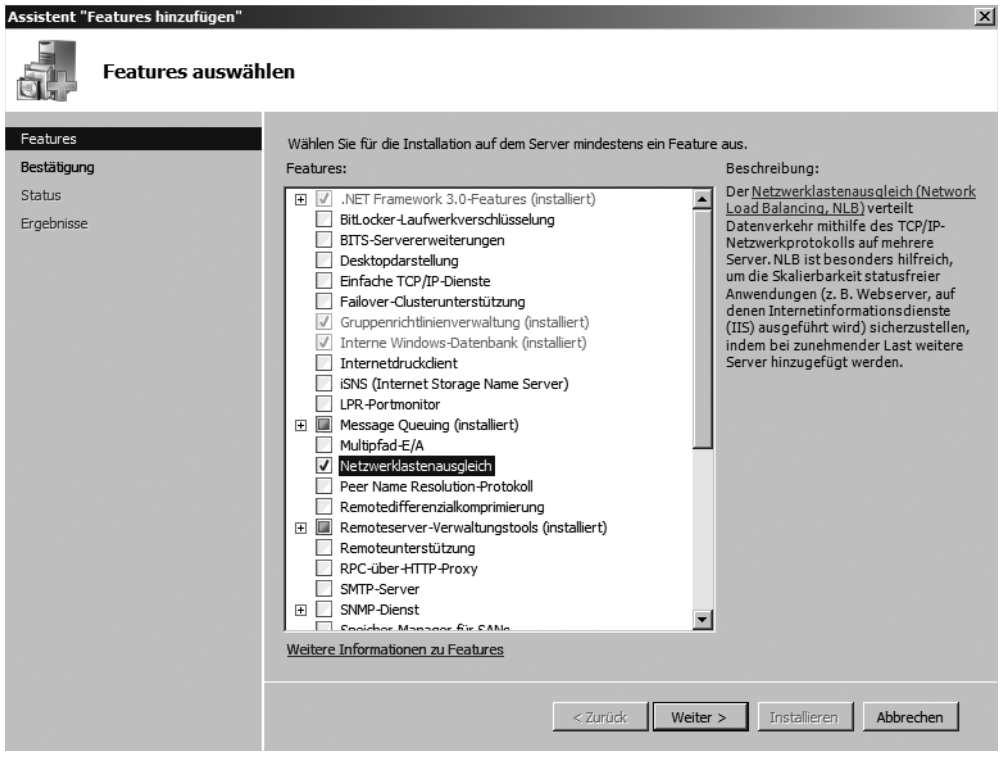
Neuerungen im Lastenausgleich

Für die Kommunikation der NLB-Hosts im NLB-Cluster kann unter Windows Server 2008 jetzt auch IPv6 verwendet werden. IPv6-Adressen können für einzelne Hosts, aber auch für den Cluster als Ganzes konfiguriert werden. Für einzelne Knoten können mehrere dedizierte IP-Adressen konfiguriert werden. Die Verwaltung mit dem Lastensausgleich-Manager wurde ebenfalls verbessert. Mit diesem Tool findet die komplette Steuerung des NLB-Clusters statt.

Lastenausgleich installieren

Der Lastenausgleich wird unter Windows Server 2008 über den Server-Manager als Feature installiert. Öffnen Sie zur Installation den Server-Manager und klicken Sie auf *Features/Features hinzufügen*. Wählen Sie das Feature *Netzwerklastenausgleich* aus und führen Sie die Installation durch. Während der Installation des Features müssen keinerlei Konfigurationen vorgenommen werden. Die Einrichtung des NLB-Clusters findet nachträglich in der entsprechenden Verwaltungskonsole statt.

Abbildg. 19.57 Netzwerklastenausgleich installieren



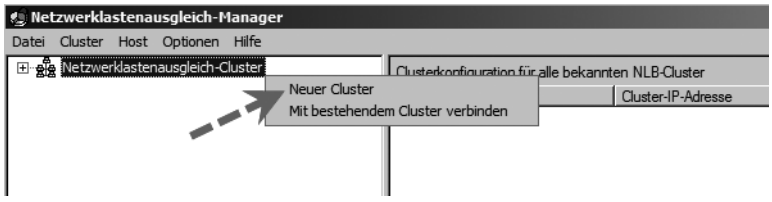
Lastenausgleich konfigurieren

Nach Installation des Features auf einem NLB-Host, wird das Verwaltungsprogramm über *Start/Verwaltung/Netzwerklastenausgleich-Manager* gestartet. Alternativ kann im Suchfeld des Startmenüs der Befehl *nlbmgr* eingegeben werden. Der wichtigste Schritt bei der Verwaltung eines solchen Clusters ist zunächst die Erstellung des NLB-Clusters. Dabei werden hauptsächlich drei Bereiche konfiguriert:

- **Hosts** Die einzelnen Clustermitglieder, Hosts genannt, müssen konfiguriert werden.
- **Cluster** Der Cluster als Sammlung der Hosts muss konfiguriert werden.
- **Regeln** Die Ports und Regeln werden konfiguriert, auf deren Basis der Cluster die Anfragen der Anwender verteilt.

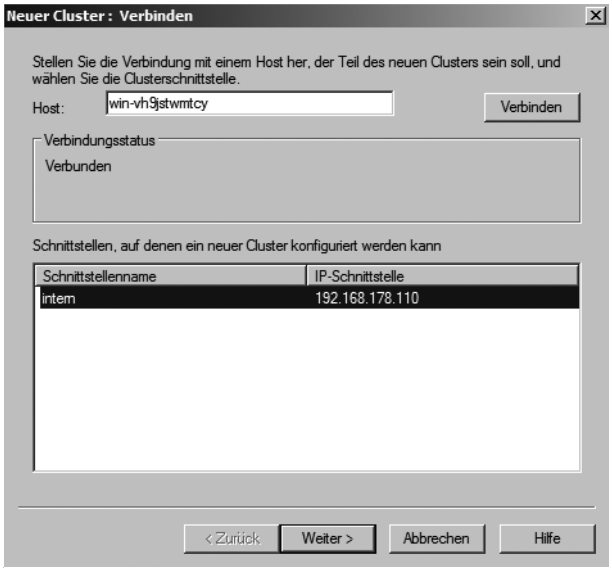
Nach dem Aufruf des Netzwerklastenausgleich-Managers wird nach einem Klick mit der rechten Maustaste auf den Knoten *Netzwerklastenausgleich-Cluster* im zugehörigen Kontextmenü der Eintrag *Neuer Cluster* ausgewählt.

Abbildg. 19.58 Erstellen eines neuen Netzwerklastenausgleich-Clusters



Im nächsten Fenster geben Sie den Namen des ersten Hosts im NLB-Cluster ein und klicken auf Verbinden. Der Assistent baut anschließend eine Verbindung mit dem Host auf. Anschließend werden die Netzwerkverbindungen des Servers angezeigt, mit denen der NLB-Cluster kommunizieren kann.

Abbildg. 19.59 Verbindung mit dem ersten Knoten des NLB-Hosts

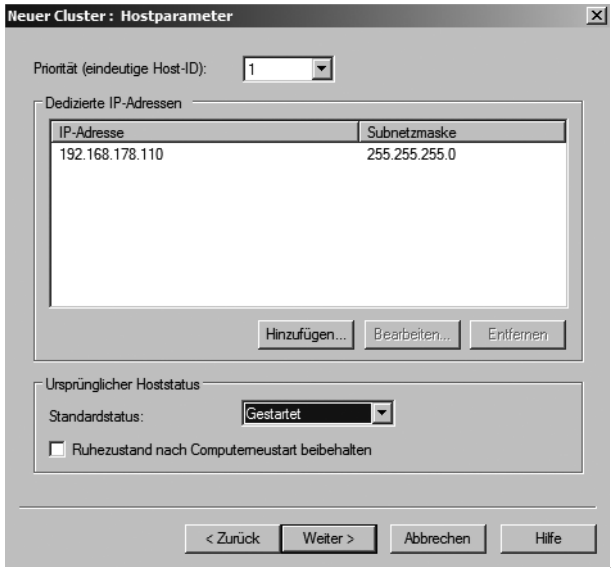


Auf der nächsten Seite des Assistenten wird zunächst die eindeutige Host-ID festgelegt. Im Cluster beantwortet der Host mit der niedrigsten ID die Anfragen der Clients, die durch keine Portregel erfasst werden. Falls ein System innerhalb des Clusters ausfällt, muss ein anderer Server dessen Arbeit übernehmen. Welcher Server das ist, bestimmen Sie, indem Sie unter *Priorität* einen Wert angeben, welcher den Server bestimmt, der die Last übernimmt. Dieser Wert kennzeichnet jeden einzelnen Server des Clusters und muss eindeutig sein.

Im Bereich *Dedizierte IP-Adressen* können, neben der bereits integrierten IP-Adresse des Servers, weitere IP-Adressen eingefügt werden, auf die der Host antwortet. Neben IPv4-Adressen können über die Schaltfläche *Hinzufügen* auch IPv6-Adressen hinzugefügt werden.

Über die Option *Ursprünglicher Hoststatus* wird festgelegt, ob NLB automatisch mit dem Betriebssystem gestartet wird und dem NLB-Cluster damit beigetreten werden kann. Es besteht auch die Möglichkeit, den Cluster manuell nach dem Start des Betriebssystems zu starten. Beim Start von Windows Server 2008 arbeitet das System in der Standardeinstellung sofort im Cluster. Falls Sie das nicht wünschen, wählen Sie unter *Ursprünglicher Hoststatus* die Einstellung *Anhalten*. Sie können die Loadbalancing-Cluster-Funktion anschließend in der Eingabeaufforderung über das Kommando *wlbs start* manuell starten und über *wlbs stop* beenden. Neben *wlbs.exe*, kann in der Befehlszeile auch das Tool *nlb.exe* zur Verwaltung eines NLB-Clusters verwendet werden. Server, deren Standardstatus auf *Gestartet* gesetzt ist, die dann aber manuell angehalten wurden, nehmen nach einem Neustart sofort wieder am Lastenausgleich teil, es sei denn, Sie aktivieren das Kontrollkästchen *Ruhezustand nach Computerneustart beibehalten*. In diesem Fall bleiben sie so lange angehalten, bis Sie die Komponenten manuell wieder starten.

Abbildg. 19.60 Hostparameter für den NLB-Cluster konfigurieren

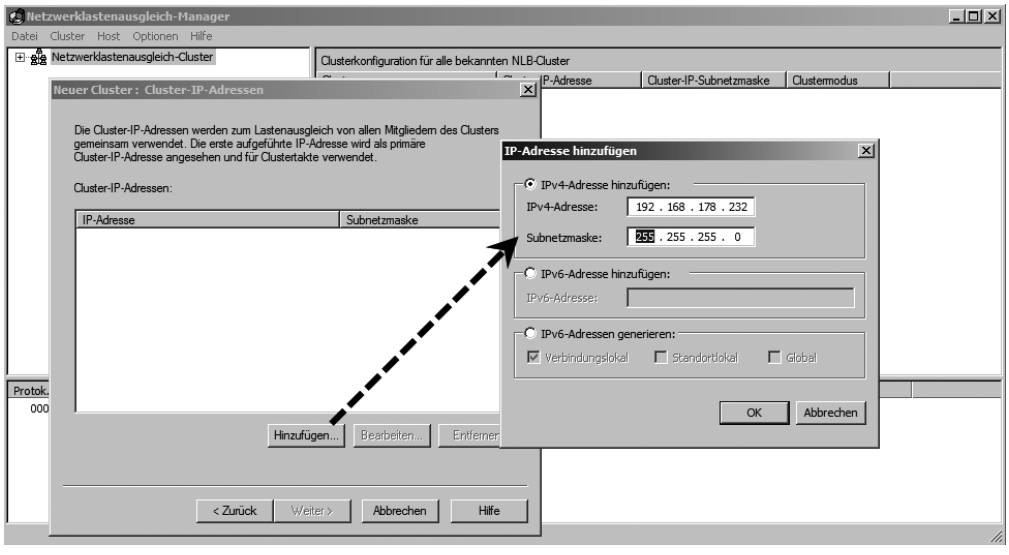


Auf der nächsten Seite des Assistenten werden die Cluster-IP-Adressen konfiguriert. Auf diese IP-Adressen reagiert der Cluster und die Anfragen der Anwender werden automatisch auf die Knoten des Clusters verteilt. Auch hier werden sowohl IPv4 als auch IPv6-Adressen unterstützt (Abbildung 19.61).

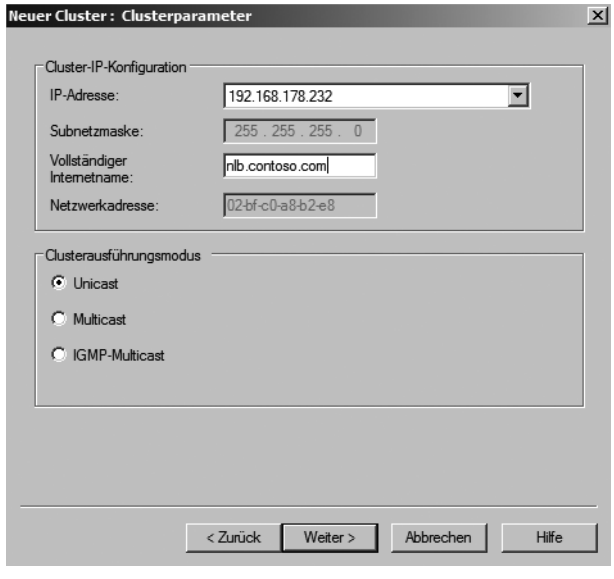
Auf der nächsten Seite des Assistenten wird der DNS-Name des Clusters, als auch der Clusterausführungsmodus konfiguriert. Im Feld *Vollständiger Internetname* geben Sie den Namen des Loadbalancing-Clusters an. Auch dieser Name muss auf allen Servern des Clusters gleich lauten. Außerdem muss eine Namensauflösung über DNS möglich sein. Damit alle Server des Clusters auf eine Verbindungsanfrage reagieren können, muss nicht nur die virtuelle IP-Adresse auf allen Computern identisch sein. Damit ein Datenpaket zugestellt werden kann, muss zu der IP-Adresse die zugehörige physische Adresse der Netzwerkkarte (die MAC-Adresse) ermittelt werden. Diese Adresse ist bei der Herstellung der Karte fest vorgegeben, kann aber später durch die Netzwerktreiber überschrieben werden. Für alle Netzwerkkarten, für die das Loadbalancing aktiviert ist, wird diese MAC-Adresse

auf den gleichen Wert gesetzt, der aus der IP-Adresse des Clusters berechnet wird. Falls die Übertragung von Daten an den Loadbalancing-Cluster auch über Multicast-Pakete erfolgen soll, was zum Beispiel bei einigen Streaming Media-Formaten der Fall ist, ändern Sie den Clusterausführungsmodus von *Unicast* auf *Multicast*. Dadurch ändert sich auch die automatisch generierte Netzwerkadresse. Um den Datenverkehr zu reduzieren, können Sie zusätzlich IGMP-Multicast aktivieren. Generell sollte aber immer besser mit Unicast gearbeitet werden.

Abbildg. 19.61 Festlegen der Cluster-IP-Adressen

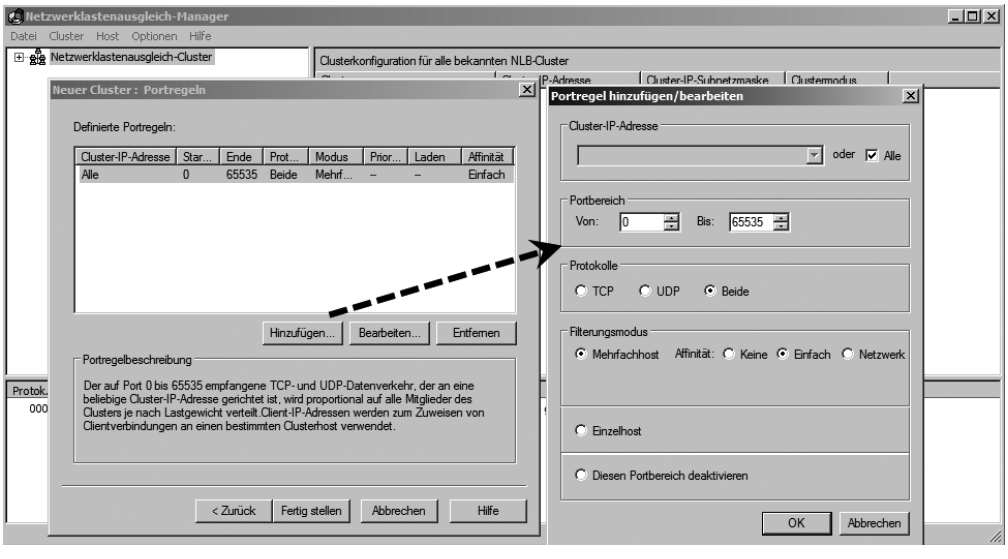


Abbildg. 19.62 Clustername und Clusterausführungsmodus konfigurieren



Auf der nächsten Seite werden die Portregeln definiert, also welche Ports mit welcher Priorität behandelt werden. Dazu werden jeweils Regeln definiert, indem Sie die gewünschten Werte einstellen und dann abschließend über *Hinzufügen* diese Werte als Regel übernehmen. Die neue Regel gilt zunächst für alle IP-Adressen des Clusters. Wenn Sie das Kontrollkästchen *Alle* deaktivieren, können Sie aber eine spezifische Adresse eingeben. Unter *Portbereich* geben Sie den Port bzw. den Bereich an, für den diese Regel gilt. Anschließend wählen Sie das verwendete Transportprotokoll *TCP, UDP* oder *Beide* aus. Wie der Server innerhalb des Loadbalancing-Clusters reagiert, geben Sie über den *Filterungsmodus* an. In der Standardeinstellung *Mehrfachhost* können die von einem Client ausgehenden Verbindungen auf mehrere Server innerhalb des Clusters verteilt werden. Dies ist jedoch an der Stelle problematisch, wenn zu einer scheinbar einzelnen Anfrage in Wirklichkeit mehrere Verbindungen hergestellt werden. Dies tritt zum Beispiel bei Webservern auf. Dort stellt der Browser mehrere Verbindungen zum Webserver her, um die auf einer Seite angezeigten Objekte parallel zu übertragen. Bei statischen Inhalten führt dies zu keinen weiteren Problemen. Anders jedoch sieht es bei dynamisch erstellten Seiten aus, bei denen der eine Webserver natürlich keine Informationen darüber erhält, welche Daten dieser für den Anwender bereitgestellt hat. Hier ist die Einstellung *Einzelhost* angebracht, wobei ein einzelner Server im Cluster alle weiteren Verbindungen eines Clients ebenfalls übernimmt. Haben Sie dagegen die Einstellung *Diesen Portbereich deaktivieren* gewählt, nimmt der Server Anfragen auf diesen Ports überhaupt nicht entgegen. Auf diese Weise kann auch sehr leicht ein einfacher Filter eingerichtet werden. Für jede IP-Adresse können unterschiedliche Regeln konfiguriert sein.

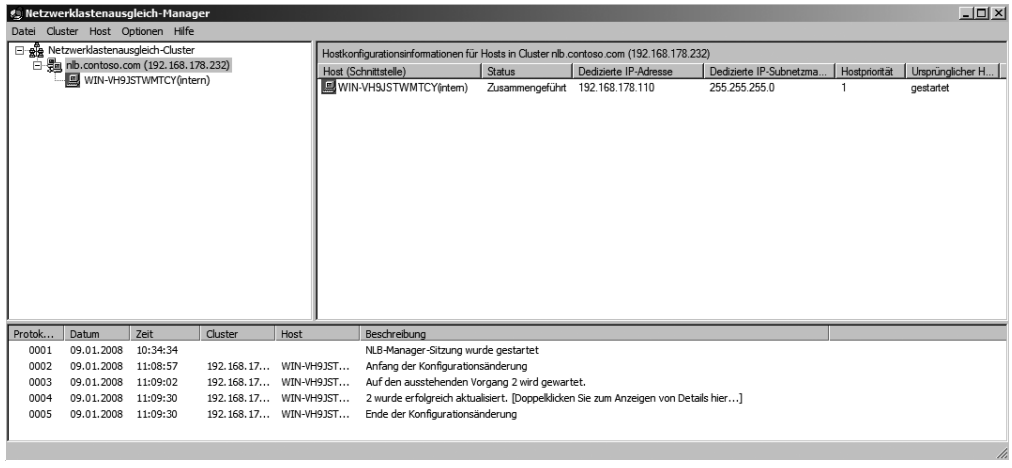
Abbildg. 19.63 Konfigurieren der Portregeln des Clusters



Über die Einstellung *Affinität* wird das Verhalten des Clusters auf eingehende Verbindungen von ein und demselben Client geregelt. In der Standardeinstellung *Einfach* werden alle Verbindungsanfragen von einem Client jeweils an denselben Server innerhalb des Clusters weitergeleitet. So nimmt auch der Zielserver an, dass alle Anfragen von einem Client an ihn gerichtet werden. Wählen Sie dagegen *Keine*, wird jede neue Anfrage an den Cluster jeweils an den am wenigsten belasteten Server weitergeleitet. Dies hat allerdings zur Folge, dass alle von ursprünglich einem Client ausgehenden

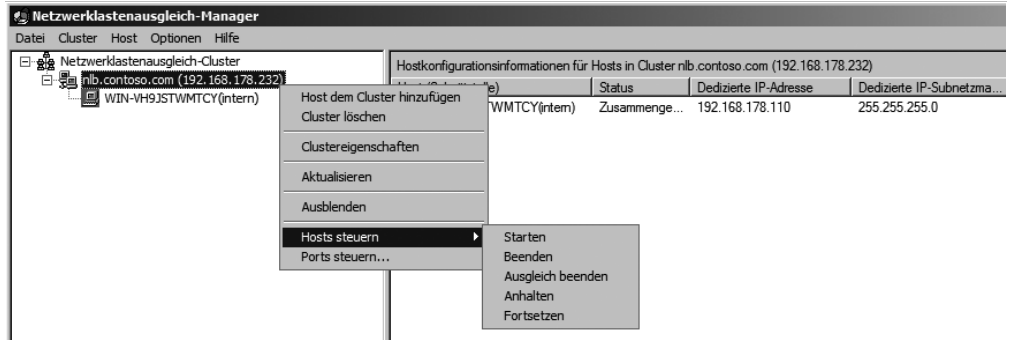
Anfragen jetzt von verschiedenen Servern innerhalb des Loadbalancing-Clusters an den Zielserver weitergeleitet werden und dieser annimmt, dass die Anfragen von verschiedenen Clients stammen – wodurch der Zielserver Zusammenhänge zwischen den Verbindungen nicht mehr erkennt und unter Umständen falsche Daten liefert. Nachdem die Regeln erstellt wurden, wird der Cluster erstellt und ist einsatzbereit.

Abbildg. 19.64 Anzeigen der Daten eines Clusters im Netzwerklastenausgleich-Manager



Die Einstellungen können jederzeit über das Kontextmenü des Clusters angepasst werden. Alle Server werden bei der Verteilung zunächst gleichwertig behandelt. Nach dem Start des Verwaltungsprogramms verbinden Sie sich über den Menübefehl *Cluster/Mit bestehendem Cluster verbinden* mit einem bereits konfigurierten Cluster. Über das Kontextmenü des Clusters und der einzelnen Hosts können Hosts hinzugefügt, gelöscht, angehalten oder konfiguriert werden. Dazu stehen verschiedene Funktionen zur Verfügung, die über Assistenten konfiguriert werden.

Abbildg. 19.65 Über das Kontextmenü wird der NLB-Cluster konfiguriert



TIPP Damit der Betrieb eines NLB-Clusters protokolliert wird, kann über den Menübefehl *Optionen/Protokolleinstellungen* die Protokollierung aktiviert und eine Datei festgelegt werden.

Zusammenfassung

Im Bereich der Clusterinstallation hat Microsoft einige Neuerungen integriert. Wie Sie am Beispiel der Testumgebung gelernt haben, kann ein Windows-Cluster auch ohne tiefgehende Kenntnisse problemlos installiert und betrieben werden. Im nächsten Kapitel zeigen wir Ihnen die Möglichkeiten der neuen Windows-PowerShell und geben Einblicke in die optimale Verwaltung eines Windows Server 2008-Netzwerkes über Skripts und leicht erlernbare Befehle.

Kapitel 20

Windows PowerShell

In diesem Kapitel:

Die Windows PowerShell ist die neue objektorientierte Befehlszeile für Windows Server 2008. Das heißt, Befehle führen nicht nur Aktionen im Betriebssystem aus, sondern können Objekte direkt ansprechen und bearbeiten. Alle Befehle aus der normalen Befehlszeile sind auch in der PowerShell verfügbar. Die Befehle werden dazu in PowerShell-Aliase übersetzt. Sie können die PowerShell auch für Windows Server 2003 Vista und XP herunterladen. Unter Windows Server 2008 haben Sie den Vorteil, dass die Shell bereits in das Betriebssystem integriert, aber noch nicht installiert ist. Die Befehlszeile von Windows Server 2008 unterscheidet sich nicht von ihrem Pendant in Windows Server 2003. Auch wenn Sie die Windows PowerShell als zusätzliche Funktion installieren, ändert sich die Befehlszeile nicht, sondern Sie müssen die PowerShell über die entsprechende Verknüpfung erst starten (Abbildung 20.1). Die meisten neuen Server-Produkte von Microsoft, zum Beispiel Exchange Server 2007, bauen auf die Windows PowerShell auf. Die grafischen Oberflächen dieser Produkte dienen dann nur noch dazu, Befehle zu generieren, so genannte Cmdlets, die durch die PowerShell ausgeführt werden. Exchange Server 2007 erweitert zum Beispiel die Windows PowerShell mit zusätzlichen Funktionen. Die neue Kommandozeile hat nichts mehr mit einer DOS-Box gemeinsam und ist extrem mächtig. Die PowerShell baut auf .NET Framework auf.

Abbildg. 20.1 Die neue Befehlszeile in Windows Server 2008

Am besten fügen Sie die Windows PowerShell als neue Feature über den Server-Manager hinzu. Standardmäßig wird die PowerShell nach der Installation von Windows Server 2008 nicht automatisch installiert. Exchange Server-Administratoren und auch Administratoren anderer Serversysteme können zukünftig alle Verwaltungsaufgaben, die auch in der grafischen Oberfläche durchgeführt werden können, in der PowerShell skriptgesteuert und automatisiert durchführen. Skriptbasierte Aktionen mussten zum Beispiel in Exchange Server 2003 noch durch komplizierte VB-Skripts durchgeführt werden, während in Exchange Server 2007 einfache PowerShell-Skripts verwendet werden können. Auch wenn Sie die Windows PowerShell als zusätzliche Funktion installieren, ändert sich die Befehlszeile nicht, sondern Sie müssen die PowerShell über die entsprechende Verknüpfung erst starten. Die herkömmliche Befehlszeile mit den bekannten Befehlen steht auch weiterhin zur Verfügung, das gilt natürlich auch für die Unterstützung von VB-Skripts. Die PowerShell ist eine Ergänzung, die parallel verwendet werden kann, das gilt für Windows Server 2003/2008 und Windows XP/Vista. Aufgaben, die Sie nicht über Gruppenrichtlinien oder sonstige Automatismen erledigen können, sind die perfekte Herausforderung für die PowerShell.

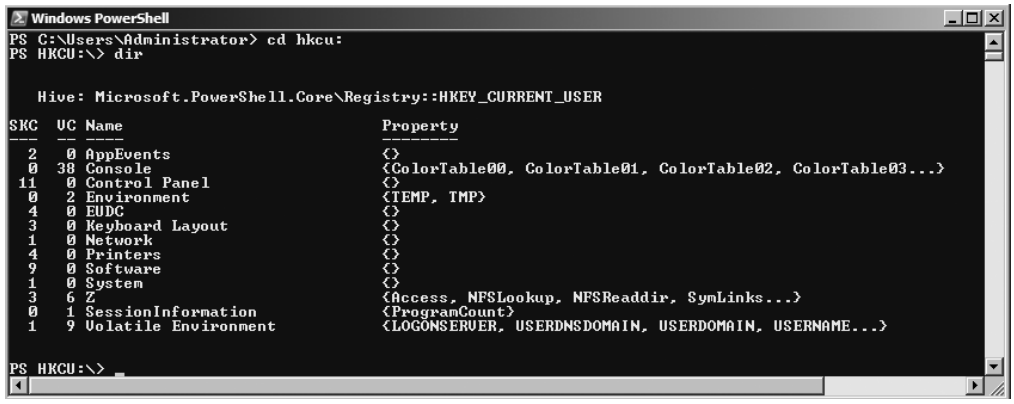
Die grundsätzliche Funktionsweise der PowerShell

Sie können Cmdlets an ihrem Aufbau erkennen: ein Verb und ein Substantiv, getrennt durch einen Bindestrich (–), beispielsweise *Get-Help*, *Get-Process* und *Start-Service*. Die meisten Cmdlets sind sehr einfach und für die Verwendung zusammen mit anderen Cmdlets vorgesehen. So werden mit *Get*-Cmdlets Daten abgerufen, mit *Set*-Cmdlets Daten erzeugt oder geändert, mit *Format*-Cmdlets Daten formatiert und mit *Out*-Cmdlets Ausgaben an ein angegebenes Ziel geleitet. Unter Windows Server 2008 können Cmdlets für die Automatisierung der neuen Serverrollen, zum Beispiel von IIS 7.0, der Active Directory-Domänendienste und der Terminaldienste verwendet werden. Für die Terminaldienste gibt es im Microsoft TechNet Script Center zum Beispiel zahlreiche Beispielskripts, welche die Verwaltung der Terminaldienste unter Windows Server 2008 enorm vereinfachen. Auch die Verwaltung der Registry, von Zertifikaten und der Ereignisanzeigen lassen sich über die PowerShell automatisieren. Windows PowerShell baut auf .NET Framework und der Common Language Runtime (CLR) von .NET auf und kann .NET-Objekte akzeptieren und zurückgeben. Diese grundlegende Änderung ermöglicht neue Tools und Skript-Verfahren für die Verwaltung und Konfiguration von Windows. Sie finden die Aktivierung der PowerShell im Server-Manager von Windows Server 2008 über *Features/Features hinzufügen*. Standardmäßig wird die PowerShell nach der Installation von Windows Server 2008 nicht automatisch installiert. Administratoren können zukünftig alle Verwaltungsaufgaben, die auch in der grafischen Oberfläche durchgeführt werden können, in der PowerShell skriptgesteuert und automatisiert durchführen. Skriptbasierte Aktionen mussten zum Beispiel in Exchange Server 2003 noch durch komplizierte VB-Skripts durchgeführt werden, während in Exchange Server 2007 einfache, aber sehr mächtige PowerShell-Skripts verwendet werden können. Nach der Installation wird die PowerShell über eine eigene Verknüpfung im Startmenü gestartet.

Die PowerShell-Laufwerke verwenden

Neben den bekannten Dateisystemlaufwerken wie *C:* und *D:* enthält Windows PowerShell auch Laufwerke, die die Registrierungsstrukturen *HKEY_LOCAL_MACHINE (HKLM:)* und *HKEY_CURRENT_USER (HKCU:)*, den Speicher für digitale Signaturzertifikate auf Ihrem Computer (*Cert:*) und die Funktionen in der aktuellen Sitzung (*Function:*) darstellen. Diese werden als *Windows PowerShell-Laufwerke* bezeichnet. Eine Liste kann mit dem Befehl *Get-PSDrive* angezeigt werden. In der PowerShell wird mit .NET-Objekten gearbeitet. Technisch gesehen ist ein .NET-Objekt eine Instanz einer .NET-Klasse, die aus Daten und zugeordneten Operationen besteht. Sie können sich ein Objekt als Dateneinheit mit Eigenschaften und Methoden vorstellen. Methoden sind Aktionen, die für das Objekt ausgeführt werden können. Wenn beispielsweise ein Dienst aufgerufen werden soll, wird eigentlich ein Objekt, das diesen Dienst darstellt, verwendet. Wenn Informationen über einen Dienst angezeigt werden, werden die Eigenschaften des zugehörigen Dienstobjekts angezeigt. Und wenn ein Dienst gestartet wird, verwendet die PowerShell eine Methode des Dienstobjekts. Um zum Beispiel in die lokale Registry in *HKEY_CURRENT_USER* zu wechseln, geben Sie in der PowerShell *CD hkcu:* ein. Den Inhalt des Registry-Hives können Sie sich mit *Dir* anzeigen lassen (Abbildung 20.2).

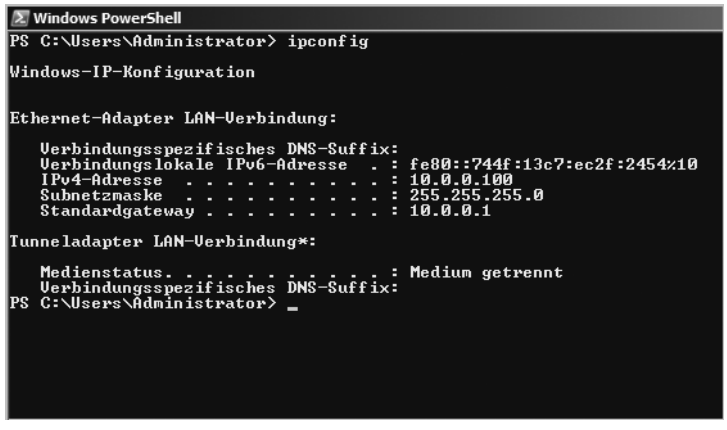
Abbildg. 20.2 Bearbeiten und Anzeigen der Registry in der PowerShell



CMD-Befehle in der PowerShell verwenden

Ein weiterer Vorteil der PowerShell liegt darin, dass die vertrauten Tools der normalen Befehlszeile nicht aufgegeben werden müssen, diese werden weiterhin unterstützt. Dazu gibt es für jeden CMD-Befehl einen PowerShell-Alias. Die Verwendung dieser Befehle ist analog zur bisherigen Eingabeaufforderung, die natürlich noch immer parallel zur Verfügung steht.

Abbildg. 20.3 Herkömmliche CMD-Befehle können wie gewohnt auch in der PowerShell eingesetzt werden



Die meisten Befehle werden als Alias in der PowerShell zur Verfügung gestellt. Über den Befehl *Alias* werden alle Aliase in der Befehlszeile angezeigt. Über den Befehl *Alias <Buchstabe>** können Sie sich die einzelnen Aliase, die mit dem angegebenen Buchstaben beginnen, anzeigen lassen. Die Aliase müssen aber für die Arbeit mit den alten Befehlen nicht bekannt sein.

Skripts mit der PowerShell erstellen

Wenn Sie immer wieder bestimmte Befehlsfolgen ausführen oder ein PowerShell-Skript für eine komplexe Aufgabe entwickeln, empfiehlt es sich, die Befehle nicht einzeln einzugeben, sondern in einer Datei zu speichern. Die Dateierweiterung für Windows PowerShell-Skripts lautet **.ps1* (das dritte Zeichen der Dateierweiterung ist die Zahl 1). Es muss immer ein vollqualifizierter Pfad zu der Skriptdatei angegeben werden, auch wenn sich das Skript im aktuellen Verzeichnis befindet. Wenn auf das aktuelle Verzeichnis verwiesen werden soll, geben Sie einen Punkt ein, zum Beispiel *.script.ps1*. Zum Schutz des Systems enthält die PowerShell verschiedene Sicherheitsfeatures, zu denen auch die Ausführungsrichtlinie zählt. Die Ausführungsrichtlinie bestimmt, ob Skripts ausgeführt werden dürfen und ob diese digital signiert sein müssen. Standardmäßig werden Skripts blockiert. Sie können die Ausführungsrichtlinie mit dem Cmdlet *Set-ExecutionPolicy* ändern. Die Ausführungsrichtlinie wird in der Windows-Registrierung gespeichert.

Mit dem Cmdlet *Start-Sleep* werden Windows PowerShell-Aktivitäten für einen bestimmten Zeitraum gestoppt. Mit dem Befehl *Start-Sleep –s 10* hält das Skript zehn Sekunden an. *Start-Sleep –m 10000* verwendet Millisekunden.

Wird die Ausgabe von Cmdlets mit der Option | *Out-Printer* an das Cmdlet *Out-Printer* übergeben, wird die Ausgabe auf dem Standarddrucker ausgedruckt. Der Drucker kann mit Anführungszeichen und der Bezeichnung in der Druckersteuerung auch angegeben werden.

Mit dem Cmdlet *Write-Warning* können eigene Warnungen in der PowerShell angezeigt werden. *Write-Host* schreibt Nachrichten. Beide sind farblich unterschiedlich formatiert. Farbzuweisungen können nur für *Write-Host* gesetzt werden. Die Farben werden mit *–foregroundcolor* und *–backgroundcolor* manuell konfiguriert. Folgende Werte sind möglich:

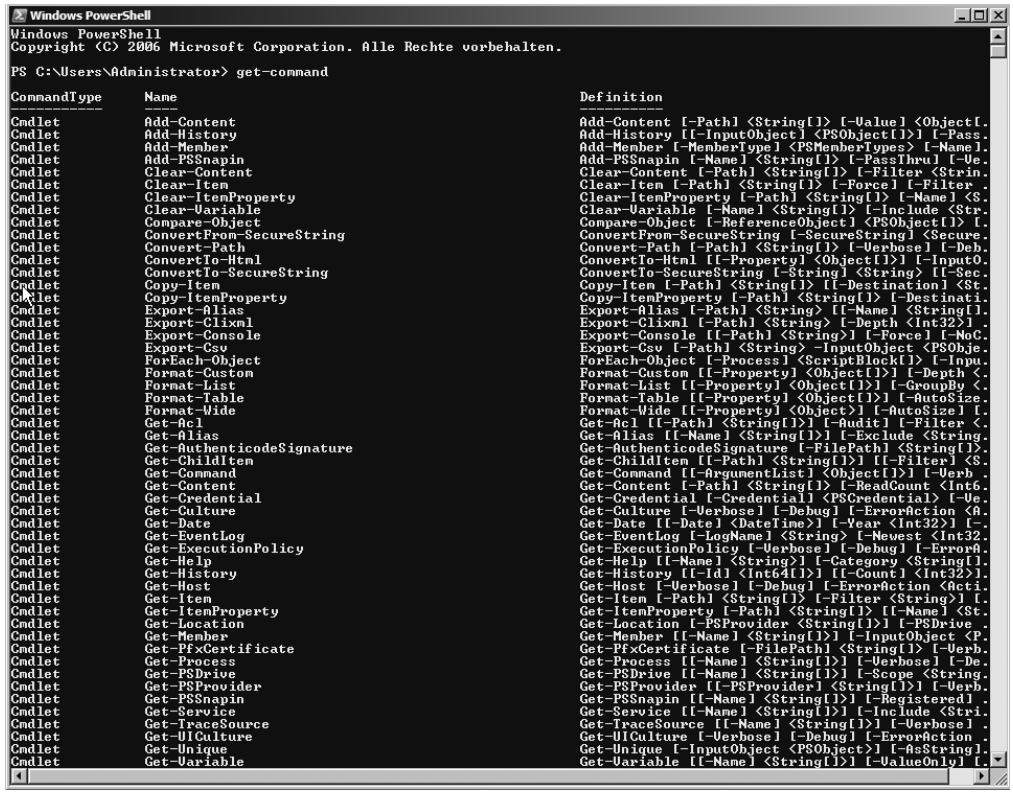
- Black (Schwarz)
- DarkBlue (Dunkelblau)
- DarkGreen (Dunkelgrün)
- DarkCyan (Dunkelzyan)
- DarkRed (Dunkelrot)
- DarkMagenta (Dunkelmagenta)
- DarkYellow (Dunkelgelb)
- Gray (Grau)
- DarkGray (Dunkelgrau)
- Blue (Blau)
- Green (Grün)
- Cyan (Zyan)
- Red (Rot)
- Magenta (Magentarot)
- Yellow (Gelb)
- White (Weiß)

Mit dem Cmdlet *Invoke-Expression*, wird in der Windows PowerShell ein Skript gestartet: *Invoke-Expression c:\scripts\test.ps1*.

Windows PowerShell zur Administration verwenden

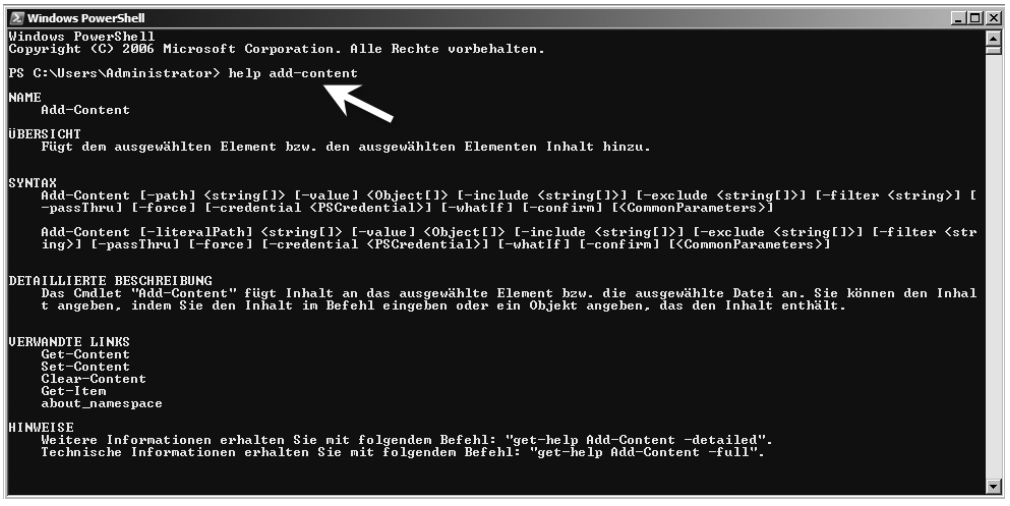
Geben Sie in der Windows PowerShell den Befehl *Get-Command* ein, um sich eine Befehlszeilen-Referenz anzeigen zu lassen. Über *Get-Command >c:\befehle.txt* werden alle Befehle in die Datei *C:\befehle.txt* umgelenkt, Sie erhalten wie immer bei der Dateiumleitung keine Bestätigung der Ausführung. Innerhalb der PowerShell funktionieren auch die herkömmlichen Befehle aus der Befehlszeile.

Abbildg. 20.4 Anzeige aller in der Windows PowerShell verfügbaren Befehle



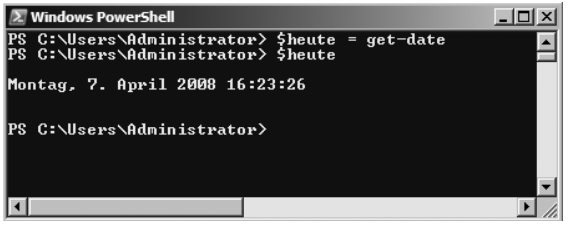
Über den Befehl *Help <Befehlname>* können Sie sich zu einzelnen Befehlen eine ausführliche Hilfe anzeigen lassen. Wenn Sie eine detaillierte Hilfe zu einem Cmdlet einschließlich Parameterbeschreibungen und Beispielen anzeigen möchten, verwenden Sie *Get-Help* mit dem *detailed*-Parameter zum Beispiel *Get-Help Get-Command –detailed*. Über die Tastenkombination Strg+C können Sie innerhalb der Shell einzelne Aktionen stoppen.

Abbildg. 20.5 Anzeige der Hilfe eines einzelnen Befehls mit *help*



Interessant ist auch die Möglichkeit, dass Sie innerhalb der Shell auch Variablen definieren können, welche aktuelle Informationen automatisch abfragen. Diese Variablen können Sie dann später innerhalb eines Skripts verwenden. Wollen Sie zum Beispiel das aktuelle Datum als Variable *$heute* hinterlegen, können Sie in der Shell den Befehl *$heute = Get-Date* eingeben. Anschließend wird das heutige Datum als Variable *$heute* hinterlegt. Geben Sie als Nächstes in der Shell *$heute* ein, wird das aktuelle Datum ausgegeben (Abbildung 20.6).

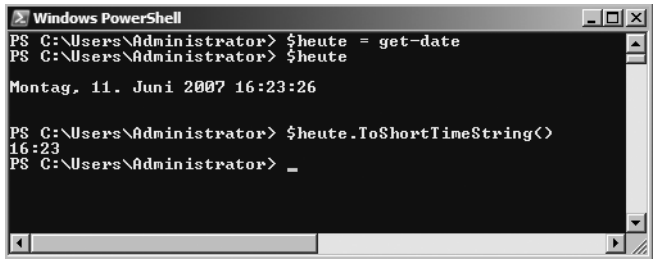
Abbildg. 20.6 Verwenden von Variablen in der PowerShell



Sie können auch auf einzelne Bestandteile der Variable getrennt zugreifen. Interessiert Sie zum Beispiel aus dem Datum lediglich die Zeit, können Sie zum Beispiel einzelne Elemente objektorientiert aus der Variable auslesen. So können Sie zum Beispiel durch Eingabe des Befehls *$heute.ToShortTimeString()* ohne viel Aufwand nur die Uhrzeit in Stunden und Minuten aus der Variable auslesen. Weitere Möglichkeiten sind die Formatierung der Ausgabe. So ist es zum Beispiel auch möglich, per Eingabe des Befehls *$heute.ToString("MMMM")* die Ausgabe des Monats zu erzwingen, oder über *$heute.ToString("MM")* den Monat als Zahl innerhalb des Kalenderjahres. Generell können Sie hinter den meisten Befehlen, die einen Status oder eine Statistik ausgeben, noch den Zusatz *|fl* eingeben. Dieser Zusatz bewirkt, dass Sie eine formatierte Liste (daher *fl*) erhalten, welche deutlich mehr Informationen ausgibt, als der Befehl ohne diesen Zusatz.

Der Befehl *Get-Date –displayhint date* zeigt nur das Datum, *Get-Date –displayhint time* nur die Uhrzeit an.

Abbildg. 20.7 Aufrufen von verschiedenen Werten aus gesetzten Variablen

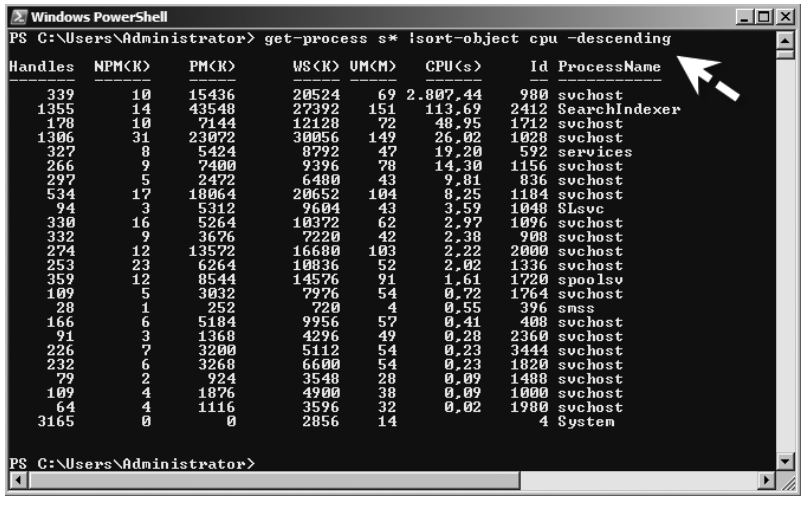


Sie können ermitteln, welche Art von Objekt von einem bestimmten Cmdlet abgerufen wird, indem die Ergebnisse des Befehls *Get* mit einem Pipelineoperator (|) an den Befehl *Get-Member* übergeben werden. So werden mit dem Befehl *Get-Service | Get-Member* abgerufenen Objekte an *Get-Member* gesendet. Mit diesem Befehl können Informationen über das .NET-Objekt angezeigt werden, das von einem Befehl zurückgegeben wird. Zu den Informationen zählen der Typ, die Eigenschaften und die Methoden des Objekts. Wenn beispielsweise alle Eigenschaften eines Dienstobjekts angezeigt werden sollen, geben Sie *Get-Service | Get-Member –membertype *property* ein.

Anzeigen und Verwalten von Prozessen mit der PowerShell

Eine häufige Administrationsaufgabe ist die Verwaltung der laufenden Prozesse auf einem Server. Über den Befehl *Get-Process* können alle laufenden Prozesse eines Servers angezeigt werden. Sollen zum Beispiel nur alle Prozesse mit dem Anfangsbuchstaben »S« angezeigt werden, geben Sie den Befehl *Get-Process s** ein. Sollen die Prozesse zusätzlich noch, zum Beispiel absteigend nach der CPU-Zeit sortiert werden, geben Sie *Get-Process s** gefolgt von der Pipe-Option *|Sort-Object cpu –descending* ein (Abbildung 20.8).

Abbildg. 20.8 Prozesse absteigend nach CPU-Verbrauch sortieren



Praxisbeispiele für die wichtigsten Cmdlets

In diesem Abschnitt zeigen wir Ihnen einige Cmdlets, die in der Praxis sehr nützlich sind und die Möglichkeiten der PowerShell im Vergleich zu herkömmlichen Befehlszeilen verdeutlichen.

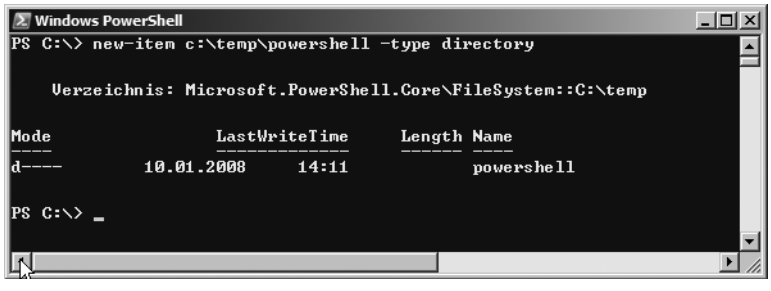
Befehle für die Datei- und Ordnerverwaltung

Mit dem Cmdlet *Copy-Item* werden Dateien oder Verzeichnisse in der PowerShell kopiert. Mit dem Befehl *Copy-Item C:\Scripts\test.txt C:\Test* wird die Datei *test.txt* kopiert. Die Syntax ist ähnlich zum Copy-Befehl der herkömmlichen Befehlszeile. Der Befehl *Copy-Item C:\Scripts* C:\Test* kopiert alle Dateien im entsprechenden Quellverzeichnis in das Zielverzeichnis. Der Befehl *Copy-Item C:\Scripts C:\Test –recurse* legt eine Kopie des Ordners *C:\Scripts* im Ordner *C:\Tests* an. Ohne die Option *–recurse* wird in *C:\Test* ein Ordner *Scripts* angelegt, aber keine Dateien und Ordner kopiert. Neben dem vollständigen Befehl kann auch mit den Abkürzungen *cpi, cp* oder *copy* gearbeitet werden.

Das Cmdlet *Move-Item* verschiebt Objekte: *Move-Item C:\Scripts\test.zip c:\test*. Auch hier kann wieder mit Platzhaltern gearbeitet werden, genauso wie beim Kopieren. Standardmäßig überschreibt *Move-Item* vorhandene Dateien im Zielordner nicht. Mit dem Parameter *–force* werden vorhandene Zieldateien oder Ordner überschrieben: *Move-Item C:\Scripts\test.zip C:\Test –force*. Mit dem Befehl *Move-Item C:\Scripts\test.log C:\Test\ad.log* werden Dateien verschoben und gleich umbenannt. Neben *Move-Item* kann auch *mi*, *mv* oder *move* verwendet werden.

Mit dem Cmdlet *New-Item* werden neue Dateien oder Ordner erstellt. Mit dem Befehl *New-Item C:\Temp\PowerShell –type directory* wird im Verzeichnis *C:\Temp* ein neues, leeres Verzeichnis *PowerShell* erstellt (Abbildung 20.9).

Abbildg. 20.9 Erstellen von neuen Verzeichnissen in der PowerShell



Um eine neue Datei zu erstellen, wird die gleiche Syntax, aber der Typ *file* verwendet: *New-Item C:\Scripts\skript.txt –type file*. Mit dem Befehl *New-Item C:\Scripts\skript.txt –type file –force* wird die vorhandene Datei durch eine neue leere Datei ersetzt. Mit dem Befehl *New-Item C:\Scripts\skript.txt –type file –force –value "Text"* wird eine neue Datei erstellt und der hinterlegte Text in die Datei geschrieben. Statt *New-Item* kann auch *ni* verwendet werden. Mit dem Cmdlet *Add-Content* können Daten an eine Textdatei angefügt werden: *Add-Content C:\Scripts\test.txt "Text"*. Standardmäßig fügt *Add-Content* den neuen Wert hinter dem letzten Zeichen in der Textdatei ein. Der Inhalt einer Datei wird mit *Set-Content* ersetzt.

Clear-Content löscht den Inhalt einer Datei. Nach der Ausführung existiert die Datei weiterhin, hat aber keinen Inhalt mehr. Auch hier kann mit Platzzeichen gearbeitet werden: *Clear-Content C:\Test\e**. Neben Textdateien unterstützt das Cmdlet auch Excel-Tabellen, Word-Dokumente und andere Dateien. Statt *Clear-Content* kann auch *clc* verwendet werden.

Das Cmdlet *Remove-Item* löscht Objekte: *Remove-Item C:\Scripts\test.txt.* Mit dem Platzhalterzeichen * werden Objekte in einem angegebenen Ordner gelöscht: *Remove-Item C:\Scripts**. Mit dem Befehl *Remove-Item C:\Scripts* –recurse* muss das Löschen nicht bestätigt werden. Der Befehl *Remove-Item C:\Scripts* –exclude *.doc* löscht alle Dateien, außer denen, die mit *–exclude* ausgeschlossen werden. Über den Befehl *Remove-Item C:\Scripts* –include .xls,.doc* werden alle Dateien behalten, nur die hinter *–include* werden gelöscht. Beide Optionen können auch gemeinsam verwendet werden, zum Beispiel: *Remove-Item C:\Scripts* –include *.txt –exclude *test*.* Hier werden alle Textdateien im Ordner gelöscht, außer Dateien mit der Zeichenfolge »test« im Dateinamen. Der Parameter *–whatif* entfernt nichts, gibt aber aus, was passieren würde: *Remove-Item C:\windows*.exe –whatif* (Abbildung 20.10).

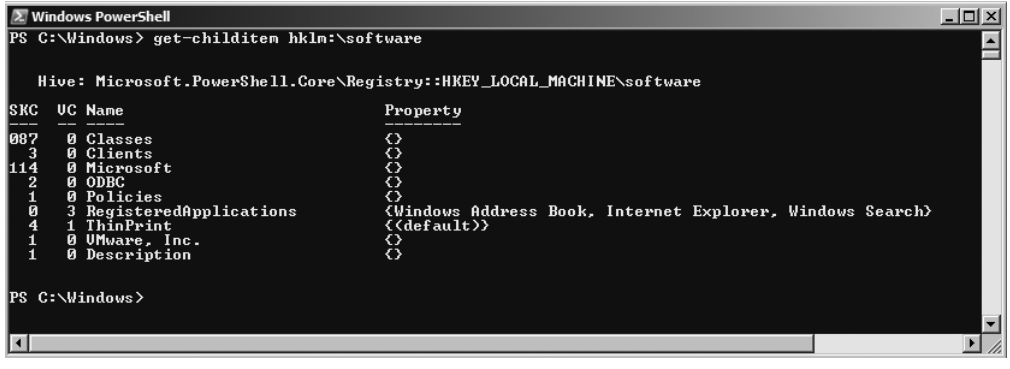
Abbildg. 20.10 Das Löschen von Dateien kann mit *–whatif* auch simuliert werden

Statt *Remove-Item* kann auch *ri, rd, erase, rm, rmdir* oder *del* verwendet werden.

Vorhandene Objekte werden mit dem Cmdlet *Rename-Item* umbenannt: *Rename-Item C:\Scripts\test.txt neu.txt*. Die Befehle *rni* und *ren* führen ebenfalls zum Ziel.

Das Cmdlet *Get-ChildItem* hat eine ähnliche Funktionalität wie der Befehl *Dir*. Mit *Get-ChildItem –recurse* wird auch der Inhalt der Unterordner angegeben, ähnlich zu *Dir /s*, nur übersichtlicher. *Get-ChildItem HKLM:\SOFTWARE* zeigt den Inhalt von Registryschlüsseln an (Abbildung 20.11).

Abbildg. 20.11 Auflisten von Registryinhalten in der PowerShell

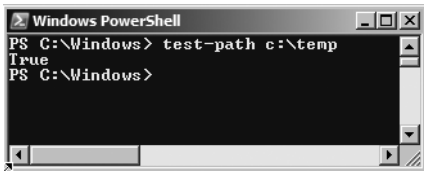


Durch die PowerShell-Laufwerke können alle Registryschlüssel auf diese Weise ausgelesen werden. Auch hier kann mit den beiden Optionen *–include* und *–exclude* gearbeitet werden: *Get-ChildItem C:\Windows*.* –include *.exe,*.pif*. Die Funktionsweise ist ähnlich zu *Copy-Item*, beziehungsweise

Remove-Item. Die zurückgegebenen Informationen können auch an das Cmdlet *Sort-Object* weitergegeben werden, um eine Sortierung durchzuführen: *Get-ChildItem C:\Windows*.* | Sort-Object length*. Mit *Get-ChildItem C:\Windows*.* | Sort-Object length –descending* wird mit den größten Dateien begonnen. Für den Befehl können auch die Aliase *gci, ls* und *dir* verwendet werden.

Das Cmdlet *Test-Path* überprüft das Vorhandensein einer Datei oder eines Ordners: *Test-Path C:\Temp*. *Test-Path* gibt *True* zurück, wenn die Datei vorhanden ist, und *False*, wenn die Datei nicht vorhanden ist. Auch hier kann mit Platzhaltern gearbeitet werden.

Abbildg. 20.12 Überprüfen, ob ein Verzeichnis vorhanden ist



Die Anweisung *Test-Path HKCU:\Software\Microsoft\Windows* testet, ob ein bestimmter Registryschlüssel vorhanden ist.

Programme starten und manipulieren

Mit dem Cmdlet *Invoke-Item* kann über die Windows PowerShell eine ausführbare Datei gestartet oder eine Datei geöffnet werden: *Invoke-Item C:\Windows\System32\Calc.exe*. Statt *Invoke-Item* kann auch *ii* verwendet werden.

Abbildg. 20.13 Starten von ausführbaren Dateien in der PowerShell

Die Communitiy – Tools für die PowerShell

Bereits vor der Veröffentlichung von Windows Server 2008 wird die PowerShell von vielen Administratoren bereits produktiv eingesetzt. Im Internet gibt es zahlreiche Communities und Zusatzprodukte, welche den Nutzen der PowerShell weiter verbessern. So können Sie zum Beispiel *PowerGadgets* einsetzen, um über diese neue Shell Gadgets für die Sidebar von Windows Vista und Windows

Server 2008 zu erstellen. Sie finden den Link im folgenden Tipp. Ebenfalls im Internet erhältlich sind Cmdlets für die PowerShell, die spezielle Aufgaben im Netzwerk durchführen, auf Active Directory zugreifen oder auch Dateien übertragen können. Auch hier haben wir für Sie Beispiele aufgeführt. Selbst eine grafische Oberfläche wird mittlerweile angeboten, die Administratoren bei der Erstellung von Cmdlets unterstützt. Die *PowerGUI* kennt nicht nur die Cmdlets der herkömmlichen PowerShell, sondern auch die Erweiterungen für Exchange Server 2007 und Microsoft Operation Manager 2007. Mit der PowerGUI können Sie Cmdlets direkt in der grafischen Oberfläche durch bequeme Menüs ausführen.

TIPP **Wichtige Internetseiten für den Umgang mit der Windows PowerShell:**

http://www.powergadgets.com

http://www.it-visions.de/scripting/powershell

http://www.nsoftware.com/powershell/

http://www.quest.com/activeroles-server/arms.aspx

http://powergui.org

http://www.microsoft.com/technet/scriptcenter/scripts/msh/ts

http://blogs.msdn.com/PowerShell/

http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.mspx

http://www.scriptinternals.de/

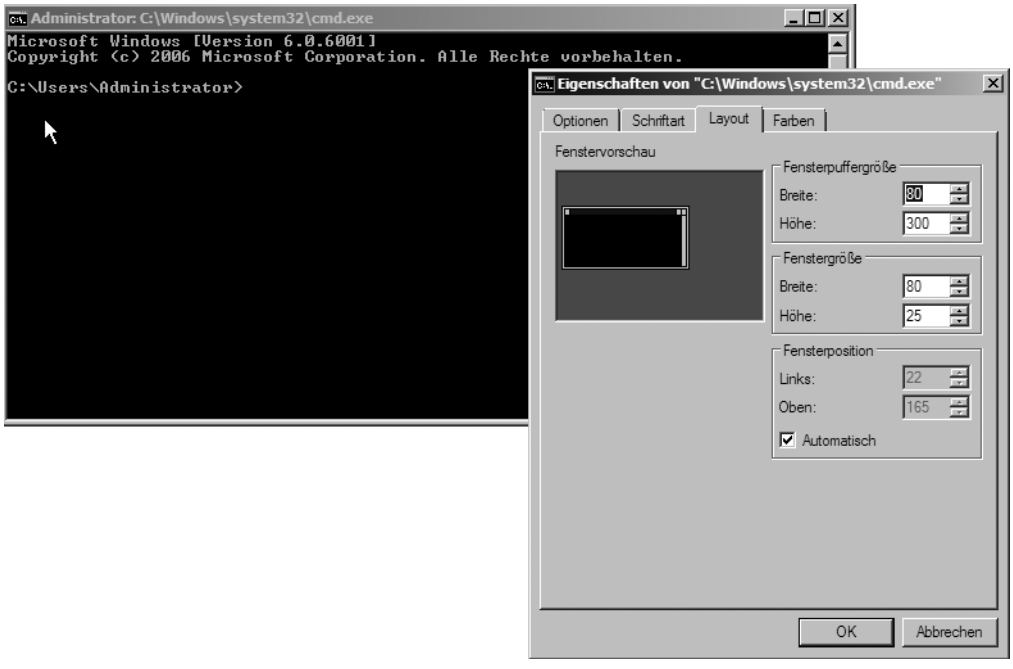
Normale Befehlszeile verwenden

Neben der neuen PowerShell besteht auch weiterhin die Möglichkeit, auf die normale Befehlszeile zu setzen. Im folgenden Abschnitt zeigen wir Ihnen ein paar Tipps und Tricks zur Arbeit mit der Befehlszeile. In diversen Kapiteln dieses Buches wurde bereits auf einzelne Befehle eingegangen, die ohne grafische Oberfläche in der Befehlszeile eingegeben werden können. Eine Befehlszeile öffnen Sie am besten über *Start/Ausführen/cmd*. Wenn Sie häufiger eine Befehlszeile benötigen, können Sie zur Datei *cmd.exe* auch eine Verknüpfung auf dem Desktop erstellen. Anders als bei Windows-Programmen steht der Anwender beim ersten Öffnen der Eingabeaufforderung zunächst einmal recht ratlos da: Es gibt keine Menüs, Schaltflächen oder sonstige Hinweise darauf, was man denn nun eigentlich anfangen kann. Nicht mal ein Druck auf die F1-Taste bringt nützliche Informationen auf den Bildschirm. Mit der Befehlszeile zu arbeiten, heißt tippen: Man erteilt dem System Befehle, indem man ihren Namen per Tastatur eingibt und die Zeile mit einem Druck auf die Eingabe-Taste abschließt. Der Rechner führt daraufhin die gewünschten Aktionen aus, schreibt die angeforderten Informationen – oder auch eine Fehlermeldung – in dasselbe Fenster und steht anschließend für weitere Eingaben zur Verfügung.

Nicht nur der eigentliche Umgang mit der Befehlszeile, auch die Auswahl an zur Verfügung stehenden Befehlen hat sich im Laufe der Zeit stark verbessert. Viele von ihnen erschließen – wie *Ping* – Funktionen, die man in der grafischen Oberfläche vergeblich sucht. Um eine weitere beliebte Startmöglichkeit der Befehlszeile schätzen zu lernen, muss man wissen, dass beim Arbeiten mit ihr immer genau ein Verzeichnis eines Laufwerks das so genannte aktuelle Verzeichnis ist. Nur Dateien in diesem Ordner lassen sich ansprechen, ohne ihnen einen Pfad voranstellen zu müssen. Zum Wechseln des aktuellen Verzeichnisses dient der Befehl *ChDir* oder kurz *CD*, der als Argument – wie

bei allen Befehlen üblich durch ein Leerzeichen abgetrennt – den Namen des Ordners benötigt, in den man wechseln will. Einmal gestartet, präsentiert sich die Eingabeaufforderung als recht schmuckloses schwarzes Fenster mit ein paar Zeilen hellgrauem Text. Wem die Darstellung nicht gefällt, findet im Systemmenü dieses Fensters den Befehl *Eigenschaften*, mit dessen Hilfe sich beispielsweise die Schriftart und -größe, die Vorder- und Hintergrundfarbe und manches andere anpassen lassen. Empfehlenswert ist auf der Registerkarte *Layout* die voreingestellte Fensterhöhe auf 50 Zeilen zu verdoppeln und die Fensterpuffergröße etwas großzügiger zu bemessen, etwa auf 300 bis 500 Zeilen. Die erste Zahl gibt an, wie viele Zeilen Text das Fenster vollständig anzeigt, die zweite definiert die Größe des Speichers, aus dem die Bildlaufleiste am rechten Rand Text zurückholen kann, der nach oben aus dem Fenster gerutscht ist. Die Breite sollte besser auf 80 Zeichen eingestellt bleiben, da manche Programme sonst nur noch wirren Zeichensalat ausgeben.

Abbildg. 20.14 Konfigurieren der Befehlszeile unter Windows Server 2008



Interessant sind noch einige Einstellungen auf der Registerkarte *Optionen*. Hier spart ein Häkchen bei *QuickEdit-Modus* ein paar Mausklicks beim Kopieren von Text aus der Eingabeaufforderung in andere Anwendungen. Um den Text zu markieren, muss man ihn nur bei gedrückter Maustaste einrahmen und dann die ↵-Taste drücken; ohne QuickEdit leitet der Befehl *Markieren* aus dem Systemmenü das Kopieren ein. Die restlichen Optionen sind mit sinnvollen Einstellungen vorbelegt; in Einzelfällen verdienen lediglich noch die Parameter im Bereich *Befehlsspeicher* Beachtung. Die Steuertasten, um die Eingabemarke um ein Zeichen oder ein Wort nach rechts oder links sowie an den Anfang oder das Ende der Zeile zu bewegen, funktionieren wie gewohnt. Dagegen dienen die Tasten Pfeil ↑, Pfeil ↓, Bild ↑ und Bild ↓ dazu, durch die Historie der vorher eingegebenen Kommandos zu blättern; die letzten beiden springen an den Anfang beziehungsweise ans Ende dieser Liste. Auch wenn ein eingetippter langer Befehl auf die nächste Bildschirmzeile umbricht, verwaltet ihn der Editor wie eine einzige Zeile. Ein Druck auf Esc löscht die Eingabezeile.

Weitere Editiermöglichkeiten stellen die Funktionstasten F1 bis F5 zur Verfügung. Beim Arbeiten mit der Eingabeaufforderung ist es recht häufig notwendig, Verzeichnis- oder Dateinamen einzugeben. Dabei kann man durch zwei verschiedene Kniffe einiges an Tipparbeit sparen. Der erste bedeutet einen Rückgriff auf die Maus und die grafische Windows-Oberfläche: Wenn Sie per Drag & Drop eine Datei oder einen Ordner aus dem Explorer auf ein Eingabeaufforderungsfenster ziehen, wird deren kompletter Name inklusive Pfad an der aktuellen Cursorposition in die gerade bearbeitete Befehlszeile eingefügt. Bei einem Druck auf die ⇥-Taste versucht der Eingabeeditor das, was vor dem Cursor steht, zu einem existierenden Datei- oder Verzeichnisnamen zu ergänzen. Eine Liste der grundlegenden Befehle gibt das System aus, wenn man den Befehl *Help* eingibt. Die meisten der angezeigten Kommandos benötigen noch weitere Parameter, etwa einen oder mehrere Datei- oder Ordnernamen oder auch so genannte Optionen, die das Verhalten des Befehls im Detail ändern. Letztere bestehen in der Regel aus einem Buchstaben mit einem vorangestellten Schrägstrich (/). Grundsätzlich muss zwischen dem eigentlichen Befehl und seinen Argumenten sowie zwischen einzelnen Parametern jeweils ein Leerzeichen stehen. Welche Argumente ein bestimmter Befehl benötigt, offenbart sich durch die Eingabe von *Help <Befehl>* oder auch *<Befehl> /?*. Die wichtigsten Befehle sind nachfolgend aufgelistet:

- **APPEND** Suche nach Dateien im Unterverzeichnis
- **ASSIGN** Verweist dem Laufwerk einen anderen Buchstaben
- **ATTRIB** Anzeige/Ändern von Dateiattributen
- **C:** Wechselt zum Laufwerk C:
- **CALL** Aufrufen einer Batchdatei aus einer anderen heraus mit Rücksprung
- **CD** Der Befehl *CD* zeigt Ihnen den Namen des aktuellen Verzeichnisses an oder wechselt den aktuellen Ordner. Wird *CD* nur mit einem Laufwerkbuchstaben (z.B. *ChDir C:*) verwendet, zeigt es diesen Laufwerkbuchstaben und den Namen des Ordners an, der auf dem Laufwerk der aktuelle Ordner ist. Ohne Parameter zeigt *CD* das aktuelle Laufwerk und den aktuellen Ordner an.
- **CHKDSK** Datenträger überprüfen
- **CHOICE** Erlaubt verschiedene Auswahlmöglichkeiten innerhalb von Batchdateien
- **CLS** Bildschirm löschen
- **COMP** Dateien miteinander vergleichen
- **COPY** Dateien kopieren
- **DATE** Aktuelles Datum anzeigen/ändern
- **DEL** Löscht eine oder mehrere Dateien
- **DELTREE** Löscht komplette Verzeichnisbäume
- **DIR** Inhaltsverzeichnisse anzeigen. Zeigt eine Liste der in einem Verzeichnis enthaltenen Dateien und Unterverzeichnisse an. Wenn Sie *Dir* ohne Parameter verwenden, wird die Datenträgervolumebezeichnung und Seriennummer des Datenträgers, gefolgt von einer Liste der Verzeichnisse und Dateien auf dem Datenträger, einschließlich der entsprechenden Namen und des Datums und der Uhrzeit der letzten vorgenommenen Änderung angezeigt. Bei Dateien zeigt *Dir* die Namenerweiterung und die Größe in Bytes an. *Dir* zeigt auch die Gesamtzahl der aufgelisteten Dateien und Verzeichnisse an, ihre Gesamtgröße und den Umfang des auf dem Datenträger noch verfügbaren Speicherplatzes (in Byte).

- **ECHO** Anzeigen von Meldungen auf dem Bildschirm aus einer Batchdatei heraus; Befehlsanzeige ein- bzw. ausschalten
- **EXIT** Mit *Exit* beenden Sie aktuelle Batchskript (mit den Parameter */b*) oder das Programm *cmd.exe* und kehren zu dem Programm, das *cmd.exe* gestartet hat, oder zum Programm-Manager zurück
- **EXPAND** Expandiert eine oder mehrere komprimierte Dateien
- **FC** Dateien vergleichen
- **FIND** Textstellen in Dateien suchen
- **FOR** Batchbefehle zur mehrfachen Wiederholung eines DOS-Befehls
- **FORMAT** Festplatten vorbereiten (formatieren)
- **FTP** Öffnet die FTP-Verbindung
- **GOTO** Sprungbefehl in Batchdatei
- **IF** Setzen von Bedingungen in Batchdateien
- **LABEL** Zuweisen, Ändern oder Löschen eines Datenträgernamens
- **MD** Unterverzeichnis erstellen
- **MENUCOLOR** Legt die Farben für das Multikonfigurationsmenü fest
- **MOVE** Verschiebt Dateien, benennt Verzeichnisse um
- **PATH** Suchpfad für ausführbare MS-DOS-Befehlsdateien festlegen oder anzeigen
- **PAUSE** Stoppt innerhalb von Batchdateien und wartet auf einen Tastendruck
- **PING** Testet eine Netzwerkverbindung
- **PRINT** Druckt Textdateien im Hintergrund aus
- **RD** Unterinhaltsverzeichnis löschen
- **REM** Kommentare in Batchdateien
- **REN** Dateien umbenennen
- **SUBST** Ersetzt einen Verzeichnisnamen durch einen Laufwerksbezeichner
- **TELNET** Öffnet das Telnet-Fenster, dazu muss aber die Funktion *Telnet-Client* installiert sein
- **TIME** Systemzeit anzeigen und ändern
- **TREE** Verzeichnisstruktur eines Datenträgers grafisch anzeigen
- **TYPE** Inhalt einer Datei auf dem Bildschirm anzeigen
- **VOL** Namen und Seriennummer eines Datenträgers
- **XCOPY** Erweitertes Kopierprogramm mit zusätzlichen Möglichkeiten zur Übertragung von Dateien und kompletten Verzeichnisbäumen

Mit *Xcopy* lassen sich Dateien und Verzeichnisse einschließlich der Unterverzeichnisse kopieren. Die Syntax dazu lautet:

Xcopy Quelle [Ziel] [/c] [/v] [/l] [/d[:TT.MM.JJ]] [/u] [/s [/e]] [/t] [/k] [/r] [/h] [{/y|/–y}] [/z]

Dabei können Sie folgende Optionen verwenden:

- **/c** Unterdrückt Fehlermeldungen
- **/v** Bewirkt, dass jede Zieldatei nach dem Schreiben überprüft wird, um sicherzustellen, dass die Zieldateien mit den Quelldateien übereinstimmen
- **/l** Zeigt eine Liste der zu kopierenden Dateien an
- **/d**[**:TT.MM.JJ**] Kopiert nur Quelldateien, die an oder nach dem angegebenen Datum geändert wurden. Wenn Sie keinen Wert für TT.MM.JJ angeben, kopiert *Xcopy* alle Dateien aus *Quelle*, die neuer sind als vorhandene Dateien aus *Ziel*. Mit dieser Befehlszeilenoption können Sie veränderte Dateien aktualisieren.
- **/u** Kopiert nur die Dateien aus der Quelle, die bereits im Ziel existieren
- **/s** Kopiert Verzeichnisse und Unterverzeichnisse, wenn diese nicht leer sind. Wenn Sie */s* weglassen, arbeitet *Xcopy* nur innerhalb eines Verzeichnisses.
- **/e** Kopiert alle Unterverzeichnisse, auch wenn diese leer sind
- **/t** Kopiert nur die Unterverzeichnisstruktur (Tree), keine Dateien. Um auch leere Verzeichnisse zu kopieren, müssen Sie die Befehlszeilenoption */e* angeben
- **/k** Kopiert Dateien und behält das Attribut *Schreibgeschützt* bei den Zieldateien bei, wenn es bei den Quelldateien gesetzt war. Standardmäßig entfernt *Xcopy* das Attribut *Schreibgeschützt*.
- **/r** Kopiert schreibgeschützte Dateien
- **/h** Kopiert Dateien mit den Attributen *Versteckt* und *System*. Standardmäßig kopiert *Xcopy* weder versteckte Dateien noch Systemdateien.
- **/y** Unterdrückt die Ausgabe einer Aufforderung zur Bestätigung des Überschreibens einer vorhandenen Zieldatei
- **/–y** Fordert Sie auf, das Überschreiben einer vorhandenen Zieldatei zu bestätigen
- **/z** Kopiert im ausführbaren Modus über ein Netzwerk

Batchdateien verwenden

Für die Befehlszeile gibt es eine Art Programmiersprache, mit der Sie Befehle automatisieren und abspeichern können. Zum Schreiben von Batchdateien benötigen Sie lediglich den Windows-Editor.

Beispiel:

In der Batchdatei sollen der erste und zweite Parameter einfach per *Echo* ausgegeben werden. Dazu sollten Sie noch am Anfang den Befehl *@Echo off* verwenden, der verhindert, dass die Befehle, die ausgeführt, am Bildschirm ausgegeben werden. Beim Speichern müssen Sie beachten, dass Sie unter Dateityp die Option *Alle Dateien* auswählen und beim Dateinamen die Endung **.bat* oder **.cmd* hinzufügen.

Nachdem Sie die Batchdatei gespeichert haben, können Sie die Datei ganz einfach über die Befehlszeile ausführen lassen. Starten Sie dazu die Befehlszeile und wechseln Sie zum Verzeichnis, in dem sich die Batchdatei befindet. Alternativ können Sie die Batchdatei auch per Doppelklick unter Windows öffnen oder eine Verknüpfung zur Datei anlegen. Die wichtigsten Befehle in Batchdateien sind folgende:

- **REM <Kommentar>** Für Kommentare, diese werden beim Ausführen nicht berücksichtigt
- **ECHO <Bemerkung>** Ausgabe einer Meldung am Bildschirm
- **FOR <Bedingung>** Führt Befehle so lange aus, solange die Bedingung zutrifft
- **IF <Bedingung>** Führt einen Befehl nur dann aus, wenn die Bedingung zutrifft
- **GOTO <Sprungmarke>** Sprungbefehl zu einer Sprungmarke
- **:<Sprungmarke>** Sprungmarke, zu der mittels *GOTO* gesprungen werden kann
- **PAUSE** Wartet so lange, bis eine Taste gedrückt wird
- **CALL <Datei>** Führt eine andere Batchdatei aus

TIPP Weiterführende Informationen zu Batchdateien finden Sie auf den folgenden Internetseiten:

- *http://www.axel-hahn.de/axel/page_compi/bat_index.htm*
- *http://de.wikipedia.org/wiki/Stapelverarbeitung*

Weitere wichtige Befehle, vor allem für Batchdateien im Netzwerkbereich, finden Sie in der folgenden Tabelle:

Tabelle 20.1 Häufige Befehle für die Verwendung in Batchdateien

Befehl	Was können Sie mit diesem Befehl erreichen?
net use	Laufwerke verbinden und trennen, Druckeranschlüsse verbinden und trennen
net view	Server und Freigaben anzeigen
net share	Freigaben erstellen, ändern und löschen
cacls	NTFS-Zugriffsrechte anzeigen und ändern
net user	Benutzer verwalten
net group	Benutzergruppen verwalten
net computer	Konten für Computer in der Domäne anlegen und löschen
net accounts	Kennworteinstellungen verändern und anzeigen
net start	Startet einen Dienst
net stop	Beendet einen Dienst
net file	Zeigt die geöffneten Dateien an
net session	Zeigt die Sitzungen auf einem Computer an Trennt eine Sitzung
net time	Führt eine Zeitsynchronisierung mit einem anderen Computer im Netzwerk aus oder zeigt dessen Uhrzeit an
cipher	Verschlüsseln oder Entschlüsseln von Dateien und Ordnern
assoc	Zeigt oder ändert die Zuordnungen von Dateiendungen zu Programmen an
setver	Spielt einem Programm eine andere Betriebssystemversion vor

Arbeiten mit Umgebungsvariablen

Sie benötigen für nahezu jedes komplexere Skript neben den Befehlen für die Batchprogrammierung auch fast immer Umgebungsvariablen, da in den wenigsten Fällen alle Betriebssysteme und Programme in denselben Verzeichnissen gespeichert sind. Um das Systemverzeichnis herauszufinden, können Sie beispielsweise die Variable *%SystemRoot%* verwenden. Mit *%username%* ermitteln Sie den Benutzernamen des angemeldeten Benutzers. In der folgenden Tabelle zeigen wir Ihnen eine Übersicht über die wichtigsten Umgebungsvariablen und deren Bedeutung.

Tabelle 20.2 Die wichtigsten Systemvariablen in der Übersicht

Variable	Beispielwert	Bedeutung
ComSpec	F:\WINNT\system32\cmd.exe	Speicherort des Befehlsinterpreters
HOMEDRIVE	H:	Laufwerkbuchstabe für das Home Directory
HOMEPATH	\admin	Verzeichnis des Home-Directory
LOGONSERVER	\\CCI2000	Welcher Server hat das Domänenlogin durchgeführt?
NUMBER_OF_PROCESSORS	1	Anzahl der Prozessoren
OS	Windows_NT	Betriebssystem (Achtung: Auch bei Windows Server 2008 liefert die Variable *Windows_NT*)
Path	F:\WINNT\system32;F:\WINNT;F:\WINNT\System32\Wbem;F:\Programme\Support Tools\;F:\Programme\Resource Kit\;c:\dos	Suchpfad für Windows-Anwendungen
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH	Dateiendungen, die als ausführbare Dateien erkannt werden
PROCESSOR_ARCHITECTURE	x86	Prozessortyp (Windows Server 2003 unterstützt nur x86, das bedeutet Pentium-kompatible Prozessoren)
PROCESSOR_IDENTIFIER		Genaue Identifikation des Prozessors
PROCESSOR_LEVEL	5	Pentium = 5, 486 = 4
PROCESSOR_REVISION	080c	Interne Versionsnummer des Prozessors
ProgramFiles	F:\Programme	Pfad für Programminstallationen
PROMPT	PG	Promptzeichen in der Eingabeaufforderung
SystemDrive	F:	Laufwerkbuchstabe der Systemplatte

Tabelle 20.2 Die wichtigsten Systemvariablen in der Übersicht *(Fortsetzung)*

Variable	Beispielwert	Bedeutung
SystemRoot	F:\WINNT	Pfad zum Windows-Verzeichnis
TEMP	F:\Temp	Pfad für temporäre Dateien
TMP	F:\Temp	Pfad für temporäre Dateien
USERDNSDOMAIN	Contoso.com	Vollständiger DNS-Name der Active Directory-Domäne
USERDOMAIN	Contoso	NetBIOS-Name der Active Directory-Domäne
USERNAME	Admin	Name des angemeldeten Benutzers
USERPROFILE	C:\Benutzer\admin	Verzeichnis, in dem das Benutzerprofil des angemeldeten Benutzers gespeichert ist.
windir	C:\Windows	Das Windows-Verzeichnis

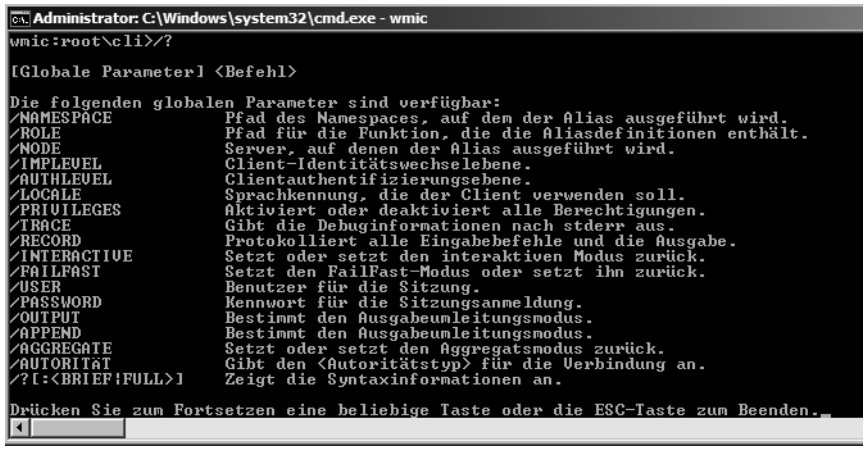
Verwaltung mit WMI und dem Tool WMIC

Die Grundidee der WMIC (Windows Management Instrumentation Commandline) ist einfach: Die umfassenden Funktionen, die WMI (Windows Management Instrumentation) potenziell bietet, sollen ohne Programmierung nutzbar werden. Das Tool ist nur für Windows XP Professional, Windows Server 2003, Windows Vista und Windows Server 2008 verfügbar, nicht für ältere Windows-Versionen. Die meisten der Funktionen, die von WMI angeboten werden, lassen sich auch mit WMIC nutzen. Die WMIC ist Teil von Windows Server 2008. Sie wird beim ersten Aufruf automatisch installiert. Dieser Prozess dauert allerdings nicht einmal eine Minute, danach kann dann die volle Funktionalität von WMIC genutzt werden. WMIC ist als Werkzeug für Administratoren konzipiert. Mit den über 80 Aliasen kann auf rund 150 Methoden zugegriffen werden. Diese Methoden haben wiederum eine Vielzahl von Eigenschaften. Die Reports können in unterschiedlichen Formaten wie Text oder XML erstellt werden. Für den Zugriff auf die insgesamt mehr als 10.000 Objekte, die standardmäßig bei Windows Server 2008 unterstützt werden, gibt es zwei WMIC-Modi:

- Im Befehlsmodus können direkt an der Eingabeaufforderung Befehle eingegeben werden.
- Im interaktiven Modus wird dagegen eine eigene WMIC-Befehlszeile geladen. Von dort aus können Sie dann durch die Strukturen der WMI navigieren.

Der interaktive Modus wird durch Eingabe von *Wmic* gestartet und kann mit *Quit* beendet werden. In diesem zweiten Modus können Sie Hilfeinformationen über die verfügbaren Aliase und Optionen anzeigen lassen. Die Hilfe rufen Sie mit */?* an der WMIC-Befehlszeile auf (Abbildung 20.15).

Abbildg. 20.15 Im interaktiven Modus können Sie durch die Strukturen der WMI navigieren



Um die Hilfefunktion an der Befehlszeile aufzurufen, verwenden Sie *Wmic /?*. Es wird dann die gleiche Hilfefunktion angezeigt. Die WMIC-Engine greift auf ein Alias-Schema zu. Dieses Schema setzt Bezeichner von WMI in die Aliase um. Das Schema kann editiert werden, sodass Sie bei Bedarf auch zusätzliche Aliase definieren können. Die WMIC-Engine greift dann auf die eigentliche WMI-Schnittstelle zu und erzeugt die Ergebnisse. Diese werden intern als XML gehandhabt und über XSLT in das gewünschte Format umgesetzt. Dabei gibt es verschiedene Standardformate wie die Anzeige an der Konsole. Diese Trennung von Komponenten gibt der WMIC eine hohe Flexibilität, weil Erweiterungen des WMI-Schemas ebenso gut umgesetzt werden können wie unterschiedliche Anforderungen an die Ausgabe. Wichtig ist bei der WMIC auch, dass nicht nur Informationen des lokalen Systems, sondern auch von externen Systemen abgefragt werden können. Je nach Befehl können auch Daten von mehreren Computern mit einer einzigen Anweisung angefordert werden. Die WMIC bietet eine Vielzahl von Möglichkeiten, was schon bei der Liste der Aliase deutlich wird. Diese können Sie sich in der Hilfefunktion anzeigen lassen. Wenn Sie den interaktiven Modus nutzen, können Sie durch die Strukturen der WMI navigieren. Die WMIC kennt dabei eine Reihe so genannter *Global Switches*, also von Schaltern, die Sie beeinflussen können und die wiederum das Verhalten der WMIC steuern. Den aktuellen Zustand dieser Schalter erfragen Sie mit dem Befehl *Context*. Zu den Switches gehört beispielsweise die Liste der Systeme, auf die zugegriffen wird. Diese finden sich beim Switch *Node(s)*. Durch den Befehl */node:Server10* können Sie zum Beispiel zusätzlich den Server mit dem Namen *Server10* in die Liste der Systeme aufnehmen, auf die zugegriffen wird. Servernamen mit Sonderzeichen müssen in Anführungszeichen gesetzt werden. Die beiden wichtigsten Befehle für den Einstieg in die WMIC sind:

- <Alias> list full
- <Alias> list brief

Der erste der beiden Befehle zeigt für den ausgewählten Alias eine umfassende Liste von Informationen an, der zweite dagegen die Kurzform dieser Liste. Sie können diesen Befehl beispielsweise mit den folgenden Aliasen testen:

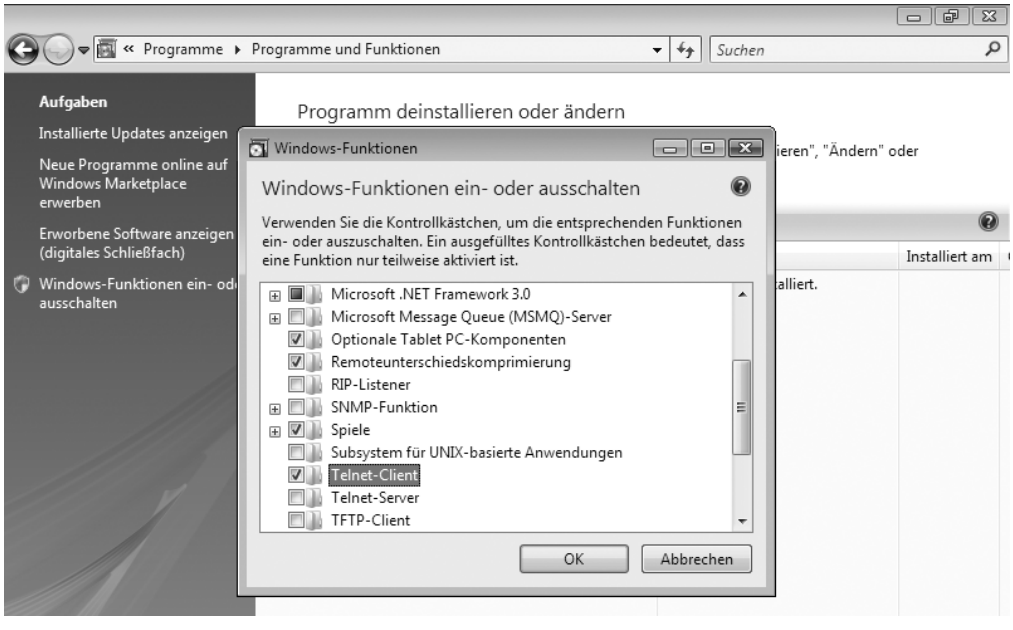
os (Betriebssytem)
nic (Netzwerkadapter)
volume (Logischer Datenträger)

Mit diesen einfachen List-Befehlen für Volumes können Sie schnell und effizient auf Zustandsdaten des Systems zugreifen. Wenn Sie sich für die Aliase mit */?* die Hilfeinformationen anzeigen lassen, werden weitere Methoden dargestellt. Dabei wird deutlich, dass es eine Reihe von Methoden gibt, die bei verschiedenen Objekten in der gleichen Form auftauchen. Es gibt aber auch Methoden, die nicht überall unterstützt werden. Um die Möglichkeiten einer Methode wie *OS Set* kennen zu lernen, geben Sie *OS Set /?* ein. In diesem Fall wird dann beispielsweise eine Liste der Eigenschaften angezeigt, die Sie für das Betriebssystem setzen können. Dazu zählt zum Beispiel die Zeitzone. Auch die vordefinierten Formate sind recht nützlich. Neben der Anzeige an der Konsole können Sie beispielsweise mit *OS List Full /format:rawxml* eine Ausgabe im XML-Format erzeugen. Über eigene XSL-Dateien könnten Sie das Ausgabeformat auch anpassen. Wichtig ist zusätzlich, dass Sie mit Abfragen arbeiten können, wobei das Format dieser Abfragen weitgehend identisch mit dem der WMI-Filter ist. Mit den Methoden *Call* und *Set* können Sie auch Änderungen an bestehenden Parametern vornehmen.

Telnet verwenden

Zwar wird heutzutage Telnet in Windows-Umgebungen nur noch selten zur Verwaltung eingesetzt, zu Testzwecken kann das Tool aber durchaus sinnvoll sein. Allerdings wird sowohl bei Windows Vista als auch bei Windows Server 2008 weder der Telnet-Client noch der Telnet-Server installiert. Unter Windows Vista wird diese Funktion in der Systemsteuerung über *Programme/Programme und Funktionen/Windows-Funktionen ein- oder ausschalten* aktiviert (Abbildung 20.16).

Abbildg. 20.16 Installieren des Telnet-Client unter Windows Vista

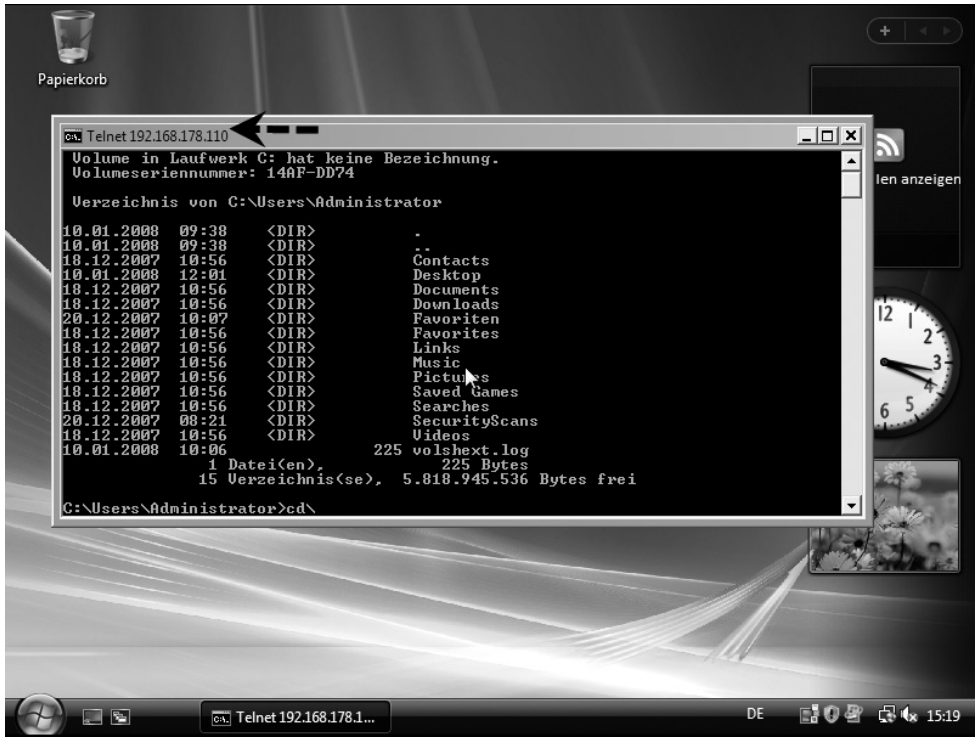


Bei Windows Server 2008 werden der Client beziehungsweise der dazugehörige Server über den Server-Manager als Feature hinzugefügt. Nach der Installation von Telnet-Server unter Windows Server

2008 muss der Systemdienst *Telnet* zunächst aktiviert und gestartet werden. Nachdem der Client und der Server installiert sind, kann über Telnet gearbeitet werden. Die wichtigsten Befehle dazu sind:

- **Open <IP-Adresse>** Öffnet eine Telnet-Verbindung mit einem Host. Nach dem Verbindungsaufbau und der Authentifizierung am Server, wird eine Befehlszeile auf dem Client geöffnet, die Befehle auf dem Server durchführt. Zunächst muss auf dem Client der Befehl *Telnet* eingegeben werden. Mit *Telnet <IP-Adresse>* wird sofort eine Verbindung aufgebaut.
- **Close** Schließt eine Telnet-Verbindung
- **Display** Zeigt die Einstellungen des Clients an

Abbildg. 20.17 Nach dem Verbindungsaufbau über Telnet kann mit der Befehlszeile des Servers gearbeitet werden



Zusammenfassung

Mit der Windows PowerShell und der herkömmlichen Eingabeaufforderung kann Windows Server 2008 sehr effizient verwaltet werden. In diesem Kapitel haben wir Ihnen den Einstieg ermöglicht sowie einige Praxisbeispiele gezeigt, die den Umgang mit der neuen Verwaltungsshell verdeutlichen sollen. Im nächsten Kapitel widmen wir uns der Datensicherung von Windows Server 2008. Auch hier hat Microsoft wieder einige Verbesserungen und Änderungen vorgenommen.

Kapitel 21

Datensicherung und Wiederherstellung

In diesem Kapitel:

Das Datensicherungsprogramm in Windows Server 2008 wurde neu entwickelt und wird standardmäßig nicht mehr automatisch installiert. Bandlaufwerke werden nicht mehr unterstützt. Natürlich besteht auch weiterhin die Möglichkeit, dass Drittanbieter Programme für Windows Server 2008 zur Verfügung stellen, die auch eine Sicherung auf Band ermöglichen. Die integrierte Sicherung lässt sich allerdings auf diese Weise nicht nutzen. Die Sicherung unterstützt jetzt besser die integrierten Sicherungsfunktionen von SQL Server 2005/2008 und Office SharePoint Server 2007. Die Verwaltung der Sicherung findet über die MMC statt. So können Sie auch über das Netzwerk mit der MMC die Datensicherung von mehreren Servern gleichzeitig konfigurieren. Neu sind die Unterstützung für DVD-Brenner sowie die automatische Überwachung des freien Festplattenplatzes auf dem Sicherungsmedium. Die neue Windows Server-Sicherung unterstützt keine Sicherung auf Band mehr. Auch die Onlinesicherung von Exchange-Servern ist mit den Bordmitteln nicht mehr möglich. Hierzu muss auf die Programme von Drittherstellern zurückgegriffen werden. Mit dem Sicherungsprogramm können aber weiterhin Daten auf dem Server als auch der Server selbst gesichert und wiederhergestellt werden.

HINWEIS Datensicherungen, die Sie mit älteren Versionen von *Ntbackup.exe* erstellt haben, sind nicht mehr kompatibel zur neuen Windows Server-Sicherung. Sollten Sie eine solche Sicherung benötigen, stellt Microsoft kostenlos das alte *ntbackup.exe* auf der Internetseite *http://go.microsoft.com/fwlink/?LinkId=82917* zur Verfügung.

Die Windows Server-Sicherung im Überblick

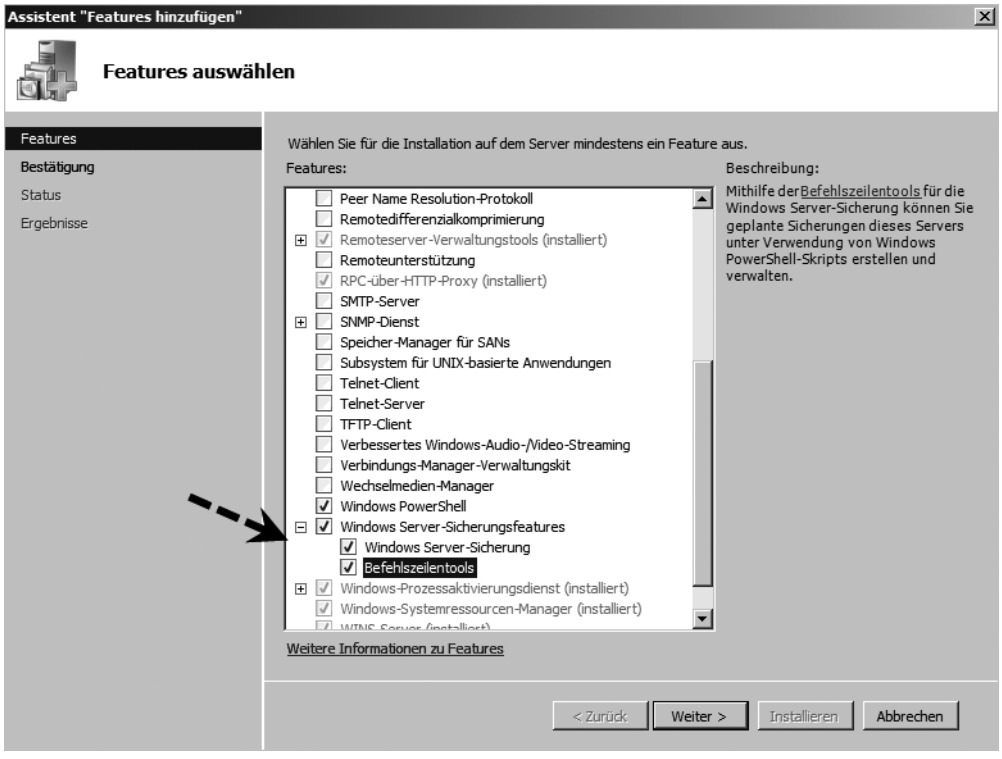
Das Programm sichert die Daten über den Schattenkopiedienst (Volume Shadow Service, VSS) mit Hilfe einer Block-Level-Backup-Technologie in VHD-Dateien. Diese Dateien werden auch bei der Sicherung von Windows Vista erstellt. Nach einem vollständigen Backup können einfach inkrementelle Sicherungen auf Blockebene erstellt werden. Auch diese benötigen deutlich weniger Platz als bei den Vorgängerversionen von Windows Server 2008. Außerdem werden Sicherungen sehr viel schneller durchgeführt. Microsoft favorisiert Backup-To-Disk oder Backup-To-DVD als Sicherungsstrategie. Auch die Wiederherstellungsmöglichkeiten wurden deutlich optimiert. Einzelne Dateien, aber auch der komplette Server, lassen sich leichter und schneller wiederherstellen als unter Windows Server 2003. Ist die Hardware defekt, lässt sich die Sicherung des Servers auch auf neuer Hardware wiederherstellen. Die Systempartitionen werden automatisch immer in alle Sicherungen integriert, sodass die auf diesen Partitionen gespeicherten Daten, auch das Betriebssystem, immer sehr leicht wiederhergestellt werden können. Mit der Windows Server-Sicherung können vollständige Server (alle Volumes), ausgewählte Volumes oder der Systemstatus gesichert werden. Sie können Volumes, Ordner, Dateien, bestimmte Anwendungen und den Systemstatus wiederherstellen. Mit der Verwaltungskonsole der Windows Server-Sicherung können Sicherungen auch für Remotecomputer erstellt und verwaltet werden. Damit die Sicherung verwendet werden kann, müssen Sie Mitglied der Gruppe *Administratoren* oder *Sicherungsoperatoren* sein.

TIPP In der Befehlszeile wird das Tool *Wbadmin.exe* zur Konfiguration und Verwaltung der Sicherungen verwendet. Außerdem sind in Windows Server 2008 einige Cmdlets für die PowerShell enthalten (siehe auch Kapitel 20). Auf der Seite *http://go.microsoft.com/fwlink/?LinkId=93317* finden Sie dazu weitere Informationen.

Windows Server-Sicherung installieren und konfigurieren

Damit die neue Windows Server-Sicherung verwendet werden kann, installieren Sie diese über den Server-Manager als neues Feature. Die Sicherungsfunktion von Windows Server 2008 ist in die beiden Unterkomponenten *Windows Server-Sicherung* und *Befehlszeilentools* unterteilt (Abbildung 21.1).

Abbildg. 21.1 Die Windows Server-Sicherung wird als Feature nachträglich installiert

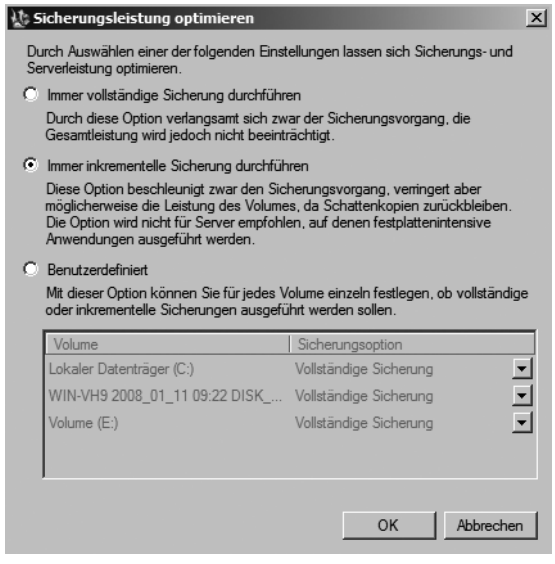


Nach der Installation kann die Windows Server-Sicherung über *Start/Verwaltung/Windows-Server-Sicherung* verwaltet werden. Alternativ können Sie im Suchfeld des Startmenüs auch *wbadmin.msc* eingeben.

HINWEIS Die Windows Server-Sicherung ist für alle 32- und 64-Bit-Editionen von Windows Server 2008 verfügbar, nicht jedoch bei Server Core-Installationen. Hier kann die Sicherung dann entweder mit *Wbadmin.exe* über die Befehlszeile verwaltet oder von einem anderen Server aus mit dem Snap-In durchgeführt werden. Auch die Cmdlets für die PowerShell sind auf Core-Servern nicht verfügbar.

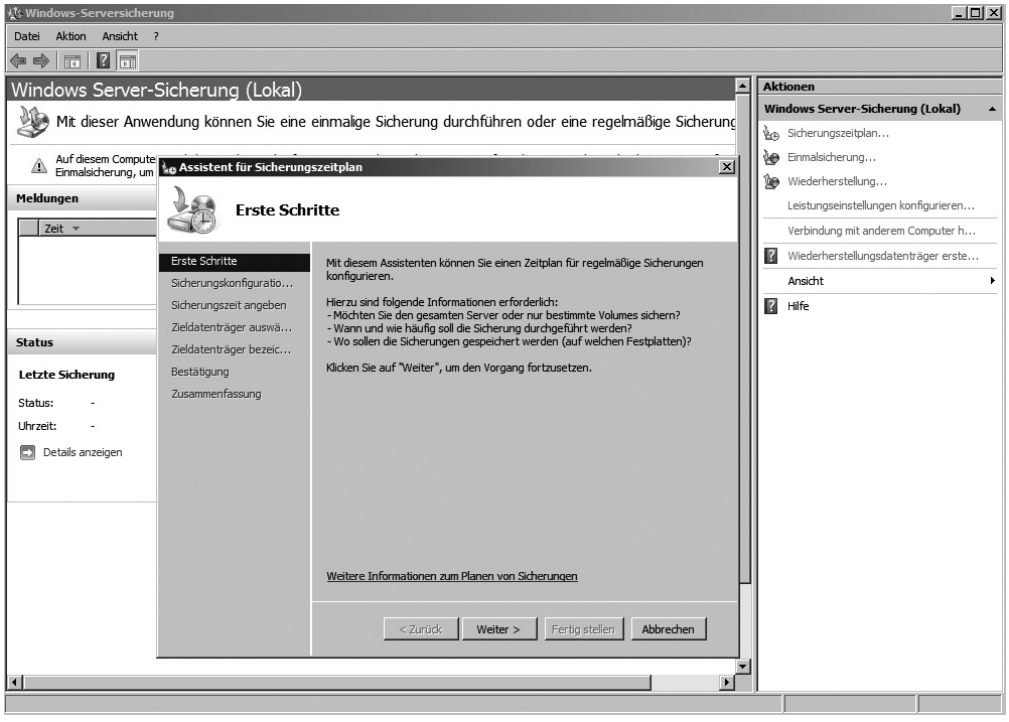
Diese Konsole kann darüber hinaus in jeder MMC geladen werden. Über Assistenten lassen sich Sicherungs- und Wiederherstellungsvorgänge sehr leicht durchführen. Auch die komplette Systemwiederherstellung wurde überarbeitet und verbessert. Die neue Datensicherung sichert die Daten blockbasiert von den Datenträgern nicht mehr pro Datei. Standardmäßig werden immer vollständige Sicherungen durchgeführt. Über den Menübefehl *Aktion/Leistungseinstellungen konfigurieren* kann aber auch eine inkrementelle Sicherung aktiviert werden (Abbildung 21.2). Eine inkrementelle Sicherung sichert alle Daten, die sich seit der letzten Sicherung geändert haben. Unveränderte Daten werden nicht gesichert, da sich diese in einer vorherigen Sicherung befinden. Bei dieser Sicherungsart bauen die Datensicherungen aufeinander auf. Zu einem gewissen Zeitpunkt benötigen Sie eine Vollsicherung, zum Beispiel freitags. Am Montag werden alle Daten gesichert, die sich seit Freitag verändert haben. Am Dienstag werden alle Daten gesichert, die sich seit Montag verändert haben.

Abbildg. 21.2 Konfigurieren der Leistungsoptionen der Sicherung



Wenn Sie daher am Freitagmorgen eine vollständige Wiederherstellung durchführen müssen, werden erst die letzte Vollsicherung des letzten Freitag und dann alle Sicherungen bis zur aktuellen inkrementellen Sicherung benötigt. Der Vorteil dabei ist, dass jeder Sicherungsvorgang sehr schnell durchgeführt werden kann, da nur wenige Daten gesichert werden müssen. Bei inkrementellen Sicherungen sollten Sie auf jeden Fall einmal in der Woche eine Vollsicherung durchführen.

Abbildg. 21.3 Die Windows Server-Sicherung bietet eine neue Oberfläche zur Verwaltung

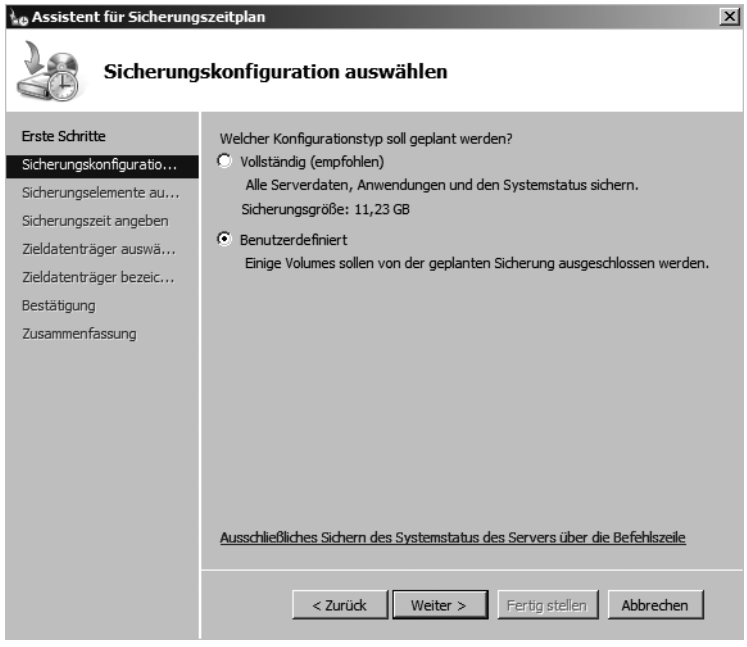


Nachdem die Sicherung und Verwaltungsprogramme installiert wurden, kann eine Datensicherung eingerichtet werden. Microsoft empfiehlt zur Sicherung einen externen Datenträger, der über USB oder Firewire mit dem Computer verbunden wird.

ACHTUNG Achten Sie darauf, dass die zur Sicherung verwendete externe Festplatte keine Daten enthält. Vor der Sicherung wird der Datenträger durch das Sicherungsprogramm automatisch formatiert, sodass alle gespeicherten Daten verloren gehen.

Um einen neuen Sicherungsauftrag zu erstellen, rufen Sie entweder über die Verwaltung die Konsole des Sicherungsprogramm auf oder geben im Suchfeld des Startmenüs den Befehl *wbadmin.msc* ein. Der Befehl *wbadmin.exe* startet das Befehlszeilen-Tool der Sicherung. Ein neuer Auftrag wird über *Aktion/Sicherungszeitplan* erstellt. Auf der nächsten Seite des Assistenten kann ausgewählt werden, ob der komplette Server gesichert werden soll oder die Partitionen und Daten selbst ausgewählt werden (Abbildung 21.4).

Abbildg. 21.4 Auswählen der zu sichernden Daten

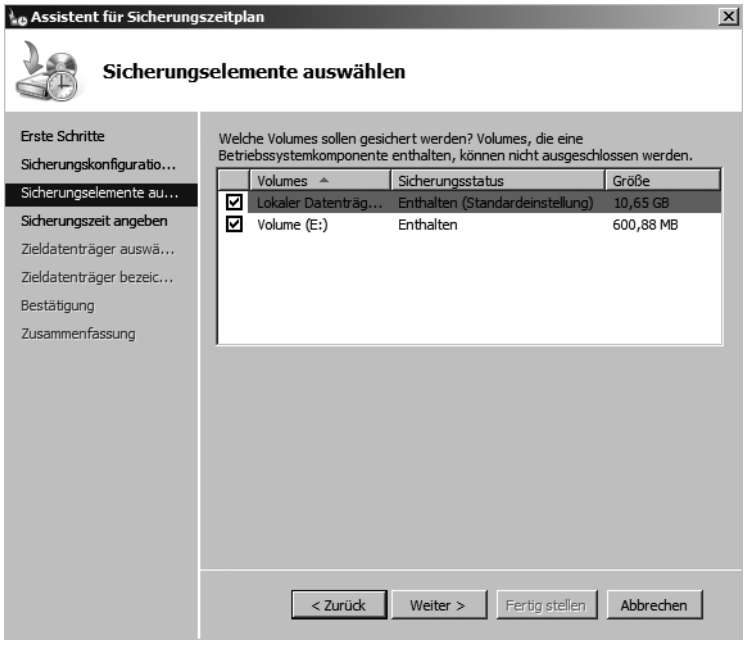


Was bei der vollständigen Sicherung gesichert wird, dürfte klar sein. Auf den folgenden Seiten beschreiben wir daher die benutzerdefinierte Auswahl etwas genauer. Auf der nächsten Seite wird ausgewählt, welche Partitionen gesichert werden sollen. Standardmäßig sind alle Partitionen aktiviert.

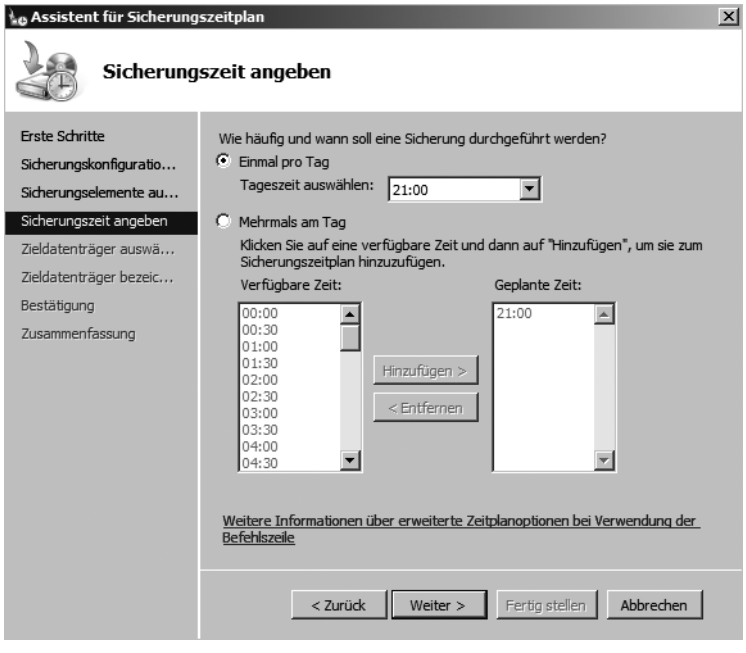
HINWEIS Das Sicherungsprogramm kann bis zu 512 Kopien einer Partition in der Sicherung speichern. Da zur Sicherung der Schattenkopiedienst genutzt wird, ist damit das Limit der Schattenkopien erreicht. Alle Partitionen, die Daten, Dateien und Programme des Betriebssystems enthalten, werden dabei immer automatisch ausgewählt und können auch nicht abgewählt werden. Diese Daten werden immer gesichert.

Auf der nächsten Seite (Abbildung 21.6) wird der Zeitplan erstellt, über den der Server gesichert wird. Hier kann festgelegt werden, ob mehrmals oder nur einmal pro Tag gesichert wird. Die Datensicherung bietet hier deutlich mehr Möglichkeiten als die Vorgängerversion in Windows Server 2003.

Abbildg. 21.5 Auswählen der zu sichernden Partitionen des Servers

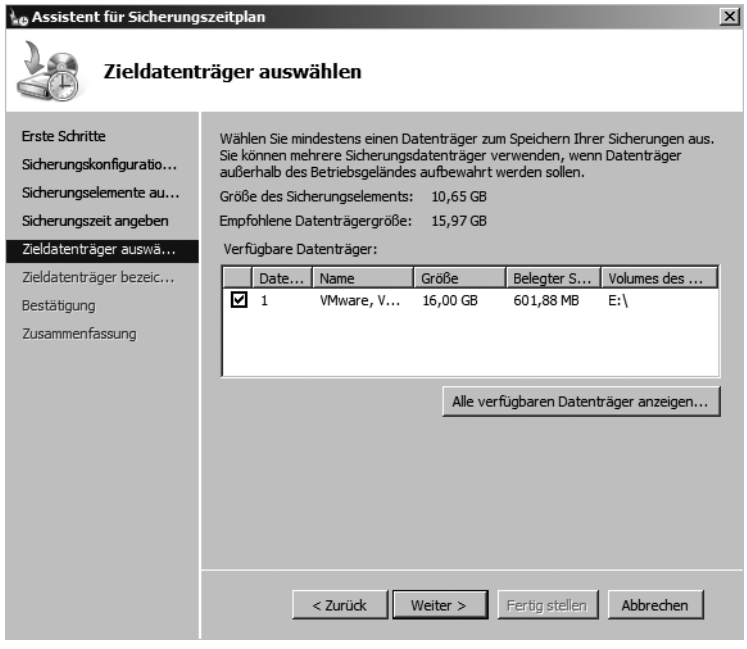


Abbildg. 21.6 Konfigurieren der Sicherungszeit



Auf der nächsten Seite wird das Sicherungsmedium ausgewählt, auf das die Daten gesichert werden sollen. Wird die Festplatte nicht angezeigt, hilft ein Klick auf die Schaltfläche *Alle verfügbaren Datenträger anzeigen*. Hier kann jetzt der entsprechende Datenträger ausgewählt werden. Datenträger, auf denen Daten des Betriebssystems gespeichert sind, können als Sicherungsmedium nicht ausgewählt werden.

Abbildg. 21.7 Auswählen des Zieldatenträgers für die Sicherung

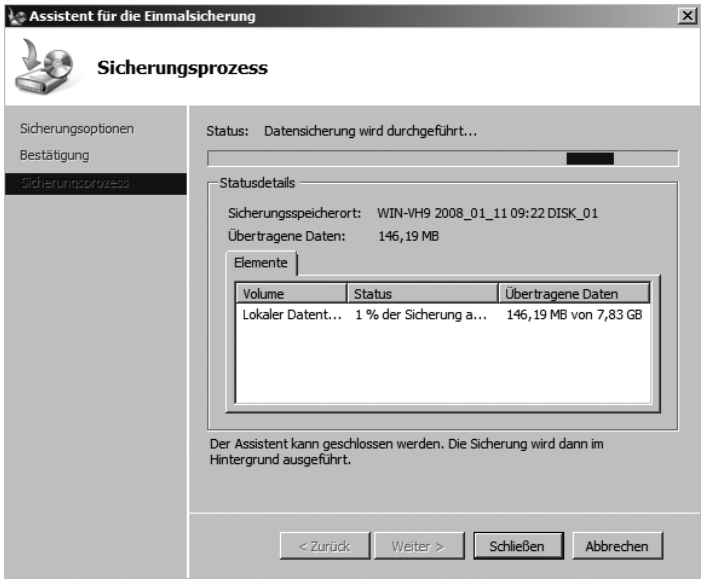


Nachdem der Datenträger ausgewählt wurde und Sie auf *Weiter* klicken, erscheint eine Meldung die darauf hinweist, dass der Datenträger formatiert wird, damit das Sicherungsprogramm einen Überblick über die Größe und Verfügbarkeit des Datenträgers erhält. Die Formatierung wird aber nicht sofort, sondern erst nach der Einrichtung durchgeführt. Auf den nächsten Seiten erhalten Sie noch eine Zusammenfassung und der Datenträger wird anschließend neu formatiert.

HINWEIS Die Sicherung überwacht automatisch den Speicherplatz auf den Datenträgern, auf denen die Sicherungen abgelegt werden. Steht nicht mehr genügend Plattenplatz zur Verfügung, informiert die Sicherung darüber und führt keine Sicherung mehr durch. Außerdem wird der Datenträger nicht mehr im Explorer des Servers angezeigt und steht ausschließlich nur für die Datensicherung zur Verfügung.

Die Einrichtung des Sicherungszeitplans ist damit abgeschlossen. Wollen Sie eine sofortige Einmalsicherung durchführen, kann der entsprechende Assistent ebenfalls über das Menü *Aktion* gestartet werden. Der Assistent übernimmt die Einstellungen der vorhandenen, geplanten Sicherung, sodass nicht so viele Eingaben gemacht werden müssen. Natürlich können für Einmalsicherungen auch unterschiedliche Optionen gewählt werden. Anschließend wird die Sicherung über den Schattenkopiedienst durchgeführt.

Abbildg. 21.8 Anzeigen des Sicherungsprozesses

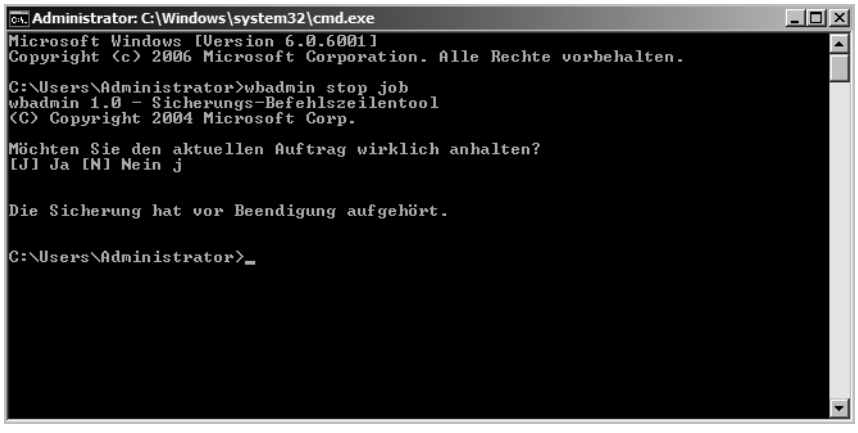


Sicherung in der Befehlszeile durchführen

Für Skripts oder Core-Server steht das Befehlszeilen-Tool *wbadmin.exe* für die Verwaltung der Sicherungen zur Verfügung. Über */?* wird für jeden der unten aufgelisteten Befehle eine entsprechende Hilfe eingeblendet. Die wichtigsten Befehle für das Tool sind:

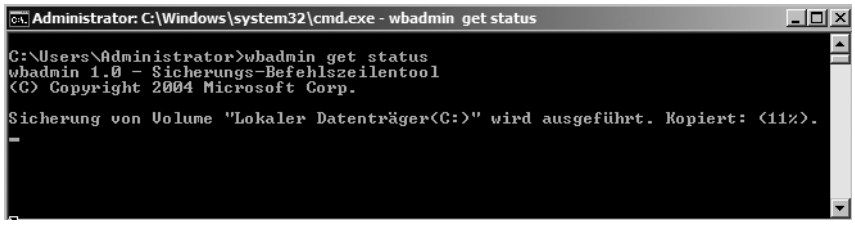
- **Wbadmin enable backup** Erstellt eine tägliche Sicherung
- **Wbadmin disable backup** Deaktiviert die tägliche Sicherung
- **Wbadmin start backup** Startet einen Sicherungsauftrag
- **Wbadmin stop job** Unterbricht eine laufende Sicherung oder Wiederherstellung

Abbildg. 21.9 Ein laufender Datensicherungsauftrag kann in der Befehlszeile gestoppt werden



- **Wbadmin get disks** Zeigt die IDs der Disk an, die gesichert und auf denen Sicherungen abgelegt werden können
- **Wbadmin get versions** Zeigt Informationen über die verfügbaren Sicherungen an
- **Wbadmin get items** Zeigt die enthaltenen Daten einer Sicherung an
- **Wbadmin start recovery** Startet eine Wiederherstellung
- **Wbadmin get status** Zeigt den Status einer laufenden Sicherung oder Wiederherstellung an

Abbildg. 21.10 Anzeigen des Sicherungsstatus einer laufenden Sicherung in der Befehlszeile



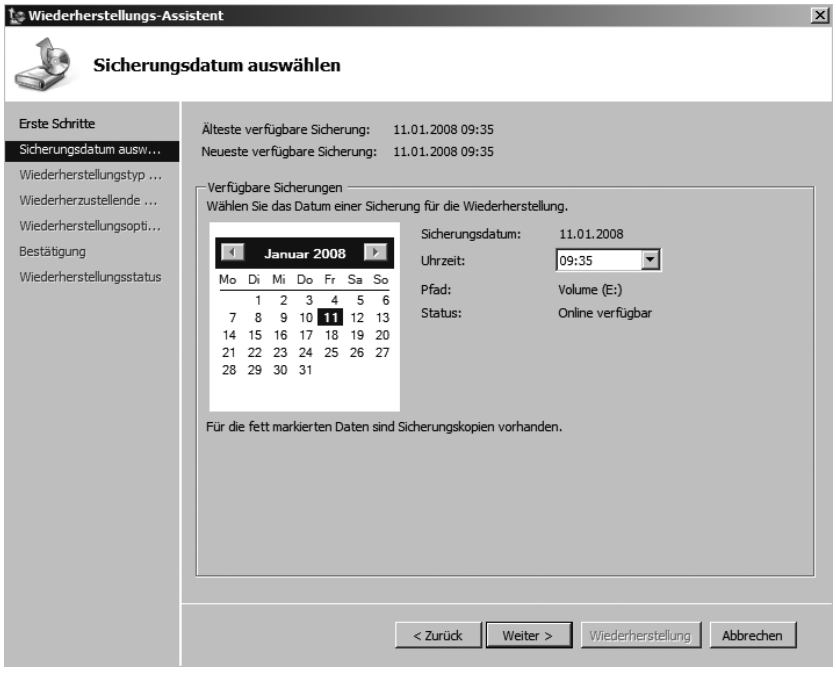
- **Wbadmin start sysstaterecovery** Stellt den Systemstatus wieder her
- **Wbadmin start sysrecovery** Startet eine vollständige Systemwiederherstellung, die später in den Computerreparaturoptionen über die Windows Server 2008-DVD wiederhergestellt werden kann

Daten mit dem Sicherungsprogramm wiederherstellen

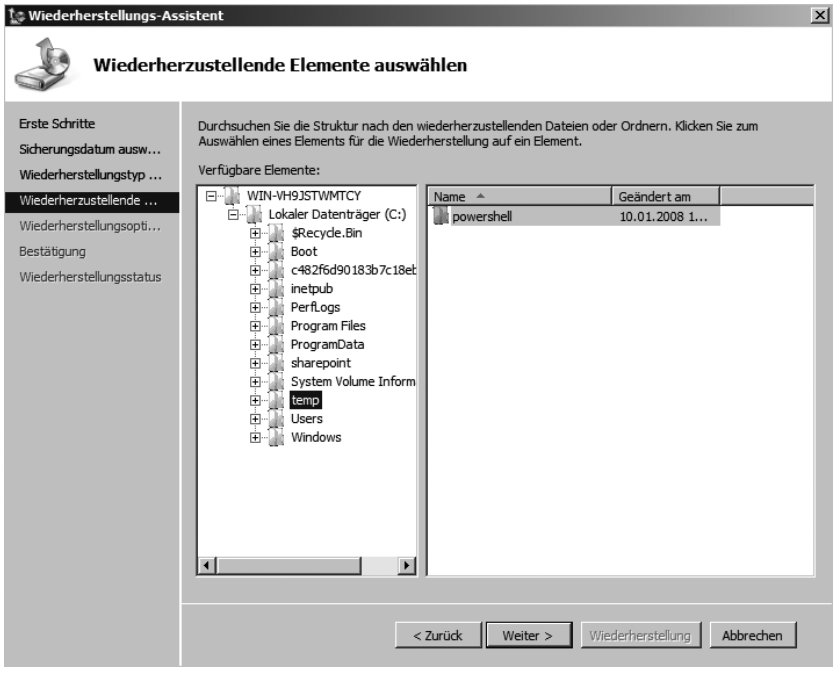
Wenn auf dem Server Sicherungen zur Verfügung stehen, besteht auch die Möglichkeit, einzelne Dateien und Ordner wiederherzustellen. Auch dazu wird das Sicherungsprogramm verwendet. Eine Wiederherstellung wird über das Menü *Aktion* gestartet. Auch hier führt ein Assistent durch die einzelnen Schritte der Wiederherstellung. Bestätigen Sie zunächst die Startseite des Assistenten. Hier kann auch ausgewählt werden, ob eine Wiederherstellung des lokalen Servers oder eines Servers im Netzwerk durchgeführt werden soll. Auf der nächsten Seite kann ausgewählt werden, zu welchem Datum Daten wieder hergestellt werden sollen.

Auf der nächsten Seite (Abbildung 21.12) wird schließlich festgelegt, welche Daten wiederhergestellt werden sollen. Hier besteht die Möglichkeit, komplette Volumes wiederherzustellen, oder nur einzelne Dateien und Ordner. Als Nächstes wird bestimmt, welche Daten aus der Sicherung wiederhergestellt werden sollen.

Abbildg. 21.11 Auswählen des Datums, zu dem Daten wiederhergestellt werden sollen

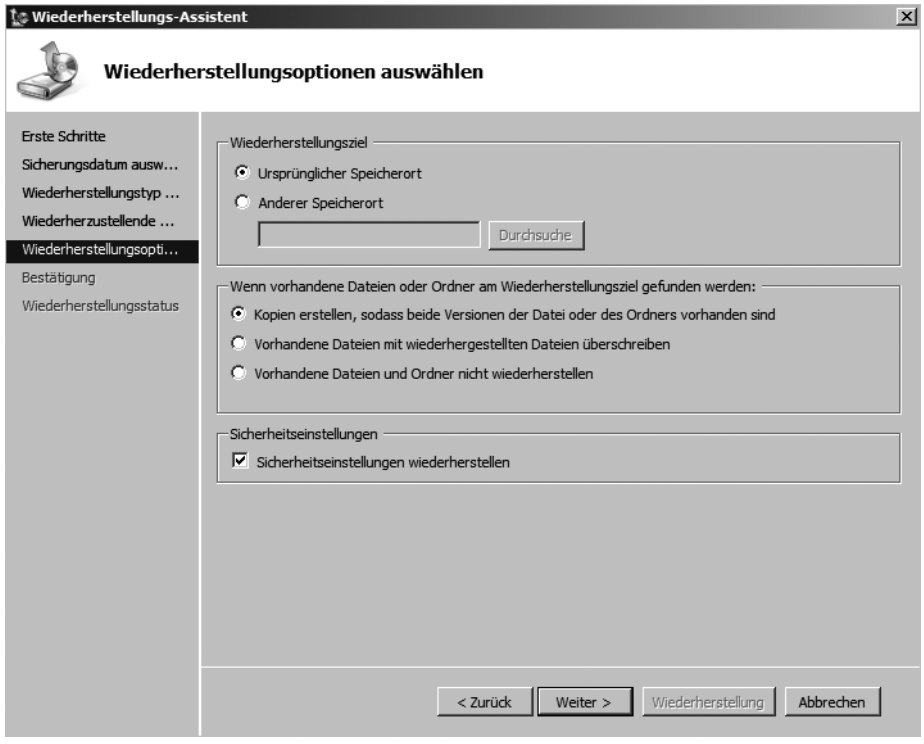


Abbildg. 21.12 Auswählen der Daten, die wiederhergestellt werden sollen



Auf der nächsten Seite wird ausgewählt, wo die Dateien wiederhergestellt werden, ob vorhandene Dateien überschrieben werden, und ob die Berechtigungen und Sicherheitseinstellungen der Dateien ebenfalls wiederhergestellt werden sollen. Die verschiedenen Optionen sind leicht verständlich und selbsterklärend. Hier hat Microsoft die Oberfläche deutlich optimiert. Anschließend beginnt der Assistent mit der Wiederherstellung der Daten.

Abbildg. 21.13 Auswählen der Wiederherstellungsoptionen



Kompletten Server mit dem Sicherungsprogramm wiederherstellen

Wurde auf dem Server eine vollständige Datensicherung erstellt, kann mit dieser der komplette Server wiederhergestellt werden, wenn dieser zum Beispiel nicht mehr starten kann. Dazu muss der Datenträger mit der Sicherung mit dem Server verbunden und der Server mit der Windows Server 2008-DVD gebootet werden. Auf der Startseite des Installationsassistenten klicken Sie auf *Weiter*. Auf der nächsten Seite wird aber statt der Installation der Menüpunkt *Computerreparaturoptionen* ausgewählt. Der Vorgang ist übrigens identisch mit Windows Vista, nur das Sicherungsprogramm sieht am Client etwas anders aus. In den Systemwiederherstellungsoptionen kann jetzt *Windows Complete PC-Wiederherstellung* ausgewählt werden (Abbildung 21.14).

HINWEIS Windows Server 2008 unterstützt die Wiederherstellung einer Systemsicherung auch auf anderer Hardware. Es muss keine Rücksicht mehr auf den Hardware Abstraction Layer (HAL) gemacht werden. Die neue Hardware muss lediglich zertifiziert für Windows Server 2008 sein.

Abbildg. 21.14 Komplette Wiederherstellung von Windows Server 2008

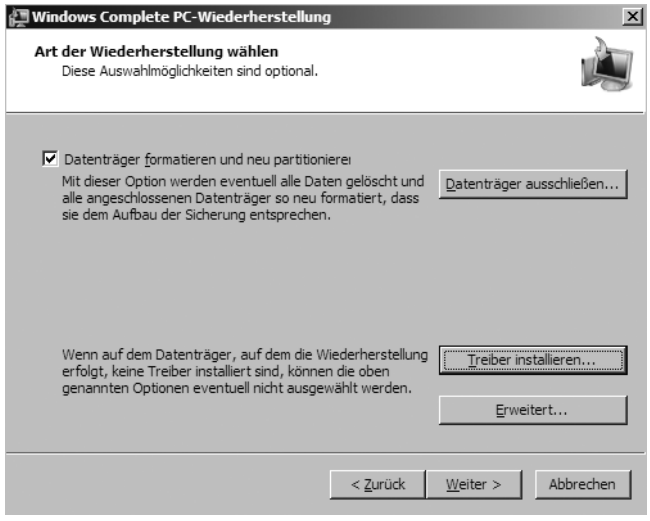
Als Nächstes durchsucht der Assistent alle verfügbaren Datenträger, und der Zeitpunkt, zu dem der Server zurückgesetzt werden soll, kann ausgewählt werden (Abbildung 21.15).

Abbildg. 21.15 Auswählen der Sicherung, die wiederhergestellt werden soll

Als Nächstes wird ausgewählt, ob der Datenträger, der wiederhergestellt werden soll, neu formatiert und partitioniert wird, oder ob die Daten auf die alte Partition zurückgesichert werden. Über die Schaltfläche *Datenträger ausschließen* werden die Datenträger ausgewählt, die nicht wiederhergestellt werden sollen, weil diese zum Beispiel Daten enthalten. Über *Treiber installieren* lassen sich wichtige Treiber integrieren, die für die Wiederherstellung unter Umständen benötigt werden. In

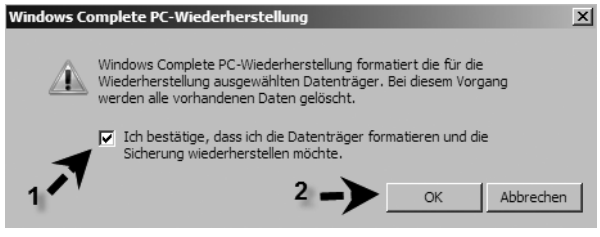
den Optionen unter *Erweitert* wird festgelegt, dass der Server automatisch nach der Wiederherstellung neu starten soll und Datenträger auf Defekte überprüft werden.

Abbildg. 21.16 Auswählen der Wiederherstellungsoptionen des Servers



Als Nächstes wird eine Zusammenfassung angezeigt und Sie können die Eingaben noch mal überprüfen. Als Abschluss erscheint eine Meldung, die darüber informiert, dass die Datenträger, die wiederhergestellt werden, neu formatiert werden müssen. Diese Meldung muss bestätigt werden, bevor die Wiederherstellung beginnt.

Abbildg. 21.17 Bestätigen der Formatierung des Systemdatenträgers



Anschließend beginnt der Assistent mit der Wiederherstellung des Servers. Nach der Wiederherstellung steht der Server wieder zur Verfügung.

Bluescreens verstehen und beheben

Wenn Wiederherstellungen auf einem Server notwendig sind, liegt häufig ein Bluescreen vor. Diese Fehler tauchen aber nicht nur bei älteren Windows-Versionen auf, sondern unter Umständen auch unter Windows Server 2008. Im folgenden Abschnitt beleuchten wir ausführlicher, wie Bluescreens entstehen und wie diese behoben werden, damit eine Wiederherstellung unter Umständen nicht

notwendig wird. So gut wie jeder Windows-Anwender kennt den blauen Bildschirm mit den kryptischen Fehlermeldungen. Was viele ärgert, soll das System jedoch schützen. Bluescreens werden von Profis auch oft als Stopp-Fehler bezeichnet. Sobald eine solche Meldung erscheint, ist Windows nicht mehr funktionsfähig und der Betrieb wird unterbrochen. Wurden geöffnete Dateien nicht gespeichert, können sogar Daten verloren gehen.

HINWEIS In diesem Abschnitt werden nicht alle Arten von Bluescreens aufgelistet, da es über 150 verschiedene Varianten gibt. Die möglichen Ursachen sowie deren Behebung sind allerdings häufig recht ähnlich. Eine ausführliche Liste aller möglichen Bluescreens unter Windows XP und Vista sowie Windows Server 2008 finden Sie auf der Webseite *http://msdn2.microsoft.com/en-us/library/ms793688.aspx*. Eine Liste der Windows-9x/ME-Bluescreens gibt es auf der Seite *http://support.microsoft.com/default.aspx?scid=kb;en-us;q150314*. Diese Listen werden aber für das Verständnis von Bluescreens selten benötigt und dienen eher der allgemeinen Information oder auch als letzte Anlaufstelle, wenn die übrigen Maßnahmen aus diesem Artikel keine Abhilfe schaffen.

Ursachenforschung bei Bluescreens betreiben

Ein Bluescreen ist in fast allen Fällen kein Fehler, der durch Windows oder eine Anwendung verursacht wird. Hauptsächlich sind fehlerhafte Treiber Schuld, dass Windows aufgibt und mit einem Fehler abstürzt. Bluescreens kommen unter Windows 9x/ME, NT 4.0 und 2000 deutlich häufiger vor als unter XP oder Windows Server 2003. Bei Windows Vista und Windows Server 2008 treten diese noch seltener auf, bedeuten in diesem Fall dafür aber auch oft größere Schwierigkeiten. Neben fehlerhaften Treibern kommen Bluescreens insbesondere dann vor, wenn Hardware defekt ist. Am häufigsten hängen entsprechende Probleme mit dem Arbeitsspeicher oder einer überhitzten CPU zusammen. Ebenfalls weit verbreitet sind defekte Festplattencontroller oder Hauptplatinen. Auch wenn Windows an einem Dateizugriff scheitert, weil die Platte defekt ist, bedeutet das oft eine Ankündigung eines Plattenausfalls. Solche Fehler äußern sich aber meist durch entsprechende Geräusche der Festplatte und Abstürze anderer Art, zum Beispiel das Einfrieren des Systems. Bei einem Bluescreen läuft Windows noch stabil genug, um den Fehler zu protokollieren und sich selbst sofort zu beenden. Bei Windows Vista und Windows Server 2008 treten Bluescreens vorwiegend nach der Installation falscher Treiber auf. Dies liegt daran, dass Windows Vista und Windows Server 2008 bei der Hardware-Verwaltung anders vorgehen als Windows XP und Windows Server 2003, um Systemabstürze durch fehlerhafte Treiber zu verhindern. Unter der 64-Bit-Version treten häufig Bluescreens auf, wenn neben der CPU nicht alle Komponenten des Computers 64-Bit-tauglich sind. In diesem Fall sollten Sie bei Ihrem Händler rückfragen oder bei einem selbst gebauten Computer selbst die Hardware wechseln. Achten Sie am besten bereits beim Kauf darauf, nur 64-Bit-kompatible Komponenten zu erwerben. Damit Windows Vista oder Windows Server 2008 in der 64-Bit-Version installiert werden kann, reicht es nicht aus, dass nur die CPU 64-Bit-tauglich ist.

Erscheint ein Bluescreen und haben Sie die Einstellungen in Windows so vorgenommen, wie wir es am Ende des Abschnitts empfehlen, erhalten Sie eine recht aussagekräftige Fehlermeldung, die als erster Anhaltspunkt für die Internetrecherche dienen kann. Meistens wird eine achtstellige Hexadezimalzahl angegeben, außerdem eine kurze Beschreibung des Fehlers, oft *IRQ_NOT_LESS_OR_EQUAL* oder *INACCESSIBLE_BOOT_DEVICE*. Manchmal wird auch die Datei angezeigt, die den Fehler verursacht hat – meistens eine **.sys*-Datei, also ein Treiber. Diese Datei muss nicht zwangsläufig Schuld am Bluescreen sein, kann aber in die Internetrecherche mit einbezogen werden, um die Ursache und damit das Suchergebnis einzugrenzen. Am Ende des Abschnitts stellen wir

Ihnen Tools vor, mit denen Sie die Protokolldateien analysieren können und die weitere Hinweise zur Fehlersuche im Internet liefern.

Warum sind fehlerhafte Treiber schuld?

Vor allem unter Windows NT 4.0 oder 9x, aber auch noch unter Windows XP und Windows Server 2003 werden Treiber im Kernelmodus betrieben, arbeiten also im gleichen Bereich des Arbeitsspeichers wie der Kern des Betriebssystems. Schreibt ein Treiber durch Programmierfehler in einen Arbeitsspeicherbereich, in dem sich bereits Daten eines anderen Treibers oder sogar des Systems befinden, werden diese Daten überschrieben. Das Betriebssystem weiß jedoch nichts von diesem Vorgang und findet beim Versuch, auf seine Daten zuzugreifen, nicht mehr den erwarteten Inhalt vor. Aus diesem Grund stellt Windows sofort seinen Betrieb ein und meldet den Fehler dann als Bluescreen. Würde das System nicht so vorgehen, könnten durch die ungültigen Bereiche im Arbeitsspeicher Daten zerstört oder im Falle von Hardware-Treibern sogar die Hardware eines Computers in Mitleidenschaft gezogen werden. Solche Kernelzugriffe von Treibern hat Microsoft in Windows 2000 Server und Windows Server 2003 verringert und mit Windows Vista sowie Windows Server 2008 nahezu abgeschafft, sodass Bluescreens in diesem Bereich eher selten auftreten. Verliert ein Teil des Arbeitsspeichers durch einen physischen Defekt jedoch Daten, kann auch unter Windows Vista oder Windows Server 2008 ein Bluescreen erscheinen. Übrigens: Bluescreens gibt es auch unter UNIX oder Linux, werden hier aber als »Kernel Panic« bezeichnet. Auch bei diesen Betriebssystemen haben die gleichen Umstände Schuld am Absturz.

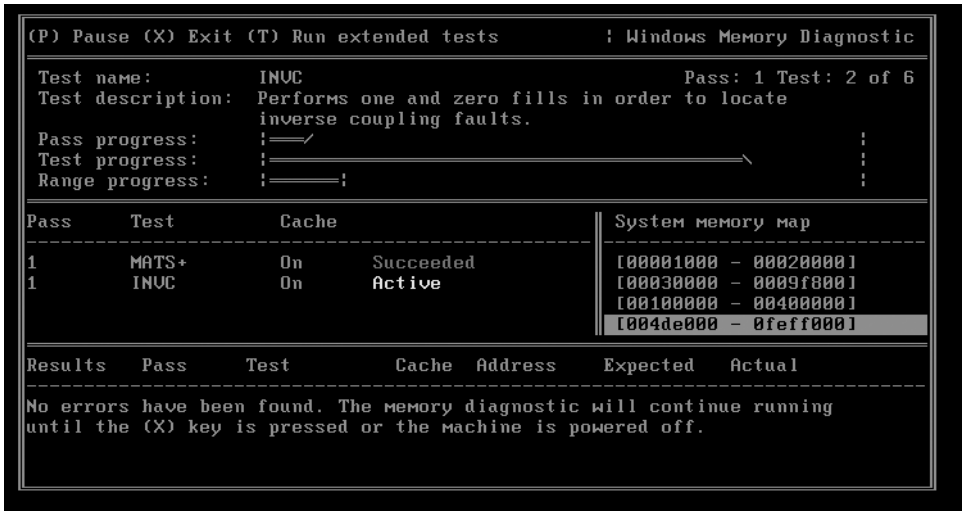
Eine häufige Ursache für Bluescreens sind überhitzte CPUs. Der Prozessor kann bei mangelnder Kühlung durch einen verschmutzten oder defekten Prozessorlüfter zu heiß werden, Übertaktung kann den Effekt noch verstärken. Haben Sie Ihren Server übertaktet und erhalten seitdem regelmäßig Bluescreens, kann sich eine Prüfung der CPU-Temperatur lohnen, zum Beispiel durch Zusatztools wie SpeedFan (*http://www.almico.com/speedfan.php*). Viele Hauptplatinen lösen in solchen Fällen Bluescreens in Windows selbst aus. Auch hier ist also nicht Windows schuld, sondern es handelt sich um eine simple Fehlervermeidungsmaßnahme. Würde kein Bluescreen erscheinen und die CPU immer heißer werden, wäre es nur eine Frage der Zeit, bis die CPU endgültig defekt ist. Übertaktete Intel-CPUs verwenden oft auch einen höheren Frontside Bus (FSB), über den Chipsatz und Arbeitsspeicher angesprochen werden. Auch hier können Bluescreens auftreten, wenn die Hardware mit dem eingestellten Takt nicht zurechtkommt. Abhilfe schafft hier die Absenkung des FSB-Taktes. Ein gutes Tool dazu ist CPU-Z von der Seite *http://www.cpu-z.de*.

Arbeitsspeicher-Diagnose

Treten auf Ihren Computer häufig Bluescreens auf, obwohl Sie nur aktuelle und offizielle Treiber einsetzen und das System nicht übertaktet haben, liegt dies wahrscheinlich am RAM. In diesem Fall können Sie den Arbeitsspeicher mit Testprogrammen überprüfen. Unter Windows Vista und Windows Server 2008 gibt es dazu das Windows-Speicherdiagnose-Tool, das Sie über den Befehl *mdsched.exe* im Suchfeld des Startmenüs aufrufen. Für die Diagnose wird der Computer neu gestartet und der Speicher in einer eigenen Umgebung getestet. Anschließend startet Windows erneut und meldet, ob Bereiche des Speichers defekt sind. Für andere Windows-Versionen oder ausführlichere Tests hilft *Windows Memory Diagnostic*, das von der Seite *http://oca.microsoft.com/de/windiag.asp* heruntergeladen werden kann. Das Tool erstellt eine Boot-Diskette oder eine bootfähige CD, von der Sie starten und dann den Arbeitsspeicher ausführlich testen lassen können. Der Standardtest läuft zweimal durch, was etwa eine halbe Stunde dauert. Drücken Sie während des Testlaufs die Taste T, startet ein erweiterter Testlauf. Dieser prüft das RAM noch gründlicher, läuft dafür aber auch ein paar Stunden. Meldet das Programm keinen Fehler im RAM, können Sie nahezu sicher

sein, dass der Bluescreen nicht durch den Arbeitsspeicher verursacht wurde. Findet die Software hingegen Fehler, erscheint eine entsprechende Meldung. Mithilfe dieser Meldung erfahren Sie, welcher Speicherriegel defekt ist und ausgetauscht werden muss. Eine Alternative für den Test des Arbeitsspeichers ist das Entfernen des betreffenden Speicherriegels. Läuft der Computer anschließend problemlos, ist der jeweilige Riegel oder die Bank auf der Hauptplatine defekt. Funktioniert der Rechner auch dann noch, wenn ein funktionsfähiger RAM-Riegel in die ursprüngliche Speicherbank gesteckt wurde, ist der entfernte Arbeitsspeicher höchstwahrscheinlich schuld am Absturz. Stürzt der Computer weiterhin ab, tauschen Sie die Riegel erneut. Hilft diese Vorgehensweise nicht, ist zwar das Problem nicht gelöst, allerdings können Sie dann sicher sein, dass es nicht am Arbeitsspeicher liegt, sondern vermutlich an einer defekten Speicherbank.

Abbildg. 21.18 Mit einer Arbeitsspeicherdiagnose defekten RAM-Riegeln auf der Spur



Bluescreens vs. Blackscreens

Die schwarzen Blackscreens tauchen auf, bevor das Betriebssystem ordnungsgemäß gestartet wurde und verhindern, dass der Bootvorgang fortgesetzt wird. Diese Screens äußern sich darin, dass – wie bei Bluescreens – Fehler gemeldet werden oder der Bildschirm komplett schwarz bleibt. Der hauptsächliche Unterschied zwischen Black- und Bluescreens ist, dass die blaue Version im laufenden Betrieb auftritt, das Betriebssystem also starten, aber nicht stabil laufen kann. Blackscreens deuten darauf hin, dass eventuell bereits während des Rechnerstarts in der BIOS-Phase Probleme bestehen. Nach dieser kommt die Boot-Phase, in welcher der Computer versucht, ein Betriebssystem zu finden und dieses zu starten.

Blackscreens beheben

Treten Fehler in einer dieser zwei Phasen auf, ist der Fehler meist leicht zu finden. Bei BIOS-Problemen werden Meldungen angezeigt oder Sie hören bestimmte Töne, die auf defekte Hardware schließen lassen. Das Mainboard-Handbuch hilft bei der Interpretation dieser Fehlercodes und verrät Ihnen so, welche Komponente das Problem verursacht. In der Boot-Phase hingegen erscheinen hauptsächlich Meldungen, wenn das Betriebssystem nicht gefunden werden kann, zum Beispiel,

wenn eine Diskette im Laufwerk liegt und die Bootreihenfolge so eingestellt ist, dass von dieser gebootet wird. Auch wenn wichtige Startdateien von Windows nicht gefunden werden können, schlägt der Bootvorgang fehl. Solche Fehler können ohne weiteres auch unter Windows Vista und Windows Server 2008 auftreten. Fehlerbehebungen in diesem Fall sind recht einfach: Bei BIOS-Problemen muss die entsprechende Hardware getauscht oder ein eventueller Einbaufehler korrigiert werden. Fehler in der BIOS-Phase kommen häufig nach Hardware-Änderungen oder -Einbauten vor und lassen schlimmstenfalls auf eine defekte Hauptplatine schließen. Beepcodes sind dann zu hören, wenn der Computer noch nicht mal anfangen kann zu starten. Dies liegt häufig an fehlerhaften oder falsch eingebauten Arbeitsspeicher-Riegeln. Erscheint nach dem Bootvorgang eine Fehlermeldung, die auf Probleme mit der Festplatte schließen lässt, wurde diese vom System nicht erkannt – im Falle älterer PATA-Platten ist oft eine falsche Jumperung die Ursache. Bei Problemen in der Boot-Phase müssen Sie den ursprünglichen Zustand des Betriebssystems wiederherstellen.

Wurden beim Starten des Computers die BIOS- sowie die Boot-Phase fehlerfrei bewältigt, lädt das Betriebssystem seine Treiber und die Benutzeroberfläche. Diese Phase wird auch als Kernelphase bezeichnet. Hier auftretende Blue- oder Blackscreens lassen sich wesentlich schwerer beheben. Meistens liegt in diesem Fall ein Problem mit einem Treiber vor. Haben Sie vor dem letzten Bootvorgang einen neuen Treiber installiert und erscheint jetzt ein Blue- oder Blackscreen, ist wahrscheinlich dieser neue Treiber schuld. In diesem Fall ist die beste Wahl zur Fehlerbehebung, beim Booten des Computers die Taste F8 zu drücken. Anschließend erscheint das Boot-Menü von Windows. Über die Option *Letzte als funktionierend bekannte Konfiguration* werden alle Änderungen seit dem letzten Start des Betriebssystems rückgängig gemacht und der alte Treiber wieder geladen. Diese Option funktioniert aber nur dann, wenn der letzte Betriebssystemstart funktioniert hat und erst der neue Treiber das System mit einem Blue- oder Blackscreen zum Absturz bringt.

Treten in unregelmäßigen Abständen Bluescreens auf und haben Sie Ihren Arbeitsspeicher getestet, sind häufig fehlerhafte Treiber schuld (wie schon ausführlich erläutert). Hier hilft oft ein Rundumschlag, also die Aktualisierung aller wichtigen Systemtreiber. Suchen Sie für die wichtigsten Komponenten wie Chipsatz, Grafikkarte, Soundkarte usw. die aktuellen Treiber und installieren Sie diese. Führen Sie ein Windows-Update durch, damit die aktuellsten Patches installiert sind. Überprüfen Sie im Geräte-Manager, ob unbekannte oder deaktivierte Geräte angezeigt werden und stellen Sie sicher, dass für diese Komponenten Treiber installiert werden. Entfernen Sie unnötige Geräte vom Computer, bis Sie sicher sind, an welchem Gerät der Fehler liegt.

Versteckte Treiber finden und entfernen

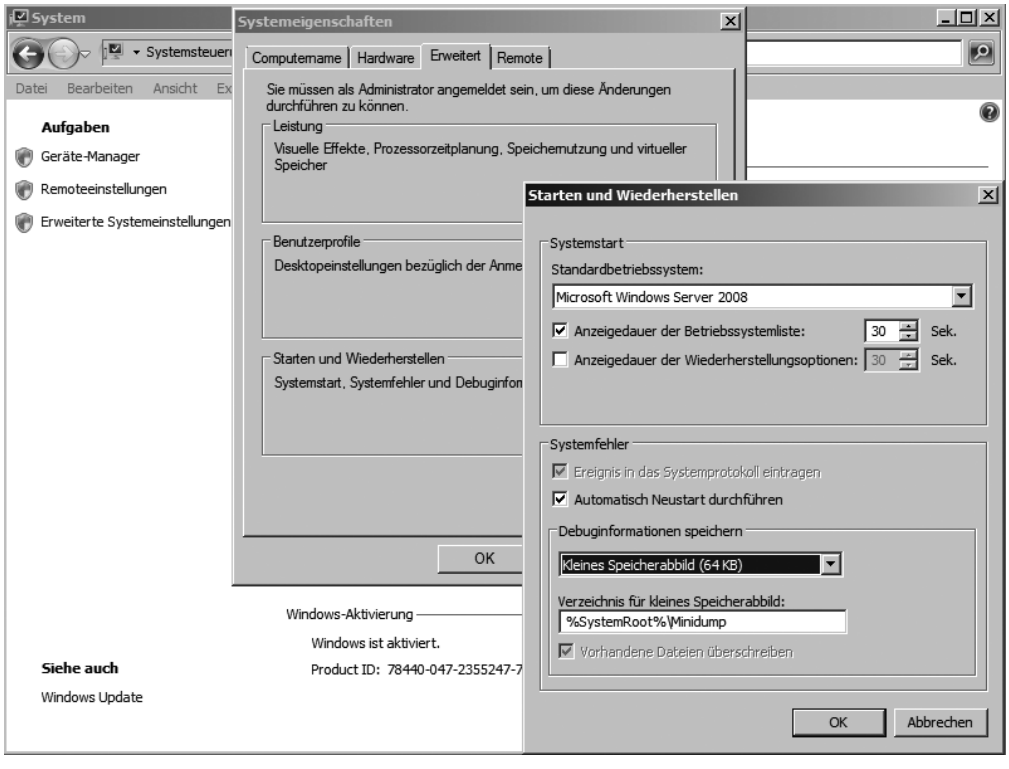
Über den Menübefehl *Ansicht/Ausgeblendete Geräte anzeigen* im Geräte-Manager lassen sich Komponenten anzeigen, deren Treiber zwar installiert wurden, aber nicht mehr benötigt werden. So besteht die Möglichkeit, veraltete Gerätetreiber vom Computer zu entfernen, da diese das System unnötig belasten und eventuell ebenfalls für Bluescreens verantwortlich sind. Wenn Sie den Menübefehl auswählen, werden allerdings nur jene Systemkomponenten angezeigt, die Windows zum Schutz des Systems vor dem Anwender versteckt. Damit auch jene Geräte angezeigt werden, die im System installiert wurden, aber nicht mehr vorhanden sind, müssen Sie den Geräte-Manager über einen speziellen Weg aufrufen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie die Eingabeaufforderung.
2. Tippen Sie den Befehl *set devmgr_show_nonpresent_devices=1* ein.
3. Starten Sie über den Befehl *start devmgmt.msc* den Geräte-Manager.
4. Rufen Sie den Menübefehl *Ansicht/Ausgeblendete Geräte anzeigen* auf. Sofern ältere Treiber auf dem PC vorhanden sind, werden diese jetzt angezeigt. Im Anschluss können Sie nach den nicht mehr benötigten Geräten suchen und diese entfernen.

Windows-Einstellungen für Bluescreens

Windows Server 2008 ist standardmäßig so eingestellt, dass nach einem Bluescreen automatisch der Rechner neu gestartet wird. Das hat zwar den Vorteil, dass der Server dann recht schnell wieder zur Verfügung steht. Allerdings kann in diesem Fall auch die entsprechende Fehlermeldung nicht gelesen werden. Erscheint der Bluescreen nach jedem Start, verfängt sich der Computer in einer Schleife, da nach jedem Bluescreen erneut gestartet wird. Die möglichen Einstellungen, wie sich Windows nach einem Bluescreen verhalten soll, finden Sie unter *Start/Systemsteuerung/System und Wartung/System/Erweiterte Systemeinstellungen*. Klicken Sie im Bereich *Starten und Wiederherstellen* auf die Schaltfläche *Einstellungen*. Über den Bereich *Systemfehler* lassen sich die Einstellungen vornehmen. Zunächst sollten Sie das Häkchen *Automatisch Neustart durchführen* deaktivieren. Im Bereich *Debuginformationen* wählen Sie über das Dropdownmenü aus, welche Art der Informationen protokolliert werden soll. Am besten ist die Variante *Kleines Speicherabbild* geeignet, da andere Informationen ohnehin eher verwirrend sind. Die hier protokollierten Informationen können übrigens mit den *Microsoft Debugging Tools* ausgelesen werden, die wir im nächsten Abschnitt besprechen. Hier legen Sie auch fest, in welchem Verzeichnis das Speicherabbild mit dem Fehler abgelegt werden soll.

Abbildg. 21.19 Windows Server 2008 für das Verhalten bei Bluescreens konfigurieren



Den Fehlern bei Bluescreens mit Zusatztools auf der Spur

Helfen die beschriebenen Wege nicht, um Bluescreens auf Ihrem System zu vermeiden, hilft entweder die komplette Neuinstallation des Betriebssystems oder zusätzliche Test-Software. Wie der Arbeitsspeicher getestet wird, haben wir bereits beschrieben. In den folgenden Abschnitten gehen wir auf weitere Freeware-Tools ein, die für die Systemdiagnose bei Bluescreens wertvolle Hilfe leisten.

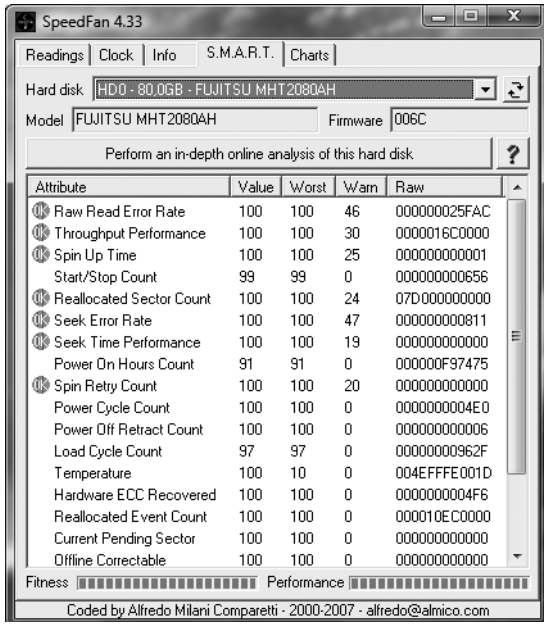
SpeedFan und Prime 95

Ein wichtiger Helfer bei der Suche nach der Ursache von Bluescreens ist SpeedFan. Nach der Installation des Tools wird die Temperatur der CPU angezeigt. Vor allem bei übertakteten Systemen bietet das Tool eine unersetzliche Hilfestellung bei der Überwachung der Prozessortemperatur.

Ebenfalls interessant ist die Registerkarte *S.M.A.R.T* des Tools. Hier werden Fehler der Festplatten angezeigt, wenn diese die SMART-Technologie (Self Monitoring Analysis And Reporting Technology) unterstützen und Sie diese Funktion im BIOS aktiviert haben. Hier sollten keinerlei Fehler gemeldet werden, ansonsten können Sie davon ausgehen, dass Ihre Festplatte defekt ist. Neben Fehlern erhalten Sie auf dieser Registerkarte ausführliche Informationen über die Leistung und den physischen Zustand der Festplatte.

Mit der Freeware Prime 95 (*http://www.mersenne.org/freesoft.htm*) wird die CPU unter Last gesetzt und damit überprüft. Auch dieses Tool ist bei übertakteter CPU ein notwendiges Werkzeug, um die Stabilität des Computers zu prüfen und so Bluescreens zu vermeiden.

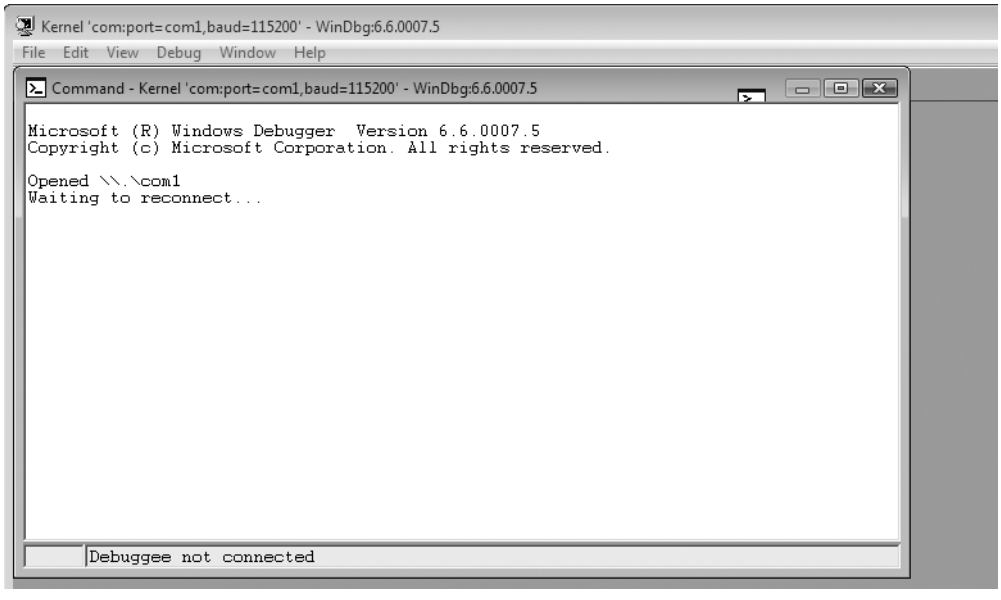
Abbildg. 21.20 Die Freeware *SpeedFan* kann neben der Temperatur auch die SMART-Informationen der Festplatten auslesen



Microsoft Debugging Tools

Mit der Freeware *Microsoft Debugging Tools* (*http://www.microsoft.com/whdc/devtools/debugging*) werden die Meldungen von Bluescreens verständlich aufbereitet. Das Tool analysiert die Protokolldatei, die beim Auftreten des Bluescreens erzeugt worden ist. Der Inhalt lässt Rückschlüsse auf den Ursprung des Fehlers zu. Achten Sie aber darauf, dass solche Protokolldateien nur dann erzeugt werden, wenn für das Laufwerk C: die Auslagerungsdatei aktiviert ist. Haben Sie die Auslagerungsdatei auf ein anderes Laufwerk verschoben, werden solche Dateien nicht erstellt. Das Tool steht auch für 64-Bit-Systeme zur Verfügung. Nach der Installation starten Sie das Programm zur Analyse über *Start/Programme/Debugging Tools für Windows/WinDbg*. Über das Menü *File/Symbol File Path* tragen Sie am besten noch den Befehl *SRV*c:\websymbols*http://msdl.microsoft.com/download/symbols* ein. Dieser bewirkt, dass das Programm automatisch notwendige Ressourcen aus dem Internet in den Ordner *C:\Websymbols* herunterlädt, wenn diese für die Analyse benötigt werden. Eine ausführliche Anleitung zur Bluescreen-Analyse finden Sie auf der Seite *http://www.microsoft.com/whdc/devtools/debugging/debugstart.mspx*.

Abbildg. 21.21 Bluescreen-Analyse mit den Microsoft Debugging Tools



Öffnen Sie eine Dumpdatei, also das Protokoll des Bluescreens, wird ein Fenster mit zwei Bereichen geöffnet: *Command* und *Disassembly*. Den meisten Anwendern reichen die Informationen unter *Command*. Die Daten unter *Disassembly* sind hauptsächlich für Programmierer gedacht, die Fehler in eigenen Anwendungen oder Treibern suchen. Interessant ist der Bereich *Bugcheck Analysis*. Hier wird ein Fehlercode angezeigt, der auch sehr gut für die Recherche im Internet geeignet ist. Auch in der Microsoft Knowledge Base unter *http://support.microsoft.com* finden Sie oft ausführliche Hinweise. Verwenden Sie in der Knowledge Base übrigens am besten immer die englischen Artikel. Durch die Eingabe des Befehls *!analyze –v* im *Command*-Fenster werden weitere Informationen angezeigt, die ebenfalls der Recherche dienen. In der Zeile *Probably caused by* wird die Datei angezeigt, die vermutlich den Fehler verursacht hat. Zusammen mit den anderen Informationen ist auch diese Information für die Suche im Internet sehr hilfreich. Über den Befehl *lm v m<Dateiname>*

erhalten Sie weitere Infos. Geben Sie den Dateinamen ohne Endung und direkt hinter *m* an, ohne Leerzeichen. Wird eine bestimmte Datei gemeldet, weist diese auf den entsprechenden Treiber hin. Geben Sie den Namen der Datei gefolgt vom Begriff *Bluescreen* in eine Suchmaschine ein.

Zusammenfassung

Auch wenn die interne Datensicherung von Windows Server 2008 selten für die Sicherung von produktiven Daten verwendet wird, bietet diese Funktion zahlreiche Möglichkeiten. In Windows Server 2008 ist es jetzt noch einfacher, einen kompletten Server zu sichern und diesen wiederherzustellen. Auch die Oberfläche der Sicherung sowie deren Funktionen wurden überarbeitet. Im nächsten Kapitel zeigen wir Ihnen, wie Sie die SharePoint Services 3.0 mit SP1 in einem Windows Server 2008-Netzwerk zum Informationsaustausch betreiben.

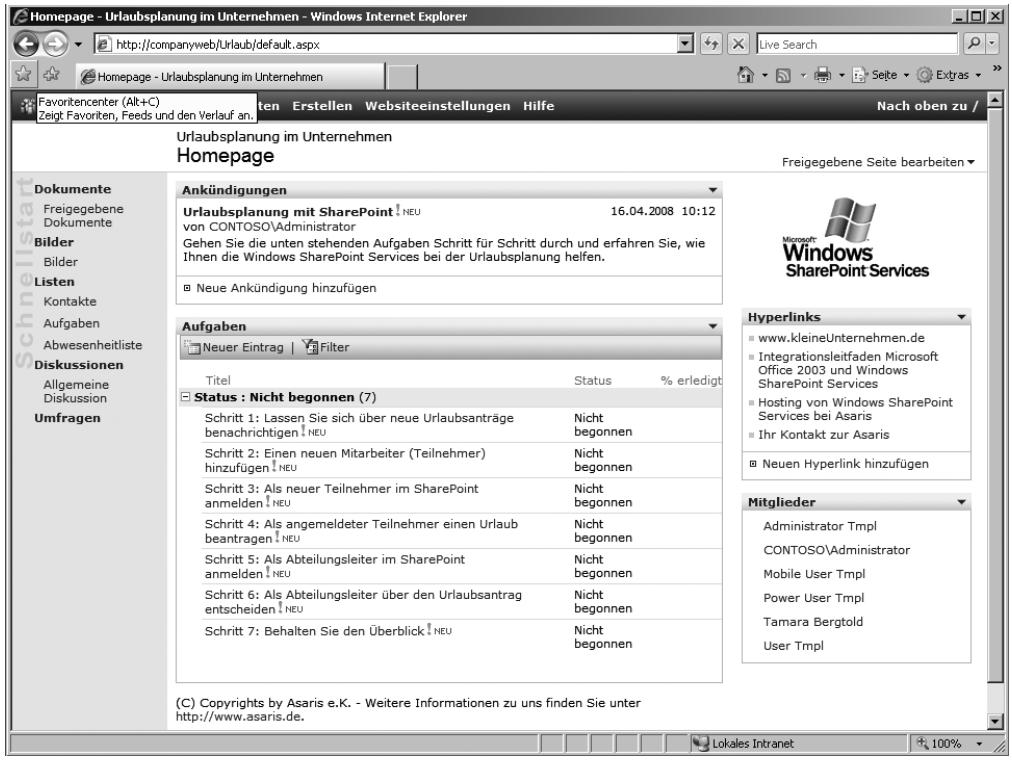
Kapitel 22

Windows SharePoint Services 3.0 mit SP1

In diesem Kapitel:

Um effizient Informationen in Unternehmen auszutauschen, reicht selbst ein E-Mail-System wie Exchange mit all seinen Möglichkeiten heutzutage nicht mehr aus. Auch Dateiserver allein sind nicht mehr optimal, um Daten und Informationen innerhalb von Unternehmen zur Verfügung zu stellen. Microsoft bietet in diesem Bereich für Unternehmen weitere Lösungen an. Die erste Lösung sind die SharePoint Services 3.0, die auch für Windows Server 2008 kostenlos zur Verfügung gestellt werden. Diese erweitern Windows Server 2008 um ein vollwertiges Intranet und ein Dokumentenmanagementsystem mit Gruppenfunktionalität. Mit den SharePoint Services lässt sich in kurzer Zeit ein voll funktionsfähiges Intranet zusammenstellen, an dem Ihre Mitarbeiter interaktiv teilnehmen können.

Abbildg. 22.1 Die Startseite der Windows SharePoint Services



HINWEIS Erst mit dem Service Pack 1 sind die Windows SharePoint Services 3.0 kompatibel mit Windows Server 2008. Die Installationsdatei für Windows SharePoint Services 3.0 mit SP1 kann bei Microsoft heruntergeladen werden. Suchen Sie am besten mit einer Suchmaschine nach dem Begriff »SharePoint Services 3.0 SP1«. Laden Sie sich aber nicht nur das 30 MB große Service Pack herunter, sondern die Installationsdatei, die bereits das SP1 enthält. Diese hat etwa eine Größe von 104 MB. Alternativ verwenden Sie den Link *http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=ef93e453-75f1-45df-8c6f-4565e8549c2a*.

Einführung in Windows SharePoint Services 3.0

In diesem Kapitel erfahren Sie, wie Sie SharePoint Services installieren, bedienen und erweitern können. Die aktuellen Office-Varianten unterstützen die Speicherung direkt in die SharePoint Services, ohne dabei den Umweg über Speichern und anschließendes Upload zu gehen.

Abbildg. 22.2 Verwenden von Dokumentenbibliotheken in SharePoint Services 3.0

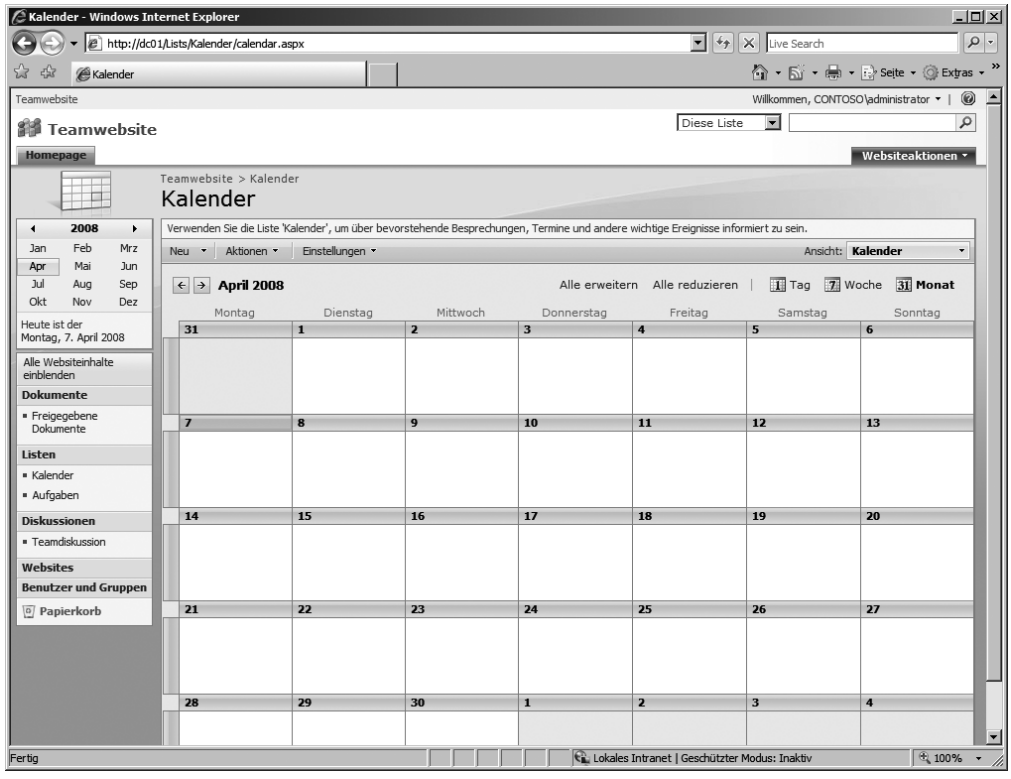
Die SharePoint Services sind für alle Nutzer schnell und einfach zu bedienen. Eine Schulung ist nicht notwendig. Eine kleine Einweisung genügt, um die Anwender in den Umgang mit den SharePoint Services einzuführen. Die SharePoint Services sind der kleine Bruder des kostenpflichtigen Share Point Servers. SharePoint umfasst zahlreiche Funktionen, die eingebunden werden können. Sie müssen nicht alle Funktionen nutzen, sondern können auch nur Teile der Funktionalitäten verwenden:

- **Dokument- und Bildbibliotheken** Zunächst können in den Windows SharePoint Services (WSS) Dokumenten-Bibliotheken angelegt werden. Anwender können Dokumente aller Art, auch Bilder, hochladen oder direkt aus den Microsoft Office-Anwendungen in den WSS speichern. Es gibt eine Versionierung, die Sie für einzelne Bibliotheken aktivieren können. Durch diese Versionierung werden Dokumente nicht überschrieben, sondern immer als neue Version veröffentlicht. Diese Bibliotheken können so konfiguriert werden, dass Mitarbeiter einzelne Dokumente erst auschecken müssen. Bei diesem Vorgang können mehrere Mitarbeiter eines Teams am gleichen Dokument arbeiten,

aber nur einer der Mitarbeiter kann schreibend auf das Dokument zugreifen. Dadurch wird verhindert, dass Teams ihre Dokumente gegenseitig überschreiben (Abbildung 22.3).

- **Listen und Diskussionen** Eine weitere Funktion ist die Möglichkeit, Listen zu erstellen, die ähnlich wie Newsgroups oder Diskussionsforen funktionieren. Sie können Gruppenkalender erstellen und Kalender aus Outlook importieren. Durch Listen können Sie ein schwarzes Brett betreiben, das bestimmte Anwender pflegen können. Auch einen Helpdesk oder eine Knowledge Base können Sie so leicht integrieren.

Abbildg. 22.3 WSS unterstützen auch Listen und Gruppenkalender



Bei herkömmlichen Intranets bleibt die Pflege entweder an Powerusern über FrontPage oder Expression Web hängen oder an der Systemadministration. Dadurch, dass alle Benutzer am Intranet mitarbeiten können, besteht die Möglichkeit, über eine ordentliche Berechtigungsstruktur das Wissen im Unternehmen schnell und effizient zur Verfügung zu stellen. Die Änderung der Ansicht erfolgt wie beim Windows-Explorer. Jeder kann Dokumente oder Bilder einzelnen Seiten hinzufügen. Anwender können Dokumente direkt aus Office auf der entsprechenden Teamseite ablegen oder ein Dokument hochladen und Dokumente auschecken und dadurch für andere als nicht überschreibbar markieren, bis diese wieder eingecheckt sind. Diese Funktion der SharePoint Services kommt ursprünglich aus der Programmierung. Durch das Auschecken eines Dokuments kann ein Mitarbeiter verhindern, dass Kollegen das gleiche Dokument zur selben Zeit bearbeiten. Erst nachdem das Dokument wieder eingecheckt wurde, können andere Mitarbeiter erneut schreibend darauf zugreifen. Vor allem bei großen Dokumenten und ausführlichen Excel-Tabellen kann diese Funktion durchaus nützlich sein, um zu

verhindern, dass die Arbeit ganzer Arbeitstage verloren geht, weil mehrere Mitarbeiter das gleiche Dokument bearbeiten und gleichzeitig speichern. Administratoren oder Benutzer mit bestimmten Rechten können das Einchecken eines Dokuments durchführen, wenn der Mitarbeiter, der das Dokument ausgecheckt hat, längere Zeit nicht im Büro ist.

Anwender können direkt aus einer Dokumentbibliothek ein neues Dokument erstellen, welches beim Speichern automatisch in den SharePoint Services gespeichert wird, ohne dass der Anwender in seinem Office-Programm besondere Einstellungen vornehmen muss. Er muss einfach auf die Schaltfläche *Neues Dokument* klicken (Abbildung 22.4).

Abbildg. 22.4 Dokumente lassen sich direkt über das Intranet erstellen

Sie können für einzelne Seiten Benachrichtigungen aktivieren und erhalten per E-Mail detaillierte Informationen, wenn Dokumente innerhalb der konfigurierten Bibliothek hinzugefügt oder geändert wurden. Viele Informationen in den SharePoint Services können importiert oder exportiert werden. Sie können Tabellen nach Excel exportieren und daraus importieren, sowie Kontakte und Kalender mit Outlook austauschen. Benutzer können auch selbst Benachrichtigungen auf einzelnen Webseiten konfigurieren. Wenn sich in einem Bereich etwas ändert, also ein neues Dokument hinzugefügt, ein altes bearbeitet oder gelöscht wird, erhält der Benutzer durch den E-Mail-Server eine Benachrichtigung zugestellt. Innerhalb einer Teamseite kann ein Team beliebig viele eigene Unterwebseiten erstellen und Berechtigungen verwalten, um das Dokumentenmanagement an die eigenen Bedürfnisse anzupassen. Bei der Verwendung eines SQL-Servers können die Dokumente indexiert werden und Anwender innerhalb der SharePoint Services schnelle Volltextsuchen durchführen. Für Dokumentbibliotheken können auch Inhaltsgenehmigungen konfiguriert werden. Wenn ein Mitarbeiter ein neues Dokument erstellt, wird es erst angezeigt, nachdem zum Beispiel der Abteilungsleiter den Inhalt genehmigt hat.

Wenn Sie sich ein wenig mit dem Layout der SharePoint Services beschäftigen, werden Sie bald feststellen, dass Sie schnell und einfach das Layout an die Bedürfnisse Ihres Unternehmens anpassen können. Mit wenigen Mausklicks lassen sich Logos einbinden, Farben ändern und das Aussehen der obersten Webseite durch die so genannten Webparts anpassen. Ebenso können in den SharePoint Services externe Daten eingeblendet werden, zum Beispiel Newsfeeds aus dem Internet für bestimmte Bereiche. Es ist möglich, Informationen aus Datenbanken, zum Beispiel ERP- oder CRM-Systemen, auszulesen und in den SharePoint Services anzuzeigen. Auf der Microsoft-Website unter *http://office.microsoft.com/de-de/FX011204871031.aspx* finden Sie ausführliche Informationen und können Dutzende kostenlose Webparts zur Integration in die SharePoint Services herunterladen. Kostenpflichtige Webparts werden von Dienstleistern angeboten. Mit den Webparts soll erreicht werden, dass die SharePoint Services immer mehr zur Zentrale der täglichen Arbeit werden.

Neuerungen der SharePoint Services 3.0

Wesentliche Neuerungen in den SharePoint Services 3.0 im Vergleich zu den Vorgängerversionen sind ein Papierkorb, über den gelöschte Objekte wiederhergestellt werden, und die Interaktion mit den aktuellen Office 2007-Produkten. Mit den SharePoint Services 3.0 können außerdem Wiki-Bibliotheken erstellt werden, also Wissens-Datenbanken ähnlich wie Wikipeda. Außerdem unterstützt die neue Version auch Blog-Arbeitsbereiche sowie RSS-Feeds. Mit Outlook 2007 können Benutzer Informationen gemeinsam nutzen und im Team an Aufgaben und Projekten arbeiten. Dadurch haben die Anwender Zugriff auf verschiedene Bereiche für die Zusammenarbeit in Windows SharePoint Services 3.0, mit deren Hilfe sie Diskussionen beginnen, Kalender freigeben, gemeinsame Kontaktlisten aktualisieren und bei gemeinsam verfassten Dokumenten Versionsüberprüfungen durchführen können. Kalenderinhalte können leichter und schneller freigegeben werden. Durch die Integration von Features aus Outlook und Windows SharePoint Services wird das Senden eines Projektzeitplans an Mitarbeiter so einfach wie das Erstellen einer neuen E-Mail-Nachricht. Empfänger können bei der empfangenen Freigabenachricht auf die neue, in der Nachricht enthaltene Schaltfläche *Diesen Kalender öffnen* klicken. Das Freigabenachrichtfeature kann auch mit anderen Arten von SharePoint-Listen und -Bibliotheken verwendet werden, zum Beispiel mit Kontakt-, Aufgaben- und Diskussionslisten.

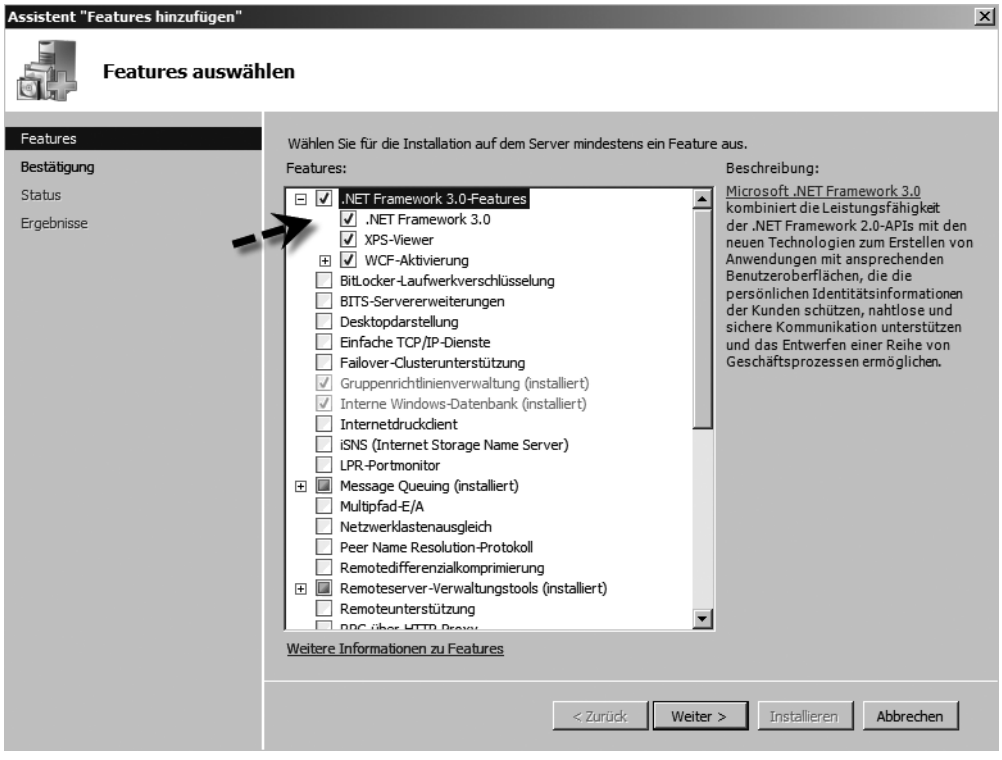
Installation der SharePoint Services 3.0 mit SP1

In diesem Abschnitt gehen wir auf die Installation und Ersteinrichtung der SharePoint Services ein. Vor der Installation laden Sie sich die Installationsdatei, die bereits das SP1 enthält, von der Microsoft-Internetseite herunter.

Installation von .NET Framework 3.0

Bevor Sie die SharePoint Services installieren können, müssen Sie auf dem Server zunächst das .NET Framework 3.0 installieren. Dazu installieren Sie über den Server-Manager die .NET Framework 3.0-Features mit den untergeordneten Funktionen (Abbildung 22.5).

Abbildg. 22.5 Installieren von .NET Framework 3.0



Sie müssen den Server nach der Installation nicht neu starten, sondern können sofort mit der Installation der SharePoint Services fortfahren.

Durchführen der Installation der SharePoint Services 3.0 mit SP1

Nachdem .NET Framework installiert worden ist, können Sie sich an die Installation der SharePoint Services 3.0 machen. Nachdem Sie die Datei – wie oben erläutert – heruntergeladen haben, klicken Sie doppelt auf die Installationsdatei. Bestätigen Sie im ersten Fenster die Lizenzbestimmungen. Als Nächstes kann ausgewählt werden, ob die Standardinstallation oder die erweiterte Installation durchgeführt werden soll.

Bei der Entscheidung für die erweiterte Installation stehen mehr Möglichkeiten zur Konfiguration zur Verfügung: So müssen auf der nächsten Seite verschiedene Einstellungen zur Installation vorgenommen werden. Hier stehen verschiedene Registerkarten zur Verfügung. Auf der Registerkarte *Servertyp* belassen Sie die standardmäßig eingestellte Option *Eigenständig*, da dies für die meisten Installationen ausreicht. Auf der Registerkarte *Datenspeicherort* legen Sie fest, wo die Dateien des Suchindexes gespeichert werden. Klicken Sie auf *Jetzt installieren*. Anschließend beginnt die Installation der SharePoint Services 3.0.

Lassen Sie die Installation abschließen. Sie können entweder den Assistent zur Einrichtung sofort starten lassen, oder nachträglich manuell. Bevor die SharePoint Services genutzt werden können, wird der Assistent auf jeden Fall benötigt.

Abbildg. 22.6 Windows SharePoint Services 3.0 installieren

Über *Start/Verwaltung/Konfigurations-Assistent für SharePoint-Produkte und -Technologien* wird das Verwaltungsprogramm gestartet, falls der Aufruf des Konfigurations-Assistenten nach der Installation nicht automatisch erfolgt. Achten Sie darauf, dass während dieser Vorgänge auch die Internetinformationsdienste beendet werden. Während des Zeitraums der Einrichtung stehen daher auch andere Webdienste auf dem Server nicht zur Verfügung. Nachdem Sie das Startfenster des Einrichtungsassistenten bestätigt haben, beginnt das Programm zunächst automatisch mit der Einrichtung der Konfigurationsdatenbank und legt Einstellungen für die SharePoint Services fest.

Abbildg. 22.7 Der Konfigurations-Assistent für die SharePoint Services richtet den Server ein

Nachdem der Assistent abgeschlossen hat, wird automatisch die neue Webseite der SharePoint Services 3.0 gestartet.

ACHTUNG Die SharePoint-Website wird als ganz neue Website in der IIS-Verwaltung angelegt. Da die SharePoint-Seite auf den gleichen Port hört, wie die Standard-Website, wird diese deaktiviert. Befinden sich unterhalb der Standard-Website aber Webseiten, die im Unternehmen benötigt werden, müssen Änderungen in der SharePoint-Konfiguration vorgenommen werden.

SharePoint Services parallel zu anderen Webseiten betreiben

In diesem Abschnitt erläutern wir die Erstellung einer neuen Webseite für die SharePoint Services, die einen anderen Port verwendet, als die Default Web Site von Windows Server 2008:

1. Starten Sie die Zentralverwaltung der SharePoint Services über *Start/Verwaltung/SharePoint 3.0-Zentraladministration*. Aktivieren Sie die Registerkarte *Anwendungsverwaltung*. Die Zentralverwaltung ist ebenfalls webbasiert. Hier können Sie die wichtigsten Einstellungen für die SharePoint Services vornehmen. Die neue Zentraladministration ermöglicht eine bessere Verwaltung der SharePoint Services. So sind die Links für die wichtigsten Administrationsaufgaben bereits auf der Startseite erreichbar. Klicken Sie auf eine solche Administrationsaufgabe, öffnet sich ein Fenster, in dem Sie die entsprechende Tätigkeit durchführen können. Die neue Zentraladministration zeigt für alle beteiligten Server an, welche Dienste gestartet sind, um einen besseren Überblick zu bieten. Die Verwaltung der Berechtigungen wurde an vielen Stellen angepasst. Domänen-Administratoren haben nicht mehr unbedingt Berechtigungen, die SharePoint Services zu verwalten, sondern müssen explizit berechtigt werden. Auch die Delegation von Berechtigungen wurde verbessert. Die Berechtigungen für IIS sowie das Starten und Stoppen der Dienste kann jetzt direkt in der Zentraladministration vorgenommen werden. Sie können die Zentralverwaltung von jedem Arbeitsplatz im Netzwerk aus starten.

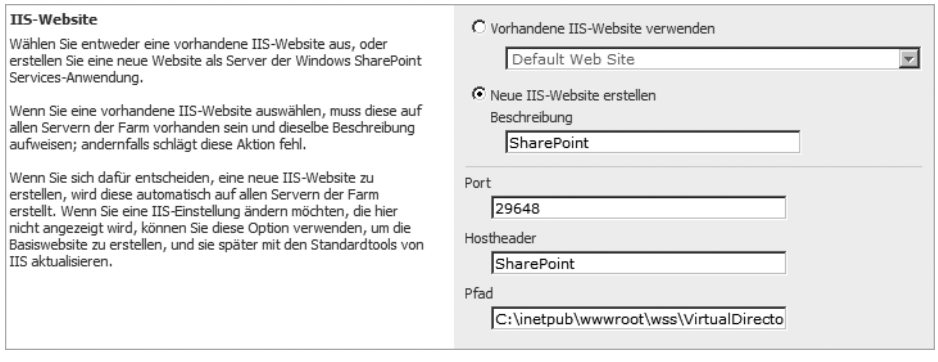
Abbildg. 22.8 Aufrufen der Anwendungsverwaltung der WSS 3.0

2. Klicken Sie im Bereich *Verwaltung von SharePoint Web-Anwendungen* auf den Link *Webanwendung erstellen oder erweitern*.

Abbildg. 22.9 Erstellen einer neuen Webanwendung

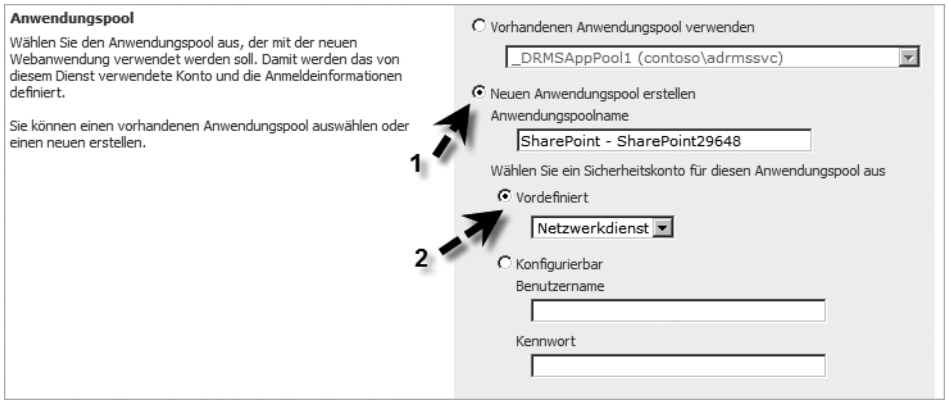
3. Klicken Sie anschließend auf den Link *Neue Webanwendung erstellen*.
4. Auf der folgenden Seite müssen verschiedene Einstellungen vorgenommen werden. Zunächst können Sie eine Beschreibung für die Webseite festlegen oder die Standardbeschreibung übernehmen. Außerdem legen Sie den Port fest, auf den diese Webseite hört. Verwenden Sie aber keinesfalls die Standardports des Servers (8080, 80, 443), sondern am besten einen Port über 10000.
5. Tragen Sie bei *Hostheader* die URL der neuen Seite ein, zum Beispiel *sharepoint.contoso.com*. Achten Sie aber darauf, dass dieser Servername im internen Netzwerk aufgelöst werden können muss. Alternativ verwenden Sie als Servernamen einfach den internen Namen des Servers oder die Bezeichnung *SharePoint*.

Abbildg. 22.10 Konfigurieren der Daten für die neue SharePoint-Seite



6. Stellen Sie sicher, dass für diese Webseite ein eigener Anwendungspool erstellt wird und das Sicherheitskonto *Netzwerkdienst* ausgewählt ist (Abbildung 22.11). Webseiten laufen in getrennten Prozessen, die durch Anwendungspools dargestellt werden. Stürzt ein Anwendungspool ab, zum Beispiel die SharePoint Services, laufen die anderen Applikationen, zum Beispiel die *Default Web Site* weiter. Die Anwendungspools können im Internetinformationsdienste-Manager angezeigt werden.

Abbildg. 22.11 Konfiguration des Anwendungspools für die neue SharePoint-Website



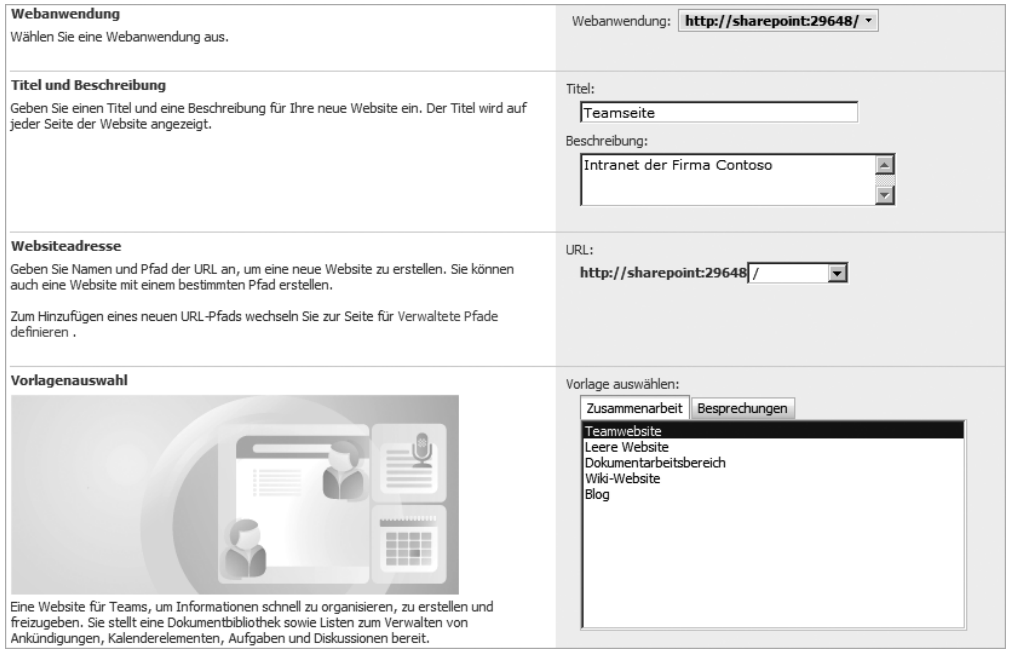
7. Wählen Sie im Listenfeld im Bereich *Suchserver* Ihren Server aus. Diese Auswahl ist für die Suche innerhalb der Windows SharePoint Services wichtig.
8. Stellen Sie sicher, dass im Bereich *Datenbankname und Authentifizierung* als Authentifizierungsmethode *Windows-Authentifizierung* aktiviert ist.
9. Klicken Sie auf *OK*, damit die Seite erstellt wird. Der Vorgang dauert einige Zeit.

Konfigurieren der neuen SharePoint-Website

Nachdem die Seite erstellt wurde, wird ein neues Fenster angezeigt. Klicken Sie in diesem Fenster auf den Link *Websitesammlung erstellen*. Dabei handelt es sich sozusagen um die oberste Webseite innerhalb der SharePoint Services. Diese oberste Webseite kann weitere untergeordnete Webseiten enthalten. Nachdem Sie die Erstellung einer Websitesammlung ausgewählt haben, müssen Sie wiederum verschiedene Konfigurationen vornehmen. Geben Sie zunächst einen beliebigen Titel und eine Beschreibung für die Sammlung ein. Stellen Sie sicher, dass die neu erstellte Webanwendung auch ausgewählt ist. Im Bereich *Vorlagenauswahl* wählen Sie *Teamwebseite* aus (Abbildung 22.12).

Geben Sie unten noch den Benutzernamen an, der die Seite verwalten soll, zum Beispiel *<Domäne>\Administrator*. Sie können auch einen weiteren Benutzernamen hinterlegen, der als zusätzlicher Administrator die Seite verwalten darf, zum Beispiel Ihr eigenes Benutzerkonto. Lassen Sie anschließend die Seite mit *OK* erstellen.

Abbildg. 22.12 Konfigurieren der neuen Teamseite



Abbildg. 22.13 Die neue Webseite mit dem neuen Port wurde erfolgreich erstellt

Löschen der Standard-Webseite der SharePoint Services 3.0

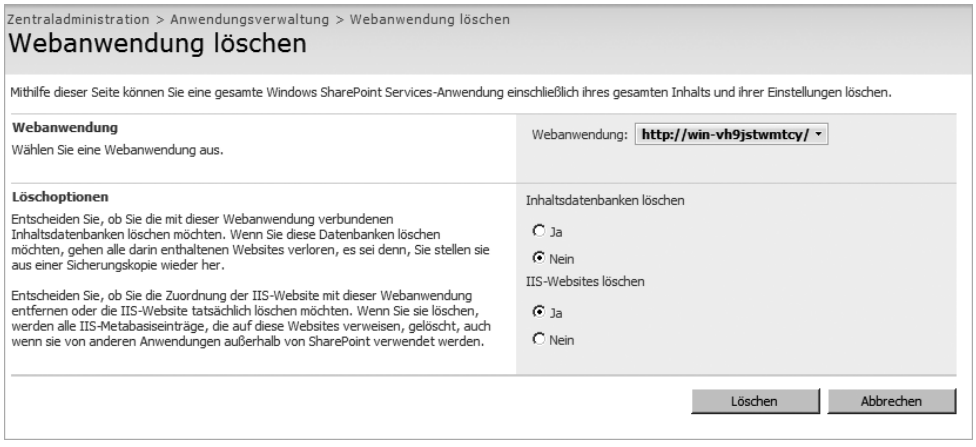
Nachdem Sie eine neue Webseite für die SharePoint Services erstellt haben, kann die vorhandene Standardwebseite der SharePoint Services gelöscht werden. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie die Zentralverwaltung über *Start/Verwaltung/SharePoint 3.0-Zentraladministration*.
2. Klicken Sie auf *Anwendungsverwaltung*.
3. Klicken Sie im Bereich *Verwaltung von SharePoint-Webanwendungen* auf *Webanwendung löschen*.
4. Klicken Sie im Bereich *Webanwendung* auf den kleinen Pfeil neben dem Listenfeld und anschließend auf *'Webanwendung' ändern*. Sie würden nämlich in der Standardauswahl Ihre neu erstellte Anwendung löschen, anstelle der alten Anwendung, die den gleichen Port wie die Standardwebseite von Windows Server 2008 verwendet. Wählen Sie in dem neuen Fenster die alte Web-

site aus, die standardmäßig erstellt wurde, normalerweise *http://<Servername>*. Achten Sie darauf, dass Sie nicht versehentlich die Webseite löschen lassen, die Sie gerade erst erstellt haben.

5. Wählen Sie anschließend im Bereich der Löschoptionen die beiden Optionen *Ja* bei *Inhaltsdatenbanken löschen* und *IIS-Websites löschen* aus.
6. Lassen Sie anschließend die Daten löschen und bestätigen Sie die zugehörige Meldung.

Abbildg. 22.14 Löschen der alten SharePoint-Seite



Abschluss der Konfiguration – Firewallausnahmen konfigurieren

Nach dem erfolgreichen Erstellen einer neuen Webseite und dem Löschen der alten kann die Default Web Site im Internetinformationsdienste-Manager wieder gestartet werden (Abbildung 22.15). Geben Sie anschließend noch in der Befehlszeile den Befehl *iisreset /noforce* ein, damit die Internetinformationsdienste neu gestartet werden. Damit über das Netzwerk auf die SharePoint Services und den neuen Port zugegriffen werden kann, muss erst eine Ausnahme in den Windows-Firewalleinstellungen eingetragen werden. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf *Start/Systemsteuerung/Windows-Firewall.*
2. Klicken Sie auf *Einstellungen ändern.*
3. Wechseln Sie zur Registerkarte *Ausnahmen.*
4. Klicken Sie auf *Port hinzufügen.*
5. Tragen Sie als Namen *SharePoint* ein.
6. Tragen Sie den Port ein, den Sie für die Seite konfiguriert haben.

Nachdem alle Einstellungen vorgenommen und alle offenen Dialogfelder bestätigt wurden, kann der interne Verbindungsaufbau getestet werden. Geben Sie dazu im Webbrowser die Adresse *http://<Servername>:<Port>* ein. Der Servername muss im internen Netzwerk aufgelöst werden können und der Port muss in der Firewall freigeschaltet sein. Da noch kein anderer Benutzer berechtigt ist, erscheint eine Authentifizierungsoberfläche. Geben Sie hier den Benutzernamen *<Domäne>\Administrator* und das Kennwort des Benutzers sein.

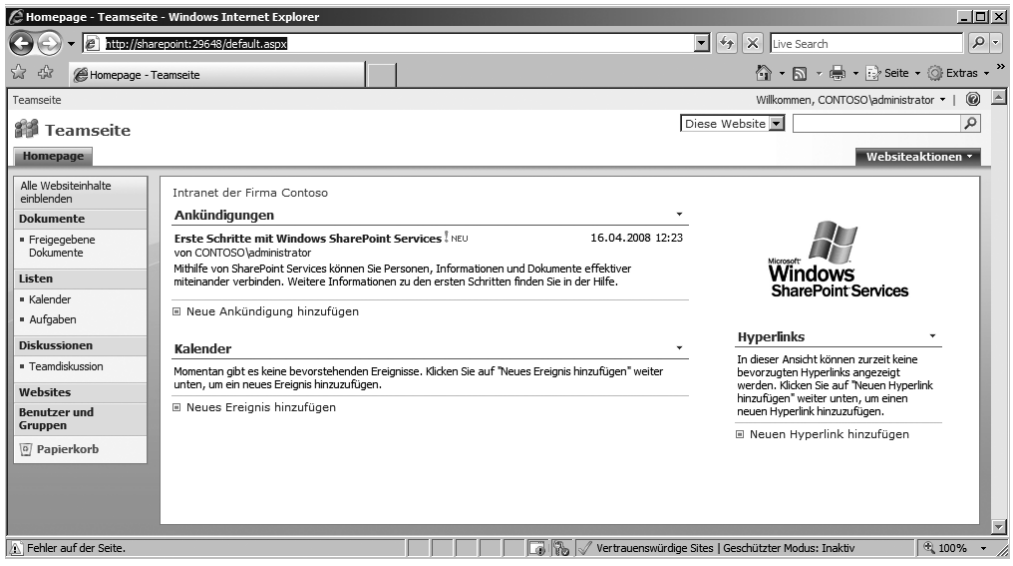
Sollte die Seite nicht aufgebaut werden können, überprüfen Sie in der Zentraladministration, ob die Zuordnung der Seite stimmt:

1. Klicken Sie dazu auf die Registerkarte *Vorgänge*.

2. Klicken Sie auf *Alternative Zugriffszuordnungen*.

Stellen Sie sicher, dass die interne URL und der Port für die Webseite übereinstimmen. Achten Sie darauf, dass der Servername in der URL von dem entsprechenden Client auch aufgelöst werden muss.

Abbildg. 22.15 Erfolgreicher Verbindungsaufbau zur neuen SharePoint-Seite

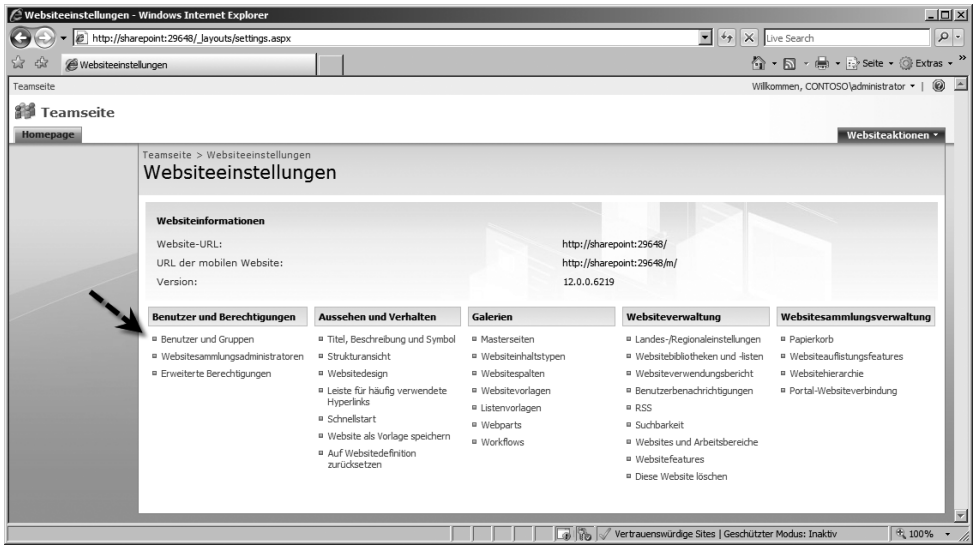


TIPP Wollen Sie als URL nicht den Servernamen verwenden, sondern eine Abkürzung wie SharePoint oder Intranet, legen Sie in der DNS-Zone der Domäne am besten einen Alias-Eintrag mit dem entsprechenden Namen an, der auf den echten Namen des Servers zeigt.

Benutzerberechtigungen in den SharePoint Services zuweisen

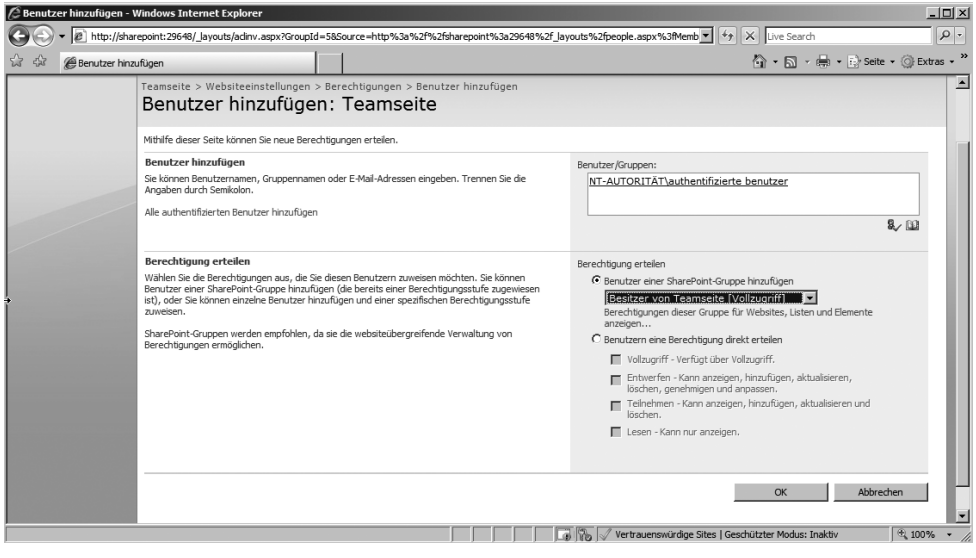
Als Abschluss der Konfiguration oder auch im Rahmen der normalen Administration sollten Sie den Anwendern in Ihrem Netzwerk noch Zugriffsrechte auf die SharePoint Services zuweisen. Nach der Installation darf nur der Administrator auf die Seite zugreifen und beliebig Änderungen vornehmen. Die normalen Anwender sollten nicht so viele Rechte haben. Die Konfiguration der Berechtigungen kann sehr detailliert in den Windows SharePoint Services durchgeführt werden. Zunächst sollten Sie jedoch alle internen Anwender generell für den Zugriff berechtigen. Öffnen Sie dazu die neue Webseite, die Sie erstellt haben. Klicken Sie oben rechts auf *Websiteaktionen* und wählen Sie *Websiteeinstellungen* aus. Es öffnet sich eine neue Webseite, auf der Sie diverse Einstellungen für diese Seite konfigurieren können. Die Berechtigungen werden über den Link *Benutzer und Gruppen* konfiguriert.

Abbildg. 22.16 Die SharePoint Services bieten vielfache Konfigurationsmöglichkeiten



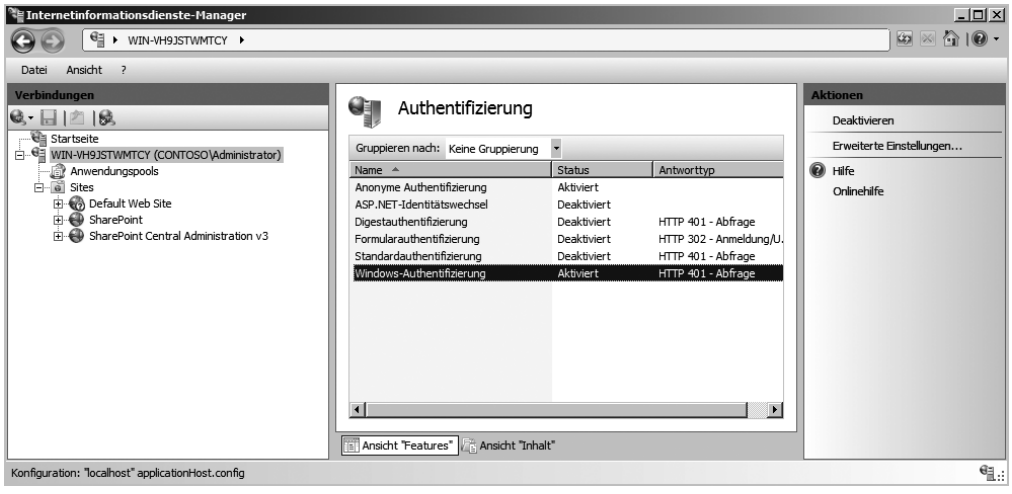
Es öffnet sich die neue Webseite zur Verwaltung der Berechtigungen Ihrer SharePoint-Seite. Über den Menübefehl *Neu* können Sie entweder Benutzer zu *Berechtigungsgruppen* hinzufügen oder neue Gruppen erstellen. Um Anwendern den Zugriff zu gestatten, wählen Sie *Benutzer hinzufügen* aus. Im neuen Fenster geben Sie die Benutzernamen im Feld *Benutzer/Gruppen* ein. Die Namen können Sie mit der Überprüfungsschaltfläche überprüfen lassen. Klicken Sie auf den Link *Alle authentifizierten Benutzer hinzufügen*, darf jeder auf den Server zugreifen, der sich an diesem authentifizieren darf, also über ein Benutzerkonto in der Domäne verfügt.

Abbildg. 22.17 Steuern der Benutzerberechtigungen für die Teamseite



Über *Berechtigung* erteilen, können den einzelnen Anwendern oder allen auf einmal verschiedene Rechte auf die SharePoint Services zugewiesen werden. Es würde den Rahmen dieses Buches sprengen, auf alle Möglichkeiten einzugehen. Am Ende des Kapitels haben wir für Sie einige Links zusammengestellt, über die Sie weitergehende Informationen für die SharePoint Services erhalten. Geben Sie am besten allen Teilnehmern das Recht *Mitglieder von SharePoint (Teilnehmen)*. In diesem Fall dürfen die Anwender neue Dateien hochladen, mit den SharePoint Services arbeiten, aber keine Systemeinstellungen ändern. Die Benutzer werden anschließend berechtigt. Die Anmeldung erfolgt auf der Startseite über den Anmeldebereich. Damit die Windows-Authentifizierung des Arbeitsplatzes zu den SharePoint Services durchgereicht wird, muss auf Serverebene im Internetinformationsdienste-Manager die Windows-Authentifizierung aktiviert werden.

Abbildg. 22.18 Aktivieren der Windows-Authentifizierung



Best Practices Analyzer for Windows SharePoint Services 3.0

Best Practices Analyzer gibt es nicht nur für Exchange Server, sondern auch für eine Reihe weiterer Serveranwendungen von Microsoft. Die jüngste Version ist *Best Practices Analyzer for Windows SharePoint Services 3.0 and the 2007 Microsoft Office System*. Nutzen Sie dieses Tool, das ebenfalls kostenlos als Download erhältlich ist, um die Leistung, Skalierbarkeit und Verfügbarkeit Ihrer SharePoint-Installation zu verbessern. Weitere Produkte, für die Best Practices Analyzer zur Verfügung stehen, sind Internet Security & Acceleration Server (ISA Server), SQL Server oder BizTalk Server 2006. Die komplette Liste finden Sie im Microsoft Download Center. Lassen Sie sich bei der Optimierung Ihrer IT-Infrastruktur durch diesen kleinen Helfer unterstützen. Sie finden das Produkt auf der Downloadseite *http://www.microsoft.com/downloads/details.aspx?FamilyID=CB944B27-9D6B-4A1F-B3E1-778EFDA07DF8&displaylang=en* oder indem Sie über eine Suchmaschine nach dem Programm suchen. Nachdem Sie die Datei heruntergeladen habe, können Sie den Best Practices Analyzer (BPA) auf dem Server installieren. Nachdem Sie das Tool in ein Verzeichnis extrahiert haben, können Sie über den Befehl *sharepointbpa.exe –cmd analyze –substitutions SERVER_NAME <Servername>* einen Bericht erstellen und diesen im Internet Explorer anzeigen

lassen. Achten Sie darauf, dass die Option *SERVER_NAME* groß geschrieben wird und Sie den korrekten Namen Ihres Servers angeben.

Praxisbeispiele für die SharePoint Services 3.0

Mittlerweile gibt es auch für die SharePoint Services 3.0 einige Vorlagen, welche den Praxisnutzen des Intranets weiter ausbauen. In diesem Abschnitt gehen wir auf Beispiele ein. Die Team-Portale sehen dank vorgegebener, aber anpassbarer Designs bereits in der Standarddarstellung sehr professionell aus. Darüber hinaus können Anwender, die mit SharePoint Services arbeiten, auch Vorlagen von der Microsoft-Webseite herunterladen, die die Zusammenarbeit noch weiter vereinfachen. Diese sind kostenlos und können ganz nach den Anforderungen der Firma und der Mitarbeiter verändert werden. Suchen Sie nach den Vorlagen auf der Seite *http://office.microsoft.com/de-de/templates/FX100595491031.aspx?pid=CL100632981031*. Auch über die Seite *http://www.microsoft.com/downloads/details.aspx?familyid=5807B5EF-57A1-47CB-8666-78C1363F127D&displaylang=en* finden Sie einige Vorlagen für die SharePoint Services, allerdings nur in englischer Sprache. Neu ist beispielsweise der *Verkaufsreport*. Hier können Vertriebsmitarbeiter in einer Excel-Liste eintragen, mit welchem Produkt sie bei welchen Kunden in welchem Quartal welche Umsätze erzielt haben. Der Unternehmer kann von überall online auf diese Daten zugreifen. Praktisch ist aber auch die Vorlage zur *Eventplanung*. Ein Team, das eine Veranstaltung organisiert, kann hier beispielsweise die Kosten für Dekorationen, Raummiete, Öffentlichkeitsarbeit, Bewirtung und so weiter eingeben. Das bringt mehr Übersichtlichkeit, insbesondere wenn mehrere Mitarbeiter die Veranstaltung planen, da jedes Teammitglied jederzeit einsehen kann, welche Kostenvoranschläge ein Kollege bereits eingeholt hat. Flattert ein besseres Angebot ins Unternehmen, kann der verantwortliche Mitarbeiter die Daten in die Liste eintippen, und alle Beteiligten sind sofort informiert, ohne dass ein zeitaufwändiger telefonischer Rundruf gestartet werden muss.

SharePoint Services erweitern mit zusätzlichen Vorlagen

Mittlerweile gibt es auch für die SharePoint Services 3.0 einige Vorlagen, welche den Praxisnutzen des Intranets weiter ausbauen. Nach deren Integration in die SharePoint Services können Sie so, neben den Listen, der Dokumentenverwaltung und dem Informationsaustausch, noch weitere Funktionen nutzen. So stellt Microsoft zum Beispiel über die Anwendungsvorlagen für Serveradministratoren folgende Erweiterungen zur Verfügung:

- Verwaltung für Abwesenheitsmeldungen und Urlaubsplan
- Budgetieren und Überwachen mehrerer Projekte
- Fehlerdatenbank
- Callcenter
- Änderungsauftragsverwaltung
- Kontaktverwaltung
- Veranstaltungsplanung

- Kostenvergütungs- und Genehmigungswebsite
- Helpdesk
- Inventarüberwachung
- IT-Team-Arbeitsbereich
- Verwaltung für Einstellungen und Bewerbungsgespräche
- Knowledge Base
- Leihbücherei
- Raum- und Ausstattungsreservierungen

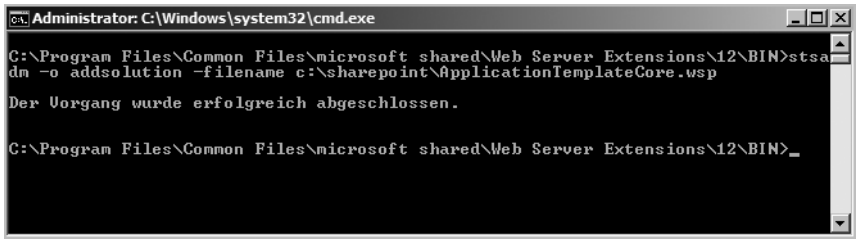
Laden Sie sich zunächst die Installationsdatei für diese Vorlagen herunter. Wir zeigen Ihnen, wie Sie diese Vorlagen als Webseite in Ihre SharePoint Services integrieren können.

Erweiterungen herunterladen und installieren

Die Integration der neuen Applikation in die SharePoint Services gestaltet sich allerdings zunächst nicht ganz einfach. Wir zeigen Ihnen aber an dieser Stelle Schritt für Schritt, wie Sie eine solche Applikation in Ihre SharePoint Services integrieren können. Gehen Sie dazu folgendermaßen vor:

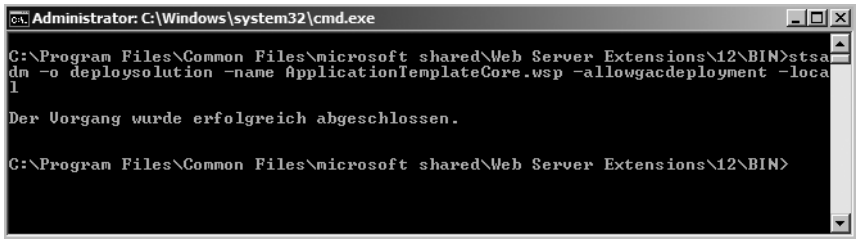
1. Bevor Sie zusätzliche Erweiterungen integrieren können, müssen Sie als Erstes die *Anwendungsvorlage: Anwendungsvorlagenbasis* installieren. Laden Sie sich daher diese Vorlage auf der Seite *http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=c1039e13-94da-4d7d-8cae-3b96fa5a4045* herunter.
2. Nachdem Sie die Vorlage heruntergeladen haben, müssen Sie das Archiv zunächst entpacken. Wählen Sie dazu ein temporäres Verzeichnis auf dem SharePoint Server, zum Beispiel *C:\sharepoint.*
3. Anschließend finden Sie in diesem Verzeichnis eine **.wsp*-Datei. Bei jeder Lösung und Erweiterung, die Sie für die SharePoint Services 3.0 herunterladen, handelt es sich um eine solche **.wsp*-Datei oder um Dateien mit der Endung **.stp*. Diese Dateien können über die Befehlszeile mit dem Tool *stsadm.exe* in die SharePoint Services integriert werden.
4. Meistens wird für *stsadm.exe* kein Pfad angelegt, sodass Sie direkt in das Verzeichnis des Tools wechseln müssen. Suchen Sie das Tool auf Ihrer Festplatte. Unter Windows Server 2008 wird es im Verzeichnis *C:\Program Files\Common Files\microsoft shared\Web Server Extensions\12\BIN* abgelegt.
5. Haben Sie in der Befehlszeile in das Verzeichnis gewechselt in dem das Tool *stsadm.exe* liegt, müssen Sie im ersten Schritt die Anwendungsvorlagenbasis in den SharePoint Services bekannt machen. Geben Sie dazu den Befehl *stsadm –o addsolution –filename c:\sharepoint\ApplicationTemplateCore.wsp* ein. Diese Basislösungsdatei wird dann dem Lösungsspeicher hinzugefügt, einer Tabelle im Windows SharePoint Services-Konfigurationsspeicher, in der die Lösungsdateien gespeichert sind. Sie erhalten daraufhin die Bestätigung, dass die Anwendung in den SharePoint Services integriert worden ist.

Abbildg. 22.19 Mit *stsadm.exe* wird eine neue Lösung in die SharePoint Services integriert



Als Nächstes müssen Sie den Befehl *stsadm –o deploysolution –name ApplicationTemplateCore.wsp –allowgacdeployment –local* eingeben, mit dem die Lösung aus dem Lösungsspeicher verfügbar gemacht wird. Auch dieser Vorgang wird von der Befehlszeile bestätigt.

Abbildg. 22.20 Nach der Integration in den Lösungsspeicher, muss die Anwendung noch verfügbar gemacht werden



Als Nächstes müssen Sie noch die notwendigen Informationen in die Systemdateien der SharePoint Services kopieren. Geben Sie dazu den Befehl *stsadm –o copyappbincontent* ein. Für diesen Befehl erhalten Sie keine Bestätigung, es sollte aber auch kein Fehler erscheinen.

Deinstallieren einer Vorlage

Bevor wir Ihnen die weitere Konfiguration von Vorlagen zeigen, sollten Sie auch noch die notwendigen Schritte kennen, um eine Vorlage wieder restlos vom System zu entfernen. Haben Sie eine bestimmte Anwendung getestet und stellt sich eventuell heraus, dass Sie diese nicht benötigen, können Sie die Bereitstellung der Vorlage aufheben und diese wieder aus den SharePoint Services entfernen. Dazu benötigen Sie zwei Schritte:

1. Im ersten Schritt wird die Bereitstellung der Vorlage wieder aufgehoben. Geben Sie dazu den Befehl *stsadm –o retractsolution –name ApplicationTemplateCore.wsp –local* ein, um in diesem Beispiel die Anwendungsvorlagenbasis zu deinstallieren.
2. Im zweiten Schritt löschen Sie die Anwendung mit dem Befehl *stsadm –o deletesolution –name ApplicationTemplateCore.wsp*.

Erweiterungen konfigurieren und verwenden

Neben der Anwendungsvorlagenbasis stehen Ihnen beim Download der verschiedenen Vorlagen noch zahlreiche Möglichkeiten zur Verfügung, mit denen Sie die SharePoint Services effizient nutzen können. Praktisch ist zum Beispiel auch die Vorlage zur Abwesenheits- und Urlaubsplanung.

Urlaubsanträge können in den SharePoint Services verwaltet werden. Dabei besteht die Möglichkeit, Urlaubseinträge zu stellen, zu bearbeiten, zu koordinieren und zu genehmigen. Und das alles fälschungssicher und papierlos. Diese Erweiterung wird ebenfalls als **.wsp*-Datei integriert. Die Vorgehensweise dazu ist ähnlich wie bei der Installation der Anwendungsvorlagenbasis. Die Urlaubsplanung liegt im Rahmen der Vorlagen als Datei *AbsenceVacationSchedule.wsp* vor. Um diese Lösung zu verwenden, gehen Sie folgendermaßen vor:

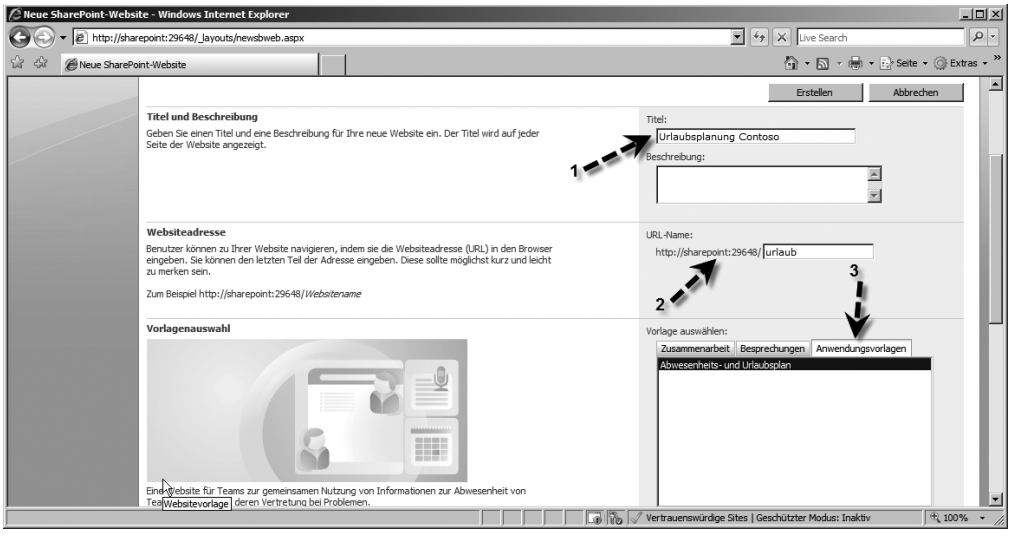
1. Laden Sie sich die Lösung herunter. Oder suchen Sie auf der Microsoft-Seite nach den Downloads für die SharePoint Services.
2. Tippen Sie anschließend den Befehl *stsadm –o addsolution –filename c:\sharepoint\ AbsenceVacationSchedule.wsp* ein und bestätigen Sie. Sie erhalten daraufhin die Meldung, dass die Anwendung in den SharePoint Services integriert worden ist.
3. Als Nächstes müssen Sie den Befehl *stsadm –o deploysolution –name AbsenceVacationSchedule.wsp –allowgacdeployment –local* eingeben, mit dem die Lösung aus dem Lösungsspeicher verfügbar gemacht wird. Auch dieser Vorgang wird von der Befehlszeile bestätigt.
4. Als Nächstes müssen Sie noch die notwendigen Informationen in die Systemdateien der SharePoint Services kopieren. Geben Sie dazu den Befehl *stsadm –o copyappbincontent* ein. Für diesen Befehl erhalten Sie keine Bestätigung, es sollte aber auch keine Fehlermeldung angezeigt werden.

Haben Sie die Anwendung wie beschrieben installiert, können Sie eine neue Webseite auf Basis dieser Vorlage erstellen. Melden Sie sich dazu als Administrator für die SharePoint Services an und klicken Sie oben links auf den Link *Websiteaktionen* und dann *Websiteeinstellungen*. Klicken Sie anschließend im neuen Fenster im Bereich *Websiteverwaltung* auf *Websites und Arbeitsbereiche*. Klicken Sie dann auf den Link *Erstellen*, um eine neue Website auf Basis der installierten Vorlage zu erzeugen.

Abbildg. 22.21 Erstellen einer neuen Webseite auf Basis einer Vorlage

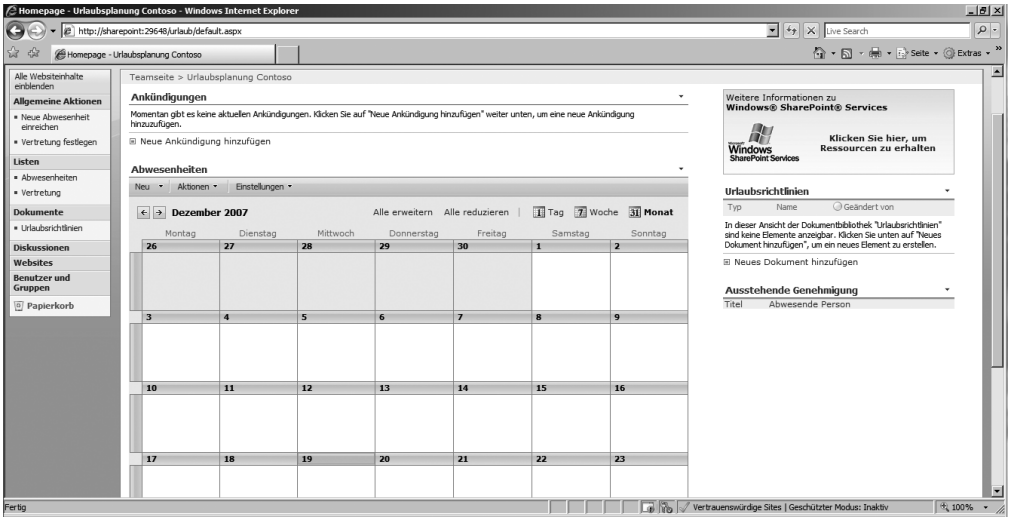
Tragen Sie im folgenden Fenster die notwendigen Daten für die Website wie Titel, URL und die weiteren Optionen ein. Aktivieren Sie die Registerkarte *Anwendungsvorlagen* und wählen Sie die Vorlage aus, auf deren Basis Sie die neue Website erstellen wollen. Diese Registerkarte wird erst dann angezeigt, wenn Sie sowohl die *Anwendungsvorlagenbasis* als auch mindestens eine Vorlage installiert haben. Klicken Sie anschließend auf *Erstellen*, damit die Website erzeugt wird.

Abbildg. 22.22 Bei der Erstellung einer neuen Website können Sie die Vorlage auswählen, auf deren Basis die Seite erzeugt werden soll



Nachdem Sie die Website erstellt haben, steht diese über den konfigurierten Link zur Verfügung und Sie können die Lösung verwenden.

Abbildg. 22.23 Urlaubsplanung mit den SharePoint Services durchführen



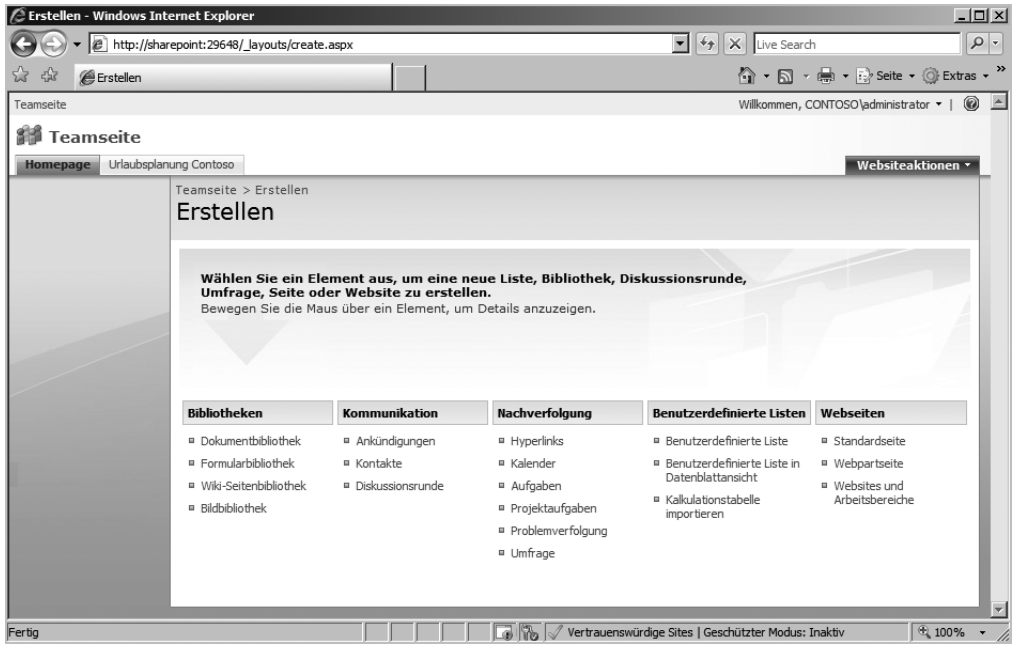
Neben diesen Lösungen finden Unternehmen sicherlich auch noch zahlreiche andere Möglichkeiten innerhalb der Vorlagen. Die neu erstellten Webseiten, die auf Basis der neuen Vorlagen arbeiten, werden auf der Startseite über verschiedene Registerkarten angezeigt. Anwender und Administratoren können bequem über diese Registerkarten zwischen dem normalen Intranet und den speziellen

Anwendungen hin und her wechseln, sodass die Übersichtlichkeit nicht leidet. Auch in der Schnellstartleiste am linken Rand werden diese Seiten angezeigt.

Webseiten einfach erweitern

Neben der Erstellung von neuen Webseiten können Sie auch innerhalb der bestehenden Webseiten neue Funktionen hinzufügen. Verwenden Sie dazu das Menü *Websiteaktionen/Erstellen*. Es erscheint ein neues Fenster, über das Sie zur bestehenden Webseite sehr einfach neue Funktionen oder Bibliotheken hinzufügen können. Diese werden dann nicht als eigene Registerkarte dargestellt, sondern innerhalb der Seite als neue Funktion.

Abbildg. 22.24 Erstellte Webseiten lassen sich mit beliebigen Bibliotheken erweitern



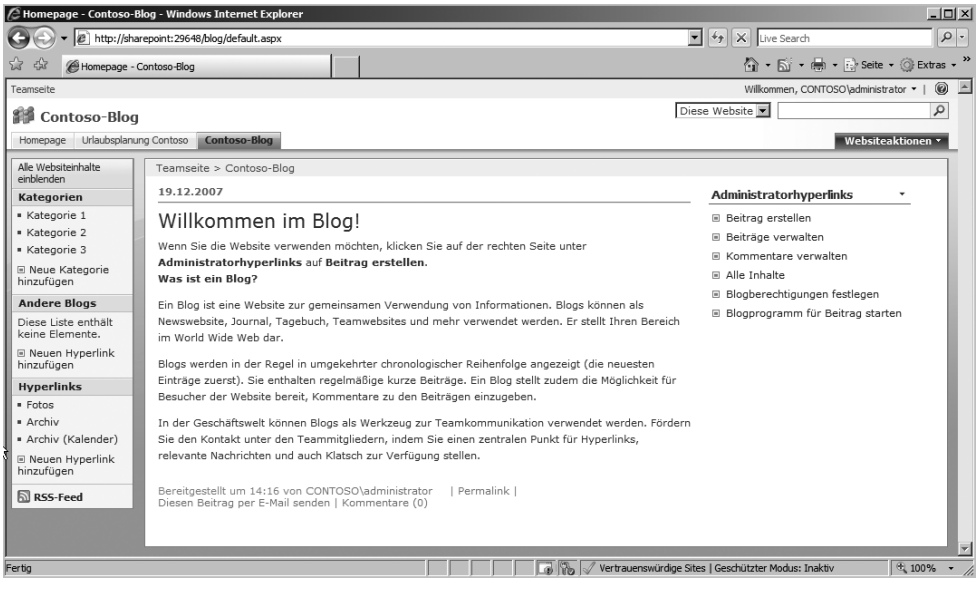
Klicken Sie zum Beispiel auf *Wiki-Seitenbibliothek*, können Sie innerhalb Ihres Intranets eine eigene kleine Wikipedia erstellen. Dies hat zum Beispiel den Nutzen, das Unternehmen Informationen zu ihren Produkten im Intranet hinterlegen können, diese aber nicht nur starr zur Verfügung stehen. Mitarbeiter können Informationen zu den Produkten eingeben, damit alle anderen Anwender immer die aktuellsten Informationen sehen. Die Änderungen werden protokolliert, sodass jederzeit festgestellt werden kann, wer Änderungen vorgenommen hat. Die neue Wiki-Seite, wird auf der Startseite als eigener Link dargestellt, ohne dass Sie sich um die grafische Umsetzung sorgen müssen. Alles funktioniert vollkommen automatisch, die Mitarbeiter im Unternehmen müssen sich nur noch um die Inhalte der Seite kümmern.

Erstellen von Blogs

Eine wichtige neue Funktion sind auch die Weblogs oder kurz Blogs in den SharePoint Services. Genauso wie Blogs im Internet können Unternehmen im internen Netzwerk einen Blog einrichten, um Brainstorming zu betreiben oder die Mitarbeiter über neue Entwicklungen einzelner Abteilungen auf dem Laufenden zu halten. Die Erstellung eines neuen Blogs erfolgt identisch zur Erstellung einer neuen Website, zum Beispiel der Urlaubs- oder Eventplanung. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf der Teamseite auf *Websiteaktionen/Websiteeinstellungen*.
2. Klicken Sie im Bereich *Websiteverwaltung* auf *Websites und Arbeitsbereiche*.
3. Klicken Sie auf *Erstellen*.
4. Geben Sie die Daten und die URL des Blogs ein.
5. Wählen Sie auf der Registerkarte *Zusammenarbeit* die Vorlage *Blog* aus und klicken Sie auf *Erstellen*.

Abbildg. 22.25 Mit den SharePoint Services lassen sich auf schnelle Arte und Weise Blogs erstellen, an denen die Mitarbeiter des Unternehmens interaktiv mitarbeiten können



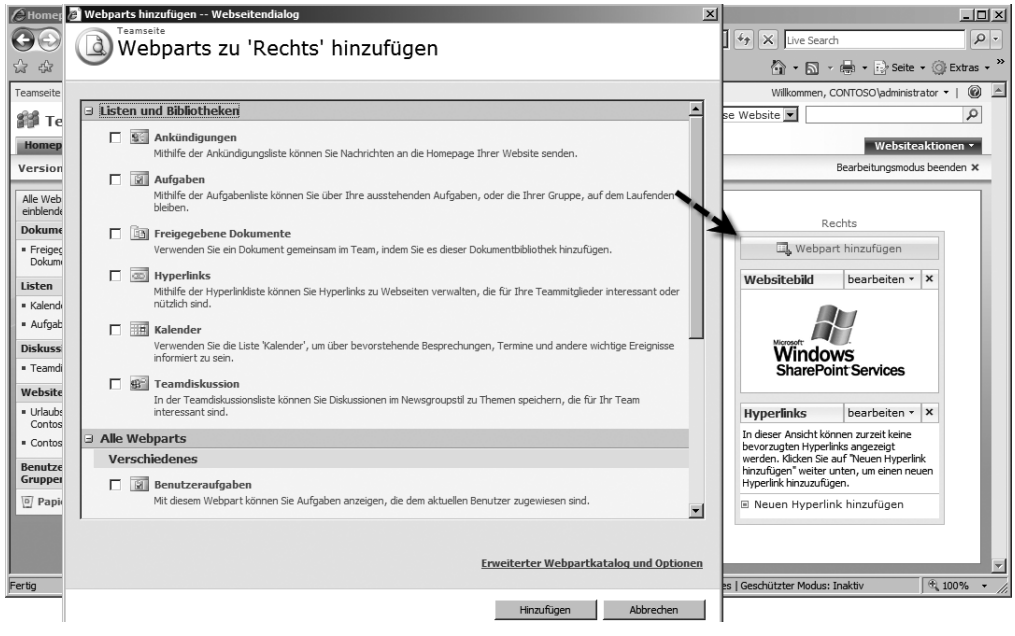
Nachdem Sie den Blog erstellt haben, können Sie Kategorien einrichten, um die Beiträge zu strukturieren. Kategorien sind besonders nützlich, wenn Sie Blogbeiträge zu verschiedenen Themen oder für unterschiedliche Zwecke erstellen. Wenn Sie für den Blog noch keine Kategorien eingerichtet haben, enthält die Liste Platzhalter für die Kategorien *Kategorie 1, Kategorie 2* und *Kategorie 3*. Klicken Sie zum Hinzufügen weiterer Kategorien in der Listensymbolleiste auf *Neue Kategorie hinzufügen* und geben Sie dann in das Feld *Titel* einen Namen für die Kategorie ein. Zum Löschen einer Kategorie klicken Sie auf deren Namen und dann auf *Element löschen*. Administratoren können die Berechtigungen und die Einstellungen für den Blog über diesen Bereich verwalten. Als Programm zum Schreiben von Blog-Beiträgen können Anwender auch Word 2007 verwenden, welches eine

eigene Schnittstelle für Blogs integriert hat. Die Beiträge können auf diese Weise bequem in Word geschrieben und mit einem Klick auf die entsprechende Schaltfläche in den SharePoint Services veröffentlicht werden. Blogeinträge können von anderen Mitarbeitern kommentiert werden und ein Administrator kann steuern, welche Kommentare zur Veröffentlichung gelangen. Dieses System kann von Unternehmen auch genutzt werden, um Blogs für Kunden oder Lieferanten über ein Extranet zur Verfügung zu stellen. Es ist keine komplizierte Entwicklungsarbeit notwendig, sondern lediglich etwas Planung und die Umsetzung mit den SharePoint Services. Schreiben Anwender Kommentare zu den Blogeinträgen, können Administratoren diese über den Link *Kommentare verwalten* in einem zentralen Fenster darstellen und gegebenenfalls löschen. Auch die Bearbeitung von Kommentaren durch Administratoren ist möglich.

Webparts in Webseiten einfügen

Erstellte Webseiten und Bibliotheken lassen sich darüber hinaus sehr einfach mit neuen Funktionen erweitern. Administratoren können über das Menü *Websiteaktionen/Seite bearbeiten* so genannte *Webparts* hinzufügen. Dabei handelt es sich um zusätzliche Funktionen und kleine Programme, die eine Bibliothek oder Webseite erweitern. Wählen Sie im neuen Fenster einfach das Webpart aus, das Sie hinzufügen wollen, und schon wird es in der Bibliothek angezeigt. Im Internet gibt es zahlreiche Anbieter für solche Webparts. Auch auf der Microsoft-Website finden Sie einige. Manche Webparts sind kostenpflichtig, andere erhalten Sie kostenlos.

Abbildg. 22.26 Mit Webparts lassen sich Webseiten oder Bibliotheken ergänzen

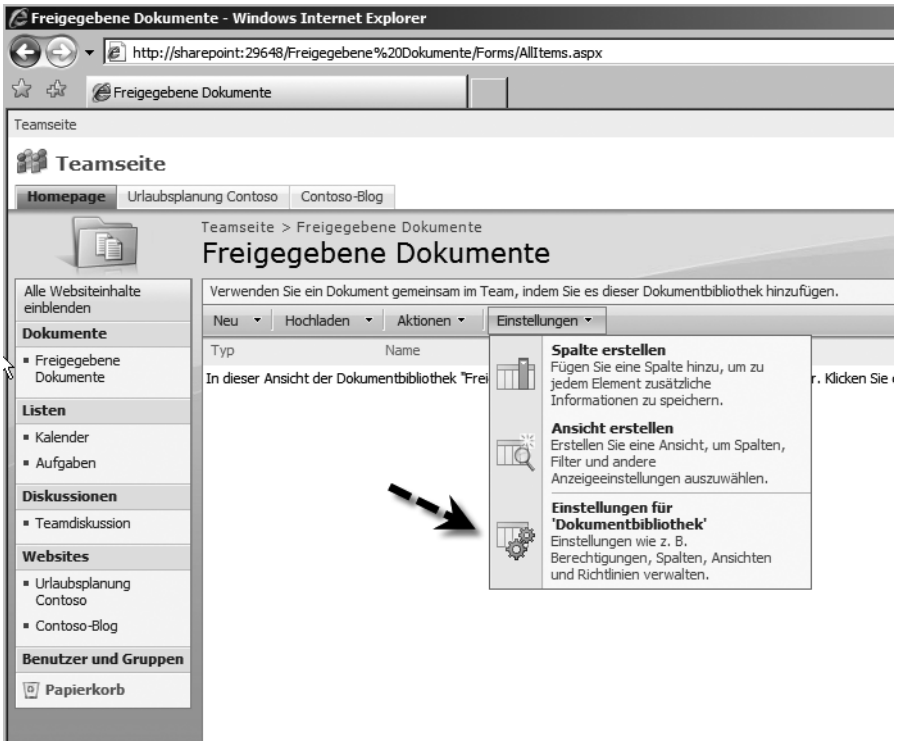


Seiteninhalte konfigurieren und einrichten

Beim Einrichten einer Liste oder Bibliothek können Sie festlegen, dass die Aufnahme neuer Elemente oder Dateien oder auch Änderungen genehmigt werden müssen. Um die Genehmigung für eine Liste oder Bibliothek zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie in der Schnellstartleiste auf den Link für die Liste oder Bibliothek.
2. Klicken Sie anschließend im Menü *Einstellungen* auf *Listeneinstellungen* oder auf die Einstellungen der Bibliothek.

Abbildg. 22.27 Mit entsprechenden Berechtigungen lassen sich auch die Einstellungen der jeweiligen Liste oder Bibliothek anpassen



3. Klicken Sie unter *Allgemeine Einstellungen* zum Beispiel auf *Versionierungseinstellungen*.
4. Klicken Sie im Abschnitt *Inhaltsgenehmigung* unter *Inhaltsgenehmigung für gesendete Elemente erforderlich?* auf *Ja*.
5. Klicken Sie auf *OK*.

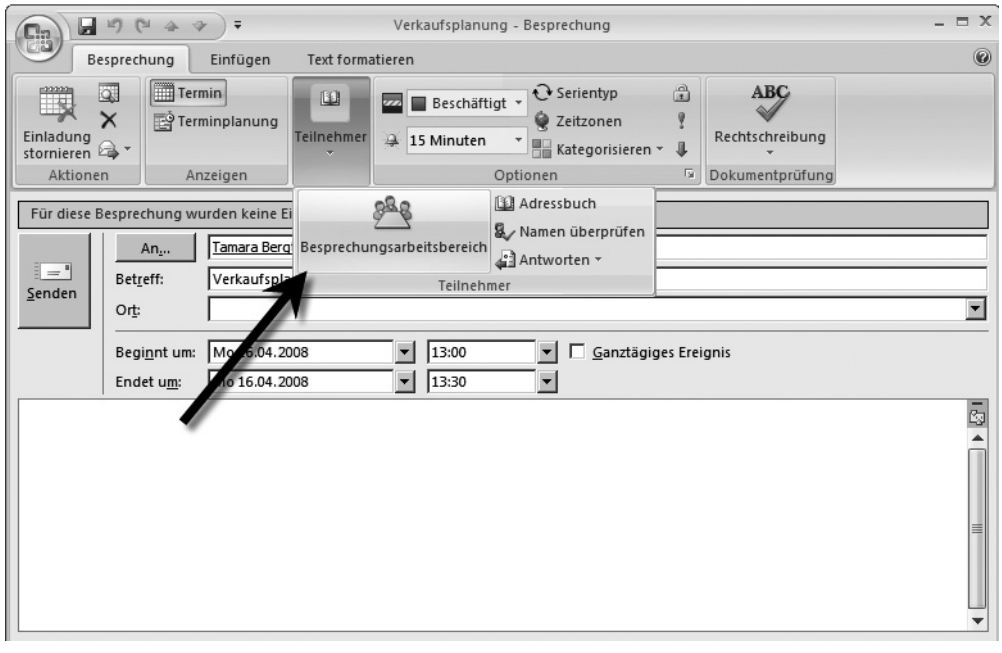
Wenn diese Einstellung für die Genehmigung des Inhalts aktiviert wird, verbleibt ein geändertes Element im Zustand »ausstehend«, bis das Element von einer Person mit den erforderlichen Rechten genehmigt oder abgelehnt wird. Der Besitzer oder der Administrator einer Seite kann über das entsprechende Aktionsmenü der Datei festlegen, ob er diese genehmigen oder ablehnen will. Dazu kann er einen Kommentar eingeben und seine Entscheidung begründen. Der entsprechende Teilnehmer wird über diese Entscheidung auf Basis seiner Benachrichtigungseinstellungen informiert. In den

Einstellungen der Bibliothek können Sie definieren, welche Anwender Entwürfe anzeigen können, bevor diese genehmigt werden. Die Einstellungen einer Bibliothek erreichen Sie auf dem bereits beschriebenen Weg zur Aktivierung der Versionierung und der Genehmigung. Klicken Sie dazu im Abschnitt *Entwurfselementsicherheit* unter *Wer Entwurfselemente anzeigen darf* auf die Benutzergruppen, die Entwürfe anzeigen dürfen.

SharePoint und Outlook verwenden – Erstellen einer Besprechung mit Besprechungsarbeitsbereich

Ein Besprechungsarbeitsbereich zentralisiert auf praktische Weise Informationen für Mitarbeiter und Kollegen, die an einem Projekt zusammenarbeiten und den Überblick über in Besprechungen getroffene Entscheidungen behalten möchten. Sie können mit den SharePoint Services ein temporäres Web erstellen, in dem Informationen und Dokumente für Besprechungen des Teams zur Verfügung gestellt werden. Dies hat den Vorteil, dass Anwender, die an einer Besprechung teilnehmen, alle notwendigen Dokumente auf einen Blick zur Verfügung haben. Der Link zum Besprechungsarbeitsbereich wird automatisch mit der Einladungs-E-Mail über Outlook verschickt. Auf diese Weise wird also eine Webseite für die Besprechung erstellt, sodass Informationen effizient ausgetauscht werden können. Nach der Besprechung können Sie auf der Arbeitsbereichswebsite die Ergebnisse der Besprechung veröffentlichen. Um mit Outlook eine Besprechung zu erstellen, die einen dazugehörigen Besprechungsarbeitsbereich zur Verfügung stellt, gehen Sie vor, wie im Folgenden beschrieben.

Abbildg. 22.28 Mit Outlook 2003/2007 können Sie zusammen mit den SharePoint Services Besprechungsarbeitsbereiche erstellen

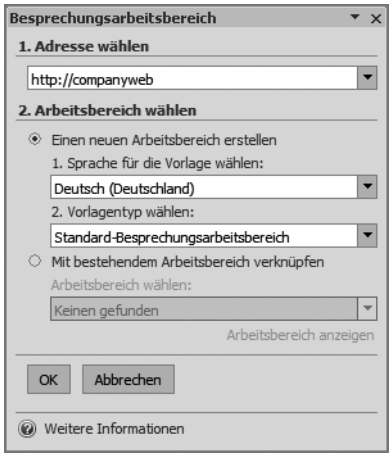


Erstellen Sie im Kalender einen neuen Termin und laden Sie den oder die entsprechenden Mitarbeiter auf Basis der Terminplanung zu diesem Termin ein. Versenden Sie die Besprechungsanfrage jedoch noch nicht.

Bei Outlook 2003 finden Sie die Schaltfläche zum Erstellen eines Besprechungsarbeitsbereiches auf der Registerkarte *Termin* in der Besprechungsanfrage. Bei Outlook 2007 finden Sie diese Schaltfläche auf der Registerkarte *Besprechung* über das Menü *Teilnehmer*. Sie können Besprechungsarbeitsbereiche für neue, aber auch für bestehende Besprechungen erstellen.

Nachdem Sie die Erstellung eines Besprechungsarbeitsbereiches ausgewählt haben, können Sie diesen über das neue Fenster und der Schaltfläche *Erstellen* in den SharePoint Services erstellen lassen. Anschließend können Sie noch einige Optionen für den Besprechungsarbeitsbereich festlegen und diesen endgültig erstellen lassen.

Abbildg. 22.29 Haben Sie die Erstellung eines Arbeitsbereiches in Outlook aktiviert, können Sie diesen noch anpassen



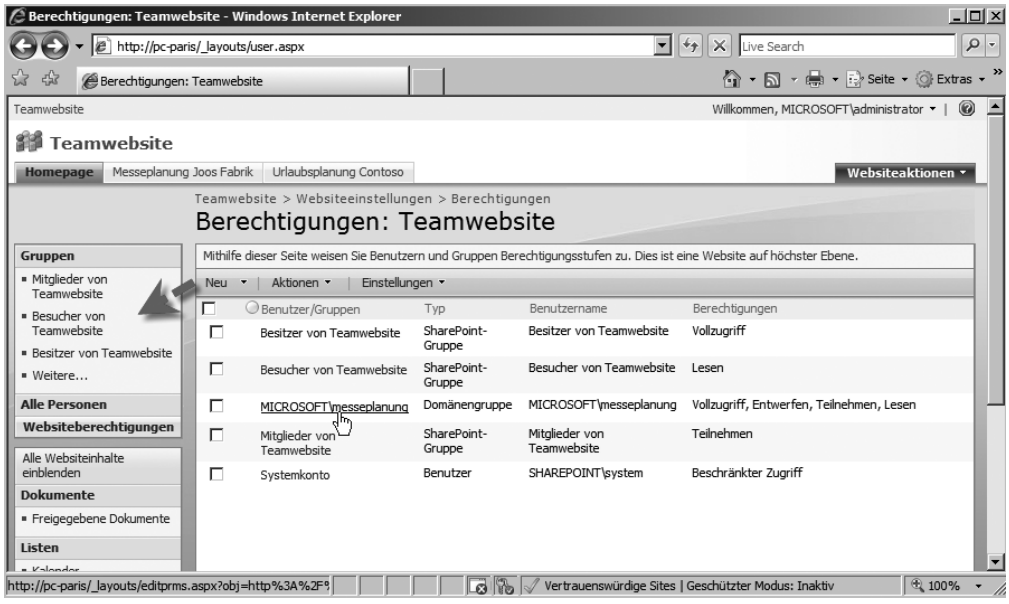
Nachdem sich Outlook mit den SharePoint Services verbunden hat (unter Umständen werden diese beim ersten Mal nicht automatisch gefunden, sondern Sie müssen die Webseite des Servers angeben), wird der Besprechungsarbeitsbereich automatisch erstellt und ein vorgegebener Text mit dem Link zum Bereich in die Besprechungsanfrage integriert. Klicken Sie oder die anderen Teilnehmer auf den Link in der E-Mail, gelangen Sie direkt zu dem Besprechungsarbeitsbereich. Sie können hier sehen, wer an der Besprechung teilnimmt, Dokumente und die Tagesordnung organisieren sowie weitere Informationen und Dokumente zur Besprechung hinterlegen.

Abbildg. 22.30 Der Arbeitsbereich für die Besprechung kann direkt über die Einladungs-E-Mail geöffnet werden

Benutzerverwaltung und Berechtigungen steuern

Innerhalb eines solchen Informationsportals wie den SharePoint Services ist es von existentieller Bedeutung, Berechtigungen vergeben zu können. Über diese Berechtigungen kann exakt gesteuert werden, welche Anwender ein Intranet nur lesen, welche schreiben und welche Benutzer auch Berechtigungen erteilen können. Die SharePoint Services arbeiten dazu mit den Benutzerkonten im Active Directory zusammen. Um Berechtigungen zu erteilen, legen Sie Gruppen in der Domäne an und nehmen die entsprechenden Benutzerkonten in diese Gruppen auf. Anschließend können Sie den entsprechenden Gruppen Berechtigungen in den einzelnen Webseiten zuweisen. Administratoren pflegen die Benutzerrechte über den Link *Benutzer und Gruppen*, der normalen Anwendern ohne Administratorrechte nicht zur Verfügung steht. Sie können festlegen, ob nur die von ihnen erstellten Elemente oder alle Elemente gelesen und bearbeitet werden können. Über diesen Link gelangen Sie zur Benutzerverwaltung der Teamseite. Hier können Sie explizite Berechtigungen für Mitarbeiter und Besucher der Webseite erteilen. Dazu können Sie entweder Benutzerkonten oder Gruppen aus der Domäne berechtigen, oder Sie nehmen diese Konten in spezielle SharePoint-Gruppen auf, denen Sie dann Berechtigungen erteilen. Ihnen stehen also zur Verwaltung der Berechtigungen innerhalb des Intranets sowohl die Domänen-Konten zur Verfügung als auch SharePoint-Gruppen, die Sie über diesen Bereich anlegen und steuern können. Alle Berechtigungen werden wiederum als Link dargestellt, über den Sie zur exakteren Konfiguration der jeweiligen Berechtigung gelangen.

Abbildg. 22.31 Die SharePoint Services lassen eine detaillierte Berechtigungstruktur zu



Einmal eingerichtete Berechtigungsstrukturen lassen sich einfach über entsprechende Gruppenmitgliedschaften in der Domäne steuern. Die Anmeldung erfolgt transparent für den Anwender. Beim Öffnen des Internet Explorers wird oben im Menü angezeigt, mit welchem Benutzernamen sich ein Anwender an den SharePoint Services angemeldet hat. Der Internet Explorer übernimmt hier die Domänenanmeldung des Anwenders. Über das Menü in der Anmeldeleiste können Sie sich aber jederzeit mit einem anderen Benutzernamen anmelden. Auf einer SharePoint-Website wird dieses Willkommensmenü immer angezeigt. Das Menü kann Benutzer auffordern, sich anzumelden und nach Abschluss des Vorgangs vollständig abzumelden. Zudem kann sich über das Menü ein anderer Benutzer mit anderen Anmeldeinformationen bei der Website anmelden. Anwender können über dieses Menü persönliche Einstellungen ändern, zum Beispiel eine E-Mail-Adresse hinterlegen, zu denen die SharePoint Services die konfigurierten Benachrichtigungen schicken können. An dieser Stelle lassen sich auch weitergehende Informationen hinterlegen, zum Beispiel ein Foto oder die Ländereinstellungen. Wollen Sie ein Foto hinterlegen und haben Sie die Datei auf dem lokalen Server gespeichert, geben Sie die URL in der Form *file://<Pfad>* ein, zum Beispiel *file://c:\sharepoint\thomas.jpg*.

Daten, die Sie in der Benutzerverwaltung hinterlegen, werden auch an jede Stelle übernommen und angezeigt, an denen Benutzereinstellungen angezeigt werden. Hinterlegte Fotos helfen dabei oft die Personen zu erkennen, was wesentlich persönlicher ist, als nur das Hinterlegen von Domänenkonten.

Design der SharePoint Services anpassen

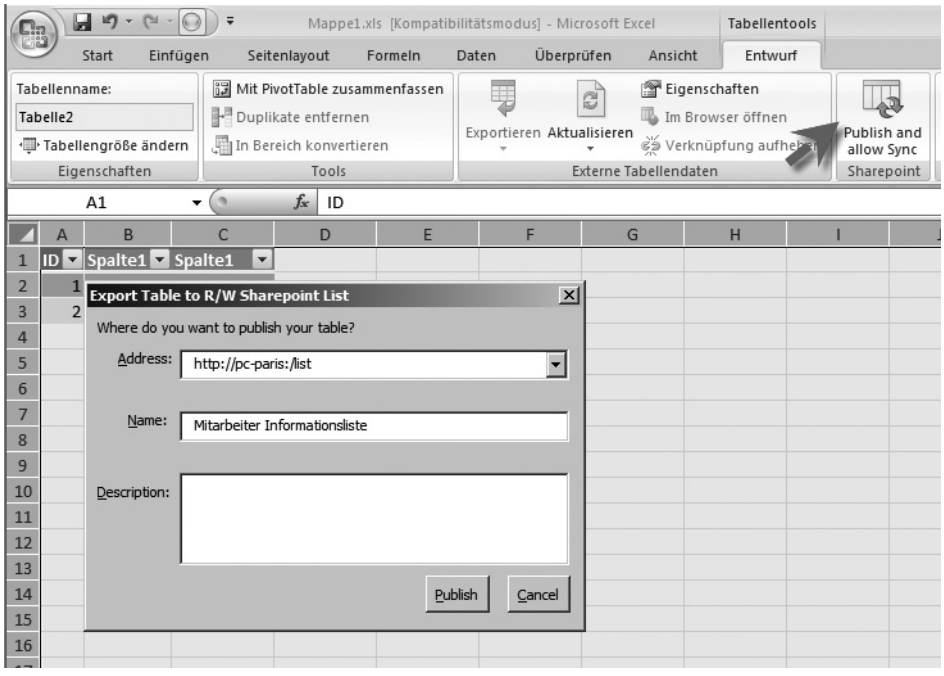
Um das Design der SharePoint Services anzupassen, müssen Sie nicht unbedingt Webentwickler sein. Das Standardaussehen der Oberfläche lässt sich genauso anpassen wie die Farben, Beschreibungen oder eventuelle Logos. Auch Administratoren oder Anwender ohne große Entwicklungserfahrung können schnell und einfach das Aussehen durch wenige Mausklicks anpassen. Über das Menü *Websiteaktionen/Websiteeinstellungen* stehen hier zahlreiche Möglichkeiten zur Verfügung. Wollen Sie zum Beispiel Ihr Firmenlogo hinterlegen, verwenden Sie den Link *Titel, Beschreibung und Symbol*. Jetzt können Sie die Beschreibung der Teamseite ändern sowie ein Logo hinterlegen. Speichern Sie das Bild für das Logo auf dem Server und geben Sie als URL den Pfad mit einem normalen Schrägstrich an, also zum Beispiel *c:/sharepoint/logo.gif*. Anschließend wird das Symbol angezeigt. Über das Menü *Websitedesign* lässt sich – ebenfalls mit wenigen Mausklicks – die Farbe der Teamseite an Ihre Unternehmensfarben anpassen. Bereits mit diesen beiden Schritten erhalten Sie ein Intranet, das sich perfekt an Ihre Unternehmensrichtlinien anpassen lässt. Auch die Schnellstartleiste an der Seite ist in Sekundenschnelle anpassbar. Klicken Sie dazu einfach auf den Link *Schnellstart* in den *Websiteeinstellungen* und wählen Sie das neue Aussehen aus. Die Änderungen werden in Echtzeit übernommen.

Office 2007 mit SharePoint verwenden

Auch wenn die Bearbeitung von Listen in den SharePoint Services sehr benutzerfreundlich gelöst wurde, ist es unter Umständen effizienter, den Inhalt diverser Listen über ein externes Programm, zum Beispiel Excel 2007, zu pflegen. Der Inhalt der Liste kann in Excel bearbeitet werden und wird anschließend mit SharePoint synchronisiert. So stehen den Anwendern immer die aktuellsten Informationen einer Liste zur Verfügung, und die Mitarbeiter, die diese Liste pflegen, können dies bequem mit Excel erledigen. Damit Sie diese Funktion nutzen können, muss in Excel 2007 eine Erweiterung installiert werden, die Microsoft kostenlos zur Verfügung stellt (*http://www.microsoft.com/downloads/details.aspx?familyid=25836e52-1892-4e17-ac08-5df13cfc5295&displaylang=en*). Diese Erweiterung trägt die Bezeichnung *Excel 2007 SharePoint List Synchronizing Add-In*. Gehen Sie zur Einrichtung der Synchronisierung von Listen mit Excel 2007 folgendermaßen vor:

1. Laden Sie sich die Erweiterung herunter und entpacken Sie das Archiv.
2. Starten Sie Excel 2007.
3. Klicken Sie auf die *Office*-Schaltfläche und dann auf die Schaltfläche *Excel-Optionen*.
4. Wählen Sie auf der linken Seite die Kategorie *Add-Ins* aus.
5. Klicken Sie im Bereich *Verwalten* auf *Excel-Add-Ins* und dann auf die Schaltfläche *Gehe zu*.
6. Klicken Sie im neuen Fenster auf *Durchsuchen* und wählen Sie das entpackte Add-In aus.
7. Anschließend sollte die Erweiterung *SynchronizeWSSandExcel* angezeigt und aktiviert sein.
8. Damit Sie diese Funktion nutzen können, müssen Sie zunächst die Excel-Datei über *Datei speichern unter* im Excel 97-2003-Format speichern.
9. Als Nächstes müssen Sie in Excel über *Einfügen/Tabelle* eine Tabelle erzeugen. Anschließend können Sie über die Registerkarte *Tabellentools/Entwurf* in der Multifunktionsleiste die erste Synchronisierung der Tabelle mit den SharePoint Services aktivieren. Sie müssen dazu die Tabelle markieren und den Befehl *Publish and allow Sync* in der Gruppe *Sharepoint* auswählen.
10. Geben Sie die URL der Liste ein, mit der Sie diese Tabelle synchronisieren wollen.

Abbildg. 22.32 Nach der Erstellung einer Tabelle in Excel 2007 können Sie diese mit den SharePoint Services synchronisieren



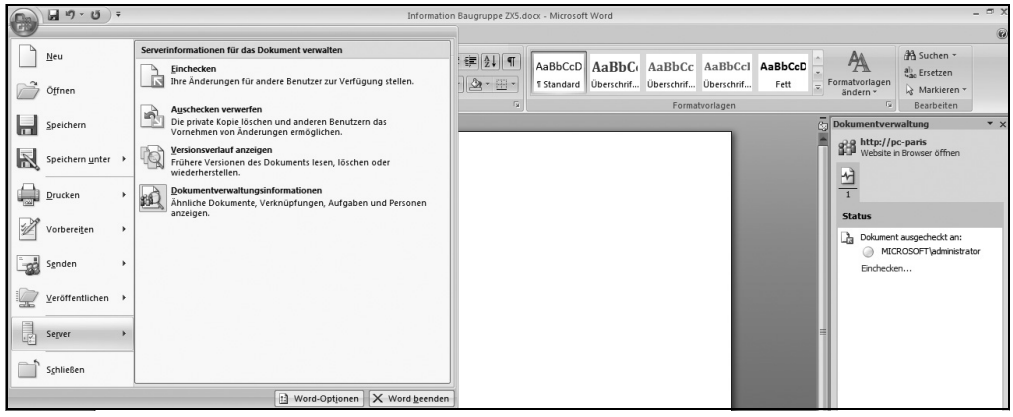
Haben Sie die erste Synchronisierung durchgeführt, können Sie später über das Kontextmenü der Tabelle und den Untermenübefehl *Tabelle/Mit SharePoint synchronisieren* den Inhalt der Tabelle jederzeit in die SharePoint Services synchronisieren. Der Inhalt wird sofort angezeigt und die Information steht allen Mitarbeitern zur Verfügung. Zusätzlich ist der Inhalt der Tabelle auch noch in der Excel-Datei enthalten.

Word 2003/2007 mit den SharePoint Services verwenden

Sie können auch direkt mit den Office-Programmen Dateien in die SharePoint Services speichern und von dort abrufen. Um ein Dokument zu bearbeiten, gehen Sie folgendermaßen vor:

1. Öffnen Sie zunächst die Dokumentenbibliothek.
2. Klicken Sie im Eigenschaftenmenü der Datei zunächst auf *Auschecken*. Dadurch ist sichergestellt, dass kein anderer Anwender die Datei zur gleichen Zeit bearbeitet.
3. Anschließend können Sie die Datei erneut aufrufen und dieses Mal die Option *In Microsoft Office Word bearbeiten* auswählen.
4. Anschließend öffnet sich das Word-Dokument und Sie können über die SharePoint-Aufgabenleiste auf der rechten Seite auch auf andere Dokumente in der gleichen Bibliothek zugreifen, Eigenschaften des Programms bearbeiten und Informationen abrufen. Sie können die Versionen des Dokuments ansehen, das Dokument einchecken, damit andere Anwender es wieder bearbeiten können, und einen Kommentar hinterlegen, der Ihre Änderung beschreibt. Nach dem Einchecken können Sie sich den Versionsverlauf der Datei anzeigen lassen, indem Sie diese Option wieder im Kontextmenü der Datei auswählen.

Abbildg. 22.33 Bearbeiten eines Dokumentes aus den SharePoint Services direkt in Word



HINWEIS **Links zu den SharePoint Services:**

Eine sehr aktive Community, viele Informationen und Anleitungen finden Sie unter *http://www.mysharepoint.de* und *http://live.sharepointcommunity.de*

Einstiegsseite für die SharePoint Services 3.0 von Microsoft *http://office.microsoft.com/de-de/getstarted/HA100738471031.aspx*

Weitere Infos finden Sie in der Wikipedia *http://de.wikipedia.org*

Excel 2007 SharePoint List Synchronizing Add-In *http://msdn2.microsoft.com/de-de/library/bb462636(office.11).aspx*

Auf der Seite *http://www.microsoft.com/germany/kleinunternehmen/tipps-und-tricks/sbs/zusammenarbeit-von-wss-und-office-word-2003.mspx* sehen Sie anhand eines kleinen Flashfilms, wie Office und die SharePoint Services miteinander interagieren.

Zusammenfassung

In diesem Kapitel haben Sie gelernt, wie die Windows SharePoint Services 3.0 mit SP1 optimal auf einem Windows Server 2008-Computer installiert und verwaltet werden. Auch die Erweiterung mit neuen Funktionen haben wir Ihnen gezeigt. Im nächsten Kapitel gehen wir auf einen weiteren zusätzlichen Serverdienst ein, mit dem ein Windows Server 2008-Netzwerk effizient mit Patches versorgt wird: die Windows Server Update Services (WSUS) 3.0 mit SP1.

Kapitel 23

WSUS 3.0 SP1 – Schnelleinstieg

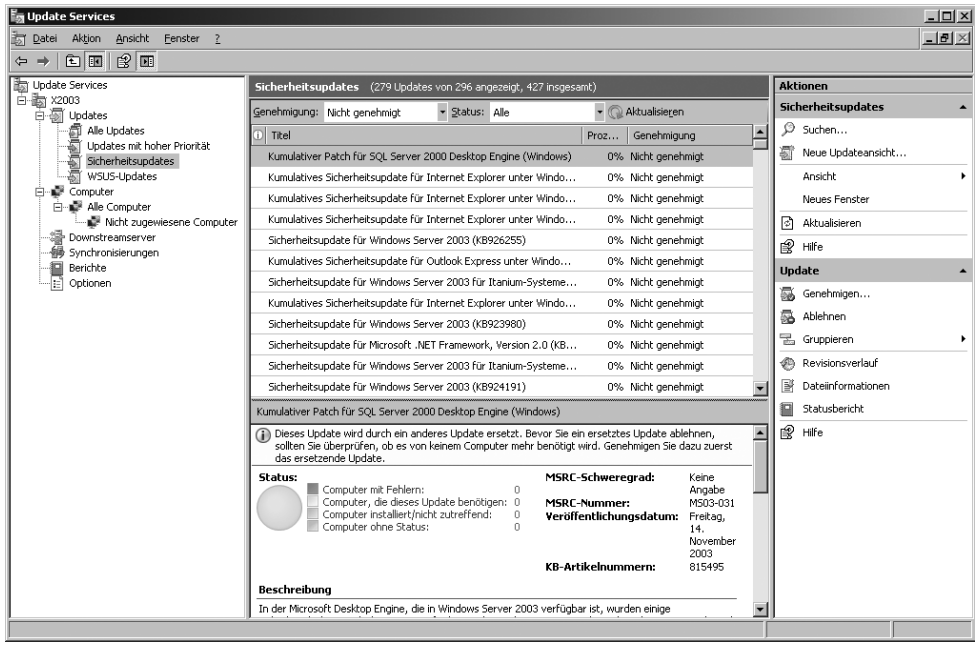
In diesem Kapitel:

Zusätzlich zum Virenschutz ist es für Unternehmen sehr wichtig, dafür zu sorgen, dass die PCs und Server immer mit den aktuellen Sicherheitspatches versorgt sind. Das Patchmanagement ist heutzutage für Unternehmen aller Größenordnungen ein extrem wichtiger Punkt in der Absicherung der Netzwerkstruktur. Da ständig neue Lücken auftauchen und Patches für diese Lücken zum Download angeboten werden, ist die manuelle Installation fast nicht mehr durchführbar. Auch der Verbindungsaufbau einzelner PCs zu Updateseiten macht keinen Sinn, da die Installation der Patches nicht überwacht und die Bandbreite zum Internet unnötig belastet wird.

TIPP Weitere Informationen, Anleitungen und Hilfen finden Sie auf den folgenden Internetseiten:

- http://www.wsus.de
- http://www.wsus-praxis.de
- http://www.wsuswiki.com
- http://blogs.technet.com/wsus
- http://www.wsus.info/forums

Abbildg. 23.1 WSUS 3.0 stellt hunderte Sicherheitspatches zentralisiert zur Verfügung

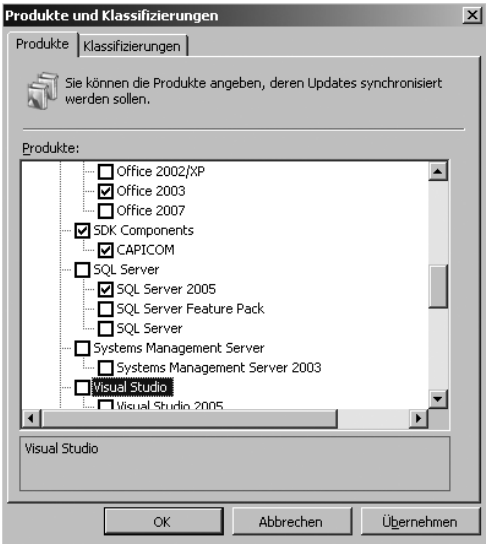


Durch eine Patchmanagementlösung werden Sicherheitspatches auf einem Server zentral bereitgestellt und müssen nur einmal heruntergeladen werden. Der Administrator kann festlegen welche Patches er für die Installation freigibt und welche nicht verteilt werden sollen. Nur durch die professionelle Verwaltung der Patches ist die Sicherheit eines Unternehmens gewährleistet. Microsoft stellt für die automatisierte Verteilung von Patches im Unternehmen die kostenlosen Windows Server Update Services (WSUS) 3.0 zur Verfügung. In diesem Kapitel stellen wir Ihnen diese Lösung und die Einrichtung vor. Als wichtiges Zusatztool für WSUS und die allgemeine Sicherheit in Windows-Netzwerken dient das Tool Microsoft Baseline Security Analyzer (MBSA).

Vorteile des zentralisierten Patchmanagements

Mit WSUS können Patches automatisch aus dem Internet heruntergeladen und an die Arbeitsstationen oder Server verteilt werden, ohne dass ein Administrator sich darum kümmern muss. Die Windows Server Update Services sind der Nachfolger der Software Update Services (SUS) 1.0. SUS konnte nur systemkritische Betriebssystemupdates verteilen. WSUS kann diesbezüglich wesentlich mehr. Die Clients im Netzwerk werden so konfiguriert, dass sie sich alle Aktualisierungen vom WSUS-Server herunterladen und diese automatisch installieren. Der WSUS-Server ist dafür verantwortlich, die Patches zentral zur Verfügung zu stellen. Dies hat den Vorteil, dass ein Administrator immer genau einen Überblick darüber hat, welche Computer derzeit aktuell sind und welche Patches im Unternehmen installiert werden. Unternehmen, gleich welcher Größe, sollten die Installation von Patches keinesfalls dem Zufall überlassen oder gar nicht durchführen. Die Einführung von WSUS 3.0 im Unternehmen gestaltet sich meist einfacher als gedacht und die Vorteile der neuen Version 3.0 der Windows Server Update Services überzeugen. Ungeübte Anwender oder Administratoren, die keine Zeit haben, sich ständig um Updates zu kümmern, können WSUS einmal konfigurieren und Regeln für die automatisierte Bereitstellung festlegen. Dadurch genügt es, alle Patches nur einmal aus dem Internet herunterzuladen, was Zeit und Bandbreite spart. Damit die Clients die Updates installieren, müssen diese so konfiguriert werden, dass keine Patches aus dem Internet heruntergeladen werden, sondern WSUS verwendet wird. Diese Einstellung kann auch über Gruppenrichtlinien durchgeführt werden, die genau steuern, wie sich die einzelnen Clients und Server bei den automatischen Updates verhalten sollen. WSUS kann darüber hinaus noch Statistiken führen, welche Patches bereits installiert wurden. Es werden nicht nur kritische Updates des Betriebssystems unterstützt, sondern WSUS kann auch andere Microsoft-Produkte aktualisieren. Microsoft aktualisiert ständig die Liste der Programme, die der WSUS aktualisieren kann. Neben Sicherheitspatches werden auch Service Packs und zusätzliche Funktionen wie zum Beispiel die Windows Vista Ultimate Extras unterstützt. Windows Vista und Windows Server 2008 werden übrigens mit WSUS 3.0 SP1 komplett unterstützt.

Abbildg. 23.2 WSUS 3.0 kann nahezu alle Microsoft-Produkte aktualisieren

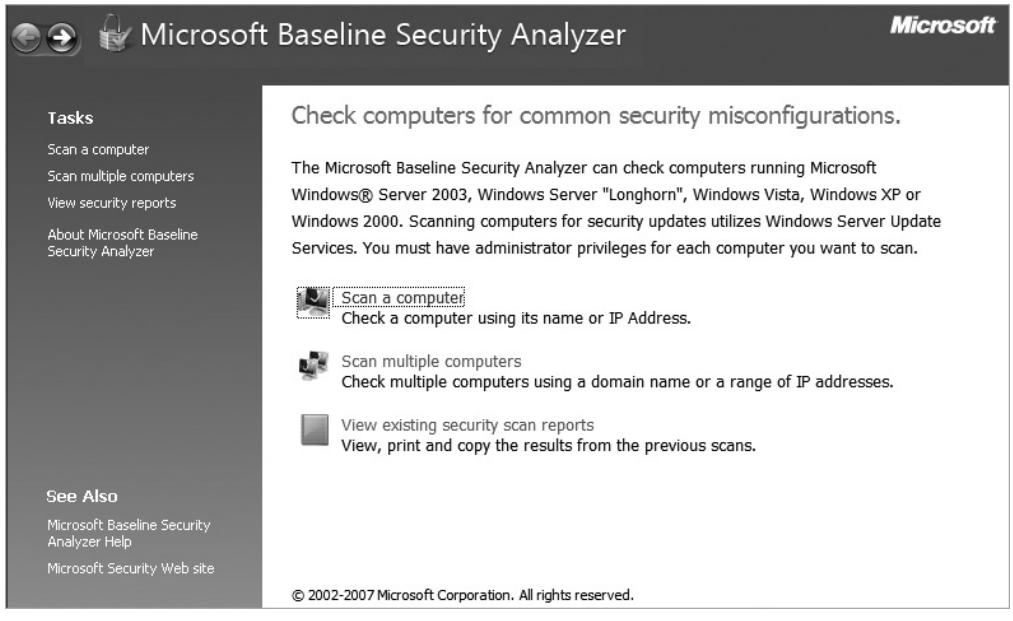


Während WSUS 2.0 eine Weiterentwicklung der Software Update Services (SUS) 1.0 ist, sind in WSUS 3.0 zahlreiche Verbesserungen integriert, die von Microsoft-Kunden gewünscht wurden. Unter anderem wurden die Reporting-Funktionen deutlich erweitert, und der Server kann besser in komplizierte Strukturen integriert werden. WSUS 3.0 unterstützt wesentlich effizienter den System Management Server (SMS) und dessen Nachfolger, den System Center Configuration Manager 2007. Die neue Version bietet die Möglichkeit, manuell heruntergeladene Patches in die Patchverteilung per Import zu integrieren. Diese Funktion kann zum Beispiel für Unternehmen sinnvoll sein, die ein spezielles Hotfix bei Microsoft anfordern und auf Computer im Netzwerk verteilen müssen. Die neue Version bietet darüber hinaus wesentlich mehr Skripting-Funktionen als die Vorgängerversion.

Microsoft Baseline Security Analyzer (MBSA)

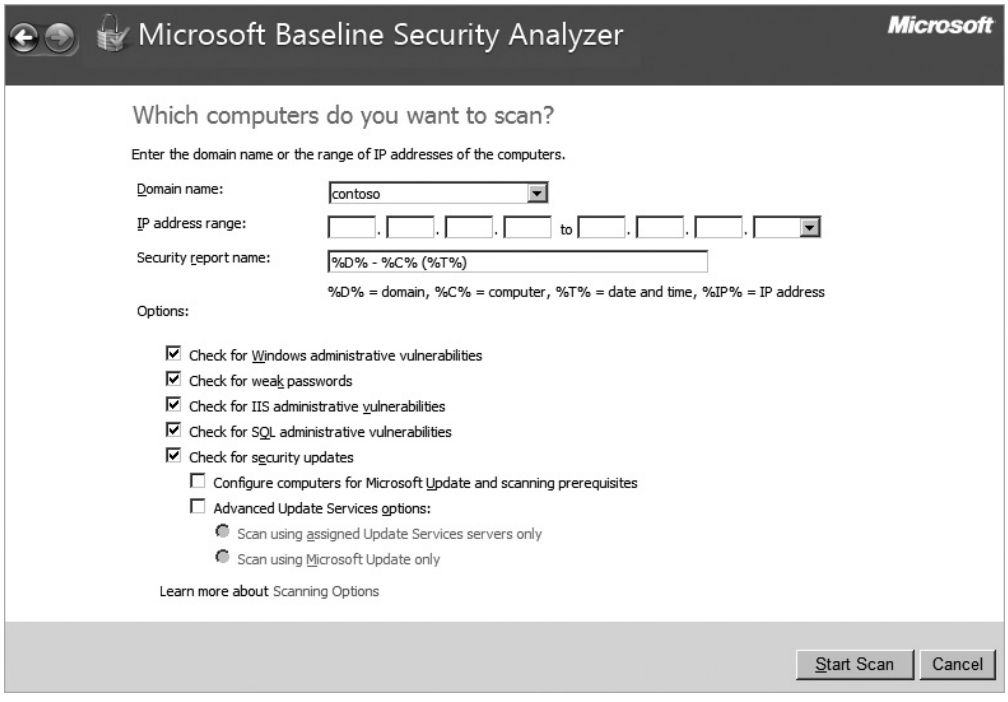
Der MBSA gehört zum Handwerkszeug jedes Beraters oder Administrators. Mit dem MBSA können Windows-Rechner und Server eines Netzwerkes auf Sicherheitslücken und fehlende Patches untersucht werden. Auch wenn in Unternehmen bereits eine Patchmanagement-Lösung wie der WSUS eingesetzt wird, schadet es nicht, ab und zu die PCs im Netzwerk zu scannen, damit sichergestellt ist, dass alle Sicherheitseinstellungen durchgeführt und die Computer aktuell mit Patches versorgt wurden. Der MBSA wird kostenlos auf der Seite *http://www.microsoft.com/technet/security/tools/MBSAHome.mspx* von Microsoft zur Verfügung gestellt.

Abbildg. 23.3 Verwenden des MBSA zum Aufdecken von Sicherheitslücken



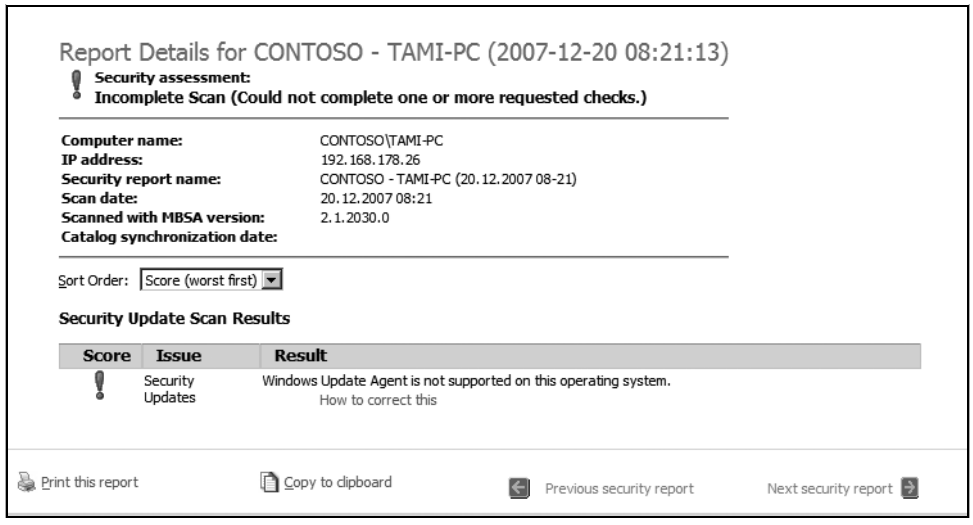
Nach der Installation kann über die Option *Scan multiple computers* das ganze Netzwerk auf einmal nach fehlenden Patches und kritischen Sicherheitslücken durchsucht werden.

Abbildg. 23.4 Auswählen des IP-Bereichs, in dem Computer gescannt werden sollen



Ab Version 2.1 werden Windows Vista und Windows Server 2008 vollständig unterstützt. Nachdem die Option *Scan multiple computers* ausgewählt wurde, kann entweder ein IP-Bereich oder eine Domäne angegeben werden, die auf Sicherheitslücken untersucht wird. Wird der Scanvorgang per Klick auf die Schaltfläche *Start Scan* aktiviert, lädt der MBSA zunächst aktuelle Sicherheitsinformationen aus dem Internet herunter. Danach beginnt das Tool den konfigurierten IP-Bereich nach Sicherheitslücken zu durchsuchen. Im Anschluss wird ein detaillierter Bericht über die fehlenden Aktualisierungen und Sicherheitslücken angezeigt. Aus diesem Bericht lässt sich ein Maßnahmenkatalog erarbeiten, zum Beispiel die Einführung der Windows Server Update Services 3.0. Der Scanvorgang des MBSA kann durchaus einige Minuten oder sogar Stunden dauern, abhängig von der Anzahl der Rechner, die im konfigurierten Subnetz integriert sind.

Abbildg. 23.5 Nach einem Scanvorgang zeigt der MBSA detailliert die Sicherheitslücken in einem Windows-Netzwerk an, samt fehlenden Patches



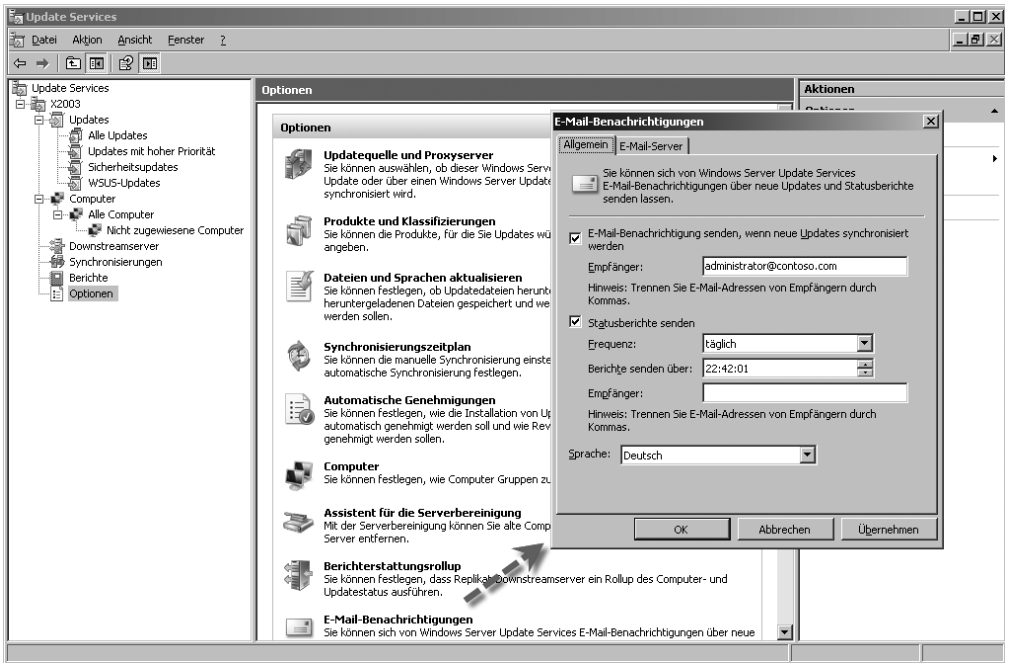
Die Berichte werden gespeichert und können über das Startfenster des MBSA jederzeit erneut angezeigt werden.

Neuerungen und Voraussetzungen für WSUS 3.0 SP1

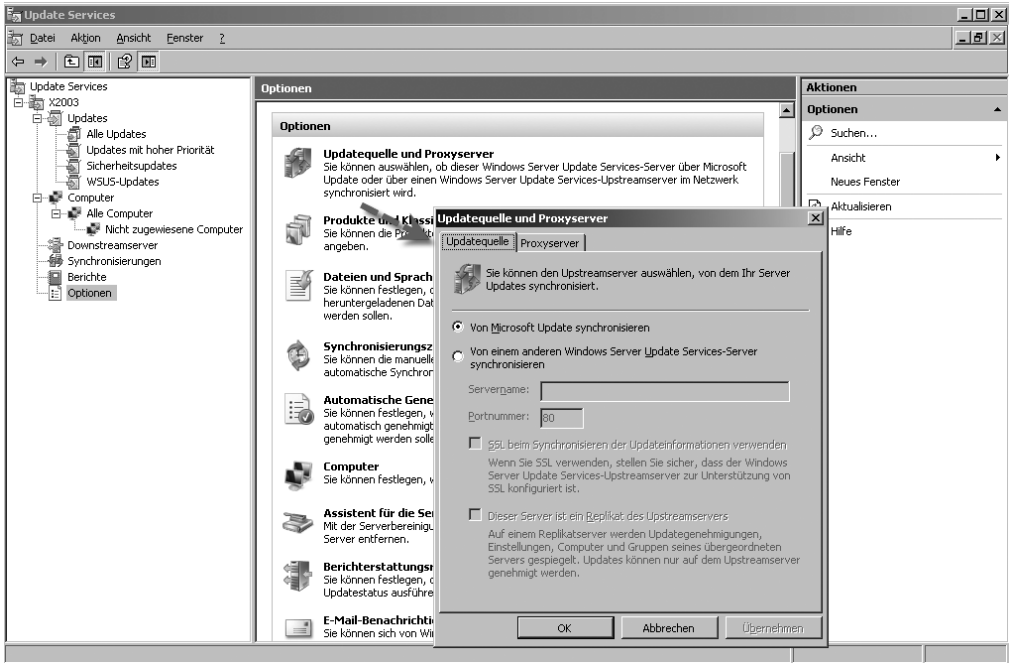
Eine wesentliche Neuerung in WSUS 3.0 ist, dass die Verwaltung jetzt nicht nur über die Weboberfläche durchgeführt werden kann, sondern hauptsächlich über ein eigenes Snap-In in der MMC 3.0. Zwar steht auch weiterhin die Weboberfläche zur Verfügung, aber viele Administratoren werden sich über die neue Management Console sicherlich freuen, da die Verwaltung hierüber wesentlich zügiger und effizienter durchgeführt werden kann. Die MMC kann auch auf PCs installiert werden. Dazu kann während der Installation von WSUS ausgewählt werden, dass nur die Verwaltungskonsole installiert wird. Die Verbindung der Verwaltungskonsole wird allerdings wieder über IIS auf dem WSUS-Server hergestellt, sowie den konfigurierten Port während der Installation. Über eine MMC können mehrere WSUS 3.0-Server in einer gemeinsamen Oberfläche verwaltet werden.

WSUS 3.0 unterstützt Windows Vista sowie Windows Server 2008. Diese beiden Betriebssysteme werden nicht nur clientseitig unterstützt, sondern auch serverseitig. Allerdings unterstützt erst WSUS 3.0 mit SP1 die Installation des Servers unter Windows Server 2008. Die Verwaltungskonsole wird darüber hinaus in den Server-Manager integriert. Es können also nicht nur Updates für diese Produkte über WSUS verteilt werden, sondern WSUS kann unter Windows Server 2008 installiert und von einer Windows Vista-Arbeitsstation aus verwaltet werden. Windows Server Update Services 3.0 kann auf einem 64-Bit-System installiert werden. Ebenfalls neu ist der eingebaute E-Mail-Benachrichtigungsdienst, über den Berichte an bestimmte E-Mail-Adressen im Unternehmen gesendet werden können. Wenn neue Updates eintreffen, kann der Server einen Administrator via E-Mail benachrichtigen.

Abbildg. 23.6 Mit E-Mail-Benachrichtigungen werden Administratoren automatisch auf dem neusten Informationsstand gehalten



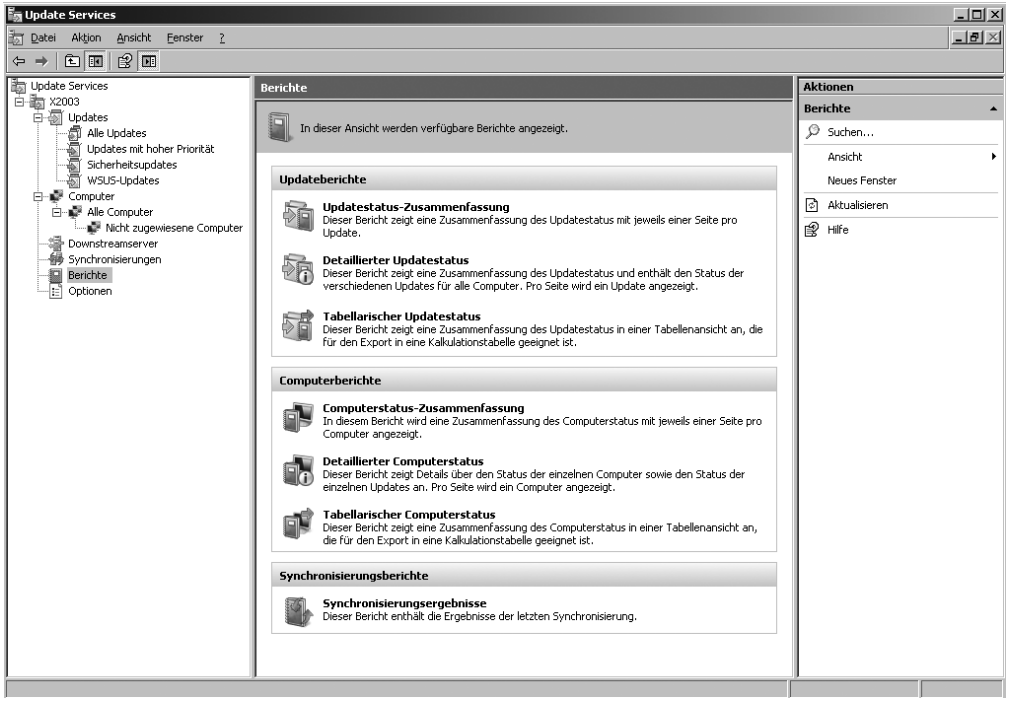
Abbildg. 23.7 Die Konfiguration der Synchronisierung kann auch nach der Installation noch angepasst werden



Durch diese Benachrichtigungen entgeht keinem Administrator mehr, wenn neue Aktualisierungen verfügbar sind. Es ist möglich, für einen WSUS 3.0-Server jederzeit den Replikationsmodus in Echtzeit zu wechseln, also ob sich der Server direkt von Microsoft Update oder einem anderen WSUS-Server im Netzwerk bedienen soll. Unter WSUS 2.0 war bei einer Replikationsänderung eine Neuinstallation notwendig. Auffällig ist die gesteigerte Performance des Servers, welche auch in der Reporting-Leistungsfähigkeit durchschlägt. Auch die erste Synchronisierung des Servers läuft in wenigen Minuten ab, was unter WSUS 2.0 noch Stunden gedauert hat.

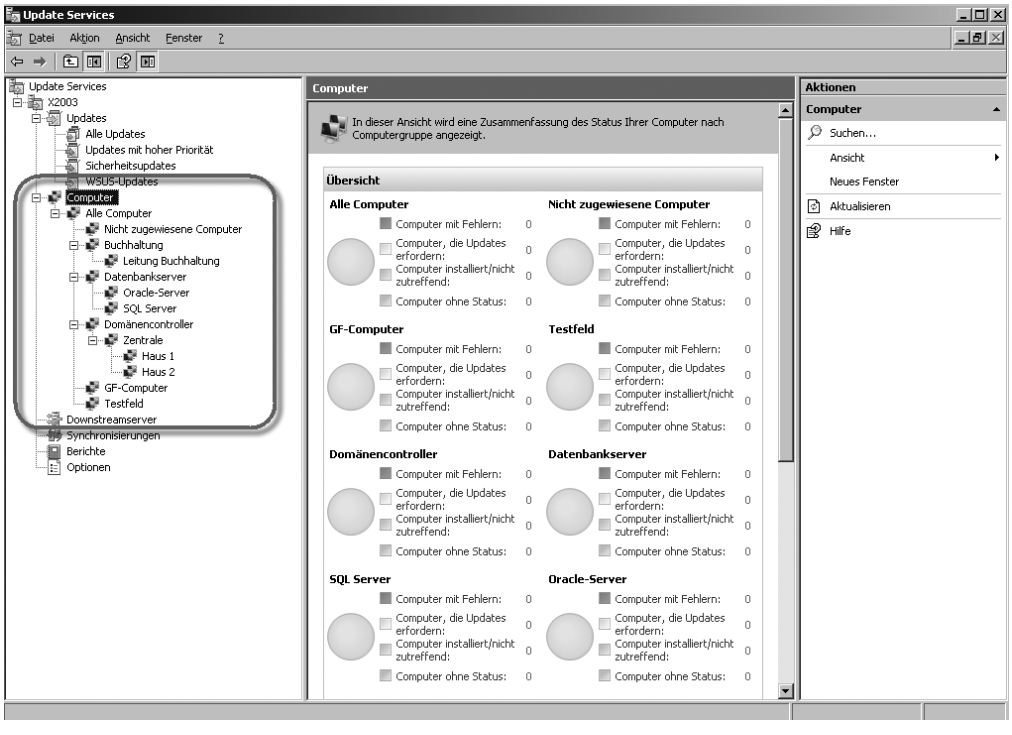
Ein WSUS 3.0-Server unterstützt bis zu 15.000 Clients und ein kürzeres Aktualisierungsintervall. Während sich ein WSUS 2.0-Server nur einmal am Tag mit Microsoft-Update synchronisieren konnte, kann dies ein WSUS 3.0-Server stündlich tun. Weitere Verbesserungen hat Microsoft bezüglich der Zuverlässigkeit integriert. WSUS 3.0 unterstützt Network Load Balancing (NLB), sowie SQL Server-Cluster. Microsoft liefert für WSUS 3.0 ein eigenes Management Pack für seinen Überwachungsserver Microsoft Operations Manager (MOM) mit aus. Mit dieser Überwachung können nicht nur Berichte abgefragt werden, sondern auch der Gesamtzustand der WSUS 3.0-Infrastruktur. Reporting-Berichte von WSUS 3.0 können in Excel importiert oder als PDF-Datei gespeichert werden. Für diese Speicherung sind keine zusätzlichen Tools notwendig, alle notwendigen Komponenten zur Speicherung von Berichten sind in der Standardinstallation von WSUS 3.0 integriert. Die Reporting-Möglichkeiten wurden im Vergleich zu WSUS 2.0 deutlich überarbeitet und erweitert. Die einzelnen Berichte bieten vielfältige Ansichtsmöglichkeiten, Kuchendiagramme und die Anzeige einzelner Updategruppen. Für die Ansicht von Berichten können ausführliche Filter definiert werden, die auch miteinander kombiniert werden können.

Abbildg. 23.8 Die Berichtsfunktion von WSUS wurde von Version 2.0 auf 3.0 stark erweitert



Die rechte Maustaste wird durchgängig unterstützt und bietet kontextsensitive angepasste Steuerungsmöglichkeiten. Die Verwaltung von WSUS 3.0 entspricht daher mittlerweile dem Microsoft-Standard, sodass ein schnelles Einlernen in die Verwaltung gegeben ist. Ebenfalls neu ist die Möglichkeit sich die Installations-Datei eines Hotfixes anzeigen zu lassen, sodass auf das Hotfix direkt über das Dateisystem zugegriffen werden kann, wenn dieses für einen PC gebraucht wird, der nicht an den WSUS angebunden ist. WSUS 3.0 unterstützt deutlich mehr Computergruppen, die für die Installation von Updates konfiguriert werden können. Im Gegensatz zu WSUS 2.0 können die Computergruppen in WSUS 3.0 weitere Gruppen enthalten, sodass auch eine Verschachtelung möglich wird. Durch diese neue Funktion können auch größere Unternehmen effizient eine Patch-Infrastruktur aufbauen und diese optimal an ihr Unternehmen anpassen. Darüber hinaus kann ein Computer auch Mitglied in mehreren Gruppen sein, damit er die Updates von mehreren Gruppen erhält. WSUS installiert nur die Patches für die Komponenten, die auf einem Server installiert sind. Auf einem Server ohne Exchange-Installation werden natürlich zum Beispiel keine Exchange-Patches installiert, nur weil dieser in der entsprechenden Gruppe ist. Wenn sich ein neuer Server beim WSUS anmeldet, werden ausführlichere Informationen angezeigt, als unter den Vorgängerversionen. WSUS 3.0 bietet die Möglichkeit, eigene Patches auch für selbst geschriebene Anwendungen zu verteilen. Diese Funktion wird sicherlich auch zukünftig von Anbietern anderer Software genutzt werden, um ihre Produkte über WSUS zu aktualisieren.

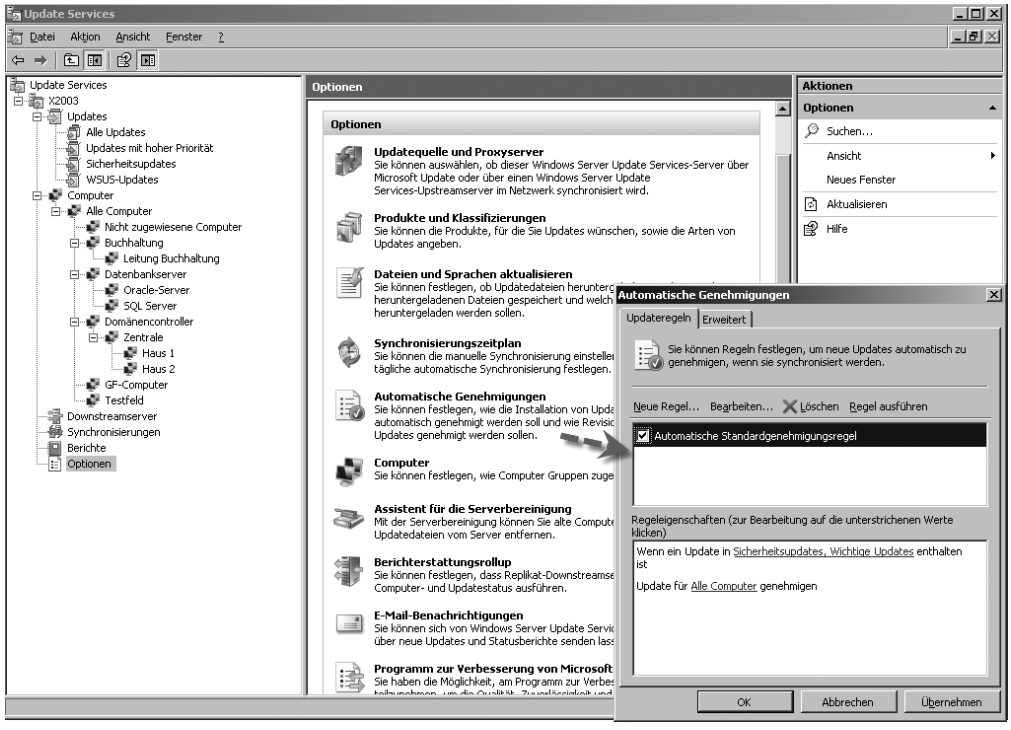
Abbildg. 23.9 In WSUS 3.0 können verschachtelte Gruppen erstellt werden, um Updates effizienter zu verteilen



Auch bei der Installations-Genehmigung (Approve Updates) von Aktualisierungen hat Microsoft Verbesserungen vorgenommen. Es können Regeln definiert werden, auf deren Basis automatische Installationen vorgenommen werden können. Zusammen mit den verschachtelten Gruppen und

den weiteren Möglichkeiten von WSUS 3.0 können Unternehmen jede noch so komplizierte Infrastruktur für die Aktualisierung von Updates einbinden. Nur genehmigte Updates werden auf die angebundenen Clients verteilt.

Abbildg. 23.10 In den Optionen können Regeln für das automatische Genehmigen von Updates erstellt werden



Die Hardwarevoraussetzungen von WSUS 3.0 sind im Großen und Ganzen identisch mit WSUS 2.0. Sie sollten natürlich über entsprechend freien Festplattenplatz verfügen (Microsoft empfiehlt ca. 30 GB, 10 GB sollten es mindestens sein), sowie mindestens 1 GB RAM und einem Prozessor mit mindestens 1 GHz. Die Daten des WSUS 3.0 werden auf einem SQL Server 2005 gespeichert, auf dem auch das SP1, besser SP2 für SQL Server 2005 installiert werden sollte. Wenn es in Ihrem Unternehmen noch keinen solchen Datenbankserver gibt, verwendet WSUS 3.0 die interne Windows-Datenbank von Windows Server 2008. Diese muss vor der Installation von WSUS 3.0 installiert werden. Windows Server 2008 hat bereits die MMC 3.0 standardmäßig integriert, sowie .NET Framework 3.0, welches von WSUS 3.0 ebenfalls unterstützt wird. Clientseitig unterstützt WSUS 3.0 Windows 2000 ab SP4, Windows XP ab SP1, Windows Vista, Windows Server 2003 (auch mit SP1, SP2 und R2), sowie Windows Server 2008 und eine Vielzahl weiterer Microsoft-Produkte. Diese Produkte werden bei der Einrichtung angezeigt und es kann ausgewählt werden, für welche Produkte der Dienst Updates aus dem Internet herunterladen soll. Die Installation kann auch, falls gewünscht, automatisiert und unbeaufsichtigt über die Befehlszeile durchgeführt werden. Dadurch wird für größere Unternehmen eine Remoteinstallation in den Niederlassungen möglich.

HINWEIS WSUS 3.0 kann nicht auf Servern installiert werden, auf denen der Terminaldienst läuft.

Installation von WSUS 3.0 SP1

Sind die entsprechenden Hardwarevoraussetzungen getroffen, gestaltet sich die Installation recht einfach. Im folgenden Abschnitt gehen wir mit Ihnen die Installation des Produktes durch. Zunächst muss die Installationsdatei des WSUS von der Seite *http://technet.microsoft.com/en-us/wsus/default.aspx* heruntergeladen werden. Wird WSUS 3.0 auf einem Server unter Windows Server 2008 installiert, muss zuvor die Funktion der internen Windows-Datenbank installiert werden, sowie die Serverrolle *Webserver*. Darüber hinaus muss der Rollendienst für *ASP* sowie der Kompatibilitätsmodus für IIS 6.0 aktiviert sein. Auch das Feature *.NET Framework 3.0* muss vor der Installation von WSUS unter Windows Server 2008 installiert werden. Alle Voraussetzungen werden über den Server-Manager durchgeführt.

HINWEIS Nur WSUS 3.0 SP1 ist kompatibel für die Installation unter Windows Server 2008. Ohne das SP1 kann WSUS 3.0 zwar Patches für Windows Server 2008 herunterladen und verteilen, selbst aber nicht unter Windows Server 2008 installiert werden.

WSUS 3.0 installieren

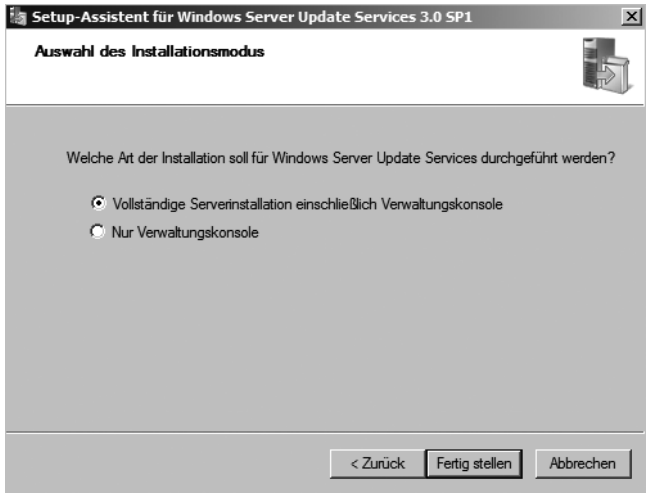
Der nächste Schritt bei der Installation ist der Doppelklick auf die Installationsdatei. Im Anschluss startet der Installationsassistent von WSUS 3.0.

Abbildg. 23.11 Starten der Installation von WSUS 3.0 SP1 unter Windows Server 2008

Auf der nächsten Seite des Assistenten wird ausgewählt, ob der vollständige Server oder nur die Verwaltungskonsole für den WSUS installiert werden soll. Sie können über diesen Weg die Verwal-

tungskonsole auch auf einen normalen PC installieren. Dazu wird .NET Framework 2.0 benötigt. Neben Windows Server 2003/2008 wird auch Windows XP und Windows Vista zur Installation der Verwaltungskonsole unterstützt. Nachdem die Installation des Servers ausgewählt wurde, müssen noch die obligatorischen Lizenzbedingungen akzeptiert werden.

Abbildg. 23.12 Auswählen der Installationsvariante von WSUS 3.0



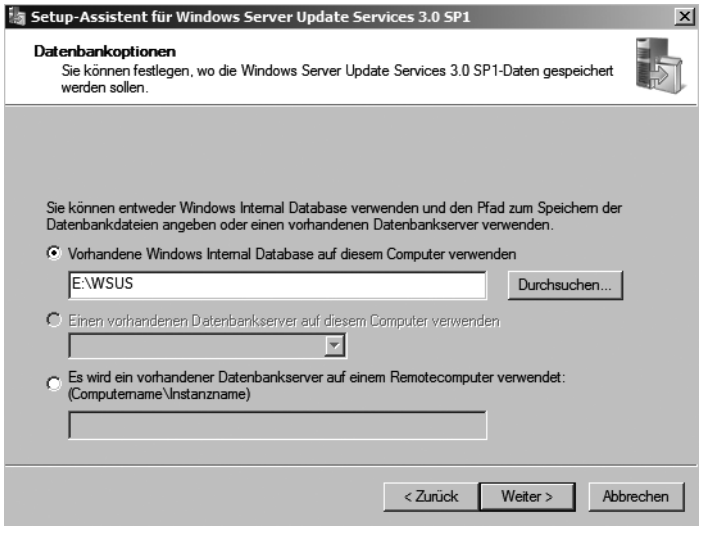
Auf der nächsten Seite erscheint eventuell eine Warnung, dass die Software *Microsoft Report Viewer Redistributable 2005* nicht auf Ihrem Server installiert ist. Sollte dies bei Ihnen der Fall sein, bestätigen Sie die Meldung. Die Software kann ohne weiteres nach der Installation von WSUS 3.0 nachinstalliert werden. Microsoft stellt das Tool ebenfalls kostenlos zur Verfügung (*http://www.microsoft.com/downloads/details.aspx?familyid=8a166cac-758d-45c8-b637-dd7726e61367&displaylang=en*). Diese Erweiterung wird von der neuen Berichtsfunktion von WSUS 3.0 benötigt. Zur Einrichtung des Servers oder der Verwaltung wird die Software nicht benötigt. Werden Berichte aus der Verwaltungskonsole gestartet, erscheint eine Fehlermeldung, wenn *Microsoft Report Viewer Redistributable 2005* nicht installiert ist. Bei der nachträglichen Installation funktionieren die Berichte nach einem Neustart der Verwaltungskonsole.

Im nächsten Schritt muss das Verzeichnis ausgewählt werden, in dem WSUS installiert werden soll. Das Verzeichnis muss mindestens über 6 GB freien Festplattenplatz verfügen, besser deutlich mehr, da hier die Installationsdateien der Sicherheitspatches abgelegt werden. Microsoft empfiehlt 20 bis 30 GB freien Plattenplatz für einen WSUS-Server. Idealerweise verfügt ein Server dazu über ein eigenes Laufwerk, auf dem genügend Platz bereitgestellt wird. Außerdem muss die Partition mit den WSUS-Daten im NTFS-Format formatiert sein. Steht nicht genügend Festplattenplatz zur Verfügung, lässt sich das lokale Speichern der Patchdateien auch deaktivieren. Dies macht allerdings keinen Sinn, da in diesem Fall bei der Verteilung der Patches diese zunächst aus dem Internet heruntergeladen werden müssen. Da Speicherplatz heutzutage keine gravierenden Kosten mehr verursacht, bietet sich die lokale Speicherung an.

Der nächste Schritt besteht in der Auswahl des SQL Servers, auf dem die Konfigurationsdaten und Berichte von WSUS gespeichert werden. Ist im Unternehmen ein SQL Server im Einsatz, können Sie

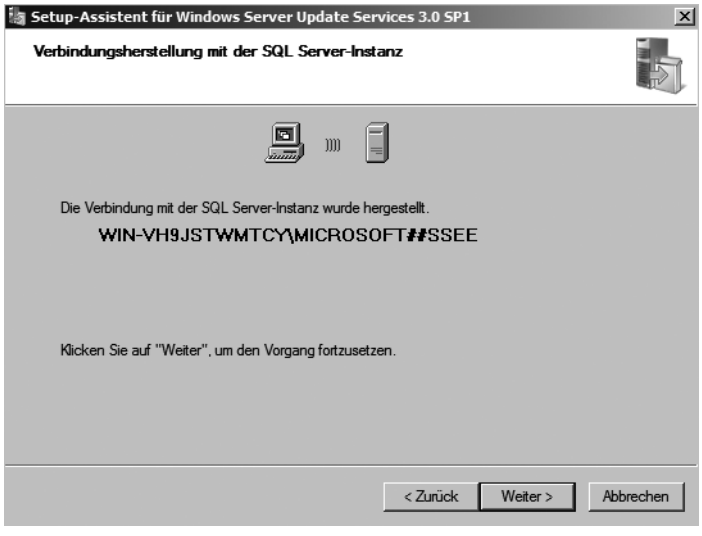
auf diesem eine eigene Instanz für den WSUS installieren. Alternativ kann WSUS 3.0 die interne Windows-Datenbank von Windows Server 2008 verwenden.

Abbildg. 23.13 Auswahl der Datenbankoptionen von WSUS



Nach dieser Auswahl testet der Installationsassistent, ob die konfigurierte Datenbankinstanz erreicht werden kann. Die Verbindung zum Server muss fehlerfrei hergestellt werden können.

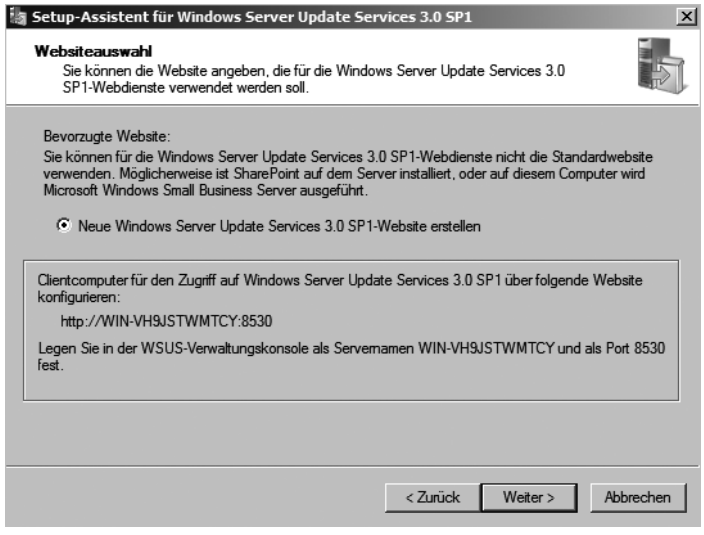
Abbildg. 23.14 WSUS verbindet sich mit der internen Windows-Datenbank



Auch wenn die Verwaltung von WSUS 3.0 hauptsächlich mit der neuen MMC 3.0 durchgeführt wird, benötigt der Serverdienst eine eigene Webseite. Die MMC verbindet sich zur Verwaltung mit

dieser Webseite und stellt die notwendigen Informationen in der Oberfläche dar. Aus diesem Grund kann entweder der Standardport und die Standardseite des Webservers zur Kommunikation verwendet oder eine neue Seite erstellt werden. Sie sollten möglichst immer eine eigene Seite erstellen, über die WSUS erreichbar ist. Dadurch ist auf dem Webserver noch Platz für andere Anwendungen, die unter Umständen später noch auf dem Server installiert werden.

Abbildg. 23.15 Erstellen einer neuen Website für WSUS

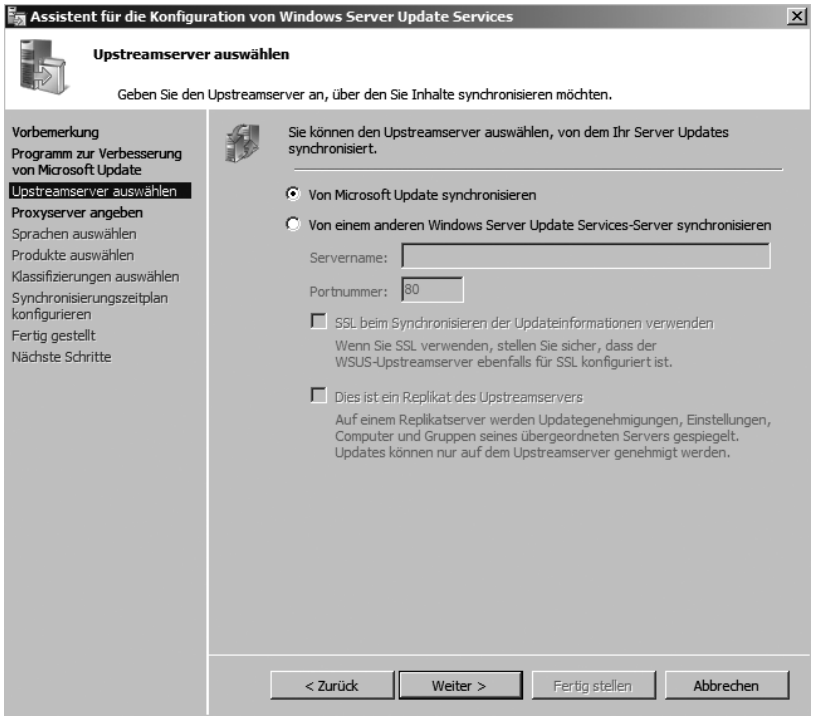


Anschließend wird noch eine Zusammenfassung angezeigt und die Installation gestartet. Nach einigen Minuten wird der Installationsassistent abgeschlossen und automatisch der Assistent für die Einrichtung von WSUS angezeigt. Über diesen Assistenten kann der Server nahezu vollständig eingerichtet werden.

WSUS 3.0 konfigurieren

Während der Einrichtung sehen Sie bereits, wie viele Produkte und Komponenten WSUS 3.0 unterstützt. Der Assistent zur Einrichtung von WSUS startet nach der Installation automatisch. Im Rahmen der Einrichtung mit dem Assistenten kann ausgewählt werden, für welche Produkte Aktualisierungen von WSUS heruntergeladen und bereitgestellt werden sollen. Auf der ersten Seite des Assistenten zur Einrichtung von WSUS 3.0 erhalten Sie zunächst allgemeine Informationen über die Voraussetzungen in der Infrastruktur. So muss ein WSUS-Server eine Verbindung zum Internet oder zu anderen WSUS-Servern herstellen können, um die Clients mit Sicherheitspatches zu versorgen. Als Nächstes kann ausgewählt werden, ob Sie am Programm zur Verbesserung von Microsoft Update teilnehmen wollen. Anschließend wird festgelegt, wo der WSUS-Server seine Aktualisierungen herunterladen soll. Werden im Unternehmen mehrere WSUS-Server eingesetzt, kann ein einzelner als so genannter Upstreamserver konfiguriert werden. Ein solcher Upstreamserver lädt die Patches aus dem Internet und stellt sie anderen WSUS-Servern bereit. Diese arbeiten dann in der Funktion als Downstreamserver. Der erste installierte WSUS-Server muss sich immer aus dem Internet aktualisieren und ist entsprechend ein Upstreamserver.

Abbildg. 23.16 Konfigurieren der Synchronisierungsquelle für WSUS 3.0



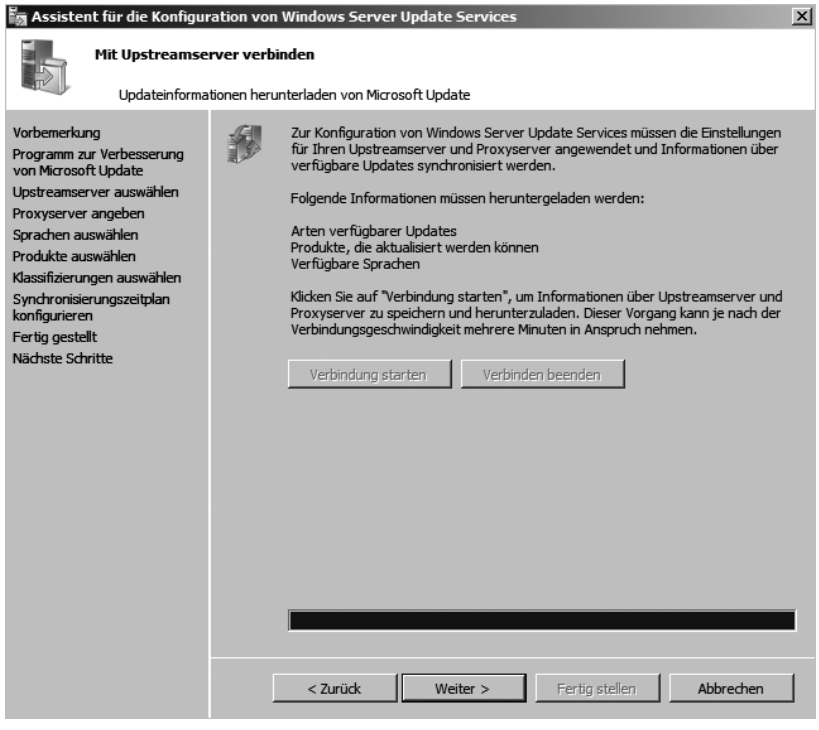
Im Anschluss wird konfiguriert, ob der WSUS-Server eine eigenständige Verbindung zum Internet besitzt oder die Verbindung über einen Proxyserver aufbaut. Wird der Verbindungsaufbau über einen Proxyserver vorgenommen, sollten Sie einen eigenen Benutzer in der Domäne für den WSUS-Server anlegen und diesen entsprechend berechtigen. Wurde die Auswahl der Internetverbindung getroffen, muss zunächst getestet werden, ob der WSUS-Server eine Verbindung zum Internet aufbauen kann. Klicken Sie dazu im Assistent auf die entsprechende Schaltfläche. Erst nach einem erfolgreichen Verbindungsaufbau lässt sich der Assistent fortsetzen.

TIPP Da die Aufgabe des WSUS darin besteht, Patches aus dem Internet herunterzuladen, muss dem Server der Zugriff auf das Internet ermöglicht werden. WSUS muss zum einen mit dem Internet kommunizieren können, zum anderen mit den Clients, um Updates zu verteilen. Wenn Sie eine interne Firewall einsetzen oder der WSUS in einer DMZ steht, muss der Port 80 (HTTP) zu diesem Server geöffnet werden, damit sich Clientcomputer mit dem Server verbinden können. WSUS muss zusätzlich mit den beiden Ports 80 und 443 eine Verbindung ins Internet herstellen können. Wird der Server darüber hinaus per SSL verwaltet, muss vom internen Netzwerk der Port 443 zum WSUS-Server geöffnet werden. Soll WSUS nur auf die Seiten im Internet Zugriff erhalten, wo die Updates heruntergeladen werden, kann die Firewall so konfiguriert werden, dass WSUS nur zu den Seiten Verbindung aufnehmen kann, die Microsoft zum Übertragen von Patches benötigt. Dazu müssen in der Firewall folgende Seiten freigeschaltet werden, alle anderen Seiten können blockiert werden:

- http://windowsupdate.microsoft.com
- http://*.windowsupdate.microsoft.com

- https://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com
- http://*.windowsupdate.com
- http://download.windowsupdate.com
- http://download.microsoft.com
- http://*.download.windowsupdate.com
- http://wustat.windows.com
- http://ntservicepack.microsoft.com

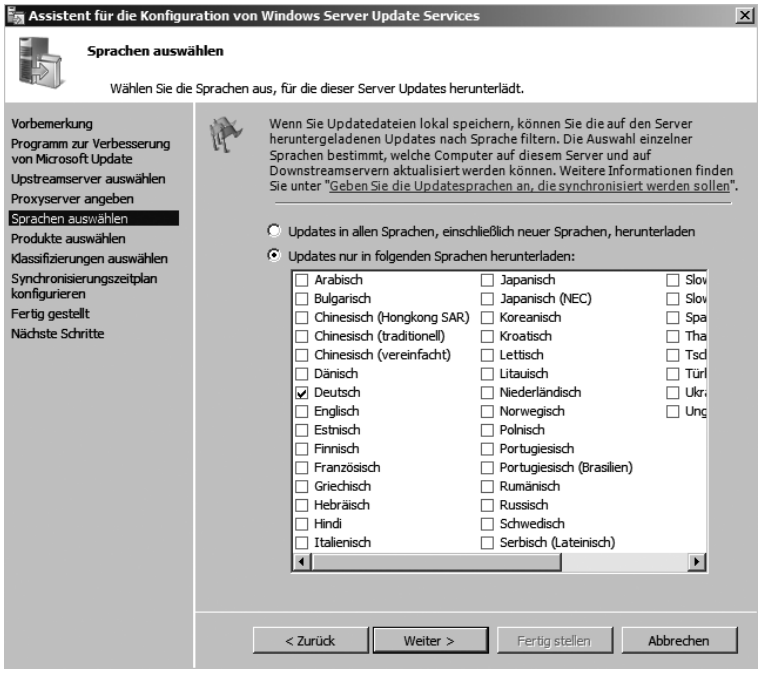
Abbildg. 23.17 Testen der Internetverbindung von WSUS



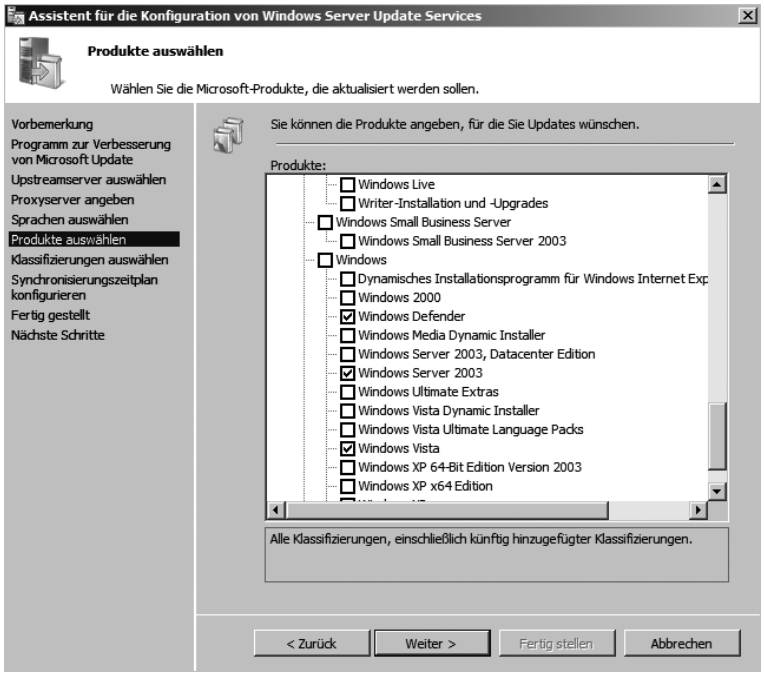
Als Nächstes kann ausgewählt werden, in welchen Sprachen die Patches heruntergeladen werden sollen (Abbildung 23.18). Unternehmen, die nur eine Sprachversion von Windows einsetzen, wählen hier die entsprechende Sprache aus. Werden mehrere Sprachen eingesetzt, kann WSUS auch für diese Sprachen die entsprechenden Updates herunterladen, allerdings erhöht sich dadurch auch die Menge an Patches.

Nun erscheint eines der wichtigsten Fenster (Abbildung 23.19). Hier wird ausgewählt, welche Produkte durch den WSUS aktualisiert werden sollen. Aktivieren Sie in diesem Fenster alle Produkte, die im Unternehmen eingesetzt werden. Entfernen Sie das Häkchen bei jenen Produkten, die nicht aktualisiert werden sollen, da somit Bandbreite und Synchronisierungszeit gespart werden kann.

Abbildg. 23.18 Auswählen der Sprachen, für die WSUS Patches herunterladen soll

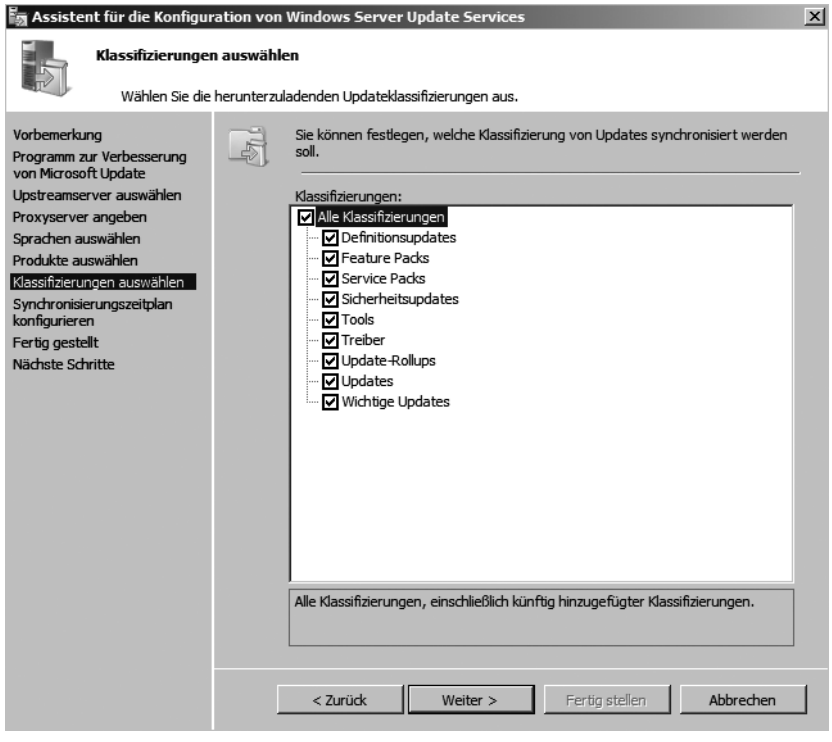


Abbildg. 23.19 Auswählen der Produkte, für die WSUS Patches herunterladen soll



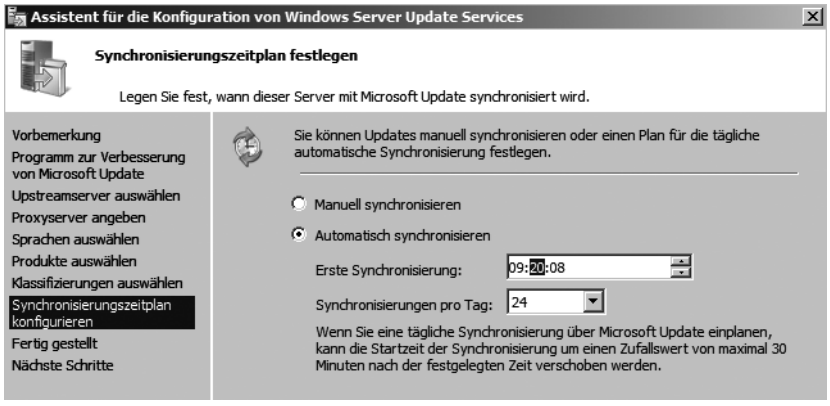
Im nächsten Fenster des Assistenten können die Klassifizierungen der Patches ausgewählt werden. Hier lässt sich konfigurieren, welche Art der Patches für die ausgewählten Produkte durch den WSUS bereitgestellt werden sollen. Grundsätzlich bietet es sich an, alle Klassifizierungen auszuwählen und besser die Produkte einzuschränken, die aktualisiert werden sollen.

Abbildg. 23.20 Auswählen der Patchtypen, die heruntergeladen werden sollen



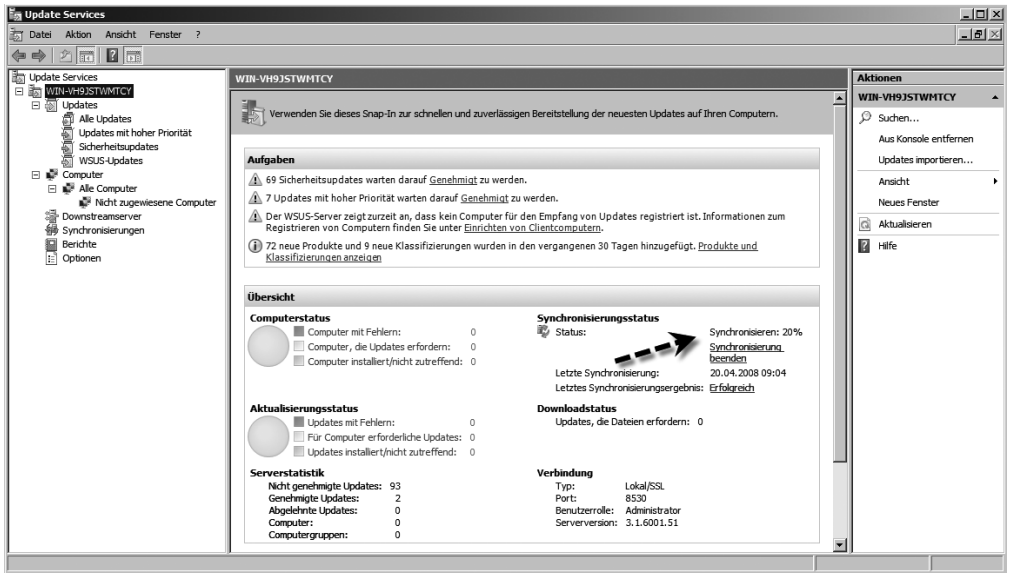
Im nächsten Schritt des Assistenten wird festgelegt, wann sich der WSUS-Server mit dem Internet oder anderen WSUS-Servern synchronisieren soll. Neben einer Uhrzeit kann hier auch festgelegt werden, wie oft an einem Tag die Synchronisierung durchgeführt werden soll. Diese Funktion ist neu in WSUS 3.0. Liegen keine aktuellen Patches vor, wird auch kein Download durchgeführt. Sind jedoch neue Patches erhältlich, sollte auch eine Aktualisierung durchgeführt und die neuen Patches an die Clients verteilt werden.

Abbildg. 23.21 WSUS kann sich mehrmals am Tag mit Patches versorgen. Die Vorgängerversion WSUS 2.0 war dazu nur einmal am Tag in der Lage.



Zum Abschluss der Konfiguration kann noch die Verwaltungskonsole gestartet werden und die erste Synchronisierung starten. Über den Eintrag *Synchronisierungen* wird in der Verwaltungskonsole angezeigt, ob der Vorgang erfolgreich war.

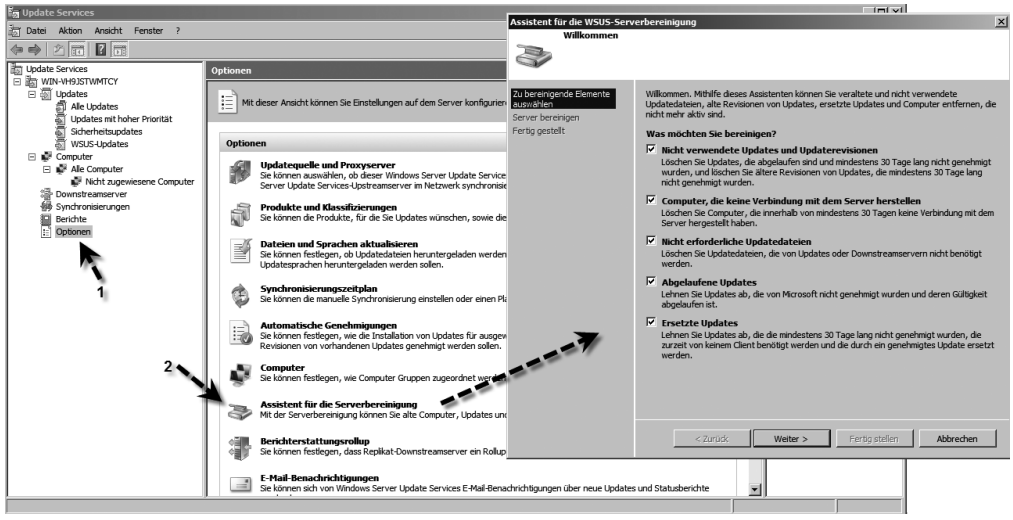
Abbildg. 23.22 Nach der Ersteinrichtung beginnt WSUS mit der Synchronisierung



TIPP Mit dem neuen *Server Cleanup Wizard* kann der Server bereinigt werden. Unter WSUS 2.0 musste hier noch die Befehlszeile bemüht werden. Auf diesem Weg können zum Beispiel Updates für Produkte, die nicht mehr eingesetzt werden, oder alte Versionen, vom Server gelöscht werden. Über den Assistenten zur Bereinigung können darüber hinaus PCs aus der Datenbank gelöscht werden, die sich nicht mehr am WSUS angemeldet haben. Veraltete oder abgelehnte Updates lassen sich löschen und weitere Bereinigungsmaßnahmen durchführen. Ein

Assistent führt durch diese Bereinigung, sodass keine unnötigen Daten auf dem Server verbleiben. Dieser Assistent wird in der Konsolenstruktur über den Eintrag *Optionen* und einen Klick auf *Assistent für die Serverbereinigung* gestartet.

Abbildg. 23.23 WSUS 3.0 verfügt über eine interne Reinigungsroutine, die über die Verwaltung in den Optionen gestartet werden kann



Anbindung der Client-Computer über Gruppenrichtlinien

WSUS 3.0 scannt heruntergeladene Updates und referenziert diese automatisch mit den verbundenen Clients. So können Berichte erstellt werden, die für einzelne Updates die Systeme in Ihrem Netzwerk ausgeben, auf denen das Hotfix installiert werden sollte. Über die Konsole kann auch erkannt werden, welche Server sich von diesem Updateserver synchronisieren (so genannte Downstreamserver). In den Optionen des Servers kann bereits auf den ersten Blick erkannt werden, dass Microsoft zahlreiche Neuerungen integriert hat, die an dieser Stelle konfiguriert werden können. Alle Optionen der WSUS 3.0 werden über die MMC erreicht, es sind keine verschiedenen Verwaltungswerkzeuge mehr notwendig. Wird eine Option aufgerufen, öffnet sich ein Dialogfeld mit verschiedenen Registerkarten, auf denen Einstellungen vorgenommen werden können.

Neue Gruppenrichtlinien-Vorlage für WSUS 3.0

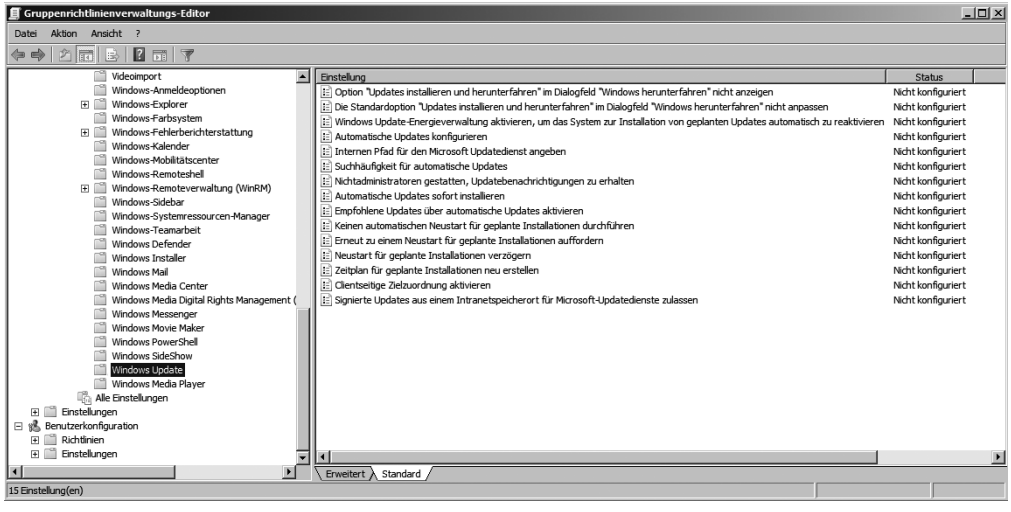
Mit WSUS 3.0 werden auch neue Einstellungen über eine neue Grupenrichtlinien-Vorlage (*wuau.adm*) für die Anbindung von Clients über Gruppenrichtlinien mitgeliefert. Diese Vorlage stellt wesentlich mehr Funktionen zur Verfügung, also die Vorgängerversion, zum Beispiel Funktionen für den Energiesparmodus von Windows Vista. Die **.adm*-Datei der neuen Gruppenrichtlinienvorlage wird im Installationsverzeichnis von WSUS abgelegt. Normalerweise befindet sich die Vorlage *wuau.adm* im Verzeichnis *C:\Programme\Update Services\ADM\deu*. Die Vorlage kann

durch einen Klick mit der rechten Maustaste auf den Konsoleneintrag *Administrative Vorlagen* im Gruppenrichtlinien-Editor hinzugefügt werden. Auf Servern mit installiertem SP2 für Windows Server 2003 oder Windows Server 2008 und Windows Vista sind die neuen Einstellungen bereits integriert.

Gruppenrichtlinien für die Anbindung von Clients

Damit die Clients Updates installieren, müssen diese so konfiguriert werden, dass sie keine Patches aus dem Internet herunterladen, sondern den internen WSUS verwenden. WSUS verteilt die Patches nicht automatisch an die Clients, sondern lädt die Aktualisierungen nur aus dem Internet herunter und stellt diese bereit. Die Clients holen die Patches selbst vom WSUS-Server und installieren diese automatisch, abhängig von den lokalen Einstellungen beziehungsweise den Einstellungen in den Gruppenrichtlinien. Um Arbeitsstationen und Server mit Patches zu versorgen, werden am besten spezielle Gruppenrichtlinien erstellt: Die Konfiguration der automatischen Updates in den Gruppenrichtlinien wird in der Gruppenrichtlinienverwaltung von Windows Server 2008, beziehungsweise der Gruppenrichtlinienverwaltungskonsole (Group Policy Management Console, GPMC) unter Windows Server 2003 unter *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Windows Update* gefunden.

Abbildg. 23.24 Anbinden der Clients über Gruppenrichtlinien an den WSUS



Die Arbeitsstationen lassen sich so konfigurieren, dass die Aktualisierungen automatisch vom WSUS heruntergeladen und installiert werden. Die Gruppenrichtlinie für die Server kann so konfiguriert werden, dass die Patches heruntergeladen, aber nicht automatisch installiert, sondern erst angezeigt werden. Ein Administrator erkennt bei der regelmäßigen Überwachung, dass neue Patches verfügbar sind und kann diese in einem Rutsch installieren. Grundsätzlich lässt sich die Konfiguration der automatischen Updates in drei Bereiche untergliedern:

- Automatisches Herunterladen der Patches vom WSUS auf den Rechner, aber keine Installation, nur die Meldung, dass Patches installiert werden können. Diese Einstellung kann für Server empfohlen werden.
- Meldung, dass neue Patches auf dem WSUS zur Verfügung stehen, aber kein Herunterladen der Patches auf den lokalen Computer. Diese Einstellung wird nicht empfohlen, da der Download das System nicht belastet und so die Patches schneller zur Installation zur Verfügung stehen.
- Automatisches Herunterladen und automatische Installation der Patches. Dies ist die optimale Einstellung für Arbeitsstationen.

Sie müssen selbst entscheiden, für welche PCs und Server Sie welche Option verwenden. Für jede Organisationseinheit (OU) in der Windows-Domäne und der zu Grunde liegenden Richtlinie können gesonderte Einstellungen vorgenommen werden. Wenn PCs oder Server in die entsprechende OU verschoben werden, sind die Geräte anhand der Konfiguration automatisch mit den entsprechenden Patches versorgt. Gehen Sie bei der Untergliederung am besten folgendermaßen vor:

1. Erstellen Sie eine OU, in der Sie die Server aufnehmen. Belassen Sie die Domänencontroller aber in der OU *Domain Controllers*. da es für diese OU bereits eine spezielle Richtlinie für Domänecontroller gibt (*Default Domain Controller Policy*).
2. Erstellen Sie eine OU für die Arbeitsstationen. Diese OU kann beliebig viele weitere Unter-OUs enthalten; die Konfigurationen für die Windows-Updates werden ganz oben vorgenommen.
3. Erstellen Sie zwei Gruppenrichtlinien, eine für die Server und eine für die Arbeitsstationen.
4. Führen Sie die Einstellungen für die automatischen Updates in den Gruppenrichtlinien durch (siehe den folgenden Abschnitt).
5. Verknüpfen Sie die Gruppenrichtlinie für die Server mit der OU für die Server und der OU *Domain Controllers*.
6. Verknüpfen Sie die Gruppenrichtlinie für die Arbeitsstationen mit der OU, in der sich die Arbeitsstationen befinden.

Navigieren Sie zur Konfiguration zu den Einstellungen der automatischen Updates unter *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Windows Update*. Hier können die notwendigen Einstellungen vorgenommen werden, durch die sich die Clients später automatisch vom WSUS-Server aktualisieren.

Die erste Option ist *Internen Pfad für den Microsoft Updatedienst angeben*. Diese Option wird zuerst aktiviert. Dann wird festgelegt, mit welchem WSUS-Server sich die Clients verbinden. Da der WSUS eine Webapplikation ist, muss der Servername mit einer HTTP-Adresse angegeben werden, zum Beispiel *http://<SERVERNAME>*.

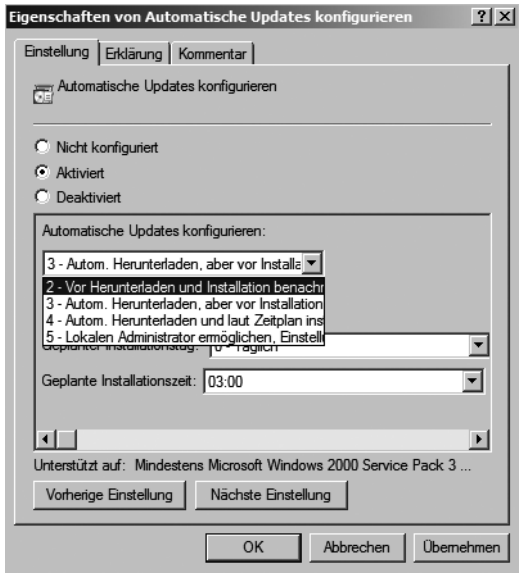
Abbildg. 23.25 Festlegen des Pfads zum internen WSUS

Die zweite wichtige Option ist das Updateverhalten, das über *Automatische Updates konfigurieren* eingestellt werden kann. Dabei stehen hauptsächlich folgende Möglichkeiten zur Verfügung:

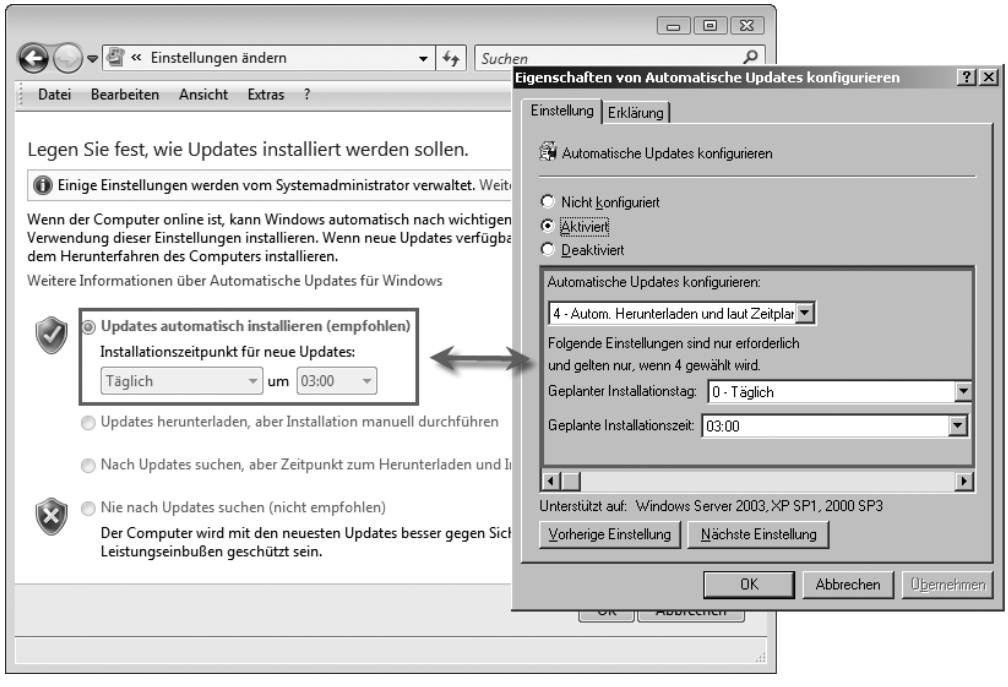
- **Vor Herunterladen und Installation benachrichtigen** Mit dieser Option wird ein angemeldeter Administrator vor dem Download und vor der Installation der Updates benachrichtigt, sobald ein neues Patch auf dem WSUS vorhanden ist. Dazu wird ein Symbol in der Taskleiste angezeigt, das dem Symbol entspricht, mit dem darauf hingewiesen wird, wenn Aktualisierungen im Internet zur Verfügung stehen.
- **Autom. Herunterladen, aber vor Installation benachrichtigen** Mit dieser Option wird das Herunterladen der Updates automatisch vom Client durchgeführt. Anschließend wird ein angemeldeter Administrator benachrichtigt und kann die Installation manuell durchführen. Da sich die Updates bereits auf dem Server befinden, geht die Installation sehr schnell vonstatten.
- **Autom. Herunterladen und laut Zeitplan installieren** Mit dieser Installation versorgt sich der Client vollkommen automatisch mit den notwendigen Updates. Wenn die Clients zum Zeitpunkt der Aktualisierung nicht eingeschaltet sind, wird die Installation automatisch nachgeholt, sobald der PC wieder eingeschaltet wird.
- **Lokalen Administrator ermöglichen, Einstellung auszuwählen** Mit dieser Option wird zugelassen, dass lokale Administratoren mit Hilfe der Option *Automatische Updates* in der Systemsteuerung die Konfiguration selbst auswählen können.

Ebenfalls interessant ist die neue Funktion, die Energieverwaltung von Windows Vista zusammen mit der Anbindung an den WSUS über Gruppenrichtlinien zu steuern. Der PC wird dazu automatisch reaktiviert, wenn Windows Update zur automatischen Installation von Updates konfiguriert ist. Wenn sich das System zum Zeitpunkt der geplanten Installation im Ruhezustand befindet, wird das System mit dem Windows-Energieverwaltungsfeature automatisch gestartet, um die Updates zu installieren. Wenn sich das System zum Zeitpunkt der Reaktivierung im Akkubetrieb befindet, werden keine Updates installiert.

Abbildg. 23.26 Konfigurieren des Updateverhaltens der Clients

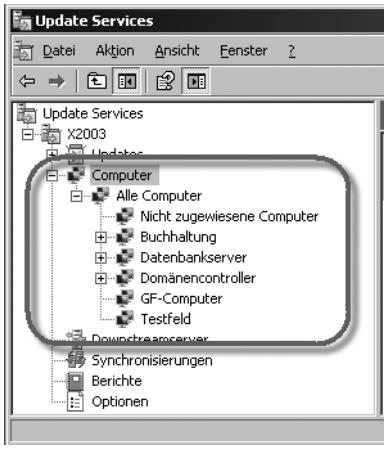


Abbildg. 23.27 Bei der Anbindung an WSUS werden lokale Einstellungen gesetzt und Änderungsmöglichkeiten deaktiviert



Durch die Einstellung *Clientseitige Zielzuordnung aktivieren* kann die Gruppe eingegeben werden, in welcher sich der Client am WSUS anmelden soll. Dazu müssen in der Verwaltung auf dem WSUS entsprechende Gruppen angelegt werden. Da ein Computer Mitglied mehrerer Gruppen in WSUS 3.0 sein darf, können Sie in der Gruppenrichtlinie auch mehrere Gruppen angeben. Trennen Sie die Bezeichnung durch ein Semikolon (;). Basierend auf diesen Gruppen kann konfiguriert werden, welche Patches auf den einzelnen Computern der Gruppe installiert werden. Es gibt zwei Standardcomputergruppen: *Alle Computer* und *Nicht zugeordnete Computer*. Standardmäßig wird jeder Client beiden Gruppen zugeordnet, sobald dieser zum ersten Mal eine Verbindung mit dem WSUS-Server herstellt. Das Erstellen von Computergruppen bietet den Vorteil, dass Updates vor der Bereitstellung auf produktiven Systemen getestet werden können. Neben der Möglichkeit der Konfiguration per Gruppenrichtlinie können Clients auch manuell in der Verwaltungskonsole der Windows Server Update Services in die Gruppen aufgenommen werden. Generell ist eine Automatisierung aber immer am besten, da dadurch bereits durch die Zuordnung eines Clients zu seiner OU festgelegt wird, welche Patches er erhält, und kein doppelter Aufwand notwendig ist.

Abbildg. 23.28 In der WSUS-Verwaltung können neben den Standardgruppen beliebig zusätzliche Gruppen angelegt werden. Die Clients werden manuell in die Gruppen verschoben oder über die entsprechenden Einstellungen in der Gruppenrichtlinie.



Problemlösungen bei der Client-Anbindung

Nach der Konfiguration der Gruppenrichtlinie kann es eine Weile dauern, bis die Arbeitsstationen und Server mit dem WSUS verbunden sind und in der Administrationsoberfläche des WSUS angezeigt werden. Auf den einzelnen Rechnern kann in der Befehlszeile durch Eingabe des Befehls *wuauclt.exe /detectnow* eine sofortige Verbindung zum WSUS erzwungen werden. Sollten die Einstellungen in der Gruppenrichtlinie auf einem Computer noch nicht angezeigt werden, wurde unter Umständen die Gruppenrichtlinie noch nicht angewendet. In diesem Fall kann mit dem Befehl *gpupdate /force* das Aktualisieren der Gruppenrichtlinie auf dem Client erzwungen werden. Sollten einige Rechner auch nach dieser Zeit nicht angezeigt werden, versuchen Sie folgende Problemlösung:

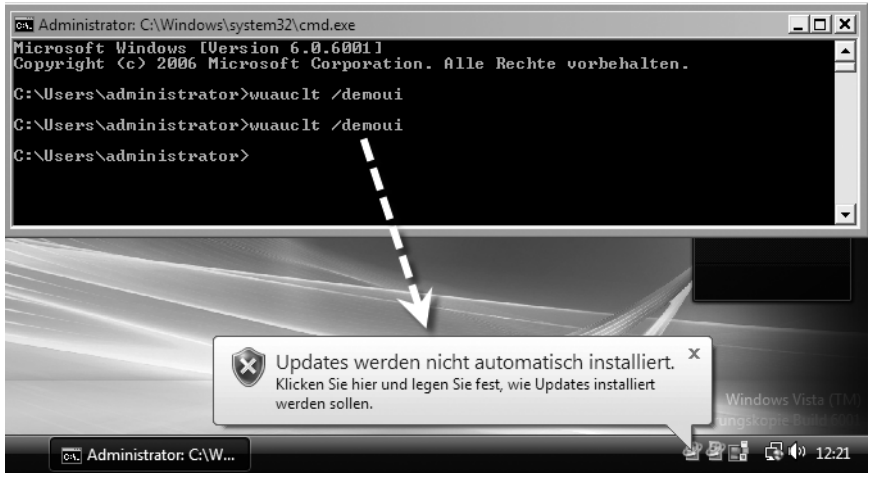
1. Auf dem Computer, der nicht im WSUS angezeigt wird, benennen Sie die Datei *\windows\system32\wuaueng.dll* in *wuaueng.old* um.

2. Kopieren Sie danach die Datei *wuaueng.dll* des WSUS-Servers aus dem gleichen Verzeichnis auf den fehlenden Computer.
3. Starten Sie diesen Computer neu.
4. Nach dem Anmelden sollten die Dateien, die mit *wu** beginnen, im Verzeichnis *\Windows\system32* ebenfalls aktualisiert worden sein.
5. Geben Sie in der Befehlszeile den Befehl *wuauclt.exe /detectnow* ein.

Sollte das nicht funktionieren, können noch im Registryschlüssel *HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/WindowsUpdate* die Einträge für den WSUS gelöscht werden. Anschließend sollte der Befehl *wuauclt /detectnow /reauthorization* eingegeben werden und die Verbindung wieder funktionieren. Auf den Clients kann sichergestellt werden, dass die Richtlinie funktioniert, wenn in den Einstellungen für die automatischen Updates die Einstellungen der Gruppenrichtlinie übernommen wurden. Das Tool gehört zu den Bordmitteln und kann daher auf jedem dieser Systeme verwendet werden. Folgende Optionen sind möglich:

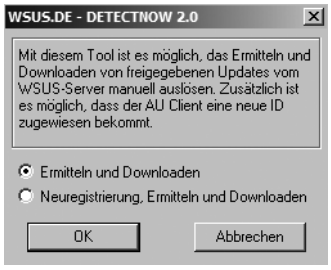
- **/ReportNow** Übermittelt den Status des Clients an den Server
- **/ShowSettingsDialog** Zeigt das Einstellungsfenster für automatische Updates an
- **/ShowWU** Zeigt die Windows Update-Seite des Computers an
- **/DemoUI** Zeigt eine Demomeldung mit Einstellungsmöglichkeiten an, um eine Benachrichtigung zu simulieren

Abbildg. 23.29 Anzeigen von Meldungen mit der Option *DemoUI* von *wuauclt.exe*



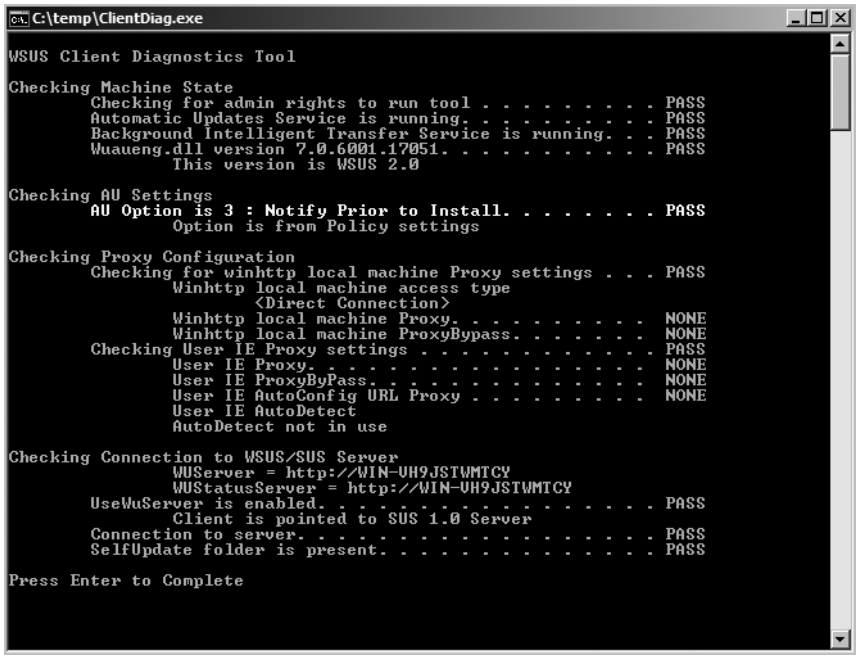
Mit dem kostenlosen Zusatztool *WSUS DETECTNOW 2.0* von der Internetseite *www.wsus.de* kann das Herunterladen von Aktualisierungen auf dem Client manuell gestartet werden. Außerdem lässt sich mit dem Tool eine neue ID für den Client erzeugen, falls die Anbindung nicht funktioniert.

Abbildg. 23.30 Clientanbindung reparieren und Patches manuell herunterladen mit *WSUS DETECTNOW*



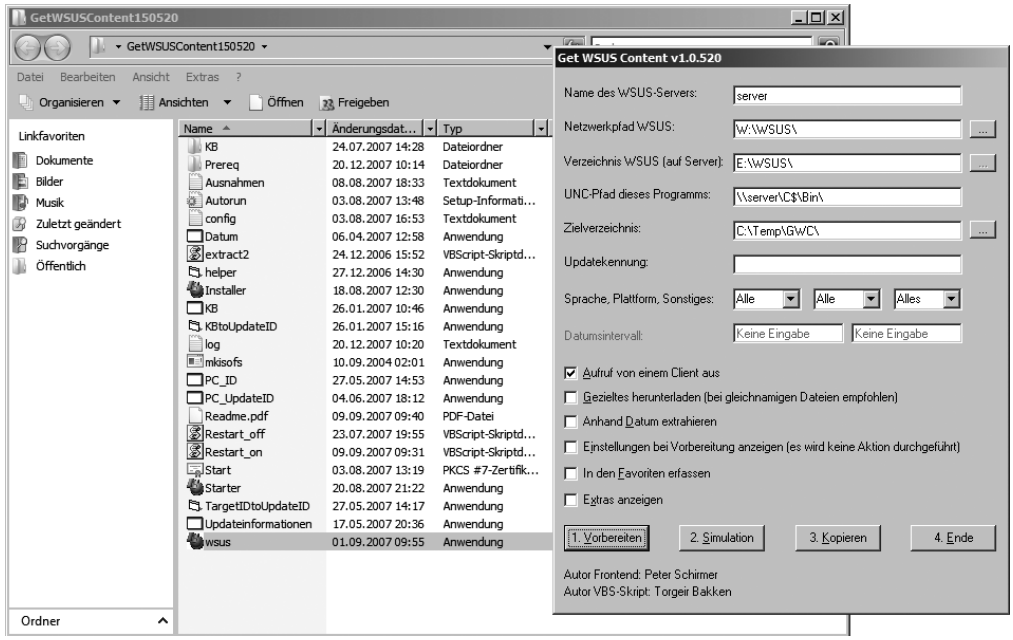
Ein ebenfalls wichtiges Hilfsmittel für die Diagnose von Clientproblemen ist das *WSUS Client Diagnostics Tool* von Microsoft (*http://technet.microsoft.com/en-us/wsus/bb466192.aspx*). Es ermittelt in der Befehlszeile, ob die Anbindung an den Server funktioniert und teilt eventuelle Probleme mit.

Abbildg. 23.31 Client mit dem *WSUS Client Diagnostics Tool* überprüfen



Mit dem Tool *Get WSUS Content*, ebenfalls von der Internetseite *www.wsus.de* herunterladbar, können Updates vom WSUS-Server über eine grafische Oberfläche und ohne Installation des Tools heruntergeladen und installiert werden. Mit dem enthaltenen Offline-Installer werden Patches vom Server heruntergeladen, die der Administrator freigegeben hat, und Sie können ein Medium erstellen lassen. Dieses kann zum Beispiel zu Außendienstmitarbeitern geschickt werden. Zur Installation dieser Patches muss der Client nicht mit dem WSUS-Server verbunden sein.

Abbildg. 23.32 Erstellen von Offline-Medien und Verwalten der Patches über *Get WSUS Content* von *www.wsus.de*

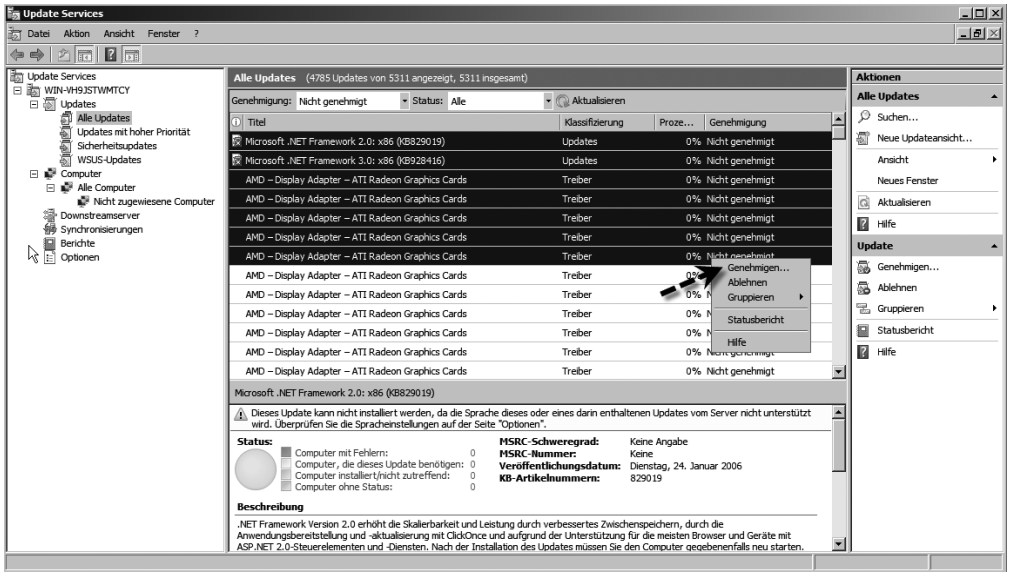


Genehmigen und Bereitstellen von Updates

WSUS lädt die konfigurierten Updates basierend auf den vorgenommenen Spracheinstellungen, Produkten und Klassifizierungen aus dem Internet herunter, installiert diese aber nicht automatisch. Erst wenn ein Administrator einen Patch genehmigt, wird dieser auf Computern installiert. Über die *Optionen* in der WSUS-Verwaltung können Regeln erstellt werden, über die Updates automatisch zur Installation auf den verschiedenen Computergruppen genehmigt werden. Updates können aber auch manuell oder in Gruppen genehmigt oder explizit abgelehnt werden. Es besteht zum Beispiel die Möglichkeit, Updates zunächst für Testcomputer freizugeben und anschließend über die Berichte zu kontrollieren, ob die Aktualisierung erfolgreich war. Ist dies der Fall, können die entsprechenden Updates für andere Computergruppen oder alle Clients freigegeben werden. Um Updates zu genehmigen, gehen Sie folgendermaßen vor:

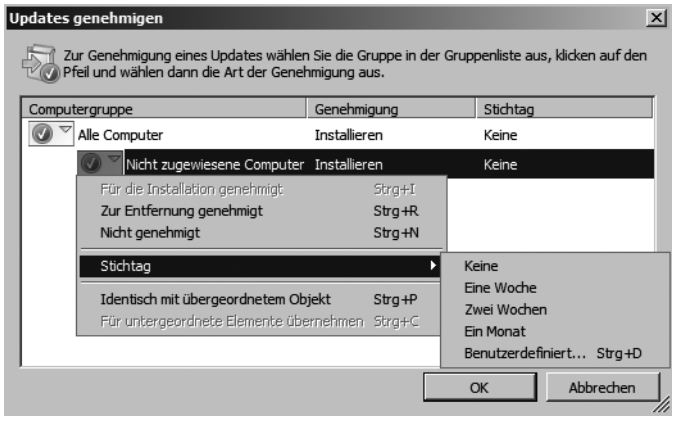
1. Klicken Sie in der WSUS-Verwaltungskonsole auf *Updates*. Anschließend wird eine Zusammenfassung der Updates angezeigt, die auf dem Server verfügbar sind.
2. Wählen Sie in der Liste die Updates aus, die Sie zum Installieren genehmigen möchten. Die Ansicht kann entsprechend gefiltert werden. Wird ein Update ausgewählt, werden im mittleren Bereich der Konsole ganz unten ausführliche Informationen angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den oder die Patches, und wählen Sie im Kontextmenü den Befehl *Genehmigen* aus. Das Dialogfeld *Updates genehmigen* wird angezeigt.

Abbildg. 23.33 Verwalten und Genehmigen von Updates



Wählen Sie die Gruppen aus und klicken Sie auf den Pfeil links neben der Gruppe. Ein Dropdownmenü mit folgenden Optionen wird angezeigt: *Für die Installation genehmigt*, *Zur Entfernung genehmigt*, *Nicht genehmigt*, *Stichtag*, *Identisch mit übergeordnetem Objekt* und *Für untergeordnete Elemente übernehmen*. Klicken Sie auf die Option *Für die Installation genehmigt* und anschließend auf *OK*. Wie Sie aus dem Menü erkennen können, kann WSUS 3.0 installierte Patches auch wieder deinstallieren, wenn diese zum Beispiel mit speziellen Applikationen Probleme bereiten.

Abbildg. 23.34 Genehmigen eines Updates zur Installation



Berichte mit WSUS abrufen

24 Stunden nach der Freigabe von Patches kann in den Berichten zum WSUS verifiziert werden, ob die Updates auf den Computern bereitgestellt wurden. Wollen Sie mit Berichten arbeiten, muss auf dem Server das Tool *Microsoft Report Viewer Redistributable 2005* installiert werden.

Abbildg. 23.35 Zum Anzeigen von Berichten im WSUS wird der *Microsoft Report Viewer* benötigt

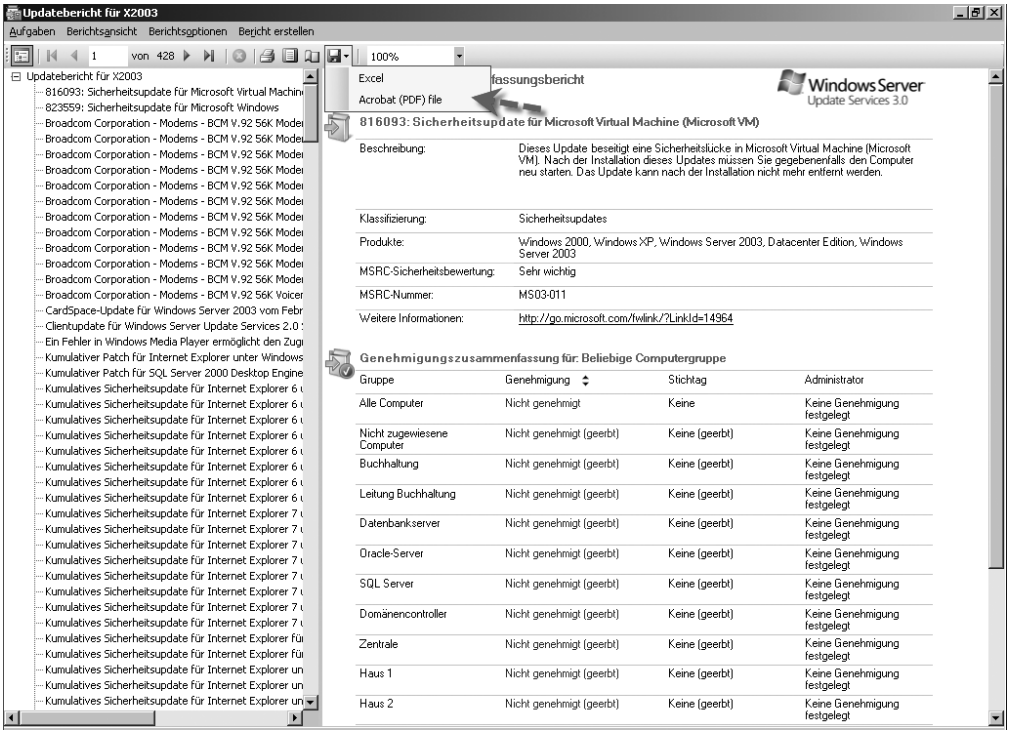
Um Updateberichte anzuzeigen, gehen Sie folgendermaßen vor:

1. Klicken Sie in der WSUS-Verwaltungskonsole im linken Fenster auf *Berichte*.
2. Klicken Sie auf die Option *Updatestatus-Zusammenfassung*.
3. Die Liste kann durch entsprechende Kriterien gefiltert werden.
4. Klicken Sie anschließend in der Symbolleiste des Fensters auf *Bericht erstellen*.

Abbildg. 23.36 Erstellen von Berichten in WSUS

5. Berichte können gespeichert (als Excel-Tabelle oder PDF-Datei) oder gedruckt werden. Klicken Sie dazu in der Symbolleiste auf das *Speichern*-Symbol.

Abbildg. 23.37 Speichern und Exportieren von Berichten in WSUS



WSUS in der Befehlszeile verwalten – *WSUSUtil.exe*

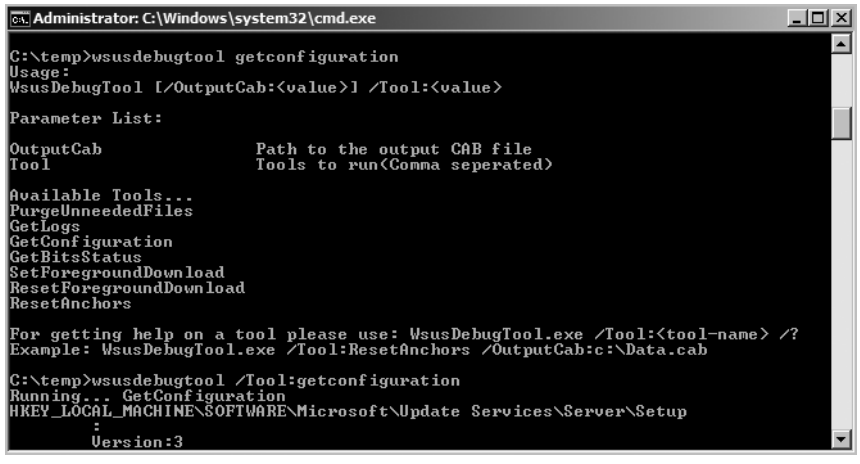
Im Installationsverzeichnis von WSUS 3.0 unter *C:\Programme\Update Services\Tools* finden Sie das Befehlszeilentool *WSUSUtil.exe*, mit dem WSUS über Skripts in der Befehlszeile verwaltet werden kann. Das Tool funktioniert allerdings nur in der 32-Bit-Version von WSUS 3.0. Hauptsächlich wird das Tool zusammen mit folgenden Optionen verwendet:

- **WSUSUtil.exe export** Mit dieser Option können Einstellungen eines WSUS-Servers in eine Datei exportiert werden, zum Beispiel aus Datensicherungsgründen oder um einen neu installierten WSUS-Server zu konfigurieren. Es werden aber nicht alle Daten exportiert.
- **WSUSUtil.exe import** Mit dieser Option kann eine exportierte Datei wieder importiert werden.
- **WSUSUtil.exe movecontent** Mit dieser Option wird der Pfad geändert, in dem der WSUS seine Dateien speichert. Das kann zum Beispiel sinnvoll sein, wenn der Plattenplatz nicht mehr ausreicht oder eine andere Festplatte für die Patchdateien vorgesehen ist.
- **WSUSUtil.exe reset** Diese Option überprüft den Datenbankinhalt auf Konsistenz. Treten Probleme auf, wird der Inhalt erneut aus dem Internet aktualisiert.

- **WSUSUtil.exe listinactiveapprovals** Durch diesen Befehl werden nicht aktive Einstellungen angezeigt, zum Beispiel Patches, die auf Grund unterschiedlicher Spracheinstellungen nicht deaktiviert werden.
- **WSUSUtil.exe removeinactiveapprovals** Dieser Befehl entfernt die Genehmigung für Patches, die nicht als aktiv gekennzeichnet sind.

Zu Diagnosezwecken in der Befehlszeile kann das Tool *WSUS Server Diagnostics Tool* dienen, das von der Internetseite *www.wsus.de* heruntergeladen werden kann. Mit dem Tool kann zum Beispiel über die Option *wsusdebugtool getconfiguration* eine Auflistung der aktuellen Konfiguration des Servers in der Befehlszeile erfolgen. Die Ausgabe kann auch in eine Datei umgeleitet werden, sodass sich das Ergebnis zur Diagnose auch versenden lässt.

Abbildg. 23.38 WSUS-Diagnose in der Befehlszeile durchführen



Zusammenfassung

In diesem Kapitel haben Sie erfahren, wie Sie die neuen Windows Server Update Services (WSUS) 3.0 mit SP1 im Netzwerk integrieren, um Patches für die wichtigsten Produkte herunterzuladen und zu installieren. Im nächsten Kapitel erläutern wir Ihnen die Vorteile und Möglichkeiten, Windows Vista, Windows Server 2008 und Microsoft Office 2007 optimal gemeinsam zu betreiben.

Kapitel 24

Windows Vista SP1 mit Windows Server 2008 betreiben

In diesem Kapitel:

In früheren Kapiteln dieses Buches wurde bereits auf die Zusammenarbeit von Windows Vista mit Windows Server 2008 eingegangen. In diesem Kapitel durchleuchten wir die Neuerungen des Service Pack 1, vor allem, wenn Windows Vista in einem Windows Server 2008-Netzwerk betrieben wird. Außerdem fassen wir die Vorteile und Möglichkeiten zusammen, Windows Vista und Windows Server 2008 gemeinsam zu betreiben. Wir verweisen auf die jeweiligen Kapitel, in denen die Vorteile weitergehend behandelt werden.

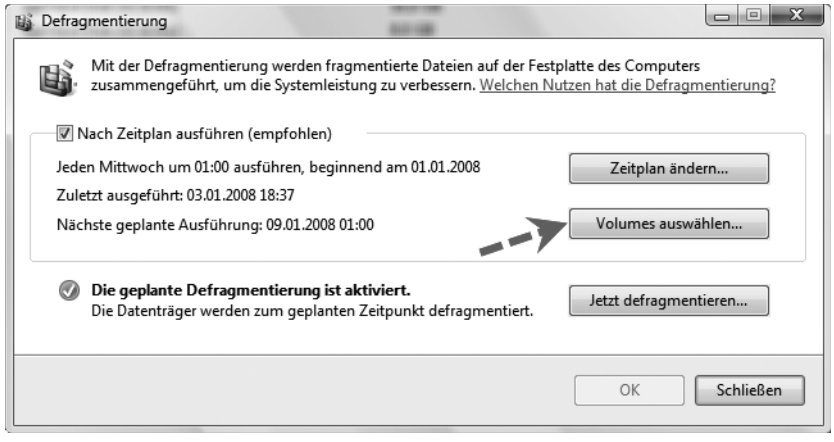
Windows Vista Service Pack 1

Erst mit dem Service Pack 1 unterstützt Windows Vista wichtige Funktionen von Windows Server 2008 wie VPN über HTTPS oder die effiziente Unterstützung der Terminaldienste. Bei diesen können jetzt veröffentlichte Anwendungen, auch RemoteApps genannt, digital signiert werden. Neben den über hundert Fehlerbehebungen seit der Fertigstellung des Betriebssystems im Januar 2007 fließen mit dem Service Pack die Verbesserungen ein, die der Quellcode von Windows Server 2008 enthält. Windows Vista und Windows Server 2008 bauen, wie Windows XP und Windows Server 2003, auf den gleichen Programmcode auf. Seit der ersten Veröffentlichung von Windows Vista hat Microsoft das Serverbetriebssystem Windows Server 2008 weiter entwickelt. Die Verbesserungen des Servers im Programmcode fließen mit dem Service Pack 1 in Windows Vista ein. Die meisten Neuerungen des Service Packs finden eher unter der Haube statt, weniger an der Oberfläche. Nach der Installation des Service Packs fällt häufig subjektiv auf, dass viele Klicks und Arbeitsabläufe schneller ablaufen. Auch das Kopieren und Verschieben von Dateien geht deutlich schneller vonstatten. Auch größere Dateien werden jetzt wesentlich schneller geöffnet als vor der Aktualisierung. Bei Tests liefen Kopiervorgänge zwischen Arbeitsstationen mit dem Service Pack 1 bis zu 50 % schneller. Ist nur eine Arbeitsstation mit dem Service Pack ausgestattet, liegt der Geschwindigkeitszuwachs immerhin noch bei über 25 %. Allerdings sind diese Vorgänge auch stark von der verwendeten Hardware und den installierten Treibern abhängig. Neben der lokalen Leistung wird die Netzwerkkommunikation und der Datenaustausch über das Netzwerk deutlich schneller abgewickelt. Durch die Installation des Service Packs wird das Betriebssystem für Erweiterungen von Drittanbietern im Bereich Windows-Suche geöffnet.

Die Unterstützung des Windows-Sicherheitscenters für zahlreiche Schutzprogramme von Drittherstellern wird verbessert. Die Festplattenverschlüsselung BitLocker wird verbessert und der Schutz erhöht. So lassen sich mit dem Service Pack 1 neben Systempartition (meistens C:) auch alle anderen Partitionen des Computers verschlüsseln. Diese Funktionalität ist in Windows Server 2008 übrigens direkt integriert. Im Bereich der Kompatibilität wird vor allem die Unterstützung von neuen Grafikkarten deutlich verbessert. Wer mit mehreren Monitoren unter Windows arbeitet, profitiert von einer verbesserten Darstellung und mehr Leistung. Die Zahl der mitgelieferten Treiber wird deutlich erhöht und neben den bereits erwähnten Grafikkarten auch mehr Drucker unterstützt, sodass veraltete und instabile Windows XP-Treiber außen vor bleiben können. Performance- und Stabilitätsprobleme beim Aufwachen aus dem Energiesparmodus oder bei der Aktualisierung von Windows XP zu Windows Vista werden mit dem Service Pack ebenfalls behoben. Von den Verbesserungen im Energiesparmodus profitieren vor allem Anwender mit Notebooks, da sich auch die Akkulaufzeit deutlich verbessert. Weiterhin ist es jetzt möglich, zu bestimmen, welche Systempartitionen vom internen Defragmentationsprogramm automatisch defragmentiert werden sollen. Wer gerne spielt, wird sich freuen, dass mit dem Service Pack auch DirectX 10.1 installiert wird, welches mehr Performance bietet, als die Version 10.0. Geschlossen werden mit dem Service Pack auch einige Lücken, die Raubkopierer verwenden, um Windows Vista ohne Aktivierung länger zu betreiben. Auch der neue WLAN-Standard IEEE 802.11

n-Draft wird durch die Installation in Windows Vista integriert. Durch das Service Pack hält das neue Dateisystem exFAT in Windows Vista Einzug, das zukünftig vor allem auf Wechselmedien wie SD-Cards oder Flash-Speichern eingesetzt werden soll.

Abbildg. 24.1 Die Laufwerke für die Defragmentierung können jetzt manuell ausgewählt werden. Es werden nicht mehr automatisch alle Laufwerke verwendet.



Anwender, die Kompatibilitätsprobleme mit Anwendungen haben, profitieren nicht direkt vom Service Pack 1. Durch die grundlegenden Unterschiede in den Sicherheitseinstellungen von Windows XP und Windows Vista laufen zahlreiche Anwendungen nicht unter Windows Vista, die noch unter Windows XP hervorragend ihren Dienst verrichtet haben. Das ist ein wichtiger Grund, warum viele Unternehmen sich noch vor der Einführung von Vista scheuen. Das Service Pack ändert an diesen Einstellungen nichts, sodass eine Anwendung, die ohne das Service Pack nicht unter Windows Vista läuft, nach der Installation von Service Pack 1 noch immer nicht funktionieren wird.

Reduced Functionality Mode (RFM) ist weg

Wird Windows Vista nach 30 Tagen nicht aktiviert, schaltet es sich in den *Reduced Functionality Mode (RFM)*. Zwar kann mit dem Befehl *slmgr.vbs –rearm* als Administrator die Testphase dreimal um 30 Tage, also insgesamt auf 120 Tage verlängert werden. Allerdings muss spätestens nach Ablauf der 120 Tage eine Aktivierung durchgeführt werden. Bei diesem Modus kann mit dem PC nur eingeschränkt gearbeitet werden. Meldet sich ein Anwender an, muss Windows Vista innerhalb einer Stunde aktiviert werden. Erfolgt die Aktivierung nicht innerhalb dieser Stunde, wird der Anwender automatisch vom PC abgemeldet, er erhält keinerlei Warnungen. Im schlimmsten Fall können Anwender also nicht mehr arbeiten. Mit dem Service Pack 1 wird dieser Modus abgeschafft. Wird Windows nicht aktiviert, kann der Anwender weiter arbeiten, erhält aber regelmäßig Meldungen. Diese Erweiterung gilt übrigens auch für Windows Server 2008.

Verbesserungen für 64-Bit-Versionen

Auch der Kernelpatch-Schutz der 64-Bit-Versionen von Windows Vista wird für Sicherheitsprogramme von Drittherstellern geöffnet. Diese Sicherheitsfunktion verhindert, dass externe Programme auf den Kern des Betriebssystems zugreifen können, wodurch Viren und Trojanern der Zugriff auf das System erschwert wird. Ebenfalls neu ist das Extensible Firmware Interface (EFI).

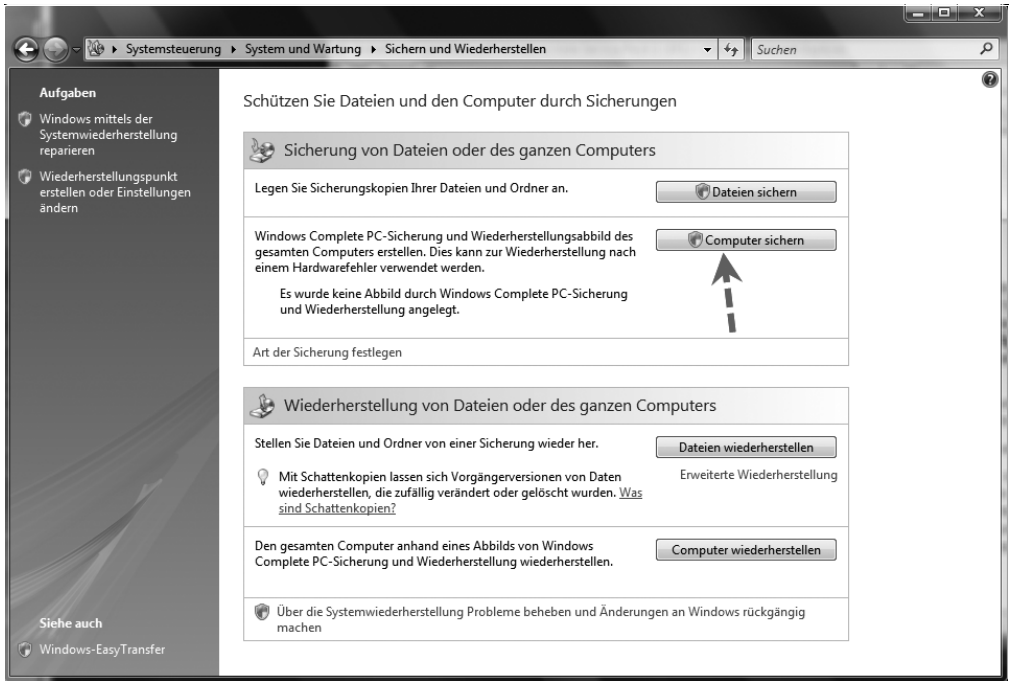
Diese Funktion dient als BIOS-Ersatz für 64-Bit-Systeme und ermöglicht unter anderem ein verbessertes Booten über das Netzwerk, was für die Bereitstellung von Windows Vista in Unternehmen eine wichtige Rolle spielt. So werden auch die Windows-Bereitstellungsdienste (WDS) für Windows Server 2003 SP2 und Windows Server 2008 für die 64-Bit-Version von Windows Vista besser unterstützt (siehe auch Kapitel 16).

Windows Vista Service Pack 1 installieren

Die Installation des Service Packs ist grundsätzlich recht einfach und auch weniger geübte Anwender können die Installation vornehmen. Während der Installation wird der Computer häufig neu gestartet. Diese Vorgänge werden vollkommen automatisiert abgewickelt. Während der Installation darf selbstverständlich nicht mit dem Computer gearbeitet werden, was aber auch durch die ständigen Neustarts ohnehin nicht möglich ist. Durch die lange Dauer der Installation sollten sich Anwender Zeit nehmen und nicht unter Zeitdruck installieren. Soll das Service Pack auf einem Notebook installiert werden, muss dieses mit dem Stromnetz verbunden werden. Die Installation im Akkubetrieb wird nicht empfohlen, da während der Installation ansonsten die Gefahr besteht, dass der Akku erschöpft ist und dadurch die Installation abgebrochen wird. Das Betriebssystem kann dadurch in einen instabilen Zustand gesetzt werden und unter Umständen gar nicht mehr starten. Selbstredend sollten vor der Installation alle geöffneten Programme und Dateien geschlossen werden, am besten auch die Autostart-Programme in der Taskleiste, zumindest soweit das möglich ist. Empfohlen wird die zeitweise Deaktivierung des Virenschutz-Programmes während der Installation, da dieses den Austausch von Systemdateien verhindern kann. Nach der Installation muss dieser Schutz manuell wieder gestartet werden. Außerdem erhalten Anwender, die auf Firewalls von Drittherstellern setzen, zahlreiche Meldungen, da auch Programme wie der Internet Explorer oder Windows Mail von der Aktualisierung betroffen sind. Übrigens lässt sich hier auch gut herausfinden, ob die Firewall etwas taugt, da veränderte Systemdateien von Firewalls immer gemeldet werden sollten. Schließlich können auch Trojaner oder Viren Änderungen vornehmen.

Für die 32-Bit- und 64-Bit-Versionen von Windows Vista steht jeweils ein eigenes Service Pack zur Verfügung. Es gibt keine unterschiedliche Version für die Home-, Business-, Enterprise- und Ultimate-Edition. Die Installation des Service Packs kann nur durchgeführt werden, wenn auf der Festplatte genügend Speicherplatz frei ist. Microsoft empfiehlt mindestens 7 GB für die 32-Bit- und 13 GB für die 64-Bit-Version. Vor der Installation des Service Packs wird automatisch ein Systemwiederherstellungspunkt erstellt, mit dem im Notfall das Betriebssystem wiederhergestellt werden kann. Dennoch ist es sinnvoll zumindest die wichtigsten Daten vor der Installation zu sichern. Wer die Windows Vista Business-, Enterprise- oder Ultimate-Edition einsetzt, kann über das Sicherungsprogramm eine vollständige PC-Sicherung mit den Systemdaten von Windows herstellen. Die Installation kann auch durchgeführt werden, wenn Windows Vista nicht aktiviert ist, eine Überprüfung über den Aktivierungszustand des Betriebssystems findet nicht statt.

Abbildg. 24.2 Mit den Windows Vista-Editionen Business, Enterprise oder Ultimate kann vor der Installation von Service Pack 1 der komplette Computer gesichert werden.



Wer bereits eine Vorabversion des Service Packs einsetzt, muss diese vor der Installation erst deinstallieren, da eine Aktualisierung von Beta- oder RC-Versionen nicht möglich ist.

Für die Installation von Service Pack 1 für Windows Vista gehen Sie folgendermaßen vor:

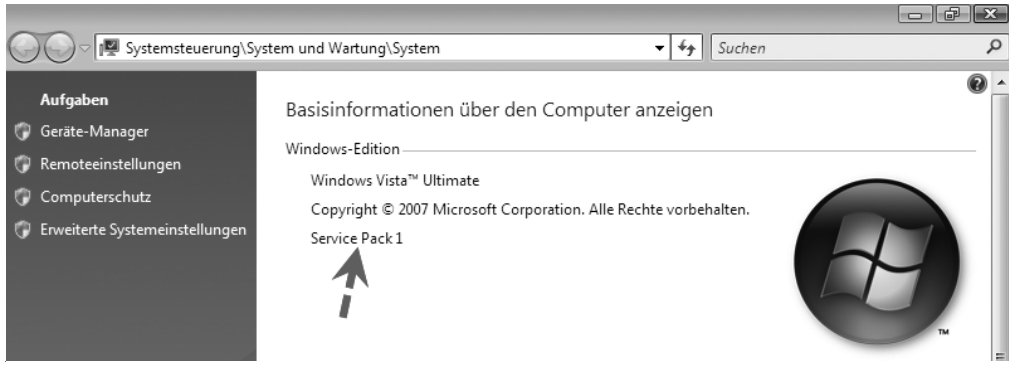
1. Laden Sie sich die Installationsdatei herunter oder lassen Sie die Installation über die Windows-Update-Funktion durchführen. Nach dem Download klicken Sie doppelt auf die Datei, nachdem der Download abgeschlossen ist. Es erscheint zunächst eine Sicherheitswarnung, die mit *Ausführen* bestätigt werden muss.
2. Auf den meisten Computern meldet sich anschließend die Benutzerkontensteuerung, die mit *Zulassen* bestätigt wird.
3. Anschließend startet der Installationsassistent des Service Packs. Über den Link *Wissenswertes vor der Service Pack 1-Installation* werden Zusatzinformationen angezeigt, die aber selten benötigt werden. Über *Weiter* startet schließlich die Installation.
4. Als Nächstes müssen die obligatorischen Lizenzbedingungen bestätigt und mit *Weiter* die Installation fortgesetzt werden.
5. Im nächsten Fenster sollte die Option *Computer automatisch neu starten* aktiviert werden. In diesem Fall startet das Service Pack den Computer immer dann automatisch, wenn ein Neustart notwendig ist, und die Installation läuft vollkommen automatisch ab. Über *Installieren* wird der Vorgang fortgesetzt.

Der Assistent beginnt daraufhin mit der etwa einstündigen Installation des Service Packs. Während der Installation wird der Computer ab und zu neu gestartet und Patches installiert. Starten Sie in diesem Fall den Computer keinesfalls manuell.

Nach erfolgreichem Abschluss der Installation zeigt der Computer das Anmeldefenster an und Sie können nun wie gewohnt weiterarbeiten.

In der *Systemsteuerung* über *System und Wartung/System* wird die erfolgreiche Installation des Service Packs angezeigt.

Abbildg. 24.3 Die Installation von Windows Vista Service Pack 1 war erfolgreich



Windows Vista Service Pack 1 deinstallieren

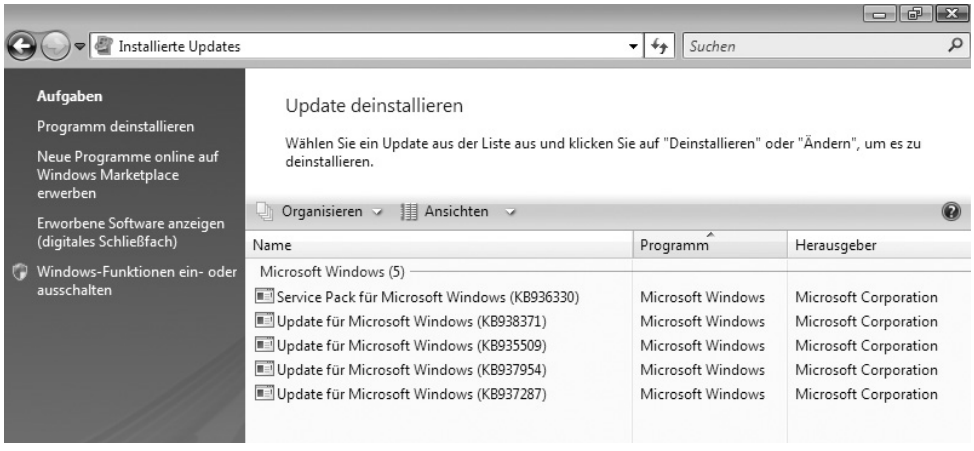
Nicht auf allen Computern wird durch die Installation des Service Packs eine Verbesserung erreicht. Da im Paket über 100 Aktualisierungen und weitere Verbesserungen integriert sind, funktioniert der Computer oder eine installierte Applikation unter bestimmten Umständen nach der Installation nicht mehr ordnungsgemäß. Aus diesem Grund wird auch die Deinstallation des Service Packs ermöglicht. Diese läuft, wie die Installation, über einen eigenen Assistenten ab. Durch die Deinstallation werden aber nicht alle installierten Patches vom System entfernt, da diese teilweise permanent integriert werden. In diesem Fall hilft das Zurücksetzen des Rechners auf einen früheren Systemwiederherstellungspunkt oder eine komplette PC-Sicherung. Beispiele für diese Aktualisierung sind die Patches aus den Microsoft Knowledge Base-Artikeln KB935509, KB937287 und KB938371.

So deinstallieren Sie das Service Pack 1 wieder:

1. Öffnen Sie die Systemsteuerung und klicken Sie auf *Programme*. Klicken Sie auf *Installierte Updates anzeigen*.
2. Hier werden alle Patches angezeigt, die auf dem Computer installiert wurden. Ist nur das Service Pack 1 installiert, werden hier nur etwa fünf Patches angezeigt, darunter *Service Pack für Microsoft Windows (KB936330)*.
3. Klicken Sie *Service Pack für Microsoft Windows (KB936330)* mit der rechten Maustaste an, wählen Sie *Deinstallieren* und bestätigen Sie den Deinstallationsvorgang.
4. Klicken Sie bei der Meldung der Benutzerkontensteuerung auf *Fortsetzen*. Anschließend startet der Assistent mit der Deinstallation des Service Packs. Diese kann bis zu einer Stunde dauern.
5. Nach einigen Minuten muss die Meldung für einen Neustart bestätigt werden.

6. Der Computer fährt nicht komplett herunter, sondern deinstalliert zunächst einige Aktualisierungen. Hierbei sollte Windows nicht unterbrochen oder der Computer ausgeschaltet werden.
7. Nach der erfolgreichen Deinstallation wird der Anmeldebildschirm angezeigt und das Service Pack ist deinstalliert. In den Eigenschaften von Computer im Startmenü wird bei der Windows-Version das Service Pack nicht mehr angezeigt.

Abbildg. 24.4 Deinstallieren des Service Pack 1 für Windows Vista



Verteilung in Unternehmen

Unternehmen, die bereits Windows Vista einsetzen und auf Service Pack 1 aktualisieren wollen, müssen das Update gut planen. Durch die lange Aktualisierungsdauer von fast einer Stunde kann diese Aktualisierung selten in den Geschäftszeiten und schon gar nicht auf allen Clients auf einmal durchgeführt werden. Offiziell wird es für das Service Pack 1 keine Slipstreaming-Möglichkeit geben, also die Integration direkt in das Installationsmedium. Unternehmen die Windows Vista verteilen, müssen also erst das Betriebssystem, dann das Service Pack installieren. Microsoft wird Unternehmen eigene Installationsmedien zur Verfügung stellen, die bereits das Service Pack 1 enthalten. Diese Datenträger können nicht selbst hergestellt werden. Da nur wenige Tastatureingaben vorzunehmen sind, kann die automatische Installation mit Tools wie *AutoIt* durchgeführt werden. Mit AutoIt können alle möglichen Windows-Aufgaben, wie zum Beispiel die Installation von Software oder das Testen von Programmen, vollkommen automatisiert werden. Das Programm und dessen Interpreter haben ähnliche Möglichkeiten wie VB-Skripts. Dazu stellt die Umgebung Möglichkeiten zur Verfügung, sowohl Maus- und Tastatureingaben zu emulieren als auch komplexere Programmiertätigkeiten durchzuführen. Skripts können mit einem Mausklick in eine EXE-Datei umgewandelt werden. Diese Datei ist auf jedem Rechner lauffähig, es muss dazu nicht AutoIt installiert werden. Auf der Seite des Herstellers unter *http://www.hiddensoft.com/autoit* kann das kostenlose Programm heruntergeladen werden. Dort gibt es auch ein Forum mit einer aktiven Community. Hauptsächlich Administratoren, die Aufgaben automatisieren wollen, aber keine Programmierer sind, können mit AutoIt sehr schnell Erfolgserlebnisse erzielen. Auch Programmierer werden erstaunt sein, welche vielfältigen Aufgaben sich mit dieser Entwicklungsumgebung durchführen lassen. Nach der Installation stehen einige Beispielskripts zur Verfügung, mit deren Hilfe Sie schnell einen Überblick über die Möglichkeiten erhalten. Auf diesem Weg lässt sich ein Skript erstel-

len, das über ein Anmeldeskript oder Computerstartskript, zum Beispiel über Gruppenrichtlinien, gestartet wird. Auch hier muss aber die Netzwerklast beachtet werden, denn die Installationsdatei des Service Packs will auch erstmal übertragen werden.

Alternativ können Unternehmen mit den Computergruppen der Windows Server Update Services (WSUS) 3.0 arbeiten, um das Service Pack nach und nach im Unternehmen zu verteilen (siehe Kapitel 23). Allerdings müssen dazu die Computer gestartet bleiben oder über Gruppenrichtlinien aus dem Ruhezustand geweckt werden. Diese Einstellungen werden aber nur in Windows Vista und Windows Server 2008 unterstützt. Das heißt, im Netzwerk muss mindestens ein Domänencontroller mit Windows Server 2008 betrieben werden.

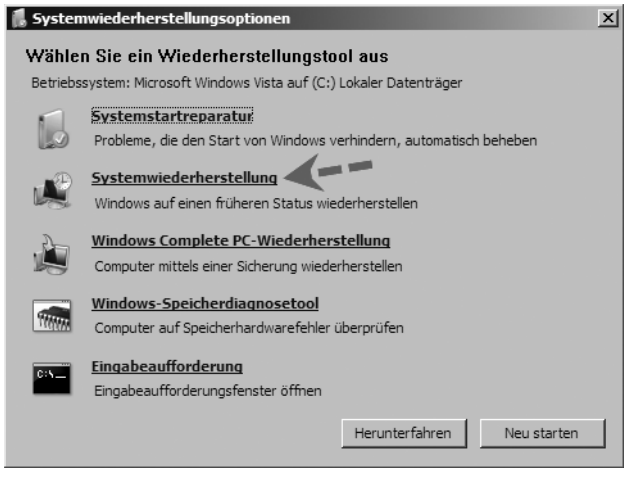
Probleme mit virtuellen Maschinen und älterer Hardware

Vor allem versierte Anwender werden das Service Pack in virtuellen Maschinen mit VMware oder Virtual PC testen. Vor allem auf älteren Computern tritt dieser Effekt häufig auf. Der Fehler ist bei virtuellen Maschinen, die mit Microsoft Virtual PC 2007 erstellt wurden, bisher nicht aufgetreten. Das Problem liegt an nicht kompatiblen Treibern, höchstwahrscheinlich für Grafikkarten. Insbesondere auf Computern, deren Hardware zwar ausreichend für Windows Vista ist, die aber nicht zertifiziert ist, taucht das Problem häufig auf. Die Installation des Service Packs kann ohne Probleme durchgeführt werden, aber beim ersten Start nach der Installation erscheint der Bluescreen. Für virtuelle Maschinen unter VMware Workstation 6.0.2 hilft es, die VMware Tools nicht zu installieren, sondern erst das Service Pack. Werden anschließend die VMware Tools installiert, läuft der virtuelle Computer problemlos. Erscheint bei Ihnen der Bluescreen, gibt es einen Weg, das Service Pack über die *Computereparaturoptionen* mit Hilfe eines Systemwiederherstellungspunktes vom Computer zu entfernen. Damit auf solchen Computern das Service Pack trotzdem installiert werden kann, sollten verschiedene Treiberversionen getestet werden, die kompatibel zu Windows Vista Service Pack 1 sein müssen. Über den nachfolgend beschriebenen Weg, lässt sich übrigens auch Windows Server 2008 reparieren, wenn das Betriebssystem nach der Installation einer Anwendung nicht mehr startet:

1. Booten Sie von der Windows Vista-DVD und klicken Sie im Fenster *Windows installieren* auf die Schaltfläche *Weiter*.
2. Wählen Sie im nächsten Fenster die Option *Computerreparaturoptionen*.
3. Im Fenster *Systemwiederherstellungsoptionen* wählen Sie die Windows-Installation aus, die repariert werden soll, und klicken Sie auf *Weiter*.
4. Im nächsten Fenster klicken Sie auf *Systemwiederherstellung*. Haben Sie vor der Installation des Service Packs eine vollständige PC-Sicherung hergestellt, kann hier auch die Option *Windows Complete PC-Wiederherstellung* gewählt werden. Bei der Systemwiederherstellung werden keine Dokumente überschrieben, nur Systemdateien. Bei der Complete PC-Wiederherstellung werden dagegen auch Dokumente auf den alten Stand zurückgesetzt.
5. Nach kurzer Zeit startet der Assistent für die Systemwiederherstellung. Auf der Startseite klicken Sie auf *Weiter*.
6. Als Nächstes wählen Sie den letzten Systemwiederherstellungspunkt aus. Dieser wird automatisch vor der Installation des Service Packs erstellt und hat normalerweise die Bezeichnung »Installation: Windows Vista Service Pack 1«.

7. Auf der nächsten Seite wird die Partition ausgewählt, die wiederhergestellt werden soll. Normalerweise wird hier nur *C* ausgewählt. Klicken Sie anschließend auf *Weiter*. Hier genügt es, den Systemdatenträger wiederherzustellen.
8. Klicken Sie zum Beginn der Wiederherstellung auf *Fertig stellen* und bestätigen Sie das Meldungsfeld mit *Ja*. Anschließend beginnt die Wiederherstellung des Systems.
9. Nachdem die Wiederherstellung abgeschlossen ist, erscheint ein weiteres Fenster. Klicken Sie hier auf die Schaltfläche *Neu starten*, um die Wiederherstellung abzuschließen.
10. Bei der nächsten Anmeldung erscheint noch ein Fenster, das Sie darüber informiert, dass ein Systemwiederherstellungspunkt zurückgesetzt wurde.

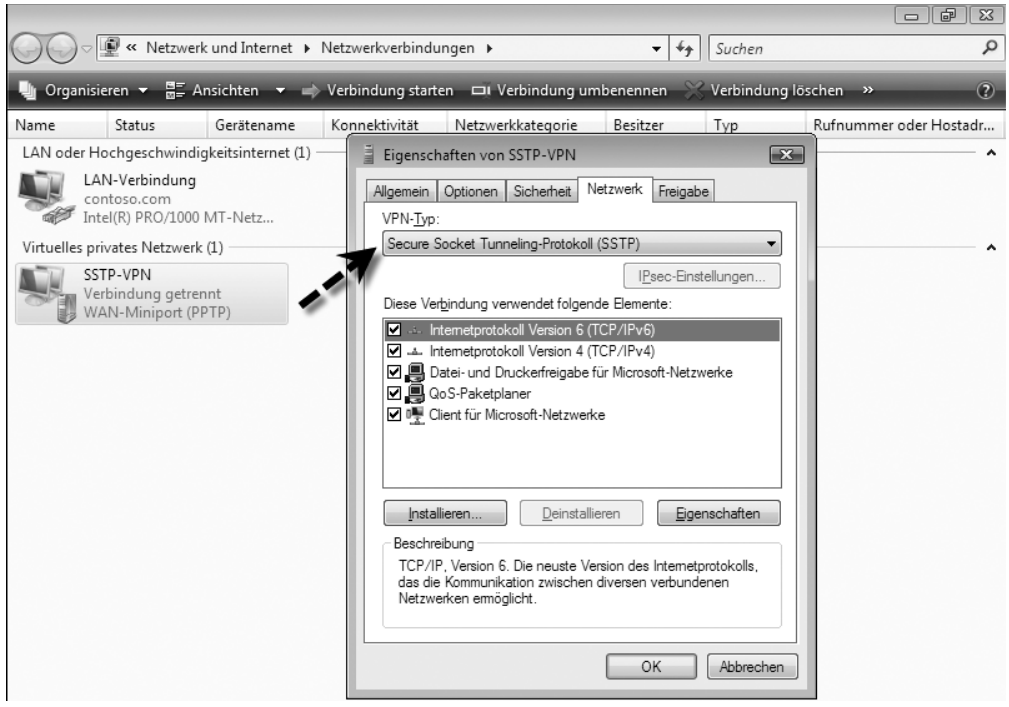
Abbildg. 24.5 Über die Systemwiederherstellung können Systemwiederherstellungspunkte zurückgesetzt werden



HTTPS-VPN über Secure Socket Tunneling Protocol

Windows Server 2008 und Windows Vista SP1 unterstützen neben PPTP und L2TP auch das Secure Socket Tunneling Protocol (SSTP). Mit diesem Protokoll wird ein VPN auf Basis von HTTPS aufgebaut, welches wesentlich leichter durch Firewalls und NAT-Geräten geschleust werden kann. Meist wird der Port 443 in Firewalls nicht geschlossen und auch eine Verbindung über Proxyserver ist möglich. SSTP unterstützt allerdings keine authentifizierten Webproxykonfigurationen, in denen der Proxy während der HTTPS-Verbindungsanforderung irgendeine Form von Authentifizierung verlangt. Um SSTP in einer Active Directory-Domäne verwenden zu können, müssen nicht alle Server und die Domäne zu Windows Server 2008 migriert werden. Es reicht der Einsatz eines VPN-Servers mit Windows Server 2008. Auf den Clients muss Windows Vista SP1 installiert sein. Die Berechtigung für die Einwahl der Benutzer erfolgt identisch zu anderen VPN-Methoden. Ohne das SP1 kann Windows Vista kein SSTP-VPN aufbauen (siehe Kapitel 15).

Abbildg. 24.6 Aufbau eines HTTP-VPN mit SSTP und Windows Vista SP1

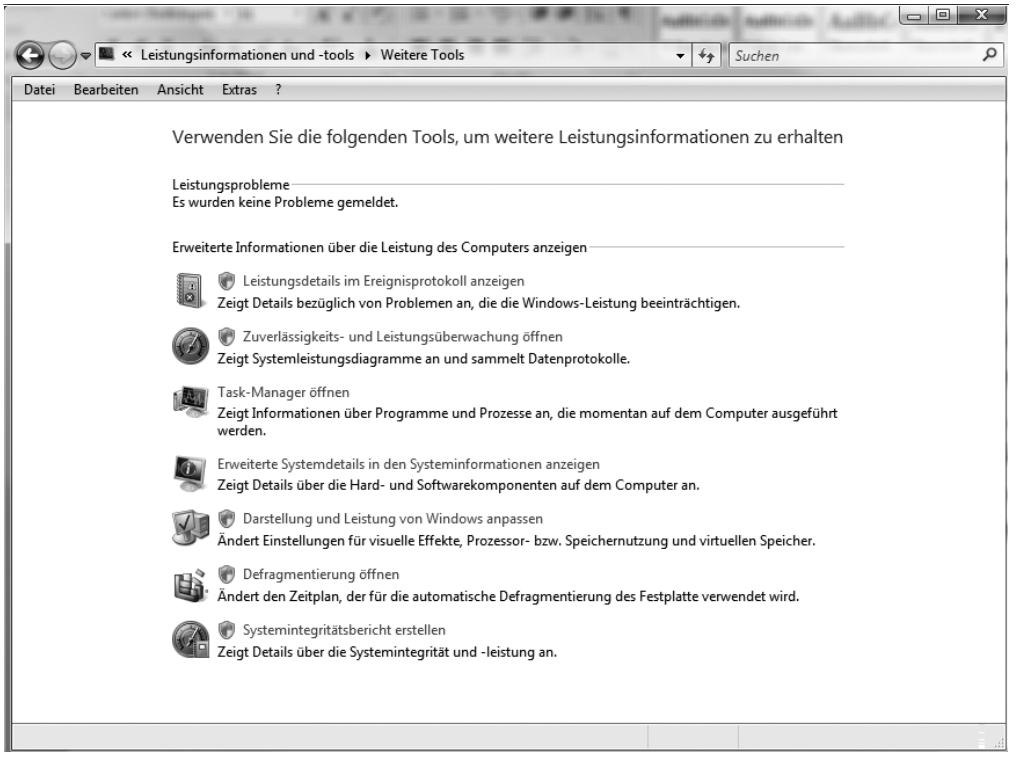


Tuning für Windows Vista

Funktioniert der Computer nach der Installation des Service Packs nicht mit genügend Leistung, helfen vielleicht ein paar kleinere Tuningmaßnahmen bei der Beschleunigung des Rechners. Über *Start/Systemsteuerung/System und Wartung/Leistungsinformationen und -tools/Weitere Tools* werden verschiedene Informations- und Tuningprogramme angezeigt. Hier finden Sie auf einen Blick alle Tuningmöglichkeiten und Stabilitätsberichte von Windows Vista.

Am häufigsten werden PCs durch Programme ausgebremst, die automatisch mit Windows gestartet, aber meist nicht gebraucht werden. Dabei handelt es sich nicht nur um die Programme, die über *Start/Alle Programme/Autostart* gestartet werden, sondern auch über Einträge, die in der Registry vorgenommen wurden. Mit dem Windows-Defender werden über *Extras/Software-Explorer* die Autostart-Programme angezeigt und unnötige Einträge können entfernt werden. Geübtere Anwender verwenden das Tool *Autoruns* von Microsoft-Sysinternals. Dieses Tool kann von der Internetseite *www.sysinternals.com* heruntergeladen werden.

Abbildg. 24.7 Windows Vista bietet eine zentrale Anlaufstelle für alle Programme zur Leistungsmessung und -verbesserung



Superfetch optimieren

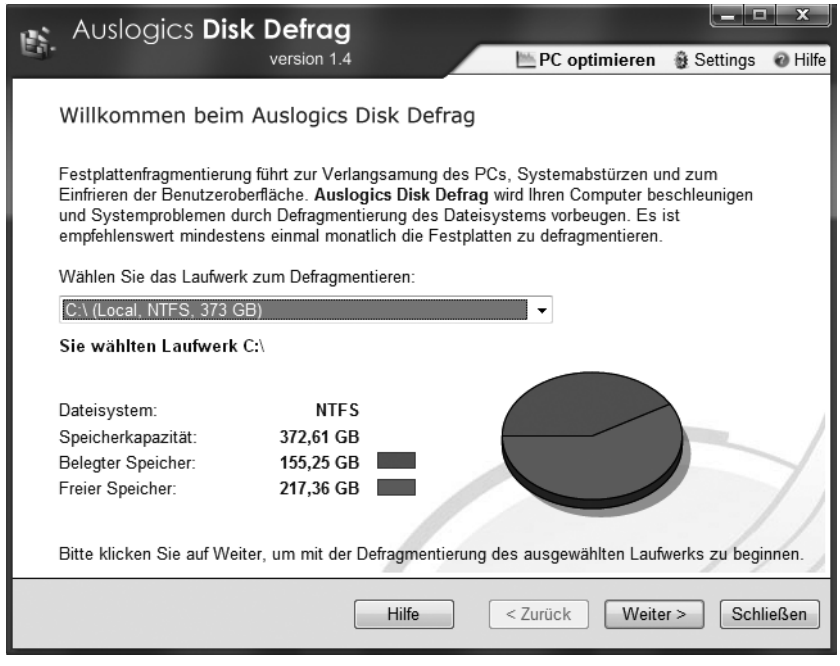
Superfetch ist eine Technologie, die Microsoft bereits mit Windows XP eingeführt, aber in Windows Vista deutlich optimiert hat. Vista merkt sich mit welchen Anwendungen ein Benutzer zu den unterschiedlichen Zeiten arbeitet und lädt diese beim Starten automatisch in den Arbeitsspeicher. Das hat den Vorteil, dass diese Applikationen sehr schnell gestartet werden, wenn der Anwender diese benötigt. Aus diesem Grund verbraucht Vista auch deutlich mehr Arbeitsspeicher als Windows XP, da alle wichtigen Programme bereits beim Systemstart geladen werden. Vista analysiert dazu ständig das Benutzerverhalten und passt Superfetch an die Bedürfnisse von Anwendern an. Diese Funktion kann über den Registrierungs-Editor konfiguriert werden. Die Konfiguration findet über den Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters* statt. Über den DWORD-Wert *EnableSuperFetch* kann diese Funktion gestartet oder deaktiviert werden. Mit dem Parameter *3* wird sowohl der Bootvorgang als auch das Starten von Programmen optimiert. Es gibt aber auch noch die folgenden Möglichkeiten:

- **0** Superfetch ausschalten
- **1** Superfetch nur für Anwendungen aktivieren
- **2** Superfetch nur für den Bootvorgang aktivieren

Festplatte defragmentieren mit Bordmitteln oder Zusatztools

Je älter ein installiertes Windows wird, desto stärker wird die Platte fragmentiert. Dies bedeutet, dass Teile von Dateien auf der Platte an verschiedenen Stellen gespeichert wurden, sodass beim Lesen zunächst alle Blöcke der Dateien von Windows zusammengesucht werden müssen und dann erst die Datei geöffnet wird. Da dadurch der Schreib-/Lesekopf der Festplatte deutlich mehr unterwegs ist, dauert auch das Öffnen der Datei unnötig lange. Beim Defragmentieren werden diese Blöcke zusammengefasst, sodass die Geschwindigkeit gesteigert werden kann. In Windows Vista sind Bordmittel integriert, die beim Defragmentieren unterstützen sollen. Das Programm wird am schnellsten über die Eingabe von *defrag* im Suchfeld des Startmenüs gestartet. Es gibt aber auch weitere kostenlose Alternativen, die sehr gut funktionieren und ebenfalls sehr beliebt sind. Eines der bekanntesten Tools in diesem Bereich ist *Disk Defrag* von Auslogics, welches kostenlos von der Seite *http://www.auslogics.com/disk-defrag* heruntergeladen werden kann. Vor allem nach der Installation eines Service Packs kann eine Defragmentierung noch etwas mehr Leistung aus dem System herausholen.

Abbildg. 24.8 Durch regelmäßiges Defragmentieren wird die Performance eines Computers ebenfalls verbessert



Systemtuning durch das Entfernen von Malware

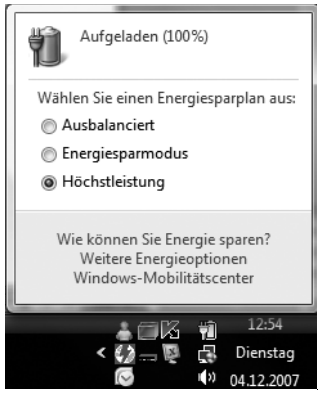
Ein weiterer wichtiger Schritt, um ein Windows-System zu beschleunigen, liegt im Beseitigen von Malware, Spyware und den Schädlingen, die sich über kurz oder lang jeder Internetsurfer einfängt. Der Rundumschlag zum Entfernen von Spyware vom System ist, neben dem Windows-Defender die kostenlose Freeware *Hitman Pro* von der Seite *http://www.hitmanpro.nl*. Das Tool scannt dazu nicht selbst nach Spyware, sondern lädt nach der Installation automatisch die gängigsten Freeware-Programme zur Spyware-Bekämpfung herunter und fasst diese in einer einheitlichen Oberfläche zusammen. Nach einem Scanvorgang mit den wichtigsten Scanengines ist jeder Computer weitgehend von Spyware befreit, was oft unglaubliche Leistungsreserven offenbart. Auch das Entfernen

von veralteten Einträgen in der Registry und alten Programmdateien kann einiges bringen. Dazu gibt es das kostenlose Tool *CCleaner*, welches zuverlässig veraltete Einträge in der Registry und Dateien vom Computer entfernen kann. Das Tool kann von der Internetseite *www.ccleaner.de* heruntergeladen werden. Die beiden Tools sind vor allem auf Heimarbeitsplätzen oder Notebooks, die sich nicht im Zugriff der Administratoren befinden, hilfreich.

Energie-Einstellungen auf Notebooks optimieren

Wird Windows Vista auf einem Notebook installiert, werden die Energieoptionen oft so eingestellt, dass die Akkulaufzeit erhöht, aber die Leistung reduziert wird. Wer sein Notebook am Stromnetz betreibt, sollte daher eher den Schwerpunkt auf die Leistung setzen. Über das Symbol der Energieoptionen in der Taskleiste kann die Geschwindigkeit eines Computers über die Energieoptionen deutlich erhöht werden.

Abbildg. 24.9 In den Energieoptionen kann die Leistung für Notebooks erhöht werden



Aktuelle Treiber installieren

Auch wenn dieser Tipp nicht der neueste ist, bringt die Installation von aktuellen Treibern immer eine Performance-Verbesserung, vor allem im Bereich des Chipsatzes und der Grafikkarte. Anwender sollten in regelmäßigen Abständen überprüfen, ob neue Treiber verfügbar sind, und diese dann herunterladen und installieren. Vor allem neue Vista-Treiber für Grafikkarten wirken oft Wunder. Auf diversen Seiten im Internet finden sich angepasste Treiber der Grafikkartenhersteller, die meist deutlich mehr Performance bringen als die Treiber des Computerherstellers, vor allem bei Highend-Notebooks. Über die Internetseite *http://www.notebookforums.com* können diese angepassten Treiber heruntergeladen werden.

Windows Vista und Windows Server 2008 gemeinsam betreiben

In verschiedenen Kapiteln dieses Buchs haben wir Ihnen viele Möglichkeiten gezeigt, die Windows Vista und Windows Server 2008 im gemeinsamen Betrieb ermöglichen. Über die verbesserte Bereitstellung (siehe Kapitel 16), bessere Unterstützung für Gruppenrichtlinien (siehe Kapitel 9) und den verbesserten Betrieb im Netzwerk (siehe Kapitel 7 und 8), bis hin zur optimierten Unterstützung der

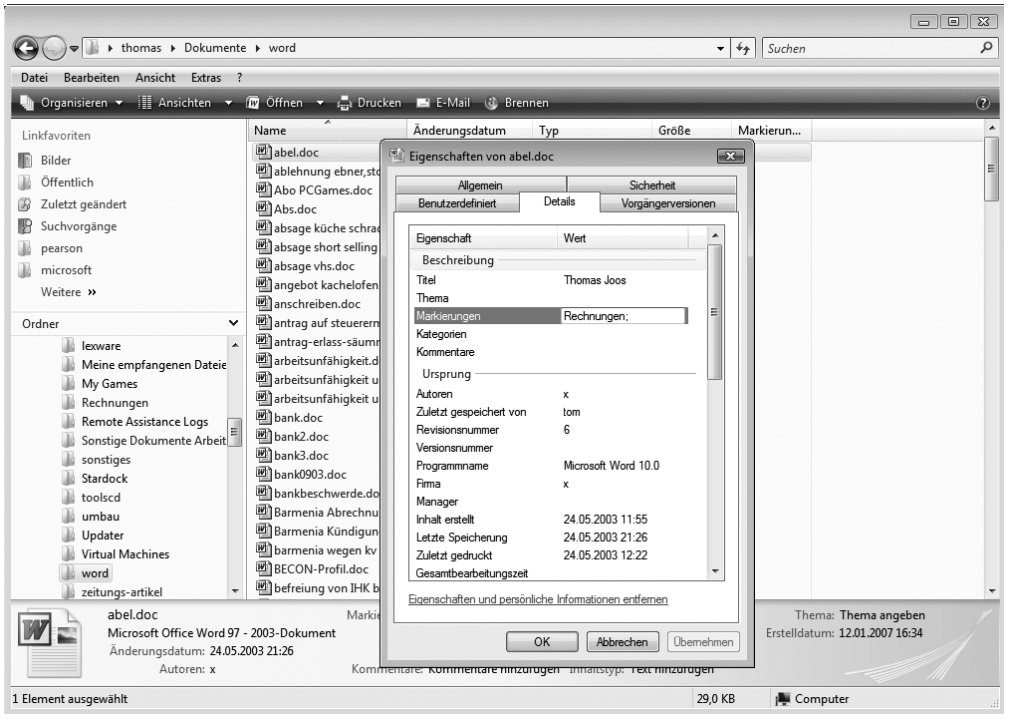
Terminaldienste (siehe Kapitel 12) und der Unterstützung des Netzwerkzugriffschutzes (siehe Kapitel 15) spielen die beiden neuen Betriebssysteme zusammen eine perfekte Rolle für mehr Effizienz im Unternehmen. In den Kapiteln 1, 2 und 3 sind wir bereits auf viele Gemeinsamkeiten eingegangen. In diesem Abschnitt durchleuchten wir die Vorteile weiter. Wesentlich ist auch, dass Windows Vista und Windows Server 2008 der gleichen Programmcodebasis entsprechen. Alle Vorteile, die in diesem Buch über Windows Server 2008 besprochen werden, gelten auch für Windows Vista, vor allem, wenn das Service Pack 1 installiert ist. Der Betrieb im gemeinsamen Netzwerk wird vor allem in Kapitel 7, der Betrieb in einer Active Directory-Domäne in Kapitel 8 besprochen.

Den neuen Explorer und die verbesserte Suche nutzen

Wie überall in Windows Vista hat Microsoft auch dem neuen Windows-Explorer eine neue Oberfläche spendiert. Es gibt eine neue Menüleiste, deren einzelne Menübefehl auch als Schaltfläche dienen, um die wichtigsten Funktionen und Ansichten zu aktivieren. Die neue Menüleiste zeigt außerdem kontextsensitive Schaltflächen an. Öffnen Sie zum Beispiel ein Verzeichnis mit Bildern, erscheint die Schaltfläche *Diashow*. Markieren Sie ein Word-Dokument, erscheinen die Schaltflächen *Drucken* und *E-Mail*. Die meisten Tastenkombinationen der Windows-Vorgängerversionen funktionieren übrigens auch noch unter Windows Vista, was vor allem Power-User interessieren dürfte. Auch wenn der neue Windows-Explorer zahlreiche neue Funktionen aufweist, ist die Bedienung noch sehr ähnlich zu XP. In der Adressleiste wird der aktuelle Pfad des gewählten Verzeichnisses angezeigt. Klicken Sie mit der Maus auf das Ordnersymbol ganz links in der Adressleiste, wird der vollständige Pfad zum Verzeichnis auf der Festplatte angezeigt, den Sie auch in die Zwischenablage kopieren können. Mit der Vor- und Zurück-Schaltfläche können Sie im Explorer genauso navigieren wie im Internet Explorer. Die klassische Menüleiste wird temporär eingeblendet, wenn Sie die Alt-Taste drücken. Dauerhaft kann diese über *Organisieren/Layout/Menüleiste* eingeblendet werden. Klicken Sie mit der Maus auf das kleine Pfeilsymbol neben einem Verzeichnis in der Adressleiste, werden Ihnen alle Unterverzeichnisse angezeigt und Sie können direkt in eines dieser Verzeichnisse wechseln.

Eine weitere Neuerung sind die Dateimarkierungen (Tags), die Sie unten im Detailfenster anzeigen lassen können. Klicken Sie eine Datei mit der rechten Maustaste an und rufen Sie deren Eigenschaften auf, können Sie auf der Registerkarte *Details* verschiedene Eigenschaften der Datei bearbeiten und eine Bewertung abgeben. Dadurch können Sie zum Beispiel Dateien mit einem gemeinsamen Schlüsselwort versehen, damit Sie durch die Windows-Suche alle Dateien mit einem gemeinsamen Schlüsselwort finden können, ohne dass diese in einem gemeinsamen Verzeichnis gespeichert wurden. Um Daten einzugeben, klicken Sie auf der Registerkarte *Details* neben der entsprechenden Eigenschaft in die Spalte *Wert*. Danach verwandelt sich der jeweilige Bereich in ein Eingabefeld. Die einzelnen Werte werden jeweils durch ein Semikolon (;) voneinander getrennt.

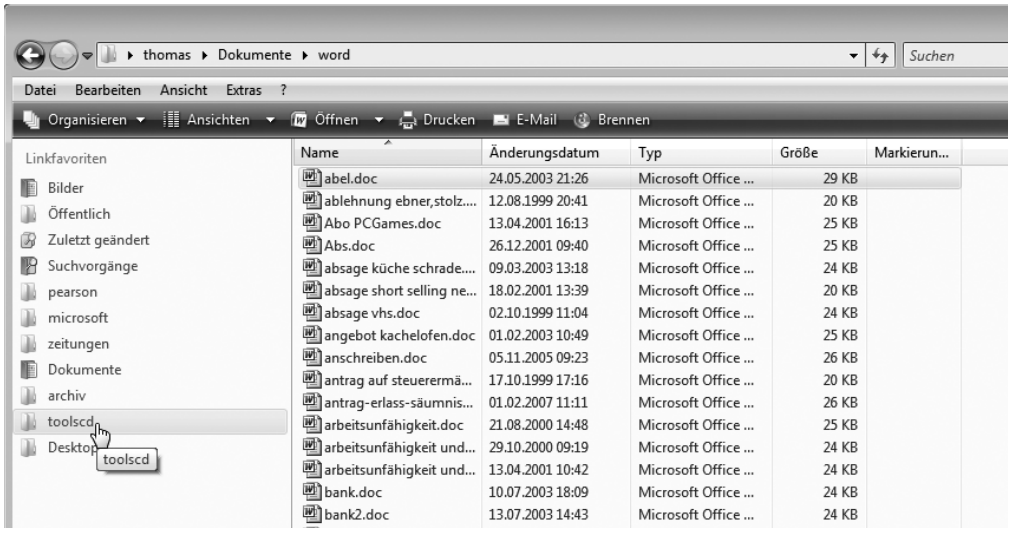
Abbildg. 24.10 Dateien können spezielle Markierungen mitgegeben werden, nach denen gesucht werden kann, und die in der Detailleiste des Windows-Explorers angezeigt werden



Sie können auch die Markierungen mehrerer Dateien gleichzeitig konfigurieren. Dazu selektieren Sie die entsprechenden Dateien und rufen deren Eigenschaften auf. Jetzt können Sie die Werte für sämtliche Dateien gleichzeitig anpassen. In der erweiterten Suche lassen sich durch diese Angaben alle Dateien einer Markierung anzeigen, unabhängig davon, in welchem Verzeichnis diese abgelegt sind. Die Markierungen können auch wieder auf den Standardwert zurückgesetzt werden. Verwenden Sie dazu den Link *Eigenschaften und persönliche Informationen entfernen*, den Sie unten auf der Registerkarte *Details* finden.

Die *Linkfavoriten* sind ebenfalls eine neue Funktion. Ähnlich wie im Internet Explorer können Sie im Windows-Explorer Favoriten zu häufig verwendeten Verzeichnissen hinterlegen. Auf diese Weise wechseln Sie schnell zu Ihren wichtigsten Verzeichnissen. Neue Linkfavoriten erstellen Sie, indem Sie das entsprechende Verzeichnis mit der Maus in den Bereich der Linkfavoriten ziehen. Warten Sie, bis die Option *Verknüpfung erstellen in Links* erscheint und lassen Sie die Maustaste dann los.

Abbildg. 24.11 Über die Linkfavoriten wechseln Sie zu Ihren wichtigsten Verzeichnissen



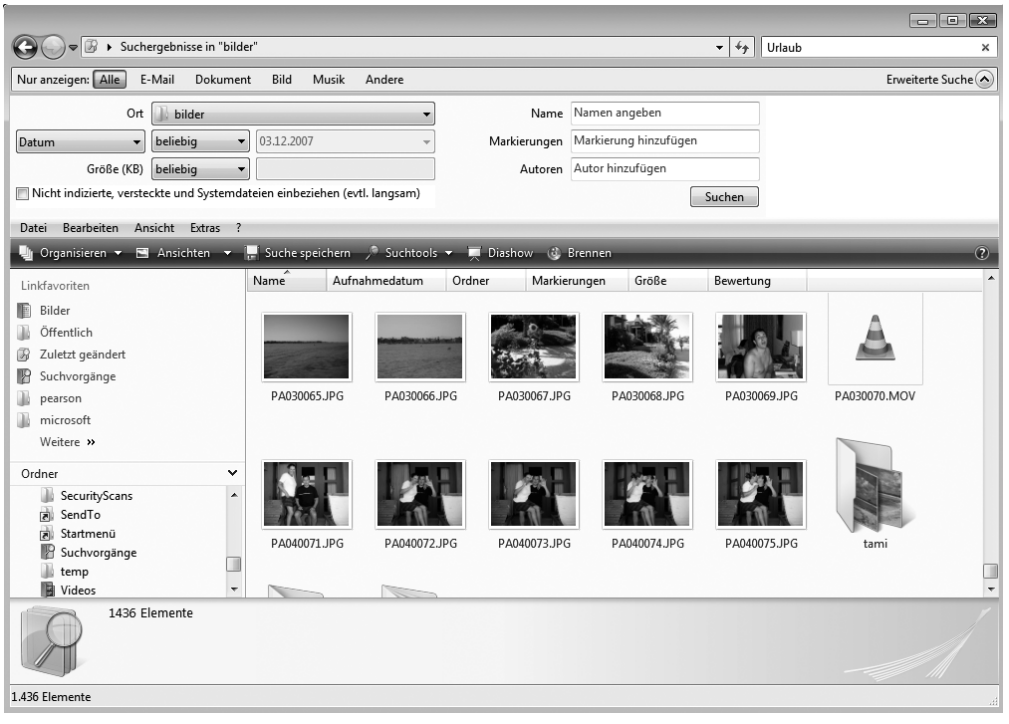
Dateien effizient lokal und im Netzwerk suchen und finden

In jedem Explorer-Fenster wird die Suchleiste eingeblendet. Auch im Startmenü finden Sie die neue Suche von Windows Vista. Sie filtert die aktuelle Ansicht auf der Grundlage des von Ihnen eingegebenen Textes. Mit dem Feld *Suchen* können Sie Dateien anhand von Text im Dateinamen, von Text innerhalb der Datei, von Markierungen und von anderen gängigen Dateieigenschaften suchen, die Sie an die Datei angefügt haben. Darüber hinaus schließt die Suche den aktuellen Ordner und alle Unterordner ein. Über den Link *Erweiterte Suche* spezifizieren Sie die Sucheigenschaften noch genauer. Mithilfe des Index wird die Suche nach Dateien erheblich beschleunigt. Anstatt die ganze Festplatte nach einem Dateinamen oder einer Dateieigenschaft durchsuchen zu müssen, muss Windows lediglich den Index überprüfen, sodass das Ergebnis in einem Bruchteil der Zeit verfügbar ist, die für eine Suche ohne Index benötigt würde. Zu den indizierten Speicherorten gehören alle Dateien in Ihrem persönlichen Ordner, beispielsweise Dokumente, Bilder, Musik und Videos, sowie E-Mail- und Offline-Dateien. Zu den nicht indizierten Dateien zählen Programm- und Systemdateien. Die Konfiguration des Index finden Sie über *Start/Systemsteuerung/System und Wartung/Indizierungsoptionen*.

Wenn Sie eine Datei mit dem Titel *Einkaufskonditionen 2007* erstellt haben, werden, sobald Sie »Eink« in das Feld *Suchen* eingeben, die meisten Dateien im Ordner nicht mehr angezeigt. Wenn Sie die Datei *Rechnung November.xls* suchen, können Sie »Nov« oder »Rech« eingeben. Um anhand einer Dateieigenschaft zu filtern, können Sie den Namen der Eigenschaft und den Suchbegriff durch einen Doppelpunkt trennen: *Name: Sonnenaufgang* liefert Dateien, deren Dateiname das Wort *Sonnenaufgang* enthält. *Tag:Sonnenaufgang* zeigt die Dateien, die eine Markierung mit dem Wort *Sonnenaufgang* aufweisen. *Geändert am 15.5.2008* sucht nach Dateien, die an diesem Datum geändert wurden. Sie können auch *Geändert:2008* eingeben, um nach Dateien zu suchen, die irgendwann in diesem Jahr geändert wurden. Welche Dateieigenschaften zur Verfügung stehen, sehen Sie, wenn Sie mit der rechten Maustaste auf einen Spaltennamen klicken. Über den Menübefehl *Weitere* werden alle möglichen Details angezeigt, nach denen Sie suchen und die Sie in der Detailansicht anzeigen können. *Urlaub AND 2007* zeigt Dateien, die sowohl das Wort *Urlaub* als auch das Wort *2007* ent-

halten. *Urlaub NOT 2006* sucht nach Dateien, die das Wort *Urlaub*, aber nicht das Wort *2006* enthalten. Sie haben auch die Möglichkeit, eingegebene Suchfilter zu speichern, indem Sie auf die Schaltfläche *Suche speichern* klicken. Windows speichert die Abfrage als Datei im Ordner *Suchvorgänge* Ihres Profils. Per Doppelklick können Sie die Suche wiederholen lassen, ohne den Filter neu definieren zu müssen. Über *Organisieren/Ordner- und Suchoptionen* geben Sie über die Registerkarte *Suchen* weitere Einstellungen für die Windows-Suche vor. Wenn Sie den Dienst *Windows-Suche* beenden und deaktivieren, findet keine Indexierung mehr statt.

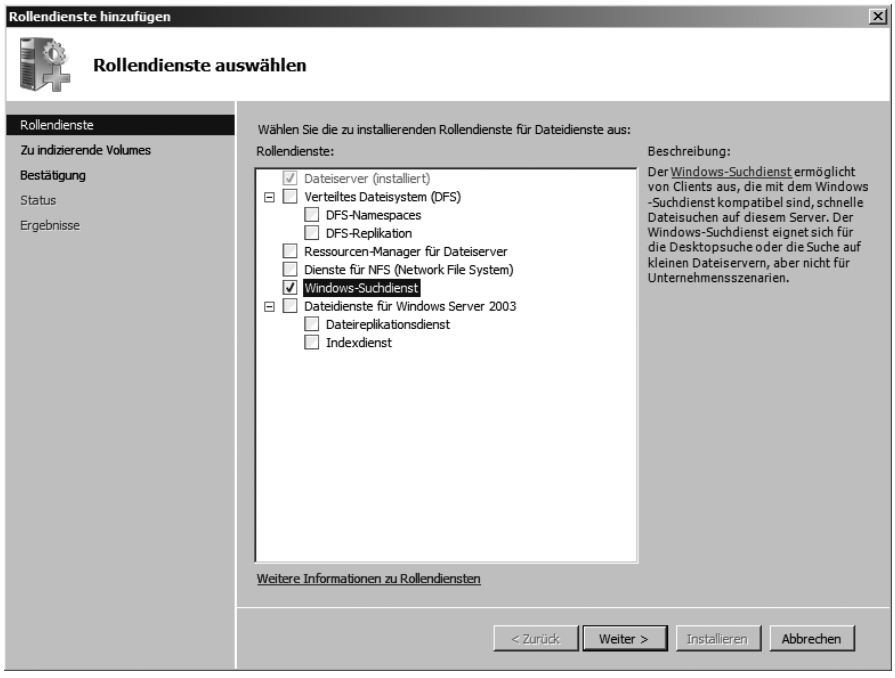
Abbildg. 24.12 Die Suche in Windows Vista ist ein mächtiges Instrument zur Dateiverwaltung



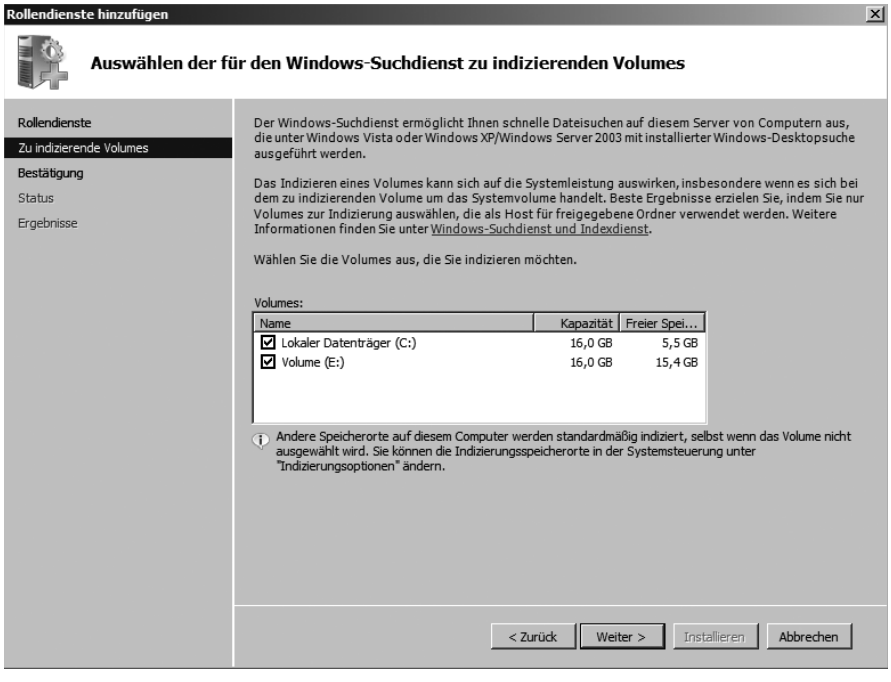
Mit Windows Server 2008 wird die Suche auch auf Netzlaufwerke ausgedehnt. Dazu nutzt Windows Vista den Index des Servers. Die Indexsuche verbraucht so gut wie keine Leistung, da diese im Hintergrund abgewickelt wird. Die Windows Vista-Suche übergibt Suchanfragen an den Index des Servers und erhält vom Server auch die Antwort zurück. Dies hat den Vorteil, dass nicht jeder Client selbst seine Netzlaufwerke indexieren muss, was die Netzwerkleistung reduzieren würde. So muss der Server nur einen Index bereitstellen. Dies ist ein sehr großer Vorteil im Vergleich zu Desktopsuchmaschinen von Drittherstellern. Damit die Windows Vista-Suche aber den Index auf dem Windows Server 2008-Dateiserver verwenden kann, muss der Rollendienst *Windows-Suchdienst* der Serverrolle *Dateiserver* installiert werden. Erst dann steht diese Funktion zur Verfügung.

Bereits bei der Installation des Rollendienstes kann ausgewählt werden, welche Partitionen auf dem Dateiserver indexiert werden sollen. Die Auswahl kann aber auch später über den Server-Manager vorgenommen werden.

Abbildg. 24.13 Installieren des Windows-Suchdienstes unter Windows Server 2008



Abbildg. 24.14 Auswählen der Partitionen, die der Suchdienst indexieren soll



Netzwerkzugriffschutz verwenden

Wird im Unternehmen Windows Vista eingesetzt, kann der Netzwerkzugriffschutz, der in Kapitel 15 ausführlich besprochen ist, optimal dazu verwendet werden, ein Netzwerk so abzusichern, dass gefährdete PCs entweder gar nicht mit dem Netzwerk verbunden oder in ein Quarantäne-Netzwerk verschoben werden. Die hierfür erforderliche Client-Software ist direkt in Windows Vista integriert. Der notwendige Client ist zwar auch in das Service Pack 3 für Windows XP integriert, allerdings ist die lokale Verwaltungsoberfläche für den Client nur in Windows Vista vollständig enthalten. Der NAP-Client ist ein zusätzliches Add-On, in Windows Vista ist er direkt in das Betriebssystem integriert. Zudem unterstützt der Netzwerkzugriffschutz auch den Windows-Defender, der in Windows Vista integriert ist. Zwar kann dieser auch unter Windows XP installiert werden, wird hier aber nicht in das Sicherheitscenter integriert und dadurch der Netzwerkzugriffschutz nicht überwacht. Auch interne Technologien wie erweiterte Authentifizierungsmöglichkeiten des Netzwerkverkehrs über IP, Single Sign-On (SSO) und die Unterstützung für 802.1x bleiben Windows Vista vorbehalten.

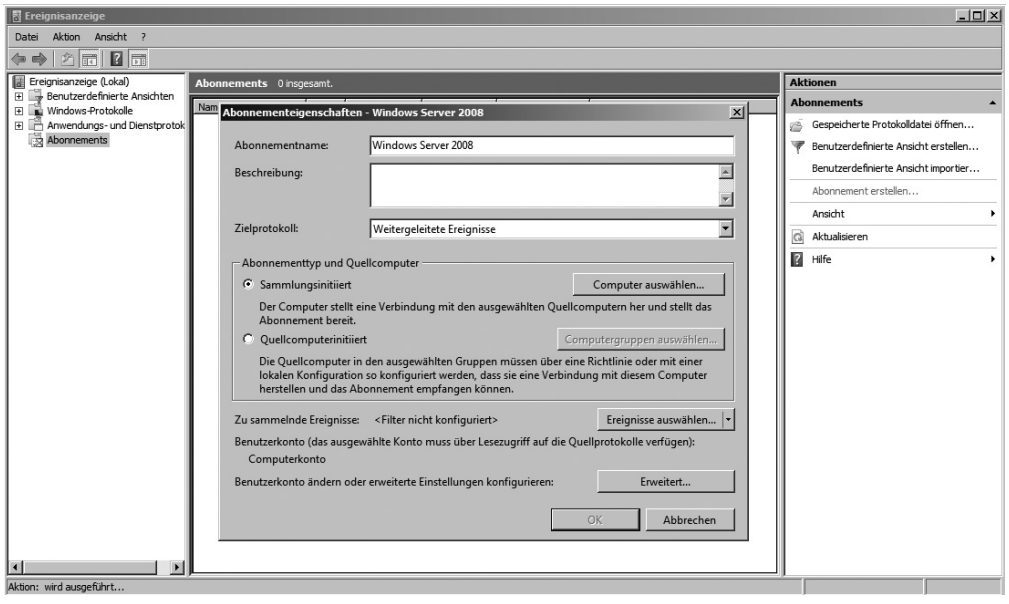
Verbesserte Bereitstellung im Unternehmen

In Kapitel 16 haben wir uns ausführlich mit der Bereitstellung von Windows Vista über die Windows-Bereitstellungsdienste gesprochen. Hier ergeben sich deutlich mehr Möglichkeiten und Vorteile im Vergleich zu Windows XP. Vor allem die WIM-Installation und die verbesserten Energiesparmöglichkeiten sind in diesem Zusammenhang Windows XP überlegen. Durch die Windows-Bereitstellungsdienste können mit einem Werkzeug Windows Server 2008 und Windows Vista automatisiert installiert werden. Die Remoteinstallationsdienste (RIS) von Windows Server 2003 unterstützen kein Windows Vista. Generell wurde die Installation erheblich optimiert, wie in Kapitel 1, 2 und 16 ausführlich besprochen wurde.

Verbesserte Ereignisanzeige

Windows Vista und Windows Server 2008 bauen auf die gleiche neue XML-basierte Struktur der Ereignisanzeigen auf. Ereignisanzeigen von Windows Server 2008 können dadurch auf einer Windows Vista-Arbeitsstation angezeigt oder importiert werden. Die Kategorien und Übersicht wurden deutlich optimiert. Mehr zu dem Thema finden Sie in Kapitel 18. Mit dem Ereignis-Abonnement können Ereignisse von Quellservern zu Zielservern geschickt werden, um diese zentral zu überwachen. Auch hier spielen Windows Vista und Windows Server 2008 perfekt zusammen.

Abbildg. 24.15 Ereignisanzeigen können in Windows Vista auch abonniert werden, um auf Admin-Arbeitsstationen die Ereignisanzeigen der Server abzubilden



Verbesserungen beim Drucken und beim Dateizugriff

Windows Vista verarbeitet Druckaufträge lokal und schickt erst dann Druckaufträge an den Server, wenn diese fertig aufbereitet sind. Dadurch wird die Last von Druckservern unter Windows Server 2008 deutlich reduziert (siehe auch die Kapitel 6 und 19). Die Daten werden im RAW-Format an den Druckserver gesendet, was die Performance verbessert und Treiberfehler durch verschiedene Treiberstände auf Client und Server verhindert. Windows Vista und Windows Server 2008 haben durch die gemeinsame Codebasis auch das gleiche Dateisystem. Beide unterstützen Transactional NTFS. Heutzutage speichern viele Anwendungen die Daten nicht mehr relational. SharePoint speichert zum Beispiel seine Daten in SQL-Datenbanken, was in sehr große Datenbanken resultiert, abhängig von den gespeicherten Dateien. SQL Server 2008 unterstützt die transaktionale Speicherung von Dateien auf dem Dateisystem, die aber weiterhin mit der Datenbank verbunden sind. Auch wenn die Daten auf dem Dateisystem gespeichert werden, verhalten sich diese, als ob sie ausschließlich in der Datenbank gespeichert sind, und können daher auch transaktional verwendet werden. Damit diese Funktion stabil und sicher funktioniert, wird das transaktionale Dateisystem verwendet. Diese neue Technik wird von Windows Server 2008 und Windows Vista unterstützt. Der Lese- und Schreibzugriff erfolgt dadurch mit NTFS-Performance und mit SQL-Sicherheit. Auch herkömmliche Zugriffe auf das Dateisystem, zum Beispiel auf Dateiserver, werden dadurch optimiert.

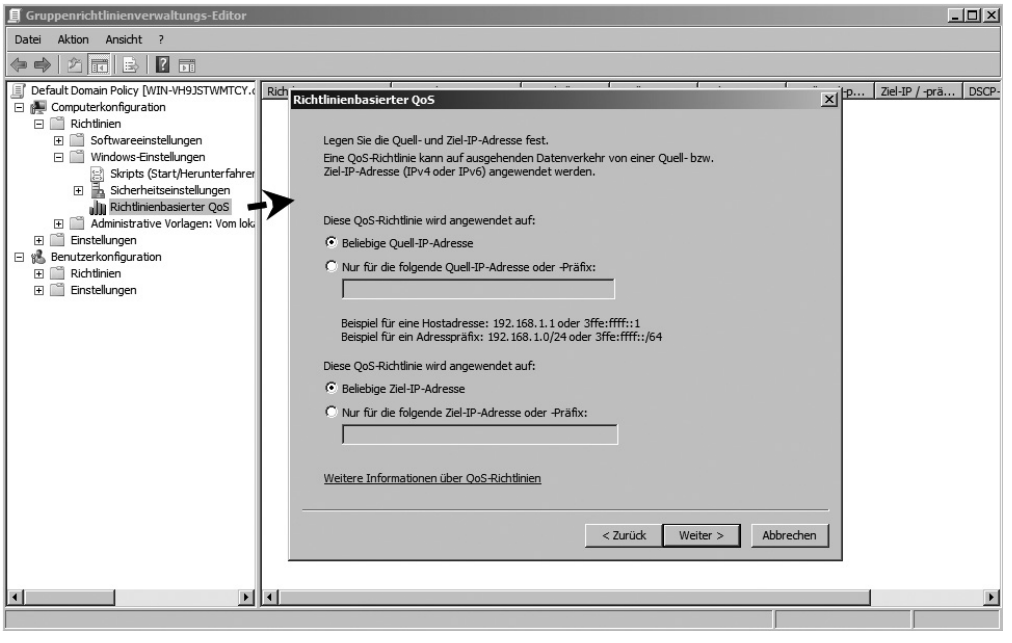
Verbesserte Offlinedateien

Im Zusammenspiel von Windows Vista mit Windows Server 2008 sind Zugriffe auf Offlinedateien wesentlich effizienter (siehe auch Kapitel 6). Die Synchronisierung ist schneller und stabiler. Der Wechsel zwischen Offline- und Onlinezustand ist flexibler. Im laufenden Betrieb können geöffnete Dateien von offline zu online gewechselt werden, was die Verwendung der Offlinedateien optimiert, weil Anwender weniger beachten müssen. Offlinedateien können über Gruppenrichtlinien konfiguriert werden.

Richtlinienbasierter Quality of Service (QoS)

Im Zusammenspiel von Windows Vista und Windows Server 2008 lässt sich Netzwerkverkehr auf Basis von Gruppenrichtlinien priorisieren. Dadurch kann zum Beispiel der Netzwerkverkehr der ERP-Anwendung höher priorisiert werden, als Zugriffe auf den Mail-Server. So wird der Zugriff auf wichtige Anwendungen im Unternehmen deutlich beschleunigt.

Abbildg. 24.16 Richtlinienbasierten Quality of Service (QoS) verwenden



Die Richtlinien unterstützen neben IPv4 zusätzlich IPv6, da Windows Vista und Windows Server 2008 auf dem gleichen Netzwerkstack aufbauen in dem IPv6 integriert ist (siehe Kapitel 7). Die Richtlinien können generell auf alle Server oder basierend auf OUs gelegt werden. Auch speziellen Anwendern, zum Beispiel der Buchhaltung oder Geschäftsführung, können höhere Prioritäten zugewiesen werden. Die Richtlinien werden auf Basis eines Assistenten erstellt. Die Richtlinien können aber nicht nur auf der Grundlage von IP-Adressen definiert werden, sondern auch auf Basis von Benutzernamen oder speziellen ausführbaren Dateien.

Server Message Block 2.0

Windows Vista und Windows Server 2008 verwenden beide SMB 2.0. Dadurch wird der Zugriff auf Dateien wesentlich beschleunigt, vor allem beim Zugriff über das Netzwerk. Auch der Zugriff auf Dateien über langsame Leitungen wird dadurch beschleunigt.

Microsoft Office 2007 im Windows Server 2008-Netzwerk

In diesem Abschnitt zeigen wir Ihnen die Möglichkeiten, um Office 2007 optimal in Unternehmen zu verteilen. Die Automatisierungsmöglichkeiten mit dem Windows Installer (*Msiexec.exe*), die noch unter Office 2003 funktioniert haben, können für Office 2007 nicht mehr eingesetzt werden. Mit der neuen Office-Version hat Microsoft aber mehr Möglichkeiten zur Verfügung gestellt, über welche die Installation vereinfacht und automatisiert werden kann. Zusätzlich wurde das Setupprogramm um neue Funktionen erweitert.

Das Microsoft Office Customization Tool

Mit dem neuen Microsoft Office Customization Tool wird über eine grafische Oberfläche die Installation von Office 2007 angepasst und automatisiert. Das Tool ersetzt die bisherigen Werkzeuge zur automatischen Office-Installation, den Custom Installation Wizard und Custom Maintenance Wizard. Änderungen, die mit dem Office Customization Tool am Office-Setup vorgenommen werden, speichert das Programm in einem Setup Customization File. Die Datei erhält als Endung **.msp*. Beim Start des Office-Setupprogrammes wird diese Datei mitgegeben, die dazu im Unterordner *\Updates* des Installationsverzeichnisses abgelegt werden sollte. Befindet sich eine MSP-Datei in diesem Verzeichnis, wird diese automatisch bei der Installation verwendet, unabhängig davon, ob es sich um eine Installationsdatei oder einen Patch handelt. Ist auf einem Computer bereits 2007 Office System installiert, können über diese Datei Anpassungen vorgenommen werden. Befinden sich auf einem Computer zum Beispiel Word, Excel, Access und Outlook und wird in der MSP-Datei zur Steuerung der Installation kein Access vorgesehen, wird beim Aufrufen des Office 2007-Setupprogramms Access 2007 automatisch vom Computer entfernt.

Neben MSP-Dateien kann auch die Standardkonfigurationsdatei *config.xml* von Office 2007 angepasst werden. Mehr zu dieser Datei erfahren Sie am Ende des Abschnitts. Allerdings ist das Anpassen der Standardkonfigurationsdatei im Vergleich zu MSP-Dateien kein effizienter Weg, da hier deutlich weniger Optionen zur Verfügung stehen. Die Konfigurationsdatei kann dafür aber auf einfachem Weg angepasst werden, und zur automatisierten Installation lassen sich angepasste MSP- und Config.XML-Dateien auch parallel einsetzen. Außerdem unterstützen viele Office-Editionen, darunter auch die Small Business-, Standard- und Professional-Edition kein OCT. Hier muss der Weg über die Konfigurationsdatei zur Automatisierung gewählt werden. Um das Office Customization Tool zu starten, wird das Setupprogramm mit der Option */admin* gestartet oder das Business Desktop Deployment Kit (BDD) 2007 verwendet. Beide Möglichkeiten beschreiben wir in diesem Abschnitt noch ausführlicher. Wie bereits bei Office 2003 steht diese Möglichkeit aber leider nicht in allen Editionen zur Verfügung. Nur die Editionen Professional Plus und Enterprise unterstützen die automatisierte Installation über das OCT. Andere Editionen müssen über Skripts, zum Beispiel per AutoIt,

direkt in Images von Windows Vista integriert werden oder die Konfigurationsdatei verwenden. Wird der Befehl *setup /admin* bei einer nicht kompatiblen Office-Edition verwendet, erscheint eine Fehlermeldung, dass Dateien fehlen.

Netzwerkanalyse für Microsoft Office 2007

Das Standard-Dateiformat von Office 2007 sind XML-basierte DOCX-Dokumente. Diese lassen sich standardmäßig nicht mit Office 2003-Programmen lesen. Microsoft stellt für Office 2003 aber die kostenlose Erweiterung *Microsoft Office Compatibility Pack für Dateiformate von Word, Excel und PowerPoint 2007* zur Verfügung. Mit dieser Erweiterung sind die 2003er-Varianten der Office-Programme in der Lage, DOCX-Dokumente zu lesen, zu bearbeiten und auch wieder zu speichern. Allerdings stellt dieser Zustand sicherlich nur für eine Übergangszeit eine sinnvolle Lösung dar. Auf Dauer sollte im Unternehmen möglichst mit einem einheitlichen Format gearbeitet werden. Zur Analyse stellt Microsoft die Office Migration Planning Manager (OMPM)-Suite kostenlos zur Verfügung. Mit dieser Sammlung von Befehlszeilentools, werden die Computer im Netzwerk auf Office-Dokumente durchsucht, sodass ein Überblick geschaffen wird, welche Dokumente es überhaupt gibt. Erfahrungsgemäß ist die Anzahl an Dokumenten so groß, dass in den wenigsten Unternehmen sinnvolle Informationen durch das manuelle Durchsuchen erhalten werden.

Nach dem Download (siehe die Links am Kapitelende) und Entpacken der Sammlung wird über das Programm *Offscan.exe* der Scanvorgang gestartet. Die entsprechenden Einstellungen werden zuvor in der Datei *Offscan.ini* vorgenommen. Beide Dateien befinden sich im Unterverzeichnis *\Scan* des OMPM-Installationsordners. Fakt ist, dass nach der Migration zu Office 2007 alle Dokumente, die mit Vorgängerversionen erstellt wurden, noch funktionieren müssen. Das stellt zwar meistens kein Problem dar, vor allem weil Office 2007 in der Lage ist, Dokumente auch im Office 2000/2003-Format zu speichern. Allerdings besteht die Möglichkeit, vor allem bei komplexen Excel 2003-Tabellen, dass diese unter Excel 2007 nicht mehr funktionieren. Zur Analyse mit dem OMPM wird auf einem Rechner die Access 2007 Runtime-Erweiterung benötigt.

Zum Downloadpaket des OMPM gehört auch der Office File Converter (OFC). Auch hierbei handelt es sich um ein Befehlszeilentool. Mit dem OFC werden Dateien, die der OMPM als nicht kompatibel zu Office 2007 deklariert, entsprechend umgewandelt. Unnötig zu sagen, dass bei diesem Vorgang eine vorherige Datensicherung erfolgen sollte. Mit dem Version Extraction Tool (VET) aus dem OMPM, werden verschiedene Versionen beispielsweise von Word 2003-Dokumenten in mehrere Dateien extrahiert. Dieser Vorgang ist allerdings selten notwendig. Wichtig ist dagegen der Scan mit *Offscan.exe*, damit sichergestellt ist, dass nach der Migration zu Office 2007 wichtige Tabellen noch funktionieren. Ob hier mit dem OFC automatisch konvertiert werden soll, manuell nachgearbeitet wird, oder entsprechende Rechner gar nicht erst umgestellt werden, muss individuell entschieden werden. Auf jeden Fall sollte vor der Migration eine Diagnose stehen, welche Dateien überhaupt betroffen sind.

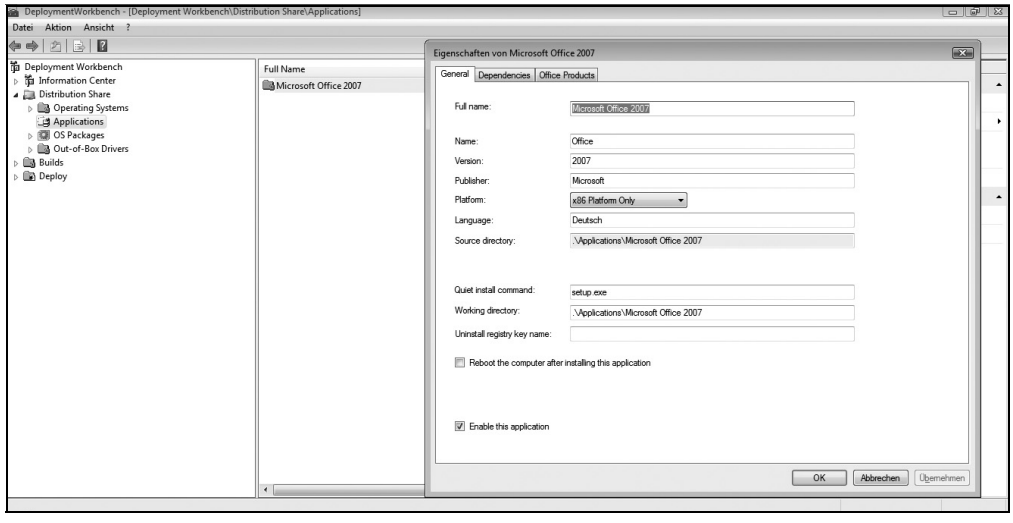
Office 2007 in BDD integrieren

Wie bei der Verteilung von Windows Vista stellt das Business Desktop Deployment Kit (BDD) 2007 und sein Nachfolger Microsoft Deployment auch für die Verteilung von Office 2007 im Unternehmen die beste Möglichkeit dar. Zwar lässt sich das Office Customization Tool auch ohne das BDD starten. Wenn aber BDD bereits für die Distribution von Vista eingesetzt wird, bietet sich die Ver-

wendung auch für Office an. Das BDD wird, wie das WAIK, kostenlos zur Verfügung gestellt und kann zur automatischen Installation von Windows Vista oder Office 2007 auf einem Admin-PC installiert werden. Sofern die Sammlung noch nicht installiert ist, kann diese bei Microsoft kostenlos heruntergeladen werden (siehe die Links am Kapitelende). Auf dem Rechner sollte neben dem BDD 2007 auch das Windows Automated Installation KIT (WAIK) installiert werden, da bei der Anpassung des Office-Setups unter Umständen auch Komponenten von dieser Sammlung benötigt werden. Der erste Schritt zur automatisierten Office-Installation über das BDD ist das Einlegen des Office-Datenträgers in das Laufwerk des Rechners, auf dem die Anpassungen vorgenommen werden.

Um die Office 2007-Installation anzupassen, muss zunächst die Deployment Workbench des Tools über die entsprechende Programmgruppe gestartet werden. Als Nächstes wird in der Konsole der Knoten *Distribution-Share* erweitert und der Eintrag *Applications* mit der rechten Maustaste angeklickt. Aus dem Kontextmenü muss jetzt *New* ausgewählt werden. Über diesen Weg wird die automatisierte Installation von Office 2007 in das BDD integriert. Bei der Erstellung der Anwendung muss die Option *Application with source files* aktiviert werden, da die Office-Installationsdateien im Netz zur Verfügung stehen und angepasst werden sollen.

Abbildg. 24.17 Durch die Integration von Office 2007 in das BDD 2007 kann die automatisierte Installation angepasst werden

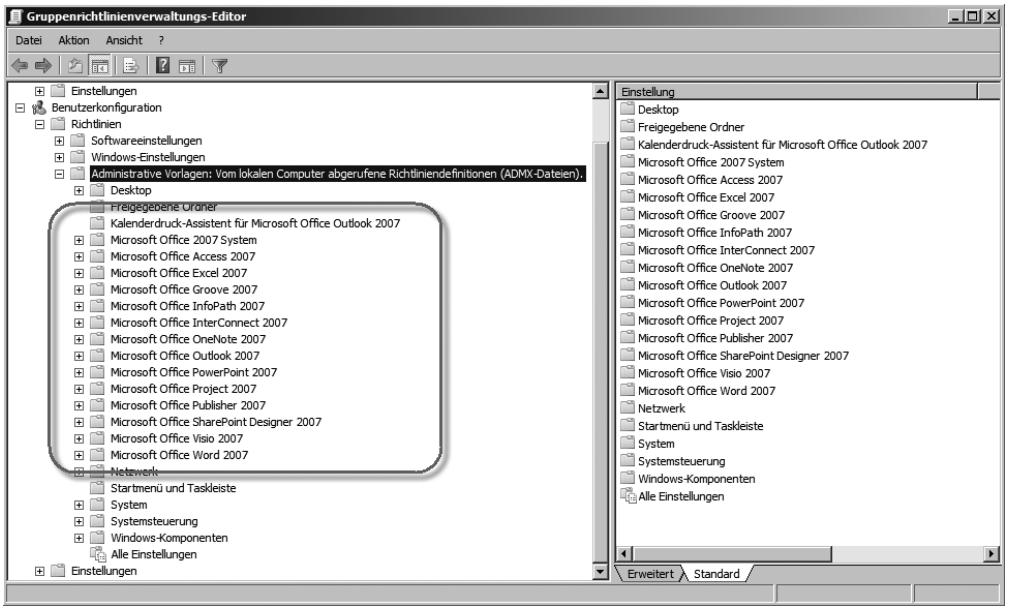


Neben den Office-Installationsoptionen, lassen sich über das OCT auch Einstellungen für Outlook-Profile festlegen. Wird im Unternehmen Exchange Server 2007 eingesetzt, ist das Hinterlegen des Postfachservers nicht mehr notwendig, wenn Outlook installiert wird. Durch die Auto-Discovery-Funktion von Outlook 2007/Exchange Server 2007 wird der Postfachserver des Anwenders beim ersten Start von Outlook automatisch erkannt und eingetragen. Weitere Outlook-Einstellungen lassen sich über Gruppenrichtlinien durchführen. Im Downloadcenter stellt Microsoft Gruppenrichtlinien-Vorlagen für Windows Server 2003 und Windows Server 2008 zur Verfügung, über die Office 2007 per Richtlinie angepasst werden kann. Damit diese unter Windows Server 2008 verwendet werden, müssen die ADMX-Dateien nach dem Entpacken auf dem Domänencontroller in das Verzeichnis *C:\PolicyDefinitions* kopiert werden. Die Gruppenrichtlinien-Sprachdateien *(*.adml)* müs-

sen aus dem jeweiligen Sprachenordner in den Ordner unter *C:\PolicyDefinitions* kopiert werden. Ein Import in die Gruppenrichtlinien wie bei Windows Server 2003 ist unter Windows Server 2008 nicht notwendig.

Nach dem Kopieren sind die Vorlagen sofort verfügbar. So können zum Beispiel in der Gruppenrichtlinienverwaltung über *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen* zahlreiche Einstellungen für Office 2007 vorgenommen werden, um die automatische Einrichtung weiter zu verbessern. Für Outlook lassen sich zum Beispiel der Speicherort der PST- und OST-Dateien, deren maximale Größe und die Rechte für Benutzer sehr modular steuern. Für jede Einstellung wird auf der Registerkarte *Erklärung* eine ausreichende Hilfe gegeben.

Abbildg. 24.18 Über Gruppenrichtlinien lassen sich Office 2007-Einstellungen weiter verbessern



Nachdem diese Option festgelegt ist, werden im nächsten Fenster Informationen zur neuen Anwendung angegeben. Diese Werte können frei gewählt werden. Als Nächstes wird das Quellverzeichnis festgelegt, das die Office-Dateien enthält. Im genannten Verzeichnis muss es sich um den Speicherort handeln, der den kompletten Office 2007-Datenträger enthält. An dieser Stelle muss noch keine Freigabe verwendet werden. Beim Abschluss der Aktion werden die notwendigen Quelldateien automatisch auf die Distributionsfreigabe kopiert oder verschoben, je nachdem welche Aktion ausgewählt wird. Aus dieser Freigabe können später die Installationsdateien in jedes beliebige Verzeichnis oder jede Freigabe verschoben werden.

Als Nächstes wird im BDD der Verzeichnisname ausgewählt, der in der Distributionsfreigabe automatisch für die Installationsdateien erstellt wird. Nachdem das Verzeichnis ausgewählt wurde, muss noch der Befehl eingegeben werden, der das Office-Installationsprogramm startet, in diesem Fall also *setup.exe*. Mit der Schaltfläche *Add* kopiert das Programm jetzt die notwendigen Installationsdateien von der DVD auf den Computer. Anschließend steht das Paket in der BDD zur Konfiguration zur Verfügung. Über die Eigenschaften im Kontextmenü des Pakets findet die Anpassung statt. Auf der Registerkarte *Office Products* wird die Anpassung über die Schaltfläche *Office Customization*

Tool gestartet. Diese Schaltfläche steht aber nur dann zur Verfügung, wenn die hinterlegte Office-Edition das Office Customization Tool (OCT) unterstützt. Anschließend besteht die Möglichkeit, eine vorhandene MSP-Datei zu editieren oder eine neue Datei zu erstellen.

Nachdem das OCT gestartet wurde, können die einzelnen Möglichkeiten zur Automatisierung per Mausklick festgelegt werden. Auf der linken Seite wird der generelle Bereich zur Automatisierung ausgewählt, auf der rechten Seite werden die Detailinformationen konfiguriert. Alle hier angebotenen Optionen können konfiguriert und in der MSP-Datei zur automatischen Installation hinterlegt werden.

Abbildg. 24.19 Im Office Customization Tool (Office-Anpassungstool) werden die einzelnen Optionen für die MSP-Datei festgelegt

Nachdem alle Einstellungen vorgenommen wurden, wird die MSP-Datei im Verzeichnis *\Updates* gespeichert. Wird die Installation von Office gestartet, zum Beispiel über einen Eintrag in einem Anmeldeskript, findet die Installation automatisiert statt, da die MSP-Datei verwendet wird. Als Quell-Verzeichnis wird entweder eine Distributionsfreigabe des BDD oder eine herkömmliche Netzwerkfreigabe verwendet. In diese werden die Installationsdateien mit dem *\Updates*-Verzeichnis kopiert, das die angepassten MSP-Dateien und eventuell sogar das Service Pack 1 für Office 2007 enthält. Das Service Pack lässt sich leicht in den Distributionsordner integrieren, doch dazu später mehr. Als Berechtigung für die Freigabe kann zum Beispiel ein eigenes Benutzerkonto in der Domäne erstellt werden, beispielsweise *office-install*. Die Freigabe wird zur Installation ans Netzlaufwerk verbunden und der Benutzer wird dazu mit angegeben. Diese Aktion kann über eine Batchdatei abgewickelt werden, in der das Laufwerk verbunden, die Installation gestartet und das Laufwerk wieder getrennt wird. Der Installationsdatei kann auch, parallel zu einer speziellen MSP-Datei, eine angepasste Konfigurationsdatei mitgegeben werden, beispielsweise mit *setup.exe /adminfile b:\office2007\Updates\off_ent.MSP /config b:\office2007\enterprise.WW\config.xml*. Zu den Konfigurationsdateien kommen wir später noch ausführlicher.

Die Setupoptionen von Office 2007

Neben den Möglichkeiten die Office 2007-Installation über MSP-Dateien im BDD zu beeinflussen, kann das Setupprogramm auch mit speziellen Optionen gestartet werden. So kann zum Beispiel mit der Option */admin* das Office Customization Tool ohne das BDD gestartet werden. Die anschließende Konfiguration ist identisch zur Anpassung im BDD. Allerdings wird auch hier diese Option nicht von allen Office-Editionen unterstützt. Es gelten die gleichen Einschränkungen wie beim BDD. Mit der Option */adminfile <MSP-Datei>* wendet das Installationsprogramm die angegebene MSP-Datei an. Standardmäßig wendet das Office-Installationsprogramm alle MSP-Dateien an, die im Verzeichnis *\Updates* liegen. Soll bei einer Installation aber nur eine bestimmte Datei verwendet werden, kann diese über die Option */adminfile* mitgegeben und in einem anderen Verzeichnis gespeichert werden. MSP-Dateien im Verzeichnis *\Updates* werden immer automatisch ausgeführt, egal wie viele hinterlegt werden. Mit der Option */config <Konfigurationsdatei>* kann das Setupprogramm angewiesen werden, eine andere Konfigurationsdatei zu verwenden, als bei einer normalen Installation. Wie bereits beschrieben, besteht auch die Möglichkeit, parallel zu MSP-Dateien Einstellungen für die Installation per Konfigurationsdatei mitzugeben.

Die Standardkonfigurationsdatei mit der Bezeichnung *config.xml* befindet sich im Office 2007-Installationsordner im Verzeichnis *<Edition>.ww*, also zum Beispiel *<Prof.ww>*. Einstellungen in der Datei *config.xml* überschreiben immer Einstellungen aus MSP-Dateien. Die Datei ersetzt die unter Office 2003 eingesetzte Datei *setup.ini* und funktioniert bei allen Editionen. Auch die Befehlszeilenoptionen des Office-Setupprogramms gibt es unter Office 2007 nicht mehr. Alle Optionen werden jetzt über die Datei *config.xml* gesteuert. Die Konfigurationsdatei wird zum Beispiel verwendet, wenn die Verteilung von Office über Gruppenrichtlinien durchgeführt werden soll oder eine Edition verwendet wird, die das OCT nicht unterstützt. Bei der Verteilung über Gruppenrichtlinien können keine MSP-Dateien verwendet werden. Über Konfigurationsdateien können allerdings weniger Einstellungen vorgenommen werden: Das zu installierende Produkt kann ausgewählt werden, sowie der Benutzer und die Firma, auf die das Produkt registriert ist. Der Lizenzschlüssel und zusätzliche Sprachpakete lassen sich ebenfalls übergeben. Aber Achtung: Im Gegensatz zur MSP-Datei wird der Produktschlüssel in der *config.xml* in Klartext, das heißt für jeden lesbar, hinterlegt.

Auch das Quellverzeichnis und das Installationsverzeichnis kann über die *config.xml* konfiguriert werden. Die Datei sollte am besten mit einem normalen Editor bearbeitet werden oder mit dem kostenlosen Microsoft XML Notepad 2007. Die wichtigsten Optionen in der Datei haben wir für Sie in der folgenden Tabelle dargestellt.

Tabelle 24.1 Variablen zur automatisierten Installation von Office 2007

Element	Beschreibung
AddLanguage	Fügt der Installation ein Sprachpaket zu Beispiel: <AddLanguage Id="en-US" />
ARP	Bestimmt das Verhalten, wie das Produkt in der Systemsteuerung angezeigt wird Beispiel: <ARP ARPCOMMENTS="Basisinstallation Office" />
COMPANYNAME	Der Firmenname oder Benutzer, der das Produkt erworben hat Beispiel: <COMPANYNAME Value="IT Administrator" />

Tabelle 24.1 Variablen zur automatisierten Installation von Office 2007 *(Fortsetzung)*

Element	Beschreibung
Command	Mit diesem Element werden während der Installation von Office eigene Befehle, Skripts oder Anwendungen gestartet. Beispiel: <Command Path=\\BDD2007\Skript\Inventory.vbs />
Display	Dieses Element legt fest, was während der Installation auf dem Bildschirm des Benutzers angezeigt werden soll. Es findet nur dann Verwendung, wenn die Konfigurationsdatei sich entweder im gleichen Ordner wie die aufrufende *Setup.exe* befindet oder durch Verwendung der »/config«-Befehlszeilenoption explizit angegeben wird. Beispiel: <Display Level="None" CompletionNotice="No" SuppressModal="No" AcceptEula="Yes" />
DistributionPoint	Legt fest, wo sich die Installationsdateien im Netzwerk befinden, also von wo aus die Installation gestartet werden soll Beispiel: <DistributionPoint Location="\\BDD2007\Office" />
INSTALLLOCATION	Diese Option legt fest, in welchem Ordner Office installiert wird. Hier können auch Variablen genutzt werden. Wird dieses Element nicht angegeben, findet die Installation im Ordner *%ProgramFiles%\Microsoft Office* statt. Beispiel: <INSTALLLOCATION Value="%SystemDrive%\Office2007" />
Logging	Dieses Element bestimmt, wie die Installation protokolliert wird. Beispiel: <Logging Type="Verbose" Path="%temp%" Template="Office2007.txt" />
OptionState	Legt die zu installierenden Komponenten der Office Suite fest. Weitere Informationen finden Sie im Office 2007 Resource Kit im Dokument »Config.xml File OptionState Id Values«. Beispiel: <OptionState Id="PubPrimary" State="Absent" Children="force" /> (Die Komponente »Publisher« wird inklusive aller Features nicht installiert.)
PIDKEY	Legt den Lizenzschlüssel für die Installation fest
Setting	Ermöglicht es, Parameter für den Windows Installer Dienst zu übergeben. Bei der Übergabe eines nicht unterstützten Parameters stoppt die Installation. Weitere Informationen finden Sie im Office 2007 Resource Kit im Dokument »Setup properties in the 2007 Office System«. Beispiel: <Setting Id="SETUP_REBOOT" Value="NEVER" /> (Führt nach oder während der Installation keinen Neustart des Systems durch.)
SetupUpdates	Legt fest, ob und in welchem Netzwerkpfad nach Anpassungsdateien gesucht werden soll, die mit dem Office Customization Tool erstellt wurden. Alle in dem angegebenen Pfad befindlichen Dateien werden nach Dateinamen sortiert und dann angewandt. Sie können mehrere Netzwerkpfade angeben. Diese müssen dann per Semikolon getrennt werden. Beispiel: <SetupUpdates CheckForUpdates="Yes" SUpdateLocation="\\BDD2007\Office\Updates" />

Tabelle 24.1 Variablen zur automatisierten Installation von Office 2007 *(Fortsetzung)*

Element	Beschreibung
SOURCELIST	Bestimmt, wo die Installationsdateien der 2007 Microsoft Office Suite im Netzwerk liegen. Es können mehrere Quellen angegeben werden, die durch ein Semikolon getrennt werden. Beispiel: <SOURCELIST Value=\\BDD2007\Office;\\BACKUP\Office />
USERINITIALS	Die Initialen des Benutzers, der mit dieser Office-Installation arbeiten wird Beispiel: <USERINITIALS Value="CD" />
USERNAME	Der vollständige Name des Benutzers, der mit dieser Office-Installation arbeiten wird Beispiel: <USERNAME Value="Thomas Joos" />

Verteilung über Systems Management Server 2003 oder System Center Essentials 2007

Neben der Verteilung von Office 2007 über den Systems Management Server (SMS) 2003 oder dessen Nachfolger System Center Configuration Manager 2007 besteht neben den hier beschriebenen Wegen, auch die Möglichkeit, die neuen Microsoft System Center Essentials 2007 zu verwenden. Die Microsoft System Center Essentials (SCE) 2007 richten sich an mittelständische Unternehmen bis maximal 30 Server und 500 Arbeitsstationen. Bei dieser Serverlösung handelt es sich um eine Servertechnologie zur einfachen Verwaltung, Inventarisierung, Softwareverteilung und Betriebsüberwachung von Servern und Arbeitsstationen im Unternehmen. Das Produkt basiert auf Technologien aus dem Microsoft System Center Operations Manager (SCOM) 2007, dem System Center Configuration Manager (SCCM) 2007 und den Windows Server Update Services 3.0. Über das Produkt lässt sich auch Office 2007 leicht in Unternehmen verteilen.

Abbildg. 24.20 Office 2007 lässt sich auch effizient über Microsoft System Center Essentials in Unternehmen verteilen

Das Service Pack 1 in den Installationsordner integrieren

Ein wichtiger Punkt bei der Verteilung von Office 2007 im Unternehmen ist die Integration von Office 2007 Service Pack 1 in das Installationsverzeichnis. Dieser Vorgang wird üblicherweise als Slipstreaming bezeichnet, auch wenn diese Beschreibung bei Office 2007 nicht mehr zutrifft. Bei Office 2007 verhält sich dieser Vorgang komplett anders als bei seinen Vorgängerversionen. Die Installationsdateien werden hier nicht ausgetauscht, sondern das Service Pack wird hinzugefügt. Zunächst muss die EXE-Datei, die das Service Pack enthält, bei Microsoft heruntergeladen werden (siehe die Links am Kapitelende). Anschließend wird das Updatepaket mit dem Befehl *office2007sp1-kb936982-fullfile-de-de.exe /extract* gestartet. Für jede Sprache gibt es ein eigenes Paket, der Vorgang zur Integration ist aber immer der gleiche. Nach der Eingabe des Befehls müssen zunächst die Lizenzbedingungen bestätigt und das Verzeichnis ausgewählt werden, in das die Dateien des Service Packs entpackt werden. Da während der Installation von Office 2007 automatisch alle MSP-Dateien aus dem Verzeichnis *\Updates* des Installationsverzeichnisses ausgeführt werden, müssen die Dateien des Service Packs auch in dieses Verzeichnis entpackt werden. Die einzelnen Updates aus dem Service Pack liegen als MSP-Datei vor, sodass auf einen Rutsch Office 2007 mit SP1 installiert wird. Bereits installierte Office-Pakete werden entweder über WSUS 3.0 oder Windows Update aktualisiert. Durch die Option */quit* des SP1-Installationsprogramms wird eine unbeaufsichtigte und automatische Installation durchgeführt. So kann zum Beispiel auch über ein Anmeldeskript das SP1 auf Arbeitsstationen mit Office 2007 verteilt werden. Ob das Service Pack installiert ist, lässt sich am schnellsten über die Office-Schaltfläche, zum Beispiel in Word, und einem Klick auf die Schaltfläche *Word-Optionen* feststellen. Nach Auswahl der Kategorie *Ressourcen* wird ganz unten der Versionsstand des Programms angezeigt.

Abbildg. 24.21 Ob das Service Pack 1 für Office 2007 auf einem Rechner installiert ist, lässt sich über die Word-Optionen feststellen

Office 2007 kann auch PDF-Dateien schreiben

Mit der Erweiterung *Add-In für 2007 Microsoft Office: Speichern unter – PDF* sind die Office 2007-Programme offiziell in der Lage, PDF-Dateien zu erzeugen. Dieser Zusatz muss aber getrennt heruntergeladen und installiert werden. Wird Office 2007 automatisiert im Unternehmen verteilt, kann im Office Customization Tool im Bereich *Installationen hinzufügen und Programme ausführen* gleich die Installation dieser Erweiterung hinterlegt werden. Dazu muss einfach die Datei *SaveAsPDFandXPS.exe* zur Ausführung hinterlegt werden. Ist die Erweiterung installiert, können Anwender über das herkömmliche *Speichern unter*-Dialogfeld PDF- und XPS-Dateien hinterlegen.

TIPP **Wichtige Links:**

- **Access 2007 Runtime** *http://go.microsoft.com/fwlink/?LinkId=83030*
- **Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats** *http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=941b3470-3ae9-4aee-8f43-c6bb74cd1466*
- **2007 Microsoft Office System Migration Guidance: Microsoft Office Migration Planning Manager** *http://www.microsoft.com/downloads/details.aspx?familyid=13580cd7-a8bc-40ef-8281-dd2c325a5a81&displaylang=en#filelist*
- **Einstiegsseite für das BDD 2007** *http://www.microsoft.com/germany/technet/desktopdeployment/default.mspx*
- **Download WAIK** *http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=de*
- **Microsoft XML Notepad 2007** *http://www.microsoft.com/downloads/details.aspx?FamilyID=72d6aa49-787d-4118-ba5f-4f30fe913628&DisplayLang=en*
- **Office 2007 Resource Kit** *http://technet2.microsoft.com/Office/en-us/library/9df1c7d2-30a9-47bb-a3b2-5166b394fbf51033.mspx?mfr=true*
- **Office 2007 SP1** *http://www.microsoft.com/downloads/details.aspx?familyid=9ec51594-992c-4165-a997-25da01f388f5&displaylang=de*
- **Office 2007 PDFs speichern** *http://www.microsoft.com/downloads/details.aspx?FamilyID=f1fc413c-6d89-4f15-991b-63b07ba5f2e5&displaylang=de*
- **Informative Seite mit Anleitungen für die Office 2007-Installation** *http://beqiraj.com/office/2007/unattended/index.asp*

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, welche Neuerungen es mit dem Service Pack 1 für Windows Vista gibt und wie Sie das Service Pack am besten im Unternehmen verteilen. Auch die Installation von Office 2007 läuft am besten automatisiert ab, da dadurch Standardisierungen im Unternehmen möglich sind. Mit ein paar Tricks und Kniffen lässt sich Windows Vista außerdem noch etwas beschleunigen. Die beste Leistung aller drei Systeme holen Sie heraus, wenn Sie Windows Server 2008, Windows Vista und Microsoft Office 2007 zusammen im Unternehmen einsetzen, sowie die neusten Service Packs installieren.

Kapitel 25

Virtualisierung mit Hyper-V

In diesem Kapitel:

Mit Hyper-V bietet Microsoft erstmals eine in das Betriebssystem integrierte Lösung zur Virtualisierung an. Mit Windows Server 2008, Hyper-V und optional noch mit dem System Center Virtual Machine Manager (SCVMM) 2007/2008 bietet Microsoft die Möglichkeit, Virtualisierung im Unternehmen ohne Programme von Drittanbietern durchzuführen. Virtuelle Rechner erstellen Administratoren mit Hyper-V unter Windows Server 2008. Mit Hilfe von SCVMM lassen sich diese dann verwalten und mit System Center Operations Manager 2007 überwachen. Hyper-V bietet mit der Hypervisor-Technologie eine direkte Verbindung mit den Virtualisierungsfunktionen der aktuellen AMD- und Intel-Prozessoren.

Ein weiteres Produkt der Hyper-V-Familie ist Microsoft Hyper-V Server 2008. Dieses Produkt stellt Microsoft kostenfrei als Download zur Verfügung. Technisch gesehen handelt es sich bei Microsoft Hyper-V Server 2008 um einen Windows Server 2008 Core-Server, der nur die Virtualisierungsfunktion enthält. Auf dem Server lassen sich neben Windows auch andere Betriebssysteme wie zum Beispiel Linux virtualisieren. Den Download sowie weitere Informationen zum Produkt finden Sie auf der Website *http://www.microsoft.com/servers/hyper-v-server*.

Die Grundlagen von Hyper-V

Hyper-V besteht aus einer kleinen, hochspezialisierten Softwareschicht, dem so genannten Hypervisor, die direkt zwischen der Serverhardware und den virtuellen Computern positioniert ist. Die Software partitioniert die Hardwareressourcen eines Servers. Dabei lassen sich übergeordnete und untergeordnete Partitionen, so genannte Parent-VMs und Child-VMs erstellen (VM steht dabei für *Virtuelle Maschine*). Während in der Parent-VM die Prozesse der virtuellen Maschine, der WMI-Provider (Windows Management Instrumentation) und der VM-Dienst laufen, sind in den Child-VMs die Anwendungen positioniert. Die Parent-VM verwaltet auch die Treiber der Computer. Hyper-V benötigt, im Gegensatz zu vielen anderen Virtualisierungslösungen, keine speziellen Treiber für aktuelle Hardware. Die Parent-VM ist sozusagen das eigentliche Hostsystem, während die Child-VMs die virtuellen Computer darstellen. Dabei tauscht nur die Parent-VM Informationen mit Hyper-V direkt aus. Untergeordnete Partitionen stellen die Anwendungen im Benutzermodus zur Verfügung, während der Kernelmodus nur die Virtualization Service Clients (VSC) und den Windows-Kernel betreibt. Dadurch steigert sich in der Theorie neben der Geschwindigkeit auch die Stabilität der Computer.

Damit die virtuellen Computer funktionieren, nimmt Hyper-V kleinere Änderungen am Kernel der Gastsysteme vor, ähnlich wie auch XEN es tut. Installieren Sie die Hyper-V-Serverrolle, setzt Windows die Boot Configuration Database (BCD)-Einstellung *hypervisorimagelaunchtypeboot* auf *auto* (automatisch) und konfiguriert den Gerätetreiber *Hvboot.sys*, um diesen beim Start des Betriebssystems sehr früh zu laden. Das System ist dadurch auf die Virtualisierung vorbereitet und lädt entweder *%SystemRoot%\System32\Hvax64.exe* (AMD-V) oder *%SystemRoot%\System32\Hvix64.exe* (Intel VT-CPU) in den Speicher. Nach dem Start von Hyper-V verwendet der Treiber die Virtualisierungserweiterungen. Benutzermodusanwendungen verwenden die Berechtigungsstufe Ring 3 des x64-Prozessors, der Kernel den Ring 0. Hypervisor arbeitet auf der Berechtigungsstufe darunter, denn er kann Code, der auf der Stufe Ring 0 ausgeführt wird, kontrollieren. Verwenden Sie nach der Installation die Hyper-V-Verwaltungskonsole, um eine untergeordnete Partition zu erstellen, verwendet diese den Treiber *%SystemRoot%\System32\drivers\Winhv.sys*.

Durch die enge Kooperation von Microsoft mit den XEN-Entwicklern ist viel Know-how dieser Virtualisierungslösung auch in Hyper-V eingeflossen. Hyper-V unterstützt die AMD- und Intel-Virtualisierungsfunktionen für x64-Server-Prozessoren und setzt diese für den Einsatz sogar voraus. Dies bedeutet, dass x86-Computer von der Virtualisierung zumindest als Hostsystem ausgeschlossen sind.

HINWEIS Hyper-V lässt sich nur auf x64-Bit-Servern mit Intel VT- oder AMD-V-Erweiterungen installieren.

Technologische Basis von Hyper-V ist eine 64-Bit-Softwareschicht, die zwischen der Hardware und dem Betriebssystem platziert ist und die die Hardwareressourcen des physischen Windows Server 2008-Hostsystems auf die einzelnen virtuellen Rechner verteilt. Administratoren ordnen die Ressourcen, zum Beispiel CPU und Arbeitsspeicher des Hostsystems, den virtuellen Betriebssystemsitzungen exakt zu. Hyper-V verwendet »synthetische« Gerätetreiber, sodass für I/O-Zugriffe keine Softwareemulation erforderlich ist. Die Geschwindigkeit der virtuellen Computer wird durch diese Funktion stark gesteigert. Microsoft setzt übrigens bereits selbst auf Hyper-V. Die Entwicklerseiten von TechNet und MSDN laufen seit einiger Zeit auf mit Hyper-V virtualisierten Serversystemen.

Wie Virtual Server 2005 R2 unterstützt auch Hyper-V Linux als Gastbetriebssystem. So ist es beispielsweise möglich, auf einem Windows Server 2008-Hostsystem einen virtuellen 64-Bit-Server, einen 32-Bit-Server und ein Linux-System parallel zu betreiben. Offiziell unterstützt Hyper-V vor allem Suse Linux Enterprise Server 10 mit SP1. Neben 32-Bit- und 64-Bit-Systemen unterstützt Hyper-V auch Mehrprozessorsysteme als Gast. Auch Windows Vista mit SP1 und Windows XP SP3 unterstützt Hyper-V.

Hyper-V lässt sich in System Center Virtual Machine Manager integrieren, aber auch in einer eigenständigen Verwaltungskonsole (MMC) unter Windows Server 2008 verwalten. Hyper-V ist außerdem eine Serverrolle für den Server Core-Betriebsmodus von Windows Server 2008. Durch das reduzierte Hostbetriebssystem können Administratoren ihre ganze Aufmerksamkeit den virtuellen Computern widmen. Während der Installation von Windows Server 2008 lässt sich auswählen, ob der Server komplett installiert werden soll oder ob der Installationsassistent eine Core-Version installieren soll. Nach der Installation bietet ein Core-Server nicht die gewohnte grafische Benutzeroberfläche. Die Verwaltung eines solchen Servers findet ausschließlich über die Befehlszeile statt. Es gibt kein Startmenü, keine Systemsteuerung, keine Snap-Ins für die MMC. Es besteht aber die Möglichkeit, einen solchen Server über das Netzwerk mit den Snap-Ins auf anderen Servern zu verwalten. Auf diesem Weg lässt sich auch Hyper-V auf einem Core-Server überwachen Die Core-Installation dient der Installation eines Servers, der nur spezielle Serverrollen annehmen kann. Dazu gehören neben der Hyper-V-Rolle auch die Rollen Dateiserver, Druckserver, Streaming Media Services, Domänencontroller, Active Directory Lightweight Directory Services, DNS-Server und DHCP-Server.

Unternehmen haben bei einem Core-Server gegenüber der vollen Installation einige Vorteile. Es werden nur die notwendigen Komponenten installiert. Dadurch erhöht sich die Sicherheit, weil kein Angriff auf unnötige Funktionen stattfinden kann. Die Stabilität des Servers erhöht sich, weil nicht benötigte Komponenten keinen Absturz verursachen. Die Installation benötigt deutlich weniger Platz. Ein Core-Server ist daher die ideale Plattform als Hostsystem für die Virtualisierung.

Auch Windows PowerShell, ebenfalls in Windows Server 2008 integriert, enthält Befehle, mit denen sich virtuelle Computer starten und stoppen lassen. In Windows PowerShell lassen sich zudem Skripts zur Automatisierung erstellen. Microsoft hat auch den Windows Server 2008-Clusterdienst für die Virtualisierung verbessert. Er bindet virtuelle Computer und deren Festplatten besser in einen Failover-Cluster ein. Fällt zum Beispiel ein physischer Server aus, der mehrere virtuelle Rechner verwaltet, erkennt Hyper-V das und führt eine so genannte Quick Migration durch. Diese Technik funktioniert allerdings aktuell nur für Windows-Systeme, somit bleibt Linux derzeit außen vor. Voraussetzung ist, dass die Rechner in einem Speichernetzwerk (Storage Area Network, SAN) liegen. Der zweite physische Knoten im Cluster startet die virtuellen Computer, so dass diese den Anwendern sofort wieder zur Verfügung stehen. Diese Funktion unterstützt geplante, aber auch ungeplante Ausfälle von Clusterknoten.

Lizenzierung, Installation und Verwaltung von Hyper-V

Einer der Hauptvorteile von Hyper-V ist die direkte Integration in das Betriebssystem. Selbst die Standard-Edition von Windows Server 2008 enthält bereits eine Lizenz für Hyper-V. Unternehmen, welche auf Windows Server 2008 Standard Edition setzen, dürfen mit einer Lizenz das Hostsystem und eine virtuelle Maschine erstellen. Die Enterprise Edition von Windows Server 2008 ermöglicht die Installation des Hostsystems mit Windows Server 2008 sowie bis zu vier virtuellen Computern ohne weitere Lizenzkosten. Unternehmen, die Windows Server 2008 einsetzen, können Hyper-V als Serverrolle installieren und mit der Virtualisierung sofort loslegen. Zusatzprogramme benötigen Systemverwalter nicht, die notwendigen Verwaltungswerkzeuge sind in das Betriebssystem integriert. Von der Kostenseite her profitieren daher Unternehmen von der Virtualisierung, ohne vorher teure Zusatzlösungen kaufen zu müssen. Allerdings müssen Unternehmen virtuelle Computer genauso lizenzieren wie physische Server. Nur die Datacenter-Editionen erlauben eine uneingeschränkte Anzahl an virtuellen Computern. Da Hyper-V die integrierten Virtualisierungstechniken von AMD und Intel unterstützt, sollte vor der Installation der Serverrolle im BIOS des Rechners diese Technik aktiviert sein. Diese Funktion ist nicht auf allen Servern per Standardeinstellung bereits aktiv.

Wie von Microsoft gewohnt, lassen sich die virtuellen Computern mit Assistenten erstellen, die Ihnen bei der gesamten Einrichtung zur Seite stehen. Über Assistenten lassen sich Arbeitsspeicher, Datenträger, CD/DVD-Laufwerke und andere Hardware voreinstellen. Die eigentliche Installation der virtuellen Server läuft etwas langsamer ab, da zu diesem Zeitpunkt die Virtualisierung noch nicht an das System angepasst ist. Wer eine virtuelle Maschine installiert, muss also etwas mehr Zeit mitbringen. Nach der Installation lässt sich die Geschwindigkeit durch die *Integrationsdienste* (Integration Services) beschleunigen. Hierbei handelt es sich um eine Software, die ähnlich wie die VMware-Tools und deren Pendant in Virtual Server 2005 R2 beziehungsweise Virtual PC 2007 funktioniert. Während der Installation ersetzen die Integrationsdienste einige Systemtreiber mit neuen Versionen, die für die Virtualisierung angepasst sind und virtuelle Computer deutlich beschleunigen.

Generell ist die Verwaltung von virtuellen Computern mit der integrierten Verwaltungskonsole sehr effizient. Zusatzprogramme wie der System Center Virtual Machine Manager helfen bei der Verwaltung mehrerer Hosts, werden aber am Anfang selten benötigt, da die Bordmittel durchaus ausreichen. Allerdings lassen sich mit dem integrierten Verwaltungswerkzeug nur die virtuellen Computer eines Servers verwalten. Unternehmen, die mehrere Hostsysteme betreiben und diese gleichzeitig verwalten müssen, haben dadurch einen etwas höheren Verwaltungsaufwand. Der SCVMM kann auch mehrere Hostsysteme und deren virtuelle Computer verwalten.

System Center Virtual Machine Manager 2008

Davon abgesehen, dass die Virtualisierung in Unternehmen eines der wichtigsten Themen ist, benötigen immer mehr Firmen eine zentrale Verwaltungsoberfläche für ihre virtuelle Infrastruktur. Diese Umgebungen sind häufig heterogen und werden mit zahlreichen unterschiedlichen Werkzeugen verwaltet. Das kostet unnötig Geld und bindet Ressourcen, die an anderer Stelle im Unternehmen fehlen. Der System Center Virtual Machine Manager (SCVMM) 2008 bietet im Vergleich zu seinem Vorgänger einige sehr wichtige Änderungen. Virtuelle Maschinen lassen sich sehr viel schneller bereitstellen. Durch neue Mechanismen und Tools ist die Migration von physischen zu virtuellen Servern (P2V) sehr einfach und nahezu ohne Ausfallzeiten durchzuführen. Auch das Übertragen von virtuellen Computern zwischen den verschiedenen Virtualisierungs-Infrastukturen (V2V) ist jetzt problemlos möglich. Rechte zum Erstellen von virtuellen Maschinen lassen sich delegieren. Auf diesem Weg erhalten untergeordnete Administratoren die Möglichkeit, virtuelle Computer zu erstellen oder deren Einstellungen zu ändern. Systemweite Einstellungen von SCVMM sind so vor Änderungen geschützt. Auch die intelligente Platzierung von virtuellen Servern auf physische Hosts übernimmt SCVMM, ohne dass Administratoren jedes Mal manuell eingreifen müssen. Für virtuelle Computer lassen sich auch Vorlagen erstellen, sodass Sie identische Einstellungen nicht immer wieder für jeden Computer vornehmen müssen. SCVMM liefert eine optimale Infrastruktur sowohl für Großunternehmen mit hunderten physischen Hosts und tausenden virtuellen Servern als auch für kleine und mittelständische Unternehmen.

System Center Virtual Machine Manager ist äußerst vielseitig: Neben der Möglichkeit, virtuelle Computer zu verwalten, die auf Virtual Server 2005 oder Windows Server 2008 Hyper-V basieren, unterstützt die neue Version jetzt auch VMware-Virtualisierungsumgebungen. Für Unternehmen ist dabei oft die Unterstützung von VMware ESX mit dem (Virtual Center ist Voraussetzung und muss vorhanden sein) und VMware Virtual Infrastructure 3 (VI3) am wichtigsten. Dadurch erhalten Unternehmen eine wirklich zentrale Verwaltungsplattform für alle virtuellen Computer. In einer einzelnen Konsole verwaltet SCVMM nicht nur die physischen Hosts der virtuellen Umgebung, sondern auch alle darin enthaltenen virtuellen Computer. Dabei sind SCVMM kaum Grenzen gesetzt. Neben hunderten physischen Hosts verwalten Sie tausende virtuelle Computer mit SCVMM. Durch diese Zentralisierung ist auch eine Verschiebung von virtuellen Computern zwischen den verschiedenen Systemen problemlos möglich. Dazu verwendet System Center Virtual Machine Manager 2008 VMware Motion, um virtuelle Computer zu VMware ESX- oder VI3-Systemen zu portieren, oder Microsoft Quick Migration für die Migration zu Hyper-V.

Auch die Migration von physischen zu virtuellen Servern (P2V) ist mit SCVMM möglich. Hier verwendet SCVMM eine sehr schnelle blockbasierte Übertragung und unterstützt auch den Schattenkopiedienst von Windows Server 2003/2008. Durch die vollständige Kompatibilität zu Hyper-V und Windows Server 2008 unterstützt der System Center Virtual Machine Manager auch 64-Bit-Betriebssysteme als Host und Gast und ist vollkommen Failoverclustering-fähig. Dies bedeutet, physische Hosts für virtuelle Computer lassen sich in einem Cluster betreiben. Fällt ein physischer Host aus, sind die virtuellen Server auf dem Host sehr schnell wieder verfügbar. Dadurch erstellen Sie hochverfügbare virtuelle Infrastrukturen, die eine optimale Ausfallsicherheit bieten. Die beste Grundlage dafür stellt Windows Server 2008 dar. Hier erkennt SCVMM automatisch ausgefallene oder neu hinzugefügte Clusterknoten und handelt entsprechend. Zusätzlich unterstützt SCVMM auch VMware Host-Cluster, bei denen die Clusterknoten unter VMware ESX-Server laufen. Außerdem unterstützt SCVMM jetzt vollständig die Windows PowerShell, die sowohl für Windows Server 2008 als auch für Windows Server 2003 zur Verfügung steht.

Für die PowerShell gibt es beispielsweise Skripts, mit denen Sie zahlreiche Aufgaben automatisieren und zwar unabhängig von der virtuellen Plattform.

Die Administrationskonsole von SCVMM basiert auf Windows PowerShell-Objekten, daher sind alle damit durchgeführten Aktionen mit der Windows PowerShell möglich. Ein weiterer Vorteil des System Center Virtual Machine Managers 2008 ist die Integration in andere System Center-Produkte. Der Betrieb dieser Lösungen ist keine Voraussetzung, jedoch steigert sich der Nutzen des SCVMM vor allem durch den Einsatz von System Center Operations Manager (SCOM) 2007 erheblich. Mit beiden gemeinsam überwachen Sie virtuelle Computer optimal. Mit der neuen Funktion Performance and Resource Optimation (PRO) hinterlegen Sie Richtlinien und Regeln, bei denen SCVMM Daten aus System Center Operations Manager 2007 verwendet, um die Verfügbarkeit und Leistung der virtuellen Computer zu verbessern und die Hardware der physischen Hosts besser auszunutzen. So kann SCVMM zum Beispiel virtuelle Computer automatisch auf andere physische Hosts mit weniger Last verschieben. Auch neue virtuelle Computer lassen sich so bereitstellen, wenn bereits vorhandene überlastet sind. Doch zurück zum System Center Virtual Machine Manager. Nicht jeder Administrator braucht für jeden virtuellen Computer vollständige administrative Rechte. Das stellen Sie jetzt in SCVMM ein. Durch das neue Rechtemodell erhalten übergeordnete Administratoren die Möglichkeit, einzelne Aufgaben oder die Verwaltung einzelner virtueller Computer an andere Administratoren zu delegieren.

Für große Unternehmen stellt Microsoft System Center Virtual Machine Manager 2008 als Teil von Server Management Suite Enterprise (SMSE) zur Verfügung. Diese enthält, neben SCVMM, noch System Center Operations Manager (SCOM) 2007 und System Center Configuration Manager (SCCM) 2007. SMSE enthält außerdem noch die Datensicherungslösung Data Protection Manager (DPM) 2007. Für mittelständische Unternehmen bietet Microsoft eine Workgroup Edition von SCVMM. Mit ihr verwalten Sie bis zu fünf physische Hosts. Der System Center Virtual Machine Manager besteht aus mehreren Komponenten. Wichtigster Teil dabei ist der Virtual Machine Manager (VMM)-Server. Dabei handelt es sich um den Kernprozess, der für die Kommunikation mit den einzelnen Hosts zuständig ist. Der Server muss auf einem Computer mit 64-Bit-Prozessor und Windows Server 2008 betrieben werden. Seine Daten speichert er in einer SQL Server-Datenbank.

Sie verwalten den VMM-Server mit der Administratorkonsole. Diese stellt die grafische Oberfläche für den VMM-Server zur Verfügung und unterstützt die PowerShell-CMDlets. Diese CMDlets lassen sich mit der PowerShell aber auch ohne die Konsole verwenden, zum Beispiel für Skripts und zur Automatisierung. Zusätzlich enthält der System Center Virtual Machine Manager ein Webportal. Mit diesem können Administratoren, denen bestimmte Rechte delegiert wurden, selbst neue virtuelle Computer erstellen. Die Systemvoraussetzungen für SCVMM sind ein Server mit 64-Bit-Prozessor, mindestens 2 GB RAM und mindestens 200 GB freiem Festplattenplatz. Setzen Sie im Unternehmen einen Host mit Virtual Server 2005 ein, können Sie diesen auch dann in die SCVMM-Infrastruktur einbinden, wenn Virtual Server noch auf einem x86-System mit 32-Bit-Servern läuft. Allerdings müssen Sie dann sicherstellen, dass SCVMM selbst auf einem Hyper-V-aktivierten Windows Server 2008-System mit 64-Bit-Prozessor läuft. Auch ein DVD-Laufwerk sollte im Server vorhanden sein. Als Betriebssystem für SCVMM müssen Sie Windows Server 2008 inklusive Hyper-V betreiben. Außerdem benötigt SCVMM sowohl .NET Framework 2.0 als auch .NET Framework 3.0. Diese integriert der Installationsassistent des SCVMM automatisch auf dem Server.

Zur Speicherung der Daten verwendet SCVMM Microsoft SQL Server 2005 Express Edition, die ebenfalls in der Installation enthalten ist. In dieser Datenbank speichert der VMM-Server beispielsweise die Leistungs- und Konfigurationsdatei und die Einstellungen der einzelnen virtuellen Computer. Für größere Umgebungen unterstützt SCVMM aber auch die Standard- oder Enterprise-Edition von

Microsoft SQL Server 2005/2008. In diesem Fall müssen Sie SQL Server jedoch auf einem eigenständigen virtuellen Rechner installieren und lizenzieren. Da SCVMM auch Windows-PowerShell unterstützt, müssen Sie diese ebenfalls auf dem Server installieren, das gilt auch für das Microsoft Windows Remote Management (WinRM). Für das Webportal von SCVMM benötigen Sie zudem Internetinformationsdienste (IIS) 7.0, die in Windows Server 2008 enthalten sind.

Für den Einsatz von SCVMM müssen Sie außerdem über Active Directory verfügen. SCVMM verwendet die Authentifizierungsinformationen von Active Directory. Hier genügen auch Umgebungen mit Windows Server 2003. Der SCVMM setzt nicht die Migration der Domänencontroller zu Windows Server 2008 voraus.

Installieren und Verwalten von Hyper-V

Die Installation von Hyper-V nehmen Sie als Serverrolle über den Server-Manager vor. Damit die Rolle im Server-Manager aber zur Verfügung steht, müssen Sie nach der Installation den Server am besten über Windows-Update auf den aktuellsten Stand bringen. Stellen Sie außerdem sicher, dass vor der Installation im BIOS des Servers die Virtualisierungsfunktionen des Prozessors aktiviert sind. Die notwendige Aktualisierung für Windows Server 2008, mit welcher die Hyper-V-Unterstützung in das Betriebssystem integriert wird, finden Sie am schnellsten, wenn Sie in einer Suchmaschine nach dem Artikel *Hyper-V-Update für Windows Server 2008 x64 Edition (KB950050)* suchen. Allerdings sollten Sie nicht nur diese Aktualisierung installieren, sondern am besten alle verfügbaren. Vor allem die beiden Updates *Update für Windows Server 2008 x64 Edition (KB951978)* und *Update für Windows Server 2008 x64 Edition (KB955020)* sind durchaus sinnvoll. Beide beheben Fehler in der Skriptverwaltung der regionalen Einstellungen von Windows Server 2008. Damit Sie Hyper-V über Windows Vista x64 verwalten können, müssen Sie auf der Arbeitsstation noch das Update *Hyper-V-Remoteverwaltungsupdate für Windows Vista für x64-Systeme (KB952627)* installieren. Nachdem Sie alle notwendigen Aktualisierungen installiert haben, steht Hyper-V als Serverrolle im Server-Manager zur Verfügung. Die Installation erfolgt identisch zu anderen Serverrollen in Windows Server 2008. Vor der Installation sollten Sie darüber hinaus die Voraussetzungen überprüfen, die Microsoft auf der Internetseite *http://go.microsoft.com/fwlink/?LinkId=122183* zur Verfügung stellt. Für Hyper-V gibt es auch verschiedene Sprachpakete. Mehr Informationen dazu finden Sie auf der Seite *http://go.microsoft.com/fwlink/?LinkID=123536*.

Zusammenfassung der Voraussetzungen für den Einsatz von Hyper-V

Im folgenden Abschnitt gehen wir in Stichpunkten auf die einzelnen Voraussetzungen ein, die erfüllt sein müssen, um Hyper-V einzusetzen:

- Server mit x64-Prozessor und entsprechender 64-Bit-Ausstattung. AMD-Prozessoren tragen die Bezeichnung AMD Virtualization (AMD-V), Intel-Prozessoren die Bezeichnung Intel Virtualization Technology (Intel VT).
- Der Prozessor muss Data Execution Prevention (DEP) unterstützen. Diese muss im BIOS auch aktiviert sein. Die Bezeichnung dafür ist Intel XD bit (Execute Disable Bit) oder AMD NX bit (No Execute Bit).

- Der Host muss über so viel physischen Arbeitsspeicher verfügen, wie Sie insgesamt den virtuellen Computern zuweisen. Die maximale Größe ist an das Betriebssystem gebunden. Für Hyper-V gelten daher nur die Einschränkungen des Betriebssystems. Windows Server 2008 Enterprise Edition unterstützt bis zu 1 Terabyte (TB) Arbeitsspeicher. Virtuellen Computern können Sie bis zu 64 GB zuweisen. Windows Server 2008 Standard Edition unterstützt bis zu 32 GB Arbeitsspeicher.
- Hyper-V unterstützt bis zu 16 logische Prozessoren pro Host. Setzen Sie zum Beispiel vier Dual-Core-Prozessoren auf dem Server ein, entspricht dies acht logischen Prozessoren.
- Jeder virtuelle Computer kann bis zu acht herkömmliche und weitere vier Legacy-Netzwerkadapter verwalten. Die Netzwerkadapter unterstützen VLANs (virtuelle lokale Netzwerke). Hyper-V unterstützt allerdings keine drahtlosen Netzwerkkarten (WLAN) für die Gastbetriebssysteme.
- Windows Server 2008 x64 Standard Edition, Enterprise Edition oder Datacenter Edition muss als Betriebssystem eingesetzt werden.
- Die maximale Festplattengröße für virtuelle Festplatten beträgt 2.040 GB. Jeder virtuelle Computer kann mehrere Festplatten mit einer Gesamtgröße von bis zu 512 TB verwalten.
- Jeder virtuelle Computer unterstützt bis zu vier IDE-Controller und vier SCSI-Controller. Jeder SCSI-Controller unterstützt bis zu 64 Festplatten. Die virtuelle Festplatte, von der das Betriebssystem startet, muss an einen virtuellen IDE-Controller angeschlossen sein.
- Sie können bis zu drei DVD-Laufwerke mit einem virtuellen Computer verbinden.
- Virtuelle Computer können nicht auf den physischen COM-Port des Hosts zugreifen. Auch der Zugriff auf das physische Diskettenlaufwerk des Hosts ist nicht möglich.
- Auf jedem Host können maximal 128 virtuelle Computer gleichzeitig gestartet sein.

Unterstützte Gastbetriebssysteme

Hyper-V unterstützt 32-Bit- und 64-Bit-Gastbetriebssysteme und kann einen, zwei oder vier virtuelle Prozessoren zuordnen, wenn auf dem Gast Windows Server 2008 installiert ist. Für Windows Server 2003 (R2) unterstützt Hyper-V einen oder zwei Prozessoren. Virtuellen Windows 2000-Servern können Sie jeweils nur einen Prozessor zuordnen.

Folgende Betriebssysteme unterstützt Hyper-V mit einem, zwei oder vier virtuellen Prozessor(en):

- Windows Server 2008 Standard und Windows Server 2008 Standard ohne Hyper-V
- Windows Server 2008 Enterprise und Windows Server 2008 Enterprise ohne Hyper-V
- Windows Server 2008 Datacenter und Windows Server 2008 Datacenter ohne Hyper-V
- Windows Web Server 2008
- Windows Server 2008 HPC Edition

Folgende Betriebssysteme unterstützt Hyper-V mit einem oder zwei virtuellen Prozessor(en):

- Windows Server 2003 R2 Standard Edition mit Service Pack 2
- Windows Server 2003 R2 Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Datacenter Edition mit Service Pack 2
- Windows Server 2003 Standard Edition mit Service Pack 2
- Windows Server 2003 Enterprise Edition mit Service Pack 2
- Windows Server 2003 Datacenter Edition mit Service Pack 2
- Windows Server 2003 Web Edition mit Service Pack 2
- Windows Server 2003 R2 Standard x64 Edition mit Service Pack 2
- Windows Server 2003 R2 Enterprise x64 Edition mit Service Pack 2
- Windows Server 2003 R2 Datacenter x64 Edition mit Service Pack 2
- Windows Server 2003 Standard x64 Edition mit Service Pack 2
- Windows Server 2003 Enterprise x64 Edition mit Service Pack 2
- Windows Server 2003 Datacenter x64 Edition mit Service Pack 2

Folgende Betriebssysteme unterstützt Hyper-V mit einem virtuellen Prozessor:

- Windows 2000 Server mit Service Pack 4
- Windows 2000 Advanced Server mit Service Pack 4
- Suse Linux Enterprise Server 10 mit Service Pack 2 (x86-Edition)
- Suse Linux Enterprise Server 10 mit Service Pack 2 (x64-Edition)
- Suse Linux Enterprise Server 10 mit Service Pack 1 (x86-Edition)
- Suse Linux Enterprise Server 10 mit Service Pack 1 (x64-Edition)

Folgende Versionen von Windows Vista in den Editionen x86 und x64 unterstützt Hyper-V mit einem oder zwei virtuellen Prozessor(en):

- Windows Vista Business mit Service Pack 1
- Windows Vista Enterprise mit Service Pack 1
- Windows Vista Ultimate mit Service Pack 1

Folgende Versionen von Windows XP unterstützt Hyper-V:

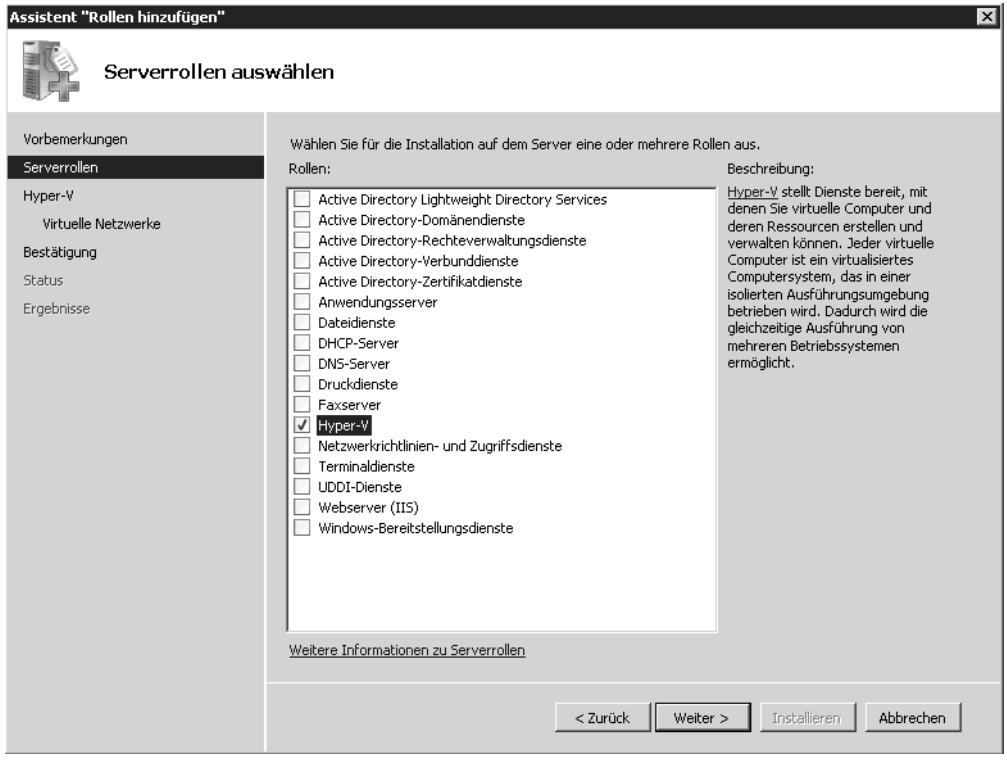
- Windows XP Professional mit Service Pack 3 (ein oder zwei virtuelle Prozessoren)
- Windows XP Professional mit Service Pack 2 (ein Prozessor)
- Windows XP Professional x64 Edition mit Service Pack 2 (ein oder zwei virtuelle Prozessoren)

Installieren von Hyper-V

Für die Installation von Hyper-V verwenden Sie den Server-Manager und fügen Hyper-V wie andere Rollen auch als Serverrolle hinzu. Auf herkömmlichen Servern startet der Assistent zum Hinzufügen von neuen Serverrollen.

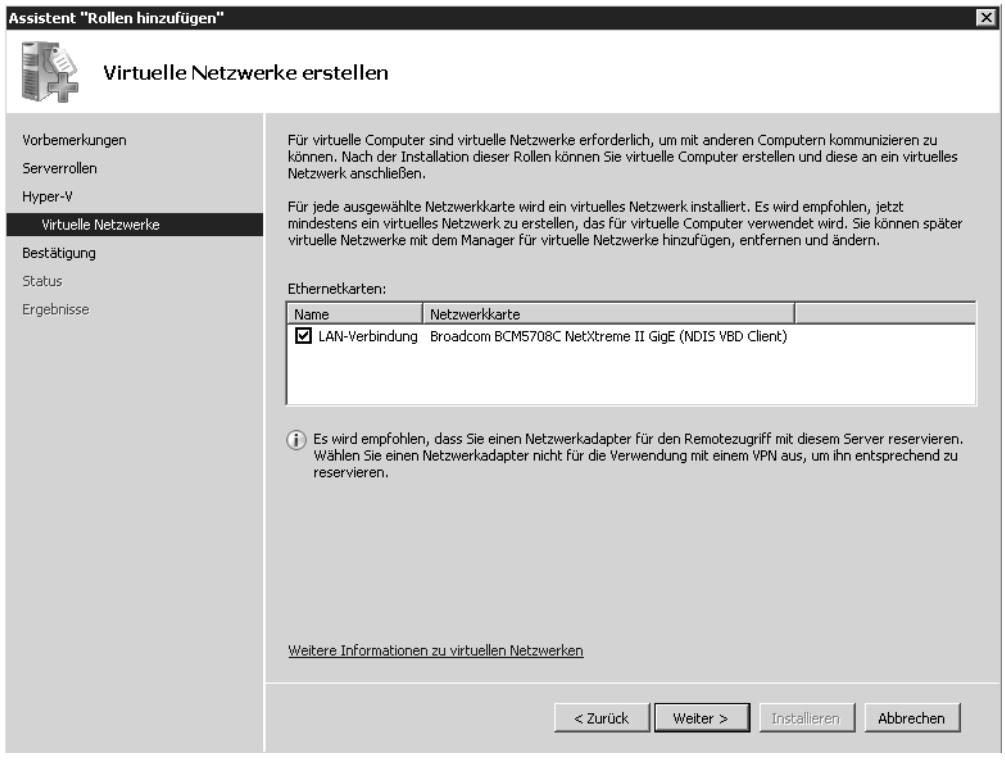
TIPP Um Hyper-V auf einem Core-Server zu installieren, verwenden Sie den Befehl *Start /w ocsetup Microsoft-Hyper-V*. Um Hyper-V remote über das Netzwerk zu verwalten, benötigen Sie einen Computer mit Windows Server 2008 oder Windows Vista SP1 sowie die Remoteverwaltungstools für Hyper-V. Sie können diese Tools von der Webseite *http://support.microsoft.com/kb/950050* herunterladen. Damit Sie auf einem Core-Server Hyper-V installieren können, müssen Sie sicherstellen, dass die Aktualisierung von Hyper-V auf dem Server installiert ist. Geben Sie dazu in der Befehlszeile den Befehl *wmic qfe list* ein. Hier muss das Update mit der Bezeichnung *kbid=950050* installiert sein. Ist das Update nicht vorhanden, laden Sie es herunter und kopieren Sie es auf den Server. Installiert Sie das Update mit dem Befehl *wusa.exe Windows6.0-KB950050-x64.msu /quiet*. Wollen Sie Hyper-V unter Server Core installieren, beachten Sie bitte unbedingt die Hinweise in den Kapiteln 3 und 4.

Abbildg. 25.1 Hyper-V lässt sich als Serverrolle installieren



Auf der nächsten Seite wählen Sie aus, welche Netzwerkkarten Hyper-V in den virtuellen Computern zur Verfügung stellen kann. Generell wird empfohlen, eine weitere Netzwerkkarte im System zu integrieren, welche ausschließlich der Verwaltung dient.

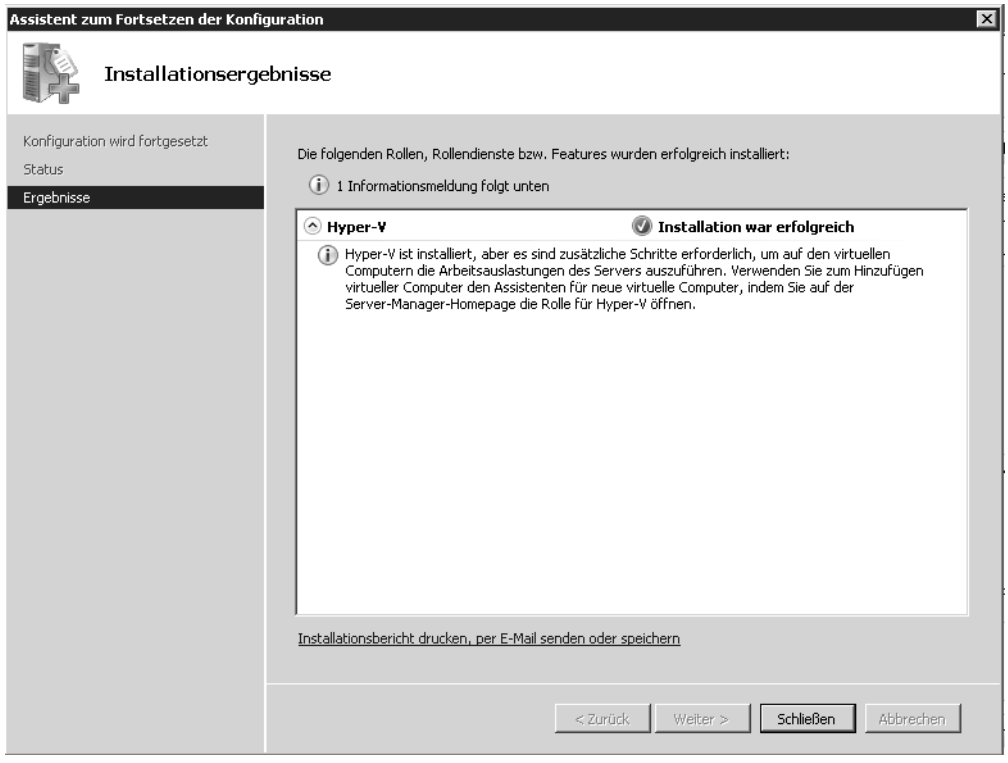
Abbildg. 25.2 Während der Installation wählen Sie aus, welche Netzwerkkarten Hyper-V nutzen darf



Nachdem Sie die Netzwerkkarten ausgewählt haben, welche die virtuellen Computer nutzen dürfen, bestätigen Sie auf der nächsten Seite die Installation von Hyper-V.

Nach der erfolgreichen Installation müssen Sie den Server neu starten. Melden Sie sich nach dem Neustart mit dem gleichen Benutzerkonto an, mit dem Sie auch die Installation durchgeführt haben. Nach der Anmeldung führt der Assistent weitere Aufgaben durch und schließt die Installation ab. Hyper-V ist jetzt erfolgreich auf dem Server installiert.

Abbildg. 25.3 Der Installationsassistent meldet die erfolgreiche Installation von Hyper-V



Erstellen und Verwalten von virtuellen Computern

Nach der Installation finden Sie im Server-Manager über *Rollen/Hyper-V* den *Hyper-V-Manager*, mit dem Sie virtuelle Computer erstellen und verwalten. In der Mitte der Konsole sehen Sie nach der Erstellung die verschiedenen virtuellen Computer. Auf der rechten Seite stehen die verschiedenen Befehle zur Verwaltung der virtuellen Computer zur Verfügung. Nach der Installation ist die Konsole jedoch noch leer, da keine virtuellen Computer vorhanden sind. Über den Link *Neu* erstellen Sie einen neuen virtuellen Computer. Anschließend können Sie das Betriebssystem auf dem neuen Server entweder mit einer CD/DVD oder über eine ISO-Datei installieren, die als CD/DVD-Laufwerk mit dem Computer verknüpft wird.

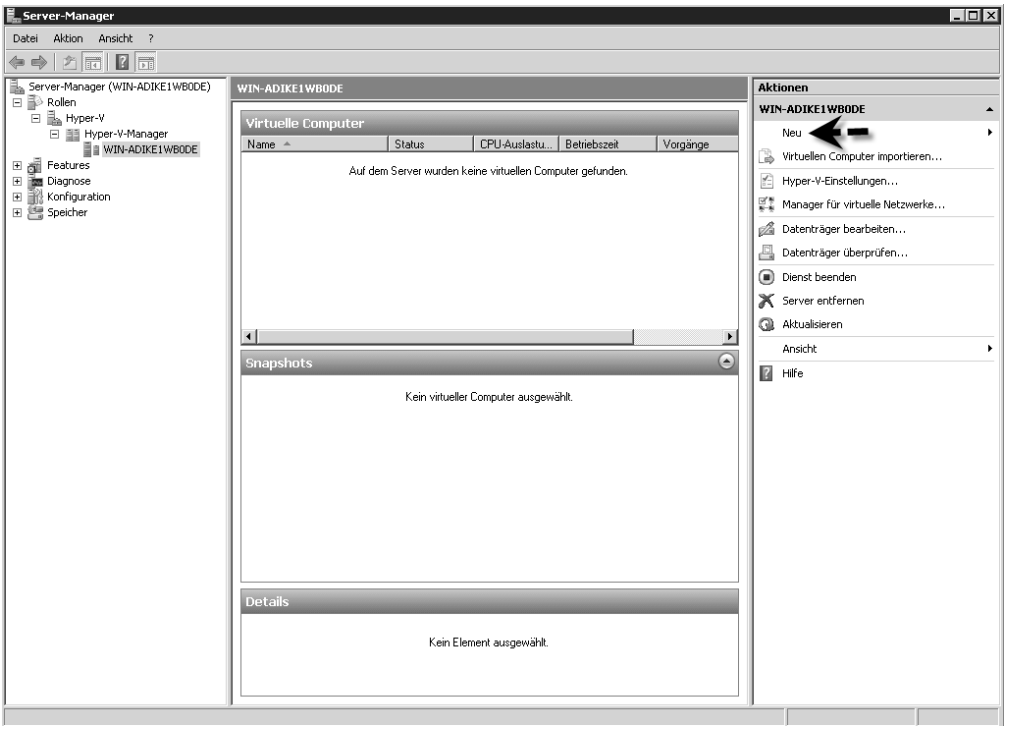
TIPP Hyper-V lässt sich auch von den 32-Bit-Editionen von Windows Server 2008 und von Windows Vista aus verwalten. Microsoft stellt dazu Verwaltungstools zum Download zur Verfügung. Sie finden die aktuellste Version dieser Tools auf den folgenden Internetseiten:

- 64-Bit-Editionen von Windows Vista mit SP1 – *http://go.microsoft.com/fwlink/?LinkId=123540*
- 32-Bit-Editionen von Windows Vista mit SP1 – *http://go.microsoft.com/fwlink/?LinkId=123541*
- 32-Bit-Editionen Windows Server 2008 – *http://go.microsoft.com/fwlink/?LinkId=123542*

Erstellen eines virtuellen Computers

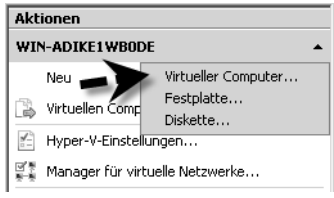
Im nächsten Abschnitt zeigen wir Ihnen zunächst, wie Sie einen neuen virtuellen Computer mit dem Hyper-V-Manager erstellen und Arbeitsspeicher, Netzwerkverbindung und virtuelle Festplatten konfigurieren. Nach der Erstellung des virtuellen Computers gehen wir ausführlicher auf die Installation und Verwaltung von neuen virtuellen Computern ein.

Abbildg. 25.4 Erstellen eines neuen virtuellen Computers im Hyper-V-Manager



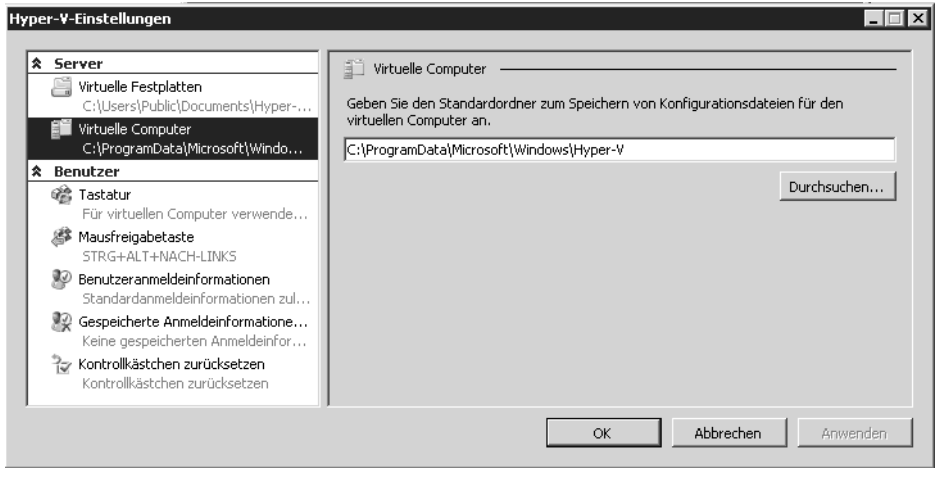
Nachdem Sie auf *Neu* geklickt haben, erstellen Sie mit dem Link *Virtueller Computer* einen neuen virtuellen Computer.

Abbildg. 25.5 Erstellen eines neuen virtuellen Computers



Anschließend startet ein Assistent, der Sie durch die Erstellung des neuen Computers führt. Auf der Startseite geben Sie noch keine wichtigen Daten ein. Hier erhalten Sie lediglich eine Einführung zum Assistenten. Auf der zweiten Seite geben Sie den Namen des Computers ein, so wie er in der Verwaltungskonsole angezeigt werden soll. Der Name hat nichts mit dem eigentlichen Computernamen zu tun. Hierbei handelt es sich lediglich um den Namen in der Konsole. Als Vorgabe speichert der Assistent die Daten des Computers im Standardverzeichnis von Hyper-V. Sie können dieses Verzeichnis im Hyper-V-Manager über den Link *Hyper-V-Einstellungen* festlegen. Hier nehmen Sie darüber hinaus weitere Einstellungen vor, die für Hyper-V selbst und alle virtuellen Computer gemeinsam gelten.

Abbildg. 25.6 In den *Hyper-V-Einstellungen* lassen sich zentrale Eingaben vornehmen, die für alle Computer gelten

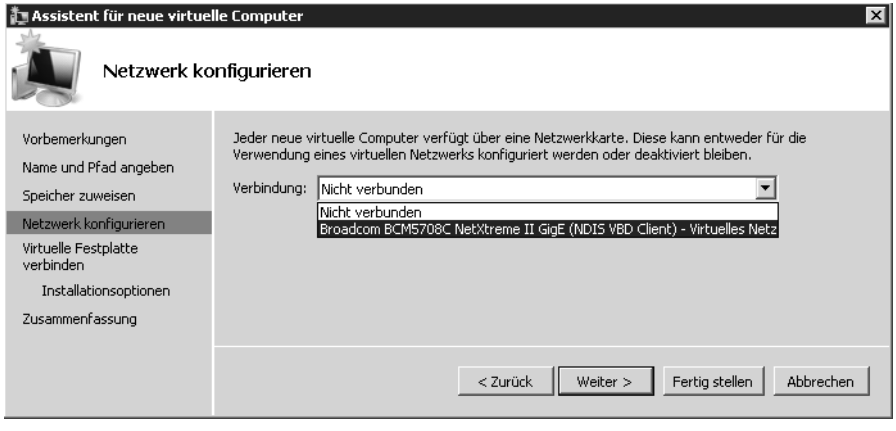


Einzelne virtuelle Computer müssen nicht unbedingt das Standardverzeichnis verwenden. Auf der nächsten Seite des Assistenten legen Sie fest, wie viel Arbeitsspeicher Hyper-V dem neuen virtuellen Computer zur Verfügung stellen soll. Generell sollten Sie darauf achten, dass der gemeinsame Arbeitsspeicher aller virtueller Computer nicht den physischen Speicher des Hosts überschreiten sollte. Natürlich lässt sich der Arbeitsspeicher des virtuellen Computers auch nach der Installation jederzeit anpassen.

Abbildg. 25.7 Festlegen des Arbeitsspeichers des neuen virtuellen Computers

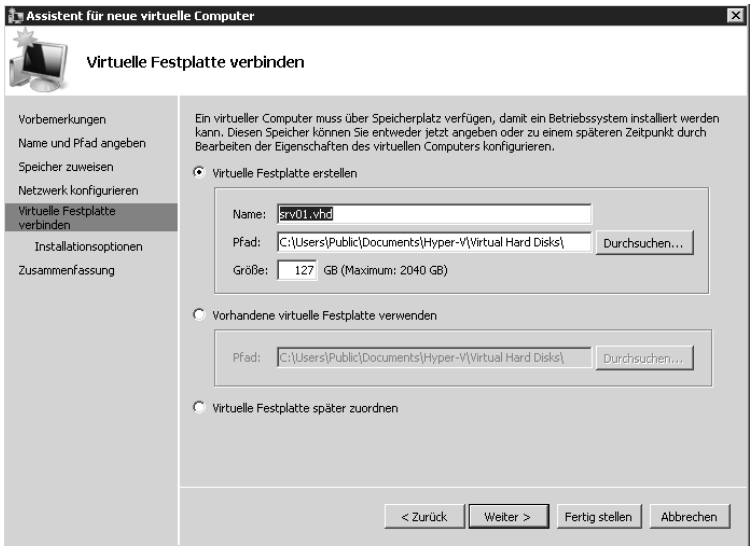
Als Nächstes legen Sie fest, ob der Computer mit dem Netzwerk verbunden sein soll und welche Netzwerkkarte dazu zur Verfügung steht. Standardmäßig ist bereits nach der Installation von Hyper-V ein virtuelles Netzwerk verfügbar. Diese virtuelle Netzwerkkarte verwendet die physische Netzwerkkarte des Servers zur Kommunikation mit dem Netzwerk. Sie verwalten virtuelle Netzwerke im Hyper-V-Manager über den Link *Manager für virtuelle Netzwerke*.

Abbildg. 25.8 Auswählen der Netzwerkverbindung für den virtuellen Computer



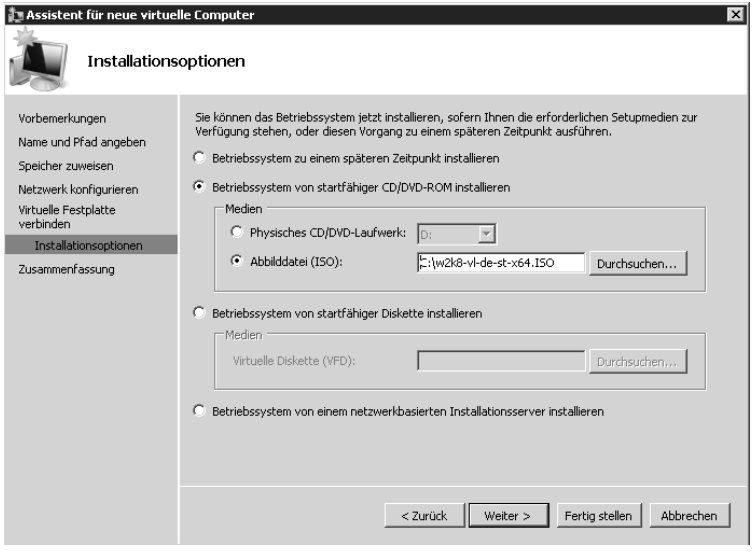
Auf der nächsten Seite legen Sie fest, ob Sie für den neuen virtuellen Computer auch eine neue virtuelle Festplatte erstellen wollen oder ob der Server eine bereits vorhandene nutzen soll. Auch der Speicherort sowie die maximale Größe dieser Festplatte lässt sich an dieser Stelle festlegen.

Abbildg. 25.9 Festlegen der virtuellen Festplatte des neuen virtuellen Computers



Im Anschluss legen Sie fest, wie Sie das Betriebssystem auf dem Computer installieren wollen. Sie können entweder einen herkömmlichen Datenträger in das CD/DVD-Laufwerk des Hosts einlegen, eine ISO-Datei als Laufwerk verknüpfen oder das Betriebssystem mit den Windows-Bereitstellungsdiensten installieren. Für virtuelle Computer bieten sich ISO-Dateien an, da so die Installation wesentlich schneller abläuft.

Abbildg. 25.10 Auswählen der Installationsart des Betriebssystems

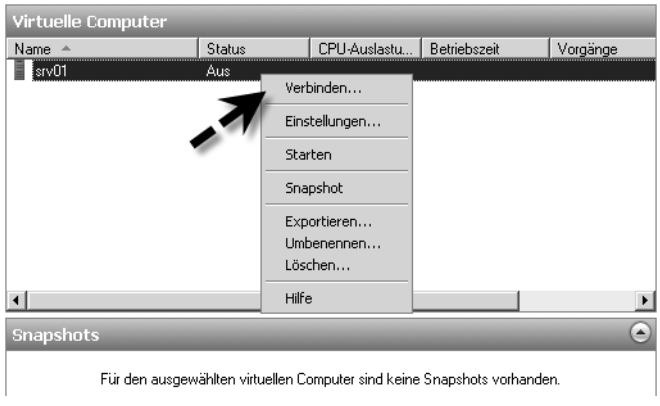


Auf der letzen Seite erhalten Sie noch eine Zusammenfassung über Ihre Eingaben und der Assistent erstellt den virtuellen Server nach Ihren Vorgaben.

Virtuelle Computer verwalten und Betriebssysteme installieren

Nach der Erstellung eines virtuellen Computers besteht der nächste Schritt darin, das Betriebssystem sowie die *Integrationsdienste*, welche den virtuellen Server für den Betrieb optimieren und beschleunigen, zu installieren. Nach der Erstellung eines oder mehrerer virtueller Computer werden diese im Hyper-V-Manager in der Mitte der Konsole angezeigt. Standardmäßig sind diese virtuellen Computer nach der Erstellung noch ausgeschaltet. Um das Betriebssystem zu installieren, klicken Sie in der Mitte der Konsole auf den Computereintrag und wählen entweder aus dem Kontextmenü oder der Aktionsleiste den Befehl *Verbinden* aus.

Abbildg. 25.11 Verbinden mit dem neuen virtuellen Computer

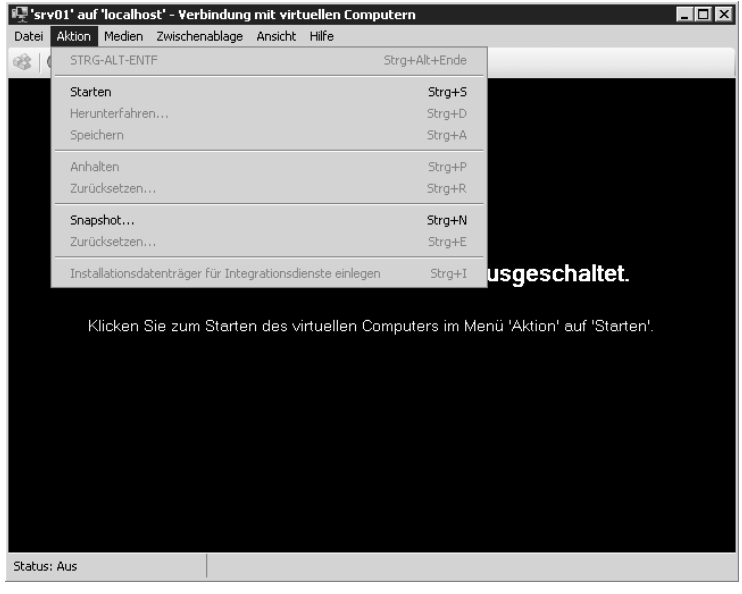


Anschließend öffnet sich ein neues Fenster, mit dem Sie den virtuellen Computer steuern. Durch das Verbinden bleibt der Computer aber ausgeschaltet. Um diesen einzuschalten, verwenden Sie entweder den Befehl *Starten* aus dem Menü *Aktion* oder die Schaltfläche zum Start des Servers. Nach dem Start verbindet sich der virtuelle Computer gleich mit der Installations-DVD des Betriebssystems und startet das Setup. Führen Sie die Installation auf gleichem Weg durch wie auf einem herkömmlichen Server. Haben Sie im BIOS die Virtualisierungsfunktion des Prozessors nicht aktiviert, erhalten Sie unter Umständen eine Fehlermeldung, dass Hyper-V nicht starten kann. Fahren Sie in diesem Fall den Host herunter und überprüfen Sie im BIOS, ob diese Funktion auch aktiviert ist. Nach erfolgreicher Aktivierung lässt sich der virtuelle Computer starten und die Installation beginnt. Sie müssen übrigens während der Installation das Fenster des virtuellen Computers nicht geöffnet lassen. Schließen Sie das Verwaltungsfenster des virtuellen Servers, bleibt dieser gestartet und führt die Installation fort. Sie sehen dann im Hyper-V-Manager den aktuellen CPU-Verbrauch des Servers.

Abbildg. 25.12 Ist die Virtualisierungsfunktion des Prozessors im BIOS nicht aktiviert, erscheint beim Starten eines virtuellen Computers eine Fehlermeldung

Klicken Sie auf den Server, sehen Sie im unteren Bereich des Hyper-V-Managers den aktuellen Bildschirm. Per Doppelklick oder durch Auswählen des Kontextmenübefehls *Verbinden* startet wieder das Fenster des Servers. Führen Sie die Installation des Betriebssystems über eine Remotedesktopverbindung durch, steht die Maus im Fenster des virtuellen Computers während der Installation noch nicht zur Verfügung. Sie können in diesem Fall die Installation aber problemlos über Tastatureingaben durchführen.

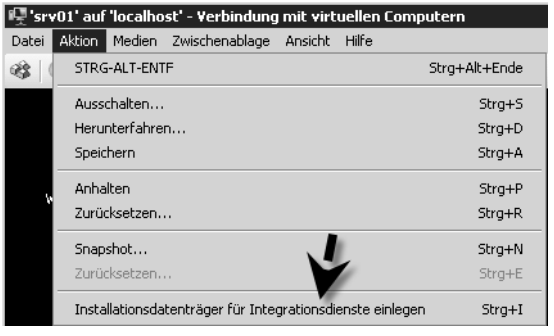
Abbildg. 25.13 Nach dem Verbindungsaufbau müssen Sie den virtuellen Computer erst starten



Installieren der Integrationsdienste

Nach der Installation des Betriebssystems müssen Sie auf dem virtuellen Computer noch die Integrationsdienste installieren. Deren Aufgaben haben wir bereits in der Einleitung zu diesem Kapitel besprochen. Diese Dienste entsprechen den VMware-Tools oder den Add-Ons von Virtual PC und beschleunigen jeden virtuellen Computer, den Sie unter Hyper-V installieren. Erst durch die Installation dieser Integrationsdienste ist der virtuelle Computer einsatzbereit. Sie installieren die Dienste, indem Sie nach der Installation des Betriebssystems den Befehl *Installationsdatenträger für Integrationsdienste einlegen* im Menü *Aktion* auswählen. Vorher müssen Sie sich noch mit einem Administratorkonto am Computer anmelden. Normalerweise startet der Installationsassistent automatisch. Ist das bei Ihnen nicht der Fall, können Sie die Installation auch manuell starten. Der Assistent verbindet den Installationsdatenträger der Integrationsdienste als herkömmliches CD/DVD-Laufwerk, welches im Explorer des virtuellen Computers zur Verfügung steht. Nach der Installation der Integrationsdienste steht der virtuelle Computer zur produktiven Nutzung zur Verfügung.

Abbildg. 25.14 Nach der Installation des Betriebssystems erfolgt die Installation der Integrationsdienste



Im Fernwartungsfenster des virtuellen Computers stehen neben der Möglichkeit, den Computer herunterzufahren, noch zwei weitere interessante Punkte zur Verfügung:

- **Anhalten** Einer laufenden VM werden sämtliche CPU-Ressourcen entzogen, sie friert im aktuellen Zustand ein. Der RAM-Inhalt, und damit der aktuelle Zustand der Maschine, bleibt erhalten und die VM läuft nach dem Fortsetzen sofort weiter.
- **Zustand speichern** Mit dieser Option wird der RAM-Inhalt in einer Datei auf dem Host abgespeichert und der Gast dann abgeschaltet. Beim späteren Starten wird dieser Status aus der Datei wieder in den Arbeitsspeicher geladen und die Maschine steht schnell wieder zur Verfügung.

Abbildg. 25.15 Schaltflächen für virtuelle Computer

Migrieren von Microsoft Virtual Server 2005 zu Hyper-V

Wollen Sie Server zu Hyper-V überführen, ist die Vorgehensweise grundsätzlich sehr einfach:

1. Entfernen Sie die VM-Additions von den virtuellen Servern unter Virtual Server 2005.
2. Kopieren Sie nur die VHD-Datei (Virtual Hard Disk) des Servers, keinerlei andere Dateien, auf den Server mit Hyper-V.
3. Erstellen Sie manuell eine neue virtuelle Maschine und weisen Sie die vorhandene VHD-Datei zu.
4. Handelt es sich beim Server nicht um einen Computer mit Windows Server 2003/2008, entfernen Sie die virtuelle Netzwerkkarte und fügen Sie einen Legacy-Netzwerkadapter über den Assistent zum Hinzufügen von Hardware hinzu.
5. Installieren Sie die Integrationsdienste.

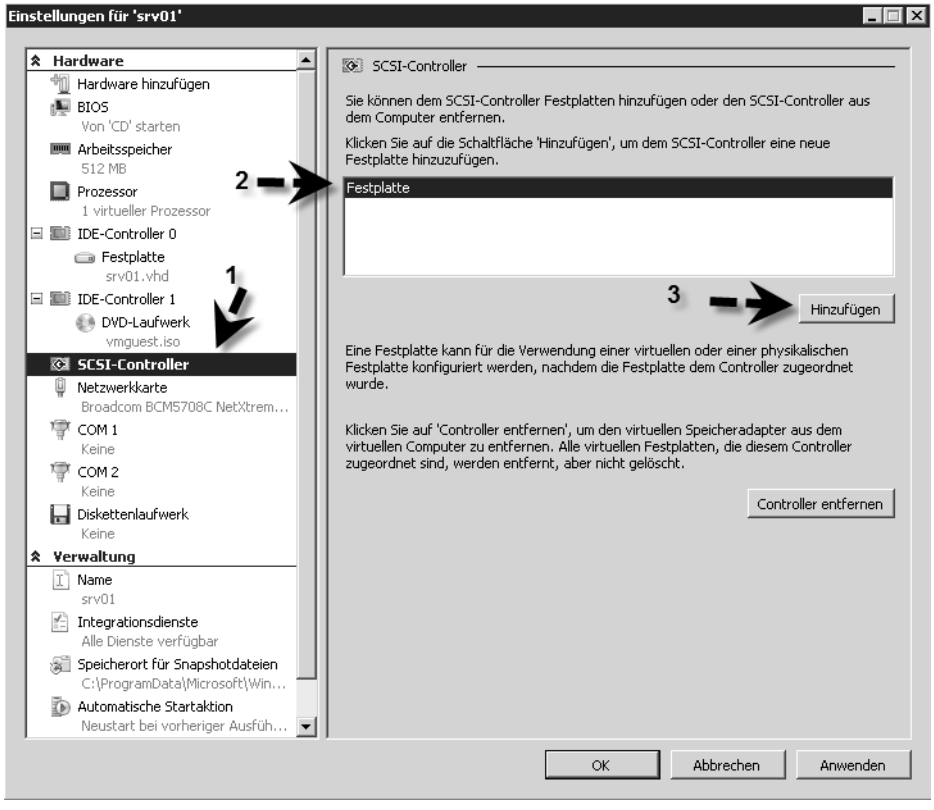
Anpassen der Einstellungen von virtuellen Computern

Über das Kontextmenü oder den Aktionsbereich lassen sich die verschiedenen Einstellungen der virtuellen Computer anpassen. Hierüber passen Sie zum Beispiel die Anzahl der Prozessoren, die Größe des Arbeitsspeichers, BIOS-Einstellungen und die Schnittstellen an. Auch neue Hardware fügen Sie über diesen Bereich hinzu. Im folgenden Abschnitt gehen wir auf die einzelnen Möglichkeiten ein.

Hinzufügen von Hardware zu virtuellen Computern

Wollen Sie einem virtuellen Computer neue Hardware hinzufügen, also z.B. eine neue Netzwerkkarte, einen SCSI-Controller, klicken Sie den virtuellen Computer mit der rechten Maustaste an, wählen *Einstellungen* und klicken dann auf *Hardware hinzufügen*. Im rechten Bereich wählen Sie die entsprechende Hardware aus und klicken auf *Hinzufügen*. Beim Hinzufügen eines Festplattencontrollers besteht zusätzlich noch die Möglichkeit, weitere Festplatten hinzuzufügen. Dazu klicken Sie den Controller im Einstellungsmenü an, wählen *Festplatte* aus und klicken auf *Hinzufügen*. Einmal hinzugefügte Geräte lassen sich übrigens über die Schaltfläche *Entfernen* wieder vom virtuellen Computer trennen. Nachdem Sie einem Controller eine Festplatte hinzugefügt haben, können Sie als Nächstes festlegen, welche SCSI-ID die Platte haben sollen und ob Sie eine neue VHD-Datei oder eine bereits vorhandene verwenden wollen.

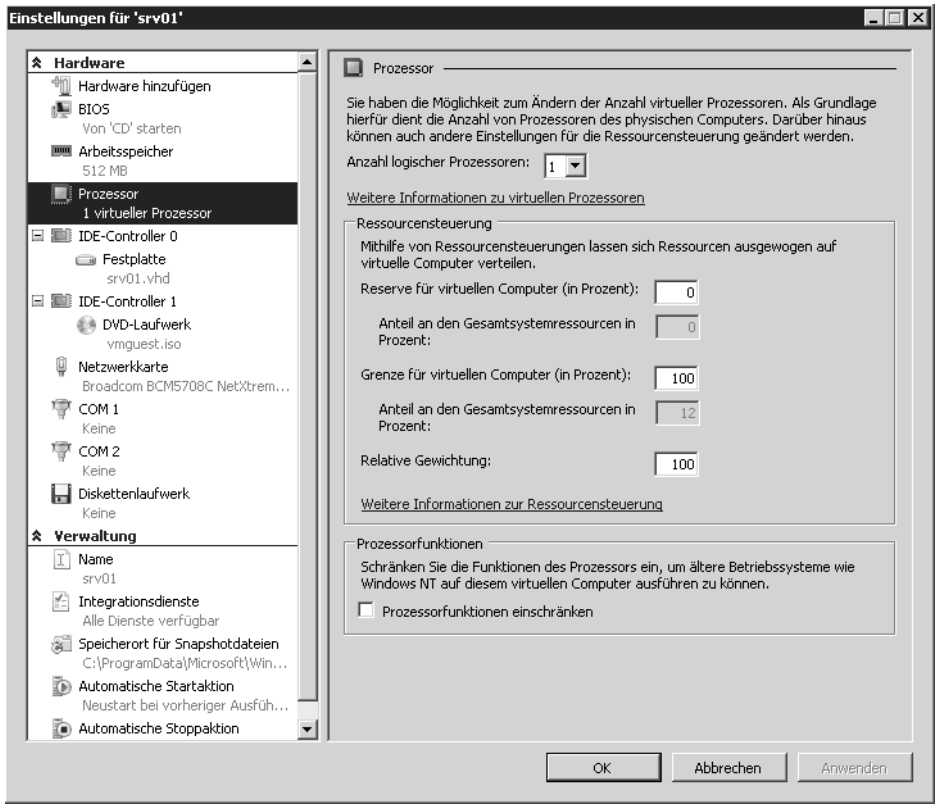
Abbildg. 25.16 Hinzufügen einer neuen Festplatte oder eines neuen SCSI-Controllers



BIOS-Einstellungen, Arbeitsspeicher und Prozessoranzahl von virtuellen Computern anpassen

Ein weiterer Bereich in den Einstellungen von virtuellen Computern sind die BIOS-Einstellungen. Die meisten Einstellungen lassen sich aber nur dann anpassen, wenn der virtuelle Computer ausgeschaltet ist. Hierüber legen Sie fest, ob die Num-Taste beim Starten automatisch aktiviert ist und welche Bootreihenfolge der Server beachten soll. Über den Menübefehl *Arbeitsspeicher* legen Sie die Größe des Arbeitsspeichers für den virtuellen Computer fest. Ausführlichere Möglichkeiten bietet die Prozessorsteuerung von virtuellen Computern. Über den Menübefehl *Prozessor* in den Eigenschaften eines virtuellen Servers stellen Sie die Anzahl der Prozessoren ein sowie eine Gewichtung der Ressourcen, die dem Prozessor zugewiesen sind.

Abbildg. 25.17 Konfigurieren der Prozessoreinstellungen von virtuellen Computern



Neben der eigentlichen Anzahl an physischen Prozessoren, die dem virtuellen Computer zugewiesen sind, steuern Sie hier, wie viel Prozessorzeit diesem virtuellen Computer zur Verfügung steht. Hier stehen mehrere Möglichkeiten zur Verfügung, die Sie über Prozentangaben steuern:

- **Reserve für virtuellen Computer** Hiermit legen Sie fest, welche Ressourcen dem virtuellen Computer mindestens zur Verfügung stehen. Der eigentliche Wert darf niemals unter diesen Wert sinken. Achten Sie aber darauf, dass die reservierte Prozessorzeit sich auch auf andere virtuelle Computer auswirkt und deren maximale Anzahl auf dem Host beschränkt.
- **Grenze für virtuellen Computer** Dieser Wert gibt an, wie viel Prozessorzeit dem virtuellen Computer maximal zur Verfügung steht.
- **Relative Gewichtung** Beim Einsatz mehrerer virtueller Computer auf dem Server, die identische Einstellungen im Ressourcenbereich haben, legt dieser Wert fest, in welcher Relation dieser Computer bevorzugt wird. Wichtige Server lassen sich dadurch bevorzugen und so sicherstellen, dass diese nicht zu wenige Ressourcen zugewiesen bekommen.

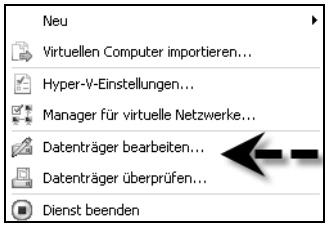
Verwalten allgemeiner Einstellungen von virtuellen Computern

Im unteren Bereich in den Einstellungen von virtuellen Computern legen Sie den Namen fest, den Hyper-V verwendet, sowie die freigeschalteten Funktionen der Integrationsdienste. Haben Sie für einen Computer noch keinen Snapshot erstellt, also eine Sicherung des Betriebssystemzustands zu einem bestimmten Zeitraum, lässt sich an dieser Stelle noch der Speicherort der Dateien des virtuellen Computers anpassen. Nach der Erstellung eines Snapshots ist keine Änderung des Speicherorts mehr möglich. Über den Menübefehl *Automatische Startaktion* legen Sie fest, wie sich der virtuelle Computer bei einem Neustart des Hosts verhalten soll. Der Bereich *Automatische Stoppaktion* dient der Konfiguration des Verhaltens, wenn der Host heruntergefahren wird.

Virtuelle Festplatten verwalten und optimieren

Im Aktionsbereich des Hyper-V-Managers findet Sie auf der linken Seite die beiden Menübefehle *Datenträger bearbeiten* und *Datenträger überprüfen*.

Abbildg. 25.18 Verwalten der Festplatten in Hyper-V

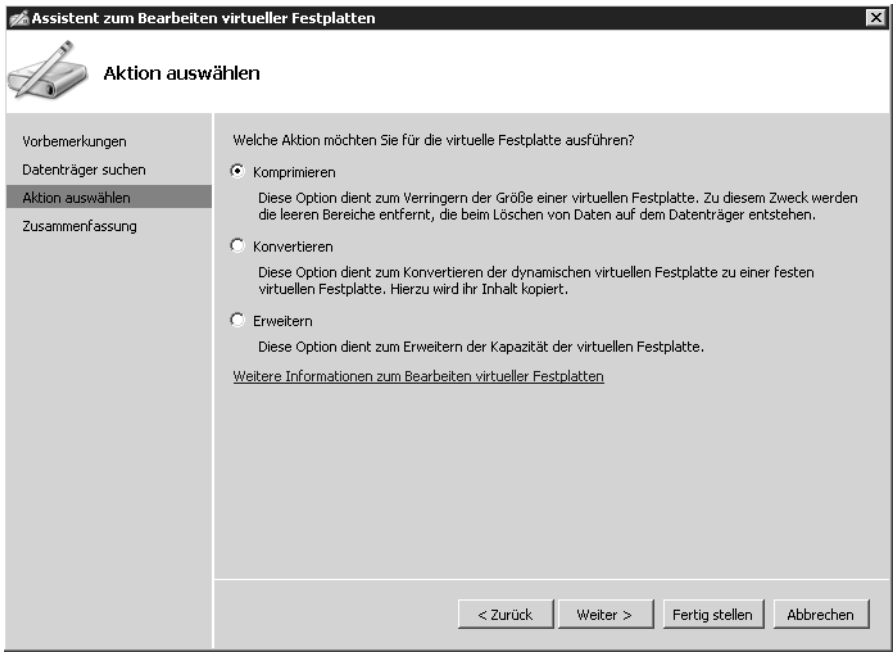


Mit *Datenträger überprüfen* starten Sie einen Scanvorgang einer beliebigen dynamischen Festplatte. Anschließend öffnet sich ein neues Fenster und zeigt die Daten dieser Platte an. So erfahren Sie, ob es sich um eine dynamisch erweiterbare Platte oder um eine Platte mit fester Größe handelt. Auch die maximale Größe sowie die aktuelle Datenmenge zeigt das Fenster an. Über *Datenträger bearbeiten* stehen Ihnen verschiedene Möglichkeiten zum Anpassen der aktuell ausgewählten Festplatte zur Verfügung:

- **Komprimieren** Diese Aktion steht nur bei dynamisch erweiterbaren Festplatten zur Verfügung. Der Vorgang löscht leere Bereiche in der VDH-Datei, sodass diese deutlich verkleinert wird. Allerdings ist dieser Vorgang nur dann sinnvoll, wenn viele Daten von der Festplatte gelöscht wurden.
- **Konvertieren** Mit diesem Vorgang wandeln Sie dynamisch erweiterbare Festplatten in Festplatten mit fester Größe um oder umgekehrt.
- **Erweitern** Dieser Befehl hilft dabei, den maximalen Festplattenplatz einer VHD-Datei zu vergrößern.
- **Zusammenführen** Der Assistent zeigt diesen Befehl nur dann an, wenn Sie eine differenzierende Festplatte auswählen, zum Beispiel die AVHD-Datei eines Snapshots. Da diese Datei nur die Datenmenge enthält, die sich von der Quell-VHD-Datei unterscheidet, lassen sich die Daten zu einer gemeinsamen VHD-Datei zusammenführen, die alle Daten enthält. Die beiden Quellfestplatten bleiben bei diesem Vorgang erhalten, der Assistent erstellt eine neue virtuelle Festplatte.

- **Verbindung wiederherstellen** Für eine differenzierende Festplatte ist es wichtig, dass die Quelldatei, also die VHD-Datei, vorhanden ist. Eine differenzierende Festplatte kann aber auch in einer Kette auf eine andere differenzierende Datei verweisen, die dann wiederum auf die VHD-Datei verweist. Das kommt zum Beispiel dann vor, wenn mehrere Snapshots aufeinander aufbauen. Ist die Kette zerstört, zum Beispiel, weil sich der Pfad einer Platte geändert hat, lässt sich mit diesem Befehl die Verbindung wieder herstellen.

Abbildg. 25.19 Virtuelle Festplatten bearbeiten



Virtuelle Festplatten lassen sich auch ohne dazugehörigen Computer erstellen, indem Sie im Aktionsbereich des Hyper-V-Managers den Befehl *Neu* auswählen. Es startet ein Assistent, über den Sie auswählen können, welche Art von virtueller Festplatte Sie erstellen wollen:

- **Dynamisch erweiterbare virtuelle Festplatte** Dieser Typ wird am häufigsten verwendet. Die hinterlegte Datei der Festplatte kann dynamisch mit dem Inhalt mitwachsen.
- **Virtuelle Festplatte mit fester Größe** Bei dieser Variante wählen Sie eine feste Größe aus, welche die virtuelle Festplatte des virtuellen Servers nicht überschreiten darf.
- **Differenzierende virtuelle Festplatte** Wenn Sie diese Festplatte auswählen, wird auf Basis einer bereits vorhandenen virtuellen Festplatte eine neue Festplatte erstellt. Damit können Sie von bereits vorhandenen virtuellen Festplatten ein Abbild erschaffen. Microsoft empfiehlt, die übergeordnete virtuelle Festplatte mit einem Schreibschutz zu versehen, damit diese nicht versehentlich überschrieben wird. In der Differenzplatte liegen nur die Änderungen, die das Gastsystem an der virtuellen Platte vorgenommen hat. Dazu werden alle Schreibzugriffe des Gastes auf die Differenzplatte umgeleitet. Lesezugriffe kombinieren den Inhalt der Differenzplatte und den Inhalt der

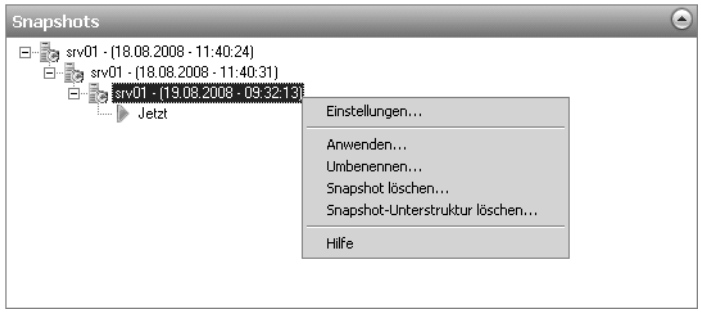
zugrunde liegenden virtuellen Platte, ohne dass der Gast etwas davon bemerkt. Die zugrunde liegende Platte wird nicht mehr verändert und die Differenzplatte bleibt relativ klein, da sie nur Änderungen enthält. Eine fertige Basisinstallation kann von mehreren VMs gleichzeitig verwendet werden, indem Sie mehrere Differenzplatten erstellen, die dieselbe virtuelle Platte verwenden. Dadurch sparen Sie sich viel Zeit und Platz beim Klonen von virtuellen Maschinen.

TIPP VHD-Dateien lassen sich in Hyper-V übrigens auch unter der übergeordneten Partition bereitstellen. Sie finden auf der Internetseite *http://blogs.msdn.com/virtual_pc_guy/archive/2008/02/01/mounting-a-virtual-hard-disk-with-hyper-v.aspx* dazu ein einfaches VBScript sowie Befehle für die PowerShell. Eine weitere Möglichkeit ist, das Tool *oscdimg.exe* aus dem Windows Automated Installation Kit (WAIK) zu verwenden (siehe Kapitel 16). Mit diesem Tool erstellen Sie aus einer VHD-Datei eine ISO-Datei, die sich dann ebenso leicht mounten lässt.

Erstellen und Verwalten von Snapshots von virtuellen Servern

Eine wichtige Funktion in Hyper-V ist die Möglichkeit, von virtuellen Computern einen Snapshot zu erstellen. Dabei fertigt Hyper-V eine Sicherung des aktuellen Zustands des Betriebssystems an, der sich jederzeit wiederherstellen lässt. Solche Snapshots sind zum Beispiel vor der Installation von Patches oder Service Packs sinnvoll. Snapshots erstellen Sie über das Kontextmenü des virtuellen Computers. Die erstellten Snapshots zeigt der Hyper-V-Manager im mittleren Bereich der Konsole an. Auch für die einzelnen Snapshots steht ein Kontextmenü zur Verfügung, über das Sie diese steuern.

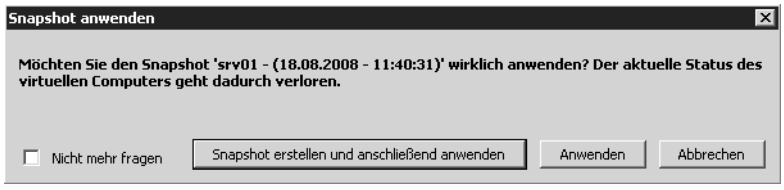
Abbildg. 25.20 Verwalten der Snapshots von virtuellen Servern



Im Kontextmenü von Snapshots stehen verschiedene Möglichkeiten zur Verfügung:

- **Einstellungen** Hierüber rufen Sie die Einstellungen des virtuellen Computers auf, zu dem dieser Snapshot gehört.
- **Anwenden** Wählen Sie diese Option aus, setzt der Assistent den virtuellen Computer wieder auf jenen Stand zurück, zu dem dieser Snapshot erstellt wurde. Vorher erscheint ein Abfragefenster, das Sie auf die Folgen hinweist. Außerdem können Sie vorher noch mal einen aktuellen Snapshot erstellen.

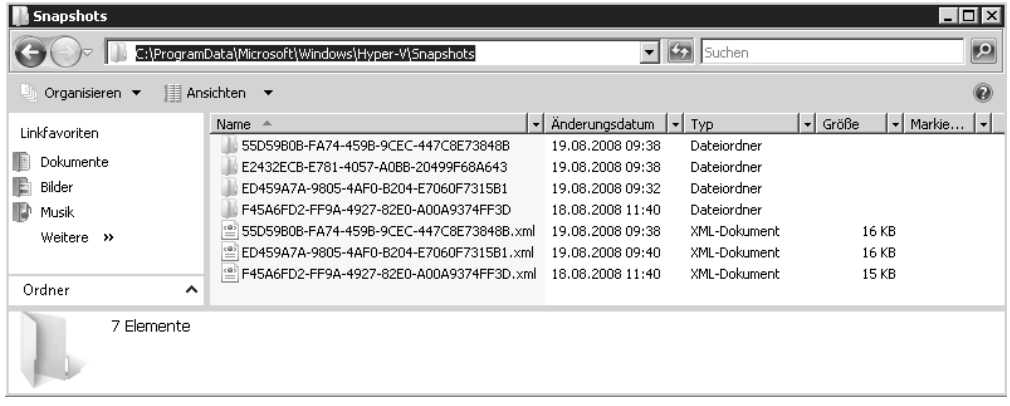
Abbildg. 25.21 Anwenden eines Snapshots



- **Umbenennen** Mit dieser Option geben Sie dem Snapshot einen anderen Namen. Hyper-V verwendet als Namen normalerweise Datum und Uhrzeit. Über diesen Menübefehl können Sie zum Beispiel noch Informationen hinzufügen, warum Sie den Snapshot erstellt haben.
- **Snapshot löschen** Löscht den Snapshot und die dazugehörigen Daten vom Server.
- **Snapshot-Unterstruktur löschen** Diese Option löscht den aktuellen Snapshot sowie alle Sicherungen, die nach dem Snapshot erstellt wurden und auf diesen aufbauen.

Hyper-V speichert die Snapshots übrigens in dem Ordner, den Sie in den Einstellungen des virtuellen Computers im Bereich *Speicherort für Snapshotdateien* angeben. Standardmäßig handelt es sich um den Ordner *C:\ProgramData\Microsoft\Windows\Hyper-V\Snapshots*. Nach der Erstellung eines Snapshots finden Sie in diesem Ordner mehrere Dateien, darunter eine XML-Datei für jeden Snapshot. Wählen Sie den Befehl *Zurücksetzen* im Kontextmenü des virtuellen Computers aus, wendet Hyper-V den letzten erstellten Snapshot aus und setzt den Computer auf diesen Stand zurück.

Abbildg. 25.22 Für jeden Snapshot gibt es einen eigenen Ordner und eine XML-Datei



Vorgang beim Erstellen eines Snapshots

Standardmäßig besteht ein virtueller Computer aus einer VHD-Datei (seiner Festplatte), einer XML-Datei, welche die Einstellungen des Servers enthält, sowie aus den Statusdateien mit den Endungen **.bin* und **.vsv*. Erstellen Sie einen Snapshot, erstellt der Hyper-V-Manager zunächst eine neue virtuelle Platte, welche aber nur die Änderungen enthält, eine so genannte **.avhd*-Datei oder auch *Differencing Disk*. Eine solche Datei zeigt auf eine herkömmliche VHD-Datei, welche die

eigentlichen Daten des Servers enthält. Das Gastsystem schreibt nur Änderungen in diese AVHD-Datei. Zukünftig verweist dann die XML-Steuerdatei des virtuellen Computers auf diese AVHD-Datei, welche die Änderungen seit dem Snapshot enthält. Setzen Sie den Snapshot zurück, benötigt Hyper-V diese nicht mehr und verweist wieder auf die ursprüngliche VHD-Datei.

Beispiel:

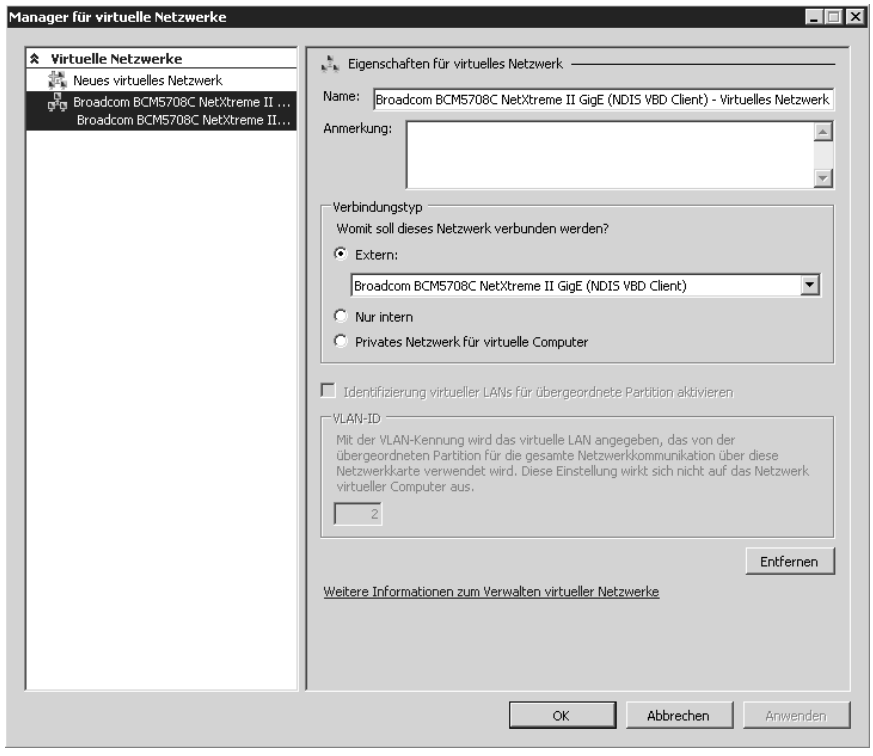
Nehmen wir an, Sie haben drei Snapshots erstellt und wollen den Computer wiederherstellen. Sie wollen auf den Zustand nach dem zweiten Snapshot zurückgehen. Da nach dem zweiten Snapshot noch ein dritter vorhanden ist, müssen Sie zunächst einen weiteren Snapshot erstellen. Machen Sie das nicht, gehen alle Snapshots verloren, die Sie nach dem zweiten Snapshot erstellt haben. Dieser neue Snapshot zeigt auf den ersten Snapshot, den Sie erstellt haben. Als Administrator müssen Sie dazu keine Aktion durchführen, denn diese Aufgabe übernimmt Hyper-V für Sie. Einfach ausgedrückt, erstellt Hyper-V beim Anwenden eines Snapshots zunächst eine Kopie der Dateien des Snapshots und wendet diese Kopien an. Dadurch ist sichergestellt, dass der Computer nach dem Zurücksetzen den gewünschten Zustand hat, aber alle verfügbaren Snapshots auch noch funktionieren.

HINWEIS Sie können für jeden virtuellen Computer maximal 50 Snapshots erstellen.

Verwalten der virtuellen Netzwerke in Hyper-V

Mit Hyper-V stehen Ihnen für Ihre virtuellen Computer mehrere Arten von Netzwerken zur Verfügung. Sie können den virtuellen Computern drei verschiedene Arten von Netzwerkverbindungen zuweisen. Bei der »internen« Verbindung handelt es sich um eine Netzwerkverbindung, die nur die Kommunikation zwischen den einzelnen virtuellen Servern untereinander und dem physischen Host selbst erlaubt. »Private« Verbindungen erlauben die Kommunikation nur zwischen den virtuellen Servern. Hierbei ist der physische Host von der Kommunikation ausgeschlossen. Bei der »externen« Verbindung dürfen die virtuellen Server mit allen Netzwerkgeräten in Ihrem Netzwerk kommunizieren. Standardmäßig bekommen neue virtuelle Computer diese Netzwerkkommunikation zugewiesen. Die virtuellen Netzwerke aller virtuellen Computer verwalten Sie im Hyper-V-Manager über den Link *Manager für virtuelle Netzwerke* auf der rechten Seite der Konsole. Es öffnet sich ein neues Fenster, über das Sie neue Verbindungen erstellen und bereits vorhandene Verbindungen verwalten. Die Konfiguration ist im Grunde genommen recht einfach. Sie markieren die Verbindung, deren Einstellung Sie anpassen wollen. Im Fenster sehen Sie jetzt den Namen der Verbindung. Dieser Name zeigt der Assistent zur Erstellung von neuen virtuellen Servern an. Im Bereich *Verbindungstyp* legen Sie Art der Verbindung fest. Bei der externen Verbindung steht ein Dropdownmenü zur Verfügung, über das Sie die physische Netzwerkkarte des Hosts auswählen, welche diese Verbindung nutzen soll. Die beiden anderen Verbindungen aktivieren Sie nach Bedarf. Wollen Sie eine neue Verbindung erstellen, klicken Sie auf *Neues virtuelles Netzwerk*, wählen die Verbindungsart aus und klicken auf *Hinzufügen*. Anschließend legen Sie den Namen der Verbindung sowie deren Eigenschaften fest. Auch bei neu erstellten Verbindungen lassen sich Einstellungen jederzeit anpassen.

Abbildg. 25.23 Verwalten der virtuellen Netzwerke in Hyper-V



Bereits erstellten virtuellen Servern lassen sich neue Verbindungen über die Einstellungen der virtuellen Computer zuweisen. Diese rufen Sie über das Kontextmenü im Hyper-V-Manager auf. Die Netzwerkeinstellungen finden Sie unter *Netzwerkkarte*. Wollen Sie einer bereits vorhandenen Netzwerkverbindung eine neue hinzufügen, klicken Sie in den Einstellungen des virtuellen Servers auf *Hardware hinzufügen* und wählen die neue Netzwerkverbindung aus. Neue Hardware lässt sich allerdings erst dann integrieren, wenn Sie den virtuellen Server herunterfahren und ausschalten.

TIPP Microsoft stellt zahlreiche interessante Webseiten zur Verfügung, die sehr wertvolle Hilfe beim Umgang mit Hyper-V bieten:

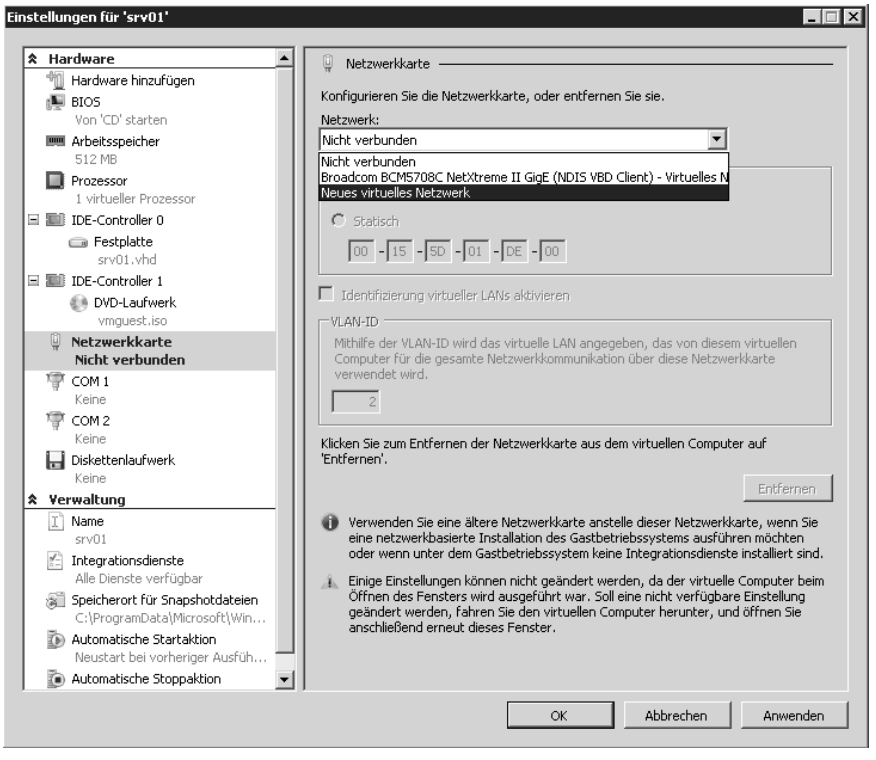
- Virtualization TechCenter: *http://technet.microsoft.com/en-us/virtualization/default.aspx*
- Hyper-V Planning and Deployment Guide: *http://download.microsoft.com/download/8/1/5/81556693-1f05-494a-8d45-cdeeb6d735e0/HyperV_Deploy.doc*
- Hyper-V Forum: *http://forums.technet.microsoft.com/en-US/winserverhyperv/threads/*
- Virtualization Solution Accelerators: *http://technet.microsoft.com/en-us/solutionaccelerators/cc197910.aspx*
- Windows Server 2008 Virtualization & Consolidation: *http://www.microsoft.com/windowsserver2008/en/us/virtualization-consolidation.aspx*
- Hyper-V FAQ: *http://www.microsoft.com/windowsserver2008/en/us/hyperv-faq.aspx*
- Windows Server 2008 Hyper-V Performance Tuning Guide: *http://www.microsoft.com/whdc/system/sysperf/Perf_tun_srv.mspx*

- MSDN & TechNet Powered by Hyper-V: *http://blogs.technet.com/virtualization/archive/2008/05/20/msdn-and-technet-powered-by-hyper-v.aspx*
- MSDN & TechNet Powered by Hyper-V Whitepaper: *http://download.microsoft.com/download/6/C/5/6C559B56-8556-4097-8C81-2D4E762CD48E/MSCOM_Virtualizes_MSDN_TechNet_on_Hyper-V.docx*
- Optimized Desktop: *http://www.microsoft.com/windows/products/windowsvista/enterprise/default.mspx*
- Microsoft Virtualization: *http://www.microsoft.com/virtualization/default.mspx*
- Virtualization Case Studies: *http://www.microsoft.com/virtualization/case-studies.mspx*

Blogs:

- *http://blogs.technet.com/virtualization/default.aspx*
- *http://blogs.msdn.com/virtual_pc_guy/*
- *http://blogs.technet.com/jhoward/*
- *http://blogs.technet.com/roblarson/*
- *http://blogs.technet.com/virtualworld/*
- *http://blogs.technet.com/windowsserver/*
- *http://blogs.technet.com/mapblog/*
- *http://blogs.technet.com/stbnewsbytes/*

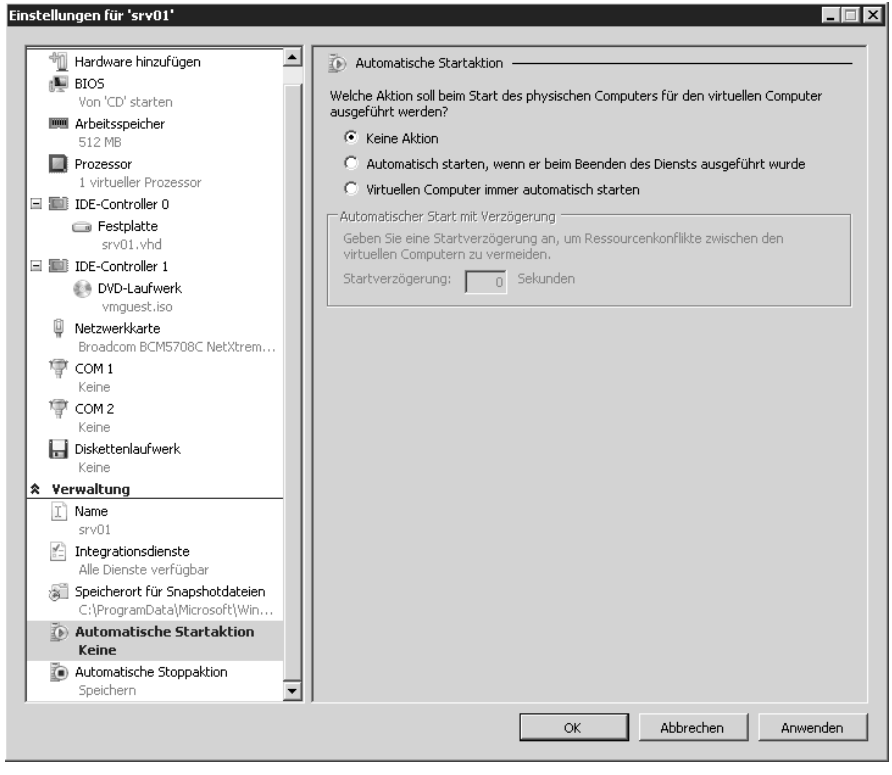
Abbildg. 25.24 Verbinden einer neuen Netzwerkverbindung mit einem bereits erstellten virtuellen Server



Betreiben von Hyper-V im Cluster

Ein weiterer sehr wichtiger Punkt beim Einsatz von Hyper-V ist die Clusterunterstützung dieser Funktion. Betreiben Sie Hyper-V in einem Cluster, können Sie sicherstellen, dass beim Ausfall eines physischen Hosts alle virtuellen Server durch einen weiteren Host automatisch übernommen werden. Im Kapitel 19 sind wir bereits ausführlich auf den Betrieb eines Clusters mit Windows Server 2008 eingegangen. Um Hyper-V in einem Cluster zu betreiben, installieren Sie zunächst einen herkömmlichen Cluster, wie bereits in Kapitel 19 beschrieben. Idealerweise sollten Sie vor der Installation der Clusterfunktion von Windows Server 2008 erst die Hyper-V-Rolle auf beiden physischen Knoten installieren. Die Installation unterscheidet sich dabei nicht von der Installation auf einem allein stehenden Server. Achten Sie aber bei der Erstellung des virtuellen Netzwerkes für Hyper-V darauf, dass die Bezeichnung dieser Verbindung auf beiden Knoten exakt identisch sein muss. Anschließend erstellen Sie einen neuen Cluster wie bereits in Kapitel 19 ausführlich beschrieben. Legen Sie anschließend neue virtuelle Computer an, müssen Sie darauf achten, dass deren Dateien auf dem gemeinsamen Datenträger des Clusters liegen. Fällt der aktive Knoten aus, kann auf diesem Weg der passive Knoten die Dienste der virtuellen Server übernehmen. Auf dem gemeinsamen Datenträger müssen auch die virtuellen Festplatten der virtuellen Server liegen. Bevor Sie einen virtuellen Computer in einem Cluster betreiben können, müssen Sie noch einige Einstellungen vornehmen. Zunächst rufen Sie die Eigenschaften des virtuellen Computers auf und wechseln zu *Verwaltung/Automatische Startaktion*. Stellen Sie sicher, dass *Keine Aktion* ausgewählt ist. Die Ausfallsicherheit konfigurieren Sie später.

Abbildg. 25.25 Virtuelle Computer in einem Cluster dürfen nach einem Ausfall nicht automatisch starten



Die Ausfallsicherheit eines virtuellen Servers stellen Sie über die Failover-Clusterverwaltung sicher. Klicken Sie nach dem Start mit der rechten Maustaste auf den Konsoleneintrag *Dienste und Anwendungen* für den Cluster und wählen Sie den Kontextmenüeintrag *Dienst oder Anwendung konfigurieren*.

Abbildg. 25.26 Konfigurieren von virtuellen Computern in einem Cluster

Wählen Sie anschließend im neuen Fenster die Option *Virtueller Computer* aus. Nach Ihrer Bestätigung öffnet sich ein neues Fenster und Sie können die virtuellen Computer auswählen, die Sie in den Cluster integrieren wollen.

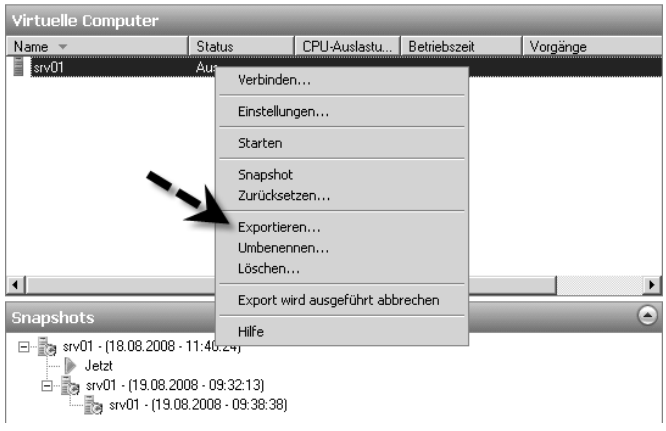
Abbildg. 25.27 Virtuelle Computer lassen sich in einen Windows Server 2008-Cluster integrieren

Nachdem Sie den virtuellen Computer ausgewählt haben, zeigt die Failover-Clusterverwaltung den Computer unterhalb der Dienste und Anwendungen an. Per Rechtsklick auf den virtuellen Computer starten Sie diesen. Die virtuellen Computer lassen sich innerhalb der Clusterknoten – wie alle Clusterressourcen – beliebig verschieben. Die generelle Verwaltung dieser Computer unterscheidet sich nicht von der Verwaltung virtueller Computer auf herkömmlichen Hosts.

Exportieren und Importieren von virtuellen Computern

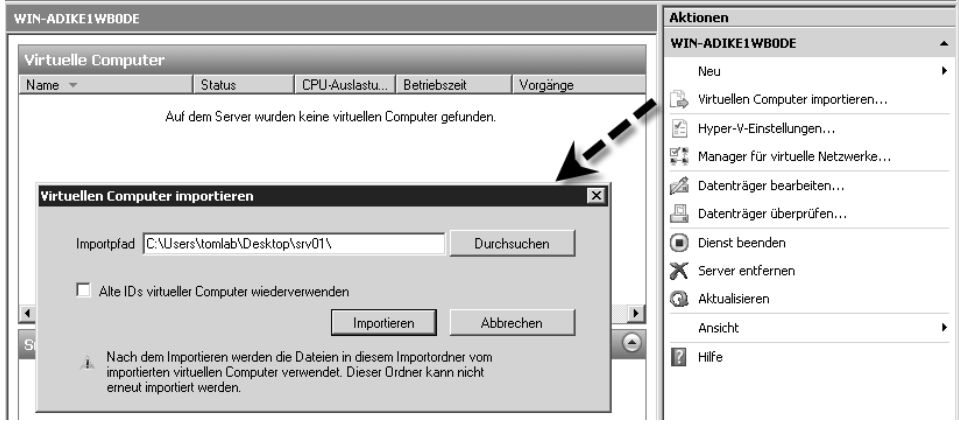
In Hyper-V lassen sich virtuelle Computer von einem Server exportieren und auf einem anderen Server wieder importieren. Dabei besteht die Möglichkeit, den kompletten virtuellen Computer mit Snapshots, Konfigurations-Dateien und VHD-Datei in ein Verzeichnis zu kopieren. Sie starten diesen Vorgang über das Kontextmenü des virtuellen Computers im Hyper-V-Manager. Anschließend wählen Sie ein Export-Verzeichnis aus. Daraufhin legt der Assistent automatisch ein neues Verzeichnis mit dem Namen des virtuellen Computers an. Dieses Verzeichnis enthält die VHD-Datei, Snapshots und die Einstellungen des virtuellen Computers.

Abbildg. 25.28 Exportieren vom virtuellen Servern in Hyper-V



Wollen Sie auf einem anderen Server einen virtuellen Computer wieder importieren, wählen Sie den Menübefehl *Virtuellen Computer importieren* aus und verwenden das Verzeichnis mit den Dateien des virtuellen Computers.

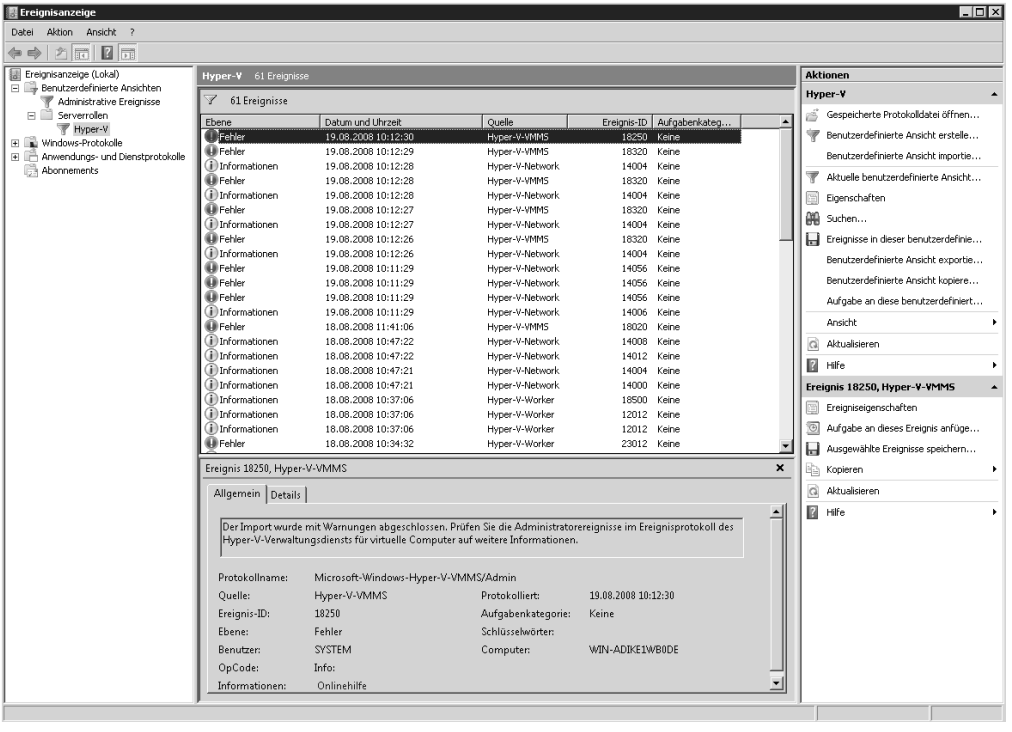
Abbildg. 25.29 Importieren eines virtuellen Computers



Finden und Beheben von Fehlern in Hyper-V

Nach der Installation von Hyper-V erstellt der Assistent im Ereignisprotokoll des Servers eine neue Ansicht, welche nur die Hyper-V-Ereignisse enthält. Sie finden diese Ereignisse über *Benutzerdefinierte Ansichten/Serverrollen/Hyper-V*.

Abbildg. 25.30 Windows Server 2008 protokolliert Hyper-V-Ereignisse im Ereignisprotokoll und erstellt automatisch eine Ansicht



TIPP Ein häufiges Problem beim Ausführen von virtuellen Computern tritt auf, wenn die Virtualisierungsfunktionen des Prozessors im BIOS nicht eingeschaltet sind. In diesem Fall erhalten Sie beim Starten von virtuellen Computern eine entsprechende Fehlermeldung. Solche Fehler treten zum Beispiel auf, wenn Sie das BIOS auf dem physischen Host aktualisiert haben und die Standardeinstellungen verwenden. Die meisten BIOS-Versionen aktivieren die Virtualisierungsunterstützung nicht automatisch.

Häufig tritt auch das Problem auf, dass der Mauszeiger innerhalb von virtuellen Computern nicht ordnungsgemäß angezeigt wird. Überprüfen Sie in diesem Fall, ob die Integrationsdienste installiert sind und installieren Sie diese – falls erforderlich – nach. Anschließend sollte sich der Mauszeiger problemlos zwischen Host und den einzelnen virtuellen Computern navigieren lassen. Die Installation der Integrationsdienste sorgt darüber hinaus auch dafür, dass die Treiber des Hosts und die verwendete Hardware im Geräte-Manager des Gastes angezeigt werden. Ohne installierte Integrationsdienste stehen die verschiedenen Treiber des Hosts nicht in den virtuellen Computern zur Verfügung.

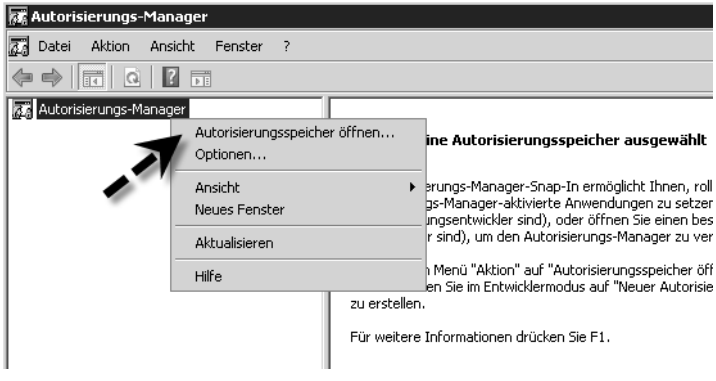
TIPP AMD stellt für seine eigenen Prozessoren über seine Website ein Tool zur Verfügung, mit dem Sie testen können, ob Ihre CPU kompatibel zu Hyper-V ist. Sie finden das Tool sowie Informationen dazu auf den folgenden Internetseiten:

- *http://www.amd.com/us-en/Processors/TechnicalResources/0,,30_182_871_9033,00.html*
- *http://www.amd.com/us-en/assets/content_type/utilities/AMD-V_Hyper-V_Compatibility_Check_Utility.zip*

Delegieren von Berechtigungen in Hyper-V

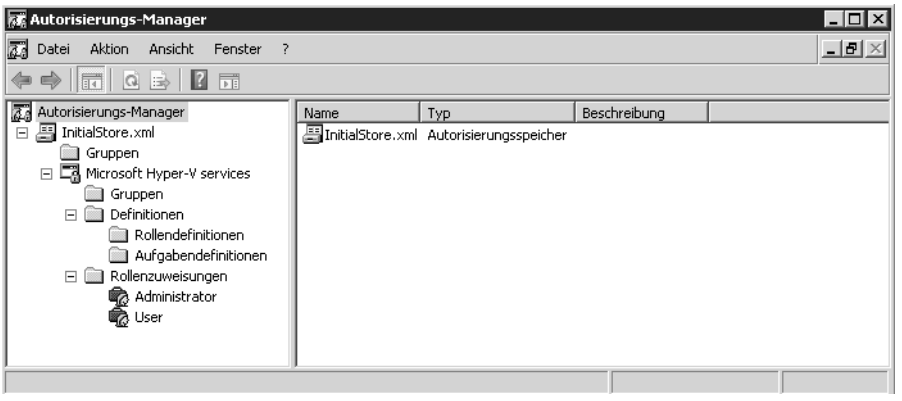
Hyper-V bietet die Möglichkeit, auf Basis der Windows-Gruppenzugehörigkeit oder des Benutzernamens bestimmte Rechte an Administratoren zu delegieren. Dies ist zum Beispiel sinnvoll, wenn nicht jeder Administrator alle Rechte an einem Server haben soll. Um diese Rechte zu delegieren, verwenden Sie den Autorisierungs-Manager von Windows Server 2008. Diesen starten Sie am schnellsten, wenn Sie den Befehl *azman.msc* in das Suchfeld des Startmenüs eingeben. Alternativ können Sie den Autorisierungs-Manager auch als Snap-In in einer MMC öffnen. Der nächste Schritt besteht darin, dass Sie einen Autorisierungsspeicher öffnen. Dazu klicken Sie mit der rechten Maustaste auf den Konsoleneintrag *Autorisierungs-Manager* und wählen im Kontextmenü den Befehl *Autorisierungsspeicher öffnen* aus.

Abbildg. 25.31 Öffnen eines Autorisierungsspeichers für den Autorisierungs-Manager



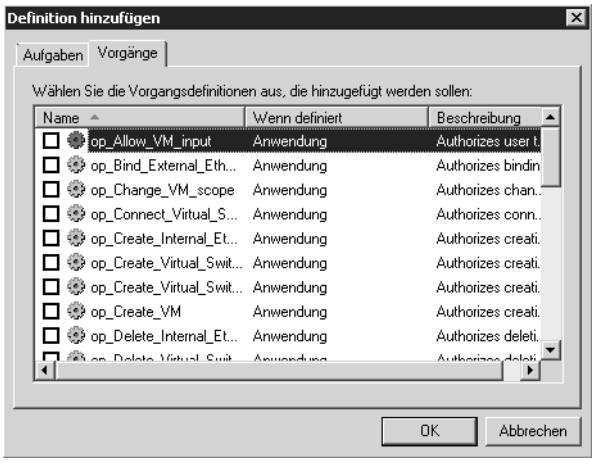
Im Anschluss navigieren Sie zum Ordner *C:\ProgramData\Microsoft\Windows\Hyper-V* und öffnen die Datei *InitialStore.xml*. Diese Datei enthält den Autorisierungsspeicher von Hyper-V, mit dem Sie alle notwendigen Aufgaben delegieren können. Achten Sie darauf, dass dazu die versteckten Systemdateien angezeigt werden müssen. Jetzt öffnet sich der Speicher. Anschließend lassen sich über das Fenster definierte Rollen erstellen und Befehle zuweisen.

Abbildg. 25.32 Hyper-V-Aufgaben mit dem Autorisierungs-Manager delegieren



Klicken Sie auf *Aufgabendefinitionen* und dann auf *Neue Aufgabendefinition*. Klicken Sie im neuen Fenster auf *Hinzufügen* und bestätigen Sie das Informationsfenster. Auf der Registerkarte *Vorgänge* werden Ihnen alle Aufgaben aufgelistet, die sich an Benutzer oder Gruppen verteilen lassen.

Abbildg. 25.33 Der Autorisierungsspeicher bietet mehrere Definitionen an, Aufgaben zu delegieren

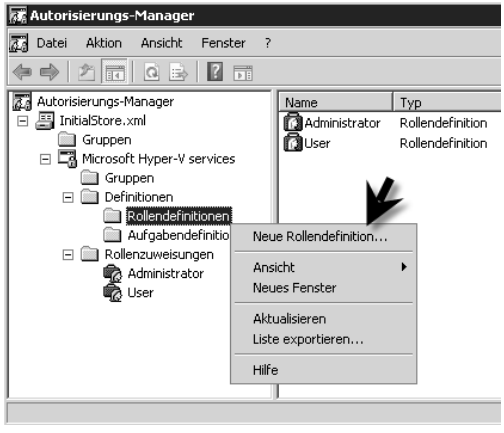


Über den Menübefehl *Rollenzuweisung* können Sie basierend auf diesen Aufgaben einzelnen Benutzern oder Gruppen Rechte zuweisen. Anstatt jedoch den Standardbereich zur Zuweisung zu verwenden, ist es besser, einen eigenen Bereich zu erstellen. Klicken Sie dazu mit der rechten Maustaste auf *Microsoft Hyper-V services* und wählen im Kontextmenü den Befehl *Neuer Bereich*. Geben Sie anschließend einen Namen ein. In der Konsole sehen Sie jetzt die gleichen Menüs für den Standardbereich und können Delegationen konfigurieren, ohne die Standardeinstellungen zu verändern.

Im folgenden Abschnitt zeigen wir Ihnen an einem Beispiel, wie Sie bei der Delegation von Rechten am besten vorgehen:

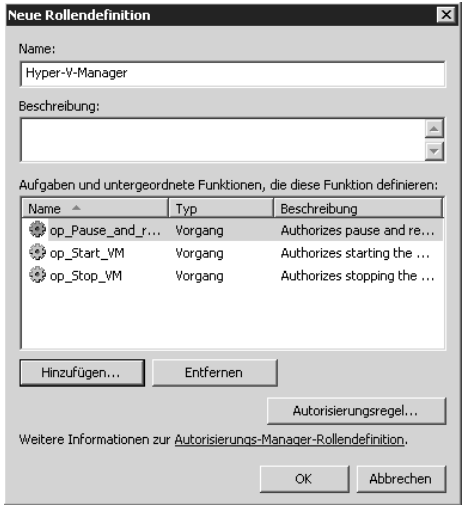
1. Öffnen Sie den Autorisierungs-Manager mit *azman.msc*.
2. Öffnen Sie die Datei *InitialStore.xml* im Ordner *C:\ProgramData\Microsoft\Windows\Hyper-V*.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste unterhalb von *Microsoft Hyper-V services/Definitionen* auf *Rollendefinitionen* und wählen *Neue Rollendefinition* aus.

Abbildg. 25.34 Erstellen einer neuen Rollendefinition für Hyper-V



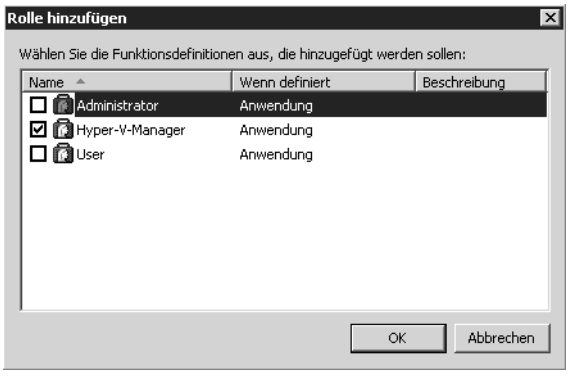
4. Fügen Sie im neuen Fenster einen Namen für die neue Rolle hinzu, zum Beispiel *Hyper-V-Manager*.
5. Klicken Sie auf die Schaltfläche *Hinzufügen*.
6. Wechseln Sie im nun geöffneten Dialogfeld *Definition hinzufügen* zur Registerkarte *Vorgänge*.
7. Wählen Sie die Aufgaben aus, die diese Rolle durchführen darf, und bestätigen Sie diese.

Abbildg. 25.35 Auswählen der Aufgaben zur Delegation



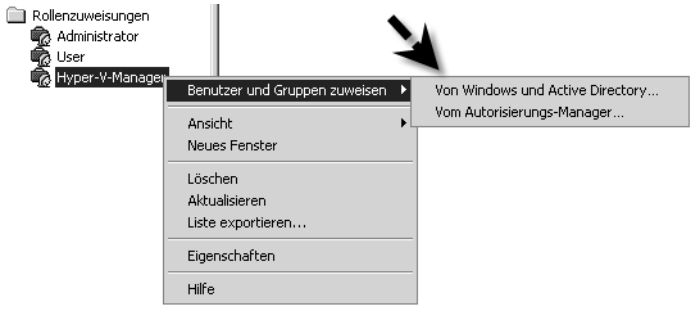
8. Nachdem Sie eine neue Rolle definiert und deren Berechtigungen konfiguriert haben, legen Sie fest, welche Windows-Benutzer mit dieser Rolle arbeiten dürfen. Legen Sie hierfür am besten eine Windows-Gruppe an, der Sie anschließend die Rolle zuweisen. Klicken Sie dazu im Autorisierungs-Manager mit der rechten Maustaste auf *Rollenzuweisung* und wählen Sie *Rollen zuweisen*.
9. Wählen Sie im neuen Dialogfeld zunächst Ihre vorhin erstellte Rollendefinition *Hyper-V-Manager* aus.

Abbildg. 25.36 Auswählen der Rolle für die Steuerung der Berechtigungen in Hyper-V



10. Klicken Sie als Nächstes mit der rechten Maustaste unterhalb von Rollenzuweisungen auf Ihre erstellte Rolle und wählen Sie im Untermenü *Benutzer und Gruppen zuweisen* den Befehl *Von Windows und Active Directory* aus.

Abbildg. 25.37 Auswählen der Gruppen für die Berechtigung in Hyper-V



11. Legen Sie anschließend die Gruppe oder den Benutzer fest, der bzw. dem Sie diese Rolle zuweisen wollen. Nach der Auswahl zeigt die Konsole die Gruppe auf der rechten Seite der Konsole an, wenn Sie die entsprechende Rollendefinition anklicken. Die Benutzer können jetzt bei der Anmeldung an Ihrem Computer genau die Aufgaben durchführen, die Sie konfiguriert haben.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie effizient mit Hyper-V umgehen und virtuelle Computer unter Windows Server 2008 erstellen. Da sich die Hyper-V-Technologie optimal in die Windows Server 2008-Infrastruktur einbindet, lassen sich alle anderen Bereiche in diesem Buch hervorragend mit Hyper-V verbinden. Die virtuellen Computer unterscheiden sich nicht von physischen im Bereich der Verwaltung.

Stichwortverzeichnis

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Der Autor

Thomas Joos

ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT-Branche tätig. Er schreibt Fachbücher und -artikel zu Microsoft-Produkten und anderen Themen in der IT und berät Unternehmen im Mittelstands- und Enterprisebereich in den Bereichen Microsoft-Netzwerke, Active Directory, Exchange Server und IT-Sicherheit.