Das Handbuch

Microsoft®

Windows Server 2012 R2

Insider-Wissen
praxisnah und kompetent

Thomas Joos

Microsoft

Thomas Joos

Microsoft Windows Server 2012 R2 – Das Handbuch

Microsoft Press

Kommentare und Fragen können Sie gerne an uns richten:

Microsoft Press Deutschland
Konrad-Zuse-Straße 1
85716 Unterschleißheim
E-Mail: *mspressde@oreilly.de*

15 14 13 12 11 10 9 8 7 6 5 4 3 2 1
16 15 14

Druck-ISBN 978-3-86645-179-7
PDF-ISBN 978-3-84834-3106-2
EPUB-ISBN 978-3-84831-0261-1
MOBI-ISBN 978-3-84832-1238-2

Fachlektorat: Georg Weiherer, Münzenberg
Korrektorat: Dorothee Klein, Siegen
Lektorat: Florian Helmchen, florian@oreilly.de
Layout und Satz: Gerhard Alfes, mediaService, Siegen (www.mediaservice.tv)
Umschlaggestaltung: Hommer Design GmbH, Haar (www.HommerDesign.com)
Gesamtherstellung: Kösel, Krugzell (www.KoeselBuch.de)

Übersicht

Inhaltsverzeichnis

Vorwort

Mit Windows Server 2012 R2 stellt Microsoft den Nachfolger von Windows Server 2012 verfügbar. Auch wenn der Name recht ähnlich ist, gibt es eine Vielzahl von Neuerungen. Im Bereich der Virtualisierung wurde Windows Server 2012 R2 mit einer neuen Version von Hyper-V ausgestattet, die wesentlich robuster ist und sich leichter replizieren lässt. Die Hochverfügbarkeit hat Microsoft deutlich verbessert.

Auch die anderen Serverdienste hat Microsoft überarbeitet. Unternehmen profitieren von der neuen Serverrolle *Essentials-Umgebung*. Diese integriert auf einem Server mit Windows Server 2012 R2 Standard/Datacenter die bekannten Features zur Datensicherung von Clients und der besseren Verwaltung von Windows Server 2012 R2 Essentials. Auch Dateiserver profitieren von Windows Server 2012 R2: Die Funktion der Datendeduplizierung wurde erweitert, virtuelle Festplatten auf Basis von VHDX-Dateien lassen sich jetzt auch als iSCSI-Ziel einsetzen, das SMB-Protokoll wurde verbessert und vieles mehr.

In diesem Buch zeigen wir Ihnen die Neuerungen von Windows Server 2012 R2 auf Basis der finalen Edition. Wir haben wie immer bewusst auf die fertige Version gewartet, da in der Preview-Version von Windows Server 2012 R2 zahlreiche Funktionen nicht oder nur teilweise integriert waren. Das gilt zum Beispiel für die neuen Arbeitsordner und Arbeitsplatznetzwerke, mit denen Sie Rechner auf Basis von Windows 8.1 besser an Windows Server 2012 R2 anbinden können. Überhaupt arbeiten Windows Server 2012 R2 und Windows 8.1 noch enger zusammen als Windows Server 2012 und Windows 8. Auch iPads und iPhones lassen sich jetzt auf Basis von Arbeitsplatznetzwerken mit Unternehmensnetzwerken und Active Directory-Gesamtstrukturen verbinden. Wir zeigen Ihnen, wie Sie dabei vorgehen.

Durch den enormen Funktionsumfang von Windows Server 2012 R2 konnten wir nicht alle Bereiche des Servers voll umfassend behandeln. Wir zeigen Ihnen alle Technologien und geben zahlreiche Tipps zu Tools und Bordmitteln. Wenn Sie sich noch tiefgehender mit Hyper-V und Windows Azure sowie der Zusammenarbeit mit System Center Virtual Machine Manager 2012 R2 und den neuen Remotedesktopdiensten auseinandersetzen wollen, empfehle ich Ihnen das erst noch erscheinende Buch »Hyper-V – Das Handbuch« bei Microsoft Press.

Zusätzlich zu den Büchern bieten wir auch mehrstündige Videotrainings zu den Themen Windows Server 2012/2012 R2, Windows Server 2012 R2 Essentials, Hyper-V, Windows 8.1, Exchange Server 2013 und vielem mehr an. Einige Videos aus den Trainings stehen online kostenfrei zur Verfügung. Die kompletten Trainings können Sie günstig abonnieren oder als DVD kaufen. Nähere Informationen dazu finden Sie auf: *http://thomasjoos.wordpress.com/*. Auch für Windows 8.1 finden Sie ein interessantes Buch mit dem Titel »Microsoft Windows 8.1 Expertentipps« bei Microsoft Press. Hier habe ich alle interessanten Tipps für Profis für das neue Betriebssystem zusammengestellt.

Auf der Supportseite zu diesem Buch finden Sie wahlweise unter *www.microsoft-press.de/support/9783866451797* oder unter *http://msp.oreilly.de/support/2437/856* eine ausführliche Linkliste, die Sie auf Ihren Rechner herunterladen können. In dieser Liste sind sämtliche Links aufgeführt, die in diesem Buch angeben sind, und Sie können so per einfachem Klick die Software bzw. jeweiligen Informationen bequem herunterladen, ohne lange Links eintippen zu müssen.

Ich wünsche Ihnen mit Windows Server 2012 R2 und Windows 8.1 viel Spaß!

Ihr
Thomas Joos

Teil A

Einstieg und erste Schritte

Kapitel 1

Neuerungen und Lizenzierung

In diesem Kapitel:

Nachfolgend zeigen wir Ihnen die Neuerungen in Windows Server 2012 R2 im Vergleich zu Windows Server 2008 R2, aber auch die Neuerungen zwischen Windows Server 2012 und Windows Server 2012 R2. Windows Server 2012 R2 bietet auch im Vergleich zum direkten Vorgänger Windows Server 2012 zahlreiche Neuerungen. Im Unterschied zu Windows 8.1 ist die Aktualisierung von Windows Server 2012 zu Windows Server 2012 R2 nicht kostenlos. Unternehmen müssen die neue Serverversion lizenzieren. Für Kunden mit Software-Assurance-Vertrag steht diese Version kostenlos zur Verfügung.

Für Unternehmen ist noch interessant zu wissen, dass System Center 2012 R2 mit den Funktionen von Windows Server 2012 R2 zusammenarbeitet. Vorteil ist, dass Unternehmen die Funktionen der neuen Serverversion zentral mit System Center-Produkten verwalten können.

Windows Server 2012 R2 – Die Neuerungen im Überblick

Der Nachfolger von Windows Server 2008 R2 bietet viele Neuerungen im Bereich der Virtualisierung und der Zusammenarbeit von Servern im Netzwerk. Um die neue Version einzusetzen, müssen Unternehmen aber nicht alle Server ersetzen. Windows Server 2012 R2 lässt sich sowohl als Mitgliedserver als auch als Domänencontroller in gemischten Netzwerken betreiben. Alle Vorteile erreichen Sie allerdings nur, wenn Sie alle Server auf die neue Version umstellen. Natürlich können Sie Windows Server 2012 R2 auch zusammen mit Windows Server 2012 betreiben.

Das Wichtigste seit Windows Server 2012 ist, dass es nur noch die Editionen Standard, Datacenter, Essentials und Foundation gibt. Das gilt auch für Windows Server 2012 R2. Das Betriebssystem ist, wie der Vorgänger, nur noch als 64-Bit-Software erhältlich. Für Unternehmen spielen vor allem die Editionen Standard und Datacenter eine Rolle. Diese beiden Editionen verfügen über exakt den gleichen Funktionsumfang. Es lassen sich also auch mit der Standard-Edition Cluster, die Rechteverwaltung und alle Funktionen der Active Directory-Zertifikatsdienste betreiben, die bisher nur den Editionen Enterprise und Datacenter in Windows Server 2008 R2 vorbehalten waren.

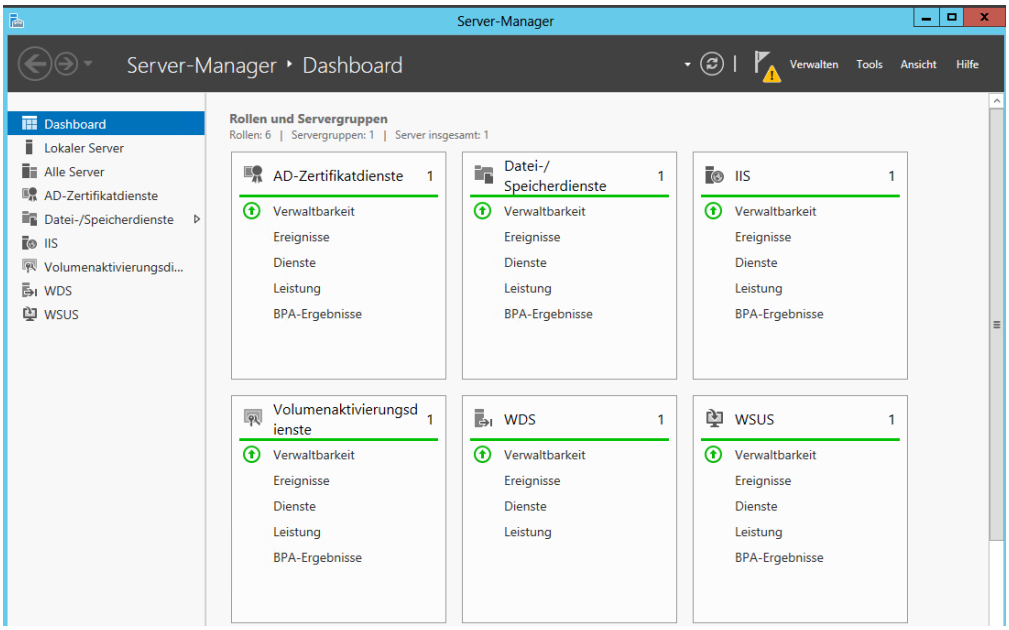
Die Editionen Standard und Datacenter unterscheiden sich in Windows Server 2012 R2 lediglich in der Lizenzierung. Das heißt, die Standard-Edition verfügt jetzt auch über alle Funktionen, die bisher nur den Enterprise-Editionen von Windows Server vorbehalten waren. Das sind zum Beispiel Failoverclustering, BranchCache – Gehosteter Cacheserver, Active Directory Federation Services (AD FS) und mehr.

Bessere Verwaltung im Server-Manager

Neuerungen finden sich nach der Installation von Windows Server 2012 zunächst im Server-Manager. Zwischen Windows Server 2012 R2 und Windows Server 2012 gibt es hier keine Unterschiede zu sehen. Der Server-Manager bietet eine wesentlich effizientere Verwaltung von mehreren Servern im Netzwerk und eine von Windows Phone und Windows 8 bzw. Windows 8.1 bekannte neue Benutzeroberfläche.

Ab Windows Server 2012 und auch in Windows Server 2012 R2 ist es zum Beispiel möglich, Serverrollen und Features über das Netzwerk auf anderen Servern zu installieren (siehe Kapitel 3 und 4).

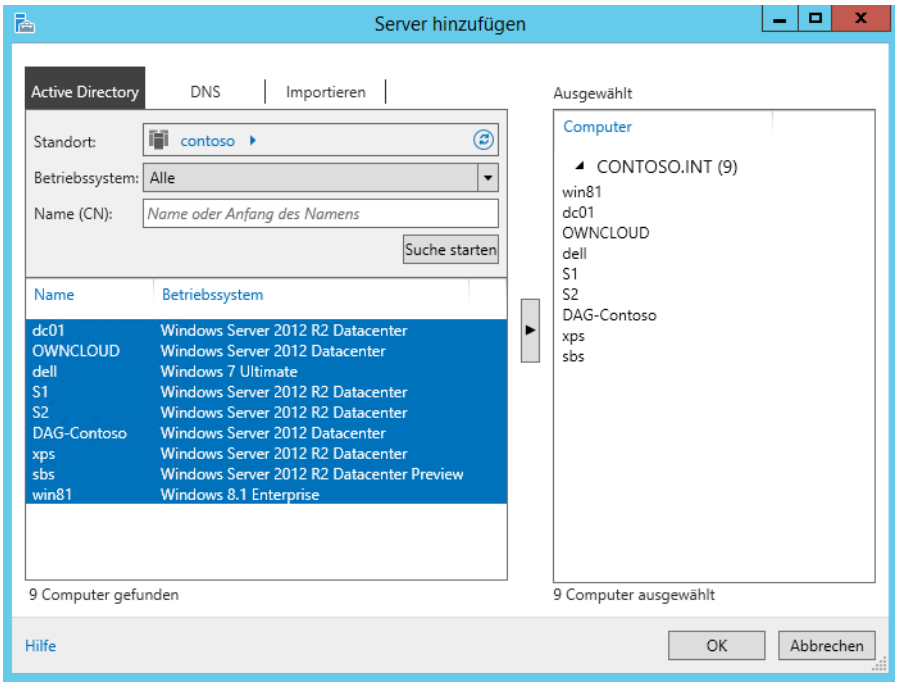
Abbildg. 1.1 Verwalten von Servern läuft in Windows Server 2012 R2 komplett über den Server-Manager



Den Assistenten zur Installation von Serverrollen und Features hat Microsoft zu einem einzelnen Assistenten zusammengefasst. So lassen sich diese einfacher und schneller installieren, da nur ein Installationsvorgang notwendig ist. Installierte Serverrollen und die entsprechenden Server zeigt der Server-Manager automatisch gruppiert an. Verwaltungswerkzeuge listet der Server-Manager direkt über das *Tools*-Menü an. Hierüber lassen sich alle wichtigen Werkzeuge starten. Die Navigation über ein Startmenü, wie Sie es in früheren Versionen gewohnt waren, ist daher nicht notwendig.

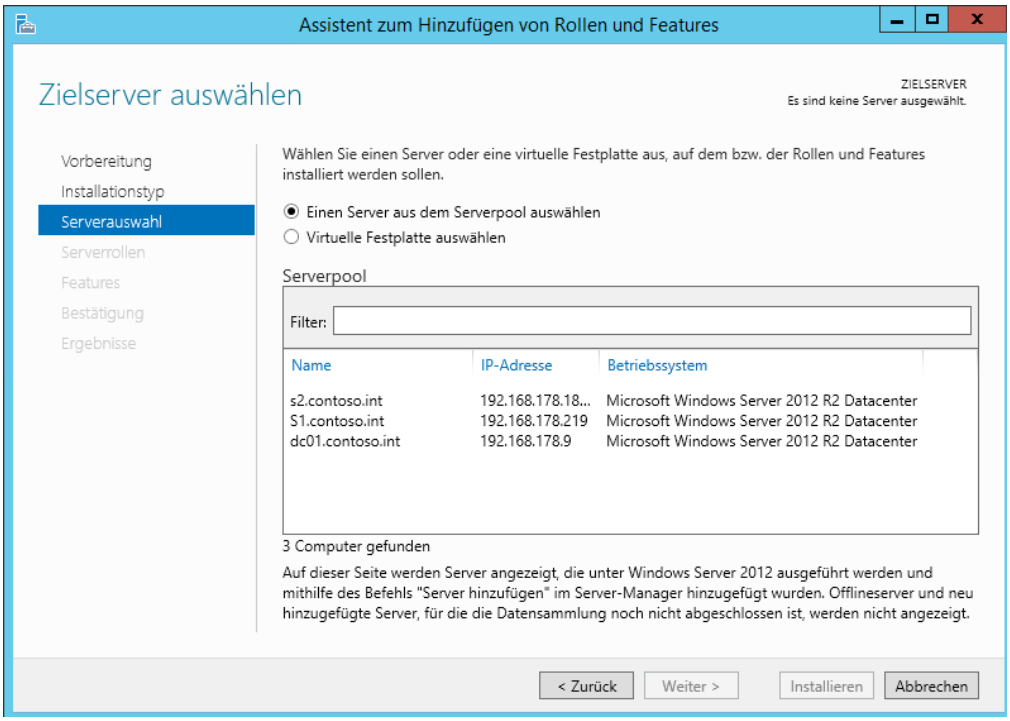
Um im Server-Manager in Windows Server 2012 R2 weitere Server anzubinden, klicken Sie auf *Verwalten* und dann auf *Server hinzufügen*. Im Fenster können Sie anschließend nach Servern suchen, um sie im lokalen Server-Manager zu verwalten. Auf diesem Weg erstellen Sie auch eigene Servergruppen, die Sie im Server-Manager zusammenfassen. Von diesen Gruppen können Sie dann Ereignismeldungen anzeigen lassen.

Abbildg. 1.2 Hinzufügen von zusätzlichen Servern im Server-Manager von Windows Server 2012 R2



Effizient arbeitet der neue Server-Manager allerdings nur mit Windows Server 2012 und Windows Server 2012 R2 zusammen. Auf Servern mit Windows Server 2008 R2 lassen sich über das Netzwerk keine Serverrollen mit dem neuen Server-Manager installieren. Bei der Installation von neuen Serverrollen und Features wählen Sie zunächst den Server aus, auf dem Sie die Rolle oder das Feature installieren wollen, und danach die gewünschten Rollen und Features. Das alles läuft über einen einzelnen Assistenten.

Abbildg. 1.3 Installieren von Rollen und Features auf mehreren Servern im Netzwerk



Neue Funktionen für Dateiserver

Mit Windows Server 2012 bringt Microsoft auch einige Neuerungen bezüglich der Speicherung von Dateien mit. Diese Neuerungen im Vergleich zu Windows Server 2008 R2 sind weiterhin auch in Windows Server 2012 R2 verfügbar, sowie einige mehr. Dateiserver lassen sich in Windows Server 2012 R2 wesentlich effizienter betreiben. Die wichtigsten Neuerungen seit Windows Server 2012 sind die Speicherpools, Datendeduplizierung, das neue Dateisystem ReFS und Verbesserungen im BranchCache. Außerdem bringt Windows Server 2012 Verbesserungen im SMB-Protokoll mit. Im Vergleich zu Windows Server 2012 gibt es weitere Neuerungen, auf die wir ebenfalls nachfolgend eingehen. Es lohnt sich also, Dateiserver auf Windows Server 2012 R2 umzustellen (siehe die Kapitel 5, 20, 21 und 22). Die Datendeduplizierung lässt sich in Windows Server 2012 R2 zum Beispiel auch virtuelle Festplatten ausdehnen.

Wichtig für den Zugriff auf Dateiserver ist das Server Message-Protokoll. Dieses stellt den Zugriff von Clientcomputern zum Server dar. Windows 8.1 und Windows Server 2012 R2 kommen dazu mit dem neuen SMB 3-Protokoll. Dieses ist vor allem für den schnellen Zugriff über das Netzwerk gedacht, wenn Daten normalerweise lokal gespeichert sein sollten. Beispiele dafür sind SQL Server-Datenbanken oder die Dateien von Hyper-V-Computern. Diese lassen sich mit SMB 3 performant auch über das Netzwerk verwenden. Die neue Version erlaubt mehrere parallele Zugriffe auf Dateifreigaben. Das heißt, einzelne Zugriffe über das Netzwerk bremsen sich nicht mehr gegenseitig aus. Von den schnellen Netzwerkzugriffen profitieren vor allem Windows 8 bzw. Windows 8.1 und Windows Server 2012/2012 R2.

HINWEIS Die Abkürzung SMB steht für Server Message Block. Dabei handelt es sich um ein Kommunikationsprotokoll für Datei-, Druck- und andere Serverdienste in Netzwerken.

Zentrale Verwaltung von Dateiservern

Der Server-Manager in Windows Server 2012 bietet wesentlich mehr Funktionen als sein Vorgänger in Windows Server 2008 R2. In Windows Server 2012 R2 gibt es allerdings keine weiteren nennenswerten Vorteile. Installieren Sie auf mehreren Servern im Netzwerk die Dateidienste, legt der Server-Manager automatisch eine neue Gruppe an, in der sich alle Server befinden. Der Vorteil dabei ist, dass Sie Funktionen der Dateiserver zentral im Server-Manager verwalten können. In der Verwaltungskonsole für Dateiserver können Sie zentral alle erstellten Volumes, physische Datenträger, Speicherpools, Freigaben und iSCSI-Einstellungen vornehmen (siehe die Kapitel 3 und 5). Mit dem Server-Manager in Windows Server 2012 R2 können Sie über diesen Weg auch Server mit Windows Server 2012 verwalten. Sie können allerdings auf Server-Managern in Windows Server 2012 keine Funktionen verwalten, die nur Windows Server 2012 R2 bietet, zum Beispiel die Anbindung von VHDX-Dateien als iSCSI-Ziel.

Continuous Availability bei geclusterten Dateiservern

Zusätzlich ermöglicht SMB 3 beim Einsatz auf geclusterten Dateiservern einen besseren Failover zwischen Clusterknoten. Dabei berücksichtigt Windows Server 2012 R2 die SMB-Sitzungen der Benutzer und behält diese auch bei, wenn Sie virtuelle Dateiserver zwischen Clusterknoten verschieben. Die Funktion ist automatisch gesetzt. Allerdings müssen Sie dazu auf den Clientcomputern mit Windows 8 bzw. Windows 8.1 und auf dem Server mit Windows Server 2012/2012 R2 arbeiten.

Neben Clientcomputern mit Windows 8 bzw. Windows 8.1 profitieren natürlich auch andere Server mit Windows Server 2012/2012 R2 von dieser Funktion. Auf diese Weise können Sie mit SQL Server 2012/2014 oder Hyper-V in Windows Server 2012 R2 auch große Datenmengen im Netzwerk speichern. In diesem Zusammenhang ist auch interessant, dass Windows Server 2012 R2 auch als NAS-Server dienen kann. Im neuen Betriebssystem lassen sich nicht nur iSCSI-Ziele mit dem Server verbinden, sondern Server mit Windows Server 2012 R2 können selbst auch als iSCSI-Ziel arbeiten. In Windows Server 2012 R2 können Sie in diesem Bereich auch VHDX-Dateien als iSCSI-Ziel zur Verfügung stellen, Windows Server 2012 hat in diesem Bereich nur VHD-Dateien beherrscht.

Die Clusterfunktion steht auch in Windows Server 2012 R2 Standard zur Verfügung. Damit die Server mit Windows Server 2012/2012 R2 und Clientcomputer mit Windows 8 bzw. Windows 8.1 untereinander schneller Daten austauschen können, ist keine Konfiguration notwendig. Diesen Geschwindigkeitszuwachs erhalten Unternehmen bereits Out-of-the-Box. Microsoft empfiehlt für den schnellen Datenaustausch auf Dateiservern Netzwerkkarten mit 10 Gbit-Adaptern, mindestens aber den Einsatz von zwei 1-Gbit-Adapter. In 100-MBit/s-Netzwerken bringt die neue Funktion keinen nennenswerten Geschwindigkeitszuwachs.

Für eine schnelle Kommunikation zwischen Windows Server 2012 R2 müssen Netzwerkkarten die RDMA-Funktion (Remote Direct Memory Access, Remotezugriff auf den direkten Speicher) unterstützen. Bei dieser Funktion können Server über das Netzwerk Daten im Arbeitsspeicher austauschen. Wichtig ist diese Funktion vor allem, wenn Sie Windows Server 2012 R2 als NAS-Server einsetzen, also iSCSI-Ziel und auf dem Server Datenbanken von SQL Server 2012/2014 oder virtuelle Maschinen von Hyper-V speichern. Eingeschränkt kann auch SQL Server 2008 R2 diese Funktion nutzen, allerdings weder Windows Server 2008 R2 oder ältere Versionen von Microsoft SQL Server (siehe Kapitel 5).

Advanced Format Technology – 4-KB-Festplatten

Das Festplattenformat für 4-KB-Festplatten trägt die Bezeichnung *Advanced Format Technology*. Es ermöglicht physische Festplatten mit einer Sektorgröße von 4 KB. Bisher nutzen Festplatten eine Größe von 512 Byte. Die erhöhte Sektorgröße ist notwendig, damit Hersteller Festplatten mit höherer Speicherkapazität herstellen können. Daher muss auch Hyper-V das neue Format unterstützen. Davon profitiert auch das Betriebssystem, da Windows Server 2012 R2 auch 4 KB große Speichereinheiten nutzt. Das heißt, logische Sektoren passen in einen einzelnen physischen Sektor und sind nicht mehr verteilt.

Administratoren können virtuelle Festplatten effizient auf 4-KB-Festplatten erstellen. Zusätzlich unterstützt Hyper-V auch virtuelle Festplatten, die auf 512e-physische Festplatten erstellt wurden. Da nicht alle Software und Hardware das neue Format unterstützen, melden sich viele Festplatten mit 512-Bit-Emulation am System an, auch 512e genannt. Die Firmware der Festplatte speichert ankommende Datenpakete dann entsprechend in den tatsächlich vorhandenen 4-GB-Sektoren. Auch bei diesen Vorgängen ist Windows Server 2012 R2 wesentlich schneller.

Beim Umgang mit diesen Festplatten ist es wichtig, dass die verwendeten Sektoren des Betriebssystems teilbar durch die Anzahl der vorhandenen physischen Sektoren sind. Ist das nicht der Fall, wird ein logischer Sektor des Betriebssystems auf mehreren physischen Sektoren verteilt, wodurch allerdings die Leistung des Systems enorm leidet.

Virtueller Fibrechannel und ODX

Ebenfalls verbessert ist der Umgang mit SANs (Storage Aera Networks) seit Windows Server 2012. Hier lassen sich Speicherplätze direkt den virtuellen Servern zuordnen. In Hyper-V können Sie mit virtuellen Fibrechannels virtuelle Servern direkt Zugriff auf Fibrechannels in SAN gewähren. Das verbessert die Leistung und erlaubt die Anbindung von Hyper-V-Hosts an mehrere SANs. Vor allem bei der Livemigration kann das echten Mehrwert bieten.

Ebenfalls eine wichtige Neuerung in diesem Bereich ist die Unterstützung von ODX, auch Offloaded Data Transfer genannt, durch Windows Server 2012. Damit kann das Betriebssystem direkt mit der Hardware kommunizieren, um Kopier- oder andere Dateiverwaltungsvorgänge wesentlich schneller und effizienter durchzuführen. Auch Windows Server 2012 R2 profitiert von dieser Funktion.

Den Datenverkehr zwischen SAN und Betriebssystem speichert Windows Server 2012 R2 in einem Puffer. Bei sehr großen Datenmengen kann Windows Server 2012 R2 solche Aktionen auch ohne das Hostsystem direkt mit der Steuerungssoftware des SAN erledigen. Das verbessert deutlich die Leistung des Systems. Für diesen Austausch nutzt Windows Server 2012 R2 ODX. Die meisten SAN-Hersteller nutzen derzeit bereits diese Technik. Vor allem Hyper-V profitiert davon, wenn zum Beispiel virtuelle Server verschoben werden sollen, zum Beispiel zur Livemigration oder der Replikation.

ReFS – Das neue Dateisystem

Datenfestplatten lassen sich in Windows Server 2012 mit dem neuen Dateisystem ReFS (Resilient File System, unverwüstliches Dateisystem) formatieren. Diese Dateisystem ist auch Bestandteil von Windows Server 2012 R2, allerdings nicht von Windows 8.1. Der größte Vorteil des Dateisystems ist dessen Robustheit und die höhere Geschwindigkeit, in der sich das Dateisystem im laufenden Betrieb reparieren lässt.

Außerdem beherrscht das Dateisystem tiefere Ordnerstrukturen und längere Dateinamen. Zusätzlich können keine Daten verloren gehen, da das neue Dateisystem eine verbesserte Version der Schattenkopien mit bringt.

ReFS-Datenträger beherrschen eine Größe von 16 Exabyte. Berechtigungen lassen sich auf ReFS-Datenträger genauso vergeben wie in NTFS. Die Zugriffsschnittstelle (API), mit der das neue Dateisystem kommuniziert, entspricht dem von NTFS. Alles in allem ist ReFS stabiler und schneller als NTFS. Das Dateisystem unterstützt derzeit allerdings keine Bootmedien von Windows Server 2012 R2. Computer mit Windows 7/8/8.1 können problemlos auf Freigaben zugreifen, die auf ReFS-Datenträgern gespeichert sind. Mehr zu diesem Thema lesen Sie in Kapitel 5.

Speicherpools und Speicherplätze

Physische Datenträger können Sie in Windows Server 2012 R2 zu Speicherpools mit einer Größe von 4 Petabyte zusammenfassen. Die Anzahl der Speicherpools auf einem Server ist nicht begrenzt. So lassen sich die Festplatten eines Servers zu logischen Pools zusammenfassen und dadurch auch wesentlich leichter austauschen. Sie können Speicherpools im laufenden Betrieb mit weiteren physischen Festplatten erweitern oder Festplatten austauschen. Speicherplätze bauen wiederum auf Speicherpools auf. Diese sind eine Teilmenge und verhalten sich wie ganz normale Laufwerke auf dem Server. Sie können in den Speicherplätzen Freigaben erstellen und einzelne Speicherplätze auch mit BitLocker verschlüsseln.

Speicherplätze sind immer auf einen Speicherpool begrenzt, aber nicht auf einen einzelnen physischen Datenträger im Pool. Das heißt, die Daten eines Speicherplatzes sind in einem Speicherpool auf die angeschlossenen physischen Festplatten verteilt. Für die Speicherplätze können Sie innerhalb eines Speicherpools auch eine Ausfallsicherheit festlegen, ähnlich zu einem RAID-System. ReFS und Speicherpools/Speicherplätze arbeiten zusammen. Entdeckt ReFS einen Fehler in einem Speicherplatz, veranlasst das Dateisystem eine automatische Reparatur.

Sie können einem Speicherplatz mehr Platz zuweisen, als der Speicherpool insgesamt zur Verfügung hat (Thin Provisioning). Geht der Speicherplatz zur Neige, können Sie einfach weitere Festplatten im Server einbauen und diese dem entsprechenden Speicherpool zuweisen. Sie können aber auch Festplatten gegen größere austauschen.

Virtuelle Festplatten (Speicherplätze) und Speicherpools ersetzen aber keine Freigaben oder Ordner. Diese liegen weiterhin auf dem entsprechenden Datenträger, also in diesem Fall dem Speicherplatz, in Windows Server 2012 R2 virtuelle Datenträger genannt. In dieser Infrastruktur handelt es sich bei den Datenträgern dann um einen virtuellen Datenträger in einem Speicherpool, der wiederum verschiedene physische Festplatten umfasst.

Nach dem Erstellen eines Speicherpools legen Sie den virtuellen Datenträger an und legen für diesen die Ausfallsicherheit fest. Sie können eine Datenspiegelung konfigurieren, keine Ausfallsicherheit oder eine Parität (etwa RAID-5). Die Ausfallsicherheit auszuschließen ist beispielsweise dann sinnvoll, wenn die physischen Festplatten des Speicherpools bereits hardwareseitig durch RAID oder ein SAN abgesichert sind. Dies wird natürlich weiterhin unterstützt. In Kapitel 5 gehen wir ausführlich auf dieses Thema ein.

SSD und SATA-Platten zu Speicherplätzen (Storage Spaces) zusammenfassen

Bereits in Windows Server 2012 können Sie mehrere Festplatten zu virtuellen Speicherplätzen (Storage Spaces) zusammenfassen und so den Speicherplatz effizienter zur Verfügung stellen. In Windows Server 2012 R2 können Sie jetzt auch SSDs mit anderen Festplatten mischen. Der Server analysiert die gespeicherten Daten und legt häufiger verwendete auf den schnelleren Datenträgern ab.

Setzen Sie Windows Server 2012 R2 als iSCSI-Ziel ein, können Sie VHDX-Festplatten mit einer Größe von bis zu 64 TB verwenden. In Windows Server 2012 werden nur VHD-Festplatten mit einer Größe von maximal 2 TB unterstützt. Die virtuellen Festplatten lassen sich jetzt auch in System Center verwalten und so als iSCSI-Target besser zur Verfügung stellen. Zusätzlich wurden in der PowerShell 4.0 weitere Cmdlets zur Verwaltung von iSCSI-Targets integriert.

Das SMB-Protokoll hat Microsoft in Windows Server 2012 R2 weiter überarbeitet und Leistung sowie Ausfallsicherheit erhöht. Verbindung zu SMB-Freigaben sind stabiler und schneller, auch beim Einsatz von Clustern oder im Bereich Hyper-V.

Windows Server 2012 R2 arbeitet problemlos auch mit Windows 8.1 zusammen. So gibt es mit den Arbeitsordnern (Work Folders) die Möglichkeit, Unternehmensdaten mit dem Client auszutauschen, ähnlich zu den Offlinedateien. Anwender, die ihr Notebook mit Windows 8.1 an das Unternehmensnetzwerk anbinden, haben so die Möglichkeit, auf die Daten der Server zuzugreifen, wenn die Administratoren dies über Richtlinien zulassen. Daten in den synchronisierten Arbeitsordnern können Administratoren remote löschen. Die Übertragung der Dateien in den Arbeitsordnern findet verschlüsselt statt.

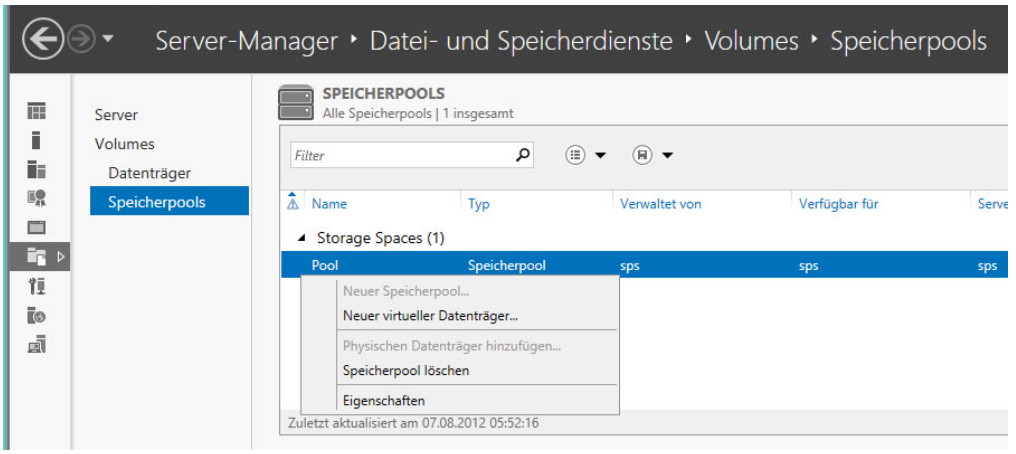
Datendeduplizierung finden und automatisiert zusammenführen

In der jüngsten Vergangenheit wurde Speicherplatz nicht mehr günstiger, sondern stieg im Preis an. Aus diesem Grund überprüfen immer mehr Unternehmen ihre Datenspeicher auf doppelt vorhandene Dateien und Datenmüll. Dieser bindet unnötig Speicherplatz und damit auch finanzielle Mittel. Die Datendeduplizierung bieten eine Funktion, um doppelte Dateien auf den Dateiservern zu finden. Mit diesem Rollendienst in Windows Server 2012 R2 erkennen Dateiserver doppelt gespeicherte Dateien in den Freigaben und können diese bereinigen.

Auf diese Weise lässt sich die Datenmenge auf den Festplatten und Sicherungsmedien sowie die Dauer der Datensicherung teilweise deutlich reduzieren. Die Datendeduplizierungsfunktion untersucht die angeschlossenen Festplatten regelmäßig und zeigt die Deduplizierungsrate im Server-Manager auch an. In Windows Server 2012 R2 können Sie mit diesem Dienst auch virtuelle Festplatten durchsuchen.

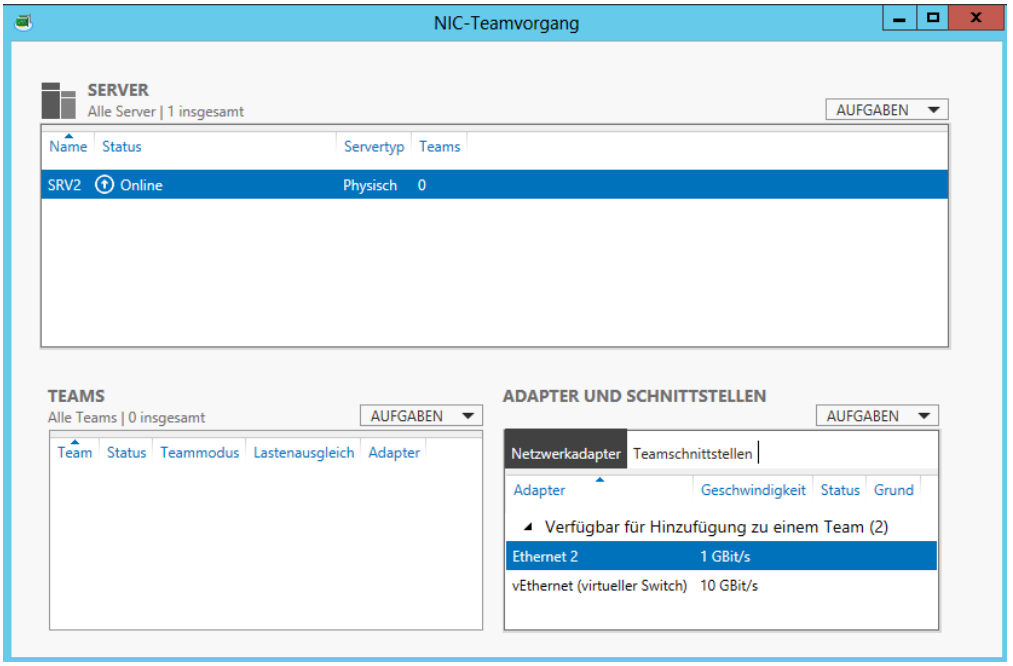
Installieren Sie den Rollendienst zur Datendeduplizierung, integriert der Installations-Assistent auch ein Befehlszeilentool, mit dem Sie die doppelten Dateien suchen können, um abzuschätzen, ob der Rollendienst auf Ihren Dateiservern überhaupt sinnvoll ist. Das Tool DDPEval befindet sich im Ordner *\Windows\System32*. Sie können das Tool auch in Windows 7-, Windows Server 2008 R2- oder Windows 8- bzw. Windows 8.1-Systemen ausführen.

Abbildg. 1.4 Zusammenfassen mehrerer Datenträger zu einem Speicherpool



Windows Server 2012 R2 kann Netzwerkkarten ohne besondere Treiber als Team zusammenfassen. Bisher war das nur mit speziellen Karten und entsprechenden Treibern möglich. Die Einstellungen dazu finden Sie im Server-Manager. Das Zusammenfassen findet über einen Assistenten statt.

Abbildg. 1.5 Zusammenfassen von Netzwerkkarten zu Teams in Windows Server 2012 R2



Verwaltete Dienstkonten bieten in Windows Server 2008 R2 eine Möglichkeit, auch für Serverdienste regelmäßige Kennwortänderungen durchzuführen und die Dienste dazu abzusichern. Aller-

dings erlaubt Windows Server 2008 R2 nur einen Server pro Dienstkonto. Dies verkompliziert die Erstellung und Verwaltung dieser Konten.

Seit Windows Server 2012 hat Microsoft die Grenze der Konten für einzelne Server aufgehoben, sodass sich die verwalteten Dienstkonten netzwerkweit auch auf mehreren Servern nutzen lassen. Das ist zum Beispiel sinnvoll, wenn ein Serverdienst auf mehreren Servern im Einsatz ist, zum Beispiel SQL Server 2012/2014. Die neue Version des Datenbankservers unterstützt die verwalteten Dienstkonten. Windows Server 2012 R2 unterstützt weiterhin auch diese Funktionen. In Kapitel 12 zeigen wir Ihnen den Umgang mit diesen Möglichkeiten.

Effizientere Virtualisierung

Mit Hyper-V Replica lassen sich virtuelle Festplatten und ganze Server asynchron zwischen verschiedenen Hyper-V-Hosts im Netzwerk replizieren und synchronisieren. Die Replikation findet über das Dateisystem statt, ein Cluster ist nicht mehr notwendig (siehe Kapitel 9). Die Replikationen lassen sich manuell, automatisiert oder nach einem Zeitplan ausführen.

Die Einrichtung nehmen Sie über einen Assistenten vor. Damit Hyper-V-Hosts eine solche Replikation zulassen, müssen Sie diese zunächst aktivieren. Auf diesem Weg lassen sich virtuelle Server auch hochverfügbar betreiben, ohne teure Cluster betreiben zu müssen. Die neue Generation virtueller Festplatten in Hyper-V sind für die Replikation optimiert. Auch die maximale Größe von virtuellen Festplatten erhöht Microsoft mit Windows Server 2012. Diese dürfen eine Größe von bis zu 64 TB erreichen. Hyper-V 3.0 berücksichtigt Prioritäten bei Clustern mit Hyper-V und überträgt wichtige Server zuerst zwischen Clusterknoten. Die neue Version kann auch mehrere virtuelle Server auf einmal übertragen, in Windows Server 2008 R2 geht das nur mit einem einzelnen Server.

Für eine bessere Leistung im Netzwerk dürfen virtuelle Server jetzt mehr auf Hardwarefunktionen von Netzwerkkarten zugreifen, was das Tempo enorm beschleunigen kann. In den Einstellungen von virtuellen Netzwerkkarten lassen sich Netzwerkbandbreite von Servern eingrenzen und unerwünschte DHCP- oder Routerpakete blockieren. Dies soll verhindern, dass virtuelle Server unerwünscht als DHCP-Server oder Router agieren und das Netzwerk beeinträchtigen. Kaufen Unternehmen neue Hostsysteme für Hyper-V, sollte darauf geachtet werden, ausreichend Netzwerkkarten in den Server einzubauen. Wichtig ist dabei auch, dass die Adapter die neuen Funktionen in Hyper-V unterstützen.

In den Netzwerkeinstellungen lassen sich unter anderem Berechnungen für IPsec vom Prozessor des virtuellen Servers auf die physische Netzwerkkarte auslagern. Ebenfalls neu in Hyper-V ist die Single-Root I/O Virtualization. Auch hier lassen sich physische Funktionen von Netzwerkkarten in Hyper-V nutzen. Dazu stellen kompatible Netzwerkkarten für virtualisierte Umgebungen implementierte E/A-Kanäle zur Verfügung, mit denen sich die Netzwerkkarte gegenüber virtualisierten Servern wie mehrere Netzwerkkarten verhält. SR-IOV ist vor allem bei E/A-intensiven Anwendungen interessant.

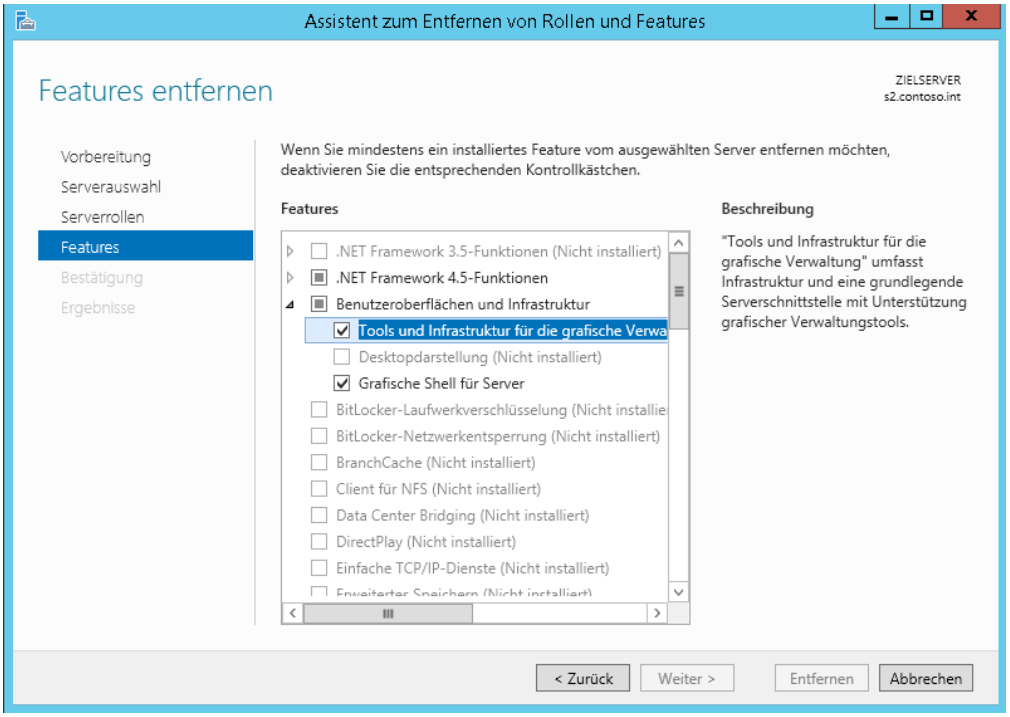
Mehr zur Virtualisierung mit Hyper-V lesen Sie in den Kapiteln 7, 8 und 9.

Core-Server in neuer Version

Die Installation als Core-Server, also ohne grafische Oberfläche, ist in Windows Server 2012 R2 weiterhin der von Microsoft offiziell empfohlene Weg der Installation. Das war bereits in Windows Server 2012 so. Diese Option ist auch standardmäßig ausgewählt, wenn Administratoren die Installation starten. Im Gegensatz zu Windows Server 2008 R2 ist es aber möglich, eine Core-Installation zu einer Installation mit grafischer Oberfläche zu aktualisieren. Dazu müssen Sie lediglich das Verwaltungsprogramm Sconfig auf dem Core-Server starten und den Menübefehl *Wiederherstellen der grafischen Benutzeroberfläche* auswählen.

Die grafische Oberfläche ist in Windows Server 2012 R2 als Serverfeature verfügbar. Das heißt, Sie können von einem vollwertigen Server die grafische Benutzeroberfläche auch wieder deinstallieren. Core-Server sind vor allem für leistungshungrige Serveranwendungen wie Hyper-V oder SQL Server 2012 sinnvoll. Die neue Version des Datenbankservers unterstützt offiziell die Installation auf Core-Servern, auch auf Servern mit Windows Server 2008 R2.

Abbildg. 1.6 Deinstallieren der grafischen Oberfläche in Windows Server 2012 R2



Mehr Sicherheit mit IPAM, DNSSEC und neuem BitLocker

Vor allem Server in Niederlassungen, die mit Servern in der Zentrale verbunden sind und wichtige Daten enthalten, sollten Administratoren besonders absichern. Hier bietet es sich an, die Festplatten mit BitLocker zu verschlüsseln. Diese Funktion arbeitet in Windows Server 2012 R2 wesentlich schneller, da das System nur die bereits verwendeten Daten der Festplatte verschlüsselt und neue Daten nach und nach inkrementell hinzufügt. Außerdem unterstützt die neue Version auch Hardwareverschlüsselungsmethoden von Serverfestplatten (siehe Kapitel 5).

Wichtige Infrastrukturdienste zur Verwaltung der IP-Adressen und Rechnernamen verwalten Administratoren jetzt in einer zentralen Konsole. Auf den neuen IP-Adressverwaltungsservern (IPAM) lassen sich Einstellungen für DHCP und DNS besser zusammen verwalten und absichern. IPAM kann als Serverdienst installiert werden (siehe Kapitel 24).

DNS-Einträge lassen sich in Windows Server 2012 R2 mit DNSSEC besser schützen als in Windows Server 2008 R2. Windows Server 2012 R2 unterstützt offizielle Standards wie NSEC3 und RSA/SHA-2 und erlaubt eine Signierung von Zonen, während diese online sind. Signierte Zonen erlauben auch dynamische DNS-Einträge. Ebenfalls neu ist die Unterstützung von DNSSEC auf schreibgeschützten Domänencontrollern (Read-only Domain Controller, RODC). Findet ein RODC mit Windows Server 2012 R2 eine signierte DNS-Zone, legt er automatisch eine sekundäre Kopie der Zone an und überträgt die Daten der DNSSEC-geschützten Zone. Die Verwaltung von DNSSEC findet über einen Assistenten statt, nicht mehr über das Befehlszeilentool Dnscmd. Die Einrichtung starten Sie über das Kontextmenü des Servers (siehe Kapitel 25).

Generell hat Microsoft auch die PowerShell 3.0 mit Windows Server 2012 deutlich verbessert (siehe Kapitel 40) und in Windows Server 2012 mit der Version 4.0 noch stärker an die Bedürfnisse von Administratoren angepasst. Diese unterstützt Administratoren jetzt wesentlich besser bei der Eingabe von Befehlen und zeigt mehr Hilfen und weniger Fehler.

Außerdem bietet PowerShell wesentlich mehr Cmdlets und Verwaltungsmöglichkeiten zur Anfertigung von Skripts. Serverdienste wie DirectAccess oder RemoteAccess lassen sich besser in der PowerShell verwalten, als noch in Windows Server 2008 R2 (siehe Kapitel 32). Die Verwaltung von RemoteAccess und DirectAccess hat Microsoft jetzt in einer gemeinsamen Konsole zusammengefasst, sodass sich auch diese Funktionen wesentlich schneller und einfacher einrichten lassen.

Im Bereich der Sicherheit hat Microsoft ebenfalls zahlreiche Verbesserungen in das Betriebssystem eingebaut. Windows Server 2012 R2 überwacht bereits den Bootvorgang durch die neue Secure-Boot-Technologie. Findet das Betriebssystem einen Virus oder anderen Angreifer auf einem Datenträger, der beim Booten geladen wird, stoppt das Betriebssystem den Startvorgang. Erreicht wird das durch das frühere Laden der neuen Antivirenfunktion in Windows Server 2012 R2. Lässt sich ein System nicht reparieren, startet Windows Server 2012 R2 das Windows Recovery Environment und erlaubt eine komplette Wiederherstellung des Betriebssystems im ursprünglichen Zustand (siehe Kapitel 35).

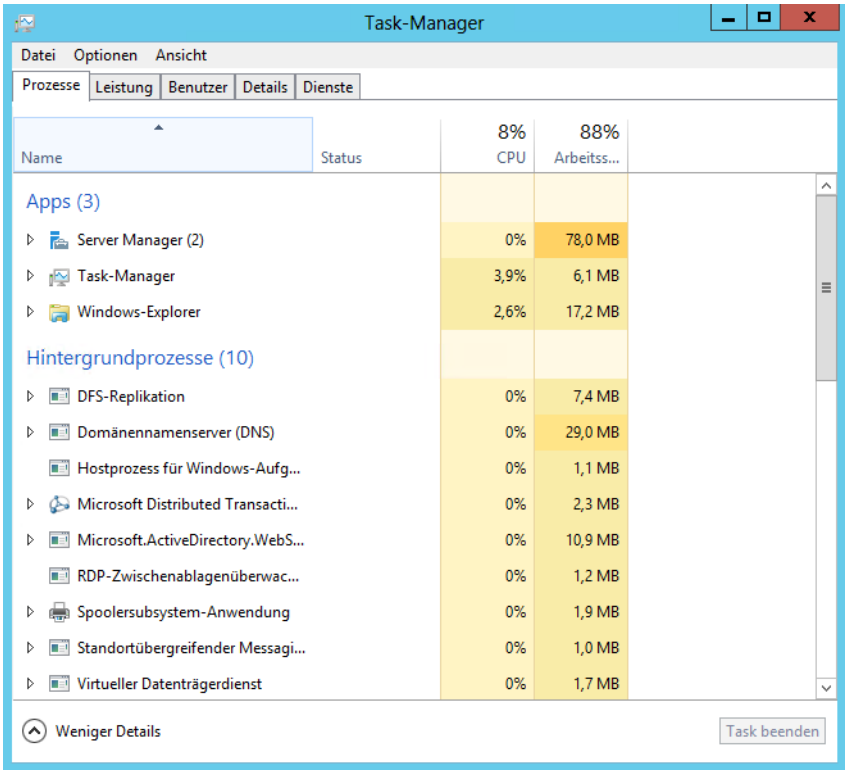
Windows Server 2012 R2 unterstützt die neue BIOS-Version UEFI und deren darin integrierte Funktion zum sicheren Starten (Secure Boot). Diese Funktion wurde in der UEFI-Spezifikation 2.3.1 eingeführt und stellt sicher, dass Firmwareversionen der integrierten Geräte vor Manipulationen geschützt sind. Firmware, die durch UEFI verwaltet wird, lässt sich durch diese Technik erst dann ändern, wenn eine zertifizierte Antivirenlösung geladen ist. Diese neuen Techniken sperren Rootkits und Bootsektorviren wesentlich zuverlässiger aus als in Windows Server 2008 R2.

Im laufenden Betrieb speichert das Betriebssystem seine Daten an zufälligen Orten im Arbeitsspeicher, sodass Angreifer diese nicht auslesen können. Diese Technik trägt die Bezeichnung Address Space Layout Randomization (zufällige Anordnung des Layouts des Adressraums, ASLR) und wurde bereits in Vista eingeführt, aber mit Windows Server 2012 R2 wesentlich erweitert und verbessert.

Fast jeder Teil, den das Betriebssystem im Speicher ablegt, ist in Windows Server 2012 R2 durch ASLR geschützt. Anwendungen, die Windows Server 2012 R2 unterstützen, verwenden zukünftig ähnliche Techniken wie ASLR und lassen sich ebenfalls weniger angreifen. Auch den Kernel in Windows Server 2012 R2 schützt Microsoft jetzt umfassender als in Vorgängerversionen. Prozesse im Benutzermodus können Teile des Kernels nicht mehr verwenden, die in den Vorgängerversionen von Windows Server 2012 R2 besonders vielen Angriffen ausgesetzt waren. Weiterhin führt Windows Server 2012 R2 viele Integritätsprüfungen ein, damit nur installierte und genehmigte Anwendungen auf Hardware und Kernel zugreifen können.

Zusätzlich hat Microsoft auch den Task-Manager in Windows Server 2012 überarbeitet. Dieser bietet wesentlich mehr Informationen als die Vorgängerversionen, was vor allem geübten Anwendern oder Administratoren dabei hilft, Probleme und Sicherheitsgefahren zu finden.

Abbildg. 1.7 Der Task-Manager in Windows Server 2012 R2 bietet mehr Übersicht



Das mit Windows Server 2012 eingeführte Serverfeature *IP Address Management (IPAM)* unterstützt auch virtuelle Umgebungen mit Windows Server 2012 R2 und arbeitet besser mit System Center

2012 R2 zusammen. Außerdem hat Microsoft die Möglichkeit, Netzwerkkarten-Teams zu erstellen, verbessert und die Leistung von NIC-Teams erhöht. Dazu hat Microsoft die Überprüfung des TCP-Datenstroms auf Paketebene optimiert. Fehler werden jetzt erkannt und an andere Teammitglieder können Datenpakete weitergeleitet werden, wenn ein Adapter Probleme beim Datenempfang hat.

Mit dynamischer Zugriffssteuerung Berechtigungen als Metadaten speichern

Die dynamische Zugriffssteuerung (Dynamic Access Control, DAC) in Windows Server 2012 R2 soll Unternehmen dabei helfen, die Berechtigungen von Dateien besser zu verwalten. Allerdings müssen Administratoren beachten, dass die Verwaltung dieser Rechte extrem kompliziert und mit viel Aufwand verbunden ist. Die grundsätzliche Funktionsweise von DAC ist recht einfach.

Die Berechtigungen, die Anwender für ein Dokument haben, sind als Metadaten im Dokument selbst gespeichert. Die Berechtigungen, also Lesen, Schreiben, Drucken und mehr bleiben im Dokument immer gültig, unabhängig davon, ob das Dokument in einen anderen Ordner verschoben wird, als E-Mail verschickt oder in SharePoint gespeichert. Das klingt erst einmal sicherer als das bisherige Modell der dynamischen Zugriffssteuerungslisten (Dynamic Access Control Lists, ACL), die Unternehmen bisher in Windows nutzen. Das bisherige Berechtigungsmodell bleibt auch in Windows Server 2012 R2 erhalten, die dynamische Zugriffskontrolle ergänzt sie nur.

Damit Daten dynamisch gesichert werden können, müssen die einzelnen Dateien erst klassifiziert werden. Das kann in Windows Server 2012 R2 durch die Dateiklassifizierungsdienste automatisch erfolgen. Auch Anwendungen können einzelne Dateien automatisch klassifizieren und Benutzer selbst haben ebenfalls die Möglichkeit, ihre Dokumente zu klassifizieren. Außerdem erben Dateien die Berechtigungstags übergeordneter Ordner.

Auf Basis dieser Tags werden durch die DAC Rechte auf Basis von Richtlinien zugewiesen, die Administratoren erstellen. So lassen sich zum Beispiel Dokumente der Geschäftsleitung entsprechend markieren und automatisch schützen. Die automatische Absicherung übernehmen dann die Active Directory-Rechteverwaltungsdienste (siehe Kapitel 33).

DAC erweitern das Standardrechtemodell um eine zusätzliche Schicht. Haben Anwender auf einen Ordner Schreibrechte, greifen aber über eine Freigabe zu, in der nur Leserechte definiert sind, haben sie effektive Rechte zum Lesen, nicht zum Schreiben. Durch den Einsatz von DAC werden beim Zugriff auf Dateien die festgelegten Rechte also noch einmal erweitert. So lässt sich ein Grundschutz für Dokumente im Netzwerk festlegen.

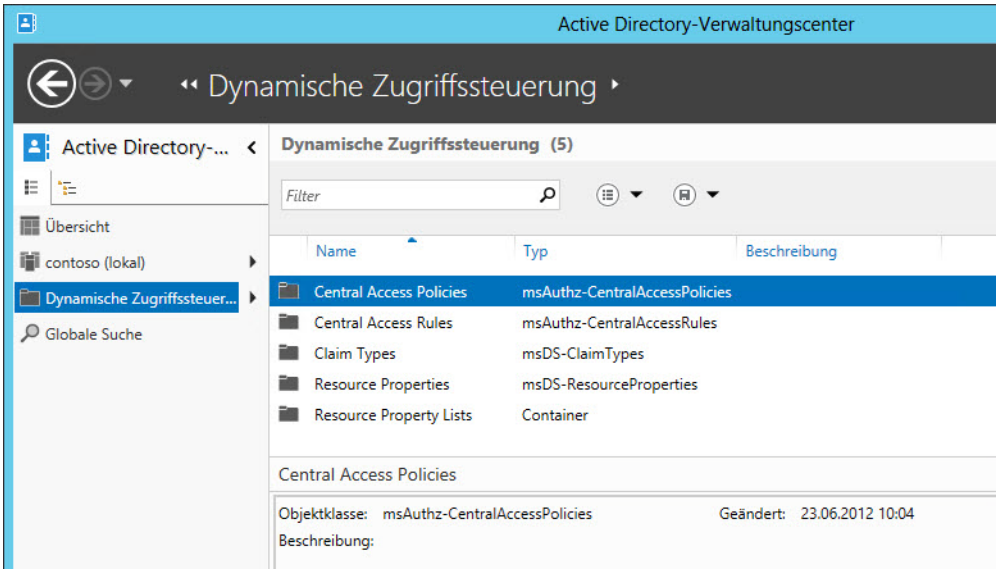
Grundlagen für die Berechtigungssteuerungen sind zentrale Zugriffsrichtlinien (Central Access Policies, CAP). Die Richtlinien steuern, welche Rechte Anwender auf Ressourcen haben, die dieser zentralen Richtlinie zugeordnet sind. Der nächste wichtige Bereich sind die zentralen Zugriffsregeln. Diese steuern, welche Berechtigungen einem bestimmten Satz Ressourcen, also Dateien, Ordner oder Bibliotheken, zugewiesen sind. Während die zentrale Zugriffsrichtlinie also steuert, wer zugreifen darf, steuern zentrale Zugriffsregeln, mit welchen Rechten die Anwender auf die klassifizierten Dateien zugreifen dürfen und welche Ressourcen die Regel verwendet.

Nachdem festgelegt ist, wer auf welche Ressourcen zugreifen darf, legen Administratoren in der zentralen Zugriffsregel fest, mit welchen genauen Rechten der Zugriff erfolgt. Auf diese Weise können Unternehmen eine Grundregel für Berechtigungen für alle Ressourcen in der Gesamtstruktur festlegen.

Damit die zentralen Zugriffsregeln Ressourcen genauer filtern können, um der zentralen Zugriffsrichtlinie die Zuteilung von Benutzern und den Zugriffsregeln das Zuteilen von Rechten zu erlauben, sind Ressourceneigenschaften notwendig. Diese Ressourceneigenschaften fassen bestimmte Dokumente zusammen. Ein weiterer Baustein sind die Claim Types, also die Zuteilung von Attributen.

Dabei handelt es sich um Attribute in Active Directory. Berücksichtigen Unternehmen zum Beispiel das Active Directory-Attribut *department*, lassen sich in der zentralen Zugriffsrichtlinie beispielsweise einzelne Abteilungen wie *Verkauf* abfragen. Allen Anwendern in dieser Abteilung können dann besondere Rechte zugeteilt werden. Unternehmen können aber auch Computerkonten mit einbeziehen und beides kombinieren.

Abbildg. 1.8 Verwalten der dynamischen Zugriffssteuerung in Windows Server 2012 R2



Mit der PowerShell Windows Server 2012 R2 effizient verwalten

Mit Windows 8.1 und Windows Server 2012 R2 stellt Microsoft die neue Version 4.0 der PowerShell zur Verfügung. Diese bietet in den neuen Betriebssystemen deutlich mehr Möglichkeiten und ist einfacher zu bedienen. Jeder Serverdienst in Windows Server 2012 R2 unterstützt jetzt die PowerShell, und auch die neuen Serverversionen von Microsoft wie SQL Server 2012 oder System Center 2012 arbeiten optimal mit der PowerShell zusammen. Die Bedienung ist auch für Anfänger kein Problem mehr.

Mit der neuen Version erweitert Microsoft nicht nur die Möglichkeiten der PowerShell und integriert eine Vielzahl neuer Cmdlets, sondern erleichtert auch die Bedienung. In der neuen PowerShell müssen Administratoren für bestimmte Cmdlets keine Module mehr laden, sondern die PowerShell erkennt selbstständig, wenn ein Modul für ein bestimmtes Cmdlet nicht vorhanden ist und lädt es automatisch nach. Die PowerShell selbst ist in Windows 8 und Windows Server 2012 R2 ohnehin

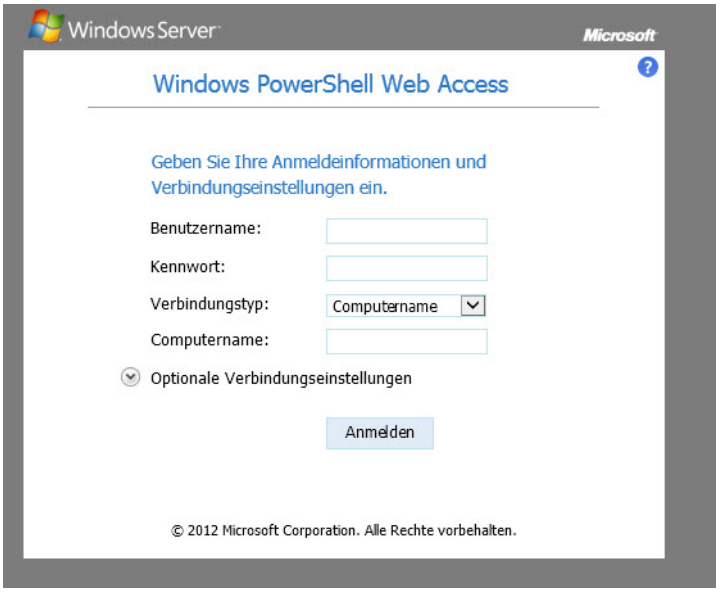
standardmäßig installiert. Auch für Windows 7 und Windows Server 2008 R2 wird Microsoft die neue PowerShell zur Verfügung stellen. Bei diesen Betriebssystemen ist auch eine parallele Installation zur PowerShell 2.0 möglich, um die Kompatibilität mit Skripts sicherzustellen.

Wer sich in die PowerShell einarbeiten will, findet bei Microsoft einen mehrteiligen Onlinelernkurs (*http://www.microsoft.com/germany/msdn/aktuell/news/show.mspx?id=msdn_de_46012* [Ms179-K01-01]) zur PowerShell 3.0. Wer sich mit dem Power Shell Web Access beschäftigen will, findet weiterführende Informationen in Microsoft TechNet (*http://technet.microsoft.com/de-DE/library/hh831611.aspx* [Ms179-K01-02]).

Mit dem Cmdlet *Show-Command* erhalten Administratoren eine umfassende Hilfe zu einzelnen Cmdlets. Verfügt der Server über eine Internetverbindung, lassen sich die Hilfedateien in der PowerShell mit *Update-Help* aktualisieren.

Installieren Sie das Feature *PowerShell Web Access* über den Server-Manager oder der PowerShell, kann auf diese auch über einen Webbrowser zugegriffen werden. So können Verwaltungsaufgaben auf einem Server auch von Tablet-PCs oder nicht kompatiblen Systemen durchgeführt werden. Der Zugriff erfolgt nach der Authentifizierung. In Kapitel 40 gehen wir ausführlich auf dieses Thema ein.

Abbildg. 1.9 Verwenden von PowerShell Web Access



Nach der Installation des Power Shell Web Access-Features und des Zertifikats können Administratoren mit allen aktuellen Browsern eine Verbindung zur PowerShell über das Netzwerk aufbauen. Die URL dazu lautet *https://<Servername>/pswa*.

Die PowerShell ermöglicht zusätzlich Remotesitzungen auf Servern im Netzwerk. In der neuen Version können Sie auch von öffentlichen Netzwerken aus zugreifen. Dazu ist die Option *SkipNetworkProfileCheck* in die Cmdlets *Enable-PSRemoting* und *Set-WSManQuickConfig* integriert. Die Option erstellt automatisch Firewallregeln, die den Zugriff erlauben.

Um eine Remotesitzung aufzubauen, verwenden Sie das Cmdlet *New-PSSession*. Mit *Enter-PSSession <Servername>* bauen Sie eine Verbindung auf. Mit *Exit-Session* beenden Sie diese Sitzung wieder. Neu ist die Möglichkeit, Sitzungen zu unterbrechen und neu aufzubauen. Bei unterbrochenen Sitzungen laufen die Cmdlets weiter, auch wenn sich Administratoren vom Server getrennt haben. Dazu setzen Sie die neuen Cmdlets *Disconnect-PSSession*, *Connect-PSSession* und *Receive-PSSession* ein.

Hyper-V in Windows Server 2012 R2

Mit Windows Server 2012 R2 liefert Microsoft auch eine neue Version seiner Visualisierungstechnologie Hyper-V (siehe Kapitel 7, 8 und 9) aus. Diese weist in der neuen Version eine Vielzahl von Neuerungen auf, auch im direkten Vergleich zu Windows Server 2012. Da die Technologie zum Lieferumfang gehört, können Unternehmen Hyper-V ohne Zusatzkosten nutzen. Außerdem bietet Microsoft noch Hyper-V Server 2012 R2 als kostenlosen Virtualisierungsserver an.

Generelle Neuerungen in Hyper-V seit Windows Server 2012

Die neuen Funktionen in Windows Server 2012 sind auch in Windows Server 2012 R2 weiterhin verfügbar. Wir zeigen Ihnen nachfolgend die Neuerungen im Bereich Hyper-V im Vergleich von Windows Server 2008 R2 SP1 zu Windows Server 2012.

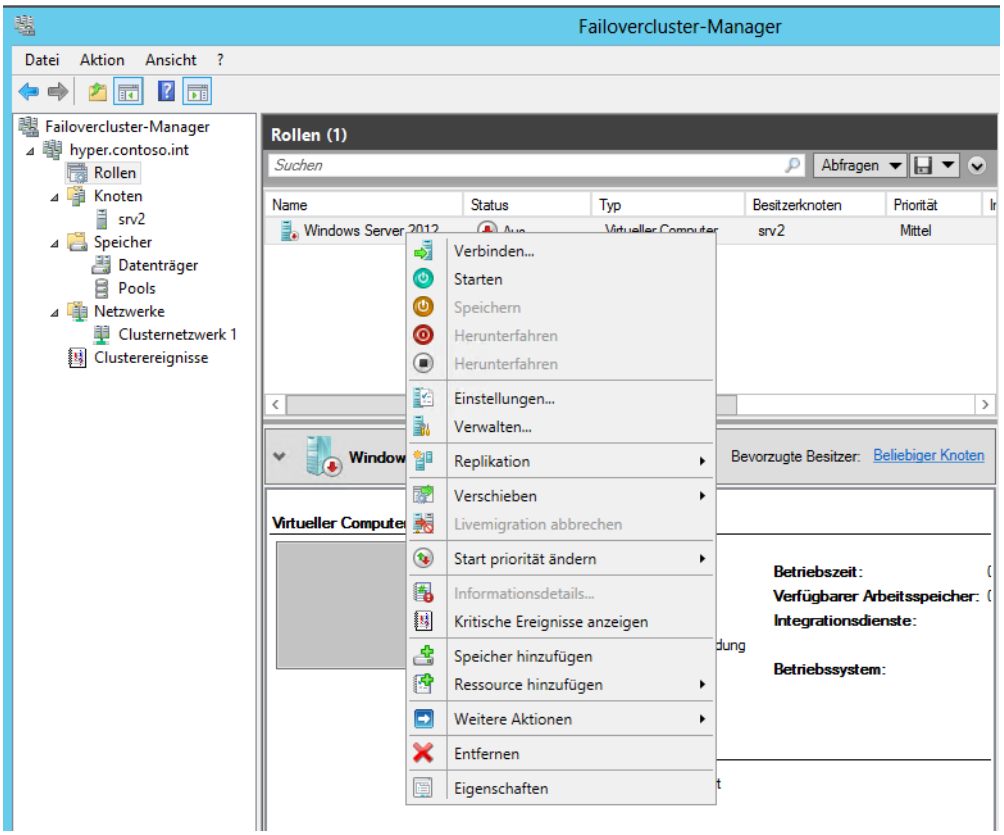
Hyper-V Hosts können 4 TB Hauptspeicher nutzen und 320 CPUs verwalten. Virtuelle Maschinen verwalten in Windows Server 2012/2012 R2 bis zu 1 TB Arbeitsspeicher. Virtuelle Festplatten auf Basis der neuen VHDX-Dateien lassen sich mit Größen von bis zu 64 TB betreiben. In den Kapitel 7, 8 und 9.

Virtuelle Maschinen lassen sich in Hyper-V-Clustern priorisieren, und mit der Livemigration lassen sich im laufenden Betrieb mehrere Server gleichzeitig zwischen Clusterknoten verschieben. Fällt ein Knoten aus, verschiebt Hyper-V die virtuellen Maschinen mit der höchsten Priorität zuerst. Das sind nur einige der von Hyper-V unterstützten Neuerungen seit Windows Server 2008 R2 SP1.

Erstellen Sie Momentaufnahmen (Snapshots) und löschen diese, schreibt Windows Server 2008 R2 die notwendigen Daten erst beim nächsten Neustart auf die übergeordnete Festplatte. Windows Server 2012/2012 R2 kann diesen Vorgang online durchführen. Das heißt, der Server schreibt Daten aus den Momentaufnahmen sofort beim Löschen auf die Festplatte (siehe Kapitel 8).

Mit Hyper-V Replica lassen sich in Windows Server 2012/2012 R2 virtuelle Festplatten und ganze Server asynchron zwischen verschiedenen Hyper-V-Hosts im Netzwerk replizieren und synchronisieren. Die Replikation findet über das Dateisystem statt, ein Cluster ist nicht notwendig. Die Replikationen lassen sich manuell, automatisiert oder nach einem Zeitplan ausführen. Auf diesem Weg lassen sich virtuelle Server auch hochverfügbar betreiben, ohne teure Cluster nutzen zu müssen. Die Einrichtung nehmen Sie über einen Assistenten im Hyper-V-Manager vor.

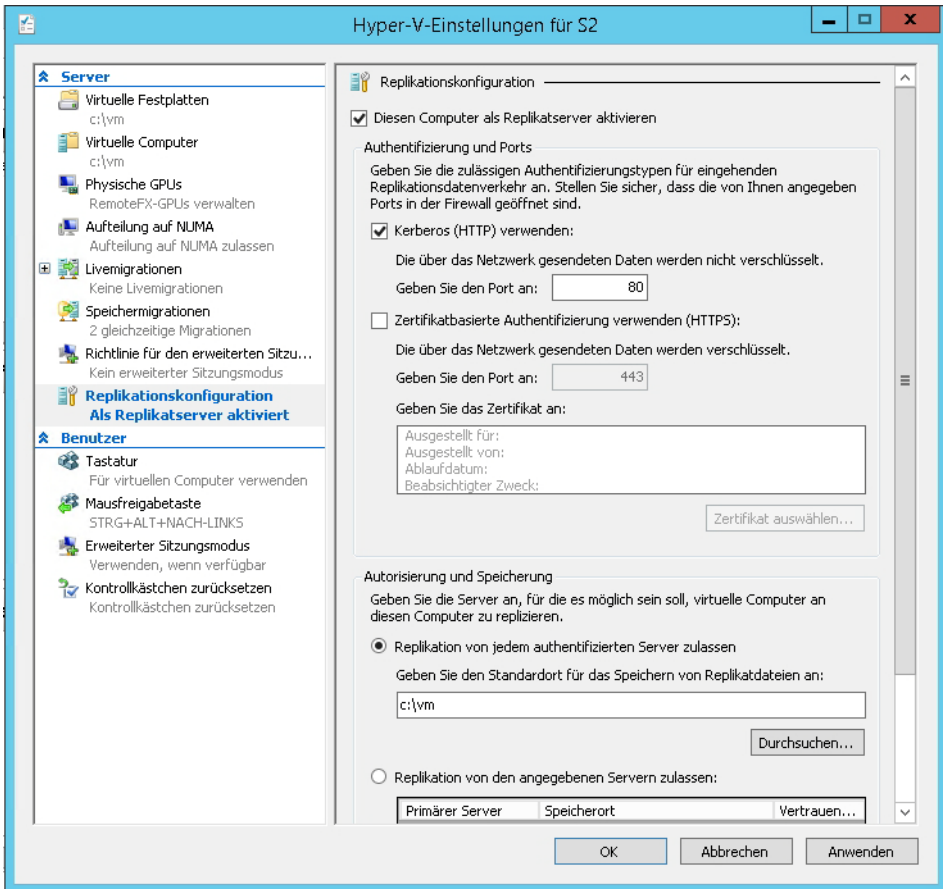
Abbildg. 1.10 Virtuelle Server lassen sich in Windows Server 2012/2012 R2 besser clustern



Auf diese Weise können Sie aber auch Testumgebungen mit produktiven Daten aufbauen oder für eine Hochverfügbarkeitslösung sorgen, indem Sie Server replizieren lassen. Die Computer müssen dabei nicht in einem Cluster konfiguriert sein. Es reicht aus, wenn auf dem Hyper-V-Host Windows Server 2012 R2 und Hyper-V installiert ist. Die entsprechende Replikation steuern Sie über einen Assistenten, den Sie über das Kontextmenü von virtuellen Servern im Hyper-V-Manager starten.

Starten Sie den Assistenten und geben Sie zunächst den Replikatserver an, also den Hyper-V-Host, auf den Sie die virtuelle Maschine replizieren wollen. Damit ein Hyper-V-Host überhaupt für Replikate zur Verfügung steht, müssen Sie diesen zunächst auf dem Server in den Hyper-V-Einstellungen im Bereich *Replikationskonfiguration* aktivieren.

Abbildg. 1.11 Konfigurieren der Hyper-V-Replikation für einen virtuellen Server

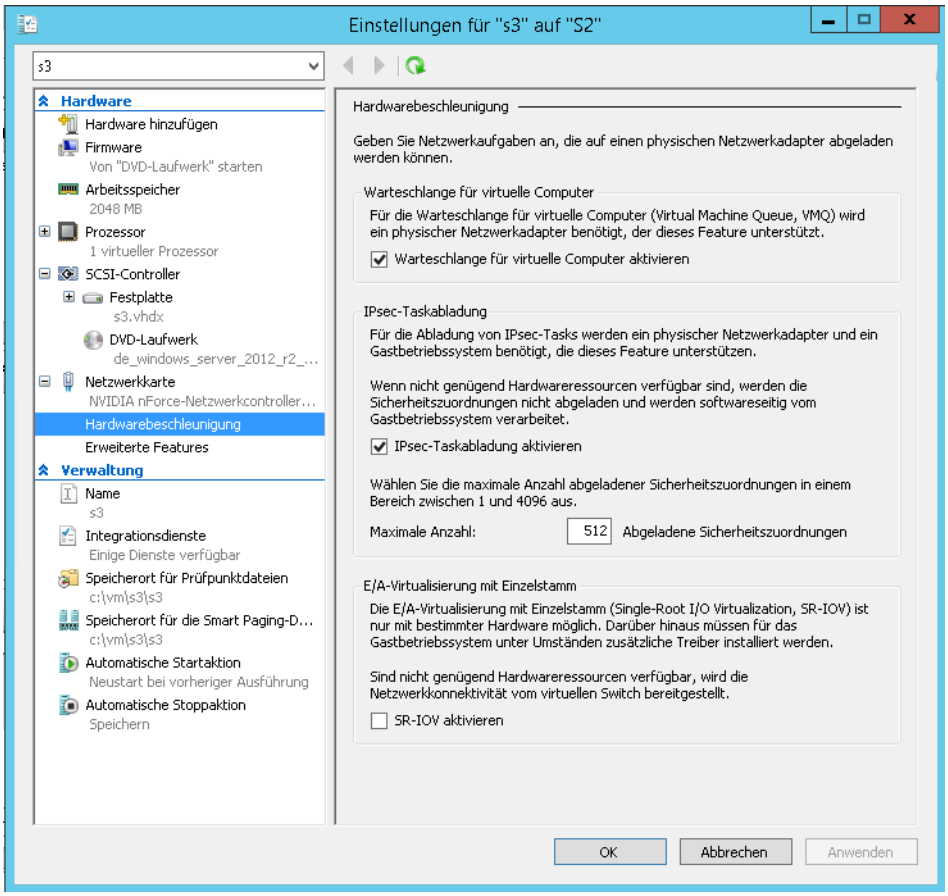


Schnelle und sichere Netzwerke

Virtuelle Server in Hyper-V haben mehr Möglichkeiten, direkt auf Netzwerkkarten in Hyper-V-Hosts zuzugreifen. Auf diesem Weg lassen sich auch netzwerklastige Server besser virtualisieren, indem Administratoren direkt physische Netzwerkkarten zuweisen. Die Steuerung der Netzwerkbandbreite von virtuellen Servern lässt sich in der neuen Version ebenfalls steuern.

Virtuelle Switches agieren als Layer 2-Netzwerkswitches und erlauben auch die Einbindung von Network Device Interface Specification (NDIS)-Filter und der Windows Filtering Platform-Treibern. Auf diese Weise lassen sich auch Plug-Ins von Drittherstellern in Hyper-V einbinden, die erweiterte Netzwerk- und Sicherheitseinstellungen für virtuelle Server erlauben. Die entsprechenden Einstellungen sind über den Menübefehl *Erweiterungen* für jeden einzelnen vSwitch zu finden.

Abbildg. 1.12 Erweiterte Funktionen von Netzwerkkarten in Windows Server 2012 R2

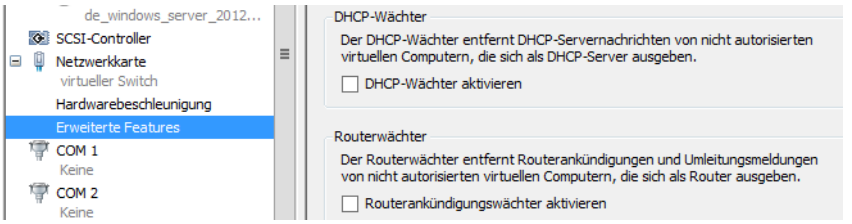


Interessant sind unterhalb der Einstellungen für die Netzwerkkarten noch die beiden Bereiche *Hardwarebeschleunigung* und *Erweiterte Features*. Bei *Hardwarebeschleunigung* können Sie den virtuellen Servern erlauben, bestimmte Berechnungen direkt an die physische Netzwerkkarte weiterzugeben. Beim Kauf der Hostsysteme sollten daher Unternehmen darauf achten, ausreichend Netzwerkkarten im Server zu verbauen und sicherzustellen, dass die Karten die neuen Funktionen in Hyper-V unterstützen.

Im unteren Bereich lassen sich noch Berechnungen für IPsec vom Prozessor des virtuellen Servers auf die physische Netzwerkkarte auslagern. Dadurch beschleunigt sich die Systemleistung des Servers und die Netzwerkgeschwindigkeit enorm. Eine weitere Einstellung ist *E/A-Virtualisierung mit Einzelstamm*. Hierbei handelt es sich ebenfalls um physische Funktionen von Netzwerkkarten die jetzt auch Hyper-V funktioniert. Netzwerkkarten, die diese Funktion unterstützen, stellen für virtualisierte Umgebungen implementierte E/A-Kanäle zur Verfügung, mit denen sich die Karte gegenüber virtualisierten Servern wie mehrere Netzwerkkarten verhält. SR-IOV (Single-Root I/O Virtualization) ist vor allem bei E/A-intensiven Anwendungen interessant, also durchaus auch für SQL Server 2012.

Unter *Erweiterte Features* finden Sie die beiden neuen Einstellungen *DHCP-Wächter* und *Routerwächter*. Die Einstellungen sollen verhindern, dass virtuelle Server unkontrolliert als DHCP-Server oder als Router zu agieren.

Abbildg. 1.13 DHCP- und Routerwächter in Windows Server 2012 R2



Bessere Hochverfügbarkeit

Windows Server 2008 R2 SP1 erlaubt zwar bereits die Livemigration, aber immer nur von einem Server gleichzeitig. Bei der Livemigration in einem Cluster überträgt Hyper-V den virtuellen Server mitsamt Inhalt des Arbeitsspeichers auf einen anderen Knoten im Cluster. Dies hat den Vorteil, dass die Server immer verfügbar sind, auch bei einer Übertragung. Windows Server 2008 R2 kann aber immer nur einen Server gleichzeitig übertragen, was in vielen Fällen nicht sehr effizient ist. Denn gerade in größeren Umgebungen kommen Cluster zum Einsatz. Und Cluster hosten normalerweise viele virtuelle Server.

Windows Server 2012 R2 kann mehrere Livemigrationen gleichzeitig durchführen. Die Einstellungen dazu finden Sie in den Hyper-V-Einstellungen des Hyper-V-Hosts im Bereich *Livemigrationen* (siehe Kapitel 9).

Es ist mit Windows Server 2012 R2 möglich, die Livemigration auch auf Hyper-V-Hosts ohne Cluster zu nutzen, oder virtuelle Maschinen zwischen Hyper-V-Hosts zu replizieren, ohne diese clustern zu müssen. Mit dem Hyper-V-Server 2012 bietet Microsoft die Hyper-Funktionen der Datacenter-Edition von Windows Server 2012 R2 vollkommen kostenlos. Mit dieser Variante von Windows Server 2012 R2 können Sie auch Cluster installieren. Cluster lassen sich jetzt auch in der Standard-Edition erstellen.

Mit Windows Server 2012 R2 ändert Microsoft zunächst den Funktionsumfang der verschiedenen Editionen. Für Unternehmen spielen vor allem die Editionen Standard und Datacenter von Windows Server 2012 R2 eine Rolle, eine Enterprise-Edition gibt es nicht mehr. Die beiden Editionen verfügen über exakt den gleichen Funktionsumfang. Es lassen sich also auch mit der Standard-Edition Cluster für Hyper-V betreiben. Die Editionen Standard und Datacenter unterscheiden sich in Windows Server 2012 R2 lediglich in der Lizenzierung.

Auf Servern mit Windows Server 2012 R2 Standard dürfen Unternehmen zwei virtuelle Server pro Lizenz installieren. Sollen auf einem Hyper-V-Host mehr virtuelle Server im Einsatz sein, sind mehrere Lizenzen für die Standard-Edition notwendig, oder eben eine Datacenter-Lizenz. Die Datacenter-Edition erlaubt den Betrieb unbegrenzt vieler virtueller Server auf einem Host. Beide Editionen decken außerdem immer nur zwei Prozessoren des Hosts ab. Die erforderliche Mindestanzahl von Betriebssystemlizenzen für jeden Server wird durch die Anzahl der physischen Prozessoren des Hosts bestimmt, sowie die Anzahl an virtueller Server, die Sie auf dem Hyper-V-Host installieren.

Außerdem stellt Microsoft noch den Hyper-V Server 2012 R2 zur Verfügung, der über die gleichen Funktionen im Bereich Hyper-V verfügt, wie die Editionen Standard und Datacenter. Diesen Server müssen Unternehmen nicht lizenzieren, er steht kostenlos zur Verfügung. Die Installation entspricht einer Core-Installation ohne grafische Oberfläche von Windows Server 2012 R2. Die Verwaltung erfolgt über grafische Verwaltungsprogramme von anderen Server, einer Arbeitsstation mit Windows 8 bzw. Windows 8.1 oder System Center Virtual Machine Manager 2012 R2. Mit diesen drei Editionen können Unternehmen die drei wichtigsten Hochverfügbarkeitsfunktionen in Windows Server 2012 R2 nutzen. Diese stellen wir nachfolgend vor.

Mit Hyper-V Replica lassen sich virtuelle Server zwischen Hyper-V-Hosts replizieren, ohne dass diese Bestandteil eines Clusters sein müssen. Der virtuelle Server wird vom Quellserver auf den Zielserver repliziert, also kopiert. Ab Windows Server 2012 R2 können Sie die Daten noch zu einem dritten Server replizieren, doch dazu später mehr. Dieser Vorgang kann ad hoc erfolgen oder über einen Zeitplan. Aktiv bleibt immer der virtuelle Server auf dem Quellserver, der virtuelle Server auf dem Zielserver bleibt ausgeschaltet. Administratoren können ein Failover des virtuellen Servers manuell durchführen oder den virtuellen Server jederzeit erneut vom Quell- auf den Zielserver replizieren.

Mit der Livemigration ohne Cluster können Administratoren virtuelle Server im laufenden Betrieb vom Quell- auf den Zielserver verschieben und online schalten. Es ist kein Cluster und kein gemeinsamer Datenträger notwendig. Neu seit Windows Server 2012 in diesem Bereich ist auch die Möglichkeit, mehrere Livemigrationen gleichzeitig durchzuführen. Im Gegensatz zur Replikation ist der virtuelle Server weiterhin nur auf einem Server verfügbar und kann im laufenden Betrieb verschoben werden.

Weiterhin gibt es in Windows Server 2012/2012 R2 die Möglichkeit, Hyper-V in einem Cluster zu betreiben und virtuelle Server als Clusterressourcen zu definieren. Hier sind die virtuellen Server schnell und einfach zwischen den Knoten verschiebbar. Einen solchen Cluster können Unternehmen jetzt auch mit der Standard-Edition aufbauen. In Windows Server 2012/2012 R2 lassen sich mehrere Livemigrationen gleichzeitig durchführen und virtuelle Server lassen sich auch priorisieren. Alle diese Funktionen stehen über Hyper-V Server 2012 R2 auch kostenlos zur Verfügung.

Mit Microsoft Hyper-V Server 2012 R2 virtualisieren

Mit dem neuen Hyper-V Server 2012 R2 bietet Microsoft eine kostenlose Virtualisierungslösung, die alle Hyper-V-Funktionen der kostenpflichtigen Editionen von Windows Server 2012 R2 bietet. Mit dem Server können Unternehmen daher vollkommen kostenlos alle Vorteile und Neuerungen von Hyper-V in Windows Server 2012/2012 R2 für virtuelle Server nutzen. Die Installation und der Betrieb ist einfach. Der Server lässt sich auch als Testumgebung nutzen und sogar mit System Center Virtual Machine Manager (SCVMM) verwalten. Die Verwaltung entspricht exakt den Vorgehensweisen in den anderen Editionen von Windows Server 2012 R2. Mehr zum Thema lesen Sie in Kapitel 7.

In der neuen Version beherrscht der Server alle Funktionen, die auch Hyper-V in Windows Server 2012/2012 R2 Standard/Datacenter beherrscht. Dazu gehört die Replikation von virtuellen Servern zwischen Hyper-V-Hosts, die Livemigration von Servern mit und ohne Cluster, das Onlinezusammenführen von Momentaufnahmen und die neuen Netzwerkfunktionen. Auch die neuen VHDX-Festplatten mit einer maximalen Größe von 64 TB und der verbesserte Zugriff auf NAS-Server sowie

das neue SMB 3-Protokoll sind Bestandteil. Hyper-V Server 2012 R2 entspricht der Core-Installation von Windows Server 2012 R2 und lässt sich von einer grafischen Oberfläche aus über das Netzwerk verwalten.

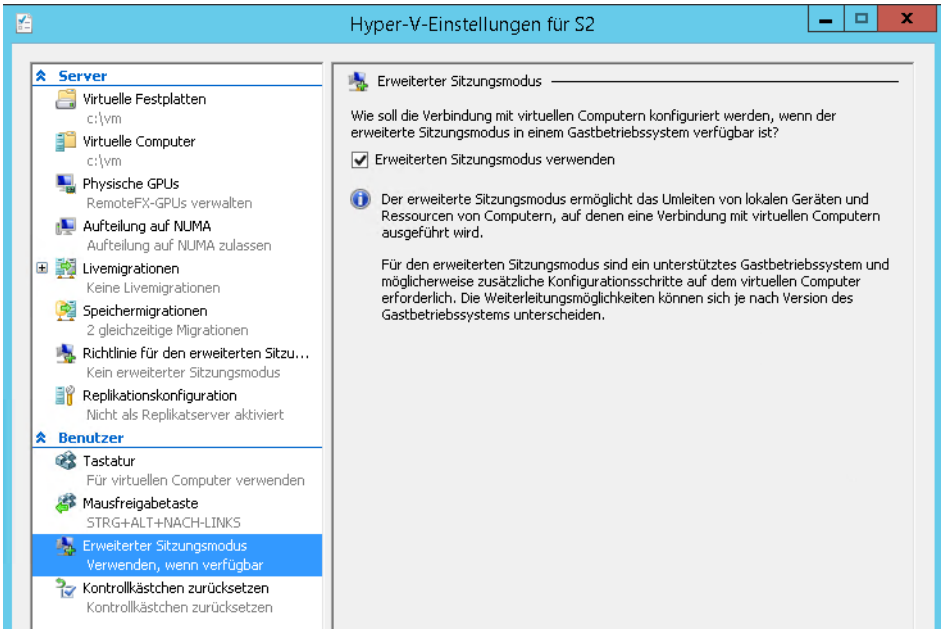
Die Installation entspricht in etwa der von Windows Server 2012 R2, die erste Einrichtung erfolgt über eine textbasierte grafische Oberfläche (Sconfig). Der Server lässt sich als alleinstehender Server betreiben, aber auch in Active Directory-Domänen. Da in Windows 8 bzw. Windows 8.1 Pro/Enterprise standardmäßig die Verwaltungswerkzeuge von Hyper-V verfügbar sind, lässt sich Hyper-V Server 2012/2012 R2 auch von Windows 8- bzw. Windows 8.1-Arbeitsstationen aus verwalten. Zusatzwerkzeuge sind dazu nicht notwendig.

Hyper-V Server 2012/2012 R2 kann natürlich nicht nur Windows Server 2012/2012 R2 virtualisieren, sondern auch Windows Server 2008 R2 und älter sowie Linux und UNIX. Das heißt, Unternehmen können weiterhin produktiv ihre herkömmlichen Server einsetzen, aber die neuen Vorteile von Windows Server 2012 R2 effizient nutzen, und das vollkommen kostenlos.

Hyper-V-Neuerungen in Windows Server 2012 R2 – Shared VHDX und mehr

Die wichtigsten und meisten Neuerungen von Windows Server 2012 R2 im Vergleich zu Windows Server 2012 hat Microsoft in Hyper-V vorgenommen. Vor allem den Zugriff auf virtuelle Server auf Basis von RDP hat Microsoft verbessert, sodass VM Connect jetzt wesentlich effizienter funktioniert.

Abbildg. 1.14 Mit dem erweiterten Sitzungsmodus lassen sich in Windows Server 2012 R2 virtuelle Computer besser verwalten



Die RDP-Sitzungen laufen in Windows Server 2012 R2 über den Host, eine direkte RDP-Verbindung zum virtuellen Server ist nicht mehr notwendig, um zum Beispiel die Zwischenablage zu nutzen. Sie können virtuelle Server automatisiert schneller und effizienter aktivieren. Viele Administratoren wird erfreuen, dass sich über VM Connect jetzt auch Dateien per Drag&Drop kopieren und verschieben lassen.

In der neuen Version können Sie die virtuellen Festplatten (VHDX) im laufenden Betrieb vergrößern und verkleinern. Virtuelle Server können sich in Windows Server 2012 R2 eine virtuelle Festplatte teilen (Shared VHDX). Das hat vor allem den Vorteil bei Festplatten, auf denen Daten gespeichert sind, oder bei Clustern auf Basis virtueller Server.

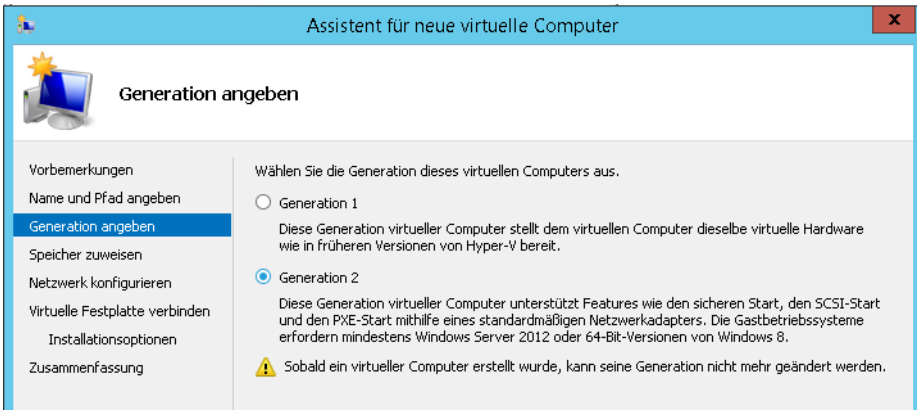
Die Livemigration, das Verschieben von virtuellen Servern zwischen Hyper-V-Hosts im laufenden Betrieb, hat Microsoft deutlich beschleunigt. Die Daten werden bei der Datenübertragung in der neuen Version effizient komprimiert. Die Livemigration ist jetzt auch für 10 Gigabit/s-Netzwerke optimiert und kann in sehr schnellen Netzwerken mit Remote Direct Memory Access (RDMA) sehr schnell die Inhalte des Arbeitsspeichers zwischen den Hosts verschieben. Die neue Livemigration ist vollständig kompatibel zu Windows Server 2012, sodass sich virtuelle Server zwischen Hosts mit Windows Server 2012 und Windows Server 2012 R2 verschieben lassen.

Virtuelle Server lassen sich jetzt im laufenden Betrieb importieren und kopieren. Dabei berücksichtigt Windows Server 2012 R2 auch Snapshots (Momentaufnahmen). Sie müssen vor dem Export also virtuelle Server nicht mehr herunterfahren und Snapshots löschen.

Außerdem unterstützen jetzt virtuelle Maschinen auch den neuen BIOS-Standard UEFI sowie die integrierte Funktion Secure Boot. Bisher war das nur dem Host vorbehalten. Administratoren können jetzt auch den Datendurchsatz für virtuelle Server steuern. Dazu wurde die neue Funktion Storage Quality of Service in Windows Server 2012 R2 integriert.

Damit Sie die neuen Funktionen für virtuelle Server, von Microsoft auch Generation 2 genannt, nutzen können, müssen Sie im Assistenten zum Erstellen virtueller Server die neue Generation auswählen. Microsoft hat dazu im Assistenten virtueller Server neue Seiten integriert. Die Konfiguration der Generation lässt sich nachträglich nicht mehr ändern. Außerdem können Sie alte virtuelle Maschinen nicht zu Generation 2-VMs migrieren. Als Generation 2-VMs können Sie nur Windows Server 2012, Windows Server 2012 R2, Windows 8 x64 und Windows 8.1 x64 verwenden. Virtuelle Maschinen auf Basis von Generation 2 nutzen aus Leistungsgründen keine emulierte Hardware mehr.

Abbildg. 1.15 In Windows Server 2012 R2 gibt es eine neue Generation virtueller Computer



Bereits mit Windows Server 2012 hat Microsoft eine Datendeduplizierung integriert, mit dem Sie Speicherverschwendung wegen doppelter Dateien entgegenwirken können. In Windows Server 2012 R2 haben Sie zusätzlich die Möglichkeit, diese Funktion auf virtuelle Festplatten auszudehnen. Das ist beim Einsatz virtueller Desktops sehr sinnvoll.

Die Replikation von virtuellen Servern (Hyper-V-Replica) ist in Windows Server 2012 R2 wesentlich flexibler und erlaubt jetzt auch die Replikation auf einen dritten Host. Windows Server 2012 beherrscht hier nur zwei Hosts. Ebenfalls verbessert hat Microsoft die Unterstützung für Linux als virtuelle Server. Sie können jetzt Dynamic Memory auch in Linux-Clients nutzen.

Verbessertes Active Directory

Ab Windows Server 2012 bietet Microsoft zahlreiche Verbesserungen im Bereich Active Directory und ermöglicht auch eine bessere und leichtere Verwaltung. Diese sind auch in Windows Server 2012 R2 eingeflossen.

Ein wichtiger Vorteil ist, dass sich Domänencontroller leichter virtualisieren lassen. Das Erstellen von Momentaufnahmen (Snapshots) für Domänencontroller stellt in Windows Server 2012 R2 kein Problem mehr dar. Allerdings empfiehlt Microsoft, zur Virtualisierung von Domänencontrollern auf Hyper-V in Windows Server 2012 R2 zu setzen. Die neue Version unterstützt virtuelle Domänencontroller standardmäßig. In den Kapiteln 10 bis 19 gehen wir ausführlich auf die Funktionen in Active Directory ein.

Virtualisierung und effizientere Installation von Active Directory

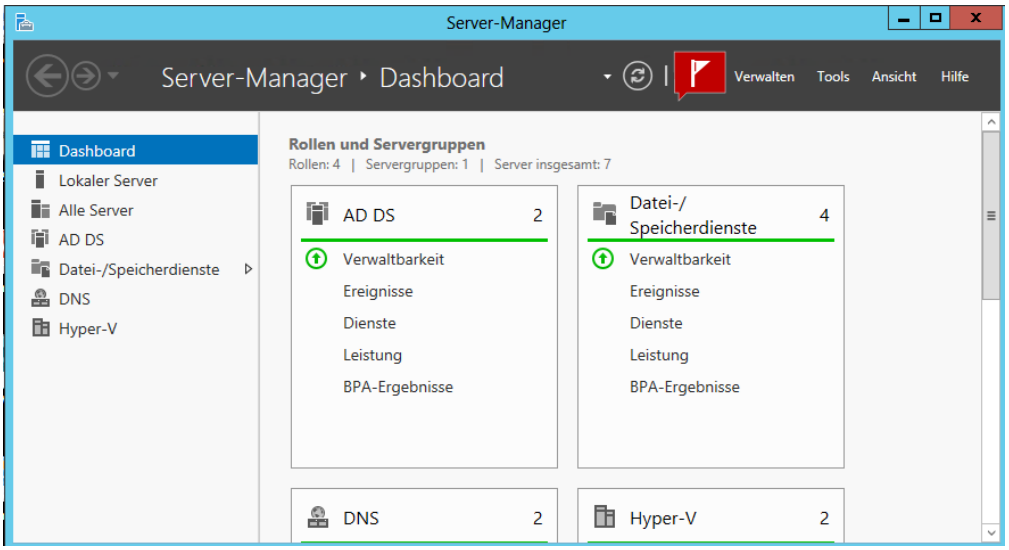
Um einen virtuellen Domänencontroller zu klonen, sind keine Spezialwerkzeuge notwendig, sondern Administratoren kopieren einfach die virtuelle Maschine und weisen dem Klon einen neuen Namen zu. Auf Basis der Generation-ID in Windows Server 2012 R2 und deren Unterstützung in Hyper-V erkennt der neue Server Active Directory und bindet sich problemlos ein.

Die verwalteten Dienstkonten (Managed Service Accounts), welche Kennwörter für Dienste selbst verwalten, lassen sich in Windows Server 2012 R2 auf mehreren Servern einsetzen. DHCP-Server können ohne einen Cluster zu Teams zusammengefasst werden. Die Eingabeaufforderung gibt es auch in Windows Server 2012 R2 weiterhin. Zusätzlich enthält der Server, aber auch Windows 8- bzw. Windows 8.1-Clients, die neue PowerShell-Version 4.0. Diese lässt sich ebenfalls wesentlich leichter bedienen als in Windows Server 2008 R2.

Mit der dynamischen Zugriffskontrolle (Dynamic Access Control, DAC) können Administratoren einfacher die Berechtigungen für den Zugriff auf Dateien, Ordner und sogar SharePoint-Bibliotheken steuern. Dazu lassen sich Dateien mit Metadaten versorgen, die nur bestimmten Anwendern, zum Beispiel allen Anwendern einer Abteilung oder der Geschäftsführung, den Zugriff erlauben, unabhängig in welchem Ordner oder welcher Freigabe die Daten gespeichert sind. Das Ganze funktioniert lückenlos auch beim Verschieben von Dateien in SharePoint-Bibliotheken. Zusätzlich lässt sich über diesen Weg auch festlegen, von welchen Geräten aus Anwender auf die Daten zugreifen dürfen. Unsichere PCs, Heimarbeitsplätze, Computer in Internet-Cafes oder Smartphones lassen sich über diesen Weg aussperren. Die Funktion nutzt dazu die Active Directory-Rechteverwaltung.

Domänencontroller lassen sich einfacher installieren und verwalten. Außerdem hat Microsoft im neuen Server-Manager Servergruppen implementiert. Dadurch können Administratoren bereits mit Bordmitteln zentral alle Server im Netzwerk verwalten. Serverrollen und Features lassen sich über den Server-Manager auch über das Netzwerk installieren. Den Installations-Assistent für Active Directory hat Microsoft überarbeitet. Der Einrichtungs-Assistent (Dcpromo) ist ab Windows Server 2012 nicht mehr vorhanden.

Abbildg. 1.16 Gruppierte Server im Server-Manager

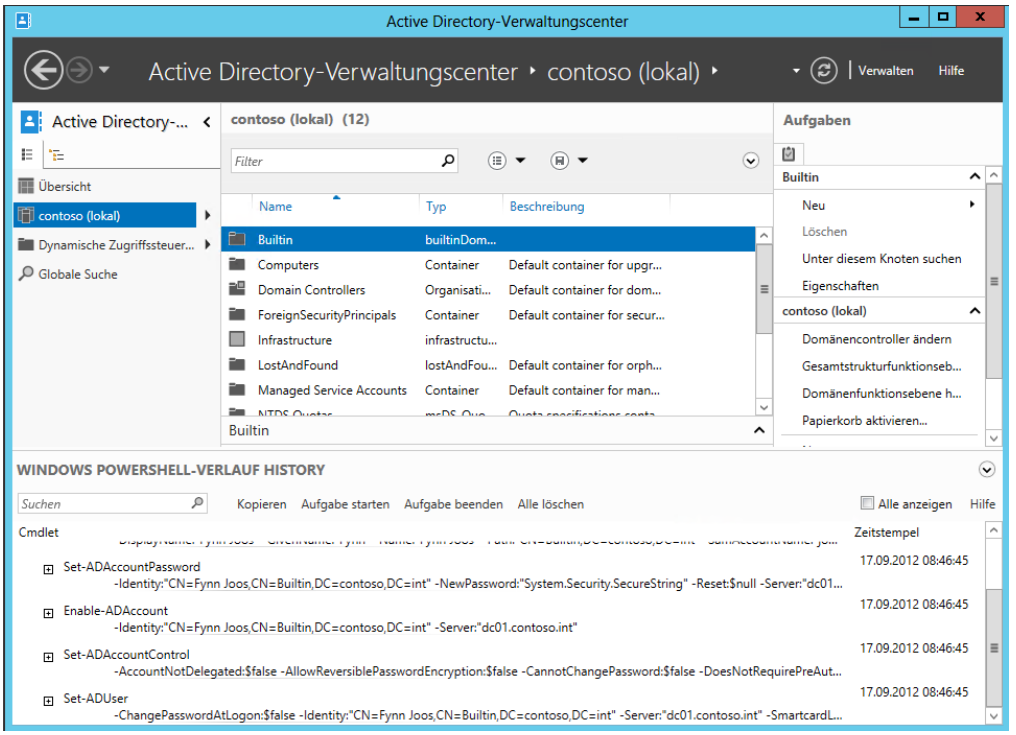


Der Assistent zur Installation von Active Directory zeigt in der neuen Version wesentlich weniger Fenster und nimmt Administratoren einige Entscheidungen ab. Das soll auch unerfahrenen Administratoren dabei helfen, Active Directory zu installieren. Erfahrene Administratoren können aber auch die PowerShell verwenden, um alle Optionen zu steuern.

Dazu steht das Modul zur Active Directory-Verwaltung zur Verfügung, welches Sie mit *Import-Module ADDSDeployment* laden. Mit dem Cmdlet *Install-ADDSDomainController* installieren Sie einen neuen Domänencontroller. Weitere Cmdlets zur Erstellung von Domänen oder Gesamtstrukturen sind *Install-ADDSDomain* und *Install-ADDSForest*.

Das Active Directory-Verwaltungscenter von Windows Server 2008 R2 hat Microsoft in Windows Server 2012 komplett überarbeitet. Die neue Version erlaubt zum Beispiel die Aktivierung und Verwendung des Papierkorbs von Active Directory und weitere Aufgaben, die in Windows Server 2008 R2 über die PowerShell durchgeführt werden mussten. Auch die Gruppenrichtlinien für Kennwörter lassen sich in der neuen Konsole konfigurieren und Organisationseinheiten zuordnen. Neu im Active Directory-Verwaltungscenter ist im unteren Fensterbereich der Abschnitt *Windows PowerShell-Verlauf History*. Dieser listet in Form eines Protokolls PowerShell-Befehle auf. Dazu müssen Administratoren nur auf den Link klicken und sehen alle durchgeführten Aufgabe der grafischen Oberfläche als Befehl für die PowerShell. Dieses Fenster gilt aber nicht nur als reines Protokoll, sondern Administratoren können Befehle für Skripts aus dem Fenster heraus kopieren.

Abbildg. 1.17 Das Active Directory-Verwaltungscenter in Windows Server 2012 R2



Um Active Directory zu installieren, wählen Administratoren die Serverrolle *Active Directory Domain Services* aus. Nach der Installation der notwendigen Systemdateien lässt sich der Einrichtungs-Assistent über einen Link im letzten Fenster starten. Im Assistenten nehmen Sie ähnliche Eingaben vor wie in Windows Server 2008 R2, allerdings erscheinen weniger Fenster und der Assistent konfiguriert wichtige Einstellungen automatisch im Hintergrund. Im letzten Fenster erhalten Sie eine Zusammenfassung angezeigt und können Active Directory installieren. Der Installations-Assistent zur Integration von Active Directory in Windows Server 2012 R2 wurde von Microsoft grundlegend überarbeitet. Er zeigt weniger Auswahlfenster und erlaubt eine schnellere Installation.

Microsoft möchte das mit Windows Server 2008 R2 eingeführte Active Directory-Verwaltungscenter mehr in die tägliche Routine von Administratoren einbinden. Mit der Verwaltungsoberfläche bietet Microsoft eine zentrale Anlaufstelle für alle Routineaufgaben in Active Directory in einer einzelnen Oberfläche. Der Aufbau der Konsole ist stark aufgabenorientiert. Im Gegensatz zu den anderen Verwaltungstools basieren die Aufgaben im Verwaltungscenter auf Befehle aus der PowerShell.

Die Standard-Verwaltungskonsolen für Active Directory, zum Beispiel das Snap-In *Active Directory-Benutzer und -Computer*, sind immer noch verfügbar. Hier haben sich im Vergleich zu Windows Server 2008 R2 keine großartigen Änderungen ergeben. Das gilt auch für die Snap-Ins *Active Directory-Standorte und -Dienste* und *Active Directory-Domänen und Vertrauensstellungen*.

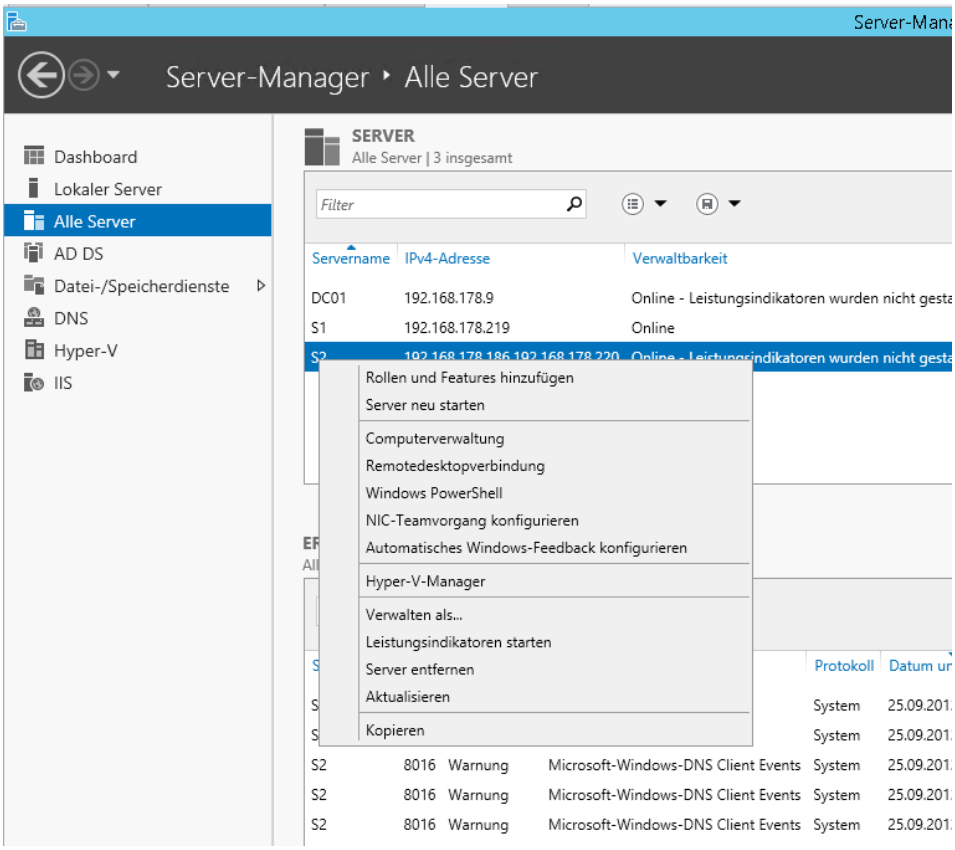
Das Active Directory-Verwaltungscenter bietet nicht alle Möglichkeiten der anderen erwähnten Snap-Ins, sondern dient vor allem der Abarbeitung von Routineaufgaben wie das Zurücksetzen von Kennwörtern oder das Anlegen von neuen Objekten. Erstellen Administratoren neue Objekte wie

Organisationseinheiten oder Benutzerkonten, zeigt das Center übersichtliche und leicht verständliche Formulare an. Das Tool verbindet sich über die Active Directory-Webdienste mit Active Directory. Administratoren starten das Active Directory-Verwaltungscenter entweder über die Programmgruppe *Tools* im Server-Manager oder indem Sie *dsac* in der PowerShell oder der Eingabeaufforderung eingeben. Auf der linken Seite der Konsole lässt sich durch die Domänen und die Organisationseinheiten navigieren. Im linken oberen Bereich können Administratoren zwischen einer Baumstruktur wie im Snap-In *Active Directory-Benutzer und -Computer* und einer Struktur ähnlich wie dem früheren Startmenü wechseln.

Verwaltungswerkzeuge starten

Da es in Windows Server 2012 R2 kein Startmenü mehr gibt, müssen Administratoren die Verwaltungswerkzeuge über andere Wege starten. Das zentrale Verwaltungswerkzeug in Windows Server 2012 R2 ist der Server-Manager. Hier sind die verschiedenen Servergruppen zusammengefasst, auch die Active Directory-Domänendienste. Klicken Sie auf *AD DS*, sind alle Domänencontroller zu sehen, die sich mit dem Manager verwalten lassen. Auch die zusammengefassten Meldungen aus allen Ereignisanzeigen sind zu sehen. Mehr zum Thema lesen Sie in Kapitel 3.

Abbildg. 1.18 Server über das Netzwerk mit dem Server-Manager verwalten



Um im Server-Manager in Windows Server 2012 R2 weitere Server anzubinden, klicken Sie auf *Verwalten* und dann auf *Server hinzufügen*. Im Fenster lässt sich anschließend nach Servern suchen, um sie im lokalen Server-Manager zu verwalten. Über das Kontextmenü von Servern können Sie Server über das Netzwerk remote neu starten lassen, eine PowerShell-Sitzung auf dem Server starten oder eine Remotedesktopverbindung öffnen. Auch die Installation von Rollen und Features über das Netzwerk ist mit dem Kontextmenü möglich.

Im Server-Manager sehen Sie am Wartungscentersymbol im oberen Bereich, ob Fehler auf einem angebundenen Server vorliegen oder Maßnahmen zur Verwaltung notwendig sind. Allerdings lassen sich auf diesem Weg nur Server mit Windows Server 2012 R2 zentral verwalten. Windows Server 2008 R2 kann nicht an den Server-Manager von Windows Server 2012 R2 angebunden werden.

Abbildg. 1.19 Anzeigen von Fehlern für alle angebundenen Server

Die wichtigsten Verwaltungswerkzeuge finden Sie jetzt ohne Umwege direkt im Server-Manager. Dazu reicht ein Klick auf das Menü *Tools* oben rechts.

Über die [⊞]-Taste lässt sich auch der Startbildschirm von Windows Server 2012 R2 anzeigen. Hierüber können Sie ebenfalls die Verwaltungsprogramme starten und nach Tools auch suchen. Mit der Tastenkombination [⊞]+[X] blenden Windows 8.1 und Windows Server 2012 R2 in der linken unteren Bildschirmecke ein sogenanntes Schnellzugriffmenü ein, über das sich ebenfalls die wichtigsten Verwaltungsprogrammen, aufrufen lassen.

PowerShell und Active Directory im Detail

Windows Server 2012 R2 kann auch über die PowerShell verwaltet werden. Dazu hat Microsoft einige neue Cmdlets integriert. Die Befehle sehen Sie, wenn Sie in der PowerShell in Windows Server 2012 R2 zunächst das entsprechende Modul mit *Import-Module ADDSDeployment* laden. Die Befehle lassen Sie sich zum Beispiel mit *Get-Command *adds** anzeigen. Mit dem Cmdlet *Install-ADDSDomainController* installieren Sie in einer bestehenden Domäne zum Beispiel einen neuen Domänencontroller. Mit *Install-ADDSDomain* installieren Sie eine neue Domäne, mit *Install-ADDSForest* eine neue Gesamtstruktur.

Um einen Domänencontroller herabzustufen, verwenden Sie das Cmdlet *UnInstall-ADDSDomainController*. Die Cmdlets fragen alle notwendigen Optionen ab und startet den Server neu. Anschließend nehmen Sie Konfigurationen wie DNS-Server und globaler Katalog vor. Diese Aufgaben müssen Sie nicht mehr im Assistenten zur Installation durchführen.

Auch neue Cmdlets, um die Installation und Betrieb von Active Directory zu testen, hat Microsoft integriert. Dazu gibt es die neuen Cmdlets *Test-ADDSDomainControllerInstallation*, *Test-ADDSDomainControllerUnInstallation*, *Test-ADDSDomainInstallation*, *Test-ADDSForestInstallation* und *Test-ADDSReadOnlyDomainControllerUnInstallation*.

Wollen Sie Domänencontroller zu Windows Server 2012 R2 aktualisieren, müssen Sie zunächst das Schema der Gesamtstruktur erweitern. Dazu führen Sie den Befehl *adprep /forestprep* auf einem Domänencontroller aus. Sie finden das Tool im Ordner *support\adprep* auf der Windows Server 2012 R2-DVD.

Damit Sie das Schema erweitern können, müssen Sie zuvor noch mit der Taste C die Erweiterung bestätigen. Nach der Aktualisierung des Schemas sollten Sie mit *adprep /domainprep* noch die einzelnen Domänen aktualisieren. Installieren Sie neue Domänencontroller, lassen sich diese problemlos in Active Directory aufnehmen. Auch Mitgliedsserver mit Windows Server 2012 R2 können Sie in bestehende Domänen aufnehmen, wenn Domänencontroller mit Windows Server 2003/2003 R2/2008/2008 R2 vorhanden sind.

Bei Migrationen können Sie Betriebsmasterrollen von Vorgängerversionen auf die neuen Domänencontroller mit Windows Server 2012 R2 übernehmen. Die Vorgänge dazu sind identisch mit der Übernahme in Windows Server 2008 R2.

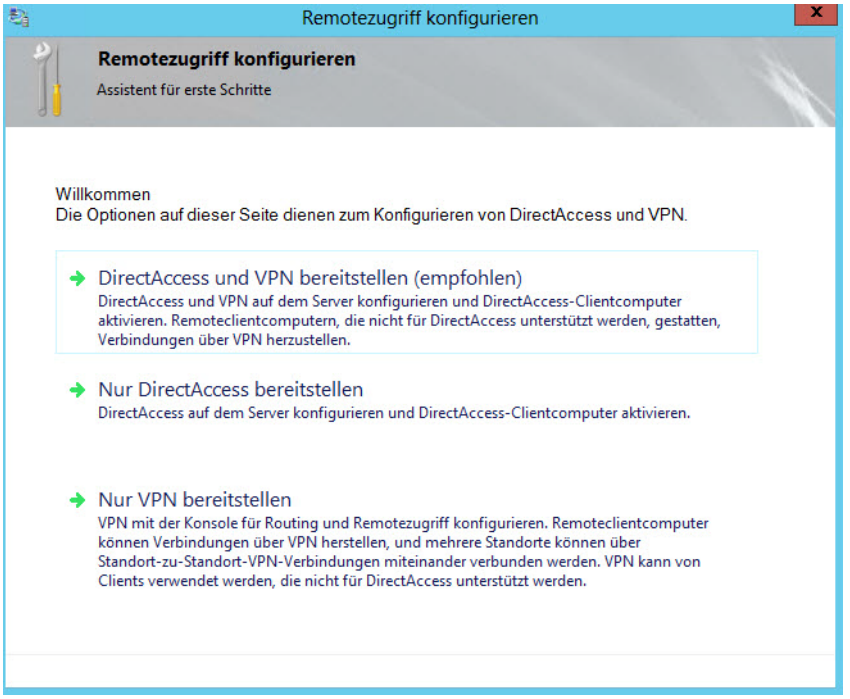
Verbesserte und vereinfachte VPN-Möglichkeiten

Mit Windows Server 2008 R2 hat Microsoft DirectAccess eingeführt. Durch diese Technik können Sie PCs mit Windows 7/8/8.1 über das Internet direkt mit dem Unternehmensnetzwerk verbinden, ohne dass Sie Zusatzsoftware einsetzen müssen. Für den Verbindungsaufbau ist kein VPN notwendig. Nach der ersten Einrichtung erkennt ein DirectAccess-PC automatisch die Verbindung, verschlüsselt sie und kann sich mit dem Netzwerk verbinden. Auch Gruppenrichtlinien lassen sich über diesen Weg ausliefern.

Nachteil von DirectAccess in Windows Server 2008 R2 war die komplizierte Einrichtung und die verschiedenen Verwaltungswerkzeuge die Administratoren nutzen mussten. Beides hat Microsoft in Windows Server 2012 optimiert. Die Einrichtung ist deutlich einfacher und für die Verwaltung von RemoteAccess und DirectAccess gibt es nur noch eine einzelne Konsole. RemoteAccess und DirectAccess lassen sich jetzt daher gemeinsam verwalten und es gibt keine Konflikte mehr beim parallelen Einsatz der Systeme.

Ansonsten haben Unternehmen weiterhin den Vorteil, den DirectAccess bereits in Windows Server 2008 bietet: Clientcomputer lassen sich effizient auch über das Internet sicher am Netzwerk anbinden, ohne dass Anwender erst VPN-Verbindungen aufbauen müssen. Der Datenzugriff funktioniert, Gruppenrichtlinien lassen sich anwenden und Software-Updates verteilen. Die Kommunikation erfolgt über IPv6. Ist dies mit der aktuellen Datenverbindung nicht möglich, kapselt das Betriebssystem die IPv6-Pakete in IPv4-Pakete und versendet sie an die Zielserver. Mehr zum Thema lesen Sie in Kapitel 32.

Abbildg. 1.20 Bereitstellen von DirectAccess und Remotezugriff



Die Installation von DirectAccess erfolgt über den Server-Manager. Über *Verwalten/Rollen und Features hinzufügen/Remotezugriff* installieren Sie die notwendigen Funktionen auf dem Server. Weitere Einstellungen – wie noch in Windows Server 2008 R2 – sind zur Installation nicht notwendig.

Nach der Installation finden Sie im Server-Manager die neue Gruppe *Remotezugriff* vor. Über das Kontextmenü der hier integrierten Server lässt sich die Verwaltung von RemoteAccess starten. Über eine gemeinsame Konsole findet dann die Einrichtung der beiden Funktionen statt. Mehr dazu lesen Sie in Kapitel 32.

Verbessertes und sicheres DNS-System

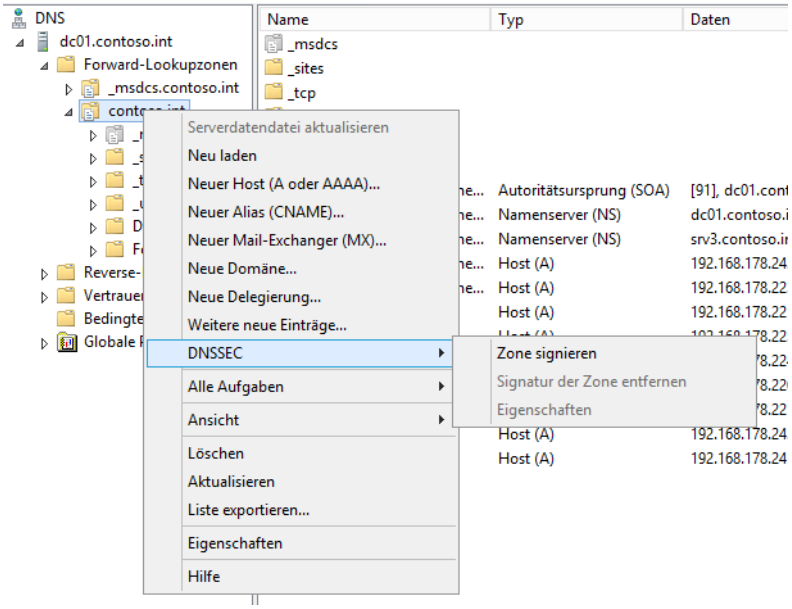
Durch die engere Verzahnung der Server miteinander ist auch eine Verbesserung des DNS-Systems notwendig, vor allem im Bereich der Sicherheit. Bereits mit Windows Server 2008 R2 hat Microsoft DNSSEC eingeführt, um Zonen und Einträge abzusichern. Die Verwaltung von DNS-Servern ist im Server-Manager von Windows Server 2012 R2 durch die Gruppierung wesentlich effizienter.

In Windows Server 2012 R2 lassen sich Zonen online digital signieren. DNSSEC lässt sich in der neuen Version komplett in Active Directory integrieren. Das umfasst auch die Möglichkeit dynamische Updates für geschützte Zonen zu aktivieren. Windows Server 2012 R2 unterstützt offizielle Standards wie NSEC3 und RSA/SHA-2.

Neu seit Windows Server 2012 ist auch die Unterstützung von DNSSEC auf schreibgeschützten Domänencontrollern (RODC). Findet ein RODC mit Windows Server 2012 R2 eine signierte DNS-Zone, legt er automatisch eine sekundäre Kopie der Zone an und überträgt die Daten der DNSEC-geschützten Zone. Das hat den Vorteil, dass auch Niederlassungen mit RODCs gesicherte Daten auflösen können, aber die Signatur und Daten der Zone nicht in Gefahr sind.

DNSSEC lässt sich über das Kontextmenü von Zonen erstellen. Eine komplizierte Konfiguration in der Eingabeaufforderung ist nicht mehr notwendig. Auch Zonen offline zu setzen, ist nicht mehr notwendig. Die Signierung der Zone erfolgt über einen Assistenten. Mit diesem können Sie recht einfach DNS-Zonen vor Manipulationen schützen. Der Assistent erlaubt die manuelle Signierung, eine Aktualisierung der Signierung und eine Signierung auf Basis automatischer Einstellungen.

Abbildg. 1.21 DNS-Zonen digital signieren



Mit Windows Server 2012 R2 lassen sich signierte Zonen auch auf andere DNS-Server im Netzwerk replizieren. Eine weitere Neuerung ist IP-Adressverwaltungsserver (IPAM). Dieser Serverdienst überwacht und steuert zentral DHCP- und DNS-Server. Die Installation erfolgt als Serverrolle. Der

Dienst kann Änderungen überwachen und die Serverdienste zentral überwachen. Mehr zum Thema lesen Sie in Kapitel 25.

Windows Server 2012 R2 lizenzieren

Mit seinen Serverprodukten System Center 2012, SQL Server 2012 und auch Windows Server 2012 R2 ändert Microsoft teilweise deutlich seine Lizenzierungspolitik. Unternehmen sollten, neben eventuellen Verträgen zu Leasing, Miete oder Kauf, auch beachten, welche Edition sie einsetzen wollen, und welche Anzahl von Lizenzen benötigt werden.

So verfügen zum Beispiel die Editionen Standard und Datacenter über den gleichen Funktionsumfang und eine Enterprise-Edition oder Webserver-Edition gibt es nicht mehr.

Editionen und Lizenzen im Vergleich

Microsoft bezeichnet Windows Server 2012 R2 als Cloudbetriebssystem. Virtualisierung und Cloudanbindung stellen einen klaren Schwerpunkt dar. Auf Servern mit Windows Server 2012 R2 Standard dürfen Unternehmen daher zwei virtuelle Server pro Lizenz installieren. Sollen auf einem Hyper-V-Host mehr virtuelle Server im Einsatz sein, sind mehrere Lizenzen für die Standard-Edition notwendig, oder eben eine Datacenter-Lizenz. Die Datacenter-Edition erlaubt den Betrieb unbegrenzt vieler virtueller Server auf einem Host. Beide Editionen decken außerdem immer nur zwei Prozessoren des Hosts ab.

Die erforderliche Mindestanzahl von Betriebssystemlizenzen für jeden Server wird durch die Anzahl der physischen Prozessoren des Hosts sowie die Anzahl an virtueller Server bestimmt, die Sie auf dem Hyper-V-Host installieren.

Setzen Unternehmen also Server mit mehreren Prozessoren ein, ist pro Prozessorpaar (nicht Kern) eine Lizenz notwendig, egal welche Edition im Einsatz ist.

Virtualisierung mit Hyper-V ist nur mit den beiden Editionen Windows Server 2012 R2 Standard und Datacenter möglich. Hyper-V-Hosts unterstützen bis zu 160 logische Prozessoren und 2 TB Arbeitsspeicher; Gäste unterstützen bis zu 32 virtuelle Prozessoren und 1 TB Arbeitsspeicher. Ansonsten orientiert sich Windows Server 2012 R2 an den Systemvoraussetzungen für Windows Server 2008 R2.

Neu in Windows Server 2012 R2 ist die Möglichkeit, auf Basis von Enterprise Agreements bestimmte Lizenzen zu erwerben, die im Betrieb zusammen mit Windows Azure Kosten sparen sollen. Lizenzen von Windows Server 2012 R2 sind direkt an die physische Hardware gebunden. Jede Lizenz deckt weiterhin zwei physische Prozessoren ab. Sie dürfen mit der Standard-Edition außerdem bis zu zwei virtuelle Server auf dem lizenzierten Host betreiben. Beim Einsatz der Datacenter-Edition dürfen Sie so viele virtuelle Server auf dem Host betreiben, wie die Hardware hergibt. Welche Edition Sie einsetzen, müssen Sie einfach durchrechnen. Einfach ausgedrückt lohnt sich die Anschaffung der Datacenter-Edition dann, wenn Sie auf einem Server mit zwei Prozessoren mehr als 14 virtuelle Server betreiben. Die Datacenter-Edition kostet laut Microsoft 6.155 US-Dollar, die Standard-Edition 882 US-Dollar.

Weiterhin gibt es die Editionen Essentials und Foundation. Windows Server 2012 R2 Essentials erlaubt die Anbindung von bis zu 25 Benutzer, dafür sind keine CALs notwendig. Setzen Sie Windows Server 2012 R2 Foundation ein, darf auf dem Server nur ein Prozessor verbaut sein. Sie dürfen

bis zu 15 Benutzer an den Server binden, auch hier sind keine CALs notwendig. Die Essentials-Edition wurde vom Preis auf etwa 501 US-Dollar erhöht, Foundation ist direkt an die Hardware gebunden, da diese Edition nur als OEM-Version verfügbar ist.

HINWEIS Die oben angegebenen Preise (in US-Dollar) gelten als grobe Anhaltspunkte für die Lizenzkosten und sind unverbindlich. Die Microsoft-Softwareprodukte lassen sich in verschiedene Lizenzmodellkategorien einteilen. Produkte, die bei einer Softwarelösung häufig gemeinsam eingesetzt werden, unterliegen in der Regel dem gleichen beziehungsweise einem vergleichbaren Lizenzmodell. Mehr Informationen zu Lizenzkosten finden Sie auf der Microsoft-Website *http://www.microsoft.com/de-de/licensing/produktlizenzierung/einfuehrung/default.aspx* [Ms179-K01-03].

Für die Editionen Standard und Datacenter benötigen Sie weiterhin Clientzugrifflizenzen (CALs). Auch in Windows Server 2012 R2 können Sie diese benutzerbasiert oder pro Gerät erwerben, dürfen diese aber weiterhin aufsplitten. Neu in Windows Server 2012 R2 ist aber die Möglichkeit, auch mit Windows Server 2012-CALs auf Server mit Windows Server 2012 R2 zugreifen zu dürfen. Dieses Entgegenkommen gilt auch für die erweiterten Serverdienste wie die Rechteverwaltung und die Remotedesktopdienste. Das heißt, Unternehmen, die bereits Windows Server 2012 umfassend lizenziert und im Einsatz haben, müssen lediglich neue Serverlizenzen erwerben und können Server direkt auf Windows Server 2012 R2 aktualisieren.

Clientzugriffslizenzen beachten

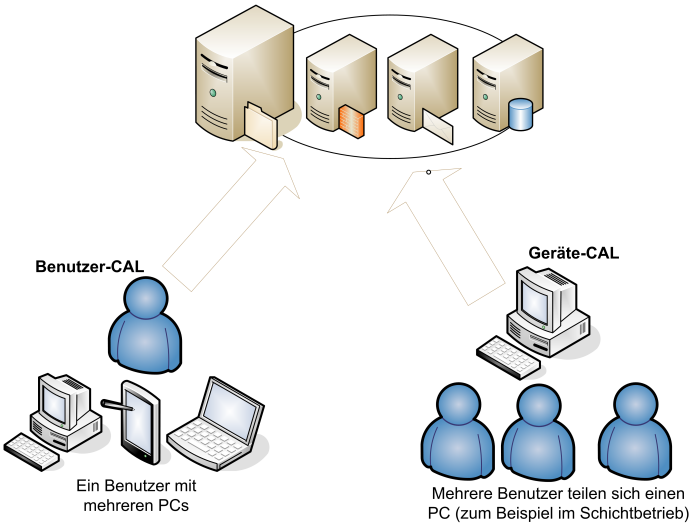
Clientzugrifflizenzen (CALs) und Remotedesktop-Clientzugrifflizenzen (RDCALs) sind auch in Windows Server 2012 R2 weiterhin notwendig, aber nur in den Editionen Standard und Datacenter. Auch hier gibt es zukünftig Gerätelizenzen oder Benutzerlizenzen für den Zugriff. Sie müssen bereits bei der Bestellung Ihrer Lizenzen im Voraus planen, welchen Lizenztyp Sie einsetzen wollen. Sie können auch die verschiedenen Lizenzen miteinander mischen.

Es ist jedoch nicht erlaubt, die einzeln erhältlichen Lizenzpakete in Geräte- und Benutzerlizenzen aufzusplitten. Sie dürfen also ein 5er-Paket Gerätelizenzen und ein 5er-Paket Benutzerlizenzen für einen Server kaufen und lizenzieren.

Es ist aber nicht erlaubt, diese Pakete aufzusplitten und zum Beispiel als 2er-Gerätelizenz und 8er-Benutzerlizenz zu verwenden. Auch nicht zulässig ist, mit CALs von Vorgängerversionen auf Server mit Windows Server 2012 R2 zuzugreifen.

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. Alternativ können Sie auch eine Benutzer-CAL kaufen.

Abbildg. 1.22 Geräte-CALs und Benutzer-CALs in Windows Server 2012 R2



Jeder Benutzer mit einer Benutzer-CAL kann an beliebig vielen PCs eine Verbindung mit einem Server aufbauen. Die CALs müssen eindeutig zugewiesen sein. Sie können daher nicht nur so viele CALs kaufen, wie gleichzeitig Benutzer arbeiten, sondern müssen die Gesamtzahl Ihrer Arbeitsstationen, Smartphones und sonstiger Geräte lizenzieren, wenn Sie Geräte-Lizenzen kaufen.

Bei Benutzerlizenzen müssen diese genau der Anzahl der Benutzer zugewiesen werden, die insgesamt mit dem Server arbeiten. Es ist nicht erlaubt, auf einem Server Lizenzen von Standard und Datacenter zu mischen. Sie dürfen eine Lizenz auch nicht auf mehrere Server aufsplitten, zum Beispiel eine Lizenz auf zwei Server mit einzelnen Prozessoren. Mehr zur Lizenzierung finden Sie über den Link *http://download.microsoft.com/download/F/3/9/F39124F7-0177-463C-8A08-582463F96C9D/Windows_Server_2012_R2_Licensing_Datasheet.pdf* [Ms179-K01-04].

In Ihrem Unternehmen sind beispielsweise 100 Mitarbeiter beschäftigt, von denen jedoch lediglich 63 mit PCs am Server arbeiten. Wenn Sie Geräte-CALs kaufen, wird jede gekauft Lizenz einem bestimmten PC zugeordnet. Mit diesen PCs können sich jetzt beliebig viele Mitarbeiter mit Server verbinden, wenn sich diese zum Beispiel PCs im Schichtbetrieb teilen. Wenn neue PCs hinzukommen, müssen Sie für diese PCs weitere Gerätelizenzen kaufen. Im nächsten Beispiel gehen wir von einer IT-Firma aus, in der 40 Mitarbeiter beschäftigt sind. Von diesen 40 Mitarbeitern arbeiten 25 mit der Windows-Domäne. Jeder dieser Mitarbeiter hat einen PC und ein Notebook, mit denen er am Server arbeitet. Obwohl in diesem Unternehmen nur 40 Mitarbeiter beschäftigt sind, verbinden sich 50 PCs mit dem Server. Es müssen in diesem Beispiel daher 50 Gerätelizenzen erworben werden. Wenn das Unternehmen seine Lizenzen jedoch als Benutzerlizenz erwirbt, werden lediglich 25 Lizenzen benötigt, da nur 25 Benutzer mit Server arbeiten.

Windows Server 2012 R2 für kleine Unternehmen

Sehr kleine Unternehmen können auf Windows Server 2012 R2 Essentials setzen. Dabei handelt es sich um den direkten Nachfolger von Small Business Server 2012 Essentials, ohne Exchange oder SQL. Mehr dazu lesen Sie in den Kapiteln 2, 3, 5, 18 und 20. Einen Nachfolger für SBS 2012 Standard mit Exchange und einem SQL-Server gibt es nicht mehr. Unternehmen, die Microsoft Exchange nutzen wollen, müssen auf Office 365 setzen oder Exchange auf einer eigenen Servermaschine getrennt lizenzieren.

Windows Server 2012 R2 Essentials verfügt über eine eigene Verwaltungsoberfläche, die als Dashboard bezeichnet wird. Mit diesem lassen sich Clientcomputer und Benutzer zentral verwalten, auch ohne IT-Kenntnisse. Der Server erlaubt die Anbindung von maximal 25 Benutzern und 50 PCs. Wenn mehr im Einsatz sind, müssen Unternehmen auf die Standard-Edition von Windows Server 2012 R2 erhöhen. CALs sind für die Benutzer nicht notwendig. Neu in Windows Server 2012 R2 ist die Möglichkeit, die Essentials-Funktionalitäten auch als Serverdienst in den Editionen Datacenter und Standard zu installieren.

Die kleinste Edition von Windows Server 2012 R2 ist Foundation. Diese stellt Microsoft nur für OEMs zur Verfügung. Der Server verfügt über die Standardverwaltungstools von Windows Server 2012 R2, also kein eigenes Dashboard wie Essentials. Außerdem lassen sich an Windows Server 2012 R2 Foundation nur maximal 15 Benutzer anbinden. Clientzugrifflizenzen sind in diesem Fall ebenfalls nicht notwendig. Wer sich ausführlich mit den verschiedenen Lizenzierungsmöglichkeiten befassen will, sollte sich die Seite *http://www.microsoft.com/de-de/server/lizenzieren-kaufen.aspx* [Ms179-K01-05] ansehen. Zusätzliche Zugriffslizenzen (Client Access License, CALs) sind für Foundation nicht erforderlich.

Windows Server 2012 R2 Essentials und Foundation werden in einem prozessorbasierenden Lizenzmodell lizenziert. Foundation ist beschränkt auf Server mit einem Prozessor. Windows Server 2012 R2 Essentials ist beschränkt auf Server mit bis zu zwei Prozessoren, benötigt dafür aber auch keine CALs.

Core-Server mit Windows Server 2012 R2

Core-Server sind eine Möglichkeit, um Windows ohne grafische Oberfläche zu installieren. Das vermeidet Sicherheitslücken und beschleunigt das System, da die ressourcenfressende grafische Oberfläche fehlt. Installieren Sie einen Core-Server, fehlen dem Betriebssystem die grafische Oberfläche und die dazugehörigen Verwaltungstools. Die Verwaltung erfolgt dann entweder über die Eingabeaufforderung, die PowerShell oder über andere Rechner. Ein Tool, um einen Core-Server einzurichten, ist Sconfig. Hierbei handelt es sich um einen textorientierten Assistenten zur Grundeinrichtung des Servers. Von den freien Ressourcen eines Core-Servers profitieren Serverdienste wie Hyper-V oder auch Domänencontroller. Auch Speicherplatz lässt sich dadurch sparen.

Eine Core-Installation von Windows Server 2012 R2 verbraucht über 4 GB weniger Speicherplatz als eine herkömmliche Installation mit grafischer Oberfläche. Betreiben Unternehmen zahlreiche virtuelle Server auf einem Host, lässt sich auf diese Weise für jeden einzelnen Server enorm Speicherplatz insgesamt auf dem Host einsparen.

Ein weiterer Vorteil ist der schnellere Neustart von Core-Servern, sowie weniger notwendige Neustarts nach der Installation von Patches. Kompromisse lassen sich eingehen, wenn Sie das Minimal Server Interface aktivieren. Dabei handelt es sich um eine dritte Möglichkeit der grafischen Oberfläche neben Core-Servern und vollständig installierten Servern in Windows Server 2012 R2.

Core-Server mit SQL Server 2012

Mit Windows Server 2012 R2 geht Microsoft in der Verwendung von Core-Servern noch ein paar Schritte weiter und integriert weitere Möglichkeiten. Zunächst unterstützen mehr Serverdienste den Core-Modus. Allen voran lässt sich der neue Microsoft-Datenbankserver SQL Server 2012 auf Core-Servern mit Windows Server 2008 R2 und Windows Server 2012 R2 installieren. Der Vorteil dabei liegt auf der Hand: Vor allem Datenbankserver benötigen sehr viel Leistung und benötigen eine weitaus höhere Serversicherheit.

In Windows Server 2012 R2 ist die Installation als Core-Server der von Microsoft empfohlene Weg und standardmäßig bereits ausgewählt. Eine wesentliche Neuerung in Windows Server 2012 R2 ist aber die Möglichkeit die grafische Oberfläche über die PowerShell nachträglich zu installieren. Das heißt, Sie können aus einem Core-Server einen vollständigen Server mit grafischer Oberfläche machen. Die installierten Serverdienste werden davon nicht beeinträchtigt. Dazu geben Sie in der Eingabeaufforderung *powershell* ein und in der PowerShell-Sitzung dann *Install-WindowsFeature Server-Gui-Shell*. Nach ein paar Minuten startet der Server neu und Windows Server 2012 R2 steht zur Verfügung.

Umgekehrt lässt sich von Servern mit grafischer Oberfläche diese in Schritten entfernen. Die grafische Oberfläche in Windows Server 2012 R2 ist ein Feature, welches sich über den Server-Manager deinstallieren lässt. Durch die flexible Installation der grafischen Oberfläche können Sie zum Beispiel Server mit der grafischen Verwaltungstools einrichten und anschließend die grafische Benutzeroberfläche entfernen.

Treten auf einem Core-Server Fehler auf, die sich mit Verwaltungstools besser lösen lassen, besteht die Möglichkeit, die grafische Verwaltungsoberfläche zu installieren, die Fehler zu beheben und den Server wieder in Funktion zu setzen. Anschließend lässt sich die grafische Oberfläche schnell und einfach wieder entfernen und der Core-Modus aktivieren.

Minimal Server Interface

Neben der reinen Core-Installation lässt Windows Server 2012 R2 aber mehr Unterscheidungen zu. Installieren Sie auf einem Server nur das Feature *Grafische Verwaltungstools und Infrastruktur*, aktiviert der Server das sogenannte Minimal Server Interface. Dieses verfügt über alle grafischen Verwaltungstools, aber der Internet Explorer, der Desktop und der Startbildschirm sowie Apps werden dabei nicht installiert. Die Microsoft Management Console (MMC), der Server-Manager und der größte Teil der Systemsteuerung sind verfügbar.

Das Minimal Server Interface können Sie nicht bei der Installation auswählen, sondern nur nachträglich im Server-Manager durch die Deinstallation der Desktopdarstellung und der grafischen Servershell aktivieren. Nach der Installation oder Deinstallation von verschiedenen Grafikoptionen ist allerdings immer ein Neustart des Servers notwendig. Erst dann sind die neuen Features aktiviert oder entfernt.

Auf Core-Servern sind die Eingabeaufforderung und die PowerShell verfügbar, aber weder der Server-Manager noch die MMC. Auch die Systemsteuerung, der Explorer, der Internet Explorer, Apps und die Hilfefunktion sind nicht verfügbar. Das gilt auch für alle Multimediafunktionen wie den Media Player.

Bei der Aktivierung des Minimal Server Interface sind Eingabeaufforderung, PowerShell, Server-Manager, MMC und Systemsteuerung verfügbar. Windows-Explorer, Taskleiste, der Desktop, Inter-

net Explorer, die Hilfe und Apps fehlen aber auch hier. Aktivieren Sie die vollständige grafische Oberfläche ohne die Desktopdarstellung sind alle grafischen Tools verfügbar, es fehlen aber Themes, Startbildschirm, Apps und der Media Player. Dieser ist erst durch die Installation der Desktopdarstellung verfügbar. Das gilt auch für Themes, den Startbildschirm und die Apps.

Features on Demand

Bis Windows Server 2008 R2 waren die Binärdateien von Features und Serverrollen auch dann auf dem Server gespeichert, wenn die Rollen oder Features nicht installiert waren. Das hat zwar den Vorteil, dass sich Features und Rollen auch ohne das Installationsmedium auf Servern integrieren lassen, verbraucht aber unnötigen Speicherplatz. Windows Server 2012 R2 bietet jetzt die Möglichkeit, auch die nicht benötigten Binärdateien von einem Server zu entfernen.

Der Vorgang lässt sich mit den Installationsmedien von Windows Server 2012 R2 jederzeit wieder rückgängig machen. Binärdateien entfernen Sie in der PowerShell mit dem Cmdlet *Uninstall-WindowsFeature*. Rückgängig machen lässt sich der Vorgang mit *Install-WindowsFeature*. Ein Vorteil von Feature on Demand ist die Bereitstellung von Servern über Images. Entfernen Administratoren vor der Erstellung eines Images nicht notwendige Binärdateien, lassen sich bis zu 1 GB Speicherplatz gewinnen.

Windows Azure und SQL Azure

Die Microsoft Azure-Plattform (*http://www.microsoft.com/de-de/cloud/services/windows_azure.aspx* [Ms179-K01-06]) ist eines der Public-Cloud-Angebote von Microsoft. Unternehmen können in Windows Azure oder SQL Azure verschiedene Ressourcen oder komplette Server, Websites und Dienste buchen und so weltweit kostengünstig nutzen.

Mit SQL Azure können Unternehmen zum Beispiel Daten zwischen einem lokal betriebenen SQL-Server und SQL Azure austauschen. Über Azure können Unternehmen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) oder Software as a Service (SaaS) bereitstellen.

Bei Windows Azure und SQL Azure geht es aber nicht nur darum, dass Sie Daten im Internet speichern. Unternehmen können gezielt Ressourcen bei Microsoft buchen und über Azure sowie den neuen Serversystemen von Microsoft an das eigene Netzwerk und Anwendungen anbinden. Dies hat den Vorteil, dass Unternehmen von der weltweiten günstigen Bereitstellung von Datenbanken, virtuellen Servern oder anderen Ressourcen profitieren können und parallel auch eigene Server betreiben. So lassen sich interne Dienste und Server nach und nach umstellen, ohne gleich komplett auf die Cloud setzen zu müssen.

Neue Microsoft-Serversysteme wie System Center 2012, Windows Server 2012 R2 und auch SQL Server 2012 arbeiten direkt mit Azure zusammen und bieten integrierte Assistenten für die Zusammenarbeit der beiden Systeme an. Auf diese Weise können Sie an zentraler Stelle die lokalen Serverdienste, aber auch Dienst in Windows Azure verwalten. Zusätzlich steht für Windows Azure auch noch eine webbasierte Oberfläche zur Verfügung.

Windows Azure in aller Kürze

Einfach ausgedrückt handelt es sich bei Windows Azure zunächst um verschiedene Dienste, die Unternehmen online buchen können. Diese werden hochverfügbar in Microsoft-Rechenzentren weltweit zur Verfügung gestellt und lassen sich über das Internet nutzen. Flankierend dazu bietet Microsoft Entwicklerwerkzeuge an, um die Bereitstellung eigener Programme zu ermöglichen. Auch Tools für die Anbindung und Migration zu Azure-Diensten stellt Microsoft kostenlos zur Verfügung.

Anwendungen können auch lokal betrieben werden und dennoch in einzelnen Bereichen auf Daten in der Cloud zugreifen. Sie können zum Beispiel lokale Datenbanken und parallel Datenbanken in Azure betreiben. Unternehmen sind dabei nicht auf Microsoft-Technologien beschränkt, sondern können fast alle bekannten Arten von Entwicklungsumgebungen nutzen. Administratoren können sich auf Wunsch ganz normal mit Remotedesktopverbindungen über das Internet mit den virtuellen Servern in der Cloud verbinden und Anwendungen bereitstellen. Eine Einführung sehen Sie in einem Video von Microsoft (*http://www.youtube.com/watch?v=rzMl7B4jiPY* [Ms179-K01-07]). Auch Windows Server 2012 R2 lässt sich in den virtuellen Servern installieren.

Unternehmen können in Windows Azure auch virtuelle Server bereitzustellen und dabei nicht nur auf Microsoft-Systeme setzen, sondern auch Linux installieren. Windows Azure ist das Herzstück und stellt das Cloudbetriebssystem und die Kernfunktion zur Verfügung. Auf diese bauen Dienste wie zum Beispiel SQL Azure auf. Unternehmen können selbst Anwendungen entwickeln und über Azure weltweit zur Verfügung stellen. Die dazu notwendigen Datenbanken liegen direkt im Azure-System und sind in Microsoft-Rechenzentren gespeichert. Auf diese Weise profitieren vor allem Unternehmen mit vielen internationalen Niederlassungen oder zahlreichen mobilen Mitarbeitern. Um den Server selbst müssen sich Unternehmen auf Wunsch nicht kümmern, das machen Microsoft-Mitarbeiter in den verschiedenen Rechenzentren.

Zusätzlich zu Windows Azure gehören zum Microsoft Cloud-Programm weitere Programme, die sich mit Windows Azure koppeln oder parallel dazu betreiben lassen. Microsoft Office Web Apps bieten eine Internetbasierte Bearbeitung von Office-Dokumenten. Microsoft Dynamic CRM Online bietet Unternehmen die Möglichkeit über das Internet Customer Relationship Management (CRM) zentral bereitzustellen. Wer online auf Exchange und SharePoint setzen will, bucht Office 365. Windows-Clients verwalten Unternehmen ebenfalls cloudgestützt mit Windows Intune. Alle diese Dienste haben generell nichts mit Windows Azure zu tun, lassen sich aber parallel dazu nutzen.

Windows Azure Virtual Machines bieten Unternehmen zum Beispiel die Möglichkeit eigene virtuelle Server in Windows Azure bereitzustellen. Die Server funktionieren genauso wie lokal installierte virtuelle Server. Auf den Servern können Sie Windows Server 2012 R2 installieren, aber auch Linux (Suse, OpenSuse, CentOS, Ubuntu). Microsoft bietet vorgefertigte virtuelle Server an, die SharePoint (SharePoint 2010), Active Directory (Windows Server 2008 R2/2012) und SQL Server (SQL Server 2008/2008 R2/2012) zur Verfügung stellen. Die virtuellen Festplatten dieser Server sind direkt in Windows Azure gespeichert, auf Wunsch auch hochverfügbar.

Die virtuellen Server müssen aber von Ihnen selbst verwaltet werden. Auch die Betriebssysteme und Patches müssen selbst gepflegt werden. Ist das nicht erwünscht, können Sie für Ihr Unternehmen auch die Windows Azure Cloud Services oder die Websites buchen, beziehungsweise die SQL-Datenbanken in SQL Azure erstellen. Im Gegensatz zu den gebuchten Diensten wie SQL-Azure oder SharePoint Online in Office 365, können Administratoren in virtuellen Servern alle Einstellungen vornehmen, die auch in einer lokalen Installation möglich sind. Die verschiedenen Möglichkeiten zeigt Microsoft in einem YouTube-Video (*http://www.youtube.com/watch?v=KgJa1IGjewQ* [Ms179-

K01-08]). Sie können auch virtuelle Festplatten einzeln in Windows Azure bereitstellen. Diese Funktion trägt die Bezeichnung Windows Azure Drives. Auch hier lässt sich die Pflege direkt zu Microsoft übergeben.

Windows Azure Websites bieten die Möglichkeit, öffentliche Internetauftritte in Windows Azure zur Verfügung zu stellen. Die Funktion ist auch für kleine Unternehmen geeignet und bietet entsprechende Vorlagen. Internetseiten müssen dabei nicht auf Microsoft-Technologien aufbauen, sondern können auch Frameworks von Drittherstellern verwenden. PHP und Java gehören zum Beispiel zu den unterstützten Modellen, auch Drupal oder Wordpress lassen sich einbinden. Um Webseiten bereitzustellen können Entwickler Windows nutzen, aber auch problemlos Linux oder Mac OS. In der Weboberfläche von Windows Azure lassen sich auch Statistiken zu Seiten anzeigen und diese skalieren, um größere Umgebungen zur Verfügung zu stellen. Mehr zu diesem Thema sehen Sie in einem Microsoft-Video (*http://www.youtube.com/watch?v=xw0Osiksue4* [Ms179-K01-09]).

Windows Azure Cloud Services sind dazu geeignet, Multi-Tier-Webanwendungen für sehr große Unternehmen bereitzustellen. Die Services sind sozusagen ein Platform-as-a-Service (PaaS)-Modell. Das heißt, Entwickler kümmern sich nur um die entsprechende Anwendung. Die im Hintergrund laufenden und notwendigen virtuellen Server und Einstellungen werden automatisch von Windows Azure übernommen und gepflegt. Auch diese Funktion ist neu seit Juni 2012. Bei dieser Funktion handelt es sich um das nächst größere Modell der Windows Azure Websites. Dieser Dienst ist vor allem für Unternehmen geeignet, die große Anwendungen zur Verfügung stellen, aber keine Pflege der notwendigen Serverinfrastruktur betreiben wollen.

Windows Azure testen

Interessierten Unternehmen stellt Microsoft auch voll funktionsfähige Testversionen von Azure zur Verfügung (*http://www.windowsazure.com/de-de/pricing/free-trial* [Ms179-K01-10]). Sie müssen zwar eine Kreditkarte beim Anmelden der Testversion angeben, allerdings dient diese nur zur Verifikation, Sie müssen nichts für den Test bezahlen. Windows Azure können Sie bis zu 90 Tage vollkommen kostenlos testen. Sie haben dabei die Möglichkeit, kostenlose Clouddienste, virtuelle Server, Datenbanken und Speicher zu erstellen. Wollen Sie das Produkt nach der Testzeit buchen, wandeln Sie den Testaccount in ein produktives Konto um. Die erstellten Daten und Server sowie die Datenbanken und Einstellungen bleiben erhalten.

Wollen Sie Windows Azure nicht weiter nutzen, läuft das Konto aus, Sie müssen nichts kündigen. Die Preise hängen davon ab, was Sie in Windows Azure nutzen wollen und welche Bandbreite Sie verwenden möchten. Microsoft bietet dazu einen Kostenrechner an (*http://www.windowsazure.com/de-de/pricing/calculator* [Ms179-K01-11]). So kostet ein virtueller Server mit Windows oder Linux und 2 x 1,6 GHz CPU, 3,5 GB RAM sowie 490 GB Speicher im Monat 81,70 Euro. Virtuelle Windows Azure-Computer bieten die vollständige Kontrolle über die Anwendungsumgebung und eine einfache Migration vorhandener Anwendungen. In einem Windows-basierten virtuellen Computer sind die Lizenzkosten für Windows Server enthalten. Eine virtuelle SQL Server-Datenbank mit 10 GB Speicher kostet etwa 32,60 Euro im Monat. Unternehmen müssen Windows Azure immer getrennt von lokalen Lizenzen bezahlen. Es ist keine Übertragung von Benutzerlizenzen oder Serverlizenzen zu Windows Azure möglich.

Windows Azure steht aktuell in 41 Ländern weltweit zur Verfügung. Als Support-Option können Unternehmen die Telefonhotline nutzen. Auch Entwicklersupport bietet Microsoft, muss aber pro Anfrage bezahlt werden. Bevor Unternehmen Windows Azure abschließen, sollten sie sich beraten

lassen, welche Vertragsmöglichkeiten es gibt und welche Supportoptionen interessant sind. Auch hierzu bietet Microsoft Informationen im Internet (*http://www.windowsazure.com/de-de/support/contact* [Ms179-K01-12]).

Zusammenfassung

In diesem Kapitel haben wir Ihnen die wichtigsten Neuerungen von Windows Server 2012 R2 gezeigt, damit Sie einen Überblick haben, welche neuen Funktionen es gibt. Wir sind in diesem Kapitel auch auf die Editionen und die Lizenzierung eingegangen. In den weiteren Kapiteln des Buchs vertiefen wir die Neuerungen und zeigen die Verwaltung von Windows Server 2012 R2.

Im nächsten Kapitel erfahren Sie, welche Möglichkeiten Sie haben, um Windows Server 2012 R2 zu installieren und einzurichten.

Kapitel 2

Installation und Grundeinrichtung

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, wie Sie Windows Server 2012 R2 installieren. Wir gehen auch darauf ein, wie Sie erweiterte Installationen durchführen, zum Beispiel mit einem USB-Stick oder auf virtuelle Festplatten, was zum Beispiel für Testumgebungen interessant ist. Wir zeigen Ihnen auch, wie Sie Core-Server installieren sowie die Installation von Hyper-V Server 2012 R2 durchführen.

Zusätzlich erfahren Sie in diesem Kapitel, wie Sie den Boot-Manager von Windows Server 2012 R2 reparieren. Der Boot-Manager funktioniert zwar generell ähnlich wie in Windows Server 2008 R2, weist aber einige wichtige Unterschiede auf. Eine weitere Möglichkeit der Installation ist die Integration in eine virtuelle Festplatte (VHD bzw. VHDX). Auch das wird von Windows Server 2012 R2 unterstützt.

TIPP Sie können sich auf der Seite *http://technet.microsoft.com/de-de/evalcenter* [Ms179-K02-01] Testversionen von Windows Server 2012 R2 Standard und Datacenter herunterladen. Auf dieser Seite finden Sie auch die Testversion von Windows 8.1 Enterprise.

Sie können die Testversion bis zu 180 Tage kostenlos einsetzen, müssen Sie aber nach spätestens 10 Tagen mit dem beim Download zur Verfügung gestellten Product Key aktivieren. Sie sehen die noch zur Verfügung stehende Testzeit auf dem Desktop oder wenn Sie in der Eingabeaufforderung den Befehl *slmgr.vbs /dlv* aufrufen.

Grundlagen zur Installation

Windows Server 2012 R2 verfügt über einen Boot-Manager, mit dessen Hilfe Sie auch mehrere Betriebssysteme parallel auf einem Computer einsetzen können. Sie haben die Möglichkeit, das Bootverhalten zu konfigurieren, die Dauer der Einblendung des Boot-Managers festzulegen, um eine Auswahl zu treffen, und können auch das Standardbetriebssystem definieren. Und auch zusätzliche Betriebssysteme lassen sich in das Bootmenü einbinden.

Windows Server 2012 R2-Installation verstehen

Windows Server 2012 R2 legt während der Installation eine versteckte Partition mit einer Größe von 350 MB auf der Startfestplatte an (in Windows Server 2008 R2 war die Partitionsgröße noch 100 MB). In diesem Bereich liegen die Startdateien von Windows Server 2012 R2 und Daten zum Entschlüsseln von BitLocker-Laufwerken (siehe Kapitel 5). Aktualisieren Sie einen Rechner von Windows Server 2008 R2 zu Windows Server 2012 R2, belässt der Assistent die Startpartition auf der Größe von 100 MB.

Wer Windows Server 2012 R2 produktiv installieren will, hat grundsätzlich vier Möglichkeiten: Die erste ist eine direkte Aktualisierung des bestehenden Windows Server 2008/2008 R2/2012-Systems zu Windows Server 2012 R2. Der Vorteil dabei ist, dass dabei alle Einstellungen und Programme von Windows Server 2008 R2 zu Windows Server 2012 R2 übernommen werden. Allerdings funktioniert manchmal die Übernahme der Programme nicht, sodass Sie diese neu installieren müssen. Benutzername, Daten und Einstellungen bleiben aber erhalten, und die meisten Programme funktionieren nach der Aktualisierung weiterhin problemlos. Empfohlen ist dieser Weg aber nicht. Sie sollten möglichst immer neu installieren.

Wir zeigen Ihnen, wie Sie die verschiedenen Möglichkeiten zur Installation einsetzen und im Notfall auch wieder rückgängig machen können. In jedem Fall ist es sehr empfehlenswert, vor der Aktuali-

sierung einer Windows Server 2008 R2-Installation eine imagebasierte Datensicherung auf einer externen Festplatte durchzuführen. Geht bei der Aktualisierung zu Windows Server 2012 R2 etwas schief, können Sie einfach das Image zurückspielen und so das bisherige Windows Server 2008 R2-System retten. Dazu verwenden Sie am besten ein Systemabbild.

Die zweite Möglichkeit zum Testen von Windows Server 2012 R2 ist eine komplette Neuinstallation von Windows Server 2012 R2 auf dem Computer. In diesem Fall sollten Sie ebenfalls vorher alle Daten von Windows Server 2008 R2 sichern. In diesem Fall müssen Sie zwar nach der Installation von Windows Server 2012 R2 alle Programme neu installieren und die Daten manuell übernehmen, erhalten dafür aber ein neues, sauberes System. Der Nachteil ist, dass Ihr bisheriges Windows Server 2008 R2-System dann verloren ist. Sie können allerdings das erstellte Image verwenden und zurückspielen. Dann ist Windows Server 2008 R2 wieder einsatzbereit.

Die dritte Möglichkeit, um Windows Server 2012 R2 zu testen, ist die Installation auf einer zweiten Partition oder Festplatte des Rechners. Auch hier können Sie eine Neuinstallation von Windows Server 2012 R2 durchführen, Windows Server 2008 R2 verbleibt dabei auf der Festplatte. Bei der Installation von Windows Server 2012 R2 wird auch der Boot-Manager von Windows Server 2008 R2 durch die neue Windows Server 2012 R2-Version ersetzt, sodass Sie auch hier die neue Version von Windows Server 2012 R2 nutzen können. Daten können Sie dann per Kopiervorgang übernehmen und Ihr bestehendes Windows-System bleibt erhalten.

Die vierte Möglichkeit, um Windows Server 2012 R2 zu testen, entspricht in etwa einer Parallelinstallation. Hier nutzen Sie aber keine zweite Partition, sondern erstellen während der Installation eine virtuelle Festplatte (VHD) und installieren Windows Server 2012 R2 in diese VHD-Datei. Der Vorteil dabei ist, dass Sie dabei die Hardware Ihres Computers nutzen, das parallele Windows unangetastet bleibt und Sie dennoch Windows Server 2012 R2 produktiv nutzen. Dabei speichert Windows Server 2012 alle Daten in einer VHD-Datei, ersetzt aber den Windows Server 2008 R2-Boot-Manager. Sie können über diesen Weg auch Hyper-V testen, also in der virtuellen Festplatte die Virtualisierung installieren. Allerdings ist das nur für Testumgebungen sinnvoll, nicht für den produktiven Einsatz.

Starten Sie Windows Server 2012 R2, mountet das System die VHD-Datei und Sie können fast genauso schnell arbeiten wie mit einer echten Festplatte. Die meisten Anwender werden keinerlei Einschränkungen bemerken. Auch leistungshungrige Anwendungen wie beispielsweise zur Video- oder Fotobearbeitung funktionieren weiter. Sie können in diesen Installationen auch die anderen physischen Festplatten des Servers einbinden.

Windows Server 2012 R2 verfügt bereits standardmäßig über eine Vielzahl an Treibern. Teilweise bieten Hersteller auch bereits neue Treiberversionen für Windows Server 2012 R2 an. Finden Sie beim Hersteller Ihres Geräts keinen passenden Treiber und ist in Windows Server 2012 R2 kein Treiber integriert, können Sie auch Windows Server 2012-Treiber in Windows Server 2012 R2 nutzen. Das sollten Sie aber nur in Ausnahmefällen tun.

Programme, die in früheren Versionen von Windows laufen, funktionieren in der Regel auch unter Windows Server 2012 R2. Allerdings sollten Sie keinesfalls Systemprogramme wie Virenscanner, Optimierungstools oder Anwendungen für die Datensicherung in Windows Server 2012 R2 nutzen, die der Hersteller nicht für diese Version freigegeben hat. Auch ältere Serverprodukte sollten Sie erst mit Windows Server 2012 R2 betreiben, wenn Updates oder Patches verfügbar sind.

Installation von Windows Server 2012 R2 vorbereiten

Damit Sie Windows Server 2012 R2 installieren können, müssen Sie zunächst die Systemvoraussetzungen beachten und einige Dinge vorbereiten. Die Systemvoraussetzungen von Windows Server 2012 R2 sind folgende:

- Mindestens 1,4-GHz-Prozessor mit 64 Bit
- Mindestens 512 MB Arbeitsspeicher
- Mindestens 32 GB freier Festplattenplatz, Computer mit mehr als 16 GB Arbeitsspeicher erfordern einen größeren Speicherplatz für Auslagerungen, Ruhezustands- und Sicherungsdateien
- Super-VGA (800 x 600)-Monitor oder Monitor mit höherer Auflösung
- Tastatur und Maus (oder andere kompatible Zeigegeräte)

Bei der Installation eines Plug & Play-Geräts werden Sie unter Umständen darauf hingewiesen, dass der Treiber nicht digital signiert ist. Bei der Installation einer Anwendung, die einen nicht digital signierten Treiber enthält, wird beim Setup kein Fehler angezeigt. In beiden Fällen wird der nicht signierte Treiber von Windows Server 2012 R2 nicht geladen. Wollen Sie diese Funktion umgehen, deaktivieren Sie die Prüfung für nicht signierte Treiber:

1. Starten Sie den Computer neu, und drücken Sie beim Start die F8-Taste.
2. Wählen Sie *Erweiterte Startoptionen* aus.
3. Wählen Sie *Erzwingen der Treibersignatur deaktivieren* aus.
4. Starten Sie Windows Server 2012 R2 und deinstallieren Sie den nicht signierten Treiber.

Weitere Informationen finden Sie unter *http://go.microsoft.com/fwlink/?LinkId=66577* [Ms179-K02-02].

Wenn der Computer mit einer unterbrechungsfreien Stromversorgung (USV) verbunden ist, trennen Sie vor dem Ausführen von Setup das serielle oder USB-Kabel dieses Geräts. Das Installationsprogramm von Windows Server 2012 R2 versucht automatisch die Geräte an den seriellen oder USB-Anschlüssen zu erkennen. Eine USV kann zu Problemen bei diesem Vorgang führen und die Installation deutlich ausbremsen oder sogar mit einem Fehler abbrechen lassen.

Sichern Sie den Server. Ihre Sicherung sollte alle erforderlichen Daten und Konfigurationsdateien für eine ordnungsgemäße Ausführung des Servers einschließen. Daten wie die Einstellungen von DHCP-Servern, Netzwerkeinstellungen, aber auch andere Daten sind wichtig für den Betrieb des Servers nach der Installation.

Deaktivieren Sie die Virenschutzsoftware des Netzwerks für diesen Server, genauso wie die Überwachung durch Managementlösungen.

Windows Server 2012 R2 installieren

In diesem Abschnitt erläutern wir Ihnen, wie Sie Windows Server 2012 R2 ganz neu installieren. Wir zeigen Ihnen auch, wie Sie Windows Server 2012 R2 über einen USB-Stick installieren. Die Installation über einen USB-Stick läuft schneller ab und Sie können damit Windows Server 2012 R2 auch auf Geräten installieren, die über kein DVD-Laufwerk verfügen.

Die Bereitstellung von Windows Server 2012 R2 basiert auf Images. Bei Images handelt es sich sozusagen um eine Kopie eines installierten Betriebssystems. Windows Server 2008 R2/Windows Server 2012/2012 R2 arbeiten mit dem WIM-Imageformat (Microsoft Windows Imaging). Statt eines sektorbasierten Imageformats 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. Mit WIM können auf dem Zielvolumen vorhandene Daten beibehalten werden. Das Einrichten eines Images löscht nicht zwingend alle vorhandenen Daten auf der Festplatte.

Windows Server 2012 R2 – Installation durchführen

Unabhängig davon, ob Sie Windows Server 2012 R2 über eine DVD oder einen USB-Stick installieren, müssen Sie den entsprechenden Datenträger mit dem Computer verbinden und im BIOS oder den Booteinstellungen vom Datenträger aus starten. Anschließend beginnt der Installations-Assistent von Windows Server 2012 R2 mit seiner Arbeit. In den meisten Fällen erscheint das Bootmenü nach dem Drücken einer Taste auf der Tastatur. Welche das ist, sehen Sie beim Starten des Rechners.

Die Installation von Windows Server 2012 R2 findet bereits beim Starten in einer grafischen Oberfläche statt. Außerdem werden weniger Fenster angezeigt und es sind weniger Eingaben für die Installation erforderlich. Außerdem werden die meisten Eingaben bereits vor Beginn der Installation durchgeführt, sodass der Computer während der Installation nicht die ganze Zeit beaufsichtigt werden muss. Sie benötigen für die Installation ein bootfähiges DVD-Laufwerk oder einen USB-Stick.

Im ersten Schritt wählen Sie die Installationssprache, das Uhrzeit- und Währungsformat sowie die Tastatur- oder Eingabemethode aus und klicken auf *Weiter*.

Auf der nächsten Seite starten Sie entweder mit *Jetzt installieren* die eigentliche Installation oder durch Auswahl von *Computerreparaturoptionen* die Systemwiederherstellung von Windows Server 2012 R2 (siehe Kapitel 35). Bis hierhin gibt es noch keine Unterschiede zur Installation von Windows Server 2008 R2 bzw. Windows Server 2012.

Abbildg. 2.1 Starten einer Windows Server 2012 R2-Installation

Starten Sie die Installation, müssen Sie im nächsten Schritt den Product Key eingeben, wenn Sie keine spezielle Edition von Windows Server 2012 R2 einsetzen. Sie können dazu entweder die Tastatur des Rechners oder die Bildschirmtastatur nutzen.

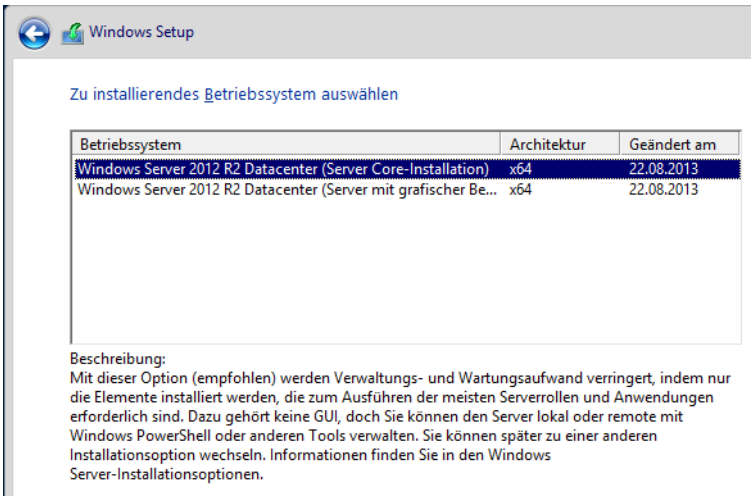
TIPP Mit der Freeware ProduKey von *http://www.nirsoft.net/utils/product_cd_key_viewer.html* [Ms179-K02-03] können Sie durch einfachen Start, also ohne Installation, die Product ID und den Product Key für installierte Office-Editionen und Windows Server 2008 R2 auslesen und anzeigen. Das Tool kann nicht den Product Key von Windows 8/8.1 und Windows Server 2012/R2 auslesen. Für Windows 8 und höher und Windows Server 2012 und höher verwenden Sie das Tool Windows 8 Product Key Viewer (*http://forums.mydigitallife.info/threads/30363-Windows-8-Product-Key-Viewer* [Ms179-K02-04] oder *http://www.chip.de/downloads/Windows-8-Product-Key-Viewer_58663752.html* [Ms179-K02-05]).

Im nächsten Schritt wählen Sie aus, ob Sie eine Server Core-Installation oder eine Installation eines Servers mit grafischer Oberfläche durchführen möchten. Die Installation als Core-Server ist standardmäßig ausgewählt. Das ist ein großer Unterschied im Vergleich zu Windows Server 2008 R2. Bei dieser Version war die Installation mit grafischer Benutzeroberfläche die Voreinstellung.

Sie können nach der Installation von Windows Server 2012 R2 als Core-Server aber die grafische Oberfläche nachinstallieren; die ist ein weiterer Unterschied zu Windows Server 2008 R2. Außerdem können Sie auf Servern mit grafischer Benutzeroberfläche diese deinstallieren und erhalten auf diesem Weg einen Core-Server.

Ein Core-Server verfügt über keine grafische Oberfläche, keine Shell, keine Mediafunktionen und keinerlei Zusatzkomponenten außer den notwendigen Serverdiensten. Der Anmeldebildschirm 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 Eingabeaufforderung.

Abbildg. 2.2 Auswählen der Installationsvariante von Windows Server 2012 R2



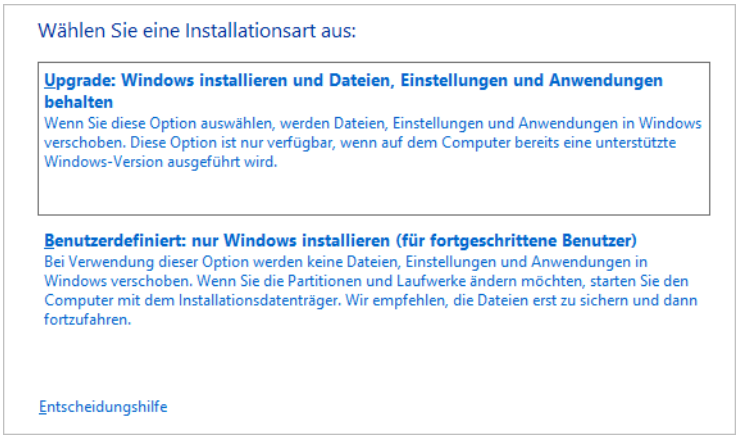
Zur Bearbeitung des Servers können Sie den Editor (Notepad) öffnen, aber zum Beispiel keinen Windows-Explorer oder Internet Explorer und keinen Registrierungs-Editor (Regedit). Durch diese Funktion können die Standardfunktionen von Windows Server 2012 R2 betrieben werden, ohne dass der Server durch unwichtige Komponenten belastet oder kompromittiert werden kann. Als Serverrollen können Sie auf Core-Servern folgende Rollen installieren:

- Active Directory-Zertifikatdienste (siehe Kapitel 30)
- Active Directory-Domänendienste (siehe Kapitel 11 bis 19)
- DHCP-Server (siehe Kapitel 24)
- DNS-Server (siehe Kapitel 25)
- Dateidienste (einschließlich Ressourcen-Manager für Dateiserver, siehe Kapitel 20 bis 23)
- Active Directory Lightweight Directory Services (AD LDS)
- Hyper-V (siehe Kapitel 7, 8 und 9)
- Druck- und Dokumentdienste (siehe Kapitel 20 bis 23)
- Streaming Media-Dienste
- Webserver (einschließlich ASP.NET, siehe Kapitel 27)
- Windows Server Update Services (siehe Kapitel 37)
- Active Directory-Rechteverwaltungsserver (siehe Kapitel 33)
- Routing- und RAS-Server (siehe Kapitel 32)

Mehr zu diesem Thema lesen Sie auch in Kapitel 3 und 4.

Um einen Server neu zu installieren, wechseln Sie zur nächsten Seite des Assistenten und bestätigen die Lizenzbedingungen. Wählen Sie danach aus, ob Sie ein bereits installiertes Betriebssystem aktualisieren oder Windows Server 2012 R2 neu installieren möchten. Bei einer Neuinstallation wählen Sie *Benutzerdefiniert* aus. Wollen Sie eine Aktualisierung durchführen, wählen Sie *Upgrade*.

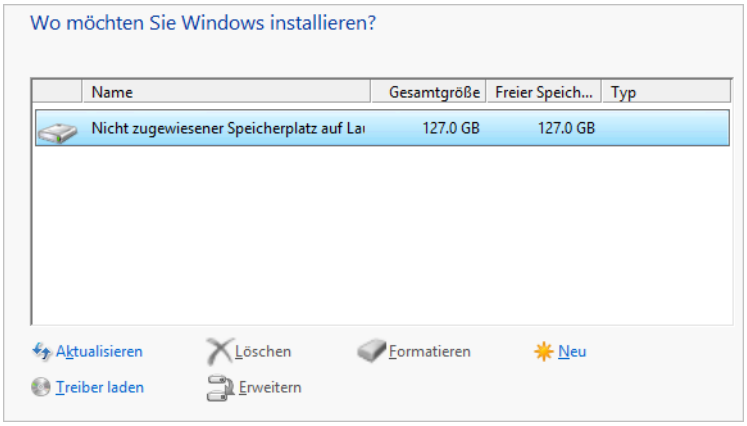
Abbildg. 2.3 Auswählen der Installationsvariante



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 Setupprogramm aus jener Windows-Installation heraus starten, die Sie aktualisieren wollen. Booten Sie das Windows Server 2012 R2-Installationsprogramm von DVD, ist nur die Option *Benutzerdefiniert* sinnvoll.

Nachdem Sie die Installationsart ausgewählt haben, gelangen Sie zum nächsten Fenster der Installationsoberfläche. Hier wählen Sie die Partition aus, auf der Windows Server 2012 R2 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. 2.4 Auswählen der Partition für die Installation



Möchten Sie die Partitionierung ändern oder eine Partition zunächst löschen, klicken Sie auf den Link *Erweitern*. Daraufhin werden weitere Auswahlmöglichkeiten angezeigt, über die Sie Partitionen

auf Ihren Laufwerken erstellen, Partitionen löschen und bestehende Partitionen auf frei verfügbaren Festplattenplatz erweitern können.

Systempartitionen und Startpartitionen sind Bezeichnungen für Partitionen oder Volumes auf einer Festplatte, die zum Starten von Windows verwendet werden. Die Systempartition enthält die hardwarebezogenen Dateien, die einem Computer mitteilen, von wo aus Windows gestartet werden kann. Eine Startpartition ist eine Partition, welche die Windows-Betriebssystemdateien enthält, die sich im Windows-Dateiordner befinden.

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. Eine Startpartition ist eine Partition, die Windows-Betriebssystemdateien enthält.

Mit einem Klick auf *Weiter* beginnt die Installation. Diese ist wie bei Windows Server 2008/R2/2012 imagebasiert und kann so deutlich schneller durchgeführt werden, als noch die Installation von Windows Server 2003.

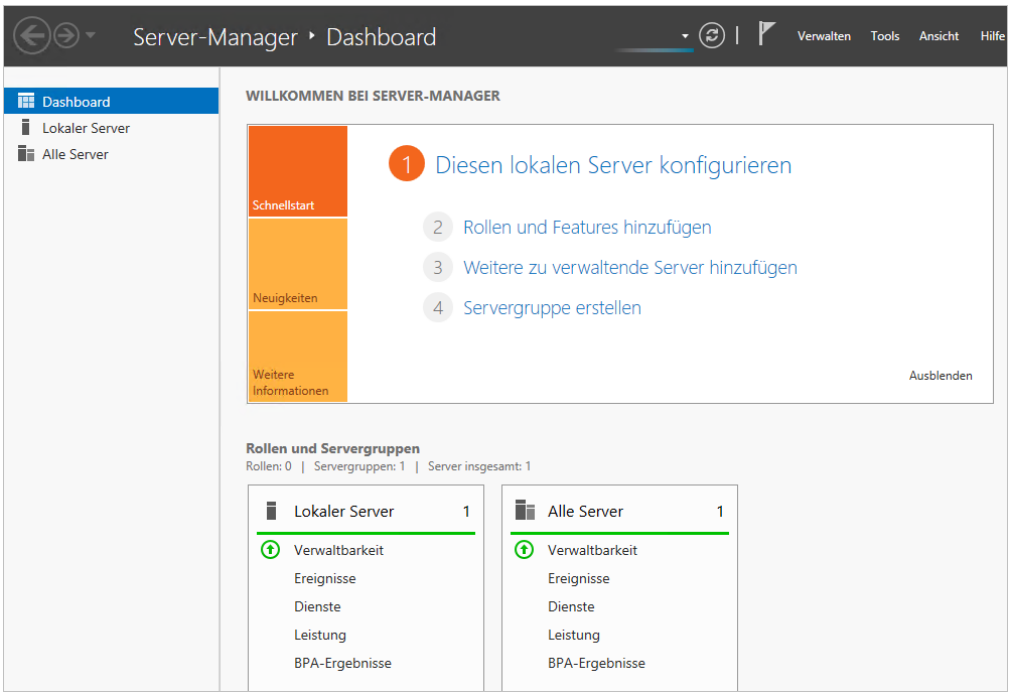
Abhängig von der Leistung des Rechners startet die Installationsroutine den Computer nach 10 bis 20 Minuten automatisch neu. Sie müssen keine weiteren Eingaben durchführen und keine Taste drücken. Sollten Sie versehentlich eine Taste gedrückt haben und die Installation startet wieder von der DVD, schalten Sie den Rechner aus und starten 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.

Sobald der Assistent seine Arbeit abgeschlossen hat, erscheint die Abfrage für das gewünschte Administratorkennwort, das Sie zur Sicherheit zwei Mal nacheinander eingeben müssen. Achten Sie beim Kennwort darauf, mindestens einen Großbuchstaben und eine Zahl oder ein Sonderzeichen zu verwenden.

Anschließend melden Sie sich mit der Tastenkombination Strg + Alt + Entf am Server an. Als Anmeldenamen verwenden Sie *Administrator* und das zuvor festgelegte Kennwort. In Windows Server 2012 R2 startet nach der Anmeldung automatisch der Server-Manager (siehe Kapitel 3). Wollen Sie das nicht, können Sie die Willkommen-Kachel und den Autostart verhindern.

Abbildg. 2.5 Windows Server 2012 startet den Server-Manager nach der Installation

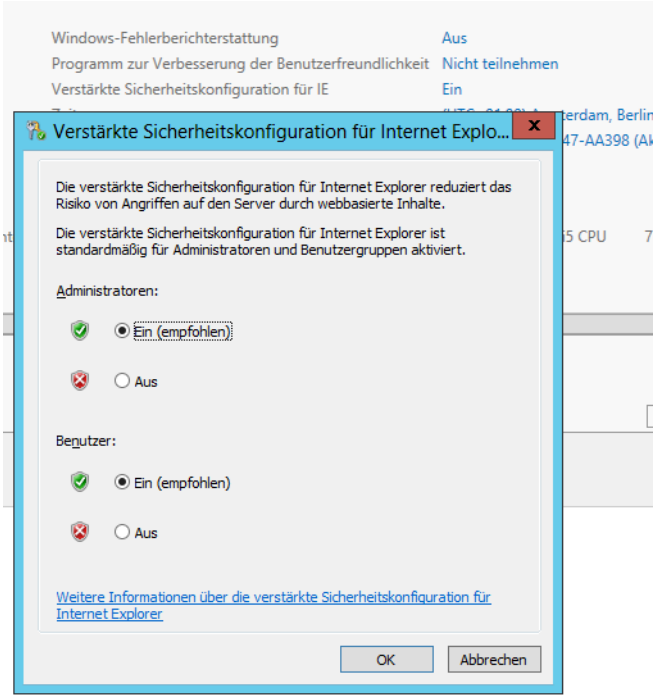


TIPP Über das Menü *Ansicht* deaktivieren Sie die Willkommen-Kachel, über *Verwalten/Server-Manager-Eigenschaften* aktivieren Sie das Kontrollkästchen *Server-Manager beim Anmelden nicht automatisch starten*, wenn Sie nicht wollen, dass der Server-Manager automatisch mit Windows starten soll.

Für die Installation von Treibern benötigen Sie normalerweise den Internet Explorer. Bei Windows Server 2012 R2 ist automatisch die verstärkte Sicherheit des Internet Explorers aktiv, was beim Herunterladen von Treibern durchaus stören kann. Sie können die erweiterte Sicherheit des Internet Explorers im Server-Manager deaktivieren:

1. Öffnen Sie den Server-Manager.
2. Klicken Sie auf der linken Seite auf *Lokaler Server*.
3. Klicken Sie im rechten Bereich im Abschnitt *Eigenschaften* neben *Verstärkte Sicherheitskonfiguration für IE* auf den Link *Ein*.
4. Deaktivieren Sie im daraufhin geöffneten Dialogfeld die Option für alle Benutzer oder nur für Administratoren.

Abbildg. 2.6 Anpassen der verstärkten Sicherheitskonfiguration für den IE



USB-Stick für Windows Server 2012 R2 erstellen

Liegen Ihnen die Windows Server 2012 R2-Installationsdateien im ISO-Format vor, können Sie die ISO-Datei einfach mit einem Archivierungsprogramm entpacken. Dazu laden Sie zum Beispiel die Freeware 7-Zip (*http://www.7-zip.de* [Ms179-K02-06]) herunter. In Windows Server 2012/R2 sowie Windows 8/8.1 können Sie die ISO-Datei auch mit Bordmitteln über das Kontextmenü oder über einen Doppelklick im Explorer bereitstellen.

Anschließend verbinden Sie den Stick mit einem Windows-Computer und bereiten diesen für die Windows Server 2012 R2-Installation vor. Verwenden Sie einen Computer mit Windows Server 2008/R2 bzw. Windows 7 oder Windows Server 2012/R2 bzw. Windows 8/8.1, da nur hier die entsprechenden Tools verfügbar sind.

Sie können den USB-Stick auch zukünftig für das Speichern von Daten nutzen. Die Installationsdateien belegen etwa einen Platz von 3,5 GB:

1. Starten Sie eine Eingabeaufforderung über das Kontextmenü im Administratormodus. Geben Sie dazu zum Beispiel *cmd* auf der Startseite ein, klicken Sie mit der rechten Maustaste auf die daraufhin angezeigte Kachel für die Eingabeaufforderung und klicken Sie im Kontextmenü auf *Als Administrator ausführen*. In Windows 8/8.1 funktioniert dies genauso. In Windows Server 2008/2008 R2 und Windows 7 geben Sie den Befehl im Suchfeld des Startmenüs ein.
2. Geben Sie *diskpart* ein.
3. Geben Sie *list disk* ein.

4. Geben Sie den Befehl *select disk <Nummer des USB-Sticks aus list disk>* ein. Sie erkennen den Stick an dessen Größe.
5. Geben Sie *clean* ein.
6. Geben Sie *create partition primary* ein.
7. Geben Sie *active* ein, um die Partition zu aktivieren. Dies ist für den Bootvorgang notwendig, denn nur so kann der USB-Stick booten.
8. Formatieren Sie den Datenträger mit *format fs=fat32 quick*.
9. Geben Sie den Befehl *assign* ein, um dem Gerät im Explorer einen Laufwerkbuchstaben zuzuordnen.
10. Beenden Sie Diskpart mit *exit*.
11. Kopieren Sie den kompletten Inhalt der Windows Server 2012 R2-DVD in den Stammordner des USB-Sticks.
12. Booten Sie einen Computer mit diesem Stick, startet die Windows Server 2012 R2-Installation.

Zu Windows Server 2012 R2 aktualisieren

Im folgenden Abschnitt zeigen wir Ihnen, wie Sie ein bestehendes Windows Server 2008 R2-System direkt zu Windows Server 2012 R2 aktualisieren. Sie können entweder identische Editionen aktualisieren, also Windows Server 2008 R2 Standard zu Windows Server 2012 R2 Standard, oder zu höherwertigen Editionen, also Standard-Edition zu Datacenter-Edition. Direkte Aktualisierungen können Sie nur von Windows Server 2008/2008 R2/2012 durchführen. Vor der Aktualisierung sollten Sie das aktuellste Service Pack installieren, also Service Pack 1 für Windows Server 2008 R2 und Service Pack 2 für Windows Server 2008 x64.

HINWEIS Von 32-Bit-Versionen, also Windows Server 2008 x86, können Sie nicht direkt zu Windows Server 2012 R2 aktualisieren. In diesem Fall müssen Sie den Server neu installieren. Sie können auch nicht zwischen Sprachversionen wechseln.

Windows Server 2003 (R2) lässt sich nicht direkt auf Windows Server 2012 R2 installieren. Da Windows Server 2012 R2 nur als 64-Bit-System zur Verfügung steht, können Sie nur von Windows Server 2008/2008 R2 direkt auf Windows Server 2012 R2 aktualisieren. Abhängig von der eingesetzten Edition stehen verschiedene Aktualisierungspfade zur Verfügung. In der Tabelle 2.1 zeigen wir Ihnen die unterstützten Pfade zur Aktualisierung.

Tabelle 2.1 Mögliche Pfade zur Aktualisierung zu Windows Server 2012

Windows Server 2008/2008 R2-Edition	Mögliche Aktualisierung zu Windows Server 2012 R2
Standard, Enterprise	Standard, Datacenter
Datacenter	Datacenter
Windows Web Server 2008/2008 R2	Standard

HINWEIS Core-Installationen von Windows Server 2008/2008 R2 lassen sich nur zu Core-Installationen von Windows Server 2012 R2 aktualisieren. Nach der Installation können Sie aber auf Wunsch die grafische Benutzeroberfläche installieren oder die minimale Serverschnittstelle aktivieren (siehe Kapitel 3).

Erstellen einer Systemabbildsicherung oder virtuellen Festplatte des alten Systems

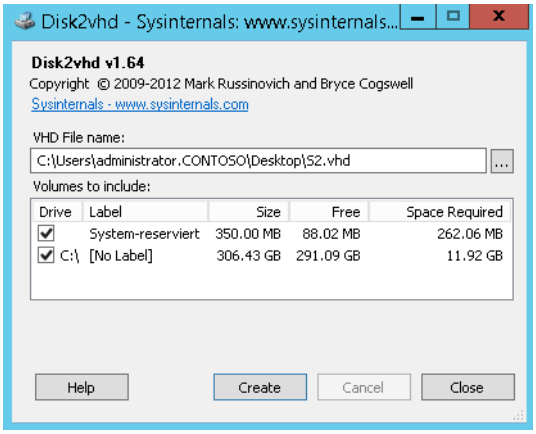
Bevor Sie Windows Server 2008/2008 R2 zu Windows Server 2012 aktualisieren, sollten Sie eine Systemabbildsicherung erstellen. Der Vorteil dabei ist, dass Sie bei Problemen schnell und einfach Ihr bisheriges Windows Server 2008/2008 R2-System wiederherstellen können.

Mit dem kostenlosen Tool Disk2vhd von Sysinternals können Sie physische Festplatten in eine VHD-Datei sichern und diese später zur Wiederherstellung von Daten nutzen. Die VHD-Datei können Sie auch in Windows Server 2012 R2 als Festplatte einbinden. Dazu starten Sie den Festplatten-Manager durch Eingabe von *diskmgmt.msc* auf der Startseite und fügen die virtuelle Festplatte an.

Nach dem Download von Disk2vhd (*http://technet.microsoft.com/de-de/sysinternals/ee656415* [Ms179-K02-07]) können Sie das Tool direkt ohne Installation starten. Legen Sie zunächst den Pfad und den Namen der anzulegenden VHD-Datei fest.

Bestimmen Sie anschließend, welche physischen Festplatten in der Sicherung enthalten sein sollen und klicken Sie auf *Create*. Daraufhin erstellt der Assistent die VHD-Datei. Diese lässt sich in alle Virtualisierungslösungen einbinden, die mit VHD-Dateien umgehen können. Im Startfenster sehen Sie auch, welche Größe die VHD-Datei nach dem Erstellen haben wird. Disk2vhd unterstützt Windows ab XP SP2, also auch Windows Server 2008/2008 R2. Auch in Windows Server 2012 und Windows 8/8.1 können Sie das Tool nutzen. Neben 32-Bit-Systemen können Sie das Tool ebenfalls unter 64-Bit-Systemen einsetzen.

Abbildg. 2.7 Mit Disk2vhd physische Festplatten in VHD-Dateien umwandeln



Einer der größten Vorteile dieses Tools ist, dass das zu sichernde System normal weiterlaufen kann. Bei den meisten Computern müssen Sie den Rechner kompliziert mit Boot-CDs starten, von denen

meist nicht genügend Festplattenplatz oder eine Verbindung zum Netzwerk zur Verfügung gestellt wird. Das Tool baut auf den Windows-Schattenkopien auf, um eine konsistente Momentaufnahme (Snapshot) eines Computers erstellen zu können.

Erstellen Sie mehrere Images gleichzeitig von mehreren eingebauten Festplatten, legt Disk2vhd für jede physische Festplatte eine eigene VHD-Datei. Sie können Festplatten auch abwählen und so beispielsweise nur Systempartitionen sichern und Datenpartitionen übergehen.

Unter Windows Server 2008/2008 R2 und Windows Server 2012/2012 R2 können Sie die VHD-Dateien ebenfalls direkt in das Betriebssystem einbinden. Allerdings sollten Sie auf einem Computer nicht die VHD-Datei booten, die der Systempartition des Rechners entspricht. Ansonsten besteht die Gefahr, dass das Betriebssystem mit den Signaturen der Festplatten durcheinander kommt. Sie können Disk2vhd auch über die Eingabeaufforderung starten. Die Syntax dafür lautet:

```
disk2vhd <[drive: [drive:]...]|[*]> <VHD-Datei>
```

Ein Beispiel für den Aufruf wäre:

```
disk2vhd * c:\vhd\snapshot.vhd
```

Verwenden Sie statt einem Laufwerkbuchstaben den Platzhalter *, sichert das Tool alle Festplatten des Computers.

Kopieren Sie die Festplatte auf einen Computer mit Windows Server 2012/2012 R2 oder Windows 8/8.1, können Sie über die Festplattenverwaltung und den Menübefehl *Aktion/Virtuelle Festplatte anfügen* die VHD-Datei bereitstellen. So erhalten Sie Zugriff auf den Inhalt über den normalen Explorer und können die VHD-Datei als Datensicherung nutzen. Sie müssen die Festplatte über das Kontextmenü anschließend noch online schalten. Der Explorer richtet daraufhin ein Laufwerk ein, über das Sie auf den Inhalt zugreifen können. Enthält die Festplatte mehrere Partitionen, legt Windows für jede Partition ein eigenes Laufwerk im Explorer an.

Beachten Sie vor der Aktualisierung die folgenden wichtigen Aktionen:

- Bevor Sie einen Server direkt auf Windows Server 2012 R2 aktualisieren, sollten Sie zunächst installierte Sicherheitsprogramme und Antivirenschutzprogramme deaktivieren
- Arbeiten Sie mit Netzwerküberwachungsprogrammen sollten Sie beachten, dass Sie den zu aktualisierenden Computer in den Wartungsmodus versetzen
- Achten Sie darauf, dass alle installierten Anwendungen, Management Packs für Netzwerküberwachungsprogramme und Tools kompatibel zu Windows Server 2012 R2 sind. Aktualisieren Sie die Programme nach der Installation von Windows Server 2012 R2.
- Achten Sie darauf, dass die Windows-Firewalleinstellungen Verbindungen zu anderen Servern nicht blockieren oder bestimmte IPsec-Regeln gesetzt sind
- Falls Sie einen Domänencontroller aktualisieren, beachten Sie, dass Sie zuvor Active Directory für Windows Server 2008 R2 vorbereiten müssen. Sie benötigen dazu das Tool Adprep aus dem Ordner *\support\adprep* von der Windows Server 2012 R2-DVD.

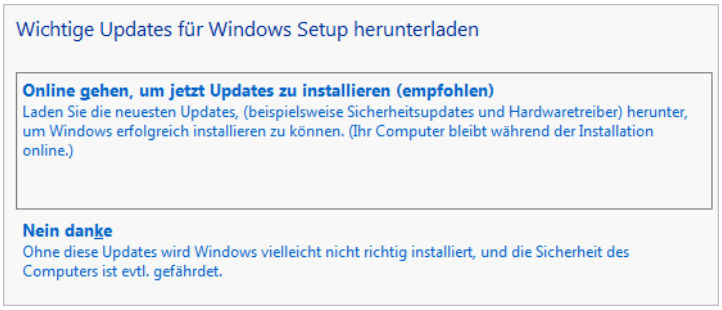
Aktualisierung zu Windows Server 2012 R2 durchführen

In diesem Abschnitt zeigen wir Ihnen, wie Sie Windows Server 2008 R2 zu Windows Server 2012 R2 aktualisieren. Dazu muss Windows Server 2008 R2 gestartet sein und fehlerfrei funktionieren. Aktualisieren können Sie von Windows Server 2008 R2 Standard/Enterprise zu Windows Server 2012 R2 Standard/Datacenter.

Sie können von Windows Server 2008 R2 Enterprise auch zu Windows Server 2012 R2 Standard aktualisieren, da die Standard-Edition in Windows Server 2012 R2 alle Funktionen von Windows Server 2008 R2 Enterprise nutzen kann. Sie können aber nicht von herkömmlichen Servern zu Core-Servern aktualisieren.

Starten Sie Windows Server 2008 R2 und legen Sie die Windows Server 2012 R2-DVD in das DVD-Laufwerk. Klicken Sie dann auf *setup.exe*, um die Installation zu starten. Klicken Sie auf *Jetzt installieren*. Im nächsten Schritt erhalten Sie die Möglichkeit, die Installationsdateien zu aktualisieren. Dazu sollten Sie die Option *Online gehen, um jetzt Updates zu installieren* auswählen. Anschließend sucht der Assistent nach Updates und bindet diese in die Installation mit ein. Dies ist nicht zwingend notwendig, aber empfohlen.

Abbildg. 2.8 Installationsdateien von Windows Server 2012 R2 vor der Installation aktualisieren

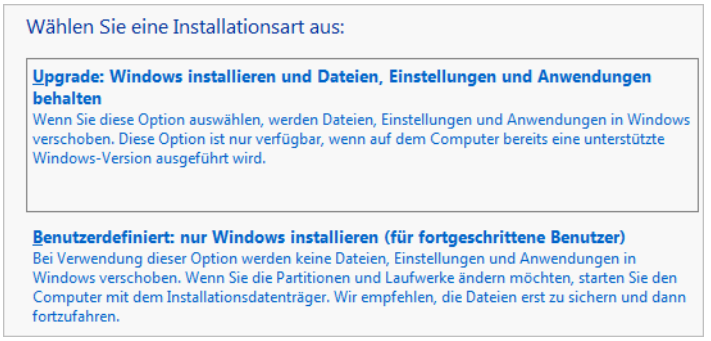


Erscheint die Abfrage des Product Key für die Installation, geben Sie den Schlüssel ein. Auf dessen Basis entscheidet es sich, ob Sie Windows Server 2012 R2 in der Standard- oder Datacenter-Edition installieren. Im unteren Feld erhalten Sie nach wenigen Sekunden den Hinweis, dass der Installations-Assistent den Schlüssel verifiziert hat. Klicken Sie dann auf *Weiter*.

Im nächsten Fenster wählen Sie aus, ob Sie einen Core-Server oder einen Server mit grafischer Benutzeroberfläche installieren wollen. Sie können von einem herkömmlichen Server mit Windows Server 2008/2008 R2 Enterprise nicht zu einer Core-Installation von Windows Server 2012 R2 Standard aktualisieren.

Im nächsten Schritt bestätigen Sie die Lizenzbedingungen. Danach erscheint ein Fenster, in dem Sie auswählen können, welche Daten Sie übernehmen wollen. Am besten belassen Sie hier die Auswahl auf *Upgrade: Windows installieren und Dateien, Einstellungen und Anwendungen behalten*. Klicken Sie auf *Weiter*, führt der Assistent noch verschiedene Vorbereitungen zur Installation durch.

Abbildg. 2.9 Auswählen der Dateien, die bei der Aktualisierung erhalten bleiben sollen



Nach einigen Tests erhalten Sie vom Installations-Assistenten den Hinweis, dass das System bereit für die Installation von Windows Server 2012 R2 ist. Klicken Sie auf *Weiter*, beginnt der Assistent mit der eigentlichen Installation. Findet der Assistent Kompatibilitätsprobleme, erhalten Sie eine Meldung angezeigt.

Nach der Installation startet der Einrichtungs-Assistent von Windows Server 2012 R2, genauso wie bei einer Neuinstallation.

Upgrade von Standard- und Testversion auf Datacenter-Edition

Haben Sie Windows Server 2012 R2 Standard installiert, können Sie auf die Datacenter-Edition aktualisieren. Sie müssen dazu Windows nicht neu installieren, die Aktualisierung kann im laufenden Betrieb erfolgen. Sie müssen lediglich nach der Aktualisierung den Server neu starten.

Zunächst geben Sie in der PowerShell den Befehl *DISM /Online /Get-TargetEditions* ein, um zu überprüfen, ob eine Aktualisierung möglich ist. Falls eine Aktualisierung möglich ist, erhalten Sie vom Tool eine Rückmeldung.

Um die Aktualisierung von Standard zu Datacenter durchzuführen, geben Sie schließlich den Befehl *DISM /Online /Set-Edition:ServerDatacenter /AcceptEula /ProductKey: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx* ein. Nach der Aktualisierung starten Sie den Server neu.

Sie haben auch die Möglichkeit, die Testversionen von Windows Server 2012 R2 (*http://technet.microsoft.com/de-de/evalcenter* [Ms179-K02-08]) zu einer vollwertigen Version umzuwandeln. Ob es sich bei der Version um eine Testversion handelt, sehen Sie durch Eingabe des Befehls *slmgr.vbs /dlv*. Auch in der Testversion sehen Sie mit *DISM /Online /Get-TargetEdition*, auf welche Edition Sie aktualisieren können.

Eine Aktualisierung nehmen Sie mit dem gleichen Befehl vor, wie bei der Aktualisierung von Standard zu Datacenter. Sie können auf diesem Weg von der Testversion von Windows Server 2012 R2 Standard zur lizenzierten Version von Windows Server 2012 Datacenter wechseln. Der Server muss dazu mindestens zweimal neu starten.

HINWEIS Sie können nicht von Vorabversionen (Preview) von Windows Server 2012 R2 zur finalen Version aktualisieren. In diesem Fall ist immer eine Neuinstallation erforderlich.

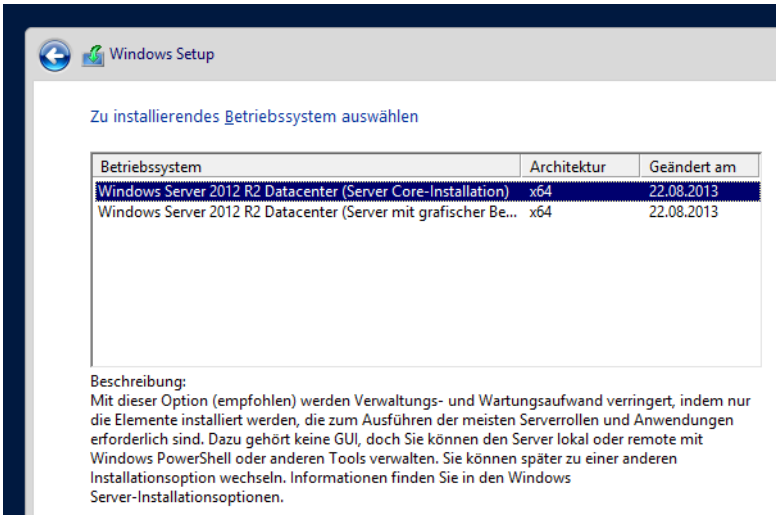
Windows Server 2012 zu Windows Server 2012 R2 aktualisieren

Sie können natürlich auch direkt von Windows Server 2012 zu Windows Server 2012 R2 aktualisieren. Dazu müssen Sie die gleichen Bedingungen einhalten, wie bei der Aktualisierung von Windows Server 2008 R2. Wenn Sie Domänencontroller zu Windows Server 2012 R2 aktualisieren wollen, müssen Sie zuerst das Schema und dann die entsprechenden Domänen auf Windows Server 2012 R2 vorbereiten. Wie Sie dabei vorgehen, lesen Sie in Kapitel 11.

Um einen Server zu Windows Server 2012 R2 zu aktualisieren, booten Sie den Server, legen die Windows Server 2012 R2-DVD ein und starten dann die Installation. Wählen Sie im Fenster *Jetzt installieren*. Es startet der Installations-Assistent. Zunächst werden temporäre Dateien kopiert, danach wählen Sie am besten die Option *Online gehen*, um jetzt Updates zu installieren. Bei diesem Vorgang lädt der Server wichtige Installationsdateien nach. Wenn der Server über keine Internetverbindung verfügt, ist das aber nicht unbedingt notwendig.

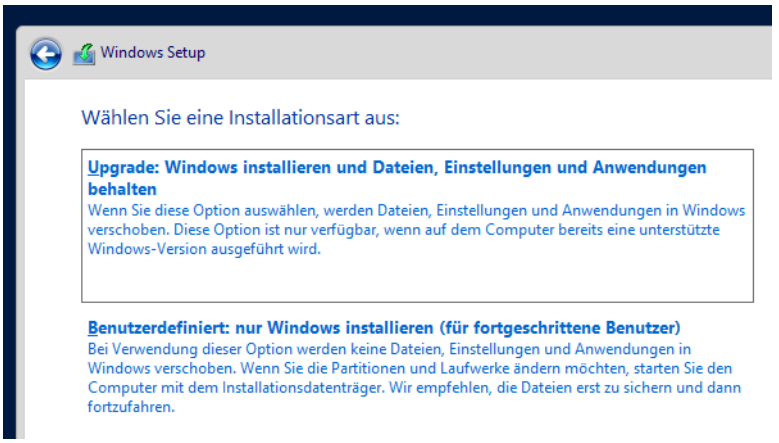
Danach müssen Sie den Produktschlüssel für Windows Server 2012 R2 eingeben. Nachdem dieser erfolgreich verifiziert wurde, wählen Sie aus, zu welcher Windows Server 2012 R2-Edition Sie den Server aktualisieren wollen.

Abbildg. 2.10 Auswählen der Edition für die Aktualisierung zu Windows Server 2012 R2



Im Anschluss bestätigen Sie die Lizenzbedingungen von Windows Server 2012 R2 und wählen dann die Option *Upgrade* aus. Hier sind die Vorgänge identisch mit der Aktualisierung von Windows Server 2012 R2.

Abbildg. 2.11 Starten der direkten Aktualisierung von Windows Server 2012 zu Windows Server 2012 R2



Im Anschluss führt der Assistent eine Prüfung der installierten Serverdienste und Anwendungen aus. Danach können Sie die Aktualisierung starten. Achten Sie aber darauf, ob die installierten Anwendungen kompatibel zu Windows Server 2012 R2 sind.

Beachten Sie, dass nicht alle Datensicherungs-Agents oder Antivirentools, die kompatibel mit Windows Server 2012 sind, auch kompatibel mit Windows Server 2012 R2 sind. Die Aktualisierung kann teilweise mehrere Stunden dauern, abhängig von Ihrer Hardwareausstattung und der Menge der zu aktualisierenden Daten.

Windows Server 2012 R2 auf virtueller Festplatte parallel installieren

Auch wenn Sie im Computer nur eine Festplatte eingebaut haben, können Sie problemlos Windows Server 2012 R2 parallel zu einem anderen Betriebssystem installieren. Dazu verwenden Sie die Möglichkeit, die bereits in Windows Server 2008 R2/2012 verfügbar war, nämlich die Installation des Betriebssystems auf eine virtuelle Festplatte, welche die Hardware Ihres Computers nutzt.

Die folgenden Abschnitte helfen auch bei der parallelen Installation von Windows Server 2012 R2 auf einer zusätzlichen Festplatte, wenn Sie keine virtuelle Festplatte verwenden. Grundsätzlich spielt es für den Boot-Manager oder das zweite installierte Betriebssystem keine Rolle, ob das zweite System auf eine virtuelle oder physische Festplatte installiert ist.

Auf diesem Weg können Sie auch Hyper-V Server 2012 R2 installieren und Windows Server 2012 R2 und Hyper-V Server 2012 R2 parallel auf einer gemeinsamen Festplatte betreiben. Natürlich ist das nur für Testumgebungen sinnvoll. Sie können mit Hyper-V Server 2012 R2 zum Beispiel Server mit Windows Server 2012 R2 Essentials virtualisieren, mit Windows Server 2012 war das noch nicht möglich.

Windows Server 2012 R2 auf einer virtuellen Festplatte installieren

Alle Daten von Windows Server 2012 R2 befinden sich nach der Installation auf dem virtuellen System. Beim Betrieb bemerken Sie davon nahezu nichts. Der Vorgang funktioniert auch mit Windows 8.1 Pro/Enterprise sowie mit Windows 7 Ultimate/Enterprise und Windows Server 2008 R2/2012. Gehen Sie dazu folgendermaßen vor:

1. Booten Sie Ihren Computer mit der Windows Server 2012 R2-DVD.
2. Bestätigen Sie im ersten Installationsfenster die Spracheinstellungen.
3. Sobald das zweite Fenster der Windows Server 2012 R2-Installation erscheint, wählen Sie nicht *Jetzt installieren*, sondern drücken Sie die Tastenkombination ⇧+F10, um eine Eingabeaufforderung zu öffnen.
4. Im nächsten Schritt geben Sie *diskpart* ein. Die nächsten Schritte bestehen darin, auf der physischen Festplatte im Computer eine neue virtuelle Festplatte als VHD-Datei zu erstellen und diese in die Windows Server 2012 R2-Installation einzubinden, die Sie gerade gestartet haben. Ihre bestehende Betriebssysteminstallation bleibt davon unberührt.
5. Zunächst erstellen Sie die virtuelle Festplatte mit dem Befehl *create vdisk file="d:\win2.vhd" type=expandable maximum=30000*. Überprüfen Sie zuvor, welcher Laufwerkbuchstabe aktuell zugewiesen ist und ersetzen Sie die Laufwerkangabe *d:* im Befehl mit dem für Ihr System gültigen Laufwerkbuchstaben. Dazu verwenden Sie in Diskpart *list disk* und *list volume* für einen Überblick. Verwenden Sie nicht den kleinen Bereich, in dem sich der Boot-Manager befindet, sondern die Datenpartition. Durch die Option *maximum* geben Sie die Größe der Platte an.
6. Haben Sie die Eingabe bestätigt, erstellt Windows Server 2012 R2 die virtuelle Festplatte. Im nächsten Schritt wählen Sie die Platte mit *select vdisk file="d:\win2"* aus.
7. Der Befehl *attach vdisk* verbindet die VHD-Datei mit der Windows Server 2012 R2-Installation, die Sie gestartet haben.

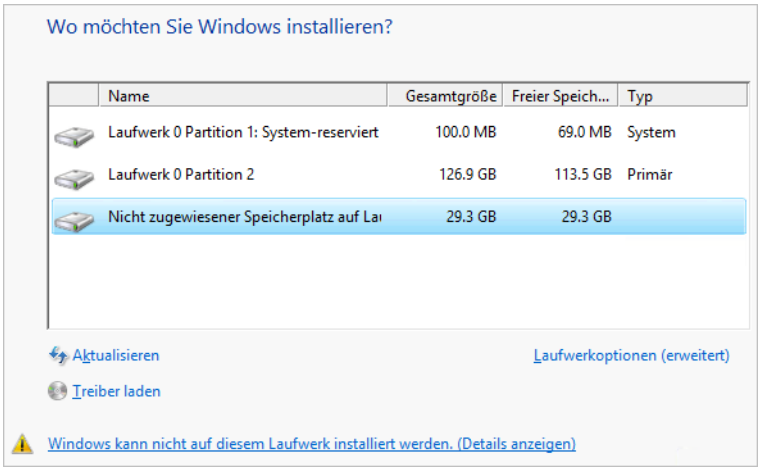
Haben Sie diese Befehle ausgeführt, schließen Sie die Eingabeaufforderung und fahren mit der Windows Server 2012 R2-Installation fort, indem Sie im Fenster auf *Jetzt installieren* klicken. Akzeptieren Sie die Lizenzbedingungen und wählen Sie bei Installationsart die Option *Benutzerdefiniert* aus.

Auf der nächsten Seite sehen Sie alle Festplatten, auch die von Ihnen erstellte virtuelle Festplatte. Diese erkennen Sie an ihrer Größe und der Fehlermeldung, wenn Sie diese auswählen. Um Windows Server 2012 R2 in dieser Festplatte zu installieren, wählen Sie sie aus. Die Meldung *Windows kann nicht auf diesem Laufwerk installiert werden* können Sie ignorieren.

Anschließend startet die Windows Server 2012 R2-Installation wie auf einer normalen Festplatte. Die Daten speichert der Installations-Assistent direkt in die VHD-Datei.

Der Installations-Assistent ersetzt auch den Boot-Manager von Windows Server 2008 R2, wenn Sie Windows Server 2012 R2 parallel zu Windows Server 2008 R2 installiert haben, bindet Windows Server 2008 R2 aber in den Windows Server 2012 R2-Boot-Manager ein.

Abbildg. 2.12 Installieren von Windows Server 2012 R2 in einer virtuellen Festplatte



Booten Sie Ihr Windows Server 2008 R2 oder ein anderes Windows Server 2012 R2-System, sehen Sie auf der Festplatte, auf der Sie die VHD-Datei angelegt haben, die VHD-Datei von Windows Server 2012 R2 als Datei im Dateisystem.

Sichern Sie diese Datei, haben Sie eine vollständige Sicherung des virtuellen Computers angelegt. Booten Sie dagegen das in der VHD-Datei installierte Windows Server 2012 R2, sehen Sie nicht die VHD-Datei, da diese im System als Festplatte eingebunden ist. Die Daten der anderen Windows Server 2008 R2-Installation sehen Sie als zusätzliche Festplatte.

Auf diese Weise können Sie zwischen den Systemen auch Daten austauschen. Alle Änderungen, die Sie im virtuellen Windows vornehmen, speichert Windows innerhalb der VHD-Datei.

Parallelinstallation durch Verkleinerung der Partition

Unter manchen Umständen kann es sinnvoll sein, Windows Server 2012 R2 parallel zu Windows Server 2008/2008 R2/2012 zu installieren, zum Beispiel, wenn Sie Daten übernehmen wollen, zum Testen oder wenn Sie beide Systeme parallel betreiben möchten. Auch wenn Ihr Rechner nur über eine Festplatte verfügt, ist das möglich. Sie können dazu den beschriebenen Weg über die virtuelle Festplatte wählen, oder eine bestehende Partition verkleinern.

Sie können mit der Windows Server 2012 R2-DVD den Computer so vorbereiten, dass beide Betriebssysteme parallel nebeneinander funktionieren. Das geht aber auch in der Festplattenverwaltung von Windows Server 2008 R2/2012. Wir zeigen Ihnen beide Möglichkeiten.

Partitionen während der Installation verkleinern

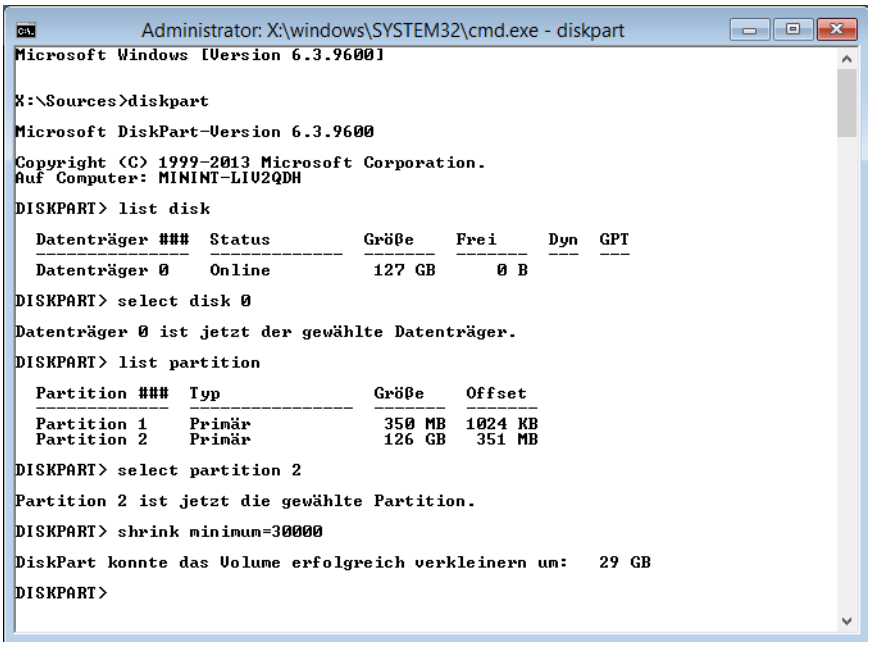
Während der Installation von Windows Server 2012 R2 können Sie eine bestehende Partition verkleinern. Im Gegensatz zur parallelen Installation über eine VHD-Datei greifen Sie dabei aber direkt in das bereits installierte System ein:

1. Starten Sie den Computer mit der Windows Server 2012 R2-DVD.
2. Klicken Sie nicht auf *Jetzt installieren*, sondern auf *Computerreparaturoptionen*.
3. Klicken Sie auf *Problembehandlung* und dann auf *Eingabeaufforderung*.

Abbildg. 2.13 Starten der Problembehandlung in Windows Server 2012

4. Tippen Sie in der Eingabeaufforderung den Befehl *diskpart* ein und bestätigen Sie. Anschließend wechselt die Eingabeaufforderung in die Diskpart-Eingabe.
5. Geben Sie *list disk* ein. Anschließend zeigt die Oberfläche die Festplatte an.
6. Geben Sie *select disk 0* ein, wenn es sich um die Festplatte 0 des Systems handelt, also der ersten Festplatte im Rechner.
7. Geben Sie *list partition* ein.
8. Geben Sie *select partition 2* ein. Hierbei kann es sich auch um eine andere Partition handeln.
9. Geben Sie *shrink minimum=30000* ein, damit Sie genügend Festplattenplatz zur Verfügung haben. Sie können hier natürlich auch deutlich mehr verkleinern, abhängig davon, wie viel Speicherplatz übrig sein soll.
10. Nach der Verkleinerung starten Sie den Rechner neu und booten von der Windows Server 2012-DVD.
11. Starten Sie die normale Installation über *Jetzt installieren*. Wählen Sie im Fenster zur Installationsauswahl aber nicht *Upgrade* aus, sondern *Benutzerdefiniert*.
12. Wählen Sie im nächsten Fenster den freien Speicherplatz aus, den Sie zuvor von der bereits installierten Windows-Systempartition verkleinert haben.
13. Anschließend beginnt Windows Server 2012 R2 mit seiner Installation. Schließen Sie diese ab und booten Sie den Rechner neu, bis das neue Bootmenü erscheint.

Abbildg. 2.14 Partition einer bestehenden Installation mit Windows Server 2012 R2 verkleinern



Partition in Windows Server 2008 R2/2012 verkleinern

Wollen Sie auf einem Rechner Windows Server 2012 R2 parallel zu Windows Server 2008 R2/2012 betreiben, können Sie eine bestehende Partition auch direkt im Betriebssystem verkleinern:

1. Starten Sie Windows Server 2008 R2/2012 und öffnen Sie den Festplatten-Manager. Tippen Sie dazu *diskmgmt.msc* im Suchfeld des Startmenüs oder in Windows Server 2012 auf der Startseite ein und bestätigen Sie.
2. Klicken Sie die Partition mit der rechten Maustaste an und wählen Sie *Volume verkleinern* aus.
3. Es startet ein Assistent, der für Sie die maximale Verkleinerung errechnet. Der verkleinerte Platz dient dann der Windows Server 2008 R2/2012-Installation als Systempartition.
4. Nach der Verkleinerung starten Sie den Rechner neu und booten von der Windows Server 2012 R2-DVD.
5. Starten Sie die normale Installation über *Jetzt installieren*. Wählen Sie im Fenster zur Installationsauswahl aber nicht *Upgrade* aus, sondern *Benutzerdefiniert*.
6. Wählen Sie im nächsten Fenster den freien Speicherplatz aus, den Sie zuvor von der Windows Server 2008 R2/2012-Systempartition verkleinert haben.
7. Anschließend beginnt Windows Server 2012 R2 mit der Installation. Schließen Sie diese ab und booten Sie den Rechner neu, bis das neue Bootmenü erscheint. Hier lässt sich dann bei jedem Start auswählen, welches Betriebssystem Sie starten wollen.

HINWEIS Haben Sie Windows Server 2012 R2 parallel zu einem anderen Betriebssystem installiert, stehen die installierten Anwendungen auf dem jeweils anderen Betriebssystem nicht zur Verfügung. Sie müssen diese jeweils parallel installieren. Bei manchen Programmen besteht die Möglichkeit, dass Sie diese auf beiden Betriebssystemen in die gleichen Ordner installieren, das spart oft Speicherplatz.

Boot-Manager-Optionen ändern

Haben Sie mehrere Betriebssysteme installiert und verwenden den Windows Server 2012-Boot-Manager, da Sie dieses Betriebssystem als Letztes installiert haben, wird dieses als Standardsystem gestartet.

Wollen Sie das Windows Server 2012 R2-Testsystem wieder entfernen oder den Windows Server 2008 R2-Boot-Manager verwenden, starten Sie am besten Windows Server 2008 R2, rufen dann das *Ausführen*-Dialogfeld mit ⊞ + R auf und tippen *msconfig* ein.

Anschließend können Sie auf der Registerkarte *Start* den Windows Server 2008 R2-Boot-Manager markieren und zum Standardsystem machen. Nach dem nächsten Start erscheint wieder das Windows Server 2008 R2/2012-Startmenü. In diesem ist Windows Server 2012 R2 ebenfalls eingebunden. Sie können diese Einstellungen später auch in Windows Server 2012 R2 durchführen, auch hier gibt es noch Msconfig.

Ist das System nicht eingebunden, können Sie dies über *bootrec /rebuildbcd* nachholen. Verwalten können Sie später die Einstellungen am besten über Msconfig.

Installieren Sie Windows Server 2012 R2 nicht über eine virtuelle Festplatte, sondern in einer echten Partition, ändern Sie auch hier den Standardeintrag über Msconfig in Windows Server 2008 R2 und formatieren dann die Partition mit Windows Server 2012 R2 einfach neu, wenn Sie Windows Server 2012 R2 wieder entfernen wollen.

Um die in eine VHD-Datei installierte Windows Server 2012 R2-Version von Ihrem System zu entfernen, starten Sie Windows Server 2008 R2/2012 und löschen die VHD-Datei. Starten Sie dann Msconfig in Windows Server 2008 R2 und setzen Sie Windows Server 2008 R2/2012 als Standardsystem. Hier löschen Sie auch den Booteintrag von Windows aus dem Menü. Geht bei diesen Vorgängen etwas schief, können Sie auch mit der Windows Server 2008 R2/2012-DVD booten und mit den beschriebenen Wegen das System wiederherstellen.

Wenn Sie Windows Server 2012 R2 parallel zu Windows Server 2008 R2/2012 installieren und Windows Server 2008 R2/2012 starten wollen, achten Sie darauf, vorher Windows Server 2012 R2 komplett herunterzufahren. Ansonsten versucht Windows Server 2008 R2 teilweise die lokale Festplatte mit Checkdisk (Chkdsk) zu reparieren, was Zeit kostet. Das passiert bei Testumgebungen, wenn Sie den Server zum Beispiel einfach ausschalten.

Windows Server 2012 R2 Essentials installieren

Die Installation von Windows Server 2012 Essentials unterscheidet sich etwas von der herkömmlichen Installation von Windows Server 2012 R2. Die Essentials-Edition übernimmt bei der Installation auch gleich die Einrichtung einer Active Directory-Domäne. Installieren Sie Windows Server 2012 R2 Essentials als Serverrolle, wird keine Domäne erstellt, sondern der Server verbleibt Mitglied in der entsprechenden Domäne. Mehr dazu finden Sie in Kapitel 41.

Die Verwaltung erfolgt anschließend über das Dashboard. Der Server-Manager ist zwar auch hier verfügbar, das zentrale Verwaltungswerkzeug ist allerdings das Dashboard.

Die grundsätzliche Installation des Servers läuft ähnlich ab wie die Installation von Windows 8.1 oder Windows Server 2012 R2. Um Windows Server 2012 R2 Essentials auf einem Server zu installieren, legen Sie die DVD ein und booten mit dieser. Es startet der Installations-Assistent. Sie wählen wie bei den anderen Editionen aus, welche Sprache Sie installieren wollen und geben danach den Product Key ein. Anschließend bestätigen Sie die Lizenzbedingungen und starten die Installation. Die Installation als Serverrolle beschreiben wir in Kapitel 41. Nachfolgend gehen wir darauf ein, wie Sie Windows Server 2012 R2 Essentials auf einem alleinstehenden Server installieren.

TIPP Windows Server 2012 R2 Essentials ist auch für die Virtualisierung freigegeben. Sie können die Version jetzt zum Beispiel mit Hyper-V Server 2012 R2 virtualisieren und auf dem Host weitere virtuelle Server erstellen. Mit Windows Server 2012 Essentials war das noch nicht möglich.

Auf der nächsten Seite wählen Sie die Festplatte aus, auf der Sie den Server installieren wollen. Reicht der Festplattenplatz nicht aus, erhalten Sie eine Fehlermeldung und die Installation bricht ab. Die Installationsfestplatte für Windows Server 2012 R2 Essentials muss mindestens 160 GB groß sein. Steht weniger Platz zur Verfügung, zum Beispiel durch eine falsche Partitionierung, müssen Sie die Installation neu beginnen. Der Installations-Assistent lässt sich nicht fortsetzen.

Der Installations-Assistent verwendet immer die komplette Festplatte des Servers und führt automatisch eine Partitionierung durch. Bereits vorhandene Daten auf dem Server gehen verloren. Der Server benötigt aber nur etwas 20 GB Festplattenplatz. Den Rest benötigt der Assistent für die Ablage der Daten.

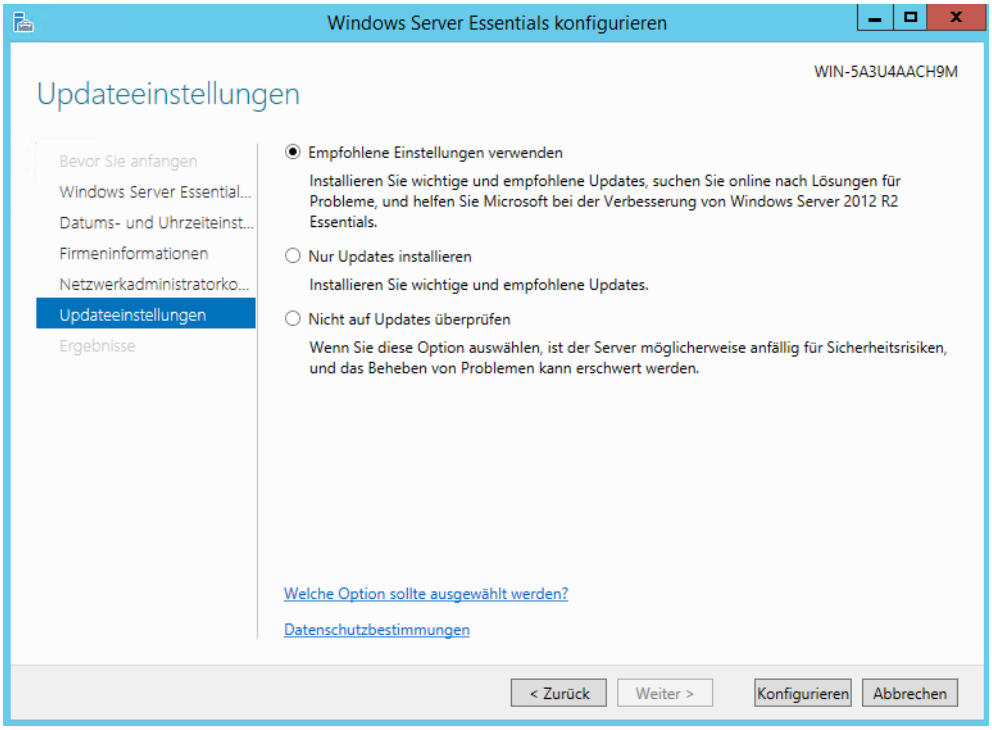
TIPP Wenn Sie den Server in einer Testumgebung mit Hyper-V installieren, sollten Sie keine dynamische Zuordnung des Arbeitsspeichers nutzen (siehe Kapitel 7), sondern einen festen Arbeitsspeicher von mindestens 2 GB zuteilen.

Nach dem Start der Installation läuft diese ähnlich ab wie bei anderen Editionen von Windows Server 2012 R2. Zunächst installiert der Assistent das Basisbetriebssystem auf dem Server. Danach startet die Installation der zusätzlichen Komponenten und die Einrichtung des Servers zu einem Domänencontroller. Aktivieren Sie die Essentials-Funktionen als Serverrolle, wird der Server nicht zum Domänencontroller heraufgestuft, sondern ist Mitgliedsserver der Domäne. Diese Vorgänge zeigen wir Ihnen in Kapitel 41.

Während der Installation des Betriebssystems müssen Sie keine weiteren Eingaben vornehmen. Schließt der Assistent die Installation von Windows ab, findet eine automatische Anmeldung statt und die Integration der Essentials-Komponenten beginnt automatisch.

Im Installations-Assistenten wählen Sie als Nächstes das Land, das Uhrzeit- und Währungsformat sowie das Tastaturlayout aus. Anschließend können Sie die Uhrzeit und das Datum überprüfen und gegebenenfalls anpassen. Achten Sie darauf, dass die Zeit genau stimmt. Danach geben Sie den Benutzernamen und das Kennwort des Administrators ein. Der Assistent legt den Benutzer an. Auch die zukünftige Installation von Windows-Patches steuern Sie während der Einrichtung.

Abbildg. 2.15 Anpassen der Updateeinstellungen von Windows Server 2012 R2 Essentials



Achten Sie darauf, Werte zu verwenden, die leicht einzugeben sind, da Anwender diese zum Verbinden mit dem Server benötigen. Verwenden Sie auch keinesfalls die Standardvorgaben.

Am besten geben Sie als Domänennamen Ihren Firmennamen oder eine Kurzform an. Auch den Servernamen sollten Sie so kurz wie möglich wählen. Sie können diese Eingaben nach der Installation nicht mehr ändern.

Achten Sie bei der Eingabe des Administratorbenutzers darauf, nicht den Standardnamen Administrator, sondern einen anderen Benutzernamen oder Namen wie *superuser* oder *adminuser* zu verwenden.

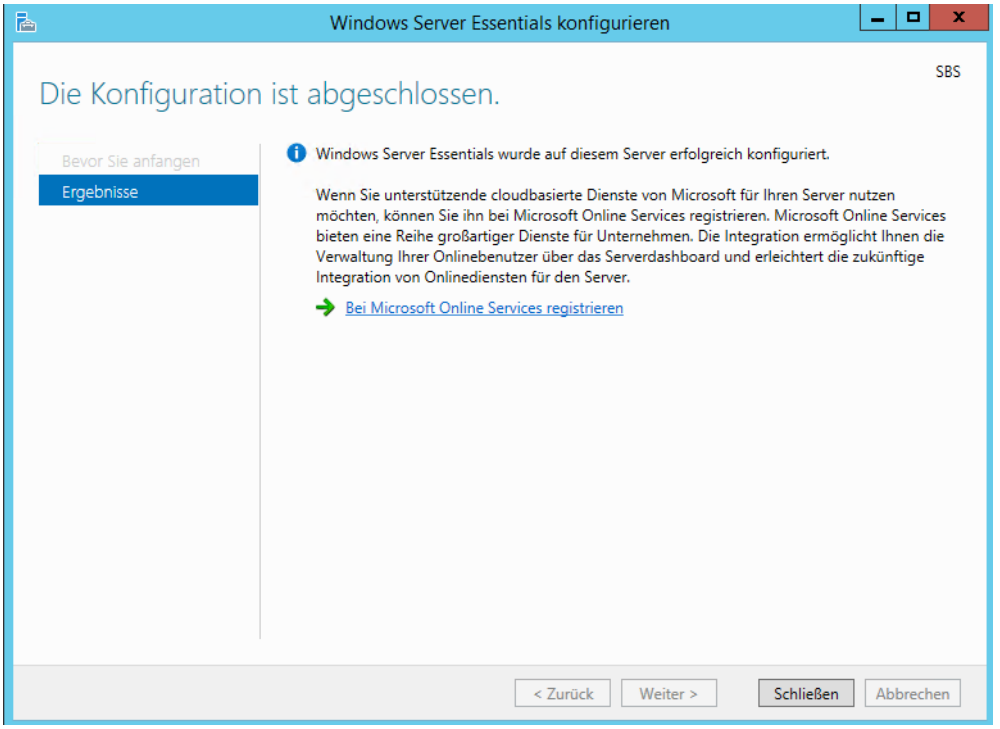
Haben Sie die Auswahl getroffen, führt der Assistent weitere Installationsaufgaben durch, um die notwendigen Komponenten zu installieren. Schalten Sie den Server nicht aus und lassen Sie den

Assistenten den Vorgang fortsetzen. Dieser dauert etwa 30 Minuten bis eine Stunde. Muss der Server neu gestartet werden, führt der Installations-Assistent diese Aufgabe automatisch durch.

Sobald der Assistent seine Arbeit abgeschlossen hat, erhalten Sie eine entsprechende Meldung angezeigt und können die Einrichtung des Servers beginnen. Die Installation ist an dieser Stelle abgeschlossen. Erst wenn diese Meldung erscheint, können Sie mit dem Server arbeiten. Vorher muss der Server noch zahlreiche Konfigurationen vornehmen. Nach der Installation ist der Server bereit. Melden Sie sich direkt am Desktop an. Sie können aber auch mit dem Remotedesktop arbeiten (siehe Kapitel 3 und 5).

Nachdem Sie die Grundinstallation des Servers abgeschlossen haben, sollten Sie in den nächsten Schritten noch die notwendigen Patches installieren und die Einrichtung des Servers abschließen. Hier gehen Sie vor wie bei den anderen Editionen von Windows Server 2012 R2 auch.

Abbildg. 2.16 Erfolgreicher Abschluss der Installation von Windows Server 2012 R2 Essentials



Nacharbeiten zur Installation von Windows Server 2012 R2

Bevor wir in den nächsten Kapiteln ausführlicher auf die Einrichtung und Verwaltung von Windows Server 2012 R2 eingehen, zeigen wir Ihnen in den nächsten Abschnitten die wichtigsten Schritte, die nach der Installation notwendig sind.

Haben Sie die Installation von Windows Server 2012 R2 abgeschlossen, sollten Sie einige erste Aufgaben durchführen, um zu überprüfen ob das System funktioniert. Auch die Aktivierung gehört zu diesen Aufgaben.

Windows Server 2012 R2 aktivieren

Nach der Installation müssen Sie die Aktivierung von Windows Server 2012 durchführen. Die Aktivierung führen Sie am besten in der Systemsteuerung über das Wartungscenter vor. Mehr Informationen erhalten Sie auch, wenn Sie auf der Startseite nach *slui* suchen.

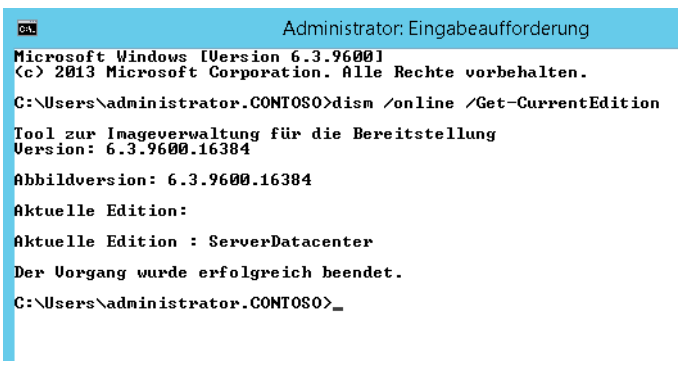
Sie können Windows Server 2012 R2 entweder über das Internet aktivieren oder per Telefon. Bei der Aktivierung per Telefon werden Sie mit einem automatischen Telefonsystem verbunden.

TIPP 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.

Über den Befehl *slui 3* wird ein Dialogfeld geöffnet, um einen neuen Produktschlüssel einzugeben. Starten Sie das Tool über die Suchfunktion der Startseite mit Administratorrechten über das Kontextmenü. In diesem Bereich aktivieren Sie Windows Server 2012 dann mit dem neuen Key. Die Startseite öffnen Sie entweder mit der -Taste auf der Tastatur oder indem Sie mit der Maus in die linke untere Ecke fahren.

Der Befehl *slui 4* öffnet die Auswahl der Aktivierungshotlines. Wollen Sie sich die aktuelle Windows Server 2012 R2-Edition anzeigen lassen, die auf dem Computer installiert ist, öffnen Sie eine Eingabeaufforderung mit Administratorrechten und geben den Befehl *DISM /Online /Get-CurrentEdition* ein. Sie erhalten daraufhin die Edition und weitere Information zur Installation angezeigt.

Abbildg. 2.17 Anzeigen der aktuell installierten Edition von Windows Server 2012



Wollen Sie anzeigen, zu welchen Editionen Sie die installierte Version aktualisieren können, verwenden Sie den Befehl *DISM /Online /Get-TargetEditions*.

Für die Verwaltung und die Abfrage von Lizenzinformationen auf Windows Server 2012 R2-Computern stellt Microsoft das Skript *slmgr.vbs* zur Verfügung, welches Sie über die Eingabeaufforderung oder das Dialogfeld *Ausführen* aufrufen. Dieses starten Sie mit der Tastenkombination ⊞+R. Das Tool kennt verschiedene Optionen:

- **/ato** Windows online aktivieren
- **/dli** Zeigt die aktuellen Lizenzinformationen an
- **/dlv** Zeigt noch mehr Lizenzdetails an
- **/dlv all** Zeigt detaillierte Infos für alle installierten Lizenzen an

Möchten Sie den Status der Aktivierung von Windows Server 2012 R2 anzeigen, geben Sie in der Befehlszeile den Befehl *slmgr.vbs /dli* ein und führen diesen aus. Anschließend werden der Name und die Beschreibung des Betriebssystems, aber auch ein Teil des Product Key und der Lizenzstatus angezeigt.

Haben Sie den Product Key eingetragen, fügen Sie die Aktivierung über die beschriebenen Weg durch. Verfügt der Computer über eine Internetverbindung, führt der Assistent die Aktivierung automatisch aus, sobald der korrekte Product Key eingegeben wurde. Sie können den Status der Aktivierung anschließend direkt einsehen, indem Sie auf der Startseite *slui* eintippen. Hier wird auch das Datum der Aktivierung angezeigt.

Sie können den Product Key einer Windows Server 2012 R2-Installation anpassen. Über diesen Weg aktivieren Sie Windows Server 2012 R2 auch auf einem Core-Server:

1. Geben Sie zum Löschen des alten Product Key in der Eingabeaufforderung den Befehl *slmgr /upk* ein. Zwar ersetzen die nächsten Punkte den vorhandenen Product Key. Allerdings funktioniert das nicht immer, wenn nicht zuvor die alte Nummer gelöscht wurde.
2. Bestätigen Sie den Löschvorgang.
3. Den neuen Product Key geben Sie dann mit *slmgr /ipk xxxxx-xxxxx-xxxxx-xxxxx-xxxxx* ein.
4. Mit *slmgr /ato* aktivieren Sie Windows Server 2012.

Da ein Core-Server über keine grafische Oberfläche verfügt, müssen Sie einen solchen Server über die Eingabeaufforderung aktivieren. Verwenden Sie zur lokalen Aktivierung des Servers den Befehl *slmgr.vbs -ato*.

Nach Eingabe des Befehls wird die Aktivierung durchgeführt. Sie können Windows Server 2012 R2 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. Sie können die Edition eines Core-Servers auch aktualisieren, indem Sie in der Eingabeaufforderung Änderungen vornehmen:

- **Anzeigen der aktuell installierten Edition** *DISM /Online /Get-CurrentEdition*
- **Mögliche Editionen zur Aktualisierung** *DISM /Online /Get-TargetEditions*
- **Aktualisierung zur Zielversion durchführen** *DISM /Online /Set-Edition:<edition ID> /ProductKey:<Seriennummer>*

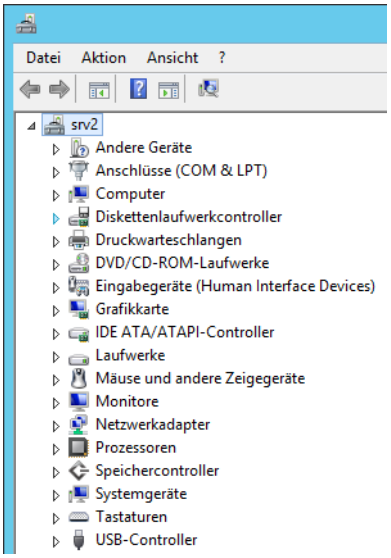
Der unterstützte Aktualisierungspfad lautet:

Windows Server 2012 R2 Standard Server Core > Windows Server 2012 R2 Datacenter Core

Treiberinstallation überprüfen

Nach der Installation überprüfen Sie auch, ob Windows Server 2012 R2 alle Geräte erkannt hat, die in Ihrem Computersystem verbaut sind. Tippen Sie dazu auf der Startseite *devmgmt.msc* ein und stellen Sie sicher, dass keine unbekannten Geräte vorhanden und alle Treiber installiert sind. Vor allem den Treiber des Netzwerkadapters und der Systemgeräte sollten Sie überprüfen.

Abbildg. 2.18 Überprüfen der installierten Treiber im Geräte-Manager



Mit dem Befehl *msinfo32* können Sie eine sehr ausführliche Übersicht über die eingebaute Hardware und die Ressourcen eines PCs abrufen.

Mit dem Befehl *systeminfo* zeigen Sie alle Informationen Ihres Computers in der Eingabeaufforderung an. Darunter finden sich Infos über Hotfixes, Netzwerkkarten, Prozessor, Betriebssystem, Hersteller usw. – sogar die aktuelle Systembetriebszeit (also wie lange Sie schon arbeiten) 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 Informationen 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.

Eines der beliebtesten Tools zum Identifizieren der eingebauten CPU oder anderer Systemkomponenten ist die Freeware CPU-Z, die Sie von der Internetseite *http://www.cpuid.com* [Ms179-K02-09] herunterladen können.

Mit dem Befehl *cpuz -txt=<Pfad>* können Sie die Informationen auch in eine Textdatei ausgeben lassen.

Mit dem kostenlosen Tool HWInfo64 Portable (*http://www.hwinfo.com/download64.html* [Ms179-K02-10]) können Sie ohne Installation umfangreiche Informationen zu der im Computer vorhandenen Hardware abrufen. Die Anwendung zeigt Informationen zu Hauptplatine, Grafikkarte, Prozessor, Laufwerke und Netzwerkverbindungen. Auch der SMART-Status der Festplatten lässt sich

auslesen. Der Entwickler bietet zusätzlich eine installierbare Version des Tools an. Um Daten auszulesen, müssen Sie das Tool lediglich starten. Es beginnt automatisch mit der Diagnose und zeigt abschließend die entsprechenden Daten an.

Netzwerkverbindung testen

Um Windows Server 2012 R2 aktuell zu halten, ist eine Verbindung mit dem Internet und damit mit dem Netzwerk notwendig. Nachdem Sie die Treiberinstallation kontrolliert haben, überprüfen Sie über das Symbol der Netzwerkverbindung in der Taskleiste, ob Windows Server 2012 mit dem Netzwerk und dem Internet kommunizieren kann. Zeigt Windows ein Netzwerksymbol ohne Fehler an, kann der Rechner mit dem Netzwerk und dem Internet kommunizieren.

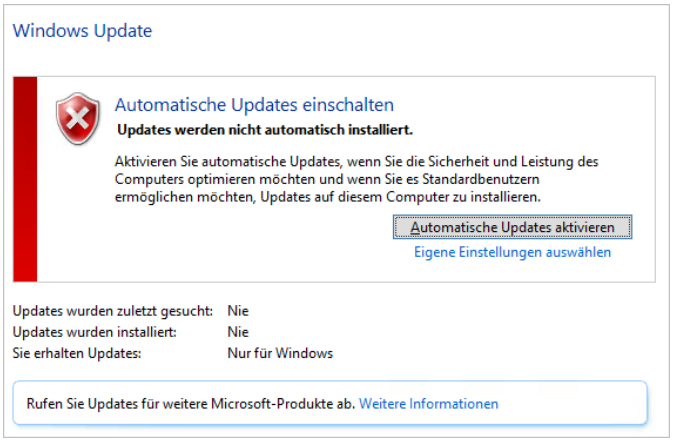
Kann der Computer mit dem Netzwerk kommunizieren, aber nicht mit dem Internet, wird das Netzwerksymbol mit einem Ausrufezeichen gekennzeichnet. In diesem Fall überprüfen Sie die Einstellungen der Netzwerkkarte. Am schnellsten geht dies, wenn Sie auf der Startseite nach *ncpa.cpl* suchen. Verfügt der PC über keine physische Netzwerkverbindung, ist das Netzwerksymbol mit einem roten X gekennzeichnet. In diesem Fall überprüfen Sie die Installation des Treibers und des Netzwerkkabels beziehungsweise der WLAN-Verbindung.

Windows Update aktivieren

Im nächsten Schritt sollten Sie, unabhängig davon, ob Sie Treiber manuell oder über Windows Update installieren wollen, die Windows Update-Funktion in der Systemsteuerung aufrufen. Das automatische Abrufen von Updates ist bei Windows 7/8/8.1 automatisch aktiv, nicht jedoch bei Windows Server 2012 R2. Sie können diese Einstellungen zwar auch über Richtlinien durchführen, aber nach der Installation von Windows Server 2012 ist es empfehlenswert, diese Funktion sofort zu aktivieren, zumindest wenn der Server Zugriff auf das Internet hat.

Nach der Installation sollten Sie die aktuellsten Windows-Updates installieren, um auch sicherzustellen, dass das Betriebssystem auf dem neusten Stand ist. Geben Sie dazu *wuapp* auf der Startseite ein, um die Windows Update-Steuerung zu aktivieren. Klicken Sie auf *Automatische Updates aktivieren*.

Abbildg. 2.19 Aktivieren von Windows Updates in Windows Server 2012 R2



Ist die Suche abgeschlossen, lassen Sie die Updates installieren, indem Sie auf den Link der gefundenen Updates klicken. Nach der Installation der Updates lassen Sie erneut nach Updates suchen, um sicherzustellen, dass keine weiteren mehr gefunden werden.

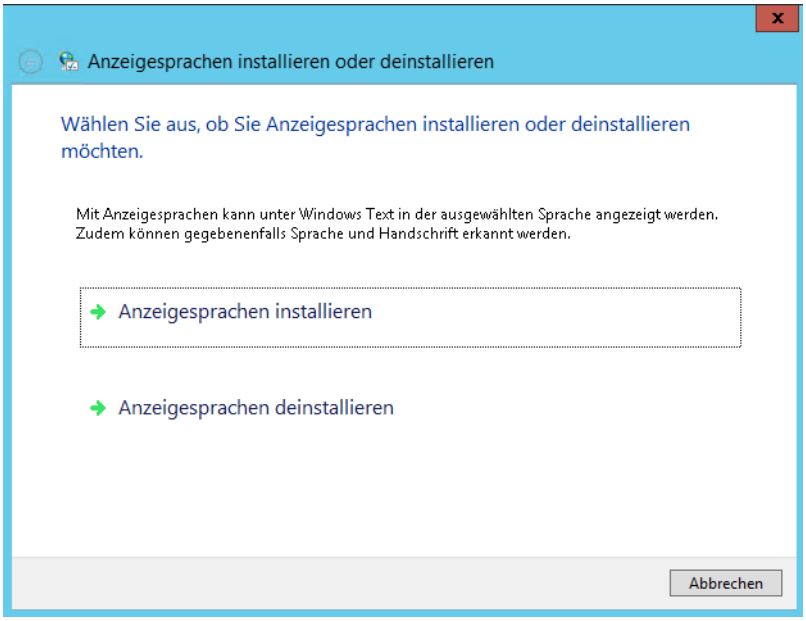
Haben Sie alle Aufgaben durchgeführt, starten Sie als Nächstes das Wartungscenter. Dieses finden Sie auf dem Desktop in der Taskleiste über das Kontextmenü der Windows-Fahne. Stellen Sie sicher, dass keine Fehler angezeigt werden. Sind Fehler vorhanden, gehen Sie diesen nach und beheben Sie diese.

Sprachpakete installieren

Verfügen Sie über ein englischsprachiges Windows-System oder eine Installation in einer anderen Sprache, können Sie beliebig weitere Sprachen installieren. Diese stehen bei Microsoft über CAB-Dateien zur Verfügung. Sie installieren die CAB-Datei und aktivieren die Sprache in Windows. Zukünftig wird die Oberfläche in der gewünschten Sprache angezeigt.

Liegt Ihnen die Sprachdatei vor, suchen Sie auf der Startseite nach *lpksetup*. Hier können Sie anschließend die Sprache installieren.

Abbildg. 2.20 Installieren von Sprachpaketen in Windows Server 2012 R2



Haben Sie die Sprache installiert, müssen Sie diese aber noch aktivieren. Dazu müssen Sie in der entsprechenden Sprache des Betriebssystems zu *Systemsteuerung/Zeit, Sprache und Region/Sprache* wechseln. Klicken Sie anschließend auf die Sprache, die Sie aktivieren wollen und dann auf *Optionen*. Hier können Sie jetzt die Sprache aktivieren.

Verwaltung des Boot-Managers mit Bcdedit

Für die Verwaltung des Boot-Managers in Windows Server 2012 R2 und auch Windows 8/8.1, gibt es keine grafische Oberfläche von Microsoft, sondern Sie müssen das Befehlszeilentool Bcdedit verwenden.

Von Drittherstellern gibt es Tools wie Easy BCD, mit denen Sie Änderungen auch in der grafischen Oberfläche ändern können. Allerdings sollten Sie hier nicht mit dem Boot-Manager von Windows Server 2012 R2 arbeiten.

Boot-Manager bearbeiten

Um die Beschreibung eines Betriebssystems im Boot-Manager zu ändern, öffnen Sie eine Eingabeaufforderung mit Administratorrechten. Klicken Sie dazu nach Eingabe von *cmd* auf der Startseite die gefundene Kachel mit der rechten Maustaste an. Im unteren Bereich, der App-Leiste, starten Sie jetzt die Eingabeaufforderung mit Administratorrechten.

Rufen Sie den Befehl *bcdedit* auf, zeigt die Eingabeaufforderung die installierten Betriebssysteme, deren Eintrag im Boot-Manager (*description*) und den Pfad der Installation an.

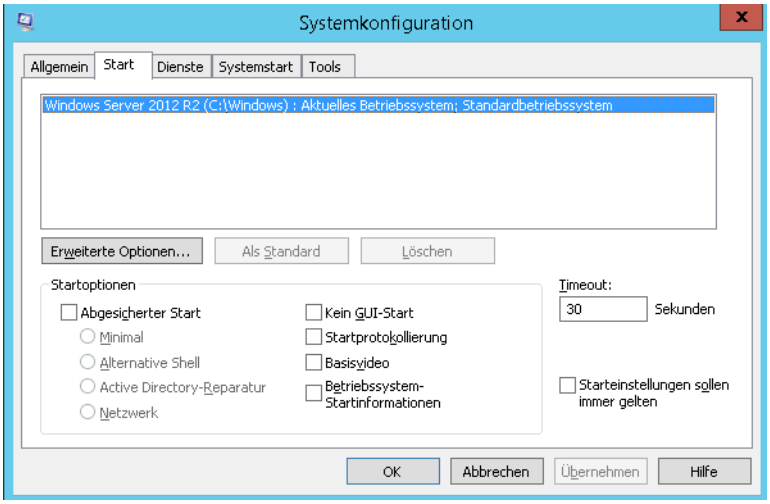
Abbildg. 2.21 Aufrufen von Bootoptionen in Windows Server 2012 R2

Um die Beschreibung zu ändern, booten Sie am besten das entsprechende Betriebssystem. Geben Sie dann den Befehl *bcdedit /set {current} description "<Beliebige Beschreibung>"* ein. Starten Sie das System beim nächsten Mal, sehen Sie die neue Bezeichnung.

Wollen Sie das Standardbetriebssystem des Bootvorgangs ändern, starten Sie das produktive System und geben *msconfig* im Suchfeld des Startmenüs ein, wenn Windows Server 2008 R2 gestartet ist. In Windows Server 2012 R2 tippen Sie den gleichen Befehl direkt auf der Startseite ein.

Wechseln Sie dann zur Registerkarte *Start*. Hier können Sie das Standardbetriebssystem anpassen. Zusätzlich haben Sie hier noch die Möglichkeit, die Dauer der Anzeige des Bootmenüs zu ändern.

Abbildg. 2.22 Anzeigen der Bootoptionen von Windows Server 2012 R2



Bevor Sie Änderungen am Boot-Manager von Windows vornehmen, sollten Sie diesen vorher sichern. Auch dazu verwenden Sie in der Eingabeaufforderung den Aufruf *bcdedit*. Mit dem Tool können Sie bei Problemen den Boot-Manager auch wieder herstellen. Dazu stehen folgende Befehle zur Verfügung:

- **Bcdedit /export <Dateiname>** Erstellt eine Sicherung der aktuellen Konfiguration
- **Bcdedit /import <Dateiname>** Stellt den Boot-Manager aus einer erstellten Sicherung wieder her

Wollen Sie auch die Reihenfolge der Betriebssysteme im Boot-Manager von Windows anpassen, benötigen Sie wieder eine Eingabeaufforderung mit Administratorrechten. Rufen Sie den Befehl *bcdedit* auf und merken Sie sich den Wert bei *Bezeichner* des Eintrags des Betriebssystems.

Sie können den Eintrag auch in die Zwischenablage kopieren, wenn Sie das Systemmenü links in der Titelleiste der Eingabeaufforderung öffnen und *Bearbeiten/Markieren* wählen. Markieren Sie den Eintrag *Bezeichner* und bestätigen Sie mit der ↵-Taste. Um die Reihenfolge anzupassen, verwenden Sie den folgenden Befehl:

```
Bcdedit /displayorder {current} {<Bezeichner des anderen Systems>}
```

Wollen Sie vorhandene Einträge kopieren, um diese zum Beispiel testweise zu bearbeiten, verwenden Sie den Befehl:

```
Bcdedit /copy {current} /d "<Neuer Name>"
```

Weitere Optionen von Bcdedit erhalten Sie mit der Option */?*.

Boot-Manager reparieren

Startet Ihr produktives System nicht mehr, haben Sie auch die Möglichkeit, über die Computerreparaturoptionen von Windows Server 2012 R2 den Boot-Manager zu reparieren. Zur Reparatur starten Sie eine Eingabeaufforderung in den Bootoptionen. Dazu starten Sie die *Computerreparaturoptionen* über die Windows Server 2012 R2-DVD. Wählen Sie dann *Problembehandlung* und *Eingabeaufforderung*.

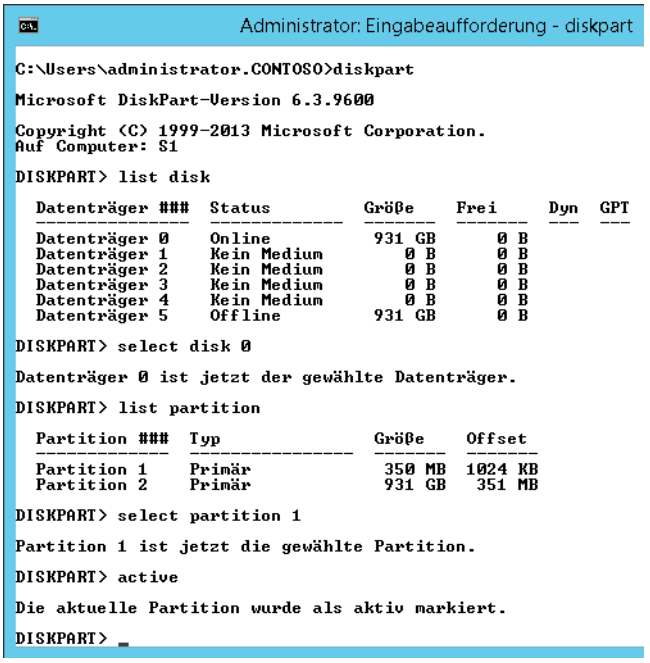
Mit dem Befehl *bootrec /fixmbr* haben Sie eine große Chance, das System zu retten. Der Befehl schreibt den Masterbootrecord neu an den Beginn der Festplatte. Hilft das nicht, lassen Sie mit *bootrec /scanos* die Betriebssysteme anzeigen, die nicht im Boot-Manager eingetragen sind. Hier sehen Sie schnell, ob es Systeme gibt, die der Manager erkennt, aber noch nicht eingebunden hat. Der Befehl *bootrec /rebuildbcd* kann diese Systeme wieder in den Boot-Manager eintragen.

Oft hilft auch *bootrec /fixboot*, wenn Sie parallel zu Windows Server 2012 R2 noch ein anderes Betriebssystem wie beispielsweise Windows Server 2008 R2 auf dem Computer installiert haben. Der Befehl erstellt den Boot-Manager *bootmgr* neu.

Windows Server 2008 R2 und Windows Server 2012 R2 starten von Bootpartitionen, die als aktiv gekennzeichnet sein müssen. Ist dies nicht der Fall, verweigern beide den Start. Um die entsprechende Festplatte als aktiv zu markieren, gehen Sie folgendermaßen vor:

1. Starten Sie den Computer mit der Installations-DVD oder, falls noch möglich, mit der F8-Taste in den *Computerreparaturoptionen*.
2. Öffnen Sie eine Eingabeaufforderung über *Problembehandlung*.
3. Geben Sie *diskpart* ein und bestätigen Sie.

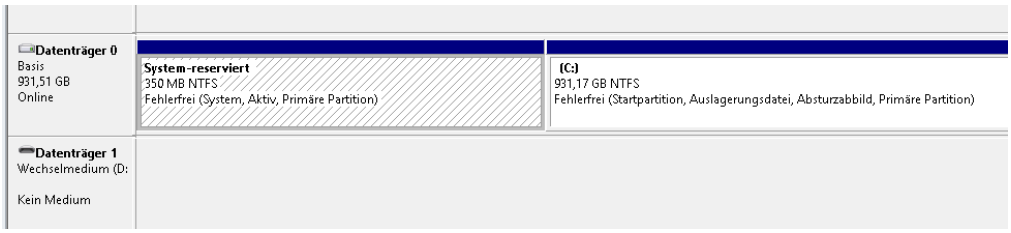
Abbildg. 2.23 Aktivieren des Bootdatenträgers in Windows Server 2012



4. Geben Sie im Diskpart-Kontext den Befehl *select disk 0* ein, um die erste Festplatte im System auszuwählen.
5. Geben Sie als Nächstes *select partition 1* ein.
6. Der nächste Befehl ist *active*.
7. Jetzt beenden Sie Diskpart mit *exit* und starten den Computer neu.

Sie erkennen den aktiven Datenträger auch, wenn Sie auf der Startseite *diskmgmt.msc* eintippen und aufrufen. Der erste Datenträger im System muss als *System-reserviert* gekennzeichnet sein. Hier ist der Boot-Manager von Windows Server 2012 R2 abgelegt. Die Partition muss als aktiv markiert sein, damit Windows Server 2012 R2 booten kann.

Abbildg. 2.24 Überprüfen des aktiven Datenträgers für den Bootvorgang von Windows Server 2012 R2



Startet weiterhin nicht der richtige Boot-Manager, starten Sie noch einmal die Computerreparaturoptionen, rufen eine Eingabeaufforderung auf und verwenden erneut die *Bootrec*-Optionen, wie zu Beginn dieses Abschnitts beschrieben.

Oft passiert es auch, dass bei Experimenten ältere Betriebssysteme wie zum Beispiel Windows Server 2003/2008 oder andere aus dem Bootmenü verschwinden. Um diese wieder einzutragen, verwenden Sie die folgenden Befehle in einer Eingabeaufforderung mit Administratorrechten:

```
Bcdedit /create {legacy} /d "Windows Server 2003/2008"
Bcdedit /set {legacy} device boot oder Bcdedit /set {ntldr} device
partition=<Laufwerkbuchstabe>
Bcdedit /set {legacy} path \ntldr
Bcdedit /displayorder {legacy} /addlast
```

In Windows Server 2012 R2 funktioniert die Option *{legacy}* von Windows Server 2008 R2 nicht mehr. In diesem Fall verwenden Sie die Option *{ntldr}* in den entsprechenden Befehlen. Die Option funktioniert auch schon in Windows Server 2008 R2.

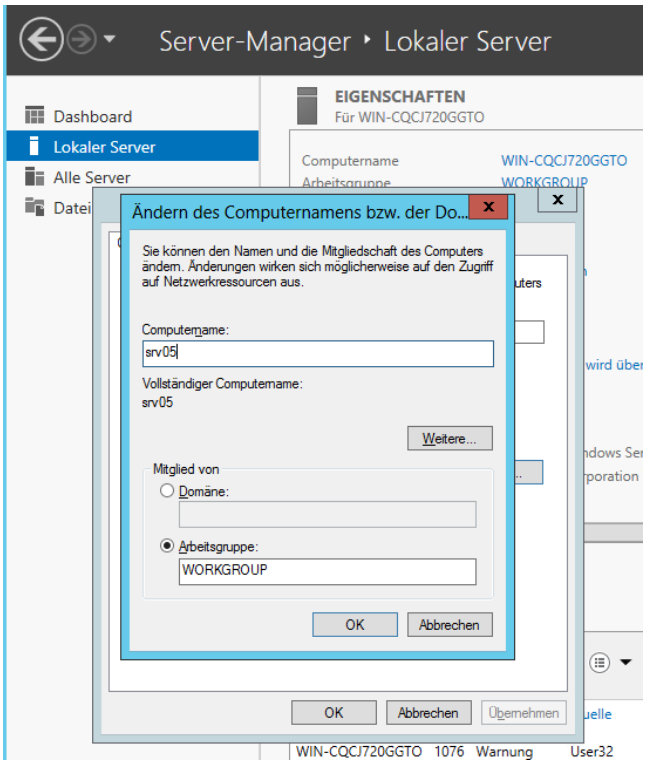
Computernamen und Domänenmitgliedschaft festlegen

Im Gegensatz zu Windows Server 2003/2008 erscheint beim Abschließen der Installation von Windows Server 2012 R2 kein Assistent, der Sie den Computernamen festlegen lässt. Sie müssen den Computernamen nach der Installation manuell festlegen. Gehen Sie dazu folgendermaßen vor:

1. Starten Sie den Server-Manager.
2. Klicken Sie auf *Lokaler Server*, dann im mittleren Bereich auf den Namen des Servers.

3. Klicken Sie im neuen Fenster auf *Ändern*.
4. Geben Sie den neuen Namen des Computers ein und booten Sie den Rechner neu.

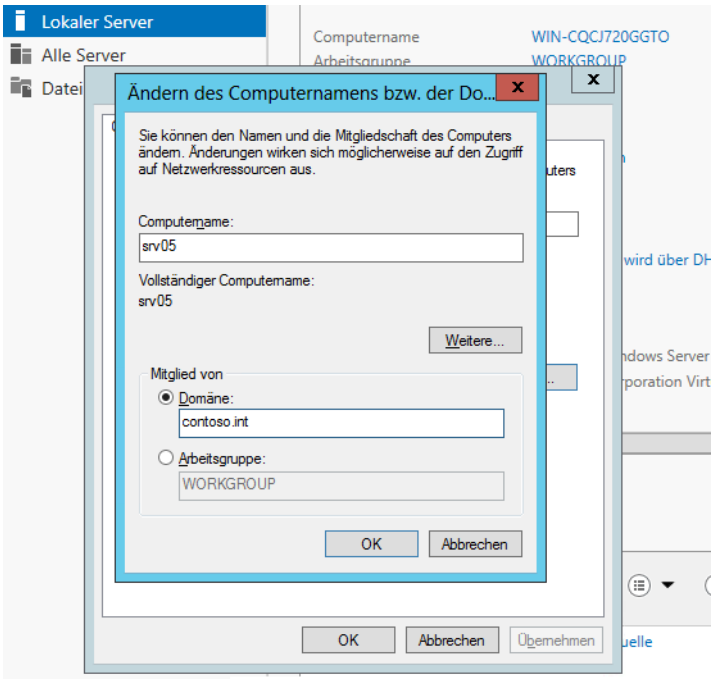
Abbildg. 2.25 Computername von Windows Server 2012 R2 anpassen



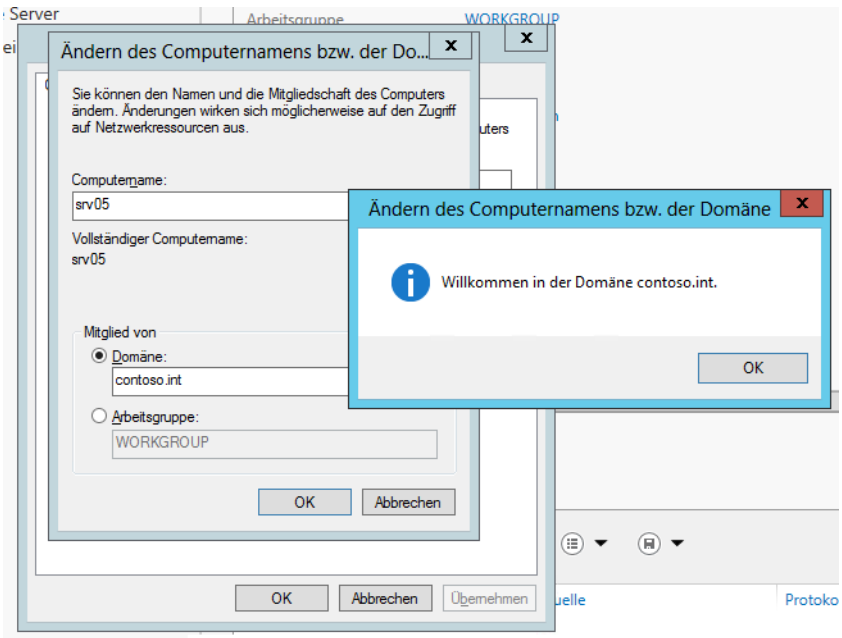
Wollen Sie den Server auch in eine Domäne aufnehmen, gehen Sie folgendermaßen vor:

1. Tippen Sie auf der Startseite *ncpa.cpl* ein und rufen Sie die Eigenschaften der Netzwerkverbindung und von IPv4 auf.
2. Stellen Sie sicher, dass als DNS-Server mindestens ein Server eingetragen ist, der die DNS-Zone der Windows-Domäne auflösen kann, der Sie beitreten wollen.
3. Klicken Sie im Server-Manager auf *Lokaler Server* und dann auf den Link bei *Arbeitsgruppe*.
4. Klicken Sie im Dialogfeld *Systemeigenschaften* auf der Registerkarte *Computername* auf die Schaltfläche *Ändern*.
5. Geben Sie im Feld *Computername* den neuen Namen des Servers in der Domäne ein und aktivieren Sie die *Domäne*.
6. Geben Sie den Namen der Domäne ein.
7. Kann der Server über seinen DNS-Server die Domäne auflösen, erscheint ein Authentifizierungsfenster. Wenn nicht, erscheint ein Fehler. In diesem Fall überprüfen Sie, ob der DNS-Server korrekt ist. Authentifizieren Sie sich an der Domäne. Kann der DNS-Server den Namen der Domäne auflösen und haben Sie sich korrekt authentifiziert, erhalten Sie eine Rückmeldung der Domänenaufnahme und können den Server neu starten.

Abbildg. 2.26 Aufnehmen eines Computers in eine Domäne



Abbildg. 2.27 Erfolgreiche Anmeldung an einer Windows-Domäne

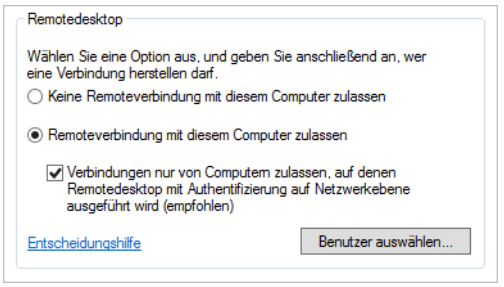


Aktivieren von Remotedesktop in Windows Server 2012 R2

Die Einrichtung von Servern direkt im Serverraum oder Rechenzentrum ist nicht gerade sehr bequem. Hier bietet es sich an, eine Remotedesktopverbindung zu aktivieren und von Ihrem Computer aus auf den Server zugreifen. Das hat den Vorteil, dass Sie auf dem Server mit Maus und Tastatur arbeiten können, und Treiber, die Sie mit dem Computer herunterladen, per Kopieren/Einfügen über den Remotedesktop auf den Server kopieren können. Um nach der Netzwerkverbindung eine Remotedesktopverbindung herzustellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie auf dem Server den Explorer, aktivieren Sie im Menüband die Registerkarte *Computer* und wählen Sie den Befehl *Systemeigenschaften* aus. Ist das Menüband noch nicht eingeblendet, klicken Sie auf den kleinen Pfeil oben rechts neben dem Hilfesymbol.
2. Klicken Sie in den Systemeigenschaften auf *Remoteeinstellungen*. Aktivieren Sie die Option *Remoteverbindung mit diesem Computer zulassen*. Funktioniert die Verbindung nicht, deaktivieren Sie noch die Option *Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird*. Bestätigen Sie die Eingabe mit *OK*.
3. Stellen Sie im unteren Bereich der Taskleiste sicher, dass eine Netzwerkverbindung hergestellt ist.

Abbildg. 2.28 Aktivieren des Remotedesktops in Windows Server 2012 R2



Um zum Beispiel von einem Windows 8.1-Computer aus eine Remotedesktopverbindung herzustellen, tippen Sie auf der Startseite *mstsc* ein. Es öffnet sich der Client für die Remotedesktopverbindung. Das funktioniert auch in Windows Server 2012 R2 über die Startseite. Sie können auch Tools wie Royal TS (*http://www.royalts.com/main/home/win.aspx* [Ms179-K02-11]) einsetzen, wenn Sie mehrere Server verwalten wollen.

Verwenden Sie den internen Remotedesktopclient in Windows 8.1, geben Sie bei *Computer* die IP-Adresse des Servers ein und bei *Benutzername* den Anmeldenamen mit der Syntax *<Name des Servers>\<Anmeldenamen>*. Auf Wunsch aktivieren Sie noch *Speichern der Anmeldeinformationen zulassen*.

Wechseln Sie zur Registerkarte *Anzeige* und verwenden Sie entweder den Vollbildmodus oder setzen die Anzeige auf die Auflösung, die auch der Server hat. Diese sehen Sie am Server, wenn Sie *desk.cpl* eintippen und das Programm starten.

Auf der Registerkarte *Lokale Ressourcen* sollten Sie die Option *Auf dem Remotecomputer anwenden* bei *Windows-Tastenkombinationen anwenden* aktivieren.

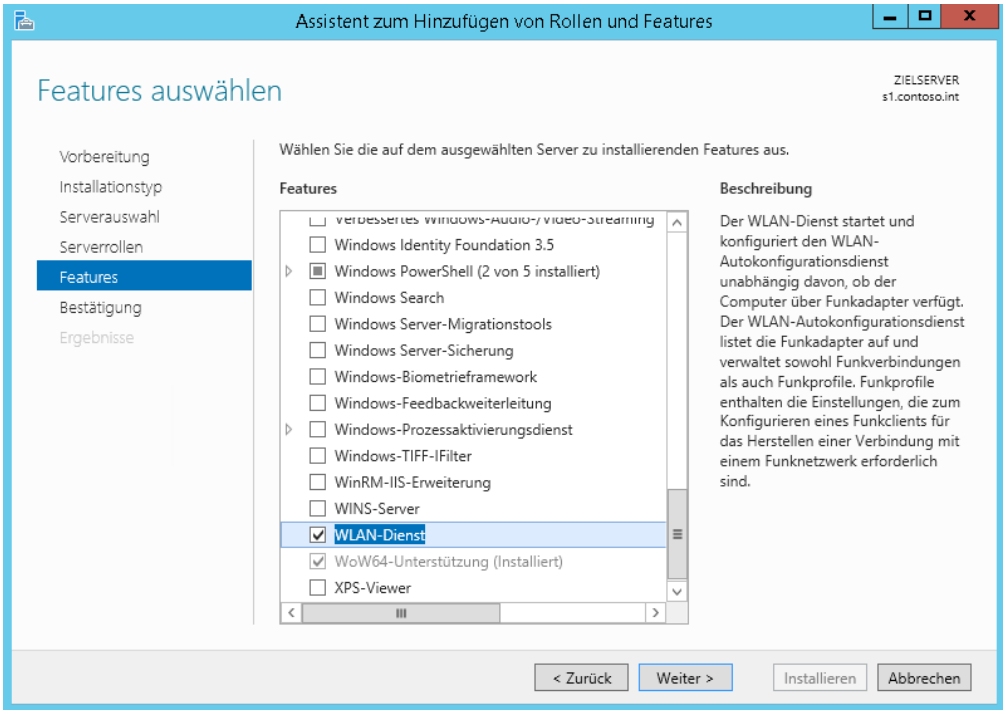
Auf der Registerkarte *Leistung* aktivieren Sie die Option *LAN (10 MBit/s oder höher)* und stellen sicher, dass alle Optionen aktiviert sind. Wechseln Sie dann zur Registerkarte *Allgemein* und speichern Sie die Verbindung mit *Speichern unter*.

Starten Sie die Verbindung, müssen Sie einmalig eine Ausnahme für die Windows-Firewall eintragen lassen, das Kennwort für das Benutzerkonto angeben und das Zertifikat bestätigen. Anschließend wird eine Remotedesktopverbindung hergestellt. Bei weiteren Verbindungen sind diese Eingaben nicht mehr notwendig, wenn Sie die entsprechenden Optionen speichern lassen.

WLAN-Anbindung von Windows Server 2012 R2

Sie können einen Server mit Windows Server 2012 R2 auch an WLANs anbinden. Zuvor müssen Sie über den Server-Manager das Feature *WLAN-Dienst* installieren.

Abbildg. 2.29 Installieren der WLAN-Unterstützung von Windows Server 2012 R2



Haben Sie eine WLAN-Karte installiert oder verwenden Sie einen WLAN-USB-Stick, können Sie den Server mit einem WLAN verbinden. Dazu klicken Sie auf das Netzwerksymbol und wählen das entsprechende WLAN aus.

Hyper-V Server 2012 R2 installieren und einrichten

Mit Hyper-V Server 2012 R2 bietet Microsoft eine kostenlose Virtualisierungslösung, die alle Hyper-V-Funktionen der kostenpflichtigen Editionen von Windows Server 2012 R2 bietet. Mit dem Server können Unternehmen daher kostenlos alle Vorteile und Neuerungen von Hyper-V in Windows Server 2012 R2 für virtuelle Server nutzen. Der Server lässt sich auch als Testumgebung nutzen und mit System Center Virtual Machine Manager (SCVMM) verwalten. Außerdem können Sie mit dem Server auch Windows Server 2012 R2 Essentials virtualisieren.

In der neuen Version beherrscht der Server alle Funktionen, die auch Hyper-V in Windows Server 2012 R2 Standard/Datacenter beherrscht. Dazu gehört die Replikation von virtuellen Servern zwischen Hyper-V-Hosts, die Livemigration von Servern mit und ohne Cluster, das Onlinezusammenführen von Snapshots und die neuen Netzwerkfunktionen. Auch die neuen VHDX-Festplatten mit einer maximalen Größe von 64 TB und der verbesserte Zugriff auf NAS-Server sowie das neue SMB 3-Protokoll sind Bestandteil. Hyper-V Server 2012 R2 entspricht der Core-Installation von Windows Server 2012 R2 und lässt sich von einer grafischen Oberfläche aus über das Netzwerk verwalten.

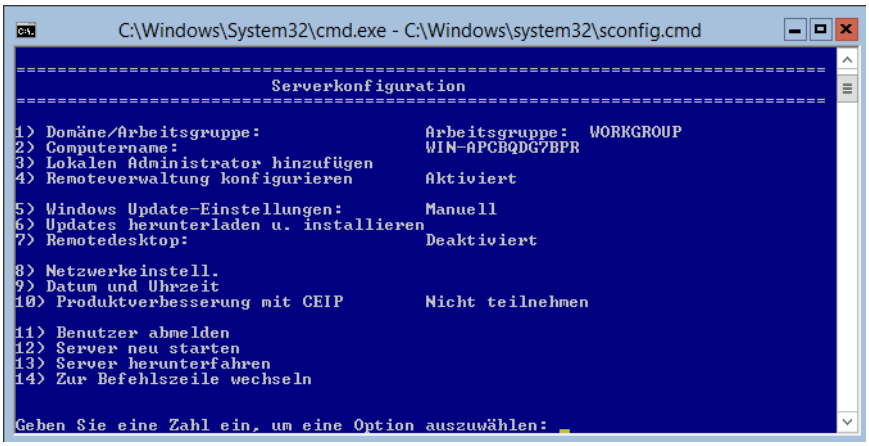
Die Installation stimmt weitestgehend mit der von Windows Server 2012 R2 überein. Die erste Einrichtung erfolgt über eine textbasierte grafische Oberfläche (Sconfig). Der Server lässt sich als alleinstehender Server betreiben, aber auch in Active Directory-Domänen. Da in Windows 8/8.1 Pro/Enterprise standardmäßig die Verwaltungswerkzeuge von Hyper-V verfügbar sind, lässt sich Hyper-V Server 2012 auch von Windows 8.1-Arbeitsstationen aus verwalten. Zusatzwerkzeuge sind dazu nicht notwendig.

Nach dem Download booten Sie die DVD mit Hyper-V Server 2012 R2 und wählen die Sprache der Oberfläche aus. Über weitere Fenster werden Einstellungen bezüglich der Partitionierung festgelegt, genauso wie bei Windows Server 2012 R2. Danach installiert sich der Server automatisch.

Abbildg. 2.30 Installieren von Hyper-V Server 2012

Nach der Installation melden Sie sich an, wie auf anderen Servern mit Windows Server 2012 R2. Es startet automatisch eine Befehlszeile und Sconfig, mit dem sich der Server anpassen lässt. Im ersten Schritt sollten Sie über den Menüpunkt 8 die Netzwerkeinstellungen vornehmen.

Abbildg. 2.31 Anpassen der Servereinstellungen in Hyper-V Server 2012 R2



Nach Auswahl der Netzwerkeinstellungen muss die Netzwerkkarte des Servers ausgewählt werden. Anschließend stellen Sie über die grafische Oberfläche die IP-Adresse, das Subnetz, die DNS-Server und das Gateway ein. Die Einstellungen lassen sich alle an dieser Stelle vornehmen.

Zurück im Hauptmenü von Sconfig lassen sich der Servername anpassen und Hyper-V Server 2012 R2 in eine Domäne aufnehmen. In Windows-Domänen kann Hyper-V deutlich einfacher betrieben werden, da auf diesem Weg auch die Replikation und Livemigration, sowie die Verwaltung und dazugehörige Authentifizierung über die Domänencontroller laufen. Über die Domänenaufnahme lässt sich auch der Rechnername ändern.

Wichtig für die Verwaltung über das Netzwerk sind noch die Punkte 4 und 7. Hierüber aktivieren Sie die Remoteverwaltung mit Tools wie den Hyper-V-Manager oder System Center Virtual Machine Manager (SCVMM). Durch Aktivierung des Remotedesktops lässt sich der Hyper-V-Server auch über den Remotedesktop verwalten.

Um virtuelle Server zu verbinden, öffnen Sie den Hyper-V-Manager auf einem anderen Server oder von einer Windows 8/8.1-Arbeitsstation aus. Hier müssen die Hyper-V-Verwaltungstools installiert sein. Die Oberfläche dazu findet sich durch Eingabe von *optionalfeatures* auf der Windows 8/8.1-Startseite. Nach dem Start des Hyper-V-Managers lassen sich die verschiedenen Server, auch Hyper-V-Server über das Kontextmenü von Hyper-V-Manager anbinden. An dieser Stelle lassen sich auch mehrere Server in der Konsole verbinden und zentral verwalten.

Um von Windows 8/8.1 aus über den Hyper-V-Manager auf Hyper-V Server 2012 R2 einen virtuellen Server zu erstellen, verbinden Administratoren den Server mit der Konsole, klicken ihn mit der rechten Maustaste an und wählen *Neu/Virtueller Computer* aus. Es startet der gleiche Assistent wie auf normalen Servern.

Hyper-V Server 2012 R2 kann natürlich nicht nur Windows Server 2012 R2 virtualisieren, sondern auch Windows Server 2008 R2 und älter sowie Linux und UNIX. Dies bedeutet, Unternehmen können weiterhin produktiv ihre herkömmlichen Server einsetzen, aber die neuen Vorteile von Windows Server 2012 effizient nutzen, und das vollkommen kostenlos.

Zusammenfassung

In diesem Kapitel wurde Ihnen anhand diverser Anleitungen gezeigt, wie Sie Windows Server 2012 R2 und Hyper-V Server 2012 R2 installieren, aber auch parallel mit älteren Windows-Versionen betreiben. Außerdem wurde Ihnen erläutert, welche wichtigen Aufgaben Sie nach der Installation durchführen müssen und wie Sie Windows Server 2012 R2 aktivieren. Die parallele Installation über virtuelle Festplatten haben wir Ihnen ebenfalls gezeigt. Und auch die Grundinstallation von Windows Server 2012 R2 Essentials war Thema in diesem Kapitel.

Außerdem sind wir darauf eingegangen, wie Sie Windows Server 2012 R2 über einen USB-Stick installieren. Zusätzlich haben Sie erfahren, wie sich der Boot-Manager reparieren lässt, und Sie haben Tipps zum Umgang mit dem Server-Manager erhalten.

Im nächsten Kapitel lesen Sie, wie Sie Windows Server 2012 R2 so einrichten, dass Sie nach der Installation optimal mit dem Server arbeiten können.

Kapitel 3

Erste Schritte mit Windows Server 2012 R2

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen die ersten Schritte, die zur Verwaltung eines Windows Server 2012 R2 notwendig sind. Eine der wichtigsten Neuerungen zur Verwaltung in Windows Server 2012 ist der verbesserte Server-Manager. In Windows Server 2012 R2 hat Microsoft keine großen Änderungen in den Server-Manager eingebaut. Administratoren, die Windows Server 2012 kennen, kommen daher auch schnell mit Windows Server 2012 R2 zurecht.

Bereits in Kapitel 1 haben wir Ihnen einige Neuerungen gezeigt. Mit diesen Funktionen wird die Verwaltung eines Servers erheblich erleichtert und übersichtlicher gestaltet. Der Server-Manager ist das zentrale Verwaltungsinstrument von Windows Server 2012 R2.

Erste Schritte nach der Installation

Während der Installation legt Windows Server 2012 R2 automatisch einen Namen für den Server fest, der nachträglich angepasst werden sollte. Wie Sie dabei vorgehen, lesen Sie in Kapitel 2. Viele Aufgaben, die zur Grundkonfiguration des Servers gehören, nehmen Sie direkt im Server-Manager vor. Dazu klicken Sie auf *Lokaler Server*. Im mittleren Bereich sehen Sie die verschiedenen Aufgaben, deren Assistenten Sie über einen Klick auf den entsprechenden Link erreichen.

Über das Menü *Ansicht* deaktivieren Sie die Kachel für Willkommen, und über *Verwalten/Server-Manager-Eigenschaften* aktivieren Sie die Option *Server-Manager beim Anmelden nicht automatisch starten*, wenn Sie nicht wollen, dass der Server-Manager automatisch mit Windows starten soll.

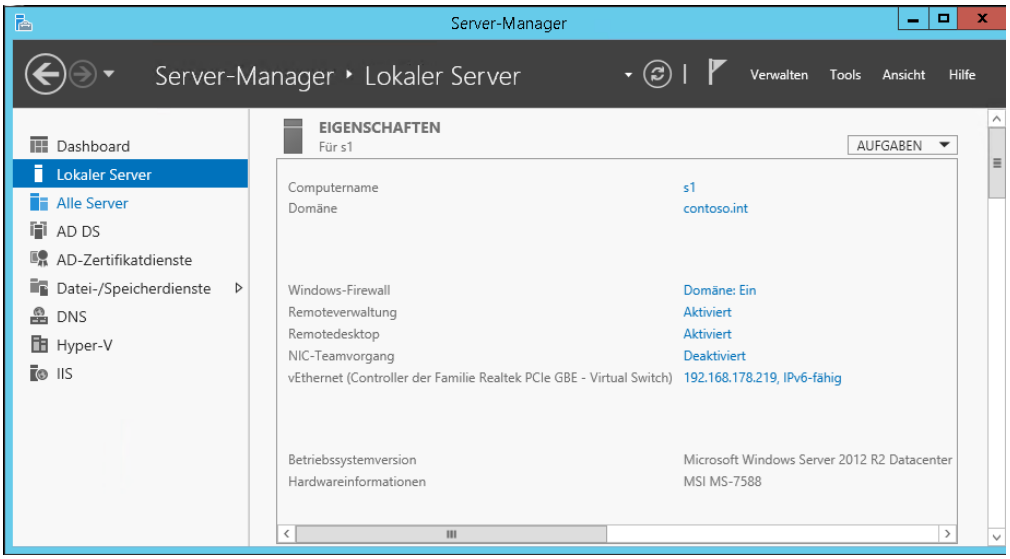
Für die Installation von Treibern benötigen Sie teilweise den Internet Explorer. Bei Windows Server 2012 R2 ist automatisch die verstärkte Sicherheit des Internet Explorers aktiv, was beim Herunterladen von Treibern durchaus stören kann. Sie können die erweiterte Sicherheit des Internet Explorers im Server-Manager deaktivieren:

1. Öffnen Sie den Server-Manager.
2. Klicken Sie auf der linken Seite auf *Lokaler Server*.
3. Klicken Sie im rechten Bereich im Abschnitt *Eigenschaften* neben *Verstärkte Sicherheitskonfiguration für IE* auf den Link *Ein*.
4. Deaktivieren Sie im daraufhin geöffneten Dialogfeld die Option für alle Benutzer oder nur für Administratoren.

In Kapitel 2 haben wir Ihnen gezeigt, wie Sie erste Aufgaben in diesem Bereich vornehmen, zum Beispiel den Namen des Servers ändern und die Aufnahme in eine Domäne. Mehr zu diesem Thema lesen Sie in den Kapiteln 10 bis 17.

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 2012 R2 ist ähnlich zu Windows 8.1. Mit dem überarbeiteten Explorer ist auch beim Serversystem der Wechsel zu häufig benötigten Ordnern über den linken Favoritenbereich möglich.

Abbildg. 3.1 Grundeinrichtung von Windows Server 2012 R2 über den Server-Manager



Windows Server 2012 R2 mit Windows 8.1 verwalten

Um Windows Server 2012 R2 mit Windows 8.1 zu verwalten, bietet Microsoft die Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT) zum Download an. Mit den Tools installieren Sie auf einer Arbeitsstation mit Windows 8.1 alle Verwaltungsprogramme, die zur Verwaltung von Windows Server 2012 R2 notwendig sind. Mit den Tools verwalten Sie auch die Serverdienste in Windows Server 2012.

Neben den verschiedenen Verwaltungstools der Serverrollen integriert der Installations-Assistent von RSAT auch den neuen Server-Manager von Windows Server 2012 R2 in Windows 8.1. Über den Server-Manager binden Sie die verschiedenen Server im Netzwerk an, auf denen Windows Server 2012 R2 installiert ist. Sie können mit dem Server-Manager auf diesem Weg auch über Windows 8.1-Arbeitsstationen aus Serverrollen auf Servern installieren. Auch im Server-Manager von Windows Server 2012 R2 können Sie andere Server mit Windows Server 2012 R2 im Netzwerk verwalten.

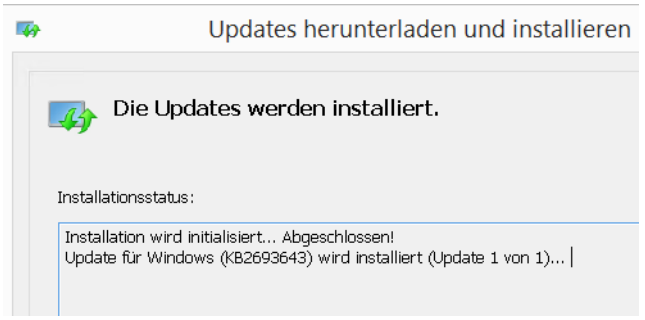
Die Remoteserver-Verwaltungstools für Windows 8.1 umfassen Server-Manager, Verwaltungstools der Serverrollen und Features von Windows Server 2012 R2, PowerShell-Cmdlets und Befehlszeilentools für die Verwaltung von Rollen und Features. Einige Tools funktionieren für die Verwaltung von Rollen und Features für Windows Server 2008 R2 und Windows Server 2012.

Die Remoteserver-Verwaltungstools lassen sich auch in der kleinsten Version Windows 8.1 installieren. Sie können die Remoteserver-Verwaltungstools für Windows 8.1 nur auf Computern installieren, auf denen Windows 8.1 installiert ist. Remoteserver-Verwaltungstools lassen sich nicht auf Computer Windows RT oder Windows Phone 8 installieren.

Remoteserver-Verwaltungstools installieren

Die Remoteserver-Verwaltungstools laden Sie als *.msu*-Datei direkt im Downloadcenter herunter (*http://www.microsoft.com/de-de/download/details.aspx?id=28972* [Ms179-K03-01]). Der Download steht als 64-Bit- und als 32-Bit-Version zur Verfügung. Bei der Installation wählen Sie keine Verwaltungstools aus, sondern installieren lediglich die Tools als Update in Windows 8.1.

Abbildg. 3.2 Die Remoteserver-Verwaltungstools stehen als Update zur Verfügung



Windows 8.1 installiert RSAT wie jedes andere Update auch, das heißt, die Installation lässt sich auch skripten. Entfernen Sie vorher alle älteren Versionen der Verwaltungstools oder Remoteserver-Verwaltungstools, auch früherer Vorabversionen sowie Versionen der Tools für verschiedene Sprachen.

Wenn Sie ein Upgrade von Windows 7 auf Windows 8.1 durchgeführt haben, müssen Sie die Remoteserver-Verwaltungstools für Windows 8.1 installieren, Sie können nicht die alten Versionen für Windows 7 parallel betreiben. Die Remoteserver-Verwaltungstools für Windows 8.1 unterstützen auch die Remoteverwaltung von Servern mit einer Core-Installation oder mit der Minimal Server Graphical Interface-Konfiguration von Windows Server 2012 R2 und teilweise auch die Server Core-Installationen von Windows Server 2008 R2 oder Windows Server 2008.

Nach der Installation finden Sie die Remoteserver-Verwaltungstools auf der Startseite in der Alle-App-Ansicht. Diese rufen Sie über den kleinen Pfeil unten links auf. Im Gegensatz zu Windows 7 sind alle Verwaltungstools nach der Installation bereits aktiv. Wollen Sie nicht alle Verwaltungstools nutzen, können Sie einzelne davon deaktivieren. Dazu geben Sie *optionalfeatures* auf der Startseite ein und suchen im Dialogfeld *Windows-Features* den Abschnitt *Remoteserver-Verwaltungstools*. Hier aktivieren oder deaktivieren Sie einzelne Verwaltungstools. Zur Installation müssen Sie nur das jeweilige Kontrollkästchen aktivieren, eine weitere Installation ist nicht notwendig. Wollen Sie die Tools komplett deinstallieren, gehen Sie folgendermaßen vor:

1. Rufen Sie über die Startseite *appwiz.cpl* auf.
2. Klicken Sie auf *Installierte Updates anzeigen*.
3. Klicken Sie mit der rechten Maustaste auf *Update für Microsoft Windows (KB2693643)* und dann auf *Deinstallieren*.
4. Bestätigen Sie die Deinstallation des Updates mit *Ja*.

TIPP Um Hyper-V in Windows Server 2012 R2, Windows 8.1 oder Hyper-V Server 2012 R2 mit Windows 8.1 zu verwalten, müssen Sie aber nicht RSAT installieren. Wenn Sie die 64-Bit-Variante von Windows 8.1 Pro/Enterprise verwenden, ist das Verwaltungstool für Hyper-V bereits in Windows 8.1 integriert. Sie installieren dieses, indem Sie auf der Startseite von Windows 8.1 *optionalfeatures* eintippen und bei *Hyper-V* die Verwaltungstools installieren.

Anschließend stehen die PowerShell-Erweiterungen und der Hyper-V-Manager zur Verfügung. Über das Kontextmenü binden Sie mehrere Server in der zentralen Konsole ein. Das funktioniert auch in einer heterogenen Umgebung mit Windows 8.1, Windows Server 2012 R2 und Hyper-V Server 2012 R2.

Abbildg. 3.3 Mit den Remoteserver-Verwaltungstools für Windows 8.1 können Sie mit dem Server-Manager auch von Windows 8.1-Rechnern aus arbeiten

Remoteverwaltung mit dem Server-Manager

Das Erste, was nach der Installation von Windows Server 2012 R2 auffällt, ist die im Vergleich zu Windows Server 2008 R2 überarbeitete Version des Server-Managers. Im Vergleich zu Windows Server 2012 sind keine Neuerungen zu sehen. Der Server-Manager bietet aber im Vergleich zu Windows Server 2008 R2 nicht nur eine neue Oberfläche, sondern auch mehr Funktionen. So ist es in der neuen Version möglich, Serverrollen und Features über das Netzwerk auf anderen Servern zu installieren.

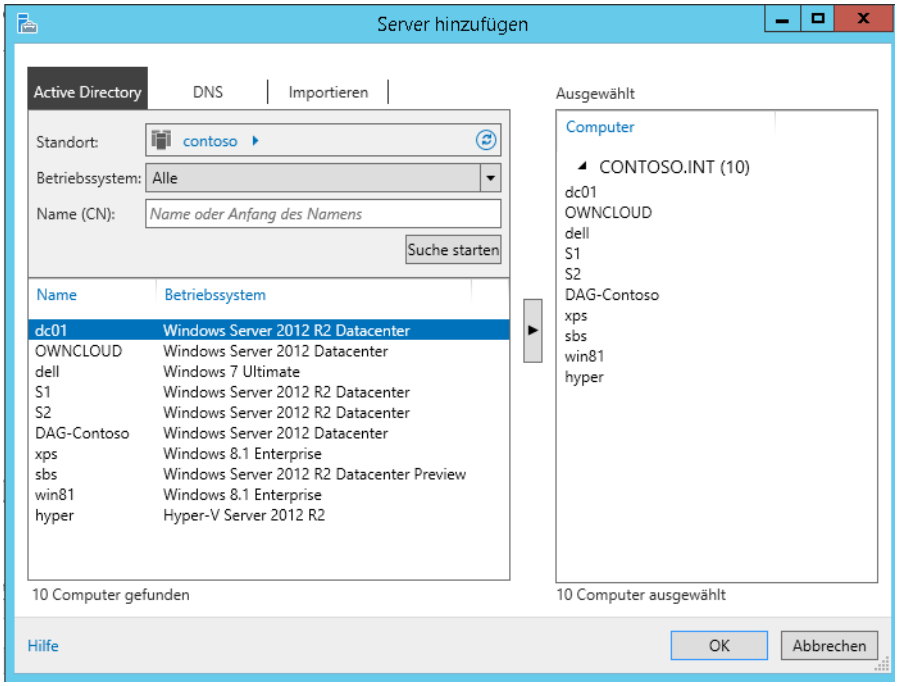
Die Server im Netzwerk lassen sich zentral im Server-Manager verwalten. Klicken Sie im Server-Manager auf *Dashboard*, können Sie über das Menü *Ansicht* die Willkommen-Kachel ausblenden und gewinnen wertvollen Platz zur Verwaltung von Servern. Über die Programmgruppe *Verwalten* erstellen Sie eigene Servergruppen.

Dazu gruppiert der Server-Manager die verschiedenen Serverfunktionen zur besseren Verwaltung. Alle installierten Serverrollen zeigt der Server-Manager automatisch gruppiert an. Verwaltungs-

werkzeuge zeigt der Server-Manager direkt über das Menü *Tools* an. Hierüber lassen sich alle wichtigen Werkzeuge starten. So stört auch die neue Oberfläche nicht, da alle Verwaltungsaufgaben zentral im Server-Manager stattfinden. Diese Funktionen sind nach der Installation von RSAT auch in Windows 8.1 verfügbar.

Um im Server-Manager in Windows Server 2012 R2 und Windows 8.1 weitere Server anzubinden, klicken Sie auf *Verwalten* und dann auf *Server hinzufügen*. Im Fenster können Sie anschließend nach Servern suchen, um sie im lokalen Server-Manager zu verwalten. Auf diesem Weg erstellen Sie auch eigene Servergruppen, die Sie im Server-Manager zusammenfassen. Von diesen Gruppen können Sie dann Ereignismeldungen anzeigen lassen. Über diesen Weg binden Sie Server mit Windows Server 2012 R2 in allen Editionen, aber auch Hyper-V Server 2012 an.

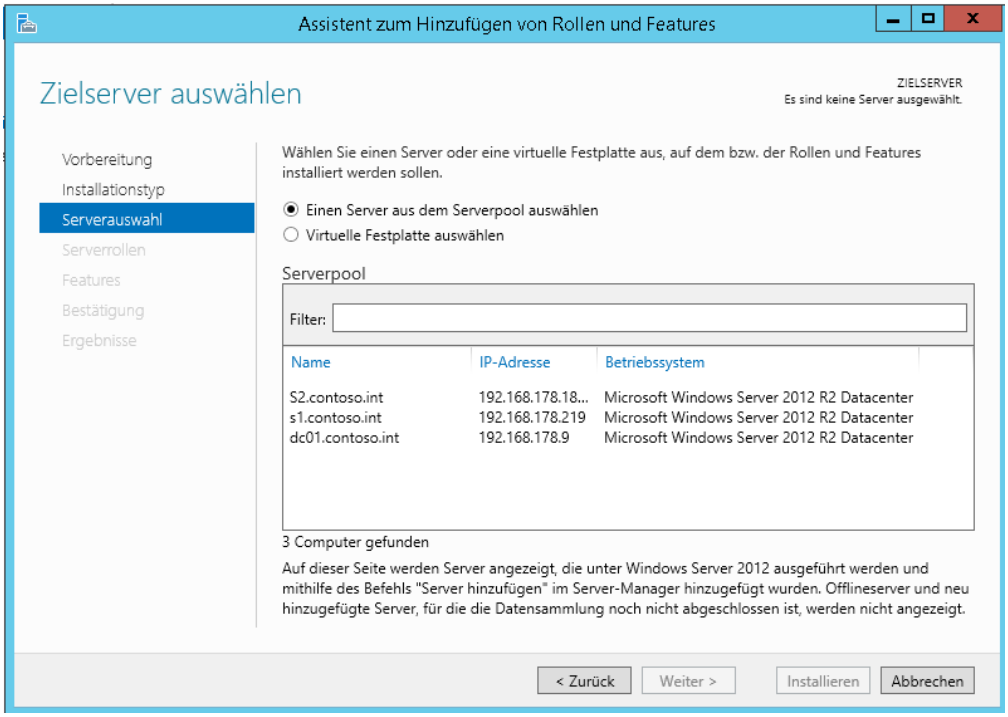
Abbildg. 3.4 Verwalten von zusätzlichen Servern im Server-Manager



Um auf Servern im Netzwerk über den Server-Manager remote Rollen oder Features zu installieren, ist eine vorherige Anbindung notwendig. Im Assistenten zum Hinzufügen von zusätzlichen Rollen erscheint ein neues Fenster, über das Sie den Server auswählen können, auf dem Sie eine neue Rolle oder ein neues Feature installieren wollen. Dazu klicken Sie auf *Verwalten/Rollen und Features* hinzufügen.

Hier fällt eine weitere Neuerung im Vergleich zu Windows Server 2008 R2 auf. In Windows Server 2012 R2 sind die Assistenten zum Hinzufügen von Rollen und Features zusammengefasst. Das heißt, Sie können über einen einzelnen Assistenten mehrere Serverrollen und Features gemeinsam und auf einmal installieren. Das erspart unnötige Neustarts und Installationen, da alles in einem Arbeitsschritt erfolgt. Im Assistenten lassen sich aber nicht nur physische Server im Netzwerk auswählen, um Serverrollen zu installieren, sondern auch virtuelle Festplatten auf Hyper-V-Hosts.

Abbildg. 3.5 Auswählen des Zielservers zur Installation von Serverrollen

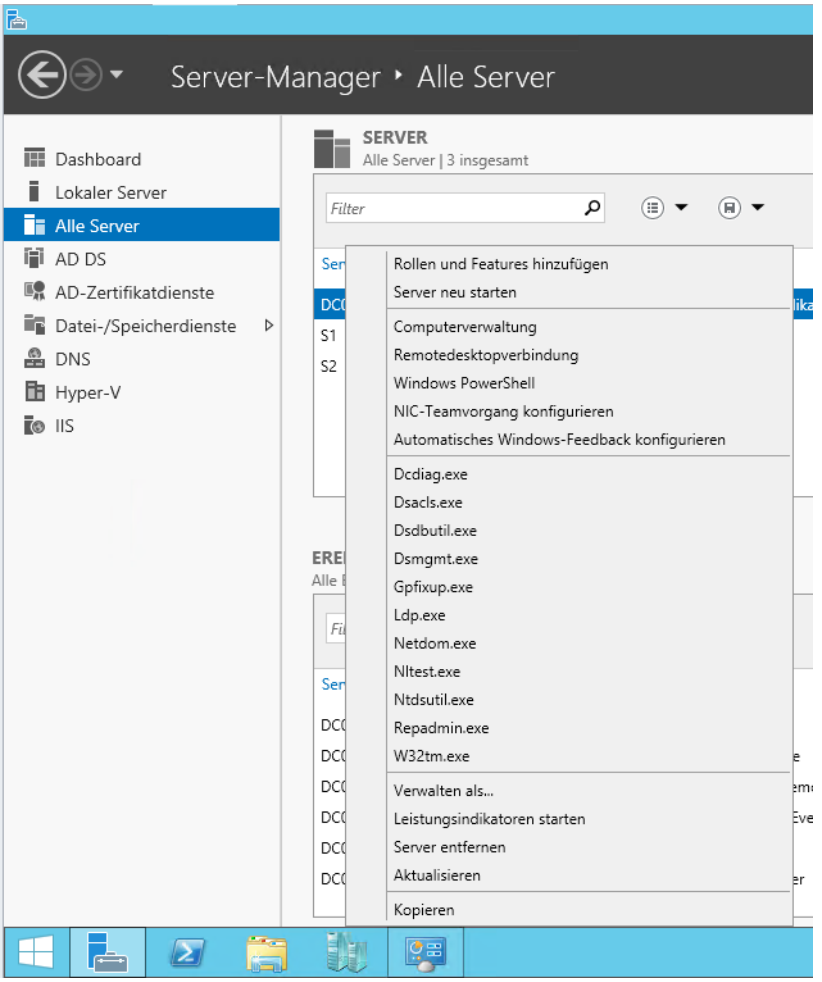


Beim Abschluss der Installation von Serverrollen und Features erhalten Sie eine Zusammenfassung angezeigt und die Möglichkeit geboten, die Konfiguration in XML-Dateien zu exportieren. Mit dieser Datei können Sie dann die gleichen Rollen oder Features auf einem anderen Server installieren. Zusätzlich haben Sie die Möglichkeit, einen alternativen Pfad zu den Installationsdateien von Windows Server 2012 R2 anzugeben. Hier sollten Sie auch die Option zum automatischen Neustart aktivieren.

In diesem Fall starten die Server automatisch neu, falls dies notwendig ist. Vor allem, wenn Sie Installationen von Serverrollen über das Netzwerk oder über eine RDP-Verbindung ausführen, ist dies sinnvoll, da viele Rollen die Netzwerkverbindung kappen können, zum Beispiel die Installation von Hyper-V. Damit der Assistent seine Arbeit erfolgreich fortsetzt, müssen Sie das Fenster nicht geöffnet lassen, sondern können es nach dem Start der Installation schließen.

Überall im neuen Server-Manager lassen sich auf diesem Weg die anderen Server im Netzwerk schnell und einfach integrieren sowie verwalten. Über das Kontextmenü von Servern können Sie Server über das Netzwerk remote neu starten lassen, eine PowerShell-Sitzung auf dem Server starten oder eine RDP-Verbindung öffnen. Damit die PowerShell funktioniert, müssen Sie teilweise Rechte freischalten. Auch die Installation von Rollen und Features über das Netzwerk ist mit dem Kontextmenü möglich.

Abbildg. 3.6 Über das Kontextmenü von Servern lassen sich Verwaltungswerkzeuge von Windows Server 2012 R2 auch in Windows 8.1 starten



Im Server-Manager sehen Administratoren am Wartungscentersymbol im oberen Bereich, ob Fehler auf einem angebundenen Server vorliegen oder Maßnahmen zur Verwaltung notwendig sind. Allerdings lassen sich auf diesem Weg nur Server mit Windows Server 2012 R2 zentral verwalten. Windows Server 2008 R2 lässt sich nicht an den Server-Manager von Windows Server 2012 R2 anbinden, Windows Server 2012 dagegen schon. Sie können sich über diesen Weg in Windows 8.1 auch gesammelt alle Fehlermeldungen aller Server anzeigen lassen.

Klicken Sie in der Ansicht *Alle Server* auf einen Server im oberen Bereich, sehen Sie unten wichtige Fehlermeldungen der Ereignisanzeige. Im oberen Bereich ist außerdem zu sehen, ob die entsprechenden Server online sind und ob Windows Server 2012 R2 aktiviert ist.

Nach der Installation von Windows Server 2012 R2 sollten Sie im Server-Manager über das Kontextmenü der Server den Befehl *Leistungsindikatoren starten* ausführen, damit der Server über das Netzwerk überwachbar ist und die neuen Best Practices Analyzer funktionieren und Daten abrufen kön-

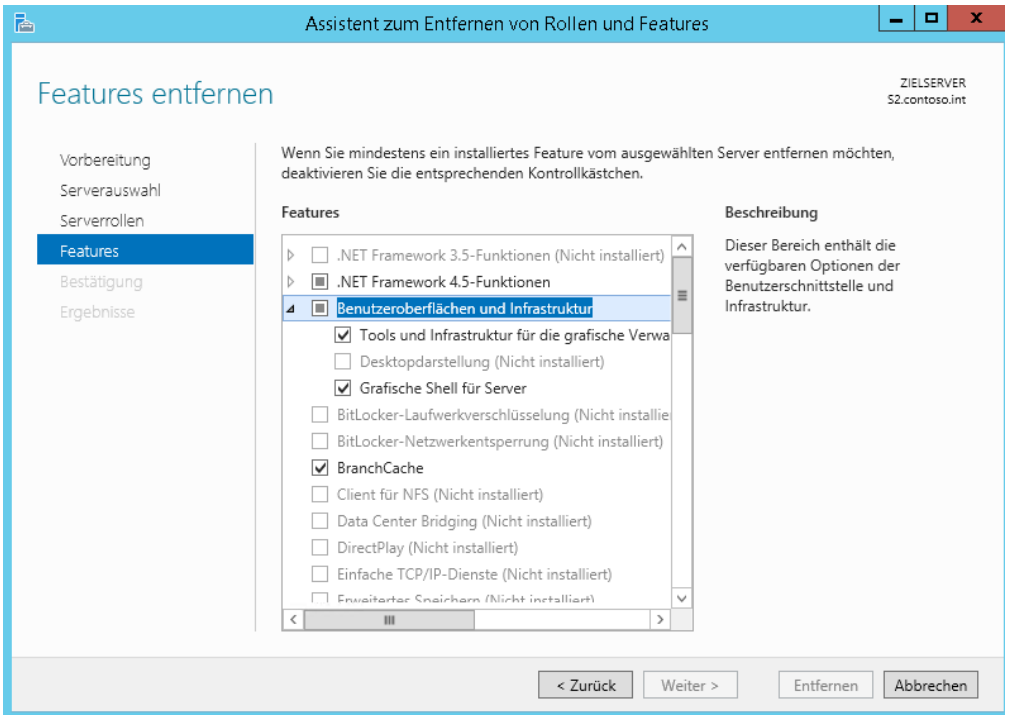
nen. Über das Kontextmenü der Server können Sie sich auch mit einem anderen Benutzernamen am Server anmelden, um diesen zu administrieren.

Core-Server, Minimal Server Interface und grafische Oberfläche

Jede Installation von Windows Server 2012 R2 besteht als Grundlage aus einem Core-Server. Dieser bietet alle wesentlichen Verwaltungsprogramme der Eingabeaufforderung und der PowerShell (siehe Kapitel 1). Es fehlen alle grafischen Verwaltungstools, Sie müssen den Server über andere Server oder mit den Remoteserver-Verwaltungstools von Windows 8.1 aus verwalten.

Während der Installation können Sie auch nur die Installation des Core-Server-Modus auswählen. Nach der Installation lassen sich in Windows Server 2012 R2 aber problemlos die Verwaltungstools und die grafische Oberfläche installieren.

Abbildg. 3.7 Deinstallieren der grafischen Oberfläche in Windows Server 2012 R2



Neu seit Windows Server 2012, neben der Möglichkeit, die grafischen Verwaltungstools auf Core-Servern zu installieren, ist das Server Minimal Interface, auf deutschen Servern als minimale Serverschnittstelle bezeichnet. Dabei handelt es sich um eine Installation der wichtigsten Verwaltungsprogramme für die grafische Oberfläche, aber keine Zusatzanwendungen wie Media Player, Explorer und Internet Explorer (siehe Kapitel 1). Auch der Desktop fehlt bei dieser Option. Diese Funktion ist auch in Windows Server 2012 R2 noch verfügbar.

Viele Programme aus der Systemsteuerung und die meisten Verwaltungsprogramme für Serverrollen und Features funktionieren. Bei der minimalen Serverschnittstelle (Minimal Server Interface)

handelt es sich um eine Zwischenstufe zwischen Core-Server und Server mit grafischer Oberfläche, nur ohne Explorer und Internet Explorer 11.

Die grafische Oberfläche deinstallieren Sie entweder im Server-Manager oder der PowerShell. Im Server-Manager verwenden Sie *Verwalten/Rollen und Features entfernen*. Auf der Seite *Features entfernen* stehen im Bereich *Benutzeroberflächen und Infrastruktur* drei Optionen zur Verfügung:

- **Tools und Infrastruktur für die grafische Verwaltung** Hierbei handelt es sich um die Verwaltungskonsolen der wichtigsten grafischen Werkzeuge auf dem Server. Ist nur dieses Feature installiert und nicht die Features *Grafische Shell für Server* und *Desktopdarstellung*, handelt es sich um einen Server mit dem Minimal Server Interface (siehe auch Kapitel 1).
- **Desktopdarstellung** Dieses Feature ist vor allem für Remotedesktopserver gedacht. Es wandelt die Oberfläche des Servers in eine Windows 8.1-Oberfläche um und bietet Tools wie Media Player, Fotoverwaltung, Themes und mehr.
- **Grafische Shell für Server** Dieses Feature deinstallieren Sie zusammen mit der Desktopdarstellung, um das Server Minimal Interface zu erhalten. Sie entfernen dabei auch den Explorer (ehemals Windows-Explorer) und den Internet Explorer vom Server. Sie können dieses Feature auch in der PowerShell mit dem Befehl *Uninstall-WindowsFeature Server-Gui-Shell* entfernen.

Installieren Sie einen Core-Server, fehlen auf dem Server auch die Binärdateien, um die grafische Oberfläche zu installieren. Sie müssen zur Installation entweder eine Internetverbindung für den Server konfigurieren, damit dieser die benötigten Daten von Windows-Update herunterladen kann, oder Sie müssen den Ordner mit den Windows Server 2012 R2-Installationsdateien angeben.

Die Installation können Sie auf Core-Servern mit der PowerShell und dem Befehl *Install-WindowsFeature Server-Gui-Mgmt-Infra* durchführen, oder Sie verbinden sich mit dem Server über den Server-Manager von einem Server im Netzwerk aus. Alternativ verwenden Sie die folgenden Befehle in der PowerShell:

```
Import-Module Dism
Enable-WindowsOptionalFeature -online -Featurename ServerCore-FullServer,Server-Gui-
Shell,Server-Gui-Mgmt
```

Auch der folgende Befehl kann die grafische Oberfläche installieren:

```
Dism /Online /Enable-Feature /Featurename:ServerCore-FullServer /Featurename:Server-Gui-
Shell /Featurename:Server-Gui-Mgmt
```

TIPP Wenn Sie auf einem Core-Server nur einen schwarzen Bildschirm sehen, ist die Eingabeaufforderung geschlossen. Um diese zu öffnen, drücken Sie Strg + Alt + Entf und starten den Task-Manager. Mit *Mehr Details* und Eingabe von *cmd* über *Datei/Neuen Task ausführen* starten Sie die Eingabeaufforderung neu.

Um das Verwaltungsprogramm von Core-Servern zu starten, rufen Sie den Befehl *sconfig* auf. Das Befehlszeilentool Sconfig steht in Windows Server 2012 R2 auch auf Servern mit grafischer Benutzeroberfläche zur Verfügung. Auf diesem Weg können Sie zum Beispiel in Fernwartungen Einstellungen vornehmen, wenn die Verbindung für grafische Werkzeuge zu langsam ist.

Müssen Sie einen Core-Server einrichten, bietet es sich oft an, einen Server mit grafischer Oberfläche zu installieren und nach der Einrichtung die Features der grafischen Oberfläche einfach zu dein-

stallieren. Sie erstellen dadurch einen Core-Server genauso wie bei der Auswahl der entsprechenden Option bei der Installation.

Features bei Bedarf

Bis Windows Server 2008 R2 waren die Binärdateien für Serverrollen, die nicht auf dem Server installiert waren, auf dem Server verfügbar. Damit wurde unnötiger Speicherplatz belegt. Mit Windows Server 2012/2012 R2 können Sie eine Rolle oder ein Feature nicht nur deaktivieren, sondern auch die zugehörigen Binärdateien vollständig entfernen.

Wollen Sie eine Rolle oder ein Feature vollständig entfernen, verwenden Sie in der PowerShell das Cmdlet *Uninstall-WindowsFeature* mit der Option *-Remove*:

```
Uninstall-WindowsFeature Server-Gui-Shell -Remove
```

Um die entsprechende Rolle oder das Feature zu installieren, benötigen Sie Zugriff auf die Installationsmedien von Windows Server 2012 R2.

Die Installation erfolgt über den Server-Manager oder der PowerShell mit dem Cmdlet *Install-WindowsFeature*. Die Option *-Source* des Cmdlets gibt einen Pfad zu einem WIM-Image an. Findet der Server kein WIM-Image, lädt der Installations-Assistent notwendige Dateien über Windows Update aus dem Internet. Dazu muss der Server über eine bestehende Internetverbindung verfügen.

Core-Server und Hyper-V Server 2012 R2 verwalten

Core-Server hat Microsoft mit Windows Server 2008 R2 eingeführt. Den Servern fehlt die grafische Oberfläche. Sie verwalten diese Server mit der Eingabeaufforderung, der PowerShell oder über das Netzwerk von anderen Servern oder auch Windows 8.1-Arbeitsstationen. Das Gleiche funktioniert auch für den neuen Hyper-V-Server 2012 R2. Core-Server lassen sich in Windows Server 2008 R2 nicht zu Servern mit grafischer Oberfläche aktualisieren und umgekehrt lässt sich die grafische Oberfläche nach der Einrichtung nicht deinstallieren.

In Windows Server 2012 R2 ist die Installation als Core-Server der von Microsoft offiziell empfohlene Weg der Installation und auch standardmäßig ausgewählt. Im Gegensatz zu Windows Server 2008 R2 ist es aber möglich, eine Core-Installation zu einer Installation mit grafischer Oberfläche zu aktualisieren. Starten Sie mit *powershell* eine PowerShell-Sitzung und rufen Sie den Befehl *Install-WindowsFeature Server-Gui-Shell* auf. Anschließend installiert Windows Server 2012 R2 die grafische Oberfläche auf dem Server. In diesem Fall können Sie den Server auch mit dem Remotedesktop und Tools auf dem Server selbst verwalten.

Haben Sie aber die Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT) in Windows 8.1 installiert, können Sie die Verwaltungstools auch von einer Windows 8.1-Arbeitsstation aus verwenden, ohne dass auf dem Core-Server eine grafische Oberfläche zur Verfügung steht.

In Hyper-V-Server 2012 R2 können Sie allerdings keine grafische Oberfläche zur Verwaltung installieren. Sie können Hyper-V Server 2012 R2 aber mit dem Hyper-V Manager in Windows 8.1 verwalten, auch ohne RSAT zu nutzen. Wichtig für die Verwaltung von Core-Servern oder Hyper-V Server 2012 R2 über das Netzwerk sind noch die Punkte 4 und 7 in Sconfig (siehe auch Kapitel 2). Hierüber aktivieren Sie die Remoteverwaltung mit Tools wie den Hyper-V-Manager. Durch Aktivierung des Remotedesktops lässt sich Hyper-V-Server auch darüber verwalten. Wie Sie dabei vorgehen, lesen Sie auch in Kapitel 2.

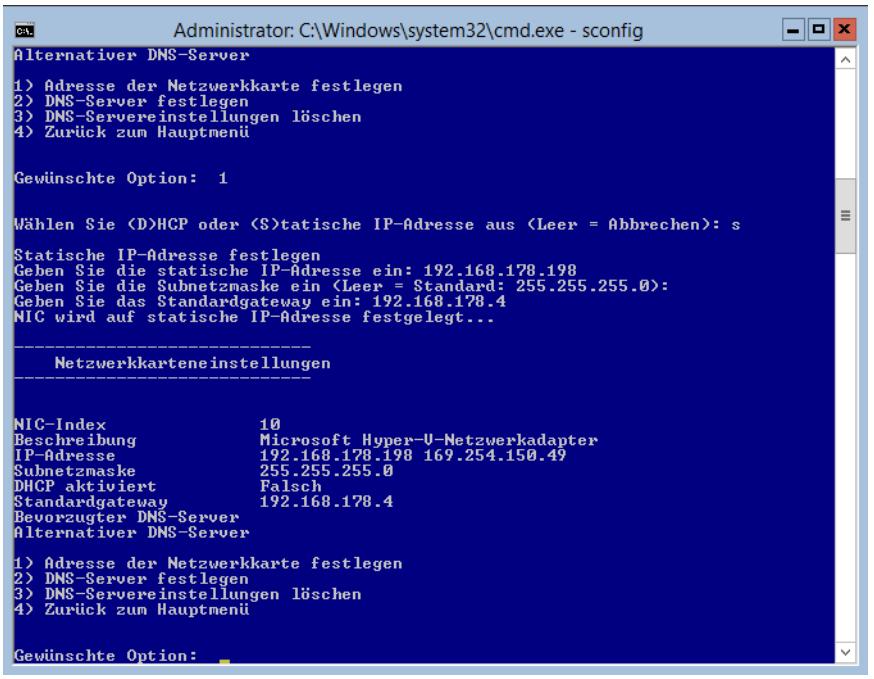
Haben Sie sich mit einem Core-Server verbunden und versehentlich die Eingabeaufforderung geschlossen, drücken Sie die Tastenkombination Strg+Alt+Entf und starten den Task-Manager. Klicken Sie danach auf *Mehr Details* und dann auf *Datei/Neuen Task ausführen*. Geben Sie *cmd* ein, um die Eingabeaufforderung erneut zu öffnen.

Haben Sie einen Core-Server installiert, legen Sie zunächst die IP-Adresse fest, konfigurieren den DNS-Server, ändern den Namen und nehmen den Server in die Active Directory-Domäne auf. Aktivieren Sie noch die Remoteverwaltung, können Sie den Server mit grafischen Verwaltungstools verwalten, wie in den ersten Abschnitten in diesem Kapitel behandelt.

Um Core-Server zu verwalten, rufen Sie zunächst in der Eingabeaufforderung den Befehl *sconfig* auf. Zur Konfiguration der Netzwerkeinstellungen wählen Sie den Menüpunkt *8) Netzwerkeinstellungen*:

1. Wählen Sie die Nummer des Adapters aus.
2. Wählen Sie *1) Adresse der Netzwerkkarte festlegen* aus, um die Adresse zu ändern.
3. Drücke Sie die Taste S, um eine statische IP-Adresse zu konfigurieren.
4. Geben Sie die statische IP-Adresse und danach die Subnetzmaske ein.

Abbildg. 3.8 Festlegen einer statischen IP-Adresse für einen Core-Server



5. Anschließend tragen Sie über den Menüpunkt *2) DNS-Server festlegen* einen DNS-Server ein, der die Active Directory-Domäne auflösen kann.
6. Im Hauptmenü zurück nehmen Sie den Server mit dem Punkt *1) Domäne/Arbeitsgruppe* in die Domäne auf und ändern den Servernamen. Anschließend starten Sie den Server neu.
7. Über die Menüpunkte 4 und 7 im Sconfig-Hauptmenü aktivieren Sie die Verwaltung des Remotedesktops und die Remoteverwaltung über grafische Tools wie den Server-Manager.

Die Verwaltung eines Core-Servers läuft hauptsächlich über die Eingabeaufforderung ab. Mit dem Befehl *start cmd /separate*, öffnen Sie ein paralleles Fenster der Eingabeaufforderung, wenn Sie zwei Fenster benötigen. Wird das eine 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 diesen Aufwand und können bei der Arbeit mit einem Skript parallel mit einer zweiten Oberfläche arbeiten.

Alle Tools, die eine grafische Oberfläche verwenden oder den 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) verwendet werden, um Skripts oder Dateien zu bearbeiten. Mit Notepad können Sie das Dateisystem durchsuchen und Skripts bearbeiten. Der Task-Manager steht ebenfalls zur Verfügung.

Um das lokale Administratorkennwort eines Servers anzupassen, gehen Sie folgendermaßen vor:

1. Geben Sie in der Eingabeaufforderung 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.

Sie können natürlich auch Einstellungen des Servers in der Eingabeaufforderung anpassen. Das Kennwort des angemeldeten Benutzers ändern Sie über die Tastenkombination Strg+Alt+Entf. Die PowerShell ist in Core-Installationen automatisch aktiviert. Daher verwenden Sie zur Konfiguration der IP-Einstellungen nicht mehr das Befehlszeilentool Netsh, sondern besser die Cmdlets *New-NetIPAddress* und *Get-NetIPConfiguration*. Ein Beispiel für die Einrichtung ist:

```
New-NetIPAddress -InterfaceIndex 12 -IPAddress 192.168.178.2 -PrefixLength 24 -
DefaultGateway 192.168.178.1
```

Die DNS-Server tragen Sie mit dem folgenden Befehl ein:

```
Set-DNSClientServerAddress -InterfaceIndex 12 -ServerAddresses 192.168.178.4
```

Mehrere DNS-Server trennen Sie jeweils mit einem Komma. Das Cmdlet *Set-DnsClientServerAddress -InterfaceIndex 12 -ResetServer* wechselt zu DHCP. Achten Sie darauf, jeweils die korrekte Indexnummer für den Netzwerkadapter zu verwenden. Diesen erhalten Sie mit *Get-NetIPConfiguration*.

Einer Windows-Domäne treten Sie mit *Add-Computer* bei. Um der lokalen Administratorengruppe ein Domänenkonto hinzuzufügen, verwenden Sie den Befehl *net localgroup administrators /add <Domäne>\<Benutzername>*. Mit dem Befehl *net localgroup administratoren* können Sie sich alle Gruppenmitglieder anzeigen lassen. Die Aufnahme funktioniert auch über Sconfig, geht aber mit der Eingabeaufforderung schneller.

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 lassen sich neue Benutzerkonten hinzufügen. Sie können die Benutzerverwaltung auch über die grafische Oberfläche von einem anderen Server aus durchführen, wenn Sie die Remoteverwaltung auf dem Server aktiviert haben. Mit dem Befehl *net localgroup administratoren /delete <Domäne>\<Benutzername>* entfernen Sie ein Benutzerkonto wieder aus der Gruppe.

Den Namen von Servern ändern Sie mit *Rename-Computer*. Der Aufruf von *Set-Date* ändert die Zeitzone und die Spracheinstellungen ändern Sie mit *control intl.cpl*.

TIPP Installieren Sie Windows-Installer-Pakete auf einem Core-Server, verwenden Sie beim Aufruf die Option */qb*.

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 Eingabeaufforderung des Core-Servers.

Hardware und Treiber auf Core-Servern installieren

Installieren Sie neue Hardware, können Sie die grafische Oberfläche verwenden oder die Eingabeaufforderung. Auf Core-Servern bleibt Ihnen keine andere Wahl, als die Eingabeaufforderung 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 2012 R2 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 einen Ordner 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 2012 R2 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

Für die Anbindung an iSCSI-Targets (siehe auch Kapitel 5) steht auf Core-Servern eine grafische Oberfläche zur Verfügung. Diese starten Sie durch Eingabe des Befehls *iscsicpl*. Für die Anbindung von Core-Servern an iSCSI-Targets steht auch der Befehl *iscsicli* zur Verfügung. Über *iscsicli /?* erhalten Sie eine ausführliche Hilfe zum Befehl (siehe Kapitel 5).

Windows Updates auf Core-Servern steuern

Um Windows-Updates zu steuern, verwenden Sie auf Core-Servern ebenfalls Sconfig. Sie können die Einstellung und die Installation von Updates aber auch in der Eingabeaufforderung durchführen. Wechseln Sie dazu in der Eingabeaufforderung in den Ordner *C:\Windows\System32*. Die Einstellungen für Windows Update fragen Sie mit dem folgenden Befehl ab:

```
Cscript scregedit.wsf /AU /v
```

Automatische Updates aktivieren Sie mit den folgenden Befehlen:

```
Net stop wuauserv
Cscript scregedit.wsf /AU 4
Net start wuauserv
```

Um die automatischen Updates wieder zu deaktivieren, führen Sie den folgenden Befehl aus:

```
Cscript scregedit.wsf /AU 1
```

Die Zahlen entsprechen den Einstellungen, die Sie für automatische Updates in den Gruppenrichtlinien setzen. Mehr zu diesem Thema lesen Sie in Kapitel 37.

Um eine sofortige Installation von Updates durchzuführen, geben Sie den Befehl *wuauclt /detectnow* ein. Die installierten Updates lassen sich durch den Aufruf von *systeminfo* oder *wmic qfe list* anzeigen.

Erste Schritte im Umgang mit der neuen Oberfläche

In diesem Abschnitt erläutern wir Ihnen die erste Bedienung von Windows Server 2012 R2, nachdem Sie das Betriebssystem installiert haben. Die Bedienung orientiert sich an Windows 8.1 Es gibt kein Startmenü mehr, sondern eine Startseite mit einer speziellen Kachelansicht. Wie Windows 8.1 verfügt Windows Server 2012 R2 wieder über eine *Start*-Schaltfläche.

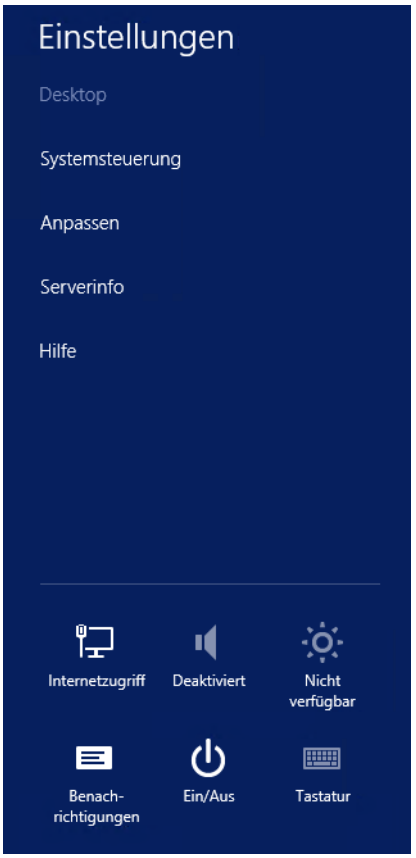
Grundlagen zum Umgang mit Windows Server 2012 R2

Zunächst erläutern wir Ihnen in aller Kürze die ersten wichtigen Schritte im Umgang mit Windows Server 2012 R2. Sie lesen in diesem Abschnitt, wie Sie Windows Server 2012 R2 generell steuern und mit den Apps umgehen.

Durch die neue Tablet-PC-orientierte Windows-Oberfläche ist die Arbeit zunächst sehr ungewohnt. Die grundsätzliche Bedienung und die Einstellungsmöglichkeiten sind in Windows Server 2012 R2 durchaus ähnlich zu Windows Server 2008 R2. Nur der Start der einzelnen Programme und die Bedienung der Oberfläche ist etwas anders. Wir zeigen Ihnen, wie Sie die wichtigsten Einstellungen finden.

Windows Server 2012 R2 bietet eine neue Leiste für Einstellungen. Diese trägt die Bezeichnung Charms-Leiste. Sie rufen diese auf, indem Sie mit der Maus an den rechten oberen oder unteren Bildschirmrand fahren. Alternativ verwenden Sie die Tastenkombination ⊞+C. Über die Charms-Leiste lassen sich Einstellungen durchführen und sie ermöglicht auch zentrale Einstellungen für den kompletten Server.

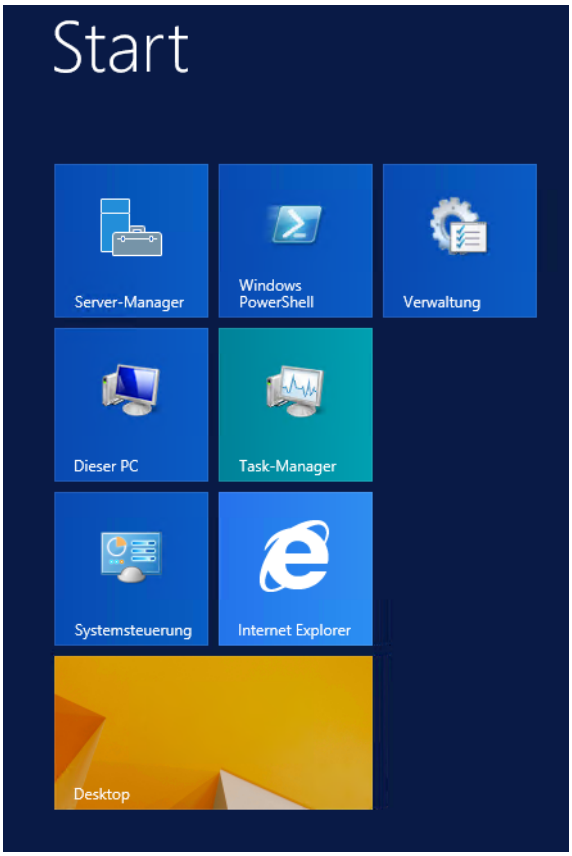
Abbildg. 3.9 Anzeigen der neuen Einstellungsleiste in Windows Server 2012 R2



Anpassen der Benutzeroberfläche

In diesem Abschnitt zeigen wir Ihnen, wie Sie die Benutzeroberfläche in Windows Server 2012 R2 anpassen können und welche erweiterten Möglichkeiten Sie dabei haben. Viele Einstellungen sind in Windows Server 2012 R2 identisch zu Windows Server 2008 R2 und lassen sich über das Kontextmenü des Desktops starten. Auf diese Möglichkeiten gehen wir nicht ein. Wir zeigen Ihnen die neuen Funktionen, die Windows Server 2012 R2 in diesem Bereich bietet.

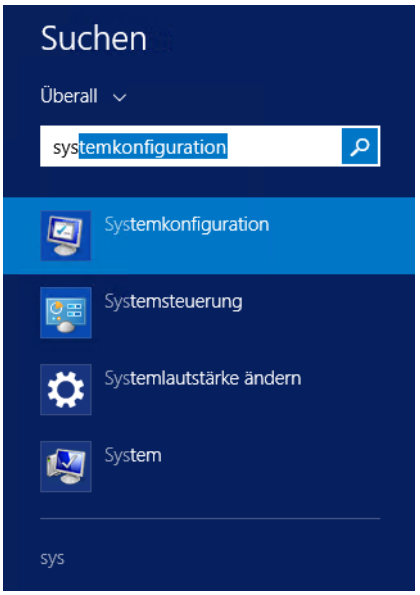
Abbildg. 3.10 Die Startseite ist der zentrale Einstieg in Windows Server 2012 R2



Befinden Sie sich auf der Startseite, reicht es, wenn Sie direkt über die Tastatur den Begriff zu einem bestimmten Element (App, Datei, Einstellung usw.) eintippen. Bereits während der Eingabe wird die *Suchen*-Leiste aktiviert und der eingetippte Text erscheint automatisch im Suchfeld. Hier geben Sie ein, was Sie suchen, und im linken Bereich der Startseite sehen Sie das Ergebnis.

In Windows Server 2012 R2 gibt es wieder die *Start*-Schaltfläche in der bisher gewohnten Form. Der Desktop ist eine der Apps auf der Startseite. Mit der Maus können Sie im unteren Bereich mit der Bildlaufleiste den Bildschirm horizontal bewegen. Die Apps, die auf der Startseite angezeigt werden, finden Sie übrigens als Verknüpfung im Ordner *C:\ProgramData\Microsoft\Windows\Start Menu\Programs*.

Abbildg. 3.11 Einstellungen und Programme suchen mit Windows Server 2012 R2



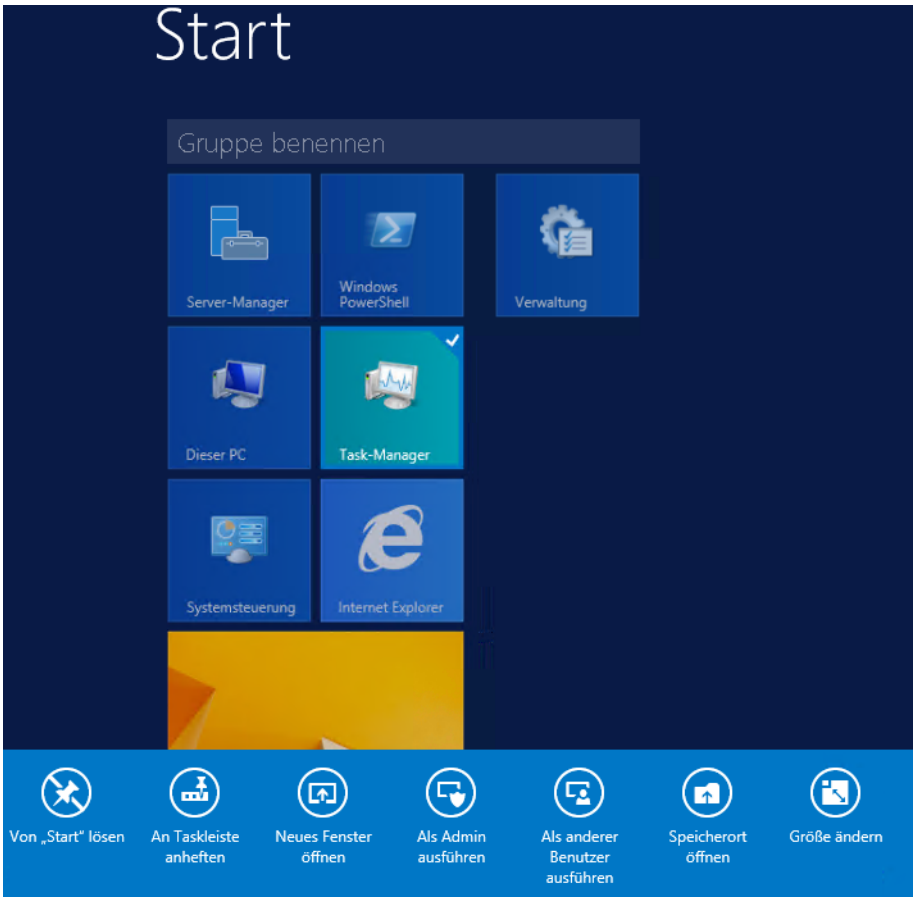
Damit Sie den Ordner sehen, müssen Sie zunächst die versteckten Ordner einblenden lassen. Dazu öffnen Sie im Menüband des Explorers (in Vorgängerversionen als »Windows-Explorer« bezeichnet) die Registerkarte *Ansicht* und aktivieren in der Gruppe *Ein-/ausblenden* das Kontrollkästchen *Ausgeblendete Elemente*.

Alternativ können Sie im Menüband des Explorers auf der Registerkarte *Ansicht* auf *Optionen/Ordner- und Suchoptionen ändern* klicken, um das Dialogfeld *Ordneroptionen* zu öffnen. Wechseln Sie im Dialogfeld zur Registerkarte *Ansicht* und aktivieren Sie im Abschnitt *Versteckte Dateien und Ordner* die Option *Ausgeblendete Dateien, Ordner und Laufwerke anzeigen*. Auf der gleichen Registerkarte des Dialogfelds können Sie durch Deaktivieren des Kontrollkästchens *Geschützte Systemdateien ausblenden* zusätzlich versteckte Systemdateien einblenden lassen.

Richten Sie ihre Verwaltungs-Apps ein und starten diese, bietet die Startseite einen echten Mehrwert. Starten lässt sich die Startseite über die ⊞-Taste, und mit Strg+⇆ schalten Sie zur Ansicht aller installierten Apps. Diese Ansicht ist beim früheren Startmenü am besten mit der *Alle Programme*-Ansicht zu vergleichen. Apps, die auf der Startseite nicht erscheinen, finden Sie in der *Alle Apps*-Ansicht. Klicken Sie dazu auf der Startseite mit der rechten Maustaste und wählen Sie im unteren Bereich *Alle Apps* aus. So lässt sich auch über das Kontextmenü von Apps festlegen, welche Apps überhaupt auf der Startseite erscheinen. Erstellen Sie eigene Verknüpfungen, können Sie diese ebenfalls in die Startseite integrieren. Dazu erstellen Sie im Desktop eine Verknüpfung und fügen diese über das Kontextmenü an die Startseite an.

Generell können Sie die Kacheln auf der Startseite per Ziehen/Ablegen so anordnen, wie Sie es wollen. Sie können auch eigene Gruppen bilden, indem Sie die Kacheln an eigene Bereiche ziehen. Die Kacheln von Windows-Apps lassen sich über die App-Leiste außerdem vergrößern oder verkleinern. Standardprogramme, die keine Windows-Apps sind, zeigt Windows Server 2012 R2 aber immer mit einem kleinen Symbol an.

Abbildg. 3.12 Anpassen von Apps auf der Startseite über die App-Leiste



Öffnen Sie eine Windows-App, zum Beispiel den Desktop, verwendet diese immer den ganzen Bildschirm. Um zur Startseite umzuschalten, drücken Sie die [⊞]-Taste. Zwischen Windows-Programmen schalten Sie um, wenn Sie mit der Maus in die linke obere Bildschirmecke fahren und dann nach unten ziehen. Über einen Rechtsklick auf eine App am linken oberen Bildschirmrand können Sie diese auch beenden.

Klicken Sie eine App mit der rechten Maustaste an, wird eine sogenannte App-Leiste im unteren Bildschirmbereich mit deren möglichen Optionen angezeigt. Wollen Sie zum Beispiel ein Programm mit Administratorrechten direkt von der Startseite aus starten, klicken Sie diese mit der rechten Maustaste an und wählen den Start mit Administratorrechten aus.

Haben Sie die Kacheln der Apps auf der Startseite per Ziehen/Ablegen Ihren Wünschen entsprechend angeordnet und gruppiert, haben Sie auch die Möglichkeit, die Gruppen zu benennen. Dazu klicken Sie mit der rechten Maustaste auf eine App in der Startseite.

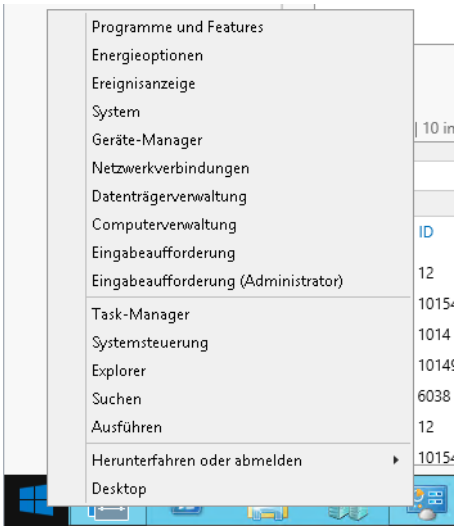
Den Gruppennamen zeigt Windows Server 2012 R2 auf der Startseite oberhalb der entsprechenden Gruppe an.

Abbildg. 3.13 Verwenden von Gruppen in Windows Server 2012 R2

Wichtige Systemprogramme zeigt Windows Server 2012 R2 im sogenannten Schnellzugriffmenü in der linken unteren Bildschirmecke an, indem Sie die Tastenkombination ⊞+X drücken. Alternativ klicken Sie mit der rechten Maustaste auf die *Start*-Schaltfläche.

Klicken Sie auf der Startseite mit der rechten Maustaste auf eine App-Kachel, können Sie diese durch Auswahl von *Von "Start" lösen* von der Startseite in die *Alle Apps*-Ansicht verschieben. Umgekehrt können Sie Apps über deren Kontextmenü in der *Alle Apps*-Ansicht oder dem Desktop an die Startseite anheften. Die App wird dadurch nicht deinstalliert, sondern bleibt weiterhin auf dem Server verfügbar.

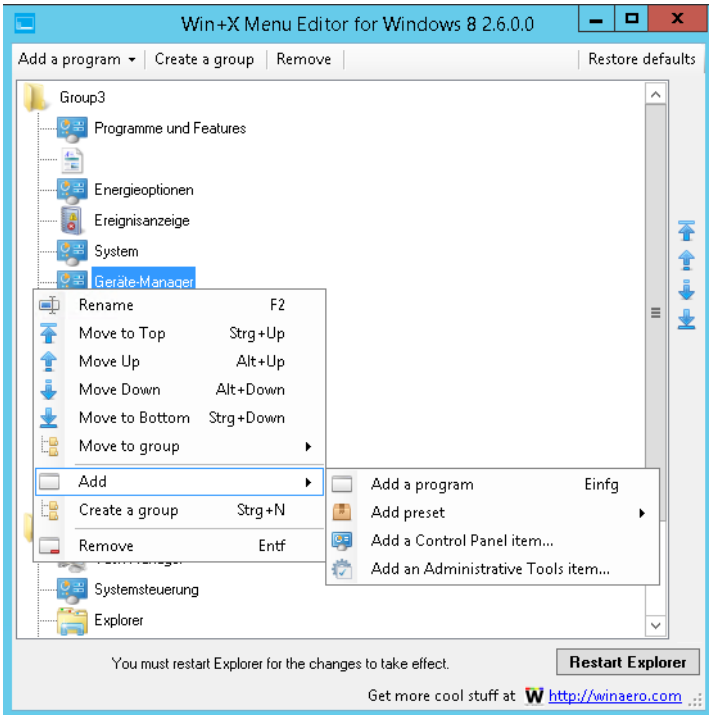
Abbildg. 3.14 Lokale Verwaltungstools über das Schnellmenü aufrufen



Herkömmliche Programme deinstallieren Sie auch in Windows Server 2012 R2 über die Systemsteuerung. Dazu suchen Sie am besten nach *appwiz.cpl* auf der Startseite.

Über das Schnellzugriffmenü finden Sie so gut wie alle wichtigen Programme, die Sie zur Verwaltung von Windows Server 2012 R2 benötigen. Sie können dieses aber über ein Tool auch bearbeiten und Befehle hinzufügen, entfernen oder gruppieren. Dazu laden Sie das Tool von der Seite *http://winaero.com/comment.php?comment.news.30* [Ms179-K03-02] herunter. Zur Bearbeitung des Schnellzugriffmenüs müssen Sie das Tool lediglich aufrufen, eine Installation ist nicht notwendig.

Abbildg. 3.15 Bearbeiten des Schnellzugriffmenüs in Windows Server 2012 R2



Eine weitere neue Tastenkombination ist ⊞+Druck. Diese Kombination erstellt automatisch einen Screenshot in Windows Server 2012 R2 und speichert ihn im *Bilder*-Ordner. Der Umweg über das Einfügen in ein Bildbearbeitungsprogramm ist nicht mehr notwendig. Mit ⊞+D starten Sie sofort den Desktop.

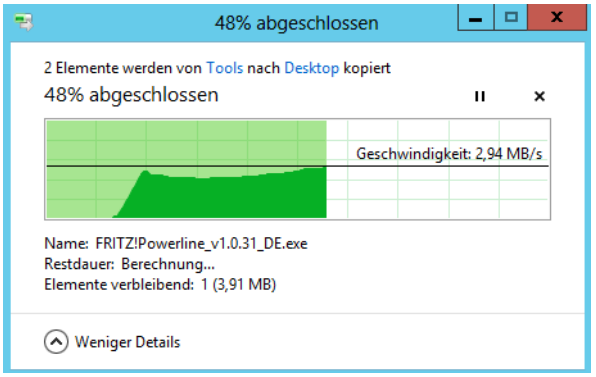
TIPP Die Systemsteuerung starten Sie durch Eingabe von *system* auf der Startseite oder über das Schnellzugriffmenü, dass sich mit ⊞+X öffnet.

Geben Sie im Suchfeld der Systemsteuerung ein kleines *L* ein (*l*), zeigt das Fenster alle verfügbaren Tools der Systemsteuerung an. Eine weitere Alternative ist die Erstellung einer Verknüpfung mit dem Befehl *Explorer.exe shell:::{ED7BA470-8E54-465E-825C-99712043E01C}*.

Ebenfalls neu ist das Kopieren/Verschieben von Dateien. Die Vorgänge lassen sich in Windows Server 2012 R2 pausieren und fortsetzen, was die Arbeit deutlich effizienter gestalten lässt. Das Dialog-

feld des Kopiervorgangs zeigt jetzt auch mehr Informationen an, zum Beispiel die Netzwerkbandbreite während des Kopiervorgangs.

Abbildg. 3.16 Dateien besser mit Windows Server 2012 R2 kopieren und verschieben



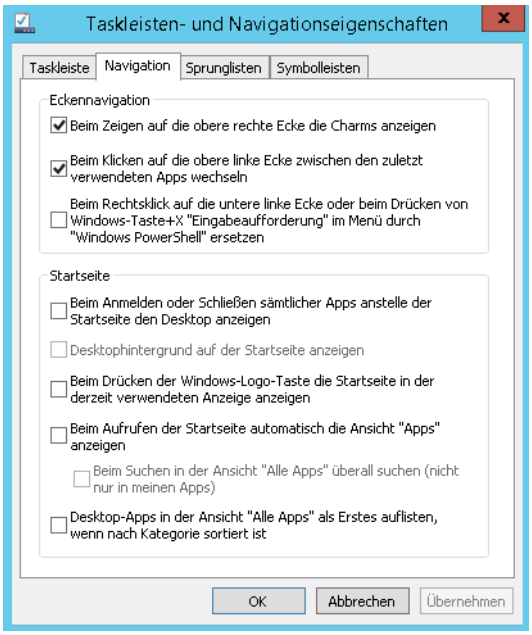
Windows Server 2012 R2 kann außerdem direkt über den Explorer ISO-Dateien und VHD/VHDX-Dateien mounten und bereitstellen. Dazu sind keine Zusatztools notwendig. Auf ISO-Dateien können Sie einfach doppelklicken, um deren Inhalt anzuzeigen. Die Einbindung von virtuellen Festplatten (VHD/VHDX-Dateien) erfolgt wesentlich einfacher und schneller als in Windows Server 2008 R2.

Neue Einstellungsmöglichkeiten für Bildschirmecken und PowerShell nutzen

Rufen Sie in Windows Server 2012 R2 über das Kontextmenü der Taskleiste die Eigenschaften auf und wechseln Sie auf die neue Registerkarte *Navigation*. Sie können jetzt verschiedene Einstellungen vornehmen. Folgende Optionen stehen Ihnen zur Verfügung:

- **Beim Zeigen auf die obere rechte Ecke die Charms anzeigen** Fahren Sie mit der Maus nach rechts oben, zeigt Windows die Charms-Leiste an. Diese können Sie auch mit ⊞+C anzeigen lassen.
- **Beim Klicken auf die obere linke Ecke zwischen den zuletzt verwendeten Apps wechseln** Klicken Sie oben links in die Ecke, können Sie zwischen den Windows-Apps umschalten, die gestartet sind. An dieser Stelle haben Sie aber nicht die Möglichkeit, zwischen Anwendungen auf dem Desktop zu wechseln. Diese fasst Windows in der Desktop-App zusammen.
- **Beim Rechtsklick auf die untere linke Ecke oder beim Drücken von Windows-Taste+(X) "Eingabeaufforderung" im Menü durch "Windows PowerShell" ersetzen"** Diese Option ersetzt die Eingabeaufforderung über das Kontextmenü der *Start*-Schaltfläche, mit der Möglichkeit die PowerShell zu starten

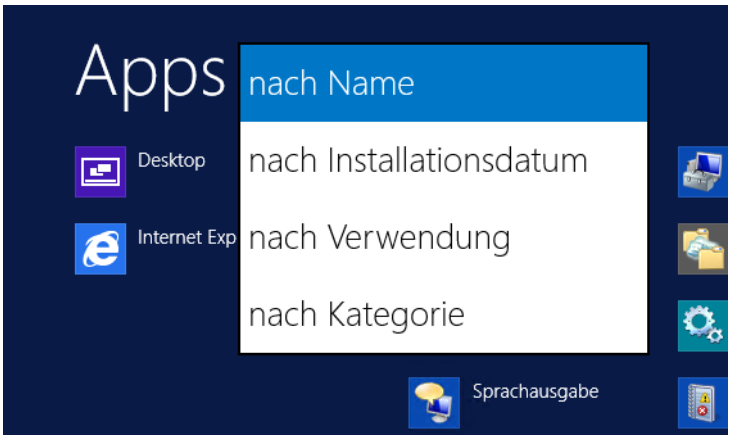
Abbildg. 3.17 Nutzen der neuen Einstellungsmöglichkeiten in Windows Server 2012 R2



- **Beim Anmelden oder Schließen sämtlicher Apps anstelle der Startseite den Desktop anzeigen** Aktivieren Sie diese Option zeigt Windows 8.1 und Windows Server 2012 R2 direkt den Desktop an, wenn Sie den Rechner starten
- **Desktophintergrund auf der Startseite verwenden** Aktivieren Sie diese Option, zeigt die Startseite das gleiche Hintergrundbild an, wie der Desktop. Dadurch entsteht der Eindruck, dass die Startseite durchsichtig ist. Sie müssen dazu aber das Feature der Desktopdarstellung in Windows Server 2012 R2 über den Server-Manager installieren.
- **Beim Drücken der Windows-Logo-Taste die Startseite in der derzeit verwendeten Anzeige anzeigen** Blendet beim Einsatz mehrerer Monitoren die Startseite immer auf dem jeweils aktiven Monitor ein
- **Beim Aufrufen der Startseite automatisch die Ansicht "Apps" anzeigen** Zeigt nicht die Startseite an, sondern die Alle-Apps-Ansicht. Aktivieren Sie noch das Kontrollkästchen *Desktop-Apps in der Ansicht „Alle Apps“ als Erstes auflisten, wenn nach Kategorie sortiert ist*, erhalten Sie eine Ansicht, ähnlich wie ein Startmenü. Nur ist dieses Menü über den kompletten Monitor verteilt.
- **Beim Suchen in der Ansicht "Alle Apps" überall suchen** Diese Option ist nur aktiv, wenn Sie die Option *Beim Aufrufen der Startseite automatisch die Ansicht "Alle Apps" anzeigen* aktivieren
- **Desktop-Apps in der Ansicht "Alle Apps" als Erstes auflisten, wenn nach Kategorie sortiert ist** Zeigt bei der Sortierung nach Kategorie in der Alle-Apps-Ansicht Programme des Desktops zuerst an

In Windows Server 2012 R2 können Sie in der Alle-Apps-Ansicht, die Sie über das Kontextmenü der Startseite starten, die Anzeige kategorisieren lassen. Dazu verwenden Sie den Pfeil in der oberen Spalte. Sie finden die Alle Apps-Ansicht auch, wenn Sie auf der Startseite den neuen Pfeil anklicken, der (manchmal erst nach einer Mausbewegung) in der linken unteren Bildschirmecke angezeigt wird.

Abbildg. 3.18 Die Apps auf der Startseite können Sie in Windows Server 2012 R2 kategorisieren lassen



Konfiguration der Startseite mit der PowerShell exportieren und importieren

In Windows 8.1 und Windows Server 2012 R2 können Sie mit dem Cmdlet *Export-StartLayout* in der PowerShell das Aussehen und die Konfiguration der Startseite in eine Datei exportieren. Mit dem Cmdlet *Import-StartLayout* importieren Sie die Einstellungen wieder. Sie können diese Funktion auch dazu nutzen, auf lokalen Rechnern festzulegen, wie die Startseite aussehen soll. Dazu passen Sie zunächst die Startseite an und exportieren diese als XML-Datei. Diese hinterlegen Sie bei den Anwendern dann als Standardseite. Die Verteilung ist auch über Gruppenrichtlinien mit Windows Server 2012 R2 möglich.

Mit dem Befehl *Get-Help <Cmdlet>* erhalten Sie eine Hilfe zu dem neuen Cmdlet. Der Umgang ist allerdings nicht sehr kompliziert. Um das aktuelle Layout zu exportieren, geben Sie folgenden Befehl ein:

```
Export-StartLayout -path <Pfad zur XML-Datei> -As XML
```

Administratoren in Unternehmensnetzwerken können sogar Veränderungen an der Startseite untersagen. Dazu gibt es ebenfalls in den Richtlinien von Windows 8.1 Pro/Enterprise und Windows Server 2012 R2 die Option *Startseitenlayout*. Diese finden Sie nach dem Aufruf von *gpedit.msc* im Editor für lokale Gruppenrichtlinien unter *Benutzerkonfiguration/Administrative Vorlagen/Startmenü und Taskleiste*. In diesem Bereich können Sie die Layoutdatei hinterlegen, die Sie vorher mit dem Cmdlet *Export-StartLayout* exportiert haben. Das funktioniert auch für lokale Rechner und lokale Richtlinien.

Ändern Sie zu viel an der Startseite und sind mit dem Ergebnis nicht zufrieden, können Sie diese relativ leicht auf den Standard nach der Installation zurücksetzen. Dazu müssen Sie im Explorer nur folgende Dateien löschen:

- *%LocalAppData%\Microsoft\Windows\appsFolder.itemdata-ms*
- *%LocalAppData%\Microsoft\Windows\appsFolder.itemdata-ms.bak*

Sie können die Dateien auch einfach verschieben oder umbenennen. Das hat den Vorteil, dass Sie diese bei Bedarf wieder aktivieren können.

Windows Server 2012 R2 herunterfahren und abmelden

Um sich ohne Zusatztools von Windows Server 2012 R2 abzumelden oder um den PC herunterzufahren, klicken Sie mit der rechten Maustaste auf die *Start*-Schaltfläche. Hier können Sie über den Befehl *Herunterfahren oder abmelden* den Server neu starten oder herunterfahren.

Tools und Möglichkeiten für das Herunterfahren

Sie können auch über den rechten oberen oder unteren Bildschirmbereich bzw. mit ⊞+C zuerst die Charms-Leiste aktivieren. Oder Sie klicken auf die Taskleiste auf dem Desktop und drücken die Tastenkombination Alt+F4.

Eine weitere Möglichkeit ist, eine eigene Verknüpfung zu erstellen und diese direkt in die Startseite zu integrieren:

Öffnen Sie den Desktop und erstellen Sie über das Kontextmenü eine neue Verknüpfung. Geben Sie den Befehl *shutdown /s /t 10* ein, um den Computer 10 Sekunden nach dem Aufruf der Verknüpfung herunterzufahren. Sie können auch eine andere Sekundenzahl eingeben; der Wert 0 fährt den PC sofort herunter.

Klicken Sie nach dem Fertigstellen der Verknüpfung mit der rechten Maustaste auf die Verknüpfung und rufen Sie die Eigenschaften auf. Klicken Sie dann auf *Anderes Symbol* und wählen Sie ein passendes Symbol für das Herunterfahren aus. Fügen Sie die Verknüpfung über das Kontextmenü der Startseite hinzu (Befehl *An "Start" anheften*). Die Verknüpfung ist jetzt auf der Startseite verfügbar. Per Ziehen/Ablegen können Sie diese an jede beliebige Stelle verschieben.

Wollen Sie noch ein Symbol für den Neustart hinterlegen, verwenden Sie den Befehl *shutdown /r /t 10*. Um den Vorgang innerhalb der vorgegebenen Zeit zu unterbrechen, verwenden Sie *shutdown /a*. Auch dafür können Sie eine Verknüpfung erstellen.

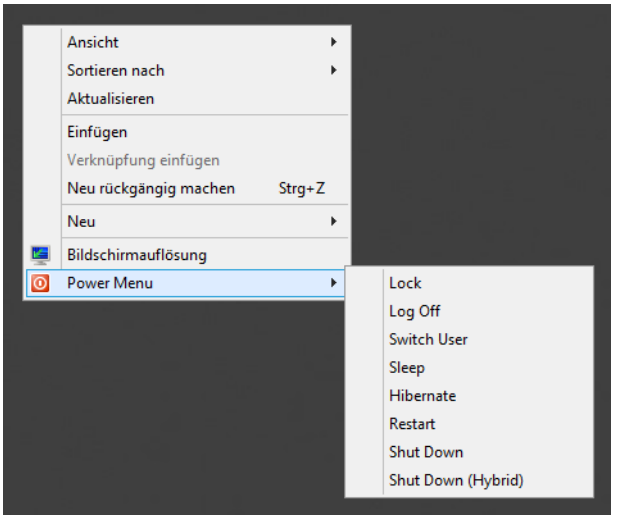
Möchten Sie zusätzlich das Abmelden hinterlegen, erstellen Sie eine Verknüpfung mit dem Befehl *logoff*. Auch hier können Sie ein eigenes Symbol verwenden. Alternativ melden Sie sich über das Kontextmenü des Benutzernamens auf der Startseite ab. Das Gleiche gilt für das Sperren.

Sie können den PC über eine Verknüpfung auf dem Desktop sperren. Verwenden Sie als Eingabeaufforderung für die Verknüpfung *rundll32.exe user32.dll, LockWorkStation*. Achten Sie auf das Komma und die Groß- und Kleinschreibung von *LockWorkStation*. Weisen Sie der Verknüpfung einen passenden Namen zu, zum Beispiel »PC sperren«. Auch diese Verknüpfung können Sie über das Kontextmenü an die Startseite anheften. Die schnellere Variante dafür ist die Tastenkombination ⊞+L.

Sie können erstellte Verknüpfungen auf dem Desktop löschen, wenn Sie diese über das Kontextmenü mit der Startseite verbunden haben. Der Nachteil beim Integrieren eigener Befehle in die Startseite ist, dass diese schnell (unnötig) unübersichtlich wird. Um Windows Server 2012 R2 einfacher herunterfahren und neu starten zu können, besteht auch die Möglichkeit, im Kontextmenü des Windows Server 2012 R2-Desktops Befehle zum Herunterfahren und Neustart zu integrieren.

Alternativ laden Sie sich das Registry-Skript von der Seite *http://www.askvg.com/add-cascading-menu-for-restart-shut-down-hibernate-and-other-power-shortcuts-in-desktop-context-menu-of-windows-7-and-8* [Ms179-K03-03] herunter. Dieses installieren Sie am einfachsten per Doppelklick. Der Download umfasst auch ein Skript, welches die Änderungen wieder entfernt. Nach der Installation finden Sie den neuen Menübefehl *Power Menu* im Kontextmenü des Desktops vor.

Abbildg. 3.19 Erstellen eines eigenen Menüs zum Herunterfahren



Eine weitere Möglichkeit, das Dialogfeld für das Herunterfahren und den Neustart zu integrieren, ist das Erstellen eines kleinen Skripts. Dieses hinterlegen Sie auf dem Desktop und können auf diesem Weg schnell und einfach den PC neu starten. Erstellen Sie dazu zunächst eine neue Textdatei und nehmen folgenden Text in die Datei auf:

Listing 3.1 Erstellen eines Skripts für das Herunterfahren von Windows

```
dim objShell
set objShell = CreateObject("shell.application")
objshell.ShutdownWindows
set objShell = nothing
```

Weisen Sie der Datei dann die Endung *.vbs* zu. Damit dies funktioniert, müssen Sie im Menüband des Explorers auf der Registerkarte *Ansicht* in der Gruppe *Ein-/ausblenden* das Kontrollkästchen *Dateinamenerweiterungen* aktivieren. Klicken Sie anschließend doppelt auf die angelegte Datei, erscheint das bekannte Dialogfeld zum Herunterfahren oder den Neustart. Wollen Sie ein eigenes Symbol festlegen, kopieren Sie das Skript in den *Windows*-Ordner und erstellen Sie auf dem Desktop eine Verknüpfung zu dieser Datei. Über das Kontextmenü können Sie noch ein eigenes Symbol zuweisen und den Befehl in die Taskleiste oder die Startseite integrieren.

In der PowerShell können Sie einen Computer mit *Restart-Computer* neu starten. Microsoft bietet in seiner TechNet Gallery (*http://gallery.technet.microsoft.com* [Ms179-K03-04]) zahlreiche Skripts für

die PowerShell an. Allerdings erstellt das Skript auch nur Kacheln, die den Befehl *Shutdown.exe* nutzen.

Eines dieser Skripts integriert Kacheln zum Herunterfahren, Neustarten und zur Abmeldung in die Startseite. Laden Sie dazu zunächst das Skript von der Seite *http://gallery.technet.microsoft.com/Create-a-ShutdownRestartLog-37c8111d* [Ms179-K03-05] herunter.

Entpacken Sie das Skript in ein beliebiges Verzeichnis und laden Sie es in eine PowerShell-Sitzung mit dem Befehl:

```
Import-Module c:\<Pfad zur PSM-Datei>\CreateWindowsTile.psm1
```

Erhalten Sie eine Fehlermeldung, dass die PowerShell keine Skripts erlaubt, müssen Sie die PowerShell zuerst für die Ausführung von Skripts konfigurieren. Danach können Sie die Sicherheitseinstellungen auf Wunsch wieder restriktiver setzen.

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.

Sie müssen immer einen vollqualifizierten Pfad zu der Skriptdatei angeben, auch wenn sich das Skript im aktuellen Verzeichnis befindet. Wenn Sie auf das aktuelle Verzeichnis verweisen wollen, 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 blockiert die PowerShell Skripts.

Sie können die Ausführungsrichtlinie mit dem Cmdlet *Set-ExecutionPolicy* ändern und mit *Get-ExecutionPolicy* anzeigen. *Set-ExecutionPolicy Restricted* verhindert das Ausführen jeglicher Skripts. Mit *Set-ExecutionPolicy AllSigned* werden nur vertrauenswürdige Skripts ausgeführt. *Set-ExecutionPolicy Unrestricted* erlaubt alle Skripts. Diese Einstellung sollten Sie setzen. Sie müssen dazu die PowerShell aber über das Kontextmenü mit Administratorrechten starten.

Nachdem Sie Skripts erlaubt haben, können Sie die Skript für die Erstellung von Kacheln laden lassen:

```
Import-Module c:\<Pfad zur PSM-Datei>\CreateWindowsTile.psm1
```

Eine umfassende Hilfe erhalten Sie mit dem Befehl:

```
Get-Help New-OSCWindowsTile -Full
```

Die Kacheln für das Herunterfahren, Abmelden und zum Neustart erzeugen Sie mit:

```
New-OSCWindowsTile
```

Die erfolgreiche Erstellung der Kacheln wird angezeigt.

Erweiterte Startoptionen nutzen

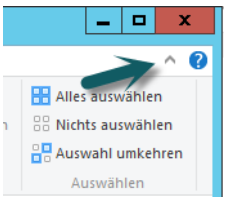
Die erweiterten Startoptionen kennt Windows Server 2012 R2 auch noch. Wir kommen in Kapitel 35 noch ausführlicher auf das Thema zu sprechen. Hier stehen verschiedene Möglichkeiten zur Verfügung:

- **Debugmodus** Startet Windows in einem erweiterten Problembehandlungsmodus
- **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 kann
- **Videomodus mit niedriger Auflösung aktivieren** Startet Windows mithilfe des aktuellen Videotreibers und mit niedrigen Einstellungen für Auflösung und Aktualisierungsrate. Mithilfe dieses Modus können Sie die Anzeigeeinstellungen zurücksetzen.
- **Abgesicherter Modus** Startet Windows mit den mindestens erforderlichen Treibern und Diensten
- **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
- **Erzwingen der Treibersignatur deaktivieren** Ermöglicht, dass Treiber mit ungültigen Signaturen installiert werden
- **Frühen Start des Treibers der Antischadsoftware deaktivieren** In Windows Server 2012 R2 startet der installierte Virenscanner wesentlich früher als in Windows Server 2008 R2. Das kann zu Problemen führen, wenn der Computer nicht mehr startet. Hier deaktivieren Sie diesen Schutz.
- **Automatischen Neustart bei Systemfehler deaktivieren** Verhindert, dass Windows nach einem durch einen eigenen Fehler 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.

Der verbesserte Explorer

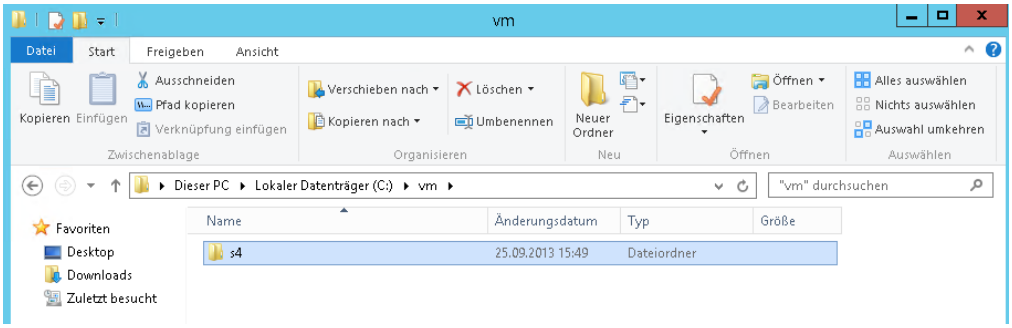
Der in früheren Windows-Versionen als Windows-Explorer bezeichnete neue Explorer lässt sich generell genauso bedienen wie in Vorgängerversionen. Im Gegensatz zu Windows Server 2008 R2 enthält die neue Explorer-Version jedoch ein Menüband wie beispielsweise Office 2013. Über den kleinen Pfeil links neben dem Hilfesymbol am rechten oberen Rand blenden Sie das Menüband ein oder aus. Die grundsätzliche Bedienung des Explorers entspricht noch der in Windows Server 2012.

Abbildg. 3.20 Menüband des Explorers ein- und ausblenden



Das Menüband zeigt immer die entsprechenden Befehle an, die das aktuelle Objekt unterstützt. Wollen Sie zum Beispiel die Anzeigeeinstellungen ändern (beispielsweise die versteckten Dateien anzeigen oder Dateiendungen auch für bekannte Dateitypen einblenden), finden Sie diese Einstellungen in Windows Server 2012 R2 auf der Registerkarte *Ansicht* in der Gruppe *Ein-/ausblenden* in Form der Kontrollkästchen *Dateinamenerweiterungen* und *Ausgeblendete Elemente*.

Abbildg. 3.21 Verwenden des neuen Menübands im Explorer



Alternativ können Sie auf der Registerkarte *Ansicht* über den Menübefehl *Optionen/Ordner- und Suchoptionen ändern* das Dialogfeld *Ordneroptionen* aufrufen. Wechseln Sie darin zur Registerkarte *Ansicht* und wählen Sie die gewünschten Einstellungen aus.

Wie die aktuellen Office-Programme verfügt jetzt auch der Explorer über eine Symbolleiste für den Schnellzugriff. Diese finden Sie in der Titelleiste im oberen Bereich.

Wollen Sie den Explorer auch auf der Startseite einblenden, haben Sie die Möglichkeit, verschiedene Ordner zu verwenden. Sie können Ordner als Verknüpfung auf der Startseite anlegen und so den Explorer direkt für einen speziellen Ordner öffnen. Diese können Sie auch in die Taskleiste des Windows Server 2012 R2-Desktops integrieren.

Der einfachste Weg ist zunächst, wenn Sie auf der Startseite nach *explorer* suchen und die daraufhin angezeigte Kachel mit der rechten Maustaste anklicken. Anschließend können Sie eine Verknüpfung des Explorers durch Auswahl von *An "Start" anheften* in der App-Leiste direkt in die Startseite integrieren.

Auf diesem Weg heften Sie den Explorer auch an die Taskleiste des Desktops mit einer Option an, direkt einen speziellen Ordner zu öffnen. Direkt auf dem Desktop können Sie in der Taskleiste weitere Verknüpfungen zu speziellen Ordnern auch mit eigenen Symbolen anlegen, um bestimmte Bereiche schneller starten zu können. Haben Sie auf dem Desktop eine Verknüpfung zu einem Ordner oder einer Datei angelegt, können Sie diese über das Kontextmenü zur Startseite hinzufügen.

HINWEIS Starten Sie den Explorer in der Taskleiste, öffnet sich die Ansicht der Benutzerordner. Bibliotheken gibt es in Windows 8.1 und Windows Server 2012 R2 nicht mehr.

Ziehen Sie einen Ordner vom Desktop per Ziehen/Ablegen in die Taskleiste, wird dieser automatisch zum Explorer-Symbol als *Angeheftet* hinzugefügt. Klicken Sie mit der rechten Maustaste auf das Explorer-Symbol, können Sie über die Sprungliste auf die häufigsten Ordner und die angehefteten Ordner zugreifen. Ordner, die in die Sprungliste aufgenommen, aber noch nicht angeheftet sind, können Sie über den Pinn anheften.

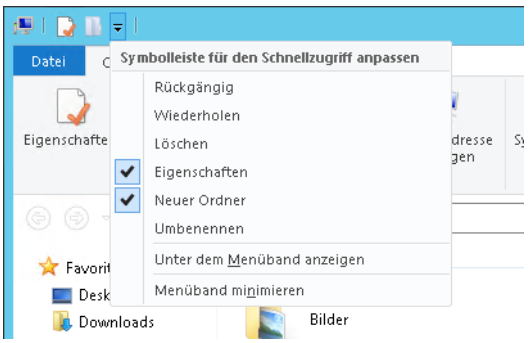
Es gibt aber auch die Möglichkeit, für einzelne Ordner eigene Symbole in der Taskleiste aufzunehmen. Der Vorteil ist, dass Sie diese Ordner dann nicht über das Explorer-Symbol aufrufen müssen, sondern ein eigenes Symbol für den Ordner mit eigenem Symbol erstellen können. Gehen Sie dazu folgendermaßen vor:

1. Erstellen Sie über das Kontextmenü des Desktops eines neue Textdatei und geben dieser Datei die Bezeichnung, wie der Ordner später in der Taskleiste erscheinen soll, und weisen Sie dieser die Endung *.exe* zu. Achten Sie darauf, dass die Datei auch ausführbar sein muss. Sind die Dateiendungen bei Ihnen noch ausgeblendet, können Sie über die Registerkarte *Ansicht* des Explorer-Menübands in der Gruppe *Ein-/ausblenden* die beiden Kontrollkästchen *Dateinamenerweiterungen* und *Ausgeblendete Elemente* aktivieren.
2. Klicken Sie die neue ausführbare Datei mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *An Taskleiste anheften*.
3. Klicken Sie als Nächstes das neu erstellte Symbol in der Taskleiste mit der rechten Maustaste an, um dessen Sprungliste aufzurufen.
4. Klicken Sie dann mit der rechten Maustaste auf den Namen des Programms und wählen Sie im Kontextmenü den Befehl *Eigenschaften*.
5. Geben Sie im daraufhin geöffneten Dialogfeld auf der Registerkarte *Verknüpfung* im Feld *Ziel* den Pfad des Ordners an, den Sie mit dem Symbol öffnen wollen.
6. Über die Schaltfläche *Anderes Symbol* wählen Sie noch ein passendes Symbol für den Ordner aus. Das neue Symbol erscheint teilweise erst nach dem Neustart des Rechners oder nach einiger Zeit.
7. Die ausführbare Datei auf dem Desktop können Sie löschen, diese benötigen Sie nicht mehr. Klicken Sie zukünftig auf das Symbol in der Taskleiste, öffnet sich der Ordner, der in den Eigenschaften festgelegt ist. Dies kann wesentlich sinnvoller sein, als über angeheftete Ordner im Explorer zu arbeiten.

Explorer im schnellen Überblick

Ein wichtiger Punkt im Menüband ist die Symbolleiste für den Schnellzugriff. Hier können Sie Funktionen hinterlegen, die Sie häufig benötigen. Dies funktioniert im Explorer genauso wie in Office 2013-Anwendungen. Sie finden diese Leiste ganz oben links im Fenster.

Abbildg. 3.22 Symbolleiste für den Schnellzugriff im Explorer



Um der Leiste eine neue Funktion hinzuzufügen, können Sie jeden beliebigen Befehl im Menüband mit der rechten Maustaste anklicken und über das Kontextmenü in die Symbolleiste für den Schnellzugriff aufnehmen.

Einen Befehl können Sie wieder entfernen, indem Sie diesen in der Symbolleiste für den Schnellzugriff mit der rechten Maustaste anklicken und im Kontextmenü den Befehl *Aus Symbolleiste für den Schnellzugriff entfernen* wählen.

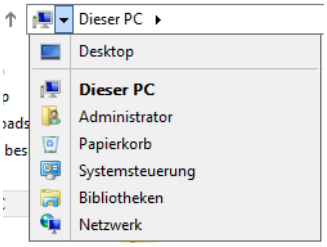
Navigieren im Explorer

Oben links im Explorer-Fenster finden Sie eine Vor- und Zurückschaltfläche. Mit diesen können Sie zum vorher geöffneten Ordner zurückwechseln. Mit der Schaltfläche *Hoch nach* (Pfeil nach oben) links neben der Adressleiste wechseln Sie in den übergeordneten Ordner.

Die Adressleiste zeigt den genauen Standort des derzeitig geöffneten Ordners an. Sie können entweder direkt auf einen übergeordneten Ordner klicken, um diesen zu öffnen, oder über das kleine Dreieck neben jedem Ordner dessen Unterordner anzeigen lassen und zu diesen navigieren.

Wenn Sie auf das erste Dreieck in der Adressleiste klicken, werden Ihnen einige Standardordner des Betriebssystems angezeigt. Über diese Standardordner können Sie jetzt auch die eigenen Dateien öffnen, die nicht mehr unter dieser Bezeichnung angezeigt werden, sondern als Benutzername des angemeldeten Benutzers. Sie können dadurch im Explorer zu jeder Zeit in den Stammordner Ihrer persönlichen Dokumente wechseln.

Abbildg. 3.23 Wechseln zwischen Ordnern im Explorer



Wenn Sie mit der rechten Maustaste auf die Adressleiste klicken, können Sie den derzeitigen Pfad in die Zwischenablage kopieren und in einem anderen Programm wieder einfügen. Mit einem Doppelklick auf den Pfad 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 Explorer die Ansicht durch die F5-Taste oder per Klick auf die Aktualisierungsschaltfläche neben der Adressleiste aktualisiert werden.

Rechts neben der Adressleiste befindet sich ein Suchfeld, in das Sie beliebige Suchbegriffe eintippen können. Auf der nun angezeigten Registerkarte *Suchen* lassen sich die Sucheinstellungen weiter verfeinern. Suchen Sie häufig nach den gleichen Begriffen, klicken Sie auf *Suche speichern*. In diesem Fall erscheint die Suchanfrage innerhalb des *Favoriten*-Ordners im Navigationsbereich des Explorer-Fensters und Sie können die Suche durch einen einfachen Klick starten.

Eine wichtige Funktion im Explorer ist der Bereich *Favoriten*. Sie können den Inhalt in dieser Ansicht selbst definieren. Wenn Sie einzelne Favoriten nicht verwenden wollen, können Sie mit der rechten Maustaste auf den entsprechenden Eintrag klicken und *Entfernen* auswählen.

Sobald Sie im Explorer auf einen solchen Favoriten klicken, wechseln Sie sofort zu diesem Ordner, was die Navigation enorm vereinfacht. Um einen Favoriten zu erstellen, navigieren Sie zunächst zu dem Ordner, den Sie als Favoriten festlegen wollen. Im Anschluss klicken Sie auf den Ordner mit der linken Maustaste und ziehen diesen in den Bereich der Favoriten. Im Anschluss wird eine Verknüpfung zu diesem Ordner in den Favoriten erstellt.

Die Detailansicht im Explorer zeigt, abhängig vom markierten Ordner, detaillierte Informationen über den Ordner, das Laufwerk oder die markierte Datei an. Sie können in diesem Fenster bei Dateien zum Beispiel einen Autor, einen Titel oder ein Thema hinterlegen, nach dem wiederum in der erweiterten Suche gesucht werden kann. Der Explorer von Windows Server 2012 R2 blendet die Dateiendungen von Dokumenten aus. Um die Dateiendungen anzuzeigen, aktivieren Sie im Menüband des Explorers die Registerkarte *Ansicht* und schalten das Kontrollkästchen *Dateinamenerweiterungen* ein. An dieser Stelle können Sie auch die versteckten Dateien einblenden lassen.

Im Explorer können Sie die Größe der einzelnen Spalten in der *Details*-Ansicht (auswählbar über die Registerkarte *Ansicht* in der Gruppe *Layout*) mit der Maus verändern. Eine Spalte lässt sich automatisch an den längsten darin enthaltenen Eintrag anpassen, indem Sie auf den Spaltentrenner doppelklicken, während der Pfeil zum Vergrößern oder Verkleinern der Spalte angezeigt wird. Klicken Sie auf eine Spaltenüberschrift und halten Sie die Maustaste gedrückt, können Sie Spalten auch neu anordnen.

Die Ansicht im Fenster wird nach der Spalte sortiert, auf deren Spaltenüberschrift Sie mit der Maus klicken. Mit jedem Klick auf die Spaltenüberschrift wird die Sortierung umgekehrt. Bei Dateinamen würde dann beispielsweise aus einer zunächst alphabetisch aufsteigenden Sortierung (A-Z) eine alphabetisch absteigende (Z-A).

Eine weitere Möglichkeit zur besseren Übersicht ist das Vorschaufenster im Explorer. Wenn Sie dieses durch Aktivierung von *Vorschaufenster* oder *Detailbereich* auf der Registerkarte *Ansicht* einblenden lassen, wird auf der rechten Seite des Explorers eine Vorschau der momentan markierten Datei angezeigt. Sie können die Größe der Vorschau stufenlos erhöhen, indem Sie den Bereich des Vorschaufensters im Explorer vergrößern. Mit der Tastenkombination Alt + P können Sie das Vorschaufenster ebenfalls aktivieren oder deaktivieren.

Wenn Sie den Explorer starten, werden Ihnen neben den Ordnern auch die Laufwerke und deren Optionen angezeigt, indem Sie im Navigationsbereich auf *Dieser PC* klicken. Sie sehen hier auf einen Blick, wie viel Speicherplatz noch auf den einzelnen Laufwerken frei ist. Der Explorer zeigt diese Informationen zusätzlich noch in einem farbigen Balken an. Wenn sich die Speicherkapazität des Laufwerks dem Ende zuneigt, wird der Balken in roter Farbe angezeigt, ansonsten ist dieser blau. Durch diese Funktion werden Ihnen die wichtigsten Informationen über die Laufwerke bereits beim Starten des Explorers angezeigt.

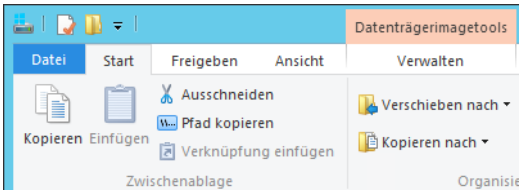
Wollen Sie eine neue Instanz eines bereits gestarteten Programms, zum Beispiel des Explorers starten oder eine neue Sitzung für den Browser, müssen Sie normalerweise das Sprungmenü der Anwendung über das Kontextmenü aufrufen. Anschließend klicken Sie auf den Namen des Programms im Sprungmenü, um eine neue Instanz zu starten. Schneller können Sie eine neue Instanz starten, wenn Sie das Symbol in der Taskleiste mit gehaltener ⇧-Taste anklicken.

Noch schneller geht der Start, wenn Sie das Symbol mit der mittleren Maustaste oder dem Mausrad anklicken.

Explorer im Schnelldurchlauf

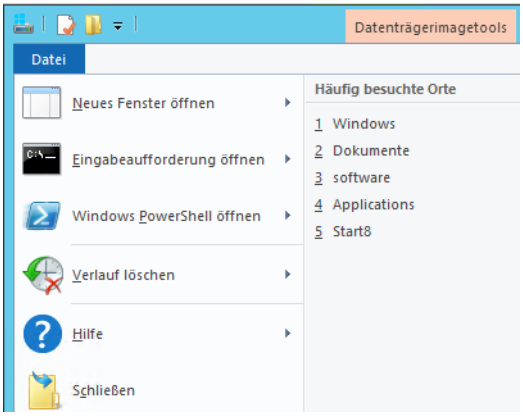
Die Funktionen im Explorer sind auf die verschiedenen Registerkarten *Start*, *Freigeben*, *Ansicht* und *Verwalten* aufgeteilt.

Abbildg. 3.24 Die verschiedenen Registerkarten im Explorer



Zusätzlich gibt es die Registerkarte *Datei*, mit der Sie Verwaltungsaufgaben wie neue Explorer-Fenster, Eingabeaufforderungen oder PowerShell-Sitzungen starten können. An dieser Stelle sehen Sie die zuletzt geöffneten Ordner und können diese schneller erreichen. Ordner können Sie an dieser Stelle anpinnen.

Abbildg. 3.25 Verwenden der Registerkarte *Datei*



Auf der Registerkarte *Start* finden Sie die wichtigen Befehle zur Verwaltung der Dateien. Sie können an dieser Stelle Dateien verschieben und kopieren. Interessant ist das Dropdownmenü zur Schaltfläche *Einfacher Zugriff* in der Gruppe *Neu*. Hierüber können Sie zum Beispiel Ordner schneller zugreifbar machen. Sie können Ordner direkt auf der Startseite anheften, zu den Explorer-Favoriten hinzufügen, in Bibliotheken aufnehmen oder als Netzlaufwerk im Explorer darstellen.

Über die Registerkarte *Freigeben* steuern Sie, wie Sie das Element (Datei oder Ordner) anderen Benutzern im Netzwerk oder auf dem PC zur Verfügung stellen wollen. Sie können Daten drucken, auf CD/DVD brennen und im Netzwerk freigeben. Mit der Schaltfläche *ZIP* erstellen Sie ein ZIP-Archiv des Ordners oder Dokuments.

Auf der Registerkarte *Ansicht* steuern Sie, wie die Ordner im Fenster angezeigt werden sollen. Sie können die Sortierung ändern, Dateinamenerweiterungen einblenden und Optionen zur Ansicht ändern.

Die Registerkarte *Verwalten* blendet der Explorer ein, wenn für einen Ordner oder eine Datei besondere Optionen zur Verfügung stehen, zum Beispiel die Möglichkeit, Kompatibilitätsprobleme zu lösen oder Programme als Administrator auszuführen. Markieren Sie ISO- oder VHD/VHDX-Dateien, lassen sich diese per Doppelklick oder über die Registerkarte *Verwalten* im Explorer bereitstellen oder direkt brennen.

Markieren Sie Bilder oder Dokumente, kommen andere Tools, abhängig von den Möglichkeiten der Datei, zum Einsatz. Klicken Sie im Navigationsbereich auf *Dieser PC*, können Sie über das daraufhin geöffnete Fenster den Computer verwalten, Netzlaufwerke verbinden, Programme deinstallieren und vieles mehr.

Markieren Sie im Explorer einzelne Laufwerke, stehen auf der Registerkarte *Verwalten* noch weitere Befehle zur Verfügung, zum Beispiel die direkte Verschlüsselung mit BitLocker, das Formatieren, Bereinigen oder die automatische Wiedergabe.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie mit der neuen Oberfläche in Windows Server 2012 R2 umgehen. Wir sind darauf eingegangen, wie Sie Server im Netzwerk verwalten und mit dem neuen Server-Manager in Windows Server 2012 R2 umgehen. Auch zahlreiche Tricks zum Umgang mit der neuen Oberfläche (die Startseite) und dem neuen Explorer haben wir Ihnen gezeigt.

Auch die Verwaltung und Einrichtung von Core-Servern sowie die Verwaltung von Windows Server 2012 R2 mit den Remoteserver-Verwaltungstools in Windows war Bestandteil des Kapitels.

Im nächsten Kapitel erfahren Sie, wie Serverrollen und Features in Windows Server 2012 R2 installiert werden. Auch hier hat sich einiges im Vergleich zu Windows Server 2008 R2 verändert.

Kapitel 4

Serverrollen und Features installieren und einrichten

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, welche verschiedenen Serverrollen und Features es gibt und wie Sie diese installieren. Microsoft hat in Windows Server 2012 R2 den Ansatz von Exchange Server fortgeführt, bei dem Sie einem Server speziell jene 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.

In Windows Server 2012 R2 installieren Sie Rollen und Features über einen gemeinsamen Assistenten, auf Wunsch auch beides gemeinsam. Das erspart Neustarts und unnötige Konfigurationen. Außerdem können Sie in Windows Server 2012 R2 Rollen und Features über den Server-Manager auch auf anderen Servern im Netzwerk installieren.

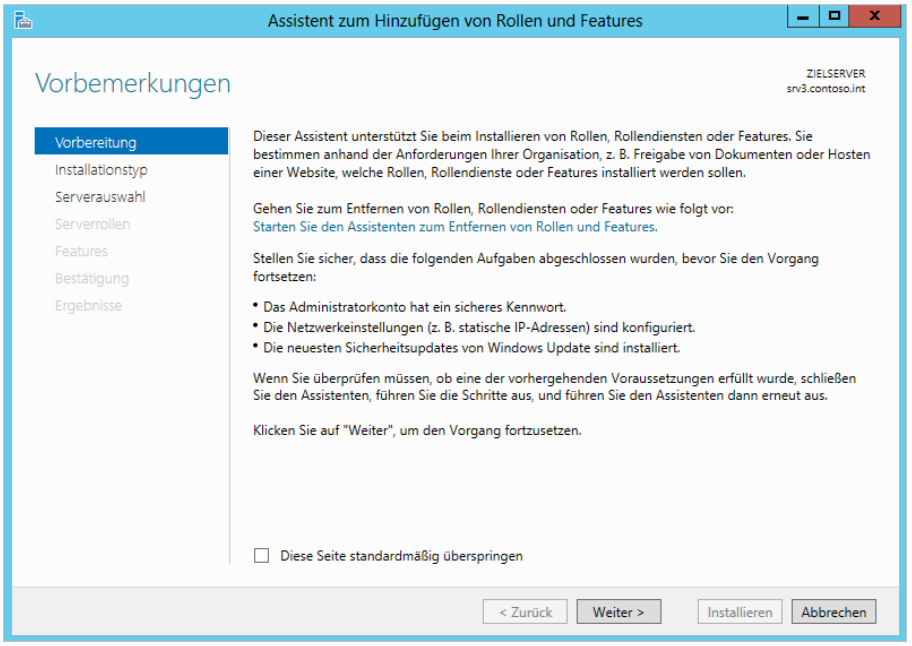
Installieren von Serverrollen und Features auf einem Server

Auf einem Server lassen sich mehrere Rollen parallel und gleichzeitig über den Assistent installieren. In Windows Server 2012 R2 können Sie über diesen Weg auch Features installieren. Über den Eintrag *Verwalten/Rollen und Features hinzufügen* im Server-Manager startet ein Assistent, über den Sie einzelne Rollen auswählen und installieren können.

Rollen installieren

Rollen sind meistens in mehrere Rollendienste aufgeteilt, die Sie auch nachträglich noch hinzufügen können. Dazu müssen Sie einfach den entsprechenden Assistenten erneut starten.

Abbildg. 4.1 Serverrollen werden über einen Assistenten installiert

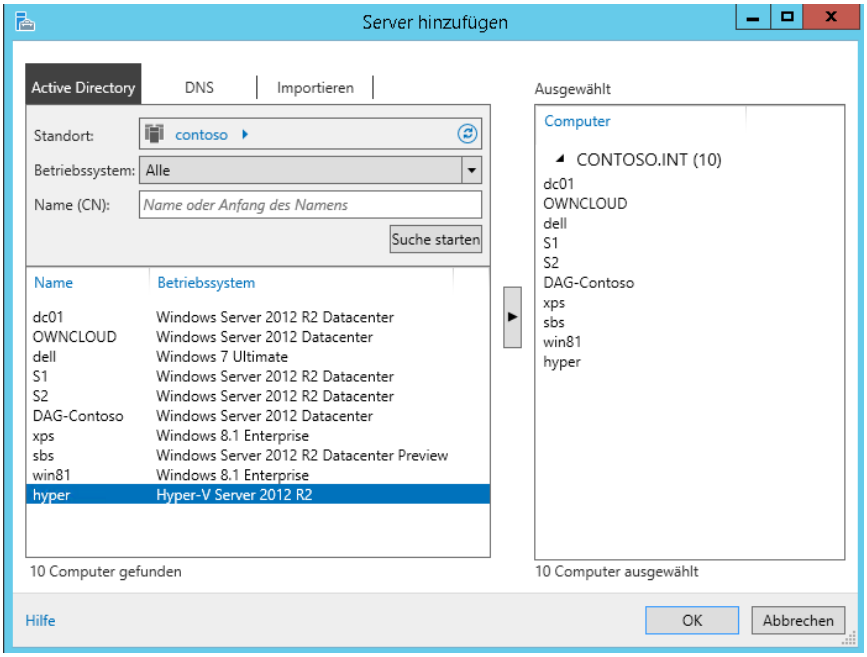


Auf der ersten Seite des Assistenten wählen Sie zunächst aus, ob Sie eine Serverrolle oder die Remotedesktopdienste installieren möchten. Diese werden in Windows Server 2012 R2 über den Assistenten zur Installation von Serverrollen getrennt eingerichtet.

Abbildg. 4.2 Auswählen des Installationstyps

Haben Sie den Installationstyp ausgewählt, können Sie auf der nächsten Seite des Assistenten den Zielserver auswählen, auf dem die Serverrolle installiert werden soll. Sie sehen im Fenster aber nur Server mit Windows Server 2012 R2 sowie Server, die Sie im Server-Manager bereits hinzugefügt haben. Außerdem müssen die Server gestartet sein. Server, die nicht eingeschaltet sind, blendet der Assistent aus.

Abbildg. 4.3 Auswählen von weiteren Servern zur Verwaltung im Server-Manager

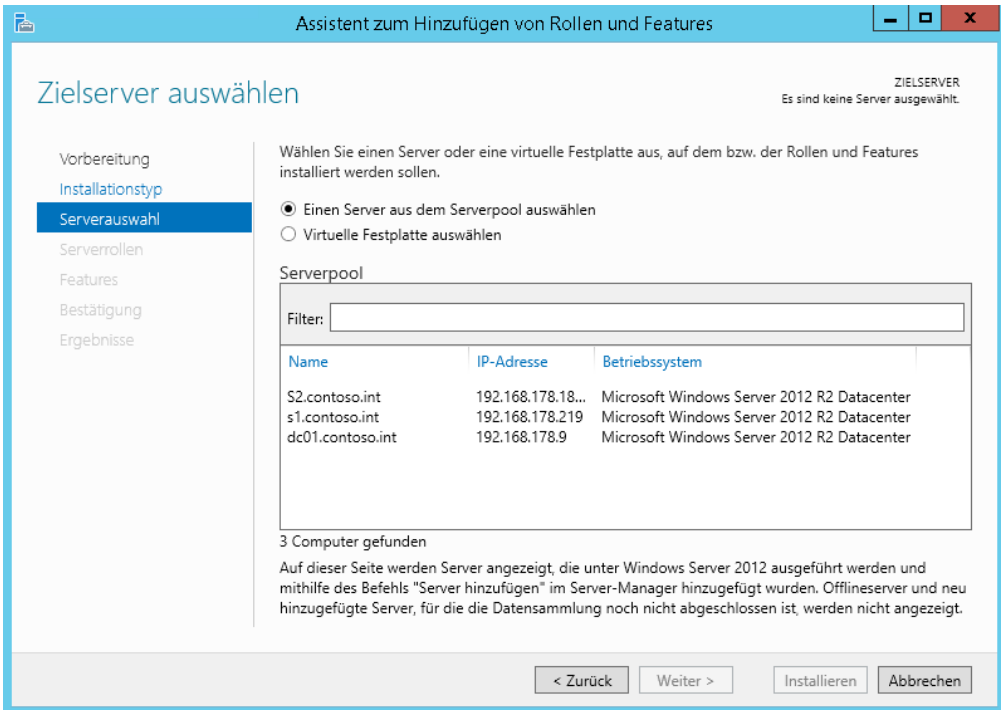


Um Server im Server-Manager hinzuzufügen, klicken Sie auf *Verwalten/Server hinzufügen*. Anschließend können Sie im Fenster eine Suche nach den Servern in der Domäne starten und diese im Assistenten hinzufügen. Damit die Server im Assistenten zum Hinzufügen von Rollen angezeigt werden, müssen Sie teilweise etwas warten und den Assistenten dann neu starten. Mehr zu diesem Thema lesen Sie in den Kapiteln 2 und 3.

Starten Sie den Installations-Assistenten für Rollen und Features, scannt der Assistent nach Servern, die im lokalen Server-Manager angebunden und die auch online sind. Aus diesen Servern können Sie den Zielserver auswählen, um Rollen und Features zu installieren.

Sie können an dieser Stelle aber nicht nur einen Server auswählen, der gerade online ist, sondern auch virtuelle Festplatten, auf denen Windows Server 2012 R2 installiert ist. Wählen Sie diese Option aus, müssen Sie im unteren Eingabefeld den Speicherort der virtuellen Festplatte angeben. Dabei kann es sich auch um eine Netzwerkfreigabe handeln.

Abbildg. 4.4 Auswählen des Zielservers zur Installation von Serverrollen und Features



Haben Sie den Server oder die virtuelle Festplatte ausgewählt, auf dem Sie Serverrollen und Features installieren wollen, wählen Sie auf der nächsten Seite aus, welche Rolle Sie installieren wollen.

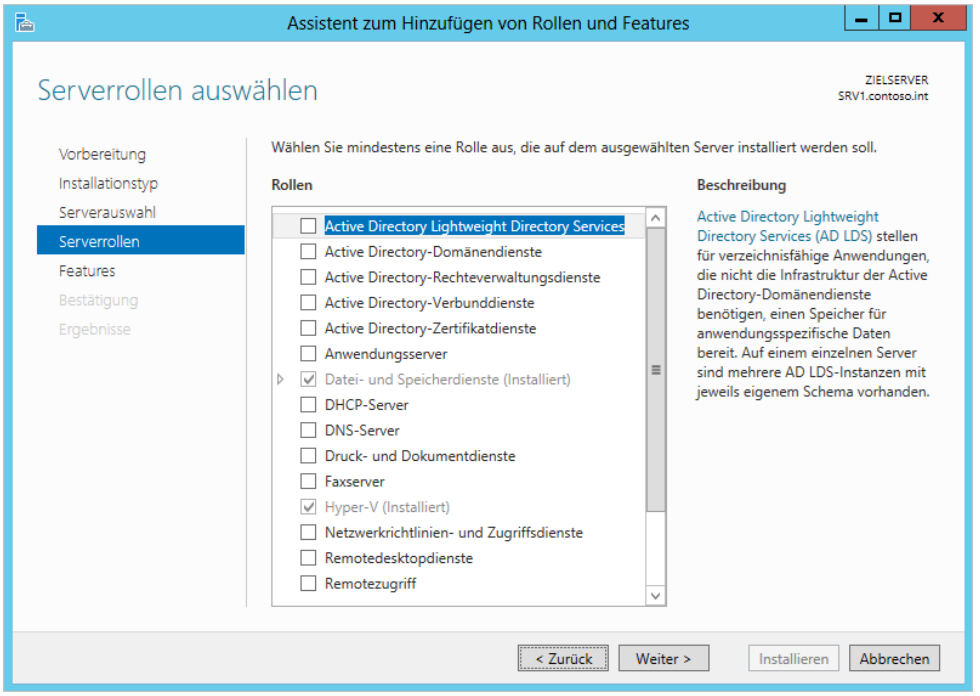
Wählen Sie eine Rolle zur Installation aus, zeigt der Assistent alle abhängigen Rollendienste und Features an, die durch Auswahl dieser Rolle auf dem Server ebenfalls notwendig sind. Folgende Rollen stehen für Windows Server 2012 R2 zur Verfügung:

- **Active Directory Lightweight Directory Services (AD LDS)** Mit diesen Diensten können Applikationen arbeiten, die Informationen in einem Ordner speichern. Im Gegensatz zu den Active Directory-Domänendiensten wird der Ordner nicht als Dienst ausgeführt. Diese Dienste

benötigen keinen reinen Domänencontroller. Auf einem Server können mehrere Instanzen laufen. Bei 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-Ordner für Anwendungen erstellt werden, die wiederum mit Active Directory synchronisiert werden und dieses auch für die Authentifizierung nutzen können. Auf einem Server lassen sich parallel mehrere Instanzen betreiben. Der Dienst ist für Organisationen entwickelt, die eine flexible Unterstützung ordnerfähiger Anwendungen benötigen. Mit dem Dienst können Unternehmen zum Beispiel andere LDAP-Ordner in Testumgebungen installieren, ohne auf Software eines Drittanbieters zurückgreifen zu müssen.

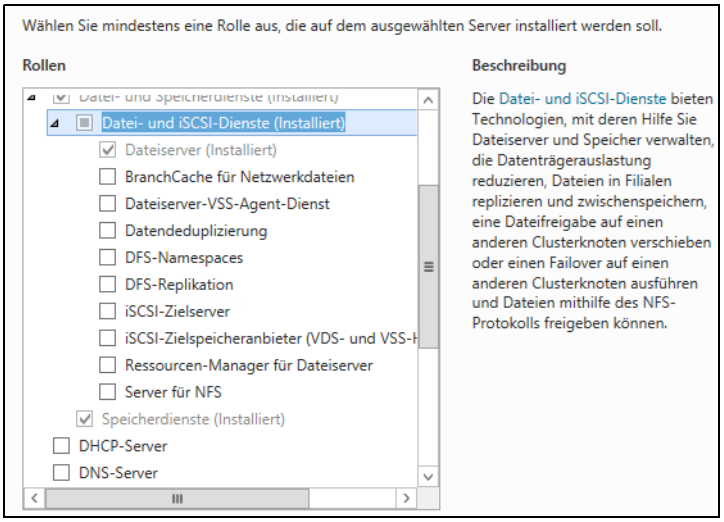
- **Active Directory-Domänendienste (Active Directory Domain Services, AD DS)** Hierbei handelt es sich um die Rolle eines Domänencontrollers für das Active Directory. Bevor Sie einen Server zum Domänencontroller für das Active Directory heraufstufen können, muss diese Rolle installiert sein. Sie finden diese Rolle in den verschiedenen Kapiteln dieses Buchs wieder. Mehr zu diesem Thema lesen Sie auch in den Kapiteln 10 bis 19.
- **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 mit »Nur Lesen«-Rechten konfiguriert werden. Die Konfiguration ist allerdings nicht ganz trivial und es werden nur die Microsoft Office-Versionen 2003/2007/2010/2013 sowie Clients mit dem Internet Explorer unterstützt. Die Dienste sind auch Grundlage für die dynamischen Zugriffsrechte (Dynamic Access Control, DAC) in Windows Server 2012 R2. Mehr zu diesem Thema lesen Sie auch im Kapitel 33.
- **Active Directory-Verbunddienste (Active Directory Federation Services, AD FS)** Mit den AD FS können Sie eine webbasierte Single Sign-On (SSO)-Infrastruktur aufbauen. Profitieren sollen hauptsächlich unternehmensinterne Verbände (auch mit mehreren Gesamtstrukturen) sowie Cloudplattformen. Der Identitätsverbund ermöglicht es Unternehmen, die in Active Directory gespeicherten Identitätsinformationen eines Benutzers auf sichere Weise über Verbundvertrauensstellungen gemeinsam zu nutzen, wodurch die Zusammenarbeit erheblich vereinfacht werden soll. In Einsatz kommen die Dienste zum Beispiel, wenn Authentifizierungsdaten zwischen lokalen Installationen und Office 365 oder Windows/SQL Azure ausgetauscht werden sollen.
- **Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS)** Diese Rolle installiert eine Zertifizierungsstelle in Windows Server 2012 R2. Viele Serverdienste wie Exchange und SQL benötigen Zertifikate, das gilt auch für Dienste wie DirectAccess oder den Netzwerkzugriffschutz. In Active Directory-Gesamtstrukturen sind oft Zertifikate unerlässlich. Aus diesem Grund kann es sich anbieten, diese Serverrolle auf Domänencontrollern mit zu installieren. Auch unter Windows Server 2012 R2 können Sie über einen Browser auf die Zertifizierungsstelle zugreifen. Diese Funktionalität wird allerdings nicht automatisch installiert, sondern muss über den Rollendienst *Zertifizierungsstellen-Webregistrierung* installiert werden. Nach der Installation des Rollendienstes steht auch die Webseite der Zertifizierungsstelle zur Verfügung. Die Adresse ist *http://<Servername>/certsrv*. Mehr zu diesem Thema lesen Sie auch in Kapitel 30.

Abbildg. 4.5 Auswählen der zu installierenden Serverrollen in Windows Server 2012 R2



- **Anwendungsserver (Application Server)** Bei dieser Rolle installieren Sie .NET Framework, Unterstützung für Webserver, Messaging Queueing und andere Funktionen, die viele Anwendungen benötigen, die Windows Server 2012 R2 als Serverhost im Netzwerk nutzen. Grundlage ist vor allem .NET Framework, welches zum Beispiel für SharePoint wichtig ist. Mehr zu diesem Thema lesen Sie auch in Kapitel 27.
- **Datei- und Speicherdienste** Installieren Sie diese Rolle, können Sie den Server als Dateiserver verwenden, um Freigaben zu erstellen. Die Dateidienste beinhalten Erweiterungen wie die Dateiklassifizierungsdienste oder Funktionen zur Unterstützung von iSCSI und Speicherpools. Auch BranchCache, Datendeduplizierung und der Ressourcen-Manager für Dateiserver (Fileserver Resource Manager, FSRM) gehört zu dieser Serverrolle. Auch das verteilte Dateisystem (Distributed File System, DFS) installieren Sie als Rollendienst über diese Rolle. Mehr zu diesem Thema lesen Sie auch in den Kapiteln 5 und 20 bis 22.
- **DHCP-Server** Diese Rolle beinhaltet die Funktion eines DHCP-Servers für das Netzwerk. Unter Windows Server 2012 R2 kann der DHCP-Server auch IPv6-Adressen verteilen, ist also vollständig DHCPv6-kompatibel. Mehr zu diesem Thema lesen Sie auch in Kapitel 24.

Abbildg. 4.6 Installieren von verschiedenen Rollendiensten und Serverrollen am Beispiel der Datei- und iSCSI-Dienste



- **DNS-Server** Installieren Sie diese Rolle, erhält der Server die Möglichkeit, DNS-Zonen zu verwalten. Das ist zum Beispiel auch für Domänencontroller notwendig, da hier wichtige Daten in DNS gespeichert werden. DNS-Server und -Clients mit Windows Server 2012 R2 bieten auch eine Unterstützung für die Domain Name System-Sicherheitserweiterungen (Domain Name System Security Extensions, DNSSEC). Sie können DNSSEC Zonen signieren und hosten, um Sicherheit für die DNS-Infrastruktur bereitzustellen. In Windows Server 2012 R2 sind diese Funktionen direkt in der grafischen Oberfläche integriert. Außerdem unterstützt DNSSEC jetzt komplett Active Directory und auch schreibgeschützte Domänencontroller. Mehr zu diesem Thema lesen Sie auch in den Kapiteln 25 und 26.
- **Druck- und Dokumentdienste** 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. Außerdem können Sie mit dieser Rolle Scanner im Netzwerk bereitstellen. Dokumente lassen sich durch Installation dieser Rolle an SharePoint-Webseiten weiterleiten. Außerdem verwalten Sie mit der Rolle auch andere Druckserver im Netzwerk zentral von einem Server aus. Mehr zu diesem Thema lesen Sie auch in Kapitel 23.
- **Faxserver** Diese Server senden und empfangen Faxe. Auch die Verwaltung von Faxressourcen über das Netzwerk wird durch diese Rolle installiert.
- **Hyper-V** Mit dieser Rolle installieren Sie Hyper-V mit den notwendigen Verwaltungsprogrammen auf dem Server. Mehr zu diesem Thema lesen Sie auch in den Kapiteln 7 bis 9.
- **Netzwerkrichtlinien- und Zugriffsdienste (Network Policy and Access Services)** Hierbei handelt es sich um die RAS-Funktion von Windows Server 2012 R2. Mit dieser Rolle können Sie Benutzern Zugriff auf verschiedene Netzwerksegmente gewähren. Mit dieser Rolle können Sie zum Beispiel auch einen VPN-Server oder einen RADIUS-Server zur Verwendung des Verbindungs-Manager-Verwaltungskits (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 Richtlinien für den Netzwerkzugriffsschutz

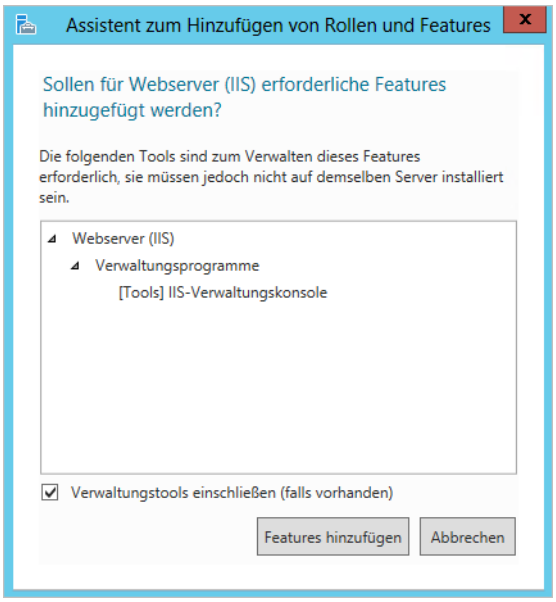
(Network Access Protection, NAP) erstellen und verwalten. Mehr zu diesem Thema lesen Sie auch in den Kapiteln 28 und 31.

- **Remotedesktopdienste** Bei dieser Funktion werden die Remotedesktopdienste im Anwendungsmodus installiert. Mehr zu diesem Thema lesen Sie auch in Kapitel 28.
- **Remotezugriff** Diese Serverrolle wurde neu in Windows Server 2012 eingeführt. Sie installieren mit dieser Rolle DirectAccess und normale RAS-Verbindungen gemeinsam. Während der Netzwerkzugriffsschutz (NAP) Richtlinien für die Einwahl zur Verfügung stellt, bieten DirectAccess und RAS (Remote Access Service) die generelle Möglichkeit der Einwahl. In Windows Server 2012 R2 erfolgt die Konfiguration von RAS und DirectAccess in einer gemeinsamen Oberfläche. Mehr zu diesem Thema lesen Sie auch in Kapitel 32.
- **Volumenaktivierungsdienste** Mit dieser Serverrolle installieren Sie einen Schlüsselverwaltungsdienst (Key Management Service, KMS) im Netzwerk. Der Server verwaltet dann zentral die Produktschlüssel für alle Clients, die Sie über KMS aktivieren. In Active Directory sorgt der Dienst für eine Überwachung und Aktivierung der Rechner.
- **Webserver (IIS)** Installieren Sie diese Rolle, werden die Internetinformationsdienste (Internet Information Services, IIS) auf dem Server aktiviert. Mehr zu diesem Thema lesen Sie auch in Kapitel 27.
- **Windows Server Essentials-Umgebung** Installiert die Funktionen von Windows Server 2012 R2 Essentials auf Servern mit Windows Server 2012 R2 Standard und Datacenter. Mehr zu diesem Thema lesen Sie in Kapitel 1, 2, 36 und 41.
- **Windows Server Update Services (WSUS) –** Unternehmen, die mehrere Microsoft-Produkte und Clientsysteme im Netzwerk einsetzen, kommen um eine zentrale Verwaltung der Patches kaum herum. Windows Server 2012 R2 bietet dazu, wie bereits der Vorgänger, die Windows Server Update Services. Die grundlegende Funktion hat sich von Windows Server 2008 R2 zu Windows Server 2012 R2 nicht geändert. Allerdings lässt sich WSUS in Windows Server 2012 R2 jetzt auch über die PowerShell verwalten. Außerdem kann der Client besser zwischen Servern und Arbeitsstationen unterscheiden. Mehr zu diesem Thema lesen Sie auch in Kapitel 37.
- **Windows-Bereitstellungsdienste (Windows Deployment Services, WDS).** Mit den Windows-Bereitstellungsdiensten können Sie Images von Windows 7/8, aber auch Windows Server 2008 R2/2012 im Netzwerk verteilen und die Installation von Servern und Arbeitsstationen automatisieren. Mehr zu diesem Thema lesen Sie auch in Kapitel 39.

Wenn Sie eine Serverrolle auswählen, erscheint ein Fenster, in dem der Assistent anzeigt, welche Features und Rollendienste noch zusätzlich notwendig sind. In diesem Fenster können Sie auch festlegen, ob auf dem entsprechenden Server auch die notwendigen Verwaltungswerkzeuge installiert werden sollen. Das ist nicht auf allen Servern notwendig, wenn Sie zum Beispiel von einem zentralen Server aus verschiedene Server verwalten wollen.

Sobald Sie eine Serverrolle auswählen, erweitert sich der Assistent automatisch um weitere Seiten, auf denen Sie die entsprechende Rolle bereits während der Installation konfigurieren oder zumindest Hinweise erscheinen, was Sie für den Betrieb der Rolle beachten müssen.

Abbildg. 4.7 Hinzufügen von notwendigen Features



Um den Assistenten abzuschließen, bestätigen Sie die weiteren Fenster. Neu seit Windows Server 2012 ist, dass im gleichen Assistenten auch Features installiert werden können. Wir gehen darauf auf den folgenden Seiten ausführlicher ein.

Auf Core-Servern stehen folgende Serverrollen zur Verfügung:

- Active Directory-Zertifikatsdienste (siehe Kapitel 30)
- Active Directory-Domänendienste (siehe die Kapitel 10 bis 19)
- DHCP-Server (siehe Kapitel 24)
- DNS-Server (siehe Kapitel 25)
- Dateidienste (einschließlich Ressourcen-Manager für Dateiserver, siehe die Kapitel 20 und 21)
- Active Directory Lightweight Directory Services (AD LDS)
- Hyper-V (siehe die Kapitel 7 bis 9)
- Druck- und Dokumentdienste (siehe Kapitel 23)
- Streaming Media-Dienste
- Webserver (einschließlich ASP.NET, siehe Kapitel 27)
- Windows Server Update Services (siehe Kapitel 37)
- Active Directory-Rechteverwaltungsserver (siehe Kapitel 33)
- Routing- und RAS-Server (siehe Kapitel 32)

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.

Verwechseln Sie Features nicht mit Rollendiensten. Features sind einzelne Funktionen, die einen Server erweitern. Auch die Features werden über den Server-Manager installiert, indem Sie den gleichen Assistenten wie bei der Installation von Serverrollen verwenden. Wählen Sie über *Verwalten/Rollen und Features hinzufügen* auf der Seite *Features auswählen* die Features aus, die Sie installieren wollen. Im folgenden Abschnitt zeigen wir Ihnen, welche Features in Windows Server 2012 R2 zur Verfügung stehen:

- **.NET Framework 3.5-Funktionen** Dieses Feature erweitert den Server um die Funktionen von .NET Framework 3.5. und 2.0. Viele Anwendungen benötigen noch die älteren Versionen von .NET Framework.
- **.NET Framework 4.5-Funktionen** Neu seit Windows Server 2012 ist das Feature zur Installation von .NET Framework 4.5 für neue Anwendungen, die für Windows Server 2012 R2 und Windows 8.1 optimiert sind.
- **Benutzeroberflächen und Infrastruktur** Auch dieses Feature ist neu seit Windows Server 2012. Sie können auf Servern gezielt die grafische Oberfläche deinstallieren oder auf Core-Servern installieren. Neben der grafischen Oberfläche können Sie auch gezielt die Tools für die grafische Verwaltung deinstallieren. Mehr zu diesem Thema erfahren Sie in Kapitel 1. Installieren Sie noch die Desktopdarstellung, werden die grafischen Funktionen von Windows 8.1 sowie der Media Player und Desktopthemes auf dem Server installiert. Durch die Installation dieser Funktion werden die grafischen Erweiterungen von Windows 8.1 nicht aktiviert. Diese müssen unter Windows Server 2012 R2 nach der Installation manuell aktiviert werden. Hauptsächlich benötigen Sie diese Funktion auf Remotedesktopservern. Die Anwender erhalten dadurch in den Sitzungen die gleiche Oberfläche wie unter Windows 8.1.
- **BitLocker-Laufwerkverschlüsselung** BitLocker bietet eine Verschlüsselung für lokale Festplatten. In Windows Server 2012 R2 und Windows 8.1 hat Microsoft BitLocker enorm verbessert. BitLocker bietet im Gegensatz zum verschlüsselnden Dateisystem (Encrypting File System, EFS) auch Schutz vor Diebstahl oder dem Ausbau des Datenträgers. Server in Niederlassungen lassen sich mit BitLocker besser verschlüsseln. Die BitLocker-Version unterstützt auch Hardwareverschlüsselungstechnologien von Festplatten und eine inkrementelle Verschlüsselung. Bei Aktivierung verschlüsselt das System nur verwendete Bereiche der Festplatte und erweitert die Verschlüsselung, wenn neue Daten auf der Festplatte gespeichert werden. Mehr zu diesem Thema lesen Sie in Kapitel 5.
- **BitLocker-Netzwerkentsperrung** Ebenfalls neu seit Windows Server 2012 R2 ist die Möglichkeit, mit BitLocker verschlüsselte Domänencomputer zentral zu entsperren. Das ist zum Beispiel sinnvoll, wenn Computer im Netzwerk gewartet werden sollen und neu starten müssen. Mit der zentralen Entsperrung optimieren Sie diesen Vorgang.
- **BranchCache** Durch die Aktivierung von BranchCache als Feature kann ein Server als Client für BranchCache dienen. Um BranchCache als Server einzusetzen, müssen Sie noch den Rollendienst für BranchCache aus der Serverrolle der Dateidienste installieren. BranchCache bietet eine Zwischenspeicherung von Dateien für den schnelleren Zugriff von Windows 7/8-Computern in Niederlassungen. Mehr zu diesem Thema lesen Sie auch in Kapitel 33.

- **Client für NFS** Mit dem Client für NFS lassen sich Server mit UNIX-NFS-Freigaben verbinden.
- **Data Center Bridging** Mit dieser Funktion erweitern Sie den Server mit Funktionen, um den Datenverkehr in großen Netzwerken steuern zu können. Unterstützt der Netzwerkadapter die Funktion Converged Network Adapter (CNA), lassen sich Daten wie iSCSI oder RDMA besser nutzen (siehe Kapitel 1). Außerdem lassen sich Bandbreiten für die verschiedenen Funktionen festlegen.
- **DirectPlay** Mit diesem bei Windows Server 2012 R2 neuen Feature integrieren Sie DirectPlay als Komponente auf einem Server. Bei diesem Protokoll können verschiedene Transport- und Übertragungsaufgaben zwischen Servern realisiert werden. Das Feature ist vor allem auf Remotedesktopservern sinnvoll einsetzbar.
- **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 sie von einer speziellen Applikation benötigt werden. Folgende Funktionen sind in den einfachen TCP/IP-Diensten enthalten: Der *Zeichengenerator (CHARGEN)* 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 Diensts 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. Der *Echo*-Befehl kann als Debugging- und Überwachungstool in Netzwerken eingesetzt werden. Das *Zitat des Tages (QUOTE)* gibt ein Zitat in Form eines ein- oder mehrzeiligen Texts 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.
- **Erweitertes Speichern** Mit dieser Funktion können Sie die Zusammenarbeit von Windows Server 2012 R2 mit externen Speichergeräten verbessern, indem die beteiligten Komponenten Berechtigungen austauschen.
- **Failoverclustering** Mit dieser Funktion installieren Sie die Clusterfunktionalität von Windows Server 2012 R2. Wie andere frühere Enterprise-Funktionen stehen auch das Clustering in Windows Server 2012 R2 in der Standard-Edition zur Verfügung. Mehr zu diesem Thema lesen Sie auch in Kapitel 9.
- **Freihand- und Handschriftdienste** Dieses Feature dient der Unterstützung von Touchpads oder Eingabestiften, wenn Sie einen Bildschirm mit Touchoberfläche einsetzen.
- **Gruppenrichtlinienverwaltung** Mit dieser Funktion installieren Sie die Gruppenrichtlinienverwaltungskonsole (Group Policy Management Console, GPMC), mit der Sie die Gruppenrichtlinien im Active Directory verwalten können. Auf Domänencontrollern wird das Feature automatisch installiert. Mehr zu diesem Thema lesen Sie auch in Kapitel 19.
- **Hostfähiger Webkern für Internetinformationsdienste** Dieses Feature ermöglicht Serveranwendungen, eigene Konfigurationsdateien für IIS zu verwenden, die sich von den anderen Kon-

figurationsdateien unterscheiden. Beispielsweise nutzen Arbeitsordner in Windows Server 2012 R2 und Windows 8.1 diese Funktion.

- **IIS-Erweiterung für OData Services for Management** Mit dieser Funktion stellen Sie PowerShell-Cmdlets für einen Webdienst zur Verfügung. Mehr zu diesem Thema lesen Sie auch in Kapitel 27.
- **Intelligenter Hintergrundübertragungsdienst** 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 so viel Bandbreite verwendet, wie derzeit bei dem Server ungenutzt ist. Andere Netzwerkanwendungen können so auf einem Server weiterhin auf die volle Netzwerkperformance zugreifen.
- **Interne Windows-Datenbank** Hierbei handelt es sich um eine kostenlose relationale Datenbank, die einige Serverdienste nutzen. Die Datenbank kann allerdings nicht von Drittherstellerprodukten verwendet werden, sondern nur von den Funktionen und Rollen in Windows Server 2012 R2.
- **Internetdruckclient** Mit diesem Feature 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.
- **IP-Adressenverwaltungsserver (IPAM-Server)** Eine der Neuerungen ab Windows Server 2012 ist das Feature *IP-Adressverwaltungsserver (IPAM)*. Die Serverlösung hat die Aufgabe, Infrastrukturserver, welche die IP-Adressen im Netzwerk verwalten, in einer gemeinsamen Oberfläche zusammenzuführen und zentral zu verwalten und zu überwachen. Natürlich gibt es weiterhin Verwaltungskonsolen für DHCP und DNS. Zwar lassen sich viele Einstellungen von DHCP auch in der IPAM-Konsole vornehmen, aber für erweiterte Aufgaben, wie Ausfallsicherheit von DHCP-Servern, ist weiterhin die DHCP-Konsole notwendig. IPAM dient nicht nur der Überwachung von DNS- und DHCP-Servern, sondern bietet auch eine effiziente Verwaltungsmöglichkeit dieser Server und zwar in einer gemeinsamen Oberfläche. Microsoft geht mit dieser Serverrolle auf die ständig wachsende Anzahl an DNS- und DHCP-Servern in Unternehmen und der damit verbundenen komplizierteren Verwaltung ein. Damit Administratoren einen Überblick über die verschiedenen IP-Adressbereiche und DNS-Domänen erhalten, sind oft Zusatztools im Einsatz oder Exceltabellen, in denen die Daten aufgelistet sind. Damit soll IPAM Schluss machen. IPAM verfügt im Groben über folgende Funktionen: Automatisches Auffinden der IP-Adresse-Infrastruktur im Unternehmen, Erstellen von Berichten für IP-Infrastruktur, Überwachung der Infrastruktur-Server im Netzwerk und der vorhandenen IP-Adressen, Überwachung von Netzwerkzugriffsschutz-Servern, Überwachung von Domänencontrollern. Mehr zu diesem Thema lesen Sie auch in Kapitel 24.
- **iSNS-Serverdienst (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 auch iSCSI-basierte SAN-Systeme an Windows Server 2012 R2 angebunden

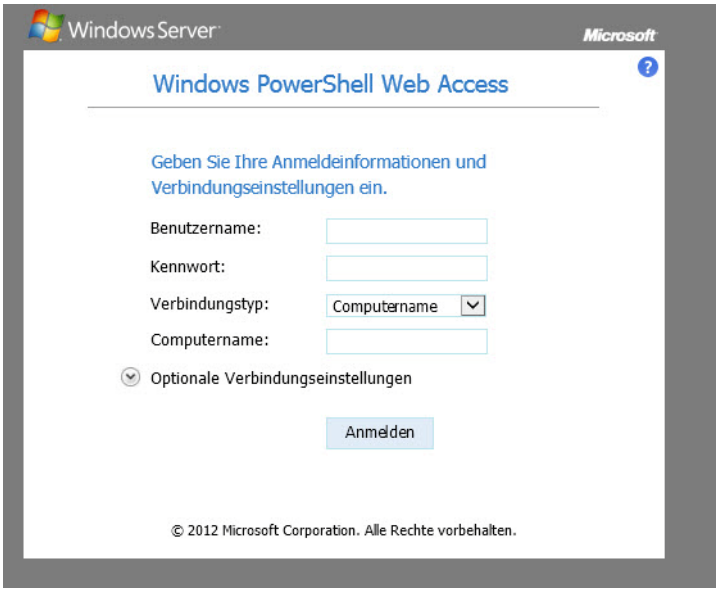
werden. Mit dem iSNS-Protokoll werden die verschiedenen Konfigurationen der iSCSI-Geräte und der Geräte von Speichernetzen (SAN) in einem IP-Speichernetz zentralisiert. Das Konzept kennt den Name Service, mit dem alle Geräte registriert werden, die Bereitstellung von Domain-Namen für das Internet Fibre Channel-Protokoll (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 sogenannte 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 Remotedruckservers. 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. Mehr zu diesem Thema lesen Sie auch in Kapitel 23.
- **Media Foundation** Dieses Feature bietet die Möglichkeit, dass Anwendungen Miniaturansichten für Mediendateien zur Verfügung stellen können. Das Tool arbeitet mit der Desktopdarstellung zusammen und ist auf Remotedesktopservern sinnvoll.
- **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 Möglichkeiten wie Installation und Verwaltung der Infrastruktur, Entwicklung von Nachrichtenanwendungen und vieles mehr.
- **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 die Funktion 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 Fibrechannel-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 die Funktion Multipfad-E/A unterstützt.
- **Netzwerklastenausgleich** Mit dieser Funktion können Sie einen Lastenausgleich zwischen mehreren Servern im Netzwerk bereitstellen. Zu den Anwendungen, die vom Netzwerklastenausgleich profitieren können, zählen IIS, Remotedesktopserver sowie virtuelle private Netzwerke, Windows Media-Dienste und viele Server mehr. 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. Mehr zu diesem Thema lesen Sie auch in Kapitel 34.
- **Peer Name Resolution-Protokoll** PNRP ermöglicht die verteilte Auflösung eines Namens in eine IPv6-Adresse und Portnummer. Einfach betrachtet ist PNRP eine P2P-Anwendung, die die Form eines Windows-Diensts annimmt. PNRP baut auf IPv6 auf.

- **RAS-Verbindungs-Manager-Verwaltungskit** Mit dem Toolkit erstellen Sie ausführbare Dateien, die auf Clientcomputern Einstellungen für RAS-Verbindungen und DirectAccess automatisieren.
- **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 (Distributed File System, verteiltes Dateisystem) verwendet.
- **Remoteserver-Verwaltungstools** Diese Funktion wird auf normal installierten Servern automatisch installiert. Sie können mit diesen Tools die Funktionen über das Netzwerk auf einem Windows Server 2012 R2 verwalten. Mehr zu diesem Thema lesen Sie auch in Kapitel 3.
- **Remoteunterstützung** Installieren Sie diese Funktion, können Sie an Kollegen eine Remoteunterstützungsanforderung schicken, damit sich diese per Remotedesktop auf den Server verbinden können. Diese Funktion wird normalerweise eher für Arbeitsstationen verwendet, als auf Servern. Es spielt keine Rolle, ob die Verbindung mit dem entfernten Rechner über das Netzwerk, Internet oder via Modem per Telefonleitung erfolgt. Auf Remotedesktopservern kann die Funktion durchaus sinnvoll sein.
- **RPC-über-HTTP-Proxy** Mit dieser Funktion werden Remoteprozeduraufrufe (Remote Procedure Call, RPC) 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 2007/2010 wird diese Funktion Outlook Anywhere genannt. Die Remotedesktopgateway-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 2007/2010 verwendet seinen eigenen SMTP-Dienst. Manche Mail-Relay-Anwendungen bauen noch auf den lokalen SMTP-Dienst von Windows Server 2012 R2 auf.
- **SNMP-Dienst** Das Simple Network Management-Protokoll (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.
- **Standardisierte Windows-Speicherverwaltung** Mit dem Feature lassen sich Hardwarespeichergeräte, die SMI-S unterstützen, an Windows Server 2012 R2 anbinden und über Windows-Tools verwalten. Es stehen auch Befehle über WMI und die PowerShell zur Verfügung.
- **Telnet-Client** Mit dem Telnet-Client können Sie sich per Telnet auf einen anderen Server verbinden. Standardmäßig ist dieser Client unter Windows Server 2012 R2 nicht 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.
- **Unterstützung für die SMB 1.0/CIFS-Dateifreigabe** Bietet Unterstützung für Dateifreigaben, die auf die alte SMB 1.0-Technologie setzen und nicht die aktuelle SMB 3.0-Technik verwenden.
- **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.
- **Windows Identity Foundation 3.5** Ermöglicht die Verwendung einiger .NET Framework 4.5-Funktionen auch für .NET Framework 3.5 und 4 zu nutzen. Allerdings ist das nur sinnvoll, wenn die entsprechende Serveranwendung kein .NET Framework 4.5 unterstützt.
- **Windows PowerShell** Hierbei handelt es sich um die PowerShell 4.0 und zusätzliche Werkzeuge für die PowerShell. Sie können an dieser Stelle noch die Unterstützung der PowerShell 2.0 aktivieren und PowerShell Web Access. Wer sich mit dem PowerShell Web Access beschäftigen will, findet weiterführende Informationen im Microsoft TechNet (*http://technet.microsoft.com/de-DE/library/hh831611.aspx* [Ms179-K04-01]). Installieren Sie das Feature PowerShell Web Access über den Server-Manager oder die PowerShell, kann auf die PowerShell auch über einen Webbrowser zugegriffen werden. So können Verwaltungsaufgaben auf einem Server auch von Tablet-PCs oder nicht kompatiblen Systemen durchgeführt werden. Mehr zu diesem Thema lesen Sie auch in Kapitel 40.

Abbildg. 4.8 Verwenden von PowerShell Web Access in Windows Server 2012 R2



- **Windows Search** Mit diesem Feature installieren Sie die Funktionen der Windows-Suche auf dem Server. Die Funktion ist für kleinere Dateiserver geeignet oder Remotedesktopserver, auf denen indexierte Dateien für die Anwender zur Verfügung stehen müssen, damit diese nach Dateien und Inhalten suchen können.

- **Windows Server-Migrationstools** Die Migrationstools unterstützen bei der Migration von Windows Server 2008 R2. Zum Migrieren von Rollen, Features und Daten über die Windows Server-Migrationstools müssen Sie die Tools auch auf den Quellservern installieren, von denen Sie Daten migrieren wollen. Die Tools sind vor allem bei der Migration wertvoll, da keine Zusatzwerkzeuge lizenziert werden müssen.
- **Windows Server-Sicherung** Das standardmäßige Datensicherungsprogramm von Windows Server wird nicht mehr automatisch installiert, sondern muss manuell nachinstalliert werden. Das Programm wurde für Windows Server 2012 R2 überarbeitet. Die Sicherung unterstützt jetzt besser die Schattenkopien sowie die integrierten Sicherungsfunktionen von SQL Server und Exchange. Die Verwaltung der Sicherung findet über die MMC oder die Eingabeaufforderung statt. So können Sie auch über das Netzwerk mit der MMC die Datensicherung von mehreren Servern verwalten. Mehr zu diesem Thema lesen Sie auch im Kapitel 35.
- **Windows-Biometrieframework** Bietet die Unterstützung von Geräten zum Erfassen von Biometrieerfassung in Windows-Netzwerken, zum Beispiel Fingerabdruckscanner.
- **Windows-Feedbackweiterleitung** Sie können mit diesem Feature über Gruppenrichtlinien festlegen welche Clients an der Feedbackinfrastruktur von Microsoft teilnehmen.
- **Windows-Prozessaktivierungssdienst** Bei der Installation der IIS in Windows Server 2012 R2 fordert Windows als Grundlage die Installation des Windows-Prozessaktivierungsdiensts (Windows Process Activation Service, WPAS). WPAS ist der Systembaustein, der für die IIS die Anwendungspools und Prozesse verwaltet.
- **Windows-TIFF-IFilter** Dieses Feature benötigen Sie für die OCR-Erkennung von eingescannten Dokumenten im Zusammenspiel mit der verbesserten Suche und der Indexierung. Eingescannte Dokumente lassen sich so automatisch indexieren und über Windows Search (Rollendienst der Dateidienste) besser durchsuchen.
- **WinRM-IIS-Erweiterung** Hierbei handelt es sich um die IIS-Erweiterung IIS zur Remoteverwaltung der Dienste im Netzwerk.
- **WINS-Server** Der Windows Internet Naming Service (WINS) spielt auch unter Windows Server 2012 R2 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. Mehr zu diesem Thema lesen Sie auch in Kapitel 26.
- **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.
- **WoW64** Das Feature unterstützt die Ausführung von 32-Bit-Anwendungen.
- **XPS-Viewer** Der Viewer ermöglicht das Lesen von XPS-Dokumenten auf dem Server.

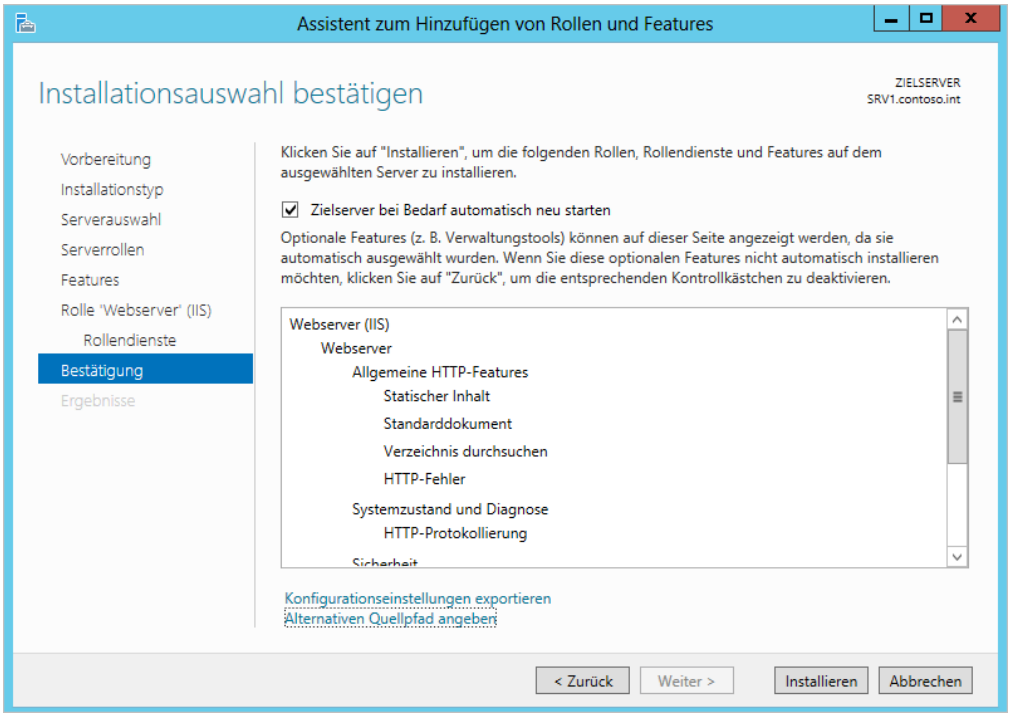
Rollen und Features lassen sich über den jeweiligen Assistenten hinzufügen, verwalten und wieder entfernen. In Windows Server 2012 R2 können Sie mehrere Rollen und Features gleichzeitig installieren, indem Sie diese markieren und den Assistenten zur Installation fortsetzen. Unter Windows Server 2003 mussten Serverfunktionen noch nacheinander installiert werden.

Installation von Rollen und Features abschließen

Haben Sie im Assistenten ausgewählt, welche Rollen und Features Sie installieren wollen, bestätigen Sie auf der letzten Seite die eigentliche Installation. Über den Link *Konfigurationseinstellungen exportieren* erstellen Sie eine XML-Datei, über die Sie die Installation der ausgewählten Rollen und Features automatisieren können.

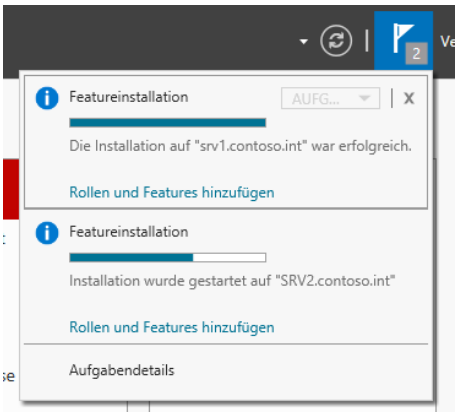
Der Link *Alternativen Quellpfad angeben* ermöglicht die Angabe eines anderen Speicherorts der Installationsdateien. Um Speicherplatz zu sparen, sind nicht alle notwendigen Binärdateien für Windows Server 2012 R2 bereits auf dem Server vorhanden. Fehlen dem Server Binärdateien, zeigt das der Server-Manager an und Sie müssen einen alternativen Speicherort angeben.

Abbildg. 4.9 Fertigstellen der Installation von Serverrollen



Sie können an dieser Stelle auch die Option aktivieren, dass der Server automatisch neu starten soll, wenn dies die Rolle oder ein ausgewähltes Feature verlangt. Sie müssen das Fenster während der Installation der Rolle oder des Features nicht geöffnet lassen, sondern können es schließen. Auf diesem Weg können Sie die Installation auf mehreren Servern starten. Wollen Sie zum Installationsfenster zurückkehren, klicken Sie im Server-Manager oben rechts auf das Benachrichtigungssymbol.

Abbildg. 4.10 Installieren von Rollen und Features auf mehreren Servern im Server-Manager



Rollen in der PowerShell und automatisiert installieren

In diesem Abschnitt zeigen wir Ihnen, wie Sie Serverrollen und Features in der PowerShell oder automatisiert installieren. Sie können dabei auch über den Assistenten zur Installation von Serverrollen eine XML-Datei erstellen und diese mit der PowerShell auf anderen Servern zur Installation von Rollen nutzen.

Serverrollen und Features in der PowerShell verwalten

Die Installation und Verwaltung von Serverrollen findet hauptsächlich über den Server-Manager statt. Neben der grafischen Oberfläche für dieses Tool gibt es die Möglichkeit, Features auch in der PowerShell zu installieren. Interessant sind vor allem die Cmdlets *Add-WindowsFeature*, *Get-WindowsFeature* und *Remove-WindowsFeature*. Auch die Cmdlets *Install-WindowsFeature* und *Uninstall-WindowsFeature* sind in dieser Hinsicht hilfreich. Hilfe zu den Cmdlets erhalten Sie wie immer über *help <Befehlname> –detailed*.

Bis Windows Server 2008 R2 waren die Binärdateien von Features und Serverrollen auf dem Server gespeichert, auch dann wenn die Rollen oder Features nicht installiert waren. Das hat zwar den Vorteil, dass sich Features und Rollen auch ohne das Installationsmedium auf Servern integrieren lassen, verbraucht aber unnötigen Speicherplatz. Windows Server 2012 R2 bietet jetzt die Möglichkeit, auch die Binärdateien von einem Server zu entfernen. Der Vorgang lässt sich aber mit den Installationsmedien von Windows Server 2012 R2 wieder rückgängig machen.

Binärdateien entfernen Sie in der PowerShell mit dem Cmdlet *Uninstall-WindowsFeature*. Rückgängig machen lässt sich der Vorgang mit *Install-WindowsFeature*. Ein Vorteil von Feature on Demand ist die Bereitstellung von Servern über Images. Entfernen Administratoren vor der Erstellung eines Images nicht notwendige Binärdateien, lassen sich bis zu 1 GB Speicherplatz gewinnen (siehe Kapitel 3). Auf diese Weise benötigt Windows Server 2012 R2 weniger Speicherplatz auf der Festplatte.

Sie können aus einem Core-Server einen vollständigen Server mit grafischer Oberfläche machen. Die installierten Serverdienste sind davon unbeeinträchtigt. Dazu geben Sie in der Eingabeaufforderung *powershell* ein und in der PowerShell-Sitzung dann *Install-WindowsFeature Server-Gui-Shell*. Nach ein paar Minuten startet der Server neu und Windows Server 2012 R2 steht zur Verfügung.

Mit dem Befehl *Get-WindowsFeature Hyper-V** zeigen Sie zum Beispiel an, ob die Rolle und die Verwaltungstools bereits installiert sind. In Windows Server 2012 R2 können Sie mit *–computername* die Installation auch auf Remoteservern im Netzwerk überprüfen. Um Hyper-V oder die Verwaltungstools zu installieren, verwenden Sie das Cmdlet *Install-WindowsFeature* (in Windows Server 2008 R2 *Add-WindowsFeature*).

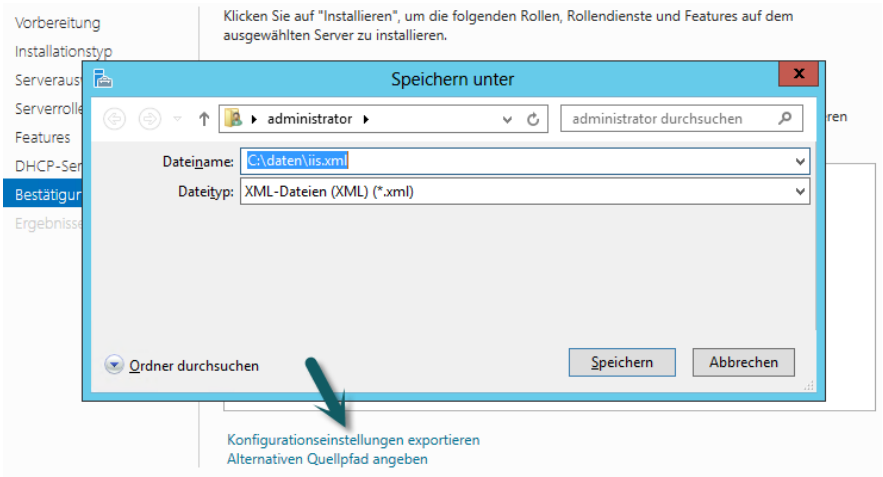
Mit *Install-WindowsFeature Hyper-V* installieren Sie die Serverrolle mit der Option *–IncludeManagementTools* inklusive der Verwaltungstools. Soll der Server gleich noch automatisch neu starten, verwenden Sie zusätzlich die Option *–restart*. Die Verwaltungstools alleine installieren Sie mit *Install-WindowsFeature Hyper-V-Tools*.

Die Installation von Features erfolgt dann mit dem Befehl *Add-WindowsFeature <Kommagetrennte Liste>*, zum Beispiel mit *Add-WindowsFeature RSAT-AD-PowerShell,RSAT-AD-AdminCenter*, die Installation der Active Directory-Verwaltungstools. Die Befehle funktionieren in der PowerShell 2.0 von Windows Server 2008 R2, in der PowerShell 3.0 von Windows Server 2012 sowie in der PowerShell 4.0 von Windows Server 2012 R2. Auf diesem Weg installieren Sie daher mehrere Features und Rollen auf einmal. Mit den Cmdlets installieren Sie auch Rollen und Features auf Core-Servern.

Unbeaufsichtigte Installation von Rollen und Features

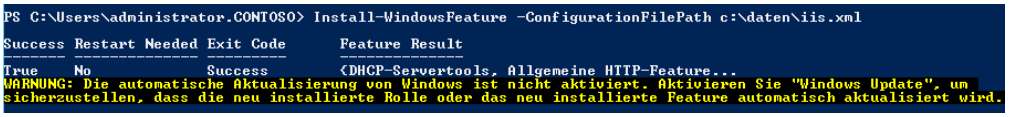
Neben der beschriebenen Möglichkeit, Rollen und Features über die PowerShell zu installieren, indem Sie den Namen der Rolle und des Features angeben, können Sie in der PowerShell auch die XML-Steuerungsdatei verwenden, die Sie im Assistenten zum Installieren von neuen Rollen im letzten Fenster speichern können.

Abbildg. 4.11 Speichern einer XML-Datei im Server-Manager



Um auf einem anderen Server die gleichen Rollen und Features zu installieren, verwenden Sie die PowerShell und geben die XML-Datei mit. Dabei verwenden Sie das Cmdlet *Install-WindowsFeature* mit der Option *–ConfigurationFilePath*, zum Beispiel *Install-WindowsFeature –ConfigurationFilePath C:\Daten\iis.xml*.

Abbildg. 4.12 Serverrollen in der PowerShell über XML-Datei installieren



Rollen und Features mit DISM installieren

Abbildverwaltung für die Bereitstellung (Deployment Image Servicing and Management, DISM) bietet zur besseren Automatisierung der Einrichtung und Installation von Serverrollen auch für Core-Server mit Windows Server 2012 R2 effiziente Möglichkeiten. Mit DISM lassen sich schnell und einfach wichtige Serverrollen installieren, auch skriptbasiert.

DISM bietet mit */Online /Get-Features* auf Core-Servern die gleichen Möglichkeiten wie bisher Oclist in Windows Server 2008 R2. Das Tool Oclist ist in Windows Server 2012 R2 nicht mehr verfügbar, das gilt auch für ServerManagerCMD. Verschiedene Verwaltungsaufgaben lassen sich mit dem Tool wesentlich schneller durchführen als in der grafischen Oberfläche. Wiederkehrende Aufgaben lassen sich mit DISM auch automatisieren. Mit diesem DISM installieren Sie Serverrollen und Features. Neben der Möglichkeit, Rollen zu installieren, lassen sich mit DISM auch Windows-Images einlesen. Verwenden Sie die Option */Online*, bearbeitet DISM das aktuell gestartete Betriebssystem. Um ein WIM-Image zu laden, ist der Befehl *dism /Mount-Wim /MountDir:<Ordner> /WimFile:<WIM-Datei> /Index:1* geeignet. Der Ordner zum Mounten muss vorhanden und leer sein.

Es lassen sich auch mehrere Images einlesen. Der Befehl ist dann der gleiche, aber der Wert für */Index* muss erhöht werden. Der Befehl *dism /Get-MountedWimInfo* zeigt alle gemounteten Images an. Gemountete Images lassen sich mit dem Befehl *dism /Unmount-Wim /MountDir:<Ordner> /<Option>* wieder unmounten. Als Option lassen sich mit */Commit* Änderungen speichern und mit */Discard* Änderungen ohne Speichern verwerfen. Mit der Option */Add-Driver /Driver:<INF-Datei>* lassen sich Treiber in Images integrieren.

Webserver mit Dism.exe remote verwalten und Serverrollen auf Core-Servern installieren

Wollen Sie die Internetinformationsdienste (IIS) auf einem Core-Server auch über das Netzwerk verwalten, ist die Vorgehensweise folgende:

1. Installieren der IIS-Verwaltung auf dem Core-Server mit *dism /Online /Enable-Feature /FeatureName:IIS-ManagementService*.
2. Aktivieren der Remoteverwaltung, indem Sie den Wert *1* beim Registrywert *EnableRemoteManagement* im Schlüssel *HKLM\SOFTWARE\Microsoft\WebManagement\Server* setzen.
3. Mit *Net start wmsvc* den Dienst für die Remoteverwaltung starten.

Eine Möglichkeit, DNS auf einem Core-Server zu installieren, ist der Befehl *dism /Online /Enable-Feature /FeatureName:DNS-Server-Core-Role*. Mit dem Befehl *dism /Online /Disable-Feature /FeatureName:DNS-Server-Core-Role* lässt sich die Rolle wieder entfernen.

Die Installation der DHCP-Serverrolle läuft ähnlich zur Installation eines DNS-Servers ab:

```
dism /Online /Enable-Feature /FeatureName:DHCPServerCore
```

Die Deinstallation erfolgt mit:

```
dism /Online /Disable-Feature /FeatureName:DHCPServerCore
```

Zusätzlich muss der Systemdienst für DHCP noch gestartet werden:

```
sc config dhcpserver start= auto
net start dhcpserver
```

Weitere Serverrollen sind zum Beispiel:

- **Dateireplikationsdienst (File Replication Service, FRS)** *dism /Online /Enable-Feature /FeatureName:FRS-Infrastructure*
- **Distributed File System Replication** *dism /Online /Enable-Feature /FeatureName:DFSN-Server*
- **Network File System** *dism /Online /Enable-Feature /FeatureName:ServerForNFS-Base* und *dism /Online /Enable-Feature /FeatureName:ClientForNFS-Base*
- **Standardrolle eines Druckservers** *dism /Online /Enable-Feature /FeatureName:Printing-ServerCore-Role-WOW64*
- **Line Printer Daemon (LPD)** *dism /Online /Enable-Feature /FeatureName:Printing-LPDPrintService*
- **Active Directory Lightweight Directory Services (AD LDS)** *dism /Online /Enable-Feature /FeatureName:DirectoryServices-ADAM-ServerCore*
- **Active Directory-Zertifikatsdienste** *dism /Online /Enable-Feature /FeatureName:CertificateServices*

Auch diese Rollen lassen sich mit der Option *Disable-Feature* beim Einsatz von DISM deinstallieren.

RemoteFX und DISM

RemoteFX ermöglicht eine bessere grafische Darstellung von Windows 8-Desktops, die zum Beispiel über Virtual Desktop Infrastructure (VDI) zur Verfügung gestellt werden. Die Technik funktioniert auch auf Remotedesktop-Sitzungshosts (Terminalserver). Dazu muss dann auf dem Server ebenfalls Windows Server 2012 R2 installiert sein.

Auf dem Clientcomputer muss dazu der Remotedesktopclient von Windows 8.1 enthalten sein. Wie genau diese Technik funktioniert, erklären die Hyper-V-Entwickler in ihrem Blog (*http://blogs.technet.com/b/virtualization/archive/2010/03/17/explaining-microsoft-remotefx.aspx* [Ms179-K04-02]). Auch ein Demovideo (*http://www.brianmadden.com/blogs/videos/archive/2010/03/18/exclusive-video-microsoft-s-tad-brockway-discusses-and-demos-remotefx.aspx* [Ms179-K04-03]) stellt Microsoft

zur Verfügung. Auf der Partnerseite für RemoteFX (*http://blogs.msdn.com/b/rds/archive/2010/03/22/partners-support-microsoft-remotefx.aspx* [Ms179-K04-04]) erhalten Sie weiterführende Informationen.

Wenn Sie Verwaltungsports an Servern mit einem speziellen Verwaltungsadapter auf dem Server verwenden, empfiehlt Microsoft die Installation des RemoteFX-Treibers, nachdem RemoteFX auf dem Server aktiviert ist. Die Fernwartungskonsole auf Servern kann die RemoteFX-Verbindung stören. Dies liegt daran, dass diese Konsolen meist noch das alte XP-Treibermodell verwenden (XPDM). RemoteFX benötigt aber das Treibermodell Windows Display Driver Model (WDDM). Auf einem Server lässt sich immer nur eine Art Treiber installieren. Ist also ein XPDM-Treiber installiert, lässt sich kein WDDM-Treiber installieren. Aus diesem Grund müssen Administratoren solche alten Karten entweder deaktivieren oder den speziellen RemoteFX-Treiber für diese Karten verwenden, wenn das Gerät kompatibel ist. Den Treiber installieren Administratoren in der Eingabeaufforderung durch Eingabe von:

```
dism /Online /Enable-Feature /FeatureName:Microsoft-Windows-RemoteFX-EmbeddedVideoCap-
Setup-Package
```

Funktionen von DISM in Windows Server 2012 R2 und Windows 8.1

Bereits in Windows Server 2008 R2 und Windows 7 hat Microsoft mit dem Tool Abbildverwaltung für die Bereitstellung (DISM) zahlreiche Möglichkeiten geschaffen, das Betriebssystem an die eigenen Bedürfnisse anzupassen und Installationsmedien zu ändern. Mit Windows 8 und Windows Server 2012 hat Microsoft diese Möglichkeiten zusätzlich erweitert. Das Tool DISM findet jetzt an noch mehr Stellen Einsatz und ersetzt Tools zur automatisierten Installation beziehungsweise ergänzt sie.

Um Windows 8.1 im Unternehmen bereitzustellen, stellt Microsoft das Windows Assessment and Deployment Kit (ADK) zur Verfügung. Dieses stellt den Nachfolger des Windows Automated Installation Kit (WAIK) dar. Das Toolkit bietet Werkzeuge und Funktionen, um Windows 8.1 und Windows Server 2012 R2 mit seinen neuen Möglichkeiten im Unternehmen zur Verfügung zu stellen. Microsoft stellt das ADK kostenlos zur Verfügung (*http://www.microsoft.com/de-de/download/details.aspx?id=30652* [Ms179-K04-05]). Das ADK unterstützt auch die Bereitstellung von Windows Server 2012 R2, Windows Server 2008/2008 R2 und auch von Windows 7.

Das ADK enthält kostenlose Werkzeuge, mit denen Administratoren automatisierte Installationspakete von Windows 8.1 erstellen und verteilen können. Bestandteil sind vor allem die folgenden Tools:

- **Application Compatibility Toolkit (ACT)** Das Tool analysiert Anwendungen im Netzwerk und den einzelnen PCs auf Kompatibilität mit Windows 8.1. ACT benötigt eine Datenbank. Im Download des ADK ist allerdings die kostenlose Datenbank SQL Server 2012 Express Edition integriert.
- **Abbildverwaltung für die Bereitstellung (DISM)** Zusätzlich sind weitere Tools wie Windows System Image Manager (SIM), OSCDIMG, BCDBoot, DISMAPI, WIMGAPI für das Erstellen von Images und Antwortdateien enthalten
- **Windows Preinstallation Environment (Windows PE)** Zum Booten von Windows 8.1 und der anschließenden Installation

- **User State Migration Tool (USMT)** Zur Übernahme der Benutzerprofile und -Daten auf den PCs. Im Gegensatz zu den anderen Tools, kann das USMT auch Daten von Windows XP-Computern zu Windows 8.1 übernehmen.
- **Tool für die Volumenaktivierungsverwaltung (VAMT)** Dient der zentralen Verwaltung der Windows-Aktivierung

Wir zeigen Ihnen nachfolgend, wie Sie ein Windows PE-Bootmedium für Windows 8.1 erstellen und damit ein Image eines Rechners erstellen können. Beim Booten mit Windows PE legt das Betriebssystem verschiedene Partitionen an. Um ein Image zu erstellen, verwenden Sie zum Beispiel den folgenden Befehl:

```
dism /Capture-Image /CaptureDir:D:\ /ImageFile: E:\ThinImage.wim /Name:"Contoso"
```

Um später ein Image auf einem Computer bereitzustellen, geben Sie die folgende Anweisung ein:

```
dism /Apply-Image /ImageFile:<Datei> /Index:1 /ApplyDir:<Laufwerk:\
```

Eine interessante Neuigkeit seit Windows 8 und Windows Server 2012 R2 ist die Möglichkeit, mit DISM auch virtuelle Festplatten (VHD und VHDX) mounten zu können. Die Syntax dazu ist:

```
dism /Mount-Image /ImageFile:"C:\win.vhd" /Index:1 /MountDir:"C:\temp\Mount"
```

Ebenfalls neu ist die Option */List-Image*. Diese kann den Inhalt eines Image anzeigen, also die enthaltenen Dateien und Ordner. Der Befehl *dism /Image:<Name> /Get-Packages* zeigt die installierten Pakete an, und der Befehl *dism /Image:<Name> /Remove-Package /PackageName: <Paket>* entfernt Pakete.

Remoteserver-Verwaltungstools für Windows 8.1

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 8.1 auch im Downloadcenter von Microsoft heruntergeladen werden (siehe Kapitel 3).

Unter Windows Server 2012 R2 können Sie diese Tools als Feature hinzufügen. Sie finden sie im Server-Manager auf der Seite *Features auswählen* über *Remoteserver-Verwaltungstools*. Nach der Installation der Tools kann mit diesen jede Rolle eines Windows Server 2012 R2 verwaltet werden, auch wenn die entsprechende Rolle lokal nicht installiert ist.

Neben RSAT und der Microsoft Management Console (MMC) in Windows Server 2012 R2 sowie dem Server-Manager können Sie auch in der PowerShell andere Server über das Netzwerk verwalten.

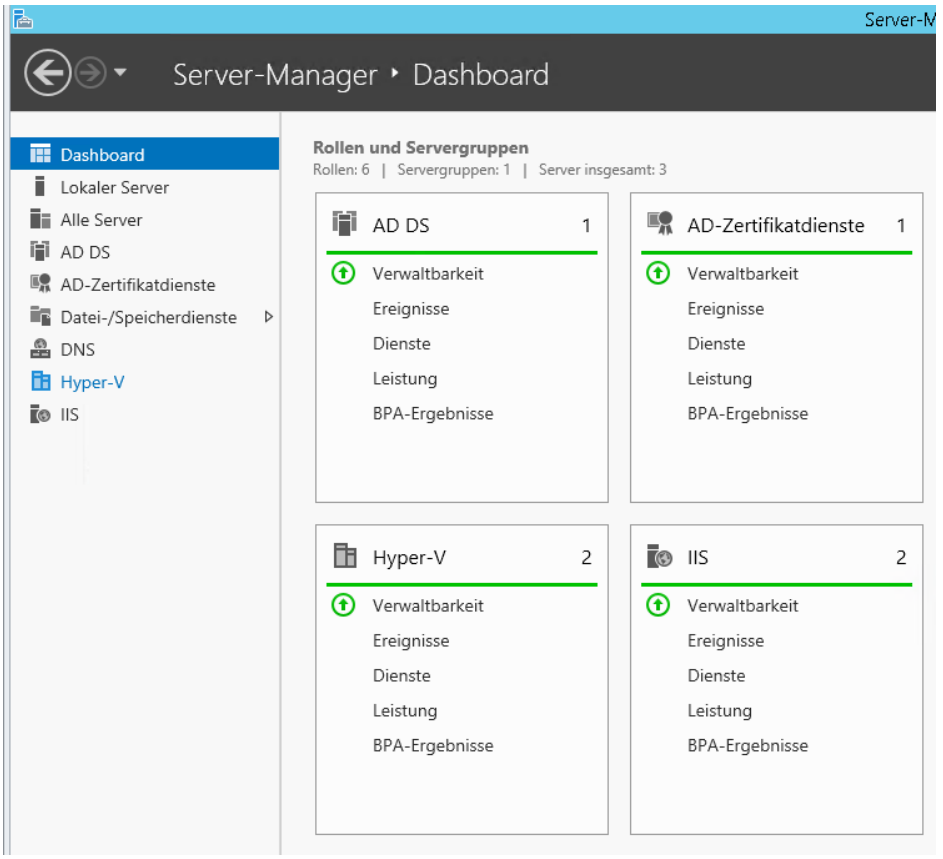
Serverrollen mit dem Best Practices Analyzer überprüfen

Mit Windows Server 2012 R2 erweitert Microsoft die automatische Überprüfung der Serverrollen durch Best Practices Analyzers. Diese gehören zu den Bordmitteln in Windows Server 2012 R2 und stehen im Server-Manager auch für die Überprüfung von Serverrollen über das Netzwerk zur Verfügung. Nahezu alle Serverrollen lassen sich effizient überprüfen und das Ergebnis zentral anzeigen.

Installieren Sie Serverrollen und konfigurieren diese, gibt es oft fehlerhafte Konfigurationen. Dazu hat Microsoft die Best Practices Analyzer entwickelt, die regelmäßig die Server auf Konfigurationsprobleme überprüfen und entsprechende Maßnahmen zur Beseitigung geben. Diese sind seit Windows Server 2008 R2 fest in das Betriebssystem integriert.

Zwar ließen sich bereits in Windows Server 2008 R2 einzelne Serverrollen mit dem internen Best Practices Analyzer überprüfen, allerdings waren die Möglichkeiten eingeschränkt und nicht optimal im Netzwerk möglich. Außerdem war das Tool schwerer zugänglich als in Windows Server 2012. In Windows Server 2012 R2 werden die Ergebnisse dieser automatischen Überprüfung direkt in den einzelnen Kacheln der verschiedenen Serverdienste im Dashboard integriert.

Abbildg. 4.13 Der BPA in Windows Server 2012 R2



Neu seit Windows Server 2012 ist auch die standardmäßige Integration des BPA für Hyper-V. Diesen mussten Sie in Windows Server 2008 R2 nachträglich installieren. Das ist in Windows Server 2012 R2 nicht mehr notwendig. Der BPA kann jetzt auch Hyper-V auf Konfigurationsprobleme überprüfen.

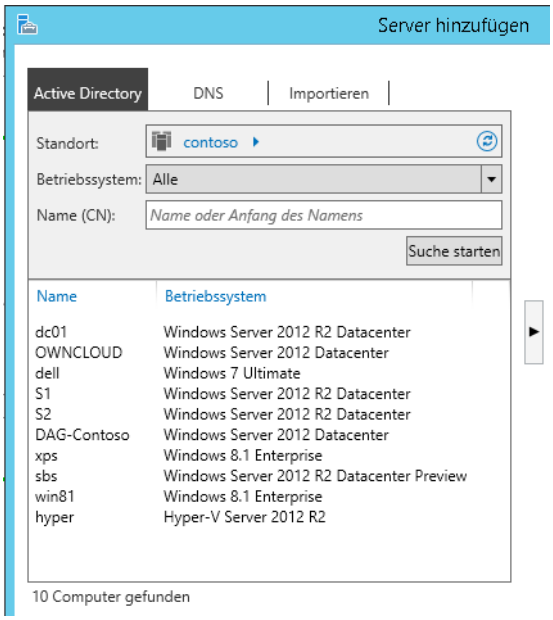
Überprüfen von Servern über das Netzwerk

In Windows Server 2012 R2 lassen sich Server über den Server-Manager vollständig über das Netzwerk verwalten. Das ging in Windows Server 2008 R2 nur eingeschränkt. Über *Verwalten/Server hinzufügen* lassen sich alle Windows Server 2012 R2-Computer im Netzwerk zum Server-Manager hinzufügen. Die Server ordnet der Server-Manager dann nach ihren Rollen und erstellt automatisch Servergruppen.

Im Dashboard des Server-Managers sind daraufhin für alle Serverrollen die BPA-Ergebnisse aller Server zu sehen. Allerdings muss dazu zunächst ein Scan der Rechner im Netzwerk gestartet werden. Klicken Sie in der Ansicht *Alle Server* auf einen Server im oberen Bereich, sehen Sie unten wichtige Fehlermeldungen der Ereignisanzeige (siehe Kapitel 3).

Im oberen Bereich ist außerdem zu erkennen, ob die entsprechenden Server online sind und ob Windows Server 2012 R2 aktiviert ist. Diese Informationen haben nichts mit dem BPA zu tun, ergänzen aber dessen Informationen.

Abbildg. 4.14 Hinzufügen weiterer Server zum Server-Manager



Nach der Installation von Windows Server 2012 R2 sollten Sie im Server-Manager über das Kontextmenü der Server den Befehl *Leistungsindikatoren starten* ausführen, damit der Server über das Netzwerk überwachbar ist, die Best Practices Analyzer funktionieren und Daten abrufen können. Über das Kontextmenü der Server können Sie sich auch mit einem anderen Benutzernamen am Server

anmelden, um diesen zu administrieren. Die Leistungsindikatoren haben aber nur am Rande etwas mit dem BPA zu tun. Die eigentliche Aktivierung erfolgt nachträglich.

BPA in der PowerShell starten

Am schnellsten starten und aktivieren Sie den BPA für Serverrollen durch Eingabe des Befehls *Get-BPAModel | Invoke-BpaModel* in der PowerShell. Dazu ist aber ein Start mit Administratorrechten notwendig. Dieser Befehl versucht auch die Aktivierung von BPAs für Serverrollen, die im Netzwerk nicht installiert sind. Das bringt zwar einige Fehlermeldungen auf den Schirm, stellt aber sicher, dass alle BPAs auch gestartet werden.

Weitere Cmdlets für die PowerShell sind *Get-BPAResult* und *Set-BPAResult*. Diese Cmdlets zeigen Ergebnisse an oder blenden sie aus. Zur Analyse verwenden Sie aber besser den Server-Manager. Auch hier können Sie auf Windows 8.1 setzen. Der Vorteil gegenüber Windows Server 2008 R2 ist, dass mit der Option *–ComputerName* auch eine Konfiguration und Abfrage der Ergebnisse über das Netzwerk hinweg erfolgen kann. Das funktioniert auch über die PowerShell.

Neben der PowerShell lässt sich der BPA für einzelne Serverrollen auch im Server-Manager starten. Dazu öffnen Sie den Server-Manager und klicken auf die Serverrolle, die überprüft werden soll. Durch einen Klick auf *Server* sind die Server mit dieser Rolle im Netzwerk zu sehen.

Hier sind allerdings nur die Server zu sehen, die Sie über *Verwalten/Server hinzufügen* dem lokalen Server-Manager hinzugefügt haben. Im unteren Bereich des Server-Managers findet sich der Bereich *Best Practices Analyzer*. Durch einen Klick auf *Aufgaben/BPA-Überprüfung starten* beginnt der Test der Serverrolle. Zunächst müssen Sie aber den Server auswählen, den der BPA überprüfen soll.

BPA im Server-Manager starten, auch von Windows 8.1-Computern

Den gleichen Assistenten finden Administratoren im Server-Manager über *Alle Server* im unteren Bereich *Best Practices Analyzer*. Auch hierüber lassen sich alle Server, die an den lokalen Server-Manager angebunden sind, überprüfen.

Diese Überprüfung lässt sich auch auf Windows 8.1-Computern starten. Dazu installieren Sie die Remoteserver-Verwaltungstools für Windows 8.1 auf dem Rechner und binden über den Server-Manager die entsprechenden Server an. Die Tools stehen auf der Seite *http://www.microsoft.com/de-de/download/details.aspx?id=28972* [Ms179-K04-06] kostenlos zum Download zur Verfügung.

BPA auswerten

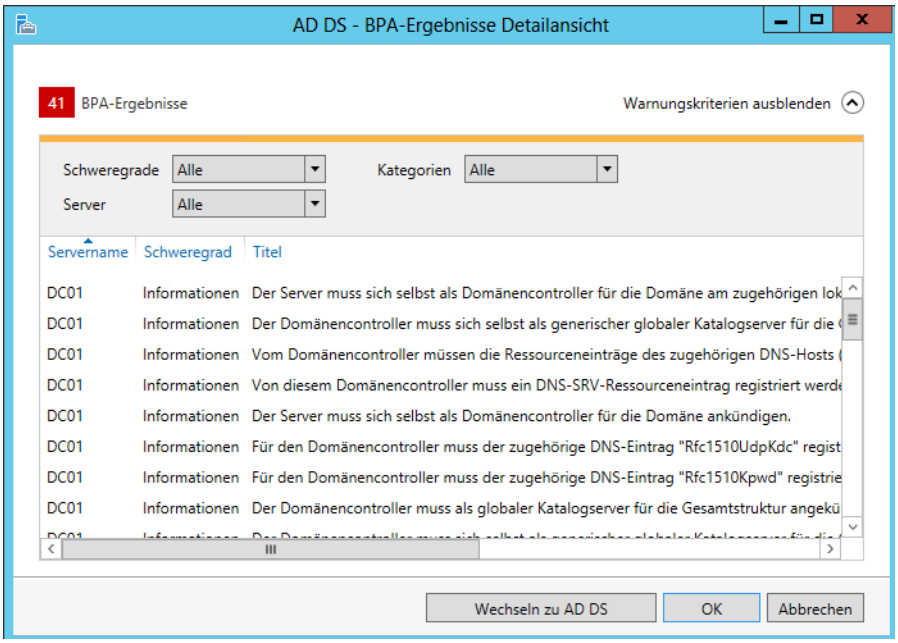
Wenn Sie die BPA-Überprüfung gestartet haben, stehen auf den einzelnen Kacheln im Server-Manager die Ergebnisse zur Verfügung. Diese sind sofort ersichtlich und lassen sich durch einen Klick auf die Kachel öffnen. Klicken Sie auf das Ergebnis der BPA-Überprüfung, zeigt der Server-Manager die gefundenen Fehler an. Hierüber lassen sich auch alle Fehler von allen Servern im Netzwerk anzeigen.

Über das Kontextmenü eines Ergebnisses lässt sich eine erneute Überprüfung für den entsprechenden Server starten, das Ergebnis ausblenden oder das Ergebnis in die Zwischenablage kopieren, zum Beispiel für eine Recherche im Internet.

Die BPA-Ergebnisse finden sich aber auch in der Ansicht *Lokaler Server* und *Alle Server* im Bereich *Best Practices Analyzer* unten im Server-Manager. Wenn für eine Serverrolle für einen der Server im Netzwerk ein BPA-Ergebnis angezeigt wird, wechselt die Kachel auch die Farbe. Auf diese Weise sehen Sie sofort, wenn für einen Server Verbesserungen möglich sind. Durch das Ausschließen eines

Ergebnisses lassen sich die einzelnen Meldungen deaktivieren. Über die Ansicht im BPA können Sie bei *Schweregrad*, *Server* und *Kategorien* das Ergebnis auch filtern lassen.

Abbildg. 4.15 Anzeigen von BPA-Ergebnissen im Netzwerk



Zusammenfassend stehen nach einem Scan mit dem BPA, den Administratoren über Aufgaben im Bereich *Best Practices Analyzer* im Server-Manager starten, die Ergebnisse an den verschiedenen Stellen zur Verfügung: in der Ansicht *Lokaler Server* für alle Rollen des lokalen Servers, über *Alle Server* für alle Rollen auf allen Servern und für alle Rollen. Klicken Sie im Server-Manager auf eine Serverrolle, können Sie die Ansicht nach dieser Rolle filtern lassen und erhalten hier auch alle Informationen von allen Servern.

Zusammenfassung

In diesem Kapitel haben Sie erfahren, welche Serverrollen und Features es gibt, was deren Funktion ist und wie diese installiert werden. Sie fanden hier eine Auflistung, welche Serverrollen und Features in Windows Server 2012 R2 zur Verfügung stehen und wie Sie diese integrieren. Auch die Überprüfung der Serverrollen mit Best Practices Analyzer sowie die Installation und Verwaltung über die PowerShell waren Themen in diesem Kapitel.

Ab den nächsten Kapiteln dieses Buchs steigen wir etwas tiefer in die Thematik ein und erläutern Ihnen, wie Sie Windows Server 2012 R2 produktiv einsetzen. Den Anfang macht das folgende Kapitel 5 mit der Verwaltung der Datenträger und des Dateisystems. Hier lernen Sie auch eine seit Windows Server 2012 und Windows 8 neue Funktion kennen: die direkte Einbindung von VHD-Dateien in das Betriebssystem. Auch den Aufbau eines Speicherpools und weitere Funktionen zeigen wir Ihnen nachfolgend.

Teil B

Grundeinrichtung des Servers

Kapitel 5

Datenträger und Speicherpools verwalten

In diesem Kapitel:

Physische Festplatten und die darauf erstellten Partitionen werden in Windows Server 2012 R2 ähnlich verwaltet wie unter Windows 7/8/8.1. Bereits mit Bordmitteln kann Windows Server 2012 softwarebasierte RAID-Systeme erstellen oder Datenträger auf mehrere physische Festplatten ausdehnen, die dann in Windows Server 2012 R2 wie eine einzelne Festplatte auftreten. Neu in Windows Server 2012 sind die Funktionen der Speicherpools, die wir bereits in Kapitel 1 besprochen haben. In Windows Server 2012 R2 hat Microsoft die Möglichkeiten noch erweitert und Wege geschaffen, auch SSD-Platten mit einzubinden. Wir zeigen Ihnen in diesem Kapitel, wie Sie Datenträger verwalten und die neuen Speicherpools einsetzen.

Die Verwaltung von Datenträgern erfolgt über die Computerverwaltung. Dort findet sich der Bereich *Datenspeicher*, über den auf verschiedene Funktionen zugegriffen werden kann. Der wichtigste Bereich davon ist die Datenträgerverwaltung.

Sie finden die Datenträgerverwaltung auch in der Systemsteuerung über *System und Sicherheit/Verwaltung/Computerverwaltung* oder im Schnellmenü von Windows Server 2012 R2 über die Tastenkombination ⊞+X.

Als weitere Möglichkeit bietet sich der Aufruf durch Eintippen von *compmgmt.msc* auf der Startseite an. Sie können die Datenträgerverwaltung ohne Umwege auch durch Eintippen von *diskmgmt.msc* auf der Startseite aufrufen. Die Computerverwaltung erreichen Sie zusätzlich über das Explorer-Menüband, indem Sie auf der Registerkarte *Computer* in der Gruppe *System* den Befehl *Verwalten* anklicken.

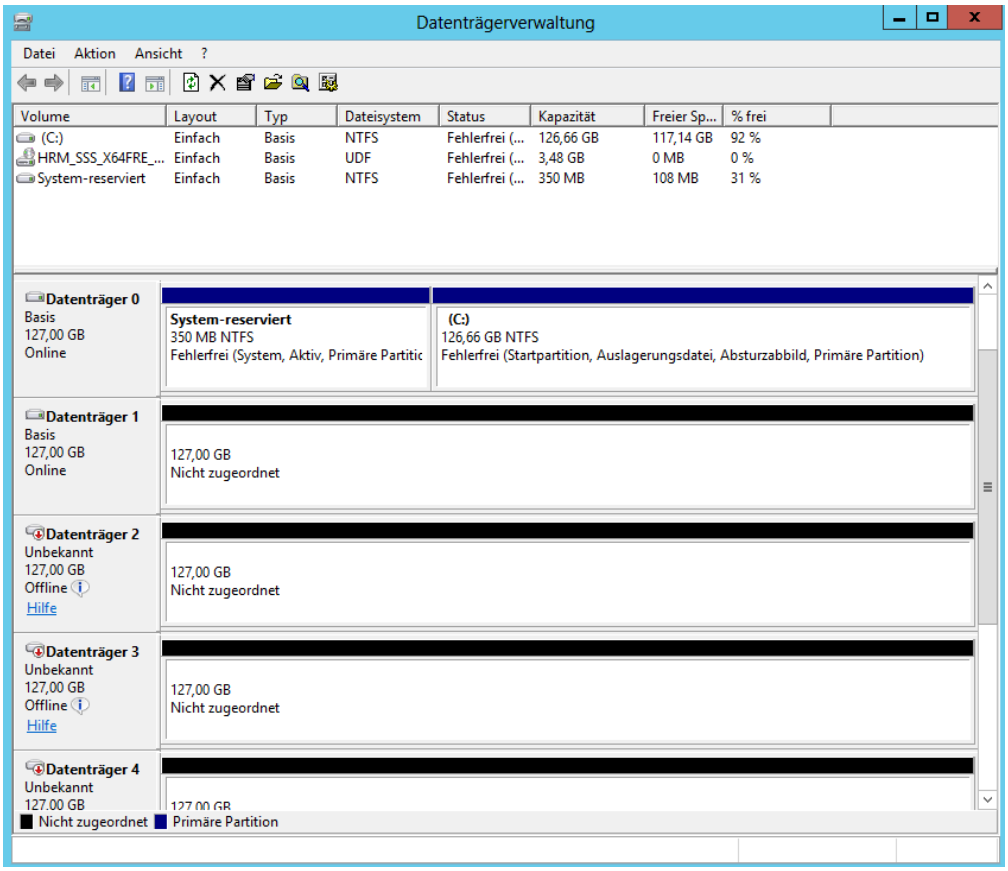
Datenträger erstellen

Starten Sie die Datenträgerverwaltung, zum Beispiel durch Eintippen von *diskmgmt.msc* auf der Startseite, werden im oberen Dialogfeldbereich alle konfigurierten Datenträger im Sinne von logischen Laufwerken angezeigt. Im unteren Bereich sind dagegen die physischen Datenträger inklusive eventuell vorhandener Wechselmedien zu sehen. Bei Festplatten wird angezeigt, auf welchen der installierten Festplatten sich die logischen Laufwerke befinden und welcher Platz noch nicht zugeordnet ist.

Im Bereich der Datenträgerverwaltung werden oft viele Fachbegriffe verwendet, die bei der Konfiguration von Datenträgern eine wichtige Rolle spielen. In diesem Abschnitt erläutern wir Ihnen die wichtigsten Begriffe in diesem Bereich.

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 sein, bevor Sie Daten darauf speichern 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 zu partitionieren.

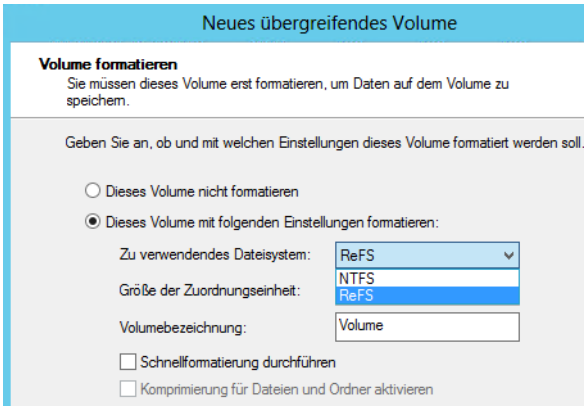
Abbildg. 5.1 Verwalten von Festplatten in Windows Server 2012 R2



ReFS und Speicherpools

Neu seit Windows Server 2012 sind ReFS-Datenträger. Diese sind auch Bestandteil von Windows Server 2012 R2. Sie haben die Möglichkeit, Festplatten auch mit dem neuen ReFS-Dateisystem zu formatieren, das geht aber nur auf Datenplatten in Windows Server 2012/2012 R2. Das Betriebssystem kann von ReFS-Datenträgern nicht booten. Windows 7/8 unterstützen den Zugriff auf Freigaben, die auf ReFS-Datenträgern gespeichert sind, Windows 8 kann allerdings selbst keine ReFS-Datenträger erstellen. Dies gilt auch für Windows 8.1.

Abbildg. 5.2 Formatieren von Laufwerken mit ReFS



Grundlagen zu ReFS

ReFS (Resilient File System, robustes Dateisystem) soll in der Lage sein, defekte Dateien automatisch zu reparieren. Außerdem gilt ReFS im Vergleich zu NTFS als wesentlich unempfindlicher gegenüber Abstürzen des Betriebssystems oder dem Ausschalten des Servers ohne vorheriges Herunterfahren. Das neue Dateisystem arbeitet optimal mit den neuen Speicherpools zusammen. Speicherpools erlauben das Zusammenfassen mehrerer physischer Datenträger zu einem logischen Pool.

Das neue Dateisystem ReFS integriert Microsoft zunächst nur in der Server-Version. Nach einiger Zeit will Microsoft auch auf dem Clientsystem ReFS integrieren, eventuell über ein Service Pack. Wann das sein wird, ist aktuell noch nicht klar. Neben der automatischen Korrektur soll das neue Dateisystem keine langen Ausfallzeiten mehr durch Reparaturmaßnahmen benötigen und zur Reparatur heruntergefahren werden.

Reparaturen lassen sich im laufenden Betrieb durchführen. Stundenlange Reparaturorgien gehören der Vergangenheit an. In ReFS lassen sich Metadaten und Prüfsummen von Dateien wesentlich effizienter integrieren als in Vorgängerversionen. Das Dateisystem protokolliert Änderungen in Dateien und kann ursprüngliche Änderungen speichern. NTFS überschreibt ältere Versionen von Metadaten und Prüfsummen unwiederbringlich. Das heißt, Daten gehen nicht verloren, sondern können im Dateisystem wieder hergestellt werden, auch wenn Anwender Dateien geändert haben. Das funktioniert ähnlich wie bei den Schattenkopien in NTFS, ist aber nicht vom Erstellen solcher Schattenkopien abhängig, sondern läuft ständig im Hintergrund. Die Technik entspricht in etwa den transaktionalen Datenbanken. Der Vorteil dabei ist, dass auch bei Stromausfällen keinerlei Daten auf ReFS-Datenträgern verloren gehen können.

Allerdings handelt es sich bei ReFS um kein Dateisystem, das Daten in Datenbanken speichern kann. Microsoft hat nur einige Vorteile des transaktionalen Systems integriert. Aktuell unterstützt ReFS auch keine Wechseldatenträger. Anwender können aber mit Windows 8-Clients auf Freigaben zugreifen, die in Windows Server 2012 R2 auf Basis von ReFS erstellt wurden.

ReFS trägt auch den immer größeren Dateien und Festplatten Rechnung. Das System unterstützt eine in nächster Zeit unerreichbare Größe von Dateien und Festplatten, die weit über die Möglichkeiten von NTFS hinausgehen. Laut Angaben von Microsoft beherrschen ReFS-Datenträger eine Größe von 16 Exabyte. Ordner auf ReFS-Dateiträgern können nahezu eine unbegrenzte Anzahl Dateien speichern, und auch die Anzahl der Ordner kann mehrere Trillionen betragen. Dateinamen

können eine Länge von 32.000 Zeichen erreichen. Die Leistung soll durch große Dateien aber nicht einbrechen, dafür sorgt die neue Technologie im Hintergrund, die Daten effizienter speichert.

Wie NTFS lassen sich auch in ReFS Berechtigungen auf Basis der Zugriffssteuerungslisten (ACL) vergeben. Daten können Anwender weiterhin mit BitLocker verschlüsseln. ReFS unterstützt aber keine Komprimierung von Dateien über das Dateisystem mehr, und auch keine Verschlüsselung einzelner Dateien. Auch Quotas auf dem Datenträger unterstützt ReFS nicht. Microsoft will konsequent wenig verwendete Features aus dem Dateisystem entfernen.

Anwender bemerken bei der Verwendung des neuen Dateisystems keinen Unterschied zu NTFS, die Bedienung ist vollkommen transparent. Auch Entwickler können die standardmäßige API von NTFS für den Zugriff auf ReFS nutzen. Laut Microsoft sollen auch keine Inkompatibilitäten mit aktuellen Anwendungen bestehen. Programme, die mit NTFS funktionieren, sollen auch mit ReFS laufen. Das liegt nicht zuletzt daran, dass die Zugriffsschnittstelle (API), mit der das Dateisystem kommuniziert, dem von NTFS entspricht. Nur die zugrunde liegende Technik ist unterschiedlich. Die Master File Table (MFT) auf ReFS-Datenträgern unterscheidet sich ebenfalls von NTFS.

Grundlagen der Speicherpools

Physische Datenträger können Administratoren zu Speicherpools zusammenfassen. Diese dürfen eine Größe von 4 Petabyte erreichen. Die Anzahl an Speicherpools ist dagegen nicht begrenzt. Es ist unerheblich, über welchen Standard die Festplatten am Computer angeschlossen sind, wichtig ist nur, dass sie in Windows 8/8.1 verfügbar sind. Speicherpools unterstützen USB, SATA (Serial ATA) oder SAS (Serial Attached SCSI). Auch heterogene Festplatten lassen sich an einem gemeinsamen Pool betreiben. Ab Windows Server 2012 R2 können Sie auch SSD-Platten mit SATA-Platten mischen, um die Leistung von Speicherpools zu verbessern.

Dabei spielt auch die Größe der angebundenen Platten keine Rolle. Es lassen sich verschiedene Anschlusssysteme mit verschiedenen Größen mischen und zu einem Pool zusammenfassen. Speicherpools sind allerdings nur in Windows 8/8.1 und Windows Server 2012 R2 verfügbar. Windows 7 und auch Windows Server 2008 R2 beherrschen diese Funktion nicht. Von der Anzahl an physischen Festplatten sind Speicherpools nicht begrenzt. Speicherpools lassen sich im laufenden Betrieb problemlos mit neuen physischen Festplatten erweitern. Festplatten können Administratoren auch austauschen.

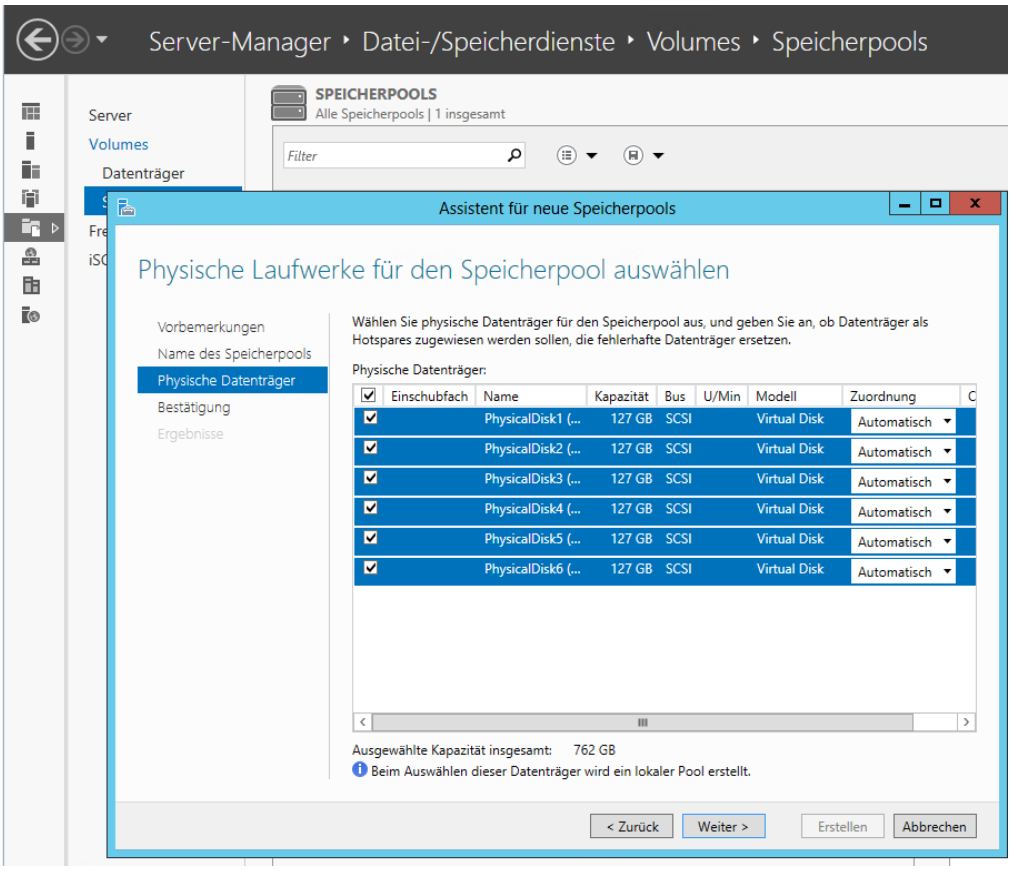
Speicherplätze (Storage Spaces) sind wiederum eine Untermenge von Speicherpools. In Windows Server 2012 R2 stellen virtuelle Festplatten die Speicherplätze dar. Die virtuellen Festplatten sind auf die physischen Festplatten im Speicherpool verteilt. Hierbei handelt es sich um zugewiesenen Speicherplatz, den Anwender wie ein normales Laufwerk verwenden. Speicherplätze entsprechen generell virtuellen Festplatten, die sich auch in Windows 7 und Windows Server 2008 R2 erstellen lassen. In den früheren Versionen sind die virtuellen Festplatten allerdings fest auf einer bestimmten physischen Festplatte gespeichert, nicht in einem Speicherpool. Speicherplätze lassen sich wie ganz normale Laufwerke in den verschiedenen Tools partitionieren, formatieren und als Speicherort für Dateien verwenden, vollkommen transparent für Anwender.

Auch BitLocker lässt sich für einzelne Speicherplätze innerhalb der Speicherpools aktivieren, unabhängig von den zu Grunde liegenden Laufwerken. Der Unterschied zu normalen Laufwerken ist aber, dass Speicherplätze auf mehrere physische Festplatten innerhalb eines Speicherpools zusammengefasst sind. Administratoren können für Speicherplätze auch Ausfallsicherheit konfigurieren, zum Beispiel durch Spiegelung der Daten auf mehrere physische Datenträger. Zusammen mit SSD-Platten im Verbund lässt sich ab Windows Server 2012 R2 die Leistung zusätzlich verbessern.

Wie RAID-Systeme unterstützen auch Speicherplätze Redundanzen über mehrere Laufwerke. Generell ist das Speicherplätze/Speicherpool-Prinzip ähnlich zu einem RAID-System, bietet aber wesentlich mehr Flexibilität bezüglich der integrierten Festplatten und deren Austausch. Im Gegensatz zu aktuellen Software-RAID-Systemen soll das neue System keine Geschwindigkeitseinbußen mit sich bringen. Microsoft verspricht Leistungen, die RAID-0- oder RAID-10-Systemen entspricht. Im Gegensatz zu ReFS sind Speicherpools und Speicherplätze in Windows 8/8.1 ebenfalls integriert. Allerdings funktionieren diese in Windows 8.1 etwas anders. In Windows Server 2012 R2 steuern Sie die Speicherpools über den Server-Manager.

Durch Speicherpools und Speicherplätze lässt sich die Datensicherheit extrem erhöhen und auch die Leistung verbessern. Auch die Flexibilität bei der Vergrößerung des Speicherplatzes ist gegenüber herkömmlichen RAID-Systemen höher. Entdeckt ReFS einen Fehler in einem Speicherplatz, veranlasst das Dateisystem eine Reparatur. Dazu verwendet es gespeicherte Prüfsummen und Metadaten des Systems. Allerdings ist dazu bei der Erstellung eines Speicherplatzes eine Ausfallsicherheit notwendig. Bei der Erstellung eines Speicherplatzes müssen Sie keine physischen Laufwerke eines Speicherpools zuweisen, sondern einfach den entsprechenden Speicherplatz auswählen. Auf welchen Datenträgern Windows die Daten speichert, legt das Betriebssystem unabhängig vom Dateisystem fest.

Abbildg. 5.3 Erstellen von Speicherpools in Windows Server 2012 R2



Zwar unterstützt auch NTFS Speicherplätze, allerdings nur eingeschränkt und ohne die Möglichkeit der Reparatur von Daten. Ist eine physische Festplatte in einem Speicherpool defekt, entdeckt der Speicherplatz dies ebenfalls unabhängig vom Dateisystem und kann Daten auf andere Festplatten auslagern, um keinen Datenverlust zu erleiden. Dazu ist ReFS aber ideal, da hier auch das Dateisystem die Integrität sicherstellt.

Allerdings ist dazu notwendig, dass Sie den Speicherpool mit Ausfallsicherheit erstellt hat. Am einfachsten gelingt das über den entsprechenden Assistenten im Server-Manager. Der Vorgang dazu findet ebenfalls transparent und ohne Zutun statt. Ist keine Ausfallsicherheit für einen Speicherplatz konfiguriert, oder ist nicht die Festplatte defekt, sondern der Arbeitsspeicher, kann ReFS auch ohne konfigurierte Ausfallsicherheit des Speicherplatzes das Dateisystem im Notfall reparieren. In diesem Fall löscht ReFS defekte Dateien, die sich nicht mehr reparieren lassen. Der Vorteil dabei ist, dass nicht defekte Dateien oder Daten nicht mehr von defekten Strukturen beeinträchtigt werden. Anschließend kann der Administrator defekte Dateien wiederherstellen. ReFS kann dazu im Hintergrund automatisch das Dateisystem reparieren. Der Vorgang dauert nicht mal eine Sekunde (sagt Microsoft).

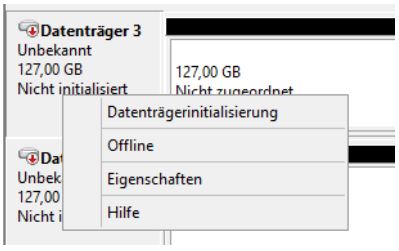
Speicherplätze unterstützen auch Thin Provisioning. Das heißt, Sie können einem Speicherplatz mehr Platz zuweisen, als der Speicherpool insgesamt zur Verfügung hat, sowie die angebundenen Festplatten zusammen. Geht die Kapazität eines Speicherplatzes zur Neige, erhält der Anwender eine Nachricht und kann zusätzliche Datenträger dem Speicherpool hinzufügen. Die Nachricht erscheint über das Wartungscenter in Windows im Infobereich der Taskleiste, welches, wie in Windows 7/8 auch, alle anderen kritischen Meldungen zeigt. Speicherpools und Speicherplätze sind extrem flexibel. Administratoren können auch einzelne Festplatten in einem Speicherpool gegen größere austauschen. Die gespeicherten Daten in den Speicherplätzen sind davon nicht betroffen und der Austausch erfolgt für Anwender vollkommen transparent.

Speicherpools lassen sich in Windows Server 2012 R2 auch als freigegebenes Clustervolume (Cluster Shared Volume, CSV) in Clustern nutzen. Verwenden Sie externe Festplattenarrays, verwendet Windows Server 2012 R2 SES (SCSI Enclosure Services) für die Verbindung. Dies beugt zum Beispiel Ausfällen vor, indem Windows Server 2012 R2 erkennt, wenn im externen Array Festplatten defekt sind.

Einrichten von Datenträgern

Wenn eine zusätzliche Festplatte im Server eingebaut wird, müssen Sie diese in Windows einbinden. Dazu ist zunächst festzulegen, wie die Festplatte initialisiert werden soll. Bestätigen Sie den Vorschlag, MBR (Master Boot Record) zu verwenden, da dies auf Windows-Systemen der Standardeinstellung entspricht. Sind die Festplatten noch als offline hinterlegt, müssen Sie diese über das Kontextmenü zunächst online schalten. Sind die Festplatten online, müssen Sie sie als Nächstes initialisieren. Erscheint kein Fenster, nehmen Sie das Initialisieren über das Kontextmenü vor.

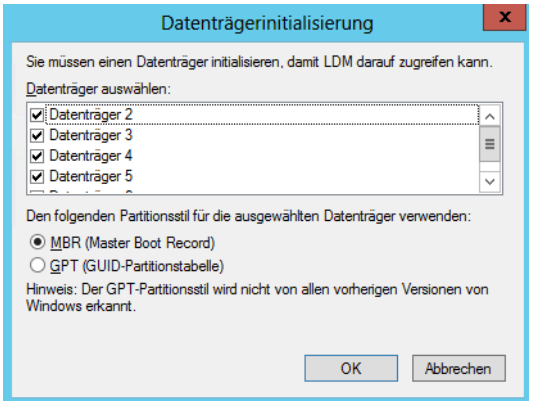
Abbildg. 5.4 Datenträger initialisieren und online schalten



Das Datenträgerpartitionsformat MBR (Master Boot Record) 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 Partitionsformat GPT (GUID-Partitionstabelle) 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.

Abbildg. 5.5 Initialisieren von Festplattenlaufwerken



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. Die Konvertierung eines MBR-Datenträgers in einen GPT-Datenträger und umgekehrt kann nur durchgeführt werden, wenn der Datenträger leer ist. Die Umwandlung nehmen Sie über das Kontextmenü des Datenträgers auf der linken Seite vor.

Nach der Initialisierung sehen Sie die Datenträger in der Datenträgerverwaltung und Sie können diese konfigurieren. Die leeren Festplatten können Sie in dynamische Datenträger umstellen, das ist aber nicht immer notwendig. Wenn Sie ein bestimmtes Speichersystem konfigurieren, zum Beispiel ein Software-RAID oder einen Speicherpool, erhalten Sie automatisch einen Hinweis, wenn Sie eine Festplatte konvertieren müssen. Windows Server 2012 R2 unterscheidet zunächst zwei Arten von Festplatten:

1. Basisdatenträger werden genauso behandelt wie Festplatten unter Windows 2000/XP/Vista und Windows 7/8. Das Modell ist weitgehend vergleichbar mit dem, das bereits zu DOS-Zeiten verwendet wurde. Sie können feste Partitionen einrichten, in denen wiederum logische Laufwerke vorhanden sind. Wenn Sie Partitionen auf einer Basisfestplatte erstellen, sind die ersten drei Partitionen, die Sie erstellen, primäre Partitionen:
   - Eine primäre Partition kann ein Betriebssystem hosten und verhält sich wie ein physischer separater Datenträger. Auf einem Basisdatenträger können bis zu vier primäre Partitionen vorhanden sein. Wenn Sie mehr als drei Partitionen erstellen möchten, erstellen Sie die vierte Partition als erweiterte Partition. Eine erweiterte Partition bietet die 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 sich formatieren lassen und denen Laufwerkbuchstaben zugewiesen werden.

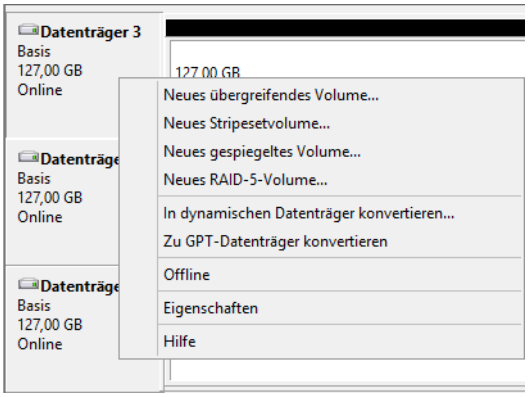
2. Dynamische Datenträger lassen sich einfacher verwalten als die Basisdatenträger. Das betrifft die Veränderung der logischen Laufwerke ohne einen Neustart des Systems. Daher ist es sinnvoll, generell mit dynamischen Datenträgern zu arbeiten, zumindest wenn Sie Datenträger unter Windows erweitern wollen. Dynamische Datenträger können eine unbegrenzte Anzahl von dynamischen Volumes enthalten und funktionieren wie die primären Partitionen, die auf Basisdatenträgern verwendet werden. Konvertieren müssen Sie die Datenträger aber erst dann, wenn eine Datenträgeraufgabe dies erfordert.

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. Für die Verwaltung von Speicherpools müssen Sie in diesem Bereich aber zunächst keine Änderungen vornehmen.

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 umwandeln* aufrufen. Es wird ein Dialogfeld angezeigt, in dem sich die zu aktualisierenden Basisfestplatten auswählen lassen. Es können also in einem Schritt alle noch vorhandenen Basisfestplatten in einem System aktualisiert werden.

Abbildg. 5.6 Verwalten von Datenträgern in Windows Server 2012 R2



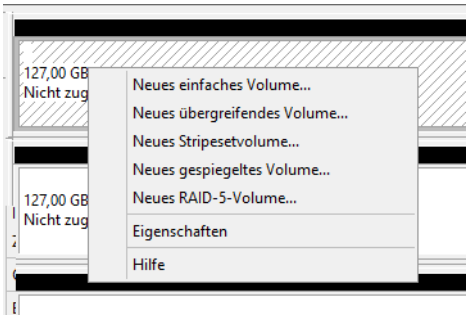
Nach der Auswahl der Festplatten zeigt Windows ein zweites Dialogfeld an, in dem Sie die gewählten Festplatten noch einmal sehen. Hier können Sie entscheiden, welche der neuen Festplatten in dynamische Datenträger umgewandelt werden sollen.

Basisdatenträger können Sie wieder in dynamische Datenträger umwandeln. Wenn Sie Datenträgerkonfigurationen wie zum Beispiel die Erweiterung eines Laufwerks 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 Sie auf diesen logische Laufwerke einrichten. Solche logischen Laufwerke, bei Windows Server 2012 R2 auch als Datenträger bezeichnet, werden mit dem Befehl *Neues einfaches Volume* im Kontextmenü eines freien Bereichs angelegt.

Abbildg. 5.7 Anlegen eines neuen Datenträgers in Windows Server 2012 R2



Um ein solches Volume anzulegen, müssen Sie einen freien Bereich auf einem Datenträger oder der Festplatte, auf Sie das neue logische Laufwerk erstellen wollen, mit der rechten Maustaste anklicken.

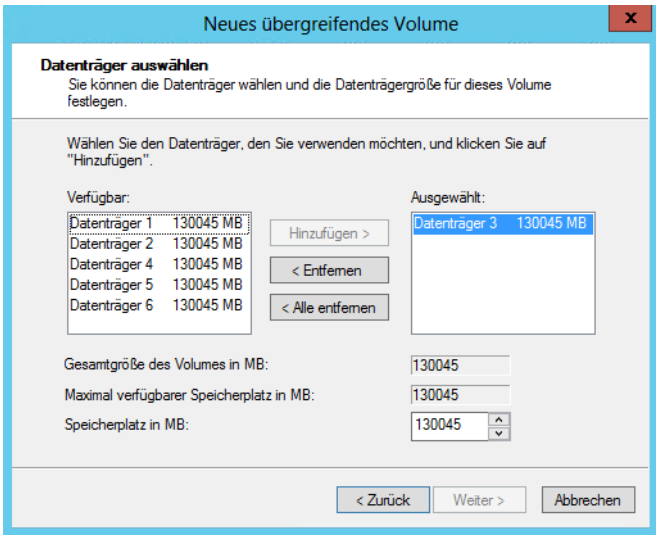
Wenn Sie mit der rechten Maustaste allerdings direkt auf den Datenträger im linken Bereich klicken und nicht auf einen freien Bereich, wird Ihnen die Option *Neues einfaches Volume* nicht angezeigt, sondern nur die beiden Optionen *Neues übergreifendes Volume* und *Neues Stripesetvolume* sowie *Neues gespiegeltes Volume* und *Neues RAID-5-Volume*.

Ein einfacher Datenträger hält Daten nur auf einer einzelnen physischen Festplatte. Ein übergreifender Datenträger erstreckt sich über mehrere physische Festplatten, erscheint im Explorer aber als einzelnes Laufwerk. Wenn der konfigurierte Speicherplatz auf dem ersten physischen Datenträger voll ist, werden weitere Daten auf dem nächsten konfigurierten Datenträger gespeichert. Dieser Ansatz ist nur dann sinnvoll, wenn sehr große logische Datenträger notwendig sind, die größer als die vorhandenen physischen Datenträger sind. Speicherpools sind in Windows Server 2012 R2 in diesem Bereich besser geeignet.

Ein Stripesetdatenträger geht einen Schritt weiter. Bei dieser Variante sind mehrere physische Festplatten beteiligt. Auf jeder dieser Festplatten belegt Windows den gleichen Speicherplatz. Die Daten liegen in Blöcken von 64 KB zunächst auf der ersten Festplatte, der zweiten und so weiter. Wenn eine Datei nur 8 KB groß ist, verwendet Windows trotzdem einen 64 KB-Block, die restlichen 56 KB sind dann verschwendet.

Dieser Ansatz bietet keine Fehlertoleranz. Durch die Verteilung der Daten über mehrere Festplatten erreichen Sie eine verbesserte Performance, allerdings sind die Daten auf dem Datenträger verloren, wenn einer der physischen Datenträger ausfällt. Besser geeignet sind Hardware-RAIDs oder die Verwendung von Speicherpools.

Abbildg. 5.8 Auswahl der beteiligten Datenträger für übergreifende Datenträger



Falls Sie einen Datenträger erzeugen, der sich über mehrere physische Festplatten erstreckt, müssen Sie bei der Definition des Datenträgertyps im folgenden Schritt die Festplatten auswählen. Der nächste Schritt ist die Zuordnung von Laufwerkbuchstaben und -pfaden. Dieser Schritt lässt sich auch jederzeit später über den Befehl *Laufwerkbuchstaben und -pfad ändern* im Kontextmenü des entsprechenden Laufwerks durchführen. Hier finden sich drei Optionen:

- Dem Laufwerk kann zunächst ein Laufwerkbuchstabe fest zugeordnet werden. Das Laufwerk lässt sich in einem leeren Ordner eines NTFS-Systems bereitstellen. Damit können Sie auch bestehende Datenträger erweitern. Diese Erweiterung kann im laufenden Betrieb erfolgen und ist sinnvoll, wenn Sie neue Ordnerstrukturen schaffen wollen, die viel Platz erfordern.
- Sie weisen dann dem Laufwerk keinen eigenen Laufwerkbuchstaben zu, sondern wählen einen bestimmten Ordner aus, der auf einem bereits konfigurierten Laufwerk liegt. Speichern Sie Daten in diesem Ordner, lagert Windows diese Daten auf den neuen Datenträger aus.
- Sie können auch auf die Zuordnung von Laufwerkbuchstaben verzichten. Dieses Laufwerk verwenden Sie dann dazu, um von einem Ordner einer Festplatte auf einen Ordner einer anderen Festplatte zu gelangen. Dazu verwenden Sie den Explorer oder den Befehl *cd* in der Eingabeaufforderung. Die ausführliche Syntax erfahren Sie, wenn Sie in der Eingabeaufforderung *cd /?* eingeben.

Im Regelfall können Sie bei der Formatierung die Standardzuordnungseinheit übernehmen. Diese setzt Windows in Abhängigkeit von der Größe des Laufwerks und ist damit in den meisten Situationen korrekt gewählt. Nur wenn feststeht, dass Sie ausschließlich mit sehr großen Dateien arbeiten, ist es durchaus sinnvoll, einen höheren Wert manuell zu setzen. Über die Befehle im Kontextmenü von Datenträgern können Sie anschließend noch weitere Funktionen ausführen.

Sie können zum Beispiel Datenträger formatieren, wobei allerdings alle vorhandenen Daten verloren gehen. Datenträger können Sie über das Kontextmenü auch erweitern. Damit können Sie bei dynamischen Datenträgern im laufenden Betrieb weiteren, nicht konfigurierten Platz hinzufügen.

Die Erweiterung eines Datenträgers kann dabei auf andere physische Festplatten erfolgen. Diese Vorgehensweise ist sinnvoll, wenn mehr Platz in einer bestehenden Ordnerstruktur notwendig ist. Die Datenträger können Sie über das Kontextmenü auch löschen und neu erstellen.

Windows Server 2012 R2 nutzt das NTFS-Dateisystem, um Festplatten anzusprechen. Windows Server 2012 R2 versteht auch das alte FAT-Format. Benutzer sollten das FAT-Dateisystem jedoch recht schnell vergessen und sich auf NTFS konzentrieren. NTFS ist stabiler, schneller und bietet vor allem die Möglichkeit, den Zugriff zu beschränken.

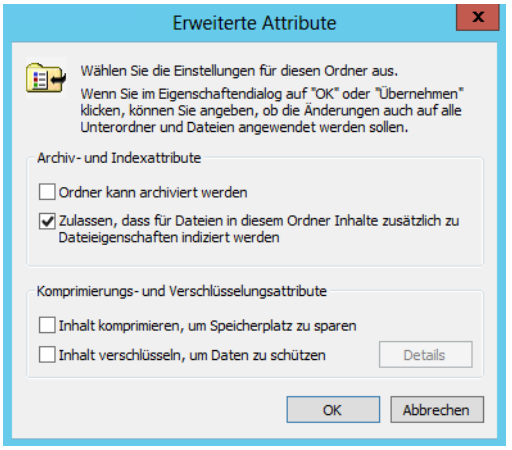
Komprimieren von Datenträgern und Ordnern

Um Speicherplatz zu sparen, können Sie Dateien auf NTFS-Laufwerken auch 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. Sie können auf einem NTFS-Datenträger einzelne Ordner oder Dateien komprimieren, während andere Ordner unkomprimiert bleiben.

ACHTUNG Die Komprimierung können Sie in den Eigenschaften eines Ordners auswählen. Komprimierte Ordner werden durch eine blaue Farbe gekennzeichnet. Die Komprimierung von Dateien steht, genau wie das verschlüsselnde Dateisystem, auf ReFS-Datenträgern nicht zur Verfügung.

Abbildg. 5.9 Verschlüsseln und komprimieren von Ordnern und Dateien auf NTFS-Datenträgern



Auch wenn die Festplatten immer größer werden, haben viele Anwender das Problem, dass der Platz irgendwann knapp wird. Windows Server 2012 R2 bietet die erwähnte Funktion, um Ordner auf der

Festplatte zu komprimieren. Der Vorteil dabei ist, dass Sie auf die Daten wie gewohnt zugreifen können, diese aber deutlich weniger Platz auf der Festplatte belegen.

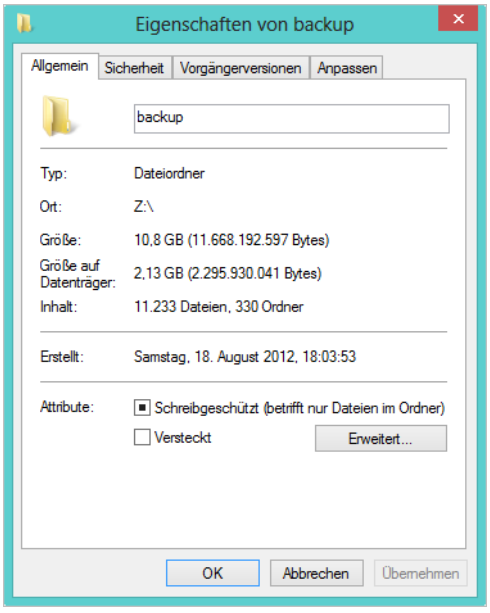
Dateien, mit denen Sie ständig arbeiten, sollten Sie nicht komprimieren, da der Zugriff auf diese Daten etwas langsamer sein kann. Archive oder Ordner mit Bildern im BMP-Format, auf die Sie nicht häufig zugreifen, lassen sich deutlich verkleinern.

Die Funktion steht nur auf NTFS-Datenträgern zur Verfügung. Diese sollten Sie aber aus Geschwindigkeits- und Stabilitätsgründen ohnehin verwenden. FAT-Laufwerke lassen sich in der Eingabeaufforderung mit dem Befehl *convert <Laufwerk> /fs:ntfs* leicht umwandeln. Allerdings lassen sich auf diesem Weg nur FAT-Laufwerke konvertieren, für ReFS-Datenträger steht diese Funktion nicht zur Verfügung. Die Komprimierung von NTFS-Laufwerken oder einzelnen Ordnern aktivieren Sie folgendermaßen:

1. Rufen Sie die Eigenschaften des Ordners auf, den Sie komprimieren wollen.
2. Klicken Sie auf der Registerkarte *Allgemein* auf *Erweitert*.
3. Aktivieren Sie das Kontrollkästchen *Inhalt komprimieren*, um Speicherplatz zu sparen.
4. Beim Bestätigen kann ausgewählt werden, ob auch die Unterordner im Ordner komprimiert werden können.
5. Anschließend werden die Ordner und Dateien komprimiert.

Die Dateinamen komprimierter Daten werden daraufhin in einer blauen Schriftfarbe dargestellt. Ist das nicht gewünscht, kann diese Einstellung im Menüband des Explorers auf der Registerkarte *Ansicht* über *Optionen/Ordner- und Suchoptionen ändern* geändert werden. Dazu wird im Dialogfeld *Ordneroptionen* auf der Registerkarte *Ansicht* das Kontrollkästchen *Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen* deaktiviert.

Abbildg. 5.10 Anzeigen der Speichergröße von Dateien



Die Platzersparnis können Sie in den Eigenschaften des Ordners leicht nachprüfen. Dort wird auf der Registerkarte *Allgemein* die originale Größe und der tatsächliche Plattenverbrauch angezeigt. Das funktioniert auch, wenn Sie die Eigenschaften von Freigaben im Netzwerk aufrufen.

Die Komprimierung lässt sich jederzeit wieder deaktivieren. Bereits komprimierte Dateien wie MP3- und JPG-Dateien oder bereits komprimierte Archive wie ZIP-Dateien profitieren nicht von der Komprimierung und werden nicht weiter verkleinert. Verschieben Sie neue Dateien in bereits komprimierte Ordner, müssen diese gegebenenfalls nachträglich komprimiert werden, da die Funktion nicht automatisch auf neue Dateien überprüft.

Festplattenverwaltung in der PowerShell und Eingabeaufforderung

Um Festplatten zu verwalten, müssen Sie in Windows Server 2012 R2 nicht immer die grafische Oberfläche nutzen. Viele Einstellungen lassen sich teilweise schneller in der PowerShell und Befehlszeile durchführen.

TIPP In Kapitel 40 zeigen wir Ihnen verschiedene Möglichkeiten, wie sich mit der PowerShell, der Eingabeaufforderung und WMI Datenträger in Windows Server 2012 R2 verwalten lassen.

In der Eingabeaufforderung können Sie zum Beispiel mit *diskpart* Partitionen erstellen und verwalten, zum Beispiel auch, um einen bootfähigen USB-Stick zu erstellen, mit dem Sie Windows Server 2012 R2 auch ohne DVD-Laufwerk installieren können (siehe Kapitel 2).

Sie können in der PowerShell aber auch mit den echten physischen Laufwerken auf dem PC arbeiten. Alle Befehle, die in der PowerShell zur Verfügung stehen, lassen Sie sich mit *Get-Command -Module Storage | Sort Noun, Verb* anzeigen. Um zum Beispiel die physischen Festplatten abzufragen, hilft der Befehl *Get-PhysicalDisk*. Die Ausgabe zeigt auch an, ob sich die Platte in einem neuen Speicherpool anordnen lässt. Dies erkennen Sie an der Option *CanPool* über den Wert *True*.

Wer genauere Informationen will, gibt *Get-PhysicalDisk |fl* ein. Durch Eingabe von Spaltennamen nach *|fl* lassen sich erweiterte Informationen angeben und unwichtige ausblenden. Ein Beispiel dafür ist *Get-PhysicalDisk |fl FriendlyName, BusType, CanPool, Manufacturer, Healthstatus*. Das funktioniert mit allen *Get*-Cmdlets. Mit *Get-Disk* lassen Sie sich ebenfalls alle Festplatten anzeigen. Die Partitionierung lässt sich mit *Get-Disk <Nummer> | Get-Partition* überprüfen.

Microsoft empfiehlt für den Datenträger, auf dem Sie Exchange-Datenbanken speichern, eine feste Größe der Zuordnungseinheit (NTFS Allocation Unit Size) von 64 KB. Diese Einstellung können Sie beim Anlegen eines neuen Volumes festlegen. Um zu überprüfen, ob der Datenträger, auf dem Sie die Exchange-Datenbank speichern, optimal konfiguriert ist, verwenden Sie die Eingabeaufforderung oder die PowerShell. Geben Sie dann den folgenden Befehl ein:

```
fsutil fsinfo ntfsinfo [Laufwerksbuchstabe:]
```

Sie sehen die Größe der Zuordnungseinheit im Bereich *Bytes pro Cluster*. Ändern können Sie diese Einstellung nur über eine Neuformatierung. Arbeiten Sie mit Datenträgerkontingenten, können Sie sich mit *fsutil* Informationen zu den Kontingenten anzeigen lassen: In der Eingabeaufforderung verwenden Sie dazu die Anweisung *fsutil quota query <Laufwerk>*.

Verwenden Sie mehrere Festplatten und unterschiedliche Partitionen auf einem Computer, kann DiskExt von der Seite *http://technet.microsoft.com/de-de/sysinternals* [Ms179-K05-01] Informationen schnell und einfach auslesen. Das Tool zeigt an, über welche physischen Festplatten eine Partition aufteilt ist und wo auf der physischen Festplatte eine Partition angelegt wurde.

Sie können die Ausgabe mit *diskext >c:\temp\disk.txt* in eine Textdatei umleiten lassen, falls Sie bei der Einrichtung eines Servers oder für Supportzwecke eine Dokumentation anfertigen möchten. Zeigt zum Beispiel die Datenträgerverwaltung in Windows oder der Explorer ein Laufwerk nicht mehr an, können Sie über DiskExt die Konfiguration der Laufwerke anzeigen lassen. Zusätzlich haben Sie auch die Möglichkeit, direkt einzelne Laufwerkbuchstaben abzufragen, indem Sie die Option *diskext <Laufwerksbuchstabe>:* verwenden, zum Beispiel *diskext c:*.

Mit GPT-Partitionen und ReFS arbeiten

Das GPT-Format für große Festplatten existiert zwar schon länger, kommt aber erst jetzt immer mehr zum Einsatz. Für Datenplatten in Windows Server 2012 R2 bietet sich das neue Dateisystem ReFS an. Beide arbeiten natürlich zusammen.

Bauen Sie in einen Server eine neue Festplatte ein, haben Sie die Möglichkeit, zwischen zwei Datenträgerpartitionsformaten auszuwählen. Dies gilt auch in Windows 8.1 und Windows Server 2012 R2. Große Datenträger mit mehr als 3 TB profitieren deutlich davon, wenn Sie als Datenträgerformat GPT nutzen und als Dateisystem ReFS. Nur die beiden neuen Systeme sind für Festplatten dieser Größe optimiert.

GPT versus MBR

Das Datenträgerpartitionsformat MBR (Master Boot Record) unterstützt Festplatten mit einer Größe von bis zu zwei TB. Im Vergleich dazu unterstützt das Partitionsformat GPT (GUID-Partitionstabelle) Festplatten mit einer Größe von bis zu 18 Exabyte und bis zu 128 Partitionen pro Datenträger.

Datenträger mit dem GPT-Partitionsformat sind besser vor Ausfällen geschützt, da sie über redundante Primär- und Sicherungspartitionstabellen verfügen. Nachdem Sie den Partitionierungsstil festgelegt haben, arbeiten Sie auf beiden Systemen identisch. Sie legen Partitionen und Volumes an und erstellen Verzeichnisse sowie Freigaben.

Auch wenn Sie generell zwischen MBR und GPT wechseln können, sollten Sie die Auswahl des Partitionierungsstils genau überdenken. Auf dem Datenträger, auf dem Sie das Betriebssystem und die Anwendungen installieren, müssen Sie für eine Konvertierung alles neu installieren. Das lohnt sich in den seltensten Fällen.

Datenträgerformat im laufenden Betrieb wechseln

Die Konvertierung eines MBR-Datenträgers in einen GPT-Datenträger und umgekehrt kann nur durchgeführt werden, wenn der Datenträger leer ist. Dazu klicken Sie in der Datenträgerverwaltung von Windows den Datenträger mit der rechten Maustaste an und wählen den entsprechenden Befehl aus. Sie können die Konvertierung aber auch in der Befehlszeile durchführen:

1. Starten Sie eine Eingabeaufforderung mit Administratorrechten.
2. Starten Sie Diskpart.
3. Geben Sie *list disk* ein.

4. Geben Sie *select disk <Nummer der zu konvertierenden Disk>* ein.
5. Geben Sie *clean* ein.
6. Geben Sie *convert gpt* ein (den umgekehrten Weg gehen Sie mit *convert mbr*).

In der Datenträgerverwaltung (*diskmgmt.msc*) finden Sie den Partitionierungsstil auf der Registerkarte *Volumes*, nachdem Sie die Eigenschaften des Datenträgers aufgerufen haben. In der PowerShell lassen Sie sich den Partitionierungsstil mit *Get-Disk | Select FriendlyName, PartitionStyle* anzeigen.

Den Partitionierungsstil legen Sie mit dem folgenden Befehl auf GPT fest:

```
Initialize-Disk <Nummer> -PartitionStyle GPT
```

Ein weiteres Beispiel um einen Datenträger zu erstellen und zu formatieren ist:

```
Get-Disk 1 | Clear-Disk –RemoveData
New-Partition -DiskNumber 1 -UseMaximumSize -IsActive -DriveLetter Z | Format-Volume -
FileSystem NTFS -NewFileSystemLabel Data
```

ReFS versus NTFS

Neben dem Partitionsstil spielt noch das Dateisystem eine wichtige Rolle. Für Datenfestplatten bietet Windows Server 2012 R2 das Dateisystem ReFS (Resilent File System, unverwüstliches Dateisystem). Dieses ist stabiler und besser vor Ausfällen des Servers sowie vor Schäden der Hardware geschützt. Eine Beschädigung von Dateien in ReFS ist sehr unwahrscheinlich.

Sie können auf ReFS-Datenträgern weder die Komprimierung noch das verschlüsselnde Dateisystem (EFS) einsetzen. Auch Windows-Datenträgerkontingente funktionieren nicht. Außerdem können Sie Datenträger nicht verkleinern oder vergrößern wie mit NTFS.

Sie können in der Eingabeaufforderung oder über die PowerShell die Formatierung durchführen und ReFS verwenden. Dazu nutzen Sie den Befehl *Format /fs:ReFS <Laufwerksbuchstabe>:* oder in der PowerShell den Aufruf *Format-Volume -DriveLetter <Buchstabe> -FileSystem ReFS -Full.*

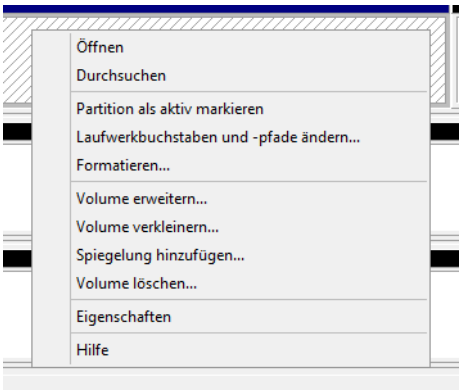
Eine Schnellformatierung führen Sie in der Eingabeaufforderumg mit *Format /fs:ReFS /q <Buchstabe>:* durch.

Sie können für Software-RAIDs in Windows Server 2012 R2 auch das ReFS-Dateisystem verwenden. Die Erstellung und Verwaltung ist identisch mit der Verwendung von NTFS.

Verkleinern und Erweitern von Datenträgern

Sie können Datenträger unter Windows Server 2012 R2 erweitern oder verkleinern. Beim Verkleinern von Laufwerken gibt Windows den konfigurierten Speicherplatz als neuen unpartitionierten Bereich frei. Den freien Speicherplatz können Sie für einen anderen Datenträger verwenden. Der verkleinerte Bereich eines Datenträgers steht genauso zur Verfügung, als wäre er nie partitioniert gewesen. Die Verkleinerung und Erweiterung nehmen Sie über das Kontextmenü des entsprechenden Datenträgers vor. Sie können dazu auch die Eingabeaufforderung verwenden. Wie Sie dabei vorgehen, lesen Sie in Kapitel 2. Sie können aber nur NTFS-Datenträger verkleinern und erweitern, ReFS unterstützt diese Funktion nicht.

Abbildg. 5.11 Erweitern und verkleinern von bestehenden Datenträgern

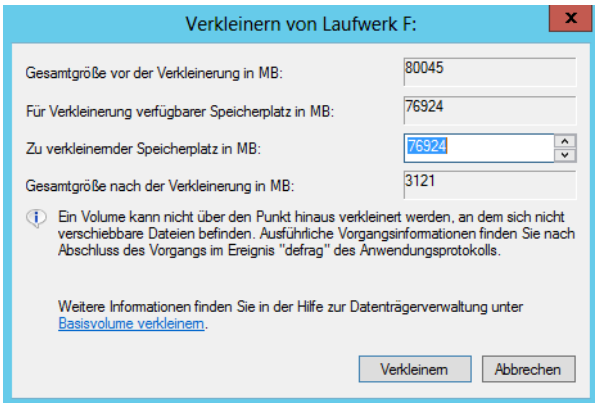


Verkleinern von Partitionen

Beim Verkleinern einer Partition verschiebt Windows nicht verschiebbare Dateien, wie beispielsweise die Auslagerungsdatei, nicht automatisch. 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 wollen, verschieben Sie die Auslagerungsdatei auf einen anderen Datenträger, verkleinern das Volume, und verschieben die Auslagerungsdatei dann wieder zurück auf den Datenträger. Sie können nur primäre Partitionen und logische Laufwerke auf unformatierten Partitionen oder Partitionen mit dem NTFS-Dateisystem verkleinern.

Abbildg. 5.12 Verkleinern von Partitionen



Klicken Sie auf *Verkleinern*, führt der Assistent die Aufgabe durch. Mehr ist zum Verkleinern eines Laufwerks nicht notwendig.

Erweitern von Partitionen

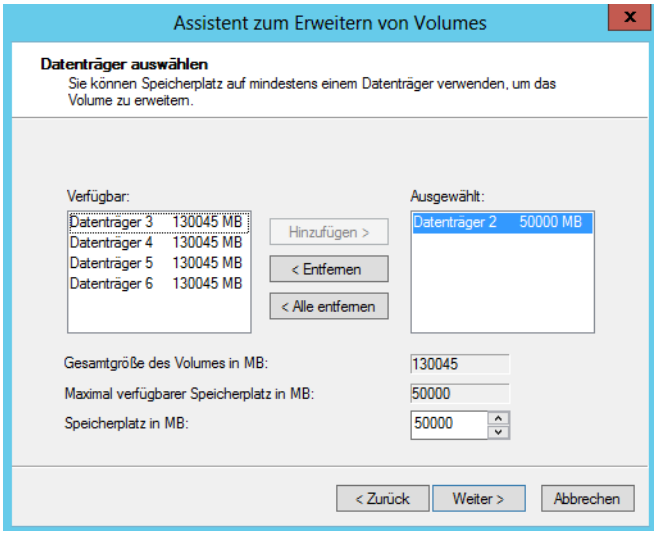
Vorhandenen primären Partitionen und logischen Laufwerken können Sie mehr Speicherplatz hinzufügen, indem Sie diese auf angrenzenden verfügbaren Speicherplatz auf demselben Datenträger erweitern.

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 hinaus 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 Volume, das Sie erweitern möchten.
2. Klicken Sie auf *Volume erweitern*.
3. Wählen Sie die Datenträger aus, auf die Sie das bestehende Volume erweitern wollen, und schließen Sie den Assistenten ab. Belassen Sie die Auswahl auf dem aktuell ausgewählten Volume, erweitert Windows den Datenträger auf den kompletten Bereich des aktuellen Datenträgers.

Abbildg. 5.13 Erweitern eines bestehenden Datenträgers



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.

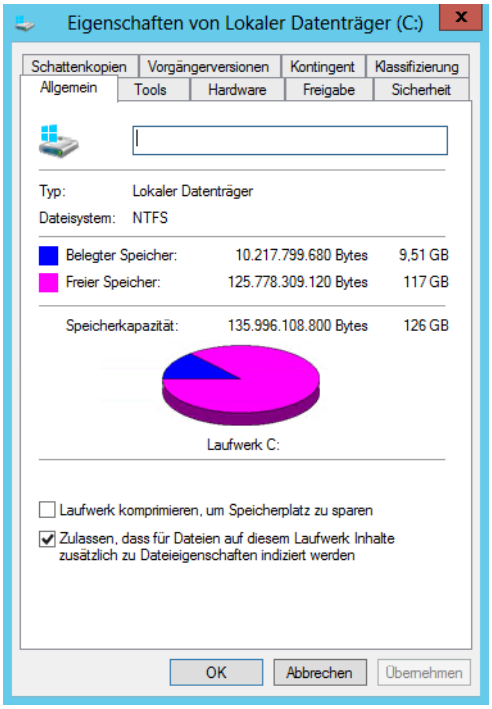
Die Systempartition enthält die hardwarebezogenen Dateien, die einem Computer mitteilen, von wo aus Windows startet (siehe Kapitel 2). Eine Startpartition ist eine Partition, die die Windows-Betriebssystemdateien enthält, die sich im *Windows*-Dateiordner befinden. Mit einem weiteren Begriff, der aktiven Partition, wird beschrieben, welche Systempartition (und daher welches Betriebssystem) der Computer zum Starten verwendet.

Verwalten von Datenträgern

Sie können erstellte Datenträger entweder im Ordnerfenster *Computer* oder in der Datenträgerverwaltung mit der rechten Maustaste anklicken und im Kontextmenü den Eintrag *Eigenschaften* wählen. Daraufhin stehen Ihnen verschiedene Registerkarten zur Verfügung.

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 und auf ReFS-Datenträgern nicht möglich ist. Auf dieser Registerkarte legen Sie auch fest, ob das Laufwerk für die Windows-Suche indexiert werden soll.

Abbildg. 5.14 Allgemeine Informationen zu einem Datenträger



Auf der Registerkarte *Tools* im Eigenschaftenfenster eines Datenträgers überprüfen Sie die physische Festplatte auf fehlerhafte Sektoren. Wollen Sie den Systemdatenträger überprüfen, müssen Sie den Computer neu starten, da die Überprüfung vor dem eigentlichen Start von Windows stattfindet.

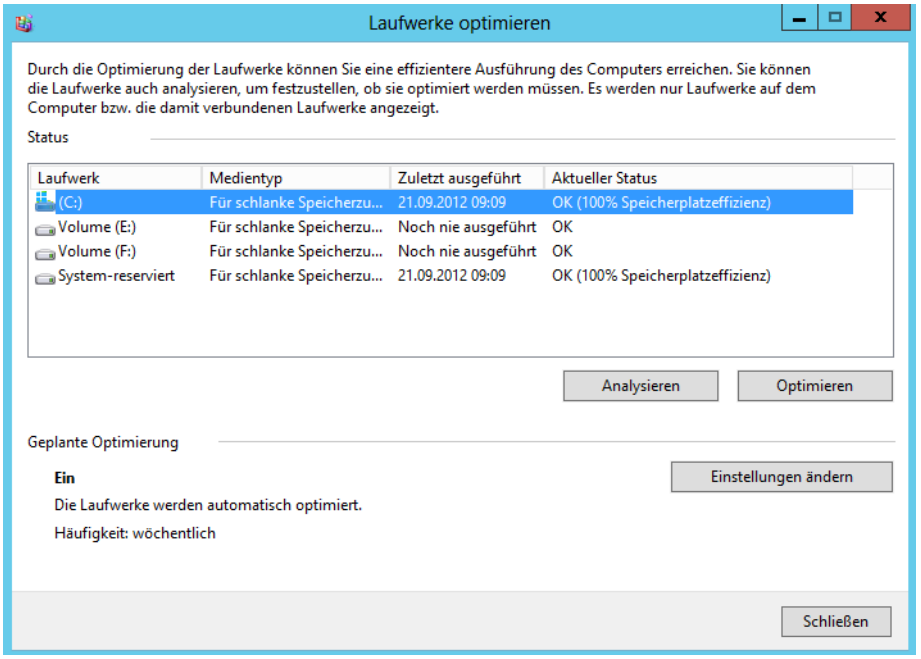
Die Defragmentierung löst ein Problem, das vor allem entsteht, wenn Dateien vergrößert werden, Anwender zusätzliche Dateien erstellen oder vorhandene löschen. Die meisten Dateien werden in Form eines Extents nicht direkt in der MFT (Master File Table) gespeichert, sondern in einem oder mehreren zusätzlichen 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. Dann 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 2012 R2 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 ergibt dies nur, wenn viele Dateien oft in der Größe geändert oder gelöscht werden.

Abbildg. 5.15 Defragmentieren von Datenträgern in Windows Server 2012 R2



Sie können an dieser Stelle die Defragmentierung sofort starten oder den Zeitplan entsprechend anpassen. Mit der Schaltfläche *Analysieren* überprüft der Assistent, ob eine Defragmentierung sinnvoll ist oder nicht.

Die Einstellungen der automatischen Defragmentierung der Festplatten können Sie so abändern, dass diese nicht mehr automatisch startet. Dies ist beispielsweise dann angebracht, wenn Sie auf ein Defragmentierungsprogramm eines anderen Herstellers setzen.

Tippen Sie dazu *dfrgui* auf der Startseite ein. Klicken Sie dann auf die Schaltfläche *Einstellungen ändern*. Dort können Sie das Kontrollkästchen *Ausführung nach Zeitplan* deaktivieren. Wollen Sie einen Bericht über die Defragmentierung beispielsweise von Laufwerk *C:* aufrufen, geben Sie den Befehl *defrag c: –a –v* in einer Eingabeaufforderung ein.

Auf der Registerkarte *Hardware* im Eigenschaftenfenster eines Datenträgers können Sie schließlich die zugrunde liegende Hardware von Datenträgern konfigurieren und die Eigenschaften überprüfen.

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 auf der Registerkarte *Hardware* des Eigenschaftenfensters ein Laufwerk markiert und die Schaltfläche *Eigenschaften* anklickt haben, klicken Sie im nächsten Fenster auf *Einstellungen ändern*. Danach 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, sobald sich diese im Cache der Platte befinden. Wenn allerdings der Strom ausfällt, während die Daten noch vom Schreibcache auf die Festplatte geschrieben werden, kann dies zum Datenverlust führen.

Abbildg. 5.16 Aktivieren des Schreibcaches einer Festplatte

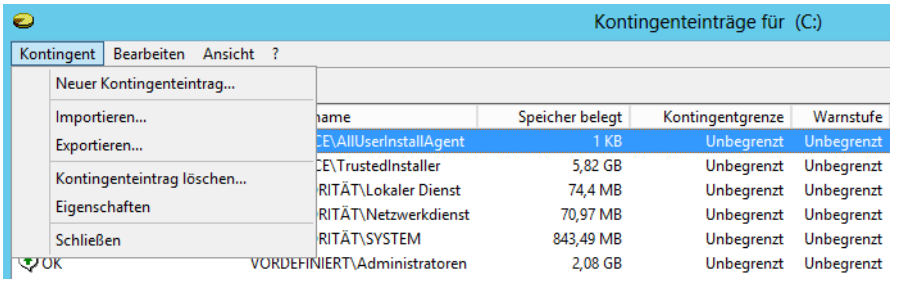
Wenn Sie den Schreibcache für eine Festplatte deaktivieren, wird die Performance des Servers beeinträchtigt. Dafür ist aber sichergestellt, dass keine Daten verloren gehen, wenn der Server ausfällt.

Auf der Registerkarte *Volumes* können Sie nach einem Klick auf die Schaltfläche *Aktualisieren* feststellen, welche Datenträger in Windows einer physischen Festplatte zugewiesen sind.

Klicken Sie ein Laufwerk im Explorer von Windows Server 2012 R2 mit der rechten Maustaste an, steht Ihnen die Registerkarte *Kontingent* zur Verfügung. Aktivieren Sie die Kontingentüberwachung, können Sie festlegen, welche Datenmenge die einzelnen Benutzer auf dem Computer speichern dürfen.

Klicken Sie zunächst auf die Schaltfläche *Kontingenteinträge*, können Sie über das daraufhin geöffnete Fenster definieren, für welche Anwender Sie besondere Grenzen festlegen wollen. Alle anderen Anwender können die maximale Datenmenge speichern, die Sie auf der Hauptseite des Fensters festlegen.

Abbildg. 5.17 Festlegen und abrufen von Kontingenteinstellungen



Sie erreichen aber durch dieses einfache Werkzeug im Explorer die Möglichkeit, die Datenträgerverwendung zu überwachen. Dazu aktivieren Sie die Kontingentüberwachung im Explorer, legen aber keine Grenzwerte fest. So erhalten Sie eine umfangreiche Überwachung der Datenträgernutzung. Über die Schaltfläche *Kontingenteinträge* sehen Sie die einzelnen Benutzer und Gruppen sowie deren Datenträgernutzung. In der Eingabeaufforderung verwenden Sie dazu die Anweisung *fsutil quota query <Laufwerk>*.

Administratoren sind von der Kontingentüberwachung nicht ausgenommen, allerdings können Administratoren auch bei harten Grenzwerten weiter speichern. Normale Benutzer dürfen beim Erreichen des Grenzwerts nicht mehr speichern.

BitLocker-Laufwerkverschlüsselung

Die BitLocker-Laufwerkverschlüsselung ist ein Feature zur Datenverschlüsselung von kompletten Festplatten. BitLocker ist in Windows 8/Windows Server 2012 R2 weiterhin enthalten, funktioniert jedoch wesentlich schneller und effizienter. Die Funktion ist nur in der Pro- und Enterprise-Edition von Windows 8/8.1 enthalten, aber in allen Editionen von Windows Server 2012 R2. Windows RT verwendet eine eigene Verschlüsselung, die »kleine« Version von Windows 8/8.1 kennt keine Verschlüsselung.

BitLocker-Laufwerkverschlüsselung ist ein Feature zur Datenverschlüsselung von kompletten Festplatten. Selbst wenn ein Angreifer die verschlüsselte Festplatte in einen anderen Computer einbaut, schützt BitLocker die Daten vor einem Zugriff.

In Windows 8.1/Windows Server 2012 R2 verschlüsselt BitLocker nicht die komplette Festplatte, sondern nur den verwendeten Teil. Sobald Anwender weitere Teile beschreiben, verschlüsselt Windows 8.1/Windows Server 2012 R2 auch diesen Bereich. BitLocker verschlüsselt bei der Aktivierung daher nur beschriebene Sektoren und fügt dann inkrementell Sektoren hinzu, wenn diese beschrieben werden. Dies heißt, die Verschlüsselung läuft sehr viel schneller ab. BitLocker arbeitet in Windows 8.1/Windows Server 2012 R2 direkt mit Hardwareverschlüsselungen von Festplatten oder RAID-Systemen zusammen.

Interessant ist die Möglichkeit, auch USB-Sticks mit BitLocker To Go zu verschlüsseln. In diesem Fall lassen sich die Daten auf dem USB-Stick erst nach der Eingabe eines Kennworts anzeigen. Auch Windows To Go lässt sich mit BitLocker absichern.

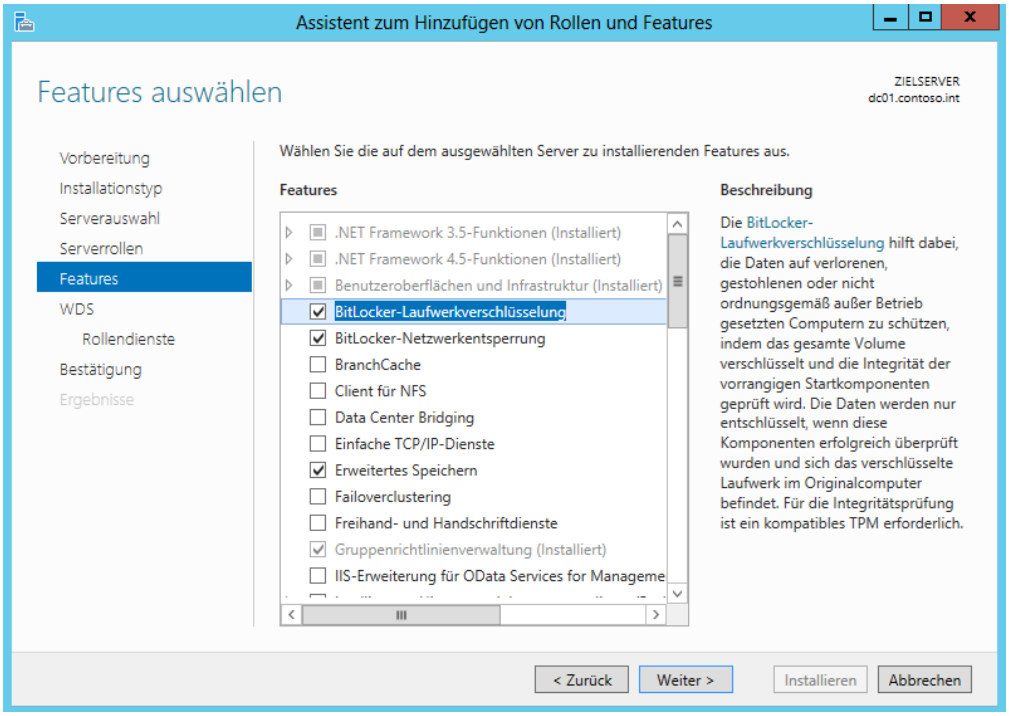
Grundlagen von BitLocker und Trusted Platform Module (TPM)

Im Idealfall ist im Computer, dessen Festplatten Sie verschlüsseln möchten, ein Chip mit der Bezeichnung TPM 1.2 (Trusted Platform Module) eingebaut. Dieser überwacht die integrierte Hardware im Computer und verweigert den Start, wenn die Festplatte in einen anderen Computer eingebaut wird, ohne die PIN zu kennen. Zur Aktivierung von BitLocker ist ein solches TPM-Modul zwar optimal, aber nicht zwingend vorgeschrieben.

Wenn Sie nicht wissen, ob Ihr Computer über einen TPM-Chip verfügt, können Sie die TPM-Verwaltungskonsole durch Eintippen von *tpm.msc* in der Startseite aufrufen. Hier erhalten Sie eine entsprechende Meldung. Allerdings muss der TPM-Chip im BIOS aktiviert werden. In vielen Fällen ist der Chip nicht aktiviert, auch wenn ein solcher im Computer verbaut ist.

Die Konfiguration von BitLocker findet über *Systemsteuerung/System und Sicherheit/BitLocker-Laufwerkverschlüsselung* statt. In Windows Server 2012 R2 müssen Sie dazu aber BitLocker erst als Feature über den Server-Manager installieren (siehe Kapitel 3 und 4).

Abbildg. 5.18 Installieren von BitLocker in Windows Server 2012 R2



Verfügt der Computer über einen TPM-Chip und haben Sie ihn im BIOS aktiviert, muss dieser nach der Installation zunächst initialisiert werden:

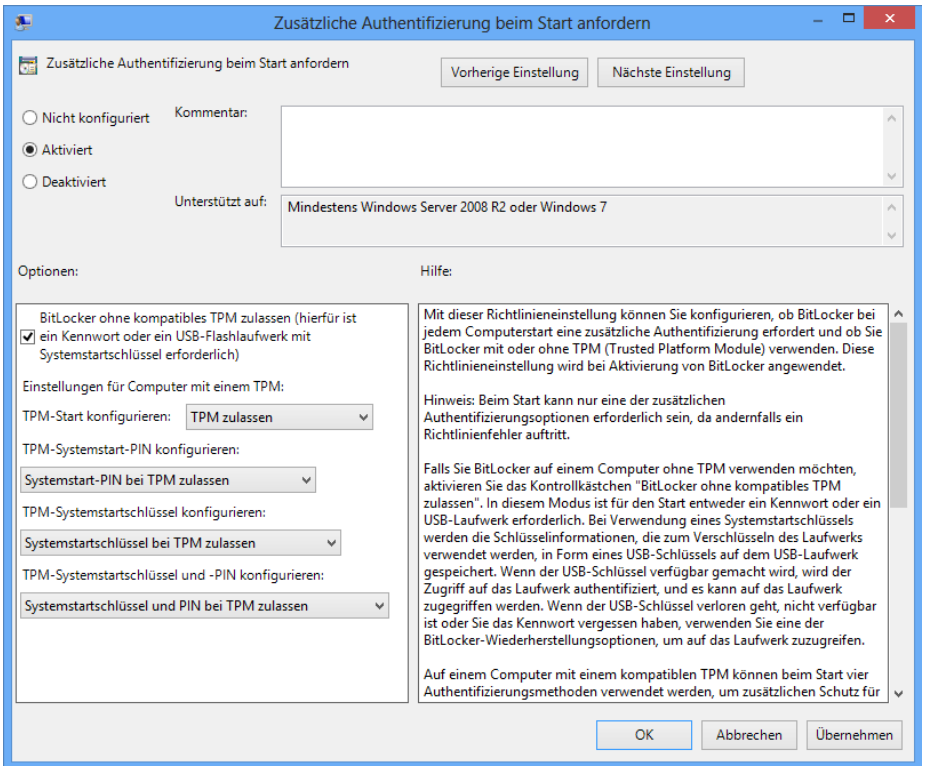
1. Öffnen Sie durch Eintippen von *tpm.msc* auf der Startseite die TPM-Verwaltungskonsole.
2. Klicken Sie im Bereich *Aktionen* auf *TPM initialisieren*, um den TPM-Initialisierungs-Assistenten zu starten. Diese Option erscheint nur, wenn ein TPM-Chip im Computer verbaut ist.
3. Starten Sie nach der Initialisierung den Computer neu.
4. Nach dem Neustart erscheint eine Bestätigungsaufforderung, um sicherzustellen, dass keine bösartige Software versucht, das TPM einzuschalten.
5. Bevor das TPM zum Schützen Ihres Computers nutzbar ist, muss es einem Besitzer zugeordnet sein. Beim Festlegen des TPM-Besitzers wird ein Kennwort zugewiesen, sodass nur der autorisierte TPM-Besitzer auf das TPM zugreifen und es verwalten kann.

BitLocker schnell und einfach aktivieren

BitLocker können Anwender auch dann nutzen, wenn kein TPM-Chip verbaut ist. Dazu ist es notwendig, in die lokale Sicherheitsrichtlinie des Computers zu wechseln oder die Einstellungen über Gruppenrichtlinien festzulegen. Gehen Sie zur Konfiguration folgendermaßen vor:

1. Starten Sie durch Eingabe von *gpedit.msc* auf der Startseite den Editor für lokale Gruppenrichtlinien oder öffnen Sie eine Gruppenrichtlinie in Active Directory.

Abbildg. 5.19 Verwenden von BitLocker ohne TPM als Richtlinie freizuschalten

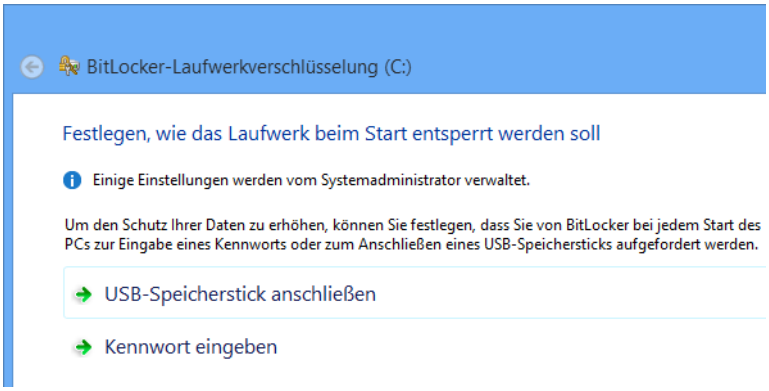


2. Wechseln Sie im Navigationsbereich zum Eintrag *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerkverschlüsselung/Betriebssystemlaufwerke*.
3. Doppelklicken Sie im rechten Bereich des Fensters auf die Richtlinie *Zusätzliche Authentifizierung beim Start anfordern*.
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 Statusspalte den Status *Aktiviert*.

Nachdem diese Aufgaben durchgeführt sind, können Sie BitLocker aktivieren. Starten Sie die Konfigurationsoberfläche von BitLocker über *Systemsteuerung/System und Sicherheit/BitLocker-Laufwerkverschlüsselung*.

Klicken Sie auf den Link *BitLocker aktivieren*. Anschließend überprüft Windows den Rechner. Im nächsten Dialogfeld erhalten Sie verschiedene Optionen angezeigt, um den PC zu starten. Sie können den Startschlüssel entweder auf einem USB-Stick speichern, oder Sie müssen ein Kennwort eingeben, damit der PC startet. Dieses Kennwort hat nichts mit der Benutzeranmeldung zu tun.

Abbildg. 5.20 Festlegen der Startoption für BitLocker

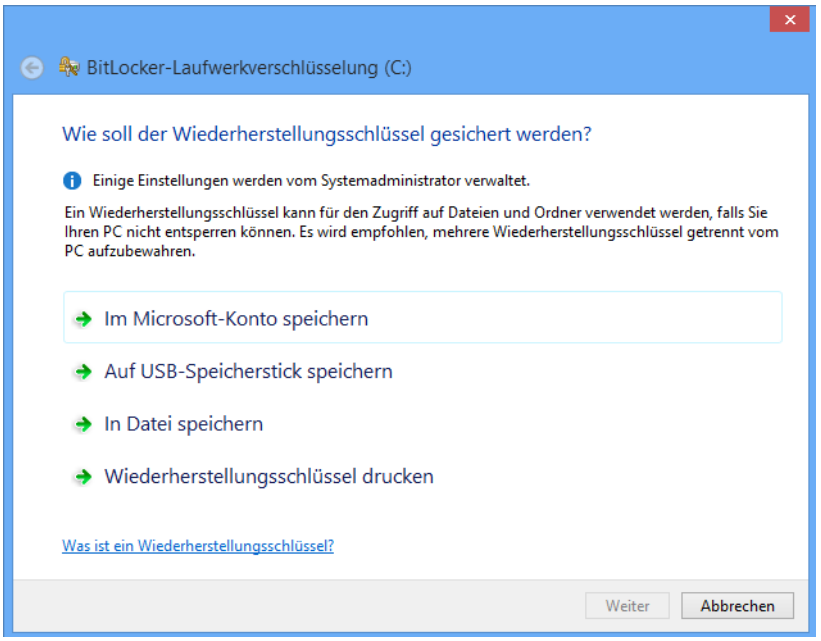


Am einfachsten ist die Verwendung eines Kennworts, welches Sie beim Starten eingeben müssen. Haben Sie das Kennwort eingegeben, müssen Sie auf der nächsten Seite den Wiederherstellungsschlüssel festlegen. Diesen benötigen Sie, wenn Sie mit dem Kennwort den Computer nicht mehr entsperren können, weil Sie es zum Beispiel vergessen haben. Sie haben an dieser Stelle verschiedene Möglichkeiten, den Wiederherstellungsschlüssel zu speichern.

Anschließend müssen Sie den PC neu starten, damit der Assistent prüfen kann, ob eine Verschlüsselung möglich ist. Beim ersten Start müssen Sie dann auch gleich das festgelegte Kennwort für den PC-Start eingeben, oder Sie müssen den USB-Stick mit dem Rechner verbinden, abhängig von der Option, die Sie gewählt haben.

Kennen Sie das Kennwort nicht, können Sie an dieser Stelle auch die Wiederherstellung mit dem Wiederherstellungsschlüssel starten. Beim ersten Start und der erfolgreichen Authentifizierung beginnt der Assistent anschließend mit der Verschlüsselung.

Abbildg. 5.21 Speichern des Wiederherstellungsschlüssels für BitLocker



Wichtig ist, dass ein vorhandener USB-Stick keinesfalls in fremde Hände gelangen darf, da sonst der komplette Schutz des Computers ausgehebelt ist. Nach der Speicherung des Schlüssels auf dem Stick können Sie zusätzlich die Speicherung auf einem anderen Laufwerk oder das Ausdrucken aktivieren.

Nach der BitLocker-Aktivierung erreichen Sie das Fenster für die Verwaltung des Kennworts jederzeit über die Systemsteuerung. So lässt sich der Schlüssel auch nachträglich ausdrucken oder speichern.

Nach der Einrichtung von BitLocker können Sie auch weitere Festplatten auf dem Computer verschlüsseln. Auch wenn Sie nachträglich Festplatten einbauen, können Sie über die BitLocker-Verwaltungsoberfläche die Verschlüsselung nachträglich für diese Laufwerke aktivieren.

Troubleshooting für BitLocker

Haben Sie das Kennwort vergessen, oder ist der USB-Stick oder das TMP defekt, mit dem Sie den Rechner starten, können Sie mit dem Wiederherstellungsschlüssel auf dem Rechner den PC starten und auf Ihre Daten zugreifen.

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 das TPM defekt, der Startschlüssel zerstört ist oder Anwender ihren PIN vergessen haben. Damit bei solchen Vorfällen, auch bei der Erweiterung des Computers, die Daten noch zugänglich sind, gibt es die BitLocker-Recovery-Konsole.

Wenn Sie BitLocker aktivieren, legen Sie sich auf jeden Fall ein Wiederherstellungskennwort an oder speichern es in einem Microsoft-Konto. Über dieses Konto können Sie anschließend den Wiederherstellungsschlüssel abfragen, benötigen dazu aber einen anderen PC.

Abbildg. 5.22 BitLocker wiederherstellen

USB-Stick mit BitLocker To Go verschlüsseln

Anwender können USB-Sticks mit Bordmitteln ebenfalls über BitLocker verschlüsseln. Dazu steht BitLocker To Go zur Verfügung:

1. Verbinden Sie den USB-Stick mit dem Rechner.
2. Markieren Sie im Explorer den Eintrag für den USB-Stick und wählen Sie nach einem Klick mit der rechten Maustaste darauf im Kontextmenü den Eintrag *BitLocker aktivieren* aus.
3. Wählen Sie für die Verschlüsselung die Kennwortmethode aus und geben Sie das Kennwort ein. Sie können statt einem Kennwort auch eine Smartcard verwenden.

Sie können einen mit BitLocker To Go verschlüsselten USB-Stick auch auf Rechnern mit Windows 7 Ultimate und Windows 8.1 Pro/Enterprise lesen. Wollen Sie den Stick auch auf anderen Rechnern nutzen, benötigen Sie das BitLocker-Lesetool. Dieses stellt Microsoft kostenlos für Windows Vista und Windows XP zur Verfügung (*http://www.microsoft.com/de-de/download/details.aspx?id=24303* [Ms179-K05-02]).

Speichern Sie das Kennwort oder drucken Sie es über die nächste Seite aus. Windows 8.1/Windows Server 2012 R2 verschlüsselt jetzt den USB-Stick und zeigt die Verschlüsselung mit einem Schloss an. Sie können noch auswählen, ob Sie den gesamten Stick verschlüsseln wollen, oder nur den aktuell verwendeten Bereich.

Auch für BitLocker To Go können Sie einen Wiederherstellungsschlüssel speichern, mit dem Sie im Notfall auf die Daten des Sticks zugreifen können. Das Kennwort zur Verschlüsselung können Sie nachträglich über das Kontextmenü des verschlüsselten USB-Sticks ändern. Sie können aber auch in der Systemsteuerung über *System und Sicherheit* auf BitLocker und BitLocker To Go zugreifen.

Schreibschutz für USB-Sticks aktivieren

Windows 8.1/Windows Server 2012 R2 ermöglichen zusätzlich das Steuern des Schreibzugriffs auf USB-Sticks. Dies funktioniert in allen Versionen über einen Registry-Eintrag. Gehen Sie dazu folgendermaßen vor:

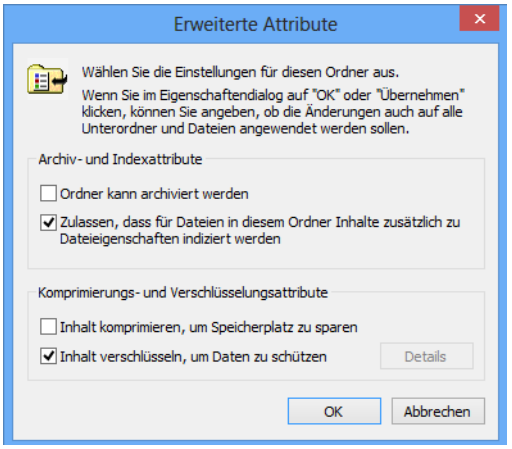
1. Öffnen Sie den Registrierungs-Editor durch Eingabe von *regedit* auf der Startseite.
2. Navigieren Sie zum Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control*.
3. Erstellen Sie hier einen neuen Schlüssel *StorageDevicePolicies*.
4. Erstellen Sie darunter einen neuen DWORD-Wert mit der Bezeichnung *WriteProtect* und dem Wert *1*. Das Lesen funktioniert weiter, aber auf USB-Sticks kann nicht mehr geschrieben werden.

Verschlüsselndes Dateisystem (EFS) – Daten einfach absichern

EFS erlaubt die Verschlüsselung von Informationen. Um Dateien lokal zu verschlüsseln, wählen Sie im Kontextmenü der Datei oder des Ordners, den Sie verschlüsseln wollen, den Befehl *Eigenschaften* aus. Über die Schaltfläche *Erweitert* finden Sie im Dialogfeld *Erweiterte Attribute* das Kontrollkästchen *Inhalt verschlüsseln, um Daten zu schützen*. Durch Aktivieren dieses Kontrollkästchens wird das verschlüsselnde Dateisystem (Encrypting File System, EFS) genutzt. Sie können EFS aber nur zusammen mit NTFS nutzen. Mit dem neuen ReFS-Dateisystem funktioniert EFS nicht.

Die Verschlüsselung und der Zugriff auf diese Informationen erfolgen transparent für die Anwender. Falls ein Ordner für die Verschlüsselung ausgewählt ist, fragt das System, ob die Einstellungen für untergeordnete Ordner übernommen werden sollen.

Abbildg. 5.23 Verschlüsseln von Dateien in Windows 8/Windows Server 2012 R2



Nachdem Sie die Daten verschlüsselt haben, erinnert Sie Windows daran, den Dateischlüssel zu sichern, damit der Zugriff auf die Daten nicht verloren gehen kann.

Anwender auf dem gleichen Rechner und natürlich auch andere Anwender können verschlüsselte Daten zwar sehen, aber die Dateien nicht öffnen und anzeigen, das gilt auch für Fotos. Auch wenn Anwender also Zugriff auf verschlüsselte Daten erhalten, sind diese nur für den Anwender sichtbar, der die Daten verschlüsselt hat. Die Dateien lassen sich von Anwendern auch nicht kopieren oder verschieben. Auf diesem Weg lassen sich also sensible Daten vor Zugriff schützen, sogar vor Anwendern auf dem gleichen PC.

Standardmäßig kennzeichnet Windows 8.1/Windows Server 2012 R2 diese Dateien in grüner Schrift. Um diese Einstellung zu ändern, wählen Sie zunächst im Menüband des Explorers auf der Registerkarte *Ansicht* den Befehl *Optionen/Ordner und Suchoptionen*. Im daraufhin geöffneten Dialogfeld *Ordneroptionen* können Sie auf der Registerkarte *Ansicht* das Kontrollkästchen *Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen* ein- oder ausschalten.

Die Funktionsweise von EFS

Das verschlüsselnde Dateisystem (Encrypting File System, 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. Die Verwaltung der Zertifikate findet über die Benutzerverwaltung statt.

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 sogenannte Wiederherstellungs-Agents möglich.

Alternativ zur grafischen Oberfläche können Sie auch den Befehl *Cipher* in der Eingabeaufforderung einsetzen, um Dateien zu ver- und entschlüsseln oder sich den Status anzeigen zu lassen. Der Befehl *cipher /e /s:C:\Vertraulich* beispielsweise verschlüsselt den Ordner *C:\Vertraulich* und alle darunterliegenden Ordner und Dateien.

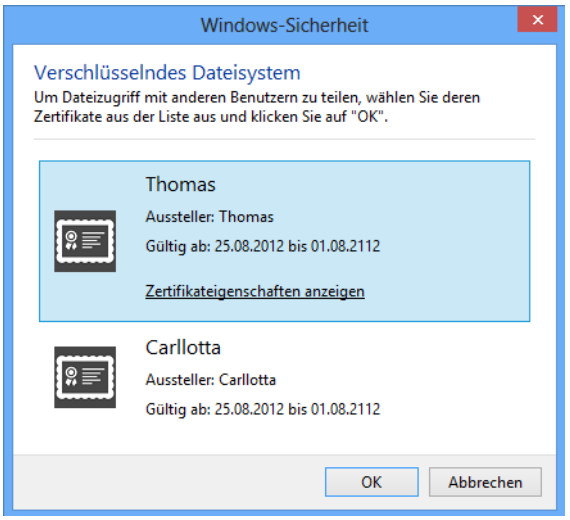
Der Befehl *cipher /d /s:C:\Vertraulich* entschlüsselt die Daten im Ordner *C:\Vertraulich* und allen darunterliegenden Ordnern.

Häufig ist es sinnvoll, vertrauliche Daten mit einer anderen Person zu teilen, beispielsweise zwischen zwei Geschäftsführern oder zwischen Chef und Sekretärin. Wenn Sie auch anderen Personen Zugriff auf Ihre verschlüsselten Dateien gewähren möchten, gehen Sie folgendermaßen vor:

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*. Sie erhalten eine Übersicht darüber, welche Benutzer auf die Datei zugreifen und welche Benutzer die Datei wiederherstellen und dabei die Verschlüsselung aufheben können.
3. 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 Basis-EFS-Zertifikat. Das erhält er am schnellsten, wenn er selbst eine Datei oder einen Ordner verschlüsselt.

Abbildg. 5.24 Gemeinsamer Zugriff auf verschlüsselte Dateien



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. Das gilt auch beim Einsatz von ReFS. Dies bedeutet, dass es unmöglich ist, eine verschlüsselte Datei auf eine CD/DVD zu brennen oder auf einen Wechseldatenträger zu kopieren, ohne die Verschlüsselung zu verlieren, da hier UDF als Dateisystem eingesetzt wird.
- 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 Verschlüsselt-Attribut besitzt. Wenn Sie also eine lokal verschlüsselte Datei auf den Computer kopieren, verliert diese ihre Verschlüsselung, falls Sie im Serverordner nicht vorher ebenfalls die Verschlüsselung aktivieren.
- Systemdateien können nicht verschlüsselt werden.
- Einige Anwendungen zerstören die Zertifikate der zusätzlichen Benutzer beim Schreiben in die Datei. Nur speziell angepasste Programme, wie beispielsweise Office, behalten die EFS-Zertifikate aller Benutzer bei der Dateibearbeitung bei.

Durch Kopieren oder Verschieben unverschlüsselter Dateien in einen verschlüsselten Ordner werden diese Dateien automatisch im neuen Ordner verschlüsselt. Der umgekehrte Vorgang entschlüsselt jedoch Dateien nicht automatisch.

Speicherpools einsetzen

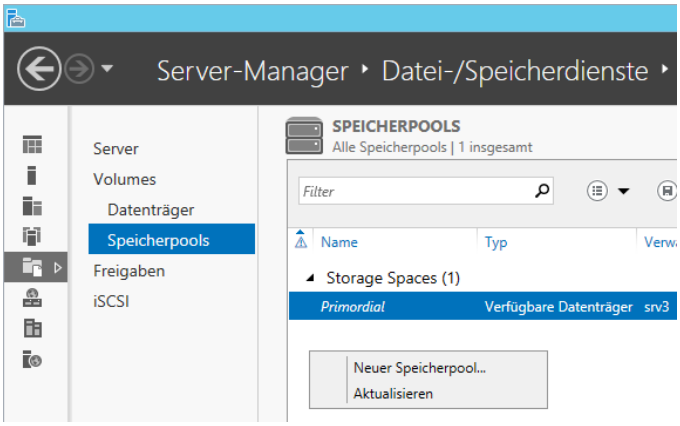
Windows Server 2012 bietet eine wesentliche Neuerung im Vergleich zu Windows Server 2008 R2: die Speicherpools. Einfach ausgedrückt fassen Sie mehrere Datenträger zusammen und konfigurieren diese als einen gemeinsamen Datenträger. In Kapitel 1 sind wir bereits kurz auf das Thema eingegangen. In Windows Server 2012 R2 hat Microsoft die Funktionen erweitert und verbessert, zum Beispiel die Unterstützung für SSD-Festplatten.

Speicherpools verwalten Sie nicht in der Datenträgerverwaltung von Windows Server 2012 R2, sondern im Server-Manager. Hier legen Sie zunächst einen Speicherpool an und weisen diesem anschließend verschiedene Speicherplätze zu. Ein Pool kann dabei mehrere Speicherplätze umfassen. Speicherplätze bestehen in Windows Server 2012 R2 aus virtuellen Festplatten, die Speicherpools zugewiesen sind.

Speicherpools erstellen

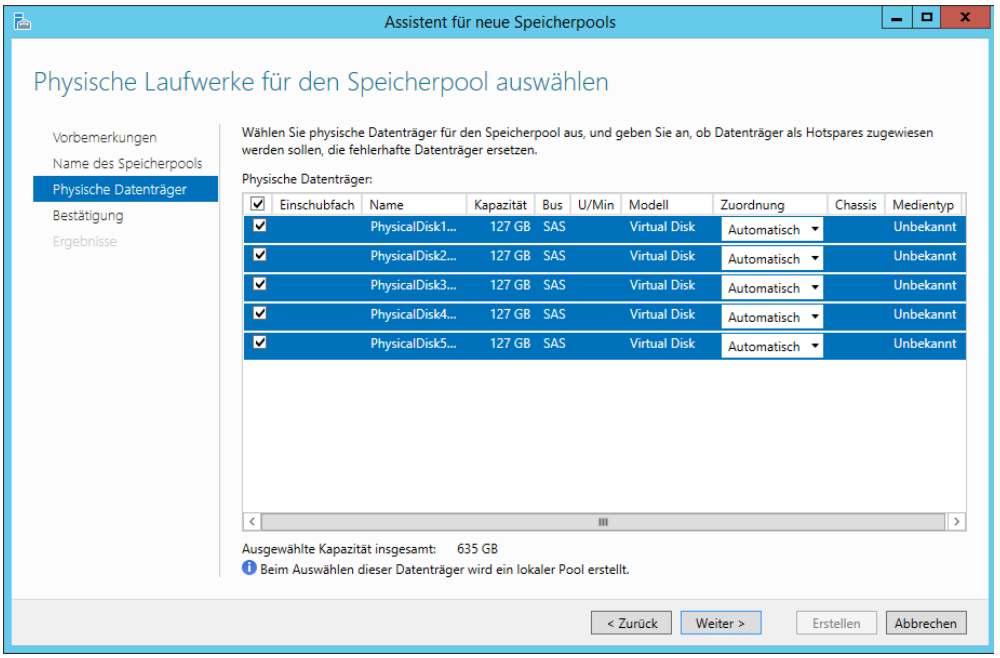
Um Speicherpools in Windows Server 2012 R2 zu erstellen, installieren Sie im Server-Manager die Serverrolle *Datei- und Speicherdienste*. Über die Kategorie *Datei-/Speicherdienste* stehen anschließend die Verwaltungswerkzeuge für Speicherpools zur Verfügung (siehe auch Kapitel 4). Klicken Sie auf *Aufgaben\Neuer Speicherpool* im Menü *Datei-/Speicherdienste/Speicherpools*, erstellen Sie einen neuen Speicherpool.

Abbildg. 5.25 Erstellen eines neuen Speicherpools



Im Assistenten legen Sie zunächst einen Namen und eine Beschreibung fest. Außerdem wählen Sie den Server aus, auf dem Sie einen Speicherpool erstellen wollen. Auf der nächsten Seite wählen Sie aus, welche Festplatten Bestandteil des Pools sein sollen. Sie können an dieser Stelle auch virtuelle Festplatten auf Basis von Hyper-V verwenden.

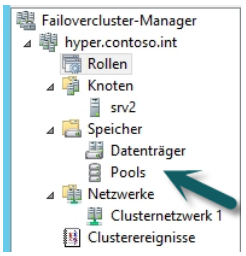
Abbildg. 5.26 Auswählen der Laufwerke für einen Speicherpool



Im Feld *Zuordnung* haben Sie noch die Möglichkeit, einzelne Festplatten als *Hot-Spare* zu kennzeichnen. In diesem Fall dient die Festplatte als Reserve im Speicherpool und wird nicht verwendet. Sie können diese Einstellung aber auch auf *Automatisch* belassen, damit Windows Server 2012 R2 selbst steuern kann, wie mit den Festplatten umgegangen wird.

Ist der Speicherpool erstellt, erstellen Sie virtuelle Festplatten, die den Speicherplatz im Speicherpool nutzen. Diese werden auch Speicherplätze (Storage Spaces) genannt. Hier hat Microsoft eine andere Bezeichnung als in Windows 8/8.1 gewählt. Ein Pool kann mehrere virtuelle Festplatten bereitstellen, die sich dann den Platz im Speicherpool teilen. Virtuelle Datenträger erstellen Sie über einen Rechtsklick auf den Pool in der Speicherverwaltung. Pools sind übrigens auch in der Clusterverwaltung von Windows Server 2012 R2 verfügbar.

Abbildg. 5.27 Pools lassen sich in Windows Server 2012 R2 auch in Clustern nutzen

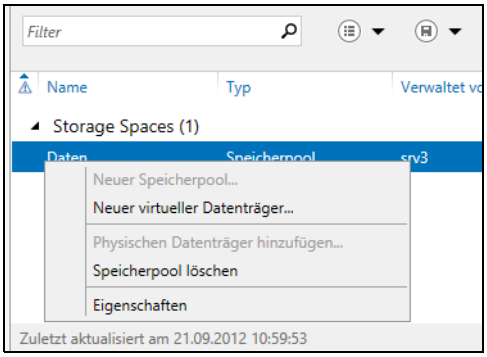


Nachdem physische Festplatten einem Pool zugewiesen sind, erscheinen sie auch nicht mehr in der Datenträgerverwaltung. Die Steuerung erfolgt komplett über den Speicherpool im Server-Manager.

Speicherplätze in Speicherpools erstellen

Klicken Sie auf einen Pool mit der rechten Maustaste, erstellen Sie mit *Neuer virtueller Datenträger* innerhalb des Pools eine neue virtuelle Festplatte. Deren Daten verteilt Windows Server 2012 R2 automatisch über den Speicherpool auf die verschiedenen physischen Datenträger, die Bestandteil des Pools sind.

Abbildg. 5.28 Erstellen von virtuellen Festplatten in Speicherpools



Wenn im Speicherpool eine SSD-Platte integriert ist, können Sie beim Erstellen von virtuellen Datenträgern die Option *Speicherebenen auf diesem virtuellen Datenträger erstellen* aktivieren. Windows Server 2012 R2 speichert dann häufig verwendete Daten im Pool vor allem auf der SSD-Platten und lagert weniger verwendete Daten auf die langsamen Platten aus.

Erstellte virtuelle Festplatten erscheinen in der Speicherverwaltung im Server-Manager unterhalb des entsprechenden Pools. Über das Kontextmenü können Sie den virtuellen Datenträger offline nehmen. Auch eine Erweiterung des Datenträgers ist möglich. Über den Befehl *Eigenschaften* lassen sich die Zustände der Daten prüfen.

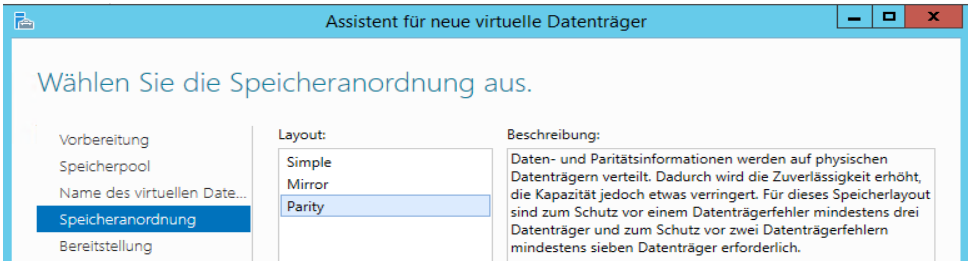
Erstellen Sie einen neuen virtuellen Datenträger, legen Sie im Fenster zunächst den Pool fest. Danach geben Sie den Namen der virtuellen Festplatte an. Als Nächstes steuern Sie die Sicherheit. Hier haben Sie die drei Möglichkeiten *Simple*, *Mirror* und *Parity*:

- **Simple** Erstellt einen normalen Datenträger ohne Ausfallsicherheit. Die Daten sind auf den physischen Festplatten auf dem Server verteilt. Die Geschwindigkeit steigt dadurch, Sie sind aber nicht vor dem Ausfall eines physischen Datenträgers geschützt.
- **Mirror** Erlaubt das Spiegeln der virtuellen Festplatte auf bis zu drei physischen Festplatten, um dem Ausfall eines Datenträgers vorzubeugen. Sie benötigen dazu im Pool mindestens zwei Festplatten, um dem Ausfall eines Datenträgers vorzubeugen oder fünf Festplatten, um dem Ausfall von zwei Datenträgern vorzubeugen.
- **Parity** Verteilt die Daten auf Festplatten im Speicher und benötigt mindestens drei Datenträger. Diese Konfiguration wird nicht für die Verwendung in Clustern unterstützt. Sie benötigen für den Ausfall eines einzelnen Datenträgers mindestens drei physische Festplatten.

Als Nächstes legen Sie den Bereitstellungstyp fest. Mit *Dünn* legen Sie das erwähnte Thin Provisioning fest. Das heißt, virtuelle Festplatten können mehr Speicherplatz verwenden als durch die physischen Festplatten verfügbar ist. Geht der Speicherplatz aus, erscheint eine Warnmeldung und Admi-

nistratoren können dem zugrunde liegenden Speicherpool mehr Speicherplatz zur Verfügung stellen. Bei dieser Konfiguration verwendet der Speicherplatz also immer nur so viel Speicher wie notwendig ist, kann aber über die Größe des maximalen Speicherplatzes hinauswachsen.

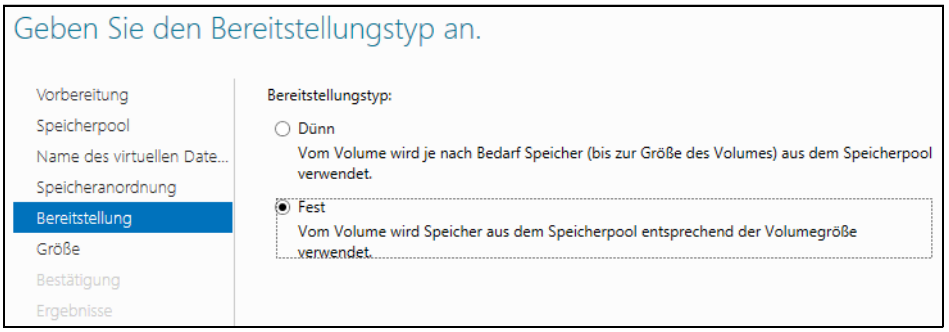
Abbildg. 5.29 Festlegen der Speicheranordnung einer virtuellen Festplatte in einem Speicherpool



Auf diesem Weg erstellen Sie zum Beispiel eine virtuelle Festplatte mit einer Größe von 1 TB, obwohl im Speicherpool nur 600 GB zur Verfügung stehen. Steigt die Größe der virtuellen Festplatte bis an den verfügbaren Platz an, können Administratoren weitere Festplatten in den Pool integrieren.

Bei der Auswahl von *Fest* erlaubt Windows Server 2012 R2 für die virtuelle Festplatte eine maximale Größe, die Sie auf der nächsten Seite festlegen.

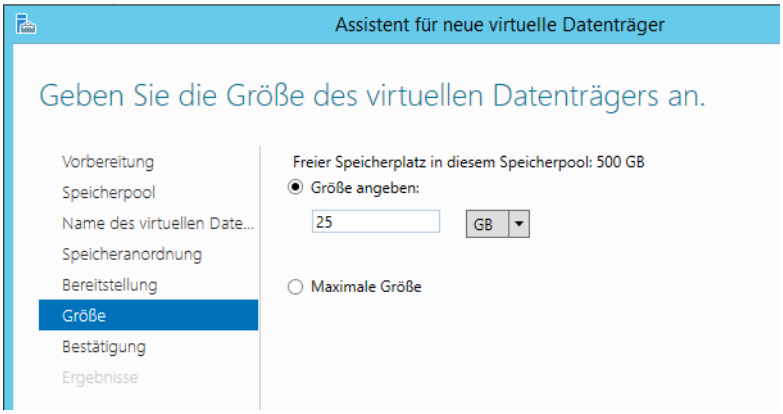
Abbildg. 5.30 Festlegen des Bereitstellungstyps von virtuellen Festplatten



Im nächsten Fenster legen Sie die Größe des virtuellen Datenträgers fest. Haben Sie auf der vorangegangenen Seite *Fest* als Bereitstellungstyp ausgewählt, können Sie im Fenster zur Größe konfigurieren, dass der virtuelle Datenträger gleich seine maximale Größe verwendet. Das erhöht die Geschwindigkeit, kostet aber Speicherplatz auf den physischen Datenträgern des Speicherpools.

Damit Anwender Daten auf den virtuellen Datenträgern im Speicherpool speichern können, müssen Sie noch Volumes anlegen, wie bei herkömmlichen Festplatten auch. Die Volumes sind Teilabschnitte eines virtuellen Datenträgers, der einem Speicherpool zugewiesen ist. Der Speicherpool wiederum ist verschiedenen physischen Festplatten zugeordnet. Wie Sie dabei vorgehen, zeigen wir Ihnen im nächsten Abschnitt.

Abbildg. 5.31 Festlegen der Größe einer virtuellen Festplatte

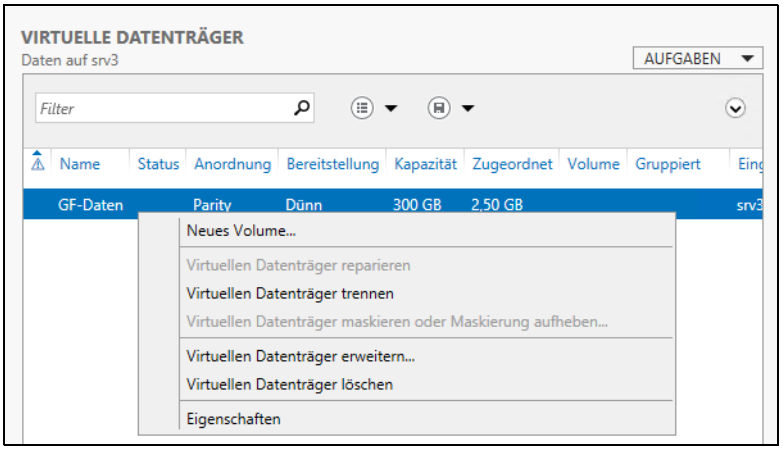


Volumes auf virtuellen Datenträgern in Speicherpools erstellen

Haben Sie einen Speicherpool mit dazugehörigen virtuellen Festplatten erstellt, können Sie auf den einzelnen virtuellen Festplatten noch Volumes erstellen. Hierbei handelt es sich um die logischen Laufwerke, während sich die virtuellen Datenträger wie Laufwerke in der Datenträgerverwaltung verhalten.

Die Volumes sind schließlich die Datenträger, die auch im Explorer erscheinen und auf denen Sie Freigaben erstellen. Klicken Sie dazu im Server-Manager in der Verwaltung der Speicherpools mit der rechten Maustaste auf den entsprechenden virtuellen Datenträger und wählen Sie *Neues Volume* aus.

Abbildg. 5.32 Erstellen von neuen Volumes auf virtuellen Festplatten

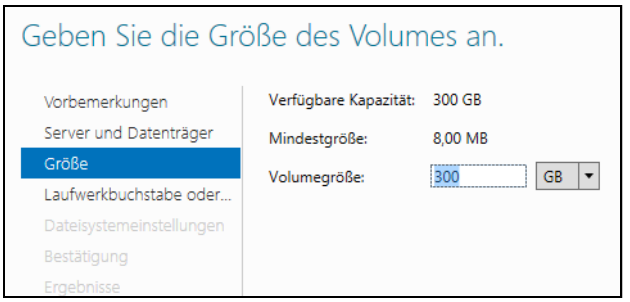


Im Assistenten haben Sie die Möglichkeit, die Volumes auch auf einem anderen Server im Netzwerk zu erstellen, wenn auf diesem Speicherpools und virtuelle Datenträger zur Verfügung stehen. Damit

das funktioniert, müssen Sie den entsprechenden Server aber im Server-Manager über das Menü *Verwalten* hinzufügen (siehe Kapitel 3).

Zunächst wählen Sie aus, auf welchem Server und welchem virtuellen Datenträger Sie ein neues Volume erstellen wollen. Auf der nächsten Seite des Assistenten legen Sie fest, wie groß das neue Volume sein soll. Sie haben auch die Möglichkeit, auf einem virtuellen Datenträger in einem Speicherpool mehrere Volumes zu erstellen.

Abbildg. 5.33 Festlegen der Größe des Volumes



Als Nächstes legen Sie wie bei normalen Laufwerken auch den Laufwerkbuchstaben und das Dateisystem fest. Speicherpools, virtuelle Festplatten und damit verbundene Volumes unterstützen auch ReFS. Das neue Dateisystem arbeitet auch wesentlich besser mit Speicherpools zusammen als NTFS.

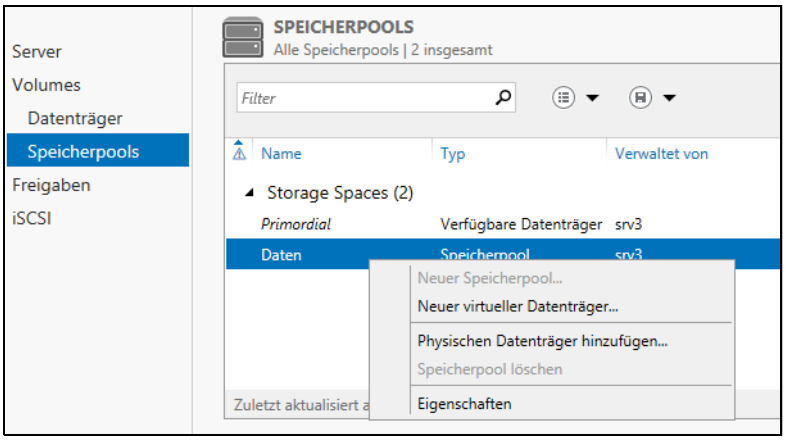
Haben Sie alle Eingaben vorgenommen, erstellt der Assistent das Volume und es steht im Explorer für das Erstellen von Freigaben zur Verfügung. Volumes und virtuelle Datenträger sehen Sie auch in der Datenträgerverwaltung. Sie können daher in der Datenträgerverwaltung Volumes löschen und verwalten. Virtuelle Datenträger verwalten Sie aber besser im Server-Manager über die Speicherpools.

Speicherpools verwalten und physische Festplatten hinzufügen

Im Server-Manager finden Sie die Speicherpools in den Datei-/Speicherdiensten. Im oberen Bereich sehen Sie die angelegten Speicherpools. Über das Kontextmenü rufen Sie Eigenschaften auf oder erstellen neue virtuelle Datenträger. Sind im Server weitere Datenträger verfügbar, können Sie über diesen Bereich neue physische Datenträger dem Pool hinzufügen.

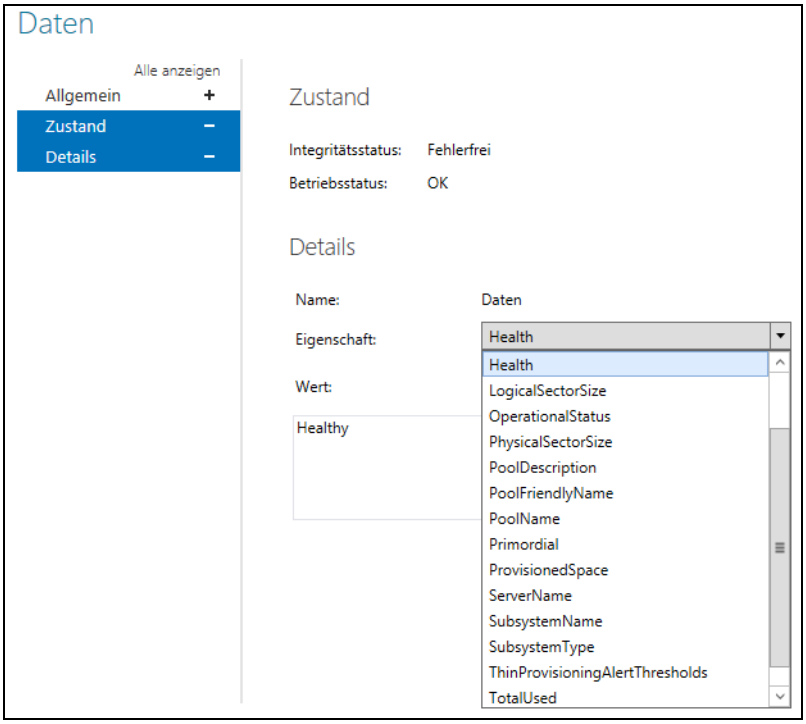
Sie können an dieser Stelle auch Speicherpools löschen, allerdings nur dann, wenn auf diesem keine Volumes und damit verbundene virtuelle Datenträger verbunden sind.

Abbildg. 5.34 Aufgaben für Speicherpools im Server-Manager



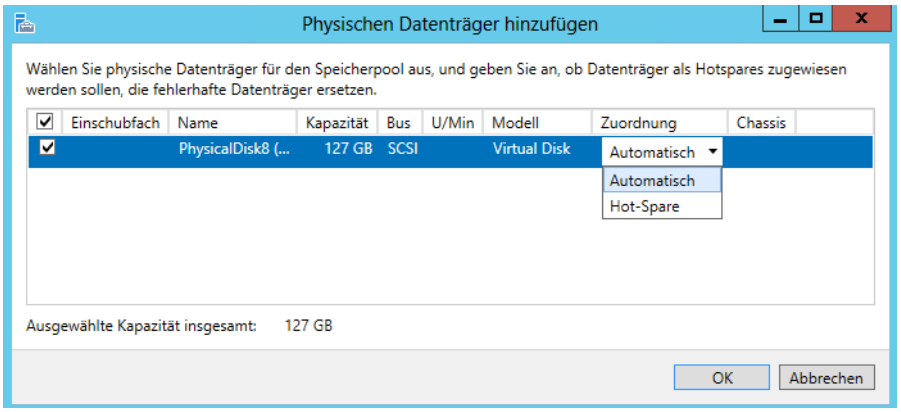
In den Eigenschaften können Sie verschiedene Informationen über den Zustand des Speicherpools abrufen. Sie sehen zum Beispiel den bereits belegten Festplattenplatz, den Zustand und die Integrität. Über *Details* können Sie verschiedene Abfragen vornehmen, indem Sie die gewünschten Eigenschaften im Dropdownmenü auswählen.

Abbildg. 5.35 Abrufen von Daten für einen Speicherpool



Über das Kontextmenü des Speicherpools fügen Sie auch weitere physische Festplatten hinzu. Diese müssen mit dem Server verbunden, aber nicht initialisiert und nicht formatiert sein.

Abbildg. 5.36 Hinzufügen von physischen Festplatten zu einem Speicherpool

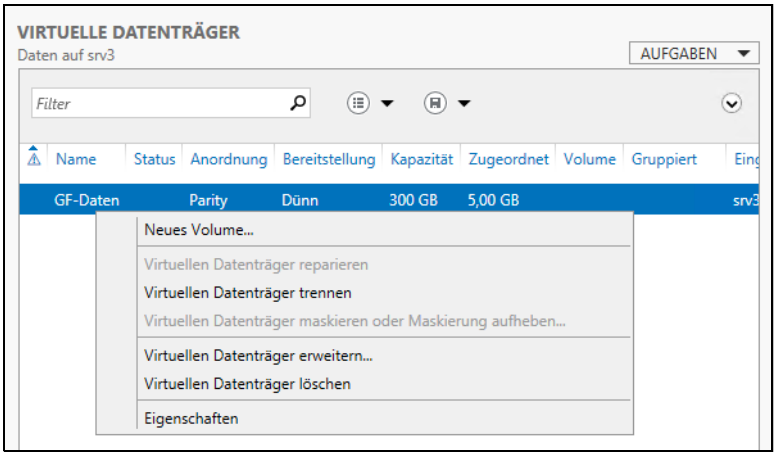


Virtuelle und physische Datenträger verwalten, trennen und löschen

Über das Kontextmenü von virtuellen Datenträgern können Sie diese zeitweise vom Speicherpool trennen, ohne dass Daten verloren gehen und Sie können virtuelle Datenträger erweitern oder löschen. Auch für virtuelle Datenträger gibt es Eigenschaften, in denen Sie Informationen abrufen können. Sie sehen für virtuelle Datenträger auch, welche physischen Festplatten mit dem virtuellen Datenträger verbunden sind.

Benötigen Sie einen bestimmten physischen Datenträger nicht mehr, können Sie ihn über dessen Kontextmenü entfernen. Das geht allerdings nur, wenn er nicht durch einen virtuellen Datenträger in Benutzung ist.

Abbildg. 5.37 Virtuelle Datenträger verwalten

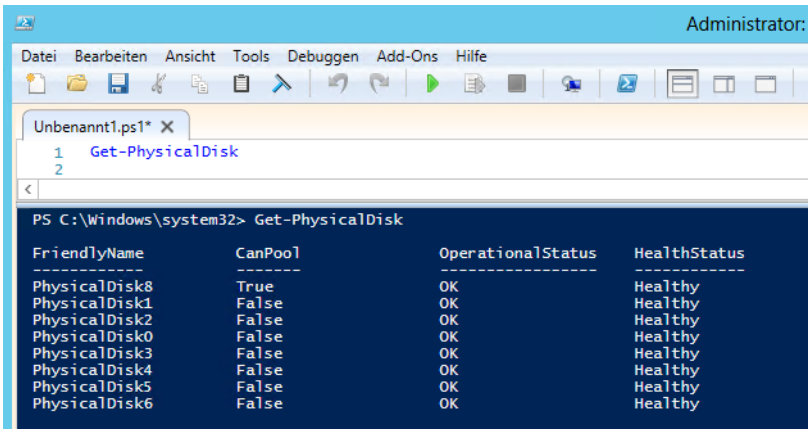


Speicherpools und virtuelle Festplatten mit PowerShell verwalten

Sie können in der PowerShell aber auch mit den echten physischen Laufwerken auf dem PC arbeiten. Alle Befehle, die in der PowerShell zur Verfügung stehen, lassen Sie sich mit *Get-Command –Module Storage | Sort Noun, Verb* anzeigen. Um zum Beispiel die physischen Festplatten abzufragen, hilft der Befehl *Get-PhysicalDisk*. Die Ausgabe zeigt auch an, ob sich die Platte in einem neuen Speicherpool anordnen lässt. Das erkennen Sie an der Option *CanPool* über den Wert *True*. Mehr zu diesem Thema lesen Sie auch in Kapitel 40.

Wer genauere Informationen will, gibt *Get-PhysicalDisk |fl* (formatierte Liste) oder *Get-PhysicalDisk |ft* (formatierte Tabelle) ein. Durch Eingabe von Spalten nach *|fl* oder *|ft* lassen sich erweiterte Informationen angeben und unwichtige ausblenden. Ein Beispiel dafür ist *Get-PhysicalDisk |fl FriendlyName, BusType, CanPool, Manufacturer, Healthstatus*. Das funktioniert mit allen Get-Cmdlets. Mit *Get-Disk* lassen Sie sich ebenfalls alle Festplatten anzeigen. Die Partitionierung lassen Sie mit *Get-Disk <Nummer> | Get-Partition* anzeigen.

Abbildg. 5.38 Anzeigen und abfragen der physischen Laufwerke



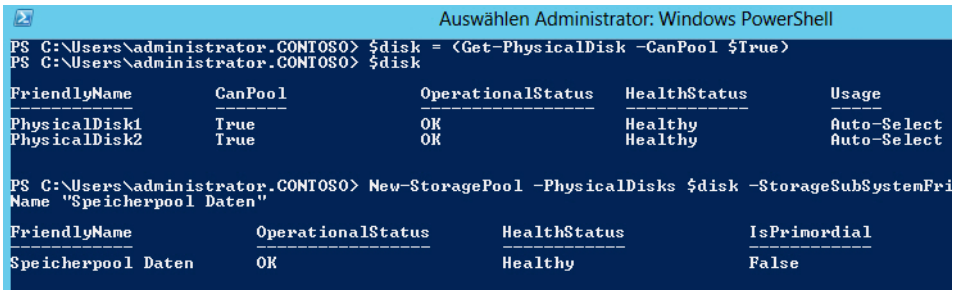
Um einen neuen Speicherpool zu erstellen, bietet es sich zum Beispiel an, Festplatten die poolfähig sind, also bei der Option *CanPool* den Wert *True* haben, in einer Variablen zu speichern. Diese Variable können Sie dann an das Cmdlet *New-StoragePool* weitergeben, um einen Speicherpool zu erstellen.

Nachdem ein Pool erstellt ist, können Sie virtuelle Laufwerke anlegen. Auch dieser Vorgang lässt sich leicht in der PowerShell durchführen. Dabei hilft das Cmdlet *New-VirtualDisk*.

In der PowerShell verwenden Sie zum Beispiel:

```
$disks= (Get-PhysicalDisk –CanPool $True
New-StoragePool –PhysicalDisks $disks –StorageSubSystemFriendlyName *Pool1* –FriendlyName
"Daten2"
New-VirtualDisk –StoragePoolFriendlyName "Daten" –ResiliencySettingName Mirror –Size 2TB –
Provisioningtype Thin –FriendlyName "Dokumente"
```

Abbildg. 5.39 Anlegen und verwalten von Speicherpools in der PowerShell



Um keine Thin Provisioning-Festplatte zu erstellen, sondern eine mit fester Größe, verwenden Sie den Befehl:

```
New-VirtualDisk –StoragePoolFriendlyName <Name> –FriendlyName <Name> –Size (<Größe>) –
ProvisioningType Fixed
```

Um die Ausfallsicherheit zu steuern, können Sie ebenfalls die PowerShell verwenden, zum Beispiel mit:

```
New-VirtualDisk –FriendlyName <Name> –Size (<Größe>) –ResiliencySettingsName Mirror
```

Get-VirtualDisk zeigt virtuelle Festplatten an, *Initialize-Disk –DiskNumber <Nummer>* initialisiert Festplatten in der PowerShell. *New-Partition –DiskNumber <Nummer> –UseMaximumSize –Assign-DriveLetter* erstellt eine neue Partition, auch auf virtuellen Festplatten. Um eine neue Partition zu formatieren, verwenden Sie zum Beispiel den Befehl *Format-Volume –DriveLetter <Buchstabe> –FileSystem NTFS*.

Sie können in der PowerShell aber nicht nur Speicherpools, virtuelle Festplatten und Partitionen erstellen, sondern diese Bereiche auch verwalten und erweitern. Um zum Beispiel die Ausfallsicherheit der verschiedenen virtuellen Festplatten anzuzeigen, verwenden Sie das Cmdlet *Get-Resiliency-Setting*.

- *Add-PhysicalDisk –StoragePoolFriendlyName <Speicherpool>* fügt eine neue Festplatte hinzu
- *Remove-VirtualDisk* löscht virtuelle Festplatten
- *Remove-StoragePool* löscht einen kompletten Speicherpool
- *Repair-VirtualDisk* kann Speicherpools reparieren

Sie können neue Festplatten auch direkt als Hot-Spare zu einem Speicherpool hinzufügen:

```
Add-PhysicalDisk –StoragePoolFriendlyName <Name> –PhysicalDisks (Get-PhysicalDisk –
friendlyname <Name>) –Usage Hot-Spare
```

Um zum Beispiel eine physische Festplatte zu entfernen, verwenden Sie folgende Befehle:

```
Set-PhysicalDisk –FriendlyName <Name> –Usage Retired
Get-PhysicalDisk –FriendlyName <Name> | Get-VirtualDisk | Repair-VirtualDisk
```

HINWEIS Achten Sie darauf, dass beim Entfernen einer physischen Festplatte noch genügend Speicherplatz im Pool zur Verfügung steht.

Arbeitsplatznetzwerke und Arbeitsordner in Windows 8.1

Mit Windows 8.1 bietet Microsoft zahlreiche Neuerungen, die auch für professionelle Anwender eine wichtige Rolle spielen. Microsoft will mit Windows 8.1 vor allem den Bring-Your-Own-Device (BYOD)-Ansatz von Unternehmen unterstützen. Ohne dass ein Windows 8.1-PC oder Tablet-PC Mitglied einer Domäne ist, kann der Computer im Netzwerk oder über das Internet auf Unternehmensressourcen zugreifen. Außerdem ist es möglich, dass Anwender Daten in einen bestimmten Ordner auf dem Client speichern und dieser Ordner mit Servern synchronisiert wird. Der Vorteil dabei ist, dass der Inhalt der Arbeitsordner auf den Server gesichert und auf allen Rechnern des Anwenders zur Verfügung gestellt wird. Für jeden Benutzer kann Windows Server 2012 R2 einen Unterordner anlegen, in dem die Daten des Anwenders gespeichert werden und auf den nur der jeweilige Anwender Zugriff hat.

Einleitung zu den Arbeitsordnern

Mit den Arbeitsordnern bieten Windows Server 2012 R2 und Windows 8.1 die Möglichkeit, Ordner auf Client-PCs zu synchronisieren, die nicht Mitglied einer Domäne sein müssen. Dies ist vor allem für Tablet-PCs und Notebooks ein interessantes Feature. Speichern Anwender die Daten in einem Arbeitsordner, werden diese Daten automatisch mit ihrem Ordner innerhalb des Arbeitsordners auf dem Server synchronisiert. Das heißt, Anwender arbeiten lokal mit bestimmten Dateien, die der Client automatisch mit dem Server synchronisiert. Diese Technik funktioniert nur mit Windows Server 2012 R2 und Windows 8.1. Der Rechner kann dazu Mitglied einer Domäne sein, muss es aber nicht.

Arbeitsplatznetzwerke (Workplace Join) geht in die gleiche Richtung und bietet Anwendern auch ohne Domänenmitgliedschaft die Möglichkeit, auf Unternehmensressourcen zugreifen zu können. Mehr zu Arbeitsplatznetzwerken lesen Sie in Kapitel 42

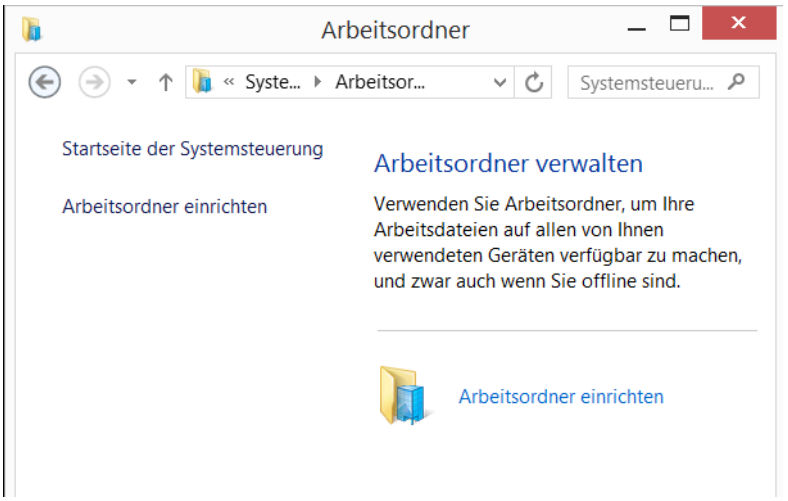
HINWEIS Windows 8.1 bietet zusammen mit Windows Server 2012 R2 die Möglichkeit, Rechner auch ohne Domänenmitgliedschaft an die Ressourcen im Unternehmen anzubinden. Auch iOS-Geräte sowie Tablet-PCs mit Windows RT 8.1 erhalten diese Möglichkeiten.

Allerdings haben diese Geräte keinen Zugriff auf die Arbeitsordner, sondern können Mitglied der Domäne über die Arbeitsnetzwerk-Funktion werden. In Windows 8.1 finden Sie die Einstellungen in der Charms-Leiste über *PC-Einstellungen ändern/Netzwerk/Arbeitsplatz*. Das Arbeitsplatznetzwerk hat nichts mit den Arbeitsordnern zu tun.

Mehr zu diesem Thema erfahren Sie auf der Seite *http://technet.microsoft.com/en-us/library/dn280938.aspx* [Ms179-K05-03]. Sie benötigen für das Arbeitsplatznetzwerk (Workplace Join) die Active Directory-Verbunddienste.

Im Netzwerk muss dazu Windows Server 2012 R2 bereitgestellt sein. In einem TechNet-Video (*http://channel9.msdn.com/posts/Introduction-to-Work-Folders* [Ms179-K05-04]) sehen Sie die Möglichkeiten des Diensts.

Abbildg. 5.40 Mit den Arbeitsordnern können Anwender Daten des Servers mit dem Notebook synchronisieren, ähnlich wie Offlinedateien



Administratoren können, ähnlich wie im Bereich Exchange ActiveSync, Sicherheitsrichtlinien für Arbeitsplatznetzwerke und Arbeitsordner festlegen. Wenn sich ein Anwender zu einer Ressource mit seinem Gerät verbindet, muss dieser bestätigen, dass er diese Richtlinien einhält. So können Administratoren zum Beispiel festlegen, dass das Benutzerkonto auf dem zugreifenden Rechner besonders sicher sein muss.

Viele Einstellungen für Windows 8.1 wie Arbeitsordner, Startseite und den Windows Store können Sie nur über Gruppenrichtlinien oder den Server-Manager vorgeben, wenn Sie einen Server mit Windows Server 2012 R2 im Netzwerk im Einsatz haben. Dies gilt auch für die Arbeitsordner. Sie müssen dazu nicht alle Server umstellen.

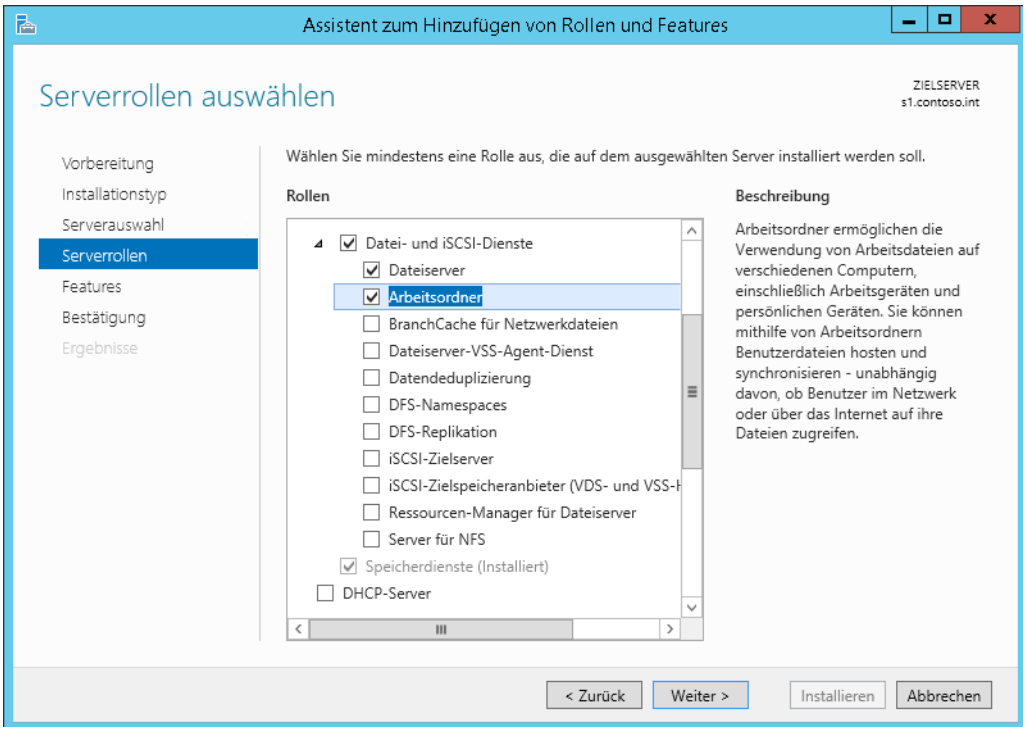
Dateiserver für Arbeitsordner konfigurieren

Um Arbeitsordner für Windows 8.1 bereitzustellen, müssen Sie auf dem entsprechenden Dateiserver mit Windows Server 2012 R2 die Serverrolle *Datei-/Speicherdienste/Datei- und iSCSI-Dienste/Arbeitsordner* installieren.

TIPP Sie können die Arbeitsordner in Windows Server 2012 R2 auch mit der PowerShell installieren. Dazu verwenden Sie das Cmdlet *Add-WindowsFeature FS-SyncShareService*.

Nachdem Sie die Serverrolle installiert haben, steht im Server-Manager der Bereich *Datei- und Speicherdienste/Arbeitsordner* zur Verfügung. In diesem Fenster starten Sie einen Assistenten, der Sie bei der Einrichtung der Arbeitsordner unterstützt.

Abbildg. 5.41 Die Arbeitsordner in Windows 8.1 installieren Sie über eine Serverrolle in Windows Server 2012 R2

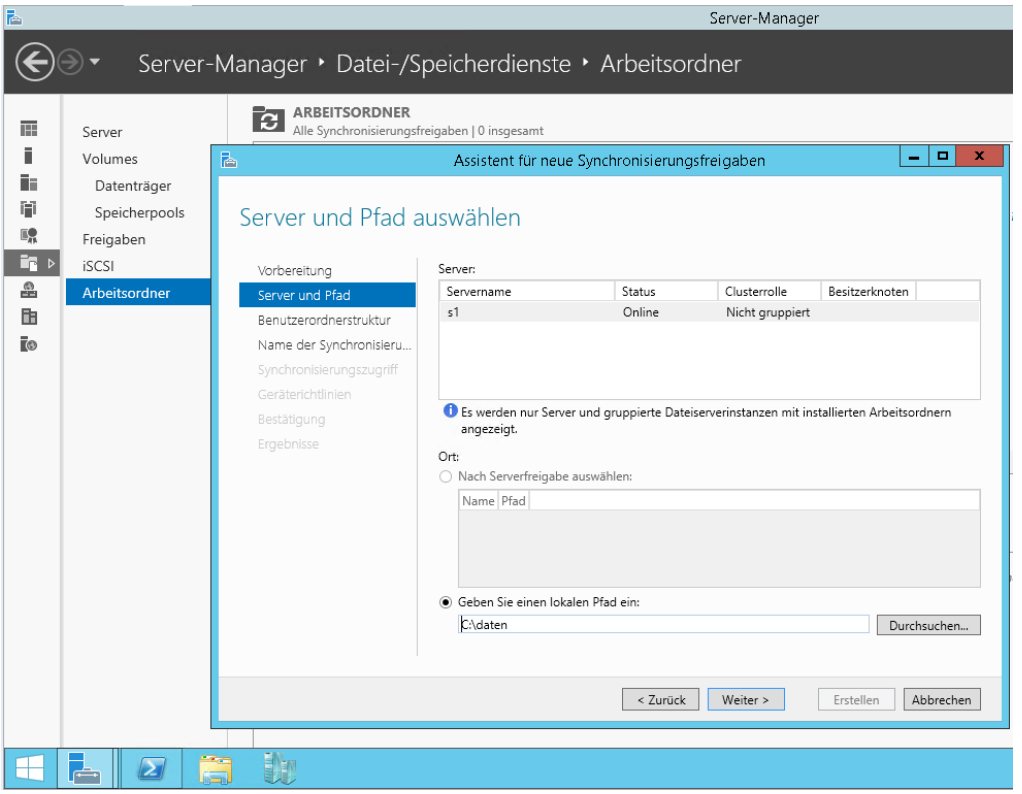


Im Assistenten legen Sie die Ordner auf den Dateiservern fest, die Anwender über Arbeitsordner verwenden können. Sie haben auch die Möglichkeit, über den Assistenten bestimmten Benutzern und Gruppen den Zugriff zu gestatten. Unterhalb des Ordners auf dem Server legt Windows Server 2012 R2 automatisch Unterordner für die Benutzerkonten an. Auf die Unterordner haben nur die jeweiligen Anwender Zugriff.

Nach der Einrichtung des Arbeitsordners müssen Sie dann lediglich noch die entsprechenden Benutzerkonten in die Gruppe mit aufnehmen. Auch die Richtlinieneinstellungen steuern Sie hier. Haben Sie den Ordner angelegt, wird dieser im Server-Manager angezeigt. Sie können die Einstellungen jederzeit ändern und die Bereitstellung von Ordnern als Arbeitsordner widerrufen.

Während der Einrichtung legen Sie fest, welche Ordner auf dem lokalen Server Sie über Arbeitsordner zur Verfügung stellen wollen und welche Benutzer Zugriff auf die Arbeitsordner erhalten sollen. Damit der Zugriff stabil funktioniert, sollten Sie am besten Freigaben verwenden, auf die Anwender auch im internen Netzwerk über SMB zugreifen. Dann können Anwender nicht nur über die Arbeitsordnertechnologie in Windows 8.1 auf den Inhalt des Ordners zugreifen, sondern auch mit einer normalen Freigabe.

Abbildg. 5.42 Im Server-Manager steuern Sie die Arbeitsordner im Unternehmen



Sie sehen alle freigegebenen Arbeitsordner im Server-Manager. Über das Kontextmenü können Sie die Einstellungen bearbeiten oder die Freigabe als Arbeitsordner entfernen.

Windows 8.1 an Arbeitsordner anbinden

Standardmäßig erlauben Windows 8.1 und Windows Server 2012 R2 den Zugriff auf Arbeitsordner nur über Secure Sockets Layer (SSL). Das heißt, auf dem Client müssen Zertifikate und SSL angepasst und konfiguriert werden.

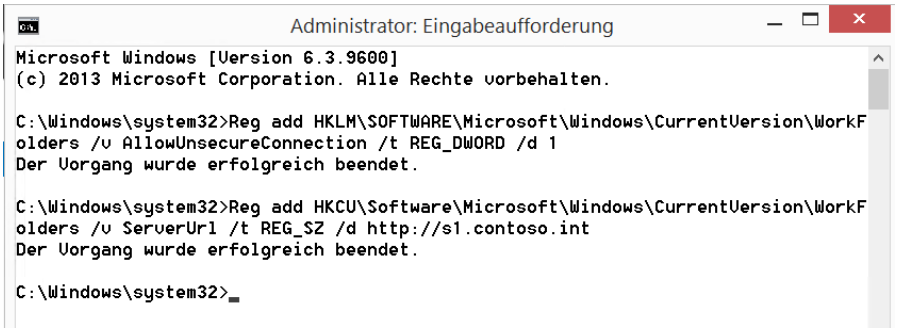
Sie können für Testumgebungen oder in Umgebungen, die ohne SSL-Zugriff funktionieren sollen, auch ohne SSL-Verbindungen mit Arbeitsordnern arbeiten. Dazu müssen Sie auf den Clients einen Registry-Schlüssel setzen. Am einfachsten erledigen Sie dies mit dem folgenden Befehl in der Eingabeaufforderung:

```
Reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WorkFolders /v
AllowUnsecureConnection /t REG_DWORD /d 1
```

Danach müssen Sie einen weiteren Eintrag vornehmen, mit dem die Verbindung zum Server mit dem Arbeitsordner hergestellt wird:

```
Reg add HKCU\Software\Microsoft\Windows\CurrentVersion\WorkFolders /v ServerUrl /t REG_SZ
/d http://<FQDN des Arbeitsordnerservers>
```

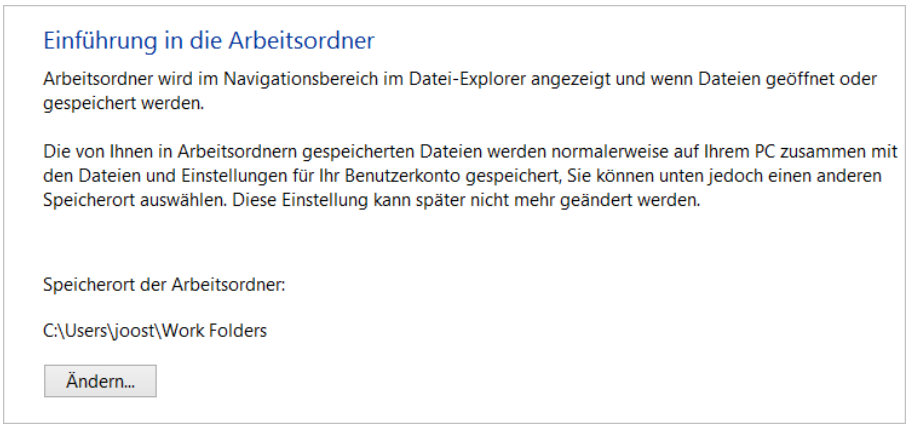
Abbildg. 5.43 Damit der Zugriff auf Arbeitsordner auch ohne SSL funktioniert, müssen Sie noch Einstellungen ändern



Um Zugriff auf den Arbeitsordner zu erhalten, starten Anwender den Assistenten über *Systemsteuerung/System und Sicherheit/Arbeitsordner*. Im Fenster geben Sie den vollständigen Anmeldenamen des Anwenders ein, zum Beispiel *thomas.joos@contoso.int*. Sie können an dieser Stelle auch die E-Mail-Adresse verwenden, wenn Sie mit Exchange Server 2013 arbeiten. In diesem Fall müssen Sie jedoch den vollständigen Anmeldenamen des Anwenders entsprechend anpassend. Sie sehen die Namen im Snap-In *Active Directory-Benutzer und -Computer* in den Eigenschaften des Benutzerkontos.

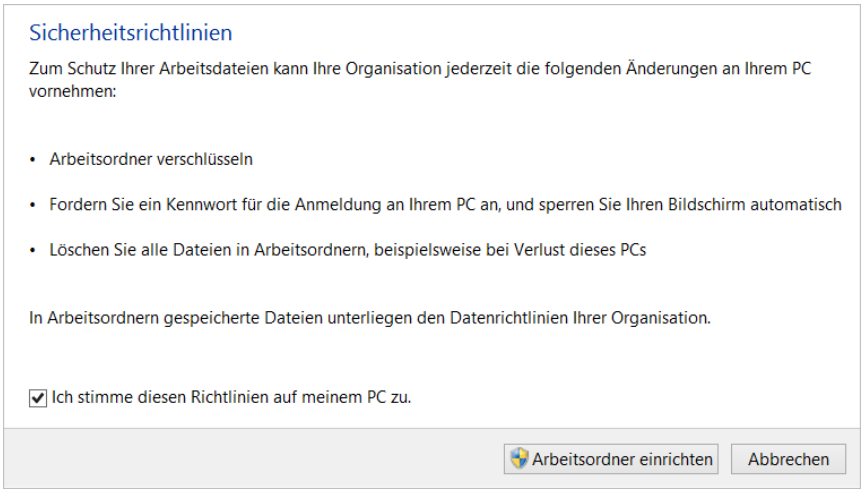
Nach der Anmeldung über den Anmeldenamen oder die E-Mail-Adresse verbindet der Server im Netzwerk den Anwender mit seinem Arbeitsordner. Ist der PC kein Mitglied der Domäne, erscheint zusätzlich ein Anmeldefenster. Hier muss der Anwender sich mit seinem Benutzernamen an der Domäne anmelden. Dies allerdings nur dann, wenn der Rechner noch kein Mitglied der Domäne ist.

Abbildg. 5.44 Anbindung von Windows 8.1 an Arbeitsordner in Windows Server 2012 R2



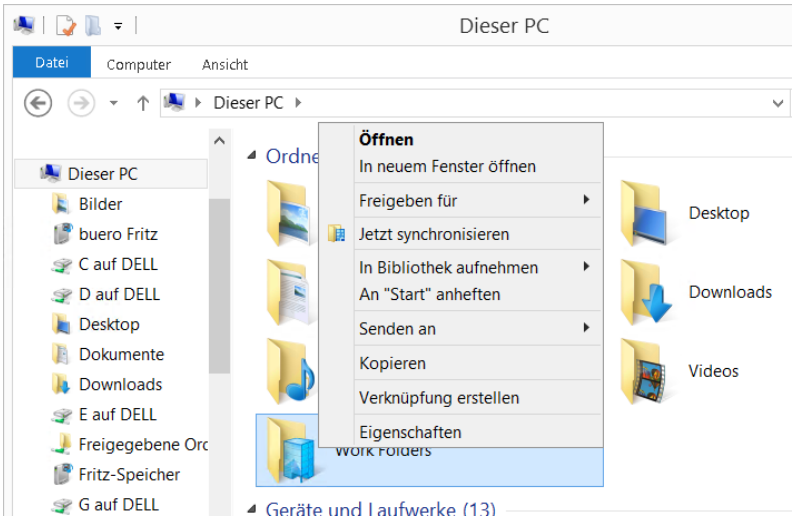
Bestätigen Sie danach die Erstellung des Arbeitsordners und übernehmen Sie die Richtlinieneinstellungen, die auf dem Server bei der Einrichtung des Arbeitsordners festgelegt wurden. Danach schließen Sie die Anbindung an den Arbeitsordner ab.

Abbildg. 5.45 Anwender müssen die Sicherheitseinstellungen für den Arbeitsordner bestätigen



Wenn Sie die Arbeitsordner angepasst haben, bindet Windows diese im Explorer an. Alle Daten im Arbeitsordner synchronisiert der Client mit dem Server. Binden Sie andere Rechner an den gleichen Arbeitsordner an, werden die Daten ebenfalls auf diesen Rechner synchronisiert. Über das Kontextmenü eines Arbeitsordners im Explorer können Sie diesen mit dem Server synchronisieren lassen.

Abbildg. 5.46 Anwender können mit den Arbeitsordnern auf dem Client arbeiten. Die Daten werden automatisch auf den Server synchronisiert.



In den Einstellungen der Arbeitsordner auf dem Client mit Windows 8.1 sehen Sie die Daten zum Arbeitsordner auf dem Server, also den verfügbaren Speicherplatz, die durchgeführten Synchronisierungen und ob Fehler bei der Synchronisierung aufgetreten sind.

Abbildg. 5.47 Die Verwendung der Arbeitsordner steuern Sie über den Client

Unternehmen haben also die Möglichkeit, Windows-PCs in Zukunft entweder in die Domäne aufzunehmen oder die Verantwortung von Rechnern den Anwendern zu überlassen und nur die Ressourcen bereitzustellen. Heimarbeitsplätze und Notebooks lassen sich so deutlich effizienter nutzen. Neben Windows 8.1 können auch iPhones/iPads mit iOS 7 diese Funktion nutzen.

Software-RAID in Windows Server 2012 R2

Neben der Möglichkeit von Speicherpools und klassischen Laufwerken, übergreifenden Volumes und Stripesetvolumes haben Sie in Windows Server 2012 R2 noch weitere Möglichkeiten, um Software-RAIDs zu erstellen. Wir gehen in diesem Abschnitt ausführlicher darauf ein.

RAID-5 und RAID-1 erstellen

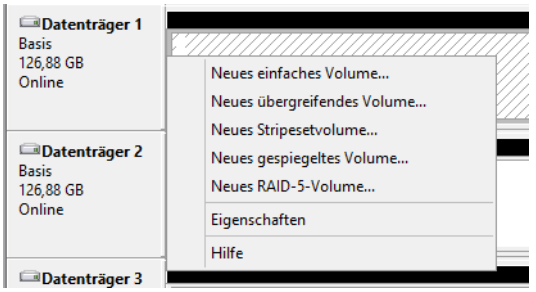
Eine fehlertolerante Variante ist das RAID-5-Volume. Dabei verwendet Windows Server 2012 R2 mindestens drei und bis zu 32 Festplatten. Es muss auf allen physischen Datenträgern gleich viel Platz zur Verfügung stehen. Wenn Sie drei Festplatten verwenden, schreibt Windows auf die 64 KB-Blöcke der ersten und zweiten Platte Daten und auf die dritte Platte Paritätsinformationen, mit denen sich die Daten im Fehlerfall wiederherstellen lassen.

Die nächsten Blöcke von Daten speichert Windows auf die zweite und dritte Festplatte, 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 verwenden Sie 33 % des Plattenplatzes für die Informationen zur Wiederherstellung, 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 und die Paritätsinformationen nicht von einem dedizierten Prozessor berechnet werden. Außerdem unterstützen Sie kein Hot-Swap. Hot-Swap bezeichnet den Wechsel von Festplatten im laufenden Betrieb. Es wird daher empfohlen, auf Hardwarelösungen für RAID-Systeme auszuweichen.

Schließlich gibt es in Windows Server 2012 R2 noch die Plattenspiegelung für Laufwerke. Dort werden alle Informationen auf zwei Festplatten geschrieben. Von gespiegelten Festplatten können Sie auch booten. 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.

Abbildg. 5.48 Erstellen von erweiterten Laufwerken in Windows Server 2012 R2



Der nächste generell zu erfolgende Schritt ist die Zuordnung von Laufwerkbuchstaben und -pfaden. Dieser Schritt kann jederzeit später über den Befehl *Laufwerkbuchstaben und -pfad ändern* im Kontextmenü des entsprechenden Laufwerks durchgeführt werden. Die Optionen sind identisch mit dem Erstellen von erweiterten Laufwerken.

Sie können für Software-RAIDs in Windows Server 2012 auch das ReFS-Dateisystem verwenden. Die Erstellung und Verwaltung ist identisch mit der Verwendung von NTFS.

Software-RAIDs reparieren

Haben Sie zum Beispiel ein Volume erstellt, das sich über mehrere Datenträger erstreckt, können Sie über das Kontextmenü das Volume reparieren, wenn einer der Datenträger defekt ist und Sie ihn ausgetauscht haben. Bei übergreifenden Datenträgern müssen Sie in diesem Fall noch Nacharbeiten vornehmen. Sind bei übergreifenden Datenträgern Aufgaben notwendig, kennzeichnet Windows diese in der Datenträgerverwaltung entsprechend.

In diesem Fall zeigt das Kontextmenü des Datenträgers im unteren Bereich weitere Einstellungsmöglichkeiten. Das Kontextmenü ist abhängig vom Datenträger, den Sie erstellt haben. Es werden nicht immer alle möglichen Optionen angezeigt.

Ist ein erweiterter Datenträger defekt, weil auf eine physische Festplatte nicht mehr zugegriffen werden kann, erscheint *Volume reparieren*, wenn Windows noch einen leeren Datenträger findet, mit dem sich das erweiterte Volume reparieren lässt. Wählen Sie diesen Menüpunkt aus, schlägt Windows automatisch den physischen Datenträger vor, mit dem das übergreifende Volume repariert werden kann. Ist also eine physische Festplatte eines RAID-5-Volumes defekt, tauschen Sie das Laufwerk aus, starten Windows neu und wählen dann im Kontextmenü den Eintrag *Volume reparieren* aus. Sie müssen dazu den Datenträger nicht initialisieren, ihn aber online schalten.

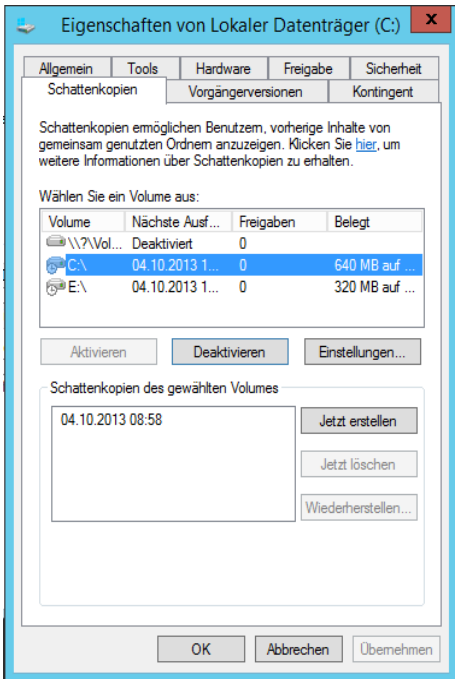
Haben Sie eine physische Festplatte nur kurzzeitig vom System getrennt und verbinden Sie diese wieder mit dem Computer, müssen Sie nicht das Volume reparieren, sondern können über das Kontextmenü des Datenträgers diesen wieder reaktivieren.

Fehlt ein physischer Datenträger eines übergreifenden Volumes, deaktiviert Windows das entsprechende Laufwerk im Explorer, falls ein technischer Zugriff nicht mehr möglich ist. Mit *Volume erneut aktivieren* können Sie den Datenträger in diesem Fall wieder aktivieren, um zum Beispiel Daten auszulagern.

Verwenden von Schattenkopien

Eine wichtige Funktionalität zur Datensicherung von Windows Server 2012 R2 sind die Schattenkopien. Diese stehen aber nur in NTFS zur Verfügung. Auf ReFS-Laufwerken können Sie keine Schattenkopien konfigurieren. 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 lassen sich das System und einzelne Dateien wiederherstellen.

Abbildg. 5.49 Aktivieren von Schattenkopien für einen Datenträger

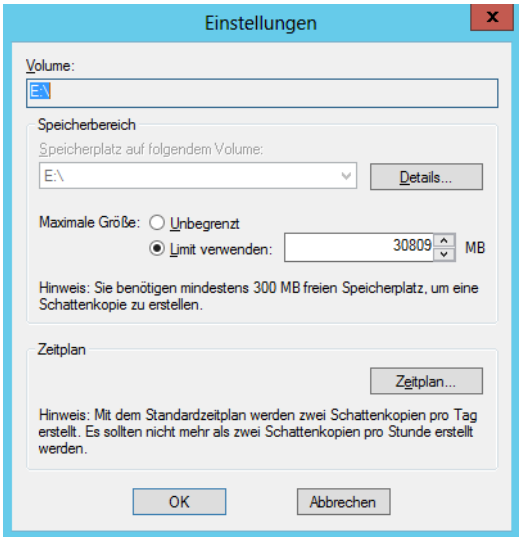


Benutzer können wieder auf frühere Versionen von Dateien zurückgreifen, indem sie diese aus einer Schattenkopie wiederherstellen. Schattenkopien werden bei den Eigenschaften von Datenträgern auf der Registerkarte *Schattenkopien* in den Eigenschaften von Datenträgern konfiguriert. Sie können die Datenträger auswählen, für die Schattenkopien erzeugt werden sollen.

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 diese 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. 5.50 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 Ordners, in dem sich die besagte Datei befindet, eine frühere 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 2012 R2 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.

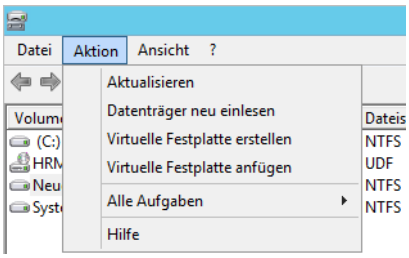
Erstellen und Verwalten von virtuellen Festplatten

Windows 8 und Windows Server 2012 R2 können VHD-Dateien direkt in das Betriebssystem einbinden und diese wie normale Laufwerke nutzen. Das funktioniert auch ohne Speicherpools (siehe Kapitel 2). Im folgenden Abschnitt zeigen wir Ihnen den Umgang mit virtuellen Festplatten. Diese spielen auch in den Kapiteln 7, 8 und 9 eine wichtige Rolle.

Virtuelle Festplatten in der Datenträgerverwaltung erstellen

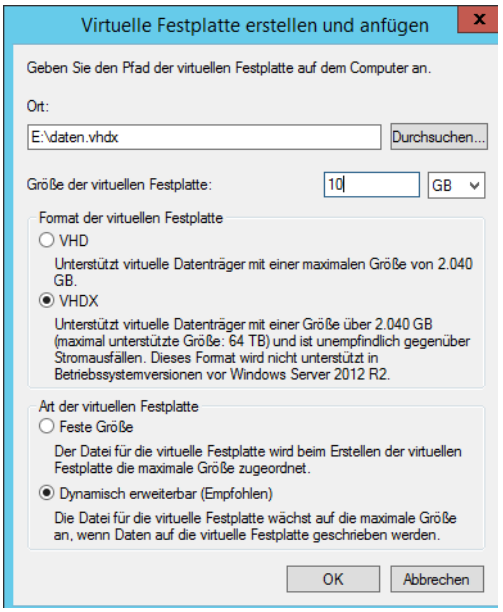
Die Steuerung dieser virtuellen Festplatten finden Sie in der Festplattenverwaltung über das Menü *Aktion*.

Abbildg. 5.51 Verwalten von virtuellen Festplatten



Klicken Sie auf den Menübefehl *Virtuelle Festplatte erstellen*, um den Assistenten zu starten. Wie Hyper-V beherrscht auch Windows Server 2012 R2 das neue VHDX-Format für virtuelle Festplatten. Diese Dateien sind unempfindlicher gegenüber Abstürzen des Host-Systems und erlauben eine Größe von bis zu 64 TB.

Abbildg. 5.52 Erstellen einer neuen virtuellen Festplatte



Im Assistenten legen Sie fest, wo Sie die VHDX-Datei der Festplatte speichern wollen und wie groß die Festplatte sein soll. An dieser Stelle legen Sie auch fest, ob die Festplatte anwachsen darf oder ob Sie eine feste Größe verwenden wollen.

Wählen Sie den Befehl *Virtuelle Festplatte anfügen* aus, können Sie bereits bestehende Datenträger an den Computer anbinden. Das funktioniert auch, wenn Sie auf eine VHD(X)-Datei doppelklicken.

Nachdem Sie die virtuelle Festplatte erstellt haben, zeigt Windows diese in der Datenträgerverwaltung an und Sie können die virtuelle Festplatte wie jede andere auch verwalten.

TIPP Mit dem kostenlosen Tool Disk2vhd von Microsoft-Sysinternals (*http://technet.microsoft.com/de-de/sysinternals/ee656415* [Ms179-K05-05]) können Sie über eine grafische Oberfläche mit einem Klick ein Image von physischen Festplatten in eine VHD-Datei erstellen.

Der Computer kann dabei problemlos weiterlaufen, der Imageprozess findet im Hintergrund statt. Das Tool kann allerdings keine VHDX-Dateien erstellen. Sie können zum Konvertieren aber den Hyper-V-Manager nutzen oder das Cmdlet convert-VHD.

Bei der Verwendung gibt es keine Unterschiede zu physischen Datenträger aber alle Daten der Festplatte liegen in der Datei. Nachdem Sie den Datenträger angelegt haben, müssen Sie diesen, wie jeden anderen Datenträger auch, initialisieren und formatieren. Klicken Sie dazu nach dem Anlegen der Festplatte mit der rechten Maustaste auf den freien Speicherplatz. Über das Kontextmenü des virtuellen Datenträgers können Sie diesen zeitweise offline schalten, also für die Verwendung deaktivieren, oder Sie können den Datenträger wieder vom System entfernen.

VHD(X)-Festplatten konvertieren und in der PowerShell verwalten

Haben Sie noch VHD-Dateien im Einsatz, können Sie diese in VHDX-Dateien umwandeln. Sie können zum Konvertieren den Hyper-V-Manager oder das Cmdlet *Convert-VHD* nutzen. Im Hyper-V-Manager (siehe Kapitel 7, 8 und 9) rufen Sie über den Link *Datenträger bearbeiten* den entsprechenden Assistenten auf. Laden Sie die VHD-Datei, können Sie im Assistenten bequem die Konvertierung durchführen. Dazu wählen Sie die Aktion *Konvertieren* aus.

Auf dem gleichen Weg lässt sich auch eine Konvertierung von VHDX-Dateien in das VHD-Format durchführen. Im Rahmen der Umwandlung wählen Sie das Datenträgerformat aus und können zusätzlich zwischen dem Typ der Festplatten, also feste Größe oder dynamisch erweiterbar, wechseln.

Das Cmdlet *Convert-VHD* steht auch zur Verfügung, wenn Sie Hyper-V in Windows 8.1 Pro/Enterprise installiert haben, also nicht nur in den Server-Betriebssystemen. Vorteil des Cmdlets ist die Möglichkeit, nicht nur VHD-Dateien in VHDX-Dateien umwandeln zu können, sondern auch den umgekehrten Weg zu gehen. Das heißt, Sie können von den Vorteilen des neuen Formats profitieren und im Notfall wieder zurückkonvertieren, wenn eine virtuelle Festplatte an ein anderes System angebunden werden muss. Die Syntax des Befehls ist sehr einfach:

```
Convert-VHD -Path <Pfad zur VHD(X)-Datei> -DestinationPath <Pfad zur Zieldatei>
```

Eine weitere Option ist die Möglichkeit, den Typ der Festplatte zu ändern, zum Beispiel mit:

```
Convert-VHD -Path <Pfad der VHD/VHDX-Datei> -DestinationPath <Zielpfad und Datei> -VHDType
Differencing -ParentPath <Übergeordnete Festplatte>
```

Ein weiteres Beispiel ist:

```
Convert-VHD -Path hd1.vhd -DestinationPath hd1.vhdx -VHDType Dynamic
```

Alle Optionen des Cmdlets finden Sie auf der Seite *http://technet.microsoft.com/en-us/library/hh848454.asp* [Ms179-K05-06]. Neben der Möglichkeit, das Format von Festplatten in der PowerShell umzuwandeln, können Sie auch die Größe von Festplatten in der PowerShell anpassen. Dabei hilft das Cmdlet *Resize-VHD*, zum Beispiel durch den folgenden Aufruf:

```
Resize-VHD -Path c:\vm\owa.vhdx -SizeBytes 1TB
```

Neben diesen Spezialaufgaben können Sie auch einfach mit *New-VHD* neue Festplatten erstellen und mit *Get-VHD* Informationen zu den Festplatten abrufen. Virtuelle Festplatten lassen sich in der PowerShell auch direkt mit virtuellen Servern verbinden:

```
Add-VMHardDiskDrive -VMName <VM> -Path <VHDX-Datei>
```

Natürlich können Sie virtuelle Festplatten auch direkt an den Host anbinden, um beispielsweise Daten auf die virtuelle Platte zu kopieren und diese erst dann dem virtuellen Server anzubinden:

```
Mount-VHD <VHD-Datei>
```

Mit dem Cmdlet *unmount-vhd* trennen Sie die virtuelle Platte wieder vom System.

Microsoft unterstützt Administratoren mit dem kostenlosen Microsoft Virtual Machine Converter (*http://www.microsoft.com/en-us/download/details.aspx?id=34591* [Ms179-K05-07]), um virtuelle Server von VMware vSphere zu Hyper-V zu migrieren. Die aktuelle Version wurde von Microsoft bereits für Windows Server 2012 R2 und Hyper-V Server 2012 R2 optimiert, unterstützt aber noch nicht das neue Festplatten-Format VHDX von Windows Server 2012 R2.

Sie können aber im Hyper-V-Manager oder mit dem Cmdlet *Convert-VHD* die erstellte VHD-Datei in eine VHDX-Festplatte umwandeln. SCVMM 2012 kann mit dem SP1 VHDX-Festplatten von Hyper-V 3.0 und auch VHD-Dateien in das VHDX-Format konvertieren

VHD-Dateien in den Boot-Manager einbinden

Sie können VHD(X)-Dateien, die Sie in Windows Server 2008 R2/2012/2012 R2 oder Windows 7/8/8.1 erstellt haben, bootfähig machen. Dazu müssen Sie lediglich eine solche virtuelle Festplatte erstellen und diese im Boot-Manager eintragen. Stellen Sie sicher, dass sich die VHD(X)-Datei direkt im Stammordner von C: befindet und Sie die Festplatte mit dem System verbunden haben. Mehr zu diesem Thema finden Sie in Kapitel 2. Haben Sie bereits eine VHD(X)-Datei mit einem installierten Betriebssystem vorliegen, binden Sie diese über die Eingabeaufforderung in den Boot-Manager ein.

Das funktioniert auch für Windows 8/Windows Server 2012 R2 und VHD(X)-Dateien aus Windows 7 oder Windows Server 2008 R2, die Sie gesichert oder kopiert haben. Liegt Ihnen eine solche Datei vor, gehen Sie folgendermaßen vor. Wir zeigen Ihnen am folgenden Beispiel, wie Sie eine virtuelle Windows 7-Installation mit dem Boot-Manager an einen Server mit Windows Server 2012 R2 ankoppeln. Das funktioniert auf dem gleichen Weg auch für Windows 8/Windows Server 2012 R2.

Öffnen Sie eine Eingabeaufforderung mit Administratorrechten und geben Sie folgende Befehle ein:

```
diskpart
select vdisk file=c:\win7.vhd
attach vdisk
```

Zur Anbindung an das Bootmenü verwenden Sie das Verwaltungstool Bcdedit, das Sie über die Eingabeaufforderung steuern. Bevor Sie jedoch Änderungen am Bootspeicher vornehmen, sollten Sie diesen über die Option */export* sichern (siehe Kapitel 2), zum Beispiel mit dem Befehl:

```
bcdedit /export c:\backup-bootmgr
```

Anschließend können Sie den Bootspeicher bearbeiten:

Der erste Befehl kopiert dazu den Eintrag einer bestehenden Installation und fügt dem Boot-Manager einen neuen Eintrag hinzu:

```
bcdedit /copy {current} /d "Booten von VHD"
```

Diesen neuen Eintrag bearbeiten Sie als Nächstes. Als Bezeichner-ID verwenden Sie die Daten, die der erste Befehl ausgibt, also die ID des neuen Eintrags im Boot-Manager. Öffnen Sie oben links in der Titelleiste der Eingabeaufforderung das Systemmenü, können Sie mit *Bearbeiten/Markieren* die GUID des Eintrags in die Zwischenablage kopieren, inklusive der geschweiften Klammern. Markieren Sie dazu den Eintrag und drücken Sie die ↵-Taste.

Abbildg. 5.53 Kopieren eines vorhandenen Booteintrags für einen neuen Eintrag

```
C:\Windows\system32>bcdedit /copy {current} /d "Windows 7 Video2Brain"
Der Eintrag wurde erfolgreich in {0ff3cb99-e79e-11e1-bc23-eaad308a9f56} kopiert.
```

Im Anschluss verbinden Sie den neuen Eintrag im Boot-Manager mit der vorhandenen VHD(X)-Datei:

```
bcdedit /set <Bezeichner-ID> osdevice vhd=[C:]\<Datei>.vhd
bcdedit /set <Bezeichner-ID> device vhd=[C:]\< Datei>.vhd
```

Abbildg. 5.54 Bearbeiten des Boot-Managers von Windows Server 2012 für die Unterstützung von VHD-Dateien

```
C:\Windows\system32>bcdedit /set {0ff3cb99-e79e-11e1-bc23-eaad308a9f56} osdevice
 vhd=[c:]\win7.vhd
Der Vorgang wurde erfolgreich beendet.

C:\Windows\system32>bcdedit /set {0ff3cb99-e79e-11e1-bc23-eaad308a9f56} device v
hd=[c:]\win7.vhd
Der Vorgang wurde erfolgreich beendet.
```

Starten Sie den Computer, sehen Sie den neuen Eintrag im Bootmenü. Dieser Eintrag bootet dann von der virtuellen Festplatte. Wie Sie die Reihenfolge anpassen, sehen Sie im Kapitel 2 und 3. Über Msconfig können Sie den Eintrag bearbeiten.

iSCSI-Ziele über virtuelle Festplatten zur Verfügung stellen

Windows Server 2012 R2 kann nicht nur auf iSCSI-Ziele zugreifen, sondern kann auch selbst virtuelle Festplatten als iSCSI-Ziel im Netzwerk zur Verfügung stellen.

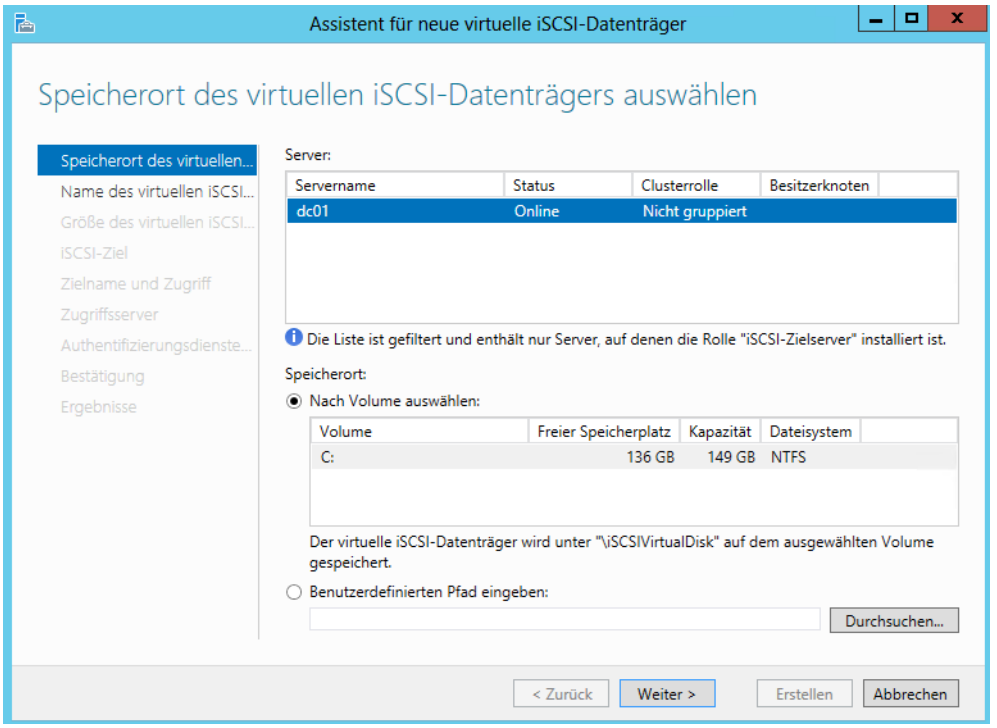
HINWEIS Im Gegensatz zu Windows Server 2012 können Sie in Windows Server 2012 R2 auch VHDX-Dateien als iSCSI-Ziel zur Verfügung stellen. Hier erhalten Sie die gleichen Vorteile wie beim Einsatz von VHDX-Dateien in Hyper-V. Die Dateien sind stabiler und erlauben eine Größe von bis zu 64 TB.

Neben der Unterstützung von VHDX-Dateien gibt es in Windows Server 2012 R2 weitere Neuerungen in den iSCSI-Zielen. In der neuen Version können Sie auch iSCSI-Initiatoren von Drittherstellern verwenden, nicht nur Windows-Server.

Dazu müssen Sie über den Server-Manager mit *Verwalten/Rollen und Features hinzufügen* den Rollendienst *iSCSI-Zielserver* über *Datei- und Speicherdienste/Datei- und iSCSI-Dienste* installieren.

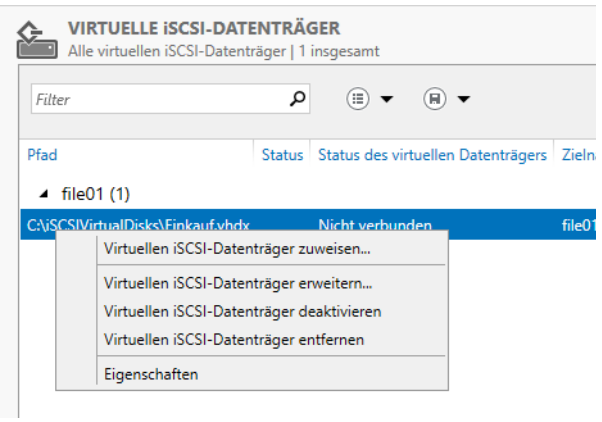
Nach der Installation des Rollendiensts können Sie über den Server-Manager und der Auswahl von *Datei-/Speicherdienste/iSCSI* virtuelle Festplatten erstellen, die als iSCSI-Ziel im Netzwerk konfiguriert werden können.

Abbildg. 5.55 Erstellen von virtuellen iSCSI-Datenträgern



Sie können über den Assistenten, wie überall im Server-Manager, auch auf anderen Servern im Netzwerk virtuelle iSCSI-Ziele erstellen. Damit das funktioniert, muss auf dem entsprechenden Server der Rollendienst *iSCSI-Zielserver* installiert sein.

Abbildg. 5.56 Verwalten virtueller iSCSI-Datenträger



Im Rahmen der Einrichtung legen Sie die Größe und den Speicherort der VHD(X)-Datei fest. Außerdem können Sie über den Assistenten steuern, welche Server im Netzwerk auf das iSCSI-Ziel zugreifen dürfen. Mit einem iSCSI-Ziel können Sie auch mehrere virtuelle iSCSI-Festplatten zur Verfügung stellen. Nachdem Sie die virtuellen Festplatten erstellt haben, können Sie über das Kontextmenü die Einstellungen ändern.

iSCSI-Festplatten verbinden

In Windows Server 2012 R2 können Sie über den iSCSI-Initiator virtuelle iSCSI-Festplatten von anderen Servern mit Windows Server 2012 R2 verbinden, aber auch iSCSI-Ziele von anderen NAS-Systemen. Dazu gehen Sie folgendermaßen vor:

Die Verbindung müssen Sie zum Beispiel im Rahmen der Clustereinrichtung vornehmen. Dazu verwenden Sie den iSCSI-Initiator, der zu den Bordmitteln von Windows Server 2012 R2 gehört. Suchen Sie nach *iscsi* im Startbildschirm und starten Sie das Tool.

Beim ersten Aufruf dieser Software müssen Sie den Start des entsprechenden Diensts zunächst bestätigen und die Blockierung aufheben. Anschließend können Sie den Dienst über mehrere Registerkarten konfigurieren. Die Anbindung ist in Windows Server 2008 R2 und Windows Server 2012 identisch. Gehen Sie zur Anbindung folgendermaßen vor:

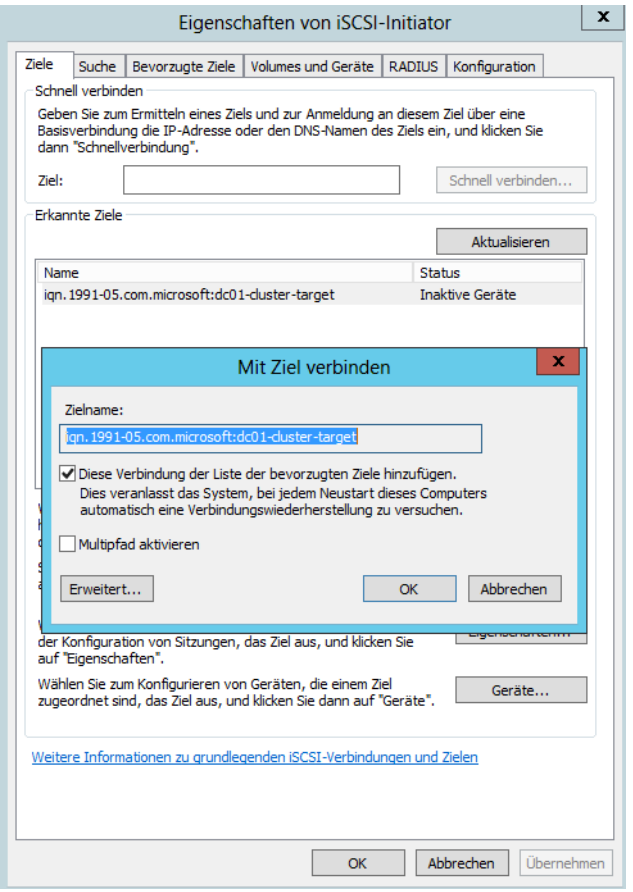
1. Wechseln Sie zur Registerkarte *Suche*.
2. Klicken Sie auf *Portal ermitteln* und geben Sie die IP-Adresse oder den Namen des NAS-Servers ein.
3. Wechseln Sie zur Registerkarte *Ziele*. Hier zeigt Windows die erstellten Laufwerke an. Sie sehen hier auch bei Windows Server 2012 R2-iSCSI-Zielen die erstellten Targets.
4. Klicken Sie auf die Schaltfläche *Verbinden*. Damit baut der Server eine Verbindung mit dem Gerät auf. Bisher ist das Gerät nur verfügbar, aber noch nicht mit dem Computer verbunden.
5. Aktivieren Sie das Kontrollkästchen *Diese Verbindung der Liste der bevorzugten Ziele hinzufügen*. Diese Option muss für alle Laufwerke separat eingestellt sein.
6. Bestätigen Sie alle Fenster mit *OK*.
7. Wenn Sie einen Cluster mit iSCSI erstellen, verbinden Sie das Target auch auf dem zweiten Server und allen weiteren Clusterknoten, auf denen Sie einen Cluster installieren wollen.

Mit *Multipfad aktivieren* können Sie festlegen, dass Windows Server 2012 R2 auch alternative Netzwerkwege zwischen Server und NAS-System verwendet. Das ist zum Beispiel bei der Ausfallsicherheit wichtig.

Nachdem Sie Targets verbunden haben, stehen in der Datenträgerverwaltung die mit diesem iSCSI-Ziel verbundenen Laufwerke zur Verfügung. Das funktioniert auf diesem Weg auch mit iSCSI-Zielen, die als virtuelle Festplatten auf Servern mit Windows Server 2012 R2 erstellt wurden.

Beim Einsatz auf Clustern müssen Sie zur Einrichtung weitere Punkte beachten. Nachdem die Laufwerke mit dem ersten Serverknoten verbunden wurden, müssen diese über die Festplattenverwaltung online geschaltet, initialisiert, partitioniert und formatiert werden.

Abbildg. 5.57 Konfigurieren von iSCSI-Targets



Belassen Sie die Datenträger als *Basis*, eine Umwandlung in dynamische Datenträger wird für den Einsatz im Cluster nicht empfohlen. 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 Onlineschalten und das Ändern der Laufwerkbuchstaben, die mit dem ersten Knoten übereinstimmen müssen.

Die Datenträgerverwaltung starten Sie durch Eingabe von *diskmgmt.msc* auf der Startseite von Windows Server 2012 R2. Über das Kontextmenü setzen Sie die iSCSI-Targets online, dann initialisieren Sie die Targets und als Letztes erstellen Sie ein Volume und formatieren dieses mit NTFS.

Festplatten testen und Speicherplatz freigeben

Administratoren kennen das Problem: Die Festplatte im Rechner macht Geräusche, der Server stürzt regelmäßig ab und unter Umständen lassen sich einige Daten nicht mehr lesen. Ein solches Problem kommt oft von einer defekten Festplatte. Aber auch wenn mit dem Datenträger alles in Ordnung ist, schadet es nicht, ab und zu die Festplatten im Computer zu testen. Festplatten verabschieden sich selten von einer Sekunde zur nächsten. Oft ist es ein schleichender Prozess. Erkennen Sie Probleme rechtzeitig, können Sie zumindest Ihre Daten retten und vielleicht sogar Windows auf eine neue Festplatte umziehen.

Datendeduplizierung einrichten

Bei der Datendeduplizierung in Windows Server 2012 R2 handelt es sich um eine Funktion, die doppelte Dateien auf den Dateiservern findet. Mit diesem Rollendienst in Windows Server 2012 R2 erkennen Dateiserver doppelt gespeicherte Dateien in den Freigaben und können diese bereinigen.

Auf diese Weise lässt sich die Datenmenge auf den Festplatten und Sicherungsmedien sowie die Dauer der Datensicherung teilweise deutlich reduzieren. Die Datendeduplizierung-Funktion untersucht die angeschlossenen Festplatten regelmäßig und zeigt die Deduplizierungsrate im Server-Manager auch an.

Installieren Sie den Rollendienst *Datendeduplizierung* über *Datei- und Speicherdienste/Datei- und iSCSI-Dienste*, integriert der Installations-Assistent auch ein Befehlszeilentool, mit dem Sie die doppelten Dateien suchen können, um abzuschätzen, ob der Rollendienst auf Ihren Dateiservern sinnvoll einsetzbar ist. Das Tool Ddpeval befindet sich im Ordner *\Windows\System32*. Sie können das Tool auch in Windows 7-, Windows Server 2008 R2- oder Windows 8/Windows Server 2012 R2-Systemen ausführen.

Ddpeval unterstützt lokale Laufwerke und Netzwerkfreigaben; die Syntax des Tools lautet *ddpeval <Volume:>*. Beispiele für die Ausführung sind *ddpeval e:* oder *ddpeval \\nas\daten*. Erst wenn das Tool doppelte Daten findet, ist es sinnvoll, die Datendeduplizierung zu verwenden. Das Tool selbst bereinigt keinerlei Dateien, sondern gibt nur an, ob die Datendeduplizierung auf dem Server sinnvoll ist.

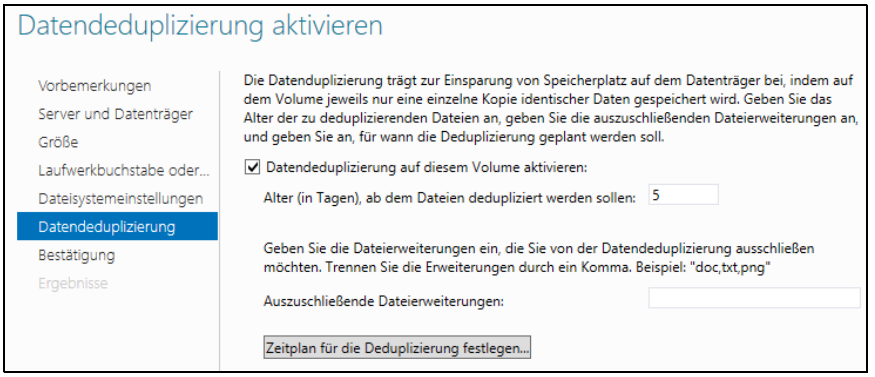
Anschließend aktivieren Sie die Datendeduplizierung auf dem entsprechenden Server. Sie können dazu entweder den Server-Manager verwenden und die Datendeduplizierung als Rollendienst installieren, oder Sie verwenden die PowerShell und das Cmdlet *Install-WindowsFeature –Name FS-Data-Deduplication*. Mit dem Cmdlet *Enable-DedupVolume <Laufwerk>* aktivieren Sie die Funktion auf einem Server. Konfigurieren können Sie die Funktion mit *Set-DedupVolume <Laufwerk> MinimumFileAgeDays <Alter>*.

HINWEIS Sie können Ddpeval nur für Laufwerke verwenden, für die Sie die Datendeduplizierung nicht aktiviert haben. Auch für System- oder Startvolumes können Sie das Tool nicht nutzen.

Die Verwaltung der Funktion nehmen Sie auch im Server-Manager vor. Dazu klicken Sie auf *Datei-/Speicherdienste* und dann mit der rechten Maustaste auf das Volume, für das Sie die Funktion aktivieren wollen. Nach der Auswahl von *Datendeduplizierung konfigurieren* richten Sie anschließend die Funktion über einen Assistenten ein. Für den Systemdatenträger können Sie die Datendeduplizierung nicht verwenden.

Die Datendeduplizierung ist auch in Speicherpools und virtuellen Festplatten möglich. Haben Sie den Rollendienst installiert, erscheint beim Anlegen neuer Volumes ein Fenster, über das Sie die Funktion für das entsprechende Volume aktivieren können. Es spielt keine Rolle, ob Sie mit der Datendeduplizierung Daten auf normalen Volumes oder virtuellen Datenträgern in Speicherpools suchen.

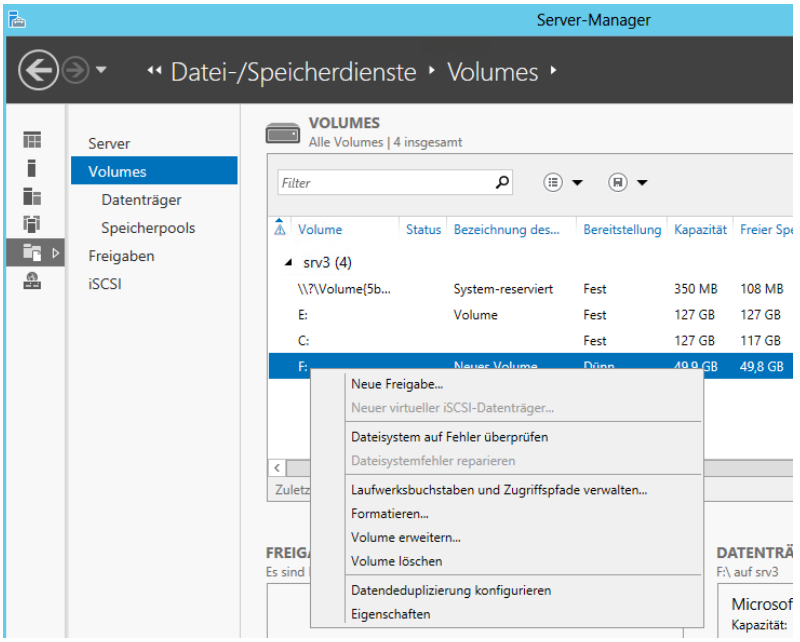
Abbildg. 5.58 Aktivieren der Datendeduplizierung



Datendeduplizierung im Server-Manager

Um die Datendeduplizierung zu verwenden, installieren Sie zunächst den bereits erwähnten Rollendienst. Anschließend überprüfen Sie mit Ddpeval, ob sich die Aktivierung für Laufwerke lohnt. Wenn Sie ein positives Ergebnis erhalten, aktivieren Sie die Datendeduplizierung im Server-Manager. Klicken Sie auf *Datei-/Speicherdienste* und dann auf *Volumes*.

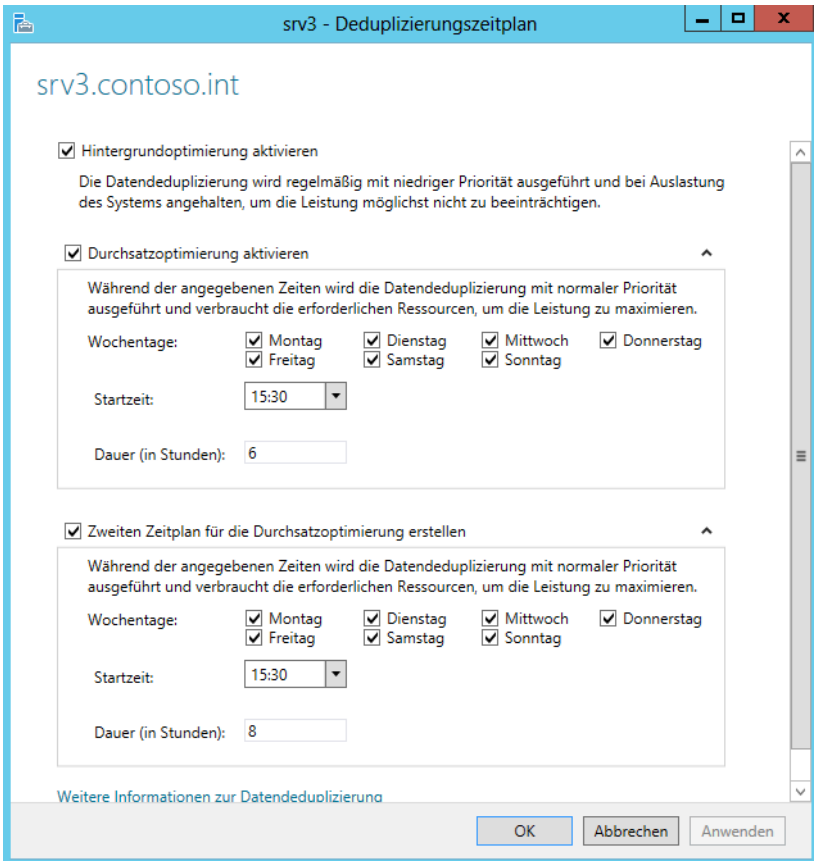
Abbildg. 5.59 Konfigurieren von Volumes und der Datendeduplizierung



Im Fenster sehen Sie alle Laufwerke, die auf dem Server angelegt sind. Über das Kontextmenü von Volumes starten Sie die Einrichtung der Datendeduplizierung.

Im neuen Fenster aktivieren Sie zunächst die Datendeduplizierung. Außerdem legen Sie das Alter fest, ab dem der Dienst Dateien als dupliziert speichern soll. Im Fenster können Sie auch Dateierweiterungen von der Suche ausschließen. Außerdem können Sie in diesem Fenster die Optimierung des Servers über Zeitpläne steuern.

Abbildg. 5.60 Konfigurieren der Datendeduplizierung im Server-Manager und festlegen eines Zeitplans



Sie können eine sofortige Durchführung der Deduplizierung mit dem folgenden Befehl starten:

```
Start-DedupJob –Volume <Laufwerkbuchstabe> –Type Optimization
```

Wollen Sie auf eine Rückgabe der Suche warten, verwenden Sie den folgenden Befehl:

```
Start-DedupJob <Laufwerkbuchstabe> –Type Optimization –Wait
```

Den aktuellen Zustand des Auftrags zeigen Sie mit *Get-DedupJob* an.

Den aktuellen Zustand der Duplizierung von Daten lassen Sie sich mit *Get-DedupStatus* anzeigen. Mehr Informationen erhalten Sie mit *Get-DedupStatus |fl*. Weitere Informationen erhalten Sie mit *Get-DedupVolume*.

Festplatten testen – SMART & Co.

Je älter eine Festplatte ist, umso höher ist auch die Gefahr, dass die Festplatte defekte Sektoren aufweist. Das bemerken Sie meist erst dann, wenn es zu spät ist und der Computer nicht mehr funktioniert. Sie sollten daher Festplatten regelmäßig auf Fehler prüfen. In Festplatten ist dazu SMART (Self-Monitoring, Analysis and Reporting Technology) integriert. Diese Funktion überwacht die Festplatte auf Fehler. Sie können den aktuellen SMART-Zustand mit Zusatztools auslesen und anzeigen.

Ein sehr interessantes Tool ist die Freeware HDDScan von der Seite *http://hddscan.com* [Ms179-K05-08]. Die Freeware kann Festplatten auf Fehler scannen. Der Vorteil dieses Tools ist, dass Sie es nicht installieren müssen und daher auch auf USB-Sticks verwenden können, um Rechner schnell und unkompliziert auf Fehler zu scannen. Sie können die Oberfläche von Festplatten testen lassen und die SMART-Informationen auslesen.

Abbildg. 5.61 Festplattenfehler genauer untersuchen und Fehler beheben

Wählen Sie dazu zunächst die entsprechende Festplatte aus und klicken Sie dann auf die Schaltfläche in der Mitte. Anschließend können Sie einen Test starten, der im unteren Bereich angezeigt wird. Klicken Sie doppelt auf einen Test, den Sie gerade ausführen, sehen Sie den aktuellen Status. Findet die Software einen Fehler, können Sie diesen auch in einer Suchmaschine eingeben und erhalten meist Hinweise, woran das Problem liegt, sowie eventuelle Anleitungen zur Behebung des Fehlers.

Vermuten Sie einen Fehler auf der Festplatte, zum Beispiel wegen klickender Geräusche und Einträgen in der Windows-Ereignisanzeige (*Windows-Protokolle/System*), sollten Sie im ersten Schritt die Sektoren der Festplatte sowie die Zuordnungen des Dateisystems testen. Die Ereignisanzeige starten Sie am schnellsten durch Eingabe von *eventvwr* auf der Startseite.

Geben Sie in der Eingabeaufforderung mit Administratorrechten *chkdsk /f /r* ein. Wollen Sie die Systemfestplatte testen, müssen Sie nach der Eingabe des Befehls den Computer neu starten. Findet der Chkdsk-Befehl Fehler und behebt diese, sollten Sie schnellstmöglich alle Daten Ihres Systems auf einen anderen Datenträger sichern und die defekte Festplatte ersetzen. Außerdem sind weitere Tests mit den folgenden Tools sinnvoll, um das Ausmaß des Fehlers zu erkennen.

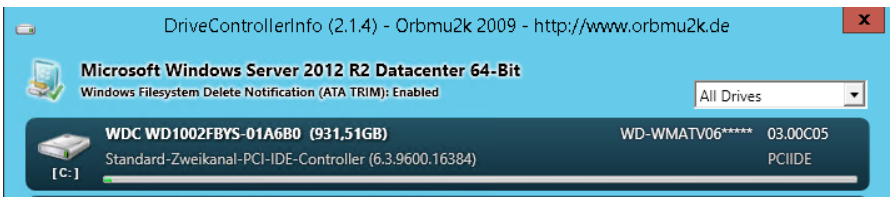
Weiterführende Tests von Festplatten nehmen Sie zum Beispiel mit der Freeware SeaTools von Seagate vor. Das Tool testet die meisten Festplatten auf Fehler, nicht nur die von Seagate selbst hergestellten. Ein sehr ausführliches Handbuch erhalten Sie über den Link *http://www.seagate.com/staticfiles/support/seatools/user%20guides/SeaTools_for_Windows.DE.pdf* [Ms179-K05-09]. Sie finden die SeaTools und weitere Informationen zum Retten von Festplatten auf der Seite *http://www.seagate.com/www/de-de/support/downloads/seatools* [Ms179-K05-10].

Western Digital bietet mit Data LifeGuard von der Seite *http://support.wdc.com/product/download.asp?lang=de* [Ms179-K05-11] ebenfalls ein solches Tool an, das auch als Windows-Anwendung zur Verfügung steht. Nach dem Start liest Data LifeGuard die Festplatten des Systems ein. Über das Kontextmenü der einzelnen Festplatten starten Sie die Tests.

Hitachi stellt seinen Drive Fitness Test als ISO-Datei auf der Seite *http://www.hgst.com/support/index-files/simpletech-legacy-downloads#DFT* [Ms179-K05-12] zur Verfügung. Brennen Sie die Tools als Image auf einen Datenträger und booten mit diesem den Computer. Mit Drive Fitness Test können Sie auch Festplatten anderer Hersteller auf Fehler überprüfen.

Ein weiteres wichtiges Tool, welches Ihnen genau anzeigt, welche Festplatte sich an welchem Controller befindet, ist DriveControllerInfo von der Seite *http://download.orbmu2k.de/download.php?id=48* [Ms179-K05-13]. Sie müssen das Tool nicht installieren, sondern können es direkt starten. Nach dem Einlesen der Informationen sehen Sie die wichtigsten Angaben zu den Laufwerken und den geladenen Treibern. Für das Tool müssen Sie das Feature *.NET Framework 3.5* installieren.

Abbildg. 5.62 Anzeigen und auslesen von Festplattendaten mit DriveControllerInfo



Festplattenplatz freigeben

In der jüngsten Vergangenheit wurde erstmalig Speicherplatz nicht mehr günstiger, sondern stieg im Preis an. Aus diesem Grund überprüfen immer mehr Anwender ihre Datenspeicher auf doppelt vorhandene Dateien und Datenmüll, der unnötig Speicherplatz und damit auch finanzielle Mittel bindet. Mit teilweise kostenlosen Tools lassen sich Dubletten und ungewöhnlich große Dateien recht zuverlässig finden und Speicherplatz freigeben.

Microsoft bietet aus der Sysinternals-Toolsammlung (*http://technet.microsoft.com/de-de/sysinternals* [Ms179-K05-14]) ebenfalls Programme an, die bei der Analyse helfen. Die Tools müssen nicht installiert werden und lassen sich auch in Skripts einbauen. Aber auch andere Anbieter stellen kostenlose Tools zur Verfügung.

Anwender, die große Datenmengen zu speichern haben, können mit dem Bereinigen von Datenträgern eine große Menge an Speicherplatz einsparen. Als Zusatzeffekt verringert sich auch der Platzbedarf von Datensicherungen und der Zeitraum, in dem die Sicherung abgeschlossen wird.

Speicheranalyse mit DiskView

Das Tool DiskView (*http://technet.microsoft.com/de-de/sysinternals/bb896650* [Ms179-K05-15]) zeigt zum Beispiel in einer grafischen Oberfläche die Dateien auf dem Datenträger an und wie viel Speicherplatz diese belegen.

Über das Textfeld *Highlight* wählen Sie Dateien aus, die DiskView hervorheben soll. Per Klick auf eine einzelne Datei ist zu sehen, wie viel Speicherplatz diese belegt. Per Doppelklick auf einen Bereich sind weitere Informationen zu sehen. Im unteren Bereich wählen Sie den vom Tool zu scannenden Datenträger sowie den Zoomlevel aus.

DiskView hilft auch dabei, die Fragmentierung einer Datei zu überprüfen. Mit dem Tool können Sie für Festplatten genau anzeigen lassen, auf welchem Cluster sich die ausgewählte Datei befindet. Die Ausgabe lässt sich auch exportieren. Das Tool ist hilfreich beim Auffinden von großen Dateien auf den Datenträgern, um Speicherplatzfresser zu eliminieren oder auf andere Datenträger auszulagern.

Zoomen Sie im unteren Bereich bis auf die einzelnen Cluster des Datenträgers, lässt sich per Klick auf einen Cluster anzeigen, welche Datei im entsprechenden Bereich gespeichert ist. Außerdem hebt DiskView alle weiteren Cluster hervor, in denen andere Teile der Datei ebenfalls gespeichert sind.

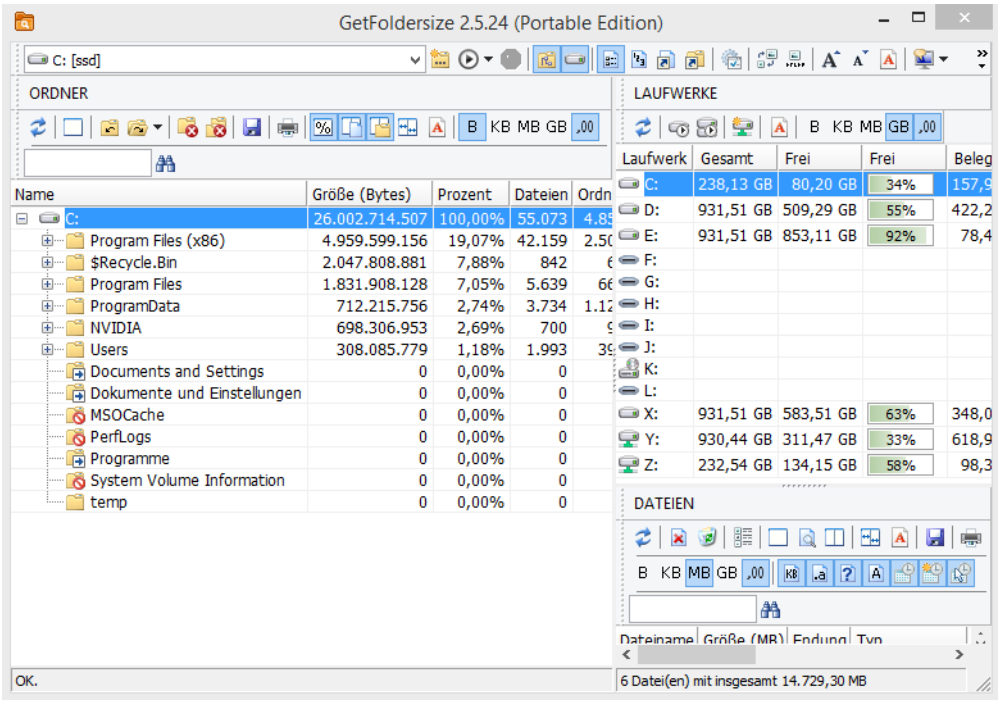
Speicheranalyse mit GetFoldersize

Die Freeware GetFoldersize (*http://www.getfoldersize.com/getfoldersize.htm* [Ms179-K05-16]) ist seit Jahren eines der bekanntesten Tools, um den Speicherverbrauch von Dateien und Ordnern auf verschiedenen Datenträgern zu analysieren. Der Anbieter stellt auch eine portable Version zur Verfügung. Nach dem Start listet das Tool zunächst alle verbundenen Datenträger auf und zeigt detaillierte Informationen zum freien beziehungsweise dem bereits belegten Speicherplatz an.

Über das Kontextmenü wählen Sie *Laufwerk einlesen* aus und erhalten auf der linken Seite eine Liste der Ordner und Dateien inklusive des verbrauchten Speicherplatzes angezeigt. Auf diesem Weg lässt sich sehr schnell feststellen, welche Ordner den meisten Speicherplatz belegen. Das Tool arbeitet auch problemlos mit Netzlaufwerken, was vor allem beim Einsatz von NAS-Systemen wichtig ist.

Vom gleichen Anbieter gibt es auch eine Freeware, um Dateidubletten zu finden. Das Tool AllDup (*http://www.alldup.de/download.htm* [Ms179-K05-17]) darf von Privatpersonen und von Unternehmen kostenlos eingesetzt werden. Das Tool erkennt auch ähnliche Fotos. In Kombination können Sie mit den beiden Tools GetFoldersize und AllDup effizient Speicherplatz auf dem Rechner freigeben.

Abbildg. 5.63 Speicherverbrauch von Laufwerken anzeigen



Filedup ist ein beliebtes Programm, um doppelte Dateien auch in kleinen Umgebungen zu finden (*http://www.h84.net/filedup.html* [Ms179-K05-18]). Das Tool kann Ordner oder ganze Festplatten auf doppelte Dateien durchsuchen. Filedup muss nicht installiert werden, sondern Sie können es direkt starten. Nach der Auswahl der Quelle analysiert Filedup den entsprechenden Ordner oder die ganze Festplatte und zeigt anschließend die doppelten Dateien an. Das Tool ist auch in großen Umgebungen für eine erste Analyse hilfreich, erfordert aber nach dem Scanvorgang einiges an Handarbeit.

Weitere kostenlose Tools in diesem Bereich sind DoubleKiller (*http://www.bigbangenterprises.de/de/doublekiller* [Ms179-K05-19]) und Anti-Twin (*http://www.aidex.de/software/antitwin* [Ms179-K05-29]).

Ähnlich wie GetfolderSize kann auch TreeSize (*http://www.jam-software.com/treesize_free* [Ms179-K05-16]) die Größe von Ordnern und Dateien analysieren und übersichtlich aufbereitet anzeigen. TreeSize zeigt nicht die einzelnen Dateien an, sondern nur die Ordner. Auch von diesem Tool gibt es eine portable Version. Die kostenlose Freeware-Version kann keine Netzlaufwerke untersuchen.

Wer eine grafisch ansprechende Analyse von Ordnern erhalten will, kann die Freeware SequoiaView (*http://w3.win.tue.nl/nl/onderzoek/onderzoek_informatica/visualization/sequoiaview* [Ms179-K05-21]) von der Technischen Universität Eindhoven verwenden. Im Gegensatz zu den anderen Tools in diesem Kapitel müssen Sie SequoiaView installieren.

Das Tool zeigt Blöcke der Dateien an. Je größer ein Block ist, umso größer ist auch die Datei. Für eine schnelle grafische Analyse ist SequoiaView ein sehr effizientes Werkzeug. Über den Menübereich lassen sich auch farbliche Unterscheidungen der verschiedenen Dateien aktivieren.

WinDirStat (*http://windirstat.info* [Ms179-K05-22]) ist ein Opensource-Tool, welches eine Analyse der Ordner bietet und eine ähnliche grafische Ansicht wie SequoiaView darstellt. WinDirStat ist bei vielen Anwendern sehr beliebt, da es umfangreiche Informationen liefert und durch die Opensource-Plattform auch weiter entwickelt wird. Das Tool muss installiert werden und erlaubt danach eine ausführliche Analyse von Ordnern und ganzen Partitionen.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Festplatten in Windows Server 2012 R2 verwalten und Laufwerke erstellen. Wir sind darauf eingegangen, wie Speicherpools und virtuelle Festplatten funktionieren und wie Sie das neue Dateisystem ReFS nutzen. Auch die Tools zur Analyse von Festplatten waren Thema dieses Kapitels.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie Windows Server 2012 R2 mit dem Netzwerk verbinden.

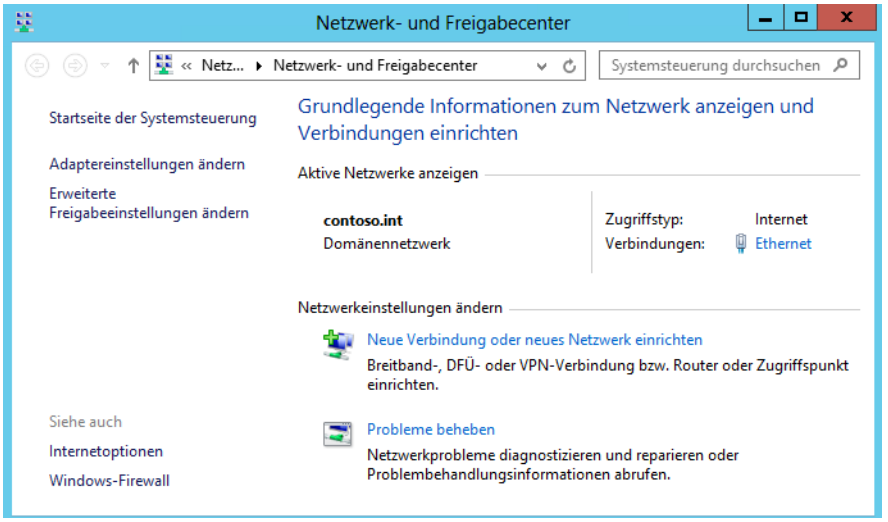
Kapitel 6

Windows Server 2012 R2 im Netzwerk betreiben

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen die Neuerungen und den Umgang mit Windows Server 2012 R2 im Netzwerk. Wir gehen auch darauf ein, wie Sie Windows Server 2012 R2 im Netzwerk betreiben. Außerdem erläutern wir, wie Sie einen Windows Server 2012 R2-Server mit Active Directory unter Windows Server 2012 R2 verbinden.

Abbildg. 6.1 Windows Server 2012 R2 über das Netzwerk- und Freigabecenter an das Netzwerk anbinden



Grundlagen der Netzwerkanbindung

Die Steuerung des Netzwerkverkehrs findet weiterhin über das Netzwerk- und Freigabecenter statt. Ist Ihr Server korrekt mit dem Netzwerk verbunden, zeigt Windows ein entsprechendes Symbol in der Taskleiste an. Klicken Sie auf das Symbol, zeigt Windows weitere Informationen an. Fahren Sie mit der Maus über das Symbol, zeigt Windows auch an, ob der Server über eine Internetverbindung verfügt. Bei fehlender Internetverbindung erscheint ein Ausrufezeichen, bei fehlender physischer Netzwerkverbindung ein rotes X.

Klicken Sie auf das Symbol, zeigt Windows alle gefundenen Netzwerke an. Mit Funknetzwerken verbinden Sie sich zum Beispiel, indem Sie das Netzwerk auswählen und auf *Verbinden* klicken. In Windows Server 2012 R2 müssen Sie dazu aber das Feature *WLAN-Dienst* installieren (siehe die Kapitel 2 bis 4).

Installieren der Netzwerkhardware

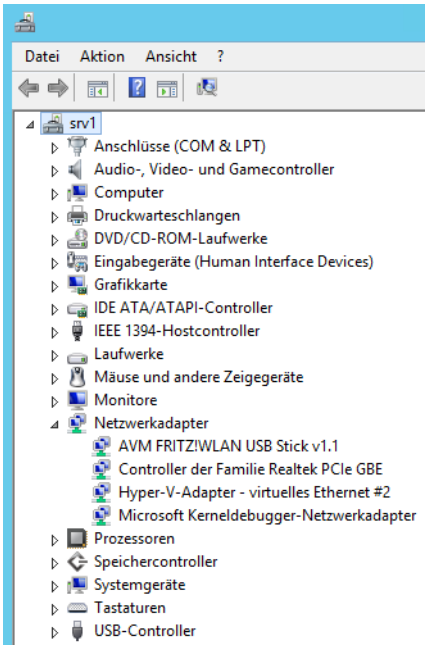
Die erste Voraussetzung, um einen Server mit dem Netzwerk zu verbinden, ist zunächst, dass die Netzwerkkarte im Geräte-Manager erkannt und installiert ist. Sollte der Treiber Ihrer Netzwerkkarte nicht ordnungsgemäß installiert sein, ist in Windows Server 2012 R2 wahrscheinlich kein Treiber für die Netzwerkkarte integriert.

Sie sollten allerdings nicht einfach einen alten Treiber installieren, sondern auf der Homepage des Herstellers überprüfen, ob es einen aktuellen Windows Server 2012 R2-Treiber gibt, und diesen installieren. Finden Sie keinen Treiber, funktionieren oft auch Treiber für Windows Server 2008 R2 oder Windows Server 2012.

Den Geräte-Manager finden Sie in Windows Server 2012 R2 über *Systemsteuerung/System und Sicherheit/System* und dann auf der linken Seite des Fensters über den Link *Geräte-Manager*. Alternativ tippen Sie *devmgmt.msc* auf der Startseite ein oder verwenden die Tastenkombination [⊞]+[Pause]. Als weitere Möglichkeit rufen Sie, wie bei allen internen Verwaltungsprogrammen, das Schnellmenü mit [⊞]+[X] auf oder klicken mit der rechten Maustaste in die linke untere Ecke des Bildschirms.

Sollte Ihre Netzwerkkarte im Bereich *Andere Geräte* eingetragen sein, wurde sie nicht erkannt, und Sie müssen den Treiber manuell installieren. Wird die Karte im Bereich *Netzwerkadapter* ohne Fehler angezeigt, wurde sie korrekt installiert.

Abbildg. 6.2 Überprüfen der installierten Hardware



Anbinden des Computers an das Netzwerk

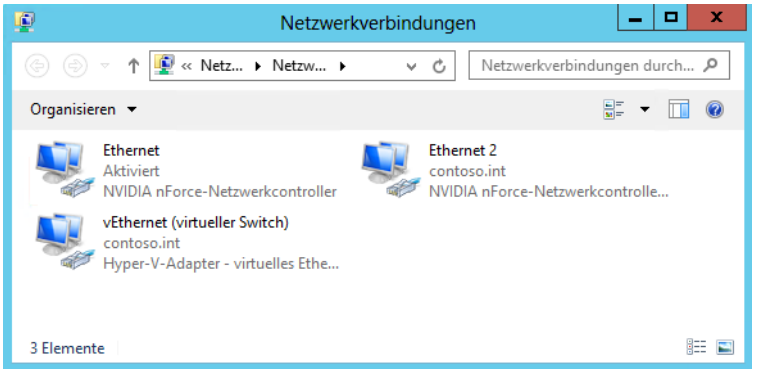
Ist die Karte ordnungsgemäß installiert und haben Sie Ihren Server an das Netzwerk mit einem DHCP-Server angeschlossen, ist der Server bereits mit einer dynamischen IP-Adresse versorgt. Hier müssen Sie keine besonderen Einstellungen vornehmen, da Windows Server 2012 R2 DHCP unterstützt, wie alle anderen Windows-Versionen vorher auch.

Die Anbindung ans Netzwerk stellen Sie am besten über das Netzwerk- und Freigabecenter her. Wenn Sie mit der rechten Maustaste auf das Netzwerksymbol in der Taskleiste neben der Uhr klicken, öffnet sich ein Kontextmenü, und Sie können das Netzwerk- und Freigabecenter öffnen.

Sie müssen zunächst die Netzwerkverbindung richtig konfigurieren. Klicken Sie dazu im Netzwerk- und Freigabecenter auf den Link *Adaptereinstellungen ändern* und rufen dann im neuen Fenster mit der rechten Maustaste die Eigenschaften Ihrer LAN-Verbindung auf. Es öffnet sich ein neues Fenster, in dem Sie die Eigenschaften der Netzwerkverbindung konfigurieren können. Sie können die Verwaltung der Netzwerkverbindungen auch über den Befehl *ncpa.cpl* starten, den Sie auf der Startseite eingeben.

Markieren Sie als Nächstes den Eintrag *Internetprotokoll Version 4*, und klicken Sie auf die Schaltfläche *Eigenschaften*. Hier können Sie jetzt eine ordnungsgemäße IP-Adresse vergeben. Haben Sie auf dem Server einen virtuellen Switch für Hyper-V erstellt, nehmen Sie die Einstellungen für die Netzwerkverbindung nicht bei der physischen Netzwerkkarte vor, sondern beim virtuellen Switch auf dem Server.

Abbildg. 6.3 Konfigurieren der Netzwerkeigenschaften beim Einsatz von virtuellen Switches



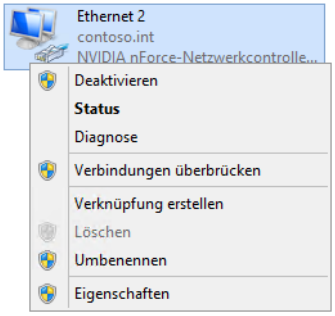
Erweiterte Verwaltung der Netzwerkverbindungen

Eine ausführliche Liste aller Netzwerkverbindungen auf dem Server erhalten Sie über den Link *Adaptereinstellungen ändern* im Netzwerk- und Freigabecenter. Nachdem Sie den Link angeklickt haben, öffnet sich ein Fenster, in dem alle Netzwerkverbindungen des Computers angezeigt werden sowie deren aktueller Verbindungsstatus. Das gleiche Fenster können Sie auch durch Eingabe von *ncpa.cpl* auf der Startseite aufrufen.

Ist eine Netzwerkverbindung aktiviert, kann aber keine Netzwerkverbindung herstellen, 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 in Windows.

Sie ändern die Bezeichnung von Netzwerkverbindungen über das Kontextmenü. Klicken Sie eine Netzwerkverbindung mit der rechten Maustaste an, stehen Ihnen verschiedene Möglichkeiten zur Verfügung, um die Einstellungen zu verwalten oder Informationen anzuzeigen.

Abbildg. 6.4 Verwalten von Netzwerkverbindungen



Im Kontextmenü stehen Ihnen folgende Optionen zur Verfügung:

- **Deaktivieren** Wenn Sie diese Option auswählen, wird die Verbindung zum Netzwerk getrennt, die Netzwerkkarte wird im Geräte-Manager deaktiviert. Die Karte verhält sich so, als wäre sie nicht installiert.
- **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. Sie erkennen, mit welcher Geschwindigkeit die Verbindung aufgebaut ist, wie lange die Netzwerkverbindung besteht und wie viele Datenpakete empfangen und gesendet worden sind. Klicken Sie auf die Schaltfläche *Details*, werden Ihnen ausführlichere Informationen über die Konfiguration der Netzwerkverbindung angezeigt. Sie erkennen die IP-Adresse, die MAC-Adresse sowie eine Vielzahl weiterer Informationen, die vor allem bei der Fehlersuche hilfreich sein können.
- **Diagnose** Startet einen Assistenten, der die Konfiguration des Adapters überprüft und Vorschläge zur Problemlösung unterbreitet.
- **Verbindungen überbrücken** Wenn Sie diese Option aus dem Kontextmenü einer Netzwerkverbindung auswählen, können Sie den Server als Verbindung zwischen zwei Netzwerken einsetzen. Dazu wird eine Netzwerkkarte mit einem 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 über den Server miteinander zu verbinden, müssen Sie zunächst die erste Verbindung auswählen, dann die Strg-Taste drücken und anschließend die zweite Verbindung auswählen. Wenn Sie dann im Kontextmenü die Option *Verbindungen überbrücken* auswählen, startet Windows Server 2012 R2 den Assistenten zum Aufbau einer Netzwerkbrücke.

Eigenschaften von Netzwerkverbindungen und erweiterte Verwaltung von Netzwerkverbindungen

Wenn Sie über das Kontextmenü einer Netzwerkverbindung die Eigenschaften aufrufen oder über den Status einer Netzwerkverbindung zur gleichen Konfiguration gelangen, können Sie das Verhalten der Netzwerkverbindung ausführlich konfigurieren.

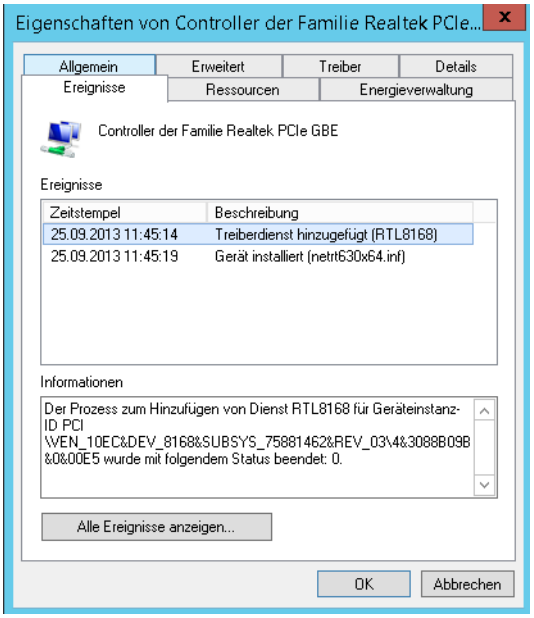
Über die Schaltfläche *Konfigurieren* können Sie die Einstellungen der Netzwerkkarte anpassen. Diese Einstellungen haben zunächst nichts mit den Netzwerkprotokollen zu tun, sondern ausschließlich mit dem Verhalten der Netzwerkkarte im Netzwerk. Die Registerkarte *Allgemein* ist zunächst weniger interessant, da hier nur einige wenige 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 oder gar nicht vorhanden.

Auf der Registerkarte *Energieverwaltung* können Sie konfigurieren, ob Windows 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. Der Dienst *QoS-Paketplaner (Quality Of Service)* in den Eigenschaften von Netzwerkverbindungen ist dafür zuständig, dass der Server 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 Server im Netzwerk verteilen, sorgt der QoS-Paketplaner dafür, dass eine minimale Anzahl an Bandbreite zur Verfügung bleibt.

Manche sogenannte Experten raten dazu, diesen Dienst zu deinstallieren, da er eine gewisse Bandbreite selbst verbraucht. Allerdings benötigen die wenigsten Anwender heutzutage wirklich jede kleine Menge Bandbreite, sondern profitieren besser davon, dass die Verbindung stabil bleibt. Wenn Sie das Gefühl haben, Ihr Server 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 testweise deaktivieren.

Neu in Windows Server 2012 R2 in den Eigenschaften von Geräten ist die Registerkarte *Ereignisse*. Hier sehen Sie für jedes Gerät, wann neue Treiber installiert wurden oder sonstige wichtige Ereignisse dieses Gerät betreffend eingetreten sind. Die Registerkarte ist auch ab Windows 8 verfügbar.

Abbildg. 6.5 Anzeigen von Ereignissen von Geräten



Netzwerk mit Jumbo Frames beschleunigen

Geht es um die Beschleunigung von Netzwerken, liest man oft von Jumbo Frames. Dabei handelt es sich um übergroße Netzwerkpakete (Frames). Jumbo Frames sind vor allem in sehr schnellen Netzwerken sinnvoll einsetzbar, bei der Datenübertragung in WAN-Leitungen oder in das Internet hingegen nur selten. Die größeren Datenpakete können schnelle Netzwerke noch schneller machen, aber langsame Netzwerke selten schneller.

Jumbo Frames im Überblick

Bei der Datenübertragung in Netzwerken werden die Daten zu Frames zusammen gefasst. Hierbei gibt es eine Standardgröße für das Netzwerk, die in den MTU-Einstellungen (Maximum Transmission Unit) der Netzwerkkarte und der Switches festgelegt sind. Der Standardwert beträgt normalerweise 1.518 Byte. Dieser ist über die Norm IEEE 802.3 festgelegt. Dieser Wert berücksichtigt die eigentliche Datenmenge des Netzwerkpakets, aber auch den Ethernetheader und die Frame Check Sequence (Blockprüfzeichenfolge). Daher verwenden IP-Netzwerke oft eine MTU von 1.500 Byte für den restlichen Datenverkehr, der Rest geht in den Overhead.

Erhöhen Sie im Netzwerk diese Größe, handelt es sich um Jumbo Frames, oft auch Giants genannt. Das Problem dabei ist, dass es keinen Standard für Jumbo Frames gibt und nicht alle Netzwerkgeräte, vor allem Switches, diese Funktion unterstützen. Jeder Hersteller verwendet eigene Standards bei der Aktivierung von Jumbo Frames.

Ein Interrupt ist eine kurze Unterbrechung der Datenübertragung. Diese Unterbrechung findet nach jedem Datenpaket im Netzwerk statt. Sind weniger Pakete im Netzwerk unterwegs, gibt es auch weniger Unterbrechungen. Das ist einer der Vorteile von Jumbo Frames.

Der Datenoverhead ist die Sammlung aller Daten, die notwendig sind, um die eigentlichen Netzwerkdaten zu verwalten. Dabei handelt es sich um Fehlerkorrekturen, TCP/IP-Header und die Ethernetprotokolle. Je weniger Pakete notwendig sind, umso geringer ist dieser Overhead. Dies ist ein weiterer Vorteil von Jumbo Frames.

Ändern Sie den maximalen Wert der Datenübertragung ab, beherrschen die Switches im Netzwerk den Standard aber nicht, bricht die Netzwerkverbindung zu den Geräten ab. Generell bricht die Verbindung beim Abändern dieses Werts ohnehin ab, wird nach der Umsetzung an der Netzwerkkarte aber wiederhergestellt. Das heißt, wenn Sie für Server im Netzwerk Jumbo Frames aktivieren, wird zunächst die Netzwerkverbindung eingestellt und dann wieder aufgebaut.

Kommt ein Jumbo Frame an einem Gerät an, das keine Jumbo Frames unterstützt, löscht es die Pakete. Das heißt, die Netzwerkleistung bricht ein, weil Pakete mehrmals gesendet werden müssen. Vor allem günstige Switches beherrschen den Standard nicht. Auf der Seite *http://www.nwlab.net/netzwerktechnik* [Ms179-K06-01] finden Sie verschiedene Geräte aufgelistet, die Jumbo Frames unterstützen. Wenn Sie Glück haben, finden Sie in der Datenbank Ihr Modell.

Auch wenn Switches Jumbo Frames unterstützen, sollten Sie überprüfen, welche maximale Datenmenge der Switch generell verwalten kann. Bei günstigen Geräten lassen sich zwar oft Jumbo Switches aktivieren, zumindest wenn die Geräte nicht älter als ein bis zwei Jahre sind. Allerdings sind die Ports an den günstigen Switches selten in der Lage, mit der großen Datenmenge zurecht zu kommen.

Wann Jumbo Frames sinnvoll sind

Viele Administratoren hoffen, ihr langsames Netzwerk mit Jumbo Frames beschleunigen zu können. Dies gelingt allerdings in den meisten Fällen nicht. Der Flaschenhals bei langsamen Netzwerken liegt sehr selten in der Paketgröße, sondern oft anderen Stellen.

Jumbo Frames ergeben vor allem in Netzwerken Sinn, in denen große Datenmengen übertragen werden und die bereits sehr schnell sind. Das können Dokumente, Multimediadateien, aber auch Datenbankdateien oder E-Mails sein. Viele Unternehmen verwenden Jumbo Frames auch bei der Datensicherung, da hier die Datenmenge besonders hoch und das Sicherungsfenster oft entsprechend klein ist. Durch die größeren Datenpakete müssen die Server auch geringere Header erzeugen, da weniger Pakete notwendig sind. Dadurch lassen sich Server, Netzwerkkarte und Betriebssystem wesentlich entlasten. Durch die Verwendung von Jumbo Frames entstehen weniger Interrupts und Protokolloverheads.

Unternehmen, die auf das Network File System (NFS) setzen, können von Jumbo Frames profitieren, da hier eine Segmentgröße von 8 KB im Einsatz ist. Dies ist zum Beispiel beim Einsatz von NAS-Geräten ein durchaus interessanter Vorteil. Wichtig ist aber, dass alle beteiligten Betriebssysteme, Netzwerkkarten, Switches und andere Geräte Jumbo Frames auch unterstützen. Manche Hersteller integrieren die Unterstützung für Jumbo Frames nur in spezielle Ports und auch nicht in allen Modellen. So geht zum Beispiel Cisco vor. Vor der Aktivierung sollten Sie also die Dokumentation Ihrer Switches durchlesen und unter Umständen Geräte an anderen Ports anschließen.

Außerdem sollte das Netzwerk bereits als Gbit-Netzwerk betrieben werden, noch besser als 10-Gbit/s-Netzwerk. Je schneller das Netzwerk ist, umso mehr lässt es sich von Jumbo Frames beschleunigen. Jumbo Frames ergeben in 100-Mbit/s-Netzwerken noch weniger Sinn als in Gbit-Netzwerken, bei denen die Geräte nicht kompatibel sind. Wollen Sie im Netzwerk eine höhere Geschwindigkeit erreichen, stellen Sie besser auf 1 Gbit/s. um, bevor Sie sich an die komplexe Konfiguration von Jumbo Frames und dem Lösen damit einhergehender Probleme machen.

Den Einsatz von Jumbo Frames sollten Sie prüfen, wenn Sie ein Gbit-Netzwerk im Einsatz haben (oder noch besser ein Netzwerk mit 10 Gbit/s), alle Switches sowie anderen Geräte Jumbo Frames unterstützen, und Sie große Datenmengen im Netzwerk hin- und her senden müssen. In diesem Fall haben Sie eine große Chance, ein schnelles Netzwerk noch schneller zu machen. Beachten Sie in diesem Fall aber auch die Nachteile, die wir nachfolgend beschreiben.

Wie bereits erwähnt, lassen sich mit dieser Tuningmaßnahme langsame Netzwerke nicht signifikant beschleunigen, dafür aber schnelle Netzwerke in noch schnellere Netzwerke verwandeln. Unternehmen, die NAS-Geräte im Netzwerk betreiben, und diese mit iSCSI anbinden, profitieren ebenfalls oft von Jumbo Frames. Allerdings muss auch hier das Gerät die Funktion unterstützen. Notieren Sie sich daher am besten für alle Geräte im Netzwerk, ob diese Jumbo Frames unterstützen und welche Größe maximalen Einsatz finden kann.

Linux, Datenbanken, Virtualisierung und Exchange mit Jumbo Frames

Viele Administratoren berichten auch von Leistungssteigerungen beim Einsatz von Jumbo Frames im Zusammenhang mit Datenbankservern. So lassen sich Datenbankspiegelungen und -sicherungen oft deutlich schneller durchführen. Anwendungen, die auf die Datenbank zugreifen müssen und ebenfalls Jumbo Frames unterstützen, profitieren dann ebenfalls von der höheren Leistung.

Auch beim Einsatz von Exchange mit Database Availability Groups (Datenbankverfügbarkeitsgruppen, DAG) in Exchange Server 2010/2013 lässt sich mit Jumbo Frames oft eine Leistungssteigerung erzielen. Dies gilt auch beim Einsatz von Livemigrationen oder Replikation in Hyper-V mit

Windows Server 2012 R2. Wollen Sie Jumbo Frames in virtuellen Servern nutzen, müssen Sie darauf achten, dass der virtuelle Switch und die Integrationsdienste dies unterstützen. Natürlich müssen die Integrationsdienste in den Servern auch installiert sein. Ab Version 3.3 der Integrationsdienste für Linux lassen sich Jumbo Frames nutzen.

Auch VMware unterstützt mit seinen verschiedenen Virtualisierungslösungen Jumbo Frames. Dazu müssen Sie lediglich die entsprechende Funktion für den entsprechenden virtuellen Switch aktivieren.

Nachteile von Jumbo Frames

Ob Jumbo Frames im Netzwerk einen Vorteil bringen, sollten Sie zunächst testen. Wenn ein Netzwerk bereits Leistungsprobleme hat, werden sich diese durch Jumbo Frames kaum beheben lassen. Das Erhöhen der maximalen Datenübertragung sollte immer der letzte Weg sein. Unterstützen einzelne Server, Anwendungen oder Netzwerkgeräte keine Jumbo Frames, bricht der Datenverkehr zusammen. Fast alle Treiber, Geräte und Anwendungen sind für Frames mit einer Größe von 1.518 Byte optimiert. Ändern Sie diesen Wert, betreiben Sie das Netzwerk außerhalb von Normen, was zu unvorhersehbaren Problemen führen sowie zu Schwierigkeiten beim Support führen kann.

Wenn Sie im Netzwerk neben der Datenübertragung noch Funktionen wie Voice over IP (VoIP) einsetzen, sollten Sie von der Verwendung von Jumbo Frames Abstand nehmen. Der Nachteil von Jumbo Frames ist die höhere Latenz der Datenpakete. Dabei handelt es sich um die Verzögerungszeit, bis ein Netzwerkpaket gepackt und anschließend verschickt wird. Durch die hohe Latenz leidet die Sprachqualität von VoIP-Geräten enorm. Die Latenz von Jumbo Frames mit einer Größe von 9.000 Byte beträgt etwa 70 ms, die Latenz in Netzwerken mit einer MTU von 1.500 beträgt um die 10 ms. Unter Umständen ist in diesem Fall eine leichte Erhöhung der Frames auf Größen um die 4.000 Byte sinnvoll. Hier müssen Sie einfach testen und die Nachteile gegen die Vorteile aufwiegen.

Das Gleiche gilt für Onlinespiele oder Onlineanwendungen. Da auch hier eine höhere Geschwindigkeit und geringere Latenz wichtiger ist als große Datenpakete, bringen Jumbo Frames mehr Nachteile als Vorteile. Dies gilt für den ganzen Datenverkehr ins Internet. Nur Netzwerkdaten profitieren von Jumbo Frames.

Was beim Aktivieren von Jumbo Frames beachtet werden muss

Aktivieren Sie Jumbo Frames im Netzwerk, sollten Sie zunächst sicherstellen, dass alle Geräte diesen Standard unterstützen. Teilweise müssen Sie Geräte im Netzwerk an andere Ports der Switches hängen und neue Treiber oder Firmware installieren. Es ist extrem wichtig, an allen Geräten die gleichen Einstellungen vorzunehmen. Das heißt, alle Netzwerkgeräte müssen die gleiche Datengröße für die Frames verwenden. Verwenden Sie dazu am besten den größten möglichen Wert zwischen den Geräten.

Nur in diesem Fall haben Sie die Chance, dass sich die Geschwindigkeit im Netzwerk erhöht. Beachten Sie, dass bei der Umstellung der Netzwerkverkehr zusammenbricht. Nehmen Sie daher die Einstellungen besser zu Zeiten vor, an denen keine Anwender mit dem Netzwerk arbeiten. Gelingt die Umstellung nicht, müssen Sie die geänderten Werte wieder auf die ursprünglichen Werte zurücksetzen. Auch dabei geht bei den Systemen die Netzwerkverbindung verloren.

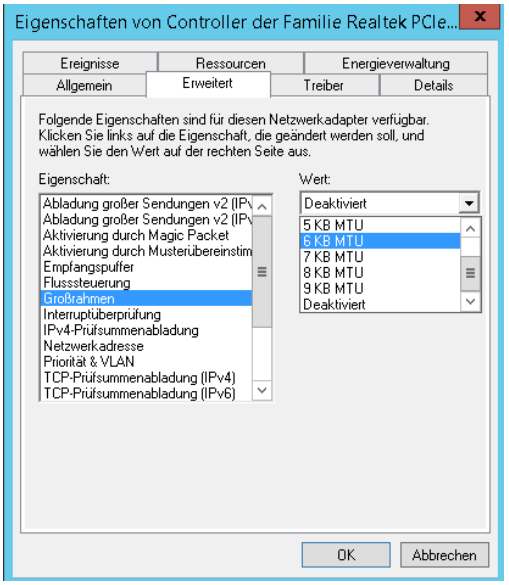
Nutzen Sie im Netzwerk zusätzlich andere Technologien wie WLAN oder PowerLine, können Sie Jumbo Frames normalerweise nicht einsetzen. Diese Technologien sind nicht dazu geeignet, größere Frames als den MTU-Standardwert von 1.518 zu verwalten. Sie können in diesem Fall zwar auch testen, aber selbst schnelle PowerLine und WLAN-Netzwerke kommen aktuell auf Werte bis zu maximal 500 Mbit/s. Selbst wenn alles ideal läuft, erhalten Sie in diesem Fall keine signifikanten Verbesserungen.

Jumbo Frames in der Praxis

Um Jumbo Frames zu aktivieren, sollten Sie auf allen Computern, auf denen Sie die Funktion nutzen wollen, den aktuellsten Treiber der Netzwerkkarte installieren. Überprüfen Sie in den Verwaltungsoberflächen der Switches, ob diese Jumbo Frames unterstützen und ob Sie diese Funktion zunächst aktivieren müssen. Schließen Sie die Computer, bei denen Sie Jumbo Frames nutzen wollen, an Ports an, welche die Funktion unterstützen.

Anschließend rufen Sie die Einstellungen der Netzwerkkarte auf. Das geht in Windows am schnellsten, wenn Sie das Programm *ncpa.cpl* starten. Rufen Sie danach die Einstellungen der Netzwerkkarte auf und wechseln Sie zur Registerkarte *Erweitert*. Suchen Sie nach Einstellungen wie Jumbo Frames, Großrahmen, Jumbo Packet oder Ähnliches. Aktivieren Sie hier den maximal möglichen Wert, der auf allen anderen Geräten und vor allem von den Switches unterstützt wird. Verwenden Sie auf jeden Fall exakt die gleiche Einstellung, also den größten gemeinsam möglichen Wert.

Abbildg. 6.6 Aktivieren von Jumbo Frames in den Einstellungen von Netzwerkkarten



Ist Ihnen nicht bekannt, ob der Router oder der Switch Jumbo Frames unterstützt, können Sie nach der Aktivierung mit dem kostenlosen Befehlszeilentool *mturoute.exe* (*http://www.elifulkerson.com/projects/mturoute.php* [Ms179-K06-02]) die MTU-Daten von Netzwerkgeräten auslesen.

Sinnvoll ist auch, wenn Sie entweder mit Netzwerkprogrammen vor und nach der Umstellung die Geschwindigkeit testen. Um schnelle Tests durchzuführen, kopieren Sie eine sehr große Datei vor der Umstellung und messen die Zeit. Kopieren Sie dann die gleiche Datei noch einmal über das Netzwerk. Beachten Sie aber, dass manche Systeme wie Windows Server 2012 R2 Dateien auch in einem Cache behalten. Das heißt, die zweite Datenübertragung kann auch dann schneller sein, wenn die Umstellung auf Jumbo Frames nicht erfolgreich war. Verwenden Sie daher am besten eine etwa gleich große andere Datei.

Testen Sie nach der Umstellung alle netzwerkabhängigen Anwendungen und deren Reaktionszeiten. Nicht alle Anwendungen unterstützen Jumbo Frames.

Daran, ob sich der Einsatz von Jumbo Frames lohnt, scheiden sich die Geister. Der Einsatz von Jumbo Frames lässt sich generell mit Einschränkungen empfehlen, wenn folgende Bedingungen im Netzwerk gegeben sind:

1. Das Netzwerk läuft bereits im 1-Gbit/s-Modus, besser im 10-Gbit/s-Modus.
2. Es werden oft und viele große Datenmengen und Dateien im Netzwerk übertragen.
3. Sie setzen kein WLAN, Powerline oder VoIP ein.
4. Es sind keine Onlinespiele oder -anwendungen im Einsatz.
5. Alle beteiligten Geräte unterstützen eine MTU von mindestens 9.000 Byte.

Falls nicht alle diese Punkte zutreffen, ist der Einsatz von Jumbo Frames nicht sinnvoll. Auch wenn Hard- und Software kompatibel sind, aber nur kleine Dateien übertragen werden, ergibt der Einsatz keinerlei Sinn. Treffen die Punkte aber zu, sollten Sie im Netzwerk einen Test wagen. In manchen Umgebungen besteht die Chance, die Geschwindigkeit des Netzwerks um fast 50 % zu erhöhen. Dies gelingt aber nur in idealen Umgebungen.

Netzwerkkarten zusammenfassen – NIC-Teaming

Windows Server 2012 R2 kann ohne Zusatzwerkzeug bis zu 32 kompatible Netzwerkkarten zu Teams zusammenfassen. Sie können während der Einrichtung auswählen, ob Sie einzelne Adapter im Team als Standby-Adapter nutzen wollen, also zur Ausfallsicherheit, oder ob Sie die Geschwindigkeit der Adapter zusammenfassen wollen, um die Leistung zu erhöhen. Sie können nur Ethernet-Verbindungen zu Teams zusammenfassen. Bluetooth oder WLAN gehören nicht zu den unterstützten Funktionen. Außerdem müssen alle Netzwerkkarten mit der gleichen Geschwindigkeit angeschlossen sein.

Eine physische Netzwerkkarte kann nur Mitglied in einem einzelnen Team sein, außerdem ist es nicht möglich, mehrere Teams zu einem gemeinsamen Team zusammenzufassen.

Sie können in allen Editionen von Windows Server 2012 R2 Netzwerk-Teams erstellen, auch in Core-Installationen. Die Verwaltung erfolgt im Server-Manager oder über die PowerShell. Die Einrichtung können Administratoren auch über das Netzwerk einrichten, auch von Windows 8-Computern aus.

Die Konfiguration dazu nehmen Sie direkt im Server-Manager vor. Damit das Teaming funktioniert, müssen Treiber und Hardware die Funktion unterstützten und die beteiligten Karten müssen mit dem Netzwerk verbunden sein.

HINWEIS Wenn Sie beabsichtigen, Netzwerkkarten auf einem Server zusammenzufassen, achten Sie darauf, dass die Karten mit identischer Geschwindigkeit betrieben werden.

Außerdem sollten Sie den Teamvorgang vor der Erstellung von virtuellen Switches in Hyper-V erstellen. Nach der Erstellung von virtuellen Switches ist die physische Netzwerkverbindung nicht mehr für den Teamvorgang verfügbar.

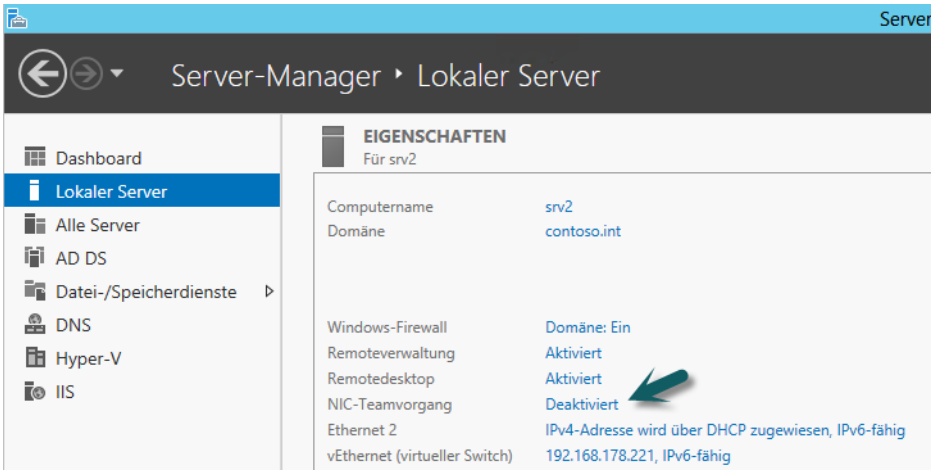
Sie dürfen die Teaming-Funktion in Windows Server 2012 R2 nicht mit Team-Funktionen von Drittherstellern kombinieren. Ansonsten besteht die Gefahr, dass der komplette Server nicht mehr funktioniert. Tritt ein solcher Fall ein, können Sie die internen Teamkonfigurationen löschen. Dazu verwenden Sie die PowerShell und geben den Befehl *Get-NetLbfoTeam | Remove-NetLbfoTeam* ein.

NIC-Team erstellen

Um ein NIC-Team zu erstellen, starten Sie den Server-Manager. Rufen Sie über die Startseite durch Eingabe von *ncpa.cpl* die Eigenschaften der Netzwerkverbindungen auf. Stellen Sie sicher, dass die Karten mit dem Netzwerk verbunden sind. Starten Sie danach den Server-Manager und klicken Sie auf *Lokaler Server*. Anschließend sehen Sie die Konfiguration des NIC-Teamings im Bereich *NIC-Teamvorgang*. Standardmäßig ist das Teaming deaktiviert. Um die Funktion zu aktivieren, klicken Sie auf den Link bei *Deaktiviert*.

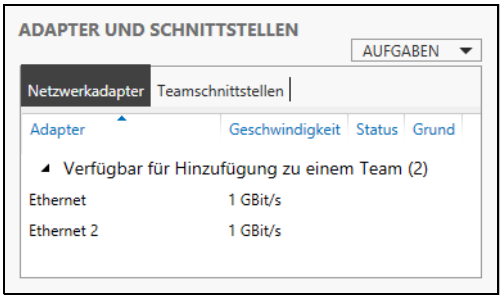
HINWEIS Sind Sie über eine der Netzwerkkarten mit dem Remotedesktop des Servers verbunden, werden Sie bei der Erstellung des Teams vom Server getrennt. Sie müssen zum Abschließen der Konfiguration eine andere Verbindung nutzen oder direkt am Server arbeiten.

Abbildg. 6.7 Starten des NIC-Teamvorgangs in Windows Server 2012 R2



Anschließend öffnet sich ein neues Fenster. Hier sehen Sie im unteren rechten Bereich, welche Netzwerkadapter im Server kompatibel zum NIC-Teaming sind.

Abbildg. 6.8 Anzeigen der kompatiblen Netzwerkkarten für das NIC-Teaming



TIPP Sie können in der PowerShell oder der Eingabeaufforderung auch das Tool Lbfo-Admin starten, um direkt zur Einrichtung von NIC-Teams zu gelangen. Das startet die Einrichtung des lokalen Servers.

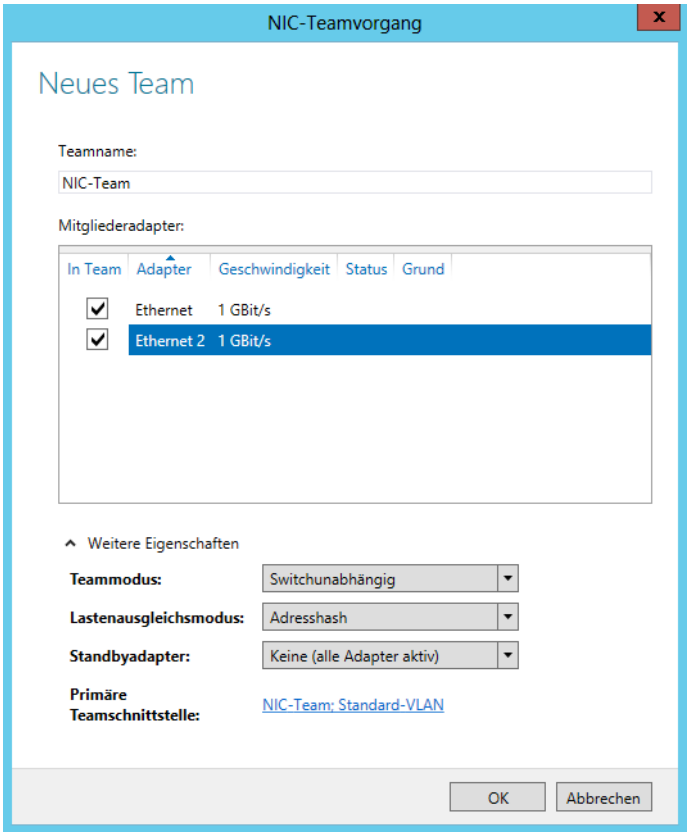
Verwenden Sie den Befehl *lbfoadmin /servers <Liste von Servern>*, starten Sie die Einrichtung auf mehreren Servern. Der Befehl *lbfoadmin /ResetConfig* stellt die Standardeinstellungen der Oberfläche wieder her.

Sie können ein NIC-Team im Server-Manager auch über das Netzwerk erstellen. Dazu klicken Sie den entsprechenden Server im Server-Manager mit der rechten Maustaste an. Im Kontextmenü finden Sie auch den Bereich zum Erstellen von neuen NIC-Teams.

Um ein Team zu erstellen, klicken Sie mit der rechten Maustaste in das Fenster bei *Adapter und Schnittstellen* und wählen *Zum neuen Team hinzufügen*. Anschließend geben Sie einen Namen für das Team ein und wählen aus, welche Netzwerkkarten verwendet werden sollen.

Über den Link *Weitere Eigenschaften* können Sie zusätzliche Einstellungen vornehmen, um das NIC-Team zu konfigurieren. Hier lässt sich zum Beispiel festlegen, dass nicht alle Adapter aktiv sein sollen, sondern ein Adapter als Standby zur Verfügung steht, wenn einer der Adapter ausfällt.

Abbildg. 6.9 Erstellen eines NIC-Teams



Bei *Teammodus* legen Sie fest, ob der Switch, an den die physischen Adapter des Teams angeschlossen sind, darüber informiert wird, dass es sich um ein Team handelt. Die Standardauswahl ist switchunabhängig, der Switch wird also nicht informiert.

Klicken Sie bei *Primäre Teamschnittstelle* auf das Team, können Sie Einstellungen bezüglich der VLAN-Anbindung des Teams anpassen. Bestätigen Sie schließlich mit *OK*, erstellt Windows Server 2012 R2 das entsprechende Team.

HINWEIS Windows Server 2012 R2 verwendet als MAC-Adresse des Teams die MAC-Adresse der primären Netzwerkkarte, also der Karte, mit der Sie das Team erstellt haben.

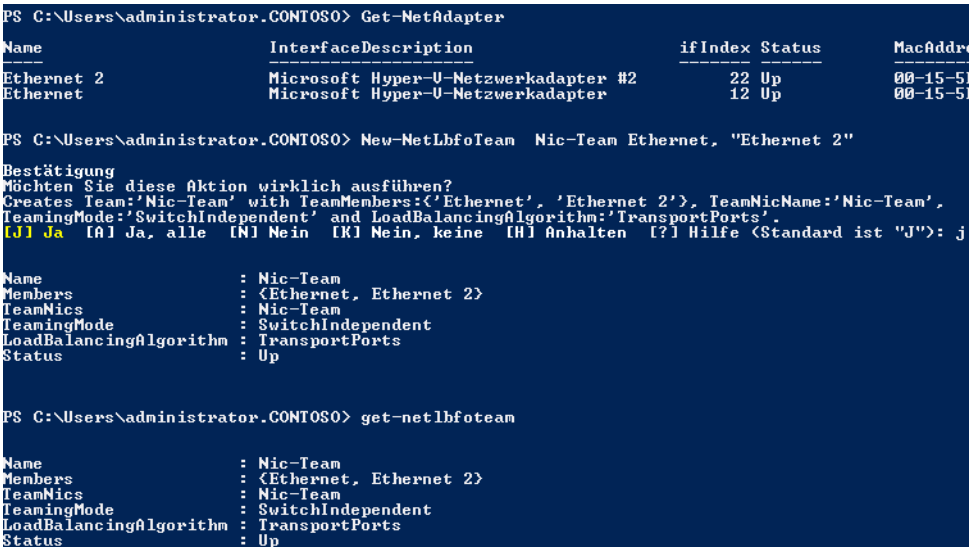
NIC-Teams auf Core-Server und in der PowerShell

Auch Core-Server unterstützen NIC-Teams. Hier können Sie die Einrichtung entweder über den Server-Manager von einem anderen Server aus durchführen, oder Sie verwenden die PowerShell.

In der PowerShell können Sie sich mit *Get-NetAdapter* die einzelnen möglichen Team-Adapter anzeigen lassen und mit *Enable-NetAdapter* beziehungsweise *Disable-NetAdapter* einzelne Adapter aktivieren oder deaktivieren. Alle Cmdlets für die Verwaltung von NIC-Teams lassen Sie sich mit *Get-Command –Module NetLbfo* anzeigen. Eine Hilfeseite lässt sich zum Beispiel mit *Get-Help New-NetLbfoTeam* öffnen.

Um ein neues Team zu erstellen, verwenden Sie das Cmdlet *New-NetLbfoTeam <Name des Teams> <Kommagetrennte Liste der Netzwerkkarten>*. Bei Leerzeichen im Namen setzen Sie den gesamten Namen in Anführungszeichen. Den Namen der Adapter erfahren Sie am schnellsten, wenn Sie *Get-NetAdapter* in der PowerShell eingeben. Haben Sie das Team erstellt, lassen Sie mit *Get-NetLbfoTeam* die Einstellungen anzeigen, und mit *Set-NetLbfoTeam* ändern Sie Einstellungen.

Abbildg. 6.10 Erstellen von NIC-Teams in der PowerShell



Beispiele für das Ändern sind folgende Befehle:

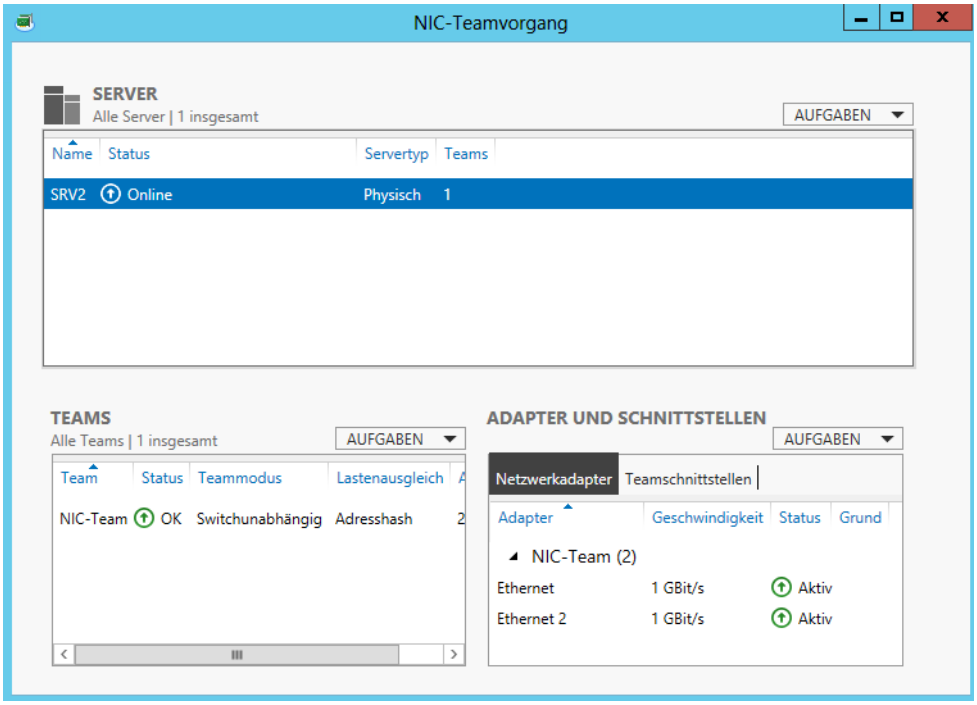
- *Set-NetLbfoTeam Team1 TeamingMode LACP*
- *Set-NetLbfoTeam Team1 TM LACP*
- *Set-NetLbfoTeam Team1 LoadBalancingAlgorithm HyperVPorts*
- *Set-NetLbfoTeam Team1 LBA HyperVPorts*

Teams können Sie auch umbenennen. Dazu verwenden Sie entweder den Server-Manager oder die PowerShell und den Befehl *Rename-NetLbfoTeam <Alter Name> <Neuer Name>*.

NIC-Teams testen und konfigurieren

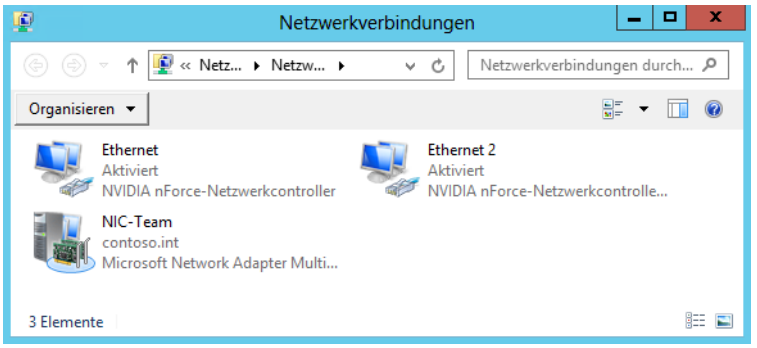
Sie müssen nach der Erstellung eines Teams noch Netzwerkeinstellungen anpassen. Windows Server 2012 R2 entfernt die IP-Bindung von den physischen Netzwerkkarten und verbindet Sie mit dem neuen virtuellen Adapter, den der Assistent für das Team erstellt. Sie sehen den Status des Teams, wenn Sie im Server-Manager in der Kategorie *Lokaler Server* bei *NIC-Teamvorgang* auf den Link *Aktiviert* klicken.

Abbildg. 6.11 Anzeigen des Status des NIC-Teamings



Werden das Team und die verbundenen Karten als *Aktiv* gekennzeichnet, passen Sie die Netzwerkeinstellungen des Teams an. Dazu rufen Sie die Adaptereinstellungen auf, indem Sie *ncpa.cpl* auf der Startseite eingeben. Hier sehen Sie das neue Team. Alle Netzwerkeinstellungen nehmen Sie an dieser Stelle vor.

Abbildg. 6.12 Windows Server 2012 legt für NIC-Teams eine neue Verbindung an



Haben Sie die IP-Konfiguration des NIC-Teams angepasst, verhält sich der Server wie beim Einsatz einer einzelnen Netzwerkverbindung, nutzt aber alle angebundenen Netzwerkkarten. Im Server-Manager können Sie das Team jederzeit über dessen Eigenschaften anpassen und auch löschen.

Einzelne Netzwerkadapter entfernen Sie über das Kontextmenü aus dem Team oder deaktivieren den Adapter, zum Beispiel für Wartungsarbeiten.

NIC-Teams und Hyper-V

Sobald Sie ein NIC-Team erstellen, verwenden Sie dieses in allen Bereichen von Windows Server 2012 R2 wie einen ganz normalen Adapter. Die physischen Netzwerkkarten nutzen Sie an dieser Stelle nicht mehr, da der interne Treiber für das Team den Datenverkehr steuert. In Hyper-V dürfen Sie keine NIC-Teams nutzen. Sie können zwar auch auf Hyper-V-Servern NIC-Teams erstellen, allerdings verliert der Server dann die Netzwerkverbindung.

Sie können aber auf Hyper-V-Hosts mehrere virtuelle Switches auf Basis der verschiedenen physischen Netzwerkkarten erstellen und innerhalb von virtuellen Servern dann NIC-Teams erstellen. Diese verwenden die einzelnen virtuellen Switches des Hyper-V-Hosts als Grundlage.

In den Eigenschaften eines NIC-Teams haben Sie die Möglichkeit, bei *Lastenausgleichsmodus* die Option auf *Hyper-V-Port* zu setzen. In diesem Fall kann Hyper-V besser die beteiligten MAC-Adressen der angeschlossenen physischen Netzwerkkarten verwalten und Datenverkehr zwischen virtuellen Computern, die ebenfalls eine eigene MAC erhalten, filtern. Der Datenverkehr wird dann an das gesamte Team weitergeleitet, nicht nur an einzelne Karten, wie bei der Standardauswahl des Modus.

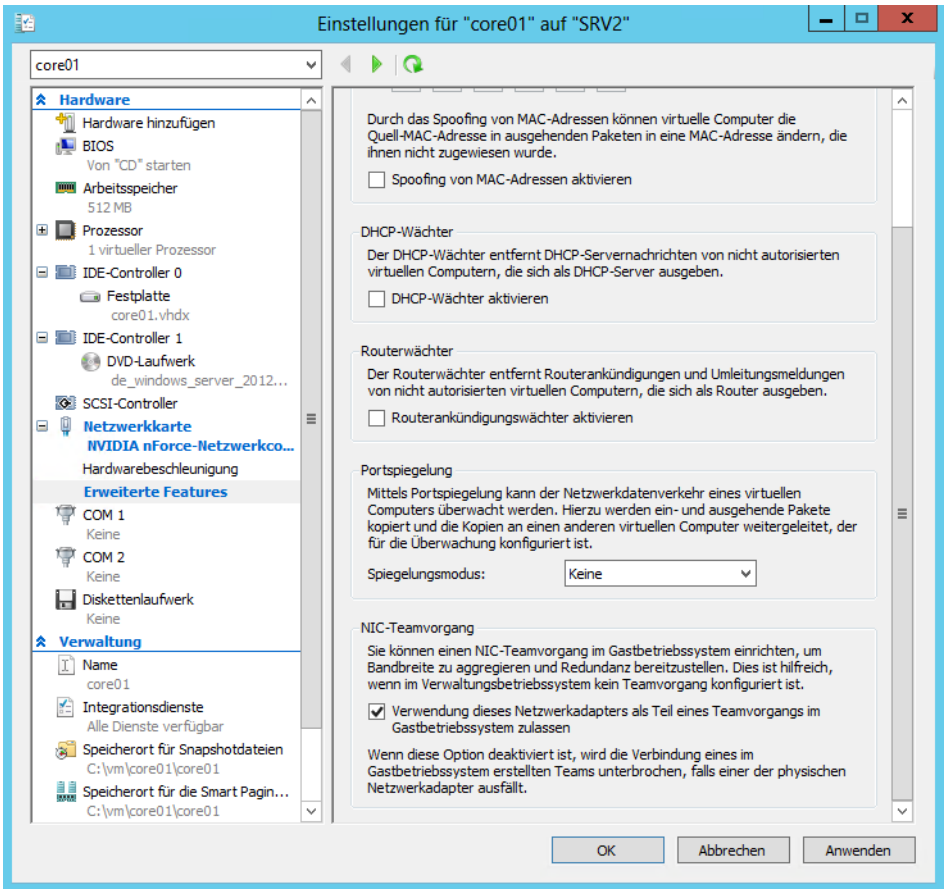
Bei der Anbindung von VLANs sollten Sie diese auf Basis der virtuellen Switches anbinden, nicht über das Team in den einzelnen virtuellen Servern. Ansonsten besteht die Gefahr von Datenkollisionen.

Sie können auch innerhalb von virtuellen Servern Teams erstellen. Dazu verwenden Sie als Grundlage die virtuellen Netzwerkkarten, die den virtuellen Servern zugewiesen sind. Die verschiedenen Netzwerkkarten sollten dann in unterschiedlichen virtuellen Switches betrieben werden. In den einzelnen virtuellen Switches sind wiederum physische Netzwerkkarten integriert, die verschiedene Funktionen nutzen können, zum Beispiel SR-IOV. Eine neue Funktion in Hyper-V in Windows Server 2012 R2 ist Single-Root I/O Virtualization. Hierbei handelt es sich um physische Funktionen von Netzwerkkarten. Netzwerkkarten, die diese Funktion unterstützen, stellen für virtualisierte

Umgebungen implementierte E/A-Kanäle zur Verfügung, mit denen sich die Karte gegenüber virtualisierten Servern wie mehrere Netzwerkkarten verhält. SR-IOV ist vor allem bei E/A-intensiven Anwendungen interessant.

Damit Sie in virtuellen Servern auf Basis der virtuellen Netzkarten, die wiederum auf virtuellen Switches des Hyper-V-Hosts basieren, Teams erstellen können, müssen Sie diese Funktion erst in den Einstellungen des virtuellen Servers in den erweiterten Einstellungen des Netzwerkadapters aktivieren. Dazu rufen Sie im Hyper-V-Manager über das Kontextmenü des virtuellen Servers seine Einstellungen auf und klicken auf *Netzwerkkarte/Erweiterte Features*. Im unteren Bereich stellen Sie bei *NIC-Teamvorgang* diese Konfiguration ein.

Abbildg. 6.13 Konfigurieren von virtuellen Servern für die Unterstützung von NIC-Teams



Diese Einstellung können Sie auf dem Hyper-V-Host aber auch in der PowerShell durchführen. Dazu verwenden Sie den folgenden Befehl:

```
Set-VMNetworkAdapter –VMName <Name des virtuellen Servers> –AllowTeaming On
```

Sie können sich die Einstellungen der virtuellen Netzwerkkarten mit dem folgenden Befehl anzeigen lassen:

```
Get-VMNetworkAdapter –VMName <Name des virtuellen Servers> |fl
```

Verwenden Sie in virtuellen Servern NIC-Teams, nutzt der virtuelle Server für den Datenverkehr immer beide Karten, zumindest wenn Sie den Lastenausgleichsmodus aktiviert haben. Allerdings unterstützen nicht alle Funktionen in Windows Server 2012 R2 NIC-Teams. Diese Daten schickt der Server dann über einzelne Netzwerkkarten. Zu den nicht unterstützten Funktionen gehören SR-IOV, RDMA, Native Host Quality of Service, TCP Chimney und 802.1X Authentication. Für eine schnelle Kommunikation zwischen Windows Server 2012 R2 müssen Netzwerkkarten die RDMA-Funktion (Remote Direct Memory Access) unterstützen. Bei dieser Funktion können Server über das Netzwerk Daten im Arbeitsspeicher austauschen. Wichtig ist diese Funktion vor allem, wenn Sie Windows Server 2012 R2 als NAS-Server einsetzen, also als iSCSI-Ziel, und auf dem Server Datenbanken von SQL Server 2012 oder virtuelle Maschinen von Hyper-V speichern.

Windows Server 2012 R2 unterstützt TCP Chimney Offload. Bei dieser Technik lassen sich Berechnungen für den Netzwerkverkehr vom Prozessor zu den Netzwerkkarten delegieren, was die Leistung des Rechners für Anwendungen und im Netzwerk erheblich beschleunigen kann und den Prozessor des Servers entlastet.

Eigenschaften von TCP/IP und DHCP

Für den Fall, dass kein DHCP-Server für das automatische Zuweisen einer IP-Adresse zur Verfügung steht, bestimmt Windows Server 2012 R2 eine Adresse in der für Microsoft reservierten IP-Adressierungsklasse, die von 169.254.0.1 bis 169.254.255.254 reicht.

Diese Adresse verwendet der Server, bis ein DHCP-Server erreichbar ist oder Sie eine statische IP-Adresse festlegen. Bei dieser Methode verwendet Windows Server 2012 R2 kein DNS, WINS oder Standardgateway, da diese Methode nur für ein kleines Netzwerk mit einem einzigen Netzwerksegment entworfen ist. WINS steht für Windows Internet Name Service und ist der Vorgänger der dynamischen DNS-Aktualisierung. Während DNS für die Namensauflösung mit voll qualifizierten Domänennamen zuständig ist, löst WINS NetBIOS-Namen auf.

IPconfig verwenden

Es können Situationen auftreten, in denen Sie die IP-Adressinformationen für einen bestimmten Server anzeigen müssen. Dies ist der Fall, wenn Ihr Server beispielsweise nicht mit anderen Computern im Netzwerk kommuniziert oder wenn andere Server nicht mit Ihrem Server kommunizieren können. In solchen Situationen müssen Sie die IP-Adresse der anderen Server kennen, um die Ursache des Problems bestimmen zu können.

Im Dialogfeld *Eigenschaften von Internetprotokoll (TCP/IP)* können Sie statische TCP/IP-Informationen anzeigen. Windows enthält ein Befehlszeilendienstprogramm mit der Bezeichnung Ipconfig, um TCP/IP-Informationen anzuzeigen. Mit diesem Dienstprogramm werden die TCP/IP-Konfigurationsoptionen auf einem Host überprüft, aber nicht festgelegt. Zu diesen Optionen zählen die IP-Adresse, die Subnetzmaske und das Standardgateway. Die Befehlssyntax für dieses Dienstprogramm lautet *ipconfig*. Starten Sie das Programm am besten über eine Eingabeaufforderung (*cmd*). Mit

Ipconfig können Sie jedoch nicht bestimmen, ob die IP-Adresse mithilfe der statischen oder der dynamischen Methode zugewiesen wurde.

Ausführlichere Informationen erhalten Sie mit Ipconfig, wenn Sie zusätzlich die Option */all* angeben. Auf dem Bildschirm werden die Informationen zu allen TCP/IP-Konfigurationsoptionen angezeigt. Nun sehen Sie, ob DHCP aktiviert ist. Ist dies der Fall und wird eine IP-Adresse für einen DHCP-Server angezeigt, bedeutet dies, dass die IP-Adresse mithilfe von DHCP bezogen wurde.

Zusätzlich lassen sich beim Aufruf von Ipconfig noch die beiden Optionen */renew* und */release* angeben:

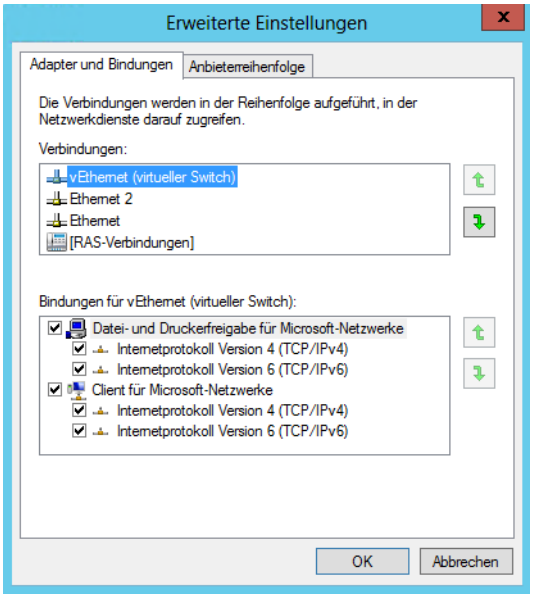
- **ipconfig /release** Entfernt die IP-Adresse vom Client und fordert keine neue an. Wenn ein Client Probleme hat, eine Verbindung mit einem DHCP-Server herzustellen, sollten Sie immer zuerst die IP-Adresse beim Client zurücksetzen.
- **ipconfig /renew** Fordert vom DHCP-Server eine erneute Verlängerung 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 Server 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 an, die Reihenfolge so zu konfigurieren, dass Ihre produktive Netzwerkkarte in der Reihenfolge ganz oben steht:

1. Damit Sie diese Reihenfolge festlegen können, sollten Sie zunächst im Netzwerk- und Freigabecenter auf den Link *Adaptereinstellungen ändern* klicken.
2. Aktivieren Sie die Menüleiste durch Drücken der Alt-Taste.
3. Rufen Sie den Menübefehl *Erweitert/Erweiterte Einstellungen* auf.

Abbildg. 6.14 Konfiguration der Bindungsreihenfolge



4. Es öffnet sich ein neues Fenster, über das Sie unter anderem die Bindungsreihenfolge der Netzwerkkarten einstellen können.
5. 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.

Verwenden von Befehlszeilentools für Netzwerkinformationen

Mithilfe von Befehlszeilentools können Sie schnell Informationen über Ihren Server und Ihr Netzwerk abrufen sowie diese zur Diagnose von Netzwerkproblemen einsetzen. Die Befehle in diesem Thema beziehen sich auf TCP/IP-Netzwerke. Wir gehen in diesem Abschnitt auf die häufigsten Fragen zur Ermittlung von Netzwerkinformationen in der Eingabeaufforderung ein.

- **Wie ermittle ich den Computernamen?** Geben Sie in der Eingabeaufforderung *hostname* ein
- **Wie ermittle ich die IP-Adresse meines Computers?** Geben Sie in der Eingabeaufforderung *ipconfig* ein
- **Wie ermittle ich die physische Adresse meines Computers (MAC-Adresse, Media Access Control)?** Geben Sie in der Eingabeaufforderung *ipconfig /all* ein. Falls Ihr Server mit mehreren Netzwerkadaptern ausgestattet ist, wird die physische Adresse für jeden Adapter einzeln aufgeführt.
- **Wie erhalte ich eine neue IP-Adresse?** Geben Sie in der Eingabeaufforderung *ipconfig /release* ein. Hierdurch geben Sie Ihre aktuelle IP-Adresse frei. Geben Sie in der Eingabeaufforderung als Nächstes *ipconfig /renew* ein, um eine neue IP-Adresse zu erhalten.
- **Wie löse ich anhand des DNS-Namens (Domain Name System) eine IP-Adresse auf?** Geben Sie in der Eingabeaufforderung *ping <DNS-Name>* ein. Dieser Vorgang wird Reverse-Lookup genannt.
- **Wie teste ich die Kommunikation mit einem anderen Server?** Geben Sie in der Eingabeaufforderung *ping <IP-Adresse>* des zu testenden Computers ein

Weitere wichtige Optionen von Ipconfig sind folgende:

- **ipconfig /registerdns** Erneuert die Registrierung des Clients am konfigurierten DNS-Server, wenn für die DNS-Zone die dynamischen Updates aktiviert sind
- **ipconfig /displaydns** Zeigt den lokalen DNS-Cache an, auch die zuletzt geöffneten Internetseiten und aufgelösten DNS-Namen. Löschen Sie den Verlauf im Browser, sind die Daten dennoch an dieser Stelle vorhanden. Sie müssen den lokalen DNS-Cache getrennt löschen, indem Sie *ipconfig /flushdns* verwenden.
- **ipconfig /flushdns** Löscht den lokalen DNS-Cache

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 von der Seite *http://www.wintotal.de/Software/index.php?id=2574* [Ms179-K06-03] im Internet herunterladen können, werden alle MAC-Adressen in einem Netzwerk in der Eingabeaufforderung ausgelesen.

Geben Sie dazu den Befehl *getmac <IP-Segment> <Startadresse> <Endadresse>* ein. So werden zum Beispiel mit *getmac 192.168.178 1 40* die MAC-Adressen aller Rechner im Subnetz *192.168.178.x* von der IP-Adresse *192.168.178.1* bis zur Adresse *192.168.178.40* ausgelesen. Danach werden die Ergebnisse in der Textdatei *used_ips.txt* ausgegeben, die im gleichen Ordner angelegt wird, aus dem Sie *getmac.bat* starten.

Mit diesem kostenlosen Tool erhalten Sie schnell alle verfügbaren MAC-Adressen in einem IP-Bereich. Öffnen Sie nach dem Scanvorgang die Textdatei *used_ips.txt*, um sich die MAC-Adressen der Clients anzeigen zu lassen.

Korrekte Namensauflösung mit Nslookup in IPv4 und IPv6 testen

Treten in einem Microsoft-Netzwerk Fehler auf oder wollen Sie den Internetzugang testen, verwenden Sie das Befehlszeilentool Nslookup. Wenn ein Servername mit Nslookup nicht aufgelöst werden kann, sollten Sie überprüfen, wo das Problem liegt:

1. Ist in den IP-Einstellungen des Computers der richtige DNS-Server als bevorzugt eingetragen?
2. Optional beim Einsatz in Active Directory: Verwaltet der bevorzugte DNS-Server die Zone, in der Sie eine Namensauflösung durchführen wollen?
3. Optional beim Einsatz in Active Directory: 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. Optional beim Einsatz in Active Directory: Wenn eine Weiterleitung eingetragen ist, kann dann der Server, zu dem weitergeleitet wird, die Zone auflösen?
5. Optional beim Einsatz in Active Directory: 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.

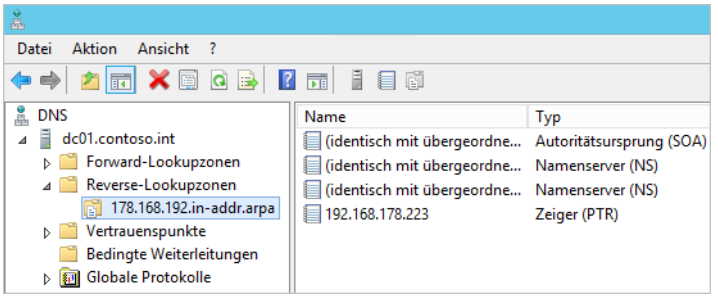
Gehen Sie strikt nach dieser Vorgehensweise vor, werden Sie bereits recht schnell den Fehler in der Namensauflösung finden, wenn Sie in Active Directory arbeiten. Sobald Sie Nslookup aufgerufen haben, können Sie beliebig Servernamen auflösen. Wenn Sie keinen vollwertigen DNS-Namen (Fully Qualified Domain Name, FQDN) eingeben, sondern nur den Computernamen, ergänzt der lokale Rechner automatisch den Namen durch das primäre DNS-Suffix des Computers bzw. durch die in den IP-Einstellungen konfigurierten DNS-Suffixe.

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 in der Eingabeaufforderung *nslookup <host> <server>*, also zum Beispiel *nslookup www.microsoft.de 192.168.178.223* ein. Bei diesem Beispiel versucht Nslookup den Host *www.microsoft.de* mithilfe des Servers 192.168.178.223 aufzulösen.

Abbildg. 6.15 Auflösen von Servernamen mit Nslookup

Damit Nslookup auch den korrekten Namen des DNS-Servers in Active Directory anzeigt, müssen Sie sicherstellen, dass der DNS-Server in der Forward-Lookupzone der Domäne registriert ist. Außerdem müssen Sie manuell eine Reverse-Lookupzone erstellen, in der die IP-Adressen der Domäne registriert sind.

Abbildg. 6.16 Für die korrekte Namensauflösung in Active Directory ist auch eine Reverse-Lookupzone notwendig



Außerdem müssen Sie noch Einstellungen in der IPv6-Konfiguration der Netzwerkkarte auf dem DNS-Server vornehmen. Hier hat Windows Server 2012 R2 die lokale Adresse des Servers hinterlegt. Diese trägt die Bezeichnung ::1, was 127.0.0.1 in IPv4 entspricht. Aktivieren Sie für IPv6 die Option *DNS-Serveradresse automatisch beziehen*. Danach erhalten Sie auch für DNS-Server in Active Directory den korrekten Namen des Servers und seine IPv4-Adresse zurück.

Sie können 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>* aufrufen, sondern können Nslookup mit dem Befehl *nslookup –<Server>* starten, wobei der Eintrag *<Server>* der Name oder die IP-Adresse des DNS-Servers ist, den Sie befragen wollen, zum Beispiel *nslookup –server 192.168.178.223.* Geben Sie den Befehl *nslookup* ohne weitere Parameter ein, können Sie in der Oberfläche mit *server 192.168.178.223* den Standardserver für das aktuelle Fenster auf den DNS-Server setzen.

Funknetzwerke nutzen

In diesem Abschnitt gehen wir auf den Betrieb von Windows Server 2012 R2 in Funknetzwerken (Wireless LANs, WLANs) ein. Achten Sie darauf, dass Sie den neuesten Windows Server 2012 R2-kompatiblen Treiber für die WLAN-Karte Ihres Computers verwenden. Eine Übersicht der Support-Homepages von fast allen Hardwareherstellern finden Sie unter *http://www.treiber.de* [Ms179-K06-04] oder *http://www.heise.de/ct/treiber* [Ms179-K06-05]. Ist kein Windows Server 2012 R2-Treiber verfügbar, können Sie auch Windows Server 2008 R2-Treiber verwenden. Damit Sie Windows Server 2012 R2 in einem WLAN betreiben können, müssen Sie das Feature *WLAN-Dienst* installieren, wie in den Kapiteln 2 und 4 gezeigt. Das Feature installieren Sie über den Server-Manager durch Auswahl von *Verwalten/Rollen und Features hinzufügen.*

Windows Server 2012 R2 an WLANs anbinden

Im Folgenden zeigen wir Ihnen, wie Sie Windows Server 2012 R2 an WLANs anbinden und wie Sie Windows entsprechend konfigurieren, damit die Anbindung auch sicher ist. Sobald das Feature *WLAN-Dienst* installiert ist und Sie eine WLAN-Karte mit dem Server verbunden haben, werden bereits alle WLANs angezeigt und können den Server anbinden.

Konfiguration von Windows Server 2012 R2 zur Anbindung an ein WLAN

Um die Konfiguration durchzuführen, öffnen Sie das Netzwerk- und Freigabecenter. Klicken Sie in Windows Server 2012 R2 mit der linken Maustaste auf das Netzwerksymbol im Infobereich der Taskleiste, zeigt Windows alle verfügbaren Netzwerke an, auch WLANs, wenn eine WLAN-Netzwerkkarte im System verfügbar ist. Hat sich Windows erfolgreich verbunden, ändert sich das Netzwerksymbol in eine Anzeige für ein WLAN.

Abbildg. 6.17 Anzeigen der WLAN-Verbindung in Windows Server 2012 R2

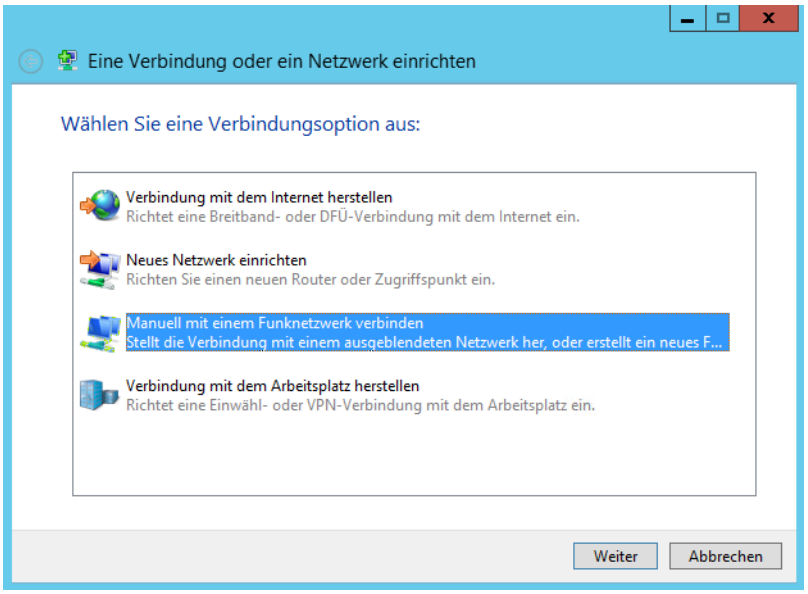
Wollen Sie die Eigenschaften der Netzwerkverbindung aufrufen, klicken Sie diese mit der rechten Maustaste an, und wählen Sie *Status*. Dazu müssen Sie zuvor von der Startseite aus durch Eingabe von *ncpa.cpl* die Netzwerkeinstellungen aufrufen.

Zeigt Windows Server 2012 R2 Ihr WLAN nicht an, klicken Sie im Netzwerk- und Freigabecenter auf den Link *Neue Verbindung oder neues Netzwerk einrichten*. Es erscheint ein neues Fenster, in dem Sie mehrere Möglichkeiten haben, ein Netzwerk einzurichten:

- *Verbindung mit dem Internet herstellen*
- *Neues Netzwerk einrichten*
- *Manuell mit einem Funknetzwerk verbinden*
- *Verbindung mit dem Arbeitsplatz herstellen*

Um sich mit einem WLAN zu verbinden, wählen Sie die Option *Manuell mit einem Funknetzwerk verbinden*. Es erscheint wiederum ein neues Fenster, in dem Sie die Daten zu Ihrem WLAN eintragen können. Im Feld *Netzwerkname* tragen Sie den SSID-Namen (Service Set Identifier) Ihres WLAN ein. Diesen sehen Sie in der Verwaltungsoberfläche des WLAN-Access-Points oder DSL-Routers. Im Feld *Verschlüsselungstyp* tragen Sie die Verschlüsselungsvariante ein, die Sie auch auf dem Access Point konfiguriert haben.

Abbildg. 6.18 Manuelles Verbinden mit einem WLAN



Für die Absicherung eines Funknetzwerks wird oft das WEP-Protokoll (Wired Equivalent Privacy) verwendet. Dieses Protokoll hat jedoch einige Sicherheitslücken und kann durch Auslesen der Verschlüsselung in wenigen Sekunden geknackt werden. Ein WEP-Key ist eine Zeichenkette von Zahlen und Buchstaben. Dieses Verfahren birgt Sicherheitsrisiken. Ein Angreifer kann versuchen, den Schlüssel rechnerisch zu rekonstruieren. Nur sehr wenige WLAN-Lösungen sehen für jeden Client einen eigenen Schlüssel vor. Der WEP-Key wird vom Benutzer definiert und sollte möglichst aus einer komplexen Zahlen- und Buchstabenreihe bestehen.

Für den Fall, dass Ihr Access Point keine Verschlüsselung mit WPA (siehe den folgenden Abschnitt) unterstützt, können Sie die ältere WEP-Verschlüsselung nutzen. Sie können Ihr Netzwerk mit WEP weitgehend vor Attacken schützen, allerdings erreichen Sie nie denselben Schutz wie mit WPA. Aus diesem Grund ist es empfehlenswert, schon vor der Anschaffung zu überprüfen, ob die gewünschte Hardware WPA-tauglich ist oder noch besser WPA2-tauglich (siehe den folgenden Abschnitt).

Die Abkürzung WPA steht für Wi-Fi Protected Access. Mithilfe der WPA-Verschlüsselung können Sie Ihr Funknetzwerk absichern.

WPA2 stellt eine deutlich verbesserte Variante seiner Vorgängerversion WPA dar. Durch ein neu aufgenommenes Verschlüsselungsverfahren mit der Bezeichnung AES-CCM (Advanced Encryption Standard – Counter with CBC-MAC) konnte die Sicherheit gegenüber WPA nochmals erheblich verbessert werden. Das Verfahren stellt allerdings auch deutlich höhere Anforderungen an die Hardware, sodass Geräte, die mit WPA umgehen können, nicht unbedingt auch WPA2 beherrschen.

Die Konfiguration des WLAN können Sie im Netzwerk- und Freigabecenter über den Link *Adaptereinstellungen ändern* in der linken Fensterspalte durchführen. Im daraufhin geöffneten Fenster lässt sich die Konfiguration des WLAN-Adapters genauso durchführen wie die Konfiguration des normalen Netzwerkadapters.

Windows Server 2012 R2 als WLAN-Access-Point betreiben – Virtual WiFi

In Windows Server 2012 R2 haben Sie die Möglichkeit, für WLAN-Verbindungen einen eigenen Access Point darzustellen. Die Virtual WiFi-Technik muss vom eingesetzten Treiber unterstützt werden. Klappt die Einrichtung bei Ihnen nicht, versuchen Sie einen neuen Treiber zu installieren. Gelingt die Einrichtung auch mit einem neuen Treiber nicht, ist Ihre WLAN-Karte nicht kompatibel.

Windows Server 2012 R2 verwendet als Verschlüsselungstechnik WPA2, das heißt die Verbindungen zum WLAN sind sicher. Die Einrichtung nehmen Sie am schnellsten für die Eingabeaufforderung vor. Das hat den Vorteil, dass Sie eine Batchdatei oder ein Skript schreiben können, mit dem Sie den Access Point mit einem Klick einrichten:

1. Öffnen Sie eine Eingabeaufforderung mit Administratorrechten.
2. Geben Sie den folgenden Befehl ein:

```
netsh wlan set hostednetwork mode=allow ssid=<Name des Netzwerks> key= <Kennwort für
den Verbindungsaufbau mit mindestens 8 Zeichen> keyUsage=persistent
```

3. Anschließend erhalten Sie die Meldung der erfolgreichen Einrichtung. Dazu müssen Sie die folgenden Meldungen erhalten:
   - *Der Modus für das gehostete Netzwerk ist so festgelegt, dass das gehostete Netzwerk zugelassen wird.*
   - *Die SSID des gehosteten Netzwerks wurde erfolgreich geändert.*
   - *Die Benutzerschlüsselpassphrase des gehosteten Netzwerks wurde erfolgreich geändert.*

Abbildg. 6.19 Erstellen eines virtuellen WLANs in Windows Server 2012 R2

```
C:\Windows\system32>netsh wlan set hostednetwork mode=allow ssid=W2k12 key= test
2000,, keyUsage=persistent
Der Modus für das gehostete Netzwerk ist so festgelegt, dass das gehostete Netzw
erk zugelassen wird.
Die SSID des gehosteten Netzwerks wurde erfolgreich geändert.
Die Benutzerschlüsselpassphrase des gehosteten Netzwerks wurde erfolgreich geänd
ert.
```

Der nächste Schritt besteht darin, dass Sie das Netzwerk aktivieren. Dazu geben Sie den Befehl *netsh wlan start hostednetwork* in einer Eingabeaufforderung ein, die Sie mit Administratorrechten gestartet haben.

Sie müssen die Meldung erhalten, dass Windows das Netzwerk erfolgreich gestartet hat. Suchen Sie auf anderen Computern oder auch mobilen Geräten wie iPhones/Android-Handys oder Notebooks und Tablet-PCs nach neuen WLANs, erscheint das Netzwerk und ist bereit für den Verbindungsaufbau.

Wollen Sie sich den Status des Netzwerks anzeigen lassen, öffnen Sie ebenfalls wieder eine Eingabeaufforderung mit Administratorrechten und geben den Befehl *netsh wlan show hostednetwork* ein. Den Sicherheitsschlüssel zeigen Sie mit *netsh wlan show hostednetwork security* an.

Wollen Sie den Schlüssel ändern, verwenden Sie den Befehl *netsh wlan set hostednetwork key=<Neues Kennwort>*.

Der Befehl *netsh wlan show settings* zeigt die globalen Einstellungen für WLANs in Windows Server 2012 R2 an.

Damit die angebundenen Clients die Internetverbindung des Servers nutzen können, müssen Sie in den Eigenschaften der Netzwerkverbindung, die mit dem Internet verbunden ist, also der WLAN-Karte, dem UMTS-Stick oder der kabelgebundenen Netzwerkverbindung, auf der Registerkarte *Freigabe* den Zugriff zulassen.

Durch die Freigabe der Internetverbindung erstellt Windows Server 2012 R2 auch einen kleinen DHCP-Server. Das heißt, die Clients die sich an das virtuelle WLAN anbinden, müssen für DHCP konfiguriert sein.

Wollen Sie verhindern, dass sich Clients mit dem virtuellen Netzwerk verbinden, können Sie es mit dem Befehl *netsh wlan stop hostednetwork* anhalten. Verbindungen verweigern Sie mit dem Befehl *netsh wlan set hostednetwork mode=disallowed*.

Remoteunterstützung auch über das Internet nutzen

Eine häufig genutzte Funktion zur Unterstützung von Administratoren über das Internet ist die Remoteunterstützung. Bei dieser Funktion schickt ein Hilfe suchender Administrator einem Supportmitarbeiter eine Einladung, die einen Link enthält, über den sich dieser mit dem Server verbinden kann. Der Verbindungsaufbau findet dazu über den Remotedesktop statt.

Um die Remoteunterstützung zu verwenden, müssen Sie jedoch nicht erst den Remotedesktop aktivieren. Obwohl die Namen ähnlich sind und in beiden Fällen eine Verbindung mit einem Remotecomputer hergestellt wird, dienen der Remotedesktop und die Remoteunterstützung unterschiedlichen Zwecken. Sie können den Remotedesktop verwenden, um von zu Hause eine Verbindung mit dem Server in Ihrem Büro herzustellen.

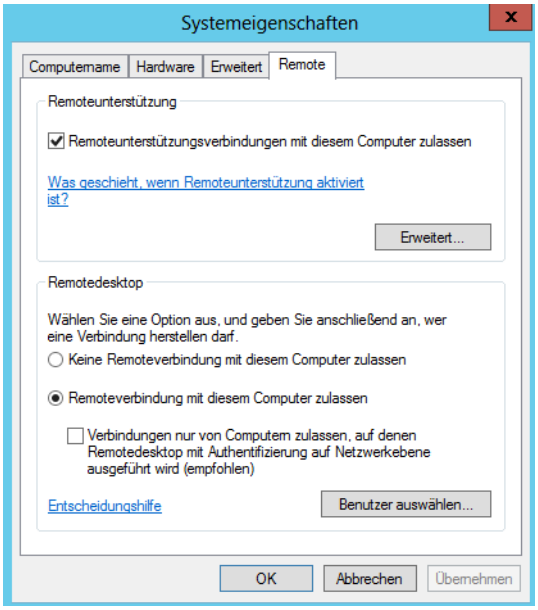
Sie verwenden die Remoteunterstützung, um remote Hilfestellung zu geben oder Hilfe zu erhalten. So könnte zum Beispiel ein Mitarbeiter des technischen Supports auf Ihren Server zugreifen, um Ihnen bei der Beseitigung eines Computerproblems zu helfen oder Ihnen ein bestimmtes Verfahren zu zeigen. Auf dieselbe Weise können Sie einem anderen Benutzer helfen. In beiden Fällen sehen Sie und die andere Person denselben Computerbildschirm. Wenn Sie beschließen, Ihrem Helfer ebenfalls die Steuerung Ihres Computers zu ermöglichen, können Sie und Ihr Helfer den Mauszeiger steuern. Die Konfiguration dieser beiden Technologien findet getrennt voneinander statt.

Netzwerksupport mit dem Remotedesktop und der Remoteunterstützung

Mit dem Remotedesktop in Windows Server 2012 R2 kann Ihr Server über das Internet oder das Netzwerk ferngesteuert werden. Sie können aber auch selbst von der Ferne auf den Desktop Ihres Servers zugreifen. In Windows Server 2012 R2 ist zusätzlich die Remoteunterstützung integriert, mit der Sie über das Internet eine Verbindung aufbauen können. Allerdings muss dazu ein Administrator am Server angemeldet sein. Die Funktion hat Vorteile, wenn zwei Administratoren zusammen in einer Sitzung arbeiten wollen und sich den Desktop teilen müssen. Damit diese Supportfunktion genutzt werden kann, müssen Sie diese in Windows zunächst aktivieren und konfigurieren:

1. Im ersten Schritt müssen Sie im Server-Manager über *Verwalten/Rollen und Features hinzufügen* das Feature *Remoteunterstützung* hinzufügen (siehe Kapitel 4).
2. Öffnen Sie *Systemsteuerung/System und Sicherheit/System*, und klicken Sie in der linken Fensterspalte auf den Link *Remoteeinstellungen*.
3. Aktivieren Sie im Bereich *Remoteunterstützung* das Kontrollkästchen *Remoteunterstützungsverbindungen mit diesem Computer zulassen*, wenn Sie neben dem Remotedesktop auch Remoteunterstützungen benötigen, also beide Benutzer alle Eingaben auf dem Desktop sehen sollen.
4. Den Remotedesktop aktivieren Sie ebenfalls an dieser Stelle. Um auch mit Zusatzwerkzeugen oder älteren Windows-Versionen per Remotedesktop auf den Server zuzugreifen, deaktivieren Sie das Kontrollkästchen *Verbindungen nur von Computern zulassen …*

Abbildg. 6.20 Aktivieren des Remotedesktops und der Remoteunterstützung in Windows Server 2012 R2



Sie können die Berechtigungen festlegen, die für den Remotebenutzer gültig sind, und aktivieren, welchen Verbindungsaufbau Sie genehmigen wollen. Klicken Sie auf die Schaltfläche *Benutzer auswählen* und dann auf *Hinzufügen/Erweitert/Jetzt suchen*. Wählen Sie den entsprechenden Benutzer aus, der Zugriff erhalten soll. Sie können auch zuvor einen eigenen Benutzer anlegen, den Sie für diesen Dienst nutzen. Die Benutzerverwaltung starten Sie durch Eingabe von *lusrmgr.msc* auf der Startseite. Mehr zum Thema lesen Sie auch in Kapitel 2.

Auf Servern, die Mitglied einer Domäne sind, können Sie auch Domänenbenutzer hinzufügen, die den Remotedesktop nutzen dürfen. Die Remoteunterstützungsverbindung verwendet zwar auch das RDP-Protokoll, lässt allerdings nur Verbindungen zu, wenn ein Administrator sich am PC angemeldet und eine Einladung verschickt hat.

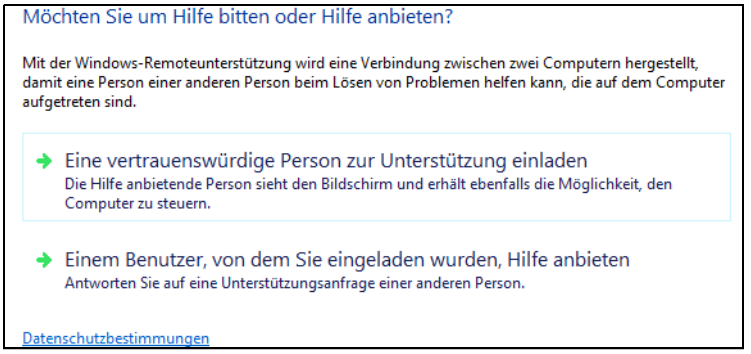
Remoteunterstützung mit Bordmitteln

Mit der Windows-Remoteunterstützung steht einer Person, der Sie vertrauen, ein Verfahren zur Verfügung, um eine Verbindung mit Ihrem Server herzustellen und Ihnen den Weg zu einer Problemlösung schrittweise aufzuzeigen, auch wenn sich diese Person nicht in der Nähe aufhält. Damit sichergestellt ist, dass nur Personen, die Sie darum gebeten haben, mithilfe der Windows-Remoteunterstützung eine Verbindung mit Ihrem Server herstellen können, werden alle Sitzungen verschlüsselt und sind durch ein Kennwort geschützt.

Die Remoteunterstützung funktioniert auch über das Internet. Mit der Easy Connect-Funktion können sich Hilfesuchende und Supportmitarbeiter über das Internet authentifizieren und schnell und einfach einen Verbindungsaufbau starten. Zusatzwerkzeuge sind dazu nicht notwendig und die Verbindung funktioniert auch über Firewalls hinweg.

Um eine Remoteunterstützung anzufordern, müssen Sie zunächst eine Einladung erstellen und die Sitzung konfigurieren. Der schnellste Weg, diese Sitzung zu konfigurieren, führt über die Eingabe von *msra* auf der Startseite. Im Anschluss öffnet sich ein neues Fenster, und Sie können die Remoteunterstützung über einen Assistenten konfigurieren.

Abbildg. 6.21 Starten der Windows-Remoteunterstützung



Damit Sie die Remoteunterstützung verwenden können, muss zuvor sichergestellt sein, dass diese auf Ihrem Server tatsächlich aktiviert ist. Nachdem Sie die Remoteunterstützung einmalig aktiviert haben, können Sie zukünftig ohne weitere Meldungen Remoteunterstützungsanforderungen absenden. Wenn Sie die Remoteunterstützung aktivieren, werden folgende Aktionen durchgeführt:

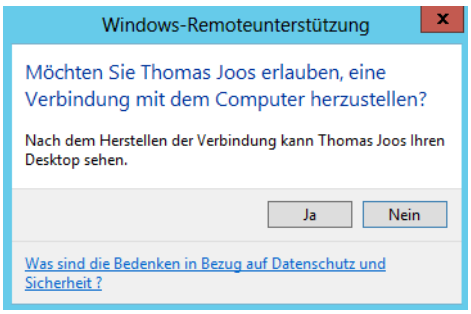
1. Sie können Windows-Remoteunterstützungseinladungen mithilfe einer E-Mail oder einer Datei senden und empfangen.
2. Die Windows-Remoteunterstützung wird von der Windows-Firewall zugelassen, sodass die Kommunikation mit dem Server des Helfers möglich ist.
3. Der Teredo-Dienst wird gestartet. Dieser Dienst ermöglicht es dem Helfer, über die meisten Router, welche die Netzwerkadressübersetzung (NAT) verwenden, eine Verbindung mit Ihrem Server herzustellen. Der Dienst fordert bei einem Microsoft Teredo-Server eine IPv6-Adresse für die Remoteverbindung an. Dazu wählen Sie die Option *Easy Connect verwenden* aus.

Wenn Sie über die Eingabe von *msra* auf der Startseite eine Einladung erstellen, können Sie diese entweder direkt als E-Mail versenden oder in einer Datei speichern. Der Administrator, der eine Verbindung mit dem Server aufbauen soll, benötigt die Einladungsdatei und das erstellte Kennwort.

Anschließend muss der entsprechende Benutzer nur doppelt auf die Einladung klicken und das Kennwort eingeben, das die Remoteunterstützung aktiviert hat. Die Verbindung funktioniert auch von Windows 8-Computern aus.

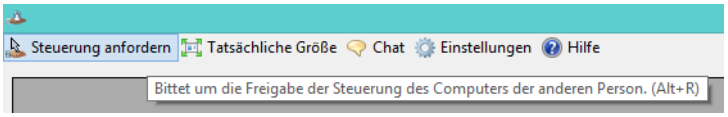
Nach einigen Sekunden stellt der Client eine Verbindung her. Es sind keine Änderungen am Client notwendig. Bevor der Administrator allerdings Remotezugriff erhält, erscheint ein Fenster, in dem der Anwender auf dem Host-Server den Zugriff zunächst freischalten muss. Bis zu dieser Bestätigung sieht der andere Client nur einen schwarzen Bildschirm.

Abbildg. 6.22 Genehmigen des Verbindungsaufbaus über die Remoteunterstützung.



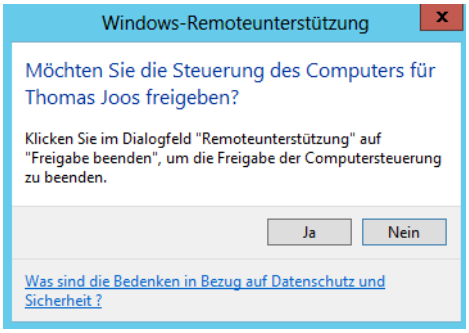
Nach der Genehmigung erfolgt der Verbindungsaufbau. Allerdings kann der Client, der sich mit dem Hostserver verbunden hat, keinerlei Eingaben vornehmen. Er kann dem Anwender mit dem Problem nur zuschauen. Damit der Supportmitarbeiter auch Aktionen vornehmen kann, muss er in der Remoteunterstützungsanwendung die Steuerung des Computers erst anfordern.

Abbildg. 6.23 Anfordern der Steuerung des Hostcomputers



Damit der Supportmitarbeiter Zugriff erhält, muss der Anwender auf dem Hostserver den Zugriff noch genehmigen. Anschließend kann der Supportmitarbeiter den Hostserver steuern. Der Administrator auf dem Hostserver kann die Freigabe jederzeit beenden und die Sitzung auch anhalten.

Abbildg. 6.24 Verwenden der Remoteunterstützung



Remoteunterstützung mit Freeware – TeamViewer

Software für die Fernwartung gibt es zuhauf. Viele Lösungen wie die verschiedenen VNC-Varianten sind kostenlos, bieten dafür aber oft weniger Leistung als professionelle Lösungen wie Dameware oder Radmin. Aber unabhängig vom Preis hat fast jede Software das gleiche Problem: Der Zugriff über das interne Netzwerk stellt kein Problem dar. Soll aber über das Internet, eine Firewall oder einen Proxyserver per HTTPS auf einen Rechner zugegriffen werden, zum Beispiel für den Anwendersupport für kleinere Niederlassungen oder Heimarbeitsplätze, spielen die wenigsten Anwendungen mit. Hier setzen die beiden Freeware-Programme TeamViewer und CrossLoop an. Beide ermöglichen mit sehr schlanken Clients Fernwartungszugriffe auf Rechner im internen Netzwerk, aber auch über das Internet, selbst durch Firewalls und Proxyserver hindurch.

Die Verwendung der Software ist denkbar einfach. Zunächst muss eine kleine Anwendung von der Internetseite *http://www.teamviewer.com* [Ms179-K06-06] heruntergeladen und auf dem Server installiert oder direkt gestartet werden, auf den zugegriffen werden soll. Auch auf dem Server, der über das Internet zugreift, muss die Anwendung installiert oder direkt gestartet sein. Im produktiven Betrieb müssen Sie die Anwendung nach einer Testphase lizenzieren. Die Preise dazu finden Sie auf der Seite des Herstellers.

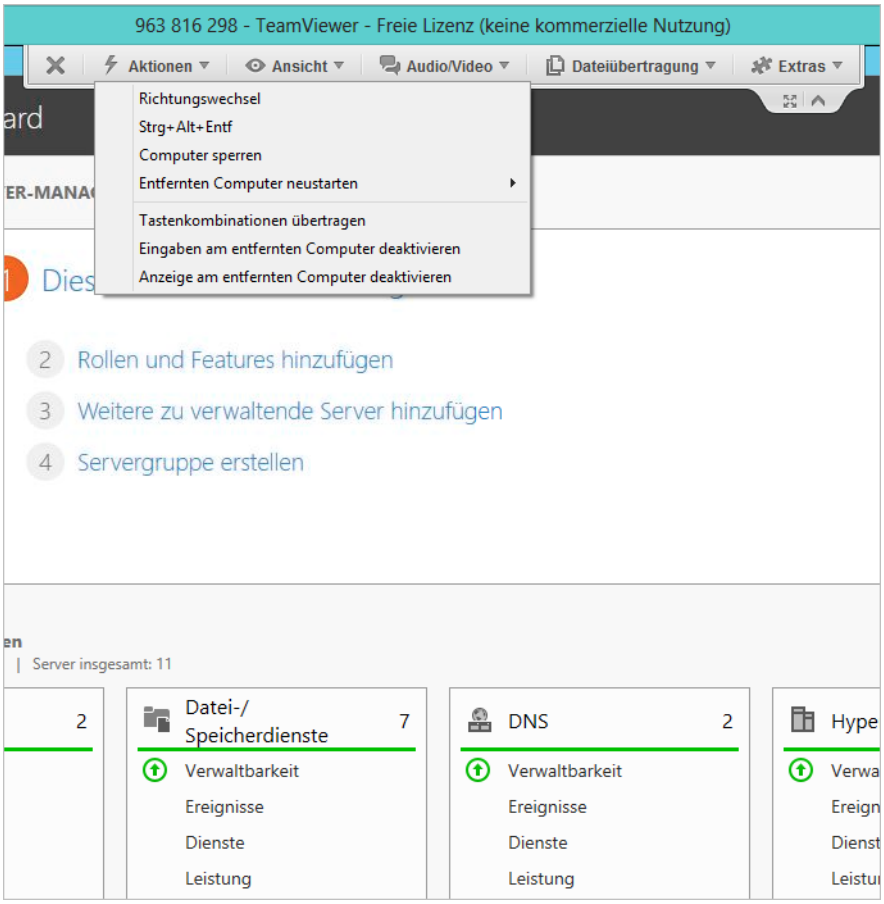
Eine Installation ist nicht zwingend vorgeschrieben, der Start ist auch ohne vorherige Installation möglich. Dadurch können Sie die Anwendung auch von einem USB-Stick aus betreiben. Die ausführbare Datei und das Installationspaket sind identisch. Beim Start der Anwendung wählen Sie den Modus aus. Für beide Varianten reichen normale Benutzerrechte aus. Ein Administratorkonto ist nicht notwendig, da das Tool keine Treiber installiert. Auch Firewall, Proxyserver oder Router müssen Sie nicht anpassen, der Verkehr darf problemlos passieren. Nach der Installation beziehungsweise dem Start der Anwendung generiert diese eine ID und Kennwort. Beides braucht der zugreifende Server.

Abbildg. 6.25 Beim Starten einer TeamViewer-Sitzung wird ein Ticket erstellt, das nur für diese Sitzung gültig ist

Auf dem zugreifenden Computer kann jetzt über die Schaltfläche *Mit Partner verbinden* eine Sitzung zum Server aufgebaut werden. Dabei tauschen die Clients die ID und das Kennwort der aktuellen Sitzung auf dem Host aus. Nach wenigen Sekunden wird das Fenster aufgebaut und die Fernwartung beginnt. Das Programm erkennt automatisch, ob die Verbindung über ein Netzwerk oder das Internet hergestellt wird, und stellt die Datenübertragung entsprechend der Bandbreite ein, sodass immer eine optimale Leistung bei der Fernwartung erzielt wird.

Auf der Internetseite des Herstellers gibt es ausführliche Hilfen, wenn die Server zum Beispiel hinter hochsicher konfigurierten Firewalls positioniert sind. Auch hier ist der Zugriff grundsätzlich möglich. Über ein Chatfenster können die beiden Teilnehmer miteinander kommunizieren. Auch Dateien lassen sich zwischen den beiden Computern austauschen.

Abbildg. 6.26 Nach dem Verbindungsaufbau kann ein Administrator sehr effizient und bequem die Fernwartung durchführen



Sind am Server, auf den über die Fernwartung zugegriffen wird, mehrere Monitore angeschlossen, kann in TeamViewer zwischen diesen Monitoren umgeschaltet werden. Wird nach dem Beenden der Sitzung die Anwendung beendet, kann kein Anwender über TeamViewer auf den Server zugreifen, bis erneut eine Sitzung erstellt und die ID und das Kennwort weitergegeben wurden. Natürlich kann diese Konfiguration angepasst werden, damit auch eine Fernwartung auf Server stattfinden kann. In diesem Fall erfolgt der Zugriff nicht über eine ID, sondern es muss eine entsprechende Authentifizierung stattfinden. Der Zugriff funktioniert auch, wenn der zugreifende Server über einen Proxyserver mit dem Internet verbunden ist.

Große Dateien über das Internet versenden – SkyDrive & Co.

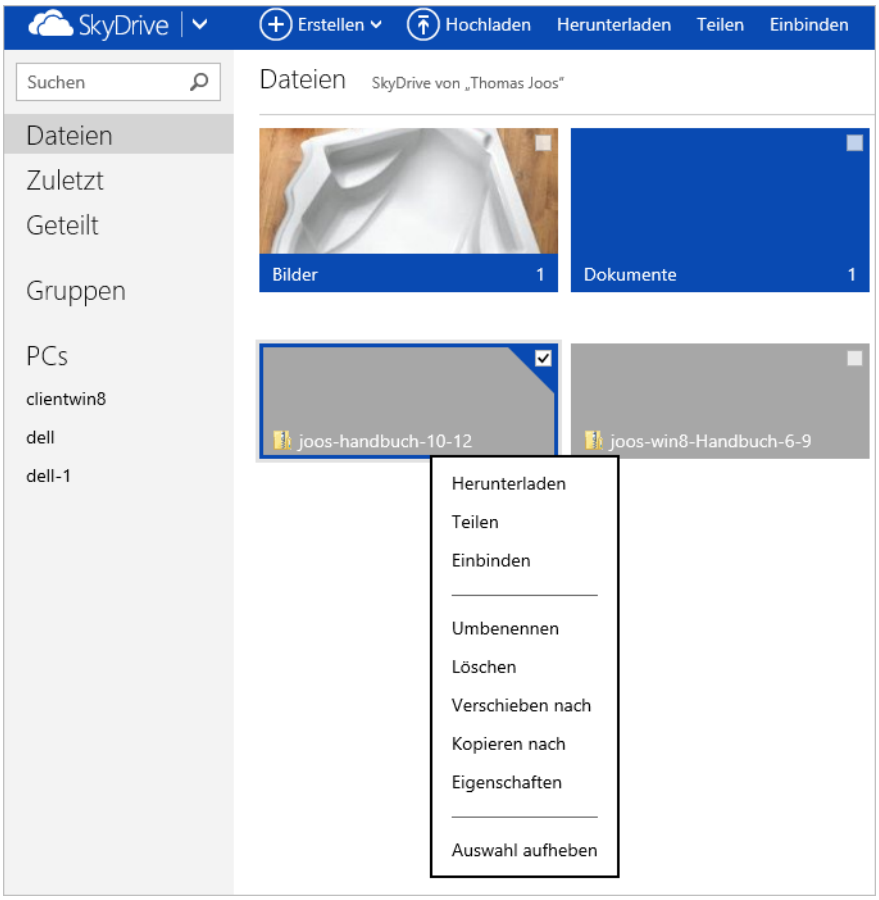
Viele Administratoren müssen ab und zu größere Dateien oder ZIP-Archive über das Internet versenden. Per E-Mail geht das meistens nicht, da die kostenlosen Anbieter von E-Mail-Adressen oft Sperren bei 4 bis 10 MB einbauen. Müssen Sie größere Dateien versenden, können Sie aber über verschiedene Webseiten die Daten hochladen. Im Fenster geben Sie eine E-Mail-Adresse an und der Empfänger kann die Daten dann über einen in der Mail angegebenen Link herunterladen. Ein Beispiel dafür ist die Seite *http://www.mailbigfile.com* [Ms179-K06-07]. Weitere Anbieter für solche Dienste sind:

- *http://www.dropsend.com* [Ms179-K06-08]
- *http://www.filemail.com* [Ms179-K06-09]
- *http://www.megaupload.com* [Ms179-K06-10]
- *http://rapidshare.com* [Ms179-K06-11]
- *http://senduit.com* [Ms179-K06-12]

Sie können auch SkyDrive zum Datenaustausch verwenden:

1. Die Datei, die Sie austauschen wollen, kopieren Sie in den SkyDrive-Ordner auf einem Administratorcomputer. Dazu müssen Sie den SkyDrive-Agenten installieren. Diesen finden Sie über den unten genannten Link.
2. Ist die Datei hochgeladen, rufen Sie am einfachsten die SkyDrive-Webseite (*https://skydrive.live.com* [Ms179-K06-13]) auf und melden sich mit Ihrem Benutzernamen an. Wenn der Synchronisierungsablauf abgeschlossen ist, klicken Sie auf der Webseite mit der rechten Maustaste auf die Datei und wählen *Teilen*.

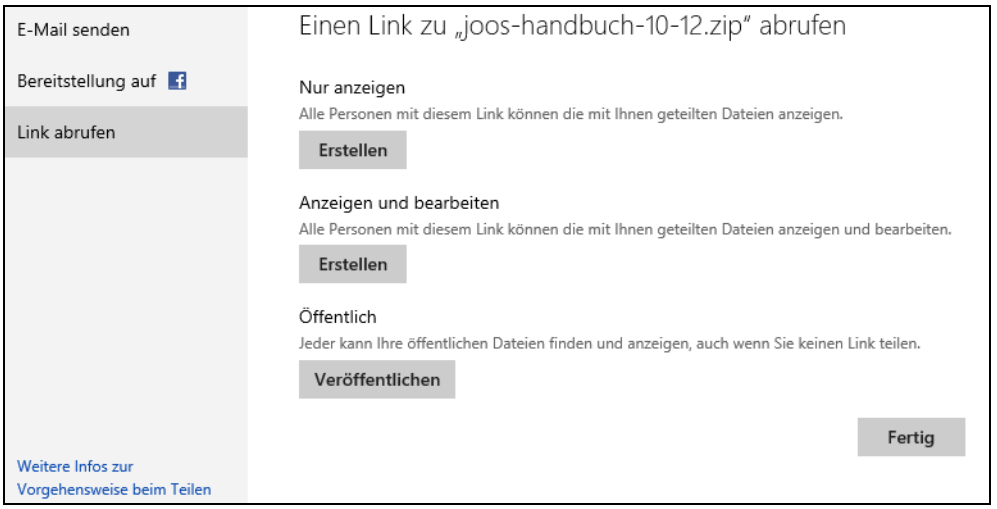
Abbildg. 6.27 Teilen einer Datei mit SkyDrive



Der einfachste Weg ist, wenn Sie auf *Link abrufen* klicken und dann die Art der Freigabe auswählen, zum Beispiel *Erstellen* im Abschnitt *Anzeigen und bearbeiten*.

Anschließend erhalten Sie einen Link angezeigt. Klicken Sie zunächst auf *Kürzen*, damit der Link gekürzt wird. Versenden Sie diesen Link per E-Mail an den Empfänger, kann dieser die Datei herunterladen. Klicken Sie abschließend auf *Fertig*.

Abbildg. 6.28 Erstellen eines Links zum Downloaden einer Datei über SkyDrive



Erweiterte Netzwerkeinstellungen – Routing und IPv6

In manchen Netzwerken sind neben der Standardkonfiguration weitere Einstellungen in Windows Server 2012 R2 notwendig. Sie können zum Beispiel manuell IP-Routen erstellen, wenn ein Server mit mehreren Netzwerken verbunden ist, oder Sie müssen IPv6 konfigurieren. Ist ein IPv6-Verkehr zwischen zwei Servern möglich, verwendet Windows Server 2012 R2 zuerst automatisch IPv6 und dann erst IPv4. Dazu ist keine Konfiguration von IPv6 notwendig.

IP-Routing unter Windows Server 2012 R2

Sie können über die 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 Server mehrere Netzwerkkarten eingebaut sind, kann immer nur ein Standardgateway pro Server 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 Eingabeaufforderung erstellt.

Wenn Ihre Routinginfrastruktur das Routing Information-Protokoll (RIP) für IPv4 verwendet, können Sie unter Windows den RIP-Listener aktivieren, mit dessen Hilfe der Server andere Routen im Netzwerk automatisch erlernen kann, indem er gesendete RIP-Meldungen abhört und anschließend der Routingtabelle IPv4-Routen hinzufügt.

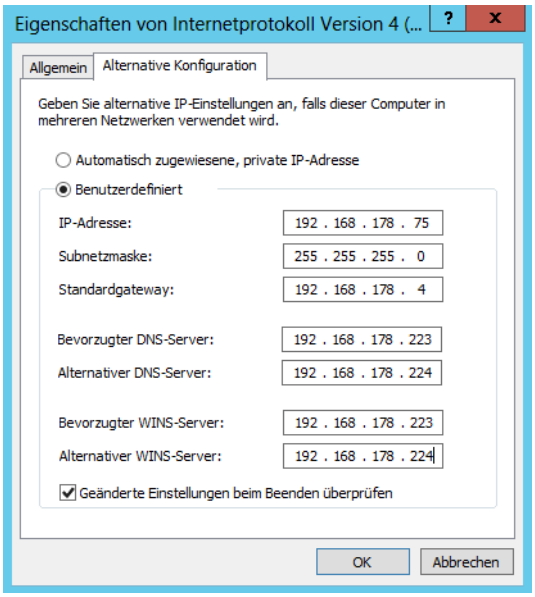
Die RIP-Überwachung lässt sich nur verwenden, wenn die Routinginfrastruktur RIP unterstützt. Alternativ können Sie den Befehl *route add –p* verwenden, um Routen manuell der IPv4-Routingtabelle hinzuzufügen.

Für IPv6 müssen Sie den Befehl *netsh interface ipv6 add route* aufrufen, um manuelle Routen zu erstellen. IPv6 wird später in diesem Kapitel behandelt.

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. Wenn Sie eine alternative Konfiguration angeben (nur IPv4), ist das Standardgateway die IP-Adresse auf der Registerkarte *Alternative Konfiguration* im Feld *Standardgateway*. Die alternative Konfiguration steht nur dann für IPv4 zur Verfügung, wenn Sie DHCP verwenden. Findet der Client keinen DHCP-Server, verwendet er automatisch die Daten der alternativen Konfiguration.

Abbildg. 6.29 Hinterlegen einer IP-Adresse für die alternative Konfiguration eines DHCP-Clients



In vielen Netzwerken ist es notwendig, Routen manuell in der Eingabeaufforderung zu erstellen. Um manuelle Routen zu erstellen, wird der Route-Befehl in der folgenden Syntax verwendet:

```
route –p add <Ziel> MASK <Netzmaske> Gateway METRIC <Metrik> IF <Schnittstelle>
```

Die einzelnen Parameter haben folgende Funktionen:

- –p Legt fest, dass die Route auch nach dem Booten des Computers weiterhin vorhanden ist. Standardmäßig werden die Routen beim Neustart wieder gelöscht.
- 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

- **Netzwerkmaske** 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.
- **Schnittstelle** 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

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 bisherige IPv4 bietet einen Adressraum von etwas über 4 Milliarden IP-Adressen, mit denen Server und andere Geräte angesprochen werden können. In den Anfangstagen des Internets, als es nur wenige Rechner gab, die eine IP-Adresse benötigten, galt dies als weit mehr als ausreichend. Eine IPv6-Adresse ist 128 Bit lang (IPv4: 32 Bit). Damit gibt es etwa 3,4 x 1038 (340,28 Sextillionen) IPv6-Adressen. IPv6-Adressen werden in hexadezimaler Notation mit Doppelpunkten geschrieben, die die Adresse in acht Blöcke mit einer Länge von jeweils 16 Bit unterteilen. Beispiel einer IPv6-Adresse:

2001:0db7:85b3:07d3:1319:8a2d:437a:63d4

Eine oder mehrere 16-Bit-Gruppen mit dem Wert 0000 können durch zwei aufeinanderfolgende Doppelpunkte ersetzt werden. Die resultierende Adresse darf höchstens einmal zwei aufeinanderfolgende 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.

Netzmasken, wie sie bei IPv4 verwendet wurden, gibt es bei IPv6 nicht. Die ersten 64 Bit der IPv6-Adresse dienen üblicherweise der Netzadressierung, die letzten 64 Bit werden zur Hostadressierung verwendet. Beispiel: Hat ein Netzwerkgerät die IPv6-Adresse 2001:0db7:85b3:07d3:1319:8a2d:437a:63d4, so stammt es aus dem Subnetz 2001:0db7:85b3:07d3::/64.

Microsoft Windows Server 2008 R2 und Windows Server 2008 nutzen beide den Next Generation TCP/IP-Stack. Hierbei handelt es sich um einen neu entworfenen 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 des NAT oder eine Änderung der Anwendungsprotokolle passieren. Teredo ist in Windows XP/Vista Service Pack 2 und Windows Server 2003 Service Pack 1 enthalten. Teredo ist auf Domänencomputern aktiviert. Beim 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. IPv6 bietet gegenüber IPv4 die folgenden Vorteile:

- **Größerer Adressraum** Der 128-Bit-Adressraum von IPv6 bietet genügend Platz, um jedes Gerät im bestehenden und zukünftigen Internet mit einer eigenen, global gültigen Adresse auszustatten
- **Effizienteres Routing** Durch den überarbeiteten IPv6-Header und das neue Adressierungsschema, das eine hierarchische Routinginfrastruktur unterstützt, können IPv6-Router den entsprechenden Netzwerkverkehr schneller weiterleiten
- **Einfache Konfiguration** IPv6-Hosts können sich entweder über DHCP oder mithilfe eines lokalen Routers selbst konfigurieren
- **Verbesserte Sicherheit** Die IPv6-Standards beheben einige der Sicherheitsprobleme von IPv4. Sie bieten einen besseren Schutz vor Adress- und Portscans. Sie schreiben vor, dass IPv6-Implementierungen IPsec (Internet Protocol Security) unterstützen müssen.

Windows Server 2012 R2 unterstützt bereits nach der Installation das neue IP-Protokoll Version 6 (IPv6). Wenn Sie die Eigenschaften der Netzwerkverbindung anzeigen lassen, sehen Sie, dass IPv6 automatisch mit den Netzwerkverbindungen verknüpft wird.

IPv6 wurde so entworfen, dass es einfacher als IPv4 zu konfigurieren ist. IPv6 kann sich automatisch selbst konfigurieren, auch ohne DHCPv6 (Dynamic Host Configuration Protocol for IPv6). Alle IPv6-Knoten konfigurieren für jede physische oder logische IPv6-Schnittstelle automatisch eine lokale Adresse mit dem Präfix fe80::/64. Diese Adressen können nur zur Kommunikation mit benachbarten Knoten verwendet werden. Sie werden nicht im DNS registriert, und wenn Daten an eine solche Adresse gesendet werden sollen, ist zusätzlich eine Zonen-ID notwendig.

Wenn Sie einen Server mit Windows Server 2012 R2 für IPv6 konfigurieren, sind folgende automatische Einstellungen möglich:

- Ein IPv6-Host sendet eine Multicastnachricht und empfängt eine oder mehrere Routernachrichten. In diesen Routernachrichten finden sich Subnetzpräfixe (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 Subnetzpräfixe 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.

Konfiguration von IPv6

Neben der automatischen Konfiguration ist auch eine manuelle Konfiguration von IPv6 möglich. Windows Server 2012 R2 stellt dazu eine grafische Oberfläche bereit, unterstützt aber auch die Konfiguration in der Eingabeaufforderung über den Befehl Netsh.

Wenn Sie in den Eigenschaften der Netzwerkverbindung die Eigenschaften von IPv6 aufrufen, können Sie verschiedene Einstellungen vornehmen:

- **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
- **IPv6-Adresse** Hier können Sie eine IPv6-Unicastadresse angeben
- **Subnetzpräfixlänge** Hier können Sie die Länge des Subnetzpräfix 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
- **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 Computers detaillierter spezifizieren:

- Für jede IPv6-Unicastadresse müssen Sie eine IPv6-Adresse und eine Subnetzpräfixlänge 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.
- Sie können festlegen, ob eine bestimmte Metrik für die IPv6-Adressen oder die Standardgateways verwendet 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 Registerkarte für IPv4.

Konfiguration von IPv6 in der Eingabeaufforderung mit Netsh

Neben der Möglichkeit, IPv6 in der grafischen Oberfläche zu konfigurieren, besteht zusätzlich die Möglichkeit, die Konfiguration über die Eingabeaufforderung durchzuführen. Für diese Konfiguration wird das Befehlszeilentool Netsh verwendet.

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 Subnetzpräfix – standardmäßig 64)
- **type** Typ 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 *active* (die Adresse wird beim Systemneustart entfernt) oder *persistent* (die Adresse bleibt beim Systemneustart 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 folgenden Abschnitt.

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
```

Erstellen manueller Routen für IPv6

Wie für IPv4 können auch für IPv6 manuelle Routen erstellt werden. Allerdings wird beim Erstellen manueller Routen für IPv4 der Befehl Route verwendet, während für IPv6 der Befehl Netsh verwendet wird. Die 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 (z. B. 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 Systemstart beibehalten
- **persistent** Änderung ist dauerhaft (Standard)

In Netzwerken mit IPv4 arbeitet Windows Server 2012 R2 nach dem alten Standard. Sind in einem Netzwerk IPv4 und IPv6 verfügbar, priorisiert Windows Server 2012 R2 den Datenverkehr über IPv6. Funktioniert der Datenverkehr nicht problemlos, erkennt dies Windows Server 2012 R2 und schaltet im Hintergrund automatisch auf IPv4 um.

Um eine Namensauflösung in Windows Server 2012 R2 zu testen, verwenden Sie am besten nicht mehr das alte Befehlszeilentool Nslookup, sondern das PowerShell-Cmdlet *Resolve-DNSname*. Auch dieses ist für IPv6 optimiert und kann anzeigen, ob bestimmte Zonen eine IPv6-Adresse verwenden. Microsoft geht auf der Seite *http://blogs.msdn.com/b/b8/archive/2012/06/05/connecting-with-ipv6-in-windows-8.aspx* [Ms179-K06-14] ausführlicher auf das Thema ein.

Windows Server 2012 R2 Active Directory

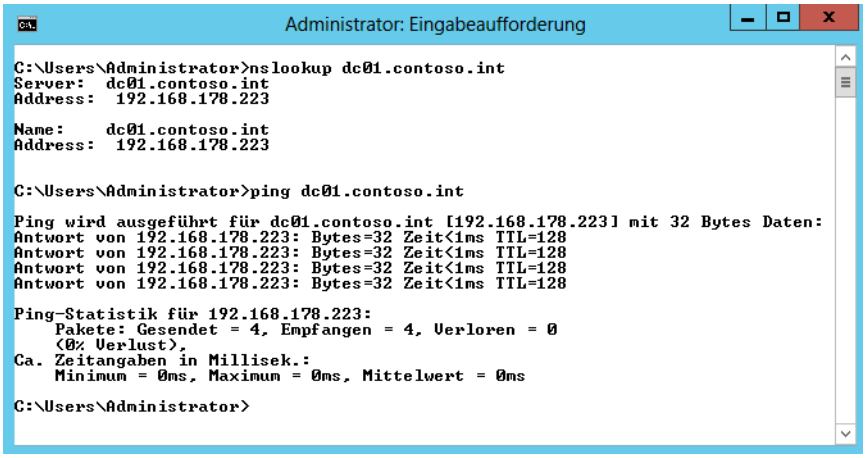
Windows Server 2012 R2 können Sie als Mitgliedsserver auch in älteren Active Directory integrieren. Dazu sind nur wenige Anpassungen notwendig. Im nächsten Abschnitt zeigen wir Ihnen, wie Sie einen Server mit Windows Server 2012 R2 in eine Domäne aufnehmen.

Netzwerkeinstellungen für die Domänenaufnahme konfigurieren

Um einen Windows Server 2012 R2-Server in Active Directory zu integrieren, rufen Sie zunächst die Verwaltung der Netzwerkverbindungen auf. Am schnellsten geht das, wenn Sie auf der Startseite nach *ncpa.cpl* suchen. Alternativ rufen Sie das Netzwerk- und Freigabecenter über das Kontextmenü der Netzwerkverbindung auf dem Desktop auf und klicken auf *Adaptereinstellungen ändern*.

Ändern Sie die IP-Einstellungen so ab, dass der Client einen DNS-Server in der Active Directory-Struktur verwendet. Um die Verbindung zu testen, öffnen Sie eine Eingabeaufforderung auf dem Client und geben *nslookup <FQDN des Domänencontrollers>* ein. Lassen Sie anschließend den Client noch den Domänencontroller anpingen.

Abbildg. 6.30 Testen der Verbindung zu einem Domänencontroller



Domänenaufnahme durchführen

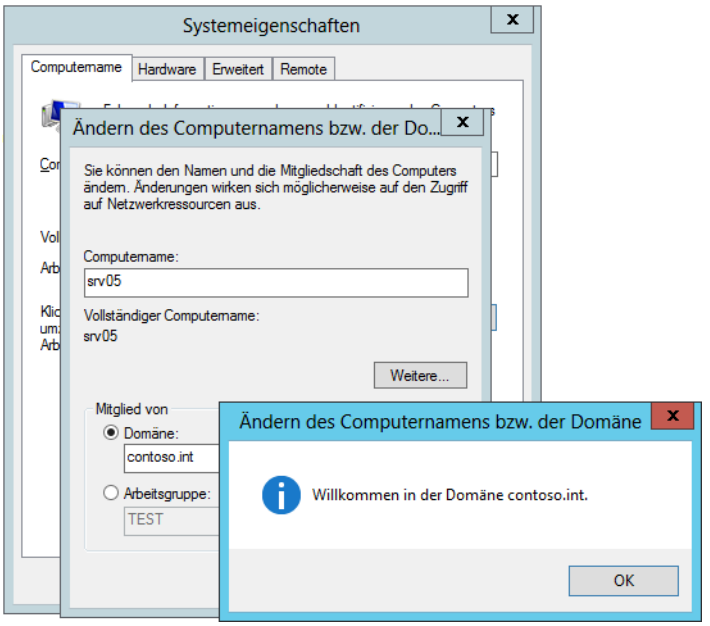
Rufen Sie die Startseite auf, indem Sie die -Taste betätigen. Suchen Sie nach *computer* und klicken Sie die Kachel *Computer* mit der rechten Maustaste an. Wählen Sie unten in der App-Leiste den Eintrag *Eigenschaften* aus. Klicken Sie anschließend bei *Einstellungen für Computernamen, Domäne und Arbeitsgruppe* auf *Einstellungen ändern*.

Klicken Sie danach auf der Registerkarte *Computername* auf *Ändern*. Geben Sie bei *Computername* den Namen des Computers ein, den er später in der Domäne erhalten soll. Aktivieren Sie dann die

Option *Domäne* bei *Mitglied von* und tragen Sie den DNS-Namen der Domäne ein, welcher der Client beitreten soll.

Als Letztes müssen Sie sich noch an der Domäne authentifizieren. Bei erfolgreicher Eingabe wird der Server in die Domäne aufgenommen. Wie bei den Vorgängerversionen von Windows müssen Sie den Server nach der Domänenaufnahme neu starten.

Abbildg. 6.31 Beitreten einer Domäne mit Windows Server 2012 R2



Haben Sie den Server nach der Domänenaufnahme neu gestartet, melden Sie sich mit einem Benutzernamen an der Domäne an.

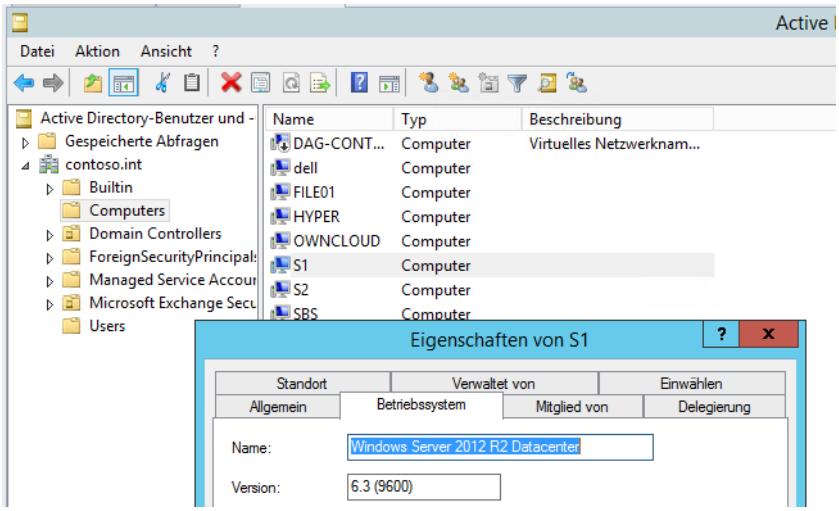
TIPP Sie können Server auch in der PowerShell benennen, neu starten und in Domänen aufnehmen. Dazu verwenden Sie die Cmdlets

- *Rename-Computer –Name [Computername]*
- *Add-Computer ?DomainName [Domänenname]*
- *Restart-Computer*

Domänenaufnahme testen

Auf dem Domänencontroller öffnen Sie in Windows Server 2012 R2 den Server-Manager und dann über das Menü *Tools* das Snap-In *Active Directory-Benutzer und -Computer*. Hier sehen Sie in der OU *Computers* den neuen Server und können dessen Eigenschaften aufrufen. Auf der Registerkarte *Betriebssystem* sehen Sie den Stand des Betriebssystems.

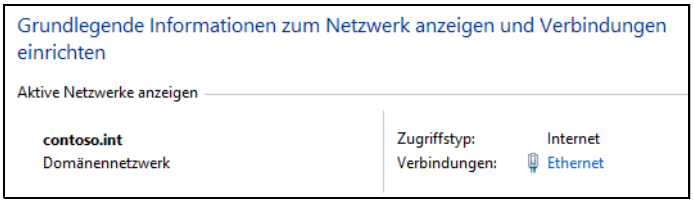
Abbildg. 6.32 Überprüfen der Domänenmitgliedschaft eines Windows Server 2012 R2-Servers



Um sich mit einem Windows Server 2012 R2-Server an Active Directory anzumelden, klicken Sie auf *Anderer Benutzer*. Geben Sie bei der ersten Anmeldung den Benutzernamen in der Syntax *<NetBIOS-Name der Domäne>\<Benutzernamen>* ein, wenn es den gleichen Benutzernamen auch auf dem lokalen Server gibt. Ist der Anmeldename in der Domäne auf dem Server nicht vorhanden, reicht auch die Anmeldung über den Benutzernamen.

Öffnen Sie nach der Anmeldung an der Domäne das *Netzwerk- und Freigabecenter* auf dem Desktop, sehen Sie ebenfalls den Domänenstatus des Servers. Sie können auch einfach auf das Netzwerksymbol klicken, um den Domänenstatus anzuzeigen.

Abbildg. 6.33 Anzeigen der Domänenmitgliedschaft in Windows Server 2012 R2



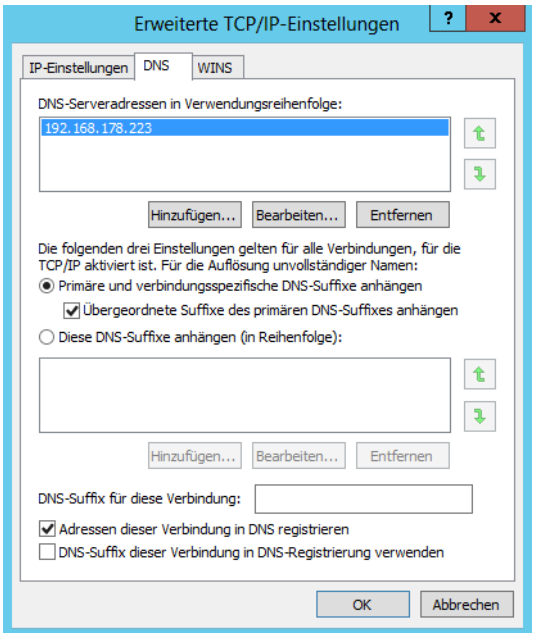
Über die Schaltfläche *Erweitert* in den Eigenschaften des TCP/IP v4-Protokolls und auch in IPv6 erreichen Sie weitere Einstellungen, um die Namensauflösung per DNS oder WINS im Netzwerk optimal einzustellen. Normalerweise werden Sie hier keine Einstellungen vornehmen müssen, da bereits die Standardeinstellungen ausreichen. Für manche Netzwerke kann jedoch eine Nachjustierung sinnvoll sein. Ob das bei Ihnen notwendig ist, erfahren Sie auf den folgenden Seiten. Vor allem wenn Sie eine Active Directory-Gesamtstruktur mit einer verschachtelten Domänenstruktur betreiben, sind Konfigurationsmaßnahmen notwendig.

Auf der Registerkarte *WINS* können Sie einen WINS-Server eintragen, sofern Sie einen solchen im Netzwerk betreiben. Zu manchen Active Directory-Domänen 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 voll qualifizierten Domänennamen zuständig ist, werden mit WINS NetBIOS-Namen aufgelöst.

Damit sich die Server 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 Einstellungen auch mithilfe eines DHCP-Servers verteilen. Mehr zu diesen Themen lesen Sie in den Kapiteln 24 bis 26.

Abbildg. 6.34 Konfigurieren der erweiterten DNS-Einstellungen in Windows Server 2012 R2



Auf der Registerkarte *DNS* werden schließlich notwendige Einstellungen vorgenommen, um Windows Server 2012 R2 besser in eine Windows-Domäne einzubinden. Für eine generelle Aufnahme von Windows Server 2012 R2 in eine Domäne sind hier keine Änderungen vorzunehmen. Zunächst sind standardmäßig immer nur die folgenden Optionen aktiviert:

- *Primäre und verbindungsspezifische DNS-Suffixe anhängen*
- *Übergeordnete Suffixe des primären DNS-Suffixes anhängen*
- *Adressen dieser Verbindung in DNS registrieren*

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.int*, wenn das primäre DNS-Suffix des Computers *contoso.int* 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.int* einen Servernamen *dc05* auflösen wollen, versucht der Rechner zunächst die Auflösung über *dc05.muenchen.de.contoso.int*, falls dies das primäre DNS-Suffix des Computers ist. Im Anschluss wird versucht, den Namen über *dc05.de.contoso.int* und dann über *dc05.contoso.int* aufzulösen, da diese Domänen der Domäne *muenchen.de.contoso.int* 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 Server zunächst die Auflösung in *dc06.contoso.int*, 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.int* ein, versucht der Server, auch den Namen nach *dc06.muenchen.de.microsoft.int* aufzulösen.
- **Adressen dieser Verbindung in DNS registrieren** Auch diese Option ist bereits standardmäßig aktiviert. Ein DNS-Server unter Windows Server 2003/2008/2008 R2/2012 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, werden 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, 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 des 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 diese Option aktivieren, wird der Server-Name 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 Servernamen in verschiedenen DNS-Zonen auflösen wollen, aktivieren Sie auf dem Server 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.int* auflösen wollen, müssen Sie immer *dc1.contoso.int* eingeben, wenn Ihr Server nicht Mitglied dieser Struktur ist. Diese Einstellung ist nur optional, erleichtert aber die Stabilität der Namensauflösung in Active Directory. Sie sollten diese Einstellung auf jedem Domänencontroller sowie auf jedem Exchange-Server in Ihrer Gesamtstruktur und auch auf Computern von Administratoren oder Powerusern durchführen, die ständig eine Verbindung zu anderen Domänen aufbauen müssen. Zuerst sollten immer die eigene Domäne und der eigene Namensraum eingetragen werden, bevor andere Namensräume abgefragt werden.

Wenn Sie diese Maßnahme durchgeführt haben, können Sie durch Eingabe des Befehls *nslookup* den Effekt überprüfen. Sie können an dieser Stelle lediglich *dc1* eingeben. Der Server befragt seinen bevorzugten DNS-Server, ob ein Server mit dem Namen *dc1.contoso.int* 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.

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 korrekt, 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 *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.

Öffnen Sie nach der Konfiguration bzw. der Aufnahme des Computers in die Domäne eine Eingabeaufforderung, 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. Überprüfen Sie, ob das primäre DNS-Suffix mit dem Zonennamen übereinstimmt. Das primäre DNS-Suffix der Domäne wird automatisch beim Aufnehmen in die Domäne zugewiesen.
2. Stellen Sie als Nächstes fest, ob die IP-Adresse des DNS-Servers korrekt in den IP-Einstellungen des Computers eingetragen wurde.

Netzwerkanalyse mit Tools

In diesem Abschnitt zeigen wir Ihnen, wie Sie Netzwerke schnell und einfach mit Zusatztools analysieren. Kostenlose Tools helfen bei der Fehlersuche oder dem Auffinden von Geräten im Netzwerk meist schneller und einfacher als Bordmittel von Windows Server 2012 R2.

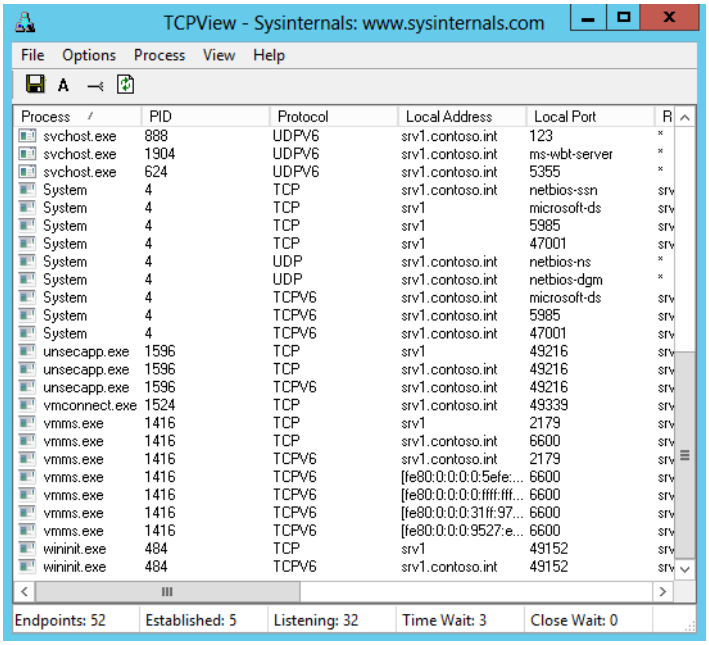
Geöffnete Ports überwachen – TCPView, NetStat und CurrPorts

Zur Analyse der Netzwerkverbindungen auf einem Server ist es unerlässlich, sich die geöffneten Ports anzuzeigen. Hierzu liefert Sysinternals mit TCPView (*http://technet.microsoft.com/de-de/sysinternals/bb897437* [Ms179-K06-15]) ein passendes Werkzeug, welches einfach zu bedienen ist und Administratoren bei der Informationsbeschaffung hilft. Auch NirSoft stellt auf der Seite *http://www.nirsoft.net/utils/cports.html* [Ms179-K06-16] ein ähnliches kostenloses Tool mit der Bezeichnung CurrPorts zur Verfügung, welches Sie ebenfalls direkt starten und nicht installieren müssen.

Mit TCPView können Sie sich in einer grafischen Oberfläche alle TCP- und UDP-Endpunkte eines Computers anzeigen lassen. Zusätzlich sehen Sie, welche Prozesse auf die Endpunkte und Ports zugreifen. Sie sehen also nicht nur geöffnete Ports wie bei anderen Programmen, sondern detaillierte Informationen über den Prozess, dessen ID, das Protokoll, die Remoteadresse und den Port.

Das Tool baut auf Informationen auf, die das Windows-Tool Netstat liefert, bietet aber mehr Informationen und ist leichter zu bedienen. Das Tool aktualisiert die Verbindungen jede Sekunde, Sie können über den Menübefehl *Options/Refresh Rate* die Abtastrate ändern. Verbindungen, die den Status innerhalb der Abtastrate ändern, sind gelb markiert. Gelöschte Endpunkte zeigt das Tool rot an, neue Endpunkte in grün. Den aktuellen Verbindungsstatus können Sie über das Menü auch abspeichern.

Abbildg. 6.35 Anzeigen geöffneter Ports mit Freeware von Microsoft



CurrPorts von NirSoft zeigt in einer grafischen Oberfläche ebenfalls die geöffneten Ports an, sowie die Anwendungen inklusive Symbole, welche die Ports geöffnet halten. Über das Kontextmenü der einzelnen Verbindungen können Sie die entsprechenden Prozesse beenden und weitere Informationen aufrufen.

Neben den Zusatztools können Sie geöffnete Ports auch mit Bordmitteln in Windows Server 2012 R2 anzeigen:

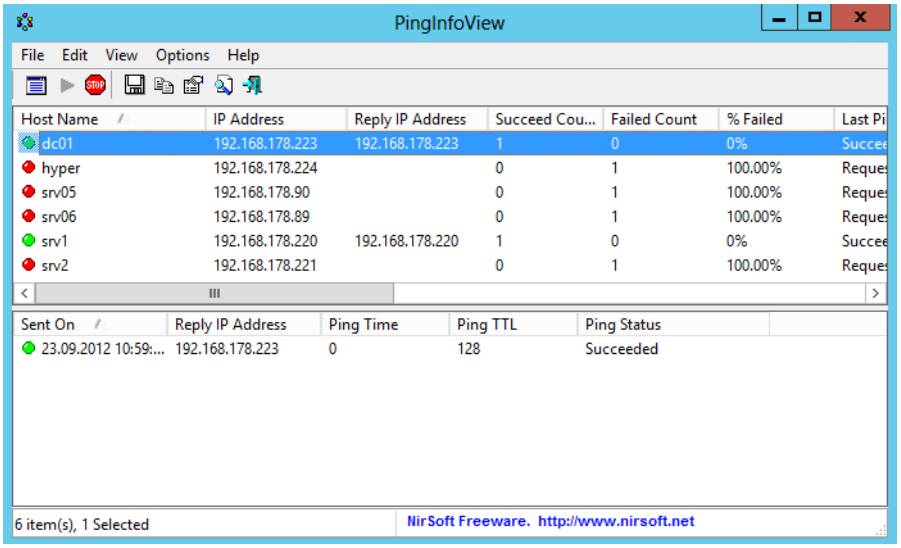
1. Starten Sie eine Eingabeaufforderung über das Kontextmenü mit Administratorrechten.
2. Geben Sie den Befehl *netstat –an* ein. Windows zeigt die geöffneten Ports an.
3. Ausführlichere Informationen erhalten Sie mit *netstat –banvo*.
4. Die Routingtabelle des Computers sehen Sie mit *netstat –r*, Statistiken zu TCP/IP zeigt das Tool mit *netstat –s* an.

Mehrere Ping-Anfragen dauerhaft durchführen und Netzwerkgeräte überwachen

Sie können zwar in der Eingabeaufforderung ohne Weiteres mit *ping <IP-Adresse oder DNS-Name> –t* einen dauerhaften Ping auf eine Netzwerkressource durchführen, aber auf Dauer ist das nicht effektiv. Wollen Sie mehrere Ressourcen auf einmal anpingen und dauerhaft beobachten, ist die Freeware PingInfoView von der Seite *http://www.nirsoft.net/utils/multiple_ping_tool.html* [Ms179-K06-17] optimal.

Starten Sie das Tool und geben Sie die Liste der Geräte an, die Sie anpingen wollen. Sie können hier mit IP-Adressen und Namen arbeiten. Starten Sie den Ping-Vorgang, zeigt das Tool alle Vorgänge übersichtlich in einem Fenster an und Sie erkennen auch die Geschwindigkeit der Verbindung.

Abbildg. 6.36 Testen von Servern im Netzwerk



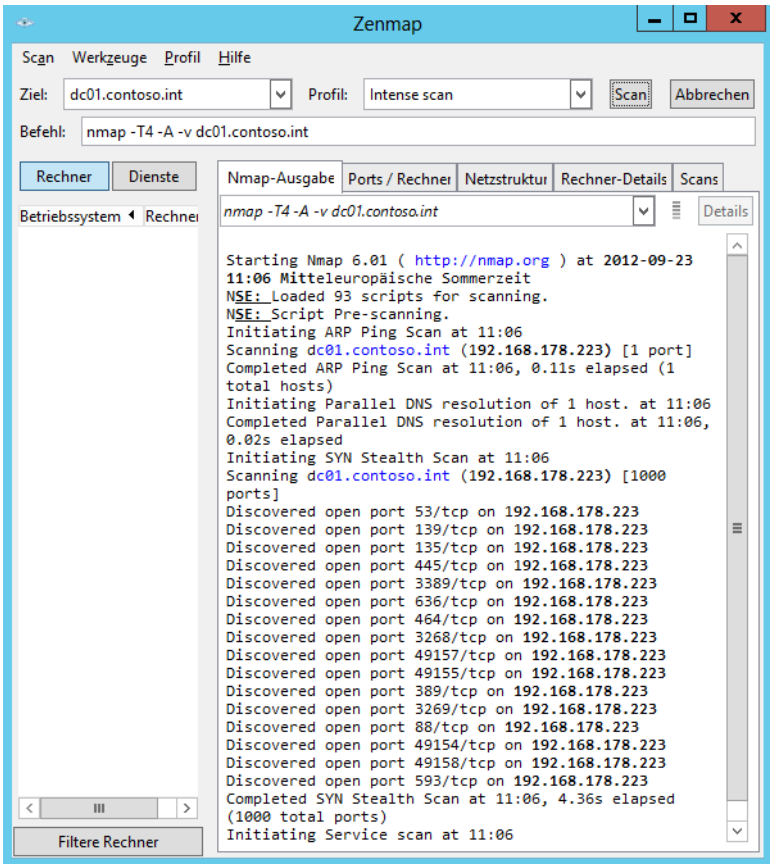
Mit Nmap Netzwerke untersuchen

Kostenlose Tools wie Nmap (*http://nmap.org* [Ms179-K06-18]) helfen bei der Suche nach Netzwerkgeräten und offenen Ports. Der Vorteil von Nmap liegt darin, dass bei den Installationsdateien bereits vorgefertigte Überwachungsskripts integriert sind. Mit diesen können Administratoren, die sich nicht tiefgehender in die Thematik einarbeiten wollen, schnell und einfach Netzwerke untersuchen.

Alles, was Sie tun müssen, ist Nmap zu installieren und zu starten. Anschließend scannt das Tool das Netzwerk. Auf der Downloadseite gibt es auch jede Menge Skripts. Diese haben alle die Endung *.nse* (Nmap Script Engine) und lassen sich in Nmap zur Spezifizierung von Scanjobs verwenden. Mit dem Tool lassen sich Rechner und Netzwerkgeräte auf offene Ports scannen. Zum Lieferumfang von Nmap gehört auch eine grafische Oberfläche, mit der Sie sehr einfach Netzwerke scannen können.

Für Windows-Rechner gibt es eine Installationsdatei für Nmap. Nach dem Download starten Sie den Assistenten und bestätigen die einzelnen Fenster für die Installation. In allen Fenstern müssen die Standardeingaben einfach nur bestätigt werden.

Abbildg. 6.37 Netzwerküberwachung mit Nmap



Nach der Installation von Nmap starten Sie Zenmap. Dabei handelt es sich um die grafische Oberfläche des Befehlszeilentools Nmap. Um einen einfachen Scan zu starten, muss im Feld *Ziel* eine IP-Adresse eingegeben werden. Anschließend klicken Sie auf *Scan*. Danach verbindet sich Nmap mit dem Rechner und zeigt alle offenen Ports an. Im Ordner *Nmap\scripts* befinden sich spezielle Skripts für Nmap, die besondere Aufgaben durchführen können, zum Beispiel um Dropbox-Rechner im Netzwerk zu finden.

Um ein ganzes Subnetz nach offenen Ports zu scannen, geben Sie den Befehl *nmap –sn <Subnetz>* ein, zum Beispiel *nmap –sn 192.168.178.0/24*. Alternativ verwenden Sie den Befehl *nmap <Start-IP-Adresse>-<Letzte Stelle der letzten IP-Adresse>*, zum Beispiel *nmap 192.168.178.1-254*. Hier gibt das Tool mehr Informationen aus.

Auf der Registerkarte *Netzstruktur* lässt sich grafisch das Netzwerk und die verbundenen Clients anzeigen. Mit den Einstellungen im unteren Bereich können Sie die Größe der Grafik anzeigen, mit *Save Graphic* lässt sich die Grafik speichern. Über das Menü *Scan/Speichere Scan* lassen sich Scanergebnisse speichern. Das kann zum Beispiel sinnvoll sein, wenn diese später mit Ndiff verglichen werden sollen. Nmap erlaubt auch mehrere parallele Scans. Diese lassen sich über die Registerkarte *Scans* abbrechen und löschen.

Abgespeicherte Scanergebnisse lassen sich mit Ndiff vergleichen. Dazu geben Sie den Befehl *ndiff <Datei1> <Datei2>* ein. Ausführlichere Ergebnisse gibt das Tool mit der zusätzlichen Option *–v* aus. Über Zenmap lassen sich die Ergebnisse mit dem Menü *Werkzeuge/Ergebnisse vergleichen* untersuchen.

Netzwerkverkehr überwachen – Microsoft Network Monitor

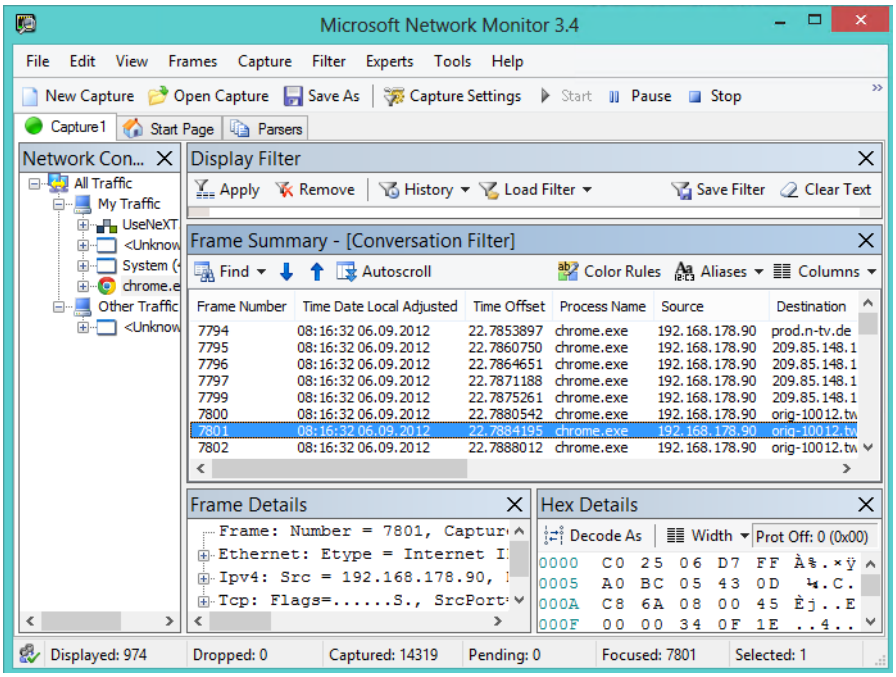
Ein effizientes Programm zum Überwachen des Netzwerksverkehrs und dem Mitschneiden von Paketen im Netzwerk zur Problemlösung bietet Microsoft vollkommen kostenlos an, den Microsoft Network Monitor (*http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=4865* [Ms179-K06-19]). Um den Netzwerkverkehr mitzuverfolgen, müssen Sie das Tool installieren. Dabei gehen Sie vor, wie bei jedem anderen Programm auch. Installieren Sie Network Monitor als typische Installation und danach die *Network Monitor Parsers* als notwendige Erweiterung. Melden Sie sich anschließend neu am Rechner an

Nach der Installation starten Sie den Scanvorgang über *New Capture/Start*. Anschließend kann Network Monitor alle Pakete empfangen, die vom Netzwerk auf dem System eingehen und die der Server versendet. Achten Sie aber darauf, dass Netzwerkpakete, die an andere Server gehen, vom Network Monitor auf dem aktuellen System nicht empfangen werden können. Nur wenn die Pakete als Broadcast oder Multicast an alle Rechner des Netzwerks gehen, kann auch der Network Monitor diese Pakete empfangen.

Arbeiten Sie regelmäßig mit Microsoft Network Monitor, sind folgende Internetseiten eine interessante Quelle:

- **Blog zu Microsoft Network Monitor** *http://blogs.technet.com/b/netmon* [Ms179-K06-20]
- **Network Monitor Open Source Parsers** *http://nmparsers.codeplex.com* [Ms179-K06-21]
- **Network Monitor Experts** *http://nmexperts.codeplex.com* [Ms179-K06-22]
- **TechNet-Forum** *http://social.technet.microsoft.com/Forums/en/netmon/threads* [Ms179-K06-23]

Abbildg. 6.38 Netzwerkverkehr mit Microsoft Network Monitor überwachen



Sobald Sie den Messvorgang gestartet haben, können Sie den Netzwerkverkehr zusätzlich auch filtern lassen. Dazu steht das Menü *Filter* zur Verfügung. Wählen Sie aus den angebotenen Filtern den gewünschten aus. Anschließend sehen Sie diesen im Bereich *Display Filter*. Um den Filter auch auf den Capturevorgang anzuwenden, müssen Sie noch auf *Apply* klicken.

Sind im Server mehrere Netzwerkkarten eingebaut, können Sie über *Capture Settings* festlegen, auf welche Netzwerkverbindungen Microsoft Network Monitor hören und Pakete mitschneiden soll.

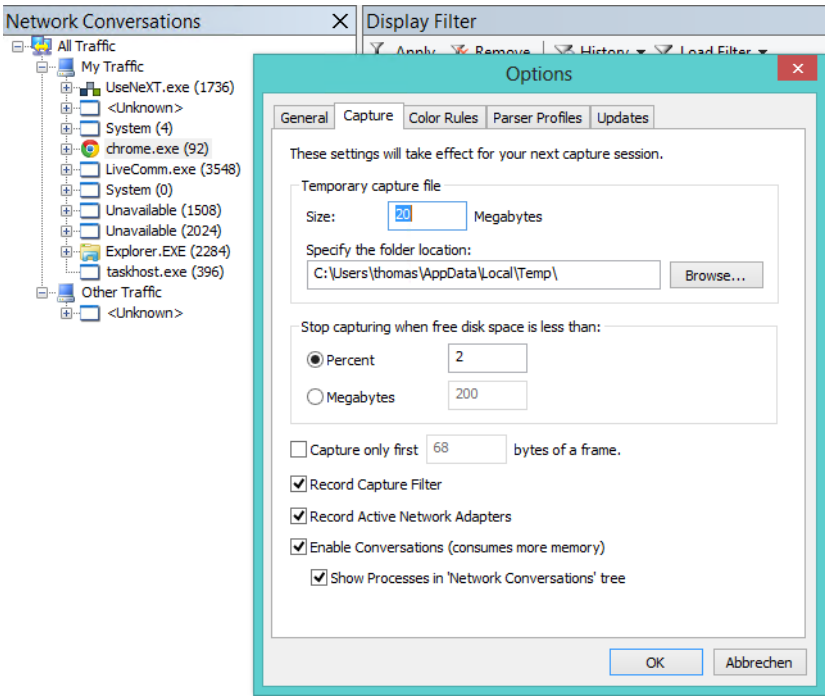
Für eine spätere Analyse können Sie einen Messvorgang als Capture auch abspeichern. Dazu verwenden Sie den Menübefehl *File/Save as*. Anschließend können Sie auf einem anderen Server, auf dem Sie Network Monitor installiert haben, über *File/Open/Capture* diesen Messvorgang laden.

Jeden Messvorgang (Capture), auch die geladenen Capturevorgänge, zeigt Network Monitor als eigene Registerkarte an. Sie können auf diesem Weg also mehrere Vorgänge starten oder laden und über einen Wechsel der Registerkarte überwachen lassen.

Generelle Einstellungen für Microsoft Network Monitor nehmen Sie über *Tools/Options* vor. Hier können Sie auf verschiedenen Registerkarten das Verhalten des Monitors anpassen. Vor allem die Registerkarte *Capture* ist wichtig, da Sie hier die eigentlichen Messvorgänge steuern.

Über das Kontrollkästchen *Enable Conversations* können Sie zum Beispiel den mitgeschnittenen Paketen Prozesse auf dem Server zuordnen. Das hilft sehr effizient bei der Analyse von Netzwerkproblemen. Bei diesem Vorgang hängt Network Monitor an jeden mitgeschnittenen Frame eine ID an. Über diese ID lässt sich jeder Frame einem Prozess auf dem Server zuordnen. Anschließend kann Network Monitor auf der linken Seite des Fensters die Pakete darstellen. Sie sehen das an der Baumstruktur der Prozesse mit den zugeordneten Paketen.

Abbildg. 6.39 Anzeigen von Prozessen zur Netzwerküberwachung



Auf der rechten Seite des Monitors sehen Sie Details zu dem ausgewählten Frame. Hier können Sie auch Filter anlegen und sehen den Inhalt des Datenpakets. Im Bereich *Frame Summary* auf der rechten Seite sehen Sie bei *Source* und *Destination*, von welchem Rechner das Paket ausgeht und an welchen Server es gesendet worden ist. Kann Network Monitor den Namen auflösen, sehen Sie an dieser Stelle direkt den Namen des Computers. Auch der zugeordnete Prozess und das verwendete Protokoll ist in diesem Fenster zu sehen.

Ein wichtiger Punkt in Network Monitor sind die sogenannten *Parser*. Diese können die aufgezeichneten Rohdatenpakete von Network Monitor verwenden und so umwandeln, dass Administratoren verstehen, welche Daten das Paket enthält, um auf diese Weise eventuelle Probleme zu finden. Parser lassen sich nachträglich installieren, zum Beispiel über die Seite *http://nmparsers.codeplex.com* [Ms179-K06-24].

Wireshark (*http://www.wireshark.org* [Ms179-K06-25]) ermöglicht eine umfassende Analyse des Netzwerkverkehrs, setzt aber auch einiges an Fachwissen voraus. Das Tool kennt nahezu alle Netzwerkprotokolle auf dem Markt. Um das Tool effizient nutzen zu können, müssen Sie noch WinPcap (*http://www.winpcap.org* [Ms179-K06-26]) installieren. Dabei handelt es sich um eine Erweiterung für Windows, die Netzwerkprogrammen erlaubt, den Datenverkehr mitzuschneiden.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Windows Server 2012 R2 in einem Netzwerk betreiben. Auch die neue Funktion der Zusammenfassung von Netzwerkkarten (NIC-Teams) haben wir in diesem Kapitel besprochen. Außerdem war die Anbindung von Windows Server 2012 R2 an WLANs sowie das IP-Routing und IPV6 Thema. Ebenfalls Bestandteil des Kapitels waren Tools für die Analyse von Netzwerken sowie die Fehlerbehebung. Natürlich haben wir auch Standardkonfigurationen behandelt und was Sie einstellen müssen, um Windows Server 2012 R2 in Active Directory zu betreiben, inklusive verschiedene Befehlszeilentools zur Fehlerbehebung.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie Hyper-V in Windows Server 2012 R2 nutzen, um Server zu virtualisieren.

Teil C

Virtualisierung mit Hyper-V

Kapitel 7

Hyper-V – Installation und Server virtualisieren

In diesem Kapitel:

Mit Hyper-V bietet Microsoft eine in das Betriebssystem integrierte Lösung zur Virtualisierung an. Hyper-V bietet mit der Hypervisor-Technologie eine direkte Verbindung mit den Virtualisierungsfunktionen den aktuellen AMD- und Intel-Prozessoren. Hyper-V besteht aus einer kleinen hochspezialisierten Softwareschicht, dem sogenannten 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, sogenannte Parent-VMs und Child-VMs, erstellen. Während in der Parent-VM die Prozesse der virtuellen Maschine, der WMI-Provider und der VM-Dienst läuft, 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.

Hyper-V unterstützt die AMD- und Intel-Virtualisierungsfunktionen für x64-Prozessoren und setzt diese für den Einsatz sogar voraus. Dies bedeutet, dass x86-Computer von der Virtualisierung, zumindest als Hostsystem, ausgeschlossen sind. Hyper-V lässt sich daher nur auf x64-Bit-Computern mit Intel VT oder AMD-V Erweiterungen installieren.

Physische und virtuelle Datenspeicher lassen sich virtuellen Maschinen in Hyper-V im laufenden Betrieb zuweisen oder von diesen Maschinen abtrennen. So lassen sich Pass-Through-Festplatten, also die Anbindung von physischem Datenspeicher an virtuelle Maschinen, ohne Beeinträchtigung der Benutzer anbinden. Dies gilt auch für herkömmliche virtuelle Festplatten. Diese Technik funktioniert sowohl bei den virtuellen VHD/VHDX-Festplatten als auch über Festplatten, die zwar am Host physisch angeschlossen, aber nur in den virtuellen Servern konfiguriert sind. Hyper-V ermöglicht dies über einen neuen virtuellen SCSI-Controller.

Neuerungen in Hyper-V

Hyper-V-Hosts können 4 TB RAM nutzen. Virtuelle Maschinen verwalten in Windows Server 2012 R2 bis zu 1 TB Arbeitsspeicher. Virtuelle Maschinen lassen sich in Hyper-V-Clustern priorisieren und mit der Livemigration lassen sich im laufenden Betrieb mehrere Server auf einmal zwischen Clusterknoten verschieben. Fällt ein Knoten aus, verschiebt Hyper-V die virtuellen Maschinen mit der höchsten Priorität zuerst.

Tabelle 7.1 Skalierbarkeit in Windows Server 2012 R2

Ressource	Windows Server 2008 R2 SP1 maximal	Windows Server 2012/2012 R2 maximal
Logische Prozessoren des Hosts	64	320
Physischer Speicher	1 Terabyte	4 Terabyte
Virtuelle Prozessoren pro Host	512	2.048

Tabelle 7.1 Skalierbarkeit in Windows Server 2012 R2 *(Fortsetzung)*

Ressource	Windows Server 2008 R2 SP1 maximal	Windows Server 2012/2012 R2 maximal
Virtuelle Prozessoren pro virtueller Server	4	64
Speicher pro virtueller Server	64 GB	1 Terabyte
Aktive virtuelle Server	384	1.024
Größe virtueller Festplatten	2 Terabyte	64 Terabyte
Clusterknoten	16	64
Virtuelle Server im Cluster	1.000	8.000
Livemigration	Nur im Cluster	Mit und ohne Cluster, Livemigration der Datenträger
Replikation virtueller Server ohne Cluster	Nicht möglich	Möglich

TIPP Hyper-V lässt sich auch weitaus besser in der PowerShell verwalten als der Vorgänger in Windows Server 2008 R2. Geben Sie in der PowerShell *Get-Command –Module Hyper-V* ein, erhalten Sie eine Liste der verfügbaren Cmdlets.

In Windows Server 2008 R2 konnten Sie 64 logische Prozessoren für Hyper-V-Hosts einsetzen und virtuellen Servern bis zu 4 virtuelle Prozessoren zuweisen. Windows Server 2012 R2 unterstützt bis zu 320 Prozessoren pro Host und Sie können virtuellen Servern bis zu 64 virtuelle Prozessoren zuordnen. Sie können außerdem bis zu 2.048 virtuelle Prozessoren auf den Hyper-V-Hosts einsetzen. Auf jedem Server können Sie bis zu 1.024 virtuelle Server installieren. Erstellen Sie einen Cluster, haben Sie die Möglichkeit, bis zu 64 Knoten einzusetzen.

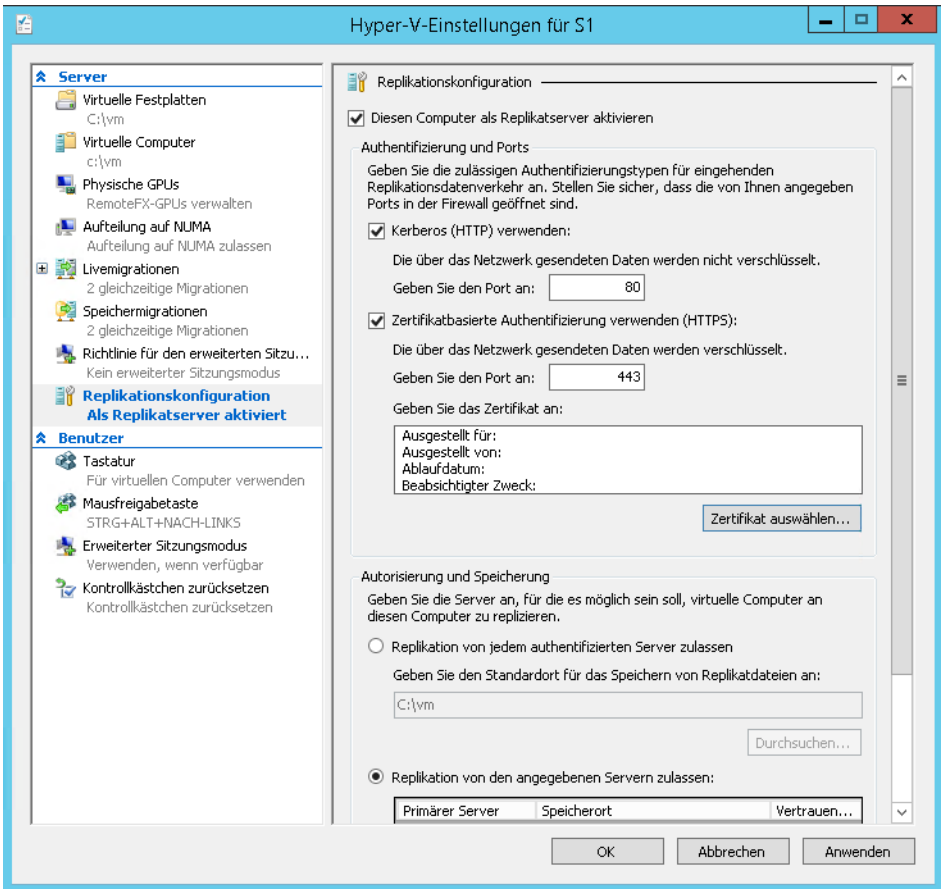
Bessere Hochverfügbarkeit

Mit Hyper-V-Replica lassen sich in Windows Server 2012 R2 virtuelle Festplatten und ganze Server asynchron zwischen verschiedenen Hyper-V-Hosts im Netzwerk replizieren und synchronisieren. Die Replikation findet über das Dateisystem statt, ein Cluster ist nicht notwendig. Die Replikationen lassen sich manuell, automatisiert oder nach einem Zeitplan ausführen. Auf diesem Weg lassen sich virtuelle Server auch hochverfügbar betreiben, ohne teure Cluster betreiben zu müssen. Die Einrichtung nehmen Sie über einen Assistenten im Hyper-V-Manager vor (siehe Kapitel 9). Außerdem können Sie die Livemigration von virtuellen Servern jetzt auch ohne Cluster verwenden (siehe Kapitel 9).

Damit Hyper-V-Hosts eine solche Replikation zulassen, müssen Sie diese zunächst generell aktivieren. Im Gegensatz zur aktuellen Version von VMware-Produkten, kann Hyper-V diese Replikation unabhängig vom eingesetzten Speichersystem durchführen und die Funktion steht kostenlos zur Verfügung. Mit dieser neuen Technologie lassen sich problemlos virtuelle Server im laufenden Betrieb zwischen verschiedenen Hyper-V-Hosts replizieren.

Auf diese Weise können Sie aber auch Testumgebungen mit produktiven Daten aufbauen, oder für eine Hochverfügbarkeitslösung sorgen, indem Sie Server replizieren lassen. Die Computer müssen dabei nicht in einem Cluster konfiguriert sein, es reicht aus, wenn auf dem Hyper-V-Host Windows Server 2012 R2 und Hyper-V installiert ist. Die entsprechende Replikation steuern Sie über einen Assistenten, den Sie über das Kontextmenü von virtuellen Servern im Hyper-V-Manager starten.

Abbildg. 7.1 Konfigurieren der Hyper-V-Replikation für einen virtuellen Server



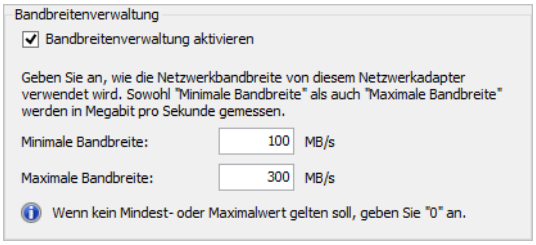
Für eine bessere Leistung im Netzwerk dürfen virtuelle Server jetzt mehr auf Hardwarefunktionen von Netzwerkkarten zugreifen, was das Tempo enorm beschleunigen kann. In den Einstellungen von virtuellen Netzwerkkarten lässt sich die Netzwerkbandbreite von Servern eingrenzen und unerwünschte DHCP- oder Routerpakete lassen sich blockieren. Dies soll verhindern, dass virtuelle Server unerwünscht als DHCP-Server oder Router agieren und das Netzwerk beeinträchtigen.

Kaufen Unternehmen neue Hostsysteme für Hyper-V, sollten diese darauf achten, genügend Netzwerkkarten in den Server einzubauen. Wichtig ist dabei auch, dass die Karten die neuen Funktionen in Hyper-V unterstützen.

Mehr Sicherheit und bessere Bandbreitenverwaltung

In den Netzwerkeinstellungen lassen sich unter anderem Berechnungen für IPsec vom Prozessor des virtuellen Servers auf die physische Netzwerkkarte auslagern.

Abbildg. 7.2 Bandbreitenverwaltung in Windows Server 2012 R2



Eine weitere Einstellung ist *E/A-Virtualisierung mit Einzelstamm*. Hierbei handelt es sich ebenfalls um physische Funktionen von Netzwerkkarten, die jetzt auch in Hyper-V funktionieren. Netzwerkkarten, die diese Funktion unterstützen, stellen für virtualisierte Umgebungen implementierte E/A-Kanäle zur Verfügung, mit denen sich die Karte gegenüber virtualisierten Servern wie mehrere Netzwerkkarten verhält. SR-IOV ist vor allem bei E/A-intensiven Anwendungen interessant, also durchaus auch für SQL Server 2012.

Bei den erweiterten Features finden Sie die beiden neuen Einstellungen *DHCP-Wächter* und *Routerwächter*. Die Einstellungen sollen verhindern, dass virtuelle Server unkontrolliert als DHCP-Server oder als Router agieren.

Ebenfalls neu seit Windows Server 2012 ist das Festplattenformat VHDX. Dieses erlaubt in Hyper-V 3.0 eine maximale Festplattengröße von 64 TB. Hyper-V unter Windows Server 2008 R2 unterstützte mit VHD-Dateien nur 2 TB. Interessant in diesem Bereich ist auch die Möglichkeit, 4 KB-Sektoren für Festplatten zu verwenden. Auch Windows Server 2012 R2 unterstützt solche Festplatten mit großen Sektoren. Wir zeigen Ihnen im folgenden Abschnitt die Hintergründe dazu. Das neue Festplattenformat für 4 KB-Festplatten trägt die Bezeichnung *Advanced Format Technology*. Es ermöglicht physische Festplatten mit einer Sektorgröße von 4 KB. Bisher nutzen Festplatten eine Größe von 512 Byte. Die erhöhte Sektorgröße ist notwendig, damit Hersteller Festplatten mit höherer Speicherkapazität herstellen können. Daher muss auch Hyper-V das neue Format unterstützen. Davon profitiert auch das Betriebssystem, da Windows Server 2012 R2 ebenfalls 4 KB große Speichereinheiten nutzt. Das heißt, logische Sektoren passen in einen einzelnen physischen Sektor und sind nicht mehr verteilt.

Außerdem bietet Hyper-V in Windows Server 2012 R2 die Unterstützung von 4 KB-Festplattensektoren. Das heißt, Sie können virtuelle Festplatten effizient auf 4 KB-Festplatten erstellen. Zusätzlich unterstützt Hyper-V auch virtuelle Festplatten, die auf 512e-physischen Festplatten erstellt wurden. Da nicht alle Software und Hardware das neue Format unterstützen, melden sich viele Festplatten mit 512 Bit-Emulation am System an, auch 512e genannt. Die Firmware der Festplatten speichern ankommende Datenpakete dann entsprechend in den tatsächlich vorhandenen 4 KB-Sektoren. Auch bei diesen Vorgängen ist Windows Server 2012 R2 wesentlich schneller.

Beim Umgang mit diesen Festplatten ist es wichtig, dass die verwendeten Sektoren des Betriebssystems teilbar durch die vorhandenen physischen Sektoren sind. Ist das nicht der Fall, wird ein logischer Sektor des Betriebssystems auf mehreren physischen Sektoren verteilt. Darunter kann enorm die Leistung des Systems leiden.

Schnellerer Datenfluss in Rechenzentren

Ebenfalls verbessert ist der Umgang mit SANs in Windows Server 2012 R2. Hier lassen sich Speicherplätze direkt den virtuellen Servern zuordnen. In Hyper-V können Sie mit virtuellen Fibrechannels virtuellen Servern direkt Zugriff auf Fibrechannels in SAN gewähren. Das verbessert die Leistung und erlaubt die Anbindung von Hyper-V-Hosts an mehrere SANs. Vor allem bei der Livemigration kann das einen echten Mehrwert bieten.

Ebenfalls eine wichtige Funktion in diesem Bereich ist die Unterstützung von ODX, auch Offloaded Data Transfer genannt. Den Datenverkehr zwischen SAN und Betriebssystem speichert Windows Server 2012 R2 in einem Puffer. Bei sehr großen Datenmengen kann Windows Server 2012 R2 solche Aktionen auch ohne das Hostsystem direkt mit der Steuerungssoftware des SANs erledigen. Das verbessert deutlich die Leistung des Systems. Für diesen Austausch nutzt Windows Server 2012 R2 ODX. Die meisten SAN-Hersteller nutzen derzeit schon die Technik. Vor allem Hyper-V profitiert von dieser Technik, wenn zum Beispiel virtuelle Server verschoben werden sollen, zum Beispiel zur Livemigration oder der Replikation.

Erweiteter Sitzungsmodus und mehr

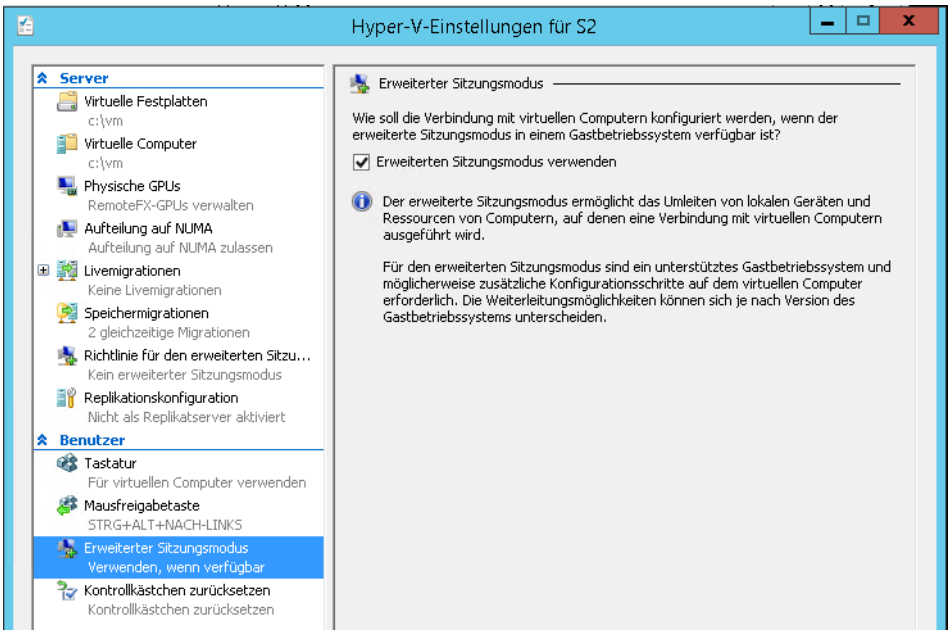
In Windows Server 2012 R2 können Sie virtuelle Festplatten auf Basis von VHDX-Dateien mehreren virtuellen Servern gleichzeitig zuordnen. Diese Funktion wird Shared VHDX genannt. Davon profitieren vor allem Unternehmen, die Windows-Cluster auf Basis virtueller Server aufbauen wollen.

Außerdem hat Microsoft die Livemigration verbessert. Während der Übertragung werden Daten komprimiert und so schneller übertragen. Die Replikation von virtuellen Servern können Sie in Windows Server 2012 R2 zwischen zwei Hyper-V-Hosts auch ohne Cluster durchführen. Das funktioniert in Windows Server 2012 R2 jetzt mit drei Knoten.

In großen Netzwerken mit 10 Gbit/s lässt sich dabei mit der Livemigration und dem verbesserten Remotezugriff auf den direkten Speicher (Remote Direct Memory Access, RDMA) zwischen Servern mit Windows Server 2012 R2 auch der Inhalt des Arbeitsspeichers austauschen. Dies beschleunigt die Livemigration noch einmal deutlich. Ebenfalls neu ist die Möglichkeit, virtuelle Server im laufenden Betrieb zu exportieren. Sie müssen die Server nicht mehr wie in Windows Server 2008 R2/2012 herunterfahren, um einen Export zu starten.

In den Hyper-V-Einstellungen von Hyper-V-Hosts müssen Sie über den Menüpunkt *Richtlinien für den erweiterten Sitzungsmodus* zunächst die Funktionen des erweiterten Sitzungsmodus aktivieren. Danach ist die Verwaltung von virtuellen Servern deutlich verbessert. Verbinden Sie sich mit einem virtuellen Server, verwendet Windows Server 2012 R2 zukünftig direkt das RDP-Protokoll, ohne dass Sie dieses auf dem virtuellen Computer zunächst aktivieren müssen. Dadurch lässt sich die Fernwartung beschleunigen und bietet die Möglichkeit, Daten per Drag & Drop auszutauschen.

Abbildg. 7.3 Der erweiterte Sitzungsmodus verbessert die Verwaltung von virtuellen Servern



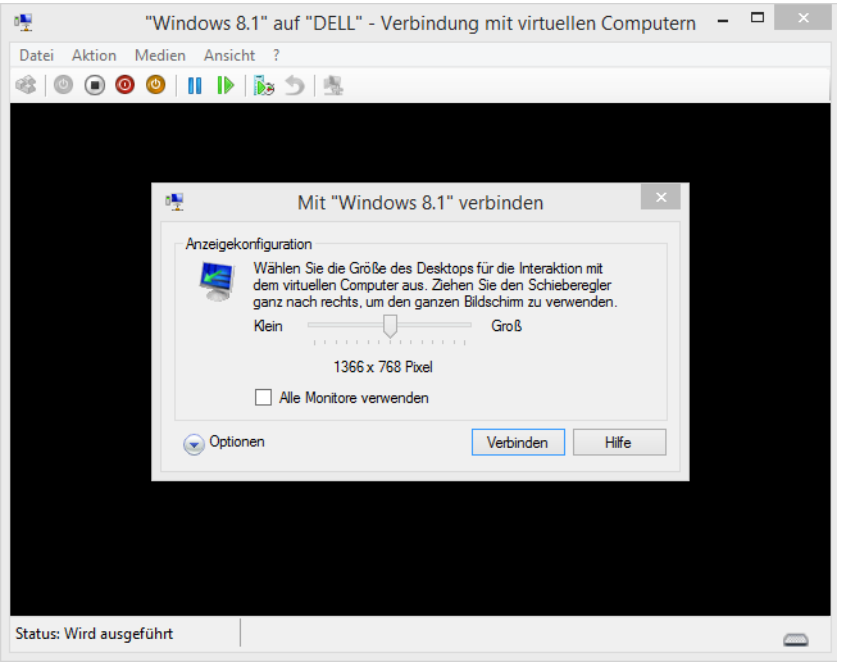
Nachdem der erweiterte Sitzungsmodus aktiviert und die Maschine neu gestartet ist, können Sie auswählen, welche Auflösung bei der Verbindung zum virtuellen Server genutzt werden soll. Dazu muss in der virtuellen Maschine das RDP-Protokoll nicht aktiviert sein.

Über *Weitere Optionen* und durch Auswahl von *Lokale Ressourcen* lässt sich auch die Zwischenablage nutzen sowie ein Drucker innerhalb der Sitzung verbinden. Microsoft nutzt für VM-Connect ab jetzt eine erweiterte Version des RDP-Protokolls. Dieses ist vor allem bei WAN-Verbindungen deutlich schneller. Nach der Verbindung über die erweiterten Optionen lassen sich diese Funktionen im VM-Connect-Fenster über *Ansicht/Erweiterte Sitzung* oder das neue Symbol im Menü *Ansicht* aktivieren oder deaktivieren.

Der größte Vorteil der erweiterten Sitzung ist (neben der deutlich höheren Geschwindigkeit) die Möglichkeit, Dateien über die Zwischenablage mit dem Host auszutauschen. Dadurch lässt sich vor allem die Installation neuer Anwendungen erheblich beschleunigen.

Beim Exportieren von virtuellen Servern dürfen diese jetzt gestartet bleiben. Auch Snapshots, jetzt Prüfpunkte genannt, dürfen vorhanden sein und werden beim Export berücksichtigt und mit exportiert.

Abbildg. 7.4 Mit der erweiterten Sitzung können sie auch Daten zwischen Host und Gast über die Zwischenablage austauschen

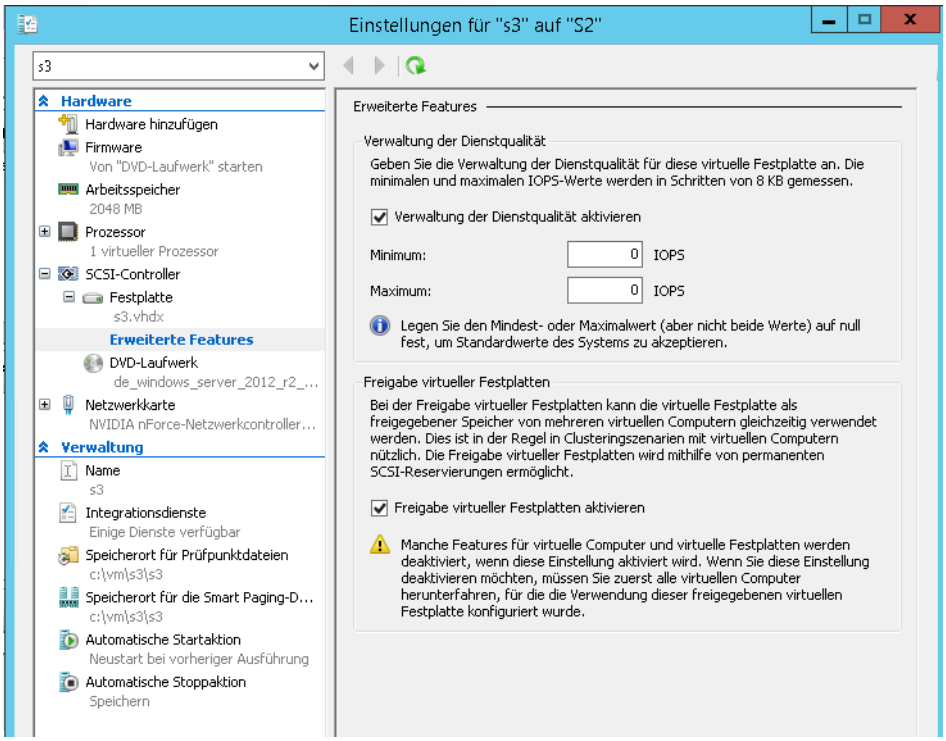


Virtuelle Server unterstützen in Windows Server 2012 R2 das UEFI-System und auch Secure Boot in UEFI. Dazu müssen Sie beim Erstellen einer virtuellen Maschine im neuen Fenster aber *Generation 2* als VM-Typ auswählen. Nach der Erstellung ist eine Änderung nicht mehr möglich.

In den Einstellungen virtueller Server lassen sich auch Festlegungen für das UEFI-System treffen. Zusätzlich können Sie die Secure-Boot-Funktion nutzen, um das Eindringen von Viren während des Bootvorgangs zu verhindern. Diess können jedoch nur virtuelle Maschinen (VMs) der zweiten Generation. Diese VMs können auch von virtuellen SCSI-Platten booten. VMs der ersten Generation unterstützen nur Bootvorgänge von virtuellen IDE-Platten. Linux lässt sich in Windows Server 2012 R2 besser als virtueller Gast nutzen. Sie können Dynamic Memory jetzt auch in Linux einsetzen.

Für virtuelle Festplatten lassen sich jetzt auch Bandbreitenbegrenzungen vorgeben, ähnlich zu den erweiterten Features für virtuelle Switches. Dadurch wird verhindert, dass ein virtueller Server eine virtuelle Festplatte zu stark auslastet. Hier lässt sich auch die Shared-VHDX-Funktion aktivieren.

Abbildg. 7.5 Virtuelle Festplatten bieten in Windows Server 2012 R2 mehr Funktionen



Virtuelle Server auf Basis der zweiten Generation nutzen keinerlei emulierte Hardware mehr, wodurch sich die Geschwindigkeit der Server deutlich erhöht. Außerdem können diese Server von virtuellen SCSI-Laufwerken oder über das Netzwerk booten. PS/2-Tastaturen und -Mäuse können Sie mit VMs der zweiten Generation nicht nutzen.

VHDX-Dateien von Servern lassen sich im laufenden Betrieb des Servers vergrößern oder verkleinern. Die Obergrenze von virtuellen Festplatten auf Basis von VHDX bleibt bei 64 TB, die von VHD-Platten bleibt bei 2 TB.

HINWEIS Virtualisieren Sie Windows Server 2012 R2 Datacenter auf einem Hyper-V-Host mit Windows Server 2012 R2 Datacenter, überprüft das Betriebssystem beim ersten Start, ob das Betriebssystem auf dem Host bereits aktiviert ist. Ist dies der Fall, aktiviert sich das Betriebssystem im Gast automatisch ebenfalls.

Hyper-V installieren und verwalten

Hyper-V installieren Sie als Serverrolle. Sie können dazu den Server-Manager verwenden oder die PowerShell. Binden Sie einen Server an System Center Virtual Machine Manager an, haben Sie ebenfalls die Möglichkeit, Hyper-V zu installieren, wenn Sie den Host anbinden. In Windows Server 2012 R2 haben Sie über den Server-Manager auch die Möglichkeit, Hyper-V remote auf Servern im Netzwerk zu installieren.

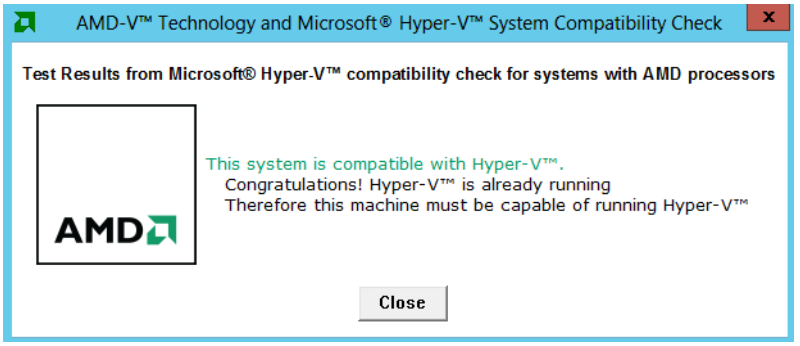
Core-Server beherrschen auch in Windows Server 2012 R2 Hyper-V. Die Verwaltung findet dann idealerweise über einen Server im Netzwerk mit grafischer Oberfläche, einer Arbeitsstation mit installierten Remoteserver-Verwaltungstools oder mit System Center Virtual Machine Manager statt. Mehr zum Thema lesen Sie in den Kapiteln 1 bis 4. Zusätzlich können Sie auch Hyper-V Server 2012 installieren. Hier ist die Serverrolle *Hyper-V* nach der Installation des Servers schon aktiviert (siehe Kapitel 2).

Voraussetzungen für den Einsatz von Hyper-V

In diesem Abschnitt gehen wir in Stichpunkten auf die einzelnen Voraussetzungen ein, die Sie erfüllen müssen, um Hyper-V einzusetzen. Sie müssen sicherstellen, dass vor der Installation im BIOS des Servers die Virtualisierungsfunktionen des Prozessors aktiviert sind. Microsoft bietet in Zusammenarbeit mit AMD und Intel zwei Tools, die beim Testen der Hyper-V-Kompatibilität helfen:

- **AMD Hyper-V Compatibility Check Utility** *http://support.amd.com/us/Pages/dynamicDetails.aspx?ListID=c5cd2c08-1432-4756-aafa-4d9dc646342f&ItemID=177* [Ms179-K07-01]
- **Intel Processor Identification Utility (Windows-Version)** *http://downloadcenter.intel.com/detail_desc.aspx?agr=n&productid=1881&dwnldid=7838* [Ms179-K07-02]

Abbildg. 7.6 AMD-Prozessoren auf Hyper-V-Kompatibilität überprüfen



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).

Sie können auch mit Bordmitteln überprüfen, ob der PC generell tauglich für Hyper-V ist. Geben Sie dazu in einer Eingabeaufforderung den Befehl *systeminfo* ein. Im unteren Bereich finden Sie *Anforderungen für Hyper-V*. Hier finden Sie Informationen, ob der PC für Hyper-V geeignet ist. *Adressübersetzung der zweiten Ebene* legt zum Beispiel fest, ob sich der Arbeitsspeicher virtualisieren lässt. Das ist für die Installation von Hyper-V notwendig.

HINWEIS Konfigurieren Sie Ihren Virenscanner auf dem Hyper-V-Server so, dass die VHD(X)- und Konfigurationsdateien der virtuellen Computer nicht gescannt werden. Vor allem beim Einsatz der Livemigration ist dies absolut notwendig, da ansonsten die Leistung des Servers leidet oder virtuelle Maschinen beschädigt werden können.

- Der Host muss so viel Arbeitsspeicher enthalten, wie Sie den virtuellen Computern zuweisen können. Die maximale Größe ist an das Betriebssystem gebunden. Für Hyper-V gelten daher nur die Einschränkungen des Betriebssystems. Windows Server 2012 R2 unterstützt bis zu 4 Terabyte (TB) Arbeitsspeicher. Damit Sie Hyper-V installieren können, muss der Server über mindestens 512 MB Speicher verfügen. Virtuellen Computern können Sie bis zu 1 TB Arbeitsspeicher zuweisen.
- Windows Server 2012 R2 muss als Betriebssystem für den physischen Host eingesetzt werden. Als kostenlose Alternative steht Hyper-V Server 2012 zur Verfügung. Dieser Server entspricht der vollwertigen Installation von Windows Server 2012 R2 als Core-Server.
- Die maximale Festplattengröße für virtuelle Festplatten beträgt 64 TB (VHDX-Dateien).

HINWEIS Achten Sie bei der Lizenzierung von Hyper-V-Servern auf die Anmerkungen zur Lizenzierung im Kapitel 1.

Hyper-V installieren

Für die Installation von Hyper-V verwenden Sie den Server-Manager und fügen Hyper-V wie andere Rollen als Serverrolle hinzu (siehe Kapitel 4). Auf herkömmlichen Servern startet der Assistent zum Hinzufügen von neuen Serverrollen. Sie können Hyper-V in Windows Server 2012 R2 auch über das Netzwerk von einem Server-Manager aus installieren. Mehr dazu lesen Sie in den Kapiteln 2, 3 und 4.

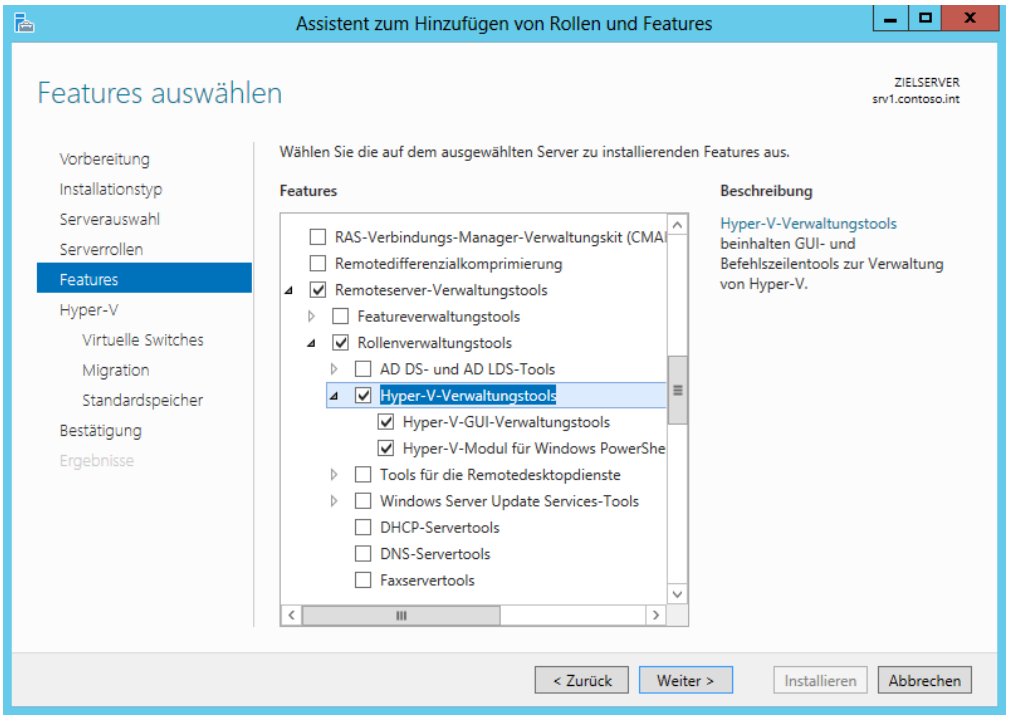
Sicherlich die einfachste Möglichkeit, um Hyper-V auf einem Server mit Windows Server 2012 R2 zu installieren, ist die Verwendung des Server-Managers. Über *Verwalten/Rollen und Features hinzufügen* wählen Sie den Server aus, auf dem Sie Hyper-V installieren wollen und anschließend die Serverrolle *Hyper-V*.

TIPP Über *Verwalten/Rollen und Features entfernen* deinstallieren Sie Hyper-V auf dem Server. Virtuelle Server bleiben beim Deinstallieren aber weiter auf dem Server gespeichert. Installieren Sie Hyper-V erneut, sind die virtuellen Server wieder verfügbar. Benötigen Sie die virtuellen Server nicht mehr, müssen Sie den Ordner mit den virtuellen Servern manuell löschen.

Bei dieser Installationsvariante hat sich im Vergleich zu Windows Server 2008 R2 nichts verändert. Neu ist bei der Installation der Serverrolle aber, dass Sie über den Assistenten auch Features installieren können. Über diesen Weg können Sie zum Beispiel die Verwaltungstools installieren. Die Installation der Verwaltungstools ist automatisch ausgewählt.

Diese können Sie so aber auch auf Servern oder Computern installieren, auf denen Sie Hyper-V nicht installiert haben, sondern von denen Sie die Server nur verwalten wollen. Sie finden die Verwaltungstools im Assistenten zum Hinzufügen von Serverrollen und Features auf der Seite *Features hinzufügen* über *Remoteserver-Verwaltungstools/Rollenverwaltungstools/Hyper-V-Verwaltungstools*. In der PowerShell installieren Sie Hyper-V und die Verwaltungstools mit *Install-WindowsFeature –Name Hyper-V –IncludeManagementTools*.

Abbildg. 7.7 Installieren der Hyper-V-Verwaltungstools in Windows Server 2012 R2



Sie können an dieser Stelle auswählen, ob Sie nur die grafische Oberfläche oder auch die PowerShell-Cmdlets installieren wollen. Mit diesen Verwaltungstools können Sie auch den kostenlosen Hyper-V Server 2012 verwalten.

Hyper-V über das Netzwerk installieren

Neu in Windows Server 2012 R2 ist die Möglichkeit, Serverrollen und Features im Server-Manager auch über das Netzwerk zu installieren. Dazu starten Sie auf einem Server mit Windows Server 2012 R2 den Server-Manager und fügen die Server hinzu, auf denen Sie Hyper-V installieren wollen. Klicken Sie dazu auf *Verwalten/Server hinzufügen* und wählen Sie die Hyper-V-Server aus.

Starten Sie anschließend die Installation von Serverrollen im Server-Manager, können Sie aus den hinzugefügten Servern denjenigen Server auswählen, auf dem Sie Hyper-V installieren wollen. Gehen Sie anschließend genauso vor, wie bei der Installation der Serverrolle auf dem lokalen Server.

Sie sehen im Assistenten zur Installation von Serverrollen oben rechts den Zielserver, auf dem Sie Hyper-V installieren. Auf dem Zielserver selbst bekommen Sie von der Netzwerkinstallation während der Installation selbst nichts mit. Sie können auch auf dem Quellserver den Assistenten zur Installation schließen. Der Installationsvorgang ist davon nicht betroffen. Auf diesem Weg können Sie den Assistenten zur Installation von Serverrollen auch mehrmals starten.

Installieren Sie die Remoteserver-Verwaltungstools für Windows 8 auf einem Computer, können Sie auch von einem PC aus über den Server-Manager Rollen wie Hyper-V installieren. Mit RSAT in Windows 7 ist das noch nicht möglich gewesen. Mehr zu diesem Thema erfahren Sie in Kapitel 3.

Abbildverwaltung für die Bereitstellung (DISM) nutzen

Neben dem Server-Manager können Sie Hyper-V auch über das Befehlszeilentool DISM installieren. Diese Funktion nutzen Sie vor allem auf Core-Servern oder zum Skripten der Installation. Das Tool DISM bietet zur besseren Automatisierung der Einrichtung und Installation von Serverrollen auch für Core-Server mit Windows Server 2012 R2 effiziente Möglichkeiten.

Die Hyper-V-Rolle installieren Sie zum Beispiel mit dem Befehl *dism /Online /Enable-Feature /FeatureName:Microsoft-Hyper-V*. Der Befehl installiert aber nicht die Verwaltungstools, sondern nur das Hyper-V-Feature. Um die Installation zu überprüfen, verwenden Sie *dism /Online /Get-FeatureInfo /FeatureName:Microsoft-Hyper-V*.

Eine Übersicht der verfügbaren Rollen erhalten Sie mit dem Befehl *dism /Online /Get-Features /Format:table*. Mit der zusätzlichen Option *|More* können Sie im Fenster manuell weiterscrollen.

PowerShell zur Installation von Hyper-V nutzen

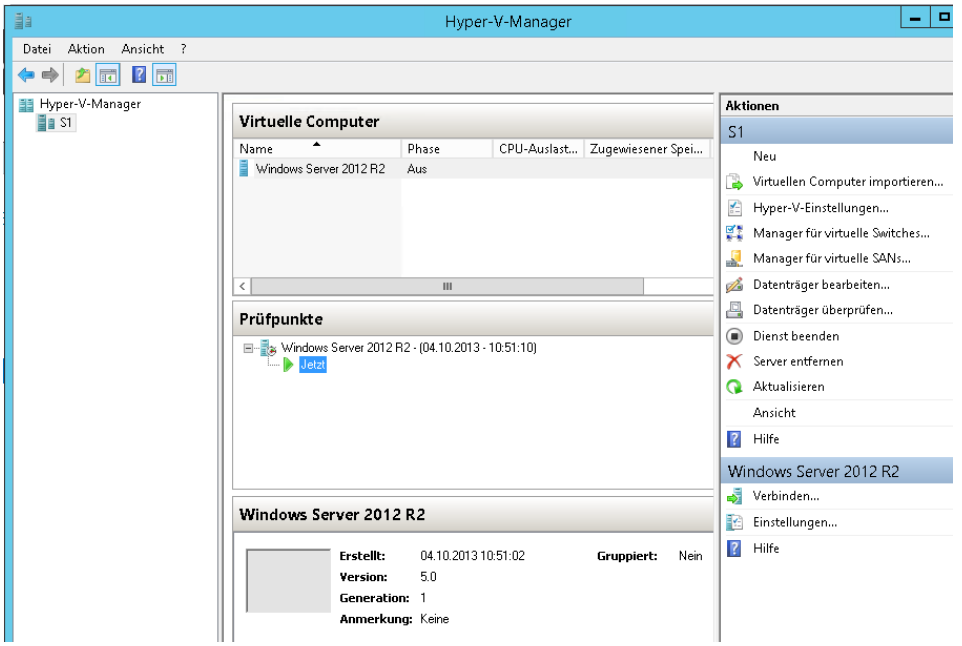
Neben dem Server-Manager und dism.exe können Sie auch die PowerShell zur Installation von Hyper-V nutzen. Mit dem Cmdlet-Aufruf *Get-WindowsFeature Hyper-V** zeigen Sie an, ob die Rolle und die Verwaltungstools bereits installiert sind. In Windows Server 2012 R2 können Sie mit *–Computername* die Installation auch auf Remoteservern im Netzwerk überprüfen. Um Hyper-V oder die Verwaltungstools zu installieren, verwenden Sie das Cmdlet *Install-WindowsFeature* (in Windows Server 2008 R2 *Add-WindowsFeature*). Mit *Install-WindowsFeature Hyper-V* installieren Sie die Serverrolle mit der Option *–IncludeManagementTools* inklusive der Verwaltungstools. Soll der Server gleich automatisch neu starten, verwenden Sie noch die Option *–Restart*. Die Verwaltungstools alleine installieren Sie mit *Install-WindowsFeature Hyper-V-Tools*.

Nach der erfolgreichen Installation müssen Sie in der Regel 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. Die ausführlichen Vorgänge zu diesem Thema lesen Sie in Kapitel 4.

Nach der Installation finden Sie auf der Startseite den *Hyper-V-Manager* vor, 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.

Über den Link *Neu* erstellen Sie einen neuen virtuellen Computer. Nach der Erstellung 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.

Abbildg. 7.8 Verwalten von Hyper-V im Server-Manager



Im nächsten Abschnitt zeigen wir Ihnen zunächst, wie Sie neue virtuelle Server mit dem Hyper-V-Manager erstellen sowie den Arbeitsspeicher, die Netzwerkverbindung und virtuelle Festplatten festlegen. Nach der Erstellung des virtuellen Computers gehen wir ausführlicher auf die Installation und Verwaltung von neuen virtuellen Computern ein. Sie können mehrere Server auf einem einzelnen physischen Host oder auf mehreren physischen Hosts virtualisieren. Der generelle Ablauf bei der Installation der Server in einer Hyper-V-Umgebung ist folgender:

1. Sie erstellen virtuelle Switches auf Basis der physischen Netzwerkkarten in Windows Server 2012 R2 (siehe auch Kapitel 6).
2. Sie erstellen und konfigurieren die virtuellen Server.
3. Sie installieren das Betriebssystem auf den virtuellen Servern. Die Installation läuft genauso ab, wie auf normalen Servern (siehe Kapitel 2).

Virtuelle Switches in Windows Server 2012 R2

Alle virtuellen Computer, die Sie erstellen, verwenden einen virtuellen Switch auf dem Windows Server 2012 R2-Computer. Dieser verbindet die virtuellen Computer mit den physischen Netzwerkkarten des Computers und erlaubt eine Kommunikation der Computer mit dem Rest des Netzwerks. Bevor Sie virtuelle Computer installieren, besteht der erste Schritt in der Konfiguration der virtuellen Switches. Dazu steht im Hyper-V-Manager der Bereich *Manager für virtuelle Switches* zur Verfügung. Wie Sie Netzwerkkarten zu Teams in Windows Server 2012 R2 zusammenfassen, lesen Sie in Kapitel 6. Setzen Sie zum Beispiel mehrere physische Netzwerkkarten ein, erstellen Sie auch

mehrere virtuelle Switches. Weisen Sie einem virtuellen Server mehrere virtuelle Switches zu, können Sie innerhalb des virtuellen Servers Teams für die virtuellen Netzwerke erstellen. Mehr dazu lesen Sie in Kapitel 6.

Für eine bessere Leistung im Netzwerk dürfen virtuelle Server in Windows Server 2012 R2 stärker auf Hardwarefunktionen von Netzwerkkarten zugreifen, was das Tempo enorm beschleunigen kann. In den Einstellungen von virtuellen Netzwerkkarten lässt sich die Netzwerkbandbreite von Servern eingrenzen und unerwünschte DHCP- oder Routerpakete lassen sich blockieren. Dies soll verhindern, dass virtuelle Server unerwünscht als DHCP-Server oder Router agieren und das Netzwerk beeinträchtigen.

Kaufen Unternehmen neue Hostsysteme für Hyper-V, sollten diese darauf achten, genügend Netzwerkkarten in den Server einzubauen. Wichtig ist dabei auch, dass die Karten die neuen Funktionen in Hyper-V unterstützen.

Network Virtualization und Extensible Switch mit Windows Server 2012 R2

Bereits mit Windows Server 2012 hat Microsoft die Möglichkeiten der Netzwerkswitches für Hyper-V deutlich erweitert und verbessert. Mit Hyper-V Network Virtualization (HNV) können Unternehmen einzelne virtuelle Netzwerke vom physischen Netzwerk trennen. Die virtuellen Server in diesen Netzwerken gehen davon aus, in einem echten physischen Netzwerk zu laufen.

Vor allem in großen Rechenzentren spielt Hyper-V Network Virtualization (HNV) eine wichtige Rolle. Allerdings profitieren auch kleinere Unternehmen von dieser Funktion. Einfach ausgedrückt erweitert HNV die Funktionen von virtuellen Servern auf die Netzwerkkonfiguration. In einem physischen Netzwerk lassen sich mehrere virtuelle Netzwerke parallel einsetzen. Diese können den gleichen oder einen anderen IP-Adressraum verwenden.

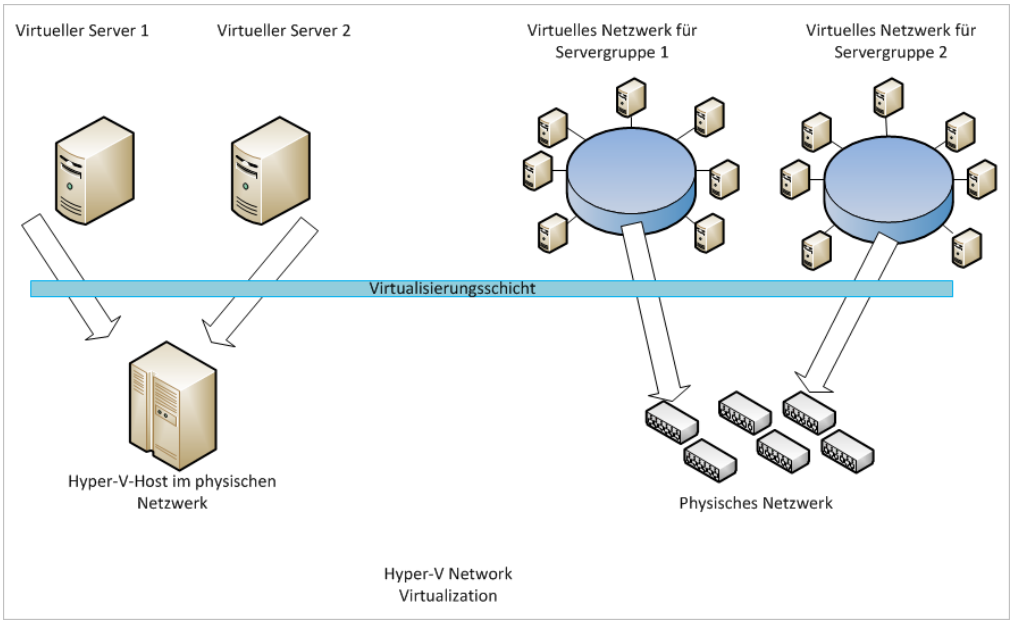
Der Datenaustausch zwischen den Netzwerken lässt sich mit HNV-Gateways einrichten. Viele Hardwareswitches von Cisco arbeiten mit dieser Konfiguration ebenfalls zusammen. Auf diesem Weg lassen sich mehrere virtuelle Netzwerke zusammenfassen, sodass Server in diesem Netzwerk kommunizieren können.

In Windows Server 2012 R2 hat Microsoft diese Möglichkeit noch erweitert und HNV deutlich verbessert und beschleunigt. Wer sich noch nicht mit HNV auseinandergesetzt hat, findet im Microsoft TechNet (*http://technet.microsoft.com/de-de/library/jj134174.aspx* [Ms179-K07-03]) umfassende Anleitungen dazu.

Eine Demo für den Einsatz von Hyper-V Network Virtualization finden Sie im Script Center von Microsoft TechNet (*http://gallery.technet.microsoft.com/scriptcenter/Simple-Hyper-V-Network-d3efb3b8/view/Discussions* [Ms179-K07-04]). Die Demo funktioniert mit Windows Server 2012 und Windows Server 2012 R2.

In Windows Server 2012 R2 können Unternehmen bereits Bandbreiten im Netzwerkbereich steuern und auch Treiber von Dritthersteller in die virtuellen Switches integrieren. Die Hyper-V Extensible Switches bieten deutlich mehr Möglichkeiten als deren Pendant in Windows Server 2008 R2 und davor. Mit Windows Server 2012 R2 will Microsoft den Drittherstellerprodukten in den Extensible Switches von Hyper-V 2012 R2 die Möglichkeit geben, ebenfalls umfassend auf die Netzwerkvirtualisierung zugreifen zu können.

Abbildg. 7.9 Mit der Network Virtualization von Hyper-V werden Netzwerke noch flexibler. Windows Server 2012 und Windows Server 2012 R2 bieten in diesem Bereich zahlreiche Neuerungen.



Hyper-V Network Virtualization (HNV) unterstützt ab Windows Server 2012 R2 auch dynamische IP-Adressen. Dies ist in großen Rechenzentren sinnvoll, um eine IP-Address-Failover-Konfiguration einbinden zu können. System Center Virtual Machine Manager 2012 R2 kann mit virtuellen Netzwerken umgehen und diese zentral steuern.

Arbeiten Unternehmen mit der HNV, werden jedem virtuellen Netzwerkadapter im Netzwerk zwei IP-Adressen zugewiesen. Die Kundenadresse (Customer Address, CA) und die Anbieteradresse (Provider Address, PA) arbeiten zusammen. Die CA ermöglicht den virtuellen Servern im Netzwerk den Datenaustausch, wie normale IP-Adresse in einem Netzwerk. Die PA dient dem Datenaustausch zwischen VM und dem Hyper-V-Host sowie dem physischen Netzwerk. Wie der Aufbau funktioniert zeigt Microsoft im TechNet (*http://technet.microsoft.com/de-de/library/jj134174.aspx* [Ms179-K07-05]).

Die erste wichtige Änderung in den virtuellen Switches von Hyper-V 2012 R2 ist die direkte Integration der Netzwerkvirtualisierung direkt in den Switch. HNV stellt keinen vorgelagerten NDIS-Filter mehr dar. Drittherstellerprodukte können auf diesem Weg direkt auf die CA zugreifen und auf PA kommunizieren. Über diesen Weg arbeiten jetzt auch virtuelle Switches und die Network Virtualization Generic Routing Encapsulation (NVGRE) zusammen. Das heißt, die Kommunikation zwischen virtuellen Netzwerkkarten und virtuellen Netzwerken ist jetzt deutlich einfacher und effizienter.

Dies gibt den Drittherstellerprodukten die Möglichkeit, über die Integration in den virtuellen Switches auf die Netzwerkvirtualisierung zugreifen zu können und mit virtuellen Servern, aber auch dem physischen Netzwerk zu kommunizieren. Der komplette Datenverkehr in den virtuellen Switches von Windows Server 2012 R2 läuft auch über die Netzwerkvirtualisierung und die integrierten Drittherstellerprodukte.

HNV ist daher keine Schnittstelle mehr zwischen Netzwerkkarten und extensible Switches, sondern integraler Bestandteil der virtuellen Switches selbst. Auch aus diesem Grund arbeiten NIC-Teams wesentlich besser mit der Netzwerkvirtualisierung zusammen.

Auf diesem Weg können große Unternehmen und Cloudanbieter auf die Berechtigungsliste (ACL) der virtuellen Switches zugreifen und Firewalleinstellungen, Berechtigungen und Netzwerkschutz für die Datencenter integrieren. Dazu bietet Windows Server 2012 R2 die Möglichkeit, auch den Port in die Firewallregeln zu integrieren, nicht nur IP- und MAC-Adresse für die Quelle und das Ziel. Diese Funktion arbeitet umfassend mit der Netzwerkvirtualisierung in Hyper-V zusammen.

Windows Server 2012 R2 unterstützt zwar bereits Teams von Netzwerkkarten, kann allerdings den Datenverkehr in Loadbalancing-Umgebungen nicht optimal zwischen den physischen Netzwerkkarten verteilen. Die neue Version kann problemlos Datenverkehr zwischen Netzwerkkarten verschieben und unterstützt für diese Funktion auch umfassend die Netzwerkkartenteams. Alles in allem ist festzustellen, dass Microsoft in der Einbindung von virtuellen Netzwerken eine echte Zukunft sieht.

Auch die Netzwerkausrüster wie Cisco sehen das so und arbeiten mit der Funktion zusammen. Sie sollten sich daher mit der Funktion vertraut machen und auf Basis der in diesem Abschnitt erwähnten Demo die Konfiguration einüben. In vielen Netzwerken kann es sinnvoll sein, bestimmte Server vom Rest des Netzwerks zu trennen oder besonders abzusichern. Cloudanbieter, egal ob groß oder klein, profitieren noch mehr von diesen Möglichkeiten. Mit HNV können Unternehmen die Netzwerke der Kunden voneinander trennen.

Hyper-V-Netzwerke optimal planen

Bei Leistungsproblemen von virtuellen Servern unter Hyper-V liegt das Problem in vielen Fällen an langsamer Kommunikation mit dem Netzwerk. Beachten Sie einige Tipps und Hinweise, lassen sich die Probleme meistens problemlos beheben. Microsoft stellt ein sehr ausführliches Whitepaper (*http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=9843* [Ms179-K07-06]) zur Verfügung, über das Administratoren die Netzwerkverwaltung von Hyper-V verstehen lernen. Die meisten Empfehlungen gelten auch noch für Windows Server 2012 R2.

Die Verbindung zwischen virtuellen Servern und dem Netzwerk führt Hyper-V über einen virtuellen Netzwerkswitch durch. Da sich die virtuellen Server die physischen Netzwerkkarten teilen müssen, besteht einiges an Optimierungspotential. Zunächst sollte jeder Server nur die Art von Netzwerkzugriff erhalten, die er benötigt. Nicht alle Server müssen mit dem Netzwerk kommunizieren können, sondern nur mit anderen Servern auf dem gleichen Host. Sie können daher verschiedene Netzwerkverbindungen für virtuelle Server erstellen.

Microsoft empfiehlt, einen eigenen Netzwerkadapter auf jedem Hyper-V-Host für die Verwaltung des Servers selbst zu verwenden. Unternehmen sollten also den Netzwerkverkehr des Hyper-V-Hosts selbst vom Netzwerkverkehr der virtuellen Maschinen trennen. Auch bei der Anbindung von Netzwerkspeicher, zum Beispiel NAS oder iSCSI, ist eine dedizierte Netzwerkkarte leistungssteigernd. Virtuelle Server, die nur wenig Netzwerkbandbreite benötigen, können Sie mit mehreren virtuellen Netzwerken zusammenfassen, bandbreitenintensive Anwendungen sollten dedizierte Netzwerkkarten und eigene externe Netzwerke erhalten.

Hyper-V unterstützt auch die Verwendung von VLANs bei Netzwerkswitches. Bei VLANs lassen sich Datenströme voneinander trennen, um die Sicherheit und die Leistung zu erhöhen. Dadurch lässt sich zum Beispiel der Netzwerkverkehr für die Verwaltung des Servers vom Netzwerkverkehr der

virtuellen Server trennen. In den Eigenschaften von Netzwerkkarten der Hyper-V-Hosts müssen Sie dazu in den erweiterten Einstellungen festlegen, mit welcher VLAN-ID im Netzwerk die Karte kommunizieren soll. Anschließend muss im Hyper-V-Manager die Netzwerkverbindung ausgewählt und ebenfalls die VLAN-ID eingegeben werden. Auch hier geben Sie die entsprechende VLAN-ID vor.

Microsoft empfiehlt beim Betrieb von Hyper-V in einem Cluster für die Kommunikation innerhalb des Clusters (Heartbeat) einen eigenen Adapter. Sie können für diesen Adapter das Protokoll *E/A-Treiber für Verbindungsschicht-Topologieerkennung* deaktivieren, das gilt auch für *Antwort für Verbindungsschicht-Topologieerkennung*. Das Protokoll *Hyper-V erweiterbarer virtueller Switch* können Administratoren für Clusternetzwerke im Heartbeat ebenfalls deaktivieren.

Haben Sie die physischen Netzwerkkarten des Computers einem virtuellen Switch zugeordnet, lassen sich diese den einzelnen virtuellen Computern zuweisen. Das erfolgt beim Erstellen der virtuellen Maschine oder nachträglich in den Einstellungen über den Bereich *Netzwerkkarte*. Die erste Einstellung besteht in der Zuweisung der virtuellen Switches. Anschließend lassen sich Einstellungen vornehmen. Verschieben Sie virtuelle Maschinen mit oder ohne Livemigration zwischen Hyper-V-Hosts, kann es passieren, dass die Netzwerkverbindung nicht mehr funktioniert, wenn sich der Name und die Konfiguration des Switches zwischen Quell- und Zielserver ändert. Überprüfen Sie daher nach Livemigrationen immer, ob die virtuelle Netzwerkkarte noch funktioniert, und starten Sie den virtuellen Server neu, falls die Netzwerkverbindung nicht funktioniert.

Virtuelle Switches agieren als Layer 2-Netzwerkswitches und erlauben auch die Einbindung von Network Device Interface Specification (NDIS)-Filter und der Windows Filtering Platform-Treiber. Auf diese Weise lassen sich auch Plug-Ins von Drittherstellern in Hyper-V einbinden, die erweiterte Netzwerk- und Sicherheitseinstellungen für virtuelle Server erlauben. Die entsprechenden Einstellungen sind über den Menübefehl *Erweiterungen* für jeden einzelnen vSwitch zu finden.

Eine weitere Einstellung ist *E/A-Virtualisierung mit Einzelstamm*. Hierbei handelt es sich ebenfalls um physische Funktionen von Netzwerkkarten, die jetzt auch in Hyper-V funktioniert. Netzwerkkarten, die diese Funktion unterstützen, stellen für virtualisierte Umgebungen implementierte E/A-Kanäle zur Verfügung, mit denen sich die Karte gegenüber virtualisierten Servern wie mehrere Netzwerkkarten verhält. SR-IOV ist vor allem bei E/A-intensiven Anwendungen interessant, also durchaus auch für SQL Server 2012.

In Windows Server 2012 R2 können Sie virtuelle Festplatten auch auf Freigaben speichern. Außerdem kann Windows Server 2012 R2 auch als NAS-Server dienen. Im neuen Betriebssystem lassen sich nicht nur iSCSI-Ziele mit dem Server verbinden, sondern Server mit Windows Server 2012 R2 können selbst auch als iSCSI-Ziel arbeiten. Wichtig für den Zugriff auf Freigaben im Netzwerk ist das Server Message Protokoll. Dieses stellt den Zugriff von Clientcomputern zum Server dar. Windows 8 und Windows Server 2012 R2 kommen dazu mit dem neuen SMB 3-Protokoll. Dieses ist vor allem für den schnellen Zugriff über das Netzwerk gedacht, wenn Daten normalerweise lokal gespeichert sein sollten.

Beispiele dafür sind SQL Server-Datenbanken oder die Dateien von Hyper-V-Computern. Diese lassen sich mit SMB 3 performant auch über das Netzwerk verwenden. Die neue Version erlaubt mehrere parallele Zugriffe auf Dateifreigaben. Das heißt einzelne Zugriffe über das Netzwerk bremsen sich nicht mehr untereinander aus. Von den schnellen Netzwerkzugriffen profitieren vor allem Windows 8 und Windows Server 2012 R2.

Für eine schnelle Kommunikation zwischen Windows Server 2012 R2 müssen Netzwerkkarten die RDMA-Funktion (Remote Direct Memory Access) unterstützen. Bei dieser Funktion können Server über das Netzwerk Daten im Arbeitsspeicher austauschen. Wichtig ist diese Funktion vor allem, wenn Sie Windows Server 2012 R2 als NAS-Server einsetzen, also iSCSI-Ziel, und auf dem Server Datenbanken von SQL Server 2012 oder virtuelle Maschinen von Hyper-V speichern.

Sind im Unternehmen mehrere Server mit Windows Server 2012 R2 im Einsatz, tauschen diese Daten über das Netzwerk mit der neuen Multichannel-Funktion aus. Mit der Funktion lassen sich von einem Server auf eine Freigabe mehrere parallele Zugriffe durchführen. Dies beschleunigt den Datenverkehr und sichert ihn auch gegen Ausfall eines einzelnen SMB-Kanals ab. Der Vorteil liegt darin, dass Serverdienste Daten auch auf Servern speichern können, nicht nur auf der eigenen Festplatte. Ein sinnvoller Einsatz dazu ist in Umgebungen mit Hyper-V-Hosts, die auf Windows Server 2012 R2 aufbauen. Dazu ist weder die Installation eines Rollendienstes notwendig noch eine Konfiguration. Diesen beschleunigten Zugriff bietet Windows Server 2012 R2 automatisch.

Damit die Funktion genutzt werden kann, müssen die Netzwerkadapter eine entsprechende Geschwindigkeit unterstützen. Microsoft empfiehlt dazu entweder die Installation eines 10-Gigabit-Adapters, oder mindestens den Einsatz von zwei 1-Gigabit-Adaptern. Für diese Funktion können Administratoren auch die neue Teamfunktion von Netzwerkkarten in Windows Server 2012 R2 nutzen. Über den Server-Manager lassen sich Netzwerkadapter zu Teams zusammenfassen, auch ohne dass die Treiber dies direkt unterstützen.

SMB Direct ist ebenfalls zwischen Servern mit Windows Server 2012 R2 aktiv. Sie müssen weder Einstellungen vornehmen noch etwas installieren. Damit diese Funktion nutzbar ist, müssen die verbauten Adapter aber die RDMA-Funktion (Remote Direct Memory Access) unterstützen. Bei dieser Funktion können Server Daten aus dem Hauptspeicher eines Systems über das Netzwerk auf einen anderen Server übertragen, der aktuell Kapazitäten frei hat. So lassen sich überlastete Server beschleunigen, indem Sie Daten auf nicht ausgelastete Server übertragen. Damit dies funktioniert, muss das Netzwerk extrem schnell sein und die Adapter müssen die Funktion nutzen können. Dies sind Adapter mit den Typen iWARP, Infiniband und RDAM over Converged Ethernet (RoCE). Von dieser Technik profitieren hauptsächlich Hyper-V und SQL Server 2008 R2/2012.

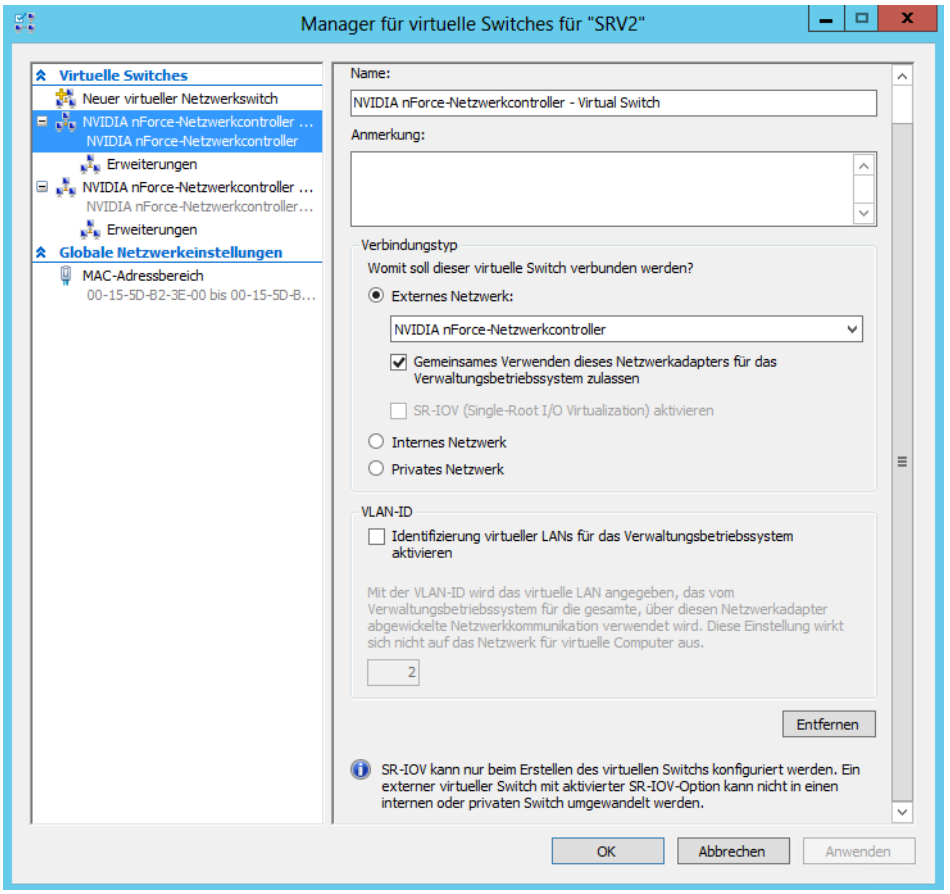
Auch Hyper-V kann in Windows Server 2012 R2 direkt auf das SMB-Protokoll zugreifen. Der Sinn ist, dass Unternehmen die virtuellen Festplatten in Hyper-V (VHDX) nicht direkt auf dem Hyper-V-Host speichern, sondern auf einer Freigabe im Netzwerk. Auf diese lässt sich dann über Hyper-V mit SMB Multichannel, SMB Direct und Hyper-V over SMP sehr schnell zugreifen. Für Unternehmen sollen dabei keinerlei Einschränkungen entstehen. Auch hochverfügbare Lösungen wie Livemigration funktionieren so. Der gemeinsame Datenträger des Clusters muss sich dann nicht mehr in einem teuren SAN befinden, sondern es reicht ein Server mit Windows Server 2012 R2 und ausreichend Speicherplatz. Auf diesem Server können auch die Konfigurationsdateien der virtuellen Server gespeichert sein und eventuell vorhandene Snapshots (Momentaufnahmen). Cluster Shared Volume (CSV), der für Hyper-V notwendige Speicherdienst für gemeinsame Datenträgern in Clustern, unterstützt das SMB 3-Protokoll und dessen neue Funktionen ebenfalls. CSV ist die Grundlage für die Speicherung von virtuellen Festplatten in Clustern.

Dazu muss ebenfalls auf beiden Servern Windows Server 2012 R2 installiert sein. Ein Server läuft mit der Hyper-V-Rolle, der andere als Dateiserver. Die Umgebung muss außerdem über ein Active Directory verfügen. Hier müssen die Domänencontroller aber nicht zwingend auf Windows Server 2012 R2 umgestellt werden. Empfohlen, aber nicht unbedingt notwendig, ist ein Cluster für Hyper-V und die Dateidienste. In diesem Fall lässt sich die Umgebung wesentlich schneller und sicherer betreiben.

Setzen Unternehmen zusätzlich zu Windows Server 2012 R2 noch SQL Server 2008 R2 oder SQL Server 2012 ein, profitieren auch hier die Datenbankserver vom neuen SMB-Protokoll. Hier gelten die gleichen Voraussetzungen wie bei Hyper-V over SMB. Ältere Editionen als SQL Server 2008 R2 können diese Funktion nicht nutzen. Auch hier ist ein Cluster wieder der beste Weg. Sinn dieser Funktion ist, dass Transaktionsprotokolle oder Datenbankdateien sowie eventuelle Sicherungen oder ausgelagerte Dateien auf Dateiservern mit Windows Server 2012 R2 ausgelagert sind. Außer-

dem hat Microsoft den Zugriff von schnellen Schreib-/Lesevorgängen deutlich optimiert. Davon profitiert vor allem SQL Server 2012. Auch den Zugriff auf Data-Warehouses hat Microsoft durch die Erhöhung des Werts für Maximum Transmission Unit (MTU) verbessert.

Abbildg. 7.10 Verwalten von virtuellen Switches



Erstellen und Konfigurieren von virtuellen Switches

Zunächst erstellen Sie für die einzelnen physischen Netzwerkkarten im Computer jeweils einen virtuellen Switch durch die Auswahl von *Neuer virtueller Switch* und dem Klick auf die Schaltfläche *Virtuellen Switch erstellen*. Im neuen Fenster wählen Sie die physische Netzwerkkarte aus, die Sie dem Switch zuweisen wollen, und legen fest, welche Art von Netzwerk Sie dem Switch zuordnen:

- **Extern** Dieses Netzwerk ermöglicht dem virtuellen Computer eine Kommunikation mit dem Netzwerk und zwischen virtuellen Computern auf dem Host. Sie können im Hyper-V-Manager immer nur ein externes Netzwerk pro verfügbarer Netzwerkkarte erstellen, aber mehrere virtuelle Computer können sich dieses externe Netzwerk und damit die Geschwindigkeit der Karte teilen.

- **Intern** Diese Netzwerke erlauben eine Kommunikation der virtuellen Computer untereinander auf dem physischen Host. Die Computer können nicht mit dem Netzwerk kommunizieren, außer mit dem Hyper-V-Host selbst und den anderen virtuellen Computer Dafür ist für diese Verbindung keine Netzwerkkarte erforderlich, da die Verbindung virtuell stattfindet.
- **Privat** Diese Netzwerke erlauben eine Kommunikation zwischen den einzelnen virtuellen Computern auf dem Host. Die Kommunikation mit dem Host selbst ist bei diesem Netzwerk nicht möglich.

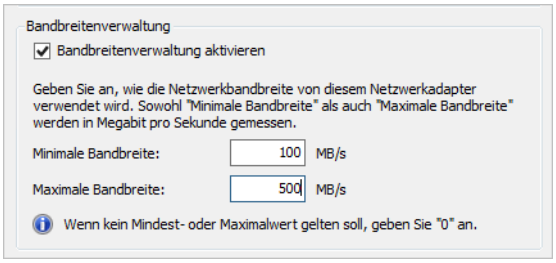
Sie können bei der Konfiguration auch festlegen, dass die verwendete physische Netzwerkkarte nur für die virtuellen Computer zur Verfügung steht, nicht für das Hostbetriebssystem selbst. Standardmäßig teilen sich virtuelle Computer und der Host die Netzwerkverbindung.

Sie können die Einstellungen jederzeit nachträglich anpassen. Haben Sie mehrere Netzwerkkarten im Hyper-V-Host verbaut, können Sie mehrere virtuelle Switches auf Basis dieser Karten erstellen. Für die virtuellen Switches können Sie das NIC-Teaming aktivieren und dann in den virtuellen Servern NIC-Teams erstellen (siehe Kapitel 6).

Haben Sie die physischen Netzwerkkarten des Computers einem virtuellen Switch zugeordnet, lassen sich diese anschließend den einzelnen virtuellen Computern als virtueller Netzwerkadapter zuweisen. Dies erfolgt beim Erstellen der virtuellen Maschine oder nachträglich in den Einstellungen über den Bereich *Netzwerkkarte*. Die erste Einstellung besteht in der Zuweisung des virtuellen Switches. Anschließend lassen sich Einstellungen vornehmen.

In den Eigenschaften steht die Steuerung der Bandbreite zur Verfügung. Auf diese Weise lassen sich die Netzwerkgeschwindigkeiten von virtuellen Computern genauer steuern. Diese Vorgaben können Sie jederzeit in den Einstellungen der virtuellen Computer anpassen, wenn Sie einen virtuellen Computer erstellt haben.

Abbildg. 7.11 Verwalten der virtuellen Netzwerkkarte für einen virtuellen Computer



Interessant sind unterhalb der Einstellungen für die Netzwerkkarten noch die beiden Bereiche *Hardwarebeschleunigung* und *Erweiterte Features*. Bei der Hardwarebeschleunigung können Sie den virtuellen Computern erlauben, bestimmte Berechnungen direkt an die physische Netzwerkkarte weiterzugeben. Im unteren Bereich lassen sich noch Berechnungen für IPsec vom Prozessor des virtuellen Servers auf die physische Netzwerkkarte auslagern. Dadurch beschleunigt sich die Systemleistung des Servers und die Netzwerkgeschwindigkeit enorm.

Innerhalb der erweiterten Features finden Sie die beiden neuen Einstellungen *DHCP-Wächter* und *Routerwächter*. Die Einstellungen sollen verhindern, dass virtuelle Server unkontrolliert als DHCP-Server oder als Router agieren. Außerdem erlauben Sie an dieser Stelle, ob die virtuelle Netzwerkkarte als Mitglied eines NIC-Teams konfiguriert werden kann (siehe Kapitel 6).

Nach der Erstellung der virtuellen Netzwerke finden Sie auf dem Host in den Netzwerkverbindungen die erstellten Verbindungen wieder. Um die Netzwerkverbindungen anzuzeigen, geben Sie *ncpa.cpl* auf der Startseite ein. Wichtig in diesem Bereich ist, dass Sie zukünftig IP-Einstellungen nicht mehr in der physischen Netzwerkverbindung vornehmen, sondern in den Einstellungen des virtuellen Switches. Diese verwendet zukünftig auch der physische Windows Server 2012 R2-Host für die Kommunikation mit dem Netzwerk, wenn Sie keine dedizierte Netzwerkkarte konfiguriert haben.

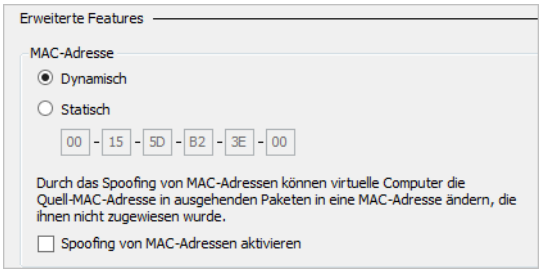
TIPP Sie können virtuelle Switches auch in der PowerShell erstellen und verwalten. Die entsprechenden Cmdlets finden Sie am schnellsten, wenn Sie in der PowerShell *Get-Command *vmswitch** eingeben.

Neben den Switches können Sie auch die virtuellen Netzwerkadapter in der PowerShell steuern. Hier sehen Sie die Befehle mit *Get-Command *vmnetworkadapter**.

MAC-Adressen optimal für Hyper-V konfigurieren

Extrem wichtig sind die Einstellungen für virtuelle MAC-Adressen in den Einstellungen der virtuellen Netzwerkkarten. Hier müssen Sie bezüglich der Livemigration und vor allem der Aktivierung des Betriebssystems auf jeden Fall Einstellungen vornehmen, da Sie ansonsten ständig die Server neu aktivieren müssen. Außerdem spielen diese Einstellungen vor allem in NLB-Clustern mit Exchange Server und auch für SharePoint Server eine sehr wichtige Rolle.

Abbildg. 7.12 Verwalten der MAC-Adressen in Windows Server 2012 R2 für virtuelle Server



Im Bereich *MAC-Adresse* lässt sich der dynamische MAC-Bereich festlegen, den die virtuellen Netzwerkkarten der Server erhalten. Für virtuelle Server lassen sich aber auch statische MAC-Adressen festlegen. Das ist wichtig bei einem Betrieb in einem Cluster. Verschieben Sie virtuelle Server zwischen den Clusterknoten, ändern sich beim Neustart die MAC-Adressen, da jeder Knoten seinen eigenen Pool hat. Das kann Probleme mit der Windows-Aktivierung geben sowie mit Netzwerklastenausgleichs-Clustern. Im MSDN-Beitrag auf der Seite *http://blogs.msdn.com/b/virtual_pc_guy/archive/2010/05/14/hyper-v-and-dynamic-mac-address-regeneration.aspx* [Ms179-K07-07] finden Sie dazu umfangreiche Informationen. Jeder Hyper-V-Host hat einen eigenen Pool aus dynamischen MAC-Adressen. Eine solche Änderung wirkt sich an vielen Stellen aus.

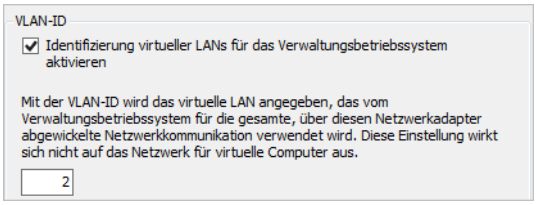
Es kann sein, dass Sie das Betriebssystem neu aktivieren müssen oder ein virtueller NLB-Cluster funktioniert nicht mehr. Microsoft beschreibt diesen Fehler auf der Webseite *http://support.microsoft.com/kb/953828/en-us* [Ms179-K07-08] noch genauer. Aus diesem Grund ist es sehr empfehlenswert, die statische Zuordnung von MAC-Adressen zu aktivieren. Sie finden diese Einstellung in den erweiterten Features im Bereich *Netzwerkkarte* der einzelnen virtuellen Server im Hyper-V-Manager.

Virtuelle LANs (VLAN) und Hyper-V

Hyper-V in Windows Server 2012 R2 unterstützt auch die Verwendung von VLANs. Bei solchen Netzwerken lassen sich Datenströme voneinander trennen, um die Sicherheit und die Leistung zu erhöhen. Die Technik muss aber direkt im Netzwerk integriert sein. Switches und Netzwerkkarten müssen die Funktion unterstützen. Dadurch lässt sich zum Beispiel der Netzwerkverkehr für die Verwaltung des Servers vom Netzwerkverkehr der virtuellen Server trennen.

Damit die Anbindung funktioniert, müssen Sie in den physischen Netzwerkkarten der Hyper-V-Hosts in den erweiterten Einstellungen der Netzwerkkarte festlegen, zu welcher VLAN-ID die Karte gehören soll. Anschließend starten Sie im Hyper-V-Manager den Manager für virtuelle Switches und wählen die Netzwerkverbindung aus, die Sie an das VLAN anbinden wollen. Auch hier geben Sie die entsprechende VLAN-ID vor.

Abbildg. 7.13 Konfigurieren der VLAN-Anbindung im Hyper-V-Manager



Dazu müssen Sie aber zunächst die Option *Identifizierung virtueller LANs für das Verwaltungsbetriebssystem aktivieren* setzen. Nachdem Sie die ID angegeben haben, fließt der Datenverkehr von dieser Verbindung über die entsprechende ID.

Auch interne Netzwerke in Hyper-V unterstützen die VLAN-Konfiguration. Zusätzlich können Sie auch virtuelle Server an VLANs anbinden. Dazu müssen Sie in den Einstellungen der virtuellen Server über die Eigenschaften der virtuellen Netzwerkkarten ebenfalls die VLAN-ID angeben. Wollen Sie, dass ein virtueller Server mit mehreren VLANs kommunizieren kann, fügen Sie dem Server einfach mehrere virtuelle Netzwerkkarten hinzu und konfigurieren das entsprechende VLAN.

Durch diese durchgehende Unterstützung von VLANs können Sie bei entsprechend kompatiblen Switches zum Beispiel Testumgebungen aufbauen oder Hyper-V-Hosts logisch voneinander trennen, auch wenn diese im selben Netzwerk konfiguriert sind.

HINWEIS Netzwerkkarten-Teams unterstützen ebenfalls die Anbindung an VLANs (siehe Kapitel 6). Verwenden Sie NIC-Teams in virtuellen Servern, empfiehlt Microsoft, die VLAN-Anbindung direkt über den virtuellen Switch durchzuführen, nicht für das virtuelle NIC-Team.

Virtuelle Server erstellen und installieren

Virtuelle Switches sind auf dem Hyper-V-Host hinterlegt und lassen sich während der Erstellung von virtuellen Servern oder auch nachträglich anpassen. Dazu erstellen Sie für virtuelle Server eine neue virtuelle Netzwerkkarte und verbinden diese mit dem virtuellen Server. Der virtuelle Switch ist wiederum mit der physischen Netzwerkkarte des Servers verbunden.

TIPP Sie sollten die Festplatten der virtuellen Server als Festplatten mit fixer Größe erstellen, nicht als dynamische Festplatten. Dies erhöht deutlich die Leistung der virtuellen Server. Microsoft empfiehlt eine solche Konfiguration auch für Exchange.

Virtualisierung von Domänencontrollern

Mit Snapshots (Momentaufnahmen) lassen sich virtuelle Server zu einem bestimmten Zeitpunkt sichern und wiederherstellen. Bei Domänencontrollern sichern Snapshots allerdings auch die Active Directory-Datenbank. Setzen Sie auf einem Domänencontroller einen Snapshot zurück, kann es zu Inkonsistenzen der Active Directory-Datenbank kommen, die auch die anderen Domänencontroller beeinflusst. Dies liegt daran, dass in Active Directory alle Objekte eine bestimmte Nummer besitzen, die Update Sequence Number (USN). Jeder Domänencontroller verfügt über eine eigene Liste dieser USNs und befindet sich auch selbst in dieser Liste. Setzen Sie einen Snapshot zurück, ändern sich USNs zahlreicher Objekte, was mit hoher Wahrscheinlichkeit zu Inkonsistenzen führt. In jedem Fall aber trennen die anderen Domänencontroller den wiederhergestellten Domänencontroller vom Netzwerk.

Durch die Neuerungen des Active Directorys in Windows Server 2012 und Hyper-V lassen sich Domänencontroller leichter mit Windows Server 2012 R2 virtualisieren. Das Erstellen von Snapshots für Domänencontroller stellt kein Problem mehr dar. Hyper-V unterstützt ab Windows Server 2012 virtuelle Domänencontroller standardmäßig, das gilt auch für Windows Server 2012 R2.

Um einen virtuellen Domänencontroller mit Windows Server 2012 R2 zu klonen, sind keine Zusatztools notwendig, sondern Sie kopieren einfach die virtuelle Maschine und weisen dem Klon einen neuen Namen zu. Auf Basis der neuen Generation-ID in Windows Server 2012 R2 und deren Unterstützung in Hyper-V erkennt der neue Server Active Directory und bindet sich problemlos ein.

Zeitsynchronisierung über Hyper-V deaktivieren

Standardmäßig versorgen sich virtuelle Server über den entsprechenden Hyper-V-Host mit der Uhrzeit. Auch das kann bei Domänencontrollern zu Problemen führen. Auf jedem virtuellen Computer installiert Hyper-V automatisch die Integrationsdienste. Dabei handelt es sich um ein Softwarepaket, welches die Leistung virtueller Server deutlich verbessert. Rufen Sie die Einstellungen auf und klicken Sie auf *Integrationsdienste*. Hier können Sie einstellen, ob sich die virtuellen Server mit dem Host synchronisieren sollen. Für virtuelle Windows-Server in Active Directory-Domänen sollten Sie diese Synchronisierung deaktivieren, da durch die Zeitsynchronisierung Inkonsistenzen auftreten können. Vor allem bei der Virtualisierung von SharePoint 2010, Exchange Server oder virtuellen Domänencontrollern liegt in dieser Konfiguration eine häufige Fehlerquelle.

Da die Server Mitglied einer Domäne sind, synchronisieren diese die Zeit mit einem Domänencontroller, genauer gesagt dem Domänencontroller mit der PDC-Masterrolle. Diesen Domänencontroller lassen Sie am besten mit einer Atomuhr im Internet oder einer Funkuhr synchronisieren. In Active Directory sind alle Domänencontroller gleichberechtigt.

Domänencontroller im Cluster

Betreiben Sie Hyper-V in einem Cluster, haben Sie die Möglichkeit, virtuelle Server zwischen den Knoten zu verschieben. Dabei können Sie Server mit der Livemigration so verschieben, dass diese immer aktiv bleiben, da Hyper-V auch den Inhalt des Arbeitsspeichers zwischen den Knoten verschiebt. Allerdings beherrscht die Livemigration in Windows Server 2008 R2 nur das gleichzeitige Verschieben eines virtuellen Servers auf einmal.

Befinden sich einem Hyper-V-Cluster mehrere Server einer Domäne, besteht die Gefahr, dass beim Verschieben Domänenmitglieder vor den Domänencontrollern verschoben werden und unter Umständen online sind, während der Domänencontroller noch offline ist. Daher sollten Sie immer zuerst die Domänencontroller verschieben, niemals zuerst die normalen Mitgliedsserver. Windows Server 2012 R2 kann virtuelle Server im Cluster priorisieren und dafür sorgen, dass Domänencontroller zuerst verschoben werden.

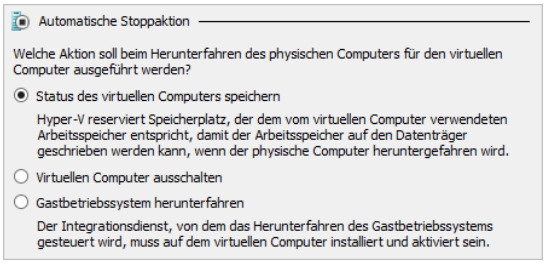
Automatisches Starten und Herunterfahren

In den Einstellungen von virtuellen Maschinen sollten Sie festlegen, wie sich der virtuelle Server beim Herunterfahren oder Starten des Hostsystems verhalten soll. Hier gelten die gleichen Probleme wie bei der Livemigration im Cluster. Bei unkontrolliertem Start, booten die einzelnen Computer nicht immer in der richtigen Reihenfolge.

Sie sollten daher beim Neustarten des Hosts auch die virtuellen Server herunterfahren lassen und beim Starten des Hosts manuell starten. Microsoft empfiehlt als Einstellung für *Automatische Stoppaktion* die Option *Gastbetriebssystem herunterfahren*. Die Speicherung des Zustands empfiehlt Microsoft nicht, da dadurch die Synchronisierung der Active Directory-Datenbank zwischen den Domänencontrollern gestört wird. Das Herunterfahren ist die optimalste Einstellung, wenn der Host neu gestartet werden muss.

Beim Herunterfahren schließt ein Domänencontroller alle noch offenen Synchronisierungsvorgänge ab, sodass beim erneuten Start keine Inkonsistenzen durch veraltete Daten entstehen können. Als automatische Startaktion empfiehlt Microsoft entweder keine Aktion oder die Einstellung, dass der Server neu starten soll, wenn er beim Herunterfahren gestartet war. Allerdings sollten Sie in diesem Fall darauf achten, dass andere Server nicht auch automatisch starten, wenn Sie von den Domänencontrollern abhängig sind.

Abbildg. 7.14 Konfigurieren der automatischen Stoppaktion für Domänencontroller



Dedizierte Netzwerkverbindungen einsetzen

Microsoft empfiehlt, einen Netzwerkadapter auf jedem Hyper-V-Host für die Verwaltung des Servers zu verwenden. Diese Vorgehensweise dient auch bei der Anbindung von Netzwerkspeicher, zum Beispiel NAS oder iSCSI. Auch hier sollten Sie für jede Verbindung eine eigene Netzwerkkarte auf dem Hyper-V-Host zur Verfügung stellen.

Diese Optimierung sollten Sie auch auf die virtuellen Hyper-V-Server ausdehnen. Domänencontroller sollten immer effizient zur Verfügung stehen, da im Active Directory ansonsten auch andere Serverdienste langsam reagieren. Die meisten Serverdienste benötigen ständige Authentifizierungen an Domänencontrollern. Daher sollten die Domänencontroller idealerweise eine eigene Netzwerk-

karte mit eigenem virtuellem Switch verwenden. Lassen Sie nicht alle Domänencontroller an der gleichen Karte laufen, da ansonsten die Gefahr besteht, dass bei Ausfall einer Karte alle Domänencontroller gleichzeitig nicht mehr verfügbar sind.

Keine differenzierende virtuelle Festplatten verwenden

In Hyper-V haben Sie die Möglichkeit, einem Gastsystem eine differenzierende virtuelle Festplatte zuzuweisen. Für Domänencontroller ist das nicht empfohlen, da sich solche Festplatten zu leicht wieder in den Ursprungszustand zurückversetzen lassen. Hier gibt es das gleiche Problem wie mit den Snapshots. Wenn Sie eine differenzierende Festplatte auswählen, erstellt Hyper-V auf Basis einer bereits vorhandenen virtuellen Festplatte eine neue Festplatte. Damit können Sie von bereits vorhandenen virtuellen Festplatten ein Abbild erzeugen. Microsoft empfiehlt zunächst, 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, also auch die Daten von Active Directory.

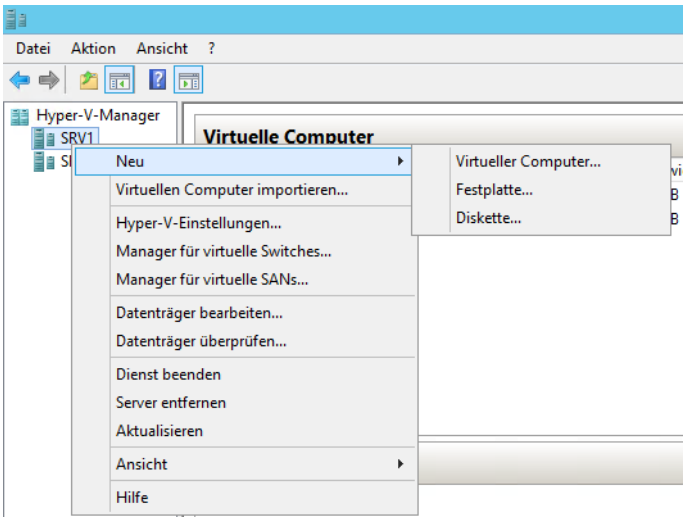
Dazu werden alle Schreibzugriffe des Gasts auf die Differenzplatte umgeleitet. Lesezugriffe kombinieren den Inhalt der Differenzplatte und den Inhalt der zugrundeliegenden virtuellen Festplatte, ohne dass der Gast etwas davon bemerkt. Die zugrundeliegende Festplatte wird nicht mehr verändert, und die Differenzplatte bleibt relativ klein, da sie nur Änderungen enthält. Eine fertige Basisinstallation kann von mehreren virtuellen Maschinen (VMs) gleichzeitig verwendet werden, indem Sie mehrere Differenzplatten erstellen, die dieselbe virtuelle Festplatte verwenden. Dadurch sparen Sie sich viel Zeit und Platz beim Klonen von virtuellen Maschinen. Was für herkömmliche Server geeignet ist, kann für Domänencontroller daher extrem schädlich sein.

Per Hyper-V-Manager virtuelle Maschinen erstellen

Nachdem Sie die virtuellen Switches für den virtuellen Computer angelegt haben, erstellen Sie die Computer, die Sie virtualisieren wollen. Dazu können Sie als Installationsmedium entweder eine DVD auswählen oder eine ISO-Datei. Um virtuelle Computer zu erstellen, gehen Sie vor, wie nachfolgend erläutert.

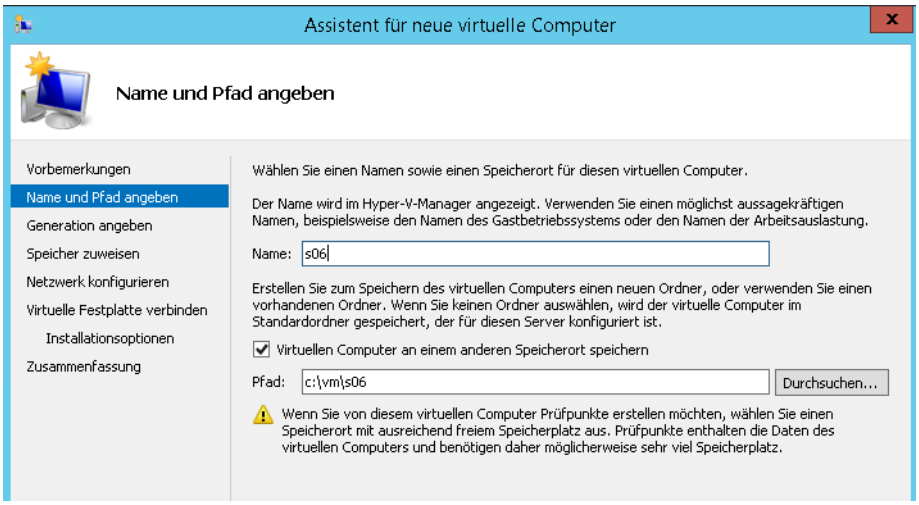
1. Starten Sie den Hyper-V-Manager über die entsprechende Kachel auf der Startseite. Warten Sie, bis der Manager eine Verbindung zum lokalen Computer aufgebaut hat. Sie können sich auch von einem anderen Server oder Computer aus mit dem Hyper-V-Host verbinden. Mehr zu diesem Thema finden Sie im Kapitel 3 und 4.
2. Klicken Sie anschließend auf *Neu/Virtueller Computer* oder verwenden Sie das Kontextmenü des Hosts zum Erstellen eines virtuellen Computers.
3. Geben Sie auf der nächsten Seite den Namen des Computers ein. Der Name hat nichts mit dem eigentlichen Computernamen zu tun. Hierbei handelt es sich lediglich um den Namen im Hyper-V-Manager. Es bietet sich aber an, den gleichen Namen zu verwenden.

Abbildg. 7.15 Starten des Assistenten zur Erstellung von virtuellen Servern



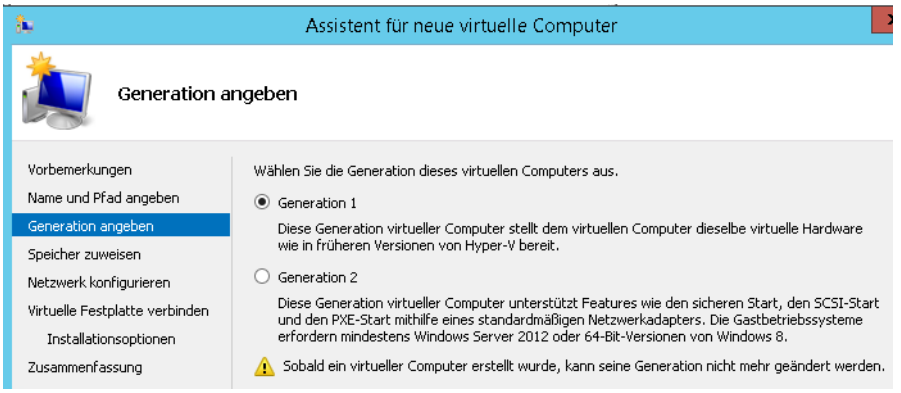
4. Aktivieren Sie das Kontrollkästchen *Virtuellen Computer an einem anderen Speicherort speichern*. Sie können diesen Ordner im Hyper-V-Manager über *Hyper-V-Einstellungen* festlegen. Hier nehmen Sie darüber hinaus weitere Einstellungen vor, die für Hyper-V selbst und alle virtuellen Computer gemeinsam gelten.
5. Wählen Sie den Ordner aus, in dem Sie die Daten des virtuellen Computers speichern wollen. Sie sollten für jeden Computer einen eigenen Pfad verwenden.

Abbildg. 7.16 Auswählen des Namens sowie des Speicherorts für den virtuellen Computer



Danach wählen Sie aus, ob der virtuelle Server eine Generation 1-VM sein soll oder die neuen Funktionen von Generation 2-VMs erfüllt. Wir sind zu Beginn des Kapitels bereits auf das Thema eingegangen. Achten Sie aber darauf, dass Sie die Generation eines virtuellen Servers nicht mehr ändern können.

Abbildg. 7.17 Auswählen des Generation-Typs eines neuen virtuellen Servers



Wählen Sie auf der nächsten Seite aus, wie viel Arbeitsspeicher Sie dem Computer zuweisen wollen. Generell sollten Sie darauf achten, dass der gemeinsame Arbeitsspeicher aller virtueller Server nicht den physischen Speicher des Hosts überschreiten sollte. Der Arbeitsspeicher des virtuellen Computers lässt sich auch nach der Installation jederzeit anpassen.

Sie können an dieser Stelle auch den dynamischen Arbeitsspeicher aktivieren. Diese Funktion ermöglicht es, dass virtuelle Computer, die nicht ihren gesamten zugewiesenen Arbeitsspeicher ausnutzen, Teile davon auch anderen virtuellen Computern zur Verfügung stellen können. Virtuelle Computer können über Hyper-V den Arbeitsspeicher teilen. Die einzelnen virtuellen Computer teilen dem Hypervisor mit, wie viel Arbeitsspeicher sie benötigen. Ist genügend Arbeitsspeicher auf dem Computer frei, teilt der Hypervisor dem virtuellen Computer den benötigten Arbeitsspeicher zu und zieht ihn von anderen Computern ab, die derzeit keinen Bedarf haben.

Sobald der Speicherbedarf des Computers steigt, fragt der Server den Speicher beim Hyper-V-Host an und erhält diesen, wenn der Speicher zur Verfügung steht. Umgekehrt teilen virtuelle Computer ständig dem Hyper-V-Host mit, wie viel Arbeitsspeicher sie abgeben können.

Für virtuelle Computer können Sie nach der Erstellung in den Einstellungen einen Startwert und einen maximalen Wert für den Arbeitsspeicher zuteilen. Die Zuteilung des tatsächlichen Arbeitsspeichers steuert Hyper-V auch auf Basis der Prioritäten, die Sie den virtuellen Computern zuweisen. Um Dynamic Memory zu nutzen, aktivieren Sie das Kontrollkästchen *Dynamischen Arbeitsspeicher für diesen virtuellen Computer verwenden*. An dieser Stelle können Sie aber keine Werte konfigurieren.

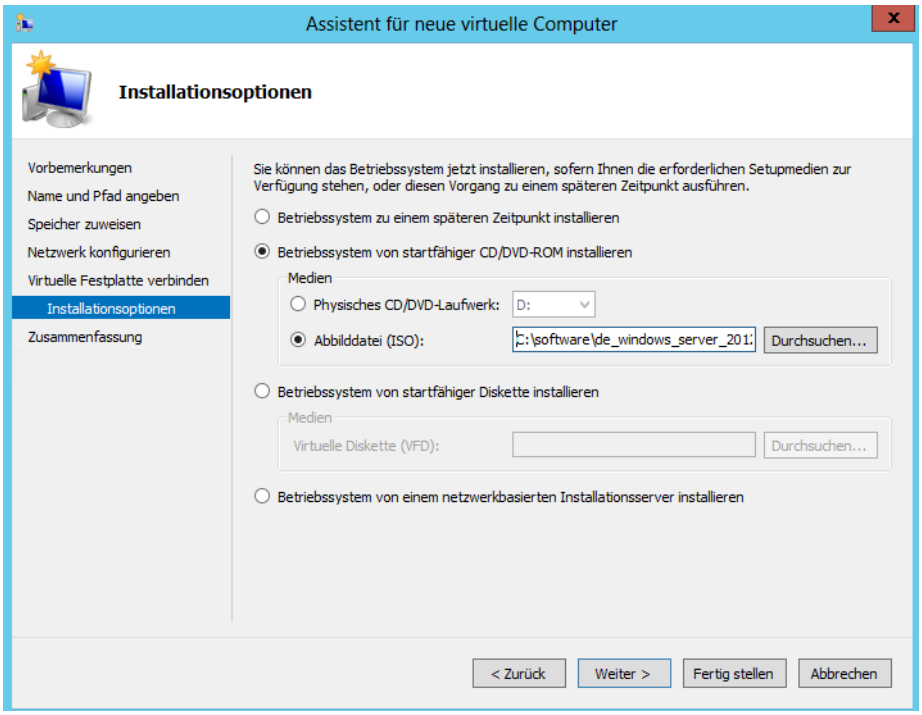
Wählen Sie auf der nächsten Seite das Netzwerk aus, das Sie für die virtuellen Server erstellt haben. Hier stehen die virtuellen Switches zur Verfügung, die Sie im Vorfeld angelegt haben. Sie können nach der Erstellung des virtuellen Servers zusätzliche virtuelle Netzwerkkarten hinzufügen und diese mit einem anderen virtuellen Switch verbinden. Auf diesem Weg können Sie dann in virtuellen Servern Netzwerkkarten zu Teams zusammenfassen. Das virtuelle Team verwendet verschiedene virtuelle Switches, die wiederum auf verschiedenen physischen Netzwerkkarten aufbauen.

Auf der nächsten Seite aktivieren Sie die Option *Virtuelle Festplatte erstellen* und wählen den Pfad und die Größe aus. Lesen sie dazu auch die Anmerkungen in den Kapiteln 1, 2 und 5. Sie können virtuellen Computern auch nachträglich jederzeit weitere virtuelle Festplatten über deren Einstellungen zuordnen.

Als Nächstes wählen Sie aus, wie Sie das Betriebssystem installieren wollen. Am besten aktivieren Sie die Option *Physisches CD/DVD-Laufwerk* oder *Abbilddatei (ISO)*. Schließen Sie auf der nächsten Seite die Erstellung der virtuellen Maschine ab, lassen Sie diese aber nicht starten.

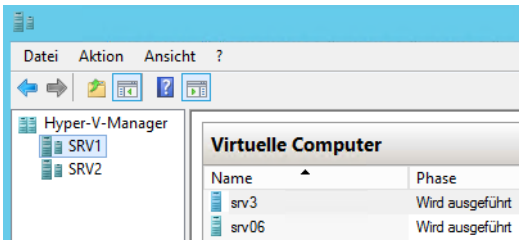
Nach der erfolgreichen Erstellung des virtuellen Computers können Sie im Hyper-V-Manager weitere Einstellungen vornehmen. Rufen Sie dazu im Kontextmenü des virtuellen Computers den Eintrag *Einstellungen* auf. Klicken Sie in den Einstellungen des Computers auf *Hardware hinzufügen*, wenn Sie zusätzliche Hardware zur virtuellen Maschine hinzufügen wollen, zum Beispiel weitere virtuelle Netzwerkkarten oder einen SCSI-Controller.

Abbildg. 7.18 Installationsoptionen von virtuellen Computern



Legen Sie die Installations-DVD in das Laufwerk des physischen Hosts oder laden Sie die ISO-Datei in den Einstellungen des virtuellen Computers. Klicken Sie im Hyper-V-Manager den virtuellen Computer mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Starten* aus. Anschließend installieren Sie auf dem Server das Betriebssystem, wie auf einem physischen Server. Hier gibt es keine Unterschiede. Beenden Sie das Verbindungsfenster zum virtuellen Computer bleibt dieser weiter gestartet. Sie sehen den Status der entsprechenden virtuellen Computer im Hyper-V-Manager.

Abbildg. 7.19 Zustand von virtuellen Servern im Hyper-V-Manager anzeigen



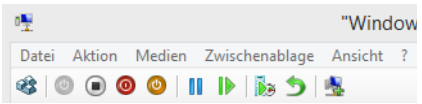
In den nächsten Abschnitten zeigen wir Ihnen, wie Sie virtuelle Server verwalten, auch in der PowerShell. Sie haben natürlich auch die Möglichkeit, virtuelle Server in der PowerShell zu erstellen. Dazu verwenden Sie das Cmdlet *New-VM –Name <Name des virtuellen Servers>*. Neue virtuelle Festplatten erstellen Sie mit *New-VHD*.

TIPP Eine Liste aller erstellten virtuellen Server eines Hyper-V-Hosts rufen Sie mit *Get-VM* ab. Mit der Option *|fl* erhalten Sie weiterführende Informationen. Sie erhalten so auch Echtzeitdaten, also auch den zugewiesenen Arbeitsspeicher, wenn Sie Dynamic Memory einsetzen.

Virtuelle Server steuern

Im Fernwartungsfenster des virtuellen Computers und auch in dessen Kontextmenü stehen verschiedene Schaltflächen zur Verfügung, mit denen Sie den Server steuern können.

Abbildg. 7.20 Symbolleiste von virtuellen Servern



- **STRG+ALT+ENTF** Mit der ersten Schaltfläche auf der linken Seite senden Sie die Tastenkombination Strg + Alt + Entf an den Server
- **Starten** Mit der *Starten*-Schaltfläche starten Sie den Server, wenn er ausgeschaltet ist
- **Ausschalten** Die Schaltfläche zum Ausschalten schaltet den Server sofort aus, ohne das Betriebssystem herunterzufahren
- **Herunterfahren** Fährt das Betriebssystem herunter
- **Speichern** Mit dieser Option wird der Inhalt des Arbeitsspeichers in einer Datei auf dem Host abgespeichert und der Gast dann abgeschaltet. Beim späteren Starten wird dieser Status aus der Datei erneut in den Arbeitsspeicher geladen und die Maschine steht wieder zur Verfügung.
- **Anhalten** Einer laufenden VM werden sämtliche CPU-Ressourcen entzogen, sie friert im aktuellen Zustand ein. Der Inhalt des Arbeitsspeichers, und damit der aktuelle Zustand der Maschine, bleibt erhalten und die VM läuft nach dem Fortsetzen sofort weiter.

- **Neu starten** Diese Schaltfläche entspricht einem Reset. Das Betriebssystem wird dazu nicht heruntergefahren, sondern der Zustand entspricht dem des Ausschaltens des Servers und einem sofortigen Neustart.
- **Prüfpunkt** Mit dieser Schaltfläche erstellen Sie einen Prüfpunkt (auch Snapshot oder Momentaufnahme genannt). Mehr zu diesem Thema erfahren Sie im nächsten Kapitel.
- **Zurücksetzen** Setzt den Server auf den letzten Prüfpunkt zurück. Mehr dazu erfahren Sie im nächsten Kapitel.
- **Erweiteter Sitzungsmodus** Mit dieser Schaltfläche aktivieren Sie für die aktuelle Verbindung zum virtuellen Server den erweiterten Sitzungsmodus auf Basis von RDP. Mehr zu diesem Thema lesen Sie im Abschnitt . Die Funktion ist neu in Windows Server 2012 R2. Mit der Schaltfläche aktivieren Sie auch wieder den einfachen Sitzungsmodus, den Sie bereits von Vorgängerversionen von Windows Server 2012 R2 kennen.

Neben der grafischen Oberfläche können Sie virtuelle Server in der PowerShell steuern. So schalten Sie mit *Stop-VM* virtuelle Maschinen aus, starten Sie mit *Start-VM* und rufen den Zustand mit *Get-VM* ab. Um sich eine Liste der verfügbaren Befehle anzuzeigen, verwenden Sie *Get-Command *vm**.

Abbildg. 7.21 Steuern von virtuellen Servern in der PowerShell

```
PS C:\Users\administrator.CONTOSO> Stop-VM srv06
PS C:\Users\administrator.CONTOSO> Start-VM srv06
PS C:\Users\administrator.CONTOSO> get-VM srv06

Name  State   CPUUsage(%) MemoryAssigned(M) Uptime   Status
----  -----   ----------- ----------------- ------   ------
srv06 Running 0           1024              00:00:06 Normaler Betrieb
```

Sie können über die PowerShell Server auch neu starten (*Restart-VM*), anhalten (*Suspend-VM*) und wieder fortführen lassen (*Resume-VM*).

Virtuelle Server können Sie mit *Import-VM* importieren und mit *Export-VM* exportieren. Snapshots erstellen Sie mit *Checkpoint-VM*.

Einstellungen von virtuellen Servern anpassen

Über das Kontextmenü oder den *Aktionen*-Bereich lassen sich die verschiedenen Einstellungen der virtuellen Computer anpassen. Hierüber passen Sie zum Beispiel die Anzahl der Prozessoren, den Arbeitsspeicher, BIOS-Einstellungen und die Schnittstellen an. Auch neue Hardware fügen Sie über diesen Bereich hinzu. In diesem Abschnitt gehen wir auf die einzelnen Möglichkeiten ein.

Viele Einstellungen stehen aber nur dann zur Verfügung, wenn der virtuelle Server ausgeschaltet ist. Einstellungen, die im laufenden Betrieb nicht möglich sind, graut der Hyper-V-Manager aus.

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.

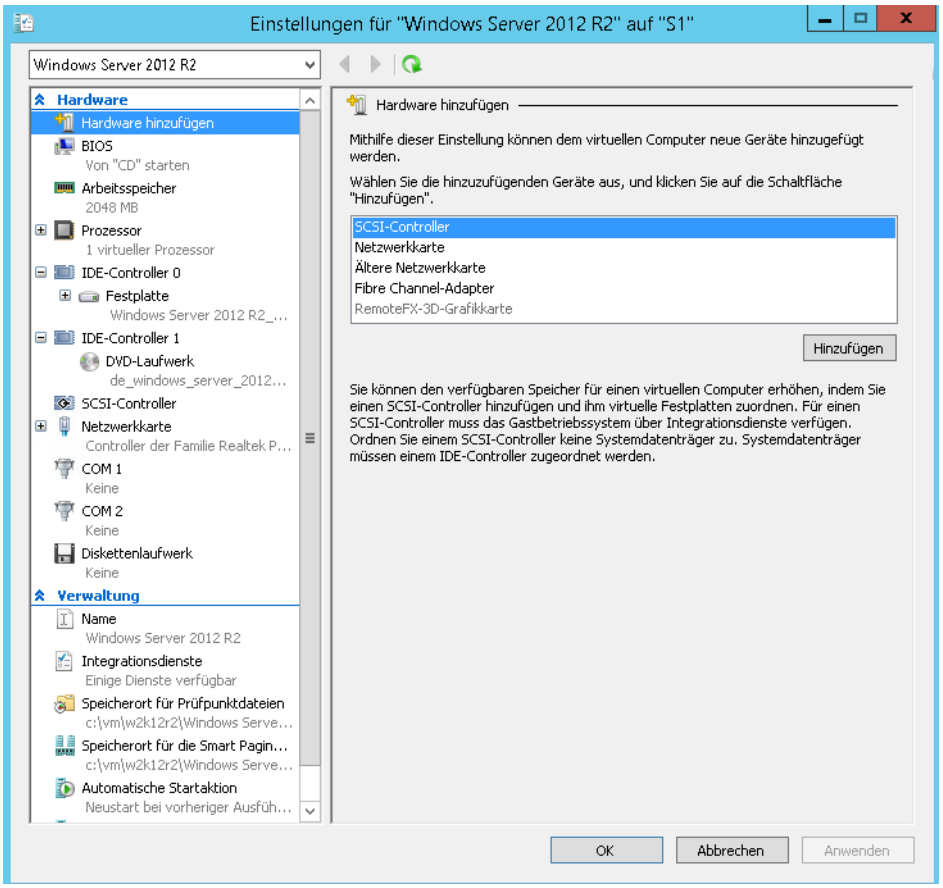
Hardware zu virtuellen Computern hinzufügen

Wollen Sie einem virtuellen Computer neue Hardware hinzufügen, also eine neue Netzwerkkarte, einen SCSI-Controller oder neue Festplatten, klicken Sie den virtuellen Computer mit der rechten Maustaste an, wählen *Einstellungen* und klicken dann auf *Hardware hinzufügen*.

TIPP Wollen Sie in Hyper-V Betriebssysteme testen, für die es keine Integrationsdienste gibt (zum Beispiel VMware-Produkte), müssen Sie dem virtuellen Server ältere Netzwerkkarten hinzufügen. Der neue Netzwerkkartentyp arbeitet nicht mit Systemen zusammen, die offiziell nicht von Hyper-V unterstützt werden.

Im rechten Bereich wählen Sie die Hardware aus, die Sie hinzufügen wollen, und klicken auf *Hinzufügen*. Beim Hinzufügen eines Festplattencontrollers besteht zusätzlich die Möglichkeit, noch weitere Festplatten hinzuzufügen. Um Hardware hinzuzufügen, muss der Server ausgeschaltet sein.

Abbildg. 7.22 Einstellungen eines virtuellen Servers ändern



Sobald Sie einem virtuellen Server einen SCSI-Controller hinzugefügt haben, können Sie weitere Festplatten hinzufügen, auch wenn der Server gestartet ist. Das geht aber nur bei virtuellen SCSI-Festplatten. Damit die Hardware hinzugefügt wird, müssen Sie die Änderung noch mit *Anwenden* oder *OK* bestätigen.

Einmal hinzugefügte Geräte lassen sich über die Schaltfläche *Entfernen* wieder vom virtuellen Computer trennen.

Interessant ist im unteren Bereich auch die Option *Speicherort für die Smart Paging-Datei*. Diese Funktion ist neu in Windows Server 2012 R2. Smart Paging soll verhindern, dass sich virtuelle Server nicht mehr starten lassen, weil der gesamte verfügbare Arbeitsspeicher bereits zugewiesen ist. Nutzen Sie Dynamic Memory (siehe nächster Abschnitt), besteht die Möglichkeit, dass andere Server auf dem Host den gesamten Arbeitsspeicher nutzen.

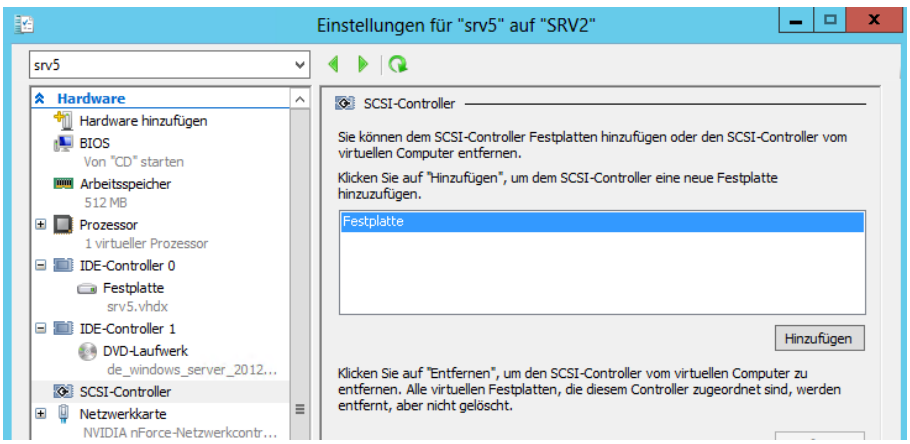
Die Smart Paging-Funktion erlaubt virtuellen Servern beim Neustart Teile der Festplatte des Hosts als Arbeitsspeicher zu nutzen. Auch diesen Bereich können Sie daher getrennt verschieben. Nach dem erfolgreichen Start wird der Festplattenplatz wieder freigegeben und der virtuelle Server erhält durch Dynamic Memory wieder seinen Speicher. In Windows Server 2012 R2 unterstützen auch virtuelle Computer auf Basis von Linux diese Funktion.

Virtuelle Festplatten zu Servern hinzufügen

Um einem Server eine neue virtuelle Festplatte hinzuzufügen, haben Sie verschiedene Möglichkeiten. Nachdem Sie einen oder mehrere SCSI-Controller als Hardware hinzugefügt haben, können Sie virtuelle Festplatten entweder zu einem virtuellen IDE-Controller hinzufügen oder einen virtuellen SCSI-Controller verwenden. Im laufenden Betrieb lassen sich virtuelle Festplatten nur an virtuelle SCSI-Controller hinzufügen. Um einen virtuellen SCSI-Controller hinzuzufügen, müssen Sie aber wiederum den virtuellen Server herunterfahren. Neue Festplatten fügen Sie im Schnelldurchlauf folgendermaßen hinzu:

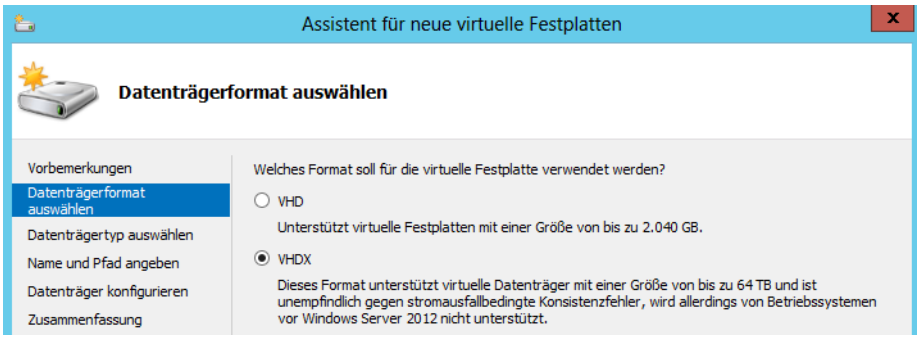
1. Klicken Sie mit der rechten Maustaste auf den virtuellen Server und dann auf *Einstellungen*.
2. Klicken Sie auf den Controller, mit dem die neue virtuelle Festplatte verbunden werden soll.
3. Klicken Sie danach auf *Festplatte* und dann auf *Hinzufügen*.

Abbildg. 7.23 Hinzufügen einer virtuellen Festplatte zu einem virtuellen Server



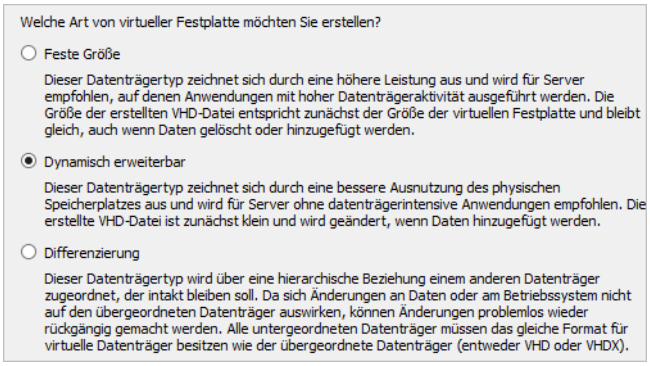
4. Aktivieren Sie im neuen Bereich die Option *Virtuelle Festplatte* und klicken Sie auf *Neu*, um den Assistenten für eine neue Festplatte zu starten.
5. Bestätigen Sie die Startseite des Assistenten zum Hinzufügen von neuen Festplatten und wählen Sie danach das Format aus, das die neue Festplatte erhalten soll, also VHD (bis 2 TB) oder VHDX (bis 64 TB).

Abbildg. 7.24 Auswählen des Datenträgerformats



6. Wählen Sie als Nächstes aus, ob die Festplatte eine feste Größe haben soll (*Feste Größe*), dynamisch erweiterbar (*Dynamisch erweiterbar*) oder auf einer vorhandenen Festplatte aufbauen soll (*Differenzierung*).
   - **Feste Größe** Bei dieser Variante legen Sie eine feste Größe fest, welche die virtuelle Festplatte des virtuellen Servers nicht überschreiten darf.
   - **Dynamisch erweiterbar** Dieser Typ wird am häufigsten verwendet. Die hinterlegte Datei der Festplatte kann dynamisch mit dem Inhalt mitwachsen.
   - **Differenzierung** 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 erzeugen. Microsoft empfiehlt, die übergeordnete virtuelle Festplatte mit einem Schreibschutz zu versehen, damit diese nicht versehentlich überschrieben wird. In der Differenzfestplatte liegen nur die Änderungen, die das Gastsystem an der virtuellen Festplatte vorgenommen hat. Dazu werden alle Schreibzugriffe des Gasts auf die Differenzfestplatte umgeleitet. Lesezugriffe kombinieren den Inhalt der Differenzfestplatte und den Inhalt der zugrunde liegenden virtuellen Festplatte, ohne dass der Gast etwas davon bemerkt. Die zugrunde liegende Festplatte wird nicht mehr verändert, und die Differenzfestplatte bleibt relativ klein, da sie nur Änderungen enthält. Eine fertige Basisinstallation kann von mehreren virtuellen Maschinen (VMs) gleichzeitig verwendet werden, indem Sie mehrere Differenzfestplatten erstellen, die dieselbe virtuelle Festplatte verwenden. Dadurch sparen Sie sich viel Zeit und Platz beim Klonen von virtuellen Maschinen.

Abbildg. 7.25 Festlegen der Art der neuen virtuellen Festplatte



7. Im Anschluss legen Sie den Pfad fest, in dem Windows Server 2012 R2 die VHD/VHDX-Datei speichern soll. Auch den Namen der Datei geben Sie hier ein.
8. Auf der nächsten Seite legen Sie die Größe der virtuellen Festplatte fest und können auch den Inhalt einer physischen Festplatte in die virtuelle Festplatte kopieren lassen. Danach erhalten Sie noch eine Zusammenfassung und erstellen mit *Fertig stellen* schließlich die virtuelle Festplatte.
9. Klicken Sie danach im Fenster auf *Anwenden*, damit die virtuelle Festplatte an den virtuellen Server angefügt wird.
10. Die Festplatte ist jetzt angefügt und kann in der Datenträgerverwaltung des virtuellen Servers verwaltet werden. Hier gehen Sie vor, wie bei physischen Festplatten (siehe Kapitel 5).

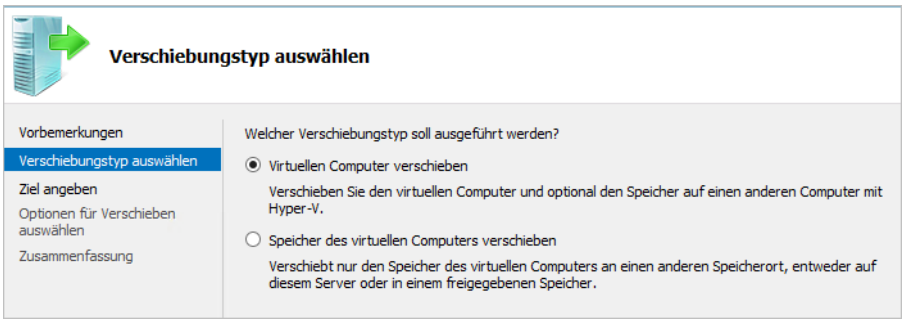
Speicher-Migration – Virtuelle Festplatten verschieben

In Windows Server 2012 R2 haben Sie auch die Möglichkeit, den Speicherort von virtuellen Festplatten auf Hyper-V-Hosts zu verschieben. Diesen Vorgang können Sie im laufenden Betrieb vornehmen. Das ist zum Beispiel sinnvoll, wenn Sie einen Datenträger vergrößern oder die virtuellen Datenträger auf ein NAS oder SAN auslagern wollen.

Den Vorgang nehmen Sie am besten im Hyper-V-Manager vor. Klicken Sie dazu mit der rechten Maustaste auf den virtuellen Server, dessen Festplatten Sie verschieben wollen. Wählen Sie danach *Verschieben* aus.

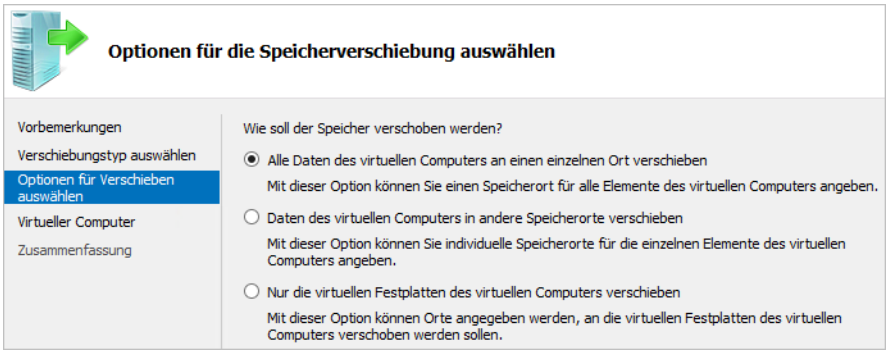
Im Assistenten wählen Sie anschließend *Speicher des virtuellen Computers verschieben* aus. Wie Sie komplette virtuelle Server zwischen Hyper-V-Hosts im laufenden Betrieb (Livemigration) verschieben, zeigen wir Ihnen in Kapitel 9. In Windows Server 2012 R2 können Sie Livemigration auch ohne Cluster nutzen.

Abbildg. 7.26 Verschieben des Speichers eines virtuellen Servers



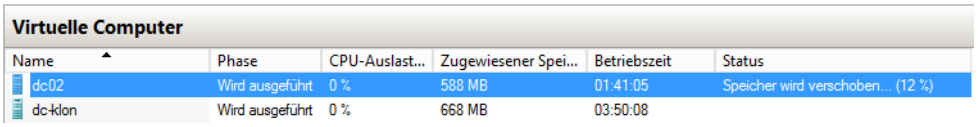
Im nächsten Fenster wählen Sie aus, ob Sie die Daten des virtuellen Servers oder nur die virtuellen Festplatten verschieben wollen.

Abbildg. 7.27 Verschieben des Speichers von virtuellen Festplatten oder aller Daten auswählen



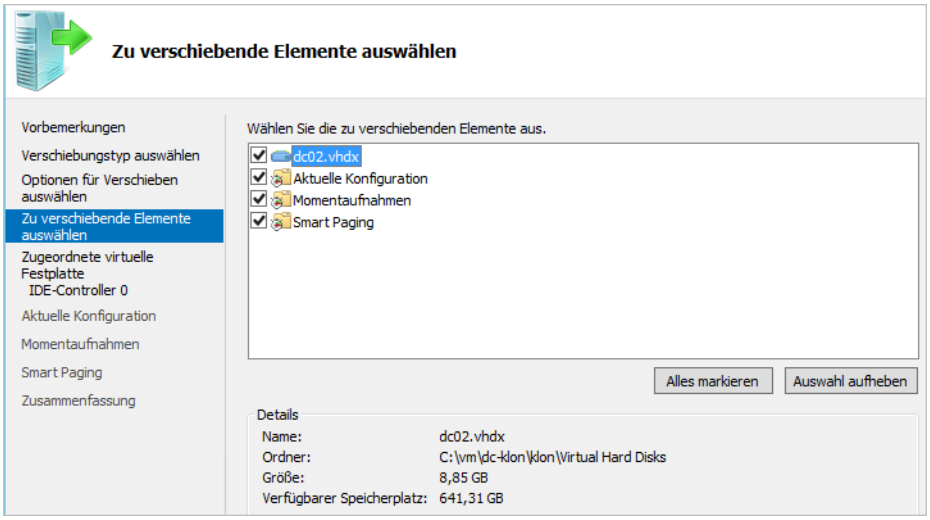
Im nächsten Fenster wählen Sie den entsprechenden Ordner aus, in dem Hyper-V die Daten des Computers speichern soll. Während des Vorgangs bleibt der virtuelle Server gestartet. Sie sehen den Status im Hyper-V-Manager. Während des Vorgangs werden die Anwender nicht vom virtuellen Server getrennt.

Abbildg. 7.28 Anzeigen des Status während des Verschiebens von virtuellen Festplatten



Wollen Sie Daten in verschiedenen Ordnern speichern, können Sie die entsprechende Option auswählen und im nächsten Fenster getrennte Speicherorte für Konfigurationsdateien, virtuelle Festplatte und Snapshots festlegen.

Abbildg. 7.29 Festlegen der Ordner beim Verschieben



Sie können neben Konfiguration, Snapshots und den virtuellen Festplatten auch Smart Paging-Dateien getrennt speichern. Smart Paging soll verhindern, dass sich virtuelle Server nicht mehr starten lassen, weil der gesamte verfügbare Arbeitsspeicher bereits zugewiesen ist. Nutzen Sie Dynamic Memory (siehe nächster Abschnitt), besteht die Möglichkeit, dass andere Server auf dem Host den gesamten Arbeitsspeicher nutzen.

Die neue Funktion Smart Paging erlaubt virtuellen Servern beim Neustart Teile der Festplatte des Hosts als Arbeitsspeicher zu nutzen. Auch diesen Bereich können Sie daher getrennt verschieben. Nach dem erfolgreichen Start wird der Festplattenplatz wieder freigegeben und der virtuelle Server erhält durch Dynamic Memory wieder seinen Speicher.

USB-Festplatten an Hyper-V anbinden

Leider unterstützt Hyper-V auch in der neuen Version von Windows Server 2012 R2 keine Anbindung von USB-Geräten. Sie haben aber die Möglichkeit, externe Festplatten, die am Hyper-V-Host angeschlossen sind, in virtuellen Servern zur Verfügung stellen.

Sie können über den nachfolgend erläuterten Weg aber auch in anderen Gastsystemen wie Linux USB-Geräte anbinden. Der Weg in diesem Abschnitt zeigt die Anbindung an Windows Server 2012 R2.

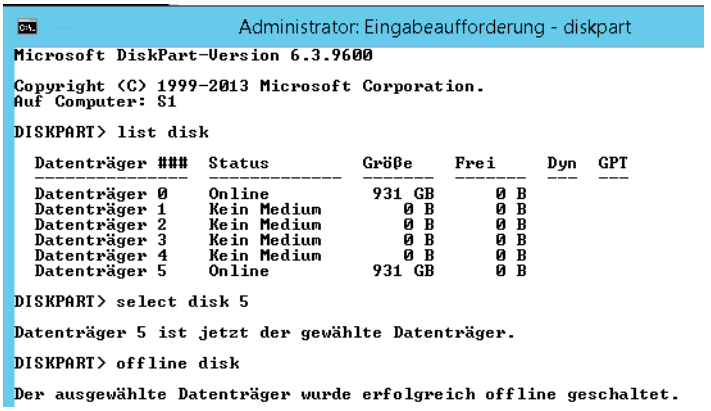
Neben den hier beschriebenen Möglichkeiten können Sie USB-Laufwerke auch über RDP-Sitzungen verwenden oder USB-Server im Netzwerk zur Verfügung stellen. Der nachfolgend beschriebene Weg ermöglicht das Verwenden von USB-Speichermedien. Sie können andere USB-Geräte wie Dongles oder Drucker nur über RDP-Sitzungen oder entsprechende Geräte in Hyper-V nutzen.

Handelt es sich bei den virtuellen Computern um Arbeitsstationen in einer Virtual Desktop Infrastructure auf Basis von Hyper-V, können Anwender über diesen Weg natürlich USB-Geräte nutzen. In diesem Fall verbinden sich die Anwender entweder mit Thin-Clients oder PCs über das RDP-Protokoll mit dem virtuellen Computer. Das heißt, hier stehen alle USB-Laufwerke zur Verfügung. Nur in der Hyper-V-Konsole lassen sich diese Geräte nicht nutzen.

Um eine USB-Festplatte mit einem virtuellen Server zu verbinden, schließen Sie diese direkt an den Hyper-V-Host an. Die Platte muss zunächst im System verfügbar sein. Haben Sie die externe Festplatte verbunden, öffnen Sie eine Eingabeaufforderung mit Administratorrechten und geben den Befehl *diskpart* ein. Mit *list disk* finden Sie die Nummer der externen Festplatte.

Im nächsten Schritt wählen Sie die USB-Festplatte aus, die Sie im virtuellen Server unter Hyper-V nutzen wollen. Verwenden Sie dazu den Befehl *select <Nummer der Festplatte>*. Anschließend setzen Sie die Festplatte mit *offline disk* offline.

Abbildg. 7.30 Um eine physische Festplatte auf virtuellen Servern zu verwenden, müssen Sie diese offline setzen



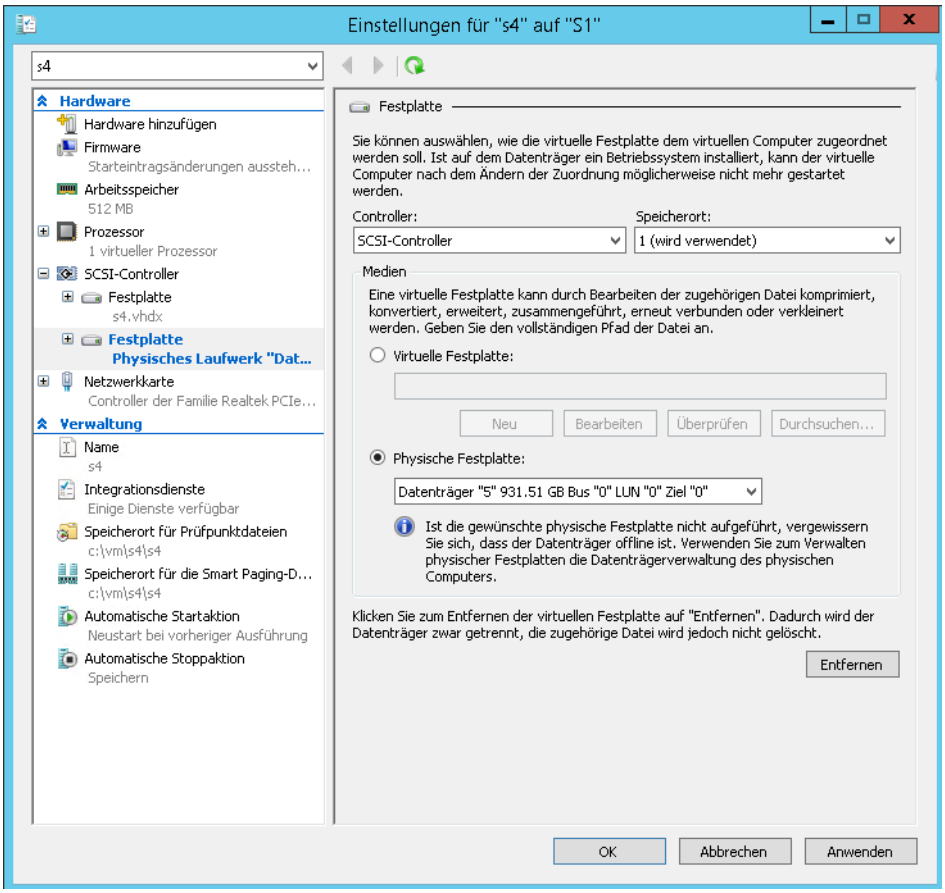
Es muss die Meldung erscheinen, dass der Datenträger offline gesetzt ist. Überprüfen Sie mit *diskmgmt.msc*, ob der Datenträger in der Datenträgerverwaltung des Hyper-V-Hosts auch tatsächlich offline angezeigt wird. Mit *diskpart* sehen Sie das auch in der Befehlszeile, wenn Sie *list disk* aufrufen.

Rufen Sie im Anschluss im Hyper-V-Manager die Einstellungen des virtuellen Servers auf, auf dem Sie diese Festplatte zur Verfügung stellen wollen. Klicken Sie in den Einstellungen auf *SCSI-Controller*, dann auf *Festplatte* und dann auf *Hinzufügen*. Sie fügen jetzt den USB-Datenträger vom Hyper-V-Host als Datenträger über den virtuellen SCSI-Datenträger an den virtuellen Server an.

Im Fenster aktivieren Sie *Physische Festplatte* und wählen den von Ihnen offline gesetzten USB-Datenträger aus. Klicken Sie danach auf *Anwenden* und bestätigen Sie mit *OK*.

Öffnen Sie auf dem virtuellen Server die Festplattenverwaltung mit *diskmgmt.msc*. Hier sehen Sie den Datenträger. Über das Kontextmenü schalten Sie diesen online. Weisen Sie dem Datenträger noch einen Laufwerksbuchstaben zu. Alle Daten sind jetzt in der virtuellen Maschine verfügbar.

Abbildg. 7.31 Physische Festplatten können Sie direkt virtuellen Computern zuordnen

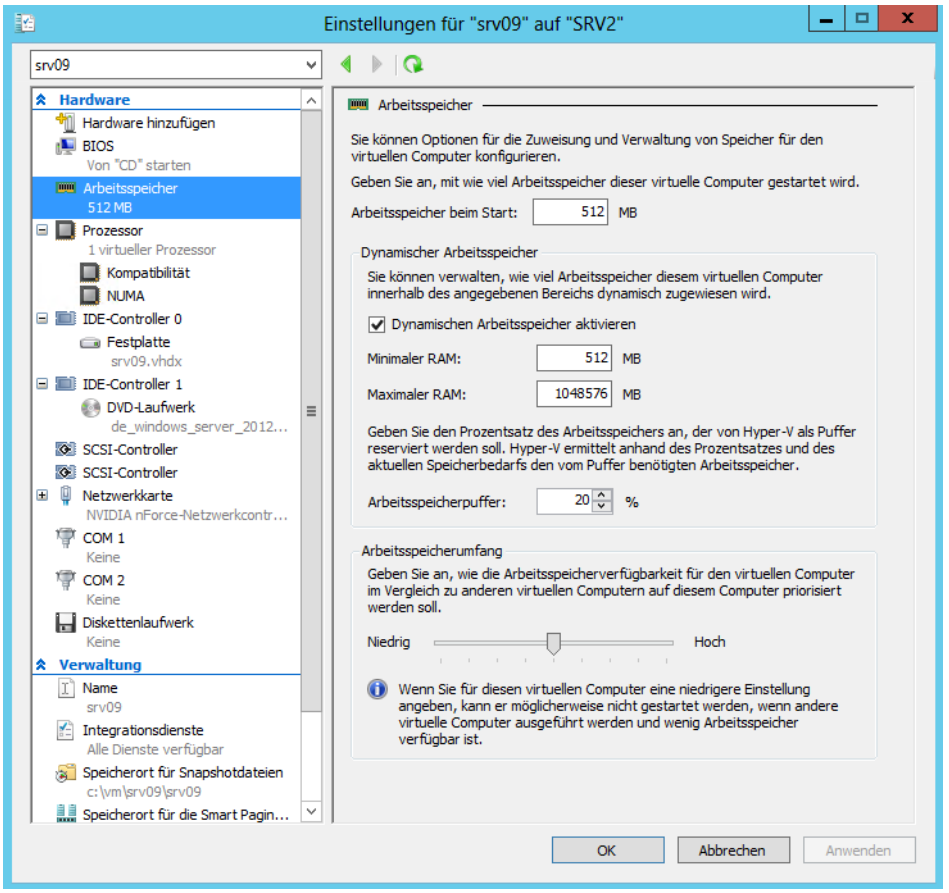


Dynamic Memory – Arbeitsspeicher anpassen

Über die Kategorie *Arbeitsspeicher* in den Einstellungen der VM bestimmen Sie die Größe des Arbeitsspeichers des virtuellen Computers. Wir gehen im nächsten Abschnitt noch genauer auf die Möglichkeiten in diesem Bereich ein. Dynamic Memory ist sicherlich die wichtigste Änderung, die das Service Pack 1 für Windows Server 2008 R2 mitbringt. In Windows Server 2012 R2 ist die Funktion standardmäßig schon integriert und erlaubt die Aktivierung bereits beim Erstellen eines virtuellen Servers.

Die Funktion ermöglicht es, dass virtuelle Computer, die nicht ihren gesamten zugewiesenen Arbeitsspeicher ausnutzen, diesen auch anderen virtuellen Computern auf dem gleichen Host zur Verfügung stellen können. Mit dieser Technik erhöht sich also die Effizienz von Hyper-V und Unternehmen können mehr virtuelle Server auf Hyper-V-Hosts betreiben. Die Zuteilung des Arbeitsspeichers übernimmt der Hypervisor.

Abbildg. 7.32 Arbeitsspeicher in Windows Server 2012 R2 konfigurieren



Benötigt ein virtueller Server mehr Arbeitsspeicher, teilt Hyper-V den Arbeitsspeicher dem virtuellen Server zu und zieht ihn von anderen Servern ab, die derzeit keinen Bedarf haben. Virtuelle Server informieren Hyper-V auch über die Speichermenge, die sie abgeben können. Auf diese Weise kann Hyper-V den tatsächlich verfügbaren Arbeitsspeicher immer optimal verteilen und kennt die Arbeitsspeicher-Bedürfnisse der einzelnen Server.

Für virtuelle Computer können Sie nach der Erstellung in den Einstellungen einen Startwert und einen maximalen Wert für den Arbeitsspeicher zuteilen. Die Zuteilung des tatsächlichen Arbeitsspeichers steuert Hyper-V auch auf Basis der Prioritäten, die Sie den virtuellen Computern zuweisen. Um Dynamic Memory zu nutzen, aktivieren Sie das Kontrollkästchen *Dynamischen Arbeitsspeicher für diesen virtuellen Computer verwenden* bei der Erstellung des virtuellen Servers. An dieser Stelle können Sie aber keine Werte konfigurieren. Dazu rufen Sie später über das Kontextmenü die Einstellungen auf und klicken in der Kategorienleiste auf *Arbeitsspeicher*.

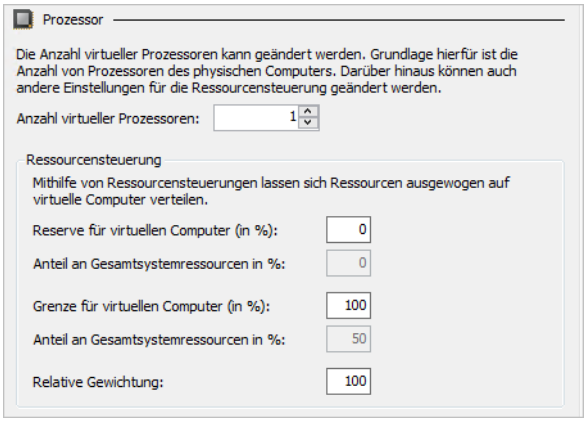
Geben Sie bei *Minimaler RAM* an, mit wie viel Speicher der Computer starten soll, und bei *Maximaler RAM*, wie viel Arbeitsspeicher der Server maximal erhalten kann.

Über *Arbeitsspeicherpuffer* legen Sie fest, wie viel zusätzlichen Arbeitsspeicher der virtuelle Computer erhalten soll. Diesen Speicher kann der Computer nutzen, um die Leistung zu erhöhen. Über *Arbeitsspeicherumfang* legen Sie fest, wie sich Anfragen des Computers im Vergleich zu anderen Computern verhalten sollen. Ist der maximale Arbeitsspeicher des Computers bereits ausgelastet, erhalten höher priorisierte Computer mehr Speicher, den unterpriorisierte abgeben müssen.

Prozessoren in Hyper-V steuern

Ausführlichere Möglichkeiten bietet die Prozessorsteuerung von virtuellen Computern. Über die Kategorie *Prozessor* in den Eigenschaften eines virtuellen Servers legen Sie die Anzahl der Prozessoren sowie eine Gewichtung der Ressourcen fest, die dem Prozessor zugewiesen sind.

Abbildg. 7.33 Konfigurieren der Prozessoreinstellungen von virtuellen Computern

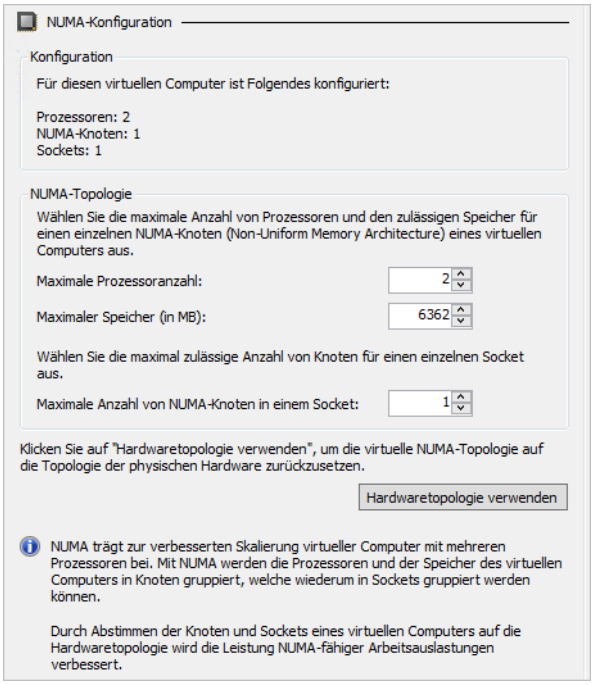


Neben der eigentlichen Anzahl an Prozessoren, die dem virtuellen Computer zugewiesen sind, steuern Sie hier, wie viel Prozessorzeit diesem virtuellen Computer zur Verfügung steht. Hier stehen mehrere Möglichkeiten zur Verfügung, die Sie über Prozentangaben steuern:

- **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.
- **Anteil an Gesamtsystemressourcen** Diese Option ist nicht anpassbar. Hier legt Hyper-V fest, welchen prozentualen Anteil die aktuell ausgewählte VM von den Gesamtressourcen erhält.
- **Grenze für virtuellen Computer** Dieser Wert in Prozent 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. Ein Computer, dem Sie eine relative Gewichtung von 200 zuweisen, erhält doppelt so viel Zugriff auf die CPU wie ein Computer, mit einer Gewichtung von 100. Es handelt sich bei diesem Wert also nicht um eine Prozentzahl, sondern um eine benutzerdefinierte Gewichtung. Wichtige Server lassen sich dadurch bevorzugen und es ist sichergestellt, dass diese nicht zu wenig Ressourcen zugewiesen bekommen.

Wichtig für die Steuerung von Prozessoren in virtuellen Servern sind noch die beiden Unterkategorien *Kompatibilität* und *NUMA* (Non-Uniform Memory Access), die unterhalb der Kategorie *Prozessor* zu finden sind. Bei *Kompatibilität* können Sie zum Beispiel sicherstellen, dass Sie den virtuellen Server mit der Livemigration auf einen anderen Hyper-V-Host verschieben können. Bei Servern mit verschiedenen Prozessoren steuern Sie über NUMA wichtige Einstellungen.

Abbildg. 7.34 NUMA in Hyper-V konfigurieren



NUMA (Non-Uniform Memory Architecture) bietet für jeden Prozessor im Server einen eigenen Speicherbereich. Diesen kann er aber anderen Prozessoren bei Bedarf zur Verfügung stellen (Distributed Shared Memory). Damit Sie in virtuellen Servern NUMA nutzen können, muss die Funktion in den Hyper-V-Einstellungen des virtuellen Servers aktiviert sein.

In Windows Server 2012 R2 ist das standardmäßig der Fall. Sie finden die Konfiguration in den Hyper-V-Einstellungen. Deaktivieren Sie diese Einstellung, dürfen VMs nur noch Speicher und Prozessorkerne des gleichen NUMA-Knotens einsetzen.

Allgemeine Einstellungen von virtuellen Computern verwalten

Im unteren Bereich der Einstellungen von virtuellen Computern legen Sie den von Hyper-V verwendeten Namen sowie die freigeschalteten Funktionen der Integrationsdienste fest. Haben Sie für einen Computer noch keinen Snapshot erstellt, also eine Sicherung des Betriebssystemzustands zu

einem bestimmten Zeitpunkt, 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 die Kategorie *Automatische Startaktion* legen Sie fest, wie sich der virtuelle Computer bei einem Neustart des Hosts verhalten soll. Die Kategorie *Automatische Stoppaktion* dient der Konfiguration des Verhaltens, wenn der Host heruntergefahren wird.

Daten von virtuellen Servern aus Hyper-V auslesen

Administratoren benötigen häufig einen Überblick zu den verschiedenen Servern im Netzwerk. Betreiben Sie im Unternehmen virtuelle Server auf Basis von Hyper-V, können Sie mit einfachen Tools und Befehlen schnell und einfach Daten wie IP-Adressen, Festplattendaten oder die Konfiguration auslesen. Dazu sind nicht immer teure Zusatztools wie System Center Virtual Machine Manager notwendig. Oft reichen Bordmittel oder günstige Freeware- beziehungsweise OpenSource-Tools.

Wir zeigen Ihnen, welche Möglichkeiten es gibt, Daten von Servern auszulesen. Vor allem Hyper-V in Windows Server 2012 R2 bietet hier mit der PowerShell einige Möglichkeiten. Die folgenden Tools und Befehle funktionieren oft auch für physische Server oder virtuelle Server, die Sie mit anderen Lösungen wie beispielsweise VMware virtualisieren. Auch für Arbeitsstationen lassen sich manche der Tools nutzen.

IP-Adressen und Daten von virtuellen Servern auslesen

Im Hyper-V-Manager sehen Sie die IP-Adressen und Netzwerkdaten von virtuellen Servern, wenn Sie einen Server markieren und ganz unten die Registerkarte *Netzwerk* aufrufen. Sie sehen an dieser Stelle auch den virtuellen Switch, mit dem der virtuelle Server verbunden ist und welchen Status die Verbindung hat. Dies funktioniert auch, wenn Sie Hyper-V in Windows 8.1 nutzen. Sie sehen im Fenster auch die aktuelle MAC-Adresse des Servers. Diese spielt zum Beispiel für den Aufbau eines Lastenausgleichclusters eine Rolle. Über diesen Weg können Sie die IP-Adressen der virtuellen Server im Hyper-V-Manager für alle angebundenen Hyper-V-Hosts anzeigen.

Rufen Sie in der PowerShell den Befehl *Get-Command -Module Hyper-V* auf, erhalten Sie eine Liste der verfügbaren Cmdlets angezeigt. Besonders wichtig ist in diesem Zusammenhang das Cmdlet *Get-VM*. Eine Liste aller erstellten virtuellen Server eines Hyper-V-Hosts rufen Sie mit *Get-VM* ab. Mit der Option *|fl* erhalten Sie weiterführende Informationen. Alternativ verwenden Sie *|ft*. Sie erhalten so zusätzlich Echtzeitdaten, also auch den zugewiesenen Arbeitsspeicher, wenn Sie Dynamic Memory einsetzen.

Um sich einen schnellen Überblick zu virtuellen Servern auf einem Hyper-V-Host zu verschaffen, ist das Cmdlet *Get-VM* ein sehr einfacher und effizienter Weg. Das Cmdlet zeigt allerdings keine IP-Adressen an. Dazu verwenden Sie Cmdlets, die wir nachfolgend vorstellen.

Sie können in der PowerShell aber nicht nur Daten von virtuellen Servern auslesen, sondern mit *Get-VMHost* auch Informationen zu den Hyper-V-Host im Netzwerk. Ausführliche Informationen erhalten Sie auch mit diesem Cmdlet über die beiden Optionen *|fl* und *|ft*.

Informationen zu virtuellen Switches zeigt die PowerShell mit *Get-VMSwitch* an. Sie können sich die Einstellungen der virtuellen Netzwerkkarten mit dem folgenden Befehl anzeigen lassen:

```
Get-VMNetworkAdapter -VMName <Name des virtuellen Servers> |fl
```

Mit diesem Cmdlet erhalten Sie auch die MAC-Adressen und IP-Adressen der virtuellen Server auf dem Hyper-V-Host. Wo die virtuellen Festplatten eines virtuellen Servers gespeichert sind, sehen Sie im Hyper-V-Manager in dessen Einstellungen im Bereich *IDE-Controller* oder *SCSI-Controller*. Sie können die virtuellen Festplatten auch in der PowerShell mit den Cmdlets *Get-VMIdeController, Get-VMScsiController, Get-VMFibreChannelHba* und *Get-VMHardDiskDrive* abfragen.

In der PowerShell haben Sie die Möglichkeit, das Ergebnis einer Get-Abfrage an ein anderes Cmdlet zu übergeben. So können Sie zum Beispiel mit *Get-VM* die virtuellen Server eines Hyper-V-Hosts auslesen und mit *Get-VMHardDiskDrive* die virtuellen Festplatten dieser Server anzeigen lassen. Dazu verwenden Sie den folgenden Befehl:

```
Get-VMHardDiskDrive (Get-VM)
```

Zum Auslesen der IP-Adressen und Netzwerkdaten können Sie daher nicht nur die Möglichkeiten des Abschnitts weiter vorne verwenden, sondern auch das Cmdlet *Get-VMNetworkAdapter*. Wollen Sie zum Beispiel aus allen virtuellen Servern die IP-Adressen auslesen, rufen Sie wieder mit *Get-VM* die virtuellen Server eines Hosts ab und übergeben das Ergebnis an *Get-VMNetworkAdapter*.

Anschließend können Sie auf Wunsch das Ergebnis noch filtern und nur die IP-Adressen der virtuellen Server anzeigen lassen. Dazu verwenden Sie zum Beispiel den folgenden Befehl:

```
Get-VM | foreach{(Get-VMNetworkAdapter $_).IPAddresses}
```

Mit dem Zusatz *foreach* liest der Befehl nacheinander die gewünschten Daten aller VMs aus und zeigt diese an. Mit dem Befehl lesen Sie aber nicht nur die IP-Adressen der virtuellen Server auf einem lokalen Hyper-V-Host aus, sondern können auch Hosts im Netzwerk abfragen. Dazu nutzen Sie den folgenden Befehl:

```
Get-VM -computername <Name des Hyper-V-Hosts> | foreach{(Get-VMNetworkAdapter
$_).IPAddresses}
```

WMI-Abfragen zur Anzeige von Festplattendaten oder IP-Adressen nutzen

Eine weitere Möglichkeit, um Daten virtuelle Server, aber auch von physischen Servern im Netzwerk abzufragen, ist die Verwendung WMI-Abfragen. Dazu nutzen Sie die PowerShell und das Cmdlet *Get-WmiObject*. Dem Cmdlet übergeben Sie ein bestimmtes WMI-Objekt und lassen sich so die entsprechenden Daten des Servers anzeigen. Um zum Beispiel Daten von Festplatten auszulesen, verwenden Sie das WMI-Objekt *Win32_LogicalDisk*. Als Beispiel nutzen Sie den Befehl *Get-WmiObject Win32_LogicalDisk*. Sie haben auch die Möglichkeit, das Ergebnis zu filtern. Dazu nutzen Sie die Option *-filter*.

Zusätzlich haben Sie mit dem Cmdlet *Get-WmiObject* die Möglichkeit, über das Netzwerk Daten von physischen oder virtuellen Servern abzufragen. Dazu nutzen Sie die Option *-Computername*. Eine ausführliche Liste der verfügbaren WMI-Objekte erhalten Sie über *Get-WmiObject -List*.

Außer Laufwerke können Sie auch Einstellungen der Netzwerkkarten abfragen. Dazu verwenden Sie die Klasse *Get-WmiObject Win32_Networkadapter*. Sie sehen hier alle wichtigen physischen Einstellungen der Netzwerkkarten. Sie können in der PowerShell anzeigen lassen, ob es sich um einen 32-Bit oder 64-Bit-Computer handelt. Dazu verwenden Sie den folgenden Befehl:

```
Get-WmiObject -Class Win32_ComputerSystem -ComputerName . | Select-Object -Property
SystemType
```

Windows Azure Virtual Machines in der PowerShell verwalten und abfragen

Viele Unternehmen setzen nicht nur lokal virtuelle Server ein, sondern arbeiten mit virtuellen Servern in Windows Azure. Microsoft bietet auf der Windows Azure-Plattform auch Virtual Machines an. Mit dieser Funktion können Sie virtuelle Server auf Basis von Hyper-V zur Verfügung stellen. Die Server lassen sich miteinander verbinden und zu einer Serverfarm zusammenfassen.

Sie können parallel Linux- und Windows-Server in der Cloud zu betreiben. Auch eine Anbindung an System Center 2012 ist möglich. Microsoft bietet bereits vorgefertigte Images an. Auf diesem Weg können Sie mit wenigen Klicks bereits vorinstallierte virtuelle Server zur Verfügung stellen.

Die virtuellen Server in der Cloud können Sie auch über die PowerShell verwalten. Dazu müssen Sie auf dem Rechner zunächst die Windows Azure PowerShell-Cmdlets installieren (*https://www.windowsazure.com/en-us/downloads/?fb=de-de* [Ms179-07-09]). Die Cmdlets funktionieren in Windows 7/8/8.1 und Windows Server 2008 R2/2012/2012 R2. Nach der Installation finden Sie die neue Verknüpfung *Windows Azure PowerShell* vor.

Sie können die Befehle aber mit dem Befehl *Import-Module Azure* auch in eine herkömmliche PowerShell-Sitzung laden. Um eine Verbindung aufzubauen, geben Sie nach dem Start zunächst *Get-AzurePublishSettingsFile* ein. Sie erstellen damit eine Datei, in der die Authentifizierung zu Ihrem Windows Azure-Abonnement aufgebaut wird. Die Datei laden Sie auf Ihren Rechner und fügen diese mit dem folgenden Cmdlet ein:

```
Import-AzurePublishSettingsFile <Pfad zur .publishsettings-Datei>
```

Um die Verbindung zu testen, rufen Sie *Get-AzureSubscription* auf. Eine Liste aller Befehle erhalten Sie mit dem Befehl *Get-Command -Module Azure*. Informationen zu virtuellen Servern in der Cloud erhalten Sie mit *Get-AzureVM*. Sie können also innerhalb einer PowerShell-Sitzung mit *Get-VM* Daten von lokalen Servern abrufen und mit *Get-AzureVM* Daten von Windows Azure-basierten virtuellen Servern.

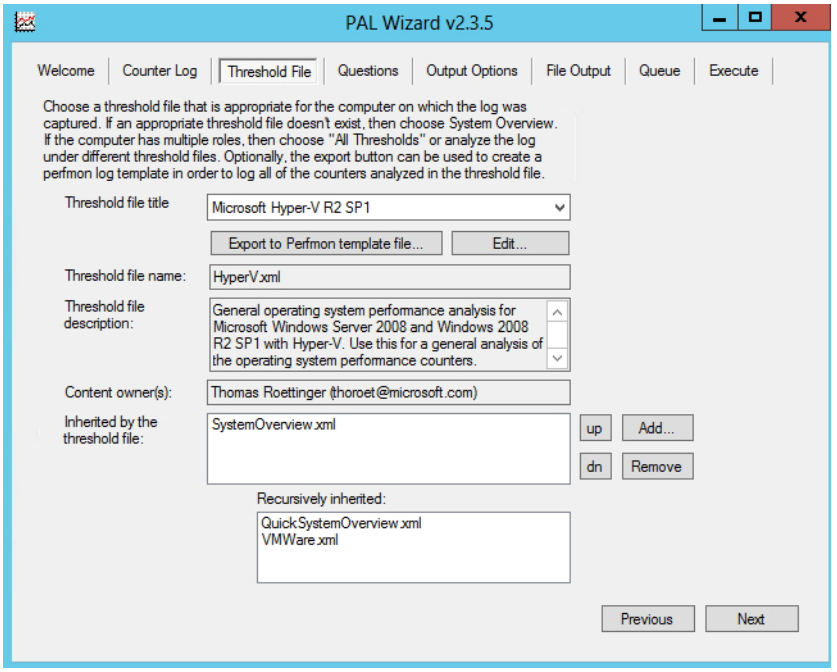
Langzeitanalyse von Hyper-V-Servern

Unternehmen, die virtuelle Server auf Basis von Hyper-V betreiben, haben die Möglichkeit, mit einem Freewaretool und der Leistungsüberwachung in Windows Engpässe zu finden und bei Bedarf zu beheben. Dazu wird die Auslastung des Servers eine bestimmte Zeit gemessen und danach ausgewertet.

Um Hyper-V effizient zu messen, nutzen Sie die Leistungsüberwachung. In Windows Server 2012 R2 suchen Sie dazu den Befehl *perfmon.msc* auf der Startseite. Um eine Langzeitmessung durchzuführen, müssen Sie einen Datensammelsatz erstellen. Klicken Sie dazu mit der rechten Maustaste auf *Datensammlersätze/Benutzerdefiniert* und erstellen Sie mit *Neu/Datensammlersatz* einen solchen Satz.

Während der Erstellung besteht die Möglichkeit, eine Vorlage einzulesen. Diese können Sie über das Tool *PAL* (*https://pal.codeplex.com* [Ms179-K07-10]) erhalten. Nach der Installation muss auf der Registerkarte *Threshold File* bei *Threshold file title* die Option *Microsoft Hyper-V R2 SP1* ausgewählt und dann auf *Export to Perfmon template file* geklickt werden. Diese Vorlage funktioniert auch mit Windows Server 2012 R2. Die Vorlage lesen Sie dann im Assistenten zum Erstellen von neuen Datensammlersätzen ein.

Abbildg. 7.35 Mit der Vorlagendatei des Tools PAL lassen Administratoren Server effizient überwachen



Nachdem der Datensammlersatz erstellt ist, müssen Sie in den Eigenschaften des Satzes noch Einstellungen vornehmen. Über *Zeitplan* erstellen Sie zunächst über *Hinzufügen* einen Zeitplan, an dem der Server den Datensammlersatz ausführt. Sinnvollerweise sollte das zu Zeiten stattfinden, an denen der Server auch belastet ist, um sinnvolle Ergebnisse zu erhalten.

Wenn der Datensammlersatz eine Zeitlang gelaufen ist, finden Sie einen Bericht in der Leistungsmessung vor. Die dazugehörige BLG-Datei ist normalerweise im Ordner *C:\Perflogs* zu finden. Die Datei lässt sich auch mit Zusatztools noch weiter auswerten, zum Beispiel mit dem bereits erwähnten Tool PAL.

Sie können die Sammlung auch mit dem Tool PAL auswerten. Dazu kopieren Sie die BLG-Datei des Berichts auf den Rechner mit PAL und öffnen die Datei über die Registerkarte *Counter Log*. Auf der Registerkarte *Threshold file* wählen Sie *Microsoft Hyper-V R2 SP1* aus. Danach wechseln Sie zur Registerkarte *Questions* und füllen die entsprechenden Fragen aus:

- **NumberOfProcessors** Anzahl an Kernen. Diese sehen Sie im Task-Manager.
- **ThreeGBSwitch** Ist der Server auf die maximale Nutzung von 3 GB begrenzt? Normalerweise ist das nicht der Fall.
- **SixtyFourBit** Handelt es sich um ein 64-Bit-Betriebssystem? Das ist bei Windows Server Windows Server 2012 R2 der Fall.
- **TotalMemory** Arbeitsspeicher des Servers
- **RAID5Drives** Laufwerkbuchstaben des RAID-5-Verbunds, falls vorhanden
- **RAID1Drives** Laufwerkbuchstaben des RAID1-Verbunds, falls vorhanden

Haben Sie alle Einstellungen vorgenommen, legen Sie auf der Registerkarte *File Output* noch den Pfad und den Namen der Exportdatei fest. Bestätigen Sie bei allen weiteren Fenstern die Standardeinstellungen.

Haben Sie die Auswertung durchführen lassen, erhalten Sie anschließend einen HTML-Bericht, mit dessen Hilfe Sie eventuelle Leistungsprobleme des Servers beheben können.

Migration von Vorgängerversionen

Eine direkte Aktualisierung auf Windows Server 2012 R2 ist von Servern mit Windows Server 2008 und Windows Server 2008 R2 möglich. Ältere Versionen lassen keine direkte Aktualisierung zu. Um einen Server mit Windows Server 2008 R2 und aktiviertem Hyper-V zu aktualisieren, starten Sie das Betriebssystem, legen den Windows Server 2012 R2-Datenträger ein und starten die Installation. Ein Assistent überprüft, ob der Server alle Voraussetzungen für eine Aktualisierung erfüllt.

Windows Server-Migrationstools nutzen

Microsoft unterstützt Unternehmen, die Serverrollen von Windows Server 2003/2008/2008 R2 zu Windows Server 2012 R2 migrieren wollen, mit den Windows Server-Migrationstools. Mit den Tools können Sie auch virtuelle Server zwischen Windows Server 2008/2008 R2 zu Windows Server 2012 R2-Zielservern migrieren. Bei den Tools handelt es sich um eine Sammlung verschiedener Cmdlets für die PowerShell.

Rufen Sie auf dem Zielserver mit Windows Server 2012 R2 das Cmdlet *Add-WindowsFeature Migration* auf, um die Tools zu aktivieren. Durch die Aktivierung ist eine Migration über die PowerShell möglich. Sind die Quelldateien auf dem Server nicht verfügbar, verwenden Sie den Aufruf *Install-WindowsFeature Migration –ComputerName <Computername>*. Um die Installation auf dem lokalen Server durchzuführen, lassen Sie *–ComputerName* weg. Benötigen Sie die Tools nicht mehr,

können Sie diese mit *Uninstall-WindowsFeature Migration –ComputerName <Computername>* wieder vom Server entfernen. Auf den Quellservern mit Windows Server 2008/2008 R2 entfernen Sie die Tools mit *smigdeploy /unregister*.

Die Tools befinden sich nach der Installation im Ordner *C:\Windows\System32\ServerMigrationTools*. Sie benötigen aus diesem Ordner zum Beispiel die Anwendung SmigDeploy auf dem Zielserver mit Windows Server 2012 R2, doch dazu später mehr.

Sie können die Migrationstools auch auf Core-Servern mit Windows Server 2012 R2 über die PowerShell installieren. In diesem Fall müssen Sie erst mit *%WinDir%\System32\WindowsPowerShell\v1.0\powershell.exe* eine PowerShell-Sitzung starten und können anschließend mit dem Cmdlet *Add-WindowsFeature Migration* die Tools installieren.

Um Hyper-V vom Quell- auf den Zielserver zu migrieren, müssen Sie auf dem Zielserver die Migrationstools installieren, wie beschrieben. Anschließend erstellen Sie auf dem Zielserver ein Installationspaket der Migrationstools für den Quellserver:

1. Öffnen Sie eine Eingabeaufforderung mit Administratorrechten.
2. Geben Sie den Befehl *cd %WinDir%\System32\ServerMigrationTools* ein.
3. Geben Sie den Befehl *smigdeploy /package /architecture amd64 /os WS08R2 /path <Ordner, zum Beispiel c:\temp\mig>* ein. Migrieren Sie von Windows Server 2003, verwenden Sie als OS den Wert *WS03*, für Windows Server 2008 verwenden Sie *WS08*.
4. Kopieren Sie diesen Ordner vom Zielserver mit Windows Server 2012 R2 auf den Quellserver.
5. Öffnen Sie auf dem Quellserver eine Eingabeaufforderung mit Administratorrechten und wechseln Sie in den Ordner mit den Migrationstools.
6. Geben Sie den Befehl *.\smigdeploy* ein, um die Migrationstools in Windows Server 2008/2008 R2 zu registrieren. In Windows Server 2008 R2 installieren Sie die Migrationstools über den Server-Manager.

Wichtig bei der Migration von Hyper-V-Servern auf Windows Server 2012 R2 ist die Kompatibilität der Prozessoren. Eine Migration ist nur dann möglich, wenn die Prozessoren des Quellservers mit den Prozessoren auf dem Zielserver kompatibel sind. Haben Sie die Migrationstools installiert, öffnen Sie zunächst eine PowerShell-Sitzung auf dem Quellserver und geben den Befehl *Add-PSSnapin Microsoft.Windows.ServerManager.Migration* ein. Mit diesem Befehl sind die Cmdlets in der PowerShell-Sitzung verfügbar.

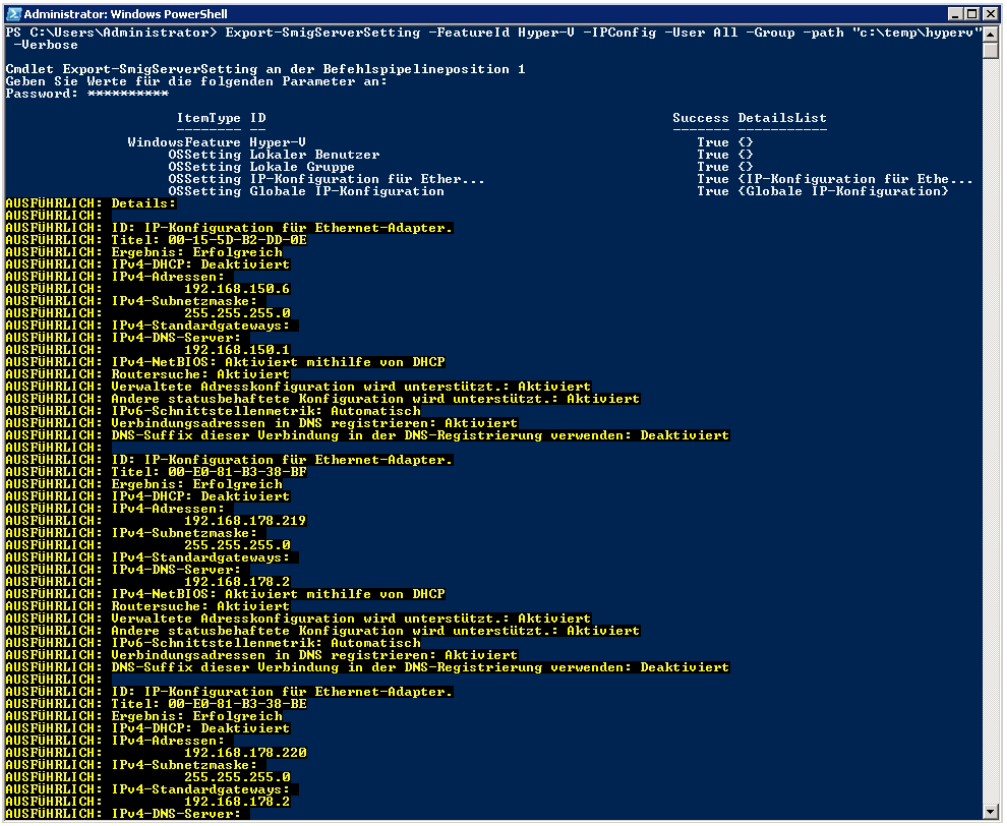
Im ersten Schritt müssen Sie auf dem Quellserver notwendige Daten für Hyper-V erfassen. Dazu verwenden Sie das Cmdlet *Export-SmigServerSetting*. Mit dem Befehl erstellen Sie eine XML-Datei, die vor allem wichtige Speicheroptionen der Daten der virtuellen Server enthält. Mit der Datei können Sie diese Einstellungen in einem Rutsch auf den Zielserver importieren.

Dazu ist es aber notwendig, dass die Laufwerkskonfiguration auf dem Quell- und dem Zielserver übereinstimmen. Ist das nicht der Fall, müssen Sie die entsprechenden Einstellungen in der XML-Datei auf dem Quellserver anpassen, bevor Sie die Migration auf den Zielserver durchführen. Ein Beispiel für die Syntax ist:

```
Export-SmigServerSetting -FeatureId Hyper-V -IPConfig -User All -Group -Path <Pfad> -
Verbose
```

Die Option *–User <Enabled | Disabled | All> –Group* bietet die Möglichkeit, auch die Sicherheitseinstellungen in die Datei zu integrieren, wenn Sie die Hyper-V-Verwaltung delegiert haben. Mit *–IPConfig* können Sie die IP-Einstellungen auf dem Quellserver mit integrieren, um diese später zu migrieren.

Abbildg. 7.36 Erstellen einer Migrationsdatei auf dem Quellserver



Hat das Cmdlet die Dateien erfolgreich erstellt, kopieren Sie diese auf den Zielserver. Ist die Laufwerks- oder Ordnerstruktur zwischen Quell- und Zielserver unterschiedlich, müssen Sie die neuen Pfade in der Datei *StoragePathMappings.xml* anpassen. Kopieren Sie in diesem Zusammenhang auch alle Daten aller virtuellen Computer auf den Zielserver, nicht nur die Migrationsdateien.

Auf dem Zielserver müssen Sie in der PowerShell zunächst wieder die Cmdlets für die Migration laden. Dazu verwenden Sie den Befehl *Add-PSSnapin Microsoft.Windows.ServerManager.Migration*. Anschließend verwenden Sie das Cmdlet *Import-SmigServerSetting* für die Migration der Einstellungen auf dem Zielserver, zum Beispiel:

```
Import-SmigServerSetting -FeatureId Hyper-V <Parameter wie -IPConfig oder -User wie beim
Export> -Path <Pfad> -Verbose -Force
```

Lassen Sie die IP-Einstellungen über *–IPConfig* migrieren, erstellen Sie eine Liste der Adressen, zum Beispiel:

```
–IPConfig All -SourcePhysicalAddress "<Quell-Adresse 1>","<Quell-Adresse 2>" -
TargetPhysicalAddress "<Ziel-Adresse 1>","<Ziel-Adresse 2>"
```

Externe virtuelle Netzwerke importiert das Cmdlet als interne virtuelle Netzwerke auf den Zielserver. Das heißt, Sie müssen nach der Migration auf dem Zielserver im Hyper-V-Manager die Einstellungen der virtuellen Netzwerke anpassen. Sie finden die Einstellungen über Manager für virtuelle Netzwerke. Hier können Sie für jedes Netzwerk festlegen, ob es intern oder extern ist.

Anschließend sollten Sie noch sicherstellen, dass alle Einstellungen der importierten virtuellen Server noch korrekt sind und diese unter Umständen nachträglich anpassen. Vor allem die Konfiguration der Datenträger, die IP-Adressen, die Konfiguration des Arbeitsspeichers und die Prozessoren sowie die generelle Konfiguration der Netzwerkverbindungen sind in diesem Zusammenhang wichtig.

Stellen Sie darüber hinaus sicher, dass der Assistent alle Computer vom Quell- auf den Zielserver importiert hat. Achten Sie auch darauf, ob die Snapshots auf dem Quell- und Zielserver übereinstimmen. Stimmt die Konfiguration, starten Sie die virtuellen Server und überprüfen im Ereignisprotokoll des Zielservers über *Anwendungs- und Dienstprotokolle/Microsoft/Windows/Hyper-V-Verwaltungsdienst für virtuelle Computer/Admin*, ob Fehler protokolliert werden.

Von VMware auf Hyper-V migrieren

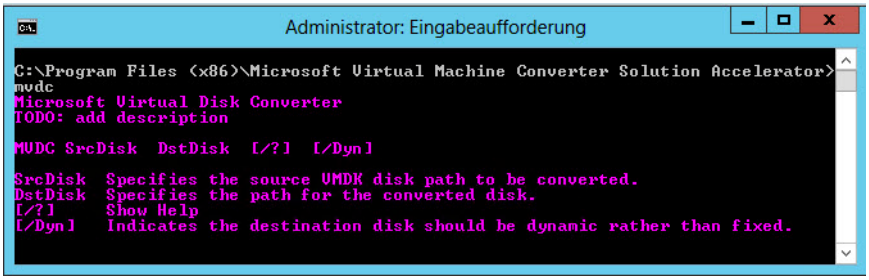
Um Unternehmen die Migration von virtuellen Servern von VMware auf Hyper-V zu erleichtern, stellt Microsoft das kostenlose Tool Microsoft Virtual Machine Converter zur Verfügung. Wollen Unternehmen außerdem noch kostenlos mit Hyper-V virtualisieren, steht zusätzlich noch Hyper-V Server 2012 zur Verfügung. Der kostenlose Server verfügt über den gleichen Funktionsumfang wie Windows Server 2012 R2 Datacenter Edition. Auch hier kann Microsoft Virtual Machine Converter helfen.

Microsoft unterstützt Sie mit dem kostenlosen Microsoft Virtual Machine Converter (*http://www.microsoft.com/en-us/download/details.aspx?id=34591* [Ms179-K07-11]), um virtuelle Server von VMware vSphere auf Hyper-V zu migrieren. Die aktuelle Version wurde von Microsoft bereits für Windows Server 2012 R2 und Hyper-V Server 2012 optimiert.

Während der Migration übernimmt das Tool nicht nur die virtuellen Festplatten aus dem VMware-Format (VMDK) zum Hyper-V-Format, sondern konfiguriert auch die virtuellen Netzwerke der virtuellen Server und passt die Server auch für Dynamic Memory an, also die dynamische Verwendung des Arbeitsspeichers, die Hyper-V seit Windows Server 2008 R2 SP1 unterstützt. Das Tool erlaubt auch die Migration von vSphere-Clustern und kann virtuelle Server zu Windows Server-Clustern übernehmen.

Als Gastbetriebssystem muss auf den virtuellen Servern Windows Server 2003/2003 R2 mit Service Pack 2, Windows Server 2008/2008 R2 oder Windows 7/Vista installiert sein. Das heißt, andere Betriebssysteme können Sie mit dem Tool nicht migrieren. Außerdem müssen alle virtuellen Server Bestandteil einer Active Directory-Gesamtstruktur sein.

Abbildg. 7.37 Die Übernahme virtueller Festplatten lässt sich auch skripten



Unternehmen müssen VMware vSphere (vCenter) 4.1/5.0 betreiben, um eine Migration zu erlauben. Die virtuellen Server lassen sich dann zu Servern mit Windows Server 2008 R2 SP1/2012, Hyper-V Server 2008 R2 SP1/2012 migrieren. Die Gastbetriebssysteme können dazu als 32-Bit oder als 64-Bit-Version vorliegen.

Während der Migration passt das Tool die Konfiguration der virtuellen Server an und berücksichtigt dabei auch die Einstellungen für den Arbeitsspeicher und den virtuellen Prozessor. Auch die VMware-Tools werden deinstalliert sowie die Hyper-V Integrationservices integriert. Die Migration findet über einen Assistenten statt. Bestandteil des Tools ist aber auch eine skriptbasierte Möglichkeit der Migration sowie eine Offlinekonvertierung der virtuellen Festplatten. Microsoft Virtual Machine Converter unterstützt dazu auch die PowerShell.

Um Migrationen in der Eingabeaufforderung durchzuführen, können Administratoren auch die beiden Befehlszeilentools Mvdc und Mvmc nutzen. Das Tool Mvdc kann virtuelle Festplatten konvertieren, und das Tool Mvmc kann die Migration kompletter virtueller Server skripten, genauso wie der Assistent mit grafischer Oberfläche.

Virtuelle Festplatten lassen sich mit dem Tool von verschiedenen Formaten zu dynamischen Festplatten oder zu Festplatten mit fester Größe konvertieren. Die Syntax der Tools inklusive Beispiele sehen Administratoren am schnellsten, wenn sie den Befehl in einer Eingabeaufforderung eingeben. Aktuell unterstützt der Converter die folgenden VMware-Festplattenformate:

- *monolithicSparse*
- *vmfsSparse*
- *monolithicFlat*
- *vmfs*
- *twoGbMaxExtentSparse*
- *twoGbMaxExtentFlat*
- *delta disk conversion*
- *Stream optimized disks*

Verwenden Sie als Zielformat eine dynamische Hyper-V-Festplatte, vergrößert das Tool diese aber auf deren maximale Größe. Es besteht aber die Möglichkeit, den leeren Plattenplatz wieder freizugeben. Wie das geht, erklärt Microsoft in der TechNet (*http://technet.microsoft.com/de-de/library/cc755149.aspx* [Ms179-K07-12]).

Wie die meisten Tools von VMware und Microsoft erlauben die Tools eine Migration nur in eine Richtung. Es besteht also keine Möglichkeit, die Server von Hyper-V zu VMware zu migrieren. Neben der Möglichkeit, offline virtuelle Festplatten zu migrieren, kann Microsoft Virtual Machine Converter auch aktive virtuelle Server migrieren. Verwenden Sie den Assistenten mit grafischer Oberfläche, muss die Quell-VM gestartet sein, sonst ist keine Migration zu Hyper-V möglich.

Das Benutzerkonto, mit dem Sie die Migration durchführen, muss über administrative Rechte in der Quell-VM als auch auf dem Hyper-V-Host verfügen und Bestandteil der gleichen Active Directory-Gesamtstruktur, besser der gleichen Domäne sein.

Außerdem muss sich das Tool per WMI mit dem Gastsystem verbinden können. Die entsprechende Option schalten Administratoren in der Firewall auf dem Server frei. Über das Netzwerk muss mit dem RPC-Port TCP 135 zugegriffen werden können. Die Datei- und Druckerfreigabe auf dem Gastserver muss ebenfalls aktiv sein, da der Assistent auch auf die TCP-Ports 139 und 445 sowie auf UDP 137 und 138 zugreifen muss.

Während der Migration verbindet sich das Tool online mit vCenter oder ESX/ESXi und hat Zugriff auf die laufenden VMware-VMs. Während der Migration erstellt das Tool einen Snapshot, passt den virtuellen Server an und kopiert die Daten auf den Hyper-V-Host.

Dabei pausiert das Tool auch den Gastserver. Nach der Migration bleibt der Quellserver auf dem VMware-Host zwar bestehen, wird durch das Tool aber abgeschaltet. Der virtuelle Server wird außerdem auf dem Hyper-V-Zielserver aktiviert. Wollen Sie das nicht, muss hier manuell eingegriffen werden. Die Einstellungen dazu nehmen Sie im Assistenten vor. Migrierte Server müssen in vielen Fällen auch neu aktiviert werden.

Klappt während der Migration etwas nicht, können Sie auch die Protokolldatei des Tools verwenden. Die Datei *MVMC.log* befindet sich im *Temp*-Ordner des Benutzerkontos, mit dem der Assistent durchgeführt wird.

Virtuelle Festplatten von Servern verwalten und optimieren

Im *Aktionen*-Bereich des Hyper-V-Managers finden Sie auf der rechten Seite die beiden Menübefehle *Datenträger bearbeiten* und *Datenträger überprüfen*.

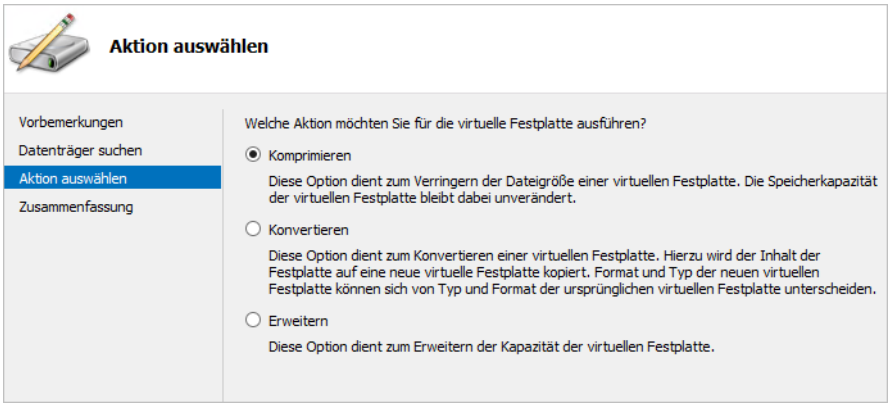
Mit *Datenträger überprüfen* starten Sie einen Scanvorgang einer beliebigen dynamischen Festplatte. Anschließend öffnet sich ein neues Fenster und zeigt die Daten dieser Festplatte an. So erfahren Sie, ob es sich um eine dynamisch erweiterbare Festplatte oder eine Festplatte mit fester Größe handelt. Auch die maximale Größe sowie die aktuelle Datenmenge zeigt das Fenster an.

Über *Datenträger bearbeiten* stehen Ihnen verschiedene Möglichkeiten zur Verfügung, um die aktuell ausgewählte Festplatte anzupassen:

- **Komprimieren** Diese Aktion steht nur bei dynamisch erweiterbaren Festplatten zur Verfügung. Der Vorgang löscht leere Bereiche in der VHD(X)-Datei, sodass diese deutlich verkleinert wird. Allerdings ergibt dieser Vorgang nur dann Sinn, 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(X)-Datei zu vergrößern
- **Zusammenführen** Der Assistent zeigt diesen Befehl nur dann an, wenn Sie eine differenzierende Festplatte auswählen, zum Beispiel die AVHD(X)-Datei eines Snapshots. Da diese Datei nur die aktuellen Unterschiede zu der VHD(X)-Quelldatei enthält und auf diese verifiziert ist, lassen sich die Daten zu einer gemeinsamen VHD(X)-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 der verifizierten VHD(X)-Datei gefunden ist. Eine differenzierende Festplatte kann aber auch in einer Kette auf eine andere differenzierende Datei verweisen, die dann wiederum auf die VHD(X)-Datei verweist. Dies kommt zum Beispiel dann vor, wenn mehrere Snapshots aufeinander aufbauen. Ist die Kette zerstört, zum Beispiel weil sich der Pfad einer Festplatte geändert hat, lässt sich mit diesem Befehl die Verbindung wiederherstellen.

Abbildg. 7.38 Virtuelle Festplatten bearbeiten



Durch verschiedene Optimierungen in Windows Server 2012 R2 können Sie virtuelle Festplatten auch auf Freigaben speichern. Außerdem kann Windows Server 2012 R2 auch als NAS-Server dienen. Im neuen Betriebssystem lassen sich nicht nur iSCSI-Ziele mit dem Server verbinden, sondern Server mit Windows Server 2012 R2 können selbst auch als iSCSI-Ziel arbeiten.

Wichtig für den Zugriff auf Freigaben im Netzwerk ist das Server Message Block-Protokoll. Dieses stellt den Zugriff von Clientcomputern zum Server dar. Windows 8 und Windows Server 2012 R2 kommen dazu mit dem neuen SMB-Protokoll 3. Dieses ist vor allem für den schnellen Zugriff über das Netzwerk gedacht, wenn Daten normalerweise lokal gespeichert sein sollten.

Beispiele dafür sind SQL Server-Datenbanken oder die Dateien von Hyper-V-Computern. Diese lassen sich mit SMB 3 performant auch über das Netzwerk verwenden. Die neue Version erlaubt mehrere parallele Zugriffe auf Dateifreigaben. Das heißt einzelne Zugriffe über das Netzwerk bremsen sich nicht mehr untereinander aus. Von den schnellen Netzwerkzugriffen profitieren vor allem Windows 8 und Windows Server 2012 R2.

Für eine schnelle Kommunikation zwischen Windows Server 2012 R2 müssen Netzwerkkarten die RDMA-Funktion (Remote Direct Memory Access) unterstützen. Bei dieser Funktion können Server über das Netzwerk Daten im Arbeitsspeicher austauschen. Wichtig ist diese Funktion vor allem, wenn Sie Windows Server 2012 R2 als NAS-Server einsetzen, also iSCSI-Ziel, und auf dem Server Datenbanken von SQL Server 2012 oder virtuelle Maschinen von Hyper-V speichern.

Sind im Unternehmen mehrere Server mit Windows Server 2012 R2 im Einsatz, tauschen diese Daten über das Netzwerk mit der neuen Multichannel-Funktion aus. Mit der Funktion lassen sich von einem Server auf eine Freigabe mehrere parallele Zugriffe durchführen. Das beschleunigt den Datenverkehr und sichert ihn auch gegen Ausfall eines einzelnen SMB-Kanals ab.

Der Vorteil liegt darin, dass Serverdienste Daten auch auf Servern speichern können, nicht auf der eigenen Festplatte. Sinnvoller Einsatz dazu ist in Umgebungen mit Hyper-V-Hosts, die auf Windows Server 2012 R2 aufbauen. Dazu ist weder die Installation eines Rollendiensts noch eine Konfiguration notwendig. Diesen beschleunigten Zugriff bietet Windows Server 2012 R2 automatisch.

Damit die Funktion genutzt werden kann, müssen die Netzwerkadapter natürlich entsprechende Geschwindigkeit liefern. Microsoft empfiehlt dazu entweder die Installation eines 10 Gigabit-Adapters oder mindestens den Einsatz von zwei 1 Gigabit-Adaptern. Für diese Funktion können Administratoren auch die neue Team-Funktion von Netzwerkkarten in Windows Server 2012 R2 nutzen. Über den Server-Manager lassen sich Netzwerkadapter zu Teams zusammenfassen, auch ohne dass die Treiber das direkt unterstützen.

SMB Direct ist ebenfalls zwischen Servern mit Windows Server 2012 R2 aktiv. Sie müssen weder Einstellungen vornehmen noch etwas installieren. Damit diese Funktion nutzbar ist, müssen die verbauten Adapter aber die RDMA-Funktion (Remote Direct Memory Access) unterstützen. Bei dieser Funktion können Server Daten aus dem Hauptspeicher eines Systems über das Netzwerk auf einen anderen Server übertragen, der aktuell Kapazitäten frei hat. So lassen sich überlastete Server beschleunigen, indem Sie Daten auf nicht ausgelastete Server übertragen. Damit das funktioniert, muss das Netzwerk extrem schnell sein und die Adapter müssen die Funktion nutzen können. Das sind Adapter mit den Typen iWARP, Infiniband und RDAM over Converged Ethernet (RoCE). Von dieser Technik profitieren hauptsächlich Hyper-V und SQL Server 2008 R2/2012.

Auch Hyper-V kann in Windows Server 2012 R2 direkt auf das SMB-Protokoll zugreifen. Der Sinn ist, dass Unternehmen die virtuellen Festplatten in Hyper-V (VHDX) nicht direkt auf dem Hyper-V-Host speichern, sondern auf einer Freigabe im Netzwerk. Diese ist dann mit SMB Multichannel, SMB Direct und Hyper-V over SMP sehr schnell zugreifbar für Hyper-V. Für Unternehmen sollen dabei keinerlei Einschränkungen entstehen. Auch hochverfügbare Lösungen wie Livemigration funktionieren so. Der gemeinsame Datenträger des Clusters muss sich dann nicht mehr in einem teuren SAN befinden, sondern es reicht ein Server mit Windows Server 2012 R2 und ausreichend Speicherplatz. Auf diesem Server können auch die Konfigurationsdateien der virtuellen Server gespeichert sein und eventuell vorhandene Snapshots. Cluster Shared Volume (CSV), der für Hyper-V notwendige Dienste für gemeinsame Datenträger in Clustern, unterstützt das SMB 3-Protokoll und dessen neue Funktionen ebenfalls.

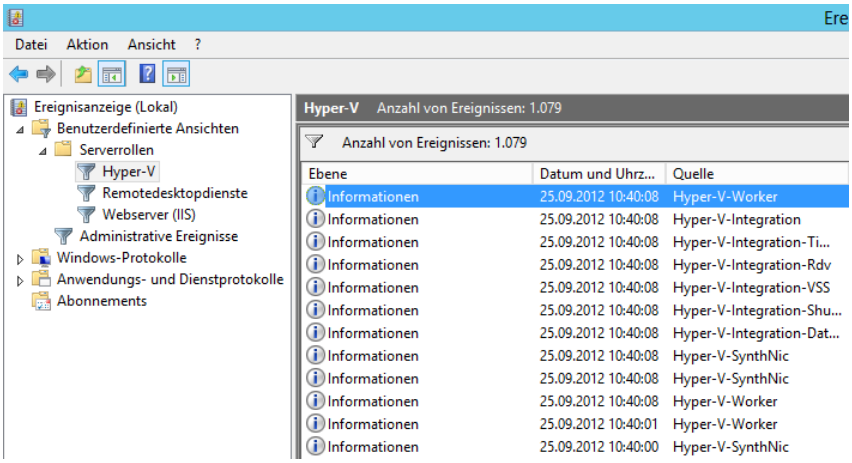
Dazu muss ebenfalls auf beiden Servern Windows Server 2012 R2 installiert sein. Ein Server läuft mit der Hyper-V-Rolle, der andere als Dateiserver. Die Umgebung muss außerdem über ein Active Directory verfügen. Hier müssen die Domänencontroller aber nicht zwingend auf Windows Server 2012 R2 umgestellt werden. Empfohlen, aber nicht unbedingt notwendig, ist ein Cluster für Hyper-V und die Dateidienste. In diesem Fall lässt sich die Umgebung wesentlich schneller und sicherer betreiben.

Setzen Unternehmen zusätzlich zu Windows Server 2012 R2 noch SQL Server 2008 R2 oder SQL Server 2012 ein, profitieren auch hier die Datenbankserver vom neuen SMB-Protokoll. Hier gelten die gleichen Voraussetzungen wie bei Hyper-V over SMB. Ältere Editionen als SQL Server 2008 R2 können diese Funktion nicht nutzen. Auch hier ist ein Cluster wieder der beste Weg. Sinn dieser Funktion ist, dass Transaktionsprotokolle oder Datenbankdateien sowie eventuelle Sicherungen oder ausgelagerte Dateien auf Dateiservern mit Windows Server 2012 R2 ausgelagert sind. Außerdem hat Microsoft den Zugriff von schnellen Schreib-/Lese-Vorgängen deutlich optimiert. Davon profitiert vor allem SQL Server 2012. Auch der Zugriff auf Data-Warehouses hat Microsoft durch die Erhöhung des Werts für Maximum Transmission Unit (MTU) deutlich verbessert.

Fehler in Hyper-V finden und beheben

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. 7.39 Windows Server 2012 R2 protokolliert Hyper-V-Ereignisse im Ereignisprotokoll



Ein häufiges Problem beim Ausführen von virtuellen Maschinen ist es, 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.

Oft 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 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 Gasts angezeigt werden. Ohne installierte Integrationsdienste stehen die verschiedenen Treiber des Hosts nicht in den virtuellen Computern zur Verfügung.

Berechtigungen in Hyper-V delegieren

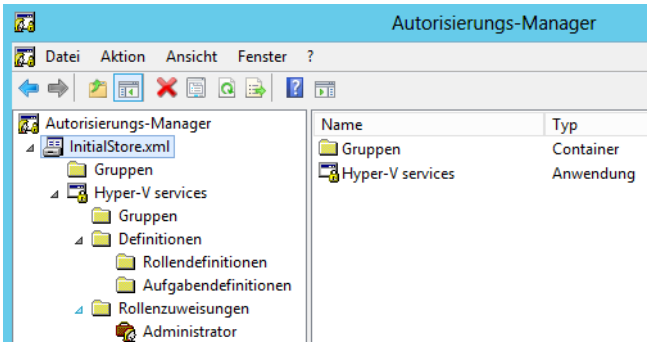
Hyper-V bietet die Möglichkeit, auf Basis der Windows-Gruppenzugehörigkeit oder des Benutzernamens bestimmte Rechte an Administratoren zu delegieren. Dies ist zum Beispiel sinnvoll, wenn nicht jeder Administrator alle Rechte an einem Server haben soll. Um diese Rechte zu delegieren, verwenden Sie den Autorisierungs-Manager von Windows Server 2012 R2. Diesen starten Sie am schnellsten, indem Sie den Befehl *azman.msc* auf der Startseite eintippen. 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 Eintrag *Autorisierungs-Manager* und wählen *Autorisierungsspeicher öffnen* aus.

Im Anschluss navigieren Sie in den 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. Damit Sie den Ordner *ProgramData* sehen, müssen Sie im Menüband des Explorers auf der Registerkarte *Ansicht* die ausgeblendeten Elemente anzeigen lassen.

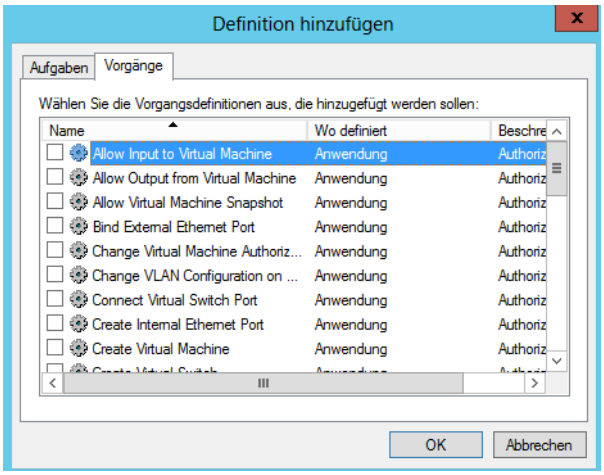
Achten Sie darauf, dass dazu die versteckten Systemdateien angezeigt werden müssen. Jetzt öffnet sich der Speicher. Anschließend lassen sich über das Fenster definierte Rollen erstellen und Befehle zuweisen.

Abbildg. 7.40 Hyper-V Aufgaben mit dem Autorisierungs-Manager delegieren



Klicken Sie mit der rechten Maustaste zunächst auf *Aufgabendefinitionen* und dann auf *Neue Aufgabendefinition*. Anschließend klicken Sie im neuen Fenster auf *Hinzufügen* und bestätigen das Informationsfenster. Auf der Registerkarte *Vorgänge* sehen Sie alle Aufgaben, die sich an Benutzer oder Gruppen verteilen lassen.

Abbildg. 7.41 Der Autorisierungsspeicher bietet mehrere Definitionen an, um Aufgaben zu delegieren



Über den Knoten *Rollenzuweisung* können Sie basierend auf diesen Aufgaben einzelnen Anwendern 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 Eintrag *Neuer Bereich* aus. 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.

In diesem 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 mit der rechten Maustaste unterhalb von *Microsoft Hyper-V services/Definitionen* auf *Rollendefinitionen* und wählen Sie im Kontextmenü den Befehl *Neue Rollendefinition* aus.
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. Es öffnet sich das neue Fenster *Definition hinzufügen*.
7. Wechseln Sie auf die Registerkarte *Vorgänge*.
8. Wählen Sie die Aufgaben aus, die diese Rolle durchführen darf, und bestätigen Sie diese.
9. Nachdem Sie eine neue Rolle definiert und deren Berechtigungen konfiguriert haben, legen Sie fest, welche Windows-Benutzer mit dieser Rolle arbeiten dürfen. Legen Sie dazu 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*.
10. Wählen Sie im neuen Fenster zunächst Ihre erstellte Rollendefinition *Hyper-V-Manager* aus.
11. Klicken Sie als Nächstes mit der rechten Maustaste unterhalb von *Rollenzuweisungen* auf Ihre erstellte Rolle und wählen Sie *Benutzer und Gruppen zuweisen* sowie *Von Windows und Active Directory* aus.

Legen Sie anschließend die Gruppe oder den Benutzer fest, dem Sie diese Rolle zuweisen wollen. Nach der Auswahl zeigt die Konsole auf der rechten Seite die Gruppe an, wenn Sie die entsprechende Rollendefinition anklicken. Die Benutzer können jetzt bei der Anmeldung an ihrem Computer die Aufgaben durchführen, die Sie konfiguriert haben.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Betriebssysteme mit der neuen Hyper-V-Version in Windows Server 2012 R2 virtualisieren. Sie finden hier zahlreiche Tricks und Praxisanleitungen zur Virtualisierung von Servern im Unternehmen. Auch die Möglichkeit, Hyper-V zentral im Netzwerk von einer Windows 8-Arbeitsstation aus zu verwalten, sind Thema dieses Kapitels. Wir sind darauf eingegangen, wie Sie virtuelle Switches und auch virtuelle Datenträger anlegen und verwalten.

Im nächsten Kapitel finden Sie weiterführende Informationen zu Hyper-V, zum Beispiel, wie Sie Snapshots (Prüfpunkte) erstellen und virtuelle Server oder Hyper-V-Server sichern.

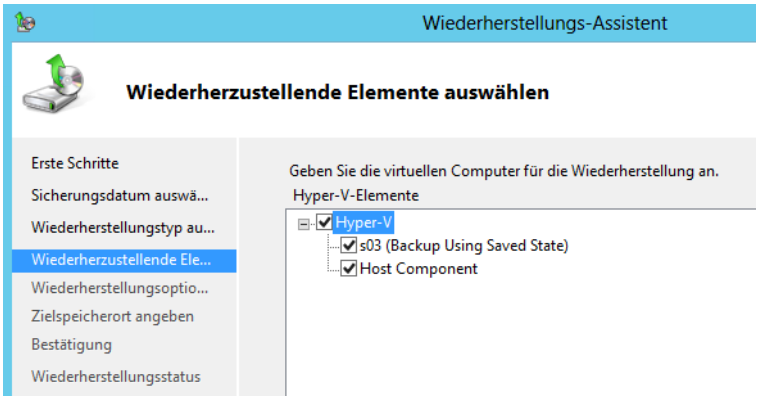
Kapitel 8

Hyper-V – Datensicherung und Wiederherstellung

In diesem Kapitel:

Im vorherigen Kapitel haben wir Ihnen gezeigt, wie Sie Hyper-V installieren und einrichten sowie virtuelle Server erstellen und konfigurieren. In diesem Kapitel gehen wir ausführlicher auf die Datensicherung und Wiederherstellung von Hyper-V ein. In Kapitel 35 zeigen wir Ihnen, wie Sie Windows Server 2012 R2 mit dem internen Sicherungsprogramm sichern und wiederherstellen. Sie haben über dieses Tool auch die Möglichkeit, virtuelle Server oder den kompletten Host wiederherzustellen. In Kapitel 35 zeigen wir Ihnen zusätzlich, wie Sie Daten in die Cloud mit Windows Azure Online Backup sichern.

Abbildg. 8.1 Mit der internen Datensicherung in Windows Server 2012 R2 können Sie auch Hyper-V und virtuelle Server wiederherstellen



Hyper-V und virtuelle Server richtig sichern

Unternehmen, die über Hyper-V oder andere Virtualisierungslösungen virtuelle Server zur Verfügung stellen, müssen das Datensicherungskonzept der virtuellen Maschinen und der zugrundeliegenden Hosts in die Sicherungsstrategie mit einbinden. Die Sicherung des Hosts sowie der installierten virtuellen Server verlangt andere Herangehensweisen als die Sicherung herkömmlicher physischer Server.

Die meisten Unternehmen setzen auf Zusatzsoftware bei der Datensicherung. Hier bieten mittlerweile viele Hersteller Unterstützung speziell für Hyper-V, VMware oder Citrix an. Diese Lösungen sichern die Server und den Host auf Ebene des Hypervisors. Ein Beispiel für eine solche Lösung ist der Data Protection Manager (DPM) 2012 R2 von Microsoft oder Symantec Backup Exec. DPM beherrscht auch die Onlinesicherung von Hyper-V-Hosts und den laufenden virtuellen Servern.

Auch virtuelle Server lassen sich mit herkömmlichen Sicherungsstrategien sichern. Dazu installieren Sie auf den virtuellen Servern die Agents der entsprechenden Sicherungslösung. Dadurch behandelt das Datensicherungsprogramm diese Server genauso wie normale physische Server. Diese Art der Datensicherung sichert aber nicht die Konfiguration der virtuellen Maschine und verwendet auch nicht die optimierten Methoden, die Hyper-V zur Verfügung stellt.

Die Agents nutzen außerdem nicht den Hypervisor und können daher weder die Schattenkopien noch Prüfpunkte (Snapshots, Momentaufnahmen) zur Sicherung nutzen. Dies erhöht die zu sichernde Datenmenge und die Dauer der Datensicherung. Datensicherungen, die Hyper-V unterstützen, nutzen Schnittstellen von Hyper-V zur optimalen Sicherung. In diesem Zusammenhang kann die Software Prüfpunkte der virtuellen Server zur Sicherung sowie den Schattenkopiedienst

verwenden. Das ist wesentlich effizienter, schneller und auch stabiler, als herkömmliche Sicherungen. Die Anwendung erstellt Prüfpunkte im laufenden Betrieb automatisch, und die virtuellen Server stehen weiterhin den Anwendern zur Verfügung. Solche Onlinesicherungen belasten die Hardware des Hosts nicht und ermöglichen auch Sicherungen während dem Betrieb.

Müssen Sie mehrere virtuelle Server auf einem Host sichern, kann eine kompatible Lösung auch gemeinsame Dateien erkennen und muss diese nicht doppelt sichern. Laufen auf einem Hyper-V-Host zum Beispiel 10 Server mit Windows Server 2008 R2/2012/2012 R2, erkennt das die Software und sichert die Daten nicht doppelt, sondern erkennt identische Systemdateien und sichert nur unterschiedliche Dateien.

Bei der Sicherung von Hyper-V spielt der Schattenkopiedienst eine wichtige Rolle, da die Sicherung auf Prüfpunkte des Servers und der virtuellen Server aufbaut. Mit aktiviertem Schattenkopiendienst lassen sich Hyper-V-Server inklusive der laufenden virtuellen Server sichern.

Im Notfall – Wiederherstellen eines Hyper-V-Hosts

Stürzt ein Hyper-V-Host ab, besteht die Gefahr, dass sich die virtuellen Maschinen nach einer Wiederherstellung nicht mehr in den Server importieren lassen. Sie können zwar problemlos auf dem neuen Server die virtuellen Server neu erstellen und die gesicherten virtuellen Festplatten zurückspielen sowie mit den neuen Servern verbinden. Allerdings ist die Konfiguration der virtuellen Maschine oft verloren, wenn auf dem Hyper-V-Server die Konfigurationsdateien der virtuellen Server nicht mitgesichert sind. Dazu kommt, dass Sie in einem solchen Fall das Betriebssystem auf dem virtuellen Server unter Umständen neu aktivieren müssen.

Ein solches Problem kann häufig auftreten, wenn die Hardware eines Servers defekt ist, zwar eine Sicherung vorhanden ist, aber die virtuellen Server nicht exportiert wurden. Zum Import einer virtuellen Maschine in Hyper-V ist eine XML-Datei notwendig, die der Assistent beim Exportieren erstellt. Ohne diese Datei lässt sich in Hyper-V kein virtueller Server ohne Weiteres importieren. Ist die Datei aber in der Datensicherung des Servers enthalten, können Sie den Server importieren.

Ist der Quellserver, auf dem Sie Hyper-V betrieben haben, defekt und Sie haben auf einem neuen Server Hyper-V neu installiert, besteht der erste Schritt darin, dass Sie den Ordner, in dem die virtuellen Server gespeichert sind, wiederherstellen. In diesem Ordner sind auch die virtuellen Festplatten der Server sowie die Konfigurationsdateien der Server gespeichert. Nach dieser Wiederherstellung können Sie im Hyper-V-Manager über den Assistenten *Virtuellen Computer importieren* prüfen, ob Sie die Server importieren können. Gelingt das ohne Fehler, ist alles in Ordnung.

Zu jedem virtuellen Server gehört eine XML-Datei mit den Einstellungen der VM. Diese finden Sie normalerweise entweder im Unterordner des virtuellen Servers oder im Verzeichnis, das Sie bei der Erstellung angegeben haben. Aus diesem Grund ist es für Hyper-V-Hosts auch sehr empfehlenswert, wenn Sie alle Festplatten einschließlich der Systemfestplatten sichern lassen. Die Datei hat eine ID als Namen, zum Beispiel *7415BF2C-5BCA-46DE-9B60-6B3FBFDC9BF3.xml*. Merken Sie sich den Namen der Datei sowie den Ordner, in dem die Datei gespeichert ist.

Damit sich der virtuelle Server in Hyper-V problemlos importieren lässt, müssen Sie in der Datensicherung also dessen XML-Datei berücksichtigt haben und diese mit den virtuellen Festplatten wiederherstellen. Notfalls können Sie in Windows mit dem Tool Mklink eine Verknüpfung im Betriebssystem herstellen, die auf die wiederhergestellte Datei verweist. Mit dieser Verknüpfung können Sie Hyper-V eine Konfigurationsdatei für den Import vortäuschen:

1. Öffnen Sie über das Schnellmenü (+ X) eine Eingabeaufforderung mit Administratorrechten.
2. Anschließend geben Sie den folgenden Befehl ein und führen ihn aus:

```
mklink "<Sollordner der XML-Datei, die der Import-Assistent benötigt>" "<Pfad, in dem
die XML-Datei gespeichert ist>"
```

Durch den Befehl erscheint anschließend im Ordner ein Junction Point zur XML-Datei des virtuellen Servers. Die Datei ist aber weiterhin in ihrem Quellordner gespeichert.

Erhalten Sie einen Syntax- oder einen anderen Fehler angezeigt, überprüfen Sie, ob im Ordner nicht bereits die Datei vorhanden ist. In diesem Fall können Sie sich die Erstellung des Junction Points sparen. Wird Ihnen während der weiteren Schritte zur Wiederherstellung ein Berechtigungsfehler angezeigt, können Sie diesen Fehler umgehen, indem Sie über das Kontextmenü die Eigenschaften des neuen Junction Points aufrufen. Wechseln Sie dann zur Registerkarte *Sicherheit* und geben dem Benutzer *Jeder* Vollzugriffsrechte auf die Datei.

Haben Sie für den virtuellen Server auch Prüfpunkte erstellt, können Sie im Unterordner *Snapshots* der Server auch die XML-Datei der einzelnen Prüfpunkte auf dem gleichen Weg verlinken.

Nachdem Sie die entsprechenden Befehle eingegeben haben, starten Sie den Hyper-V-Dienst auf dem Server neu. Sie können den Dienst auch in der Eingabeaufforderung mit dem Befehl *net stop vmms* beenden und mit *net start vmms* neu starten. Die virtuellen Server sollten anschließend wieder im Hyper-V-Manager verfügbar sein. Überprüfen Sie als Nächstes deren Konfiguration und ändern Sie Einstellungen ab, falls diese nicht korrekt übernommen wurden. Um die Konfiguration optimal abzuschließen, sollten Sie jetzt die virtuellen Server über deren Kontextmenü exportieren, danach im Hyper-V-Manager löschen und neu importieren lassen.

Prüfpunkte von virtuellen Servern erstellen

Prüfpunkte helfen dabei, den Zustand von virtuellen Servern vor Konfigurationsänderungen oder zur Sicherung zu sichern. Das heißt Sie können bei Problemen in wenigen Sekunden den virtuellen Server auf den ursprünglichen Zustand zurücksetzen. Prüfpunkte sind aber auch bei der Sicherung von Servern nützlich, zumindest wenn ein optimales Datensicherungsprogramm für Hyper-V im Einsatz ist.

HINWEIS In Windows Server 2012 R2 hat Microsoft Snapshots in Prüfpunkte umbenannt, in Windows Server 2012 war die Bezeichnung noch Momentaufnahmen. Die Technik beschreibt die gleiche Funktion wie Snapshots.

Prüfpunkte verstehen und Unterschiede zwischen Windows Server 2008 R2 und Windows Server 2012 R2

Erstellen Sie einen Prüfpunkt, sperrt Hyper-V die *.vhd(x)*-Datei des virtuellen Servers vor zukünftigen Änderungen und speichert alle zukünftigen Daten in eine neue differenzierende Festplatte (*.avdx*). Erstellen Sie auf Basis dieses Prüfpunkts einen weiteren Prüfpunkt, verwendet auch dieser eine neue *.avdx*-Datei, die wiederum auf die vorangegangene *.avdx*-Datei verweist. Je mehr Prüfpunkte Sie erstellen, desto mehr *.avdx*-Dateien werden angelegt, was die Leistung des Servers beeinträchtigt.

Nach der Erstellung eines Prüfpunkts finden Sie in diesem Ordner mehrere Dateien, darunter eine *.xml*-Datei für jeden Prüfpunkt. Standardmäßig besteht ein virtueller Server aus einer *.vhd(x)*-Datei (seiner Festplatte), einer *.xml*-Datei, welche die Einstellungen des Servers enthält, sowie den Statusdateien mit den Endungen *.bin* und *.vsv*.

Erstellen Sie einen Prüfpunkt, legt der Server zunächst eine neue virtuelle Platte (eine *.avhd(x)*-Datei) an. Diese Datei verwendet als Basis die *.vhd(x)*-Datei. Der Prüfpunkt schreibt zukünftige Änderungen des Servers in die *.avhd(x)*-Datei. Ab jetzt verweist die *.xml*-Datei des virtuellen Servers auf die *.avhd(x)*-Datei, welche die Änderungen seit dem Prüfpunkt enthält. Diese verwendet wiederum die *.vhd(x)*-Datei als Grundlage.

Setzen Sie den Server zum Stand eines Prüfpunkts zurück, verwendet Hyper-V nicht mehr die *.avhd(x)*-Datei, sondern wieder die originale *.vhd(x)*-Datei. Sie sehen den Verweis zu der *.avhd(x)*-Datei auch in der *.xml*-Konfigurationsdatei des Servers. Ein Prüfpunkt eines virtuellen Servers besteht aus der *.bin*- und *.vsv*-Date mit der Konfiguration des Servers zum Zeitpunkt des Prüfpunkts. Auf diese Dateien verweist die *.xml*-Datei des Prüfpunkts. Das heißt, ein Prüfpunkt eines virtuellen Servers enthält folgende Dateien:

- Eine *.xml*-Datei, die auf die Statusdateien (*.vsv* und *.bin*) verweist
- Eine neue *.vsv*-Datei und eine neue *.bin*-Datei
- Eine neue differenzierende Festplatte (*.avhd(x)*), welche die produktive Festplatte des Servers (*.vhd(x)*) als Quelle nutzt

Erstellen Sie einen weiteren Prüfpunkt, der auf den Stand des ersten Prüfpunkts aufbaut, verwendet dieser ebenfalls eine neue differenzierende Festplatte (*.avhd(x)*). Diese erhält als Quelle aber nicht die produktive virtuelle Festplatte des Servers (*.vhd(x)*), sondern die *.avhd(x)*-Datei des vorherigen Prüfpunkts. Dies liegt daran, dass der neue Prüfpunkt auf dem alten Prüfpunkt beruht. Daher muss hier ein stufenweiser Aufbau erfolgen.

Da heißt, je mehr Prüfpunkte eines Servers Sie erstellen, umso mehr differenzierende Festplatten (*.avhd(x)*) setzen Sie ein, die aufeinander aufbauen. Durch diesen Aufbau kann die Leistung eines Servers stark einbrechen.

Bewahren Sie Prüfpunkte also nur so lange auf, wie es unbedingt notwendig ist. Löschen Sie einen Prüfpunkt, entfernt Hyper-V auch die erstellten *.xml*, *.vsv*- und *.bin*-Dateien. Die differenzierenden Festplatten (*.avhd(x)*) schreibt Hyper-V in Windows Server 2008 R2 aber erst dann in die produktive virtuelle Festplatte (*.vhd(x)*), wenn Sie den Server einmal ausschalten, nachdem Sie den Prüfpunkt gelöscht haben. In Windows Server 2012 R2 findet dieser Vorgang online statt, der Server muss dazu nicht neu gestartet werden (Onlinemerge).

Löschen Sie einen oder mehrere Prüfpunkte eines virtuellen Servers, fahren Sie in Windows Server 2008 R2 den Server einmal herunter und schalten ihn aus. Bei diesem Vorgang schreibt Hyper-V die Daten der differenzierenden virtuellen Festplatten (*.avhd*) in die produktive Festplatte (*.vhd*) und löscht anschließend die *.vhd*-Datei. Erst nach diesem Vorgang steigt die Leistung des virtuellen Servers wieder an. Löschen Sie mehrere Prüfpunkte auf einmal, kann das Herunterfahren und Ausschalten eines Servers auch länger dauern. In Windows Server 2012 R2 können Sie sich diesen Vorgang sparen.

Prüfpunkte von virtuellen Servern erstellen

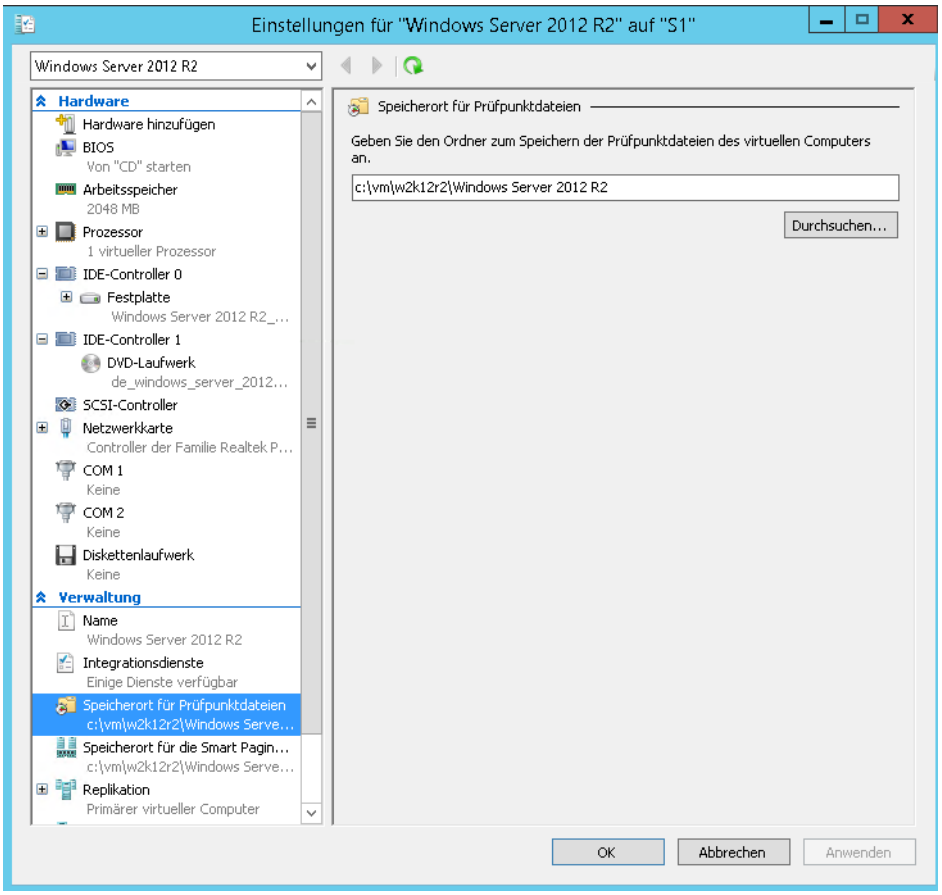
Hyper-V ermöglicht die Erstellung von Prüfpunkten auch ohne dass Sie Zusatzanwendungen installieren. Den entsprechenden Befehl finden Sie im Kontextmenü der virtuellen Computer im Hyper-V-Manager.

Mit Windows Server 2012 hat Microsoft die Prüfpunkte verbessert. So besteht jetzt die Möglichkeit, Prüfpunkte zusammenzuführen, ohne dass virtuelle Server heruntergefahren werden müssen. Diese Onlinemerges sollen die Ausfallzeiten von virtuellen Servern reduzieren. Verwenden Sie die neue Hyper-V-Replikation in Windows Server 2012 R2, überträgt der Assistent die Daten auf Basis von Prüfpunkten und erstellt für bereits übertragene virtuelle Server auf dem Zielserver erneut Prüfpunkte.

Während der Erstellung des Prüfpunkts bleibt der Computer online und steht weiterhin den Anwendern zur Verfügung. Die erstellten Prüfpunkte zeigt der Hyper-V-Manager im mittleren Bereich der Konsole an. Hyper-V speichert die Prüfpunkte in dem Ordner, den Sie in den Einstellungen des virtuellen Computers im Bereich *Speicherort für Prüfpunktdateien* angeben. Sobald ein Prüfpunkt erstellt ist, können Sie den Ordner nicht mehr ändern.

Rufen Sie den Befehl *Zurücksetzen* im Kontextmenü des virtuellen Computers auf, wendet Hyper-V den letzten erstellten Prüfpunkt an und setzt den Computer auf diesen Stand zurück. Prüfpunkte ersetzen allerdings keine Datensicherung, sondern bieten nur eine Rückversicherung vor einer Konfigurationsänderung auf dem Server.

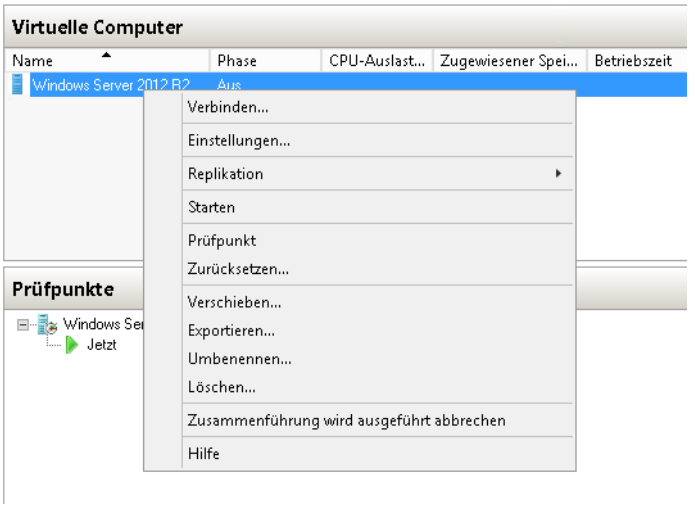
Abbildg. 8.2 Festlegen des Speicherorts von Prüfpunkten



Prüfpunkte selbst erstellen Sie über den Befehl *Prüfpunkt* im Kontextmenü. Durch diesen Vorgang erstellt der Server eine neue differenzierende Festplatte der aktuellen Systemfestplatte. Beim Zurücksetzen gehen aber keine Änderungen verloren, sondern werden wiederum in einem anderen Prüfpunkt erfasst.

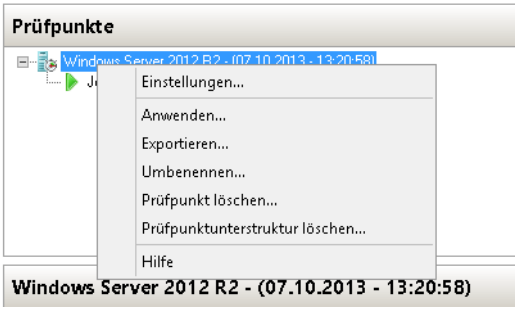
Wenn Sie einen Server zurücksetzen oder einen älteren Prüfpunkt anwenden beziehungsweise Prüfpunkte löschen und die differenzierende Festplatte des Prüfpunkts in die übergeordnete *.vhdx*-Datei überführen, vergrößert sich unter Umständen diese Datei. In diesem Fall sollten Sie diese im Hyper-V-Manager bearbeiten und verkleinern lassen. Sie finden dazu im *Aktionen*-Bereich den Eintrag *Datenträger bearbeiten*.

Abbildg. 8.3 Erstellen von Prüfpunkten oder Zurücksetzen eines Servers mit dem Prüfpunkt



Auch für die einzelnen Prüfpunkte steht ein Kontextmenü zur Verfügung, über das Sie diese steuern. Setzen Sie eine Hyper-V-kompatible Datensicherung ein, kann diese ebenfalls automatisiert einen solchen Prüfpunkt erstellen und dessen Daten sichern.

Abbildg. 8.4 Verwalten der Prüfpunkte von virtuellen Servern



Verwalten der Prüfpunkte von virtuellen Servern

Im Kontextmenü von Prüfpunkten stehen verschiedene Möglichkeiten zur Verfügung:

- **Einstellungen** Hierüber rufen Sie die Einstellungen des virtuellen Computers auf, zu dem dieser Prüfpunkt gehört. Es handelt es sich dabei um die Einstellungen, die zum Zeitpunkt des Erstellens gültig waren. Haben Sie Einstellungen nach dem Erstellen des Prüfpunkts geändert, sind diese an dieser Stelle nicht zu sehen. Auf diese Weise schützen Sie auch die Einstellungen von virtuellen Servern.
- **Anwenden** Wählen Sie diese Option aus, setzt der Assistent den virtuellen Computer wieder auf den Stand zurück, an dem Sie diesen Prüfpunkt erstellt haben. Vorher erscheint aber ein Abfragefenster, das Sie auf die Folgen hinweist. Außerdem können Sie vorher noch mal einen

aktuellen Prüfpunkt erstellen. Dieser sichert dann den aktuellen Zustand. Im Gegensatz zum Zurücksetzen über das Kontextmenü der VM können Sie hier nicht nur den letzten Prüfpunkt verwenden, sondern beliebige Prüfpunkte.

- **Exportieren** Beim Exportieren von virtuellen Servern in Windows Server 2012 R2 können Sie jetzt auch Prüfpunkte (Snapshots) berücksichtigen. Über das Kontextmenü eines Prüfpunkts können Sie daher einen virtuellen Server mit dem Stand des Prüfpunkts exportieren und auf anderen Servern wieder importieren. Ebenfalls neu ist die Möglichkeit, dass Sie diese Vorgänge im laufenden Betrieb des virtuellen Servers durchführen können.
- **Umbenennen** Mit dieser Option weisen Sie dem Prüfpunkt einen anderen Namen zu. Hyper-V verwendet als Namen normalerweise das Datum und die Uhrzeit. Über diesen Menübefehl können Sie zum Beispiel noch Informationen hinzufügen, warum Sie den Prüfpunkt erstellt haben.
- **Prüfpunkt löschen** Löscht den Prüfpunkt und die dazugehörigen Daten vom Server und überführt die notwendigen Daten in die produktive Festplatte. Die Zusammenhänge erklären wir im nächsten Abschnitt. Beim Löschen eines Prüfpunkts gehen daher keine Daten verloren, sondern Änderungen, die Sie seit dem Erstellen des Prüfpunkts durchgeführt haben, werden in die virtuelle Festplatte des Servers geschrieben und anschließend wird der Prüfpunkt und seine differenzierende Festplatte gelöscht (*.avdx*). In Windows Server 2012 R2 kann dieser Vorgang auch online durchgeführt werden. Der virtuelle Server kann also weiter in Betrieb sein.
- **Prüfpunkt-Unterstruktur löschen** Diese Option löscht den aktuellen Prüfpunkt sowie alle Sicherungen, die Sie nach dem Prüfpunkt erstellt haben und auf diesen aufbauen. Der Vorgang ist ähnlich zu *Prüfpunkt löschen*, führt aber alle zusammengehörigen Prüfpunkte zusammen.

Datensicherung und Prüfpunkte bei Hyper-V im Cluster

Setzen Sie Hyper-V im Cluster ein, um beispielsweise die Livemigration zu nutzen, müssen Sie bei der Datensicherung und der Erstellung von Prüfpunkten einige wichtige Punkte beachten. Sie sollten es möglichst vermeiden, Prüfpunkte von laufenden virtuellen Maschinen in Clustern zu erstellen. Setzen Sie nämlich einen solchen Prüfpunkt zurück, setzt dieser nicht nur den Inhalt der virtuellen Festplatte zurück, sondern auch den des Arbeitsspeichers der VM. Dieser Umstand bereitet vor allem im Zusammenhang mit der Livemigration Probleme. Wenn Sie also Prüfpunkte von VMs in einem Cluster durchführen wollen, fahren Sie die VM herunter. Auch wenn Sie einen Prüfpunkt auf eine VM anwenden wollen, sollten Sie die Maschine dazu herunterfahren.

Bei Domänencontrollern sichern Prüfpunkte auch die Active Directory-Datenbank. Setzen Sie auf einem Domänencontroller mit Windows Server 2008 R2 einen Prüfpunkt zurück, kann es zu Inkonsistenzen der Active Directory-Datenbank kommen, die auch die anderen Domänencontroller beeinflusst. Das liegt daran, dass in Active Directory alle Objekte eine bestimmte Nummer besitzen, die Update Sequence Number (USN).

Jeder Domänencontroller hat eine eigene Liste dieser USNs und befindet sich auch selbst in dieser Liste. Setzen Sie einen Prüfpunkt zurück, ändern sich die USNs zahlreicher Objekte, was mit hoher Wahrscheinlichkeit zu Inkonsistenzen führt. In jedem Fall aber trennen die anderen Domänencontroller den wiederhergestellten Domänencontroller vom Netzwerk, um Fehler zu beheben.

Vermeiden Sie daher möglichst Prüfpunkte auf Domänencontrollern. Zwar hat Microsoft das Problem in Windows Server 2012 R2 mit der GenerationID besser im Griff, aber generell ist das Sichern von Servern, die eine Datenbank bereitstellen, nicht über Prüfpunkte empfohlen, zumindest wenn es sich vermeiden lässt. Das Gleiche gilt übrigens für alle Server, die eine Datenbank nutzen, auch Exchange und SQL. Sie sollten solche Datenbanken niemals über Prüfpunkte zurücksetzen.

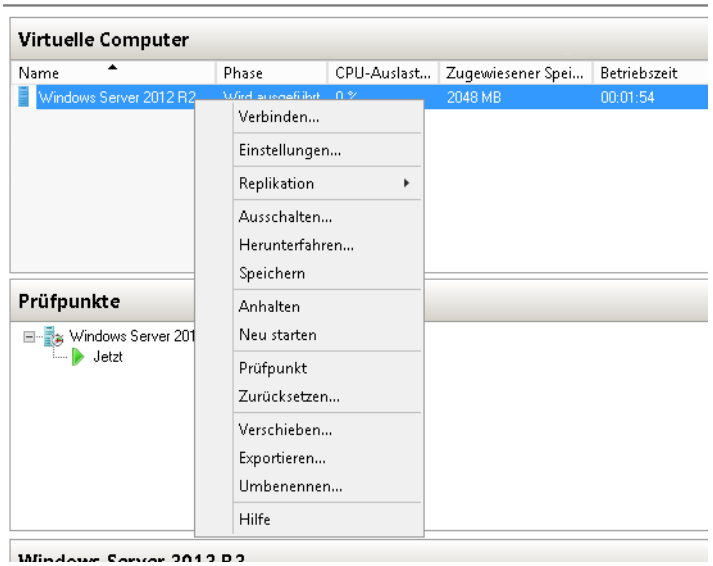
In Hyper-V haben Sie die Möglichkeit, einem Gastsystem eine differenzierende virtuelle Festplatte zuzuweisen. Dazu bauen die Festplatten auf eine übergeordnete Festplatte mit einer Windows-Installation auf und speichern die Daten auf einer eigenen Festplatte. Für Domänencontroller ist das nicht empfohlen, da sich solche Festplatten zu leicht wieder in den Ursprungszustand zurückversetzen lassen. Hier gibt es das gleiche Problem wie mit den Prüfpunkten.

Sicherung durch Export

Die Sicherung von Hyper-V-Hosts besteht vor allem in der Sicherung der einzelnen virtuellen Server, die auf dem Host betrieben werden. In der Verwaltungskonsole von Hyper-V haben Sie noch die Möglichkeit, die virtuellen Server zu exportieren. Solche exportierten Server lassen sich auch wieder importieren. Das funktioniert auf dem gleichen Hyper-V-Host, aber auch auf einem anderen Server.

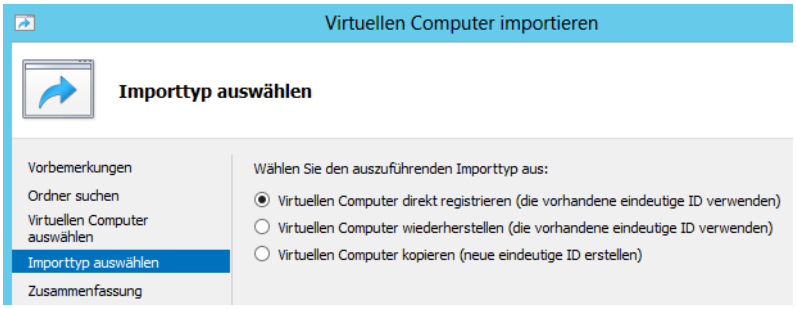
Der Befehl zum Exportieren steht über das Kontextmenü von virtuellen Servern zur Verfügung. In Windows Server 2012 funktioniert diese Technik nur dann, wenn der virtuelle Server nicht gestartet ist. Das ist in Windows Server 2012 R2 anders. Sie können hier auch im laufenden Betrieb einen Export durchführen. Der Exportvorgang umfasst die *.vhd*-Dateien, Prüfpunkte und die Einstellungen des virtuellen Servers. Die Größe der Exportdateien entspricht der Größe der Quelldateien.

Abbildg. 8.5 Exportieren von virtuellen Servern



Wollen Sie einen virtuellen Computer wieder importieren, steht der Befehl *Virtuellen Computer importieren* zur Verfügung. Über den Assistenten wählen Sie den Ordner aus, in dem sich die Exportdatei befindet, und erhalten im nächsten Fenster Informationen zum Servernamen angezeigt. Auf der nächsten Seite wählen Sie die Optionen aus, um den Server zu importieren.

Abbildg. 8.6 Importieren eines virtuellen Servers



Virtuelle Server kostenlos und professionell sichern – Veeam Backup

Der bekannte Hersteller für die Sicherung von virtuellen Servern, Veeam, bietet ein kostenloses Tool, mit dem sich die Datensicherung virtueller Exchange-Server vollkommen kostenlos auslesen und einzelne Objekte wiederherstellen lassen (Single-Item-Recovery). Auch herkömmliche Server können Sie auf diesem Weg sichern und wiederherstellen.

Basis des Tools ist das Produkt Veeam Backup Free Edition (*http://www.veeam.com/free-backup* [Ms179-K08-01]). Mit der kostenlosen Sicherungssoftware lassen sich virtuelle Server ohne Downtime sichern, nicht nur virtuelle Exchange-Server. Die Software unterstützt VMware und Microsoft Hyper-V. Mit Veeam Backup Free Edition können Sie sogar System Center Virtual Machine Manager anbinden und auch Hyper-V-Cluster integrieren. Binden Sie einen SCVMM-Server an Veeam Backup an, kann die Software alle angebundenen Server automatisch einlesen und die darauf gespeicherten virtuellen Server sichern. Die Software sichert nicht die einzelnen Virtualisierungshosts, sondern ist auf die Sicherung der virtuellen Server spezialisiert.

Veeam Backup Free Edition im Überblick

Veeam Backup Free Edition (*http://www.veeam.com/free-backup* [Ms179-K08-01]) sichert virtuelle Server von angebundenen Hosts im laufenden Betrieb oder im ausgeschalteten Zustand. Dabei gibt es keinerlei Einschränkungen bezüglich der Anzahl der VMs. Die kostenlose Edition sichert immer eine VM nach der anderen. Die Sicherungen müssen manuell gestartet werden, nur die kostenpflichtige Edition beherrscht geplante Backupvorgänge.

Aus den Sicherungsdateien lassen sich virtuelle Server auf anderen Systemen wiederherstellen, zum Beispiel für ein Desaster-Recovery oder eine Testumgebung. So können Administratoren vor der Installation von Patches schnell eine Sicherung durchführen und auf einem Testsystem wiederherstellen, ohne den produktiven Server zu beeinträchtigen. Sie können natürlich virtuelle Server auf

dem gleichen Host wiederherstellen oder nur einzelne Dateien aus der Sicherung, wie die virtuellen Festplatten oder die Konfigurationsdateien. Der Wiederherstellungs-Assistent unterstützt auch die Wiederherstellung einzelner Dateien innerhalb virtueller Windows-Server.

Veeam unterstützt VMware vSphere und Microsoft Hyper-V in Windows Server 2012 R2. Bei der Sicherung berücksichtigt das Produkt nur beschriebene Bereiche der virtuellen Festplatten und sichert keine leeren Bereiche.

Alle Konfigurationsdateien und virtuellen Festplatten sichert das Tool in eine einzelne Datei. Neben der kostenlosen Edition bietet Veeam noch eine kostenpflichtige Version von Veeam Backup an. Diese beherrscht auch geplante Sicherungen und Sicherungsjobs, sowie die Möglichkeit, inkrementelle Sicherungen durchzuführen. Außerdem kann die kostenpflichtige Edition mehrere VMs gleichzeitig sichern. Sie haben jederzeit die Möglichkeit, von der kostenlosen Edition zur kostenpflichtigen Edition zu wechseln, ohne den Server neu installieren zu müssen. Neben der Möglichkeit, virtuelle Server im laufenden Betrieb in eine einzelne Datei zu sichern und auf anderen Hosts wiederherzustellen, lassen sich aus den Sicherungen auch einzelne Dateien wiederherstellen (Instant File Recovery). Auch hier können Sie die Ziele der Wiederherstellung frei wählen.

Zusätzlich zu Veeam Backup Free Edition bietet Veeam den Explorer für Microsoft Exchange an. Mit der Anwendung lassen sich Daten aus Exchange-Sicherungen auslesen und einzelne Elemente, wie zum Beispiel E-Mails, wiederherstellen. Die Dateien lassen sich aus der Exchange-Sicherung exportieren, entweder in das *.msg*-Format oder als *.pst*-Datei.

Dabei kann das Tool auf die Sicherungen zurückgreifen, die Sie mit Veeam Backup Free Edition angefertigt haben. Das heißt, Sie können vollkommen kostenlos alle VMs sichern und Sicherungen und Daten wiederherstellen, auch einzelne Exchange-Elemente. Grundlage für die Wiederherstellung von einzelnen Exchange-Objekten mit Veeam Explorer für Microsoft Exchange ist daher Veeam Backup Free Edition.

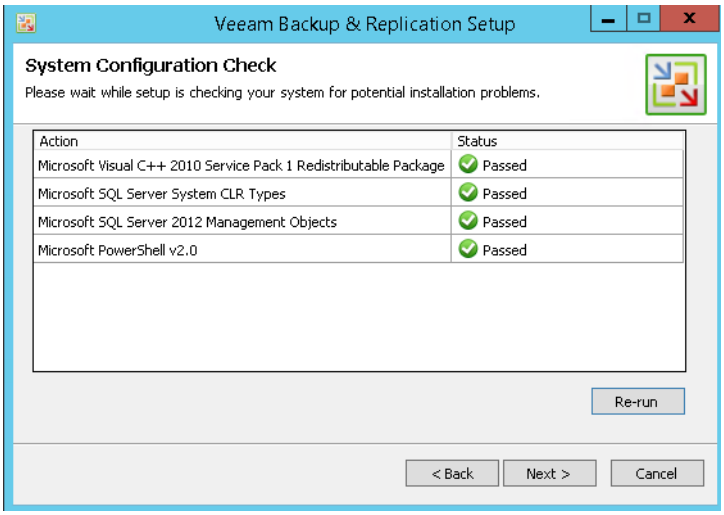
Veeam Backup Free Edition installieren

Um Veeam Backup Free Edition einzusetzen, laden Sie sich zunächst die Installationsdateien (*http://www.veeam.com/free-backup* [Ms179-K08-01]) herunter. Anschließend starten Sie die Installation auf Ihrem Hyper-V-Server oder einem anderen Server. Während der Installation können Sie eine Lizenzdatei hinterlegen, wenn Sie die kommerzielle Version installieren wollen. Für die kostenlose Free Edition ist das aber nicht notwendig. Sie können die Lizenzdatei auch jederzeit nachträglich integrieren.

Außerdem wählen Sie aus, welche Komponenten Sie installieren wollen. Neben der grafischen Oberfläche unterstützt Veeam Backup Free Edition auch eine Steuerung über die PowerShell.

Veeam Backup Free Edition benötigt auch Zugriff auf einen SQL-Server. Haben Sie noch keinen im Einsatz, kann der Installations-Assistent einen eigenen Server installieren. Sie können bereits installierte SQL-Server problemlos anbinden. Während der Installation testet das Tool, ob alle notwendigen Voraussetzungen für die Sicherungsanwendung erfüllt sind. Fehlen Erweiterungen, weist der Assistent darauf hin, und Sie können die Erweiterung mit der Schaltfläche *Install* auf den Server installieren.

Abbildg. 8.7 Veeam Backup überprüft den Server auf fehlende Erweiterungen

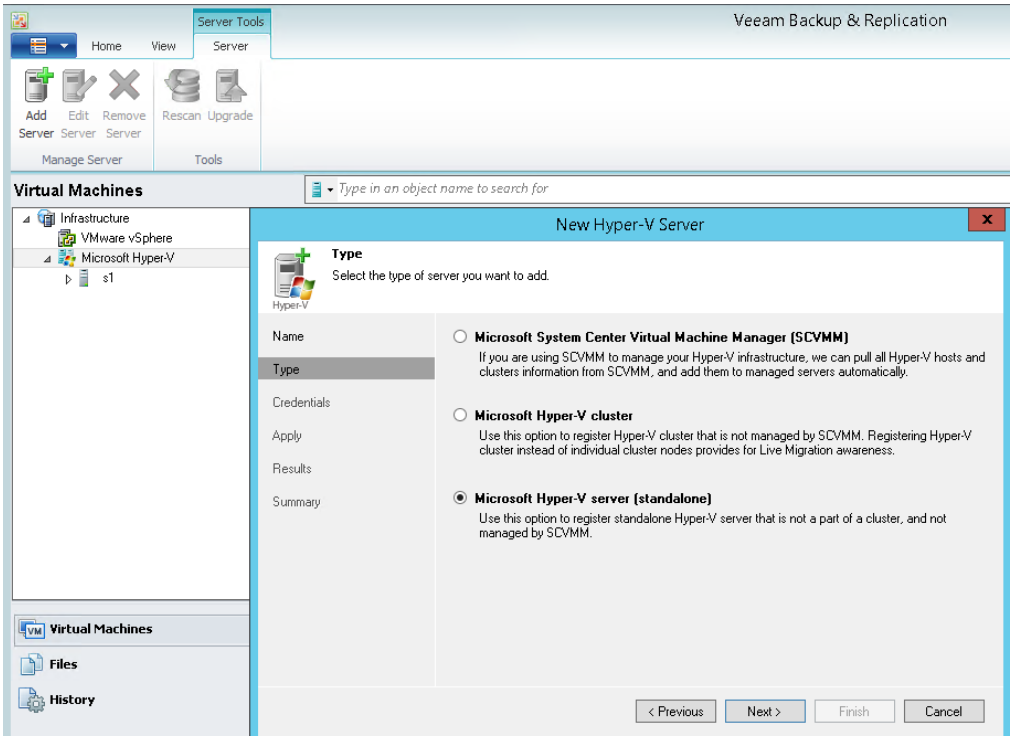


Während der Installation legen Sie auch den Anmeldenamen des Diensts für Veeam Backup fest. Der Benutzer des Diensts muss Zugriff auf die SQL-Datenbank erhalten. Installieren Sie die SQL-Instanz mit Veeam Backup zusammen, richtet das der Installations-Assistent automatisch ein. Die weiteren Fenster können Sie auf den Standardvorgaben belassen. Auf dem SQL-Server legt Veeam eine neue Datenbank an, in der die Software seine Konfigurationsdaten speichert.

Nach der Installation von Veeam Backup Free Edition binden Sie die Hyper-V-Hosts, VMware-Server und System Center Virtual Machine Manager an die Lösung an. Diese liest die installierten virtuellen Server auf den Hosts ein und kann sie im laufenden Betrieb sichern. Dafür sorgt die Software VeeamZIP, die zu Veeam Backup Free Edition gehört, und die Sie über die Verwaltungskonsole von Veeam Backup starten.

Die Anbindung der Hosts nehmen Sie über die Verwaltungskonsole von Veeam Backup vor. Diese installiert der Assistent auch auf dem Desktop. Sie können in der Verwaltungskonsole zentral Sicherungen auch verschiedener Virtualisierungstechnologien durchführen. Im ersten Schritt klicken Sie in der Konsole auf *Add Server* oder wählen den Befehl über das Kontextmenü von *Microsoft Hyper-V* oder *VMware vSphere* aus. Anschließend geben Sie den Namen oder die IP-Adresse des Virtualisierungshosts an. Auf der nächsten Seite des Assistenten legen Sie fest, ob es sich bei dem entsprechenden Server um einen Hyper-V-Host, einen Server mit VMware vSphere (ESXi) oder System Center Virtual Machine Manager handelt.

Abbildg. 8.8 In der Veeam-Konsole binden Sie Hyper-V-Hosts an



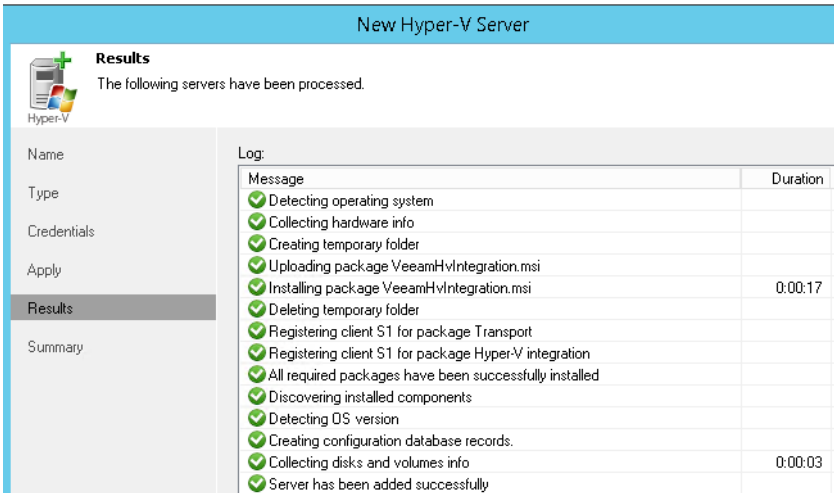
Binden Sie Hyper-V-Server an, können Sie auf dem Fenster auch einen Cluster angeben. Auch hier kann Veeam Backup Free Edtion problemlos virtuelle Server sichern. Für jeden Server können Sie eigene Anmeldedaten hinterlegen. Um einen Server mit System Center Virtual Machine Manager anzubinden, muss auf dem Server, auf dem Sie Veeam Backup installiert haben, die Verwaltungskonsole von SCVMM installiert sein.

Binden Sie einen Server ein, prüft der Assistent zunächst, ob der entsprechende Host kompatibel zu Veeam Backup ist. Anschließend legen Sie fest, ob Veeam Backup Erweiterungen auf dem Server installieren darf, um ihn an Veeam anzubinden. Kann sich der Client nicht anbinden, müssen Sie in der Systemsteuerung in der Firewall verschiedene Apps kommunizieren lassen. Klicken Sie dazu in der Systemsteuerung auf *System und Sicherheit/Windows-Firewall* und dann auf *Eine App oder ein Feature durch die Windows-Firewall zulassen*.

Wählen Sie an dieser Stelle die *Remotedienstverwaltung*, *Remoteverwaltung geplanter Aufgaben*, *Windows-Remoteverwaltung* und vor allem *Windows-Verwaltungsinstrumentation aus (WMI)* aus.

Bestätigen Sie die Fenster, installiert der Assistent remote die entsprechenden Erweiterungen und bindet den Server an. Sie sehen im Fenster den Status der Anbindung. Damit Veeam virtuelle Server auf dem Host sichern kann, müssen die Systemdienste *Veeam Backup Hyper-V Integration Service* und *Veeam Backup Proxy Service* gestartet sein.

Abbildg. 8.9 Installieren der notwendigen Erweiterungen auf Hyper-V-Hosts für die Unterstützung von Veeam

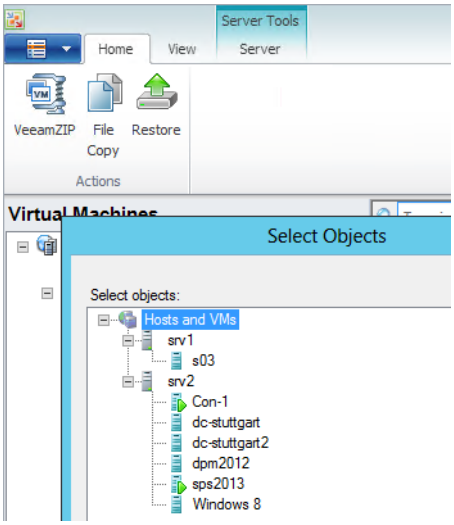


HINWEIS Sie können mit Veeam Backup zwar Hyper-V in Windows Server 2012 R2 sichern, aber kein Hyper-V in Windows 8.

Virtuelle Server mit VeeamZIP sichern

Wollen Sie Server sichern, verwenden Sie VeeamZIP. Dazu klicken Sie auf *Home* und dann auf *VeeamZIP*. Im Fenster sehen Sie die angebundenen Hosts und darunter die installierten virtuellen Server. Sie sehen auch den Status der Server.

Abbildg. 8.10 Anzeigen der virtuellen Server eines Hosts



Haben Sie einen Server ausgewählt, legen Sie als Nächstes einen Pfad auf dem Veeam-Server fest, in dem die Daten gesichert werden sollen. Hier bestimmen Sie auch, ob Sie die Sicherung komprimieren wollen.

Im nächsten Schritt sichert Veeam den Server im laufenden Betrieb. Sie sehen den Status direkt im Fenster. Ist die Sicherung abgeschlossen, erhalten Sie eine Rückmeldung. Im Ordner, den Sie angegeben haben, befindet sich anschließend die Sicherungsdatei des Servers. Diese enthält den Namen und das Datum sowie die Uhrzeit der Erstellung der Sicherung. Klicken Sie doppelt auf die Sicherungsdatei, erhalten Sie weiterführende Informationen zum virtuellen Server und der Sicherung angezeigt.

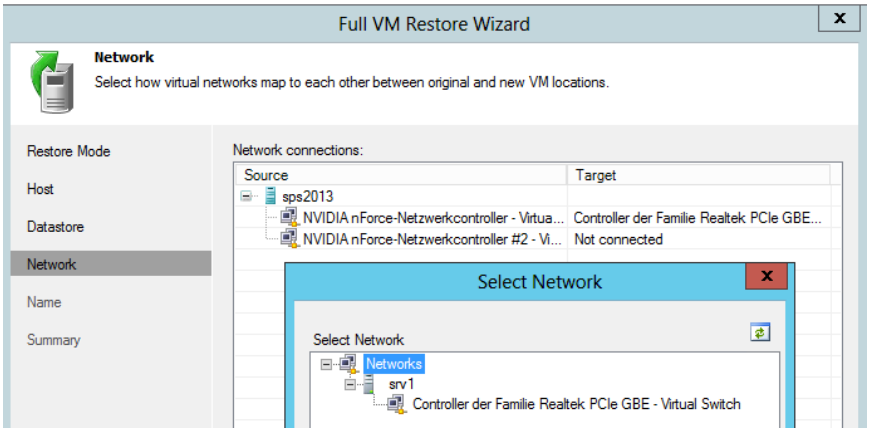
Daten und virtuelle Server aus Veeam Backup wiederherstellen

Wollen Sie einen virtuellen Server aus Veeam Backup wiederherstellen, klicken Sie auf der Registerkarte *Home* auf *Restore*. Anschließend wählen Sie die Sicherungsdatei aus, von der Sie Daten wiederherstellen wollen. Veeam liest anschließend die Daten der Sicherung ein. Im Fenster sehen Sie den Namen und den Typ des virtuellen Servers. Mit *Restore* stellen Sie diesen wieder her.

Im Fenster haben Sie die Wahl, einzelne Dateien der Sicherung wiederherzustellen, den kompletten Server oder Daten aus der Sicherung von innerhalb des virtuellen Servers. Haben Sie ausgewählt, was Sie wiederherstellen wollen, legen Sie als Nächstes fest, wo Sie den virtuellen Server wiederherstellen wollen. Sie haben hier die Möglichkeit, den ursprünglichen Server oder einen anderen Server, den Sie an Veeam angebunden haben, auszuwählen.

Veeam stellt anschließend eine Verbindung mit dem Zielserver her. Um einen virtuellen Server wiederherzustellen, darf der entsprechende Server auf dem Zielserver nicht gestartet sein. Nach der Wiederherstellung des virtuellen Servers können Sie diesen automatisch wieder starten lassen. Die entsprechende Option dazu finden Sie im Fenster zur Wiederherstellung.

Abbildg. 8.11 Zuordnen von virtuellen Switches bei der Wiederherstellung



Im Rahmen der Wiederherstellung können Sie auch die virtuellen Netzwerke von Servern wiederherstellen, wenn Sie einen virtuellen Server auf einem anderen Hyper-V-Host wiederherstellen wollen. Dazu verbindet sich der Assistent mit dem Zielhost, und Sie können der virtuellen Maschine, die Sie wiederherstellen wollen, einen virtuellen Switch zuordnen.

Die Sicherungsdatei von Veeam Backup Free Edition können Sie auch zum Einlesen für Veeam Explorer für Microsoft Exchange verwenden. Die Exchange-Datenbanken in dieser Datei lassen sich einlesen und einzelne Elemente aus den Datenbanken extrahieren. Dazu starten Sie das Tool Veeam Explorer for Exchange und wählen die Sicherungsdatei des Servers aus.

Veeam Backup verwalten und erweiterte Funktionen nutzen

Klicken Sie in Veeam Backup in den unteren Bereich auf *History*, sehen Sie alle Aufgaben, die Sie mit dem Tool durchgeführt haben. So lassen sich Sicherungsaufgaben und Wiederherstellungen überprüfen. Mit *Files* können Sie die Dateisysteme aller angebundenen Server durchsuchen und Dateien kopieren.

Veeam Backup beherrscht auch ein Rollenmodell. Sie können verschiedene Benutzer anlegen und diesen unterschiedliche Rechte zuteilen. Das Tool kann auch Benutzer aus Active Directory einlesen und verwenden. Die entsprechenden Benutzer können die Verwaltungskonsole auf ihrem Rechner installieren, um auf den Veeam-Server zugreifen zu können.

Benutzer legen Sie über das Hauptmenü und die Auswahl von *Users and Roles* fest. Bestandteil von Veeam ist auch ein Putty-Client, mit dem sich Telnet-Sitzungen aufbauen lassen. Sie können Veeam Backup Free Edition schnell und einfach zu einer vollwertigen Installation lizenzieren. Eine Neuinstallation ist dabei nicht notwendig. Die entsprechende Option finden Sie über das Hauptmenü und die Auswahl von *Help/License*. Sie müssen an dieser Stelle nur eine Lizenzdatei hinterlegen.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt wie Sie Hyper-V-Hosts und virtuelle Server mit Bordmitteln sichern. Wir sind auch darauf eingegangen, wie Sie Prüfpunkte von virtuellen Servern erstellen und wie Sie den Hyper-V-Host wiederherstellen. Auch das Sichern von Hyper-V mit kostenlosen Tools oder Export- und Importvorgänge waren Bestandteil dieses Kapitels. Mehr zum Thema Datensicherung lesen Sie im Kapitel 35.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie Hyper-V hochverfügbar betreiben und die neuen Techniken der Livemigration und Replikation nutzen.

Kapitel 9

Hyper-V – Hochverfügbarkeit

In diesem Kapitel:

Microsoft hat in Windows Server 2012 R2 die Hochverfügbarkeit in allen Bereichen weiter verbessert und zusätzliche Möglichkeiten für kleinere Unternehmen integriert. Ein Cluster ist nicht immer notwendig und virtuelle Server lassen sich einfach zwischen Hyper-V-Hosts replizieren.

So ist es zum Beispiel seit Windows Server 2012 möglich, die Livemigration auch auf Hyper-V-Hosts ohne Cluster zu nutzen, oder virtuelle Maschinen zwischen Hyper-V-Hosts zu replizieren, ohne diese clustern zu müssen. Bei der Livemigration mit und ohne Cluster verschieben Sie virtuelle Server zwischen Hyper-V-Hosts in der Gesamtstruktur. Ebenfalls möglich ist, die virtuellen Festplatten eines Servers mit der Livemigration zu verschieben. Das heißt, die virtuellen Server selbst verbleiben auf dem aktuellen Host, nur der Speicherort der Dateien ändert sich. So können Sie zum Beispiel die Dateien auf eine Freigabe verschieben. In Windows Server 2012 R2 hat Microsoft die Funktionen weiter deutlich verbessert. Mehr zu diesem Thema lesen Sie auch in den Kapiteln 1 und 7.

Mit Hyper-V-Replikat replizieren Sie virtuelle Server auf andere Server, ebenfalls im laufenden Betrieb. Als Verbindung ist nur eine Netzwerkleitung notwendig, kein gemeinsamer Datenträger. Bei Windows Server 2012 können Sie virtuelle Server zwischen zwei Hyper-V-Hosts replizieren, in Windows Server 2012 R2 stehen drei Server zur Verfügung.

Mit dem Hyper-V-Server 2012 R2 bietet Microsoft die Hyper-Funktionen der Datacenter-Edition von Windows Server 2012 R2 kostenlos an. Mit dieser Variante von Windows Server 2012 R2 können Sie auch Cluster installieren sowie die Funktionen nutzen, die wir nachfolgend beschreiben. Cluster lassen sich jetzt auch in der Standard-Edition erstellen. Cluster konnten in Windows Server 2008 R2 maximal 16 Knoten einsetzen. Windows Server 2012 R2 erlaubt bis zu 64 Clusterknoten, auch in der Standard-Edition.

Windows Server 2008 R2 unterstützt zwar bereits die Livemigration, aber immer nur von einem Server gleichzeitig. Bei der Livemigration in einem Cluster überträgt Hyper-V den virtuellen Server mitsamt Inhalt des Arbeitsspeichers auf einen anderen Knoten im Cluster. Das hat den Vorteil, dass die Server immer verfügbar sind, auch bei einer Übertragung.

Windows Server 2008 R2 kann aber immer nur einen Server auf einmal übertragen, was in vielen Fällen nicht sehr effizient ist. Denn gerade in größeren Umgebungen kommen Cluster zum Einsatz. Und Cluster hosten normalerweise viele virtuelle Server. Windows Server 2012 R2 kann jetzt mehrere Livemigrationen auf einmal durchführen und Sie können auch Prioritäten festlegen.

Arten der Hochverfügbarkeit in Windows Server 2012 R2 und Hyper-V

Mit Windows Server 2012 R2 ändert Microsoft zunächst den Funktionsumfang der verschiedenen Editionen. Für Unternehmen spielen vor allem die Editionen Standard und Datacenter von Windows Server 2012 R2 eine Rolle. Eine Enterprise-Edition gibt es nicht mehr. Die beiden Editionen verfügen über exakt den gleichen Funktionsumfang. Es lassen sich also auch mit der Standard-Edition Cluster für Hyper-V betreiben. Die Editionen Standard und Datacenter unterscheiden sich in Windows Server 2012 R2 lediglich in der Lizenzierung.

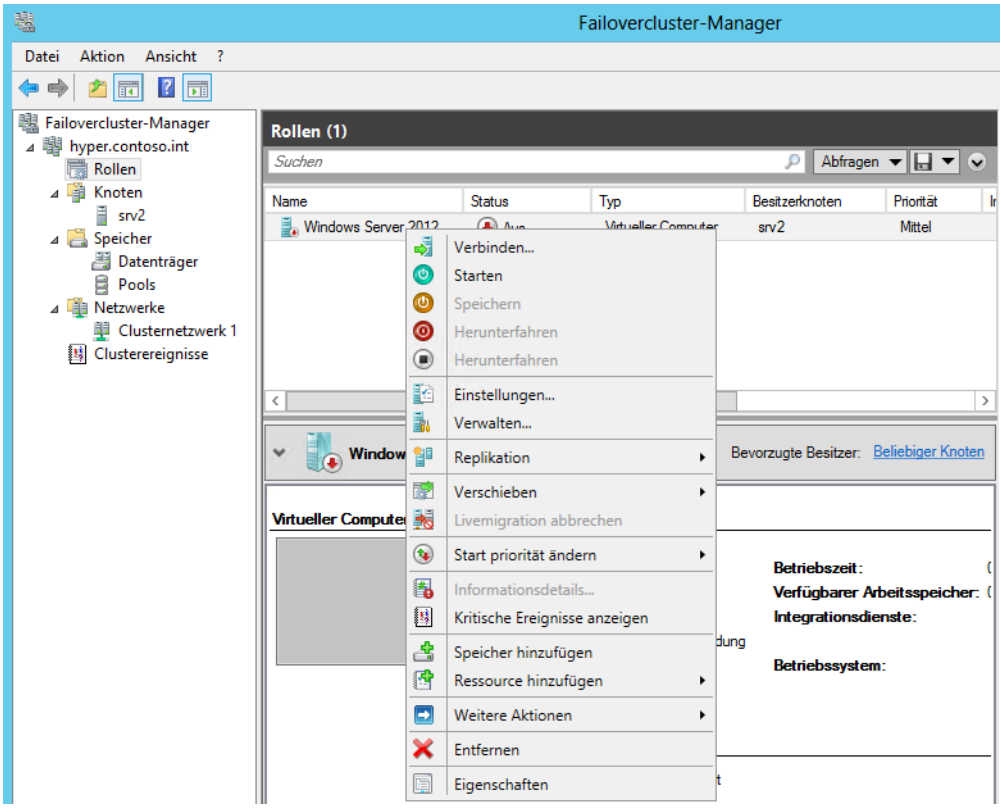
Auf Servern mit Windows Server 2012 R2 Standard dürfen Unternehmen zwei virtuelle Server pro Lizenz installieren. Sollen auf einem Hyper-V-Host mehr virtuelle Server im Einsatz sein, sind mehrere Lizenzen für die Standard-Edition notwendig oder eben eine Datacenter-Lizenz. Die Datacenter-Edition erlaubt den Betrieb unendlich vieler virtueller Server auf einem Host. Beide Editionen decken außerdem immer nur zwei Prozessoren des Hosts ab. Die erforderliche Mindestanzahl von

Betriebssystemlizenzen für jeden Server wird durch die Anzahl der physischen Prozessoren des Hosts bestimmt, sowie die Anzahl an virtueller Server, die Sie auf dem Hyper-V-Host installieren.

Außerdem stellt Microsoft noch den kostenlosen Hyper-V Server 2012 zur Verfügung, der über die gleichen Funktionen im Bereich Hyper-V verfügt wie die Editionen Standard und Datacenter. Diesen Server müssen Unternehmen nicht lizenzieren. Die Installation entspricht einer Core-Installation ohne grafische Oberfläche von Windows Server 2012 R2. Die Verwaltung erfolgt über grafische Verwaltungsprogramme von anderen Servern, einer Arbeitsstation mit Windows 8.1 oder System Center Virtual Machine Manager 2012 R2. Mit diesen drei Editionen können Unternehmen die drei wichtigsten Hochverfügbarkeitsfunktionen in Windows Server 2012 R2 nutzen. Diese stellen wir nachfolgend vor.

Mit Hyper-V-Replikat lassen sich virtuelle Server zwischen Hyper-V-Hosts replizieren, ohne dass diese Bestandteil eines Clusters sein müssen. Der virtuelle Server wird vom Quellserver auf den Zielserver repliziert, also kopiert. Dieser Vorgang kann ad hoc oder über einen Zeitplan erfolgen. Aktiv bleibt immer der virtuelle Server auf dem Quellserver, der virtuelle Server auf dem Zielserver bleibt ausgeschaltet. Administratoren können ein Failover des virtuellen Servers manuell durchführen oder den virtuellen Server jederzeit erneut vom Quell- auf den Zielserver replizieren. In Windows Server 2012 R2 können Sie zwei Zielserver definieren, um virtuelle Server zu replizieren.

Abbildg. 9.1 Verwalten virtueller Server im Cluster



Mit der Livemigration ohne Cluster können Administratoren virtuelle Server im laufenden Betrieb vom Quell- auf den Zielserver verschieben und online schalten. Es ist kein Cluster und kein gemeinsamer Datenträger notwendig. Neu seit Windows Server 2012 in diesem Bereich ist auch die Möglichkeit, mehrere Livemigrationen gleichzeitig durchzuführen. In Windows Server 2012 R2 kommt noch die Komprimierung der Daten dazu, sowie die Möglichkeit, den Inhalt des Arbeitsspeichers zwischen zwei Hyper-V-Hosts zu übertragen. Die beiden Punkte beschleunigen die Hochverfügbarkeit enorm. Mehr zu diesem Thema lesen Sie in den Kapiteln 1 und 7. Im Gegensatz zur Replikation ist der virtuelle Server weiterhin nur auf einem Server verfügbar und kann im laufenden Betrieb verschoben werden.

Weiterhin gibt es in Windows Server 2012 R2 die Möglichkeit, Hyper-V in einem Cluster zu betreiben und virtuelle Server als Clusterressourcen zu definieren. Hier sind die virtuellen Server schnell und einfach zwischen den Knoten verschiebbar. Einen solchen Cluster können Unternehmen jetzt auch mit der Standard-Edition aufbauen. In Windows Server 2012 R2 lassen sich mehrere Livemigrationen gleichzeitig durchführen und virtuelle Server lassen sich auch priorisieren. Alle diese Funktionen stehen über Hyper-V Server 2012 R2 kostenlos zur Verfügung.

Hyper-V-Replikation

Mit der Funktion Hyper-V-Replikat lassen sich in Windows Server 2012 R2 und Hyper-V Server 2012 R2 virtuelle Festplatten und komplette virtuelle Server asynchron zwischen drei Hyper-V-Hosts im Netzwerk replizieren und synchronisieren. Windows Server 2012 unterstützt zwei Hyper-V-Hosts für die Replikation. Sie können für die Replikation auch eine Kette konfigurieren. So kann zum Beispiel ServerA zu ServerB und dieser den gleichen virtuellen Server zu ServerC replizieren.

In Windows Server 2012 konnten Sie den Synchronisierungsintervall nur bis zu 5 Minuten einstellen. Ab Windows Server 2012 R2 haben Sie hier auch die Möglichkeit, alle 30 Sekunden die Daten zwischen den Hosts replizieren zu lassen. Alternativ können Sie jetzt die Replikation auf ein Intervall von bis zu 15 Minuten ausdehnen.

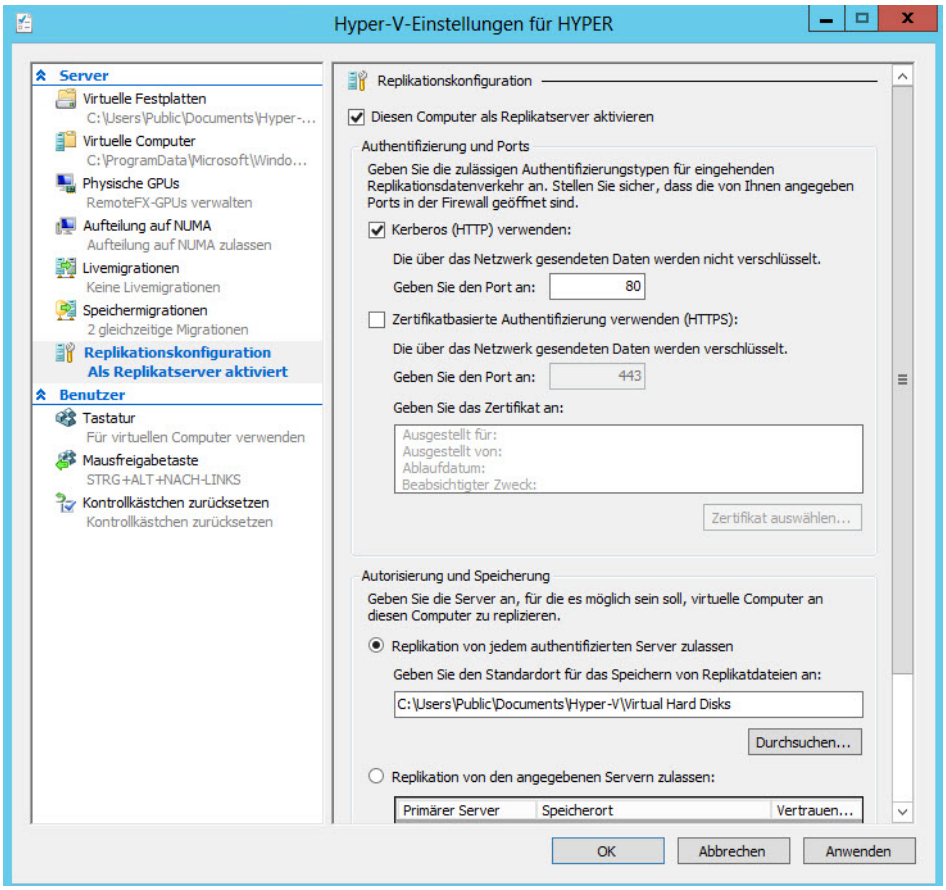
Die Replikation findet über das Dateisystem und das Netzwerk statt, ein Cluster ist nicht notwendig. Die Replikationen lassen sich manuell, automatisiert oder nach einem Zeitplan ausführen. Sie können auf diesem Weg eine Testumgebung ausbauen oder die replizierten Server bei Ausfall eines Hyper-V-Hosts aktiv schalten. Mit Hyper-V-Replikat können kleine und mittelständische Unternehmen eine effiziente Ausfallsicherheit erreichen.

Hyper-V-Hosts für Replikation aktivieren

Die Konfiguration erfolgt über einen Assistenten im Hyper-V-Manager oder der PowerShell. Auf diesem Weg lassen sich virtuelle Server auch hochverfügbar betreiben, ohne teure Cluster betreiben zu müssen. Die Einrichtung nehmen Sie über einen Assistenten im Hyper-V-Manager vor.

Interessant ist diese Funktion zum Beispiel für den Betrieb einer Testumgebung oder eines Backendservers. Mittelständische Unternehmen erreichen mit der Technologie eine Ausfallsicherheit ihrer virtuellen Server. Die Quell-VM läuft bei diesem Vorgang weiter. Fällt ein Hyper-V-Host aus, lassen sich die replizierten Server online schalten. Nach der ersten Übertragung müssen nur noch Änderungen übertragen werden. Die erste Übertragung können Sie mit einem externen Datenträger vornehmen.

Abbildg. 9.2 Aktivieren der Replikationskonfiguration in Hyper-V



Die Replikation ist auch in Clustern möglich. In diesem Fall starten Sie die Replikation über das Kontextmenü der entsprechenden virtuellen Maschine in der Failovercluster-Verwaltung. Die Einrichtung entspricht nach dem Start des Assistenten der Einrichtung ohne Cluster. Die Einstellungen für die Replikation nehmen Sie ebenfalls in der Clusterverwaltung vor. Dazu klicken Sie mit der rechten Maustaste auf den virtuellen Server.

Damit Hyper-V-Hosts eine solche Replikation ermöglichen, müssen Sie diese zunächst für alle beteiligten Hyper-V-Hosts aktivieren. Starten Sie den Assistenten über das Kontextmenü des virtuellen Servers auf dem Quellserver, geben Sie zunächst den Zielserver ein, also den Hyper-V-Host, auf den Sie die virtuelle Maschine replizieren wollen. Der virtuelle Server auf dem Quellserver bleibt aber weiterhin verfügbar und aktiv.

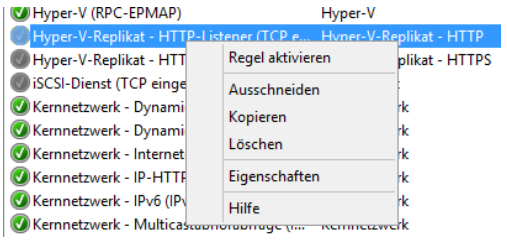
Damit ein Hyper-V-Host für Replikate zur Verfügung steht, müssen Sie auf dem entsprechenden Server in den Hyper-V-Einstellungen im Bereich *Replikationskonfiguration* diese Funktion zunächst aktivieren und konfigurieren. Sie legen hier den Datenverkehr fest und von welchen Servern der aktuelle Server Replikate entgegennimmt. Daher müssen Sie diese Funktion zunächst auf allen Hyper-V-Hosts aktivieren.

Setzen Sie Hyper-V Server 2012 R2 ein, können Sie diesen Server auch über den Hyper-V-Manager von einem anderen Server aus verwalten und auf diesem Weg die gleichen Einstellungen vornehmen (siehe Kapitel 2 und 3). Hier gibt es keinerlei Unterschiede zu den kostenpflichtigen Editionen von Windows Server 2012 R2.

TIPP Achten Sie darauf, noch die Regel in der erweiterten Konfiguration der Firewall (*wf.msc*) für Hyper-V-Replikat zu aktivieren. Diese hat die Bezeichnung *Hyper-V-Replikat – HTTP-Listener*. Es gibt auch einen Listener für HTTPS.

Bei den Regeln handelt es sich um eingehende Netzwerkregeln, für den ausgehenden Datenverkehr müssen Sie keine Änderungen vornehmen.

Abbildg. 9.3 Replikatverkehr von Windows Server 2012 R2 erlauben



In produktiven Umgebungen sollten Sie die Daten virtueller Server besser SSL-verschlüsselt mit HTTPS übertragen. In diesem Fall muss den entsprechenden Hyper-V-Hosts ein Zertifikat von einer internen Zertifizierungsstelle, am besten auf Basis der Active Directory-Zertifikatdienste, zugewiesen sein. Das heißt, in sicheren Umgebungen verwenden Sie Zertifikate zur Übertragung. Dazu verwenden Sie ein Zertifikat, das Clients und Server authentifizieren kann und dem Namen des Hyper-V-Hosts entspricht.

TIPP Wollen Sie Hyper-V-Replikat mit HTTP nutzen, aktivieren Sie die entsprechende Firewallregel mit *Enable-NetFirewallRule -DisplayName "Hyper-V Replica HTTP Listener (TCP-In)"* auch in der PowerShell. Bei der Kerberos-Authentifizierung werden die replizierten Daten nicht verschlüsselt. Nur bei der zertifikatbasierten Authentifizierung werden die replizierten Daten während der Übertragung verschlüsselt. Wollen Sie HTTPS verwenden, schalten Sie auch diese Regeln frei.

Hyper-V-Replikation mit SSL konfigurieren

In diesem Abschnitt zeigen wir Ihnen, wie Sie die Hyper-V-Replikation mit SSL übertragen und dadurch für mehr Sicherheit sorgen. Sie benötigen dazu entweder eine interne Zertifizierungsstelle oder Sie arbeiten mit einem selbstsignierten Zertifikat. Wir zeigen Ihnen nachfolgend beide Wege.

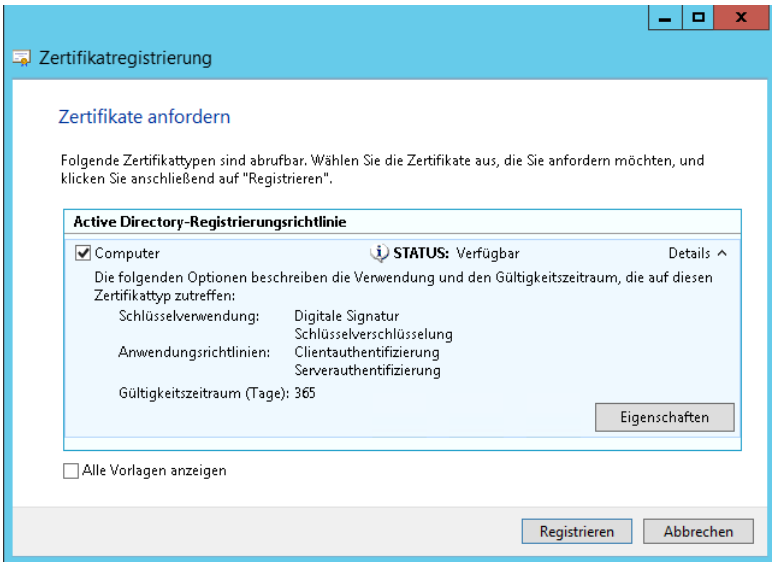
Zertifikate für Hyper-V-Replikation aufrufen

In der lokalen Verwaltung von Zertifikaten können Sie in Active Directory Zertifikate auf einem Server installieren. Diese Zertifikate verwenden Sie dann für Hyper-V-Replikat. Dazu gehen Sie folgendermaßen vor:

1. Starten Sie durch Eingabe von *certlm.msc* auf der Startseite die Verwaltung der lokalen Zertifikate.

2. Klicken Sie mit der rechten Maustaste auf *Eigene Zertifikate* und wählen Sie *Alle Aufgaben/Neues Zertifikat anfordern*.
3. Bestätigen Sie die Option *Active Directory-Registrierungsrichtlinie*.
4. Aktivieren Sie auf der nächsten Seite die Option *Computer* und klicken Sie auf *Registrieren*. Das Zertifikat erscheint anschließend in der Konsole und lässt sich nutzen.
5. Sobald Sie diese Vorgänge abgeschlossen haben, ist das Zertifikat in Hyper-V verfügbar.

Abbildg. 9.4 Registrieren eines neuen Zertifikats in der Zertifikateverwaltung der lokalen Server



Sie können Zertifikate aber auch in der Eingabeaufforderung erstellen lassen. Um ein Zertifikat abzurufen, erstellen Sie am besten eine Datei, mit der Sie eine Anfrage bei der internen oder externen Zertifizierungsstelle starten können.

Speichern Sie dazu eine Textdatei mit dem folgenden Inhalt. Passen Sie den Servernamen in der Spalte *Subject* an Ihre Bedürfnisse an:

```
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=SERVER.CONTOSO.COM"
Exportable = TRUE                    ; Private key is exportable
KeyLength = 2048                     ; Common key sizes: 512, 1024, 2048, 4096, 8192, 16384
KeySpec = 1                          ; AT_KEYEXCHANGE
KeyUsage = 0xA0                      ; Digital Signature, Key Encipherment
MachineKeySet = True                 ; The key belongs to the local computer account
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = CMC
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ;Server Authentication
OID=1.3.6.1.5.5.7.3.2 ;Client Authentication
```

Speichern Sie die Datei zum Beispiel mit dem Namen *replica.inf* ab. Achten Sie auf die korrekte Endung der Datei. Aus dieser Datei erstellen Sie in der Eingabeaufforderung eine weitere Datei mit einer Zertifikatanfrage. Dazu verwenden Sie den folgenden Befehl:

```
Certreq -new replica.inf replica.req
```

Wechseln Sie in das Verzeichnis, in das Sie die INF-Datei gespeichert haben. Nachdem Sie den Befehl durchgeführt haben, befinden sich zwei Dateien im Verzeichnis. Auf Basis der REQ-Datei stellen Sie danach bei Ihrer internen Zertifizierungsstelle auf Basis der Active Directory-Zertifikatdienste eine neue Onlineanfrage. Dazu verwenden Sie den folgenden Befehl:

```
Certreq -submit -config "dc01.contoso.int\contoso-dc01-ca" replica.req replica.cer
```

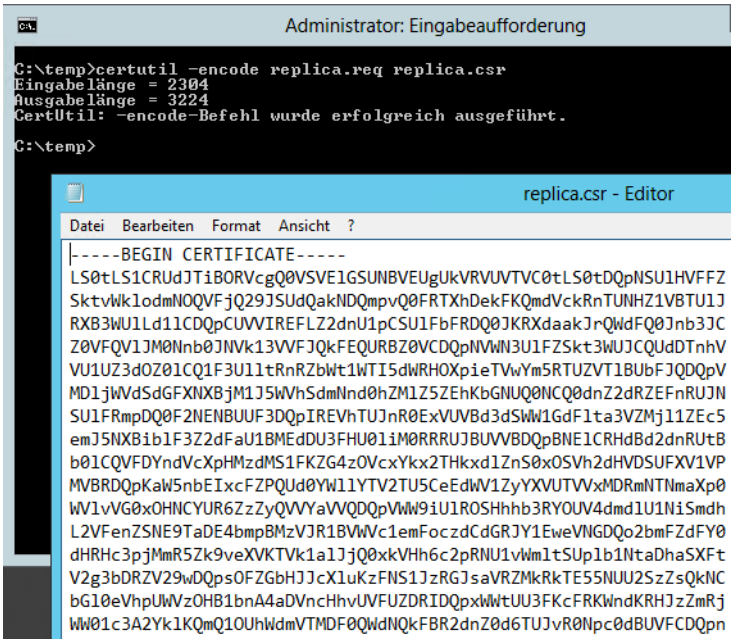
Erhalten Sie eine Fehlermeldung, dass die Zertifikatvorlage fehlt, verwenden Sie zusätzlich noch die Option *-attrib "CertificateTemplate:<Vorlage>"*.

Alternativ erstellen Sie eine Zertifikatsignieranforderung (Certificate Signing Request, CSR), mit der Sie eine Anfrage bei einer externen Zertifizierungsstelle stellen oder mit der Sie auch von internen Zertifizierungsstellen mit der Weboberfläche ein Zertifikat anfragen können. Dazu verwenden Sie den folgenden Befehl:

```
Certutil -encode replica.req replica.csr
```

Anschließend öffnen Sie die CSR-Datei mit einem Editor und kopieren den kompletten Inhalt der Datei in die Zwischenablage. Mit dem Inhalt dieser Datei schließen Sie die Anfrage ab.

Abbildg. 9.5 In der Eingabeaufforderung erstellen Sie eine CSR-Datei, mit der Sie ein Zertifikat anfordern



Rufen Sie im lokalen Zertifikatspeicher des Servers (*certlm.msc*) die eigenen Zertifikate auf und lassen Sie sich die Eigenschaften anzeigen. Sie sehen bei der erweiterten Verwendung des Schlüssels die Möglichkeiten zur Client- und Serverauthentifizierung.

Mit selbstsignierten Zertifikaten arbeiten

Alternativ haben Sie auch die Möglichkeit, mit selbstsignierten Zertifikaten auf den beiden Hyper-V-Hosts zu arbeiten.

Dazu verwenden Sie das Tool *Makecert.exe* aus dem Windows 8/8.1 SDK (*http://msdn.microsoft.com/de-de/windows/desktop/aa904949.aspx* [Ms179-K09-01]). Sie benötigen das Tool nach der Installation des SDK auch auf dem anderen Hyper-V-Host. Sie finden *Makecert.exe* im Verzeichnis *C:\Program Files (x86)\Windows Kits\8.0\bin\x64*. Danach erstellen Sie zunächst auf dem ersten Server ein selbstsigniertes Zertifikat und danach auf dem zweiten Server. Um ein selbstsigniertes Zertifikat zu erstellen, gehen Sie folgendermaßen vor:

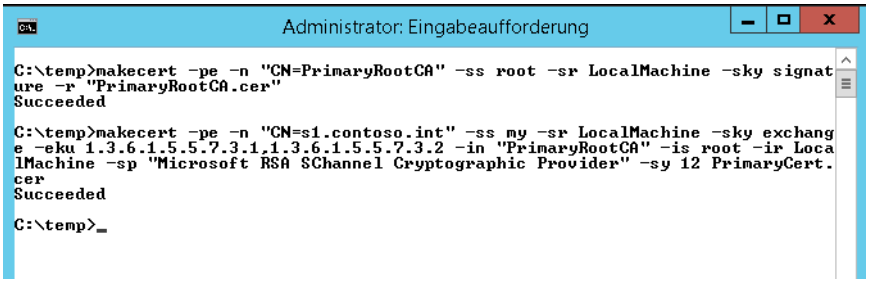
1. Kopieren Sie das Tool *Makecert.exe* auf beide Server.
2. Öffnen Sie eine Eingabeaufforderung auf dem ersten Server und geben Sie den folgenden Befehl ein:

```
Makecert -pe -n "CN=PrimaryRootCA" -ss root -sr LocalMachine -sky signature -r
"PrimaryRootCA.cer"
```

3. Geben Sie danach folgenden Befehl ein:

```
Makecert -pe -n "CN=<FQDN des Servers>" -ss my -sr LocalMachine -sky exchange -eku
1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2 -in "PrimaryRootCA" -is root -ir LocalMachine -sp
"Microsoft RSA SChannel Cryptographic Provider" -sy 12 PrimaryCert.cer
```

Abbildg. 9.6 In der Eingabeaufforderung erstellen Sie Zertifikate, die Sie für die Replikation nutzen können



4. Wechseln Sie anschließend auf den zweiten Server. Kopieren Sie das Tool *Makecert.exe* auf den Replikatserver, falls noch nicht geschehen. Führen Sie den folgenden Befehl aus, um ein selbstsigniertes Stammzertifizierungsstellenzertifikat auf dem zweiten Server zu erstellen:

```
Makecert -pe -n "CN=SecondaryRootCA" -ss root -sr LocalMachine -sky signature -r
"SecondaryRootCA.cer"
```

5. Geben Sie danach den folgenden Befehl ein:

```
Makecert -pe -n "CN=<FQDN>" -ss my -sr LocalMachine -sky exchange -eku
1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2 -in "SecondaryRootCA " -is root -ir LocalMachine -
sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12 SecondaryCert.cer
```

6. Kopieren Sie die Datei *SecondaryRootCA.cer* vom Replikatserver auf den primären Server und geben Sie anschließend den folgenden Befehl ein:

```
Certutil -addstore -f Root "SecondaryRootCA.cer"
```

7. Kopieren Sie die Datei *PrimaryRootCA.cer* vom primären Server auf den Replikatserver und geben Sie danach folgenden Befehl ein*:*

```
Certutil -addstore -f Root "PrimaryRootCA.cer"
```

8. Öffnen Sie auf beiden Servern den Registry-Editor und navigieren Sie zu:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization\Replication
```

9. Setzen Sie den Wert *DisableCertRevocationCheck* auf 1.
10. Falls vorhanden, navigieren Sie zu:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization\FailoverReplication
```

11. Setzen Sie auch hier Setzen Sie den Wert *DisableCertRevocationCheck* auf 1.

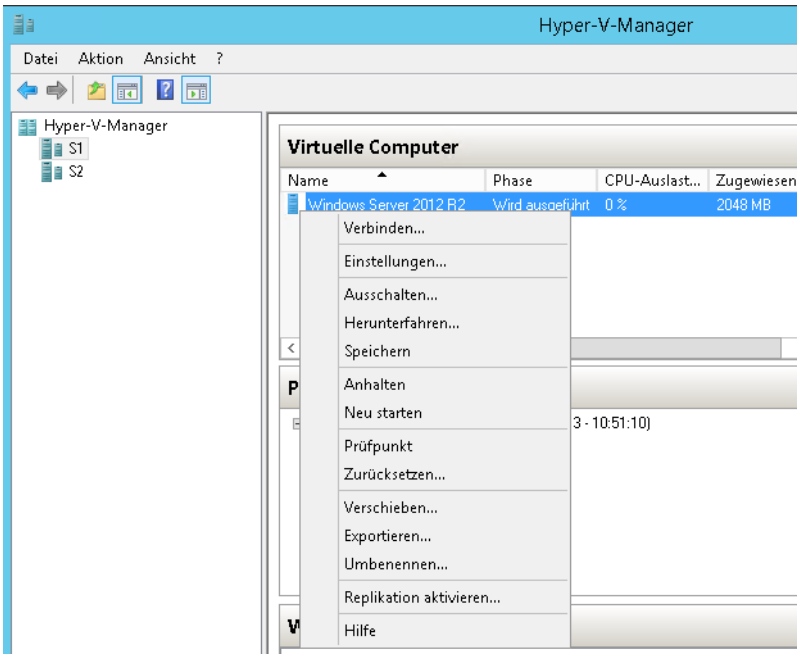
Achten Sie darauf, dass die erstellten Zertifizierungsstellen auf den beiden Servern, mit denen Sie die selbst signierten Zertifikate erstellt haben, auf beiden Server als vertrauenswürdig angezeigt werden. Sie sehen die Zertifikate im Zertifikatespeicher des Servers. Diesen rufen Sie über *certlm.msc* auf.

Wollen Sie Hyper-V-Replikat im Cluster nutzen, müssen Sie einen Hyper-V Replikatbroker im Cluster-Manager von Windows Server 2012 R2 erstellen. Dabei gehen Sie vor wie bei jeder anderen Clusterressource. Zuvor sollten Sie aber ein neues Computerkonto im Snap-In *Active Directory-Benutzer und -Computer* erstellen. Rufen Sie die Registerkarte *Sicherheit* des neuen Objekts auf und geben Sie dem Computerkonto des Clusters Vollzugriff auf das neue Konto.

Hyper-V-Replikat mit SSL konfigurieren

Um SSL zu nutzen, rufen Sie auf beiden Hyper-V-Servern die Hyper-V-Einstellungen auf und klicken auf *Replikationskonfiguration*. Aktivieren Sie die Option *Zertifikatbasierte Authentifizierung verwenden (HHTPS)* und wählen Sie das Zertifikat aus, welches Sie für die Übertragung verwenden wollen.

Abbildg. 9.7 Aktivieren der zertifikatbasierten Authentifizierung für die Replikation



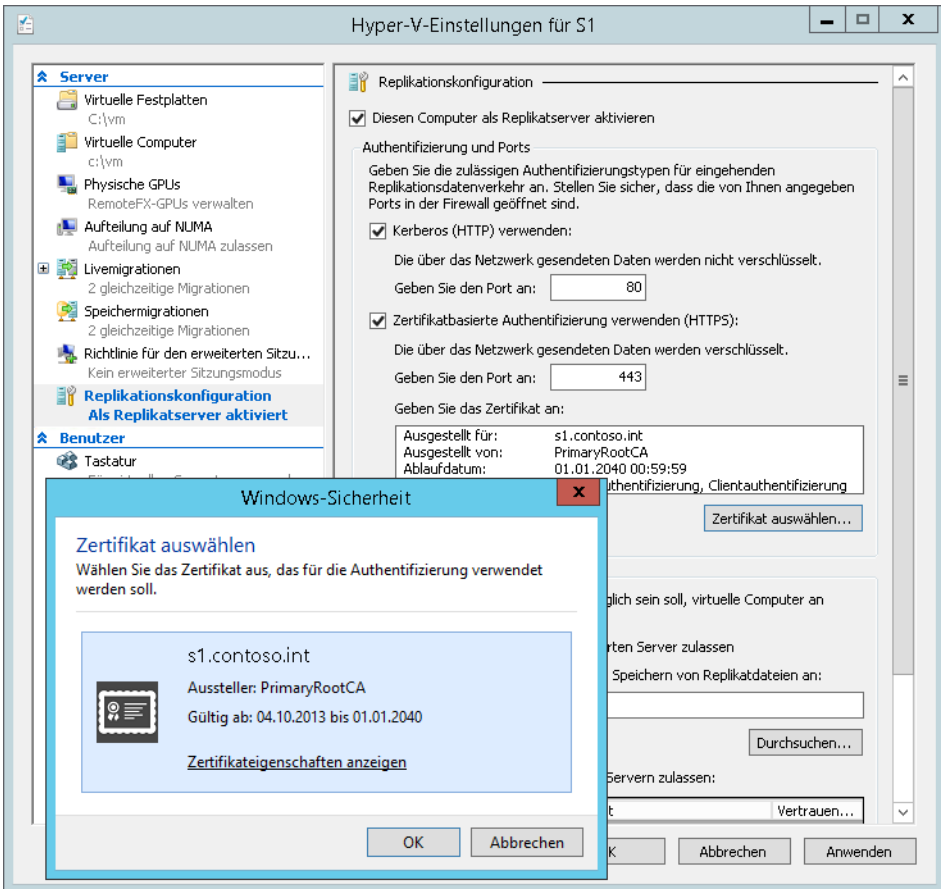
Diese Einstellungen müssen Sie auf allen beteiligten Servern vornehmen. Richten Sie danach die Replikation ein, wie auf den folgenden Seiten erläutert.

Virtuelle Server zwischen Hyper-V-Hosts replizieren

Haben Sie die Konfiguration nicht vor Aktivierung der Replikation auf den Hosts vorgenommen, erkennt das der Replikations-Assistent und schlägt die Konfiguration des Zielservers vor, während der Replikation vor. Diese Konfiguration ist dann auch über das Netzwerk möglich. Es ist allerdings empfehlenswert, diese Konfiguration vor der Einrichtung der Replikation von virtuellen Servern vorzunehmen.

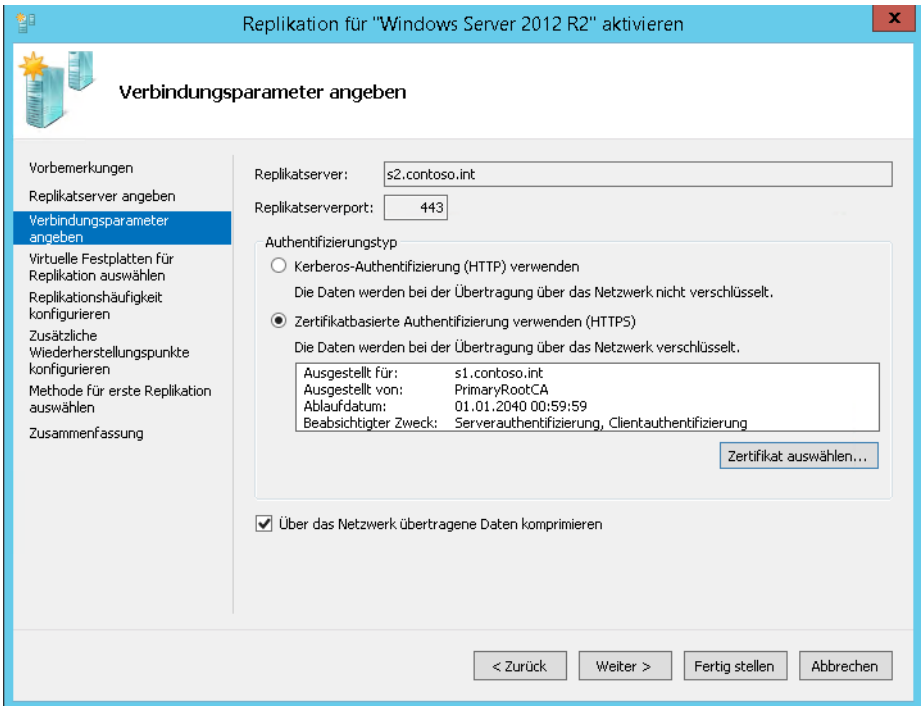
Um einen virtuellen Server zwischen Hyper-V-Hosts mit Windows Server 2012 R2 oder Hyper-V Server 2012 R2 zu replizieren, klicken Sie nach der Konfiguration der Hosts mit der rechten Maustaste auf den entsprechenden virtuellen Server und wählen *Replikation aktivieren*. Es startet ein Assistent, in dem Sie detailliert festlegen, wie Sie den ausgewählten Server vom Quellserver auf den Zielserver replizieren. Der virtuelle Server auf dem Quellserver bleibt dabei erhalten.

Abbildg. 9.8 Starten der Replikation von virtuellen Servern



Im Assistenten legen Sie danach die Zielserver und anschließend den Authentifizierungstyp fest. Für Testumgebungen verwenden Sie am besten zunächst die Kerberos-HTTP-Übertragung. Welche Authentifizierung der Zielserver akzeptiert, bestimmen Sie auf dem Zielserver in den Hyper-V-Einstellungen über *Replikationskonfiguration*.

Abbildg. 9.9 Festlegen der Verbindungsparameter zur Replikation

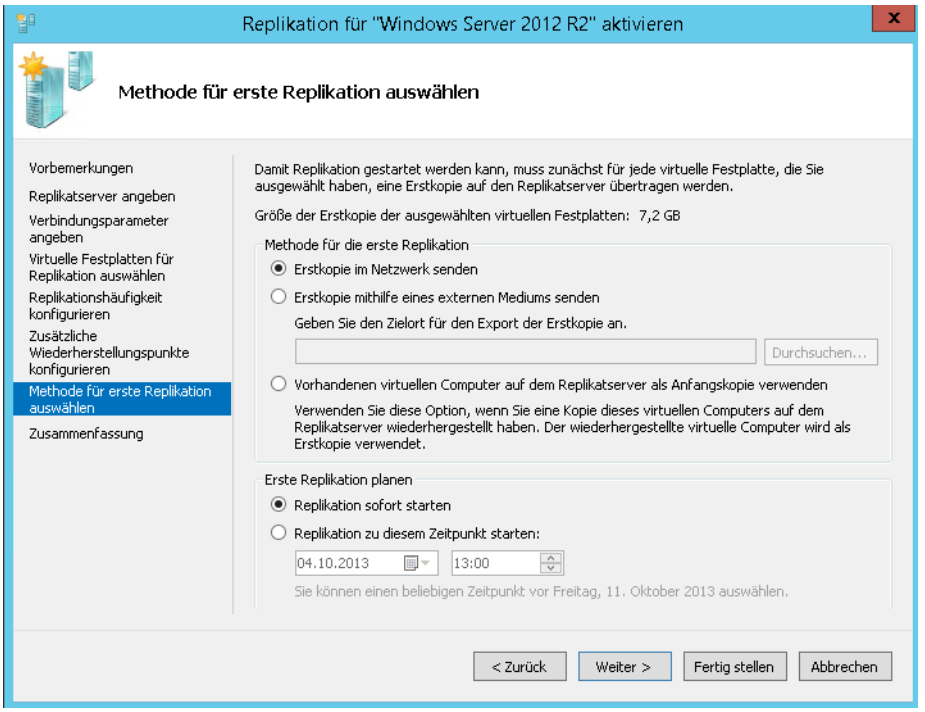


Wenn Sie auf dem Server ein Zertifikat installiert, in den Hyper-V-Einstellungen auch das Zertifikat hinterlegt sowie die zertifikatbasierte Authentifizierung aktiviert haben, können Sie für die Verbindung auch diesen Authentifizierungstyp wählen.

Außerdem steuern Sie im Assistenten, welche virtuellen Festplatten Sie replizieren möchten und in welchem Intervall die Replikation durchgeführt werden soll, nachdem Sie diese eingerichtet haben.

Im Assistenten können Sie auch die Prüfpunkte (Snapshots oder auch Momentaufnahmen) des Servers übertragen. Außerdem bestimmen Sie, ob die erste Replikation über ein Speichermedium wie eine externe Festplatte oder direkt über das Netzwerk durchgeführt werden soll. Auch einen Zeitplan legen Sie an dieser Stelle fest.

Abbildg. 9.10 Festlegen des Zeitplans der Replikation

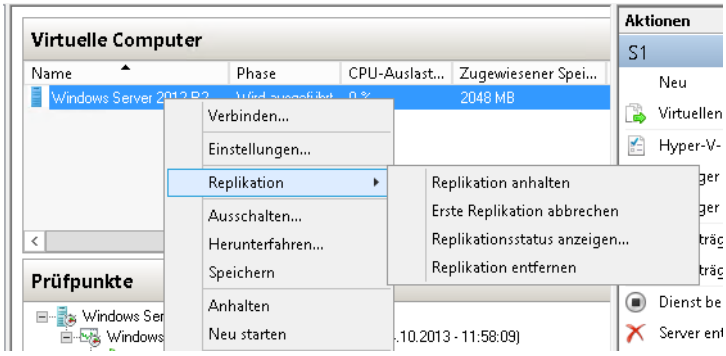


Damit die Replikation funktioniert, müssen Sie auf dem Zielserver in den erweiterten Einstellungen der Windows-Firewall (*wf.msc*) die Regeln für den HTTP-Listener oder den HTTPS-Listener aktivieren, je nachdem, welchen Datenverkehr Sie verwenden wollen. Die Regeln sind bereits angelegt, aber noch nicht aktiviert.

Nachdem Sie die Replikation durchgeführt haben, befindet sich der virtuelle Server auf den Zielservern, ist aber ausgeschaltet. Über das Kontextmenü des virtuellen Servers auf dem Quellserver können Sie über *Replikation* das Replikationsverhalten anpassen und den Status abrufen. Die Replikation können Sie auch zwischen verschiedenen Editionen von Windows Server 2012 R2 durchführen und auch Hyper-V Server 2012 R2 als Quell- und Zielserver nutzen. Am besten funktioniert die Replikation, wenn Sie eine Active Directory-Gesamtstruktur zur Authentifizierung nutzen.

Über das Kontextmenü des replizierten virtuellen Servers auf dem Zielserver und der Auswahl von *Replikation* können Sie auch ein Failover durchführen. In diesem Fall kann der virtuelle Server auf einem der Zielserver (Replikat) die Aufgaben des virtuellen Servers auf dem Quellserver (Original) übernehmen. Die Replikation können Sie jederzeit beenden. Bei jeder erneuten Replikation legt Hyper-V auf dem Zielserver einen Prüfpunkt des virtuellen Servers an.

Abbildg. 9.11 Verwalten der Replikation auf dem Quellserver nach der Einrichtung in Windows Server 2012 R2



Eine wichtige Rolle auch für Hyper-V spielt der deutlich verbesserte und beschleunigte Zugriff auf Dateifreigaben in Windows Server 2012 R2. Durch die Verbesserungen lassen sich jetzt auch virtuelle Festplatten auf Freigaben speichern. Dies beschleunigt die Replikation und auch die Livemigration. Wichtig für den Zugriff auf Dateiserver ist das Server Message-Protokoll. Dieses stellt den Zugriff von Clientcomputern zum Server dar. Windows 8.1 und Windows Server 2012 R2 verfügen dazu über das neue SMB 3-Protokoll. Dieses ist vor allem für den schnellen Zugriff über das Netzwerk gedacht, wenn Daten normalerweise lokal gespeichert sein sollten. Beispiele dafür sind SQL Server-Datenbanken oder die Dateien von Hyper-V-Computern. Die neue Version erlaubt mehrere parallele Zugriffe auf Dateifreigaben. Das heißt, einzelne Zugriffe über das Netzwerk bremsen sich nicht mehr untereinander aus.

Zusätzlich ermöglicht SMB 3 beim Einsatz auf geclusterten Dateiservern einen besseren Failover zwischen Clusterknoten. Dabei berücksichtigt Windows Server 2012 R2 die SMB-Sitzungen der Benutzer sowie Server und behält diese auch bei, wenn Sie virtuelle Dateiserver zwischen Clusterknoten verschieben.

Windows Server 2012 R2 kann auch als NAS-Server dienen. Im neuen Betriebssystem lassen sich nicht nur iSCSI-Ziele mit dem Server verbinden, sondern Server mit Windows Server 2012 R2 können selbst auch als iSCSI-Ziel arbeiten (siehe Kapitel 5). Die Clusterfunktion steht auch in Windows Server 2012 R2 Standard zur Verfügung.

Damit die Server mit Windows Server 2012 R2 und Clientcomputer mit Windows 8.1 untereinander schneller Daten austauschen können, ist keine Konfiguration notwendig. Diesen Geschwindigkeitszuwachs erhalten Unternehmen bereits standardmäßig. Von diesen Funktionen profitiert vor allem Hyper-V, wenn Sie Daten der virtuellen Servern auf Freigaben mit Windows Server 2012 R2 speichern.

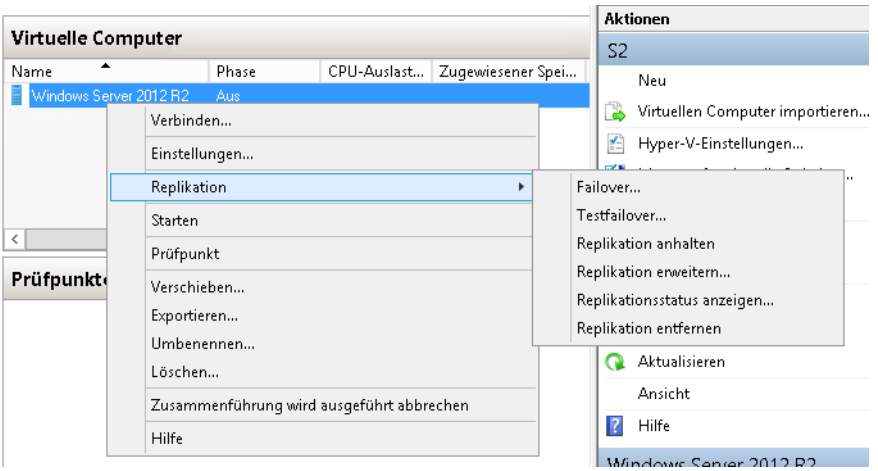
Sie können alle Einstellungen für Hyper-V-Replikat in den Einstellungen der einzelnen virtuellen Server anpassen. Sie können auch festlegen, wann die Replikation stattfinden soll oder ob Sie die Replikation manuell durchführen wollen. In den Einstellungen können Sie auch festlegen, welche virtuellen Festplatten Sie replizieren wollen.

TIPP Mit dem Cmdlet *Measure-VMReplication* lassen Sie sich den Status der Replikate auf den einzelnen Hyper-V-Hosts anzeigen.

Failover mit Hyper-V-Replikat durchführen

Der Vorteil von Hyper-V-Replikat ist, dass Sie bei Ausfall eines Servers ein Failover durchführen können. Dazu klicken Sie den entsprechenden virtuellen Server, den Sie repliziert haben, im Hyper-V-Manager an und wählen im Kontextmenü den Untermenübefehl *Replikation/Failover*.

Abbildg. 9.12 Verwalten der Replikation und Starten eines Failovers



Sie können auch einen geplanten Failover durchführen. In diesem Fall starten Sie das Failover vom Server aus, auf dem Sie die Quell-VM betreiben.

Anschließend wählen Sie aus, zu welchem Wiederherstellungspunkt Sie den Failover durchführen wollen, und können den Failover starten. Das funktioniert aber nur, wenn der Quell-VM ausgeschaltet ist. Während des Failovers startet der Assistent den replizierten Server, der im Netzwerk dann zur Verfügung steht, genau wie die Quell-VM.

Abbildg. 9.13 Durchführen eines Failovers

Auch wenn Sie ein geplantes Failover durchführen, müssen Quell-VM und Ziel-VM ausgeschaltet sein. Der Vorteil bei einem geplanten Failover vom Quell-Hyper-V-Host aus ist, dass Hyper-V noch nicht replizierte Änderungen an den Zielserver senden kann, sodass dieser über den neusten Stand verfügt. Haben Sie ein geplantes Failover durchgeführt, ist der alte Quell-VM später die neue Ziel-VM, und die alte Ziel-VM die neue Quell-VM für die Replikation. Das heißt, Sie können diesen Vorgang auch wieder umkehren.

Livemigration ohne Cluster

Neben der Hyper-V-Replikation können Sie virtuelle Server mit der neuen Livemigration auf einen anderen Hyper-V-Host verschieben, auch wenn dieser nicht Bestandteil eines Clusters ist. Bei diesem Vorgang kann die entsprechende virtuelle Maschine gestartet sein, genauso wie in einem Cluster. Sie müssen für die Livemigration auf beiden Servern den gleichen Prozessortyp einsetzen. Ansonsten bricht der Vorgang mit einem Fehler ab. In diesem Fall nutzen Sie Hyper-V-Replikat. Diese Funktion benötigt keine identischen Prozessoren.

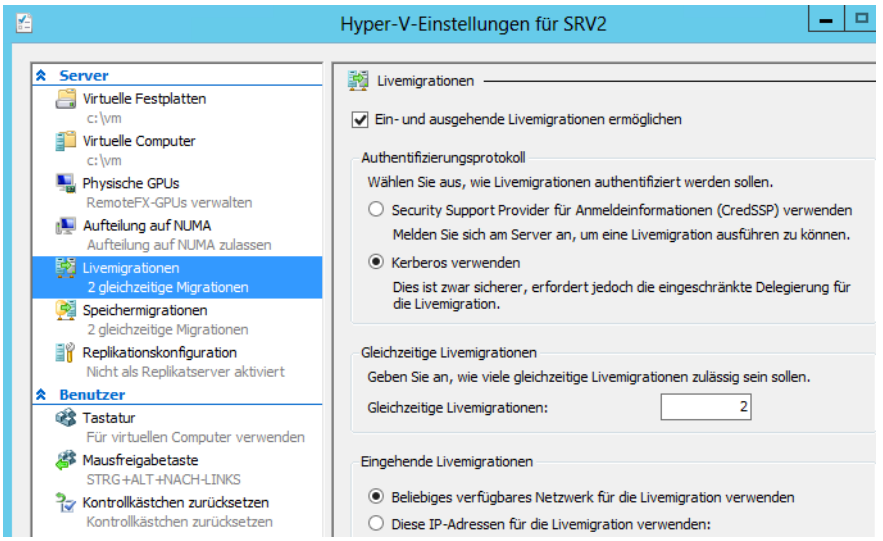
Damit Sie die Livemigration ohne Cluster nutzen können, müssen die entsprechenden Hyper-V-Hosts Mitglied der gleichen Active Directory-Domäne sein. Das Verschieben von virtuellen Servern mit der Hyper-V-Rolle muss ein Domänen-Administrator durchführen. Außerdem muss das Konto Mitglied der lokalen Administratorgruppe auf beiden Hyper-V-Hosts sein. Damit Sie zwischen Hyper-V-Hosts ohne Cluster-Livemigrationen durchführen können, müssen Sie für die entsprechenden Computerkonten in Active Directory Einstellungen bezüglich der Kerberos-Authentifizierung vornehmen.

Rufen Sie dazu in *Active Directory-Benutzer und -Computer* jeweils die Eigenschaften der beiden Computer auf und wechseln Sie zur Registerkarte *Delegierung*. Aktivieren Sie die Option *Computer bei Delegierungen angegebener Dienste vertrauen* sowie die Option *Nur Kerberos verwenden*. Klicken Sie anschließend auf *Hinzufügen* und wählen Sie den Server und die Dienste aus, die für das entsprechende Computerkonto Berechtigungen haben sollen. Für die Livemigration legen Sie dazu den Server und die Dienste *Cifs* und *Microsoft Virtual System Migration Service* sowie *Microsoft Virtual Control Service* fest. Nehmen Sie diese Einstellung auf allen Hyper-V-Hosts vor, die virtuelle Maschinen austauschen sollen. Auch hier können Sie virtuelle Server zwischen verschiedenen Editionen von Windows Server 2012 R2 auswählen und auch auf Hyper-V Server 2012 R2 setzen.

Im nächsten Schritt müssen Sie auf beiden Hyper-V-Hosts in den *Hyper-V-Einstellungen* im Hyper-V-Manager die Livemigration aktivieren. Sie finden diese Einstellung im Bereich *Livemigrationen*. Aktivieren Sie zunächst die Option *Ein- und ausgehende Livemigration ermöglichen* und danach bei *Authentifizierungsprotokoll* die Option *Kerberos verwenden*.

Legen Sie fest, wie viele Livemigrationen gleichzeitig auf dem Server erlaubt sein sollen. Der Standardwert in diesem Bereich ist 2. Aktivieren Sie dann bei *Eingehende Livemigrationen* entweder *Beliebiges verfügbares Netzwerk für die Livemigration verwenden* oder hinterlegen Sie manuell IP-Adressen.

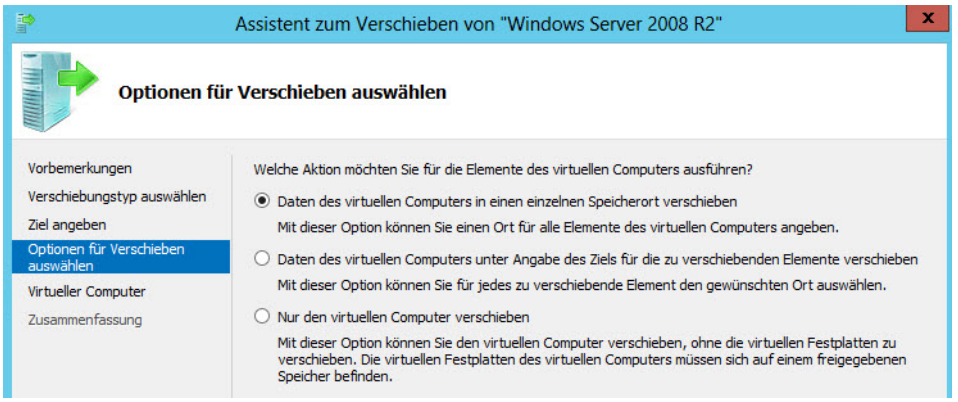
Abbildg. 9.14 Konfigurieren von Livemigration in Hyper-V



Wie die meisten Einstellungen in Windows Server 2012 R2 können Sie auch diese Einstellung über die PowerShell vornehmen. Dazu verwenden Sie der Reihe nach die folgenden Cmdlets:

```
Enable-VMMigration
Set-VMMigrationNetwork <IP-Adresse>
Set-VMHost –VirtualMachineMigrationAuthenticationType Kerberos
```

Abbildg. 9.15 Livemigration ohne Cluster



Anschließend können Sie virtuelle Server verschieben. Klicken Sie mit der rechten Maustaste auf den virtuellen Server, den Sie zwischen Hyper-V-Hosts verschieben wollen, und wählen Sie aus dem Kontextmenü die Option *Verschieben*. Anschließend wählen Sie auf der Seite *Verschiebungstyp auswählen* die Option *Virtuellen Computer verschieben*. Danach wählen Sie den Zielcomputer aus, auf den Sie den entsprechenden Computer verschieben wollen. Sie können neben kompletten virtuellen

Servern auch nur die virtuellen Festplatten verschieben. Auch den Speicherort der Daten legen Sie im Assistenten fest.

Im nächsten Fenster können Sie die Livemigration noch genauer spezifizieren. Sie haben die Möglichkeit, verschiedene Daten des virtuellen Servers in unterschiedliche Ordner oder alle Daten des Servers inklusive der virtuellen Festplatten in einen gemeinsamen Ordner zu verschieben. Liegt die virtuelle Festplatte eines virtuellen Servers auf einer Freigabe, können Sie auch nur die Konfigurationsdateien zwischen den Hyper-V-Hosts verschieben.

Haben Sie die Option zum Verschieben ausgewählt, verbindet sich der Assistent mit dem Remoteserver über den Remotedateibrowser und Sie können den lokalen Ordner auswählen, in den Hyper-V die virtuelle Festplatten und Konfigurationsdaten des virtuellen Servers verschieben soll. Als Letztes erhalten Sie noch eine Zusammenfassung angezeigt und starten das Verschieben mit *Fertig stellen*.

Diesen Vorgang können Sie ebenfalls skripten. Öffnen Sie dazu auf dem Quellserver eine PowerShell-Sitzung und geben Sie den folgenden Befehl ein:

```
Move-VM <Virtueller Server> <Zielserver> -IncludeStorage -DestinationStoragePath <Lokaler
Pfad auf dem Zielserver>
```

Damit die Übertragung funktioniert, müssen die Prozessoren der Hyper-V-Hosts kompatibel miteinander sein. Ist das nicht der Fall, erhalten Sie eine Fehlermeldung angezeigt und können den Server nicht im laufenden Betrieb übertragen. Sie können in diesem Fall aber den virtuellen Server herunterfahren und den Vorgang erneut starten. Ist der Name des virtuellen Switchs auf dem Zielserver nicht mit dem Quellserver identisch, erhalten Sie eine Fehlermeldung angezeigt und können den neuen virtuellen Switch auf dem Zielserver auswählen, damit dem virtuellen Server auch auf dem neuen Host eine Netzwerkverbindung zur Verfügung steht.

Hyper-V im Cluster – Livemigration in der Praxis

Sie können auch in Windows Server 2012 R2 weiterhin Hyper-V im Cluster betreiben und virtuelle Server als Clusterressourcen betreiben. Unternehmen, die Server mit Hyper-V virtualisieren und eine Hochverfügbarkeit erreichen wollen, setzen auf die Livemigration im Cluster.

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. Dazu betreiben Sie die virtuellen Server als Clusterressourcen.

Clusterknoten vorbereiten

Ein Cluster braucht auch in Windows Server 2012 R2 zunächst ein Quorum, also einen gemeinsamen Datenträger, auf den alle Clusterknoten zugreifen dürfen.

Legen Sie einen Namen für den Cluster fest. Dieser Name erhält kein Computerkonto, wird aber für die Administration des Clusters verwendet. Jeder Knoten des Clusters erhält ein Computerkonto in derselben Domäne. Daher erfordert jeder physische Knoten einen entsprechenden Rechnernamen.

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 Server und die Netzwerkkarten für die private Kommunikation des Clusters erhalten je eine IP-Adresse in einem getrennten Subnetz (wichtig!).

Auf den Clusterknoten installieren Sie zunächst Windows Server 2012 R2 und nehmen diese Installation in die Domäne auf. Alle Clusterknoten müssen sich in der gleichen Active Directory-Domäne befinden.

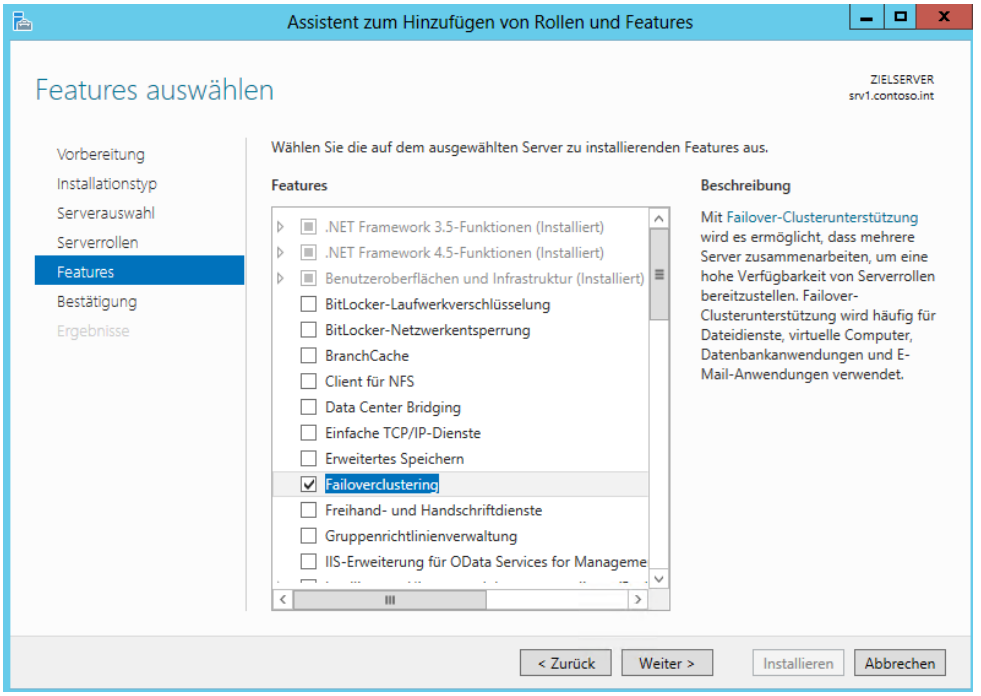
Haben Sie das Betriebssystem auf dem Server installiert und die iSCSI-Laufwerke verbunden, nehmen Sie die IP-Einstellungen für die Knoten vor. Eine Netzwerkkarte dient dabei zur Kommunikation der Server mit dem Netzwerk. Die andere Netzwerkkarte dient zur Kommunikation der Knoten untereinander, dem Heartbeat. Benennen Sie nach der Konfiguration der Netzwerkkarte die Verbindungen am besten um, zum Beispiel in *private* und *public*.

Cluster mit Windows Server 2012 R2 installieren

Um Hyper-V in einem Cluster zu betreiben, installieren Sie zunächst einen herkömmlichen Cluster mit Windows Server 2012 R2. Das funktioniert jetzt auch mit der Standard-Edition oder auch mit der kostenlosen Serverversion Hyper-V Server 2012 (siehe Kapitel 2).

Die Dateien der virtuellen Server sind auf dem gemeinsamen Datenträger des Clusters gespeichert. Fällt der aktive Knoten aus, kann der passive Knoten die virtuellen Server übernehmen. Auf dem gemeinsamen Datenträger sind auch die virtuellen Festplatten der virtuellen Server gespeichert.

Abbildg. 9.16 Installieren der Clusterunterstützung in Windows Server 2012 R2



Setzen Sie Hyper-V im Cluster ein, müssen Sie bei der Datensicherung und der Erstellung von Prüfpunkten einige wichtige Aspekte beachten. Sie sollten es möglichst vermeiden, Prüfpunkte von laufenden virtuellen Maschinen in Clustern zu erstellen. Setzen Sie einen solchen Prüfpunkt zurück, setzt dieser nicht nur den Inhalt der virtuellen Festplatte zurück, sondern auch den des Arbeitsspeichers der VM.

Dieser Umstand führt vor allem im Zusammenhang mit der Livemigration zu Problemen. Wenn Sie also Prüfpunkte von VMs in einem Cluster durchführen wollen, fahren Sie die VM herunter. Auch wenn Sie einen Prüfpunkt auf eine VM anwenden wollen, sollten Sie die Maschine vorher herunterfahren.

Grundlage für Livemigration mit Hyper-V oder dem generellen Betrieb von Hyper-V im Cluster ist zunächst ein normaler Cluster mit Windows Server 2012 R2. Jeder Knoten des Clusters erhält ein Computerkonto in derselben Domäne in Active Directory. Jeder physische Knoten benötigt eine IP-Adresse, der Cluster erhält eine IP-Adresse, jeder virtuelle Server und die Netzwerkkarten für die private Kommunikation des Clusters erhalten eine IP-Adresse in einem getrennten Subnetz.

Setzen Sie in den Einstellungen der Netzwerkverbindung auf der Registerkarte *WINS* in den erweiterten Einstellungen für IPv4 die Option *NetBIOS über TCP/IP deaktivieren*, da NetBIOS die interne Kommunikation eines Clusters stören kann. Ändern Sie die Bindungsreihenfolge so ab, dass die Netzwerkverbindung ins herkömmliche Netzwerk ganz oben ist. Die Einstellungen für den internen Clusterverkehr ordnen Sie danach ein.

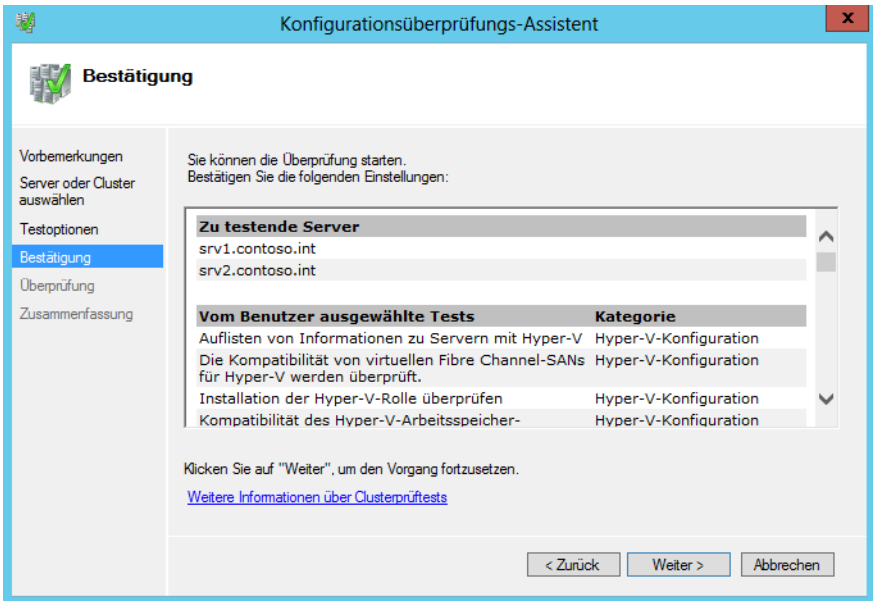
In den erweiterten Eigenschaften der Windows-Firewall sollten Sie auf der Registerkarte *Erweitert* die Firewall für das private Clusternetz und für das Netzwerk zum Datenspeicher deaktivieren. Clustering installieren Sie auch in Windows Server 2012 R2 als Feature über den Server-Manager. Während der Installation nehmen Sie keine Einstellungen vor. Achten Sie darauf, dass die gemeinsamen Datenträger auf allen Knoten verbunden und mit dem gleichen Laufwerksbuchstaben versehen sind. Sie können hier auch iSCSI-Ziele verwenden, wie in Kapitel 5 beschrieben.

Um die notwendigen Features für einen Hyper-V-Cluster zu installieren, können Sie auch die PowerShell verwenden. Geben Sie die folgenden Cmdlets ein:

```
Add-WindowsFeature Hyper-V
Add-WindowsFeature Failover-Clustering
Add-WindowsFeature Multipath-IO
```

Starten Sie dann auf dem ersten Knoten die Failovercluster-Verwaltung durch Eingabe von *cluster* auf der Startseite. Klicken Sie auf den Link *Konfiguration überprüfen*. Sie wählen im Fenster zunächst die potentiellen Clusterknoten aus und legen fest, welche Tests das Tool durchführen soll.

Abbildg. 9.17 Testen der Server für die Clusterinstallation



Nachdem der Assistent alle wichtigen Punkte erfolgreich getestet hat, erstellen Sie den Cluster. Sie können auch in der PowerShell einen Cluster erstellen. Die Syntax dazu lautet:

```
New-Cluster -Name <Clustername> -StaticAddress <IP-Adresse des Clusters> -Node <Knoten 1>,
<Knoten 2>
```

Beim Erstellen des Clusters geben Sie zunächst den Namen sowie dessen IP-Adresse ein. Der Name des Clusters wird zur Verwaltung genutzt und mit der IP-Adresse greifen Sie auf den Cluster zu.

Cluster Shared Volumes aktivieren

Ein wichtiger Punkt für die Livemigration sind die freigegebenen Clustervolumes (Cluster Shared Volumes, CSV). Diese ermöglichen es, dass mehrere Server in einem gemeinsamen Datenträger gleichzeitig auf einen gemeinsamen Datenträger zugreifen können. Das hat folgenden Hintergrund: Neben einem automatischen Failover lassen sich virtuelle Server auch manuell übertragen, auch Livemigration genannt. Der Start einer Livemigration kann entweder über die Clusterkonsole erfolgen, per Skript (auch PowerShell) oder über den System Center Virtual Machine Manager (SCVMM). Die Livemigration setzt voraus, dass der Clusterknoten, der die VM hostet, noch läuft. Die Livemigration liest den Arbeitsspeicher virtuellen Servers aus und überträgt ihn zum Zielserver. Alle Systeme, die mit Hyper-V laufen, lassen sich mit der Livemigration absichern. Das heißt, es lassen sich auch Linux- oder ältere Windows-Server per Livemigration im Cluster absichern.

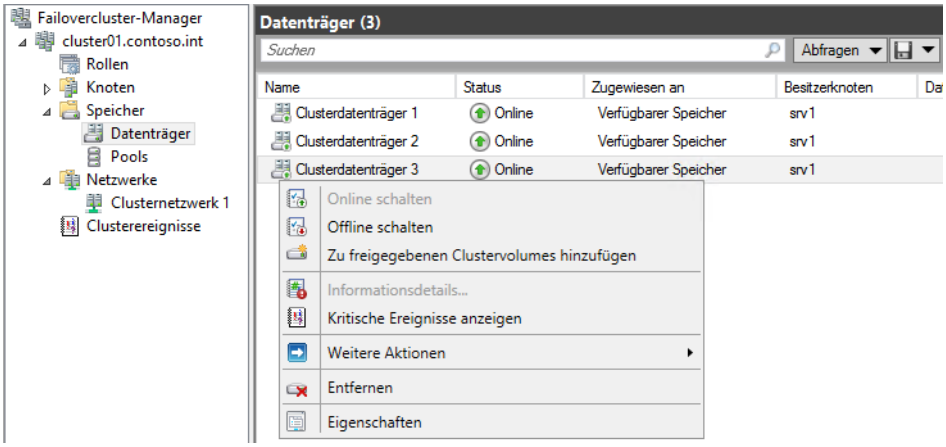
Um Hyper-V mit Livemigration in einem Cluster zu betreiben, aktivieren Sie die freigegebenen Clustervolumes (CSV) für den Cluster, nachdem Sie diesen erstellt haben. Windows legt dann auf der Betriebssystempartition im Ordner *ClusterStorage* Daten ab. Diese liegen aber nicht tatsächlich

auf der Festplatte *C:* des Knotens, sondern auf dem gemeinsamen Datenträger, dessen Abruf auf den Ordner *C:\ClusterStorage* umgeleitet ist.

Die VHD(X)-Dateien der VMs liegen in diesem Ordner und sind daher von allen Knoten gleichzeitig zugreifbar. Fällt eine Netzwerkverbindung zum SAN von einem Knoten aus, verwendet der Knoten alternative Strecken über andere Knoten. Die virtuellen Maschinen, deren Dateien im CSV liegen, laufen uneingeschränkt weiter. Um CSV für einen Cluster zu aktivieren, gehen Sie folgendermaßen vor:

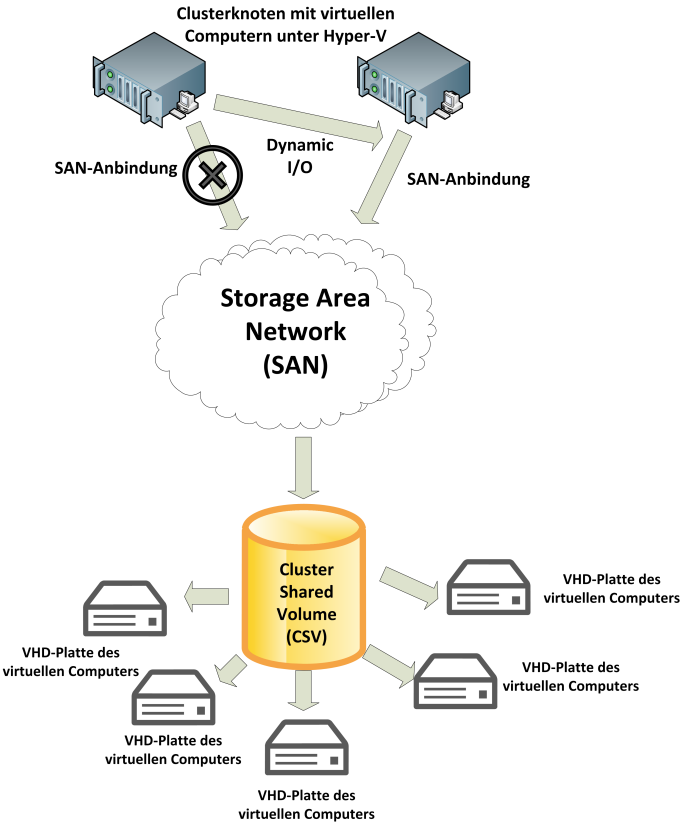
1. Starten Sie das Verwaltungsprogramm für den Failovercluster.
2. Klicken Sie mit der rechten Maustaste im Bereich *Speicher/Datenträger* auf den Datenträger, den Sie für Hyper-V nutzen wollen, und wählen *Zu freigegebenen Clustervolumes hinzufügen*.

Abbildg. 9.18 Freigegebene Clustervolumes erstellen



Cluster in Windows Server 2012 R2 beherrschen Dynamic I/O. Wenn die Datenverbindung eines Knotens ausfällt, kann der Cluster den Datenverkehr der für die Kommunikation zu den virtuellen Computern im SAN notwendig ist, automatisch über die Leitungen des zweiten Knotens routen, ohne dazu ein Failover durchführen zu müssen. Sie können einen Cluster so konfigurieren, dass die Clusterknoten den Netzwerkverkehr zwischen den Knoten und zu den CSV priorisieren.

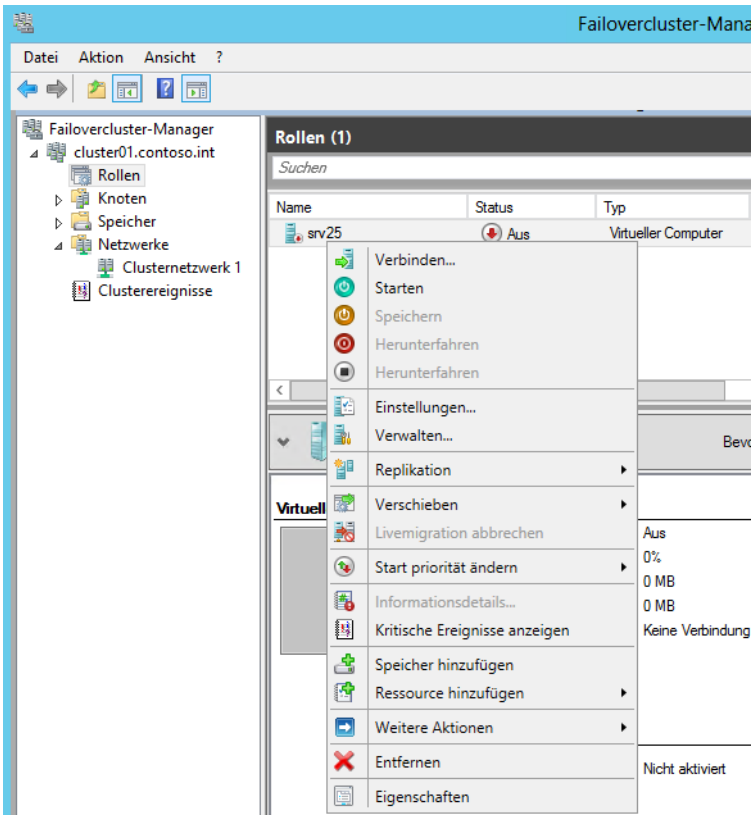
Abbildg. 9.19 Dynamic I/O in einem Hyper-V-Cluster



Damit Sie die Livemigration nutzen können, müssen Sie als Nächstes auf allen Clusterknoten Hyper-V installieren, genauso wie auf herkömmlichen Servern, auf denen Sie Hyper-V betreiben wollen. Danach können Sie virtuelle Server in der Clusterverwaltung oder im System Center Virtual Machine Manager erstellen:

1. Um eine virtuelle Maschine in einem Cluster zu erstellen, verwenden Sie den Failovercluster-Manager. Klicken Sie mit der rechten Maustaste auf *Rollen/Virtueller Computer/Neuer virtueller Computer* und starten Sie den Assistenten.
2. Wählen Sie den Clusterknoten, auf dem Sie diesen Server bereitstellen wollen.
3. Schließen Sie die Erstellung des virtuellen Servers ab. Der Assistent konfiguriert ihn automatisch für den Cluster. Die Konfiguration entspricht der Einrichtung von virtuellen Servern mit dem Hyper-V-Manager (siehe Kapitel 7).
4. Klicken Sie mit der rechten Maustaste auf den virtuellen Computer, sehen Sie, dass im Failovercluster-Manager auch die Steuerung der virtuellen Maschinen hinterlegt ist. Sie können über diesen Weg den virtuellen Server komplett verwalten. Wählen Sie *Virtuelle Computer starten* aus. Dadurch wird die Ressource online geschaltet und die virtuelle Maschine startet. Über das Kontextmenü können Sie sich jetzt mit dem virtuellen Computer verbinden und das Betriebssystem installieren.

Abbildg. 9.20 Virtuelle Computer im Failovercluster-Manager verwalten



Standardmäßig kann die Livemigration nach der Installation eines Clusters und der Integration von virtuellen Computern verwendet werden. Wollen Sie eine Livemigration durchführen, klicken Sie den virtuellen Computer mit der rechten Maustaste an, rufen im Kontextmenü den Eintrag *Verschieben/Livemigration* auf und wählen den Knoten aus. Zuvor müssen Sie aber die Livemigration auf den entsprechenden Hyper-V-Hosts in den Hyper-V-Einstellungen konfigurieren. Dabei gehen Sie vor, wie bei der Konfiguration von Livemigration ohne Cluster.

Während des ganzen folgenden Ablaufs läuft die VM uneingeschränkt weiter und Anwender können ungestört mit dem virtuellen Server arbeiten. Der Ablauf dabei ist folgender:

1. Beim Start baut der Quellserver eine Verbindung zum Zielserver auf, der die virtuelle Maschine in Echtzeit erhalten soll.
2. Anschließend überträgt der Quellserver die Konfiguration der VM auf den Zielserver.
3. Der Zielserver erstellt auf Basis dieser leeren Konfiguration eine neue VM, die der zu verschiebenden VM entspricht.
4. Anschließend überträgt der Quellserver die einzelnen Seiten des Arbeitsspeichers zur Ziel-VM in einer Standardgröße von etwa 4 KB. In diesem Schritt zeigt sich die Geschwindigkeit des Netzwerks. Je schneller das Netzwerk ist, umso schneller wird der Inhalt des Arbeitsspeichers übertragen.

5. Als Nächstes übernimmt der Zielserver die virtuellen Festplatten des Quellservers für die zu übertragende virtuelle Maschine.
6. Anschließend setzt der Zielserver die virtuelle Maschine online.
7. Als Nächstes wird die virtuelle Hyper-V-Switch informiert, dass Netzwerkverkehr jetzt zur MAC-Adresse des Zielservers gesendet werden soll.

Die Leistung der Netzwerkkarte spielt dabei ebenfalls eine besondere Rolle. Aus diesem Grund spielen hier dedizierte Karten eine besondere Rolle. Der Unterschied zur Schnellmigration ist, dass die Maschinen während der Übertragung durch Livemigration aktiv bleiben und auch der Arbeitsspeicherinhalt zwischen den Servern übertragen wird. Bei der Schnellmigration deaktiviert Hyper-V die Maschinen erst. Windows Server 2012 R2 beherrscht neben der Livemigration auch weiterhin die Schnellmigration (*Verschieben/Schnellmigration*).

Sie können einen Cluster mit Windows Server 2012 R2 so konfigurieren, dass die Clusterknoten den Netzwerkverkehr zwischen den Knoten und zu den gemeinsamen Datenträgern priorisiert. Für einen schnellen Überblick, welche Netzwerkeinstellungen der Cluster zur Kommunikation mit dem Cluster Shared Volume (CSV) nutzt, starten Sie eine PowerShell-Sitzung auf dem Server und rufen das Cmdlet *Get-ClusterNetwork* auf.

TIPP Sie können über das Kontextmenü von geclusterten virtuellen Servern auch eine Replikation starten, genauso wie bei normalen Hyper-V-Hosts auch.

Virtuelle Server im Cluster verwalten

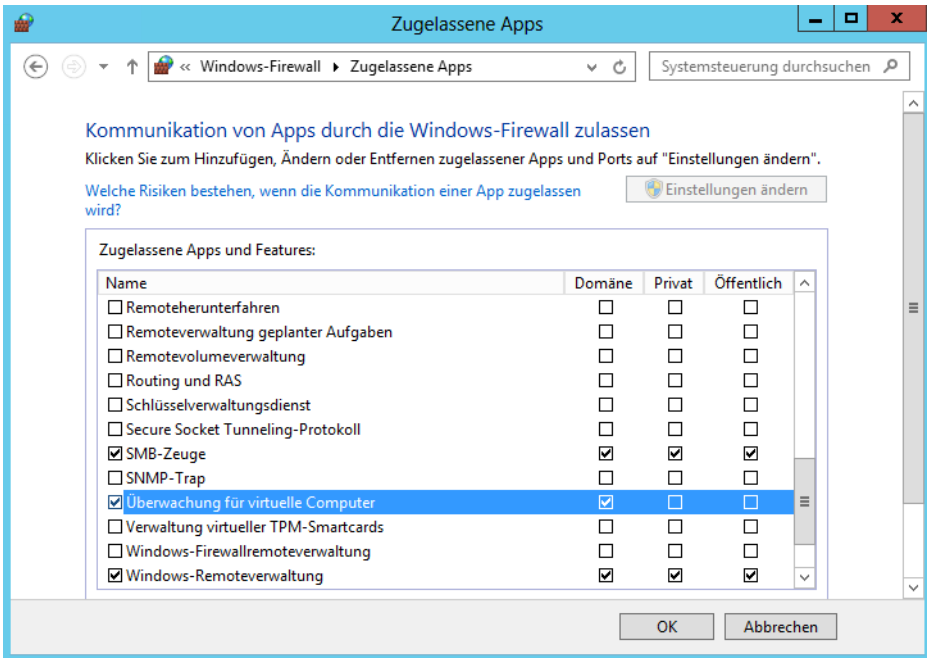
Die virtuellen Server, die Sie im Cluster erstellen, müssen Sie in der Failovercluster-Verwaltung steuern. Klicken Sie auf einen virtuellen Server, stehen im Aktionsbereich die verschiedenen Funktionen zur Verfügung. Diese erhalten Sie auch über das Kontextmenü des virtuellen Servers. Neu ist zum Beispiel der Bereich *Startpriorität ändern*. So können Sie festlegen, wann bestimmte virtuelle Server starten sollen.

Ebenfalls neu ist die Möglichkeit, die Überwachung für virtuelle Server im Cluster festzulegen. Sie finden diese Einstellung über *Weitere Aktionen/Überwachung konfigurieren*. Anschließend wählen Sie die Dienste aus, die der Cluster überwachen soll. Fällt in der VM einer der ausgewählten Dienste aus, kann der Cluster die VM neu starten oder auf einen anderen Knoten verschieben. Damit Sie diese Funktion nutzen können, müssen Sie in der Windows-Firewall allerdings die Überwachung in der Firewall zulassen:

1. Starten Sie die Systemsteuerung und navigieren Sie zu *System und Sicherheit/Windows-Firewall*.
2. Klicken Sie auf *Eine App oder ein Feature durch die Windows-Firewall zulassen*.
3. Aktivieren Sie das Feature *Überwachung für virtuelle Computer* und lassen Sie es für das Domänennetzwerk zu.

Alternativ aktivieren Sie die Remoteverwaltung mit der PowerShell, indem Sie *Enable-PSRemoting* eingeben und die Regeln aktivieren lassen. Anschließend können Sie vom Hyper-V-Host aus mit der PowerShell eine Verbindung mit der VM aufbauen und die Überwachung aktivieren. Das ist zum Beispiel sinnvoll für Core-Server.

Abbildg. 9.21 Zulassen der Überwachung eines virtuellen Servers



MAC-Adressen im Cluster konfigurieren

Wichtig sind die Einstellungen für virtuelle MAC-Adressen in den Einstellungen der virtuellen Netzwerkkarten. Hier müssen Sie bezüglich der Livemigration, beim Betrieb von Hyper-V im Cluster und vor allem der Aktivierung des Betriebssystems von virtuellen Servern Einstellungen vornehmen, da Sie ansonsten ständig die Server neu aktivieren müssen. Außerdem spielen diese Einstellungen auch in NLB-Clustern mit Exchange und auch für SharePoint eine Rolle.

Verschieben Sie einen virtuellen Server mit aktivierten dynamischen MAC-Adressen im Cluster auf einen anderen Host durch die Livemigration, ändert sich dessen MAC-Adresse beim nächsten Start dieser virtuellen Maschine. Im MSDN-Beitrag auf der Seite *http://blogs.msdn.com/b/virtual_pc_guy/archive/2010/05/14/hyper-v-and-dynamic-mac-address-regeneration.aspx* [Ms179-K09-02] finden Sie dazu umfangreiche Informationen. Jeder Hyper-V-Host hat einen eigenen Pool aus dynamischen MAC-Adressen. Welcher das ist, sehen Sie im Hyper-V-Manager über den Manager für virtuelle Switches. Microsoft beschreibt dieses Problem auf der Webseite *http://support.microsoft.com/kb/953828/de-de* [Ms179-K09-03] noch genauer. Der Beitrag bezieht sich zwar auf Windows Server 2008, ist aber weiterhin gültig. Aus diesem Grund ist es empfehlenswert, die statische Zuordnung von MAC-Adressen für virtuelle Server zu aktivieren.

Sie finden diese Einstellung im Bereich *Netzwerkkarte* der einzelnen virtuellen Server im Hyper-V-Manager. In diesen Einstellungen können Sie auch das Spoofing für Netzwerkkarten steuern. Hyper-V kann genau unterscheiden, welche Netzwerkdaten zu den einzelnen Servern gesendet werden sollen, und verwendet dazu die MAC-Adresse des virtuellen Servers. Das heißt, virtuelle Server empfangen nur die Daten, die für ihre MAC-Adresse gedacht sind.

Nacharbeiten: Überprüfung des Clusters und erste Schritte mit der Clusterverwaltung oder der PowerShell

Die zentrale Verwaltungsstelle eines Clusters ist die Failovercluster-Verwaltung, mit der Sie neue Cluster erstellen, neue Knoten hinzufügen und den Cluster verwalten. Das Befehlszeilentool *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 /?*. Vor allem zur Automatisierung oder für Administratoren, die lieber mit Befehlszeilenanweisungen arbeiten, bietet Microsoft, neben dem bekannten Befehl *Cluster* mit den verschiedenen Optionen, auch das Cmdlet *Get-Cluster*, mit dem Sie in der PowerShell Aufgaben der Clusterverwaltung durchführen.

Generell bietet das Cmdlet *Get-Cluster* (und weitere Cmdlets) in der PowerShell die gleichen Möglichkeiten wie das Tool *Cluster.exe* in der herkömmlichen Eingabeaufforderung. Damit Sie Failovercluster in der PowerShell verwenden können, müssen Sie nicht mehr das Modul für Failovercluster in der PowerShell laden. Module kann die PowerShell automatisch laden.

Tabelle 9.1 Clusterverwaltung in der PowerShell und Eingabeaufforderung

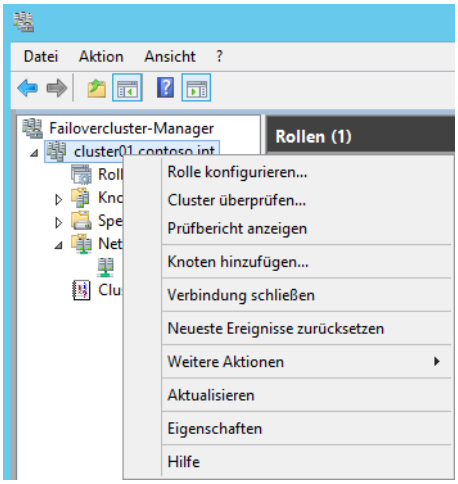
Aufgabe	Eingabeaufforderung	PowerShell
Clustereigenschaften anzeigen	*Cluster /prop*	*Get-Cluster*
Cluster erstellen	*Cluster /create*	*New-Cluster*
Cluster löschen	*Cluster /destroy*	*Remove-Cluster*
Clusterknoten hinzufügen	*Cluster /add*	*Add-ClusterNode*
Cluster herunterfahren	*Cluster /shutdown*	*Stop-Cluster*
Clusterquorum verwalten	*Cluster /quorum*	*Get-ClusterQuorum* *Set-ClusterQuorum*
Status von Clusterknoten	*Cluster node /status*	*Get-ClusterNode |fl **
Clusterknoten anhalten	*Cluster node /pause*	*Suspend-ClusterNode*
Clusterknoten fortsetzen	*Cluster node /resume*	*Resume-ClusterNode*
Clusterknoten starten	*Cluster node /start*	*Start-ClusterNode*
Clusterknoten stoppen	*Cluster node /stop*	*Stop-ClusterNode*
Clusterknoten entfernen	*Cluster node /evict*	*Remove-ClusterNode*
Clusterinformationen nach dem Löschen bereinigen	*Cluster node /forcecleanup*	*Clear-Clusternode*
Clustergruppen anzeigen	*Cluster group*	*Get-ClusterGroup*
Eigenschaften von Clustergruppen	*Cluster group /prop*	*Get-ClusterGroup |fl **

Tabelle 9.1 Clusterverwaltung in der PowerShell und Eingabeaufforderung *(Fortsetzung)*

Aufgabe	Eingabeaufforderung	PowerShell
Clustergruppen erstellen	*Cluster group <Name> /create*	*Add-ClusterGroup* *Add-ClusterFileServerRole* *Add-ClusterPrintServerRole* *Add-ClusterVirtualMachineRole* Hilfe über: *Get-Help Add-Cluster*role*
Clustergruppe löschen	*Cluster group <Name> /delete*	*Remove-ClusterGroup <Name>*
Clustergruppe online/offline schalten	*Cluster group <Name> /online /offline*	*Start-ClusterGroup <Name>* *Stop ClusterGroup <Name>*
Clustgergruppe auf anderen Knoten verschieben	*Cluster group <Name> move*	*Move-ClusterGroup*
Clusterressourcen anzeigen	*Cluster resource /prop*	*Get-ClusterResource |fl **
Clusterressource erstellen/ löschen	*Cluster resource <Name> /create /delete*	*Add-ClusterResource* *Remove-ClusterResource*
Clusterressource online/offline schalten	*Cluster resource <Name> /online /offline*	*Start-ClusterResource* *Stop-ClusterResource*
Clusternetzwerk verwalten	*Cluster network /prop*	*Get-ClusterNetwork*

Klicken Sie den Namen des Clusters in der grafischen Verwaltungsoberfläche der Clusterverwaltung mit der rechten Maustaste an, können Sie die Eigenschaften des Clusters überprüfen und anpassen. Ebenso bietet das Kontextmenü zahlreiche Verwaltungsmöglichkeiten an.

Abbildg. 9.22 Verwalten von Clustern



Auf der Registerkarte *Allgemein* in den Eigenschaften des Clusters können Sie den Name des Clusters anpassen. Über die Registerkarte *Ressourcentypen* definieren Sie, welche Windows-Ressourcen

dem Cluster zur Verfügung stehen. Und über die Registerkarte *Clusterberechtigungen* steuern Sie den administrativen Zugriff der Administratoren auf den Cluster.

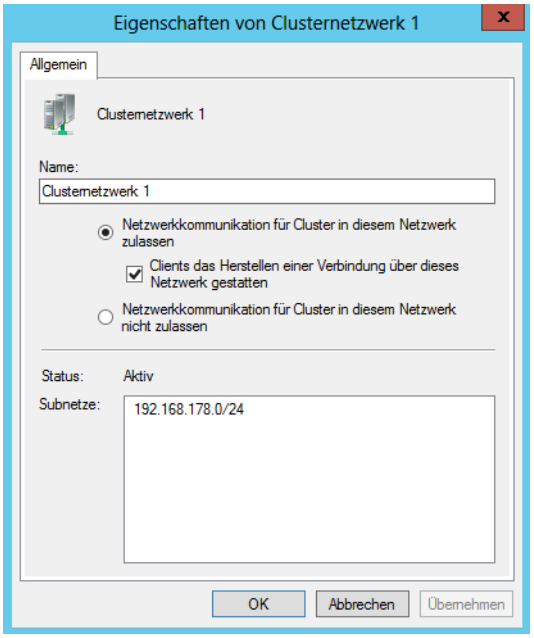
Nach einem Klick auf den Konsoleneintrag *Speicher* in der Clusterverwaltung sehen Sie die gemeinsamen Datenträger. Hier sehen Sie auch den derzeitig aktuellen Knoten, der den Cluster aktiv verwaltet. Der zweite Knoten steht offline zur Verfügung. Hierüber fügen Sie auch neue Datenträger dem Cluster hinzu oder schalten vorhandene Ressourcen offline.

In einer Produktivumgebung sollten Sie auf jeden Fall den Konsoleneintrag *Netzwerke* aufrufen. Hier verwalten Sie die öffentlichen und privaten Verbindungen des Clusters. In den Eigenschaften der Verbindungen ist 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.

Achten Sie darauf, dass bei der privaten Verbindung nur die Option *Netzwerkkommunikation für Cluster in diesem Netzwerk zulassen* aktiviert ist. Dadurch ist sichergestellt, dass dem Heartbeat ein privater Kanal im Netzwerk zur Verfügung steht.

Bei den Eigenschaften der *public*-Verbindung sollten Sie die Option *Netzwerkkommunikation für Cluster in diesem Netzwerk zulassen* sowie die Option *Clients das Herstellen einer Verbindung über dieses Netzwerk gestatten* aktivieren. Damit ist auf jeden Fall sichergestellt, dass die Clusterverbindung intern funktioniert, auch wenn eine private Netzwerkkarte ausfällt. Bei einer fast perfekten Ausfallsicherheitskonfiguration verfügt jeder Clusterknoten über mindestens drei Netzwerkkarten. Eine Karte dient der internen Kommunikation, eine ausschließlich der privaten und die dritte zur Ausfallsicherheit und ist für den gemischten Modus aktiviert. Nur dadurch erhalten Sie eine optimale Ausfallsicherheit.

Abbildg. 9.23 Konfigurieren eines Clusternetzwerks für den öffentlichen und privaten Zugriff



Wollen Sie weitere Laufwerke im Cluster zur Verfügung stellen, müssen Sie diese in die Clusterverwaltung integrieren. Zuvor müssen Sie die Laufwerke aber auf allen Knoten verfügbar machen. Bereits integrierte Laufwerke sehen Sie, wenn Sie den Menübefehl *Speicher/Datenträger* aufrufen. Hier zeigt die Failovercluster-Verwaltung alle bereits integrierten Laufwerke und deren Status an. Wählen Sie nach einem Klick mit der rechten Maustaste den Kontextmenübefehl *Speicher/Datenträger*, können Sie mit *Datenträger hinzufügen* neu installierte Datenträger in den Cluster integrieren.

Zusammenfassung

In diesem Kapitel haben wir Ihnen die Funktionen gezeigt, mit denen Sie Hyper-V hochverfügbar zur Verfügung stellen. Neben der neuen Replikation und der Livemigration ohne Cluster war auch der Betrieb eines Clusters mit Windows Server 2012 R2 Thema dieses Kapitels.

Im nächsten Kapitel erfahren Sie mehr über den Umgang mit Active Directory.

Teil D

Active Directory

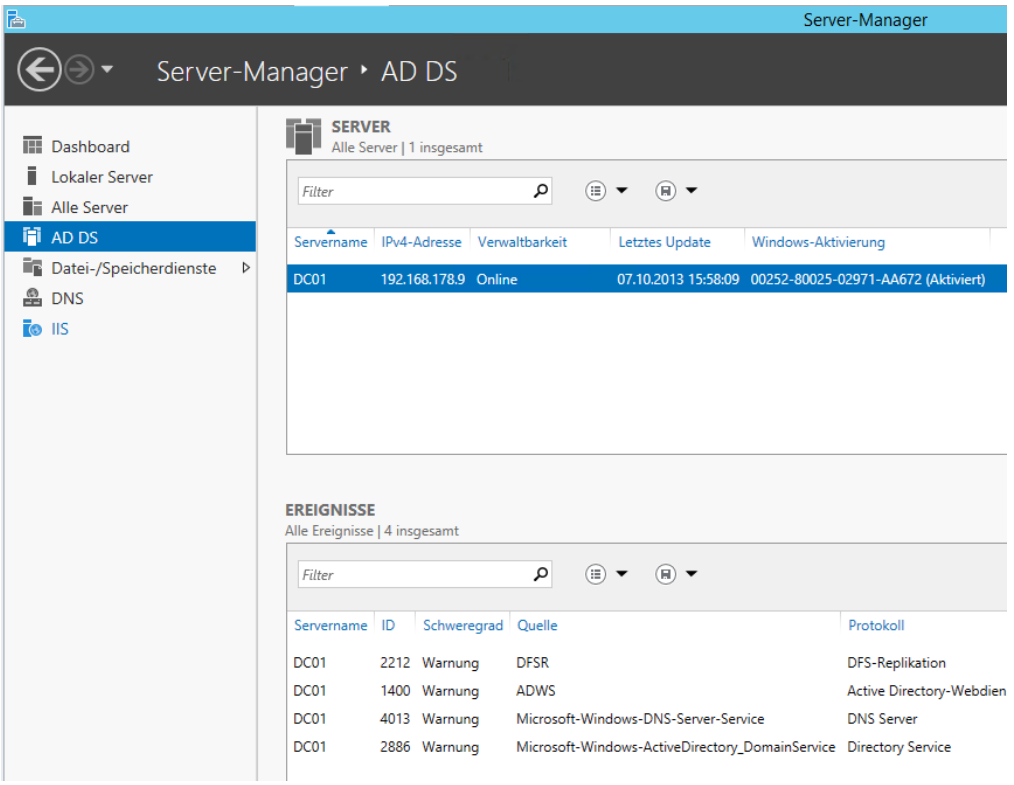
Kapitel 10

Active Directory – Grundlagen und erste Schritte

In diesem Kapitel:

Mit Windows Server 2012 bietet Microsoft zahlreiche Verbesserungen im Bereich Active Directory und ermöglicht auch eine bessere und leichtere Verwaltung. Diese Neuerungen sind auch Bestandteil in Windows Server 2012 R2. In diesem Kapitel zeigen wir Ihnen die wichtigsten Neuerungen und deren praktischen Einsatz. In den weiteren Kapiteln gehen wir dann ausführlicher auf die Installation und Verwaltung von Active Directory ein.

Abbildg. 10.1 Domänencontroller im Server-Manager verwalten



Neuerungen in Active Directory im Überblick

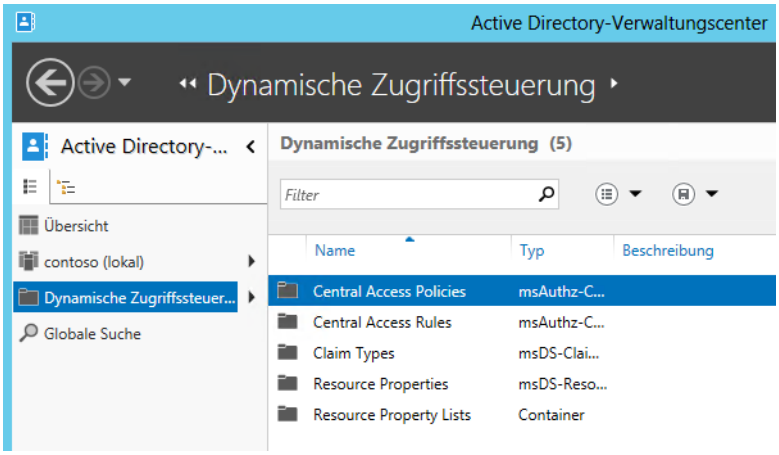
Ein wichtiger Vorteil seit Windows Server 2012 ist, dass sich Domänencontroller leichter virtualisieren lassen, das gilt uneingeschränkt auch für Windows Server 2012 R2. Das Erstellen von Snapshots mit Hyper-V für Domänencontroller stellt in Windows Server 2012 R2 kein Problem mehr dar. Allerdings empfiehlt Microsoft, zur Virtualisierung von Domänencontrollern auf Hyper-V in Windows Server 2012/2012 R2 zu setzen. Die neue Version unterstützt virtuelle Domänencontroller standardmäßig. Um einen virtuellen Domänencontroller zu klonen, sind keine Spezialwerkzeuge notwendig, sondern Sie kopieren einfach die virtuelle Maschine und geben dem Klon einen neuen Namen. Auf Basis der neuen GenerationID in Windows Server 2012 R2 und deren Unterstützung in Hyper-V erkennt der neue Server Active Directory und bindet sich problemlos ein.

Die verwalteten Dienstkonten (Managed Service Accounts) die Kennwörter für Dienste selbst verwalten, lassen sich in Windows Server 2012/2012 R2 auf mehreren Servern einsetzen, in Windows Server 2008 R2 ist jedes Dienstkonto nur auf einem Server unterstützt. DHCP-Server lassen sich ohne einen Cluster zu Teams zusammenfassen. Die Eingabeaufforderung gibt es auch in Windows Server 2012 R2 weiterhin. Zusätzlich enthält der Server, aber auch der Windows 8/8.1-Client, die neue Version 4.0 der PowerShell. Diese lässt sich ebenfalls wesentlich leichter bedienen als noch in Windows Server 2008 R2.

Mit der dynamischen Zugriffssteuerung (Dynamic Access Control, siehe Kapitel 33) können Sie einfacher die Berechtigungen für den Zugriff auf Dateien, Ordner und sogar SharePoint-Bibliotheken steuern. Dazu lassen sich Dateien mit Metadaten versorgen, die nur bestimmten Anwendern, zum Beispiel allen Anwendern einer Abteilung oder der Geschäftsführung, den Zugriff erlauben, unabhängig davon, in welchem Ordner oder in welcher Freigabe die Daten gespeichert sind. Das Ganze funktioniert lückenlos, auch beim Verschieben von Dateien in SharePoint-Bibliotheken.

Zusätzlich lässt sich über diesen Weg auch festlegen, von welchen Geräten aus Anwender auf die Daten zugreifen dürfen. Unsichere PCs, Heim-Arbeitsplätze, Computer in Internet-Cafés oder Smartphones lassen sich über diesen Weg aussperren. Die Funktion nutzt dazu die Active Directory-Rechteverwaltung.

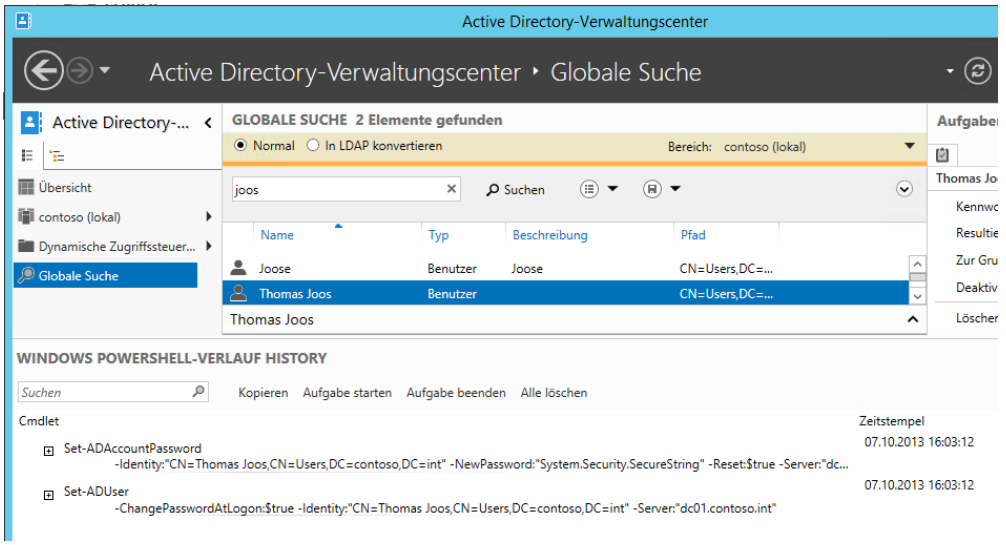
Abbildg. 10.2 Die dynamische Zugriffssteuerung in Windows Server 2012 R2



Domänencontroller lassen sich leichter installieren und verwalten. Den Installations-Assistenten für Active Directory hat Microsoft überarbeitet. Dcpromo, der Einrichtungs-Assistent in Vorgängerversionen, ist nicht mehr vorhanden. Die Verwaltungskonsole *Active Directory-Verwaltungscenter* von Windows Server 2008 R2 hat Microsoft in Windows Server 2012 überarbeitet. Diese Version erlaubt zum Beispiel die Aktivierung und Verwendung des Papierkorbs von Active Directory und weitere Aufgaben, die in Windows Server 2008 R2 über die PowerShell erledigt werden mussten.

Auch die Gruppenrichtlinien für Kennwörter lassen sich in der neuen Konsole konfigurieren und Organisationseinheiten zuordnen. Neu im unteren Bereich des Active Directory-Verwaltungscenters ist die Windows PowerShell History. Diese bietet PowerShell-Befehle als Protokoll an. Dazu müssen Sie nur auf den Link klicken und sehen alle durchgeführten Aufgabe der grafischen Oberfläche als Befehl für die PowerShell. Dieses Fenster gilt aber nicht nur als Protokoll, sondern Administratoren können Befehle für Skripts aus dem Fenster herauskopieren.

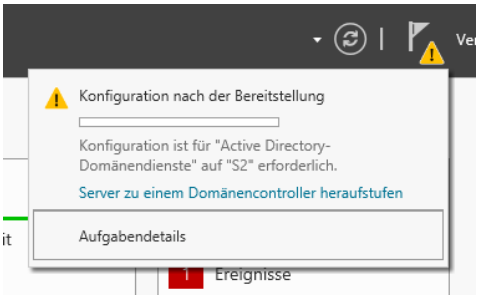
Abbildg. 10.3 Anzeigen von PowerShell-Befehlen im Active Directory-Verwaltungscenter



Um Active Directory zu installieren, wählen Sie die Serverrolle *Active Directory Domänendienste* aus. Nach der Installation der notwendigen Systemdateien lässt sich der Einrichtungs-Assistent über einen Link im letzten Fenster starten. Alternativ starten Sie die Einrichtung über das Benachrichtigungsfenster im Server-Manager. Im Assistenten nehmen Sie ähnliche Eingaben vor wie in Windows Server 2008 R2, allerdings erscheinen weniger Fenster und der Assistent konfiguriert wichtige Einstellungen automatisch im Hintergrund.

Im letzten Fenster erhalten Sie eine Zusammenfassung und können Active Directory installieren. Der Installations-Assistent zur Integration von Active Directory in Windows Server 2012 R2 wurde von Microsoft grundlegend überarbeitet. Er zeigt weniger Auswahlfenster und erlaubt eine schnellere Installation. Das Tool Dcpromo ist nicht mehr im System integriert. Während der Installation der eigentlichen Serverrolle installieren Sie nur die Active Directory-Systemdateien, Sie nehmen keine Einstellungen vor.

Abbildg. 10.4 Nach der Installation der Domänendienste meldet sich das Benachrichtigungscenter des Server-Managers



Wie Sie bei der Einrichtung und Installation von Active Directory vorgehen, zeigen wir Ihnen in den nächsten Kapiteln.

Active Directory mit dem Verwaltungscenter verwalten

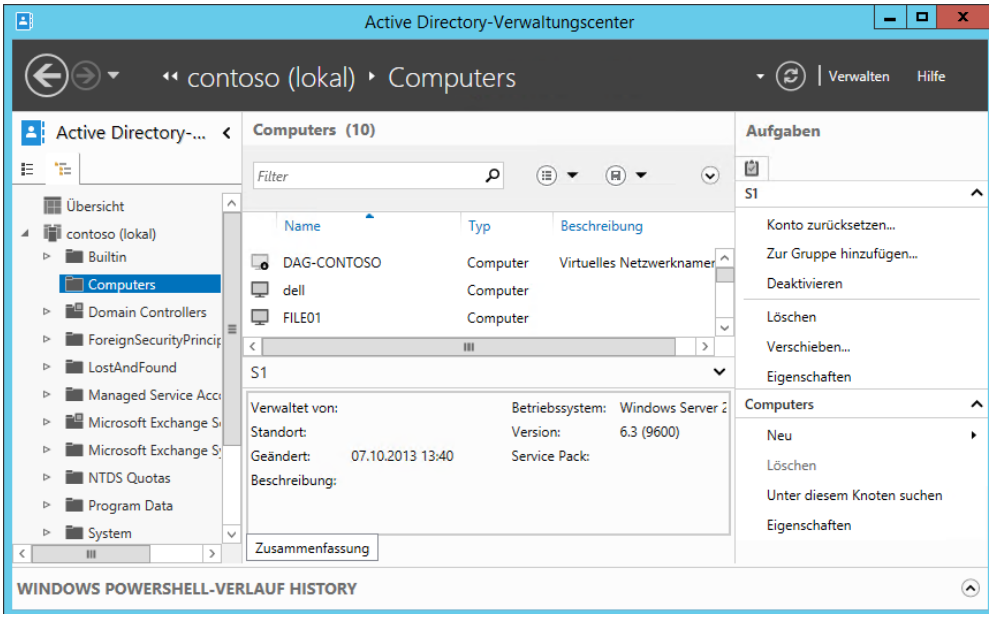
Microsoft möchte das mit Windows Server 2008 R2 eingeführte Active Directory-Verwaltungscenter mehr in die tägliche Routine von Administratoren einbinden. Mit der Verwaltungsoberfläche bietet Microsoft eine zentrale Anlaufstelle für alle Routineaufgaben in Active Directory in einer einzelnen Oberfläche. Der Aufbau der Konsole ist stark aufgabenorientiert. Im Gegensatz zu den anderen Verwaltungstools basieren die Aufgaben im Verwaltungscenter auf Befehle aus der PowerShell.

Die Standard-Verwaltungskonsolen für Active Directory, zum Beispiel *Active Directory-Benutzer und -Computer*, sind immer noch verfügbar. Hier haben sich im Vergleich zu Windows Server 2008 R2 keine größeren Änderungen ergeben. Das gilt auch für die Snap-Ins *Active Directory-Standorte und -Dienste* und *Active Directory-Domänen und Vertrauensstellungen*.

Das *Active Directory-Verwaltungscenter* bietet nicht alle Möglichkeiten der anderen beschriebenen Snap-Ins, sondern dient vor allem der Abarbeitung von Routineaufgaben wie das Zurücksetzen von Kennwörtern oder das Anlegen von neuen Objekten. Erstellen Sie neue Objekte wie Organisationseinheiten oder Benutzerkonten, zeigt das Center übersichtliche und leicht verständliche Formulare an.

Das Tool verbindet sich über die Active Directory-Webdienste mit Active Directory. Sie starten das Active Directory-Verwaltungscenter entweder über die Programmgruppe *Tools* im Server-Manager oder indem Sie *dsac* in der PowerShell oder der Eingabeaufforderung eingeben. Auf der linken Seite der Konsole lässt sich durch die Domänen und die Organisationseinheiten navigieren. Im linken oberen Bereich können Sie zwischen einer Baumstruktur wie in *Active Directory-Benutzer und -Computer* und einer Struktur ähnlich wie dem Startmenü von Windows Server 2008 R2 wechseln.

Abbildg. 10.5 Mit dem Active Directory-Verwaltungscenter verwalten Sie Active Directory in Windows Server 2012 R2 leichter

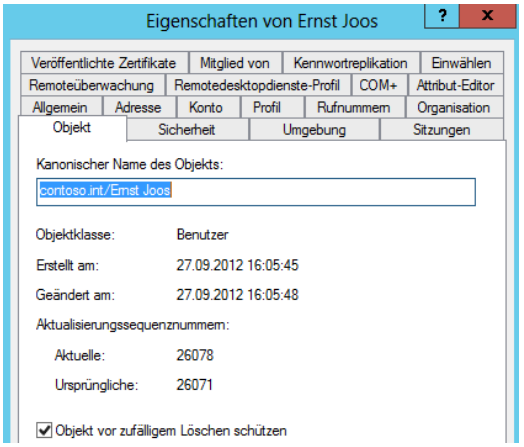


Verwenden Sie die Listenansicht (ändern über die Registerkarten oben links), lässt sich beim Einblenden einer Organisationseinheit der Inhalt dieser OU an das Startfenster des Verwaltungscenters anheften, sodass dieser Bereich dauerhaft im Verwaltungscenter erscheint. Dazu muss lediglich auf das blaue Pinnsymbol oben rechts geklickt werden, wenn Sie das entsprechende Menü öffnen. Über den Pinn können Sie den Vorgang auch wieder rückgängig machen. Über den Menüpunkt *Globale Suche* lässt sich nach Objekten in allen Domänen der Gesamtstruktur suchen, unabhängig von der Domäne, mit der das Verwaltungscenter aktuell verbunden ist.

Direkt auf der Startseite können Sie häufige Aufgaben durchführen wie das Zurücksetzen eines Benutzerkennworts oder das Durchsuchen von Active Directory. Sie können den Navigationsbereich des Active Directory-Verwaltungscenters jederzeit anpassen, indem Sie verschiedene Container aus jeder beliebigen Domäne als separate Knoten hinzufügen. Die Liste der zuletzt verwendeten Objekte wird automatisch unter einem Navigationsknoten angezeigt.

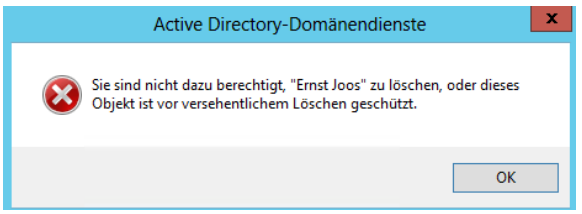
In Windows Server 2012 R2 sind Active Directory-Objekte vor dem versehentlichen Löschen geschützt. Dieser Schutz ist standardmäßig aktiviert. Nachdem Sie über das Menü *Ansicht* in *Active Directory-Benutzer und -Computer* die erweiterte Ansicht aktiviert haben, finden Sie auf der Registerkarte *Objekt* das Kontrollkästchen *Objekt vor zufälligem Löschen schützen* vor.

Abbildg. 10.6 In Windows Server 2012 R2 sind Active Directory-Objekte vor dem versehentlichen Löschen geschützt



Diese Option steuert die Berechtigungen auf der Registerkarte *Sicherheit*. Der Gruppe *Jeder* wird der Eintrag *Löschen* verweigert. Dies äußert sich darin, dass ein Administrator vor dem Löschen eines solchen geschützten Objekts zunächst das Kontrollkästchen zu dieser Option deaktivieren muss, bevor er das Objekt löschen kann. Deaktivieren Sie das Kontrollkästchen nicht, erhalten Sie eine Fehlermeldung, dass der Zugriff verweigert wird, wenn Sie das Objekt löschen wollen.

Abbildg. 10.7 Geschützte Objekte in Active Directory können auch durch Administratoren nicht gelöscht werden



PowerShell und Active Directory

Windows Server 2012 R2 lässt sich auch in der PowerShell verwalten. Dazu hat Microsoft einige neue Cmdlets integriert. Mit dem Cmdlet *Install-ADDSDomainController* installieren Sie in einer bestehenden Domäne zum Beispiel einen neuen Domänencontroller. Mit *Install-ADDSDomain* installieren Sie eine neue Domäne, mit *Install-ADDSForest* eine neue Gesamtstruktur.

Um einen Domänencontroller herabzustufen, verwenden Sie das Cmdlet *Uninstall-ADDSDomainController*. Die Cmdlets fragen alle notwendigen Optionen an und startet den Server neu. Konfigurationen wie *DNS-Server* und *globaler Katalog* nehmen Sie anschließend vor. Diese Aufgaben müssen Sie nicht mehr im Assistenten zur Installation vorgeben.

Auch neue Cmdlets, um die Installation und Betrieb von Active Directory zu testen, hat Microsoft integriert. Dazu gibt es die neuen Cmdlets *Test-ADDSDomainControllerInstallation*, *Test-ADDSDomainControllerUninstallation, Test-ADDSDomainInstallation*, *Test-ADDSForestInstallation* und *Test-ADDSReadOnlyDomainControllerunInstallation*. Mehr dazu lesen Sie in diesem Kapitel und in Kapitel 11.

TIPP Um Active Directory-Objekte abzurufen, stellt Microsoft zahlreiche neue Cmdlets zur Verfügung. Eine Liste erhalten Sie über den Befehl *Get-Command Get-Ad**.

Um neue Objekte zu erstellen, gibt es ebenfalls zahlreiche neue Cmdlets. Die Liste dazu erhalten Sie durch Eingabe von *Get-Command New-Ad**.

Eine Liste mit Befehlen zum Löschen von Objekten zeigt die PowerShell mit *Get-Command Remove-Ad**.

Änderungen an Active Directory-Objekten nehmen Sie mit *Set*-Cmdlets vor. Eine Liste erhalten Sie über *Get-Command Set-Ad**.

Abbildg. 10.8 Neue Cmdlets zum Anzeigen von Active Directory-Objekten

```
PS C:\Users\Administrator> get-command get-ad*

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Get-ADAccountAuthorizationGroup                    ActiveDirectory
Cmdlet          Get-ADAccountResultantPasswordReplicationPolicy    ActiveDirectory
Cmdlet          Get-ADCentralAccessPolicy                          ActiveDirectory
Cmdlet          Get-ADCentralAccessRule                            ActiveDirectory
Cmdlet          Get-ADClaimTransformPolicy                         ActiveDirectory
Cmdlet          Get-ADClaimType                                    ActiveDirectory
Cmdlet          Get-ADComputer                                     ActiveDirectory
Cmdlet          Get-ADComputerServiceAccount                       ActiveDirectory
Cmdlet          Get-ADDCCloningExcludedApplicationList             ActiveDirectory
Cmdlet          Get-ADDefaultDomainPasswordPolicy                  ActiveDirectory
Cmdlet          Get-ADDomain                                       ActiveDirectory
Cmdlet          Get-ADDomainController                             ActiveDirectory
Cmdlet          Get-ADDomainControllerPasswordReplicationPolicy    ActiveDirectory
Cmdlet          Get-ADDomainControllerPasswordReplicationPolicy... ActiveDirectory
Cmdlet          Get-ADFineGrainedPasswordPolicy                    ActiveDirectory
Cmdlet          Get-ADFineGrainedPasswordPolicySubject             ActiveDirectory
Cmdlet          Get-ADForest                                       ActiveDirectory
Cmdlet          Get-ADGroup                                        ActiveDirectory
Cmdlet          Get-ADGroupMember                                  ActiveDirectory
Cmdlet          Get-ADObject                                       ActiveDirectory
Cmdlet          Get-ADOptionalFeature                              ActiveDirectory
Cmdlet          Get-ADOrganizationalUnit                           ActiveDirectory
Cmdlet          Get-ADPrincipalGroupMembership                     ActiveDirectory
Cmdlet          Get-ADReplicationAttributeMetadata                 ActiveDirectory
Cmdlet          Get-ADReplicationConnection                        ActiveDirectory
Cmdlet          Get-ADReplicationFailure                           ActiveDirectory
Cmdlet          Get-ADReplicationPartnerMetadata                   ActiveDirectory
Cmdlet          Get-ADReplicationQueueOperation                    ActiveDirectory
Cmdlet          Get-ADReplicationSite                              ActiveDirectory
Cmdlet          Get-ADReplicationSiteLink                          ActiveDirectory
Cmdlet          Get-ADReplicationSiteLinkBridge                    ActiveDirectory
Cmdlet          Get-ADReplicationSubnet                            ActiveDirectory
Cmdlet          Get-ADReplicationUpToDatenessVectorTable           ActiveDirectory
Cmdlet          Get-ADResourceProperty                             ActiveDirectory
Cmdlet          Get-ADResourcePropertyList                         ActiveDirectory
Cmdlet          Get-ADResourcePropertyValueType                    ActiveDirectory
Cmdlet          Get-ADRootDSE                                      ActiveDirectory
Cmdlet          Get-ADServiceAccount                               ActiveDirectory
Cmdlet          Get-ADTrust                                        ActiveDirectory
Cmdlet          Get-ADUser                                         ActiveDirectory
Cmdlet          Get-ADUserResultantPasswordPolicy                  ActiveDirectory
```

Migration zu Active Directory mit Windows Server 2012 R2

Wollen Sie Domänencontroller zu Windows Server 2012 R2 aktualisieren, müssen Sie zunächst das Schema der Gesamtstruktur erweitern. Dazu führen Sie den Befehl *adprep /forestprep* auf einem Domänencontroller aus. Sie finden das Tool im Ordner *support\adprep* auf der Windows Server 2012 R2-DVD.

Damit Sie das Schema erweitern können, müssen Sie zuvor noch mit *c* die Erweiterung bestätigen. Diese Maßnahmen lassen sich nicht mehr rückgängig machen lassen. Nach der Aktualisierung des Schemas sollten Sie mit *adprep /domainprep* noch die einzelnen Domänen aktualisieren. Installieren Sie neue Domänencontroller, lassen sich diese problemlos in Active Directory aufnehmen. Auch Mitgliedsserver mit Windows Server 2012 R2 können Sie in bestehende Domänen aufnehmen, wenn Domänencontroller mit Windows Server 2003/2003 R2/2008/2008 R2/2012 vorhanden sind.

Bei Migrationen können Sie Betriebsmasterrollen von Vorgängerversionen auf die neuen Domänencontroller mit Windows Server 2012 R2 übernehmen. Die Vorgänge dazu sind identisch mit der Übernahme in Windows Server 2008 R2.

Verbessertes und sicheres DNS-System in Windows Server 2012 R2

Durch die engere Verzahnung der Server miteinander ist auch eine Verbesserung des DNS-Systems notwendig, vor allem im Bereich der Sicherheit. Bereits mit Windows Server 2008 R2 hat Microsoft DNSSEC eingeführt, um Zonen und Einträge abzusichern. Die Verwaltung von DNS-Servern ist im Server-Manager von Windows Server 2012 R2 durch die Gruppierung wesentlich effizienter.

In Windows Server 2012 R2 lassen sich Zonen online digital signieren. DNSSEC lässt sich in der neuen Version komplett in Active Directory integrieren. Das umfasst auch die Möglichkeit, dynamische Updates für geschützte Zonen zu aktivieren. Windows Server 2012 R2 unterstützt offizielle Standards wie NSEC3 und RSA/SHA-2. Neu ist auch die Unterstützung von DNSSEC auf schreibgeschützten Domänencontrollern (RODC, siehe Kapitel 13). Findet ein RODC mit Windows Server 2012 R2 eine signierte DNS-Zone, legt er automatisch eine sekundäre Kopie der Zone an und überträgt die Daten der DNSEC-geschützten Zone. Dies hat den Vorteil, dass auch Niederlassungen mit RODCs gesicherte Daten auflösen können, aber die Signatur und Daten der Zone nicht in Gefahr sind.

DNSSEC lässt sich über das Kontextmenü von Zonen erstellen. Eine komplizierte Konfiguration in der Eingabeaufforderung ist nicht mehr notwendig. Auch das Offlinesetzen von Zonen ist nicht mehr notwendig. Die Signierung der Zone erfolgt über einen Assistenten. Mit diesem können Sie recht einfach DNS-Zonen vor Manipulationen schützen.

Der Assistent erlaubt die manuelle Signierung, eine Aktualisierung der Signierung und eine Signierung auf Basis automatischer Einstellungen. Mit Windows Server 2012 R2 lassen sich signierte Zonen auch auf andere DNS-Server im Netzwerk replizieren. Eine weitere Neuerung ist der IP-Adressverwaltungsserver (IPAM, siehe Kapitel 24). Dieser Serverdienst überwacht und steuert zentral DHCP- und DNS-Server. Die Installation erfolgt als Serverrolle. Der Dienst kann Änderungen überwachen und die Serverdienste zentral überwachen.

Active Directory remote verwalten

Administratoren können zur Remoteverwaltung von Active Directory-Domänencontrollern entweder per Remotedesktop auf den Server zugreifen oder von der eigenen Arbeitsstation aus mit der PowerShell. Neben der PowerShell stehen aber auch andere Tools auf Arbeitsstationen zur Verfügung, um Active Directory zu verwalten. Das funktioniert mit Windows 7 und Windows Server 2008 R2 sowie auch in Windows 8.1 und Windows Server 2012 R2. Wollen Sie Windows Server 2012 R2 von Arbeitsstationen mit Windows 8 verwalten, verwenden Sie die Remoteserver-Verwaltungstools (siehe Kapitel 3).

Die Verwaltungstools für Active Directory finden Sie zum Beispiel über *Rollenverwaltungstools/AD DS-/AD LDS-Tools*. Hier stehen auch die Cmdlets zur Verwaltung von Active Directory zur Verfügung, zum Beispiel das Active Directory-Modul für Windows PowerShell. Damit Sie einen Server über die PowerShell remote verwalten können, müssen Sie die Remoteverwaltung auf dem Server aktivieren. Dazu geben Sie auf dem entsprechenden Server den Befehl *Enable-PSRemoting –Force* ein. Der Befehl aktiviert auch die Ausnahmen in der Windows-Firewall. Mit *Disable-PSRemoting –Force* können Sie die Remoteverwaltung eines Servers über die PowerShell wieder deaktivieren.

In Remote-PowerShell-Sitzungen verwenden Sie die gleichen Cmdlets wie auf den lokalen Servern. Allerdings erlauben nicht alle Cmdlets eine Remoteverwaltung. Sie sehen die kompatiblen Cmdlets am schnellsten, indem Sie überprüfen, ob das Cmdlet die Option *–ComputerName* unterstützt. Mit dem Befehl *Get-Help * –Parameter ComputerName* lassen Sie sich eine Liste aller dieser Cmdlets anzeigen.

Rufen Sie eine Hilfe zu Cmdlets auf, kann sich die PowerShell selbstständig aktualisieren. Die PowerShell bietet seit der Version 3.0 das neue Cmdlet *Update-Help*, welches die Hilfedateien der PowerShell aktualisieren kann.

Dazu muss der Server über eine Internetverbindung verfügen. Der Befehl ruft die Hilfe direkt aus dem Internet ab. Ebenfalls über die PowerShell aufrufbar ist das Cmdlet *Show-Command*. Dieses blendet ein neues Fenster mit allen Befehlen ein, die in der PowerShell verfügbar sind. Sie können im Fenster nach Befehlen suchen und sich eine Hilfe zum Befehl anzeigen lassen sowie Beispiele.

Sie können in der PowerShell auch eine Remotesitzung auf einem Server starten. Am besten verwenden Sie dazu die PowerShell Integrated Scripting Environment (ISE). Diese ist bereits aktiviert. Nach dem Start können Sie eine Verbindung mit *Datei/Neue Remote-PowerShell-Registerkarte* öffnen. Hier geben Sie einen Servernamen und einen Benutzernamen ein, mit dem Sie sich verbinden wollen. Mehr zu diesem Thema erfahren Sie in Kapitel 40.

Active Directory mit Windows Server 2012 R2 installieren und verstehen

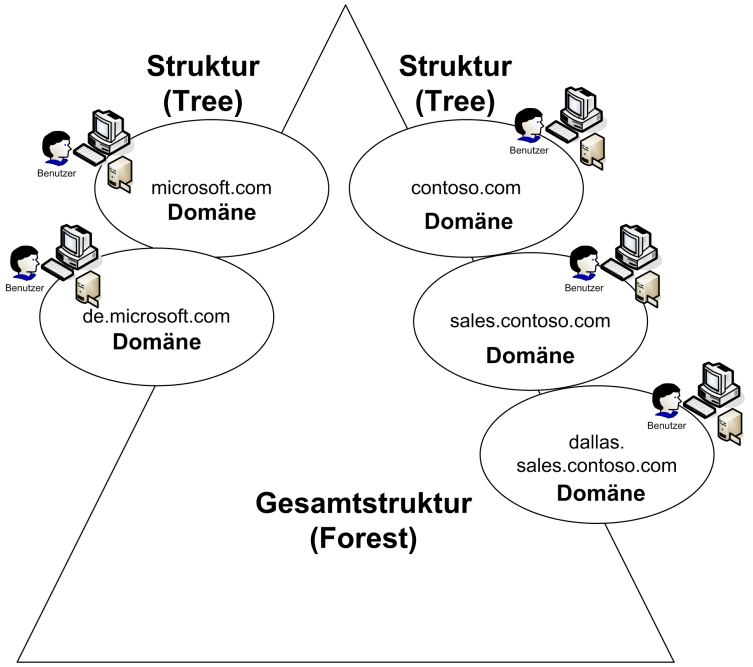
In diesem Abschnitt zeigen wir Ihnen, wie Active Directory grundsätzlich aufgebaut ist und wie Sie eine Testumgebung mit einer neuen Domäne installieren. Im Kapitel 11 erweitern wir diese Erläuterungen noch.

Aufbau von Active Directory

Zwei Begriffe aus dem klassischen Domänenmodell finden sich in Active Directory immer wieder: Es gibt Active Directory-Domänen und Domänencontroller. Die Domäne ist die grundlegende Strukturierungseinheit. Die Domänencontroller übernehmen die Verwaltung der Ordnerinformationen 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.

Active Directory kann aus mehreren selbstständigen Domänen bestehen, die zu einer gemeinsamen Organisation gehören. Alle verbundenen Domänen von Active Directory teilen sich eine Datenbank und ein Schema. Diese Domänen bilden eine Gesamtstruktur, im Englischen auch Forest genannt. Ein Forest ist die Grenze des Verzeichnisdiensts eines Unternehmens, in dem einheitliche Berechtigungen vergeben und delegiert werden können.

Abbildg. 10.9 Aufbau einer Active Directory-Gesamtstruktur



Jede Domäne in Active Directory ist eine eigene Partition im Ordner, die automatisch angelegt wird. Jede Partition wird von unterschiedlichen Domänencontrollern verwaltet. Diese Partitionierung erfolgt automatisch. Das Namensmodell von Active Directory orientiert sich stark am DNS. Domänen werden in 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.

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. Jedes Active Directory muss aus mindestens einer Struktur bestehen. Der ersten Domäne von 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 Rootdomäne der Gesamtstruktur. Wenn Sie ein Active Directory mit nur einer Domäne planen, bildet diese Domäne die Gesamtstruktur, die erste und einzige Struktur und die Rootdomäne von Active Directory. Die Domänen einer Struktur (Tree) teilen sich einen sogenannten Namensraum.

Im Beispiel von Abbildung 10.9 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 (Childdomänen genannt) haben, die wiederum wieder Childdomänen beinhalten können. Alle Domänen eines Namensraums werden als eigenständige Struktur bezeichnet.

Childdomänen sind wie die übergeordneten Domänen vollkommen eigenständig, teilen sich jedoch einen Namensraum und eine Active Directory-Gesamtstruktur. Sie bilden jeweils eigene Partitionen in Active Directory, die durch getrennte Domänencontroller verwaltet werden. Jede Domäne kann unterschiedliche Organisationseinheiten beinhalten. Organisationseinheiten können Sie sich wie Ordner im Explorer vorstellen, in denen Dateien liegen.

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. Organisationseinheiten sind die kleinsten Container in Active Directory. Eine Organisationseinheit kann mehrere Unterorganisationseinheiten beinhalten.

In 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 von Active Directorys
- **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.

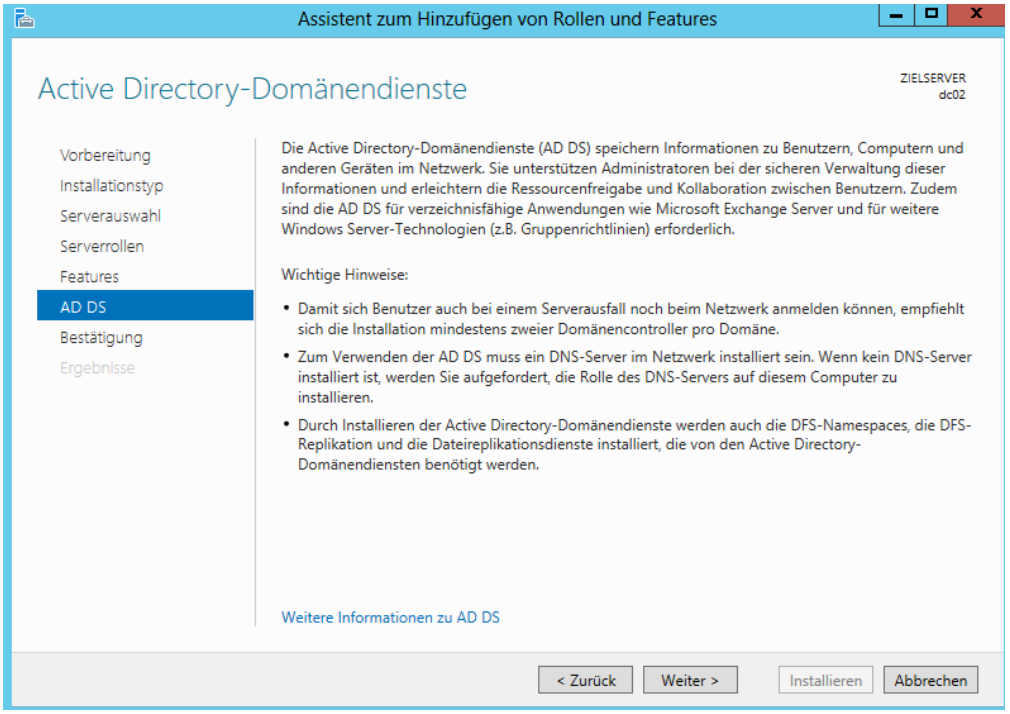
Der wichtigste Container in Active Directory ist die Domäne. Sie ist die logische Struktur, in der das Unternehmen abgebildet ist. Gleichzeitig hat eine Domäne Auswirkung auf die physische Speicherung von Informationen: Die Domäne stellt die Grenze dar, innerhalb der Informationen gemeinsam verwaltet werden. Der erste Schritt in der Planung von Active Directory ist daher die Gestaltung von Domänen.

Installieren einer neuen Gesamtstruktur

Im nächsten Abschnitt zeigen wir Ihnen in einer Schritt-für-Schritt-Anleitung, wie Sie Active Directory in Windows Server 2012 R2 installieren, zum Beispiel für eine Testumgebung. Mit Windows Server 2012 R2 hat Microsoft die Installation von Active Directory angepasst. Der Assistent Dcpromo ist nicht mehr verfügbar, dafür lassen sich Domänencontroller jetzt leichter über die PowerShell installieren. Aber auch im neuen Server-Manager können Sie eine Domäne installieren. Dazu blendet das neue Serversystem weniger Fenster ein, um ungeübten Administratoren die Installation zu vereinfachen

Um sich eine Testumgebung mit Active Directory in Windows Server 2012 R2 zu installieren, sind nach der Installation zunächst nur wenige Schritte notwendig. Im folgenden Kapitel 11 gehen wir ausführlicher auf die einzelnen Schritte der Installation von Active Directory ein.

Abbildg. 10.10 Installieren von Active Directory auf einem neuen Server



HINWEIS Microsoft hat die Schemaänderungen, die für die Installation von Active Directory notwendig sind, in den Assistenten zur Installation von Active Directory integriert.

Sie können Adprep von der Windows Server 2012 R2-DVD, aber auch weiterhin getrennt von der eigentlichen Installation von Windows Server 2012 R2 durchführen. Die Ausführung ist auch über das Netzwerk durchführbar und lässt sich ebenfalls von Servern mit Windows Server 2008 x64/2008 R2/2012 starten. Sie können das Tool allerdings nicht auf Servern mit Windows Server 2003 starten.

Nach der Installation ändern Sie zunächst den Namen des Servers ab. Starten Sie den Server-Manager und klicken Sie auf *Lokaler Server*. Anschließend klicken Sie auf der rechten Seite auf den Computernamen des Servers und dann auf die Schaltfläche *Ändern*. Tragen Sie den Namen des Servers ein, zum Beispiel *dc02*. Bestätigen Sie die Änderung mit *OK* und lassen Sie den Server neu starten.

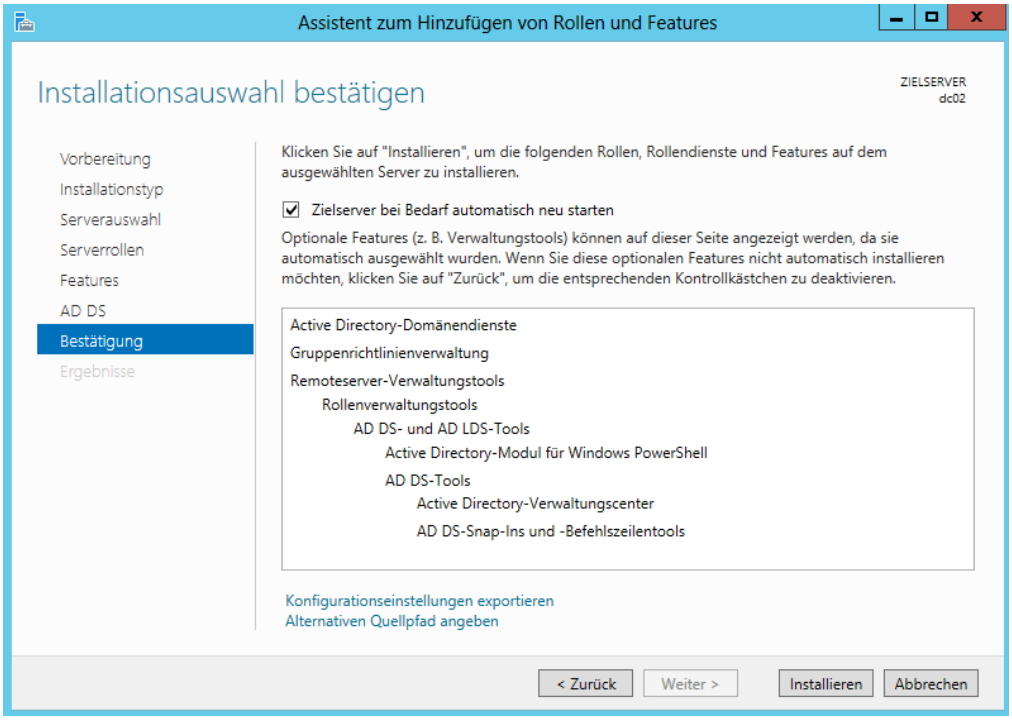
Nach dem Neustart klicken Sie mit der rechten Maustaste auf das Netzwerksymbol im unteren Bereich und dann auf *Netzwerk- und Freigabecenter* öffnen. Anschließend klicken Sie auf den Link *Adaptereinstellungen ändern* links im Fenster. Rufen Sie die Eigenschaften der Netzwerkverbindung auf und dann die Eigenschaften von *Internetprotokoll Version 4*.

Tragen Sie eine statische IP-Adresse ein und aktivieren Sie die Option *Folgende DNS-Serveradressen verwenden*. Tragen Sie als IP-Adresse die IP-Adresse des Servers ein, da in Active Directory die Domänencontroller auch DNS-Server sein sollten (siehe Kapitel 6 und 25). Installieren Sie den Server als zusätzlichen Domänencontroller, tragen Sie als DNS-Server die IP-Adresse eines bereits vorhandenen DNS-Servers ein.

Schließen Sie alle Fenster und öffnen Sie den Server-Manager. Klicken Sie dann auf *Verwalten* im oberen Bereich und wählen Sie *Rollen und Features hinzufügen* aus. Bestätigen Sie die Startseite und wählen Sie dann *Rollenbasierte oder featurebasierte Installation* aus. Wählen Sie den lokalen Server aus der Liste im nächsten Fenster aus.

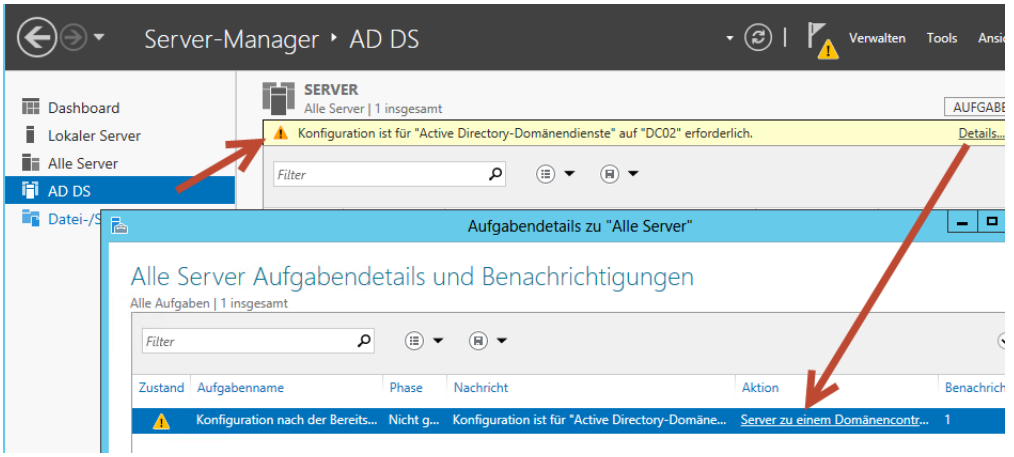
Wählen Sie die Rolle *Active Directory-Domänendienste* aus und bestätigen Sie dann die Schaltfläche *Features hinzufügen*, um die notwendigen Erweiterungen zum Server hinzuzufügen. Bestätigen Sie die nächsten Fenster und aktivieren Sie dann im Fenster *Installationsauswahl bestätigen* die Option *Zielserver bei Bedarf automatisch* neu starten. Klicken Sie danach auf *Installieren*.

Abbildg. 10.11 Starten der Active Directory-Installation



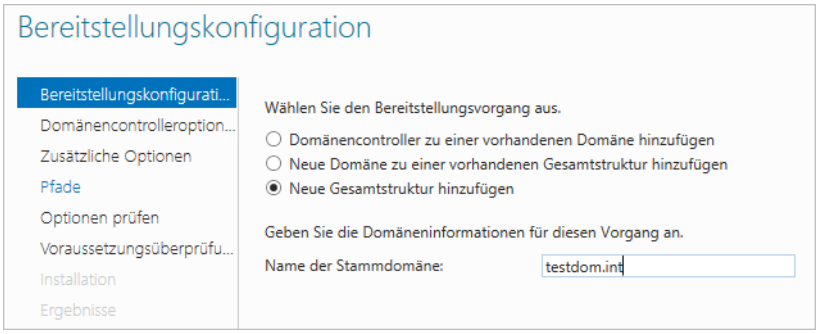
Nach der Installation klicken Sie im Server-Manager auf *AD DS* und dann im oberen Bereich bei *Konfiguration ist für "Active Directory-Domänendienste" auf "XXX" erforderlich* auf den Link *Details*. Wählen Sie in den Aufgabendetails in der Spalte *Aktion* den Link *Server zu einem Domänencontroller heraufstufen*.

Abbildg. 10.12 Starten der Heraufstufung eines Domänencontrollers



Aktivieren Sie dann die Option *Neue Gesamtstruktur hinzufügen* und geben Sie den DNS-Namen der Domäne an, zum Beispiel *testdom.int*.

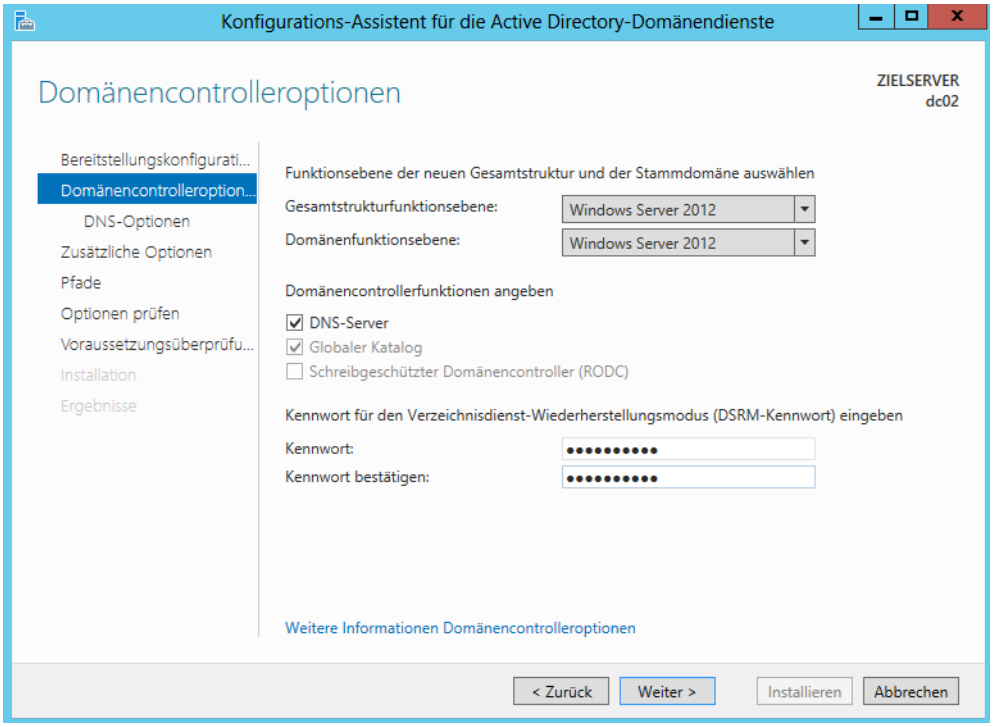
Abbildg. 10.13 Erstellen einer neuen Gesamtstruktur



Auf der nächsten Seite belassen Sie die Standardeinstellungen und legen die Funktionsebene für Gesamtstruktur und Domäne fest. Geben Sie ein Kennwort für den Wiederherstellungsmodus ein. Der erste Domänencontroller muss globaler Katalog sein und darf nicht als schreibgeschützter Domänencontroller betrieben werden. Daher sind die Optionen bereits vorgewählt und lassen sich nicht ändern.

Bestätigen Sie das nächste Fenster *DNS-Optionen*. Dieses besagt nur, dass noch kein DNS-Server für die Gesamtstruktur vorhanden ist und daher keine Delegierung eingerichtet werden kann. Geben Sie danach den NetBIOS-Namen der Domäne an. Im nächsten Kapitel gehen wir genauer auf die einzelnen Punkte während der Einrichtung ein.

Abbildg. 10.14 Konfigurieren der Optionen für einen neuen Domänencontroller



HINWEIS Sie können Domänencontroller mit Windows Server 2012 R2 auch in Gesamtstrukturen im Betriebsmodus Windows Server 2012 betreiben. Die Funktionsebene Windows Server 2003 ist aus Windows Server 2012 R2 entfernt worden.

Die nächsten Fenster müssen Sie nur bestätigen. Auf der Seite *Optionen prüfen* können Sie mit *Skript anzeigen* die Befehle anzeigen lassen, um den gleichen Vorgang in der PowerShell durchführen zu können. Bestätigen Sie die restlichen Fenster und klicken Sie dann auf *Installieren*. Ignorieren Sie die Warnungen. Nach der Installation steht der Domänencontroller zur Verfügung.

Abbildg. 10.15 Beispiel eines Skripts, um eine Domäne in der PowerShell zu installieren

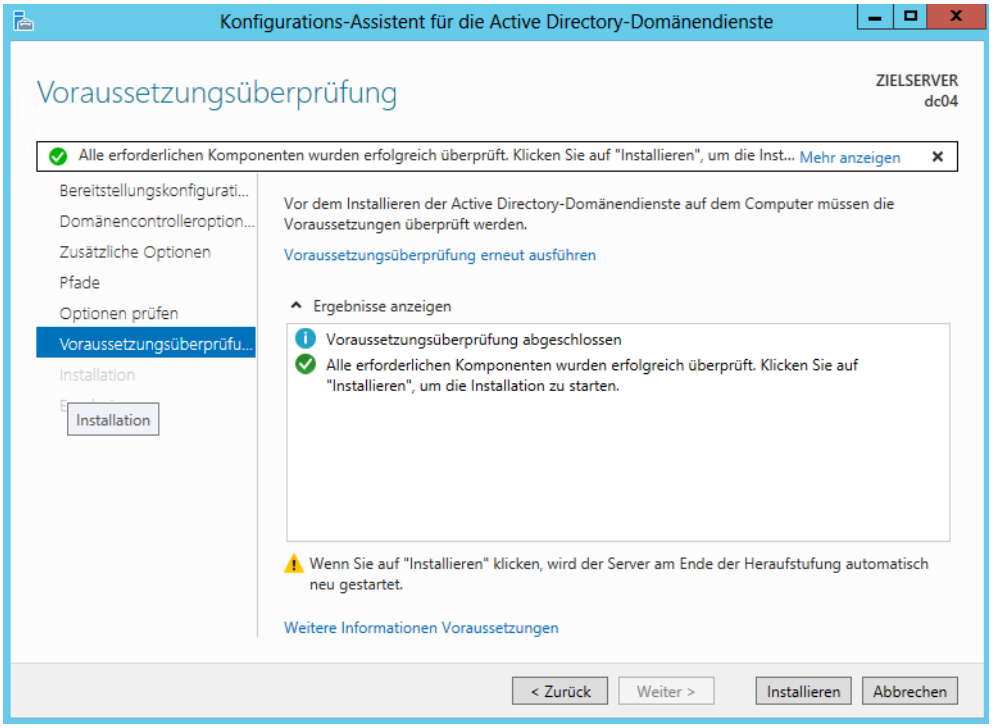
tmpFE56.tmp - Editor

Datei Bearbeiten Format Ansicht ?

```
#
# Windows PowerShell-Skript für AD DS-Bereitstellung
#

Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "Win2012" `
-DomainName "testdom.int" `
-DomainNetbiosName "TESTDOM" `
-ForestMode "Win2012" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

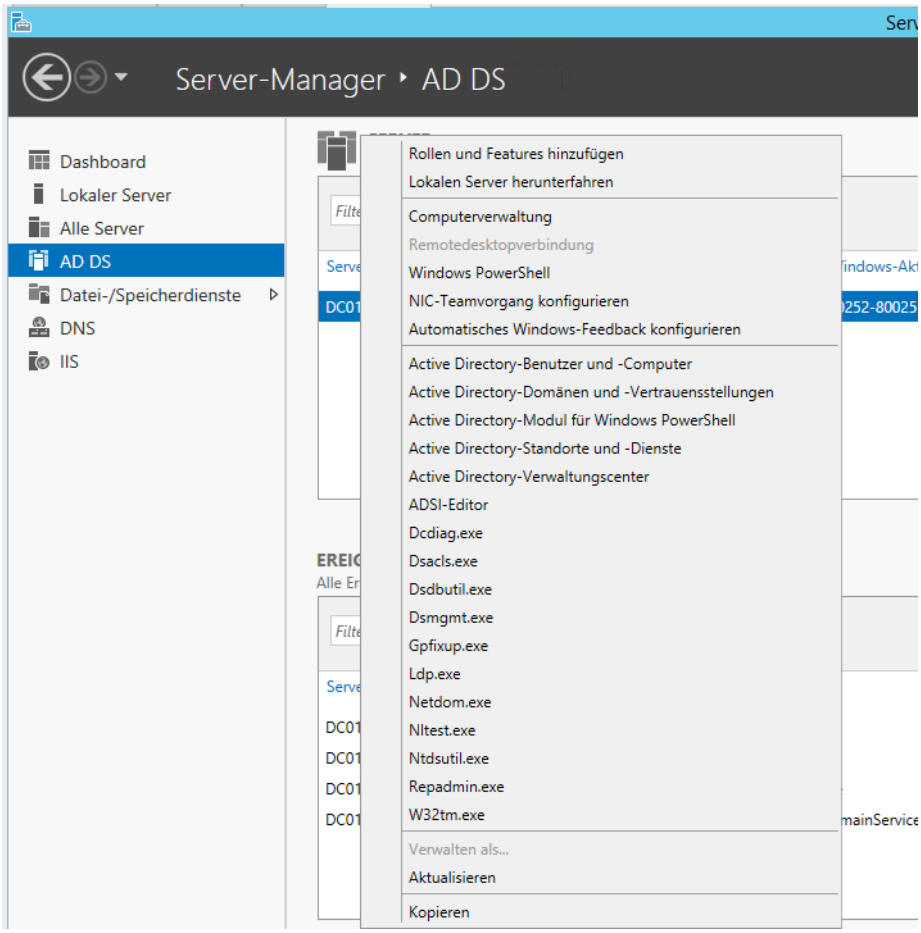
TIPP Der Einrichtungs-Assistent von Active Directory überprüft vor der Einrichtung von Active Directory, ob Probleme beim Heraufstufen zu erwarten sind. Sie erhalten daraufhin Warnungen und Fehlerhinweise, bevor der Assistent startet.

Abbildg. 10.16 Der Assistent überprüft, ob der Server fehlerfrei heraufgestuft werden kann



Nach der Installation finden Sie im *Tools*-Menü des Server-Managers die verschiedenen Verwaltungswerkzeuge von Active Directory aufgelistet, zum Beispiel das Active Directory-Verwaltungscenter. Im Bereich *AD DS* des Server-Managers sind die Domänencontroller und deren Warnungen und Fehler zu sehen. Über das Kontextmenü des Servers im Bereich *AD DS* sind ebenfalls die Befehle für Active Directory zu erreichen.

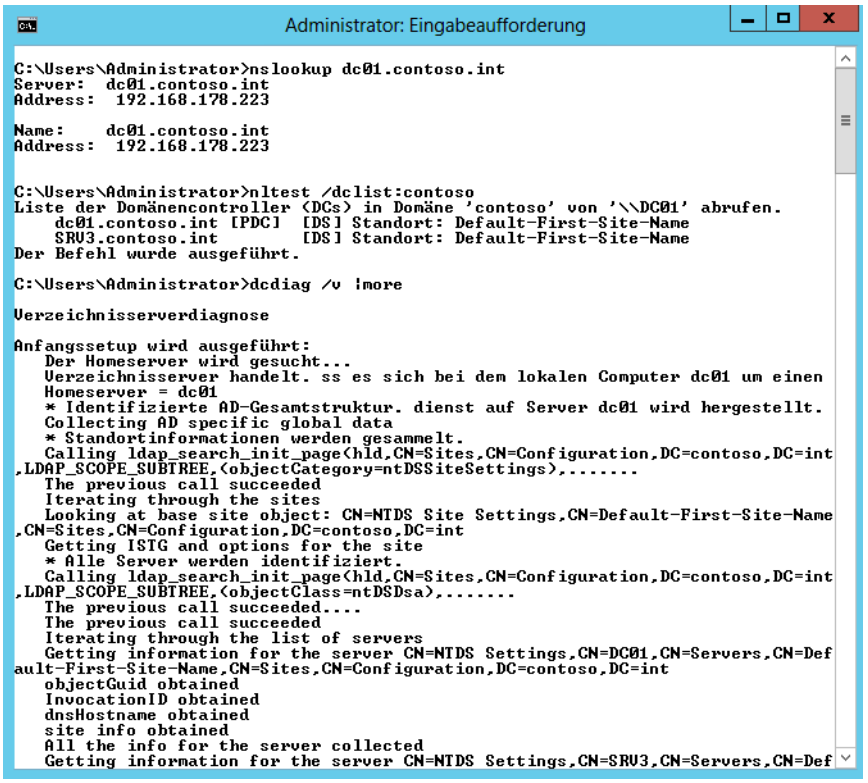
Abbildg. 10.17 Domänencontroller im Server-Manager verwalten



Um Active Directory zu testen, starten Sie eine Eingabeaufforderung, zum Beispiel durch Eingabe von *cmd* auf der Startseite. Die Startseite starten Sie mit der ⊞-Taste oder einem Klick mit der Maus unten links im Bildschirm. Geben Sie dann *dcdiag* ein.

Mit *nltest /dclist:<NetBIOS-Domänennamen>* lassen Sie sich den Namen des Domänencontrollers anzeigen, mit *nslookup <Vollständiger Name des DC>* muss der Name und die IP-Adresse verfügbar sein. Mehr zu diesem Thema erfahren Sie auch in Kapitel 6.

Abbildg. 10.18 Active Directory testen



TIPP Unter Windows Server 2012 R2 ist es möglich, den Dienst 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. 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 Dienststeuerung. Diese können Sie ausführen, indem Sie *services.msc* auf der Startseite eintippen. Der Dienst kann auch, wie alle anderen Dienste, über die Eingabeaufforderung mit *net stop ntds* gestoppt und mit *net start ntds* wieder gestartet werden.

Active Directory remote mit der PowerShell verwalten

Mit Windows Server 2012 R2 haben Sie die Möglichkeit, von einer lokalen PowerShell-Sitzung von Arbeitsstationen aus remote auf Domänencontroller zuzugreifen, um Active Directory zu verwalten. Das ist oftmals wesentlich bequemer und effizienter als mit Remotedesktopsitzungen.

Um Server im Netzwerk über Arbeitsstationen mit Windows 8.1 zu verwalten, sind die Remoteserver-Verwaltungstools notwendig. In Kapitel 3 zeigen wir Ihnen, wie Sie diese installieren und betreiben. Damit sich Active Directory remote über die PowerShell verwalten lässt, müssen Sie *Rollenverwaltungstools/AD DS-/AD LDS-Tools/Active Directory-Modul für Windows PowerShell* installiert haben. Die Installation überprüfen Sie, wenn Sie *optionalfeatures* auf der Startseite auf dem Windows 8-Compuer eingeben.

Zusätzlich ist noch .NET Framework 3.5.1 notwendig. Soll Active Directory von einem Server aus verwaltet werden, der kein Domänencontroller ist, lassen sich die Verwaltungstools von Active Directory direkt über den Server-Manager installieren. Die Installation erfolgt im Server-Manager über die Auswahl von *Remoteserver-Verwaltungstools/Rollenverwaltungstools/AD DS- und AD LDS-Tools/Active Directory-Modul für Windows PowerShell*.

Remote-PowerShell aktivieren und Verbindungsprobleme beheben

Damit sich ein Server in der PowerShell remote verwalten lässt, muss die Funktion auf dem Zielserver zunächst aktiviert werden. Dazu geben Sie in einer PowerShell-Sitzung auf dem Ziel-Server den Befehl *Enable-PSRemoting –Force* ein. Der Befehl richtet die entsprechenden Ausnahmen in der Firewall ein und aktiviert die notwendigen Funktionen. Rückgängig machen lässt sich der Vorgang mit *Disable-PSRemoting –Force*.

Abbildg. 10.19 Remote-PowerShell-Sitzungen aktivieren, deaktivieren und überprüfen

```
PS C:\Users\Administrator> Disable-PSRemoting -force
WARNUNG: Durch Deaktivieren der Sitzungskonfigurationen werden nicht alle Änderungen rü
 "Enable-PSRemoting" oder "Enable-PSSessionConfiguration" vorgenommen wurden. Möglicher
manuell rückgängig machen, indem Sie die folgenden Schritte ausführen:
    1. Beenden und deaktivieren Sie den WinRM-Dienst.
    2. Löschen Sie den Listener, der Anforderungen auf beliebigen IP-Adressen akzeptier
    3. Deaktivieren Sie die Firewallausnahmen für die WS-Verwaltungskommunikation.
    4. Setzen Sie den Wert von "LocalAccountTokenFilterPolicy" auf 0 zurück. Dadurch wi
Mitglieder der Gruppe "Administratoren" auf dem Computer eingeschränkt.
PS C:\Users\Administrator> Enable-PSRemoting -force
WinRM ist bereits zum Empfangen von Anforderungen auf diesem Computer konfiguriert.
WinRM ist bereits für die Remoteverwaltung auf diesem Computer eingerichtet.
PS C:\Users\Administrator> WinRM enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 192.168.178.223, ::1, fe80::100:7f:fffe%14, fe80::5efe:192
9ade:c2f1%12
```

Verbinden Sie sich von einem anderen Server oder von einer Arbeitsstation mit Active Directory oder mit Verwaltungstools für Serverdienste, verwendet die Konsole immer eine Remote-PowerShell-Sitzung für die Verwaltung. Alle Befehle werden als Cmdlet übertragen, die grafische Oberfläche ist in vielen Fällen nur ein Hilfsmittel. Damit die Verbindung über das Netzwerk funktioniert, verwendet der Server die Funktionen Windows Remote Management (WinRM) und Web Services for Management (WSMan). Durch die Remote-PowerShell-Sitzung überträgt der Client seine Befehle an den Server.

Sollte die Verbindung nicht funktionieren, geben Sie in der Eingabeaufforderung noch den Befehl *winrm enumerate winrm/config/listener* ein. Ein Listener mit dem Port 5985 muss aktiv und an alle IP-Adressen des Servers gebunden sein. Selbstverständlich darf der Port nicht durch eine Firewall blockiert werden. Standardmäßig schaltet Windows Server 2012 R2 den Port in der Windows-Firewall frei. Setzen Unternehmen eine weitere Firewall zwischen Client und Server ein, müssen Sie diesen Port durchlassen.

Innerhalb einer Active Directory-Gesamtstruktur sind keine Maßnahmen notwendig. Damit der Zugriff auch über Domänengrenzen hinweg oder von einer Arbeitsgruppe zu einer Domäne funktioniert, müssen Sie auf dem Zielserver noch die Computer eintragen, die auf den Server zugreifen dürfen. Dazu verwenden Sie den folgenden Befehl:

```
winrm set winrm/config/client @{TrustedHosts="<Alle Quellcomputer, durch Komma getrennt>"}
```

Cmdlets für die Remoteverwaltung und Abrufen der Hilfe

Nicht alle Cmdlets eignen sich für eine Remoteverwaltung von Servern. Sie können vor allem die Cmdlets nutzen, welche über die Option *–ComputerName* verfügen. Um sich alle Cmdlets anzeigen zu lassen, die diese Option unterstützen, also Server auch über das Netzwerk verwalten können, hilft der Befehl *Get-Help * –Parameter ComputerName*.

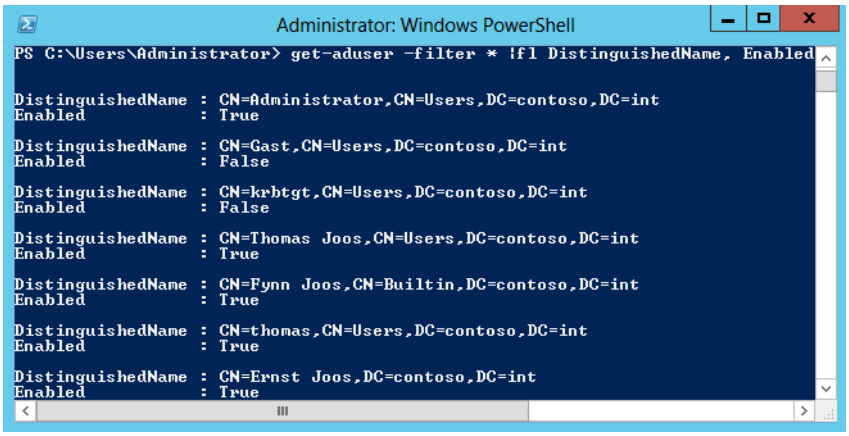
Wollen Sie ausführliche Hilfen anzeigen, bietet das *Get-Help*-Cmdlet noch die Möglichkeit, ausführliche Hilfen und Beispiele anzuzeigen, zum Beispiel mit den Optionen *–Examples*, *–Detailed* und *–Full*. Generell ist der Umgang mit der PowerShell nicht sehr kompliziert. Geben Sie *Get-Command* ein, sehen Sie alle Befehle, welche die Shell zur Verfügung stellt. Die PowerShell bietet eine ausführliche Hilfe an.

Haben Sie nur den Teil eines Befehls in Erinnerung, können Sie mit dem Platzhalter * arbeiten. Der Befehl *Get-Command *user* zeigt zum Beispiel alle Cmdlets an, deren Namen mit *user* enden. Ist der gesuchte Befehl nicht dabei, können Sie auch mehrere Platzhalter verwenden, zum Beispiel den Befehl *Get-Command *user**. Dieser Befehl zeigt alle Befehle an, in denen das Wort »user« vorkommt.

Wurde das gewünschte Cmdlet gefunden, unterstützt die PowerShell mit weiteren Möglichkeiten. Für nahezu alle Cmdlets gilt die Regel, dass diese in vier Arten vorliegen: Es gibt Cmdlets mit dem Präfix *New-*, um etwas zu erstellen, zum Beispiel *New-ADUser*. Das gleiche Cmdlet gibt es dann immer noch mit *Remove-*, um etwas zu löschen, zum Beispiel *Remove-ADUser*.

Wollen Sie das Objekt anpassen, gibt es das Präfix *Set-* zum Beispiel *Set-ADUser*. Als Letztes gibt es noch das Cmdlet *Get-*, zum Beispiel *Get-ADUser*, um Informationen zum Objekt abzurufen. Neben dieses Cmdlets gibt es natürlich noch viele andere, zum Beispiel *Start-* und *Stop*-Cmdlets oder *Export-* und *Import*-Cmdlets. Geben Sie nur diesen Befehl ein, passiert entweder überhaupt nichts, das Cmdlet zeigt alle Objekte an oder Sie werden nach der Identität des Objekts gefragt. So listet das Cmdlet *Get-ADUser –Filter** alle Benutzer der Organisation auf.

Abbildg. 10.20 Active Directory mit der PowerShell verwalten



Mit dem Befehl *Help <Cmdlet>* erhalten Sie eine Hilfe zum entsprechenden Cmdlet, zum Beispiel *Help New-ADUser*. Für viele Cmdlets gibt es noch die Option *Help <Cmdlet> –Detailed*. Dieser Befehl bietet noch mehr Informationen. Mit dem Befehl *Help <Cmdlet> –Examples* lassen sich Beispiele für den Befehl anzeigen. Auch das funktioniert für alle Befehle in der PowerShell. Ab PowerShell 3.0 hat Microsoft deutlich die Hilfefunktion erweitert.

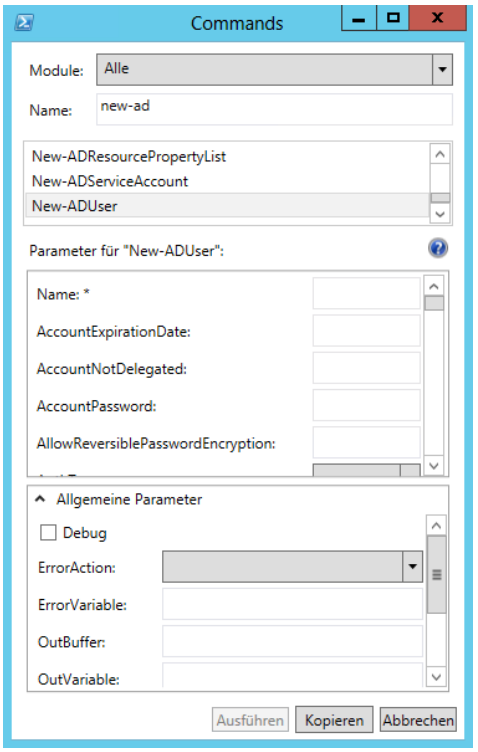
Rufen Sie eine Hilfe zu Cmdlets auf, kann sich die PowerShell selbstständig aktualisieren. Die PowerShell bietet das Cmdlet *Update-Help*, welches die Hilfedateien der PowerShell aktualisieren kann.

Dazu muss der Server über eine Internetverbindung verfügen. Der Befehl ruft die Hilfe direkt aus dem Internet ab. Ebenfalls eine interessante Funktion in der PowerShell ist das Cmdlet *Show-Command*. Dieses blendet ein neues Fenster mit allen Befehlen ein, die in der PowerShell verfügbar sind. Sie können im Fenster nach Befehlen suchen und sich eine Hilfe zum Befehl anzeigen lassen sowie Beispiele.

Mit *Get*-Cmdlets lassen Sie sich Informationen zu Objekten anzeigen. Die Option *|fl* formatiert die Ausgabe. Wollen Sie aber nicht alle Informationen, sondern nur einzelne Parameter anzeigen, können Sie diese nach der Option *|fl* anordnen. Wollen Sie zum Beispiel für Benutzer nur den *DistinguishedName* und den Status anzeigen lassen, verwenden Sie den Befehl *Get-ADUser –Filter * |fl DistinguishedName, Enabled*. Groß- und Kleinschreibung spielen für die Cmdlets keine Rolle.

Sie können in der PowerShell auch eine Remotesitzung auf einem Server starten. Am besten verwenden Sie dazu die PowerShell Integrated Scripting Environment (ISE). Diese ist in Windows 8 bereits aktiviert, muss teilweise in Windows 7 als Windows-Feature nachträglich aktiviert werden. Nach dem Start können Sie eine Verbindung mit *Datei/Neue Remote-PowerShell-Registerkarte öffnen*. Hier geben Sie einen Servernamen und einen Benutzernamen ein, mit dem Sie sich verbinden wollen.

Abbildg. 10.21 Anzeigen und Suchen von Cmdlets



Um eine Remotesitzung in der normalen PowerShell aufzubauen, verwenden Sie das Cmdlet *New-PSSession*. Mit *Enter-PSSession <Servername>* bauen Sie eine Verbindung auf. Mit *Exit-Session* beenden Sie diese Sitzung wieder. Neu ist die Möglichkeit, Sitzungen zu unterbrechen und neu aufzubauen. Bei unterbrochenen Sitzungen laufen die Cmdlets weiter, auch wenn Sie sich vom Server getrennt haben. Dazu nutzen Sie die neuen Cmdlets *Disconnect-PSSession*, *Connect-PSSession* und *Receive-PSSession*.

TIPP Über die normale PowerShell starten Sie die PowerShell ISE, indem Sie den Befehl *ise* eingeben.

Die PowerShell erlaubt auch die Ausführung von Befehlen, wie von der Eingabeaufforderung gewohnt. Der Vorteil der Ausführung in der PowerShell ist, dass sich die Ausgabe auch filtern lässt. Geben Administratoren zum Beispiel *ipconfig /all* ein, erhalten sie die gleichen Informationen wie in der Eingabeaufforderung. Es sind also keine zwei Konsolen nebeneinander notwendig. Soll die Ausgabe gefiltert werden, hilft die Option *Select-String –Pattern "<Text>"*, zum Beispiel *ipconfig /all | select-string –pattern "gateway"*. Auf diesem Weg lassen sich Informationen wesentlich gezielter auslesen.

Durch die zahlreichen neuen Cmdlets in der PowerShell erhalten Sie in der PowerShell für Anmeldeskripts deutlich mehr Möglichkeiten. In der neuen Version lassen sich jetzt auch Netzlaufwerke in Windows verbinden. Dazu verwenden Sie das Cmdlet *New-PSDrive*. Dabei hilft die neue Option *-Persist*. Alle Optionen des Cmdlets sind über *Get-Help New-PSDrive –Detailed* verfügbar.

Verwalten der Betriebsmasterrollen von Domänencontrollern

In Active Directory sind zunächst alle Domänencontroller gleichberechtigt. Allerdings gibt es fünf unterschiedliche Rollen, die ein Domänencontroller annehmen kann und die seine zentrale Aufgabe in Active Directory steuern. Die verschiedenen Rollen werden als Flexible Single Master Operators (FSMOs) bezeichnet. Jede dieser Rollen ist entweder einmalig pro Domäne (PDC-Emulator, Infrastrukturmaster, RID-Master) oder einmalig pro Gesamtstruktur (Schemamaster, Domänennamenmaster). Fällt eine dieser Rollen aus, kommt es in Active Directory zu Fehlfunktionen.

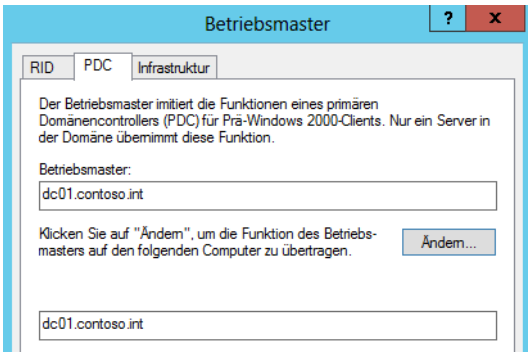
PDC-Emulator verwalten

Die Rolle des PDC-Emulators gibt es in jeder Active Directory-Domäne ein Mal. 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 nicht mehr verwaltet werden, da spezielle Verwaltungskonsolen wie die Gruppenrichtlinien-Verwaltungskonsole 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. Der PDC-Master ist auch beim Klonen virtueller Domänencontroller beteiligt (siehe Kapitel 11). Ihn selbst können Sie nicht klonen, andere Domänencontroller schon.

Außerdem ist der PDC-Emulator der Zeitserver einer Domäne. Alle hier beschriebenen Funktionen sind gestört, wenn der PDC-Emulator nicht mehr zur Verfügung steht.

Wollen Sie überprüfen, welcher Domänencontroller die Rolle des PDC-Emulators in der Domäne verwaltet, öffnen Sie das Snap-In *Active Directory-Benutzer und -Computer* im Server-Manager oder über *dsa.msc* auf der Startseite. Mit einem Klick mit der rechten Maustaste auf die Domäne im Snap-In und der Auswahl von *Betriebsmaster* im Kontextmenü öffnet sich ein neues Fenster. Hier sind die FSMOs der Domäne zu sehen.

Abbildg. 10.22 Verwalten der Betriebsmasterrolle in Active Directory



Auf der Registerkarte *PDC* ist der aktuelle PDC-Emulator der Domäne zu sehen. Sie können sich den aktuellen PDC-Emulator auch mithilfe des Befehls *dsquery server –hasfsmo pdc* in der Eingabeaufforderung anzeigen lassen oder den PDC-Master mit dem folgenden Cmdlet:

```
Get-ADComputer(Get-ADDomainController –Discover –Service "PrimaryDC").Name –Property * |
Format-List DNSHostname,OperatingSystem,OperatingSystemVersion
```

RID-Master – Neue Objekte in der Domäne aufnehmen

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 Bezeichner (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, 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. Auf der Registerkarte *RID* wird der RID-Master der Domäne angezeigt.

Der Befehl *dsquery server –hasfsmo rid* zeigt den Master in der Eingabeaufforderung an. Außerdem können Sie sich die erfolgreiche Verbindung und den Status des RID-Pools anzeigen lassen. Geben Sie in der Eingabeaufforderung den Befehl *dcdiag /v /test:ridmanager* ein. Suchen Sie dann den Bereich *Starting test: RidManager*. Hier sehen Sie, ob der Domänencontroller fehlerfrei eine Verbindung zum RID-Master aufbauen kann. Tritt an dieser Stelle ein Fehler auf, sollten Sie am besten den RID-Master auf einen anderen Server transferieren oder verschieben.

Abbildg. 10.23 Testen des RID-Managers mit Dcdiag

```
Starting test: RidManager
   * Available RID Pool for the Domain is 3101 to 1073741823
   * dc01.contoso.int is the RID Master
   * DsBind with RID Master was successful
   * rIDAllocationPool is 1101 to 1600
   * rIDPreviousAllocationPool is 1101 to 1600
   * rIDNextRID: 1120
```

Die Security-ID (SID) von Domänencomputer ist in Domänen immer einzigartig und ein wichtiger Punkt bei der Bereitstellung von Windows beziehungsweise dem Überprüfen von Rechten. In manchen Fällen, vor allem beim Klonen, kann es passieren, dass doppelte SIDs im Netzwerk vorhanden sind.

Hier hilft das Sysinternals-Tool PsGetSid (*http://technet.microsoft.com/de-de/sysinternals/bb897417* [Ms179-K10-01]), welches in der Eingabeaufforderung die SID von Computern anzeigen kann. Sie müssen dazu lediglich *psgetsid* eingeben. PsGetSid liest die SID von Computern ohne große Umwege aus und funktioniert auch im Netzwerk. Das heißt, Sie können mit dem Tool auch die SIDs von Remotecomputern auslesen. Mit *PsGetSid* lassen sich zusätzlich auch die SIDs von Benutzerkonten sowie zu Namen auslesen. Wollen Sie die SID eines Computers anzeigen, geben Sie den Namen als Argument an. Dies funktioniert auch für Benutzernamen. Um die SID zu einem Namen zu übersetzen, geben Sie die SID als Argument ein.

Infrastrukturmaster – Auflösen von Gruppen über Domänen hinweg

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. Clients in der Domäne haben möglicherweise Schwierigkeiten dabei, Objekte in anderen Domänen zu finden, wenn die Rolle nicht mehr funktioniert. Der Infrastrukturmaster sollte nicht auf einem globalen Katalog positioniert werden.

Er wird außerdem für die Auflösung von Verteilergruppen verwendet, wenn Unternehmen Microsoft Exchange Server einsetzen, da auch an dieser Stelle eine Gruppe Mitglieder aus verschiedenen Domänen der Gesamtstruktur enthalten kann. Auf der Registerkarte *Infrastruktur* ist dieser zu sehen oder in der Eingabeaufforderung mit *dsquery server –hasfsmo infr*.

Schemamaster – Active Directory erweitern

Active Directory verfügt über ein erweiterbares Schema. Dieses bietet die Möglichkeit, zusätzliche Informationen im Ordner flexibel zu speichern. Diese Funktion wird beispielsweise von Exchange genutzt. Alle notwendigen Informationen zu einem E-Mail-Postfach werden in Active Directory abgelegt. Bei der Installation von Exchange 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 schlägt fehl. Der erste installierte Domänencontroller der ersten Domäne und Struktur einer Gesamtstruktur erhält die Rolle des Schemamasters. Der Schemamaster hat ansonsten keine Auswirkungen auf den laufenden Betrieb.

Damit der Schemamaster angezeigt werden kann, müssen Administratoren zunächst das Snap-In registrieren, welches das Schema anzeigt. Aus Sicherheitsgründen wird dieses Snap-In zwar installiert, jedoch nicht angezeigt. Durch Eingabe des Befehls *regsvr32 schmmgmt.dll* in der Eingabeaufforderung wird die Konsole verfügbar gemacht.

Im Anschluss können Sie das Snap-In *Active Directory-Schema* in eine MMC über *Datei/Snap-In hinzufügen* integrieren. Mit einem Klick mit der rechten Maustaste auf das Menü *Active Directory-Schema* und der Auswahl von *Betriebsmaster* öffnet sich ein neues Fenster, in dem der Betriebsmaster angezeigt wird. Sie können mithilfe dieses Fensters später den Betriebsmaster auch auf einen anderen Domänencontroller verschieben. Dazu müssen Sie sich über das Kontextmenü von Active Directory-Schema mit dem Domänencontroller verbinden, auf den Sie die Rolle übertragen wollen. Auch den Schemamaster können Sie sich in der Eingabeaufforderung anzeigen lassen: *dsquery server –hasfsmo schema*.

Abbildg. 10.24 Anzeigen des Schemamasters einer Gesamtstruktur

Domänennamenmaster – Neue Domänen hinzufügen

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 im Kontextmenü den Eintrag *Betriebsmaster* aus, öffnet sich ein neues Fenster, in dem der Domänennamenmaster dieser Gesamtstruktur angezeigt wird. Auch den Domänennamenmaster können Sie sich in der Eingabeaufforderung anzeigen lassen: *dsquery server –hasfsmo name*.

Der globale Katalog

An jedem Standort in 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.

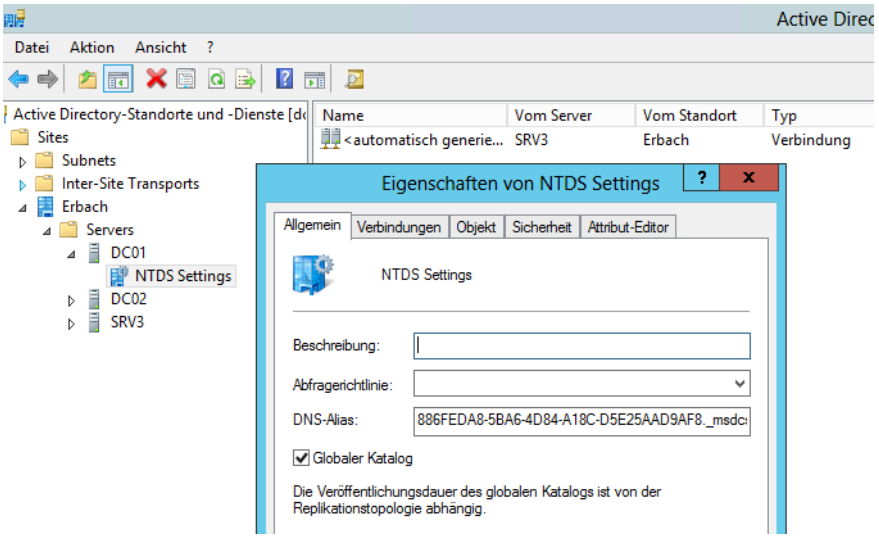
Dem globalen Katalog kommt in einer Active Directory-Domäne eine besondere Bedeutung zu. Er enthält einen Index aller Domänen einer Gesamtstruktur. Aus diesem Grund wird er von Serverdiensten wie Exchange Server und Suchanfragen verwendet, wenn Objekte aus anderen Domänen Zugriff auf eine Ressource der 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 Sie sich langsamer 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. In 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 Menü *Tools* im 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. 10.25 Festlegen eines globalen Katalogs



Vor allem bei Unternehmen mit mehreren Niederlassungen, vielen Domänencontrollern und zahlreichen globalen Katalogservern besteht die Notwendigkeit, sicherzustellen, dass die globalen Kataloge korrekt funktionieren. Alle globalen Katalogserver werden als SRV-Records in der Active Directory-Zone im DNS registriert.

Um sich die globalen Katalogserver anzeigen zu lassen, öffnen Sie das Snap-In *DNS* und navigieren zu der DNS-Zone der Rootdomäne in der Gesamtstruktur. Klicken Sie mit der Maus auf die *_tcp*-Zone. In dieser Zone werden Ihnen alle globalen Katalogserver angezeigt. Die SRV-Records dieser Server verweisen auf den Port 3268.

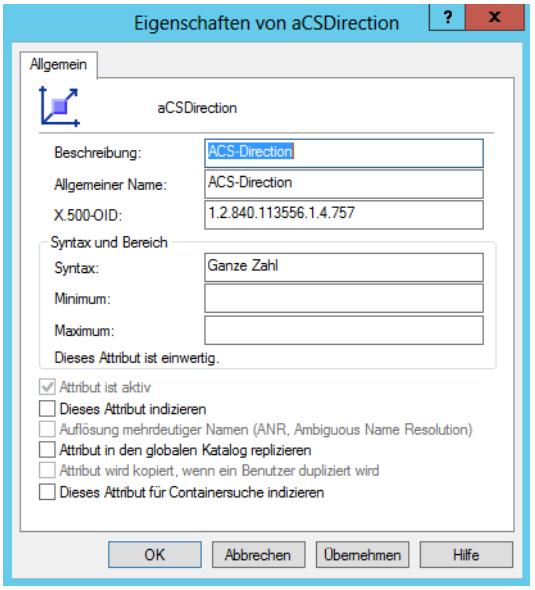
Hinzufügen von Attributen für den globalen Katalog

Microsoft hat vordefiniert, welche Attribute im globalen Katalog gehalten werden. Wenn Active Directory erweitert wird, kann es erforderlich werden, weitere Attribute in den Katalog aufzunehmen, nach denen häufig von Anwendern oder Anwendungen gesucht wird. Diese Anpassung kann über das Snap-In *Active Directory-Schema* erfolgen. Da durch die Modifizierung dieser Einstellungen Änderungen am Schema vorgenommen werden, dürfen Anpassungen nur durch die *Schema-Admins* vorgenommen werden. In diese Gruppe müssen die Administratoren explizit aufgenommen werden. Fehler bei der Verwaltung des Schemas können schwerwiegende Folgen haben. Daher muss gut überlegt werden, welche Administratoren in diese Gruppe aufgenommen werden und damit die Berechtigung erhalten, Attribute in den globalen Katalog aufzunehmen.

Die Konfiguration erfolgt im Bereich *Attribute* des Schema-Snap-Ins. Bei den Eigenschaften eines Attributs können mehrere Optionen gesetzt werden. Zwei der Optionen sind von besonderer Bedeutung für die Effizienz von Zugriffen auf Active Directory:

- Mit *Dieses Attribut für Containersuche indizieren* wird festgelegt, dass auf den globalen Katalogservern eine Indexierung des Attributs erfolgt. Das ist sinnvoll, wenn das Attribut für Abfragen verwendet wird.
- Mit *Attribut in den globalen Katalog replizieren* wird konfiguriert, dass ein Attribut in den globalen Katalog aufgenommen wird

Abbildg. 10.26 Attribute in den globalen Katalog übernehmen



Verwaltung und Verteilung 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.

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 verschiedene Domänencontroller.

Empfehlungen zur Verteilung von Betriebsmastern

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
- 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

TIPP Um sich einen Überblick über alle Betriebsmaster einer Gesamtstruktur zu verschaffen, können Administratoren den Befehl *netdom query fsmo* in der Eingabeaufforderung aufrufen.

Übertragen eines Betriebsmasters

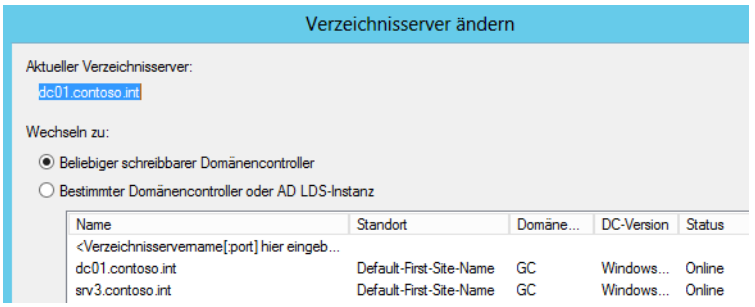
Auf Basis dieser Empfehlungen sollten Sie daher nach der Installation die Betriebsmaster entsprechend auf die einzelnen Domänencontroller der Domänen bzw. der Gesamtstruktur aufteilen. Betriebsmasterrollen können ohne Weiteres im laufenden Betrieb von einem auf den anderen Domänencontroller übertragen 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.

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:

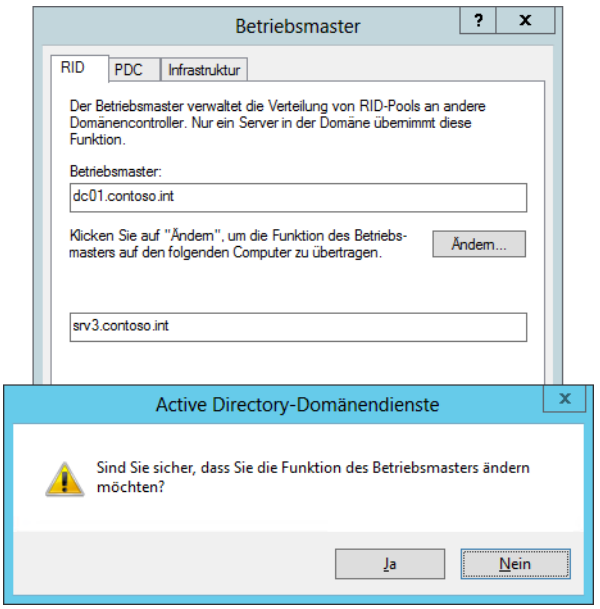
1. Klicken Sie mit der rechten Maustaste im Snap-In *Active Directory-Benutzer und -Computer* auf die Domäne und wählen Sie im Kontextmenü den Eintrag *Domänencontroller ändern* aus.
2. Wählen Sie im nächsten Fenster den Domänencontroller aus, auf den Sie die Rolle übertragen wollen, und bestätigen Sie die Eingabe.

Abbildg. 10.27 Ändern des Domänencontrollers in einer Verwaltungskonsole



3. Klicken Sie dann wieder mit der rechten Maustaste auf die Domäne und wählen Sie dieses Mal im Kontextmenü den Eintrag *Betriebsmaster* aus.
4. Auf den drei Registerkarten *PDC*, *RID* 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.
8. Auf dieselbe Weise gehen Sie bei der Übertragung der Betriebsmaster, Schemamaster und Domänennamenmaster vor. Diese beiden Betriebsmaster werden in der bekannten jeweiligen Verwaltungskonsole übertragen.

Abbildg. 10.28 Übertragen von Betriebsmastern



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 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 benötigt.

Voraussetzungen für die Besitzübernahme einer FSMO-Rolle

Wenn Sie eine FSMO-Rolle auf einen anderen Domänencontroller verschieben wollen, ohne dass der bisherige Rolleninhaber das mitbekommt, sollten Sie zwei Voraussetzungen berücksichtigen:

1. 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 ins das Netzwerk integrieren. Zunächst sollten Sie jedoch die Active Directory-Replikation für den Verschiebevorgang abwarten.
2. Verschieben Sie den Domänennamenmaster und den Schemamaster am besten wieder auf einen anderen Domänencontroller der Rootdomäne in der Gesamtstruktur, der auch die Rolle eines globalen Katalogs hat.

Durchführen der Besitzübernahme in der Eingabeaufforderung

Um die Betriebsmasterrolle auf einen anderen Domänencontroller zu verschieben, öffnen Sie eine Eingabeaufforderung. Gehen Sie danach in folgender Reihenfolge vor:

1. Nach dem Aufruf von *ntdsutil* 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. Wurde die Verbindung erfolgreich hergestellt, geben Sie den Befehl *quit* ein, um wieder zum vorherigen Menü *fsmo maintenance* zurückzukehren.
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* (Infrastrukturmaster) oder *domain 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.

TIPP 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 domain naming master*

Schreibgeschützte Domänencontroller (RODC)

Eine Möglichkeit, Domänencontroller in Niederlassungen abzusichern, 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 dieses neue Feature können Sie auch Domänencontroller in kleineren Niederlassungen betreiben, ohne dass das Sicherheitskonzept eines Unternehmens beeinträchtigt ist, weil die Domänencontroller in den Niederlassungen nicht geschützt sind.

Ein RODC schützt Active Directory davor, dass Kennwörter ausspioniert werden können. Ein RODC kennt zwar alle Objekte in 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. Der erste Domänencontroller muss allerdings ein normaler Domänencontroller sein. In diesem Fall repliziert sich der Domänencontroller von anderen Domänencontrollern, gibt aber selbst keine Änderungen weiter. Ein RODC nimmt keinerlei Änderungen an der Datenbank von Active Directory an, ein lesender Zugriff ist allerdings erlaubt. Schreibende Domänencontroller richten keine Replikationsverbindung zu RODCs ein, da eine Replikation nur von normalen Domänencontrollern (DCs) zu RODCs erfolgen kann. RODCs richten Replikationsverbindungen zu den schreibenden Domänencontroller ein, die Sie bei der Heraufstufung angeben.

Klicken Sie im Snap-In *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf die OU *Domain Controllers*, können Sie im zugehörigen Kontextmenü den Eintrag *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.

Ein RODC bietet ein vollständiges Active Directory, allerdings ohne gespeicherte Kennwörter. Dieser Ordner auf dem RODC ist, wie der Name schon sagt, schreibgeschützt (read only), also nur lesbar. Zwar kann auch ein RODC Kennwörter speichern, aber nur genau diejenigen, die ein Administ-

rator angibt. Bei der Verwendung von RODCs werden folgende Abläufe beim Anmelden eines Benutzers abgewickelt:

1. Ein Anwender meldet sich am Standort des RODCs an.
2. Der RODC überprüft, ob das Kennwort des Anwenders auf den Server repliziert wurde. Falls 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 Kerberos-Ticket zugewiesen.
5. Der RODC stellt dem Anwender jetzt noch ein eigenes Kerberos-Ticket 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.
7. Bei der nächsten Anmeldung dieses Anwenders beginnt der beschriebene Prozess von vorne.

TIPP 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 und es ist nur die lokale Anmeldung am Server möglich.

Installieren Sie auf einem RODC den DNS-Dienst (Domain Name System, DNS), wird dieser Server zum schreibgeschützten DNS-Server. Hier gelten die gleichen Einschränkungen für einen RODC. Ein schreibgeschützter DNS-Server nimmt nur Änderungen von normalen DNS-Servern entgegen und akzeptiert selbst keine Änderungen. Ein schreibgeschützter DNS-Server 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 Rückmeldung, 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 schreibgeschützten DNS Server repliziert.

Zusammenfassung

In diesem Kapitel haben Sie einen ersten Überblick zum Thema Active Directory in Windows Server 2012 R2 erhalten. Wir haben Ihnen gezeigt, welche neuen Funktionen es gibt und welche Vorteile diese haben. Außerdem sind wir in diesem Kapitel auf die Installation von Active Directory in einer Testdomäne eingegangen und haben erläutert, wie Sie die Betriebsmaster verwalten. Ebenfalls Bestandteil dieses Kapitels war die Verwaltung von Active Directory über die PowerShell.

Im nächsten Kapitel gehen wir ausführlicher auf die Installation von Active Directory ein.

Kapitel 11

Active Directory – Installation und Betrieb

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, wie Sie Active Directory mit Windows Server 2012 R2 aufbauen und verwalten. Wir gehen darauf ein, welche Vorbereitungen Sie für einen Domänencontroller treffen müssen und wie der beste Weg ist, um ein Active Directory zu installieren. Dieses Kapitel stellt die Grundlage für die nächsten Kapitel dar, in denen wir uns noch tiefgehender mit den Möglichkeiten von Active Directory beschäftigen. Damit Sie Windows Server 2012 R2 als Domänencontroller im Netzwerk einsetzen können, muss die Funktionsebene der Domäne und der Gesamtstruktur mindestens auf Windows Server 2012 gesetzt sein.

Im letzten Kapitel haben wir Ihnen bereits gezeigt, wie Sie Active Directory in einer Testumgebung installieren. In den folgenden Abschnitten bauen wir die Installationsmöglichkeiten weiter aus. Haben Sie den Computernamen festgelegt, sollten Sie die IP-Einstellungen des Servers anpassen, wie im letzten Kapitel erläutert.

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. Der nächste Schritt besteht darin, den DNS-Server für Active Directory vorzubereiten.

An dieser Stelle müssen Sie noch keinen alternativen DNS-Server eintragen. Der alternative DNS-Server in den IP-Einstellungen wird erst von einem Client befragt, wenn der bevorzugte DNS-Server nicht mehr antwortet. Auch eine fehlerhafte Auflösung akzeptiert ein DNS-Client als Antwort. Die IP-Einstellungen für Netzwerkverbindungen erreichen Sie im Netzwerk- und Freigabecenter über den Link *Adaptereinstellungen ändern*. Am schnellsten gelangen Sie zu dieser Konfiguration über die Eingabe von *ncpa.cpl* auf der Startseite.

HINWEIS In Kapitel 6 geben wir ebenfalls wichtige Hinweise für den Betrieb von Servern in Active Directory. Diese Anmerkungen gelten auch für Domänencontroller.

DNS für Active Directory installieren

Der Assistent für die Installation von Active Directory kann zwar auch im Rahmen der Einrichtung die DNS-Funktionalität installieren und einrichten. Für ein besseres Verständnis der Thematik allerdings ist diese Vorgehensweise nicht optimal, da Sie viele Einstellungen später nicht verstehen. Außerdem legt der Assistent keine Reverse-Lookupzone an, also die Möglichkeit, IP-Adressen nach Namen aufzulösen (siehe Kapitel 6).

Das ist zwar für den Betrieb von Active Directory nicht zwingend notwendig, allerdings verbessern Reverse-Lookupzonen die Namensauflösung und Sie erhalten bei Nslookup keine Fehlermeldungen. Um DNS zu installieren, starten Sie den Server-Manager und klicken auf *Verwalten/Rollen und Features hinzufügen*. Wählen Sie die Rolle *DNS-Server* aus. 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 von Windows Server 2012 R2 zunächst die DNS-Erweiterung zu installieren. Nach der Installation finden Sie das Verwaltungsprogramm für den DNS-Server im Server-Manager über den Bereich *Tools*.

Standardmäßig werden Sie mit dem lokal installierten DNS-Server verbunden. Erstellen Sie später eine einheitliche Managementkonsole (Microsoft Management Console, 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 *DNS*, können Sie sich mit zusätzlichen DNS-Servern verbinden.

Mit den Knoten *Forward-Lookupzonen* und *Reverse-Lookupzonen* legen Sie die Zonen an, die Active Directory für seinen Betrieb benötigt. Im Menü *Globale Protokolle/DNS-Ereignisse* finden Sie gefilterte Meldungen der Ereignisanzeige des Servers. Über *Bedingte Weiterleitungen* können Sie Anfragen zu bestimmten DNS-Zonen an fest definierte DNS-Server weiterleiten.

Erstellen der notwendigen DNS-Zonen für Active Directory

Der nächste Schritt zur Erstellung von Active Directory besteht in der Erstellung der neuen Zonen, welche die DNS-Domänen von Active Directory verwalten. Starten Sie dazu die DNS-Verwaltung.

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 *Forward-Lookupzonen* und wählen Sie im Kontextmenü den Eintrag *Neue Zone* aus. Es startet der Assistent zum Erstellen von neuen Zonen. Im nächsten Fenster können Sie festlegen, welche Art von Zone Sie erstellen wollen.

Wählen Sie die Option *Primäre Zone* aus. Beim Erstellen neuer Domänen in Active Directory werden ausschließlich primäre Domänen benötigt. Auf der nächsten Seite des Assistenten legen Sie den Namen der neuen Zone fest. Hier ist es extrem wichtig, dass Sie als Zonennamen exakt den Namen wählen, den Sie als DNS-Suffix des Servers eingetragen haben und den Sie als DNS-Namen der Active Directory-Domäne wählen wollen. Das DNS-Suffix des Namens legt der Installations-Assistent automatisch an, die Forward-Lookupzone auch. Das DNS-Suffix des Domänencontrollers wird später in diese Zone integriert und die erste Active Directory-Domäne speichert ihre SRV-Records ebenfalls in dieser Domäne.

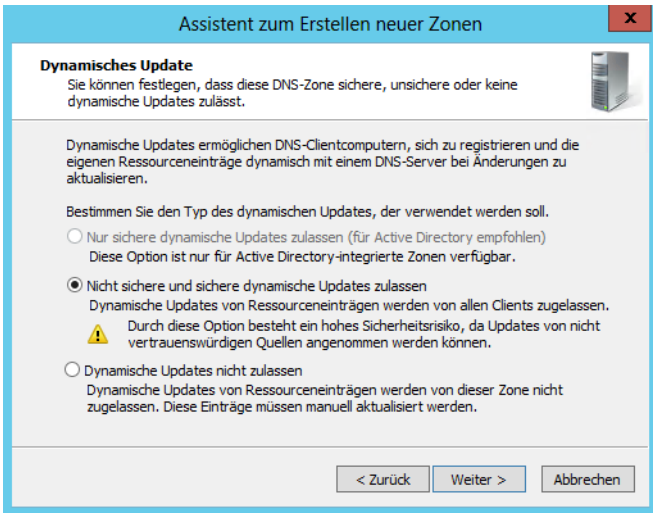
In diesem Beispiel lautet die Zone *test.int*. Im Anschluss erscheint das Fenster, in dem Sie die Erstellung einer neuen Datei für die Zone bestätigen müssen. Sie könnten an dieser Stelle den Namen der Datei zwar ändern, sollten ihn aber möglichst immer so belassen, wie er festgelegt wurde.

Im nächsten Fenster legen Sie die dynamischen Updates der DNS-Zone fest. DNS-Server unter Windows Server 2012 R2 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 Installations-Assistent von Active Directory muss in einer Zone Dutzende Einträge automatisch erstellen können. Aktivieren Sie daher im Fenster die Option *Nicht sichere und sichere dynamische Updates zulassen*. Sichere Updates können Sie nach der Erstellung von Active Directory konfigurieren. Vor der Installation ist diese Einstellung deaktiviert.

Im Anschluss erhalten Sie nochmals eine Zusammenfassung Ihrer Angaben aufgelistet. 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.

Abbildg. 11.1 Aktivieren der dynamischen Updates für eine Zone



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 von Active Directory nicht zwingend benötigt, gehören aber dennoch zu einer ordentlichen Namensauflösung im Netzwerk.

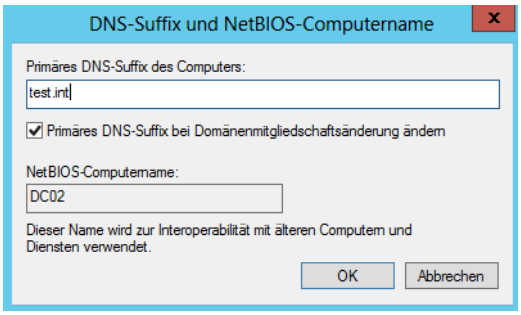
Klicken Sie mit der rechten Maustaste auf den Menüpunkt *Reverse-Lookupzone* und wählen Sie *Neue Zone* aus. Auf der ersten Seite des Assistenten wählen Sie wieder die Option *Primäre Zone*. Auf der nächsten Seite können Sie festlegen, ob Sie eine IPv4- oder eine IPv6-Reverse-Lookupzone anlegen wollen. 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-Bereichs unter *Netzwerk-ID* den IP-Bereich ein, den Sie verwalten wollen. Für jeden eigenständigen IP-Bereich müssen Sie eine eigene Zone anlegen. Verwalten Sie ein Klasse-B-Netz (255.255.0.0), können Sie auch einfach die letzte Stelle leer lassen. Hat sich bei einer Zone, die Sie für die Netzwerkkennung *192.168.* konfiguriert haben, ein Server mit der IP-Adresse *192.168.178.20* registriert, legt der DNS-Server automatisch eine Sortierung für die verschiedenen Subnetze an.

Sie müssen daher bei einem Klasse-B-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. 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 Eingabeaufforderung die dynamische Registrierung anstoßen. Danach sollte die IP-Adresse des Servers in der Zone registriert sein. Das funktioniert aber nur dann, wenn Sie das DNS-Suffix des Servers vorher anpassen. Konfigurieren Sie daher zunächst über *Systemsteuerung/System und Sicherheit/System/Erweiterte Systemeinstellungen/Computername/Ändern* neben den NetBIOS-Namen des neuen Domänencontrollers zum

Beispiel *dc02* noch das DNS-Suffix. Klicken Sie dazu im 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 *test.int*.

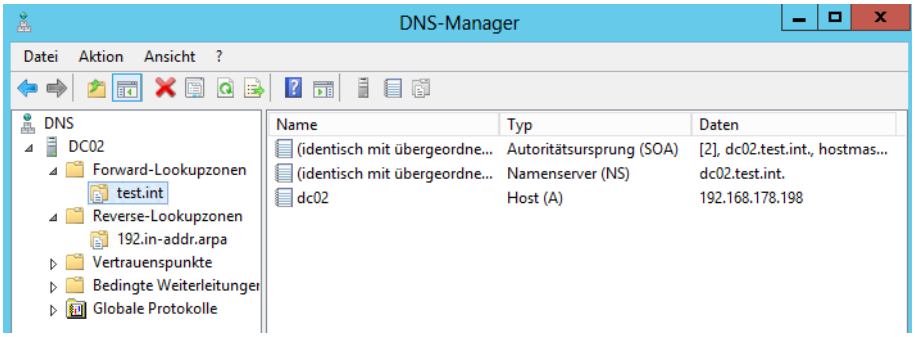
Abbildg. 11.2 Definieren des Computernamens und des DNS-Suffixes eines Domänencontrollers



Der vollständige Name des Servers (FQDN) setzt sich aus dem Computernamen und dem primären DNS-Suffix zusammen. Der vollständige Computername des Domänencontrollers lautet *dc02.test.int.* Haben Sie die Änderungen vorgenommen, müssen Sie den Server neu starten.

Nach dem Neustart können Sie überprüfen, ob sich der Server in seine DNS-Zone eingetragen hat sowie in die Reverse-Lookupzone, die Sie erstellt haben.

Abbildg. 11.3 Überprüfen des Eintrags des DNS-Servers in die eigene Zone

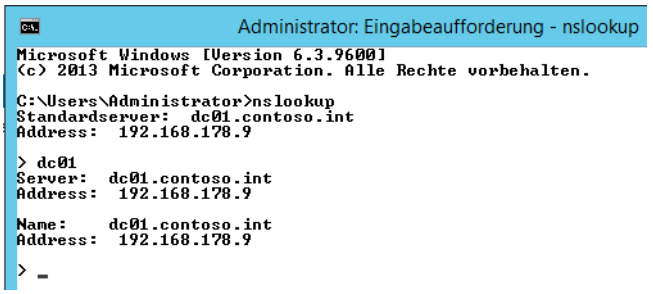


Überprüfung und Fehlerbehebung der DNS-Einstellungen

Bevor Sie Active Directory auf dem Server installieren, sollten Sie sicherstellen, dass alle DNS-Einstellungen korrekt vorgenommen sind. Überprüfen Sie, ob sich der Server sowohl in der Forward- als auch in der Reverse-Lookupzone korrekt eingetragen hat.

Öffnen Sie danach eine Eingabeaufforderung 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. Suchen Sie in Nslookup noch nach der IP-Adresse, muss diese nach dem Servernamen aufgelöst werden.

Abbildg. 11.4 Namensauflösung in der Eingabeaufforderung testen



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 Eingabeaufforderung. Überprüfen Sie, ob sich der Server in die Zone eingetragen hat.
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.

Treten keine Fehler auf, können Sie mit der Erstellung von Active Directory auf diesem Server beginnen. Dazu gehen Sie vor, wie in Kapitel 10 erläutert.

Haben Sie Active Directory installiert, stehen auch in Windows Server 2012 R2 die bekannten Tools Dcdiag, Repadmin & Co. zur Analyse zur Verfügung. Für die Namensauflösung können Sie weiterhin Nslookup verwenden oder die neuen Cmdlets zur Verwaltung von DNS, zum Beispiel *Resolve-DnsName*.

Installation der Active Directory-Domänendienste-Rolle

Nachdem Sie diese Vorbereitungen getroffen haben, können Sie Active Directory auf dem Server installieren. Wie Sie dabei vorgehen, lesen Sie in Kapitel 10. In den folgenden Abschnitten gehen wir ausführlicher auf die Einrichtung einer neuen Gesamtstruktur ein.

TIPP Neben dem Server-Manager (siehe Kapitel 10) können Sie die Binärdateien von Active Directory inklusive der Verwaltungstools auch in der PowerShell installieren. Dazu verwenden Sie den Befehl *Install-WindowsFeature –Name AD-Domain-Services –IncludeManagementTools*.

Alle Befehle, die für Active Directory zur Verfügung stehen, erhalten Sie über *Get-Command –Module ADDSDeployment* angezeigt. Hilfestellungen rufen Sie über *Get-Help <Cmdlet>* ab.

Test der Voraussetzungen zum Betrieb von Active Directory

In der PowerShell testen Sie Domänencontroller mit den Cmdlets *Test-ADDSDomainControllerInstallation, Test-ADDSDomainControllerUninstallation, Test-ADDSDomainInstallation, Test-ADDSForestInstallation* und *Test-ADDSReadOnlyDomainControllerAccountCreation*.

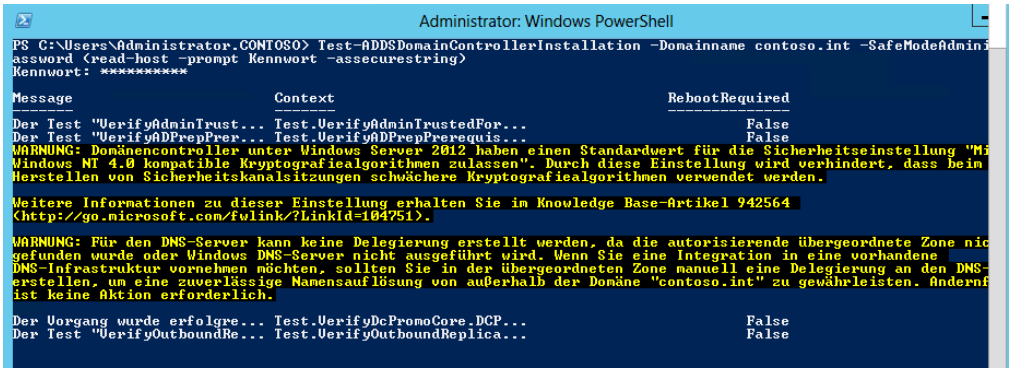
Das Cmdlet *Test-ADDSDomainControllerInstallation* (*http://technet.microsoft.com/en-us/library/hh974725.aspx* [Ms179-K11-01]) ermöglicht das Testen der Voraussetzungen für die Installation eines Domänencontrollers. Die Voraussetzungen für schreibgeschützte Domänencontroller testen Sie mit *Test-ADDSReadOnlyDomainControllerAccountCreation* (*http://technet.microsoft.com/en-us/library/hh974721* [Ms179-K11-02]).

Test-ADDSDomainControllerUninstallation (*http://technet.microsoft.com/en-us/library/hh974716.aspx* [Ms179-K11-03]) testet die Voraussetzungen für die Deinstallation eines Domänencontrollers. Das Tool bereitet sozusagen die Ausführung des Cmdlets *Uninstall-ADDSDomainController* (*http://technet.microsoft.com/en-us/library/hh974714* [Ms179-K11-04]) vor.

Mit *Test-ADDSDomainInstallation* testen Sie die Voraussetzungen für die Installation einer neuen Domäne in Active Directory, *Test-ADDSForestInstallation* testet das Gleiche für eine neue Gesamtstruktur auf Basis von Windows Server 2012 R2. Damit Sie die Tests ausführen können, müssen Sie an verschiedenen Stellen noch Kennwörter eingeben. Diese akzeptiert das entsprechende Cmdlet aber nur als sichere Eingabe. Ein Beispiel für den Befehl ist:

```
Test-ADDSDomainControllerInstallation –DomainName <DNS-Name der Domäne> –
SafeModeAdministratorPassword (Read-Host –Prompt Kennwort –AsSecureString)
```

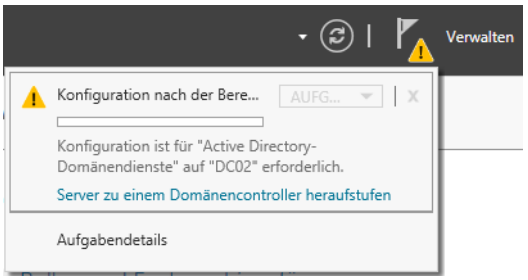
Abbildg. 11.5 Erfolgreicher Test der Installation eines neuen Domänencontrollers



Starten der Installation von Active Directory

Nachdem Sie die Serverrolle installiert haben, beginnen Sie mit der Einrichtung der Domäne. Diesen Vorgang starten Sie im Server-Manager über das Wartungssymbol.

Abbildg. 11.6 Heraufstufen eines Servers zu einem Domänencontroller



TIPP Sie können die Einrichtung von Active Directory auch in der PowerShell auf einem Computer im Netzwerk durchführen. Dazu verwenden Sie den folgenden Cmdlet-Aufruf:

```
Invoke-Command {Install-ADDSDomainController -DomainName <Domäne> -Credential (Get-
Credential) -ComputerName <Name des Servers>.
```

Wenn Sie die erste Domäne für Ihre Gesamtstruktur erstellen, wählen Sie die Option *Neue Gesamtstruktur hinzufügen* aus. Sie erstellen durch diese Auswahl eine neue Domäne und auch die dazugehörige Gesamtstruktur. Insgesamt gibt es in Active Directory die drei Container *Gesamtstruktur*, *Struktur* und *Domäne*. In den nächsten Kapiteln gehen wir ausführlicher auf dieses Thema ein.

Als Nächstes wählen Sie den DNS-Namen der Domäne. Dieser muss mit der erstellten DNS-Zone und dem DNS-Suffix des ersten Domänencontrollers übereinstimmen. Auf der nächsten Seite des Assistenten legen Sie die Funktionsebene der Gesamtstruktur und damit aller Domänen fest sowie einzelner Domänen. Active Directory kann unter verschiedenen Funktionsebene betrieben werden:

- Funktionsebene der einzelnen Domänen in der Gesamtstruktur
- Funktionsebene der Gesamtstruktur, die dann für alle Domänen gültig ist

HINWEIS Sie können die Funktionsebene für die Domänen im Snap-In *Active Directory-Benutzer und -Computer* über das Kontextmenü der Domäne einstellen. Die Funktionsebene für die Gesamtstruktur stellen Sie über das Snap-In *Active Directory-Domänen und -Vertrauensstellungen* ein, ebenfalls über das Kontextmenü. Das Abändern der Funktionsebene lässt sich nicht rückgängig machen.

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 teilweise unabhängig voneinander jeweils verschiedene Funktionsebenen annehmen. Diese Funktionsebenen haben keine Kompatibilitätsunterschiede für Mitgliedsserver oder -PCs. Wichtig ist der Modus nur für die integrierten Domänencontroller. Das heißt, auch im Betriebsmodus *Windows Server 2012 R2* dürfen Sie Server mit Windows Server 2003/2008/2008 R2 als Mitgliedsserver betreiben, nur eben nicht als Domänencontroller.

- **Windows Server 2003** Diese Funktionsebene ist nur noch Bestandteil in Windows Server 2012. In Windows Server 2012 R2 ist diese Funktionsebene nicht mehr verfügbar. Ab dieser Funktionsebene können Sie Domänen in der Gesamtstruktur umbenennen und umstrukturieren. Sie können Gesamtstruktur-übergreifende Vertrauensstellungen erstellen. In dieser Funktionsebene werden schreibgeschützte Domänencontroller (RODC) unterstützt, sofern sich der PDC-Emulator auf einem Domänencontroller unter Windows Server 2012 befindet.
- **Windows Server 2008** Diese Funktionsebene weist funktional keine großen Unterschiede zum Windows Server 2003-Modus auf. In dieser Funktionsebene werden Kennwortrichtlinien für mehrere Organisationseinheiten (OUs) unterstützt. Außerdem nutzt Windows in diesem Modus zur Replikation des *SYSVOL*-Ordners DFS, was wesentlich performanter und stabiler funktioniert. In diesem Modus können Sie den Kerberosverkehr mit AES 128 oder 256 verschlüsseln.
- **Windows Server 2008 R2** Diese Funktionsebene ist für die Unterstützung des Active Directory-Papierkorbs notwendig oder wenn Sie Authentifizierungsrichtlinien mit Active Directory-Verbunddiensten konfigurieren wollen
- **Windows Server 2012** Diese Funktionsebene ist notwendig, wenn Sie die neuen Active Directory-Funktionen in Windows Server 2012/2012 R2 nutzen wollen. Dazu gehören die Möglichkeit, Domänencontroller zu klonen oder verwaltete Dienstkonten auf mehreren Servern einzusetzen. Auf der Windows Server 2012/2012 R2-Domänenfunktionsebene ist die Kerberos-Domänencontrollerrichtlinie für die Unterstützung der dynamischen Zugriffssteuerung und Kerberos Armoring aktiv. Die Windows Server 2012/2012 R2-Gesamtstrukturfunktionsebene bietet keine neuen Features, stellt aber sicher, dass alle in der Gesamtstruktur erstellten neuen Domänen automatisch auf Windows Server 2012/2012 R2-Domänenfunktionsebene gestellt werden.
- **Windows Server 2012 R2** Diese neue Funktionsebene aktivieren Sie, wenn Sie nur noch Domänencontroller mit Windows Server 2012 R2 einsetzen. Die Funktionsebene bietet die gleichen Möglichkeiten wie Windows Server 2012. Haben Sie alle Ihre Domänencontroller auf Windows Server 2012 R2 aktualisiert, sollten Sie die Gesamtstrukturfunktionsebene und die Domänenfunktionsebenen der Domänen auf Windows Server 2012 heraufstufen, wenn Sie tiefgehende Active Directory-Funktionen aus Windows Server 2012 R2 nutzen, um zum Beispiel Webanwendungen mit Claim-Based-Authentication und AD FS zusammen betreiben.

Auf der gleichen 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.

TIPP Installieren Sie Active Directory in der PowerShell, können Sie steuern, ob der neue Domänencontroller auch als DNS-Server fungieren soll. Dazu verwenden Sie die Option *–InstallDNS*:

- *InstallDNS:$false*
- *InstallDNS:$true*

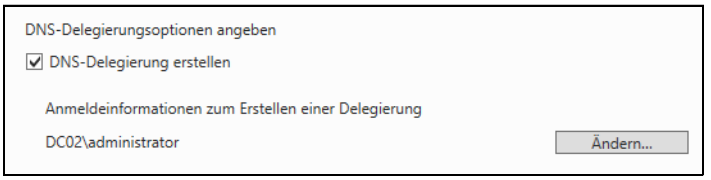
Der neue Domänencontroller wird darüber hinaus auch zwingend der erste globale Katalog-Server. Auf dieser Seite können Sie auch festlegen, ob ein Domänencontroller zum schreibgeschützten Domänencontroller (RODC) werden soll. Hierbei wird auf dem Domänencontroller ein Replikat der Active Directory-Datenbank gespeichert, die keinerlei Änderungen akzeptiert.

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, da dem ersten Domänencontroller gewisse Verpflichtungen zukommen, die Sie an dieser Stelle nicht ändern können. Wir kommen bei der Integration eines zusätzlichen Domänencontrollers noch auf dieses Thema zurück.

Auf dem Fenster legen Sie auch das Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus an. Hierbei handelt es sich um das Kennwort des lokalen Administrators, wenn Sie zur Wiederherstellung von Active Directory ohne den Active Directory-Dienst starten.

Auf der nächsten Seite erkennt der Assistent, dass bereits eine Zone vorhanden ist, wenn Sie diese zuvor angelegt haben, wie in diesem Abschnitt besprochen. Der Assistent bietet an, eine neue Zone für Active Directory zu installieren und diese unterhalb der aktuellen Zone zu integrieren. Diese DNS-Delegierung sollten Sie aktivieren, damit die Daten von Active Directory in einer eigenen Zone unterhalb der aktuellen Zone gebündelt werden.

Abbildg. 11.7 Konfigurieren der DNS-Delegation für Active Directory



Wollen Sie Active Directory aber genau innerhalb der Zone speichern, deaktivieren Sie die Option *DNS-Delegierung erstellen*. DNS-Delegierungen können Sie auch für andere Zonen anlegen, nicht nur für Active Directory.

DNS-Delegierung funktioniert folgendermaßen: Wenn Sie eine untergeordnete Domäne erstellen wollen, zum Beispiel die Domäne *de* unterhalb der Domäne *contoso.com*, haben Sie zwei Möglichkeiten, die Namensauflösung 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. Vor allem bei größeren Unternehmen kann die Erstellung von untergeordneten DNS-Domänen Probleme bereiten. Wenn zum Beispiel in der Zentrale in Dallas die Rootdomäne *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 könnte.

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 eine Verbindung zu der Zone *de.contoso.com* herstellen können, wird in der Hauptzone *contoso.com* eine sogenannte *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

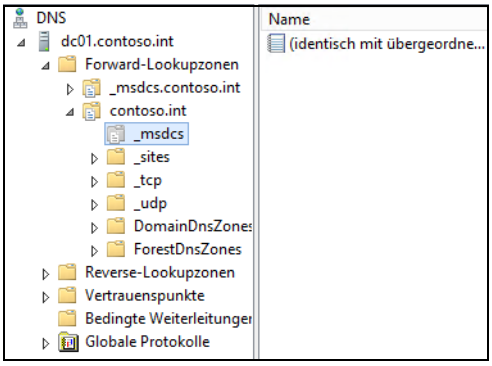
in Deutschland. Durch diese Konfiguration können weiterhin alle Namen aufgelöst werden, aber die Administratoren der Niederlassungen können nur ihre eigenen Zonen verwalten, nicht die Zonen der anderen Niederlassungen.

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.

Ein DNS-Server der Zone *contoso.com*, der eine Anfrage für die Domäne *de.contoso.com* erhält, gibt 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 verwaltet, genauso verwaltet wie die Zone *contoso.com* auf dem Haupt-DNS-Server. Die Delegation auf den DNS-Servern der Zone *contoso.com* hat keinerlei Auswirkungen auf die Verwaltung der Zone *de.contoso.com*. Die Delegation ist 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. Lassen Sie den Assistenten zum Erstellen von Active Directory eine Delegation einrichten, erstellt er eine neue DNS-Zone mit dem Namen *_msdcs_<DNS-Name des Servers>*. In der originalen DNS-Zone legt der Assistent eine Delegierung zur neu angelegten Zone an. So ist sichergestellt, dass Anpassungen an der DNS-Zone des Servers Active Directory nicht beeinträchtigen. Legen Sie keine Delegierung an, erstellt der Assistent innerhalb der bereits vorhandenen DNS-Zone einen neuen Ordner mit der Bezeichnung *_msdcs*.

Abbildg. 11.8 DNS-Delegierung für Active Directory



Nachdem Sie die Konfiguration von DNS abgeschlossen und einen Benutzernamen mit Administratorrechten für die Änderung der Zone eingegeben haben, wechseln Sie auf die nächste Seite des Assistenten. Hier geben Sie den NetBIOS-Namen der neuen Domäne fest.

Im nächsten Fenster legen Sie den Speicherort der Datenbank und der Protokolle fest, die Active Directory zum Speichern der Informationen benötigt. 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.

Anschließend erhalten Sie eine Zusammenfassung angezeigt. Klicken Sie auf *Weiter*, testet der Assistent den Server, ob Active Directory installiert werden kann. Sie erhalten noch Informationen und Warnungen, die Sie berücksichtigen sollten. Mit *Installieren* beginnt der Assistent die Installation von Active Directory.

Über das Kontextmenü eines Domänencontrollers in der Servergruppe *AD DS* können Sie Verwaltungstools und Tools zur Analyse der Domäne starten. Es öffnet sich eine Eingabeaufforderung, in der Sie mit den bereits bekannten Mitteln aus Windows Server 2008 R2 eine Analyse durchführen können.

Die Analyse startet aber nicht, indem Sie das Tool im Kontextmenü des Servers im neuen Server-Manager starten. Hier öffnet sich lediglich eine neue Eingabeaufforderung, welche die Hilfe des Tools anzeigt. Die Diagnose selbst starten Sie nach der Installation von Active Directory, indem Sie eines der Tools Dcdiag oder Repadmin verwenden und dabei auf die verschiedenen Optionen der Befehle setzen. Mehr zu diesem Thema erfahren Sie in Kapitel 10 und den folgenden Kapiteln in diesem Buch.

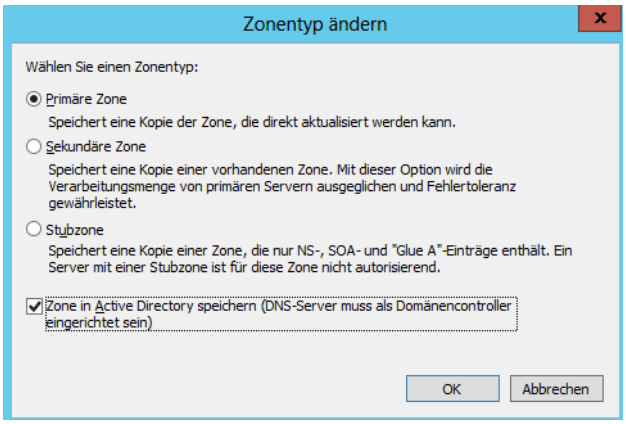
DNS in Active Directory integrieren und sichere Updates konfigurieren

Die erste Maßnahme, die Sie nach der Installation von Active Directory durchführen sollten, ist die Integration der DNS-Zonen in Active Directory. Windows Server 2012 R2 führt diesen Vorgang automatisch durch, wenn der Assistent die Zone erstellt. Sie sollten die Einstellungen aber überprüfen.

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 Active Directory, sind die Zonen bereits automatisch in Active Directory integriert. Um diese Konfiguration zu überprüfen, rufen Sie zunächst das DNS-Snap-In über den Server-Manager auf. Erweitern Sie die Zone, sehen Sie die Erweiterungen, die Active Directory hinzugefügt hat. In den einzelnen Unterdomänen der Zone finden Sie die verschiedenen SRV-Records. Um die Zone in Active Directory zu integrieren, markieren Sie die gesamte DNS-Zone.

1. Klicken Sie mit der rechten Maustaste auf die Zone und wählen Sie im Kontextmenü den Eintrag *Eigenschaften*.
2. Auf der Registerkarte *Allgemein* können Sie durch Klicken auf die Schaltfläche *Ändern* im Bereich *Typ* die Zone in 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. 11.9 Speichern von DNS-Zonen in Active Directory

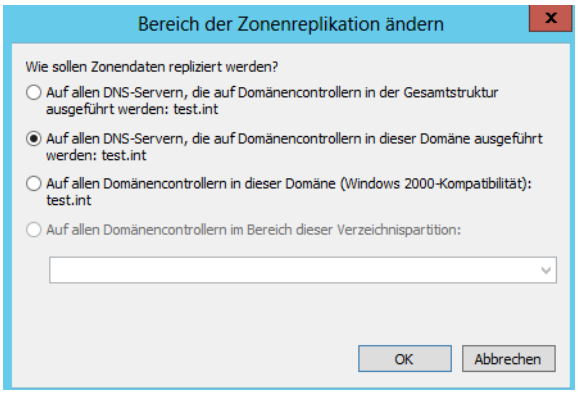


Bei dieser Einstellung können sich nur Computer, die sich erfolgreich in Active Directory authentifizieren, dynamisch in DNS registrieren.

Bei der Integration der DNS-Zone in Active Directory sehen Sie auch die Möglichkeit, eine Stubzone zu erstellen. Eine Stubzone ist die Kopie einer Zone, die nur die für diese Zone erforderlichen Ressourceneinträge zum Identifizieren der autorisierenden DNS-Server enthält.

Haben Sie die Zone in 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. 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. 11.10 Konfiguration der DNS-Datenreplikation



DNS-IP-Einstellungen anpassen

Windows Server 2012 R2 hat die Eigenart, die Konfiguration der Netzwerkverbindungen automatisch abzuändern, sodass die Einstellungen für manche Administratoren verwirrend sein können. Dieser Abschnitt geht darauf ein, wie Sie die Einstellungen wieder an Ihre Bedürfnisse anpassen. Geben Sie nach der Fertigstellung der Installation von Active Directory auf dem Domänencontroller in der Eingabeaufforderung *nslookup* ein, erhalten Sie unter Umständen eine etwas verwirrende Ausgabe. Der Server gibt als Adresse *::1* zurück. In Kapitel 6 sind wir bereits auf das Thema eingegangen.

Die Ausgabe wird durch eine Konfiguration der Netzwerkverbindungen verursacht. Rufen Sie zunächst die Verwaltung Ihrer Netzwerkverbindungen auf. Der schnellste Weg ist, wenn Sie *ncpa.cpl* in der Startseite eingeben. Rufen Sie zunächst die Eigenschaften des IPv6-Protokolls auf. Wie Sie sehen, hat Windows Server 2012 R2 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. Legen Sie entweder eine IPv6-Reverse-Lookupzone an und stellen Sie sicher, dass ein Zeiger zur IPv6-Adresse des Servers eingetragen wird.

Aktivieren Sie am besten die Option *DNS-Serveradresse automatisch beziehen*. Durch diese Konfiguration vermeiden Sie die irreführende Meldung in Nslookup. 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 Eingabeaufforderung 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, die Sie als Datenträger gespeichert haben, müssen zuvor einige Vorbereitungen getroffen werden.

Für die Installation eines Domänencontrollers in Niederlassungen oder bereits ausgelasteten Netzwerken bietet es sich an, auf einem Quelldomänencontroller zunächst Daten aus Active Directory zu exportieren, auf einen Datenträger zu kopieren und zur Niederlassung zu senden. Bei der Heraufstufung eines Domänencontrollers kann dieses Medium verwendet werden.

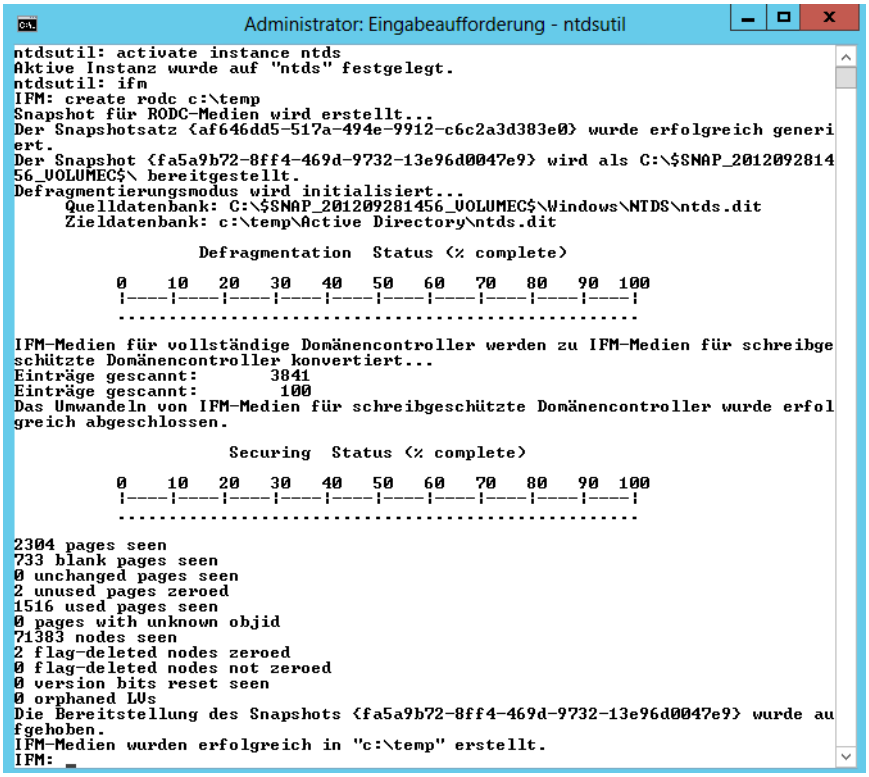
So muss der Domänencontroller in der Niederlassung nur noch das Delta zwischen Medium und aktuellen Daten mit seinen Replikationspartnern synchronisieren, was deutlich Netzwerklast spart. Auf den folgenden Seiten zeigen wir Ihnen, wie Sie dazu am besten vorgehen.

Vorbereiten des Active Directory-Installationsmediums

Um ein Installationsmedium vorzubereiten, müssen Sie sich an einem Domänencontroller mit Adminrechten anmelden. Gehen Sie im Anschluss folgendermaßen vor:

1. Öffnen Sie eine Eingabeaufforderung 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.
4. Geben Sie *create rodc c:\temp* ein, um ein Installationsmedium für einen RODC (schreibgeschützter Domänencontroller) zu erstellen. Um einen vollwertigen DC mit dem Installationsmedium zu erstellen, geben Sie *create full c:\temp* ein. Soll der *SYSVOL*-Ordner nicht mit eingeschlossen werden, verwenden Sie einen der beiden Befehle *create nosysvol rodc c:\temp* oder *create nosysvol full c:\temp*. Den Ordner können Sie natürlich beliebig ändern.
5. Beenden Sie Ntdsutil mit der wiederholten Eingabe von *quit*.
6. Überprüfen Sie, ob der Ordner erstellt wurde und die Daten darin enthalten sind.

Abbildg. 11.11 Erstellen eines Installationsdatenträgers für Active Directory

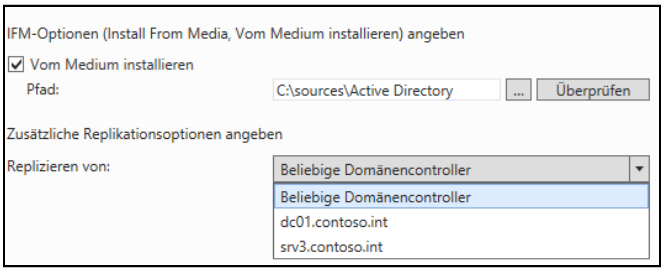


Domänencontroller mit Medium installieren

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 die Hinweise am Ende dieses Kapitels), 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 den lokalen Ordner aus, in dem die Daten abgelegt wurden. Dieses Fenster erscheint, wenn Sie über den Installations-Assistenten von Active Directory einen zusätzlichen Domänencontroller installieren (siehe Kapitel 12).

Abbildg. 11.12 Erste Replikation eines Domänencontrollers von Installationsmedium ausführen



Active Directory mit PowerShell installieren – Server Core als Domänencontroller

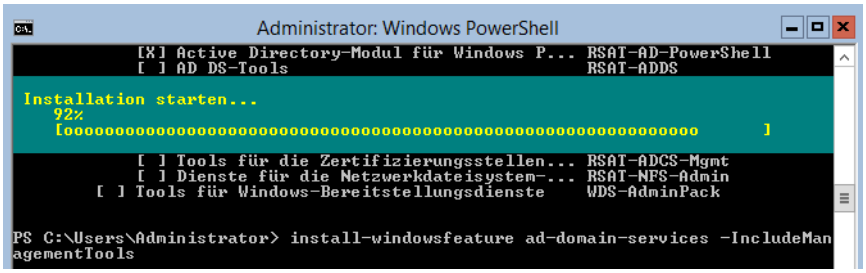
Auch Core-Server können Sie als Domänencontroller verwenden. Die Installation von Active Directory nehmen Sie am besten über die PowerShell vor. Dazu hat Microsoft einige neue Cmdlets integriert. Mit dem Cmdlet *Install-ADDSDomainController* installieren Sie in einer bestehenden Domäne zum Beispiel einen neuen Domänencontroller. Mit *Install-ADDSDomain* installieren Sie eine neue Domäne, mit *Install-ADDSForest* eine neue Gesamtstruktur. In den einzelnen Abschnitten dieses Kapitels und in Kapitel 10 haben wir Ihnen bereits einige Cmdlets und Optionen zur Installation von Active Directory mit der PowerShell gezeigt.

Um einen Domänencontroller herabzustufen, verwenden Sie das Cmdlet *Uninstall-ADDSDomainController*. Die Cmdlets fragen alle notwendigen Optionen an und starten den Server neu. Konfigurationen wie *DNS-Server* und *globaler Katalog* nehmen Sie anschließend vor. Diese Aufgaben müssen Sie nicht mehr im Assistenten zur Installation vorgeben.

Bevor Sie einen Core-Server als Domänencontroller installieren, nehmen Sie die IP-Einstellungen auf dem Server vor. Gehen Sie dazu vor wie in den Kapiteln 2, 3, 4 und 6 besprochen. Sie haben auch die Möglichkeit, Active Directory in der grafischen Benutzeroberfläche zu installieren und danach die grafische Oberfläche vom Server zu entfernen (siehe Kapitel 3). Alternativ aktivieren Sie die Remoteverwaltung und nehmen die Einrichtung über Veraltungstools von anderen Servern vor oder über eine Arbeitsstation. In diesem Fall nehmen Sie den Core-Server in die Domäne auf (siehe Kapitel 6), verbinden sich mit dem Server über einen anderen Rechner und den Server-Manager. Über diesen Weg können Sie auf einem Core-Server Active Directory genauso installieren wie mit lokalen Verwaltungswerkzeugen.

Um Active Directory mit der PowerShell zu installieren, geben Sie in der Eingabeaufforderung zunächst *powershell* ein. Im ersten Schritt müssen Sie mit *Install-WindowsFeature AD-Domain-services –IncludeManagementTools* die Active Directory-Domänendienste auf dem Server installieren.

Abbildg. 11.13 Installieren von Active Directory auf einem Domänencontroller



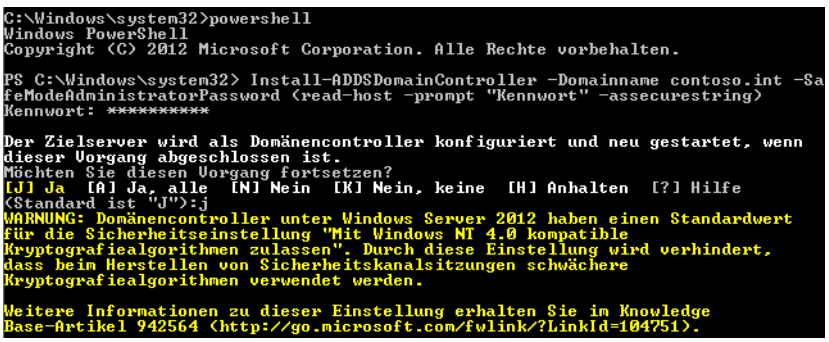
Anschließend stehen die bereits genannten Cmdlets zur Verfügung. Geben Sie keine Optionen für die Cmdlets ein, fragt der Assistent die notwendigen Daten ab. Sie können sich die Befehle auch anzeigen lassen, wenn Sie den Assistenten auf einem Server durchlaufen und sich am Ende das Skript anzeigen lassen. Hier sehen Sie die Befehle und Optionen, die Sie für die PowerShell benötigen.

Um zum Beispiel einen neuen Domänencontroller zu installieren, verwenden Sie das Cmdlet *Install-ADDSDomainController*. Damit der Befehl funktioniert, geben Sie den Namen der Domäne ein und konfigurieren das Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus als SecureString. Dazu verwenden Sie folgenden Befehl:

```
Install-ADDSDomainController -DomainName <DNS-Name der Domäne> -
SafeModeAdministratorPassword (Read-Host -Prompt Kennwort -AsSecureString)
```

Der Befehl fragt nach dem Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus und speichert dieses als sichere Zeichenfolge ab.

Abbildg. 11.14 Installieren eines zusätzlichen Domänencontrollers in der PowerShell



Sie können natürlich alle notwendigen Optionen für die Installation im Cmdlet angeben, zum Beispiel noch die Installation von DNS oder die Funktionsebene von Domäne und Gesamtstruktur. Dazu verwenden Sie zum Beispiel die Befehle:

- *–ForestMode <{Win2008 | Win2008R2 | Win2012 | Win2012R2}>*
- *–DomainMode <{Win2008 | Win2008R2 | Win2012 | Win2012R2}>*
- *–InstallDNS <{$false | $true}>*
- *–SafeModeAdministratorPassword <secure string>*

Eine neue Gesamtstruktur installieren Sie mit dem Cmdlet *Install-ADDSForest –Domainname <DNS-Name>*. Ein Beispiel für die Ausführung ist folgender Befehl:

```
Install-ADDSForest -DomainName corp.contoso.com -CreateDNSDelegation -DomainMode Win2012 -
ForestMode Win2012R2 -DatabasePath d:\NTDS -SYSVOLPath d:\SYSVOL -LogPath e:\Logs
```

In Kapitel 13 zeigen wir Ihnen, wie Sie in einer Gesamtstruktur weitere Domänencontroller, Domänen oder Strukturen integrieren. Um zum Beispiel eine neue Domäne im Betriebsmodus Windows Server 2012 in einer Gesamtstruktur zu installieren, verwenden Sie als Beispiel den Befehl

```
Install-ADDSDomain -SafeModeAdministratorPassword -Credential (Get-Credential
corp\EnterpriseAdmin1) -NewDomainName child -ParentDomainName corp.contoso.com -InstallDNS
-CreateDNSDelegation -DomainMode Win2012 -ReplicationSourceDC DC1.corp.contoso.com -
SiteName Houston -DatabasePath d:\NTDS -SYSVOLPath d:\SYSVOL -LogPath e:\Logs -
Confirm:$False
```

Um in dieser Domäne dann wiederum einen weiteren Domänencontroller zu installieren, verwenden Sie den Befehl

```
Install-ADDSDomainController -Credential (Get-Credential corp\administrator) -DomainName
corp.contoso.com
```

Ist der entsprechende Server bereits Mitglied der Domäne und haben Sie sich mit einem Domänenadministrator angemeldet, können Sie auch den Befehl *Install-ADDSDomainController –DomainName corp.contoso.com* verwenden. Ein weiteres Beispiel für die Installation eines neuen Domänencontrollers ist:

```
Install-ADDSDomainController -Credential (Get-Credential contoso\EnterpriseAdmin1) -
CreateDNSDelegation -DomainName corp.contoso.com -SiteName Boston -InstallationMediaPath
"c:\ADDS IFM" -DatabasePath "d:\NTDS" -SYSVOLPath "d:\SYSVOL" -LogPath "e:\Logs".
```

Im Kapitel 13 zeigen wir Ihnen ausführlich, wie Sie schreibgeschützte Domänencontroller (RODC) installieren. Sie können auch diese Domänencontroller in der PowerShell installieren. Ein Beispiel ist:

```
Add-ADDSReadOnlyDomainControllerAccount -DomainControllerAccountName RODC1-DomainName
corp.contoso.com -SiteName Boston DelegatedAdministratorAccountName joost
```

Um dann auf dem Server Active Directory zu installieren, verwenden Sie:

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```

Den Server stufen Sie dann mit dem folgenden Befehl zum Domänencontroller:

```
Install-ADDSDomainController -DomainName corp.contoso.com -SafeModeAdministratorPassword
(Read-Host -Prompt "DSRM Password:" -AsSecureString) -Credential (Get-Credential
Corp\joost) -UseExistingAccount
```

Mehr zu diesem Thema lesen Sie in Kapitel 13.

Virtuelle Domänencontroller betreiben – Klonen und Snapshots

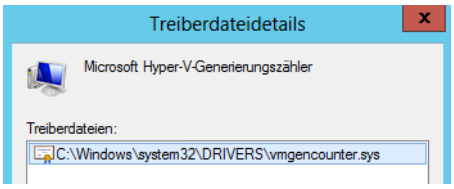
Mit Windows Server 2012 R2 hat Microsoft den Betrieb von virtuellen Domänencontrollern optimiert. Im Gegensatz zu Vorgängerversionen stellen Snapshots und geklonte Domänencontroller keine Gefahr mehr für das komplette Active Directory dar. Microsoft empfiehlt sogar Domänencontroller virtuell zu klonen, da sich so neue Domänencontroller wesentlich schneller zur Verfügung stellen lassen als mit einer herkömmlichen Installation. Bis Windows Server 2008 R2 mussten Sie Domänencontroller manuell oder mit einer Antwortdatei hochstufen.

HINWEIS Damit Sie Domänencontroller optimal virtualisieren und auch klonen können, müssen mindestens folgende Bedingungen eingehalten werden:

- Der PDC-Emulator muss sich auf einem Domänencontroller mit Windows Server 2012 befinden (siehe Kapitel 10)
- Den PDC-Emulator können Sie nicht klonen, er muss während des Klonvorgangs immer verfügbar sein
- Die Domäne muss bereits über mindestens zwei Domänencontroller mit Windows Server 2012 verfügen, da Sie nur den zweiten klonen können. Der erste stellt den PDC-Emulator zur Verfügung.
- Die Virtualisierungslösung muss diese neue Technik unterstützen (VM-Generation ID). Aktuell ist das nur Hyper-V in Windows Server 2012/2012 R2.

Ob die von Ihnen eingesetzte Virtualisierungslösung die neue VM-Generation ID unterstützt, erkennen Sie im Geräte-Manager eines virtualisierten Servers mit Windows Server 2012 R2. Bei den Systemgeräten muss der Treiber *Microsoft Hyper-V-Generierungszähler* (*Microsoft Hyper-V Generation Counter)* mit der Treiberdatei *vmgencounter.sys* existieren.

Abbildg. 11.15 Anzeigen der Treiberdetails für die Unterstützung virtueller Domänencontroller



Möglichkeiten zur Virtualisierung von Domänencontrollern

Mit Windows Server 2012 R2 haben Sie zum Beispiel die Möglichkeit, einen virtuellen Domänencontroller zu installieren, diesen mit Sysprep vorzubereiten und dieses Image für das Klonen zu verwenden. Um einen Domänencontroller zu klonen, ist die Datei *DCCloneConfig.xml* wichtig. Diese muss sich im Ordner mit der Active Directory-Datenbank befinden (standardmäßig *C:\Windows\NTDS*).

Kopieren Sie die virtuelle Festplatte des virtuellen Domänencontrollers oder exportieren und importieren Sie den virtuellen Server zu einem neuen Server, erkennt das Windows Server 2012 R2. Das Betriebssystem stuft den neuen Server automatisch zum Domänencontroller, erstellt eine neue lokale Active Directory-Datenbank und verwendet als Replikationsquelle die geklonte lokale Datenbank. Nach der erfolgreichen Heraufstufung repliziert sich der neue Domänencontroller dann ganz normal mit den anderen Domänencontrollern, wie jeder andere Domänencontroller auch.

Sie können mit diesem Klonvorgang Domänencontroller auch in neue Domänen, Strukturen oder sogar Gesamtstrukturen installieren. Damit die Sicherheit in Active Directory nicht beeinträchtigt wird, lässt sich der Vorgang auch delegieren. So müssen Domänenadmins das Klonen von neuen Domänencontrollern erst genehmigen. Das Klonen nehmen dann Hyper-V-Admins vor. Das müssen nicht unbedingt die gleichen Mitarbeiter sein. Die Grundlage, um virtuelle Domänencontroller zu klonen, ist die Datei *DCCloneConfig.xml*. Diese müssen Administratoren in der PowerShell erstellen lassen. Es lassen sich generell alle Domänencontroller klonen, Sie müssen keine besonderen Vorbereitungen treffen.

Auch die Wiederherstellung mit Snapshots ist in Windows Server 2008 R2 bei Domänencontrollern ein Problem. Setzen Sie auf einem Domänencontroller einen Snapshot zurück, kann es zu Inkonsistenzen der Active Directory-Datenbank kommen, die auch die anderen Domänencontroller beeinflusst. Das liegt daran, dass in Active Directory alle Objekte eine bestimmte Nummer besitzen, die Update Sequence Number (USN).

Jeder DC hat eine eigene Liste dieser USNs und befindet sich auch in dieser Liste. Setzen Sie einen Snapshot zurück, ändern sich USNs zahlreicher Objekte, was mit hoher Wahrscheinlichkeit zu Inkonsistenzen führt. So besteht zum Beispiel die Gefahr, dass Objekte identische USNs erhalten. In jedem Fall aber trennen die anderen Domänencontroller den wiederhergestellten Domänencontroller vom Netzwerk.

Windows Server 2012 R2 erkennt jetzt ein Zurücksetzen mit einem Snapshot und kann die fehlenden Daten zwischen lokaler Active Directory-Datenbank und der Datenbank von anderen Domänencontrollern replizieren. Sie müssen bei diesen Vorgängen nichts beachten, sondern können beliebige Snapshots erstellen und diese wieder zurücksetzen, wenn das notwendig ist.

Dazu erhält neben jeder Transaktion in Active Directory (USN) auch jede Active Directory-Datenbank selbst eine ID, InvocationID genannt. Zusammen mit der USN einer Transaktion und der InvocationID der Active Directory-Datenbank auf dem jeweiligen Domänencontroller ergibt das eine eindeutige Nummerierung aller Transaktionen in Active Directory. Diese Nummerierung kann daher in Windows Server 2008 R2 zu Problemen führen, wenn Sie einen Domänencontroller zurücksetzen. Bei diesem Vorgang ändert sich seine InvocationID nicht.

Installieren Sie einen Domänencontroller mit Windows Server 2012 R2 auf einem Hyper-V-Host mit Windows Server 2012 R2, erstellt der Server eine eindeutige VM Generation ID und speichert diese im Computerobjekt des Domänencontrollers in Active Directory. Auf diesem Weg kann Active Directory erkennen, welcher Domänencontroller virtuell betrieben wird und wie dessen ID ist.

Setzen Sie einen Snapshot auf einem Windows Server 2012 R2-Domänencontroller zurück, erkennt Active Directory das. Allerdings muss der Hypervisor diese Funktion auch unterstützten. Das kann aktuell nur Hyper-V 3.0 in Windows Server 2012 R2.

Bereitstellung virtueller Domänencontroller vorbereiten – XML-Dateien erstellen

Um einen virtuellen Domänencontroller zu klonen, können Sie nicht einfach seine Festplatte kopieren oder den Server exportieren und importieren, sondern Sie müssen für den Server eine Datei *DCCloneConfig.xml* in der PowerShell erstellen. Diese Datei können Sie auf Basis einer Vorlage erstellen und an Ihre eigenen Bedürfnisse anpassen.

HINWEIS Damit Sie virtuelle Domänencontroller klonen können, muss die Domäne über mindestens zwei Domänencontroller verfügen. Der Domänencontroller, den Sie klonen, darf nicht der PDC-Master sein (siehe Kapitel 10). Dieser spielt beim Klonen eine wichtige Rolle und steuert die Verwaltung der neuen GenerationID.

Bevor Sie einen virtuellen Domänencontroller klonen, müssen Sie auf dem Server das Cmdlet *Get-ADDCCloningExcludedApplicationList* ausführen. Das Cmdlet überprüft, ob es auf dem virtuellen Server Anwendungen gibt, die das Klonen nicht unterstützen.

Abbildg. 11.16 Überprüfen, ob sich ein Domänencontroller klonen lässt

```
PS C:\Users\Administrator> Get-ADDCCloningExcludedApplicationList
Es wurden keine ausgeschlossenen Anwendungen erkannt.
PS C:\Users\Administrator> _
```

Entdeckt das Cmdlet nicht-kompatible Dienste, zum Beispiel den DHCP-Dienst oder einen installierten Virenscanner, erhalten Sie entsprechende Informationen. In diesem Fall müssen Sie den entsprechenden Dienst erst vom Server entfernen. Alternativ tragen Sie den Dienst später in die Datei *CustomDCCloneAllowList.xml* ein. Diese muss in etwa folgendermaßen aussehen:

Listing 11.1 Beispiel für eine angepasste Datei *CustomDCCloneAllowList.xml*

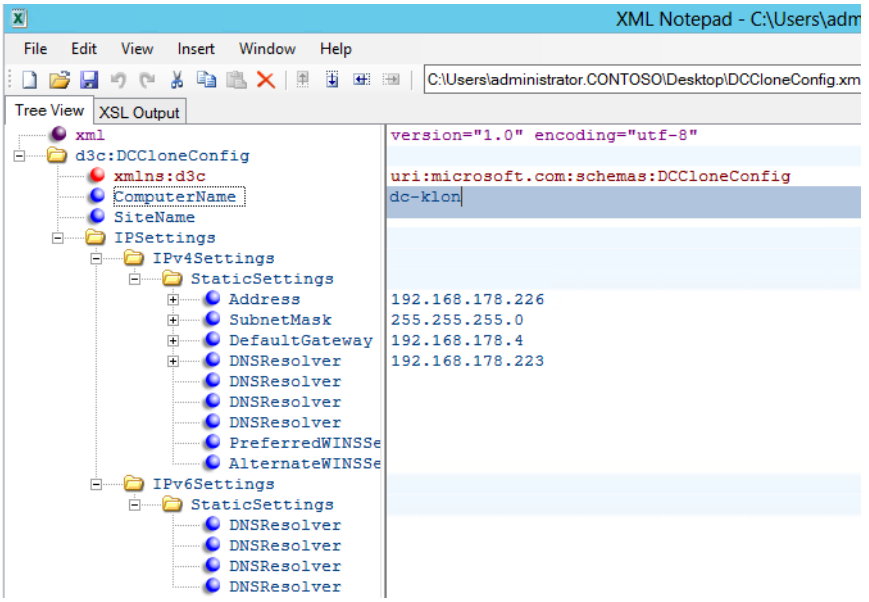
```
<?xml version=1.0 encoding=utf-8 ?>
<AllowList>
    <Allow>
      <Name></Name>
      <Type>Service</Type>
    </Allow>
    <Allow>
      <Name></Name>
      <Type>Program</Type>
    </Allow>
</AllowList>
```

Eine Liste der Anwendungen und Dienste, die das Klonen unterstützen, finden Sie in der Datei *c:\windows\system32\DefaultDCCloneAllowList.XML* auf dem virtuellen Domänencontroller. Die Konfiguration für das Klonen nehmen Sie später in der Datei *DCCloneConfig.xml* vor. Die Beispieldatei *SampleDCCloneConfig.xml* finden Sie im Ordner *C:\Windows\System32*.

Um XML-Dateien zu bearbeiten, können Sie zwar den Editor in Windows verwenden. Microsoft stellt aber zwei Programme kostenlos zur Verfügung, die in dieser Hinsicht einfacher zu verwenden sind:

- Visual Studio 2012 Express *http://www.microsoft.com/visualstudio/deu/products/visual-studio-express-products* [Ms179-K11-05]
- XML Notepad *http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=7973* [Ms179-K11-06]

Abbildg. 11.17 Erstellen einer XML-Datei für das Klonen von Domänencontrollern



In der XML-Datei pflegen Sie in den verschiedenen Bereichen die IP-Adresse des neuen Servers sowie die Subnetzmaske, das Standardgateway und die DNS-Server, die der neue Server zur Namensauflösung verwenden soll. Sie legen hier auch den neuen Namen des Domänencontrollers fest.

Microsoft empfiehlt den Einsatz von Visual Studio 2012 Express, aber das XML Notepad ist kleiner und schneller installiert. Dafür hat Visual Studio 2012 Express bereits integrierte Vorlagen für das Klonen von Domänencontrollern. Diese laden Sie über ein neues Projekt und der Auswahl von *Tools/Settings/Expert Settings/vdc cloning xml*.

Verwenden Sie das einfachere XML Notepad 2007, kopieren Sie einfach die Beispieldatei *SampleDCCloneConfig.xml* aus dem Ordner *C:\Windows\System32* in das Arbeitsfenster von XML Notepad. Wählen Sie danach *View/Expand All*, um alle Einstellungsmöglichkeiten zu sehen. Außerdem müssen Sie noch die Schemadatei für das Klonen in XML Notepad laden. Dazu verwenden Sie *View/Schemas* und die Datei *c:\windows\system32\DCCloneConfigSchema.xsd* vom Domänencontroller. Sie können jetzt die einzelnen Optionen der Datei bearbeiten und in der Datei *DCCloneConfig.xml* speichern.

TIPP Nachdem Sie die Datei *DCCloneConfig.xml* erstellt haben, kopieren Sie diese in den Ordner mit der Active Directory-Datenbank, also normalerweise in den Ordner *C:\Windows\NTDS*. Den Ordner legen Sie während der Heraufstufung zum Domänencontroller fest. In der PowerShell erstellen Sie die Datei neu, indem Sie das Cmdlet *New-ADDCCloneConfigFile* verwenden. Beispiel:

```
New-ADDCCloneConfigFile –Offline –CloneComputerName CloneDC1 –SiteName REDMOND -
IPv4Address "10.0.0.2" -IPv4DNSResolver "10.0.0.1" -IPv4SubnetMask "255.255.0.0" -
IPv4DefaultGateway "10.0.0.1" –Static –Path F:\Windows\NTDS
```

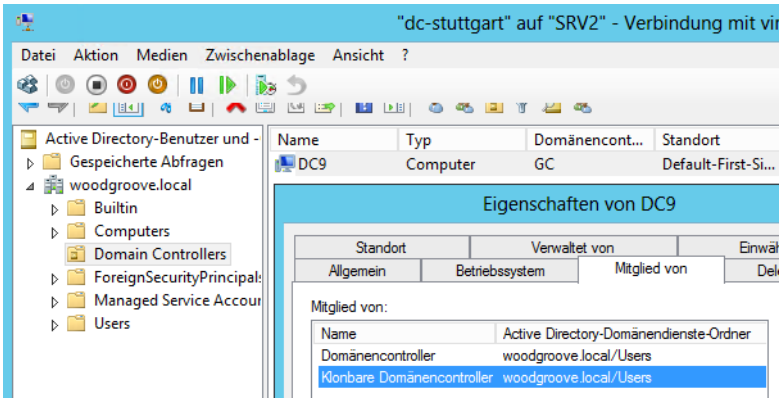
Befinden sich auf dem Quellserver nicht-kompatible Anwendungen, die das Cmdlet *Get-ADDCCloningExcludedApplicationList* anzeigt, müssen Sie diese entweder entfernen oder in die Datei *CustomDCCloneAllowList.xml* im gleichen Ordner aufnehmen.

Quelldomänencontroller vor dem Klonen überprüfen und vorbereiten

Bevor Sie den Quellcomputer klonen können, müssen Sie zunächst die in den vorangegangenen Abschnitten besprochen Vorbereitungen treffen. Außerdem müssen Sie sicherstellen, dass der Quell-DC problemlos in Active Directory funktioniert. Wie Sie Diagnosen durchführen, lesen Sie in den Kapiteln 10, 14 und 15.

Der Quelldomänencontroller muss mit dem PDC-Master der Domäne kommunizieren können (siehe Kapitel 10). Das testen Sie zum Beispiel mit den beiden Befehlen *dcdiag /test:locatorcheck /v* und *nltest /server:<PDC-Emulator> /dclist:<Domäne>*. Mehr zu den beiden Befehlen lesen Sie in den Kapiteln 10 und 15.

Abbildg. 11.18 Aufnehmen von Domänencontrollern in die Active Directory-Gruppe der klonfähigen Domänencontroller



Sie können nur Quelldomänencontroller klonen, die Mitglied der Gruppe *Klonbare Domänencontroller* in Active Directory sind. Nehmen Sie Domänencontroller dazu am besten im Snap-In *Active Directory-Benutzer und -Computer* auf der Registerkarte *Mitglied von* in dieser Gruppe auf.

HINWEIS Sie können nur Domänencontroller klonen, die nicht eingeschaltet sind. Das heißt, Sie müssen den entsprechenden Domänencontroller herunterfahren, bevor Sie ihn klonen können.

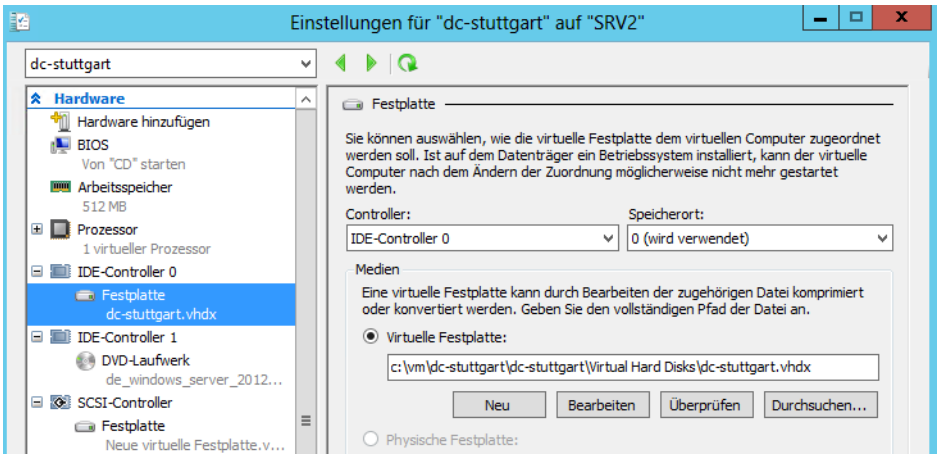
Festplatten von virtuellen Domänencontrollern kopieren

Um die Festplatten eines virtuellen Domänencontrollers zu kopieren, den Sie klonen wollen, haben Sie zwei Möglichkeiten. Sie können die Festplatten mit dem Explorer kopieren und in einen neuen Server einbinden oder Sie exportieren den virtuellen Computer (siehe Kapitel 8). Microsoft empfiehlt, immer alle virtuellen Festplatten eines virtuellen Domänencontrollers zu kopieren, nicht nur die Systemfestplatte.

HINWEIS Bevor Sie einen virtuellen Domänencontroller exportieren oder dessen virtuelle Festplatten kopieren, löschen Sie zuvor alle seine Prüfpunkte (siehe Kapitel 8). Sie können nach dem Vorgang problemlos Prüfpunkte für den neuen Domänencontroller und für den Quell-DC erstellen.

Wo die virtuellen Festplatten des Domänencontrollers gespeichert sind, sehen Sie im Hyper-V-Manager in dessen Einstellungen im Bereich *IDE-Controller* oder *SCSI-Controller*.

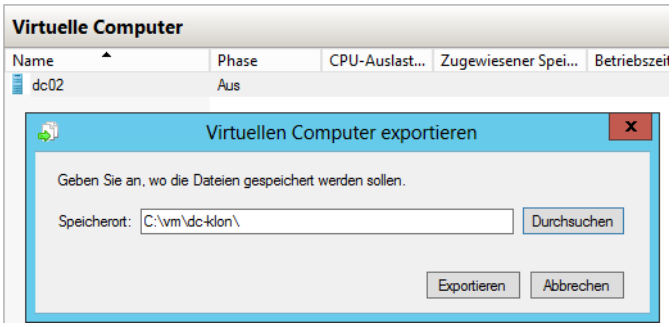
Abbildg. 11.19 Virtuelle Festplatten eines virtuellen Domänencontrollers überprüfen



Sie können die virtuellen Festplatten auch in der PowerShell mit den Cmdlets *Get-VMIdeController*, *Get-VMScsiController*, *Get-VMFibreChannelHba* und *Get-VMHardDiskDrive* abfragen.

Um einen virtuellen Server zu exportieren, müssen Sie ihn ausschalten. Anschließend erscheint im Kontextmenü des Servers der Menübefehl *Exportieren*.

Abbildg. 11.20 Exportieren eines virtuellen Computers im Hyper-V-Manager



Geklonten Domänencontroller für die Aufnahme in Active Directory vorbereiten

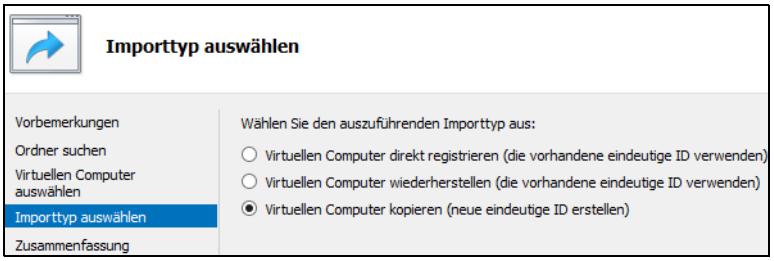
Bevor Sie den neuen Domänencontroller in Active Directory aufnehmen können, müssen Sie die durch den Klonvorgang angepasste Datei *DCCloneConfig.xml* vom Quellcomputer in den Ordner mit der Active Directory-Datenbank, also normalerweise in den Ordner *C:\Windows\NTDS*, vom Quell- auf den Zielcomputer kopieren. Windows hat den Namen der Datei angepasst, um zu zeigen, dass ein Klonvorgang stattgefunden hat. Ändern Sie den Namen wieder um zu *DCCloneConfig.xml*.

HINWEIS Bis Sie den Zielcomputer in Active Directory eingebunden haben, muss der Quell-DC ausgeschaltet bleiben. Der Ziel-DC muss aber Kontakt zum PDC-Emulator der Domäne aufbauen können, von der er geklont wurde (siehe Kapitel 10).

Befinden sich auf dem Quellserver nicht kompatible Anwendungen, die das Cmdlet *Get-ADDCCloningExcludedApplicationList* anzeigt, müssen Sie die Datei *CustomDCCloneAllowList.xml* im gleichen Ordner aufnehmen. Dazu starten Sie aber den neuen virtuellen Domänencontroller nicht, sondern binden seine virtuelle Festplatte in den Explorer des Hyper-V-Hosts ein und kopieren die Datei (siehe Kapitel 6). Nach dem Kopieren werfen Sie die virtuelle Festplatte wieder aus.

Anschließend erstellen Sie entweder einen neuen virtuellen Computer und verwenden die kopierte Festplatte (siehe Kapitel 7) oder Sie importieren den exportierten Server (siehe Kapitel (8) mit dem Hyper-V-Manager oder der PowerShell. Beim Importieren wählen Sie die Option *Virtuellen Computer kopieren* aus.

Abbildg. 11.21 Importieren eines virtuellen Domänencontrollers



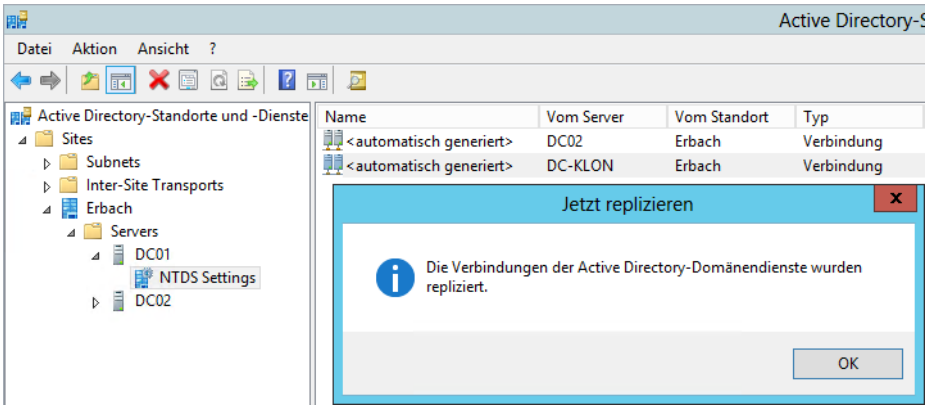
Starten Sie den Domänencontroller, liest er die Datei *DCCloneConfig.xml* ein und bereitet sich selbst für das Klonen vor. Während des Windows-Starts erhalten Sie auch eine entsprechende Meldung.

Abbildg. 11.22 Windows Server 2012 R2 klont Active Directory auf dem neuen virtuellen Domänencontroller

Melden Sie sich nach dem erfolgreichen Start an, können Sie die Domänendienste normal nutzen. Überprüfen Sie, ob sich der neue Domänencontroller in Active Directory eingebunden hat (siehe Kapitel 15). Der Domänencontroller muss in der OU *Domain Controllers* in *Active Directory-Benutzer und -Computer* eingetragen sein. Als Name verwendet der Klonvorgang den Namen, den Sie in der Datei *DCCloneConfig.xml* eingetragen haben.

Außerdem muss Windows eine Replikationsverbindung eingetragen haben. Testen Sie diese über das Kontextmenü.

Abbildg. 11.23 Überprüfen der Replikation des neuen Domänencontrollers



HINWEIS Achten Sie darauf, dass weder der Quell- noch der Ziel-DC über aktive Snapshots verfügen dürfen. Löschen Sie alle Snapshots. Sie können nach dem Klonvorgang für beide Domänencontroller neue Snapshots erstellen.

Achten Sie darauf, dass der Quell-DC ausgeschaltet ist und der PDC-Emulator der Quelldomäne verfügbar ist. Starten Sie anschließend die Ziel-VM. Diese muss eine Verbindung zum PDC-Emulator aufbauen können. Der Quell-DC darf im Netzwerk aber nicht online sein.

TIPP In der Ereignisanzeige finden Sie Einträge der IDs 29218 und 29248 bis 29266. Achten Sie außerdem auf die Quellen *Microsoft-Windows-DirectoryServices-DSROLE-Server* und *Microsoft-Windows-ActiveDirectory_DomainService*.

Domänencontroller entfernen

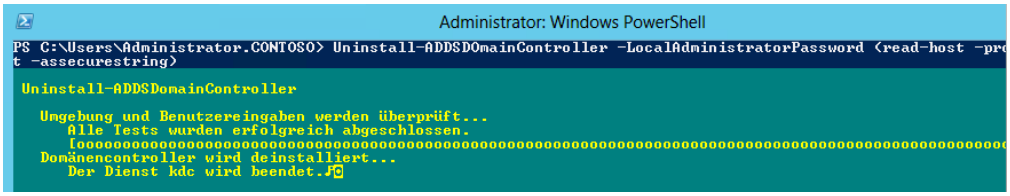
In Kapitel 15 zeigen wir Ihnen, wie Sie einen Domänencontroller in Active Directory bei einem Fehler entfernen und die Metadaten bereinigen. In Windows Server 2012 R2 können Sie dazu auch zunächst nur das Computerkonto aus der Organisationseinheit *Domain Controllers* entfernen und hier die Metadaten löschen lassen.

Herabstufen eines Domänencontrollers in der PowerShell

Ein gelöschtes Domänencontrollerkonto können Sie mit dem Active Directory-Verwaltungscenter und dem Active Directory-Papierkorb wiederherstellen (siehe Kapitel 12). Damit das funktioniert, müssen Sie den Active Directory-Papierkorb aber zunächst aktivieren. In Kapitel 12 zeigen wir Ihnen, wie Sie dazu vorgehen.

Um einen Domänencontroller herabzustufen, also von einem Domänencontroller zu einem Mitgliedsserver zu machen, verwenden Sie das Cmdlet *Uninstall-ADDSDomainController*. Mehr zu diesem Thema lesen Sie in Kapitel 15.

Abbildg. 11.24 Deinstallieren eines Domänencontrollers



Um einen Domänencontroller herabzustufen, verwenden Sie den folgenden Befehl:

```
UnInstall-ADDSDomainController -LocalAdministratorPassword (Read-Host -Prompt Kennwort
-AsSecureString
```

Über diesen Weg setzen Sie auch gleich das lokale Kennwort des Administrators. Handel es sich um den letzten Domänencontroller, verwenden Sie noch die Option *–LastDomaincontrollerInDomain*. Lesen Sie sich zu diesen Anmerkungen auch das Kapitel 15 durch. Haben Sie den Domänencontroller herabgestuft, können Sie die Active Directory-Domänendienste-Rolle ebenfalls in der PowerShell entfernen (siehe Kapitel 4). Dazu verwenden Sie zum Beispiel den folgenden Befehl:

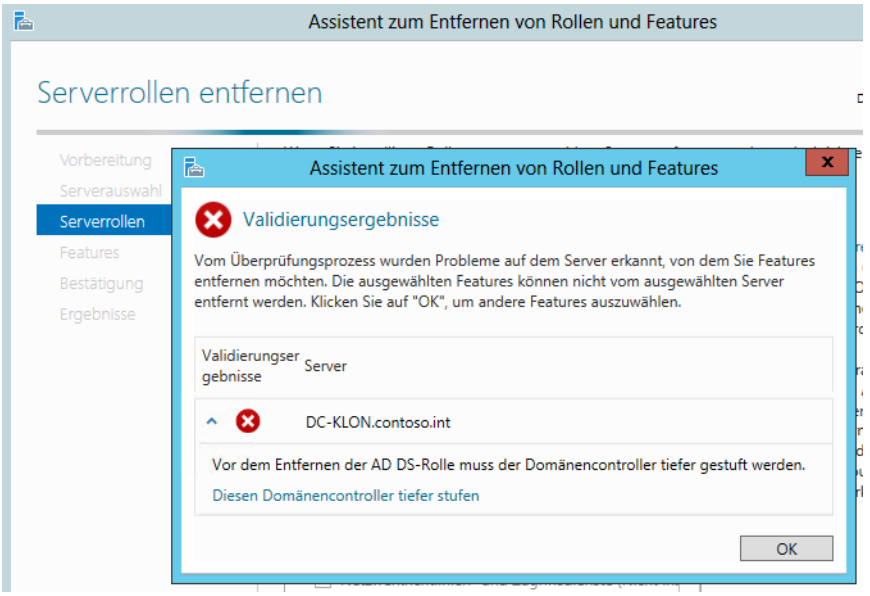
```
Uninstall-WindowsFeature AD-Domain-Services
```

Entfernen von Active Directory über den Server-Manager

Starten Sie auf einem Domänencontroller den Assistenten zum Entfernen von Rollen und Features im Server-Manager, können Sie den Domänencontroller herabstufen und die Binärdateien ebenfalls entfernen. Lesen Sie sich dazu auch das Kapitel 4 durch.

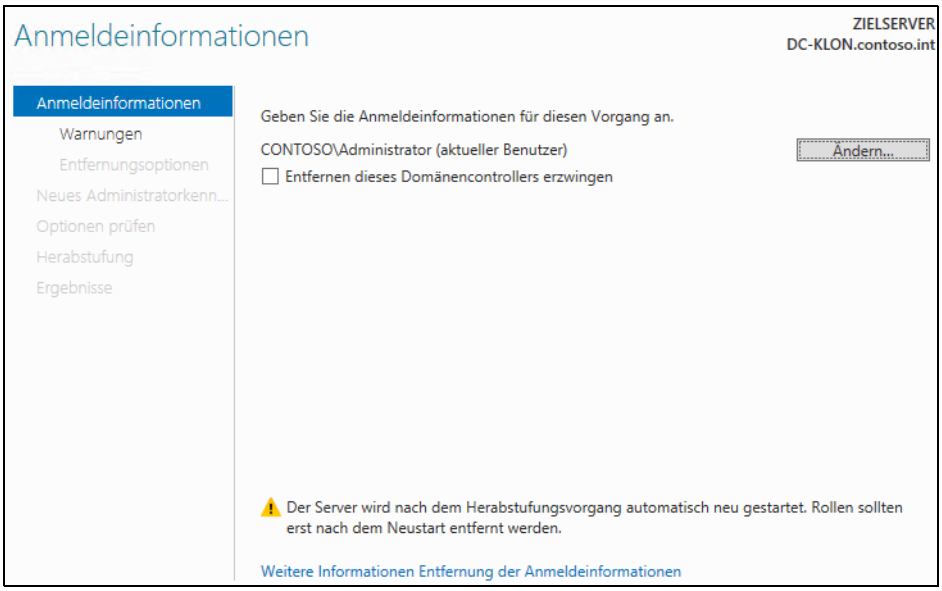
Starten Sie den Assistenten zum Entfernen und wählen Sie Active Directory-Domänendienste zum Entfernen aus. Der Assistent erkennt, dass der Server bereits zum Domänencontroller heraufgestuft wurde, und bietet eine Herabstufung über den Link *Diesen Domänencontroller tiefer stufen* an.

Abbildg. 11.25 Herabstufen eines Domänencontrollers im Server-Manager



Haben Sie den Link ausgewählt, startet der Assistent zur Herabstufung. Sie können im Fenster auswählen, ob der Server eine Verbindung zu anderen Domänencontrollern aufbauen soll, um sich herabzustufen, oder ob Sie Active Directory erzwungen vom Server entfernen wollen.

Abbildg. 11.26 Herabstufen eines Domänencontrollers



Auf der nächsten Seite des Fensters erhalten Sie Informationen, welche Rollen auf dem Server von dem Entfernen betroffen sind, vor allem, ob es sich um einen DNS-Server oder einen globalen Katalog handelt. Anschließend müssen Sie das Entfernen dieser Rollen sowie das Entfernen der DNS-Delegierung noch bestätigen. Im Assistenten legen Sie auch das neue lokale Administratorkennwort fest. Durch einen Klick auf *Tiefer stufen* entfernen Sie schließlich den Domänencontroller.

Migration zu Windows Server 2012 R2 – Active Directory

Sie können Domänencontroller mit Windows Server 2012 R2 auch in Netzwerken mit Windows Server 2003/2008/2008 R2/2012 integrieren. Dazu muss allerdings das Schema vorbereitet werden. Sie verwenden dazu das Tool Adprep von der Windows Server 2012 R2-DVD. Die Syntax dazu ist:

```
adprep /forestprep /forest <Gesamtstruktur> /userdomain <Domäne> /user <Benutzername>
/password *
```

Mit der zusätzlichen Option */logdsid* aktivieren Sie eine detailliertere Protokollierung. Die Datei *adprep.log* befindet sich im Ordner *%WinDir%\System32\Debug\Adprep\Logs*.

Der Befehl *adprep /domainprep /gpprep* wird bei der AD DS-Installation ausgeführt. Mit dem Befehl werden Berechtigungen festgelegt, die für den Richtlinienergebnissatz (Resultant Set of Policy, RSOP) wichtig sind. Wir gehen nachfolgend auf die einzelnen Vorgänge ein.

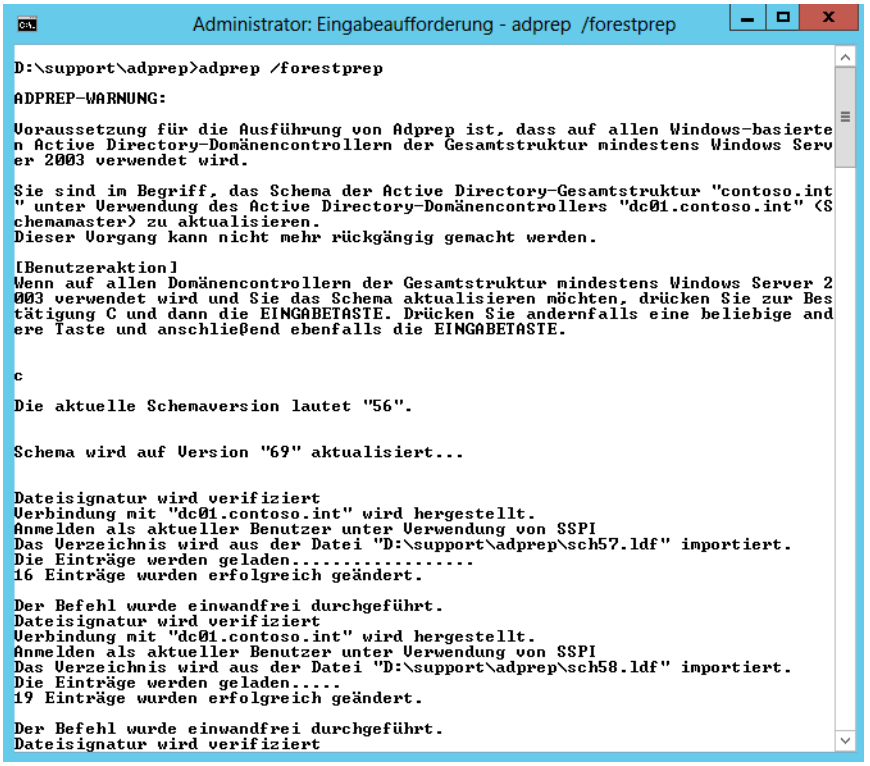
Domänen auf Windows Server 2012 R2 aktualisieren

Eine direkte Aktualisierung auf Windows Server 2012 R2 ist nur für Domänencontroller mit Windows Server 2008 x64 und Windows Server 2008 R2/2012 möglich. In Domänen mit Windows Server 2003 installieren Sie einen neuen Domänencontroller mit Windows Server 2012 R2 und entfernen die Domänencontroller mit Windows Server 2003. Achten Sie dabei aber auf die Übertragung der Betriebsmaster (siehe Kapitel 10 und 15).

HINWEIS Damit Sie Domänencontroller mit Windows Server 2012 R2 in Domänen integrieren können, müssen die Gesamtstrukturfunktionsebene und die Domänenfunktionsebene auf Windows Server 2003 oder höher gesetzt sein.

Wollen Sie Domänencontroller zu Windows Server 2012 R2 aktualisieren, müssen Sie zunächst das Schema der Gesamtstruktur erweitern. Dazu führen Sie den Befehl *adprep /forestprep* auf einem Domänencontroller aus. Sie finden das Tool im Ordner *support\adprep* auf der Windows Server 2012 R2-DVD.

Abbildg. 11.27 Erweitern des Active Directory-Schemas für Windows Server 2012 R2



Damit Sie das Schema erweitern können, müssen Sie zuvor noch mit der Taste C die Erweiterung bestätigen. Nach der Aktualisierung des Schemas müssen Sie mit *adprep /domainprep* noch die einzelnen Domänen aktualisieren. Installieren Sie neue Domänencontroller, lassen sich diese problemlos in Active Directory aufnehmen. Auch Mitgliedsserver mit Windows Server 2012 R2 können Sie in bestehende Domänen aufnehmen, wenn Domänencontroller mit Windows Server 2003/2003 R2/2008/2008 R2/2012 vorhanden sind.

Bei Migrationen können Sie Betriebsmasterrollen von Vorgängerversionen auf die neuen Domänencontroller mit Windows Server 2012 R2 übernehmen. Die Vorgänge dazu sind identisch mit der Übernahme in Windows Server 2008 R2/2012. Wie Sie dabei vorgehen, lesen Sie in Kapitel 10.

Nach der Aktualisierung der Domäne können Sie neue Domänencontroller mit Windows Server 2012 R2 in das Netzwerk integrieren oder Sie aktualisieren die bestehenden Domänencontroller direkt zu Windows Server 2012 R2. Das geht aber nur mit Windows Server 2008 x64 und Windows Server 2008 R2/2012. Mehr zu diesem Thema lesen Sie in Kapitel 2.

Abbildg. 11.28 Aktualisieren eines Domänencontrollers zu Windows Server 2012 R2

Active Directory bereinigen und Domänencontroller entfernen

Haben Sie neue Domänencontroller mit Windows Server 2012 R2 im Einsatz, wollen Sie unter Umständen die alten Server entfernen. Wie Sie dabei vorgehen, lesen Sie in diesem Abschnitt. Ein weiterer wichtiger Schritt ist das Herabstufen von Domänencontrollern in Vorgängerversionen. Achten Sie aber darauf, vorher noch einige Einstellungen zu überprüfen:

- Stellen Sie sicher, dass der Domänencontroller nicht als bevorzugter oder alternativer DNS-Server von einem anderen Rechner der Domäne verwendet wird (auch nicht als DNS-Weiterleitungsserver)
- Entfernen Sie – falls möglich – vor der Herabstufung DNS von diesem Domänencontroller. Haben Sie 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. Entfernen Sie aber nicht den Hosteintrag des Servers, da dieser für die Herabstufung noch benötigt wird.

- Stellen Sie sicher, dass der Domänencontroller nicht an irgendeiner Stelle als Domänencontroller explizit eingetragen ist, zum Beispiel auf einem Linux- oder einem anderen Server
- Entfernen Sie alle Active Directory-abhängigen Dienste wie VPN, Zertifizierungsstelle oder andere Programme, die nach der Herabstufung nicht mehr funktionieren werden
- 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* das Häkchen bei *Globaler Katalog*

Starten Sie als nächsten Schritt auf dem Server den Assistenten zum Entfernen von Active Directory über 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 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 gesamte Domäne. Nach der Herabstufung eines Domänencontrollers wird dieser als Mitgliedsserver in die Domäne aufgenommen.

Das Active Directory-Verwaltungscenter und PowerShell

Die meisten Bereiche für Routineaufgaben können Sie im Active Directory-Verwaltungscenter durchführen. Das Tool verbindet sich über die Active Directory-Webdienste mit Active Directory und stellt Routineaufgaben zur Verfügung. Microsoft hat den Funktionsumfang des Tools erweitert, zum Beispiel mit der Möglichkeit, den Active Directory-Papierkorb zu aktivieren oder die neue Active Directory-Rechteverwaltung zu verwenden.

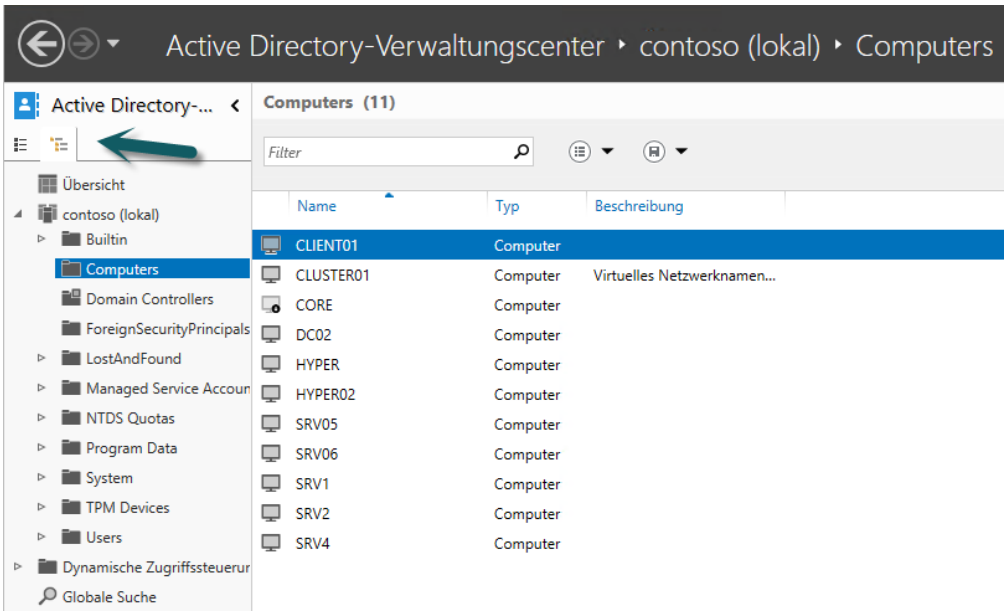
Auch in der PowerShell können Sie viele Bereiche von Active Directory verwalten. Wir zeigen Ihnen nachfolgend die wichtigsten Möglichkeiten dazu.

Wir sind im Kapitel 10 bereits auf das Thema eingegangen und zeigen auch in Kapitel 1 Neuerungen zum Active Directory-Verwaltungscenter. Im nächsten Kapitel 12 zeigen wir Ihnen ebenfalls viele wichtige Aufgaben, die Sie mit dem Active Directory-Verwaltungscenter durchführen können.

Sie starten das Active Directory-Verwaltungscenter entweder über die Programmgruppe *Tools* im Server-Manager oder indem Sie *dsac* auf der Startseite eintippen. Auf der linken Seite der Konsole navigieren Sie durch die Domäne und die Organisationseinheiten. Im linken oberen Bereich können Sie die Ansicht anpassen.

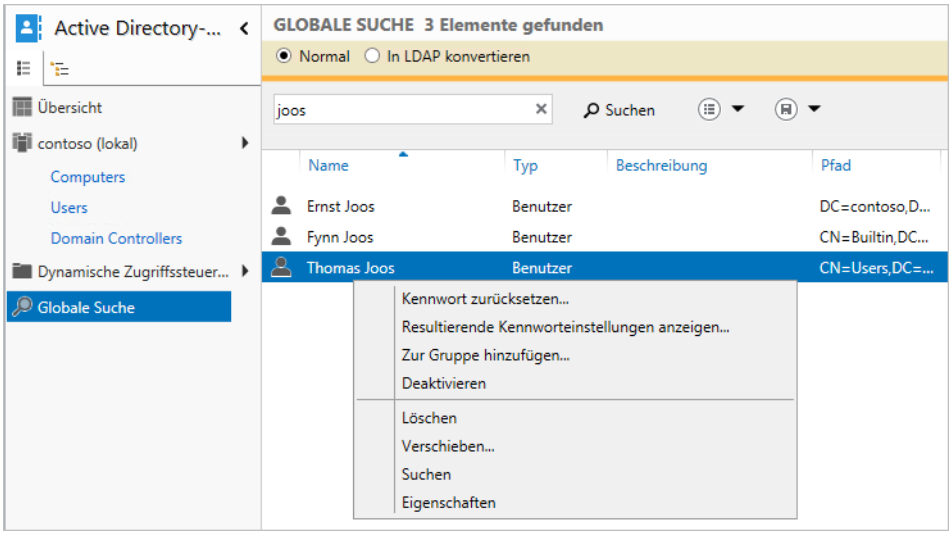
Verwenden Sie die linke Ansicht, verhält sich die Navigation ähnlich zum alten Startmenü. Sie können beim Einblenden einer Organisationseinheit den Inhalt dieser OU auf das Startfenster des Verwaltungscenters anheften, sodass dieser Bereich dauerhaft im Verwaltungscenter erscheint, ohne dass Sie erst zu der jeweiligen OU navigieren müssen. Auf diese Weise erreichen Sie wichtige Bereiche der Domäne schneller. Über den Pinn können Sie den Vorgang auch wieder rückgängig machen. Sie müssen dazu die Listenansicht aktivieren und können die entsprechende OU aufklappen und dann anpinnen.

Abbildg. 11.29 Ändern der Ansicht im Active Directory-Verwaltungscenter



Über die Kategorie *Globale Suche* können Sie in allen Domänen der Gesamtstruktur suchen, unabhängig von der Domäne, mit der Sie aktuell verbunden sind.

Abbildg. 11.30 Suchen nach Objekten

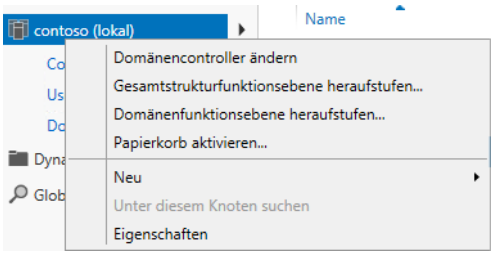


Direkt auf der Startseite (Kategorie *Übersicht*) können Sie häufige Aufgaben durchführen wie das Zurücksetzen eines Benutzerkennworts oder das Durchsuchen von Active Directory. Sie können die Seite *Verwaltungscenter – Übersicht* jederzeit durch Anzeigen oder Ausblenden verschiedener Fenster anpassen.

Wenn Sie das Active Directory-Verwaltungscenter öffnen, wird die Domäne, an der Sie derzeit auf diesem Server angemeldet sind, im linken Bereich des Active Directory-Verwaltungscenters angezeigt. Auch Domänen, die nicht zu derselben Gesamtstruktur wie die lokale Domäne gehören, können Sie anzeigen und verwalten, wenn diese über eine Vertrauensstellung verfügen. Sowohl unidirektionale als auch bidirektionale Vertrauensstellungen werden unterstützt.

In der Listenansicht können Sie Spalten anzeigen, die mehr Informationen anzeigen als das Snap-In *Active Directory-Benutzer und -Computer*. Sie können den Navigationsbereich des Active Directory-Verwaltungscenters jederzeit anpassen, indem Sie verschiedene Container aus jeder beliebigen Domäne als separate Knoten hinzufügen. Sie können Ihre Active Directory-Domänen über verschiedene Domänencontroller verwalten. Dazu klicken Sie die Domäne mit der rechten Maustaste an und wählen *Domänencontroller ändern* an. Über diesen Weg ändern Sie auch die Funktionsebene von Gesamtstruktur und Domäne und aktivieren den Active Directory Papierkorb für die entsprechende Gesamtstruktur.

Abbildg. 11.31 Verwalten von Domänen und Gesamtstrukturen



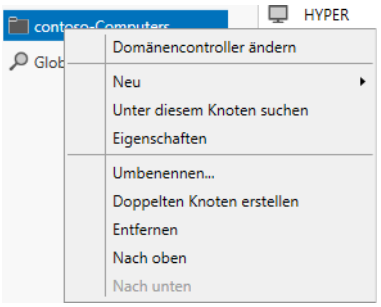
Klicken Sie auf *Verwalten/Navigationsknoten hinzufügen* und im daraufhin geöffneten Fenster rechts unten auf den Link *Verbindung mit anderen Domänen herstellen*. Tippen Sie in das Feld *Verbindung herstellen* den Namen der Domäne ein, die Sie zusätzlich verwalten wollen. Wählen Sie die Container aus, die dem Navigationsbereich hinzugefügt werden sollen.

TIPP Sie können das Active Directory-Verwaltungscenter auch mit unterschiedlichen Anmeldeinformationen öffnen, indem Sie den Befehl *runas /user:<Domäne\Benutzerkonto> dsac* verwenden, zum Beispiel über eine Verknüpfung. Vor dem Start erscheint dann ein Fenster, in dem Sie das Kennwort für das Konto eingeben.

Zur Anpassung des Navigationsbereichs können Sie manuell Knoten hinzufügen, umbenennen oder entfernen, Duplikate dieser Knoten erstellen oder sie im Navigationsbereich nach oben oder unten verschieben. Klicken Sie mit der rechten Maustaste auf den Knoten, den Sie ändern möchten. Sie können die Position oder den Namen des Knotens ändern oder den Knoten duplizieren.

Die Liste der zuletzt verwendeten Objekte wird automatisch unter einem Navigationsknoten angezeigt, wenn Sie mindestens einen Container innerhalb dieses Navigationsknotens besuchen. Für jeden Navigationsknoten können Sie einen bestimmten Domänencontroller konfigurieren.

Abbildg. 11.32 Bearbeiten hinzugefügter Knoten



Benutzerkonten in Active Directory mit Z-Hire und Z-Term anlegen und löschen

Administratoren, die häufig Benutzerkonten erstellen und an Exchange, Lync oder Office 365 anbinden müssen, können mit Zusatztools oft weitaus besser und effizienter arbeiten, als mit Bordmitteln oder der PowerShell.

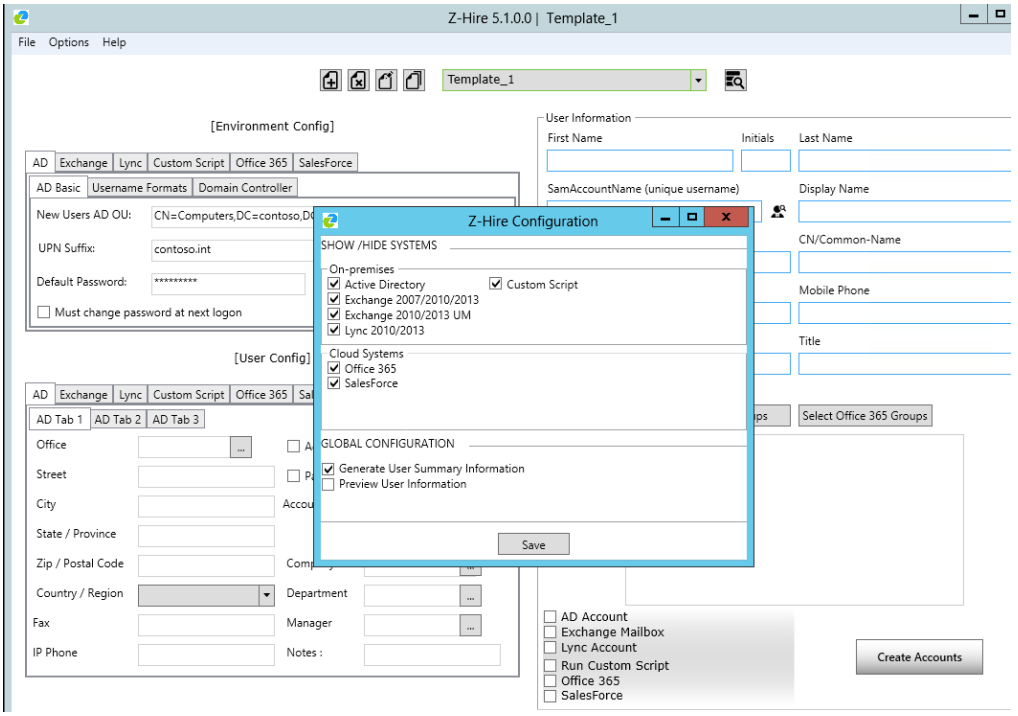
Wir zeigen Ihnen die kostenlosen Tools *Z-Hire* und *Z-Term*. Mit diesen Werkzeugen lassen sich schnell und einfach Benutzerkonten anlegen und pflegen sowie die Zusatzattribute verwalten, die Exchange, Lync und Office 365 notwendig machen. Arbeiten Sie mit delegierten Rechten in Active Directory und Exchange, können Sie mit dem Tool auch Anwendern und untergeordneten Administratoren notwendige Werkzeuge kostenlos an die Hand geben.

Benutzer anlegen mit Z-Hire

Z-Hire steht über Microsoft TechNet auf der Seite *http://gallery.technet.microsoft.com/Z-Hire-Employee-Provisionin-e4854d6b* [Ms179-K11-07] zum Download bereit. Hier finden Sie auch die jeweils aktuellste Version. Microsoft entwickelt das Tool ständig weiter. Im Archiv von Z-Hire finden Sie auch das Tool Z-Term, mit dem Sie Benutzerkonten in Active Directory löschen und anpassen können. Die Tools sind für die Automatisierung der Benutzerverwaltung optimiert und werden daher voneinander getrennt. Das heißt, Sie können delegieren, welche Administratoren Benutzerkonten erstellen und welche Administratoren Konten anpassen und löschen dürfen. Die Einstellungen der Tools lassen sich in XML-Dateien festlegen; eine Installation der Werkzeuge ist nicht notwendig. Das heißt, Sie können die Programme auch mobil zum Beispiel über einen USB-Stick nutzen.

Z-Hire unterstützt Sie beim Anlegen von neuen Benutzerkonten in Active Directory. Zusätzlich können Sie mit dem Tool auch Exchange-Konten anlegen, Benutzerkonten an Lync anbinden, Konten für Office 365 verwalten und auch Salesforce-Cloud-Konten anlegen und verwalten. Sie haben auch die Möglichkeit, Vorlagen zu erstellen und auf deren Basis dann neue Benutzerkonten anzulegen. In den Vorlagen können Sie wiederkehrende Einstellungen speichern und auf diese Weise noch schneller Benutzerkonten anlegen. Um das Tool zu nutzen, muss der entsprechende Anwender oder Administrator Benutzerkonten, Exchange-Konten und, falls vorhanden, Lync-Konten anlegen dürfen.

Abbildg. 11.33 Mit Z-Hire legen Sie Benutzerkonten in Active Directory an



Um Z-Hire zu nutzen, müssen Sie das Tool nicht installieren. Sie entpacken das Archiv und rufen die Startdatei auf. Sie können das Tool auch auf Arbeitsstationen einsetzen, wobei diese allerdings Mitglied in Active Directory sein müssen. Anschließend füllen Sie die notwendigen Felder aus, um das Benutzerkonten zu erstellen.

Über den Bereich *Options* können Sie Einstellungen für Z-Hire vornehmen. Im oberen Bereich legen Sie Vorlagen an, auf deren Basis Sie wiederum Benutzerkonten erstellen können. Es ist aber nicht notwendig, mit Vorlagen zu arbeiten, Sie können jederzeit auch ohne Vorlagen Benutzerkonten erstellen. Einstellungen speichern Sie in der dazugehörigen XML-Datei über *File/Save configuration*.

Auf diese Weise können Sie das Tool auch im Netzwerk verteilen und immer auf die gleichen Einstellungen zugreifen. Legen Sie Benutzerkonten an, haben Sie auch die Möglichkeit, Kennwörter für die neuen Konten vorzugeben. Außerdem können Sie festlegen, dass Benutzer bei der ersten Anmeldung ihr Kennwort ändern müssen. Haben Sie alle notwendigen Daten für das neue Benutzerkonto angelegt, klicken Sie auf *Create Accounts*. Fehlen Daten, erhalten Sie einen entsprechenden Hinweis angezeigt. Kann Z-Hire das Benutzerkonto anlegen, erscheint im unteren Bereich des Fensters die Meldung *Completed*. Mehr ist nicht zu tun, um ein neues Konto anzulegen.

Über die Registerkarten *AD, Exchange, Lync, Custom Script, Office 365* und *Salesforce* legen Sie zentral fest, welche Einstellungen den neuen Benutzerkonten mitgegeben werden sollen. Es bietet sich an, mit verschiedenen Vorlagen zu arbeiten und diesen auch Namen zuzuweisen. Um neue Konten mit bestimmten Einstellungen anzulegen, müssen Sie über das Menü die entsprechende Vorlage auswählen. Mit der Vorlage gespeicherte Eingaben werden dann automatisch geladen und Sie müssen nur noch die Einstellungen für das entsprechende Benutzerkonto anpassen.

Z-Hire kann fast alle Standarddaten von Benutzerkonten in Vorlagen speichern und auch die Active Directory-Gruppen auslesen. Das heißt, Sie können auch Vorlagen anlegen, in denen festgelegt ist, in welchen Sicherheitsgruppen die neuen Konten Mitglied sein sollen. Die Vorlagen können Sie über *Options* an Ihre Vorstellungen anpassen und umbenennen.

Seine eigenen Einstellungen speichert Z-Hire in der Datei *Z-Hire.exe.config*. Die Vorlagen sind in der Datei *ZHi-reV5Settings.xml* abgelegt. Diese Daten befinden sich alle im gleichen Verzeichnis wie die EXE-Datei. Sie können also nach der ersten Einrichtung Z-Hire auch auf mehreren Rechnern nutzen und durch Kopieren sogar die gleichen Einstellungen nutzen.

Mit Z-Hire können Sie lediglich Benutzerkonten anlegen. Es besteht keine Möglichkeit, Einstellungen für vorhandene Benutzerkonten zu ändern oder Konten zu löschen. Das Tool eignet sich daher optimal dazu, das Anlegen von neuen Benutzerkonten in Unternehmen zu delegieren. Die Einarbeitung erfolgt sehr schnell, da das Tool sehr intuitiv ist. Darüber hinaus lässt sich Z-Hire sehr umfassend an die eigenen Bedürfnisse anpassen und durch Kopieren schnell und einfach zwischen Anwendern und Administratoren verteilen, inklusive der vorhandenen Vorlagen.

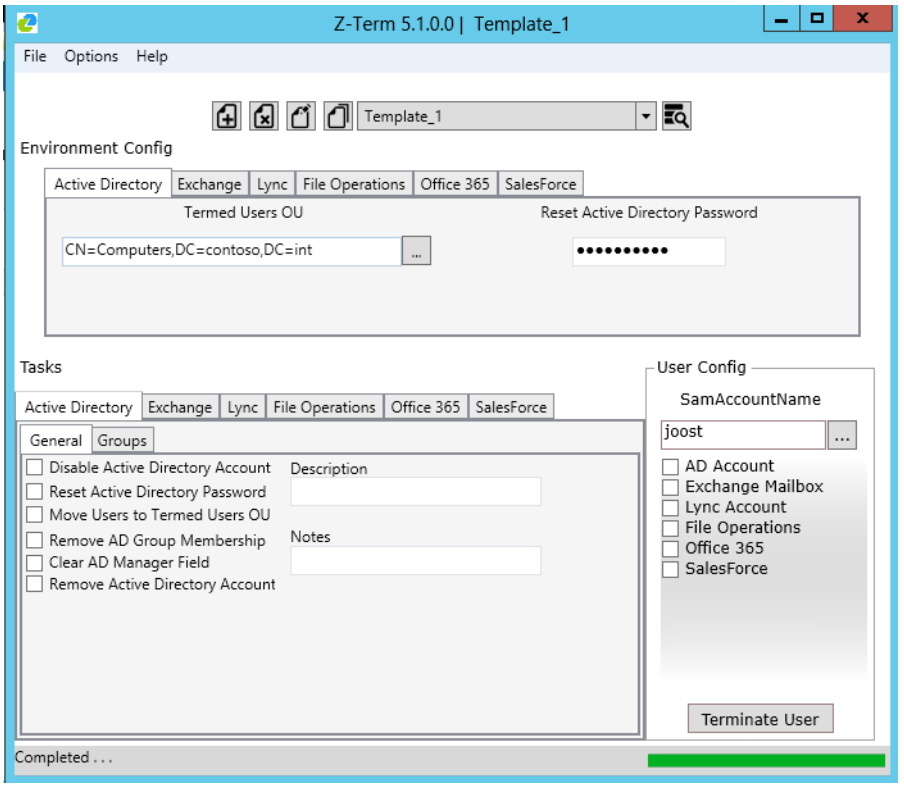
Benutzer anpassen und löschen mit Z-Term

Im Lieferumfang des Downloadarchivs finden Sie auch das Tool Z-Term. Dieses starten Sie auf dem gleichen Weg wie Z-Hire. Mit Z-Term können Sie keine Benutzerkonten anlegen, aber Einstellungen ändern und Konten löschen oder deaktivieren. Nachdem Sie im oberen Bereich die Organisationseinheit und im Bereich *User config* das zu bearbeitende Benutzerkonto ausgewählt haben, können Sie im Bereich *Tasks* festlegen, was mit dem Benutzerkonto geschehen soll.

Neben der Möglichkeit, das Benutzerkonto zu löschen, können Sie auch Konten deaktivieren, Kennwörter ändern, Mitgliedschaften in Gruppen ändern und weitere Einstellungen für Active Directory, Exchange, Lync, Office 365 und SalesForce anpassen. Deaktivieren Sie Benutzerkonten, können Sie die entsprechenden Konten automatisch mit Z-Term in eine vorgegebene Organisationseinheit (Organizational Unit, OU) verschieben.

Haben Sie die gewünschten Aktionen ausgewählt, klicken Sie auf *Terminate User*, um diese in Active Directory zu speichern. Löschen Sie ein Benutzerkonto, können Sie auf der Registerkarte *File Operations* Dateien des Benutzerkontos in andere Ordner sichern. Hier haben Sie die Möglichkeit, die Exchange-Einstellungen in eine PST-Datei zu exportieren, ein Skript ausführen zu lassen und den Home-Ordner sowie das servergespeicherte Profil des Anwenders zu kopieren.

Abbildg. 11.34 Mit Z-Term verwalten Sie Benutzerkonten in Active Directory



Über den Bereich *Tasks* und den dazugehörigen Registerkarten rufen Sie die verschiedenen Aufgaben auf, die Z-Term zur Verfügung stellt. Bietet ein bestimmter Bereich, zum Beispiel Exchange, weitere Einstellmöglichkeiten, erscheinen unterhalb weitere Registerkarten, um die Auswahl zu verfeinern.

Im Fall von Exchange können Sie zum Beispiel auch Abwesenheitsnachrichten von Anwendern steuern, Besprechungen absagen, Berechtigungen anpassen, E-Mails automatisch weiterleiten lassen, den kompletten Inhalt des Postfaches in eine PST-Datei exportieren und vieles mehr. Ähnliche Möglichkeiten haben Sie auch bei Office 365.

Wie bei Z-Hire haben Sie auch bei Z-Term die Möglichkeit, Vorlagen zu erstellen, auf deren Basis Sie Änderungen vornehmen wollen. Die Vorlagen speichert Z-Term in der gleichen Datei wie Z-Hire, allerdings in einem eigenen Unterordner. Dies müssen Sie beim Kopieren und Verteilen im Netzwerk beachten. Die beiden Tools arbeiten zwar generell zusammen, sind von der Konfiguration her aber komplett voneinander getrennt.

Active Directory und die PowerShell

Um Active Directory-Objekte in der PowerShell abzurufen, stellt Microsoft zahlreiche neue Cmdlets zur Verfügung. Eine Liste erhalten Sie am schnellsten über den Befehl *Get-Command Get-Ad**. Um neue Objekte zu erstellen, gibt es ebenfalls zahlreiche neue Cmdlets. Die Liste dazu erhalten Sie durch Eingabe von *Get-Command New-Ad**.

Eine Liste mit Befehlen zum Löschen von Objekten zeigt die PowerShell mit *Get-Command Remove-Ad**. Änderungen an Active Directory-Objekten nehmen Sie mit Set-Cmdlets vor. Eine Liste erhalten Sie über *Get-Command Set-Ad**.

Neu im unteren Bereich des Active Directory-Verwaltungscenters ist die *Windows PowerShell History*. Diese bietet PowerShell-Befehle als Protokoll an. Dazu müssen Sie nur auf den Link klicken und sehen alle durchgeführten Aufgaben der grafischen Oberfläche als Befehl für die PowerShell. Dieses Fenster stellt aber nicht nur ein Protokoll dar, sondern Administratoren können Befehle für Skripts aus dem Fenster herauskopieren.

Ebenfalls eine wichtige Funktion in der PowerShell ist das Cmdlet *Show-Command*. Dieses blendet ein neues Fenster mit allen Befehlen ein, die in der PowerShell verfügbar sind. Sie können im Fenster nach Befehlen suchen und sich eine Hilfe zum Befehl sowie Beispiele anzeigen lassen. Außerdem können Sie hier Befehle zusammenfügen und anschließend ausführen.

Nicht alle Cmdlets eignen sich zur Remoteverwaltung von Servern. Sie können vor allem die Cmdlets nutzen, welche über die Option *-ComputerName* verfügen. Um sich alle Cmdlets anzeigen zu lassen, die diese Option unterstützen, also Server auch über das Netzwerk verwalten können, hilft der Befehl *Get-Help * -Parameter ComputerName*.

Haben Sie Active Directory installiert, stehen auch in Windows Server 2012 R2 die bekannten Tools *Dcdiag*, *Repadmin* & Co. zur Analyse zur Verfügung. Für die Namensauflösung können Sie weiterhin *Nslookup* oder die Cmdlets zur Verwaltung von DNS, zum Beispiel *Resolve-DnsName*, verwenden.

Damit Sie die Befehle ausführen können, müssen Sie an verschiedenen Stellen noch Kennwörter eingeben. Diese akzeptiert das entsprechende Cmdlet aber nur als sichere Eingabe. Ein Beispiel für den Befehl ist:

```
Test-ADDSDomainControllerInstallation -Domainname <DNS-Name der Domäne> -
SafeModeAdministratorPassword (read-host -prompt Kennwort -assecurestring)
```

Um zum Beispiel einen neuen Domänencontroller zu installieren, verwenden Sie das Cmdlet *Install-ADDSDomainController*. Damit der Befehl funktioniert, geben Sie den Namen der Domäne an und konfigurieren das Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus als SecureString. Dazu verwenden Sie folgenden Befehl:

```
Install-ADDSDomainController -Domainname <DNS-Name der Domäne> -
SafeModeAdministratorPassword (read-host -prompt Kennwort -assecurestring)
```

Der Befehl fragt nach dem Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus und speichert dieses als sichere Zeichenfolge ab. Sie können natürlich alle notwendigen Optionen für die Installation im Cmdlet angeben, zum Beispiel noch die Installation von DNS oder die Funktionsebene von Domäne und Gesamtstruktur. Dazu verwenden Sie zum Beispiel die Befehle:

```
-ForestMode <{Win2003 | Win2008 | Win2008R2 | Win2012}>
-DomainMode <{Win2003 | Win2008 | Win2008R2 | Win2012}>
-InstallDNS <{$false | $true}>
-SafeModeAdministratorPassword <secure string>
```

Domänencontroller können Sie auch in der PowerShell an neue Standorte verschieben:

```
Get-ADDomainController <Name des Servers> | Move-ADDirectoryServer -Site <Name des
Standorts>
```

Sie können die Replikationsverbindungen auch in der PowerShell anzeigen. Dazu verwenden Sie den Befehl *Get-AdReplicationConnection*. Außerdem können Sie in der PowerShell auch ausführliche Informationen zu den einzelnen Standorten anzeigen lassen. Dazu verwenden Sie den Befehl *Get-ADReplicationSite -Filter **. Um sich nur den Namen anzeigen zu lassen, verwenden Sie *Get-ADReplicationSite -Filter * | ft Name*, eine Liste der Domänencontrollern und Standorten erhalten Sie mit *Get-ADDomainController -Filter * | ft Hostname,Site*.

Falls Replikationsprobleme in Active Directory auftreten, sollten Sie zunächst sicherstellen, dass die Domänencontroller, die Probleme bei der Replikation haben, für den richtigen Standort konfiguriert sind. Zu diesem Weg geben Sie in der Eingabeaufforderung den Befehl *Nltest /dsgetsite* ein. In der Anzeige sehen Sie, welchem Standort der Domänencontroller zugewiesen ist und ob er seinen Standort auch erkennt.

Objekte schützen und wiederherstellen

In Windows Server 2012 R2 sind Active Directory-Objekte vor dem versehentlichen Löschen geschützt. Dieser Schutz ist standardmäßig aktiviert. Nachdem Sie über das Menü *Ansicht* in *Active Directory-Benutzer und -Computer* die erweiterte Ansicht aktiviert haben, finden Sie auf der Registerkarte *Objekt* das Kontrollkästchen *Objekt vor zufälligem Löschen schützen* vor.

Diese Option steuert die Berechtigungen auf der Registerkarte *Sicherheit*. Der Gruppe *Jeder* wird der Eintrag *Löschen* verweigert. Dies äußert sich darin, dass ein Administrator vor dem Löschen eines solchen geschützten Objekts zunächst das Kontrollkästchen zu dieser Option deaktivieren muss, bevor er das Objekt löschen kann.

Den Papierkorb für gelöschte Objekte verwalten Sie in Windows Server 2012 R2 nicht mehr in der PowerShell oder Eingabeaufforderung, sondern können die Aktivierung und die Wiederherstellung von Objekten vollständig im Active Directory-Verwaltungscenter vornehmen.

Grundlage ist der Papierkorb von Active Directory, den Sie zunächst für die Gesamtstruktur aktivieren müssen. Diesen Vorgang nehmen Sie über das Kontextmenü der Gesamtstruktur auf der linken Seite der Konsole im Active Directory-Verwaltungscenter vor. Sie können den Papierkorb nur dann aktivieren, wenn die Funktionsebene der Gesamtstruktur auf Windows Server 2008 R2 gesetzt ist.

Um gelöschte Objekte wiederherzustellen, verwenden Sie am besten das Active Directory-Verwaltungscenter in Windows Server 2012 R2. Vorteil ist, dass Ihnen eine grafische Oberfläche zur Verfügung steht. Nachdem Sie den Papierkorb aktiviert und das Active Directory-Verwaltungscenter neu gestartet haben, ist für die entsprechende Gesamtstruktur ein neuer Ordner *Deleted Objects* vorhanden.

Benutzer-Fotos in Active Directory, Lync und Exchange integrieren

Unternehmen, bei denen Anwender über Exchange, VoIP-Telefone, Lync, Outlook und anderen Programmen kommunizieren, profitieren davon, wenn Fotos der Benutzer in Active Directory hinterlegt sind. Fotos sehen Anwender in Exchange zum Beispiel zusätzlich in der globalen Adressliste, wenn Sie Exchange Server 2010/2013 einsetzen. In Outlook und auch im Lync-Client sowie an einer Vielzahl weiterer Stellen sind ebenfalls Fotos zu sehen.

Der Vorgang, Fotos zu hinterlegen, ist vor allem dann interessant, wenn mehrere Kommunikationsinstrumente im Unternehmen eingesetzt werden, die auf Active Directory aufbauen. Outlook kann zum Beispiel Fotos genauso anzeigen wie Lync und die meisten VoIP-Telefone. Bereits beim Einsatz von Exchange kann sich der Einsatz lohnen. Auch in Outlook Web App lassen sich über diesen Weg Fotos anzeigen.

Durch die Integration von Fotos in Active Directory können Anwender E-Mails und Kontakte zügiger und leichter zuordnen, da sie die Personen wesentlich schneller erkennen können.

Fotos lassen sich dazu als Attribut in Active Directory ablegen. Die Fotos werden dann auch über die Replikation der Active Directory-Datenbank repliziert und sind domänenweit verfügbar. Dieser Vorgang lässt sich mit der Freeware *AD Photo Edit*, aber auch mit Bordmitteln recht einfach umsetzen. Wir zeigen Ihnen nachfolgend beide Wege. Laden Sie dazu das Tool von der Seite *http://www.cjwdev.co.uk/Software/ADPhotoEdit/Download.html* [Ms179-K11-08] herunter und installieren es auf einem Computer, der Mitglied der Domäne ist.

Abbildg. 11.35 Hinzufügen von Fotos zu einem Active Directory-Benutzer mit AD Photo Edit

Starten Sie das Tool und geben Sie den Benutzernamen des Benutzers ein, für den Sie ein Foto hinterlegen möchten. Sie können auf Wunsch auch mehreren Benutzern gleichzeitig ein Foto zuweisen. Haben Sie das Benutzerkonto gefunden, können Sie mit *Edit Image* ein Bild zuordnen. Achten Sie darauf, dass Sie Fotos mit einer Größe von 96x96 Pixel verwenden. Neue Anwendungen wie Lync 2013 beherrschen zwar auch höhere Auflösungen. Allerdings müssen Sie zusätzlich beachten, dass die Daten in Active Directory gespeichert werden und sich dadurch das Datenvolumen der Active Directory-Datenbanken erhöht.

Damit die Fotos angezeigt werden, müssen Sie warten, bis Exchange die globale Adressliste überarbeitet hat. Über *Tools/Options* legen Sie die Domäne fest, in die Sie Fotos integrieren wollen. Außerdem steuern Sie hier den Benutzernamen und das Kennwort des Anwenders, mit dem das Tool die Änderungen durchführen kann.

Sie haben zusätzlich die Möglichkeit, gespeicherte Fotos wieder zu exportieren. Auch dazu steht eine Schaltfläche im Tool zur Verfügung. Mehr ist nicht notwendig, Sie müssen lediglich die Replikation von Active Directory abwarten.

Lync Server 2013 ermöglicht zusammen mit Exchange Server 2013 und dem aktuellen Lync Client 2013 die Speicherung hochauflösender Fotos direkt im Exchange-Speicher. Hochauflösende Fotos können Benutzer mit Outlook Web App hochladen. Benutzer können aber nur ihre eigenen Fotos aktualisieren. Sie können mit der Exchange-Verwaltungsshell die Fotos aller Benutzer aktualisieren. Verwenden Sie dazu die folgende Befehlsfolge:

```
$photo = ([Byte[]] $(Get-Content -Path "e:\Photos\joos.jpg" -Encoding Byte -ReadCount 0))
Set-UserPhoto -Identity "Thomas Joos" -PictureData $photo -Confirm:False
Set-UserPhoto -Identity "Thomas Joos" -Save -Confirm:False
```

Damit ein hochgeladenes Foto dem Benutzerkonto zugewiesen wird, muss der Benutzer in den Optionen das Bild noch speichern. Um als Administrator das Foto beispielsweise dem Benutzerkonto von Thomas Joos zuzuweisen, verwenden Sie als Befehl:

```
Set-UserPhoto -Identity "Thomas Joos" -Save -Confirm:False
```

Um zu prüfen, ob das neue Foto dem Benutzerkonto zugewiesen wurde, meldet sich der Benutzer in Lync an und lässt sich sein Bild anzeigen.

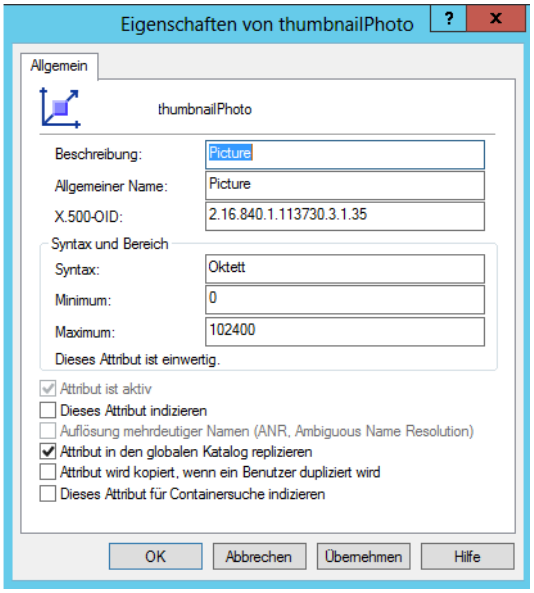
In Exchange ohne Lync können Sie, neben AD Photo Edit, ebenfalls die Exchange-Verwaltungsshell nutzen, um Anwendern ein Bild zuzuordnen. Dazu verwenden Sie das Cmdlet *Import-RecipientDataProperty*. Das Cmdlet bearbeitet das Attribut *thumbnailPhoto* in Active Directory.

Dieses sehen Sie auch im Snap-In *Active Directory-Benutzer und -Computer*, wenn Sie über *Ansicht/Erweiterte Features* alle Ansichten aktivieren. Rufen Sie einen Benutzer auf und wechseln Sie zur Registerkarte *Attribut-Editor*. Im unteren Bereich sehen Sie das Attribut *thumbnailPhoto*. Ist das Attribut leer, haben Sie dem Benutzer kein Foto zugewiesen. Wenn Sie mit Fotos arbeiten, sollten Sie dieses Attribut durch die globalen Kataloge replizieren lassen. Dazu rufen Sie das Snap-In *Active Directory-Schema* auf und dann die Eigenschaften des Attributs *thumbnailPhoto*.

Damit Sie das das Schema anpassen und verwalten können, müssen Sie zunächst das Snap-In registrieren, welches das Schema anzeigt. Aus Sicherheitsgründen wird dieses Snap-In zwar installiert, jedoch nicht angezeigt. Durch Eingabe des Befehls *Regsvr32 schmm-gmt.dll* in der Eingabeaufforderung, wird die Konsole verfügbar gemacht.

Über den Aufruf von *mmc.exe* und der Auswahl von *Datei/Snap-In hinzufügen/Active Directory-Schema* können Sie das Schema jetzt verwalten. Klicken Sie auf *Attribute* und rufen Sie die Eigenschaften von *thumbnailPhoto* auf. Achten Sie darauf, dass die Option *Attribut in den globalen Katalog replizieren* aktiviert ist.

Abbildg. 11.36 Sie können Attribute wie Benutzerfotos in den globalen Katalog integrieren



Zeitsynchronisierung in Windows-Netzwerken

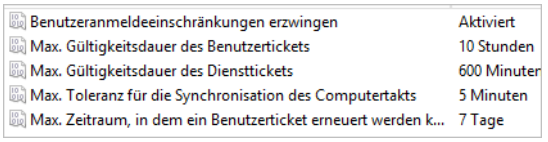
Administratoren, die mehrere Server und verschiedene Arbeitsstationen im Netzwerk verwalten, müssen vor allem beim Einsatz in Active Directory auf die Zeitsynchronisierung achten. Während sich alleinstehende Rechner direkt mit einer Zeitquelle im Internet oder einer Funkuhr synchronisieren können, arbeiten Windows-Rechner in einem Netzwerk zusammen, vor allem beim Einsatz von Active Directory. Die Konfiguration des Zeitdiensts in Windows ist nur über die Registry oder das Befehlszeilentool W32tm möglich. Eingeschränkte Möglichkeiten bietet auch der Befehl *net time*. Es steht allerdings keine grafische Oberfläche für die Konfiguration zur Verfügung. Wie Sie dabei vorgehen, lesen Sie in den nächsten Abschnitten.

Grundlagen der Zeitsynchronisierung in Active Directory

In Active Directory sollten die Uhren der Rechner und Server nicht mehr als fünf Minuten voneinander abweichen. Da Active Directory bei der Authentifizierung mit Kerberos arbeitet, ein System das stark auf Tickets, Zeitstempel und damit gültige Uhrzeiten aufbaut, besteht die Gefahr, dass Authentifizierungsaufgaben nicht funktionieren, wenn die Uhren einzelner Rechner mehr voneinander abweichen.

Standardmäßig toleriert Kerberos in Active Directory eine Zeitdifferenz von 5 Minuten. Diese Einstellungen sollten Sie nicht ändern, haben aber die Möglichkeit dazu. Sie müssen für diese Änderung die Gruppenrichtlinie der entsprechenden Computer anpassen. Navigieren Sie dazu zu *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Kontorichtlinien/Kerberos-Richtlinie*. Hier finden Sie die verschiedenen Einstellungen für die Gültigkeit der Tickets.

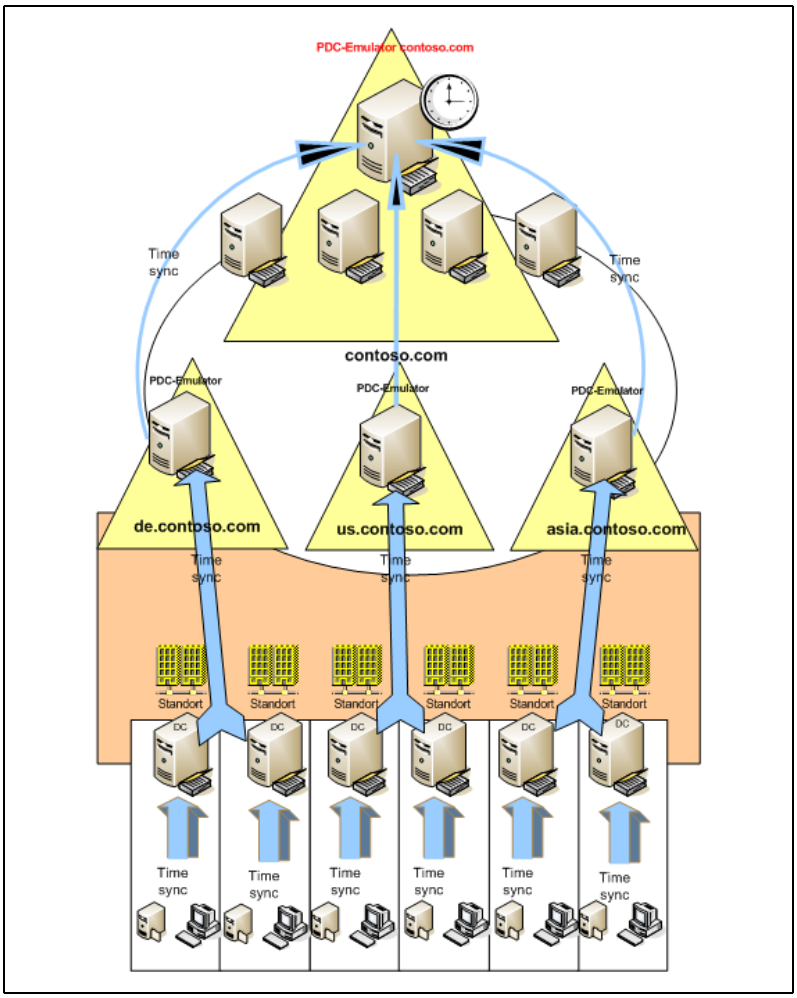
Abbildg. 11.37 Gruppenrichtlinien-Einstellung für die Gültigkeit von Kerberos-Tickets



Der PDC-Master einer Active Directory-Domäne ist der autorisierende Zeitserver der Domäne und für die Uhrzeiten aller anderen Domänencontroller, Mitgliedsserver und Arbeitsstationen in der Gesamtstruktur verantwortlich (siehe Kapitel 10). Alle Domänencontroller einer Domäne synchronisieren ihre Zeit mit dem PDC-Emulator der eigenen Domäne. Zum Synchronisieren der Zeit verbindet sich der Client oder Mitgliedsserver mit dem Domänencontroller, an dem er sich an der Domäne anmeldet.

Setzen Sie im Unternehmen eine verschachtelte Struktur mit mehreren Domänen ein, synchronisieren sich die einzelnen PDC-Master der Domänen jeweils mit dem PDC-Master der übergeordneten Domäne. Der PDC-Master der Stammdomäne ist schließlich der Server, von dem sich alle anderen Server die Zeit holen. Auf diese Weise gibt es keine Schleifen bei der Konfiguration, da die Synchronisierung der Uhrzeit genau festgelegt ist. Hierarchisch geht es vom ersten PDC-Emulator der Gesamtstruktur nach unten zu den anderen PDC-Emulatoren, den Domänencontrollern und schließlich zu den einzelnen Mitgliedsservern und Arbeitsstationen.

Abbildg. 11.38 Zeitsynchronisierung in komplexeren Active Directory-Umgebungen



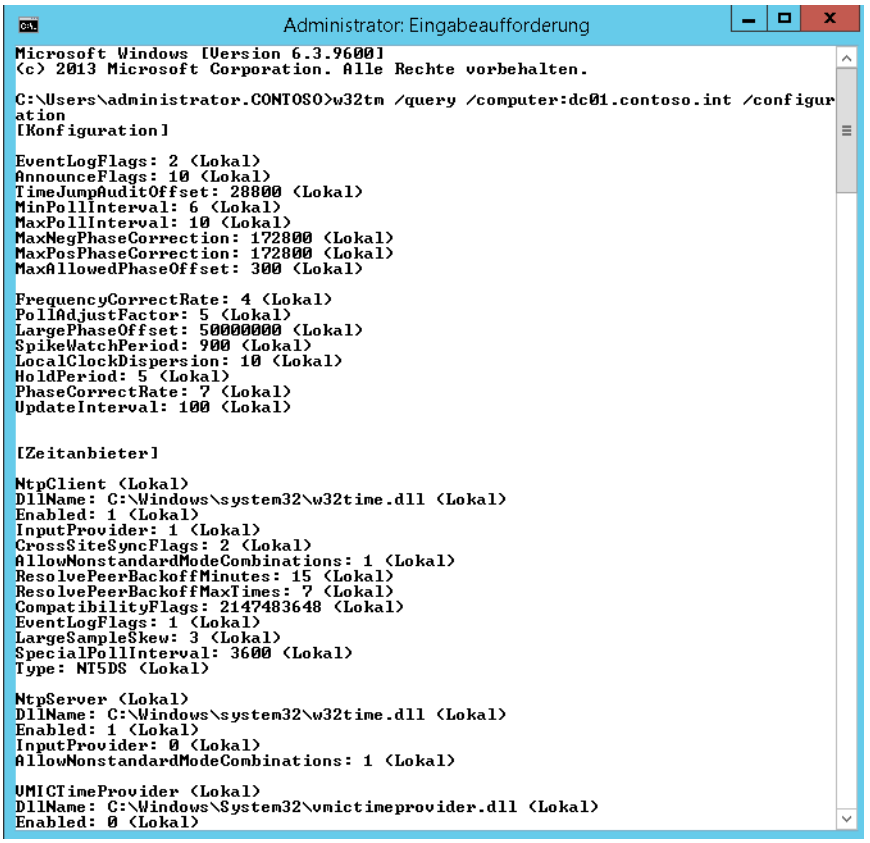
Das heißt, beim ersten Domänencontroller einer Gesamtstruktur müssen Sie darauf achten, entweder die Zeit mit dem Internet oder mit einer Funkuhr zu synchronisieren. Standardmäßig verwenden den PDC-Master die BIOS-Zeit des Rechners, wenn im Netzwerk kein übergeordneter Zeitserver oder PDC-Emulator angegeben ist. Hier können Sie natürlich von anderen Zeitquellen synchronisieren, neben Internetuhren und Funkuhren auch kompatible Layer-3-Netzwerkwitches. Wichtig ist nur die NTP-Kompatibilität des entsprechenden Geräts. Die Rolle des PDC-Emulators gibt es in jeder Active Directory-Domäne ein Mal. Der erste installierte Domänencontroller einer Active Directory-Domäne bekommt diese Rolle automatisch zugewiesen. Er ist für die Anwendung und Verwaltung der Gruppenrichtlinien zuständig und darüber hinaus für Kennwortänderungen bei Benutzern verantwortlich. Er steuert die externen Vertrauensstellungen einer Domäne und stellt den Zeitserver der Domäne zur Verfügung.

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 *dsa.msc*. Klicken Sie mit der rechten Maustaste im Snap-In auf die Domäne und wählen Sie im Kontextmenü den Eintrag *Betriebsmaster* aus. Es öffnet sich ein neues Fenster. Klicken Sie auf die Registerkarte *PDC*. Mehr zu diesem Thema lesen Sie in Kapitel 10. Sie können sich den aktuellen PDC-Emulator auch mithilfe des Befehls *dsquery server –hasfsmo pdc* in der Eingabeaufforderung anzeigen lassen.

Das NTP-Protokoll und Befehle zur Zeitsynchronisierung

Windows verwendet für die Synchronisation der Uhren das NTP-Protokoll (Network Time Protocol). Dieses Protokoll kommuniziert über den UDP-Port 123. Das heißt, dieser Port muss zwischen allen Clientcomputern und dem entsprechenden Domänencontroller geöffnet sein. Windows synchronisiert die Zeit beim Starten von Windows und in regelmäßigen Abständen automatisch mit dem Windows Time Service (WTS oder auch W32Time).

Abbildg. 11.39 Anzeigen der Zeitsynchronisierung in Netzwerken



Sie können auf einer Arbeitsstation oder einem Server einen manuellen Synchronisierungsvorgang auslösen, indem Sie in einer Eingabeaufforderung den Befehl *w32tm /resync* ausführen. Der PC oder Server verbindet sich mit seinem Zeitserver und synchronisiert die Uhrzeit. Außer der Option *resync* stehen für den W32tm-Befehl noch weitere Optionen zur Verfügung. Diese sehen Sie, wenn Sie in der Eingabeaufforderung *w32tm* eingeben. Auf der Seite *http://technet.microsoft.com/en-us/library/w32tm(WS.10).aspx* [Ms179-K11-09] erhalten Sie Informationen zu den einzelnen Optionen. Mit dem Befehl *w32tm /query /computer:<Computername> /configuration* lassen Sie sich zum Beispiel die aktuelle Konfiguration des Zeitdiensts anzeigen. Mit diesem Tool steuern Sie alle Zeiteinstellungen.

Achten Sie vor allem auf Domänencontrollern darauf, dass in der Ereignisanzeige unter *System* keine Fehlermeldungen der Quelle *W32Time* stehen. Bei regelmäßigen Fehlern deutet das darauf hin, dass der Domänencontroller Probleme hat, die Zeit mit seinem PDC-Emulator zu synchronisieren.

Der beste Weg, die Zeit des obersten PDC-Emulators aktuell zu halten, ist ein Zeitserver im Internet, zum Beispiel die Zeitserver der Technischen Universität in Braunschweig. Diese erreichen Sie über die Servernamen *ptbtime1.ptb.de, ptbtime2.ptb.de* und *ptbtime3.ptb.de*. Auf der Seite *http://www.pool.ntp.org* [Ms179-K11-10] finden Sie eine Liste zahlreicher Zeitserver im Internet.

Standardmäßig konfigurieren sich Windows-Rechner automatisch mit Domänencontrollern, sobald diese Mitglied einer Domäne sind. Der Client oder Mitgliedsserver verbindet sich dazu mit dem Domänencontroller, an dem er sich an der Domäne anmeldet, zum Synchronisieren der Zeit. Sie können mit dem Befehl *w32tm /config /syncfromflags:domhier /update* diese Synchronisierung nachträglich aktivieren, wenn diese nicht funktioniert oder Sie diese ausgeschaltet haben. Anschließend müssen Sie auf dem Computer aber den Zeitdienst neu starten. Verwenden Sie dazu zum Beispiel die beiden folgenden Befehle:

```
net stop w32time
net start w32time
```

Das Windows-Server-Team pflegt für technische Tipps zum Zeitdienst auch einen eigenen Blog, den Sie auf der Seite *http://blogs.msdn.com/b/w32time* [Ms179-K11-11] erreichen.

Net Time versus W32tm

Alle Zeiteinstellungen auf einem Server oder einem Mitgliedscomputer nehmen Sie mit dem Tool W32tm in der Eingabeaufforderung vor. Zusätzlich können Sie auch noch mit *net time* in der Eingabeaufforderung verschiedene Aufgaben durchführen. Der Befehl *net time* ist allerdings ein komplett unabhängiger Mechanismus zu W32tm und ermöglicht zum Beispiel die Zeitabfrage von Remotecomputern im Netzwerk. Das geht zwar auch mit W32tm, ist aber komplizierter und funktioniert weniger zuverlässig, vor allem wenn Ports geschlossen sind.

Net ist ein Tool im *System32*-Ordner von Windows, welches verschiedene Aufgaben im Netzwerk steuert, zum Beispiel auch das Verbinden von Netzlaufwerken (*net use * \\<Freigabe>*). Wollen Sie die Uhrzeit eines Servers im Netzwerk anzeigen, verwenden Sie den Befehl *net time \\<Servername>*. Die Verbindung erfolgt dabei über das RPC-Protokoll, nicht mit NTP.

Sie können auch die lokale Zeit eines Computers mit der Zeit eines Servers im Netzwerk synchronisieren. Dazu verwenden Sie den Befehl *net time \\<Servername> /set /yes*. Der Befehl funktioniert aber nicht von alleinstehenden Servern zu Domänencontrollern aufgrund von Sicherheitsrichtlinien. Mit dem Befehl *net help time* lassen Sie sich eine ausführliche Hilfe zu *net time* anzeigen.

Abbildg. 11.40 Verwenden von *net time* zur Zeitsynchronisierung

```
C:\Users\administrator.CONTOSO>net time \\dc01 /set /yes
Aktuelle Zeit auf \\dc01 ist 07.10.2013 16:55:14.

Der Befehl wurde erfolgreich ausgeführt.
```

Rufen Sie in einer Domäne *net time* ohne Optionen auf, versucht sich der Computer mit einem Domänencontroller zu verbinden, um dessen Zeit anzuzeigen. Mit der Option */domain* können Sie die entsprechende Domäne angeben, in welcher der Client einen Domänencontroller zur Anzeige suchen soll.

Funkuhr versus Internetzeit – Zeitsynchronisierung konfigurieren

Wie bereits erläutert wurde, ist der einfachste Weg zur Zeitsynchronisierung die Verwendung einer Uhr im Internet. Das Problem bei dieser Konfiguration ist, dass der Server beim Ausfall der Internetleitung oder der entsprechenden Zeitserver seine Uhrzeit nicht mehr synchronisieren kann. Sie haben in diesem Fall aber die Möglichkeit, mit einer lokalen Uhr zu konfigurieren.

Haben Sie aber am PDC-Emulator direkt eine Funkuhr angeschlossen, die dessen BIOS-Zeit automatisch steuert, müssen Sie keine Server mit W32tm hinterlegen. In diesem Fall sollten Sie aber die Registry auf dem PDC-Emulator so anpassen, dass der Server konfiguriert ist, seine eigene BIOS-Zeit zu verwenden, keine externen Zeitserver.

Ansonsten erhalten Sie in der Ereignisanzeige des Servers verschiedene Fehler angezeigt, die darauf hinweisen, dass der Server seine Zeit nicht synchronisieren darf. Durch die folgende Konfiguration legen Sie in der Registry fest, dass der Domänencontroller ein zuverlässiger Zeitserver für alle Computer im Netzwerk ist, da er sich selbst mit einer Funkuhr synchronisiert. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie den Registrierungs-Editor und navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config*.
2. Suchen Sie den Wert *AnnounceFlags*.
3. Ändern Sie den Wert von *AnnounceFlags* auf den Wert *A* ab.
4. Starten Sie den Zeitdienst auf dem Server neu, zum Beispiel mit dem Befehl *net stop w32time* && *net start w32time*.

Gehen Sie folgendermaßen vor, um einen Domänencontroller für die Synchronisierung mit einer externen Zeitquelle zu konfigurieren:

1. Öffnen Sie durch Eingabe von *regedit* auf der Startseite den Registrierungs-Editor.
2. Navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters*.
3. Klicken Sie im rechten Bereich mit der rechten Maustaste auf *Type* und ändern Sie den Wert von *NT5DS* auf *NTP* ab.

4. Navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config*.
5. Ändern Sie den Wert *AnnounceFlags* auf den Wert *5* ab.
6. Navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer*.
7. Klicken Sie im rechten Bereich mit der rechten Maustaste auf *Enabled* und ändern Sie den Wert auf *1* ab.
8. Navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters*.
9. Klicken Sie im rechten Bereich mit der rechten Maustaste auf *NtpServer* und ändern Sie den Wert auf den gewünschten NTP-Server ab. Tragen Sie am besten eine durch Leerzeichen getrennte Liste ein. Sie müssen *,0x1* an das Ende der einzelnen DNS-Namen anhängen. Tragen Sie ein *,0x2* hinter den Eintrag ein, verwendet Windows diesen Server nur, wenn er Server mit dem Eintrag *,0x1* nicht erreichen kann. Klappt nach der Konfiguration die Zeitsynchronisierung nicht, unterstützt der entsprechende Server nicht die Standardkonfiguration von NTP. In diesem Fall tragen Sie *,0x4* nach dem Servernamen ein. Diese Option aktiviert den Symmetric Active Mode. Normalerweise verwendet NTP einen Client/Server-Modus, der auch für die meisten Zeitserver funktioniert.
10. Navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient*.
11. Klicken Sie im rechten Bereich mit der rechten Maustaste auf *SpecialPollInterval* und ändern Sie den Wert auf *Dezimal* ab. Tragen Sie den Intervall in Sekunden ein, in dem sich der Server mit dem Internet synchronisiert. Der von Microsoft empfohlene Dezimalwert ist 900. Dieser Wert konfiguriert den Zeitserver für ein Intervall von 15 Minuten.
12. Geben Sie in der Eingabeaufforderung den Befehl *net stop w32time && net start w32time* ein.

Anschließend können Sie in der Ereignisanzeige des Domänencontrollers über *System* überprüfen, ob die Synchronisierung funktioniert. Hier sehen Sie entsprechende Meldung der Quelle *Time-Service*. Neben den Eintragungen über die Registry können Sie die Einstellungen auch über *w32tm.exe* vornehmen, zum Beispiel mit den folgenden Befehlen:

```
w32tm /config /manualpeerlist:<Zeitserver> /syncfromflags:manual /reliable:yes /update
net stop w32time
net start w32time
```

Die Zeitserver trennen Sie durch Leerzeichen voneinander. Die gesamte Liste der Zeitserver tragen Sie in Anführungszeichen ein. Der Befehl hat grundsätzlich die gleichen Auswirkungen wie die Anpassungen in der Registry. Führen Sie den Befehl vor der Bearbeitung der Registry aus, sehen Sie die erstellten Einträge, zum Beispiel bei den hinterlegten Zeitservern.

Die Option *reliable* definiert den Zeitserver als vertrauenswürdige Zeitquelle. *Syncfromflags* legt fest, dass sich der Server mit einem Zeitserver im Internet *(/syncfromflags:manual)* oder in der Gesamtstruktur *(/syncfromflags:domhier)* synchronisieren soll.

Mit dem Befehl *w32tm /monitor* können Sie die Synchronisierung überwachen und die Einstellungen anzeigen. Den Status der Synchronisierung sehen Sie mit dem Befehl *w32tm /query /status*. Überprüfen Sie nach der Konfiguration, ob sich der Server problemlos mit dem externen Zeitserver synchronisiert und keine Fehler in der Ereignisanzeige erscheinen. Die verschiedenen Einstellungen, die Sie in der Registry vornehmen können, finden Sie im Knowledge Base-Artikel auf der Seite *http://support.microsoft.com/kb/816042* [Ms179-K11-12].

Zeitsynchronisierung bei der Virtualisierung beachten

Virtualisieren Sie Server, müssen Sie bei der Zeitsynchronisierung in der entsprechenden Virtualisierungslösung eventuell ebenfalls Konfigurationen vornehmen. Vor allem, wenn Sie Domänencontroller, SharePoint oder Exchange-Server virtualisieren, sind Konfigurationsmaßnahmen notwendig. Auf jedem virtuellen Computer installiert Hyper-V automatisch die Integrationsdienste. Dabei handelt es sich um ein Softwarepaket, welches die Leistung virtueller Server deutlich verbessert (siehe die Kapitel 7 bis 9).

Rufen Sie dazu für jeden Server die Einstellungen auf und klicken Sie auf *Integrationsdienste*. Hier können Sie einstellen, ob sich die virtuellen Server mit dem Host synchronisieren sollen. Für virtuelle Windows-Server in Active Directory-Domänen sollten Sie diese Synchronisierung deaktivieren, da durch die Zeitsynchronisierung Inkonsistenzen auftreten können. Vor allem bei der Virtualisierung von SharePoint, Exchange oder virtuellen Domänencontrollern liegt in dieser Konfiguration eine häufige Fehlerquelle.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie einen Active Directory-Domänencontroller installieren. Auch den ersten Umgang mit dem Active Directory-Verwaltungscenter haben Sie in diesem Kapitel kennengelernt. Ebenfalls ein wichtiger Punkt war die Installation von Active Directory über ein Installationsmedium oder per Antwortdatei auf Core-Servern. Und schließlich war das Thema Zeitsynchronisierung ein wichtiger Bestandteil des Kapitels.

In den folgenden Kapiteln widmen wir uns der Erweiterung von Active Directory mit zusätzlichen Domänencontrollern, zum Beispiel schreibgeschützten Domänencontrollern. Auch die Installation zusätzlicher Domänen und Domänenstrukturen sind Thema dieser Kapitel.

Kapitel 12

Active Directory – Erweitern und absichern

In diesem Kapitel:

In diesem Kapitel gehen wir darauf ein, wie Sie Computer über das Netzwerk und delegiert zu Domänen hinzufügen und wie Sie die verwalteten Dienstkonten einsetzen. Auch den Papierkorb zeigen wir Ihnen in diesem Kapitel.

Offline-Domänenbeitritt – Djoin.exe

In Windows Server 2012 R2 können Sie Computerkonten von Windows 7/8/8.1-Computern auch dann einer Domäne hinzufügen, wenn diese aktuell keine Verbindung mit dem Domänencontroller haben. Sobald der Client eine Verbindung hat, wendet er die notwendigen Einstellungen und Berechtigungen an, die für einen Domänenbeitritt notwendig sind. So können Sie zum Beispiel Clients von Niederlassungen in Domänen aufnehmen, wenn aktuell keine Verbindung zur Domäne besteht.

Neu in Windows Server 2012 R2 ist die Möglichkeit, Computer an Domänen anzubinden, die mit DirectAccess angebunden sind. Auch hierzu können Sie das Befehlszeilentool Djoin.exe verwenden. Wir zeigen Ihnen diese Vorgänge ebenfalls in diesem Kapitel. Mehr zu DirectAccess lesen Sie in Kapitel 32.

Vorteile und technische Hintergründe zum Offline-Domänenbeitritt

Wollen Sie zum Beispiel viele virtuelle Computer gleichzeitig zur Domäne aufnehmen, beispielsweise in einem Virtual Desktop Infrastructure-Szenario, können Sie das Active Directory so vorbereiten, dass sich die Computer schnell und problemlos anbinden lassen. Sobald ein solcher Client das erste Mal startet, führt er die notwendigen Änderungen durch. Ein erneuter Start des Rechners ist nicht notwendig. Dadurch beschleunigt sich auch das Bereitstellen von Windows 7/8/8.1-Computern im Netzwerk.

Djoin.exe funktioniert auch zusammen mit schreibgeschützten Domänencontrollern (RODC). Dazu nehmen Sie mit Djoin.exe die Computer in die Domäne auf und lassen die Konten zum RODC replizieren. Sobald sich die Computer in der Niederlassung mit dem Netzwerk verbinden, authentifizieren Sie sich am schreibgeschützten Domänencontroller und sind in Active Directory verfügbar.

Ein weiterer Vorteil ist der automatisierte Domänenbeitritt von neuen Computern beim Deployment von Windows 7/8/8.1 im Unternehmen, da Sie die notwendigen Befehle für den Domänenbeitritt in die Antwortdatei der automatischen Installation aufnehmen können.

Voraussetzungen für die Verwendung des Offline-Domänenbeitritts

Damit Sie den Offline-Domänenbeitritt verwenden können, müssen Sie Windows 7/8/8.1 oder Windows Server 2008 R2/2012/2012 R2 als Betriebssystem einsetzen. Sie können diese Betriebssysteme aber auch in Domänen aufnehmen, die noch keine Domänencontroller unter Windows Server 2012 R2 betreiben. In diesem Fall verwenden Sie die Option */downlevel*. Standardmäßig geht Djoin.exe davon aus, dass eine Verbindung zu einem Domänencontroller unter Windows Server 2012 R2 besteht.

Zusammenfassend heißt das, dass Sie nur Computer, auf denen Windows 7/8/8.1 oder Windows Server 2008 R2/2012 installiert sind, per Djoin.exe zu einer Domäne aufnehmen können. Bei der Domäne kann es sich auch um Active Directory unter Windows Server 2008/2008 R2 handeln. Nur Benutzer, die über die Rechte verfügen, Computer einer Domäne hinzuzufügen, können Djoin.exe nutzen. Dazu müssen Sie entweder über Domänenadminrechte verfügen oder ein Administrator muss die entsprechenden Rechte delegieren.

TIPP Die Rechte, um Computer in eine Domäne aufzunehmen, können Sie über Gruppenrichtlinien setzen. Bearbeiten Sie dazu unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Zuweisen von Benutzerrechten* den Wert *Hinzufügen von Arbeitsstationen zur Domäne*. Nehmen Sie hier die Benutzerkonten auf, die über die entsprechenden Rechte verfügen sollen.

Durchführen des Offline-Domänenbeitritts

Der Offline-Domänenbeitritt erfolgt über das Tool Djoin.exe in der Eingabeaufforderung auf einem Computer unter Windows 7/8/8.1 oder Windows Server 2008 R2/2012, der bereits Mitglied der Domäne ist. Sie müssen für die Verwendung über das Schnellmenü (⊞ + X) eine Eingabeaufforderung mit Administratorrechten starten und über Rechte verfügen, um Computerkonten zur Domäne hinzuzufügen.

Die Ausgabe in die Datei oder auf dem Bildschirm enthält die Metadaten für den Domänenbeitritt. Microsoft bezeichnet diese auch als Blob. Bei der Ausführung können Sie entweder eine verschlüsselte Datei erstellen, die Sie dann auf dem Clientrechner verwenden müssen. Oder Sie speichern die Daten in einer Datei *Unattend.xml*, um Antwortdateien vollkommen zu automatisieren. Das Tool Djoin.exe besitzt verschiedene Optionen, die in Tabelle 12.1 detailliert aufgelistet sind.

Tabelle 12.1 Optionen von Djoin.exe

Option von Djoin.exe	Erläuterung
/provision	Erstellen eines Computerkontos in der Domäne
/domain <Name der Domäne>	Domäne, in der Sie das Konto erstellen wollen
/machine <Name>	Name des Computers, den Sie zur Domäne hinzufügen
/machineou <Organisationseinheit>	OU, in der das Konto erstellt werden soll. Ohne Angabe einer OU, verwendet Djoin.exe die OU *Computer*
/dcname <Name>	Name des Domänencontrollers, auf dem das Konto zuerst verfügbar sein soll
/reuse	Verwenden eines bereits vorhandenen Computerkontos, dessen Kennwort zurückgesetzt wird
/downlevel	Aufnehmen eines Computers auf einem Domänencontroller, auf dem nicht Windows Server 2012 R2 installiert ist
/savefile <Name der Datei>.txt	Textdatei, in der Daten des Domänenbeitritts für die Ausführung auf dem Client gespeichert werden. Der Inhalt der Datei ist verschlüsselt.
/defpwd	Verwendet das standardmäßige Kennwort für Computerkonten (nicht notwendig)

Tabelle 12.1 Optionen von Djoin.exe *(Fortsetzung)*

Option von Djoin.exe	Erläuterung
/nosearch	Überspringt Konflikte, wenn das Konto bereits vorhanden ist. Benötigt die Option */dcname*.
/printblob	Gibt einen Base64-kodierten Wert für Antwortdateien aus
/requestodj	Führt einen Offline-Domänenbeitritt beim nächsten Neustart aus
/loadfile	Verwendet die Ausgabe einer vorherigen Ausführung von Djoin.exe
/windowspath <Pfad>	Pfad zum *Windows*-Ordner, wenn nicht der Standard verwendet werden soll
/loalos	Zielcomputer, den Sie der Domäne hinzufügen wollen. Diese Option kann nicht auf einem Domänencontroller durchgeführt werden.

Generell ist der Ablauf bei einem Domänenbeitritt recht einfach. Sie führen im Grunde genommen folgende Schritte durch:

1. Sie verwenden *djoin /provision*, um die Metadaten für den Domänenbeitritt des Zielcomputers zu erstellen. Als Option geben Sie die Domäne an. Achten Sie darauf, dass Sie die Eingabeaufforderung im Administratormodus öffnen. Ein Beispiel für die Datei wäre:

   ```
   djoin /provision /domain contoso.com /machine client134 /savefile c:\client134.txt
   ```

   Inhalt der Datei sind das Kennwort der Maschine, der Name der Domäne und des Domänencontrollers sowie die SID der Domäne. Kopieren Sie die Datei auf den Rechner. Der Inhalt ist verschlüsselt und bringt Außenstehenden nichts.
2. Auf dem Zielcomputer verwenden Sie den folgenden Befehl, um den Rechner in die Domäne aufzunehmen:

   ```
   djoin /requestodj /loadfile c:\client134.txt /windowspath %SystemRoot% /localos
   ```

3. Starten Sie den Zielcomputer, wird der Computer automatisch in die Domäne aufgenommen, sobald eine Verbindung zu einem Domänencontroller besteht.

Offline-Domänenbeitritt bei einer unbeaufsichtigten Installation über Antwortdatei

Wollen Sie einen Offline-Domänenbeitritt während der Installation zum Beispiel im unbeaufsichtigten Modus durchführen, ist dies ebenfalls möglich. Dazu müssen Sie beim Erstellen des Computerkontos auf der Domäne den Inhalt der Metadaten anstatt in einer verschlüsselten Datei in eine Antwortdatei integrieren. Antwortdateien unter Windows Server 2008 R2/2012/2012 R2 und Windows 7/8/8.1 tragen normalerweise die Bezeichnung *Unattend.xml*. Sie müssen in der Antwortdatei dazu eine neue Sektion erstellen. Diese trägt die Bezeichnung:

Microsoft-Windows-UnattendJoin/Identification/Provisioning

Diese Sektion enthält darüber hinaus eine Unterstruktur, die folgendermaßen aussieht:

```
<Component>
<Component name=Microsoft-Windows-UnattendedJoin>
     <Identification>
          <Provisioning>
               <AccountData>Base64Encoded Blob</AccountData>
          </Provisioning>
     </Identification>
</Component>
```

Sie müssen die Metadaten, die Sie beim Erstellen der Datei erhalten, zwischen die Tags *<AccountData>* und *</AccountData>* einfügen. Nachdem Sie die Datei erstellt haben, können Sie den Computer unbeaufsichtigt installieren. Die Syntax bei Antwortdateien ist *setup /unattend:<Antwortdatei>*.

DirectAccess Offline Domain Join

Sie können über den Offline-Domänenbeitritt auch Clients anbinden, die mit DirectAccess an das Netzwerk angebunden sind (siehe Kapitel 32). Allerdings funktioniert das nur mit Windows Server 2012/2012 R2 und Windows 8/8.1.

Auch in diesem Fall nutzen Sie den Aufruf *djoin /provision*, um das Konto zu erstellen und eine Blob-Datei zu erhalten:

```
djoin /provision /domain <Name der Domäne> /machine <Name des Computers> /policynames <DA
Client GPO> /rootcacerts /savefile <Datei> /reuse
```

Haben Sie eine Zertifizierungsstelle im Einsatz, verwenden Sie:

```
djoin /provision /machine <Name des Computers> /domain <Name der Domäne>> /policynames <DA
Client GPO > /certtemplate <Name des Zertifikats> /savefile <Datei> /reuse
```

Mit *djoin /requestodj* lesen Sie die Daten aus der Blob-Datei auf dem Zielcomputer ein. Anschließend starten Sie den entsprechenden Computer und schon ist der Mitglied der Domäne. Die Reihenfolge des Offline-Domänenbeitritts zusammen mit DirectAccess ist folgende:

1. Sie verwenden *djoin /provision* wie in diesem Kapitel besprochen, um das Konto in der Domäne zu erstellen.
2. Sie nehmen das Konto des erstellten Clients in die DirectAccessClients-Sicherheitsgruppe auf.
3. Sie kopieren die Blob-Datei auf den Client oder versenden diese per E-Mail. Sie führen auf dem Client den Befehl *djoin /requestodj* aus.
4. Sie starten den PC neu.

Verwaltete Dienstkonten – Managed Service Accounts

Die verwalteten Dienstkonten sind eine Neuerung in Windows Server 2008 R2 und wurden in Windows Server 2012 R2 deutlich verbessert. In der neuen Version können Sie zum Beispiel ein verwaltetes Dienstkonto für mehrere Server nutzen. Dazu hat Microsoft zu den bereits bekannten verwalteten Dienstkonten (Managed Service Accounts, MSA) noch die gruppierten verwalteten Dienstkonten (Grouped Managed Service Accounts, gMSA) entwickelt. Im Fokus der neuen Funktion stehen die Dienstkonten von Serveranwendungen wie Exchange oder SQL Server 2012/2014, die zum einen wichtig für den Betrieb, zum anderen aber auch kritisch im Bereich der Sicherheit sind, da die Benutzerkonten, mit denen diese Dienste starten, oft über weitreichende Rechte verfügen.

Vor allem die Dienste *Lokaler Dienst*, *Netzwerkdienst* und *Lokales System* werden häufig für Serveranwendungen verwendet. Der Nachteil dieser lokalen Dienste ist die fehlende Möglichkeit, Einstellungen auf Domänenebene vorzunehmen. Verwenden Administratoren statt diesen Konten Benutzerkonten aus Active Directory, ergeben sich bezüglich der Verwaltung der Kennwörter neue Probleme.

Damit Sie die OU *Managed Service Accounts* und die darin angelegten Dienstkonten sehen, müssen Sie unter Umständen im Snap-In *Active Directory-Benutzer und -Computer* die erweiterte Ansicht über das Menü *Ansicht* aktivieren.

HINWEIS Die Administration der verwalteten Dienstkonten findet ausschließlich in der PowerShell statt. Verwenden Sie nicht das Snap-In *Active Directory-Benutzer und -Computer*.

Verwaltete Dienstkonten – Technische Hintergründe

Verwaltete Dienstkonten sind Benutzerkonten in Active Directory, die zur Verwendung von lokalen Diensten verwendet werden. Dabei werden die Kennwörter dieser Konten nicht manuell, sondern automatisch bei bestimmten Bedingungen durch Active Directory geändert. Administratoren können solche Änderungen manuell anstoßen.

Der Vorteil ist, dass die Systemdienste, welche diese Benutzerkonten verwenden, bei Kennwortänderungen nicht von Administratoren konfiguriert werden müssen, sondern die Änderung der Kennwörter automatisch übernehmen. Die Verwaltung solcher Dienstkonten lässt sich auch an Nichtadministratoren delegieren, zum Beispiel internen Programmierern des Datenbanksystems.

Diese Dienste werden nur unter Windows Server 2008 R2 und Windows 7/8/8.1 sowie Windows Server 2012/2012 R2 unterstützt. Auf anderen Windows-Versionen können Sie diese Dienste nicht nutzen. Die Domäne darf zwar noch Domänencontroller mit Windows Server 2008/2008 R2 enthalten, allerdings müssen Sie dann zusätzliche Konfigurationen durchführen.

Damit Sie verwaltete Dienstkonten in Domänen mit Windows Server 2008/2008 R2-Domänencontrollern nutzen können, muss das Schema erweitert werden. Sie müssen in der Domäne *adprep /domainprep* ausführen und in der Gesamtstruktur *adprep /forestprep*. Mindestens ein Domänencontroller muss unter Windows Server 2012 R2 laufen. Das Tool Adprep finden Sie auf der Windows Server 2012 R2-DVD im Ordner *Support\Adprep*.

Bei den Schemaänderungen integriert Windows Server 2008 R2 und Windows Server 2012 R2 das Objekt *msDS-ManagedServiceAccount*. Dieses Benutzerkonto hat die Attribute von Benutzerkonten und von Computerkonten vereint. Das Kennwort des Computers verhält sich wie das Kennwort eines Computerkontos in Active Directory, lässt sich also zentralisiert durch das System selbst steuern.

Dies bedeutet, dass das verwaltete Benutzerkonto eines Computers dann aktualisiert wird, wenn Active Directory auch das Kennwort des jeweiligen Computerkontos anpasst, das dem verwalteten Dienstkonto zugewiesen ist. Diese Einstellungen lassen sich auf dem Server in der Registry anpassen. Navigieren Sie dazu zu folgendem Schlüssel:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters

Wichtig sind an dieser Stelle die beiden folgenden Werte:

- **DisablePasswordChange** Der Wert muss auf *0* oder *1* gesetzt sein. Ist der Wert nicht vorhanden, geht Windows vom Wert *0* aus.
- **MaximumPasswordAge** Hier legen Sie einen Wert zwischen 1 und 1.000.000 in Tagen fest. Der Standardwert ist 30, auch wenn der Wert nicht vorhanden ist.

Das automatisch gesetzte Kennwort hat eine Länge von 240 Zeichen und ist stark verschlüsselt. Außerdem besteht das Kennwort aus verschiedenen Zeichen, lässt sich also nicht erraten oder hacken.

In der Verwaltungskonsole *Active Directory-Benutzer und -Computer* finden Sie eine neue OU mit der Bezeichnung *Managed Service Accounts*. Diese OU ist für die Verwaltung der verwalteten Dienstkonten von zentraler Bedeutung. Verwaltete Dienstkonten lassen sich so nutzen, wie die standardmäßig vorhandenen Benutzer.

Verwaltete Dienstkonten – Produktiver Einsatz

Sie legen die Dienstkonten über die PowerShell, genauer gesagt über das Active Directory-Modul der PowerShell mit dem Cmdlet *New-ADServiceAccount "Name Account"* an. Standardmäßig legt das Cmdlet in Windows Server 2012 R2 ein neues gruppiertes verwaltetes Dienstkonto an. Wollen Sie ein verwaltetes Dienstkonto nur für einen einzelnen Server anlegen, verwenden Sie zusätzlich die Option *–Standalone*. Eine vollständige Liste der Optionen finden Sie auf der Seite *http://technet.microsoft.com/en-us/library/hh852236.aspx* [Ms179-K12-01].

HINWEIS Bevor Sie gruppierte Konten anlegen, müssen Sie zunächst einen neuen Masterschlüssel für die Domäne erstellen:

```
Add-KdsRootKey –EffectiveImmediately
```

Standardmäßig dauert es ab diesem Moment 10 Stunden, bis Sie verwaltete Dienstkonten anlegen können. In Testumgebungen können Sie den Zeitraum mit dem folgenden Befehl umgehen:

```
Add-KdsRootKey –EffectiveTime ((Get-Date).addhours(–10))
```

TIPP Die Verwaltung der verwalteten Dienstkonten (Managed Service Accounts) findet ausschließlich in der PowerShell statt. Es gibt aber Zusatztools wie Managed Service Accounts GUI (*http://www.cjwdev.co.uk/Software/MSAGUI/Info.html* [Ms179-K12-02]).

Die Freeware kann verwaltete Dienstkonten in Windows Server 2008 R2 verwalten und berücksichtigt auch die neuen Funktionen in Windows Server 2012/2012 R2.

Der Ablauf beim manuellen Anlegen in der PowerShell bei der Verwendung von Managed Service Accounts ist folgender:

1. Sie legen das verwaltete Dienstkonto in Active Directory an.
2. Sie verbinden das Konto mit einem Computerkonto, also dem SQL-Server. Auf dem Computer muss dazu Windows Server 2008 R2, Windows Server 2012/2012 R2 oder Windows 7/8/8.1 sowie SQL Server 2012/2014 installiert sein. Um ein Dienstkonto auf mehreren Servern zu nutzen, müssen Sie Domänencontroller mit Windows Server 2012 einsetzen.
3. Sie installieren das verwaltete Benutzerkonto auf dem Computer.
4. Sie passen die Systemdienste auf dem lokalen Computer an, um das neue Konto zu nutzen.

Zukünftig ändert sich das Kennwort für dieses Konto vollkommen automatisch, ohne dass Sie eingreifen müssen.

Die Befehlssyntax zum Anlegen eines Dienstkontos sieht folgendermaßen aus:

```
New-ADServiceAccount <Name> -DNSHostName <DNS-Name des Diensts> -PrincipalsAllowedTo
RetrieveManagedPassword <Gruppe der Computer die das Konto nutzen> -KerberosEncryptionType
RC4, AES128, AES256 -ServicePrincipalNames <Service Principal Names>
```

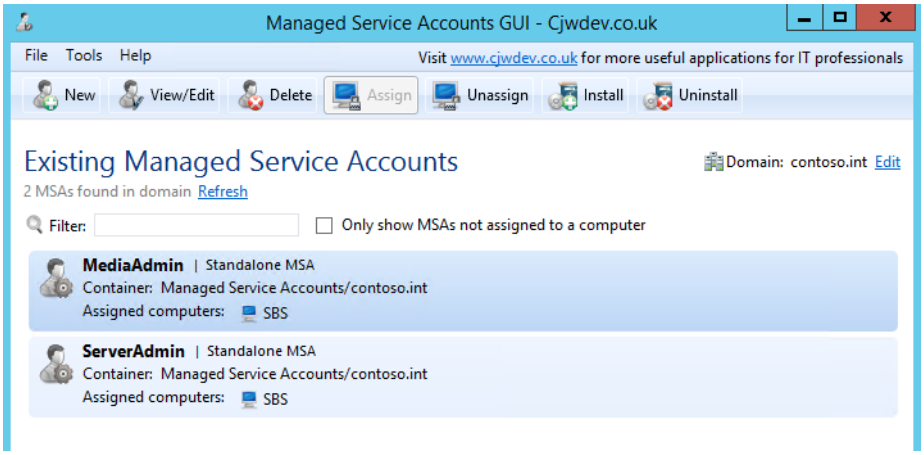
Sie haben auch die Möglichkeit, die Computerkonten die das verwaltete Dienstkonto nutzen sollen, in einer Gruppe aufzunehmen. So lässt sich zum Beispiel das Konto für eine Lastenausgleichsfarm verwenden. Sie können die Funktion aber nicht in Failoverclustern verwenden.

Verwaltete Dienstkonten in der grafischen Oberfläche anlegen

Ab der Version 1.5 der Freeware *Managed Service Accounts GUI* (*http://www.cjwdev.co.uk/Software/MSAGUI/Info.html* [Ms179-K12-02]) legen Sie wesentlich einfacher verwaltete Dienstkonten in Windows Server 2008 R2 und Windows Server 2012/2012 R2 an.

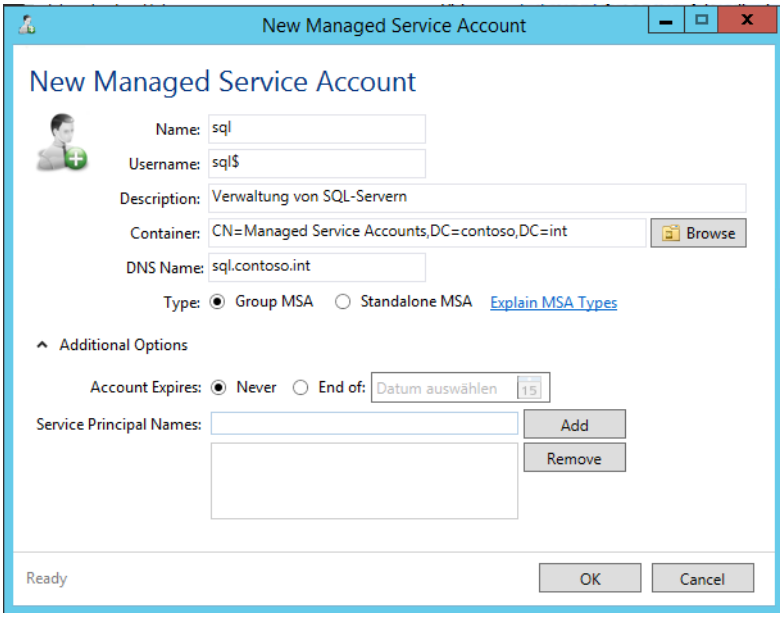
Sie können mit dem Tool auch gruppierte verwaltete Konten anlegen. Dazu laden Sie das Tool herunter und installieren es entweder auf einer Arbeitsstation mit installierten RSAT oder auf einem Server. Starten Sie das Tool, können Sie bequem in der grafischen Oberfläche einen verwalteten Dienst anlegen.

Abbildg. 12.1 Verwaltete Dienstkonten können Sie schnell und einfach mit der Freeware Managed Service Accounts GUI anlegen



Um ein neues verwaltetes Dienstkonto anzulegen, klicken Sie im Tool auf *New*. Im daraufhin geöffneten Fenster geben Sie alle gewünschten Daten ein. Hier wählen Sie auch aus, ob Sie ein klassisches verwaltetes Dienstkonto oder ein gruppiertes Konto von Windows Server 2012 R2 anlegen möchten.

Abbildg. 12.2 In der grafischen Oberfläche legen Sie neue verwaltete Dienstkonten an



Sobald Sie mit *OK* bestätigen, wird das Konto in Active Directory angelegt. Sie sehen das neue Konto auch in der OU *Managed Service Accounts*, wenn Sie das Snap-In *Active Directory-Benutzer und -Computer* starten.

Bevor Sie in Managed Service Accounts GUI gruppierte Konten anlegen können, müssen Sie – wie beim herkömmlichen Anlegen auch – einen neuen Masterschlüssel für die Domäne erstellen. Dazu verwenden Sie den Befehl *Add-KdsRootKey -EffectiveImmediately*. Standardmäßig dauert es auch hier 10 Stunden, bis Sie gruppierte verwaltete Dienstkonten anlegen können. Schneller geht es, wenn Sie *Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))* eingeben.

Nachdem Sie das verwaltete Dienstkonto angelegt haben, bietet Managed Service Accounts GUI an, das Konto direkt einem Server zuzuweisen. Sie können das aber auch jederzeit manuell in der PowerShell oder nachträglich über Managed Service Accounts GUI durchführen. Das Tool kann nicht nur verwaltete Dienstkonten anlegen, sondern auch verwalten und Servern zuweisen.

Im Gegensatz zu herkömmlichen verwalteten Dienstkonten können Sie gruppierte verwaltete Dienstkonten direkt mehreren Servern zuweisen. Dazu führen Sie in Managed Service Accounts GUI einfach den Assistenten zur Verwaltung des gruppierten Kontos aus und weisen die Computerkonten zu. Klicken Sie dazu auf *Add* und geben Sie den Namen des Servers ein.

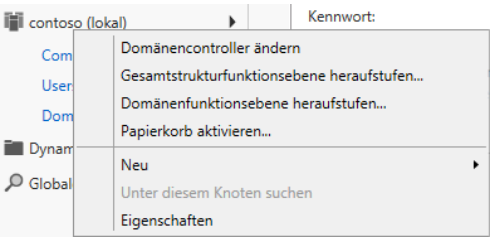
Der Active Directory-Papierkorb im Praxiseinsatz

Den Papierkorb für gelöschte Objekte verwalten Sie nicht mehr in der PowerShell oder Eingabeaufforderung, sondern können die Aktivierung und die Wiederherstellung von Objekten vollständig im Active Directory-Verwaltungscenter vornehmen.

Active Directory-Papierkorb verstehen und aktivieren

Grundlage ist der Papierkorb von Active Directory, den Sie zunächst für die Gesamtstruktur aktivieren müssen. Diesen Vorgang nehmen Sie über das Kontextmenü der Gesamtstruktur auf der linken Seite der Konsole im Active Directory-Verwaltungscenter vor.

Abbildg. 12.3 Erweitern des Papierkorbs in Active Directory



Sie können den Papierkorb auch weiterhin in der PowerShell aktivieren. Der Befehl dazu am Beispiel der Domäne *contoso.com* lautet:

```
Enable-ADOptionalFeature –Identity 'CN=Recycle Bin Feature,CN=Optional
Features,CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=contoso,DC=com' –Scope ForestOrConfigurationSet –Target
'contoso.com'
```

HINWEIS Starten Sie nach der Aktivierung des Active Directory-Papierkorbs das Active Directory-Verwaltungscenter neu. Erst dann stehen alle Funktionen zur Verfügung, um gelöschte Objekte wiederherstellen zu können.

Sie können den Papierkorb nur dann aktivieren, wenn die Funktionsebene der Gesamtstruktur auf Windows Server 2008 R2 gesetzt ist (siehe Kapitel 10). Wiederherstellen können Sie Objekte im Active Directory-Verwaltungscenter von Windows Server 2012 R2. Haben Sie den Vorgang nicht bereits durchgeführt, können Sie das über die PowerShell mit dem folgenden Befehl erledigen:

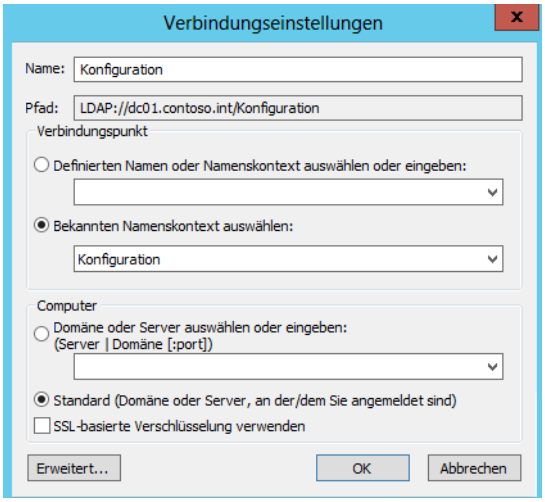
```
Set-ADForestMode -Identity contoso.com -ForestMode Windows2008R2Forest -Confirm:$false
```

Der Papierkorb arbeitet mit dem Wert *isDeleted* und mit dem neuen Wert *isRecycled*. Ist der Wert *isRecycled* für ein Active Directory-Objekt auf *True* gesetzt, können Sie dieses nicht wiederherstellen. Nur Objekte, bei denen *isDeleted* auf *True* gesetzt ist, lassen sich restaurieren.

Objekte lassen sich innerhalb von Tombstone-Lifetime wiederherstellen. Dieser beträgt bei Windows Server 2012 R2 180 Tage. Sie finden den jeweiligen Wert für Ihr Active Directory am besten in ADSI-Edit über den Container *Konfiguration*.

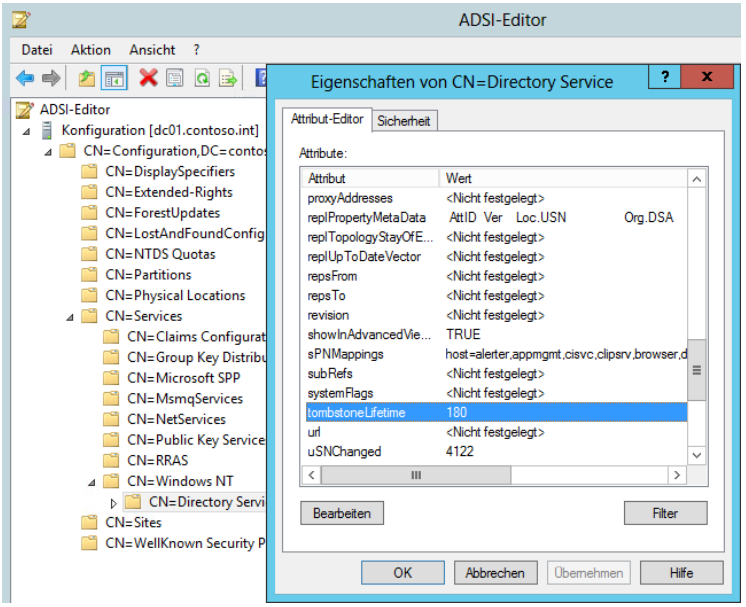
Dazu öffnen Sie ADSI-Edit über den Startbildschirm und verbinden sich über das Kontextmenü von ADSI-Edit mit der Domäne. Wählen Sie bei *Bekannten Namenskontext auswählen* die Option *Konfiguration* aus.

Abbildg. 12.4 Laden des Konfigurationscontainers von Active Directory



Navigieren Sie zu *Konfiguration/Configuration/Services/Windows NT/Directory Service*. Rufen Sie die Eigenschaften von *Directory Service* auf. Den Tombstone-Wert finden Sie auf der Registerkarte *Attribut-Editor* beim Wert *tombstoneLifetime*. Sie können den Wert an dieser Stelle auch anpassen, das ist allerdings in den wenigsten Fällen notwendig.

Abbildg. 12.5 Anzeigen des *tombstoneLifetime* für eine Gesamtstruktur



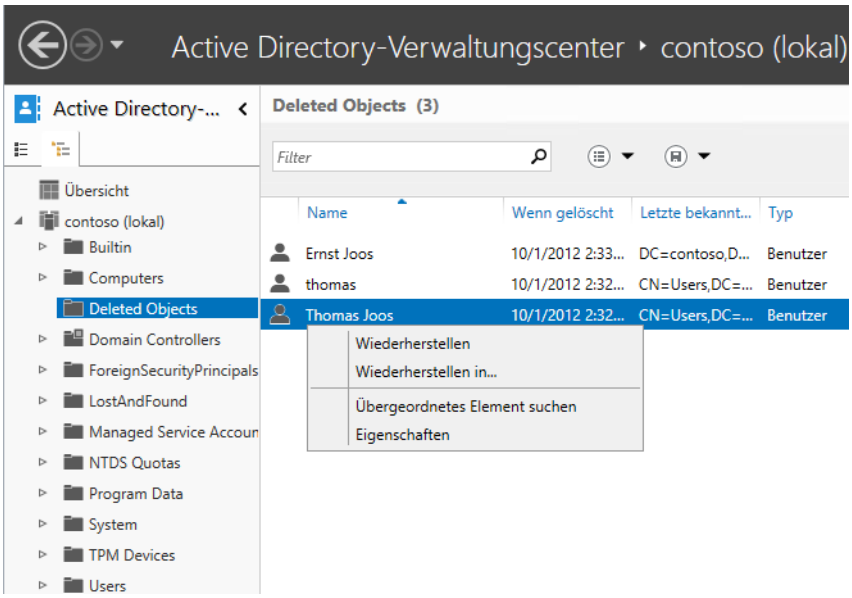
Sobald Sie ein Objekt im Active Directory löschen, erhält dieses den Wert *True* bei *isDeleted* und ist in Active Directory nicht mehr verfügbar, lässt sich aber noch wiederherstellen. Der Zeitraum, in dem Sie das Objekt durch *isDeleted* auch wiederherstellen können, bezeichnet Microsoft als Deleted Object Lifetime (DOL).

Diesen Wert, der ebenfalls 180 Tage beträgt, finden Sie über *msDS-deletedObjectLifetime*. Nach 180 Tagen, festgelegt durch den DOL erhält das Objekt den Wert *True* bei *isRecycled* und ist **nicht** mehr wiederherstellbar. Ist auch der Tombstone-Lifetime abgelaufen, wird das Objekt komplett aus der Datenbank gelöscht. Da beide Werte identisch sind, wird das Objekt nach 180 Tagen standardmäßig aus der Datenbank gelöscht.

Objekte aus dem AD-Papierkorb mit Bordmitteln wiederherstellen

Um gelöschte Objekte wiederherzustellen, verwenden Sie am besten das Active Directory-Verwaltungscenter in Windows Server 2012 R2. Dies hat den Vorteil, dass Ihnen eine grafische Oberfläche zur Verfügung steht. Nachdem Sie den Papierkorb aktiviert und das Active Directory-Verwaltungscenter neu gestartet haben, existiert für die entsprechende Gesamtstruktur ein neuer Ordner mit der Bezeichnung *Delete Objects*. In diesem können Sie nach gelöschten Objekten suchen und diese wiederherstellen. Dazu klicken Sie die Objekte mit der rechten Maustaste an.

Abbildg. 12.6 Wiederherstellen von Objekten aus dem Active Directory-Papierkorb



Sie können die Wiederherstellung auch in der PowerShell durchführen. Dazu verwenden Sie den Befehl

```
Get-ADObject -Filter {<Name des Objekts>} -IncludeDeletedObjects | Restore-ADObject
```

Wenn Sie zum Beispiel das Benutzerkonto mit dem Anzeigenamen *Thomas Joos* wiederherstellen wollen, geben Sie ein:

```
Get-ADObject -Filter {displayName -eq "Thomas Joos"} -IncludeDeletedObjects | Restore-
ADObject
```

Handelt es sich bei dem Objekt, das Sie wiederherstellen wollen, um ein untergeordnetes Objekt, müssen Sie erst alle Objekte herstellen, die dem Objekt übergeordnet sind, wenn diese ebenfalls gelöscht wurden. Ansonsten bricht die Wiederherstellung untergeordneter Objekte mit einem Fehler ab. Mit dem folgenden Befehl lassen Sie sich gelöschte Objekte mit dem passenden Namen zunächst anzeigen:

```
Get-ADObject -Filter {displayName -eq "Thomas Joos"} -IncludeDeletedObjects
```

Haben Sie zum Beispiel eine OU mit Benutzerkonten gelöscht, müssen Sie erst die OU, dann die einzelnen Benutzerkonten wiederherstellen. Mit *Get-ADObject* zeigen Sie die Objekte an und übergeben diese per Pipeline-Zeichen (|) an das Cmdlet *Restore-ADObject*. Kennen Sie die ursprüngliche Hierarchie der Organisationseinheit nicht, müssen Sie mit dem Cmdlet *Get-ADObject* die Hierarchie erst wieder herausfiltern:

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=contoso,DC=com" -ldapFilter:"(msDs-
lastKnownRDN=Thomas Joos)" -IncludeDeletedObjects -Properties lastKnownParent
```

Dieser Befehl gibt auch übergeordnete Objekte des gelöschten Objekts an.

Mit dem folgenden Befehl lassen Sie sich alle untergeordneten Objekte in der besagten OU anzeigen:

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=contoso,DC=com" -Filter {lastKnownParent –
eq 'OU=Einkauf\\0ADEL:26e19d03-80db-4c9c-b7dd-e472193222e0,CN=Deleted
Objects,DC=contoso,DC=com'} -IncludeDeletedObjects -Properties lastKnownParent | ft
```

Den Namen verwenden Sie aus der vorangegangenen Verwendung von

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=contoso,DC=com" -ldapFilter:"(msDs-
lastKnownRDN=Thomas Joos)" -IncludeDeletedObjects -Properties lastKnownParent
```

Sie müssen bei der Verwendung im Cmdlet *Get-ADObject* unbedingt einen weiteren umgekehrten Schrägstrich im Namen verwenden. Sie müssen also zunächst die Organisationseinheit *Einkauf* wiederherstellen, bevor Sie das untergeordnete Objekt *Thomas Joos* wiederherstellen können. Da alle bisherigen Untersuchungen mit dem *lastKnownParent*-Attribut durchgeführt wurden, das auf das direkt übergeordnete Objekt verweist, aber nicht angibt, ob das nächste übergeordnete Objekt ebenfalls gelöscht wurde, müssen Sie mit dem Wert *lastKnownParent* überprüfen, ob *Einkauf* nicht noch einer weiteren Organisationseinheit untergeordnet ist, die ebenfalls gelöscht wurde:

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=contoso,DC=com" -ldapFilter:"(msDs-
lastKnownRDN=Einkauf)" -IncludeDeletedObjects -Properties lastKnownParent
```

Im Beispiel sehen Sie, dass die OU *Einkauf* direkt in der Domäne *contoso.com* angelegt ist, also keine weitere Organisationseinheit gelöscht wurde. Es reicht also, wenn Sie die OU *Einkauf* wiederherstellen, um das Objekt *Thomas Joos* wiederherzustellen:

```
Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=Einkauf)" -IncludeDeletedObjects | Restore-
ADObject
```

Der Befehl gibt keine Ausgabe aus. Öffnen Sie das Snap-In *Active Directory-Benutzer und -Computer* und aktualisieren Sie die Ansicht mit F5. Die OU muss jetzt wieder vorhanden sein.

Der Befehl stellt allerdings nur die OU wieder her, nicht die gelöschten Objekte innerhalb der OU. Diese müssen Sie manuell herstellen, zum Beispiel mit:

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=contoso,DC=com" -Filter {lastKnownParent -
eq "OU=Einkauf,DC=contoso,DC=com"} -IncludeDeletedObjects | Restore-ADObject
```

Die Lebensdauer des gelöschten Objekts wird vom Wert des *msDS-deletedObjectLifetime*-Attributs bestimmt. Die Lebensdauer eines veralteten Objekts wird vom Wert des *tombstoneLifetime*-Attributs bestimmt. Standardmäßig sind diese Attribute auf NULL festgelegt. Die Lebensdauer des veralteten Objekts beträgt also 180 Tage.

Sie können die Werte von *msDS-deletedObjectLifetime* und *tombstoneLifetime* jederzeit ändern. Innerhalb der Lebensdauer können Sie ein gelöschtes Objekt wiederherstellen. In der Active Directory-Datenbank wird beim Löschen eines Objekts das Attribut *isDeleted* auf den Wert *True* gesetzt. Das gelöschte Objekt wird in den versteckten Container *Deleted Objects* verschoben und sein *Distinguished Name (DN)* erhält dadurch einen neuen Wert. Die *Deleted Object Lifetime* wird durch den Wert im Attribut *msDS-DeletedObjectLifetime* bestimmt. Ist die Zeit des im Attribut *msDS-DeletedObjectLifetime* definierten Werts abgelaufen, ändert sich das logisch gelöschte Objekt zu einem *Recycled Object*.

Zusammenfassung

In diesem Kapitel sind wir auf die praktischen Hintergründe der neuen Funktionen von Active Directory in Windows Server 2012 R2 eingegangen. Sie haben erfahren, wie man mit verwalteten Dienstkonten das Netzwerk absichert oder mit dem neuen Active Directory-Papierkorb Objekte wiederherstellt.

Im nächsten Kapitel gehen wir auf Erweiterungsmöglichkeiten von Active Directory und auf schreibgeschützte Domänencontroller (RODC) ein.

Kapitel 13

Active Directory – Neue Domänen und Domänencontroller

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, wie Sie existierende Domänen und Gesamtstrukturen mit weiteren Domänen, Domänencontrollern oder Strukturen ergänzen. Wir gehen auch darauf ein, wie Sie schreibgeschützte Domänencontroller installieren und verwalten. In den Kapiteln 10 und 11 sind wir bereits darauf eingegangen, wie Sie Domänencontroller installieren, auch über die PowerShell.

Schreibgeschützter Domänencontroller (RODC)

Haben Sie eine neue Domäne installiert, sollten Sie immer so schnell wie möglich einen zusätzlichen Domänencontroller installieren. 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 und Anwender sich weiter anmelden können. Wir zeigen Ihnen in diesem Abschnitt, wie zusätzliche Domänencontroller in einer Domäne installiert werden.

Dabei muss es sich nicht zwingend um einen schreibgeschützten Domänencontroller handeln, wir gehen aber in diesem Beispiel davon aus. RODCs können von Clients mit Windows Server 2003/2008/2008 R2/2012/2012 R2 und Windows XP/Vista oder Windows 7/8/8.1 verwendet werden. Es sind keine Änderungen an diesen Betriebssystemen notwendig.

HINWEIS Wollen Sie einen schreibgeschützten Domänencontroller (Read-only Domain Controller, RODC) installieren, achten Sie darauf, dass der PDC-Emulator der Domäne auf einem Windows Server 2008-DC positioniert sein muss, besser auf einem Server mit Windows Server 2012/2012 R2. Außerdem muss sich die Gesamtstruktur mindestens im Windows Server 2008-Betriebsmodus befinden.

Ein RODC empfängt Daten der Domänenpartition nur von Windows Server 2008 und R2-Domänencontrollern sowie von Windows Server 2012/2012 R2. Andere Daten aus Active Directory können auch von Windows Server 2008-Domänencontrollern empfangen werden. Das heißt, in jeder Domäne muss es mindestens einen Windows Server 2008-Domänencontroller geben, der vom RODC zur Replikation erreicht werden kann.

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 (siehe Kapitel 2 und 3). Achten Sie darauf, dass Sie den Server mit dem gleichen Stand des Betriebssystems installieren, damit Sie eine homogene Umgebung erhalten.

ACHTUNG Exchange Server 2007/2010/2013 unterstützt keine schreibgeschützten Domänencontroller. An jedem Standort, an dem ein Exchange-Server betrieben wird, muss auch ein normaler Domänencontroller positioniert werden, egal ob mit Windows Server 2008/2008 R2 oder Windows Server 2012/2012 R2.

Keine Probleme haben dagegen ISA Server, Threat Management Gateway, SQL Server, System Center Configuration Manager, Outlook, System Center Operations Manager sowie SharePoint Server. Auch die Serverrollen in Windows Server 2012/2012 R2 haben keine Schwierigkeiten mit einem RODC.

Weisen Sie dem zusätzlichen Domänencontroller zunächst einen passenden Namen zu, zum Beispiel *dc03*, und konfigurieren Sie das primäre DNS-Suffix auf dem Server. Gehen Sie bei diesem Schritt so vor wie bei der Erstellung des ersten Domänencontrollers (siehe Kapitel 10 und 11).

Installieren Sie auf dem Server nach dem Neustart des Servers, wie beim ersten Server, ebenfalls die DNS-Rolle (siehe Kapitel 11). Haben Sie den Server als Domänencontroller in Active Directory mit aufgenommen, steht er ebenfalls als DNS-Server für die Mitgliedsserver und Arbeitsstationen zur Verfügung.

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.

Integration eines neuen Domänencontrollers

Installieren Sie im Anschluss die Active Directory-Domänendienste wie bei der Installation eines normalen Domänencontrollers auch. Die Unterscheidung der Konfiguration findet erst im Rahmen der Einrichtung des Servers statt. Wählen Sie daher im Assistenten zur Einrichtung von Active Directory die Option *Domänencontroller zu einer vorhandenen Domäne hinzufügen*. Sie können diesen Vorgang auch in der PowerShell durchführen. Wie das geht, zeigen wir Ihnen in Kapitel 11. Auch die Installation in der PowerShell remote auf einem anderen Server ist möglich:

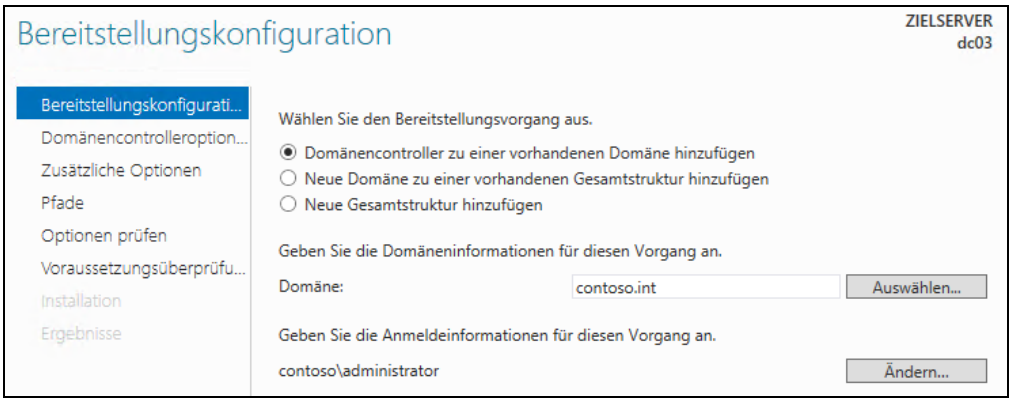
```
Invoke-Command {Install-ADDSDomainController -DomainName <Domäne> -Credential (Get-
Credential)} -ComputerName <Domänencontrollername>
```

Haben Sie die Option ausgewählt, müssen Sie noch die Domäne angeben, der Sie einen Domänencontroller hinzufügen wollen. Über die Schaltfläche *Ändern* müssen Sie das Konto eines Administrators festlegen, der über die Rechte verfügt, Domänencontroller zu einer Domäne hinzufügen zu dürfen. Verwenden Sie dazu die Syntax *<Domäne>\<Benutzername>*.

Im nächsten Fenster wählen Sie die Optionen des Servers aus. Sie können über dieses Fenster die DNS-Rolle installieren, den Server zum globalen Katalog heraufstufen und den Domänencontroller zu einem schreibgeschützten Domänencontroller heraufstufen.

Außerdem wählen Sie den physischen Standort des Domänencontrollers aus. 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.

Abbildg. 13.1 Installieren eines neuen Domänencontrollers



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 in 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 Active Directory-Replikation
- Konfiguration von Zeitplänen und Kosten für die optimale Standortreplikation

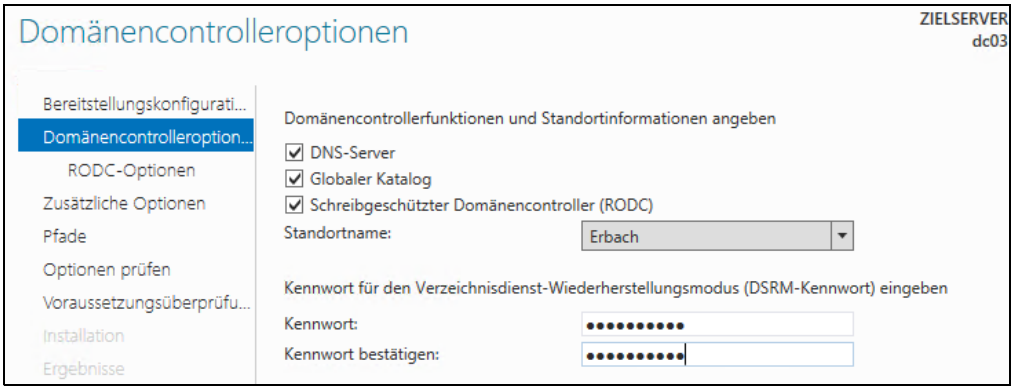
Damit Sie die standortübergreifende Replikation von Active Directory verwenden können, sollten Sie in jedem Standort, an dem später ein Domänencontroller angeschlossen wird, ein unabhängiges IP-Subnetz verwenden. Dieses IP-Subnetz wird in der Active Directory-Verwaltung hinterlegt und dient fortan zur Unterscheidung der Standorte in Active Directory.

Das wichtigste Verwaltungswerkzeug, um Standorte in Active Directory zu verwalten, ist das Snap-In *Active Directory-Standorte und -Dienste*, das auch über den Server-Manager zur Verfügung gestellt wird.

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 (RODC) verwendet wird, also dieser Server keine Änderungen entgegennimmt außer als Replikation von seinem übergeordneten Domänencontroller. Im gleichen Fenster geben Sie auch das Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus an.

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 Kennworts 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 Domänencontroller anmelden dürfen und welche nicht.

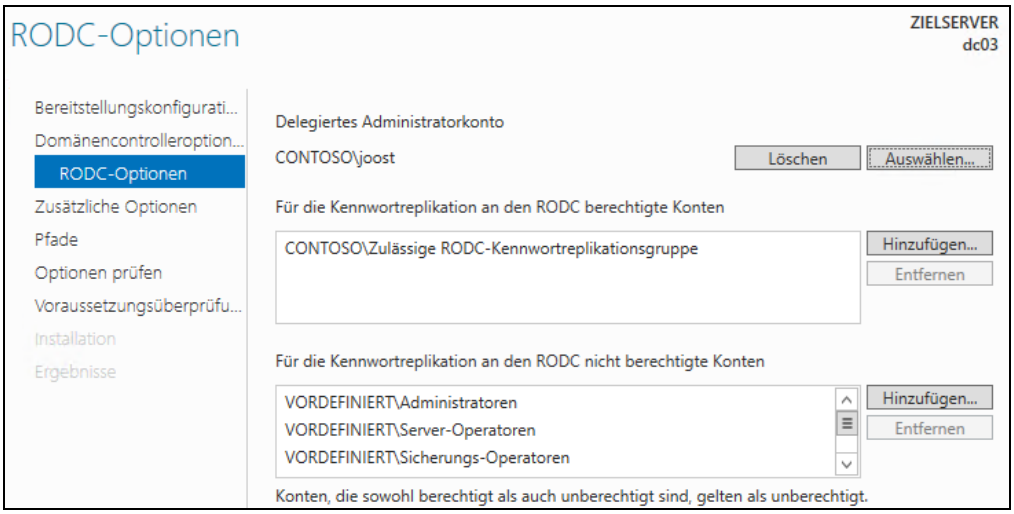
Abbildg. 13.2 Konfiguration des zusätzlichen Domänencontrollers als schreibgeschützten Domänencontroller (RODC)



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. 13.3 Festlegen der Benutzerkonten und Gruppen, deren Kennwörter auf den RODC repliziert werden



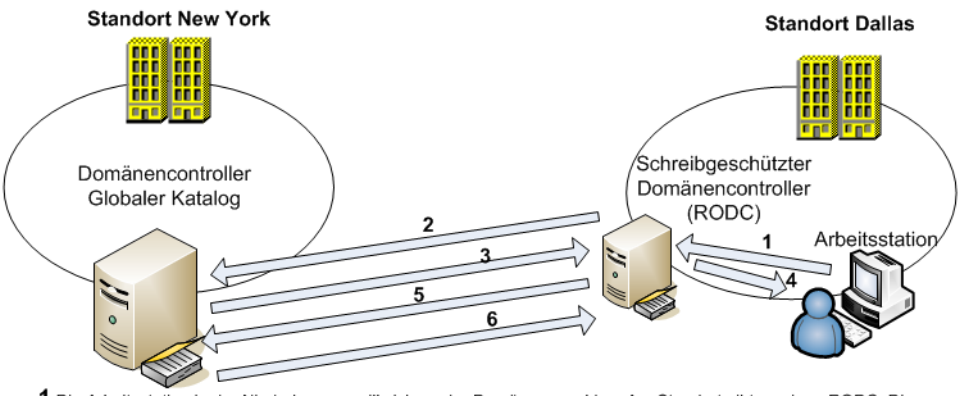
In der OU *Users* gibt es bereits die standardmäßigen Benutzergruppen *Zulässige RODC-Kennwortreplikationsgruppe* und *Abgelehnte RODC-Kennwortreplikationsgruppe*. Benutzerkonten, die Sie diesen Benutzergruppen zuordnen, können sich an diesem Domänencontroller anmelden, da die

Kennwörter repliziert wurden (*Zulässige RODC-Kennwortreplikationsgruppe*). Oder sie können sich nicht anmelden, da die Kennwörter nicht zur Verfügung stehen (*Abgelehnte RODC-Kennwortreplikationsgruppe*).

Sie können die Einstellungen, die Sie in diesem Dialogfeld vornehmen, jederzeit über die Eigenschaften des Computerkontos im Server-Manager wieder anpassen, nachdem der Server zum Domänencontroller heraufgestuft worden ist.

Auf der nächsten Seite des Assistenten geben Sie eine Benutzergruppe an, welche die Berechtigung zur Verwaltung des Domänencontrollers erhält. Mitglieder der angegebenen Gruppe dürfen den Server verwalten beziehungsweise Änderungen auf dem Server vornehmen. Die Gruppe oder der Benutzer, die bzw. den Sie hier angeben, erhalten lokale Administratorberechtigungen auf dem Controller, aber keinerlei Rechte in der Active Directory-Domäne.

Abbildg. 13.4 Ablauf bei der Anmeldung von Anwendern über schreibgeschützte Domänencontroller



1. Die Arbeitsstation in der Niederlassung will sich an der Domäne anmelden. Am Standort gibt es einen RODC. Die Station stellt einen TGT (Ticket Granting Ticket)-Antrag an den Domänencontroller.

2. Der RODC hat das Kennwort des Anwenders noch nicht zwischengespeichert und gibt die TGT-Anfrage an einen Windows Server 2012-Domänencontroller weiter.

3. Der Domänencontroller authentifiziert den Anwender, stellt ein Ticket Granting Ticket (TGT) aus und weist dieses dem RODC zu.

4. Der RODC teilt dem Anwender das Ergebnis mit und sendet das TGT an die Arbeitsstation weiter.

5. Nachdem das TGT an den Anwender ausgestellt wurde, fragt der RODC beim schreibenden Domänencontroller nach, ob das Kennwort für zukünftige Authentifizierungen auf dem RODC zwischengespeichert werden darf. Der Domänencontroller überprüft die Replikationsrichtlinie für Kennwörter, ob das Kennwort repliziert werden darf.

6. Entspricht die Replikation den Richtlinien, darf das Kennwort auf dem RODC zwischengespeichert werden, und der RODC speichert das Kennwort für zukünftige Zwecke.

Im nächsten Dialogfeld 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 von Active Directory verwenden möchten (siehe Kapitel 11). 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/DVD brennen, mit der Post verschicken und diese anschließend auf dem Server einlesen.

Abbildg. 13.5 Festlegen des Quellmediums für die Active Directory-Replikation

Auf der Seite des Assistenten wählen Sie auch aus, von welchem Domänencontroller Sie die Replikation zum neuen Domänencontroller für die Installation ausführen wollen. Alle weiteren Fenster sind identisch mit der Installation des ersten Domänencontrollers.

Ein Beispielskript für die Installation eines schreibgeschützten Domänencontrollers für die PowerShell sehen Sie in Listing 13.1.

Listing 13.1 Installieren eines schreibgeschützten Domänencontrollers in der PowerShell

```
Import-Module ADDSDeployment
Install-ADDSDomainController `
-AllowPasswordReplicationAccountName @("CONTOSO\Zulässige RODC-Kennwortreplikationsgruppe")
`
-NoGlobalCatalog:$false `
-Credential (Get-Credential) `
-CriticalReplicationOnly:$false `
-DatabasePath "C:\Windows\NTDS" `
-DelegatedAdministratorAccountName "CONTOSO\joost" `
-DenyPasswordReplicationAccountName @("VORDEFINIERT\Administratoren", "VORDEFINIERT\Server-
Operatoren", "VORDEFINIERT\Sicherungs-Operatoren", "VORDEFINIERT\Konten-Operatoren",
"CONTOSO\Abgelehnte RODC-Kennwortreplikationsgruppe")
-DomainName "contoso.int"
-InstallDns:$true
-LogPath "C:\Windows\NTDS"
-NoRebootOnCompletion:$false
-ReadOnlyReplica:$true
-SiteName "Erbach"
-SysvolPath "C:\Windows\SYSVOL"
-Force:$true
```

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. Die Exchange Server 2003/2007/2010/2013-Versionen unterstützen keine RODCs für den Zugriff auf den globalen Katalog.
- Fällt die WAN-Verbindung zwischen RODC und einem normalen Domänencontroller aus, können am Standort mit dem RODC keine Kennwortänderungen der Anwender durchgeführt werden. Auch Computerkonten lassen sich nicht anlegen. Außerdem wird die Anmeldung aller Konten, deren Kennwort nicht auf den RODC repliziert ist, abgelehnt.
- Werden an einem Standort mit einem RODC neue Computerkonten aufgenommen, werden die dazu notwendigen RID (Relative Identifier) von einem schreibgeschützten Domänencontroller bezogen. Ein RODC verfügt über keinen RID-Pool.

Damit sich Benutzer aus der Domäne an einem RODC authentifizieren können, müssen diese zwingend in der Gruppe *Zulässige RODC-Kennwortreplikationsgruppe* sein, ansonsten wird die Anmeldung verweigert.

In den Eigenschaften des Computerkontos des schreibgeschützten Domänencontrollers auf der Registerkarte *Kennwortreplikationsrichtlinie* werden nach einem Klick auf die Schaltfläche *Erweitert* alle auf dem RODC zwischengespeicherten Kennwörter und Benutzer angezeigt.

Delegierung der RODC-Installation

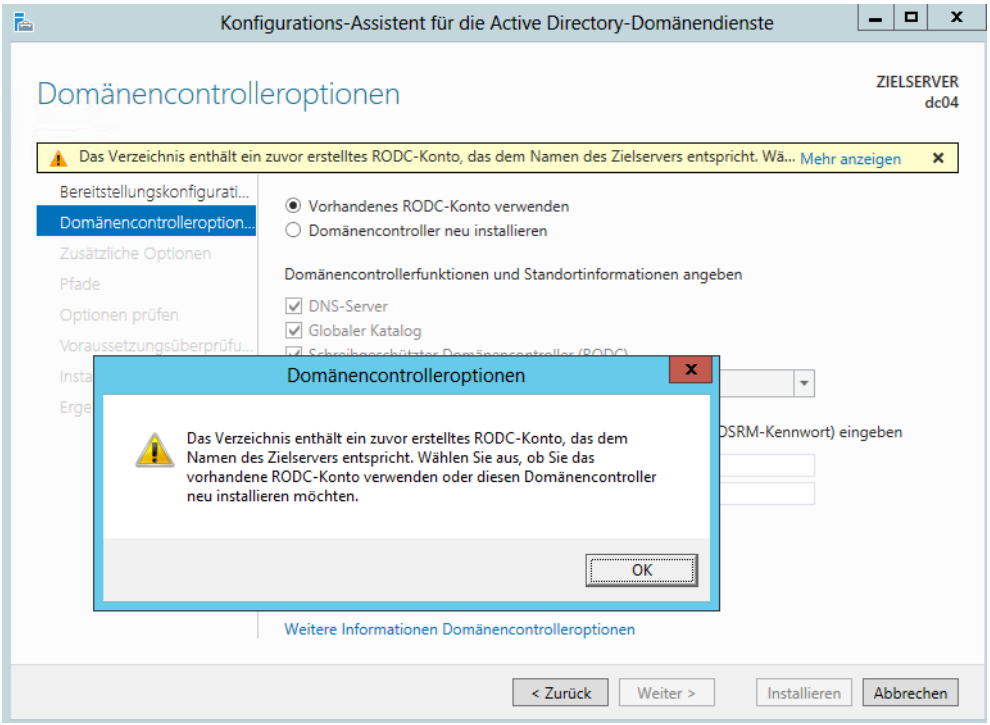
Da es sich bei RODC meist um Server in Niederlassungen handelt, besteht auch die Möglichkeit, die Installation des Servers zu delegieren. Dazu wird vorher ein neues Computerkonto für den RODC in der Domäne erstellt und der Administrator vor Ort darf den Server dann installieren und zum RODC der Domäne 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*.
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 den Server-Manager starten.

Sie können ein Konto für einen schreibgeschützten Domänencontroller auch in der PowerShell mit dem Cmdlet *Add-ADDSReadOnlyDomainControllerAccount* durchführen. Installieren Sie einen neuen schreibgeschützten Domänencontroller, können Sie ein bereits existierendes Konto verwenden.

Dabei überprüft der Assistent, ob der aktuelle Servername mit dem Namen eines vorbereiteten Kontos übereinstimmt, sobald ein Administrator den Server heraufstufen will. Der Server darf allerdings noch kein Mitglied der Domäne sein.

Abbildg. 13.6 Installieren eines neuen RODCs mit einem existierenden Computerkonto



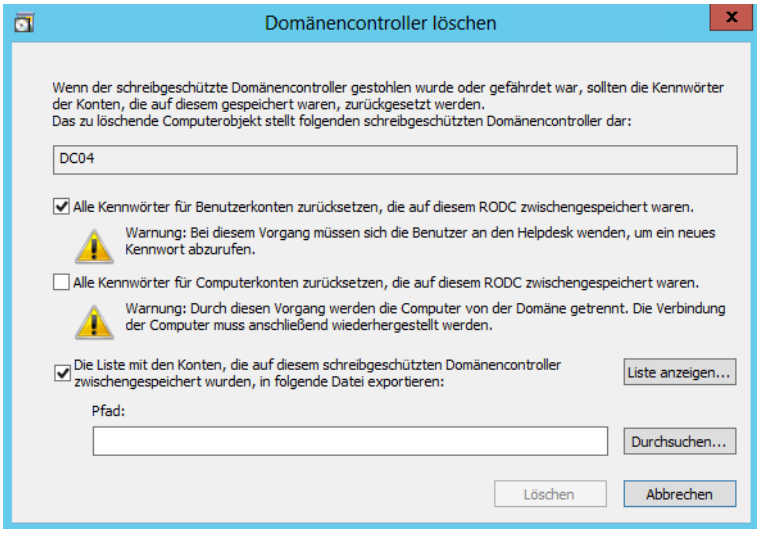
RODC löschen

Wenn Sie ein Computerkonto eines RODCs löschen, können Sie über einen Assistenten veranlassen, dass alle Benutzer, deren Konto auf dem RODC gespeichert war, ihr Kennwort ändern müssen. Sie können auch eine Liste der Benutzer erstellen lassen. Das ist zum Beispiel sinnvoll, wenn ein RODC verloren gegangen ist und Sie das Konto aus Active Directory löschen lassen wollen.

HINWEIS Wird ein schreibgeschützter Domänencontroller gestohlen, enthält dieser ausschließlich nur die Daten der Benutzerkonten, die zur Replikation auf den Server explizit ausgewählt sind. 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, über das die Kennwörter der Benutzer und Computer, die auf den RODC repliziert sind, zurückgesetzt werden können.

Selbst wenn es einem Dieb gelingen sollte, die Daten vom RODC auszulesen, sind diese wertlos, weil sie zurückgesetzt wurden. Bei diesem Vorgang löscht Active Directory nicht die Benutzer- und Computerkonten selbst, sondern ausschließlich die Kennwörter. Diese Daten lassen sich außerdem nicht nur zurücksetzen, sondern über den Assistenten besteht zusätzlich eine Exportmöglichkeit der Konten.

Abbildg. 13.7 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 *DNS-Verwaltung* starten.

Überprüfen Sie, ob die Daten der DNS-Zonen auf den Domänencontroller repliziert wurden. Ist sichergestellt, dass die DNS-Daten repliziert sind, ist die DNS-Funktionalität auf dem zusätzlichen Domänencontroller vorhanden. Die Replikation kann allerdings durchaus einige Minuten dauern.

IP-Adresse und DNS-Server auf Domänencontrollern anpassen

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 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 Ausfall-

sicherheit ist es daher immer am besten, wenn ein Domänencontroller jeweils einen anderen Domänencontroller als bevorzugten DNS-Server verwendet. Nur wenn dieser bevorzugte Server nicht zur Verfügung steht, werden die eigenen Daten des Domänencontrollers verwendet. Haben Sie diese Einstellungen vorgenommen, können Sie mit Befehlszeilentool Nslookup überprüfen, ob die Namensauflösung auf den Domänencontrollern noch fehlerfrei funktioniert.

Öffnen Sie dazu eine Eingabeaufforderung und rufen Sie den Befehl *nslookup* auf. Geben Sie danach einmal die Bezeichnung des ersten und dann die des zweiten Domänencontrollers ein, also in diesem Beispiel *dc01.contoso.com* und *dc03.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. Mehr zum Thema lesen Sie in Kapitel 10 und 11.

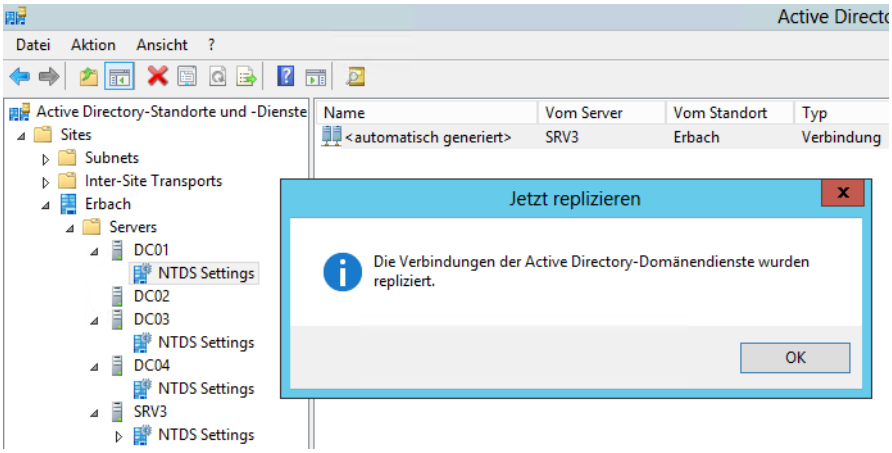
Replikation der beiden Domänencontroller überprüfen

Nach einigen Minuten sollten Sie die Replikation der beiden Domänencontroller überprüfen. Starten Sie dazu das Snap-In *Active Directory-Standorte und -Dienste* über das Menü *Tools* im Server-Manager. Navigieren Sie zum Knoten des Namens des Standorts und öffnen Sie den Knoten *Servers*.

An dieser Stelle sollten alle Domänencontroller angezeigt werden. Klicken Sie bei den Servern auf das Pluszeichen, sehen Sie darunter einen weiteren Eintrag mit der Bezeichnung *NTDS-Settings*. Klicken Sie auf diesen, wird auf der rechten Seite jeder Replikationspartner des Domänencontrollers angezeigt. Klicken Sie auf diese automatisch erstellten Verbindungen mit der rechten Maustaste, können Sie im Kontextmenü die Option *Jetzt replizieren* auswählen. Im Anschluss daran erscheint ein Fenster, das Sie über die erfolgreiche Replikation informiert.

HINWEIS Normale Domänencontroller richten Replikationsverbindungen nur zu anderen normalen Domänencontrollern ein. Schreibgeschützte Domänencontroller sind mit einer einseitigen Replikationsverbindung konfiguriert.

Abbildg. 13.8 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.

Sie sollten auch die Betriebsmaster auf den verschiedenen Servern optimal verteilen. Lesen Sie dazu die Anmerkungen in den Kapiteln 10 und 11.

Erstellen einer neuen untergeordneten Domäne

Eine weitere 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 Rootdomäne der Gesamtstruktur. Viele Unternehmen binden an diese Domäne weitere Domänen, die als untergeordnete Domänen bezeichnet werden.

Ein Beispiel hierfür ist die Domäne *contoso.int* als erste Domäne in einer Active Directory-Gesamtstruktur. Sie können an diese Domäne beliebig weitere untergeordnete Domänen anbinden, zum Beispiel die Domäne *de.contoso.int*. 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 Rootdomäne (oft auch als Stammdomäne bezeichnet) erstellt und die einzelnen Niederlassungen werden als untergeordnete Domänen angebunden. Auch wenn die Rootdomäne 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 Rootdomäne 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 Rootdomäne 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 Rootdomäne getrennt sind, besteht die Notwendigkeit, die DNS-Daten der untergeordneten Domäne in die Niederlassung zu replizieren. In diesem Fall müssen Berechtigungskonzepte erstellt werden, da ansons-

ten Administratoren der untergeordneten Domäne Änderungen an der DNS-Infrastruktur der übergeordneten Domäne durchführen können.

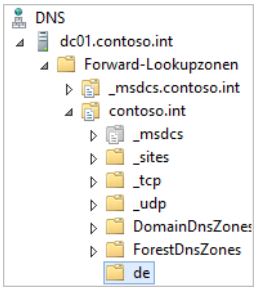
In vielen Unternehmen wird dieses Sicherheitsproblem dadurch gelöst, dass die untergeordnete Domäne als eigenständige Zone ausschließlich von den Administratoren der untergeordneten Domäne verwaltet wird. Dadurch ist sichergestellt, dass jede Domäne ihre eigene DNS-Zone verwaltet, damit die Administratoren 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 Rootdomäne auf den Rootdomänencontrollern. Diese Domäne befindet sich auf dem DNS-Server in der gleichen Zone wie die DNS-Domäne der Rootdomäne.

Um eine neue Domäne unterhalb einer DNS-Domäne zu erstellen, müssen Sie zunächst das Snap-In zur DNS-Verwaltung 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 Eintrag *Neue Domäne* aus. Im nächsten Fenster müssen Sie die Bezeichnung der neuen Domäne eingeben.

Abbildg. 13.9 Erstellen einer 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 Rootdomäne angeben. In diesem Beispiel lautet die Bezeichnung *de* unterhalb der Zone *contoso.int*. Nachdem Sie die Erstellung bestätigt haben, wird die neue Domäne unterhalb der Zone angezeigt. Weitere Angaben sind nicht erforderlich, da die Einstellungen für die Replikation der dynamischen Updates und Berechtigungen durch die übergeordnete Zone an die untergeordnete Domäne weitergegeben werden.

Damit Sie auf dem Domänencontroller der untergeordneten Domäne 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 Rootdomäne 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 dann 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. 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, selbst wenn unter Umständen die DNS-Server der untergeordneten Domäne nicht zur Verfügung stehen.

Da diese Aufgabe erst durchgeführt werden kann, wenn Active Directory auf den neuen Domänencontrollern installiert wurde, müssen Sie zunächst die Heraufstufung der untergeordneten Domänencontroller vornehmen.

Delegierung von DNS-Zonen

Die zweite Variante der Namensauflösung einer neuen untergeordneten Domäne ist die sogenannte Delegierung. Installieren Sie zunächst auf dem neuen Domänencontroller die DNS-Erweiterung. Anschließend erstellen Sie auf dem neuen DNS-Server eine neue Zone. Dabei gehen Sie so vor, wie in Kapitel 11 erläutert.

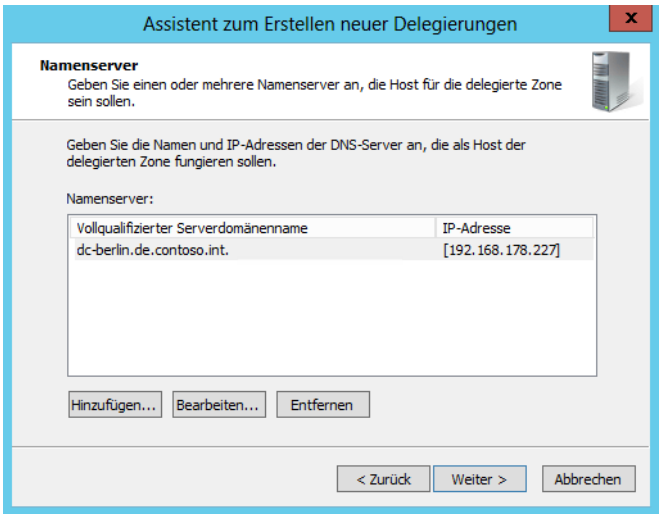
Die neue Zone erhält dieselbe Bezeichnung wie die neue untergeordnete Domäne. In diesem Beispiel wird der Domänencontroller *dc-berlin* der erste Domänencontroller der untergeordneten Domäne *de.contoso.int* unterhalb der Domäne *contoso.int*. Gehen Sie dazu folgendermaßen vor:

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.int*. Mehr zu diesem Thema lesen Sie in Kapitel 10 und 11.
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.int*. An dieser Stelle spielt die bereits vorhandene DNS-Domäne der Rootdomäne noch keinerlei Rolle. Achten Sie auf die dynamischen Updates der Zone (siehe Kapitel 11).

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 Rootdomäne 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 im Kontextmenü den Eintrag *Neue Delegierung* aus.

Abbildg. 13.10 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. 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 ist.

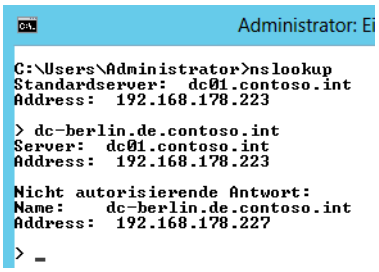
Wenn ein Client oder ein Server einen DNS-Server der übergeordneten Domäne als bevorzugten DNS-Server eingetragen hat und einen Namen der untergeordneten Domäne auflösen will (zum Beispiel ein zweiter Domänencontroller für die Active Directory-Replikation), kann nach der erfolgreichen Einrichtung der 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.

Im Assistenten müssen Sie den Namenserver 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. Dazu klicken Sie zunächst auf die Schaltfläche *Hinzufügen*.

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 Sie auf *OK*. Nach dieser Aktion wird dieser DNS-Server als Namenserver 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. Im Anschluss daran wird die delegierte Domäne abgeblendet in der DNS-Domäne angezeigt.

Überprüfen Sie jetzt mit dem Befehlszeilentool Nslookup, ob die Auflösung fehlerfrei funktioniert. Öffnen Sie dazu die Eingabeaufforderung und geben Sie auf dem DNS-Server der Rootdomäne (oder einem Client, der diesen als bevorzugten DNS-Server konfiguriert hat) den Befehl *nslookup* ein. Überprüfen Sie den FQDN des DNS-Servers der untergeordneten Domäne, in diesem Beispiel also *dc-berlin.de.contoso.com*. Die IP-Adresse des Servers muss fehlerfrei zurückgegeben werden. Das funktioniert aber erst dann, wenn Sie auf dem untergeordneten Domänencontroller DNS für die untergeordnete Domäne konfiguriert haben und sich der DNS-Server eingetragen hat. Gehen Sie hier so vor, wie in Kapitel 11 gezeigt. Lesen Sie auch die Anmerkungen in Kapitel 6 zu diesem Thema durch.

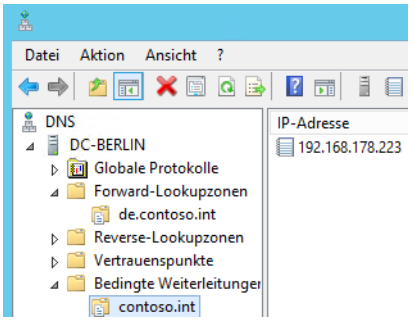
Abbildg. 13.11 Überprüfen der Namensauflösung von der übergeordneten zur untergeordneten Domäne



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 eine Weiterleitung:

1. Klicken Sie dazu mit der rechten Maustaste im Snap-In der DNS-Verwaltung auf *Bedingte Weiterleitungen*.
2. Wählen Sie im Kontextmenü den Eintrag *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.
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.

Abbildg. 13.12 Konfigurieren eines Weiterleitungsservers in der untergeordneten Domäne



5. Nachdem Sie diese Konfiguration vorgenommen haben, öffnen Sie wieder eine Eingabeaufforderung 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.int* ein untergeordneter Domänencontroller und *dc01.contoso.int* ein Domänencontroller der übergeordneten Domäne *contoso.int*.

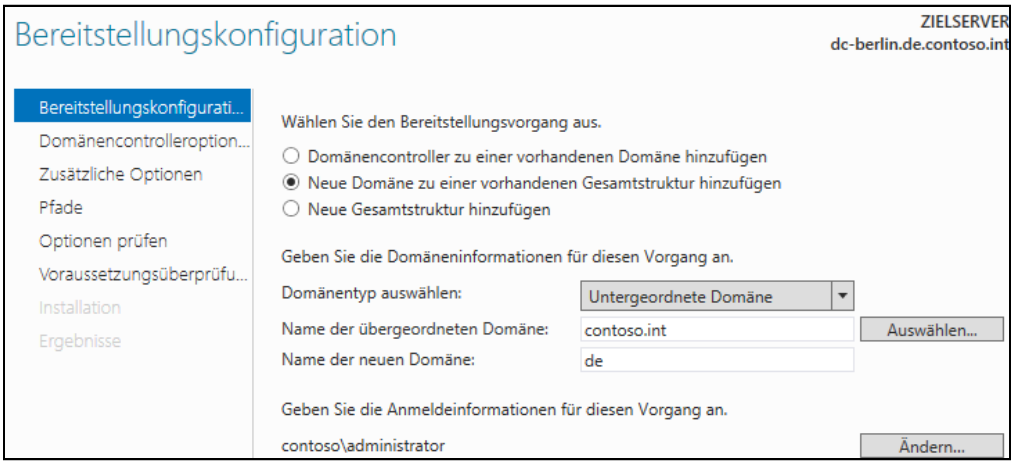
Achten Sie darauf, dass beim Einsatz von mehreren untergeordneten Domänen auch die Namensauflösung zwischen den untergeordneten Domänen untereinander funktioniert. Nur durch eine lückenlos konfigurierte Namensauflösung ist die Replikation in Active Directory sichergestellt. Damit haben Sie die Konfiguration der DNS-Einstellungen abgeschlossen. Die Namensauflösung sollte sowohl innerhalb der Domänen als auch zwischen den Domänen reibungslos funktionieren.

Heraufstufen eines Domänencontrollers für eine neue untergeordnete Domäne

Nachdem Sie sichergestellt haben, dass die Namensauflösung für die neue untergeordnete Domäne funktioniert und der zukünftige Active Directory-Domänencontroller der untergeordneten Domäne auch die Namen in der übergeordneten Domäne auflösen kann, können Sie mit dem Assistenten zur Einrichtung von Active Directory die neue Domäne erstellen. Dabei gehen Sie analog vor, wie in den Kapiteln 10 und 11 bereits behandelt. Sie installieren die Serverrolle der Active Directory-Domänendienste und starten den Assistenten zur Einrichtung.

Aktivieren Sie im Assistenten die Option *Neue Domäne zu einer vorhandenen Gesamtstruktur hinzufügen* aus. Wählen Sie aus, ob Sie einer vorhandenen Domäne eine weitere Domäne hinzufügen möchten, zum Beispiel *de.contoso.int* (untergeordnete Domäne), oder ob Sie in der Gesamtstruktur einen weiteren unabhängigen Namensraum hinzufügen möchten (Strukturdomäne), zum Beispiel der Gesamtstruktur *contoso.int* den Namensraum *woodgroove.local*. Beide Domänen können sich im gleichen Namensraum befinden. Mehr dazu erfahren Sie im nächsten Abschnitt dieses Kapitels.

Abbildg. 13.13 Erstellen einer neuen Domäne in einer vorhandenen Gesamtstruktur



Im Fenster geben Sie außerdem den Namen der übergeordneten Domäne und der neuen untergeordneten Domäne ein. Außerdem müssen Sie einen Benutzernamen festlegen, der das Recht hat, neue Domänen in die Gesamtstruktur aufzunehmen.

Auf der nächsten Seite wählen Sie die Funktionsebene der Domäne aus und die Optionen für den Domänencontroller (siehe auch Kapitel 10 und 11). Die Vorgehensweise ist identisch zur Installation einer neuen Gesamtstruktur, wie in den Kapiteln 10 und 11 bereits behandelt.

Sie können sich anschließend an dem Server an der untergeordneten Domäne anmelden und die Domäne wie jede andere auch verwalten. Von der Verwaltung unterscheiden sich untergeordnete Domänen nicht von übergeordneten Domänen, sie erleichtern jedoch die Verteilung der Administration innerhalb von Active Directory. Untergeordnete Domänen werden im Snap-In *Active Directory-Domänen und -Vertrauensstellungen* in der Baumstruktur entsprechend unter ihrer übergeordneten Domäne angezeigt.

HINWEIS Nachdem Sie den DNS-Server der neuen untergeordneten Domäne zum Domänencontroller heraufgestuft haben, sollten Sie die Zone der neuen Domäne ebenfalls in Active Directory integrieren und die Replikation der DNS-Daten so einstellen, wie Sie es wünschen.

Standardmäßig werden die Daten auf allen Domänencontrollern der neuen Domäne bereits repliziert und angezeigt, sobald die DNS-Funktion installiert wird. Sie sollten auch darauf achten, dass in den Netzwerkeinstellungen des neuen Domänencontrollers er selbst bzw. ein anderer Domänencontroller mit DNS-Funktionalität dieser Domäne als DNS-Server eingetragen ist. Auch den Betriebsmodus dieser Domäne müssen Sie separat zu den anderen Domänen in Ihrem Active Directory heraufstufen.

Ein Beispiel für das Erstellen einer untergeordneten Domäne in der PowerShell ist:

```
Install-ADDSDomain -NewDomainName de -ParentDomainName Contoso.int -DomainType Child
-SafeModeAdministratorPassword (Read-Host -Prompt "Kennwort:" -AsSecureString)
```

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.int* mit der untergeordneten Domäne *de.contoso.int*. In manchen Unternehmen kann es jedoch sinnvoll sein, unabhängige Namensräume zu erstellen, die zwar Bestandteil der Gesamtstruktur, aber vom Namen her von den anderen Domänen unabhängig sind.

Ein Beispiel wäre die neue Struktur *woodgroove.local* in der Gesamtstruktur *contoso.int*. 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 Rootdomäne der Gesamtstruktur, mit dem Unterschied, dass sie einen eigenen Namensraum aufweist.

Bevor Sie eine neue Struktur einführen können, müssen Sie auch hier zunächst die passende DNS-Infrastruktur erstellen. Bei der Erstellung einer neuen Struktur gibt es keine Möglichkeit, eine neue

Delegierung zu erstellen, 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 in 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*. 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 Rootdomänen der einzelnen Strukturen.

Wenn Anwender auf Daten verschiedener untergeordneter Domänen zugreifen wollen, muss die Authentifizierung daher immer den Weg bis zur Rootdomäne der eigenen Struktur gehen, dann zur Rootdomäne 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 anzulegen, müssen Sie zunächst 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 in diesem Kapitel 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 in 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 Rootdomäne 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. Kann der bevorzugte DNS-Server den DNS-Namen nicht auflösen und meldet dies 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 in Windows lassen sich weitere Einstellungen vornehmen, um die Zusammenarbeit mit DNS zu konfigurieren. 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)*. Tragen Sie als Nächstes zuerst den Namensraum der eigenen Struktur ein und hängen Sie danach die Namensräume der anderen Strukturen an. Lesen Sie sich dazu das Kapitel 5 durch, in dem wir diese Optionen detailliert behandeln, da diese auch für Mitgliedserver wichtig sind.

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.int* auflösen wollen, müssen Sie immer *dc01.contoso.int* eingeben. Zuerst sollten immer die eigene Domäne und der eigene Namensraum eingetragen sein, bevor andere Namensräume abgefragt werden. Wenn Sie diese Maßnahme durchgeführt haben, lässt sich mit Nslookup der Effekt überprüfen. Sie können an dieser Stelle lediglich *dc01* eingeben. Der Server befragt seinen bevorzugten DNS-Server, ob ein Server mit dem Namen *dc01.woordgroove.local* 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.int*.

Da die Zone *contoso.int* 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 Namensraums zeigt. Diese Vorgehensweise ist aber nicht korrekt, 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 einem größeren Active Directory 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 *woodgroove.local* einen neuen Eintrag *dc01* für den Domänencontroller *dc01.contoso.int* erstellen, der auf die IP-Adresse des Servers verweist, wird der Name als *dc01.woodgroove.local* aufgelöst, obwohl der eigentliche Name des Servers *dc01.contoso.int* ist. Dadurch funktioniert zwar die Auflösung, aber es wird ein falscher Name zurückgegeben.

Erstellen der neuen Domänenstruktur

Sobald sichergestellt ist, dass die Namensauflösung funktioniert und die Active Directory-Domänendienste-Rolle auf dem Server installiert ist, verwenden Sie den Assistenten, um Active Directory einzurichten. Aktivieren Sie im Assistenten die Option *Neue Domäne zu einer vorhandenen Gesamtstruktur hinzufügen*.

Wählen Sie aus, ob Sie einer vorhandenen Domäne eine weitere Domäne hinzufügen möchten, zum Beispiel *de.contoso.int* (untergeordnete Domäne), oder ob Sie in der Gesamtstruktur einen weiteren unabhängigen Namensraum, also eine Struktur hinzufügen möchten (Strukturdomäne), zum Beispiel der Gesamtstruktur *contoso.int* den Namensraum *woodgroove.local*. Beide Domänen können sich im gleichen Namensraum befinden. Die weitere Einrichtung entspricht der Konfiguration von untergeordneten Domänen.

Das Active Directory-Schema erweitern

Das Schema ist das Herzstück von Active Directory. Mit dem Schema wird definiert, welche Informationen im Verzeichnis abgelegt werden können. Gleichzeitig ist das Schema aus mehreren Gründen besonders sensibel. Je mehr Informationen in Active Directory abgelegt werden, desto größer wird die Datenbank. Die Performance ist allerdings nur bei bestimmten Operationen wie einer domänenweiten Abfrage betroffen.

Im Regelfall wird bei Abfragen über Indizes gearbeitet, sodass die Größe der Datenbank und damit die Erweiterung des Schemas dafür keine Rolle spielen. Es gibt zudem Abfragen, die nicht über den globalen Katalog laufen und die erfordern, dass alle Objekte angefasst werden.

Dazu zählen Operationen, bei denen sichergestellt werden muss, dass kein eindeutiger Name gesetzt wurde. In Active Directory können Objektklassen und Attribute hinzugefügt werden. Diese können nicht mehr entfernt werden. Objekte und Attribute lassen sich allenfalls deaktivieren. Das entspricht dem Ansatz der meisten professionellen Datenbankmanagementsysteme.

Im Kern bedeutet dies, dass Änderungen nicht vollständig rückgängig gemacht werden können und daher wohl überlegt sein müssen. Allerdings gilt, dass nicht mehr erforderliche Objekte und Attribute keine Auswirkungen auf die Größe von Active Directory und die Performance haben. Daher ist die Verwaltung des Schemas an die Gruppe der Schemaadmins gebunden. Die wichtigsten Fragestellungen sind:

- Die Schritte für die Änderung des Schemas erfordern eine gründliche Planung. Dazu gehört eine saubere Planung, je nachdem, ob Sie neue Objektklassen definieren oder Attribute zu bestehenden Objektklassen hinzufügen wollen.
- Überlegen Sie genau, ob die geplanten Änderungen am Schema erforderlich sind. Dies bedeutet, ob Informationen in Active Directory oder in einer Datenbank gespeichert werden. Bei Anwendungen, die auf Verzeichnisdienste zugreifen, wird häufig sowohl mit Informationen im LDAP-Verzeichnis und mit einem Datenbankmanagementsystem gearbeitet. Die Grundregel für das Design der Anwendungen ist, dass die stabilen Informationen zu Benutzern und anderen Verzeichnisobjekten im Verzeichnis abgelegt werden, während Daten, die sich permanent ändern, in der Datenbank gespeichert werden.
- Die oben bereits angesprochenen Problemstellungen im Zusammenhang mit der Erweiterung des Schemas müssen vertraut sein

- Es müssen Verwaltungsanwendungen oder Erweiterungen bestehender Verwaltungsanwendungen entwickelt werden, mit deren Hilfe die neuen Objekte und Attribute verwaltet werden können. Dazu ist erforderlich, dass Sie mit den Methoden für die Entwicklung und Erweiterung von Administrationsanwendungen vertraut sind.

Dies sind die wichtigsten Überlegungen, die vor der eigentlichen Implementierung von Änderungen im Schema durchgeführt werden müssen. Die Administration des Schemas kann über das MMC-Snap-In *Active Directory-Schema* erfolgen. Das Snap-In muss manuell in eine MMC eingefügt werden. Mit diesem Snap-In lassen sich die Informationen zu den Klassen und Attributen im Schema anzeigen.

Hier können Sie auch neue Klassen und Attribute anlegen und außerdem die Zugriffsberechtigungen für das Schema anpassen. Beim Erstellen einer Klasse müssen im ersten Schritt die Identifikationen für die Klasse eingegeben werden. Dazu zählen neben einem eindeutigen Namen die Objekt-ID im X.500-Schema und der Typ der Klasse. Im nächsten Dialogfeld können die Attribute konfiguriert werden, die in die Klasse aufgenommen werden sollen. Es werden zwei Arten unterschieden:

- Verbindliche Attribute müssen in jedem Fall eingegeben werden. Diese können nicht deaktiviert werden.
- Optionale Attribute können deaktiviert werden und müssen vom Benutzer nicht eingegeben werden

Mit der Festlegung von verbindlichen Attributen sollte Sie grundsätzlich sehr zurückhaltend sein. Wenn es Situationen gibt, in denen dieses Attribut bei einem Objekt doch nicht verwendet werden soll, darf es auf keinen Fall gesetzt werden. Im Zweifelsfall macht es mehr Sinn, Plausibilitätsprüfungen bei den Administrations-Anwendungen durchzuführen, über die Attributwerte verändert werden können. Bei den Attributen sind zunächst die Namen zu definieren. Zusätzlich müssen Syntax und Wertebereich konfiguriert werden. Für die Syntax gibt es eine Vielzahl vorgegebener Auswahlen. Mit der Option *Mehrwertig* kann konfiguriert werden, dass mehrere Werte für dieses Attribut eingegeben werden können. Das ist zum Beispiel bei Telefonnummern sinnvoll.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie zusätzliche Domänencontroller, auch schreibgeschützte Domänencontroller, im Netzwerk integrieren. Auch die Erweiterung von Active Directory mit zusätzlichen Domänen und Domänenstrukturen war Thema dieses Kapitels. Wir sind auch ausführlich auf die Zusammenarbeit von DNS und Active Directory eingegangen.

Im nächsten Kapitel widmen wir uns der Verwaltung verschiedener Active Directory-Standorte sowie der Replikation zwischen verschiedenen Domänencontrollern.

Kapitel 14

Active Directory – Replikation

In diesem Kapitel:

Ein weiterer wichtiger Bereich in der Verwaltung und Erstellung von Active Directory ist die Replikation der Domänencontroller, vor allem über mehrere Standorte hinweg. Active Directory-Domänen lassen sich über mehrere physische Standorte verteilen. Die Trennung der einzelnen Standorte in Active Directory erfolgt durch IP-Subnetze. Dazu müssen die Administratoren eines Unternehmens alle IP Subnetze anlegen, die im Unternehmen verwendet werden, und diese Subnetze wiederum einzelnen Standorten zuweisen. Zwischen den Standorten können Standortverknüpfungen erstellt werden, über die alle Domänencontroller ihre Daten replizieren.

Die Replikation zwischen Standorten erfolgt mit komprimierten Daten und weit weniger häufig als innerhalb eines LANs. Die Hauptaufgabe von Standorten besteht darin, den Datenverkehr über WAN-Leitungen so niedrig wie möglich zu halten und die Replikation von Domänencontrollern zu optimieren. In diesem Kapitel zeigen wir Ihnen, wie Sie die Replikation einrichten und Fehler beheben.

HINWEIS Im Kapitel 10 haben wir Ihnen bereits einige neue Cmdlets für die Verwaltung von Active Directory gezeigt. Auch für die Einrichtung der Replikation können Sie die PowerShell verwenden. Eine Liste der verfügbaren Befehle erhalten Sie durch Eingabe von *Get-Command *adreplication**. Um sich eine Hilfe zu den Cmdlets anzuzeigen, verwenden Sie *Get-Help <Cmdlet>*.

Grundlagen der Replikation

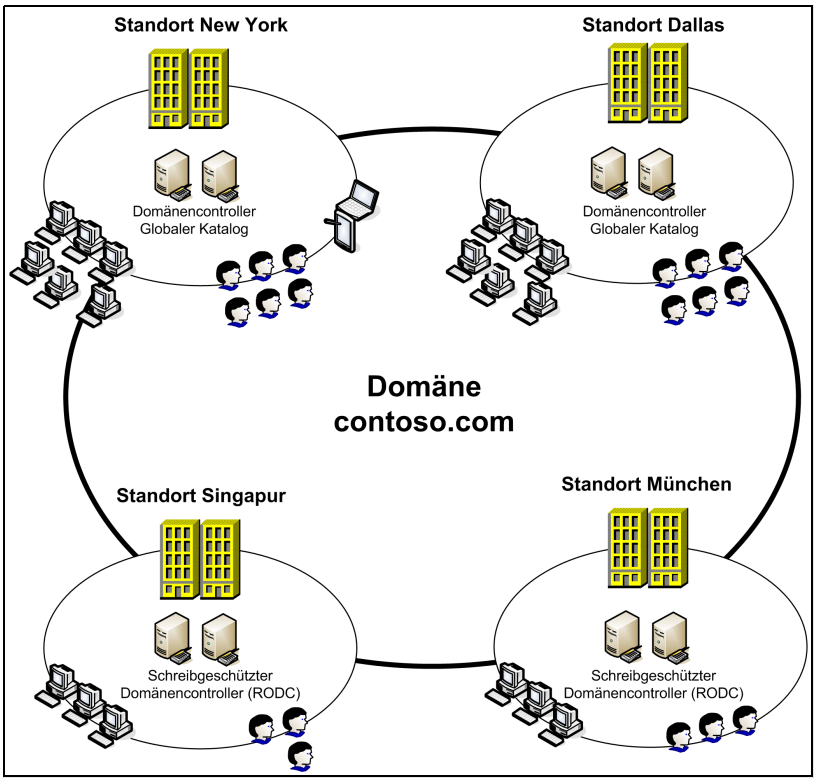
Das Active Directory verwendet einen integrierten Dienst, der die Replikation innerhalb und zwischen Standorten automatisch steuert. Dieser Dienst, Konsistenzprüfung (Knowledge Consistency Checker, KCC) genannt, verbindet die Domänencontroller der verschiedenen Standorte und erstellt automatisch eine Replikationstopologie auf Basis der definierten Zeitpläne und Standortverknüpfungen. 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 sogenannte Bridgeheadserver, welche die Informationen ihres Standorts 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. Damit Sie die Replikation zwischen Standorten nutzen können, müssen Sie zunächst Standorte definieren. Diesen Standorten müssen Sie alle IP-Subnetze zuweisen, die in Ihrem Unternehmen eingesetzt werden. Als Nächstes müssen Sie zwischen den Standorten Standortverknüpfungen herstellen und schließlich die bereits vorhandenen Domänencontroller auf die einzelnen Standorte verteilen.

Wenn Sie Standorte definiert haben, werden zukünftig Domänencontroller abhängig von ihrer IP-Adresse automatisch dem Standort zugewiesen, zu dessen Subnetz die IP-Adresse gehört. Bereits vorhandene Domänencontroller, oder bereits einem Standort zugewiesene, müssen nachträglich manuell innerhalb des Snap-Ins *Active Directory-Standorte und -Dienste* dem richtigen Standort zugewiesen werden. Sie können auch während der Heraufstufung von Domänencontrollern bereits den Standort zuweisen. Das geht aber auch jederzeit nachträglich.

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 sein, allerdings können Sie die Domäne von einem zentralen Standort aus verwalten, von dem die Änderungen auf die einzelnen Standorte repliziert werden können.

Abbildg. 14.1 AD-Replikation im Überblick

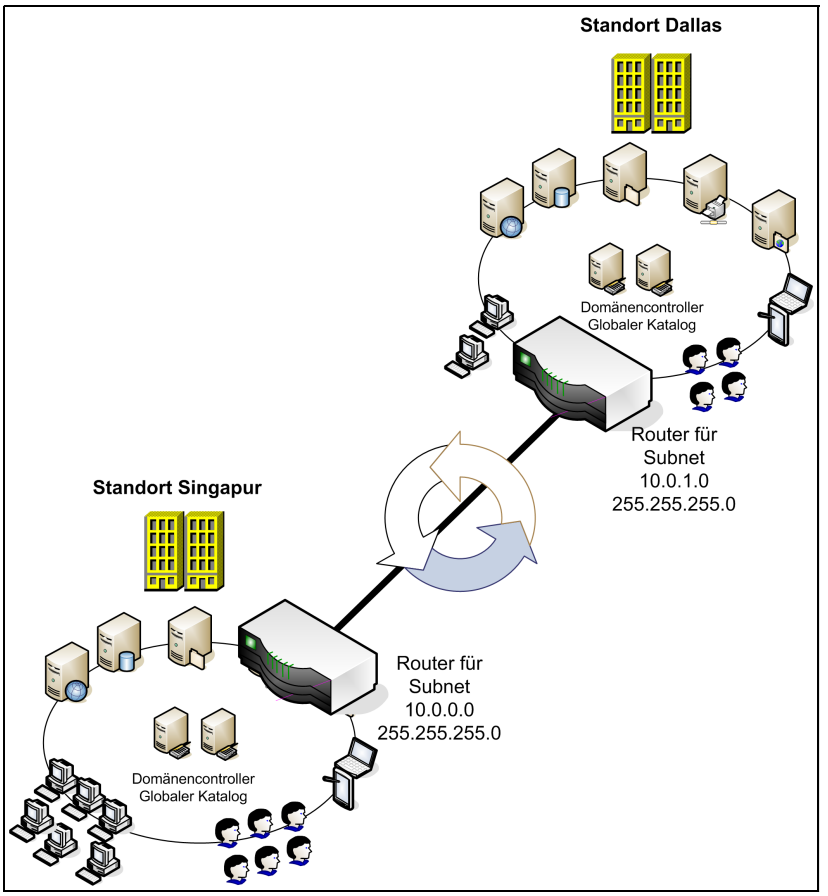


Konfiguration der Routingtopologie in Active Directory

Die Replikation zwischen verschiedenen Standorten in 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 Active Directory
- Erstellen von IP-Subnetzen und Zuweisen an die Standorte
- Erstellen von Standortverknüpfungen für die Active Directory-Replikation
- Konfiguration von Zeitplänen und Kosten für die optimale Standortreplikation

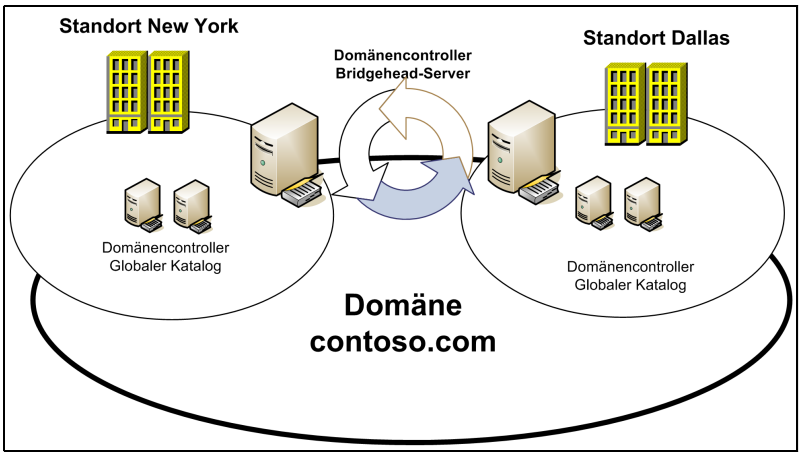
Abbildg. 14.2 Standorte auf Basis von IP-Subnetzen



Damit Sie die standortübergreifende Replikation von Active Directory verwenden können, sollten Sie in jedem Standort, an dem später ein Domänencontroller angeschlossen ist, ein unabhängiges IP-Subnetz verwenden. Dieses IP-Subnetz wird in der Active Directory-Verwaltung hinterlegt und dient fortan zur Unterscheidung der Standorte in Active Directory.

Das wichtigste Verwaltungswerkzeug, um Standorte in Active Directory zu verwalten, ist das Snap-In *Active Directory-Standorte und -Dienste*. Um neue Standorte zu erstellen, müssen Sie Mitglied der Gruppe *Organisations-Administratoren* sein. Administratoren, die nicht Mitglieder dieser Gruppe sind, dürfen keine Standorte in Active Directory erstellen.

Abbildg. 14.3 Die Replikation zwischen Standorten nehmen Bridgehead-Server vor



Es ist nicht unbedingt notwendig, dass jeder Standort mit der Zentrale durch eine Sterntopologie angebunden ist. Die Replikation in 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.

Active Directory unterscheidet auf Basis dieser IP-Subnetze, ob Domänencontroller zum gleichen oder zu unterschiedlichen Standorten gehören, und steuert entsprechend die Replikation

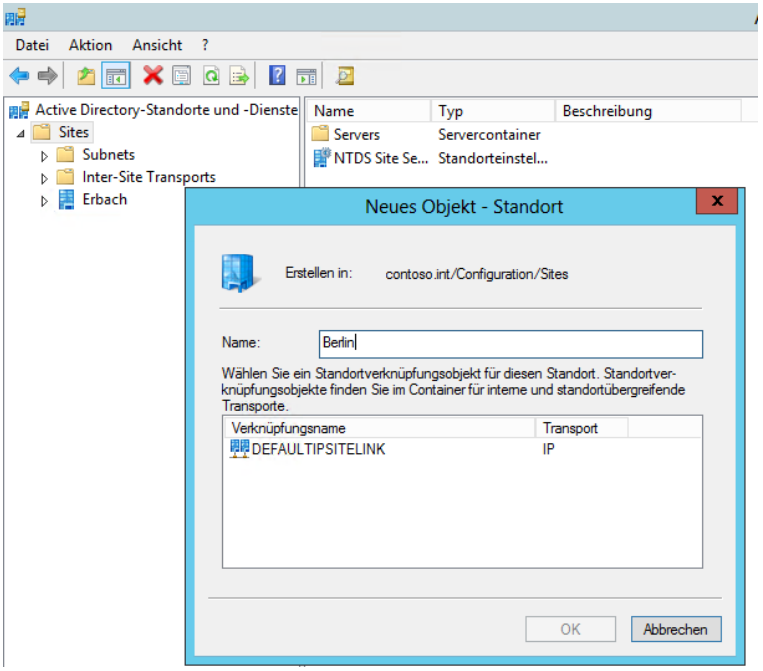
Erstellen von neuen Standorten über *Active Directory-Standorte und -Dienste*

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 Eintrags *Sites* der erste Standort als *Standardname-des-ersten-Standorts* bezeichnet. Sie finden das Snap-In am schnellsten über den Server-Manager im Menü *Tools*. Im ersten Schritt sollten Sie für diesen Standardnamen den richtigen Namen eingeben, indem Sie ihn mit der rechten Maustaste anklicken und im Kontextmenü den Befehl *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 auf *Sites* und wählen im Kontextmenü den Eintrag *Neuer Standort* aus.

Sie können Standorte auch in der PowerShell erstellen. Dazu verwenden Sie den Befehl *New-ADReplicationSite <Standort>*.

Abbildg. 14.4 Erstellen eines neuen Standorts in Active Directory



Es öffnet sich ein neues Fenster, in dem Sie den Namen des Standorts 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 Standorts zunächst diese Standortverknüpfung.

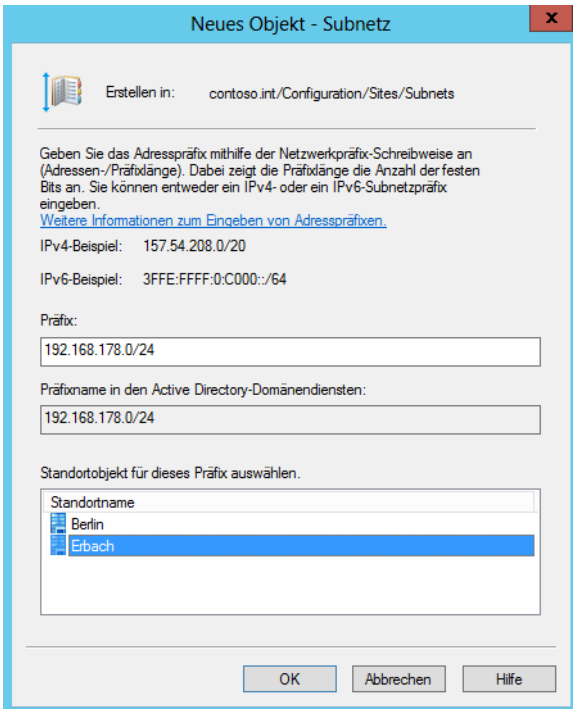
Bestätigen Sie die Erstellung mit *OK*, erhalten Sie eine Meldung angezeigt, welche Aufgaben nach der Erstellung noch notwendig sind. Bestätigen Sie diese Meldung, damit der Standort erstellt wird. Anschließend erscheint der neue Standort im Snap-In. Legen Sie auf die gleiche Weise alle Standorte in Ihrer Gesamtstruktur an. Nur Mitglieder der Gruppe *Organisations-Admins* dürfen neue Standorte in Active Directory erstellen.

TIPP Erstellen Sie eine CSV-Datei, die mit der Zeile *name* beginnt, können Sie eine Liste von Standorten in eigenen Zeilen erstellen. Diese können Sie dann auf einen Schlag mit dem Befehl *Import-Csv –Path C:\newsites.csv | New-ADReplicationSite* als Standort anlegen.

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* auf den Konsoleneintrag *Subnets* und wählen 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.

Abbildg. 14.5 Erstellen von Subnetzen in Windows Server 2012 R2



In Windows Server 2012 R2 können Sie auch Subnetze auf IPv6-Basis erstellen. Nachdem Sie das Subnetz erstellt haben und die Erstellung mit *OK* bestätigen, wird es unterhalb des Konsoleneintrags *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 Eintrag *Subnets* in der Konsole 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

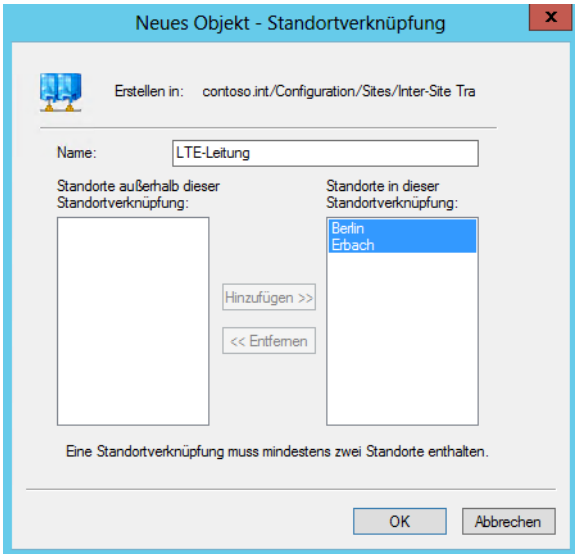
Nachdem Sie Standorte und die in den Standorten vorhandenen IP-Subnetze erstellt haben, können Sie neue *Standortverknüpfungen* anlegen. Bei der Installation von Active Directory wird bereits automatisch die Standortverknüpfung *DEFAULTIPSITELINK* angelegt. Für viele Unternehmen reicht diese Verknüpfung bereits aus.

Wenn Sie in Ihrem Unternehmen verschiedene Bandbreiten von WAN-Leitungen einsetzen, macht es Sinn, auch verschiedene Standortverknüpfungen zu erstellen. Sie können auf Basis jeder Stand-

ortverknüpfung 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 von *Inter-Site Transports* und wählen im Kontextmenü den Eintrag *Neue Standortverknüpfung* aus.

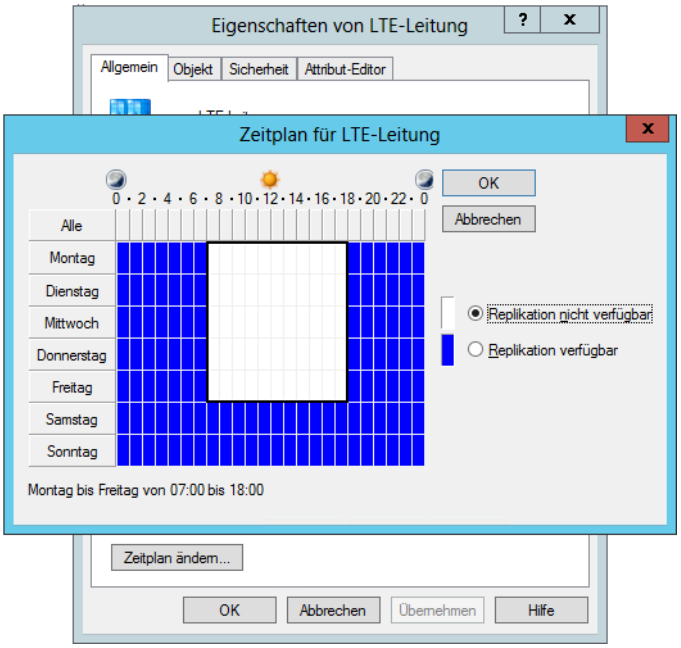
Abbildg. 14.6 Erstellen von Standortverknüpfungen zur Anbindung von Niederlassungen



Nachdem Sie die Erstellung einer neuen Standortverknüpfung gewählt haben, erscheint das Fenster, in dem Sie die Bezeichnung der Standortverknüpfung sowie die Standorte eingeben. 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 <> Frankfurt*, oder auch die Art der Verbindung zwischen den verschiedenen Niederlassungen.

In diesem Fenster können Sie auswählen, welche Standorte mit dieser Standortverknüpfung verbunden sein sollen. 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.

Abbildg. 14.7 Konfigurieren der Replikation von verschiedenen Standorten



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.

Den Befehl *Neue Standortverknüpfungsbrücke* im Kontextmenü 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 Elements *IP* unterhalb von *Inter-Site Transports* aufrufen und das Kontrollkästchen *Brücke zwischen allen Standortverknüpfungen herstellen* deaktivieren.

TIPP Neue Standortverknüpfungen erstellen Sie auch in der PowerShell. Ein Beispiel dafür ist:

```
New-ADReplicationSiteLink CORPORATE-BRANCH1 -SitesIncluded CORPORATE,BRANCH1 -
OtherAttributes @{'options'=1}
```

Die Kosten und den Zeitrahmen der Synchronisierung können Sie ebenfalls in der PowerShell festlegen:

```
Set-ADReplicationSiteLink CORPORATE-BRANCH1 -Cost 100 -ReplicationFrequencyInMinutes 15
```

Zuweisen der Domänencontroller zu den Standorten

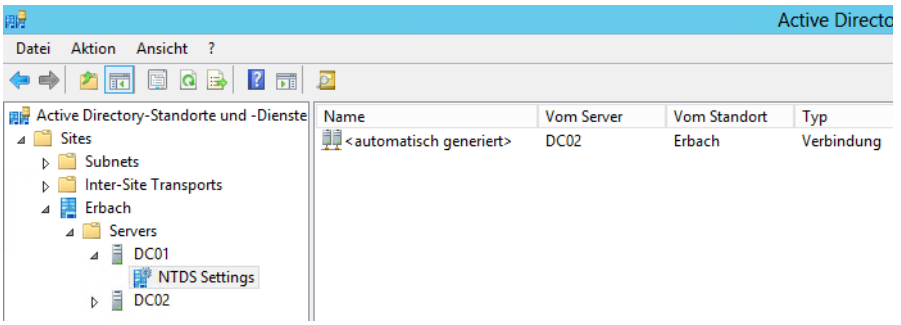
Nachdem Sie die Routingtopologie erstellt haben, werden neu installierte Domänencontroller durch ihre IP-Adresse automatisch dem richtigen Standort zugewiesen. Bereits installierte Domänencontroller müssen Sie jedoch manuell an den richtigen Standort verschieben.

Klicken Sie dazu den Server im Snap-In *Active Directory-Standorte und -Dienste* mit der rechten Maustaste an und wählen Sie im Kontextmenü die Option *Verschieben* aus. Daraufhin werden Ihnen alle Standorte angezeigt und Sie können den neuen Standort des Domänencontrollers auswählen. Nachdem Sie den Domänencontroller an einen anderen Standort verschoben haben, sollten Sie den Server neu starten.

Sie können einen Domänencontroller auch per Ziehen/Ablegen 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 Standorts passen.

Die Replikationsverbindungen richtet Windows Server 2012/2012 R2 automatisch ein. Sie sehen diese im Snap-In *Active Directory-Standorte und -Dienste* über *Sites/<Standort>/<Servers>/<Servername>/NTDS-Settings*. Sie können hier auch manuelle Verbindungen einrichten, indem Sie über das Kontextmenü *Neue Verbindung für die Active Directory-Domänendienste* auswählen.

Abbildg. 14.8 Anzeigen von Replikationsverbindungen zwischen Domänencontrollern



Domänencontroller können Sie auch in der PowerShell an neue Standorte verschieben:

```
Get-ADDomainController <Name des Servers> | Move-ADDirectoryServer -Site <Name des
Standorts>
```

Sie können die Replikationsverbindungen auch in der PowerShell anzeigen. Dazu verwenden Sie den Befehl *Get-ADReplicationConnection*.

Abbildg. 14.9 Anzeigen der Replikationsverbindungen in der PowerShell

```
PS C:\Users\Administrator> get-adreplicationconnection


AutoGenerated                       : True
DistinguishedName                   : CN=db723d66-4c79-4709-92b2-0ba792b52cea,CN=NTDS
                                      Settings,CN=DC01,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
InterSiteTransportProtocol          :
Name                                : db723d66-4c79-4709-92b2-0ba792b52cea
ObjectClass                         : nTDSConnection
ObjectGUID                          : 7496dc68-a162-4fe6-97b1-691310ac92cd
PartiallyReplicatedNamingContexts   : {}
ReplicatedNamingContexts            : {DC=ForestDnsZones,DC=contoso,DC=int, DC=DomainDnsZones,DC=contoso,DC=int,
                                      CN=Schema,CN=Configuration,DC=contoso,DC=int,
                                      CN=Configuration,DC=contoso,DC=int...}
ReplicateFromDirectoryServer        : CN=NTDS
                                      Settings,CN=DC02,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
ReplicateToDirectoryServer          : CN=DC01,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
ReplicationSchedule                 : System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule

AutoGenerated                       : True
DistinguishedName                   : CN=e2aa7468-7b64-4939-a87d-73e88706bb59,CN=NTDS
                                      Settings,CN=DC01,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
InterSiteTransportProtocol          :
Name                                : e2aa7468-7b64-4939-a87d-73e88706bb59
ObjectClass                         : nTDSConnection
ObjectGUID                          : 28f301c2-86dd-485c-aa38-aac608cd8b78
PartiallyReplicatedNamingContexts   : {}
ReplicatedNamingContexts            : {DC=ForestDnsZones,DC=contoso,DC=int, DC=DomainDnsZones,DC=contoso,DC=int,
                                      CN=Schema,CN=Configuration,DC=contoso,DC=int,
                                      CN=Configuration,DC=contoso,DC=int...}
ReplicateFromDirectoryServer        : CN=NTDS Settings,CN=DC-KLON,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=conto
                                      so,DC=int
ReplicateToDirectoryServer          : CN=DC01,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
ReplicationSchedule                 : System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule


PS C:\Users\Administrator> _
```

TIPP Sie können sich in der PowerShell auch ausführliche Informationen zu den einzelnen Standorten anzeigen lassen. Dazu verwenden Sie den Befehl *Get-ADReplicationSite –Filter **.

Um sich nur den Namen anzeigen zu lassen, verwenden Sie *Get-ADReplicationSite -Filter * | ft Name*, eine Liste der Domänencontroller und Standorte erhalten Sie mit *Get-ADDomainController –Filter * | ft Hostname,Site*.

Abbildg. 14.10 Anzeigen von Informationen zu Active Directory-Standorten in der PowerShell

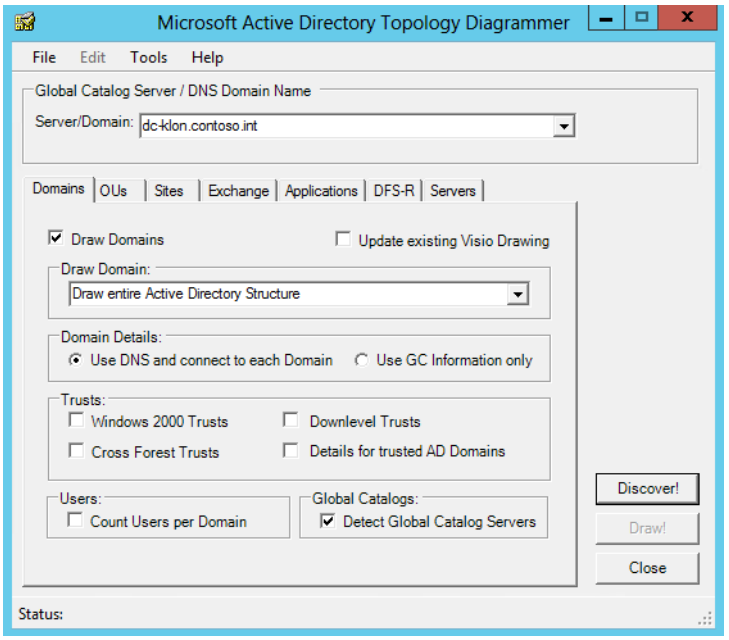
```
PS C:\Users\Administrator.CONTOSO> Get-ADReplicationSite -Filter *


Description                         :
DistinguishedName                   : CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
InterSiteTopologyGenerator          : CN=NTDS
                                      Settings,CN=DC01,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC
ManagedBy                           :
Name                                : Erbach
ObjectClass                         : site
ObjectGUID                          : 3025971a-353a-4b34-b949-02a46cfc673b
ReplicationSchedule                 : System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule
UniversalGroupCachingRefreshSite    :
```

Microsoft Active Directory Topology Diagrammer

Mit dem kostenlosen Tool Active Directory Topology Diagrammer, welches Microsoft im Downloadcenter zur Verfügung stellt, erstellen Sie auf Basis von LDAP-Abfragen eine Microsoft Visio-Zeichnung Ihrer Umgebung. Diese können Sie nachträglich mit Microsoft Visio bearbeiten.

Das Diagramm zeigt Domänen, Standorte, Server, Organisationseinheiten und andere Informationen zur Gesamtstruktur an. Nach der Installation finden Sie das Tool im Verzeichnis *C:\Program Files (x86)\Microsoft Active Directory Topology Diagrammer*. Nach dem Start geben Sie den Domänencontroller ein, mit dem sich das Tool verbinden soll, und können so die Daten von Active Directory einlesen lassen. Zum Tool gehört auch eine Hilfedatei.

Abbildg. 14.11 Verbindungsaufbau mit der Active Directory-Gesamtstruktur



Die Konsistenzprüfung (Knowledge Consistency Checker)

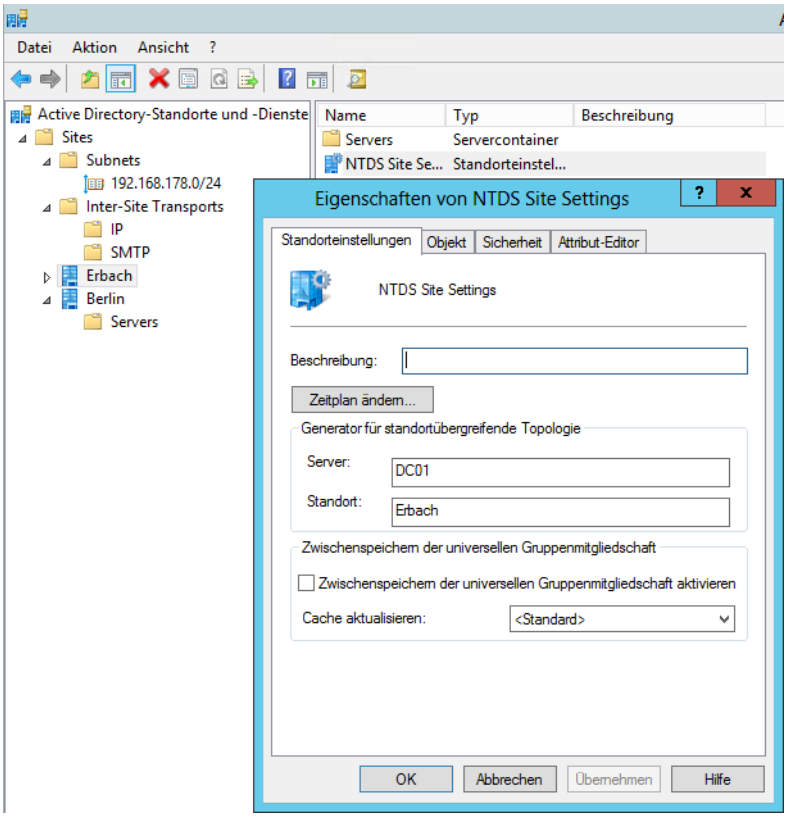
Wenn Sie die Routingtopologie erstellt haben, kann der Knowledge Consistency Checker (KCC) die Verbindung der Domänencontroller automatisch herstellen. Der KCC konfiguriert auf Basis der konfigurierten Standorte, der Standortverknüpfungen und deren Zeitplänen und Kosten sowie den enthaltenen Domänencontrollern 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. Innerhalb eines Standorts 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 Bridgeheadserver (Brückenkopfserver) 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 jeden 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 Eintrags auf, wird Ihnen im Abschnitt *Generator für standortübergreifende Topologie* der derzeitige ISTG angezeigt.

Abbildg. 14.12 Anzeigen des ISTG eines Standorts



An dieser Stelle können Sie auch das Kontrollkästchen *Zwischenspeichern der universellen Gruppenmitgliedschaft aktivieren* einschalten. Diese Option hat dann eine Bedeutung, wenn Sie am Standort keinen globalen Katalog betreiben, der die Mitgliedschaften der universellen Gruppen zwischenspeichert, oder Sie diesen globalen Katalog entlasten wollen.

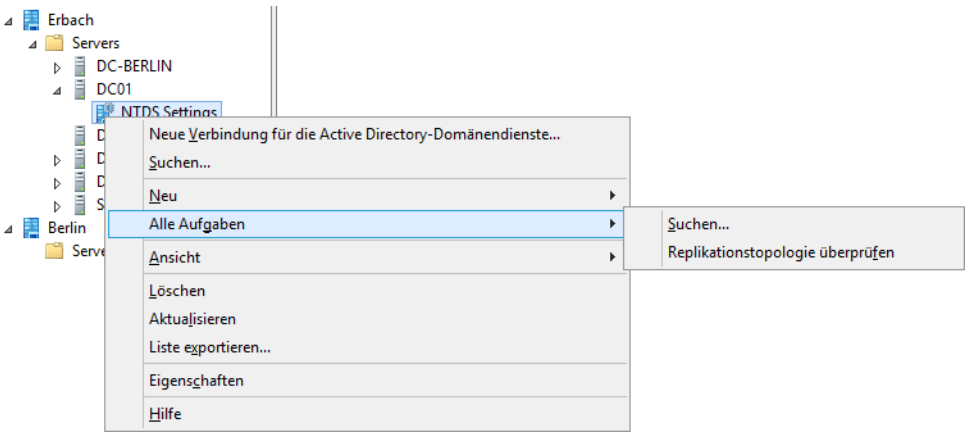
Da universelle Gruppen Mitglieder aus mehreren Domänen und Standorten enthalten können, ist die Information, welche Benutzerkonten Mitglied sind, bei der Anmeldung eines Benutzers oder dem Zugreifen auf Ressourcen sehr wichtig. Haben Sie an einem Standort keinen globalen Katalog installiert, sollten 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 beziehungsweise der globale Katalog wird entlastet
- 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 den derzeitigen ISTG-Rolleninhaber des Standorts.
4. Klicken Sie mit der rechten Maustaste auf den Konsoleneintrag *NTDS-Settings* und wählen Sie im Kontextmenü den Untermenüeintrag *Alle Aufgaben/Replikationstopologie überprüfen* aus.

Abbildg. 14.13 Manuelles Starten der Routingtopologieüberprüfung



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.

Sie können die Replikation zwischen zwei Domänencontrollern jederzeit manuell starten. Die Verbindungen, die der KCC erstellt hat, werden automatisch angezeigt. 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, wird eine Fehlermeldung angezeigt.

Fehler bei der Active Directory-Replikation beheben

Häufige Fehlerursache ist in Active Directory mit vielen Niederlassungen und zahlreichen Domänencontrollern die Replikation zwischen diesen Standorten. Beim Einsatz eines einzelnen Standorts werden nur selten Probleme auftreten. Bei der Fehlersuche bezüglich der Replikation sollten Sie zunächst die beteiligten Domänencontroller überprüfen und testen, ob diese innerhalb ihres Standorts 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 mithilfe dieser Fehlermeldungen können Sie auf den nachfolgend genannten Internetseiten eine Lösung für das Problem finden:

- *http://www.eventid.net* [Ms179-K14-01]
- *http://www.experts-exchange.com* [Ms179-K14-02]
- *http://support.microsoft.com* [Ms179-K14-03]

Bei Problemen mit der Active Directory-Replikation sollte immer eine vollständige Diagnose der Domänencontroller vorausgehen, die bereits auf den vorigen Seiten beschrieben wurde. Fertigen Sie eine einfache Skizze der Replikationsverbindungen der Domänencontroller an und halten Sie genau fest, welche Domänencontroller sich nicht mehr mit welchen anderen Domänencontrollern replizieren können. Wenn Sie mithilfe dieser Skizze die Probleme verdeutlichen, werden Sie schnell erkennen, welcher Domänencontroller die Hauptursache für das Problem ist.

Suche mit der Active Directory-Diagnose

Wenn die Replikationen zu Domänencontrollern im gleichen Standort funktionieren und auch die Replikation zu anderen Standorten, lässt sich das Problem vielleicht besser eingrenzen. Auch die Replikationsprobleme zu dem oder den Domänencontrollern, zu denen nicht repliziert werden kann, sollten eingegrenzt werden.

Zunächst sollten Sie die Replikationswege von Active Directory aufzeichnen und genau feststellen, welche Domänencontroller sich nicht mehr mit anderen Domänencontrollern replizieren. An dieser Stelle können Sie als Nächstes mit den Diagnosetools wie Dcdiag die problematischen Domänencontroller genauer untersuchen.

Ausschließen der häufigsten Fehlerursachen

Bevor Sie mit Tools die Replikation genauer untersuchen, sollten Sie zunächst die gravierendsten und häufigsten Fehlerursachen ausschließen:

- Liegt auf dem Domänencontroller, der sich nicht mehr replizieren kann, ein generelles Problem vor, welches sich mit Dcdiag herausfinden lässt? Liegen also die Probleme überhaupt nicht in der Replikation, sondern hat der Domänencontroller eine Funktionsstörung?
- Wurde auf dem Domänencontroller eine Software installiert, welche die Replikation stören kann, wie Sicherheitssoftware, Virenscanner, Firewall oder sonstiges?
- Ist auf dem Domänencontroller, mit dem die Replikation nicht mehr stattfinden kann, die Hardware ausgefallen?
- Liegt unter Umständen nur ein Leitungs-, Router- oder Firewallproblem vor?
- Lässt sich der entsprechende Domänencontroller noch anpingen und lässt sich der DNS-Name des Servers auflösen?
- Gibt es generelle Probleme mit der Authentifizierung zwischen den Domänencontrollern, die durch Zugriff verweigert-Meldungen gemeldet werden?
- Sind die Replikationsintervalle zwischen Standorten so kurz eingestellt, dass die vorherige Replikation noch nicht abgeschlossen ist und die nächste bereits beginnt?
- Wurden Änderungen an der Routingtopologie vorgenommen, die eine Replikation verhindern können?

Nltest zum Erkennen von Standortzuweisungen eines Domänencontrollers

Falls Replikationsprobleme in Active Directory auftreten, sollten Sie zunächst sicherstellen, dass die Domänencontroller, die Probleme bei der Replikation haben, für den richtigen Standort konfiguriert sind. Zu diesem Weg geben Sie in der Eingabeaufforderung den Befehl *nltest /dsgetsite* ein. In der Anzeige sehen Sie, welchem Standort der Domänencontroller zugewiesen ist und ob er seinen Standort auch erkennt. Wird an dieser Stelle der Standort fehlerfrei aufgelöst, ist diese Konfiguration schon mal in Ordnung.

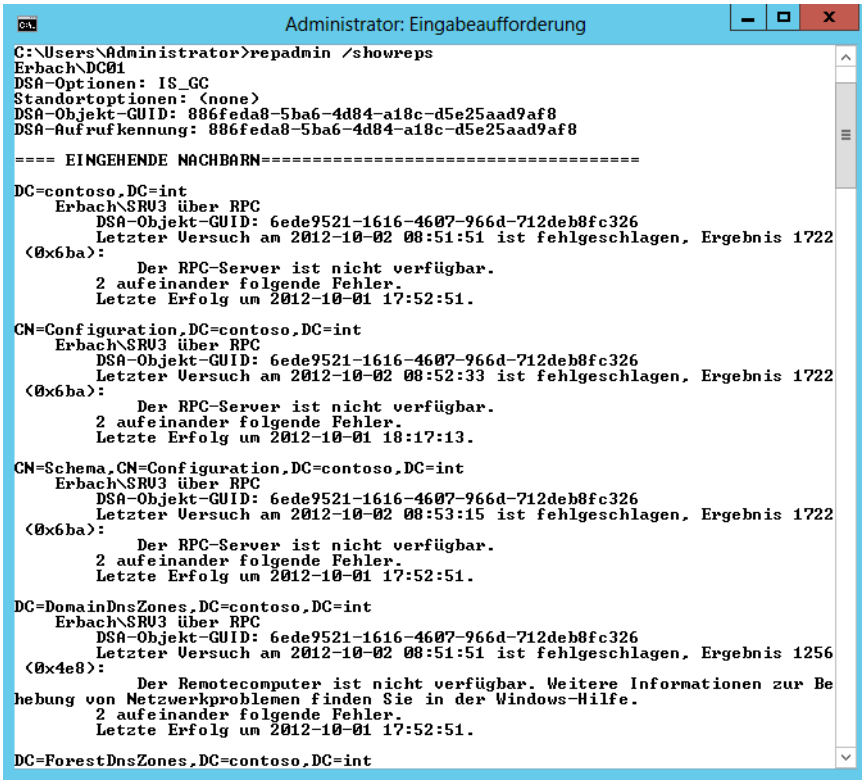
Repadmin zum Anzeigen der Active Directory-Replikation

Das wichtigste Tool, um die Replikation in Active Directory zu überprüfen, ist Repadmin. Geben Sie in der Eingabeaufforderung den Befehl *repadmin /showreps* ein. Angezeigt werden alle durchgeführten Replikationsvorgänge von Active Directory sowie etwaige Fehler, die auf die Ursache für eine nicht funktionierende Replikation hinweisen. Sie können sich die Anzeige auch in eine Datei mit *repadmin /showreps >c:\repl.txt* umleiten lassen.

TIPP Mit *repadmin /showreps * /csv > reps.csv* leiten Sie die Replikationsinformationen in eine *.csv*-Datei um.

Untersuchen Sie bei Problemen genau, wann welche Replikation funktioniert und welche Verbindung nicht funktioniert. In der Anzeige erhalten Sie auch die Gründe, warum die Replikation nicht durchgeführt werden kann.

Abbildg. 14.14 Diagnose der Active Directory-Replikation



Funktioniert die interne Replikation im gleichen Standort zu Domänencontrollern ohne Probleme, stellen Sie sicher, dass die Replikation nur einige Minuten zurückliegt. Dann können Sie interne Replikationsprobleme der Domänencontroller ausschließen.

Sehen Sie, dass ein Domänencontroller nicht replizieren kann, erhalten Sie eine Meldung. Die Fehlermeldung können Sie zum Beispiel in einer Suchmaschine verwenden. Wenn sich der lokale Domänencontroller replizieren kann, liegt vermutlich ein Problem auf dem entfernten Domänencontroller oder mit der Verbindung vor. Untersuchen Sie auf anderen Domänencontrollern, ob diese replizieren können. Wenn nicht, liegt sicherlich ein Problem mit dem entfernten Domänencontroller vor.

Fehlermeldungen können Sie direkt in einer Suchmaschine eingeben und erhalten oft schon hilfreiche Lösungsvorschläge. Sie sehen, dass Sie bereits einige Maßnahmen aus dem Tool ableiten können, die Sie bei der Fehlersuche unterstützen. Wichtig auch in diesem Bereich der Fehlersuche ist, dass Sie die Beschreibung des Fehlers so genau wie möglich wählen, damit Sie bei der Suche im Internet nur die wirklich passenden Antworten präsentiert bekommen.

Replikation in der PowerShell testen

Den Status der Replikation erfahren Sie auch in der PowerShell. Dazu verwenden Sie das Cmdlet *Get-ADReplicationUpToDatenessVectorTable <Name des Servers>*. Eine Liste aller Server erhalten Sie mit:

```
Get-ADReplicationUpToDatenessVectorTable * | Sort Partner,Server | ft
Partner,Server,UsnFilter
```

Um die einzelnen Standorte und die Domänencontroller der Standorte anzuzeigen, verwenden Sie die beiden Cmdlets:

```
Get-ADReplicationSite -Filter * | ft Name
Get-ADDomainController -Filter * | ft Hostname,Site
```

Sie können die Replikationsverbindungen auch in der PowerShell anzeigen. Dazu verwenden Sie den Befehl *Get-ADReplicationConnection*.

Sie können sich in der PowerShell auch ausführliche Informationen zu den einzelnen Standorten anzeigen lassen. Dazu verwenden Sie den Befehl *Get-ADReplicationSite –Filter **. Weitere interessante Cmdlets in diesem Bereich sind:

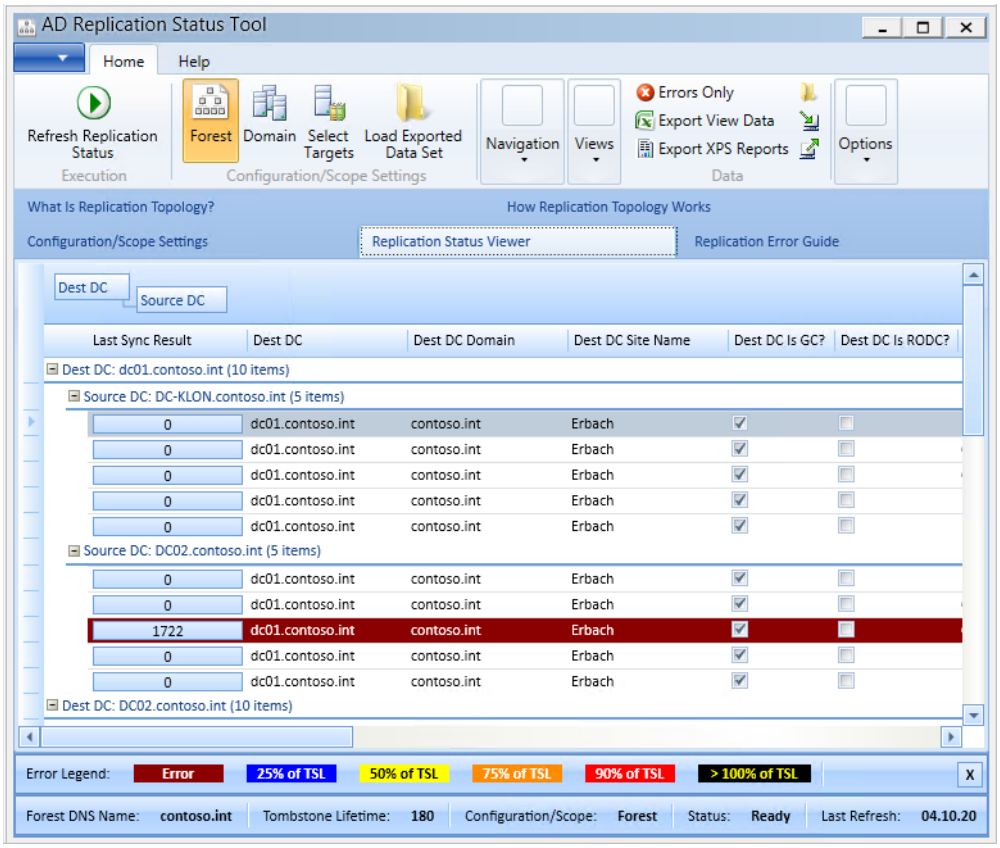
- *Get-ADReplicationPartnerMetadata*
- *Get-ADReplicationFailure*
- *Get-ADReplicationQueueOperation*

Active Directory Replication Status Tool

Microsoft stellt für die Diagnose der Replikation von Domänencontrollern das Tool AD Replication Status kostenlos im Download Center zur Verfügung (*http://www.microsoft.com/en-us/download/details.aspx?id=30005* [Ms179-K14-04]).

Mit dem Tool sehen Sie in einem übersichtlichen Fenster, ob die Replikation zwischen den Domänencontrollern funktioniert. Nach der Installation starten Sie das Tool über seine Verknüpfung. In der Oberfläche klicken Sie zunächst auf *Refresh Replication Status*. Anschließend scannt das Tool die Domänencontroller und zeigt eventuelle Replikationsprobleme an.

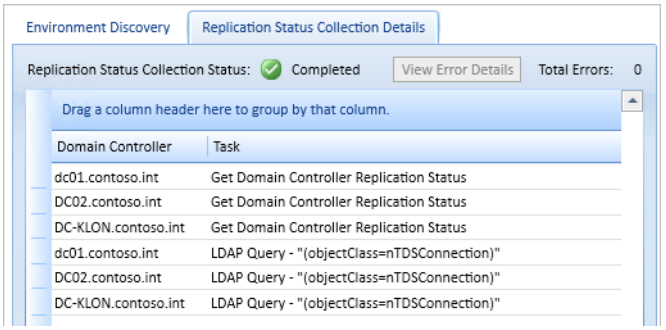
Abbildg. 14.15 Replikationsdiagnose mit dem AD Replication Status Tool



Über die Schaltfläche *Domain* wählen Sie zunächst die Domänen aus, in der Sie die Replikation testen wollen. Zunächst zeigt das Tool alle gefundenen Domänencontroller an und ob diese erreichbar sind. Sie sehen im Fenster auch, wie viele Fehler auf den Domänencontrollern im Bereich der Replikation aufgetreten sind.

Sie können mit dem Tool die komplette Gesamtstruktur mit allen Domänencontrollern oder auch nur einzelne Domänen untersuchen. Auch die Überprüfung einzelner Domänencontroller können Sie mit dem Tool durchführen. Fehler kennzeichnet das Tool in Rot. Klicken Sie doppelt auf einen Fehler, verbindet sich AD Replication Status Tool mit dem Internet und zeigt Hinweise und Lösungsvorschläge an.

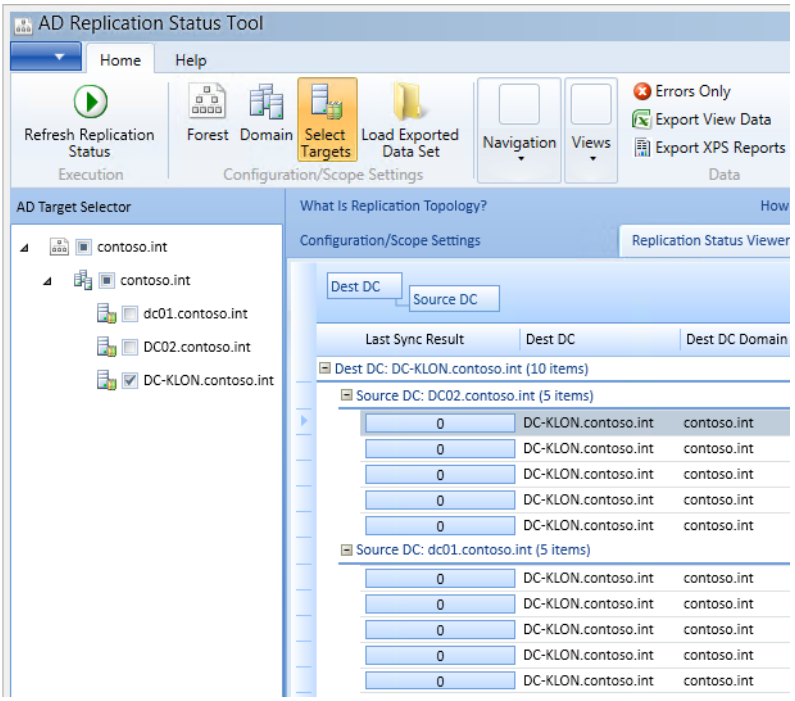
Abbildg. 14.16 Anzeigen des Status der Domänencontroller in einer Domäne



Wollen Sie nur einige oder einen Domänencontroller testen, klicken Sie auf *Select Targets* und wählen die Domänencontroller aus, die Sie testen wollen.

Im Menüband können Sie nur Fehler einblenden lassen und die Daten zu Excel-Tabellen oder XPS-Dateien exportieren. Mit *Refresh Replication Status* lässt sich die Ansicht aktualisieren.

Abbildg. 14.17 Auswählen der Domänencontroller zur Überprüfung der Replikation



Kerberostest mit Dcdiag ausführen

Die Version von Dcdiag, die mit Windows Server 2012 R2 ausgeliefert wird, enthält einen neuen Test, mit dem sich Replikationsprobleme anzeigen lassen, die von Kerberosproblemen verursacht werden.

Öffnen Sie eine neue Eingabeaufforderung und geben Sie den folgenden Befehl ein:

```
dcdiag /test:CheckSecurityError /s:<Name des Domänencontrollers, der Probleme hat>
```

Anschließend überprüft Dcdiag für diesen Domänencontroller, ob irgendeine Active Directory-Replikationsverbindung Probleme mit der Übertragung von Kerberos hat. Sie erhalten eine detaillierte Ausgabe aller Probleme, die der Quelldomänencontroller bei der Replikation im Zusammenhang mit Kerberos hat.

Die Ausgabe dieser Probleme ist eine wertvolle Hilfe bei der Suche nach Problemen in Active Directory. Oft spielen auch Sicherheitsprobleme bei der Replikation von Domänencontrollern eine Rolle. In diesem Fall erscheinen häufig Fehlermeldungen der Art »Zugriff verweigert«.

Überprüfung der notwendigen SRV-Records im DNS unter *_msdcs*

Jeder Domänencontroller in Active Directory hat neben seinem Host-A-Namen, zum Beispiel *dc01.contoso.int*, noch einen zugehörigen *CNAME*, der das sogenannte 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 Knoten *_msdcs* zu finden. Der CNAME ist die GUID dieses DSA-Objekts. Domänencontroller versuchen Ihren Replikationspartner nicht mit dem herkömmlichen Host-A-Eintrag aufzulösen, sondern mit dem hinterlegten CNAME. Sollte die Replikation nicht funktionieren, weil unterhalb der Active Directory-DNS-Domäne *_msdcs*-Einträge fehlen, können Sie in der Eingabeaufforderung durch Eingabe des Befehls *dcdiag /fix* die Einträge wiederherstellen. Überprüfen Sie nach der Ausführung dieses Befehls, ob der CNAME des Servers registriert ist.

Zusammenfassung

In diesem Kapitel haben wir Ihnen erläutert, wie Sie Active Directory auf verschiedene physische Standorte verteilen, die Replikation der Domänencontroller einrichten und eventuell dabei auftretende Fehler beheben.

Im nächsten Kapitel zeigen wir ausführlich, wie Sie Fehler in Active Directory finden und beheben.

Kapitel 15

Active Directory – Fehlerbehebung und Diagnose

In diesem Kapitel:

Treten in 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. In diesem Kapitel zeigen wir Ihnen, wie Sie effizient und schnell Fehler finden und diese beheben.

Ab Windows Server 2012 hat Microsoft einige Funktionen in Active Directory geändert und die Verwaltung und Überwachung verbessert. Die Installation von Active Directory läuft in Windows Server 2012/2012 R2 komplett über den Server-Manager oder PowerShell. Tools wie Dcpromo gibt es nicht mehr. Die Assistenten hat Microsoft vereinfacht und neue Cmdlets zur Überwachung integriert.

HINWEIS Im Kapitel 14 sind wir ebenfalls auf Diagnosetools und Fehlerbehebung im Bereich Replikation eingegangen.

Bordmittel zur Diagnose verwenden

In den folgenden Abschnitten zeigen wir Ihnen die wichtigsten Bordmittel, mit denen Sie Domänencontroller überprüfen und Fehler einschränken. Fehler, die Sie durch die Tools aufdecken, können Sie in einer Suchmaschine eingeben und erhalten auf diesem Weg meist schon einen Ansatz zur Fehlerbehebung.

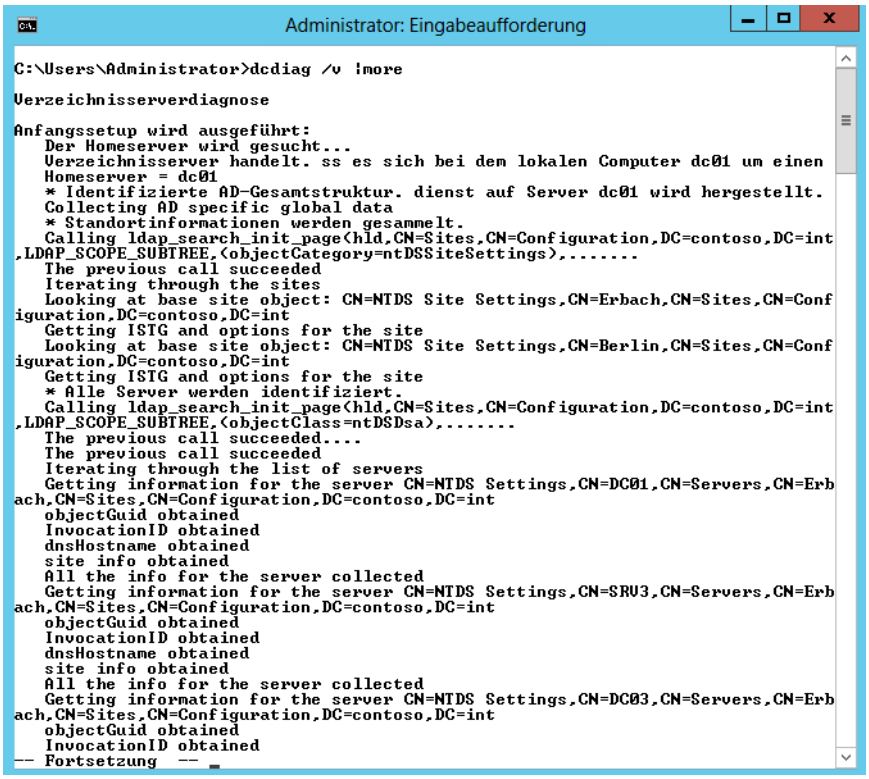
Haben Sie Active Directory installiert, stehen auch in Windows Server 2012 R2 die bekannten Tools Dcdiag, Repadmin & Co. zur Analyse zur Verfügung. Für die Namensauflösung können Sie weiterhin Nslookup verwenden oder die neuen Cmdlets zur Verwaltung von DNS, zum Beispiel *Resolve-DNSName*. Über das Kontextmenü eines Domänencontrollers in der Servergruppe *AD DS* können Sie Verwaltungstools und Tools zur Analyse der Domäne starten. Es öffnet sich eine Eingabeaufforderung, in der Sie mit den bereits aus Windows Server 2008 R2/2012 bekannten Mitteln eine Analyse durchführen können. Die Analyse startet aber nicht, indem Sie das Tool im Kontextmenü des Servers im neuen Server-Manager starten. Hier öffnet sich lediglich eine neue Eingabeaufforderung, welche die Hilfe des Tools anzeigt. Die Diagnose selbst starten Sie nach der Installation von Active Directory, indem Sie Dcdiag oder Repadmin verwenden und dabei auf die verschiedenen Optionen der Befehle setzen.

Verwenden der Domänencontrollerdiagnose

Das wichtigste Tool für die Diagnose von Domänencontrollern ist Dcdiag. Sie können das Tool in der Eingabeaufforderung mit Administratorrechten aufrufen, indem Sie *dcdiag* eingeben. Eine ausführliche Diagnose erhalten Sie durch *dcdiag /v*.

Möchten 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 weitergeben können. Die Eingabeaufforderung könnte dann zum Beispiel *dcdiag/v >c:\dcdiag.txt* lauten. Für die erste Überprüfung reicht die normale Diagnose mit Dcdiag jedoch vollkommen aus. Fehler sollten Sie in einer Suchmaschine recherchieren und beheben. Im idealen Fall sollte Dcdiag keine Fehler zeigen.

Abbildg. 15.1 Domänencontrollerdiagnose mit Dcdiag



Der Systemdienst *Dateireplikation* verbindet die Domänencontroller der verschiedenen Standorte und erstellt automatisch eine Replikationstopologie auf Basis der definierten Zeitpläne und Standortverknüpfungen. Die Konsistenzprüfung (Knowledge Consistency Checker, KCC) ist ein automatischer Mechanismus in Active Directory. Dieser läuft auf jedem Domänencontroller und erstellt sowie 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.

Der KCC 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 Standorts spielt der Netzwerkverkehr keine große Rolle. Die Replikationsdaten innerhalb eines Standorts werden daher, im Gegensatz zur Replikation zwischen Standorten, nicht komprimiert. Der KCC versucht automatisch innerhalb eines Standorts eine Ringtopologie und maximal drei Hops zwischen zwei Domänencontrollern zu erstellen. Das heißt, dass nicht unbedingt jeder Domänencontroller mit jedem anderen Domänencontroller Daten replizieren muss, aber dass auch maximal drei Schritte zwischen zwei Domänencontrollern liegen dürfen.

Je mehr Standorte in Active Directory definiert sind, desto mehr muss der KCC die Routingtopologie dauerhaft überwachen. Aus diesen Gründen müssen Domänencontroller über mehr Perfor-

mance 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 sogenannte Bridgeheadserver, welche die Informationen ihres Standorts 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 für jeden Standort automatisch die am besten geeigneten Bridgeheadserver 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 Standorts. Außerdem besteht darüber hinaus noch die Gefahr, dass bei Ausfall aller bevorzugten Bridgeheadserver keine Replikation zu und von diesem Standort durchgeführt werden kann.

TIPP Mit *dcdiag /a* überprüfen Sie alle Domänencontroller am gleichen Active Directory-Standort, über *dcdiag /e* werden alle Server in der Gesamtstruktur getestet.

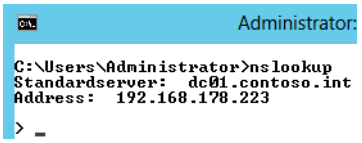
Um sich nur die Fehler und keine Informationen anzeigen zu lassen, verwenden Sie *dcdiag /q*. Die Option *dcdiag /s:<Domänencontroller>* ermöglicht den Test eines Servers über das Netzwerk.

Es wird während des Tests auch geprüft, ob das Computerkonto in 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 behebt, ist *dcdiag /fix*.

Testen der Namensauflösung mit Nslookup

Die Namensauflösung ist einer der wichtigsten Bereich für die Diagnose von Active Directory und Windows-Netzwerken. Funktioniert ein Serverdienst nicht, liegt das Problem in den meisten Fällen entweder an Berechtigungen oder der Namensauflösung. Ein wichtiger Test in Active Directory besteht darin, dass Sie in der Eingabeaufforderung *nslookup* eintippen. An dieser Stelle sollte kein Fehler auftreten. Lesen Sie sich zu diesem Thema auch das Kapitel 5, 10 und 11 durch.

Abbildg. 15.2 Erste Diagnose mit Nslookup



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, 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 Eingabeaufforderung eine erneute automatische Registrierung beim DNS-Server. Das ist eine häufige Fehlerquelle. Lesen sie dazu die Anmerkungen in den Kapiteln 5, 10 und 11. Danach sollten Sie durch die Eingabe

des vollständigen Computernamens aller restlichen Domänencontroller feststellen, dass alle notwendigen Domänencontroller per DNS erreicht werden können.

Treten in Active Directory Fehler auf, sollten Sie immer zunächst überprüfen, ob sich die beteiligten Server im DNS auflösen können. Verwenden Sie dazu das Befehlszeilentool Nslookup. Neben Nslookup besprechen wir im nächsten Abschnitt noch weitere Tools, die für die Fehlersuche und Verwaltung von DNS unter Windows Server 2012 R2 eine besondere Rolle spielen. Nslookup gehört zu den Bordmitteln von Windows Server 2012 R2 und ist auch in Windows 7/8/8.1 integriert. Wenn ein Servername mit Nslookup nicht aufgelöst werden kann, sollten Sie überprüfen, wo das Problem liegt:

1. Ist in den IP-Einstellungen des PCs, auf dem Sie das Tool Nslookup aufrufen, der richtige DNS-Server als bevorzugt eingetragen?
2. Verwaltet der bevorzugte DNS-Server die Zone, in der Sie eine Namensauflösung durchführen wollen (siehe Kapitel 11)?
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 (siehe Kapitel 13)?
4. Wenn eine Weiterleitung eingetragen ist, kann dann der Server, zu dem weitergeleitet wird, die Zone auflösen (siehe die Kapitel 5, 10, 11 und 12)?
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-Lookupzone 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 (siehe Kapitel 5).

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 in der Eingabeaufforderung *nslookup <host> –<server>* ein (also zum Beispiel *nslookup dc02.microsoft.com dc01.contoso.com*).

Bei diesem Beispiel versucht Nslookup den Host *dc02.microsoft.com* mithilfe 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 Eingabeaufforderung einen DNS-Server mit seinem FQDN eingeben, setzt dies 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 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*

Sie können die beiden eben erwähnten Optionen auch kombinieren:

- 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
- Nslookup wird in der Eingabeaufforderung 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 dies 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 Servername 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 soll der Rechnername *dc02.microsoft.com* vom Server *10.0.0.13* aufgelöst werden. Der Server *10.0.0.13* kann jedoch den Servername *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. Der Standardserver kann den Servername problemlos auflösen, was zeigt, dass diese Konfiguration in Ordnung ist.

Standard-OUs per Active Directory-Benutzer und -Computer überprüfen

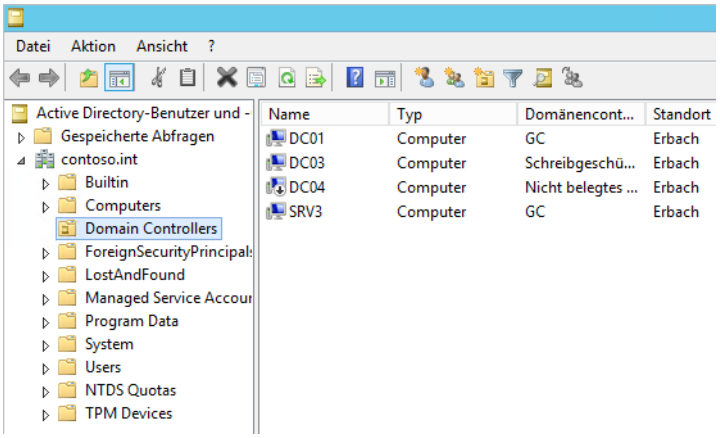
Nach einer Neuinstallation sollten Sie überprüfen, ob sich das Snap-In *Active Directory-Benutzer und -Computer* über *Tools* im Server-Manager fehlerfrei öffnen lässt und die fünf wichtigsten Organisationseinheiten (Organizational Units, OUs) angezeigt werden. Diese OUs sind in jeder Domäne identisch und müssen vorhanden sein:

- **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 in Active Directory verwaltet.
- **Users** Im Container *Users* stehen die Benutzer und Gruppen, die von Windows Server 2012 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
- **Managed Service Accounts** Dieser Container dient der Unterstützung verwalteter Benutzerkonten für Dienste, eine neue Funktion in Windows Server 2012

Sie müssen nicht den Inhalt der Container überprüfen. Es genügt, wenn Sie testen, ob diese angelegt wurden. Achten Sie darauf, im Snap-In über das Menü *Ansicht* die *Erweiterten Features* zu aktivieren.

Abbildg. 15.3 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 zum Exchange-Server werden soll, in der Eingabeaufforderung testen, ob dieser Server seinen Standort auflösen kann und korrekt 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 (siehe Kapitel 5, 10, 11 und 12). Auch die IP-Subnetze und deren korrekte Zuordnung zu den richtigen Standorten sollte hier überprüft werden (siehe Kapitel 14). Den Standardnamen des ersten Standorts passen Sie am besten im Server-Manager über *Rollen/Active Directory-Domänendienste/Active Directory-Standorte und -Dienste an*. Klicken Sie dazu den Standort mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Umbenennen* (siehe Kapitel 14).

Die Replikationsverbindungen richtet Windows Server 2012 automatisch. Sie sehen diese im Snap-In *Active Directory-Standorte und -Dienste* über *Sites\<Standort>\<Servers>\<Servername>\NTDS-Settings*. Sie können hier auch manuelle Verbindungen einrichten, indem Sie über das Kontextmenü *Neue Verbindung für die Active Directory-Domänendienste* auswählen. Überprüfen Sie, ob Replikationsverbindungen vorhanden sind und diese auch funktionieren.

Überprüfen der Domänencontrollerliste

Geben Sie in der Eingabeaufforderung 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. 15.4 Anzeigen der vollständigen Domänencontrollerliste und des Standorts in der Eingabeaufforderung

```
C:\Users\Administrator>nltest /dsgetsite
Erbach
Der Befehl wurde ausgeführt.

C:\Users\Administrator>nltest /dclist:contoso
Liste der Domänencontroller (DCs) in Domäne 'contoso' von '\\DC01' abrufen.
    dc01.contoso.int [PDC]  [DS] Standort: Erbach
    SRV3.contoso.int        [DS] Standort: Erbach
    DC03.contoso.int [RODC] [DS] Standort: Erbach
    DC04.contoso.int [RODC] [DS] Standort: Erbach
Der Befehl wurde ausgeführt.
```

TIPP Starten Sie mit *net stop netlogon* und dann *net start netlogon* den Anmeldedienst auf dem Domänencontroller neu, versucht der Dienst die Daten der Datei *netlogon.dns* aus dem Ordner *\Windows\System32\config\netlogon.dns* erneut in DNS zu registrieren. Gibt es hierbei Probleme, finden sich im Ereignisprotokoll unter *System* Einträge des Diensts, die bei der Problemlösung weiterhelfen.

Auch der Befehl *nltest /dsregdns* hilft oft bei Problemen in der DNS-Registrierung. Funktioniert die erneute Registrierung durch Neustart des Anmeldedienstes nicht, löschen Sie die DNS-Zone *_msdcs* und die erstellte Delegierung. Beim nächsten Start des Anmeldedienstes liest dieser die Daten von *netlogon.dns* ein, erstellt die Zone *_msdcs* neu und schreibt die Einträge wieder in die Zone. Mit Dcdiag lassen sich danach die Probleme erneut diagnostizieren. Einen ausführlichen Test führen Administratoren mit *dcdiag /v* durch.

Überprüfen der Active Directory-Dateien

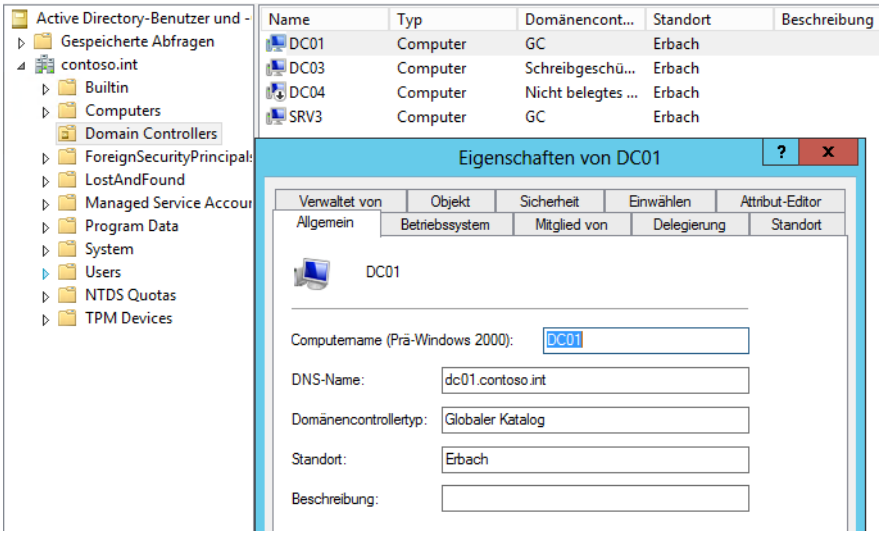
Die Active Directory-Daten werden in einer Datenbank gespeichert. Diese Datenbank ist eine Datei im Dateisystem auf den Domänencontrollern. Die Active Directory-Datenbank wird in der Datei *ntds.dit* in dem Ordner gespeichert, den Sie bei der Heraufstufung zum Domänencontroller festgelegt haben. Standardmäßig wird die Active Directory-Datenbank im Ordner *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.

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 und Kennwort zurücksetzen

Die Domänencontroller sollten im Snap-In *Active Directory-Benutzer und -Computer* in der OU *Domain Controllers* angezeigt werden. 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. 15.5 Anzeigen der Eigenschaften des Computerkontos eines Domänencontrollers



Außerdem können Sie mit dem Befehl *net accounts* in der Eingabeaufforderung 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.

Bei Kerberos werden die Identität des Benutzers und die Identität des authentifizierenden Servers festgestellt. Kerberos arbeitet mit einem sogenannten 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 2003/2008/2008 R2/2012/2012 R2-Domänencontrollern ausgeführt und ist für die Ausstellung der Authentifizierungstickets zuständig. Der zuständige Kerberos-Client läuft auf allen Windows-Arbeitsstationen. Wenn sich ein Benutzer an einer Arbeitsstation in 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 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 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. Sollten Probleme mit dem Schlüsselverteilungscenter oder Kerberos im Allgemeinen auftreten, besteht unter Umständen noch ein Problem bei der Kerberosauthentifizierung. In diesem Fall wird allerdings normalerweise eine entsprechende Fehlermeldung bei Dcdiag oder Netdiag angezeigt, die auf Probleme mit LDAP oder Kerberos hinweisen. Kerberos ist für die Anmeldung in Active Directory von existenzieller Wichtigkeit. Aber auch wenn diese Tools keine Fehler gezeigt haben, kann das Zurücksetzen des Maschinenkennworts eine letzte Hoffnung sein, einen ausgefallenen Server oder Domänencontroller wieder zur Zusammenarbeit mit seiner Domäne zu bewegen. Um das Kennwort zurückzusetzen, müssen Sie folgendermaßen vorgehen:

1. Beenden Sie auf dem problematischen Domänencontroller den Dienst *Kerberos-Schlüsselverteilungscenter*.
2. Setzen Sie den Dienst auf *Manuell*.
3. Öffnen Sie eine neue Eingabeaufforderung mit Administratorrechten und geben Sie den folgenden Befehl ein:

```
netdom resetpwd /server:<Ein Domänencontroller der Domäne, der noch funktioniert> /
userd:<Administratorbenutzert der Domäne> /passwordd:<Kennwort des Administrators>.
```

4. Wenn Sie den Befehl ausführen, muss auf jeden Fall eine positive Rückantwort kommen, welche bestätigt, dass das Kennwort der Maschine zurückgesetzt wurde.
5. Starten Sie im Anschluss den Server neu.
6. Starten Sie den Dienst *Kerberos-Schlüsselverteilungscenter* auf dem Server wieder und setzen Sie den Dienst auf *Automatisch*.
7. Jetzt sollte der Server wieder uneingeschränkt funktionieren. Überprüfen Sie die korrekte Verbindung mit der Domäne durch die Tools *Dcdiag*.

Abbildg. 15.6 Zurücksetzen des Computerkontos eines Servers

```
C:\Users\administrator.CONTOSO>netdom resetpwd /server:dc01.contoso.int /userd:c
ontoso\administrator /passwordd:t
Das Computerkonto-Kennwort für den lokalen Computer wurde zurückgesetzt.

Der Befehl wurde ausgeführt.
```

Überprüfen der administrativen Freigaben

Auf Domänencontrollern gibt es verschiedene Freigaben, die für den Betrieb von Active Directory notwendig sind. Die beiden Freigaben *netlogon* und *SYSVOL* sollten fehlerfrei dargestellt werden. Überprüfen Sie die Freigaben mithilfe des Aufrufs *net share* in der Eingabeaufforderung. Standardmäßig werden die beiden folgenden Ordner freigegeben:

- *C:\Windows\SYSVOL\sysvol\<DOMÄNE>\SCRIPTS* als Freigabe *netlogon*
- *C:\Windows\SYSVOL\sysvol* als Freigabe *SYSVOL*

Beide Freigaben werden durch *net share* in der Eingabeaufforderung angezeigt.

Abbildg. 15.7 Anzeigen der administrativen Freigaben in der Eingabeaufforderung

```
C:\Users\Administrator>net share

Name         Ressource                       Beschreibung
------------------------------------------------------------------------------
C$           C:\                             Standardfreigabe
IPC$                                         Remote-IPC
ADMIN$       C:\Windows                      Remoteverwaltung
NETLOGON     C:\Windows\SYSVOL\sysvol\contoso.int\SCRIPTS
                                             Ressource für Anmeldeserver
SYSVOL       C:\Windows\SYSVOL\sysvol        Ressource für Anmeldeserver
Der Befehl wurde erfolgreich ausgeführt.
```

Alternativ überprüfen Sie die administrativen Freigaben im Server-Manager über *Datei-/Speicherdienste/Freigaben*. Auch hier werden die Freigaben angezeigt.

Überprüfen der Gruppenrichtlinien

Automatisch werden nach der Installation durch Active Directory die beiden folgenden Gruppenrichtlinien angelegt:

- *Default Domain Controller Policy*
- *Default Domain Policy*

Die Einstellungen der beiden Gruppenrichtlinien werden im Dateisystem auf den Domänencontrollern gespeichert. Für beide Richtlinien gibt es im Ordner *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:

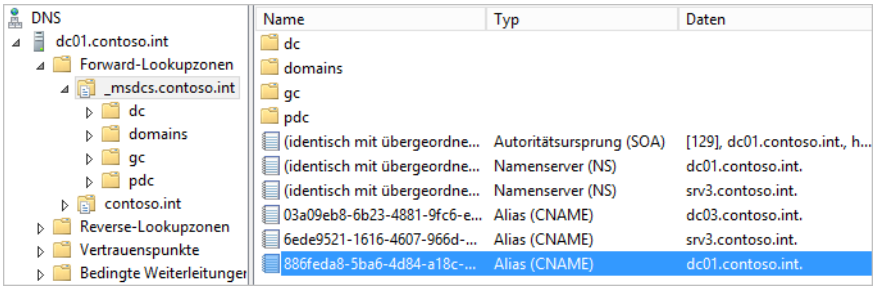
- *{31B2F340-016D-11D2-945F-00C04FB984F9}* = Default Domain Policy
- *{6AC1786C-016F-11D2-945F-00C04fB984F9}* = Default Domain Controller Policy

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 erkennen, ob überhaupt Einträge erstellt wurden. Alle notwendigen Dienste von Active Directory werden als SRV-Record im DNS gespeichert.

Die häufigsten Fehler aller Art innerhalb von Active Directory oder anderen Netzwerken, bei denen die Namensauflösung eine wichtige Rolle spielt, sind Fehler im DNS. Jeder Domänencontroller in Active Directory hat neben seinem Host A-Namen, zum Beispiel *dc01.contoso.int*, noch einen zugehörigen CNAME, der das sogenannte 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 Knoten *_msdcs* zu finden.

Abbildg. 15.8 Anzeigen der DNS-DSA-Objekte von Domänencontrollern



Der CNAME ist die GUID dieses DSA-Objekts. Domänencontroller versuchen ihren Replikationspartner nicht mit dem herkömmlichen Host A-Eintrag aufzulösen, sondern mit dem hinterlegten CNAME. Ein Domänencontroller versucht 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 entweder über Broadcast oder einen WINS-Server aufzulösen.

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 nicht funktionieren, steht Ihnen noch das Tool Dnslint zur Verfügung, mit denen die SRV-Records in Active Directory überprüft werden können. Sie können das Tool bei Microsoft auf der Seite *http://download.microsoft.com/download/2/7/2/27252452-e530-4455-846a-dd68fc020e16/dnslint.v204.exe* [Ms179-K15-01] herunterladen. Entpacken Sie das Tool nach dem Herunterladen in einen Ordner. Sie müssen es nicht installieren. 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

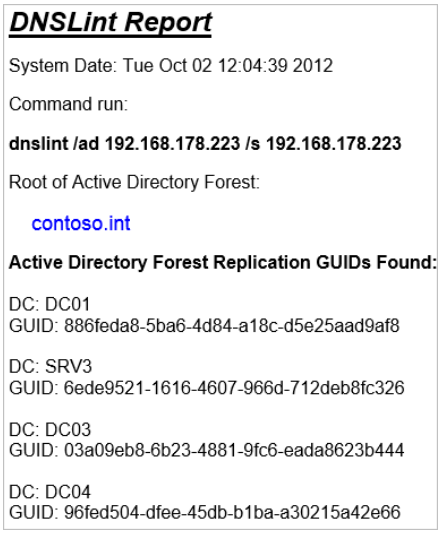
Die Syntax lautet:

```
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 /ad* können Sie überprüfen, ob Ihre Domänencontroller die DNS-Einträge in Active Directory zur Replikation abrufen können. Geben Sie zur Überprüfung den Befehl *dnslint /ad <IP-Adresse des ersten DC> /s <IP-Adresse des zweiten DC>* ein. Das Tool benötigt einige Sekunden und überprüft, ob in 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. Testen Sie 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 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.

Abbildg. 15.9 Überprüfen der DNS-Einträge für Domänencontroller



Nachdem der Befehl abgeschlossen ist, wird Ihnen ein 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 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 genü-

gend 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.

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 und mit */ql* fordern Sie DNS-Abfragetests von einer Liste ab. Die Befehlszeilenoption */ql* versendet die DNS-Abfragen, die in einer Texteingabedatei angegeben sind. 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.

Wenn Sie */ad* verwenden, müssen Sie die Option */s* angeben, um einen DNS-Server zu bestimmen, 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 localhost* 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 HTML-Bericht. Die Textdatei wird in denselben Ordner gespeichert wie die HTML-Berichtsdatei.

Verwenden Sie */test_tcp*, um den TCP-Port 53 zu testen. 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* erhalten Sie eine Ausgabe auf dem Bildschirm. Bei dieser Option zeigt das Tool auf dem Bildschirm an, welche Schritte es ausführt, um Daten zu sammeln.

Testen der Betriebsmaster

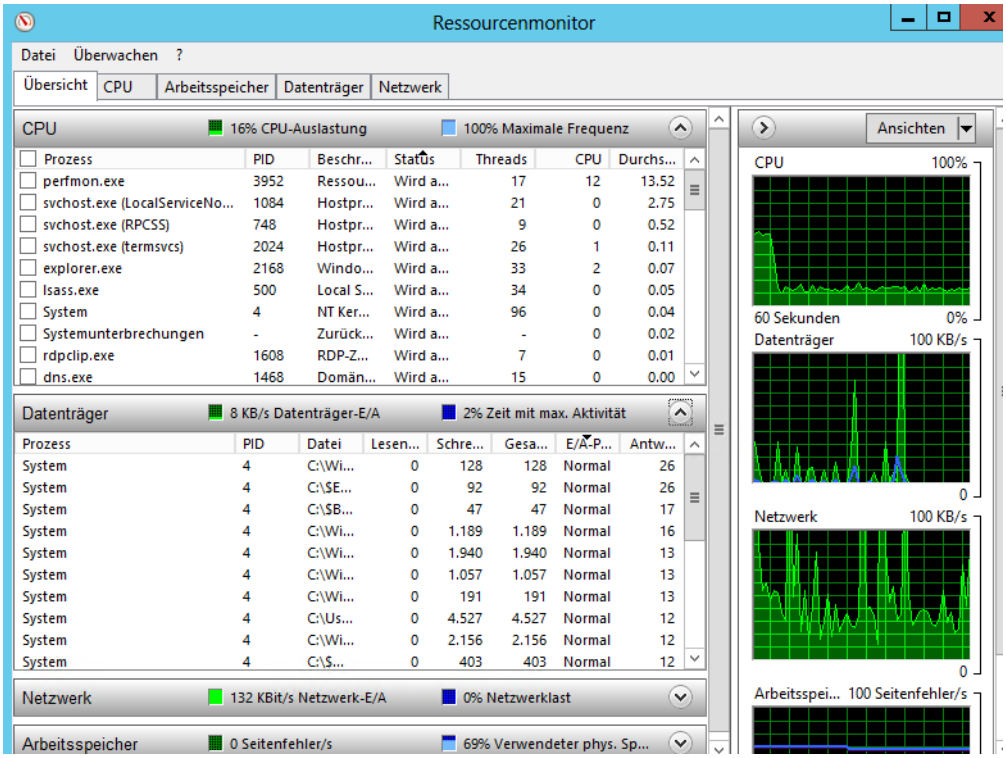
Als Nächstes sollten Sie auf einem neuen Domänencontroller testen, ob dieser alle FSMO-Rolleninhaber kennt (siehe Kapitel 10). Diese lassen Sie sich gebündelt mit *netdom query fsmo* anzeigen oder einzeln über die Befehle *dsquery server –hasfsmo pdc* (PDC-Master), *dsquery server –hasfsmo rid* (RID-Master), *dsquery server –hasfsmo infr* (Infrastrukturmaster), *dsquery server –hasfsmo schema* (Schemamaster) und *dsquery server –hasfsmo name* (Domänennamenmaster).

Leistungsüberwachung zur Diagnose nutzen

Windows Server 2012 stellt mit der Leistungsüberwachung ein mächtiges Tool zur Verfügung, um Performanceprobleme auf einem Server aufzudecken. Das Tool konnten Sie bereits in Windows Server 2008 R2/2012 nutzen, um eine Diagnose in Active Directory durchzuführen. Die Bedienung hat sich im Vergleich zu den Vorgängerversionen nur wenig geändert. Sie finden das Tool im Server-Manager über *Tools/Leistungsüberwachung*.

Schneller starten Sie das Tool durch Eingabe von *perfmon.msc* im Startbildschirm. Mit *perfmon /res* starten Sie den Ressourcenmonitor der eine Echtzeitanzeige der aktuell verbrauchten Ressourcen bietet, ähnlich zum Task-Manager. Vor allem wenn in einem Active Directory noch Zusatzdienste installiert sind, zum Beispiel SharePoint, Exchange oder SQL, tauchen schnell Leistungsprobleme auf, die sich oft aber durch die Leistungsüberwachung aufdecken und beheben lassen.

Abbildg. 15.10 Leistungsüberwachung von Active Directory



Liegen Leistungsprobleme in Exchange oder anderen Serverdiensten die von Active Directory abhängen vor, zum Beispiel bezüglich des Postfachzugriffs oder dem Versenden von Nachrichten, liegt häufig auch ein Problem in Active Directory oder DNS vor. Das heißt, parallel zur Leistungsüberwachung sollten Sie noch eine Diagnose der Namensauflösung sowie eine Diagnose der Domänencontroller durchführen, zum Beispiel über Dcdiag. Exchange, aber auch andere Dienste, welche Active Directory benötigen, greifen über die Systemdatei *wldap32.dll* auf Active Directory zu. Dabei laufen (vereinfacht) folgende Vorgänge ab:

1. Die Datei *wldap32.dll* auf dem Exchange-Server erhält durch einen Exchange-Prozess eine Anfrage, um auf den globalen Katalog zuzugreifen.
2. Per DNS versucht der Server den globalen Katalog-Server aufzulösen, um auf diesen zugreifen zu können. Dauert dieses Auflösen zu lange, verzögert sich bereits an dieser Stelle der Active Directory-Zugriff.
3. Nach der Namensauflösung baut die *wldap32.dll* eine Verbindung zum globalen Katalog auf und überträgt die Anfrage.

4. Anschließend wird eine TCP-Verbindung aufgebaut und eine LDAP-Abfrage gestartet. Damit die Verbindung funktioniert, benötigt die TCP-Verbindung drei Bestätigungen durch den Domänencontroller. Bei einer Latenz von 10 Millisekunden im Netzwerk dauert der Zugriff in diesem Fall also 30 Millisekunden, bevor der Exchange-Server die LDAP-Abfrage übertragen kann.
5. Die LDAP-Abfrage wird zur Datei *lsass* auf dem Domänencontroller übertragen, die auf den LDAP-Port des Servers hört.
6. Der Domänencontroller nimmt die Abfrage an den globalen Katalog entgegen und führt die Suche in seinem globalen Katalog durch.
7. Der globale Katalog sendet die Daten über die Netzwerkkarte zur Datei *wldap32.dll* auf dem Exchange-Server. Handelt es sich um eine hohe Anzahl an Daten, zum Beispiel beim Auflösen der Mitglieder einer Verteilergruppe, müssen erst alle Daten übertragen werden, bevor Exchange mit der Verarbeitung weitermachen kann.

Ein sehr großer Teil der Leistung hängt also bei Servern von der Netzwerkgeschwindigkeit zwischen Exchange-Server und dem globalen Katalog oder Domänencontroller ab. Aus diesem Grund sollten Sie bei Leistungsproblemen der Exchange-Infrastruktur auch immer die Geschwindigkeit des Netzwerks messen. Auch die Geschwindigkeit zum DNS-Server und eine schnelle, stabile und korrekte Namensauflösung ist sehr wichtig. Die Geschwindigkeit zum DNS-Server darf 50ms nicht überschreiten, wenn Sie die Leistung optimieren wollen. Dauert die Anfrage länger, haben Sie schon den ersten Flaschenhals in der Exchange-Leistung. Dazu reicht das Pingen des Servers aus, Sie benötigen noch nicht mal die Leistungsüberwachung.

Wichtig für die Verbindung von Exchange zu Active Directory ist die Indikatorgruppe *MSExchange ADAccess-Prozesse* in der Leistungsüberwachung. Diese fügt der Exchange-Installationsassistent auf einem Server hinzu. Erweitern Sie diese Gruppe. Interessant sind in dieser Gruppe die beiden Indikatoren *LDAP-Lesedauer* und *LDAP-Suchdauer*.

Klicken Sie dazu auf das Pluszeichen neben der Indikatorgruppe im oberen Bereich und dann auf die beiden Indikatoren. *LDAP-Lesedauer* misst die Zeit, die eine LDAP-Abfrage bis zur Datenübermittlung benötigt. *LDAP-Suchdauer* zeigt die Zeit an, welche der Server für eine Suche per LDAP in Active Directory benötigt. Der Durchschnittswert für diese Indikatoren sollte unter 50 Millisekunden liegen, die Maximaldauer sollte nicht über 100 Millisekunden steigen.

Über die Symbolleiste der Leistungsüberwachung können Sie die Anzeige zwischen *Linie*, *Histogrammleiste* und *Bericht* hin und her wechseln. Auf diesem Weg können Sie zum Beispiel schneller eine Übersicht erhalten, wenn ein bestimmter Server Probleme beim Verbinden mit dem Active Directory hat.

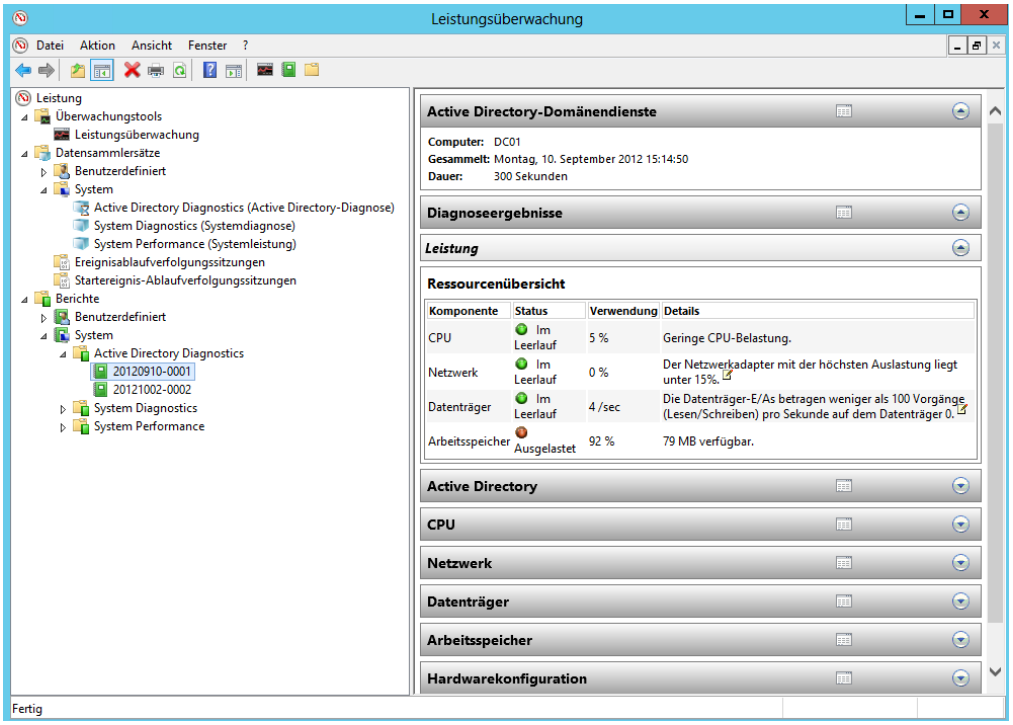
LDAP-Zugriff auf Domänencontrollern überwachen

Damit Active Directory-abhängige Dienste schnell und effizient Daten aus dem Active Directory abrufen können, muss der globale Katalog schnell antworten und darf und nicht überlastet sein. Um diese Auslastung zu überprüfen, können Sie ebenfalls die Leistungsüberwachung verwenden. Klicken Sie anschließend auf *Datensammlersätze/System/Active Directory Diagnostics*.

Klicken Sie anschließend auf das grüne Dreieck in der Symbolleiste, um den Sammlungssatz zu starten. Hat ein Server Leistungsprobleme, starten Sie den Sammlungssatz und lassen die Abfragen messen. Nach einiger Zeit beenden Sie die Messung über das Kontextmenü des Sammlungssatzes oder die Symbolleiste.

Anschließend können Sie über *Berichte/System/Active Directory Diagnostics* die Daten der letzten Messung anzeigen lassen. In verschiedenen Bereichen sehen Sie alle durchgeführten Aufgaben und deren Daten und Zugriffsgeschwindigkeiten. Auf diesem Weg sehen Sie schnell, wo Probleme auf dem Server verursacht werden.

Abbildg. 15.11 Active Directory-Diagnose in Windows Server 2012 R2



Zurücksetzen des Kennworts für den Wiederherstellungsmodus in Active Directory

Um das Kennwort für den Wiederherstellungsmodus auf einem Domänencontroller wiederherzustellen, benötigen Sie das Tool Ntdsutil. Um das Kennwort für den Wiederherstellungsmodus zurückzusetzen, müssen Sie zunächst eine Eingabeaufforderung öffnen und Ntdsutil starten:

1. Rufen Sie in der Eingabeaufforderung *ntdsutil* auf.
2. Geben Sie den Befehl *set dsrm password* ein und bestätigen Sie.
3. Geben Sie in der Zeile *DSRM-Administratorkennwort zurücksetzen* den Befehl *reset password on server <Servername>* ein. Beim lokalen Server können Sie auch den Wert *null* eingeben und bestätigen.
4. Geben Sie das neue Kennwort ein und bestätigen Sie.
5. Geben Sie das neue Kennwort erneut ein.
6. Mit zweimal *quit* verlassen Sie Ntdsutil. Das Kennwort für den Wiederherstellungsmodus ist jetzt zurückgesetzt und dient als Kennwort des lokalen Administrators.

Konfiguration der Ereignisprotokollierung von Active Directory

Im nächsten Schritt besteht auch die Möglichkeit, die Diagnoseprotokollierung von Active Directory zu erhöhen. Standardmäßig schreiben Domänencontroller nur kritische Fehler von Active Directory in die Ereignisanzeige, speziell in das Protokoll *Verzeichnisdienst*. In diesem Protokoll sollten keine Fehler stehen. Tauchen dennoch Fehler auf, sollten diese genau überprüft und die Ursachen abgestellt werden.

Wenn Ihnen diese Protokollierung nicht ausreicht, besteht auch die Möglichkeit, diese zu erhöhen. Active Directory speichert in diesem Fall deutlich mehr Informationen, die zur Überwachung oder Fehlerbehandlung von Active Directory verwendet werden können. In diesem Bereich ist auch der Best Practices Analyzer hilfreichen. Mehr dazu finden Sie in Kapitel 3.

Sie können die Ereignisprotokollierung von Active Directory über die Registry steuern. Wenn Sie die Protokollierung auf einem Domänencontroller erhöhen wollen, müssen Sie mit einem Registrierungs-Editor die Registry öffnen und zu dem Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics* navigieren. An dieser Stelle können Sie für einzelne Bereiche den Wert mit einem REG_DWORD-Eintrag anpassen. Jeder Eintrag in diesem Schlüssel steht für einen eigenen Eventtyp. Sie müssen nicht generell die Überwachung für alle Einträge ändern, sondern können genau die Werte anpassen, die Sie genauer überwachen wollen.

Abbildg. 15.12 Erhöhen der Protokollierung in Active Directory

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
1 Knowledge Consistency Checker	REG_DWORD	0x00000000 (0)
10 Performance Counters	REG_DWORD	0x00000000 (0)
11 Initialization/Termination	REG_DWORD	0x00000000 (0)
12 Service Control	REG_DWORD	0x00000000 (0)
13 Name Resolution	REG_DWORD	0x00000000 (0)
14 Backup	REG_DWORD	0x00000000 (0)
15 Field Engineering	REG_DWORD	0x00000000 (0)
16 LDAP Interface Events	REG_DWORD	0x00000000 (0)
17 Setup	REG_DWORD	0x00000000 (0)
18 Global Catalog	REG_DWORD	0x00000000 (0)
19 Inter-site Messaging	REG_DWORD	0x00000000 (0)
2 Security Events	REG_DWORD	0x00000000 (0)
20 Group Caching	REG_DWORD	0x00000000 (0)
21 Linked-Value Replication	REG_DWORD	0x00000000 (0)
22 DS RPC Client	REG_DWORD	0x00000000 (0)
23 DS RPC Server	REG_DWORD	0x00000000 (0)
24 DS Schema	REG_DWORD	0x00000000 (0)
25 Transformation Engine	REG_DWORD	0x00000000 (0)
26 Claims-Based Access Control	REG_DWORD	0x00000000 (0)
3 ExDS Interface Events	REG_DWORD	0x00000000 (0)
4 MAPI Interface Events	REG_DWORD	0x00000000 (0)
5 Replication Events	REG_DWORD	0x00000000 (0)
6 Garbage Collection	REG_DWORD	0x00000000 (0)
7 Internal Configuration	REG_DWORD	0x00000000 (0)
8 Directory Access	REG_DWORD	0x00000000 (0)
9 Internal Processing	REG_DWORD	0x00000000 (0)

Ihnen stehen verschiedene Ereignistypen zur Verfügung. Jeder dieser Werte wird durch einen eigenen REG_DWORD-Wert repräsentiert. Jedem Wert ist standardmäßig der Wert 0 zugeordnet. Durch Erhöhung dieses Werts können für die einzelne Bereiche detaillierte Ereignisprotokollierungen eingestellt werden. Um die Protokollierung zu detaillieren, müssen Sie, wie bereits erwähnt, den Wert der einzelnen REG_DWORD-Einträge anpassen. Dazu sind sechs Stufen von 0 bis 5 zur Verfügung:

- 0 Diese Einstellung ist bereits standardmäßig für alle Ereignistypen gesetzt und protokolliert ausschließlich kritische Fehler
- 1 Bei dieser minimalen Einstellung werden auch etwas weniger kritische Probleme in der Ereignisanzeige protokolliert. Wenn Sie die Protokollierung von Active Directory erhöhen, sollten Sie zunächst mit diesem Wert beginnen. Bereits bei dieser Stufe werden deutlich mehr Meldungen in die Ereignisanzeige geschrieben. Stellen Sie daher zunächst sicher, ob diese Stufe ausreichend ist, bevor Sie weiter erhöhen.
- 2 Bei dieser Stufe wird die Protokollierung noch etwas erhöht. Sollte die Stufe 1 für Sie nicht ausreichen, dann wählen Sie zunächst Stufe 2.
- 3 Ab der Stufe 3 werden alle Schritte der einzelnen Aufgaben in Active Directory protokolliert. Während sich die Stufen 0 bis 2 hauptsächlich für die Fehlersuche im weiteren Sinne anbieten, wird ab Stufe 3 sehr viel mehr protokolliert. Ab dieser Stufe wird der Server durch die starke Protokollierung extrem belastet. Wenn Sie die Protokollierung auf mehr als Stufe 2 erhöhen, sollten Sie über eine extrem leistungsfähige Hardware verfügen. Zur Überwachung und Fehlerbehebung von Active Directory reichen die Stufen von 0 bis 2 normalerweise aus.
- 4 Diese Stufe erhöht den Protokollierungsgrad noch mal etwas höher als Stufe 3. Allerdings findet in diesem Fall nicht die starke Steigerung wie bei der Erhöhung von 2 auf 3 statt.
- 5 Diese Stufe ist die höchste, die Sie für einen Wert einstellen können. Bei dieser Stufe werden alle Informationen in die Ereignisanzeige geschrieben, die Active Directory protokollieren kann. Diese Stufe sollte nur für sehr wenige Kategorien gleichzeitig eingestellt werden, da der Protokollierungsgrad ansonsten die Übersicht in der Ereignisanzeige zu stark einschränkt.

Mit kostenlosen Zusatztools Active Directory überwachen

In diesem Abschnitt zeigen wir Ihnen verschiedene kostenlose Microsoft-Tools, mit denen Sie Fehler in Active Directory und DNS finden und beheben können.

AdExplorer (Active Directory Explorer)

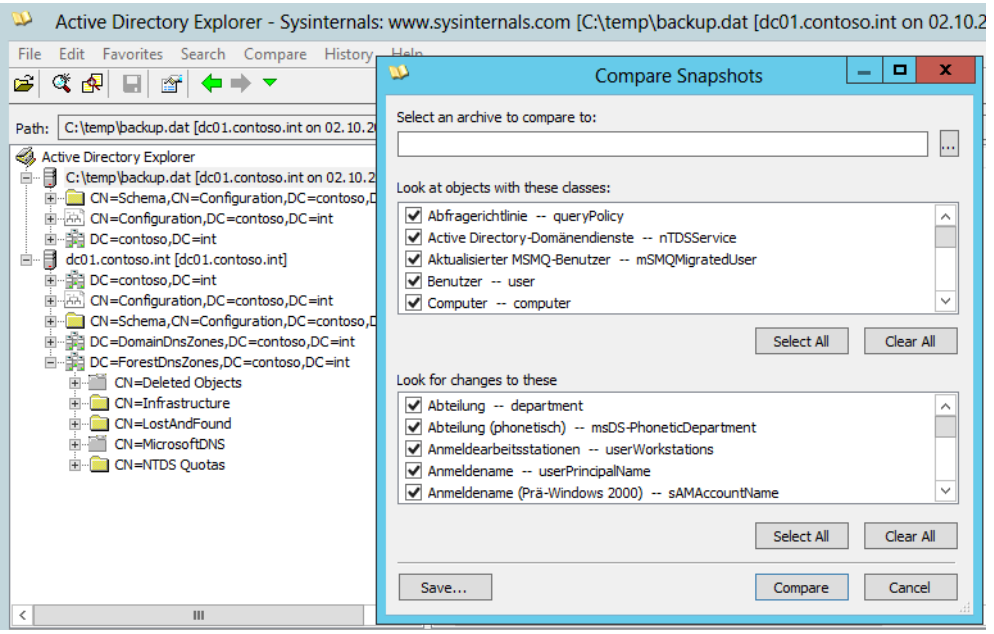
Active Directory Explorer (*http://technet.microsoft.com/de-de/sysinternals/bb963907* [Ms179-K15-02]) von Sysinternals bietet eine Verwaltungsoberfläche für die Active Directory-Datenbank, ähnlich zu ADSI-Edit. Beim Verbindungsaufbau legen Sie den Domänencontroller sowie die Benutzer fest, mit denen Sie sich verbinden wollen. Sie können die eingegebenen Daten auch abspeichern, sodass Sie nicht jedes Mal eine Authentifizierung durchführen müssen, um sich mit Active Directory zu verbinden.

Das Tool hat eine Explorer-ähnliche Oberfläche und erlaubt die Navigation in Active Directory. Sie können zur Analyse auch Momentaufnahmen (Snapshots) des produktiven Active Directory erstellen. Die Momentaufnahmen lassen sich nachträglich bearbeiten. Über den Menübefehl *File/Create Snapshot* erstellen Sie eine solche Momentaufnahme. Im Fenster können Sie einstellen, bis zu welcher CPU-Last die Momentaufnahme den Server belasten soll.

Haben Sie eine Momentaufnahme erstellt, können Sie diese parallel zur Verbindung mit dem aktuellen Active Directory oder einer anderen Momentaufnahme über das Menü *File* laden. Anschließend steht das Menü *Compare* zur Verfügung, über das Sie einen Vergleich zwischen den Momentaufnahmen oder dem produktiven Active Directory durchführen können.

Zwar kann Windows Server 2012 R2 solche Momentaufnahmen auch über das Befehlszeilentool Ntdsutil erstellen, aber nicht so einfach und leicht bedienbar wie Active Directory Explorer. Sie können das Tool auf jedem Computer starten, der Mitglied einer Domäne ist, Sie müssen nicht den Domänencontroller verwenden. Sie haben auch die Möglichkeit, mehrere Momentaufnahmen (Snapshots) zu unterschiedlichen Zeitpunkten zu erstellen. Diese können Sie nachträglich vergleichen, um so Änderungen nachzuverfolgen.

Abbildg. 15.13 Momentaufnahmen von Active Directory vergleichen



Active Directory Explorer ermöglicht auch das Anpassen von Einstellungen in Active Directory direkt auf Ebene der Datenbank. Sie können Attribute ändern, Einstellungen anpassen und Objekte löschen oder erstellen. Sie haben über das Menü *Favorites* auch die Möglichkeit, verschiedene Bereiche in Active Directory direkt wieder anwählen zu können, wenn Sie diese häufiger benötigen, zum Beispiel bestimmte Organisationseinheiten.

Über *Search* haben Sie die Möglichkeit, sehr detaillierte Suchabfragen in Active Directory durchzuführen. Komplexe Suchabfragen lassen sich im Suchfenster auch abspeichern und auf diesem Weg jederzeit wieder aufrufen. Im Suchfenster können Sie zusätzlich nach Attributen sowie nach Kombinationen von Attributen suchen. Außerdem haben Sie die Möglichkeit, über den Befehl *Properties* im Kontextmenü von Objekten die Sicherheitseinstellungen und Berechtigungen anpassen.

AdInsight (Insight for Active Directory)

Mit AdInsight von der Seite *http://technet.microsoft.com/de-de/sysinternals/bb897539* [Ms179-K15-03] analysieren Sie die LDAP-Verbindungen eines Servers in Echtzeit. Das Tool verwendet dazu die Datei *wldap32.dll*, welche den Zugriff auf Active Directory steuert. Das Tool zeigt, ähnlich zum Netzwerkmonitor für den Netzwerkverkehr, alle Anfragen von Clients an den Domänencontroller an, auch Daten, die der Domänencontroller blockiert. AdInsight hilft also dabei, Authentifizierungsprobleme von Anwendungen und Computern zu Active Directory zu finden und zu beheben.

Sie können die Daten, die das Tool ausliest, auch als Textdatei speichern und so nachträglich analysieren. Klicken Sie mit der rechten Maustaste auf einen Eintrag, erhalten Sie weitere Informationen über die einzelnen Einträge. Das Tool zeigt Verbindungsdaten an, sobald ein Programm oder Server Daten aus Active Directory abrufen will. Nach dem Start sehen Sie daher nicht gleich einen Eintrag, sondern erst, wenn ein Tool über das Netzwerk auf Active Directory über die Datei *wldap32.dll* zugreifen will.

Über das Menü *File* können Sie den aktuellen Scanvorgang abspeichern und nachträglich über AdInsight öffnen. Mit *File/Export to Text* lässt sich die Ausgabe als Textdatei exportieren. Da sich beim Verbindungsaufbau mit Active Directory viele Daten ansammeln, haben Sie die Möglichkeit, über den Menübefehl *Edit/Find* die Anzeige auch zu filtern. Weitere Filtermöglichkeiten stehen über das Menü *View* zur Verfügung.

Die verschiedenen Anzeigen lassen sich auch farblich hervorheben, um einen besseren Überblick zu erhalten. Diese Informationen finden Sie über das Menü *Highlight*. In den verschiedenen Spalten zeigt AdInsight genauere Daten an. Die Spalte *User* enthält, falls verfügbar, den Benutzernamen, mit dem die Anwendung versucht, auf Active Directory zuzugreifen. Sie müssen für die Messung das Tool nicht installieren, aber direkt auf dem Server starten. Das Tool bietet vor allem eine sehr wertvolle Hilfe, wenn ein Active Directory-abhängiger Dienst wie Exchange nicht funktioniert. Durch die umfangreichen Filtermöglichkeiten sehen Sie schnell, woran der Fehler liegt.

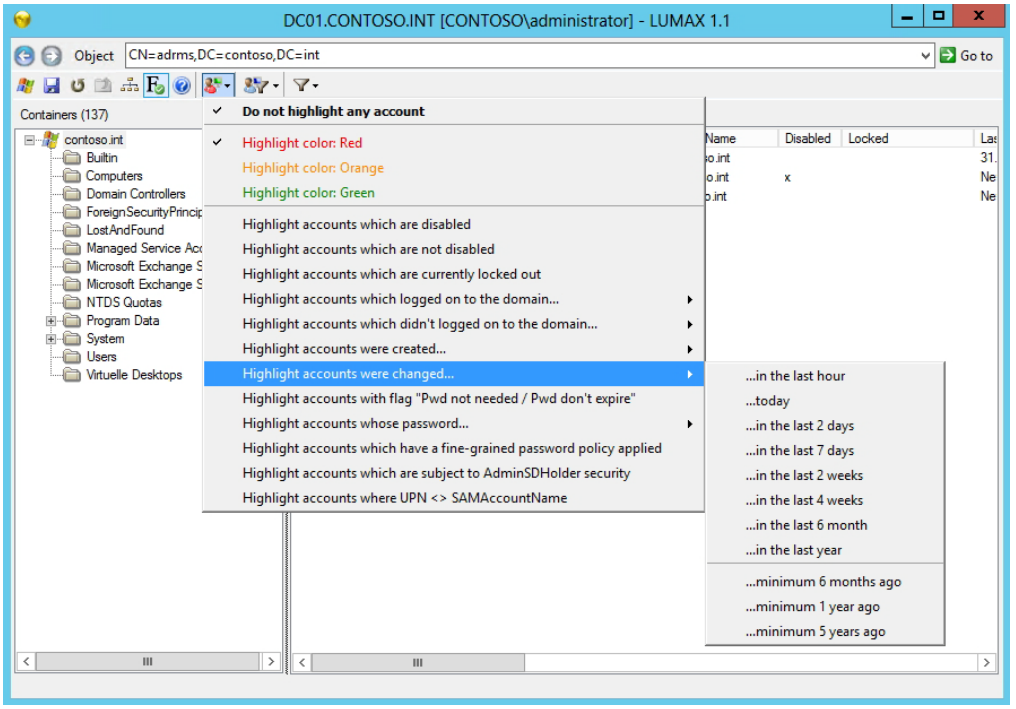
Active Directory-Datenbank mit Lumax abfragen

Wenn Sie Berichte über Einstellungen und Attribute von Benutzern in Active Directory erstellen wollen, sind Bordmittel oft nicht ausreichend. Es gibt aber kostenlose Tools wie Lumax, die dabei helfen, die Datenbank von Active Directory abzufragen und Berichte zu erstellen. Auch wichtige Systeminformationen wie die letzte Anmeldung lassen sich auf diesem Weg erfassen.

In Windows Server 2012 R2 können Sie auch mit dem Active Directory-Verwaltungscenter Informationen anzeigen und sortieren sowie Abfragen erstellen. Es lassen sich aber weder das letzte Anmeldedatum noch spezielle Abfragen zur Kennwortsicherheit nutzen. Sie sollten sich daher Lumax (*http://www.ldapexplorer.com/de/lumax.htm* [Ms179-K15-04]) herunterladen und testen, um Berichte zu erstellen.

Lumax muss weder installiert noch auf direkt auf einem Domänencontroller betrieben werden. Nach dem Download starten Sie einfach die EXE-Datei. Das Tool liest mit den Anmeldedaten des aktuellen Kontos die Domäne aus und zeigt erste Informationen an. Mit den Schaltflächen am oberen Rand lassen sich Einstellungen vornehmen und direkt Berichte erstellen.

Abbildg. 15.14 Abfragen von Active Directory-Objekten mit Lumax



Neben der einfachen Erstellung von Berichten lassen sich über die Schaltflächen am oberen Rand auch eigene Filter erstellen, um so zwischen verschiedenen Active Directory-Objekten zu unterscheiden. Sie können Computer, Benutzerkonten, beides oder einfach alle Objekte in Active Directory abfragen.

Berechtigungen in Active Directory mit AD ACL Scanner dokumentieren

Vor allem in Unternehmen, bei denen mehrere Administratoren Active Directory verwalten und ein komplexeres Berechtigungsmodell im Einsatz ist, kann es sinnvoll sein, die Berechtigungen in Active Directory auszulesen und zu dokumentieren. Dazu gibt es das kostenlose Tool AD ACL Scanner (*https://adaclscan.codeplex.com* [Ms179-K15-05]).

Bei AD ACL Scanner handelt es sich um ein PowerShell-Skript mit einer grafischen Oberfläche, das Tool muss daher nicht installiert werden. Sie benötigen mindestens die PowerShell 2.0 und Tool läuft problemlos auf der PowerShell 4.0

Mit AD ACL Scanner lesen Sie Berechtigungen detailliert aus. Ohne das Tool müssen Sie in *Active Directory- Benutzer und -Computer* in den Eigenschaften der einzelnen Objekte auf der Registerkarte *Sicherheit* zunächst manuell überprüfen, welche Rechte Benutzer oder andere Administratoren haben.

Interessant ist das Tool beispielsweise dann, wenn Sie sicherstellen möchten, dass bestimmte Anwender oder Administratoren nicht über Rechte verfügen, die sie nicht mehr haben sollten. Ein weiteres Szenario ist die Überprüfung von Rechten abhängig der Organisationseinheit. Beispielsweise könnte es sein, dass bestimmte Anwender Rechte für falsche Bereiche der Domäne haben. Dies können Sie mit AD ACL Scanner feststellen. Außerdem sehen Sie im Tool, ob Benutzer mit delegierten Rechten unter Umständen zu viele Rechte erhalten haben.

Ebenfalls möglich ist das Auffinden von Redundanzen. Haben Sie Rechte an mehrere Gruppen erteilt, können Sie diese leichter vergleichen und unter Umständen Gruppen zusammenführen.

Wie erwähnt, handelt es sich bei AD ACL Scanner um ein PowerShell-Skript. Laden Sie es von der genannten Seite herunten und starten Sie dann die PowerShell. Wechseln Sie zum Ordner, in den Sie das Skript kopiert haben.

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 blockiert die PowerShell Skripts.

Sie können die Ausführungsrichtlinie mit dem Cmdlet *Set-ExecutionPolicy* ändern und mit *Get-ExecutionPolicy* anzeigen. *Set-ExecutionPolicy Restricted* verhindert das Ausführen jeglicher Skripts. Mit *Set-ExecutionPolicy AllSigned* werden nur vertrauenswürdige Skripte ausgeführt. *Set-ExecutionPolicy Unrestricted* erlaubt die Ausführung aller Skripts. Diese Einstellung sollten Sie setzen. Sie müssen dazu die PowerShell aber über das Kontextmenü mit Administratorrechten starten.

Wenn Sie auf dem Server oder Computer nicht über umfassende Administratorrechte verfügen, können Sie die vorher genannten Einstellungen auch nur für Ihr Benutzerkonto ändern:

```
Set-ExecutionPolicy Unrestricted -Scope CurrentUser
```

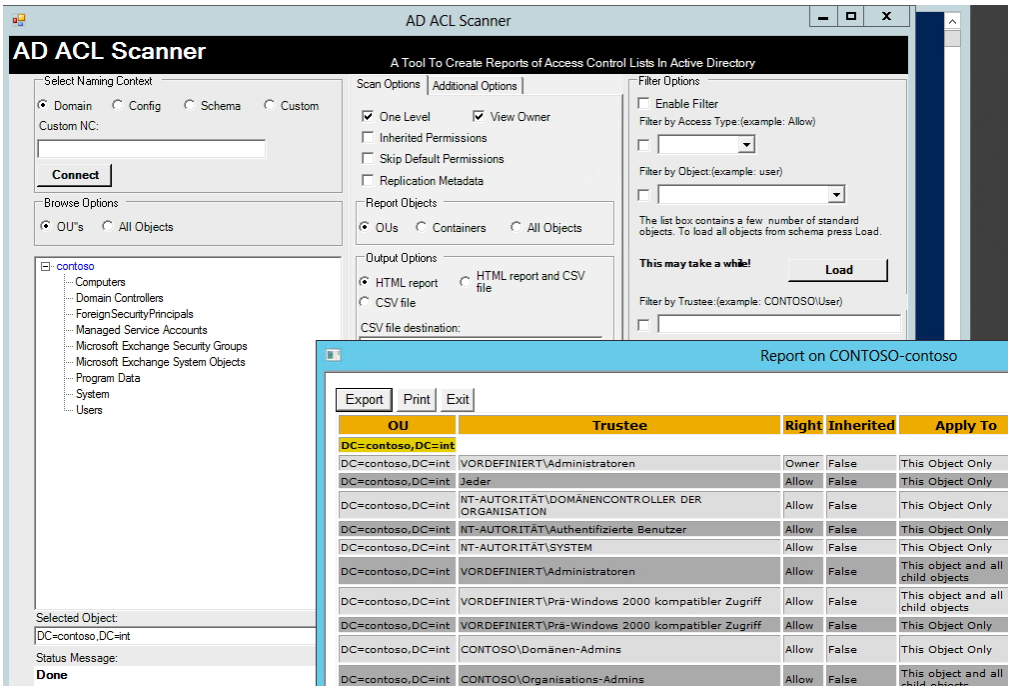
Anschließend rufen Sie in der PowerShell den Befehl *.\adaclscan1.2.ps1* auf. Sie müssen sich dazu im Ordner mit dem Tool befinden. Anschließend startet die grafische Oberfläche von AD ACL Scan. Wählen Sie hier zunächst die Scanoptionen aus.

Falls Sie das Tool auf einem Domänenmitglied aufgerufen haben, reicht es aus, wenn Sie auf *Connect* klicken. Anschließend verbindet sich das Tool mit den Rechten des Benutzers, der es startet, mit der Domäne und zeigt Daten an.

Klicken Sie dann im unteren Feld auf die OU oder Domäne, die Sie scannen möchten, und klicken Sie danach auf *Run scan*. Anschließend liest das Tool die Rechte aus und zeigt Sie in einem Bericht an. Den Bericht können Sie in eine HTML-Datei exportieren oder ausdrucken.

Das Tool bietet im rechten Bereich die Möglichkeit, die Ausgabe zu filtern. Dazu stehen zum Beispiel die Option *Skip Default Permissions* zur Verfügung. Außerdem können Sie nach der Verbindung mit der Domäne eine einzelne OU auswählen, um nicht alle Rechte angezeigt zu bekommen.

Abbildg. 15.15 AD ACL Scanner zeigt Berechtigungen in der Domäne als HTML-Bericht an



Standardmäßig zeigt AD ACL Scanner nicht die Rechte für untergeordnete Organisationseinheiten (OUs) an. Wollen Sie auch diese in den Bericht integrieren, müssen Sie die Option *One Level* in den Optionen deaktivieren. Um feststellen, wann die Rechte gesetzt wurden, aktivieren Sie vor dem Scan die Option *Replication Metadata*.

Mit AD Info kostenlos Berichte für Active Directory erstellen

Administratoren, die Active Directory verwalten, müssen in vielen Fällen für die Dokumentation oder Vorgesetzte Berichte erstellen können. Wer keine professionellen und kommerziellen Tools im Einsatz hat, muss solche Berichte entweder manuell mit Visio und Excel anfertigen oder kann alternativ auf kostenlose Tools setzen. Ein Beispiel für ein solches Tool ist AD Info. Wir zeigen Ihnen die Möglichkeiten und den Umgang mit diesem Freewaretool.

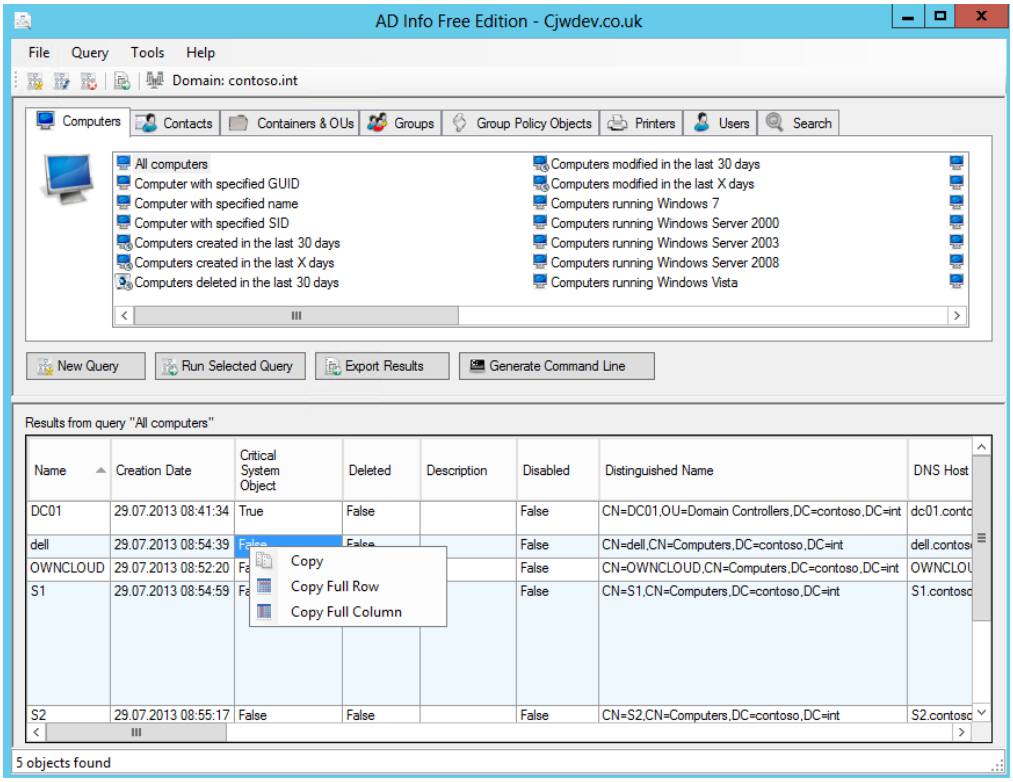
AD Info (*http://www.cjwdev.co.uk/Software/ADReportingTool/Info.html* [Ms179-K15-06]) kann Berichte aus Ihren Domänen auslesen. Offiziell gibt es noch keine Berichte für Windows Server 2012 R2 oder Windows 8.1, das Tool kann Daten von PCs mit diesen Betriebssystemen aber dennoch auslesen. Es ist in der kostenlosen Variante jedoch nicht möglich, sich zum Beispiel alle Computer mit den aktuellen Microsoft-Betriebssystemen anzuzeigen. Die neuen Betriebssysteme tauchen aber auf, wenn Sie zum Beispiel alle Computer anzeigen lassen. Der Hersteller erlaubt die kostenlose Nutzung unbegrenzt auch für kommerzielle Anwender.

Von AD Info gibt es darüber hinaus eine kommerzielle Variante. Diese ermöglicht das umfassende Exportieren von Berichten in verschiedene Formate wie Excel oder auch HTML. CSV-Dateien und HTML können Sie aber auch mit der kostenlosen Variante erstellen. Außerdem können Sie mit der kommerziellen Variante eigene Abfragen und Berichte erstellen. Die Abfragen lassen sich skripten und auf diesem Weg auch automatisch durchführen. Außerdem stellt der Entwickler für die kommerzielle Variante eine Gruppenrichtlinienvorlage zur Verfügung, mit der Sie Einstellungen des Tools noch besser automatisieren können. In den meisten Fällen reichen die Möglichkeiten der kostenlosen Version aus.

AD Info müssen Sie installieren, eine mobile Variante ist leider nicht verfügbar. Das Tool benötigt .NET Framework 3.5. Dieses müssen Sie zum Starten des Tools auf dem Server aktivieren. Nach dem Start des Tools sehen Sie im oberen Bereich über Registerkarten die verschiedenen Bereiche, für die Sie Berichte erstellen können. Auf der Registerkarte *Computer* können Sie durch Auswahl des entsprechenden Berichts alle Computer mit bestimmten Bedingungen anzeigen lassen.

Auf der Registerkarte *Computer* können Sie neben allen Computern die Anzeige auch nach SID, GUID, Erstellungsdatum des Kontos, Betriebssystem, Aktivität und mehr filtern lassen. Klicken Sie doppelt auf einen Bericht, lässt sich auswählen, welche Daten das Tool auslesen und anzeigen soll. Anschließend liest AD Info die Daten aus Active Directory aus.

Abbildg. 15.16 Mit AD Info erstellen Sie Berichte über die verschiedenen Bereiche in Active Directory



Im unteren Bereich wird nach dem Scanvorgang das Ergebnis angezeigt. Über das Kontextmenü können Sie den Inhalt der Felder, Zeilen und Spalten in die Zwischenablage kopieren und anderweitig weiterverwenden. Sie haben aber auch die Möglichkeit, über den Menübefehl *File* den Bericht als CSV- oder HTML-Datei zu speichern. Dabei können auch bestehende Dateien erweitert werden. Es ist nicht immer notwendig, eine neue Datei zu erstellen.

Sie können beim Starten eines Berichts neben den ausgewählten Feldern auch festlegen, welchen Container das Tool scannen soll. Es besteht die Möglichkeit, ganze Domänen oder nur einzelne Organisationseinheiten zu untersuchen. Neben Computern und Servern können Sie über die verschiedenen Registerkarten in AD Info auch andere Objekte aus Active Directory auslesen.

Ebenfalls erfassbar sind die Gruppenrichtlinienobjekte in der Domäne. Sie können auch diese nach verschiedenen Kriterien filtern lassen und überprüfen, welche Richtlinien für die Computerkonfiguration und die Benutzerkonfiguration gedacht sind.

Sie müssen das Tool nicht auf einem Domänencontroller oder Server installieren, sondern können dazu auch eine Arbeitsstation verwenden. Offiziell unterstützt das Tool noch nicht Windows Server 2012 R2 oder Windows 8.1, Sie können AD Info aber auf den beiden Betriebssystemen installieren und Daten ebenfalls auswerten lassen.

Active Directory kostenlos mit AD-Inspector analysieren

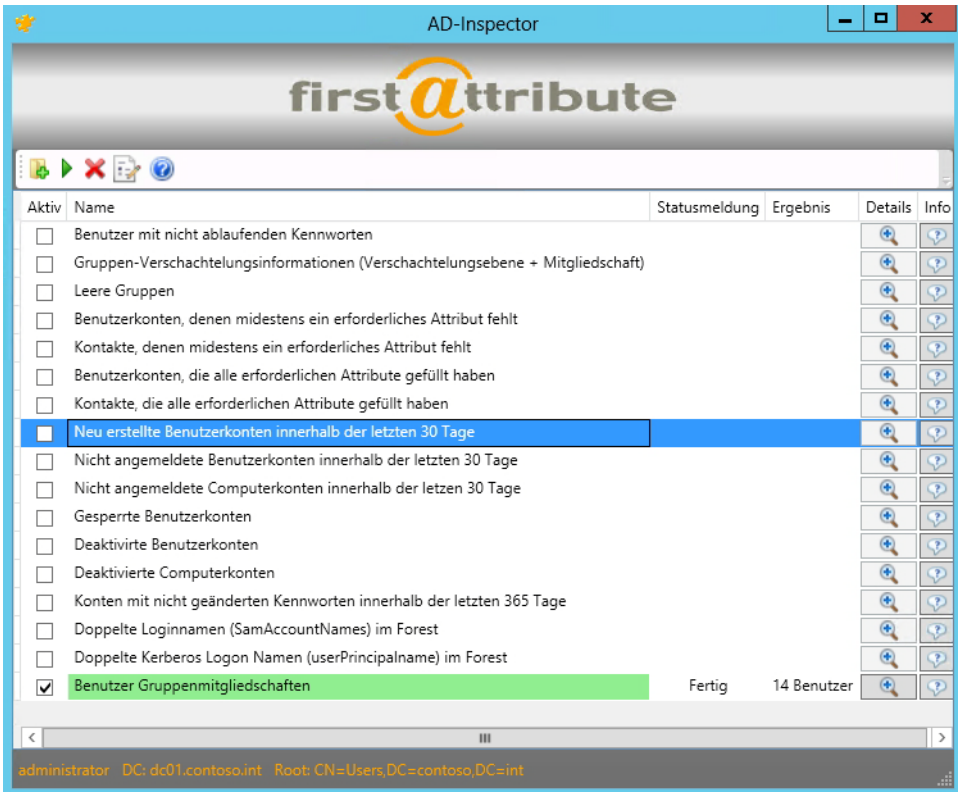
Administratoren stehen oft vor der Aufgabe, Active Directory in Unternehmen sauber zu halten. Leere Gruppen müssen entfernt, Benutzer mit abgelaufenen Kennwörter informiert und nicht verwendete Benutzerkonten identifiziert werden. Oft sind auch Informationen zu verschachtelten Gruppen, Gruppenmitgliedschaften, doppelten Benutzernamen in einer Gesamtstruktur oder auch Konten mit nicht geänderten Kennwörtern in einer bestimmten Zeit notwendig.

Das und noch mehr können Sie mit dem kostenlosen AD-Inspector analysieren. Wir zeigen Ihnen, wie Sie dabei vorgehen. AD-Inspector laden Sie von der Seite *http://www.firstattribute.com/de/active-directory-tools/ad-analysieren* [Ms179-K15-07] herunter. Sie müssen sich zwar für den Download registrieren, brauchen dazu allerdings keine echten Daten einzugeben. Der Download startet direkt nach der Eingabe der Daten, Sie erhalten keine E-Mail. Sie müssen das Tool nicht installieren, sondern können einfach die EXE-Datei starten. Das heißt, Sie können AD-Inspector auch mobil einsetzen.

Nach dem Download des Archivs entpacken Sie die ZIP-Datei und starten die Datei *FirstWare-AD-Inspector.exe*. Das Tool meldet sich mit dem Benutzernamen bei Active Directory an, mit dem Sie am Server oder PC angemeldet sind. Wie Sie ein anderes Benutzerkonto verwenden, zeigen wir Ihnen später noch ausführlich.

Im ersten Schritt wählen Sie mit dem Ordnersymbol oben links aus, welchen Container in Active Directory Sie analysieren möchten. Sie können entweder die ganze Domäne oder nur einzelne Organisationseinheiten untersuchen lassen. Im unteren Bereich des Tools sehen Sie, mit welchem Benutzernamen die Verbindung zu Active Directory stattfindet und welchen Domänencontroller AD-Inspector verwendet. Außerdem ist der Container angegeben, den Sie untersuchen lassen.

Abbildg. 15.17 AD-Inspector erstellt schnelle und einfache Analysen für Active Directory



Um zum Beispiel eine Analyse der Gruppenmitgliedschaften durchzuführen, aktivieren Sie das Kontrollkästchen *Benutzer Gruppenmitgliedschaften*. Klicken Sie danach auf das grüne Dreieck im oberen Bereich des Tools. Anschließend führt AD-Inspector eine Analyse durch und zeigt die Spalte dann in grün an. Sie sehen in der Spalte *Ergebnis* die gewünschten Informationen und die Anzahl an Objekten, für welche die entsprechende Bedingung zutrifft.

Klicken Sie in der entsprechenden Spalte des durchgeführten Scans auf das Lupensymbol, erhalten Sie mehr Informationen und einen ausführlichen Bericht angezeigt. Es öffnet sich ein neues Fenster, in dem die gefundenen Benutzer mit den entsprechenden Informationen aufgelistet sind. Mit einem Klick auf das Diskettensymbol speichern Sie den Bericht in eine CSV-Datei.

AD-Inspector startet mit dem Benutzerkonto, mit dem Sie am PC oder Server angemeldet sind. Sie haben aber mit Bordmitteln in Windows die Möglichkeit, das Tool unter einem anderen Benutzernamen zu starten. Dazu verwenden Sie die Eingabeaufforderung und das Tool *Runas.exe*. Mit dem Befehlszeilentool starten Sie Programme mit beliebigen Benutzernamen. Um zum Beispiel AD-Inspector mit dem Benutzernamen *joost* in der Domäne *contoso.int* zu starten, geben Sie den folgenden Befehl ein:

```
runas /user:joost@contoso.int "c:\temp\firstware-ad-inspector\firstware-ad-inspector.exe"
```

Einbrüche in Active Directory effizient erkennen

Mit Windows Server 2008 R2 und Windows Server 2012 hat Microsoft die Möglichkeiten und den Umfang der Ereignisanzeige stark erweitert. Diese enthält allerdings auch in vielen Fällen Einträge, die Sie nicht benötigen. Um Einbrüche und Angriffe auf Active Directory und die gesetzten Berechtigungen zu erkennen, gibt es aber effiziente Überwachungsrichtlinien. Die entsprechenden Einstellungen dazu nehmen Sie über Gruppenrichtlinien vor.

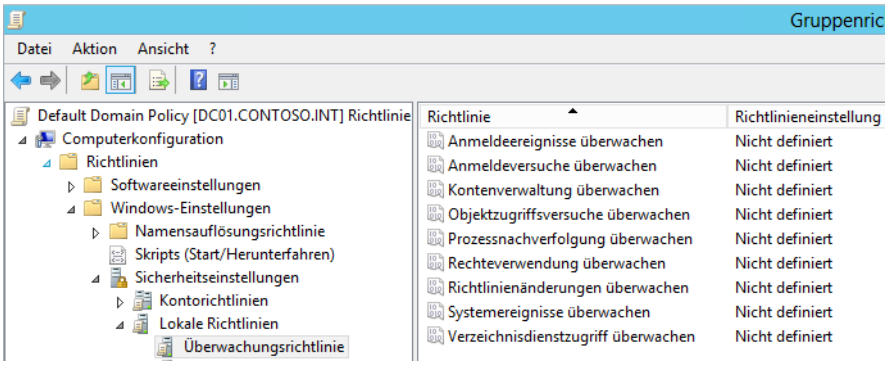
Um Zugriffe auf Active Directory zu überwachen, besteht der erste Schritt darin, eine bestehende Richtlinie zu bearbeiten, die den Domänencontrollern zugewiesen ist, zum Beispiel die *Default Domain Controller Policy*, oder eine neue Richtlinie zu erstellen und den Domänencontrollern zuzuweisen. In den Richtlinien werden dann die zu überwachenden Ereignisse konfiguriert.

Sobald die Domänencontroller die Einstellungen übernehmen, beginnen sie mit der Überwachung und speichern die Daten in der Ereignisanzeige. Diese müssen Sie allerdings entsprechend filtern oder so konfigurieren, dass eine automatische Antwort erfolgt.

Aktivieren der einfachen Überwachung

Sollen Sie auf Computern, Dateiserver oder Domänencontroller den Zugriff auf Dateien und Objekte überwachen, müssen Sie die entsprechenden Einstellungen in der Überwachungsrichtlinie festlegen. Diese findet sich in der Richtlinienüberwachung im Bereich *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Überwachungsrichtlinien*. Die Überwachung der Zugriffe auf das Dateisystem von Servern unterscheidet sich von der Überwachung der Objekte in Active Directory nicht besonders. Dazu aktivieren Sie die Option *Objektzugriffsversuche überwachen*. Neben Dateizugriffen überwachen Sie mit dieser Einstellung auch Zugriffe auf Drucker. In der Standardeinstellung ist die Überwachung zunächst nicht aktiviert.

Abbildg. 15.18 Überwachen von Active Directory in Windows Server 2012 R2



Nach der Aktivierung müssen Sie noch auswählen, ob erfolgreiche und/oder fehlgeschlagene Zugriffsversuche protokolliert werden sollen.

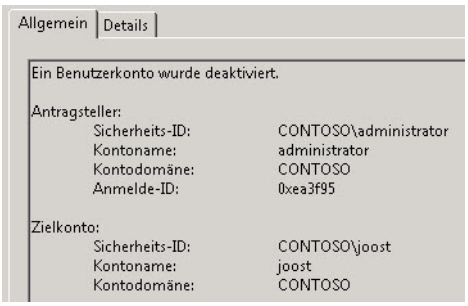
Um Anmeldungen in Active Directory zu überwachen, muss die Richtlinie *Anmeldeereignisse überwachen* aktiviert sein. Sie können auswählen, ob die Domänencontroller erfolgreiche Anmeldungen überwachen sollen oder auch erfolglose Anmeldungen an Active Directory. Die Option überwacht allerdings keine Anmeldungen an den Arbeitsstationen, sondern nur für die Domänencontroller selbst. Um auch Arbeitsstationen zu überwachen, muss die Richtlinie als Gruppenrichtlinie mit allen Computern verknüpft sein. Bei allen Einstellungen bedeutet die Überwachung von Fehlern, dass die Änderung versucht wurde, aber nicht geklappt hat. Mit *Erfolgreich* werden vollzogene Änderungen protokolliert.

Sobald die Überwachung aktiviert ist, schreibt der Server in der Ereignisanzeige über *Windows-Protokolle/Sicherheit* die Daten der Überwachung. Aus den Ereignissen ist ersichtlich, wann sich ein Benutzer an- und wieder abgemeldet hat.

Um die Überwachung auszudehnen, gibt es noch die Richtlinieneinstellung *Anmeldeversuche überwachen*, ebenfalls wieder mit den Möglichkeiten *Erfolgreich* oder *Fehler*. Im Gegensatz zu den Anmeldeereignissen überwachen die Anmeldeversuche auch die Anmeldungen an Arbeitsstationen und Mitgliedsservern der Domäne. Diese Überwachung findet daher nur auf Domänencontrollern statt, da diese die Anmeldung von Benutzerkonten auf Mitgliedscomputern erst ermöglichen.

Die nächste Stufe der Überwachung ist die Bearbeitung der Benutzerkonten in Active Directory mit der Einstellung *Kontenverwaltung überwachen*. Domänencontroller können überwachen, wenn ein Administrator Änderungen an einem Benutzerkonto durchführt. Die Kontenverwaltung überwacht das Erstellen, Ändern und Löschen von Benutzerkonten sowie das Umbenennen, Aktivieren oder Deaktivieren. Auch die Änderung von Kennwörtern überwacht die Richtlinie. In der Ereignisanzeige unter *Windows-Protokolle/Sicherheit* findet sich dann der Eintrag, welcher Benutzer zu welchem Zeitpunkt eine Änderung durchgeführt hat und was die Änderung war.

Abbildg. 15.19 Überwachen von Active Directory



Ein weiterer wichtiger Punkt bei der Überwachung ist *Systemereignisse überwachen*. Hierbei zeichnet der Server Aktionen wie das Herunterfahren von Computern und Änderungen auf, die das Betriebssystem betreffen. Um diesen Bereich noch weiter auszubauen, lässt sich noch *Richtlinienänderungen überwachen* aktivieren. Dabei halten die Server auch Anpassungen der Gruppenrichtlinien und lokalen Richtlinien fest. Sollen die Server auch das Beenden und Starten von Prozessen überwachen, hilft die Einstellung *Prozessnachverfolgung überwachen*. Diese erzeugt aber eine große Anzahl von Einträgen.

Lassen Sie die *Objektzugriffsversuche überwachen* besteht auch die Möglichkeit, den Zugriff auf Dateiservern, Freigaben und die enthaltenen Dateien inklusive der Änderungen nachzuverfolgen. Nach dieser Aktivierung müssen Sie aber zusätzlich die Überwachung in den Eigenschaften des ent-

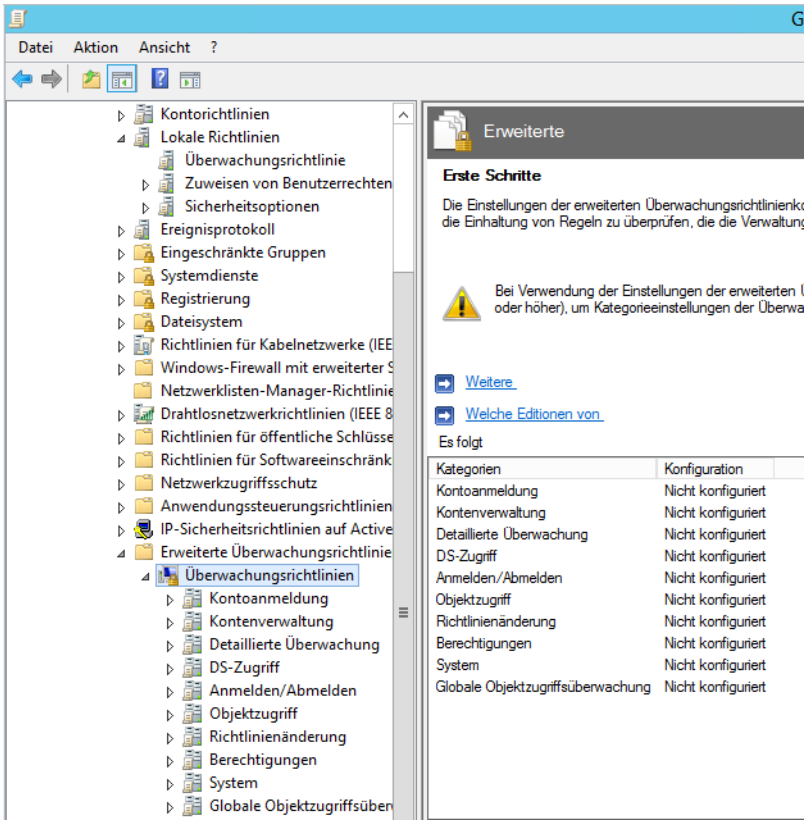
sprechenden Ordners aktivieren. Nachdem Sie die Überwachung aktiviert haben, müssen Sie die eigentliche Überwachung für die entsprechenden zu überwachenden Dateien und Ordnern aktivieren. Dazu sind die Eigenschaften des Ordners und die Registerkarte *Sicherheit* wichtig.

Erweiterte Überwachung nutzen

Neben den herkömmlichen Überwachungseinstellungen lassen sich mit Windows Server 2012/2012 R2 noch detaillierte Maßnahmen treffen, um das eigene Netzwerk effizient zu schützen. Hierzu hat Microsoft neben Richtlinien auch in der PowerShell neue Möglichkeiten integriert.

Unwichtige Überwachungsinformationen lassen sich auf diesem Weg deaktivieren, sodass Windows nur das Wichtigste protokolliert. Generell ist es empfehlenswert, die klassische Überwachung und die neue Überwachung nicht parallel zu verwenden, sondern sich für Basisüberwachung oder die erweiterte Überwachung zu entscheiden. Allerdings unterstützen die neuen Funktionen nur Computer mit Windows Server 2008 R2/2012/2012 R2 und Windows Vista/7/8. Beispiel für die neue Überwachung ist die einfache Überwachung der An- oder Abmeldung an Computern. Die erweiterte Überwachung bietet hierzu eine Untergliederung in neun Unterbereiche an.

Abbildg. 15.20 Erweiterte Sicherheitsüberwachung in Windows Server 2012 R2



Die erweiterten Einstellungen sind über *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Erweiterte Überwachungsrichtlinienkonfiguration* zu finden. Wie bei der normalen Überwachung ist es sehr empfehlenswert, für die Überwachung eine eigene Gruppenrichtlinie für Überwachungseinstellungen zu erstellen und zuzuweisen.

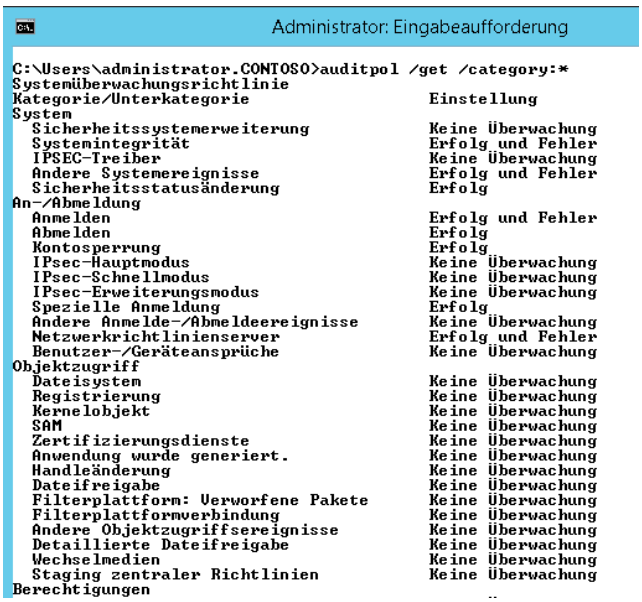
Der Vorteil der neuen Überwachungsfunktionen ist eine spezifischere Aufgliederung der überwachten Ereignisse. Es lassen sich zum Beispiel die einzelnen Anmeldefunktionen ausführlich überwachen und untergliedern. Die Einstellungen dazu sind bei *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Erweiterte Überwachungsrichtlinienkonfiguration/Überwachungsrichtlinien/Kontoanmeldung* zu finden.

Um auszuschließen, dass sich alte Einstellungen und Optionen in den erweiterten Überwachungseinstellungen überschneiden, sollten Sie die Einstellungen setzen, in denen festgelegt ist, dass die neuen Einstellungen die alten immer außer Kraft setzen. Die Einstellung *Überwachung: Unterkategorieeinstellungen der Überwachungsrichtlinie erzwingen* ist in den Richtlinien über *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Sicherheitsoptionen* zu finden.

Ein wichtiger Punkt bei der Überwachung sind die Benutzerkonten und vor allem die Sicherheitsgruppen in Active Directory. Durch Ändern der Mitgliedschaft können nicht unerhebliche Sicherheitsgefahren entstehen, vor allem bei Administratorgruppen. Diese Überwachung ist im Bereich *Kontenverwaltung* der erweiterten Einstellungen zu finden. Da hierbei Active Directory überwacht wird, muss die entsprechende Gruppenrichtlinie mit den Domänencontrollern verknüpft sein, zum Beispiel mit der Organisationseinheit *Domain Controllers*. Die Verwendung der Standardrichtlinie *Default Domain Controllers Policy* ist nicht empfohlen.

Nachdem die Richtlinie erstellt und die Einstellungen gesetzt sind, sollten Sie die Richtlinie auf den Domänencontrollern mit *gpupdate /force* in der Eingabeaufforderung übernehmen. Ob die Einstellung übernommen wurde, testen Sie mit dem Befehl *auditpol /get /category:**.

Abbildg. 15.21 Überprüfen der Überwachung von Domänencontrollern



Lassen Sie über Richtlinien zum Beispiel Sicherheitsgruppen überwachen, muss als Nächstes noch festgelegt werden, welche Sicherheitsgruppen die Überwachung berücksichtigen soll. Sie müssen dazu die Eigenschaften der Sicherheitsgruppe in der Konsole *Active Directory-Benutzer und -Computer* aufrufen, die Registerkarte *Sicherheit* anzeigen, auf *Erweitert* klicken und anschließend auf die Registerkarte *Überwachung*. Diese Registerkarte ist nur zu sehen, wenn *Ansicht/Erweiterte Features* aktiviert ist. Um die Überwachung zu aktivieren, klicken Sie doppelt auf den ersten Eintrag *Jeder* und wählen dann *Alle Eigenschaften schreiben* aus. Nach der Änderung übernehmen die Domänencontroller die Änderungen durch Eingabe von *gpupdate /force*.

Ist die Überwachung erfolgreich, finden Sie in der Ereignisanzeige auf den Domänencontrollern über *Windows-Protokolle/Sicherheit* einen neuen Eintrag mit der ID 4728, wenn der Sicherheitsgruppe, zum Beispiel den Domänenadmins, neue Benutzer hinzugefügt werden. In der Meldung der Ereignisanzeige ist zu sehen, welcher Benutzer die Änderung durchgeführt hat und welcher Benutzer aufgenommen wurde. Wird ein Benutzer entfernt, erscheint eine Meldung mit der ID 4729.

Sie können über das Kontextmenü der IDs eine Aufgabe hinterlegen. Über diese Aufgabe besteht zum Beispiel die Möglichkeit, eine E-Mail zu senden, sobald eine Änderung stattfindet. In der Aufgabe legen Sie den Absender fest, den Empfänger, einen Text und den SMTP-Server. Neben E-Mails lassen sich über diesen Weg auch Programme und Batchdateien starten. Mit etwas Feinarbeit können Sie also komplett ohne Zusatzwerkzeuge eine umfangreiche Überwachungskonfiguration betreiben.

Windows Server 2012 R2 kann auch mit Bordmitteln die Ereignisanzeigen verschiedener Server im Netzwerk zusammentragen und anzeigen. Diese Funktion trägt die Bezeichnung *Abonnements* und lässt sich direkt in der Ereignisanzeige einrichten. Basis ist der Systemdienst *Windows-Ereignisammeldienst*. Dieser muss auf dem Server gestartet sein, der die verschiedenen Ereignisse sammeln soll, sowie auf allen beteiligten Servern. Im ersten Schritt müssen Sie die Remoteverwaltung auf den einzelnen Servern aktivieren.

Dazu führen sie auf jedem Quellcomputer und dem Sammlungscomputer in einer Eingabeaufforderung mit Administratorrechten (über das Schnellmenü mit ⊞+X gestartet) den Befehl *winrm quickconfig* aus. Im nächsten Schritt ist noch der Befehl *wecutil qc* notwendig. Das Tool konfiguriert das Weiterleiten von Ereignissen über das Netzwerk zu einem Sammlungscomputer.

Anmeldungen im Netzwerk überwachen

Mit dem Befehlszeilentool LogonSessions von Sysinternals (*http://technet.microsoft.com/de-de/sysinternals/bb896769* [Ms179-K15-08]) zeigen Sie alle angemeldeten Sitzungen auf einem Computer an. Geben Sie den Befehl ohne Optionen ein, reicht unter Umständen der Puffer der Eingabeaufforderung nicht aus, da zu viele Informationen enthalten sind. Verwenden Sie in diesem Fall die Option *logonsessions | more* oder vergrößern Sie den Puffer der Eingabeaufforderung über deren Eigenschaften. Alternativ lassen Sie die Ausgabe über die Option > *logon.txt* in eine Datei umleiten.

Mithilfe dieses Programms erhalten Sie sehr schnell ausführliche Informationen, welche Sitzungen gerade auf dem Computer geöffnet sind. Verwenden Sie zusätzlich noch die Option *–p*, zeigt das Tool auch die geöffneten Prozesse der einzelnen Sitzungen und damit der angemeldeten Benutzer an. So können Sie effizient überwachen, wer auf einem Server angemeldet ist und mit welchen Applikationen der Anwender arbeitet. Neben den angemeldeten Benutzern zeigt das Tool auch die Systemkonten an. Außer auf Terminalservern ist das Tool auch hervorragend in Active Directory-Umgebungen einsetzbar.

Bereinigen 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 Active Directory zu integrieren. Durch die erneute Integration erhält der Domänencontroller wieder die Daten von den anderen Domänencontrollern der Domäne. Wenn Sie einen Domänencontroller aus dem Active Directory entfernen müssen, gibt es grundsätzlich folgende 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 zu Active Directory verloren. Er soll heruntergestuft werden, ohne Verbindung mit Active Directory zu haben oder neu installiert zu werden. Active Directory muss dazu nachträglich bereinigt werden.
3. Der Domänencontroller ist komplett ausgefallen und funktioniert nicht mehr. Active Directory muss mitgeteilt werden, dass der Domänencontroller nicht mehr verfügbar ist.

Auf den folgenden Seiten sind die Abläufe der einzelnen Möglichkeiten beschrieben, einen Domänencontroller aus dem Active Directory zu entfernen.

Vorbereitungen beim Entfernen eines Domänencontrollers

Wird ein Domänencontroller aus Active Directory entfernt, sollten Sie einige Vorbereitungen treffen, damit die Anwender durch seinen Ausfall nicht betroffen sind:

- Stellen Sie sicher, dass der Domänencontroller nicht als bevorzugter oder alternativer DNS-Server von einem anderen Rechner der Domäne verwendet wird (auch nicht als DNS-Weiterleitungsserver)
- Entfernen Sie – falls möglich – vor der Herabstufung DNS von diesem Domänencontroller. Haben Sie DNS entfernt, überprüfen Sie auf einem anderen DNS-Server in den Eigenschaften der DNS-Zone, dass der Server auf der Registerkarte *Namenserver* nicht mehr aufgeführt wird. Entfernen Sie aber nicht den Hosteintrag des Servers, da dieser für die Herabstufung noch benötigt wird.
- 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 (siehe Kapitel 10)
- 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

Um einen Domänencontroller herunterzustufen, verwenden Sie am besten die PowerShell und das Cmdlet *Uninstall-ADDSDomainController*. Sie müssen mindestens noch das lokale Kennwort des Administrators über den Befehl festlegen. Dieses müssen Sie als SecureString in der PowerShell definieren. Die Syntax dazu lautet:

```
Uninstall-ADDSDomainController -LocalAdministratorPassword (Read-Host -Prompt "Kennwort" -
AsSecureString)
```

Mit *Get-Help Uninstall-ADDSDomainController* erhalten Sie mehr Informationen zu dem Befehl.

Abbildg. 15.22 Herunterstufen eines Domänencontrollers in der PowerShell

Wenn es sich bei dem Domänencontroller, den Sie herabstufen wollen, um einen globalen Katalog handelt, werden Sie darüber mit einer Meldung informiert. Mit der Option *–LastDomainControllerInDomain* können Sie 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 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.

HINWEIS Auch wenn ein herabgestufter Domänencontroller im Anschluss noch als Mitgliedsserver verwendet werden kann, sollten Sie sicherheitshalber das Computerkonto aus der Domäne entfernen und das Betriebssystem neu auf dem Server installieren, um Altlasten zu entsorgen. Auch den Servernamen sollten Sie ändern, wenn aus dem Namen hervorgeht, dass es sich um einen Domänencontroller gehandelt hat.

Wenn Sie einen Domänencontroller, der die Verbindung mit dem Active Directory verloren hat, nicht neu installieren wollen, können Sie Active Directory trotz fehlender Verbindung entfernen. Verwenden Sie in diesem Fall noch die Option *–force*. Nach der erzwungenen Entfernung von Active Directory ist der Domänencontroller allerdings kein Mitgliedsserver mehr, sondern ein allein stehender Server. Sie können sich daher an diesem Server nicht mehr bei der Domäne anmelden.

HINWEIS Mehr zur Herabstufung eines Domänencontrollers und dem Entfernen von Active Directory von einem Server lesen Sie in Kapitel 11.

Bereinigen der Metadaten von Active Directory

Die Metadaten von Active Directory enthalten alle Einträge und Servernamen, die zu Active Directory gehören. Wenn ein Domänencontroller ausfällt oder erzwungen aus dem Active Directory entfernt wird, sollten die Metadaten nachträglich bereinigt werden. Für diese Bereinigung benötigen Sie wiederum das Befehlszeilentool Ntdsutil, das Sie bereits beim Verschieben der FSMO-Rollen kennen gelernt haben (siehe Kapitel 10). Um die Metadaten von Active Directory zu bereinigen, starten Sie zunächst Ntdsutil in der Eingabeaufforderung von Active Directory. Gehen Sie wie in den folgenden Schritten beschrieben vor:

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, um wieder zum Menü *metadata cleanup* zurückzukehren.
5. Als Nächstes geben Sie *select operation target* ein.
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 Standorts>*.
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. Nachdem Sie den Server ausgewählt haben, geben Sie *quit* ein, damit Sie wieder zum Menü *metadata cleanup* gelangen.
13. Geben Sie nun den Befehl *remove selected server* ein. Es folgt eine Warnmeldung, in der Sie das Entfernen des Servers bestätigen müssen. Nach der Bestätigung dieser 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. 15.23 Entfernen eines Domänencontrollers aus Active Directory

```
C:\Users\Administrator>ntdsutil
ntdsutil: metadata cleanup
metadata cleanup: connections
server connections: connect to server dc01.contoso.int
Bindung mit "dc01.contoso.int" ...
Eine Verbindung mit "dc01.contoso.int" wurde unter Verwendung der Benutzerinform
ationen des lokal angemeldeten Benutzers wurde hergestellt.
server connections: quit
metadata cleanup: select operation target
select operation target: list domains
1 Domäne(n) gefunden
0 - DC=contoso,DC=int
select operation target: select domain 0
Kein aktueller Standort
Domäne - DC=contoso,DC=int
Kein aktueller Server
Kein aktueller Namenskontext
select operation target: list sites
2 Standort(e) gefunden
0 - CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
1 - CN=Berlin,CN=Sites,CN=Configuration,DC=contoso,DC=int
select operation target: select site 0
Standort - CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
Domäne - DC=contoso,DC=int
Kein aktueller Server
Kein aktueller Namenskontext
select operation target: list servers in site
4 Server gefunden
0 - CN=DC01,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
1 - CN=SRV3,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
2 - CN=DC03,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
3 - CN=DC04,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
select operation target: select server 1
Standort - CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=int
Domäne - DC=contoso,DC=int
Server - CN=SRV3,CN=Servers,CN=Erbach,CN=Sites,CN=Configuration,DC=contoso,DC=in
t
        DSA-Objekt - CN=NTDS Settings,CN=SRV3,CN=Servers,CN=Erbach,CN=Sites,CN=C
onfiguration,DC=contoso,DC=int
        DNS-Hostname - srv3.contoso.int
        Computerobjekt - CN=SRV3,OU=Domain Controllers,DC=contoso,DC=int
Kein aktueller Namenskontext
select operation target: quit
metadata cleanup: remove selected server
```

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. Nachdem 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*. Im nächsten Schritt müssen Sie den Domänencontroller noch aus dem Standort löschen, dem er zugeordnet war. Verwenden Sie dazu das Snap-*In Active Directory-Standorte und -Dienste*.

Navigieren Sie dazu zum Standort des Domänencontrollers, wählen Sie im zugehörigen Kontextmenü den Befehl *Löschen* aus oder drücken Sie die Entf-Taste. Der Server sollte sich ohne Probleme löschen lassen. Überprüfen Sie als Nächstes in den NTDS-Settings jedes Domänencontrollers in Active Directory, ob der Domänencontroller noch als Replikationspartner eingetragen ist, und entfernen Sie in diesem Fall die Verbindung. Der Server sollte sich mit keinem anderen Domänencontroller mehr replizieren.

Zusammenfassung

In diesem Kapitel haben wir Ihnen ausführlich gezeigt, wie Sie Fehler in Active Directory beheben und Ihre Domänen auf Funktionalität hin überprüfen können. Neben der Fehlersuche sollten Sie die Tools in diesem Kapitel auch zur Diagnose der Domänencontroller einsetzen.

Im nächsten Kapitel erfahren Sie, wie sich Active Directory sichern und wiederherstellen lässt.

Kapitel 16

Active Directory – Sicherung, Wiederherstellung und Wartung

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, wie Sie die Active Directory-Datenbank sichern, wiederherstellen und die Datenbank warten. Wollen Sie einzelne Objekte wiederherstellen, verwenden Sie den Active Directory Papierkorb und das Active Directory-Verwaltungscenter. Dieses behandeln wir in Kapitel 11. Active Directory ist, wie die Exchange-Datenbank, eine Jet-basierte Datenbank. Die Datenbank liegt in Form der Datei *ntds.dit* auf jedem Domänencontroller im Ordner *\Windows\NTDS*. Für die Datensicherung und anschließende Wiederherstellung reicht es jedoch nicht aus, nur diese Datei zu sichern. Es sind einige Maßnahmen notwendig, die bei der Sicherung und einer eventuell notwendigen Wiederherstellung benötigt werden.

Die Sicherung von Active Directory erfolgt zusammen mit der Sicherung von anderen wichtigen Systemkomponenten eines Servers. Bei dieser Sicherung, die auch durch das Windows-eigene Datensicherungsprogramm durchgeführt werden kann, werden alle zusammenhängenden Daten, die Active Directory benötigt, ebenfalls gesichert. Sie sollten mit Ihrem Datensicherungsprogramm regelmäßig eine Datensicherung von Active Directory durchführen. Alternativ kann die Active Directory-Datensicherung durch das Windows-Datensicherungsprogramm in eine Datei erfolgen, die dann wieder durch die Datensicherung auf eine CD/DVD oder über das Netzwerk gesichert wird.

In Kapitel 11 sind wir bereits auf wichtige Zusatztools eingegangen, mit denen Objekte in Active Directory wiederhergestellt werden können, falls diese versehentlich gelöscht wurden. Wird die Systempartition eines Domänencontrollers gesichert, enthält diese Sicherung zusätzlich noch den Boot Configuration Data Store (BCD-Store), die kompletten Windows-Systemdateien mit der Registry, den Inhalt des *SYSVOL*-Ordners, die Active Directory-Datenbank (*ntds.dit*) sowie die Logdateien von Active Directory. Auch wenn bei der Sicherung alle Daten gesichert werden, gibt es weiterhin verschiedene Möglichkeiten der Wiederherstellung: Es kann der komplette Server wiederhergestellt werden, der Systemstatus kann wiederhergestellt werden, aber auch einzelne Dateien und Ordner können aus der Sicherung wieder zurückgespielt werden. Um den Systemstatus zurückzuspielen, muss unter Windows Server 2012 R2 der Domänencontroller im Verzeichnisdienst-Wiederherstellungsmodus gestartet werden.

Active Directory sichern und wiederherstellen

In diesem Abschnitt zeigen wir Ihnen die notwendigen Schritte, um eine Datensicherung von Active Directory auf einem Domänencontroller herzustellen. Die hier beschriebene Sicherung lässt sich manuell durchführen, es kann aber auch ein Zeitplan erstellt werden. Mehr zum Thema Datensicherung erfahren Sie auch in den Kapiteln 8, 16, 35 und 36.

Active Directory mit der Windows Server-Sicherung sichern

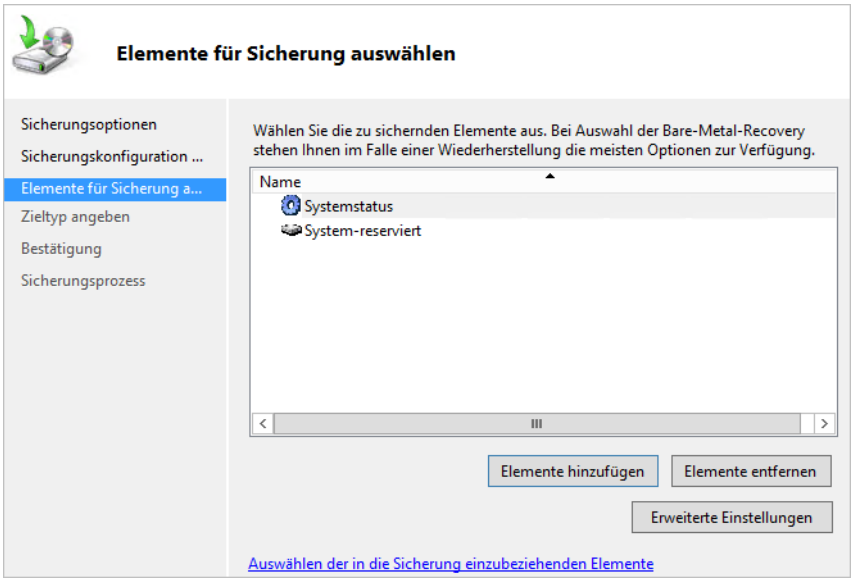
Rufen Sie zunächst die Windows Server-Sicherung auf und starten Sie den Assistenten für eine Einmalsicherung oder einem Sicherungszeitplan. Wählen Sie bei der Option der Sicherung *Benutzerdefiniert* aus.

HINWEIS Die Windows-Serversicherung ist standardmäßig nicht installiert. Sie müssen das Feature über den Server-Manager nachinstallieren (siehe Kapitel 4). Das Verwaltungsprogramm zur Sicherung finden Sie nach der Installation des Windows-Features über den Menüpunkt *Tools* im Server-Manager.

Natürlich besteht auch die Möglichkeit, die Option *Vollständig* für die Sicherung des Servers auszuwählen. In diesem Fall wird neben der Datensicherung von Active Directory der komplette Server mit allen vorhandenen Festplatten und Partitionen gesichert.

Auf der nächsten Seite wählen Sie über *Elemente hinzufügen* aus, was gesichert werden soll. Aktivieren Sie die Optionen *Systemstatus* und *System-reserviert*, damit notwendige Daten zur Wiederherstellung von Active Directory mitgesichert werden.

Abbildg. 16.1 Auswählen der zu sichernden Elemente



Auf der nächsten Seite wählen Sie aus, wo die Daten im Netzwerk gesichert werden sollen. Die Datensicherung unterstützt das Ablegen der Sicherung nicht auf der gleichen Partition, die gesichert wird.

Durch Aktivierung der Option *VSS-Kopiesicherung* in den erweiterten Einstellungen, nutzt das Sicherungsprogramm den Volumeschattenkopie-Dienst (Volume Shadow Copy Service, VSS). Nach der Bestätigung der restlichen Eingaben beginnt der Assistent mit der Sicherung.

TIPP Das Sicherungsprogramm ermöglicht es, die Datensicherung über die Eingabeaufforderung zu konfigurieren. Das kann zum Beispiel sinnvoll sein, wenn die Sicherung über ein Skript oder unter Server Core durchgeführt werden soll. Mit dem folgenden Befehl wird die Sicherung der notwendigen Partitionen auf die Zielfestplatte durchgeführt:

```
wbadmin start backup –allCritical –backuptarget:<Zielfestplatte> –quiet
```

Durch Eingabe von *–quit* muss die Eingabe nicht bestätigt werden, sondern die Sicherung beginnt sofort.

Mit dem folgenden Befehl werden alle hinterlegten Partitionen in die Sicherung eingeschlossen:

```
wbadmin start backup –include:<Partition1>:,<Partition2>:,<PartitionN> –
backuptarget:<Zielfestplatte>: –quiet
```

Die Partitionen werden durch Komma ohne Leerzeichen voneinander getrennt.

Wiederherstellen von Active Directory aus der Datensicherung

Um eine Wiederherstellung durchzuführen, starten Sie zunächst den Domänencontroller neu und drücken direkt nach dem Start die Taste F8, bis das Bootmenü erscheint. Achten Sie aber darauf, dass sich die Datei, welche die Datensicherung enthält, lokal auf dem Server befindet, da diese zur Wiederherstellung benötigt wird.

Wählen Sie in den Bootoptionen den Menüpunkt *Verzeichnisdienstwiederherstellung* aus, anschließend startet Windows. Melden Sie sich bei der Anmeldung mit dem Kennwort des Verzeichnisdienst-Wiederherstellungsmodus an. Nachdem Sie sich angemeldet haben, können Sie die Wiederherstellung durchführen.

TIPP Soll ein Domänencontroller beim nächsten Start mit dem Verzeichnisdienst-Wiederstellungsmodus gestartet werden, geben Sie den Befehl *bcdedit /set safeboot dsrepair* ein. Befindet sich der Server im Verzeichnisdienst-Wiederherstellungsmodus, wird mit dem Befehl *bcdedit /deletevalue safeboot* beim nächsten Mal wieder normal gestartet.

So ersparen Sie sich das Drücken der Taste F8, wenn Sie sich zum Beispiel nicht direkt an der Konsole befinden. Mit dem Befehl *shutdown t 0 –r* wird der Server dann neu in dem jeweilig konfigurierten Modus gestartet.

Beachten Sie, dass ein Domänencontroller den Anwendern nicht zur Verfügung steht, während er sich im Verzeichnisdienst-Wiederherstellungsmodus befindet. Sie sollten daher dafür sorgen, dass noch andere Domänencontroller zur Verfügung stehen, bei denen sich die Anwender anmelden können. Achten Sie darauf, dass am Domänencontroller keine Anmeldung an der Domäne möglich ist. Die Anmeldung erfolgt über die Schaltfläche *Anderer Benutzer*. Als Benutzername wird *Administrator* verwendet und das Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus.

Sie müssen sicherstellen, dass der Server, auf dem Sie die Active Directory-Daten wiederherstellen wollen, wieder funktioniert. Das Betriebssystem muss in der gleichen Version wie vor dem Ausfall installiert sein. Auch der Name des Servers und die Festplattenkonfiguration müssen identisch sein. Nachdem Sie diese Vorbedingungen sichergestellt haben, können Sie den Server in den Verzeichnisdienst-Wiederherstellungsmodus starten. Da das Betriebssystem auf dem Server neu installiert wurde, lässt sich dieser Vorgang problemlos durchführen. Nachdem Sie den Server im Verzeichnisdienst-Wiederherstellungsmodus gestartet haben, führen Sie, wie weiter vorne beschrieben, eine nicht autorisierende Wiederherstellung durch, um sicherzustellen, dass alle Daten auf den Server

zurückgespielt wurden. Starten Sie nach dem Wiederherstellungsvorgang den Server normal durch und stellen Sie wie bei der nicht autorisierenden Wiederherstellung fest, ob der Server wieder normal in Active Directory funktioniert.

Wenn ein Domänencontroller einer Domäne ausfällt, werden Sie in den wenigsten Fällen den Weg einer nicht autorisierenden Wiederherstellung gehen müssen. Die einzige Ausnahme wäre, der Server der Domäne steht in einer Niederlassung, die nur durch eine schmalbandige Leitung mit der Domäne in der Zentrale verbunden ist. Wenn Sie einen Domänencontroller einer Niederlassung wiederherstellen wollen, ist der beste Weg, den Domänencontroller neu zu installieren und wieder in die Domäne als zusätzlicher Domänencontroller mit aufnehmen (siehe Kapitel 13). In diesem Fall erhält der Domänencontroller alle Funktionen und Daten von Active Directory zurück. Wenn Sie einen ausgefallenen Domänencontroller wiederherstellen möchten, ohne dass ein Backup benötigt wird, gehen Sie folgendermaßen vor:

1. Stellen Sie zunächst sicher, dass ein weiterer Domänencontroller in der Domäne und dem Standort verfügbar ist. Ohne einen weiteren Domänencontroller der Domäne ist die Wiederherstellung eines Domänencontrollers nicht möglich.
2. Bereinigen Sie zunächst das Active Directory von den alten Daten des Domänencontrollers, wie in Kapitel 15 beschrieben.
3. Stellen Sie sicher, dass der noch vorhandene Domänencontroller alle FSMO-Rollen von dem ausgefallenen Domänencontroller übernommen hat (siehe Kapitel 10 und 11).
4. Konfigurieren Sie den noch vorhandenen Domänencontroller als globalen Katalogserver, falls außer dem ausgefallenen Server kein anderer Domänencontroller dieser Niederlassung ein globaler Katalogserver ist (siehe Kapitel 10).
5. Stellen Sie sicher, dass die Bereinigung von Active Directory in alle Niederlassungen repliziert wurde (siehe Kapitel 14 und 15).
6. Installieren Sie den ausgefallenen Domänencontroller neu mit Windows Server 2012 R2 und allen Patches (siehe Kapitel 2 und 3).
7. Installieren Sie auf dem Server auch die DNS-Funktionalität, falls diese vorher auch auf diesem Server installiert war (siehe Kapitel 10 und 11).
8. Geben Sie dem Server den gleichen Netzwerknamen wie vor dem Ausfall und stellen Sie in den Netzwerkeinstellungen ein, dass ein DNS-Server der Domäne verwendet wird, der verfügbar ist (siehe Kapitel 5).
9. Rufen Sie den Assistenten für die Erstellung von Active Directory auf (siehe Kapitel 10 und 13).
10. Nachdem der Server erfolgreich als Domänencontroller installiert wurde, können Sie die Rollen, die er vor dem Ausfall hatte, auf ihn zurückschieben (siehe Kapitel 10). Die Active Directory-Daten werden automatisch auf ihn repliziert werden.

Der Weg, einen Domänencontroller einfach neu in die Domäne aufzunehmen, anstatt eine Datensicherung zu verwenden, ist oft schneller und sauberer. Achten Sie jedoch unbedingt darauf, vor der erneuten Aufnahme in eine Domäne die Metadaten von Active Directory zu bereinigen, damit sichergestellt ist, dass keine veralteten Daten in Active Directory die erneute Heraufstufung des Domänencontrollers verhindern (siehe Kapitel 15).

Active Directory-Datenbank warten

Mit dem Zusatztool Ntdsutil können auch verschiedene Wartungsmaßnahmen mit der Active Directory-Datenbank durchgeführt werden. Diese beschreiben wir in diesem Abschnitt.

Verschieben der Active Directory-Datenbank

Unter manchen Umständen, wenn zum Beispiel der Festplattenplatz auf dem Server nicht mehr ausreicht oder wenn der Domänencontroller an ein hochsicheres SAN angeschlossen wird, kann es sinnvoll sein, den Datenordner von Active Directory auf einen anderen Datenträger zu verschieben. Damit Sie die Datenbank von Active Directory auf einem Domänencontroller verschieben können, müssen Sie den Server im Verzeichnisdienst-Wiederherstellungsmodus starten. Gehen Sie zum Verschieben folgendermaßen vor:

1. Starten Sie zunächst den Domänencontroller im Verzeichnisdienst-Wiederherstellungsmodus und melden Sie sich am Server an.
2. Starten Sie Ntdsutil und geben Sie anschließend den Befehl *activate instance ntds* ein.
3. Geben Sie den Befehl *files* ein.
4. Geben Sie den Befehl *move db to <Lauferk:\Ordner>* ein, um die Datenbank zu verschieben. Wenn der Name des neuen Ordners Leerzeichen enthält, setzen Sie die Bezeichnung in Anführungszeichen.
5. Nachdem Sie den Befehl bestätigt haben, läuft ein Skript ab, welches die Datenbank in den gewünschten Ordner verschiebt.
6. Geben Sie nach dem erfolgreichen Verschieben der Datenbank den Befehl *move logs to <Laufwerk:\Ordner>* ein, damit die Logdateien von Active Directory ebenfalls verschoben werden.
7. Geben Sie an dieser Stelle den Befehl *integrity* ein, um die Konsistenz der Active Directory-Datenbank zu überprüfen.
8. Verlassen Sie Ntdsutil und überprüfen Sie, ob die Dateien im neuen Ordner angelegt wurden.
9. Stellen Sie sicher, dass die Dateiberechtigungen auf NTFS-Ebene für den neuen Ordner der Active Directory-Datenbank noch stimmen. Rufen Sie dazu die Eigenschaften des Ordners auf und wechseln Sie zur Registerkarte *Sicherheit*. In den Berechtigungen sollten die vier Gruppen *Administratoren*, *Ersteller-Besitzer*, *Lokaler Dienst* und *System* eingetragen sein.
10. Die beiden Gruppen *Administratoren* und *System* sollten Vollzugriff auf den Ordner haben. Bei den anderen Benutzergruppen sind keinerlei Berechtigungen eingetragen und keine Berechtigungen verweigert. Die Berechtigungen dürfen auch nicht von übergeordneten Ordnern vererbt werden, sondern sollten direkt in diesem Ordner gesetzt sein. Vererbte Berechtigungen werden in Grau angezeigt. Sollten die Berechtigungen bei Ihnen nicht exakt so gesetzt sein, ändern Sie die Berechtigungen entsprechend ab.

Offlinedefragmentation der Active Directory-Datenbank

Bei der Active Directory-Datenbank handelt es sich, wie bei der Datenbank von Exchange, um eine Jet-basierte ESE-Datenbank. Das Active Directory wächst zwar nicht so stark an wie die Datenbank eines Exchange-Servers, aber dennoch kann es sinnvoll sein, die Active Directory-Datenbank zu defragmentieren. Vor allem in größeren Organisationen, bei denen das Active Directory durchaus mehrere Gigabyte groß werden kann, sollte zumindest jährlich eine Offlinedefragmentation durchgeführt werden.

Bevor Sie eine Offlinedefragmentation durchführen, sollten Sie eine Sicherung des Systemstatus Ihres Active Directory durchführen. Wie bei der Offlinedefragmentation von Exchange wird zunächst die Datenbank kopiert, dann offline defragmentiert und anschließend zurückkopiert. Stellen Sie daher sicher, dass sich auf dem Datenträger, auf dem Sie die Offlinedefragmentation durchführen, genügend Speicherplatz frei ist. Um eine Offlinedefragmentation durchzuführen, gehen Sie folgendermaßen vor:

1. Starten Sie den Server im Verzeichnisdienst-Wiederherstellungsmodus.
2. Öffnen Sie eine Eingabeaufforderung und starten Sie Ntdsutil.
3. Geben Sie anschließend den Befehl *activate instance ntds* ein.
4. Geben Sie den Befehl *files* ein, um zur *file maintenance* zu gelangen.
5. Geben Sie den Befehl *compact to <Laufwerk:\Ordner>* ein. Wählen Sie als Verzeichnis einen beliebigen Ordner auf der Festplatte aus. Ntdsutil kopiert die Datenbankdatei in diesen Ordner und defragmentiert sie.
6. Wenn keine Fehlermeldungen während der Offlinedefragmentation auftreten, können Sie die Datei *ntds.dit* aus dem Ordner, in welchen sie defragmentiert wurde, zurück in den Datenbankpfad der produktiven Datenbank kopieren. Diesen Vorgang führt Ntdsutil nicht automatisch aus, Sie müssen die Datei manuell kopieren. Sichern Sie die alte Version der *ntds.dit* aus dem produktiven Datenbankordner. Verschieben Sie die defragmentierte Datei in den produktiven Ordner der Datenbank und überschreiben Sie die alte Version.
7. Geben Sie in der *file maintenance* von Ntdsutil den Befehl *integrity* ein, um die Integrität der Datenbank festzustellen.
8. Wenn die Integrität der neuen Datenbank sichergestellt ist, können Sie den Domänencontroller ganz normal neu starten. Sollten Fehler auftreten, kopieren Sie die zuvor gesicherte Originalversion zurück und führen Sie einen erneuten Integritätstest durch. Ist der Test diesmal erfolgreich abgeschlossen, versuchen Sie erneut eine Offlinedefragmentation und starten Sie den Test erneut. Sie sollten den Domänencontroller erst in den normalen Modus starten, wenn sichergestellt ist, dass die Datenbank auch konsistent ist.

TIPP Da Active Directory als Systemdienst läuft, kann dieser für die Defragmentation auch beendet werden. In diesem Fall muss der Server nicht im Verzeichnisdienst-Wiederherstellungsmodus gestartet werden, sodass andere Dienste auf dem Server weiter von den Anwendern verwendet werden können.

Reparieren der Active Directory-Datenbank

Unter manchen Umständen kann es vorkommen, dass die Active Directory-Datenbank nicht mehr funktioniert. Gehen Sie bei einem solchen Problem folgendermaßen vor:

1. Starten Sie den Server im Verzeichnisdienst-Wiederherstellungsmodus.
2. Öffnen Sie eine Eingabeaufforderung und starten Sie Ntdsutil.
3. Geben Sie anschließend den Befehl *activate instance ntds* ein.
4. Geben Sie *files* ein, um zu *file maintenance* zu gelangen.
5. Geben Sie *integrity* ein, um einen Integritätstest der Datenbank durchzuführen. Wenn dieser Test einen Fehlermeldung anzeigt, können Sie versuchen, die Datenbank in Ntdsutil zu retten.
6. Verlassen Sie mit *quit* die *file maintenance*, aber bleiben Sie in der Oberfläche von Ntdsutil.
7. Geben Sie den Befehl *semantic database analysis* ein.
8. Geben Sie zunächst den Befehl *verbose on* ein, damit Sie detaillierte Informationen erhalten.
9. Geben Sie als Nächstes den Befehl *go fixup* ein.
10. Das Tool beginnt daraufhin mit der kompletten Diagnose der Active Directory-Datenbank und versucht eine Reparatur durchzuführen.
11. Verlassen Sie im Anschluss Ntdsutil und starten Sie den Domänencontroller neu. Überprüfen Sie, ob die Active Directory-Datenbank wieder funktioniert. Sollten noch immer Schwierigkeiten auftreten, stellen Sie die Datenbank aus einer Datensicherung wieder her und überprüfen Sie im Anschluss, ob Active Directory bei diesem Stand noch konsistent war. Sie sollten so lange Backups zurückspielen, bis sichergestellt ist, dass die Datenbank wieder konsistent ist.

Erstellen von Snapshots der Active Directory-Datenbank

In Windows Server 2012 R2 ist es möglich, einen Snapshot der Active Directory-Datenbank zu erstellen und diesen bereitzustellen. Diese bereitgestellte Offlineversion der Datenbank kann dann ebenso bearbeitet werden wie die Onlineversion. Der Snapshot wird als Schattenkopie der Datenbank erstellt. Die Bereitstellung der Active Directory-Datenbank wird durch das Tool Dsamain durchgeführt.

Die Erstellung von Snapshots wird wiederum mit dem Befehl *snapshot* in Ntdsutil gestartet. Auf den Snapshot kann mit beliebigen LDAP-Tools, wie zum Beispiel Ldp oder dem Snap-In *Active Directory-Benutzer und -Computer*, zugegriffen werden. Snapshots dürfen nur von Domänen-Admins und Organisationsadmins erstellt werden.

Um einen Snapshot bereitzustellen, muss nicht unbedingt ein solcher mit Ntdsutil erstellt werden. Auch eine Datensicherung von Active Directory kann bereitgestellt werden. Der beste und schnellste Weg, einen Snapshot zu erstellen, ist folgender:

1. Öffnen Sie eine Eingabeaufforderung und starten Sie Ntdsutil.
2. Geben Sie *snapshot* ein.
3. Geben Sie den Befehl *activate instance ntds* ein.
4. Geben Sie *create* ein. Der Snapshot wird anschließend erstellt und dessen GUID angezeigt.

5. Geben Sie den Befehl *mount <GUID* des Snapshots> ein. Mit *list mounted* werden alle gemounteten Snapshots angezeigt. Mit *unmount <GUID>* wird die Bereitstellung wieder aufgehoben und mit *delete <GUID>* der Snapshot wieder gelöscht.

TIPP Per Skript oder als geplante Aufgabe wird ein Snapshot auch durch die Eingabe des Befehls *ntdsutil "activate instance ntds" snapshot create quit quit* erstellt.

Mit dem Befehl *dsamain /dbpath <Pfad zur Datenbankdatei> /ldapport <Port>* kann eine Offlinekopie der Active Directory-Datenbank auch als LDAP-Server bereitgestellt werden. Anschließend kann auf diese Offlinekopie wie auf jeden LDAP-Server auch zugegriffen werden.

Zusammenfassung

Wir haben Ihnen in diesem Kapitel gezeigt, wie Sie die Active Directory-Daten sichern und wiederherstellen können. Im Gegensatz zum Active Directory-Papierkorb, den wir in den Kapiteln 10 und 11 besprechen, haben wir in diesem Kapitel erläutert, wie Sie Daten mit der Windows-Serversicherung sichern und später wieder herstellen können. Und auch die Pflege der Datenbank, zum Beispiel die Offlinedefragmentation, war Thema dieses Kapitels.

Im nächsten Kapitel gehen wir auf die Erstellung von Vertrauensstellungen für Active Directory ein.

Kapitel 17

Active Directory – Vertrauensstellungen

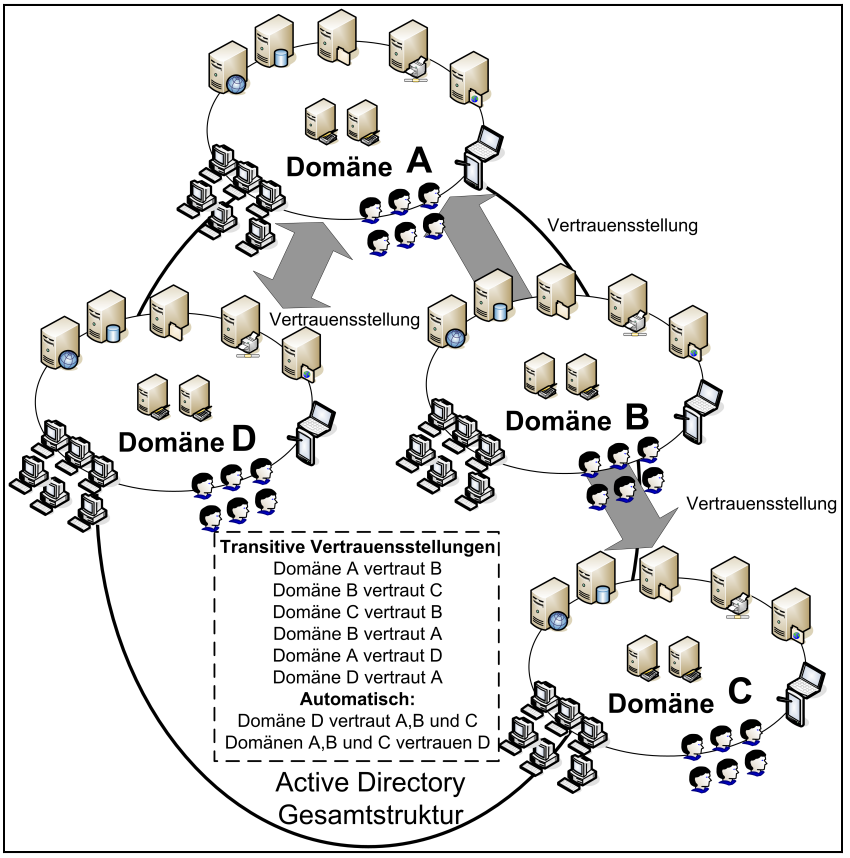
In diesem Kapitel:

In Active Directory spielen Vertrauensstellungen eine wichtige Rolle. In einer Gesamtstruktur werden bei der Erstellung von Domänen automatisch Vertrauensstellungen eingerichtet zwischen Domänen und Strukturen eingerichtet. Diese Vertrauensstellungen sind transitiv. Wenn Sie in Windows Server 2012 R2 eine Vertrauensstellung zwischen den Domänen A und B sowie zwischen B und C einrichten, dann vertraut auch Domäne A der Domäne C oder umgekehrt die Domäne C der Domäne A.

Wichtige Grundlagen der Vertrauensstellungen in Active Directory

Durch Domänen, untergeordnete Domänen und Strukturen gibt es die Möglichkeit, fast unbegrenzt Domänen anbinden zu können, die sich automatisch untereinander vertrauen. In Active Directory vertraut jede Domäne jeder anderen Domäne, die Bestandteil der gleichen Gesamtstruktur ist. Es ist nicht mehr notwendig, zahlreiche manuelle Vertrauensstellungen einzurichten.

Abbildg. 17.1 Transitive Vertrauensstellungen unter Windows Server 2012 R2 in Active Directory



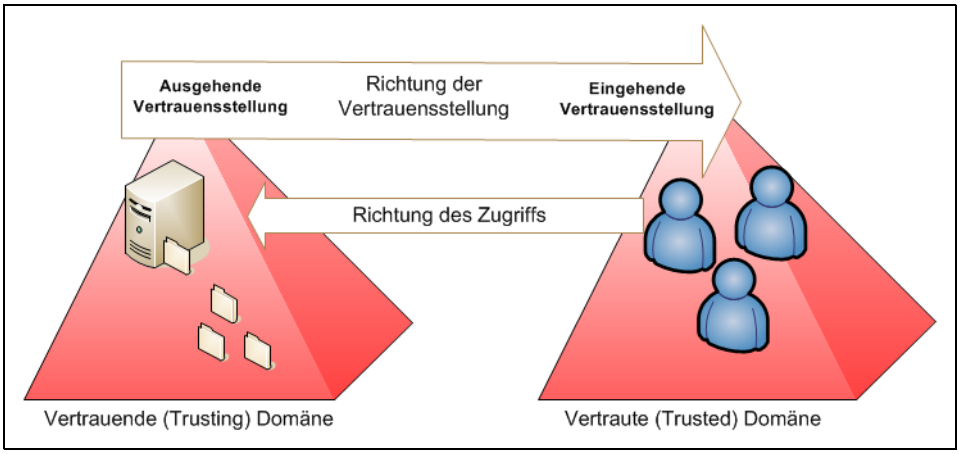
Administratoren müssen keinerlei Maßnahmen vornehmen, damit sich Domänen in einer Gesamtstruktur untereinander vertrauen. In einer Gesamtstruktur werden jedoch nicht automatisch Vertrauensstellungen zwischen allen Domänen eingerichtet, sondern es wird ein gewisses Schema beibehalten:

- 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.

Die Verwaltung der Vertrauensstellungen findet mithilfe 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.

Außer den automatisch eingerichteten Vertrauensstellungen können Sie 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 in 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 auch umgekehrt denkbar.

Abbildg. 17.2 Vertrauensstellungen in Active Directory verstehen



Weitere Unterscheidungen der Vertrauensstellungen in 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.

Bevor eine Vertrauensstellung erstellt wird, prüft der Server die Eindeutigkeit in folgender Reihenfolge:

- Den NetBIOS-Namen der Domäne
- Den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) der Domäne
- Die Sicherheits-ID (SID) der Domäne

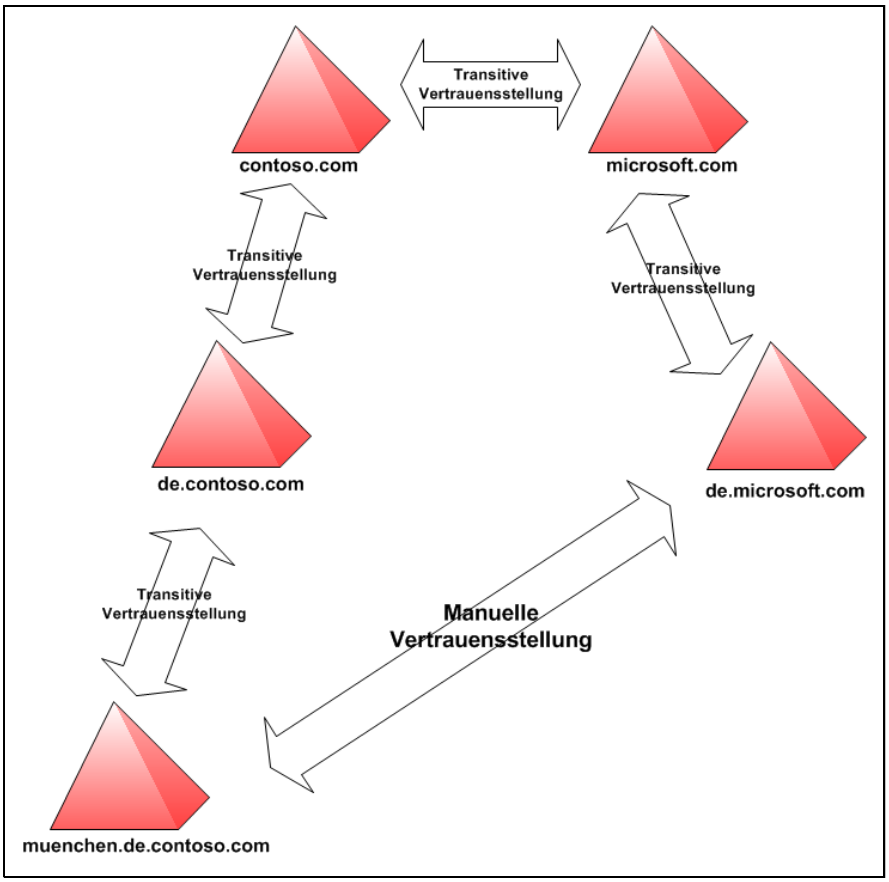
Diese drei Punkte müssen eindeutig sein, da ansonsten keine Vertrauensstellung erstellt werden kann. Wenn die Domänen-SID identisch ist, muss eine der beiden Domänen erneut installiert werden. Diese Szenarien können eintreffen, wenn eine Domäne von der anderen geklont oder nach dem Installieren des Betriebssystems auf einem Server dieser geklont wurde und anschließend Sysprep nicht angewendet 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 in Active Directory

Neben den beschriebenen Vertrauensstellungen in Active Directory gibt es verschiedene Möglichkeiten, nachträglich manuelle Vertrauensstellungen einzurichten:

- Externe Vertrauensstellungen zu einer anderen Struktur oder Domäne
- Gesamtstruktur-übergreifende Vertrauensstellungen, um die Rootdomänen von zwei unterschiedlichen Gesamtstrukturen zu verbinden. Alle Domänen der beiden Gesamtstrukturen vertrauen sich anschließend automatisch transitiv.
- Vertrauensstellungen zu einem Nicht-Windows-Kerberossystem
- Vertrauensstellungen zwischen untergeordneten Domänen verschiedener Strukturen, sogenannte Shortcut Trusts oder abkürzende Vertrauensstellungen, sind ebenfalls möglich. Diese Art der Vertrauensstellung wird häufig verwendet, um den Zugriff auf Ressourcen zwischen Domänen zu beschleunigen. In Active Directory vertrauen sich alle Domänen innerhalb einer Struktur untereinander. Diese Einrichtung der transitiven Vertrauensstellungen erfolgt automatisch. 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 Rootdomäne der eigenen Struktur gehen, dann zur Rootdomäne der anderen Struktur und schließlich zur entsprechenden untergeordneten Domäne. Diese Authentifizierung kann durchaus einige Zeit dauern.

Abbildg. 17.3 Pfad der Vertrauensstellungen mit mehreren Domänenstrukturen in einer Gesamtstruktur

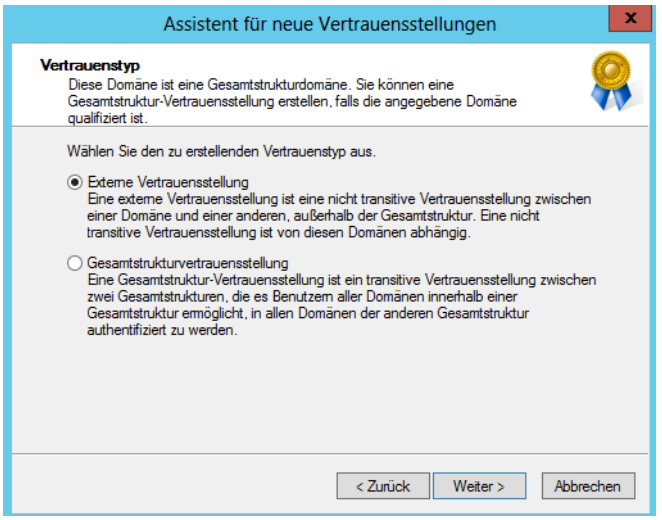


Einrichtung einer Vertrauensstellung

Wenn Sie eine Vertrauensstellung zu einer externen Domäne erstellen wollen, sollten Sie zunächst sicherstellen, dass die Namensauflösung zwischen den Domänen fehlerfrei funktioniert (siehe Kapitel 13). Erst wenn die Namensauflösung stabil und zuverlässig funktioniert, sollten Sie die Vertrauensstellung einrichten.

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. Bestätigen Sie das Fenster und geben Sie auf der zweiten Seite den Namen der Domäne an, zu der Sie eine Vertrauensstellung einrichten wollen.
4. Wenn Sie eine Vertrauensstellung zu einer Active Directory-Domäne aufbauen wollen, verwenden Sie am besten den DNS-Namen. Wählen Sie als Nächstes die Art der Vertrauensstellung aus.

Abbildg. 17.4 Auswählen der Art der Vertrauensstellung



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 eine vollständige Kerberos-Integration zwischen Gesamtstrukturen bieten, und zwar bidirektional und transitiv.

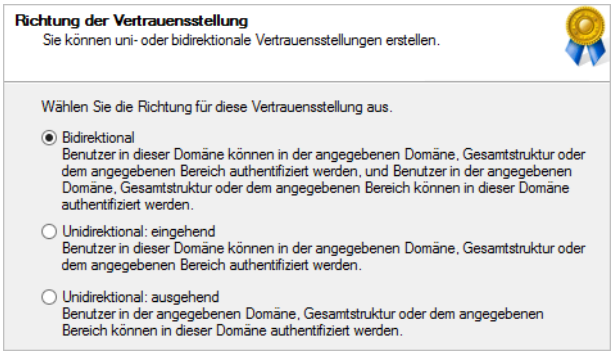
Für die Gesamtstruktur-übergreifende Vertrauensstellungen müssen einige Voraussetzungen geschaffen werden:

- Gesamtstruktur-übergreifende Vertrauensstellungen werden nur in Windows Server 2008/2008 R2/2012/2012 R2-Gesamtstrukturen unterstützt
- Stellen Sie sicher, dass sich die Domänenfunktionsebene und die Gesamtstrukturfunktionsebene zumindest im Windows Server 2008 R2-Modus befinden
- 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 (siehe Kapitel 13). 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.

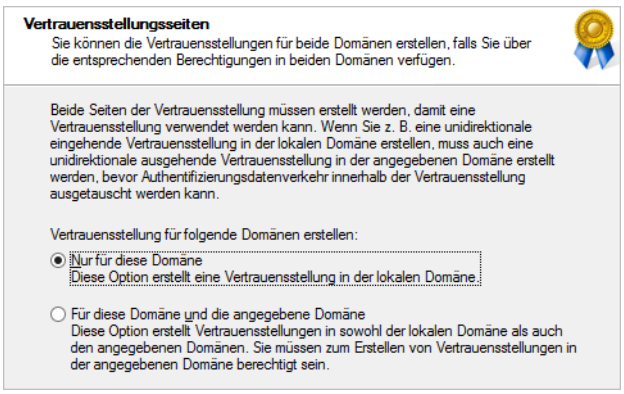
- **Bidirektional** In diesem Fall können sich die Anwender beider Domänen in der jeweils anderen Domäne authentifizieren
- **Unidirektional: eingehend** Bei dieser Variante legen Sie fest, dass es sich bei dieser Domäne um die vertraute Domäne der Vertrauensstellung handelt. In diesem Fall können sich 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. 17.5 Festlegen der Richtung von Vertrauensstellungen



Im nächsten Fenster können Sie bei *Gesamtstrukturvertrauensstellung* auswählen, ob Sie auch gleich die Vertrauensstellung in der anderen Domäne der anderen Gesamtstruktur erstellen wollen.

Abbildg. 17.6 Auswählen, ob die Gesamtstrukturvertrauensstellung in beiden Domänen eingerichtet werden soll



Im nächsten Fenster legen Sie den Bereich der Authentifizierung der Vertrauensstellung fest. Die meisten Administratoren verwenden hier die Option *Ausgewählte 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.

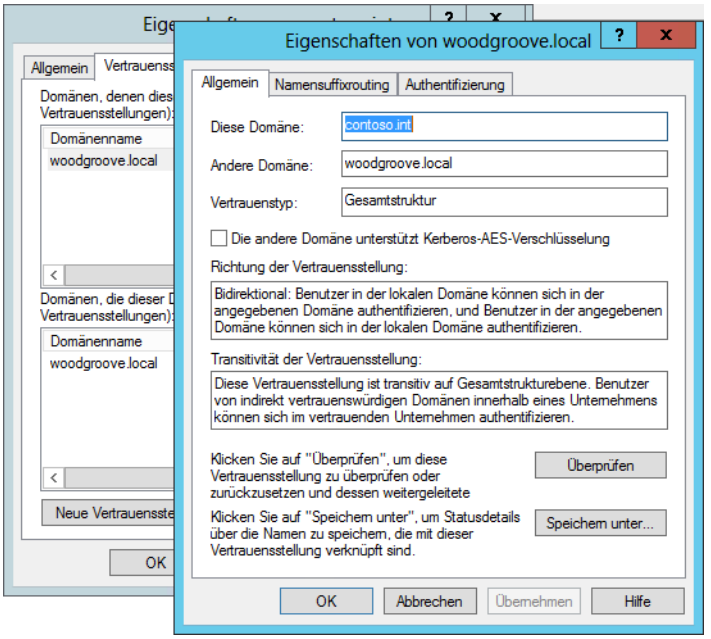
Wenn Sie die Variante *Ausgewählte Authentifizierung* auswählen, müssen Sie für jeden Server, auf den die Anwender der anderen Domäne zugreifen dürfen, in den Sicherheitseinstellungen die Option *Darf authentifizieren* aktivieren. Durch diese Einstellung erhöhen Sie zwar die Sicherheit auf der anderen 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. 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 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 erneut in der anderen Domäne authentifizieren.

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 *Namensuffixrouting* verwenden.

Abbildg. 17.7 Konfigurieren des Namensuffixroutings für eine Gesamtstrukturvertrauensstellung



Automatisch aktivierte SID-Filterung

Der SID-Filter wird automatisch aktiviert, wenn eine Vertrauensstellung zu einer externen Domäne eingerichtet wird. Mit der SID-Filterung werden ausgehende Vertrauensstellungen gesichert. Dadurch 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 ist, könnte ein außenstehender Benutzer, der Administratorrechte 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 Administratorrechten 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. Wenn Sie für Ressourcen in der vertrauenden Domäne Berechtigungen für eine universale Gruppe aus 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 Befehlszeilentool Netdom. Um die SID-Filterung zu deaktivieren, geben Sie in der Eingabeaufforderung den folgenden Befehl ein:

```
netdom trust <VertrauendeDomäne> /domain:<VertrauteDomäne> /quarantine:no /
userD:<Domänenadministrator> /passwordD:<KennwortDesDomänenAdministrators>
```

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: <KennwortDesDomänenAdministrators>
```

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Vertrauensstellungen innerhalb einer Active Directory-Gesamtstruktur einrichten, um die Leistung zu verbessern, aber auch Vertrauensstellungen zwischen Gesamtstrukturen einrichten, was vor allem bei Migrationen eine wichtige Rolle spielt.

Im nächsten Kapitel widmen wir uns der Benutzerverwaltung in Active Directory und der verschiedenen Möglichkeiten der Benutzerprofile in Windows 7/8/8.1 und Windows Server 2008 R2/2012/2012 R2.

Kapitel 18

Benutzerverwaltung und Profile

In diesem Kapitel:

In diesem Kapitel erfahren Sie, wie Benutzer in Active Directory und auf lokalen Servern verwaltet werden. Außerdem gehen wir darauf ein, wie Sie Benutzerprofile in Active Directory und auf Clients mit Windows 7/8/8.1 verwalten. Wir zeigen Ihnen in diesem Kapitel auch die User Environment Virtualization (UE-V), den Nachfolger der Benutzerprofile in Windows Server 2012/2012 R2 und Windows 8/8.1. Außerdem erfahren Sie, wie Benutzer mit dem Active Directory-Verwaltungscenter administriert werden. Mehr dazu lesen Sie auch in den vorangegangenen Kapiteln.

Die Verwaltung von Benutzern einer Domäne findet meistens mit dem Snap-In *Active Directory-Benutzer und -Computer* statt. Lokale Benutzerkonten verwalten Sie über den lokalen Benutzer-Manager, den Sie über *lusrmgr.msc* auf der Startseite starten. Um Kennwörter zurückzusetzen oder routinemäßige Aufgaben wie das Anlegen von Benutzern durchzuführen, verwenden Sie auch das neue Active Directory-Verwaltungscenter.

Grundlagen der Verwaltung von Benutzern

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 in Active Directory. Diese Gruppen befinden sich im Container *Users*. 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 in 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 Rootdomäne.
- **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, 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 innerhalb der Gesamtstruktur eingerichteten Domäne definiert. Andere Gruppen erstellt Windows Server 2012 R2 erst nach der Installation bestimmter Dienste wie DNS und DHCP. Wir gehen nachfolgend ausführlicher auf diese Gruppen ein.

Vor allem in Gesamtstrukturen sind diese Standardgruppen in der Rootdomäne besonders wichtig:

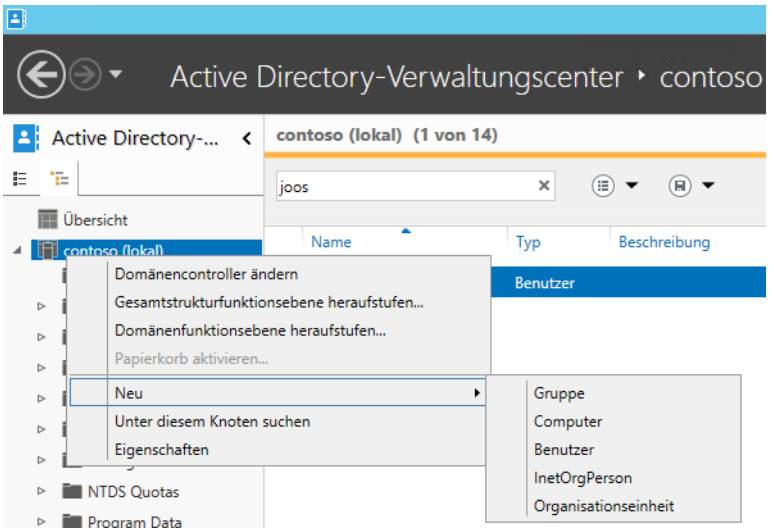
- **DHCP-Administratoren** Dürfen DHCP-Server in der Domäne verwalten. Die Gruppe wird nach der Installation des ersten DHCP-Servers auf einem Domänencontroller der Domäne erstellt.
- **DHCP-Benutzer** Enthält Benutzerkonten, die lesend auf die Informationen des DHCP-Diensts zugreifen, aber keine Änderungen 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.
- **DnsAdmins** Diese Gruppe 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 in Active Directory verwaltet.
- **DnsUpdateProxy** In dieser Gruppe 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.
- **Richtlinien-Ersteller-Besitzer** Diese Gruppe umfasst die Anwender, die Gruppenrichtlinien für die Domäne erstellen dürfen. Das können Administratoren sein, die sich nur um diese Aufgabe in der Gesamtstruktur kümmern.
- **WINS Users** Diese Gruppe 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.

Die Gruppen *DnsUpdateProxy, Organisations-Admins, Schema-Admins* und *DnsAdmins* werden in der ersten Domäne, die in einer Gesamtstruktur eingerichtet wird, definiert. Dies 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, klicken Sie im ersten Schritt mit der rechten Maustaste auf die Organisationseinheit (Organizational Unit, OU). Im Kontextmenü dieses Containers wählen Sie im Untermenü *Neu* den Befehl *Benutzer* aus. Alternativ verwenden Sie auch das Active Directory-Verwaltungscenter.

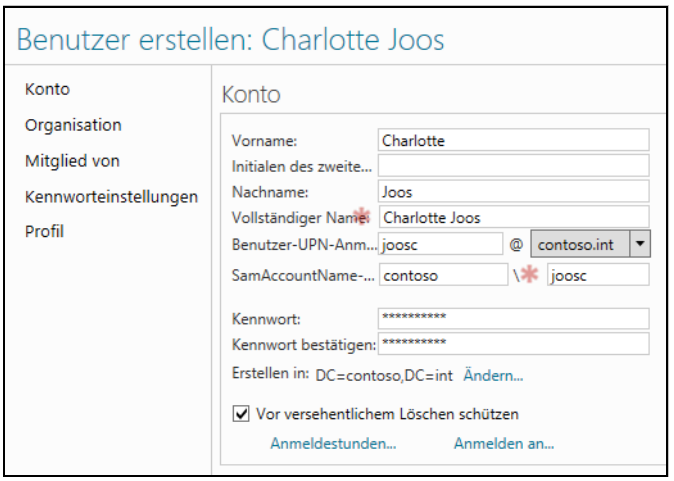
Abbildg. 18.1 Anlegen neuer Objekte im Active Directory-Verwaltungscenter



Im ersten Dialogfeld legen Sie die Namensinformationen für diesen Benutzer fest, wenn Sie *Active Directory-Benutzer und -Computer* verwenden. Im Active Directory-Verwaltungscenter finden Sie alles auf einer Seite. Mit dem kleinen Pfeil können Sie einzelne Optionen ein- und ausblenden lassen. Hier können der Vorname, ein oder mehrere Mittelinitialen und der Nachname angegeben werden.

Der Benutzeranmeldename legen Sie als DNS-Name für Windows Server 2012 R2 (*joost@contoso.int*) und als NetBIOS-kompatibler Name (*contoso\joost*) fest. Meist 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 darf aber mehrere Benutzer mit dem gleichen Benutzernamen in unterschiedlichen Domänen der Gesamtstruktur geben, da sich hier der Name schon durch die verschiedenen Domänen unterscheidet.

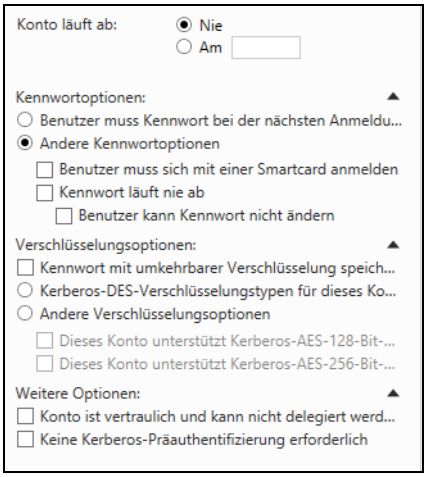
Abbildg. 18.2 Erstellen eines neuen Benutzerkontos unter Windows Server 2012 R2



Durch Auswahl der Schaltfläche *Weiter* wechseln Sie zur zweiten Seite des Assistenten, wenn Sie *Active Directory-Benutzer und -Computer* verwenden. Falls Sie den Benutzer im Active Directory-Verwaltungscenter anlegen, nehmen Sie alle Einstellungen auf der ersten Seite des Assistenten vor. Wichtig sind noch folgende Optionen, unabhängig davon, ob Sie *Active Directory-Benutzer und -Computer* oder das Active Directory-Verwaltungscenter verwenden:

- 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.
- *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
- Durch das Kontrollkästchen *Konto ist deaktiviert* in *Active Directory-Benutzer und -Computer* 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.

Abbildg. 18.3 Verwalten der Kennworteinstellungen



Zum Anlegen sind keine weiteren Einstellungen möglich. Sie können ohnehin nach dem Anlegen eines Benutzers alle weiteren Einstellungen nachträglich anpassen. Auch hier können Sie das Snap-In *Active Directory-Benutzer und -Computer* oder das Active Directory-Verwaltungscenter einsetzen.

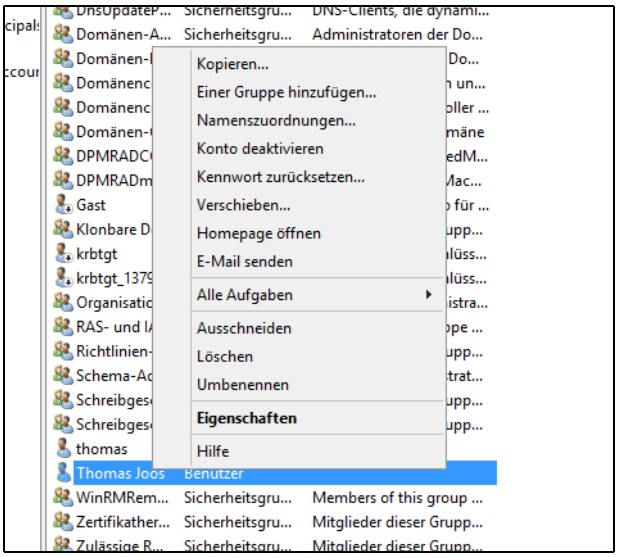
Verwalten von Benutzerkonten

Im Kontextmenü eines angelegten Benutzers in *Active Directory-Benutzer und -Computer* steht Ihnen eine Reihe von Möglichkeiten zur Verfügung. Auf diese gehen wir nachfolgend ein. Viele Einstellungen erreichen Sie auch über das Active Directory-Verwaltungscenter.

- Mit dem Befehl *Kopieren* können Sie die meisten Einstellungen dieses Benutzerkontos in ein neues Konto übernehmen. Die Einstellungen für den Benutzernamen und das 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. 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* lässt sich ein Dialogfeld öffnen, 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 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. Haben Sie den Active Directory-Papierkorb aktiviert (siehe Kapitel 12), können Sie das Objekt mit dem Active Directory-Verwaltungscenter wiederherstellen. Durch das Anlegen eines Benutzers mit gleichem Namen erzeugen Sie nicht das gleiche Benutzerkonto, da sich die SID ändert. Die Wiederherstellung muss in diesem Fall über den Active Directory-Papierkorb ablaufen.

Im Active Directory-Verwaltungscenter stehen an dieser Stelle weniger Optionen zur Verfügung, da hier nur die wichtigsten Befehle notwendig sind. Häufige Aufgaben finden Sie hier auch gleich auf der Startseite, zum Beispiel das Zurücksetzen von Benutzerkennwörtern.

Abbildg. 18.4 Kontextmenü von Benutzerkonten



Die meisten Informationen liefert der Befehl *Eigenschaften* im Kontextmenü. Damit können Sie im Snap-In auf ein Dialogfeld zugreifen, in dem Sie über eine Vielzahl von Registerkarten die Eigenschaften von Benutzern anpassen können. Im Active Directory-Verwaltungscenter erhalten Sie die gleiche formularbasierte Ansicht wie beim Anlegen. Über die Kategorie *Erweiterungen* zeigt aber auch das Active Directory-Verwaltungscenter die fehlenden Registerkarten an. Auch hier lassen sich wieder einzelne Bereiche ein- und ausblenden. Rufen Sie im Snap-In *Active Directory-Benutzer und -Computer* zuvor den Menübefehl *Ansicht/Erweiterte Features* auf, damit alle Registerkarten angezeigt werden:

- Auf der Registerkarte *Allgemein* befinden sich unter anderem die Informationen zum vollständigen Namen des Benutzers, die Sie beim Anlegen des Benutzerkontos eingegeben haben
- Auf der Registerkarte *Konto* werden die Einstellungen für Kennwörter und Anmeldenamen verwaltet:
  - **Anmeldezeiten** Mit dieser Schaltfläche öffnen Sie ein Dialogfeld, in dem Sie die Zeiten festlegen, zu denen sich ein Benutzer anmelden darf
  - **Anmelden an** Über diese Schaltfläche wählen Sie Computer aus, an denen sich der Anwender anmelden darf
  - **Kontosperrung aufheben** Dieses Kontrollkästchen wählen Sie, nachdem ein Konto gesperrt wurde. Die Situationen, in denen ein Konto gesperrt werden soll, können Sie in den Gruppenrichtlinien konfigurieren (siehe Kapitel 19).
  - **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

- **Kennwort mit umkehrbarer Verschlüsselung speichern** Führt dazu, dass Administratoren die Kennwörter auslesen können
- **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 zur 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.
- **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. Das gilt auch für das Festlegen des maximalen Verschlüsselungszustands in den nachfolgenden beiden Punkten.
- **Keine Kerberos-Präauthentifizierung erforderlich** Laut dem Kerberos-Standard ist die TGT-Anforderung des Clients ein unverschlüsseltes Paket, da es keine sicherheitssensiblen Daten enthält. Bei Verwendung der Kerberos-Präauthentifizierung ist dieses Paket bereits mit dem privaten Schlüssel des Benutzers/Anforderers verschlüsselt. Für die Interoperabilität mit anderen Kerberos-Implementierungen kann diese Präauthentifizierung deaktiviert werden.

Zusätzlich legen Sie im unteren Bereich ein Ablaufdatum für das Konto fest. Die Registerkarte *Mitglied von* zeigt eine Liste der Gruppen an, in denen der Benutzer Mitglied ist.

Über die Registerkarte *Einwählen* können Sie die RAS-Berechtigungen für diesen Benutzer konfigurieren. Eine weitere interessante Registerkarte bei den Eigenschaften eines Benutzers ist *Objekt*. 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 in 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. Auf dieser Registerkarte können Sie auch konfigurieren, dass das Objekt nicht gelöscht werden kann.

Benutzerverwaltung für Remotedesktopbenutzer

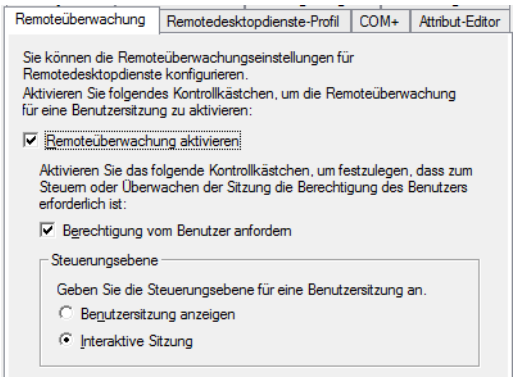
In den Eigenschaften eines Benutzers stehen Ihnen mehrere Registerkarten zur Verfügung, auf denen Sie die Eigenschaften des Benutzerkontos für die Anmeldung auf Remotedesktopserver (siehe auch Kapitel 28) speziell anpassen können:

- *Umgebung*
- *Sitzungen*
- *Remoteüberwachung*
- *Remotedesktopdienste-Profil*

Auf der Registerkarte *Remoteüberwachung* legen Sie fest, ob dieser Benutzer von Administratoren gespiegelt werden kann und mit welchen Optionen das möglich ist. Hier legen Sie auch fest, ob sich

Administratoren ohne Bestätigung durch den Benutzer auf die Sitzung spiegeln können. Die Einstellungen in den Benutzerkonten haben nur für diesen Benutzer Gültigkeit.

Abbildg. 18.5 Konfigurieren der Remoteüberwachung für ein Benutzerkonto



Auf der Registerkarte *Remotedesktopdienste-Profil* 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. Hier bestimmen Sie auch, ob sich ein Benutzer überhaupt auf einem Remotedesktop anmelden darf. Zu den servergespeicherten Profilen kommen wir noch in den nächsten Abschnitten zurück.

Die Registerkarten *Umgebung* und *Sitzungen* entsprechen den entsprechenden Einstellungen für das Remotedesktopprotokoll in der Konfiguration der Remotedesktopdienste. Wenn der Remotedesktop 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 Remotedesktop verändern.

Benutzerprofile und User Experience Virtualization (UE-V)

Um einen Windows 8/8.1-Computer in Windows Server 2012 R2-Active Directory zu integrieren, rufen Sie zunächst die Verwaltung der Netzwerkverbindungen auf. Am schnellsten geht das, wenn Sie auf der Startseite nach *ncpa.cpl* suchen. Alternativ rufen Sie das Netzwerk- und Freigabecenter über das Kontextmenü der Netzwerkverbindung auf dem Desktop auf und klicken auf *Adaptereinstellungen ändern*.

Ändern Sie die IP-Einstellungen so ab, dass der Client einen DNS-Server in der Active Directory-Struktur verwendet. Um die Verbindung zu testen, öffnen Sie eine Eingabeaufforderung auf dem

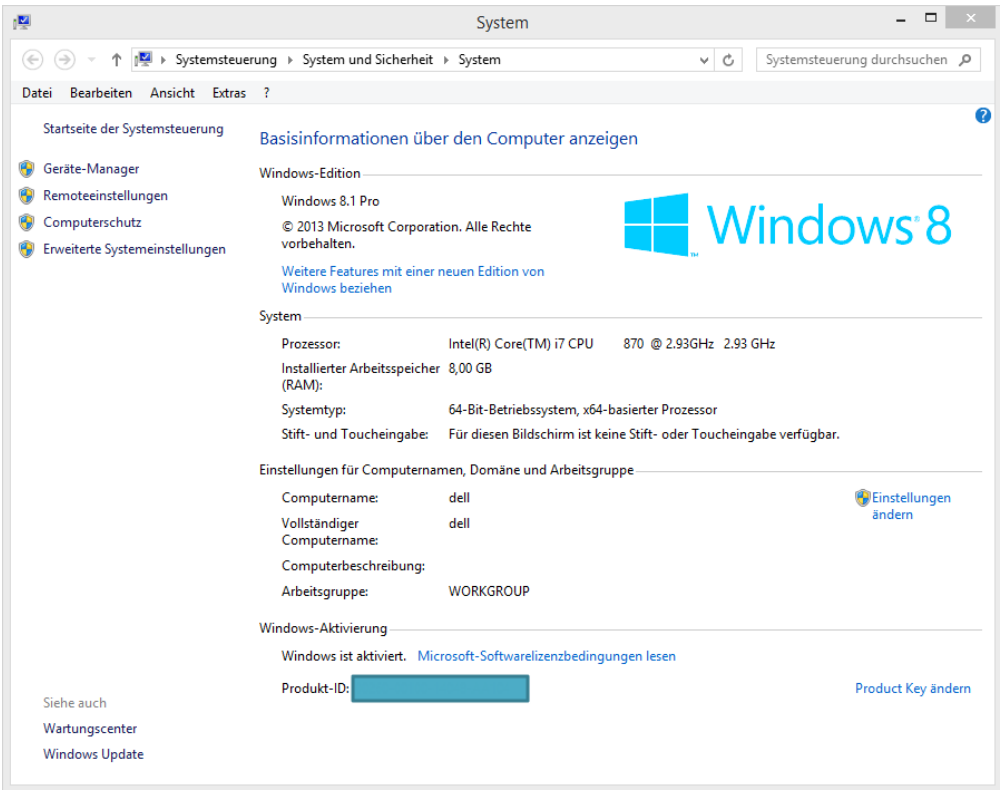
Client und geben *nslookup <FQDN des Domänencontrollers>* ein. Lassen Sie anschließend den Client noch den Domänencontroller anpingen.

Rufen Sie anschließend die Startseite auf, indem Sie die ⊞-Taste betätigen. Suchen Sie nach *Computer* und klicken Sie das angezeigte Symbol mit der rechten Maustaste an. Wählen Sie unten in der App-Leiste den Befehl *Eigenschaften* aus, um das *System*-Fenster zu öffnen.

TIPP Ganz schnell können Sie das *System*-Fenster über die Tastenkombination ⊞ + Pause aufrufen.

Klicken Sie anschließend bei *Einstellungen für Computernamen, Domäne und Arbeitsgruppe* auf den Link *Einstellungen ändern*.

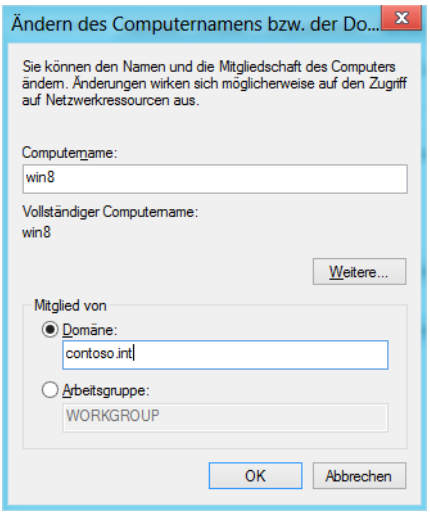
Abbildg. 18.6 Aufrufen der Eigenschaften des Computers



Klicken Sie anschließend auf der Registerkarte *Computername* auf *Ändern*. Geben Sie bei *Computername* den Namen des Computers ein, den er später in der Domäne erhalten soll. Aktivieren Sie dann unter *Mitglied von* die Option *Domäne* und tragen Sie den DNS-Namen der Domäne ein, welcher der Client beitreten soll.

Als Letztes müssen Sie sich noch an der Domäne authentifizieren. Bei erfolgreicher Eingabe wird der PC in die Domäne aufgenommen. Wie bei den Vorgängerversionen müssen Sie auch unter Windows 8/8.1 den Computer nach der Domänenaufnahme neu starten.

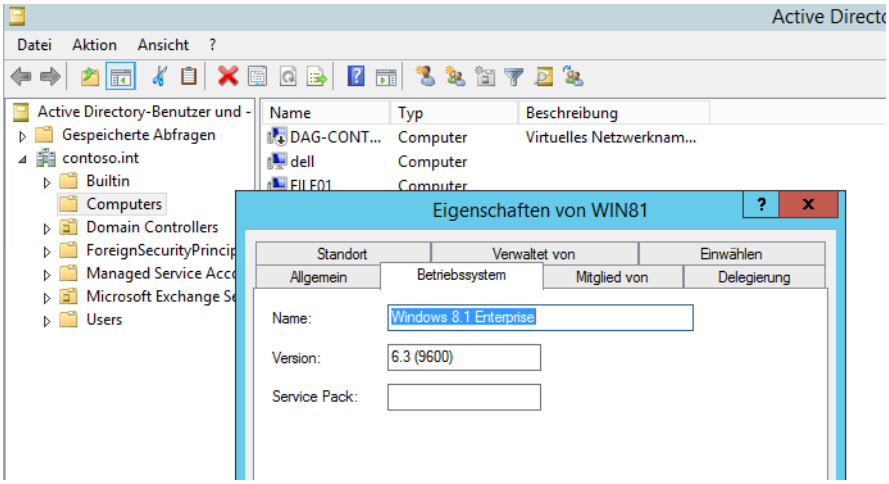
Abbildg. 18.7 Beitreten einer Domäne mit Windows 8/8.1



Haben Sie den Computer nach der Domänenaufnahme neu gestartet, melden Sie sich mit einem Benutzernamen an der Domäne an.

Auf dem Domänencontroller öffnen Sie in Windows Server 2012 R2 den Server-Manager und rufen dann über das Menü *Tools* das Snap-In *Active Directory-Benutzer und -Computer* auf. Hier sehen Sie in der OU *Computers* den neuen PC und können über das Kontextmenü dessen Eigenschaften aufrufen. Auf der Registerkarte *Betriebssystem* sehen Sie die Windows 8/8.1-Edition.

Abbildg. 18.8 Überprüfen der Domänenmitgliedschaft eines Windows 8/8.1-PCs



Um sich über den Windows 8/8.1-PC an Windows Server 2012 R2 anzumelden, klicken Sie auf *Anderer Benutzer*. Geben Sie bei der ersten Anmeldung den Benutzernamen in der Syntax *<NetBIOS-Name der Domäne>\<Benutzernamen>* ein, wenn es den gleichen Benutzernamen auch auf

dem lokalen PC gibt. Ist der Anmeldename in der Domäne auf dem PC nicht vorhanden, reicht auch die Anmeldung über den Benutzernamen.

Abbildg. 18.9 Anmelden von Windows 8/8.1 an Active Directory mit Windows Server 2012 R2

Den Sperrbildschirm, der unter Windows 8/8.1 vor der Anmeldeseite angezeigt wird, müssen Sie nicht mit der Maus wegschieben. Es reicht aus, wenn Sie eine Taste drücken, damit dieser verschwindet. Öffnen Sie nach der Anmeldung an der Domäne das Netzwerk- und Freigabecenter auf dem Desktop, sehen Sie ebenfalls den Domänenstatus des PC. Sie können auch einfach auf das Netzwerksymbol klicken, um den Domänenstatus anzuzeigen.

Benutzerprofile lokal und im Profieinsatz verstehen

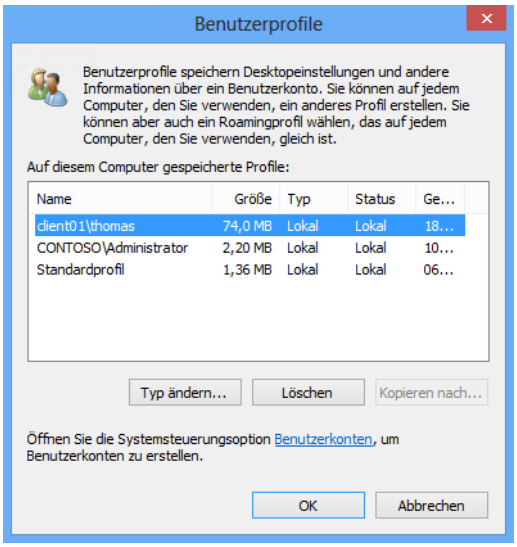
Alle persönlichen Einstellungen der einzelnen Benutzer auf einem Computer speichert Windows in einem Benutzerprofil. Dieses Profil ist ein Ordner mit dem Namen des Benutzers im Ordner *C:\Benutzer* beziehungsweise *C:\Users*. Dieser Ordner ist neu in Windows Vista und Windows 7 sowie Windows Server 2008/2008 R2. Microsoft hat diese Vorgehensweise in Windows 8/8.1 beibehalten und mit Zusatztools wie die User Environment Virtualization (UE-V) verbessert.

Unter Windows XP hatte dieser Ordner noch die Bezeichnung *C:\Dokumente und Einstellungen*. Wenn Sie ein Profil löschen, erstellt Windows dieses neu, sobald sich der Benutzer erneut am Computer anmeldet. Alle Einstellungen des Benutzers werden beim Löschen zurückgesetzt, das Profil wird neu erstellt und ist entsprechend vollkommen leer. Beachten Sie aber, dass beim Löschen eines Profils alle Daten des jeweiligen Benutzers verloren gehen. Sie sollten diese daher vorher möglichst sichern. Ausnahme ist, wenn Sie die Ordner im Profil über Gruppenrichtlinien umleiten.

Verwaltung von Benutzerprofilen

Über den Link *Erweiterte Benutzerprofileigenschaften konfigurieren* im Fenster *Benutzerkonten* der Systemsteuerung (*Systemsteuerung/Benutzerkonten und Family Safety/Benutzerkonten*) können Sie sich alle Benutzerprofile auf einem PC unter Windows 8/8.1 anzeigen lassen und diese verwalten. Sie sehen an dieser Stelle auch die Größe des jeweiligen Profils. Im Ordner auf der Festplatte des Profils befinden sich mehrere Unterordner. Die persönlichen Daten jedes Benutzers liegen in seinem eigenen Ordner, auf den nur er selbst sowie die Administratoren Zugriff haben.

Abbildg. 18.10 Verwalten der Benutzerprofile unter Windows 8/8.1



Die Benutzerprofile erstellt Windows zunächst als Kopie des Standardprofils, des Default Users. Zusätzlich gibt es einen Ordner *All Users*. 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 Ordner angezeigt werden, müssen Sie die versteckten Dateien einblenden lassen.

In Windows 8/8.1 öffnen Sie dazu im Menüband des Explorers die Registerkarte *Ansicht*. Klicken Sie anschließend auf *Optionen/Ordner- und Suchoptionen ändern*. Auf der Registerkarte *Ansicht* können Sie anschließend versteckte Dateien anzeigen lassen. Sie können die Aktivierung auch über Kontrollkästchen auf der Registerkarte *Ansicht* durchführen.

Ordnerstruktur von Profilen

Zur Abwärtskompatibilität hat Microsoft zusätzlich einige Verknüpfungen eingefügt, die in den vorangegangen Windows-Versionen noch verwendet wurden oder die direkt auf einen anderen Ordner verweisen.

Folgende Ordner spielen dabei eine wesentliche Rolle. Achten Sie aber darauf, dass einige Ordner standardmäßig im Explorer ausgeblendet sind. Sie müssen zunächst die versteckten Dateien aktivieren:

- **Desktop** Symbole und Einstellungen des Benutzerdesktops
- **Eigene Dokumente** Standardmäßiger Speicherort aller persönlicher Dateien eines Benutzers
- **Downloads** Speicherort aller Downloads
- **Favoriten** Favoriten des Internet Explorers
- **Eigene Musik** Ablageort von Musikdateien

- **Eigene Videos** Ablageort für gespeicherte Filmdateien
- **Eigene Bilder** Ablageort für Bilddateien und Grafiken
- **Suchvorgänge** Ablageort für abgespeicherte Suchen
- **AppData** Ablageort für benutzerspezifische Daten und Systemdateien von Applikationen. Diesen Ordner sehen Sie nur, wenn Sie in den Explorer-Optionen die versteckten Dateien anzeigen lassen.
- **Gespeicherte Spiele** Zentraler Ablageort für Spielstände von kompatiblen Windows-Spielen
- **Links** Hierbei handelt es sich um die Favoriten im Windows-Explorer

Neben den Ordnern findet sich im Profilpfad die Datei *NTUSER.DAT*. Diese enthält die Einstellungen der Registry, die sich dort unter *HKEY_CURRENT_USER (HKLM)* finden. Die gesamten benutzerspezifischen Einstellungen sind hier enthalten. Sie müssen dazu die versteckten und geschützten Systemdateien einblenden lassen. Sie finden diese Möglichkeit auf der Registerkarte *Ansicht* im Explorer nach einem Klick auf *Optionen/Ordner- und Suchoptionen ändern*.

Zur Vereinheitlichung von anwendungsspezifischen Daten hat Microsoft den Ordner *AppData* im Benutzerprofil eingeführt. Dieser Ordner enthält die drei Unterordner:

- *Local*
- *LocalLow*
- *Roaming*

In den beiden Ordnern *Local* und *LocalLow* speichert Windows Daten von Anwendungen, die nicht mit dem Benutzer bei der Verwendung von verschiedenen Arbeitsstationen mitwandern.

Hier handelt es sich vor allem um Daten auf dem lokalen Computer. Der Ordner *Local* ist identisch mit dem Ordner *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 mitwandern. Dieser Ordner entspricht dem Ordner *C:\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten* in Windows XP.

Unter den Windows-Versionen vor Windows Vista und Windows 7 hat der Ordner *All Users* die Inhalte zur Verfügung gestellt, die für alle Anwender auf dem PC gegolten haben. So war es möglich, durch Bearbeitung eines einzelnen Ordners die Einstellungen aller Benutzer anzupassen. Beispiel für den Einsatz von *All Users* war das Startmenü oder der Inhalt des Desktops, der sich immer aus dem eigenen Benutzerprofil und dem Inhalt des Ordners *All Users* zusammensetzte.

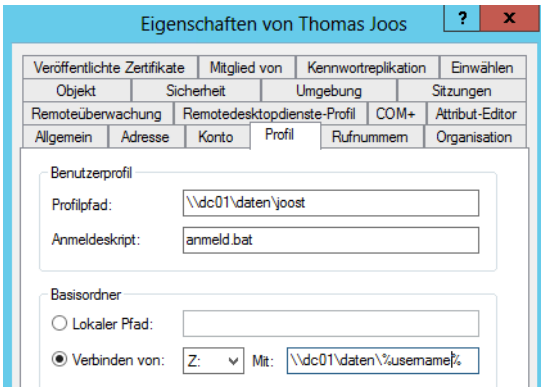
Hatten Sie eine Verknüpfung in den Ordner *\All Users\Startmenü* kopiert, wurden diese bei allen Benutzern des PCs im Startmenü angezeigt. In Windows 8/8.1 ist der Ordner *C:\Users\All Users* nur noch als Verknüpfung vorhanden, die auf den Ordner *C:\ProgramData* verweist. Hier wird wiederum auf das Profil *Öffentlich* unter *C:\Users* verlinkt.

Wie bei den Vorgängerversionen legt Windows 8/8.1 automatisch ein neues Profil an, wenn sich Benutzer das erste Mal am PC anmelden.

Servergespeicherte Profile für Benutzer in Active Directory festlegen

Auf der Registerkarte *Profil* eines Benutzerkontos im Snap-In *Active Directory-Benutzer und -Computer* können Sie die notwendigen Angaben hinterlegen, um komplette Profile auf den Server auszulagern.

Abbildg. 18.11 Anzeigen der Profileigenschaften im Snap-In *Active Directory-Benutzer und -Computer*



Um servergespeicherte Profile für Anwender festzulegen, rufen Sie die Eigenschaften des Benutzerkontos auf und wechseln zur Registerkarte *Profile*. Bei *Profilpfad* geben Sie den Ordner an, in den Windows das Benutzerprofil des Anwenders beim Abmelden speichern und beim Anmelden laden soll.

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*%.

Der Profilpfad verweist auf den Ordner, in dem das Benutzerprofil des Anwenders abgelegt ist. Haben Sie keinen Pfad angegeben, arbeitet Windows nur mit lokalen Benutzerprofilen. Wenn sich ein Benutzer anmeldet, überprüft Windows, ob für diesen Benutzer ein Profilpfad angegeben und damit ein serverbasierendes Profil definiert ist. Ist dies der Fall, vergleicht Windows, ob das serverbasierende oder das lokale Profil aktueller ist. Ist das serverbasierende Profil aktueller, lädt Windows die geänderten Dateien aus diesem Profil auf das lokale System.

Achten Sie aber darauf, dass die Gruppe *Jeder* – oder eine Sicherheitsgruppe, in der sich die Benutzer befinden – das Recht haben muss, Ordner in der Freigabe für die Profile zu erstellen und in die Ordner zu schreiben.

Bei der Abmeldung aktualisiert Windows das serverbasierende Profil durch die lokal veränderten Dateien. Bei der ersten Anmeldung eines Benutzers nach der Definition eines Profilpfads lädt Windows entweder ein vordefiniertes Profil vom Server oder kopiert bei der Abmeldung das bisherige lokale Profil des Benutzers auf den Server.

Die zweite Einstellung bezieht sich auf das Anmeldeskript. Hier können Sie angeben, dass Windows ein Programm ausführen soll, wenn sich ein Benutzer anmeldet. In den meisten Fällen handelt es

sich um eine Batchdatei oder ein VB-Skript. Diese Einstellung ist nicht mehr erforderlich, da Skripts für die An- und Abmeldung von Benutzern über die Gruppenrichtlinien konfiguriert werden können. Mehr dazu lesen Sie im nächsten Kapitel.

Der Basisordner gibt an, welches Netzwerklaufwerk für den Benutzer automatisch verbunden werden soll.

Auf der Registerkarte *Remotedesktopdienste-Profil* können Sie angeben, ob ein Benutzer auf einem Remotedesktopserver ein zusätzliches Profil bekommt. Die Einstellung des Profilpfads erlaubt die Verwendung eines zweiten Benutzerprofils ausschließlich für die Nutzung mit dem Remotedesktop. Beim Verwenden von gleichen Profilen auf den Arbeitsstationen und dem Remotedesktop können sich Konflikte ergeben, wenn für die Remotedesktop kein eigenes Profil verwendet wird.

Verbindliche Profile (Mandatory Profiles)

Windows unterscheidet zwischen persönlichen und verbindlichen Profilen. Ein persönliches Profil kann nur einem Benutzer zugeordnet sein und dient diesem als Ausgangsposition. Die Anpassungen, die er vornimmt, speichert Windows in diesem Profil. Ein Benutzer, dem ein verbindliches Profil zugeordnet ist, 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 der Datei *Ntuser.dat* in *Ntuser.man*.

Verbindliche Profile können mehrere Anwendern gemeinsam verwenden. Dazu geben Sie für alle Anwender den gleichen Benutzerprofilpfad an. Sie müssen nur einen Ordner auf dem Server erstellen, in dem Sie das Profil speichern. Falls sich ein Benutzer zum ersten Mal anmeldet, lädt der Client das Profil vom Server. Bei der Abmeldung des Benutzers aktualisiert Windows das Profil auf dem Server, wenn es sich um normale servergespeicherte Profile handelt. Bei der Verwendung von verbindlichen Profilen erfolgt keine Aktualisierung des serverbasierenden Profils. Bei der nächsten Anmeldung vergleicht Windows die Daten für das lokale Profil und für das auf dem Server gespeicherte Profil. Das aktuellere der beiden Profile wird geladen.

Verwenden Sie ein verbindliches Profil, lädt Windows dieses immer automatisch. Ein verbindliches Profil wird also bei jeder Anmeldung geladen. Ist der Server, auf dem das Profil gespeichert ist, nicht verfügbar, verwendet Windows eine lokal zwischengespeicherte Kopie des Profils. Wenn sich ein Benutzer an einer anderen Arbeitsstation anmeldet, wird bei der Anmeldung über den Eintrag für den Benutzerprofilpfad bei den Eigenschaften des Benutzers im Snap-In *Active Directory-Benutzer und -Computer* erkannt, dass dieser Benutzer über ein Benutzerprofil verfügt. Ändern Sie die Bezeichnung der Datei *Ntuser.man* wieder in *Ntuser.dat* ab, darf der Anwender wieder Änderungen vornehmen.

Eine weitere Steigerung von verbindlichen Profilen sind superverbindliche Profile (Super Mandatory Profiles). 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 PC keine Verbindung zum Server herstellen kann, wird die Anmeldung verweigert. Um ein solches verbindliches Profil zu erstellen, gehen Sie zunächst genauso vor wie beim Anlegen eines verbindlichen Profils. Ändern Sie den Namen des Benutzerprofilordners so ab, dass dieser Ordner der Syntax *<Profilname>.man.v2* entspricht. Fügen Sie auf der Registerkarte *Profil* in Active Directory hinter den Pfad des Benutzerprofils noch die Endung *.man* hinzu, diesmal ohne das *v2*.

Durch diese Aktion wurde aus dem verbindlichen Profil mit der Datei *Ntuser.man* ein superverbindliches Profil, bei dem auch der Ordner des Profils die Endung *.man.v2* hat.

Erstellen eines Default-Netzwerkbenutzerprofils

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 oder Windows 7/8 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 Domänenadminkonto an.
5. Erstellen Sie in der NETLOGON-Freigabe auf einem Domänencontroller den neuen Ordner *Default User.v2*. Das *v2* definiert das Profil, welches nur für Windows Vista und Windows 7/8-PCs verwendet wird.
6. Klicken Sie auf dem PC mit der rechten Maustaste auf *Computer* im Startmenü und rufen Sie den Befehl *Eigenschaften* auf.

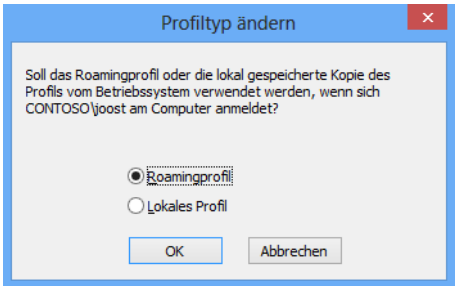
   In Windows 8/8.1 öffnen Sie auf dem Desktop ein Explorer-Fenster und klicken im Navigationsbereich auf *Computer*. Alternativ können Sie auch einfach die Tastenkombination ⊞ + Pause drücken.
7. Klicken Sie links im Fenster auf den Link *Erweiterte Systemeinstellungen*.
8. Klicken Sie im Bereich *Benutzerprofile* auf *Einstellungen*.
9. Markieren Sie den Benutzer, dessen Profil Sie als Standard definieren wollen, und klicken Sie auf *Kopieren nach*. Ist die Option für das jeweilige Profil nicht aktiv, dann kopieren Sie den Inhalt des Ordners über den Explorer in das Default-Profil auf dem Server. Achten Sie aber darauf, die versteckten Dateien zu aktivieren, genauso wie die geschützten Systemdateien. Bearbeiten Sie anschließend die Sicherheitseigenschaften des Ordners auf dem Server und weisen Sie der Gruppe *Jeder* das Recht *Ändern* für das Profil zu. Um Manipulationen des Profils zu vermeiden, können Sie auch eine Sicherheitskopie erstellen, mit der Sie das Profil wiederherstellen können, wenn das notwendig ist. Die NETLOGON-Freigabe befindet sich auf dem Domänencontroller im Ordner *C:\Windows\SYSVOL\sysvol\contoso.com\scripts*.
10. Geben Sie den Pfad zum *Default User*-Ordner in der NETLOGON-Freigabe an, welches Sie zuvor angelegt haben, zum Beispiel *\\x2k10\NETLOGON\Default User.v2*.
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.

Melden sich Benutzer an Rechnern an die Mitglied der Domäne sind, erhalten diese darauf hin exakt das Profil zugeteilt, das Sie in der Freigabe *\\NETLOGON* auf dem Anmeldedomänencontroller angelegt haben. In den Profileigenschaften der Anwender legen Sie aber einen anderen Profilpfad fest, zum Beispiel *\\<Server>\Profiles\%UserName%*. Dann speichert der Computer das erstellte Profil für den Anwender servergespeichert im hinterlegten Pfad ab, da nur bei der ersten Anmeldung das Standardprofil der Freigabe *\\netlogon* verwendet wird.

Sie können darüber hinaus im unteren Bereich des Dialogfelds 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.

Abbildg. 18.12 Ändern des Profiltyps in Windows 8/8.1



Ordnerumleitungen von Profilen

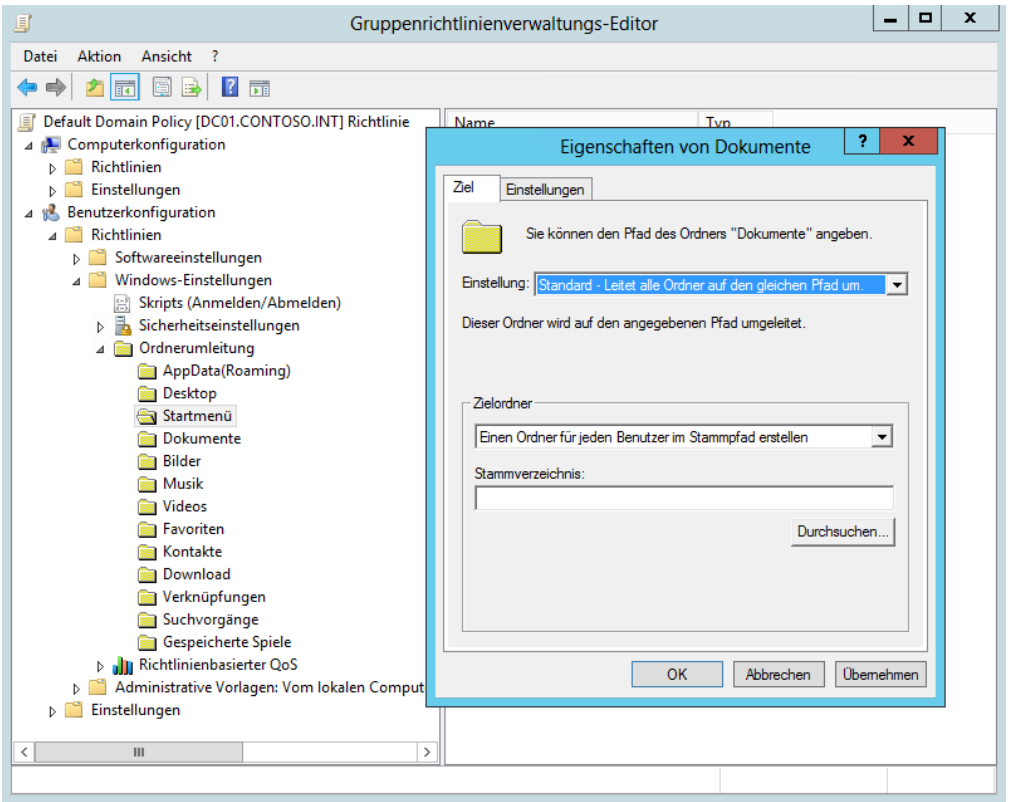
Windows 8/8.1 bietet die Möglichkeit, verschiedene Ordner innerhalb des Profils auf ein Serverlaufwerk umzuleiten. Dadurch ist sichergestellt, dass die Daten der Anwender sicher auf einem Server gespeichert werden, aber dennoch transparent zugreifbar sind, wenn ein Anwender zum Beispiel seinen *Dokumente*-Ordner öffnet. Die Größe der Profile ist dadurch reduziert, die Anmeldezeit verkürzt. Sie finden die Ordnerumleitungen im Gruppenrichtlinienverwaltungs-Editor unter *Benutzerkonfiguration/Richtlinien/Windows-Einstellungen/Ordnerumleitungen*.

Die effizienteste Möglichkeit, um Ordner umzuleiten, ist über eine Gruppenrichtlinie in einer Active Directory-Domäne. Windows Server 2012 R2 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 Ordner auf den Servern umleiten oder für jeden Anwender in einem spezifischen Ordner automatisch einen Ordner für die Ordnerumleitung anlegen lassen. Die Einstellungen in den Richtlinien für die Ordnerumleitung sind selbsterklärend. Sie konfigurieren die Einstellungen über das Kontextmenü und wählen den Befehl *Eigenschaften* aus.

Auf der Registerkarte *Ziel* legen Sie die Umleitungsoptionen fest. Einen Stammordner, also eine Freigabe, auf die alle Anwender zugreifen dürfen, müssen Sie daher zuvor anlegen. Innerhalb des Stammordners legt Windows Unterordner für die Benutzer an und konfiguriert automatisch entsprechende Rechte exklusiv für den Benutzer, genauso wie bei den Profilen.

Abbildg. 18.13 Aktivieren der Ordnerumleitung über Gruppenrichtlinien



Der Ordner *Dokumente* in einem Profil in Windows Vista und Windows 7/8 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.

Der Ordner *AppData* spielt bei der Ordnerumleitung eine wichtige Rolle, da hier die maßgeblichen Unterschiede zur Ordnerstruktur eines Profils zwischen Windows XP und Windows 8/8.1 bestehen. Um die Ordnerumleitung durchzuführen, lassen Sie über den beschriebenen Weg der Gruppenrichtlinien zunächst den Ordner *AppData* in einen Ordner 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.

Für die Anwender ändert sich bei der Umleitung nichts. Diese arbeiten mit den normalen Verknüpfungen des Rechners. Der Vorteil ist, dass Profile schlank bleiben und wichtige Daten automatisch auf den Servern landen, ohne Benutzer zu beeinträchtigen oder dass komplizierte Konfigurationen notwendig sind. Haben Sie das automatische Anlegen von Ordnern aktiviert, legt Windows diese erst dann in der konfigurierten Freigabe an, wenn Anwender auf diese zugreifen und Daten speichern.

In den Eigenschaften der Bibliotheken auf dem Clientrechner lässt sich der Pfad der Umleitung anzeigen.

Sie können die entsprechende Freigabe auch als Netzlaufwerk verbinden und stellen fest, dass alle Daten der umgeleiteten Ordner im Netzwerk liegen und für den Anwender vollkommen transparent zugreifbar sind.

Profile löschen mit Delprof2

Das Freeware-Tool Delprof2 (*http://helgeklein.com/free-tools/delprof2-user-profile-deletion-tool/* [Ms179-K18-01]) ermöglicht das Löschen von Profilen, wenn zum Beispiel Berechtigungs- oder Zugriffsprobleme vorliegen.

Mit dem Tool lassen sich Computer von alten Profilen sehr schnell bereinigen. Neben den Standardoptionen lassen sich mit dem Tool auch die lokalen Kopien von servergespeicherten Profilen löschen. Auch Zeitabfragen sind möglich. Dadurch können Sie Profile mit einem bestimmten Alter löschen lassen. Das Tool starten Sie über die Eingabaufforderung oder auch innerhalb eines Anmeldeskripts. Die Syntax des Tools lautet:

```
delprof2 [/q] [/i] [/p] [r] [/c:[\\]] [/d:]
```

- /q Keine Rückmeldungen
- /i ignoriert Fehler und führt den Löschvorgang fort
- /p Erfordert eine Bestätigung für das Löschen jedes einzelnen Profils
- /r Löscht lokale Kopien von servergespeicherten Profilen
- /c:<Computername> Löscht Profile auf einem Remotecomputer
- /d:<Tage> Löscht Profile mit einem bestimmten Alter in x Tagen
- /l Zeigt nur an, welche Profile gelöscht werden, wenn das Tool startet (What-if)

Mit User Experience Virtualization (UE-V) Benutzerprofile in Windows 8/8.1 synchronisieren

Mit dem neuen Tool User Experience Virtualization aus dem Microsoft Desktop Optimization Package (MDOP) können Sie Einstellungen in Profilen über XML-Dateien automatisieren und deutlich effizienter und stabiler konfigurieren als mit herkömmlichen servergespeicherten Profilen.

Es lassen sich alle persönlichen Einstellungen von Programmen und Windows-Funktionen in den Benutzerprofilen einstellen. Auch die Datenmenge der Profile lässt sich deutlich senken.

Grundlagen von UE-V

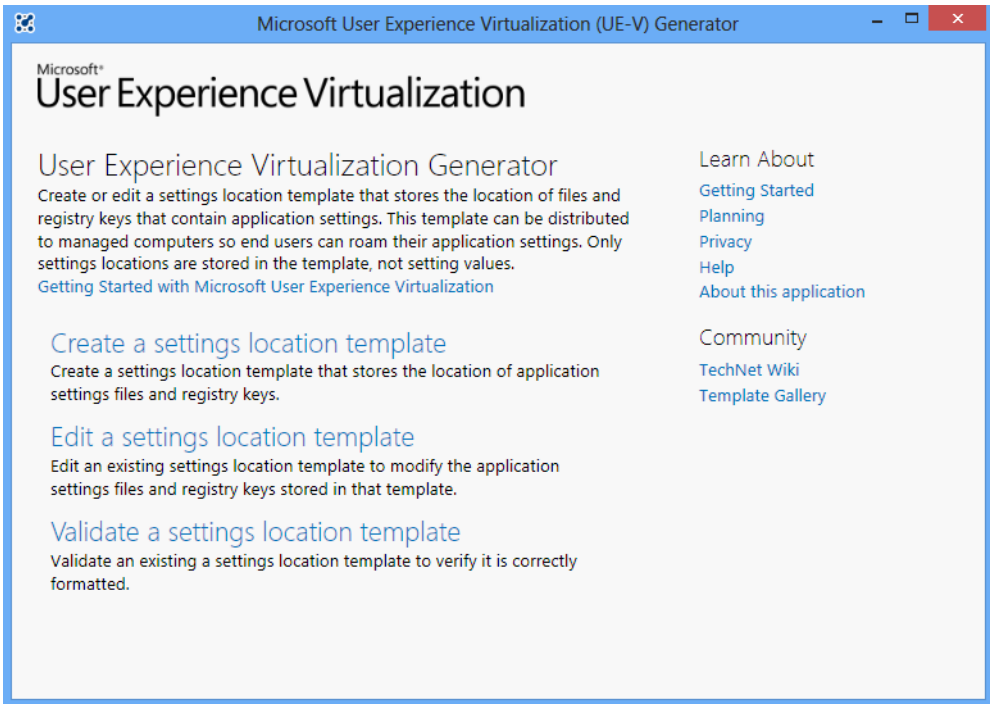
Ordnerumleitungen spielen mit UE-V eine wichtige Rolle, da UE-V nur Konfigurationen speichert, keinerlei Benutzerdaten. Windows 7 und Windows 8/8.1 bieten die Möglichkeit, Ordner innerhalb des Profils auf ein Serverlaufwerk umzuleiten. Leiten Sie zum Beispiel den Ordner der Dokumente vom Profil auf den Server um, können Anwender weiterhin problemlos auf die eigene Bibliothek zugreifen, die Daten sind dabei aber direkt auf dem Server gespeichert.

Die Größe der Profile ist dadurch reduziert, die Anmeldezeit verkürzt sich. Die Ordnerumleitungen nehmen Administratoren über Gruppenrichtlinien vor. Im Gruppenrichtlinienverwaltungs-Editor unter *Benutzerkonfiguration/Richtlinien/Windows-Einstellungen/Ordnerumleitung* sind die entsprechenden Konfigurationen zu finden.

Für die Anwender ändert sich bei der Umleitung nichts. Diese arbeiten mit den normalen Verknüpfungen des Rechners. In den Eigenschaften der Bibliotheken auf dem Clientrechner lässt sich der Pfad der Umleitung anzeigen, Benutzer sind bei der Arbeit aber nicht beeinträchtigt.

Eigentlich hat UE-V überhaupt nichts mit Virtualisierung zu tun. Eine Infrastruktur ist nicht notwendig. Einfach ausgedrückt besteht UE-V aus einer normalen Dateifreigabe, in der Einstellungen der Benutzer gespeichert und durch einen Client auf die Arbeitsstationen übertragen werden.

Abbildg. 18.14 Arbeiten mit UE-V in Windows 8/8.1 und Windows Server 2012 R2



Die Funktion UE-V im MDOP baut zunächst auf die Ordnerumleitungen auf. UE-V unterstützt neben Windows 8/8.1 auch Windows 7. Ältere Versionen werden in UE-V nicht unterstützen. UE-V kann keinerlei Benutzerdaten speichern, sondern dient nur der Konfiguration von Profilen. Administratoren, die UE-V nutzen wollen, sollten daher zunächst die Ordnerumleitung konfigurieren, wenn Benutzer im Profil Daten speichern sollen. UE-V hat die Aufgabe, verschiedene Bereiche in Profilen, also Einstellungen der Programme, der Benutzereinstellungen, E-Mail, Internet Explorer und viele andere zu speichern und festzulegen.

Für jedes Programm und jeden Einstellungsbereich gibt es dazu eine XML-Datei. Diese liegt auf einer Freigabe im Server und enthält entsprechende Einstellungen des Programms. Startet ein

Benutzer zum Beispiel Outlook, überprüft Windows 8/8.1, ob eine XML-Datei zur Konfiguration vorliegt und lädt die XML-Datei vom Server herunter.

XML-Dateien werden zusätzlich noch beim An- und Abmelden oder dem Sperren des PCs geladen. Das heißt, nicht alle Einstellungen werden gleich beim Anmelden oder Abmelden übertragen, sondern erst dann, wenn die Einstellung benötigt wird. Das geht schneller und entlastet das Netzwerk. Die Dateien sind natürlich auch mobil einsatzfähig. Dazu nutzt UE-V Offlinedateien, um XML-Dateien mit den Einstellungen auch lokal vorzuhalten. Auf den Clients läuft ein UE-V-Agent als Systemdienst, der die Änderungsdateien von einer herkömmlichen Freigabe übertragen kann. Eine komplizierte Infrastruktur ist nicht notwendig.

Diesen Client installieren Administratoren mit einer *.msi*-Datei. Über den UE-V-Generator erstellen Sie XML-Dateien für die verschiedenen Einstellungen und speichern diese auf dem Server. Diese Einstellungen lassen sich dann nicht nur auf normalen Arbeitsstationen nutzen, sondern auch für Remotedesktopserver oder auch in Virtual Desktop Infrastructure-Umgebungen.

Administratoren müssen daher nicht mehrere Profile pflegen, wie beim Einsatz von servergespeicherten Profilen, sondern nur noch die XML-Dateien, die überall gültig sind. In der XML-Datei sind die Dateien gespeichert, die für die entsprechende Konfiguration notwendig sind, sowie Registry-Einstellungen, die geändert werden müssen. UE-V lässt sich auch in der PowerShell konfigurieren und auf diesem Weg auch skripten. Wenn ein Programm zurückgesetzt werden soll, geschieht dies über das Löschen der entsprechenden XML-Datei. Der Vorteil dabei ist, dass alle anderen Einstellungen dabei erhalten bleiben.

Microsoft liefert mit UE-V bereits Vorlagendateien aus, zum Beispiel für Office 2010, Lync 2010 und den neuen Internet Explorer 10. Mit dem Generator können Sie die vorhandenen Vorlagen anpassen und neue Vorlagen erstellen.

Die Vorlagen liegen später auf der Freigabe im Netzwerk und werden durch den Agent geladen. Um eine Vorlage zu erstellen, laden Sie einfach die entsprechende *.exe*-Datei des Programms, nehmen die Einstellungen vor und speichern die Vorlage als XML-Datei auf der konfigurierten Freigabe. Startet der Anwender das Programm, lädt UE-V die Datei aus der Freigabe und nimmt die entsprechenden Einstellungen automatisch vor.

Benutzer finden daher immer identische Einstellungen ihrer Programme vor. Administratoren können parallel dazu Vorlagen zentral im Netzwerk zur Verfügung stellen, um Anwendungen schon vorzukonfigurieren. Microsoft zeigt in einer Demo die Vorteile von UE-V *(http://technet.microsoft.com/en-us/windows/hh925634* [Ms179-K18-02]). Zum Einsatz ist lediglich der UE-V-Agent auf den Clientcomputern und eine Freigabe notwendig. Das Tool zum Erstellen der Einstellungsdateien, der UE-V-Generator, gehört zum Lieferumfang des Downloads.

UE-V ist effizienter als servergespeicherte Profile. Im Gegensatz zur kompletten Übertragung aller Daten bei jedem Anmelden, wie bei den servergespeicherten Profilen, ruft Windows die UE-V-Vorlagen erst dann ab, wenn eine bestimmte Maßnahme stattfindet, die eine Vorlage benötigt. Das heißt, das An- oder Abmelden von Benutzern geht mit UE-V wesentlich schneller. Auch das Starten von Anwendungen, die über eine XML-Vorlage verfügen, kann einen solchen Vorgang auslösen, zum Beispiel das Starten von Word oder Excel, das Sperren eines Computers oder eben das An- und Abmelden.

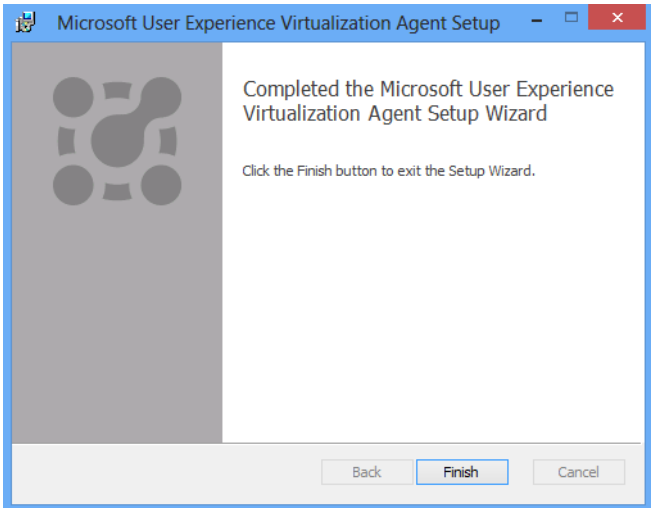
UE-V können Unternehmen in verschiedenen Szenarien nutzen. Neben der Verwendung von normalen Arbeitsplätzen unterstützt UE-V auch den Remotedesktopdienst und App-V aus dem MDOP. Auch Virtual Desktop Infrastructures (VDI) lassen sich mit UE-V nutzen. Natürlich ist auch ein Mischbetrieb unterstützt. Der Vorteil der Verwendung von mehreren Vorlagen liegt darin,

dass bei Problemen nicht das gesamte servergespeicherte Profil gelöscht werden muss, sondern nur die Vorlage des problematischen Bereichs. Alle anderen Einstellungen bleiben dabei erhalten, das gilt dann auch für die hinterlegten Einstellungen. Wie servergespeicherte Profile kann UE-V nur Einstellungen ändern, die zum Profil eines Benutzers gehören.

Im Gegensatz zu servergespeicherten Profilen, bei denen Administratoren Einstellungen in den Kontoeinstellungen von Active Directory hinterlegen, läuft auf den angebundenen Clients ein UE-V-Agent als Systemdienst. Dieser synchronisiert die verschiedenen Vorlagen, sobald das notwendig ist und speichert Benutzerdaten in einem eigenen Ordner der Stammfreigabe.

Startet ein Benutzer zum Beispiel kein Outlook, ist auch die Übertragung der entsprechenden Vorlage nicht notwendig und würde nur den Anmeldevorgang blockieren. Startet ein Benutzer Outlook, lädt UE-V die entsprechende Vorlage und hinterlegt die Einstellungen, Dateien und Registry-Einträge im System. Wie bei den servergespeicherten Profilen verfügt bei UE-V jeder Anwender über einen eigenen Ordner in einer Freigabe auf dem Dateiserver. Dieser enthält die entsprechenden Einstellungen für den Benutzer.

Abbildg. 18.15 UE-V benötigt einen Agent auf den angebundenen Client-PCs



Mit Windows 7 hat Microsoft die Möglichkeit der servergespeicherten Profile zwar verbessert, aber nicht revolutioniert. Daran hat sich auch bei Windows 8/8.1 nichts geändert. UE-V unterstützt daher auch Windows 8/8.1.

UE-V verwendet die Einstellungen, die als letztes gespeichert wurden. Es findet keine Synchronisierung zwischen verschiedenen Agents auf unterschiedlichen Computern statt, sondern UE-V speichert die Daten in der Freigabe auf dem Server. Arbeiten Anwender daher mit mehreren Computern gleichzeitig und führen Aktionen durch, die UE-V zum Abrufen oder Speichern veranlassen, ist das letzte Speichern der gültige Vorgang und diese Daten werden hinterlegt. Das ist dann wichtig, wenn Benutzer Einstellungen auf mehreren Computern gleichzeitig ändern.

Erstellen der Freigabe für UE-V

UE-V speichert Einstellungen der Benutzerprofile als XML-Datei in einer Freigabe im Netzwerk. Für jedes Programm gibt es eine solche XML-Datei. Um die Einstellungen nutzen zu können, benötigen Unternehmen daher zunächst die entsprechende Freigabe auf einem beliebigen Server im Netzwerk. Es muss sich dabei nicht um einen Domänencontroller handeln. Wichtig bei den Rechten der Freigabe ist, dass die Gruppe *Jeder* einen *Vollzugriff* auf Freigabeebene erhält.

Anschließend müssen noch die Rechte im Dateisystem für den Ordner mit den Daten gesetzt werden. Diese finden sich auf der Registerkarte *Sicherheit* über *Erweitert*. Hier müssen anschließend die Rechte für die Gruppe *Jeder* bearbeitet werden. Ist die Gruppe nicht vorhanden, muss diese hinzugefügt werden.

Durch Anklicken von Bearbeiten für die Gruppe *Jeder* lassen sich die erweiterten Rechte steuern. Das Häkchen darf nur bei den folgenden Einstellungen gesetzt sein. Bei allen anderen Einstellungen entfernen Sie das Häkchen bei dem entsprechenden Recht:

- *Ordner durchsuchen/Datei ausführen*
- *Ordner auflisten/Daten lesen*
- *Attribute lesen*
- *Erweiterte Attribute lesen*
- *Ordner erstellen/Daten anhängen*
- *Attribute schreiben*
- *Erweiterte Attribute schreiben*
- *Berechtigungen lesen*

Nach dem Bestätigen der entsprechenden Rechte ist die Freigabe für UE-V eingerichtet. Mehr Arbeit ist auf Seiten des Servers nicht notwendig. Der nächste Schritt besteht darin, den Agent auf den PCs einzurichten. Dieser speichert XML-Dateien mit den Einstellungen von Programmen entweder für alle Benutzer zentral oder für jeden Benutzer einzeln.

UE-V-Agent auf den Zielcomputern einrichten

Während bei servergespeicherten Profilen die Einstellungen über die Eigenschaften des Benutzerkontos erfolgen, übernimmt bei UE-V ein Agent auf den Clientcomputern die Übertragung der Daten von der Freigabe auf den Computer und umgekehrt. Dieser ist für 32-Bit und 64-Bit-Systeme verfügbar. Den Agent installieren Sie über die Setupdatei, Einstellungen sind bei der Installation keine notwendig. Allerdings können Sie bereits bei der Installation des Agents Einstellungen mitgeben, zum Beispiel die Stammfreigabe, in welcher der Agent die Daten des entsprechenden Benutzers speichern soll. Dazu besitzt die *.msi*-Datei über die folgenden Optionen:

- **/quiet, /norestart** Der Agent unterstützt alle Optionen, die ohnehin alle *.msi*-Dateien unterstützen und die nichts mit dem UE-V-Agent zu tun haben. Die Optionen lassen sich gemeinsam mit den UE-V-Optionen nutzen.
- **/l*v <Pfad>** Erstellen einer Protokolldatei
- **SettingsStoragePath** *SettingsStoragePath=\\<Servernname>\<Freigabe>\%UserName%*. Stammordner der Freigabe.

- **SettingsTemplateCatalogpath** Pfad oder Freigabe, in welcher der Agent automatisch nach neuen Vorlagen sucht
- **MaxPackageSizeInBytes** Legt die maximale Paketgröße fest

Die Installation des Agents erfordert Administratorrechte und einen Neustart des Rechners. Der Agent liegt dazu auch als *.msi*-Datei im entsprechenden Ordner vor. Um den Agent schnell bereitzustellen, können Administratoren die Installation manuell durchführen, eine Installation über Gruppenrichtlinien starten, System Center Configuration Manager verwenden oder Anmeldeskripts verwenden. Der Agent unterstützt allerdings nur die Editionen Ultimate, Enterprise und Professional von Windows 7 mit installiertem Service Pack 1, Windows 8/8.1, Windows Server 2008 R2 sowie Windows Server 2012 R2. Ältere Windows-Versionen werden von UE-V nicht unterstützt.

Konfigurieren Sie UE-V in Active Directory, kann der UE-V-Agent als Dateifreigabe und Speicherort für die Vorlagen für UE-V automatisch den Ordner verwenden, der in den Eigenschaften der Benutzerkonten als Stammordner festgelegt ist. Den Ordner können Sie aber auch über die Registry oder per WMI-Abfrage festlegen. In der Dateifreigabe legt UE-V automatisch für die Benutzer eigene Unterordner an.

Die Vorlagen in UE-V sind an die ausführbare Datei gekoppelt, deren Einstellungen Sie zentral vorgeben oder die mit dem Benutzer mitwandern sollen. In der XML-Datei sind die Registry-Änderungen enthalten sowie eine Liste der Dateien, welche die Änderungen betreffen.

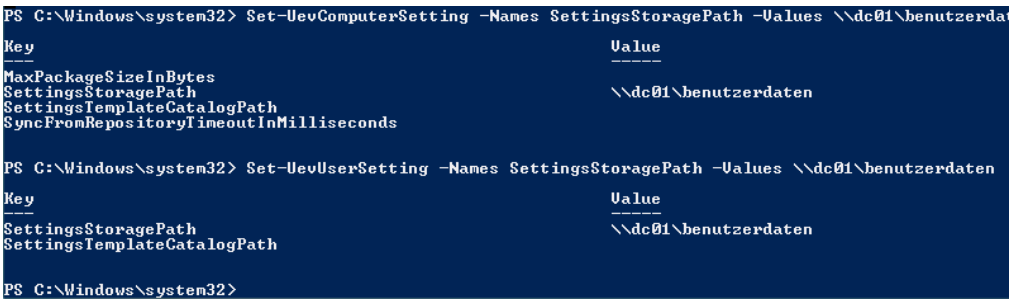
Der UE-V-Agent lässt sich auch mit der PowerShell verwalten. Dazu müssen Sie auf dem entsprechenden Computer aber erst das Modul für UE-V laden. Verwenden Sie den Cmdlet-Aufruf *Import-Module Microsoft.UEV.commands*. Vorher geben Sie den Befehl *Set-ExecutionPolicy RemoteSigned* ein, um Skripts mit den neuen Cmdlets zu erlauben. Dazu müssen Sie die PowerShell auf dem Client natürlich mit Administratorrechten über das Kontextmenü starten. Sie können die Ausführungsrichtlinie mit dem Cmdlet *Set-ExecutionPolicy* ändern und mit *Get-ExecutionPolicy* anzeigen. Die Ausführungsrichtlinie speichert ihre Daten in der Windows-Registrierung.

Sie können folgende Einstellungen vornehmen:

- **Restricted** Standardeinstellung, keine Skripts erlaubt
- **AllSigned** Nur signierte Skripts erlaubt
- **RemoteSigned** Bei dieser Einstellung müssen Sie Skripts durch eine Zertifizierungsstelle signieren lassen
- **Unrestricted** Mit dieser Einstellung funktionieren auch die SharePoint-Skripts

Haben Sie das Modul geladen, können Sie die Dateifreigabe auch mit Cmdlets in der PowerShell steuern. Dazu verwenden Sie die Cmdlets *Set-UevComputerSetting* und *Set-UevUserSetting*. Mit *Get-UevSetting* lassen Sie die aktuellen Einstellungen anzeigen.

Abbildg. 18.16 Konfigurieren von UE-V in der PowerShell



Die Vorlagen lassen sich ebenfalls mit der PowerShell abfragen. Dazu verwenden Sie den Befehl *Get-UevTemplate*. Steuern können Sie die Vorlagen mit *Register-UevTemplate*, *Unregister-UevTemplate* und *Update-UevTemplate*. Überprüfen lassen sich Vorlagen mit *Confirm-UevTemplate*.

Um UE-V in Active Directory zu verteilen, legen Sie zunächst in den Profileinstellungen von Anwendern ein Stammordner fest. Anschließend können Sie den UE-V-Agent über ein Skript installieren. Dazu können Sie zum Beispiel den folgenden Befehl verwenden:

```
msiexec /i "<Pfad zur .msi-Datei>" /quiet /norestart /l*v "%Temp%\UEV.log"
```

Innerhalb der Freigabe sind die Benutzerdaten nur dann zu sehen, wenn sie die versteckten und die Systemdateien in den Ordneroptionen einblenden lassen.

Wollen Sie die Vorlagen auch für mobile Computer steuern oder in Niederlassungen, die mit langsamen Leitungen angebunden sind, verwenden Sie noch Offlinedateien. Dazu sollten Sie aber in den Gruppenrichtlinien für solche Computer noch Einstellungen festlegen, zum Beispiel die schnellere Synchronisierung der Offlinedateien. Die Einstellungen dazu finden Sie über *Administrative Vorlagen/Netzwerk/Offlinedateien/Hintergrundsynchronisierung konfigurieren*. Setzen Sie den Wert zum Beispiel auf 5 Minuten. Um die Leistung zu verbessern, aktivieren Sie noch die Einstellung *Transparentes Zwischenspeichern aktivieren*.

Die Einstellungen des Agents sind in der Registry im Schlüssel *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\UEV\Agent\Configuration* gespeichert. Auf 64-Bit-Computern sind zusätzlich Einstellungen im Schlüssel *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Note\Microsoft\UEV\Agent\Configuration* gespeichert.

Wichtig ist, dass im Schlüssel *Configuration* ein REG_SZ-Wert mit der Bezeichnung *SettingsStoragePath* und dem Pfad zur Freigabe in der Form *\\dc01\uev\%UserName%* hinterlegt ist.

Wollen Sie Vorlagen für mobile Computer steuern, sollten in den Gruppenrichtlinien noch Einstellungen festgelegt werden, zum Beispiel die schnellere Synchronisierung der Offlinedateien. Die Einstellungen dazu finden Sie über *Administrative Vorlagen/Netzwerk/Offlinedateien/Hintergrundsynchronisierung*. Hier ist ein Wert von 5 Minuten ideal. Die Einstellung *Transparentes Zwischenspeichern aktivieren* sollte ebenfalls gesetzt sein.

UE-V-Vorlagen vorgeben und testen

Um eigene Vorlagen zu erstellen oder die vorhandenen Vorlagen anzupassen, verwenden Sie den User Experienence Virtualization Generator. Diesen installieren Sie über die Datei ToolsSetup. Auch für diese Installation sind Administratorrechte notwendig. Die genaue Vorgehensweise zur Einrichtung von UE-V zeigt Microsoft in zwei PDF-Dateien, die zum Lieferumfang des Downloads gehören. In diesen Dateien ist auch zu sehen, welche Möglichkeiten es gibt, den Agent unbeaufsichtigt zu installieren und Einstellungen vorzunehmen. Über den Generator lassen sich schnell und einfach auf Basis von *.exe*-Dateien Vorlagen erstellen und vorhandene Vorlagen bearbeiten oder testen.

Um eine Vorlage für ein Programm zu erstellen, müssen Sie im Generator zunächst die *.exe*-Datei des Programms laden. Anschließend überprüft der Generator, wo die Einstellungen des Programms gespeichert sind. Im nächsten Schritt startet der Generator das Programm und Sie können es wieder beenden. Durch diese Schritte kann der UE-V-Generator die Dateien und Registry-Einträge erfassen, in denen die Daten des entsprechenden Programms gespeichert sind.

Sobald die Freigabe für UE-V erstellt und auf den ersten Computern die Agents installiert sind, können Sie Vorlagen konfigurieren, registrieren und verwenden. Die mitgelieferten Vorlagen von UE-V finden Sie im Ordner *C:\Program Files\Microsoft User Experience Virtualization\Templates*.

Neben der Möglichkeit, dass Anwender ihre Einstellungen automatisiert in der entsprechenden Freigabe speichern können und damit auf allen Computern zur Verfügung haben, können Sie auch Einstellungen zentral vorgeben. Dazu muss auf den Zielcomputern ein neuer REG_SZ-Wert mit der Bezeichnung *SettingsTemplateCatalogPath* erstellt werden. Als Wert wird der Pfad angegeben, in dem Administratoren die XML-Dateien speichern. Startet ein Anwender ein Programm, für das es eine solche XML-Datei gibt, lädt der UE-V-Agent diese vom Pfad herunter und stellt die Anwendung entsprechend ein.

Um eine Vorlage für ein Programm zu erstellen, müssen Sie im Generator zunächst die *.exe*-Datei des Programms laden. Anschließend überprüft der Generator, wo die Einstellungen des Programms gespeichert sind. Im nächsten Schritt startet der Generator das Programm und Sie können es wieder beenden. Durch diese Schritte kann der UE-V-Generator die Dateien und Registry-Einträge erfassen, in denen die Daten des entsprechenden Programms gespeichert sind.

Anmelde- und Abmeldeskripts für Benutzer und Computer

Sie können Benutzern in Active Directory Anmeldeskripts zuweisen, die ein Computer ausführt, sobald sich der Benutzer anmeldet. Über Gruppenrichtlinien lassen sich sogar Skripts starten, die beim Starten, Herunterfahren, bei der Abmeldung und zusätzlich noch bei der Anmeldung ablaufen. Es gibt daher fünf Arten von Skripts, die Administratoren Anwendern oder Computern zuweisen können. Es ist auch möglich, mehrere Arten von Skripts zu mischen. Windows-Computer führen alle aus.

Um automatisch Befehle beim Anmelden von Benutzern ausführen zu lassen, oder auch wenn PCs starten, gibt es folgende Möglichkeiten:

1. Das klassische Anmeldeskript, das in den Eigenschaften des Profils eingetragen ist. Die Ausführung sieht der Anwender teilweise in einem Fenster der Eingabeaufforderung.
2. Anmeldeskripts in den Gruppenrichtlinien für Benutzer
3. Abmeldeskripts in den Gruppenrichtlinien für Benutzer
4. Skripts in den Gruppenrichtlinien beim Hochfahren eines Computers, unabhängig vom Benutzer
5. Skripts in den Gruppenrichtlinien beim Herunterfahren eines Computers, unabhängig vom Benutzer

Die klassischen Anmeldeskripts, die Programme und Befehle ausführen, hinterlegen Sie auf der Registerkarte *Profil* in den Eigenschaften der Benutzer. An dieser Stelle haben Sie auch die Möglichkeit, das lokale Benutzerprofil des Anwenders auf eine Freigabe zu speichern. Damit die Skripts beim Anmelden von Benutzern auch starten, müssen Sie die Dateien und die Programme, welche die Skripts starten sollen, in der NETLOGON-Freigabe auf den Domänencontrollern speichern.

Wenn Sie ein Skript in die NETLOGON-Freigabe eines Domänencontrollers kopieren, wird es durch den Dateireplikationsdienst (File Replication Service, FRS) automatisch auf die anderen Domänencontroller repliziert. Überprüfen Sie den Vorgang oder kopieren Sie das Skript manuell.

Der lokale Speicherort der NETLOGON-Freigabe ist der Ordner *\Windows\SYSVOL\sysvol\<Domänennamen>\scripts*.

Die Skripts können entweder einfache Batchdateien, spezielle Varianten mit KiXtart (*http://www.kixtart.org* [Ms179-K18-03]) oder AutoIT (*http://www.autoitscript.com/site/* [Ms179-K18-04]), aber auch VBScript-Dateien sein. Windows muss die Skripts nur ausführen können und über die entsprechende Erweiterung verfügen.

Klassische Anmeldeskripts laufen sichtbar ab, wenn sich ein Anwender bei seinem Computer anmeldet. Mit klassischen Anmeldeskripts ist es auch nicht möglich, Skripts zu schreiben, die ein Computer bereits beim Starten abarbeitet. In einem Active Directory können Sie neben den klassischen Skripts auch Skripts beim Anmelden und Abmelden sowie beim Starten und Herunterfahren eines Computers über Richtlinien festlegen (siehe Kapitel 19). Dies hat den Vorteil, dass sich solche Skripts auch Organisationseinheiten oder ganzen Domänen zuordnen lassen. 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

Die Abarbeitung von Skripts in den Gruppenrichtlinien hat den Vorteil, flexibler zu sein. Es besteht auch die Möglichkeit, herkömmliche Anmeldeskripts einfach über Gruppenrichtlinien ausführen zu lassen, nicht mehr über die Eigenschaften der Benutzerprofile. Die Skripts in den Gruppenrichtlinien laufen nicht sichtbar im Hintergrund ab. Benutzer bekommen von den Skripts nichts mit, auch wenn herkömmliche *.bat*- oder *.cmd*-Dateien im Einsatz sind. Um Skripts in den Gruppenrichtlinien zu verwenden, gehen Sie folgendermaßen vor:

1. Legen Sie die entsprechende Gruppenrichtlinie an und verknüpfen Sie diese mit der Domäne oder den gewünschten Organisationseinheiten.
2. Öffnen Sie die Bearbeitung der Gruppenrichtlinie 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*. Neben herkömmlichen Skripts lassen sich an dieser Stelle auch PowerShell-Skripts anbinden.
4. Klicken Sie auf die Schaltfläche *Dateien anzeigen*. Es öffnet sich ein Explorer-Fenster.
5. Kopieren Sie anschließend Ihre Skriptdatei in diesen geöffneten Ordner.
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. Das heißt, manche Skripts können in den Eigenschaften der Benutzerkonten gespeichert sein und ablaufen, andere in den Gruppenrichtlinien. 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 starten.

Sie können alle möglichen Formen miteinander kombinieren. Wenn Unternehmen mit klassischen und Gruppenrichtlinienskripts arbeiten, laufen beide parallel ab. Diesen Sachverhalt sollten Administratoren in den Skripts beachten, wenn zum Beispiel Abhängigkeiten existieren. Skripts in den Gruppenrichtlinien laufen meistens vor den klassischen Anmeldeskripts.

Außer speziellen Skripts lassen sich in den Gruppenrichtlinien auch diverse Einstellungen hinterlegen, die den Ablauf der Skripts steuern. Die Einstellungen sind in den Gruppenrichtlinien zu finden. Die entsprechenden Erläuterungen und Hilfen finden Administratoren direkt in der Hilfe der jeweiligen Einstellung. Folgende Richtlinieneinstellungen spielen dabei eine Rolle:

- *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*

Gruppen verwalten

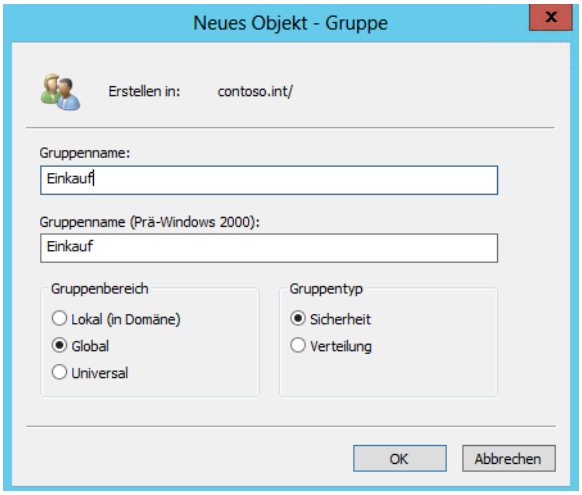
Nicht weniger wichtig als die Verwaltung von Benutzern ist die Verwaltung von Gruppen in Active Directory. Im nachfolgenden Abschnitt gehen wir darauf ein, wie Sie Gruppen anlegen und verwenden.

Gruppen anlegen und verwenden

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. 18.17 Erstellen einer neuen Gruppe



Bei der Unterscheidung und Verwendung dieser Gruppen müssen Sie folgende Punkte beachten:

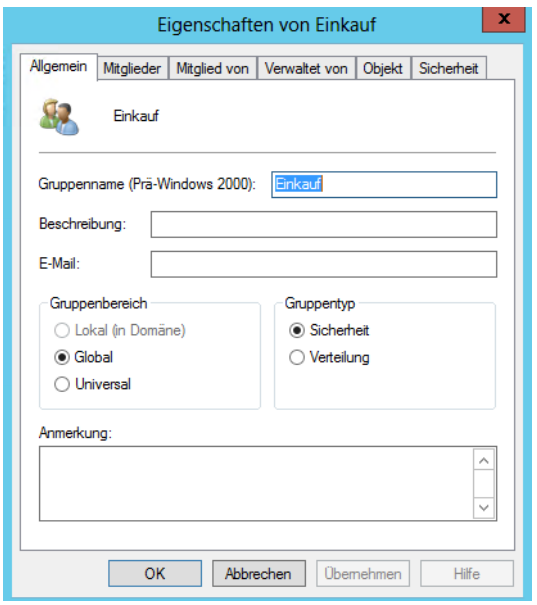
- **Lokale Gruppen** Werden für die Zusammenfassung von globalen Gruppen oder in Ausnahmefällen Benutzern eingesetzt, denen Sie Zugriffsberechtigungen erteilen. Aus lokalen Gruppen in einem Active Directory automatisch domänenlokale Gruppen. Der Unterschied besteht darin, dass diese Gruppen einheitlich auf allen Mitgliedssystemen der Domäne zu sehen sind. Der Vorteil ist, dass damit eine lokale Gruppe 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. Globale Gruppen können zudem verschachtelt werden.
- **Universellen Gruppen** Alle Informationen über Zugehörigkeiten zu universellen Gruppen sind auf den globalen Katalogservern gespeichert. Universelle Gruppen sind in allen Domänen der Gesamtstruktur verfügbar und können Mitglieder aus allen Domänen enthalten. Durch die Replikation im globalen Katalog belasten Sie allerdings das Netzwerk und die globalen Katalog-Server.

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 können Sie zusätzlich als E-Mail-Verteilerliste verwenden.
- **Verteilung** Gibt an, dass die Gruppe nur für Verteiler in E-Mail-Programmen zur Verfügung steht. Sie können diese Gruppen aber nicht für die Zuordnung von Zugriffsberechtigungen verwenden.

Die Eigenschaften von Gruppen können Sie auch nach dem Erstellen bearbeiten. Dazu rufen Sie die Eigenschaften der Gruppen auf.

Abbildg. 18.18 Verwalten von Gruppen



- Neben dem Gruppennamen können Sie eine Beschreibung für die Gruppe eingeben
- Auf der Registerkarte *Mitglieder* können Sie über die Schaltflächen *Hinzufügen* und *Entfernen* neue Benutzer in Gruppen aufnehmen oder entfernen
- Auf der Registerkarte *Mitglied von* werden die Gruppen angezeigt, in denen diese Gruppe Mitglied ist
- Über die Registerkarte *Verwaltet von* sehen Sie den Benutzer, der für eine Gruppe zuständig ist. Dazu wird über die Schaltfläche *Ändern* eine Liste der Benutzer und Gruppen geöffnet, aus der der entsprechende Benutzer ausgewählt werden kann.

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, müssen Sie ein Benutzerkonto nur der Gruppe zuordnen, die Zugriff auf einen Ordner hat. Die Berechtigungen müssen nicht verändert werden. Ebenso lassen sich die Zugriffsberechtigungen einzelnen Benutzern entziehen, indem Sie diese aus der Gruppe entfernen.

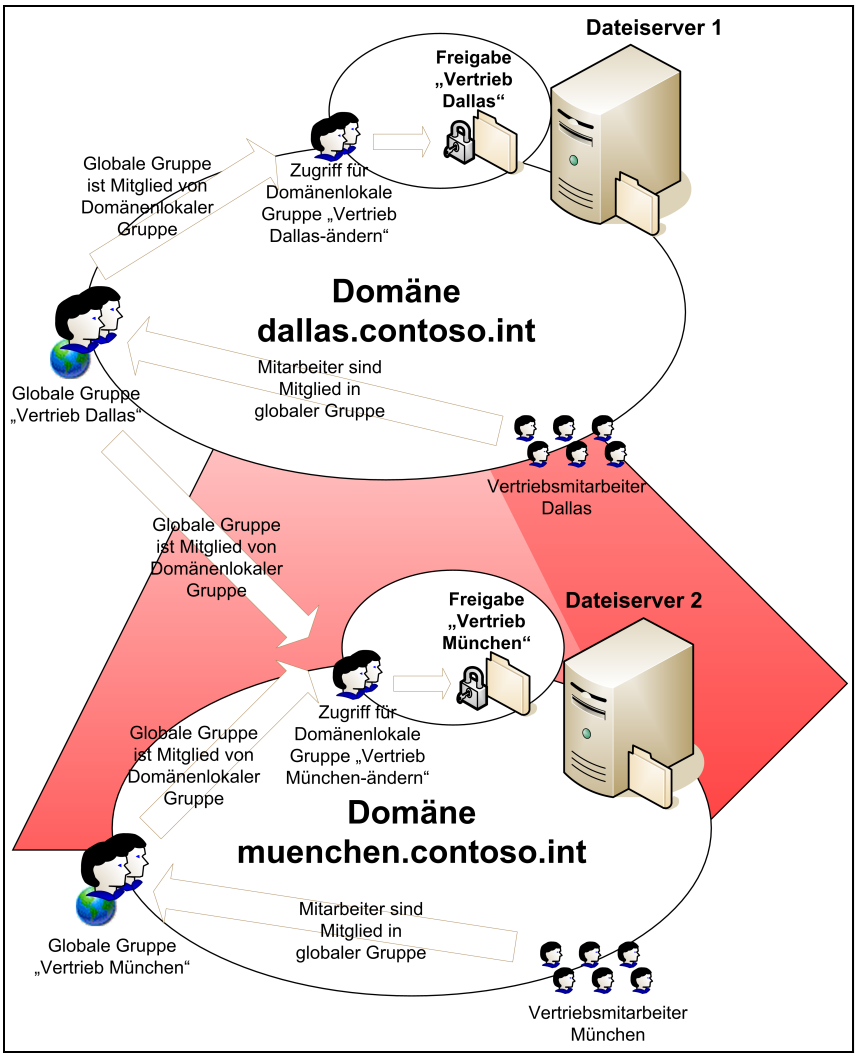
Microsoft empfiehlt folgende Berechtigungsstruktur:

1. Eine domänenlokale Gruppe erhält Berechtigung auf den Ordner und Freigabe
2. Globale Gruppen mit Benutzern werden in die lokale Gruppe aufgenommen
3. Benutzerkonten der Anwender sind Mitglieder der einzelnen globalen Gruppen

Die Berechtigungen im Dateisystem speichert Windows in der Zugriffssteuerungsliste (Access Control List, ACL). Während der Anmeldung erstellt ein Domänencomputer für den Benutzer ein Zugriffstoken, das die Sicherheits-ID (Security ID, SID) des Benutzerkontos enthält sowie die SIDs der Gruppen, in denen der Benutzer Mitglied ist. Beim Zugriff auf eine Freigabe vergleicht der Server die Einträge des Token mit der ACL und ermittelt daraus die Berechtigung. Dazu addiert Windows die Berechtigungen für jeden übereinstimmenden Eintrag. Ein Benutzer bekommt die Berechtigungen, die seinem Konto zugewiesen sind, sowie alle Berechtigungen, die den Gruppen zugewiesen sind, in denen er Mitglied ist.

Geben Sie einem Benutzerkonto die Berechtigung *Lesen* 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, aktivieren Sie in den Eigenschaften des Ordners oder der Datei die Registerkarte *Sicherheit*. Zusätzlich ist es möglich, einzelnen Benutzern oder Gruppen Berechtigungen zu verweigern, wobei die Verweigerung immer Vorrang hat.

Abbildg. 18.19 Aufbau einer Berechtigungsstruktur basierend auf Gruppen



Beispiel:

Auf eine Datei sollen alle Mitarbeiter der Abteilung *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.

Die Verbindung der Clients erfolgt zunächst zu einem Server. Auf diesem Server steht eine Freigabe zur Verfügung. Eine Freigabe definiert, auf welche Ordner auf den Datenträgern Anwender zugrei-

fen können. Der Client sieht nicht die physischen Festplatten auf den Servern und die dort definierten Ordnerstrukturen. Vielmehr stellt ihm eine Freigabe einen Eintrittspunkt zum Server bereit, von dem aus er die dort definierten Ordnerstrukturen durchsuchen kann. 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 Administratoren Zugriffsberechtigungen definieren. Auch hier ist die Arbeit mit Gruppen der beste Weg. Damit können Sie Freigaben als weitere Ebene der Sicherheit einsetzen, zusätzlich zu den Berechtigungen auf der Ebene des Dateisystems.

Auf Ordner im Dateisystem sollten die Administratoren Vollzugriff erhalten. Zusätzlich sollten Sie eine domänenlokale Gruppe anlegen, die Berechtigung auf der Ordnerebene 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 sind, können Sie die Gruppen auch in andere domänenlokale Gruppen in anderen Domänen von Active Directory aufnehmen. Das hat in großen Organisationen den Vorteil, dass Freigaben sehr effizient überall zur Verfügung stehen.

Mitgliedschaften und Änderungen sollten Sie deshalb auf ein Minimum reduzieren. Sie sollten keine einzelnen Benutzer zu den Berechtigungen auf Freigabe- oder Dateiebene hinzufügen. Zugriffsberechtigungen vergeben Sie im Regelfall pro Ordner einheitlich. Eine Anpassung von Berechtigungen für einzelne Dateien ist nur in Ausnahmen sinnvoll und lässt sich oft dadurch umgehen, dass Sie mit eigenen Ordnern arbeiten. Im Beispiel von Abbildung 18.19 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 in 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.

Szenario: Delegierung zum administrativen Verwalten einer Organisationseinheit

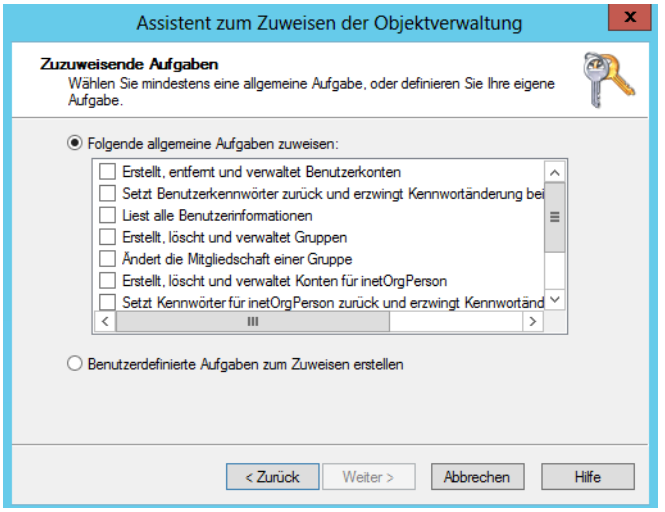
Ein gutes Praxisbeispiel für die Delegierung von Benutzerrechten in Active Directory ist das Zurücksetzen von Kennwörtern, welches zum Beispiel Support-Mitarbeiter erhalten sollen. Wenn Anwender ihr Kennwort vergessen oder ein neues Kennwort zugewiesen bekommen, sollte das nicht die Aufgabe der Systemadministratoren sein. In diesem Fall könnte zum Beispiel der Abteilungsleiter oder ein Poweruser diese Aufgaben übernehmen. Es besteht außerdem die Möglichkeit, an eine bestimmte Gruppe genau diese Rechte für seine OU zu delegieren:

1. Legen Sie zunächst eine globale oder universelle Benutzergruppe an, welche die Rechte der Delegierung erhalten soll. Auch wenn die Gruppe zunächst keinen Benutzer enthält, sollten Sie in den Berechtigungen von Active Directory niemals nur einzelne Konten eintragen, da ansonsten

die Berechtigungsstruktur sehr kompliziert wird. Außerdem müssen Sie bei jeder Änderung dann direkt Änderung am System vornehmen, anstatt nur Benutzer der Gruppe hinzuzufügen oder aus der Gruppe zu entfernen.

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. Welche Rechte die Gruppe erhält, legen Sie erst später fest.
4. Aktivieren Sie im nächsten Fenster als zuzuweisende Aufgabe zum Beispiel das Recht *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. Wollen Sie speziellere Rechte erteilen, aktivieren Sie die Option *Benutzerdefinierte Aufgaben zum Zuweisen erstellen*.

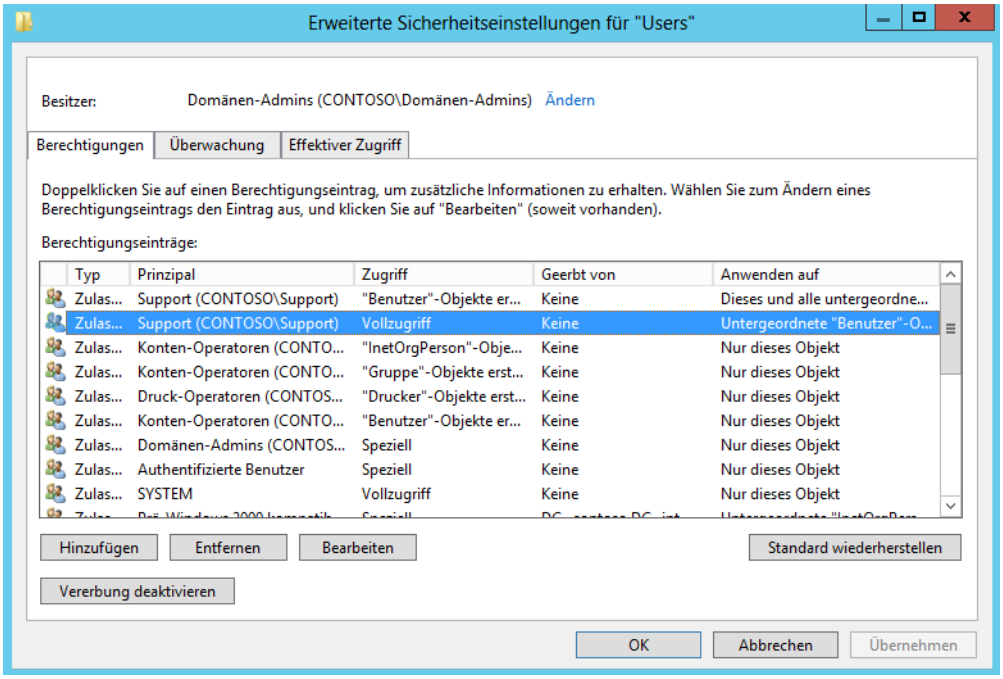
Abbildg. 18.20 Auswählen von Rechten für die Gruppe, der Sie Rechte delegieren wollen



Beenden Sie den Assistenten, um die Delegierung abzuschließen. Anschließend erhalten alle Mitglieder, die Sie in die Gruppe aufnehmen, die entsprechenden Rechte. Entfernen Sie ein Benutzerkonto aus der Gruppe, verliert es diese Rechte. Bei der Änderung von Gruppenmitgliedschaften muss sich der entsprechende Benutzer in den meisten Fällen neu anmelden, bevor er die entsprechenden Rechte erhält.

Die entsprechenden Rechte für diese Gruppe finden Sie, indem Sie 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 und die Registerkarte *Sicherheit* öffnen, sehen Sie die delegierten Rechte. Klicken Sie hier auf *Erweitert*, finden Sie im folgenden Fenster auf der Registerkarte *Berechtigungen* die genauen Rechte der Gruppe aufgelistet, die Sie delegiert haben. Wenn Sie die Delegierung wieder rückgängig machen wollen, müssen Sie einfach an dieser Stelle die Rechte der Gruppe wieder entfernen.

Abbildg. 18.21 Anzeigen der delegierten Berechtigungen auf der Registerkarte *Berechtigungen* des delegierten Containers



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 das sie die OU verwalten können. Dazu verwenden Sie am besten die Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT). Mehr dazu finden Sie in den Kapiteln 3, 4 und 7.

TIPP Im Internet gibt es auch einige Freeware-Tools die genau auf solche Kennwortänderungen ausgelegt sind. Ein Beispiel für eine solche Lösung ist Password Control (*http://www.wisesoft.co.uk/software/passwordcontrol/default.aspx* [Ms179-K18-05]). Die Software lässt sich schnell und einfach installieren.

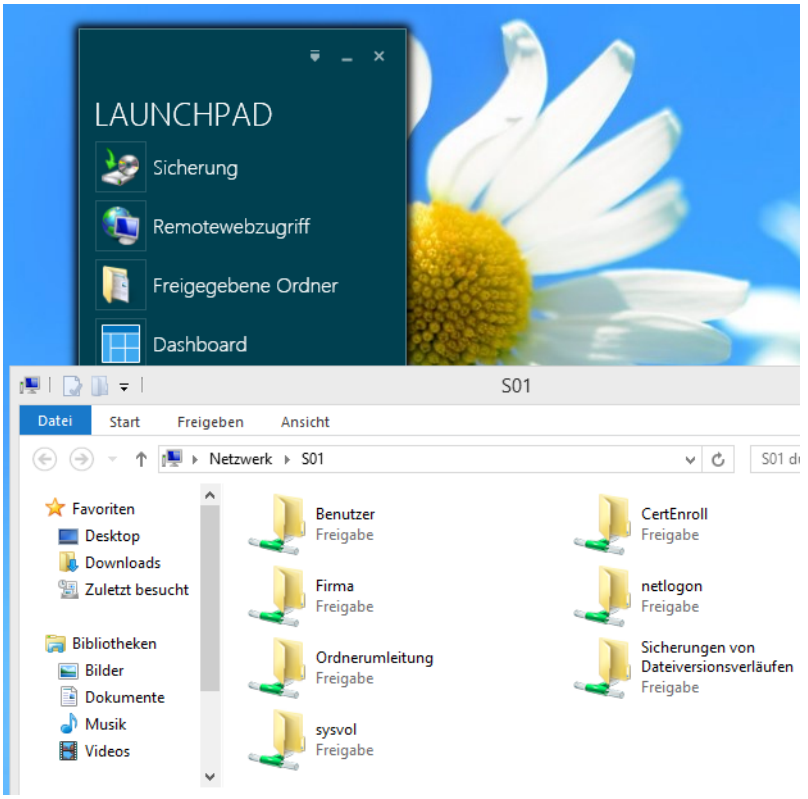
Haben Administratoren bestimmten Benutzern das Recht erteilt, Kennwörter zu ändern, können diese das dann zukünftig über dieses Tool durchführen. Der Vorteil des Tools ist auch dessen leichte Bedienbarkeit.

Für SharePoint gibt es ebenfalls zahlreiche Webparts, die Unternehmen einbinden können. Auch über diese Webparts (*http://www.sharepointboost.com/password-change-expiration.html* [Ms179-K18-06]) lassen sich Self-Service-Portale aufbauen.

Benutzer in Windows Server 2012 R2 Essentials

Die Verwaltung der Benutzer und Computer läuft in Windows Server 2012 R2 Essentials etwas anders ab. Wir gehen in Kapitel 36 ausführlicher auf die Einrichtung der Sicherung und die Anbindung von Computern an Windows Server 2012 R2 Essentials ein. In Kapitel 2 zeigen wir Ihnen, wie Sie den Server installieren. In den folgenden Abschnitten erklären wir Ihnen, wie Sie Benutzer im Dashboard von Windows Server 2012 R2 Essentials anlegen. In Kapitel 41 gehen wir ausführlicher auf Windows Server 2012 R2 Essentials ein. Legen Sie ein neues Benutzerkonto an, können Sie automatisch Benutzerrollen zuweisen, um dem Anwender Standard- oder Administratorrechte zuzuweisen. Sie haben auch die Möglichkeit, eine Benutzerrolle jederzeit zu ändern. Auf diese Weise können Sie zum Beispiel aus einem Standardbenutzer einen Administratorbenutzer machen. Administratoren dürfen das Dashboard auf ihrem Client starten und auf diese Weise den Server verwalten. Normale Anwender erhalten nach der Anmeldung auf ihrem PC ein Launchpad angezeigt, über das sie auf die Freigaben auf dem Server zugreifen können. Dazu muss der Clientcomputer über einen Connector an den Server angebunden werden (siehe Kapitel 36).

Abbildg. 18.22 Nach der Anmeldung erhalten Anwender einen direkten Zugriff auf die Daten des Servers



Neues Benutzerkonto anlegen

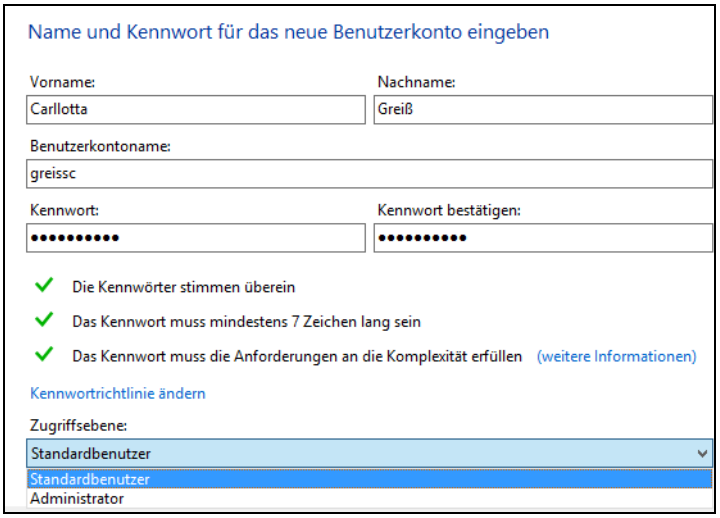
Um einen neuen Benutzer anzulegen, rufen Sie das Dashboard auf, klicken auf *Benutzer* und anschließend über den rechten Bereich auf die Option *Benutzerkonto hinzufügen*. Das Dashboard können Administratorbenutzer auch direkt auf ihrem Client aufrufen, nachdem dieser an den Server angebunden ist.

Es startet ein Assistent, über den Sie die Daten des Anwenders eingeben. Sie legen zunächst den Vor- und Nachnamen sowie zusätzlich den Benutzerkontonamen fest. Mit diesem meldet sich der Benutzer an seinem Computer an, sobald der Connector installiert ist (siehe Kapitel 36). Benutzer brauchen Namen und Kennwort auch für die Installation des Connectors. Mehr zu diesem Thema lesen Sie auch in Kapitel 41.

Anschließend legen Sie noch das Kennwort für den Anwender fest und dessen Zugriffsebene. *Standardbenutzer* dürfen auf Freigaben zugreifen, *Administratoren* dürfen über das Launchpad auch noch das Dashboard aufrufen, den Server verwalten und auf alle Daten zugreifen.

Sie können in der Steuerung der Freigaben festlegen, welche Rechte einzelne Benutzer, alle Standardbenutzer und Administratoren für einzelne Freigaben erhalten.

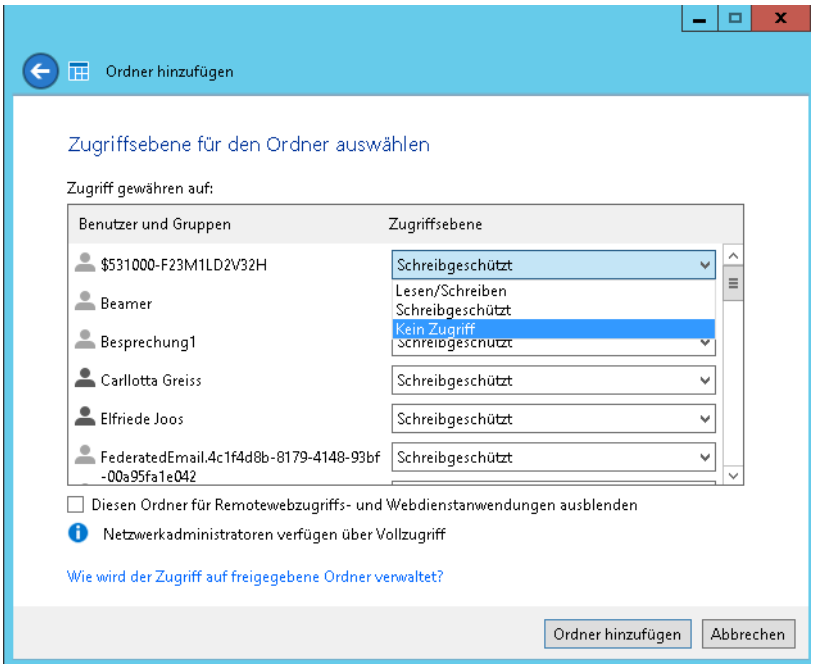
Abbildg. 18.23 Anlegen eines neuen Benutzerkontos in Windows Server 2012 R2 Essentials



Auf der nächsten Seite zeigt der Assistent alle vorhandenen Freigaben an und Sie können festlegen, welche Rechte der Benutzer auf die Freigaben erhalten soll.

Standardmäßig gibt es nach der Installation von Windows Server 2012 R2 Essentials nur die Freigabe *Firma*. Die Standardbenutzer dürfen auf die Freigabe lesend zugreifen, Administratoren dürfen schreiben. Sie haben die Möglichkeit, für jedes einzelne Benutzerkonto festzulegen, ob der entsprechende Anwender lesend (schreibgeschützt) oder lesend und schreibend auf die Freigaben zugreifen darf.

Abbildg. 18.24 Festlegen der Rechte für das neue Benutzerkonto



Erstellen Sie weitere Freigaben (siehe Kapitel 20), können Sie in den Eigenschaften der Benutzerkonten und in den Eigenschaften der Freigabe steuern, welche Rechte Benutzer auf die Freigabe erhalten. Die Freigaben erscheinen automatisch im Launchpad.

Auf der nächsten Seite legen Sie fest, auf welche Bereiche des Remotewebzugriffs der Anwender zugreifen darf. Diesen können Anwender zum Beispiel über das Internet aufrufen. Sie können einzelne Bereiche ausklammern oder den kompletten Remotewebzugriff für den Benutzer sperren, indem Sie das Kontrollkästchen *Remotewebzugriff nicht zulassen* aktivieren. Sobald der Computer des Anwenders mit dem Server verbunden ist (siehe Kapitel 36), kann er sich mit seinem Benutzerkonto anmelden und auf die Daten auf dem Server zugreifen.

Scheidet ein Benutzer dauerhaft aus dem Unternehmen aus, können Sie das Benutzerkonto komplett löschen. Dazu wählen Sie im Kontextmenü den Befehl *Benutzerkonto entfernen* aus. Anschließend löscht der Assistent das Konto komplett vom Server. Bevor das Konto gelöscht wird, können Sie noch auswählen, ob der Server auch die Daten des Benutzers löschen soll. Diese befinden sich auf dem Server im Ordner *Benutzer*.

Auf persönliche Ordner zugreifen

Beim Hinzufügen eines neuen Benutzerkontos legt der Assistent automatisch einen Ordner für das Benutzerkonto auf dem Server an. Auf diesen Ordner darf nur der entsprechende Benutzer über die Freigaben im Launchpad zugreifen. Alle Daten, die der Benutzer in diesem Ordner speichert, liegen auf dem Server.

Für den schnellen Zugriff kann der Anwender auch die Freigabe *Benutzer* über das Kontextmenü als Netzlaufwerk verbinden. Bei der Sicherung berücksichtigt der Server automatisch die Daten in dieser Freigabe.

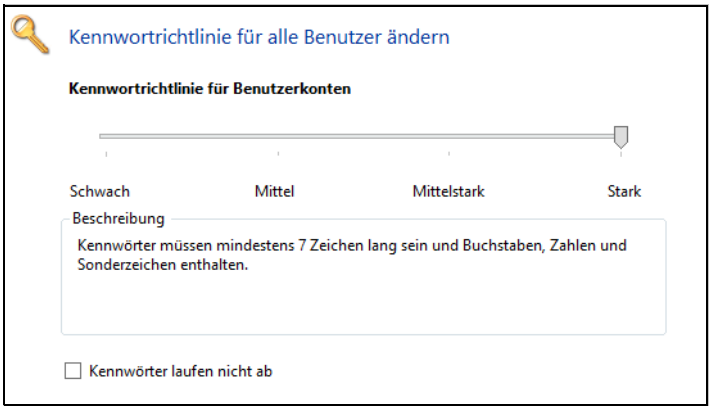
Um auf die Daten zuzugreifen, können Sie aber nicht die Freigabe verwenden, sondern müssen direkt auf dem Server oder über den Remotedesktop auf den Ordner auf der Festplatte des Servers zugreifen. Standardmäßig befindet sich der Ordner auf dem Server im Pfad *C:\ServerFolders\Benutzer*.

Benutzerkonten verwalten

Nachdem Sie ein Benutzerkonto angelegt haben, können Sie jederzeit Änderungen an den Rechten, dem Kennwort und den Optionen des Kontos vornehmen. Auch dazu verwenden Sie wieder das Dashboard auf dem Server. Müssen Sie auf dem Server das Kennwort des Benutzers ändern, klicken Sie mit der rechten Maustaste im Dashboard auf den Eintrag für das Benutzerkonto und wählen im Kontextmenü den Befehl *Benutzerkennwort ändern*. Anschließend geben Sie zweimal das neue Kennwort ein und klicken auf *Kennwort ändern*.

Mit Windows Server 2012 R2 Essentials können Sie die Konfiguration der Kennwörter festlegen bzw. ändern. Dazu steht im Dashboard der Link *Kennwortrichtlinie ändern* zur Verfügung. Über den Assistenten können Sie mit einem Schieberegler festlegen, wie die Kennwörter der Anwender aufgebaut sein sollen.

Abbildg. 18.25 Konfigurieren der Kennwortrichtlinie



Aktivieren Sie das Kontrollkästchen *Kennwörter laufen nicht ab*, müssen die Anwender das Kennwort nicht nach Ablauf von 180 Tagen ändern, sondern können es dauerhaft behalten.

Klicken Sie doppelt auf ein Benutzerkonto im Dashboard, öffnen sich die Eigenschaften und Sie können über verschiedene Registerkarten Einstellungen ändern. Auf der Registerkarte *Allgemein* können Sie nachträglich noch den Vor- und Nachnamen sowie die Zugriffsebene ändern. Den Kontonamen können Sie nach der Erstellung aus Sicherheitsgründen nicht mehr ändern.

Außerdem können Sie an dieser Stelle das Konto deaktivieren, indem Sie das Kontrollkästchen *Benutzer ist aktiv* deaktivieren. Standardmäßig zeigt der Connector für Windows Server 2012 R2 Essentials auf den Clientcomputern nur Fehler auf dem Client an (siehe Kapitel 36). Sie können für einzelne Benutzer aber auch festlegen, dass diese alle Warnungen im Netzwerk in der Meldungsan-

zeige sehen, auch die Fehler des Servers. Die Anwender benötigen dazu keine Administrationsrechte. Damit der Connector auf Clientcomputern alle Fehler anzeigt, rufen Sie im Dashboard die Eigenschaften des Benutzerkontos auf. Anschließend aktivieren Sie die Option *Benutzer kann Integritätswarnungen für das Netzwerk anzeigen* auf der Registerkarte *Allgemein* in den Benutzereigenschaften.

Auf der Registerkarte *Freigegebene Ordner* können Sie für jede Freigabe auf dem Server (siehe Kapitel 20) den Zugriff für das Benutzerkonto steuern. Hier ändern Sie zum Beispiel die Rechte, wenn Sie nach der Erstellung des Benutzerkontos noch weitere Freigaben angelegt haben.

Mit der Registerkarte *Zugriff überall* steuern Sie die Funktionen, auf die das Benutzerkonto zugreifen darf, wenn der Zugriff über Remoteweb erfolgen soll. Standardmäßig darf jeder Benutzer den Remotewebzugriff nutzen. Sie können die Berechtigung aber für jeden einzelnen Benutzer steuern.

Auf der Registerkarte *Computerzugriff* können Sie festlegen, auf welche Computer der Anwender über den Remotedesktop zugreifen darf, wenn er sich mit dem Remotewebzugriff verbindet. Verbindet sich der Anwender über das Internet mit der Adresse *https://<Servername>/remote*, kann er sich direkt am Server authentifizieren. Computer, die Sie in den Eigenschaften des Benutzerkontos für den Zugriff berechtigen, erscheinen im Remotewebzugriff und der Anwender kann auf den Desktop des Computers zugreifen. Der Computer muss dazu eingeschaltet sein.

Ist ein Anwender im Urlaub oder längere Zeit nicht im Haus, können Sie sicherstellen, dass sich kein Benutzer mit dem Konto anmelden kann, indem Sie es zeitweise deaktivieren. Alle Daten des Benutzers bleiben dabei erhalten und Sie können das Konto jederzeit wieder aktivieren. Die Deaktivierung nehmen Sie im Dashboard vor. Dazu rufen Sie die Registerkarte *Benutzer* auf und klicken mit der rechten Maustaste auf das Benutzerkonto. Wählen Sie aus den Optionen *Benutzerkonto deaktivieren* aus.

Zusammenfassung

Auch wenn die Verwaltung der Benutzer und die Delegation von Rechten noch sehr ähnlich zu Windows Server 2003/2008/2008 R2/2012 ist, haben Sie in diesem Kapitel erfahren, dass vor allem im Bereich der Benutzerprofile und der Verwendung von servergespeicherten Profilen in Windows Server 2012 R2 Änderungen integriert wurden, welche die Möglichkeiten im Netzwerk deutlich verbessern. Auch auf die neue User Experience Virtualization (UE-V) wurde in diesem Kapitel eingegangen.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie mit Gruppenrichtlinien die Konfiguration von Computern und Benutzereinstellungen weitgehend automatisieren können.

Kapitel 19

Richtlinien im Windows Server 2012 R2-Netzwerk

In diesem Kapitel:

Die Einstellungen, die Anwender im Windows Server 2012 R2-Netzwerk erhalten, die Anpassungen an den Computern und die Ordnerumleitungen nimmt Windows Server 2012 R2 über Gruppenrichtlinien vor. Sie können die Einstellungen direkt in diesen Richtlinien bearbeiten oder eigene Richtlinien setzen, um bestimmte Einstellungen zu automatisieren.

Mit den Richtlinien in Windows Server 2012 R2 können Sie nicht nur Desktopeinstellungen anpassen, sondern auch sicherheitsrelevante Einstellungen und die Konfiguration von Programmen wie Internet Explorer, Explorer oder Office-Programmen oder die Zuweisung von Sicherheitseinstellungen und Zertifikaten sowie die Konfiguration von Firewallregeln. Für diese Verwaltungsarbeiten stehen die Gruppenrichtlinien zur Verfügung.

Bei der Verwaltung eines Windows Server 2012 R2-Servers sollten Sie sich mit diesen Richtlinien auseinandersetzen, da nahezu alle Automatismen im Windows Server 2012 R2-Netzwerk auf diese Richtlinien aufbauen. Mit diesen lassen sich zahlreiche Einstellungen auf einem Server oder PC automatisch vorgeben. So lässt sich beispielsweise das Verhalten des Internet Explorers oder die Konfiguration der Kennwörter definieren.

Lokale Sicherheitsrichtlinien arbeiten auch unter Windows Server 2012 R2 mit speziellen Registryschlüsseln, 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.

Erste Schritte mit Richtlinien

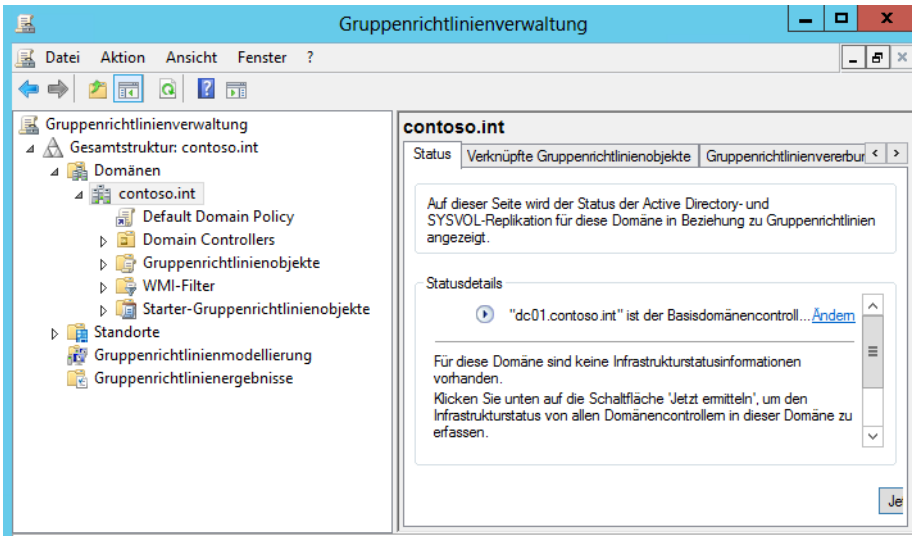
Viele Einstellungen der Gruppenrichtlinien in Windows Server 2012 R2 funktionieren nur auf Clients mit Windows 7/8/8.1 oder Windows Vista, zum Beispiel die Einstellungen der Energieverwaltung, die Sie für Clients konfigurieren. Die meisten Einstellungen übernehmen auch Arbeitsstationen mit Windows Vista und Windows XP.

Beim Zusammenspiel von Windows Server 2012 R2 und Windows 7/8/8.1 lassen sich jetzt auch Gruppenrichtlinien automatisch anwenden, wenn sich ein Client per VPN mit dem Netzwerk verbindet. Dafür sorgt die DirectAccess-Technik in Windows 7/8/8.1 und Windows Server 2012 R2. Damit Sie die Gruppenrichtlinienverwaltung von Windows Server 2012 R2 auf einem Computer mit Windows 8/8.1 ausführen können, benötigen Sie die Remoteserver-Verwaltungstools (RSAT), die Sie bei Microsoft herunterladen können (siehe Kapitel 3 und 4).

Über diese Tools lassen sich unter anderem die Richtlinien verwalten. Achten Sie aber darauf, möglichst keine Änderungen an den Einstellungen der Standardrichtlinien von Windows Server 2012 R2 vorzunehmen. Damit Richtlinien angewendet werden, benötigen Clients keine zusätzliche Software, der Beitritt zur Windows Server 2012 R2-Domäne reicht aus.

Sie können Gruppenrichtlinien über die Windows-PowerShell verwalten. Dazu steht das PowerShell-Modul *GroupPolicy* zur Verfügung, das Sie mit dem Befehl *Import-Module GroupPolicy* in Windows-PowerShell ISE importieren können. PowerShell 3.0 ist in Windows Server 2012 R2 automatisch installiert, ebenso die grafische Oberfläche (ISE, Integrated Scripting Environment). Die Konfiguration der Gruppenrichtlinien nehmen Sie mit dem Verwaltungsprogramm *Gruppenrichtlinienverwaltung* vor. Sie finden dieses über das Menü *Tools*. Über das Kontextmenü einer Richtlinie können Sie deren Bearbeitung starten und Einstellungen in der Richtlinie ändern.

Abbildg. 19.1 Verschiedene Richtlinien in Windows Server 2012 R2



Sie starten die Gruppenrichtlinienverwaltung auch über *gpedit.msc*. Nach der Installation von Active Directory in Windows Server 2012 R2 gibt es bereits zwei Gruppenrichtlinienobjekte. Diese Richtlinien sollten Sie möglichst nicht verändern. Wenn Sie neue Einstellungen durchführen möchten, sollten Sie möglichst eigene Gruppenrichtlinien definieren und die Einstellungen der Standardrichtlinien so belassen, wie sie sind.

Viele Einstellungen, die Sie bei den Benutzern und Clients vornehmen, zum Beispiel Energieverwaltung oder Ordnerumleitung, nimmt Windows Server 2012 R2 über Richtlinien vor. Bei der Verwendung eigener Einstellungen bietet es sich an, möglichst eigene Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) zu erstellen. Nach dem Start verbindet sich die Konsole der Gruppenrichtlinienverwaltung (Group Policy Management Console, GPMC) automatisch mit der Windows Server 2012 R2-Domäne. Über das Kontextmenü einer Richtlinie und der Auswahl von *Bearbeiten* startet der Gruppenrichtlinienverwaltungs-Editor. Dieser besteht aus zwei Hälften. Auf der linken Seite können Sie auswählen, für welchen Bereich Sie Einstellungen vornehmen wollen:

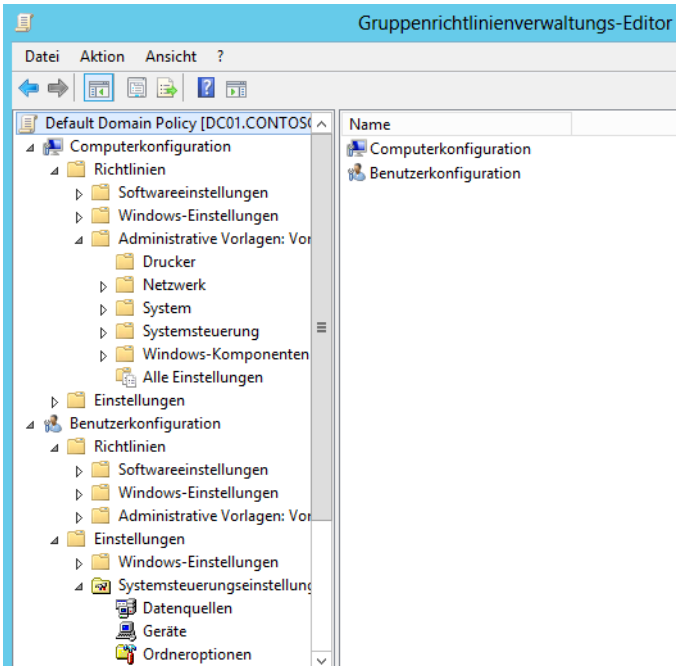
- Die Einstellungen unter *Computerkonfiguration* werden auf Server und PCs angewendet, sobald diese gestartet werden
- Die Einstellungen unter *Benutzerkonfiguration* werden auf die Profile der einzelnen Anwender angewendet, sobald sich diese beim Server anmelden

Die Einstellungen sind jeweils in drei weitere Einträge unterteilt:

- **Softwareeinstellungen** Über diesen Eintrag können Sie Applikationen automatisch verteilen lassen, deren Installation auf *.msi*-Dateien beruhen
- **Windows-Einstellungen** In diesem Bereich befinden sich die meisten Einstellungen, die Sie vornehmen können. Für jede Einstellung finden Sie auch zahlreiche Erklärungen.
- **Administrative Vorlagen** Hier finden sich Möglichkeiten zur Einstellung und Automatisierung von Windows Server 2012 R2 und Windows Vista/Windows 7/8/8.1. Sie können Einstellungen im 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 Änderungen vornehmen, die an die Benutzer bei der Benutzerkonfiguration oder die Server bei der Computerkonfiguration weitergegeben werden.

Abbildg. 19.2 Richtlinienverwaltung in Windows Server 2012 R2

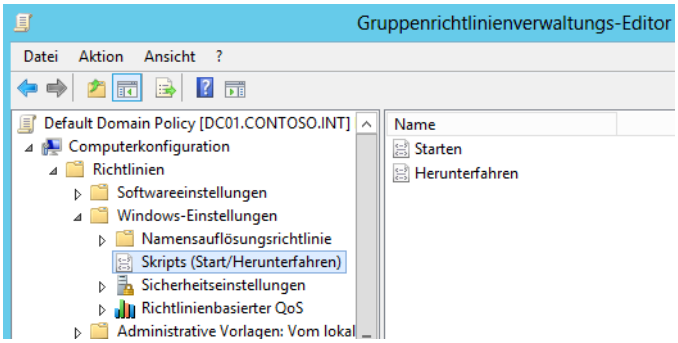


Die Gruppenrichtlinien ermöglichen auch Einstellungen, bei denen PowerShell-Skripts beim Starten/Herunterfahren bzw. An- oder Abmelden immer vor normalen Skripts ablaufen. Sie finden diese Einstellungen über *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Skripts*. Mehr zu diesem Thema erfahren Sie in Kapitel 18. Interessant sind auch die erweiterten Starter-Gruppenrichtlinienobjekte. Bei diesen Richtlinien handelt es sich um schreibgeschützte Vorlagen, die Sie bei der Erstellung von neuen Richtlinien nutzen können. Wir gehen in diesem Kapitel noch ausführlicher auf diese Themen ein.

Windows Server 2012 R2 unterstützt als Neuerung zum Beispiel die Konfiguration der Energiesparoptionen für Windows Vista und Windows 7/8/8.1. 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 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 2012 R2, zusammen mit Windows Vista und Windows 7/8/8.1, 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.

Abbildg. 19.3 Auch Skripts lassen sich in Gruppenrichtlinien verwalten



Eine Einstellung kann verschiedene Zustände annehmen. Diese können Sie direkt in den einzelnen Einstellungen konfigurieren. Viele Einstellungen entsprechen folgendem Prinzip:

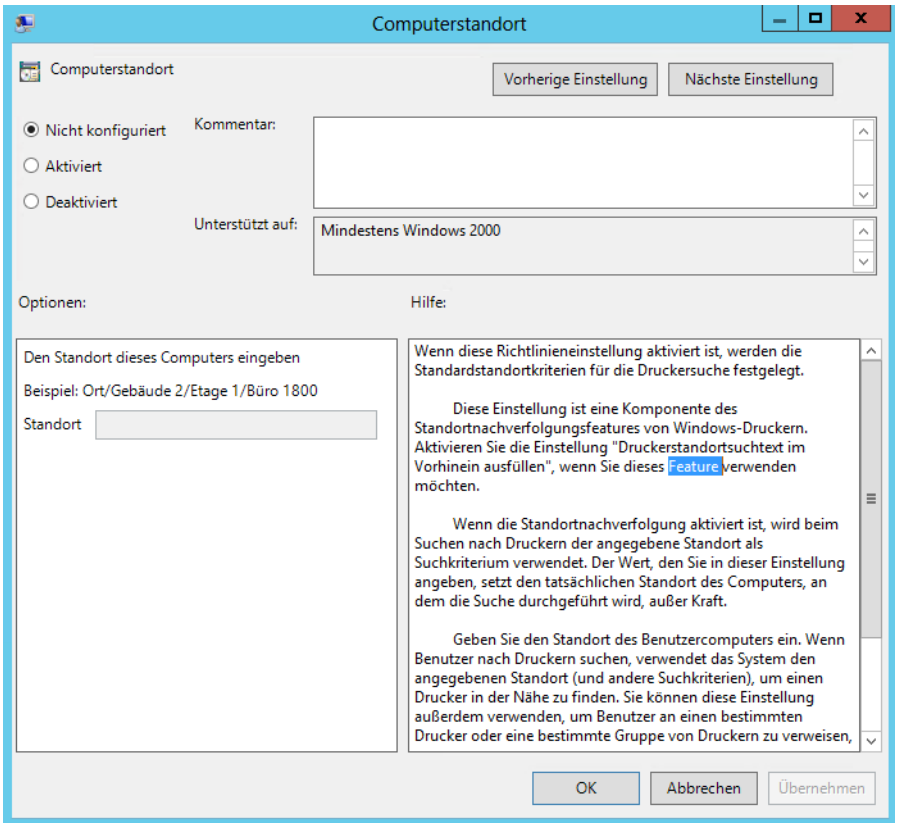
- **Aktiviert** Bei dieser Einstellung wird die Konfiguration auf das Zielobjekt angewendet und weitergegeben
- **Deaktiviert** Bei dieser Einstellung wird die Konfiguration der Gruppenrichtlinie auf dem Server auf den Standard zurückgesetzt
- **Nicht konfiguriert** Bei dieser Einstellung wird die lokale Einstellung des Clients beibehalten und durch die Gruppenrichtlinie nicht geändert

Im Bereich *Hilfe* finden Sie eine ausführliche Erklärung zu der Einstellung und deren Auswirkungen. Bevor Sie eine Einstellung aktivieren, sollten Sie sich möglichst immer die Erklärung genau durchlesen. Bietet eine Richtlinie weitere Einstellungen, können Sie diese entsprechend über Menüs, Dropdownfelder oder die Eingabe von Werten konfigurieren.

Durch die Unterstützung der Verwaltung von USB-Sticks und anderen tragbaren Datenträgern in den Gruppenrichtlinien ist es nicht mehr notwendig, den gesamten USB-Port eines Servers oder PCs zu sperren, damit Anwender keine USB-Sticks mehr anschließen können.

Windows Server 2012 R2 und Windows Vista/Windows 7/8/8.1 verwenden sogenannte Geräteidentifikationsstrings und Gerätesetupklassen, um die angeschlossene Hardware 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 Anwender einen USB-Stick an einem PC anschließen, 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 sich USB-Festplatten ab einer gewissen Größe komplett aussperren lassen. Sie können auch bestimmte USB-Sticks erlauben und andere verbieten.

Abbildg. 19.4 Einstellungsmöglichkeiten in Gruppenrichtlinien



Beim Anschluss eines USB-Geräts überträgt dieses ausführliche generische Informationen, mit denen Windows auch zusätzliche Funktionen identifizieren kann. Dies ermöglicht einem Unternehmen zum Beispiel, firmeneigene USB-Sticks zuzulassen, aber private Sticks zu sperren. Erwerben Sie zum Beispiel spezielle Sticks, können Sie diese explizit zulassen. Natürlich könnten sich Anwender den gleichen Stick besorgen, allerdings schaffen Sie auf diese Weise schon eine gewisse Grundsicherheit. So lässt sich vermeiden, dass Mitarbeiter Daten aus dem Unternehmen schmuggeln können oder private Daten in das Netzwerk kopieren. Grundsätzlich können in Windows folgende Einstellungen über Richtlinien vorgenommen werden:

- Sie können die Geräteinstallation verhindern, wenn die Installation des Geräts nicht den Richtlinien des Unternehmens entspricht
- Administratoren können gesetzte Richtlinien überschreiben
- Die Installation von Geräten lässt sich auch auf Basis der Geräte-ID oder der Geräteklasse erlauben oder verbieten. So können Sie selbst entscheiden, ob eine Positiv- oder Negativliste für Sie einfacher zu implementieren ist.

Gruppenrichtlinien verknüpfen Sie mit einem Container in der Windows Server 2012 R2-Domäne. 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 im Kontextmenü den Befehl *Domänen anzeigen* aus. Danach können Sie alle Domänen aktivieren, die in Ihrer Gesamtstruktur vorhanden sind.

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*.

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. Sie können in der GPMC auch neue Organisationseinheiten erstellen und Verknüpfungen zwischen den neuen OUs und Gruppenrichtlinien.

Gruppenrichtlinien-Einstellungen effizient einsetzen

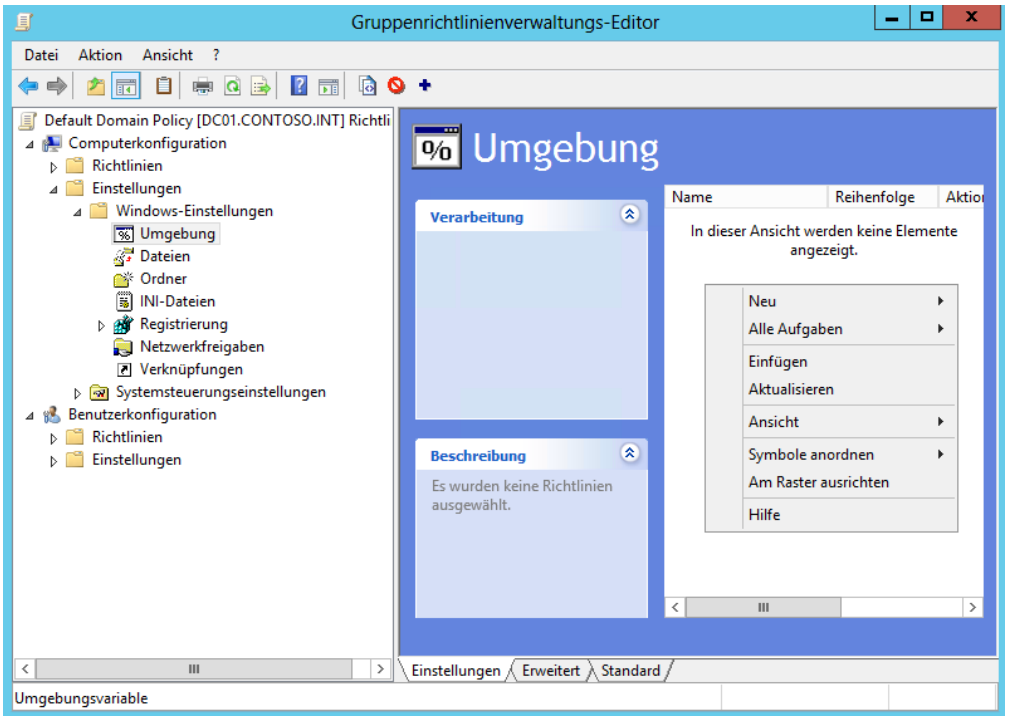
Ein wichtiger Punkt im Bereich der Richtlinienverwaltung ist der Knoten *Einstellungen (Preferences)* unter den Richtlinieneinstellungen, wenn Sie die Bearbeitung einer Richtlinie in der Gruppenrichtlinienverwaltung starten.

Über diese Vorgaben ermöglichen Sie Einstellungsvorschläge, die Anwender aber nicht zwingend übernehmen müssen. Das heißt, Sie geben bestimmte Einstellungen vor, die jedoch vom Anwender geändert werden können. Die Einstellungen setzt das Betriebssystem um, lässt aber Anwendern die Möglichkeit, Einstellungen selbst zu ändern.

Richtlinien sind wiederum sind feste Vorgaben, die Anwender auch zwingend übernehmen müssen. Eine Änderung auf dem Client ist nicht möglich, da die Richtlinie die entsprechenden Einstellungen deaktiviert. Setzen Sie in den Gruppenrichtlinien Anpassungen um, können Anwender auf ihren Computern entweder gar keine Änderungen in diesem Bereich mehr vornehmen, da diese abgeblendet dargestellt sind, oder die Einstellungen werden beim Neustart wieder durch die Richtlinien überschrieben.

Über den Knoten *Einstellungen* lassen sich hingegen Vorgaben festlegen, welche von den Clientcomputern auch übernommen werden, genauso wie herkömmliche Richtlinien. Allerdings können Anwender diese Einstellungen auf ihre Bedürfnisse hin anpassen. Nehmen Sie Einstellungen in den Preferences vor, bleiben diese auch dann auf den Rechnern erhalten, wenn Sie sie in der Richtlinie wieder entfernen.

Abbildg. 19.5 Verwenden von Einstellungen in Gruppenrichtlinien



Anwender können solche Einstellungen aber selbst lokal anpassen. Nehmen Sie im Knoten *Einstellungen* im Gruppenrichtlinienverwaltungs-Editor Einstellungen vor, verwendet dieser Editor die gleiche grafische Oberfläche wie die entsprechende Einstellung auf dem Computer selbst.

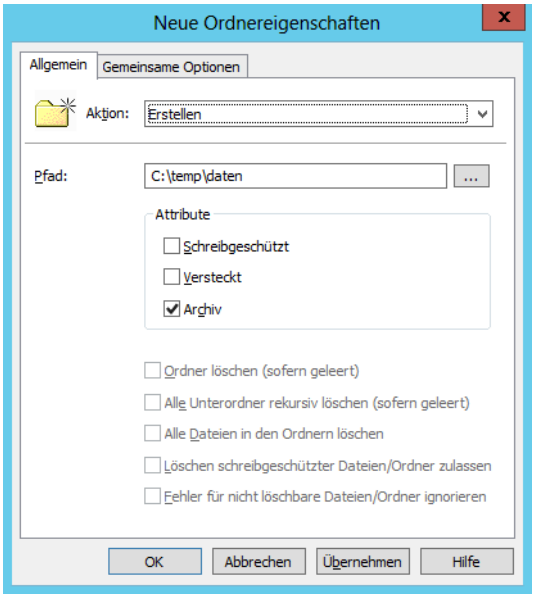
Sie wählen die Einstellungen aus, klicken mit der rechten Maustaste in den Ergebnisbereich rechts und wählen im Kontextmenü den Eintrag *Neu*. Anschließend können Sie Einstellungen vorgeben, welche an die Computer übergeben werden. Über die Einstellungen können Sie beispielsweise auch neue Ordner oder Dateien im Dateisystem auf den Rechnern anlegen lassen.

Über die Registerkarte *Gemeinsame Optionen* einer solchen Preference können Sie darüber hinaus mit Filtern genau auswählen, auf welche Art von Rechnern die Richtlinie angewendet werden soll. Über diese Einstellungen können Sie beispielsweise auch Netzwerkfreigaben verbinden lassen. Die Übernahme dieser Einstellungen funktioniert neben Windows 7/8/8.1 auch bei Windows Vista und Windows XP. Die Einstellungen sind alle selbsterklärend. Um Preferences zu erstellen, gehen Sie folgendermaßen vor:

1. Starten Sie die Gruppenrichtlinienverwaltung.
2. Klicken Sie mit der rechten Maustaste auf *Gruppenrichtlinienobjekte* und wählen Sie im Kontextmenü den Eintrag *Neu*.
3. Erstellen Sie eine neue Gruppenrichtlinie, klicken Sie diese mit der rechten Maustaste an und wählen Sie *Bearbeiten*.
4. Klicken Sie unter *Computerkonfiguration* oder *Benutzerkonfiguration* auf *Einstellungen*.

5. Wählen Sie die Einstellung aus, die Sie auf den Rechnern vorgeben, auf die Sie die Richtlinie anwenden wollen.
6. Klicken Sie mit der rechten Maustaste im rechten Bereich des Fensters und wählen Sie im Kontextmenü den Eintrag *Neu*.
7. Erstellen Sie die Einstellung und nehmen Sie Ihre Änderungen vor.

Abbildg. 19.6 Erstellen einer neuen Einstellung



Wählen Sie auf der Registerkarte *Gemeinsame Optionen* über *Zielgruppenadressierung* die Filterung aus, auf deren Basis Sie die Durchführung der Richtlinie starten wollen. Anschließend müssen Sie die neue Richtlinie mit den Einstellungen noch mit der Domäne oder einer bestimmten Gruppe verknüpfen. Wie das geht, zeigen wir Ihnen in den folgenden Abschnitten zur Verwaltung von herkömmlichen Gruppenrichtlinien.

Gruppenrichtlinien verwalten

Wenn Sie mit der Verwaltung von Gruppenrichtlinien beginnen, sollten Sie zunächst zwei Definitionen verstehen, die oft verwechselt werden. Beide Bereiche tauchen auch in der Gruppenrichtlinienverwaltung auf:

- Gruppenrichtlinienobjekte (Group Policy Objects, GPOs)
- Gruppenrichtlinienverknüpfungen

Allgemein wird oft von Gruppenrichtlinien gesprochen. Damit sind meist die GPOs gemeint. Ein GPO ist eine Gruppenrichtlinie, in der Einstellungen vorgenommen und gespeichert sind. Diese Einstellungen legen für Benutzer-PCs oder Benutzerkonten fest, wie sich die Systeme verhalten, zum Beispiel die automatische Konfiguration des Internet Explorers.

Diese Einstellungen sind innerhalb eines Containers, der GPO, gespeichert. Damit diese Einstellungen jedoch auch angewendet werden, muss die GPO mit Organisationseinheiten oder einer ganzen Domäne verknüpft sein. Erst wenn eine GPO mit einer Organisationseinheit oder der ganzen Domäne verknüpft ist, wenden die Computer in der Domäne die Einstellungen innerhalb der GPO auf die entsprechende OU oder die ganze Domäne an. In diesem Fall spricht man von Gruppenrichtlinienverknüpfungen. Ein GPO kann nicht nur mit einer OU verknüpft sein, sondern mit mehreren. Wenn Sie Einstellungen in einem GPO ändern, wendet die GPO diese Änderungen auf alle verknüpften OUs an. Ändern Sie aber Einstellungen in einem GPO ab, das noch nicht mit einer OU verknüpft ist, übernehmen Computer auch keinerlei Änderungen. Diese erfolgen erst dann, wenn das GPO verknüpft ist.

Neue Gruppenrichtlinie erstellen

In den folgenden Abschnitten zeigen wir Ihnen die typischen Aufgaben, die Sie in der Gruppenrichtlinienverwaltung durchführen können, anhand 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

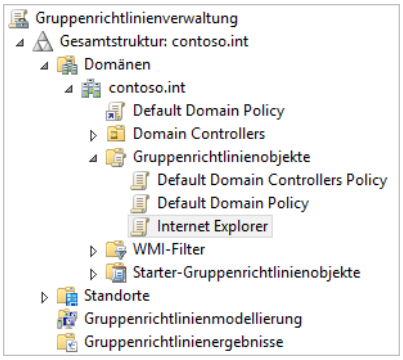
Um ein neues GPO zu erstellen, klicken Sie in der Gruppenrichtlinienverwaltung auf den Knoten *Gruppenrichtlinienobjekte* und wählen im Kontextmenü den Befehl *Neu* aus. Geben Sie danach dem GPO einen passenden Namen, der wiedergibt, welche Einstellungen mit diesem GPO verteilt werden.

In diesem Beispiel erläutern wir Ihnen die Verteilung der Internet Explorer-Einstellungen. Sie können beliebige Einstellungen durchführen oder parallel zu den Internet Explorer-Einstellungen weitere Definitionen vorgeben. Weisen Sie daher dem GPO eine Bezeichnung wie »Internet Explorer« oder einen ähnlichen Namen zu. Das GPO wird dann unter dem Menüpunkt *Gruppenrichtlinienobjekte* angezeigt. Hier finden Sie alle GPOs, die Sie erstellt haben oder die Windows Server 2012 R2 bereits automatisch angelegt hat.

Neu seit Windows Server 2012 R2 sind an dieser Stelle die Starter-Gruppenrichtlinienobjekte, die als eine Art Vorlage dienen können. Erstellen Sie eine neue Richtlinie, können Sie eine Starter-Richtlinie auswählen und deren bereits vorhandenen Einstellungen in die neue Richtlinie übernehmen. Klicken Sie auf den Knoten *Starter-Gruppenrichtlinienobjekte*, können Sie in Windows Server 2012 R2 Vorlagen erstellen lassen.

Nach der Erstellung des Gruppenrichtlinienobjekts (GPO) ist dieses in der Windows Server 2012 R2-Domäne vorhanden. Allerdings gibt die GPO keine Einstellungen weiter, da das GPO noch nicht verknüpft ist und keinerlei Einstellungen enthält.

Abbildg. 19.7 Erstellen und Verwalten von neuen Gruppenrichtlinienobjekte



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 ist und weitere Einstellungen im Internet Explorer.

Klicken Sie im Knoten *Gruppenrichtlinienobjekte* mit der rechten Maustaste auf das neu erstellte GPO und wählen Sie im Kontextmenü den Eintrag *Bearbeiten* aus. Damit öffnet sich der Gruppenrichtlinienverwaltungs-Editor, mit dessen Hilfe Sie die Einstellungen innerhalb des GPOs vornehmen. Der Gruppenrichtlinienverwaltungs-Editor besteht aus zwei Hälften. Auf der linken Seite können Sie auswählen, für welchen Bereich Sie Einstellungen vornehmen wollen. Gruppenrichtlinieneinstellungen nehmen Sie über den Knoten *Richtlinien* vor.

- Die Einstellungen unter *Computerkonfiguration* wenden PCs beim Starten an
- Die Einstellungen unter *Benutzerkonfiguration* wendet Windows an, wenn sich ein Benutzer am PC anmeldet

Wenn Sie sich durch die Knoten auf der linken Seite klicken, sehen Sie auf der rechten Seite die Einstellungen, 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.

Eine der vielen möglichen Einstellungen einer Gruppenrichtlinie ist die Konfiguration der Internet Explorer-Einstellungen der Rechner in der Windows Server 2012 R2-Domäne. Sie finden diese Einstellung in der Konsolenstruktur unter *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Internet Explorer*. Klicken Sie diesen Eintrag an, können Sie auf der rechten Seite wichtige Einstellungen vornehmen, um die Clients zu konfigurieren.

Wollen Sie die Möglichkeit deaktivieren, Änderungen im Internet Explorer vorzunehmen, erledigen Sie das am besten über den Knoten *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Internet Explorer* in der Konsolenstruktur. An dieser Stelle finden Sie zahlreiche Einstellmöglichkeiten für den Internet Explorer. Wichtig ist hier, die vier folgenden Einstellungen zu aktivieren:

- *Assistenten für Internetzugang deaktivieren*
- *Änderung der Verbindungseinstellungen deaktivieren*

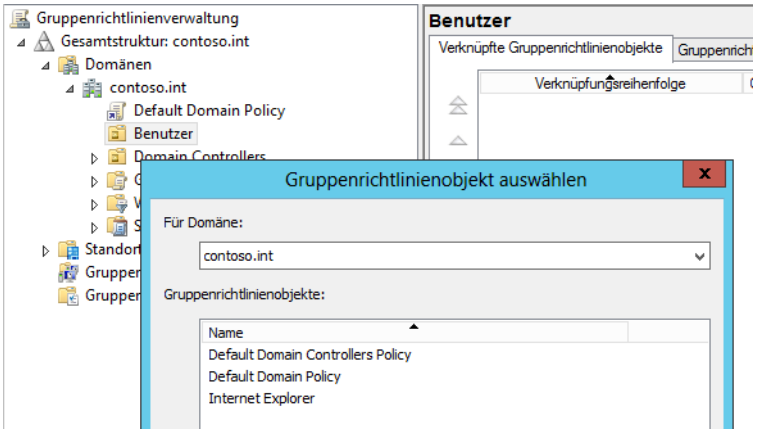
- *Änderung der Proxyeinstellungen deaktivieren*
- *Änderung der Einstellungen für automatische Konfiguration deaktivieren*

Setzen Sie die Einstellung einer Gruppenrichtlinie auf *Aktiviert*, bedeutet das die Aktivierung dieser Einstellung. Wenn in dieser Einstellung aber eine Windows-Funktion deaktiviert wird, ist die Funktion direkt auf dem PC deaktiviert. Durch die Aktivierung einer Einstellung im GPO bewirken Sie also eine Deaktivierung der entsprechenden Funktion in Windows. Neben den Internet Explorer-Einstellungen können Sie in Ihrer Richtlinie natürlich noch beliebige viele weitere Einstellungen vornehmen.

GPO mit einem Container verknüpfen

Damit die Einstellungen in der Gruppenrichtlinie angewendet werden, müssen Sie diese mit einer OU oder der ganzen Domäne 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 im Kontextmenü den Eintrag *Vorhandenes Gruppenrichtlinienobjekt verknüpfen* aus. Sie können auch direkt in der Gruppenrichtlinienverwaltung neue Organisationseinheiten erstellen.

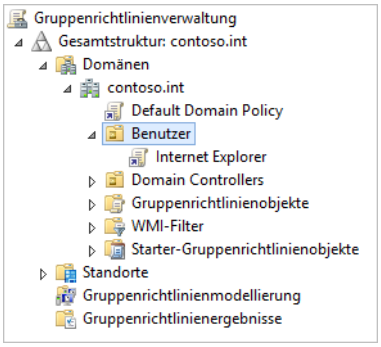
Abbildg. 19.8 Verknüpfen einer GPO mit einem Container im Windows Server 2012 R2-Netzwerk



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*. Nach der erfolgreichen Auswahl wird die Verknüpfung des GPOs unterhalb der Domäne beziehungsweise der entsprechenden Organisationseinheit 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 Gruppenrichtlinienverwaltung erkennen Sie durch die übersichtliche Baumstruktur unter jedem Container, welche Gruppenrichtlinien verknüpft sind. 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. 19.9 Anzeigen der verknüpften GPOs



Gruppenrichtlinien erzwingen und Priorität erhöhen

Da Sie mehrere GPOs mit einer OU verknüpfen können, lässt sich auch die Priorität von Richtlinien so setzen, dass eine Richtlinie gezwungenermaßen immer vor einer anderen gestartet wird. Außerdem besteht die Möglichkeit, eine Einstellung in einer Richtlinie zu setzen und in einer anderen Richtlinie wieder zurückzunehmen, zum Beispiel in einer untergeordneten OU.

Sie haben auch die Möglichkeit, die Erzwingung einer Einstellung zu veranlassen. Das heißt, auch wenn in untergeordneten OUs eine Einstellung wieder rückgängig gemacht wird, bleibt die Einstellung so gesetzt, wie in der erzwungenen Richtlinie konfiguriert. Sie können zum Beispiel die Einstellung aktivieren, dass nach gewisser Zeit der Bildschirmschoner auf den Arbeitsstationen 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.

Falls der Bildschirm nicht gesperrt ist, können ungehindert andere Anwender unter dem Namen des angemeldeten Benutzers Aktionen durchführen. Sie finden die Einstellungen für Bildschirmschoner unter *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Systemsteuerung/Anpassung*. Zur Konfiguration können Sie entweder eine neue GPO erstellen oder eine bereits vorhandene konfigurieren. Die Standardrichtlinien im Windows Server 2012 R2-Netzwerk sollten Sie möglichst auch bei einer solchen Konfiguration nicht ändern. Konfigurieren Sie die folgenden Einstellungen:

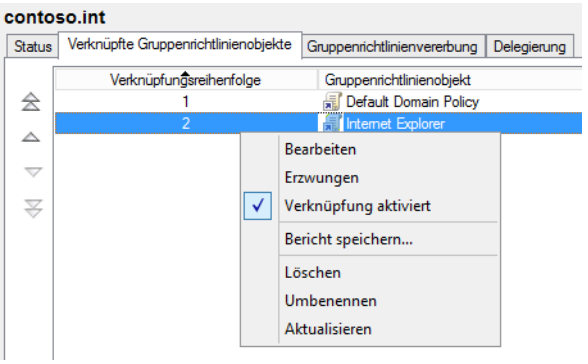
- *Bildschirmschoner aktivieren* auf *Aktiviert*
- *Kennwortschutz für den Bildschirmschoner verwenden* ebenfalls auf *Aktiviert*
- *Zeitlimit für Bildschirmschoner* auf *Aktiviert* und als Einstellung 600 Sekunden bis zur Aktivierung

Haben Sie die gewünschten Eintragungen vorgenommen, können Sie den Gruppenrichtlinienverwaltungs-Editor wieder schließen. Verknüpfen Sie die erstellte Richtlinie wieder mit der Domäne oder einer OU.

Wenn Sie die Richtlinie erstellt und verknüpft haben, klicken Sie die Domäne in der Gruppenrichtlinienverwaltung an. Auf der rechten Seite sehen Sie alle Gruppenrichtlinien, die direkt mit der Domäne verknüpft sind. Markieren Sie die Verknüpfung der Bildschirmschoner-Richtlinie auf der

rechten Seite der Gruppenrichtlinienverwaltung und klicken Sie auf die Pfeile, bis die Verknüpfung ganz oben angeordnet ist. Dadurch ist sichergestellt, dass diese Verknüpfung und die Einstellungen des verknüpften GPOs zuerst angewendet werden.

Abbildg. 19.10 Priorisieren 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.

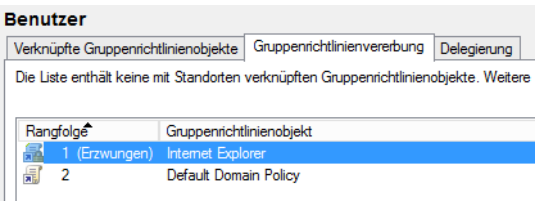
Für Benutzer innerhalb eines Containers gilt immer die zuletzt angewendete Richtlinie. Wenn also in der Domänenrichtlinie eine Einstellung gesetzt wird, die in der OU des Benutzers zurückgenommen wird, gilt das auch für den Benutzer. Wenn Domänenadministratoren sicherstellen wollen, dass gewisse Gruppenrichtlinien 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 den Eintrag *Erzwungen* aus.

Nach der Auswahl erscheint eine Meldung, in der Sie das Erzwingen der Richtlinie bestätigen müssen. Nach der Bestätigung wird die Richtlinie als *Erzwungen* angezeigt. Dadurch stellen Sie sicher, dass diese Einstellungen für alle Benutzer der Domäne Gültigkeit haben und in keiner OU aufgehoben werden können.

Wenn Sie anschließend eine untergeordnete OU aktivieren, sehen Sie auf der rechten Seite auf der Registerkarte *Gruppenrichtlinienvererbung*, dass die Richtlinie auch hier als *Erzwungen* angezeigt wird. Das heißt, die Anwendung dieser Richtlinie kann nicht verhindert werden.

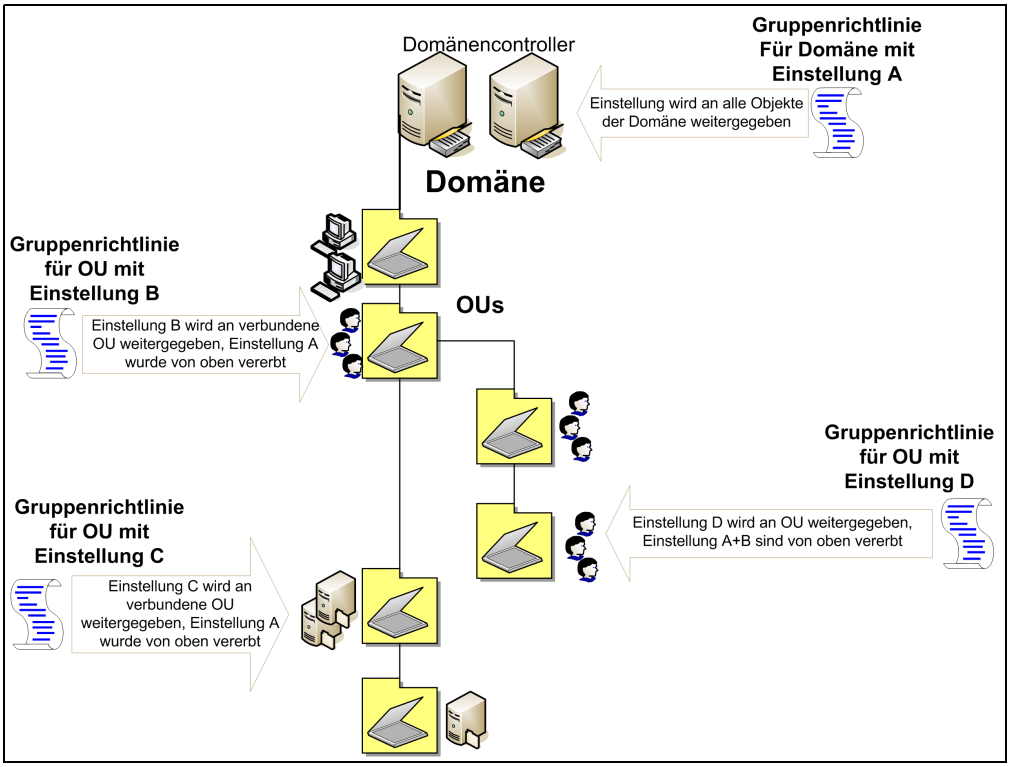
Abbildg. 19.11 Anzeige von erzwungenen Richtlinien in der Gruppenrichtlinienvererbung



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 Einstellungen weitergeben wollen, in einer anderen OU aber nicht, können Sie in dieser OU die Verwendung der Richtlinie deaktivieren, auch wenn diese mit der ganzen Domäne verknüpft ist.

Abbildg. 19.12 Gruppenrichtlinien vererben sich in Domänen nach unten

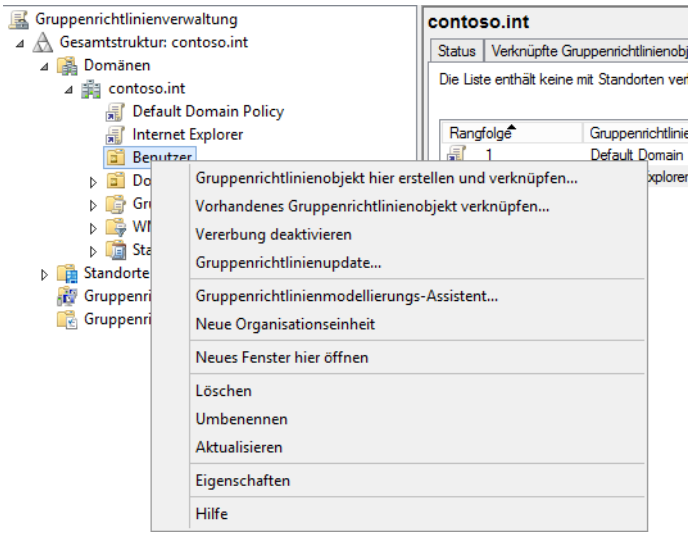


Die Grenzen von Gruppenrichtlinien stellen immer Domänen dar. Über Domänen hinweg lassen sich keine Gruppenrichtlinien festlegen.

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. 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 Eintrag *Vererbung deaktivieren* aus.

Abbildg. 19.13 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.

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. Achten Sie aber im Windows Server 2012 R2-Netzwerk darauf, dass Sie bei der Deaktivierung der Vererbung die Windows Server 2012 R2-Richtlinien manuell mit der OU verknüpfen. Erzwungene Gruppenrichtlinien lassen sich auch durch die Deaktivierung der Vererbung nicht deaktivieren. Diese Richtlinien bleiben immer aktiv.

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.

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*-Ordner 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* [Ms179-K19-01]. 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. Nach der Erstellung des zentralen Speicherorts 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 Eingabeaufforderung.
2. Kopieren Sie alle sprachneutralen Dateien (**.admx*) in den zentralen Ordner *\PolicyDefinitions*.
3. Kopieren Sie alle sprachspezifischen Dateien (**.adml*) in die entsprechenden Unterordner.

Gruppenrichtlinien testen und Fehler beheben

Im Anschluss an die Konfiguration und Anbindung von Richtlinien daran können Sie die Gruppenrichtlinie auf einer Windows-Arbeitsstation mit *gpupdate /force* in der Eingabeaufforderung übertragen. Alternativ können Sie auch die Arbeitsstation neu starten. Sie können auch den Bildschirmschoner in der Gruppenrichtlinie festlegen, allerdings dürfen die Anwender auch diesen dann nicht mehr verändern.

Beim Einsatz von Gruppenrichtlinien ist es notwendig, zu überprüfen, ob Einstellungen auf den Clients überhaupt verwendet werden und wie sich diese auswirken. Eine Fehlersuche bei Gruppenrichtlinien ist ebenfalls eine häufige Aufgabe, wenn bestimmte Einstellungen oder ganze Richtlinien nicht mehr wirksam sind. Viele Einstellungen der Gruppenrichtlinien in Windows Server 2012 R2 funktionieren nur auf Clients mit Windows 7/8/8.1, zum Beispiel die Einstellungen von BranchCache (siehe Kapitel 22) und DirectAccess (siehe Kapitel 32). Die meisten Einstellungen übernehmen aber auch Arbeitsstationen mit Windows Vista und teilweise auch Windows XP.

Sie sehen in der Beschreibung der meisten Richtlinien, mit welchen Betriebssystemen diese kompatibel sind. Beim Zusammenspiel von Windows Server 2012 R2 und Windows 7/8/8.1 lassen sich jetzt auch Gruppenrichtlinien automatisch anwenden, wenn sich ein Client per VPN mit dem Netzwerk verbindet.

Dazu ist noch nicht mal eine direkte VPN-Einwahl notwendig, denn Windows 7 kann Netzwerkverkehr kapseln und über das Internet zu einem veröffentlichten Server senden. Ein auf diese Weise angebundener Computer verhält sich so, als wäre er im lokalen Netzwerk positioniert. Dafür sorgt die DirectAcess-Technik in Windows 7/8/8.1 und Windows Server 2012 R2. Das heißt, Gruppenrichtlinien lassen sich jetzt auch mit Heimarbeitsplatzrechnern anwenden, was die Überprüfung aber teilweise erschwert.

Sie haben auch die Möglichkeit, die Verwaltungswerkzeuge von Gruppenrichtlinien, also vor allem die Gruppenrichtlinienverwaltungskonsole auf einem Clientrechner zu installieren. Der Vorteil dabei ist, dass Sie Testtools nicht auf Servern installieren müssen, sondern Arbeitsstationen des Administrators verwenden können. Auf einem Admin-PC sind Zusatztools wesentlich besser aufgehoben als auf einem Server.

Damit Sie die Gruppenrichtlinienverwaltung von Windows Server 2012 R2 auf einem Computer mit Windows 8/8.1 ausführen können, benötigen Sie die Remoteserver-Verwaltungstools (RSAT), die Sie bei Microsoft herunterladen können (siehe Kapitel 3 und 4). Über diese Tools lassen sich unter anderem die Richtlinien verwalten.

Damit Clientcomputer Richtlinien anwenden, benötigen PCs grundsätzlich keine zusätzliche Software. Entweder ist der Computer kompatibel mit der entsprechenden Richtlinieneinstellung oder nicht. Windows 7/8/8.1 und Windows Server 2012 R2 bieten die Möglichkeit, Gruppenrichtlinien über die Windows-PowerShell zu verwalten. Dazu steht das neue PowerShell-Modul *GroupPolicy* zur Verfügung, das Sie mit dem Befehl *Import-Module GroupPolicy* in die Windows-PowerShell ISE oder einer normalen PowerShell-Sitzung importieren können. Die wichtigsten Cmdlets können Sie sich anzeigen lassen, wenn Sie *Get-Command *gpo** eingeben.

Abbildg. 19.14 Verwalten von Gruppenrichtlinien in der PowerShell

```
PS C:\Users\Administrator> Get-Command *gpo*

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Function        Open-NetGPO                                        NetSecurity
Function        Save-NetGPO                                        NetSecurity
Cmdlet          Backup-GPO                                         GroupPolicy
Cmdlet          Copy-GPO                                           GroupPolicy
Cmdlet          Get-GPO                                            GroupPolicy
Cmdlet          Get-GPOReport                                      GroupPolicy
Cmdlet          Get-GPStarterGPO                                   GroupPolicy
Cmdlet          Import-GPO                                         GroupPolicy
Cmdlet          New-GPO                                            GroupPolicy
Cmdlet          New-GPStarterGPO                                   GroupPolicy
Cmdlet          Remove-GPO                                         GroupPolicy
Cmdlet          Rename-GPO                                         GroupPolicy
Cmdlet          Restore-GPO                                        GroupPolicy
Application     chgport.exe
Application     dcgpofix.exe
```

Mit dem Befehl *Help <Cmdlet>* erhalten Sie eine Hilfe zum entsprechenden Cmdlet, zum Beispiel *Help New-GPO*. Für viele Cmdlets gibt es noch die Option *Help <Cmdlet> –Detailed*. Dieser Befehl bietet noch mehr Informationen. Mit dem Befehl *Help <Cmdlet> –Examples* lassen sich Beispiele für den Befehl anzeigen. Auch das funktioniert für alle Befehle in der PowerShell.

Um Gruppenrichtlinien lokal zu testen, können Sie die Gruppenrichtlinie auf einer Windows-Arbeitsstation mit *gpupdate /force* in der Eingabeaufforderung übertragen. Alternativ können Sie auch die Arbeitsstation neu starten. Wenn Sie die Einstellungen korrekt vorgenommen haben, können Sie in feststellen, ob die Arbeitsstation oder der Server die Richtlinie angewendet hat.

Abbildg. 19.15 Gruppenrichtlinien manuell übernehmen

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.

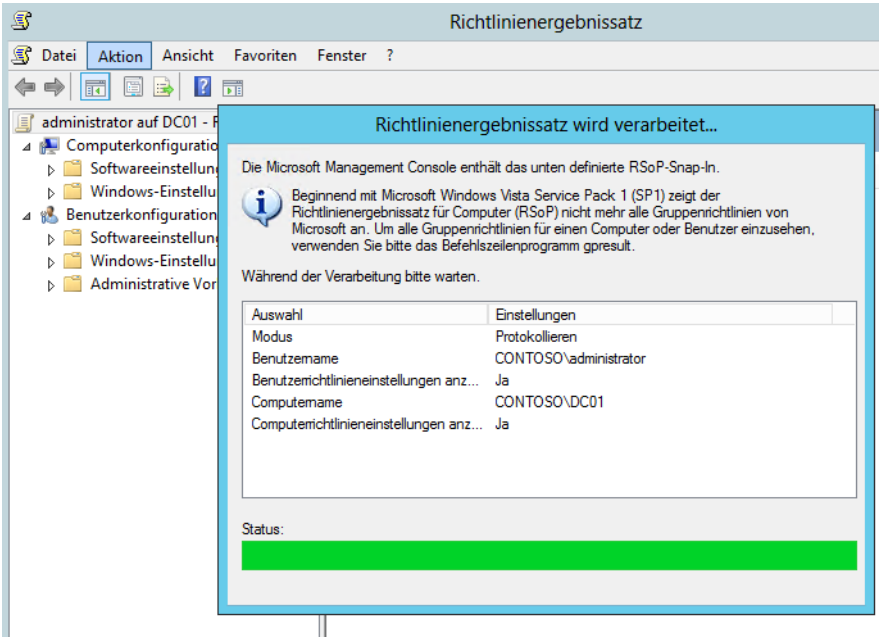
Falls Gruppenrichtlinien nicht funktionieren, können die Ursachen sehr unterschiedlich sein. Sie sollten Schritt für Schritt untersuchen, wo das Problem liegen könnte. Legen Sie am besten für die unterschiedlichen Einstellungen verschiedene Gruppenrichtlinien an und verknüpfen Sie diese mit der entsprechenden OU oder der ganzen Domäne. Bei der Überprüfung helfen noch folgende Punkte:

- Stellen Sie sicher, dass die Clients den DNS-Server verwenden, auf dem die SRV-Records von Active Directory gespeichert sind, also den Windows Server 2012 R2-Server
- Überprüfen Sie mit Nslookup in der Eingabeaufforderung, ob auf den Clients der Windows Server 2012 R2-Server 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? Dies ist nicht ohne Weiteres möglich.
- Stimmt die Vererbung? In welcher Reihenfolge starten die Gruppenrichtlinien?
- Haben Sie etwas an der standardmäßigen Vererbung der Richtlinie verändert?
- Haben Sie irgendwo *Erzwungen* oder *Vererbung deaktivieren* aktiviert?
- Geben Sie auf dem PC in der Eingabeaufforderung als angemeldeter Benutzer *gpresult > gp.txt* ein, um sich das Ergebnis der Richtlinie anzeigen zulassen

Das Windows-MMC-Snap-In *Richtlinienergebnissatz* bietet eine grafische Oberfläche und wertet die angewendeten Richtlinien aus. Sie können sich den Richtlinienergebnissatz auf einer Arbeitsstation über *MMC/Datei/Snap-In hinzufügen/Richtlinienergebnissatz* anzeigen lassen. Eine weitere Möglichkeit ist die Eingabe von *rsop.msc* im Suchfeld des Startmenüs oder der Startseite in Windows Server 2012 R2 und Windows 8/8.1.

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 den Menübefehl *Aktion/Abfrage aktualisieren*.

Abbildg. 19.16 Überprüfen der übertragenen Einstellungen auf einem PC oder Server



Auf der Internetseite *http://www.gruppenrichtlinien.de* [Ms179-K19-02] finden Sie weiterführende Informationen und Tipps rund um den Einsatz von Gruppenrichtlinien und der Fehlerbehebung. Schauen Sie sich auf dieser Seite um, wenn Sie planen, Gruppenrichtlinien einzusetzen.

Auch auf der englischsprachigen Seite *http://www.gpoguy.com* [Ms179-K19-03] finden Sie ausführliche Informationen und Tools für Gruppenrichtlinien. Im deutschsprachigen Gruppenrichtlinien-Forum von Microsoft (*http://social.technet.microsoft.com/Forums/de-DE/gruppenrichtliniende/threads* [Ms179-K19-04]) erhalten Administratoren ebenfalls umfassende Informationen.

Mit Standardmitteln lässt sich nicht ohne Weiteres überprüfen, ob eine gesetzte Gruppenrichtlinie bei den Clients im Netzwerk auch ankommt. Auch ob Clients die Einstellungen übernehmen, die Sie in Gruppenrichtlinien gesetzt haben, ist nicht immer sicher. Der einzige Weg besteht über die Überwachung der Ereignisanzeige und das Auswerten entsprechender Fehlermeldungen.

Administratoren können auf der Website von SDM Software (*http://www.sdmsoftware.com/freeware* [Ms179-K19-05]) das kostenlose Cmdlet *Group Policy Health* herunterladen. Nachdem Sie das Cmdlet in die PowerShell eingebunden haben, können Sie mit dem Befehl *Get-SDMGPHealth –Computer <Computername>* überprüfen, ob gesetzte Gruppenrichtlinien funktionieren. Dazu verbindet sich das Tool mit dem Zielrechner, auf Wunsch auch mit mehreren, und überprüft, ob der Ablauf von Richtlinien auf dem entsprechenden Computer funktioniert.

Nach dem Download installieren Sie das Tool zunächst. Im nächsten Schritt müssen Sie noch eine DLL des Cmdlets registrieren. Auf 64-Bit-Systemen, also vor allem auf Windows Server 2008 R2 und Windows Server 2012 R2, müssen Sie einen anderen Ordner verwenden, als in 32-Bit-Servern wie zum Beispiel mit Windows Server 2008:

1. Öffnen Sie eine Eingabeaufforderung im Ordner *C:\Windows\Microsoft.NET\Framework\v2.0.50727*. Sie können dazu im Explorer den Ordner einfach mit der rechten Maustaste anklicken und dabei die ⇧-Taste gedrückt halten. Anschließend finden Sie im Kontextmenü den Befehl zum Öffnen einer Eingabeaufforderung in diesem Ordner. Setzen Sie ein 64-Bit-System ein, müssen Sie den gleichen Befehl im Ordner *Framework64* durchführen.
2. Um die DLL-Datei zu registrieren, geben Sie den Befehl *installutil "C:\Programm Files (x86)\SDM Software\Group Policy Health Cmdlet\GetSdmGPHealth.dll"* ein. Achten Sie darauf, dass der Befehl nur in einer Eingabeaufforderung funktioniert, die Sie mit Administratorrechten gestartet haben.

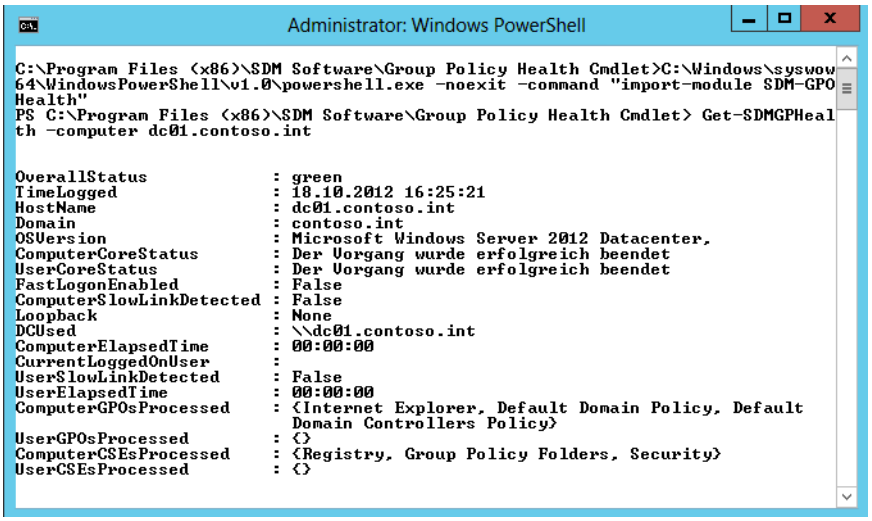
Abbildg. 19.17 Installieren der notwendigen DLL für Group Policy Health Cmdlet

```
C:\Windows\Microsoft.NET\Framework64\v2.0.50727>installutil "C:\Program Files (x
86)\SDM Software\Group Policy Health Cmdlet\GetSDMGPHealth.dll"
Microsoft (R) .NET Framework-Installationsprogramm, Version 2.0.50727.6387
Copyright (c) Microsoft Corporation. Alle Rechte vorbehalten.


Eine transaktive Installation wird ausgeführt.

Die Installationsphase wird gestartet.
Die Protokolldatei enthält den Fortschritt der Assembly C:\Program Files (x86)\S
DM Software\Group Policy Health Cmdlet\GetSDMGPHealth.dll.
Die Datei befindet sich in C:\Program Files (x86)\SDM Software\Group Policy Heal
th Cmdlet\GetSDMGPHealth.InstallLog.
Assembly C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet\GetSDMGP
Health.dll wird installiert.
Betroffene Parameter:
   assemblypath = C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet
\GetSDMGPHealth.dll
   logfile = C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet\GetS
DMGPHealth.InstallLog
   logtoconsole =

Die Installationsphase ist abgeschlossen, und die Commitphase beginnt.
Die Protokolldatei enthält den Fortschritt der Assembly C:\Program Files (x86)\S
DM Software\Group Policy Health Cmdlet\GetSDMGPHealth.dll.
Die Datei befindet sich in C:\Program Files (x86)\SDM Software\Group Policy Heal
th Cmdlet\GetSDMGPHealth.InstallLog.
Assembly C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet\GetSDMGP
Health.dll wird ausgeführt.
Betroffene Parameter:
   assemblypath = C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet
\GetSDMGPHealth.dll
   logfile = C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet\GetS
DMGPHealth.InstallLog
   logtoconsole =

Die Commitphase wurde erfolgreich abgeschlossen.

Die transaktive Installation ist abgeschlossen.
```

Um das Cmdlet zu verwenden, rufen Sie die PowerShell über den Befehl *Launch PowerShell on x64 with GP Health Snap-In* über die Startseite auf. Im Ordner *C:\Program Files (x86)\SDM Software\Group Policy Health Cmdlet* finden Sie eine Hilfedatei zum Cmdlet.

Der einfachste Weg, um zu überprüfen, ob ein Computer GPOs abruft, ist der Befehl *Get-SDMGPHealth -computer <Computername>*. In der Ausgabe sehen Sie, welche Computerrichtlinien und Benutzerrichtlinien der Computer angewendet hat. Das heißt, die Gruppenrichtlinien in dieser Aufzählung kommen am Client an.

Abbildg. 19.18 Überprüfen eines Computers auf angewendete Gruppenrichtlinien



Lokal auf einem Computer können Sie in der Eingabeaufforderung mit dem Tool *gpresult /h <HTML-Datei>* einen HTML-Bericht erstellen, der anzeigt, welche Gruppenrichtlinien der Client anwendet und welche Einstellungen enthalten sind. Mit der Option */x* erstellen Sie wiederum eine *.xml*-Datei, die Sie in Programmen oder Skripts einlesen können.

Ein Beispiel ist der Befehl *gpresult /h c:\temp\test.html*. Anschließend können Sie die Datei im Browser öffnen und sich den Bericht anzeigen lassen. Das Tool kann noch mehr Berichte erstellen. Auf der TechNet-Seite von GPResult (*http://technet.microsoft.com/en-us/library/cc733160%28WS.10%29.aspx* [Ms179-K19-06]) erhalten Sie Hilfe zu allen Optionen des Tools.

Datensicherung und Wiederherstellung von Gruppenrichtlinien

Beim Einsatz von Gruppenrichtlinien sollten Sie diese in regelmäßigen Abständen sichern. Vor allem, wenn Sie eigene Richtlinien erstellen, bietet sich eine solche Sicherung an. Zu einer richtigen Backupstrategie des kompletten Windows Server 2012 R2-Servers gehört in einem Unternehmen auch die Sicherung der Gruppenrichtlinien. Sichern Sie am besten die Gruppenrichtlinie immer in einen speziellen Ordner auf der lokalen Festplatte und kopieren Sie danach diesen Ordner 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.

Um eine Datensicherung einzelner oder aller Gruppenrichtlinien durchzuführen, klicken Sie in der GPMC auf den Knoten *Gruppenrichtlinienobjekte*. Dieser Knoten enthält alle Gruppenrichtlinien. Klicken Sie mit der rechten Maustaste auf eine Gruppenrichtlinie und wählen Sie im Kontextmenü den Eintrag *Sichern* aus.

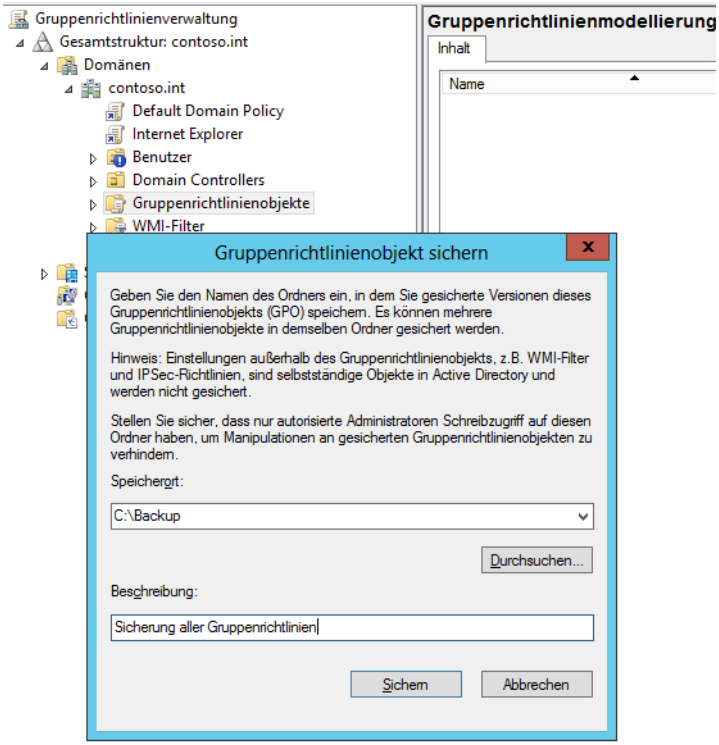
Bei der Sicherung von Gruppenrichtlinien werden die Einstellungen in eine Datei exportiert. Diese Datei können Sie zur Wiederherstellung importieren. Sie können auch direkt auf den Knoten *Gruppenrichtlinienobjekte* klicken und im Kontextmenü den Eintrag *Alle sichern* auswählen, um sämtliche Gruppenrichtlinien einer Domäne auf einmal zu sichern. 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

Danach erscheint ein Fenster, in dem Sie einen Ordner auf der Festplatte auswählen und eine Beschreibung der Sicherung hinterlegen können.

Nach der Bestätigung Ihrer Eingaben beginnt der Sicherungs-Assistent mit der Datensicherung der Gruppenrichtlinie und speichert diese im ausgewählten Ordner der Festplatte. Jede Datensicherung wird auf der Festplatte mit einer eindeutigen GUID im ausgewählten Ordner abgelegt.

Abbildg. 19.19 Starten der Datensicherung von Gruppenrichtlinien



Die Verwaltung der gesicherten Gruppenrichtlinien findet allerdings nicht über das Dateisystem statt, sondern ebenfalls mit der GPMC. Klicken Sie in der GPMC mit der rechten Maustaste auf den Knoten *Gruppenrichtlinienobjekte*. 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. Bei der Wiederherstellung einer Gruppenrichtlinie werden die Daten der exportierten Datei wieder in die produktive Richtlinie importiert. Sie können eine Wiederherstellung durchführen, falls Sie die Gruppenrichtlinie versehentlich gelöscht haben oder einen älteren Versionsstand der Einstellungen der Gruppenrichtlinie wiederherstellen möchten.

Bei der Wiederherstellung einer Gruppenrichtlinie stellt Windows, neben den Einstellungen der Richtlinien, auch die Berechtigungen für das Gruppenrichtlinienobjekt sowie, falls vorhanden, die Verknüpfungen der WMI-Filter wieder her. Um eine Gruppenrichtlinie zu restaurieren, klicken Sie in der Verwaltung der Sicherungen auf die Schaltfläche *Wiederherstellen*.

Sie können Gruppenrichtlinien auch komplett kopieren. Bei einem Kopiervorgang erstellt Windows eine komplett neue Gruppenrichtlinie mit neuer GUID und importiert die Einstellungen der Quellrichtlinie. Nach diesem Vorgang sind die beiden Gruppenrichtlinien vollkommen unabhängig voneinander, haben aber identische Einstellungen. 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. Es erscheint keine weitere Meldung, wenn Sie die Gruppenrichtlinie kopiert haben.
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.
4. Anschließend erscheint der Assistent zum domänenübergreifenden Kopieren von Gruppenrichtlinien.
5. 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.
6. 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.
7. Danach erhalten Sie noch ein Informationsfenster und der Assistent beginnt mit dem Import der Gruppenrichtlinie.

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. Wollen Sie für die Verwaltung der Gruppenrichtlinien in der GPMC von externen Gesamtstrukturen nicht gleich eine Vertrauensstellung einrichten, können Sie die Überprüfung für Vertrauensstellung deaktivieren.

In diesem Fall müssen Sie in der Systemsteuerung mithilfe von *Benutzerkonten/Anmeldeinformationsverwaltung* 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*.

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.

Neben dem kompletten Kopieren von Gruppenrichtlinien können Sie auch nur die Einstellungen einer Gruppenrichtlinie in eine bereits vorhandene Richtlinie übernehmen. Beim Importieren einer Gruppenrichtlinie werden die Einstellungen aus der Datensicherung der Gruppenrichtlinie verwendet. Beim Importvorgang werden alle Einstellungen der Zielrichtlinie gelöscht und danach die Einstellungen der Quellrichtlinie übernommen.

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 Eintrag *Einstellungen importieren* aus. Es erscheint der Importeinstellungen-Assistent.

Beim Importieren der Einstellungen gehen alle Einstellungen der Zielrichtlinie verloren. Aus diesem Grund schlägt Ihnen der Assistent zunächst die Sicherung des Ziel-GPOs vor.

Im nächsten Fenster müssen Sie zunächst den Sicherungsordner der Gruppenrichtlinien auswählen. Danach können Sie die Quellrichtlinie auswählen, aus der Sie die Einstellungen in die Zielrichtlinie übernehmen wollen. An dieser Stelle können Sie die Einstellungen mit der Schaltfläche *Einstellungen anzeigen* noch einmal überprüfen. Danach erhalten Sie eine Zusammenfassung angezeigt, nach der die Einstellungen schließlich von der Quell- in die Zielrichtlinie übernommen werden.

Gruppenrichtlinienmodellierung

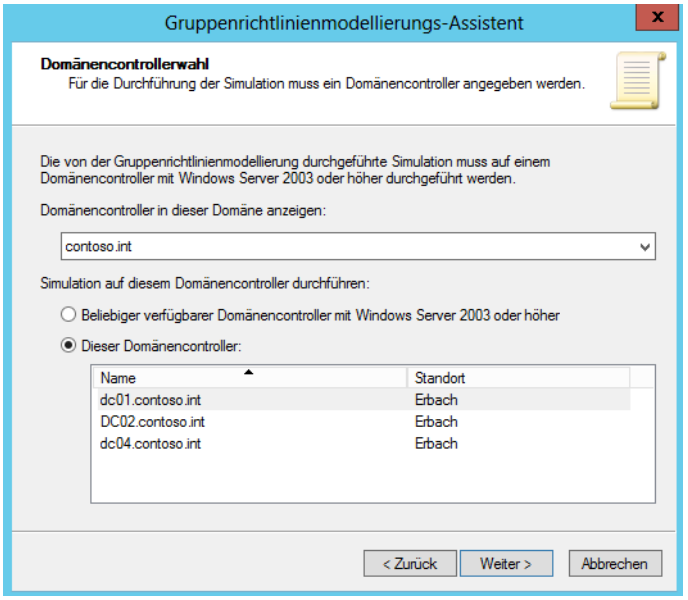
Mit der Gruppenrichtlinienmodellierung aus der GPMC lassen sich die Auswirkungen von Gruppenrichtlinien simulieren. Durch diese Funktion können Sie die Einstellungen vor der eigentlichen Inbetriebnahme einer Gruppenrichtlinie ausführlich testen. Um eine Simulation für eine bestimmte Domäne oder OU durchzuführen, klicken Sie mit der rechten Maustaste auf den Knoten und wählen im Kontextmenü den Eintrag *Gruppenrichtlinienmodellierungs-Assistent* aus. Es erscheint das Startfenster des Assistenten.

Zunächst wählen Sie die Domäne aus sowie einen Domänencontroller. Danach müssen Sie den Container auswählen, in dem sich die Benutzer und Computer befinden, für die Sie die Simulation durchführen wollen. Hier trägt der Assistent standardmäßig die OU ein, über die Sie den Assistenten gestartet haben.

Im nächsten Fenster können Sie Optionen bezüglich des Standorts und der Netzwerkverbindung auswählen. Normalerweise können Sie die vorgegebenen Einstellungen übernehmen. Auf weiteren Seiten können Sie simulieren, was passieren würde, wenn die getesteten Benutzer nicht mehr in ihren entsprechenden Sicherheitsgruppen Mitglied wären, können Active Directory-Standorte und langsame Verbindungen simulieren und erstellte WMI-Filter integrieren. Danach können Sie die gleichen Einstellungen für die Computerkonten auswählen. In den meisten Fällen 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. Im Anschluss daran erhalten Sie einen detaillierten Bericht im *.html*-Format über die Auswirkungen der simulierten Gruppenrichtlinien für den konfigurierten Container angezeigt.

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. 19.20 Simulieren von Gruppenrichtlinien



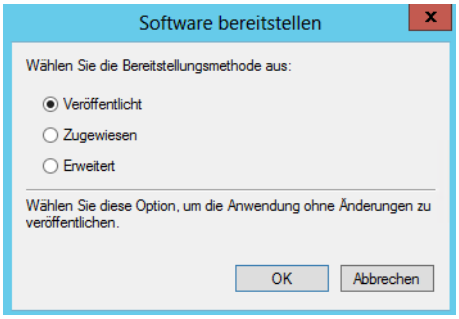
Softwareverteilung über Gruppenrichtlinien

Die Konfiguration der Softwareverteilung bei Windows Server 2012 R2 kann über die Gruppenrichtlinien erfolgen. Dort können Sie *.msi*-Dateien für die Installation auf Clientsystemen zuordnen. Das ist zwar nicht so komfortabel wie mit System Center Configuration Manager 2012, aber für einzelne Anwendungen oder Tools durchaus sinnvoll.

Die Softwareverteilung erfolgt über die in diesem Kapitel ausführlich behandelten Gruppenrichtlinien. 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 führen Sie die Bereitstellung eines Programms auf Basis von *.msi*-Dateien durch. Dazu kopieren Sie zunächst die Installationsdateien des Programms, welches Sie installieren wollen, auf eine Netzwerkfreigabe, die Anwender auch lesen dürfen. Anschließend binden Sie die *.msi*-Datei ein. Installationen, die auf *.exe*-Dateien aufbauen, funktionieren mit diesen Möglichkeiten nicht.

Abbildg. 19.21 Erstellen eines neuen Softwarepakets zur automatischen Installation

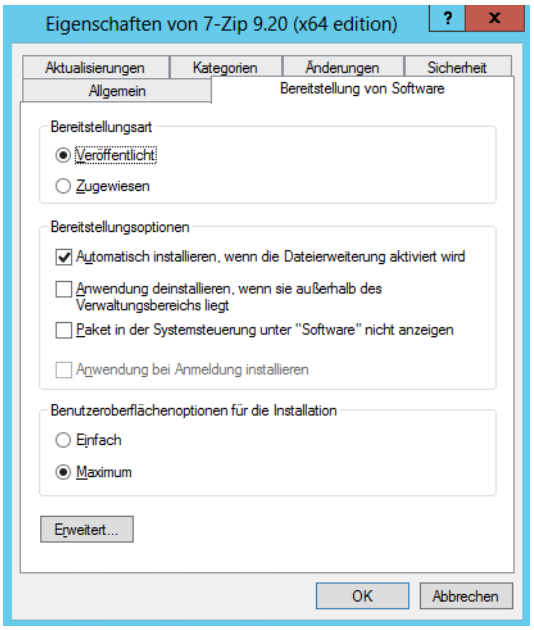


Wählen Sie anschließend die *.msi*-Datei von der Netzwerkfreigabe aus. Als Nächstes können Sie die Bereitstellungsmethode auswählen. Stellen Sie das Paket für Computer bereit, nicht für Benutzer, steht die Option *Veröffentlicht* nicht zur Verfügung.

Wählen Sie die Option *Veröffentlicht* aus, erscheint das Paket auf dem Client zur manuellen Installation in der Systemsteuerung. Alle erforderlichen Einstellungen sind automatisch gesetzt. Durch einen Doppelklick auf das Paket können Sie die Eigenschaften bearbeiten.

Wählen Sie die Option *Zugewiesen* aus, erstellt Windows ebenfalls automatisch einen Eintrag. Wählen Sie besser die Option *Erweitert* aus. Bei dieser Auswahl können Sie Einstellungen genau setzen. Es öffnet sich ein neues Fenster mit verschiedenen Registerkarten, über die Sie die automatische Installation konfigurieren können.

Abbildg. 19.22 Bearbeiten eines Softwarepakets zur automatischen Installation



Über die Registerkarte *Bereitstellung von Software* wählen Sie zwischen *Veröffentlicht* und *Zugewiesen* aus. Abhängig von der Auswahl stehen im unteren Bereich weitere Optionen zur Verfügung, welche die Installation beeinflussen:

- **Automatisch installieren, wenn die Dateierweiterung aktiviert wird** Diese Option bewirkt, dass die Anwendung beim Öffnen einer Datei, deren Dateityp für diese Anwendung registriert ist, automatisch installiert wird. Vorher ist die Anwendung auf dem Computer nicht verfügbar.
- **Anwendung deinstallieren, wenn sie außerhalb des Verwaltungsbereichs liegt** Mit dieser Option legen Sie fest, dass der Computer eine Anwendung automatisch von den Clientsystemen entfernt, wenn die Gruppenrichtlinien, über die sie eingerichtet ist, keine Gültigkeit mehr für diesen Benutzer oder Computer hat. Das ist bei Anwendungen sinnvoll, die Zugriff auf kritische Informationen im Unternehmen gewähren.
- **Paket in der Systemsteuerung unter "Software" nicht anzeigen** Hiermit legen Sie fest, 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.
- **Anwendung bei Anmeldung installieren** Durch diese Option lässt sich definieren, dass die Anwendung bei der Anmeldung eines Benutzers automatisch installiert wird

Über die Einstellungen für Benutzeroberflächenoptionen konfigurieren Sie, ob dem Benutzer alle Installationsmeldungen präsentiert werden oder ob sich das System darauf beschränkt, nur den Installationsfortschritt anzuzeigen.

Auf der Registerkarte *Aktualisierungen* sehen Sie Informationen über die Zusammenhänge zwischen verschiedenen *.msi*-Paketen, die Sie verteilen. Im oberen Bereich können Sie über die Schaltfläche *Hinzufügen* Pakete aus dieser oder anderen Gruppenrichtlinien angeben, die durch das aktuell bear-

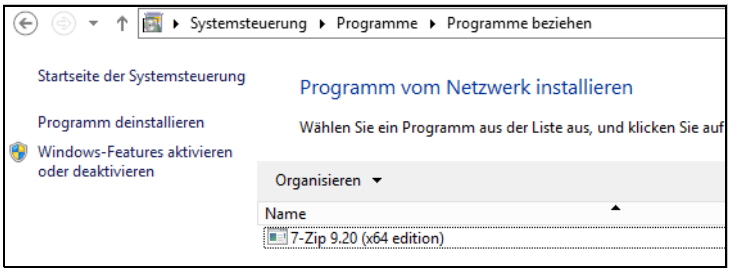
beitete Paket aktualisiert werden sollen. Im unteren Bereich sind Pakete aufgeführt, die dem bearbeiteten Paket übergeordnet sind.

Über die Registerkarte *Kategorien* können Sie Kategorien angeben, unter denen diese Anwendung im Bereich Software der Systemsteuerung aufgelistet sein soll. Über *Änderungen* können Sie *.mst*-Dateien angeben, die Sie für das Paket anwenden wollen. Mit solchen Transformations-Dateien können Sie Einstellungen für die Installation anpassen, zum Beispiel bei der automatischen Installation von Office.

Mit der Registerkarte *Sicherheit* lassen sich die Zugriffsberechtigungen für die Nutzung der Installationspakete konfigurieren. Haben Sie alle Einstellungen vorgenommen, bestätigen Sie die Eingaben und schließen das Fenster. Im Fenster der Gruppenrichtlinienverwaltung sehen Sie das Paket und können es auf Wunsch auch nachträglich bearbeiten. Verteilen Sie Anwendungen und Tools am besten über eigenständige Gruppenrichtlinien. Diese verknüpfen Sie anschließend mit der OU oder der ganzen Domäne, wie jede andere Gruppenrichtlinie auch. Im laufenden Betrieb eines Rechners lassen Sie mit *appwiz.cpl* die Richtlinie auf den Computer übertragen.

Haben Sie eine Anwendung veröffentlicht, finden Anwender diese in der Systemsteuerung über *Programm vom Netzwerk beziehen* in der Verwaltung der Programme. Diese starten Sie am schnellsten über das Tool *appwiz.cpl*. Durch die Auswahl von *Installieren* installiert sich die Anwendung auf dem Computer.

Abbildg. 19.23 Anzeigen der veröffentlichten Programmen



Geräteinstallation mit Gruppenrichtlinien konfigurieren

Sie haben in den Gruppenrichtlinien oder lokale Richtlinien von Windows Server 2012 R2 und auch Windows 8/8.1 die Möglichkeit, die Installation von Geräten auf den Clientcomputern zu steuern. In diesen Bereich fällt auch die Konfiguration und Anbindung von USB-Sticks. Generell können Sie verschiedene Aufgaben durchführen, welche die Geräteinstallation von Benutzern betreffen. Die Anwender haben dann das Recht, entsprechende Geräte auch ohne Administratorrechte zu installieren, beziehungsweise erhalten eine Meldung, falls nicht unterstützte Geräte mit den Computern verbunden werden sollen:

- Sie können verhindern, dass Anwender Geräte installieren und dabei genau festlegen, welche Geräte die Anwender nicht installieren dürfen
- 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 oder externe Festplatten.

Geräteidentifikationsstring und Gerätesetupklasse

Windows untersucht bei der Anbindung eines neuen Geräts zwei Informationen, die das angeschlossene Gerät übermittelt. Auf Basis dieser Informationen kann Windows entscheiden, ob ein interner Windows-Treiber Einsatz findet oder ob der Treiber des Drittherstellers verwendet werden soll. Auch zusätzliche Funktionen der Endgeräte lassen sich dadurch aktivieren.

Diese beiden Informationen zur Installation von Gerätetreibern sind die Geräteidentifikationsstrings und die Gerätesetupklasse. Ein Gerät verfügt normalerweise über mehrere Geräteidentifikationsstrings, die der Hersteller festlegt. Dieser String ist auch in der INF-Datei des Treibers hinterlegt. Auf dieser Basis entscheidet Windows, welchen Treiber es installieren soll. Es gibt zwei Arten von Geräteidentifikationsstrings:

- **Hardware-IDs** Diese Strings liefern eine detaillierte und spezifische Information über ein bestimmtes Gerät. Hier ist der genaue Name, das Modell und die Version des Geräts als sogenannte Geräte-ID festgelegt. Teilweise liefert der Treiber nicht alle Informationen, zum Beispiel die Version, mit. In diesem Fall kann Windows selbst entscheiden, welche Version des Treibers installiert wird.
- **Kompatible IDs** Diese IDs verwendet Windows, wenn kein passender Treiber zum Gerät gefunden werden kann. Diese Informationen sind allerdings optional und sehr allgemein gehalten. Der Treiber unterstützt dann nur Grundfunktionen des Geräts. Verwendet Windows diese ID zur Treiberinstallation, lassen sich zumindest die Grundfunktionen des Geräts verwenden.

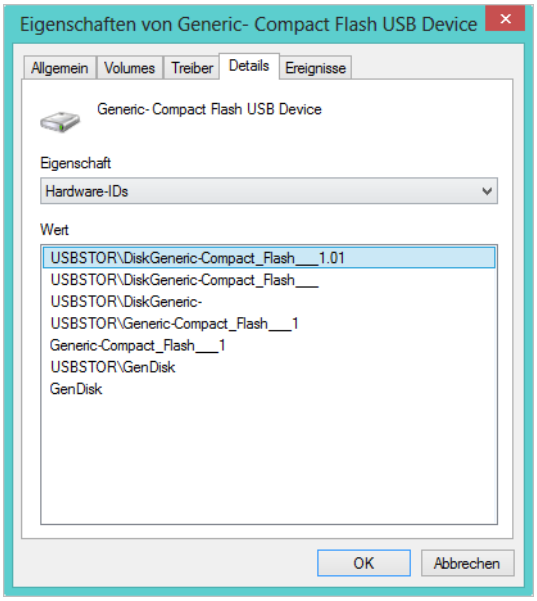
Windows weist Treiberpaketen einen gewissen Rang zu. Je niedriger der Rang, umso besser passt der Treiber zum Gerät. Der beste Rang für einen Treiber ist 0. Je höher der Rang, umso schlechter passt der Treiber. In Windows 8/8.1 und Windows Server 2012 R2 können beide Informationen nicht nur zur Identifikation des Gerätetreibers verwendet werden, sondern auch zur Zuweisung von Richtlinien über welche Windows die Funktionen und Berechtigungen des Geräts verwaltet.

Die Gerätesetupklassen sind eigene Arten von Identifikationsstrings. Auch auf diese Strings verweist das Treiberpaket. Alle Geräte, die sich in einer gemeinsamen Klasse befinden, installiert Windows auf die gleiche Weise, unabhängig von ihrer eindeutigen Hardware ID.

Dies bedeutet beispielsweise, dass Windows alle DVD-Laufwerke auf exakt die gleiche Weise installiert. Die Gerätesetupklasse ist durch einen Globally Unique Identifier (GUID) angegeben. Um die Hardware-ID oder die Gerätesetupklasse eines Geräts zu ermitteln, verbinden Sie dieses am besten zunächst mit einem Windows-PC und lassen den Treiber installieren. Im Anschluss rufen Sie den Geräte-Manager auf. Öffnen Sie die Eigenschaften des Geräts und wechseln Sie zur Registerkarte *Details*. Über die Auswahl der Option Hardware-IDs im Dropdown-Menü *Eigenschaften* können Sie sich alle Hardware-IDs eines Geräts anzeigen lassen. Diese Informationen können Sie später in der Richtlinie hinterlegen.

Über dieses Menü können Sie auch weitere Informationen über die Eigenschaften des Geräts anzeigen lassen, unter anderem auch die Geräteklasse. Die Werte lassen sich markieren und über die Tastenkombination Strg+C in die Zwischenablage kopieren sowie bei Bedarf wieder in die Gruppenrichtlinien einfügen.

Abbildg. 19.24 Anzeigen der Hardware-IDs eines Geräts, zum Beispiel eines USB-Sticks



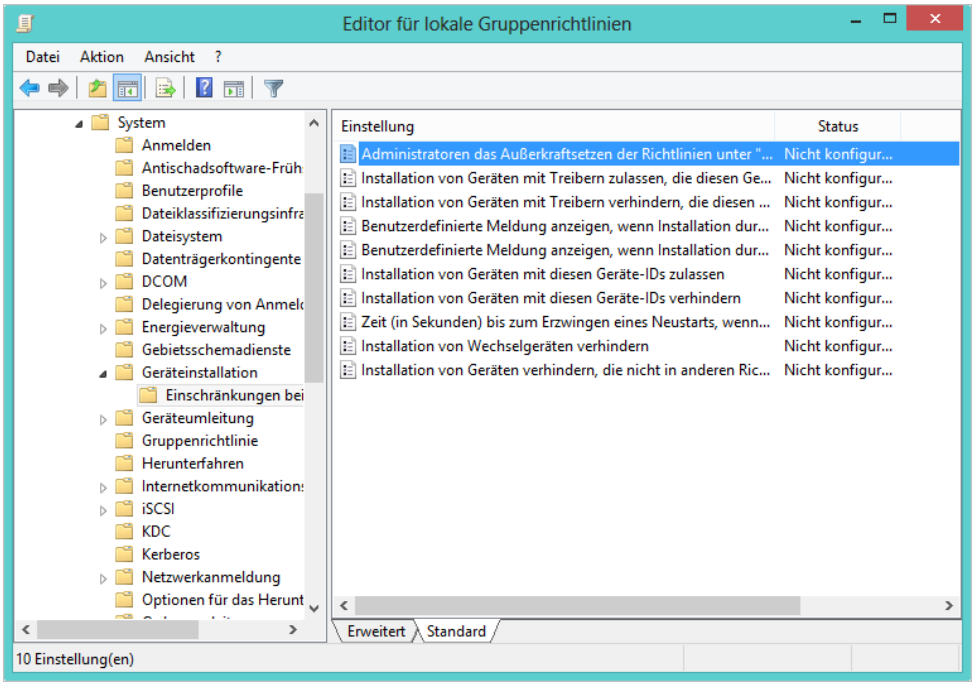
Die Einstellungen für die Geräteinstallationen nehmen Sie über Gruppenrichtlinien vor. Die Einstellungen finden Sie über *Computerkonfiguration/Administrative Vorlagen/System/Geräteinstallation/Einschränkungen bei der Geräteinstallation*.

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 Assistenten zum Hinzufügen von Hardwaretreibern installieren. Das funktioniert auch dann, wenn Sie bestimmte Geräte von der Installation ausschließen.

Zusätzlich haben Sie an dieser Stelle weitere Möglichkeiten, die Sie per Richtlinie verteilen können:

- **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 mit Treibern zulassen, die diesen Gerätesetupklassen entsprechen* definiert sind
- **Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind** Wenn Sie diese Richtlinie nicht konfigurieren oder aktivieren, können Anwender alle Geräte installieren. Ausgenommen davon sind Geräte, die in den Einstellungen *Installation von Geräten mit diesen Geräte-IDs verhindern* oder *Installation von Geräten mit Treibern verhindern, die diesen Gerätesetupklassen entsprechen* oder *Installation von Wechselgeräten verhindern* definiert sind.

Abbildg. 19.25 Konfiguration von Gruppenrichtlinien für die Steuerungen von USB-Sticks an Anwender-PCs



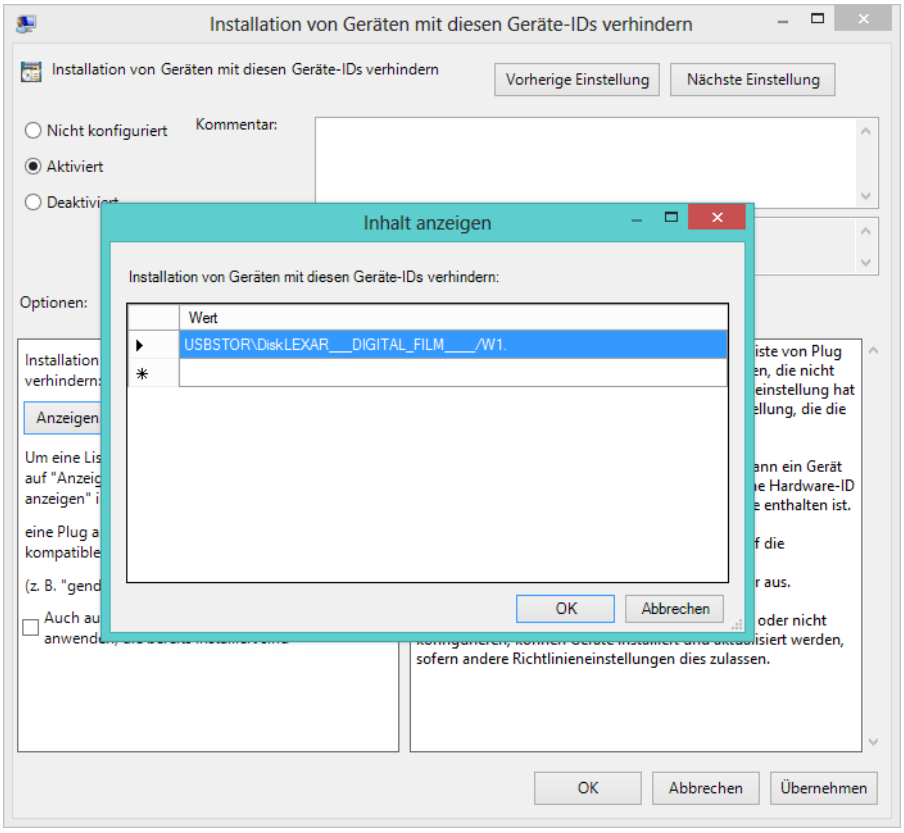
- **Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallation" erlauben** Bei dieser Einstellung können die Mitglieder der lokalen Administratoren-Gruppe jede Art von Treiber installieren, unabhängig von den Gruppenrichtlinieneinstellungen. Dazu muss der Administrator allerdings den Assistenten zum Hinzufügen von neuer Hardware verwenden. Wenn diese Einstellung nicht gesetzt ist, dürfen auch die Administratoren die entsprechenden Geräte nicht installieren.
- **Installation von Geräten mit diesen Geräte-IDs verhindern** Hier können Sie eine Liste festlegen, in der Sie alle Hardware-IDs und kompatible 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 ist.
- **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 kompatiblen ID hinterlegen, welche die Anwender installieren dürfen. Diese Richtlinie ist aber nur in Verbindung mit der Richtlinie *Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind* sinnvoll, 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 Geräteklassen die Anwender installieren dürfen

So funktioniert die Steuerung in Geräteinstallationen über Gruppenrichtlinien

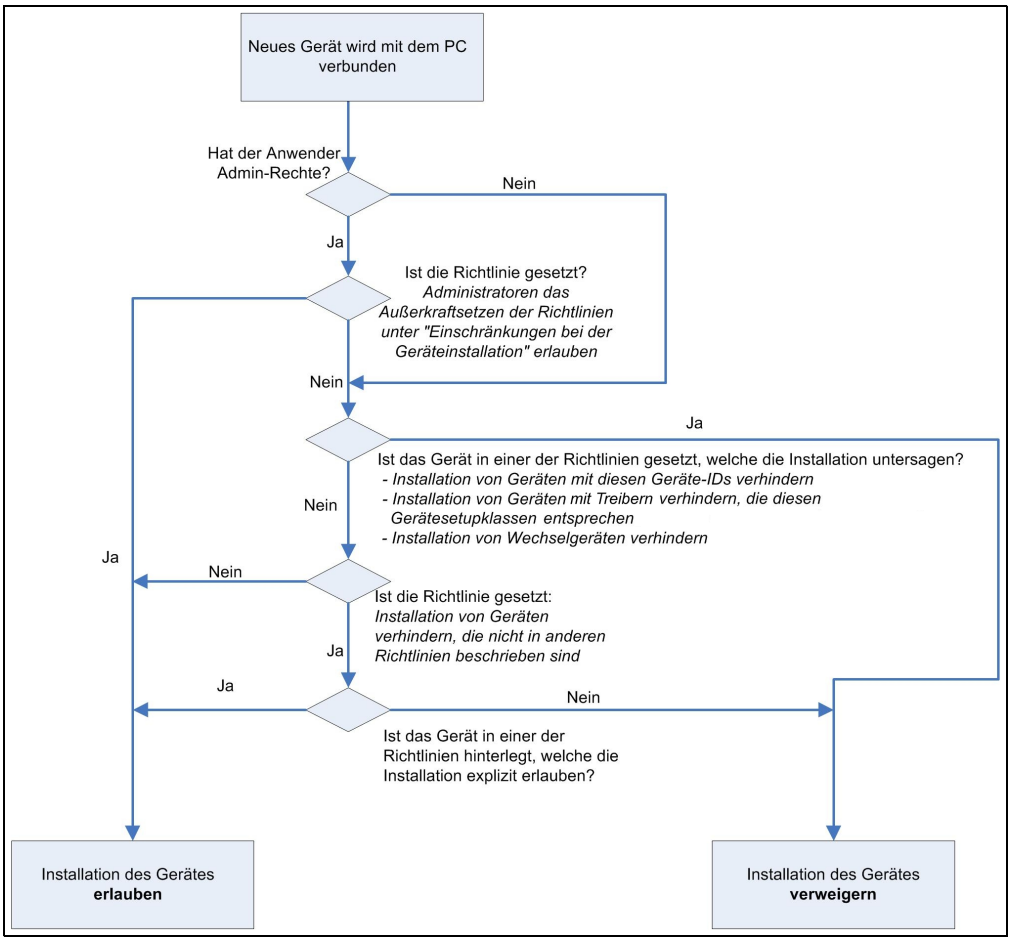
Um in den Richtlinien für die Zulassung oder Verhinderung der Installation von Geräten Hardware-IDs aufzunehmen, rufen Sie die Eigenschaften dieser Einstellung auf und aktivieren Sie diese. Klicken Sie im Anschluss auf die Schaltfläche *Anzeigen* und dann auf Schaltfläche *Hinzufügen*. Hier können Sie die Hardware-ID einfügen, die Sie zuvor in den Eigenschaften des Geräts im Geräte-Manager in die Zwischenablage kopiert haben.

Abbildg. 19.26 Konfiguration der Gruppenrichtlinie zur Unterbindung der Treiberinstallation



Wird die Installation eines Geräts untersagt, erhält der Anwender eine entsprechende Fehlermeldung angezeigt, die darauf hinweist, dass die Installation auf Basis einer Richtlinie untersagt ist. In den Richtlinien können Sie auch einen benutzerdefinierten Text hinterlegen.

Abbildg. 19.27 Verwenden von Richtlinien zur Steuerung der Geräteinstallation in Windows



Konfiguration von Gruppenrichtlinien für den Zugriff auf Wechselmedien

Zusätzlich zur Möglichkeit, die Installation von Geräten zu steuern, können in Windows 8/8.1 Gruppenrichtlinien erstellt sein, welche den schreibenden und lesenden Zugriff auf Wechselmedien steuern. Die Richtlinie zur Steuerung von Wechselmedien können Sie sowohl unter der Computerkonfiguration als auch in der Benutzerkonfiguration durchführen. 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 eine ausführliche Information über die Auswirkungen der Richtlinie. 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 verweigern.

Windows Store sperren

Wollen Sie auf Rechnern den Windows Store sperren, damit andere Anwender keine Apps installieren können, haben Sie die Möglichkeit, den Gruppenrichtlinienverwaltungs-Editor zu verwenden. Dieser steht aber nur in den Editionen Pro und Enterprise von Windows 8/8.1 zur Verfügung. Für eine zentrale Vorgabe für alle Windows 8/8.1-PCs müssen Sie auf Domänencontrollern mit Windows Server 2012 R2 eine zentrale Gruppenrichtlinie erstellen:

- Suchen Sie auf der Startseite nach *gpedit.msc*
- Navigieren Sie zu *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Store*
- Aktivieren Sie die Richtlinieneinstellungen zur Deaktivierung des kompletten Stores oder nur das automatische Herunterladen von Updates
- Starten Anwender nach der Einrichtung den Store, erscheint eine entsprechende Meldung

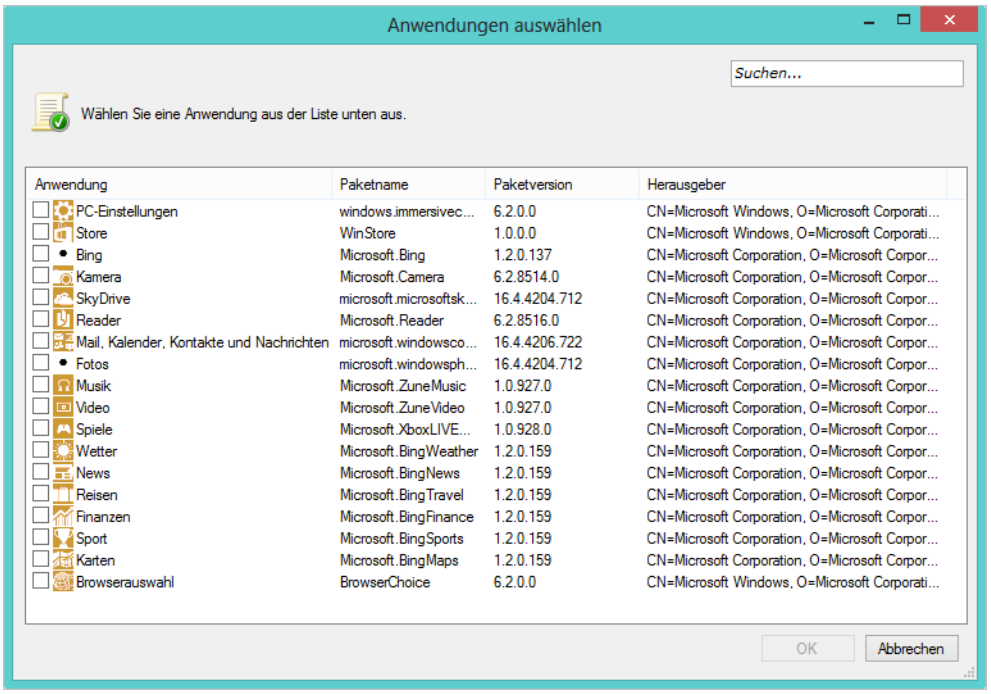
Mit AppLocker Desktop- und Windows-Apps in Netzwerken steuern

Administratoren in Windows-Netzwerken können mit Windows Server 2012 R2 und Windows 8/8.1 über Richtlinien unerwünschte Anwendungen sperren und so Sicherheitslücken schließen. Die Funktionen sind der Enterprise-Version von Windows 8/8.1 vorbehalten und waren auch schon in Windows 7 Bestandteil.

In Windows 8/8.1 lassen sich mit den erweiterten Möglichkeiten aber noch besser Anwendungen sperren. So können in Windows 8/8.1 auch Einstellungen für Windows-Apps und die Startseite in AppLocker hinterlegt werden.

Auf diesem Weg können Sie verhindern, dass Anwender transportable Programme über USB-Stick, E-Mail oder anderen Speichermöglichkeiten ausführen können. Durch die Einbindung in Gruppenrichtlinien haben Sie zusätzlich die Möglichkeit, für verschiedene Gruppen unterschiedliche Einstellungen vorzunehmen.

Abbildg. 19.28 Windows 8/8.1 bietet auch Neuerungen für AppLocker



Auch wenn Anwender keine Administratorrechte haben, können sie doch problemlos viele Programme starten. Die Programme haben dann die gleichen Rechte wie der Benutzer und können teilweise sogar Daten ins Internet übertragen. Aus diesem Grund ist eine gewisse Einschränkung durchaus sinnvoll.

AppLocker in Unternehmen nutzen

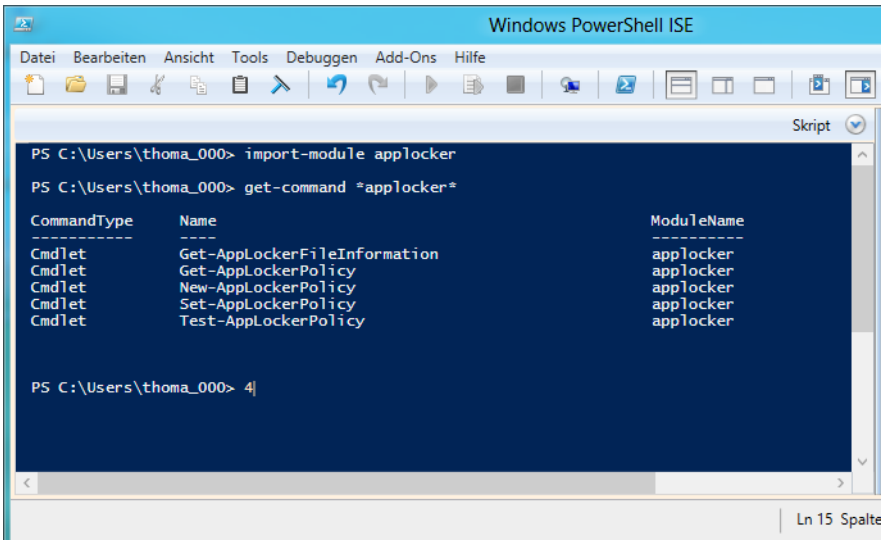
Damit Sie AppLocker nutzen können, müssen Sie im Unternehmen Windows 8/8.1 in der Edition Enterprise einsetzen. AppLocker ist außerdem in den Editionen Standard, Enterprise und Datacenter von Windows Server 2012 R2 enthalten. Über diesen Weg erstellen Sie Richtlinien, die auf den Windows 8/8.1-Clients automatisch angewendet werden.

Betriebssysteme und Versionen von Windows 8/8.1, die nicht kompatibel mit AppLocker sind, wenden die Regeln nicht an. Es besteht also keine Gefahr, dass Sie Rechner außer Funktion setzen, wenn Sie AppLocker einsetzen und das Betriebssystem die Regeln nicht versteht.

AppLocker ermöglicht die Erstellung von Whitelists und Blacklists. Auch eine Kombination von Regeln ist möglich. AppLocker kann Anwendungen sperren und für fortgeschrittene Einsatzszenarien sogar einzelne DLL-Dateien. Auch konkrete Versionen von Programmen und DLL-Dateien lassen sich berücksichtigen.

AppLocker kann auch automatische Regeln erstellen und bestimmte Ordner auf neue Programme hin überwachen. Neben Gruppenrichtlinien können Sie auch über Sicherheitsgruppen filtern. AppLocker können Sie auch in der PowerShell steuern. Dazu laden Sie in der PowerShell mit *Import-Module applocker* die entsprechenden Cmdlets. Eine Liste der verschiedenen Cmdlets erhalten Sie mit *Get-Command *applocker**.

Abbildg. 19.29 Verwalten von AppLocker in der PowerShell



Microsoft bietet verschiedene Dokumente zur Planung und Umsetzung von AppLocker-Richtlinien zum Download an (*http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=13431* [Ms179-K19-07]). Auch in Microsoft TechNet finden Sie Anleitungen zum Thema (*http://technet.microsoft.com/de-de/library/dd723686(WS.10).aspx* [Ms179-K19-08]).

Ein Video, welches ebenfalls bei der Einrichtung hilft, finden Sie auf der Internetseite *WindowsSecurity.com* (*http://www.windowsecurity.com/articles/Video-AppLocker-Tips-Tricks.html* [Ms179-K19-09]).

Die Informationen beziehen sich noch auf Windows 7 und Windows Server 2008 R2, gelten aber weiterhin auch für Windows 8/8.1.

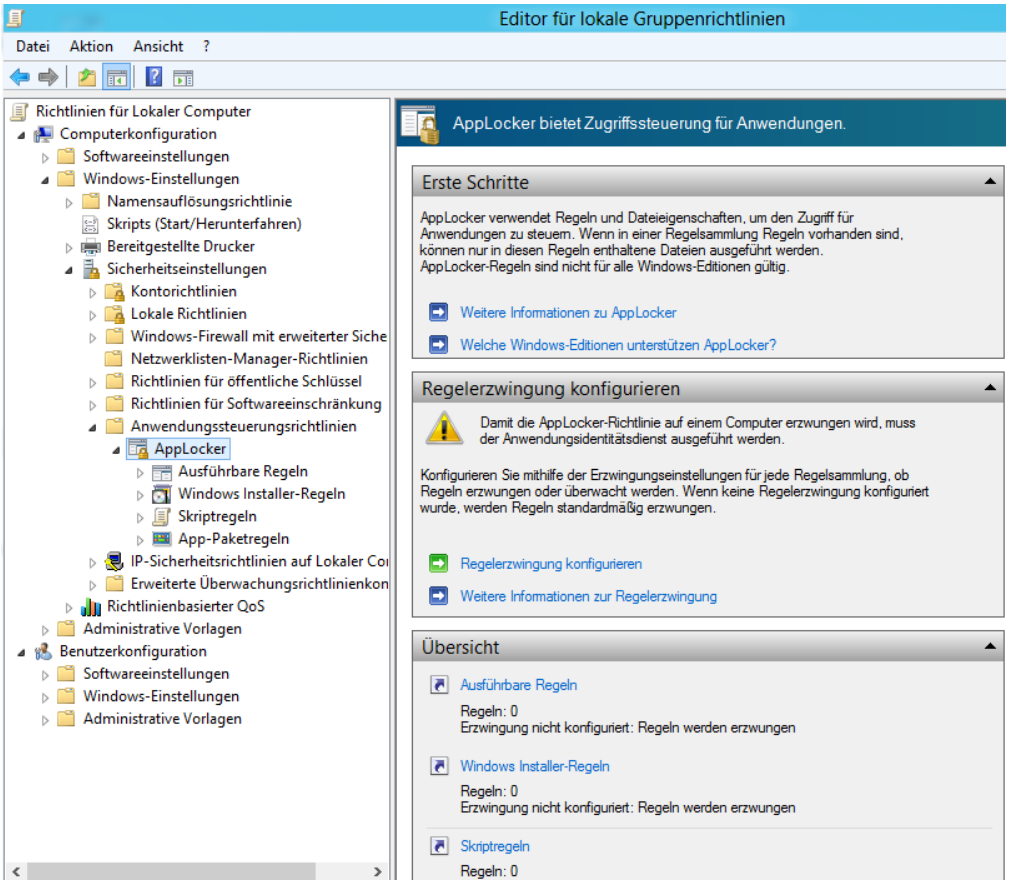
Gruppenrichtlinien für AppLocker erstellen

Die Konfiguration von Richtlinien finden in zwei Stufen statt. Sie erstellen eine Richtlinie und weisen dieser AppLocker-Regeln zu. Die Gruppenrichtlinie erstellen Sie genau so wie jede andere auch. Um ein neues Gruppenrichtlinienobjekt (GPO) zu erstellen, starten Sie die Gruppenrichtlinienverwaltung, klicken in der GPMC auf den Knoten *Gruppenrichtlinienobjekte* und wählen im Kontextmenü den Befehl *Neu* aus.

Nach der Erstellung verknüpfen Sie die Richtlinie mit der OU oder Domäne, um die Einstellungen anzuwenden. Sie können aber auch innerhalb der AppLocker-Regeln filtern, indem Sie bestimmte Sicherheitsgruppen verwenden. Sie können die Einstellungen auch auf einzelnen Computern vornehmen.

Um AppLocker zu verwenden, navigieren Sie zu *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Anwendungssteuerungsrichtlinien*. Klicken Sie auf *AppLocker*. Hier erstellen Sie die Regeln für AppLocker.

Abbildg. 19.30 Verwenden von AppLocker in Windows 8/8.1 und Windows Server 2012 R2



- Bei *Ausführbare Regeln* erstellen Sie Regeln für Programme mit den Endungen *.exe* und *.com*
- *Windows Installer-Regeln* steuern die Ausführung von Setupdateien (*.msi* und *.msp*)
- Über *Skriptregeln* erfassen Sie Dateien mit den Endungen *.js*, *.ps1*, *.vbs*, *.cmd* und *.bat*
- Neu in Windows 8/8.1 ist der Knoten *App-Paketregeln*. Hier steuern Sie den Zugriff der Anwender auf Windows-Apps auf den Windows 8/8.1-PCs.

Die Regeln lassen sich kombinieren und Sie können auswählen, ob die entsprechende Regel Programme erlauben oder sperren soll. Zusätzlich können Sie bei jeder Regel noch Ausnahmen für bestimmte Programme hinterlegen.

Verweigerungsregeln überschreiben die Zulassungsregeln. Wenn Sie die Ausführung von Programmen verweigern, haben Sie nicht die Möglichkeit, eine Regel zu erstellen, die einer bestimmte

Gruppe die Ausführung erlaubt. In diesem Fall sollten Sie die Filterung in der Regel so steuern, dass nicht alle Benutzer eingeschränkt sind.

AppLocker unterstützt bei diesen Vorgängen auch Gruppen in Active Directory. Erstellen Sie eine neue AppLocker-Regel und hinterlegen Sie die Benutzergruppe. Später können Sie dann die Ausführung von Programmen über die Gruppenmitgliedschaft steuern, ohne die AppLocker-Regeln neu erstellen oder ändern zu müssen.

Erstellen von Regeln für AppLocker

Ausführbare Regeln bieten einen Einstieg in AppLocker. Hier können Sie bestimmte Programme blockieren oder bestimmte Versionen sperren lassen:

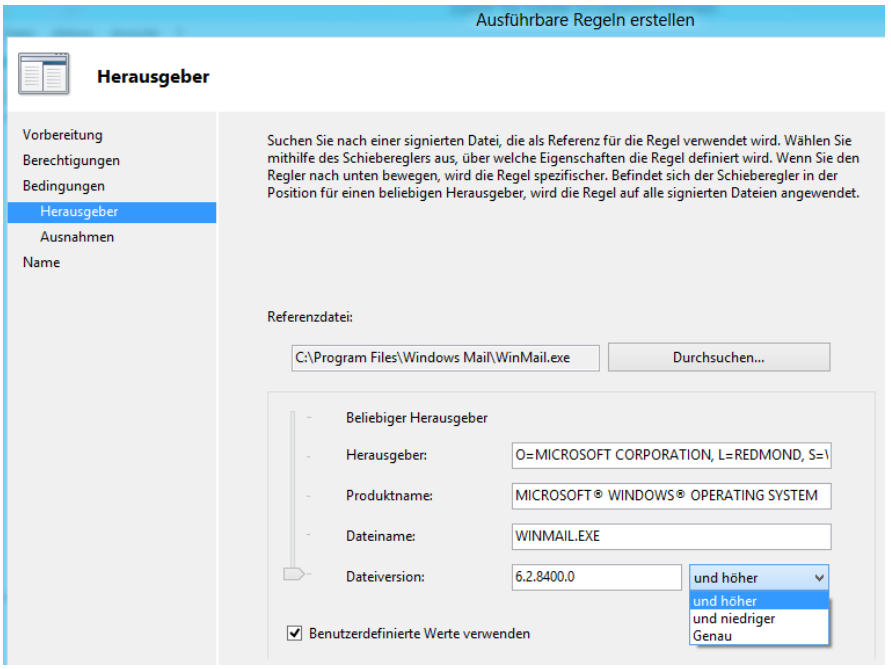
1. Navigieren Sie zu *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Anwendungssteuerungsrichtlinien*. Klicken Sie auf *AppLocker*. Die Steuerung können Sie auch auf einzelnen Computern vornehmen. Dann finden Sie AppLocker im Editor für lokale Gruppenrichtlinien über *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Anwendungssteuerungsrichtlinien*.
2. Klicken Sie mit der rechten Maustaste auf *Ausführbare Regeln*.
3. Wählen Sie im Kontextmenü den Eintrag *Neue Regel erstellen* aus.
4. Bestätigen Sie die erste Seite *Vorbereitung* mit einem Klick auf *Weiter* und wählen Sie auf der Seite *Berechtigungen* aus, ob die Regel Anwendungen zulassen oder verweigern soll.
5. Wählen Sie im Dropdownmenü die Gruppe aus, auf die Sie diese Regel anwenden wollen.
6. Auf der nächste Seite legen Sie fest, auf welcher Grundlage Sie Programme sperren möchten:
   - **Herausgeber** Durch diese Auswahl können Sie Anwendungen auf Basis ihres Zertifikats filtern. Dazu muss die Anwendung jedoch digital signiert sein. Bei Standardsoftware ist das oft der Fall, beim Einsatz selbst entwickelter Anwendungen funktioniert das nicht, wenn Sie die Anwendung nicht signiert haben. Diese Auswahl ist am besten geeignet, da sie sich nur schwer umgehen lässt. Die Zertifikate einer ausführbaren Datei lassen sich von normalen Benutzern nicht aushebeln. Diese Auswahl ist also empfohlen.
   - **Pfad** Mit dieser Auswahl berücksichtigt die Regel Programme in einem bestimmten Ordner. Anwender können in diesem Fall aber Programme aus dem Ordner verschieben. In diesem Fall greift die Regel nicht mehr. Benutzer können daher solche Regeln ganz einfach aushebeln. Diese Auswahl ist also nicht empfohlen.
   - **Dateihash** Hierbei handelt es sich einfach ausgedrückt um den Fingerabdruck der Datei. Dieser ändert sich bei jeder neuen Version und Aktualisierung. Bei jeder Änderung des Programms müssen Sie auch die entsprechende Regel ändern.

Die weiteren Fenster unterscheiden sich etwas, abhängig von der Auswahl, die Sie zum Filtern verwenden.

Zunächst wählen Sie ein Referenzprogramm des Herstellers aus, dessen Programme Sie filtern wollen. Mit dem Schieberegler legen Sie Einstellungen wie die Version des Programms fest, welches Sie in der Regel erfassen wollen.

Sie haben auch die Möglichkeit, Versionen von Programmen zu sperren. Aktivieren Sie die Option *Benutzerdefinierte Werte verwenden*, können Sie bestimmen, ab oder bis welcher Version Sie das Programm in der Regel erfassen wollen. Auf diesem Weg lassen sich unerwünschte Versionen von Programmen ausfiltern.

Abbildg. 19.31 Auswählen der Filteroptionen für das Programm



Über die weiteren Fenster des Assistenten legen Sie fest, ob Sie Ausnahmen für die Regel erfassen wollen. Regeln lassen sich natürlich jederzeit nachträglich anpassen. Auf diesem Weg erstellen Sie alle Regeln, die Sie in der GPO erfassen wollen. Sobald Sie die GPO mit den Regeln fertiggestellt haben, verknüpfen Sie diese mit einer OU oder der Domäne. Anschließend wenden die Computer die Richtlinie an und setzen die hinterlegten Regeln um.

Die Umsetzung von AppLocker-Richtlinien testen Sie am besten durch einen Neustart oder indem Sie *gpupdate /force* in einer Eingabeaufforderung mit Administratorrechten eingeben.

Automatisches Erstellen von Regeln und Erzwingen von AppLocker

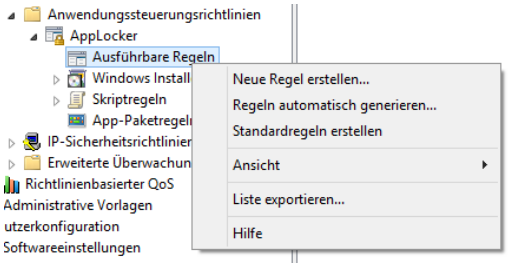
Sie können AppLocker auch veranlassen, automatisch Regeln zu erstellen. Dazu legen Sie einen bestimmten Ordner fest. Diesen Ordner scannt AppLocker automatisch nach neuen Programmen und nimmt diese direkt in die Regeln auf.

Klicken Sie zur Erstellung einer solchen automatischen Regel mit der rechten Maustaste auf *Ausführbare Regeln* und wählen Sie im Kontextmenü den Eintrag *Regeln automatisch generieren*. Wählen Sie im Assistenten den Ordner aus, welchen AppLocker einbinden soll, sowie die Benutzergruppe, für welche Sie die Regel anwenden wollen. Im Anschluss wählen Sie aus, auf welcher Grundlage AppLocker die Regel erstellen soll.

Auch hier haben Sie die Möglichkeit, den Herausgeber, den Dateihash oder einen Pfad zu verwenden, genauso wie bei den manuellen Regeln. Ähnliche Dateien lassen sich auch in gemeinsame

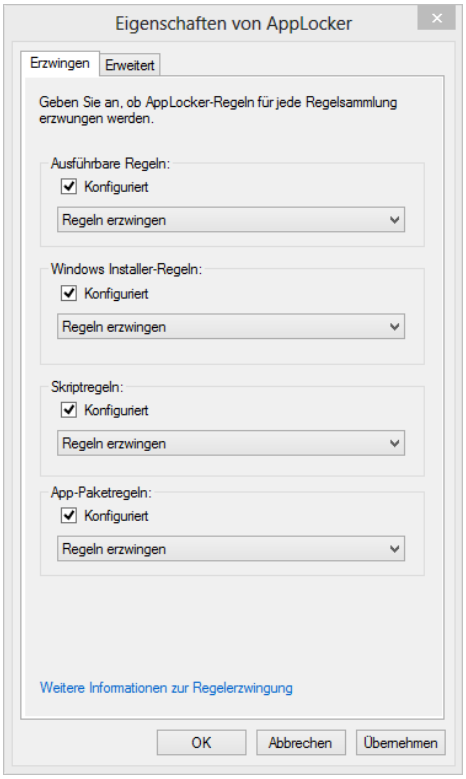
Regeln zusammenfassen. Anschließend erstellt der Assistent Zulassungsregeln für die gefundenen Programme. Auch diese Regeln können Sie nachträglich anpassen.

Abbildg. 19.32 AppLocker-Regeln automatisch erstellen



Klicken Sie auf AppLocker im linken Bereich der Konsole, können Sie auf der rechten Seite festlegen, wie sich AppLocker auf den Clientcomputern verhalten soll. Dazu wählen Sie die Option *Regelerzwingung konfigurieren*. Aktivieren Sie *Regeln erzwingen* oder die Einstellung *Nur überwachen*. Im Überwachungsmodus setzt AppLocker die Regeln nicht um, sondern protokolliert nur die betroffenen Anwendungen. Sie finden die Meldungen in der Ereignisanzeige über *Anwendungs- und Dienstprotokolle/Microsoft/AppLocker*.

Abbildg. 19.33 Konfigurieren von AppLocker



Auf der Registerkarte *Erweitert* aktivieren Sie die DLL-Regeln. Nach der Aktivierung finden Sie im linken Bereich der Konsole die neue Option *DLL-Regeln*. Hier erstellen Sie AppLocker-Regeln auf Basis von DLL-Dateien. Diesen Bereich sollten Unternehmen aber erst dann verwenden, wenn es bereits eine AppLocker-Infrastruktur gibt.

DLL-Regeln erstellen Sie genauso wie ausführbare Regeln. Der Unterschied dabei ist nur, dass Sie keine *.com*- oder *.exe*-Dateien auswählen, sondern DLL-Dateien, welche die Regel erfassen soll. Auch hier können Sie – wie bei ausführbaren Regeln – bestimmte Versionen sperren, erlauben oder filtern.

Die Erstellung dieser Regeln funktioniert genauso wie alle anderen Regeln. Das Filtern von DLL-Dateien kann die Clientcomputer stark ausbremsen und eine hohe Anzahl an Anwendungen ungewollt sperren.

Die Vorgängerversion von AppLocker sind die Richtlinien für Softwareeinschränkung (Windows Software Restrictions). Diese müssen Sie einsetzen, wenn Sie nicht kompatible Betriebssysteme für AppLocker im Einsatz haben. Die Richtlinien für Softwareeinschränkung unterstützen Windows XP/Vista, aber auch Windows Server 2003/2008.

Benutzerkontensteuerung über Richtlinien konfigurieren

In Unternehmen lässt sich das Verhalten der Benutzerkontensteuerung per Gruppenrichtlinie konfigurieren. Die dazu notwendigen Einstellungen finden Sie über *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Sicherheitsoptionen*.

Führt ein Anwender Aufgaben durch, die Administratorrechte benötigen, erscheint ein Bestätigungsfenster oder ein Authentifizierungsfenster, wenn Sie an einer Arbeitsstation als Standardbenutzer angemeldet sind. Auch auf diesem Weg lassen sich Anwendungen sperren.

Erstellen einer neuen Gruppenrichtlinie für sichere Kennwörter

Navigieren Sie zu den Einstellungen der Kennwörter unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Kontorichtlinien/Kennwortrichtlinien* in einer Gruppenrichtlinie, können Sie bestimmen, welche Struktur die Kennwörter der Anwender haben sollen. In Windows Server 2012 R2 gibt es verschiedene 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. 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 bleiben sollen, die ein Anwender bisher bereits verwendet hat. 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 speichert Windows die Kennwörter so, dass die Administratoren sie auslesen können. Sie sollten 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
- **Minimale Kennwortlänge** Der Wert legt fest, wie viele Zeichen ein Kennwort mindestens enthalten muss. Dafür wird ein Wert von acht Zeichen empfohlen.
- **Minimales Kennwortalter** Hier steuern Sie, wann ein Anwender ein Kennwort frühestens ändern 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.

Firewalleinstellungen über Gruppenrichtlinien setzen

Auf Client-PCs erstellen Sie neue Regeln in der Windows-Firewall über die erweiterte Konsole. Diese starten Sie durch Eingabe von *wf.msc* auf der Startseite. Sie können aber auch über Gruppenrichtlinien Firewallregeln erstellen und diese an die Clients verteilen.

Sie finden die Einstellungen über *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Windows-Firewall mit erweiterter Sicherheit.*

Hier können Sie eingehende und ausgehende Regeln festlegen. Die Oberfläche dazu ist die gleiche wie bei der lokalen Verwaltung der Firewall.

Microsoft Security Compliance Manager

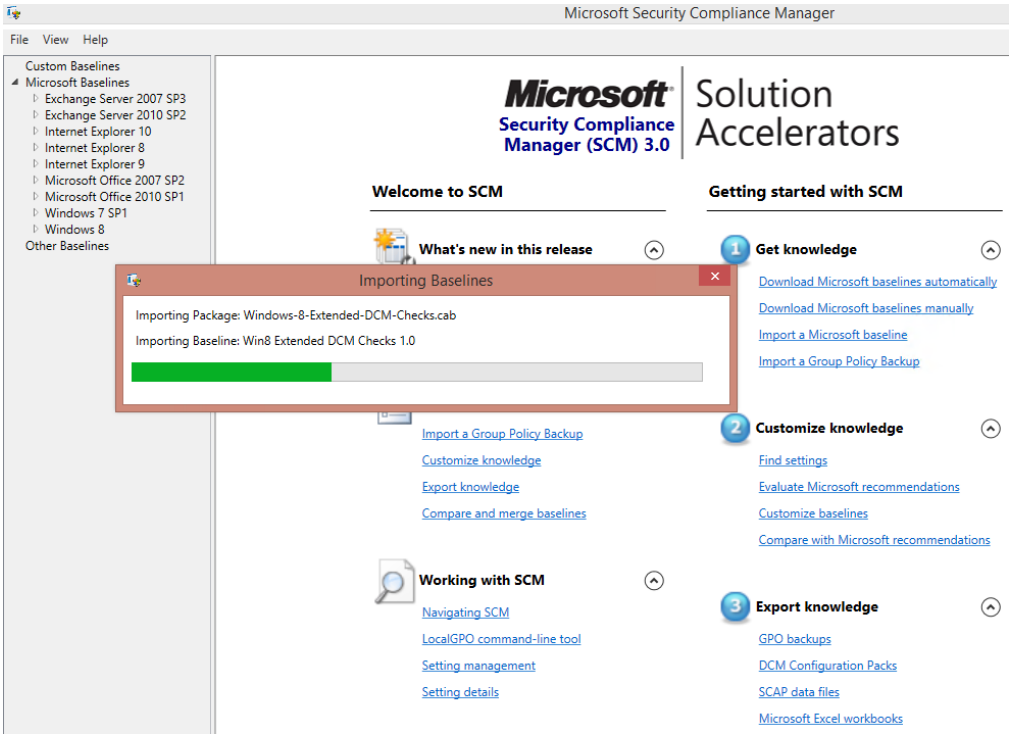
Wollen Sie Ihre Server optimal absichern, funktioniert das in Windows-Netzwerken vor allem über Gruppenrichtlinien. Dabei helfen Vorlagen und Tools, um das System besser abzusichern. Microsoft bietet dazu das kostenlose Tool Microsofts Security Compliance Manager (SCM). Microsoft bietet dazu das kostenlose Tool Security Compliance Manager (SCM) auf der Seite *http://www.microsoft.com/en-us/download/details.aspx?id=16776* [Ms179-K19-10].

Für Windows 8/8.1/2012/2012 R2 benötigen Sie SCM 3.0. Neben Windows-Computern lassen sich aber auch andere Programme und Microsoft-Server-Systeme mit SCM absichern. Internet Explorer 8/9, Office 2007/2010 und Exchange Server 2007/2010, inklusive der aktuellen Service Packs unterstützen ebenfalls SCM.

Weitere Tools, die bei der Optimierung der Sicherheit helfen, sind *Microsoft Attack Surface Analyzer* und der *Microsoft Baseline Security Analyzer*. Beide Tools stehen ebenfalls kostenlos zur Verfügung. Die Installation des Tools muss nicht auf einem Server erfolgen, sondern Administratoren können SCM problemlos auf der eigenen Arbeitsstation betreiben.

Allerdings muss auf der Arbeitsstation Windows 7/8/8.1 als 64-Bit-Version installiert sein. Wollen Sie später Einstellungen von SCM in eine Exceltabelle exportieren, muss auf dem entsprechenden Computer Excel 2007/2010/2013 installiert sein. Das ist allerdings nur optional und nur dann notwendig, wenn Sie verschiedene Einstellungen aus dem SCM in Excel importieren wollen.

Abbildg. 19.34 Computer und Server sichern Sie mit Richtlinien aus SCM ab



Grundlagen von Security Compliance Manager

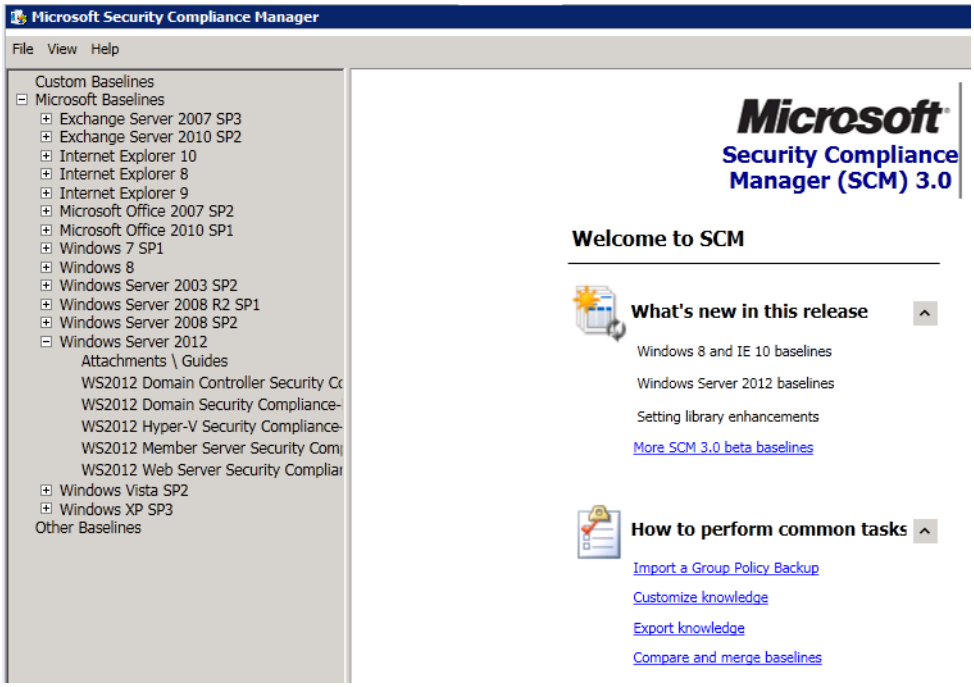
Bestandteil von Windows Server 2012 R2 ist der Security Configuration Wizard (SCW). Auch mit diesem Produkt lassen sich Server absichern. Alle diese Produkte arbeiten Hand in Hand und lassen sich auch parallel einsetzen.

SCM 2.5 unterstützt die Absicherung von Windows Server 2003/2008/2008 R2 sowie die Clientbetriebssysteme Windows XP/Vista und Windows 7. In der Version 2.5 des SCM ist noch keine Absicherung für Windows 8/8.1 und Windows Server 2012 R2 möglich. Für die beiden neuen Betriebssysteme benötigen Sie SCM 3.0. Neben Windows-Servern lassen sich aber auch andere Programme und Microsoft-Server-Systeme mit SCM absichern. Internet Explorer 8/9, Office 2007/2010 und Exchange Server 2007/2010 inklusive der aktuellen Service Packs unterstützt SCM.

Das neue Office 2013 sowie Internet Explorer 10 sind ebenfalls Bestandteil. Sie können SCM auch auf einer Arbeitsstation installieren, für den Betrieb ist kein Server oder Agent notwendig. Die Absicherung erfolgt komplett über eine Gruppenrichtlinieninfrastruktur. Alleinstehende Server können Sie aber auch absichern. Dazu lesen Sie die Richtlinien von SCM in eine lokale Sicherheitsrichtlinie ein.

Damit Sie SCM verwenden können, müssen Sie .NET Framework 4.0 über den Server-Manager installieren. Anschließend installieren Sie SCM 2.5 auf dem Rechner. Sie können SCM nicht auf Windows Server 2012 R2 oder Windows 8/8.1 installieren. Verwenden Sie bei dieser Version am besten einen Rechner mit Windows 7 SP1 oder Windows Server 2008 R2 SP1. Ab SCM 3.0 können Sie das Tool auch auf Servern mit Windows Server 2012 R2 installieren.

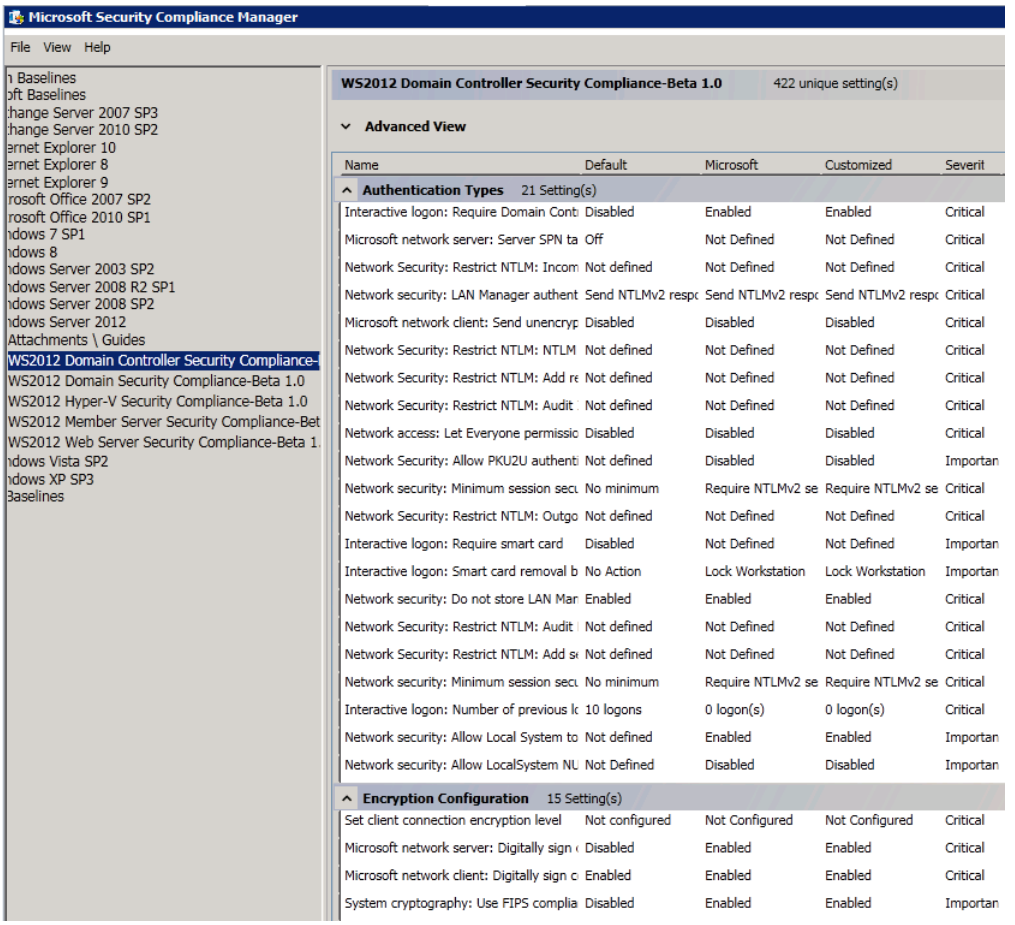
Abbildg. 19.35 Absichern von Windows Server 2012 R2 mit SCM 3.0



SCM installieren

Das Tool benötigt Zugriff auf eine Datenbank. Sie können SQL Server Express-Edition verwenden oder eine vollständige Version einer aktuellen SQL Server-Version. Nach der Installation starten Sie das Tool über dessen Programmgruppe. Lassen Sie zunächst nach dem Start die Daten des Tools einlesen. Auf der linken Seite wählen Sie anschließend das Produkt aus, welches Sie absichern wollen. Sie können zum Beispiel auch für Windows Server 2012 R2 einzelne Serverrollen besonders absichern. Klicken Sie auf eine Baseline, sehen Sie im rechten Bereich, welche Einstellungen bereits gesetzt sind.

Abbildg. 19.36 Anzeigen der Einstellungen für eine Richtlinie



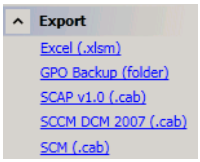
Um einen Server abzusichern, klicken Sie auf eine vorhandene Standard-Baseline und erstellen mit dem Befehl *Duplicate* im rechten Bereich eine Kopie der Vorlage. Die neue Richtlinie erscheint anschließend bei *Custom Baselines* im oberen Bereich der Konsole.

Der nächste Schritt besteht darin, dass Sie die Einstellungen der Richtlinie an Ihre Bedürfnisse anpassen. Die meisten Einstellungen belassen Sie so wie sie sind, um den entsprechenden Server optimal abzusichern. Der Vorteil im Vergleich einer leeren Gruppenrichtlinie ist, dass alle Einstellungen in der Richtlinie bereits so gesetzt sind, wie sie Microsoft als optimal und sicher betrachtet.

Haben Sie alle Einstellungen vorgenommen, besteht der nächste Schritt darin, dass Sie die Baseline als Gruppenrichtlinie exportieren. Sie können aber auch mit anderen Techniken die Richtlinie einlesen. Der Import als Gruppenrichtlinie ist aber am einfachsten für Active Directory-Domänen. Den Ordner mit dem Export integrieren Sie später dann in der Gruppenrichtlinienverwaltungskonsole entweder als neue Richtlinie oder Sie integrieren die Einstellungen in eine bereits vorhandene Richtlinie.

In eine bestehende Gruppenrichtlinie übernehmen Sie die Einstellungen durch Auswahl von *Einstellungen importieren* im Kontextmenü. Setzen Sie im Unternehmen System Center Configuration Manager ein, können Sie die Einstellungen aber auch in einem kompatiblen Format für SCCM exportieren und einlesen.

Abbildg. 19.37 Exportieren und Importieren von Einstellungen des SCM in eine neue Gruppenrichtlinie



In SCM können Sie über den Bereich *Import* exportierte Gruppenrichtlinien aus Active Directory auch in SCM einlesen. Diese Richtlinien können Sie dann später mit einer von Ihnen erstellten Richtlinie in SCM zusammenführen und diese Richtlinie wiederum exportieren. Mit der Gruppenrichtlinienverwaltung (GPMC) können Sie einzelne Gruppenrichtlinien sichern und wiederherstellen, ohne eine Datensicherung des Active Directory verwenden zu müssen. Da die Datensicherung von Gruppenrichtlinien in Dateien gespeichert wird, können Sie die Sicherung auch zum Erstellen neuer Gruppenrichtlinien verwenden.

Um eine exportierte Richtlinie von SCM in einer Gruppenrichtlinie zu importieren, öffnen Sie den Gruppenrichtlinienverwaltungs-Editor und erstellen entweder eine neue GPO oder klicken mit der rechten Maustaste auf eine bestehende GPO. Wählen Sie danach *Einstellungen importieren* und navigieren Sie anschließend zum Ordner, in den Sie in SCM die Einstellungen exportiert haben. Schließen Sie danach den Importvorgang ab.

Klicken Sie auf eine Gruppenrichtlinie im Gruppenrichtlinienverwaltungs-Editor, lassen Sie sich auf der Registerkarte *Einstellungen* die neuen Einstellungen anzeigen. Um Gruppenrichtlinien von Active Directory in SCM zu integrieren, klicken Sie diese zunächst im Gruppenrichtlinienverwaltungs-Editor an und sichern Sie die Richtlinie. Kopieren Sie den Sicherungsordner auf den PC mit SCM und lassen Sie die Richtlinie importieren.

Setzen Sie kein Active Directory ein oder wollen Sie einen alleinstehenden Server absichern, haben Sie auch die Möglichkeit, die Baseline in eine lokale Sicherheitsrichtlinie zu integrieren. Dazu verwenden Sie das Befehlszeilentool LocalGPO aus der Programmgruppe *Microsoft Security Compliance Manager*. Damit lassen sich Einstellungen lokal aus SCM in eine Richtlinie auf dem Server importieren.

Haben Sie mehrere Baselines im Einsatz, können Sie diese auch miteinander vergleichen oder in eine gemeinsame Baseline zusammenführen. Dazu verwenden Sie den Menüpunkt *Compare/Merge* in der Verwaltungsoberfläche des SCM auf der rechten Seite. Wählen Sie aus, mit welcher Baseline Sie die aktuell ausgewählte Baseline vergleichen wollen. Sie können hier auch selbst erstellte Baselines mit den Standard-Baselines vergleichen. Auf diesem Weg sehen Sie die Unterschiede zwischen den Baselines.

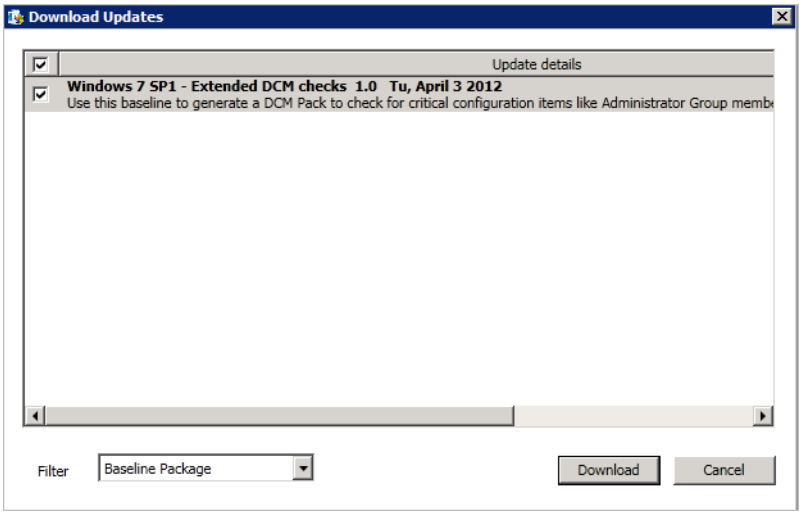
Sind Baselines miteinander kompatibel, können Sie auf diesem Weg mit *Merge Baselines* die Einstellungen zusammenführen. Diese Einstellungen können Sie wiederum exportieren und eine GPO wieder importieren. Während der Zusammenführung erstellen Sie eine neue Baseline, deren Namen Sie im Assistenten angeben.

Um eine bessere Übersicht zu erhalten oder einzelne Einstellungen in produktive Umgebungen nicht zu übernehmen, klicken Sie diese in der Baseline an und wählen dann im rechten Bereich *Delete*. Auf diese Weise entfernen Sie Einstellungen aus der Baseline. Über *Add* können Sie Einstellungen auch wieder hinzufügen. Mit *Lock* verhindern Sie die Möglichkeit, Einstellungen für eine Baseline zu ändern. Die Bearbeitung aktivieren Sie dann wieder mit *Edit*.

Sie sollten in regelmäßigen Abständen die Baselines in SCM über das Internet aktualisieren lassen. Verwenden Sie dazu den Link *Download Microsoft Baselines manually* im Startbildschirm des SCM. Das Tool öffnet den Internet Explorer, verbindet sich mit dem Internet und schlägt neue Baselines zur Installation vor, wenn diese zur Verfügung stehen. Über die Seite *http://social.technet.microsoft.com/wiki/contents/articles/1865.microsoft-security-compliance-manager-scm-baseline-download-help-en-us.aspx* [Ms179-K19-11] können Sie ebenso Baselines herunterladen und in SCM integrieren.

Einfacher lassen sich Baselines mit dem Menüpunkt *Download Microsoft baselines automatically* übernehmen. Der Assistent scannt nach neuen Baselines oder neuen Versionen bereits vorhandener Baselines und ermöglicht deren Integration in SCM über einen Assistenten.

Abbildg. 19.38 Aktualisieren von Baselines in SCM 3.0



Baselines bearbeiten und dokumentieren

Haben Sie die Baseline erstellt und die Bearbeitung gestartet, finden Sie im mittleren Bereich mehrere Spalten, in denen Sie die Einstellungen festlegen. Ganz links sehen Sie den Namen der Einstellung. Im Bereich *Default* ist die Standardeinstellung des entsprechenden Serversystems zu sehen. Die Einstellung *Microsoft* zeigt die Empfehlung von Microsoft für diesen Bereich. Ändern Sie Einstellungen ab, finden Sie diese in der Spalte *Customized*. Die Spalte *Severit* zeigt die Wichtigkeit an, die Microsoft der entsprechenden Einstellung zumisst.

Die letzte Spalte *Path* zeigt an, wo die Einstellung in der Registry zu finden ist oder ob die Einstellung über die PowerShell eingestellt wird.

Haben Sie eigene Baselines erstellt, sind diese im Bereich *Custom Baselines* zu finden. Hier gibt es auch den neuen Menüpunkt *Attachments/Guides*. Über diesen Bereich können Sie zu Baselines eigene Dokumentationen, Tools und Informationen anhängen, die für die Umsetzung notwendig sind. Bei den Anhängen handelt es sich nicht um Konfigurationsdateien, sondern vor allem um unterstützende Informationen für die Baseline sowie Dokumentationen. Anhänge lassen sich auf diesem Weg ausdrucken, anzeigen, exportieren, speichern oder direkt anzeigen.

Alle Änderungen, die Sie an Baselines in SCM vornehmen, protokolliert das Tool. Die Protokollierung öffnen Sie über *View/Baseline Change Log*. Im Fenster sehen Sie alle Aktionen, die Sie in SCM vorgenommen haben, auch Änderungen an den Baselines.

Einstellungen exportieren und importieren

Haben Sie alle Einstellungen in einer oder mehreren Baselines abgeschlossen, können Sie im rechten Bereich bei *Export* auswählen, wie Sie diese Einstellungen auf den Servern verteilen oder dokumentieren wollen. Dazu stehen die folgenden Optionen zur Verfügung:

- **Excel** Hier erstellt das Tool eine XLSM-Datei, die mit Excel 2007/2010/2013 kompatibel ist. Die Datei können Sie natürlich jederzeit auch für andere Zwecke nutzen. Sie müssen dazu nicht unbedingt auf dem Zielrechner SCM installieren.
- **GPO Backup** Erstellt einen Ordner mit einer GPO-Sicherung der Baseline. Diese können Sie in der produktiven Umgebung wieder importieren wie eine normale Gruppenrichtlinie. Dazu erstellen Sie eine neue Gruppenrichtlinie in Active Directory und stellen die Einstellungen aus dem GPO-Backup in dieser neuen Sicherung wieder her.
- **SCAP** Erstellt eine Datei auf Basis von Security Content Automation Protocol (SCAP). Dieses kann auch in anderen Systemen verwendet werden.
- **SCCM DCM** Erstellt Pakete, die kompatibel mit Microsoft System Center Configuration Manager sind. Sie lassen sich zur Überwachung und Konfiguration der angebundenen Zielcomputer nutzen.
- **SCM** Erstellt eine *.cab*-Datei, die Sie in anderen SCM-Installation wieder importieren können und dadurch weiter bearbeiten

Haben Sie einen SCM-kompatiblen Export durchgeführt, können Sie diese Einstellungen zwar nicht für den Import von Gruppenrichtlinien nutzen, aber Sie können die Einstellungen in der SCM-Oberfläche wieder importieren und weiter bearbeiten. Den Import starten Sie entweder über den Menübereich *Import* auf der rechten Seite oder Sie verwenden die Tastenkombination Strg + I, I. Im *Import Baselines Wizard* wählen Sie das Paket aus, welches Sie importieren wollen. Klicken Sie auf *Next*, liest der Assistent die Daten ein und zeigt die integrierten Baselines an. Mit einem Klick auf *Import* integriert der Assistent die Baselines in der *.cab*-Datei in SCM auf dem lokalen Rechner. Sie haben in diesem Bereich auch die Möglichkeit, Datensicherungen von Gruppenrichtlinien zu importieren. Dazu wählen Sie in diesem Bereich die Option *Import/GP Backup (folder)* aus.

Einstellungen skripten, importieren und exportieren

Um Windows-Server mit SCM abzusichern, ist aber kein Active Directory notwendig. Die Einstellungen lassen sich auch in lokale Richtlinien einlesen. Dazu stellt SCM das Zusatztool LocalGPO zur Verfügung. Mit dem Tool aus der Programmgruppe Microsoft Security Compliance Manager lassen sich Einstellungen lokal aus SCM in eine Richtlinie auf dem Server importieren. Das Tool arbeitet in der Eingabeaufforderung und stellt verschiedene Optionen für den Import zur Verfügung. LocalGPO ist vor allem für Server gedacht, die über keine Domänenanbindung verfügen. Im ersten Schritt installieren Sie das Tool auf dem Server und können anschließend in der Eingabeaufforderung Einstellungen importieren.

Nach der Installation starten Sie dazu LocalGPO in der Programmgruppe *LocalGPO*. Um die Einstellungen einer SCM-Baseline auf einem lokalen Server zu importieren, erstellen Sie zunächst die Baseline, wie zuvor beschrieben. Anschließend exportieren Sie diese als GPO-Backup in einen Ordner. Diesen kopieren Sie auf den Server, auf dem Sie die Richtlinien umsetzen wollen. Anschließend geben Sie den Befehl *cscript LocalGPO.wsf /Path:<Pfad zur GPO-Sicherung>* ein.

Bei der Umsetzung der neuen Einstellungen speichert LocalGPO die Einstellungen der lokalen Richtlinie. So können Sie diese jederzeit wiederherstellen. Um die ursprünglichen Einstellungen auf dem Server wiederherzustellen, verwenden Sie den Befehl *cscript LocalGPO.wsf /Restore*.

Mit LocalGPO haben Sie auch die Möglichkeit, die Einstellungen der lokalen Sicherheitsrichtlinie in eine GPO-Datensicherung zu sichern. Diese können Sie zum einen ebenfalls zum Wiederherstellen nutzen, indem Sie diese auf einem Server wieder importieren. Zum anderen haben Sie die Möglichkeit, diese Sicherung auf anderen lokalen Servern zu importieren. Außerdem können Sie auf Basis dieser Sicherung eine neue Active Directory-Gruppenrichtlinie erstellen und diese Einstellungen importieren. Verwenden Sie dazu den Befehl *cscript LocalGPO.wsf /Path: <Pfad> /Export*. Importieren können Sie diese Sicherung entweder mit LocalGPO oder Sie verwenden die Gruppenrichtlinienverwaltungskonsole.

Sie können aber auch die lokale Sicherheitsrichtlinie eines Servers in ein GPOPack exportieren. Mit diesem können Sie die Sicherheitseinstellungen auf einem anderen Server importieren, ohne dass Sie *LocalGPO* auf dem Zielsystem installieren müssen. Verwenden Sie dazu den Befehl *cscript LocalGPO.wsf /Path: "<Pfad>" /Export /GPOPack*. Mehr zu diesem Thema lesen Sie auf der Internetseite *http://blogs.technet.com/b/secguide/archive/2011/07/05/scm-v2-beta-localgpo-rocks.aspx* [Ms179-K19-12].

Zusammenfassung

In diesem Kapitel sind wir ausführlich darauf eingegangen, wie Sie Gruppenrichtlinien mit Windows Server 2012 R2 verwenden. Wir haben Ihnen auch gezeigt, wie Sie Tools und Programme über Gruppenrichtlinien verteilen. Auch die Absicherung von Servern mit dem neuen Security Compliance Manager 3.0 war Thema dieses Kapitels.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie Dateiserver mit Windows Server 2012 R2 optimal betreiben.

Teil E

Dateiserver und Freigaben

Kapitel 20

Dateiserver und Daten im Netzwerk freigeben

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen den Umgang mit Windows Server 2012 R2 als Datei- oder Druckserver. Wir gehen dabei auf die Möglichkeiten ein, Freigaben zu erstellen und zu verwalten, aber auch auf die Sicherheitsoptionen und Einstellungen, die auf einem Dateiserver notwendig sind.

Damit auf einen Windows Server 2012 R2 über Freigaben zugegriffen werden kann, müssen Sie zunächst sicherstellen, dass im Netzwerk- und Freigabecenter die Dateifreigaben aktiviert sind. Erst dann ist der Zugriff über das Netzwerk möglich. Installieren Sie auch auf dem Server die Rolle *Dateiserver*, um auf alle Möglichkeiten zugreifen zu können. In Kapitel 5 gehen wir auf die Verwaltung der Datenträger ein. Lesen Sie sich zum Aufbau eines Dateiservers daher auch das Kapitel 5 durch. In Kapitel 4 sind wir ebenfalls auf den Rollendienst eingegangen. Daher sollten Sie sich auch das Kapitel 4 ansehen.

Berechtigungen für Dateien und Ordner verwalten

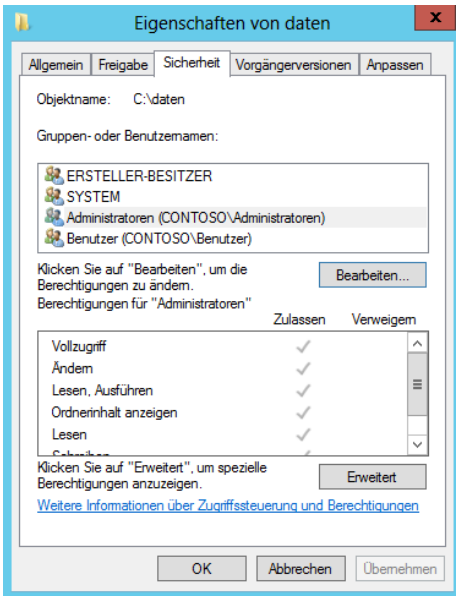
Die Berechtigungen im Dateisystem sind in der Zugriffssteuerungsliste (Access Control List, ACL) gespeichert. Während der Anmeldung generiert Windows für den Benutzer ein sogenanntes Zugriffstoken, das die Sicherheits-ID (Security ID, SID) des Benutzerkontos enthält sowie die SIDs der Gruppen in denen der Benutzer Mitglied ist.

Beim Zugriff auf eine Datei vergleicht Windows die Einträge des Token mit der ACL und ermittelt daraus die Berechtigung. Dazu addiert das System die Berechtigungen für jeden übereinstimmenden Eintrag. Ein Benutzer bekommt die Berechtigungen, die seinem Konto zugewiesen sind, sowie alle Berechtigungen, die den Gruppen zugewiesen sind, in denen er Mitglied ist.

Geben Sie einem Benutzerkonto die Berechtigung *Lesen* 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 Ordners oder der Datei die Registerkarte *Sicherheit*. Mehr zu diesem Thema lesen Sie auch in Kapitel 18.

Zusätzlich ist es möglich, einzelnen Benutzern oder Gruppen Berechtigungen zu verweigern, wobei die Verweigerung immer Vorrang hat. Auch wenn ein Benutzer in einer Gruppe Mitglied ist, die Berechtigungen auf einen Ordner hat, verweigert Windows den Zugriff, wenn er über eine Gruppe oder sein Benutzerkonto in der Verweigerungsliste eingetragen ist.

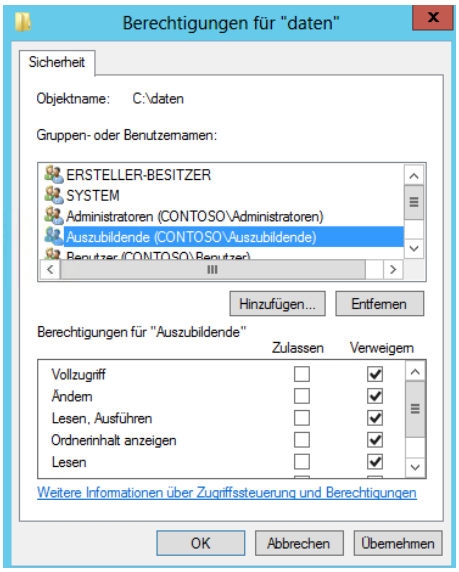
Abbildg. 20.1 Verwalten von Berechtigungen für Ordner und Dateien



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.

Abbildg. 20.2 Verweigern von Berechtigungen für bestimmte Gruppen



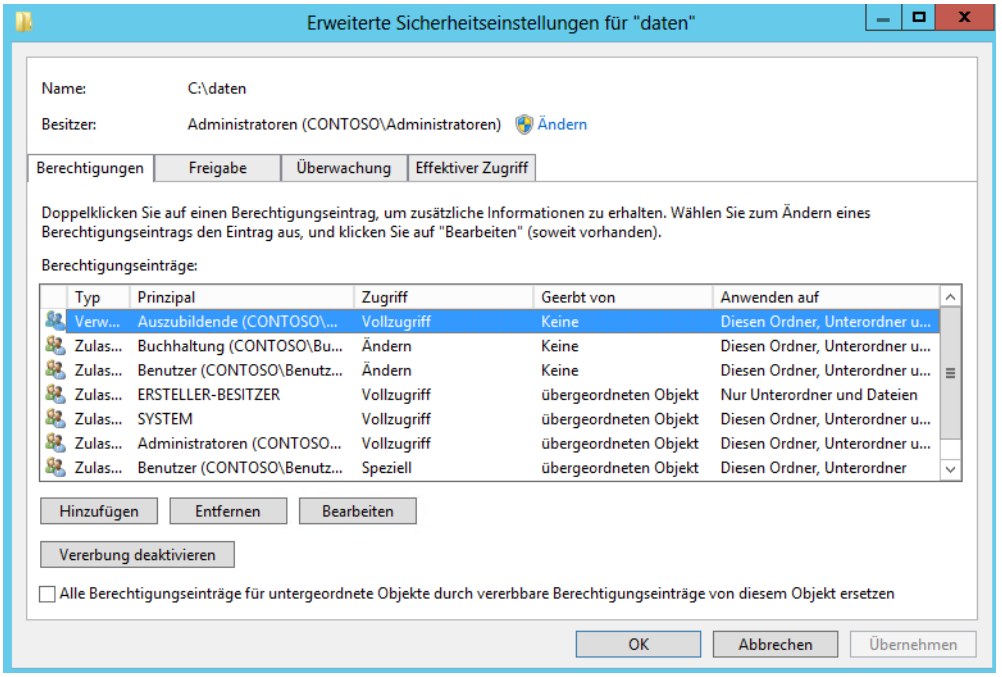
Wenn der Gruppe *Buchhaltung* der Zugriff auf diese Datei erlaubt ist, erhalten auch die Auszubildenden Zugriff, da sie Mitglied der Gruppe sind. Sie können der Gruppe *Auszubildende* den Zugriff verweigern. So erhalten die Auszubildenden zwar den Zugriff durch die Mitgliedschaft in der Gruppe *Buchhaltung*, der ihnen aber durch die Mitgliedschaft in der Gruppe *Auszubildende* verweigert wird.

Erweiterte Berechtigungen auf Ordner

Um spezielle Berechtigungen zu setzen und weitere Einstellungen vorzunehmen, wählen Sie auf der Registerkarte *Sicherheit* die Schaltfläche *Erweitert*. 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. 20.3 Bearbeiten der erweiterten Berechtigungen für Ordner



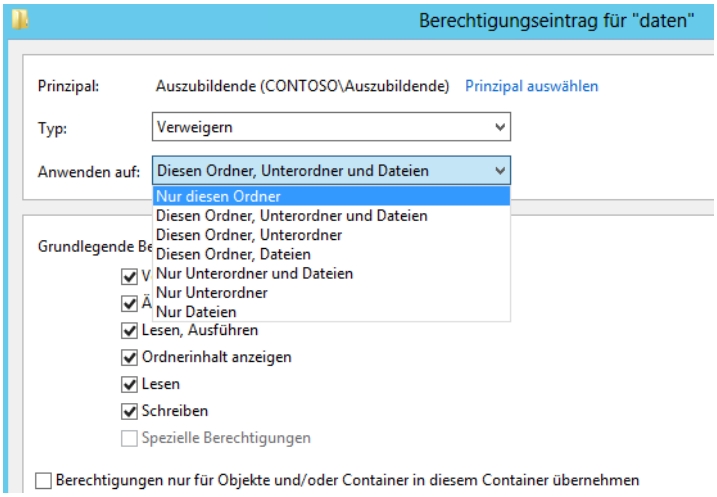
Damit Sie für den Ordner erweiterte Berechtigungen zuweisen können, müssen Sie entscheiden, wie weit sich diese Berechtigungen auswirken. Dazu wählen Sie aus der Liste *Übernehmen für* in den Eigenschaften eines Eintrags aus, in welchem Bereich sich die speziellen Berechtigungen auswirken sollen.

- **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 Ordnerstruktur angewendet und gelten für alle Ordner und Dateien unterhalb dieses Ordners
- **Diesen Ordner, Unterordner** Die Berechtigungen werden nur auf diesen Ordner und alle Unterordner gesetzt, Berechtigungen auf Dateien werden nicht gesetzt
- **Diesen Ordner, Dateien** Die Berechtigungen gelten nur für diesen Ordner und die darin enthaltenen Dateien
- **Nur Unterordner und Dateien** Dieser Ordner wird von der Vergabe der Berechtigungen ausgenommen, sondern auf darin enthaltene Dateien und andere Ordner gesetzt
- **Nur Unterordner** Dieser Ordner wird von der Vergabe der Berechtigungen ausgenommen und nur auf darin enthaltene Ordner gesetzt
- **Nur Dateien** Dieser Ordner 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.

Abbildg. 20.4 Bearbeiten der erweiterten Reche für einen Ordner und einen Benutzer



Zunächst werden nur die grundlegenden Berechtigungen angezeigt. Klicken Sie daher auf den Link *Erweiterte Berechtigungen* anzeigen, um zusätzliche Berechtigungen angezeigt zu bekommen.

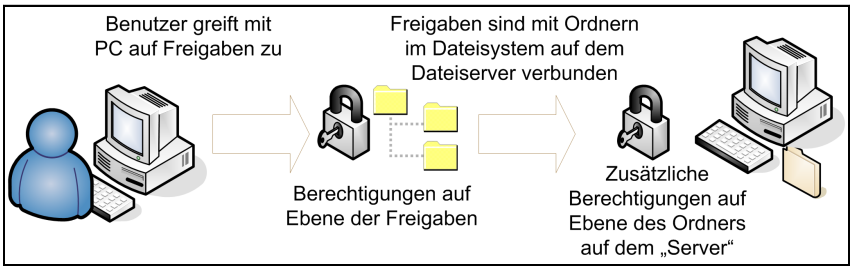
Berechtigungen verstehen

Weisen Sie einem Benutzerkonto die Berechtigung *Lesen* für einen Ordner zu und bekommt zusätzlich eine Gruppe, in der dieser Benutzer Mitglied ist, die Berechtigung *Schreiben* zugewiesen, ergeben die effektiven Berechtigungen *Lesen* und *Schreiben*.

Es gelten grundsätzlich die engsten Einschränkungen der Zugriffsberechtigungen. Wenn ein Benutzer Vollzugriff auf eine Freigabe hat und ein Ordner auf dem PC nur lesen darf, darf er es auch tatsächlich nur lesen, auch wenn er per Vollzugriff über das Netzwerk zugreift.

Hat er im Dateisystem *Vollzugriff* und wurde auf die Freigabe nur das Leserecht vergeben, darf er auf den Ordner über das Netzwerk nur lesend zugreifen. Er kann allerdings lokal auf dem Computer oder über andere überlappende Freigaben, die diese Einschränkung nicht haben, mit mehr Rechten zugreifen. Die Berechtigungen bilden daher immer eine Schnittmenge zwischen Freigabeberechtigungen und Berechtigungen auf dem Dateisystem (NTFS).

Abbildg. 20.5 Berechtigungsebenen in Windows



Berechtigungen für den Zugriff über das Netzwerk nehmen Sie über die Registerkarte *Freigabe* in den Eigenschaften des Ordners über die Schaltfläche *Erweiterte Freigabe* vor. Mit *Berechtigungen* legen Sie fest, wer über das Netzwerk auf den PC zugreifen darf. Den jeweiligen Benutzer müssen Sie vorher auf dem PC mit der Freigabe anlegen.

Die Festlegung auf NTFS-Ebene, also für das Dateisystem, erfolgt über die Eigenschaften eines Ordners auf der Registerkarte *Sicherheit*. Nach jeweils einem Klick auf die Schaltflächen *Bearbeiten* und *Hinzufügen* können Sie neue Benutzer, denen Sie Berechtigungen gewähren wollen, hinzufügen. Dabei haben Sie folgende Möglichkeiten:

- **Vollzugriff** Erlaubt den vollen Zugriff auf den Ordner oder die Datei. Bei Ordnern bedeutet das, dass Benutzer Dateien hinzufügen und löschen dürfen. Bei Dateien stehen alle Funktionen zur Verfügung. Dazu gehört auch die Veränderung von Zugriffsberechtigungen. Mit diesem Recht sollten Sie vorsichtig umgehen.
- **Ändern** Die Berechtigungen sind im Vergleich mit dem Vollzugriff auf das Schreiben, Lesen, Ändern und Löschen beschränkt. Benutzer können keine Berechtigungen erteilen, sonst aber alles mit den Dateien machen.
- **Lesen, Ausführen** Für Programmdateien relevant, da diese ausgeführt werden dürfen. Fehlt dieses Recht, darf ein Benutzer keine Programme starten, die in diesem Ordner gespeichert sind.
- **Ordnerinhalt auflisten (nur bei Ordnern)** Benutzer dürfen den Inhalt des Ordners anzeigen. Die Inhalte der Dateien im Ordner lassen sich aber nicht anzeigen.
- **Lesen** Definiert, dass eine Datei gelesen, aber nicht ausgeführt oder geöffnet werden darf
- **Schreiben** Die Datei darf verändert, jedoch nicht gelöscht werden. Anwender dürfen nur Daten hinzufügen.

Mit dem Befehlszeilentool Openfiles können Sie Dateien und Ordner, die auf einem System geöffnet wurden, auflisten und 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.

Erst nach der Aktivierung dieses Flags werden mit Openfiles geöffnete Dateien angezeigt. Nachdem Sie das Flag gesetzt haben, müssen Sie den Computer neu starten. Wenn Sie nach dem Neustart in der Eingabeaufforderung *openfiles* eingeben, werden die geöffneten Dateien angezeigt.

Möchte man feststellen, welche Dateien auf einem wechselbaren Datenträger (zum Beispiel USB-Stick) geöffnet sind, empfiehlt sich der Befehl *openfiles |find /i "z:"*, wobei z: der Laufwerkbuchstabe des USB-Sticks 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 <user>*. Als *<id>* wird die von Openfiles mitgeteilte ID eingetragen, als *<user>* die mitgeteilte Nutzerkennung.

Abbildg. 20.6 Anzeigen geöffneter Dateien

```
C:\Users\Administrator>openfiles
FEHLER: Daten können nicht abgefragt werden.
Das System konnte die eingegebene Umgebungsoption nicht finden.


Über das Netzwerk über lokalen Freigaben geöffnete Dateien:
-----------------------------------------------

Kennung  Zugriff durch        Typ        Open File (Pfad\ausführbare Datei)
======== ==================== ========== ====================================
136      joost                Windows    C:\daten\
138      joost                Windows    C:\..B2-311C-4DC2-8398-D6A170DA28EA}
139      joost                Windows    C:\..\DomainSysvol
140      joost                Windows    C:\..\DomainSysvol\GPO
141      joost                Windows    C:\..\DomainSysvol\GPO\Machine
142      joost                Windows    C:\..\GPO\Machine\microsoft
143      joost                Windows    C:\..\Machine\microsoft\windows nt
144      joost                Windows    C:\..\microsoft\windows nt\SecEdit
145      joost                Windows    C:\..\GPO\Machine\Preferences
146      joost                Windows    C:\..\Machine\Preferences\Folders
147      joost                Windows    C:\..\GPO\Machine\Scripts
148      joost                Windows    C:\..\GPO\Machine\Scripts\Shutdown
149      joost                Windows    C:\..\GPO\Machine\Scripts\Startup
150      joost                Windows    C:\..\DomainSysvol\GPO\User
151      joost                Windows    C:\daten\joost
157      joost                Windows    C:\daten\
158      joost                Windows    C:\daten\manifest.xml
```

So setzen Sie diese Berechtigungen optimal:

1. Um Berechtigungen für einen Ordner oder eine Datei zu setzen, wählen Sie in den Eigenschaften des Ordners oder der Datei die Registerkarte *Sicherheit*.
2. Im oberen Bereich sehen Sie, welche Benutzer oder Gruppen bereits Berechtigungen für den Ordner haben.
3. Klicken Sie im oberen Bereich auf eine Gruppe oder einen Benutzer, sehen Sie dessen Standardrechte im unteren Bereich.
4. Über die Schaltfläche *Bearbeiten* können Sie die Berechtigungen steuern.
5. Klicken Sie auf *Hinzufügen*, um neue Benutzer oder Gruppen der Liste hinzuzufügen, oder auf *Entfernen*, um eine Gruppe zu löschen.

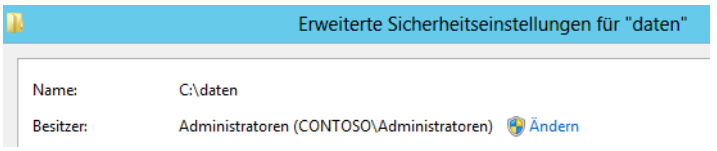
6. Wollen Sie Benutzer hinzufügen, klicken Sie erst auf *Hinzufügen* und anschließend im neuen Fenster auf *Erweitert*.
7. Klicken Sie im neuen Fenster auf *Jetzt suchen*. Windows zeigt dann alle Benutzerkonten und Gruppen an, die Sie auf dem Computer angelegt haben.
8. Wählen Sie das Benutzerkonto aus, dem Sie Rechte erteilen wollen.
9. Das Benutzerkonto steht jetzt in der Liste und Sie können zunächst Standardrechte erteilen. Was die verschiedenen Rechte bedeuten, ist nachfolgend erläutert.

Besitzer für ein Objekt festlegen

Der Objektbesitzer ist der Anwender mit den umfangreichsten Rechten für einen Ordner oder eine Datei. Vor allem wenn Anwender versehentlich auch den Administrator von der Berechtigungsliste streichen, kommt dem Objektbesitzer eine besondere Bedeutung zu. Dieser kann nämlich auf den Administrator geändert werden. So lassen sich auch versehentlich gesperrte Ordner durch die Hintertür wieder öffnen:

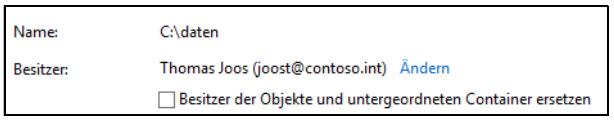
1. Um den Besitzer einer Datei festzustellen oder zu ändern, öffnen Sie zunächst die Eigenschaften des Objekts und wählen dort die Registerkarte *Sicherheit*.
2. Anschließend klicken Sie auf die Schaltfläche *Erweitert*.
3. Auf der Registerkarte *Berechtigungen* sehen Sie unter *Besitzer* den Inhaber dieses Objekts.

Abbildg. 20.7 Anpassen des Objektbesitzers



4. Um den Besitz zu übernehmen, klicken Sie auf *Ändern* und wählen dann das Konto in der Liste aus.
5. Wollen Sie den Besitzer nicht nur für diesen Ordner, sondern auch für alle Unterordner und darin enthaltenen Dateien ersetzen, aktivieren Sie das Kontrollkästchen *Besitzer der Objekte und untergeordneten Container ersetzen*.

Abbildg. 20.8 Objektbesitzer in Unterordner übernehmen

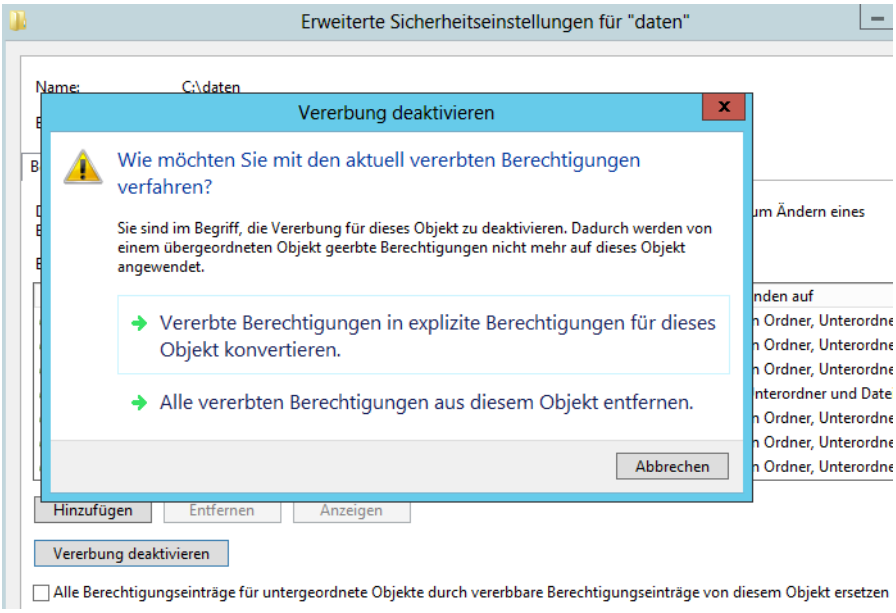


Vererbung von Berechtigungen

Grundsätzlich gilt bei Ordnerstrukturen das Prinzip der Vererbung. Das heißt, eine Berechtigung, die ein Benutzer auf einen Ordner erhält, erhält er auch auf die darin enthaltenen Verzeichnisse und Dateien. Weisen Sie einem Benutzerkonto die Berechtigung *Ändern* für einen Ordner zu, sehen Sie in den untergeordneten Ordnern, dass der Benutzer die gleichen Berechtigungen hat. Allerdings sind die entsprechenden Felder grau unterlegt. Damit wird angezeigt, dass die Berechtigungen nicht explizit in diesem Ordner zugewiesen werden, sondern vom übergeordneten Ordner vererbt sind.

Sie können für Unterordner einzelne Rechte verweigern. Wählen Sie auf der Registerkarte *Sicherheit* die Schaltfläche *Erweitert*. Mit der Schaltfläche *Vererbung deaktivieren*, schalten Sie die Berechtigungsweitergabe ab. Anschließend können Sie bereits gesetzte Rechte übernehmen oder die Liste löschen lassen und neu setzen. Sie können über die Schaltfläche auch die Vererbung wieder aktivieren.

Abbildg. 20.9 Deaktivieren der Vererbung für einen Ordner

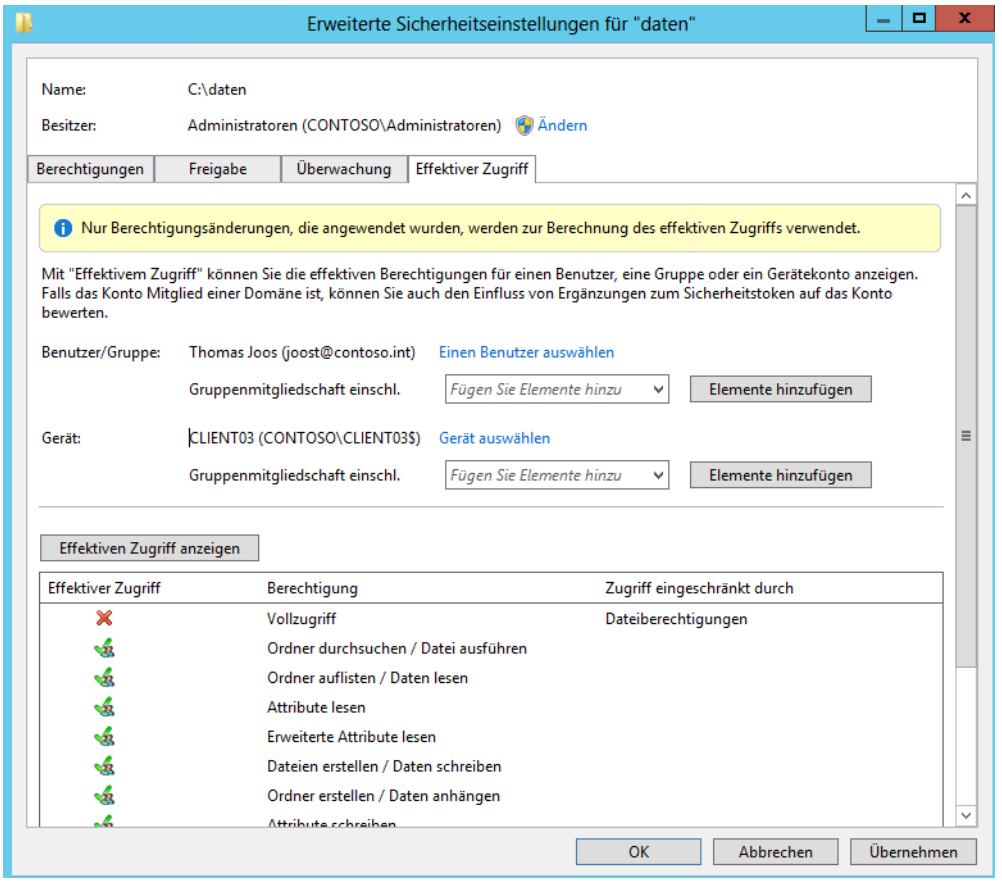


Wichtig ist noch das Kontrollkästchen *Alle Berechtigungseinträge für untergeordnete Objekte durch vererbbare Berechtigungseinträge von diesem Objekt ersetzen*. Aktivieren Sie diese Option, übernimmt Windows die hier gesetzten Rechte für alle Ordner und Dateien, die in dem aktuellen Ordner gespeichert sind. Windows setzt alle bereits konfigurierten Berechtigungen zurück. In der Liste der Berechtigungen sehen Sie den Vererbungsstatus von Berechtigungen in der Spalte *Geerbt von*.

Effektive Berechtigungen

Um die effektiven Berechtigungen anzuzeigen, öffnen Sie in den Eigenschaften des Ordners die Registerkarte *Sicherheit* und dann die erweiterten Einstellungen. Wählen Sie die Registerkarte *Effektiver Zugriff* aus. Sie sehen alle speziellen Berechtigungen, die der Benutzer in Summe hat. Um die Berechtigungen für einen anderen Benutzer anzuzeigen, wählen Sie über *Einen Benutzer auswählen* ein anderes Konto aus.

Abbildg. 20.10 Anzeigen der effektiven Berechtigungen eines Benutzers für einen Ordner



Tools zur Überwachung von Berechtigungen

In diesem Abschnitt gehen wir auf Tools ein, die dabei helfen, Berechtigungen für Dateien und Ordner zu überprüfen und zu überwachen.

Berechtigungen von Ordnern und der Registry überwachen – AccessChk

Mit AccessChk von der Seite *http://technet.microsoft.com/de-de/sysinternals/bb664922* [Ms179-K20-01] können Sie in der Eingabeaufforderung eine ausführliche Liste anzeigen lassen, welche Rechte ein Benutzer auf Dateien, Dienste oder Teile der Registry hat. Das Tool hilft dabei, die Berechtigungen auch für verschachtelte Ordnerstrukturen auszulesen. Die Syntax lautet:

```
accesschk [-s][-r][-w][-n][-p][-k][-c|[-d]] <Benutzername> <Datei, Ordner, Registry-
Schlüssel oder Dienst>
```

Tabelle 20.1 Optionen von *AccessChk*

Option	Auswirkung
–c	Diese Option verwenden Sie, wenn es sich um einen Dienst handelt. Wenn Sie den Platzhalter * eingeben, zeigt das Tool die Rechte für alle Systemdienste an.
–d	Verarbeitet nur Ordner
–k	Diese Option liest Rechte in der Registry aus, zum Beispiel *HKLM\SOFTWARE*
–n	Zeigt nur Objekte an, für die kein Zugriff besteht
-p	Angeben eines Prozessnamens. Die Option unterstützt auch den Platzhalter *.
–r	Zeigt nur Leserechte an
-s	Rekursive Abfrage
–w	Zeigt nur Schreibrechte an

Wenn Sie sich die Rechte des Benutzers *joost* für einen Ordner *C:\Einkauf* anzeigen lassen wollen, verwenden Sie den Befehl *accesschk joost c:\einkauf*. Bei jeder Datei erhalten Sie die Information, ob Leserechte (R), Schreibrechte (W) oder beides (RW) bestehen.

Wollen Sie die Zugriffsberechtigungen für einen Benutzer für einen bestimmten Registry-Schlüssel abprüfen, können Sie zum Beispiel den Befehl *accesschk –kns contoso\joost hklm\software* verwenden. Geben Sie keinen Benutzernamen an, sondern nur einen Ordner, zeigt AccessChk alle Benutzerkonten und deren Rechte auf den Ordner an.

AccessChk ist hervorragend für Skripts geeignet und um festzustellen, welche effektiven Berechtigungen Anwender oder Gruppen haben. Effektive Berechtigungen sind die Berechtigungen, die ein Anwender tatsächlich auf einen Ordner oder eine Datei hat, auch auf Basis seiner Gruppenmitgliedschaften. Um die effektiven Berechtigungen anzuzeigen, öffnen Sie in den Eigenschaften des Ordners 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.

Sie können das Tool aber auch mit einer grafischen Oberfläche bedienen. Dazu verwenden Sie AccessEnum aus den Sysinternals-Tools (siehe den folgenden Abschnitt).

Mit dem Tool überprüfen Sie also die Berechtigungsstruktur im Netzwerk. Die Berechtigungen im Dateisystem sind in der Zugriffssteuerungsliste (Access Control List, ACL) gespeichert. Während der Anmeldung wird für den Benutzer ein sogenanntes Zugriffstoken generiert, das die Sicherheits-ID (SID) des Benutzerkontos enthält sowie die SIDs der Gruppen, in denen der Benutzer Mitglied ist.

Berechtigung mit grafischer Oberfläche auslesen – AccessEnum

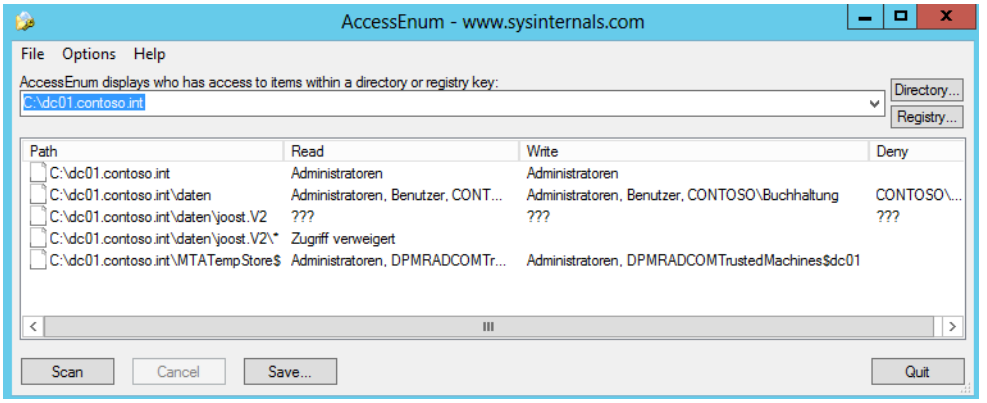
Mit AccessEnum aus den Sysinternals-Tools von der Seite *http://technet.microsoft.com/de-de/sysinternals/bb897332* [Ms179-K20-02] erhalten Sie eine grafische Oberfläche für AccessChk, mit der Sie Berechtigungen eines Benutzers oder einer ganzen Gruppe für Ordner oder Teile der Registry über-

prüfen können. Sie wählen in der Oberfläche einen Ordner aus und lassen sich anschließend die Berechtigungen anzeigen.

Das Tool zeigt auch an, wenn Sie Rechte für einen Ordner oder eine Datei verweigern lassen. Den Ordnernamen sehen Sie in der Spalte *Path*, in der Spalte *Read* sehen Sie die entsprechenden Rechte. Ein Anwender, der zum Beispiel Schreibrechte auf den Ordner *c:\users\joost* und alle darunterliegenden Ordner besitzt, aber über kein Schreibrecht auf den Ordner *C:\Users* verfügt, wird mit dem Eintrag *C:\Users\Joost* und dem Namen des Kontos in der Spalte *Write* dargestellt.

Über das Menü stehen Ihnen Einstellungsmöglichkeiten zur Verfügung. Ist die Option *Show Local System account* aktiviert, zeigt AccessEnum auch die Zugriffsrechte des lokalen Systemkontos. Deaktivieren Sie diese, ignoriert das Tool die Zugriffsrechte, die sich auf den lokalen Systemaccount (*NT-AutoritätSystem*) beziehen. Über die Option *File display options* lässt sich festlegen, dass das Tool nur dann die Rechte von untergeordneten Objekten anzeigt, wenn diese von dem entsprechenden übergeordneten Objekt abweicht. Mit einem Klick auf die Spaltenüberschriften können Sie die Einträge sortieren. Über die Schaltfläche *Registry* können Sie auch innerhalb der Registrierungsdatenbank nach Berechtigungen durchsuchen lassen.

Abbildg. 20.11 Anzeigen von Berechtigungen für Ordner



Vor allem bei der Kontrolle der Berechtigungen für verschiedene Freigaben hilft das Tool, einen schnellen Überblick zu erhalten, welche Benutzer und Gruppen Zugriffe auf die verschiedenen Ordner haben. Kann das Tool die Rechte nicht korrekt lesen oder die Sicherheits-ID (SID) nicht umsetzen, sehen Sie drei Fragezeichen.

Überwachung von Dateien und Ordnern

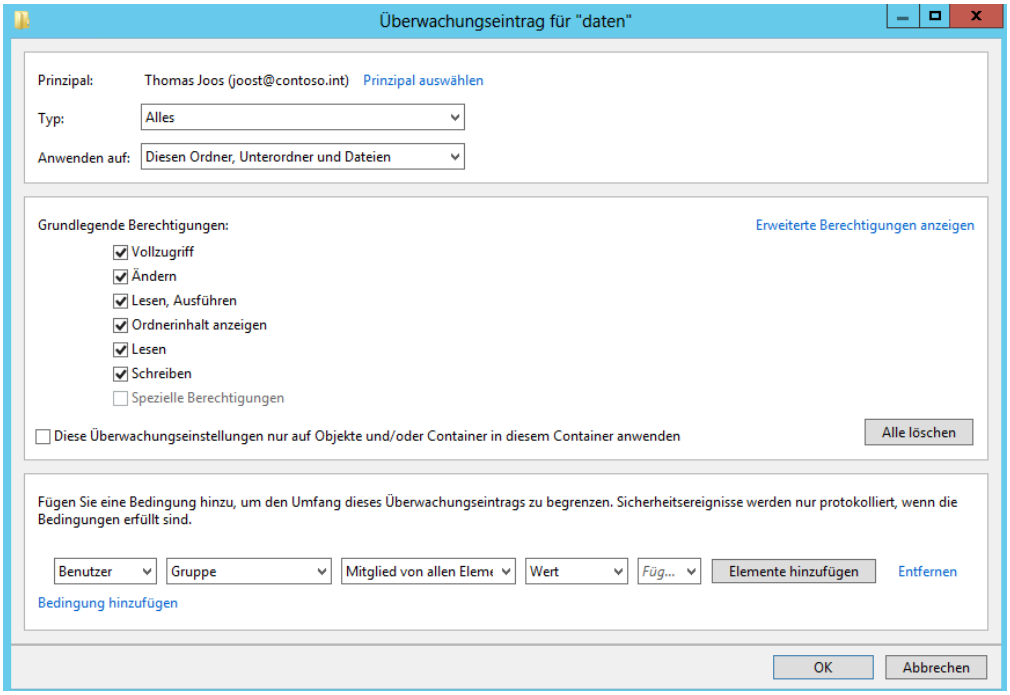
In den meisten Fällen kann eine Überwachung der Zugriffe auf Ordner nützlich sein. Bei der Überwachung hält Windows in Protokolldateien fest, wer bestimmte Operationen auf Dateien und Ordnern ausführt. Die Aktivierung der Überwachung von Ordnern aktivieren Sie am besten über lokale Richtlinien oder über Gruppenrichtlinien in Windows-Domänen.

Nachdem Sie die Überwachung für den Computer im Allgemeinen aktiviert haben, müssen Sie die eigentliche Überwachung für die entsprechenden zu überwachenden Dateien und Ordner 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 Windows protokollieren soll. Damit Sie die bei der Überwachung anfallenden Protokolldaten sinnvoll bearbeiten können, sollten Sie von diesen Einschränkungsmöglichkeiten Gebrauch machen und nur das Nötigste protokollieren. Über *Bearbeiten* legen Sie fest, welche Gruppen/Benutzer das System überwachen soll.

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 den Link *Prinzipal auswählen* 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 Ordner auswirken. Wählen Sie anschließend im Feld *Anwenden auf* aus, welche Zugriffe Windows protokollieren soll.

Abbildg. 20.12 Konfigurieren der Überwachung für einen Ordner



Die Anzeige der Protokollierung erfolgt in der Ereignisanzeige. Diese starten Sie am schnellsten durch Eintippen von *eventvwr* auf der Startseite. In der Ereignisanzeige finden Sie die protokollierten Zugriffsversuche im Protokoll *Sicherheit* unterhalb des Knotens *Windows-Protokolle*.

Die mit einem Schlüssel gekennzeichneten Einträge stehen für erfolgreiche Zugriffe, wogegen ein Schloss für fehlgeschlagene Zugriffe steht. Genauere Informationen zu einem Eintrag erhalten Sie angezeigt, indem Sie diesen öffnen. Ein einzelner Zugriff erzeugt eine ganze Reihe von Einträgen im Sicherheitsprotokoll.

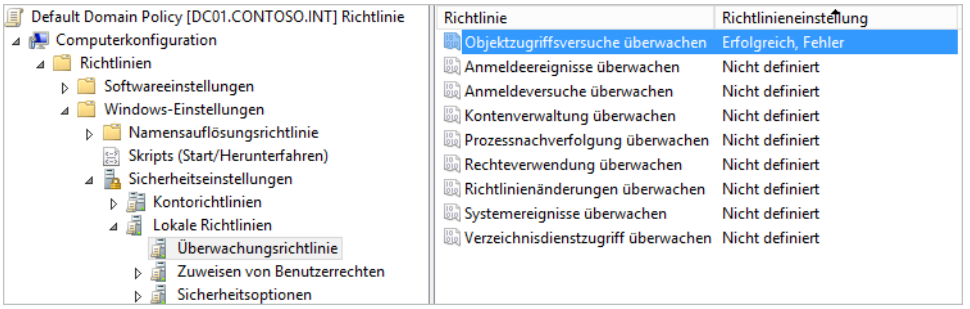
Auch wenn Sie Berechtigungen in einem Ordner vergeben, kommt es durchaus vor, dass Dateien verändert oder sogar gelöscht werden. Mit der Objektüberwachung können Sie genau feststellen, wann welche Anwender mit welchen Rechten auf Dateien zugegriffen haben:

Öffnen Sie die lokale Richtlinie für den Computer über den Befehl *gpedit.msc*. Sie können natürlich auch Gruppenrichtlinien verwenden und so mehrere Server anbinden.

Navigieren Sie zu *Computerkonfiguration/(Richtlinien)/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Überwachungsrichtlinie*.

In den Standardeinstellungen ist die Überwachung nicht aktiviert. Nach der Aktivierung der einzelnen Optionen müssen Sie noch auswählen, ob Windows erfolgreiche und/oder fehlgeschlagene Zugriffsversuche protokollieren soll.

Abbildg. 20.13 Aktivieren von Überwachungsrichtlinien



Die Überwachung der Zugriffe auf das Dateisystem aktivieren Sie über *Objektzugriffsversuche überwachen*. Neben Dateizugriffen überwachen Sie mit dieser Einstellung auch Zugriffe auf Drucker. Nach der Aktivierung müssen Sie noch auswählen, ob erfolgreiche und/oder fehlgeschlagene Zugriffsversuche protokolliert werden sollen.

Die Freigabe von Ordnern

Ordner stellen Sie auch in Windows Server 2012 R2 über Freigaben zur Verfügung. Sie können für Freigaben Benutzern das Recht geben, zu schreiben, zu lesen oder auch Daten zu verändern. Achten Sie darauf, dass Sie im Benutzer-Manager von Windows die Benutzerkonten erst anlegen müssen, für die Sie Rechte vergeben wollen, wenn der Computer nicht Mitglied einer Windows-Domäne ist.

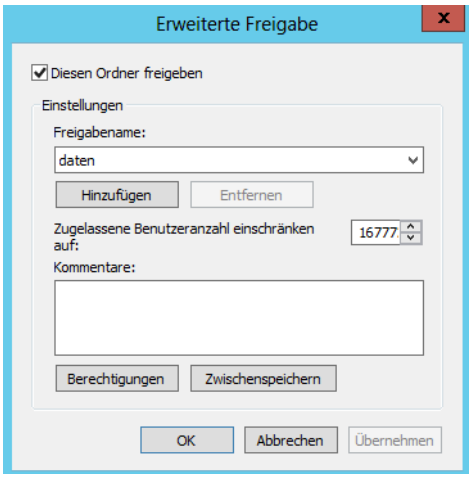
Die Anwender müssen sich dann bei der Verbindung mit der Freigabe mit dem Benutzernamen und dem konfigurierten Kennwort authentifizieren. Wichtig in diesem Zusammenhang sind die vorangegangenen Abschnitte sowie die Kapitel 5 und 18.

Freigaben erstellen

Alle Unterordner, die ein freigegebener Ordner enthält, sind ebenfalls im Netzwerk verfügbar. Klicken Sie den Ordner mit der rechten Maustaste an und wählen Sie im Kontextmenü die Option *Eigenschaften* und dann auf der Registerkarte *Freigabe* die Option *Erweiterte Freigabe* aus.

Standardmäßig darf die Gruppe *Jeder* lesend auf die Freigabe zugreifen. Wenn Sie möchten, dass alle Anwender im Netzwerk schreiben dürfen, müssen Sie das Schreibrecht vergeben. Das Recht *Ändern* berechtigt zum Lesen, Schreiben und Löschen.

Abbildg. 20.14 Konfiguration einer Dateifreigabe



Über die Schaltfläche *Berechtigungen* legen Sie fest, welche Anwender über die Freigabe auf den Rechner zugreifen dürfen. Mit *OK* schließen Sie die Freigabe ab. Um Benutzerkonten zusätzlich zu den Berechtigungen hinzuzufügen, klicken Sie auf *Berechtigungen/Hinzufügen* und dann auf *Erweitert*. Im folgenden Fenster können Sie sich alle Benutzerkonten Ihres Computers oder der Domäne anzeigen lassen und den Benutzer auswählen, für den Sie Berechtigungen vergeben wollen.

Sie können auf der Registerkarte *Sicherheit* in den Eigenschaften des Ordners zusätzlich noch Berechtigungen auf Basis des Dateisystems vergeben. Klicken Sie dazu auf Bearbeiten. Die einzelnen Möglichkeiten, die Sie hier haben, lesen Sie in den vorangegangenen Abschnitten in diesem Kapitel und in Kapitel 18.

TIPP Freigaben lassen sich in der Eingabeaufforderung durch den Befehl *net share <Name der Freigabe> <Pfad des Ordners, der freigegeben werden soll>* ebenfalls freigeben.

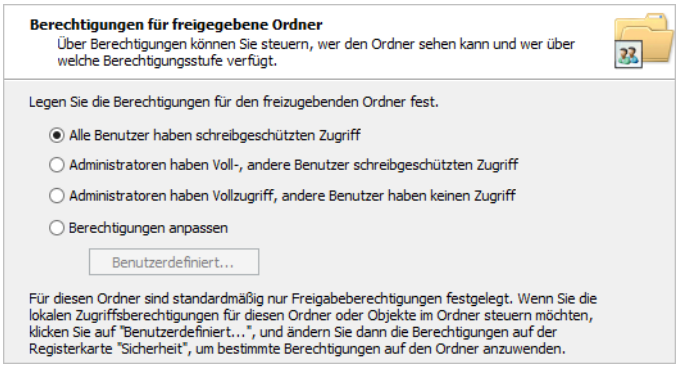
Der Assistent zum Erstellen von Freigaben

Durch Eintippen von *shrpubw* auf der Startseite rufen Sie den Assistenten zur Erstellung von Freigaben auf. Nach einem Klick auf *Weiter* können Sie im nächsten Fenster des Assistenten 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. Wir kommen dazu noch in einem weiteren Abschnitt. Ist eine Freigabe offline verfügbar, kann diese zum Beispiel mithilfe von Offlinedateien synchronisiert werden. Das ist für mobile Computer sinnvoll.

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 abgeschlossen.

Abbildg. 20.15 Erstellen von Freigaben



Anzeigen über das Netzwerk geöffneter Dateien – PsFile

Öffnen Anwender eine Datei auf einem Computer über das Netzwerk, lässt sich das ebenfalls anzeigen. Dazu verwenden Sie das Tool PsFile von *http://technet.microsoft.com/de-de/sysinternals/bb897552* [Ms179-K20-03]. Auch mit Openfiles können Sie die Dateien anzeigen. Mehr dazu lesen Sie in den vorangegangenen Abschnitten. Sie können zwar auch mit dem Befehl *net file* eine Liste der über das Netzwerk geöffneten Dateien anzeigen. Allerdings schneidet der Befehl lange Pfadnamen ab. Außerdem können Sie mit *net file* keine Daten auf Remotecomputern abfragen, sondern nur für das lokale System.

Geben Sie nur den Befehl *psfile* an, zeigt das Tool geöffnete Dateien an, inklusive des genauen Dateipfads. Wollen Sie die geöffneten Dateien auf einem Computer im Netzwerk abfragen, können Sie dazu ebenfalls PsFile verwenden. Die Syntax dazu lautet:

```
psfile [\\<Computer> [-u <Benutzername> [-p <Kennwort>]]] [[Id | <Pfad>] [-c]]
```

- **–u** Mit dieser Option können Sie den Benutzernamen zum Anmelden am Remotecomputer angeben
- **–p** Mit dieser Option geben Sie das Kennwort für den Benutzernamen mit. Wenn Sie kein Kennwort angeben, müssen Sie dieses bei der Ausführung des Befehls angeben.
- **Id** Hier können Sie die ID der Datei angeben, von der Sie ausführlichere Informationen anzeigen lassen wollen oder die geschlossen werden soll
- **Pfad** Pfad der Dateien, die angezeigt werden sollen
- **–c** Schließt die Dateien, deren ID Sie angegeben haben

Abbildg. 20.16 Anzeigen geöffneter Dateien mit Openfiles und PsFile

```
C:\temp>openfiles
FEHLER: Daten können nicht abgefragt werden.
Das System konnte die eingegebene Umgebungsoption nicht finden.


Über das Netzwerk über lokalen Freigaben geöffnete Dateien:
-----------------------------------------------

Kennung  Zugriff durch         Typ         Open File (Pfad\ausführbare Datei)
======== ==================== ========== ==================================
343      FILE01$              Windows     C:\..\Adm
369      joost                Windows     C:\daten\
372      joost                Windows     C:\..\einkauf-geheime-preise.docx
385      joost                Windows     C:\..\EINKAUF-GEHEIME-PREISE.DOCX
386      joost                Windows     C:\..\EINKAUF-GEHEIME-PREISE.DOCX

C:\temp>psfile

psfile v1.02 - psfile
Copyright © 2001 Mark Russinovich
Sysinternals

Files opened remotely on DC01:

[343] C:\Windows\SYSVOL\sysvol\contoso.int\Policies\{A40E2811-0AD9-48C0-BCE1-A64
F4217409B}\Adm
    User:   FILE01$
    Locks:  0
    Access: Read
[369] C:\daten\
    User:   joost
    Locks:  0
    Access: Read
[372] C:\daten\einkauf-geheime-preise.docx
    User:   joost
    Locks:  0
    Access: Read
[385] C:\daten\EINKAUF-GEHEIME-PREISE.DOCX
    User:   joost
    Locks:  0
    Access: Read Write
[386] C:\daten\EINKAUF-GEHEIME-PREISE.DOCX
    User:   joost
    Locks:  0
    Access: Read
```

Versteckte Freigaben

Auch wenn es möglich ist, die Zugriffsberechtigungen auf eine Freigabe so einzustellen, dass einem unbefugten Anwender der Zugriff auf die Dateien und Ordner der Freigabe verwehrt wird, 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. Sie können sich mit dieser Freigabe jetzt nur noch durch direkte Eingabe des Freigabenamens (inklusive Dollarzeichen) verbinden.

HINWEIS Administratoren können auf die komplette Festplatte über das Netzwerk zugreifen, indem sie die Freigabe *C$* bzw. *<Laufwerksbuchstabe>$* verwenden. Diese Freigaben werden Adminfreigaben genannt. Nur Administratoren haben Zugriff darauf.

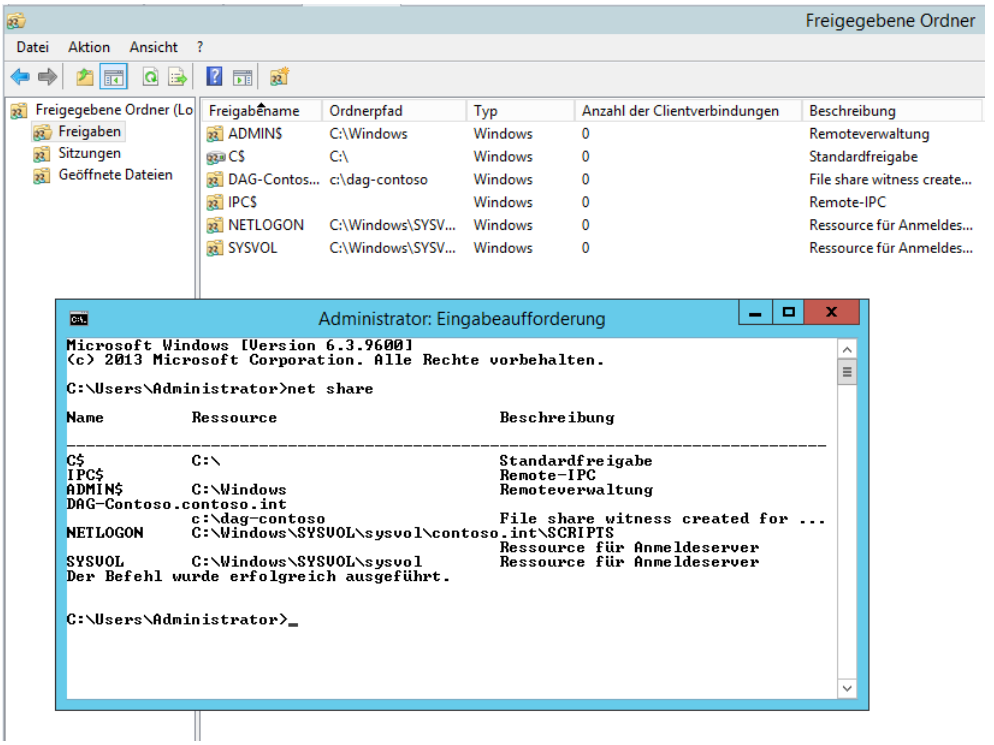
Sie sollten auf der Ebene der Freigaben die gleichen Gruppen berechtigen wie auf NTFS-Ebene. Die Festlegung auf NTFS-Ebene erfolgt über die Eigenschaften eines Ordners auf der Registerkarte *Sicherheit*.

Anzeigen aller Freigaben

Sie können in der Computerverwaltung alle Freigaben Ihres Servers verwalten. Sie finden die Verwaltung der Freigaben in der Computerverwaltung. Alternativ können Sie die Computerverwaltung über *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.

In der Eingabeaufforderung sehen Sie Freigaben, wenn Sie den Befehl *net share* eingeben. Eine weitere Möglichkeit ist der Aufruf von *fsmgmt.msc*. Mit diesem Tool können Sie sich auch in der grafischen Oberfläche die geöffneten Dateien anzeigen lassen.

Abbildg. 20.17 Anzeigen von Freigaben eines Servers in der Eingabeaufforderung und der grafischen Oberfläche



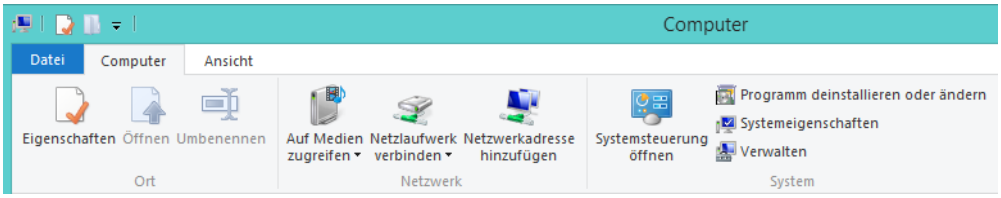
Im Bereich *Freigegebene Ordner* stehen Ihnen an dieser Stelle drei verschiedene Einträge zur Verfügung, über die Sie Freigaben verwalten und überprüfen können:

- **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.

Auf Freigaben über das Netzwerk zugreifen

Wenn Sie eine Freigabe eines anderen Computers im Netzwerk als Laufwerk verbinden wollen, öffnen Sie am besten den Explorer und klicken dann im Navigationsbereich auf *Computer*. Wählen Sie im Menüband den Eintrag *Netzlaufwerk verbinden* aus.

Abbildg. 20.18 Verbinden eines Netzlaufwerks im Explorer



Geben Sie als Nächstes den Freigabenamen im Feld Ordner ein. Die Syntax dazu lautet \\<*Computername oder IP-Adresse*>\<*Name der Freigabe*>. Alternativ klicken Sie auf *Durchsuchen* und dann doppelt auf den Computer, auf dem sich die Freigabe befindet, mit der Sie sich verbinden wollen. Klicken Sie auf *Fertig stellen*, öffnet sich eventuell ein Anmeldefenster, in dem Sie die Authentifizierungsdaten eines Benutzers auf dem Remotecomputer eingeben müssen.

Eine weitere Möglichkeit, Netzlaufwerke zu verbinden, steht Ihnen über die Eingabeaufforderung mit dem Befehl *net use* zur Verfügung. Eine Eingabeaufforderung öffnen Sie entweder durch Eintippen von *cmd* auf der Startseite. Rechtsklick in die linke untere Bildschirmecke (oder ⊞+X) und den Befehl *Eingabeaufforderung* oder *Eingabeaufforderung (Administrator)* anklicken ist eine weitere Möglichkeit.

- **net use** Zeigt alle derzeit verbundenen Netzlaufwerk an
- **net use <Laufwerksbuchstabe>: /del** Trennt das angegebene Netzlaufwerk. Verwenden Sie *, trennt Windows alle Netzlaufwerke.
- **net use <Laufwerksbuchstabe>: \\<Computer mit Freigabe>\<Freigabename>** Durch Eingabe dieses Pfads verbinden Sie das Netzlaufwerk. Verwenden Sie *, aktiviert Windows den nächsten freien Buchstaben.

Sie können den Befehl auch mit der folgenden Syntax aufrufen:

```
net use <Laufwerksbuchstabe>: \\<Computer mit Freigabe>\<Freigabename> <Benutzername>
<Kennwort>
```

Mit diesem Befehl können Sie ein Laufwerk mithilfe eines anderen Benutzers als dem derzeitig angemeldeten verbinden.

Verbundene Netzlaufwerke zeigt Windows im Explorer an. Sie können verbundene Laufwerke per Rechtsklick wieder trennen.

Offlinedateien für den mobilen Einsatz unter Windows 8/8.1

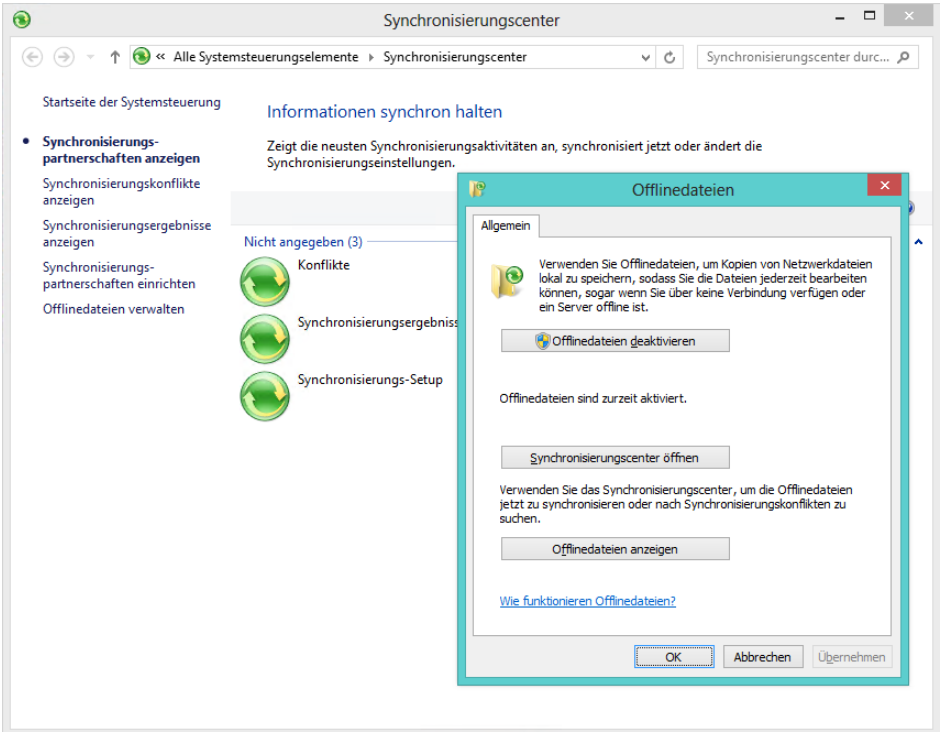
Mit den Offlinedateien haben Sie die Möglichkeit, Dateien aus dem Netzwerk, zum Beispiel von einem Dateiserver, auch dann verfügbar zu machen, wenn Sie mit einem Notebook unterwegs sind. Dazu wird auf dem Notebook eine Kopie der entsprechenden Datei erstellt, sodass diese auch ohne Netzwerkverbindung zur Verfügung steht. Lesen Sie sich zu dem Thema auch den Abschnitt zu den neuen Arbeitsordner in Windows Server 2012 R2 in Kapitel 5 durch.

Sie können die entsprechenden Dateien auch dann 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.

So funktionieren Offlinedateien

Die Verwaltung der Offlinedateien unter Windows 8/8.1 findet über das Synchronisierungscenter statt, das Sie durch Eingabe von *mobsync* auf der Startseite aufrufen können. Über den Link *Offlinedateien verwalten* im Synchronisierungscenter öffnet sich ein neues Fenster, über das Sie entsprechende Einstellungen vornehmen können. In Zusammenarbeit mit Windows 8 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.

Abbildg. 20.19 Offlinedateien unter Windows 8/8.1 verwalten



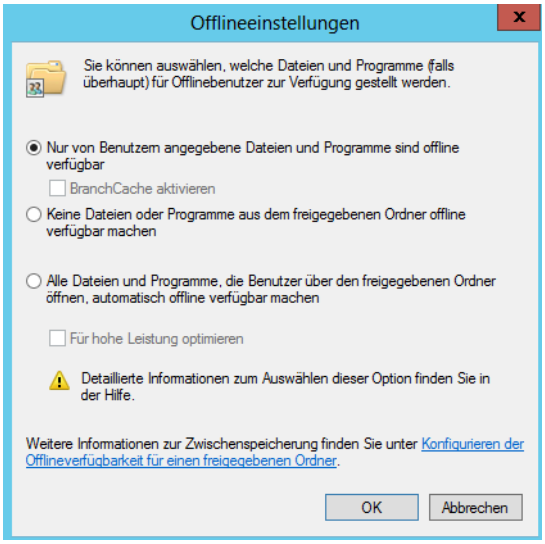
In den Eigenschaften jeder Offlinedatei können spezielle Einstellungen vorgenommen werden. Nachdem das System für den Offlinebetrieb aktiviert ist, können Sie Ordner und Dateien von Servern für den Offlinebetrieb verfügbar machen. Hier gibt es Steuerungsmöglichkeiten sowohl vom Client als auch vom Server aus.

Vom Client aus verwenden Sie den Befehl *Immer offline verfügbar*, der sich im Kontextmenü findet, wenn Sie eine Freigabe, eine Datei oder einen Ordner auf einem Server markiert haben, die oder der für den Offlinezugriff freigegeben ist.

Sie können auf diese Weise einzelne Dateien, ganze Ordner 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 Speicherplatzbedarf mit der Anzahl der Offlinedateien zunimmt. Sie sollten daher möglichst nur Dateien offline verwenden, die Sie auch tatsächlich benötigen, nicht gleich alle auf einmal. Bei der ersten Auswahl dieser Option bereitet Windows den Computer vor und nimmt die Dateien und Ordner in den Offlinemodus mit auf.

Vom Server mit der entsprechenden Freigabe aus kann die Nutzung von Offlinedateien über die Freigabe gesteuert werden. Beim Erstellen von Freigaben findet sich die Option *Zwischenspeichern* in den erweiterten Einstellungen der Freigabe. Wenn Sie diese auswählen, können Sie steuern, ob das Zwischenspeichern von Dateien in dem freigegebenen Ordner zugelassen ist. Standardmäßig wird das manuelle Zwischenspeichern von Dateien zugelassen. Das heißt, Freigaben lassen es zu, dass Anwender die Offlinedateien von Clients aus konfigurieren.

Abbildg. 20.20 Konfigurieren von Offlinedateien einer Freigabe in Windows Server 2012 R2



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

- Mit der Option *Nur von Benutzern angegebene Dateien und Programme sind offline verfügbar* können die Benutzer auswählen, indem Sie die entsprechende Option im Kontextmenü der Freigabe oder des Ordners innerhalb der Freigabe verwenden

- Die Option *Alle Dateien und Programme, die Benutzer über den freigegebenen Ordner öffnen, automatisch offline verfügbar machen* bewirkt, dass alle Dokumente und ausführbaren Dateien in dieser Freigabe lokal zwischengespeichert werden. In diesem Fall muss sich der Benutzer nicht mehr darum kümmern, die Dokumente offline verfügbar zu machen.
- Über das Kontrollkästchen *Für hohe Leistung optimieren* lässt sich festgelegen, 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 sein, um zu verhindern, dass Windows veränderte Programme zurückspeichert.

Sie können die Einstellungen der Synchronisierungseigenschaften von Offlinedateien im Synchronisierungscenter von Windows 8 anpassen. Das Synchronisierungscenter finden Sie über die Startseite oder die Systemsteuerung.

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 ebenfalls 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.

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, das die Datei als Offlinedatei kennzeichnet.

Den Status der Verbindung sehen Sie unten im Explorer-Fenster. 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. Außerdem zeigt Windows für offline verfügbare Ordner den grünen Kreis an und für nicht verfügbare Ordner ein X, welches kennzeichnet, dass Sie keinen Zugriff auf diese Dateien haben.

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

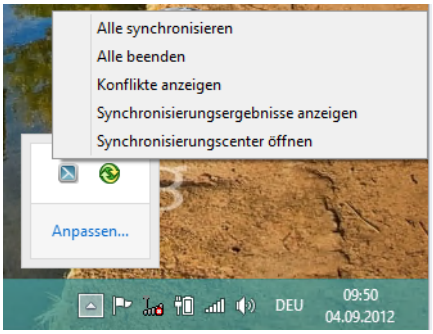
1. Öffnen Sie wie beschrieben die Verwaltung der Offlinedateien in Windows über das Synchronisierungscenter und klicken Sie auf *Offlinedateien verwalten*.
2. Klicken Sie im Dialogfeld *Offlinedateien* auf die Schaltfläche *Offlinedateien anzeigen*.

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 Bei-

spiel *Alle synchronisieren*. Das Symbol befindet sich eventuell bei dem Pfeil links, über den Sie die weniger aktiven Symbole erreichen.

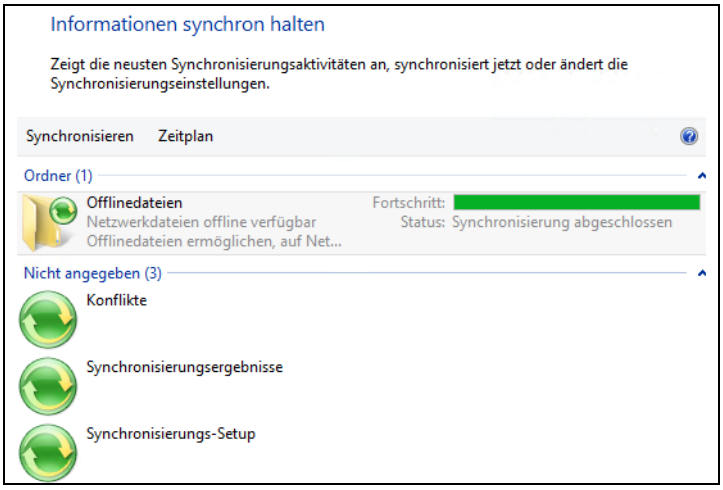
Abbildg. 20.21 Synchronisieren von Offlinedateien



Neben dieser Möglichkeit können Sie die Synchronisierung auch auf andere Wege erreichen:

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

Abbildg. 20.22 Synchronisieren von Offlinedateien im Synchronisierungscenter



Wenn Sie nur den Inhalt eines bestimmten Ordners synchronisieren möchten, öffnen Sie den Ordner im Explorer und klicken mit der rechten Maustaste auf den Ordner oder die Datei. Wählen Sie anschließend *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. Sie erreichen den Zeitplan, die Konfliktanzeige und die Eigenschaften über das Kontextmenü.

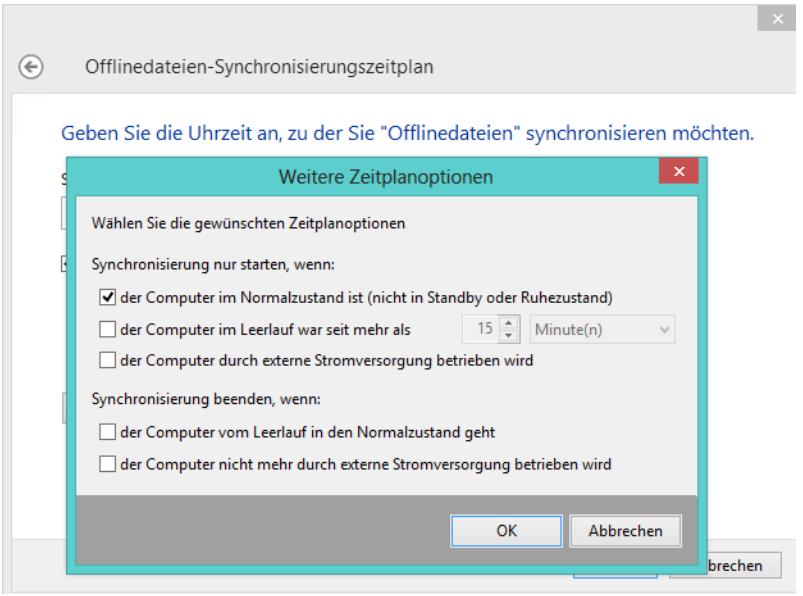
Zusätzlich können Sie in den Eigenschaften eines offline verfügbaren Ordners auf der Registerkarte *Offlinedateien* den aktuellen Stand des Ordners einsehen. Hier lässt sich auch die Offlineverfügbarkeit des Ordners steuern und die Synchronisierung aktivieren.

Wenn Sie im Synchronisierungscenter die Synchronisierungspartnerschaft der Offlinedateien öffnen, können Sie über die Schaltfläche *Zeitplan* genau einstellen, wann die Offlinedateien synchronisiert werden sollen. Auf der ersten Seite des Assistenten legen Sie zunächst fest, für welche übergeordnete Netzlaufwerke Sie den Zeitplan für die Synchronisierung steuern wollen.

Auf der nächsten Seite bestimmen Sie, ob die Synchronisierung zeitabhängig oder nach einer bestimmten Aktion, zum Beispiel der Anmeldung am PC, erfolgen soll. Wählen Sie zur Synchronisierung die Option *Nach Zeitplan* aus, können Sie auf der nächsten Seite den Zeitpunkt der Synchronisierung definieren. Zusätzlich können Sie hier einstellen, wie oft die Synchronisierung stattfinden und in welchen Abständen sie wiederholt werden soll.

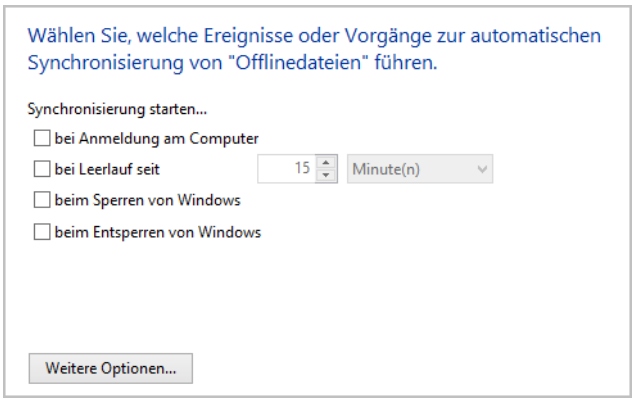
Über die Schaltfläche *Weitere Optionen* lässt sich detailliert einstellen, wann die Synchronisierung starten soll und wann nicht. Hier können vor allem für Notebooks Einstellungen vorgenommen werden, die eine Synchronisierung verhindern, um die Akkulaufzeit zu erhöhen.

Abbildg. 20.23 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 *Beim Eintreten eines Ereignisses*. Im Anschluss stellt Ihnen Windows 8 die Ereignisse zur Verfügung, die eine Synchronisierung auslösen. Über die Schaltfläche *Weitere Optionen* erreichen Sie die gleichen Detaileinstellungen wie bei der Synchronisierung nach Zeitplan.

Abbildg. 20.24 Konfigurieren der Synchronisierung nach einem Ereignis



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

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

Dateien und Freigaben auf Windows Server 2012 R2 migrieren

Eine wichtige Aufgabe bei der Migration ist die Übernahme der Dateien und der Freigaben auf den neuen Server mit Windows Server 2012 R2. Im folgenden Abschnitt zeigen wir Ihnen verschiedene Wege, wie Sie diese Daten übernehmen können.

Daten mit Robocopy übernehmen

Microsoft empfiehlt die Übernahme der Daten mit Robocopy, welches zu den Bordmitteln von Windows Server 2012 R2 gehört. Verwenden Sie zum Beispiel folgenden Befehl:

```
robocopy \\<Quellserver>\Users \\<Zielserver>\UserShares /E /COPY:DATSOU /R:10
/LOG:C:\migration.txt
```

Robocopy ist ein Tool für die Eingabeaufforderung, welches ähnlich wie Xcopy funktioniert, aber deutlich mehr Möglichkeiten bietet. Das Tool gehört zu den Bordmitteln von Windows 7 und Windows Server 2008 R2 und damit auch zu Windows 8 und Windows Server 2012 R2. Mit Robocopy sind sehr komplexe Dateireplizierungsaufgaben möglich.

Das Tool spiegelt Ordner deutlich schneller als die meisten Synchronisierungstools mit grafischen Oberflächen. Zwar ist die Erstellung eines Skripts zunächst etwas aufwendig, dafür läuft der Kopiervorgang wesentlich schneller ab als bei vielen Tools. Zum Beispiel können Sie mit Robocopy vollständig gespiegelte Duplikate von zwei Dateistrukturen einschließlich aller Unterordner und Dateien anlegen.

Mit Robocopy lassen sich sehr umfangreiche Datensicherungsskripts erstellen. Robocopy unterstützt außerdem alle verbundenen Dateiinformationen einschließlich der Datums- und Zeitstempel, Zugriffssteuerungslisten (Access Control Lists, ACL) und vieles mehr. Vor allem für kleinere Unternehmen kann die Datensicherung oder die Migration per Skript über Robocopy sehr effizient sein. 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. Das Tool kann nicht nur Windows-Berechtigungen kopieren, sondern auch Dateien verschieben und löschen.

Das Werkzeug verfügt über eine Vielzahl von Optionen und kann zum Beispiel per Skript einen Ordner mit einem anderen 1:1 abgleichen, auch mehrmals täglich. Es ist auch möglich, nur veränderte Dateien zu kopieren und gelöschte Dateien des einen Ordners auf dem anderen zu löschen. Mit diesen Möglichkeiten können Unternehmen schnell und leicht Ordner spiegeln und so einem Datenverlust vorbeugen, unabhängig von einem Datensicherungskonzept.

Robocopy kann Ordner mit Unterordnern kopieren und dabei einzelne Dateien ausschließen. Der Zeitstempel von Dateien lässt sich auslesen und so lassen sich auf Basis des Erstellungs- oder Änderungsdatums Dateien kopieren oder auch löschen. Wenn Sie häufig einen Ordner über das Netzwerk spiegeln wollen, lässt sich mit dem Tool deutlich Zeit sparen, da Sie zum Beispiel nur veränderte Dateien kopieren müssen und bereits vorhandene einfach übergehen können.

Der Aufruf von Robocopy sieht folgendermaßen aus:

```
robocopy <Quelle> <Ziel>< Datei(en)>/< Option>
```

Platzhalter sind erlaubt. Wenn Sie keine Dateien oder Platzhalter eingeben, verwendet Robocopy standardmäßig (*.*), kopiert also alle Dateien. Als Quelle und Ziel kann ein Ordner, ein Laufwerk oder auch ein UNC-Pfad angegeben sein (*\\<Server>\<Freigabe>*). Die Optionen werden hinter dem Befehl angehängt. Sie können beliebig viele Optionen miteinander kombinieren.

Tabelle 20.2 Mögliche Optionen von Robocopy

Option	Funktion
/S	Kopiert Unterordner (außer leere Ordner)
/E	Kopiert Unterordner (auch leere Ordner)
/LEV:n	Kopiert nur bis zu einer Verzeichnistiefe von *n*. Die restlichen Ordner 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 Backupmodus kopiert. Es werden also alle Dateien kopiert, auch diejenigen, mit denen die Option */Z* Probleme hat.

Tabelle 20.2 Mögliche Optionen von Robocopy *(Fortsetzung)*

Option	Funktion
/ZB	Es wird zunächst die Option */Z* probiert. Schlägt das bei einer Datei fehl, verwendet Robocopy die Option */B*.
/COPY:copyflags	Kopiert nur die Dateiattribute, die definiert werden. Dazu muss das Dateisystem auf dem Quell- und dem Zielordner 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 Ordner
/PURGE	Löscht Dateien und Ordner im Zielverzeichnis, die auf dem Quellordner nicht mehr vorhanden sind
/MIR	Spiegelt einen kompletten Ordner. 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
/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 Ordner, falls diese in der Quelle ebenfalls vorhanden sind
/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 kompatibel zu NTFS sind, aber eigentlich nur das FAT-Dateisystem beherrschen (wird eher selten benötigt)
/MON:n	Zählt die Änderungen von Dateien im Quellordner mit und startet nach *n* Änderungen den Kopiervorgang nach dem Zeitraum, der mit */MOT* (s.u.) definiert wird. Verwenden Sie diese Option, um Robocopy im Hintergrund laufen zu lassen.
/MOT:n	Führt den Kopiervorgang nach *n* Minuten erneut aus. In Kombination mit */MON* möglich.
/RH:hhmm-hhmm	Definiert, innerhalb welcher Zeit kopiert werden darf. Die Werte sind im 24 Stunden-Format angegeben und müssen im Format 0000 bis 2359 eingegeben werden.

Tabelle 20.2 Mögliche Optionen von Robocopy *(Fortsetzung)*

Option	Funktion
/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 über die Eigenschaften einer Datei durchgeführt werden)
/M	Wie */A*, allerdings wird das Archivattribut in der Quelldatei zurückgesetzt
/XF file [file]	Kopiert diese Dateien nicht. Sie können mehrere hintereinander schreiben. Diese Option setzen Sie am Ende des Befehls. Sie können auch mit * als Platzhalter arbeiten.
/XD dir [dir]	Kopiert diese Ordner nicht. Auf diese Weise können Sie Unterordner beim Spiegeln überspringen lassen, indem Sie deren Pfad im Befehl angeben
/XC	Schließt Dateien aus, die im Quellordner als geändert markiert sind
/XN	Kopiert keine Dateien, die im Quellordner als neuer deklariert sind
/XO	Wie */XN*, nur werden Dateien nicht kopiert, die im Quellordner als älter definiert sind
/MAX:n	Kopiert keine Dateien, die größer als *n* Bytes sind
/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 s.o.)
/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. Die Option ist sinnvoll, um einen Kopiervorgang zu simulieren. Sie setzen dazu die Option einfach ans Ende des Befehls.
/TS	Zeigt den Zeitstempel der Quelldateien in der Protokolldatei an

Tabelle 20.2 Mögliche Optionen von Robocopy *(Fortsetzung)*

Option	Funktion
/FP	Zeigt den vollen Pfadnamen in der Protokolldatei
/NS	Zeigt nicht die Datei- und Ordnergröße in der Protokolldatei an
/NFL	Protokolliert 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 Protokoll in der definierten Datei
/LOG+:file	Hängt das Protokoll an eine bereits bestehende Protokolldatei an
/TEE	Zeigt die Vorgänger auch in der Eingabeaufforderung an, nicht nur im Protokoll
/JOB:job	Liest die Parameter von einer Jobdatei aus
/SAVE:job	Speichert die Parameter in einer Jobdatei
/QUIT	Führt nichts aus. Zeigt in Verbindung mit dem *job*-Schalter den Inhalt der Jobdatei an.

Wenn der Kopiervorgang einer Datei aus irgendwelchen Gründen fehlschlägt, die Datei in Benutzung ist oder Windows den Zugriff verweigert hat, 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 verwendet der Kopiervorgang die Optionen */W* und */R*. Sind im Befehlsaufruf die Optionen */R* und */W* nicht gesetzt, verwendet das Tool die Standardwerte.

Wenn Sie Datei- oder Ordnernamen kopieren, die ein Leerzeichen enthalten, geben Sie den Pfad in Anführungszeichen an, zum Beispiel *Robocopy "\fs01\einkauf\lieferanten 2011" \fs01\archiv\einkauf*. Alle Optionen verwendet das Tool von links nach rechts. Nach unserer Erfahrung verwenden die meisten Administratoren die Option */MIR*, weil so schnell und einfach eine Spiegelung eines Ordners angelegt wird. Ein Beispielskript, auch auf Basis der Optionen von Tabelle 20.2, könnte folgendermaßen aussehen:

```
echo on
del C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Documents" "x:\backup\dokumente" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Pictures" "x:\backup\Pictures" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Documents" "z:\backup\dokumente" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Pictures" "z:\backup\Pictures" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Documents" "u:\backup\dokumente" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Pictures" "u:\backup\Pictures" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
shutdown /s /t 30
```

Um die Daten in einer Freigabe auf einen anderen Rechner zu spiegeln, schreiben Sie am besten ein Skript mit dem Befehl *robocopy <Quellordner> <Sicherungslaufwerk>:\<Sicherungsordner> /mir*. Mit dem Befehl *robocopy c:\users\thomas\documents y:\backup /mir* kopiert Windows die Ordner und Dateien aus dem *Dokumente*-Ordner auf das Laufwerk *Y:* in den Ordner *backup*. Die Option */mir* kopiert nur geänderte Dateien und löscht Dateien im Zielordner, die im Quellordner nicht mehr vorhanden sind. 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 Quellordner eine Datei, löscht der Kopiervorgang diese auch im Backupordner.

So erhalten Sie immer eine 1:1-Kopie Ihrer wichtigsten Daten. Sie können ohne Weiteres auch mehrere Ordner sichern. Verwenden Sie in diesem Fall einfach mehrmals den Befehl nacheinander in einem Skript.

Nur Freigaben und deren Rechte übernehmen

Wollen Sie keine Daten kopieren, sondern nur die bestehenden Freigaben und Rechte vom Quell- auf den Zielserver übertragen, benötigen Sie die Registry:

1. Öffnen Sie auf dem Server die Registry durch Eingabe von *regedit*.
2. Navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Shares*.
3. Exportieren Sie diesen Schlüssel über das Kontextmenü.
4. Wollen Sie nicht alle Freigaben übernehmen, öffnen Sie die exportierte Datei und löschen Sie die Einträge der Freigaben, die Sie nicht übernehmen wollen.
5. Kopieren Sie die Datei auf den Zielserver und klicken Sie doppelt auf die Datei, um sie auf den Zielserver zu importieren. Achten Sie aber darauf, dass dieser Import die Einträge der vorhandenen Freigaben auf dem Zielserver überschreibt.
6. Starten Sie anschließend den Server neu.
7. Überprüfen Sie auf dem Server, ob die Freigaben vorhanden sind.

Dateiserver-Migrationstoolkit

Wollen Unternehmen Dateiserver auf neuere Hardware umstellen, ist das Problem dabei, meist die ganzen Freigaben neu zu erstellen, die Daten zu übernehmen und die Rechte neu einzutragen. Zwar gibt es viele Werkzeuge, um Daten zu synchronisieren, allerdings können die wenigsten Tools auch NTFS-Rechte übernehmen und Freigaben erzeugen. Hier hilft Microsoft mit dem kostenlosen Dateiserver-Migrationstoolkit. Das Tool hilft dabei, Migrationen für die Benutzer vollkommen transparent durchzuführen, auch auf ganze DFS-Stämme (Distributed File System, verteiltes Dateisystem) zu Windows Server 2008 R2, Windows Server 2012 oder Windows Server 2012 R2.

Überblick zur Migration zu Windows Server 2012 R2

Das Tool übernimmt komplette Ordner, legt Ordner und Freigaben an, kopiert Dateien und setzt die NTFS-Rechte korrekt um. Auch Berichte erstellt das Tool. Die ganze Übernahme findet mit einem einfach zu bedienenden Assistenten statt. Außerdem kann das Tool sehr schnell Daten kopieren, sodass auch mehrere hundert Gigabyte kein Problem darstellen. Selbst das Kopieren nur geän-

derter Daten ist möglich, sodass Sie zunächst eine Datensicherung zurücksichern können und dann erst die Daten mit dem Tool übernehmen. Das Dateiserver-Migrationstoolkit führt alle Aufgaben in einem Aufwasch durch und Sie können die Konfiguration sehr detailliert über einen Assistenten oder durch Anpassen einer XML-Datei steuern.

Ein weiterer Vorteil des Dateiserver-Migrationstoolkits ist die Möglichkeit, auch mehrere Dateiserver auf einen neuen Server umzuziehen, auch zu DFS, und zwar unabhängig vom Betriebssystem. Da das Tool auch Windows Server 2008 R2 und damit Windows Server 2012 R2 unterstützt, lässt sich so die Migration zum neuen Betriebssystem deutlich vereinfachen. Sie können dieses Tool bei Microsoft auf der Seite *http://www.microsoft.com/de-de/download/details.aspx?id=10268* [Ms179-K20-04] herunterladen. Auf der Seite *http://www.microsoft.com/en-us/download/details.aspx?id=17959* [Ms179-K20-05] erhalten Sie weitere Informationen sowie ein Whitepaper, welches bei der Migration unterstützt. Auf der Seite *http://technet.microsoft.com/de-de/edge/technet-video-fileserver-konsolidierung-mit-dem-file-server-migration-toolkit* [Ms179-K20-06] finden Sie ein deutschsprachiges Video, das die Bedienung des Toolkits ausführlicher erläutert.

Das Dateiserver-Migrationstoolkit unterstützt alle Betriebssysteme ab Windows NT 4.0 aufwärts, auch die neuesten Varianten Windows 7 und Windows Server 2008 R2 sowie Windows Server 2012 R2. Quellserver und Zielserver müssen nicht mit dem gleichen Betriebssystem installiert sein, was bei der Migration zu Windows Server 2012 R2 sehr hilfreich ist. Und das Toolkit kann auch Daten von mehreren Dateiservern in einem Durchlauf auf einen neuen Server übernehmen, mit allen gesetzten Rechten. Neben einer 32-Bit-Version steht das Dateiserver-Migrationstoolkit auch als 64-Bit-Software zur Verfügung.

Vor allem bei der Migration zu Windows Server 2012 R2 ergibt dies Sinn, da der Server nur als 64-Bit-Version zur Verfügung steht. Sie können das Toolkit zwar auch als 32-Bit-Version auf einem 64-Bit-Betriebssystem installieren, allerdings ist vor allem bei großen Dateimengen der Einsatz der 64-Bit-Version zu empfehlen. Sie können das Tool auch in deutscher Sprache herunterladen. Das Dateiserver-Migrationstoolkit ist vollständig kompatibel zu Windows Server 2012 R2. Mit dem Dateiserver-Migrationstoolkit können Sie sowohl zu DFS-Stämmen als auch zu ganz normalen Dateiservern migrieren. DFS als Quelle ist jedoch nicht möglich, sondern nur als Zielsystem.

Selbst Clusterdienste unterstützt das Tool als Quelle und als Ziel. Gibt es bei der Datenübernahme Probleme, kann das Toolkit auch einen Rollback durchführen. Erkennt das Tool bei der Eintragung von Rechten, dass sich bestimmte SIDs nicht auflösen lassen, entfernt es automatisch die problematischen Berechtigungen von den Freigaberechten. Diese Option können Sie aber einstellen, dazu später mehr. Der generelle Ablauf ist ganz einfach:

1. Sie installieren einen neuen Server mit Windows Server 2012 R2 auf neuer Hardware
2. Im Anschluss installieren Sie das Dateiserver-Migrationstoolkit und konfigurieren den Prozess der Migration.
3. Wollen Sie nachträglich noch Daten am Prozess anpassen, konfigurieren Sie einfach die entsprechende XML-Datei des Projekts. Das ist zum Beispiel sinnvoll, wenn Sie den Zielpfad ändern wollen, da das Tool als Stammordner immer den Namen des Quellservers verwendet. Diese Konfiguration können Sie nur in der XML-Datei vornehmen.
4. Sie starten das Projekt und kopieren die Daten auf den neuen Server. Das Dateiserver-Migrationstoolkit kopiert die Daten, die Ordnerstruktur und die Berechtigungen auf den neuen Server. Die Daten auf dem alten Server bleiben erhalten, die Freigaben auf Wunsch auch.

Einrichten der Migration von Daten

Nachdem Sie das Dateiserver-Migrationstoolkit auf dem neuen Dateiserver installiert haben, rufen Sie aus der Programmgruppe das Programm *Dateiservermigrations-Assistent* auf. Dieser Assistent führt Sie durch die Migration. Wollen Sie zu DFS migrieren, müssen Sie zunächst Vorarbeiten durchführen. Dazu später mehr.

Wenn Sie den Assistenten gestartet haben, können Sie entweder ein neues Migrationsprojekt beginnen oder ein abgespeichertes fortsetzen. Wenn Sie ein neues Migrationsprojekt beginnen, erscheint zunächst der Willkommensbildschirm des Dateiserver-Migrationstoolkits.

Nachdem Sie diesen Bildschirm bestätigt haben, können Sie einen Projektnamen und den Speicherort für die Projektdatei festlegen. Die Daten des zu migrierenden Dateiservers werden nicht in diesen Ordner migriert. Im Projektordner liegen nur die Konfigurationsdaten des Projekts, die Sie bei einem erneuten Start laden können. Die Konfiguration speichert das Tool in einer XML-Datei, die Sie nachträglich bearbeiten können. Sie können später den Ordner festlegen, in den die Daten kopiert werden.

Im nächsten Fenster des Assistenten können Sie festlegen, ob Sie einen DFS-Stamm migrieren wollen. Wenn Sie einen normalen Dateiserver migrieren wollen, können Sie in diesem Fenster das Kontrollkästchen deaktivieren. Im nächsten Fenster legen Sie den Speicherort der Dateien und Ordner fest, die von dem zu migrierenden Dateiserver auf den neuen Server kopiert werden sollen. Wenn Sie diese Angaben vorgenommen haben, können Sie den Assistenten mit *Fertig stellen* beenden. An dieser Stelle sind keine weiteren Maßnahmen notwendig und der Assistent ist bereit zur Migration.

Sie sollten sicherstellen, dass Sie diese Migration außerhalb der Geschäftszeiten durchführen, da während des Kopiervorgangs alle Anwender von ihren Freigaben auf dem Quelldateiserver getrennt werden. Bis zu dieser Stelle brauchen Sie nichts zu befürchten. Hier nehmen Sie nur allgemeine Angaben vor, ohne Aktionen durchzuführen.

Nach dem Beenden des Assistenten beginnt erst die eigentliche Migration. Zunächst müssen Sie mit *Server hinzufügen* den Namen des zu migrierenden Quellservers eingeben. Nachdem Sie den Server hinzugefügt haben und der Assistent den Namen des Servers auflösen kann, zeigt das Tool alle Freigaben auf diesem Server in der Liste an und markiert diese automatisch. Sie können mit dem Tool auch Daten zwischen Dateiservern mit Windows Server 2012 R2 migrieren.

Bei Windows Server 2008 R2/Windows Server 2012 R2 oder Windows 7/8 kann es passieren, dass das Dateiserver-Migrationstoolkit keine Verbindung mit WMI zum Quellserver aufbauen kann. In diesem Fall müssen Sie die WMI-Regeln für die Windows-Firewall erst aktivieren, um die Kommunikation zu gestatten. Dazu verwenden Sie am besten den folgenden Befehl:

```
netsh advfirewall firewall set rule group="Windows-Verwaltungsinstrumentation (WMI)" new
enable=yes
```

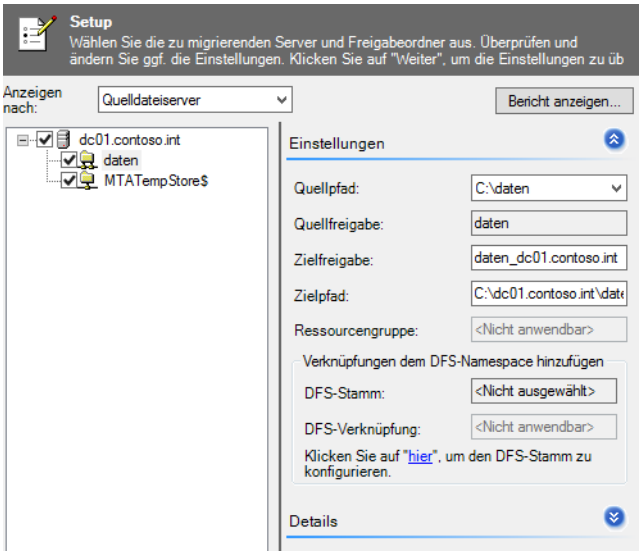
Bei der Aktivierung der Regeln darf keine Fehlermeldung erscheinen. Sie können sich die grafische Verwaltungsoberfläche der Windows-Firewall in Windows Server 2008 R2/2012 und Windows 7/8 auch anzeigen lassen, wenn Sie *wf.msc* im Startbildschirm eingeben. Unter *Eingehende Regeln* finden Sie dann die aktivierten Regeln, die ab jetzt den Zugriff gestatten.

Sollten die Befehle in der Eingabeaufforderung nicht funktionieren, aktivieren Sie die entsprechenden WMI-Regeln direkt über die grafische Verwaltungsoberfläche. Wählen Sie dazu die eingehenden und die ausgehenden Firewallregeln aus und aktivieren Sie diese über das Kontextmenü dieser Regeln.

Sie können entscheiden, welche Freigaben das Tool auf den neuen Server übernehmen soll, und einzelne Freigaben für die Übernahme deaktivieren. Im rechten Bereich der Konsole sehen Sie unter *Details*, wie viele Daten die einzelnen Freigaben enthalten und wie groß die Datenmenge ist.

Bei der Durchführung der späteren Migration übernimmt der Assistent die Ordnerstrukturen und die Dateiinhalte der Ordner. Zusätzlich gibt der Assistent die Ordner wieder unter dem gleichen Namen frei wie auf dem Quelldateiserver. Auch die NTFS-Berechtigungen werden auf den neuen Dateiserver uneingeschränkt übernommen.

Abbildg. 20.25 Anzeigen der Freigaben des Quellservers



Wenn Sie mit dem Dateiserver-Migrationstoolkit Ordner auf einen neuen Server migrieren, entfernt der Assistent auf dem Quellserver alle Freigaben. Die freigegebenen Ordner und alle Daten bleiben auf dem Datenträger erhalten, auch die NTFS-Berechtigungen und der Inhalt bleiben bestehen. Das Dateiserver-Migrationstoolkit entfernt allerdings alle Freigaben, damit die Anwender nicht versehentlich auf die alten Freigaben zugreifen. Sie können diesen Vorgang allerdings während der Migration einstellen.

Stellen Sie sicher, dass in der Anzeige des Quellservers alle Freigaben angezeigt und für die Migration markiert sind. Sobald dies gewährleistet ist, gelangen Sie mit *Fortsetzen* zur nächsten Seite des Assistenten. Sie können bei der Auswahl des Quellservers auswählen, ob die NTFS-Berechtigungen kopiert und die Freigaben auf dem Quelldateiserver beendet werden sollen. Sie können an dieser Stelle mehrere Dateiserver auswählen und mit einem Schritt verschiedene Dateiserver auf den neuen Server migrieren.

Sobald Sie sichergestellt haben, dass Ihre Eingaben korrekt vorgenommen sind, können Sie mit *Fortsetzen* zur nächsten Seite des Assistenten wechseln. Im folgenden Schritt überprüft der Assistent, ob alle Freigaben verfügbar sind und darauf zugegriffen werden kann. Bei allen Freigaben, die migriert werden können, setzt der Assistent ein Häkchen. Achten Sie darauf, dass bei allen Freigaben die Möglichkeit der Migration besteht, und beseitigen Sie bereits an dieser Stelle etwaige Berechtigungs-

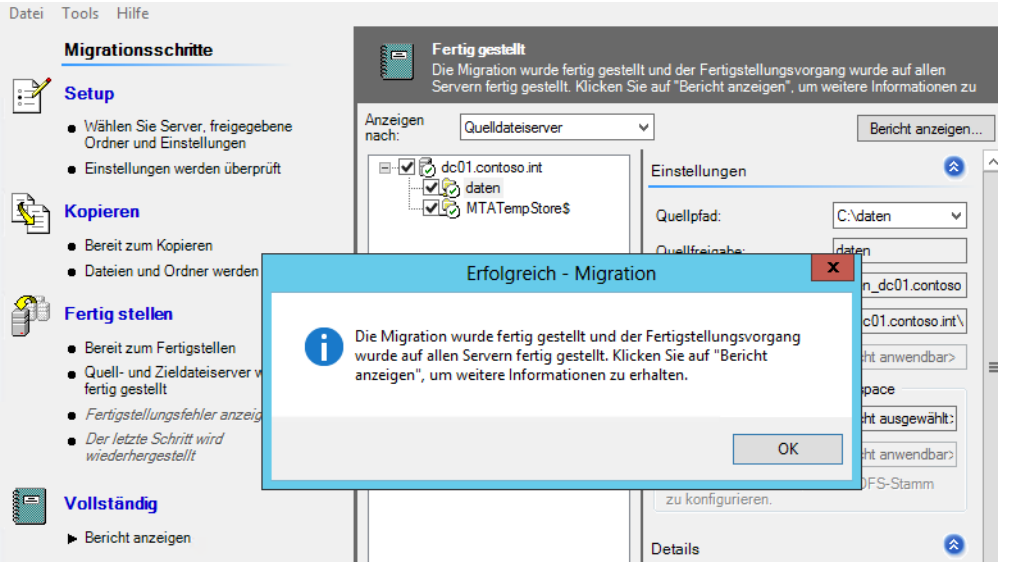
oder Zugriffsprobleme. Der Assistent zeigt Ihnen nach der Überprüfung die Anzahl der Dateien und die Gesamtgröße der zu migrierenden Daten an.

Vor allem bei Dateiservern mit einer großen Anzahl an Freigaben und vielen Daten sollten Sie zuvor genau evaluieren, wie lange der Kopiervorgang über das Netzwerk andauert. Während der Migration der Daten sollten keine Anwender auf den Quell- oder Zielserver zugreifen, um sicherzustellen, dass der Assistent alle Daten ungestört migrieren und die Berechtigungen so setzen kann, wie diese auf dem Quellserver eingestellt sind. Vergleichen Sie die Gesamtzahl der zu migrierenden Dateien im Assistenten mit der tatsächlichen Anzahl von Dateien auf dem Quellserver. Nur so ist sichergestellt, dass der Assistent auch alle Daten übernehmen kann.

Im Anschluss können Sie mit *Fortsetzen* die Migration beginnen. Sie erhalten eine Warnmeldung, dass alle Anwender von ihren Freigaben getrennt und die Freigaben zurückgesetzt werden. Wollen Sie noch Änderungen vornehmen, zum Beispiel einstellen, dass der Stammordner auf dem Zielserver nicht den Namen des Quellservers enthält, bearbeiten Sie die XML-Datei im Projektordner mit einem Editor und ändern Sie den Pfad auf Wunsch ab. Im Anschluss beginnt der Assistent mit der Migration der Daten. Im Bereich *Details* sehen Sie in Echtzeit, welche Daten der Assistent bereits übernommen hat und wo es Probleme gibt. Mit *Abbrechen* können Sie den Kopiervorgang beenden. Alle Ordner des Quellservers werden im konfigurierten Unterordner auf dem Zielserver angelegt und freigegeben.

Der Assistent kopiert nur neue Daten von den Quellservern auf den Zielserver, das heißt, Sie können vor dem Kopieren der Daten durch das Dateiserver-Migrationstoolkit auch eine Datensicherung auf dem neuen Server zurückspielen, was oft schneller geht. Führen Sie dann den Assistenten durch, übernimmt das Toolkit nur neue Dateien, was zu einem wesentlichen Geschwindigkeitsgewinn führt. Die NTFS-Berechtigungen auf dem Quellserver übernimmt der Assistent auf den Zielserver, löscht aber keine Daten auf dem Quellserver. Die Freigaben auf dem Quellserver werden entfernt, wenn Sie diese Option ausgewählt haben. Nach dem erfolgreichen Kopiervorgang erscheint ein Fenster, das Sie über den Abschluss informiert. Zusätzlich können Sie sich in diesem Fenster einen detaillierten Bericht über die Migration anzeigen lassen.

Abbildg. 20.26 Übernehmen der Daten zu Windows Server 2012 R2



Speichern Sie den Bericht ab und legen Sie ihn auf einem Laufwerk ab, damit Sie später auch nachweisen können, dass alle Daten auf den neuen Server migriert wurden. Im Anschluss finden Sie im Zielordner des Zielservers einen neuen Unterordner mit der Bezeichnung des Rechnernamens des Quellservers, falls Sie die Konfiguration in der XML-Datei nicht entsprechend angepasst haben. Unterhalb dieses Ordners finden Sie alle Ordner in der gleichen Struktur wie auf dem Quellserver. Das Tool hat alle Dateien übernommen, die Ordner sind freigegeben und die NTFS-Berechtigungen kopiert. Auf dem Quellserver sind weiterhin alle Daten vorhanden und die Freigaben wurden entfernt.

Bevor Sie jedoch Anwender auf die Freigaben zugreifen lassen, sollten Sie die Rechtestruktur überprüfen, um sicherzustellen, dass auch wirklich alle Rechte korrekt übernommen worden sind.

Der DFS-Konsolidierungsstamm-Assistent

Im Vergleich zur Migration von herkömmlichen Freigaben ist die Migration von Freigaben zu DFS-Stämmen auf neue Server etwas komplizierter. Mit dem Dateiserver-Migrationstoolkit können Sie keine DFS-Stämme migrieren, also kein DFS als Quelle verwenden, aber von mehreren herkömmlichen Dateiservern zu DFS (Distributed File System, verteiltes Dateisystem) unter Windows Server 2012 R2 migrieren.

Die notwendigen Namensräume legt ein Assistent an, und die ursprünglichen Pfade der Anwender funktionieren weiter. Dazu ist es vor der Migration aber notwendig, dass Sie die Dateinamen der aktuellen Dateiserver umbenennen. Sinn ist, dass auf neuen Dateiservern DFS eingerichtet ist und die neuen Dateiserver auf Clientanfragen antworten, wenn Anwender auf die alten Servernamen zugreifen. Das ist wichtig, weil sich für Anwender in den Verknüpfungen und Netzlaufwerken nichts ändern soll. In diesem Fall dürfen die alten Dateiserver aber nicht mehr auf ihren bisherigen Namen antworten. Das heißt, für die Anwender ändert sich nach der Migration nichts, die UNC-Pfade bleiben gleich. Da Sie aber die Dateiserver umbenennen müssen, können Anwender in dieser Phase nicht mehr auf die Daten zugreifen, sondern erst, nachdem der Assistent eingerichtet ist. Wollen Sie den Vorgang aber erst testen, ohne Ihre Dateiserver umzubenennen, gibt es auch dazu eine Möglichkeit.

Neben dem Assistenten zur Übernahme von Daten enthält das Dateiserver-Migrationstoolkit noch den DFS-Konsolidierungsstamm-Assistenten, den Sie als eigene Verknüpfung in der Programmgruppe des Toolkits finden. Dieser Assistent sorgt dafür, dass der UNC-Pfad von Freigaben auf den Quelldateiservern erhalten bleibt und Anwender zukünftig mit der alten Verbindung auf den neuen Server zugreifen dürfen, auch wenn es sich hierbei um eine DFS-Infrastruktur handelt. Auch der Zugriff auf die Dateien, die sich noch auf den alten Servern befinden, die den neuen Namen haben, funktioniert.

Beispiel: Sie wollen den Dateiserver *fs01* zum DFS-Dateiserver *fs2012* migrieren. Auf *fs2012* ist DFS eingerichtet. Bevor Sie den DFS-Assistenten des Dateiserver-Migrationstoolkits starten, müssen Sie den Server *fs01* umbenennen, zum Beispiel in *fs01mig*. Im Assistenten hinterlegen Sie später diesen Namen, sodass dieser die entsprechende Konfiguration für die Namensauflösung durchführen kann und Anwender weiter mit dem alten Namen auf den Server mit dem neuen Namen zugreifen können. Auf diese Weise bleiben Verknüpfungen zu den verschiedenen Ordnern auch zum neuen DFS-Stamm gültig.

Der Assistent ändert dazu auch die notwendigen DNS- und WINS-Einträge der Quell- und Zielserver ab, beziehungsweise erstellt neue Einträge. Das Tool unterstützt auch Failovercluster und DFS-Hochverfügbarkeit. Passende Netzwerknamensressourcen kann der Assistent problemlos erstellen. Anwender, die den ursprünglichen UNC-Pfad auf die Dateien verwenden, leitet der Server zum

neuen Pfad um, auch wenn dieser in einem DFS liegt. Unabhängig davon, ob die Dateien noch auf dem Quelldateiserver liegen oder bereits auf den Zieldateiserver mit DFS migriert sind, funktioniert der alte UNC-Pfad weiterhin.

Microsoft empfiehlt, den DFS-Konsolidierungsstamm-Assistenten als Übergangslösung während der Migration zu verwenden. Auf der Seite *http://support.microsoft.com/kb/829885* [Ms179-K20-07] finden Sie weitere Informationen zur Migration von DFS-Stämmen.

Auf der Startseite finden Sie auch einen Link zur Hilfedatei des Toolkits. Starten Sie den Assistenten, müssen Sie zunächst den Namen des DFS-Stammservers angeben, auf dem Sie den DFS-Stamm zur Migration anlegen können.

Microsoft empfiehlt, für diese Konfiguration einen alleinstehenden DFS-Stamm zu verwenden, keinen domänenintegrierten. Nachdem Sie den Servernamen eingegeben haben, überprüft der Assistent noch dessen Konfiguration. Als Nächstes müssen Sie den Pfad angeben, in den der Assistent die einzelnen DFS-Stämme speichern kann. Für jeden Dateiserver, den Sie mit dem Tool zu DFS migrieren, ist ein eigener Stamm notwendig, der sich in diesem Ordner auf den DFS-Servern befindet. Ist der Ordner auf dem Server noch nicht angelegt, übernimmt dies der Assistent automatisch.

Auf der nächsten Seite geben Sie jetzt den alten Namen des Dateiservers und dessen neuen Namen ein. An dieser Stelle können Sie auch den Test durchführen, den wir weiter vorne bereits erwähnt haben. Geben Sie im Assistenten den Namen des ursprünglichen Servernamens mit einem temporären Namen an. Wollen Sie den Server *dfs* migrieren, geben Sie *dfs* als aktuellen Namen und *dfs-test* als ursprünglichen Namen an. Um zu testen, ob der Assistent die Änderungen erfolgreich durchgeführt hat, versuchen Sie anschließend mit dem Pfad *dfs-test*\<*Freigabename*> auf den Server zuzugreifen. Um diese Änderungen zu entfernen, verwenden Sie das Befehlszeilentool Dfsconsolidate mit der Option */DeleteRoot*. Sie finden das Tool im Installationsordner des Dateiserver-Migrationstoolkits.

Führen Sie die eigentliche Migration durch, müssen Sie vor der Ausführung des Assistenten den Servernamen ändern. Bei *Ursprünglicher Name* tragen Sie den Namen vor der Umbenennung, bei *Aktueller Name* den Namen nach der Umbenennung ein.

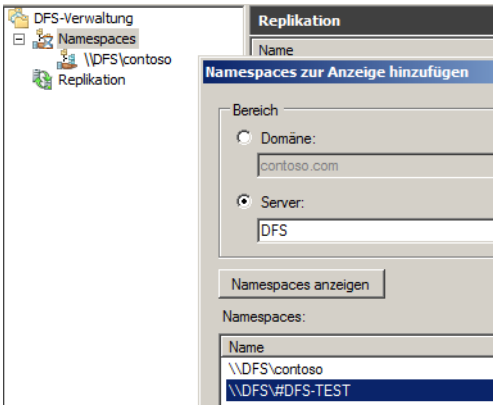
Wichtig ist, dass der Server im Bereich *Aktueller Name* verfügbar ist. Klicken Sie sich weiter durch den Assistenten, legt das Tool die entsprechenden Daten fest und meldet die erfolgreiche Konfiguration. Sie finden in der Forward-DNS-Zone einen neuen Eintrag zum aktuellen Server, der auf die alte IP-Adresse verweist. Sie können also bereits auf die entsprechenden Freigaben auf dem alten Dateiserver mit dem neuen Namen zugreifen. Im entsprechenden Rootordner auf dem DFS-Server befindet sich ein neuer Ordner mit dem Namen des Servers und den entsprechenden Verknüpfungen.

Alle Freigaben des alten Servers sind jetzt auch über den neuen und den alten Namen verfügbar. Außerdem hat der Assistent den Servernamen als DFS-Namensraum hinzugefügt. Um diesen anzuzeigen, gehen Sie folgendermaßen vor:

1. Rufen Sie die DFS-Verwaltung auf und klicken mit der rechten Maustaste auf *Namespaces*.
2. Wählen Sie aus dem Kontextmenü die Option *Namespaces zur Anzeige hinzufügen*.
3. Aktivieren Sie die Option *Server* und geben Sie den Servernamen des DFS-Servers ein.
4. Klicken Sie auf *Namespaces anzeigen*.
5. Wählen Sie den neuen Namensraum aus. Dieser trägt die Bezeichnung des ursprünglichen Servernamens des Quellservers.
6. Klicken Sie auf *OK*.
7. Der Namensraum wird jetzt angezeigt.

8. Sobald Sie auf den Namensraum klicken, sehen Sie alle Freigaben des Quellservers.
9. Auf den Clients können Sie den Vorgang testen, indem Sie auf die Freigaben zugreifen, genauso wie vorher. Für Benutzer ändert sich absolut nichts und es sind keine Konfigurationen notwendig.

Abbildg. 20.27 Hinzufügen des migrierten Namensraums



Der letzte Schritt der Migration ist die Datenübernahme der Freigaben und Ordner auf den neuen Server. Um die Daten zu übernehmen, verwenden Sie den normalen Assistenten zur Übernahme von Ordnern wie bei herkömmlichen Dateiservern auch. Wie Sie dabei vorgehen, haben wir weiter vorne in diesem Abschnitt bereits behandelt.

Im Fenster des Assistenten, auf dem Sie festlegen, ob Sie zu DFS migrieren wollen, aktivieren Sie die Option *Verwenden Sie folgenden DFS-Stammserver* und geben den Namen des DFS-Servers ein. Anschließend überprüft der Assistent den Server und zeigt die erstellten Namensräume und verbundenen Freigaben an.

Die weiteren Schritte entsprechen der Übernahme von normalen Dateiservern. Das gilt auch für die restliche Migration. Sie sehen in den Fenstern auch den Namen des DFS-Servers und den alten Namen des Servers.

Daten über Dateifreigaben zu SharePoint übernehmen

Sie können Daten von Dateiservern auch zu SharePoint übernehmen. Das ist auch bei einer Migration zu Windows Server 2012 R2 sinnvoll, wenn Sie Dateiserver ablösen und die Daten in SharePoint-Bibliotheken übernehmen wollen. SharePoint 2010 bietet für Bibliotheken auch die Möglichkeit, mehrere Dateien auf einmal hochzuladen.

Sie haben auch die Möglichkeit, Bibliotheken in SharePoint auf den Clientcomputern oder Servern als Netzlaufwerk zu verbinden. Der Vorteil dabei ist, dass die Anwender auf die Daten in SharePoint zugreifen können, genauso wie über normale Dateiserver. Auch mehrere Dateien gleichzeitig lassen sich über diesen Weg in Bibliotheken kopieren, was vor allem bei Migrationen sehr hilfreich ist. Der Verbindungsaufbau findet dazu mit WebDAV (Web-based Distributed Authoring and Versioning) statt.

Der Verbindungsaufbau auf den Clients mit Windows 7/8/8.1 ist denkbar einfach. Sie verbinden ein neues Netzlaufwerk und geben als Adresse *http://<Servername>/<Bibliothek>* an.

Nach der Verbindung sehen Sie die Bibliothek und alle Dateien im Explorer. Der Umgang entspricht dem Zugriff auf herkömmliche Dateifreigaben. Das heißt, Sie können Daten von Dateiservern sehr schnell kopieren. Die kopierten Dateien sind dann auch in der Bibliothek verfügbar. Neben der grafischen Oberfläche können Sie die Verbindung auch mit *net use* herstellen lassen, zum Beispiel über Anmeldeskripts. Die Syntax dazu lautet:

```
net use <Buchstabe> "http://<Name des Servers>/Bibliothek>" /User:<Domäne><Benutzername>
<Kennwort>
```

Der Verbindungsaufbau über WebDAV erfolgt durch den Dienst *WebClient Service*. Dieser ist standardmäßig in Windows XP, Windows Vista sowie Windows 7/8/8.1 enthalten und gestartet, aber in Windows Server 2008 und Windows Server 2008 R2/2012/2012 R2 nicht installiert. Aus diesem Grund können Sie auf Servern standardmäßig nicht mit WebDAV arbeiten. Sie haben aber die Möglichkeit, über den Server-Manager das Feature *Desktopdarstellung* zu installieren. Dieses enthält auch den WebClient-Dienst. Nach der Installation können Sie auch in Windows Server 2008 und Windows Server 2008 R2/2012 mit Netzlaufwerken und SharePoint-Bibliotheken arbeiten.

Sollte auch nach der Installation des Features der Verbindungsaufbau nicht funktionieren, starten Sie den Systemdienst *WebClient* neu. Der Verbindungsaufbau mit WebDAV ist in vielen Umgebungen sehr langsam. Meist lässt sich das Problem beheben, indem Sie die Option *Automatische Suche der Einstellungen* im Internet Explorer deaktivieren. Sie finden diese Einstellung in den Internetoptionen auf der Registerkarte *Verbindungen* über die Schaltfläche *LAN-Einstellungen*. Außerdem sollten Sie dafür sorgen, dass die SharePoint-Server zu der Intranetzone gehören. Diese Einstellung finden Sie auf der Registerkarte *Sicherheit*. Sie sehen die Zuordnung im unteren Bereich des Internet Explorers, wenn Sie die Bibliothek aufrufen. Achten Sie auch darauf, dass die Ports 137,138,139 und 445 zwischen Client und Server verfügbar sind.

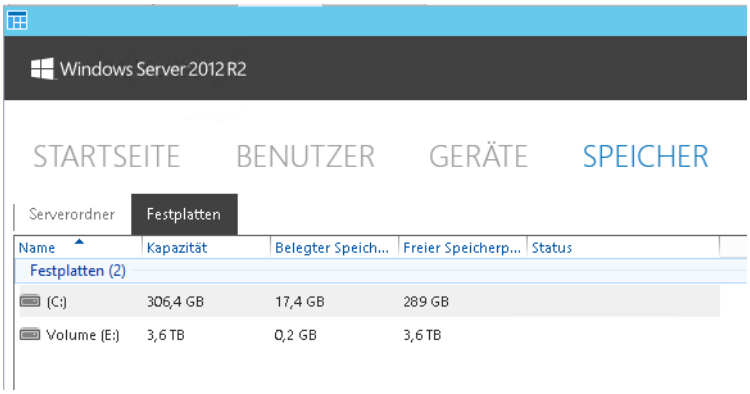
Arbeiten Sie mit SSL, muss noch der Port 443 offen sein. Haben Sie Webanwendungen mit anderen Ports konfiguriert, müssen Sie auch diese öffnen. Microsoft bietet ein kostenloses Skript zum Upload von Dokumenten an. Sie finden das PowerShell-Skript auf der Seite *http://gallery.technet.microsoft.com/ScriptCenter/en-us/f538c34c-4f74-4645-9649-fd25e49805d6* [Ms179-K20-08]. Das Skript hat allerdings den Nachteil, ziemlich komplex zu sein, da sich Administratoren zum einen mit den neuen Dateiklassifizierungsdiensten in Windows Server 2008 R2 und Windows Server 2012 R2 auseinandersetzen müssen, zum anderen mit der PowerShell und den Rechten im Dateisystem und in SharePoint. Mehr zu diesem Thema lesen Sie im nächsten Kapitel.

Serverspeicher in Windows Server 2012 R2 im Dashboard verwalten

Im folgenden Abschnitt zeigen wir Ihnen, wie Sie Festplatten in das Dashboard von Windows Server 2012 R2 Essentials integrieren und Daten in kleinen Netzwerken freigeben. Im Dashboard auf dem Server können Sie über *Speicher* auf der Registerkarte *Festplatten* den aktuell verfügbaren Speicher auf dem Server überprüfen.

Sie haben an dieser Stelle auch die Möglichkeit, über Assistenten einzelne Freigaben auf neue Datenträger zu verschieben. Die Konsole zeigt allerdings nur Datenträger an, die Sie im Betriebssystem integriert und formatiert haben. Hier gehen Sie vor, wie in Kapitel 5 beschrieben. Sie können auch in Windows Server 2012 R2 Essentials Speicherpools nutzen und einrichten. Lesen Sie sich dazu das Kapitel 5 durch.

Abbildg. 20.28 Verwalten des Serverspeichers von Windows Server 2012 R2 Essentials



Wollen Sie neuen Serverspeicher integrieren, müssen Sie zunächst die Hardware mit dem Server verbinden und mit der Datenträgerverwaltung von Windows Server 2012 R2 vorbereiten. Alternativ erstellen Sie über den Link *Erweitert: Speicherplatz verwalten* einen Speicherpool (siehe Kapitel 5).

Sobald der Datenträger formatiert ist oder Sie einen Speicherpool eingerichtet haben, lässt er sich im Dashboard verwenden. Auf der Registerkarte *Serverordner* haben Sie die Möglichkeit, Daten von Anwendern mit Assistenten und auf einen Rutsch auf neue Datenträger zu verschieben und Freigaben zu erstellen.

Abbildg. 20.29 Verwalten der Freigaben in Windows Server 2012 R2 Essentials

Ordner im Dashboard verwalten

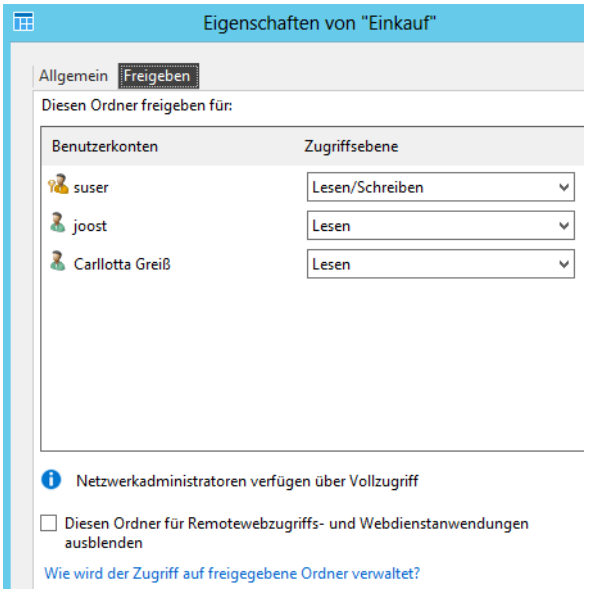
Windows Server 2012 R2 Essentials ermöglicht zwar auch die Freigabe und Verwaltung von Ordnern mit den Windows Server 2012 R2-Bordmitteln, aber im Dashboard sind einfach zu bedienende Assistenten integriert, um Ordner freizugeben. Sie sollten daher primär das Dashboard für das Freigeben von Ordnern verwenden.

Um Freigaben zu verwalten, klicken Sie im Dashboard zunächst auf die Schaltfläche *Speicher*. An dieser Stelle sehen Sie die bereits freigegebenen Ordner in Windows Server 2012 R2 Essentials. Klicken Sie eine bereits existierende Freigabe mit der rechten Maustaste in der Konsole an, können Sie mit *Ordner öffnen* ein Explorer-Fenster öffnen, das den Inhalt des Ordners anzeigt.

Mit dem Kontextmenübefehl *Freigabe des Ordners beenden* heben Sie die Freigabe auf und Anwender können sich nicht mehr mit dem Ordner verbinden. Die Daten bleiben aber auf dem Server und die Freigabe lässt sich jederzeit wieder neu erstellen.

Mit dem Kontextmenübefehl *Ordnereigenschaften anzeigen* starten Sie ein neues Fenster, in dem Sie einstellen, welche Benutzer Zugriff auf die Freigabe erhalten sollen. Auf der Registerkarte *Freigeben* sehen Sie die angelegten Benutzer und können über das Dropdownmenü deren Rechte festlegen.

Abbildg. 20.30 Verwalten der Rechte einer Freigabe



Freigaben im Dashboard erstellen

Wollen Sie eine neue Freigabe im Dashboard erstellen, klicken Sie im Dashboard im rechten Fensterbereich unter der Überschrift *Serverordner-Aufgaben* auf den Befehl *Ordner hinzufügen*.

Es startet ein Assistent, über den Sie festlegen können, wie die Freigabe den Anwendern zur Verfügung steht. Der erste Schritt besteht darin, bei *Ort* den freizugebenden Ordner auf dem Server auszuwählen sowie den Namen der Freigabe. Auch eine Beschreibung legen Sie an dieser Stelle fest.

Wählen Sie die Festplatte aus, auf der Sie die Daten der Freigabe speichern wollen. Sie müssen den Ordner vorher nicht im Explorer anlegen, der Assistent erstellt auch den entsprechenden Unterordner im Ordner *ServerFolders* der Festplatte. Hier sind immer alle Freigaben verfügbar, die Sie auf dem Server verwenden. Setzen Sie mehrere Festplatten ein, befindet sich auf jeder Festplatte dieser Ordner.

Auf der nächsten Seite legen Sie die Berechtigungen fest. Diese Rechte können Sie in den Eigenschaften der Freigabe jederzeit anpassen. Auch in den Eigenschaften der Benutzerkonten im Dashboard legen Sie fest, wie die einzelnen Anwender auf die verschiedenen Freigaben zugreifen dürfen.

Nachdem Sie die Freigabe erstellt haben, sollten Sie noch definieren, dass die Daten der Freigabe auch mit gesichert werden (siehe Kapitel 36).

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Windows Server 2012 R2 als Dateiserver betreiben und Freigaben erstellen. Auch die Konfiguration von Zugriffsberechtigungen über Gruppen und im NTFS war Thema dieses Kapitels. Und schließlich sind wir auch auf die Verwendung der Offlinedateien näher eingegangen.

Im nächsten Kapitel beschäftigen wir uns ausführlicher mit dem Ressourcen-Manager für Dateiserver und das verteilte Dateisystem, beides Bereiche für Enterprise-Umgebungen.

Kapitel 21

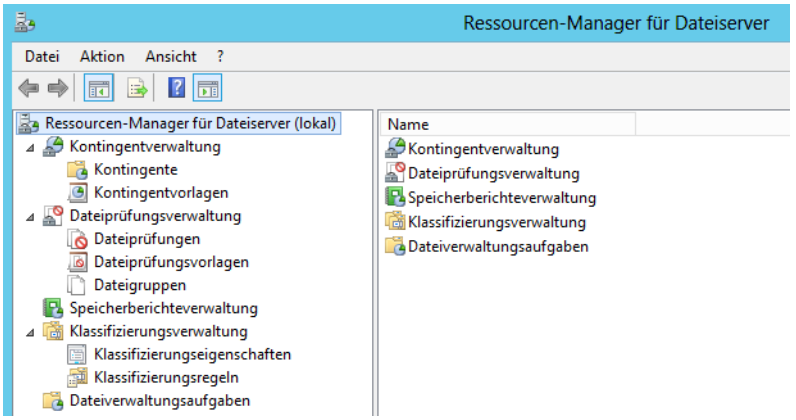
Ressourcen-Manager für Dateiserver

In diesem Kapitel:

Mit dem Ressourcen-Manager für Dateiserver organisieren Sie Ihre Dateiserver im Unternehmen. Sie können mit dem Tool Kontingente erstellen, Freigaben auf bestimmte Dateitypen durchsuchen oder Daten mit Metadaten versorgen. Auch in Zusammenarbeit mit SharePoint bieten die Dienste eine wertvolle Hilfe. Wir zeigen Ihnen in diesem Kapitel, wie Sie die verschiedenen Möglichkeiten des Ressourcen-Managers für Dateiserver nutzen. Wir gehen in diesem Kapitel auch auf das verteilte Dateisystem (DFS) sowie auf die Anbindung von UNIX-Rechnern mit NFS ein.

Der Ressourcen-Manager für Dateiserver ist standardmäßig nicht installiert. Sie können das Tool über den Server-Manager hinzufügen. Die Optionen dazu finden Sie über *Datei- und iSCSI-Dienste*. Nach der Installation starten Sie das Tool am schnellsten durch Eingabe von *fsrm.msc* auf der Startseite.

Abbildg. 21.1 Verwenden des Ressourcen-Managers für Dateiserver



TIPP Nachdem Sie das Programm gestartet haben, können Sie über *Optionen konfigurieren* im Kontextmenü zum Eintrag *Ressourcen-Manager für Dateiserver* detaillierte Benachrichtigungen und Berichte erstellen lassen.

Vor allem die E-Mail-Adressen der Administratoren sollten Sie konfigurieren, damit Sie später die konfigurierten Berichte und Warnungen erhalten. Nachdem Sie die Administratoren eingetragen haben, sollten Sie zunächst mit der Schaltfläche *Test-E-Mail senden* überprüfen, ob die E-Mail beim gewünschten Empfänger ankommt.

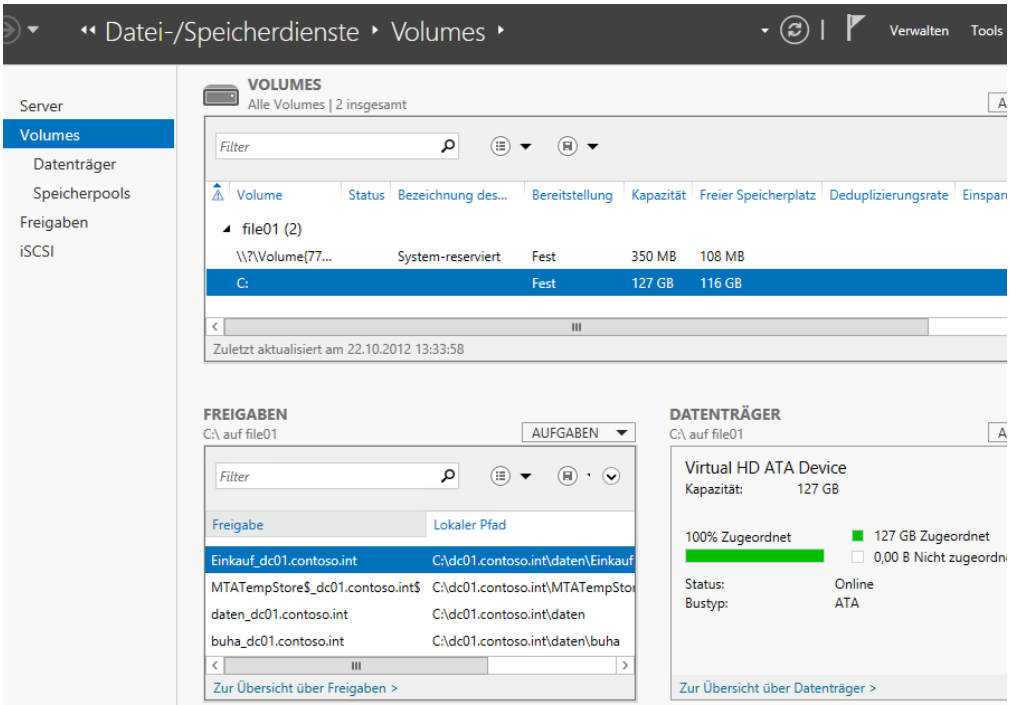
Kontingentverwaltung in Windows Server 2012 R2

Windows 8 und Windows Server 2012 R2 bieten, wie die Vorgängerversionen auch, die Möglichkeit, Datenkontingente festzulegen. Administratoren können so steuern, wie viele Daten Anwender speichern dürfen. Der Ressourcen-Manager für Dateiserver (Fileserver Resource Manager, FSRM) erlaubt eine Steuerung dieser Funktion. 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 eine Kachel auf der Startseite oder durch Eingabe von *fsrm.msc* auf der Startseite. Standardmäßig ist der Rollendienst nicht installiert. Wollen Sie diesen nutzen, müssen Sie ihn zunächst installieren. Dazu wählen Sie *Verwalten/Rollen und Features installieren* und wählen dann über die Serverrollen *Datei- und Speicherdienste/Ressourcen-Manager für Dateiserver aus*.

In Windows Server 2012 R2 sehen Sie im Server-Manager über *Datei-/Speicherdienste* bereits ausführliche Informationen zur Speichernutzung und auch zu den doppelten Dateien (siehe Kapitel 1).

Abbildg. 21.2 Verwalten der Speicherplätze in Windows Server 2012 R2

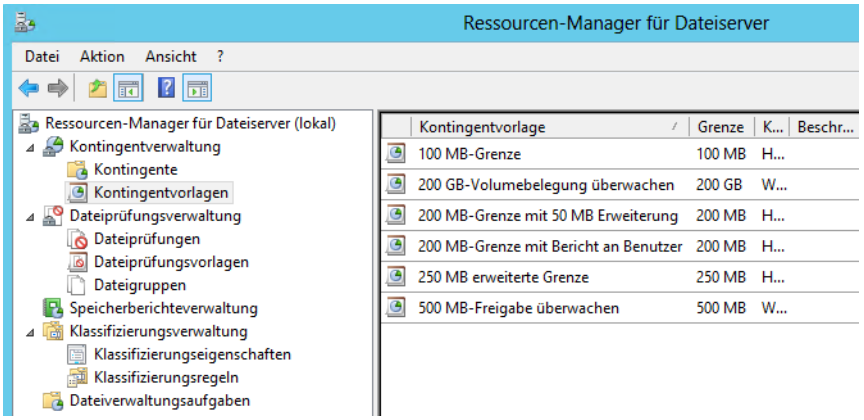


Kontingentverwaltung mit FSRM

Mit einem Kontingent können Sie festlegen, dass ein Benutzer nur eine bestimmte Menge Daten in einem Laufwerk speichern kann. Sie können mithilfe von FSRM eine E-Mail an Administratoren und den Benutzer senden, damit dieser rechtzeitig Daten auf seinem Laufwerk löschen kann.

Erweitern Sie den Konsoleneintrag *Kontingentverwaltung*, steht Ihnen die Konfiguration von Kontingenten und von Kontingentvorlagen an dieser Stelle zur Verfügung. Sie können hier für einzelne Freigaben oder ganze Datenträger Kontingente festlegen, also Speichergrenzen, die von den Anwendern nicht überschritten werden dürfen.

Abbildg. 21.3 Dateiserver mit dem Ressourcen-Manager für Dateiserver verwalten



Beispiele

Sie können eine Grenze von 200 Megabyte für den persönlichen Ordner eines Benutzers auf einem Server festlegen und bestimmen, dass Sie und der Benutzer benachrichtigt werden, wenn 180 MB Speicherplatz überschritten sind.

Für den gemeinsam verwendeten Ordner einer Gruppe legen Sie ein flexibles Kontingent von 500 MB fest. Erreicht die Gruppe diese Speicherbeschränkung, informiert der Server alle Benutzer in der Gruppe per E-Mail, dass das Speicherkontingent temporär auf 520 MB erweitert wurde.

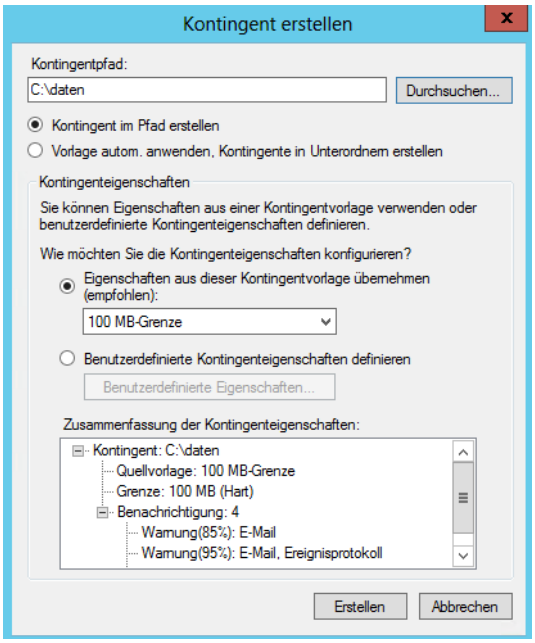
Sie können festlegen, dass Sie eine Benachrichtigung erhalten, wenn die Größe eines Ordners 2 GB erreicht, ohne jedoch das Kontingent dieses Ordners zu beschränken.

Erstellen von Kontingenten und Kontingentvorlagen

Kontingente erstellen Sie aus einer Vorlage oder individuell für einzelne Ordner. Wenn Sie Kontingente aus Vorlagen erstellen, können Sie die Kontingente zentral verwalten, indem Sie statt der einzelnen Kontingente die Vorlagen konfigurieren. Alle Kontingente, welche diese Vorlage nutzen, werden dann auf Wunsch automatisch aktualisiert. Bei der Erstellung gehen Sie folgendermaßen vor:

1. 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.
2. Wählen Sie unter *Kontingentpfad* den Pfad zu dem Ordner aus, für den das Kontingent gelten soll. Um ein Kontingent basierend auf einer Vorlage zu erstellen, wählen Sie unter *Kontingentvorlagen* die Vorlage aus, auf der das neue Kontingent basieren soll.
3. Klicken Sie dann mit der rechten Maustaste auf die Vorlage und wählen Sie im Kontextmenü den Befehl *Kontingent mithilfe einer Vorlage erstellen*.
4. 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.

Abbildg. 21.4 Erstellen eines neuen Kontingents



5. Alle Vorlageneigenschaften werden unter *Zusammenfassung der Kontingenteigenschaften* angezeigt. 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 automatisch anwenden, Kontingente in Unterordnern erstellen* aktivieren. Sobald in dem konfigurierten Ordner ein neuer Unterordner erstellt wird, wendet der Server dieses Kontingent für diesen Unterordner automatisch an.

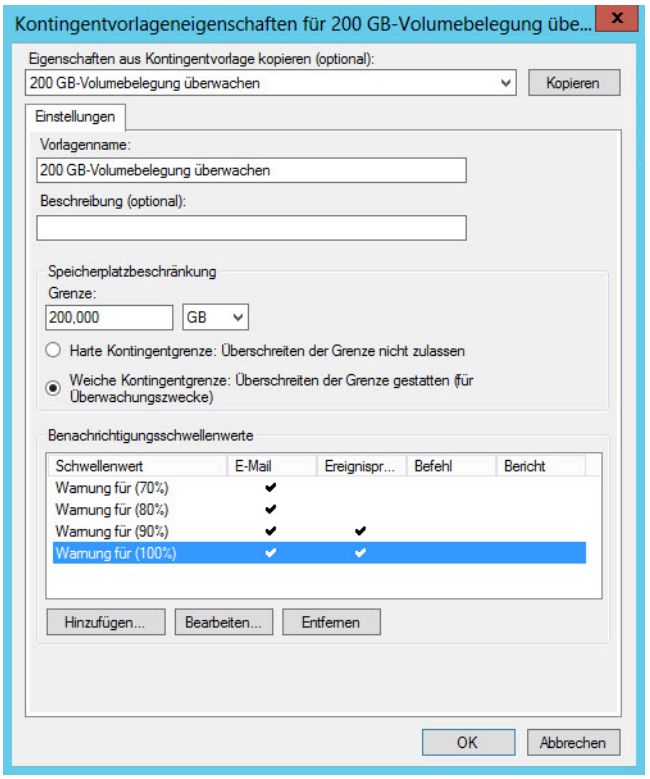
Schwellenwerte und Grenzwerte verstehen

Sie können einer Vorlage durch Klicken auf die Schaltfläche *Hinzufügen* verschiedene Schwellenwerte und 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.

Bei der Erstellung von Kontingentvorlagen oder herkömmlichen Kontingenten 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 Ordner 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.

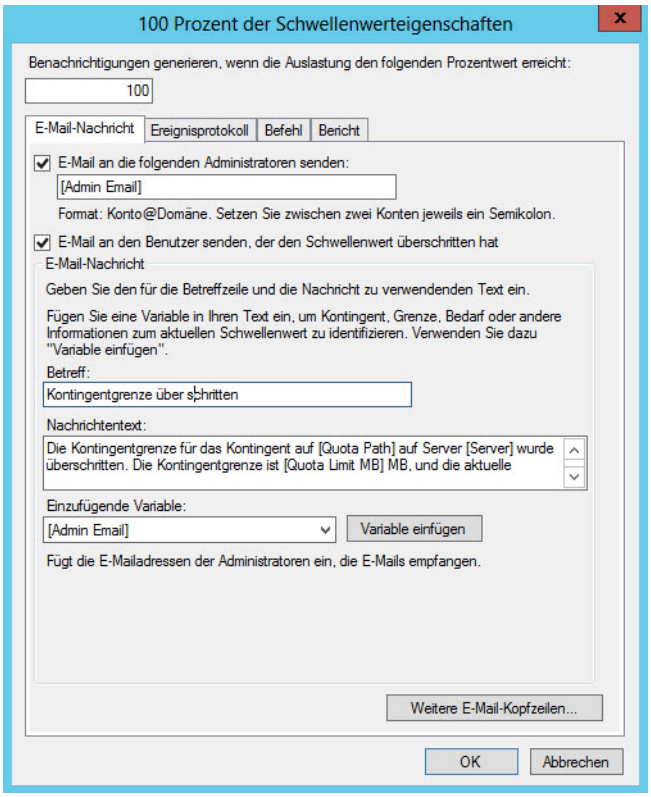
Abbildg. 21.5 Festlegen der Grenzen für ein Kontingent



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 Semikola 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.

Abbildg. 21.6 Bearbeiten einer Kontingentvorlage



- 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.

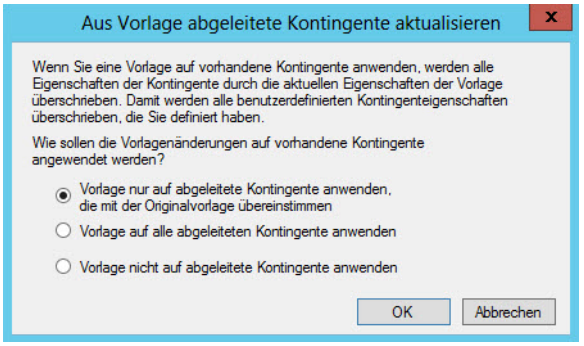
Anpassen von Kontingentvorlagen

Sie können die Eigenschaften der vorhandenen oder von Ihnen erstellten Kontingentvorlagen jederzeit bearbeiten, wenn Sie auf der entsprechenden Vorlage oder dem Kontingent 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. 21.7 Aktualisieren von Kontingenten nach Bearbeitung einer Vorlage



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.

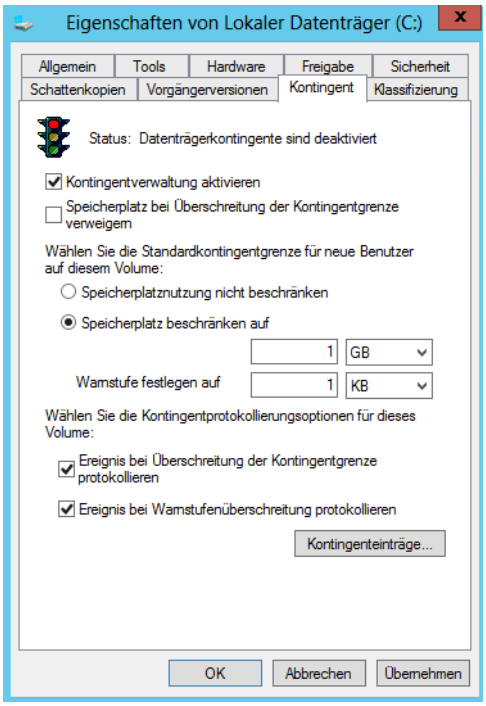
Wechseln Sie in diesem Fall im Knoten *Kontingentverwaltung* zu *Kontingente* und wählen Sie dann den Kontingenteintrag mit dem Problem aus. Klicken Sie im Aktionsbereich auf *Kontingente anzeigen, die sich auf Ordner auswirken* und suchen Sie nach Kontingenten, die auf übergeordnete Ordner angewendet sind. So können Sie identifizieren, welche Kontingente restriktive Einstellungen für das ausgewählte Kontingent haben.

Datenträgerkontingente für Laufwerke festlegen

Klicken Sie ein Laufwerk im Explorer von Windows Server 2012 R2 mit der rechten Maustaste an, steht Ihnen die Registerkarte *Kontingent* zur Verfügung. Aktivieren Sie die Kontingentüberwachung, können Sie festlegen, welche Datenmenge die einzelnen Benutzer auf dem Computer speichern dürfen. Das funktioniert auch bei Windows 8 Pro und Enterprise.

Der Unterschied zur Kontingentverwaltung im Ressourcen-Manager ist, dass Sie an dieser Stelle immer nur einen Eintrag für komplette Datenträger erstellen. Sie können an dieser Stelle weder Ordner mit Kontingenten berücksichtigen oder mehrere Server oder Laufwerke zentral verwalten. Klicken Sie auf die Schaltfläche *Kontingenteinträge*, können Sie festlegen, für welche Anwender Sie besondere Grenzen festlegen wollen. Alle anderen Anwender können die maximale Datenmenge speichern, die Sie auf der Hauptseite des Fensters festlegen.

Abbildg. 21.8 Festlegen von Kontingenteinträgen für ganze Laufwerke



Sie erreichen aber durch dieses einfache Werkzeug im Explorer die Möglichkeit, die Datenträgerverwendung zu überwachen. Dazu aktivieren Sie die Kontingentüberwachung im Explorer, legen aber keine Grenzwerte fest.

So erhalten Sie auch ohne die Verwendung des Ressourcen-Managers für Dateiserver eine umfangreiche Überwachung der Datenträgernutzung. Über die Schaltfläche *Kontingenteinträge* sehen Sie die einzelnen Benutzer und Gruppen sowie deren Datenträgernutzung. In der Eingabeaufforderung verwenden Sie dazu den Aufruf *fsutil quota query <Laufwerk>*.

Administratoren sind von der Kontingentüberwachung nicht ausgenommen, allerdings können Administratoren auch bei harten Grenzwerten weiter speichern. Normale Benutzer dürfen beim Erreichen des Grenzwerts nicht mehr speichern.

Kontingente und ReFS

Datenfestplatten lassen sich in Windows Server 2012 R2 auch mit dem neuen Dateisystem ReFS (Resilient File System, unverwüstliches Dateisystem) formatieren (siehe Kapitel 5). ReFS kann allerdings keine Kontingente verwalten. Das heißt, Sie müssen Datenträger mit NTFS formatieren, wenn Sie Kontingente im Explorer oder über den Ressourcen-Manager erstellen wollen.

Der größte Vorteil des neuen Dateisystems soll dessen Robustheit sein und die höhere Geschwindigkeit, in der sich das Dateisystem im laufenden Betrieb reparieren lässt. Außerdem beherrscht das Dateisystem tiefere Ordnerstrukturen und längere Dateinamen. Außerdem sollen keine Daten verloren gehen, da das neue Dateisystem eine verbesserte Version der Schattenkopien mitbringt.

ReFS Datenträger beherrschen eine Größe von 16 Exabyte. Berechtigungen lassen sich auf ReFS-Datenträger genauso vergeben wie in NTFS. Die Zugriffsschnittstelle (API), mit der das neue Dateisystem kommuniziert, entspricht dem von NTFS. Alles in allem ist ReFS stabiler und schneller als NTFS. Das Dateisystem unterstützt derzeit allerdings keine Bootmedien von Windows Server 2012 R2. In Windows 8 ist ReFS aktuell nicht integriert. Allerdings können Computer mit Windows 7/8 problemlos auf Freigaben zugreifen, die auf ReFS-Datenträgern gespeichert sind.

Dateiprüfungsverwaltung nutzen

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.

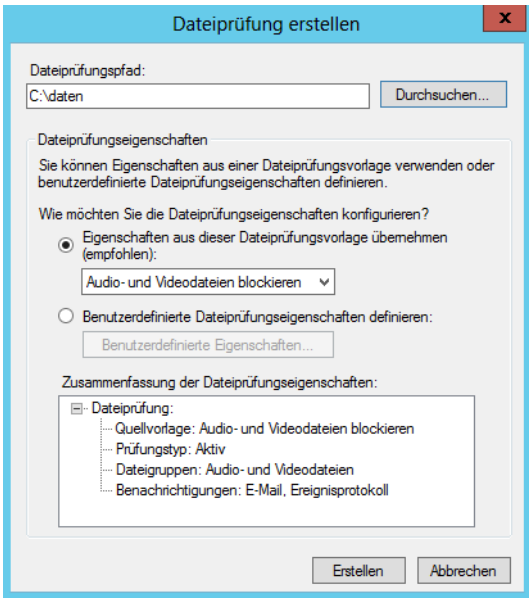
Speziellen Anwendern im Unternehmen können dagegen besondere Privilegien zum Speichern beliebiger Dateien in seinem persönlichen Ordner gewährt werden. Mit diesem Feature von FSRM können Sie also Ihren Anwendern das Speichern von bestimmten Dateianhängen wie zum Beispiel **.mp3*, **.mpeg* oder **.wmv* untersagen. Versucht ein Anwender, eine solche Datei zu speichern, können Sie Benachrichtigungen konfigurieren, die automatisch verschickt werden.

Erstellen einer Dateiprüfung

Wenn Sie in 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 anlegen oder eine benutzerdefinierte Prüfung definieren. 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).

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.

Abbildg. 21.9 Erstellen einer Dateiprüfung



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 mithilfe dieser Vorlage erstellt wurden.

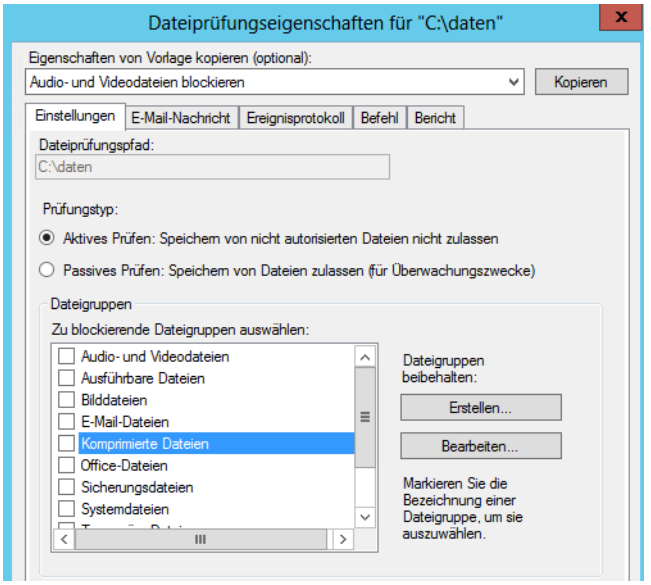
Wählen Sie unter *Wie möchten Sie die Dateiprüfungseigenschaften konfigurieren?* die Option *Benutzerdefinierte Dateiprüfungseigenschaften definieren* aus und klicken Sie dann auf die Schaltfläche *Benutzerdefinierte Eigenschaften*. Möchten Sie Eigenschaften aus einer vorhandenen Vorlage kopieren, wählen Sie die zu verwendende Vorlage aus und klicken Sie auf *Kopieren*. Wählen Sie unter *Prüfungstyp* den Typ 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.

Abbildg. 21.10 Erstellen einer Dateiprüfung



Dateiprüfungsausnahmen

Um Dateien zuzulassen, die von 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. 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 viele Dateigruppen angelegt, die Sie beliebig bearbeiten können. Um eine neue Dateigruppe zu erstellen, klicken Sie in der Konsolenstruktur von 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 in FSRM

Sie können mit dem Ressourcen-Manager für Dateiserver auch Berichte erstellen, welche die Nutzung der Freigaben und Ordner visualisieren. Dazu nutzen Sie den Eintrag *Speicherberichteverwaltung* in der Konsolenstruktur von FSRM.

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.

Ein Bericht kann zum Beispiel alle doppelt vorhandenen Dateien auf einem Laufwerk oder auf einem Server 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 Sie erstellen einen Bericht für Dateien nach Besitzer, um zu analysieren, wie einzelne Benutzer die gemeinsamen Speicherressourcen verwenden.

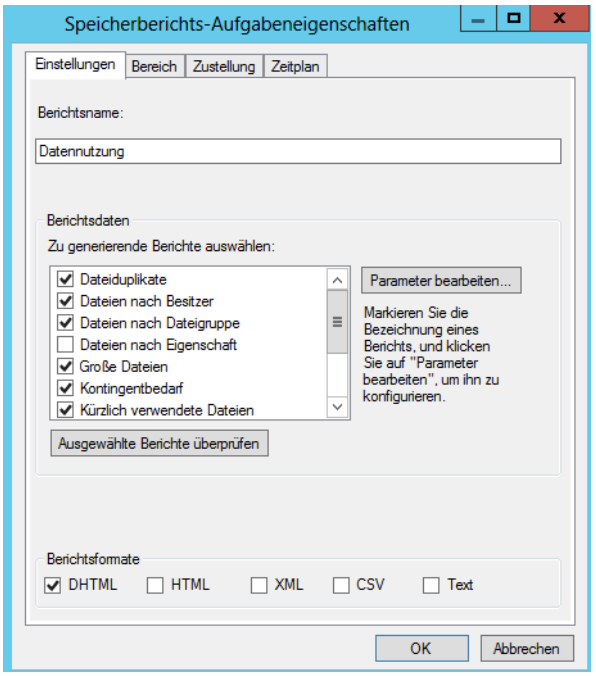
Jeder Bericht kann ein eigenes Format haben. Sie können zum Beispiel regelmäßige HTML-Berichte und Abteilungsberichte erstellen, die den Abteilungsleitern einen Überblick über den aktuellen Speicherbedarf der Dateien verschaffen. Durch die Speicherberichte können Sie sich bequem per E-Mail regelmäßig 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.

Wollen Sie einen Speicherbericht erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf *Speicherberichteverwaltung* und dann auf *Neue Berichtaufgabe planen*.
2. Klicken Sie im daraufhin geöffneten Dialogfeld auf der Registerkarte *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* auf der Registerkarte *Einstellungen* 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*.
6. Bearbeiten Sie die Parameter nach Bedarf und bestätigen Sie mit *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. 21.11 Verwenden der Speicherberichteverwaltung



Dateiklassifizierungsinfrastruktur einsetzen

Die Dateiklassifizierungsinfrastruktur (File Classification Infrastructure, FCI) im Ressourcen-Manager für Dateiserver stellen eine interessante Funktion für Dateiserver dar, um zum Beispiel Daten zu SharePoint zu migrieren. Die Dienste können bestehende Dokumente untersuchen, Inhalte feststellen und entsprechende Richtlinien anwenden.

Dazu können Sie Dokumenten zusätzliche Eigenschaften zuweisen wie in SharePoint. Die Eigenschaften liegen direkt im Dokument, nicht im NTFS-Dateisystem. Die Dateiklassifizierungsdienste gehören zum Rollendienst *Ressourcen-Manager für Dateiserver*. Sie verwalten daher diese Funktion auch über die Verwaltungskonsole des Ressourcen-Managers für Dateiserver (FSRM). Über den Menüpunkt *Klassifizierungsverwaltung* verwalten Sie die Dateiklassifizierung.

HINWEIS Die Dateiklassifizierung funktioniert auch in Failoverclustern und bei eingescannten Dokumenten, die per OCR bearbeitet sind.

Klassifizierungseigenschaften und Klassifizierungsregeln verstehen und einsetzen

Die Eigenschaften verhalten sich ähnlich zu den Eigenschaften von Dateien in SharePoint. Eigenschaften, die Sie an dieser Stelle für Dokumente festlegen, werden nicht im NTFS, sondern in der Datei direkt gespeichert.

Klicken Sie mit der rechten Maustaste auf *Klassifizierungseigenschaften*, können Sie mit *Nur für* festlegen, welche neuen Kriterien Dateien zugeordnet werden sollen. So lässt sich zum Beispiel festlegen, ob ein Dokument zu einem Projekt gehört, private Daten enthält, nur für den internen Gebrauch oder für bestimmte Personen nutzbar sein soll:

1. Im neuen Fenster geben Sie zunächst den Namen der neuen Eigenschaft an, zum Beispiel *Nur für internen Gebrauch*.
2. Geben Sie anschließend eine Beschreibung der Eigenschaft an, falls diese nicht aus dem Namen ersichtlich ist.
3. Über *Eigenschaftentyp* stehen Ihnen verschiedene Möglichkeiten zur Verfügung, die Eigenschaft festzulegen. Neben Ja/Nein, können Sie eine Multiple Choice-Liste erstellen, eine Nummer angeben oder eine Uhrzeit hinterlegen.
4. Im unteren Bereich bearbeiten Sie schließlich die Eingaben genauer, die als Klassifizierung zur Auswahl stehen.

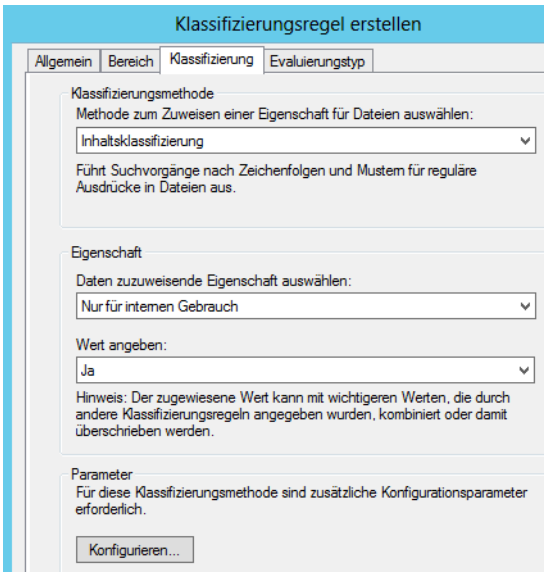
Sie können mehre Eigenschaften festlegen und diese auch nachträglich ändern. Die Eigenschaften werden in FSRM unter *Klassifizierungsverwaltung/Klassifizierungseigenschaften* angezeigt.

Das Anlegen und Bearbeiten von Klassifizierungseigenschaften ändert aber noch keine Dokumente ab, sondern bietet nur die Verwendung der jeweiligen Eigenschaften an. Damit diese auch mit Dokumenten verknüpft werden, müssen Sie Klassifizierungsregeln erstellen über das Kontextmenü von *Klassifizierungsregeln*.

Erstellen Sie eine neue Regel, legen Sie zunächst den Namen der Regel fest und bestimmen auf der Registerkarte *Bereich*, welche Ordner im Dateisystem die Regel berücksichtigen sollen. Auf der Registerkarte *Klassifizierung* legen Sie fest, dass Sie Dateien mit der Ordnerklassifizierung ändern möchten, und wählen die erstellte Klassifizierungseigenschaft und den Wert aus, den der Server den Dateien zuordnen soll. Anschließend stempelt die Regel alle Dateien in den entsprechenden Ordnern automatisch mit den hinterlegten Klassifizierungseigenschaften.

Über den Befehl *Klassifizierungszeitplan konfigurieren* im Kontextmenü der *Klassifizierungsregeln* können Sie festlegen, wann Klassifizierungsregeln starten sollen, ob Sie einen Bericht erhalten möchten (wenn ja, in welchem Format) und zahlreiche weitere Einstellungen.

Abbildg. 21.12 Festlegen der Metadaten für die Dateien im ausgewählten Ordner

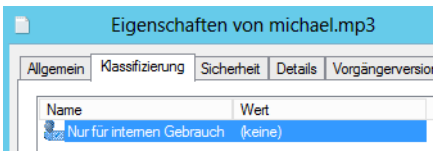


Klassifizierungsregeln werden durch Klassifizierungszeitpläne gesteuert. Speichern Anwender neue Dokumente in den entsprechenden Ordnern, stempelt der Server automatisch die Dateien mit den entsprechenden Metadaten. Die Klassifizierungsregeln verwenden dann wiederum die Klassifizierungseigenschaften. Sie können die Regeln an dieser Stelle auch sofort ausführen lassen. Auf der Registerkarte *Klassifizierung* in den Eigenschaften einer Regel legen Sie bei *Klassifizierungsmethode* fest, ob Sie die Klassifizierung auf Basis des Ordners, in dem das Dokument gespeichert ist, durchführen wollen, oder auf Basis des Inhalts. Bei *Eigenschaft* wählen Sie die Klassifizierungseigenschaft aus, die Sie für die Regel und den hinterlegten Bereich untersucht und festgelegt haben wollen.

Auf der Registerkarte *Klassifizierung* können Sie über *Parameter* erweiterte Eigenschaften festlegen, die auf .NET Framework basieren. Welche Möglichkeiten Sie hier haben, erfahren Sie am schnellsten über die Webseite *http://msdn.microsoft.com/de-de/library/20bw873z.aspx* [Ms179-K21-01]. Sie müssen die zusätzlichen Klassifizierungsparameter aber nicht verwenden. Der Einsatz ist nur sinnvoll, wenn Sie sich mit den programmtiertechnischen Hintergründen von .NET Framework auskennen. Der Hintergrund an dieser Stelle sind die .NET Regular Expressions. An dieser Stelle können Sie den Inhalt des Dokuments entsprechend nach bestimmten Inhalten und Textstellen durchsuchen.

Sie können mehrere Regeln erstellen und komplexere Regeln anwenden. Auch das Zuteilen von einzelnen Eigenschaften zu Dateien ist möglich. Haben Sie den Suchlauf gestartet, sehen Sie in den Eigenschaften der Dateien auf der Registerkarte *Klassifizierung* die zugeordneten Eigenschaften.

Abbildg. 21.13 Anzeigen der Eigenschaften von Dateien nach dem Suchlauf

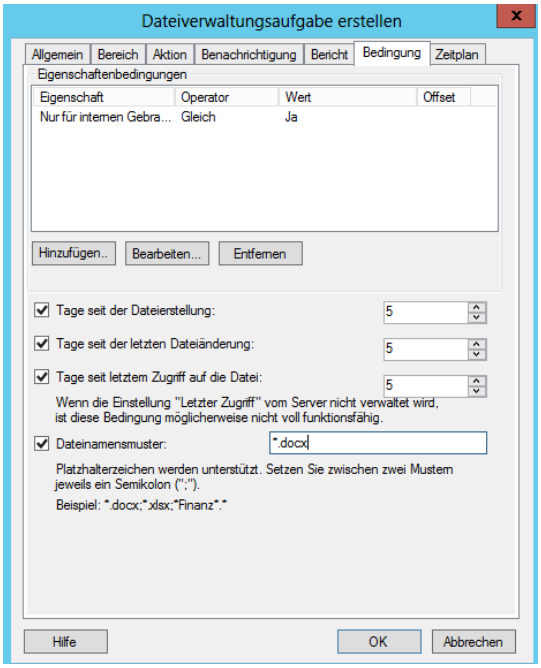


Dateiverwaltungsaufgaben bei der Dateiklassifizierung einsetzen

Nachdem Sie Klassifizierungsregeln erstellt haben, die zum festgelegten Zeitpunkt die Dateiklassifizierungseigenschaften auf bestimmte Dateien anwenden, können Sie über Dateiverwaltungsaufgaben festlegen, was der Server mit den gefundenen Dateien machen soll. Diese Aufgaben spielen allerdings für das Zusammenspiel mit SharePoint eine untergeordnete Rolle. Über das Kontextmenü von Dateiklassifizierungsaufgaben legen Sie eine neue Aufgabe an. Auf verschiedenen Registerkarten steuern Sie wieder den Ablauf:

1. Auf der Registerkarte *Allgemein* legen Sie den Namen sowie den Bereich fest, auf den die Aufgabe angewendet werden soll.
2. Auf der Registerkarte *Bereich* legen Sie den Ordner oder das Laufwerk fest, welchen bzw. welches Sie mit der Aufgabe verwalten wollen.
3. Auf der Registerkarte *Aktion* legen Sie schließlich fest, was die Aufgabe durchführen soll. Sie können zum Beispiel abgelaufene Dateien, also Dateien die schon lange nicht mehr im Einsatz sind, archivieren oder löschen. Oder Sie können benutzerdefinierte Skripts hinterlegen, zum Beispiel bestimmte Rechte setzen oder Dateien in andere Ordner verschieben.
4. Auf der Registerkarte *Bedingung* legen Sie fest, auf welche Dateien die Aktion der Registerkarte *Aktion* angewendet werden sollen. Zusätzlich legen Sie auf der Registerkarte *Bedingung* noch die Tage fest, nach deren Grenzwerte die Aktion auf der Registerkarte *Aktion* durchgeführt werden soll, zum Beispiel wenn Sie die Archivierung nach der Aktion *Dateiablauf* festlegen wollen.
5. Auf der Registerkarte *Zeitplan* legen Sie fest, wann die Aufgabe starten soll. Über das Kontextmenü können Sie eine Aufgabe auch sofort starten.

Abbildg. 21.14 Konfigurieren einer Dateiverwaltungsaufgabe



Haben Sie Dokumente auf dem Dateisystem mit Metadaten versorgt, können Sie über die *Inhaltsorganisation* Regeln festlegen, welche die Dokumente auf Basis der hinterlegten Metadaten in speziellen Ordnern speichert. Dazu müssen Sie lediglich zusätzliche Regeln für den Inhalt erstellen und diese an die Metadaten der Klassifizierungsverwaltung anbinden.

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).

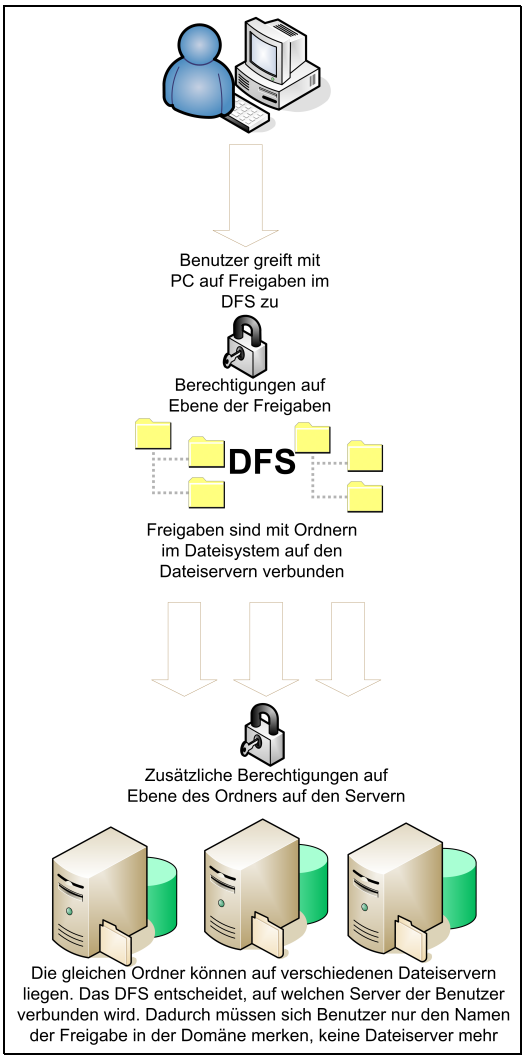
Einführung und wichtige Informationen beim Einsatz von DFS

In einem DFS wird eine logische Struktur über physische Ordner entwickelt, die auf einem oder mehreren Servern liegen können. Windows Server 2012 R2 unterstützt zwei Varianten des DFS. Der Domänen-DFS-Stamm verwendet Active Directory, um die Struktur- und Konfigurationsinformationen für das DFS zu speichern.

Einfach ausgedrückt bietet das DFS die Möglichkeit, Freigaben zu definieren, die auf unterschiedlichen Dateiservern liegen. Anwender müssen nicht 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.

Für ein Domänen-DFS muss der Server, auf dem der Konsolenstamm bereitgestellt ist, ein Domänencontroller oder ein Mitgliedsserver einer Active Directory-Domäne sein. Wichtig ist, dass bei Domänen-DFS mehrere DFS-Roots auf einem Server gehostet werden können.

Abbildg. 21.15 DFS im Praxiseinsatz



Über das DFS selbst steuern Sie keine Zugriffsberechtigungen. Die Rechte von Benutzern legen Sie vielmehr über die Dateisysteme fest. DFS-Verknüpfungen sind Ordner im DFS-Baum, die auf eine Freigabe verweisen. Wenn eine DFS-Verknüpfung *Excel-Dateien* angelegt ist, 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 Unterordner des Ordners *Budgets* zugreifen.

Bei der Erstellung einer DFS-Verknüpfung geben Sie den Namen ein, unter dem die Freigabe im DFS erscheinen soll. Mit dieser Freigabe wird ein freigegebener Ordner verbunden. Die DFS-Root 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, Remoteunterschiedskomprimierung) 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 Sie freigegebene Ordner, die sich auf unterschiedlichen Servern befinden, zusammenfassen und den Benutzern als virtuelle Ordnerstruktur, den sogenannten 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.

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

- 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. 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.
- 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 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 Eingabeaufforderung *dfsradmin* ein, erhalten Sie ausführliche Informationen über die Syntax.

- 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 Prestaging 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 Remoteunterschiedskomprimierung (RDC) nur die Änderungen, die seit dem Prestaging der Daten aufgetreten sind.

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 bereits gespeichert wurden, die später gefiltert werden sollen. Die Dateiprüfung entdeckt nur, wenn neue Dateien abgelegt werden, bereits vorhandene Dateien werden nicht blockiert.

Auf jeden Fall sollten Sie sicherstellen, dass kein Ordner 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 Ordner 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 sein. Zunächst benötigen Sie Active Directory, da nur unter dem Betrieb eines DFS-Stamms in Active Directory die Struktur sinnvoll ist. Des Weiteren benötigen Sie idealerweise Dateiserver unter Windows Server 2012 R2.

Sie können das DFS auch so einrichten, dass mehrere Dateiserver ihre Daten miteinander replizieren. Dazu verwendet 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 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 DFS dafür sorgt, dass die Daten von und zu den Niederlassungen repliziert werden.

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 eine DFS-Root 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-Rootserver.

Sie können für jede DFS-Verknüpfung, also jede Freigabe, die in DFS hinterlegt ist, mehrere 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.

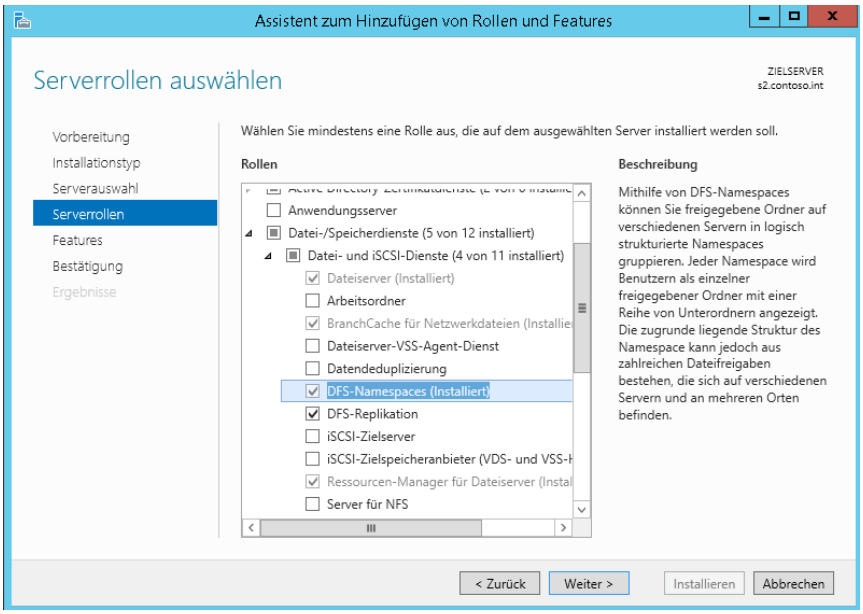
Installation und Einrichtung von DFS

Wollen Sie im Unternehmen DFS einsetzen, müssen Sie das Schema Ihrer Gesamtstruktur auf Windows Server 2008 aktualisieren, besser auf Windows Server 2008 R2. DFS installieren Sie am besten über den Server-Manager und die Rolle *Datei- und Speicherdienste/Datei- und iSCSI-Dienste*.

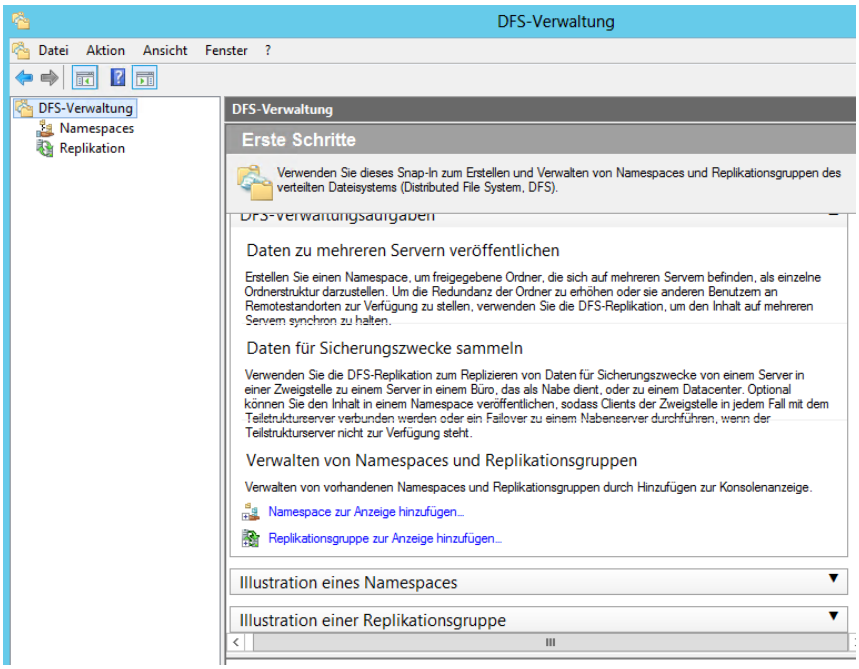
Stellen Sie sicher, dass die Rollendienste *DFS-Namespace* und *DFS-Replikation* installiert sind. Überprüfen Sie nach der Installation, ob die Systemdienste *DFS-Replikation* und *DFS-Namespace* auf *Automatisch* gesetzt und gestartet sind.

Nachdem Sie die notwendigen Rollendienste installiert haben, können Sie das Snap-In *DFS-Verwaltung* über das Tool im Server-Manager starten. Alternativ starten Sie die Verwaltungsoberfläche über *dfsmgmt.msc*. Die Verwaltungsoberfläche dient zur Konfiguration und Verwaltung sowohl des DFS-Namespace als auch der DFS-Replikation.

Abbildg. 21.16 Installieren von DFS



Abbildg. 21.17 Konfigurieren von DFS mit der DFS-Verwaltung



Sie können DFS auch auf Core-Servern installieren. Wie Sie dabei vorgehen, lesen Sie in Kapitel 3 und 4.

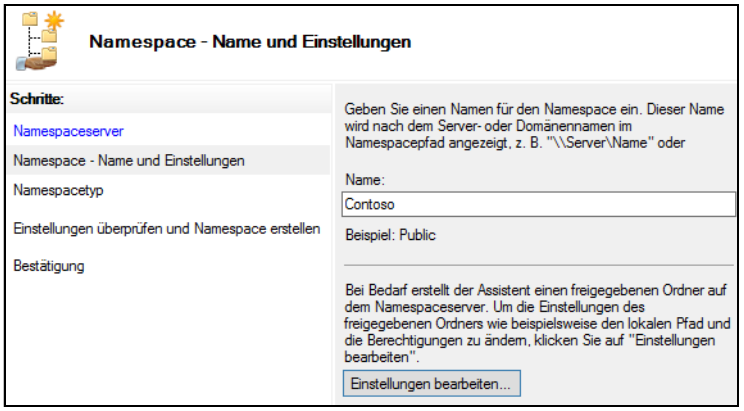
Einrichten eines DFS-Namespace

Die Einrichtung eines DFS-Namespace nehmen in der DFS-Verwaltung vor. 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 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 Sie 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.
3. Im nächsten Dialogfeld wählen Sie den Namen für den neuen Namespace aus.
4. Der Namespacestamm ist der Ausgangspunkt des Namespace.

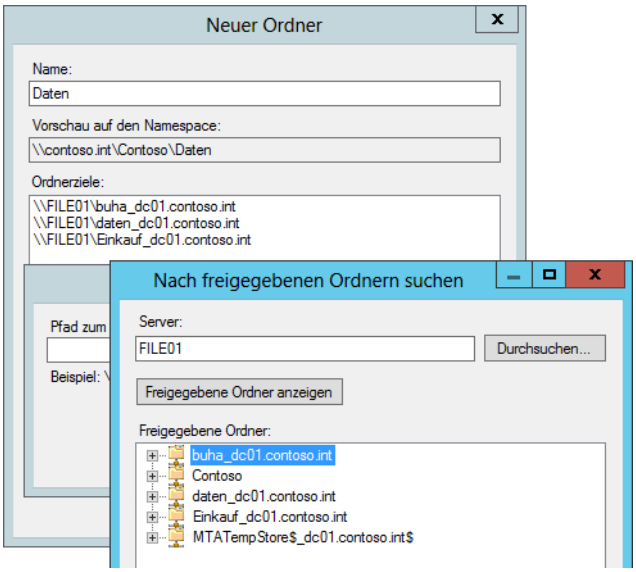
Abbildg. 21.18 Erstellen eines neuen DFS-Namespace



5. 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.
6. Nachdem Sie die Daten eingegeben haben, können Sie den Namespace erstellen lassen, der anschließend in der DFS-Verwaltung angezeigt wird. Sie können zur Ausfallsicherheit jederzeit dem Namespace weitere Namespaceserver hinzufügen. Dies allerdings nur dann, wenn Sie einen domänenbasierten Namespace erstellt haben. Klicken Sie zum Hinzufügen mit der rechten Maustaste auf den erstellten Namespace.

7. Klicken Sie anschließend mit der rechten Maustaste auf den neuen Namespace und wählen Sie *Neuer Ordner* aus. Danach können Sie einen neuen Ordner erstellen, auf den die Anwender zugreifen. Ordnerziele verweisen auf physische Freigaben auf Servern. 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. 21.19 Erstellen von neuen Ordnern mit Ordnerzielen



Anschließend verbindet DFS den erstellten virtuellen Ordner mit den tatsächlich vorhandenen Freigaben auf den verschiedenen Servern. Der nächste Schritt besteht in der Konfiguration von Verweisen.

Haben Sie den Namespace erstellt, können Anwender auf Daten zugreifen, indem Sie \\<*Active Directory-Domäne*\<*Name des Namespace*> eingeben. In der Freigaben erscheinen alle Ordner, die Sie angelegt haben. Der virtuelle DFS-Ordner zeigt den Inhalt der festgelegten Ordnerziele an. Die Anwender müssen dazu nicht die tatsächlichen Server oder die Namen der Freigabe kennen.

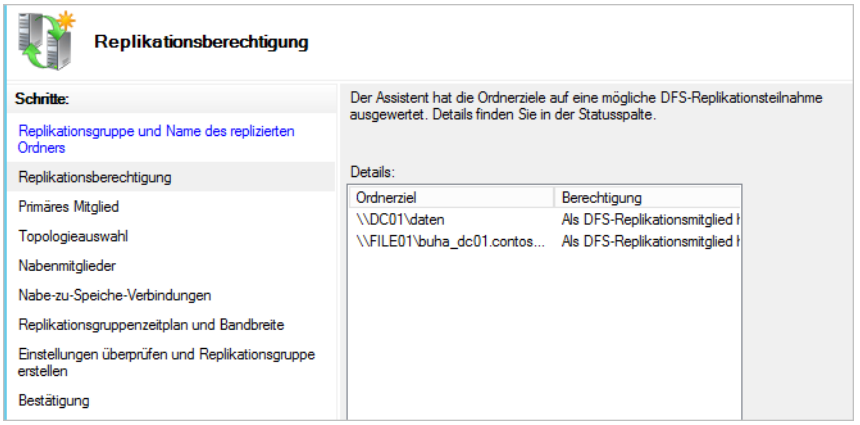
Einrichten der DFS-Replikation

Wollen Sie den Inhalt von physischen 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. Über die Technologie kann DFS die Daten in den Freigaben zwischen den Ordnerzielen in einem DFS-Ordner replizieren.

Auf der ersten Seite legen Sie den Namen der Replikationsgruppe fest. Eine Replikationsgruppe besteht aus einer Reihe von Servern, die an der Replikation eines replizierten Ordners beteiligt sind. Der Name der Replikationsgruppe stimmt mit dem Namespacepfad überein und der Name des replizierten Ordners mit dem Ordnernamen in der DFS-Verwaltung.

Auf der nächsten Seite werden die Freigaben und die dazugehörigen Server angezeigt, deren Freigaben repliziert werden.

Abbildg. 21.20 Einrichten der DFS-Replikation



Als Nächstes wählen Sie das primäre Mitglied der Replikationsgruppe aus. Bestimmen Sie hier den Server, der den aktuellsten Inhalt enthält. Im Anschluss legen Sie fest, welche Replikationstopologie Sie verwenden wollen. Die Definitionen der Replikationstopologien sind selbsterklärend.

Auf der nächsten Seite definieren Sie die Bandbreite oder den Zeitplan für die Replikation. 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.

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.

Klicken Sie auf eine Replikationsverbindung, können Sie in der Mitte der Konsole über vier Registerkarten die Einstellungen der Replikationsgruppe anpassen. Auf diesen Registerkarten werden unterschiedliche Details zur ausgewählten Replikationsgruppe, ihren Mitgliedern und ihren replizierten Ordnern angezeigt.

Zusammenfassung

In diesem Kapitel sind wir auf die Verwaltungsmöglichkeiten von Dateiservern mit dem Ressourcen-Manager für Dateiserver eingegangen. Mit diesem Werkzeug können Sie die Freigaben im Netzwerk effizient mit Kontingenten, Dateiprüfungen und Klassifizierungen verwalten. Ebenfalls Bestandteil des Kapitels war das verteilte Dateisystem in Windows Server 2012 R2 (DFS).

Im nächsten Kapitel beschäftigen wir uns mit der BranchCache-Funktion von Windows Server 2012 R2. Mit dieser Funktion können Windows 7/8-Rechner in Niederlassungen wesentlich schneller auf Dateifreigaben in der Zentrale zugreifen.

Kapitel 22

BranchCache

In diesem Kapitel:

Windows 7/8/8.1 zusammen mit Windows Server 2012 R2 ermöglicht einen schnelleren Zugriff zu Dateien in Freigaben von Dateiservern. Dies auch dann, wenn die Verbindung durch langsame WAN-Leitungen erfolgt. Damit BranchCache optimal funktioniert, muss auf den beteiligten Webservern und Dateiservern Windows Server 2012 R2 betrieben werden, nicht beteiligte Server können Sie auch mit Windows Server 2008/2008 R2/2012 betreiben.

Für die Bereitstellung von BranchCache in Organisationen unterschiedlicher Größe benötigen Sie in Windows Server 2012 R2 und Windows 8/8.1 nur ein einziges GPO. Es sind keine verschiedenen Einstellungen mehr für unterschiedliche Niederlassungen notwendig. Clients können Sie mit Gruppenrichtlinien standardmäßig als verteilte Cachemodusclients konfigurieren. Die Computer suchen aber nach einem gehosteten Cacheserver. Ist ein solcher verfügbar, werden Clients automatisch als gehostete Cachemodusclients konfiguriert. Diese Funktion ist neu in Windows 8/8.1 und Windows Server 2012 R2.

Mit Windows Server 2008 R2/2012 konnten Sie nur einen gehosteten Cacheserver pro Filiale bereitstellen. Mit Windows Server 2012 R2 können Sie so viele gehostete Cacheserver wie benötigt bereitstellen. BranchCache verwendet die Datenbanktechnologie Extensible Storage Engine (ESE) von Microsoft Exchange Server. Das macht die Speicherung der Daten wesentlich stabiler.

In Windows Server 2012 R2 sind keine Serverzertifikate mehr erforderlich. Wir zeigen Ihnen in diesem Kapitel aber dennoch, wie Sie Zertifikate bereitstellen können.

TIPP BranchCache können Sie jetzt auch umfassend in der PowerShell verwalten. Die entsprechenden Befehle erhalten Sie durch Eingabe von *Get-Command *bc** und auf der Seite *http://technet.microsoft.com/library/hh848392.aspx* [Ms179-K22-01].

BranchCache im Überblick – Niederlassungen effizient anbinden

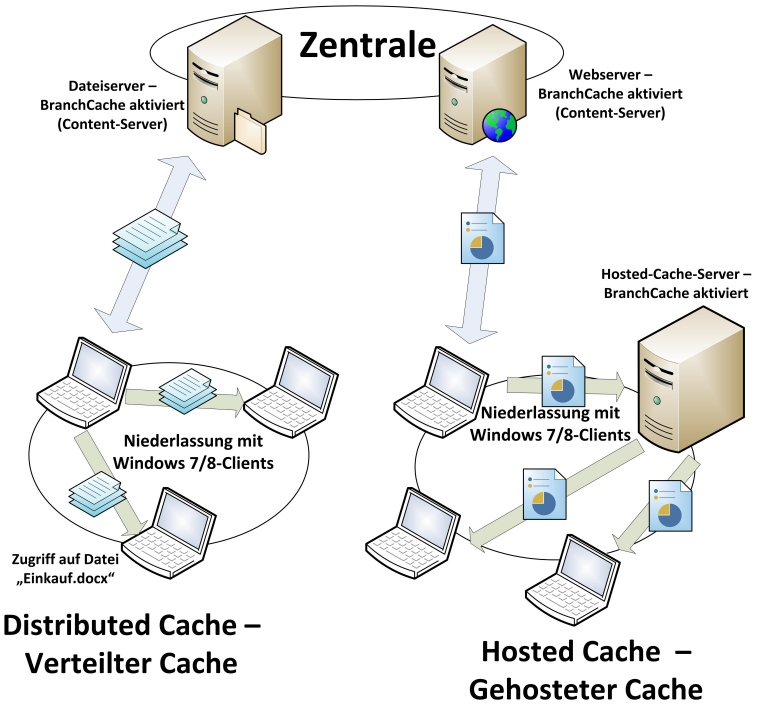
Windows 7/8/8.1 kann über das Netzwerk kopierte Dateien automatisch auf der Festplatte zwischenspeichern. Beim erneuten Zugriff auf die gleiche Datei muss Windows 7/8/8.1 nur noch neue Daten laden, alles, was schon mal übertragen wurde, bleibt auf der Festplatte im Cache, gesichert durch Zugriffsberechtigungen, gespeichert.

Ändern sich an der Quelle Dateien, überträgt Windows 7/8/8.1 nicht die kompletten geänderten Dateien erneut, sondern nur die Blöcke, die sich geändert haben. Das gilt auch für den Zugriff über DirectAccess oder andere VPN-Szenarien und in allen Konfigurationen von BranchCache. Alleine dadurch beschleunigt sich der Datenzugriff enorm. Diese Technik funktioniert auch ohne Windows Server 2012 R2.

Setzen Unternehmen aber auch noch die neue Version des Windows-Servers ein, erhalten diese weitere Vorteile. Windows Server 2012 R2 unterstützt ebenfalls BranchCache. Die beiden Betriebssysteme können diese Technik miteinander verbinden. Ruft ein Client mit Windows 7/8/8.1 in einer Niederlassung Daten von der Zentrale ab, speichert der durch BranchCache aktivierte Dateiserver in der Niederlassung die Daten zwischen. Ruft ein weiterer Client die gleichen Daten ab, stellt der Dateiserver diesem Client die zwischengespeicherten Daten zur Verfügung, sodass diese nicht erneut über das Netzwerk übertragen werden müssen. Das beschleunigt den Zugriff enorm und spart Bandbreite im WAN ein, die für andere Anwendungen zur Verfügung steht.

BranchCache unterstützt für die Übertragung der Daten verschiedene Sicherheitstechniken. Neben IPv4 und IPv6, lassen sich Datenzugriffe per SSL oder IPsec absichern. Auch die Autorisierung findet in einem solchen Szenario beschleunigt statt. Diese Technik ist natürlich verschlüsselt.

Abbildg. 22.1 BranchCache im Überblick



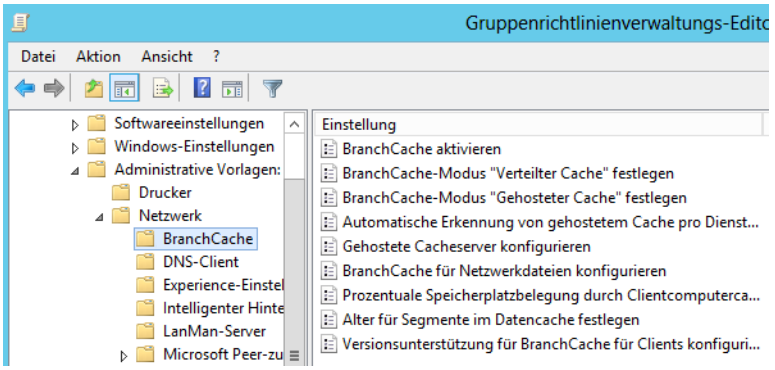
Gehosteter Cache (Hosted Cache) nutzen

BranchCache lässt sich in den beiden Betriebsmodi Hosted Cache und Distributed Cache betreiben. Bei Hosted Cache stellen Unternehmen in der Niederlassung, in der Windows 7/8/8.1-Computer installiert sind, einen Host zur Verfügung, der die Daten vom zentralen Dateiserver über die WAN-Leitung zwischenspeichern kann.

Befindet sich also in einer Niederlassung mit Windows 7/8/8.1-Computer noch ein Server mit Windows Server 2012 R2, lassen sich auf diesem Server über Hosted Cache zentral Daten zwischenspeichern, sodass der Zugriff von allen Clientcomputern unter Windows 7/8/8.1 aus enorm beschleunigt wird, ohne dass die Sicherheit darunter leidet. Die Computer greifen dann auf den Host in der Niederlassung zu, um Daten der Zentrale abzurufen. Benötigen Clients Daten, die noch nicht auf dem Hosted-Cache-Server liegen, ruft dieser die Daten vom Content-Server, dem Datei- oder Webserver in der Zentrale ab. Der erste Zugriff der Clients ist dadurch etwas langsamer, weitere Zugriffe laufen aber deutlich schneller ab.

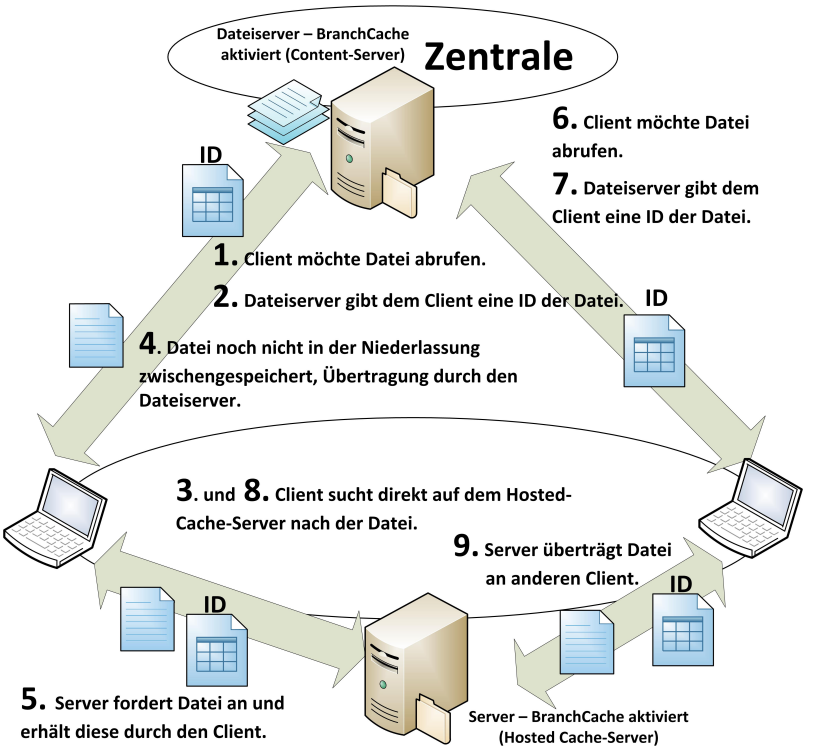
Die Konfiguration dieser Technik erfolgt in den Gruppenrichtlinien. Sie finden die Einstellungen unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Netzwerk*. Über *LanMan-Server* nehmen Sie Einstellungen für die Server vor. Die Clientkonfiguration nehmen Sie über *BranchCache* vor.

Abbildg. 22.2 Konfiguration von BranchCache über Gruppenrichtlinien mit Windows Server 2012 R2



HINWEIS Eine Hosted-Cache-Konfiguration ist unabhängig von Active Directory-Standorten und wird über Gruppenrichtlinien gesteuert. In den Gruppenrichtlinieneinstellungen legen Sie fest, ab welcher Netzwerkgeschwindigkeit Clients BranchCache nutzen sollen. Die ganze Konfiguration ist vollkommen unabhängig von der Active Directory-Infrastruktur.

Abbildg. 22.3 BranchCache mit Hosted-Cache-Server betreiben



Hosted Cache – Gemeinsamer Cache

Microsoft empfiehlt die Konfiguration über eine eigene Richtlinie. Über Richtlinien lassen sich auch genauere Einstellungen für die Energieverwaltung einstellen, wenn Sie Windows Server 2012 R2 zusammen mit Windows 7/8/8.1 betreiben.

Mit der Gruppenrichtlinieneinstellung *Hashversionsunterstützung für BranchCache* können Sie angeben, ob Hashes der Version 1 (V1), der Version 2 (V2) oder V1- und V2-Hashes im Einsatz sind. Hashes werden auf Basis der Daten in freigegebenen Ordnern, für die BranchCache aktiviert ist, erstellt. Durch V2-Inhaltsinformationen werden kleinere Datenblöcke mit variabler Größe beschrieben und größere Einsparungen von WAN-Bandbreite ermöglicht. V1-Hashes sind mit Windows 7 und Windows Server 2008 R2/2012 kompatibel, V2-Hashes mit Windows 8/8.1 und Windows Server 2012 R2.

Mit der neuen Richtlinieneinstellung *Alter für Segmente im Datencache festlegen* können Sie den Zeitraum in Tagen angeben, für den Segmente im BranchCache-Datencache auf Clientcomputern gültig sind. Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird ein Standardalter von 28 Tagen festgelegt.

Mit *Unterstützung für die BranchCache-Clientversion konfigurieren* können Sie angeben, ob BranchCache-fähige Clientcomputer in einem herabgestuften Modus betrieben werden. Wenn Sie diese Richtlinieneinstellung aktivieren, wird auf allen Clients die Version von BranchCache verwendet, die Sie in den Richtlinienoptionen angegeben haben.

Über *Gehostete Cacheserver konfigurieren* bestimmen Sie, ob Clientcomputer für die Verwendung des gehosteten Cachemodus konfiguriert werden. Zusätzlich können Sie die Computernamen der gehosteten Cacheserver angeben. Im gehosteten Cachemodus kann durch Clientcomputer Inhalt von einem oder mehreren gehosteten Cacheservern abgerufen werden, die in derselben Filiale installiert sind. Mit dieser Einstellung können Sie Clientcomputer automatisch konfigurieren, die für den gehosteten Cachemodus mit Computernamen der gehosteten Cacheserver in der Filiale konfiguriert sind. Damit diese Richtlinieneinstellung wirksam wird, müssen Sie auch die Richtlinieneinstellung *BranchCache aktivieren* auswählen. Diese Richtlinieneinstellung kann nur auf Clientcomputer angewendet werden, auf denen Windows 8/8.1 installiert ist. Diese Richtlinie hat keine Auswirkungen auf Computer, auf denen Windows 7 oder Windows Vista installiert ist.

Mit *Automatische Suche nach gehosteten Cacheservern pro Dienstverbindungspunkt aktivieren* werden Clientcomputer so konfiguriert, dass diese mit Active Directory nach gehosteten Cacheservern suchen. Es werden die gefundenen Server und der gehostete Cachemodus und nicht die manuelle BranchCache-Konfiguration oder die BranchCache-Konfiguration durch andere Gruppenrichtlinien verwendet. Wenn Sie diese Richtlinieneinstellung zusätzlich zu der Richtlinieneinstellung *BranchCache aktivieren* setzen, wird durch BranchCache-Clients in der lokalen Filiale nach gehosteten Cacheservern gesucht. Wenn gehostete Cacheserver gefunden werden, wird der gehostete Cachemodus aktiviert. Werden keine gehosteten Cacheserver gefunden, wird der gehostete Cachemodus nicht aktiviert und eine andere manuell oder durch eine Gruppenrichtlinie festgelegte Konfiguration verwendet.

Wenn die Richtlinieneinstellung *BranchCache-Modus „Gehosteter Cache" festlegen* angewendet wird, erfolgt keine automatische Suche nach gehosteten Cacheservern. Dies gilt auch für die Richtlinieneinstellung *Gehostete Cacheserver konfigurieren*. Diese Richtlinieneinstellung kann nur auf Clientcomputer angewendet werden, auf denen Windows 8/8.1 installiert ist. Diese Richtlinie hat keine Auswirkungen auf Computer, auf denen Windows 7 oder Windows Vista installiert ist. Wenn Sie diese Einstellung deaktivieren oder nicht konfigurieren, erfolgt keine Suche nach gehosteten Cacheservern anhand von Dienstverbindungspunkten.

Mit *BranchCache aktivieren* können Sie festlegen, ob BranchCache auf Clientcomputern aktiviert wird. Zusätzlich müssen Sie angeben, ob es sich bei den Clientcomputern um gehostete Cachemodus- oder verteilte Cachemodusclients handelt. Konfigurieren Sie dazu die folgenden Richtlinieneinstellungen:

- *BranchCache-Modus "Verteilter Cache" festlegen*
- *BranchCache-Modus "Gehosteter Cache" festlegen*
- *Gehostete Cacheserver konfigurieren*

Im verteilten Cachemodus wird durch Clientcomputer Inhalt von BranchCache-fähigen Inhaltsservern in der Zentrale heruntergeladen, der Inhalt lokal zwischengespeichert und anderen Clients im verteilten BranchCache-Cachemodus in der Filiale zur Verfügung gestellt.

Wenn Clientcomputer als Clients im gehosteten Cachemodus konfiguriert sind, kann zwischengespeicherter Inhalt von einem gehosteten Cacheserver in der Filiale heruntergeladen werden. Beim Abrufen von Inhalt von einem Inhaltsserver durch die gehosteten Cacheclients kann der Inhalt außerdem auf die gehosteten Cacheserver hochgeladen werden, damit der Inhalt für andere gehostete Cacheclients in der Filiale verfügbar ist.

Auf dem Server in der Niederlassung müssen Sie im Server-Manager das Feature *BranchCache* installieren (Seite *Features auswählen*), damit dieser mit den anderen Clients der Niederlassung und den zentralen Dateiservern zusammenarbeiten kann.

In den Gruppenrichtlinien legen Sie genau fest, wie viel Bandbreite zur Verfügung stehen muss, damit das Feature Daten zwischenlagert. Ist das Netzwerk zu langsam, soll es durch solche Funktionen natürlich nicht ausgebremst werden.

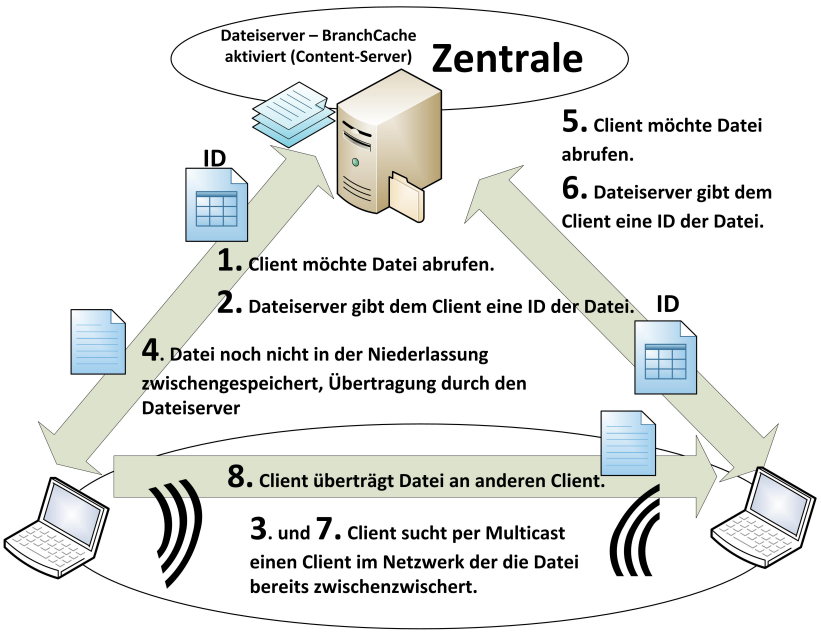
Auf dem zentralen Dateiserver installieren Sie dazu noch den Rollendienst *BranchCache für Netzwerkdateien*, der zur Rolle *Datei- und iSCSI-Dienste* gehört. Installieren Sie diesen Rollendienst, müssen Sie das bereits erwähnte Feature nicht installieren. Erst nach der Installation des Rollendiensts lässt sich BranchCache für Freigaben aktivieren. Um einen Hosted-Cache-Server in einer Niederlassung zu betreiben, müssen Sie keinen dedizierten Server zur Verfügung stellen, es muss sich nur um einen Server mit Windows Server 2012 R2 handeln, zum Beispiel auch einen Domänencontroller in der Niederlassung. Der Ablauf dabei ist recht einfach:

1. Ein Client ruft vom zentralen Dateiserver eine Datei ab oder einen aktualisierten Teil einer Datei, wenn sich diese bereits im Cache befinden sollte.
2. Das Dokument wird vom zentralen Dateiserver auf den Client übertragen. Dabei authentifiziert der zentrale Dateiserver, in diesem Szenario der Content-Server, den Anwender und seinen Computer im Active Directory.
3. Der Client überprüft auf Basis des Hashes, ob der Teil der Datei oder die Datei selbst schon auf dem Hosted-Cache-Server der Niederlassung liegt.
4. Der Hosted-Cache-Server verbindet sich mit dem Client und überträgt über einen gesicherten Kanal fehlende Daten auf den Server. Die Daten werden dabei über AES 128 verschlüsselt.
5. Benötigt ein anderer Client der Niederlassung das gleiche Dokument, ruft der Client dieses automatisch vom Hosted-Cache ab. Die Authentifizierung findet aber über den zentralen Server, den Content-Server statt.

Verteilter Cache (Distributed Cache) nutzen

In kleineren Niederlassungen in denen Unternehmen keinen eigenen Server, aber Clients mit Windows 7/8/8.1 betreiben wollen, können Sie auch den Distributed Cache verwenden. Bei diesem Modus gibt es keinen Hostserver in der Niederlassung, sondern Windows 7/8/8.1-Clients rufen Daten ab und speichern diese lokal zwischen. Andere Windows 7/8/8.1-Clients in der Niederlassung können auf die Daten zugreifen, sodass auch hier einmal abgerufene Daten deutlich effizienter und schneller zur Verfügung stehen.

Abbildg. 22.4 Verteilten Cache nutzen



Distributed Cache – Verteilter Cache

So lässt sich die Positionierung von Servern in der Niederlassung vermeiden und BranchCache dennoch nutzen. Diese Technik funktioniert aber nur innerhalb eines einzelnes Subnetzes. Wird ein Client, der den Inhalt bereitstellt, heruntergefahren, stehen die Daten natürlich nicht zur Verfügung. Braucht ein anderer Client diese Daten, müssen diese erneut über das WAN übertragen werden.

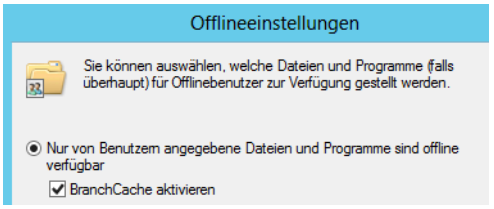
HINWEIS Arbeiten Sie mit Distributed-Cache, tauschen die Windows 7/8/8.1-Clients zwischengespeicherte Dateien über das HTTP-Protokoll aus. Dazu müssen Sie sicherstellen, dass auf den Clients die Firewalleinstellungen BranchCache zulassen und den HTTP-Verkehr sowie das WS-Discovery-Protokoll nicht blockieren. Diese Einstellung nehmen Sie entweder lokal auf den Rechnern vor oder besser über eine Gruppenrichtlinie.

Standardmäßig verwendet Windows Server 2012 R2 nicht für alle Freigaben BranchCache, Sie können die Einstellung für jede Freigabe getrennt vornehmen:

1. Rufen Sie dann die Eigenschaften der Freigabe auf, für die Sie BranchCache aktivieren wollen:
2. Über die Schaltfläche *Erweitert* und die Registerkarte *Zwischenspeichern* steuern Sie den BranchCache-Zugriff der Anwender.

Bei der Übertragung teilt der BranchCache die Daten in Blöcken auf und erstellt für jeden Block einen Hashwert. Beim Übertragen der Daten komprimiert der Server die Blöcke, wobei die Datenmenge enorm reduziert werden kann.

Abbildg. 22.5 Konfiguration von BranchCache in den erweiterten Eigenschaften einer Freigabe



Sie können die Funktion aber erst dann aktivieren, wenn Sie den bereits erwähnten Rollendienst installiert haben, ansonsten ist die Funktion deaktiviert. Bei Distributed Cache und mehreren Windows 7/8/8.1-Computern in der Niederlassung arbeiten die Clients mit dem Web Services Discovery Multicast-Protokoll, um im Subnetz abzufragen, ob ein Windows 7/8/8.1-Client die benötigten Daten bereits lokal gespeichert hat.

Abbildg. 22.6 Konfiguration von BranchCache über die Eingabeaufforderung mit Netsh

```
PS C:\Users\administrator.CONTOSO> netsh branchcache

Folgende Befehle sind verfügbar:

Befehle in diesem Kontext:
?               - Zeigt eine Liste der Befehle an.
dump            - Zeigt ein Konfigurationsskript an.
exportkey       - Exportiert den Schlüssel für die Informationen zum Inhalt.
flush           - Löscht den Cacheinhalt.
help            - Zeigt eine Liste der Befehle an.
importkey       - Importiert einen neuen Schlüssel für die Informationen
                  zum Inhalt.
reset           - Setzt den BranchCache-Dienst zurück.
set             - Legt Konfigurationsparameter fest.
show            - Zeigt Konfigurationsparameter an.
smb             - Wechselt zum "netsh branchcache smb"-Kontext.

Folgende Unterkontexte sind verfügbar:
 smb

Geben Sie den Befehl, gefolgt von einem Leerzeichen und ? ein, um Hilfe
bezüglich des entsprechenden Befehls zu erhalten.

PS C:\Users\administrator.CONTOSO> netsh branchcache show

Folgende Befehle sind verfügbar:

Befehle in diesem Kontext:
show hostedcache - Zeigt den Speicherort des gehosteten Caches an.
show localcache - Zeigt den Status des lokalen Caches an.
show publicationcache - Zeigt den Status des lokalen Veröffentlichungscaches an.
show status      - Zeigt den aktuellen Status des BranchCache-Diensts an.
PS C:\Users\administrator.CONTOSO> netsh branchcache show status


Status des BranchCache-Diensts:
-------------------------------------------------------------------------------
Dienstmodus      = Lokales Zwischenspeichern
Aktueller Status = Wird ausgeführt
```

Viele Einstellungen in BranchCache nehmen Sie über Gruppenrichtlinien vor. Sie können in der Eingabeaufforderung aber auch mit *netsh branchcache* verschiedene Einstellungen vornehmen und Informationen abrufen. In den folgenden Abschnitten zeigen wir Ihnen auch jeweils die Konfiguration von BranchCache über die Eingabeaufforderung. Geben Sie in der Eingabeaufforderung nur *netsh branchcache* ein, erhalten Sie eine Zusammenfassung angezeigt, welche Möglichkeiten Sie in der Eingabeaufforderung haben.

BranchCache auf dem Hosted-Cache-Server konfigurieren

Der Hosted-Cache-Server ist der BranchCache-Server, der in der Niederlassung positioniert ist und für die Clients in der Niederlassung die Daten zwischenspeichert. Er verbindet sich dazu mit dem Dateiserver in der Zentrale, um Daten abzurufen.

Feature für Hosted-Cache installieren

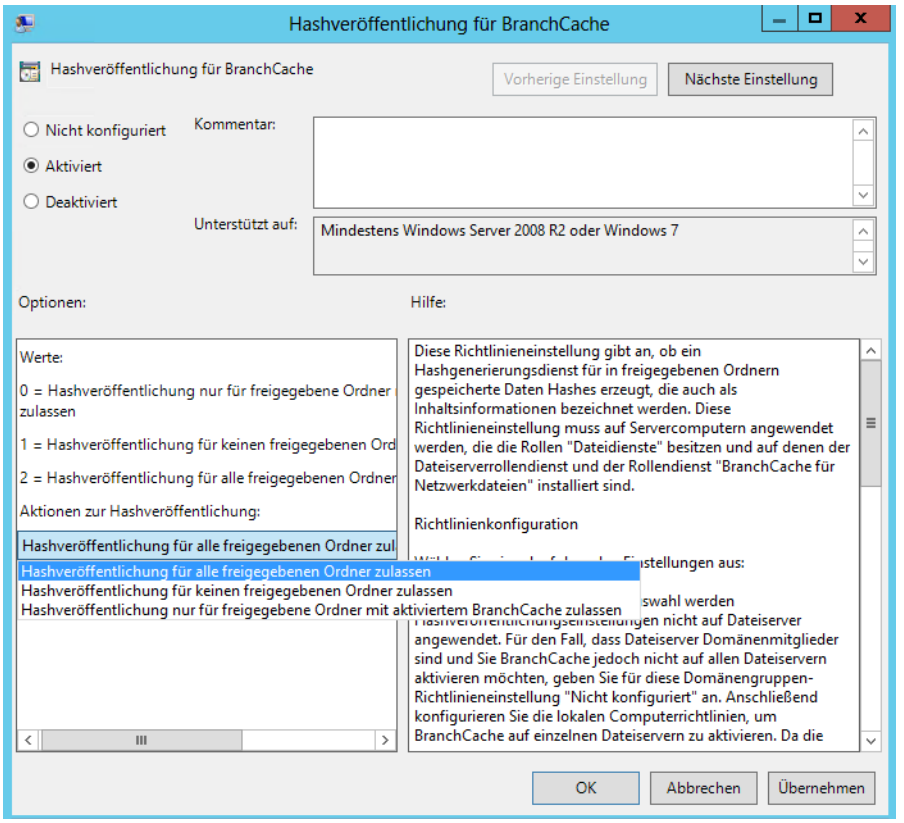
Auf dem Hosted-Cache-Server müssen Sie zunächst das Feature *BranchCache* installieren und den Server anschließend als Hosted-Cache-Server konfigurieren. Sie verwenden dazu den Server-Manager und die bereits erwähnte Seite *Features auswählen*. Die Einrichtung erfolgt über Gruppenrichtlinien. Sie können aber auch mit PowerShell-Skripts arbeiten. Die Einrichtung erfolgt dabei in mehreren Schritten:

1. Aktivierung von BranchCache unter Windows 7/8/8.1.
2. Auswahl des Modus, also Hosted-Cache oder Distributed-Cache.
3. Konfiguration der Cachegröße auf dem Client beim Einsatz von Distributed Cache. Standardmäßig verwendet Windows 7/8/8.1 fünf Prozent des lokalen Speicherplatzes.
4. Verwenden Sie Hosted-Cache, müssen Sie den Hosted-Cache-Server in der Niederlassung angeben.

HINWEIS Wollen Sie die lokalen Daten auf dem Server bei Hosted-Cache oder auf den Clients bei Distributed-Cache verschlüsseln, ist der Einsatz von BitLocker empfehlenswert. BitLocker arbeitet problemlos mit BranchCache zusammen, ohne dass Sie die beiden Technologien miteinander verbinden müssen. Es reicht aus, auf dem Server oder Client BitLocker zu aktivieren. Auch das verschlüsselnde Dateisystem (EFS) kann die lokalen Daten auf dem Server absichern (siehe Kapitel 5).

Die Einstellungen für Dateiserver in Gruppenrichtlinien finden Sie über *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Netzwerk*. Über *LanMan-Server* nehmen Sie Einstellungen für die Server vor. Die Clientkonfiguration nehmen Sie über *BranchCache* vor. Auf dem Dateiserver, der als Contentserver dient, aktivieren Sie die Einstellung *Hashveröffentlichung für BranchCache*.

Abbildg. 22.7 Konfigurieren von BranchCache auf dem Dateiserver (Contentserver)



Stellen Sie die Veröffentlichung nur für Freigaben ein, auf denen Sie manuell BranchCache aktivieren, müssen Sie beachten, dass Sie für Freigaben diese Einstellungen auch vornehmen müssen. Wie das geht, haben Sie auf den vorherigen Seiten erfahren. Arbeiten Sie mit einem Cluster, müssen Sie die Verschlüsselungsdaten zwischen den Clusterknoten replizieren lassen, damit der Zugriff von den Clients aus funktioniert. Dazu müssen Sie auf allen Clusterknoten eine Eingabeaufforderung mit Administratorrechten öffnen und den folgenden Befehl eingeben:

```
netsh branchcache set key passphrase=<Selbstdefinierter Schlüssel>
```

Welchen Schlüssel Sie verwenden, bleibt Ihre Sache. Sie müssen den Befehl auf allen Knoten eingeben.

Zertifikate auf dem Hosted-Cache-Server betreiben

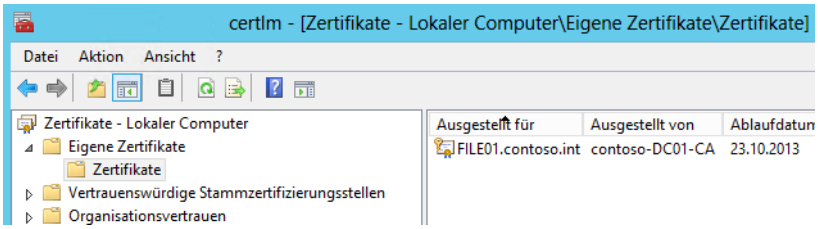
Die Kommunikation der Clients mit dem Hosted-Cache-Server wird für den Datenaustausch über Transport Layer Security (TLS) abgewickelt. Dabei arbeiten Clients und Server mit Zertifikaten. Auf

dem Hosted-Cache-Server muss in Windows Server 2008 R2/2012 und Windows 7 dazu ein Zertifikat zur Verfügung stehen, dem die Clients vertrauen. Das ist in Windows 8/8.1 und Windows Server 2012 R2 nur noch optional.

Am besten arbeiten Sie dazu mit einer internen Zertifizierungsstelle. Auf dem Hosted-Cache Server installieren Sie ein Serverzertifikat, dessen Zertifizierungsstelle die Clients in der Niederlassung vertrauen müssen. Haben Sie das Zertifikat installiert oder ein Zertifikat eines Drittherstellers erworben, muss dieses im lokalen Computerkonto auf dem Hosted-Cache-Server abgelegt sein. Um das zu überprüfen, gehen Sie folgendermaßen vor:

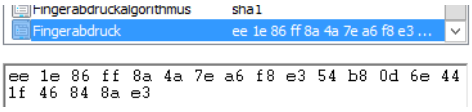
1. Geben Sie *certlm.msc* auf der Startseite ein.
2. Unter *Eigene Zertifikate/Zertifikate* muss das Zertifikat des Servers hinterlegt sein.
3. Ist das Zertifikat bereits vorhanden, klicken Sie doppelt auf das Zertifikat. Wie Sie Zertifikate ausstellen, lesen Sie in Kapitel 30.

Abbildg. 22.8 Überprüfen von Zertifikaten auf einem BranchCache-Server



4. Wechseln Sie zur Registerkarte *Details*.
5. Klicken Sie auf das Feld *Fingerabdruck* des Zertifikats.
6. Kopieren Sie den Wert in die Zwischenablage oder eine Textdatei.

Abbildg. 22.9 Kopieren des Fingerabdruckwerts eines Serverzertifikats



Sie benötigen diesen Wert des Fingerabdrucks, um das Zertifikat ordnungsgemäß mit BranchCache zu verbinden. Öffnen Sie dazu auf dem Hosted-Cache-Server eine Eingabeaufforderung mit Administratorrechten und geben Sie den folgenden Befehl ein:

```
NETSH HTTP ADD SSLCERT IPPORT=0.0.0.0:443 CERTHASH=<Fingerabdruck ohne Leerzeichen>
APPID={d673f5ee-a714-454d-8de2-492e4c1bd8f8}
```

Achten Sie darauf, an der entsprechenden Stelle alle Werte des Fingerabdrucks zu verwenden, aber die Leerzeichen zu entfernen. Ein Beispiel des Befehls wäre:

```
NETSH HTTP ADD SSLCERT IPPORT=0.0.0.0:443
CERTHASH=?9651f566c7d0e42679805a6df8688fe14646fc3a APPID={d673f5ee-a714-454d-8de2-
492e4c1bd8f8}
```

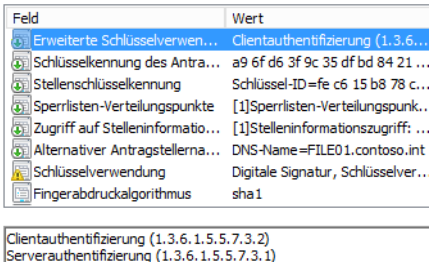
Abbildg. 22.10 Aktivieren des SSL-Zertifikats für BranchCache

```
C:\Users\administrator.CONTOSO>NETSH HTTP ADD SSLCERT IPPORT=0.0.0.0:443 CERTHAS
H=ee1e86ff8a4a7ea6f8e354b80d6e441f46848ae3 APPID={d673f5ee-a714-454d-8de2-492e4c
1bd8f8}

Das SSL-Zertifikat wurde erfolgreich hinzugefügt.
```

Mit dem Befehl *netsh http show urlacl* können Sie überprüfen, ob das Zertifikat korrekt mit der URL *https://+:443/C574AC30-5794-4AEE-B1BB-6651C5315029/* verbunden ist. Sie finden diese URL oft ganz unten im Fenster.

Klicken Sie doppelt auf das Serverzertifikat in der *Zertifikate*-Konsole, sehen Sie auf der Registerkarte *Details* im Bereich *Erweiterte Schlüsselverwendung*, ob das Zertifikat für Clientauthentifizierung und Serverauthentifizierung konfiguriert ist.

Abbildg. 22.11 Überprüfen der erweiterten Schlüsselverwendung



Achten Sie darauf, dass die Clients der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, vertrauen. Dazu muss das Zertifikat der Stammzertifizierungsstelle als vertrauenswürdig bei den Clients hinterlegt sein.

Einstellungen auf dem Hosted-Cache-Server anpassen

Standardmäßig verwendet der Hosted-Cache-Server ein Prozent des Speicherplatzes für BranchCache. Wollen Sie den Wert ändern, verwenden Sie den folgenden Befehl:

```
netsh branchcache set cachesize size=<Prozent> percent=true
```

Nehmen Sie die Einstellungen über Gruppenrichtlinien vor, können Sie den Wert nicht mehr über die Eingabeaufforderung anpassen. Konfigurieren Sie die Einstellungen nicht über eine Richtlinie, können Sie den Hosted-Cache auf dem Server auch mit dem Befehl *netsh branchcache set service mode=HOSTEDSERVER* aktivieren. Der Server nimmt standardmäßig auf den beiden Ports 80 und 443 Daten entgegen. Der Port 80 dient der Verbindung von Clients, die Daten vom Server abrufen wollen, der Port 443 dient dem Hochladen von Daten von anderen Clients in den Cache. Generell lassen sich diese Ports anpassen. Allerdings ist diese Anpassung nicht empfehlenswert, da Sie diese auf allen Clients manuell anpassen und Registrywerte ändern müssen.

TIPP Mit dem Befehl *netsh branchcache show status all* lassen Sie sich auf dem Hosted-Cache-Server die Einstellungen anzeigen. Hier sehen Sie, ob alle Werte korrekt hinterlegt sind.

Content-Server konfigurieren

Der Content-Server ist der Datei- oder Webserver in der Zentrale, auf dem Sie den Rollendienst und das Feature für BranchCache installiert, über Gruppenrichtlinien den Hashzugriff aktiviert und bei den Freigaben BranchCache auch aktiviert haben. Führen Sie auch auf dem Content-Server in der Eingabeaufforderung den Befehl *netsh branchcache show status all* aus, um dessen Konfiguration zu überprüfen.

Wie Sie die Einstellungen vornehmen, lesen Sie auf den vorangegangenen Seiten. Die Einstellungen für Server, die als Hosted-Cache-Server dienen, finden Sie in den Gruppenrichtlinien über *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Netzwerke*. Über *LanMan-Server* nehmen Sie Einstellungen für die Server vor. Die Clientkonfiguration nehmen Sie über *BranchCache* vor. Auf dem Dateiserver, der als Content-Server dient, aktivieren Sie die Einstellung *Hashveröffentlichung für BranchCache*. BranchCache aktivieren Sie dann über die Eigenschaften der Freigabe:

1. Rufen Sie die Eigenschaften der Freigabe auf, für die Sie BranchCache aktivieren wollen.
2. Klicken Sie auf der Registerkarte *Freigabe* auf die Schaltfläche *Erweitert*.
3. Wechseln Sie auf die Registerkarte *Zwischenspeichern*.
4. Aktivieren Sie das Kontrollkästchen *BranchCache*.

BranchCache auf Clients konfigurieren

Standardmäßig ist BranchCache auf Windows 7/8/8.1-Clients deaktiviert. Damit BranchCache im Netzwerk funktioniert, müssen Sie die Funktion auf den Servern aktivieren, für Freigaben aktivieren und anschließend die Clients im Netzwerk an die BranchCache-Infrastruktur anbinden.

Deaktivieren Sie den Netzwerkverkehr von BranchCache über die Firewalleinstellungen in Windows 7/8/8.1, können andere Clients im Netzwerk bei einer Distributed-Cache-Umgebung nicht auf die Daten des Rechners zugreifen. Arbeiten an dem Client aber verschiedene Benutzer, profitieren diese dennoch von BranchCache, allerdings nur lokal auf dem Rechner.

HINWEIS Ist die Niederlassung mit einem ISA/TMG-Server am Netzwerk angebunden, deaktivieren Sie auf dem Server den Compression-Filter. Ansonsten besteht die Möglichkeit, dass BranchCache nicht funktioniert, da dadurch der HTTP-Verkehr der beteiligten Komponenten gestört wird.

Clientkonfiguration mit Gruppenrichtlinien konfigurieren

Zur Aktivierung von BranchCache erstellen Sie am besten eine neue GPO und weisen diese den Clients zu, welche BranchCache nutzen sollen. Die Clientaktivierung finden Sie über die Einstellungen für Dateiserver und in den Gruppenrichtlinien finden Sie diese über *Computerkonfiguration/*

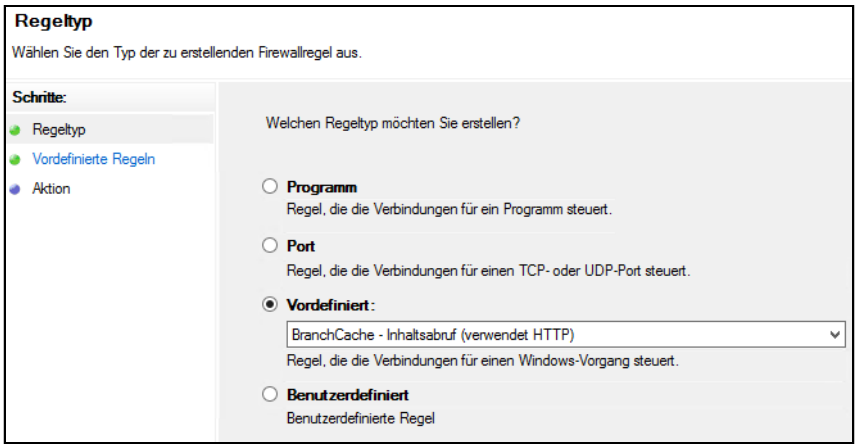
Richtlinien/Administrative Vorlagen/Netzwerk. Hier aktivieren Sie auch den unterstützten Modus und den freien Speicherplatz für BranchCache. Aktivieren Sie *BranchCache-Modus "Gehosteter Cache" festlegen*, müssen Sie über die Richtlinie auch den FQDN des Servers in der Niederlassung festlegen (Hosted-Cache-Server), der die Daten vom Dateiserver der Zentrale (Content-Server) abruft.

Firewalleinstellungen für BranchCache setzen

Damit BranchCache funktioniert, müssen Sie auf den Clients noch Firewalleinstellungen anpassen. Diese Einstellungen sind für den Modus *Distributed Cache* und den Modus *Hosted Cache* notwendig. Am besten verwenden Sie auch dazu eine Gruppenrichtlinie:

1. Sie finden die Einstellungen über *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Windows-Firewall mit erweiterter Sicherheit/Eingehende Regeln*.
2. Erstellen Sie über das Kontextmenü eine neue Regel.
3. Wählen Sie die Option *Vordefiniert*.
4. Wählen Sie als Regel *BranchCache – Inhaltsabruf (verwendet HTTP)* und schließen Sie die Erstellung der Regel ab.

Abbildg. 22.12 Erstellen einer neuen Firewallregel für BranchCache für Clients



Betreiben Sie BranchCache im Modus *Distributed Cache*, müssen Sie auf dem gleichen Weg eine weitere Regel erstellen. Wählen Sie als vordefinierte Regel *BranchCache – Peerermittlung (verwendet WSD)*. Über das WSD-Protokoll ermitteln Clients, ob eine benötigte Datei bereits auf einem Windows 7/8/8.1-Client im Netzwerk gespeichert ist. Diese Regel benötigt eine Kommunikation auf Port 3702, die Inhaltsübermittlung verwendet Port 80.

Clientkonfiguration mit Netsh

Neben der Möglichkeit über Gruppenrichtlinien können Sie auch mit der Eingabeaufforderung den Cachemodus bearbeiten und Einstellungen vornehmen.

HINWEIS Gruppenrichtlinieneinstellungen haben Vorrang vor Einstellungen, die Sie mit *netsh* vornehmen, und überschreiben die Einstellungen wieder, wenn sich diese überschneiden.

BranchCache für Distributed Cache aktivieren

Wollen Sie in der Niederlassung mit Distributed Cache arbeiten, verwenden Sie den Befehl:

```
netsh branchcache set service mode=DISTRIBUTED
```

Sind bereits Richtlinien gesetzt, erhalten Sie bei der Ausführung auf dem Client eine entsprechende Meldung. Geben Sie den Befehl ein, wird die Firewall auf dem Client bereits automatisch für die beiden erwähnten Firewallregeln aktiviert.

BranchCache für Hosted Cache aktivieren

Wollen Sie mit Hosted Cache in der Niederlassung arbeiten, verwenden Sie folgenden Befehl:

```
netsh branchcache set service mode=HOSTEDCLIENT LOCATION=<Server in Niederlassung der als
Hosted-Cache-Server funktioniert>
```

Auch dieser Befehl konfiguriert automatisch die Firewall auf dem Client.

Mit dem Befehl *netsh branchcache show status all* können Sie sich einen Status der Clientkonfiguration anzeigen lassen. Mit dem Befehl *netsh branchcache show hostedcache* lassen Sie sich den Hosted-Cache-Server anzeigen.

TIPP Mit dem Befehl *netsh branchcache flush* löschen Sie den lokalen Cache auf den Clientcomputern.

Die beiden neuen Technologien BranchCache und DirectAccess arbeiten zusammen. Setzen Sie im Unternehmen Windows Server 2012 R2 und Windows 7/8/8.1 in einem VPN ein, können Client-Rechner auf alle Funktionen im Netzwerk zugreifen, genauso wie beim internen Zugriff. Das hat zum Beispiel den Vorteil, dass auch Gruppenrichtlinien jetzt auf eingewählten VPN-Clients funktionieren, das war bisher noch nicht notwendig.

Damit dieser Zugriff funktioniert, muss der DirectAccess-Server im internen Netzwerk unter Windows Server 2012 R2 laufen. Dieser Server ist sozusagen der neue VPN-Server, den Sie im Netzwerk integrieren. Die Verbindung zwischen Client und Server funktioniert über ein IPsec-gesichertes virtuelles Privates Netzwerk (VPN). Die Kommunikation erfolgt dazu mittels IPv6 zwischen Windows 7/8/8.1 und dem DirectAccess-Server unter Windows Server 2012 R2.

Sobald sich der Client mit Netzwerk verbunden hat, kommuniziert dieser weiter mit IPv4, die IPv6-Verbindung endet aus Sicherheitsgründen am DirectAccess-Server. Verwenden Sie im Unternehmen IPv6, kann der IPsec-Datenverkehr natürlich auch im internen Netzwerk fortgeführt werden. Auf dem DirectAccess-Server legen Sie auch fest, auf welche internen Server der Zugriff erfolgen darf.

Zwischen den Clients, die BranchCache nutzen, muss der Port 3702 erlaubt sein, auch der Port 80 darf nicht blockiert werden. Für die Verschlüsselung verwenden die Clients und der Hosted-Cache-Server auch oft SSL und benötigen daher die Kommunikation über den Port 443.

Leistungsüberwachung und BranchCache

In Windows Server 2012 R2 finden Sie einige Erweiterungen für den Leistungsmonitor bezüglich BranchCache. Wollen Sie BranchCache überwachen, fügen Sie am besten alle Leistungsindikatoren hinzu und wechseln über die dritte Schaltfläche von links in den Modus *Bericht*. So erhalten Sie einen guten Überblick.

Den Leistungsmonitor starten Sie am schnellsten, wenn Sie *perfmon* auf der Startseite eingeben. Damit die Leistungsindikatoren verfügbar sind, müssen Sie das Feature *BranchCache* auf dem Server aktivieren. Mehr zu diesem Thema lesen Sie in Kapitel 38.

TIPP Mit dem Befehl *netsh branchcache show localcache* lassen Sie sich den Ordner und die Größe des Caches auf dem Server anzeigen. Mit *netsh branchcache show status all* können Sie sich über den aktuellen Status informieren.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie den Zugriff auf Dateien in Windows 7/8/8.1 und Windows Server 2012 R2 mit dem neuen BranchCache-Feature beschleunigen. Sie konnten in diesem Kapitel lesen, wie Sie die Einrichtung mit oder ohne einen zusätzlichen Server durchführen und welche Konfigurationen notwendig sind.

Im nächsten Kapitel gehen wir auf die Konfiguration eines Druckservers im Windows-Netzwerk ein.

Kapitel 23

Druckerserver

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, wie Sie Windows Server 2012 R2 als Druckerserver betreiben. Wir gehen auch darauf ein, wie Sie Smartphones und Tablet-PCs anbinden und Drucken auch mit diesen Geräten ermöglichen.

Wollen Sie einen Windows Server 2012 R2 auch als Druckerserver einsetzen, installieren Sie die Serverrolle *Druck- und Dokumentdienste* über den Server-Manager. In diesem Fall werden die notwendigen Verwaltungsprogramme installiert und in der Windows-Firewall die Ausnahmen für freigegebene Drucker eingetragen. Windows Server 2012 R2 ist standardmäßig mit einer Vielzahl von Druckertreibern ausgestattet, die auch in früheren Windows-Versionen einsetzbar sind. Damit ein Drucker im Netzwerk zur Verfügung gestellt wird, müssen Sie diesen zunächst auf dem Druckerserver installieren. Die Installation erfolgt dabei genauso wie die Installation eines lokalen Druckers auf einer Arbeitsstation.

Drucken im Netzwerk und mit Smartphones oder Tablet-PCs

Es gibt eine Vielzahl an Möglichkeiten, Drucker an das Netzwerk anzubinden und an die verschiedenen PCs, Smartphones oder Tablet-PCs anzubinden. Viele Drucker beherrschen WLAN und auch die Anbindung von PowerLine-Adapern, die Stromleitungen für das Netzwerk nutzen, sind ein möglicher Weg, um auch entfernte Drucker an Windows Server 2012 R2 anzubinden.

Drucker im Netzwerk zur Verfügung zu stellen, ist heutzutage kein Problem mehr. An PCs lassen sich Drucker schnell und einfach über Windows freigeben. Viele Drucker verfügen über eine eigene Netzwerkschnittstelle, die eine direkte Ansteuerung erlaubt. Dazu kommen noch Drucker mit WLAN-Fähigkeit.

Auch viele DSL-Router und Firewalls bieten mittlerweile die Möglichkeit, Drucker per USB anzubinden und im Netzwerk freizugeben. Das ist vor allem für kleine Unternehmen sehr wichtig. Wollen Sie Drucker im Netzwerk freigeben, muss zum Drucken dieser Computer angeschaltet sein. Einfacher ist es, Drucker direkt im Netzwerk zur Verfügung zu stellen, am besten mit einer eigenen Schnittstelle. Auch hier können Sie aber Drucker zusätzlich noch an Druckerserver mit Windows Server 2012 R2 anbinden.

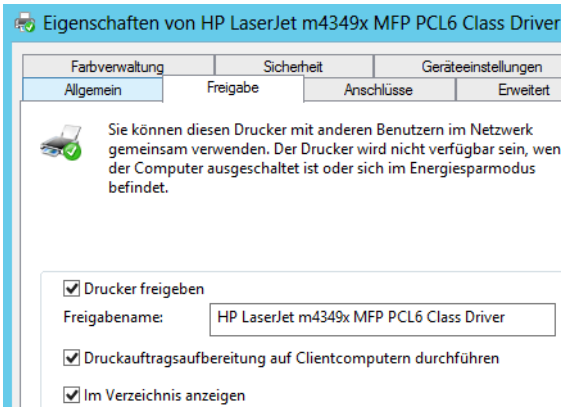
Drucker in Windows freigeben

Wenn Sie einen Drucker an einem Server mit Windows Server 2012 R2 angeschlossen haben und von anderen PCs im Netzwerk zugreifen wollen, können Sie diesen recht einfach freigeben:

1. Dazu installieren Sie den Drucker auf dem Server. Rufen Sie anschließend in der Systemsteuerung *Geräte und Drucker anzeigen* auf. Hier sehen Sie den entsprechenden Drucker.
2. Über das Kontextmenü rufen Sie Druckereigenschaften auf. Wechseln Sie zur Registerkarte *Freigabe*.
3. Anschließend aktivieren Sie die Option *Drucker freigeben* und geben einen Namen für den Drucker ein. Dieser sollte so kurz wie möglich sein, da Clientcomputer sich mit diesem Namen mit dem Computer verbinden.
4. Aktivieren Sie die Option *Druckauftragsbearbeitung auf Clientcomputern durchführen*. So entlasten Sie den Druckerserver.

5. Sie haben noch die Möglichkeit, durch Aktivieren des Kontrollkästchens *Im Verzeichnis anzeigen* den Drucker über das Active Directory auffindbar zu machen. Doch dazu später mehr.

Abbildg. 23.1 Drucker in Windows Server 2012 R2 freigeben



Wichtig ist noch die Schaltfläche *Zusätzliche Treiber*. Wenn sich ein Clientcomputer mit der Freigabe des Druckers verbindet, erhält er vom PC auch einen passenden Treiber. Unterscheidet sich aber das Betriebssystem des Druckerhosts vom Clientcomputer, lässt sich der Drucker nicht verbinden. Das gilt auch dann, wenn auf dem Host ein 64-Bit-System installiert ist und der Client ein 32-Bit-System verwendet. In diesem Fall aktivieren Sie bei den zusätzlichen Treibern noch die Option für das jeweilige Betriebssystem.

Bestätigen Sie die Eingaben mit *OK*, ist der Drucker freigegeben. Nach diesen Maßnahmen steht der Drucker im Netzwerk zur Verfügung. Damit sich dieser auf Clientcomputern verbinden lässt, ist der einfachste Weg die Zeichenfolge \\<*Server-Name des Drucker-Hosts*>\<*Name der Druckerfreigabe*>. Den Drucker sehen Sie auch im Explorer, wenn Sie auf *Netzwerk* klicken. Ist der Drucker nicht sofort ersichtlich, klicken Sie auf den Namen des Computers, der den Drucker zur Verfügung stellt.

Drucker über WLAN anbinden

Effizient lassen sich Drucker über WLAN anbinden. Dazu müssen Sie einen Drucker einsetzen, der über einen eigenen WLAN-Adapter verfügt, oder ihn an einen WLAN-Accesspoint anbinden. Zunächst binden Sie diesen über seine eigene Steuerung an das WLAN-Netzwerk an. Das funktioniert normalerweise direkt an der entsprechenden Hardware über einfach zu bedienende Assistenten. Ist der Drucker im Netzwerk verfügbar, sollten Sie den aktuellsten Druckertreiber beim Hersteller herunterladen und den Drucker anbinden. Netzwerkwissen ist in den wenigsten Fällen notwendig, da der Treiber die entsprechenden Schritte erledigt.

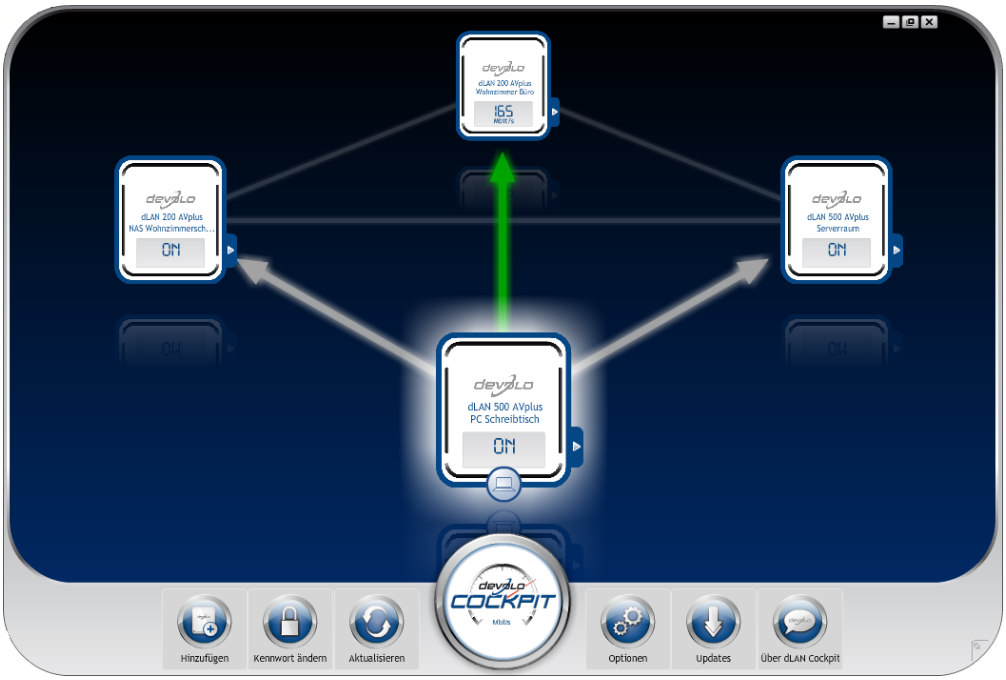
Abbildg. 23.2 Druckertreiber können WLAN-Drucker schnell und einfach anbinden

Anschließend müssen Sie den Druckertreiber nur noch an den Geräten anschließen, die den Drucker nutzen wollen. Konfigurieren Sie noch die Energiesparoptionen auf dem Gerät entsprechend, schaltet sich der Drucker in einen Energiesparmodus, wenn er nicht drucken muss. Der Vorteil bei dieser Technik ist, dass kein Computer angeschaltet sein muss, um den Drucker zu nutzen, sondern er ständig im Netzwerk zur Verfügung steht. Die Drucker verfügen in den meisten Fällen auch über einen internen Webserver, der verschiedene Einstellungen und Statusabfragen erlaubt. Auf diesem Weg lassen sich besonders leicht Smartphones und Tablet-PCs anbinden.

Auf dem gleichen Weg binden Sie Drucker direkt über eine normale Netzwerkschnittstelle an (LAN). In diesem Fall müssen Sie den Drucker entweder mit einem Router oder WLAN-Accesspoint verbinden, der auch über eine normale Netzwerkschnittstelle verfügt. Ist kein direkter Anschluss möglich, verwenden Sie Powerline-Adapter. Diese können den Netzwerkverkehr direkt über Steckdosen weiterleiten. Damit dies funktioniert, sollten sich die Steckdosen idealerweise im gleichen Stromkreis befinden. Ansonsten besteht die Möglichkeit, dass sich die verschiedenen Adapter nicht finden. Elektriker können in diesem Fall aber mit elektronischen Bauteilen wie Phasengleichschaltern eine Verbindung herstellen. Entsprechende Adapter gibt es zum Beispiel von AVM, Devolo, aber auch Netlink und anderen Herstellern.

Verwenden Sie möglichst immer Adapter eines Herstellers, auch wenn viele kompatibel miteinander sind. Die Adapter verfügen über ein eigenes Steuerungsprogramm. Sie können für den Datenverkehr ein Kennwort hinterlegen, sodass in Mehrfamilienhäusern niemand den Datenverkehr mitschneiden kann. So können auch kleine Unternehmen Drucker schnell und einfach anbinden.

Abbildg. 23.3 Powerline-Adapter lassen sich zentral im Devolo Cockpit steuern

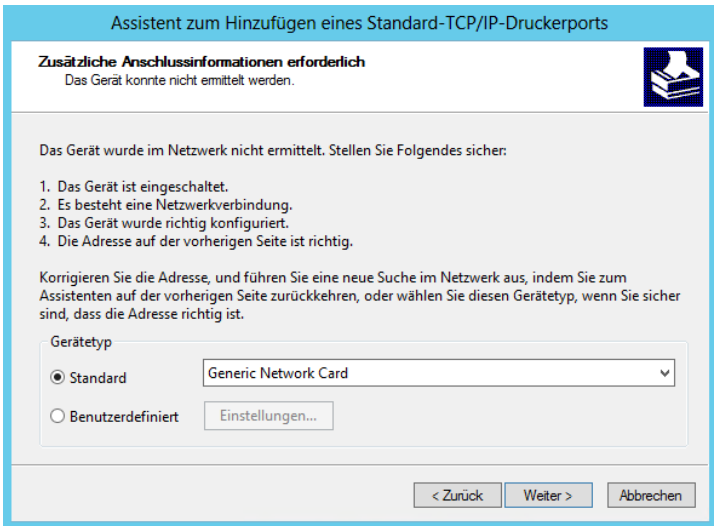


Eigenen Netzwerkanschluss konfigurieren

Wenn die Drucker über keinen optimierten Treiber verfügen, der eine direkte Anbindung an das Netzwerk erlaubt, können Sie die entsprechende Verbindung auch manuell herstellen. Auch beim Anschluss eines USB-Druckers an einen externen Druckerserver können Sie auf dem Druckerserver manuell einen Netzwerkanschluss erstellen, der den Druckertreiber mit dem Drucker verbindet. Auch hier profitieren wieder kleine Unternehmen, wenn zum Beispiel eine AVM Fritz!Box im Einsatz ist. Die Verbindung funktioniert natürlich auch mit professionelleren Druckerservern:

1. Dazu installieren Sie den Druckertreiber auf dem Server und wählen irgendeinen Anschlussport aus. Dieser muss nicht funktionieren.
2. Nach der Installation rufen Sie über das Kontextmenü die *Druckeigenschaften* auf und wechseln zur Registerkarte *Anschlüsse*. Klicken Sie auf *Hinzufügen* und wählen Sie *Standard TCP/IP-Port* aus.
3. Es startet ein Assistent, der Sie bei der Anbindung unterstützt. Geben Sie bei *Druckername oder -IP-Adresse* die IP-Adresse ein, die im Drucker konfiguriert ist. Diese sehen Sie direkt am Drucker in den Netzwerkeinstellungen. Das Feld *Portname* lassen Sie leer, außer der Hersteller des Hardwaredruckerservers gibt eine bestimmte Angabe vor.
4. Anschließend versucht der Assistent eine Erkennung und bindet den Drucker an. Findet der Assistent keinen Anschlussnamen, verwenden Sie die Einstellung *Generic Network Card*.
5. Stellen Sie sicher, dass auf der Registerkarte *Anschlüsse* der neue Port hinzugefügt und ausgewählt ist. Der Drucker sollte jetzt funktionieren.

Abbildg. 23.4 Auswählen der Netzwerkkarte des Netzwerkdruckers



Drucken mit iPhone und iPad – AirPrint

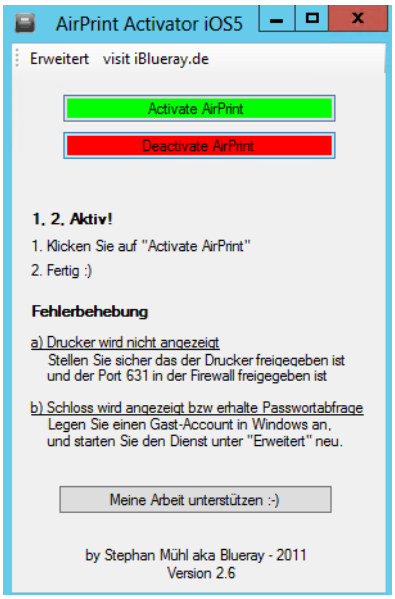
Ein häufiges Problem ist das Drucken von Dateien über das Smartphone. Während auf PCs einfach das Installieren eines Druckertreibers ausreicht, lassen sich an Smartphones über diesen einfachen Weg keine Druckausgaben durchführen.

Drucker lassen sich per USB auch nicht so einfach an Smartphones anschließen. Für iPhone und iPad gibt es die Funktion AirPrint. Diese erlaubt das Drucken über WLAN, offiziell aber nur auf ausgewählte HP-Drucker. Wir zeigen Ihnen aber, wie Sie diese Funktion auch für andere Drucker nutzen können und das vollkommen kostenlos. Um diese Funktion zu nutzen, ist keine Installation notwendig. Sie müssen einfach die *Weiterleiten*-Funktion auswählen und den Druck starten. Anschließend scannt das iPhone/iPad das Netzwerk auf kompatible Drucker und bietet eine Druckerauswahl an. Den Druckauftrag sendet das Gerät per WLAN direkt an den Drucker. Sie benötigen dazu keine App und auch keinen Druckerserver. Alle Apps, die eine interne Druckfunktion haben, können AirPrint nutzen.

Leider unterstützen nicht alle Drucker AirPrint. Dafür gibt es aber ein Tool, welches Drucker über iTunes zur Verfügung stellt. In diesem Fall können Sie den Drucker nicht direkt ansprechen, sondern über einen Computer, auf dem iTunes installiert ist. Das Tool steht auch für Windows zur Verfügung. Um AirPrint in Windows zu aktivieren, installieren Sie auf dem Computer den Druckertreiber. Geben Sie den Drucker ganz normal frei, wie in diesem Kapitel beschrieben. Anschließend verwenden Sie den AirPrint Activator von der beschriebenen Seite und gehen folgendermaßen vor:

1. Installieren Sie iTunes auf dem Server. Wollen Sie keinen produktiven Server beeinträchtigen, installieren Sie einen virtuellen Server nur für das Drucken von Smartphones.
2. Entpacken Sie das Archiv von AirPrint Activator und starten Sie die Datei mit der rechten Maustaste über *Als Administrator ausführen*.
3. Klicken Sie anschließend auf *Activate AirPrint*.

Abbildg. 23.5 AirPrint Activator starten, um Drucker für iPhones zur Verfügung zu stellen



4. Klicken Sie auf *Systemsteuerung/System und Sicherheit/Windows-Firewall*.
5. Klicken Sie auf der linken Seite auf *Eine App oder ein Feature durch die Windows-Firewall zulassen*.
6. Klicken Sie auf *Andere App zulassen* und wählen Sie die Datei *Airprint.exe* im Ordner *C:\AirPrint* aus, wenn diese noch nicht freigegeben ist.
7. Klicken Sie auf *OK*, damit das Programm im Netzwerk kommunizieren darf.
8. Tippen Sie auf der Startseite *wf.msc* ein.
9. Erstellen Sie eine eingehende neue Regel, die den TCP-Port 631 zulässt.
10. Tippen Sie *lusrmgr.msc* auf der Startseite ein und klicken Sie auf *Benutzer*. Stellen Sie sicher, dass das Benutzerkonto *Gast* aktiviert ist.
11. Wählen Sie die Druckfunktion in der App auf dem Smartphone, über das Sie drucken wollen. Im *E-Mail-Bereich* wählen Sie zum Beispiel die *Weiterleiten*-Funktion und dann *Drucken*.
12. Wählen Sie *Drucker auswählen*.
13. Die freigegebenen Drucker auf dem Server mit Windows Server 2012 R2 sollte jetzt angezeigt werden.

Viele Druckerhersteller bieten im Apple App-Store oder auch im Android-Market-Place Apps an, die das Drucken erlauben. Dies gilt auch für Windows Phone 7.5/8. Ein Blick in den jeweiligen Store lohnt sich daher. Mit der kostenlosen App Cortado, die für iPhone und iPad zur Verfügung steht, aber auch für BlackBerry, Symbian und Android, können Anwender Dokumente auf einem Server im Internet speichern. Bereits die kostenlose Einzelplatzlösung ermöglicht zusätzlich noch das Ausdrucken von Dokumenten auf Netzwerkdruckern. Dazu muss der Drucker nicht AirPrint-fähig sein, sondern Sie können jeden Netzwerkdrucker anbinden. Um Cortado zu nutzen, installieren Sie die kostenlose App über den Market oder den App-Store.

Freigegebene Drucker verwalten

Unabhängig davon, wie Sie einen Drucker installiert und freigegeben haben, können Sie in der Systemsteuerung auf dem Druckerserver Einstellungen vornehmen, um den Drucker im Netzwerk anzupassen und auch Rechte zur konfigurieren.

Anpassen der Einstellungen von Druckern

Sie finden die Einstellungen in der Systemsteuerung über *Hardware/Geräte und Drucker*. Klicken Sie mit der rechten Maustaste auf den Drucker und wählen Sie *Druckereigenschaften*.

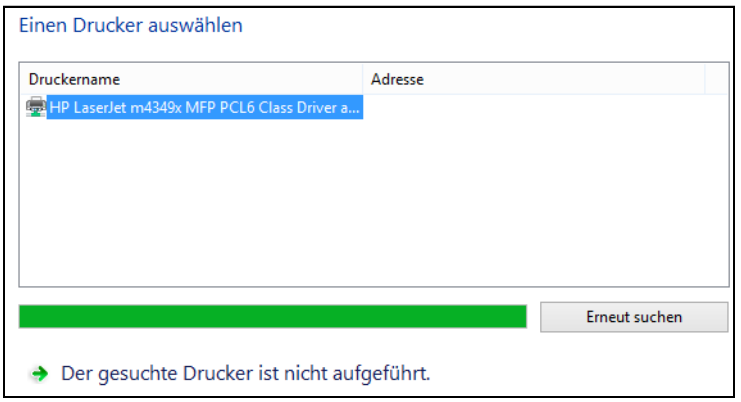
Über die Registerkarte *Sicherheit* lassen sich die Zugriffsberechtigungen für Drucker konfigurieren. Hier gibt es drei Berechtigungen, die standardmäßig zugeordnet werden können:

- **Drucken** Erlaubt die Ausgabe von Dokumenten auf dem Drucker
- **Diesen 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 mit Windows 8/8.1

Drucken können Sie wie Netzlaufwerke im Explorer durch die Syntax \\<*Servername*>\<*Drucker*> oder mit *net use* <*Servername*>\<*Drucker*> verbinden. Um auf einen freigegebenen Drucker im Netzwerk zuzugreifen, können Sie auch den Assistenten für die Druckerinstallation verwenden. Das ist zum Beispiel sinnvoll, wenn Sie den Drucker im Ordner, also in Active Directory, veröffentlicht haben. Klicken Sie auf *Drucker hinzufügen*, finden Windows 7 und Windows 8/8.1 veröffentlichte Drucker automatisch.

Abbildg. 23.6 Freigegebenen Drucker im Active Directory suchen



Verwaltung von Druckjobs

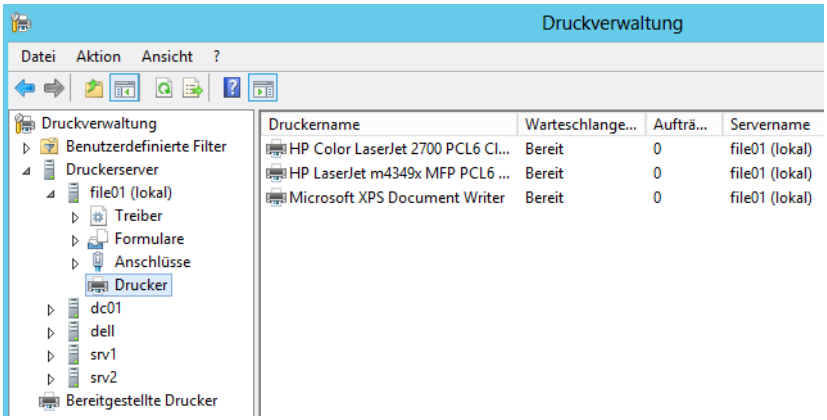
Führt ein Drucker viele Druckjobs aus, ist es oft notwendig, dass Sie diese Jobs beobachten und unter Umständen beenden, wenn ein Job einen ganzen Drucker blockiert. Klicken Sie in der Druckersteuerung doppelt auf den entsprechenden Drucker und wählen Sie dann *Druckausgabe anzeigen*. Damit wird die 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. 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 Eingabeaufforderung *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 Druckerserver

Die Druckverwaltung ist eine zentrale Verwaltungsoberfläche für Drucker in Ihrem Unternehmen. Sie starten das Tool über die Programmgruppe *Tools* im Server-Manager. Sie können mit dieser Konsole alle Druckerserver Ihres Unternehmens an zentraler Stelle verwalten und neue Drucker hinzufügen oder entfernen.

Abbildg. 23.7 Druckerserver mit der Druckverwaltung überwachen und konfigurieren

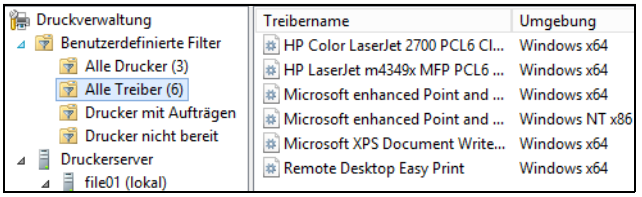


Klicken Sie mit der rechten Maustaste auf der Konsolenstruktur auf den Eintrag *Druckerserver*, können Sie weitere Server der Verwaltungskonsole hinzufügen, die Sie zukünftig über diese zentrale Stelle verwalten können. Auf den Servern müssen aber die Druck- und Dokumentdienste installiert sein, wie zu Beginn des Kapitels beschrieben. Die Drucker der verbundenen Druckerserver werden in der Druckverwaltung an drei Orten gespeichert: *Benutzerdefinierte Druckerfilter*, *Druckerserver* 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.

Abbildg. 23.8 Anzeige der Drucker im Unternehmen und deren Status auf dem Druckerserver



Sie können erkennen, welche Drucker derzeit nicht bereit sind, und zwar von allen Druckerservern, 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 den 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.

Exportieren und Importieren von Druckern

Klicken Sie mit der rechten Maustaste auf einen der verbundenen Druckerserver, können Sie verschiedene Aufgaben durchführen. Unter anderem können Sie alle Druckertreiber auf einen Schlag exportieren. Die Exportdatei können Sie auf einem anderen Druckerserver 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.

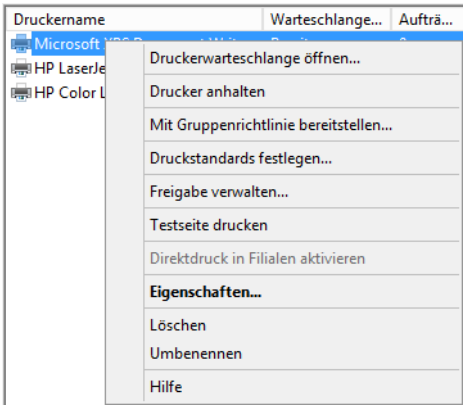
Über das Kontextmenü können Sie auch neue Drucker hinzufügen. Im Gegensatz zum normalen Installations-Assistenten für Drucker können Sie über den Assistenten in der Druckverwaltung auch automatisch nach verfügbaren Druckern im gleichen Subnetz suchen lassen.

Drucker verwalten und über Gruppenrichtlinien verteilen lassen

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

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. 23.9 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. 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 Ordner *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.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Drucker unter Windows Server 2012 R2 freigeben und diese Drucker effizient im Netzwerk verwalten und verteilen können. Auch die Anbindung von Smartphones und Tablet-PCs konnten Sie in diesem Kapitel lesen.

Im nächsten Kapitel zeigen wir Ihnen, wie DHCP in Windows Server 2012 R2 funktioniert und wie Sie die Funktionen von DHCP in Windows Server 2012 R2 nutzen.

Teil F

Infrastruktur und Webdienste

Kapitel 24

DHCP- und IPAM-Server einsetzen

In diesem Kapitel:

In diesem und den folgenden Kapiteln beschäftigen wir uns mit den wichtigen Infrastrukturdiensten von Windows Server 2012 R2. Über diese Dienste stellen Sie Funktionen im Netzwerk bereit, die Server und Arbeitsstationen nutzen, um mit dem Netzwerk zu kommunizieren. Wir zeigen Ihnen in diesem Kapitel, wie Sie DHCP einsetzen, in den nächsten Kapiteln lesen Sie mehr zu DNS und WINS.

Ab Windows Server 2012 gibt es einige Neuerungen in diesem Bereich, zum Beispiel den neuen Serverdienst IP-Adressverwaltungsserver (IPAM). In den Einstellungen für virtuelle Switches in Hyper-V können Sie den DHCP-Wächter aktivieren. Dieser verhindert, dass virtuelle Server im Netzwerk IP-Adressen verteilen, obwohl das nicht gewünscht ist. Neu sind auch Richtlinien in DHCP. Auf diese Weise lassen sich IP-Adressen besser verteilen. Ebenfalls neu ist die Zusammenarbeit und Synchronisierung von zwei DHCP-Servern im Netzwerk. Diese neue Failovertechnologie benötigt keinen Cluster, sondern nur zwei DHCP-Server mit Windows Server 2012. Die Technologien hat Microsoft in Windows Server 2012 R2 verbessert und im Bereich IPAM zum Beispiel die Unterstützung für virtuelle Infrastrukturen eingebaut.

DHCP-Server lassen sich auf diesem Weg zu Teams zusammenfassen. DHCP-Server mit Windows Server 2012 R2 können Einstellungen, IP-Bereiche und Leases untereinander synchronisieren und replizieren. Fällt ein DHCP-Server aus, übernimmt ein anderer DHCP-Server dessen Aufgabe und kann die Leases der Clients weiterverwalten. Einfach ausgedrückt können DHCP-Server mit Windows Server 2012 R2 den exakt gleichen Bereich verwalten, und zwar gleichzeitig. Wie Sie diese Dienste konfigurieren, zeigen wir Ihnen in diesem Kapitel.

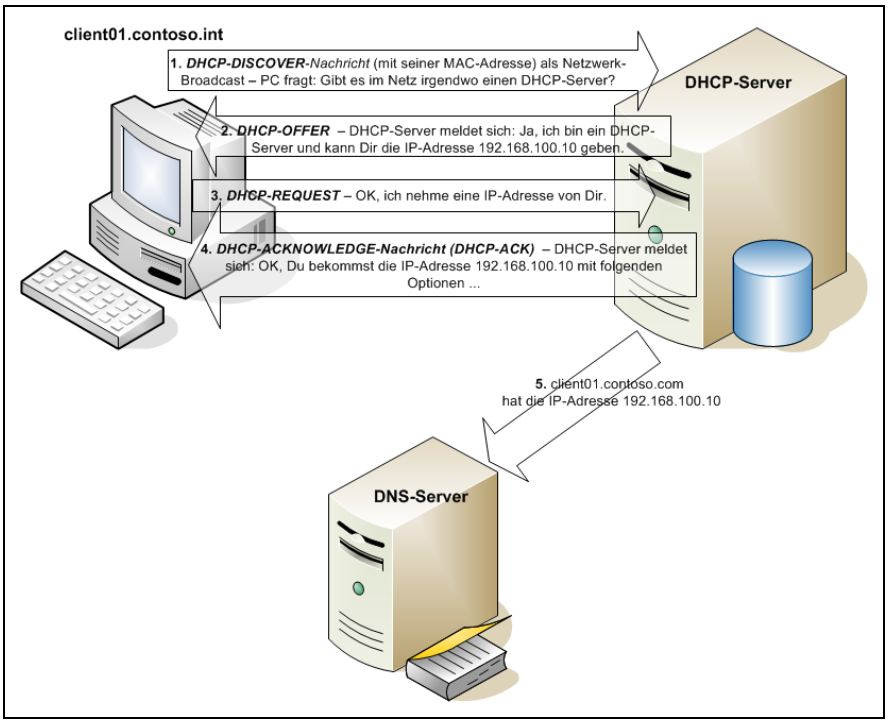
DHCP-Server einsetzen

DHCP steht für Dynamic Host Configuration-Protokoll. 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 2012 R2 ist die Integration in DNS und die gemeinsame Verwaltung mit IPAM.

Installation eines DHCP-Servers

Der DHCP-Server-Dienst wird über den Server-Manager installiert. Um diese einem Server hinzuzufügen, installieren Sie über den Server-Manager die Rolle *DHCP-Server*. Dadurch installieren Sie auch die Verwaltungstools für DHCP. Im Gegensatz zu Windows Server 2008 R2 richten Sie den Dienst nicht mehr während der Installation der Rolle ein, sondern nachträglich über einen Assistenten. Wie alle anderen Rollen können Sie auch DHCP im Server-Manager auch über das Netzwerk installieren.

Abbildg. 24.1 Datenverkehr bei der Verwendung von DHCP

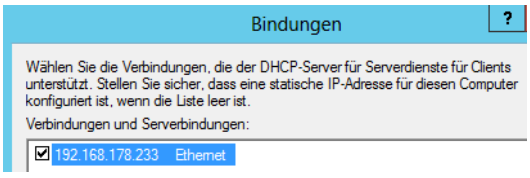


Grundkonfiguration eines DHCP-Servers

Haben Sie die Serverrolle installiert, starten Sie die Einrichtung über das Wartungssymbol oben rechts im Server-Manager. Über einen Assistenten nehmen Sie die Grundeinrichtung des DHCP-Servers vor. In den ersten Schritten legen Sie über den Assistenten die notwendigen Sicherheitsgruppen für DHCP an und autorisieren den Server in Active Directory. Erst nach der Autorisierung verteilt der Server IP-Adressen im Netzwerk. Den eigentlichen Dienst verwalten Sie über das Verwaltungsprogramm *DHCP*.

In den Eigenschaften von IPv4 und IPv6 legen Sie auf der Registerkarte *Erweitert* mit der Schaltfläche *Bindungen* fest, auf welchen Netzwerkkarten der Server auf DHCP-Anfragen antwortet. Sind in einem Server mehrere Netzwerkkarten eingebaut, besteht auch die Möglichkeit, den Server auf mehrere dieser Schnittstellen hören zu lassen.

Abbildg. 24.2 Auswählen der Bindungen für einen DHCP-Server

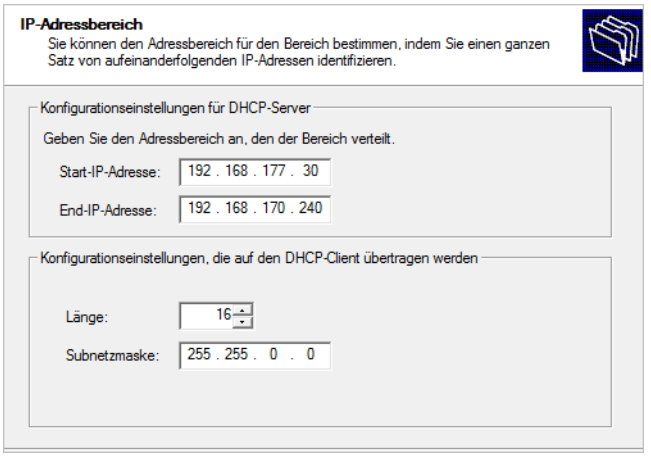


Bereiche erstellen

Ein DHCP-Server verteilt bestimmte IP-Adressen auf Basis von Bereichen, die Sie im Kontextmenü von IPv4 oder IPv6 anlegen. Hier steuern Sie, welche IP-Adressen Computer von diesem DHCP-Server erhalten sollen. Zunächst geben Sie einen Namen und eine Beschreibung für einen Bereich an.

Auf der nächsten Seite legen Sie die Start-IP-Adresse und die End-IP-Adresse sowie die Subnetzmaske des Bereichs fest.

Abbildg. 24.3 Festlegen der Start- und End-Adresse eines Bereichs



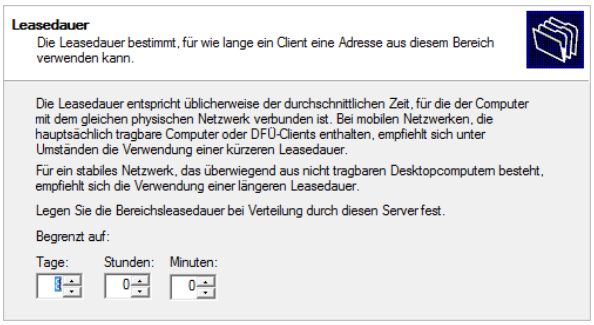
Als Nächstes legen Sie die IP-Bereiche innerhalb des neuen Bereichs fest, aus denen der Server keine IPO-Adressen verteilen soll. Sie können in diesem Bereich auch nur einzelne IP-Adressen ausschließen oder die Antwort des Servers verzögern lassen, sodass unter Umständen andere DHCP-Server vorher auf die Anfragen von Clients antworten.

Bei der Einrichtung des DHCP-Bereichs legen Sie im Anschuss die Leasedauer in fest. Diese Einstellung lässt sich nachträglich noch bearbeiten. Weist ein DHCP-Server einem Client eine IP-Adresse zu, dann ist diese Zuweisung immer auf einen gewissen Zeitraum beschränkt, die sogenannte Leasedauer, die in der Standardeinstellung 8 Tage beträgt. Windows Server 2012 R2 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, umso 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.

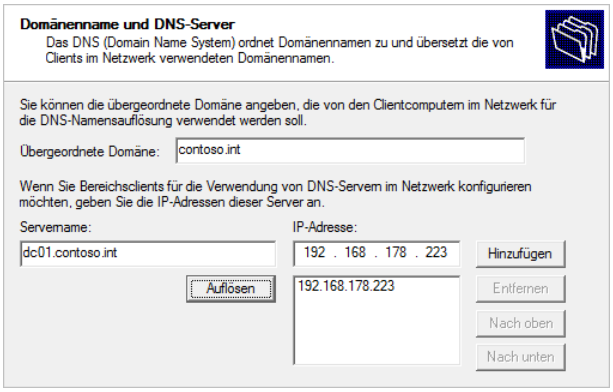
Abbildg. 24.4 Konfigurieren der Leasedauer für einen Bereich



Anschließend können Sie für den Bereich noch erweiterte Einstellungen wie DNS oder WINS festlegen. Zunächst legen Sie in den erweiterten Optionen das Standardgateway fest, welches der Server an Clients verteilen soll.

Anschließend legen Sie die DNS-Einstellungen fest, die an die Clients verteilt werden sollen. An dieser Stelle können neben DNS-Servern auch die DNS-Domänen 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 *Auflösen* sichergestellt werden, dass die IP-Adresse des Servers stimmt und der Server auch erreicht werden kann.

Abbildg. 24.5 Konfigurieren der DNS-Einstellungen für DHCP-Clients



Auf der nächsten Seite legen Sie die WINS-Server fest, die den Clients zugewiesen werden sollen. Auch wenn in Active Directory WINS keiner so eine wichtige Rolle spielt wie DNS, schadet der Einsatz des Systems nicht, wie wir Ihnen im Kapitel 26 zeigen.

WINS sorgt parallel zu DNS für eine Namensauflösung im Netzwerk oder verursacht eine zu große Serverlast. Durch den parallelen Einsatz von WINS und DNS wird außerdem eine gewisse Ausfallsicherheit der Namensauflösung im Netzwerk erreicht, auch für die Replikation in Active Directory. WINS kann zwar eine DNS-Struktur nicht ersetzen, einzelne fehlende DNS-Einträge oder ausgefallene DNS-Server aber schon, zumindest kurzzeitig.

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 und Windows 7/8 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. Dieses Beziehen 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, die Einstellungen auf den Standardwerten zu belassen.

Nach der Erstellung eines DHCP-Bereichs in der Verwaltungskonsole können Sie jederzeit festlegen, wie der Server auf Anfragen reagieren soll und welche Adressen er bereits verteilt hat. Sie können über das Kontextmenü ebenfalls Einstellungen von Bereichen anpassen.

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. Bei *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.

Zusätzlich zu den Einstellungen bei der Erstellung des Bereichs können Sie die Leasedauer auf *Unbegrenzt* setzen, wenn Sie die Eigenschaften des Bereichs aufrufen. 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.

TIPP Wenn ein Bereich aktiviert ist, sollten Sie ihn erst dann deaktivieren, wenn die enthaltenen IP-Adressen nicht weiter im Netzwerk verfügbar sein sollen. Nach dem Deaktivieren eines Bereichs akzeptiert der DHCP-Server diese Adressen nicht mehr als gültig.

Wenn Adressen nur zeitweise deaktiviert sein sollen, können Sie durch Bearbeiten oder Ändern von Ausschlussbereichen in einem aktiven Bereich das gewünschte Resultat ohne ungewollte Nebeneffekte erzielen. Ausgeschlossene Bereiche lassen sich über das Kontextmenü des Eintrags *Adresspool* erzeugen.

Die Einstellungen eines Bereichs können Sie auch in der PowerShell abfragen. Dazu verwenden Sie den Befehl *Get-DhcpServerv4Scope*. Alle neuen Cmdlets zur Verwaltung von DHCP in Windows Server 2012 R2 erhalten Sie durch die Eingabe von *Get-Command *dhcp**.

DHCP-Server autorisieren

Sobald der DHCP-Server Mitglied in einer Active Directory-Domäne ist, muss der Server in Active Directory autorisiert werden, falls diese Aktion nicht bereits während der Installation durchgeführt wurde. Daher erscheint der entsprechende Einrichtungsassistent in Windows Server 2012 R2 direkt nach der Installation der Serverrolle.

Nur Mitglieder der Gruppe *Organisations-Admins* können standardmäßig DHCP-Server autorisieren. 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. Auf diesem Weg können Sie die Autorisierung auch wieder aufheben.

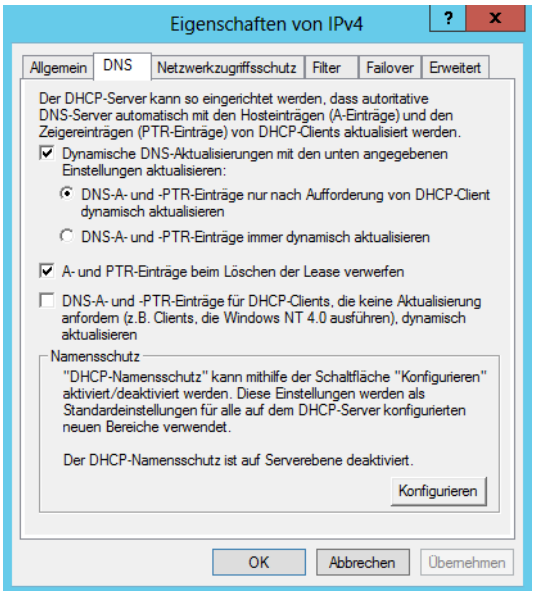
Wenn der DHCP-Serverdienst von Windows Server 2012 R2 startet, fragt er zunächst Active Directory, um festzustellen, ob er sich in der Liste der autorisierten DHCP-Server befindet. Ist dies der Fall, sendet er eine *DHCPinform*-Nachricht in das Netzwerk, um festzustellen, ob es andere Verzeichnisdienste gibt und er bei diesen gültig ist. Falls der DHCP-Server dagegen keinen Eintrag in 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 Active Directory gearbeitet wird.

Bei alleinstehenden Servern mit Windows Server 2012 R2 und DHCP-Dienst kann der DHCP-Serverdienst nur genutzt werden, solange keine Active Directory-Domäne im Netzwerk gefunden wird. Der Schutz von Active Directory greift natürlich nicht, wenn auch andere, nicht auf Windows Server 2012 R2 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.

Abbildg. 24.6 Konfiguration der DNS-Anbindung eines DHCP-Servers



Setzen Sie noch Clients ein, die kein dynamisches DNS unterstützen, sollten Sie in den Eigenschaften des DHCP-Servers auf der Registerkarte *DNS* das Kontrollkästchen *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*.

Über die Schaltfläche *Konfigurieren* auf der Registerkarte *DNS* in den Eigenschaften des DHCP-Servers können Sie noch den Namenschutz aktivieren, der bereits existierende Einträge im DNS vor Änderungen schützt.

In der Gruppe *DnsUpdateProxy* in der Domäne befinden sich Computer, die als Proxy für die dynamische Aktualisierung von DNS-Einträgen fungieren können. DHCP-Server werden in diese Gruppen nicht automatisch aufgenommen. Sie sollten die Computerkonten der DHCP-Server in die Gruppe *DnsUpdateProxy* aufnehmen, wenn die DNS-Aktualisierung nicht funktioniert. Alternativ können Sie auf der Registerkarte *Erweitert* in den Eigenschaften für IPv4 oder IPv6 Anmeldedaten hinterlegen, die eine Aktualisierung ermöglichen.

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 ebenfalls vor, nur leider in den seltensten Fällen an der Außenblende.

Sie können die MAC-Adresse auch über die Eingabeaufforderung mit dem Kommando *ipconfig /all* ermitteln. Die MAC-Adresse wird in der Zeile *Physikalische Adresse* angezeigt.

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* [Ms179-K24-01] im Internet herunterladen können, werden alle MAC-Adressen in einem Netzwerk in der Eingabeaufforderung ausgelesen. Geben Sie dazu den Befehl *getmac <Subnetz> <Startadresse> <Endadresse>* ein.

So werden zum Beispiel mit *getmac 192.168.178 1 40* 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 Ordner angelegt wird, aus dem Sie *getmac.bat* starten.

Mit diesem kostenlosen Tool erhalten Sie schnell alle verfügbaren MAC-Adressen in einem IP-Bereich. Öffnen Sie nach dem Scanvorgang die Textdatei *used_ips.txt*, um sich die MAC-Adressen der Clients anzeigen zu lassen.

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.

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.

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

TIPP Wichtig ist die Überprüfung der Konsistenz der DHCP-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 daraufhin, ob die Inhalte der Bereiche und der Datenbank konsistent sind und keine Überschneidungen auftreten.

Konfigurieren von DHCP mit der richtlinienbasierten Zuweisung

Eine der wesentlichen Neuerungen in Windows Server 2012 R2 ist das richtlinienbasierte Zuweisen von IP-Adressen. Die richtlinienbasierte Zuweisung (Policy Based Assignment, PBA) ermöglicht es, DHCP-Clients nach bestimmten Attributen zu gruppieren, die im DHCP-Clientanforderungspaket enthalten sind. Die Richtlinien sind einfach ausgedrückt deutlich verbesserte Reservierungen, die über die Abfrage von MAC-Adressen hinausgehen.

DHCP-Richtlinien verstehen

Eine Richtlinie enthält eine Gruppe von Bedingungen. Je nach Typ des Clients können Sie zum Beispiel unterschiedliche Einstellungen für die Leasedauer einstellen. Die folgenden Felder in der DHCP-Clientanforderung sind beim Definieren von Richtlinien verfügbar:

- Herstellerklasse
- Benutzerklasse
- MAC-Adresse
- Client-ID
- Informationen zum Relay-Agent

Es gibt drei Typen von Richtlinieneinstellungen, die Sie den Clients zuteilen können:

- **IP-Adressbereich** Sie können auf Basis der Richtlinie unterschiedliche IP-Adressbereiche verwenden
- **Standard-DHCP-Optionen** Sie können mehrere Standard-DHCP-Optionen zum Versand an einen Client konfigurieren
- **Herstellerspezifische DHCP-Optionen** Es lassen sich eine oder mehrere herstellerspezifische DHCP-Optionen zum Versand an den Client konfigurieren

Der DHCP-Server wertet Richtlinien nach einer fest definierten Reihenfolge aus. Wenn Richtlinien auf den Server- und Bereichsebenen vorhanden sind, wendet der Server beide Gruppen von Richtlinien an und wertet die Bereichsrichtlinien vor den Serverrichtlinien aus. Wenn auf Bereichsebene keine Richtlinien definiert sind, gelten die Richtlinien auf der Serverebene für den Bereich. Eine einzige Clientanforderung kann mehreren Richtlinien entsprechen.

Wenn eine Clientanforderung den Bedingungen einer Richtlinie entspricht, weist der Server die erste freie IP-Adresse aus dem Bereich gemäß der Bestimmungen durch die Regel zu. Wenn einer Richtlinie mehrere Adressbereiche zugeordnet sind, weist der Server IP-Adressen zu, indem er zunächst versucht, eine IP-Adresse aus dem niedrigsten Adressbereich zuzuweisen. Wenn in keinem der Adressbereiche, die durch die Richtlinie zugeordnet sind, freie IP-Adressen verfügbar sind, verarbeitet der Server die nächste passende Richtlinie, wie durch die Verarbeitungsreihenfolge definiert wird.

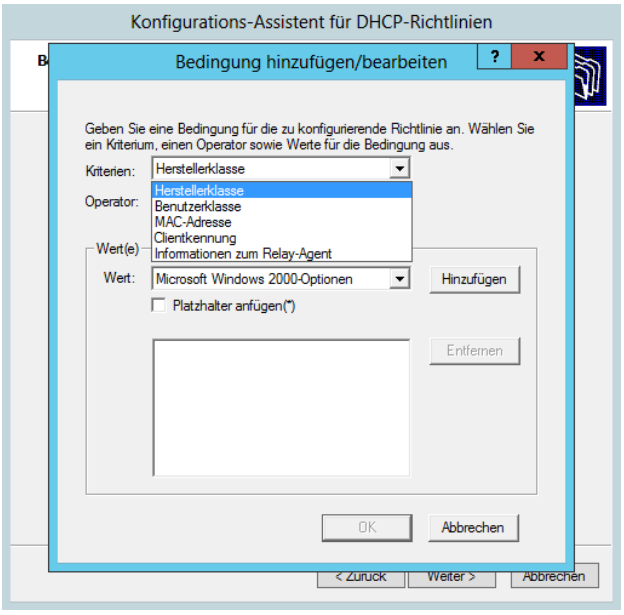
Wenn keine der passenden Richtlinien über eine freie IP-Adresse verfügt, löscht der Server das Clientpaket und protokolliert ein Ereignis. Wenn ein DHCP-Clientpaket keiner der für den Bereich gültigen Richtlinien entspricht oder wenn keine der passenden Richtlinien für ein Clientpaket einem IP-Adressbereich zugeordnet ist, leiht der Server dem Client eine IP-Adresse aus dem IP-Adressbereich, der für den Bereich ohne richtlinienspezifische IP-Adressbereiche konfiguriert ist.

Der DHCP-Server wertet die Felder in der Clientanforderung in Bezug auf die einzelnen anwendbaren Richtlinien für den Bereich in der angegebenen Reihenfolge aus. Wenn die Clientanforderung den Bedingungen einer für den Bereich anwendbaren Richtlinie entspricht und die Einstellungen bestimmte Optionen umfassen, gibt der Server diese Optionen an den Client zurück. Wenn mehrere Richtlinien den Clientanforderungen entsprechen, gibt der Server die Summe der Optionen zurück, die für die einzelnen passenden Richtlinien angegeben werden.

Erstellen von DHCP-Richtlinien

Um Richtlinien zu erstellen, verwenden Sie den neuen Menüpunkt *Richtlinien in der DHCP-Verwaltung von Windows Server 2012 R2*. Über das Kontextmenü erstellen Sie eine neue Richtlinie. Zunächst geben Sie einen Namen und eine Beschreibung für die Richtlinie ein. Anschließend legen Sie im nächsten Fenster eine oder mehrere Bedingungen fest.

Abbildg. 24.7 Festlegen von Bedingungen für eine DHCP-Richtlinie



Klicken Sie auf der Seite *Bedingungen für die Richtlinie konfigurieren* auf *Hinzufügen*. Wählen Sie im Dialogfeld *Bedingung hinzufügen/bearbeiten* die Option bei Kriterien aus, die Sie verwenden wollen. Legen Sie die Bedingung fest. Sie können mehrere Bedingungen definieren und diese auch mit Und/Oder miteinander verknüpfen.

Klicken Sie auf *Weiter*, können Sie dem Client noch verschiedene DHCP-Server-Optionen oder IP-Adressen zuteilen. Klicken dann auf *Fertig stellen*. Sie können die Richtlinien in der Verarbeitungsreihenfolge nach oben und unten verschieben sowie löschen oder deaktivieren. Außerdem können Sie die Eigenschaften einer Richtlinie jederzeit anpassen.

Migration – 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 Quellserver 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 Ordner *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 Zielserver 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*.

Eine weitere Möglichkeit, die DHCP-Daten zu exportieren, besteht über die Eingabeaufforderung. Geben Sie dazu die folgenden Befehle ein:

```
Netsh
Dhcp
Server <IP-Adresse des Quell-Servers>
Export <Pfad und Datei> all
```

Anschließend kopieren Sie die Datei auf den Zielserver und importieren die Datenbank wieder. Verwenden Sie dazu folgende Befehle:

1. Beenden Sie den DHCP-Server mit *net stop dhcpserver*.
2. Löschen Sie die Datei *dhcp.mdb* im Ordner *C:\Windows\System32\dhcp*.
3. Starten Sie den DHCP-Server mit *net start dhcpserver* neu.
4. Geben Sie *netsh* ein.
5. Geben Sie *dhcp* ein.

6. Geben Sie *server <IP-Adresse des Zielservers>* ein.
7. Geben Sie *import <Pfad der Datei>* ein.
8. Beenden Sie den DHCP-Server mit *net stop dhcpserver*.
9. Starten Sie den DHCP-Server mit *net start dhcpserver* neu.

Core-Server – DHCP mit Netsh über die Eingabeaufforderung verwalten

Der DHCP-Dienst von Windows Server 2012 R2 lässt sich mit dem Befehl Netsh auch über die Eingabeaufforderung 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 Eingabeaufforderung zunächst *netsh* ein und bestätigen Sie.

Anschließend geben Sie *dhcp* ein und bestätigen Sie. Jetzt können die spezifischen DHCP-Befehle in der Eingabeaufforderung verwendet werden. Die folgenden 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. Die Syntax dazu lautet *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. Die Syntax dazu lautet *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

MAC-Filterung für DHCP in Windows Server 2012 R2 nutzen

Eine weitere Funktion in Windows Server 2012 R2 ist die MAC-Filterung des DHCP-Servers. Diese Funktion steuern Sie in der DHCP-Konsole über den Menüpunkt *IPv4/Filter*. Der Filter ermöglicht spezielle Zulassungsfilter und Verweigerungsfilter.

Mit der Liste können Sie sicherstellen, dass speziell festgelegte Geräte eine DHCP-Adresse erhalten oder der Server bestimmte Geräte blockiert. Sie können weiße Listen erstellen, bei denen kein Gerät eine IP-Adresse erhält außer die Geräte auf der Liste. Und Sie können zusätzlich auch schwarze Listen pflegen. Im Gegensatz zu weißen Listen blockieren schwarze Listen nur die Geräte auf der Liste, alle anderen Geräte erhalten vom DHCP-Server eine Adresse zugeteilt. Standardmäßig ist der DHCP-Server für eine schwarze Liste konfiguriert, enthält aber keine MAC-Adressen, die er blockiert.

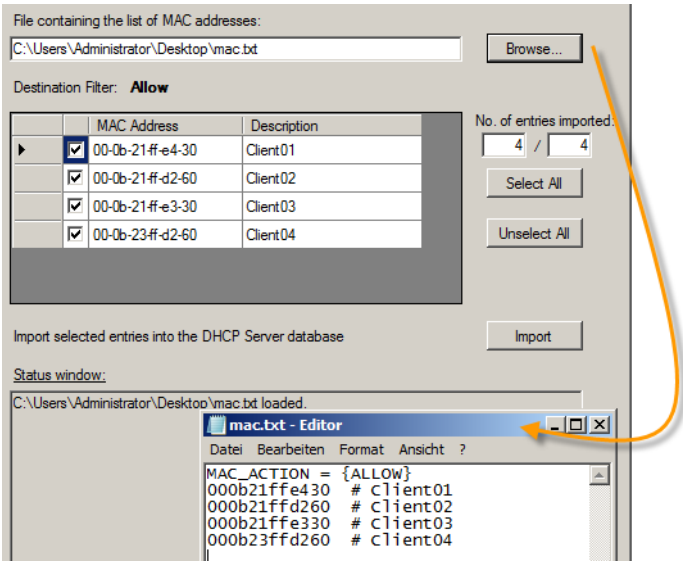
Die MAC-Adressen können Sie über die grafische Oberfläche manuell eingeben oder mit Platzhaltern einen ganzen Bereich blockieren oder erlauben. Sie können Listen aber auch über das Kontextmenü einzelner Leases des Servers pflegen. Eine weitere Möglichkeit ist das Importieren einer Textdatei zum Blockieren. Klicken Sie mit der rechten Maustaste auf einen Rechner unter *Adressleases* eines Bereichs, können Sie den Rechner mit *Zu Filter hinzufügen* zu einem der Filter hinzufügen.

Anschließend sehen Sie die entsprechenden Rechner innerhalb des Filters. Die Filter sind standardmäßig deaktiviert. Wollen Sie diese aktivieren, können Sie das über das Kontextmenü erledigen. Sobald Sie eine MAC-Adresse im Verweigerungsfilter aufgenommen haben und der Filter aktiv ist, erhält dieses Gerät keine IP-Adresse mehr von diesem DHCP-Server. Aktivieren Sie den Filter *Zulassen*, blockiert der Server alle Anfragen außer die MAC-Adressen, die im Zulassungsfilter aufgenommen sind. Aktivieren Sie beide Filter, vergibt der DHCP-Server auch dann nur Adressen an Rechner, die in der Zulassungsliste enthalten sind, mit Ausnahme von Geräten, deren MAC-Adressen in der Verweigerungsliste stehen.

Klicken Sie mit der rechten Maustaste auf den Bereich *IPv4* in der DHCP-Konsole und rufen Sie die Eigenschaften auf, können Sie auf der Registerkarte *Filter* weitere Einstellungen vornehmen. Wollen Sie manuell MAC-Adressen in die einzelnen Filter aufnehmen, klicken Sie auf den Filter mit der rechten Maustaste und wählen Sie *Neuer Filter* aus. Sie können auch mit dem Zeichen * bei der Eingabe des Filters arbeiten. Haben Sie eine Liste von MAC-Adressen, die Sie in die Filter aufnehmen wollen, können Sie das kostenlose Zusatzprogramm von Microsoft mit der Bezeichnung MAC Filter Import Tool (*http://blogs.technet.com/teamdhcp/archive/2009/02/16/mac-filter-import-tool.aspx* [Ms179-K24-02]) verwenden. Die Syntax in der Textdatei sieht folgendermaßen aus:

```
MAC_ACTION = {ALLOW}
000b21ffe430 # Client01
000b21ffd260 # Client02
000b21ffe330 # Client03
000b23ffd260 # Client04
```

Abbildg. 24.8 Hinzufügen von Filtern zum MAC-Filter



Nachdem Sie auf *Import* geklickt haben, sind die MAC-Adressen Bestandteil der entsprechenden Filterliste. Neben der Konfiguration mit der grafischen Oberfläche können Sie die Filterlisten in der Eingabeaufforderung pflegen. Dazu nutzen Sie das Tool Netsh. Die Aktivierung der Listen erfolgt nach folgender Syntax:

```
netsh dhcp server v4 set filter [enforceallowlist=1|0] [enforcedenylist=1|0]
```

Wollen Sie zum Beispiel die Zulassungsliste aktivieren, verwenden Sie den Befehl:

```
netsh dhcp server v4 set filter enforceallowlist=1
```

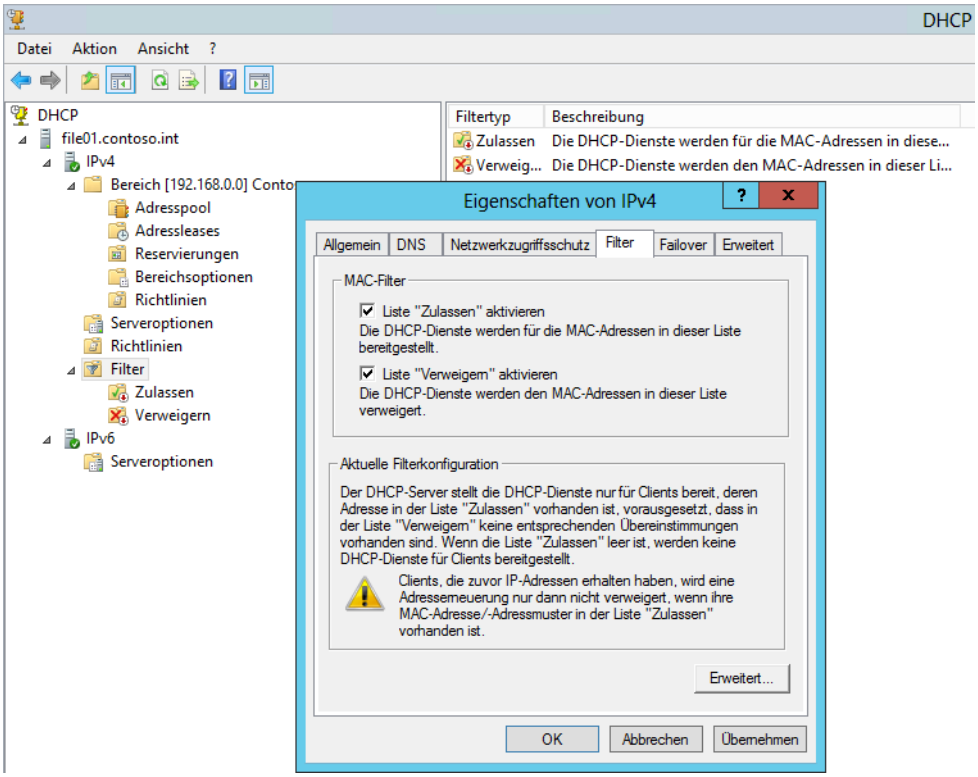
Um MAC-Adressen zu den Listen hinzuzufügen, verwenden Sie den Befehl:

```
netsh dhcp server v4 add filter allow|deny mac-address ["Kommentar"]
```

Ein Beispiel dafür ist:

```
netsh dhcp server v4 add filter allow 01-1b-23-de-db-61 "client01"
```

Abbildg. 24.9 MAC-Filter verwenden



Ausfallsicherheit von DHCP-/DNS-Servern

Server, die für den Betrieb der Infrastruktur zuständig sind, wie zum Beispiel DNS- oder DHCP-Server, sind für den Betrieb in Unternehmen von immenser Bedeutung. Fallen diese Server aus, können andere Computer im Netzwerk keine Verbindung mehr miteinander herstellen, weil entweder IP-Adressen oder eine korrekte Namensauflösung fehlen. Die Vergabe von IP-Adressen in Unternehmen erfolgt meistens per DHCP. Allerdings machen sich nicht alle Administratoren über die Ausfallsicherheit Gedanken. Dabei hat der Ausfall eines solchen Servers für ein Unternehmen oft enorme Auswirkungen. Erhalten die Arbeitsstationen und VPN-Server zum Beispiel keine IP-Adresse mehr, ist der Verbindungsaufbau zu wichtigen Serverdiensten unterbrochen. Die beiden Serverdienste bieten aber einfache Möglichkeiten zur Schaffung der Ausfallsicherheit.

Mit Windows Server 2012 R2 geht Microsoft noch einige Schritte weiter und verbessert die Ausfallsicherheit von DHCP-Servern weiter. Sie können neben den bekannten Möglichkeiten zur Ausfallsicherheit, die bereits für Windows Server 2008 R2 gelten, in Windows Server 2012 R2 verschiedene DHCP-Server zu Teams zusammenfassen, auch ohne Cluster.

Die DHCP-Funktionalität ist clusterfähig. Durch die Einführung eines Clusters erhält jedes Unternehmen einen hervorragenden Ausfallschutz der DHCP-Server. Allerdings besteht der große Nachteil dieser Lösung in den hohen Kosten und der komplizierten Verwaltbarkeit eines Clusters. Aus diesem Grund setzen nur sehr wenige Unternehmen einen Cluster ausschließlich für DHCP ein. Meistens finden andere Lösungen in Unternehmen Einzug, um die Ausfallsicherheit von DHCP-Server zu gewährleisten.

DHCP für Failover konfigurieren

DHCP-Failover in Windows Server 2012 R2 ermöglicht die Bereitstellung einer ausfallsicheren DHCP-Serverstruktur auch ohne Cluster. Wenn ein DHCP-Server nicht mehr erreichbar ist, kann der DHCP-Client seine aktuelle IP Adresse weiterverwenden, indem er einen anderen DHCP-Server im Unternehmensnetzwerk kontaktiert.

TIPP DHCP-Failover unterstützt nur zwei Server mit IPv4-Konfiguration. Die Server können auch Mitglied einer Arbeitsgruppe sein, eine Domänenmitgliedschaft ist nicht unbedingt erforderlich.

DHCP-Failover in Windows Server 2012 R2 verstehen

Mit dem DHCP-Failoverfeature können zwei DHCP-Server IP-Adressen und Optionskonfiguration für dasselbe Subnetz oder denselben Bereich bereitstellen. Zwischen den zwei DHCP-Servern werden Leaseinformationen ausgetauscht. Es ist auch möglich, das Failover in einer Lastausgleichskonfiguration zu konfigurieren, in der Clientanforderungen auf die zwei Server verteilt sind.

DHCP-Failover in Windows Server 2012 R2 stellt Unterstützung für maximal zwei DHCP-Server bereit. Die Failoverbeziehung ist auf IPv4-Bereiche und -Subnetze beschränkt. Computer, die IPv6 verwenden, bestimmen ihre eigene IPv6-Adresse mit der statuslosen automatischen IP-Konfiguration. In diesem Modus stellt der DHCP-Server nur die DHCP-Optionskonfiguration bereit. Der Server behält keine Leasestatusinformationen. Eine Bereitstellung mit hoher Verfügbarkeit für statusloses DHCPv6 ist möglich, indem zwei Server mit identischer Optionskonfiguration eingerichtet werden.

Ein Server ist primär oder sekundär im Kontext eines Subnetzes. Ein Server mit der Rolle eines primären Servers für ein angegebenes Subnetz kann aber auch ein sekundärer Server für ein anderes

Subnetz sein. In einer Lastenausgleichsmodus-Bereitstellung verarbeiten die beiden Server gleichzeitig IP-Adressen und Optionen für Clients in einem angegebenen Subnetz. Die Clientanforderungen werden per Lastenausgleich verarbeitet und auf die beiden Server verteilt.

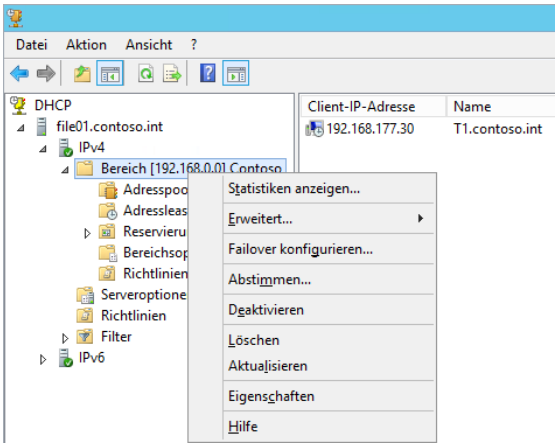
Damit DHCP-Failover funktioniert, muss die Zeit zwischen den beiden Servern in einer Failoverbeziehung stets synchronisiert sein (siehe Kapitel 11). Wenn der Assistent für die Failoverkonfiguration startet, vergleicht er die aktuelle Uhrzeit auf den Servern, die für Failover konfiguriert werden soll. Wenn der Zeitunterschied zwischen den Servern größer als eine Minute ist, wird der Failover-Einrichtungsprozess angehalten und eine Fehlermeldung angezeigt.

Konfigurieren eines Failovers

DHCP-Failover kann auch auf einem Arbeitsgruppencomputer konfiguriert werden, der Betrieb in einer Active Directory-Domäne ist aber stabiler. Das Konfigurieren eines DHCP-Bereichs auf dem zweiten Server ist nicht notwendig. Ein DHCP-Bereich wird automatisch konfiguriert, wenn Sie eine Failoverbeziehung erstellen.

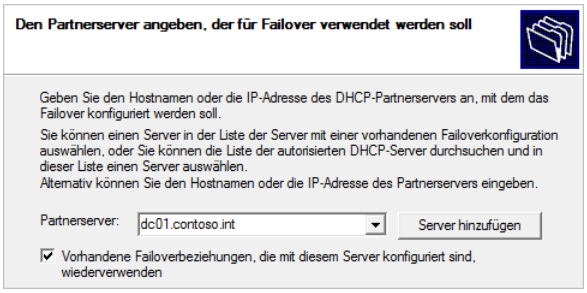
Öffnen Sie auf dem DHCP-Server die DHCP-Konsole, klicken Sie mit der rechten Maustaste auf den DHCP-Bereich, den Sie ausfallsicher betreiben wollen, und klicken Sie dann auf *Failover konfigurieren*. Klicken Sie im Assistenten für die Failoverkonfiguration auf *Weiter*.

Abbildg. 24.10 Failover konfigurieren



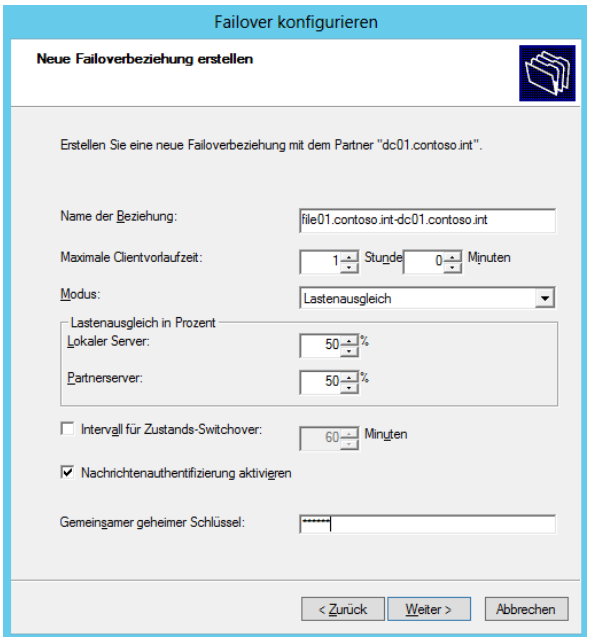
Geben Sie auf der zweiten Seite den Partnerserver an und klicken Sie dann auf *Weiter*.

Abbildg. 24.11 Festlegen des Partnerservers für DHCP



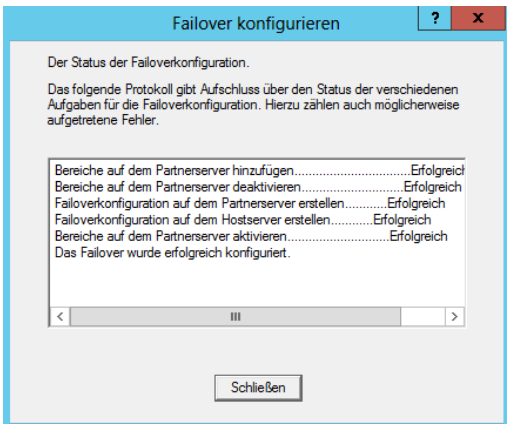
Geben Sie unter *Neue Failoverbeziehung erstellen* einen Namen ein oder übernehmen Sie den angezeigten Standardnamen. Legen Sie auch einen gemeinsamen geheimen Schlüssel für diese Failoverbeziehung fest. Sie können hier auch den Modus auswählen, mit dem Sie die Ausfallsicherheit verwenden wollen. Sie können *Lastenausgleich* oder *Hot Standby* auswählen. Standardmäßig ist der Modus *Lastenausgleich* ausgewählt. Hier teilen sich die Server die Anfragen.

Abbildg. 24.12 Konfigurieren der Failoverbeziehung



Klicken Sie auf *Weiter* und anschließend auf *Fertig stellen*. Stellen Sie sicher, dass die Failoverkonfiguration erfolgreich ist, und klicken Sie dann auf *Schließen*.

Abbildg. 24.13 Erfolgreiche Einrichtung eines Failovers

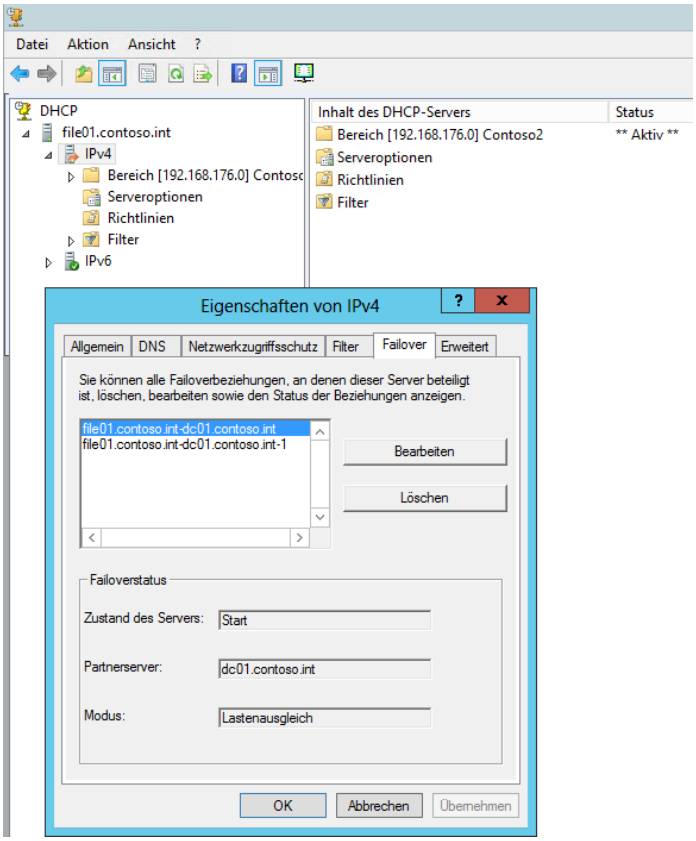


Aktualisieren Sie auf dem zweiten Failoverserver die DHCP-Konsole und überprüfen Sie, ob dieselbe DHCP-Bereichskonfiguration, die auf dem ersten Server vorhanden ist, jetzt auf dem zweiten vorhanden ist.

Nachdem Sie die Einrichtung angeschlossen haben, können Sie das Failover in den Eigenschaften des IP-Bereichs auf der Registerkarte *Failover* anzeigen. Stellen Sie sicher, dass neben *Zustand des Servers* und *Partnerserver* jeweils korrekte Einträge angezeigt werden.

Über das Kontextmenü des Bereichs können Sie auch außerhalb des definierten Replikationsplans die Daten zwischen den Servern replizieren oder die Beziehung auch wieder aufheben. Bearbeiten können Sie das Failover auch in den Eigenschaften von IPv4 auf dem ersten und zweiten Server. Hier können Sie auch den Modus anpassen.

Abbildg. 24.14 Bearbeiten des Failovers in der DHCP-Konsole



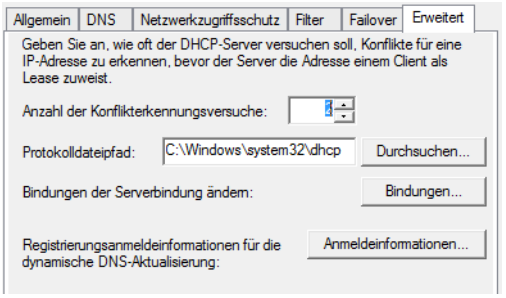
Ausfallsicherheit durch Konflikterkennung

Als praktisch hat sich die Funktion der Konflikterkennung erwiesen, bei der ein DHCP-Server zunächst versucht, einen Verbindungsaufbau mit der IP-Adresse zu herzustellen, die er als Nächstes vergeben will. Bekommt er darauf keine Antwort, ist die Adresse unbenutzt und steht für den nächsten Client zur Verfügung.

Gibt es bereits einen Client mit der gleichen IP-Adresse, erkennt das der Server und verwendet einfach die nächste Adresse aus seinem IP-Bereich. Sind im Unternehmen mehrere DHCP-Server im Einsatz, ist der beste Weg, beide mit den exakt gleichen Bereichen aus einem identischen Adresspool zu konfigurieren.

Die Konflikterkennung stellen Sie in den Eigenschaften von IPv4 oder IPv6 auf der Registerkarte *Erweitert* ein. Standardmäßig ist diese auf *0* gesetzt und damit nicht aktiv. Durch das Abändern dieses Wertes auf *1* oder *2* aktivieren die Server diese Erkennung und die Gefahr der Vergabe von gleichen IP-Adressen besteht nicht mehr.

Abbildg. 24.15 Verwenden der Konflikterkennung



Mit Windows Server 2012 R2 hat Microsoft diese Funktion erheblich verbessert und ermöglicht sogar eine Replikation der Daten zwischen DHCP-Servern. Der einzige Nachteil dabei ist, dass sich die Dauer der Adressvergabe etwas erhöht. Das stellt aber normalerweise kein Problem dar, vor allem Angesichts der Tatsache, dass dadurch die Ausfallsicherheit deutlich verbessert ist.

Beachtet werden muss dabei aber auch, dass alle eingesetzten DHCP-Server hinsichtlich ihrer Hardware so ausgestattet sind, dass diese den Ausfall eines Servers abfangen können. Dazu gehören neben CPU- und Speicherausstattung auch entsprechende Leistung im Netzwerk. Am besten sind in einem DHCP-Server mehrere Netzwerkkarten integriert, welche sich die Last teilen. Für jeden zusätzlichen Konflikterkennungsversuch des DHCP-Diensts verzögert sich die Adressvergabe um zusätzliche Sekunden. Aus diesem Grund sollte die Anzahl der Konflikterkennungsversuche zwei Versuche nicht übersteigen.

Ausfallsicherheit mit der 80/20-Regel

Eine weitere Möglichkeit und Strategie der Ausfallsicherheit für DHCP-Server ist die sogenannte 80/20-Regel. Diese Regel ist ähnlich der Variante, den verfügbaren Adresspool auf mehrere Bereiche aufzuteilen. Bei dieser Variante verwaltet ein DHCP-Server 80 % der Adressen des Adresspools und ein zweiter Server die restlichen 20 %. Die IP-Adressen dürfen sich in diesem Fall nicht überlappen. Fällt ein Server aus, kann der zweite Server zumindest teilweise übernehmen. Idealerweise ist der zweite Server so ausgestattet, dass er im Notfall alle Clients mit IP-Adressen versorgen kann.

Diese Variante ist zum Beispiel auch beim Einsatz mehrerer Subnetze denkbar. Auch hier lassen sich die Adressen aus den verschiedenen Subnetzen 80/20 auf verschiedene Server aufteilen. Allerdings muss bei dieser Technik der primäre Server wieder so schnell wie möglich funktionieren, damit dem Backupserver nicht die IP-Adressen ausgehen. Teilen sich mehrere DHCP-Server einen Bereich im Netzwerk, müssen Sie auf allen Servern die Reservierungen entsprechend eintragen.

Bereichsgruppierung (Superscopes)

Wenn ein DHCP-Server ausfällt, muss nicht immer das Betriebssystem oder die Hardware schuld sein. Es besteht auch die Möglichkeit, dass der Server keine IP-Adressen mehr zur Verfügung hat, weil die IP-Adressen des Bereichs erschöpft sind. Automatisch bedient sich ein DHCP-Server nämlich nicht mit den freien IP-Adressen aus weiteren Bereichen, die eventuell auf dem Server konfiguriert sind. Um diesem Problem vorzubeugen, helfen die Bereichsgruppierungen (Superscopes), die mehrere Bereiche auf einem Server unter einem Dach zusammenfassen.

Clients, die IP-Adressen anfragen, erhalten IP-Adressen aus allen Bereichen des Superscopes. Sind die IP-Adressen eines Bereichs erschöpft, erhalten Clients IP-Adressen aus einem anderen Bereich auf dem Server, der noch über freie Adressen verfügt. Dadurch besteht keine Gefahr, dass der DHCP-Server die Anfragen von Clients ablehnt, nur weil ein Bereich für IP-Adressen erschöpft ist. Der Server vergibt an Clients einfach Adressen aus anderen Bereichen innerhalb des gleichen Superscopes. In diesem Fall muss zusätzlich sichergestellt sein, dass das Routing im Unternehmen so konfiguriert ist, dass die Clients mit den neuen IP-Adressen auch alle notwendigen Server erreichen.

Mehrere IP-Bereiche auf DHCP-Servern ergeben hauptsächlich dann Sinn, wenn sich diese in verschiedenen Subnetzen befinden. Da der DHCP-Server bei der Adressvergabe aber nicht überprüft, ob das Routing noch funktioniert, ist es sinnvoll, vor der Erstellung von Bereichsgruppierungen zunächst den Routingweg im Unternehmen zu überprüfen und anzupassen, sofern dies notwendig ist. Schließlich muss sichergestellt sein, dass DHCP-Clients alle notwendigen Netzwerkverbindungen aufbauen können, unabhängig davon, welche IP-Adresse der DHCP-Server aus dem Superscope zuweist.

Ebenfalls wichtig: Sofern die Anfragen an DHCP-Server über Router erfolgen, ist es notwendig, dass die Router keine DHCP-Requestpakete blockieren, sondern diese passieren lassen. Da nicht alle Router diese Option unterstützen beziehungsweise nicht in allen Unternehmen nur wegen der DHCP-Konfiguration die Router angepasst werden können, besteht auch die Möglichkeit, ein DHCP-Relay zu verwenden.

Diese Funktion ermöglicht die Verbindung zwischen Clients und DHCP-Servern in verschiedenen Netzwerken. Dazu fordern die Clients vom DHCP-Relay eine IP-Adresse an. Das Relay ist im gleichen Subnetz positioniert wie die Clients. Anschließend fordert das DHCP-Relay vom eigentlichen DHCP-Server eine Adresse an und teilt diese dem Client zu. Der Vorgang dauert auch nicht wesentlich länger als bei der Verwendung der Konflikterkennung.

Ausfallsicherheit bei DHCP-Servern durch verschiedene Bereiche herstellen

Die Ausfallsicherheit bei DHCP-Servern herzustellen, gestaltet sich etwas schwieriger, als das zum Beispiel beim DNS oder Domänencontrollern der Fall ist. Aufgrund der laufenden und schnellen Änderungen an der DHCP-Datenbank ist eine Replikation zwischen zwei DHCP-Servern bis Windows Server 2012 R2 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.

Der häufigste Weg, um eine Ausfallsicherheit herzustellen, besteht darin, dass Administratoren den verfügbaren IP-Adresspool im Unternehmen auf verschiedene Server aufteilen. Jeder DHCP-Server erhält in diesem Fall einen eigenen Pool von IP-Adressen, der sich nicht mit dem anderen DHCP-

Server überlappen darf. Den kompletten Adresspool aufzuteilen ist aber nur dann sinnvoll, wenn ein Server allein alle Computer-IP-Adressen versorgen könnte.

Eine weitere Möglichkeit ist, auf allen Servern einen Bereich zu konfigurieren, der den gesamten Adresspool enthält. Auf jedem Server hinterlegen Sie in der DHCP-Konfiguration als Ausnahmen die IP-Adressen, welche die anderen DHCP-Server im Unternehmen verteilen sollen. Fällt ein DHCP-Server aus, lassen sich diese Ausnahmen problemlos entfernen und die noch laufenden Server übernehmen die Aufgaben des ausgefallenen Servers. Allerdings müssen bei dieser Lösung auch Reservierungen auf den Servern ihre Berücksichtigung finden.

Die Reservierungen lassen sich für jeden DHCP-Bereich getrennt auf dem Server festlegen. Benötigt zum Beispiel eine bestimmte Arbeitsstation oder ein Server immer die gleiche IP-Adresse und erhält diese per DHCP, spielen Reservierungen eine wichtige Rolle. Aus diesem Grund müssen auf allen DHCP-Servern, die als DHCP-Bereiche identische Adresspools haben, also die gleichen IP-Adressen vergeben können, auch alle Reservierungen hinterlegt sein. Dadurch ist sichergestellt, dass jeder beteiligte DHCP-Server auch alle Reservierungen kennt und an die entsprechenden Clients zuweisen kann.

Erhalten nämlich bestimmte Clients nicht die IP-Adresse, die als Reservierung vorgesehen ist, sondern durch den Ausfall eines DHCP-Servers eine andere Adresse, kann das zu unvorhergesehenen Problemen führen, zum Beispiel beim Netzwerkzugriff direkt über die IP-Adresse. Aber auch wenn der Zugriff nicht über die IP-Adresse, sondern über den DNS- oder NetBIOS-Namen erfolgt, kann es durchaus einige Zeit dauern, bis alle WINS- und DNS-Server oder lokale Konfigurationen wie HOST- und LMHOST-Dateien und vor allem die verschiedenen Zwischenspeicher auf den Servern und Arbeitsstationen mit der neuen IP-Adresse aktualisiert sind.

Daher ist es beim Einsatz von Reservierungen extrem wichtig, diese Komponente bei der Ausfallplanung zu berücksichtigen und bereits rechtzeitig festzulegen, was passieren soll, wenn der DHCP-Client nicht seine vorgesehene IP-Adresse erhält. Eine Alternative ist in diesem Fall, mit der Vergabe von statischen IP-Adressen anstatt mit Reservierungen zu arbeiten.

Standby-Server mit manueller Umschaltung

Ein weiterer Weg zur Herstellung der Ausfallsicherheit ist, einen Standbyserver für den produktiven DHCP-Server zu konfigurieren. Die Umschaltung kann jedoch nur manuell erfolgen, ein Automatismus ist bei diesem Weg nicht möglich. Der Vorteil der Lösung ist jedoch der günstige Preis im Vergleich zur hohen Ausfallsicherheit. Grundlage für einen Standby-DHCP-Server ist die Möglichkeit, DHCP mit dem Befehl Netsh zu konfigurieren.

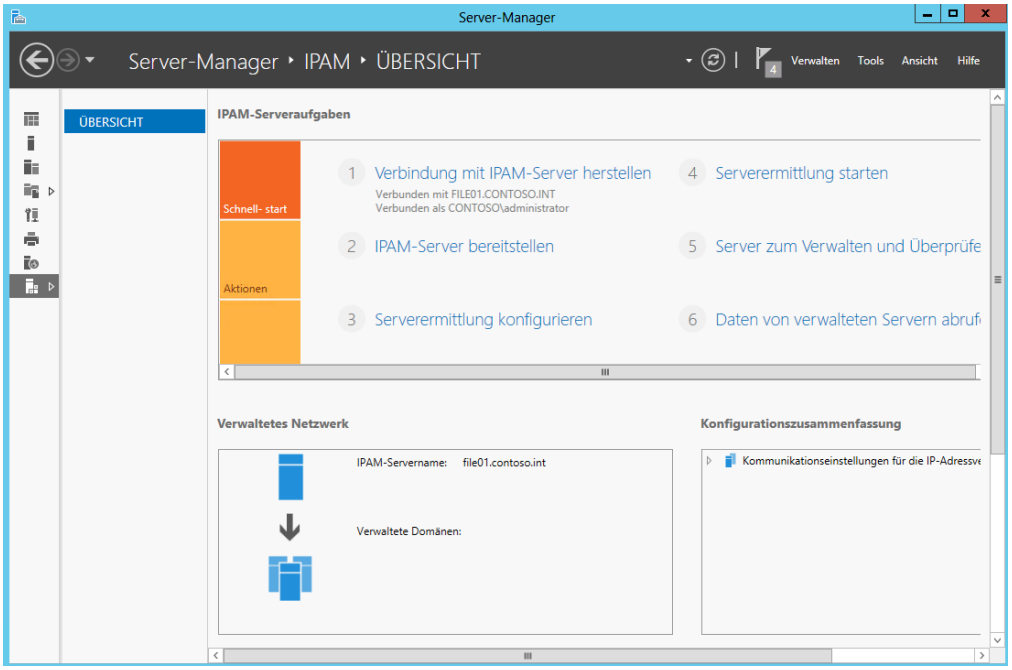
Dadurch lassen sich alle notwendigen Maßnahmen in einer Batchdatei zusammenfassen. Die Ausführung erfolgt manuell oder per geplantem Task. Mit der Batchdatei ist es möglich, die Sicherung des aktiven Servers auf den Standby-DHCP-Server zu übertragen, und das regelmäßig. Die Batchdatei verwendet dazu die Option *export* von Netsh. So lassen sich alle aktuellen Konfigurationen und aktuellen DHCP-Leases erfassen und auf den Backup-DHCP-Server kopieren.

Der zweite DHCP-Server ist in Active Directory nicht autorisiert, vergibt also keine IP-Adressen an die Clients, bis Sie entsprechende Konfigurationen vornehmen. Fällt der primäre Server aus, muss dessen Autorisierung nur noch aufgehoben und der Datenaustausch deaktiviert werden. Im Gegenzug autorisieren Sie den Backupserver, der mit der aktuellsten Konfiguration mit seiner Arbeit beginnt und IP-Adressen verteilt.

IPAM im Praxiseinsatz

Mit Windows Server 2012 R2 bietet Microsoft weitere Funktionen, um DHCP-Server stabil, sicher und hochverfügbar im Netzwerk zur Verfügung zu stellen. Eine Neuerung seit Windows Server 2012 ist IP-Adressverwaltungsserver (IPAM). Dieser Serverdienst überwacht und steuert zentral DHCP- und DNS-Server. Die Installation erfolgt als Serverfeature, die Verwaltung über Assistenten im Server-Manager.

Abbildg. 24.16 IPAM in Windows Server 2012 R2 nutzen



Der Dienst kann Änderungen und die Serverdienste zentral überwachen. Unternehmen, die zahlreiche Namenserver verwalten müssen, sollten einen Blick auf IPAM werfen. IPAM dient nicht nur der Überwachung von DNS- und DHCP-Servern, sondern bietet auch eine effiziente Verwaltungsmöglichkeit dieser Server und zwar in einer gemeinsamen Oberfläche. Microsoft geht mit der neuen Serverrolle auf die ständig wachsende Anzahl an DNS- und DHCP-Servern in Unternehmen und der damit verbundenen komplizierteren Verwaltung ein. Damit Administratoren einen Überblick über die verschiedenen IP-Adressbereiche und DNS-Domänen erhalten, sind oft Zusatztools im Einsatz oder Excel-Tabellen, in denen die Daten aufgelistet sind. Damit soll IPAM Schluss machen. IPAM verfügt im Groben über folgende Funktionen:

- Automatisches Auffinden der IP-Adressinfrastruktur im Unternehmen
- Erstellen von Berichten über die IP-Infrastruktur
- Überwachung der Infrastrukturserver im Netzwerk und der vorhandenen IP-Adressen
- Überwachung von Netzwerkzugriffschutzservern
- Überwachung von Domänencontrollern

IPAM-Grundlagen

IPAM sollte auf einem Mitgliedsserver der Domäne installiert sein. Microsoft erlaubt aber auch die Installation auf einem Domänencontroller. Bei der Bereitstellung gibt es mehrere Möglichkeiten. Administratoren können in jeder Niederlassung einen IPAM-Server installieren oder einen zentralen IPAM-Server, der alle Daten des Unternehmens sammelt. Setzen Unternehmen verschiedene IPAM-Server ein, können diese ihre Daten aber nicht untereinander austauschen. Alle Server arbeiten komplett getrennt voneinander.

IPAM hat seine Grenzen in der Gesamtstruktur. Das heißt, ein Server kann immer nur die Infrastrukturserver einer Gesamtstruktur und aller angebundenen Domänen verwalten. Der Server muss zwingend Mitglied einer Domäne in der Gesamtstruktur sein. Welche das ist, spielt keine Rolle. Außerdem lassen sich mit IPAM nur korrekt konfigurierte und funktionierende Infrastrukturserver (NPS, DC, DNS und DHCP) verwalten und überwachen. Neben Windows Server 2012 R2 kann IPAM auch Infrastrukturserver mit Windows Server 2008 und Windows Server 2012 anbinden. Externe Geräte, DHCP Relays oder WINS kann IPAM nicht überwachen. Dies gilt auch für Infrastrukturdienste aus anderen Betriebssystemen. Auch eine Überprüfung der Konsistenz der IP-Adressen mit Routern oder Switches ist nicht möglich.

Ein einzelner IPAM-Server kann bis zu 150 DCHP-Server, 500 DNS-Server, 6000 DHCP-IP-Adressbereiche, 3 Millionen IPv4-Adressen, 3 Millionen IPv6-Adressen, 40.000 DNS-Einträge und bis zu 300 DNS-Zonen überwachen.

Seine Daten speichert IPAM in einer eigenen Datenbank bis zu 3 Jahre lang. Dabei berücksichtigt der Server auch IP-Adressen-Leases und An- oder Abmeldevorgänge von Benutzern. Das Löschen der internen Windows-Datenbank von IPAM müssen Administratoren manuell in der Verwaltungskonsole vornehmen. Die IPAM-Daten liegen immer in der internen Windows-Datenbank. Es gibt keine Möglichkeit die Daten in einer externen Datenbank auszulagern, auch nicht zu Microsoft SQL-Servern.

Nach der Installation des Serverfeatures über den Server-Manager müssen Sie zunächst festlegen welchen IP-Bereich, welche Domäne oder welche Gesamtstruktur IPAM nach zu verwalteten Servern durchsuchen soll.

Den festgelegten Bereich durchsucht IPAM automatisch und bindet neue Server oder IP-Bereiche an das System an. Damit sich Infrastrukturserver mit IPAM verwalten lassen, müssen Einstellungen in der Firewall gesetzt sein. Diese können Sie manuell setzen oder über Gruppenrichtlinien. Die Regeln lassen sich über einen Assistenten erstellen und einrichten. Den Assistenten finden Administratoren im Server-Manager. Zur Kommunikation mit den verwalteten Servern im Netzwerk verwendet IPAM RPC und WMI.

Sobald die Richtlinien oder manuellen Einstellungen gesetzt sind, können Sie das Netzwerk auf kompatible Server hin untersuchen lassen. Auch diesen Vorgang starten Sie über den Server-Manager im IPAM-Bereich. Hierbei muss auch ausgewählt werden, welche Server IPAM anbinden soll. Zur Auswahl stehen Domänencontroller, DHCP-Server und DNS-Server. Diese lassen sich für jede Domäne genau auswählen. IPAM sucht über einen Zeitplan ständig nach neuen Servern im festgelegten Bereich. Den Zeitplan ändern Sie über die Windows-Aufgabe *Microsoft/Windows/IPAM/DiscoveryTask*. Für jeden einzelnen Server lässt sich festlegen, ob dieser an IPAM angebunden werden soll oder nicht. Zur Verwaltung verfügt IPAM auch über ein Rechtemodell auf Basis der Mitgliedschaft in Sicherheitsgruppen:

- **IPAM Users** Mitglieder dieser Gruppe dürfen IPAM-Daten lesen, aber keine Einstellungen ändern
- **IPAM MSM Administrators** Mitglieder dieser Gruppe dürfen lesen und schreiben. Auch IPAM-Aufgaben dürfen die Administratoren durchführen, genauso wie die Verwaltung der angebundenen Server durchführen.
- **IPAM ASM Administrators** Diese Administratoren dürfen IP-Adressbereiche verwalten und andere IPAM-Aufgaben durchführen. In dieser Gruppe sollten die Netzwerkadministratoren Mitglied sein.
- **IPAM IP Tracking Administrators** Diese Administratoren dürfen die Trackingdaten der IP-Adressen betrachten
- **IPAM Administrators** Diese Administratoren dürfen innerhalb von IPAM alle Aufgaben durchführen

IPAM verwaltet IP-Adressen in IP-Adressbereichen und fasst Bereiche zu ganzen Blöcken zusammen. Die Blöcke können Sie bearbeiten und überwachen. DNS- und DHCP-Server bindet IPAM ebenfalls an. Für DHCP-Server können Sie zum Beispiel Bereiche erstellen, Servereinstellungen ändern oder Klassen anlegen.

Auf diese Weise verwalten Unternehmen alle DHCP-Server zentral in der IPAM-Konsole. Für DNS-Server lassen sich alle Zonen anzeigen und überwachen. Die IPAM-Konsole zeigt darüber hinaus noch die gesammelten Ereignisanzeigen aller angebundenen Serverdienste an. Die komplette Verwaltung von IPAM nehmen Sie im Server-Manager vor. Hierüber lassen sich auch die einzelnen Aufgaben erstellen und verwalten.

IPAM einrichten

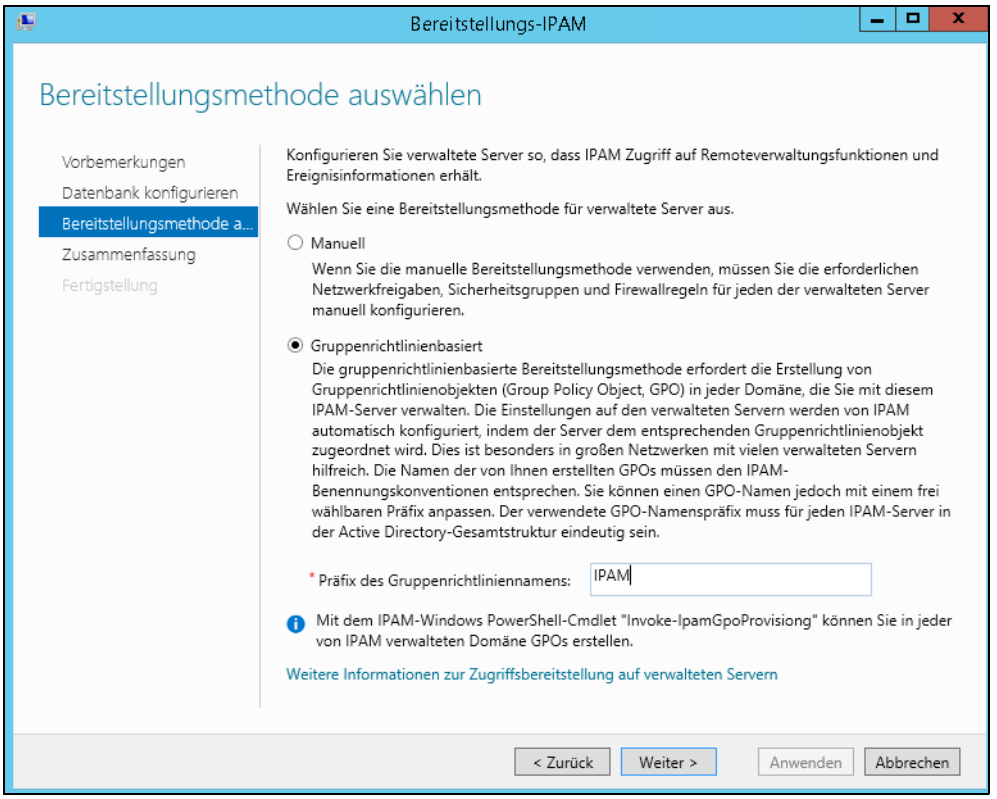
Um IPAM zu nutzen, installieren Sie das Feature IP-Anwendungsserver auf einem Server. Anschließend finden Sie im Server-Manager einen neuen Verwaltungsbereich für IPAM. Hierüber richten Sie den Server mit einem Assistenten ein.

TIPP Sie können IPAM auch über die PowerShell mit *Install-WindowsFeature IPAM -IncludeManagementTools* installieren.

Im ersten Schritt klicken Sie auf *Verbindung mit IPAM-Server herstellen*. Wählen Sie im Fenster den IPAM-Server aus, den Sie im Unternehmen bereitstellen wollen. Danach klicken Sie auf *IPAM-Server bereitstellen*. So richten Sie die IPAM-Server ein. In Windows Server 2012 R2 können Sie außerdem auswählen, ob Sie die IPAM-Datenbank auf dem lokalen Server in einer internen Windows-Datenbank (WID) oder auf einem SQL-Server speichern wollen. In den meisten Fällen reicht die interne Windows-Datenbank aber aus.

Lassen Sie auf der Seite zur Einrichtung der Bereitstellung die Option *Gruppenrichtlinienbasiert* aktiviert und geben Sie unten ein Präfix für die neue Gruppenrichtlinie ein, zum Beispiel *IPAM*.

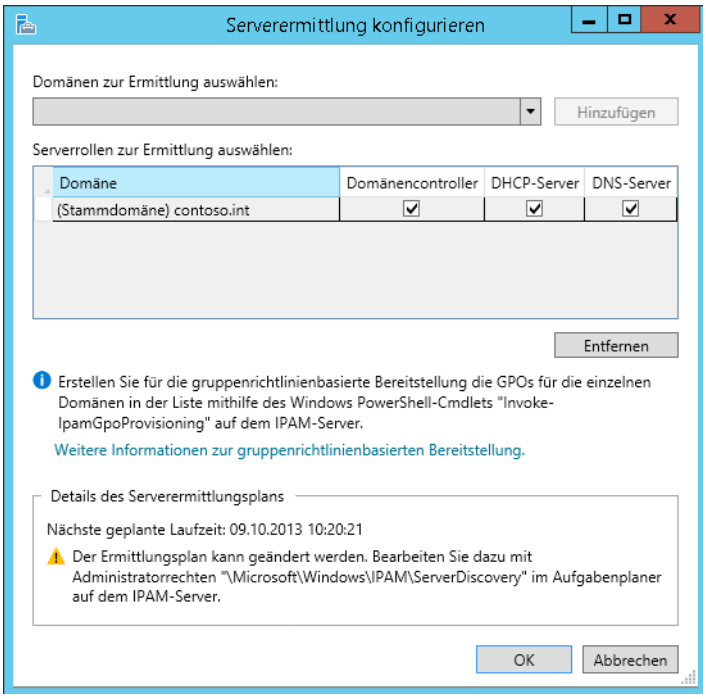
Abbildg. 24.17 IPAM-Server einrichten



Nutzen Sie die gruppenrichtlinienbasierte Einrichtung von IPAM, lassen sich alle Server automatisiert anbinden und Sie müssen nicht alle Einstellungen für jeden IPAM-Server manuell vorgeben. Klicken Sie auf der nächsten Seite auf *Anwenden* und schließen Sie damit die Einrichtung von IPAM ab.

Nachdem Sie IPAM eingerichtet haben, binden Sie die verschiedenen Infrastrukturserver an die IPAM-Struktur an. Dazu wählen Sie im Server-Manager den Punkt 3 *Serverermittlung konfigurieren*. Hier legen Sie fest, welche Domäne Sie anbinden wollen. Klicken Sie dazu auf *Hinzufügen*. Wählen Sie dann im unteren Feld aus, welche Server aus der angebundenen Domäne Sie anbinden wollen. Klicken Sie auf *OK*.

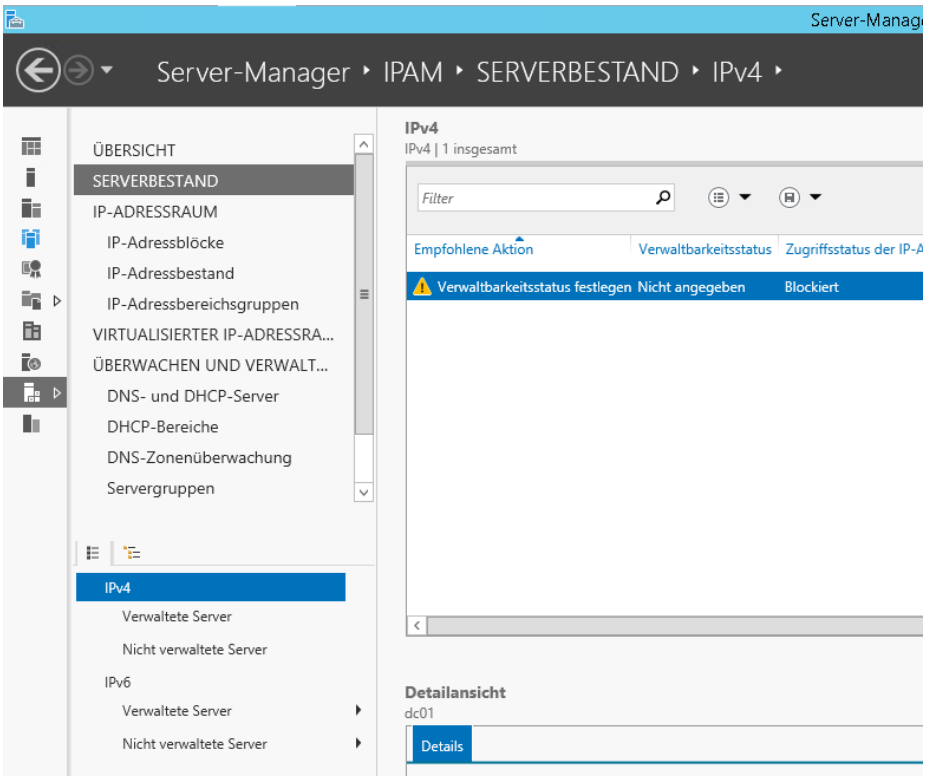
Abbildg. 24.18 Anbinden von Infrastrukturservern an IPAM



Nachdem Sie den Ermittlungsplan für die Anbindung der Server konfiguriert haben, klicken Sie in der IPAM-Übersicht auf *Server zum Verwalten und Überprüfen des IPAM-Zugriffs auswählen*. Es dauert aber eine Weile, bis der Ermittlungsplan die gefundenen Server an IPAM anbindet. Die Konsole bleibt daher zunächst leer.

Lassen Sie die Ansicht aktualisieren, sollten nach einiger Zeit die ersten Server erscheinen. Sie sehen den Status der Ermittlung, wenn Sie in der IPAM-Übersicht auf *Serverermittlung starten* und dann auf *Details* klicken. Nach dem Abschluss der Aufgabe sehen Sie die verschiedenen Server. Diese sind allerdings zunächst blockiert. Sie müssen die Verwaltung erst freischalten.

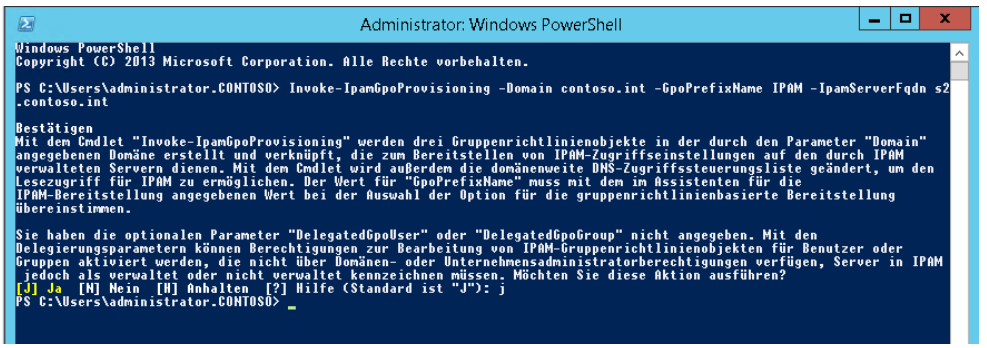
Abbildg. 24.19 Anzeigen der angebundenen Server



Damit Sie die angebundenen Server auch verwalten können, starten Sie auf dem IPAM-Server eine PowerShell-Sitzung mit Administratorrechten. Geben Sie in der PowerShell dann den folgenden Befehl ein:

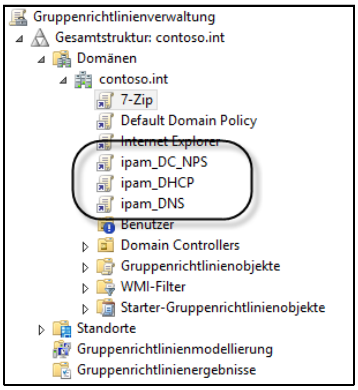
```
Invoke-IpamGpoProvisioning -Domain <Domäne> -GpoPrefixName <Präfix der GPO> -
IpamServerFqdn <IPAM-Server>
```

Abbildg. 24.20 IPAM richten Sie auch über Gruppenrichtlinien ein



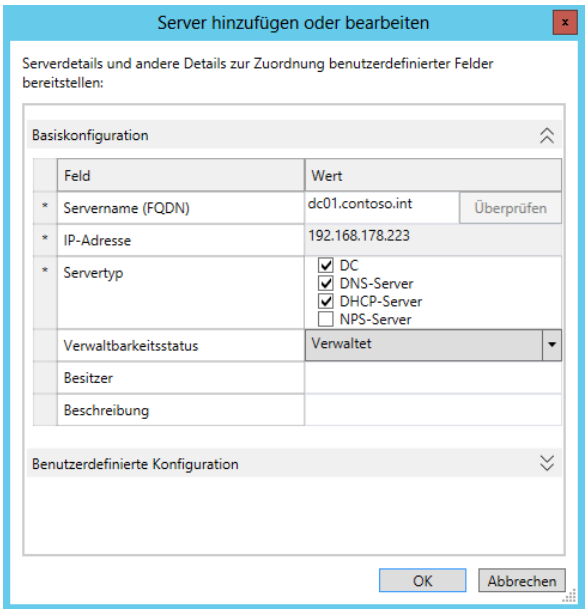
Nachdem der Befehl erfolgreich durchgelaufen ist, überprüfen Sie in der Gruppenrichtlinienverwaltung, ob neue Gruppenrichtlinien zur Anbindung von IPAM verfügbar sind. Für jede Serverrolle gibt es eine eigene Richtlinie.

Abbildg. 24.21 IPAM benötigt neue Gruppenrichtlinien zur Anbindung von Servern



Anschließend klicken Sie im Bereich *Serverbestand* mit der rechten Maustaste auf alle gefundenen Server in der IPAM-Konsole und wählen im Kontextmenü den Eintrag *Server bearbeiten* aus. Ändern Sie den *Verwaltbarkeitsstatus* auf *Verwaltet* und klicken Sie auf *OK*. Führen Sie diesen Vorgang für alle Server durch, die Sie an IPAM anbinden wollen.

Abbildg. 24.22 Anpassen der Verwaltbarkeit von Infrastrukturservern



Die Server lassen sich aber erst dann verwalten, wenn die erstellten Gruppenrichtlinien angewendet wurden (siehe Kapitel 19). Am besten geben Sie dazu auf den einzelnen Servern in der Eingabeaufforderung mit Administratorrechten *gpupdate /force* ein (siehe Kapitel 19). Lassen Sie die Ansicht aktualisieren. Stellen Sie sicher, dass der Server als verwaltet angezeigt wird. Über das Kontextmenü legen Sie auch fest, welchen Serverdienst Sie auf dem Server überwachen wollen.

Fehlerbehebung der Anbindung von IPAM-Clients

Werden Server nicht angezeigt, liegt entweder ein Problem mit der Zuordnung der entsprechenden Gruppenrichtlinie vor oder die Firewall blockiert den Zugriff. Wenn Sie einen Infrastrukturserver an IPAM angebunden und über dessen Kontextmenü eine Serverrolle ausgewählt und als verwaltet konfiguriert haben, wird dem Server eine der drei Richtlinien oder ihm werden alle drei Richtlinien zugeordnet. Führen Sie in einer Eingabeaufforderung mit Administratorrechten erneut den Befehl *gpupdate /force* aus und stellen Sie sicher, dass der Server die Richtlinien anwendet.

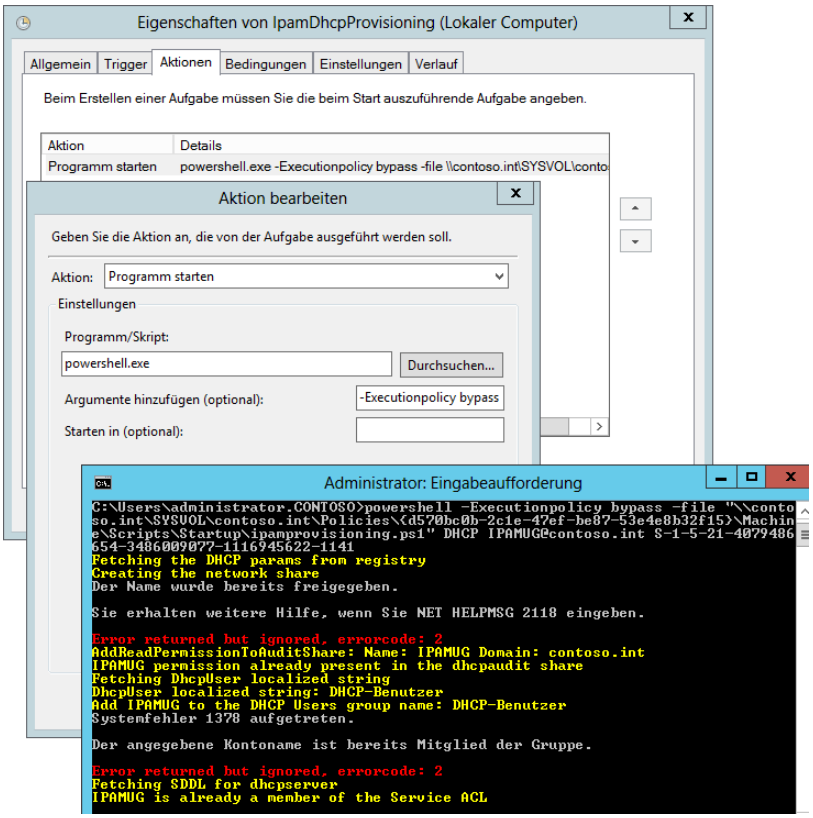
Auf dem Client finden Sie Protokolldateien, über die Sie erkennen können, warum sich ein Client nicht an IPAM anbindet. Sie finden die Dateien im Ordner *%WinDir%\temp named*. Diese tragen die Bezeichnung *IpamDhcpLog.txt* und *IpamDnsLog.txt*.

Tippen Sie anschließend auf der Startseite *Aufgabe* ein und starten Sie die Aufgabenplanung. Klicken Sie auf *Aufgabenplanungsbibliothek*, sehen Sie die Aufgabe, welche über die Gruppenrichtlinie erstellt wird, um den Server an IPAM anzubinden. Über das Kontextmenü rufen Sie deren *Eigenschaften* auf. Auf der Registerkarte *Aktionen* sehen Sie in der Aufgabe, welchen Befehl die Aufgabe ausführen will. Um zu überprüfen, ob die Aufgabe funktioniert, gehen Sie folgendermaßen vor:

1. Öffnen Sie auf dem Client eine Eingabeaufforderung mit Administratorrechten.
2. Geben Sie den Befehl *powershell* ein und bestätigen Sie aber nicht.
3. Tragen Sie hinter *powershell* den Befehl aus der Spalte *Argumente hinzufügen* ein. Sie können diesen in die Zwischenablage kopieren und in die Eingabeaufforderung einfügen.
4. Setzen Sie Anführungszeichen zwischen der Option *–file* und am Ende von *ipamprovisioning.ps1* und führen Sie den Befehl aus.
5. Erhalten Sie die Meldung, dass die Optionen bereits gesetzt sind, funktioniert das Skript. Erhalten Sie andere Fehler, haben Sie einen Ansatz, woran das Problem liegt. Meistens liegt das an bestimmten Firewalleinstellungen.

Damit ein Server von IPAM überwacht werden kann, muss dieser in der IPAM-Konsole als verwaltbar markiert sein und die Gruppenrichtlinie anwenden. Erst wenn ein Server mit allen überwachten Serverrollen mit dem Status *Blockierung aufgehoben* angezeigt wird, unterstützt der IPAM. Überprüfen Sie auch in den Firewalleinstellungen auf den Clients, ob IPAM eingetragen und der Verkehr nicht blockiert wird.

Abbildg. 24.23 Überprüfen des IPAM-Skripts eines Servers



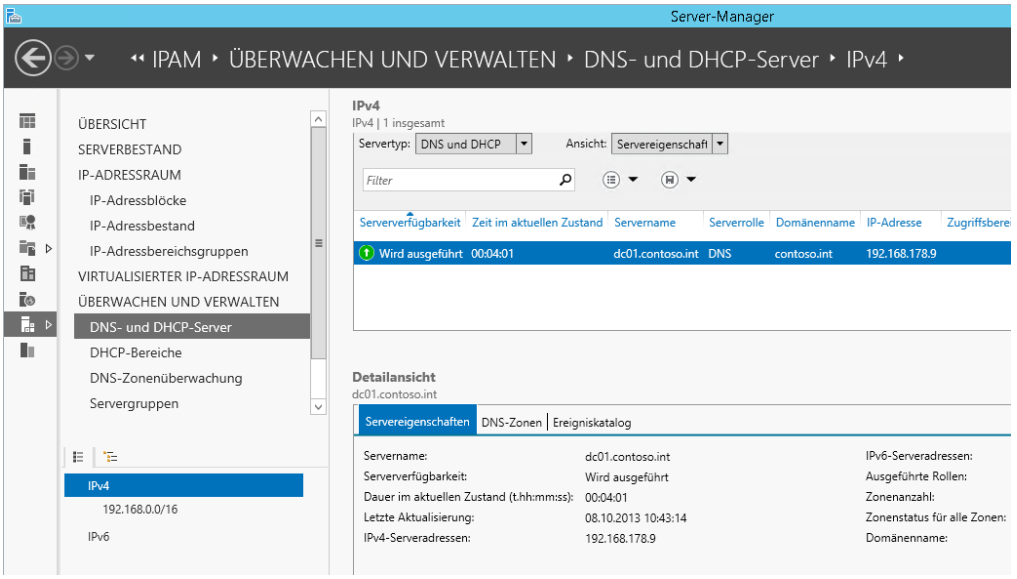
IPAM arbeitet auf den angebundenen Servern und den IPAM-Servern selbst mit Aufgaben, die bestimmte Konfigurationen vornehmen. Zur Verwaltung des Diensts können Sie diese Aufgaben auch anpassen oder überwachen. Sie finden diese Aufgaben in der Aufgabenplanung unter *Microsoft/Windows/IPAM*. Wichtig sind vor allem die folgenden Aufgaben:

- **DiscoveryTask** Ermittelt die Domänencontroller, DHCP- und DNS-Server in der Gesamtstruktur. Die Aufgabe startet einmal am Tag.
- **AddressUtilizationCollectionTask** Die Aufgabe sammelt Daten zur Adressraumverwendung von den angebundenen DHCP-Servern und startet alle zwei Stunden.
- **AuditTask** Sammelt Überwachungsinformationen von DHCP- und IPAM-Servern sowie IP-Leaseüberwachungsprotokolle von NPS- und DC-Servern. Die Aufgabe startet ebenfalls einmal am Tag.
- **ConfigurationTask** Sammelt Überwachungsinformationen von DHCP- und DNS-Servern. Die Aufgabe startet alle sechs Stunden.
- **ServerAvailabilityTask** Sammelt den Dienstverfügbarkeitsstatus für DHCP- und DNS-Server alle 15 Minuten.

Infrastrukturüberwachung und -verwaltung

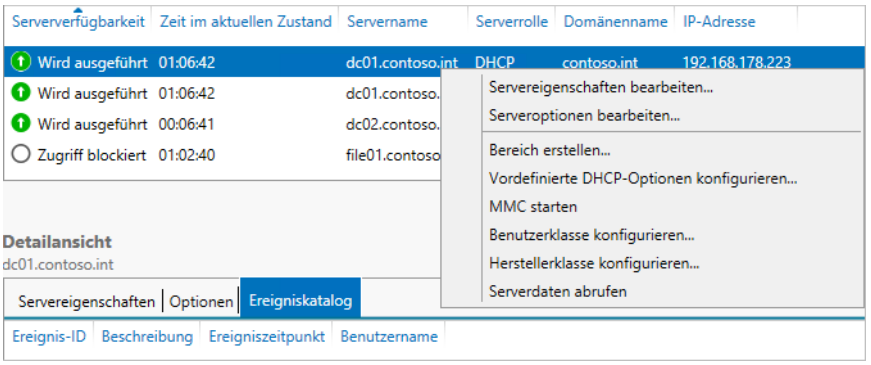
Klicken Sie im IPAM-Navigationsbereich unter *ÜBERWACHEN UND VERWALTEN* auf *DNS- und DHCP-Server*. Neben *Servertyp* können Sie einen der Einträge *DNS*, *DHCP* oder *DNS und DHCP* auswählen. Angezeigt werden die Serververfügbarkeit, die Dauer im aktuellen Zustand, der Servername, die Serverrolle, der Domänenname und die IP-Adresse.

Abbildg. 24.24 Überwachen von Servern mit IPAM



Klicken Sie auf einen DHCP-Server und überprüfen Sie unter *Detailansicht* die Informationen auf den Registerkarten *Servereigenschaften*, *Optionen* und *Ereigniskatalog*. Klicken Sie mit der rechten Maustaste auf den DHCP-Server. Sie können den DHCP-Server direkt über die IPAM-Konsole konfigurieren.

Abbildg. 24.25 Verwalten von Servern aus der IPAM-Konsole



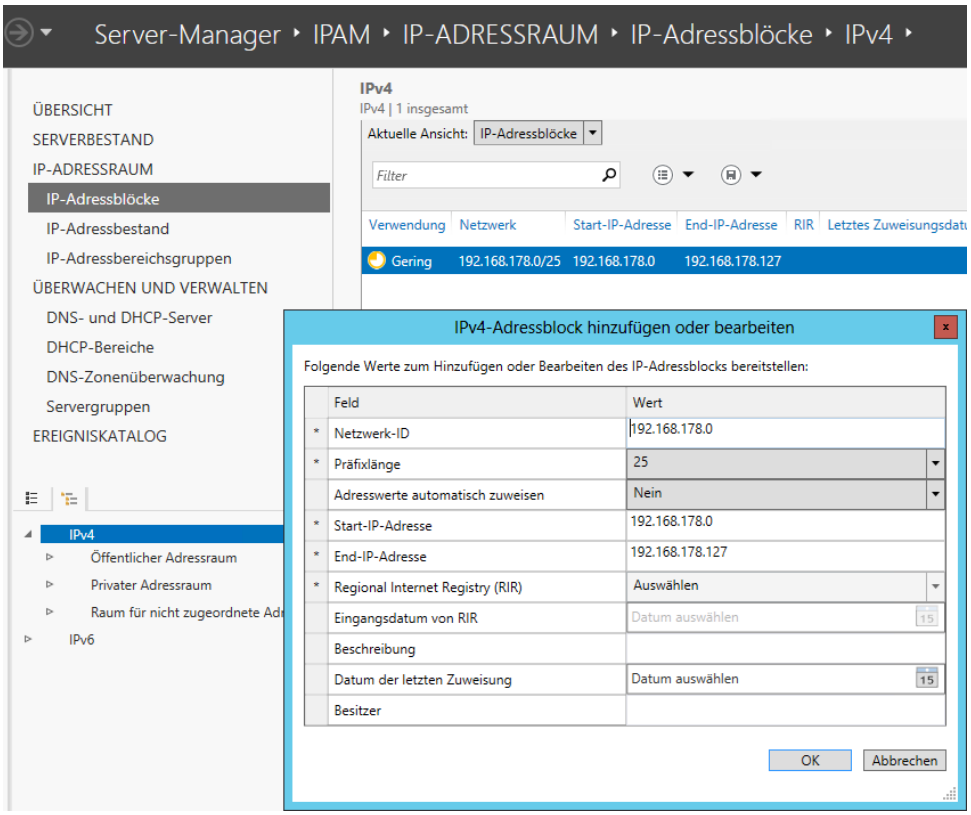
Wählen Sie neben *Servertyp* die Option *DHCP* und dann neben *Ansicht* die Option *Bereichseigenschaften* aus. Klicken Sie mit der rechten Maustaste auf den DHCP-Bereich und dann im Kontextmenü auf *DHCP-Bereich duplizieren*, können Sie Bereiche kopieren. Auf dem gleichen Weg überwachen Sie die angebundenen DNS-Server und deren Zonen. Neben der Überwachung können Sie noch IP-Gruppen definieren, die mehrere DHCP-Server zusammenfassen.

IP-Adressblöcke mit IPAM

IP-Adressblöcke in IPAM sind größere Bereiche aus IP-Adressen. IP-Adressbereiche sind kleinere Bereiche aus IP-Adressen, diese entsprechen einem DHCP-Bereich. IP-Adressbereiche werden in IPAM zu IP-Adressblöcken zugeordnet. Diese Zuordnung nehmen Sie in der IPAM-Konsole vor:

1. Klicken Sie im IPAM-Navigationsbereich auf *IP-Adressblöcke*.
2. Klicken Sie im unteren Navigationsbereich mit der rechten Maustaste auf *IPv4* und dann auf *IP-Adressblock hinzufügen*.
3. Wählen Sie die Netzwerk-ID und die Präfixlänge aus, also das Subnetz.
4. Klicken Sie auf *OK* und wählen Sie dann neben *Aktuelle Ansicht* die Option *IP-Adressblöcke* aus. Über das Kontextmenü bearbeiten Sie Adressblöcke nachträglich.

Abbildg. 24.26 Verwalten von IP-Adressblöcken



Auf der Registerkarte *Konfigurationsdetails* im unteren Bereich der Konsole sehen Sie bei *Verwendete Adressen*, dass zurzeit IP-Adressen verwendet werden. Das sind ausgestellte Leases von DCHP-Servern, die an IPAM angebunden sind.

Wählen Sie neben *Aktuelle Ansicht* die Option *IP-Adressbereiche* aus. Überprüfen Sie die auf der Registerkarte *Konfigurationsdetails* angezeigten Informationen. Hier sollten die Bereiche der angebundenen DHCP-Server zu sehen sein.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie einen DHCP-Server effizient und sicher im Netzwerk betreiben. Auch über die Ausfallsicherheit von DHCP durch den Betrieb mehrerer DHCP-Server konnten Sie in diesem Kapitel mehr erfahren. Ebenfalls Bestandteil des Kapitels war der neue MAC-Filter von Windows Server 2012 R2 sowie die neuen Funktionen zur Ausfallsicherheit von DHCP in Windows Server 2012 R2. Und auch auf den neuen IP-Adressenverwaltungsserver (IPAM) sind wir in diesem Kapitel eingegangen.

Im nächsten Kapitel gehen wir auf den Betrieb von DNS-Servern mit Windows Server 2012 R2 ein.

Kapitel 25

DNS einsetzen und verwalten

In diesem Kapitel:

DNS spielt auch in Windows Server 2012 R2 zur Namensauflösung eine wichtige Rolle. In den vorangegangenen Kapiteln 10 bis 17 sind wir bereits bei der Einrichtung von Active Directory auf DNS eingegangen. Allerdings bietet der DNS-Server unter Windows Server 2012 R2 noch wesentlich mehr Funktionen, als für einzelne Active Directory-Domänen die Namensauflösung zur Verfügung zu stellen.

DNS wird unter Windows Server 2012 R2 weiterhin als Serverrolle installiert und konfiguriert. Für die Einrichtung von Active Directory muss diese Rolle nicht zwingend installiert sein, da der Server-Manager in diesem Fall DNS automatisch mitinstalliert. Unabhängig davon, ob ein DNS-Server Active Directory-Zonen verwaltet, kann er beliebig weitere DNS-Domänen in verschiedenster Ausprägung verwalten.

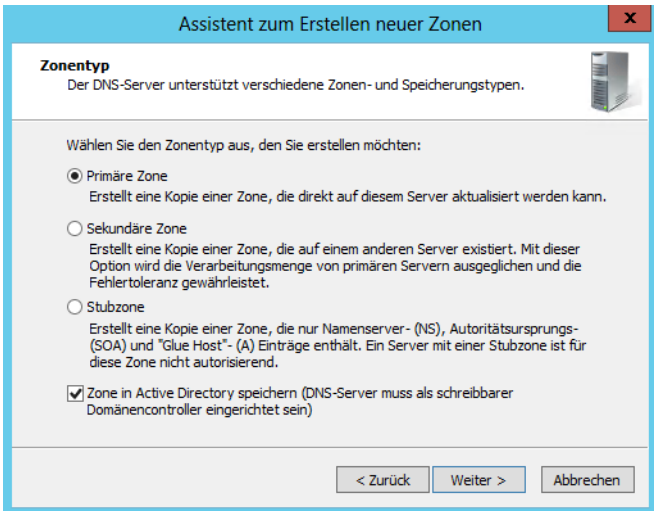
Erstellen von Zonen und Domänen

In diesem Abschnitt zeigen wir Ihnen, wie Sie manuell Zonen, Domänen und Einträge erstellen können. Clients, die den DNS-Server verwenden, können Abfragen dieser Zonen durchführen.

Erstellen von neuen Zonen

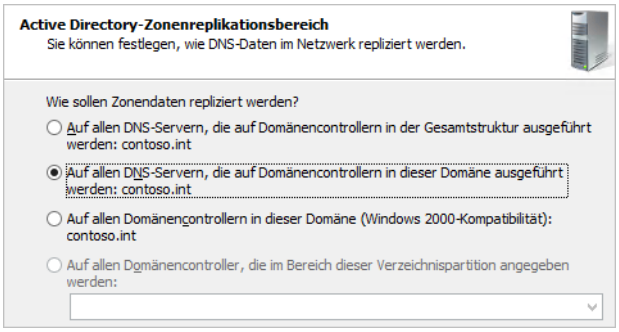
Über das Menü zur Verwaltung von DNS können Sie verschiedene Zonen erstellen. Forward-Lookupzonen übersetzen DNS-Namen in IP-Adressen. Eine Reverse-Lookupzone übersetzt dagegen IP-Adressen in DNS-Namen. Lesen Sie dazu auch die Kapitel 10 bis 17 durch. Nur auf Domänencontrollern kann mit den Active Directory-integrierten Zonen gearbeitet werden. Unterschieden wird weiterhin zwischen primären und sekundären Zonen sowie 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 mit Active Directory-integrierten Zonen arbeiten sollten. Das bedeutet in der Konsequenz allerdings, dass die DNS-Serverdienste immer auf Domänencontrollern installiert werden müssen. Mehr zum Thema lesen Sie in den Kapiteln 10 bis 17.

Abbildg. 25.1 Festlegen des Zonentyps



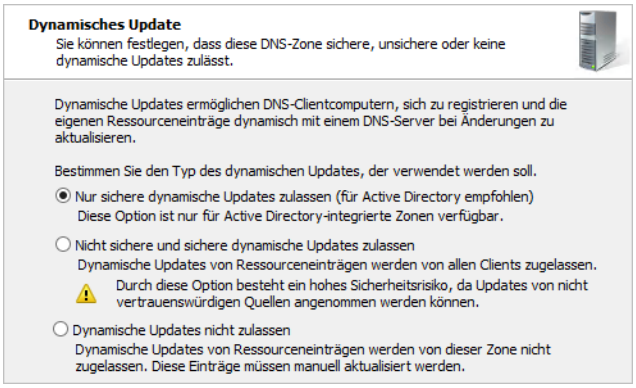
Speichern Sie eine Zone in Active Directory, legen Sie fest, auf welche DNS-Server in der Gesamtstruktur diese Zone repliziert werden soll. Dieses Fenster erscheint aber nur, wenn eine Zone in Active Directory gespeichert ist. Die Reihenfolge der folgenden Fenster kann variieren, abhängig davon, welche Einstellungen Sie wählen.

Abbildg. 25.2 Festlegen des Replikationsbereichs für eine DNS-Zone



Der nächste Schritt ist die Festlegung des Zonennamens. Als Nächstes legen Sie fest, ob die Zone dynamische DNS-Einträge erlaubt und welche Bedingungen dafür zutreffen müssen. 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. 25.3 Festlegen der dynamischen Updates für eine DNS-Zone



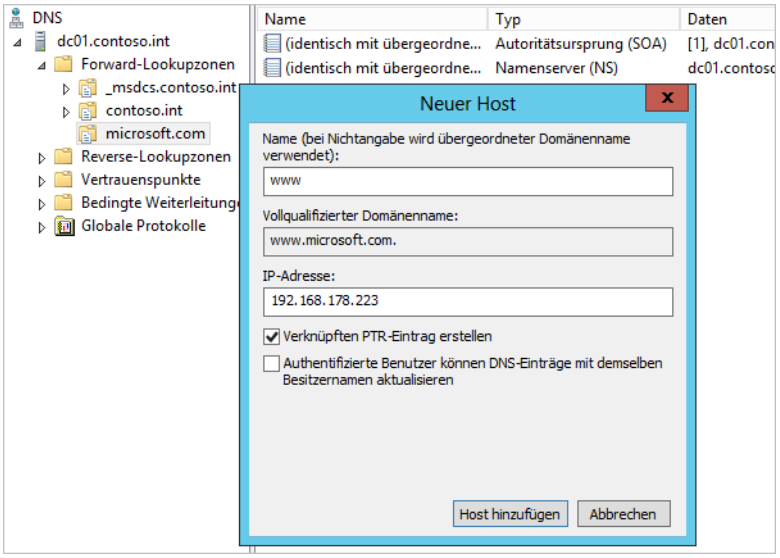
Bei den Einstellungen für die Reverse-Lookupzone müssen Sie die Netzwerkkennung eingeben. Diese wird automatisch in den Namen der Reverse-Lookupzone umgesetzt. Diese Art von Zonen hat vorgegebene Namen. Falls mehrere IP-Subnetze zu der von Ihnen verwendeten Forward-Lookupzone gehören, müssen Sie mehrere Reverse-Lookupzonen erstellen.

Erstellen von statischen Einträgen in der DNS-Datenbank

Die Administration der DNS-Server erfolgt über den Server-Manager durch Aufruf des Befehls *DNS* im Menü *Tools*. 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. 25.4 Erstellen von neuen statischen Hosteinträgen



Wenn Sie mit der rechten Maustaste auf eine Zone klicken, stehen Ihnen verschiedene Möglichkeiten zur Verfügung, um 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 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. Der AAAA-Eintrag enthält eine IPv6-Adresse, ein Host-A-Eintrag enthält eine IPv4-Adresse.
- **Neuer Alias (CNAME)** Dieser Menübefehl 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 Domäne 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 von Active Directory erstellen wollen, können Sie unterhalb der bereits erstellten Rootdomäne eine Unterdomäne erstellen oder eine eigene Zone, die allerdings getrennt verwaltet werden muss. In den Kapiteln 10 bis 17 gehen wir ausführlich auf diese Themen ein.
- **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 ergibt Sinn, wenn Sie eine Unterdomäne erstellten wollen, aber ein anderer DNS-Server in einer anderen Niederlassung für diese Zone zuständig sein soll.

HINWEIS Wird der erste Domänencontroller einer neuen untergeordneten Domäne erstellt, richtet der Assistent unter Windows Server 2012 R2 automatisch eine Delegation auf dem übergeordneten DNS-Server ein.

- **Weitere neue Einträge** Zusätzlich zum MX-Record können Sie weitere Servicerecords eintragen. Diese werden aber nur in Ausnahmefällen benötigt und nicht für den Betrieb von Active Directory.

Einstellungen und Verwalten von Zonen

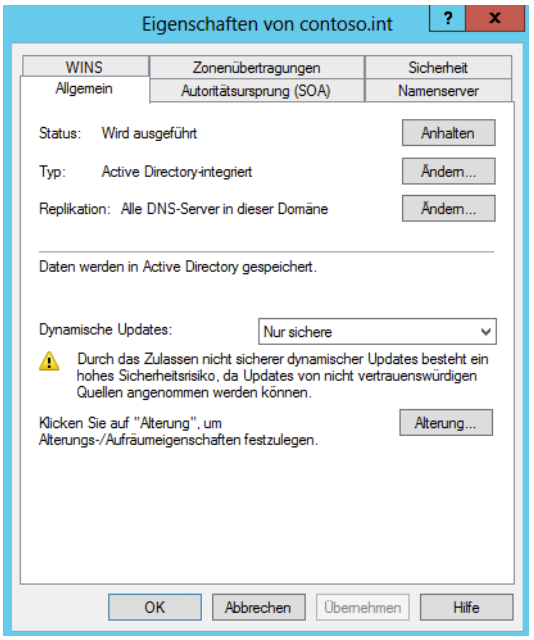
Wenn Sie die Eigenschaften einer Zone aufrufen, stehen Ihnen verschiedene Registerkarten zur Verfügung, auf denen Sie die Konfiguration der Zone anpassen können. Die Registerkarte *WINS* ist ausführlich im Kapitel 26 besprochen.

Die Registerkarte *Sicherheit* dient zur Konfiguration der Sicherheitseinstellungen und der Berechtigungen für die Verwaltung der Zone. Hier können Sie Einstellungen vornehmen, um die Berechtigungsstruktur anzupassen, damit einige Benutzergruppen oder Administratoren zwar Informationen der Zone lesen, aber keine Informationen schreiben dürfen.

Allgemeine Einstellungen für DNS-Zonen

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 sinnvoll sein, wenn Sie neben den sicheren auch unsichere Aktualisierungen zulassen. Die Namensauflösung in Microsoft-Netzwerken ist ausgesprochen bedeutsam. 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 Active Directory integrieren.

Abbildg. 25.5 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 Computer, die irgendwann mal in Betrieb waren, sich dynamisch registriert haben und irgendwann wieder außer Betrieb genommen wurden.

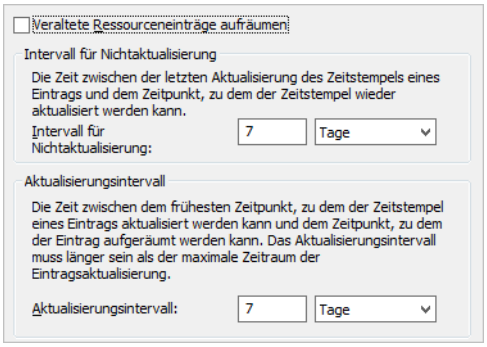
Die zugehörigen DNS-Einträge verbleiben allerdings in der Datenbank und erhöhen natürlich den Platzbedarf, die Zeit für Suchen in der Datenbank sowie die Übertragungszeiten bei der Replikation zu anderen DNS-Servern. Um diesem Wachstum Einhalt zu gebieten, sollten Sie die Alterung der dynamischen Einträge 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 sogenannten 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. 25.6 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.

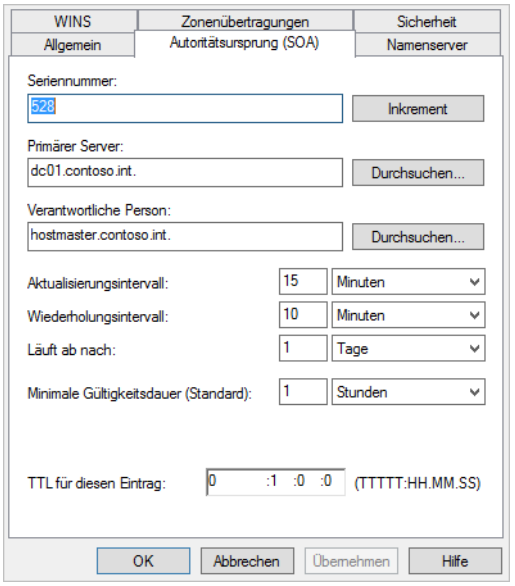
Autoritätsursprung (SOA) von DNS-Zonen

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. 25.7 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. 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.int*. 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 nach* 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.

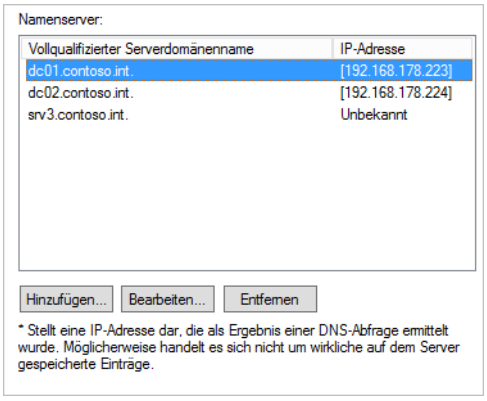
Eine Einstellung von drei Tagen dagegen hätte die Daten bis Montag Nachmittag gültig sein lassen. Um die bei DNS-Abfragen entstehende Datenmenge zu reduzieren, werden die Ergebnisse auf Clients wie auf DNS-Servern in einem Cache zwischengespeichert. Wie lange sie gespeichert werden, wird über die TTL (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.

Namenserver einer DNS-Zone verwalten

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 Namensservereintrag 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. 25.8 Konfigurieren der Namenserver 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.

Zonenübertragungen für DNS-Zonen zulassen

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.

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.

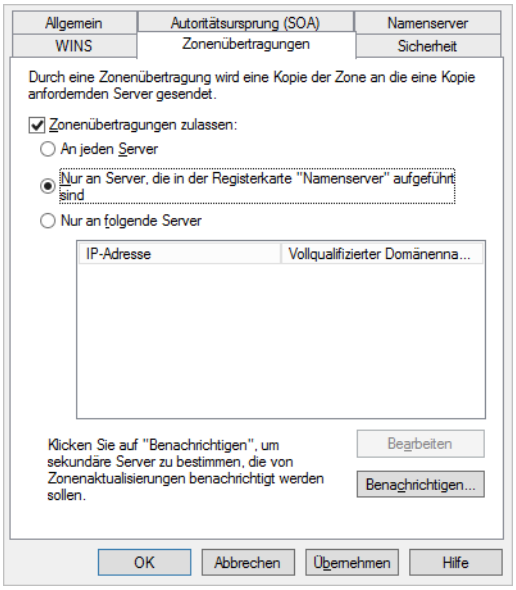
Der klassische Replikationsprozess sieht vor, dass ein sekundärer DNS-Server zunächst das Replikationsintervall aus dem SOA-Eintrag der Zone ausliest und dann in diesem Intervall den primären DNS-Server nach der aktuellen Versionsnummer der Zonendatenbank fragt. Diese Methode birgt allerdings zwei Risiken:

1. 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.
2. 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 Pullverfahren, 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.

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.

Abbildg. 25.9 Konfigurieren der DNS-Zonenübertragungen an andere DNS-Server



Verwalten der Eigenschaften eines DNS-Servers

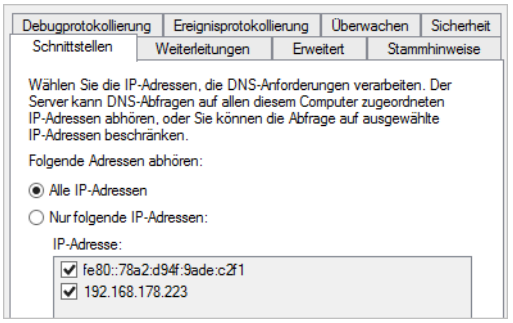
Neben den Eigenschaften der einzelnen Zonen, die Sie über das Kontextmenü aufrufen können, stehen auch in den Eigenschaften des DNS-Servers selbst einige Möglichkeiten zur Konfiguration zur Verfügung. Wir gehen im folgenden Abschnitt ausführlicher auf die einzelnen Registerkarten in den Eigenschaften eines DNS-Servers ein.

Schnittstellen eines DNS-Servers verwalten

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 die gewünschte Adresse aus.

Abbildg. 25.10 Auswählen der Netzwerkschnittstellen eines DNS-Servers



Erweiterte Einstellungen für einen DNS-Server

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 einen Fehler zurückgeben** 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
- **Roundrobin aktivieren** Die einfachste Form der Lastverteilung auf mehrere Computer wird als DNS-Roundrobin 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 der Ausfallsicherheit dienen sollen. Wenn Sie die Funktion lediglich für bestimmte Typen deaktivieren möchten, 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 Roundrobin 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 Roundrobin 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.
- **DNSSEC-Überprüfung für Remoteantworten aktivieren** Diese Option ist automatisch gesetzt und stellt sicher, dass der DNS-Server auch DNSSEC unterstützt. Wir kommen in einem eigenen Abschnitt noch ausführlicher zu diesem Thema.

Zonendaten beim Start des DNS-Servers einlesen

Welche Zonendaten der DNS-Server bei seinem Start einliest, erfährt er in der Regel aus Active Directory und der Registry. Wenn kein Active Directory verwendet wird, können Sie die Einstellung auch auf *Von 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 Ordner *%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.

Protokollierung für DNS konfigurieren

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.
- **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 steht. 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.

Ereignisprotokollierung konfigurieren

Wie Sie in der Standardanzeige der Verwaltungskonsole bereits sehen, verfügt der DNS-Server über einen eigenen Abschnitt im Ereignisprotokoll (*Anwendungs- und Dienstprotokolle/DNS Server*). Sie können die Ereignisse aber auch direkt in der DNS-Konsole abrufen.

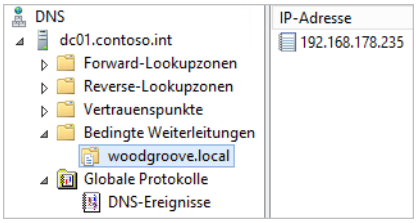
Über die Registerkarte *Ereignisprotokollierung* definieren Sie, welche Ereignisse in dieses Protokoll geschrieben werden. Wählen Sie unter *Folgende Ereignisse protokollieren* die gewünschte Option:

- **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 Diensts, 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 verwenden

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. In den Kapiteln 10 bis 17 gehen wir auf diese Thematik ebenfalls ein.

Abbildg. 25.11 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.

Damit die Benutzer und Server eine Verbindung ins Internet herstellen können, müssen Sie dafür sorgen, dass die Domänennamen 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 verwen-

den. Die Active Directory-DCs fragen die DNS-Server Ihres Internetproviders nach DNS-Zonen, für die sie nicht selbst zuständig sind, oder verwenden 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 den Firewalls 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 der Firewall 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.

Konfigurieren 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. Sekundäre DNS-Server können Anfragen von Benutzern beantworten, verwalten aber keine eigene Zone, sondern erhalten Zonen von übergeordneten (primären) DNS-Servern. Haben Sie die Zonen in Active Directory integriert, gibt es nur primäre DNS-Server, da hier alle Server gleichgestellt sind.

Ein primärer DNS-Server kann aber auch für andere Zonen als sekundärer DNS-Server dienen. Die Konfiguration erfolgt pro Zone, nicht pro Domäne:

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.
3. Anschließend müssen Sie 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. In diesem Fall wählen Sie einfach einen der bereits vorhandenen sekundären DNS-Server aus. Die Liste wird anschließend, beginnend mit dem obersten Eintrag, 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.

Falls Sie den Transfer manuell (außerhalb des regulären Intervalls) starten wollen, wählen Sie im Kontextmenü der Zone den Eintrag *Übertragung vom Master*. Danach wird ermittelt, ob es neue Einträge gibt, die anschließend angefordert werden. Der Eintrag *Neue Kopie der Zone 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.

DNS-Troubleshooting

In den meisten Netzwerken, vor allem beim Einsatz von Active Directory, hängen Fehler in den meisten Fällen von der DNS-Konfiguration ab. 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 als Reverse-Lookup bezeichnet. Da viele Serverdienste von einer sauberen Namensauflösung abhängen, funktionieren diese nicht mehr richtig wenn das DNS-System nicht korrekt konfiguriert oder sogar fehlerhaft ist. Computernamen im DNS bestehen nicht nur aus einem NetBIOS-Namen, wie zum Beispiel *dc01*, sondern zusätzlich aus dem Domänennamen, wie zum Beispiel *contoso.com*. Einen vollständigen Rechnernamen bezeichnet man auch als voll qualifizierten Domänennamen (Full Qualified Domain Name, FQDN). Der FQDN eines Servers *dc01* in der Domäne *contoso.com* lautet *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 sogenannten 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 sein.

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 sind. 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. Aber auch Active Directory legt solche SRV-Einträge an. 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.

Überprüfung und Fehlerbehebung der DNS-Einstellungen

Funktioniert die Namensauflösung nicht, sollten Sie strukturiert vorgehen, um Fehler zu finden. Auch wenn der Fehler im ersten Blick nichts mit DNS zu tun hat, lohnt es sich, zu überprüfen, ob sich Namen korrekt auflösen lassen. Überprüfen Sie, ob sich der Server sowohl in der Forward- als auch in der Reverse-Lookupzone korrekt eingetragen hat. Öffnen Sie danach eine Eingabeaufforderung 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 Eingabeaufforderung.

2. Sollte der Fehler weiterhin auftreten, überprüfen Sie, ob das primäre DNS-Suffix auf dem Server mit dem Zonennamen der DNS-Zone übereinstimmt.
3. Stellen Sie als Nächstes fest, ob die IP-Adresse des Servers stimmt und der Eintrag des bevorzugten DNS-Servers in den IP-Einstellungen korrekt ist.
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.

Wenn sich ein Servername mit Nslookup nicht auflösen lässt, gehen Sie auch hier am besten Schritt für Schritt vor:

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?

In Ausnahmefällen kann es vorkommen, dass die Aktualisierung der Reverse-Lookupzone nicht funktioniert hat. In diesem Fall ist der Server zwar in der Forward-Zone hinterlegt, aber nicht in der Reverse-Zone. 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, 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 können von dem lokalen Rechner aus auch andere DNS Server mit der Auflösung befragen. Geben Sie dazu in der Eingabeaufforderung die Anweisung *nslookup <host><server>*, also zum Beispiel *nslookup dc02.microsoft.com dc01.contoso.com* ein. Bei diesem Beispiel versucht *nslookup* den Host *dc02.microsoft.com* mithilfe 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.

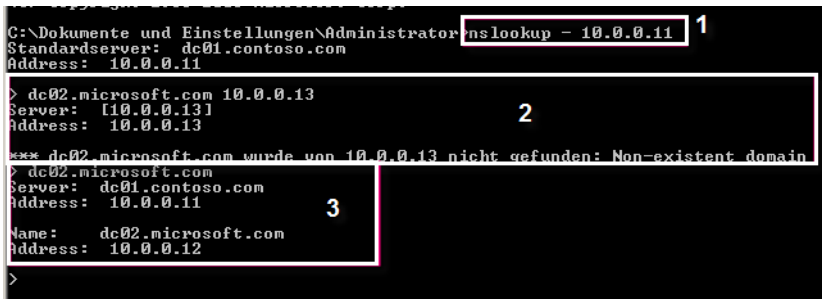
Wenn Sie als Servereintrag bei dieser Eingabeaufforderung einen DNS-Server mit seinem FQDN eingeben, setzt dies voraus, dass der DNS-Server, den der lokale Rechner verwendet, zwar nicht den Host *dc02.microsoft.com* auflösen kann, aber dafür den Server *dc01.contoso.com*. Der DNS-Server *dc01.contoso.com* 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 aufdecken. 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 Name oder die IP-Adresse des DNS-Servers ist, den Sie befragen wollen, zum Beispiel *nslookup –server 10.0.0.11*. Sie können die beiden Optionen auch kombinieren.

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. 25.12 Diagnose von DNS-Problemen mit Nslookup



Nslookup startet in der Eingabeaufforderung und ist so konfiguriert, dass das Tool den DNS-Server 10.0.0.11 zur Namensauflösung verwendet.

Nslookup überprüft, ob der lokal konfigurierte DNS-Server in seiner Reverse-Lookupzone die IP-Adresse 10.0.0.11 zu einem Servernamen auflösen kann (1). Da das funktioniert, zeigt die Ausgabe als Standardserver für diese Nslookup-Befehlszeile den DNS-Server 10.0.0.11 mit seinem FQDN *dc01.contoso.com* an. 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 Servername (Reverse).

In der nächsten Zeile (2) soll der Rechnername *dc02.microsoft.com* vom Server 10.0.0.13 aufgelöst werden. Der Server 10.0.0.13 kann jedoch den Servername *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 (3). Der Standardserver kann den Servernamen problemlos auflösen, was zeigt, dass diese Konfiguration in Ordnung ist.

Zusätzlich können Sie mit Nslookup auch die SRV-Records von Active Directory überprüfen. Clients können im DNS nachfragen, welcher Host im Netzwerk für die einzelnen Serverdienste verantwortlich ist. Active Directory baut stark auf diese SRV-Records auf. Aus diesem Grund ist eine Diagnose dieser Einträge mit Nslookup durchaus sinnvoll. Alle SRV-Records von Active Directory befinden sich parallel in der Datei *\%WinDir%\System32\config\netlogon.dns*. Die Datei lässt sich mit einem Editor auch anzeigen. Fehlen Einträge in den DNS-Zonen, die Active Directory benötigt, ist es meist hilfreich, wenn Sie den Befehl *dcdiag /fix* ausführen. Dabei versucht das Tool, auch fehlende Einträge aus der Datei *netlogon.dns* einzubauen.

Ipconfig für DNS-Diagnose verwenden

Ein weiteres wichtiges Tool ist Ipconfig, welches ebenfalls zum Lieferumfang von Windows Server 2012 R2 gehört. Vor allem die beiden Optionen */registerdns* und */flushdns* sollten jedem Administrator bekannt sein, der einen DNS-Server verwaltet.

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-Server 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 Eingabeaufforderung 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 Fehlerbehebung diesen Cache ebenfalls löschen lassen. Sie finden diese Möglichkeit im Kontextmenü des DNS-Servers im Snap-In *DNS*.

Startet ein Windows-Client, 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 neu booten wollen, können Sie in der Eingabeaufforderung mit dem Befehl *ipconfig/registerdns* eine manuelle Aktualisierung der Einträge auf dem DNS durchführen.

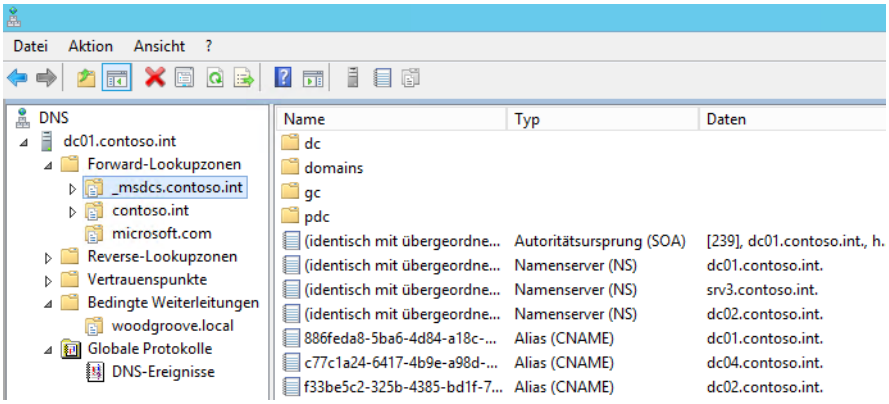
Nach der Eingabe des Befehls sollten die Einträge recht schnell auf dem DNS aktualisiert sein. Sollte das dynamische Aktualisieren noch immer nicht funktionieren, überprüfen Sie in den Eigenschaften der Zone, ob die dynamische Aktualisierung aktiviert ist. Wenn sich an der Zone auch Arbeitsstationen und Server dynamisch registrieren sollen, die nicht Mitglied der Gesamtstruktur sind, können Sie auch die Option *Nicht sichere und sichere* aktivieren.

Probleme bei der Replikation durch fehlerhafte DNS-Konfiguration – DNSLint

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 sogenannte 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 Knoten *_msdcs* zu finden.

Abbildg. 25.13 DNS-DSA-Objekte von Domänencontrollern



Der CNAME ist die GUID dieses DSA-Objekts. Domänencontroller versuchen, Ihren Replikationspartner nicht mit dem herkömmlichen Host-A-Eintrag aufzulösen, sondern mit dem hinterlegten CNAME. Ein Domänencontroller versucht 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 zur Verfügung, mit denen die SRV-Records in Active Directory überprüft werden können. Sie können sich das Tool bei Microsoft von der Seite *http://download.microsoft.com/download/2/7/2/27252452-e530-4455-846a-dd68fc020e16/dnslint.v204.exe* [Ms179-K25-01] herunterladen. Entpacken Sie das Tool nach dem Herunterladen in einen Ordner. 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]
```

In Kapitel 15 sind wir bereits auf dieses Tool ausführlich eingegangen.

Domänencontroller kann nicht gefunden werden

Erhalten Clients oder Server die Meldung, dass der Domänencontroller nicht erreicht werden kann, sollten Sie auf dem beteiligten Computer zunächst per Ping testen, ob eine Verbindung zur IP-Adresse des Servers funktioniert. Klappt das, stellen Sie sicher, dass in den Netzwerkeinstellungen der Server die IP-Adresse eines DNS-Servers eingetragen ist, welcher den Domänencontroller auflösen kann. Auch auf den Domänencontrollern selbst müssen in den Netzwerkeinstellungen die DNS-Server so gesetzt sein, dass die Auflösung funktioniert.

Achten Sie dabei auch in den erweiterten Netzwerkeinstellungen darauf, ob spezielle DNS-Suffixe gesetzt sind (siehe Kapitel 6). Auch der Test mit Nslookup zur Namensauflösung ist wichtig. Verwenden Sie nicht den vollständigen DNS-Namen des aufzulösenden Servers (FQDN), stellen Sie sicher, dass das DNS-Suffix des Clients korrekt ist oder in den erweiterten DNS-Einstellungen der Netzwerkverbindung eingetragen ist.

Haben Sie diese Grundlagentests durchgeführt, aber die Auflösung funktioniert noch immer nicht, fehlen unter Umständen DNS-Einträge der Domänencontroller in den DNS-Zonen. Diese Einstellungen finden Sie unter *_msdcs* auf den DNS-Servern. Auf den Domänencontrollern finden Sie solche Fehler am schnellsten, wenn Sie *dcdiag* in der Eingabeaufforderung eingeben. Überprüfen Sie auch mit *nltest /dsgetsite*, ob der Domänencontroller dem richtigen Active Directory-Standort zugewiesen ist. Mit *nltest /dclist:<NetBIOS-Name der Domäne>* lassen Sie sich eine Liste aller Domänencontroller einer entsprechenden Domäne anzeigen.

Die Einträge sollten als FQDN aufgelistet sein. Ebenfalls ein wichtiger Befehl ist *nltest /dsgetdc:<NetBIOS-Name der Domäne>*. Dieser Befehl listet Name, IP-Adresse, GUID, FQDN von Active Directory und weitere Informationen auf. Alle Informationen sollten ohne Fehler angezeigt werden.

Starten Sie mit *net stop netlogon* und dann *net start netlogon* den Anmeldedienst auf dem Domänencontroller neu. Beim Starten versucht der Dienst, die Daten der Datei *netlogon.dns* erneut in DNS zu registrieren. Gibt es hierbei Probleme, finden Sie im Ereignisprotokoll unter *System* einen Eintrag des Diensts, der bei der Problemlösung weiterhilft.

Auch der Befehl *nltest /dsregdns* hilft oft bei Problemen in der DNS-Registrierung. Funktioniert die erneute Registrierung durch Neustart des Anmeldedienstes nicht, löschen Sie die DNS-Zone *_msdcs* und die erstellte Delegierung ebenfalls. Starten Sie dann den Anmeldedienst neu, liest dieser die Daten von *netlogon.dns* ein, erstellt die Zone *_msdcs* neu und schreibt die Einträge wieder in die Zone. Testen Sie anschließend wieder mit Dcdiag, ob die Probleme behoben sind. Einen ausführlichen Test führen Sie mit *dcdiag /v* durch.

Namensauflösung von Mitgliedsservern

Stellen Sie Probleme bei der Namensauflösung von Mitgliedsservern fest, lassen sich diese leichter beheben. Die Server müssen die richtigen DNS-Server in den Netzwerkeinstellungen eingetragen haben, außerdem muss ein Host-A-Eintrag in der entsprechenden Zone gesetzt sein. Arbeiten Sie mit dynamischer DNS-Registrierung, achten Sie darauf, dass dynamische Aktualisierungen für die Zone in den Eigenschaften von DNS erlaubt sind.

Vor allem wenn es sich um Server handelt, die nicht Mitglied einer Domäne sind, aber von Active Directory-DNS-Servern aufgelöst werden sollen, müssen Sie darauf achten, die entsprechenden Namenseinträge manuell zu setzen oder auch unsichere Aktualisierungen für die Zone in den Eigenschaften der Zone festzulegen. Im laufenden Betrieb starten Sie mit dem Befehl *ipconfig /registerdns*

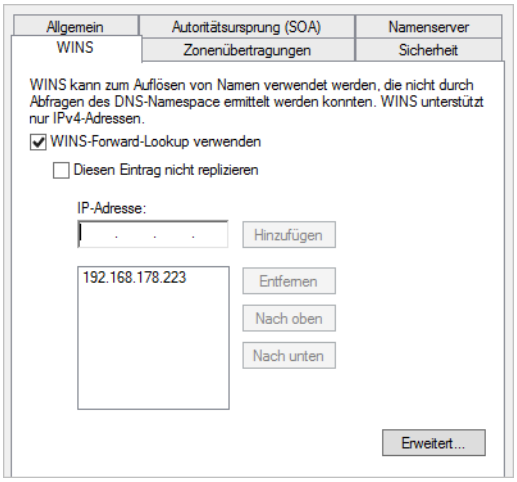
die dynamische Aktualisierung auf dem Mitgliedsserver. Starten Sie mit *net stop netlogon* und *net start netlogon* den Anmeldedienst neu, um sicherzustellen, dass die Aktualisierung funktioniert hat.

Integrieren von WINS in DNS

Seit Windows Server 2003 SP1 sind 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 2012 R2 übernommen worden. 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.

Abbildg. 25.14 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 Sie für jede Zone auf den Servern eintragen. 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).

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 Active Directory erheblich verbessert.

Namensauflösung durch Weiterleitung, Stammhinweise, sekundäre DNS-Server und durch Firewalls

Findet ein DNS-Server keine Daten zu einem Client, leitet der Server diese an den Server weiter, der als Weiterleitungsserver für die Domäne hinterlegt ist. Sind keine Weiterleitungsserver konfiguriert, verwenden DNS-Server die Server, die auf der Registerkarte *Stammhinweise* in den Eigenschaften des DNS-Servers hinterlegt sind.

Ein weiteres Problem kann darin liegen, dass der DNS-Server nicht bei allen eingebauten Netzwerkkarten und -Verbindungen auf Anfragen wartet. In den Eigenschaften des DNS-Servers finden Sie auf der Registerkarte *Schnittstelle* eine Auflistung aller IP-Adressen, bei denen der Server auf DNS-Anfragen wartet. Wollen Sie im Unternehmen auch sekundäre DNS-Zonen einsetzen, die nicht unbedingt unter Windows installiert sein müssen, können Sie auf diesen Servern nur dann die Zonen übertragen, wenn Sie in den Eigenschaften der Zone auf dem primären DNS-Server auf der Registerkarte *Zonenübertragungen* diese Übertragung erst zulassen. Standardmäßig verweigern Windows-DNS-Servern eine solche Übertragung.

Ist zwischen verschiedenen DNS-Servern oder DNS-Server und Client eine Firewall positioniert, blockiert diese unter Umständen DNS-Abfragen. DNS-Server verwenden den TCP- UDP-Port 53, den Sie für DNS-Abfragen freischalten sollten. Gelingt der Verbindungsaufbau immer noch nicht, schalten Sie UDP-Ports über 1023 frei.

Ein häufiges Problem ist die Namensauflösung der eigenen Internetdomäne über interne DNS-Server, vor allem dann, wenn die Active Directory-Domäne die gleiche Bezeichnung hat. Dieses Problem lösen Sie sehr einfach dadurch, indem Sie manuell entweder nur einen Host-A-Eintrag mit der Bezeichnung »www« und der externen IP-Adresse der Internetseite erstellen, oder für jeden Servernamen, den Sie extern auflösen lassen wollen, einen eigenen Eintrag. In diesem Fall lösen die internen DNS-Server den Eintrag der WWW-Seite korrekt nach der externen IP-Adresse auf.

Geänderte IP-Adressen, DHCP und die DNS-Namensauflösung

Ändern Sie die IP-Adresse eines Servers, wird nicht unbedingt gleich der entsprechende DNS-Eintrag des Servers geändert. Funktioniert nach einer IP-Änderung die Namensauflösung auch nach dem Ausführen von *ipconfig /registerdns* nicht, löschen Sie den Host-A-Eintrag auf dem Server und versuchen die dynamische Registrierung erneut. Ist auf dem Client der korrekte DNS-Server eingetragen und auf dem DNS-Server die dynamische Aktualisierung aktiv, sollte sich der Server neu registrieren. Arbeiten Sie mit DHCP, müssen Sie noch weitere Bereiche beachten.

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 (siehe Kapitel 24).

Setzen Sie noch Clients ein, die kein dynamisches DNS unterstützen, 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. Sie sollten die Computerkonten der DHCP-Server

in die Gruppe *DnsUpdateProxy* aufnehmen, wenn die DNS-Aktualisierung nicht funktioniert. Alternativ können Sie auf der Registerkarte *Erweitert* in den Eigenschaften für IPv4 oder IPv6 Anmeldedaten hinterlegen, die eine Aktualisierung ermöglichen. Ändern Sie die IP-Adresse des DNS-Servers selbst, stellen Sie sicher, dass in den Eigenschaften der Zonen, die dieser Server verwaltet, auf der Registerkarte *Namenserver* der korrekte Name und die richtige IP-Adresse hinterlegt sind.

Nslookup 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. Wenn Sie aber 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 Eingabeaufforderung 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. 25.15 Debuginformationen über einen DNS-Server mit Nslookup abrufen

```
C:\Users\Administrator>nslookup
Standardserver:  www.microsoft.com
Address:  192.168.178.223

> set debug
> file01
Server:  www.microsoft.com
Address:  192.168.178.223

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        file01.contoso.int, type = A, class = IN
    ANSWERS:
    ->  file01.contoso.int
        internet address = 192.168.178.233
        ttl = 1200 (20 mins)

------------
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 1,  additional = 0

    QUESTIONS:
        file01.contoso.int, type = AAAA, class = IN
    AUTHORITY RECORDS:
    ->  contoso.int
        ttl = 3600 (1 hour)
        primary name server = dc01.contoso.int
        responsible mail addr = hostmaster.contoso.int
        serial  = 528
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
```

Durch die Eingabe *nslookup contoso.int* können Sie überprüfen, welche Namenserver für die DNS-Domäne *contoso.int* zuständig sind. Sie können auch auf einem Remoteserver feststellen, welche Namenserver für eine Domäne konfiguriert sind, ohne in das Snap-In *DNS* wechseln zu müssen.

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 lässt sich 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 Eingabeaufforderung 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. 25.16 Überprüfen der MX-Einträge für bestimmte Domänen (auch über das Internet)

```
C:\Users\Administrator>nslookup
Standardserver:  dc01.contoso.int
Address:  192.168.178.223

> set q=mx
> joos.onmicrosoft.com
Server:  dc01.contoso.int
Address:  192.168.178.223

Nicht autorisierende Antwort:
joos.onmicrosoft.com    MX preference = 0, mail exchanger = joos.mail.eo.outlook
.com

joos.mail.eo.outlook.com        internet address = 216.32.181.178
joos.mail.eo.outlook.com        internet address = 65.55.88.22
> _
```

Komplette Zonen mit Nslookup übertragen

Zusätzlich können Sie alle Einträge einer Zone in Nslookup anzeigen lassen. Starten Sie dazu in der Eingabeaufforderung Nslookup. Geben Sie als Nächstes den Befehl *ls <Domäne>* ein, zum Beispiel *ls contoso.com*. Nslookup stellt eine Verbindung zum Namenserver dieser Zone her und überträgt den Inhalt der kompletten Zone auf den lokalen Rechner, um diesen anzuzeigen.

Allerdings muss diese Übertragung auf der Registerkarte *Zonenübertragungen* erst aktiviert werden. Standardmäßig verweigert Windows Server 2012 R2 eine solche Übertragung. 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 2012 R2 standardmäßig diese Abfrage. Sie können jedoch diese Sicherheitseinstellungen für jede einzelne Zone auf einem DNS-Server anpassen. Rufen Sie dazu die

Eigenschaften der Zone auf und wechseln Sie zur Registerkarte *Zonenübertragung*. An dieser Stelle können Sie die Übertragung auf einzelne Server zulassen oder verweigern.

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. 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 *\%WinDir%\System32\config\netlogon.dns*.

Dnscmd zur Verwaltung eines DNS-Servers in der Eingabeaufforderung

Ein weiteres wichtiges Befehlszeilenprogramm ist Dnscmd, mit dem Sie einen DNS-Server über die Eingabeaufforderung verwalten können. Mit Dnscmd 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 Eingabeaufforderung verwalten, zum Beispiel über Skripts. Über *dnscmd /?* erhalten Sie zusätzliche Informationen zu den verfügbaren Optionen angezeigt.

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 in 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 Ordner *\%WinDir%\System32\dns* kopieren. Active Directory-integrierte Zonen werden nicht in *.dns*-Dateien gespeichert, sondern direkt in die Active Directory-Datenbank eingefügt. Um mit Dnscmd eine Active Directory-integrierte DNS-Zone in eine Testdatei zu kopieren, öffnen Sie eine Eingabeaufforderung und geben zum Beispiel den folgenden Befehl ein:

```
dnscmd dc01.contoso.com /zonexport contoso.com contoso.txt
```

Die Zonendatei wird in den Ordner *\%WinDir%\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 Eingabeaufforderung
- **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 Standardanwendungspartitionen.

- **dnscmd createdirectorypartition** Mit dieser Option können neben den Standardpartitionen weitere Anwendungspartitionen erstellt werden, um die DNS-Replikation detailliert 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 Registryschlüssel *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. Entsprechende Aufrufe sind 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 Festplatte geschrieben wurden, und speichert diese dann auf der Festplatte
- **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 Schlüssel *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
```

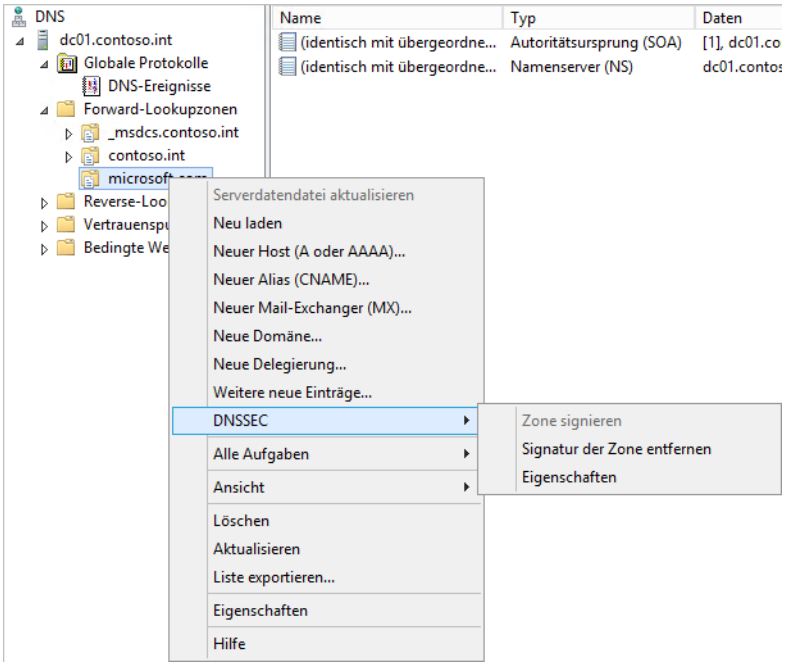
- **dnscmd zonepause** Pausiert eine Zone. Clientanfragen an diese Zone werden nicht beantwortet.
- **dnscmd zoneprint** Zeigt alle Einträge einer Zone an
- **dnscmd zoneresettype** Ändert den Typ einer Zone
- **dnscmd zonerefresh** Zwingt einen sekundären DNS-Server zum Abgleich der Zone mit seinem Master
- **dnscmd zonereload** Lässt eine Zone aus Active Directory oder deren Textdatei aus dem Ordner *\%WinDir%\System32\dns* neu laden
- **dnscmd zoneresetmasters** Setzt die IP-Adresse des Master-DNS-Server auf die 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 Active Directory
- **dnscmd zonewriteback** Überprüft, ob im Arbeitsspeicher für eine bestimmte Zone noch Einträge stehen, und schreibt diese auf die Festplatte

DNSSEC in Windows Server 2012 R2

Mit Windows Server 2012 R2 erweitert Microsoft auch die Möglichkeit der DNS-Verwaltung und verbessert die Sicherheit der DNS-Einträge. Das ist vor allem bei der Einbindung von Servern in Cloudstrukturen wichtig. Die Installation von DNS erfolgt über den Server-Manager wie alle anderen Rollen. Die Installation kann auch hier über das Netzwerk auf andere Server erfolgen. Bereits mit Windows Server 2008 R2 hat Microsoft DNSSEC eingeführt, um Zonen und Einträge abzusichern. Mit Windows Server 2012 R2 verbessert Microsoft die Möglichkeiten von DNS noch weiter.

Abbildg. 25.17 Zonen lassen sich in Windows Server 2012 R2 digital signieren



Windows Server 2008 R2 konnte bereits Zonen digital signieren und dadurch vor unerlaubten Änderungen schützen. Die Erstellung des Schlüssels erfolgt manuell über das Befehlszeilentool

Dnscmd. Dynamische DNS-Updates sind bei dieser Konfiguration nicht erlaubt. Die Verwaltung von DNS-Servern ist im Server-Manager von Windows Server 2012 R2 durch die Gruppierung wesentlich effizienter.

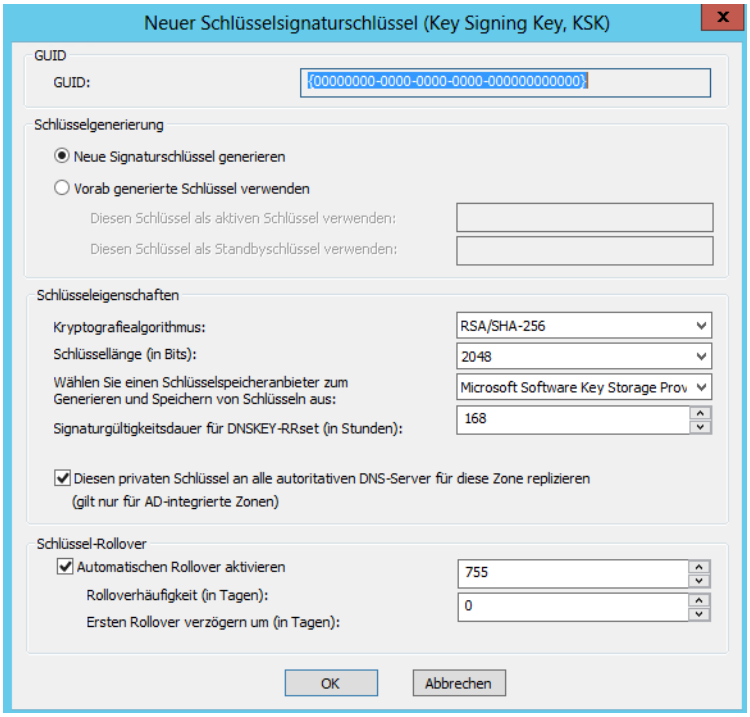
In Windows Server 2012 R2 lassen sich Zonen auch online digital signieren. Es ist nicht notwendig, diese vorher offline zu setzen. DNSSEC lässt sich in der neuen Version komplett in Active Directory integrieren. Dies umfasst auch die Möglichkeit, dynamische Updates für geschützte Zonen zu aktivieren. Windows Server 2012 R2 unterstützt offizielle Standards wie NSEC3 und RSA/SHA-2. Windows Server 2008 R2 konnte das noch nicht. Die Verwaltungsoberfläche für DNS hat Microsoft ebenfalls verbessert und auch die Windows-PowerShell ermöglicht jetzt die Verwaltung von DNS über Skripts.

Neu ist auch die Unterstützung von DNSSEC auf schreibgeschützten Domänencontrollern (Read-only Domain Controller, RODC). Findet ein RODC mit Windows Server 2012 R2 eine signierte DNS-Zone, legt er automatisch eine sekundäre Kopie der Zone an und überträgt die Daten der DNSEC-geschützten Zone. Dies hat den Vorteil, dass auch Niederlassungen mit RODCs gesicherte Daten auflösen können, aber die Signatur und Daten der Zone nicht in Gefahr sind.

Über das Menü *Tools* im Server-Manager lässt sich das Verwaltungswerkzeug starten. DNSSEC lässt sich über das Kontextmenü von Zonen erstellen. Eine komplizierte Konfiguration in der Eingabeaufforderung ist nicht erforderlich. Auch das Offlinesetzen von Zonen ist nicht mehr notwendig.

Die Signierung der Zone erfolgt über einen Assistenten. Mit diesem können Administratoren recht einfach DNS-Zonen vor Manipulationen schützen. Der Assistent erlaubt die manuelle Signierung, eine Aktualisierung der Signierung und eine Signierung auf Basis automatischer Einstellungen.

Abbildg. 25.18 Festlegen der Verschlüsselung einer Zone



Im Assistenten legen Sie auch den Schlüssel für die eigentliche Signatur fest. Auch dieser Vorgang lässt sich direkt in der Verwaltungskonsole über einen Assistenten festlegen. Sind die notwendigen Schlüssel erstellt, also der Schlüsselsignaturschlüssel (Key Signing Key, KSK) und der Zonensignaturschlüssel (Zone Signing Key, ZSK).

Nachdem die Schlüssel festgelegt sind, lässt sich die Absicherung festlegen. Windows Server 2012 R2 unterstützt hierbei Next Secure 3 (NSEC3), aber auch die ältere Version NSEC. In Windows Server 2012 R2 stellt ein DNS-Server den Key-Master-Server dar. Dieser Server verwaltet die primäre Zone. Verwenden Sie NSEC3, lässt sich die Zone nicht auf DNS-Server mit Windows Server 2008 R2 übertragen. Die Zone muss dann auf Servern mit Windows Server 2012 R2 gehostet werden. Auch auf den Clientcomputern muss Windows 8/8.1 installiert sein, um Daten von NSEC3-Zonen lesen zu können.

Mit Windows Server 2012 R2 lassen sich signierte Zonen auch auf andere DNS-Server im Netzwerk replizieren. Dazu muss es sich bei dem DNS-Server um einen Domänencontroller handeln. Der Assistent lässt sich für weniger geübte Administratoren leicht durcharbeiten. Anschließend signiert der Server die Zone entsprechend der Auswahl. Dabei handelt es sich um den Server, auf dem Administratoren DNSSEC aktivieren. Der Key Master ist für alle Schlüssel der Zone verantwortlich.

In den DNSSEC-Eigenschaften einer Zone lassen sich die Einstellungen und Schlüssel jederzeit anpassen. Hier stehen alle Eigenschaften zur Verfügung, die auch der Assistent bietet. Auch das Aufheben der Signierung ist über diesen Weg möglich.

In den normalen DNS-Eigenschaften einer Zone lassen sich mit Windows Server 2012 R2 auch dynamische Updates festlegen. Sobald ein Server der signierten Zone ein genehmigtes Update erhält, trägt der die Daten in die signierte Zone ein und repliziert die Daten zu den anderen Servern.

Zusammenfassung

In diesem Kapitel haben wir Ihnen die Verwaltung und den Betrieb von DNS-Servern mit Windows Server 2012 R2 erläutert. Auch die neuen Möglichkeiten zur Absicherung von DNS über DNSSEC sowie Möglichkeiten zum Troubleshooting waren Thema dieses Kapitel. In den Kapiteln 10 bis 17 finden Sie Hinweise zur Verwaltung von DNS-Servern, die vor allem im Bereich von Active Directory eine wichtige Rolle spielen.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie mit WINS ebenfalls eine Namensauflösungsinfrastruktur im Netzwerk, auch zusammen mit DNS, betreiben.

Kapitel 26

Windows Internet Name Service (WINS)

In diesem Kapitel:

WINS steht für Windows Internet Name Service und ist der Vorgänger der dynamischen DNS-Aktualisierung. Vor allem in Umgebungen mit mehreren Domänen kann eine WINS-Auflösung eine wertvolle Ergänzung zu DNS sein, da WINS zusammen mit DNS interagieren kann. Vor allem bei Problemen der DNS-Infrastruktur kann ein WINS-Server beachtliche Hilfe sein. Dies gilt auch für ältere Windows-Systeme, die DNS noch nicht unterstützen.

Während DNS für die Namensauflösung mit voll qualifizierten Domänennamen zuständig ist, zum Beispiel *dc01.contoso.int*, werden mit WINS NetBIOS-Namen aufgelöst, zum Beispiel *dc01*. 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.

HINWEIS In Windows Server 2012 R2 sind Erweiterungen integriert, welche die Namensauflösung zur Replikation von Active Directory über WINS abwickeln können, falls DNS Probleme hat. Auch aus diesem Grund kann WINS interessant sein, sozusagen als Failover für das DNS-System.

Installieren und Konfigurieren eines WINS-Servers

Um den WINS-Dienst zu installieren, rufen Sie im Server-Manager über *Verwalten/Rollen und Features hinzufügen* den Assistenten zur Installation von neuen Rollen und Features auf. WINS finden Sie auf der Seite *Features hinzufügen*. Die viertletzte Funktion im Fenster ist *WINS-Server*. Sie müssen keine weiteren Eingaben vornehmen, damit der Dienst installiert wird. Nach der Installation steht WINS sofort zu Verfügung. Sie müssen keine Zonen erstellen und auch keine dynamischen Updates aktivieren.

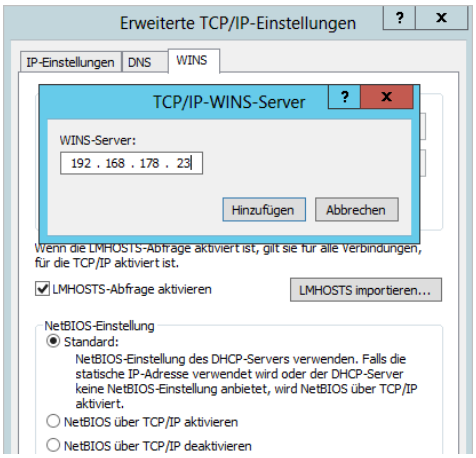
Konfigurieren der IP-Einstellungen für WINS

Damit sich die Server und Arbeitsstationen beim WINS registrieren und Daten aus WINS abfragen können, sind in den IP-Einstellungen der Server die WINS-Server einzutragen. Sie müssen nicht auf allen Domänencontrollern einer Domäne WINS installieren, zwei WINS-Server pro Standort reichen durchaus aus.

Nachdem Sie WINS installiert haben, können Sie in den IP-Einstellungen der Computer unter *Erweitert* auf der Registerkarte *WINS* die WINS-Server hinzufügen. 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 mithilfe eines DHCP-Servers verteilen.

Neben der Namensauflösung über WINS können Sie auch die lokal gespeicherte Textdatei *LMHosts* verwenden. Dies ist allerdings sehr aufwändig, da Sie diese Datei auf alle Computer im Netzwerk verteilen und vor allem den Inhalt manuell pflegen müssen. Die NetBIOS-Namensauflösung funktioniert generell auch ohne den Einsatz eines WINS-Servers, wobei die gesuchte IP-Adresse über Broadcasts ins Netzwerk ermittelt wird.

Abbildg. 26.1 Konfiguration der Computer für die Verwendung von WINS



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, verringert wird.

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.

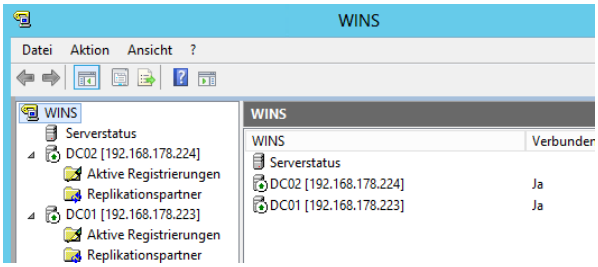
Clientcomputer, die WINS abfragen, tragen sich automatisch auf dem WINS-Server ein. Sie müssen keine dynamische Aktualisierung vornehmen oder Einträge manuell eintragen.

Einrichten der WINS-Replikation

Nachdem WINS installiert und konfiguriert sowie die IP-Einstellungen auf den Servern angepasst sind, können Sie die Replikation der WINS-Server einrichten, damit sich die Datenbanken untereinander abgleichen.

Für die Verwaltung von WINS verwenden Sie das Snap-In *WINS*, welches über das Menü *Tools* im Server-Manager zur Verfügung steht. Über das Kontextmenü von WINS können Sie zur Verwaltung auch die anderen Server hinzufügen.

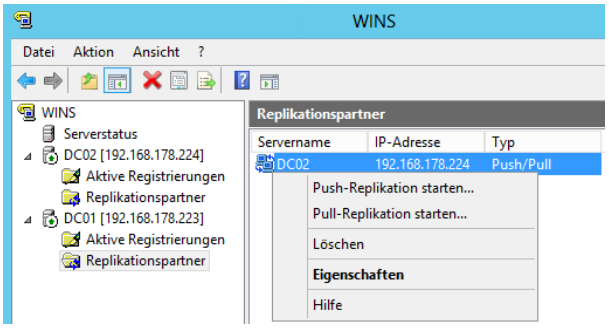
Abbildg. 26.2 Verwalten von WINS über den Server-Manager



Nach der Installation sollte der Server den WINS-Dienst als aktiv und verbunden anzeigen. WINS hat eine eigene Datenbank und kann seine Daten nicht wie DNS in Active Directory speichern. Aus diesem Grund müssen Sie auf WINS-Servern die Replikation manuell und getrennt von Active Directory einrichten:

1. Klicken Sie zunächst mit der rechten Maustaste im Knoten *WINS* auf den Eintrag *Replikationspartner* und wählen im Kontextmenü den Befehl *Neuer Replikationspartner* aus.
2. Tragen Sie die IP-Adresse oder den Namen 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.
3. Sie müssen die Replikationspartner aber immer auf beiden Servern pflegen. Wenn Sie *dc02* mit *dc01* replizieren lassen, repliziert *dc01* seine Daten nicht automatisch mit *dc02*.
4. 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.

Abbildg. 26.3 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 ist, 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*. Die Einrichtung ist abgeschlossen, wenn die Replikation fehlerfrei stattfindet.

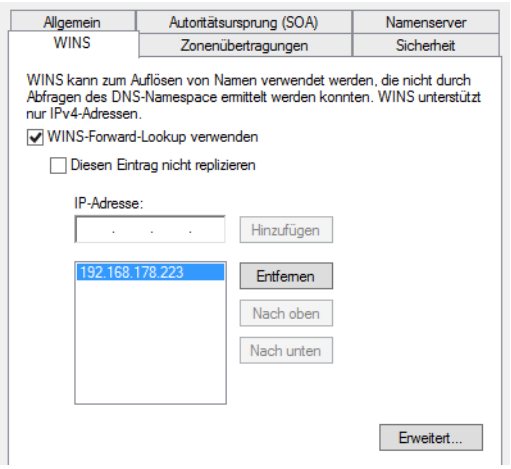
Integrieren von WINS in DNS

Um WINS in DNS zu integrieren, müssen Sie die Eigenschaften der einzelnen Zonen im DNS öffnen. Dort wählen Sie auf der Registerkarte *WINS* die Option *WINS-Forward-Lookup verwenden* und geben die IP-Adresse der WINS-Server ein.

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 einzeln durchgeführt werden.

Abbildg. 26.4 WINS-Forward-Lookup verwenden, um die Namensauflösung zu optimieren



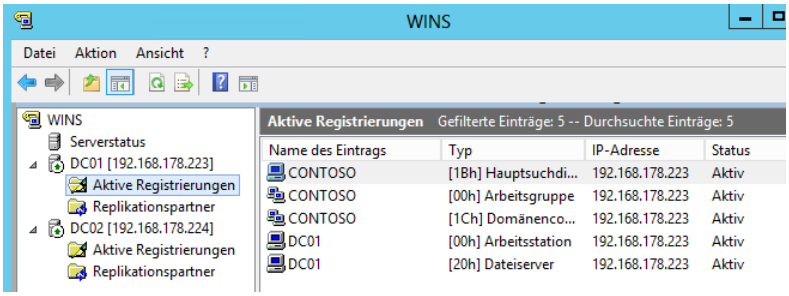
DNS speichert außerdem die WINS-Antwort in seinem Cache. Über die Schaltfläche *Erweitert* definieren Sie unter *Cachezeitlimit*, wie lange ein Eintrag, der von einem WINS-Server geliefert wurde, im DNS-Cache verbleibt (Standard 15 Minuten) und wie lange der DNS-Server auf die Antwort eines WINS-Servers wartet, bevor er zum nächsten Server in der Liste übergeht (Standard 2 Sekunden).

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 Active Directory erheblich verbessert, wobei vor allem Unternehmen mit Exchange-Servern in verschiedenen Domänen und Strukturen profitieren.

Die WINS-Datenbank verwalten

Um die Inhalte der WINS-Datenbank anzuzeigen, klicken Sie mit der rechten Maustaste auf den Eintrag *Aktive Registrierungen* und wählen im Kontextmenü den Befehl *Datensätze anzeigen* aus.

Abbildg. 26.5 Anzeigen des Inhalts 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 den von Ihnen vorgegebenen Ordner geschrieben. Diese Kopie können Sie bei Bedarf in den Ordner *%WinDir%\System32\wins* zurückkopieren.

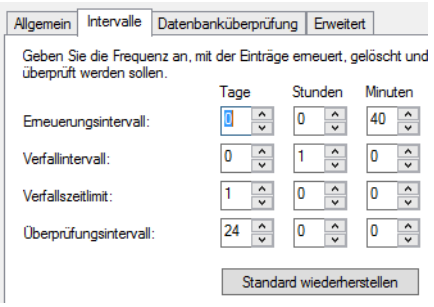
Die Sicherung und Wiederherstellung der WINS-Datenbank können Sie auch über das Kontextmenü des WINS-Servers in der Konsole durchführen.

Damit die Einträge in den WINS-Datenbanken immer möglichst aktuell bleiben, nimmt WINS die Registrierungen immer nur für eine bestimmte Zeit auf. Wenn der Client den Eintrag nicht innerhalb des angegebenen Erneuerungsintervalls bestätigt, gibt der WINS-Server den Eintrag wieder frei. Ein freigegebener Eintrag wird nach Ablauf der unter *Verfallintervall* angegebenen Zeit als verfallen angesehen und zur Löschung vorbereitet. Diese Einstellung finden Sie in den Eigenschaften des Servers auf der Registerkarte *Intervalle*.

Dazu setzt WINS in der Datenbank zu diesem Objekt einen Tombstone (Grabstein). Die Einstellung können Sie auf der Registerkarte *Intervalle* in den Eigenschaften eines WINS-Servers vornehmen. Nachdem der Tombstone länger als die unter *Verfallintervall* angegebene Zeit gesetzt war, löscht WINS das Objekt endgültig aus der Datenbank.

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. 26.6 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. Die Einstellungen dazu finden Sie auf der Registerkarte *Datenbanküberprüfung* in den Eigenschaften eines WINS-Servers.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie WINS zur Namensauflösung verwenden, zum Beispiel als Failback für DNS. Außerdem haben Sie erfahren, wie WINS installiert, konfiguriert und verwaltet wird. Und auch die Ausfallsicherheit von WINS-Servern haben wir in diesem Kapitel behandelt.

Im nächsten Kapitel gehen wir auf die Einrichtung eines Webservers mit Windows Server 2012 R2 ein, was auf Basis der neuen Internetinformationsdienste (IIS) 8.0 geschieht. Auch die Einrichtung eines FTP-Servers auf Basis von IIS 8 lernen Sie im nächsten Kapitel kennen.

Kapitel 27

Webserver – Internet-informationsdienste (IIS) 8.5

In diesem Kapitel:

Microsoft hat in Windows Server 2012 R2 auch die Internetinformationsdienste (Internet Information Services, IIS) überarbeitet. In Windows Server 2012 R2 sind die Internetinformationsdienste 8.5 enthalten. Wir gehen in diesem Kapitel ausführlicher auf den Webdienst ein. Im Kapitel 30 finden Sie ebenfalls weitere Informationen zum Thema IIS.

Für die Remoteverwaltung von Webservern wird unter Windows Server 2012 R2 nicht das RPC-Protokoll verwendet, sondern HTTP und HTTPS. Die einzelnen Komponenten zur Verwaltung sind in der Oberfläche schneller zu finden und leichter zu bedienen als bei den Vorgängerversionen.

Auf den beiden Seiten *http://www.iis.net* [Ms179-K27-01] und *http://www.microsoft.com/web* [Ms179-K27-02] erhalten Sie zusätzliche Informationen und Tools rund um IIS.

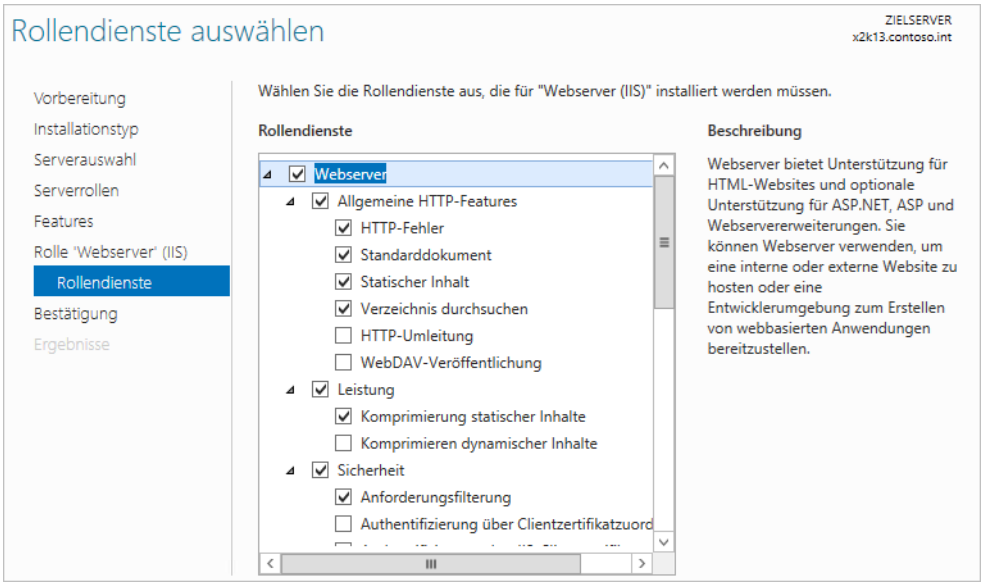
Neu in IIS ist die bessere Unterstützung mehrerer Prozessoren und Prozessorkerne. Außerdem lassen sich die Internetinformationsdienste besser vor Denial of Service (DoS)-Angriffen schützen. Der IP-Filter in IIS kann dynamisch IP-Adressen filtern und blockieren. Diese Funktion installieren Sie als eigenes Feature für IIS im Server-Manager.

Seit Windows Server 2012 haben Sie zusätzlich noch die Möglichkeit, SSL-Zertifikate einer IIS-Farm zentral zu speichern. Bis Windows Server 2008 R2 mussten Sie diese Daten noch lokal auf jedem Server der Farm speichern.

Installation, Konfiguration und erste Schritte

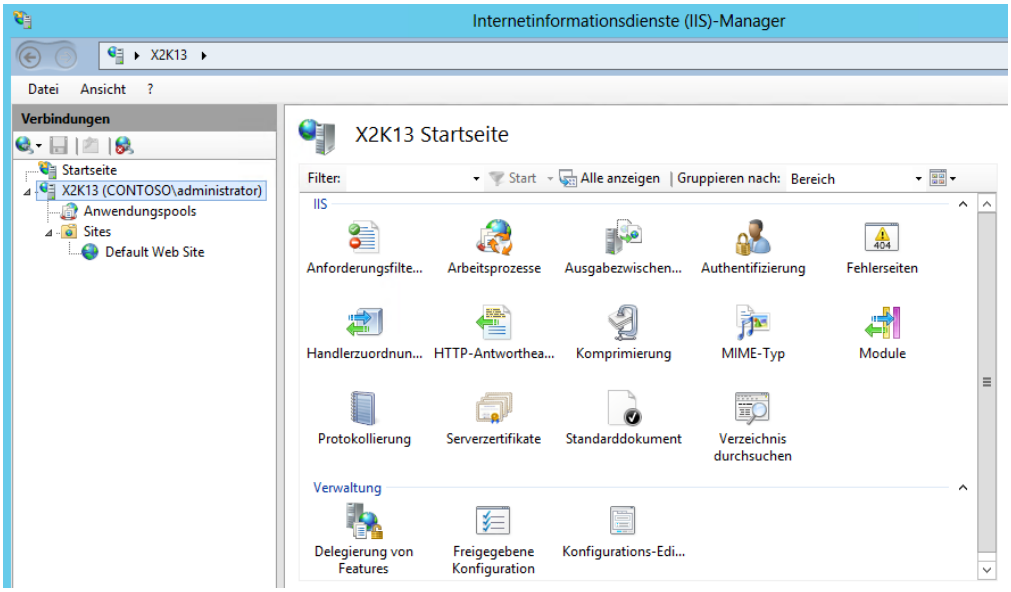
IIS 8.5 installieren Sie als Rolle über den Server-Manager. Das Verwaltungstool finden Sie nach der Installation über den Server-Manager oder durch Eingabe von *inetmgr* auf der Startseite. Die Installation von weiteren Rollendiensten können Sie jederzeit über den Server-Manager durchführen.

Abbildg. 27.1 Auswählen der Rollendienste für die Installation des Webservers



Der Internetinformationsdienste-Manager ist das zentrale Werkzeug zur Verwaltung des Webservers in Windows Server 2012 R2. Lesen Sie sich dazu auch das Kapitel 30 durch.

Abbildg. 27.2 Verwalten der Internetinformationsdienste



Sie können die Internetinformationsdienste auch über die Befehlszeile installieren. Dazu verwenden Sie den Befehl:

```
Start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-
StaticContent;IIS-DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-
HealthAndDiagnostics;IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-
Security;IIS-RequestFiltering;IIS-HttpCompressionStatic;IIS-WebServerManagementTools;IIS-
ManagementConsole;WAS-WindowsActivationService;WAS-ProcessModel;WAS-NetFxEnvironment;WAS-
ConfigurationAPI
```

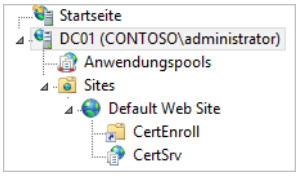
Wichtig für den Betrieb von IIS ist der Ordner *C:\Windows\System32\inetsrv*. Dieses enthält die Dateien zur Konfiguration, Verwaltung und Module, die der Server benötigt. Standardmäßig liest und schreibt Appcmd Änderungen in die Datei *applicationHost.config* aus dem Ordner *C:\Windows\System32\inetsrv\config*. Es handelt sich dabei um eine editierbare XML-Datei. Sie enthält Definitionen für alle Websites, Anwendungen, virtuelle Ordner und Anwendungspools. Auch globale Einstellungen sind hier hinterlegt. Aus diesem Grund ist daher die Sicherung mit Appcmd besonders sinnvoll.

Der Ordner *C:\inetpub* ist der Arbeitsordner von IIS. Es enthält verschiedene Unterordner. Hier sind die Webseiten gespeichert (*C:\inetpub\wwwroot*), die Fehlerseiten (*C:\inetpub\custerr*) und verschiedene Protokolldateien (*C:\inetpub\logs*). Auch eine regelmäßige Sicherung der Konfiguration (*C:\inetpub\history*) und der temporäre Arbeitsordner (*C:\inetpub\temp*) finden Sie hier. Diese Dateien sichern Appcmd nicht. Diese Dateien müssen Sie manuell sichern.

Anzeigen der Webseiten in IIS

Die Webseiten, die ein IIS-Server verwaltet, können Sie in der grafischen Verwaltungsoberfläche oder über die Eingabeaufforderung anzeigen. In der grafischen Oberfläche sehen Sie die Webseiten und deren virtuellen Ordner in einer Baumstruktur wie im Explorer angezeigt.

Abbildg. 27.3 Anzeigen der Webseiten eines IIS-Servers



Neben der grafischen Oberfläche können Sie die Webseiten auch in der Eingabeaufforderung über den Befehl *appcmd list site* anzeigen. Mit diesem Befehl werden aber nur die Webseiten, nicht die enthaltenen virtuellen Ordner angezeigt. Auch der Status der einzelnen Seiten wird in der Eingabeaufforderung angezeigt.

Abbildg. 27.4 Anzeigen von Webseiten und deren Status in der Eingabeaufforderung

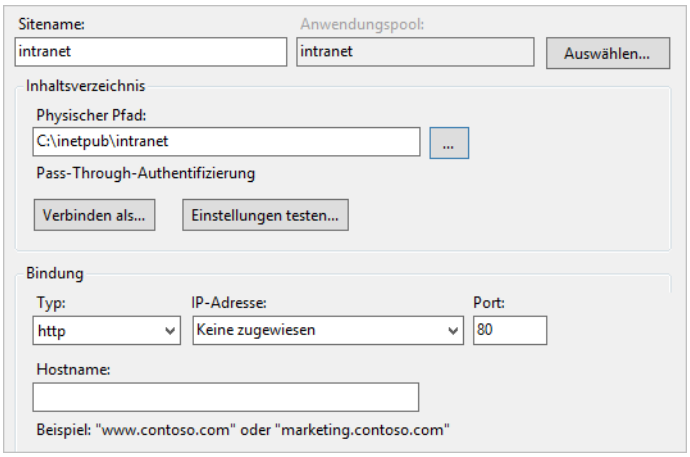
```
C:\Windows\System32\inetsrv>appcmd list site
SITE "Default Web Site" (id:1,bindings:http/*:80:,state:Started)
```

Hinzufügen und Verwalten von Webseiten

Das Hinzufügen von Webseiten übernehmen viele Applikationen selbst, wie zum Beispiel Exchange, die Terminaldienste, SharePoint oder die Active Directory-Zertifikatsdienste (siehe Kapitel 30). 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. Dieser Menübefehl steht auch im *Aktionen*-Bereich der MMC zur Verfügung.

Auf dem neuen Fenster geben Sie die Daten für die neue Webseite ein. Hier wählen Sie auch den Anwendungspool aus sowie den physischen Pfad zu den Daten der Webseite. Zusätzlich wählen Sie aus, mit welchem Benutzerkonto sich das System in dem physischen Ordner anmeldet, um auf die Daten des Servers zuzugreifen. Im Bereich *Bindung* wählen Sie aus, mit welchem Protokoll auf die Webseite zugegriffen werden kann, welche IP-Adresse im Einsatz ist und welcher Port für den Zugriff offen ist. Mehr zu diesem Thema lesen Sie auch in Kapitel 30.

Abbildg. 27.5 Erstellen und Konfigurieren einer neuen Webseite in IIS



Neben der grafischen Oberfläche können Sie neue Webseiten auch über die Eingabeaufforderung erstellen:

```
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

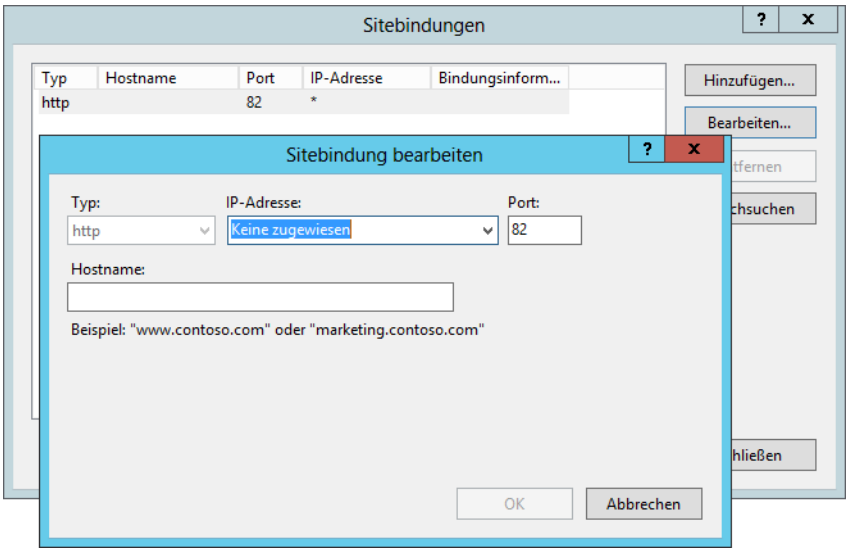
Um eine Seite mit der ID 2 aus dem physischen Ordner *c:\contoso*, die auf HTTP-Anfragen zum Port 88 auf alle IP-Adressen und der Domäne *shop.contoso.com* hört, zu erstellen, verwenden Sie den folgenden Befehl:

```
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 Sie die Bindungen, also das Protokoll, die IP-Adresse und den Port, über den die Webseite zur Verfügung steht, anpassen. Über das Bindungs-Menü können Sie auch Hostnamen von Webseiten nachträglich bearbeiten. Lesen Sie sich dazu auch das Kapitel 30 durch.

Abbildg. 27.6 Die Bindungen von Webseiten können nachträglich angepasst werden

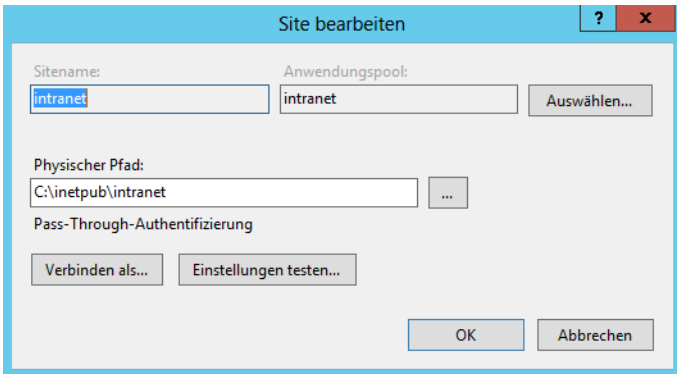


Über die Bindungen aktivieren Sie zum Beispiel auch SSL für eine Webseite. Wie Sie dabei vorgehen, lesen Sie in Kapitel 30.

Grundeinstellungen von Webseiten bearbeiten

Über den Link *Grundeinstellungen* im *Aktionen*-Bereich der Verwaltungskonsole passen Sie den physischen Pfad und den Anwendungspool einer Webseite nachträglich an. Zu den Anwendungspools kommen wir später noch.

Abbildg. 27.7 Bearbeiten der Grundeinstellungen einer Webseite



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 müssen Sie nicht den ganzen Server booten, sondern Sie können die Dienste von IIS einzeln beenden und starten. Das Beenden und den Start von IIS können Sie über die Verwaltungskonsole durchführen, indem Sie die entsprechenden Punkte aus dem Kontextmenü des Servers oder im *Aktionen*-Bereich auswählen.

Alternativ können Sie in der Eingabeaufforderung auch den Befehl *net stop w3svc* zum Beenden und *net start w3svc* zum Starten des Diensts eingeben. In vielen Fällen verwenden Sie zum Neustart das Dienstprogramm Iisreset in der Eingabeaufforderung. Damit keine Daten verloren gehen, sollten Sie den Befehl möglichst immer mit der Option *iisreset /noforce* starten.

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 *Aktionen*-Bereich der Konsole werden im Abschnitt *Website verwalten* die Befehle zum Neustart und zum Beenden angezeigt.

Über die Eingabeaufforderung können Sie mit dem Tool Appcmd ebenfalls eine Neustart oder das Beenden durchführen. Zum Beenden 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.

IIS in der Eingabeaufforderung verwalten – Appcmd

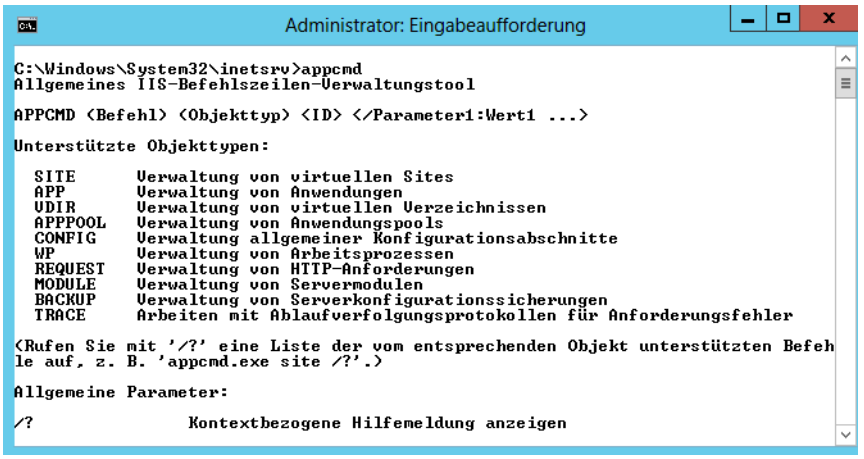
Neben der Verwaltung in der grafischen Oberfläche bietet IIS 8.5 auch ein Befehlszeilentool für die Verwaltung mit der Bezeichnung Appcmd an. Für die Verwaltung von IIS werden nicht mehr verschiedene Tools und Skripts benötigt, wie noch für IIS 6, sondern alle Verwaltungsaufgaben werden jetzt in einem Befehlszeilentool zusammengefasst.

Das Tool befindet sich allerdings nicht direkt im Pfad der Eingabeaufforderung, kann also nicht direkt aufgerufen werden. Sie müssen zuvor in den Ordner *\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 gehörigen Befehle.

Mit Appcmd 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*.

Abbildg. 27.8 Befehlszeilen-Verwaltungstool für IIS



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 Ordnern 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 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.

Abbildg. 27.9 Mit Appcmd die Einstellungen von IIS sichern, auflisten und wiederherstellen

```
C:\Windows\System32\inetsrv>appcmd add backup iis-backup
Das BACKUP-Objekt "iis-backup" wurde hinzugefügt.

C:\Windows\System32\inetsrv>appcmd list backups
BACKUP "iis-backup"
BACKUP "CFGHISTORY_0000000001"
BACKUP "CFGHISTORY_0000000002"
```

Das Tool sichert vor allem die folgenden Dateien und kann diese daher auch wiederherstellen:

- *config\applicationHost.config*
- *config\administration.config*
- *config\redirection.config*
- *config\metabase.xml*
- *config\mbschema.xml*
- Alle Schemadateien in *config\schema*

Nutzen Sie aber eine verteilte Konfiguration in IIS, sind die Konfigurationsdateien nicht auf dem lokalen Server gespeichert, sondern in einer Freigabe. Diese nutzen mehrere Webserver für ihre Konfiguration. Appcmd sichert allerdings nur lokale Dateien, keine Freigaben. Sichern Sie mit Appcmd in einer verteilten Konfiguration die Internetinformationsdienste, berücksichtigt das Tool aber die Datei *redirection.config*. Hier ist gespeichert, wo die Konfigurationsdateien von IIS liegen.

Sichern Sie also den Server vor der Änderung zu einer verteilten Konfiguration und stellen diese wieder her, haben Sie nach der Wiederherstellung wieder eine lokale Konfiguration vorliegen.

Sie können zum Beispiel eine regelmäßige Aufgabe in Windows erstellen und die Konfiguration von IIS in eine Datei sichern. Die Datei lässt sich in der Sicherung des Servers integrieren. Dazu verwenden Sie den Befehl:

```
%WinDir%\system32\inetsrv\appcmd.exe add backup "<Name der Datensicherung>"
```

Natürlich können Sie vorhandene Sicherungen auch wieder löschen. Dazu verwenden Sie den Befehl:

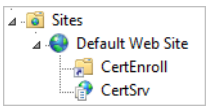
```
appcmd.exe delete backup "<Name der Datensicherung>"
```

Verwalten der Webanwendungen und virtuellen Ordner einer Webseite

Eine einzelne Webseite kann aus mehreren virtuellen Ordnern 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 Eingabeaufforderung können Sie die Anwendungen eines Webservers mit dem Befehl *appcmd list app* anzeigen.

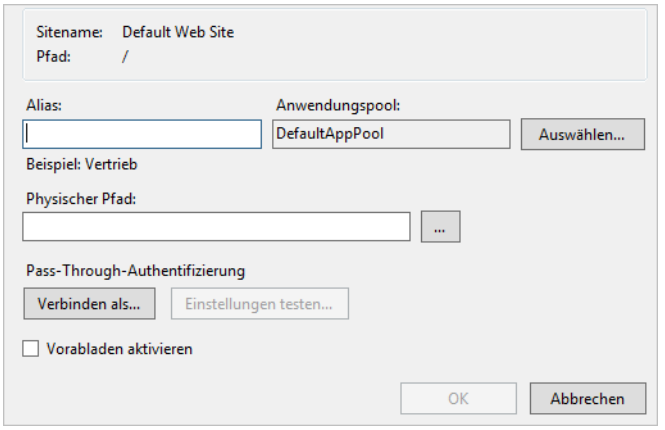
Abbildg. 27.10 Anzeigen der Webanwendungen einer Webseite



Wollen Sie nur die Anwendung einer einzelnen Webseite anzeigen, verwenden Sie den Befehl *appcmd list app /site.name:<Name>*.

Um eine neue Webanwendung zu erstellen, die eine bereits angelegte Webseite nutzt, 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. Wollen Sie einen virtuellen Ordner hinzufügen, verwenden Sie im Kontextmenü die Option *Virtuelles Verzeichnis hinzufügen*.

Abbildg. 27.11 Hinzufügen von neuen Anwendungen zu einer Webseite



Es öffnet sich ein neues Fenster, über das Sie die Daten für die neue Anwendung konfigurieren. Hier geben Sie den Alias, den Anwendungspool, den physischen Pfad und den Benutzer an, mit dem der Dienst auf den Pfad zugreifen soll.

Nachdem die Anwendung erstellt ist, sehen Sie diese als untergeordnetes Objekt der Webseite. Über die Eingabeaufforderung 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 *Aktionen*-Bereich der Konsole bearbeiten.

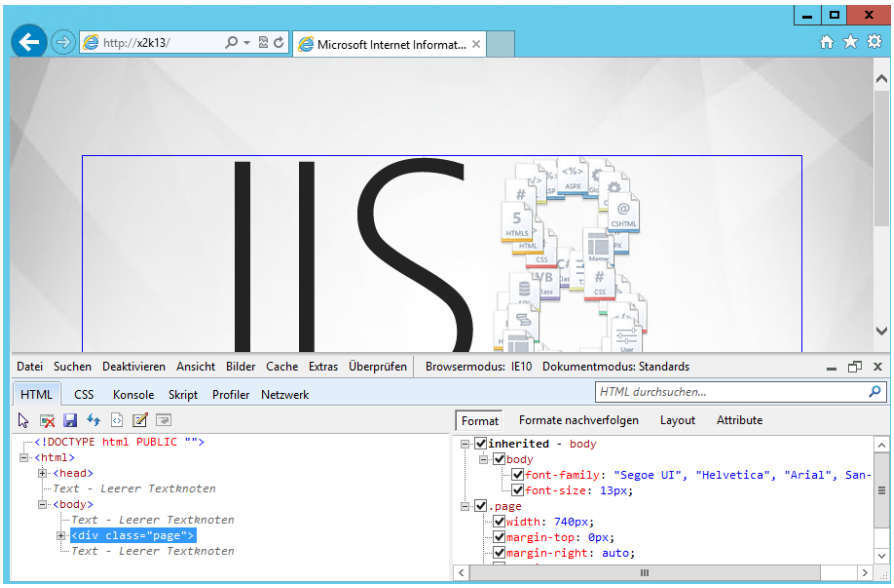
Die erweiterten Einstellungen einer Webanwendung oder der kompletten Seite lassen sich durch den Link *Erweiterte Einstellungen* im *Aktionen*-Bereich oder im Kontextmenü mit dem Befehl *Anwendung verwalten* beziehungsweise *Website verwalten* aufrufen.

Entwicklungstools im Internet Explorer aufrufen oder Fiddler verwenden

Vor allem für Administratoren, aber auch für Entwickler sind die Entwicklertools in IE 10 interessant. Diese rufen Sie über die F12-Taste auf. Die Tools zeigen den Quelltext zu einer Seite an und helfen bei der Fehleranalyse, wenn zum Beispiel eine Seite lange zum Laden dauert.

Über die Registerkarte *Netzwerk* können Sie die Ladedauern von Seiten überprüfen, um festzustellen, welche Bereiche einer Website das Laden verzögern.

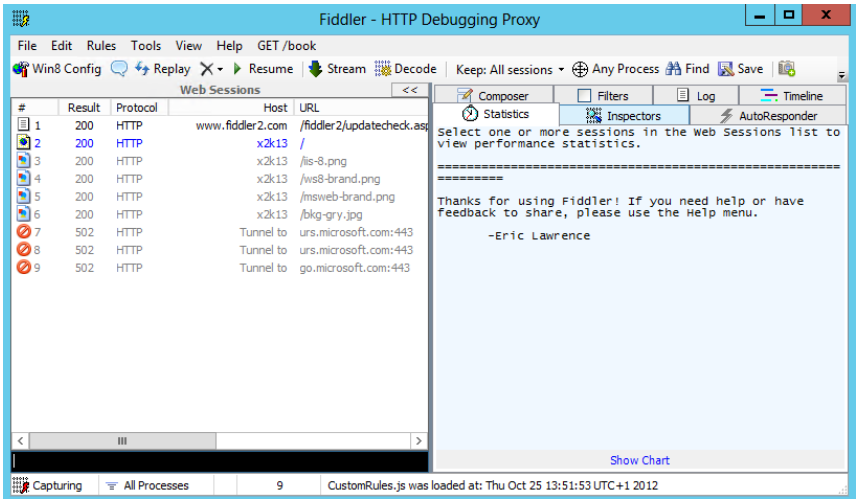
Abbildg. 27.12 Verwenden der Entwicklertools im IE 10/11 bei der Anbindung an IIS 8.5



Um eine Seite auch nachträglich zu analysieren, können Sie die Ausgabe speichern. Um eine Analyse durchzuführen, lässt sich die gespeicherte XML-Datei allerdings nicht in den Entwicklungstools des IE einlesen. Sie können dazu aber das Freewaretool Fiddler von der Seite *http://www.fiddler2.com* [Ms179-K27-03] verwenden:

1. Starten Sie Fiddler.
2. Wählen Sie *File/Import Sessions*.
3. Wählen Sie die Option *IE's F12 NetXML* und dann die abgespeicherte Datei aus.

Abbildg. 27.13 Analysieren des Netzwerkzugriffs mit Fiddler

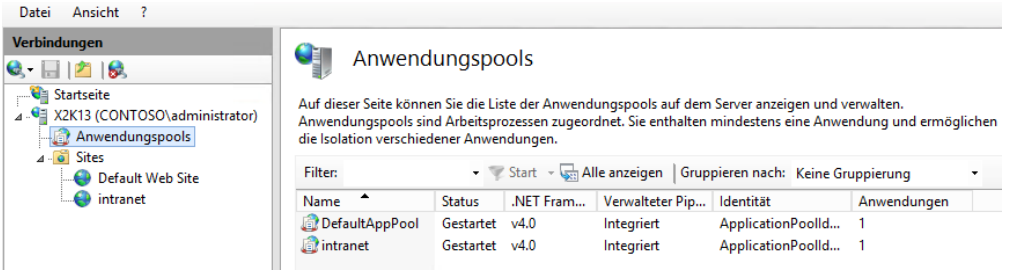


Verwalten von Anwendungspools

Webseiten und Webanwendungen können Sie in eigenen Anwendungspools und damit Speicherbereichen installieren. Der Absturz einer einzelnen Anwendung führt dabei nicht unweigerlich zum Absturz anderer Anwendungen oder des kompletten Servers.

Alle Anwendungspools werden im Internetinformationsdienste-Manager über den Eintrag *Anwendungspools* in der Konsolenstruktur angezeigt und konfiguriert. Über die Eingabeaufforderung können Sie die Anwendungspools über *appcmd list apppool* anzeigen lassen.

Abbildg. 27.14 Verwalten und Anzeigen der Anwendungspools



Über den Befehl *Anwendungen anzeigen* im Kontextmenü oder *Aktionen*-Bereich des Anwendungspools zeigen Sie die Webseiten und Anwendungen, die sich diesen Anwendungspool teilen, an. Über die *Zurück*-Schaltfläche in der Oberfläche kommen Sie im Fenster wieder zur Hauptansicht zurück.

In der Eingabeaufforderung werden die Anwendungen eines Anwendungspools über *appcmd list app /apppool.name:<Name>* angezeigt.

Erstellen und Verwalten von Anwendungspools

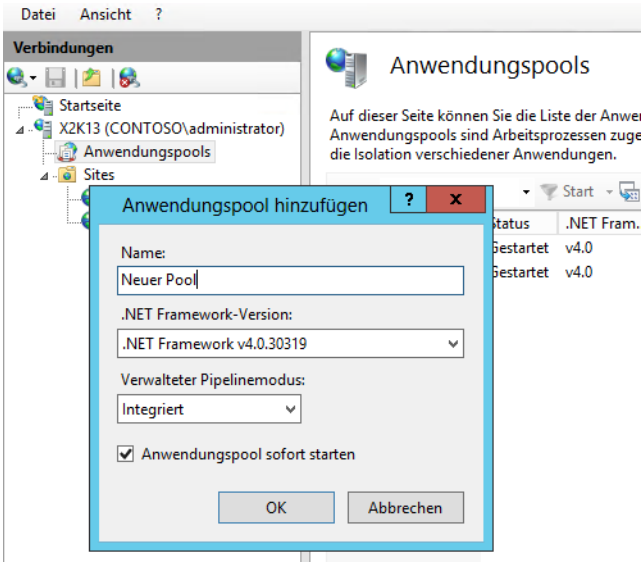
Beim Erstellen einer neuen Webseite können Sie im Fenster einen neuen Anwendungspool erstellen. Über den Eintrag *Anwendungspools* in der Konsolenstruktur des Internetinformationsdienste-Managers können Sie ebenfalls neue Anwendungspools über das Kontextmenü oder den *Aktionen*-Bereich erstellen.

Beim Erstellen geben Sie in dem Standardfenster den Namen, die Version der unterstützten .NET-Version und der verwaltete Pipelinemodus an. 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.

Wollen Sie die Identität des Anwendungspools oder erweiterte Einstellungen anpassen, rufen Sie nach der Erstellung den Befehl *Erweiterte Einstellungen* oder *Anwendungspoolstandardwerte festlegen* im Kontextmenü oder dem *Aktionen*-Bereich auf. In dem Fenster passen Sie die Einstellungen des Anwendungspools an.

Beenden Sie einen Anwendungspool auf einem Server, sind auch die in diesem Pool verankerten Anwendungen nicht mehr verfügbar. Das ist zum Beispiel beim Einsatz von Exchange interessant. Wollen Sie ActiveSync für einen kompletten Clientzugriffsserver (Client Access Server) sperren, deaktivieren Sie am besten den virtuellen Ordner, welcher die Synchronisierung steuert.

Abbildg. 27.15 Erstellen eines neuen Anwendungspools



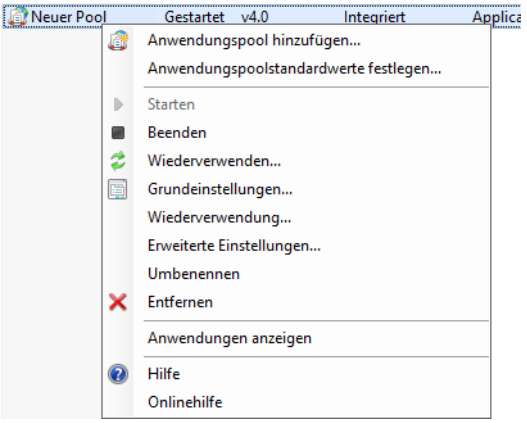
Exchange ActiveSync läuft als eigener Anwendungspool in IIS. Anwendungspools können für eine oder mehrere webbasierende Anwendungen definiert werden. Die Pools werden in getrennten Prozessräumen ausgeführt, sodass ein Fehler einer Anwendung in einem Pool keine Auswirkungen auf Anwendungen in anderen Pools hat.

Beenden Sie einen Pool, sind auch die enthaltenen Applikationen nicht mehr verfügbar. Da Exchange-ActiveSync seinen eigenen Pool hat, können Sie über das Beenden des Pools auch Exchange ActiveSync dauerhaft oder für bestimmte Zeit auf diesem Server deaktivieren. Gehen Sie zur Deaktivierung von Exchange ActiveSync auf einem Clientzugriffsserver folgendermaßen vor:

1. Starten Sie den Internetinformationsdienste-Manager.
2. Öffnen Sie den Baum unter dem Servernamen.
3. Öffnen Sie das Menü unter *Anwendungspools*.
4. Klicken Sie mit der rechten Maustaste auf den Anwendungspool *MSExchangeSyncAppPool* und wählen Sie den Befehl *Beenden*.

Auf die gleiche Weise können Sie auch andere Anwendungen zeitweise beenden. Funktioniert eine Anwendung nicht, sollten Sie deren Anwendungspool überprüfen und feststellen, ob dieser funktioniert. Überprüfen Sie in der IIS-Verwaltung über Anwendungspools auch, ob alle notwendigen Exchange-Anwendungspools gestartet sind, vor allem der Pool *MSExchangePowerShellAppPool*, wenn zum Beispiel die Remoteverwaltung von Exchange nicht funktioniert. Viele Webanwendungen legen automatisch eigene Anwendungspools in IIS an.

Abbildg. 27.16 Deaktivieren von Anwendungspools auf einem Server



Stellen Sie auch sicher, dass das Benutzerkonto, welches dem Anwendungspool der Webanwendung zugeordnet ist, Mitglied einer Administratorengruppe ist, wenn Webanwendungen bestimmte Rechte erhalten sollen. Um diesen Benutzer anzuzeigen, starten Sie den IIS-Manager und klicken auf *Anwendungspools*. Klicken Sie anschließend auf den Anwendungspool der Webanwendung.

Klicken Sie auf den Anwendungspool, sehen Sie auch die zugeordnete Identität. Alternativ klicken Sie im *Aktionen*-Bereich des IIS-Managers auf *Erweiterte Einstellungen*, nachdem Sie den Anwendungspool markiert haben.

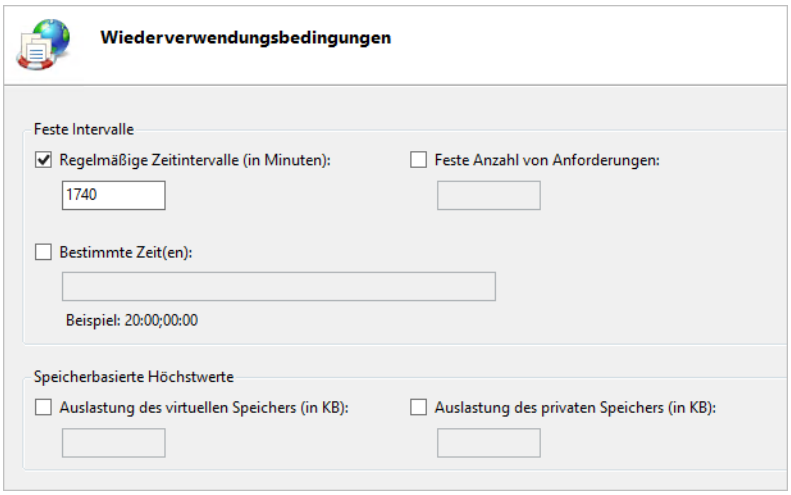
Zurücksetzen von Arbeitsprozessen in Anwendungspools

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.

Das Zurücksetzen von Arbeitsprozessen bereinigt laufende Anwendungen und kann diese nach dem Neustart beschleunigen. Dieses Wiederverwenden kann über das Kontextmenü konfiguriert werden. Dazu wählen Sie den Befehl *Wiederverwendung*. 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.

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.

Abbildg. 27.17 Zurücksetzen von Arbeitsprozessen für Anwendungspools



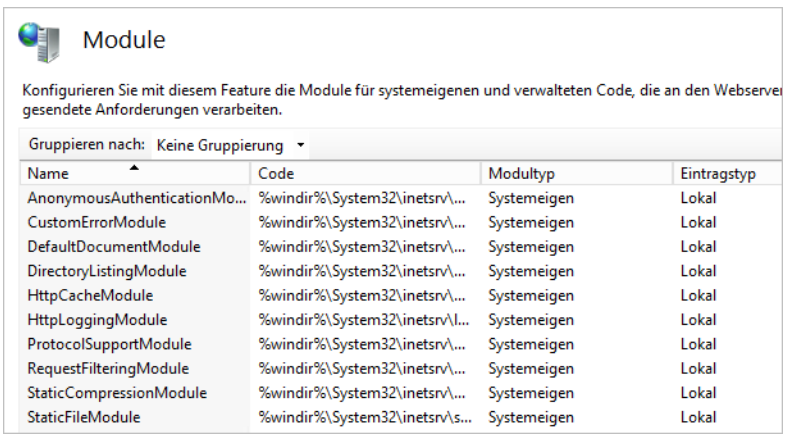
Verwalten von Modulen in IIS 8.5

IIS 8.5 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 Buchs 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 8.5 mit Anwendungen und Webseiten basierend auf diesen beiden Modultypen umgeht. Module werden über *Module* auf der Hauptseite des Internetinformationsdienste-Managers verwaltet und konfiguriert.

Abbildg. 27.18 Verwalten der Module im IIS-Manager



Native Module werden geladen, wenn der Arbeiterprozess (Worker Process) einer Anwendung gestartet und initialisiert wird. Native Module werden immer auf Serverbasis hinzugefügt, können für einzelne Webseiten oder Anwendungen aber deaktiviert werden.

Um ein systemeigenes Modul hinzuzufügen, wählen Sie in der Moduleverwaltung aus dem Kontextmenü oder dem *Aktionen*-Bereich 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.

Nachdem Sie auf die Schaltfläche *Registrieren* geklickt haben, können Sie einen Namen für das Modul festlegen sowie die entsprechende DLL-Datei für das native Modul auswählen. Auf dem gleichen Weg kann ein Modul wieder deinstalliert werden, wenn dieses nicht mehr benötigt wird.

Delegierung der IIS-Verwaltung

Mit IIS 8.5 können Sie die Verwaltung von einzelnen Webseiten oder des kompletten Servers delegieren. 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 beim Delegieren von Berechtigungen

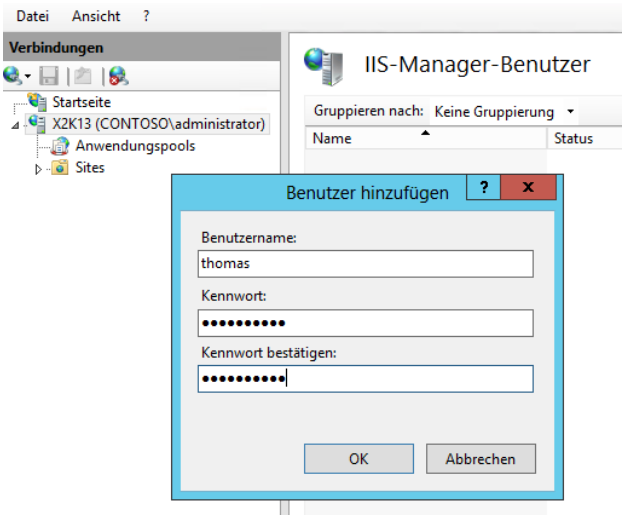
Um Benutzern das Recht der Verwaltung für einzelne Webseiten oder Anwendungen zu erteilen, können entweder Windows-Benutzerkonten oder spezielle IIS-Konten verwendet werden. Die IIS-Konten können ausschließlich nur innerhalb des Webservers für die Delegierung von Rechten verwendet werden. Damit die Webadministratoren ihre Webseiten auch verwalten können, muss der Verwaltungsdienst auf dem Webserver so konfiguriert sein, dass der Zugriff gestattet wird.

Verwalten von IIS-Manager-Benutzern

Damit Benutzerkonten speziell in IIS verwaltet werden können, starten Sie den *Internetinformationsdienste-Manager* in der Programmgruppe *Verwaltung*. Sie können das Tool auch durch Eintippen von *inetmgr* auf der Startseite aufrufen. Die Benutzerverwaltung wird über den Menüpunkt *IIS-Manager-Benutzer* durchgeführt. Klicken Sie darauf, werden im Fenster alle bereits angelegten Benutzer in IIS angezeigt. Über dieses Fenster können weitere Benutzer angelegt, die Kennwörter geändert, oder Benutzer gelöscht werden.

Dieses Feature wird allerdings nur dann angezeigt, wenn der Rollendienst *Verwaltungsdienst* unterhalb der *Verwaltungsprogramme* für den Webserver installiert ist. Über das Kontextmenü eines IIS-Manager-Benutzers können Sie verschiedene Verwaltungsaufgaben durchführen. So besteht zum Beispiel auch die Möglichkeit, Benutzer zu deaktivieren. In diesem Fall kann der Benutzer bis zu seiner Aktivierung nicht mehr auf die Verwaltungsoberfläche zugreifen.

Abbildg. 27.19 Über den IIS-Manager können die Manager-Benutzer innerhalb von IIS verwaltet werden

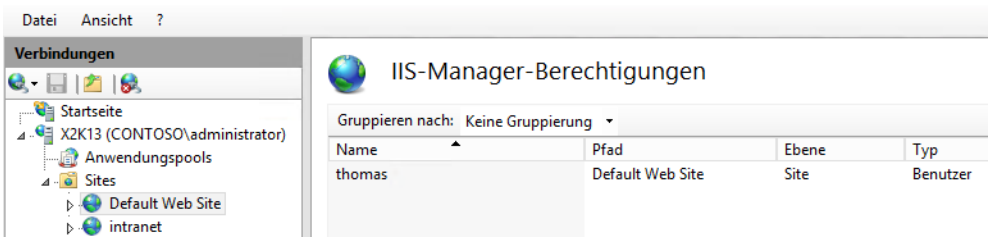


Von den installierten Rollendiensten hängen die angezeigten Verwaltungsmöglichkeiten von IIS ab. Sollen lokale IIS-Konten verwaltet werden, benötigen Sie den Rollendienst *Verwaltungsdienst*.

Berechtigungen der IIS-Manager-Benutzer verwalten

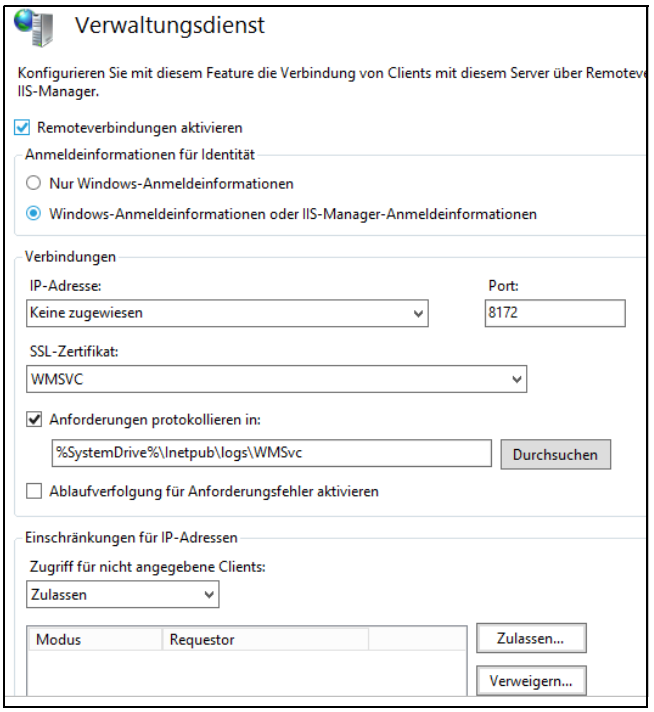
Nachdem die Benutzerkonten in IIS für die Delegierung angelegt sind, können Sie die Rechte für diese Benutzer über den Menüpunkt *IIS-Manager-Berechtigungen* verwalten. Dazu verwenden Sie aber nicht das Symbol in der Serverkonfiguration, sondern klicken auf die Webseite, für die Sie den IIS-Manager delegieren wollen und wählen den Menüpunkt aus. Anschließend klicken Sie auf *Benutzer zulassen*. Es öffnet sich ein neues Fenster, über das Sie auswählen können, welche Benutzer zugelassen werden, um den Server zu verwalten.

Abbildg. 27.20 Zulassen eines Benutzers für eine bestimmte Webseite



TIPP Damit Sie Benutzer für Webseiten zulassen können, müssen Sie zunächst den *Verwaltungsdienst* im IIS-Manager unter Verwaltung aktivieren und die entsprechenden Einstellungen vornehmen.

Abbildg. 27.21 Aktivieren und Konfigurieren des Verwaltungsdiensts für die Remoteverwaltung



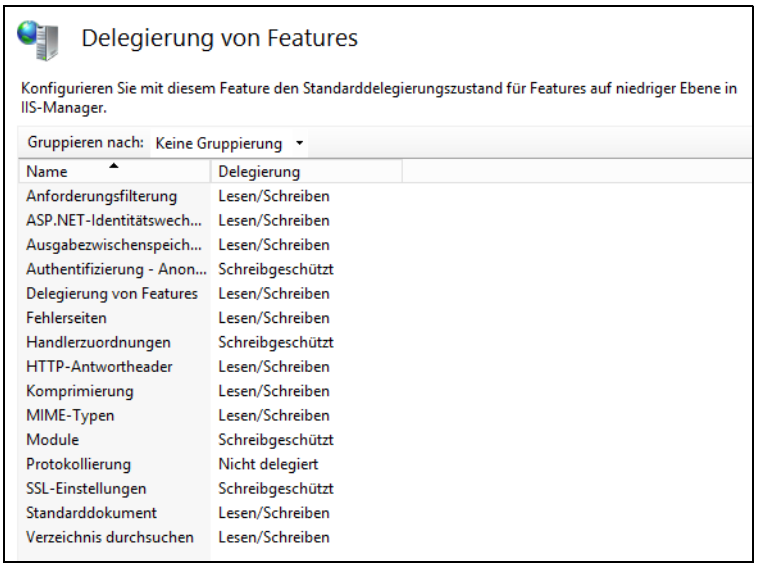
HINWEIS Standardmäßig ist die Möglichkeit, IIS-Manager für eine Webseite zu delegieren, deaktiviert, da der Server nur Windows-Benutzerkonten zulässt. Damit auch die angelegten IIS-Manager-Benutzer verwendet werden können, muss auf Serverebene über das Feature *Verwaltungsdienst* die Option *Windows-Anmeldeinformationen oder IIS-Manager-Anmeldeinformationen* aktiviert und bestätigt sein. Der Dienst muss anschließend gestartet werden. Erst dann kann in den IIS-Manager-Berechtigungen auch ein IIS-Manager ausgewählt werden.

Verwalten der Delegierung

Nachdem den entsprechenden IIS-Manager-Benutzern und/oder Windows-Benutzern das Recht zur Anmeldung für spezielle Webseiten gewährt wurde, können Sie festlegen, welche Rechte überhaupt für Webseiten auf dem Server delegiert werden können.

Da die Delegierungseinstellungen 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. Die Verwaltung der Delegierung findet dann über das Feature *Delegierung von Features* statt.

Abbildg. 27.22 Starten der Delegierung



In diesem Bereich legen Sie fest, welche Rechte die einzelnen Manager-Benutzer erhalten sollen. Über das Kontextmenü oder den *Aktionen*-Bereich der Konsole können bereits gesetzte Delegierungen wieder zurückgesetzt oder benutzerdefinierte Delegierungen konfiguriert werden.

Durch die benutzerdefinierte Delegierung können Sie Aufgaben für einzelne untergeordnete Sites festlegen. Auch hier werden die Rechte wieder an die untergeordneten Webseiten vererbt. Die benutzerdefinierten Delegierungen können Sie aber ebenfalls jederzeit entweder wieder auf den Standard oder auf Vererbung von oben zurücksetzen.

Für die einzelnen Features, die delegiert werden können, besteht die Möglichkeit, unterschiedliche Rechte festzulegen:

- **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
- **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 dieser 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 Delegierungen verwendet werden können, muss auf einem Server die Remoteverwaltung konfiguriert und aktiviert sein. Diese Option findet auf Serverebene über den Menüpunkt *Verwaltungsdienst* statt. Damit die Einstellungen angepasst werden können, muss ein gestarteter Verwaltungsdienst zunächst beendet werden.

Erst dann können Sie Einstellungen vornehmen. Neben der allgemeinen Aktivierung und der Möglichkeit, neben Windows-Benutzern auch IIS-Manager-Benutzer zu berechtigen, können Sie in diesem Bereich der Konsole weitere Einstellungen zur Remoteverwaltung eines Servers vornehmen:

- 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 Standardport 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 Servername angegeben.

- 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. Mehr zu diesem Thema lesen Sie in Kapitel 30.
- Im Ordner 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.

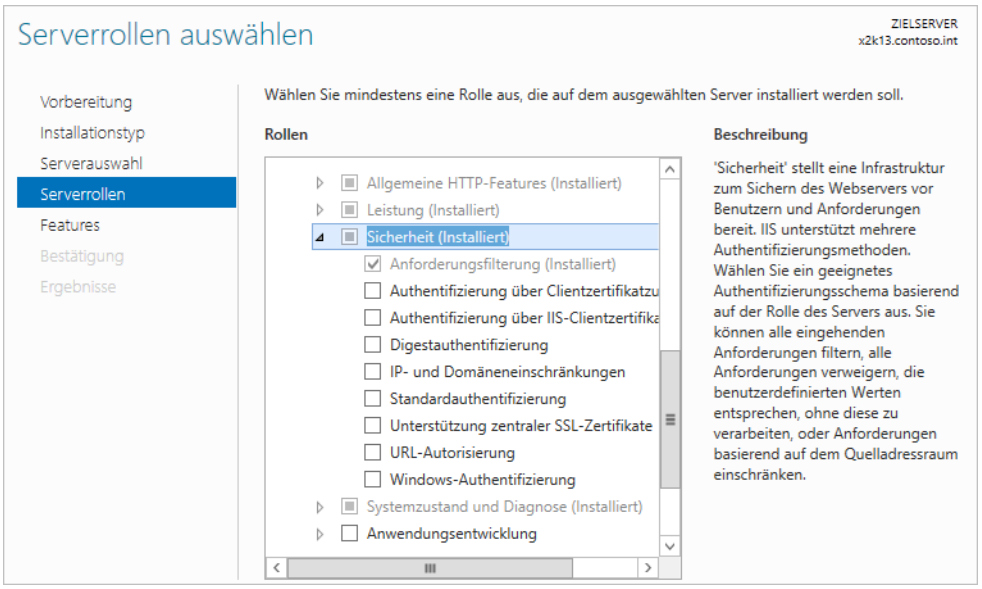
Auf der rechten Seite der Konsole werden die Einstellungen schließlich bestätigt und der Verwaltungsdienst gestartet oder beendet. Änderungen können nur vorgenommen werden, wenn der Dienst beendet wurde.

Sicherheit in IIS 8.5 konfigurieren

In diesem Abschnitt beschäftigen wir uns maßgeblich mit der Sicherheit und der Authentifizierung in IIS 8.5. Die Konfiguration der Authentifizierung ist eine der wichtigsten Konfigurationsmaßnahmen auf einem Webserver. Bei Windows Server 2012 R2 können Sie die verschiedenen Authentifizierungsoptionen nachträglich installieren oder einzeln deinstallieren.

Auf dem Server stehen nur die Authentifizierungsoptionen zur Verfügung, die auch bei der Installation als Rollendienst ausgewählt wurden. Über den Server-Manager können Sie einzelne Rollendienste und auch Authentifizierungsoptionen nachträglich installieren oder deinstallieren.

Abbildg. 27.23 Nachträgliche Installation von Authentifizierungsmöglichkeiten in IIS



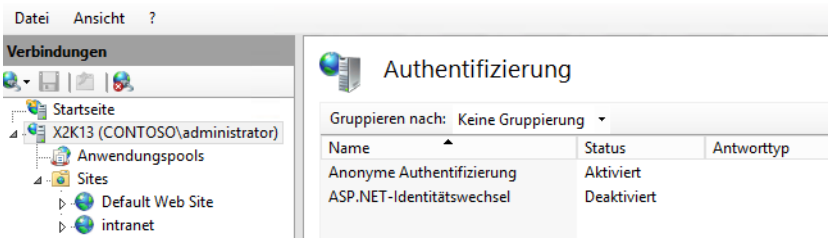
Konfiguration der anonymen Authentifizierung

Häufig wird auf Webservern ein Zugriff benötigt, bei dem keinerlei Authentifizierung stattfindet. In IIS 8.5 ist diese anonyme Authentifizierung standardmäßig bereits aktiviert. Soll daher den Anwendern der Zugriff auf einige Ordner 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. 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 den Netzwerkmonitor angezeigt werden. Sie können aber den Datenverkehr mit SSL verschlüsseln (siehe Kapitel 30). In diesem Fall ist auch die Standardauthentifizierung verschlüsselt.

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.

Abbildg. 27.24 Die anonyme Authentifizierung kann über den Internetinformationsdienste-Manager für den kompletten Server gesteuert werden



An dieser Stelle aktivieren oder deaktivieren Sie auch die anderen Authentifizierungsoptionen, die auf dem Server verfügbar sein sollen.

Über die Eingabeaufforderung deaktivieren Sie die anonyme Authentifizierung mit dem Befehl

```
appcmd set config /section:anonymousAuthentication /enabled:false
```

Mit dem folgenden Befehl wird die anonyme Authentifizierung wieder aktiviert:

```
appcmd set config /section:anonymousAuthentication /enabled:true
```

Achten Sie darauf, dass der Ordner *C:\Windows\System32\Inetsrv,* in dem sich das Befehlszeilentool Appcmd von IIS 8.5 befindet, nicht im Standardpfad des Servers enthalten ist. Sie müssen daher entweder den Pfad hinzufügen oder in der Eingabeaufforderung zunächst in den Ordner wechseln. Die erfolgreiche Aktivierung oder Deaktivierung wird in der Eingabeaufforderung gemeldet und im IIS-Manager auch angezeigt.

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. Sie können entweder ein spezielles Benutzerkonto auswählen oder es wird das Benutzerkonto verwendet, mit dem der Anwendungspool gestartet wird, in welcher die Anwendung, die den anonymen Zugriff verwendet, gespeichert ist.

Auch diese Einstellungen können Sie in der Eingabeaufforderung durchführen. Dazu verwenden Sie den folgenden Befehl:

```
appcmd set config /section:anonymousAuthentication /userName:<Name> /password:<Kennwort>
```

Konfigurieren 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 (siehe Kapitel 30). 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 aktiviert 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. Sie müssen aber zuvor den Rollendienst für die Standardauthentifizierung aktivieren.

Über die Eingabeaufforderung 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 der Ordner *C:\Windows\System32\Inetsrv*, in dem sich das Befehlszeilentool Appcmd von IIS 8.5 befindet, nicht im Standardpfad des Servers enthalten ist. Sie müssen daher entweder den Pfad hinzufügen, oder in der Eingabeaufforderung zunächst in den Ordner wechseln. Die erfolgreiche Aktivierung oder Deaktivierung wird in der Eingabeaufforderung 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* können Sie auch diese Authentifizierungsmethode konfigurieren.

Über die Eingabeaufforderung deaktivieren Sie die Windows-Authentifizierung mit dem Befehl

```
appcmd set config /section:windowsAuthentication /enabled:false
```

Mit dem folgenden Befehl wird die Windows-Authentifizierung aktiviert:

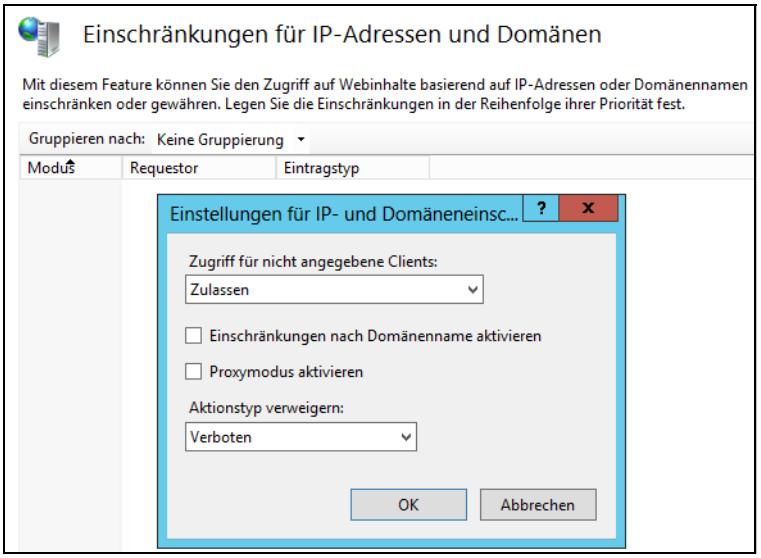
```
appcmd set config /section:windowscAuthentication /enabled:true
```

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 den *Aktionen*-Bereich können bestimmte Zulassungs- oder Verweigerungsregeln für einzelne IP-Adressen oder komplette Bereiche erstellt werden.

Damit 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 muss darüber hinaus zunächst aktiviert werden. Klicken Sie dazu im Bereich *Einschränkungen für IP-Adressen und Domänen* mit der Maustaste auf die Option *Featureeinstellungen bearbeiten*. Damit Sie diese Funktion nutzen können, müssen Sie den Rollendienst *IP- und Domänenbeschränkungen installieren*.

Abbildg. 27.25 Die Einstellungen der Einschränkungen für IPv4-Adressen und Domänen müssen zunächst konfiguriert werden



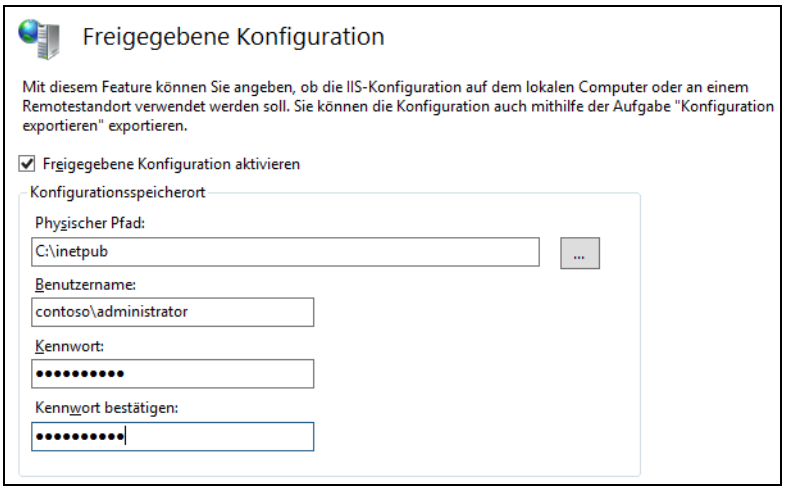
Anschließend öffnet sich ein neues Fenster. Hier legen Sie zunächst fest, was mit Clients passieren soll, für die keine Regeln hinterlegt wurden. Standardmäßig dürfen alle Clients zugreifen, außer die, für die Sie Ablehnungseinträge konfigurieren.

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. 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.

Freigegebene Konfiguration

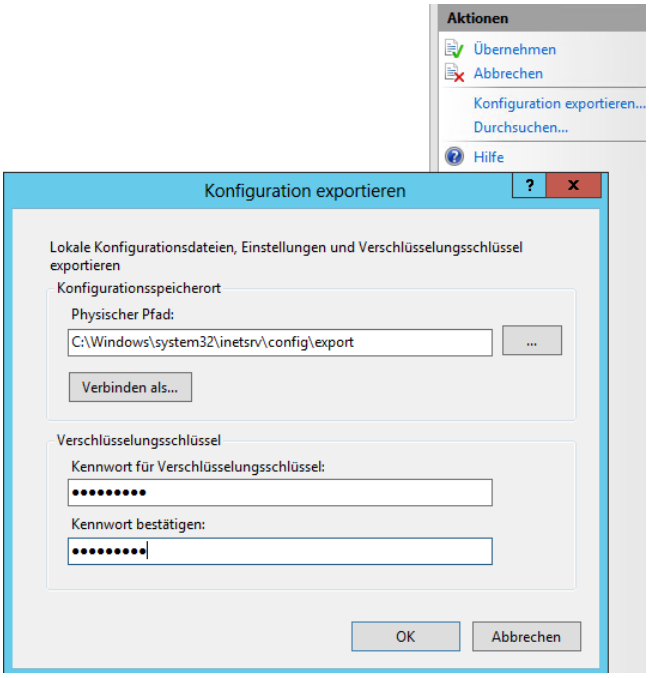
Mit IIS 8.5 ist es möglich, die Konfiguration des Webservers an einer zentralen Stelle im Netzwerk freizugeben, sodass mehrere Webserver von einer zentralen Stelle aus verwaltet werden können. Die Konfiguration dieser Funktion erfolgt im Internetinformationsdienste-Manager im Abschnitt *Verwaltung* über das Feature *Freigegebene Konfiguration*.

Abbildg. 27.26 In IIS 8.5 kann eine Konfiguration für mehrere Webserver konfiguriert werden



Im angegebenen Ordner müssen sich alle Konfigurationsdateien von IIS befinden. Erst dann lässt sich die Konfiguration durchführen. 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.

Abbildg. 27.27 Exportieren der Konfiguration eines Webservers für die gemeinsame Konfiguration



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.

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.

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.html* eingeben, sondern die Seite *default.html* kann in IIS bereits hinterlegt sein.

Sie können aber nicht nur ein Dokument angeben, sondern eine komplette Liste, die der Server nach und nach abarbeitet. Wird kein Standarddokument hinterlegt oder kann der entsprechende Ordner nicht durchsucht werden, erhält der Anwender eine *404 – Datei nicht gefunden*-Meldung.

Festlegen des Standarddokuments

Damit ein Standarddokument angezeigt wird, muss diese Funktion erst aktiviert und entsprechende Standarddokumente hinterlegt sein. Die Konfiguration des Standarddokuments eines Servers findet über das Feature *Standarddokument* im Internetinformationsdienste-Manager statt.

Die Funktion ist standardmäßig bereits aktiviert und es sind einige Dokumente hinterlegt. 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 lassen sich auf Ebene des Servers, aber auch für einzelne Webseiten und Anwendungen hinterlegen.

Abbildg. 27.28 Konfigurieren von Standarddokumenten in IIS

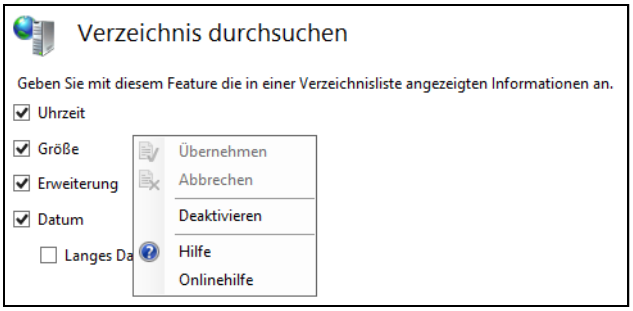
Das Feature *Verzeichnis durchsuchen* aktivieren und verwalten

Neben der Anzeige einer Webseite können Sie auch den Inhalt eines Ordners anzeigen lassen, um zum Beispiel Dokumente zum Download zur Verfügung zu stellen.

Aktivieren Sie im Internetinformationsdienste-Manager das Feature *Verzeichnis durchsuchen* und konfigurieren die Funktion, sehen Anwender den kompletten Inhalt des hinterlegten Ordners wie im Explorer, wenn in der URL nicht ein spezifisches Dokument hinterlegt ist. Auch wenn kein Standarddokument hinterlegt ist oder das Feature *Standarddokument* deaktiviert wurde, sehen Anwender in diesem Fall den ganzen Ordner, keine spezielle Webseite.

Standardmäßig ist dieses Feature deaktiviert. Durch diese Funktion können schnell verschiedene Dateien zur Verfügung gestellt werden, zum Beispiel ohne eine HTML-Seite zu konfigurieren. Klicken Sie im mittleren Bereich der IIS-Konsole doppelt auf den Menüpunkt *Verzeichnis durchsuchen*.

Abbildg. 27.29 Damit der Ordner einer Webseite durchsucht wird, muss die Funktion erst aktiviert werden



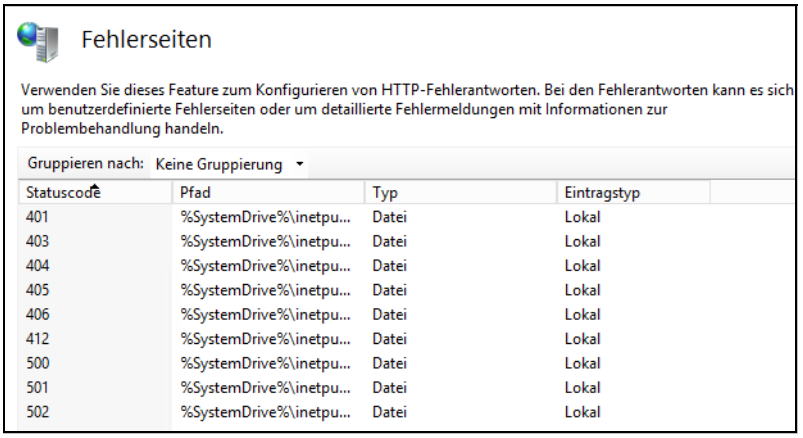
Diese Funktion können Sie auf Ebene des Servers, also der Standardwebseite, oder für einzelne Webseiten und Anwendungen aktivieren. Sollen nicht alle Ordner oder Dateien angezeigt werden, können Sie auch mit NTFS-Berechtigungen arbeiten.

Konfigurieren der HTTP-Fehlermeldungen und -Umleitungen

Auf Ebene des Servers oder der einzelnen Webseiten können Sie die Fehlermeldungen, die den Anwendern angezeigt werden, ebenfalls bearbeiten und konfigurieren. Über das Feature *Fehlerseiten* im Internetinformationsdienste-Manager können Sie sich eine Liste aller hinterlegten Fehlermeldungen anzeigen lassen. Über das Kontextmenü können entweder andere HTML-Seiten hinterlegt oder neue Fehlermeldungen konfiguriert und angezeigt 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.

Abbildg. 27.30 Die Fehlerseiten in IIS können modular bearbeitet werden



Um angepasste Fehlermeldungen anzuzeigen, öffnen Sie die Verwaltung der Fehlerseiten im Internetinformationsdienste-Manager. Klicken Sie im *Aktionen*-Bereich auf den Link *Hinzufügen*. Anschließend öffnet sich ein Dialogfeld, über das Sie die verschiedenen Daten der Fehlermeldung konfigurieren können.

Konfigurieren von HTTP-Umleitungen

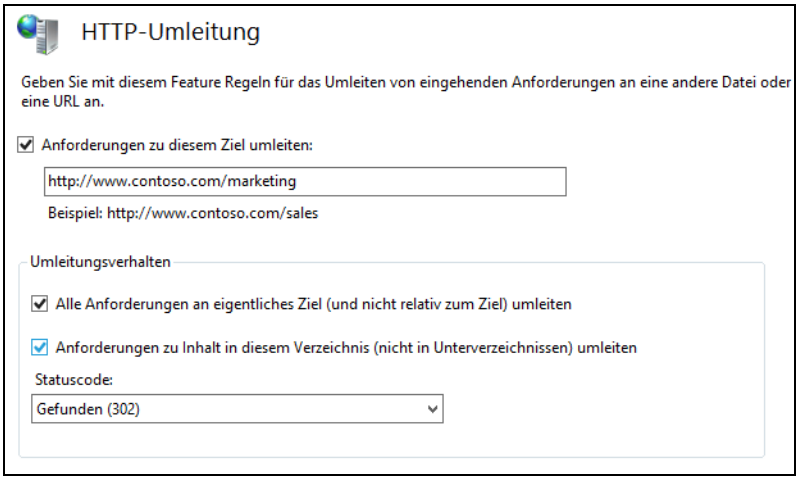
Bei einer HTTP-Umleitung werden alle Zugriffe auf eine bestimmte URL zu einer anderen URL automatisch umgeleitet. So können Sie zum Beispiel Ihre Seite umleiten lassen, wenn Teile davon bearbeitet werden.

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 Sie auf Serverebene oder auf Ebene der Webseiten über das Feature *HTTP-Umleitung* durchführen. Sie müssen diese Funktion aber zunächst als Rollendienst installieren.

Neben der Umleitung können Sie an dieser Stelle auch das Verhalten dieser Konfiguration festlegen. 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 Unterordner gestellt werden. Aktivieren Sie das Kontrollkästchen *Anforderungen zu Inhalt in diesem Verzeichnis (nicht in Unterverzeichnissen) umleiten*, leitet der Server Anfragen, die an Unterordner des umgeleiteten Ordners gerichtet sind, direkt an das Weiterleitungsziel um.

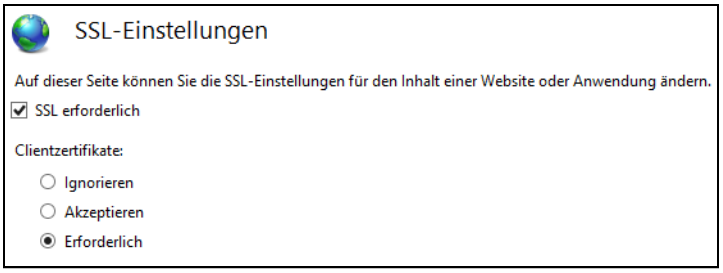
Abbildg. 27.31 Konfigurieren der HTTP-Umleitung



Automatische Umleitung auf SSL-Seiten aktivieren

Versuchen Anwender per HTTP auf die Seite zuzugreifen, erhalten diese eine HTTP-403-Fehlermeldung, wenn Sie SSL aktiviert und in den Einstellungen von IIS festgelegt haben. In Kapitel 30 beschreiben wir das Thema SSL ausführlicher.

Abbildg. 27.32 Erzwingen von SSL in IIS von SharePoint Server 2010



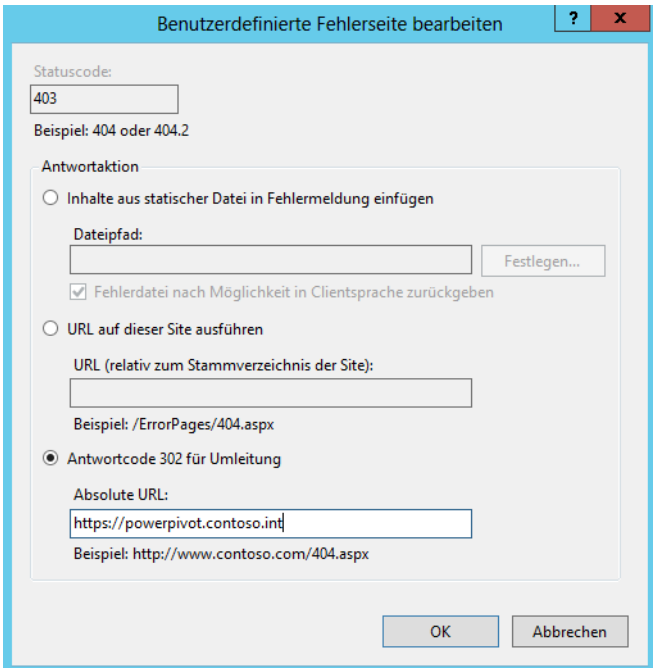
Solche Fehlermeldungen verwirren allerdings die meisten Anwender und belasten unnötig die IT-Abteilung. Aus diesem Grund ist der beste Weg, wenn Sie statt der Anzeige des Fehlers eine automatische Umleitung auf die richtige SSL-Adresse auf dem Server hinterlegen.

Sie haben zwei Möglichkeiten der Umleitung. Die entsprechende Konfiguration führen Sie in der Konfiguration der HTTP-403-Fehlermeldung durch:

1. Rufen Sie auf dem Server den IIS-Manager auf.
2. Klicken Sie auf den Servernamen. Alternativ können Sie diese Umleitung auch durchführen, wenn Sie die Website anklicken. Auch hier gibt es die Option *Fehlerseiten*.

3. Doppelklicken Sie auf der Startseite im Bereich *IIS* auf *Fehlerseiten*.
4. Klicken Sie doppelt auf den Fehler 403.
5. Aktivieren Sie die Option *Antwortcode 302 für Umleitung* und tragen Sie die HTTPS-URL ein, auf die die Anwender zugreifen sollen.
6. Bestätigen Sie mit *OK*.

Abbildg. 27.33 Aktivieren einer automatischen Umleitung für HTTP-Anfragen

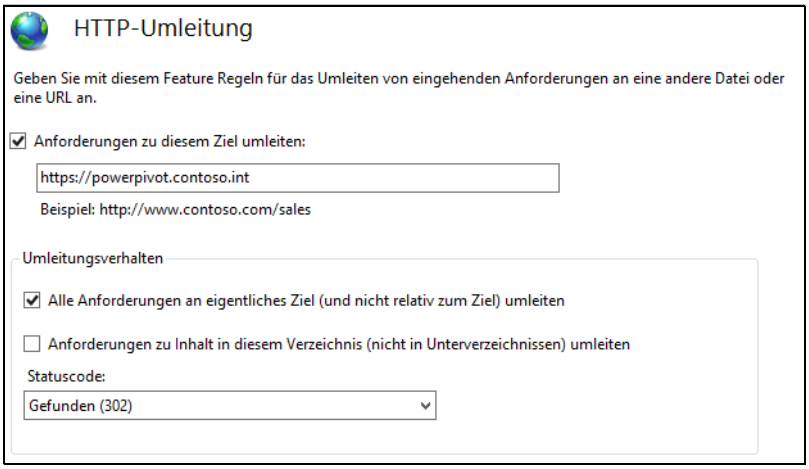


Diese Art der Umleitung funktioniert allerdings nicht immer, in diesem Fall verwenden Sie die zweite Möglichkeit für die Umleitung:

1. Starten Sie den IIS-Manager.
2. Klicken Sie auf die Seite, für die Sie die HTTP-Umleitung konfigurieren wollen.
3. Klicken Sie auf *Bindungen* (siehe auch Kapitel 30).
4. Ändern Sie den Port der Bindung von Port 80 auf einen anderen freien Port ab, zum Beispiel 8001.
5. Klicken Sie mit der rechten Maustaste auf *Sites* und erstellen Sie eine neue Website mit dem Befehl *Website hinzufügen*.
6. Weisen Sie der neuen Website bei *Sitename* den Namen zu, mit dem Anwender per HTTP auf den Server zugreifen, zum Beispiel *powerpivot.contoso.int*.
7. Legen Sie einen physischen Pfad an. Der Ordner bleibt leer, Sie benötigen diesen nur wegen IIS, nicht für die Konfiguration.

8. Belassen Sie die Bindung auf Port 80. Da Sie die Bindung der Standardseite bereits geändert haben, ist dieser Port frei. Tragen Sie als Hostname noch den Namen ein, auf den der Server antworten soll, zum Beispiel *powerpivot.contoso.int*.
9. Bestätigen Sie die Erstellung der Website. Sie erhalten eine Meldung, dass der Port 80 bereits gelegt ist, auch wenn Sie den Port der SharePoint-Site von 80 auf einen anderen Port geändert haben. Dies liegt daran, dass der Port 80 noch der *Default Web Site* innerhalb von IIS zugeordnet ist. SharePoint beendet diese Site aber bei der Installation, sodass diese auf SharePoint-Servern keine Bedeutung mehr hat.
10. Klicken Sie als Nächstes auf die neu erstellte Seite und doppelklicken dann im Bereich *IIS* auf *HTTP-Umleitung*.
11. Aktivieren Sie das Kontrollkästchen *Anforderungen zu diesem Ziel umleiten*.
12. Tragen Sie die HTTPS-Adresse ein, zu welcher der Server die Anfragen umleiten soll.
13. Aktivieren Sie das Kontrollkästchen *Alle Anforderungen an eigentliches Ziel umleiten*.
14. Klicken Sie auf *Übernehmen*.
15. Geben Anwender jetzt die URL ein, für die Sie eine Umleitung konfiguriert haben, wird der Zugriff von IIS erkannt und leitet die Anfrage automatisch um.

Abbildg. 27.34 Aktivieren einer automatischen Umleitung



Vereinfachen von URLs

Damit Anwender zum Beispiel auf Outlook Web App zugreifen können, müssen sie die URL *https://<Clientzugriff-Server>/owa* verwenden. Sie können aber diese URL vereinfachen. Ein Beispiel ist, dass Sie alle Zugriffe auf den Clientzugriffserver zur URL */owa* weiterleiten. Eine weitere Möglichkeit ist, dass Sie einen DNS-Eintrag *mail* erzeugen, damit Anwender nur noch *https://mail.<Domäne>* für den Zugriff eingeben müssen. Gehen Sie für die Konfiguration folgendermaßen vor:

1. Öffnen Sie den IIS-Manager auf dem Server.
2. Erweitern Sie *<Servername>\Sites*.
3. Klicken Sie auf *Default Web Site*.
4. Im rechten Bereich des Fensters finden Sie unten die Option *HTTP-Umleitung*.

5. Öffnen Sie das Feature per Doppelklick.
6. Aktivieren Sie die Option *Anforderungen zu diesem Ziel umleiten*.
7. Geben Sie den vollständigen Pfad zu OWA ein, zum Beispiel *https://dell-exchange01.contoso.com/owa*.
8. Aktivieren Sie im Bereich *Umleitungsverhalten* die Option *Anforderungen zu Inhalt in diesem Verzeichnis (nicht in Unterverzeichnissen) umleiten*.
9. Wählen Sie bei *Statuscode* die Option *Gefunden (302)* aus.
10. Bestätigen Sie die Eingabe durch Klicken auf *Übernehmen*.
11. Geben Sie in der Eingabeaufforderung den Befehl *iisreset* ein, um IIS auf dem Server neu zu starten.

ACHTUNG Konfigurieren Sie eine HTTP-Umleitung für eine übergeordnete Webseite, übernimmt IIS diese Einstellung für alle untergeordneten Webseiten und virtuellen Ordner.

Wollen Sie die Umleitung für diese untergeordneten Ordner deaktivieren, klicken Sie auf den Ordner und wählen Sie auch hier das Feature *HTTP-Umleitung* aus, um es zu deaktivieren. Das ist zum Beispiel für Autodiscover oder den Remotezugriff der PowerShell sinnvoll.

IIS 8.5 überwachen und Protokolldateien 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 Ordnern abgewickelt werden.

Ablaufverfolgungsregeln für Anforderungsfehler

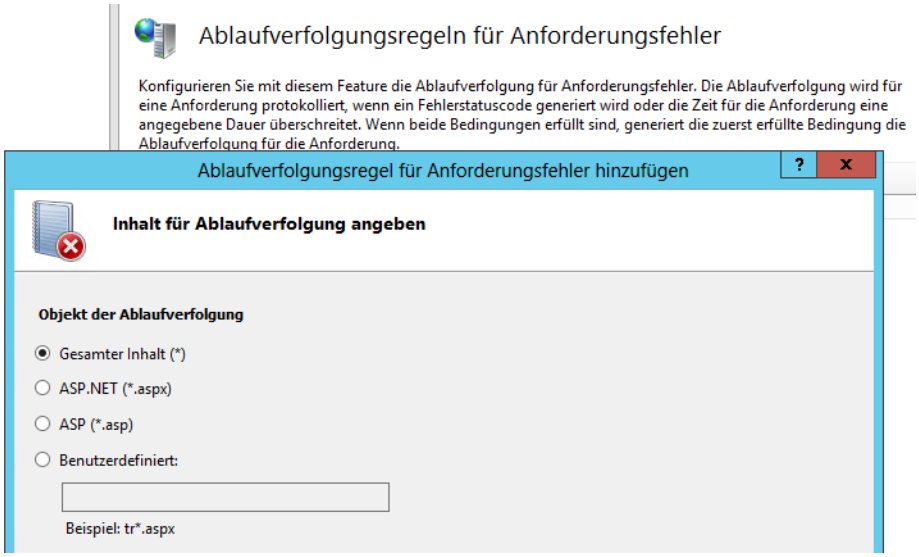
Doppelklicken Sie im Internetinformationsdienste-Manager auf das Feature *Ablaufverfolgungsregeln für Anforderungsfehler*, können Sie Regeln erstellen, mit denen Sie die fehlerhaften Zugriffe auf den Server überwachen.

Neue Regeln lassen sich über das Kontextmenü oder den *Aktionen*-Bereich erstellen. Das Feature ist aber erst verfügbar, wenn Sie die Rollendienste *Ablaufverfolgung* und *Anforderungsüberwachung* bei *Systemzustand und Diagnose* installieren.

Auf der nächsten Seite des Assistenten legen Sie fest, welche Fehler protokolliert werden sollen. Sobald eine der hinterlegten Bedingungen auftritt, wird der Fehler protokolliert.

Auf einer weiteren Seite des Assistenten legen Sie fest, welche der Anbieter Sie überwachen wollen, 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.

Abbildg. 27.35 Erstellen und Verwalten von Regeln für die Ablaufverfolgung



Nach der Erstellung der Regel wird diese im Fenster angezeigt. Sie können weitere Regeln erstellen und vorhandene Regeln können Sie über deren Kontextmenü bearbeiten. Die Protokolldateien sind standardmäßig im Ordner *\inetpub\logs\FailedReqLogFiles* gespeichert.

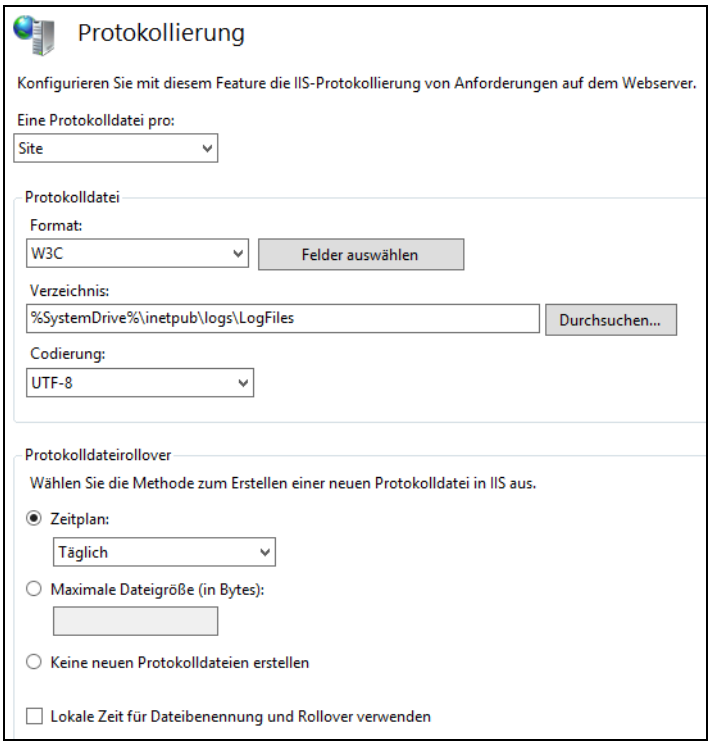
Allgemeine Protokollierung aktivieren und konfigurieren

Neben der Ablaufverfolgung für fehlerhafte Anforderungen können Sie auch den normalen Betrieb von IIS protokollieren. 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. Standardmäßig ist die Protokollierung für den Server an sich und für Webseiten aktiviert.

Über den *Aktionen*-Bereich der Konsole kann die Protokollierung für einzelne Bereiche gezielt deaktiviert werden. Die Protokolldateien können in einem beliebigen Ordner abgelegt werden und befinden sich standardmäßig im Ordner *\inetpub\logs\LogFiles*.

Abbildg. 27.36 Konfigurieren der Protokollierung für IIS



Im ersten Auswahlfeld wählen Sie über ein Listenfeld aus, 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 (*http://www.microsoft.com/en-us/download/details.aspx?id=24659* [Ms179-K27-04]) 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, ein-

schließlich 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 eine 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* [Ms179-K27-05]).

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

In diesem Abschnitt gehen wir auf Möglichkeiten ein, Anfragen an IIS mit den Bordmitteln des Internetinformationsdienste-Managers zu verbessern.

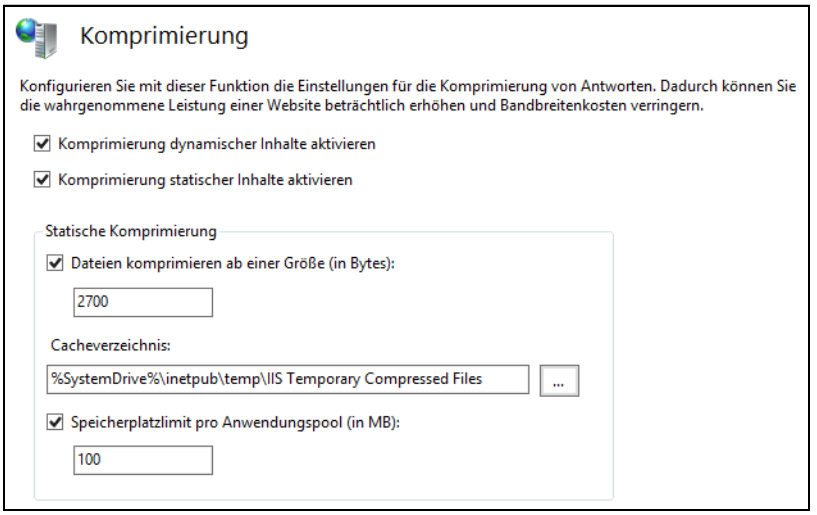
Komprimierung aktivieren

Mit der Komprimierung werden die Antwortzeiten eines Servers verbessert und bei der Übertragung von Webseiten kann Bandbreite gespart werden. Die Komprimierung steuern Sie über das Feature *Komprimierung* im Internetinformationsdienste-Manager.

Manche Einstellungen stehen nur auf Serverebene zur Verfügung. Viele Einstellungen können Sie aber auch auf Ebene der Websites und Anwendungen vornehmen, sodass jede Anwendung eigene Einstellungen für die Komprimierung verwenden kann. Aktivieren Sie die Komprimierung, belastet das zwar die Serverhardware, aber die Netzwerkleistung erhöht sich. 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 8.5 die Komprimierung von statischen Inhalten standardmäßig bereits aktiviert.

Haben Sie statischen 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. Damit Sie auch dynamische Inhalte komprimieren können, müssen Sie zunächst den entsprechenden Rollendienst installieren.

Abbildg. 27.37 Konfigurieren der Komprimierung für IIS

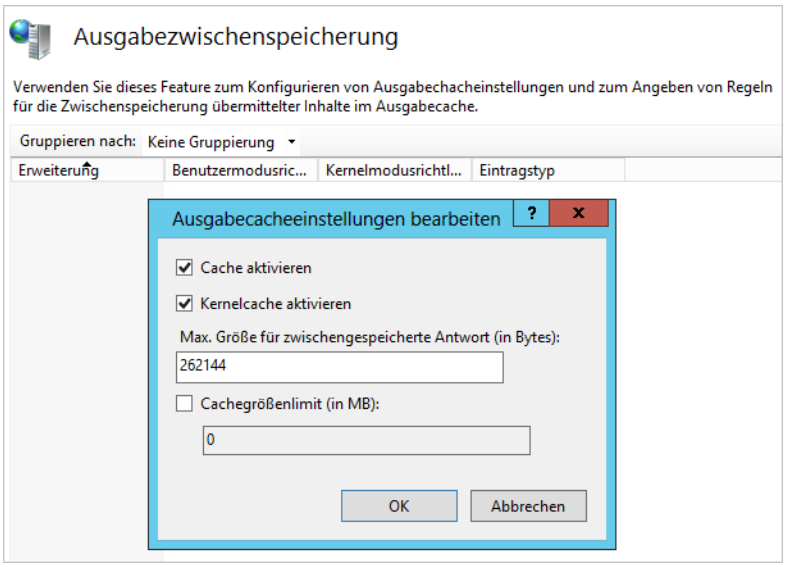


Sie können hier auch festlegen, ab welcher Größe Dateien komprimiert werden sollen und wie viel Speicherplatz jedem Anwendungspool und den darin enthaltenen Webseiten und Anwendungen zur Verfügung steht. Auch der Speicherplatz des Caches wird an dieser Stelle festgelegt.

Ausgabezwischenspeicherung verwenden

Im Cache des Webservers können Teile der Webseiten zur Verfügung gestellt werden, sodass die Abrufe dieser Teile den Server nicht belasten. 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 *Aktionen*-Bereich vorgenommen.

Abbildg. 27.38 Konfigurieren der Ausgabezwischenspeicherung



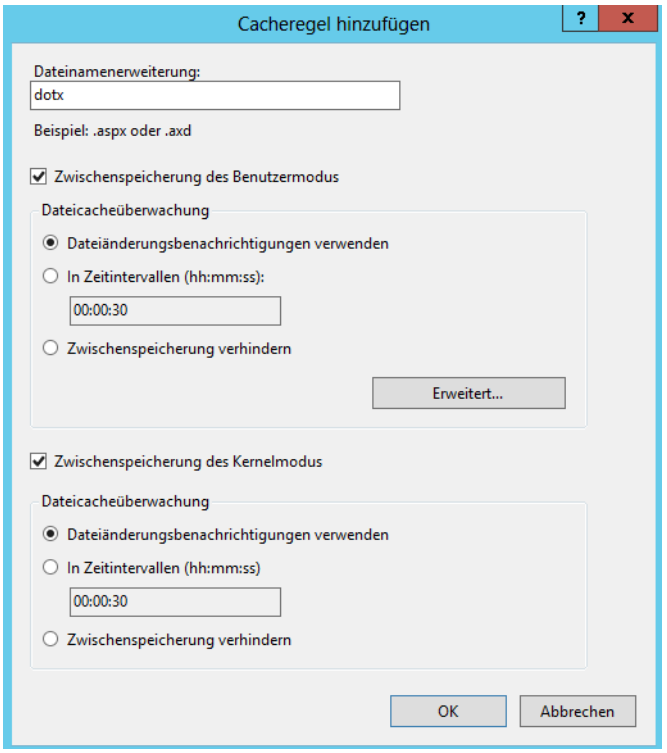
Der Cache ist standardmäßig aktiviert. In den Einstellungen können Sie die Funktion aktivieren sowie ein Limit festlegen. Der Cache wird allerdings erst dann produktiv genutzt, wenn Regeln festgelegt sind, die bestimmen, welche Daten der Server zwischenspeichern soll.

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. 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 erstellen Sie neue Regeln für den Cache. Es öffnet sich ein neues Fenster, über das Einstellungen vorgenommen werden, wie Inhalte für den Benutzermodus und den Kernelmodus zwischengespeichert werden sollen. Zunächst legen Sie fest, welche Dateien zwischengespeichert werden können. Als Nächstes legen Sie fest, wie lange die Daten im Zwischenspeicher verbleiben sollen.

Sie können entweder eine Zwischenspeicherung bis zur Änderung der Datei oder ein Zeitintervall festlegen. Auch das generelle Verhindern der Zwischenspeicherung für einige Dateitypen kann an dieser Stelle konfiguriert werden. Sie können beliebig viele Cacheregeln erstellen. Die Regeln lassen sich nach der Erstellung jederzeit bearbeiten.

Abbildg. 27.39 Aktivieren des Caches



FTP-Server betreiben

Mit IIS 8.5 lässt sich auch ein FTP-Server betreiben, um zum Beispiel 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.

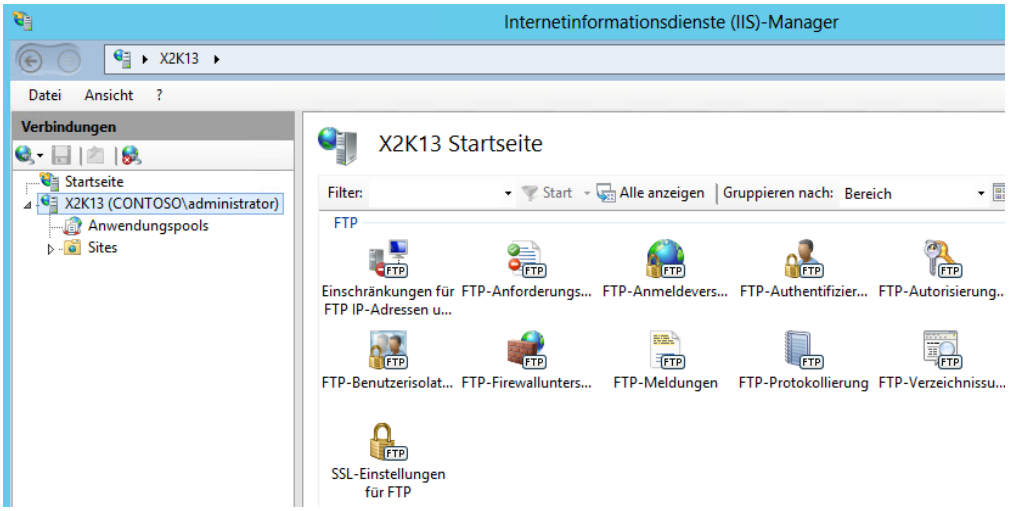
Damit IIS auch als FTP-Server verwendet werden kann, benötigen Sie den Rollendienst *FTP-Server*. Sie können in Windows Server 2012 R2 FTP auch mit SSL zur Verfügung stellen. Mit dem FTP-Server lässt sich ein virtueller Hostname für eine FTP-Site festlegen. Dadurch können Sie mehrere FTP-Sites erstellen, die zwar dieselbe IP-Adresse verwenden, aber auf Basis ihrer eindeutigen virtuellen Hostnamen unterschieden werden. Über einen Webbrowser greifen Sie mit der Adresse *ftp://<Servername>* zu. Sie können im Ordner normale Unterordner anlegen und mit NTFS-Berechtigungen arbeiten.

Konfigurieren 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.

Die Einstellungen zu FTP finden Sie nach der Installation über den Bereich *FTP* im Internetinformationsdienste-Manager.

Abbildg. 27.40 FTP mit Windows Server 2012 R2 verwenden



Schritt-für-Schritt-Anleitung zum Installieren eines FTP-Servers in IIS 8.5

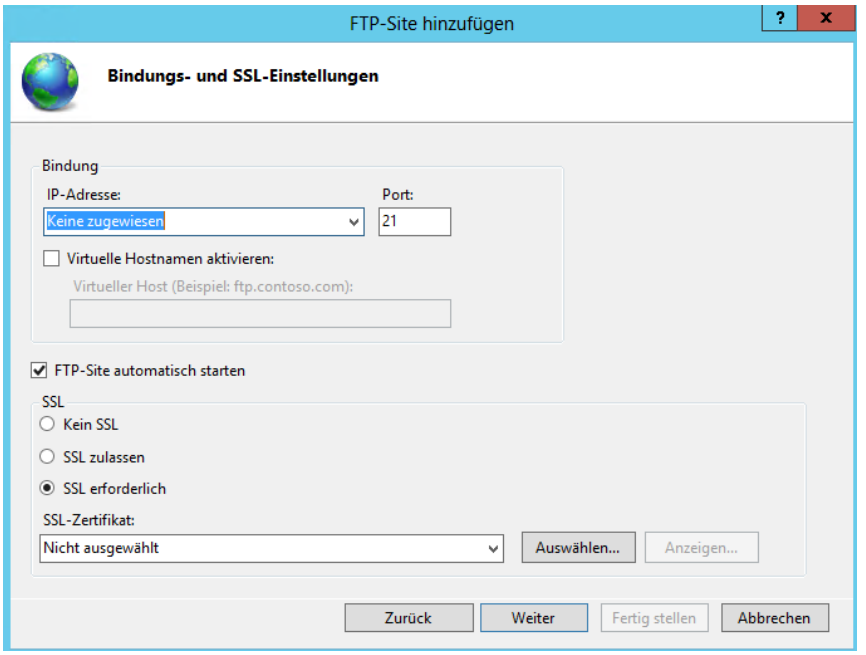
Die Installation eines FTP-Servers ist schnell durchgeführt. In den folgenden Abschnitten zeigen wir Ihnen Schritt für Schritt, wie Sie einen FTP-Server installieren, einrichten und betreiben.

FTP-Server installieren

Zunächst müssen Sie den Rollendienst *FTP-Server* für IIS installieren. Anschließend steht die Verwaltung im IIS-Manager zur Verfügung. Nach der Installation müssen Sie zunächst eine FTP-Site erstellen:

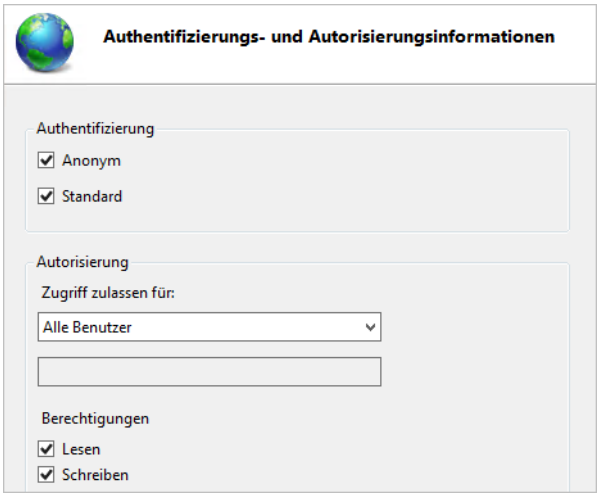
1. Klicken Sie zum Erstellen einer FTP-Site mit der rechten Maustaste auf den Menüpunkt *Sites* im IIS-Manager und wählen Sie *FTP-Site hinzufügen*.
2. Es startet der Assistent zur Einrichtung. Geben Sie den Namen sowie den Ordner auf der Festplatte an, in dem die Daten des FTP-Servers liegen.
3. Auf der nächsten Seite konfigurieren Sie die IP-Adresse, den Port und auf Wunsch einen virtuellen Hostnamen, wenn Sie zum Beispiel mehrere FTP-Server betreiben wollen.
4. Auf dieser Seite können Sie auch SSL für den FTP-Server aktivieren sowie das passende Zertifikat auswählen.

Abbildg. 27.41 Konfigurieren einer FTP-Site in IIS 8



5. Als Nächstes wählen Sie aus, welche Authentifizierung Sie auf dem Server unterstützen möchten und welche Rechte diese Benutzer haben sollen.
6. Klicken Sie anschließend auf *Fertig stellen*, um die Seite zu erstellen.

Abbildg. 27.42 Festlegen der Rechte für den FTP-Server



Anschließend sehen Sie die FTP-Site im IIS-Manager wie jede andere Website und können Einstellungen für diese Seite zur Verwaltung vornehmen. Andere Tools benötigen Sie an dieser Stelle nicht.

Firewall konfigurieren

Wollen Sie die Authentifizierung weiter anpassen, wählen Sie den Menüpunkt *FTP-Authentifizierung* aus. Über den Menüpunkt *FTP-Firewallunterstützung* legen Sie fest, welche Ports der Server unterstützen soll und auf welche externe IP-Adresse der FTP-Server hören soll. Sollte der Verbindungsaufbau von Clients zum Port 21 nicht funktionieren, müssen Sie diesen Port in der Windows-Firewall erst freischalten.

Neben diesen Einstellungen müssen Sie, abhängig von Ihrer Konfiguration, weitere Einstellungen in der Firewall vornehmen, indem Sie neue Regeln erstellen.

Verwenden Sie dazu den folgenden Befehl:

```
netsh advfirewall firewall add rule name="FTP (non-SSL)" action=allow protocol=TCP dir=in
localport=21
```

Wollen Sie dynamische Ports für FTP freischalten und die statusbehaftete FTP-Filterung verwenden, geben Sie den folgenden Befehl ein:

```
netsh advfirewall set global StatefulFtp enable
```

Mit dem folgenden Befehl deaktivieren Sie die Filterung wieder:

```
netsh advfirewall set global StatefulFtp disable
```

Wollen Sie FTP über SSL erlauben, müssen Sie auch diesen Verkehr freischalten. Verwenden Sie dazu den Befehl

```
netsh advfirewall firewall add rule name="FTP for IIS7" service=ftpsvc action=allow
protocol=TCP dir=in
```

Abbildg. 27.43 Freischalten der notwendigen Firewallregeln für FTP-Server

```
C:\Users\administrator.CONTOSO>netsh advfirewall firewall add rule name="FTP (no
n-SSL)" action=allow protocol=TCP dir=in localport=21
OK.

C:\Users\administrator.CONTOSO>netsh advfirewall set global StatefulFtp enable
OK.

C:\Users\administrator.CONTOSO>netsh advfirewall firewall add rule name="FTP for
 IIS7" service=ftpsvc action=allow protocol=TCP dir=in
OK.
```

Authentifizierung konfigurieren

Über das Kontextmenü von *Anonyme Authentifizierung* oder *Standardauthentifizierung* legen Sie fest, über welches Benutzerkonto oder Domäne die jeweilige Anmeldung erfolgen soll. Die Konfiguration ist grundsätzlich identisch zur Konfiguration der jeweiligen Einstellung für Webseiten.

Über das Kontextmenü können Sie die jeweilige Anmeldung auch aktivieren oder deaktivieren. Über FTP-Autorisierungsregeln konfigurieren Sie die Rechte, die Benutzer auf die FTP-Site erhalten sollen. Neben den standardmäßig vorhandenen Regeln können Sie zusätzliche Regeln anlegen oder bestehende Regeln anpassen.

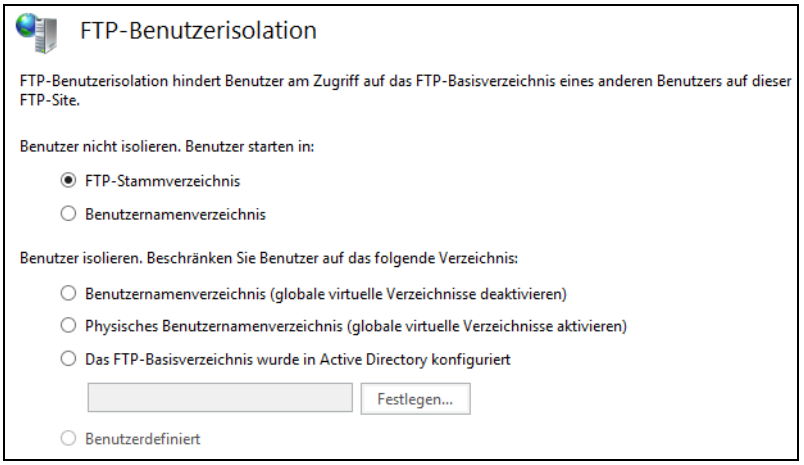
Die Möglichkeit, den IIS fernzuwarten, indem Sie den Verwaltungsdienst nutzen, funktioniert auch für den FTP-Server. Gehen Sie zur Einrichtung der Fernwartung analog vor. In diesem Fall müssen Sie bei der FTP-Authentifizierung noch über den Menüpunkt *Benutzerdefinierte Anbieter* das Modul *IisManagerAuth* aktivieren.

Daraufhin wird bei der FTP-Authentifizierung zusätzlich noch die Authentifizierung über den IIS-Manager angezeigt. Anschließend müssen Sie über *IIS-Manager-Berechtigungen/Benutzer zulassen* noch identische Einstellungen vornehmen, wie bei der Delegierung von IIS-Seiten. Legen Sie am besten für die FTP-Verwaltung einen eigenen Benutzer im IIS-Manager an und schalten Sie diesen dann explizit für FTP frei. Anschließend müssen Sie für den Adminbenutzer die gleichen Zulassungsregeln analog erstellen, wie für normale FTP-Benutzer auch. Um auf den Server zuzugreifen, verwenden Sie entweder ein FTP-Programm oder den Internet Explorer.

FTP-Benutzerisolation einsetzen

Mit der Benutzerisolation für FTP können Sie einzelne Benutzer auf dem FTP-Server voneinander abschotten und für Anwender jeweils einen eignen Ordner zur Verfügung stellen. Aktivieren Sie *Benutzernamenverzeichnis*, werden die Benutzer mit ihrem eigenen Verzeichnis auf dem FTP-Server verbunden, aber nicht isoliert.

Abbildg. 27.44 Konfigurieren der FTP-Benutzerisolation



Der Ordner muss die gleiche Bezeichnung wie der Benutzernamen des Anwenders haben. Ist ein solcher Ordner oder auch virtueller Ordner nicht vorhanden, wird der Benutzer mit dem Stammordner auf dem FTP-Server verbunden. Aktivieren Sie die Option *FTP-Stammverzeichnis*, sehen alle Anwender den gleichen Ordner, die Isolierung ist komplett deaktiviert.

Die Ordnernamen variieren von der Authentifizierungsebene:

- Verwenden Sie Benutzer innerhalb von IIS und die anonyme Verbindung, müssen Sie im FTP-Rootordner die Ordnerstruktur *<LocalUser>\Public* anlegen
- Arbeiten Sie mit lokalen Benutzerkonten auf dem Server auf IIS-Ebene und nicht mit der anonymen Authentifizierung, verwenden Sie *%FtpRoot%\LocalUser\%UserName%* als Pfad

- Arbeiten Sie mit lokalen Benutzerkonten auf dem Server auf Windows-Ebene und nicht mit der anonymen Authentifizierung, verwenden Sie *%FtpRoot%\LocalUser\%UserName%* als Pfad
- Arbeiten Sie mit Domänenkonten, verwenden Sie den Pfadnamen *%FtpRoot%\%UserDomain%\%UserName%*.

Die Pfadangabe *%FtpRoot%* entspricht dabei dem Stammordner der FTP-Seite, die Sie erstellt haben. Alle virtuellen Ordner, die Sie auf der Stammebene der FTP-Seite erstellt haben, können von allen Benutzern eingesehen werden, die über entsprechende Rechte verfügen.

Aktivieren Sie eine der Isolierungsoptionen im unteren Bereich, stehen folgende Auswahlmöglichkeiten zur Verfügung. In diesem Fall sehen die Anwender nur den isolierten Bereich, keinerlei andere Ordner:

- **Benutzernamenverzeichnis** Bei dieser Option dürfen Benutzer nur auf ihren eigenen Ordner zugreifen und in der Navigation in der Baumstruktur in keine anderen Ordner wechseln
- **Physikalisches Benutzernamenverzeichnis** Bei dieser Option erhalten Anwender nur Zugriff auf physisch vorhandene FTP-Ordner, keine virtuellen Ordner. Sind globale, virtuelle Ordner auf dem Server vorhanden, sind diese für alle Anwender zugreifbar.
- **Das FTP-Basisverzeichnis in Active Directory konfiguriert** Bei dieser Option legen Sie den Zugriff auf den Stammordner im Benutzerkonto in Active Directory des Anwenders fest

Virtuelle Ordner legen Sie über das Kontextmenü der FTP-Seite im IIS-Manager an. Diese verweisen auf einen physischen Ordner, den Sie entweder vorher oder während der Einrichtung der virtuellen Seiten anlegen können. Wollen Sie in einer isolierten Umgebung Zugriffe auf Benutzerebene festlegen, sollten Sie innerhalb des FTP-Stammordners einen weiteren Ordner mit der Bezeichnung der Benutzerdomäne oder der Bezeichnung *LocalUser* anlegen. Innerhalb dieses Ordners legen Sie dann die Ordner der jeweiligen Benutzer fest.

Ordnername, virtueller Ordner und Benutzername müssen übereinstimmen. Sind globale Ordner deaktiviert, reicht es auch, einzelnen Anwendern nur virtuelle Ordner zur Verfügung zu stellen. Der einfachste Weg, eine zuverlässig funktionierende Benutzerisolierung durchzuführen, ist das Anlegen von physischen Ordnern, das Erstellen von virtuellen Ordnern mit Verweis auf die physischen Ordner und das durchgehend einheitliche Verwenden der gleichen Bezeichnungen der Ordnernamen und Benutzernamen. Wichtig ist auch das lokale Anlegen des Ordners *LocalUser* oder der jeweiligen Domäne. Legen Sie alle Ordner innerhalb des FTP-Stammordners an.

Die einzelnen physischen Ordner der Anwender können Sie auch mit NTFS-Berechtigungen absichern, wenn Sie mit Windows- oder Domänenkonten arbeiten. Wollen Sie zusätzlich noch Quotas einsetzen, verwenden Sie am besten den Ressourcen-Manager für Dateiserver (siehe Kapitel 21).

E-Mail-Anbindung von Servern

Wenn Sie auf einem Server mit Windows Server 2012 R2 eine Serveranwendung betreiben, die eingehende oder ausgehende E-Mails verwenden muss, zum Beispiel SharePoint, können Sie den internen SMTP-Dienst in Windows Server 2012 R2 verwenden.

Sie können zum Beispiel SharePoint für eingehende E-Mails konfigurieren. Durch diese Funktion können SharePoint-Websites E-Mails und Anlagen in Listen und Bibliotheken empfangen und automatisch speichern. In einer einfachen Lösung installieren Sie den SMTP-Dienst auf dem Server mit SharePoint. Für ein einfaches Szenario muss auf mindestens einem Server der SMTP-Dienst installiert und konfiguriert sein.

SMTP-Dienst installieren und verwenden

Der SMTP-Dienst gehört zum Lieferumfang von Windows Server 2012 R2. Diesen zu installieren und einzurichten ist kein kompliziertes Unterfangen. Dabei gehen Sie folgendermaßen vor:

1. Öffnen Sie den Server-Manager.
2. Klicken Sie auf *Verwalten/Rollen und Features hinzufügen*.
3. Wählen Sie auf der Seite *Features auswählen* die Option *SMTP-Server* aus.
4. Schließen Sie den Assistenten durch Bestätigen der jeweils angezeigten Seite ab.

Zum Verwalten des SMTP-Diensts verwenden Sie den IIS 6.0-Manager. Diesen installiert der Assistent automatisch zusätzlich zum SMTP-Server.

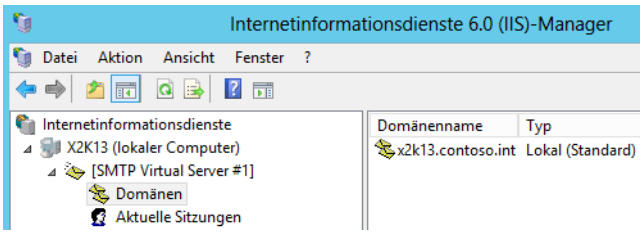
SMTP-Dienst konfigurieren

Zur Verwaltung des SMTP-Diensts und der Konfiguration des Nachrichteneingangs starten Sie über die Programmgruppe *Tools* im Server-Manager den *Informationsdienste 6.0 (IIS)-Manager*. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf den virtuellen SMTP-Server und dann auf *Starten*. Ist die Option abgeblendet dargestellt, ist der Server bereits aktiv. Als Nächstes passen Sie den SMTP-Server für die Unterstützung von anderen Serveranwendungen, zum Beispiel SharePoint an:

1. Klicken Sie mit der rechten Maustaste auf den virtuellen SMTP-Server und dann auf *Eigenschaften*.
2. Holen Sie die Registerkarte *Zugriff* in den Vordergrund und klicken Sie im Bereich *Zugriffssteuerung* auf *Authentifizierung*.
3. Aktivieren Sie das Kontrollkästchen *Anonymer Zugriff*.
4. Bestätigen Sie mit *OK*.
5. Klicken Sie auf der Registerkarte *Zugriff* im Bereich *Relayeinschränkungen* auf *Relay*.
6. Aktivieren Sie die Option *Alle, mit Ausnahme der Computer in der Listen unten*. Alternativ können Sie auch die einzelnen Server, von denen Sie E-Mails entgegen nehmen wollen, manuell in der Liste aufnehmen.
7. Klicken Sie auf *OK*.
8. Öffnen Sie die Verwaltung der Systemdienste, indem Sie *services.msc* auf der Startseite eintippen.
9. Klicken Sie auf *Simple Mail Transfer Protocol (SMTP)* und wählen Sie dann den automatischen Start für den Dienst aus. Stellen Sie sicher, dass der Dienst gestartet ist.

Stellen Sie sicher, dass die in IIS unter dem SMTP-Server aufgelisteten Domänen, die SharePoint oder ein anderer Serverdienst empfangen soll, dem vollqualifizierten Domänennamen des E-Mail-empfangenden Servers entsprechen, zum Beispiel *sps2010.contoso.com*.

Abbildg. 27.45 Überprüfen des korrekten Namens des SMTP-Servers



Die Server, die E-Mails senden, müssen den Namen in DNS auflösen können. Am besten testen Sie das mit Nslookup. Damit die Auflösung funktioniert, muss die DNS-Zone entweder die automatische Registrierung von Einträgen unterstützen oder Sie müssen manuell einen Host-Eintrag für den Server in der Zone erstellen lassen. In den IP-Einstellungen auf dem Server muss der DNS-Server eingetragen sein, der die Zone auflösen kann, damit eine automatische Registrierung erfolgen kann.

Wollen Sie auf dem Server eine eigene Domäne erstellen und verwalten, die Sie für den E-Mail-Empfang verwenden wollen, müssen Sie wieder den IIS6-Manager auf dem Server starten und mit der rechten Maustaste auf *Domänen* klicken. Erstellen Sie dann mit *Neu/Domäne* eine eigene Domäne. Wählen Sie für die neue SMTP-Domäne die Option *Alias*. Als Name für die Domäne geben Sie die Adresse ein, mit welcher der Server E-Mails empfangen soll.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie den neuen Webserver in Windows Server 2012 R2 mit der Version IIS 8.5 betreiben. Erläutert wurden auch die Installation, Einrichtung und Absicherung von Webservern. Ebenso sind wir auf die Verwaltung in der Eingabeaufforderung sowie das Erstellen von neuen Webseiten eingegangen. Und schließlich konnten Sie mehr über den Betrieb eines FTP-Servers erfahren und einige Praxistricks zum Einsatz von IIS lesen.

Im nächsten Kapitel gehen wir auf die Einrichtung der Remotedesktopdienste und der Anbindung von Anwendern ein. Auch die Virtualisierung über den Remotedesktop ist Bestandteil des nächsten Kapitels.

Teil G

Private Cloud und Desktop-virtualisierung

Kapitel 28

Remotedesktopdienste – Anwendungen virtualisieren

In diesem Kapitel:

Mit den Remotedesktopdiensten (ehemals Terminalserver) stellen Sie Anwendungen oder den Desktop für Anwender zentral auf Servern zur Verfügung. Im Vergleich zu Windows Server 2008 R2 hat Microsoft weitere Neuerungen in die Remotedesktopserver integriert. Mit den Remotedesktopdiensten hat Microsoft bereits in Windows Server 2008 R2 zahlreiche Funktionen eingeführt, die auch in Windows Server 2012 R2 weiter verfügbar sind.

TIPP Viele Informationen zu den Remotedesktopdiensten erhalten Sie im Blog der Entwickler auf der Seite *http://blogs.msdn.com/b/rds* [Ms179-K28-01].

Neuerungen bei den Remotedesktopdiensten

Die Neuerungen von Windows Server 2012 hat die neue Version Windows Server 2012 R2 weiterhin mit an Bord. Im folgenden Abschnitt zeigen wir Ihnen die Neuerungen, die Microsoft zusätzlich in Windows Server 2012 R2 integriert.

Eine wichtige Neuerung in Windows Server 2012 R2 ist ein alter Bekannter, die Sitzungsspiegelung. Mit dieser Funktion konnten Administratoren in Vorgängerversionen von Windows Server 2012 R2 Sitzungen der Anwendern spiegeln, um zum Beispiel bei Problemen zu helfen. Windows Server 2012 hat nicht mehr über diese Technik verfügt. In Windows Server 2012 R2 hat Microsoft diese Funktion wieder integriert. Über das Kontextmenü von Sitzungen im Server-Manager können Sie auf Remotedesktop-Sitzungshosts Sitzungen von Anwendern anzeigen. Die Funktion wurde jetzt ebenfalls in den Server-Manager integriert, auch hier sind keine Zusatzwerkzeuge mehr notwendig.

Damit die Verbindung funktioniert, muss der entsprechende Anwender zustimmen. Die Einstellungen lassen sich jetzt auch wieder über die Gruppenrichtlinien steuern. Sie finden die Konfiguration über *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Remotedesktopdienste/Remotedesktop-Sitzungshost/Verbindungen*.

In Windows Server 2012 R2 ist es wieder möglich, auf einem Domänencontroller den Verbindungsbroker zu installieren. Dies war in Windows Server 2012 nicht mehr möglich. Vor allem kleinere Firmen profitieren von diesen Nachbesserungen.

RemoteFX hat Microsoft ebenfalls in Windows Server 2012 R2 verbessert. Die Geschwindigkeit steigt, die Anzeige wird besser. Auf diesem Weg lassen sich effizient Desktops für Anwender zur Verfügung stellen, ohne dass der Netzwerkverkehr zu stark leidet. Unternehmen, die RemoteFX einsetzen, profitieren deutlich von den Leistungssteigerungen in Windows Server 2012 R2. RemoteFX und die integrierte vCPU unterstützen jetzt auch DirectX 11.1. Die neuen Codecs belasten Netzwerke deutlich weniger. Grundsätzlich steigt die Netzwerkleistung der Remotedesktopdienste auch in anderen Bereichen an. Wird ein Client aufgrund von Netzwerkproblemen vom Server getrennt, verbindet der neue Verbindungsbroker in Windows Server 2012 R2 den Anwender wesentlich schneller mit seiner Sitzung als Windows Server 2012. In Windows Server 2012 R2 arbeitet RemoteFX auch mit NUMA zusammen. NUMA (Non-Uniform Memory Access) bietet in Mehrprozessorsystemen die Möglichkeit, dass die verschiedenen Prozessoren untereinander Daten austauschen können und sich gegenseitig bei Berechnungen unterstützen.

Wenn Sie eine Virtual Desktop Infrastructure auf Basis von Windows Server 2012 R2 und Windows 8 oder Windows 8.1 aufbauen, können Sie die VHD(X)-Dateien der Clients auch auf Dateifreigaben von Servern mit Windows Server 2012 R2 speichern. Die neue Serverversion verwendet weitere Ver-

besserungen des Server Message Blocks (SMB), damit auf diese Daten schneller zugegriffen werden kann. Außerdem erkennt die verbesserte Datendeduplizierung in Windows Server 2012 R2 doppelt gespeicherte Dateien in den virtuellen Servern und kann so deutlich Speicherplatz einsparen.

Ebenfalls neu in den Remotedesktopdiensten von Windows Server 2012 R2 ist der Restricted-Admin-Modus im Remotedesktopclient. Arbeiten Sie mit Windows 8/8.1 und Windows Server 2012 R2, können Sie sich mit diesem Modus mit einem Remotedesktop-Sitzungshost verbinden. Bei dieser Verbindung werden die Anmeldedaten nicht zum Server durch den Remotedesktopclient geschickt. Der Client verbindet sich dazu mit einem Server, der diese Funktion unterstützt. Dazu prüft der Server, ob der Anwender über Administratorrechte verfügt. Ist dies der Fall, lässt er die Verbindung zu. Über diesen Modus werden also keinerlei Authentifizierungsdaten über das Netzwerk geschickt. Die Funktion lässt sich ausschließlich nur mit Windows 8/8.1 und Windows Server 2012 R2 nutzen.

Natürlich gibt es auch in der neuen Serverversion die bekannten Funktionen aus Windows Server 2012. Die Installation erfolgt über den neuen Server-Manager. Auch in Windows Server 2012 R2 handelt es sich bei den Remotedesktopdiensten um eine Serverrolle, die verschiedene Rollendienste umfasst:

- **Remotedesktop-Virtualisierungshost** Der Dienst wird in Hyper-V integriert, um in einem Pool virtuelle Desktops mit RemoteApp- und Desktopverbindung bereitzustellen. Ähnliche Funktionen gibt es auch in Windows Server 2008 R2.
- **Remotedesktop-Sitzungshost** RemoteApp-Programme oder sitzungsbasierte Desktops nutzen diesen Dienst. Hierbei handelt es sich um den Nachfolger von den Terminaldiensten.
- **Remotedesktop-Verbindungsbroker** Benutzer können erneut eine Verbindung mit ihren vorhandenen virtuellen Desktops, RemoteApp-Programmen und sitzungsbasierten Desktops herstellen. Die Verbindungsdaten merkt sich der Broker.

Web Access für Remotedesktop ermöglicht Benutzern den Zugriff auf RemoteApp- und Desktopverbindung über einen Webbrowser. Auf diesem Weg stellen Sie zum Beispiel Remotedesktops im Internet zur Verfügung.

Die Remotedesktoplizenzierung verwaltet die Lizenzen, die für eine Verbindung mit einem Remotedesktop-Sitzungshostserver oder einem virtuellen Desktop erforderlich sind. Sie können die RD-Lizenzierung zum Installieren, Ausstellen und Nachverfolgen der Verfügbarkeit von Lizenzen verwenden.

Der Remotedesktopgateway ermöglicht es autorisierten Benutzern, von jedem Gerät mit Internetzugang eine Verbindung mit virtuellen Desktops, RemoteApp-Programmen und sitzungsbasierten Desktops in einem internen Unternehmensnetzwerk herzustellen.

Die Installation der Dienste hat Microsoft wesentlich vereinfacht. Die Konfiguration erfolgt komplett im Server-Manager. Es gibt nicht mehr zahlreiche Tools, alles was Sie brauchen, ist der Server-Manager. Dieser kann alle installierten Remotedesktopserver und alle Rollen zentral verwalten. Der Remotedesktop Connection Broker stellt diese Verbindung her. Sie können im neuen Server-Manager zentral alle Server mit allen notwendigen Rollen installieren. Windows Server 2012 R2 bietet Sammlungen für Sitzungshosts (ehemals Terminalserver) und in Virtual Desktop Infrastructure-Umgebungen (VDI) auch für Virtualization-Hosts. In Windows Server 2012 R2 können Sie mit den Remotedesktopdiensten auch virtuelle Desktops auf Basis von Windows 8/8.1 zur Verfügung stellen. Auch diese profitieren von den Neuerungen in Windows Server 2012 R2.

Generell ist in Windows Server 2012 R2 die Erstellung virtueller Desktops wesentlich leichter zu automatisieren und zu administrieren. Sie können Vorlagen für virtuelle Desktops erstellen und personifizierte sowie öffentliche Desktops erstellen. In den einzelnen Abschnitten dieses Kapitels gehen wir ausführlicher auf die Neuerungen ein.

Abbildg. 28.1 Einrichten der Remotedesktopdienste

Microsoft hat die Verwaltung der Remotedesktopdienste in Windows Server 2012 vereinfacht. Auch in Windows Server 2012 R2 verhält sich der entsprechende Assistent ähnlich. Im Server-Manager hat Microsoft dazu neue Assistenten integriert, um die Rollen von Remotedesktopservern bereitzustellen. Auch die Verwaltungskonsole zum Erstellen einer Virtual Desktop Infrastructure (VDI) hat Microsoft deutlich vereinfacht.

Eine Sitzungssammlung, früher Farm genannt, ist eine Gruppierung von RD-Sitzungshostservern für eine bestimmte Sitzung. Eine Sitzungssammlung wird verwendet, um sitzungsbasierte Desktops oder RemoteApp-Programme zur Verfügung zu stellen. Die Sitzungsvirtualisierung erfolgt über den Server-Manager. Dieser ermöglicht, RD-Sitzungshostserver von einem zentralen Ort aus zu installieren und zu konfigurieren. Während der Installation haben Sie zwei Möglichkeiten:

- **Schnellstart** Alle notwendigen Remotedesktopdienste-Rollendienste werden auf einem einzigen Server installiert. Das ist zum Beispiel für Testumgebungen oder in kleineren Unternehmen sinnvoll.
- **Standardbereitstellung** Ermöglicht Ihnen die flexible Bereitstellung der unterschiedlichen Remotedesktopdienste-Rollendienste auf unterschiedlichen Servern für den Produktionsbetrieb

Haben Sie die Auswahl getroffen, können Sie im Assistenten auswählen, ob Sie virtuelle Desktops zur Verfügung stellen wollen, oder Remotedesktopsitzungen, also einen Terminalserver mit Anwendungen. Im Assistenten wählen Sie auf den folgenden Seiten die verschiedenen Server im Pool aus,

denen Sie die unterschiedlichen Rollendienste zuweisen. Haben Sie im Szenario alle Server ausgewählt, die an der Infrastruktur teilnehmen sollen, schließen Sie die Installation über den Server-Manager ab.

Installieren Sie zum Beispiel einen Remotedesktop-Sitzungshost, um Anwendungen und Desktops zentral zur Verfügung zu stellen, müssen Sie nach der Installation der Rollendienste im Server-Manager eine Sitzungssammlung erstellen, also eine Terminalserverfarm.

Installation eines Remotedesktopservers

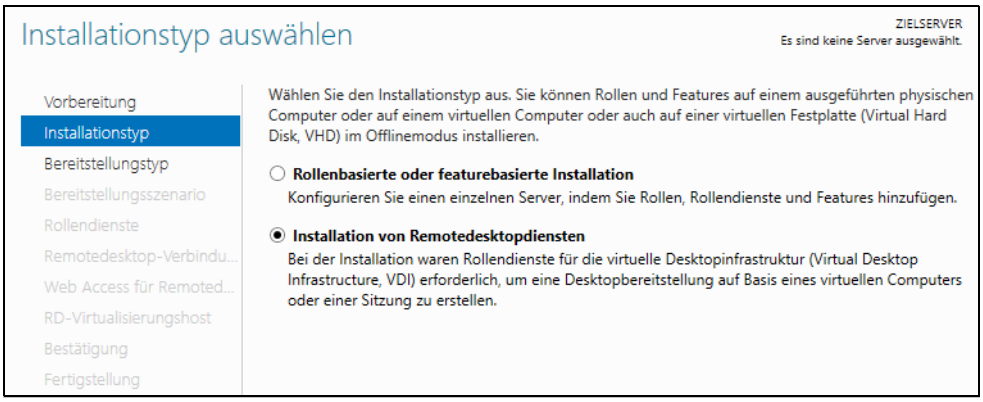
In den nächsten Abschnitten gehen wir darauf ein, wie Sie Remotedesktopserver in Windows Server 2012 R2 installieren und die Serverdienste im Netzwerk verteilen.

Installation und Verteilen der notwendigen Rollendienste

Die Installation eines Remotedesktopservers findet über den Server-Manager statt, indem Sie *Verwalten/Rollen und -Features hinzufügen* auswählen. Im Gegensatz zu herkömmlichen Rollen installieren Sie die Remotedesktopdienste über einen eigenen Assistenten, den Sie direkt vor der Installation eigentlicher Rollen starten.

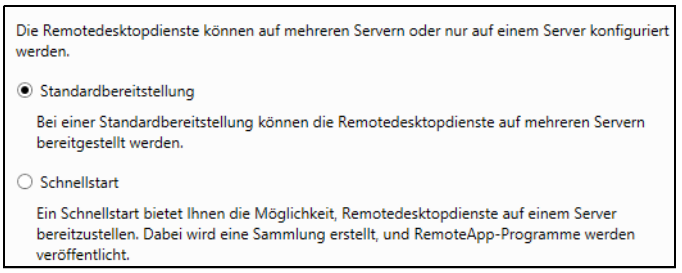
Um die Serverrollen auf mehrere Server zu verwalten, müssen Sie diese zuvor über *Verwalten/Server hinzufügen* dem lokalen Server-Manager hinzufügen (siehe Kapitel 3).

Abbildg. 28.2 Installieren der Remotedesktopdienste



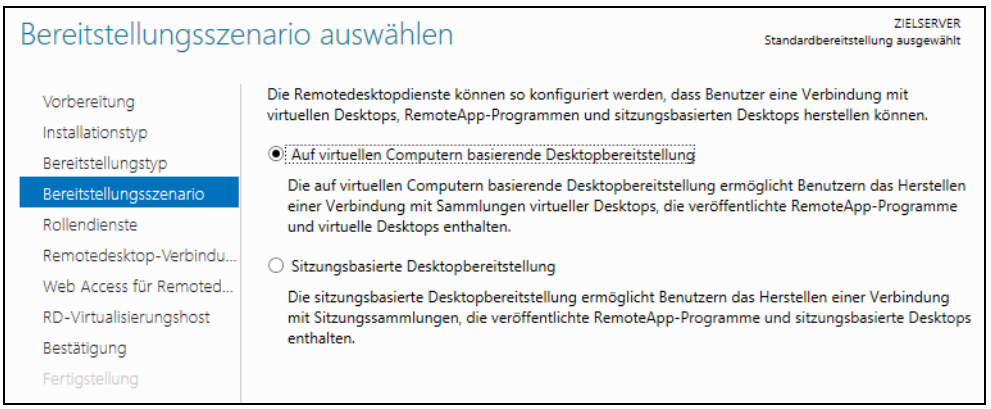
Auf der zweiten Seite wählen Sie aus, ob Sie eine Standardbereitstellung durchführen wollen oder eine Schnellstartinstallation mit nur einem einzelnen Server installieren wollen. Mit der Standardinstallation können Sie eine Serverfarm mit mehreren Remotedesktop-Sitzungshosts installieren.

Abbildg. 28.3 Auswählen der Bereitstellung für die Installation der Remotedesktopdienste



Über den Assistenten legen Sie auch fest, ob Sie eine Virtual Desktop Infrastructure (VDI) installieren wollen, also virtuelle Computer auf Basis von Hyper-V, die Anwendern zur Verfügung gestellt werden, oder eine sitzungsbasierte Bereitstellung, also Server, die Anwendungen oder den Desktop den Anwendern zur Verfügung stellen.

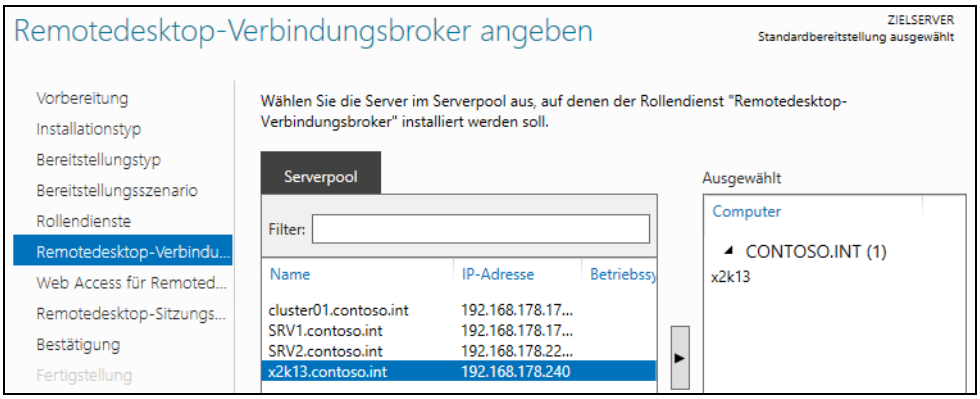
Abbildg. 28.4 Auswählen des Bereitstellungsszenarios



Haben Sie das Szenario ausgewählt, bestätigen Sie die zu installierenden Rollendiensten, die zum Szenario installiert werden müssen. Auf einem Server in der Farm müssen Sie den Remotedesktop-Verbindungsbroker installieren. Dieser war in Windows Server 2008 R2 optional, ist in Windows Server 2012 R2 aber zwingend notwendig.

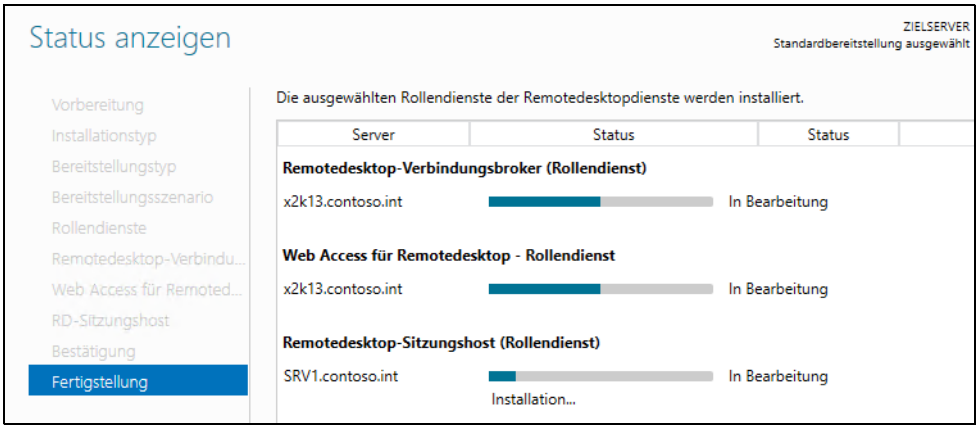
Mit diesem Dienst können Sie Anwender mit ihrer ursprünglichen Sitzung wiederverbinden, wenn Sie mehrere Remotedesktopserver in einem Loadbalancing-Verbund einsetzen. Der Verbindungsbroker stellt einen Aggregationspunkt für RemoteApps im Unternehmen zur Verfügung und verbindet alle installierten Server, damit Sie diese zentral im Server-Manager verwalten können. Er sammelt RemoteApps der verschiedenen Server ein und stellt diese bei Windows 7 im Startmenü, in Windows 8.1 auf der Startseite und für andere Betriebssysteme auch per Webzugriff zur Verfügung. Webzugriffsserver holen sich dazu die Daten von einem Server mit dem Verbindungsbroker.

Abbildg. 28.5 Installieren des Remotedesktop-Verbindungsbroker



Als Nächstes wählen Sie einen Server mit Web Access aus, der die RemoteApps der Farm zentral zur Verfügung stellt. Als Letztes wählen Sie noch den eigentlichen Server aus, der den Remotedesktop-Sitzungshost bereitstellt. Klicken Sie im letzten Fenster auf *Bereitstellen*, damit der Assistent auf den ausgewählten Servern die entsprechende Funktion installiert.

Abbildg. 28.6 Der Server-Manager in Windows Server 2012 R2 installiert auf allen beteiligten Servern die notwendigen Dienste



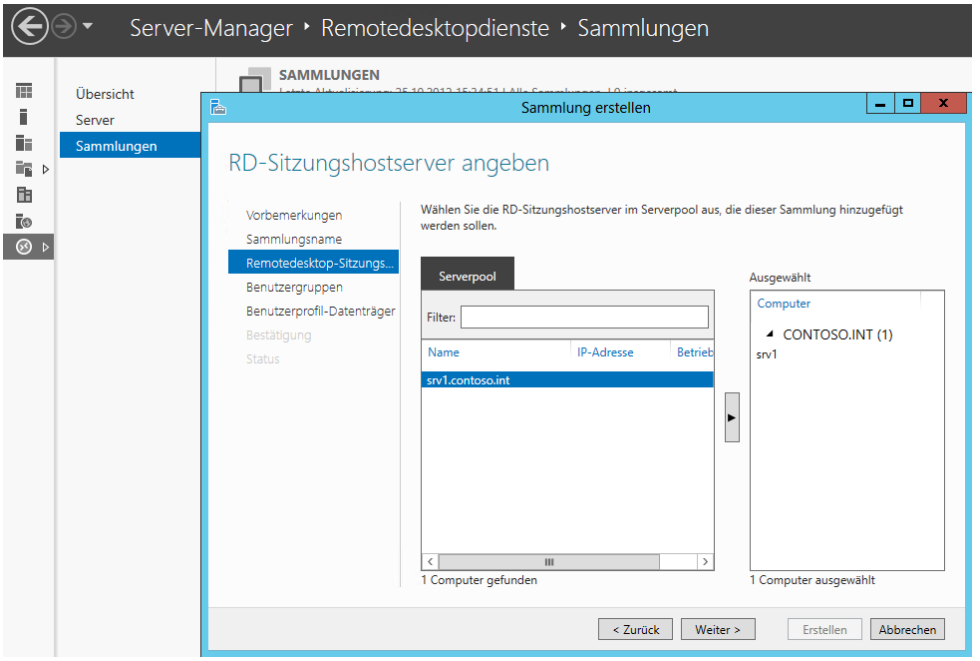
Einrichten einer neuen Serverfarm

Installieren Sie zum Beispiel einen Remotedesktop-Sitzungshosts, um Anwendungen und Desktops zentral zur Verfügung zu stellen, müssen Sie nach der Installation der Rollendienste im Server-Manager eine Sitzungssammlung erstellen, also eine Terminalserverfarm. Dazu steht die neue Gruppe *Remotedesktopdienste* zur Verfügung, über die Sie die Infrastruktur installieren:

1. Klicken Sie in der linken Seite des Fensters auf *Remotedesktopdienste*.
2. Klicken Sie auf *Sammlungen*.
3. Klicken Sie auf *Aufgaben/Sitzungssammlung erstellen*. Es startet der Assistent zum Erstellen einer Sitzungssammlung (Farm).

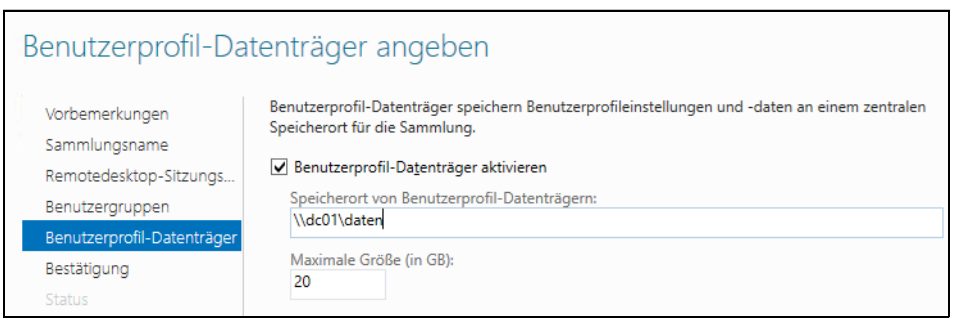
4. Geben Sie im Assistenten zunächst einen Namen für die Sammlung ein.
5. Wählen Sie auf der nächsten Seite die Server aus, die der Sitzungssammlung (Farm) beitreten sollen.
6. Legen Sie danach fest, welche Gruppe aus Active Directory Zugriff auf den Server erhalten soll. Hier bietet es sich an, wie in den Vorgängerversionen, eigene Gruppen anzulegen. Auf diese Weise können Sie über die Gruppenmitgliedschaft den Zugriff steuern.
7. Übernehmen Sie auf der Seite *Benutzergruppen angeben* die Standardauswahl und klicken Sie auf *Weiter*.

Abbildg. 28.7 Erstellen einer neuen Sitzungssammlung (ehemals Serverfarm)



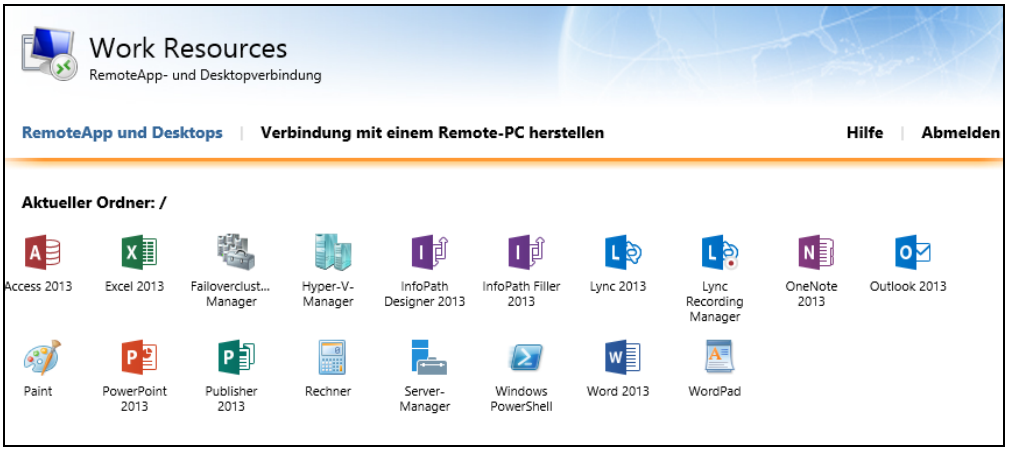
In Windows Server 2012 R2 können Sie über den Assistenten auch einen Benutzerprofildatenträger eingeben. Dazu verwenden Sie eine Freigabe. Hierbei handelt es sich um den Nachfolger der Terminaldiensteprofile. Schließen Sie die Erstellung der Gruppe ab. Anschließend steht die Farm zur Verfügung.

Abbildg. 28.8 Auswählen des Benutzerprofil-Datenträgers



Haben Sie die Sammlung erstellt und auch den Webzugriff über den Installations-Assistenten installiert, können Sie bereits mit der URL *https://<Servername>/rdweb* auf die Webfreigabe zugreifen. Per Webzugriff haben Sie auch die Möglichkeit, eine Verbindung mit anderen Servern oder mit PCs herzustellen, auf denen der Remotedesktop aktiviert ist.

Abbildg. 28.9 Web Access für Remotedesktopdienste steht nach der Installation bereits über SSL zur Verfügung



RemoteApp – Anwendungen virtualisieren

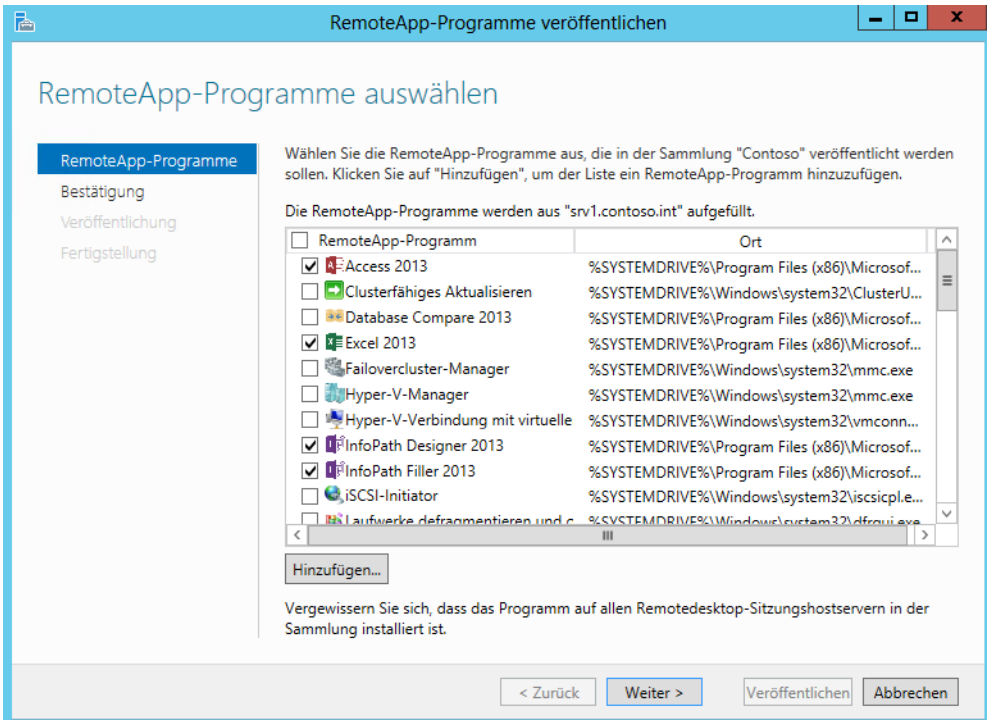
Wollen Sie nicht nur den Desktop zur Verfügung stellen, sondern auch einzelne Programme, die Anwender direkt über die Weboberfläche starten, klicken Sie im Server-Manager auf *Remotedesktopdienste* und dann auf die *Sammlung*. Hier sehen Informationen zur aktuellen Sammlung und können die verschiedenen Bereiche bearbeiten. Dazu klicken Sie jeweils in dem Bereich, den Sie verwalten wollen, auf *Aufgaben* und wählen dann aus, welche Konfiguration Sie anpassen möchten.

Um eine Anwendung der Liste hinzuzufügen, klicken Sie im Bereich *RemoteApp-Programme* auf den Link *RemoteApp-Programme veröffentlichen*. Im Anschluss startet der RemoteApp-Assistent, über den Sie die Anwendungen der Liste hinzufügen können. Wählen Sie entweder das Programm aus der Liste aus oder klicken Sie auf *Durchsuchen*, um die Startdatei der Anwendung hinzuzufügen. Sie können an dieser Stelle mehrere Anwendungen auswählen. Sie können die Eigenschaften der Applikationen jederzeit anpassen.

RemoteApps stehen nach der Veröffentlichung automatisch für alle Clients über den Webzugriff zur Verfügung. Diesen erreichen Sie über die URL *https://<Servername>/rdweb*. Nach der Authentifizierung stehen sofort alle RemoteApps zur Verfügung, die Sie veröffentlichen, Berechtigungen vorausgesetzt.

Sie können im Server-Manager über diesen Bereich jederzeit weitere Anwendungen veröffentlichen. Achten Sie aber darauf, dass die Anwendungen auf den Remotedesktop-Sitzungshosts installiert sein müssen, nicht auf dem Server mit Web Access oder dem Remotedesktop-Verbindungsbroker.

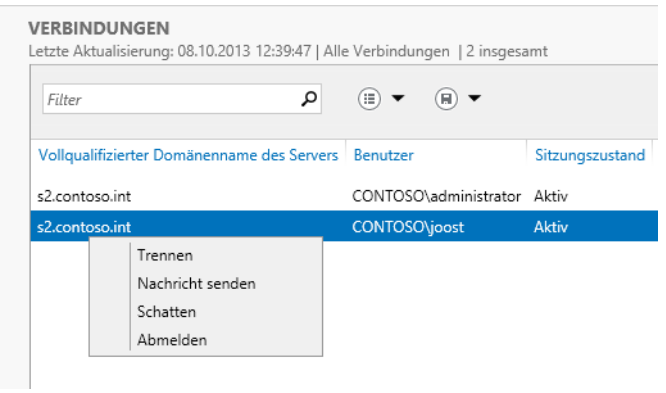
Abbildg. 28.10 Veröffentlichen von Anwendungen im Server-Manager



Um weitere Anwendungen hinzuzufügen, klicken Sie im Server-Manager in der Verwaltung der Remotedesktopdienste auf die entsprechende Sammlung. Im Bereich *Aufgaben* der App-Verwaltung können Sie veröffentlichte Anwendungen auch wieder entfernen.

Im Server-Manager sehen Sie die aktuell verbundenen Benutzer im Bereich *Verbindungen*, wenn Sie auf die Sammlung klicken. An dieser Stelle können Sie einzelne Verbindungen auch trennen.

Abbildg. 28.11 Verwalten der verbundenen Benutzer



TIPP Neu in Windows Server 2012 R2 ist die Option *Schatten* im Kontextmenü von Benutzersitzungen. Hierüber können Sie, wie in Vorgängerversionen von Windows Server 2012, eine Verbindung zur Sitzung des Anwenders (auch spiegeln genannt) aufbauen. Dieser muss dazu die Verbindung bestätigen.

Remotedesktoplizenzierung

Sie benötigen für jeden Remotedesktopserver (Remotedesktop-Sitzungshost) eine Windows Server-Lizenz. Zusätzlich benötigen Sie für jeden Benutzer, wie bei normalen Serverzugriffen auf Datei- oder Druckserver, eine entsprechende Client-Zugriffslizenz. Diese CALs sind bei keinem Betriebssystem integriert, sondern müssen immer gesondert erworben werden.

HINWEIS In Windows Server 2012 R2 können Sie auch Benutzer-CALs und RDS-CALs von Windows Server 2012 verwenden. Sie müssen also keine CALs neu erwerben, wenn Sie bereits Windows Server 2012 einsetzen.

Setzen Sie Citrix XenApp, Citrix XenDesktop, Ericom PowerTerm WebConnect, Quest Virtual Access Suite, GraphOn Go-Global oder andere Lösungen für den Remotedesktop ein, müssen Sie trotzdem RDS-CALs erwerben.

Setzen Sie neue RDS-CALs ein, können Sie diese auch mit Vorgängerversionen von Windows Server 2012 R2 betreiben. Welche Versionen miteinander erlaubt sind, sehen Sie auf der Seite *http://social.technet.microsoft.com/wiki/contents/articles/14988.rds-and-ts-cal-interoperability-matrix.aspx* [Ms179-K28-02].

Bei einem Remotedesktopserver benötigen Sie zusätzlich für jeden Client, der sich mit dem Remotedesktopserver verbindet, eine spezielle Remotedesktopserver-Zugriffslizenz (RDS-CAL). Diese Lizenz wird pro PC oder pro Benutzer vergeben und gilt nicht pro gleichzeitigem Zugriff (siehe auch Kapitel 1). Das heißt, Sie müssen nicht so viele Lizenzen kaufen, wie gleichzeitig Benutzer mit dem Remotedesktopserver arbeiten, sondern so viele Lizenzen, wie Benutzer überhaupt mit dem Remotedesktopserver arbeiten.

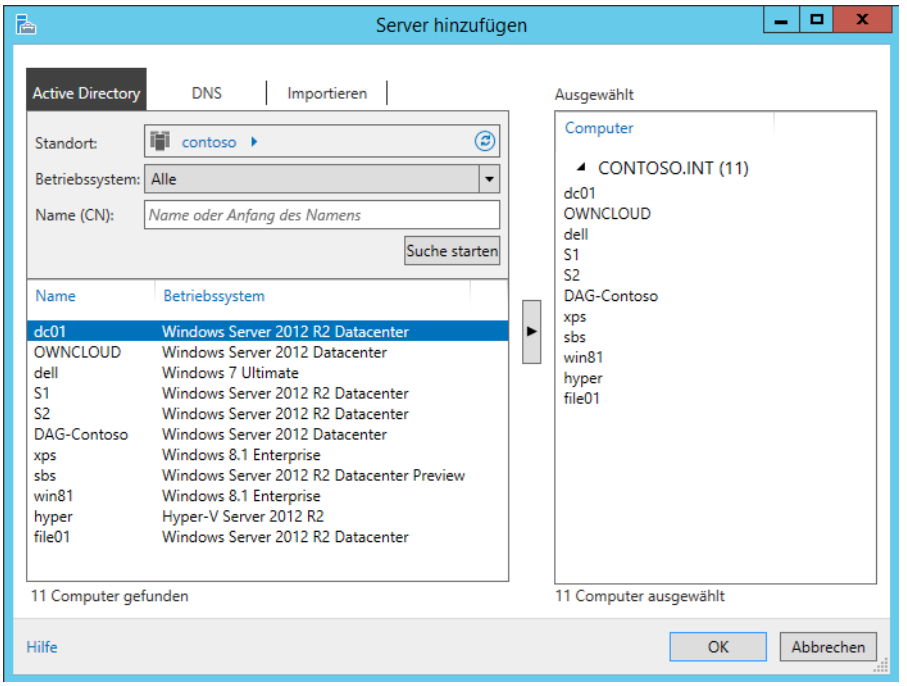
Microsoft bietet für die Lizenzierung der RD-CALs die gleichen Lizenzierungsmöglichkeiten wie bei den normalen CALs (siehe Kapitel 1). Es gibt RD-Geräte-CALs und RD-Benutzer-CALs. Befindet sich der Remotedesktopserver in Active Directory, sollten Sie die Remotedesktopdienste-Lizenzierung auf einem Domänencontroller installieren. Haben Sie in Ihrer Umgebung nur einen Remotedesktopserver, können Sie auch auf diesem die Remotedesktopdienste-Lizenzierung installieren. Sie haben 120 Tage Zeit, bevor Sie den Lizenzierungsdienst auf einem Server installieren und aktivieren müssen. Ein Remotedesktopserver findet in Active Directory Lizenzserver automatisch. Der Ablauf bei der Lizenzierung ist folgender:

1. Ein Client verbindet sich mit einem Remotedesktopserver (Remotedesktop-Sitzungshost).
2. Der Remotedesktopserver ruft von einem Remotedesktoplizenzserver eine Lizenz ab. Hierbei muss es sich nicht um den lokalen Remotedesktopserver handeln. Ein Lizenzserver kann Lizenzen für mehrere Remotedesktopserver zur Verfügung stellen. Für die Verbindung mit einem Administratorkonto benötigen Sie auch auf einem Remotedesktopserver keine Lizenz, es dürfen aber nur zwei gleichzeitige Admins verbunden sein.
3. Der Remotedesktopserver stellt dem Client die Lizenz zur Verfügung.

Lizenzserver in den Remotedesktopdiensten registrieren sich automatisch in Active Directory. Installieren Sie einen neuen Remotedesktopserver, können Sie manuell Lizenzserver zuweisen. So ist sichergestellt, dass einzelne Remotedesktopserver genau mit den Lizenzservern arbeiten, die Sie als Administrator hinterlegen.

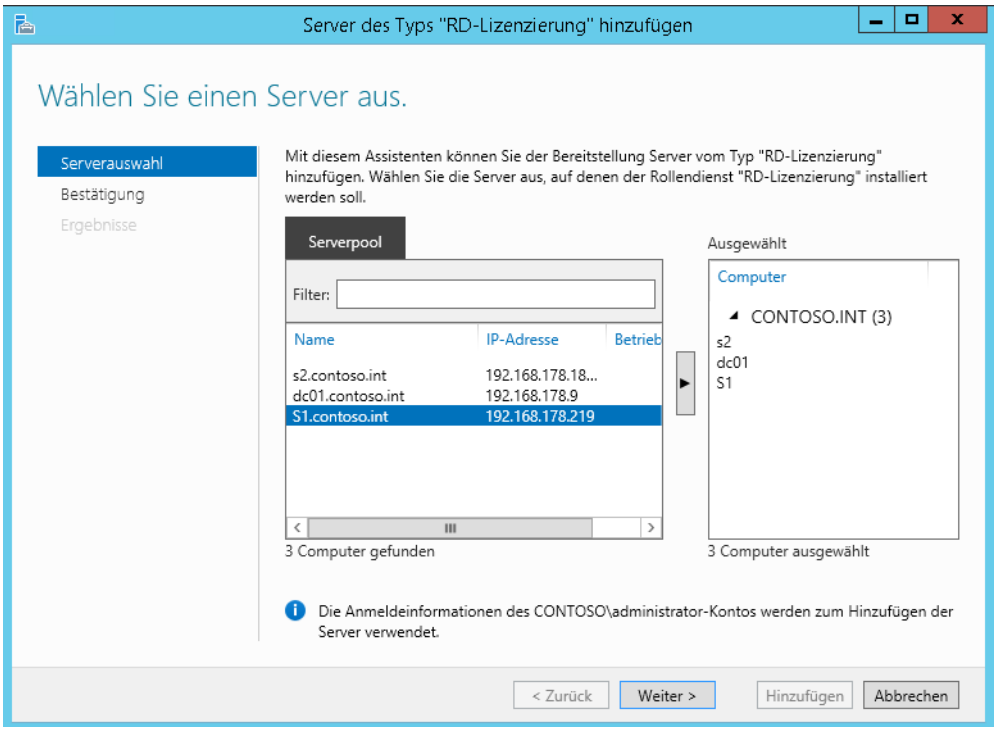
Um die Remotedesktopdienste-Lizenzierung zu installieren, wählen Sie im Server-Manager den Link *Die Remotedesktopdienste* aus und klicken auf *Übersicht*. Über den Link *Remotedesktoplizenzierung* wählen Sie den Server aus, der die Lizenzierung steuert. Sie können an dieser Stelle allerdings nur Server auswählen, die Sie im Server-Manager über *Verwalten/Server hinzufügen* integriert haben.

Abbildg. 28.12 Anbinden von Servern zur Steuerung im Server-Manager



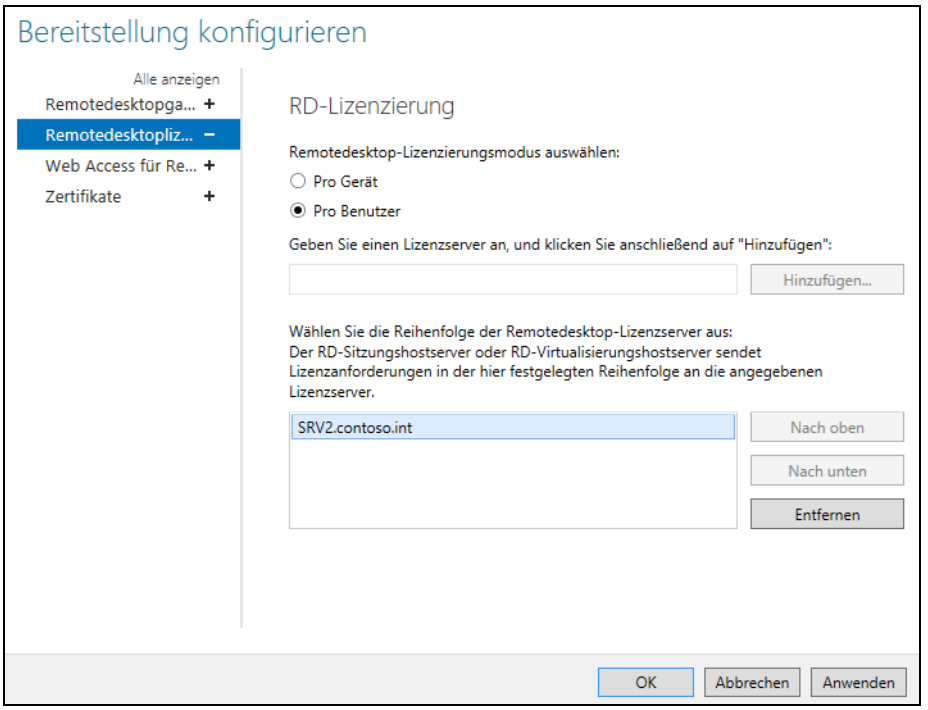
Haben Sie die Server im Server-Manager integriert, können Sie schließlich über den Link *Remotedesktoplizenzierung* einen oder mehrere Server auswählen, auf denen Sie diesen Dienst betreiben wollen. Schließen Sie den Assistenten ab, um die Lizenzierung zu aktivieren.

Abbildg. 28.13 Auswählen der Remotedesktoplizenzserver im Unternehmen



Nachdem Sie die Remotedesktoplizenzierung installiert haben, müssen Sie noch Einstellungen für die Sammlung konfigurieren. Dazu klicken Sie im Server-Manager bei *Remotedesktopdienste/Übersicht bei Bereitstellungsübersicht* auf Aufgaben und dann auf *Bereitstellungseigenschaften bearbeiten*. Klicken Sie danach auf *Remotedesktoplizenzierung*. Hier legen Sie fest, welche Lizenzierung Sie verwenden wollen und welchen Lizenzserver die Sammlung verwenden soll. Klicken Sie danach auf *Anwenden*.

Abbildg. 28.14 Festlegen der Remotedesktoplizenzierung

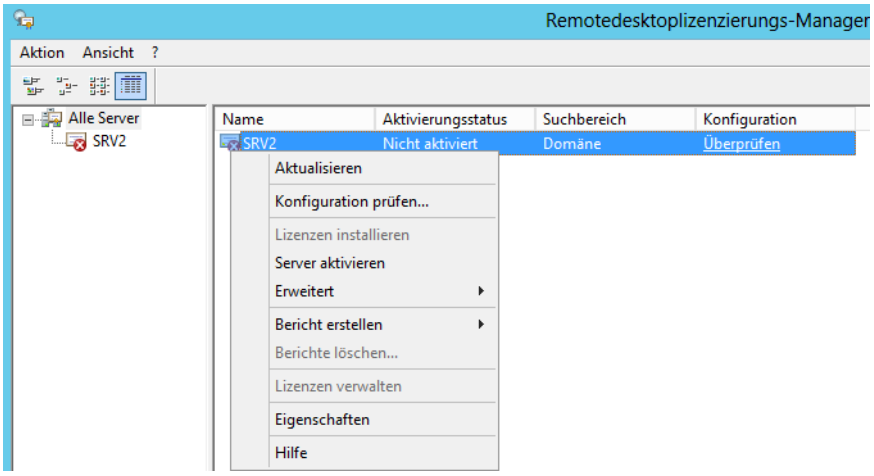


Auf dem Server, den Sie als Remotedesktoplizenzierungs-Server installiert haben, finden Sie nach der Installation auf der Startseite das neue Tool *Remotedesktoplizenzierungs-Manager* vor. Dieses starten Sie auch durch Eingabe von *licmgr*.

Haben Sie das Programm gestartet, durchsucht das Programm das Netzwerk und zeigt die gefundenen Lizenzserver an. Nicht aktivierte Lizenzserver werden entsprechend hervorgehoben. 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.

Abbildg. 28.15 Verwalten der Remotedesktoplizenzierungs-Server



Die Aktivierung können Sie auch über einen Webbrowser durchführen. Dazu verwenden Sie die URL *https://activate.microsoft.com* [Ms179-K28-03] und geben die Produkt-ID ein, die Sie vom Lizenzierungs-Manager erhalten. Danach erhalten Sie eine Lizenzserver-ID, die Sie im Assistenten des Remotedesktoplizenzierungs-Manager eintragen.

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 nicht die RD-CALs, die Sie später benötigen. Die RD-Cals erhalten Sie als Seriennummer, die Sie über das Kontextmenü des Lizenzservers im Remotedesktoplizenzierungs-Manager eintragen. Für die Aktivierung eines Lizenzservers benötigen Sie noch keine RD-CALs. Die Aktivierung ist kostenlos und notwendig, damit der Server zumindest Testlizenzen ausstellen kann, die bis zu 120 Tage gültig sind.

Nach der erfolgreichen Aktivierung wird der Lizenzserver als fehlerfrei dargestellt, aber oft mit einer Warnung. Klicken Sie auf den Server mit der rechten Maustaste und wählen Sie *Konfiguration prüfen* aus. Sie erhalten die Information, dass der Server nicht Mitglied der Windows-Gruppe *Terminalserver-Lizenzserver* ist. Durch einen Klick auf die Schaltfläche neben der Meldung können Sie das Computerkonto in die Gruppe aufnehmen.

Die Aufnahme ist notwendig, damit der Server Benutzern in der Domäne Lizenzen für den Zugriff auf den Remotedesktopserver zuteilen kann. Neben der Aktivierung müssen Sie auch noch den Lizenzmodus festlegen, wie auf den vorangegangenen Seiten beschrieben.

Im Remotedesktoplizenzierungs-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 Remotedesktopserver und die Arbeitsstationen in einer Active Directory-Domäne befinden.

Abbildg. 28.16 Hinzufügen eines Lizenzservers

Weitere Optionen der Lizenzierung, wie den Suchmodus für den Lizenzserver oder den Lizenzierungsmodus, können Sie im Server-Manager einstellen. Dazu klicken Sie im Bereich *Bereitstellungsübersicht* auf *Aufgaben* und wählen *Bereitstellungseigenschaften bearbeiten*.

Klicken Sie auf *Lizenzierungsdiagnose*, können Sie sich Meldungen zur Lizenzierung anzeigen lassen. Dieses Programm finden Sie über die Startseite auf den Remotedesktop-Sitzungshosts. In diesem Tool können Sie auch Zertifikate hinterlegen und das Remotedesktopgateway anpassen. Dazu später mehr.

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 Ordner *\Windows\System32\lserver*.

Sie können die Arbeitsweise des Lizenzservers mit Gruppenrichtlinien steuern. Wenn Sie eine Gruppenrichtlinie aufrufen, finden Sie die Richtlinien für die Remotedesktopserver-Lizenzierung in der Konsolenstruktur unter *Computerkonfiguration/(Richtlinien)/Administrative Vorlagen/Windows-Komponenten/Remotedesktopdienste/Remotedesktoplizenzierung*.

Nacharbeiten zur Installation

Haben Sie auf einem Server die Remotedesktopdienste installiert, sollten Sie einige empfohlene Nacharbeiten durchführen, die wir im folgenden Abschnitt ausführlicher besprechen.

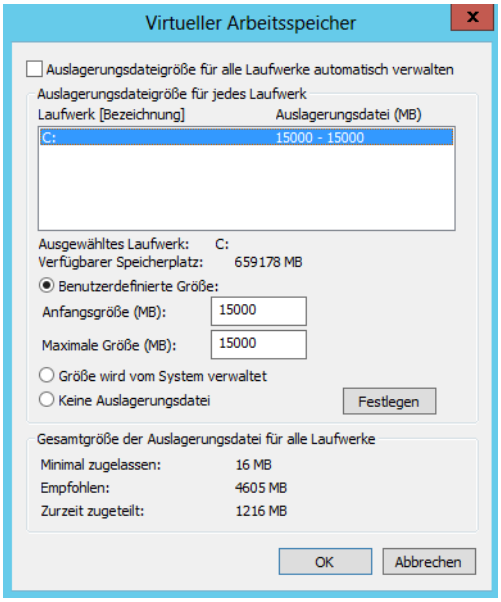
Auslagerungsdatei auf einem Remotedesktop-Sitzungshost optimieren

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 *Systemsteuerung/System und Sicherheit/System/Erweiterte Systemeinstellungen/Leistung/Einstellungen/Erweitert/Virtueller Arbeitsspeicher/Ändern*.
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. 28.17 Konfiguration der Auslagerungsdatei auf einem Remotedesktopserver

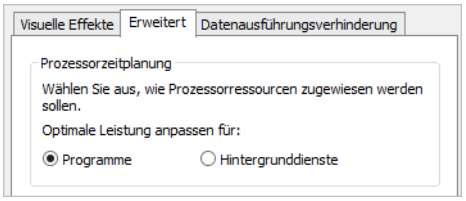


Prozessorzeitplanung anpassen

Standardmäßig ist Windows Server 2012 R2 darauf optimiert, Hintergrunddienste zu beschleunigen. Wenn Sie auf einem Server die Remotedesktopdienste 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.

Abbildg. 28.18 Optimieren der Prozessorzeitplanung für Remotedesktopserver



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.

Loopbackverarbeitung von Gruppenrichtlinien berücksichtigen

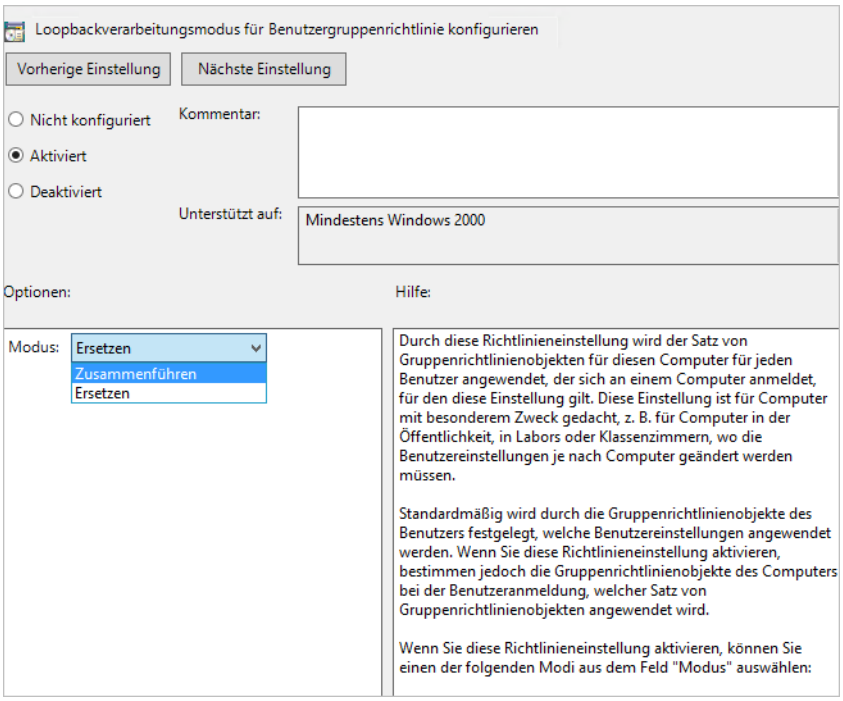
Setzen Sie Remotedesktop-Sitzungshosts zusammen mit Gruppenrichtlinien ein, bietet es sich an, die Server in einer eigenen OU abzulegen und für diese OUs dann Gruppenrichtlinien mit den gewünschten Einstellungen zu aktivieren.

Für diese Richtlinien sollten Sie auch den Loopbackverarbeitungsmodus aktivieren. Bei diesem Modus wendet die Gruppenrichtlinie auch Einstellungen des Benutzerbaums an, wenn das Konto der Anwender nicht in der OU gespeichert ist, in der die Richtlinie definiert ist, sondern nur der entsprechende Server. So erhalten Sie die Möglichkeit, Benutzereinstellungen für Remotedesktopserver festzulegen, die nur bei der Anmeldung der Anwender auf den Remotedesktopservern angewendet werden, nicht bei der Anmeldung an ihren lokalen Computern.

Sie finden diese Einstellung über *Computer/Richtlinien/Administrative Vorlagen/System/Gruppenrichtlinie*. Aktivieren Sie die Richtlinie *Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie*. Aktivieren Sie die Richtlinie, können Sie zwischen zwei Modi auswählen:

- **Ersetzen** Aktivieren Sie diesen Modus, ersetzt die Richtlinie Einstellungen, die bereits von anderen Richtlinien an gleicher Stelle gesetzt sind
- **Zusammenführen** Bei dieser Einstellung werden die normalen Richtlinien des Anwenders angewendet und die Einstellungen für den Benutzer in der Remotedesktopserver-Richtlinie. Gibt es Konflikte, gewinnt die Richtlinie der Remotedesktopserver.

Abbildg. 28.19 Aktivieren der Loopbackverarbeitung für Gruppenrichtlinien



Drucken mit Remotedesktop-Sitzungshosts

Verbinden sich Clients mit einem Remotedesktopsitzungshost, sind die installierten Drucker der Clients und die Drucker auf dem Server verfügbar. In den folgenden Abschnitten gehen wir auf einige Bereiche zur Einstellung des Druckerverhaltens in Windows Server 2012 R2 ein.

Remotedesktop Easy Print Driver

Der Remotedesktop Easy Print Driver kann Druckaufträge verschiedener Drucker an den Client umleiten. Auch in den Gruppenrichtlinien wurden viele Einstellungen für die Konfiguration von Druckern integriert. Damit Sie den Easy Print Driver verwenden können, müssen Sie den aktuellen RDP-Client verwenden.

Sie benötigen dazu Windows 7 oder Windows 8/8.1, mindestens jedoch Windows Vista SP1. Der Druckertreiber unterstützt eine Vielzahl neuerer und älterer Drucker, sodass auf einem Remotedesktopserver 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 Druckauftrags wird durch den Treiber verbessert.

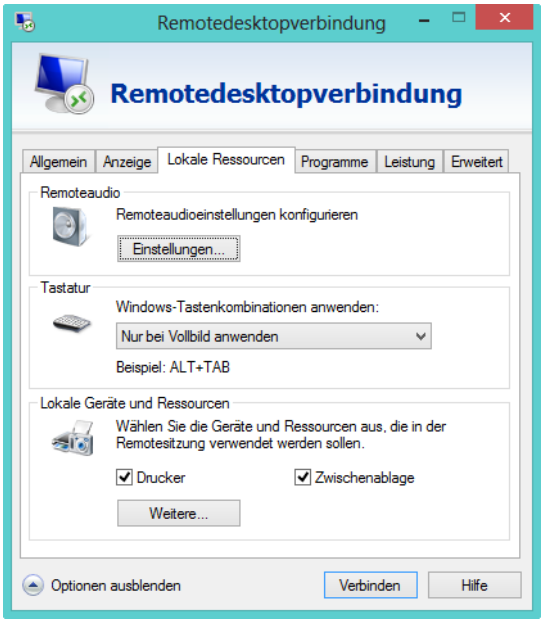
Unterstützen Clients diesen universalen Druckertreiber nicht, muss auf dem Remotedesktopserver weiterhin ein aktueller Treiber der Drucker installiert sein. Auf dem Server ist beim Einsatz des Easy Print Drivers ein Abbild des Druckertreibers des Clients angezeigt, aber nicht installiert. Druckt ein Anwender in der Sitzung, leitet der Treiber den Druck in eine XPS-Datei um und schickt diese zum Client, auf dem der Druck schließlich auf dem Drucker ausgegeben wird.

Damit der Easy Print Driver funktioniert, muss nichts auf dem Server installiert sein. Die auf dem Client verfügbaren Drucker übernimmt der Server, sofern diese kompatibel sind. Auch die spezifischen Einstellungen des Druckers zeigt der Server an und leitet diese beim Abrufen wieder auf den Client zurück. Ob Drucker umgeleitet werden, muss im RDP-Client eingestellt sein. Auf der Registerkarte *Lokale Ressourcen* auf dem Client muss dies zunächst aktiviert werden.

TIPP Unterstützen Ihre Unternehmensdrucker den neuen Easy Print Driver nicht, können Sie auch unter Windows Server 2012 R2 den Weg einer Druckermapping-Datei gehen. Diese Möglichkeit gibt es bereits seit Windows 2000 Server.

Dabei können 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* [Ms179-K28-04] oder *http://support.microsoft.com/kb/239088/de-de* [Ms179-K28-05] an.

Abbildg. 28.20 Aktivieren der Druckerumleitung in Windows 8.1

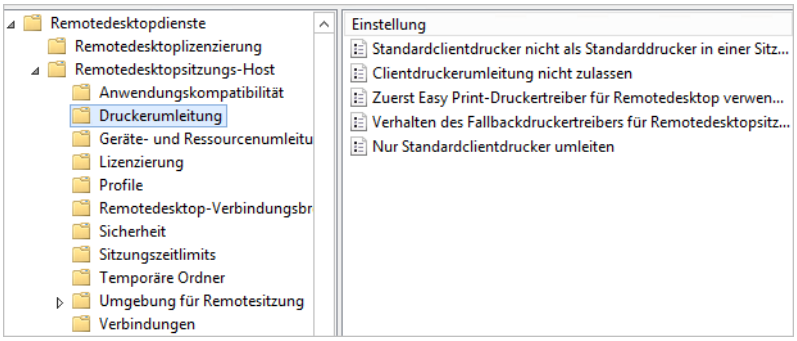


TIPP Am schnellsten starten Sie den Remotedesktopclient, wenn Sie auf der Startseite nach *mstsc* suchen.

Gruppenrichtlinien für die Steuerung von Druckern

In Windows Server 2012 R2 gibt es auch Möglichkeiten, die Anbindung von Druckern über Gruppenrichtlinien zu steuern. Die meisten Einstellungen für Gruppenrichtlinien werden im Gruppenrichtlinien-Editor unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Remotedesktopdienste* vorgenommen.

Abbildg. 28.21 Die Remotedesktopdienste in Windows Server 2012 R2 können jetzt effizient mit Gruppenrichtlinien gesteuert werden



Die Verwaltung von Druckern findet über den Untereintrag *Remotedesktopsitzungs-Host/Druckerumleitung* statt. Hier können auch Einstellungen des Easy Print Drivers angepasst werden.

HINWEIS Wird die Richtlinie *Zuerst Easy Print-Druckertreiber für Remotedesktop verwenden* aktiviert, versucht ein Remotedesktopserver zuerst diesen Treiber zu verwenden, bevor ein anderer Treiber installiert wird. Auch wenn diese Richtlinie nicht konfiguriert ist, verwendet der Remotedesktopserver standardmäßig zuerst den Easy Print Driver.

Unterstützt der Drucker diesen Treiber nicht, sucht der Remotedesktopserver als Nächstes lokal nach einem passenden Treiber. Findet der Server keinen Treiber, kann der Drucker in der Sitzung nicht verwendet werden. Standardmäßig ist diese Richtlinie nicht konfiguriert.

Deaktivieren Sie diese Einstellung, 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 Remotedesktopserver Software für die Benutzer installieren, sollten Sie darauf achten, dass die entsprechende Software auch mit der Installation auf einem Remotedesktopserver kompatibel ist. Die aktuellen Microsoft-Programme aus dem Office-Paket sind standardmäßig kompatibel mit der Installation auf einem Remotedesktopserver. Allerdings können OEM- oder MSDN-Versionen von Office 2007/2010/2013 nicht auf Remotedesktopservern installiert werden. Sie benötigen dazu entsprechende Lizenzen.

Achten Sie beim Einsatz von Unternehmenssoftware darauf, ob diese Terminalserver, Remotedesktop oder Remotedesktop-Sitzungshosts unterstützt. Ist das nicht der Fall, testen Sie die Anwendung zuvor in einer Testumgebung. Die meisten Programme sind kompatibel zum Remotedesktop, allerdings nicht alle.

Installieren Sie eine Applikation auf einem Remotedesktopserver, sollten Sie den Server zuvor in den Installationsmodus versetzen. Sie verwenden dazu den Befehl *change user* in der Eingabeaufforderung.

Mit *change user /install* wird der Remotedesktopserver in den Installationsmodus versetzt. Sie geben diesen Befehl ein und installieren danach die Software. Durch den Befehl erstellt Windows im Systemordner INI-Dateien für die Anwendung. Diese Dateien verwendet Windows als Masterkopien für benutzerspezifische INI-Dateien.

Wenn die Anwendung das erste Mal startet, durchsucht sie das Basisordner nach INI-Dateien. Wenn sich die INI-Dateien nicht im Basisordner, sondern im Systemordner befinden, werden sie von den Remotedesktopdiensten in den Basisordner kopiert. So wird gewährleistet, dass jeder Benutzer über eine eindeutige Kopie der INI-Dateien der Anwendung verfügt.

Neue INI-Dateien werden im Basisordner 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 der *Windows*-Ordner von der Anwendung durch Systemaufrufe abgefragt wird, gibt der Remotedesktopserver den Ordner *Systemroot* zurück
- Werden Einträge in der INI-Datei mithilfe von Systemaufrufen hinzugefügt, werden sie zu den INI-Dateien im Ordner *Systemroot* hinzugefügt

Geben Sie nach der Installation *change user /execute* ein, um den Ausführungsmodus zu aktivieren. Versucht die Anwendung eine nicht vorhandene INI-Datei zu lesen, wird diese INI-Datei von den Remotedesktopdiensten im Systemstamm gesucht.

Befindet sich die INI-Datei im Systemstamm, wird sie in den Unterordner *\Windows* des Basisordners des Benutzers kopiert. Fragt die Anwendung den Ordner *Windows* ab, gibt der Remotedesktopserver den Unterordner *\Windows* des Basisordners des Benutzers zurück. Melden sich Benutzer an, wird von den Remotedesktopdiensten 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 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 Remotedesktopservern zu vermeiden, sollte das Programm einmal ausgeführt werden, bevor der Installationsmodus auf einem Remotedesktopserver verlassen wird.

Mit *change user /execute* wird der Remotedesktopserver wieder in den Ausführungsmodus versetzt. Wenn Sie den Remotedesktopserver durchstarten, befindet er sich immer im ausführenden Modus, auch wenn der heruntergefahren wurde, weil Sie zuvor die Option */install* ausgeführt haben. Mit *change user /query* fragen Sie den aktuellen Status des Servers ab. Unabhängig davon, wie Sie eine Applikation auf dem Remotedesktopserver installieren, sollten Sie nach der Installation in einer Remotedesktop-Serversitzung überprüfen, ob die Applikation auf dem Remotedesktopserver funktioniert.

Um einen zuverlässigen Test durchzuführen, sollten Sie die Applikation möglichst in zwei gleichzeitig laufenden Sitzungen starten, da erst in diesem Fall die Remotedesktopserver-Kompatibilität 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 Remotedesktopservern bereits gesetzt.

Abbildg. 28.22 Verwenden von Change user auf Remotedesktop-Sitzungshosts

```
C:\Users\TEMP.CONTOSO>change user /install
Benutzersitzung ist bereit für die Installation von Anwendungen.

C:\Users\TEMP.CONTOSO>change user /execute
Benutzersitzung ist für die Ausführung von Anwendungen bereit.

C:\Users\TEMP.CONTOSO>change user /query
AUSFÜHRUNGSMODUS für Anwendungen ist aktiviert.

C:\Users\TEMP.CONTOSO>change user
ändert den Installationsmodus.

CHANGE USER {/EXECUTE | /INSTALL | /QUERY}

  /EXECUTE  Aktiviert Ausführungsmodus (Standardeinstellung).
  /INSTALL  Aktiviert Installationsmodus.
  /QUERY    Zeigt aktuelle Einstellungen an.
```


Remotedesktopclient

Remotedesktopserver unter Windows Server 2012 R2 können in den Terminalsitzungen deutlich mehr Geräte des angeschlossenen Clients verwenden. So sind in Terminalsitzungen jetzt auch Digitalkameras und Media Player unterstützt, die an den Remotedesktopclient angeschlossen sind. Auch Plug & Play für diese Geräte wird unterstützt.

Wollen Sie die Weiterleitung von an den Client angeschlossenen Plug & Play-Geräte in die Remotedesktop-Serversitzung erlauben, nehmen Sie im RDP-Client über *Optionen/Lokale Ressourcen/Weitere* die Einstellungen vor.

Die Remotedesktopdienste unterstützen zahlreiche Auflösungen, zum Beispiel 1.680 x 1.050 oder 1.900 x 1.200. Auch der Einsatz von Mehrmonitorlösungen wird unterstützt. Durch die Monitor-Spanning-Funktion können Remotedesktop-Serversitzungen über mehrere Monitore gestreckt werden. Neben den herkömmlichen Auflösungen im 4:3-Format unterstützt Windows Server 2012 R2 auch Auflösungen im 16:9- und 16:10-Format. Damit alle neuen Funktionen der Remotedesktopdienste in Windows Server 2012 R2 verwendet werden können, empfiehlt Microsoft den Einsatz des neuen Remotedesktopclients, der Bestandteil in Windows 7/8/8.1 und Windows Server 2008 R2/2012 ist.

Der neue Client kann Audiosignale bidirektional wiedergeben, das heißt, dass am Client auch ein Mikrofon angeschlossen sein kann und Audiosignale vom Server zum Client geleitet werden, als ob diese lokaler Bestandteil des Computers wäre.

TIPP Sie finden den Client für den Remotedesktop über *Remotedesktopverbindung* auf der Startseite von Windows 8.1. Schneller können Sie den Client aufrufen, wenn Sie das Befehlzeilentool Mstsc aufrufen:

- Über den Befehl *mstsc /w:<Auflösung> /h:<Auflösung>* geben Sie beim Starten des Clients die Auflösung an
- Geben Sie *mstsc /span* ein, kann die Remotedesktop-Serversitzung in einer Mehrmonitorumgebung genutzt werden. Über die Option *span:i:1* wird die Erweiterung in einer RDP-Datei hinterlegt.

Erweiterte Desktopdarstellung (Desktop Experience)

Installieren Sie auf einem Remotedesktopserver über den Server-Manager das Feature *Desktopdarstellung* über *Benutzeroberflächen und Infrastruktur*, erhalten die Anwender in einer Remotedesktop-Serversitzung die gleiche Oberfläche wie bei Windows 8.1. Bestandteil sind dann auch der Windows Media Player, Designs, die Fotoverwaltung und andere Funktionen.

Eine weitere Funktion ist die Schriftartglättung im RDP Client. Mit dieser Funktion werden ClearType-Schriftarten in einer Remotedesktop-Serversitzung besser dargestellt. Sie können die Funktion *Schriftartglättung* in den Option des RDP-Clients über die Registerkarte *Leistung* aktivieren. 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 weniger stark 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 Monitor deutlich verbessert werden. Sie können aber auch herkömmliche Monitore (CRT) verwenden.

Optimalere Ergebnisse erreicht man aber beim Einsatz von LCD-/TFT-Monitoren, da ClearType für LCD entwickelt und optimiert ist. 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 eine Farbtiefe von 32 Bit. Dieser Modus ist der effizienteste im Kompromiss zwischen Darstellung und Netzwerkverkehr. Eine Herabstufung auf 24 oder 16 Bit bringt keine Geschwindigkeitsvorteile, schränkt aber die Anzeige ein.

Befehlszeilenparameter für den Remotedesktopclient

Der RDP-Client hat einige Optionen für die Eingabeaufforderung, mit denen Sie einige Einstellungen direkt beim Aufrufen mitgeben können:

```
mstsc [<Verbindungsdatei>] [/v:<server[:port]>][/console] [/f[ullscreen]] [/w:<width>]
[/h:<height>]
[/public] | [/span] [/edit "Verbindungsdatei"] [/migrate] [/?] /v:<Server[:Port]>
```

- **/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 Clientverbindungs-Manager erstellt wurden, in neue RDP-Verbindungsdateien um

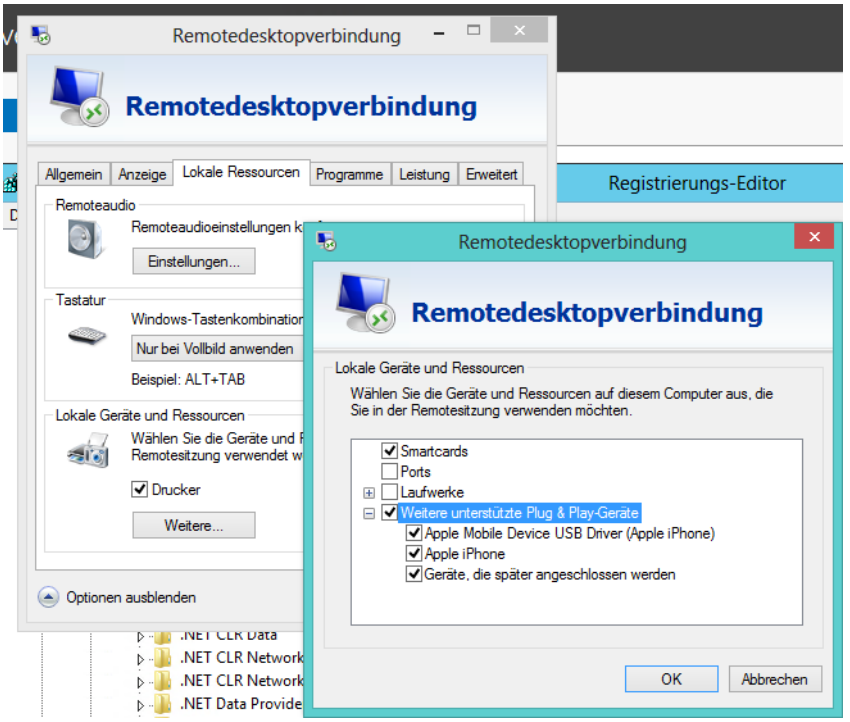
TIPP Auf der Internetseite *http://support.microsoft.com/?kbid=885187* [Ms179-K28-06] erhalten Sie ausführliche Informationen, wie Sie gespeicherte RDP-Dateien nachträglich mit einem Texteditor bearbeiten.

Die Einstellungen gelten für Windows Server 2008 R2/2012/2012 R2 und für Windows XP/Vista und Windows 7 sowie in Windows 8/8.1.

Umleitung von Digitalkameras und Mediaplayer

Plug & Play-Geräte wie Digitalkameras und Mediaplayer können Sie auf den Remotedesktopserver umleiten. Die Einstellungen finden sich im RDP-Client auf der Registerkarte *Lokale Ressourcen*. Über die Schaltfläche *Weitere* aktivieren Sie die Umleitung von Plug & Play-Geräten. Diese Umleitung funktioniert auch, wenn das Gerät nach dem Verbindungsaufbau mit dem Remotedesktopserver verbunden wird.

Abbildg. 28.23 Auch lokale Plug & Play-fähige Geräte können mit dem RDP-Client auf den Remotedesktopserver umgeleitet werden



HINWEIS Der Remotedesktopclient unterstützt für Remotedesktopserver unter Windows Server 2012 R2 auch die Umleitung für Geräte, welche die Funktion *Microsoft Point of Service* nutzen, also zum Beispiel Kassen oder Inventurgeräte.

Dazu muss auf dem Remotedesktopserver noch die Erweiterung *Microsoft Point of Service for .NET 1.12* von der Internetseite *http://www.microsoft.com/en-us/download/details.aspx?id=5355* [Ms179-K28-07] installiert werden, oder eine neuere Version, wenn diese das Endgerät unterstützt.

Verwaltung eines Remotedesktop-Sitzungshosts

In diesem Abschnitt gehen wir auf die Verwaltung der neuen Funktionen ein und beleuchten zunächst ausführlich die Konfiguration und Verwaltung der Standardfunktionen eines Remotedesktopservers.

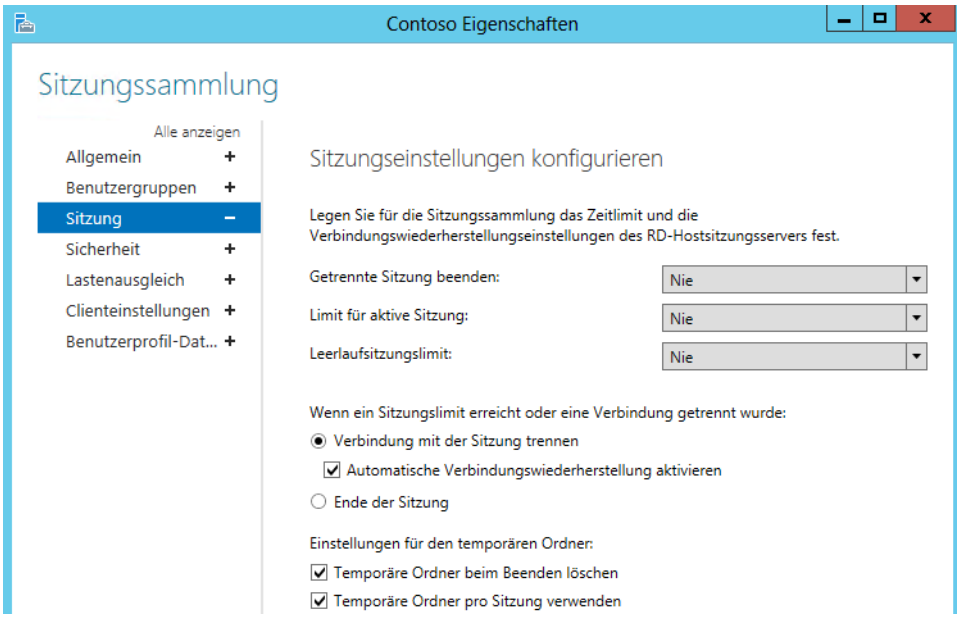
Bevor Sie sich mit speziellen Funktionen wie dem Gateway oder Webzugriff auseinandersetzen, sollten Sie zunächst die Standardverwaltung eines Servers verstehen. Im Gegensatz zu Windows Server 2008 R2 benötigen Sie keine verschiedenen Werkzeuge mehr, sondern nehmen alle Einstellungen zentral im Server-Manager über den Bereich *Remotedesktopserver* vor.

Konfiguration des Remotedesktop-Sitzungshosts

Um Systemeinstellungen für eine Sammlung (ehemals Farm) und den enthaltenen Remotedesktop-Sitzungshosts vorzunehmen, verwenden Sie den Server-Manager und den Bereich *Remotedesktopdienste*. Klicken Sie auf *Sammlungen* und dann auf die Sammlung. Passen Sie anschließend über *Aufgaben* die Systemeinstellungen an.

Sie passen an dieser Stelle den Namen der Sammlung an sowie die Benutzer, die Zugriff auf die veröffentlichen Apps haben.

Abbildg. 28.24 Anpassen einer Sitzungssammluung



Im Bereich *Sitzung* bestimmen Sie, wie sich die Remotedesktop-Serversitzungen der Benutzer bei den verschiedenen Zuständen verhalten sollen. Diese Einstellungen gelten für alle Benutzer, die sich mit dem Remotedesktopserver verbinden.

Für einzelne Benutzer können Sie in *Active Directory-Benutzer und -Computer* identische Einstellungen in den Eigenschaften des Benutzerkontos auf der Registerkarte *Sitzungen* einstellen. 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 Remotedesktopserver bestehen und alle Programme laufen weiter. Der Benutzer kann sich erneut mit dem Remotedesktopserver 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.

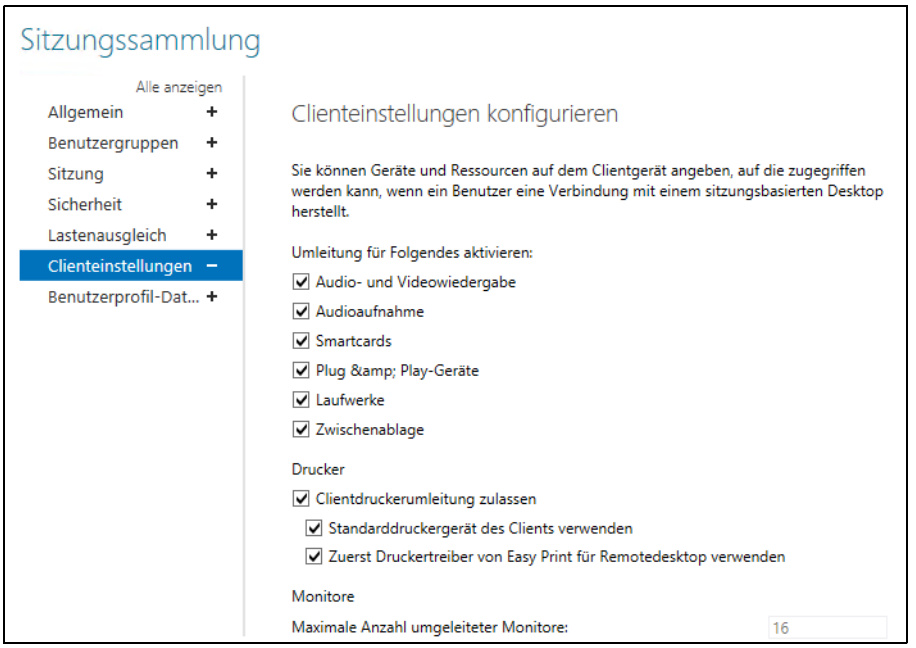
Sie können einstellen, dass eine Sitzung nach einer bestimmten Zeit getrennt wird oder getrennte Sitzungen zurückgesetzt werden. Sie definieren hier Grenzwerte für spätere Sitzungen. Diese Einstellungen sind für alle Benutzer bindend.

Im Bereich *Sicherheit* 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.

Bei *Lastenausgleich* steuern Sie beim Einsatz mehrerer Remotedesktop-Sitzungshosts, in welcher relativen Gewichtung neue Benutzer auf die Server in der Sammlung verteilt werden sollen.

Über den Bereich *Clienteinstellungen* legen Sie noch auf Seiten des Servers fest, welche Funktionen der Clients auf dem Server verfügbar sein sollen. Hier steuern Sie, ob lokale Laufwerke verfügbar sind oder die Zwischenablage. Auch das Umleiten von Druckern steuern Sie hier.

Abbildg. 28.25 Clienteinstellungen für Sammlungen steuern

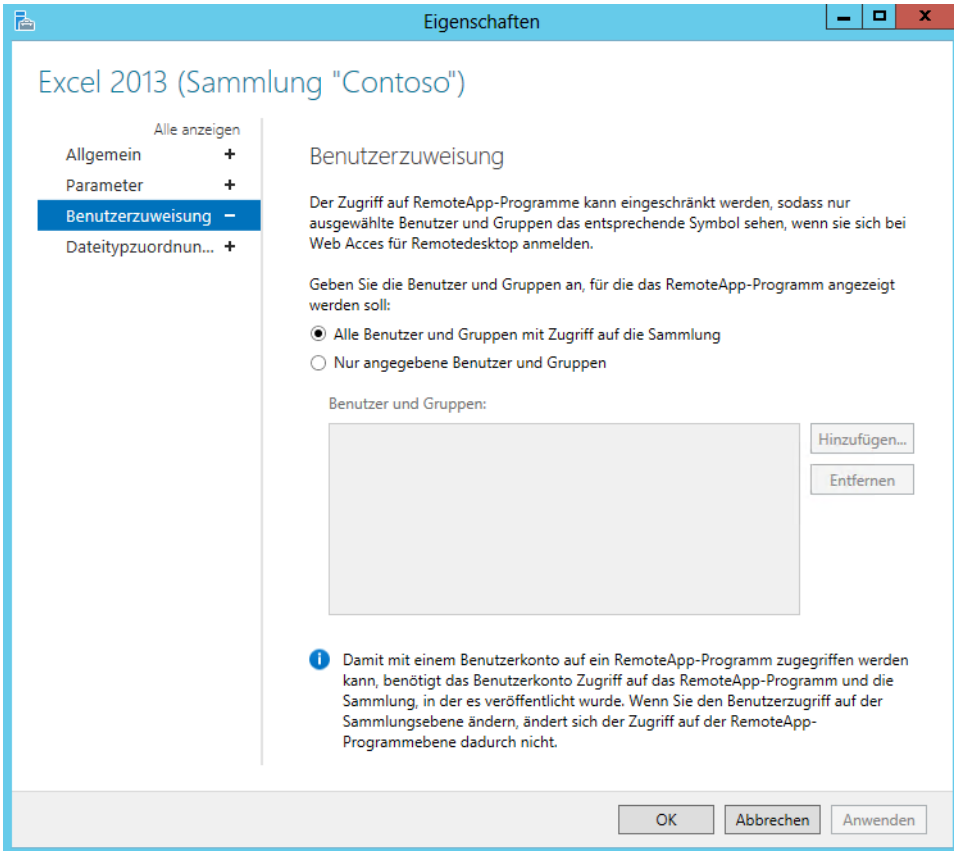


Über *Benutzerprofil-Datenträger* steuern Sie, wo der Remotedesktopsitzungshosts die Daten der Benutzer speichern soll. Sie können festlegen, welche Benutzerordner zentral gespeichert werden sollen, oder das komplette Profil berücksichtigen.

Remotedesktopdienste verwalten

Im Bereich *Verbindungen* einer Sammlung können Sie in Echtzeit sehen, welche Benutzer mit einem Server verbunden sind, welche Apps zur Verfügung stehen und welche Remotedesktop-Sizungshosts und Sie können verschiedene Einstellungen vornehmen. In diesem Bereich können Sie Benutzersitzungen trennen und getrennte Sitzungen zurücksetzen. Sie können für jede veröffentliche App Einstellungen aufrufen und die App an Ihre Bedürfnisse anpassen.

Abbildg. 28.26 Anpassen von veröffentlichten Apps



Unabhängig von den Einstellungen der kompletten Sammlung können Sie für einzelne veröffentlichte Apps Sicherheitseinstellungen vornehmen und festlegen, welche Benutzer auf die einzelnen Apps zugreifen dürfen. Müssen bestimmte Anwendungen mit Optionen starten, können Sie auch diese hier festlegen. Klicken Sie eine Sitzung mit der rechten Maustaste an, können Sie diese Sitzung im Kontextmenü über die Option *Abmelden* wieder freigeben.

Single Sign-On (SSO) für Remotedesktop-Sitzungshosts

In Windows Server 2012 R2 und Windows 8/8.1 können Sie SSO-Szenarien erstellen, damit sich Anwender nur einmal authentifizieren müssen, zum Beispiel an ihrer Arbeitsstation. Der Zugriff auf weitere Server im Netzwerk, RemoteApps und veröffentlichten Desktops (siehe Kapitel 30) erfolgt dann ohne weitere Authentifizierung. In Windows Server 2012 R2 hat Microsoft die Konfiguration dazu deutlich erleichtert.

Damit Sie diese Funktionalität nutzen können, müssen Sie Windows 8/8.1 zusammen mit Windows Server 2012 R2 einsetzen. Außerdem müssen sich beide Systeme in der gleichen Active Directory-Gesamtstruktur befinden. Auf den Arbeitsstationen unter Windows 7/8 können Sie entweder die lokale Richtlinie bearbeiten oder Sie erstellen eine Gruppenrichtlinie. Navigieren Sie zum Bereich *Computerkonfiguration/Administrative Vorlagen/System/Delegierung von Anmeldeinformationen*.

1. Öffnen Sie die Richtlinie *Delegierung von Standardanmeldeinformationen zulassen*.
2. Aktivieren Sie diese Richtlinie.
3. 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. In einer Remotedesktopdienste-Infrastruktur verwenden Sie als Servernamen den FQND des Remotedesktop-Verbindungsbrokers. Die anderen Server müssen Sie an dieser Stelle nicht mehr eintragen. Dies war in Windows Server 2008 R2 noch notwendig.

Remotedesktopsitzungen spiegeln

Mit Windows Server 2012 R2 integriert Microsoft zahlreiche Neuerungen in das Server-Betriebssystem. Viele Neuerungen betreffen auch die Remotedesktopdienste, mit denen sich Anwendungen oder Desktops für das Netzwerk virtualisieren lassen. Eine wichtige Neuerung in Windows Server 2012 R2 ist ein alter Bekannter, die Sitzungsspiegelung. Mit dieser Funktion konnten Administratoren in Vorgängerversionen von Windows Server 2012 Sitzungen der Anwender spiegeln, um zum Beispiel bei Problemen zu helfen.

Windows Server 2012 hat nicht mehr über diese Technik verfügt. In Windows Server 2012 R2 hat Microsoft diese Funktion jetzt wieder integriert. Wir zeigen Ihnen, wie Sie diese Funktion einrichten, verwalten und nutzen, um Anwendern bei Problemen zu helfen. Neben der Möglichkeit, die Spiegelung für Administratoren zu ermöglichen, zeigen wir Ihnen auch, wie Sie den Helpdesk oder Supportmitarbeiter berechtigen, Sitzungen zu spiegeln. Auch auf die Steuerung der Spiegelungen über lokale Richtlinien oder Gruppenrichtlinien gehen wir nachfolgend ein.

Windows Server 2012 R2 von Windows 8.1 aus verwalten

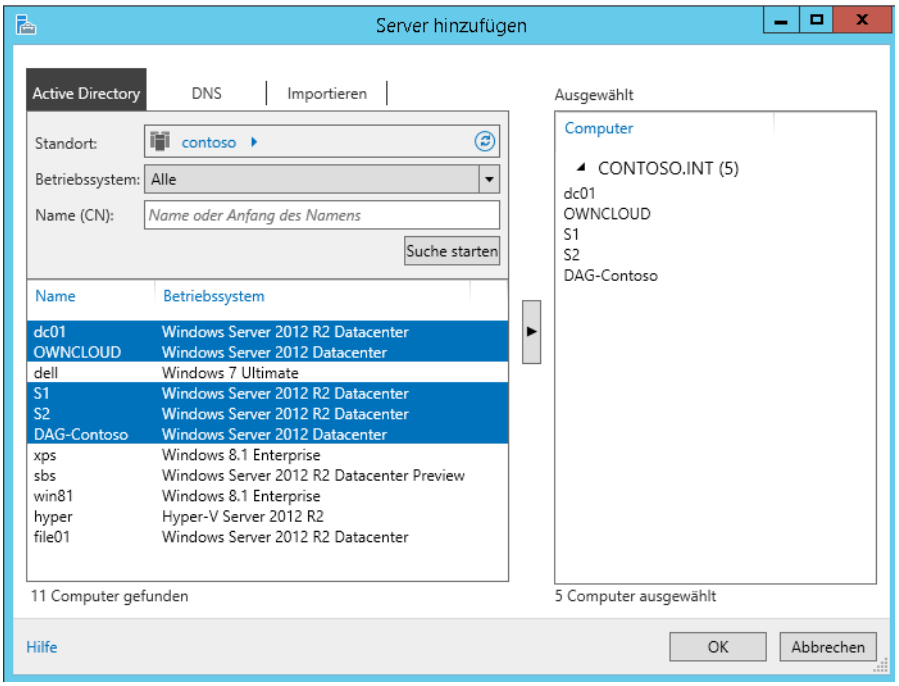
Sie können Ihre Remotedesktopserver entweder direkt per Remotedesktop oder von anderen Servern mit dem Server-Manager verwalten. Bequemer ist die Verwaltung von Servern aber von Arbeitsstationen aus. Dies ist seit Windows Server 2012 ein sehr effizienter Weg, da Sie mittlerweile auch den Server-Manager auf Arbeitsstationen installieren und alle Server einfach und effizient vom eigenen Rechner aus verwalten können. Die Verwaltung von Servern in Windows Server 2012 R2 können Sie daher komplett von Rechnern mit Windows 8.1 aus erledigen.

Dazu brauchen Sie die Remoteserver-Verwaltungstools für Windows 8.1 (*http://www.microsoft.com/de-de/download/details.aspx?id=39296* []Ms179-K28-08). Diese enthalten auch den Server-Manager und die Möglichkeit, Benutzersitzungen zu spiegeln, ohne dass Sie weitere Tools installieren müssen. Nachdem Sie das Update installiert haben, stehen die Verwaltungswerkzeuge zur Verfügung und Sie können auch alle weiteren Einstellungen der Remotedesktopdienste auf diesem Weg verwalten.

Nebenbei können Sie mit RSAT (Remote Server Administration Tool) alle weiteren Serverdienste genauso verwalten wie mit dem Server-Manager auf lokal installierten Servern mit Windows Server 2012 R2. Haben Sie den Server-Manager in Windows 8.1 aufgerufen, klicken Sie auf *Verwalten/Server hinzufügen*. Hier durchsuchen Sie jetzt Ihre Domäne und wählen alle Server aus, die Sie von der Arbeitsstation aus verwalten möchten.

Um Benutzersitzungen zu spiegeln, müssen Sie mindestens die Remotedesktop-Sitzungshosts und die Verbindungsbroker auswählen. Berechtigen Sie Anwender zum Spiegeln von Sitzungen, zum Beispiel Supportmitarbeiter oder den Helpdesk, installieren Sie auf den Rechnern der entsprechenden Mitarbeiter am besten auch die Remoteserver-Verwaltungstools und fügen zum Server-Manager die Remotedesktop-Sitzungshosts (ehemals Terminalserver) hinzu.

Abbildg. 28.27 Im Server-Manager können Sie alle Server der Domäne anbinden, unabhängig davon, ob Sie mit Windows 8.1 oder mit Windows Server 2012 R2 arbeiten



Nachfolgend zeigen wir Ihnen, wie Sie Benutzersitzungen in Windows Server 2012 R2 über den Server-Manager spiegeln können. Die Vorgänge sind dabei auf Arbeitsstationen mit Windows 8.1 und auf Servern mit Windows Server 2012 R2 identisch. Mit RSAT in Windows 8.1 können Sie auch die Serverdienste in Windows Server 2012 verwalten, nicht nur die Dienste von Windows Server 2012 R2. Unter Windows 8 können Sie mit RSAT nur sehr eingeschränkt die Dienste in Windows Server 2012 R2 verwalten. Aus diesem Grund sollten Sie auf den Arbeitsstationen am besten auf Windows 8.1 setzen.

Benutzersitzungen auf Serverfarmen verwalten

Wenn Sie nach der Installation der Remotedesktopdienste im Server-Manager eine Sammlung erstellt und Anwender angebunden sowie Apps veröffentlicht haben, können die Anwender mit den Programmen oder dem veröffentlichten Desktop arbeiten. Dies funktioniert in Windows Server 2012 R2 noch genauso wie in Windows Server 2012.

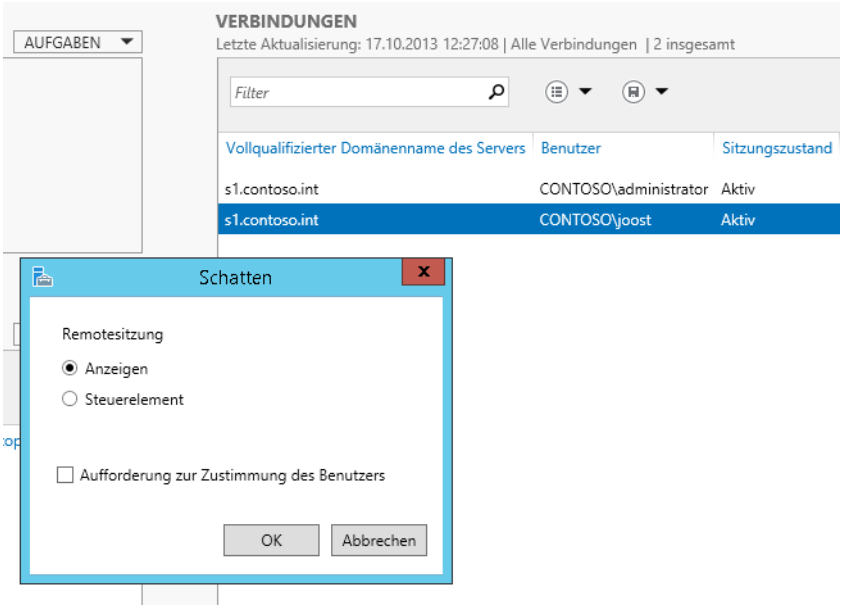
Die Verwaltung der Remotedesktopdienste findet im Server-Manager über den Bereich *Remotedesktopdienste* statt. Nachdem Sie die Farm eingerichtet haben, sehen Sie die angebundenen Anwender im Bereich *Verbindungen*, wenn Sie auf den Namen der entsprechenden Sammlung klicken. Hier sind alle angebundenen Benutzer in der Farm zu sehen. Über das Kontextmenü verwalten Sie die Benutzer und starten auf Wunsch auch die Spiegelung. Dazu später mehr.

Spiegelungen von Benutzersitzungen durchführen

Über das Kontextmenü von Sitzungen im Server-Manager können Sie auf Remotedesktop-Sitzungshosts Sitzungen von Anwendern spiegeln. Klicken Sie eine Sitzung mit der rechten Maustaste an, haben Sie – wie bereits in Windows Server 2012 – verschiedene Möglichkeiten, die Benutzer zu verwalten.

Neu ist die Option *Schatten* im Kontextmenü der Benutzersitzungen. Mit dieser Option können Sie Sitzungen wie in Vorgängerversionen von Windows Server 2012 spiegeln. Dazu sind keine weiteren Konfigurationen notwendig. Sobald Sie eine Sammlung erstellt und RemoteApps veröffentlicht habenen, sind die Anwendungen zur Spiegelung bereit.

Abbildg. 28.28 Über das Kontextmenü von Benutzersitzungen können Sie in Windows Server 2012 R2 Sitzungen spiegeln. Dazu wählen Sie die Option *Schatten* aus.



Spiegeln können Sie daher nicht nur Desktopsitzungen, sondern auch RemoteApps inklusive deren Steuerelemente. Klicken Sie die Option zum Spiegeln an (*Schatten*), wählen Sie zunächst aus, ob Sie die Sitzung nur sehen wollen, ohne selbst steuern zu können (*Anzeige*), oder ob Sie in der Sitzung auch Eingaben vornehmen möchten (*Steuerelement*). Standardmäßig ist nach der Installation der Remotedesktop-Sitzungshosts beides erlaubt und möglich. Sie müssen dazu keinerlei Einstellungen vornehmen.

Außerdem können Sie festlegen, ob der Benutzer die Verbindung bestätigen muss oder ob die Verbindung auch ohne Bestätigung stattfinden soll. Standardmäßig ist in den Richtlinien von Remotedesktopservern die Zustimmung der Benutzer festgelegt. Möchten Sie sich mit Sitzungen ohne Bestätigung der Anwender verbinden, sind zunächst Änderungen in den Richtlinien der Remotedesktopserver notwendig. Auf diesen Einstellungen kommen wir später noch zurück. Auch diese Einstellungen lassen sich schnell und einfach über lokale Richtlinien oder mit Gruppenrichtlinien festlegen.

Aktivieren Sie die Anzeige einer Sitzung und bestätigt der entsprechende Anwender die Spiegelung, sehen Sie den Remotedesktop oder die geöffnete RemoteApp des Anwenders. Sie sehen allerdings nicht den Rechner des Anwenders selbst oder andere Anwendungen, sondern nur dessen Remotedesktopsitzung. Sie können bei der Verwendung der reinen Anzeige auch keinerlei Eingaben vornehmen, sondern Sie sehen nur das, was der Benutzer in seiner RemoteApp oder seinem RDP-Desktop sieht.

Eine Interaktion mit dem Benutzer ist nicht möglich, auch keine Unterhaltung, Datenaustausch oder sonstige Funktionen. Minimiert der Anwender die RemoteApp auf seinem Rechner, wird die App auch in der Spiegelsitzung minimiert und es ist kein Inhalt mehr in der Anwendung zu sehen. Generell ist durch die Spiegelung immer festgelegt, dass nur die Anwendung und deren Informationen angezeigt werden, die auch in der gespiegelten Sitzung laufen. Alle anderen Daten des zugreifenden Rechners sind für den zugreifenden Administrator nicht sichtbar.

In den Standardeinstellungen von Remotedesktopservern erscheint bei den Anwendern immer eine Meldung auf dem Bildschirm, wenn eine Spiegelung erfolgen soll. Der Anwender kann in dieser Meldung die Spiegelung erlauben oder verweigern. Die Entscheidung des Benutzers kann von Administratoren nicht überstimmt werden. Nachdem die Spiegelung aufgebaut ist, kann der Administrator die Spiegelung durch das Schließen des Fensters beenden, der Anwender kann die Spiegelung in diesem Zusammenhang nicht schließen. Der Anwender erhält auch keine Information darüber, ob sich der Administrator von der Sitzung wieder getrennt hat.

RDP-Sitzungen remote steuern

Neben der Möglichkeit, die Sitzungen anzuzeigen, können Sie Benutzersitzungen auch komplett steuern. Dazu müssen Sie als Option *Steuerelement* aktivieren, wenn Sie die Option *Schatten* für eine Benutzersitzung ausgewählt haben. Auch hier muss der entsprechende Benutzer die Verbindung zunächst genehmigen, wenn Sie mit den Standardeinstellungen arbeiten.

Die Trennung der Sitzung erfolgt auf dem gleichen Weg wie bei der reinen Anzeige. Der Administrator muss das Fenster lediglich schließen. Der Anwender, den Sie spiegeln, sieht alle von Ihnen durchgeführten Eingaben. Leider fehlen Funktionen wie Chat oder Dateiaustausch. Auch Drag & Drop funktioniert zwischen den Sitzungen nicht. Ansonsten lassen sich in der Sitzungen aber alle Aufgaben durchführen, die auch der gespiegelte Benutzer durchführen kann. Beide Benutzer arbeiten gleichzeitig mit dem Desktop oder der RemoteApp.

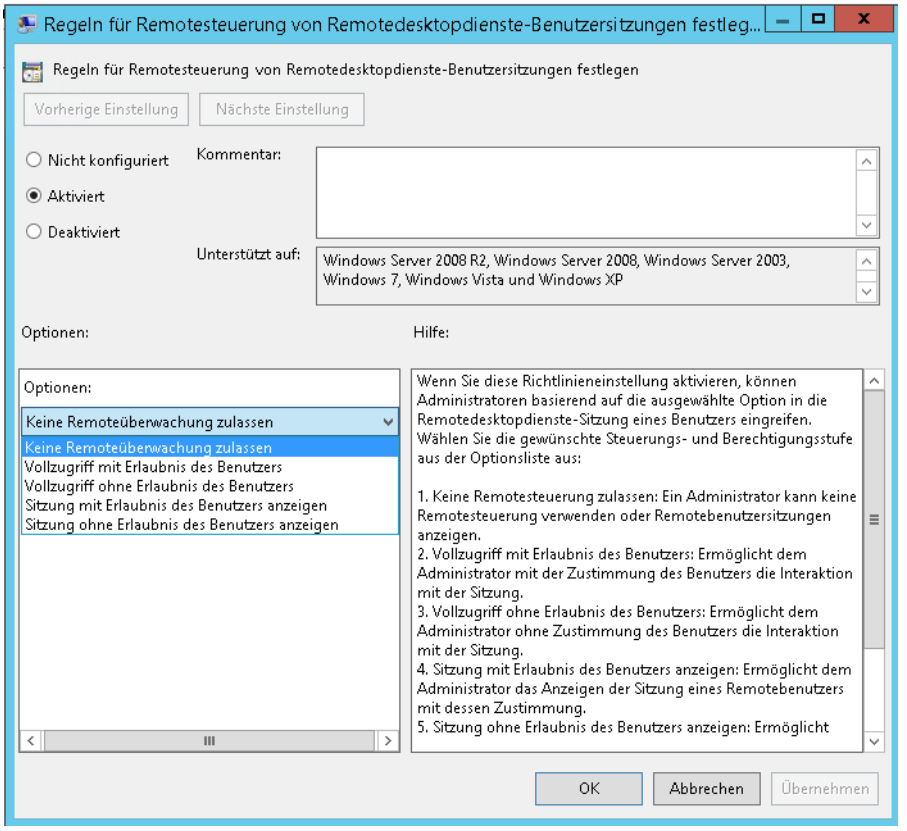
Gruppenrichtlinieneinstellungen und Systemeinstellungen für die Spiegelung

Einstellungen für die Spiegelung nehmen Sie über lokale Richtlinien oder in den Gruppenrichtlinien vor, die Sie den Remotedesktop-Sitzungshosts zuweisen. Sie finden die Konfiguration über *Benutzerkonfiguration/(Richtlinien)/Administrative Vorlagen/Windows-Komponenten/Remotedesktopdienste/Remotedesktopsitzungs-Host/Verbindungen*.

Hier finden Sie die Einstellung *Regeln für Remotesteuerung von Remotedesktopdienstebenutzern festlegen*. Sie können an dieser Stelle entweder eine Gruppenrichtlinie in der Domäne erstellen und den Remotedesktop-Sitzungshosts zuweisen oder Sie nehmen die Einstellung einfach in den lokalen Richtlinien der einzelnen Remotedesktops-Sitzungshosts vor (*gpedit.msc*).

Ohne dass Sie etwas einstellen, dürfen nach der Erstellung einer Farm Administratoren im Server-Manager die Spiegelung durchführen, wie zuvor besprochen. Es sind keine Zusatzwerkzeuge oder besondere Einstellungen notwendig, Spiegelungen funktionieren in Windows Server 2012 R2 automatisch und immer. Aktivieren Sie die Richtlinie auf einem Server, haben Sie verschiedene Einstellungsmöglichkeiten.

Abbildg. 28.29 Über lokale Richtlinien oder mit Gruppenrichtlinien legen Sie fest, ob und wie Administratoren auf Remotedesktop-Sitzungshosts Sitzungen spiegeln dürfen



Um Einstellungen zu ändern, aktivieren Sie die Richtlinie und wählen dann im Dropdownmenü aus den angezeigten Optionen aus:

- **Keine Remotesteuerung zulassen** Administratoren können keine Remotesteuerung verwenden oder Remotebenutzersitzungen anzeigen. Eine Spiegelung ist daher nicht erlaubt. Wenn ein Administrator eine Sitzung spiegeln will, erscheint die Meldung, dass die Funktion über Richtlinien geblockt ist.
- **Vollzugriff mit Erlaubnis des Benutzers** Erlaubt Administratoren mit der Zustimmung des entsprechenden Benutzers die Steuerung einer Sitzung, also auch die Bedienung. In diesem Fall ist auch das Anzeigen erlaubt.
- **Vollzugriff ohne Erlaubnis des Benutzers** Erlaubt Administratoren auch ohne Zustimmung des Benutzers die Steuerung der Sitzung. In diesem Fall können Administratoren beim Spiegeln auch das Kontrollkästchen bei der Option deaktivieren, dass der Benutzer gefragt werden muss. Auch die Anzeigefunktion ist mit dieser Einstellung erlaubt.
- **Sitzung mit Erlaubnis des Benutzers anzeigen** Erlaubt Administratoren das Anzeigen von Sitzungen mit Zustimmung des Benutzers. Eine Steuerung der Sitzungen ist aber nicht erlaubt.
- **Sitzung ohne Erlaubnis des Benutzers anzeigen** Ermöglicht Administratoren das Anzeigen von Sitzung auch ohne Zustimmung des Benutzers

Wenn Sie diese Richtlinieneinstellung deaktivieren, können Administratoren mit der Zustimmung des Benutzers in dessen Remotedesktopdienstesitzung eingreifen und Sitzungen spiegeln. Das geht auch, wenn Sie gar nichts konfigurieren.

Spiegelung für Nicht-Administratoren

Standardmäßig dürfen nur Administratoren des Servers Sitzungen auf den Remotedesktop-Sitzungshosts spiegeln. Sollen auch normale Anwender, zum Beispiel Supportmitarbeiter, Sitzungen spiegeln dürfen, müssen Sie die entsprechenden Benutzerkonten erst dazu berechtigen. Sie können dazu die Eingabeaufforderung auf dem Remotedesktop-Sitzungshost verwenden:

```
Wmic /NameSpace:\\root\cimv2\TerminalServices PATH
WIN32_TSPermissionsSetting.TerminalName="RDP-TCP" call AddAccount "<Domäne\Benutzer>",
<Wert>
```

Für <*Wert*> stehen folgende Möglichkeiten zur Verfügung:

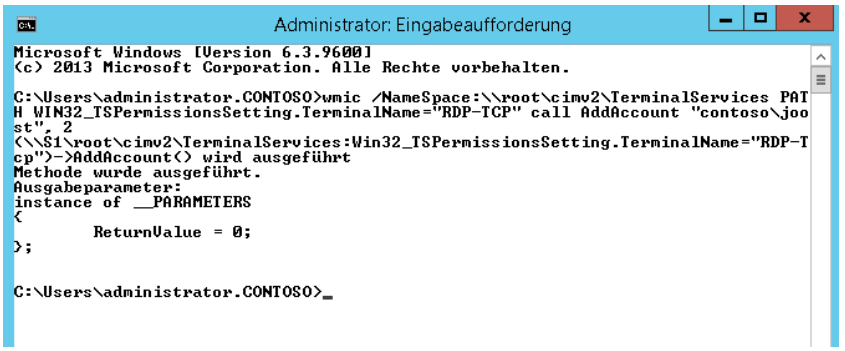
- 0 = WINSTATION_GUEST_ACCESS
- 1 = WINSTATION_USER_ACCESS
- 2 = WINSTATION_ALL_ACCESS

Damit die Anwender die Spiegelung auch durchführen können, ist der beste Weg, wenn Sie auf den Arbeitsstationen der Anwender die Remoteserver-Verwaltungstools für Windows 8.1 installieren und den Server-Manager zur Verfügung stellen.

Mit welchen Optionen sich die Anwender zur Spiegelung verbinden können, also Anzeigen oder Steuern von Sitzungen, legen Sie über die Gruppenrichtlinien fest, wie zuvor beschrieben. Sobald Sie Anwendern das Spiegeln erlauben, dürfen diese die Spiegelung auch durchführen, selbst wenn Sie

noch keine weiteren Einstellungen vorgenommen haben. Nach der entsprechenden Berechtigung dürfen die Anwender auch Administratorsitzungen spiegeln, allerdings nicht die Konsolensitzung direkt auf dem Server.

Abbildg. 28.30 Auch Anwendern können Sie für Remotedesktop-Sitzungshosts das Spiegeln von Sitzungen erlauben



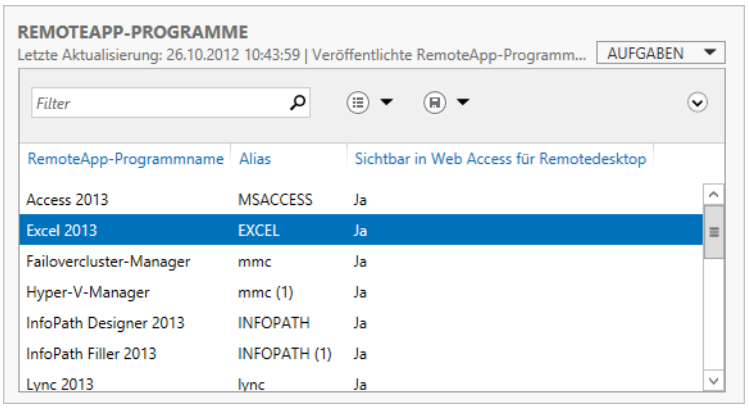
TIPP Was viele Firmen in diesem Zusammenhang interessieren wird, ist die Tatsache, dass Sie Ihre Remotedesktops-Sitzungshosts recht einfach von Windows Server 2012 zu Windows Server 2012 R2 aktualisieren können.

Clientzugriffslizenzen und Remotedesktoplizenzen von Windows Server 2012 sind auch in Windows Server 2012 R2 gültig, Sie brauchen daher lediglich eine neue Serverlizenz und können nach der Aktualisierung Sitzungen spiegeln.

RemoteApps verwalten

Wie in den vorangegangenen Abschnitten bereits behandelt, hat Microsoft in Windows Server 2012 R2 die Veröffentlichung von Apps über den Server-Manager erleichtert. Die können Anwendungen, die auf dem Remotedesktop-Sitzungshost installiert sind, für Anwender freigeben. Über den gleichen Weg können Sie die Bereitstellung der Apps auch wieder aufheben.

Abbildg. 28.31 Verwalten der veröffentlichten Apps



Anwender können ohne Desktopverbindung auf die veröffentlichte Anwendung zugreifen. Für den Anwender ist diese Technik transparent, er kann nicht feststellen, ob diese Anwendung lokal oder in einer Remotedesktop-Serversitzung 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.

HINWEIS Veröffentlichte Anwendungen und Remotedesktops oder virtuelle Desktops von Computern lassen sich in Windows 7/8/8.1 auch im Startmenü bzw. auf der Startseite anzeigen. Wir kommen in diesem Kapitel noch ausführlicher auf diese Konfiguration.

Die Bedienung von veröffentlichten Anwendung ist identisch mit der Bedienung eines lokalen Programms auf dem PC. 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 Remotedesktopserver installiert werden können, Sie müssen dazu keine besonderen Versionen kaufen. Beim Einsatz von Office 2007/2010/2013 benötigen Sie aber eine Lizenz, die für den Remotedesktopeinsatz freigegeben ist.

Anwender können natürlich mit ihrem Desktop parallel zu den serverbasierten RemoteApp-Anwendungen auch lokale Anwendungen starten, ein Mischbetrieb ist daher ohne Weiteres möglich, auch ein Datenaustausch. So können Anwender zum Beispiel mit Ihren Anwendungen arbeiten und Sie können den SAP-Client über einen Remotedesktopserver zur Verfügung stellen.

Die RemoteApp-Programme können Sie über eine Weboberfläche zur Verfügung stellen (*https://<Servername>/rdweb*). Die Verknüpfungen lassen sich auch durch die Softwareverteilung in den Gruppenrichtlinien in die Startmenüs/Startseiten oder Desktops auf den Clients pushen.

Konfiguration von Remotedesktopdienste-RemoteApp

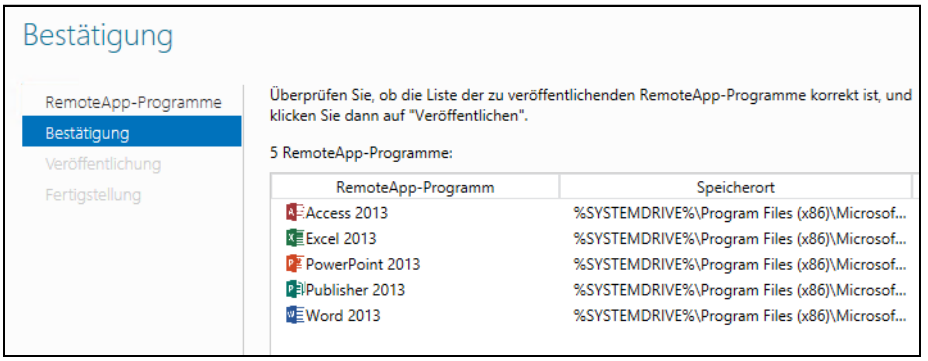
Um eine Anwendung als RemoteApp zur Verfügung zustellen, müssen Sie zunächst den Remotedesktopserver regulär installieren und die Sammlung einrichten, wie in den vorangegangenen Abschnitten besprochen.

Auch die Anwendungen werden auf normalem Weg auf dem Server installiert. Nachdem Sie den Server vorbereitet haben, finden Sie alle notwendigen Einstellungen im Server-Manager über *Remotedesktopdienste/Sammlungen/<Name der Sammlung>* im Bereich *RemoteApp-Programme*.

Über diesen Bereich können Sie zusätzliche Anwendungen hinzufügen und die Anwendungsliste verwalten. Auch Einstellungen für Apps rufen Sie auf diesem Weg auf. Um eine Anwendung der Liste hinzuzufügen, klicken Sie in der Spalte *Aufgaben* auf *RemoteApp-Programme veröffentlichen*. Im Anschluss startet der RemoteApp-Assistent, über den Sie die Anwendungen der Liste hinzufügen können. Wählen Sie entweder das Programm aus der Liste aus oder klicken Sie auf *Hinzufügen*, um die Startdatei der Anwendung hinzuzufügen. Achten Sie darauf, dass die Anwendung auf den Remotedesktop-Sitzungshosts installiert sein muss. Sie können an dieser Stelle mehrere Anwendungen auswählen.

Auf der nächsten Seite sehen Sie eine vollständige Liste und veröffentlichen die Anwendung über die Schaltfläche *Veröffentlichen*. Die Apps sind anschließend schon im Web Access der Remotedienste verfügbar.

Abbildg. 28.32 Veröffentlichen von Apps im Server-Manager



Neben der Konfiguration der RemoteApp-Liste sollten Sie auch die globalen Einstellungen für die Remotedesktopserver konfigurieren. Die globalen Einstellungen haben die Aufgabe, die Remotedesktopserver so zu steuern, dass nur authentifizierte und berechtigte Benutzer auf die RemoteApps zugreifen können.

TIPP Über die Eigenschaften einer RemoteApp können Sie auf der Registerkarte *Benutzerzuweisung* auf Basis von Benutzergruppen oder Benutzern in Active Directory festlegen, welche Benutzer auf RemoteApps zugreifen dürfen.

Mit Windows 8.1 auf RemoteApps zugreifen

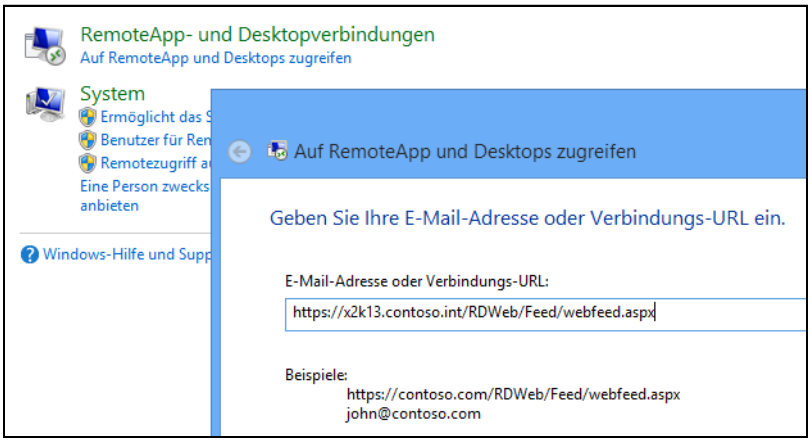
RemoteApps stehen nach der Veröffentlichung automatisch für alle Clients über den Webzugriff zur Verfügung. Diesen erreichen Sie über die URL *https://<Servername>/rdweb*. Nach der Authentifizierung stehen sofort alle RemoteApps zur Verfügung, die Sie veröffentlichen, Berechtigungen vorausgesetzt. In diesem Kapitel zeigen wir Ihnen auch, wie Sie RemoteApps auf der Startseite von Windows 8.1 automatisiert bereitstellen.

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 Remotedesktopserver ausgeführt wird, Daten über die Zwischenablage in ein lokales Excel zu übernehmen oder umgekehrt. 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:

1. Um die Anbindung der veröffentlichten Anwendungen auf Windows 8.1-Clients zu testen, melden Sie sich am Client an und suchen in der Systemsteuerung nach *RemoteApp*.
2. Öffnen Sie die Verwaltung der RemoteApps und klicken Sie auf *Auf RemoteApps und Desktops zugreifen*.

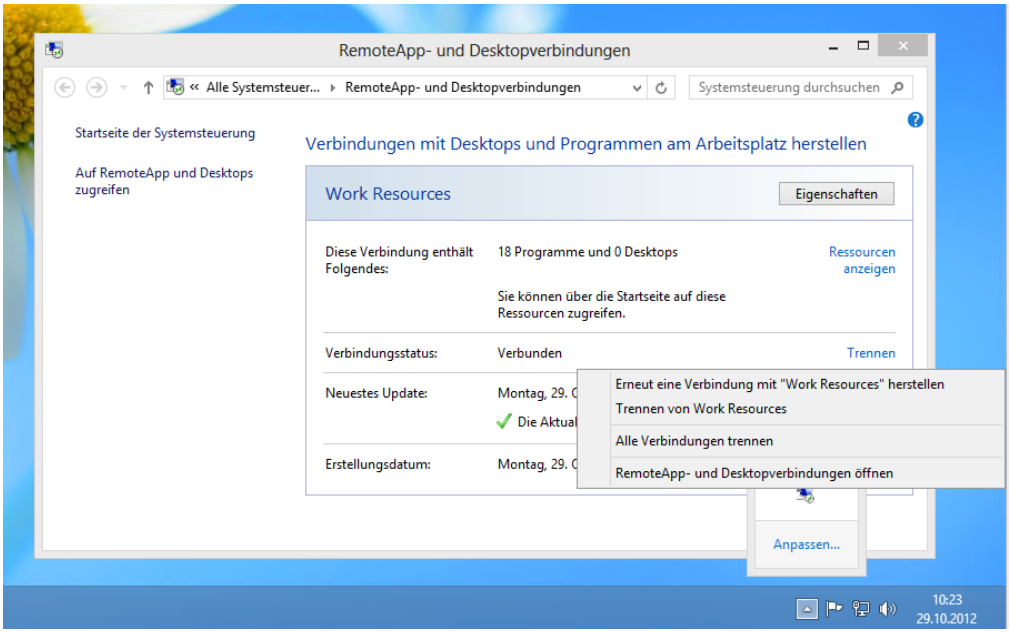
3. Geben Sie die URL *https://<Webzugriff-Server>/RDWeb/Feed/webfeed.aspx* ein. Der Webzugriffsserver erhält seine Daten vom Verbindungsbroker, auf dem Sie als Quelle wiederum den Remotedesktopserver eingerichtet haben.

Abbildg. 28.33 Hinzufügen von RemoteApps zu Windows 8.1-Clients



Anschließend lädt der Client alle Daten zu den RemoteApps herunter und stellt diese auf der Startseite zur Verfügung. Sie erhalten hierzu ein Informationsfenster angezeigt. Sie sehen den aktuellen Verbindungsstatus auch über ein Symbol in der Taskleiste. Hier können Sie die Verbindung zum Server trennen oder sich die Einstellungen der Programme und den Status der Verbindung anzeigen lassen.

Abbildg. 28.34 Anzeigen des Verbindungsstatus eines Clients zu einer Remotedesktopsammlung



Anwender finden die Anwendungen auf der Startseite und können diese aufrufen wie lokal installierte Anwendungen auch. Klicken Anwender auf eine Verknüpfung, öffnet sich die Anwendung auf dem Remotedesktopserver, aber die Anwender können mit der Software arbeiten, als ob diese lokal installiert ist.

Remotedesktopdienste-Webzugriff

Windows Server 2012 R2 bietet einen Webzugriff für die Remotedesktopdienste an. Der Funktionsumfang ist ähnlich zu Outlook Web Access von Exchange. Über den Remotedesktopdienste-Webzugriff können Sie zum Beispiel einen Remotedesktopserver im Internet zur Verfügung stellen oder Ihre RemoteApps veröffentlichen. Standardmäßig werden die Applikationen, die Sie als RemoteApps zur Verfügung stellen, über den Remotedesktopdienste-Webzugriff zur Verfügung gestellt.

HINWEIS Wird der RemoteApps-Liste eine neue Anwendung hinzugefügt, wird diese automatisch im Remotedesktopdienste-Webzugriff angezeigt; es sind keine weiteren Maßnahmen zur Konfiguration notwendig.

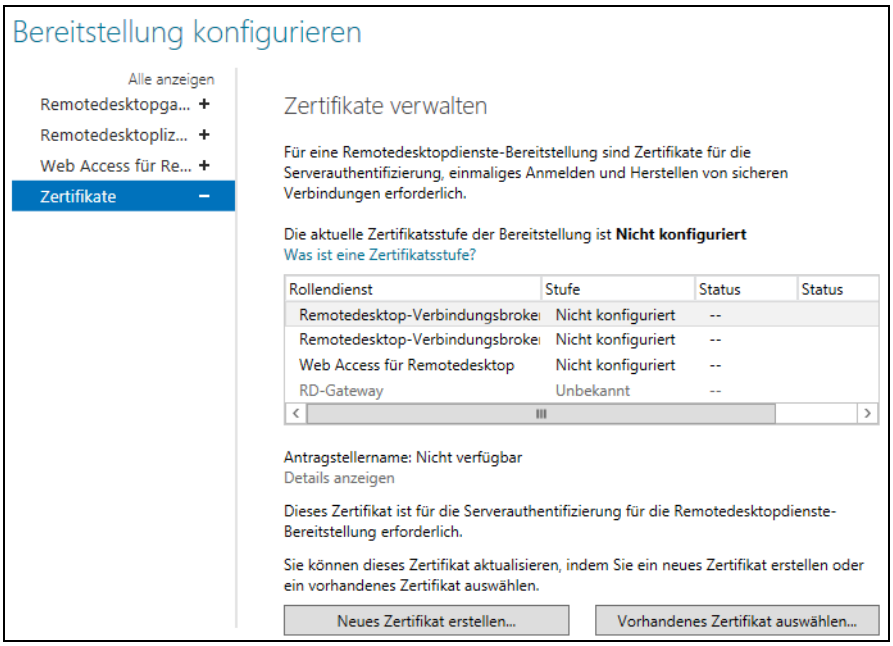
Der Remotedesktopdienste-Webzugriff ist ein Rollendienst der Remotedesktopdienste, den Sie entweder bereits bei der Installation oder auch nachträglich anpassen können. Die Einstellungen dazu finden Sie im Server-Manager über *Remotedesktopdienste/Sammlungen*. Klicken Sie bei der entsprechenden Sammlung auf Aufgaben und dann auf *Bereitstellungseigenschaften bearbeiten.* Nach der Einrichtung steht Ihnen der Web Access über *https://<Servername>/rdweb* der Webzugriff zur Verfügung.

Erstellen Sie eine neue Sammlung, wie auf den vorangegangenen Seiten besprochen, legen Sie bereits bei der Einrichtung die Einstellungen für den Webzugriff fest. Die Rolle sollte auf einem Windows Server 2012 R2 mit installiertem IIS 8 durchgeführt werden (siehe Kapitel 27). Beim Server mit Web Access muss es sich aber nicht unbedingt um einen Remotedesktop-Sitzungshost handeln. Greifen Anwender über das Webportal auf den Remotedesktopserver zu, müssen diese nicht zuvor auch den RDP-Client gestartet haben. Anwendungen, die als RemoteApp konfiguriert sind, stehen standardmäßig automatisch auch über den Remotedesktopdienste-Webzugriff zur Verfügung und lassen sich über einen einfachen Klick starten.

HINWEIS Handelt es sich beim Webzugriff-Server um einen anderen Server als den Remotedesktopserver, über den Sie die Applikationen zur Verfügung stellen, müssen Sie auf dem Remotedesktopserver mit den RemoteApps das Computerkonto des Servers mit Web Access in die Sicherheitsgruppe *RDS-Remotezugriffsserver* hinzufügen.

Standardmäßig arbeitet der Remotewebzugriff mit einem selbstsignierten Zertifikat. Dieses sollten Sie in produktiven Umgebungen aber gegen ein Zertifikat einer internen Zertifizierungsstelle austauschen. Mehr zu diesem Thema lesen Sie in Kapitel 30. Sie finden die Einstellungen dazu im Server-Manager über *Remotedesktopdienste/Sammlungen*. Klicken Sie die Sammlung an, für die Sie das Zertifikat anpassen wollen, und wählen Sie *Aufgaben/Bereitstellungseigenschaften* bearbeiten. Im Bereich *Zertifikate* erstellen Sie ein neues Zertifikat für die entsprechenden Dienste.

Abbildg. 28.35 Neues Zertifikat für Remotedesktopdienste



Wie Sie Zertifikate auf den Servern installieren, lesen Sie in Kapitel 30. Sie sollten möglichst mit den Active Directory-Zertifikatdiensten arbeiten, lokal auf den Servern Zertifikate installieren und diese dann über den Assistenten hinzufügen.

Remotedesktopgateway

Die Aufgabe des Remotedesktopgateway besteht darin, Anwendern, die sich über das Internet mit dem Unternehmen mit HTTPS verbinden, Zugriff auf die internen Remotedesktopserver zu gestatten. Ein Remotedesktopgateway verbindet das RPD- mit dem HTTPS-Protokoll, um eine gesicherte Verbindung zu allen möglichen Remotedesktopservern, 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. 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.

Gateways ermöglichen den Zugriff auf RDP-Sitzungen über Firewalls oder Netzwerkadressübersetzung (Network Address Translation, NAT) hinweg. Die Verbindung zwischen Client und Gateway erfolgt über den Port 443 (SSL). Nur die Verbindung zwischen Gateway und Remotedesktopserver erfolgt über den RDP-Port (3389).

Bisher konnten Anwender über das Internet nicht auf Remotedesktopserver zugreifen, wenn der Port 3389 blockiert ist, was meistens der Fall und auch sinnvoll ist. Sie können mit einem Gatewayserver unter Windows Server 2012 R2 den Zugriff auf Remotedesktopserver gewähren, die unter Windows Server 2003/2008/2008 R2, Windows 2000 Server und sogar Windows NT 4.0 Terminalserver Edition installiert sind. Auch der Zugriff auf den Remotedesktop von Windows XP oder Windows Vista/7 oder Windows 8.1 wird unterstützt.

Über Richtlinien können Sie festlegen, wer sich über das Internet auf die Remotedesktopserver 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.

Gateways können auch die Netzwerkzugriffsschutz (Network Access Protection, NAP)-Funktion von Windows Server 2012 R2 und Windows Vista/7 nutzen, um den Zugriff zu steuern (siehe Kapitel 31). Verwenden Sie als Zertifizierungsstelle am besten eine interne Zertifizierungsstelle, genauso wie bei einer Veröffentlichung von Outlook Web Access (siehe Kapitel 30). Achten Sie darauf, dass der Name des Zertifikats mit dem DNS-Namen des 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 Gateways und des Clients integrieren. Befinden sich Gateway und Firewall in einer Active Directory-Domäne, wird die Zertifizierungsstelle automatisch als vertrauenswürdig integriert.

Der Verbindungsaufbau der Clients zu den Remotedesktopservern findet über die Richtlinien auf dem Gateway statt. Diese werden auch als *Verbindungsautorisierungsrichtlinien* bezeichnet. Außerdem gibt es noch die *Ressourcenautorisierungsrichtlinien*. Diese steuern, auf welche Server die Clients zugreifen dürfen, die Sie in mindestens einer Verbindungsautorisierungsrichtlinie festgelegt haben. Bevor der Zugriff über das Internet auf ein Gateway und die Remotedesktopserver funktioniert, müssen Sie mindestens eine Verbindungsautorisierungsrichtlinie und eine Ressourcenautorisierungsrichtlinien konfiguriert haben.

Einrichtung und Konfiguration eines Remotedesktopgateways

Um ein Gateway zu installieren, wählen Sie im Server-Manager im Bereich *Remotedesktopdienste/Übersicht* den Link *Remotedesktopgateway* aus. Es startet ein Assistent, über den Sie das Gateway einrichten. Achten Sie aber darauf, dass Sie den Server im Server-Manager vorher über *Verwalten/Server hinzufügen* verbinden müssen.

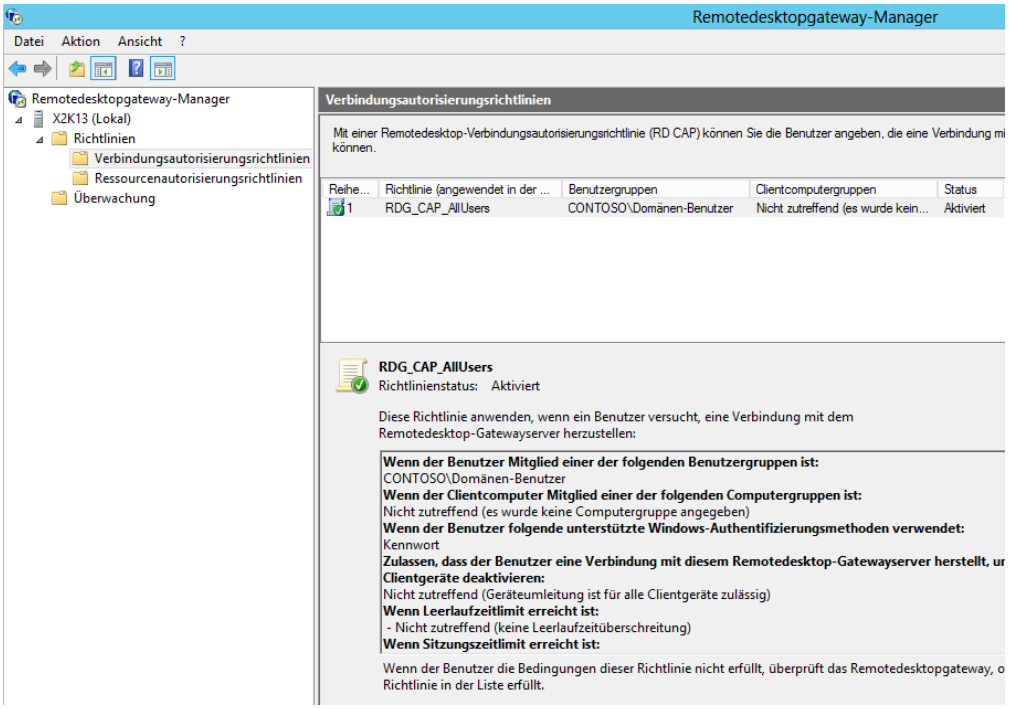
Während der Installation können Sie bereits das Zertifikat für die SSL-Verbindung auswählen. Für Testzwecke können Sie auch das selbstsignierte Zertifikat der Remotedesktopdienste verwenden. In einer produktiven Umgebung sollten Sie jedoch möglichst eine eigene Zertifizierungsstelle verwenden oder ein Zertifikat von einer öffentlichen Zertifizierungsstelle, der die beteiligten Server und Arbeitsstationen vertrauen müssen. Sie können das Zertifikat in den Bereitstellungseigenschaften jederzeit ändern.

Abbildg. 28.36 Verwalten des Zertifikats für das Remotedesktopgateway

Nachdem der Server-Manager die Rolle für das RD-Gateway installiert hat, sollten Sie die notwendigen Richtlinien bearbeiten, mit denen sich Clients verbinden können. Die Einstellungen zur Konfiguration des RD-Gateways können Sie auch jederzeit in den Bereitstellungseigenschaften anpassen.

Die Richtlinien für das Gateway können Sie nicht über den Server-Manager erstellen, sondern benötigen den Remotedesktopgateway-Manager. Diesen rufen Sie über die Gruppe *Terminal Services* im Menü *Tools* des Server-Managers auf.

Abbildg. 28.37 Verwalten der Richtlinien für das Remotedesktopdienste-Gateway



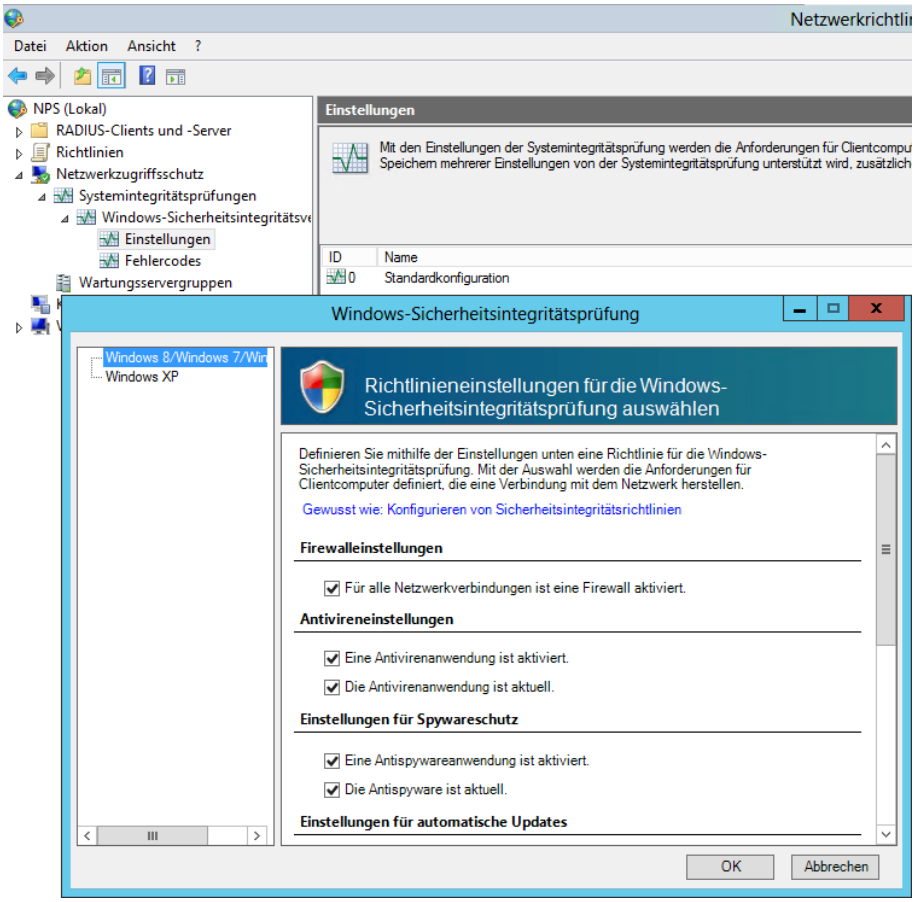
Über den Eintrag *Richtlinien/Verbindungsautorisierungsrichtlinien* in der Konsolenstruktur erstellen Sie im Remotedesktopgateway-Manager neue Richtlinien oder ändern Einstellungen vorhandener Richtlinien.

An dieser Stelle konfigurieren Sie, in welcher Gruppe sich die Anwender in Active Directory befinden müssen, damit die Einwahl funktioniert. Sie können die Umleitung der Ressourcen auf den Clients konfigurieren und die Art der Anmeldung. Über das Kontextmenü von *Verbindungsautorisierungsrichtlinien* starten Sie einen Assistenten, mit dem Sie gleichzeitig eine Verbindungsautorisierungsrichtlinie (RD-CAP) und ein eine Ressourcenautorisierungsrichtlinie (RD-RAP) erstellen. Standardmäßig sind nach der Installation eines RD-Gateways bereits entsprechende Richtlinien vorhanden.

Remotedesktopgateway und Netzwerkzugriffsschutz (NAP)

Remotedesktopgateways arbeiten mit dem Netzwerkzugriffschutz (Network Access Protection, NAP, siehe Kapitel 31) zusammen. Auf der Registerkarte *RD CAP-Speicher* in den Eigenschaften des Gatewayservers konfigurieren Sie, ob die Clients, die sich über das Gateway authentifizieren, auch über eine NAP-Richtlinie berechtigen müssen.

Abbildg. 28.38 Konfigurieren der Integritätsüberprüfung von Computern im Netzwerk



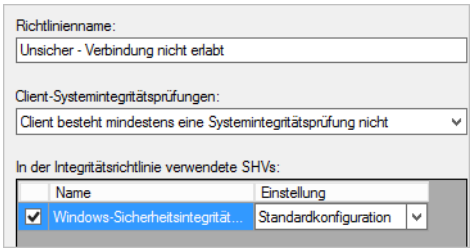
Aktivieren Sie in diesem Fall auf dieser Registerkarte die Option *Clients müssen SoH (Statement of Health) senden*. Damit ein Remotedesktopgateway NAP unterstützt, müssen Sie anschließend eine entsprechende Richtlinie auf dem Netzwerkrichtlinienserver konfigurieren oder anpassen:

1. Diese Einstellungen nehmen Sie im Server-Manager über *Tools/Netzwerkrichtlinienserver* vor.
2. Öffnen Sie in den Konsolenstruktur den Knoten *Netzwerkzugriffschutz*.
3. Klicken Sie auf *Netzwerkzugriffschutz/Systemintegritätsprüfungen*.
4. Klicken Sie auf *Standardkonfiguration* bei der Option *Windows-Sicherheitsintegritätsprüfung/Einstellungen*.
5. Rufen Sie im Kontextmenü der Option *Standardkonfiguration* den Befehl *Eigenschaften* auf.
6. Hier können Sie jetzt einstellen, welche Voraussetzungen ein Client erfüllen muss, um auf das Netzwerk zugreifen zu können.

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. Aktivieren Sie *Windows-Sicherheitsintegritätsprüfung* und klicken Sie auf *OK*.

Abbildg. 28.39 Erstellen einer neuen Integritätsrichtlinie



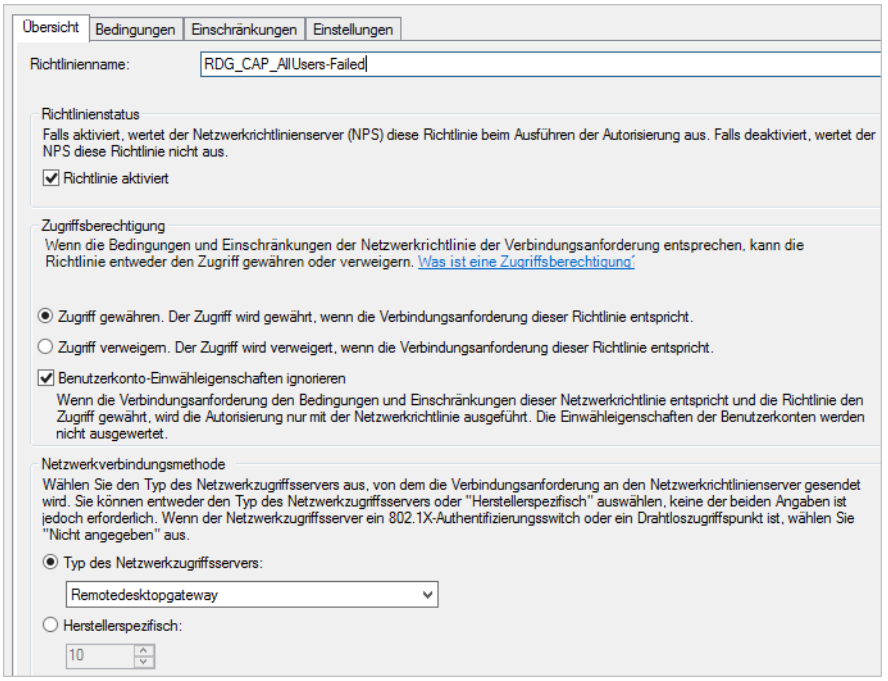
Erstellen Sie eine weitere Richtlinie, in der Sie konfigurieren, dass dem Client der Zugriff gestattet wird, wenn der PC die Richtlinien erfüllt. Die Erstellung ist analog zur ersten Richtlinie. Geben Sie den Namen *Sicher-Verbindung erlaubt* und wählen Sie die Option *Client besteht alle Systemintegritätsprüfungen*.

Durch Konfiguration dieser beiden Richtlinien wird allerdings noch kein Zugriff gestattet oder verweigert, sondern nur der Status festgelegt auf Basis der hinterlegen Sicherheitsintegritätsverifizierung. Sie müssen im nächsten Schritt zunächst eine Netzwerkrichtlinie bearbeiten oder erstellen, welchen 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 RD-CAP in der Mitte der Konsole auf.

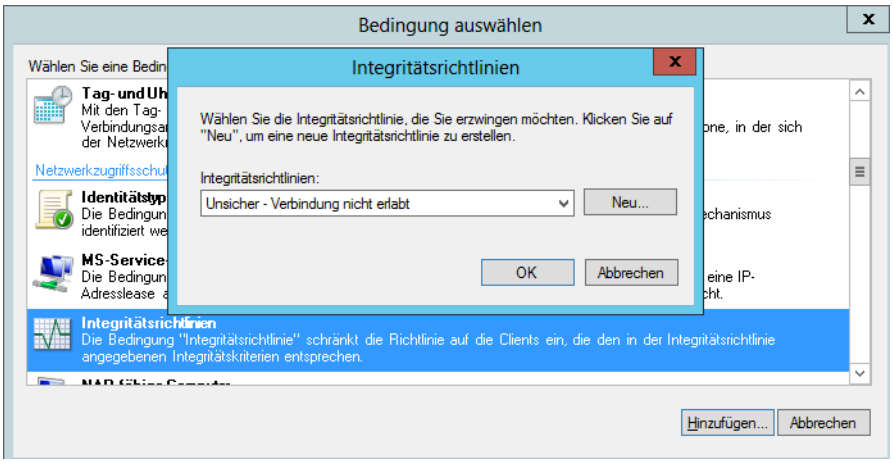
3. Sinnvollerweise bearbeiten Sie die erste standardmäßige Richtlinie so, dass Sie den Zugriff auf das Gateway verweigern, wenn der zugreifende PC nicht sicher ist. Als Basis für diese Richtlinie dient die erstellte Integritätsüberprüfungs-Richtlinie, die Sie zuvor erstellt haben.
4. Ändern Sie daher den Namen der Richtlinie auf *RD-CAP-Failed* ab.
5. Stellen Sie sicher, dass die Richtlinie aktiviert ist.
6. Aktivieren Sie die Option *Zugriff gewähren*. Sie können hier zwar auch die Verbindung gleich verweigern. Besser ist jedoch, hier die Verbindung zu gewähren und später auf die Server einzuschränken, von welchen Computer Updates oder Antivirenprogramme herunterladen werden können.
7. Stellen Sie sicher, dass die Option *Remotedesktopgateway* bei *Typ des Netzwerkzugriffsservers* aktiviert ist.
8. Wechseln Sie zur Registerkarte *Bedingungen*.

Abbildg. 28.40 Konfiguration einer NAP-Richtlinie für den Zugriff für das Remotedesktopgateway



9. Klicken Sie auf der Registerkarte *Bedingungen* auf *Hinzufügen*.
10. Markieren Sie *Integritätsrichtlinien*.
11. Klicken Sie auf *Hinzufügen*.
12. Wählen Sie die Richtlinie *Unsicher – Verbindung nicht erlaubt* aus.

Abbildg. 28.41 Bearbeiten einer Richtlinie und Hinterlegen einer neuen Prüfung



13. Aktivieren Sie auf der Registerkarte *Einschränkungen* die Option *Clientverbindung ohne Aushandlung einer Authentifizierungsmethode zulassen*.
14. Wechseln Sie zur Registerkarte *Einstellungen*.
15. Klicken Sie auf die Option *NAP-Erzwingung*.
16. Stellen Sie sicher, dass die Option *Eingeschränkten Zugriff gewähren* aktiviert ist, und hinterlegen Sie die Adressen der Wartungsserver. Alternativ lassen Sie weiter vorne bereits die Verbindung verweigern, wenn ein Client den Bedingungen nicht entspricht.
17. Erstellen Sie eine zweite Richtlinie, zum Beispiel mit der Bezeichnung *RD-CAP-Pass,* die Sie über das Kontextmenü als Kopie der ersten Richtlinie erstellen.
18. Gehen Sie bei dieser Richtlinie analog vor und verwenden Sie als Integritätsrichtlinie die Zugriffsrichtlinie, wenn der PC NAP-Bedingungen erfüllt und gewähren Sie diesen Clients 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).

Durch diese Richtlinien steuern Sie also, ob Clients eine Verbindung mit dem Netzwerk über das Remotedesktopgateway aufbauen können.

Ressourcenautorisierungsrichtlinien erstellen

Die Konfiguration der Richtlinie, in der definiert wird, auf welche Remotedesktopserver die Anwender zugreifen können (RD-RAP), finden Sie über den Knoten *Ressourcenautorisierungsrichtlinien* im Remotedesktopgateway-Manager.

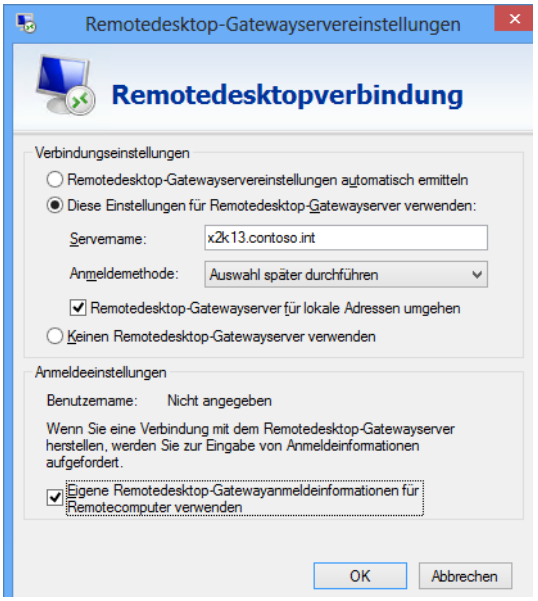
Stellen Sie hier nach der Installation sicher, ob in der entsprechenden Richtlinie die Remotedesktopserver entweder als einzelnes Computerkonto oder besser als Gruppe hinterlegt sind. Sie müssen an dieser Stelle sicher sein, dass Ihre Auswahl konsistent ist. Das heißt, dass für die Gruppen, die Sie in der RD-CAP definieren, eine RD-RAP existieren muss, die auf die entsprechende Gruppe in Active Directory verweist, in der sich die Computerkonten der Remotedesktopserver befinden.

Damit das Remotedesktopgateway funktioniert, müssen Sie darüber hinaus sicherstellen, dass der Systemdienst *Remotedesktopgateway* gestartet ist. Ohne diesen Dienst ist keine Verbindung möglich. Auch die Standardwebseite in der IIS-Verwaltung muss gestartet sein, damit der Zugriff funktioniert. Stellen Sie sicher, dass das Zertifikat für den Gatewayserver 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. Mehr zu diesem Thema lesen Sie in Kapitel 30.

Damit sich Clients über das Internet mit dem Gateway verbinden, müssen Anwender in den Optionen für den Remotedesktopclient auf der Registerkarte *Erweitert* die Schaltfläche *Einstellungen* anklicken. Anschließend können Sie Einstellungen für den Verbindungsaufbau über ein Gateway konfigurieren.

Abbildg. 28.42 Konfigurieren des Verbindungsaufbaus zu einem Remotedesktopgateway im RDP-Client



Remotedesktop-Verbindungsbroker

Der Remotedesktop-Verbindungsbroker hat die Aufgabe, Benutzer wieder mit ihren getrennten Sitzungen zu verbinden, wenn Sie die Remotedesktopdienste in einer Sammlung (in Windows Server 2008 R2 noch Farm genannt) einsetzen. Im Gegensatz zu Windows Server 2008 R2 ist der Betrieb eines Verbindungsbrokers in Windows Server 2012 R2 zwingend notwendig, nicht mehr optional. Daher müssen Sie auch einen Server als Remotedesktop-Verbindungsbroker angeben, wenn Sie eine neue Sammlung erstellen.

Beim Einsatz von Loadbalancing, also mehrerer Server in der Sammlung, speichert diese Funktion den Benutzernamen, die Sitzungs-ID und den Remotedesktopserver, auf dem der Anwender verbunden war. Damit die Benutzer wieder mit der entsprechenden Sitzung auf ihrem Remotedesktop-

server verbunden werden, müssen allerdings alle Server in der Loadbalancing-Farm unter Windows Server 2012 R2 laufen. Eine gemischte Umgebung mit Windows Server 2003 wird für diese Funktion nicht unterstützt, ein Mischbetrieb mit Windows Server 2008/2008 R2 ist auch nicht optimal.

TIPP Sie haben auch die Möglichkeit, Remotedesktop-Verbindungsbroker zusammen mit SQL Server 2008 R2/2012 hochverfügbar betreiben. Dies funktioniert auch in einer Clusterumgebung. Wie Sie dabei vorgehen, lesen Sie auf der Seite *http://blogs.msdn.com/b/rds/archive/2012/06/27/rd-connection-broker-high-availability-in-windows-server-2012.aspx* [Ms179-K28-09].

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 (siehe Kapitel 34). 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 Remotedesktopdienste sinnvoll.

HINWEIS Der Remotedesktop-Verbindungsbroker sollte nicht auf einem Remotedesktop-Sitzungshost installiert werden. Da der Remotedesktop-Verbindungsbroker auf die Network Loadbalancing (NLB)-Funktion von Windows Server 2012 R2 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 Remotedesktop-Verbindungsbroker die Benutzeranmeldungen verteilt.

Sie können leistungsfähigeren Servern mehr Benutzer zuteilen, als weniger leistungsfähigen Servern. Diese Einstellungen sind zum Beispiel in den Gruppenrichtlinien enthalten. Die entsprechenden Einstellungen finden Sie unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Remotedesktopdienste/Remotedesktopsitzungs-Host/Remotedesktop-Verbindungsbroker.*

RemoteFX – Virtual Desktop Infrastructure und Remotedesktop-Sitzungshost

Eine wichtige neue Funktion in SP1 für Windows Server 2008 R2 ist RemoteFX. Diese hat Microsoft auch in Windows Server 2012 R2 eingebaut und verbessert. Hierbei handelt es sich um eine erweiterte Funktion des Remotedesktopprotokolls (RDP), das die bessere grafische Darstellung von Windows 8.1-Desktops ermöglicht, die Sie zum Beispiel über Virtual Desktop Infrastructure (VDI) zur Verfügung stellen (siehe Kapitel 29). Sie können die Technik auch auf Remotedesktop-Sitzungshosts (Terminalserver) verwenden. Dazu muss dann auf dem Server ebenfalls Windows Server 2012 R2 installiert sein. Vor allem 3D-Grafiken, Audio und Animationen wie zum Beispiel Flash und Silverlight laufen schneller in der neuen Version.

Neben einer Verbesserung der grafischen Darstellung enthält RemoteFX eine Verbesserung der USB-Unterstützung von virtuellen Windows 8.1-Computern zur Anbindung von USB-Laufwerken, Smartphones oder Digitalkameras. Damit Sie RemoteFX nutzen können, muss auf dem Server

Windows Server 2012 R2 und auf dem virtuellen Computer Windows 8.1 installiert sein. Auf dem Clientcomputer, mit dem Sie auf den virtuellen Windows 8.1-Computer zugreifen, muss Windows 8.1 installiert sein (mehr dazu siehe Kapitel 29).

Wie diese Technik genau funktioniert, erklären die Hyper-V-Entwickler in ihrem Blog (*http://blogs.technet.com/b/virtualization/archive/2010/03/17/explaining-microsoft-remotefx.aspx* [Ms179-K28-10]). Auch ein Demovideo (*http://www.brianmadden.com/blogs/videos/archive/2010/03/18/exclusive-video-microsoft-s-tad-brockway-discusses-and-demos-remotefx.aspx* [Ms179-K28-11]) stellt Microsoft zur Verfügung. Auf der Partnerseite für RemoteFX (*http://blogs.msdn.com/b/rds/archive/2010/03/22/partners-support-microsoft-remotefx.aspx* [Ms179-K28-12]) finden Sie weiterführende Informationen.

Grundlagen und Voraussetzungen von RemoteFX

Bevor Sie RemoteFX nutzen, sollten Sie den aktuellsten Treiber für die Grafikkarte auf dem Hyper-V-Host installieren. Natürlich muss der Hyper-V-Host dazu über eine leistungsfähige Grafikkarte verfügen. Alle Berechnungen zu 3D-Grafiken und Aero nimmt der Server vor und leitet diese an den Client weiter, der die Daten nur noch anzeigen muss. RemoteFX ist kein eigenständiges Remoteprotokoll, sondern nur eine Erweiterung des Remotedesktopprotokolls (RDP). Auf der Seite *http://go.microsoft.com/fwlink/?LinkId=191918* [Ms179-K28-13] finden Sie mehr Informationen über die Hardwarevoraussetzungen für RemoteFX.

Sie können als Host für RemoteFX-Clients auch den kostenlosen Hyper-V-Server 2012 einsetzen (siehe Kapitel 7). Wollen Sie RemoteFX nicht nur für Hosted Desktops (siehe Kapitel 29), sondern auch für Sitzungen eines Remotedesktopdienste-Sitzungshost verwenden, muss auf dem Server ebenfalls Windows Server 2012 R2 installiert sein. Damit Sie RemoteFX nutzen können, muss der Prozessor Second Level Address Translation (SLAT) unterstützen (siehe Kapitel 7).

Intel verwendet hier auch die Bezeichnung *Extended Page Tables*, AMD nennt die Funktion *Nested Page Tables*. Der Grafikprozessor (GPU) muss DirectX 9.0c und DirectX 10.0 unterstützen. Verwenden Sie mehrere Grafikkarten pro Server, müssen diese identisch sein, das gilt auch für Clusterknoten in einem Hyper-V-Cluster.

Generell ist die Installation des Grafikkartentreibers vor der Installation der Serverrollen für die Remotedesktopdienste oder Hyper-V zu empfehlen. Ein Monitor für eine virtuelle Maschine (VM), den Sie für RemoteFX konfiguriert haben, wird auf dem Server genauso wie ein lokal angeschlossener Monitor behandelt. Das heißt, der Server muss den Bildaufbau berechnen. Jede Sitzung benötigt in etwa 200 MB Grafikkartenspeicher bei der Verwendung von RemoteFX (bei 1.024 x 768 etwa 75 MB, bei 1.920 x 1.200 etwa 220 MB). Betreiben Sie mehrere Monitore, verdoppelt sich nicht die Anforderung, sondern es kommen noch einmal etwa 50 bis 100 MB hinzu. Allerdings arbeiten die Karten nicht immer zusammen und können nur ihren eigenen Speicher nutzen. Sie ordnen nicht selbst die Sitzungen oder virtuellen Clients den Karten zu, sondern der Hyper-V-Host skaliert automatisch.

Wenn Sie spezielle Verwaltungsports an Servern mit einem speziellen Verwaltungsadapter auf dem Server verwenden, empfiehlt Microsoft die Installation des RemoteFX-Treibers, nachdem Sie RemoteFX auf dem Server installiert und aktiviert haben. Die Fernwartungskonsole auf Servern kann die RemoteFX-Verbindung stören. Dies liegt daran, dass diese Konsolen meist noch das alte XP-Treibermodell verwenden (XPDM).

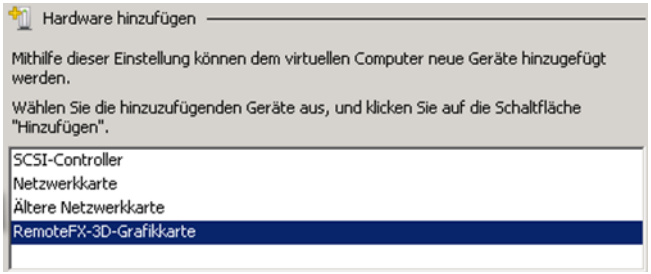
RemoteFX benötigt aber das neue Treibermodell Windows Display Driver Model (WDDM). Auf einem Server lässt sich immer nur eine Art Treiber installieren. Ist also ein XPDM-Treiber installiert, lässt sich kein WDDM-Treiber installieren. Aus diesem Grund müssen Sie solche alten Karten entweder deaktivieren oder Sie verwenden den speziellen RemoteFX-Treiber für diese Karten, falls das Gerät kompatibel ist. Den Treiber installieren Sie in der Eingabeaufforderung durch Eingabe von

```
dism /online /enable-feature /featurename:Microsoft-Windows-RemoteFX-EmbeddedVideoCap-
Setup-Package
```

Probleme bereiten können I/O-Virtualisierung (Intel VT-d, AMD-Vi und IOMMU). Diese Funktionen sollten Sie im BIOS des Servers ausschalten. Auch Intel Trusted Execution Technology (TXT) kann Probleme mit RemoteFX auslösen. Data Execution Prevention (DEP) muss auf dem Hyper-V-Host aktiv sein. AMD nennt diese Technik Enhanced Virus Protection (EVP), Intel bezeichnet sie mit *No Execution (NX)*.

Der Treiber unterstützt RemoteFX auch beim Booten des Rechners, sodass Sie auf das BIOS zugreifen können. Damit Sie RemoteFX nutzen können, müssen Sie vorher auf dem Gastssystem Windows 8.1 installiert sein. Anschließend können Sie dem virtuellen Computer eine neue Grafikkarte zuordnen, wenn Sie diesen ausgeschaltet haben. Dazu rufen Sie die Einstellungen des virtuellen Computers auf, klicken *Hardware*, wählen *RemoteFX-3D-Grafikkarte* aus und klicken auf *Hinzufügen*.

Abbildg. 28.43 Hinzufügen der RemoteFX-3D-Grafikkarte zu einem virtuellen Computer



Ist die *Funktion*-Schaltfläche deaktiviert, unterstützt die Grafikkarte oder der installierte Treiber diese Funktion nicht. Außerdem muss auf dem Server, auf dem Sie RemoteFX nutzen wollen, die Serverrolle *Remotedesktopdienste* installiert sein. Dieser enthält die notwendigen Funktionen für RemoteFX. Sie müssen diesen Rollendienst auch installieren, wenn Sie RemoteFX auf einem Remotedesktop-Sitzungshost (Terminalserver) zur Verfügung stellen wollen, nicht nur in einer VDI-Struktur (siehe Kapitel 29). Nach dem Hinzufügen haben Sie noch die Möglichkeit, die Anzahl der unterstützten Monitore sowie die Auflösung zu konfigurieren.

Ein weiterer Vorteil von RemoteFX ist die verbesserte Unterstützung von USB-Geräten auf den virtuellen Desktops. Verbinden Sie ein USB-Gerät mit dem Client, der über RDP mit dem RemoteFX-Gerät verbunden ist, installiert Windows 8.1 den Treiber. Es ist kein Treiber auf dem Client notwendig, der sich mit dem virtuellen Computer verbindet, sondern der USB-Stick ist lediglich auf dem virtuellen Windows 8.1-Client zu installieren. Diese Technik vermeidet Treiberprobleme auf den Clients und notwendige Umleitungen. Für Anwender ist die Umleitung der USB-Geräte absolut transparent.

RemoteFX produktiv einrichten und verwalten – VDI und Remotedesktop-Sitzungshost

Auf dem Client, mit dem Sie sich mit dem RemoteFX-Client auf den Hyper-V-Server verbinden, muss ebenfalls Windows 8.1 installiert sein. Auf dem Hyper-V-Server muss außerdem ein aktueller Grafikkarten-Treiber installiert sein, die Standard-VGA-Karte reicht hier nicht aus. In Notfällen können Sie auf Servern mit Windows Server 2012 R2 auch Treiber für Windows 8.1 x64 installieren. Allerdings sollten Sie in produktiven RemoteFX-Umgebungen besser auf eine optimale Grafikkarte setzen, die auch RemoteFX und Windows Server 2012 R2 optimal unterstützt. Die in Windows Server 2012 R2 enthaltenen Grafikkartentreiber unterstützen kein RemoteFX.

Abbildg. 28.44 Überprüfen des korrekten Treibers für die Grafikkarte auf dem Hyper-V-Host

Haben Sie die notwendigen Vorbereitungen getroffen, können Sie für den virtuellen Client, auf dem Sie RemoteFX zur Verfügung stellen wollen, die Funktion integrieren:

1. Starten Sie den Hyper-V-Manager (siehe Kapitel 7).
2. Schalten Sie den virtuellen Client aus.
3. Rufen Sie über das Kontextmenü die Einstellungen des virtuellen Clients auf.
4. Klicken Sie auf *Hardware hinzufügen*.
5. Wählen Sie *RemoteFX-3D-Grafikkarte* aus.
6. Klicken Sie auf *Hinzufügen*. Sie können immer nur eine RemoteFX-3D-Karte pro Client aktivieren.
7. Starten Sie den virtuellen Client.
8. Melden Sie sich am Client an.
9. Windows 8.1 installiert jetzt den Treiber im virtuellen Client für die RemoteFX-3D-Karte.
10. Starten Sie den Client neu.

Im Verbindungsfenster des Hyper-V-Managers bringt Ihnen RemoteFX nichts, Sie können nach der Installation der RemoteFX-3D-Karte auch diese Möglichkeit nicht mehr für den Verbindungsaufbau zum Client verwenden. Sie können RemoteFX nur über den Remotedesktopclient oder kompatible Thin-Clients nutzen. Damit Thin-Clients RemoteFX auf dem Hyper-V-Server nutzen können, müssen diese mindestens RDP 7.1 unterstützen.

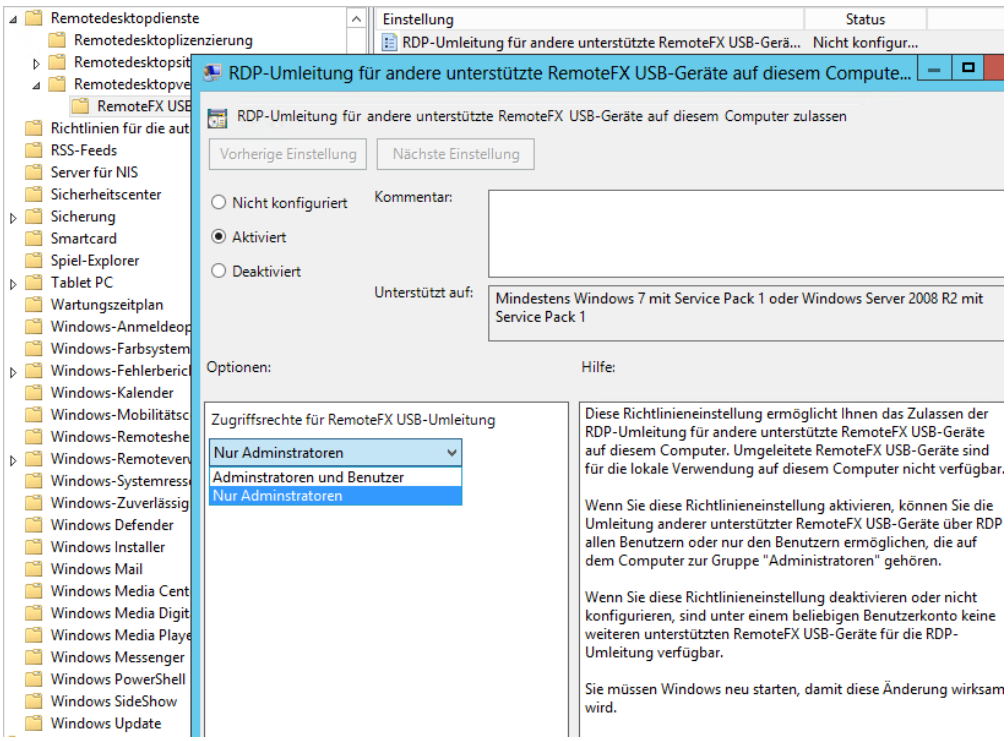
Klappt der Verbindungsaufbau über das RDP-Protokoll nicht, rufen Sie die Einstellungen des virtuellen Clients auf und klicken auf *RemoteFX-3D-Grafikkarte*. Im rechten Bereich des Fensters können Sie jetzt die Karte entfernen. Sie können Einstellungen an der Hardware aber nur vornehmen, wenn der virtuelle Client ausgeschaltet ist. Anschließend können Sie sich wieder über den Hyper-V-Manager mit dem Client verbinden.

Damit Sie die USB-Umleitung von RemoteFX auch für Sitzungen auf einem Remotedesktop-Sitzungshost nutzen können, müssen Sie noch eine Gruppenrichtlinie oder lokale Richtlinie erstellen, die auf die Remotedesktop-Sitzungshosts gebunden ist. Die entsprechende Einstellung finden Sie über die Richtlinie:

Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Remotedesktopdienste/Remotedesktopverbindungs-Client/RemoteFX-USB-Geräteumleitung

Hier finden Sie die entsprechende Einstellung, damit USB-Geräte, die Sie mit dem Client verbinden, der wiederum mit RDP-RemoteFX mit dem virtuellen Client oder der Remotedesktopsitzung verbunden ist, in die Sitzung umgeleitet werden. Haben Sie die Richtlinie aktiviert und wenden diese auf den Remotedesktop-Sitzungshost oder die virtuellen Clients an, sind alle USB-Geräte, die Sie mit dem Client verbinden, in der Sitzung verfügbar.

Abbildg. 28.45 Aktivieren der Umleitung für USB-Geräte mit RemoteFX

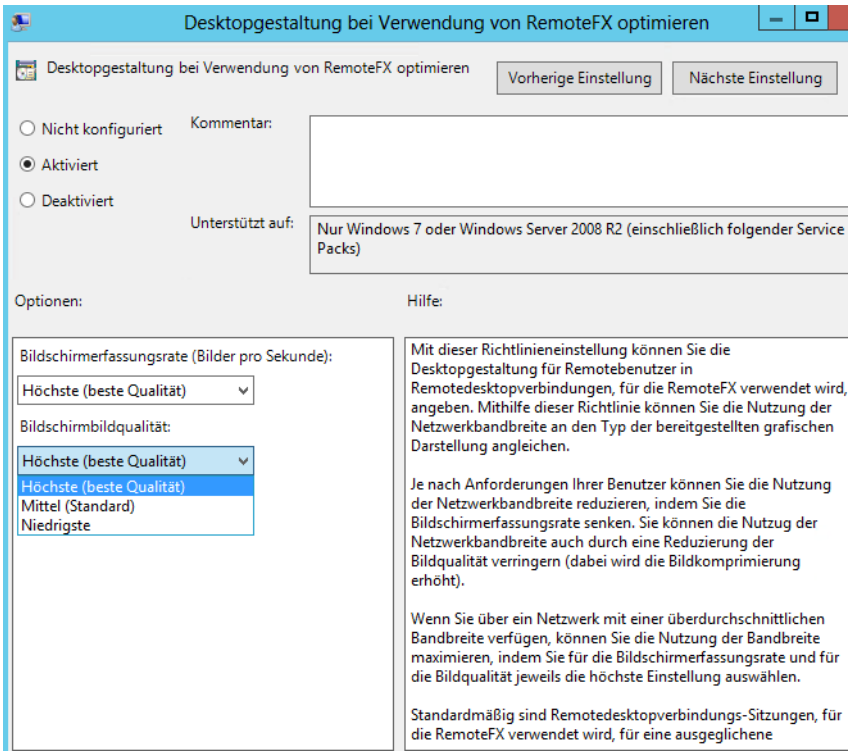


Um auf Servern, die Sie als Remotedesktop-Sitzungshosts verwenden, die optimale Leistung für RemoteFX herauszuholen, navigieren Sie noch zur Richtlinie *Computerkonfiguration/Administrative Vorlagen/Windows-Komponenten/Remotedesktopdienste/Remotedesktopsitzungs-Host/Umgebung für Remotesitzung.*

Hier können Sie verschiedene Einstellungen vornehmen, um die Oberfläche optimal anzupassen. Aktivieren Sie die Option *Desktopdarstellung bei Verwendung von RemoteFX optimieren*. Sie sollten bei den Einstellungen jeweils *Höchste Einstellung (beste Qualität)* wählen.

TIPP Auch ohne dass Sie eine RemoteFX-Karte hinzufügen, können Sie die USB-Umleitung mit RemoteFX nutzen. Sobald Sie ein Gerät mit einem Computer verbinden, der mit einer RemoteFX-Sitzung verbunden ist, erscheint in der Menüleiste oben ein neues Symbol. Über dieses lässt sich das Gerät dann in der Sitzung verwenden.

Abbildg. 28.46 Konfigurieren der Einstellung für RemoteFX



Tools für Remotedesktopserver

Für die bessere Verwaltung von Remotedesktopservern bringt Windows Server 2012 R2 bereits einige Bordmittel mit, welche einzelne Aufgaben deutlich erleichtern. Im folgenden Abschnitt gehen wir auf die wichtigsten Befehlszeilentools für die Verwaltung von Remotedesktopservern ein sowie auf Zusatztools, welche die Arbeit enorm erleichtern.

Sie können Remotedesktopserver auch in der PowerShell verwalten. Um zum Beispiel alle Server in einer Sammlung anzuzeigen, verwenden Sie den Befehl *Get-RdServer*. Sie sehen über diesen Befehl auch die Rollen, die auf den Servern installiert sind.

Abbildg. 28.47 Anzeigen der Remotedesktopserver in der PowerShell

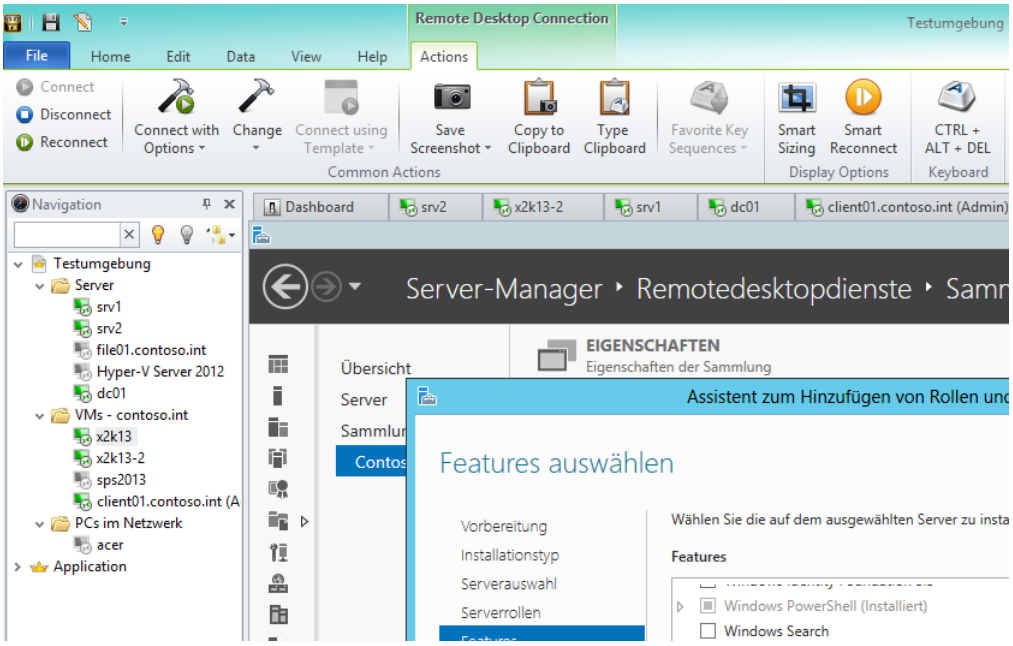
```
PS C:\Users\administrator.CONTOSO> get-rdserver

Server                                          Roles
------                                          -----
X2K13.CONTOSO.INT                               {RDS-CONNECTION-BROKER, RDS-WEB-ACCESS}
srv2.contoso.int                                {RDS-VIRTUALIZATION}
```

Um sich eine Liste der Befehle für die Verwaltung von den Remotedesktopdiensten in der PowerShell anzeigen zu lassen, verwenden Sie den Befehl *Get-Command *rd**.

Royal TS – Remotedesktops verwalten

Viele Administratoren kennen das Problem: Im Unternehmen müssen zahlreiche Server verwaltet werden und zwar meist auch noch gleichzeitig. Die Verwaltung einzelner Server findet häufig über Remotedesktop statt. Die Verwaltung der einzelnen Remotedesktop (RDP)-Verbindungen gestaltet sich leider mit Bordmitteln relativ kompliziert. Vor allem, wenn Sie mehrere Verbindungen parallel öffnen, wird die Arbeit schnell unübersichtlich.

Abbildg. 28.48 Verwalten von Remotedesktops mit Royal TS



Royal TS kann zahlreiche RDP-Verbindungen zentral verwalten. Für bis zu zehn Computer können Sie das Tool kostenlos nutzen. Zunächst laden Sie das Tool von der Internetseite *http://www.roy-alts.com/main/home/win.aspx* [Ms179-K28-14] herunter. Auf der Seite gibt es auch ein Forum, in welchem Fehler und neue Funktionen des Tools besprochen werden und der Programmierer direkt antwortet.

Der größte Nutzen ist die gemeinsame Verwaltung von mehreren Remotedesktops, die auch parallel geöffnet sein können. Administratoren können durch einen Mausklick zwischen den verschiedenen geöffneten RDP-Sitzungen wechseln. Den geöffneten Remotedesktop zeigt das Tool in der Mitte der Konsole als Vollbild an. Wem das nicht gefällt, kann einzelne Verbindungen so konfigurieren, dass sich diese in einem eigenen Fenster öffnen.

Query und Reset – Informationen für Remotedesktop-Sitzungshosts anzeigen und steuern

Mit dem Befehlszeilentool Query können Sie in der Eingabeaufforderung verschiedene Abfragen starten, um sich einen Überblick zu verschaffen, welche Prozesse zurzeit laufen und welche Benutzer angemeldet sind. Sie können sich alle Remotedesktopserver des Standorts anzeigen lassen:

- **query process** Dieser Befehl zeigt alle laufenden Prozesse auf dem Remotedesktopserver
- **query session** Mit diesem Befehl werden alle laufenden Remotedesktopsitzungen angezeigt
- **query termserver** Alle Remotedesktopserver im Subnetz werden angezeigt
- **query user** Alle auf dem Remotedesktopserver angemeldeten Benutzer werden angezeigt

Abbildg. 28.49 Informationen auf Remotedesktop-Sitzungshosts anzeigen

```
C:\Users\IEMP.CONTOSO>query process
 BENUTZERNAME          SITZUNGSNAME        ID    PID  ABBILD
>administrator         rdp-tcp#0            2   3884  taskhostex.exe
>administrator         rdp-tcp#0            2   1224  rdpclip.exe
>administrator         rdp-tcp#0            2   3452  explorer.exe
>administrator         rdp-tcp#0            2   3916  servermanage...
 administrator                              4   4996  servermanage...
 administrator                              4   3308  taskhostex.exe
 administrator                              4   4252  rdpclip.exe
 administrator                              4   4160  rdpinit.exe
 administrator                              4   2368  rdpshell.exe
>administrator         rdp-tcp#0            2    416  mmc.exe
>administrator         rdp-tcp#0            2   5020  cmd.exe
>administrator         rdp-tcp#0            2   4364  conhost.exe
>administrator         rdp-tcp#0            2   3876  query.exe
>administrator         rdp-tcp#0            2   3384  qprocess.exe
```

Mit dem Befehlszeilentool Reset können Sie anhand ihrer ID Sitzungen auf dem Remotedesktopserver zurücksetzen. Sie können zum Beispiel mit der Anweisung *query session* alle Sitzungen mit deren ID anzeigen lassen.

Im Anschluss können Sie mit *reset session <Nummer der Sitzung>* eine bestimmte Sitzung zurücksetzen. Dieser Vorgang geht oft schneller als im Server-Manager.

Abbildg. 28.50 Anzeigen und Trennen von Sitzungen

```
C:\Users\IEMP.CONTOSO>query session
 SITZUNGSNAME       BENUTZERNAME              ID  STATUS
 services                                      0  Getr.
 console                                       1  Verb.
>rdp-tcp#0          administrator               2  Aktiv
                    joost                       3  Getr.
                    Administrator               4  Getr.
 rdp-tcp                                    65536  Abhör.

C:\Users\IEMP.CONTOSO>reset session 3
```

TSCON, TSDISCON und TSKILL

Mit TSCON und TSDISCON können Remotedesktopsitzungen verbunden oder abgemeldet werden. 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.

Mit dem Parameter */dest:<Sitzungsname>* können Sie die Sitzung eines anderen Benutzers mit einer anderen Sitzung verbinden. Geben Sie im Parameter *Password* 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 Remotedesktopserver herzustellen und um die aktuelle Sitzung zu trennen.

Geben Sie *tscon 23 /password:<meinkennwort>* ein, um eine Verbindung mit Sitzung 23 auf dem aktuellen Remotedesktopserver 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.

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.

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.

Mit *TSKILL* können Sie einzelne Prozesse auf einem Remotedesktopserver 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. Die Syntax des Befehls lautet

```
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 Remotedesktopserver an, auf dem sich der zu beendende Prozess befindet. Erfolgt keine Angabe, wird der aktuelle Remotedesktopserver 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. 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 Funktionen in den Remotedesktopdiensten wie RemoteApp, das Remotedesktopgateway, den Remotedesktopdienste-Webzugriff sowie den neuen RDP-Client stellen die Remotedesktopdienste in Windows Server 2012 R2 ein mächtiges Werkzeug zur Anwendungsvirtualisierung dar. Wir haben Ihnen in diesem Kapitel ausführlich gezeigt, wie Sie einen Remotedesktopserver unter Windows Server 2012 R2 installieren und betreiben.

Im nächsten Kapitel erläutern wir Ihnen, wie Sie Desktops in Unternehmen zusammen mit Hyper-V und den Remotedesktopdiensten virtualisieren.

Kapitel 29

Virtual Desktop Infrastructure – Arbeitsstationen virtualisieren

In diesem Kapitel:

Zusammen mit Hyper-V und den Remotedesktopdiensten haben Unternehmen die Möglichkeit, virtuelle Computer auf Basis von Windows 8, aber auch Windows 7/Vista und XP Anwendern per Remotedesktop zur Verfügung zu stellen. Im Vergleich zur Arbeit mit dem Desktop auf einem Remotedesktop-Sitzungshost steht so Anwendern – wenn auch nur virtuell – ein eigener Computer zur Verfügung und beeinflussen die Arbeit anderer Benutzer nicht.

Unternehmen sind bei der Konfiguration dieser Desktops durch diese Technik wesentlich flexibler, als wenn alle Anwender mit einem Desktop der RemoteApps auf den Servern arbeiten würden. Diese virtuellen Computer lassen sich aus Kompatibilitätsgründen oder für Testzwecke bereitstellen, oder einfach, um Energie zu sparen, da leistungsfähige Computer über das Netzwerk zur Verfügung stehen.

Virtuelle Computer erstellen Sie mit Hyper-V, die Anbindung erfolgt über den Remotedesktop-Verbindungsbroker, die Konfiguration im Server-Manager und die Bereitstellung über den Webzugriff (Web Access), als RDP-Datei oder über die Startseite herkömmlicher Computer mit Windows 8. Damit Sie diese Technik, auch Virtual Desktop Infrastructure (VDI) genannt, nutzen können, benötigen Sie einen Hyper-V-fähigen Server und einen Remotedesktopserver. Unternehmen haben die Möglichkeit, Anwendern direkt auf Basis ihres Benutzerkontos einen persönlichen virtuellen Computer bereitzustellen oder einen Pool zu installieren.

Es lassen sich auch mehrere Pools bereitstellen, zum Beispiel auf Basis des Betriebssystems, der Konfiguration oder der installierten Anwendungen. Dieser Pool steht dann verschiedenen Anwendern zur Verfügung. Unabhängig davon können die Anwender mit dem Computer so arbeiten, als ob es sich um einen herkömmlichen Computer handelt. Sie können mehrere Pools, zum Beispiel mit unterschiedlichen Programmen oder Konfigurationen, erstellen und diesen Anwendern über Web Access für Remotedesktop zur Verfügung stellen. Anwender sehen ein entsprechendes Symbol in der Weboberfläche für jeden Pool und werden beim Start mit einem freien Rechner des Pools verbunden oder eben mit einem fest definierten Rechner, wenn die virtuellen Computer fest zugeteilt sind.

Arbeiten Sie mit Pools, sollten Sie Anwender darauf hinweisen, dass diese lokal keine Daten speichern sollen. Da Rechner im Pool verschiedenen Anwendern zur Verfügung stehen und es nicht festgelegt ist, mit welchem Rechner im Pool ein Anwender beim nächsten Start verbunden wird, ist ein Speichern in Netzwerkfreigaben besser. Oder Sie arbeiten alternativ mit zugewiesenen virtuellen Computern, damit jeder Benutzer seinen eigenen Rechner hat.

HINWEIS Als Betriebssystem auf virtuellen Computern in einer Virtual Desktop Infrastructure (VDI) sind nur Windows-Clientbetriebssysteme geeignet. Sie können zum Beispiel nicht Windows Server 2012 als Poolrechner zur Verfügung stellen. Mehr zu diesem Thema lesen Sie auch in Kapitel 28.

Windows 8 als virtuellen Computer in einer VDI-Struktur einsetzen

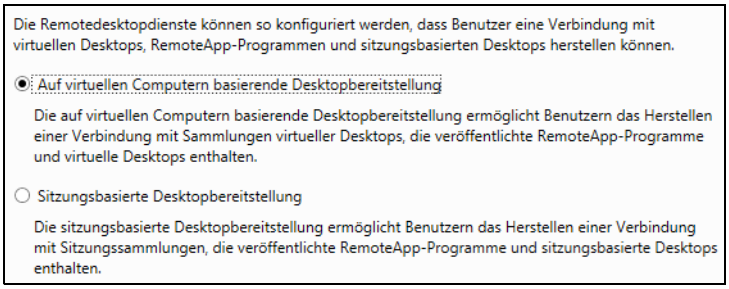
Viele Unternehmen, die bisher noch auf Windows XP setzen und auf Windows 8 aktualisieren wollen, benötigen dennoch teilweise noch Windows XP-Computer im Netzwerk für die eine oder andere Anwendung. Dazu kann eine VDI-Infrastruktur mit Windows XP nützlich sein, bei der Anwender einen eigenen PC erhalten und sich mit diesem schnell und einfach über das Startmenü oder über Web Access für Remotedesktop verbinden können.

Installieren des Remotedesktop-Sitzungshosts

Damit Sie Hyper-V mit den Remotedesktopservern verbinden können, müssen Sie auf dem Server, auf dem Sie die virtuellen Desktops installieren, den Rollendienst für Remotedesktopdienste installieren. Dabei gehen Sie vor wie in Kapitel 28 besprochen. Die Konfiguration ist in Windows Server 2012 wesentlich einfacher als noch in Windows Server 2008 R2.

Wählen Sie über den Server-Manager *Verwalten/Rollen und Features hinzufügen* und anschließend *Installation von Remotedesktopdiensten*. Auf der Seite *Bereitstellungstyp* wählen Sie *Standardbereitstellung* (siehe auch Kapitel 28). Auf der Seite *Bereitstellungsszenario auswählen* wählen Sie schließlich *Auf virtuellen Computern basierende Desktopbereitstellung* aus. Installieren Sie Remotedesktop-Sitzungshosts (ehemals Terminalserver) und wollen Anwendungen veröffentlichen oder Desktops auf den Servern (siehe Kapitel 28), wählen Sie die Option *Sitzungsbasierte Desktopbereitstellung* aus.

Abbildg. 29.1 Erstellen einer neuen VDI-Infrastruktur

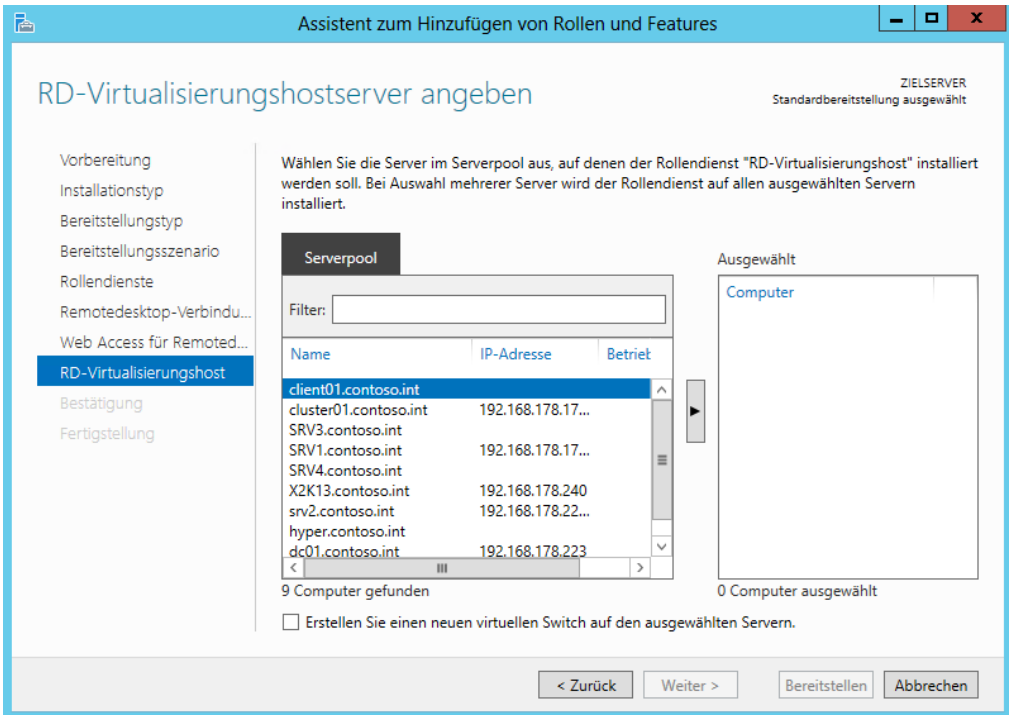


Haben Sie das Szenario ausgewählt, sehen Sie auf der nächsten Seite des Assistenten, welche Rollendienste der Assistent installiert. Auf der folgenden Seite wählen Sie, wie bei Remotedesktop-Sitzungshosts auch (siehe Kapitel 28), den Remotedesktop-Verbindungsbroker aus. Dieser stellt die Verbindung zwischen Clients und der VDI/Remotedesktopinfrastruktur zur Verfügung. Hier können Sie nur Server auswählen, die Sie zuvor im Server-Manager über *Verwalten/Server hinzufügen* angebunden haben.

Haben Sie im Netzwerk bereits eine Remotedesktopinfrastruktur installiert und ist damit bereits ein Remotedesktop-Verbindungsbroker vorhanden, erkennt das der Assistent und schlägt die Anbindung an den Verbindungsbroker vor.

Im Rahmen der Installation wählen Sie danach die Server aus, auf denen Sie virtuelle Computer zur Verfügung stellen wollen. Diese tragen die Bezeichnung RD-Virtualisierungshostserver. Die Server müssen Hyper-V 3.0 unterstützen.

Abbildg. 29.2 Festlegen des RD-Virtualisierungshostservers



Nach der Auswahl installiert der Assistent die notwendigen Rollendienste auf allen ausgewählten Servern und startet die Server bei Bedarf neu. Sie erhalten eine Zusammenfassung angezeigt, welche Rollendienste der Assistent auf den verschiedenen Servern installiert.

Abbildg. 29.3 Bestätigen der Serverrollen für die VDI-Infrastruktur

Nachdem Sie die Installation abgeschlossen haben, verwalten Sie die VDI-Infrastruktur im Server-Manager genauso wie die Remotedesktopdienste. Sie finden die Konfiguration über *Remotedesktopdienste*. Wie bei der Verwendung von Remotedesktop-Sitzungshosts (siehe Kapitel 28) erstellen Sie auch bei der Virtualisierung von Desktops eine neue Sammlung. Diese trägt die Bezeichnung *Sammlung virtueller Desktops erstellen*.

In den Remotedesktopdiensten sind zwei Arten virtueller Desktopsammlungen verfügbar: persönliche und im Pool zusammengefasste Sammlungen. Sie können im Pool zusammengefasste virtuelle Desktops automatisch in einer Sammlung durch Remotedesktopdienste verwalten lassen oder sie manuell verwalten.

Eine verwaltete, im Pool zusammengefasste Sammlung virtueller Desktops bietet das automatische Erstellen von im Pool zusammengefassten virtuellen Desktops auf Basis einer virtuellen Desktopvorlage. Auch automatisches Installieren von Sicherheitsupdates und Anwendungen auf Basis einer virtuellen Desktopvorlage sind möglich.

Auf einem Benutzerprofildatenträger werden Benutzerprofilinformationen auf einer separaten virtuellen Festplatte gespeichert, sodass die Benutzerprofileinstellungen über in Pools zusammengefasste virtuelle Desktops verfügbar bleiben.

Beim Erstellen der virtuellen Desktopsammlung müssen Sie bei dem Computer mit einem Benutzerkonto mit der Berechtigung zum Hinzufügen von Computern zur Domäne angemeldet sein. Die virtuelle Desktopvorlage für Computer im Pool muss als virtueller Hyper-V-Computer hinzugefügt werden. Der virtuelle Computer muss mit Sysprep generalisiert und heruntergefahren werden. Sie müssen die virtuelle Desktopvorlage zu Hyper-V hinzufügen, damit Sie sie der im Pool zusammengefassten Sammlung virtueller Desktops zuweisen können. Wie Sie dabei vorgehen, lesen Sie in den nächsten Abschnitten.

Virtuelle Computer installieren und für VDI vorbereiten

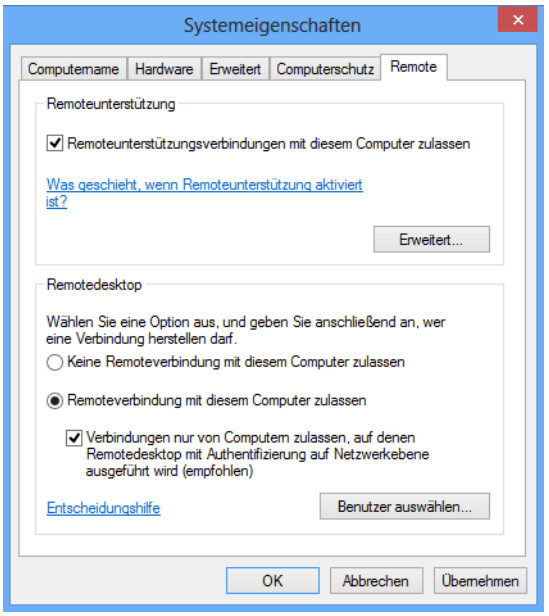
Im nächsten Schritt installieren Sie virtuelle Computer, die Sie als Vorlage für den Pool verwenden wollen, auf dem RD-Virtualisierungshosts. Möchten Sie die virtuellen Computer in einem Pool bereitstellen, können Sie Windows 8 installieren, aber auch Windows Vista und Windows XP funktionieren. Nehmen Sie die Computer in die Domäne auf und bereiten Sie den Computer mit dem Befehlszeilentool Sysprep vor.

Neben der Anbindung an die Domäne müssen Sie bei der Installation zunächst nichts beachten. Nach der Installation, Aktivierung und Anbindung an die Domäne sind auf den Computern noch einige Vorbereitungen zu treffen, damit diese optimal in einem VDI-Pool funktionieren.

Remotedesktop auf Clientcomputern aktivieren und konfigurieren

Im ersten Schritt aktivieren Sie Remotedesktop auf den Clientcomputern. Sie finden die Einstellung, wenn Sie die *Eigenschaften* von *Computer* aufrufen (⊞+Pause) und auf den Link *Remoteeinstellungen* klicken. Aktivieren Sie den Remotedesktop mit der Option, dass nur sichere Verbindungen erlaubt sind.

Abbildg. 29.4 Aktivieren des Remotedesktops in Windows 8



Zusätzlich müssen Sie noch festlegen, welche Benutzer über den Remotedesktop auf den virtuellen Computer zugreifen dürfen. Klicken Sie dazu auf die Schaltfläche *Benutzer auswählen* oder rufen Sie über *lusrmgr.msc* den lokalen Benutzer-Manager des Computers auf.

Standardmäßig dürfen per Remotedesktop *Administratoren* und Mitglieder der lokalen Gruppe *Remotedesktopbenutzer* zugreifen, das Gleiche gilt auch für Server. Entweder nehmen Sie die einzelnen Benutzerkonten aus der Domäne in die lokale Gruppe *Remotedesktopbenutzer* auf oder Sie erstellen eine Gruppe in der Domäne und nehmen diese in die lokale Gruppe *Remotedesktopbenutzer* auf.

Die einzelnen Benutzerkonten nehmen Sie dann nur noch in die Gruppe in der Domäne auf. So ist sichergestellt, dass alle berechtigten Anwender per RDP auf die Rechner im VDI-Pool zugreifen dürfen und Sie nur Mitgliedschaften konfigurieren müssen.

Remote RPC-Zugriff auf Clientcomputern erlauben

Damit sich die Clients optimal an die VDI-Infrastruktur anbinden, sollten Sie mit Adminrechten auf den Clientcomputern noch den Registrierungs-Editor durch Eintippen von *regedit* auf der Startseite öffnen:

1. Navigieren Sie zum Schlüssel *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer*.
2. Klicken Sie doppelt auf den Wert *AllowRemoteRPC* und geben Sie den Wert *1* ein.

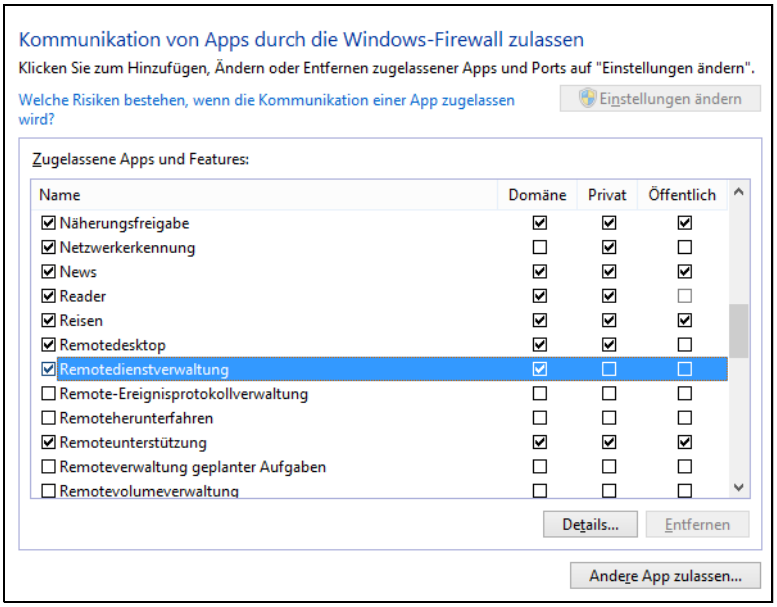
Firewalleinstellungen auf Clientcomputern konfigurieren

Im nächsten Schritt müssen Sie auf den Clientcomputern noch die Firewalleinstellungen anpassen:

1. Öffnen Sie über das Schnellmenü (+ X) die Systemsteuerung.

2. Navigieren Sie zu *System und Sicherheit/Windows-Firewall*.
3. Klicken Sie auf *Eine App oder Feature durch die Firewall kommunizieren lassen*.
4. Aktivieren Sie *Remotedienstverwaltung*.

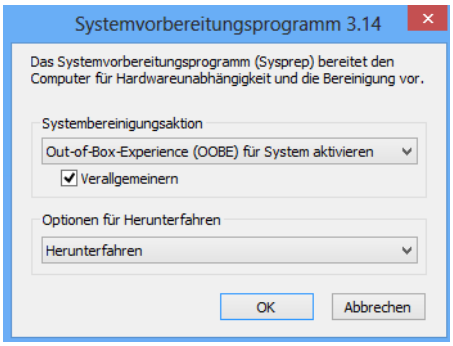
Abbildg. 29.5 Aktivieren der Remotedienstverwaltung in der Windows 8-Firewall



System mit Sysprep vorbereiten

Damit Sie den vorbereiteten Computer als Vorlage für einen virtuellen Desktoppool verwenden können, müssen Sie ihn mit dem Befehlszeilentool Sysprep vorbereiten. Sie finden dieses im Ordner *C:\Windows\System32\Sysprep*. Starten Sie das Tool über dessen Kontextmenü mit Administratorrechten. Wählen Sie *Out-of-Box-Experience (OOBE) für System aktivieren*, *Verallgemeinern* und *Herunterfahren* aus.

Abbildg. 29.6 Vorbereiten einer Vorlage für einen virtuellen Desktop



Konfigurieren des virtuellen Desktop-Pools

Nachdem Sie die Clients vorbereitet haben, können Sie fortfahren, den Pool zu generieren und an die Umgebung anzubinden. Erstellen Sie die verwaltete, in einem Pool zusammengefasste Sammlung virtueller Desktops, damit Benutzer eine Verbindung zu den Desktops in der Sammlung herstellen können.

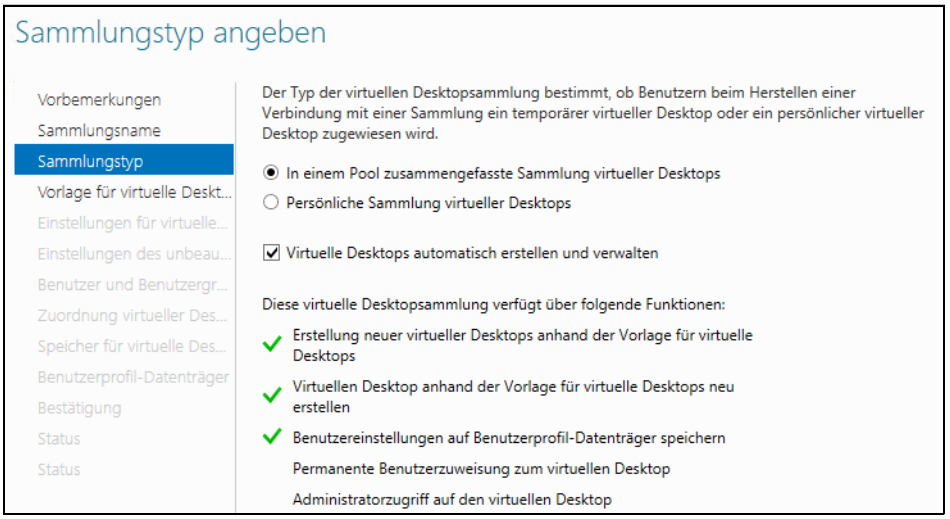
HINWEIS Die Verwaltung der Sammlungen für virtuelle Desktops entspricht weitgehend der Verwaltung von Sammlungen für RemoteApps und Remotedesktop-Sitzungshosts. Lesen Sie sich daher zur Verwaltung einer VDI-Infrastruktur auch das Kapitel 28 durch.

Sammlung virtueller Pools im Server-Manager erstellen

Um eine Sammlung für virtuelle Pools zu erstellen, gehen Sie folgendermaßen vor:

1. Klicken Sie im linken Bereich auf *Remotedesktopdienste* und anschließend auf *Sammlungen*.
2. Klicken Sie auf *Aufgaben* und dann auf *Sammlung virtueller Desktops erstellen*.
3. Klicken Sie auf der Seite *Vorbemerkungen* auf *Weiter*.
4. Tippen Sie auf der Seite *Namen für die Sammlung angeben* im Feld *Name* eine Bezeichnung für die Sammlung ein.
5. Klicken Sie auf der Seite *Sammlungstyp angeben* auf die Option *In einem Pool zusammengefasste Sammlung virtueller Desktops*. Stellen Sie sicher, dass das Kontrollkästchen *Virtuelle Desktops automatisch erstellen und verwalten* aktiviert ist, und klicken Sie dann auf *Weiter*.

Abbildg. 29.7 Erstellen einer neuen Sammlung auf Grundlage einer Desktopsammlung

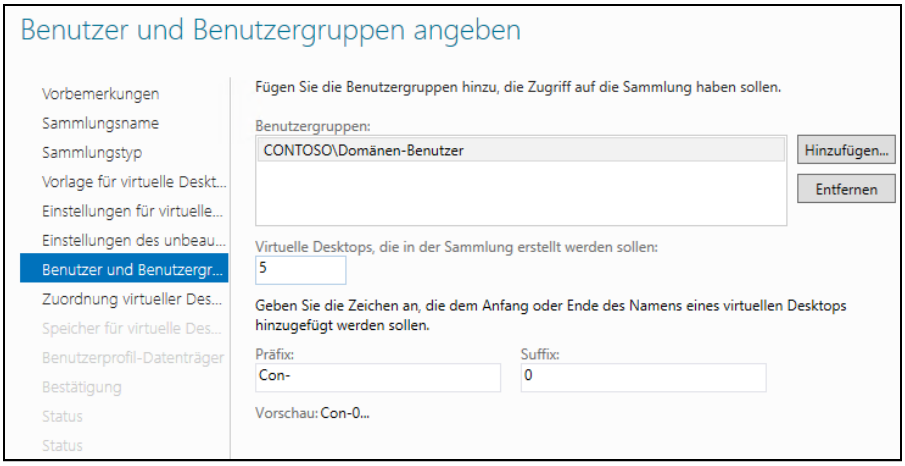


6. Klicken Sie auf der Seite *Vorlage für virtuelle Desktops angeben* auf den Computer, den Windows Server 2012 als Vorlage verwenden soll. Wie Sie virtuelle Computer erstellen, lesen Sie in Kapitel 7

und in den vorherigen Abschnitten. Der virtuelle Computer, den Sie als Vorlage verwenden, muss im Hyper-V-Manager erstellt worden und ausgeschaltet sein.

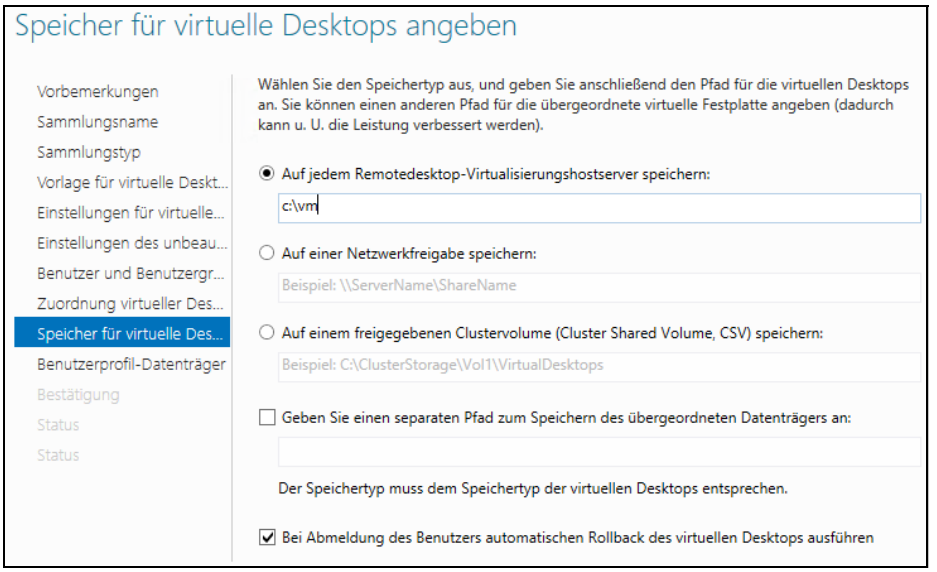
7. Klicken Sie auf der Seite *Einstellungen für virtuelle Desktops angeben* auf *Einstellungen für die unbeaufsichtigte Installation angeben* und klicken Sie dann auf *Weiter*. In diesem Schritt des Assistenten können Sie auch eine Antwortdatei hinterlegen. Weitere Informationen finden Sie auf der Microsoft TechNet-Website *http://technet.microsoft.com/library/cc749317(WS.10).aspx* [Ms179-K29-01].
8. Geben Sie auf der Seite *Einstellungen des unbeaufsichtigten Modus angeben* die folgenden Informationen ein, behalten Sie die Standardeinstellungen für nicht angegebene Optionen bei, und klicken Sie dann auf *Weiter*.
9. Klicken Sie im Feld *Zeitzone* auf die Ihrem Standort entsprechende Zeitzone.
10. Legen Sie fest, in welcher Organisationseinheit die Computerkonten abgelegt werden sollen.
11. Wählen Sie aus, welche Benutzer Zugriff auf die virtuellen Desktops erhalten dürfen. Außerdem können Sie festlegen, wie viele virtuelle Desktops der Assistent vorbereiten soll und wie die Namen der Computer aufgebaut sein sollen.

Abbildg. 29.8 Festlegen der Benutzerberechtigungen für virtuelle Desktops



12. Wählen Sie aus, wie viele virtuelle Desktops Sie auf den einzelnen RD-Virtualisierungshosts erstellen wollen.
13. Als Nächstes können Sie steuern, wo Sie die Dateien der virtuellen Computer speichern wollen. Sie können an dieser Stelle auf jedem Host, in einer Netzwerkfreigabe oder in einem CSV-Clusterlaufwerk die Dateien speichern lassen (siehe Kapitel 9).
14. Geben Sie auf der Seite *Benutzerprofil-Datenträger angeben* im Feld *Speicherort von Benutzerprofil-Datenträgern* eine entsprechende Freigabe an und klicken Sie dann auf *Weiter*. Stellen Sie sicher, dass die Computerkonten auf dem RD-Virtualisierungshost über Lese- und Schreibrechte für diesen Speicherort verfügen. In diesem Fall lassen sich die Daten der Anwender auf die Freigabe auslagern.
15. Klicken Sie auf der Seite *Auswahl bestätigen* auf *Erstellen*. Anschließend exportiert der Assistent den virtuellen Computer auf dem RD-Virtualisierungshost und importiert die virtuellen Computer in die RD-Infrastruktur. Sie sehen die Vorgänge auch im Hyper-V-Manager.

Abbildg. 29.9 Festlegen des Speicherorts der virtuellen Desktops



Desktop testen und verwenden

Zur Überprüfung, ob die verwaltete, im Pool zusammengefasste Sammlung virtueller Desktops erfolgreich erstellt wurde, bauen Sie zunächst eine Verbindung zum Server mit Web Access für Remotedesktop auf. Hier gehen Sie vor wie im Kapitel 28 beschrieben. Die Adresse ist normalerweise *https://<Servername>/rdweb*.

Wenn Sie eine Verbindung zwischen einem Server und einer Website eines Servers mit Web Access für Remotedesktop herzustellen wollen, müssen Sie im Server-Manager die verstärkte Sicherheitskonfiguration für Internet Explorer deaktivieren (siehe Kapitel 3).

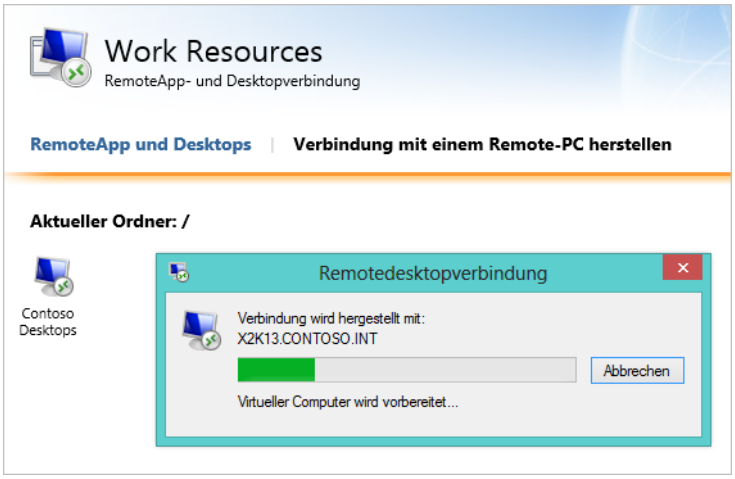
Um den Pool zu testen, melden Sie sich mit dem Benutzerkonto an Web Access für Remotedesktop an, welches Sie berechtigt haben, RDP-Sitzungen auf den Clients zu öffnen. Klicken Sie auf das Symbol, das den virtuellen Desktoppool darstellt, und melden Sie sich an.

Unter Umständen müssen Sie erneut eine Authentifizierung für den Computer durchführen, wenn der zugreifende Computer zum Beispiel über das Internet zugreift oder kein Mitglied der Domäne ist. Anschließend baut sich die RDP-Sitzung zu einem der freien Rechner im Pool auf. Die Anwender müssen dazu nicht wissen, welcher Rechner das ist, sondern werden automatisch weitergeleitet und können mit der RDP-Sitzung auf dem Computer arbeiten.

TIPP Haben Sie RemoteApps über die Startseite an Windows 8-Clients verteilt (siehe Kapitel 28), finden Anwender auch auf der Startseite eine Verknüpfung zu den Rechnern im virtuellen Pool.

Das gilt auch, wenn Sie einem Anwender einen persönlichen Desktop zur Verfügung stellen. Über den gleichen Weg wie die Verteilung der RemoteApps stellen Sie auch virtuelle Clients als Desktop zur Verfügung. Sie müssen dazu alle Schritte der vorangegangenen Abschnitte durchführen sowie die Schritte, die wir Ihnen im Abschnitt zu den RemoteApps in Kapitel 28 zeigen.

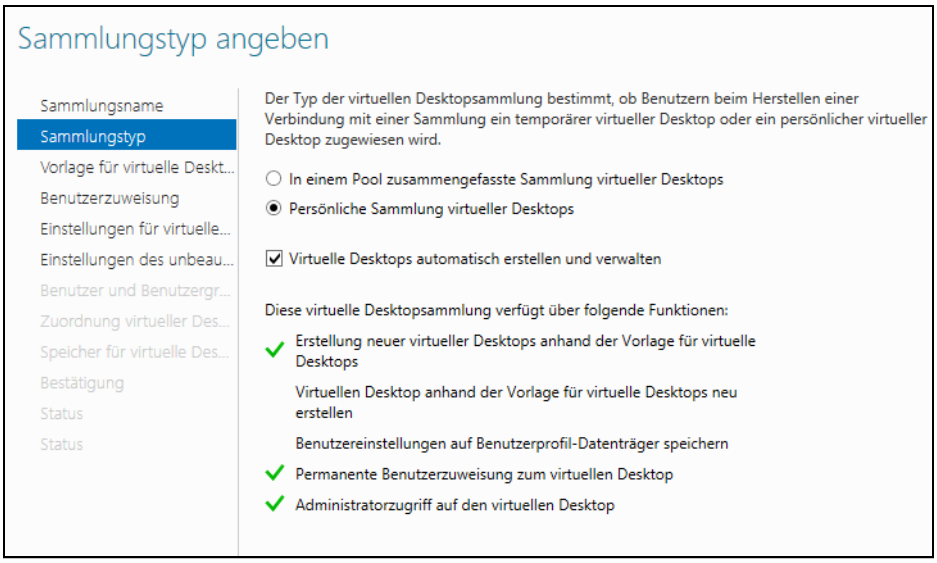
Abbildg. 29.10 Auf virtuelle Desktops über Web Access für Remotedesktop zugreifen



Personalisierte virtuelle Rechner verwenden

Wollen Sie einzelnen Anwendern keinen Rechner aus einem Pool zur Verfügung stellen oder zusätzlich noch einen virtuellen Rechner, den Sie persönlich dem jeweiligen Anwender zuweisen, gehen Sie bei der Einrichtung generell fast identisch vor. Sie wählen in diesem Fall auf der Seite *Sammlungstyp* aber die Option *Persönliche Sammlung von Desktops* aus.

Abbildg. 29.11 Erstellen persönlicher Desktops



Deaktivieren Sie auf Wunsch das Kontrollkästchen *Virtuelle Desktops automatisch erstellen und verwalten* und klicken Sie dann auf *Weiter*.

Klicken Sie auf der Seite *Vorhandene virtuelle Desktops angeben* auf den Namen des virtuellen Desktops und klicken Sie dann auf *Hinzufügen*.

Eigenes Hintergrundbild für gehostete Desktops aktivieren

Viele Unternehmen wollen Anwendern ein festes Hintergrundbild zuweisen, wenn diese mit einem virtuellen Computer arbeiten. Dazu arbeiten Sie am besten mit Gruppenrichtlinien. Legen Sie die Computerkonten der virtuellen Computer in eine eigene Organisationseinheit (OU) und konfigurieren auf dieser OU eine Gruppenrichtlinie.

Da das Hintergrundbild, wie viele Einstellungen, eine benutzerspezifische Einstellung ist, müssen Sie zunächst eine Einstellung festlegen, dass das Hintergrundbild für Computer fest vorgegeben wird. Mit der Richtlinie *Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie* im Bereich *Computerkonfiguration/Richtlinie/Administrative Vorlagen/System/Gruppenrichtlinie* legen Sie fest, dass Einstellungen von Benutzern auf alle Computer angewendet werden. Mehr zu diesem Thema lesen Sie auch in Kapitel 29.

Aktivieren Sie die Richtlinie, können Sie als Option entweder *Ersetzen* oder *Zusammenführen* wählen. Wählen Sie *Ersetzen*, dann ersetzt die Richtlinie alle Einstellungen, die auf Benutzer festgelegt sind, auch aus anderen Richtlinien. Wählen Sie *Zusammenführen*, verwendet die Richtlinie alle Einstellungen. Bei Konflikten verwendet Windows Server 2012 die Richtlinie, für die Sie den Loopverarbeitungsmodus aktiviert haben. Anschließend können Sie das Hintergrundbild aktivieren. Die Einstellung für Hintergrundbilder finden Sie bei *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen/Desktop/Desktop* in der Richtlinie *Desktophintergrund*.

Zusammenfassung

In diesem Kapitel haben wir Ihnen erläutert, wie Sie neben der Sitzungs-Virtualisierung mit Remotedesktop-Sitzungshosts auch virtuelle Computer über die Remotedesktopdienste zur Verfügung stellen. Dazu arbeiten in Windows Server 2012 die Remotedesktopdienste noch enger mit Hyper-V zusammen.

Im nächsten Kapitel zeigen wir Ihnen in der Praxis, wie Sie Zertifikate mit einer Active Directory-Zertifizierungsstelle zur Verfügung stellen.

Teil H

Sicherheit und Überwachung

Kapitel 30

Active Directory-Zertifikatdienste

In diesem Kapitel:

Der Einsatz einer interne Zertifizierungsstelle ist in Active Directory nahezu unerlässlich. Viele aktuelle Serversysteme von Microsoft oder auch Drittanbietern benötigen Zertifikate für den Zugriff. Beispiel dafür ist Exchange Server 2007/2010/2013 oder auch SharePoint 2010/2013. Auch SQL Server 2012 benötigt ein Zertifikat, wenn Sie Verbindungen verschlüsseln wollen. Die Installation und der Betrieb einer solchen Zertifizierungsstelle ist nicht sehr kompliziert, benötigt aber etwas Planung und Grundwissen, um Zertifikate optimal abrufen zu können.

HINWEIS Da die Standard-Edition von Windows Server 2012 die gleichen Funktionen und Serverrollen unterstützt wie Windows Server 2012 Datacenter Edition, können Sie alle verfügbaren Funktionen der Active Directory-Zertifikatdienste auch auf Servern mit Windows Server 2012 Standard Edition betreiben.

Außerdem unterstützen alle Funktionen der Active Directory-Zertifikatdienste vollständig Core-Installationen von Windows Server 2012 (siehe die Kapitel 2, 3 und 4).

Für die Veröffentlichung von Outlook Web Access, Outlook Anywhere und Exchange ActiveSync (EAS) sind ebenfalls oft eigene Zertifikate notwendig. In Zusammenhang mit einem ISA-Server oder dessen Nachfolger dem Forefront Threat Management Gateway ist der Einsatz sinnvoll. Dies gilt auch beim Einsatz des Netzwerkzugriffschutzes. Mit den Webdiensten für die Zertifikatregistrierung und den Zertifikatregistrierungsrichtlinien können Sie Zertifikate über HTTP auch für verschiedene Gesamtstrukturen zur Verfügung stellen. So lassen sich Zertifizierungsstellen mit mehreren Gesamtstrukturen betreiben.

TIPP Eine Übersicht der Active Directory-Zertifikatdienste (AD CS) finden Sie auf der Seite *http://go.microsoft.com/fwlink/p/?LinkId=242237* [Ms179-K30-01]. Die neuen Cmdlets zur Verwaltung von AD CS in der PowerShell finden Sie auf den folgenden Seiten:

- *http://go.microsoft.com/fwlink/p/?LinkID=242169* [Ms179-K30-02]
- *http://go.microsoft.com/fwlink/p/?LinkID=242165* [Ms179-K30-03]

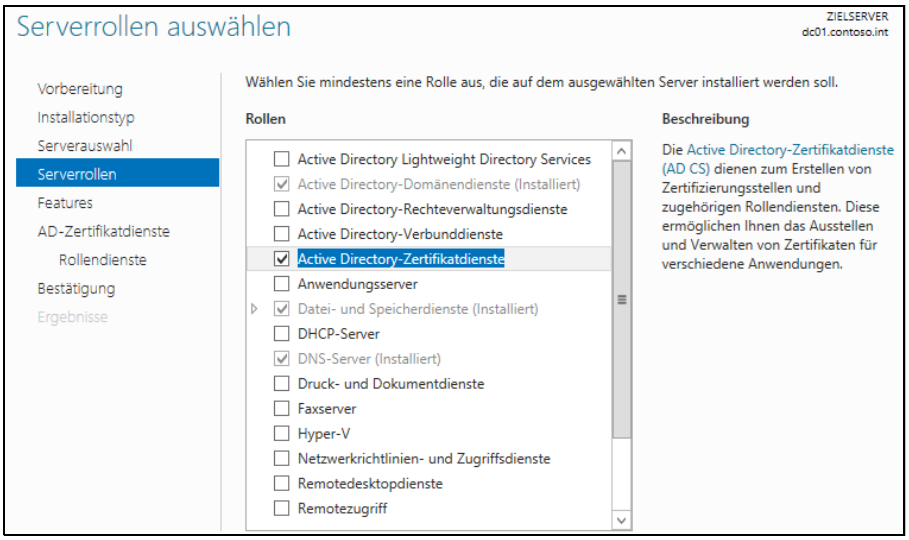
Installation einer Windows Server 2012-Zertifizierungsstelle

Installieren Sie die Zertifizierungsstelle entweder auf einem Domänencontroller oder einem anderen Server im Netzwerk. Entfernen Sie allerdings den Server, der die Zertifizierungsstelle verwaltet, aus der Domäne, verlieren die Zertifikate ihre Gültigkeit.

Serverrolle für Active Directory-Zertifikatdienste installieren

Die Installation führen Sie über das Hinzufügen der Rolle *Active Directory-Zertifikatdienste* im Server-Manager durch. Wählen Sie diese Rolle aus, können Sie die Zertifikatdienste mit einem Assistenten installieren, über den Sie verschiedene Auswahlmöglichkeiten haben.

Abbildg. 30.1 Installieren der Active Directory-Zertifikatdienste

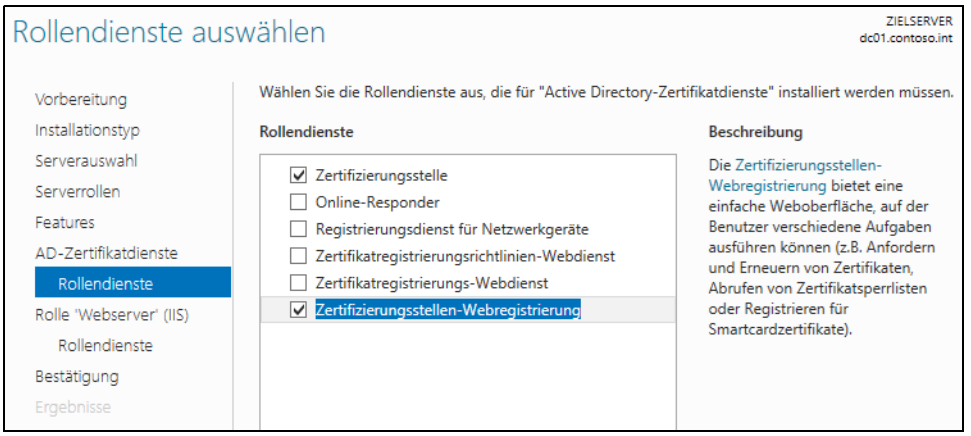


Insgesamt können Sie bei der Installation unter sechs Rollentypen auswählen:

- **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.
- **Online-Responder** Dieser Rollendienst stellt die Funktion zur Verfügung, über die den Clients erweiterte Informationen über den aktuellen Zustand der Zertifikatsabfrage gegeben werden. Der Dienst setzt die Installation des IIS voraus. Es wird ein neues Web mit der Adresse *http://<Servername>/ocsp* erstellt.
- **Registrierungsdienst für Netzwerkgeräte** Diese Funktion kann nur alleine installiert werden, nicht zusammen mit einer Zertifizierungsstelle. Mit diesem Rollendienst wird die Funktion zum automatischen Ausstellen von Zertifikaten an Netzwerkgeräte ermöglicht.
- **Zertifikatregistrierungsrichtlinie-Webdienst** Diesen Dienst benötigen Sie, wenn Sie eine richtlinienbasierte Zertifikatregistrierung ermöglichen, der Clientcomputer jedoch kein Mitglied einer Domäne ist. Der Webdienst verwendet HTTPS, um Informationen zur Zertifikatrichtlinie an Computer weiterzuleiten. Sie benötigen diesen Dienst nicht im Zusammenhang mit SharePoint.
- **Zertifikatregistrierungs-Webdienst** Stellt einen Webdienst zur Verfügung, der Clients eine Aktualisierung der Zertifikate erlaubt, ohne dass die Computer Mitglied einer Domäne sein müssen
- **Zertifizierungsstellen-Webregistrierung** Wird dieser Rollendienst installiert, können auch Zertifikate über die Webadresse *http://<Servername>/certsrv* angefordert werden. Hierbei handelt es sich um die Webschnittstelle der Zertifikatdienste.

Sie sollten die Rollendienste *Zertifizierungsstelle* und *Zertifizierungsstellen-Webregistrierung* auswählen. Der Rollendienst *Zertifizierungsstellen-Webregistrierung* stellt die Weboberfläche der Zertifikatdienste zur Verfügung, die Sie über *http://<Servername>/certsrv* aufrufen können, um Zertifikate anzufordern.

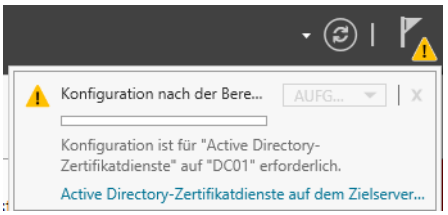
Abbildg. 30.2 Auswählen der Rollendienste für die Zertifizierungsstelle



Zertifizierungsstelle einrichten

Im Gegensatz zu Windows Server 2008 R2 nehmen Sie keine Einstellungen bezüglich der Zertifizierungsstelle während der Installation vor. Wie bei der Installation von Active Directory starten Sie nach der Installation der Serverrolle für die Zertifizierungsstelle den Einrichtungs-Assistenten über das Wartungssymbol im Server-Manager.

Abbildg. 30.3 Einrichten der Zertifizierungsstelle nach der Installation



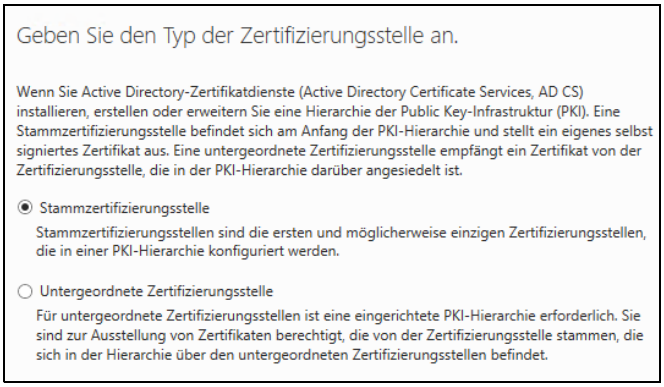
Nach dem Start des Assistenten geben Sie den Benutzernamen ein, mit dem Sie den Dienst einrichten wollen. Standardmäßig übernimmt der Assistent den Benutzer, mit dem Sie am Server angemeldet sind. Als Nächstes wählen Sie aus, welche Rollendienste Sie konfigurieren wollen. Nicht installierte Rollendienste sind deaktiviert.

Auf der nächsten Seite legen Sie den Setuptyp fest. Hier sollten Sie die Option *Unternehmenszertifizierungsstelle* auswählen, da Sie bei der ersten CA eine Root-CA installieren. Bei dieser Auswahl wird auch die CA in Active Directory integriert. Dadurch verteilt die Zertifizierungsstelle das Zertifikat der Zertifizierungsstelle auf allen Servern und Clientcomputern im Netzwerk.

Abbildg. 30.4 Auswählen des Installationstyps der Zertifizierungsstelle

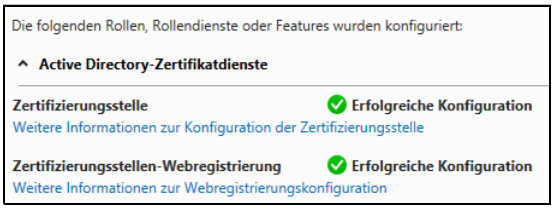
Auf der nächsten Seite des Assistenten legen Sie den Zertifizierungsstellentyp fest. Hier sollten Sie bei der ersten Installation möglichst eine *Stammzertifizierungsstelle* auswählen.

Abbildg. 30.5 Auswählen 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. Auf der nächsten Seite des Assistenten wählen Sie aus, mit welcher Verschlüsselung Sie Zertifikate ausstellen wollen. Hier sollten Sie möglichst den Standard belassen.

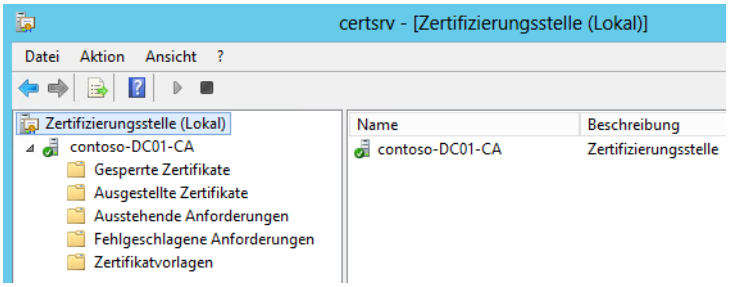
Abbildg. 30.6 Erfolgreiche Konfiguration der Zertifizierungsstelle



Über die folgende Seite legen Sie den Namen für die neue Zertifizierungsstelle fest. Hier sollten sie bei der ersten Stammzertifizierungsstelle im Unternehmen einen passenden Namen wählen. Im Anschluss bestimmen Sie die Gültigkeitsdauer für die Zertifikate und schließen die Konfiguration ab.

Nach der Installation können Sie über das Verwaltungsprogramm *Zertifizierungsstelle* im Menü *Tools* des Server-Managers überprüfen, ob die Installation erfolgreich war. Der Server sollte mit einem grünen Häkchen in der Verwaltungsoberfläche angezeigt werden.

Abbildg. 30.7 Verwalten der Zertifizierungsstelle

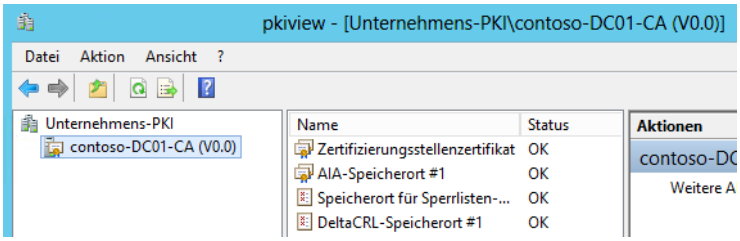


Haben Sie bei der Installation noch den Rollendienst *Zertifizierungsstellen-Webregistrierung* ausgewählt, steht zusätzlich noch die Weboberfläche der Zertifizierungsstelle über den Link *http://<Servername>/certsrv* zur Verfügung. Diese Webseite sollte sich nach erfolgter Authentifizierung fehlerfrei öffnen lassen.

Abbildg. 30.8 Aufrufen der Webseite einer neu installierten Zertifizierungsstelle

Zusätzlich gibt es das Zusatztool Pkiview, mit dem sehr schnell der allgemeine Zustand der Zertifizierungsstelle überprüft werden kann. Findet das Tool Fehler, werden diese in einer Konsole angezeigt. Das Tool starten Sie am schnellsten durch Eingabe von *pkiview* in einer Eingabeaufforderung.

Abbildg. 30.9 Überprüfen des Status einer Zertifizierungsstelle



Alle Mitgliedcomputer einer Domäne vertrauen einer internen Stammzertifizierungsstelle mit dem Typ *Unternehmen* automatisch. Das Zertifikat dieser Zertifizierungsstelle wird dazu auf den Clientcomputern und Mitgliedsservern in den Zertifikatspeicher 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 *Users*.

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. Auf dem gleichen Weg lassen sich auch Daten wiederherstellen.

Eigenständige Zertifizierungsstellen

Eigenständige Zertifizierungsstellen werden dazu verwendet, S/MIME oder SSL-Zertifikate auszustellen, wenn keine Active Directory-Unterstützung benötigt wird. 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 Active Directory gelesen werden können. Administratoren müssen außerdem jede Anfrage manuell genehmigen.

TIPP Installieren Sie eine eigenständige Zertifizierungsstelle auf einem Domänencontroller, erhalten wie bei der Unternehmenszertifizierungsstelle alle Mitgliedscomputer 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.

Installieren einer untergeordneten Zertifizierungsstelle

Während der Einrichtung der Zertifikatdienste wählen Sie aus, ob Sie eine untergeordnete Zertifizierungsstelle einrichten wollen. 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.

Zuweisen und Installieren von Zertifikaten

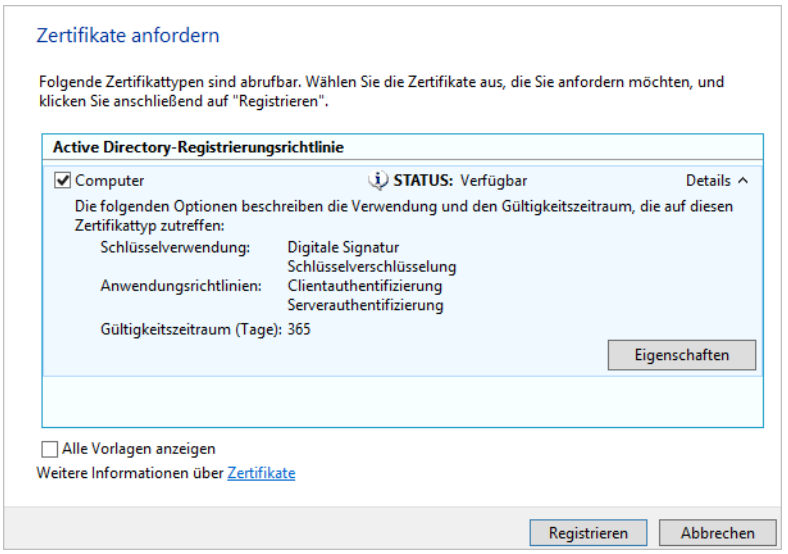
In diesem Abschnitt zeigen wir Ihnen, wie Sie von einem Computer ein Zertifikat von einer Zertifizierungsstelle anfordern und installieren. Generell können Sie bei der Zuweisung eines Zertifikats auch den Weg über die lokale Verwaltung der Zertifikate gehen. Die Zuweisung über die Weboberfläche der Zertifikatdienste funktioniert ebenso zuverlässig. Wir zeigen Ihnen nachfolgend die verschiedenen Möglichkeiten, die Sie zum Abrufen von Zertifikaten haben.

Zertifikate mit Assistenten aufrufen

In der lokalen Verwaltung von Zertifikaten können Sie in Active Directory auch Zertifikate auf einem Server installieren. Dazu gehen Sie folgendermaßen vor:

1. Starten Sie durch Eingabe von *certlm.msc* auf der Startseite die Verwaltung der lokalen Zertifikate.
2. Klicken Sie mit der rechten Maustaste auf *Zertifikate* und wählen Sie dann *Alle Aufgaben/Neues Zertifikat anfordern*.

Abbildg. 30.10 Registrieren eines neuen Zertifikats



3. Bestätigen Sie auf der nächsten Seite die Option *Active Directory-Registrierungsrichtlinie*.
4. Aktivieren Sie auf der folgenden Seite die Option *Computer* und klicken Sie auf *Registrieren*. Das Zertifikat erscheint anschließend in der Konsole und lässt sich nutzen.

Zertifikate im IIS-Manager abrufen

Sie können SSL auf Webservern, zum Beispiel SharePoint, nur verwenden, wenn der Server über ein Serverzertifikat verfügt. Dieses müssen Sie zunächst von der internen Zertifizierungsstelle anfordern und installieren. Sie können neben dem beschriebenen Weg der Zertifikateverwaltung auch den IIS-Manager auf einem Server nutzen:

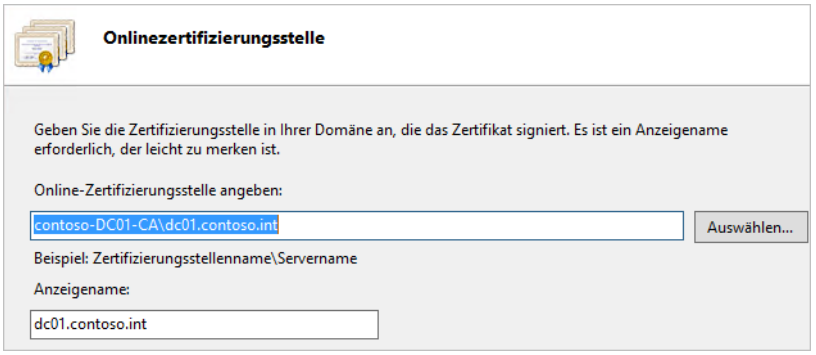
1. Öffnen Sie den IIS-Manager über das Menü *Tools* im Server-Manager.
2. Klicken Sie auf den *Servernamen*.
3. Doppelklicken Sie auf das Feature *Serverzertifikate* im mittleren Bereich der Konsole. Hier sehen Sie alle Serverzertifikate, die Sie verwenden können, damit sich Anwender per SSL verbinden können.
4. Klicken Sie im Bereich *Aktionen* auf *Zertifikatanforderung erstellen*. Alternativ können Sie auch *Domänenzertifikat erstellen* auswählen, wenn Sie mit den Active Directory-Zertifikatdiensten arbeiten. Die folgenden Fenster sind dabei identisch.

Geben Sie im neuen Fenster den Namen des Zertifikats ein. Achten Sie darauf, dass der Name, den Sie im Feld *Gemeinsamer Name* eingeben, dem Servernamen entspricht, mit dem Anwender auf den Server zugreifen. Verwenden Anwender für den Zugriff einen anderen Namen als den gemeinsamen Namen des Zertifikats, erhalten die Anwender eine Zertifikatewarnung, die besagt, dass das Zertifikat für eine andere Seite ausgestellt ist.

Auch wenn Sie den FQDN eines Servers verwenden, zum Beispiel *sps01.contoso.com*, erhalten Anwender eine Fehlermeldung, wenn der Zugriff über den NetBIOS-Namen erfolgt, zum Beispiel mit *sps01*. Soll der Zugriff auf den Server mit *www.contoso.com* erfolgen, muss der gemeinsame Name des Zertifikats auch *www.contoso.com* sein. Greifen Sie mit verschiedenen Hostnamen einer Domäne zu, zum Beispiel *sps01.contoso.com* und *portal.contoso.com*, können Sie als gemeinsamen Namen auch mit dem Platzhalter * arbeiten, zum Beispiel **.contoso.com*. In diesem Zusammenhang spricht man von einem Platzhalterzertifikat.

Wählen Sie auf der nächsten Seite *Eigenschaften für Kryptografiedienstanbieter* Werte für *Kryptografiedienstanbieter* und *Bitlänge* aus und klicken Sie dann auf *Weiter*. In den meisten Fällen können Sie den Standardwert belassen. Erstellen Sie ein Domänenzertifikat, können Sie auf der nächsten Seite direkt über *Auswählen* die Zertifizierungsstelle auswählen, wenn Sie in Active Directory eine Zertifizierungsstelle installiert haben.

Abbildg. 30.11 Auswählen der Zertifizierungsstelle beim Erstellen eines Domänenzertifikats



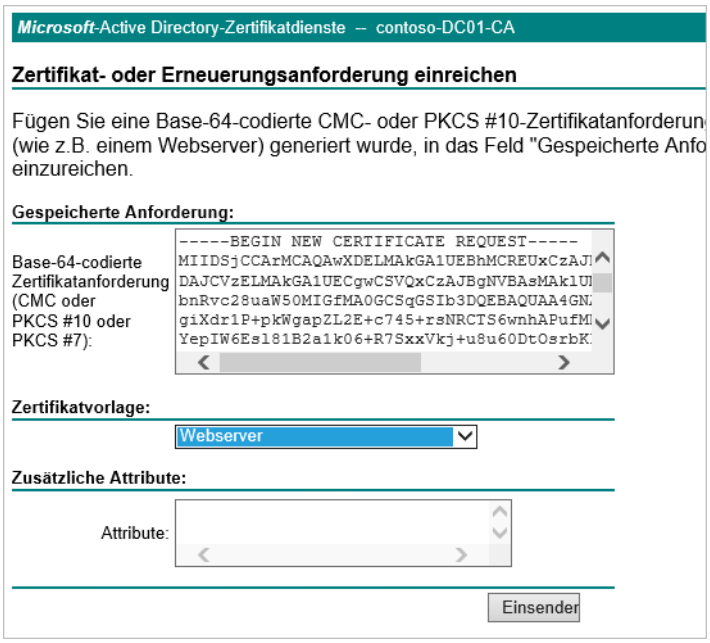
Klicken Sie auf *Fertig stellen*, um das Zertifikat auf dem Server zu installieren. Speichern Sie die Anfrage als Datei, wenn Sie ein normales Zertifikat verwenden. Arbeiten Sie mit einem Domänenzertifikat, können Sie den Assistenten an dieser Stelle schon abschließen. Bei diesem Vorgang überträgt der Assistent automatisch das Zertifikat von den Active Directory-Zertifikatdiensten auf den Server.

Arbeiten Sie mit einer manuellen Zertifikatanfrage für ein Zertifikat eines Drittanbieters oder auch mit den Active Directory-Zertifikatdiensten, müssen Sie noch weitere Schritte durchführen. Sie speichern dazu die Anfrage in einer Datei. Im nächsten Schritt öffnen Sie das Webfrontend des Zertifikateausstellers. Arbeiten Sie mit den Active Directory-Zertifikatdiensten, können Sie diese über die Adresse *http://<Servername>/certsrv* erreichen.

Wählen Sie anschließend auf der Webseite für die Zertifizierungsstelle die Option *Ein Zertifikat anfordern* und wählen Sie dann die *Erweiterte Anforderung* aus. Als Nächstes wählen Sie die Option *Reichen Sie eine Zertifikatanforderung ein, die eine Base64-codierte CMD- oder PKCS10-Datei verwendet, oder eine Erneuerungsanforderung, die eine Base64-codierte PKCS7-Datei verwendet, ein.*

Im nächsten Fenster geben Sie im Feld *Gespeicherte Anforderung* den kompletten Text der *.txt*-Datei ein, die Sie im Vorfeld erstellt haben. Sie können dazu die Datei im Editor öffnen und den Inhalt in die Zwischenablage kopieren. Sie müssen den kompletten Text der Datei dazu verwenden. Klicken Sie dazu in die Datei und markieren Sie den kompletten Text mit Strg+A. Mit Strg+C kopieren Sie den Text in die Zwischenablage, mit Strg+V fügen Sie ihn in das Feld ein. Wählen Sie als Zertifikatvorlage noch Webserver aus, wenn Sie die Internetinformationsdienste (IIS) oder einen Serverdienst absichern wollen, und klicken Sie dann auf *Einsenden*.

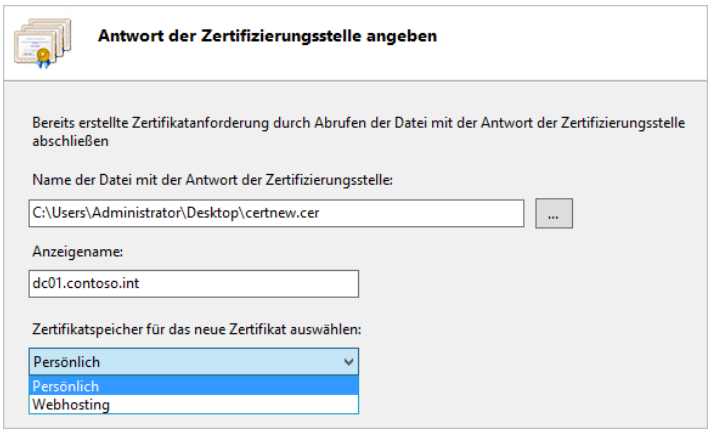
Abbildg. 30.12 Einreichen einer Zertifikatanforderung



Im nächsten Schritt laden Sie das Zertifikat als DER- oder Base-64-Datei auf den Server und schließen den Browser. Als Nächstes müssen Sie das Zertifikat aus der heruntergeladenen *.cer*-Datei auf dem Server installieren:

1. Doppelklicken Sie im Internetinformationsdienste-Manager auf das Feature *Serverzertifikate*.
2. Wählen Sie *Zertifikatanforderung abschließen* im Aktionsbereich aus.
3. Geben Sie einen Anzeigenamen für das Zertifikat ein und klicken Sie auf *OK*. Verwenden Sie als Anzeigenamen am besten den gemeinsamen Namen des Zertifikats, den Sie bei der Erstellung ausgewählt haben.

Abbildg. 30.13 Installieren eines Zertifikats



Zertifikate über Webinterface ausstellen

In diesem Abschnitt zeigen wir Ihnen, wie Sie von einem Server ein Zertifikat von einer Zertifizierungsstelle unter Windows Server anfordern und installieren. Generell können Sie bei der Zuweisung eines Zertifikats auch den Weg über die lokale Verwaltung der Zertifikate gehen, aber die Zuweisung über die Weboberfläche funktioniert ebenso zuverlässig. Sie können zum Beispiel die Verschlüsselung in SQL Server 2012 nur verwenden, wenn der Server über ein Serverzertifikat verfügt. Dieses müssen Sie zunächst von der internen Zertifizierungsstelle anfordern und installieren.

Aktivieren Sie auf der Webseite für die Zertifizierungsstelle (*http://<Servername>/certsrv*) die Option *Ein Zertifikat anfordern* und wählen Sie dann die *Erweiterte Zertifikatanforderung* aus. Aktivieren Sie vorher noch SSL für die Seite, wie im nächsten Abschnitt behandelt. Rufen Sie die Webseite der Zertifizierungsstelle auf, blockiert der Server viele Einstellungen. Nur beim Aufrufen über SSL funktioniert der Abruf von Zertifikaten:

1. Als Nächstes wählen Sie die Option *Eine Anforderung an diese Zertifizierungsstelle erstellen und einreichen*.
2. Wählen Sie als Vorlage die Option *Webserver* und als Name den vollständigen Domänennamen des Servers aus. Klicken Sie anschließend auf *Einsenden* und dann auf *Dieses Zertifikat installieren*.
3. Dadurch ist das Zertifikat auf dem Server verfügbar.

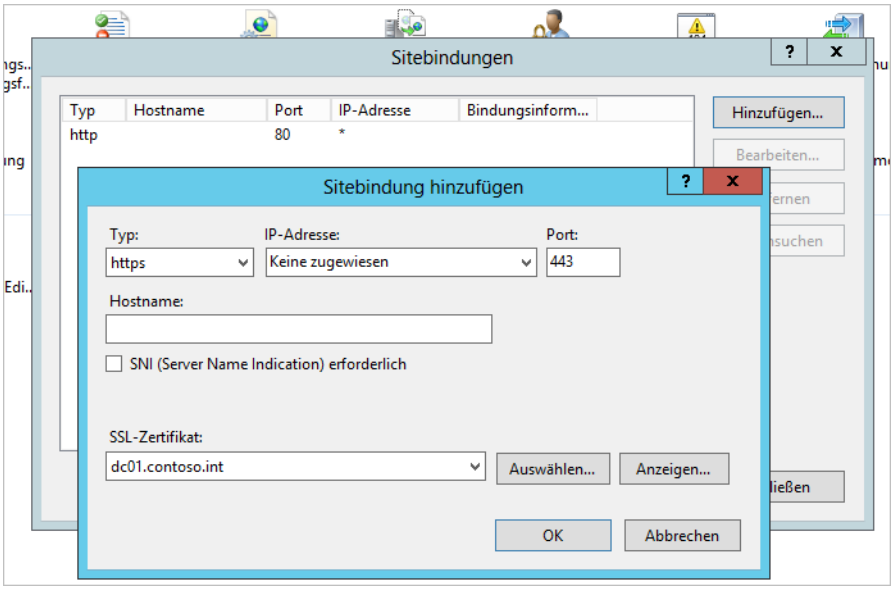
Damit das Zertifikat fehlerfrei funktioniert, muss das Zertifikat der Zertifizierungsstelle, von der Sie das Zertifikat haben, bei den vertrauenswürdigen Stammzertifizierungsstellen auf dem Server hinterlegt sein sowie auf den Clients, die auf den Server zugreifen. Wie das geht, zeigen wir ebenfalls in den nachfolgenden Abschnitten.

SSL für Zertifikatdienste einrichten

Viele Optionen für den Webdienst der Zertifizierungsstelle funktionieren erst dann, wenn Sie SSL für die Webdienste aktivieren. Standardmäßig erreichen Sie den Webdienst über *http://<Servername>/certsrv*. Wenn Sie ein Zertifikat über diese URL abrufen wollen, erhalten Sie aber die Meldung, dass Sie erst SSL für den Webdienst aktivieren müssen. Dazu gehen Sie folgendermaßen vor:

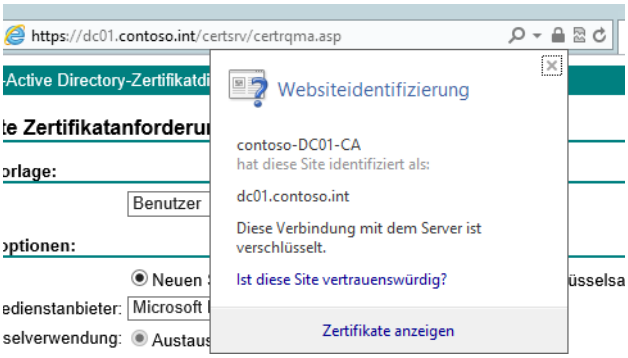
1. Klicken Sie im Internetinformationsdienste-Manager auf *Sites/Default Web Site*.
2. Klicken Sie rechts auf *Bindungen*.
3. Klicken Sie im neuen Fenster auf *Hinzufügen* und wählen Sie *https* aus.
4. Wählen Sie bei *SSL-Zertifikat* ein Zertifikat aus. Sie können das Zertifikat jederzeit anpassen.
5. Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

Abbildg. 30.14 Konfigurieren der SSL-Bindung für die Webdienste der Zertifizierungsstelle



Sobald Sie die Bindung definiert haben, können Sie bereits auf die Seite per SSL zugreifen. Es sind zwar noch Optimierungsarbeiten notwendig, die wir in den nächsten Abschnitten behandeln, ein Zugriff ist aber per SSL bereits möglich. Dazu verwenden Sie den Link *https://<Servername>/certsrv*.

Abbildg. 30.15 SSL-Zugriff auf eine Website



Greifen Sie mit URLs auf den Server zu, erscheint unter Umständen mehrere Male ein Authentifizierungsfenster. Die Ursache liegt in einer Sicherheitsfunktion, die seit Windows Server 2003 integriert ist. Diese verhindert den Zugriff auf einen Server über das Netzwerk mit einem anderen Namen als dem Servernamen.

In diesem Fall sollten Sie zunächst überprüfen, ob im Browser die Adresse auch als lokales Intranet konfiguriert ist. Achten Sie in diesem Fall auch darauf, dass Sie entweder mit einem Platzhalterzertifikat arbeiten, wie in den vorangegangenen Abschnitten besprochen, oder für die entsprechende

URL den richtigen Namen im Zertifikat angeben. Zusätzlich sollten Sie auf dem Server diese URLs noch in die Registry eintragen. Gehen Sie dazu folgendermaßen vor:

1. Rufen Sie mit *regedit* den Registrierungseditor auf.
2. Navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0*.
3. Klicken Sie mit der rechten Maustaste auf *MSV1_0*, wählen Sie *Neu* und dann *Wert der mehrteiligen Zeichenfolge*.
4. Geben Sie als Namen *BackConnectionHostNames* ein.
5. Klicken Sie mit der rechten Maustaste auf *BackConnectionHostNames* und dann auf *Ändern*.
6. Geben Sie in das Feld *Wert* die Hostnamen für die Sites ein, die sich auf dem lokalen Server befinden, und klicken Sie danach auf *OK*.
7. Starten Sie IIS mit *iisreset* neu.

Hilft diese Vorgehensweise nicht, können Sie auf dem Server noch einen anderen Registryeintrag bearbeiten, der eventuell den Fehler behebt:

1. Navigieren Sie zu *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa*.
2. Klicken Sie mit der rechten Maustaste auf *Lsa*, wählen Sie *Neu* und dann *DWORD-Wert*.
3. Geben Sie dem neuen Wert den Namen *DisableLoopbackCheck*.
4. Klicken Sie mit der rechten Maustaste auf *DisableLoopbackCheck* und dann auf *Ändern*.
5. Geben Sie in das Feld *Wert* den Wert *1* ein und klicken Sie anschließend auf *OK*.
6. Starten Sie den Server neu.

Zertifikate von Stammzertifizierungsstellen verwalten

Damit das Zertifikat fehlerfrei funktioniert, muss das Zertifikat der Zertifizierungsstelle, von der Sie das Zertifikat haben, bei den vertrauenswürdigen Stammzertifizierungsstellen auf dem Server hinterlegt sein sowie auf den Clients, die auf den Server zugreifen.

Veröffentlichen Sie den Server über Forefront TMG/UAG 2010 im Internet, muss auch auf diesem Server das Zertifikat vorhanden sein. Fügen Sie das Snap-In *Zertifikate* zu einer MMC hinzu (*certlm.msc*) und stellen Sie sicher, dass das Zertifikat der Zertifizierungsstelle für das lokale Computerkonto des Servers im Knoten *Vertrauenswürdige Stammzertifizierungsstellen* angezeigt wird. Das Zertifikat der Stammzertifizierungsstelle muss hinterlegt sein, damit der Server den Zertifikaten dieser Zertifizierungsstelle vertraut. Haben Sie die Active Directory-Zertifikatdienste installiert, können Sie den Import des Zertifikats auf Clients und dem Server beschleunigen, wenn Sie auf dem Server über *gpupdate /force* die Gruppenrichtlinien erneut abrufen.

Die Installation der Zertifikate von internen Zertifizierungsstellen findet über die Gruppenrichtlinie in Active Directory statt. Arbeiten Sie mit einer Zertifizierungsstelle eines Drittanbieters, müssen Sie das Zertifikat der Zertifizierungsstelle in die vertrauenswürdigen Stammzertifizierungsstellen importieren. Zertifikate überprüfen Sie auf folgendem Weg:

1. Geben Sie *certlm.msc* auf der Startseite ein.
2. Erweitern Sie in der Konsole *Zertifikate/Vertrauenswürdige Stammzertifizierungsstellen/Zertifikate*.
3. Überprüfen Sie an dieser Stelle, ob das Zertifikat der Zertifizierungsstelle hinterlegt ist. Finden Sie das Zertifikat nicht, dann geben Sie in einer Eingabeaufforderung *gpupdate /force* ein, um per

Gruppenrichtlinie das Zertifikat abzurufen. Erscheint auch dann das Zertifikat nicht, exportieren Sie dieses auf dem Zertifikatserver selbst und importieren es auf dem Server.

Sofern die Zertifizierungsstelle in der gleichen Active Directory-Domäne installiert wurde, in der auch der Server installiert ist, für den Sie ein Zertifikat nutzen wollen, sollte dies automatisch stattfinden. Dies ist anders, sofern die Zertifizierungsstelle nicht in Active Directory integriert ist. In diesem Fall können Sie das Zertifikat leicht auf dem Server mit der Zertifizierungsstelle exportieren.

Die vertrauenswürdigen Zertifizierungsstellen finden Sie auch 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 Server auf, der über das Zertifikat bereits verfügt.

Hier sollte das Zertifikat der Zertifizierungsstelle hinterlegt sein. Markieren Sie diese Zertifizierungsstelle und klicken Sie auf die Schaltfläche *Exportieren*. Unter Umständen tauchen an dieser Stelle mehrere Zertifikate Ihrer Stammzertifizierungsstelle auf, wählen Sie im Zweifel das mit dem höchsten Ablaufdatum aus. Erscheint beim Exportieren eine Abfrage des privaten Schlüssels des Zertifikats, haben Sie das falsche erwischt. Verwenden Sie dann einfach das andere Zertifikat. Exportieren Sie auf dem Server das Zertifikat in eine *.cer*-Datei.

Klicken Sie doppelt auf das Zertifikat, wird es auf dem Server angezeigt und Sie können es installieren. Klicken Sie auf die Schaltfläche *Zertifikat installieren*, damit das Zertifikat auf dem Server installiert wird. Lassen Sie das Stammzertifikat in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen importieren. Überprüfen Sie anschließend, ob das Zertifikat erfolgreich importiert ist.

Auf allen beteiligten Servern und Arbeitsstationen muss der Zertifizierungsstelle des Unternehmens auf dieser Registerkarte vertraut werden. Eine weitere Möglichkeit, das Zertifikat der vertrauenswürdigen Stammzertifizierungsstelle zu ex- und importieren, ist das Snap-In zur Verwaltung von Zertifikaten. Um das Zertifikat über die MMC-Konsole zu exportieren, gehen Sie folgendermaßen vor:

1. Tippen Sie *certlm.msc* auf der Startseite ein.
2. Erweitern Sie in der Konsole *Zertifikate/Eigene Zertifikate/Zertifikate*.

Die Zertifizierungsstellentypen und -Aufgaben

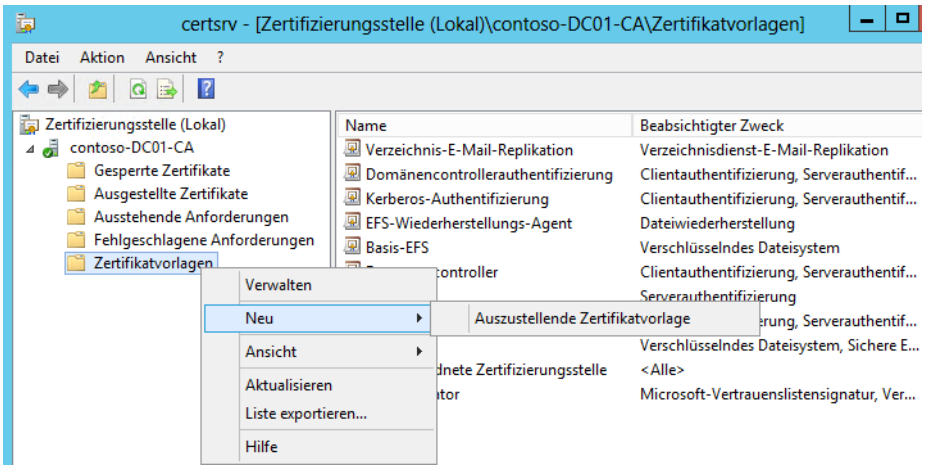
Bei der Installation der Active Directory-Zertifikatdienste wählen Sie aus, ob der Typ *Unternehmen* oder *Eigenständig* installiert werden soll. Wählen Sie *Unternehmen* aus, integriert Windows die Zertifikatdienste in Active Directory. Außerdem verteilt eine Zertifizierungsstelle (Certificate Authority, CA) das Zertifikat für die vertrauenswürdigen Stammzertifizierungsstellen auf den Computern automatisch über eine Gruppenrichtlinie. Wir haben diese Vorgänge zu Beginn des Kapitels besprochen.

HINWEIS Alle Mitgliedcomputer einer Domäne vertrauen einer internen Stammzertifizierungsstelle mit dem Typ *Unternehmen* automatisch. Das Zertifikat dieser Zertifizierungsstelle wird dazu auf den Clientcomputern und Mitgliedsservern in den Zertifikatspeicher 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 *Users*.

Innerhalb einer Unternehmenszertifizierungsstelle werden die Zertifikate auf Basis von Zertifikatvorlagen ausgestellt. Sie können in der Verwaltungskonsole (*certsrv.msc*) jederzeit weitere Vorlagen erstellen.

Abbildg. 30.16 Anzeigen und Verwalten der Zertifikatvorlagen



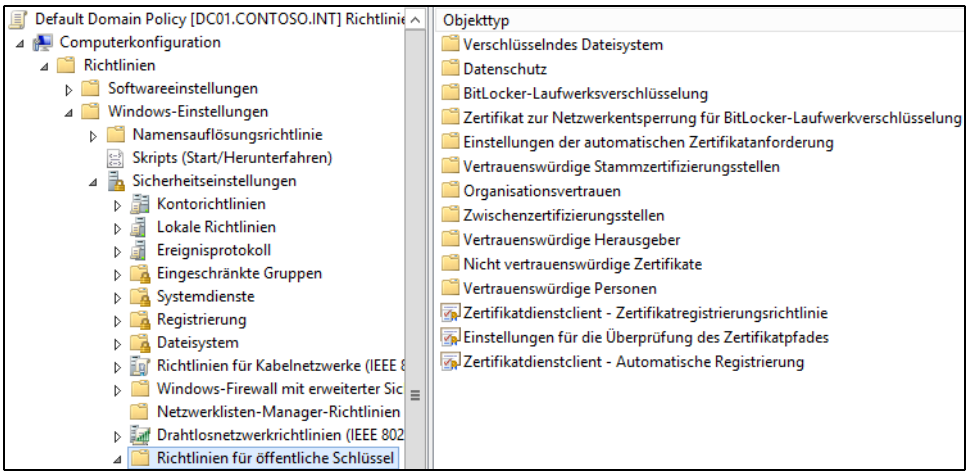
Die Zertifikatvorlagen verwalten Sie aber hauptsächlich mit dem Snap-In *Zertifikatvorlagen*. Dieses startet, wenn Sie im Kontextmenü *Zertifikatvorlagen* in der Verwaltungskonsole *Zertifizierungsstelle* auf den Menüpunkt *Verwalten* klicken. Direkt starten Sie die Verwaltung durch die Eingabe von *certtmpl.msc* auf der Startseite. Neben den Standardvorlagen gibt es noch zahlreiche weitere, die über die Verwaltungskonsole konfiguriert und aktiviert werden können.

Jede Zertifikatvorlage verfügt über eine eigene Sicherheitsverwaltung, die Sie über das Kontextmenü in den Eigenschaften auf der Registerkarte *Sicherheit* aufrufen. Erstellen Sie Zertifikate auf Basis der Zertifikatvorlagen, können die Zertifikatdienste die Daten und den Namen des Antragstellers automatisch aus Active Directory auslesen.

Verteilung der Zertifikateinstellungen über Gruppenrichtlinien

Die Einstellungen für Zertifikate finden Sie unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Richtlinien für öffentliche Schlüssel*. Über die Einstellungen an dieser Stelle werden zentral für alle Rechner einer Domäne Einstellungen vorgegeben. So kann zum Beispiel eingestellt werden, dass Anwender nur geprüfte und vertrauenswürdige Zertifikate herunterladen dürfen. In Kapitel 28 sind wir ausführlich auf diese Themen eingegangen.

Abbildg. 30.17 Verwalten der Zertifikateinstellungen einer Domäne über Gruppenrichtlinien



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 in das Berechtigungsmodell von Active Directory integriert.

Zertifizierungsstellenverwaltung delegieren

Verwaltungsrollen können an verschiedene Personen in einer Organisation verteilt werden. Die rollenbasierte Verwaltung wird von Unternehmenszertifizierungsstellen und eigenständigen Zertifizierungsstellen unterstützt. 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 auf die einzelnen Gruppen. In Windows Server 2012 sind Zertifikatvorlagen enthalten, die unterschiedliche Registrierungs-Agenttypen aktivieren.

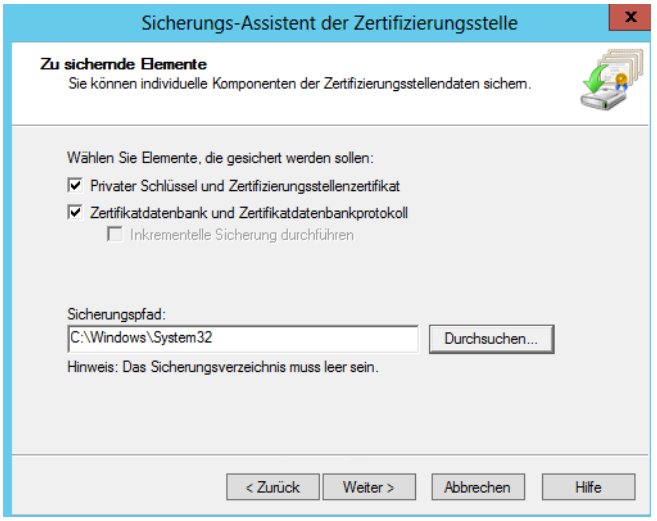
Die Einstellungen für diese Agents werden auf der Registerkarte *Registrierungs-Agents* durchgeführt. Klicken Sie im Bereich *Registrierungs-Agents* auf *Hinzufügen* und geben Sie die Namen des Benutzers oder der Gruppen ein.

Auf der Registerkarte *Überwachung* werden die zu überwachenden Ereignisse ausgewählt. Die generellen Optionen der Überwachungsrichtlinie können in Gruppenrichtlinie unter *Computerkonfiguration/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.

Abbildg. 30.18 Sichern einer Zertifizierungsstelle



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.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Zertifizierungsstellen installieren, einrichten und in Active Directory verwenden, um zum Beispiel SSL-Zertifikate für Webserver anzufordern und zu installieren.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie Netzwerke mit dem Netzwerkzugriffschutz (Network Access Protection, NAP) absichern.

Kapitel 31

Netzwerkzugriffsschutz

In diesem Kapitel:

Mit dem Netzwerkzugriffsschutz (Network Access Protection, NAP) in Windows Server 2012 können Unternehmen alle Rechner und Server im Netzwerk auf optimale Sicherheitseinstellungen prüfen. Entspricht ein Client nicht den vorgegebenen Richtlinien, zum Beispiel weil ein Virenscanner fehlt oder er nicht aktuell ist, können die Server den Zugriff des Clients sperren. Mit NAP besteht auch die Möglichkeit, den Client zu Wartungsservern umzuleiten, von denen er Aktualisierungen des Virenscanners erhalten kann.

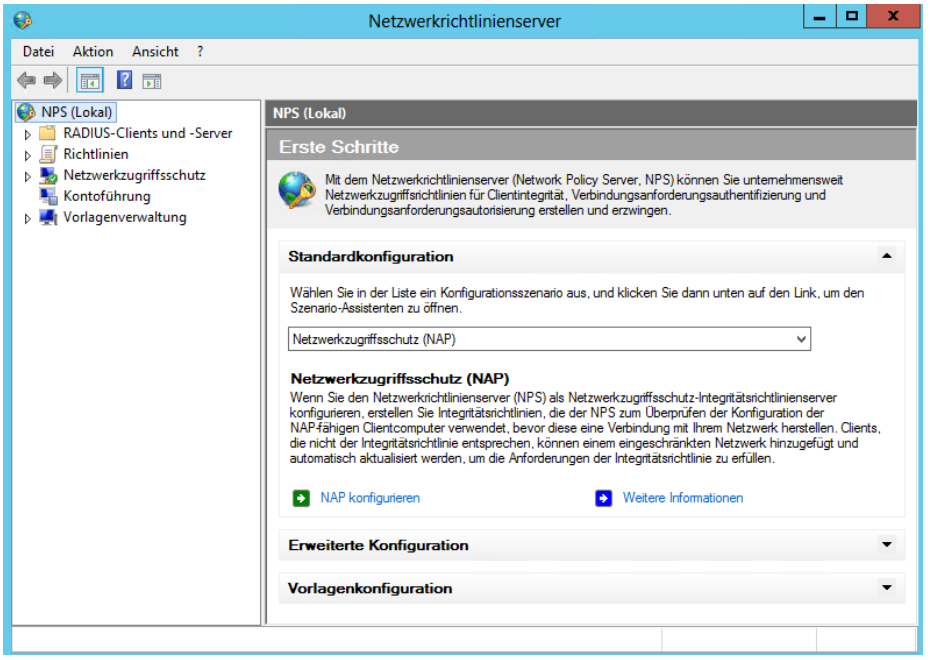
Der Netzwerkzugriffsschutz ist also dafür zuständig, zu überprüfen, ob die Sicherheitskonfigurationen auf einem Computer ausreichend gesetzt sind. Dadurch können Unternehmen Gefahren vermeiden, die von Heim-PCs und Notebooks ausgehen. Fremdsysteme, Internet-Cafés und unsichere Heimarbeitsplätze lassen sich so effizient vom Netzwerk ausschließen und bei der VPN-Einwahl blockieren, auch wenn der Anwender über entsprechende Einwahlrechte verfügt.

Netzwerkzugriffsschutz in der Praxis – Erste Schritte

Im nächsten Abschnitt zeigen wir Ihnen in aller Schnelle, wie Sie den Netzwerkzugriffsschutz einrichten. In den weiteren Abschnitten in diesem Kapitel gehen wir ausführlicher auf das Thema ein.

In Windows 7 und Windows 8 ist der Netzwerkzugriffsschutz in das Wartungscenter des Betriebssystems integriert. Die Konfiguration führen Sie über Gruppenrichtlinien durch. Die Einstellungen hierfür finden sich im Bereich *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Netzwerkzugriffsschutz*. Die Steuerung übernimmt ein Netzwerkschutz-Richtlinienserver (NPS).

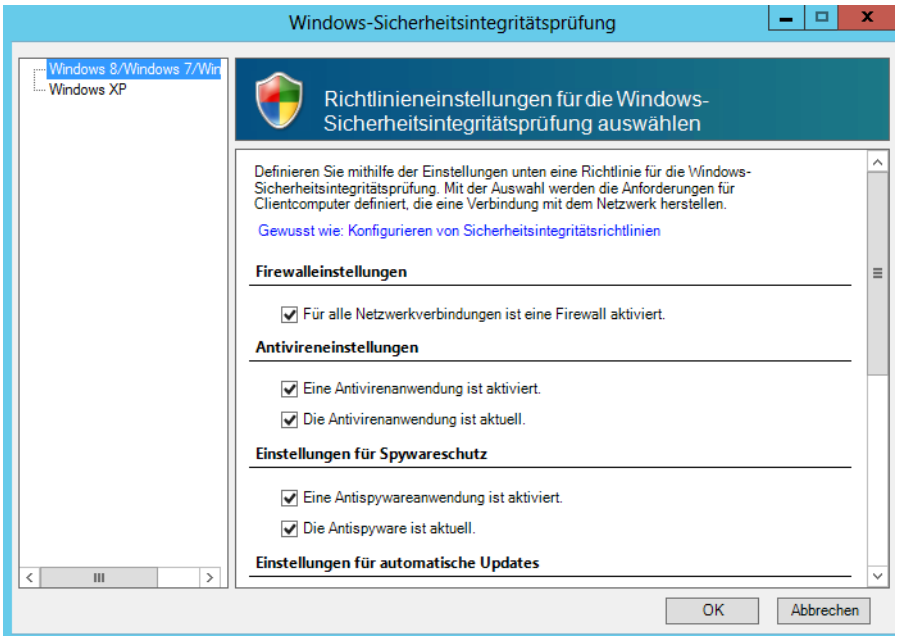
Abbildg. 31.1 Die Verwaltungskonsole von NAP nach der Installation der Serverrolle



Den Netzwerkzugriffsschutz installieren und konfigurieren Sie über den Server-Manager. Die Installation und Konfiguration erfolgt über *Verwalten/Rollen und Features hinzufügen/Netzwerkrichtlinien- und Zugriffsdienste*.

Die Einstellungen finden Sie nach der Installation in der Konsole *Netzwerkrichtlinienserver* über *NPS/Netzwerkzugriffsschutz/Systemintegritätsprüfungen/Windows-Sicherheitsintegritätsverifizierung*. In der Mitte sind zunächst die Eigenschaften der Prüfung aufzurufen, zum Beispiel *Windows-Sicherheitsintegritätsverifizierung*. Hier können Sie festlegen, was Clients erfüllen müssen, um Bestandteil des Netzwerks zu werden. Diese Systemintegritätsprüfungen bezeichnet Microsoft auch als Security Health Agents (SHA).

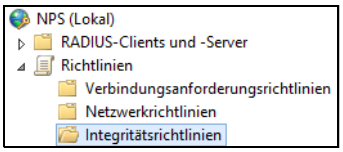
Abbildg. 31.2 Sicherheitsintegritätsüberprüfungen für Windows 8



Über *NPS/Richtlinien/Integritätsrichtlinien* legen Sie anschließend Richtlinien fest. Die Integritätsrichtlinie entscheidet, ob ein Client konform oder nicht konform ist. Abhängig ist dies von der Systemintegritätsprüfung. Netzwerkrichtlinien basieren wiederum auf Integritätsrichtlinien.

In Netzwerkrichtlinien steuern Sie, wie sich Server gegenüber Clients verhalten sollen, welche die Prüfung bestehen oder die Prüfungen nicht bestehen. Die NAP-Infrastruktur basiert daher auf Systemintegritätsprüfungen (System Health Validators), Integritätsrichtlinien (Health Policies) und Netzwerkrichtlinien (Network Policies).

Abbildg. 31.3 Richtlinien steuern den Zugriff auf Basis der Integritätsprüfungen



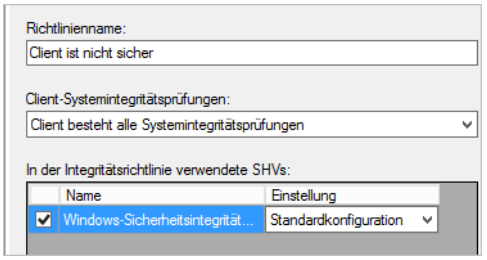
Eine einfache Verwendung von NAP ist die Integration in DHCP. Unsichere Clients (welche die Integritätsprüfung nicht bestehen) erhalten entweder keine IP-Adresse oder eine IP-Adresse in einem sicheren Bereich des Netzwerks.

Für die Verwendung müssen Sie zunächst die Systemintegritätsprüfungen konfigurieren, zum Beispiel die Windows-Sicherheitsintegritätsverifizierung. Anschließend muss eine Integritätsrichtlinie (Health Policy) erstellt werden, welche die konfigurierte Systemintegritätsprüfung verwendet.

Zur Erstellung einer Integritätsrichtlinie klicken Sie mit der rechten Maustaste auf *Richtlinien/Integritätsrichtlinien*. Hier lässt sich festlegen, wann ein Client zu welcher Integritätsrichtlinie gehören soll. Am einfachsten ist eine Struktur mit zwei Integritätsrichtlinien: eine Richtlinie für Clients, die alle Tests der Integritätsprüfung bestehen, und eine Richtlinie für Clients, die bei den Tests durchfallen.

Für Systemintegritätsprüfungen können Unternehmen mehrere verschiedene Versionen von Richtlinien einsetzen. Eine Konfiguration kann zum Beispiel für bestimmte Rechner Virenschutz und Patches abprüfen, während eine andere Prüfung nur die Firewall überprüft. Dadurch können Unternehmen wesentlich flexibler mit dem Netzwerkzugriffsschutz arbeiten und Clients verschiedenen Richtlinien zuordnen.

Abbildg. 31.4 Zuordnen einer neuen Integritätsrichtlinie zu einer Integritätsprüfung



Netzwerkrichtlinien erstellen Sie schließlich über *Richtlinien/Netzwerkrichtlinien*. Auch hier ist der beste Weg, zwei Richtlinien zu erstellen: eine Richtlinie für die Integritätsrichtlinie der sicheren Clients und eine Netzwerkrichtlinie für die Integritätsrichtlinie der unsicheren Clients.

Auf der Seite *Bedingungen angeben* steht über *Hinzufügen* die Option *Integritätsrichtlinien* zur Verfügung. Hier stehen die erstellten Integritätsrichtlinien zur Verfügung, die wiederum auf die Integritätsprüfungen aufbauen. Nachdem die Richtlinie für konforme NAP-Clients erstellt ist, müssen Sie eine Netzwerkrichtlinie erstellen, die den Netzwerkzugriff für nicht-konforme Clients steuert.

Der Vorgang dabei ist ähnlich. Sie erstellen also eine Integritätsprüfung und auf deren Basis zwei Integritätsrichtlinien: eine Richtlinie für Clients, welche die Tests bestehen, und eine Richtlinie für Clients, die die Tests nicht bestehen. Anschließend legen Sie über Netzwerkrichtlinien fest, in welchem Bereich des Netzwerks sich die verschiedenen Clients bewegen dürfen.

Zur Verwendung von NAP über DHCP müssen Sie den DHCP-Server konfigurieren, damit dieser NAP und die erstellten Richtlinien nutzen kann (siehe Kapitel 24). Die Einstellungen finden in der DHCP-Verwaltungskonsole statt (*dhcpmgmt.msc*). Die Einstellungen von NAP nehmen Sie in den Eigenschaften des Bereichs auf der Registerkarte *Netzwerkzugriffsschutz* über die Option *Für diesen Bereich aktivieren* vor. Die Option *Netzwerkzugriffsschutz-Standardprofil verwenden* aktiviert NAP.

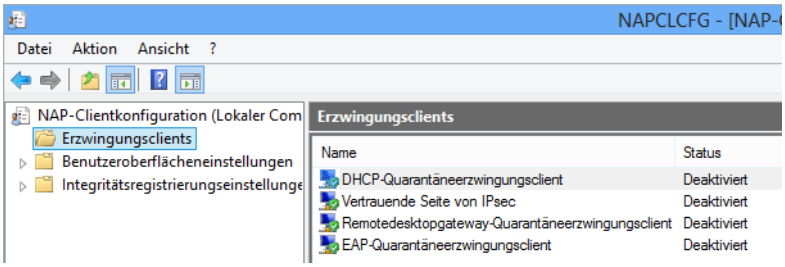
Im nächsten Schritt muss der DHCP-Server so konfiguriert werden, dass er NAP-konformen Clients eine IP-Adresse zuteilt. Über das Kontextmenü von *Bereichsoptionen* wählen Sie dazu *Optionen kon-*

figurieren aus. Auf der Registerkarte *Erweitert* muss im Dropdownlistenfeld *Benutzerklasse* die Option *Standardbenutzerklasse* aktiviert werden. Hier können Sie die Optionen auswählen, die NAP-konformen Clients zugewiesen werden sollen, zum Beispiel DNS-Server, WINS, und DNS-Domäne.

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, oder eben keine IP-Adressen, was den Zugriff auf das Netzwerk unterbindet. Dazu steht im Dropdownlistenfeld *Benutzerklasse* die Option *Standardmäßige Netzwerkzugriffsschutz-Klasse* zur Verfügung.

Die nächste Aufgabe ist die Aktivierung der DHCP-NAP-Unterstützung auf den Clients. Über *napclcfg.msc* starten Sie die Verwaltungskonsole des NAP-Clients in Windows 8. Über *Erzwingungsclients/DHCP-Quarantäneerzwingungsclient* lässt sich die DHCP-Unterstützung aktivieren. Diese Einstellung finden Sie auch in den Gruppenrichtlinien unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Netzwerkzugriffsschutz/NAP-Clientkonfiguration/Erzwingungsclients*.

Abbildg. 31.5 Der NAP-Client verbindet PCs mit der NAP-Infrastruktur



Windows 7 und Windows 8 erkennt, wenn ein Computer nicht dem Zugriffschutz im Netzwerk entspricht, und informiert den Anwender entsprechend. Klicken Anwender doppelt auf die Meldung oder das dazugehörige Symbol, erhalten sie eine ausführliche Statusangabe anzeigt.

Alle Ereignisse der NAP-Konfiguration sind zusätzlich in der Ereignisanzeige aufgeführt. Die Ereignisse auf dem Client finden Sie in der Ereignisanzeige über *Anwendungs- und Dienstprotokolle/Microsoft/Windows/Network Access Protection*. Auf dem Server sind die Fehler im Systemprotokoll zu finden.

Netzwerkzugriffsschutz (NAP) – Ausführliche Erläuterungen und Grundlagen

NAP ist dafür zuständig, zu überprüfen, ob die Sicherheitskonfigurationen auf einem Computer ausreichend gesetzt sind. Bei dem Vorgang lässt sich überprüfen, ob aktuelle Patches installiert, die Firewall aktiviert und weitere Sicherheitskonfigurationen gesetzt sind. Entspricht ein Client nicht den Bedingungen für das Netzwerk, wird diesem nur ein eingeschränkter Zugriff zum Netzwerk oder überhaupt kein Zugriff gewährt.

NAP stellt sicher, dass die Endpunkte in einem Netzwerk, also die PCs, einem fest definierten Sicherheitsstandard entsprechen. 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, den er an den Netzwerkrichtlinienserver übergibt.
3. Dieser entscheidet auf Basis der zentralen Richtlinie, ob das Statement of Health gültig ist oder nicht.
4. Auf Basis dieses Ergebnisses wendet der Server eine Richtlinie an, die den Zugriff gestattet oder nicht.
5. In Windows 7 und Windows 8 ist der Netzwerkzugriffsschutz direkt in das Wartungscenter integriert, was für Administratoren und Endanwender den Überblick deutlich erhöht.

Erste Schritte mit NAP

Die clientseitige Konfiguration von NAP führen Sie am besten über Gruppenrichtlinien durch. Die Einstellungen hierfür finden Sie in der Gruppenrichtlinienverwaltung unter *Computerkonfiguration/(Richtlinien)/Windows-Einstellungen/Sicherheitseinstellungen/Netzwerkzugriffsschutz*.

Über diese Einstellungen lässt sich das Verhalten der Clientcomputer konfigurieren. Hier können Sie zum Beispiel die einzelnen Clients für NAP für die einzelnen Funktionen aktivieren oder deaktivieren.

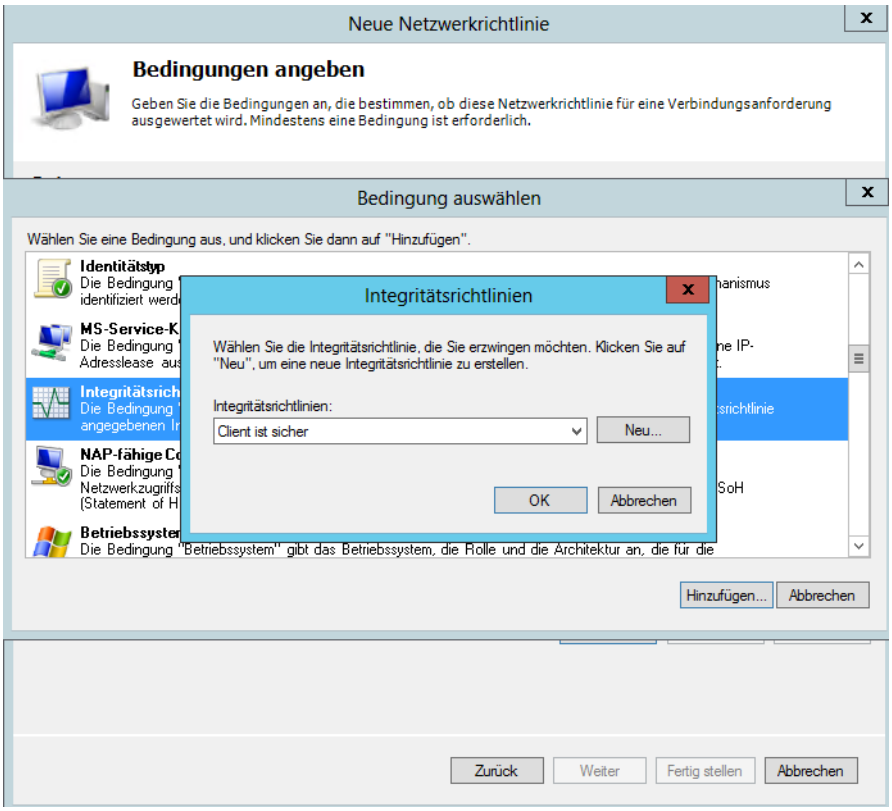
Die Servereinstellungen von NAP führen Sie über den Server-Manager durch. Die Verwaltung baut zunächst auf die Sicherheitsintegritätsprüfung auf. Diese ruft von den Clients das Statement of Health (SoH) ab. Diese Einstellungen finden Sie in der Verwaltungskonsole über *NPS/Netzwerkzugriffsschutz/Systemintegritätsprüfungen/Windows-Sicherheitsintegritätsverifizierung*. Rufen Sie in der Mitte des Fensters 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 sendet also das SoH an den Netzwerkrichtlinienserver (NPS), der die Informationen dann auswertet.

Über den Konsoleneintrag *NPS/Richtlinien/Integritätsrichtlinien* legen Sie anschließend Richtlinien fest, auf deren Basis bestimmt wird, was mit Clients passieren soll, welche die Sicherheitsverifizierung bestehen oder nicht. 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.

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.

Abbildg. 31.6 Konfigurieren der Netzwerkrichtlinie auf Basis der Integritätsrichtlinie



Praxis: 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 umfangreiche Änderungen in der Infrastruktur.

Konfigurieren der Systemintegritätsüberprüfung

Der NAP-Schutz in DHCP ist zwar die unsicherste Variante des NAP-Schutzes (Clients könnten sich auch manuell eine IP-Adresse zuteilen), dafür aber auch die am schnellsten einführbare:

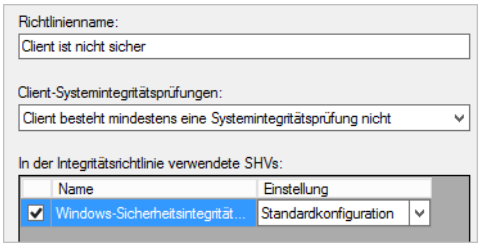
1. Klicken Sie dazu in der NAP-Konsole auf *Netzwerkzugriffsschutz/Systemintegritätsprüfungen/Windows-Sicherheitsintegritätsverifizierung/Einstellungen*.
2. Rufen Sie die Eigenschaften der *Standardkonfiguration* auf.
3. Hier legen Sie fest, welche Bedingungen eine Arbeitsstation erfüllen muss, damit diese mit dem Netzwerk kommunizieren darf.

Erstellen von Integritätsrichtlinien auf Basis von Systemintegritätsprüfungen

Der nächste Schritt besteht darin, dass Sie eine Integritätsrichtlinie (Health Policy) erstellen, die als Grundlage die konfigurierte Systemintegritätsprüfung 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:

1. Klicken Sie zur Erstellung einer Integritätsrichtlinie mit der rechten Maustaste auf *Richtlinien/Integritätsrichtlinien* und wählen Sie im Kontextmenü den Befehl *Neu*.
2. Weisen Sie der Richtlinie die Bezeichnung *Client ist sicher* zu.
3. Stellen Sie sicher, dass im Listenfeld *Client-Systemintegritätsprüfen* der Eintrag *Client besteht alle Systemintegritätsprüfungen* ausgewählt ist.
4. Aktivieren Sie das Kontrollkästchen *Windows-Sicherheitsintegritätsverifizierung*.

Abbildg. 31.7 Erstellen einer neuen Integritätsrichtlinie



5. Erstellen Sie eine weitere Integritätsrichtlinie.
6. Weisen Sie dieser die Bezeichnung *Client ist nicht sicher* zu.
7. Wählen Sie im Listenfeld den Eintrag *Client besteht mindestens eine Systemintegritätsprüfung nicht* aus.
8. Aktivieren Sie das Kontrollkästchen *Windows-Sicherheitsintegritätsverifizierung*.

Erstellen von Netzwerkrichtlinien auf Basis von Integritätsrichtlinien

Im Anschluss legen Sie fest, welchen Netzwerkzugriff die Clients bekommen, die der jeweiligen Integritätsrichtlinie zugewiesen sind. Diese Aufgabe erledigen Sie mit Netzwerkrichtlinien. Einfach ausgedrückt basieren Netzwerkrichtlinien auf Integritätsrichtlinien, welche wiederum auf Systemintegritätsprüfungen aufbauen.

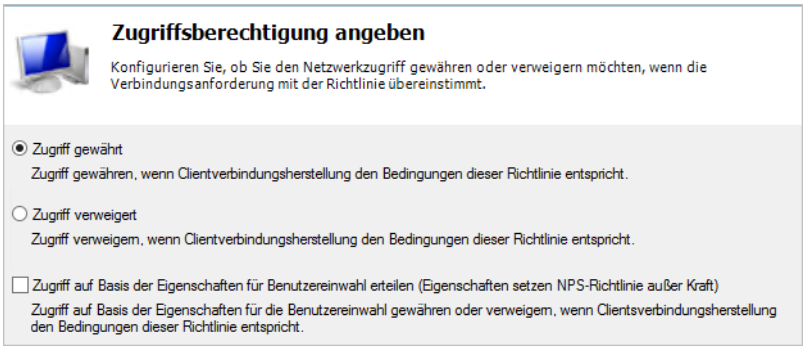
Nachdem Sie die Systemintegritätsprüfung festgelegt haben, in denen konfiguriert ist, welche Bedingungen ein NAP-konformer-Client erfüllen muss, wird mit den Integritätsrichtlinien festgelegt, ob ein Client NAP-konform oder nicht-NAP-konform ist. Die Netzwerkrichtlinien steuern wiederum, was mit NAP-konformen bzw. nicht-NAP-konformen Clients im Netzwerk passieren soll und welchen Zugriff diese erhalten dürfen. Die NAP-Infrastruktur basiert daher auf den drei Pfeilern:

1. Systemintegritätsprüfungen (System Health Validators) und System Health Agents (SHA)
2. Integritätsrichtlinien (Health Policies)
3. 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, wenn diese noch nicht deaktiviert sind. Im ersten Schritt erstellen Sie die Netzwerkrichtlinie für konforme Clients:

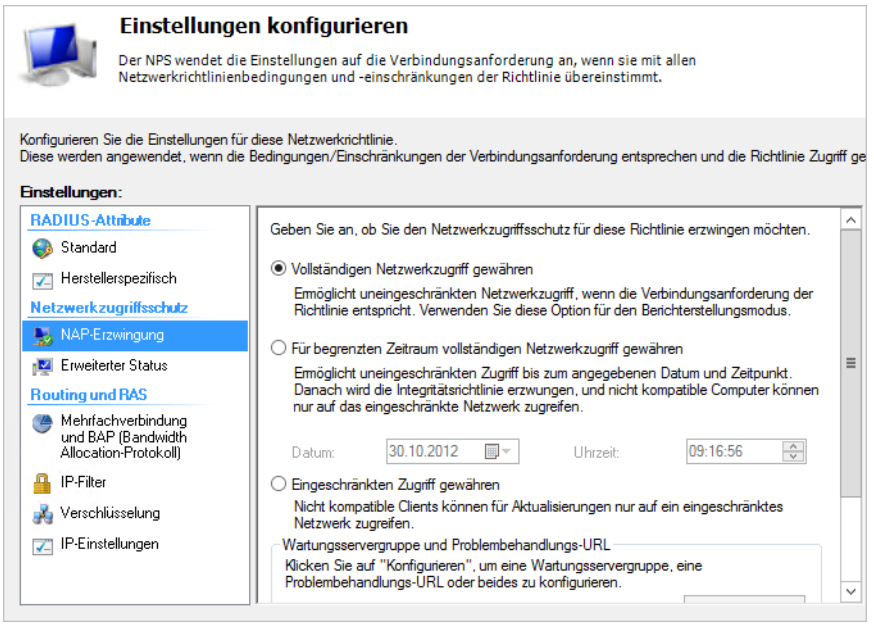
1. Klicken Sie dazu mit der rechten Maustaste auf den Konsoleneintrag *Richtlinien/Netzwerkrichtlinien* und wählen Sie im Kontextmenü den Befehl *Neu* aus.
2. Geben Sie der Richtlinie eine Bezeichnung in der Form *Vollzugriff für NAP-Konforme Clients*.
3. Setzen Sie die Option *Zugriff gewähren*.
4. Aktivieren Sie bei *Typ des Netzwerkzugriffservers* die Option *DHCP-Server*.
5. Klicken auf der nächsten Seite *Bedingungen angeben* auf *Hinzufügen*.
6. Wählen Sie als Option *Integritätsrichtlinien* aus. Sie sehen, dass Sie hier neben den Integritätsrichtlinien noch zahlreiche weitere Methoden haben, um Richtlinien für den Netzwerkzugriff der Clients festzulegen. Es besteht dabei auch die Möglichkeit, dass Sie mehrere Bedingungen festlegen, die für verschiedene Netzwerkzugriffe notwendig sind.
7. Klicken Sie auf *Hinzufügen*.
8. Wählen Sie die Richtlinie *Client ist sicher* aus.
9. Auf der nächsten Seite des Fensters legen Sie den Netzwerkzugriff der Richtlinie fest. Wählen Sie hier *Zugriff gewährt* aus.

Abbildg. 31.8 Erlauben von Netzwerkzugriffen für sichere Clients



10. Klicken Sie auf *Weiter*, um zum Fenster *Authentifizierungsmethoden konfigurieren* zu gelangen.
11. Deaktivieren Sie die Standardeinstellungen und aktivieren Sie noch die Option *Nur Integritätsprüfung für Computer durchführen*.
12. Klicken Sie auf *Weiter* und belassen Sie im nächsten Fenster alle Einstellungen, wie sie sind. Auf diesem Fenster legen Sie die Einschränkungen fest.
13. Klicken Sie im Fenster *Einschränkungen konfigurieren* ebenfalls auf *Weiter*. Sie gelangen auf das Fenster *Einstellungen konfigurieren*.
14. Klicken Sie hier auf *NAP-Erzwingung* und stellen Sie sicher, dass die Option *Vollständigen Netzwerkzugriff gewähren* aktiviert ist.

Abbildg. 31.9 Netzwerkclients den Zugriff zum Netzwerk gestatten



Klicken Sie nach der Einstellung auf *Weiter* und schließen Sie die Erstellung der Richtlinie ab. Durch diesen Vorgang dürfen jetzt sichere Clients, welche die Systemintegritätsprüfung bestehen, mit dem Netzwerk kommunizieren. Im Anschluss erstellen Sie eine Richtlinie für Clients, die den Zugriff nicht bestehen.

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, also *Kein Zugriff für unsichere Clients*.
2. Wählen Sie diesmal als Integritätsrichtlinie die Richtlinie *Client ist nicht sicher* aus.
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*.
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*.

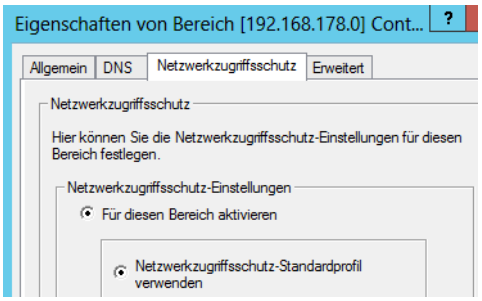
10. Schließen Sie die Erstellung der Netzwerkrichtlinien ab. Diese werden nach der Erstellung in der NPS-Konsole angezeigt. Alle anderen Richtlinien sollten als deaktiviert angezeigt werden.

Konfigurieren des DHCP-Servers für NAP

Im nächsten Schritt müssen Sie den DHCP-Server unter Windows Server 2012 konfigurieren, damit dieser NAP nutzen kann. Rufen Sie die Verwaltungskonsole des DHCP-Servers auf. Sie finden die Konsole im Server-Manager (siehe Kapitel 24). Um DHCP für NAP zu konfigurieren, gehen Sie folgendermaßen vor:

1. Rufen Sie die Eigenschaften des Bereichs auf.
2. Wechseln Sie auf die Registerkarte *Netzwerkzugriffsschutz*.
3. Aktivieren Sie die Option *Für diesen Bereich aktivieren*.
4. Aktivieren Sie die Option *Netzwerkzugriffsschutz-Standardprofil verwenden*.

Abbildg. 31.10 Konfigurieren von NAP für einen DHCP-Bereich



Im nächsten Schritt konfigurieren Sie den DHCP-Server so, dass nicht-NAP-konforme Clients eine IP-Adresse vom Server erhalten, aber besondere Einstellungen. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf *Richtlinien* und wählen Sie *Neue Richtlinie*.
2. Geben Sie der Richtlinie einen Namen, zum Beispiel *Nicht-NAP-konforme Clients*.
3. Fügen Sie auf der nächsten Seite eine neue Bedingung hinzu.
4. Wählen Sie bei Kriterien *Benutzerklasse* aus.
5. Wählen Sie als Wert *Standardmäßige Netzwerkzugriffsschutz-Klasse* und klicken Sie auf *Hinzufügen*.
6. Geben Sie eine Start- und eine Endadresse für Clients ein, die im Bereich für NAP-Clients liegt.
7. Sie können jetzt die Optionen auswählen, die Ihren nicht-NAP-konformen Clients zugewiesen werden sollen.
8. Wählen Sie die Option *006 DNS-Server* aus und hinterlegen Sie die IP-Adresse Ihres DNS-Servers.
9. Wählen Sie die Option *015 DNS-Domänenname* aus und hinterlegen Sie als Namen einen DNS-Namen, zum Beispiel *restricted.contoso.com*.

Damit die Windows-Sicherheitsintegritätsverifizierung unter Windows Server 2012 Daten empfangen kann, muss in Windows das Wartungscenter aktiviert sein. Das Sicherheitscenter oder das Wartungscenter fragt die entsprechenden Daten auf dem PC ab und sendet diese zum NPS-Server. Auf Windows Vista-Computern, die Mitglied einer Domäne sind, ist das Sicherheitscenter deaktiviert,

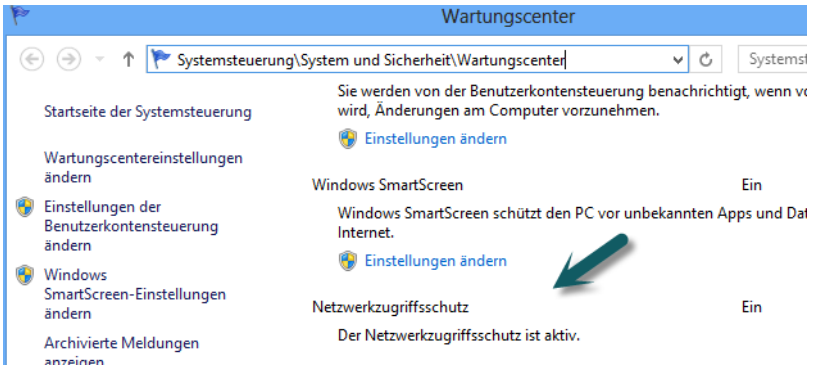
bei Windows 7 und Windows 8 ist das Wartungscenter auch bei einer Domänenmitgliedschaft aktiv. Der beste Weg dazu ist die Aktivierung über Gruppenrichtlinien. Die nächste Aufgabe, die Sie durchführen müssen, ist die Aktivierung der DHCP-NAP-Unterstützung:

1. Starten Sie dazu auf dem PC über *napclcfg.msc* die Verwaltungskonsole des NAP-Clients.
2. Klicken Sie in der Konsolenstruktur auf den Eintrag *Erzwingungsclients*.
3. Aktivieren Sie den *DHCP-Quarantäneerzwingungsclient*. Alternativ können Sie Erzwingungsclients für den Netzwerkzugriffsschutz auch über Gruppenrichtlinien aktivieren. Diese Einstellung finden Sie unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Netzwerkzugriffsschutz/NAP-Clientkonfiguration/Erzwingungsclients*.

Windows 8 an den Netzwerkzugriffsschutz anbinden

Der nächste Schritt zur Anbindung an eine NAP-Infrastruktur ist die Aktivierung des Systemdiensts *NAP-Agent* (Network Access Protection). Setzen Sie nach Aufruf der Dienstekonsole über *services.msc* den Starttyp dieses Diensts auf *Automatisch* und starten Sie diesen. Öffnen Sie das Wartungscenter, sehen Sie im Bereich *Sicherheit*, dass NAP aktiv ist.

Abbildg. 31.11 NAP ist auf dem Client aktiv



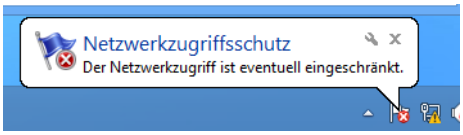
Durch die Einstellung in der Netzwerkrichtlinie, dass sich die angebundenen PCs automatisch warten sollen, wenn diese nicht NAP-konform sind, wird die Windows-Firewall immer wieder in Echtzeit automatisch aktiviert, wenn Sie diese deaktivieren. Dadurch ist sichergestellt, dass auch auf PCs, an denen 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.

Sie können testweise die Einstellung testen, indem Sie die Windows-Firewall auf dem PC deaktivieren. Dazu klicken Sie auf *Systemsteuerung/System und Sicherheit/Windows-Firewall* und dann auf *Windows-Firewall ein- oder ausschalten*. Deaktivieren Sie an dieser Stelle die Windows-Firewall für das Domänennetzwerk.

Abbildg. 31.12 Deaktivieren der Windows-Firewall für das Domänennetzwerk

Der NAP-Client bemerkt sofort das Problem und trennt den PC vom Netzwerk. Anwender erhalten auch eine entsprechende Meldung.

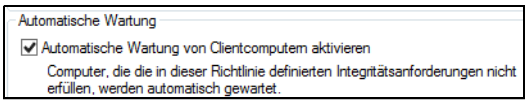
Abbildg. 31.13 Meldung des Netzwerkzugriffsschutzes bei deaktivierter Firewall



Nur wenn Sie die automatische Wartung aktiviert haben, startet der NAP-Client die Firewall neu. Ansonsten erhalten Sie nur eine Fehlermeldung und Windows schränkt den Zugriff auf Basis der hinterlegten Regeln ein.

Die automatische Wartung aktivieren Sie in der Netzwerkrichtlinie für nicht-konforme Clients, indem Sie auf der Registerkarte *Einstellungen* auf *NAP-Erzwingung* klicken und im unteren Bereich das Kontrollkästchen *Automatische Wartung von Clientcomputern aktivieren* einschalten.

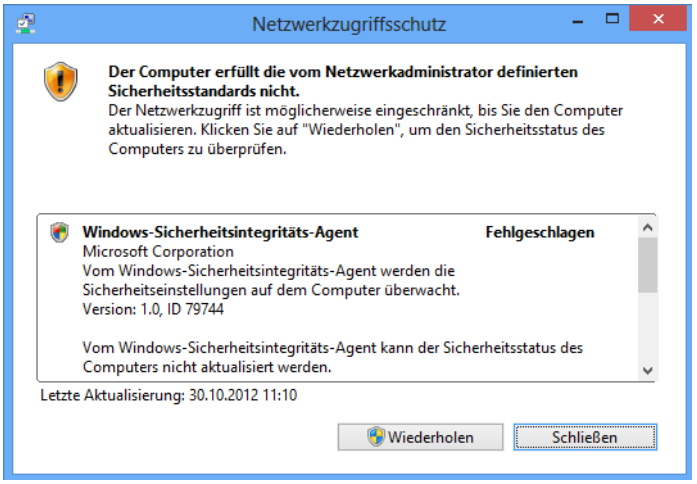
Abbildg. 31.14 NAP-Clients lassen sich automatisch warten



Klicken Sie doppelt auf die Meldung oder das dazugehörige Symbol, erhalten Sie eine ausführliche Statusangabe anzeigt, wenn der Zugriffschutz nicht mehr hergestellt werden kann. Außerdem zeigt der Netzwerkzugriffsschutz Fehler bei der Verbindung im Wartungscenter von Windows 7 und Windows 8 an, sodass Anwender auch hier einfach eine Lösung und Informationen erhalten und nicht einfach nur blockiert werden.

In den folgenden Abschnitten beschäftigen wir uns ausführlicher mit NAP, das im Zusammenhang mit dem Remotedesktopgateway in Kapitel 28 ebenfalls bereits einleitend beschrieben wurde. Neben der NAP-Funktionalität bietet ein Netzwerkrichtlinien- und Zugriffserver auch die Remoteeinwahl.

Abbildg. 31.15 Der Netzwerkzugriffsschutz erkennt, wenn ein Client nicht mehr den Voraussetzungen für einen sicheren Betrieb entspricht



Die Remote Authentication Dial-In User Service (RADIUS)-Funktion von Windows Server 2012 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 2008/2008 R2 oder Windows Server 2012 laufen.

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). Diese sendet den Statement of Health des Clients (SoH) an die HRA.
  b. Die HRA sendet die Anfrage an den Netzwerkrichtlinienserver (Network Policy Server, NPS).
  c. Der NPS gibt den Status an den HRA zurück, ob der Client konform ist oder nicht, und verweist den Client zusätzlich an die notwendigen Wartungsserver, zum Beispiel einen Server mit WSUS, von dem der Client aktuelle Patches ziehen kann.
  d. Ist der Client NAP-konform, teilt die HRA ein Zertifikat zu.

e. Ist der Client nicht konform, erhält er kein Zertifikat, sondern die Anforderung, sich mit dem Wartungsserver zu verbinden.

f. Der Client sendet eine Updateanforderung an den Wartungsserver, wenn er nicht-NAP-konform ist.

g. 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. Nichtkonforme 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 Quarantänelösung verwendet. Diese wird in Windows Server 2012 durch NAP ersetzt und ist deutlich effizienter und leichter zu konfigurieren.
- **Remotedesktopgateway** Ein Remotedesktopgateway verbindet mehrere Remotedesktopserver über HTTP/RDP-Kommunikation mit dem Internet. Diese Funktion ist neu in Windows Server 2012. Auch diese Verbindungen werden durch NAP geschützt (siehe Kapitel 28).
- **DHCP-Server** Nicht-konforme NAP-Clients können am Beziehen einer IP-Adresse durch einen DHCP-Server gehindert werden. Alternativ erhalten die Clients spezielle IP-Adressen und kein Standardgateway. DHCP-Server unter Windows Server 2012 haben bei der Konfiguration eines Bereichs für die Verwaltung von NAP eine zusätzliche Registerkarte, über die 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.

HINWEIS 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 und Windows 7 und Windows 8 unterstützt auch Cisco NAC. Für Cisco NAC muss daher kein zusätzlicher Client installiert werden. Auch die Cisco-EAP (Extensible Authentication-Protokoll)-Module werden durch Windows Update unterstützt. Neben Cisco arbeiten auch zahlreiche andere Unternehmen mit NAP zusammen (zum Beispiel Nortel, Juniper).

Die Interoperabilität sieht folgendermaßen aus:

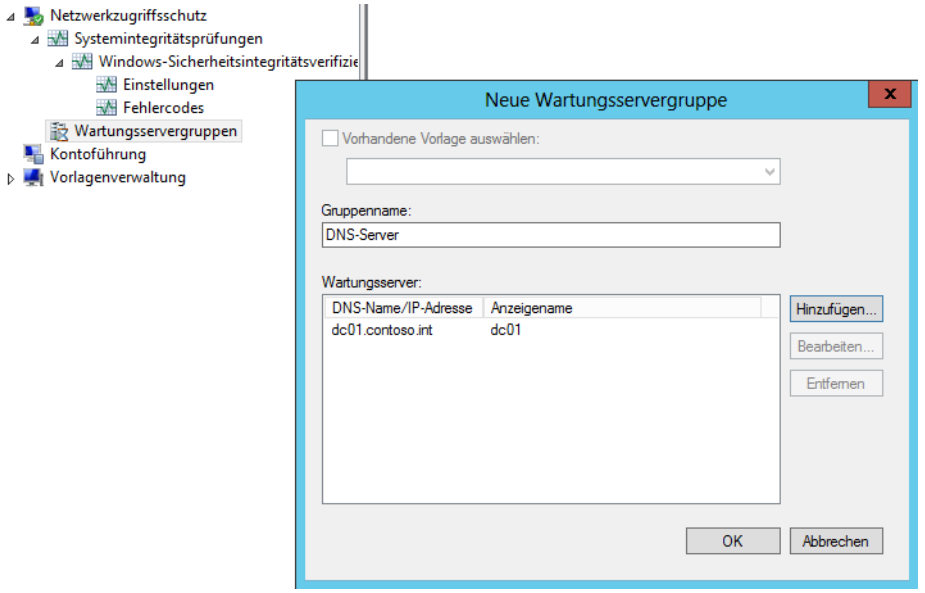
1. Der Client sendet seinen Statement of Health (SoH) an den Cisco Secure Access Control Server (ACS).
2. Der ACS sendet den SoH an den Netzwerkrichtlinienserver (Network Policy Server, NPS) weiter. Dabei wird das Host Credential Authorization-Protokoll (HCAP) verwendet.
3. Auf Basis der Richtlinien des NPS wird der Zugriff des Clients gesteuert.

Konfigurieren 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.

Sie können auch 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 Kontextmenübefehl *Neu* auf und hinterlegen Sie die Daten des DNS-Servers.

Abbildg. 31.16 Erstellen einer neuen Wartungsservergruppe



TIPP 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*. Auf dem Server finden Sie die Fehler im Systemprotokoll.

Netzwerkzugriffsschutz (NAP) mit VPN

NAP ergibt auch für Clients Sinn, die sich per VPN in das Netzwerk einwählen. Bei diesen Clients können Sie 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.

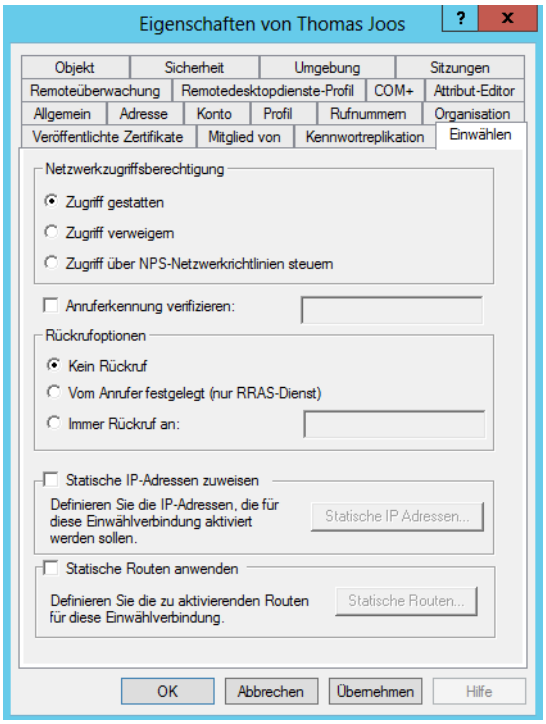
Bei der Einwahl verbindet sich der Client aus dem Internet mit dem RAS-VPN-Server. Dieser fordert wie bei DHCP ein Statement of Health (SoH) vom Client und gibt dieses an den Netzwerkrichtlinienserver weiter. Auf diesem Server werden wieder die entsprechenden Regeln angewendet, die wir bereits im vorangegangenen 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 es werden entsprechende Regeln angewendet.

Erstellen eines Benutzerkontos mit Einwahlberechtigungen

Für eine Testumgebung sollten Sie ein Beispielkonto anlegen und diesem Konto entsprechende Einwahlberechtigungen erteilen. Aktivieren Sie auf der Registerkarte *Einwählen* im Bereich *Netzwerkzugriffsberechtigung* die Option *Zugriff gestatten*.

In einer produktiven Umgebung können Sie auch die Option *Zugriff über NPS-Netzwerkrichtlinien steuern* wählen. In diesem Fall erstellen Sie eine Gruppe in Active Directory, zum Beispiel mit der Bezeichnung *VPN-Zugriff* und nehmen die Benutzerkonten in die Gruppe mit auf, denen Sie VPN-Zugriff gestatten wollen.

Abbildg. 31.17 Konfigurieren der Einwahl für ein Benutzerkonto



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 Gruppenmitglied-

schaft die Einwahl steuern. Nehmen Sie in dieser Testumgebung den Benutzer auch in die Gruppe der Domänenadministratoren auf, damit die Einwahl funktioniert und entsprechende Konfigurationen durchgeführt werden können.

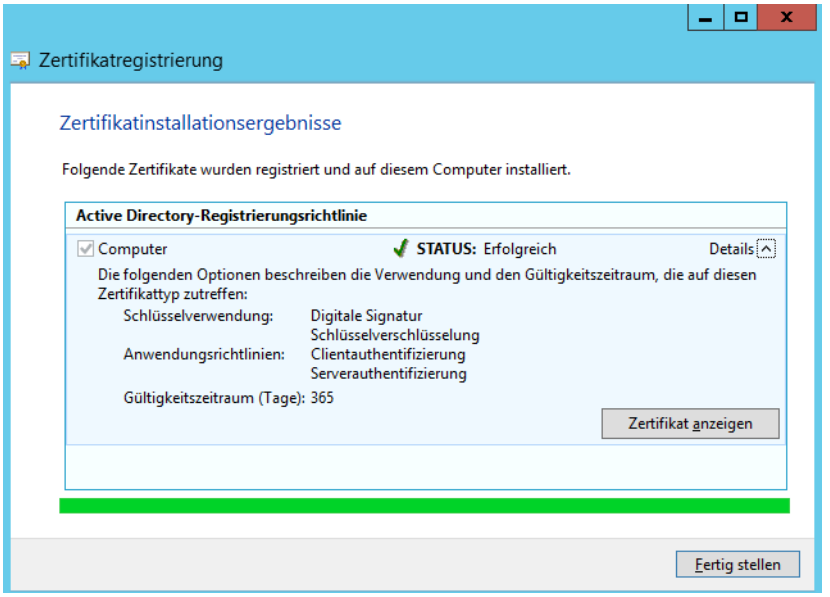
Auf Wunsch können Sie dem Anwender auch im Bereich *Statische IP-Adressen zuweisen* eine feste IP-Adresse zuteilen, die sein Rechner bei der Einwahl erhält.

Zertifikat für den NPS-Server zuweisen

Im nächsten Schritt sollten Sie dem NPS-Server ein Zertifikat zuweisen. Mehr zu diesem Thema lesen Sie auch in Kapitel 30. Gehen Sie dazu folgendermaßen vor:

1. Geben Sie auf der Startseite des NPS-Servers den Befehl *certlm.msc* ein.
2. 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.
3. 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 Computerzertifikat beherrscht. Allerdings sollten Sie den NPS- und VPN-Server am besten auf einem getrennten Server installieren.
4. Klicken Sie auf *Registrieren*, um das Zertifikat anzufordern. Nach wenigen Sekunden sollte das Zertifikat als erfolgreich ausgestellt angezeigt werden.

Abbildg. 31.18 Registrieren eines Zertifikats für den NPS-Server



Konfiguration des NPS-Servers

Im Anschluss können Sie den NPS-Server konfigurieren. Starten Sie dazu die Verwaltungskonsole für die Netzwerkrichtlinien. Als Nächstes konfigurieren Sie die Systemintegritätsprüfungen exakt so, wie weiter vorne in diesem Kapitel für NAP über DHCP erläutert. Im Anschluss erstellen Sie die Integritätsrichtlinien genauso, wie weiter vorne in diesem Kapitel für NAP über DHCP dargestellt. 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 Wartungscenter an den Server übermittelt. Auf Basis dieser Verifizierung wird der Client einer Integritätsrichtlinie zugeordnet, also zum konformen oder nicht-konformen Client erklärt. Anschließend kann eine Netzwerkrichtlinie auf Basis der definierten Integritätsrichtlinie den Zugriff steuern

Erstellen der Netzwerkrichtlinien für die VPN-Einwahl – IP-Filter

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 Integritätsrichtlinien 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.

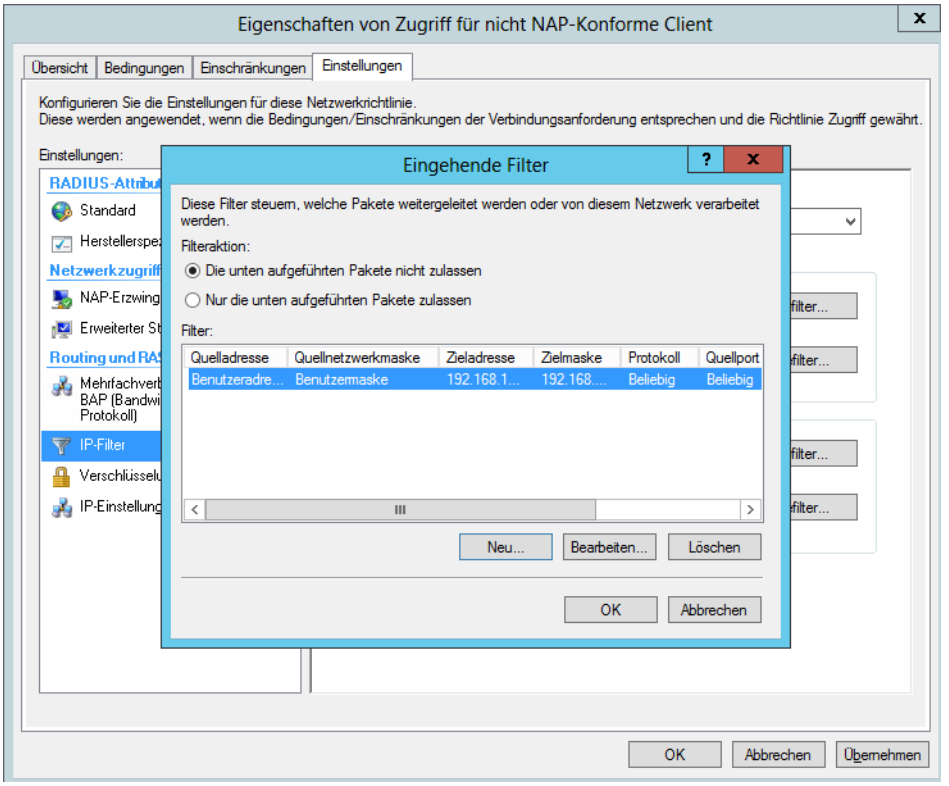
Bevor Sie neue Richtlinien erstellen, sollten Sie die standardmäßig angelegten Richtlinien zunächst deaktivieren. Klicken Sie diese dazu mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Deaktivieren* aus. Erstellen Sie die Netzwerkrichtlinie für konforme NAP-Clients genauso, wie im Abschnitt über DHCP besprochen. Sie haben jetzt jeweils eine Richtlinie, die festlegt, wann ein Client konform für das Netzwerk ist und wann nicht.

Wir zeigen Ihnen in den folgenden Abschnitten, wie Sie einen IP-Filter definieren. Mit diesem können Sie festlegen, auf welche Rechner im Netzwerk nicht-konforme Clients zugreifen dürfen. 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, da sie einen IP-Filter verwendet. Die Richtlinie für konforme Clients bleibt identisch.

1. Wählen Sie als Integritätsrichtlinie dieses Mal die Integritätsrichtlinie aus, die Sie für nicht-konforme Clients erstellt haben.
2. Bei *Typ des Netzwerkzugriffsservers* wählen Sie *RAS-Server (VPN-DFÜ)*.
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. Belassen 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.
15. Bestätigen Sie die Eingabe mit *OK*.

Abbildg. 31.19 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.

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 oder in der Reihenfolge unterhalb der Richtlinien für den VPN-Zugriff angeordnet sein.

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:

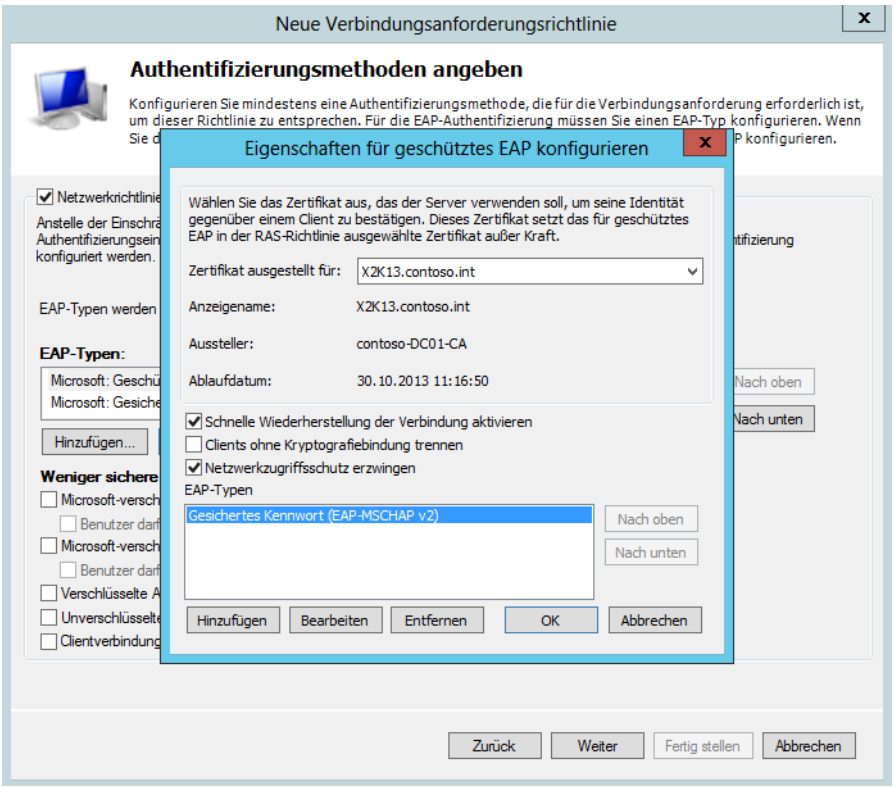
1. Deaktivieren Sie zunächst die Standardrichtlinien.
2. Erstellen Sie eine neue Richtlinie, indem Sie mit der rechten Maustaste auf *Verbindungsanforderungsrichtlinien* klicken und *Neu* wählen.
3. Geben Sie der Richtlinie einen passenden Namen, zum Beispiel *VPN-Verbindungen*.
4. Wählen Sie im Listenfeld zur Option *Typ des Netzwerkzugriffsservers* den Eintrag *RAS-Server (VPN-DFÜ)* aus.
5. Klicken Sie auf *Weiter*.
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. 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.
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*.
11. Klicken Sie auf *Weiter*.
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-Protokoll (EAP) handelt es sich um eine Erweiterung des Point-to-Point-Protokoll (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, Einmalkennwörtern, Smartcards und anderweitigen zertifikatbasierten Protokollen, wie sie in VPN (Virtual Private Network) eingesetzt werden.

Im VPN werden unterschiedliche Authentifizierungsprotokolle wie PAP, CHAP, MSCHAP oder zertifikatbasierte Protokolle unterstützt. Auch für die Datenverschlüsselung sind verschiedene Protokolle wie PPTP (Point To Point Tunnel-Protokoll) oder L2TP (Layer 2 Tunnel-Protokoll) verfügbar. Windows Server 2012 bietet von Haus aus die Unterstützung von mehreren 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 (DoS)-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*.
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 Datenaustauschs über MS-CHAP zu minimieren, unterstützt MS-CHAP v2 nicht mehr die Änderung des Kennworts 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*.
18. Stellen Sie sicher, dass das Kontrollkästchen *Netzwerkzugriffsschutz erzwingen* eingeschaltet ist.
19. Wählen Sie das Zertifikat aus, das Sie zuvor für den Server ausgestellt haben.
20. Bestätigen Sie in den restlichen Fenstern die Standardeinstellungen und schließen Sie die Erstellung der Richtlinie ab.

Abbildg. 31.20 Konfigurieren der Authentifizierung



Der nächste Schritt bei der Einrichtung von NAP über VPN ist die Konfiguration des RADIUS-Clients. Dies ist dann notwendig, 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 im Kontextmenü den Eintrag *Neu* aus.
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.
3. Aktivieren Sie noch das Kontrollkästchen *RADIUS-Client ist NAP-fähig* auf der Registerkarte *Erweitert*.
4. Hinterlegen Sie im Feld *Gemeinsamer geheimer Schlüssel* ein Kennwort und bestätigen Sie dieses.
5. Schließen Sie das Fenster mit *OK*.

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 die Rolle *Remotezugriff* auswählen. Wie Sie dabei vorgehen, lesen Sie in Kapitel 32. In Windows Server 2012 richten Sie VPN-Server und DirectAccess in einer gemeinsamen Konsole ein. Sie können Netzwerkrichtlinienserver und VPN-Server auf einem gemeinsamen Server installieren.

Testen der DirectAccess/RAS-Verbindung mit Windows 8

Die nächste Aufgabe, die Sie durchführen müssen, ist die Aktivierung der RAS-Client-NAP-Unterstützung auf dem VPN-Client:

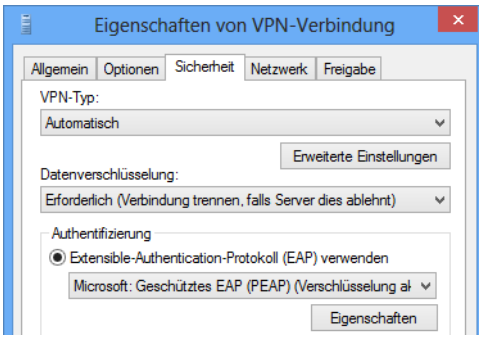
1. Starten Sie dazu auf dem PC die Verwaltungskonsole des NAP-Clients, indem Sie den Befehl *napclcfg.msc* eingeben.
2. Klicken Sie auf den Konsoleneintrag *Erzwingungsclients*.
3. Aktivieren Sie den *EAP-Quarantäneerzwingungsclient*.

Der nächste Schritt zur Anbindung von Windows 8 an eine NAP-Infrastruktur ist die Aktivierung des Systemdiensts *NAP-Agent (Network Access Protection)*. Setzen Sie den Starttyp dieses Diensts auf *Automatisch* und starten Sie diesen.

Der nächste Schritt 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:

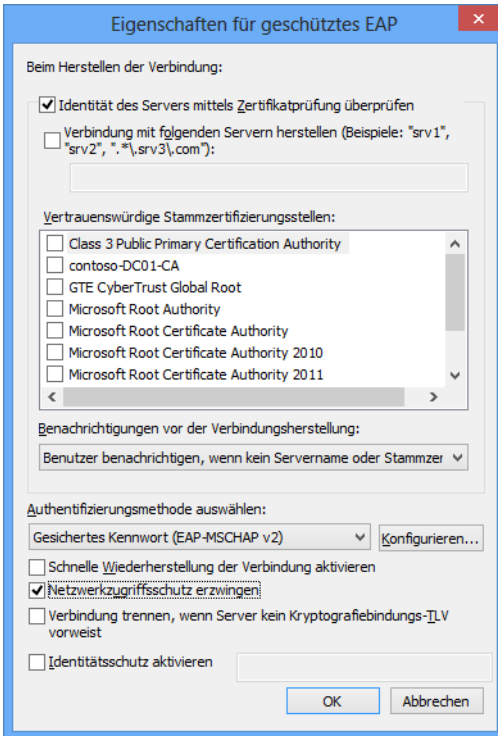
1. Sie können den Assistenten zum Aufbau einer VPN-Verbindung über den Link *Neue Verbindung oder neues Netzwerk einrichten* im Netzwerk- und Freigabecenter starten.
2. Wählen Sie im Anschluss die Option *Verbindung mit dem Arbeitsplatz* herstellen.
3. Klicken Sie zur Einrichtung einer VPN-Verbindung die Option *Die Internetverbindung (VPN) verwenden* an.
4. Als Nächstes geben Sie die IP-Adresse oder den vollständigen Namen der Verbindung an. Klicken Sie auf *Erstellen*.
5. Anschließend erstellt Windows die Verbindung und zeigt diese als bereit an. Sie finden die Einstellung über *Adaptereinstellungen ändern* im Netzwerk- und Freigabecenter.
6. Im Anschluss wird die Verbindung noch konfiguriert. Klicken Sie dazu im Netzwerk- und Freigabecenter auf den Link *Adaptereinstellungen ändern*. Dieses Konfigurationsfenster, das auch für die Konfiguration der Netzwerkverbindungen im LAN verwendet wird, können Sie auch über die Eingabe von *ncpa.cpl* starten.
7. Rufen Sie die Eigenschaften der VPN-Verbindung auf und wechseln Sie zur Registerkarte *Sicherheit*.
8. Aktivieren Sie die Option *Extensible-Authentication-Protokoll (EAP) verwenden*.
9. Wählen Sie aus dem Dropdownmenü die Option *Geschütztes EAP (PEAP) (Verschlüsselung aktiviert)* aus.
10. Klicken Sie auf *Eigenschaften*.
11. Stellen Sie sicher, dass die Option *Identität des Servers mittels Zertifikatüberprüfung* aktiviert ist.

Abbildg. 31.21 Konfigurieren der VPN-Verbindung für den EAP-Verbindungsaufbau



12. Deaktivieren Sie die Option *Verbindung mit folgenden Servern herstellen*.
13. Aktivieren Sie als Authentifizierungsmethode die Option *Gesichertes Kennwort (EAP-MSCHAP-v2)*.
14. Deaktivieren Sie die Option *Schnelle Wiederherstellung der Verbindung aktivieren*.
15. Aktivieren Sie die Option *Netzwerkzugriffsschutz erzwingen*.
16. Bestätigen Sie alle Fenster mit *OK*.

Abbildg. 31.22 Konfigurieren der VPN-Verbindung für die Unterstützung von NAP



Damit sich ein Client einwählen kann, benötigt er ein Zertifikat. Dieses kann aber vom VPN-Server nur dann ausgestellt werden, wenn das Zertifikat der Stammzertifizierungsstelle auf dem Client in die vertrauenswürdigen Stammzertifizierungsstellen integriert worden ist (siehe Kapitel 30).

Ist der Client Mitglied der Domäne, wurde diese bereits automatisch durchgeführt. Ist der Client kein Mitglied der Domäne, können Sie das Zertifikat der Stammzertifizierungsstelle 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, indem Sie *certlm.msc* starten.
2. Klicken Sie auf den Menüpunkt *Zertifikate/Vertrauenswürdige Stammzertifizierungsstellen/Zertifikate*.
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)*.
5. Im nächsten Fenster wählen Sie den Pfad aus, in dem das Zertifikat gespeichert werden soll.
6. Schließen Sie den Export des Zertifikats ab.
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 Zertifikatdatei.
9. Es öffnet sich das Zertifikat und Sie erkennen auf einen Blick, dass dieses nicht als gültig klassifiziert wird, weil Windows die Zertifizierungsstelle nicht erkennt.
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 Zertifikatspeicher 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.
15. Bestätigen Sie die Sicherheitsmeldung und lassen Sie das Zertifikat installieren.
16. Klicken Sie anschließend nochmals doppelt auf die Zertifikatdatei, sehen Sie, dass jetzt die Zertifizierungsstelle als vertrauenswürdig klassifiziert worden ist. Das Zertifikat wird anschließend auch in dem ausgewählten Zertifikatspeicher auf dem Client angezeigt.

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 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.

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 müssen auf dieser aufbauen.

Schließlich verwenden die Netzwerkrichtlinien die Integritätsrichtlinie zur Verwaltung der Clients. Alle standardmäßigen Netzwerkrichtlinien sollten deaktiviert sein. Nur Ihre manuell erstellten Richtlinie sollten aktiviert sein und sich in der Hierarchie ganz oben befinden.

Überprüfung der Clienteinstellungen

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.

Windows-Firewall und IPsec

Die Windows-Firewall lehnt jeglichen eingehenden Netzwerkverkehr ab, der nicht als Antwort auf eine Anfrage eingeht oder für den keine Ausnahme konfiguriert ist Die Firewall lässt allerdings ausgehenden Netzwerkverkehr automatisch zu. In der Verwaltungskonsole für die Windows-Firewall sind Einstellungen für IPsec (Internet Protocol Security) integriert.

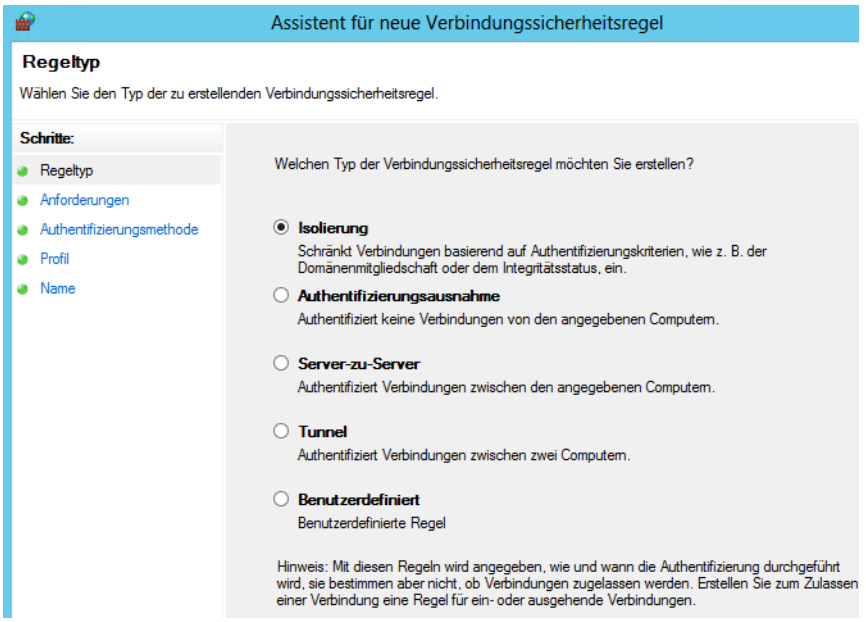
Damit können Sie eigene Verschlüsselungsregeln erstellen oder IPsec zusammen mit dem Netzwerkzugriffsschutz verwenden. Wie Sie dabei vorgehen, lesen Sie ausführlich auch im Microsoft-TechNet (*http://technet.microsoft.com/de-de/library/cc753220(WS.10).aspx* [Ms179-K31-01]).

Konfigurieren von Verbindungssicherheitsregeln

Öffnen Sie die Verwaltungskonsole für die Windows-Firewall über *wf.msc*. 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 für IPsec-Verbindungen. Sie können über den Assistenten mehrere Bedingungen für die Regel festlegen.

Erstellen Sie Gruppenrichtlinien mit integrierten Firewallregeln, können Sie diese über diese im Netz auf weitere Server verteilen. Alternativ erstellen Sie auf den einzelnen Servern manuell Regeln für IPsec. Lesen Sie sich dazu auch die Anmerkungen und Anleitungen im Microsoft-TechNet (*http://technet.microsoft.com/de-de/library/cc783420(WS.10).aspx* [Ms179-K31-02]) durch.

Abbildg. 31.23 Erstellen einer Verbindungssicherheitsregel mit der Windows-Firewall



Folgende Konfigurationen lassen sich als Basis einer Verbindungssicherheitsregel vornehmen, unabhängig davon, ob Sie diese als Richtlinie oder lokal in der Firewall-Konsole erstellen:

- **Isolierung** Legt über Active Directory oder über den Status von Computern fest, welche Computer von anderen isoliert sind. Sie müssen angeben, wann eine Authentifizierung zwischen den Computern stattfinden soll (zum Beispiel bei eingehendem oder ausgehendem Netzwerkverkehr) und ob die Verbindung geschützt sein muss oder ob dies nur angefordert wird, aber keine Voraussetzung ist. Die Isolation über den Status eines Computers nutzt den Netzwerkzugriffsschutz. Auf diesem Weg sichern Sie den Zugriff auf sensible Server auf IP-Ebene ab.
- **Authentifizierungsausnahme** Legt über die 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 ist. Sie müssen Endpunkte (IP-Adressen) bestimmen, wann die Authentifizierung stattfinden soll. Außerdem müssen Sie die Authentifizierungsmethode festlegen.
- **Tunnel** Legt eine durch einen Tunnel geschützte Verbindung fest, zum Beispiel bei Verbindungen über das Internet. Sie müssen die Tunnelendpunkte über deren IP-Adressen angeben.
- **Benutzerdefiniert** Erstellt eine frei konfigurierbare Regel, mit allen zur Verfügung stehenden Optionen für IPsec

Erstellen von IPsec-Richtlinien über Gruppenrichtlinien

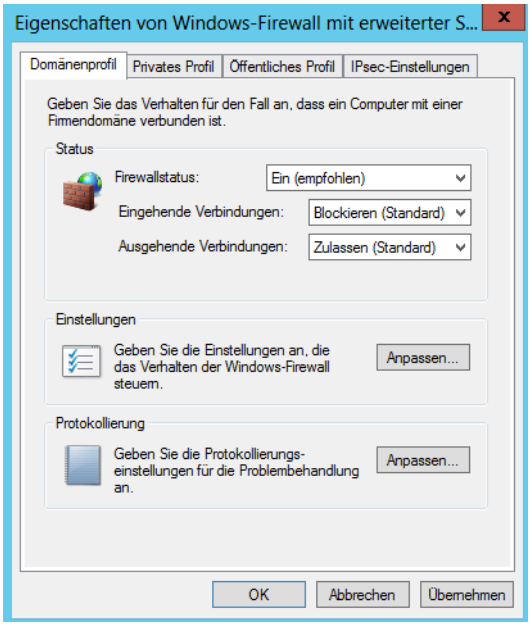
IPsec-Richtlinien können Sie entweder zusammen mit dem Netzwerkzugriffsschutz (NAP) einrichten oder als einzelne Firewallregel zwischen Servern. Wollen Sie IPsec zusammen mit NAP einsetzen, sollten Sie zunächst die NAP-Einstellungen vornehmen.

IPsec-Richtlinien erstellen Sie 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 mit der OU verknüpfen, in der Sie die Computerkonten der Server und PCs aufnehmen, die per IPsec kommunizieren können sollen:

Sie finden die notwendigen Einstellungen für IPsec in der Gruppenrichtlinienverwaltung über *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Windows-Firewall mit erweiterter Sicherheit*:

1. Rufen Sie über die rechte Maustaste die Eigenschaften von *Windows-Firewall mit erweiterter Sicherheit* auf.
2. Anschließend stehen Ihnen verschiedene Registerkarten zur Verfügung, auf denen Sie Voreinstellungen treffen. Hauptsächlich nehmen Sie die Einstellungen für die verschiedenen Netzwerkprofile der Computer vor. Sie sollten für alle Netzwerkprofile identische Einstellungen vornehmen.
3. Setzen Sie den *Firewallstatus* auf *Ein (Empfohlen)*.
4. Setzen Sie die Option für *Eingehende Verbindungen* auf *Blocken (Standard)*.
5. Setzen Sie die Option auf *Ausgehende Verbindungen* auf *Zulassen (Standard)*.
6. Führen Sie diese Einstellungen für alle drei Netzwerkprofile durch.
7. Bestätigen Sie die Eingaben mit *OK*.

Abbildg. 31.24 Aktivieren der Windows-Firewall und sicherer Verbindungen über Gruppenrichtlinien



Klicken Sie 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, wie im vorangegangenen Abschnitt besprochen.

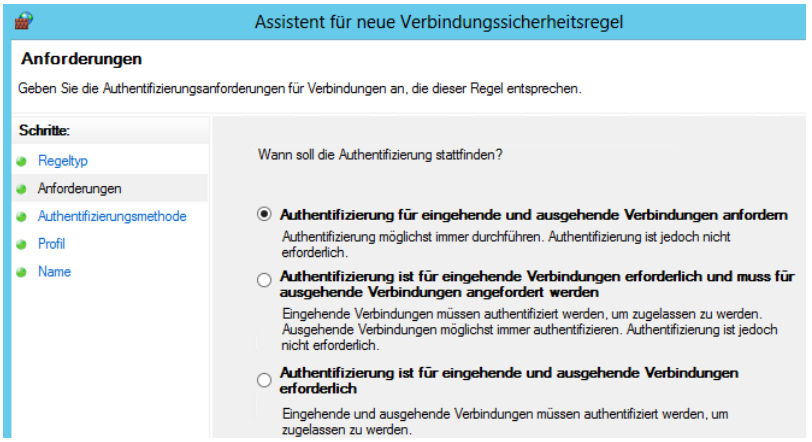
Für die Einrichtung von IPsec-Verbindungen eignen sich die Optionen *Isolierung* oder *Server-zu-Server*. Eine Isolierungsregel schränkt Verbindungen auf Grundlage der von Ihnen definierten Authentifizierungskriterien ein. Sie können Computer Ihrer Domäne von Computern außerhalb der Domäne isolieren.

Die Authentifizierungsausnahme verwenden Sie, um Computer von der Anforderung auszunehmen. Dieser Regeltyp kommt zum Einsatz, um den Zugriff auf Domänencontroller, Zertifizierungsstellen oder DHCP-Server sicherzustellen. Der Regeltyp *Server zu Server* kümmert sich um die Kommunikation zwischen zwei Computern. Mit einem Tunnel sichern Sie die Kommunikation von Computern zwischen Tunnelendpunkten ab, zum Beispiel bei virtuellen privaten Netzwerken oder L2TP-Tunneln (IPsec Layer Two Tunneling-Protokoll).

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. Sie haben hier aber alle Möglichkeiten zur Auswahl, müssen sich aber über die Konsequenzen im Klaren sein, wenn die Authentifizierung nicht funktioniert.

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 erfolgreich ist, ist auch der Datenverkehr authentifiziert. Die Option *Authentifizierung ist für eingehende und ausgehende Verbindungen erforderlich* legt fest, dass der gesamte ein- und ausgehende Datenverkehr authentifiziert ist oder Windows den Datenverkehr blockiert.

Abbildg. 31.25 Festlegen der Authentifizierung für eine IPsec-Isolierungsregel



Auf der nächsten Seite legen Sie fest, welche Art die Authentifizierung verwenden soll. Wählen Sie hier *Standard* aus. Haben Sie Als Regeltyp *Server-zu-Server* festgelegt, verwenden Sie hier *Computerzertifikat*. Die Option *Standard* legt die Authentifizierungsmethode auf Basis der Konfiguration

auf der Registerkarte *IPsec-Einstellungen* in den Eigenschaften der Windows-Firewall mit erweiterter Sicherheit fest.

Bei *Computer und Benutzer (Kerberos V5)* verwenden Sie sowohl die Computer- als auch die Benutzerauthentifizierung. Kerberos lässt sich nur verwenden, wenn der Computer und die Benutzer Mitglied einer Domäne sind. Bei *Computer (Kerberos V5)* ist die Computerauthentifizierung über Kerberos Version 5 erforderlich oder wird angefordert. *Benutzer (Kerberos V5)* ist die Benutzerauthentifizierung über Kerberos Version 5.

Aktivieren Sie die Option *Nur Integritätszertifikate akzeptieren*. Bei dieser Methode ist ein gültiges Integritätszertifikat zur Authentifizierung erforderlich oder Windows fordert dieses an. Diese Option erscheint nur bei der Auswahl des Regeltyps *Server-zu-Server*.

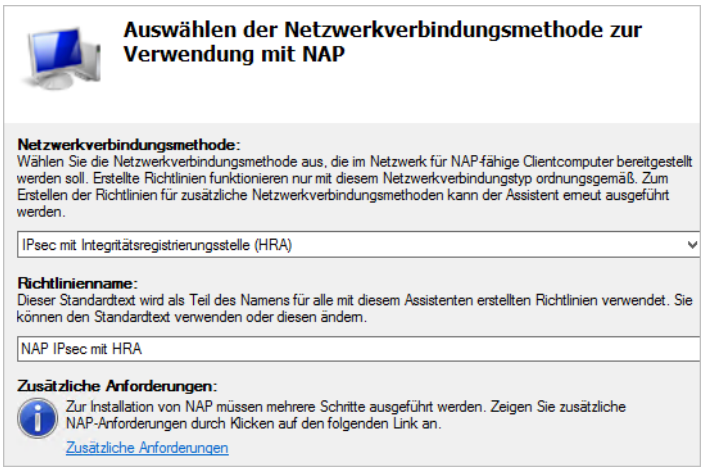
Klicken Sie auf *Durchsuchen* und wählen Sie die Root-CA aus. Aktivieren Sie auf der nächsten Seite die Regel für alle drei Netzwerkprofile. Schließen Sie die Erstellung der Regel mit der Definition der Bezeichnung ab. Die Regel wird anschließend in der Gruppenrichtlinie unter den Verbindungsregeln angezeigt.

Konfigurieren des Netzwerkrichtlinienservers für die Verwendung des Netzwerkzugriffsschutzes mit IPsec

Sie können auf Basis der Windows-Sicherheitsintegritätsverifizierung sicherstellen, welche Clients eine sichere IPsec-Verbindung aufbauen können. Diese Konfiguration führen Sie mit dem Assistenten für den Netzwerkzugriffsschutz durch. Starten Sie dazu die Verwaltung des Netzwerkrichtlinienservers. 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.
2. Wählen Sie als *Netzwerkverbindungsmethode* die Option *IPsec mit Integritätsregistrierungsstelle (HRA) aus*.

Abbildg. 31.26 Konfigurieren des Netzwerkzugriffsschutzes (NAP) über IPsec



3. Auf der nächsten Seite des Assistenten legen Sie den Netzwerkzugriffserver fest, auf dem die Integritätsregistrierungsstelle (HRA) installiert ist.
4. Als Nächstes können 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.
6. Bestätigen Sie die Optionen und schließen Sie den Assistenten ab.
7. 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.

Konfigurieren der Clients für die IPsec-Kommunikation

Die Clients im Netzwerk konfigurieren Sie so, dass die Kommunikation IPSec- und NAP-geschützt stattfinden kann. 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). Die nächste Aufgabe, die Sie durchführen müssen, ist die Aktivierung der NAP-Unterstützung auf dem Client:

1. Starten Sie dazu auf dem Computer über *napclcfg.msc* die Verwaltungskonsole des NAP-Clients.
2. Klicken Sie auf den Konsoleneintrag *Erzwingungsclients*.
3. Aktivieren Sie *Vertrauende Seite von IPsec*.

Alternativ können Sie Erzwingungsclients für den Netzwerkzugriffsschutz auch über Gruppenrichtlinien aktivieren. Diese Einstellung finden Sie unter *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Netzwerkzugriffsschutz/NAP-Clientkonfiguration/Erzwingungsclients*.

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 auf dem nächsten Fenster der Gruppe eine Bezeichnung ein. Geben Sie zum Beispiel *HRA-Server* ein.
3. Deaktivieren Sie das Kontrollkästchen *Serververifizierung (https:) ist für alle Server in dieser Gruppe erforderlich.*
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 ist sichergestellt, dass sich Clients erst authentifizieren müssen, um ein Zertifikat zu erhalten. Gelingt das nicht, verwendet Windows die zweite URL, welche ebenfalls einen anonymen Zugriff gestattet.
6. Schließen Sie die Konfiguration ab. Anschließend sollten die vertrauten Server und deren URL in der NAP-Clientverwaltungskonsole angezeigt werden.

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 Zertifikatspeicher. Hier sollte ein Zertifikat angezeigt werden, das durch die Zertifizierungsstelle ausgestellt worden ist.

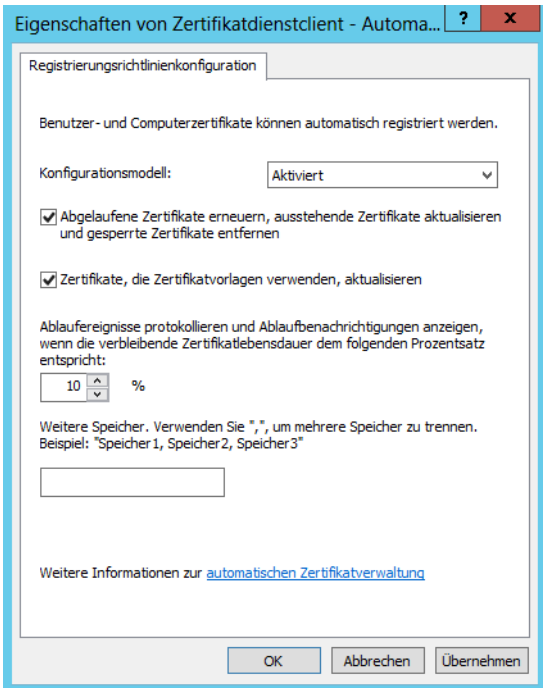
Dazu muss eine lokale Zertifizierungsstelle so eingerichtet sein, dass Sie Zertifikate für IPsec-Clients ausstellen kann. Achten Sie aber darauf, dass die Zertifizierungsstelle entsprechend konfiguriert sein muss. Wie das geht, lesen Sie im Microsoft-TechNet (*http://technet.microsoft.com/de-de/library/cc731916(WS.10).aspx* [Ms179-K31-03]).

Erstellen einer Zertifikatvorlage

Zertifikatvorlagen für IPsec erstellen Sie am besten über die Verwaltungskonsole auf dem Zertifikatserver:

1. Die Verwaltungskonsole für Zertifikatvorlagen rufen Sie über *certtmpl.msc* auf.
2. Klicken Sie mit der rechten Maustaste auf die Vorlage *Arbeitsstationsauthentifizierung* und wählen Sie im Kontextmenü den Eintrag *Vorlage duplizieren* aus.
3. Wählen Sie aus, für welche Zertifizierungsstelle das Zertifikat kompatibel sein soll.
4. Geben Sie auf der Registerkarte *Allgemein* eine passende Bezeichnung für die neue Vorlage ein, zum Beispiel *Systemintegritäts-Authentifizierung*.
5. Aktivieren Sie auf der Registerkarte *Allgemein* das Kontrollkästchen *Zertifikat in Active Directory veröffentlichen*. Wenn ein Antragsteller ein Zertifikat erhält, das auf dieser Vorlage basiert, wird das ausgestellte Zertifikat zum 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 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.
8. Klicken Sie auf *Anwendungsrichtlinien* und dann auf *Bearbeiten*.
9. Klicken Sie auf *Hinzufügen*.

Abbildg. 31.27 Konfigurieren einer neuen Zertifikatvorlage



10. Klicken Sie auf *Neu*.
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 Gruppe *NAP-Ausnahmen* auf und aktivieren Sie bei den Optionen *Automatisch registrieren* und *Registrieren* das Kontrollkästchen *Zulassen*. Diese Gruppe erstellen Sie in Active Directory und nehmen Computerkonten auf, die kein NAP verwenden sollen.
16. Klicken Sie auf *OK*, um die Eingaben abzuschließen.

Veröffentlichen der Zertifikatvorlage

Nachdem Sie die neue Vorlage für das Zertifikat erstellt haben, müssen Sie in den Zertifikatdiensten noch konfigurieren, dass diese Zertifikatvorlage für neue Zertifikate verwendet werden darf. Gehen Sie dazu folgendermaßen vor:

1. Starten Sie die Verwaltung der Zertifizierungsstelle über *certsrv.msc*.
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.

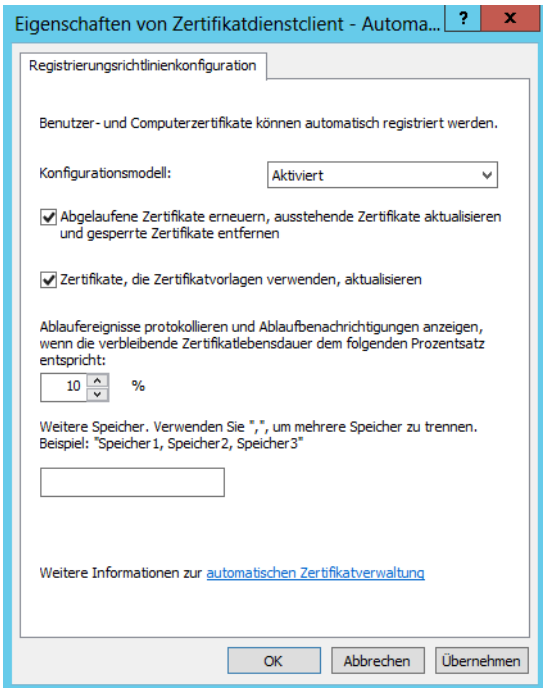
4. Wählen Sie die erstellte Zertifikatvorlage *Systemintegritäts-Authentifizierung* aus und klicken Sie auf *OK*.
5. Im Anschluss sollte die Vorlage in der Zertifizierungsstelle angezeigt werden.

Konfigurieren der automatischen Registrierung von Zertifikaten in Active Directory

Die Zertifizierungsstelle im Unternehmen sollte so konfiguriert sein, dass Sie automatisch Zertifikate ausstellt. Auf Basis dieser Zertifikate bauen Windows-Clients später die IPsec-Kommunikation auf. Für die automatische Registrierung von Zertifikaten verwenden Sie am besten die Gruppenrichtlinien:

1. Navigieren Sie zu *Computerkonfiguration/Richtlinien/Windows-Einstellungen/Sicherheitseinstellungen/Richtlinien für öffentliche Schlüssel*.
2. Klicken Sie auf der rechten Seite doppelt auf die Richtlinie *Zertifikatdienstclient – Automatische Registrierung*.
3. Setzen Sie die Richtlinie auf *Aktiviert*.
4. Aktivieren Sie zusätzlich noch die beiden Optionen *Abgelaufene Zertifikate erneuern* und *Zertifikate, die Zertifikatvorlagen verwenden, aktualisieren*.
5. Bestätigen Sie alle Fenster und schließen Sie den Editor für die Gruppenrichtlinien wieder.

Abbildg. 31.28 Konfigurieren der automatischen Registrierung von Zertifikaten



Installation einer untergeordneten Zertifizierungsstelle und einer Integritätsregistrierungsstelle

Als nächsten Schritt wird der Netzwerkrichtlinienserver (Network Policy Server, NPS) konfiguriert. Sie sollten auf dem NPS Windows Server 2012 installieren und die Rolle eines Netzwerkrichtlinienservers zuweisen.

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 Eingabeaufforderung den Befehl *gpupdate /force* ein. Die Aktualisierung der Gruppenrichtlinie sollte für die Benutzerkonfiguration und die Computerkonfiguration erfolgreich abgeschlossen werden.

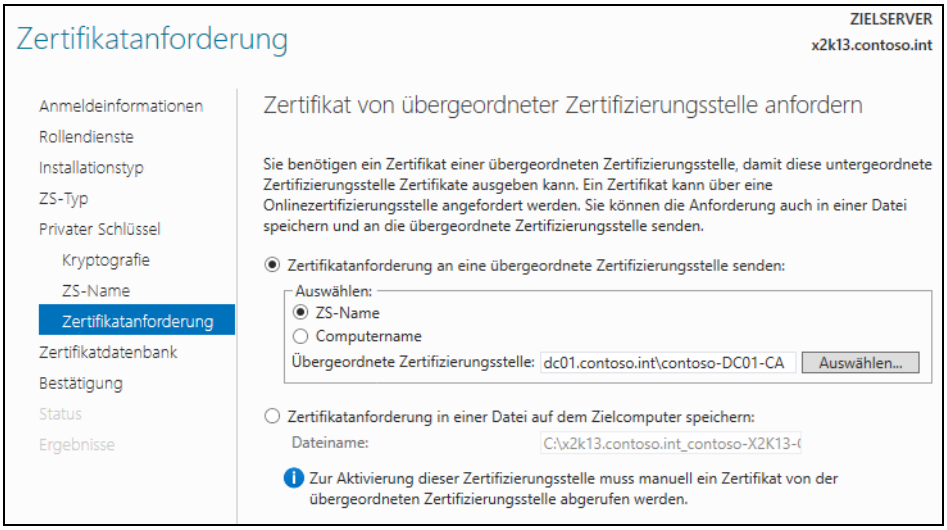
Installieren einer untergeordneten Zertifizierungsstelle auf dem Netzwerkrichtlinienserver

Zusätzlich wird auf dem NPS eine untergeordnete Zertifizierungsstelle installiert, die an die IPsec-Umgebung angepasst werden kann. Fügen Sie dazu auf dem Server neben der Rolle *Netzwerkrichtlinien und -Zugriffsdienste* auch die Rolle *Active Directory-Zertifikatdienste* hinzu.

Haben Sie auf dem Server bereits die Netzwerkrichtlinien installiert, müssen Sie den Rollendienst *Integritätsregistrierungsstelle* installieren. Installieren Sie vor diesem Rollendienst jedoch zunächst die Active Directory-Zertifikatdienste auf dem Server:

1. Installieren Sie die Active Directory-Zertifikatdienste auf dem Server und starten Sie anschließend die Einrichtung (siehe Kapitel 4 und 30).
2. Wählen Sie als Rollendienst die Option *Zertifizierungsstelle* aus.
3. Auf dem nächsten Fenster wählen Sie als Setuptyp *Eigenständige Zertifizierungsstelle* aus.
4. Auf dem nächsten Fenster wählen Sie *Untergeordnete Zertifizierungsstelle* aus.
5. Bestätigen Sie alle Fenster, bis Sie zum Fenster *Zertifikat von übergeordneter Zertifizierungsstelle anfordern* gelangen.
6. Aktivieren Sie auf diesem Fenster die Option *Zertifikatanforderung an übergeordnete Zertifizierungsstelle senden* und klicken Sie auf *Auswählen*.
7. Wählen Sie die bereits installierte Root-CA aus.
8. Schließen Sie die Installation der CA ab.

Abbildg. 31.29 Auswählen der übergeordneten Zertifizierungsstelle bei der Installation einer untergeordneten Zertifizierungsstelle



Installieren der Integritätsregistrierungsstelle

Fügen Sie nach der Installation und Einrichtung der untergeordneten CA den Netzwerkrichtlinien-Rollendienst *Integritätsregistrierungsstelle* über den Server-Manager hinzu:

1. Bestätigen Sie bei der Auswahl des Rollendiensts, dass notwendige zusätzliche Features installiert werden.
2. Wählen Sie auf dem nächsten Fenster die Option *Zertifizierungsstelle später mittels HRA-Konsole auswählen* aus.
3. Im Fenster *Authentifizierungsanforderungen* aktivieren Sie die Option *Nein, anonyme Anforderungen von Integritätszertifikaten zulassen*.
4. Bestätigen Sie alle restlichen Fenster und lassen Sie die Installation abschließen.

Konfigurieren der untergeordneten Zertifizierungsstelle

Nachdem Sie die untergeordnete Zertifizierungsstelle und die Integritätsregistrierungsstelle installiert haben, müssen Sie diese noch konfigurieren. Diese Konfiguration ist gleichzeitig eine Überprüfung der Installation:

1. Starten Sie nach der Installation die Verwaltungskonsole der Zertifikatdienste über *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 *Der Einstellungen der Zertifikatvorlage folgen, falls zutreffend. Zertifikat ansonsten automatisch ausstellen*.
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*.

Konfigurieren der Integritätsregistrierungsstelle

Nach diesen Konfigurationen müssen Sie als Nächstes die Integritätsregistrierungsstelle über deren Verwaltungsoberfläche konfigurieren. Rufen Sie das Verwaltungsprogramm *Integritätsregistrierungsstelle* im Server-Manager über *Tools* auf. Anschließend startet die Verwaltungsoberfläche der Integritätsregistrierungsstelle:

1. Klicken Sie mit der rechten Maustaste auf *Zertifizierungsstelle* und *Zertifizierungsstelle hinzufügen*.
2. Klicken Sie auf *Durchsuchen* und wählen Sie die untergeordnete Zertifizierungsstelle aus, nicht die übergeordnete Root-CA.
3. Klicken Sie anschließend nochmals auf den Konsoleneintrag *Zertifizierungsstelle* und überprüfen Sie, ob die Zertifizierungsstelle eingetragen ist.

Fehlersuche bei der Einrichtung von NAP über IPsec

Sie können mit dem Befehl *netsh nap client show configuration* die Konfiguration des NAP-Clients in der Eingabeaufforderung anzeigen lassen. Um ein neues Integritätszertifikat anzufordern, reicht es, wenn Sie den Systemdienst des NAP-Agents neu starten.

Wichtig ist, dass der Erzwingungsclient für IPsec aktiviert ist, die URLs für die vertrauenswürdige Servergruppe stimmen und der NAP-Clientdienst gestartet ist. Die aktuelle Protokolldatei für den NPS finden Sie auf dem Server im Ordner *C:\Windows\System32\LogFiles*. Hier finden Sie viele Infos, was die Arbeit des NPS transparenter macht.

Auch in den Ereignisanzeigen des NPS-Servers schreibt Windows viele Ereignisse, 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* 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:

Stellen Sie sicher, dass das Computerkonto des NPS-Servers in den Eigenschaften der Zertifizierungsstelle auf der Registerkarte *Sicherheit* eingetragen ist und über die Rechte *Zertifikate ausstellen und verwalten* und *Zertifikate anfordern* verfügt. Überprüfen Sie, ob für die Zertifizierungsstelle auf der Registerkarte *Richtlinienmodul* die automatische Registrierung aktiviert ist.

Stellen Sie sicher, dass die Objekterkennung von Zertifikatvorlagen in der Zertifikatvorlagenverwaltung auf der Registerkarte *Erweiterungen* über *Anwendungsrichtlinien/Bearbeiten/Systemintegritätsauthentifizierung/Bearbeiten* auf *1.3.6.1.4.1.311.47.1.1* gesetzt ist. Testen Sie, ob der NPS-Server, der auch als Health Registration Authority dient, ein Systemintegritätsauthentifizierungs-Zertifikat hat.

Rufen Sie zusätzlich die Eigenschaften der Richtlinie auf. Holen Sie die Registerkarte *Einschränkungen* in den Vordergrund und klicken Sie auf *Authentifizierungsmethoden*. Stellen Sie sicher, dass nur das Kontrollkästchen *Nur Computerintegritätsprüfung ausführen* aktiviert ist, keine anderen Authentifizierungsoptionen.

Sollten Sie immer noch kein Zertifikat erhalten, können Sie über die Zertifikatverwaltung des Clients durch Rechtsklick auf *Eigene Zertifikate/Alle Aufgaben/Neues Zertifikat anfordern* ein Zertifikat manuell ausstellen. Hier sollte auf jeden Fall das Zertifikat für die Systemintegritätsauthentifizie-

rung vorhanden sein. 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.

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 solange 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 verschoben werden, bevor diese Zugriff auf das Netzwerk erhalten.

Damit Sie NAP in einer 802.1x-konformen Umgebung testen können, sollten Sie sicherstellen, dass Ihr Switch diese Umgebung unterstützt und das Anlegen von virtuellen LANs ermöglicht. Abhängig von den NAP-Richtlinien unter Windows Server 2012 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 für die Clients im Netzwerk, für die Sie kein NAP verwenden wollen
- Ein VLAN für NAP-konforme Clients
- 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 mindestens auf Windows Server 2003, besser auf Windows Server 2008 oder Windows Server 2012, gesetzt wird.

Vorbereitungen für eine 802.1x-Infrastruktur mit Netzwerkzugriffsschutz

Damit Sie diese Infrastruktur aufbauen können, muss sich in der Domäne eine Zertifizierungsstelle befinden, deren Installation bereits beschrieben worden ist. Zusätzlich benötigen Sie einen Netzwerkrichtlinienserver, dem Sie auch ein Computerzertifikat zuweisen müssen:

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.

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-Netzwerkswitches. 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.
7. Aktivieren Sie im 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. 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.

9. Markieren Sie als Nächstes die Option *Microsoft: Geschütztes EAP (PEAP)* und klicken Sie auf *Bearbeiten*.
10. Stellen Sie sicher, dass die Option *Netzwerkzugriffsschutz erzwingen* aktiviert ist.
11. Wählen Sie das Zertifikat aus, das Sie zuvor für den Server ausgestellt haben.
12. 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 der Konsole diese Eigenschaften der Verifizierungsmethode auf, zum Beispiel von der standardmäßigen vorhandenen *Windows-Sicherheitsintegritätsverifizierung/Einstellungen/Standardkonfiguration*.
3. 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 dem Switch in verschiedene VLANs zugeordnet werden, abhängig davon, ob diese NAP-konform sind oder nicht-NAP-konform.

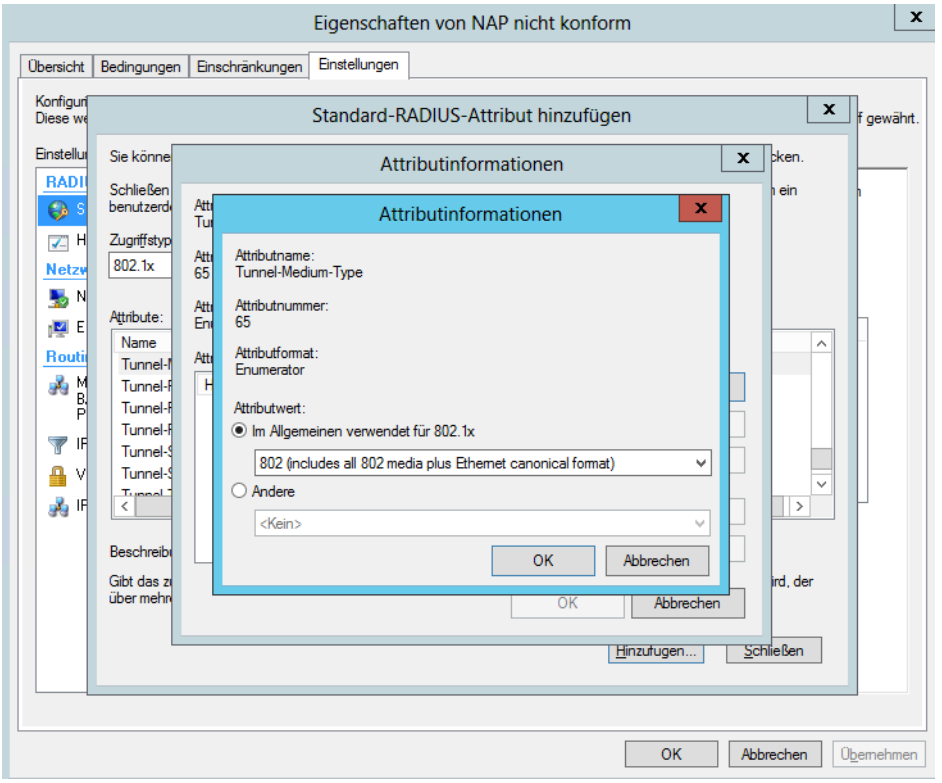
Erstellen der Netzwerkrichtlinie für nicht konforme und konforme NAP-Clients

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-Attribute* (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. 31.30 Windows Server 2012 fit für NAP über 802 machen



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 dem Switch handeln, mit dem die nicht-konformen Clients verbunden werden. Für NAP-konforme Clients verwenden Sie die ID 3. Die ID 1 auf dem 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.
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 Ihres Switchs 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.

Zusammenfassung

In diesem Kapitel haben Sie erfahren, wie Sie mit dem Netzwerkzugriffsschutz bereits mit einem einzelnen Windows Server 2012-Computer im Netzwerk Arbeitsstationen unter Windows 7 und Windows 8 vor der Verbindung abprüfen können. Diese neue Sicherheitsfunktion ist vor allem für Unternehmen interessant, die Außendienstmitarbeiter über ein Remotedesktopgateway anbinden oder die eine hochsichere Umgebung zur Verfügung stellen wollen.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie Arbeitsstationen mit Windows 7 und Windows 8 und Windows Server 2012 mit der neuen DirectAccess-Funktion per VPN oder das Internet mit dem Netzwerk verbinden.

Kapitel 32

Remotezugriff mit DirectAccess und VPN

In diesem Kapitel:

Mit Windows Server 2008 R2 hatte Microsoft DirectAccess eingeführt. Mit dieser Technik konnten Sie PCs mit Windows 7 über das Internet direkt mit dem Unternehmensnetzwerk verbinden, ohne dass Sie Zusatzsoftware einsetzen mussten. Für den Verbindungsaufbau ist kein VPN notwendig. Nach der ersten Einrichtung erkennt ein DirectAccess-PC automatisch die Verbindung, verschlüsselt sie und kann sich mit dem Netzwerk verbinden. Auch Gruppenrichtlinien lassen sich über diesen Weg ausliefern.

Nachteil von DircectAccess in Windows Server 2008 R2 war die komplizierte Einrichtung und die verschiedenen Verwaltungswerkzeuge, die Administratoren nutzen mussten. Beides hat Microsoft in Windows Server 2012 optimiert. Die Einrichtung ist deutlich einfacher und für die Verwaltung von Remotezugriff und DirectAccess gibt es nur noch eine einzelne Konsole. Remotezugriff und DirectAccess lassen sich jetzt daher gemeinsam verwalten und es gibt keine Konflikte mehr beim parallelen Einsatz der Systeme. DirectAccess in Windows Server 2012 funktioniert vor allem zusammen mit Windows 8 optimal und ist einfach einzurichten.

Ansonsten haben Unternehmen weiterhin den Vorteil, den DirectAccess bereits in Windows Server 2008 R2 bietet: Clientcomputer lassen sich effizient auch über das Internet sicher am Netzwerk anbinden, ohne dass Anwender erst VPN-Verbindungen aufbauen müssen. Der Datenzugriff funktioniert, Gruppenrichtlinien lassen sich anwenden und Software-Updates verteilen. Die Kommunikation erfolgt über IPv6. Ist dies mit der aktuellen Datenverbindung nicht möglich, kapselt das Betriebssystem die IPv6-Pakete in IPv4-Pakete und versendet sie an die Zielserver.

In Windows Server 2012 und Windows 8 hat Microsoft in diesem Zusammenhang auch einige Neuerungen eingeführt, welche Windows 8-Clients die DirectAccess-Anbindung erleichtern:

- Sie können nur Windows 8 Enterprise und Windows 7 Ultimate/Enterprise mit DirectAccess nutzen. Optimal arbeitet nur Windows 8 Enterprise mit DirectAccess von Windows Server 2012 zusammen.
- Die Verbindung zwischen Client und Server erfolgt nur noch mit IP über HTTPS. Alle anderen Technologien werden nicht mehr unterstützt.
- Sie benötigen keine zwei öffentlichen IP-Adressen mehr
- Eine Zertifizierungsstelle und deren Einrichtung ist nur noch optional, nicht mehr zwingend notwendig. DirectAccess-Server arbeiten jetzt wesentlich besser mit Kerberos und Active Directory zusammen.
- Windows Server 2012 erfordert keine IPv6-Anpassungen mehr, sondern richtet notwendige Einstellungen automatisch ein

Remotezugriff installieren und einrichten – Erste Schritte

Die Installation von DirectAccess und dem Remotezugriff erfolgt über den Server-Manager. Über *Verwalten/Rollen und Funktionen hinzufügen/Remotezugriff* installieren Sie die notwendigen Funktionen auf dem Server. Weitere Einstellungen, wie noch in Windows Server 2008 R2, sind zur Installation nicht notwendig. Sie installieren auf diesem Weg nur die notwendigen Systemdateien auf dem Server.

Remotezugriff in Windows Server 2012 – Die Grundlagen

In Windows Server 2012 sind DirectAccess und RRAS-VPN (Routing und RAS-Dienst) zu einer einzigen Remotezugriffsrolle zusammengefasst und werden in einer gemeinsamen Oberfläche verwaltet. Clientcomputer, auf denen Windows 8 und Windows 7 ausgeführt wird, können Sie als DirectAccess-Clientcomputer konfigurieren. Diese Clients können über DirectAccess auf interne Netzwerkressourcen zugreifen, ohne sich über eine VPN-Verbindung einzuloggen. Andere Clientcomputer können per VPN eine Verbindung zum internen Netzwerk herstellen, aber kein DirectAccess nutzen.

DirectAccess-Clientcomputer im Internet können von Remotezugriffsadministratoren über DirectAccess verwaltet werden, auch wenn sich die Clientcomputer nicht im internen Unternehmensnetzwerk befinden. Mehrere RAS/DirectAccess-Server lassen sich über eine einzelne Remotezugriffs-Verwaltungskonsole verwalten.

Die Remotezugriffsrolle wird über den Server-Manager oder die PowerShell installiert. Die Rolle umfasst DirectAccess (bisher ein Feature unter Windows Server 2008 R2) sowie die Routing- und RAS-Dienste (bisher ein Rollendienst unter der Serverrolle für Netzwerkrichtlinien- und Zugriffsdienste). Die Remotezugriffsrolle besteht aus zwei Komponenten:

- **DirectAccess und Routing- und RAS-Dienste (RRAS) VPN** DirectAccess und VPN werden gemeinsam in der Remotezugriffs-Verwaltungskonsole verwaltet
- **RRAS-Routing** RRAS-Routingfeatures werden in der Vorgängerversion der Routing- und RAS-Konsole verwaltet

Die RAS-Serverrolle ist von den folgenden Serverrollen/-features abhängig:

- **Internetinformationsdienste-Webserver (Internet Information Services, IIS)** Dieses Feature ist erforderlich, um den Netzwerkadressenserver auf dem RAS-Server und den Standardwebtest zu konfigurieren
- **Interne Windows-Datenbank** Wird zur lokalen Kontoführung auf dem Remotezugriffsserver verwendet
- **Feature Tools für die Remotezugriffsverwaltung** Die Tools zur Verwaltung, also die Remotezugriffs-Verwaltungskonsole und die PowerShell-Cmdlets, können Sie auch auf Servern oder PCs installieren, auf denen Sie kein RAS betreiben, aber verwalten wollen (siehe Kapitel 3)

Auf dem RAS-Server muss mindestens ein Netzwerkadapter installiert, aktiviert und mit dem internen Netzwerk verbunden sein. Werden zwei Adapter verwendet, sollte ein Adapter mit dem internen Unternehmensnetzwerk und der andere mit dem externen Netzwerk (Internet oder privates Netzwerk) verbunden sein.

HINWEIS Es können nur die folgenden Betriebssysteme als DirectAccess-Clients verwendet werden: Windows Server 2012, Windows Server 2008 R2, Windows 8 Enterprise, Windows 7 Enterprise und Windows 7 Ultimate.

Der Remotezugriffsserver muss Domänenmitglied sein. Der Server kann an der Schwelle zum internen Netzwerk oder geschützt durch eine Edgefirewall oder ein anderes Gerät bereitgestellt werden. Wird der RAS-Server durch eine Edgefirewall oder ein NAT-Gerät geschützt, muss das Gerät so konfiguriert sein, dass ein- und ausgehender Datenverkehr für den RAS-Server zugelassen wird.

Der Anwender, der den Remotezugriff auf dem Server einrichtet, muss lokale Administratorberechtigungen für den Server und Benutzerberechtigungen für die Domäne besitzen. Zusätzlich benötigt der Administrator Berechtigungen für die Gruppenrichtlinien, die bei der DirectAccess-Bereitstellung verwendet werden. Um die Features nutzen zu können, die die DirectAccess-Bereitstellung auf mobile Computer beschränken, ist die Berechtigung zum Erstellen von WMI-Filtern für den Domänencontroller erforderlich.

DirectAccess-Clients müssen Domänenmitglieder sein. Domänen, die Clients enthalten, können zur selben Gesamtstruktur gehören wie der Remotezugriffsserver oder eine bidirektionale Vertrauensstellung mit der Remotezugriffsserver-Gesamtstruktur oder -Domäne verwenden. Eine Active Directory-Sicherheitsgruppe wird benötigt, um die Computer aufzunehmen, die als DirectAccess-Clients konfiguriert werden.

Geben Sie beim Konfigurieren der DirectAccess-Clienteinstellungen keine Sicherheitsgruppe an, wird das Client-Gruppenrichtlinienobjekt standardmäßig auf alle Notebooks in der Sicherheitsgruppe *Domänencomputer* angewendet.

Die Active Directory-Domäne muss mit mindestens einem Windows Server 2008 R2-, Windows Server 2008- oder Windows Server 2012-basierten Domänencontroller betrieben werden. Arbeitsgruppen werden nicht unterstützt. Wenn der Windows Server 2012-RAS-Server kein Domänenmitglied ist, kann der Prozess zum Beitreten einer Domäne mit dem Assistenten für erste Schritte aufgerufen werden. Dafür ist ein Neustart des Servers erforderlich. Die Installation wird nach dem Neustart automatisch fortgesetzt.

Die DirectAccess-Konfiguration kann nur von einem Domänenbenutzer mit lokalen Administratorrechten für den DirectAccess-Server durchgeführt werden. Das verwendete Konto muss außerdem Mitglied der Gruppe *Konten-Operatoren* sein oder dem Konto muss die zum Erstellen von Sicherheitsgruppen in Active Directory geeignete Berechtigung übertragen werden. Außerdem sind Berechtigungen zum Erstellen und Bearbeiten von Gruppenrichtlinienobjekten in der Domäne, zum Verknüpfen von Gruppenrichtlinienobjekten mit der Domäne und zum Anwenden von WMI-Filterberechtigungen beim Übernehmen von DirectAccess-Richtlinien für Notebooks erforderlich.

DirectAccess ist eine IPv6-abhängige Anwendung. Daher dürfen die IPv6- und IPv6-Übergangstechnologien auf dem RAS-Server nicht deaktiviert sein und die IPv6-Übergangstechnologien dürfen durch Gruppenrichtlinien nicht deaktiviert werden. Die Active Directory-Domäne muss erreichbar sein.

Vorbereiten der Installation von DirectAccess und Remotezugriff

Passen Sie die Netzwerkadapter auf dem DirectAccess-Server an. Wenn Sie zwei Adapter verwenden, verbinden Sie die Schnittstelle zum internen Netzwerk und die Schnittstelle zum Internet und konfigurieren Sie die entsprechenden IP-Adressen. Benennen Sie auch die Namen der Netzwerkverbindungen entsprechend.

ACHTUNG Konfigurieren Sie kein Standardgateway auf Intranetschnittstellen beim Einsatz von DirectAccess-Server und fügen Sie den DirectAccess-Server Ihrer Domäne hinzu.

Für die Installation von DirectAccess sind anschließend drei Schritte notwendig:

1. **Installieren der RAS-Serverrolle**

   Die RAS-Serverrolle fasst das DirectAccess-Feature und den RRAS-Rollendienst in einer neuen, einheitlichen Serverrolle zusammen. Diese neue Remotezugriffsserver-Rolle ermöglicht die zentrale Verwaltung, Konfiguration und Überwachung sowohl von DirectAccess- als auch von VPN-basierten Remotezugriffsdiensten.

2. **Konfigurieren von DirectAccess**

   Der neue Assistent für erste Schritte sorgt für eine Vereinfachung der Konfiguration.

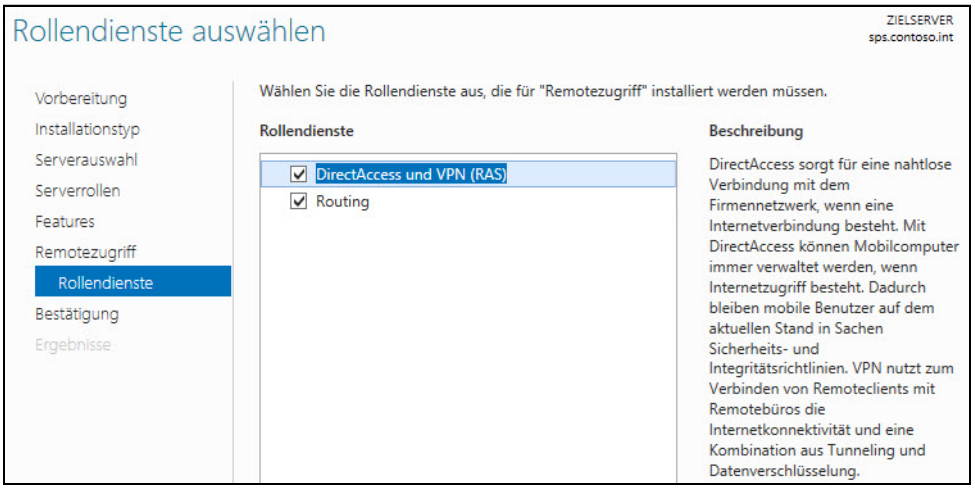
3. **Aktualisieren von Clients mit der DirectAccess-Konfiguration**

   Zum Verwenden der DirectAccess-Einstellungen müssen Clients die Gruppenrichtlinien aktualisieren, während sie mit dem Intranet verbunden sind. Anschließend können diese eine Verbindung per DirectAccess auch über das Internet herstellen.

Rollendienste installieren und Remotezugriff aktivieren

Starten Sie im Server-Manager *Verwalten/Rollen und Features hinzufügen* und installieren Sie die Rolle *Remotezugriff*. Auf der Seite *Rollendienste auswählen* können Sie festlegen, ob der Server als Router oder als Remotezugriffsserver mit RAS und DirectAccess funktionieren soll. Es wird nicht mehr zwischen DirectAccess und RAS unterschieden, die Installation erfolgt immer parallel.

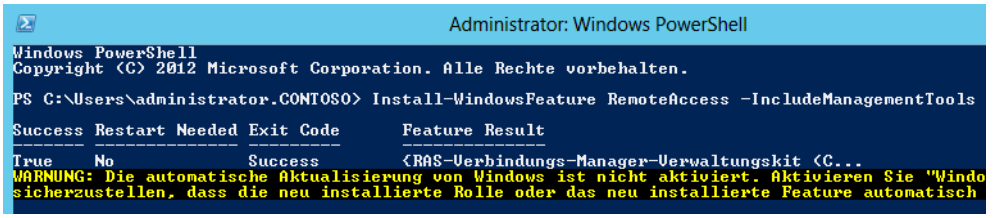
Abbildg. 32.1 Installieren von DirectAccess und VPN über den Server-Manager



TIPP Sie können den Remotezugriff auch über die PowerShell installieren. Dazu verwenden Sie den folgenden Cmdlet-Aufruf:

Install-WindowsFeature RemoteAccess –IncludeManagementTools

Abbildg. 32.2 Installieren des Remotezugriffs in der PowerShell



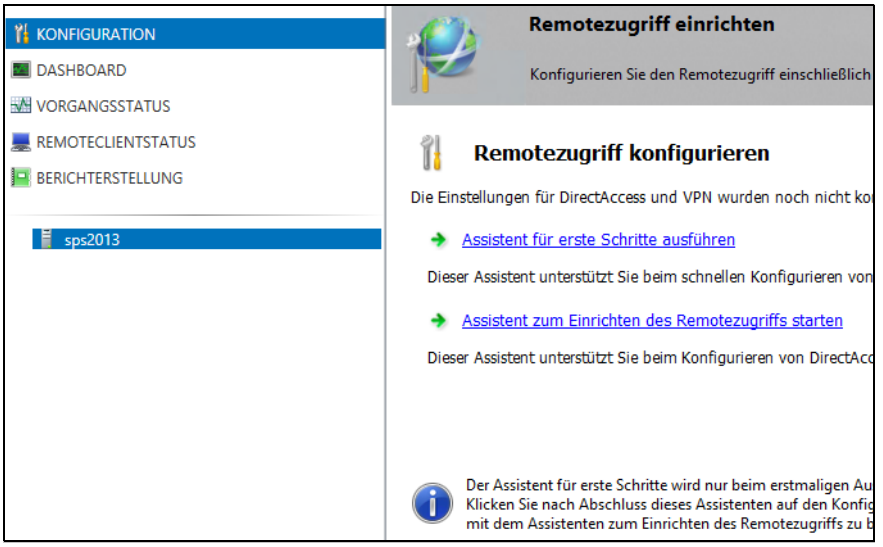
DirectAccess und VPN-Zugang einrichten

Nach der Installation findet sich im Server-Manager die neue Gruppe *Remotezugriff*. Über das Kontextmenü der hier integrierten Server lässt sich die Verwaltung des Remotezugriffs starten. Über eine gemeinsame Konsole findet dann die Einrichtung der beiden Funktionen statt.

Nach der Installation erscheint im Server-Manager auch die Meldung, dass eine Konfiguration für den Serverdienst erforderlich ist. Über die Meldung starten Sie den Assistenten für die erste Einrichtung. Dieser führt komplett durch alle Schritte der Einrichtung.

Sie können den Assistenten auch über die Remotezugriffs-Verwaltungskonsole starten. Diese finden Sie im Menüpunkt *Tools* des Server-Managers. Auch hier starten Sie den Assistenten zur Einrichtung.

Abbildg. 32.3 Starten des Assistenten zur Einrichtung von DirectAccess



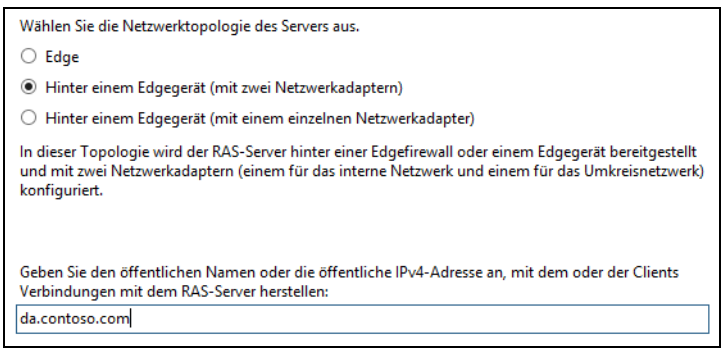
Wählen Sie am besten den Link *Assistent für erste Schritte ausführen*. Dieser fragt nur die wichtigsten Optionen ab und richtet die Funktion ein. Sie können anschließend immer noch Änderungen vornehmen.

Der Assistent ermöglicht die Auswahl, ob auf dem Server DirectAccess und/oder RAS genutzt werden soll. Der parallele Weg ist von Microsoft der empfohlene.

Abbildg. 32.4 Einrichten von DirectAccess und Remotezugriff

Wählen Sie die Topologie Ihrer Netzwerkkonfiguration aus und geben Sie den öffentlichen Namen ein, mit dem Remotezugriffclients eine Verbindung herstellen sollen. Klicken Sie auf *Weiter*. Nach der Auswahl prüft der Assistent zunächst die Voraussetzungen und startet danach die Einrichtung. Auf der ersten Seite wählen Sie aus, wo der Server positioniert ist und wie der Zugriff auf den Server erfolgen soll.

Abbildg. 32.5 Auswählen der Netzwerktopologie für die Einrichtung von DirectAccess

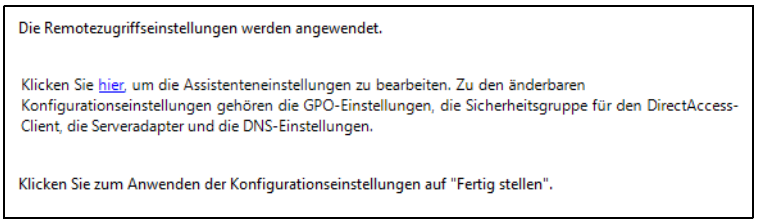


Achten Sie nach der Einrichtung darauf, die Firewallregeln zu überprüfen, die DirectAccess auf dem Server einrichtet. Dies gilt vor allem, wenn Sie die Einrichtung nur mit einer einzelnen Netzwerkkarte vornehmen. In diesem Fall ist der DirectAccess-Server unter Umständen per RDP erreichbar

und auch IIS 8.0 ist im Internet verfügbar. Sie können die Einstellungen aber in der Firewall des Servers steuern, nachdem Sie DirectAccess eingerichtet haben.

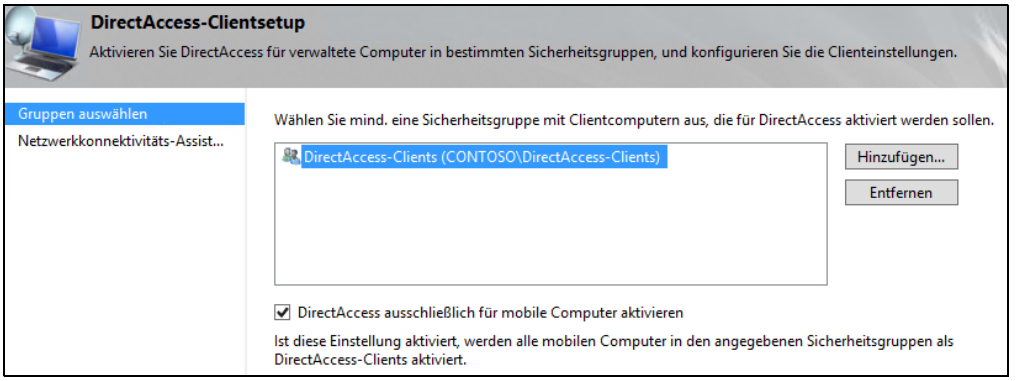
Standardmäßig stellt der Assistent für erste Schritte DirectAccess für Laptops und Notebookcomputer in der Domäne bereit, indem er einen WMI-Filter auf das Gruppenrichtlinienobjekt für die Clienteinstellungen anwendet. Klicken Sie an dieser Stelle aber noch nicht auf *Fertig stellen*, sondern auf den Link *hier*, um Einstellungen anzupassen.

Abbildg. 32.6 Anpassen der notwendigen Einstellungen für DirectAccess vor dem Fertigstellen des Assistenten



Standardmäßig erlaubt der Einrichtungs-Assistent den Zugriff per DirectAccess für alle Domänencomputer. Diese Einstellung sollten Sie möglichst anpassen und eine eigene Sicherheitsgruppe erstellen. Computer, deren Konten Sie in diese Gruppe aufnehmen, dürfen sich dann mit DirectAccess verbinden. Andere Computer dürfen das nicht.

Abbildg. 32.7 Anpassen der DirectAccess-Gruppe



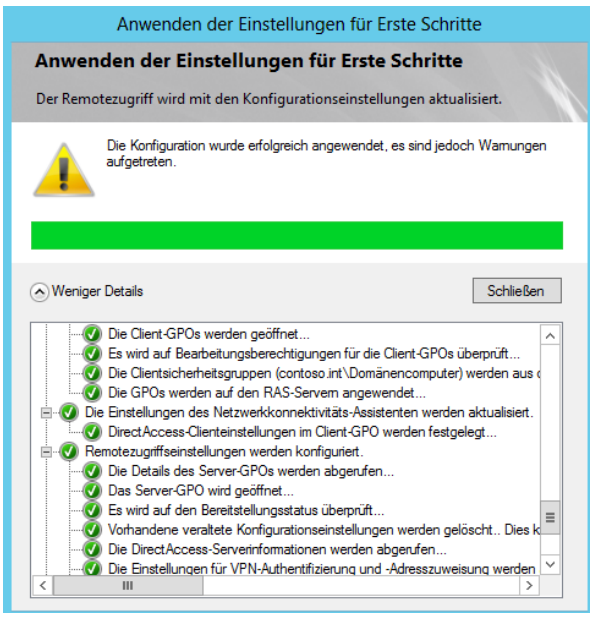
Standardmäßig erstellt der Assistent automatisch WMI-Filter für die Gruppenrichtlinien von DirectAccess, die den Zugriff nur für Notebooks oder andere mobile Computer erlaubt. Sie können den Haken an dieser Stelle aber entfernen, da Sie den Zugriff ohnehin schon für einzelne Computer über die Sicherheitsgruppe einschränken.

Passen Sie die Einstellungen an, können Sie neben der Sicherheitsgruppe für DirectAccess auch noch die Gruppenrichtlinien anzeigen, die für den Betrieb notwendig sind. Hier sollten Sie aber keine Einstellungen anpassen.

Abbildg. 32.8 Anpassen der Sicherheitsgruppe und der Gruppenrichtlinien vor der Einstellung

Lassen Sie anschließend den Assistenten seine Arbeit beenden. Nach der ersten Einrichtung können Sie in der Verwaltungskonsole weitere Maßnahmen durchführen. Wenn der Assistent die Einrichtung erfolgreich abschließt, erhalten Sie entsprechende Meldungen und können die Einrichtung überprüfen. Warnungen zeigt der Assistent auch an. Hier sollten Sie in den Details überprüfen, wo das Problem liegt.

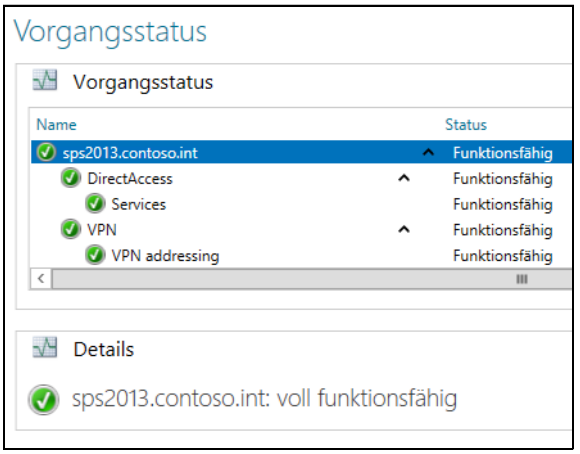
Abbildg. 32.9 Erfolgreiche Einrichtung von DirectAccess mit Warnungen



Nach der Einrichtung startet der Assistent die bereits von Windows Server 2008 R2 bekannte Oberfläche zur Einrichtung.

Klicken Sie in der Konsolenstruktur der Remotezugriffs-Verwaltungskonsole auf *Vorgangsstatus*. Warten Sie, bis der Status aller Monitore *Funktionsfähig* lautet. Klicken Sie danach im Bereich *Aufgaben* unter *Überwachung* auf *Aktualisieren*, um die Anzeige zu aktualisieren.

Abbildg. 32.10 Erfolgreiche Einrichtung des Remotezugriffs überprüfen



Aktualisieren von Clients mit der DirectAccess-Konfiguration

Haben Sie DirectAccess eingerichtet, sollten Sie die Clients aktualisieren, die sich mit DirectAccess verbinden sollen. Rufen Sie zunächst die Gruppenrichtlinien für den Client ab. Geben Sie dazu in der Eingabeaufforderung *gpupdate /force* ein. Mehr zu diesem Thema lesen Sie auch in Kapitel 19.

Warten Sie, bis die Computerrichtlinien erfolgreich aktualisiert wurden, und geben Sie in der PowerShell *Get-DnsClientNrptPolicy* ein. Die Einträge in der Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) für Direct Access werden angezeigt. Der Assistent für erste Schritte hat diesen DNS-Eintrag für den DirectAccess-Server automatisch erstellt und ein zugehöriges selbstsigniertes Zertifikat bereitgestellt, sodass der DirectAccess-Server als Netzwerkadressenserver fungieren kann.

Geben Sie *Get-NCSIPolicyConfiguration* ein. Die vom Assistenten bereitgestellten Einstellungen für die Statusanzeige der Netzwerkkonnektivität werden angezeigt. Achten Sie auf den Wert von *DomainLocationDeterminationURL*. Sobald auf diese Netzwerkadressenserver-URL zugegriffen werden kann, ermittelt der Client, dass sich diese innerhalb des Unternehmensnetzwerks befindet, und die NRPT-Einstellungen werden nicht angewendet.

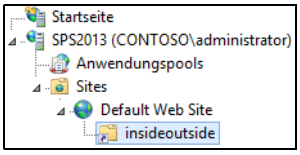
Abbildg. 32.11 Überprüfen von DirectAccess nach der Einrichtung auf dem Client

```
PS C:\Users\administrator> Get-NCSIPolicyConfiguration

Description                    : NCSI Configuration
CorporateDNSProbeHostAddress   : fd05:f3fb:3151:7777::7f00:1
CorporateDNSProbeHostName      : directaccess-corpConnectivityHost.contoso.int
CorporateSitePrefixList        : {fd05:f3fb:3151:1::/64, fd05:f3fb:3151:7777::/96, fd05:f3fb:3151:1000::1/128,
                                 fd05:f3fb:3151:1000::2/128}
CorporateWebsiteProbeURL       : http://directaccess-WebProbeHost.contoso.int
DomainLocationDeterminationURL : https://DirectAccess-NLS.contoso.int:62000/insideoutside
```

Geben Sie *Get-DAConnectionStatus* ein. Wenn der Client die Netzwerkadressenserver-URL erreichen kann, wird der Status *ConnectedLocally* angezeigt.

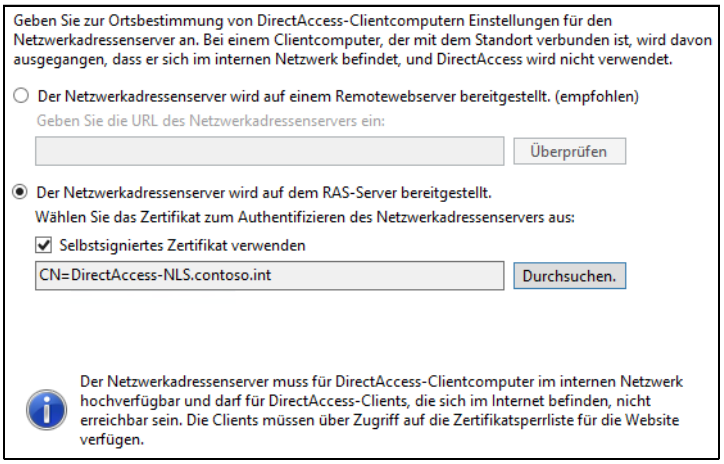
Diesen Status ruft der DirectAccess-Client vom Infrastruktur-Server ab. Er verwendet dazu die Internetinformationsdienste auf dem DirectAccess-Server.

Abbildg. 32.12 DirectAccess nutzt den IIS auf dem Infrastrukturserver, um zu testen, ob der Client intern oder extern verbunden ist



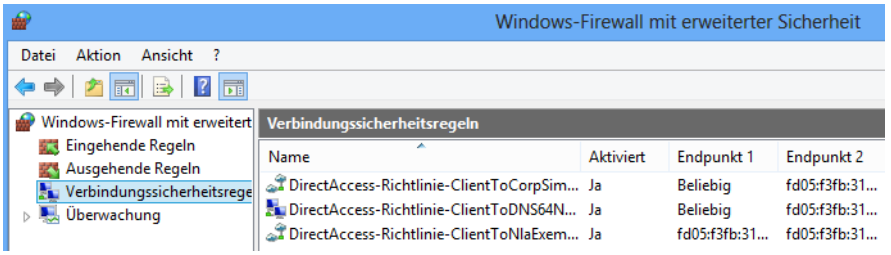
Sie können die entsprechenden Einstellungen über die Verwaltungskonsole anpassen. Klicken Sie dazu im Bereich *Infrastrukturserver-Setup* auf *Bearbeiten*. Hier können Sie den Server und das dazugehörige Zertifikat auswählen.

Abbildg. 32.13 Anpassen des Infrastrukturservers



Clients, die per DirectAccess verbunden sind, finden Sie über den Link *Remoteclientstatus* in der Remotezugriffs-Verwaltungskonsole. Sie können in der Konsole auch Berichte erstellen, um die Nutzung des Servers zu messen. Die Gruppenrichtlinien für die Anbindung an DirectAccess erstellen auch Firewallregeln und Verbindungssicherheitsregeln. Diese lassen Sie über *wf.msc* auf dem Client anzeigen.

Abbildg. 32.14 Anzeigen der Verbindungssicherheitsregeln auf den Clients



Während der Einrichtung legt der Assistent auch DNS-Einträge fest, mit denen er überprüfen kann, ob sich Clients im internen Netzwerk befinden oder mit DirectAccess einwählen. Verbindet sich ein Client mit DirectAccess, sehen Sie die Verbindung, wenn Sie auf das Netzwerksymbol klicken.

Abbildg. 32.15 Anzeigen des DirectAccess-Verbindungsstatus

Überprüfen der Bereitstellung

Im vorangegangenen Abschnitt haben wir bereits besprochen, wie Sie DirectAccess auf dem Client testen. Sobald die HTTPS-Verbindung zum Netzwerkadressenserver (Infrastruktur-Server) erfolgreich hergestellt wurde, deaktiviert der DirectAccess-Client die DirectAccess-Clientkonfiguration und verwendet eine direkte Verbindung zum Unternehmensnetzwerk.

Verbinden Sie einen Clientcomputer mit Ihrem Unternehmensnetzwerk und melden Sie sich mit einem Domänenbenutzernamen an. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und rufen Sie den Befehl *ipconfig /all* auf. Im Abschnitt *Tunneladapter iphttpsinterface* sehen Sie, ob die Verbindung intern oder über DirectAccess erfolgt.

Abbildg. 32.16 Überprüfen der Verbindung über DirectAccess

```
Tunneladapter iphttpsinterface:

   Medienstatus. . . . . . . . . . . . : Medium getrennt
   Verbindungsspezifisches DNS-Suffix:
   Beschreibung. . . . . . . . . . . . : Microsoft-IP-HTTPS-Plattformadapter
   Physische Adresse . . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP aktiviert. . . . . . . . . . . : Nein
   Autokonfiguration aktiviert . . . . : Ja
```

Geben Sie in der PowerShell *Get-DAConnectionStatus* ein. Der Status sollte als *ConnectedRemotely* angegeben werden. In diesem Fall sind Sie mit DirectAccess verbunden. Sie erkennen sie auch, wenn Sie im Desktop auf das Netzwerksymbol klicken. Auch hier sehen Sie den Status der Verbindung. Für *Arbeitsbereichverbindung* muss der Status *Verbunden* angegeben sein. Dabei handelt es sich um den Standardverbindungsnamen, der vom DirectAccess-Assistenten angegeben wird. Sie können während der Einrichtung aber auch einen eigenen Namen angeben.

Geben Sie in der PowerShell *Get-NetIPAddress* ein, um die IPv6-Konfiguration zu prüfen. Kontrollieren Sie, ob der Tunneladapter *iphttpsinterface* aktiv ist und über eine gültige IP-HTTPS-Adresse verfügt. Ihr Client verwendet IP-HTTPS für das Tunneling von IPv6-Datenverkehr zum DirectAccess-Server über das Internet.

Geben Sie *wf.msc* ein. Erweitern Sie *Überwachung* und dann *Sicherheitszuordnungen*, um die festgelegten IPsec-Sicherheitszuordnungen zu prüfen. Es müssen die Authentifizierungsmethoden *Computer (Kerberos)* und *Benutzer (Kerberos)* verwendet werden. Der Client nutzt den Kerberosproxy, der vom DirectAccess-Assistenten automatisch bereitgestellt wird. Wählen Sie im Konsolenbaum *Verbindungssicherheitsregeln*, um die zugeordneten Richtlinien zu prüfen, die angewendet werden.

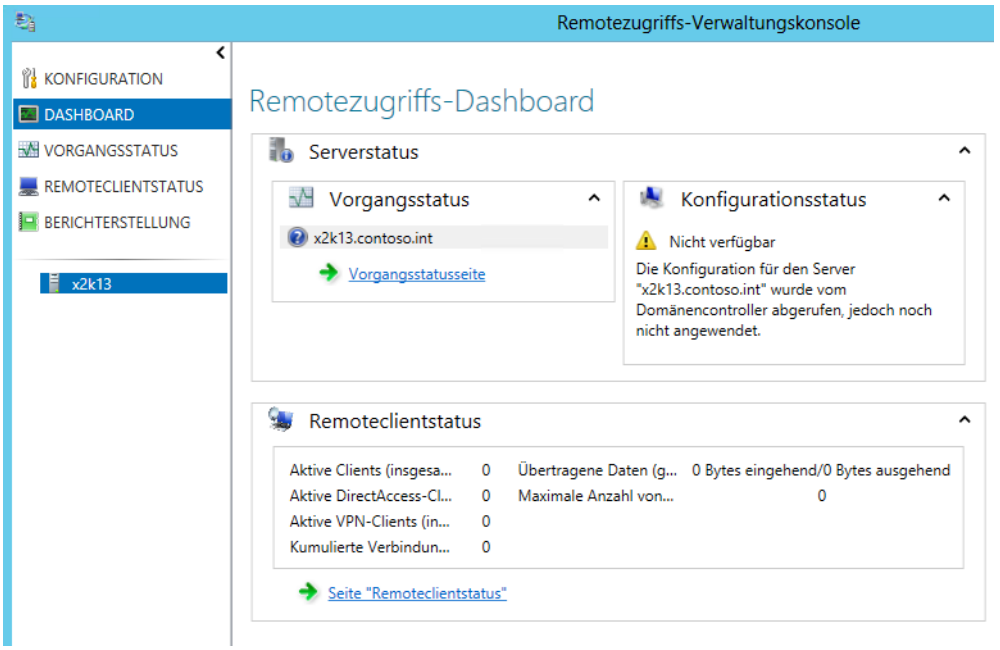
Remotezugriff verwalten

Unabhängig davon, ob Sie DirectAccess oder den Remotezugriff mit VPN/DFÜ nutzen, findet die Verwaltung in Windows Server 2012 über die Remotezugriffs-Verwaltungskonsole statt. Diese finden Sie direkt im Server-Manager. Schließen Sie den Assistenten zur Einrichtung ab. Dieser integriert die notwendigen Einstellungen, erstellt Gruppenrichtlinien und ändert Einstellungen auf dem Server.

Nach der ersten Einrichtung lässt sich die Remotezugriffs-Verwaltungskonsole öffnen. Hier können Sie auch jederzeit Änderungen vornehmen. Die Konsole lässt sich auch über das Kontextmenü der Remotezugriffsserver im Server-Manager starten.

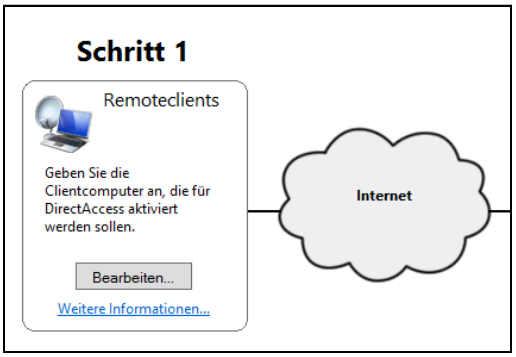
Über die Kategorie *Konfiguration* auf der linken Seite ändern Sie Einstellungen. Durch einen Klick auf die entsprechende Schaltfläche im mittleren Bereich können Sie verschiedene Einstellungen anpassen.

Abbildg. 32.17 Die neue Verwaltungskonsole für Remoteverbindungen in Windows Server 2012



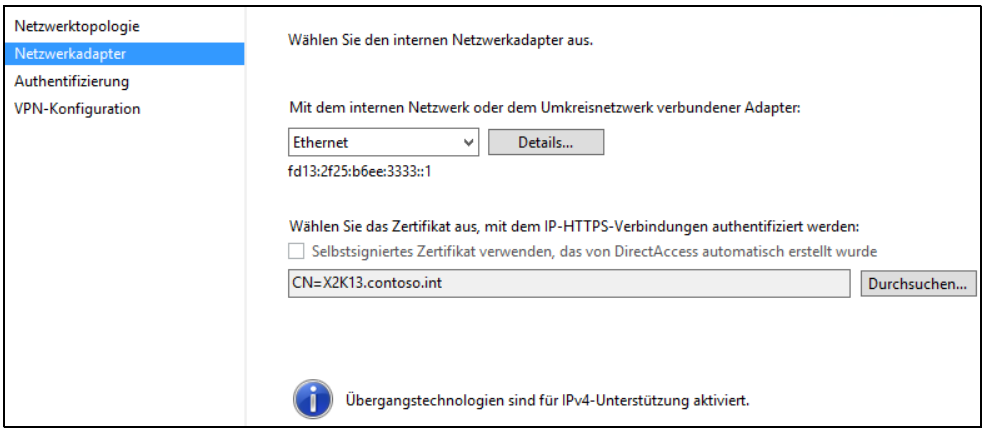
Über *Remoteclients* legen Sie fest, welche Benutzer und Clientcomputer sich mit dem Netzwerk verbinden dürfen. Hier bietet es sich an, mit Gruppen aus Active Directory zu arbeiten und diese im Assistenten zu hinterlegen. Standardmäßig dürfen alle Benutzer von extern eine Verbindung aufbauen. Hier ist eine eigene Active Directory-Gruppe besser geeignet.

Abbildg. 32.18 Festlegen der Remoteclients für den Zugriff auf das Netzwerk



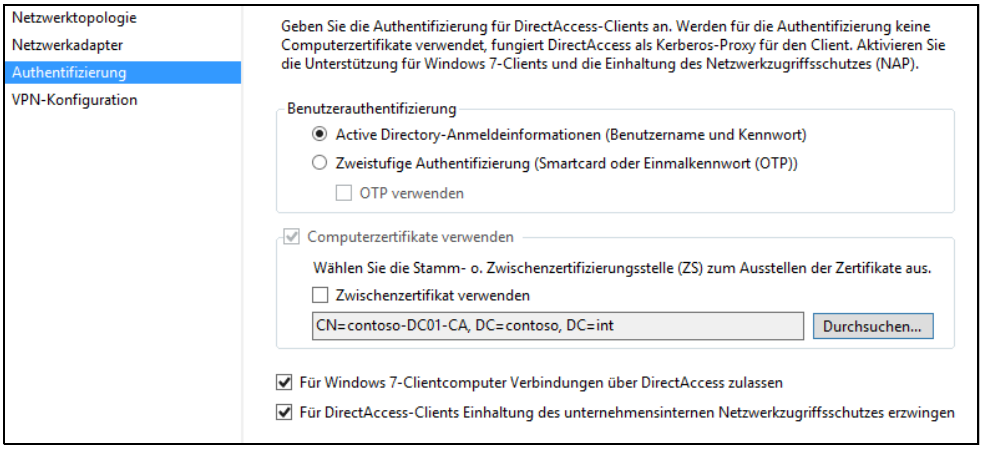
Über den Assistenten lassen sich WMI-Filter hinterlegen und in den Einstellungen des RAS-Servers in der Mitte die Einstellungen ändern, die bei der Einrichtung über den Assistenten vorgenommen wurden. DirectAccess kann mit internen Zertifizierungsstellen arbeiten oder mit selbst signierten Zertifikaten, was die Einrichtung vereinfacht. Besser ist eine Zertifizierungsstelle auf Basis der Active Directory-Zertifikatdienste (siehe Kapitel 30).

Abbildg. 32.19 RAS im Assistenten für den Remotezugriff einrichten



Über die Einrichtung des Servers legen Sie die Art der Authentifizierung fest. An dieser Stelle müssen Sie auch die Verbindung von Windows 7-Computern genehmigen, wenn außer Windows 8 auch noch Clients mit dem älteren Betriebssystem Zugriff erhalten sollen. Standardmäßig lässt DirectAccess in Windows Server 2012 nur Windows 8-Computer zu. Hier aktivieren Sie auch die Unterstützung des Netzwerkzugriffschutzes mit DirectAccess (siehe Kapitel 31).

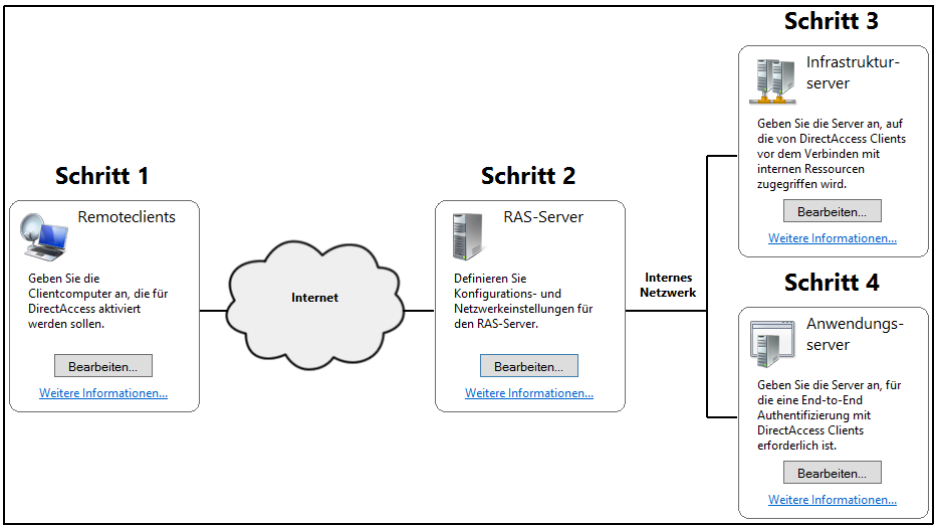
Abbildg. 32.20 Auswählen der Authentifizierung für Clients



Die notwendigen Einstellungen für Clientcomputer nimmt der Assistent über Gruppenrichtlinien vor. Deren Einstellungen lassen sich in der Gruppenrichtlinienverwaltung anpassen. Auch für die Einstellungen der DirectAccess-Server sind Gruppenrichtlinien verantwortlich. In den erweiterten Firewalleinstellungen finden sich auf dem DirectAccess-Server ebenfalls Einstellungen für die Verbindung. Die Einstellungen lassen sich auch in der PowerShell überprüfen. Dabei hilft zum Beispiel das Cmdlet *Get-NetTeredoConfiguration*.

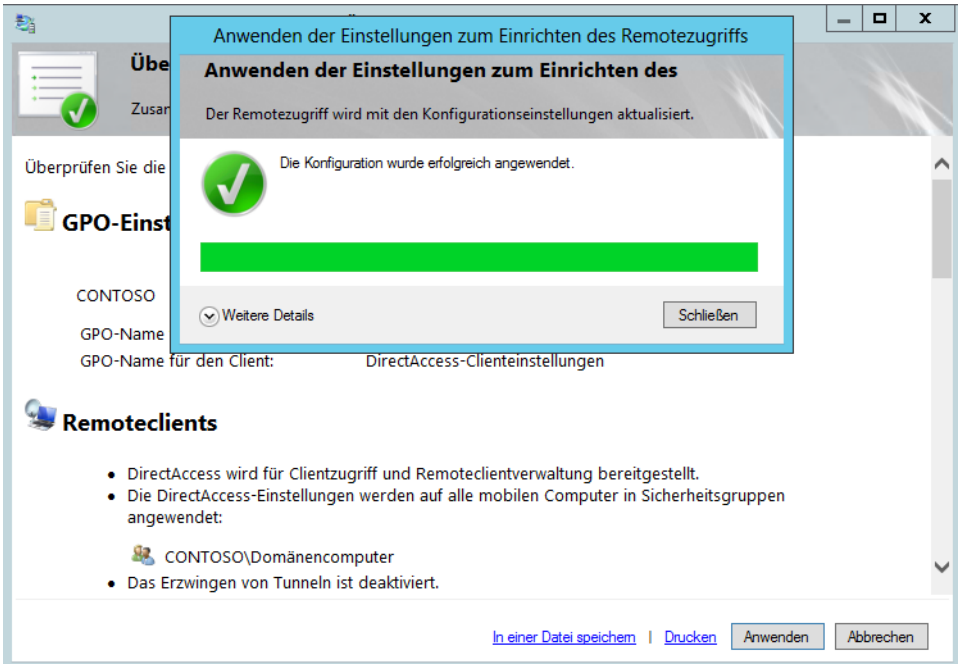
Die Einstellungen können Sie jederzeit anpassen. Dazu rufen Sie die Remotezugriffs-Verwaltungskonsole auf und klicken auf den DirectAccess/VPN-Server, den Sie verwalten wollen.

Abbildg. 32.21 Nachträgliches Bearbeiten des Remotezugriffs



Haben Sie alle Einstellungen vorgenommen, klicken Sie unten im Fenster auf *Fertig* und dann auf *Anwenden*, damit der Assistent die Einstellungen übernimmt. Im Fenster sehen Sie die Änderungen, die der Assistent vornimmt, und ob die Einstellungen erfolgreich übernommen wurden. Überprüfen Sie danach auch immer über den Link *Vorgangstatus*, ob alles noch funktioniert.

Abbildg. 32.22 Erfolgreiche Einrichtung von DirectAccess und des Remotezugriffs



Routing und RAS verwalten

Windows Server 2012 arbeitet aber nicht nur mit der neuen Remotezugriffs-Verwaltungskonsole, sondern auch mit der klassischen Routing- und RAS-Konsole. Auch hier können Sie weiterhin Einstellungen vornehmen und zum Beispiel Konfigurationen von PPTP anpassen sowie Clients steuern.

Verwalten und Konfigurieren der RAS-Benutzer und RAS-Ports

Eine einfache Methode, um mit Windows Server 2012 ein VPN aufzubauen, ist der Einsatz von PPTP. Dieser Verbindungstyp ist zwar nicht so sicher wie L2TP oder IPsec, ist aber dennoch für viele Unternehmen sinnvoll.

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.

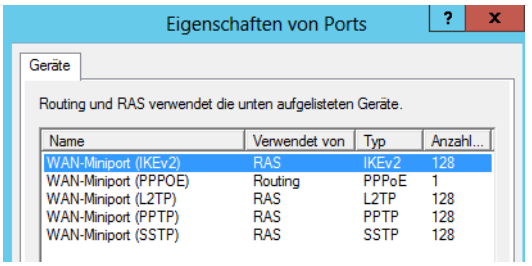
Viele Experten stufen PPTP mittlerweile als sicher ein, auch wenn die Verschlüsselung nicht so stark ist wie die von L2TP. PPTP ermöglicht die verschlüsselte Einkapselung von verschiedenen Netzwerkprotokollen und unterstützt Schlüssellängen bis zu 128 Bit. Nachdem die Authentifizierung durchgeführt wurde, 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.

Eine weitere Variante, ein VPN aufzubauen, ist das Layer 2 Tunnel-Protokoll (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 VPNs 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 VPNs auf Basis von L2TP setzt eine Zertifizierungsstellen-Infrastruktur 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 funktioniert. Für den schnellen, effizienten und sicheren Aufbau eines VPNs ist PPTP sicherlich die beste Wahl.

Sie können die Konfiguration im Server-Manager über *Tools/Routing und RAS* überprüfen. Öffnen Sie dieses Snap-In, sehen Sie die Konfigurationen, die der Assistent auf dem Windows Server 2012 durchgeführt hat. 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.

Klicken Sie mit der rechten Maustaste auf den Eintrag *Ports*, können Sie die Anzahl der Ports und damit der gleichzeitig möglichen Einwahlen definieren. 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 und die Einwahlmöglichkeiten in diesem Bereich komplett deaktivieren.

Abbildg. 32.23 Konfiguration der Einwählports unter Windows Server 2012



HTTPS-VPN über Secure Socket Tunneling-Protokoll

Windows Server 2012 und Windows 8 unterstützen neben PPTP und L2TP auch das Secure Socket Tunneling-Protokoll (SSTP) für die VPN-Einwahl. Mit diesem Protokoll wird ein VPN auf Basis von HTTPS aufgebaut, welches viel leichter durch Firewalls und NAT-Geräte 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 Remotezugriff eingehende Verbindungen überwacht. Es können jedoch gleichzeitig sowohl Remotezugriff 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.

Ablauf beim Verbinden über SSTP

Wenn ein Benutzer auf einem Computer, der Windows Server 2012 Windows 8 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 SSTP-Serverzertifikats.
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. Das 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 entsprechen.

   Der RAS-Client und der RAS-Server tauschen Nachrichten entsprechend des ausgehandelten Authentifizierungsprotokolls aus. Wenn EAP (Extensible Authentication-Protokoll) 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 2012 migriert werden. Es reicht der Einsatz eines VPN-Servers mit Windows Server 2012. Auf den Clients muss Windows Vista, Windows 7 und Windows 8 installiert sein. Die Berechtigung für die Einwahl der Benutzer erfolgt identisch zu den Berechtigungen über andere VPN-Methoden. Benutzern müssen nur die entsprechenden Rechte zugewiesen werden.

Vorbereiten der Installation von SSTP – Zertifizierungsstelle vorbereiten

Damit SSTP verwendet werden kann, muss der Rollendienst *Zertifizierungsstellen-Webregistrierung* der Rolle *Active Directory-Zertifikatdienste* installiert sein (siehe Kapitel 30). Der beste Weg ist, wenn Sie auf dem VPN-Server selbst eine Zertifizierungsstelle installieren und zwar als Typ *Eigenständig*, keine *Unternehmenszertifizierungsstelle*. Richten Sie zuerst die Zertifizierungsstelle ein und installieren Sie danach über den Server-Manager noch den Rollendienst *Zertifizierungsstellen-Webregistrierung*.

Die Zertifizierungsstelle muss außerdem als Stammzertifizierungsstelle installiert sein. Alle weiteren Einstellungen wählen Sie so, wie in Kapitel 30 besprochen. Für eine Testumgebung und auch für die meisten Produktivumgebungen verwenden Sie einfach die Standardeinstellungen.

Sicherheitseinstellungen im Internet Explorer auf dem VPN-Server konfigurieren

Nachdem die Zertifizierungsstelle auf dem Server installiert ist, müssen Sie auf dem VPN-Server noch das Serverzertifikat installieren, über welches das SSTP-VPN ermöglicht wird. Da der Internet Explorer von Windows Server 2012 sehr strenge Sicherheitseinstellungen aufweist, müssen Sie zunächst in den Optionen des Internet Explorers Änderungen vornehmen:

1. Starten Sie den Internet Explorer.
2. Drücken Sie die Alt-Taste und klicken Sie auf *Extras/Internetoptionen*.
3. Wechseln Sie zur Registerkarte *Sicherheit*.
4. Klicken Sie auf *Lokales Intranet* und stellen Sie sicher, dass die Sicherheitsstufe auf *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 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:

1. Geben Sie auf der Startseite *certlm.msc* ein.
2. Klicken Sie anschließend mit der rechten Maustaste auf *Eigene Zertifikate/Zertifikate* und wählen Sie *Alle Aufgaben/Neues Zertifikat anfordern*.
3. Bestätigen Sie den Assistenten.
4. Klicken Sie auf der Seite *Zertifikatregistrierung* auf *Weiter*.
5. Wählen Sie *Computer* als Zertifikat aus und klicken Sie auf *Registrieren*.

Wird bei Ihnen kein Zertifikat angezeigt, müssen Sie auf dem Zertifikatserver in einer MMC das Snap-In *Zertifikatvorlagen* laden:

1. Klicken Sie mit der rechten Maustaste auf das Zertifikat *Computer* und rufen Sie die *Eigenschaften* auf.
2. Wechseln Sie auf die Registerkarte *Sicherheit*.
3. Klicken Sie auf *Authentifizierte Benutzer* oder *Domänen-Admins*, je nachdem, wem Sie das Recht zum Registrieren ermöglichen möchten.
4. Klicken Sie bei dem Recht *Registrieren* auf *Zulassen* und bestätigen Sie das Fenster.
5. Starten Sie auf dem NPS-Server das Snap-In *Zertifikate* erneut und überprüfen Sie, ob das Zertifikat jetzt registriert werden kann. Bis das Zertifikat angezeigt wird, kann es etwas dauern.

VPN-Client konfigurieren

Damit Sie ein VPN über HTTPS mit SSTP verwenden können, muss auf den Clients Windows Vista, Windows 7 oder Windows 8 installiert sein. Damit sich der VPN-Client verbinden kann, muss das Zertifikat der Stammzertifizierungsstelle auf dem Client installiert werden.

Diese Vorgänge sind ausführlich in den Kapiteln 30 und 31 erläutert. Im folgenden Abschnitt gehen wir darauf ein, wie das Zertifikat der Zertifizierungsstelle über die Weboberfläche der Zertifizierungsstelle in Ihrem Unternehmen angefordert wird. Computer, die Mitglied der gleichen Active Directory-Gesamtstruktur wie der Zertifikatserver sind, vertrauen dem Server automatisch.

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 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 (*https://<Servername>/certsrv*). Nach einem Klick auf den Link *Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste* erscheint eine Sicherheitsmeldung im Internet Explorer, die Sie mit *Ja* bestätigen.

Abbildg. 32.24 Herunterladen des Zertifizierungsstellenzertifikats

Klicken Sie in der nächsten Seite auf den Link *Download des Zertifizierungsstellenzertifikats*. Wählen Sie im Downloadfenster *Öffnen* aus. Klicken Sie im neuen Fenster auf *Zertifikat installieren*. Schließen Sie den Assistenten zur Installation mit den Standardeinstellungen ab.

Anschließend muss das Zertifikat noch in den richtigen Zertifikatspeicher verschoben werden. Aktuell befindet sich das Zertifikat im Speicher des Benutzers, muss aber in den Speicher des lokalen Computerkontos, und zwar in den Speicher der vertrauenswürdigen Stammzertifizierungsstellen (siehe Kapitel 30 und 31). Gehen Sie dazu folgendermaßen vor:

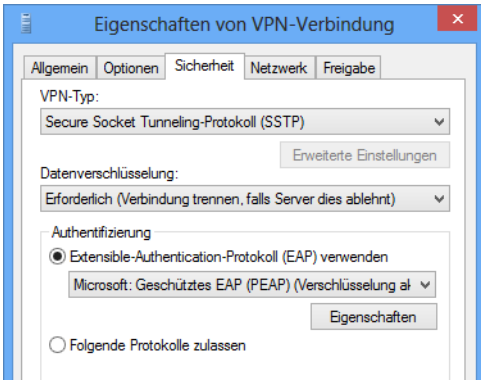
1. Öffnen Sie einen neue MMC-Konsole.
2. Fügen Sie das Snap-In *Zertifikate* hinzu.
3. Wählen Sie als Option *Eigenes Benutzerkonto* aus.
4. Fügen Sie noch mal das Snap-In *Zertifikate* hinzu.
5. Wählen Sie als Option *Computerkonto* aus und wählen den lokalen Computer aus.
6. Öffnen Sie den Konsoleneintrag *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 *Sicherheit*.
7. Wählen Sie bei *VPN-Typ* die Option *Secure Socket Tunneling-Protokoll (SSTP)* aus.

Abbildg. 32.25 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 fehlerhaften 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 im Microsoft-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* [Ms179-K32-01] aufrufen.

Auf der Registerkarte *Sicherheit* des Routing- und RAS-Servers konfigurieren Sie noch das Zertifikat, das die SSTP-Verbindung verwenden soll. In den Eigenschaften für Ports legen Sie die Anzahl und Konfiguration der Ports für SSTP fest.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Clientcomputer über das Internet an Active Directory-Domänen anbinden. Zusätzlich haben Sie erfahren, wie Sie ein VPN aufbauen und wie Sie Clients mit DirectAccess anbinden.

Im nächsten Kapitel erläutern wir Ihnen, wie Sie die Active Directory-Rechteverwaltung nutzen und den dynamischen Zugriffschutz einsetzen.

Kapitel 33

Active Directory-Rechteverwaltungsdienste und dynamische Zugriffssteuerung

In diesem Kapitel:

Mit Windows Server 2012 R2 stellt Microsoft eine verbesserte Version der Active Directory-Rechteverwaltung zur Verfügung. Die wichtigste Neuerung ist die dynamische Zugriffssteuerung (Dynamic Access Control, DAC). Diese speichert Berechtigungen direkt im Dokument und behält diese bei, unabhängig davon, wohin der Benutzer die Datei verschiebt. Auch SharePoint und Exchange lassen sich so in das Rechtemodell mit einbeziehen.

Active Directory-Rechteverwaltung im Überblick

In Windows Server 2012 R2 gibt es für Unternehmen vor allem die beiden Editionen Standard und Datacenter zur Auswahl. Eine Enterprise-Edition gibt es nicht mehr. Außerdem beherrscht die Standard-Edition alle Funktionen und Rollen der Datacenter-Edition. Der Unterschied der beiden Editionen liegt lediglich in der erlaubten Anzahl von virtuellen Maschinen, die Unternehmen mit einer Lizenz betreiben dürfen. In der Standard-Edition ist die Anzahl von VMs auf zwei begrenzt, in der Datacenter-Editionen dürfen Administratoren unbegrenzt virtuelle Server installieren.

Neuerungen der Active Directory-Rechteverwaltungsdienste

Die Active Directory-Rechteverwaltung (AD RMS) ist daher jetzt auch umfassend in der Standard-Edition des Windows-Servers enthalten und erlaubt auch kleineren Unternehmen, diese Funktion zu nutzen. In Windows Server 2012 R2 ist es nicht mehr notwendig, dass das Installationskonto, mit dem Sie die Active Directory-Rechteverwaltung (AD RMS) installieren, über lokale Administratorrechte auf dem SQL-Server verfügen muss.

Auf dem SQL-Server speichern AD RMS wichtige Daten in einer Datenbank. Allerdings muss das Konto innerhalb von SQL Server umfassende Administratorrechte erhalten. Außerdem muss auf dem SQL-Server der SQL Server-Browser gestartet sein, damit AD RMS auf den Server zugreifen darf. Vor der Installation von AD RMS muss der SQL-Server, auf dem die Dienste Daten speichern sollen, vorbereitet werden.

Offiziell unterstüzen AD RMS SQL Server 2005 Service Pack 3, SQL Server 2008 Service Pack 3 und SQL Server 2008 R2 Service Pack 1 sowie SQL Server 2012. Mehr Informationen dazu bietet Microsoft in der TechNet (*http://technet.microsoft.com/en-us/library/dd772673(WS.10).aspx* [Ms179-K33-01]).

AD RMS und dynamische Zugriffssteuerung

AD RMS und die dynamische Zugriffssteuerung (*http://technet.microsoft.com/de-de/library/hh831717.aspx* [Ms179-K33-02]) arbeiten zusammen. Wie bei der Rechteverwaltung lassen sich auch bei der dynamischen Zugriffssteuerung Richtlinien für den Zugriff auf Dateien erstellen. Diese Richtlinien steuern den Zugriff auf Dokumente parallel zum herkömmlichen Rechtemodell.

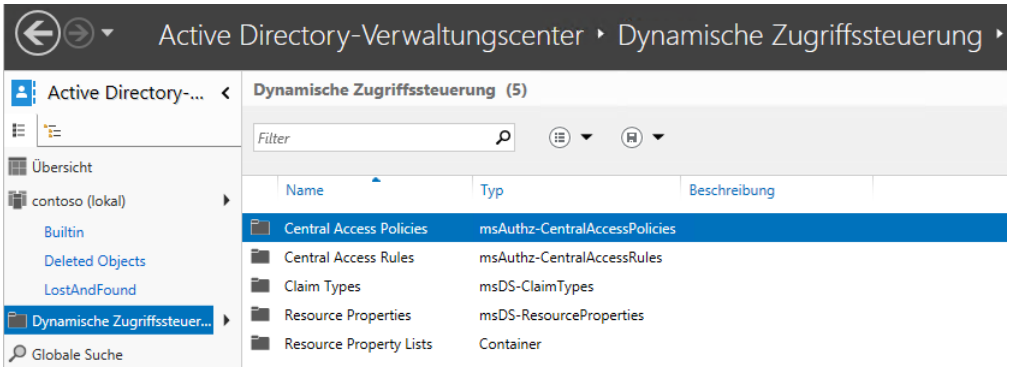
Dieses hat sich auch in Windows Server 2012 R2 nicht geändert. In diesem Bereich arbeitet die dynamische Zugriffssteuerung auch mit den Dateiklassifizierungsdiensten zusammen (siehe Kapitel

21). Dieser Windows-Dienst erlaubt die Zuteilung von Metadaten (Tags) zu Dateien, die den Zugriff regeln. Auf Basis der Klassifizierung erstellen Administratoren zentrale Zugriffsrichtlinien (Central Access Policies, CAPs) (*http://technet.microsoft.com/de-de/library/hh831425* [Ms179-K33-03]) als zusätzliche Berechtigungsebene.

Darf ein Anwender auf eine Datei über das Dateisystem zugreifen, verweigert die CAP aber den Zugriff, ist das Öffnen der Datei trotzdem nicht zulässig. Dies gilt auch umgekehrt. Verweigerungen haben auch in Windows Server 2012 R2 immer Vorrang vor erteilten Berechtigungen. Dürfen Anwender eine Datei nicht öffnen, besteht die Möglichkeit, direkt einen Administrator per E-Mail zu benachrichtigen. Dazu setzen Unternehmen am besten noch parallel zu Windows Server 2012 R2 auf SharePoint 2013 und Exchange 2013.

Der Zugriff auf Dateien wird durch Ordner nach unten vererbt, genauso wie bei herkömmlichen Berechtigungen. Anwender dürfen auch noch selbst Rechte erteilen und auch Anwendungen dürfen automatisch Metadaten in Dateien schreiben, die sich anschließend auf die Rechte auswirken. Die CAP des Unternehmens prüft die Metadaten der Dateien und weist die entsprechenden Rechte zu. Der Vorgang lässt sich dann mit AD RMS auch automatisieren.

Abbildg. 33.1 Verwalten der dynamischen Zugriffssteuerung im neuen Active Directory-Verwaltungscenter von Windows Server 2012 R2



Active Directory-Rechteverwaltung, Dateiklassifizierungsdienste (siehe Kapitel 21) und dynamische Zugriffssteuerung erlauben eine granulare und hochsichere Speicherung und Absicherung von Dokumenten.

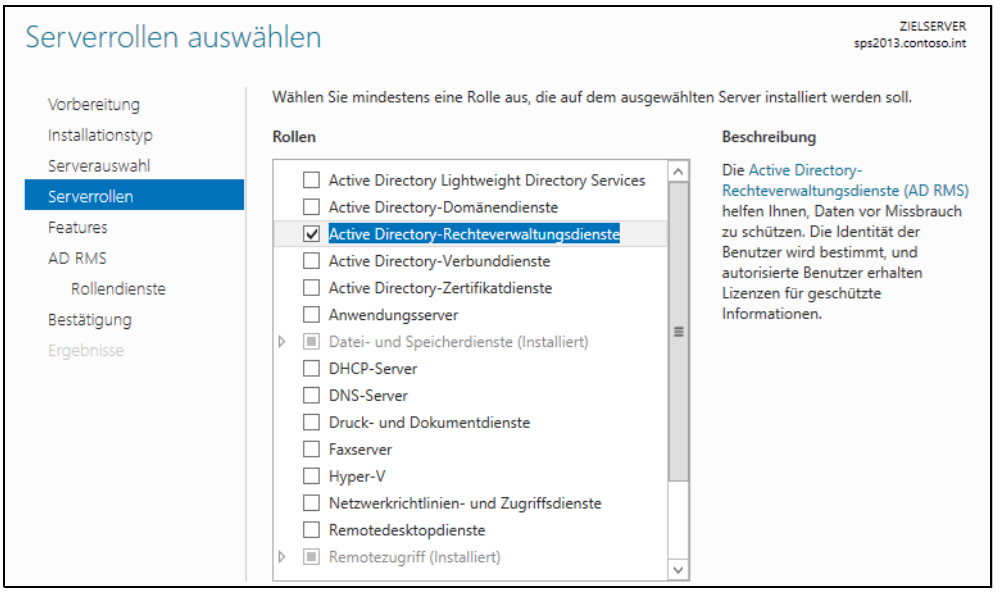
Da durch die dynamische Zugriffssteuerung und die Rechteverwaltung aber eine weitere Ebene der Sicherheit eingeführt wird, müssen Sie ein sehr detailliertes Konzept für das Rechtemodell ausarbeiten, da ansonsten ein regelrechter Wildwuchs bei den Rechten entstehen kann. Eine optimale Planung ist daher bei diesem Bereich besonders wichtig.

Rechteverwaltung installieren und testen

Die Installation der Active Directory-Rechteverwaltung findet über den Server-Manager statt. Sie rufen dazu *Verwalten/Rollen und Funktionen hinzufügen* auf und wählen die Rolle *Active Directory-Rechteverwaltungsdienste* aus. Die notwendigen zusätzlichen Features müssen ebenfalls bestätigt

werden. In Windows Server 2012 R2 lassen sich die Dienste über den Server-Manager auch remote installieren.

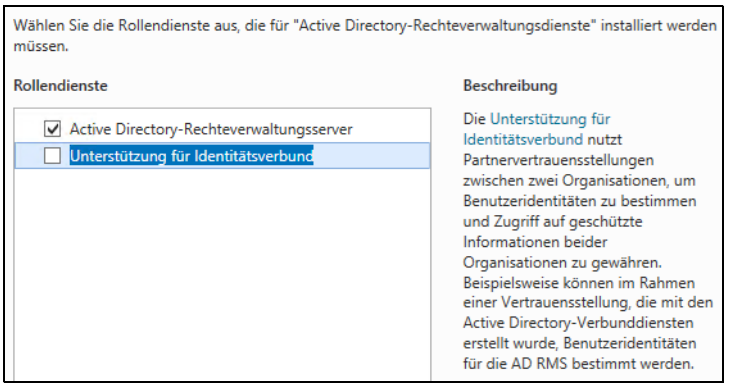
Abbildg. 33.2 Sie installieren AD RMS über den Server-Manager oder die PowerShell



Die Active Directory-Rechteverwaltungsdienste bieten eine umfassende Unterstützung von PowerShell 3.0. Um die Dienste in PowerShell zu installieren, geben Administratoren den Befehl *Add-WindowsFeature ADRMS –IncludeAllSubFeature* ein. Mit *Install-ADRMS* lassen sich die Dienste ebenfalls installieren.

Während der Installation muss ausgewählt werden, welche Rollendienste der Server bereitstellen soll. Auf diesem Weg lassen sich die Active Directory-Rechteverwaltungsdienste in einer einzelnen Gesamtstruktur betreiben oder mit dem Rollendienst *Unterstützung für Identitätsverbund* über mehrere Strukturen hinweg.

Abbildg. 33.3 Auswählen der zu installierenden Rollendienste von AD RMS



Auf Core-Servern mit Windows Server 2012 R2 können Sie die Active Directory-Rechteverwaltung ebenfalls installieren. Parallel dazu lassen sich auch auf Core-Servern noch Active Directory-Domänendienste (Active Directory Domain Services, AD DS) und Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) installieren (siehe die Kapitel 4, 10 bis 17 und 30).

Nach der Installation der Active Directory-Rechteverwaltungsdienste müssen Sie über den Server-Manager zunächst den Einrichtungs-Assistenten starten. Erst nachdem dieser Assistent durchgelaufen ist, funktionieren die AD RMS.

Sobald der AD RMS-Schutz für eine Datei hinzugefügt wird, bleibt der Schutz für die Datei bestehen. Standardmäßig kann der Schutz für eine Datei nur vom Inhaltsbesitzer entfernt werden. Der Inhaltsbesitzer gewährt anderen Benutzern das Recht, Aktionen am Inhalt der Datei vorzunehmen, zum Beispiel die Möglichkeit, die Datei anzuzeigen, zu kopieren oder zu drucken.

HINWEIS Starten Sie den SQL Server-Browserdienst auf dem SQL-Server, bevor Sie die Active Directory-Rechteverwaltung einrichten. Erstellen Sie auch eine Ausnahme in der Windows-Firewall auf dem SQL-Server. Wie Sie dabei vorgehen, lesen Sie in den nächsten Abschnitten.

SQL-Server für AD RMS vorbereiten

AD RMS benötigen Zugriff auf einen SQL-Server. Sie können an dieser Stelle auch die kostenlose Express-Edition von SQL Server 2012 verwenden (*http://www.microsoft.com/de-de/download/details.aspx?id=29062* [Ms179-K33-04]).

Wenn das TCP/IP-Protokoll aktiviert ist und eine Instanz von SQL Server 2012 startet, wird dem Server ein TCP/IP-Port zugewiesen. Ist das Named Pipes-Protokoll aktiviert, lauscht SQL Server an einer speziell benannten Pipe. Dieser Port wird von der betreffenden Instanz zum Zugriff mit Clientanwendungen verwendet. Bei der Installation von SQL Server 2012 wird der TCP-Port 1433 und die Pipe *\sql\query* der Standardinstanz zugewiesen. Die Einstellungen lassen sich aber ändern.

Da ein Port oder eine Pipe von nur jeweils einer Instanz von SQL Server verwendet werden kann, verwenden benannte Instanzen andere Portnummern und Pipenamen. Sie können einer Instanz von SQL Server einen bestimmten Port zuweisen. Beim Verbindungsaufbau können Clients einen bestimmten Port angeben.

Wie das geht, zeigen wir im folgenden Abschnitt noch genauer. Wenn der Port jedoch dynamisch zugewiesen wird, kann sich die Portnummer bei jedem Neustart von SQL Server ändern, sodass die richtige Portnummer dem Client unbekannt bleibt. Das heißt, auf dem SQL-Server muss ein Dienst dafür sorgen, dass sich Anwender mit den Instanzen verbinden können, ohne den entsprechenden Port zu kennen. Diese Funktion übernimmt der Systemdienst *SQL Server-Browser*. Der Dienst ist nur dann notwendig, wenn auf einem SQL-Server mehr als eine Instanz installiert ist und wenn Sie Active Directory-Rechteverwaltungsdienste einsetzen.

Beim Starten verwendet SQL Server-Browser den UDP-Port 1434. Der SQL Server-Browser liest die Registrierung des Servers, identifiziert alle Instanzen auf dem Server und speichert die verwendeten Ports und Named Pipes. Wenn ein Server über zwei oder mehr Netzwerkkarten verfügt, gibt der SQL Server-Browser den ersten gefundenen aktivierten Port zurück.

Der SQL Server-Browser unterstützt IPv4 und IPv6. Wenn SQL Server-Clients eine Verbindung mit einer Instanz aufbauen, sendet der Client über den Port 1434 eine UDP-Nachricht an den Server.

SQL Server-Browser antwortet anschließend mit dem TCP/IP-Port oder der Named Pipe der angeforderten Instanz. Wenn der SQL Server-Browserdienst nicht ausgeführt wird, können Sie dennoch eine Verbindung herstellen, wenn Sie den Port oder die Pipe der Instanz angeben. Allerdings funktioniert das nicht mit den Active Directory-Rechteverwaltungsdiensten.

Damit Anwendungen wie die Active Directory-Rechteverwaltungsdienste auf einen Server zugreifen dürfen, um zum Beispiel selbst Datenbanken zu erstellen, müssen Sie Firewallregeln erstellen und im Konfigurations-Manager Protokolle freischalten. Dazu muss auf dem SQL-Server eine neue Firewallregel erstellt werden, da die Firewall die beiden TCP Ports 1433 und 1434 blockiert. Mit diesen Ports bauen Clients eine Verbindung zum Server auf:

1. Geben Sie dazu auf dem SQL-Server auf der Startseite *wf.msc* ein.
2. Klicken Sie auf *Eingehende Regeln*.
3. Klicken Sie dann auf *Neue Regel*.
4. Aktivieren Sie auf der ersten Seite des Assistenten zum Erstellen von neuen Firewallregeln die Option *Port*.
5. Aktivieren Sie auf der nächsten Seite die Optionen *TCP* und *Bestimmte lokale Ports*.
6. Geben Sie im Feld neben der Option *Bestimmte lokale Ports* den Wert *1433-1434* ein.
7. Aktivieren Sie auf der nächsten Seite die Option *Verbindung zulassen* und auf der folgenden Seite die Profile, für die Sie den Zugriff gestatten wollen. In sicheren Umgebungen reicht es auch aus, wenn Sie nur das Domänenprofil aktivieren.
8. Weisen Sie abschließend der Regel einen passenden Namen zu und bestätigen Sie die Erstellung.

Abbildg. 33.4 Festlegen der Ports für die neue Regel

TIPP Haben Sie auf dem Server noch benannte Instanzen installiert und wollen auf diese über das Netzwerk mit dem Management Studio zugreifen, erstellen Sie eine weitere Regel, welche die Ports UDP 1433-1434 zulässt. Auch wenn Sie Active Directory-Rechteverwaltungsdienste einsetzen, müssen Sie diese Einstellung vornehmen.

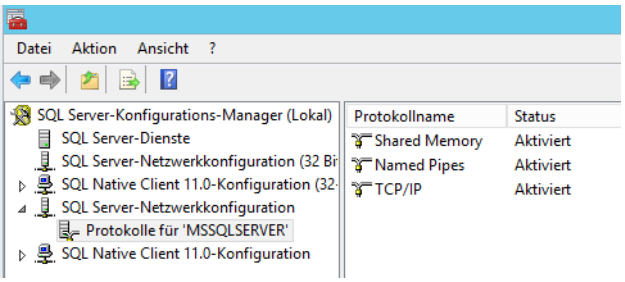
Außerdem muss für die Verbindung der Systemdienst *SQL Server-Browser* gestartet sein. Dieser nimmt Abfragen aus dem Netzwerk entgegen und verteilt diese an die entsprechende Instanz oder Server. Dazu ist es notwendig, dass der Server über das Netzwerk mit TCP/UDP erreichbar ist und die Ports TCP/UDP 1433-1434 in der Firewall freigeschaltet sind.

Erhalten Sie Fehler beim Netzwerkzugriff angezeigt, schalten Sie über die Standardeinstellung der Firewall in der Systemsteuerung noch die Remoteverwaltung des Servers frei. Sie finden die Einstellung in der Systemsteuerung unter *System und Sicherheit/Windows-Firewall* über den Link *Eine App oder ein Feature durch die Windows-Firewall durchlassen*.

Außerdem müssen Sie an dieser Stelle auch die verschiedenen anderen SQL Server-Dienste freischalten, vor allem den SQL Server-Browser. Dieser nimmt Anfragen aus dem Netzwerk entgegen und verbindet die Clients mit der entsprechenden Instanz.

Funktioniert die Verbindung zum SQL-Server nicht, öffnen Sie auf dem SQL-Server den SQL Server-Konfigurations-Manager in der Untergruppe *Konfigurationstools*. Klicken Sie dann auf *SQL Server-Netzwerkkonfiguration/Protokolle für <Instanz>* und stellen Sie sicher, dass *TCP/IP* und *Named Pipes* aktiviert sind. Für den Zugriff über das Netzwerk ist vor allem TCP/IP notwendig. Named Pipes steuert den Zugriff auf dem lokalen Server.

Abbildg. 33.5 Für die Verbindung von SharePoint zu SQL Server müssen *Named Pipes* und *TCP/IP* aktiviert sein



Vor allem bei der Developer Edition oder bei der kostenlosen Express Edition von SQL Server ist TCP/IP meist deaktiviert. In den Eigenschaften von *Protokolle für <Instanz>* nehmen Sie ebenfalls Einstellungen vor, genauso wie in den Eigenschaften von einzelnen Protokollen auf der rechten Seite.

Für die Eigenschaften aller Protokolle können Sie zum Beispiel eine Verschlüsselung aktivieren. Dann dürfen sich nur noch verschlüsselte Clients mit dem Server verbinden. Aktivieren Sie die Verschlüsselung, können Sie in den Eigenschaften von *Protokolle für <Instanz>* noch ein Zertifikat hinterlegen, welches Sie für die Verschlüsselung verwenden.

An dieser Stelle nehmen Sie für alle installierten Instanzen Einstellungen für die verwendeten Protokolle vor. Über das Kontextmenü von *Protokolle für <Instanz>* finden Sie die Eigenschaften für alle Protokolle dieser Instanz. Hier können Sie ein installiertes Zertifikat hinterlegen und die Verschlüsselung aktivieren. Auf den Clients können Sie ebenfalls die Verschlüsselung aktivieren, sodass der Server nur noch verschlüsselte Verbindungen erlaubt. Standardmäßig ist die Verschlüsselung nicht aktiv.

TIPP Funktioniert die Verbindung zu einer benannten Instanz über das Netzwerk nicht und erhalten Sie noch den Fehler 26 bei der Verbindung angezeigt, sollten Sie zunächst auf dem Server, mit dem Sie auf die Instanz des anderen Servers zugreifen wollen, die Verbindung zum SQL Server-Browserdienst testen lassen. Die Verbindung muss funktionieren, da ansonsten das Management Studio oder andere Clients nicht auf benannte Instanzen zugreifen können. Sie können dazu das Microsoft-Tool PortQry nutzen:

1. Laden Sie die *PortQryV2.exe* von der Seite *http://www.microsoft.com/en-us/download/details.aspx?id=17148* [Ms179-K33-05] herunter.
2. Rufen Sie das Tool mit den folgenden Optionen auf:

```
portqry.exe -n <Servername> -p UDP -e 1434
```

3. Es muss eine Antwort des SQL Server-Browserdiensts und es müssen die verschiedenen Instanzen des Servers erscheinen. Nur wenn eine Instanz vom Browserdienst erkannt wird, kann der Systemdienst die Benutzeranfragen an die entsprechende Instanz weiterleiten.

Die Verbindung setzt voraus, dass die Server über Ping miteinander kommunizieren können und auch die Namen per DNS auflösbar sind. Sobald auf einem Server mehrere Instanzen installiert sind, muss der Systemdienst *SQL Server-Browser* gestartet sein. Ansonsten lässt sich auf benannte Instanzen nicht über das Netzwerk zugreifen. Sie können die Funktion des SQL Server-Browsers auch in der Eingabeaufforderung mit *sc query sqlbrowser* testen. Der Dienst muss fehlerfrei funktionieren.

Funktioniert die Verbindung nicht, wenn Sie sich im Management Studio verbinden, können Sie das Verbindungsprotokoll des Management Studios auch steuern. Dazu geben Sie nicht die Verbindung in der Syntax *<Server>\<Instanz>* an, sondern mit *tcp:<Server>\<Instanz>* oder *np:<Server>\<Instanz>*, je nachdem, wie Sie die Verbindung testen wollen, also mit TCP/IP oder Named Pipes. Haben Sie in den Eigenschaften des TCP/IP-Protokolls für die Instanz einen Port definiert, können Sie auf dem Server, mit dem Sie auf die Instanz zugreifen wollen, diesen in der Verbindung mit der Syntax *<Server>\<Instanz>,<Port>* angeben. Hier funktioniert dann in der Regel die Verbindung.

Ist das entsprechende Protokoll auf dem Zielserver im SQL Server-Konfigurations-Manager für die Instanz freigeschaltet, muss die Verbindung auch funktionieren.

Wollen Sie zeitweise oder dauerhaft eine Instanz von SQL Server im Netzwerk ausblenden, also noch verfügbar machen, aber nicht mehr über das Netzwerk zur Verfügung stellen, verwenden Sie den SQL Server-Konfigurations-Manager. Rufen Sie die Eigenschaften von *Protokolle für <Instanz >* auf und wechseln Sie zur Registerkarte *Flags*. Konfigurieren Sie die Option *Instanz ausblenden* mit *Ja*.

Konfigurieren von AD RMS

Ist der SQL-Server verfügbar und die Rollendienste von AD RMS installiert, machen Sie sich an die Einrichtung der Funktion. Der erste Server in einer AD RMS-Umgebung ist der Stammcluster. Ein AD RMS-Stammcluster besteht aus einem oder mehreren AD RMS-Servern, die in einer Lastenausgleichsumgebung konfiguriert sind.

Unter Windows Server 2012 R2 stellen das Hinzufügen der AD RMS-Rolle und die Konfiguration eines neuen AD RMS-Clusters zwei separate Vorgänge dar. Das war in Windows Server 2008 R2 noch anders. Nachdem Sie die Rolle erfolgreich hinzugefügt haben, ist eine weitere Konfiguration erforderlich, um die AD RMS-Rolle bereitzustellen:

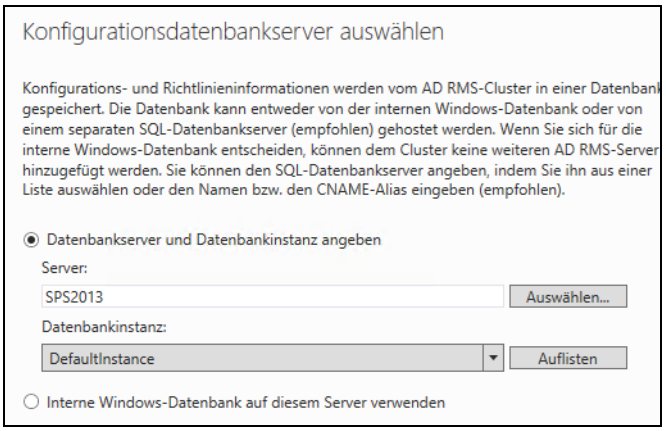
1. Klicken Sie in Server-Manager auf das Symbol *Benachrichtigungen*.
2. Klicken Sie bei dem Taskereignis *Konfiguration für Active Directory-Rechteverwaltungsdienste erforderlich* auf *Zusätzliche Einstellungen konfigurieren*.
3. Der AD RMS-Konfigurations-Assistent wird geöffnet.

4. Klicken Sie im Konfigurations-Assistenten auf *Weiter*.

Abbildg. 33.6 Starten des Assistenten zur Einrichtung von AD RMS

5. Akzeptieren Sie die Standardauswahl für den AD RMS-Cluster (*AD RMS-Stammcluster erstellen*) und klicken Sie auf *Weiter*.
6. Akzeptieren Sie die Standardauswahl für die Konfigurationsdatenbank (*Datenbankserver und Datenbankinstanz angeben*) und klicken Sie auf *Auswählen*.
7. Wählen Sie den SQL-Server aus und klicken Sie danach auf *Auflisten*, um die Instanzen einzulesen.

Abbildg. 33.7 Verbinden von AD RMS mit dem SQL-Datenbankserver



8. Wählen Sie im Listenfeld *Datenbankinstanz* den Eintrag *DefaultInstance* aus und klicken Sie auf *Weiter*.
9. Klicken Sie im Dialogfeld *Dienstkonto angeben* auf *Angeben* und wählen Sie einen Administratorbenutzer aus. Sie können den Benutzer auch direkt eingeben. Sie benötigen für den Vorgang ein anderes Benutzerkonto als das Konto, mit dem Sie AD RMS einrichten.
10. Akzeptieren Sie den Kryptografiemodus 2 und klicken Sie dann auf *Weiter*.
11. Übernehmen Sie für *Clusterschlüsselspeicher* die Standardeinstellung (*Zentral verwalteten AD RMS-Schlüsselspeicher verwenden*) und klicken Sie dann auf *Weiter*.

12. Geben Sie auf der Seite *Clusterschlüsselkennwort* ein Kennwort ein und bestätigen Sie es. Klicken Sie auf *Weiter*.
13. Akzeptieren Sie für die Clusterwebsite die Standardeinstellung (*Standardwebsite*) und klicken Sie dann auf *Weiter*.
14. Übernehmen Sie für *Verbindungstyp* die Standardeinstellung (*SSL-verschlüsselte Verbindung (https://) verwenden*) und geben Sie für *Vollqualifizierter Domänenname* den Namen des Servers ein.

Abbildg. 33.8 Auswählen der Clusteradresse

15. Akzeptieren Sie bei *Serverzertifikat* die Standardeinstellung *(Selbstsigniertes Zertifikat zur SSL-Verschlüsselung erstellen)* und klicken Sie dann auf *Weiter*. Sie können an dieser Stelle auch eigene Zertifikate verwenden, wenn Sie auf die Active Direcotry-Zertifikatdienste setzten (siehe Kapitel 30). Am schnellsten fordern Sie ein Zertifikat an, wenn Sie *certlm.msc* starten. Wenn Sie ein selbstsigniertes Zertifikat für das Cluster verwenden, können Sie eine Kopie des Zertifikats im Ordner *Vertrauenswürdige Stammzertifizierungsstellen* erstellen, damit diesem Zertifikat vertraut wird. Diesen Vorgang führen Sie ebenfalls in der Konsole *certlm.msc* durch. Sie kopieren dazu über das Kontextmenü einfach das Zertifikat und fügen es danach bei den vertrauenswürdigen Stammzertifizierungsstellen ein.
16. Akzeptieren Sie für *Lizenzgebendes Zertifikat* den Standardnamen und klicken Sie dann auf *Weiter*.
17. Akzeptieren Sie für *Dienstverbindungspunkt registrieren* die Standardeinstellung (*SCP jetzt registrieren*) und klicken Sie dann auf *Weiter*.
18. Überprüfen Sie zur Bestätigung Ihre Installationsauswahl und klicken Sie anschließend auf *Installieren*.
19. Klicken Sie auf *Schließen*.

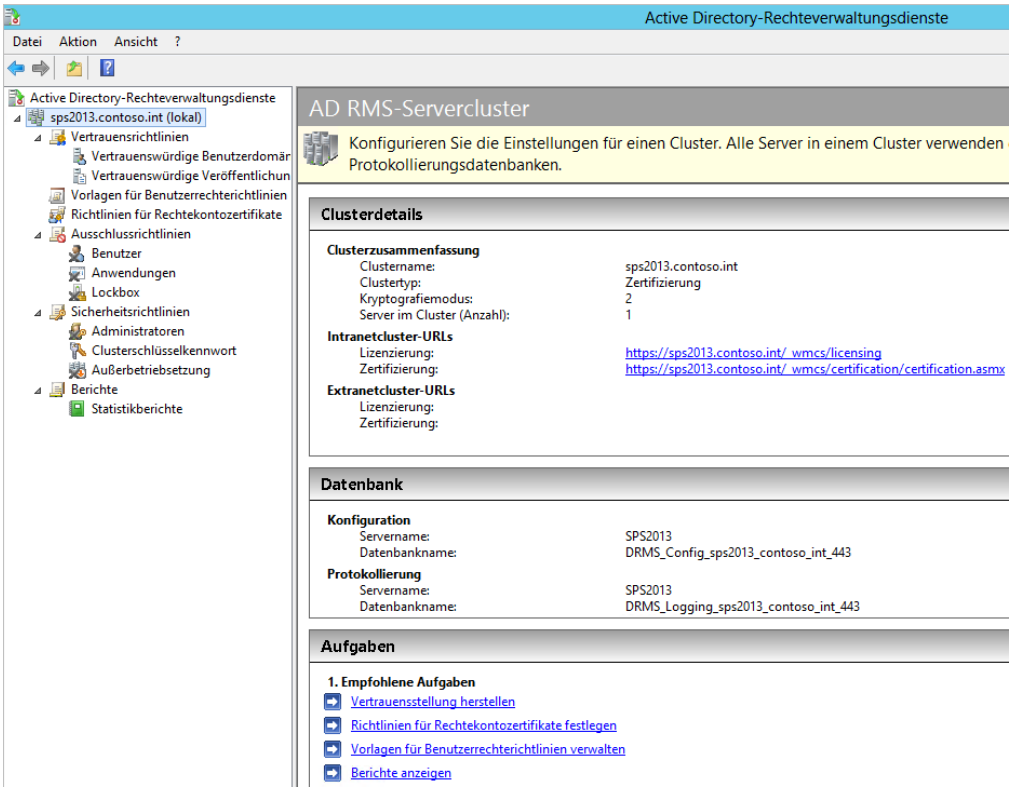
20. Melden Sie sich vom Server ab und anschließend wieder an, um den Sicherheitstoken für das angemeldete Benutzerkonto zu aktualisieren.

Das Benutzerkonto, das bei der Installation der AD RMS-Serverrolle angemeldet ist, wird automatisch zu einem Mitglied der lokalen AD RMS-Gruppe *Organisations-Admins*. Ein Benutzer muss Mitglied dieser Gruppe sein, um AD RMS verwalten zu können. Der AD RMS-Stammcluster ist jetzt installiert und konfiguriert. Sobald Sie sich erneut anmelden, können Sie AD RMS über die Konsole der Active Directory-Rechteverwaltungsdienste verwalten.

AD RMS nach der Installation verwalten und überprüfen

Nach der Installation und Einrichtung verwalten Sie AD RMS mit dem Server-Manager. Klicken Sie dazu im Server-Manager auf *Tools* und wählen Sie *Active Directory-Rechteverwaltungsdienste* aus. Über die Konsole können Sie Vertrauensrichtlinien und Ausschlussrichtlinien konfigurieren und Vorlagen für Benutzerrechterichtlinien erstellen.

Abbildg. 33.9 Verwalten von AD RMS nach der Installation

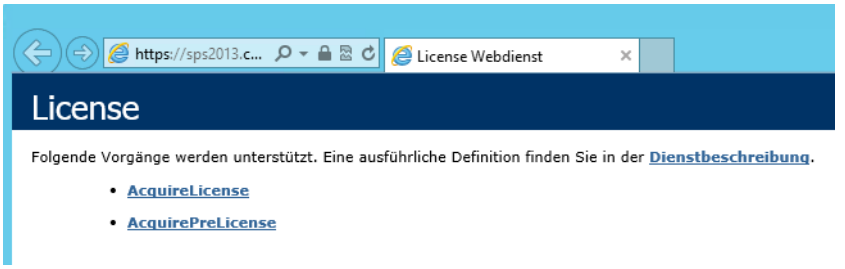


Bevor Sie durch Rechte geschützten Inhalt verwenden können, müssen Sie die URL des AD RMS-Clusters zur Sicherheitszone *Lokales Intranet* auf den Clients mit Windows 8 hinzufügen:

1. Klicken Sie auf der Taskleiste im Windows 8-Client auf das Internet Explorer-Symbol.
2. Klicken Sie auf *Extras* (mit der Alt-Taste einblenden) und dann auf *Internetoptionen*.
3. Klicken Sie auf die Registerkarte *Sicherheit* und dann auf *Lokales Intranet*.
4. Klicken Sie dann auf *Sites*.
5. Klicken Sie auf *Erweitert*.
6. Geben Sie unter *Diese Website zur Zone hinzufügen* die Adresse *https://<Servername des AD RMS-Clusters>* ein und klicken Sie dann auf *Hinzufügen*.
7. Klicken Sie auf *Schließen*.

Sie können den Zugriff auf die AD RMS-Lizenzierungswebsite überprüfen, indem Sie die URL im Internet Explorer eingeben. Es sollte eine Warnung zu den Zertifikaten für diese Website angezeigt werden. Dies ist kommt daher, dass Sie bei der Konfiguration von AD RMS ein selbst signiertes Zertifikat verwendet haben.

Abbildg. 33.10 Verbindungsaufbau zu den Lizenzdiensten von AD RMS



Klicken Sie im Menü *Datei* auf *Dokument schützen*, zeigen Sie dann auf *Berechtigung nach Personen einschränken* und klicken Sie auf *Eingeschränkter Zugriff*. Sie können an dieser Stelle Vorlagen vom AD RMS-Cluster herunterladen und in Office verwenden.

Über die dynamische Zugriffssteuerung Berechtigungen als Metadaten speichern

Die neue dynamische Zugriffssteuerung (Dynamic Access Control, DAC) in Windows Server 2012 R2 soll Unternehmen dabei helfen, die Berechtigungen von Dateien besser zu verwalten. Allerdings müssen Administratoren beachten, dass die Verwaltung dieser Rechte extrem kompliziert und mit viel Aufwand verbunden ist. Wir zeigen Ihnen, welche Hürden es zu umschiffen gibt und wie DAC im Unternehmen eingeführt werden kann.

TIPP Mehr zu diesem Thema lesen Sie auch auf der Seite *http://technet.microsoft.com/de-de/library/hh831717.aspx* [Ms179-K33-06].

Die grundsätzliche Funktionsweise von DAC ist recht einfach. Die Berechtigungen, die Anwender für ein Dokument haben, sind im Dokument selbst als Metadaten gespeichert. Die Berechtigungen,

also Lesen, Schreiben, Drucken und mehr, bleiben im Dokument immer gültig, unabhängig davon, ob das Dokument in einen anderen Ordner verschoben, als E-Mail verschickt oder in SharePoint gespeichert wird. Das bisherige Berechtigungsmodell bleibt auch in Windows Server 2012 R2 erhalten, die dynamische Zugriffssteuerung ergänzt sie nur.

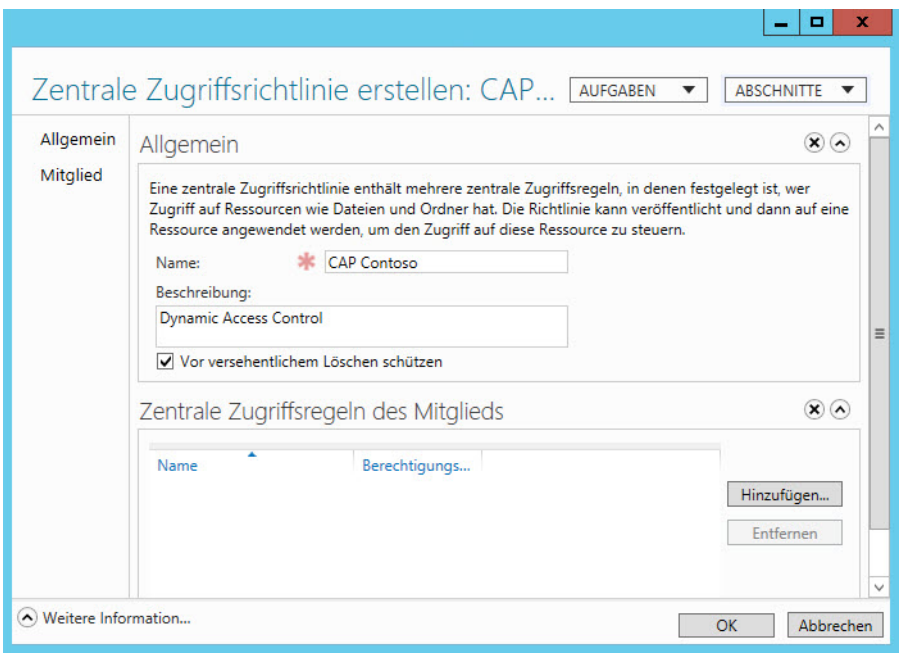
Damit Daten dynamisch gesichert werden können, müssen die einzelnen Dateien zunächst klassifiziert werden (siehe Kapitel 21). Dies kann in Windows Server 2012 R2 durch die Dateiklassifizierungsdienste automatisch erfolgen. Auch Anwendungen können einzelne Dateien automatisch klassifizieren und Benutzer selbst haben ebenfalls die Möglichkeit, ihre Dokumente zu klassifizieren.

Außerdem erben Dateien die Berechtigungstags übergeordneter Verzeichnisse. Auf Basis dieser Tags werden durch die DAC Rechte auf der Grundlage von Richtlinien zugewiesen, die Administratoren erstellen. So lassen sich zum Beispiel Dokumente der Geschäftsleitung entsprechend markieren und automatisch schützen. Die automatische Absicherung übernehmen dann die Active Directory-Rechteverwaltungsdienste.

DAC erweitert das Standardrechtemodell um eine zusätzliche Schicht. Haben Anwender auf einen Ordner Schreibrechte, greifen aber über eine Freigabe zu, in der nur Leserechte definiert sind, haben sie effektive Rechte zum Lesen, nicht zum Schreiben. Beim Einsatz von DAC werden beim Zugriff auf Dateien die festgelegten Rechte also noch einmal erweitert. So lässt sich ein Grundschutz für Dokumente im Netzwerk festlegen.

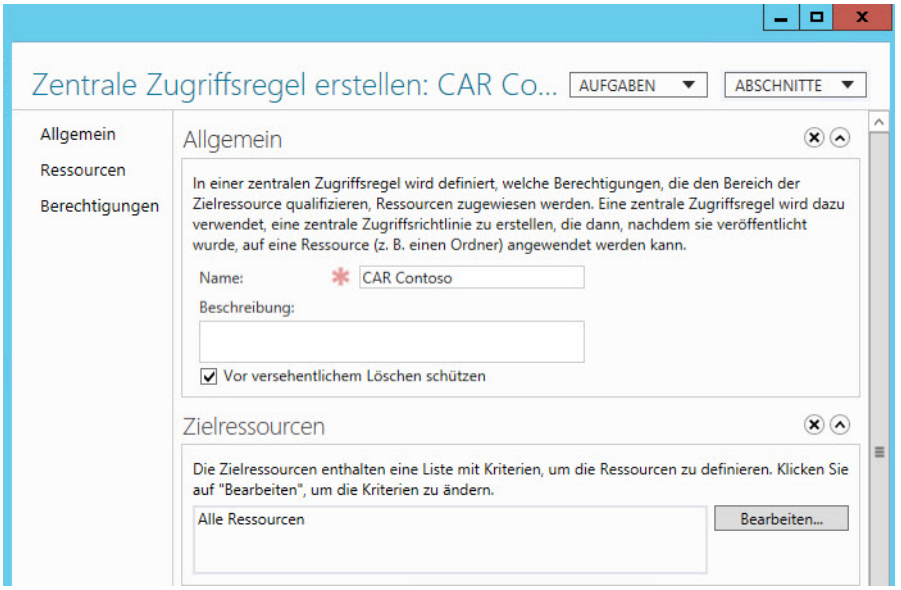
Die Verwaltung von Rechten und Zugriffsrichtlinien nehmen Sie im neuen Active Directory-Verwaltungscenter vor. Grundlagen für die Berechtigungssteuerungen sind zentrale Zugriffsrichtlinien (Central Access Policies, CAP). Auch diese legen Sie im Active Directory-Verwaltungscenter fest. Die Richtlinien steuern, welche Rechte Anwender auf Ressourcen haben, die dieser zentralen Richtlinie zugeordnet sind.

Abbildg. 33.11 Erstellen einer neuen zentralen Zugriffsrichtlinie



Die zentralen Zugriffsregeln steuern, welche Berechtigungen einem bestimmten Satz Ressourcen, also Dateien, Ordner oder Bibliotheken, zugewiesen sind. Während die zentrale Zugriffsrichtlinie steuert, wer zugreifen darf, steuern zentrale Zugriffsregeln, mit welchen Rechten die Anwender auf die klassifizierten Dateien zugreifen dürfen und welche Ressourcen die Regel verwendet.

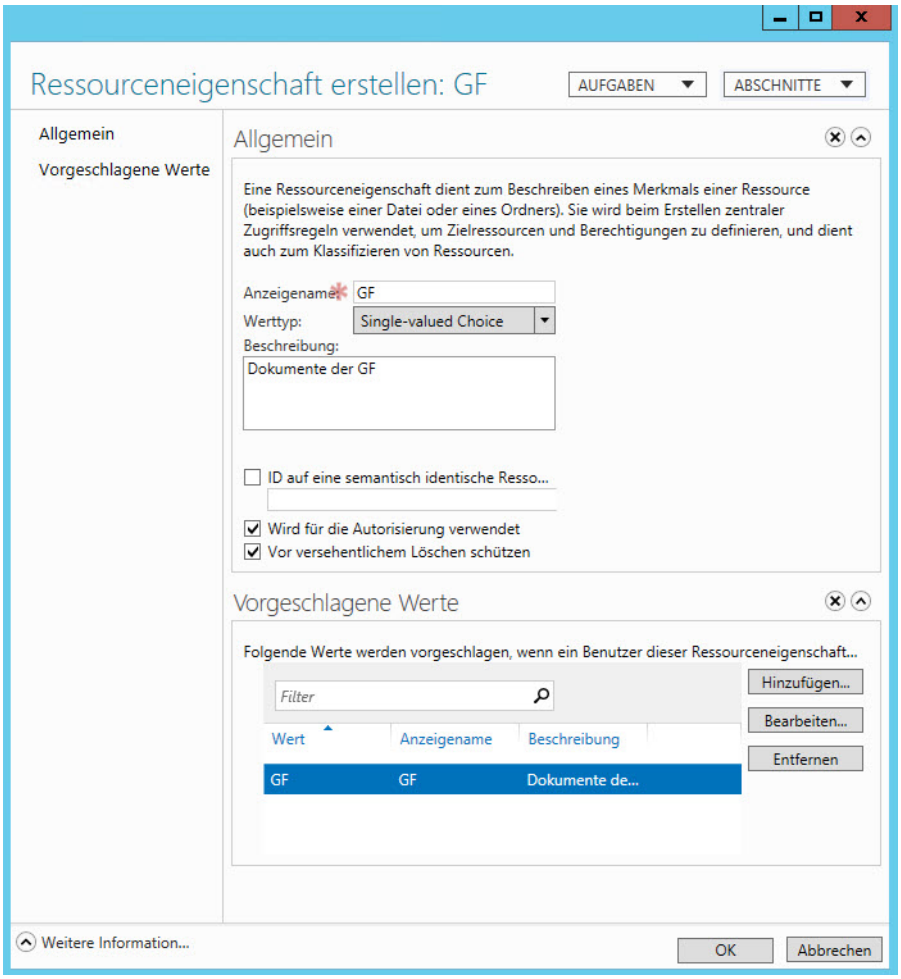
Abbildg. 33.12 Erstellen einer zentralen Zugriffsregel



Nachdem festgelegt ist, wer auf welche Ressourcen zugreifen darf, legen Sie in der zentralen Zugriffsregel fest, mit welchen genauen Rechten der Zugriff erfolgt. Auf diese Weise können Unternehmen eine Grundregel für Berechtigungen für alle Ressourcen in der Gesamtstruktur festlegen.

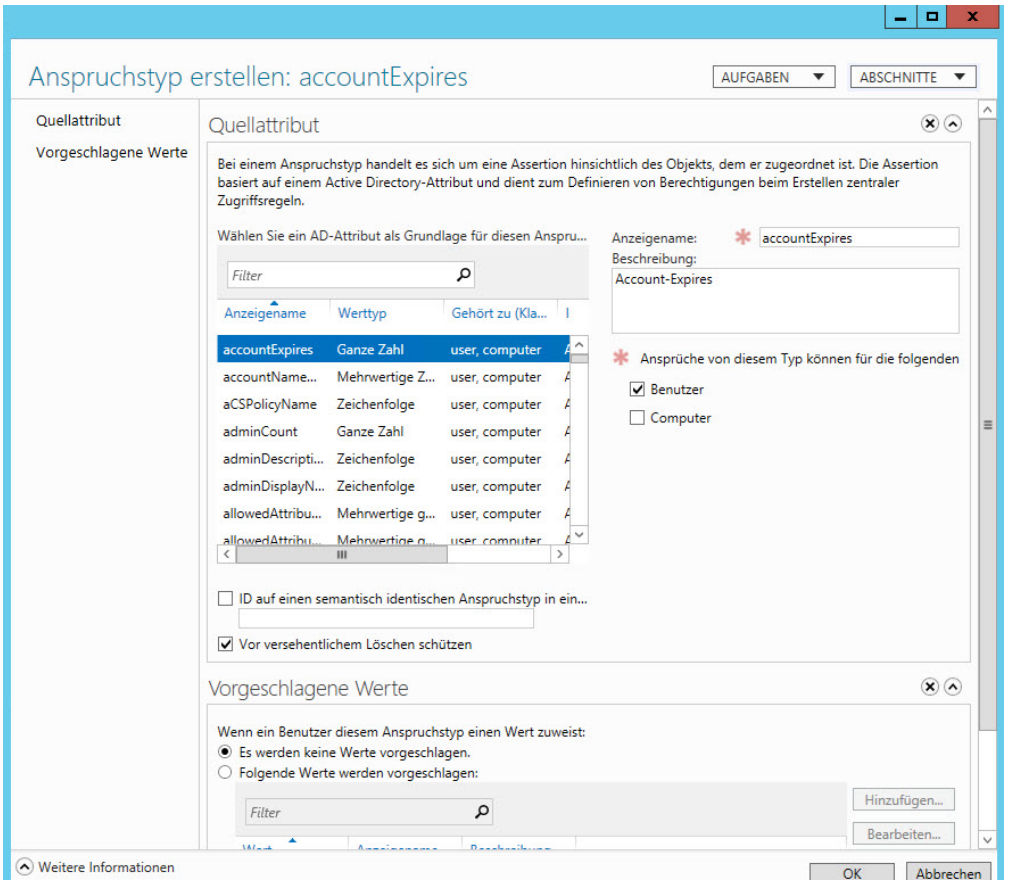
Damit die zentralen Zugriffsregeln Ressourcen genauer filtern können, um der zentralen Zugriffsrichtlinie die Zuteilung von Benutzern und den Zugriffsregeln das Zuteilen von Rechten zu erlauben, sind Ressourceneigenschaften notwendig. Diese Ressourceneigenschaften fassen bestimmte Dokumente zusammen.

Abbildg. 33.13 Erstellen von Ressourceneigenschaften



Ein weiterer Baustein sind die Anspruchstypen (Claim Types), also die Zuteilung von Attributen. Dabei handelt es sich um Attribute in Active Directory. Berücksichtigen Unternehmen zum Beispiel das Active Directory-Attribut *department*, lassen sich in der zentralen Zugriffsrichtlinie zum Beispiel einzelne Abteilungen abfragen, zum Beispiel *Verkauf*. Alle Anwender in dieser Abteilung lassen sich dann besondere Rechte zuteilen. Unternehmen können aber auch Computerkonten mit einbeziehen und beides kombinieren.

Abbildg. 33.14 Einsetzen von Anspruchstypen (Claim Types)



Einer der wichtigsten Bausteine von DAC sind die Dateiklassifizierungsdienste (siehe Kapitel 21). Diese steuern Sie über den Ressourcen-Manager für Dateiserver. Die Installation erfolgt als Rollendienste der Rolle *Datei- und Speicherdienste* über den Server-Manager (siehe Kapitel 4 und 21).

Klassifizierungseigenschaften, die Sie für Dokumente festlegen, werden nicht im Dateisystem, sondern in der Datei direkt gespeichert. Klicken Sie mit der rechten Maustaste auf *Klassifizierungseigenschaften*, können Sie mit *Eigenschaft erstellen* festlegen, welche neuen Kriterien Dateien zugeordnet werden können. So lässt sich zum Beispiel bestimmen, ob ein Dokument zu einem Projekt gehört, private Daten enthält, nur für den internen Gebrauch oder für bestimmte Personen nutzbar sein soll. Mehr zu diesem Thema lesen Sie in Kapitel 21.

Für die Eigenschaft geben Sie den Namen der neuen Eigenschaft an, zum Beispiel *Nur für internen Gebrauch*. Über *Eigenschaftentyp* stehen verschiedene Möglichkeiten zur Verfügung, die Eigenschaft festzulegen. Neben *Ja/Nein* können Sie eine Multiple Choice-Liste erstellen, eine Nummer oder eine Uhrzeit hinterlegen. Im unteren Bereich bearbeiten Sie dann die Eingaben genauer, die als Klassifizierung zur Auswahl stehen.

Das Anlegen und Bearbeiten von Klassifizierungseigenschaften ändert aber noch keine Dokumente ab, sondern bietet nur die Verwendung der Eigenschaften an. Damit diese auch mit Dokumenten verknüpft werden, müssen Administratoren Klassifizierungsregeln erstellen. Über den Menübefehl *Klassifizierungszeitplan konfigurieren* können Sie festlegen, wann Klassifizierungsregeln starten sollen, ob Sie einen Bericht erhalten wollen, und wenn ja, in welchem Format. Klassifizierungsregeln werden durch Klassifizierungszeitpläne gesteuert. Die Klassifizierungsregeln verwenden wiederum die Klassifizierungseigenschaften.

Zusammenfassung

Dieses Kapitel sollte dazu dienen, Ihnen einen kurzen Einstieg zur Active Directory-Rechteverwaltung zu bieten. Und auch die Grundlagen der dynamischen Zugriffssteuerung waren Thema dieses Kapitels.

Im nächsten Kapitel zeigen wir Ihnen die Hochverfügbarkeit mit Windows Server 2012 R2. Wir sind bereits in Kapitel 9 auf Cluster und die Hochverfügbarkeit mit Hyper-V eingegangen.

Kapitel 34

Hochverfügbarkeit und Lastenausgleich

In diesem Kapitel:

In Kapitel 9 haben wir Ihnen bereits gezeigt, wie Sie Cluster mit Windows Server 2012 und Hyper-V aufbauen. In diesem Kapitel erfahren Sie, wie Sie den Netzwerklastenausgleich in Windows Server 2012 nutzen. Die Installation und Verwaltung von Clustern ist Thema von Kapitel 9.

Anwender greifen zum Beispiel über SharePoint-Webserver auf die SharePoint-Anwendungsserver zu. Um Webserver ausfallsicher zur Verfügung zu stellen, auch ohne SharePoint, ist der beste Weg der Einsatz eines Netzwerklastenausgleich-Clusters (Network Load Balancing, NLB). SharePoint 2013 bietet die Möglichkeit, zusammen mit dem Netzwerklastenausgleich (Network Load Balancing, NLB) von Windows Server 2012 einen NLB-Cluster für Webserver zu erstellen. Auf diese Weise können Sie auch diese Server leichter hochverfügbar machen.

Grundlagen des Lastenausgleichs

Die Anwender verbinden sich mit dem NLB-Cluster, der die Anwender anschließend auf die einzelnen Server verteilt. Netzwerklastenausgleich-Cluster haben die Aufgabe, die Last eines Servers auf mehrere Server zu verteilen, damit die Auslastung einzelner Server gesenkt und die Performance verbessert wird. Auch beim Einsatz der Remotedesktopdienste nutzen Sie diese Funktion (siehe Kapitel 28). Hier nehmen Sie die Einrichtung aber über die Remotedesktop-Verwaltungskonsole vor. Sobald Sie einen Serverdienst auf mehrere Server verteilen können, zum Beispiel bei Webservern, ergibt ein NLB-Cluster Sinn.

Generell ist es unerheblich, ob Anwender zum ersten oder zweiten Server verbunden werden. Bei NLB bauen die Clients eine Verbindung zum NLB-Cluster auf, der wie ein Failovercluster einen eigenen Namen und IP-Adresse hat. Anschließend verteilt der Cluster die entsprechende Anforderung der Anwender an einen Server im Cluster.

Beim Netzwerklastenausgleich können Sie bis zu 32 Server zu einem Netzwerklastenausgleich-Cluster zusammenfügen, der von außen über eine gemeinsame virtuelle IP-Adresse angesprochen wird und somit wie ein einziger Computer erscheint. Beim Zugriff durch die Anwender verteilt der Netzwerklastenausgleich die Anwender auf die Anwendungsserver der Farm. Dabei können Sie das Lastenausgleichsgewicht der einzelnen Hosts im Cluster für jeden einzelnen Server konfigurieren.

Fällt ein Host des Clusters aus, übernehmen die anderen Server im Cluster die Zugriffe der Anwender. Daten tauscht der NLB-Cluster allerdings nicht aus und NLB-Cluster verwenden auch keinen gemeinsamen Datenträger.

Das ist Sache eines Failoverclusters. Serverdienste wie Webserver können Sie aber vor Ausfall schützen, da diese keine Daten speichern müssen, sondern Daten nur weiterleiten. Der Zugriff der Clients erfolgt zwar über die virtuelle IP-Adresse des NLB-Clusters, aber letztlich auf die physischen Server in diesem Cluster. Für die Kommunikation der NLB-Hosts im NLB-Cluster können Sie auch IPv6 verwenden. Für einzelne Knoten lassen sich mehrere dedizierte IP-Adressen konfigurieren.

Mit dem Netzwerklastenausgleich-Manager nehmen Sie die komplette Steuerung des NLB-Clusters vor.

ACHTUNG Sie können Webserver auch über Hyper-V und NLB clustern, müssen aber an dieser Stelle bei der Konfiguration einiges beachten. Erstellen Sie einen NLB-Cluster, spielt die MAC-Adresse eine wichtige Rolle. In einigen Fällen ändert Windows diese MAC-Adresse in Hyper-V ab (siehe die Kapitel 7 bis 9). Standardmäßig verwendet Hyper-V dynamische MAC-Adressen. Jeder Host im Hyper-V-Cluster verfügt über einen eigenen Pool an MAC-Adressen.

Führen Sie im Cluster einen Failover durch, ändert sich die MAC-Adresse des virtuellen Servers beim nächsten Neustart. In diesem Fall funktioniert der virtuelle NLB-Cluster nicht mehr. Mehr zu diesem Thema lesen Sie auch in Kapitel 9. Sie können diesen Fehler aber leicht umgehen. Rufen Sie die Einstellungen der virtuellen Server im Hyper-V-Manager auf, klicken Sie auf *Netzwerkkarte* und aktivieren Sie die statische Zuordnung der MAC-Adressen. Diese Einstellung lässt sich aber nur vornehmen, wenn der Server ausgeschaltet ist. Aktivieren Sie außerdem noch Spoofing von MAC-Adressen für die Webserver. Microsoft beschreibt diesen Fehler auf der Webseite *http://support.microsoft.com/kb/953828/en-us* [Ms179-K34-01] noch genauer.

Notwendige Vorbereitungen für NLB-Cluster

Setzen Sie mehrere Netzwerkkarten in den Webservern ein, sollten Sie entweder für eine der Karten ein Standardgateway eintragen oder IP-Forwarding aktivieren. Diese Funktion ist in Windows Server 2012 allerdings standardmäßig deaktiviert. Um diese Funktion zu aktivieren, geben Sie in der Eingabeaufforderung den folgenden Befehl ein:

```
netsh interface ipv4 set int "<Name der LAN-Verbindung> forwarding=enabled
```

Durch diese Option erlauben Sie dem Server, IP-Pakete, die nicht zum lokalen Server gehören, an andere Server weiterzuleiten. Da die Server in einem Cluster laufen, ist das unbedingt notwendig.

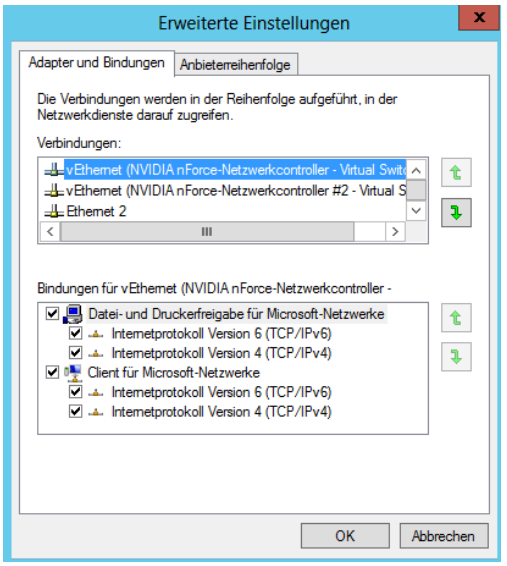
Sind im Server zwei Netzwerkkarten verfügbar, sollten Sie eine Karte für den NLB-Cluster, die andere für das produktive Netzwerk einsetzen, mit denen sich die Anwender verbinden. Außerdem sollten Sie sicherstellen, dass die Namen dieser Verbindungen im Netzwerk- und Freigabecenter entsprechend gesetzt sind. Ist im Server nur eine Netzwerkkarte vorhanden, müssen Sie hierbei nichts beachten.

Außerdem müssen Sie die Bindungsreihenfolge der Netzwerkkarten so anpassen, dass die Karte für das produktive Netzwerk an erster Stelle steht. 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 sind, bietet es sich an, die Reihenfolge so zu konfigurieren, dass Ihre produktive Netzwerkkarte 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 *Adaptereinstellungen ändern*.
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.
4. 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 Abschnitt *Verbindungen* auf die ausgewählte LAN-Verbindung und dann auf die Schaltflächen mit den Pfeilen, damit die gewünschte Verbindung ganz nach oben gesetzt wird.

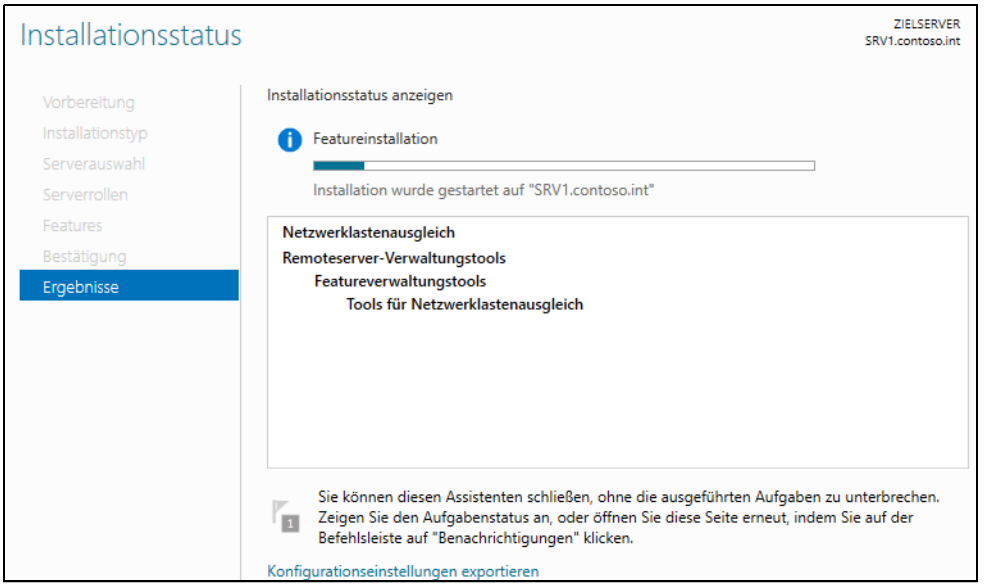
Abbildg. 34.1 Konfigurieren der Bindungsreihenfolge der Netzwerkverbindungen



Netzwerklastenausgleich installieren

Als Nächstes müssen Sie auf allen Webservern, die Sie in den NLB-Cluster aufnehmen wollen, das Netzwerklastenausgleich-Feature installieren. Unter Windows Server 2012 erfolgt dies über den Server-Manager.

Abbildg. 34.2 Netzwerklastenausgleich installieren



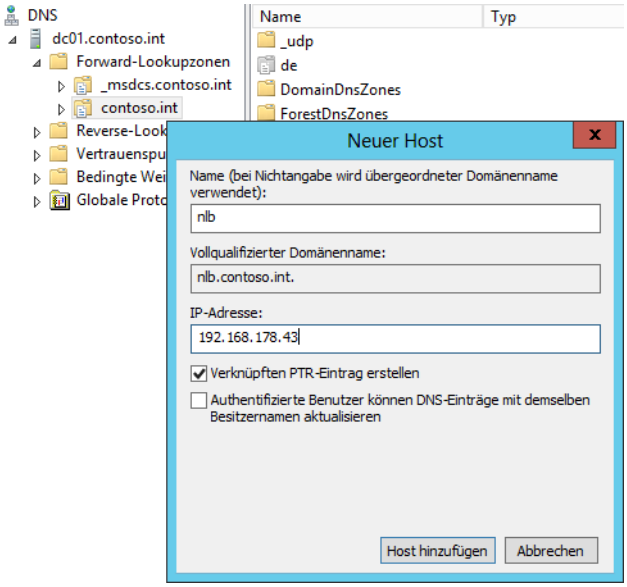
Öffnen Sie zur Installation den Server-Manager und klicken Sie auf *Verwalten/Rollen und Features hinzufügen*. Wählen Sie das Feature *Netzwerklastenausgleich* aus und führen Sie die Installation durch. Während der Installation des Features müssen keinerlei Konfigurationen vorgenommen werden.

Die Einrichtung des NLB-Clusters findet nachträglich in der entsprechenden Verwaltungskonsole statt. Installieren Sie das Feature auf allen Servern, die Sie zum NLB-Cluster hinzufügen wollen. Fügen Sie im Server-Manager über *Verwalten/Server hinzufügen* weitere Server hinzu, können Sie das Feature auf allen Servern im Cluster gleichzeitig installieren (siehe die Kapitel 3 und 4).

Nach der Installation können Sie auch gleich den DNS-Eintrag erstellen, in dem Sie den Namen und die IP-Adresse des NLB-Clusters hinterlegen. Anwender verwenden den Namen, den Sie an dieser Stelle hinterlegen, und werden zur IP-Adresse des NLB-Clusters weitergeleitet.

Rufen Sie zur Erstellung das DNS-Verwaltungsprogramm auf und erstellen Sie einen neuen Host-A-Eintrag mit dem Namen, den Sie dem NLB-Cluster geben wollen, und der IP-Adresse, die Sie dem NLB-Cluster zuweisen wollen (siehe Kapitel 25).

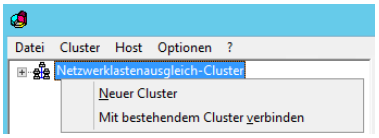
Abbildg. 34.3 Erstellen eines DNS-Eintrags für den NLB-Cluster



NLB-Cluster erstellen

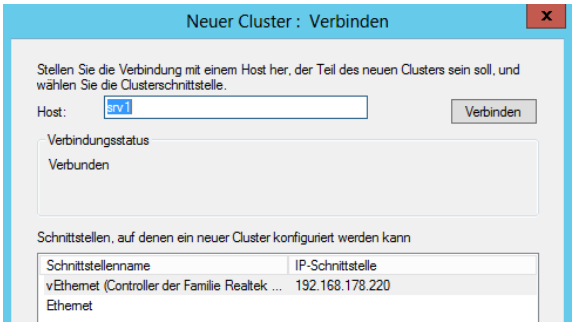
Nach der Installation erstellen Sie in der Netzwerklastenausgleich-Verwaltung einen neuen NLB-Cluster. Starten Sie dazu das Verwaltungsprogramm *Netzwerklastenausgleich-Manager* über das Menü *Tools* im Server-Manager. Klicken Sie dann mit der rechten Maustaste auf *Netzwerklastenausgleich-Cluster* und dann auf *Neuer Cluster.*

Abbildg. 34.4 Erstellen eines neuen NLB-Clusters



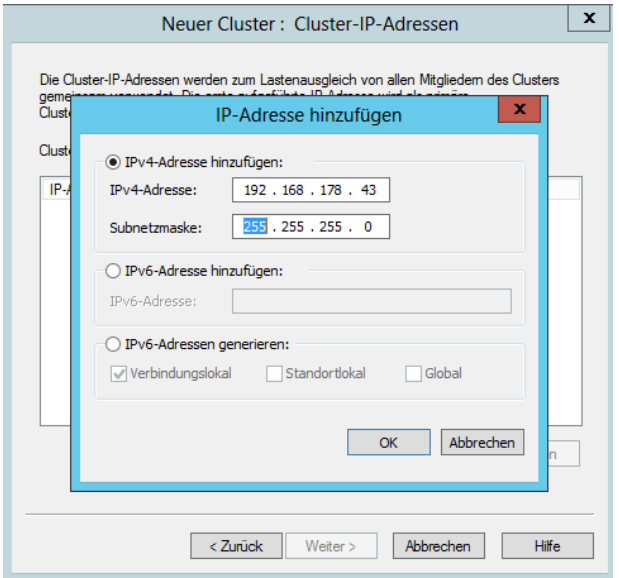
Geben Sie im neuen Fenster den Servernamen des ersten Clusterknotens ein und klicken Sie dann auf *Verbinden*. Wählen Sie die Netzwerkverbindung aus, die Sie für den NLB-Cluster verwenden wollen, und klicken dann auf *Weiter*.

Abbildg. 34.5 Verbindungsaufbau mit dem ersten Clusterknoten im NLB-Cluster



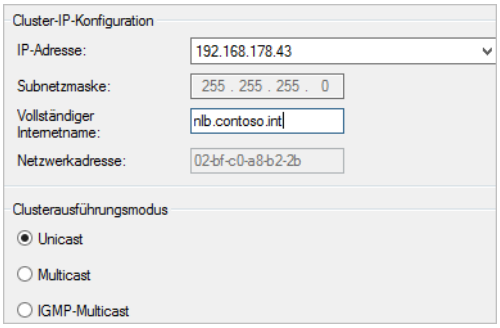
Belassen Sie auf der nächsten Seite *Hostparameter* alle Einstellungen, wie sie sind. Auf der nächsten Seite fügen Sie die IP-Adresse hinzu, die Sie dem NLB-Cluster als Ganzes zuweisen wollen. Hier tragen Sie die IP-Adresse ein, die Sie auch als Hosteintrag auf dem DNS-Server hinterlegt haben.

Abbildg. 34.6 Festlegen der IP-Adresse des NLB-Clusters



Auf der nächsten Seite hinterlegen Sie bei *Vollständiger Internetname* den DNS-Eintrag als FQDN, den Sie in DNS hinterlegt haben. Belassen Sie den Clusterausführungsmodus auf *Unicast*. Stellen Sie Verbindungsprobleme fest, können Sie an dieser Stelle auch *Multicast* verwenden.

Abbildg. 34.7 Festlegen des Namens des NLB-Clusters



Bei Unicast erhält jeder Server im NLB-Cluster die gleiche MAC-Adresse. Die vorhandene MAC-Adresse der Netzwerkkarten entfernt der Assistent dabei. Setzen Sie Multicast ein, fügt der Assistent den MAC-Adressen der Netzwerkkarten eine zusätzliche MAC-Adresse hinzu. Die Clients können dann über ihre alte MAC-Adresse und über die neue des NLB-Clusters kommunizieren.

Auf der nächsten Seite belassen Sie die angelegte Standardregel oder passen diese an, wenn die Standardeinstellungen nicht für Ihre Umgebung geeignet sind, zum Beispiel bei besonderen Sicherheitsvorgaben.

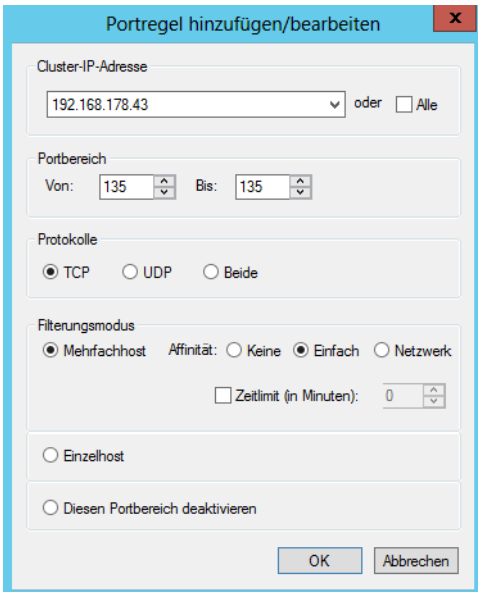
Nutzen Sie Mulicast-IP-Adressen mit IGMP, sind Class-D IP-Adressen erforderlich. Auf der nächsten Seite löschen Sie auf Wunsch die angelegte Standardregel und erstellen mit *Hinzufügen* eine neue Regel. Die Regeln dienen dem Zugriff der Clients über das Netzwerk. Standardmäßig wartet ein NLB-Cluster auf allen Ports seiner konfigurierten IP-Adressen auf Anfragen. Diese sollten Sie in sicheren Umgebungen aber einschränken.

Erstellen Sie eine eigene Regel, deaktivieren Sie die Option *Alle* bei *Cluster-IP-Adresse* und wählen Sie die IP-Adresse des Clusters aus. Wollen Sie zum Beispiel einen NLB-Cluster für *Exchange-Clientzugriffserver erstellen* (auch CAS-Array genannt), haben Sie die Möglichkeit, die Regeln anzupassen:

1. Als Portbereich verwenden Sie *135* als Anfangs- und als Endwert.
2. Aktivieren Sie bei *Protokolle* die Option *TCP*.
3. Aktivieren Sie bei *Filterungsmodus* die Option *Mehrfachhost*.
4. Belassen Sie die Einstellung für *Affinität* auf *Einfach*.
5. Klicken Sie dann auf *OK*.

Erstellen Sie beim Einsatz von Exchange anschließend eine weitere Regel. Hier hinterlegen Sie als Portbereich die Ports, die von Outlook und dem CAS-Array verwendet werden. Haben Sie einen statischen Port für die Kommunikation festgelegt, können Sie diesen eintragen.

Abbildg. 34.8 Anpassen einer Portregel für einen NLB-Cluster



Arbeiten Sie nicht mit dem statischen Port, sondern mit der Standardeinstellung von Exchange Server 2007/2010/2013, müssen Sie den Portbereich auf TCP 1024 bis 65535 verwenden. Sollen sich über das CAS-Array auch andere Clients verbinden, sollten Sie noch weitere Regeln für den entsprechenden Portbereich hinterlegen. Verwenden Sie dazu die gleichen Einstellungen und setzen Sie die notwendigen Ports ein. Setzen Sie noch IMAP oder POP3 ein, sollten Sie die Affinität für diese Regeln auf *Keine* setzen. Folgende Ports sind notwendig:

- Outlook Anywhere, Exchange ActiveSync, Outlook Web App – TCP 443
- IMAP4-SSL – TCP 993
- POP3-SSL – TCP 995
- IIS-Umleitung von HTTP auf HTTPS – TCP 80

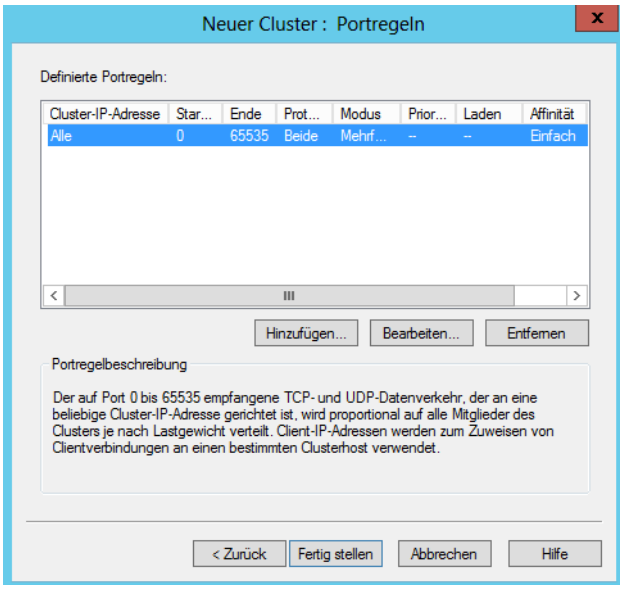
Diese Regeln müssen Sie aber nur hinterlegen, wenn Sie die entsprechenden Protokolle auch tatsächlich verwenden. Haben Sie alle Regeln erstellt oder verwenden Sie die vorgefertigte Standardregel, klicken Sie auf *Fertig stellen*.

Achten Sie bei der Konfiguration auch bei der Zuweisung des Zertifikats zu den Servern auf den allgemeinen Zugriffsnamen des Zertifikats. Da die Clients nicht den Servernamen verwenden, sondern den Namen des NLB-Clusters, muss dieser Name auch als allgemeiner Name im Zertifikat hinterlegt sein. Alle NLB-Mitglieder sollten am besten das gleiche Zertifikat verwenden, und zwar mit dem identischen Namen, den Sie auch als Name für den NLB-Cluster verwenden. Häufig kommen dabei Subject Alternative Name (SAN) SSL-Zertifikate zum Einsatz. Mit diesen können Sie mehrere Domänen mit einer einzelnen IP-Adresse verbinden.

Auf diesem Weg lassen sich mehrere Webseiten, Domänen und URLs mit einem einzigen Zertifikat abdecken. Verbindet sich ein Client per MAPI mit einem Clientzugriffserver, also mit Outlook im internen Netzwerk oder über Outlook Anywhere über das Internet, spielt das RPC-Protokoll mit seinen dazugehörigen Ports eine wichtige Rolle. Zwischen dem Clientzugriffserver findet eine Verbindung zwischen dem Port 135 und dem dynamischen Portbereich 6005-59530 statt.

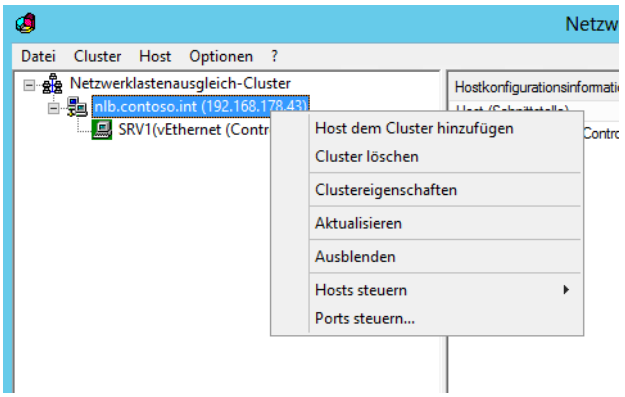
Vor allem beim externen Zugriff kann es sinnvoll sein, den dynamischen Bereich einzugrenzen, da Sie ansonsten zahlreiche Ports in Firewalls oder Routern öffnen müssen. Dazu sind Änderungen in der Registry auf den Clientzugriffservern und den Postfachservern vorzunehmen. Haben Sie alle Regeln bearbeitet oder erstellt, klicken Sie auf *Fertig stellen*.

Abbildg. 34.9 Konfigurieren von Zugriffsregeln für NLB-Cluster



Anschließend sehen Sie in der Verwaltung des Netzwerklastenausgleichs den Cluster, der aktuell nur ein Mitglied hat. Im nächsten Schritt fügen Sie weitere Webserver zum NLB-Cluster hinzu. Achten Sie darauf, dass auf allen Mitgliedern auch das Feature für den Netzwerklastenausgleich installiert sein muss. Klicken Sie mit der rechten Maustaste auf den erstellten Cluster und wählen Sie die Option *Host dem Cluster hinzufügen* aus.

Abbildg. 34.10 Hinzufügen weiterer Server zum NLB-Cluster



Geben Sie den Namen des Servers ein, den Sie hinzufügen wollen, und klicken Sie auf *Verbinden*. Übernehmen Sie die Standardeinstellungen auf der Seite *Hostparameter*. Behalten Sie die bereits erstellten Portregeln bei und klicken Sie auf *Fertig stellen*. Fügen Sie alle Server auf dem gleichen Weg hinzu und stellen Sie sicher, dass die Verbindung funktioniert, also kein Fehler in der Clusterverwaltung angezeigt wird.

Exchange-Hub-Transport auf NLB-Clustern

Haben Sie die Hub-Transport-Rolle auf den gleichen Servern installiert wie die Clientzugriffsrolle, können Sie den NLB-Cluster nicht für Hub-Transport-Server verwenden. Exchange arbeitet intern mit bestimmten Mechanismen für den E-Mail-Versand und die Sicherheit zwischen Hub-Transport-Servern, sodass dieser Einsatz nicht empfohlen ist.

Um Hub-Transport-Server ausfallsicher zu gestalten, reicht es aus, pro Active Directory-Standort einfach mehrere Hub-Transport-Server zu installieren. In Exchange Server 2010/2013 hat Microsoft auch Techniken integriert, um den Ausfall von Hub-Transport-Servern abzufangen und den Versand von E-Mails sicherzustellen, indem der Quellserver diese erneut versendet.

Bei Exchange Server 2010/2013 wartet immer der sendende Server darauf, dass der empfangende Server die E-Mail entweder in ein Postfach oder einen weiteren Transportserver zugestellt hat. Bemerkt der sendende Server, dass eine E-Mail auf dem Empfangsserver nicht zugestellt werden kann, versucht Exchange Server 2010/2013 eine Zustellung auf einem alternativen Weg.

Beispiel: Server A schickt eine Mail an Server B, der die E-Mail zwar entgegennimmt, aber aufgrund von Netzwerkproblemen nicht an Server C weiterleiten kann. Server A hat die E-Mail zwar erfolgreich an Server B zugestellt, diese aber noch nicht gelöscht. Stellt Server A fest, dass Server B die E-Mail nicht an Server C weitersenden kann, versucht Server A auf einem alternativen Weg, zum Beispiel über Server D, die E-Mail an Server C zuzustellen. Auch hier behält Server A die E-Mail weiterhin auf dem Server, bis sichergestellt ist, dass Server D die E-Mail an Server C zugestellt hat. Die Kommunikation für diese Technik erfolgt mit den beiden SMTP-Befehlen XSHADOW und XQDISCARD.

NLB versus DNS-Roundrobin

Neben NLB können Sie auch über DNS-Roundrobin eine gewisse Ausfallsicherheit und Lastverteilung für Webserver ermöglichen. Die Konfiguration ist zwar sehr einfach, aber bei Weitem nicht so effizient wie ein NLB-Cluster.

Roundrobin ist ein einfacher Mechanismus, mit dem DNS-Server die Last auf Netzwerkressourcen, also auch verschiedene Server, verteilen können. Sie verwenden diese Funktion, um die Reihenfolge der zurückgegebenen Ressourceneinträgen bei DNS-Abfragen in der Antwort auf eine Abfrage zyklisch zu ändern, wenn es für den verlangten DNS-Domänennamen mehrere Einträge desselben Typs gibt. Einfach gesagt, erstellen Sie für jeden Server einen DNS-Eintrag mit demselben Namen und der jeweiligen IP-Adresse. Auf diese Weise können Sie in DNS konfigurieren, dass Clients bei der Namensabfrage eines Servers immer eine andere IP-Adresse erhalten und diese dann verwenden.

Dabei tragen Sie einen Hostname mehrfach mit jeweils einer anderen IP-Adresse in die DNS-Zone ein. 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 steht im Durchschnitt jeder Eintrag gleich häufig an erster Stelle.

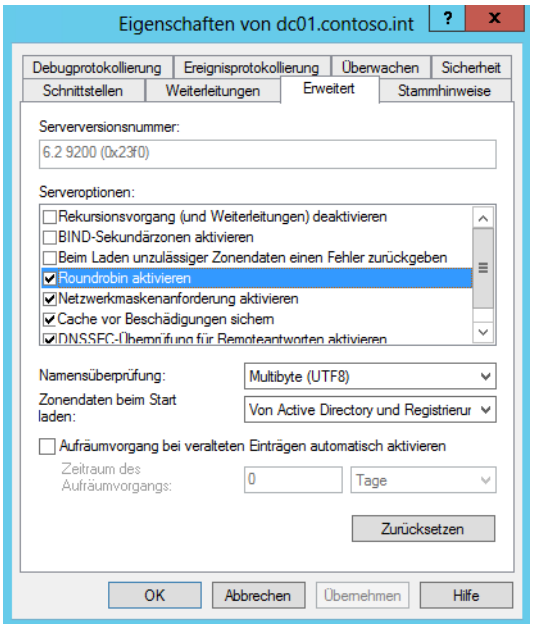
Um dem Client möglichst einen Server direkt in seiner Nähe zu nennen, ermittelt Roundrobin bei Hostnamen mit mehreren zugeordneten IP-Adressen vor der Umsortierung, ob es einen Eintrag gibt, der dem Subnetz des Clients zuzuordnen ist. Diesen setzt das DNS-System dann anschließend an die erste Stelle der zurückgegebenen Liste. Nur wenn kein passender eindeutiger Eintrag vorhanden ist, kommt Roundrobin zur Netzwerklastverteilung zum Einsatz. Um einen Roundrobin-Eintrag 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-Lookupeintrag mit der Bezeichnung des Roundrobin-Verbunds. Verwenden Sie als Namen keinesfalls den Namen eines Servers innerhalb der Verbunds, sondern einen eigenständigen Namen.
3. Tragen Sie als IP-Adresse die Adresse eines Servers 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 eines anderen Servers zeigt.
5. Abschließend haben Sie für jeden Server in der Farm einen Eintrag mit gleichem Namen und jeweils einer IP-Adresse für einen Server in der Farm.

Antwortet ein Server auf eine Clientanfrage nicht, erhält der Client einen Hinweis und muss die Anfrage wiederholen. Im Beispiel von Outlook äußert sich das in einer Fehlermeldung und die Anwender müssen Outlook neu starten und hoffen, dass der nächste Server verfügbar ist.

Aus diesem Grund ist NLB ein wesentlich effizienteres Mittel, um die Last zu verteilen und für die Ausfallsicherheit zu sorgen. Damit ein DNS-Server Roundrobin unterstützt, müssen Sie in der DNS-Verwaltung das Kontrollkästchen *Roundrobin aktivieren* in den Eigenschaften des Servers aktivieren (siehe Kapitel 25).

Abbildg. 34.11 Aktivieren von Roundrobin für DNS-Server mit Windows Server 2012



Data Center Bridging (DCB)

Data Center Bridging (DCB, siehe auch Kapitel 4) ist eine Suite aus IEEE-Standards (Institute of Electrical and Electronics Engineers), die verschiedene Datencenter miteinander verbinden können. DCB bietet eine hardwarebasierte Bandbreitenzuweisung (Bandwidth Allocation) für einen bestimmten Typ des Datenverkehrs und verbessert die Zuverlässigkeit der Datenübertragung durch die Verwendung von Prioritäten.

Die hardwarebasierte Bandbreitenzuweisung ist notwendig, wenn der Datenverkehr im Betriebssystem umgangen und auf einen Converged Network Adapter verlegt werden soll, der SCSI (Small Computer System Interface), Remotezugriff auf den direkten Speicher (RDMA) über Converged Ethernet oder Fiberchannel über Ethernet (FCoE) unterstützt.

Unternehmen, die zum Beispiel über ein großes Fibrechannel-SAN verfügen, erhalten durch DCB die Möglichkeit, ein Ethernet-basiertes Converged Fabric für Speicher- und Datennetzwerke zu erstellen. Damit die Funktion genutzt werden kann, müssen Switches und Netzwerkkarten diese neue Funktion unterstützen. Lesen Sie dazu auch das Kapitel 1 durch.

Administratoren können Anwendungen zu einer bestimmten Datenverkehrsklasse oder zu prioritätsbasierten Protokollen, TCP/UDP-Ports oder NetworkDirect-Ports anbinden. Die Steuerung erfolgt hauptsächlich über PowerShell-Cmdlets.

DCB verwenden das DCB Exchange Protocol (DCBX). Dieses erlaubt die Konfiguration von Servern, Netzwerkkarten und kompatiblen Switches. Sie installieren das Serverfeature am schnellsten in der PowerShell über *Install-WindowsFeature Data-Center-Bridging*. Sie können die Installation auch über den Server-Manager durchführen (siehe die Kapitel 3 und 4).

Müssen Sie den Server neu starten, verwenden Sie zum Beispiel das Cmdlet *Restart-Computer*. Eine Liste der wichtigsten Cmdlets sowie eine Hilfe dazu erhalten Sie mit dem Befehl *Help *qos**. Ausführliche Hilfen erhalten Sie in der PowerShell wie für alle anderen Cmdlets auch (siehe Kapitel 40). Wichtige Cmdlets in diesem Zusammenhang sind:

- *Set-NetQosPolicy...*
- *Disable-NetQosFlowControl*
- *Enable-NetQosFlowControl*
- *Get-NetQosDcbxSetting*
- *Get-NetQosFlowControl*
- *Get-NetQosTrafficClass*
- *New-NetQosTrafficClass*
- *Remove-NetQosTrafficClass*
- *Set-NetQosDcbxSetting*
- *Set-NetQosFlowControl*
- *Set-NetQosTrafficClass*
- *Disable-NetAdapterQos*
- *Enable-NetAdapterQos*
- *Get-NetAdapterQos*
- *Set-NetAdapterQos*

TIPP *New-NetQoSTrafficClass* zeigt ebenfalls Informationen an. Sie können den Befehl auch für andere Cmdlets nutzen. Auch *Get-Gelp New-NetQoSTrafficClass –Full | More* zeigt ausführliche Hilfen an. Sie können ebenfalls wieder jedes Cmdlet verwenden.

Bevor Sie eine umfassende Hilfe erhalten, müssen Sie mit *Update-Help* die PowerShell aktualisieren.

Sie können bis zu sieben Verkehrsklassen erstellen. Bei mehr Klassen sind aktuelle Netzwerkadapter überfordert. Die aktuellen Klassen lassen Sie sich mit *Get-NetQoSTrafficClass* anzeigen. Änderungen nehmen Sie mit *Set-NetQoSTrafficClass* vor, neue Klassen erstellen Sie mit *New-NetQoSTrafficClass.*

Enable-NetQosFlowControl aktiviert die Flusskontrolle, *Get-NetQosFlowControl* zeigt Informationen dazu an, mit *Disable-NetQosflowControl* deaktivieren Sie diese Funktion wieder.

New-NetQosPolicy erstellt neue Richtlinien, *Get-NetQosPolicy* zeigt die erstellten Richtlinien an, *Set-NetqosPolicy* ermöglicht das Ändern einer Richtlinie, *Remove-NetQosPolicy* löscht erstellte Richtlinien.

Get-NetAdapterQos zeigt Einstellungen für DCB für Netzwerkadapter an, *Disable-NetAdapterQos* deaktiviert DCB für einen Netzwerkadapter, *Enable-NetAdapterQos* aktiviert die Unterstützung.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie mit dem Netzwerklastenausgleich eine hochverfügbare Serverinfrastruktur für viele Server erschaffen. Im Kapitel 9 haben wir Ihnen bereits den Aufbau eines Failoverclusters am Beispiel von Hyper-V gezeigt. Ebenfalls Bestandteil dieses Kapitels ist Data Center Bridging, eine neue Funktion in Windows Server 2012 für sehr große Unternehmen.

Im nächsten Kapitel erfahren Sie, wie Sie Windows Server 2012 sichern und wiederherstellen können.

Kapitel 35

Datensicherung und Wiederherstellung

In diesem Kapitel:

Windows Server 2012 R2 verfügt über ein eigenes Sicherungsprogramm, mit dem Sie den Server und die Daten wiederherstellen können. Außerdem gibt es die Möglichkeit, die Datensicherung von Windows Server 2012 R2 an Windows Azure Online Backup (*http://www.windowsazure.com/de-de/home/features/online-backup* [Ms179-K35-01]) anzubinden. In diesem Fall können Sie Daten mit der Windows Server-Sicherung online in die Cloud sichern. Wie Sie dabei vorgehen, zeigen wir Ihnen in diesem Kapitel ebenfalls.

Sie haben auch die Möglichkeit, den kompletten Server mit der Windows Server-Sicherung zu sichern und dabei auch SQL Server-Datenbanken oder andere Daten zu berücksichtigen. Das Programm sichert die Daten über den Volumeschattenkopiedienst (Volume Shadow Service, VSS) mithilfe einer Technologie, die als Sicherung auf Blockebene (Block Level Backup) bezeichnet wird, in *.vhd*-Dateien.

HINWEIS In Kapitel 8 sind wir bereits auf die Sicherung von virtuellen Servern eingegangen. In Kapitel 16 zeigen wir Ihnen die Datensicherung von Active Directory. In diesem Kapitel erläutern wir die komplette Sicherung des Servers. Wie Sie Windows Server 2012 R2 Essentials sichern, lesen Sie im folgenden Kapitel 36.

Grundlagen der Datensicherung

Nach einem vollständigen Backup des Servers können einfach inkrementelle Sicherungen auf Blockebene erstellt werden. Auch diese benötigen deutlich weniger Platz als bei den Vorgängerversionen von Windows Server 2012 R2.

Die Systempartitionen des Servers werden automatisch immer in alle Sicherungen integriert, sodass die auf diesen Partitionen gespeicherten Daten immer sehr leicht wiederhergestellt werden können. Auf diese Weise stellen Sie nicht nur Daten wieder her, sondern auch die Systemdateien von Windows Server 2012 R2 und den installierten Serveranwendungen.

Mit der Windows Server-Sicherung lassen sich vollständige Server (alle Volumes), ausgewählte Volumes oder der Systemstatus sichern. Anschließend können Sie einzelne Volumes, Ordner, Dateien, bestimmte Anwendungen und den Systemstatus wiederherstellen. Mit der Verwaltungskonsole der Windows Server-Sicherung können Sie auch Sicherungen für Remotecomputer erstellen und verwalten. Damit Sie die Sicherung verwenden können, müssen Sie Mitglied der Gruppe *Administratoren* oder *Sicherungsoperatoren* sein.

TIPP In der Eingabeaufforderung verwenden Sie das Tool Wbadmin zur Konfiguration und Verwaltung der Sicherungen. Außerdem sind in Windows Server 2008 R2 und Windows Server 2012 R2 einige Cmdlets für die PowerShell enthalten. Auf der Seite *http://go.microsoft.com/fwlink/?LinkId=93317* [Ms179-K35-02] finden Sie dazu weitere Informationen.

Windows Server-Sicherung installieren und konfigurieren

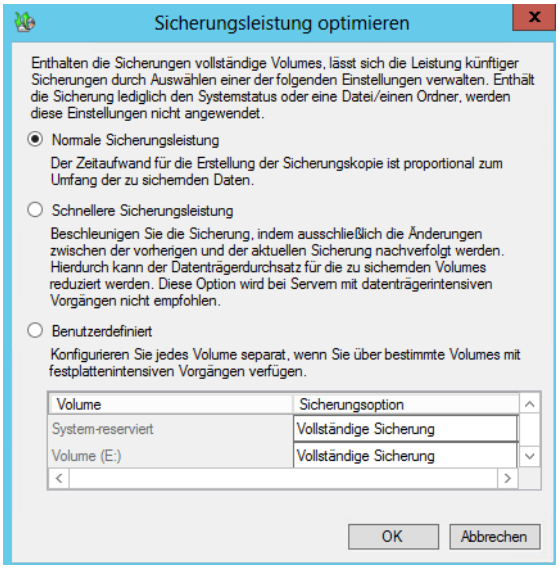
Damit Sie die Windows Server-Sicherung verwenden können, installieren Sie diese über den Server-Manager als neues Feature. Die Sicherungsfunktionen von Windows Server 2008 R2 sind in die beiden Unterkomponenten *Windows Server-Sicherung* und *Befehlszeilentools* unterteilt. In Windows Server 2012 R2 gibt es dazu nur noch ein einziges Feature mit der Bezeichnung *Windows Server-Sicherung*.

Nach der Installation starten Sie die Windows Server-Sicherung über das Menü *Tools* im Server-Manager mit dem Befehl *Windows Server-Sicherung*. Alternativ können Sie auf der Startseite nach *wbadmin.msc* suchen. Diese Konsole können Sie darüber hinaus in jeder Microsoft Management Console (MMC) laden.

Die Datensicherung sichert die Daten blockbasiert von den Datenträgern, nicht pro Datei. Standardmäßig führt das Tool immer vollständige Sicherungen durch. Über den Menübefehl *Aktion/Leistungseinstellungen konfigurieren* können Sie aber auch eine inkrementelle Sicherungen aktivieren. 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. 35.1 Konfigurieren der Leistungsoptionen der Sicherung



Wenn Sie daher am Freitag Morgen eine vollständige Wiederherstellung durchführen müssen, werden erst die letzte Vollsicherung des letzten Freitags 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.

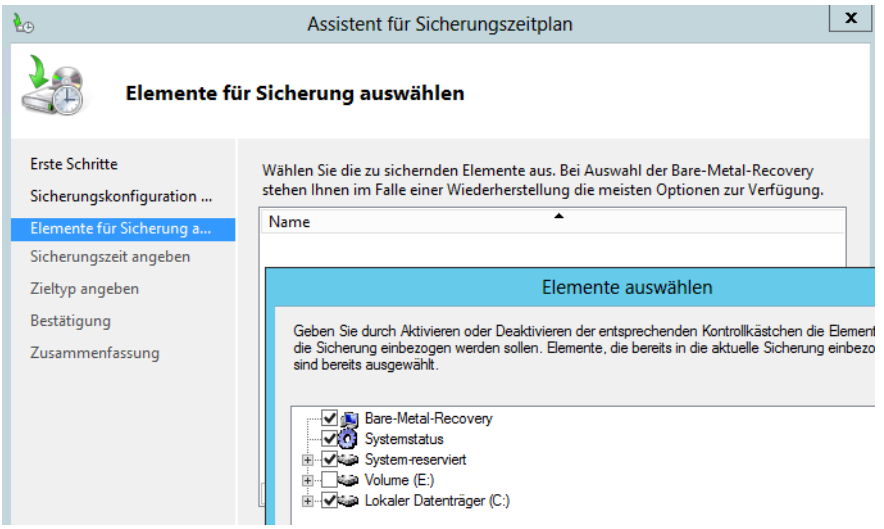
Nachdem die Sicherung und Verwaltungsprogramme installiert sind, können Sie eine Datensicherung einrichten. Microsoft empfiehlt zur Sicherung einen externen Datenträger, der über USB oder Firewire mit dem Computer verbunden ist.

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 bisher darauf gespeicherten Daten verloren gehen.

Um einen neuen Sicherungsauftrag zu erstellen, rufen Sie entweder über die Verwaltung die Konsole des Sicherungsprogramms auf oder geben auf der Startseite den Befehl *wbadmin.msc* ein. Der Befehl *wbadmin.exe* startet das Befehlszeilentool der Sicherung.

Einen neuen Auftrag erstellen Sie über *Aktion/Sicherungszeitplan*. Nach der Bestätigung der Begrüßungsseite wählen Sie auf der ersten Seite des Assistenten aus, ob Sie den kompletten Server sichern wollen oder benutzerdefinierte Volumes/Dateien auswählen möchten. Bei der benutzerdefinierten Sicherung wählen Sie auf nächsten Seite aus, welche Partitionen gesichert werden sollen.

Abbildg. 35.2 Auswählen der zu sichernden Partitionen des Servers



Auf der nächsten Seite legen Sie den Zeitplan fest, über den der Server gesichert werden soll. Hier definieren Sie, ob Sie die Sicherung mehrmals oder nur einmal pro Tag durchführen möchten. Als Nächstes wählen Sie aus, wie Sie Daten sichern wollen, also das Zielmedium. Haben Sie dieses ausgewählt, spezifizieren Sie die Auswahl auf der nächsten Seiten.

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 angezeigt und der Datenträger wird anschließend neu formatiert.

HINWEIS Die Windows Server-Sicherung überwacht automatisch den Speicherplatz auf den Datenträgern, auf denen die Sicherungen abgelegt werden. Steht nicht mehr genügend Plattenplatz zur Verfügung, werden Sie entsprechend darüber informiert und die Sicherung wird nicht durchgeführt. 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, können Sie den entsprechenden Assistenten über das Menü *Aktion* starten. Der Assistent übernimmt auf Wunsch die Einstellungen der vorhandenen geplanten Sicherung, erlaubt aber auch eigenständige Einstellungen.

Sicherung in der Eingabeaufforderung und PowerShell konfigurieren

Für Skripts oder Core-Server steht das Befehlszeilentool Wbadmin für die Verwaltung der Sicherungen zur Verfügung. Über */?* erhalten Sie für jeden der unten aufgelisteten Befehle eine entsprechende Hilfe eingeblendet. Die wichtigsten Befehle für das Tool sind:

- **Wbadmin enable backup** Erstellt oder ändert eine tägliche Sicherung
- **Wbadmin disable backup** Deaktiviert die tägliche Sicherung
- **Wbadmin start backup** Startet einmalig einen Sicherungsauftrag
- **Wbadmin stop job** Unterbricht eine laufende Sicherung oder Wiederherstellung
- **Wbadmin get disks** Zeigt aktuelle Datenträger an, die online sind
- **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
- **Wbadmin start systemstaterecovery** Stellt den Systemstatus wieder her
- **Wbadmin start sysrecovery/systemstatebackup** Startet eine vollständige Systemsicherung, die später in den Computerreparaturoptionen über die Windows Server 2008 R2- bzw. Windows Server 2012 R2-DVD wiederhergestellt werden kann
- **Wbadmin delete systemstatebackup -keepversions:n** Löscht alle Systemstatussicherungen bis auf die letzten *n* Versionen
- **Wbadmin delete systemstatebackup -deleteoldest** Löscht die jeweils älteste Systemstatussicherung

Weitere Befehle zur Sicherung sind:

- **Vssadmin list shadows /for=x:** Zeigt die vorhandenen Sicherungen für das Laufwerk *x:* an
- **Vssadmin delete shadows /for=x: /oldest** Löscht die jeweils älteste Sicherung des Laufwerks *x:*

Neben Wbadmin können Sie in Windows Server 2008 R2 die Datensicherung auch über die PowerShell steuern. Dazu müssen Sie in der PowerShell oder in PowerShell ISE zunächst die Befehle für die Datensicherung laden. Verwenden Sie dazu den Befehl *Add-PSSnapin Windows.Serverbackup*. Mit dem Befehl *Get-PSSnapin* überprüfen Sie, ob das Snap-In erfolgreich geladen ist.

Die PowerShell 3.0, die in Windows Server 2012 R2 integriert ist, muss keine PowerShell-Module laden, um die Befehle zu nutzen. Das verfügbare Modul für Windows Server 2012 R2 trägt die Bezeichnung *WindowsServerbackup*, muss aber nicht mehr geladen werden.

Mit dem Befehl *Get-Command –Module WindowsServerbackup* lassen Sie sich in Windows Server 2012 R2 die Cmdlets der PowerShell anzeigen. Mit den drei folgenden Befehlen lassen Sie sich eine ausführliche Hilfe und Beispiele der Cmdlets in der PowerShell anzeigen:

- *Get-Help <Cmdlet_Name> –Detailed*
- *Get-Help <Cmdlet_Name> –Examples*
- *Get-Help <Cmdlet_Name> –Full*

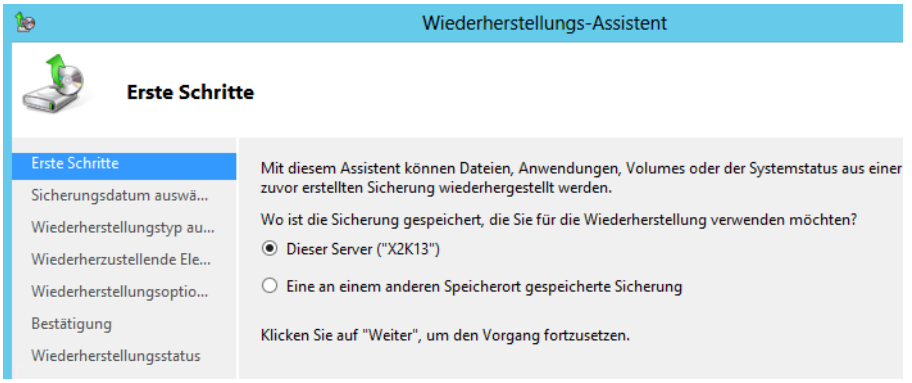
Um eine neue Sicherung über die PowerShell zu erstellen, müssen Sie zunächst einen Sicherungssatz anlegen, also eine Richtlinie, die steuert, welche Daten der Server sichern soll.

Daten mit dem Sicherungsprogramm wiederherstellen

Wenn auf dem Server Sicherungen zur Verfügung stehen, besteht auch die Möglichkeit, einzelne Dateien und Ordner wiederherzustellen. Auch dazu verwenden Sie das Sicherungsprogramm. Eine Wiederherstellung starten Sie über das Menü *Aktion*.

Auch hier führt ein Assistent durch die einzelnen Schritte der Wiederherstellung. Bestätigen Sie zunächst die Begrüßungsseite des Assistenten. Auf der nächsten Seite wählen Sie den Server aus, den Sie wiederherstellen wollen.

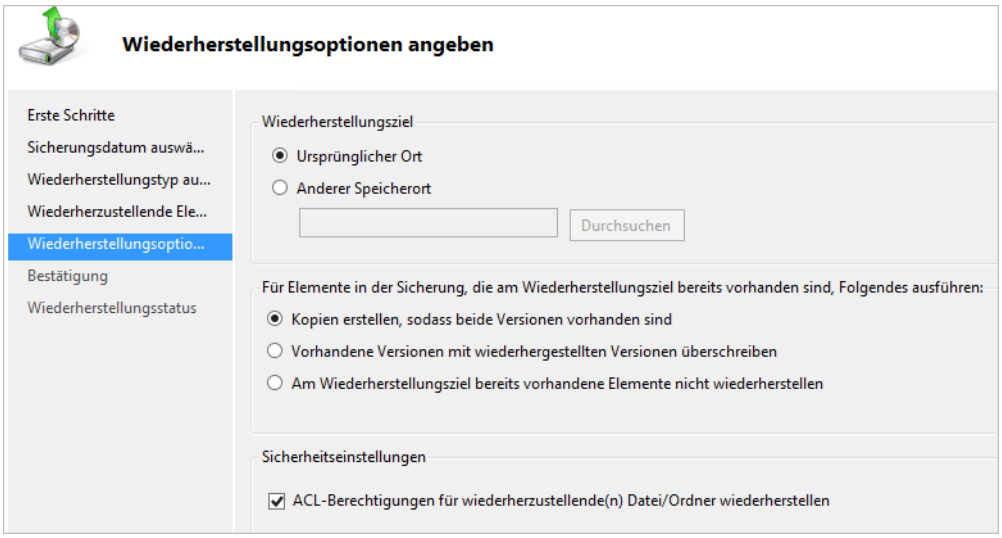
Abbildg. 35.3 Starten der Wiederherstellung und Auswählen des Servers



Danach legen Sie das Datum der Sicherung fest, aus der Sie Daten wiederherstellen wollen. Auf der nächsten Seite legen Sie fest, welche Daten Sie wiederherstellen wollen. Hier besteht die Möglichkeit, komplette Volumes wiederherzustellen oder nur einzelne Dateien und Ordner.

Auf der nächsten Seite wählen Sie aus, wo Sie die Dateien wiederherstellen wollen, ob vorhandene Dateien überschrieben werden dürfen und ob die Berechtigungen und Sicherheitseinstellungen der Dateien ebenfalls wiederhergestellt werden sollen.

Abbildg. 35.4 Auswählen der Wiederherstellungsoptionen



Kompletten Server mit dem Sicherungsprogramm wiederherstellen

Haben Sie auf dem Server eine vollständige Datensicherung erstellt, können Sie damit den kompletten Server wiederherstellen, falls dieser zum Beispiel nicht mehr starten kann. Dazu muss der Datenträger mit der Sicherung mit dem Server verbunden und dieser mit der Windows Server 2012 R2-DVD gebootet werden.

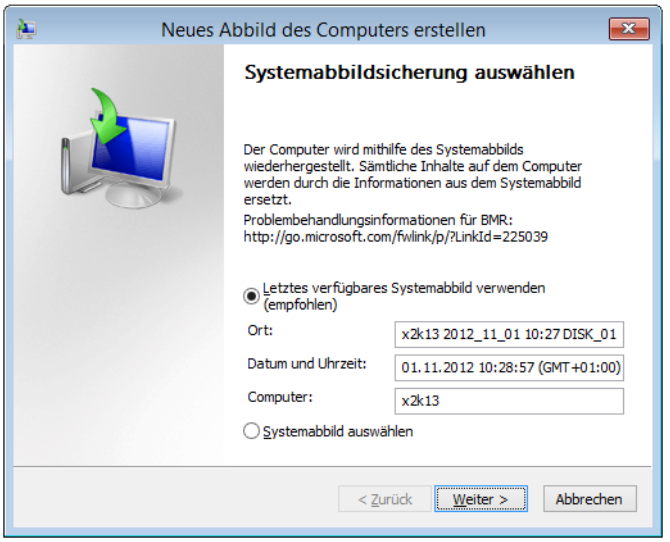
Auf der Startseite des Installations-Assistenten klicken Sie auf *Weiter*. Auf der nächsten Seite wählen Sie *Computerreparaturoptionen* aus. In den Systemwiederherstellungsoptionen wählen Sie die Option zur Wiederherstellung einer Systemabbildsicherung aus. Dazu klicken Sie auf *Problembehandlung* und *Systemimage-Wiederherstellung*.

Abbildg. 35.5 Erweiterte Wiederherstellungsmöglichkeiten in Windows Server 2012 R2

HINWEIS Windows Server 2008 R2 und Windows Server 2012 R2 unterstützen die Wiederherstellung einer Systemsicherung auch auf andere Hardware.

Sie können auswählen, aus welcher Sicherung Sie den Server wiederherstellen wollen, und anschließend auch die Datenträger, die wiederhergestellt werden sollen. Auf diese Weise können Sie das Betriebssystem wieder in einen lauffähigen Zustand zurückführen. Wichtig ist dabei, dass Sie die Bare-Metal-Restore-Möglichkeit bei der Sicherung ausgewählt haben.

Abbildg. 35.6 Auswählen der Sicherung, mit der Sie den Server wiederherstellen wollen



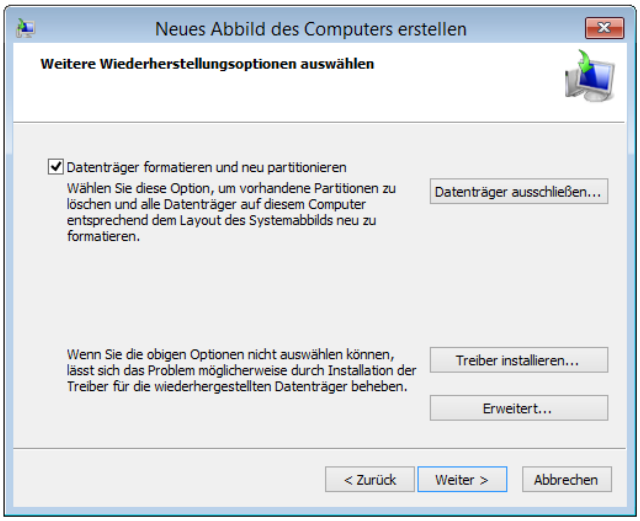
Als Nächstes wählen Sie aus, ob Windows den Datenträger formatieren und partitionieren soll oder ob Sie die Daten auf die bisherige Partition zurücksichern wollen.

Über die Schaltfläche *Datenträger ausschließen* wählen Sie die Datenträger aus, die nicht wiederhergestellt werden sollen, weil diese zum Beispiel Datenbankdateien von SQL Server 2012 enthalten.

Über *Treiber installieren* lassen sich wichtige Treiber integrieren, die für die Wiederherstellung unter Umständen benötigt werden. In den Optionen unter *Erweitert* legen Sie fest, dass der Server automatisch nach der Wiederherstellung neu starten und Datenträger auf Defekte überprüfen soll.

Zum Abschluss erscheint eine Meldung, die darüber informiert, dass die Datenträger neu formatiert werden. Diese Meldung müssen Sie bestätigen, bevor die Wiederherstellung beginnt. Anschließend beginnt der Assistent mit der Wiederherstellung des Servers. Nach der Wiederherstellung steht der Server wieder zur Verfügung. Sie sollten nach erfolgreicher Wiederherstellung den Status der Datenbanken überprüfen und unter Umständen aktuelle Sicherungen der SQL-Datenbanken wiederherstellen.

Abbildg. 35.7 Auswählen der Optionen zur Wiederherstellung eines Servers



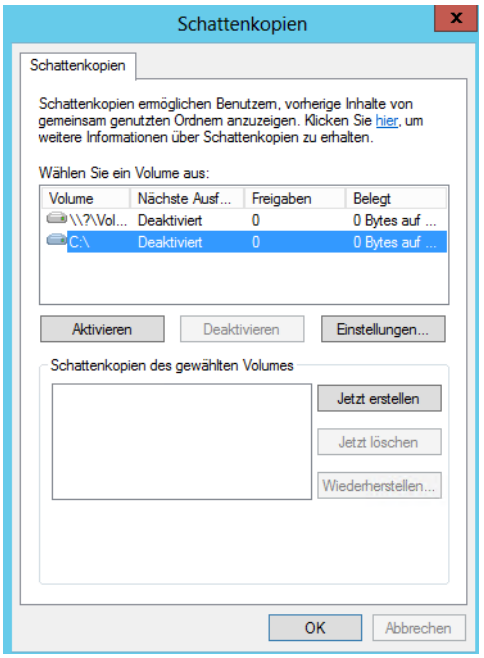
Verwenden von Schattenkopien

Eine Funktionalität von Windows Server 2012 R2 sind die Schattenkopien (siehe Kapitel 5). Die Idee ist, dass Änderungen auf einem Datenträger regelmäßig erfasst und gesichert werden. Auf diese Weise entstehen sozusagen Momentaufnahmen (Snapshots) des Systems zu unterschiedlichen Zeitpunkten. Damit lässt sich das System und einzelne Dateien wiederherstellen.

Schattenkopien konfigurieren

Benutzer können wieder auf frühere Versionen von Dateien zurückgreifen, indem Sie sie aus einer Schattenkopie wiederherstellen. Schattenkopien werden bei den Eigenschaften von Datenträgern auf der Registerkarte *Vorgängerversionen* verwaltet. Über das Kontextmenü eines Datenträgers im Explorer starten Sie die Konfiguration der Schattenkopien. Wählen Sie dazu den Befehl *Schattenkopien konfigurieren*. Wir kommen in den folgenden Abschnitten noch genauer auf diese Konfiguration zurück.

Abbildg. 35.8 Schattenkopien aktivieren und konfigurieren



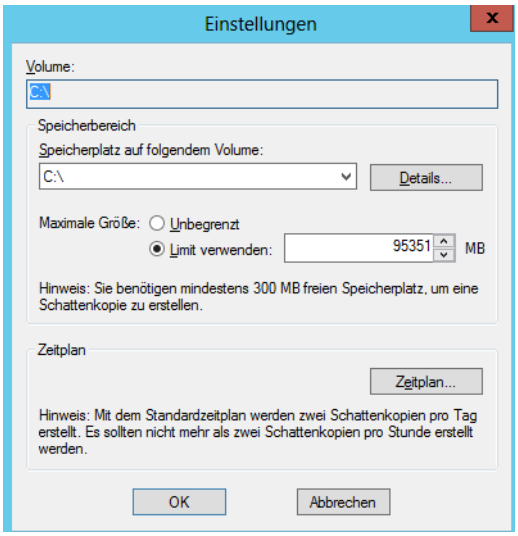
Konfigurieren Sie zunächst die Datenträger über die Schaltfläche *Einstellungen*, bevor Sie sie aktivieren. Bei der Nutzung von Schattenkopien müssen Sie berücksichtigen, dass dafür einiges an Speicherplatz erforderlich ist, da alle Änderungen gespeichert werden müssen.

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 diese 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.

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 Ordners, in dem sich die besagte Datei befindet, eine ältere Version der Sicherung wiederherzustellen.

Abbildg. 35.9 Konfigurieren der Schattenkopien für einen Datenträger



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 2012 R2 an jedem Wochentag (Montag bis Freitag) um 07:00 Uhr und um 12:00 Uhr eine Schattenkopie.

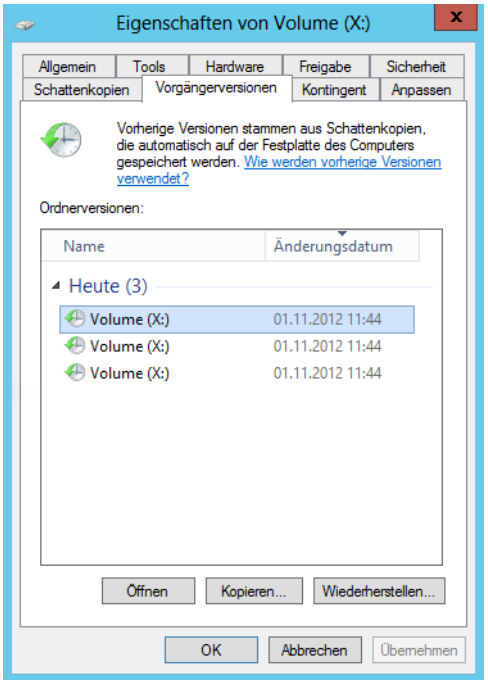
Je öfter Schattenkopien erstellt werden, umso mehr Versionen der Dateien stehen folglich zur Verfügung und können von ihren Benutzern oder Administratoren wiederhergestellt werden. Mit steigender Anzahl von Schattenkopien steigt auch der Speicherplatzbedarf.

Vorherige Version wiederherstellen

Schattenkopien können Kopien von Dateien auf Ihrem Computer oder freigegebene Dateien auf einem Computer in einem Netzwerk sein. Mithilfe vorheriger Dateiversionen können Sie Dateien wiederherstellen, die Sie versehentlich geändert oder gelöscht haben oder die beschädigt sind. Abhängig vom Datei- oder Ordnertyp können Sie eine vorherige Version öffnen, an einem anderen

Speicherort speichern oder wiederherstellen. Auch diese Wiederherstellung führen Sie über das Kontextmenü aus. Wählen Sie auf einem Clientcomputer die Option *Vorgängerversionen wiederherstellen* aus.

Abbildg. 35.10 Wiederherstellen von älteren Versionen Ihrer Dateien



Es öffnet sich ein neues Fenster, in dem der Client alle Versionen der Datei anzeigt, die sich wiederherstellen lassen. Sie können die vorherige Version entweder unter dem gleichen Namen in den gleichen Ordner kopieren oder die vorherige Version parallel zur vorhandenen Version wiederherstellen.

Wenn Sie auf die Schaltfläche *Wiederherstellen* klicken, wird die vorhandene Version der Datei durch die Schattenkopie ersetzt. Wählen Sie die Schaltfläche *Kopieren* aus, können Sie die ausgewählten Schattenkopien unter einem anderen Namen oder in einen anderen Ordner kopieren. Die ursprüngliche Version bleibt dabei erhalten.

Erweiterte Wiederherstellungsmöglichkeiten

In den folgenden Abschnitten zeigen wir Ihnen verschiedene Möglichkeiten, um Windows Server 2012 R2 wieder zu reparieren oder wiederherzustellen, falls der Server nicht mehr funktioniert. Um Windows Server 2012 R2 wiederherzustellen, verwenden Sie entweder die Windows Server 2012 R2-Installations-DVD oder drücken beim Bootvorgang die F8-Taste.

Problemaufzeichnung – Fehler in Windows nachvollziehen und beheben

Windows Server 2012 R2 bietet die Möglichkeit, Fehler in Windows aufzuzeichnen und für Spezialisten so aufzubereiten, dass diese den Fehler leicht nachvollziehen und überprüfen können. Diese schrittweise Aufzeichnung von Fehlern hat die Bezeichnung *Problemaufzeichnung*.

Am schnellsten starten Sie die Problemaufzeichnung, indem Sie *psr* auf der Startseite eintippen. Es öffnet sich die Oberfläche, mit der Sie die Aufzeichnung durchführen. Um einen Fehler aufzuzeichnen und weitergeben zu können, gehen Sie folgendermaßen vor:

1. Tippen Sie *psr* auf der Startseite ein.
2. Klicken Sie nach dem Start des Tools auf *Aufzeichnung starten*.
3. Gehen Sie exakt die Schritte in Windows oder dem jeweiligen Programm durch, die zum Fehler führen.
4. Per Klick auf *Kommentar hinzufügen* können Sie eigene Hinweise einfügen, wenn der Fehler nicht schnell offensichtlich ist.
5. Haben Sie den Fehler nachgestellt, klicken Sie auf *Aufzeichnung beenden*.
6. Speichern Sie die Datei als ZIP-Archiv ab.
7. Das Tool speichert die eigentliche Aufzeichnung als *.mht*-Datei, die Sie mit dem Internet Explorer öffnen können. Extrahieren Sie die *.zip*-Datei per Rechtsklick oder klicken Sie doppelt auf die *.zip*-Datei und dann auf die *.mht*-Datei. Sie sehen die Aufzeichnung des Problems als Dokument, das jeder nachvollziehen kann.

Bootprobleme beheben

Neben den standardmäßigen Wiederherstellungsmöglichkeiten in Windows Server 2012 R2 stehen Ihnen, wie in Windows Server 2008 R2, auch erweiterte Funktionen zur Reparatur zur Verfügung. Dazu booten Sie den Computer mit der Windows Server 2012 R2-DVD und starten die Computerreparaturoptionen. Alternativ wählen Sie *Computer reparieren* im erweiterten Bootmenü. Dieses erreichen Sie mit der F8-Taste beim Starten des Servers.

Es startet die Wiederherstellungsoberfläche von Windows Server 2012 R2. Klicken Sie auf *Problembehandlung*. Wählen Sie *Erweiterte Optionen* aus, um weitere Werkzeuge für die Reparatur zur starten. An dieser Stelle stehen Ihnen verschiedene Optionen zur Verfügung. Über *Systemimage-Wiederherstellung* kann Windows über eine Imagedatei wiederherstellen, die Sie zuvor auf dem Server mit der Windows Server-Sicherung erstellt haben. Die Erstellung läuft in Windows Server 2012 R2 genauso ab wie in Windows Server 2008 R2 bzw. Windows Server 2012.

Der Eintrag *Eingabeaufforderung* öffnet eine Eingabeaufforderung, über die Sie verschiedene Wiederherstellungsvorgänge starten können. In vielen Fällen hilft die Eingabe von *bootrec /fixmbr*, um den Boot-Manager zu reparieren, falls Windows Server 2012 R2 nicht mehr startet.

Funktioniert die deutsche Tastatur nicht korrekt, findet Sie den Schrägstrich »/« auf der Taste -. Der Befehl *bootrec /scanos* zeigt Betriebssysteme an, die zwar auf der Festplatte installiert, nicht aber im Boot-Manager eingetragen sind. Mit *bootrec /rebuildbcd* können Sie Windows Server 2012 R2-Installationen, die Sie mit *bootrec /scanos* gefunden haben, in den Boot-Manager integrieren. Oft hilft auch *bootrec /fixboot*, wenn Sie parallel zu Windows Server 2012 R2 noch ein anderes Betriebs-

system wie beispielsweise Windows Server 2008 R2 oder Hyper-V Server 2008 R2/2012 auf dem Server installiert haben.

Abbildg. 35.11 Erweiterte Startoptionen von Windows Server 2012 R2

Starten Sie den Server neu und drücken die F8-Taste, können Sie aus verschiedenen Optionen zur Wiederherstellung auswählen:

- **Debugmodus** Startet Windows in einem erweiterten Problembehandlungsmodus
- **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
- **Videomodus mit niedriger Auflösung aktivieren** Startet Windows mithilfe des aktuellen Videotreibers und mit niedrigen Einstellungen für Auflösung und Aktualisierungsrate. Mithilfe dieses Modus können Sie die Anzeigeeinstellungen zurücksetzen.
- **Abgesicherter Modus** Startet Windows mit den mindestens erforderlichen Treibern und Diensten
- **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
- **Erzwingen der Treibersignatur deaktivieren** Ermöglicht, dass Treiber mit ungültigen Signaturen installiert werden
- **Frühen Start des Treibers der Antischadsoftware deaktivieren** In Windows Server 2012 R2 startet der installierte Virenscanner wesentlich früher als in Windows Server 2008 R2. Das kann zu Problemen führen, wenn der Server nicht mehr startet. Hier deaktivieren Sie diesen Schutz.
- **Automatischen Neustart bei Systemfehler deaktivieren** Verhindert, dass Windows nach einem durch einen eigenen Fehler 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.

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 2012 R2 deutlich stabiler als seine Vorgänger.

Seit Windows Server 2012 ist es möglich, ohne aktivierte Antischadsoftware zu starten. Dies sollten Sie jedoch nur in Ausnahmefällen tun, da die Funktion verhindert, dass Viren vor dem Start des Virenscanners geladen werden.

Datensicherung über Ereignisanzeige starten

Mit Windows Server 2012 R2 können Sie eine Datensicherung des Servers auf einem Netzwerkspeicher anlegen, zum Beispiel einem NAS-System. Als zusätzliche Möglichkeit können Sie nach der erfolgreichen Datensicherung weitere Sicherungsmaßnahmen im Netzwerk durchführen, zum Beispiel durch selbst erstellte Batchdateien auf Basis des Befehlszeilentools Robocopy. Sobald ein Sicherungsjob startet, protokolliert Windows Server 2012 R2 einen Eintrag in der Ereignisanzeige.

An dieses Ereignis lässt sich sehr leicht eine Aufgabe über die Aufgabenplanung anbinden. Die Aufgabe wiederum kann eine Batchdatei starten, in welcher Daten auf verschiedene Freigaben im Netzwerk repliziert werden und Rechner heruntergefahren werden. Die Einrichtung ist nicht sehr kompliziert und baut komplett auf Bordmittel von Windows Server 2012 R2 auf.

Sie haben die Möglichkeit, über die Ereignisanzeige, zusammen mit der Aufgabenplanung, in Windows Server 2012 R2 weitere Aktionen durchführen zu lassen. Wollen Sie nach bestimmten Ereignissen in der Ereignisanzeige noch Batchdateien oder Befehle ausführen, können Sie die Funktion in Windows Server 2012 R2 nutzen, mit der sich Aufgaben an bestimmte Ereignisse anhängen lassen. Dazu klicken Sie mit der rechten Maustaste auf das Ereignis und wählen *Aufgabe an dieses Ereignis anfügen*. Das heißt, Windows startet die Aufgabe immer genau dann, wenn das entsprechende Ereignis auftritt. Im folgenden Assistenten wählen Sie dann aus, welche Befehle Windows ausführen soll. Im ersten Fenster weisen Sie der Aufgabe einen Namen zu.

Im zweiten Fenster sehen Sie noch einmal das Ereignis, zu dem Windows die Aufgabe startet. Im dritten Fenster wählen Sie die Option *Programm starten* aus. Als Nächstes geben Sie den Befehl und die Optionen ein, die Windows ausführen soll. Wollen Sie zum Beispiel nach der Sicherung verschiedene Aufgaben durchführen, zum Beispiel Replikationen mit Robocopy oder den Rechner herunterfahren oder auch beides, schreiben Sie am besten eine Batchdatei und lassen diese an dieser Stelle ausführen.

Ein Beispielskript könnte folgendermaßen aussehen. Als Dateiendung verwenden Sie entweder *.bat* oder *.cmd*.

Listing 35.1 Erstellen einer Batchdatei zur Sicherung

```
echo on
del C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Documents" "x:\backup\dokumente" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Pictures" "x:\backup\Pictures" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Documents" "z:\backup\dokumente" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Pictures" "z:\backup\Pictures" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Documents" "u:\backup\dokumente" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
robocopy "C:\Users\thomas\Pictures" "u:\backup\Pictures" /mir /r:5 /
log+:C:\Users\thomas\Desktop\backup.log
shutdown /s /t 30
```

So erhalten Sie immer eine 1:1-Kopie Ihrer wichtigsten Daten. Sie können ohne Weiteres auch mehrere Ordner sichern. Verwenden Sie in diesem Fall einfach mehrmals den Befehl nacheinander in einem Skript.

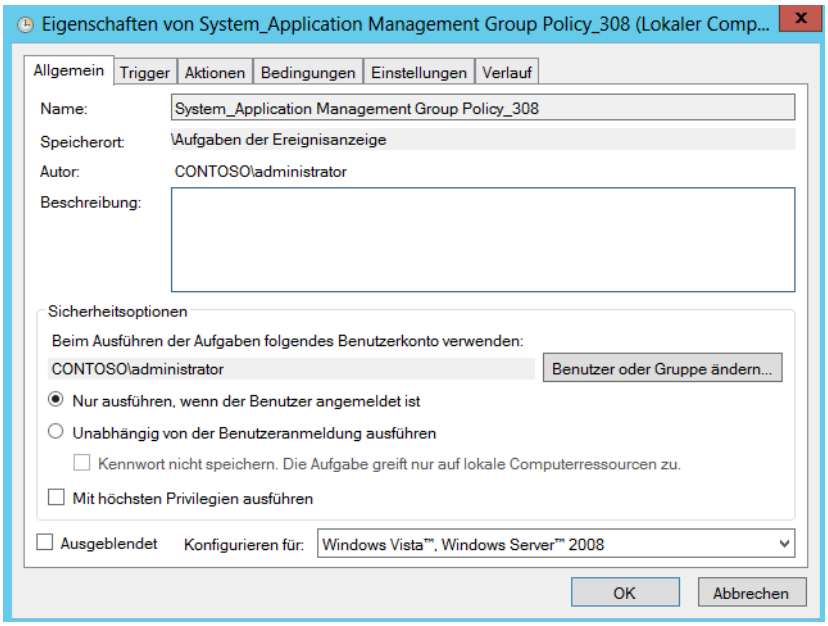
Haben Sie die Batchdatei ausgewählt, aktivieren Sie am Ende des Assistenten noch die Option *Beim Klicken auf "Fertig stellen", die Eigenschaften für diese Aufgabe öffnen*. Schließen Sie die Erstellung der Aufgabe ab, können Sie diese noch an Ihre Bedürfnisse anpassen.

Sie können die Aufgabe aber auch ohne diese Option jederzeit anpassen. Dazu starten Sie durch Eintippen von *Aufgabe* auf der Startseite die Aufgabenplanung. Die Aufgabe finden Sie über *Aufgabenplanungsbibliothek/Aufgaben der Ereignisanzeige*. Über das Kontextmenü rufen Sie die Eigenschaften der Aufgabe auf. Zunächst sollten Sie auf der Registerkarte *Allgemein* im unteren Bereich bei *Sicherheitsoptionen* ein Benutzerkonto auswählen, um die Aufgabe zu starten. Außerdem aktivieren Sie die Option *Mit höchsten Privilegien ausführen*, falls dies notwendig ist.

Auf der Registerkarte *Trigger* überprüfen Sie, ob die korrekte Ereignismeldung als Startwert ausgewählt ist. Bei *Aktionen* sollte Ihre Batchdatei erscheinen. Bei *Bedingungen* können Sie weitere Konfigurationen vornehmen, das gilt auch für die Registerkarte *Einstellungen*.

Alle Aufgaben, die Sie ausführen wollen, müssen Sie nur noch in die Batchdatei aufnehmen. Zur Sicherung und Replikation im Netzwerk bietet es sich zum Beispiel noch an, verschiedene Ordner an andere Ordner und Rechner im Netzwerk zu replizieren, am besten mit Robocopy. Anschließend können Sie den Rechner mit *Shutdown* herunterfahren lassen. Beide Tools gehören zum Lieferumfang von Windows Server 2012 R2.

Abbildg. 35.12 Konfigurieren einer Aufgabe für die Aufgabenplanung



Wenn Sie Datei- oder Ordnernamen kopieren, die ein Leerzeichen enthalten, geben Sie den Pfad in Anführungszeichen an, zum Beispiel *robocopy "C:\Users\thomas\Documents" "x:\backup\dokumente" /mir*. Alle Optionen verwendet das Tool von links nach rechts. Nach unserer Erfahrung verwenden die meisten Administratoren die Option */mir*, weil so schnell und einfach eine Spiegelung eines Ordners angelegt wird. Um die Daten in einer Freigabe auf einen anderen Rechner zu spiegeln, schreiben Sie am besten ein Skript mit dem Befehl *robocopy <Quellordner> <Sicherungslaufwerk>:\<Sicherungsordner> /mir*.

Die Option */mir* kopiert nur geänderte Dateien und löscht Dateien im Zielordner, die im Quellordner nicht mehr vorhanden sind. Das heißt, der erste Kopiervorgang dauert recht lange, da erst alle Dateien kopiert werden müssen. Der Zweite läuft aber deutlich schneller ab, da nur geänderte Dateien kopiert werden. Löschen Sie im Quellordner eine Datei, löscht der Kopiervorgang diese auch im Backupordner. So erhalten Sie immer eine 1:1-Kopie Ihrer wichtigsten Daten. Sie können ohne Weiteres auch mehrere Ordner sichern. Verwenden Sie in diesem Fall einfach mehrmals den Befehl nacheinander in einem Skript.

Gelöschte Dateien mit kostenlosen Profitools wiederherstellen

Haben Sie Dateien gelöscht oder ist eine Festplatte defekt, haben Sie mit Bordmitteln in Windows Server 2012 R2 nur dann die Möglichkeit, Daten wiederherzustellen, wenn Sie eine Datensicherung angefertigt haben. Ohne Datensicherung haben Sie unter Umständen keinen Zugriff mehr auf Dateien. Und auch alle Daten nach der letzten Sicherung sind weg. In solchen Notfällen können aber kostenlose Profitools helfen, die Daten wiederherzustellen.

Zur Wiederherstellung von nicht sicher gelöschten Dateien laden Sie sich zunächst das Freewaretool Restoration von der Seite *http://www3.telus.net/mikebike/RESTORATION.html* [Ms179-K35-03] herunter. Mit diesem Tool können Sie Computer auf gelöschte Dateien hin durchsuchen. Ein weiteres kostenloses Tool, welches bei der Wiederherstellung gelöschter Dateien helfen kann, ist PC Inspector File Recovery von der Seite *http://www.pcinspector.de* [Ms179-K35-04]. Auch hier erhalten Sie eine grafische Oberfläche, mit der Sie eine Wiederherstellung gelöschter Dateien durchführen können.

Das Tool PhotoRec ist eines der mächtigsten Werkzeuge, um Dateien wiederherzustellen, die Windows selbst nicht mehr reparieren kann. Laden Sie die Freeware von der Seite *http://www.cgsecurity.org/wiki/PhotoRec_DE* [Ms179-K35-05]. Auf der Seite erhalten Sie auch Hinweise und Anleitungen zum Umgang mit dem Tool. Auch hier müssen Sie das Tool nicht installieren, sondern können es direkt starten.

Es ist sehr wichtig, dass Sie das Tool über einen USB-Stick ausführen, damit Sie bei der Wiederherstellung nicht versehentlich Daten auf dem Computer überschreiben. Der Umgang mit dem Tool ist etwas komplizierter als Restoration, dafür kann PhotoRec weit mehr Dateien wiederherstellen.

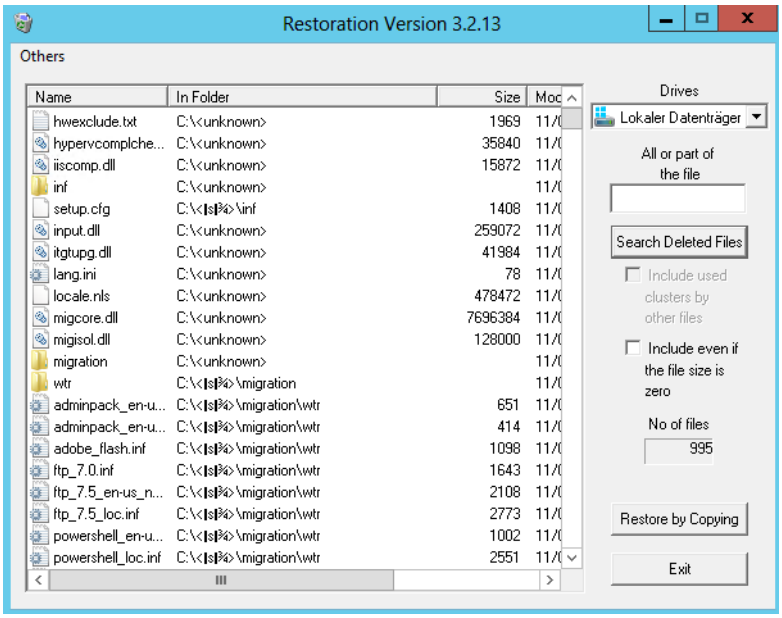
Dateien mit Restoration wiederherstellen

Restoration ist eines der bekanntesten Tools, um Daten wiederherzustellen, die normale Tools und Bordmittel nicht mehr lesen können

1. Laden Sie das Tool Restoration von der Seite *http://www3.telus.net/mikebike/RESTORATION.html* [Ms179-K35-03] und entpacken Sie das Archiv.
2. Kopieren Sie das Tool auf einen USB-Stick, um zu verhindern, versehentlich Dateien auf dem Computer zu überschreiben. Eine Installation ist nicht notwendig.
3. Starten Sie das Tool per Rechtsklick auf *restoration.exe* mit Administratorrechten.
4. Nach dem Start wählen Sie bei *Drives* die Festplatte aus, die Sie durchsuchen wollen.
5. Tragen Sie bei *All or part of the file* Dateiendungen in der Form **.bmp* ein, wenn Sie nicht alle gelöschten Dateien anzeigen wollen.
6. Klicken Sie auf *Search Deleted Files*.
7. Anschließend durchsucht das Tool die Festplatte und zeigt wiederherstellbare Dateien an.
8. Über *Restore by Copying* können Sie Dateien wiederherstellen und an einen beliebigen Ort kopieren.

ACHTUNG Verwenden Sie solche Wiederherstellungstools nur im absoluten Notfall und nur dann, wenn keine Datensicherung verfügbar ist. Auf Datenträgern mit dem neuen Dateisystem ReFS (siehe Kapitel 5) können Sie das Tool nicht einsetzen.

Abbildg. 35.13 Dateien mit Restoration wiederherstellen

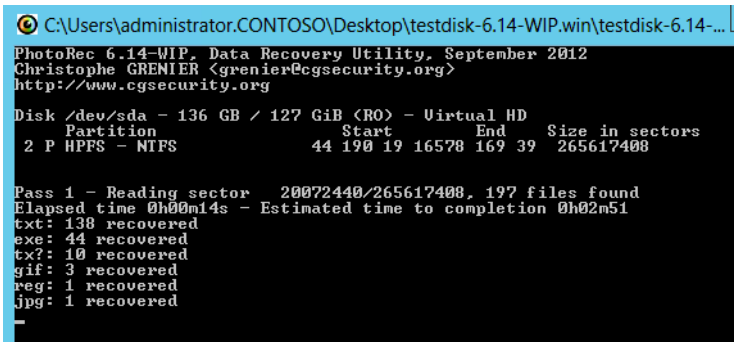


Dateien mit PhotoRec wiederherstellen

Neben Restoration ist PhotoRec (*http://www.cgsecurity.org/wiki/PhotoRec_DE* [Ms179-K35-05]) ebenfalls ein sehr bekanntes Tool, um gelöschte Dateien wiederherzustellen. Auch dieses Tool steht kostenlos zur Verfügung. Die Wiederherstellung erfolgt auf folgendem Weg:

1. Nach dem Entpacken des Archivs starten Sie *photorec_win.exe*.
2. Im ersten Schritt wählen Sie die Festplatte aus, von der Sie Daten wiederherstellen wollen.
3. Im nächsten Schritt wählen Sie die Art der Partitionstabelle aus, von der Sie Daten wiederherstellen wollen. Hier ist *Intel* die optimale Wahl für Windows-Betriebssysteme.
4. Neben der Auswahl der Partition müssen Sie noch das Dateisystem bestätigen.
5. Wählen Sie zunächst mit *Free* den freien Speicherplatz auf dem Datenträger zum Durchsuchen aus.
6. Als Nächstes wählen Sie den Datenträger und den Ordner aus, in den Sie die Daten speichern wollen. Hier können Sie durch Auswahl der zwei Punkte immer einen Ordner hochwechseln.
7. Mit der Taste [Y] bestätigen Sie, dass wiederherstellbare Dateien in dem entsprechenden Ordner gesichert werden sollen. Anschließend stellt das Tool die Daten wieder her.

Abbildg. 35.14 Daten mit PhotoRec wiederherstellen



Windows-Abstürze analysieren und beheben

Bluescreens sind in Windows Server 2012 R2 schon lange nicht mehr so häufig anzutreffen wie bei vorangegangenen Windows-Versionen. Was viele ärgert, soll das System jedoch schützen. 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. Neben fehlerhaften Treibern kommen Bluescreens auch sehr oft dann vor, wenn Hardware defekt ist.

Am häufigsten liegen dann Probleme mit dem Arbeitsspeicher oder einer überhitzten CPU vor. Ebenfalls weit verbreitet sind defekte Festplattencontroller oder Hauptplatinen. Auch wenn Windows an einem Dateizugriff scheitert, weil die Festplatte defekt ist, bedeutet das oft eine Ankündigung eines Plattenausfalls. Bei einem Bluescreen läuft Windows noch stabil genug, um den Fehler zu protokollieren und sich selbst sofort zu beenden.

Meistens erscheint eine achtstellige Hexadezimalzahl sowie eine kurze Beschreibung des Fehlers, oft IRQ_NOT_LESS_OR_EQUAL oder INACCESSIBLE_BOOT_DEVICE. Manchmal zeigt Windows auch die Datei an, die den Fehler verursacht hat – meistens eine *.sys*-Datei, also ein Treiber. Schreibt ein Treiber durch Programmierfehler in einen Arbeitsspeicherbereich, in dem sich bereits Daten eines anderen Treibers oder sogar des Systems befinden, stellt Windows sofort seinen Betrieb ein und meldet den Fehler als Bluescreen. Würde das System nicht so vorgehen, könnten durch die ungültigen Bereiche im Arbeitsspeicher Daten zerstört oder im Falle von Hardwaretreibern sogar die Hardware eines Computers in Mitleidenschaft gezogen werden.

Solche Kernelzugriffe von Treibern hat Microsoft 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 Server 2012 R2 ein Bluescreen erscheinen.

Bluescreens gibt es auch unter UNIX oder Linux, werden hier aber als »Kernel panic« bezeichnet. Der Prozessor kann bei mangelnder Kühlung zu heiß werden und eine eventuelle Übertaktung den Effekt noch verstärken. In Windows Server 2012 R2 gibt es das Windows-Speicherdiagnosetool, das Sie über den Befehl *mdsched* auf der Startseite aufrufen.

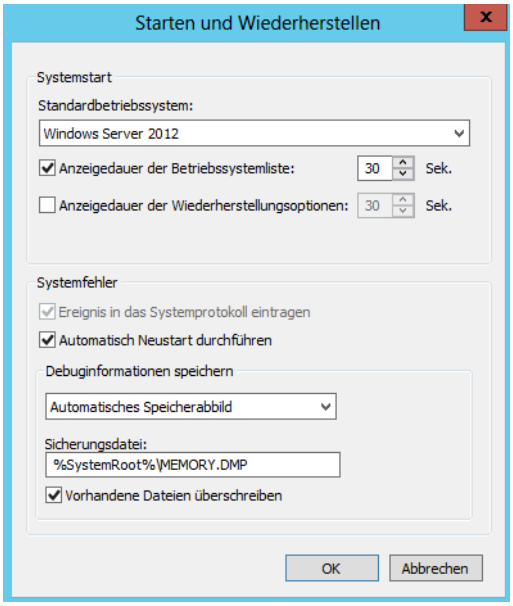
Windows Server 2012 R2 ist standardmäßig so eingestellt, dass nach einem Bluescreen automatisch der Rechner neu startet. Dies hat den Vorteil, dass der Server dann recht schnell wieder zur Verfügung steht. Allerdings können Sie in diesem Fall auch die entsprechende Fehlermeldung nicht lesen.

Erscheint der Bluescreen nach jedem Start, verfängt sich der Computer in einer Schleife, da er nach jedem Bluescreen neu startet. Die möglichen Einstellungen, wie sich Windows nach einem Bluescreen verhalten soll, finden Sie unter *Systemsteuerung/System und Sicherheit/System/Erweiterte Systemeinstellungen*. Klicken Sie im Abschnitt *Starten und Wiederherstellen* auf die Schaltfläche *Einstellungen*.

Über den Abschnitt *Systemfehler* lassen sich die Einstellungen vornehmen. Zunächst sollten Sie das Kontrollkästchen *Automatisch Neustart durchführen* deaktivieren, wenn Sie wollen, dass der Rechner bei der Anzeige des Bluescreens stehen bleiben soll. Über das Listenfeld *Debuginformationen speichern* wählen Sie aus, welche Art von Informationen das Betriebssystem protokollieren soll.

Am besten ist die Variante *Automatisches Speicherabbild* oder *Kleines Speicherabbild* geeignet, da andere Informationen ohnehin eher verwirrend sind. Hier legen Sie auch fest, in welchem Ordner das Speicherabbild mit dem Fehler abgelegt werden soll. Um eine *.dmp*-Datei mit den nachfolgend genannten Tools zu analysieren, laden Sie diese ganz normal in das jeweilige Programm.

Abbildg. 35.15 Windows Server 2012 R2 für Bluescreens konfigurieren



Eine gute Möglichkeit, um Bluescreens auf die Spur zu kommen, ist die Software BlueScreenView, die Sie von der Seite *http://www.nirsoft.net/utils/blue_screen_view.html* [Ms179-K35-06] herunterladen können. Sie erhalten Informationen zu den Bluescreens und können schneller Fehler finden. Der Vorteil des Tools ist, dass Sie den Viewer nicht installieren müssen. Er lässt sich daher auch über einen USB-Stick aufrufen.

Das Tool analysiert die Datei *memory.dmp*, die Windows mit dem Bluescreen erzeugt. Liegt diese Datei im Ordner *C:\Windows\minidump*, liest das Tool die Datei automatisch ein. Findet das Tool die Datei nicht, kopieren Sie *memory.dmp* von *C:\Windows* in den Ordner *C:\Windows\minidump*. Ist der Ordner nicht vorhanden, legen Sie ihn an. Nach dem Einlesen der Datei liefert der Fehler in der Spalte *Bug Check String* schon einen ersten Hinweis, den Sie für die Internetrecherche nutzen können.

Zusätzlich verwenden Sie noch den Code in der Spalte *Bug Check Code*. Klicken Sie doppelt auf *memory.dmp*, öffnet sich ein Detailfenster des Absturzes. Hat ein Treiber den Bluescreen verursacht, sehen Sie diesen in der Spalte *Caused by Driver*. Auch diese Information sollten Sie in die Recherche mit einbeziehen.

Können Sie den Bluescreen eingrenzen und erhalten über eine Suchmaschine nähere Informationen, zum Beispiel das Ändern bestimmter Registry-Schlüssel, sind Sie schon ein Stück weiter. Ist ein Treiber schuld am Fehler, installieren Sie eine aktualisierte oder ältere Version. Tritt ein Fehler bei Ihnen erst nach der Installation eines neuen Treibers auf, können Sie in Windows den vorherigen Treiber aktivieren, mit dem das System noch stabil läuft. Das geht natürlich nur dann, wenn Windows noch startet und Sie den Geräte-Manager aufrufen können.

Haben Sie den Treiber über ein Installationsprogramm installiert oder ist der Absturz nicht durch einen Treiber verursacht, sondern von einer von Ihnen installierten Anwendung, können Sie in Windows auch den Systemzustand wiederherstellen wie vor der Installation der Anwendung. Um den Zustand zurückzusetzen, müssen Sie Windows starten oder den Rechner über die Windows-DVD oder einen Rettungsdatenträger booten und die Computerreparaturoptionen starten. Setzen Sie in diesem Fall den Systemwiederherstellungspunkt zurück.

Oft stürzt in Windows nur ein einzelner Prozess ab oder belegt zu viele Ressourcen. Finden Sie diesen Prozess und beenden ihn, läuft Windows Server 2012 R2 in den meisten Fällen aber problemlos weiter:

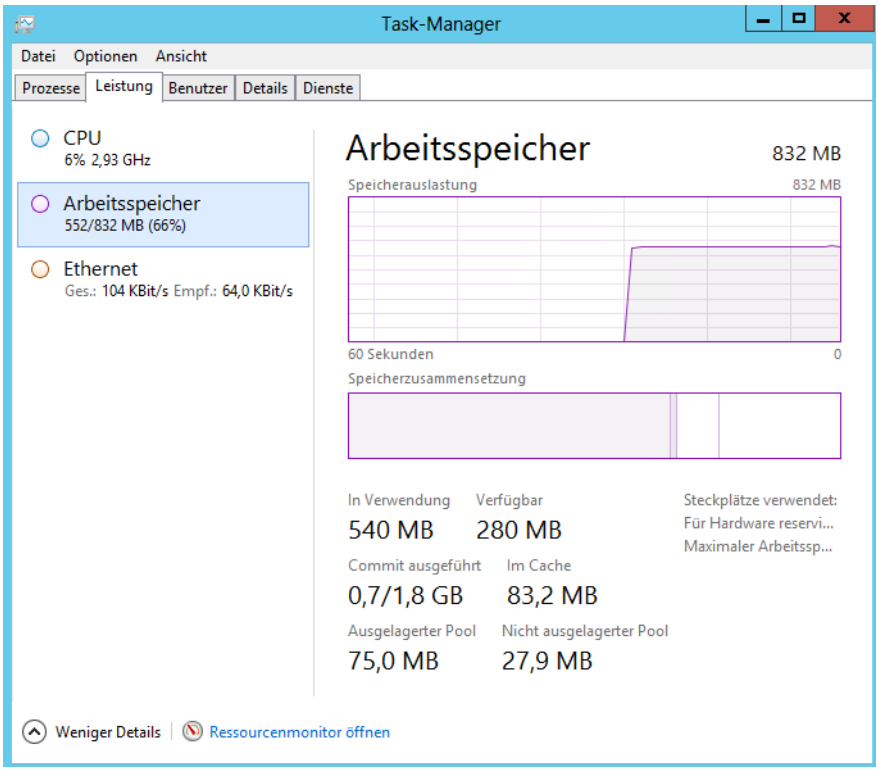
1. Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen Sie im Kontextmenü den Befehl *Task-Manager*. Alternativ starten Sie den Task-Manager auch mithilfe von Strg + Alt + Entf und der Auswahl des entsprechenden Befehls. Aktivieren Sie im unteren Bereich immer die Option *Mehr Details*.
2. Wechseln Sie zunächst zur Registerkarte *Leistung*. Manchmal verursachen Prozesse eine hohe CPU-Last von bis zu 100 % oder belegen den kompletten Arbeitsspeicher. Dauerhaft sollte die Belastung immer schwanken und nicht dauerhaft mehr als 30 bis 40 % betragen.

Rufen Sie anschließend die Registerkarte *Prozesse* auf. Hier sehen Sie Programme, die gestartet sind, und bei *Status* die Meldung *Keine Rückmeldung*, wenn ein Programm nicht mehr funktioniert. Versuchen Sie, ein solches Programm mit *Task beenden* zu beenden.

Auch wenn keine hohe CPU-Last vorliegt, kann dennoch ein Prozess das System lahmlegen. Handelt es sich um einen Prozess, der eine hohe CPU-Last verursacht, klicken Sie auf die Spalte *CPU*. Der Task-Manager sortiert anschließend die Prozesse absteigend nach dem CPU-Verbrauch. Hier sehen Sie recht schnell, welcher Prozess das Problem verursacht.

Verursacht ein Prozess zu viel Last, können Sie ihn beenden. Aber Achtung: Dabei können auch ungespeicherte Daten verloren gehen. Bevor Sie einen Prozess beenden, suchen Sie nach dessen Namen im Internet, wenn Sie ihn nicht kennen.

Abbildg. 35.16 Überwachen der Systemleistung in Windows Server 2012 R2



Speichern Sie möglichst alle Programme, die noch reagieren, und beenden Sie diese ordnungsgemäß. Klicken Sie den Prozess mit der rechten Maustaste an und wählen Sie *Task beenden*. Teilweise erscheint noch eine Rückfrage nach einigen Sekunden, dann beendet Windows den Prozess.

Reagiert Windows wieder, sollten Sie möglichst alle noch offenen Programme beenden und Daten speichern. Starten Sie anschließend den Rechner neu, damit Windows wieder alle notwendigen Prozesse starten kann. Beenden Sie den Explorer, fehlt oft die grafische Oberfläche. Diese starten Sie dann einfach über den Task-Manager mit *Datei/Neuen Task ausführen* und der Eingabe von *explorer*.

Windows Azure Online Backup

Eine der Neuerungen in Windows Server 2012 R2 ist die Möglichkeit der internen Datensicherung, eine Sicherung in der Cloud bei Microsoft abzulegen. Der Windows Azure Online Backup ist direkt in die Windows-Datensicherung integriert und lässt sich getrennt von einer lokalen Sicherung aktivieren und einstellen. Zusätzlich benötigen Sie einen speziellen Agent (*http://www.windowsazure.com/de-de/home/features/online-backup* [Ms179-K35-07]), der die Daten online speichern kann. Sie nutzen zur Sicherung und Wiederherstellung aber die bereits gewohnte Oberfläche der Windows-Datensicherung. Auch eine Steuerung in der Windows-PowerShell ist möglich. Dazu stellt PowerShell 3.0 ein eigenes Modul zur Verfügung.

Der Online Backup Service unterstützt auch inkrementelle Sicherungen und überträgt nur geänderte Blöcke bei der Sicherung. Die Daten der Sicherung werden durch den Agent verschlüsselt übertragen. Die Daten liegen dann auch verschlüsselt in Windows Azure. Nach der Sicherung überprüft Online Backup Service automatisch die Integrität der Daten. Außerdem können Sie für ältere Versionen von Sicherungen einen automatischen Verfall über Richtlinien festlegen. Die Daten der Sicherung werden in Windows Azure gespeichert. Wollen Sie den Onlinedienst nutzen, müssen Sie noch einen Agent auf dem entsprechenden Server installieren, der den Zugang herstellt.

Online Backup einrichten

Um die Datensicherung einzurichten, installieren Sie zunächst die Windows-Server-Sicherung. Dies müssen Sie über den Server-Manager mit *Verwalten/Rollen und Features hinzufügen* durchführen. Installieren Sie dazu das Feature *Windows Server-Sicherung* wie bei der herkömmlichen Sicherung

Anschließend installieren Sie den Online Backup Agent auf dem Server. Dieser installiert automatisch alle notwendigen Voraussetzungen (*http://www.windowsazure.com/de-de/home/features/online-backup* [Ms179-K35-07]).

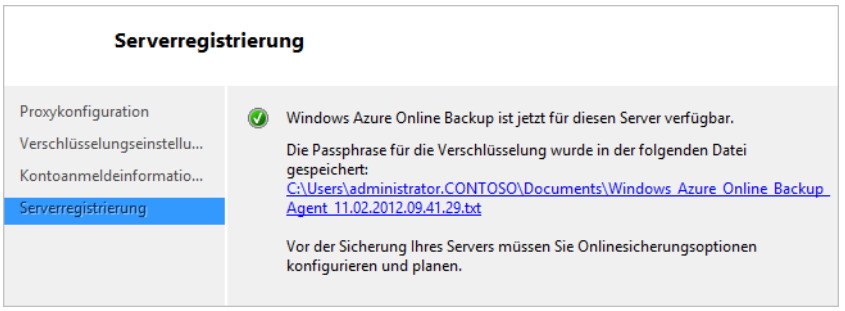
Während der Installation des Agents müssen Sie keine Eingaben durchführen. Die Einrichtung erfolgt nach der Installation des Agents über die Windows Server-Sicherung. Sie können die Installation des Agents aber auch in der Eingabeaufforderung mit verschiedenen Optionen skripten:

- /q Installation ohne Rückmeldung
- /l Installationsordner, zum Beispiel */l:"D:\Online-Agent"*
- /d Deinstallieren

Nach dem Start der Windows Server-Sicherung müssen Sie zunächst den Server in Windows Azure als Backupquelle registrieren. Sie müssen dazu die Anmeldedaten für Windows Azure kennen, die Sie zur Sicherung erhalten haben. Wir zeigen Ihnen in den nächsten Abschnitten, wie Sie die Registrierung in der grafischen Oberfläche und der PowerShell 3.0 durchführen. Registrierte Server können Sie über das Kontextmenü oder über die PowerShell wieder von Online Backup entfernen.

Dies hat den Vorteil, dass Sie die entsprechende Lizenz dann für einen anderen Server nutzen können. Für eine Onlinesicherungs-ID können Sie auch mehrere Server registrieren und lizenzieren. Alle Server können Sie dann zentral verwalten, um zum Beispiel Daten wiederherzustellen.

Abbildg. 35.17 Erfolgreiche Registrierung eines Servers für Windows Azure Online Backup



Haben Sie die Windows Server-Sicherung und den Agent installiert, finden Sie im Startbildschirm zwei neue Symbole zur grafischen Oberfläche und direkt zur Microsoft Online Backup Shell, dem PowerShell 3.0-Modul der Onlinesicherung. Sie finden die grafische Oberfläche aber auch in der normalen Verwaltungsoberfläche der Datensicherung von Windows Server 2012 R2 (*wbadmin.msc*). Die Befehle für die Onlinesicherung in der PowerShell können Sie auch in einer normalen PowerShell 3.0-Sitzung eingeben.

In der PowerShell lassen Sie sich die verfügbaren Cmdlets der Onlinesicherung mit *Get-Command *ob** anzeigen. Alternativ verwenden Sie den Befehl *Get-Command –Module MSOnlineBackup*. Sie müssen dazu keine Module mehr laden. Die PowerShell 3.0 kann Module automatisch beim Eingeben eines Cmdlets laden. In der PowerShell 3.0 hat Microsoft deutlich die Hilfefunktion erweitert. Rufen Sie eine Hilfe zu Cmdlets auf, kann sich die PowerShell selbstständig aktualisieren. Dies funktioniert eingeschränkt auch mit der früheren PowerShell 2.0, wenn Sie für das Cmdlet *Get-Help* die Option *–Online* verwenden, zum Beispiel mit *Get-Help Get-Command –Online*. Die PowerShell 3.0 bietet das neue Cmdlet *Update-Help*, welches die Hilfedateien der PowerShell aktualisieren kann. Dazu muss der Server über eine Internetverbindung verfügen. Der Befehl ruft die Hilfe direkt aus dem Internet ab.

Ebenfalls eine neue Funktion in der PowerShell 3.0 ist das Cmdlet *Show-Command*. Dieses blendet ein neues Fenster mit allen Befehlen ein, die in der PowerShell verfügbar sind. Sie können im Fenster nach Befehlen suchen und sich eine Hilfe zum Befehl sowie Beispiele anzeigen lassen. Sie müssen dazu aber die grafische Oberfläche PowerShell ISE nutzen. Um sich die Befehle von Online Backup anzeigen zu lassen, wählen Sie das Modul *MSOnlineBackup* aus.

Um die Verwaltung der Datensicherung zu starten, geben Sie auf der Startseite am besten *wbadmin.msc* ein und starten die Verwaltungskonsole. Sie finden eine entsprechende Kachel auch auf der Startseite. Klicken Sie als Nächstes auf *Online Backup*. Die Konsole überprüft den installierten Agent. Zunächst klicken Sie auf *Server registrieren*. Im Fenster geben Sie Zugangsdaten zu einem Proxyserver ein, wenn die Verbindung über einen Proxy laufen muss. Danach legen Sie ein Kennwort für die Verbindung fest. Anschließend geben Sie den Namen und das Kennwort für den Zugang ein. Sie sollten sich die Passphrase notieren. Geht diese verloren, haben Sie keinen Zugang mehr zur Sicherung. Hier kann auch Microsoft nicht helfen, da diese Daten geheim sind.

Im letzten Schritt schließen Sie den Vorgang zum Registrieren ab. Erst danach können Sie die Datensicherung einrichten. Schließt der Vorgang nicht erfolgreich ab, überprüfen Sie das Kennwort und den Anmeldenamen für den Zugang.

Sie können die Einrichtung über die PowerShell auch skripten. Dazu verwenden Sie die nachfolgenden Befehle. Im ersten Schritt speichern Sie das Kennwort für den Online Backup-Zugang verschlüsselt in einer Variablen:

```
$pwd = ConvertTo-SecureString -String <Kennwort> -AsPlainText -Force
```

Im nächsten Schritt speichern Sie die Anmeldung an Online Backup ebenfalls in einer Variablen und verwenden dazu die bereits gespeicherte Variable mit dem Kennwort:

```
$cred = New-Object -TypeName System.Management.Automation.PsCredential -ArgumentList
<Anmeldenamen>, $pwd
```

Haben Sie die Anmeldung gespeichert, führen Sie die Registrierung durch:

```
Start-OBRegistration –Credential $cred
```

Mit dem Cmdlet *Set-OBMachineSetting* legen Sie anschließend die Passphrase für das Verschlüsseln fest. Dazu können Sie zuvor auch diese Passphrase, wie bereits das Kennwort, verschlüsselt abspeichern:

```
$pass = ConvertTo-SecureString –String <Passphrase> -AsPlainText –Force
```

Wollen Sie in der PowerShell einen Proxyserver hinterlegen, verwenden Sie das Cmdlet:

```
$proxypwd = ConvertTo-SecureString -String <Passphrase> -AsPlainText –Force
Set-OBMachineSetting -ProxyServer <Name des Proxys> -ProxyPort <Port> -ProxyUsername
<Domäne\Benutzername> -ProxyPassword $proxypwd
```

Danach legen Sie die Passphrase für den Server fest:

```
Set-OBMachineSetting -EncryptionPassphrase $pass
```

Um einen Server in der PowerShell wieder von Online Backup zu entfernen, verwenden Sie

```
Start-OBUnregistration -Credential (Get-Credential)
```

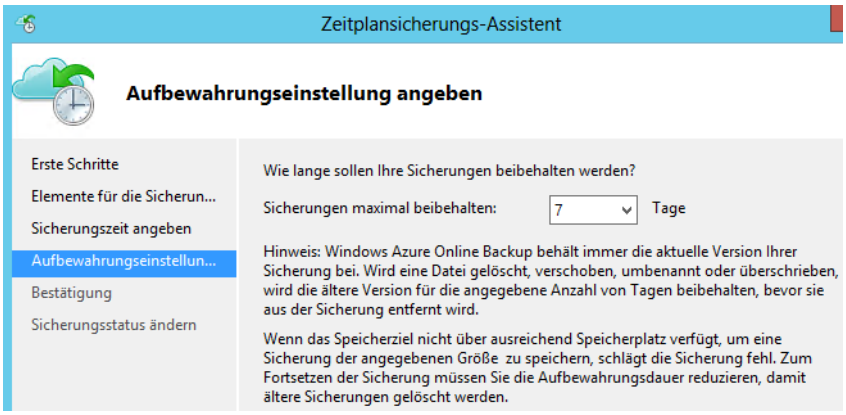
Zeitplan für die Onlinesicherung festlegen

Haben Sie den Server registriert, können Sie in der Verwaltungsoberfläche einen Zeitplan für die Sicherung festlegen. Dazu klicken Sie auf *Online Backup/Sicherung planen*. Zunächst legen Sie fest, welche Dateien Sie in die Sicherung mit einbeziehen wollen.

Haben Sie die Daten ausgewählt, legen Sie die Zeiten der Sicherung fest. Hier unterscheidet sich die Einrichtung nicht von der normalen Verwendung der Datensicherung. Als Nächstes definieren Sie, wie lange die Sicherung aufbewahrt werden soll. Ältere Sicherungen ersetzt der Assistent mit neuen Sicherungen, sobald der Zeitraum abgelaufen ist. Die Sicherungen bleiben so lange erhalten, bis eine neuere Sicherung den Platz benötigt.

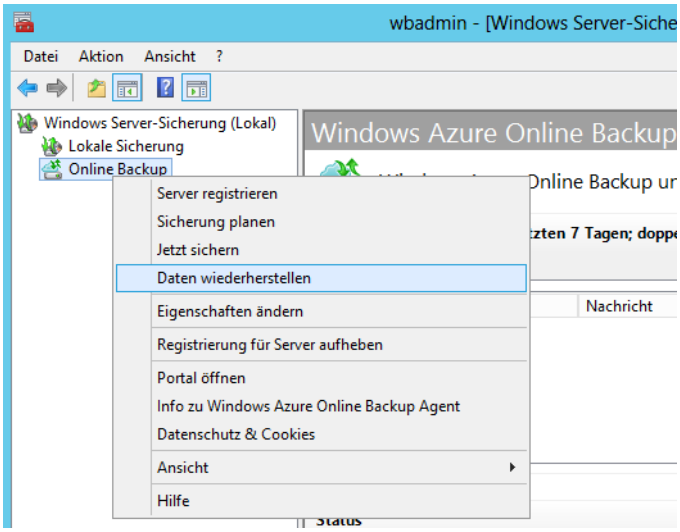
Bestätigen Sie danach die Eingaben und schließen Sie die Einrichtung ab. Sie können die Daten auch außerhalb des Sicherungszeitraums sichern. Dazu klicken Sie auf *Online Backup* und starten die sofortige Sicherung über den *Aktionen*-Bereich oder das Kontextmenü.

Abbildg. 35.18 Festlegen des Aufbewahrungszeitraums der Sicherung



Sie können immer nur einen Onlinesicherungsjob anlegen, aber parallel einen Zeitplan für eine lokale Sicherung und eine Onlinesicherung. Dies hat den Vorteil, dass Sie mit der lokalen Sicherung alle Daten sichern und mit der Onlinesicherung nur wichtige Daten. Sie können aber problemlos den Onlinesicherungsjob an mehreren Zeiten am Tag starten lassen.

Abbildg. 35.19 Verwalten der Onlinesicherung



Auch den Sicherungsjob können Sie in der PowerShell konfigurieren. Sie verwenden dazu am besten mehrere Cmdlets.

Zunächst erstellen Sie eine neue Richtlinie für die Sicherung und speichern diese in einer Variablen:

```
$policy = New-OBPolicy
```

Danach legen Sie den Ordner fest, welchen Sie mit der Sicherung berücksichtigen wollen. Auch hier verwenden Sie wieder eine Variable:

```
$files = New-OBFileSpec -FileSpec C:\daten
```

Danach legen Sie den Zeitplan fest, zudem Sie die Sicherung ausführen wollen. Auch diesen speichern Sie in einer Variablen:

```
$sched = New-OBSchedule -DaysofWeek Wednesday -TimesofDay 19:30
```

Anschließend legen Sie noch eine Richtlinie fest, die steuert, wann die Sicherung ablaufen soll:

```
$ret = New-OBRetentionPolicy
```

Wollen Sie die Einstellung vom Standardwert 7 Tage auf den Maximalwert 30 Tage setzen, verwenden Sie den Befehl:

```
$ret = New-OBRetentionPolicy -RetentionDays 30
```

Sie können die Richtlinie auch folgendermaßen erstellen, um die Sicherung zum nächsten festgelegten Zeitpunkt zu starten:

```
Add-OBFileSpec -Policy $policy -FileSpec $files
```

Anschließend verbinden Sie die Richtlinie mit dem erstellten Zeitplan:

```
Set-OBSchedule -policy $policy -Schedule $sched
Set-OBRetentionPolicy -Policy $policy -RetentionPolicy $ret
```

Handelt es sich um die erste Sicherung nach der Registrierung des Servers, müssen Sie noch sicherstellen, dass die Passphrase für die Sicherung gesetzt ist:

```
$passphrase = ConvertTo-SecureString <pPassphrase> -AsPlainText –Force
Set-OBMachineSetting -EncryptionPassphrase $passphrase
```

Speichern Sie dann die Online Backup-Sicherungsrichtlinie:

```
Set-OBPolicy -Policy $policy
```

Sie können eine erstellte Sicherung auch in der PowerShell starten. Dazu verwenden Sie das Cmdlet

```
Get-OBPolicy|Start-OBBackup
```

Onlinesicherung anpassen, überwachen und Fehler beheben

Sie können die Einstellungen der Sicherung natürlich jederzeit anpassen. Außerdem können Sie über *Eigenschaften ändern* die Bandbreite begrenzen, welche der Onlinesicherung zur Verfügung steht. Sie können hier Daten von 256 KBit/s bis 1 GBit/s eintragen und auch Zeitpunkte festlegen, wann diese Werte gültig sein sollen. Sie haben auch die Möglichkeit, diese Einstellungen in der PowerShell vorzunehmen. Beispiele dafür sind:

```
$mon = [System.DayOfWeek]::Monday
$tue = [System.DayOfWeek]::Tuesday
Set-OBMachineSetting -WorkDay "Mo", "Tu" -StartWorkHour "9:00:00" -EndWorkHour "18:00:00"
-WorkHourBandwidth (512*1024) -NonWorkHourBandwidth (2048*1024)
```

Sie sehen den Zeitplan der Onlinesicherung auch in der Aufgabenverwaltung von Windows Server 2012 R2 im Bereich *Microsoft/OnlineBackup*. Auch hier können Sie Änderungen vornehmen. Im unteren Bereich können Sie den Zeitraum einstellen, in dem die Sicherung gültig bleiben soll und erhalten bleibt.

In der Verwaltungskonsole der Onlinesicherung finden Sie auch die Registerkarte *Alerts* vor. Hier sehen Sie Meldungen des Diensts. Das können zum Beispiel Meldungen bezüglich des Speicherplatzes sein oder wenn eine neue Version des Agents zur Verfügung steht.

Um sich einen Überblick zum konfigurierten Sicherungsjob anzeigen zu lassen, verwenden Sie in der PowerShell den Befehl *Get-OBJob*.

Fehler hält der Agent neben der Ereignisanzeige auch in Protokolldateien fest. Diese finden Sie zum Beispiel im Ordner *C:\Program Files\Microsoft Online Backup Service Agent\Temp*. In der Ereignisanzeige finden Sie genauere Meldungen unter *Anwendungs- und Dienstprotokolle/CloudBackup*.

Die Sicherung wird durch den Systemdienst *Windows Azure Online Backup Agent* bereitgestellt. Diesen können Sie zur Fehlerbehebung neu starten lassen oder beenden. In der Eingabeaufforderung verwenden Sie dazu *NET START OBENGINE* oder *NET STOP OBENGINE*.

Funktioniert der Verbindungsaufbau des Servers ins Internet nicht, lassen sich auch keine Daten online sichern. Die Verbindung läuft über den Port 443 (SSL).

Daten aus Online Backup wiederherstellen

Daten stellen Sie mit Online Backup Service genauso wieder her wie bei einer lokalen Sicherung. Sie klicken mit der rechten Maustaste auf *Online Backup* und wählen die Wiederherstellung von Daten. Im Assistenten legen Sie zunächst fest, von welchem Datenträger und zu welchem Zeitpunkt Sie die Daten wiederherstellen wollen. Auch den Speicherort der wiederhergestellten Daten definieren Sie im Fenster. Generell gibt es hierbei keine Unterschiede zum Wiederherstellen von Daten in Windows Server 2012 R2.

Sie können beim Starten der Wiederherstellung auch einen Server auswählen, von dem Sie Daten wiederherstellen wollen. Der Assistent zeigt alle Server an, die Sie über die entsprechende Online Backup-ID registriert haben. Neben der grafischen Oberfläche können Sie auch hier die PowerShell verwenden.

Sie legen dazu die entsprechenden Daten wieder in Variablen fest und starten dann zum Schluss die Wiederherstellung:

```
$source = Get-OBRecoverableSource
$item = Get-OBRecoverableItem -Source $source[0]
$FinalItem = Get-OBRecoverableItem -ParentItem $item[0]
$recover_option = New-OBRecoveryOption
Start-OBRecovery -RecoverableItem $FinalItem -RecoveryOption $recover_option
```

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie mit der Windows Server-Sicherung in der grafischen Oberfläche, der Eingabeaufforderung und der PowerShell Daten sichern und wiederherstellen. Außerdem sind wir darauf eingegangen, wie Sie mit dem Befehlszeilentool Robocopy manuell oder automatisiert Daten sichern. Auch auf kostenlose Profitools zur Wiederherstellung verloren geglaubter Daten haben wir hingewiesen. Das Thema Cloud finden Sie in diesem Kapitel ebenfalls in Form des Windows Azure Online Backups.

Im nächsten Kapitel gehen wir auf die Sicherung und Wiederherstellung von Servern mit Windows Server 2012 R2 Essentials ein.

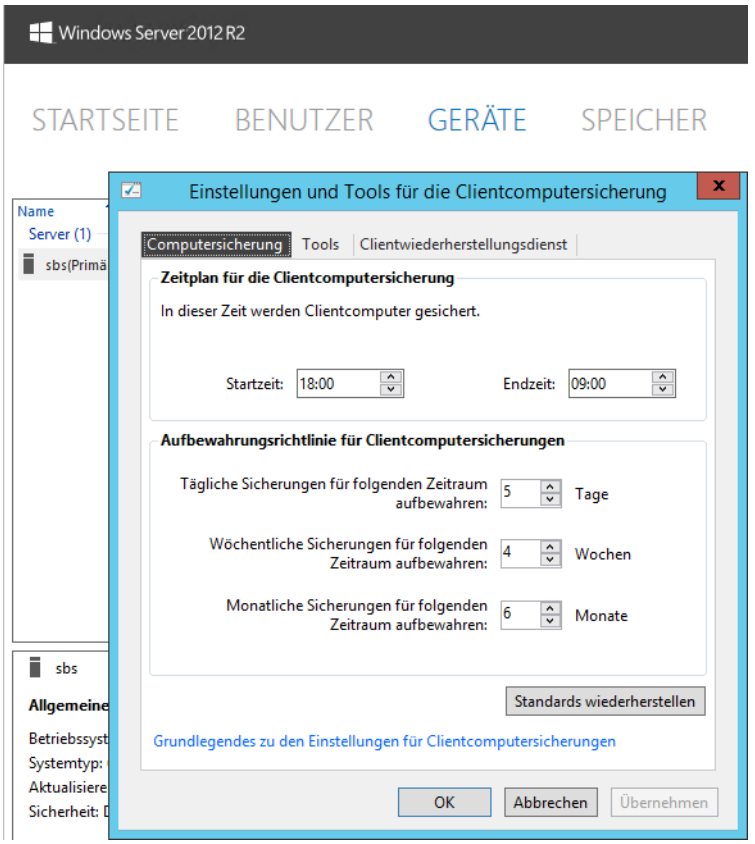
Kapitel 36

Datensicherung mit Windows Server 2012 R2 Essentials

In diesem Kapitel:

Für kleine Niederlassungen oder kleine Unternehmen ist Windows Server 2012 R2 Essentials eine Möglichkeit, schnell und einfach eine zentrale Datenablage zur Verfügung zu stellen. Mit Windows Server 2012 R2 Essentials bietet Microsoft den Nachfolger von Small Business Server 2011 Essentials an. In den Kapiteln 2 und 41 gehen wir ebenfalls auf Windows Server 2012 R2 Essentials ein. In diesem Kapitel widmen wir uns vor allem der Datensicherung der Clientcomputer auf den Server.

Abbildg. 36.1 Vorteil von Windows Server 2012 R2 Essentials ist die Sicherung der Clients auf den Server



Der Vorteil von Windows Server 2012 R2 Essentials ist die angepasste Oberfläche, über die auch ungeübte Administratoren schnell und einfach den Server verwalten. Selbst die Active Directory-Domäne und auch die Freigaben auf dem Server werden automatisch angelegt. Die herkömmlichen Verwaltungswerkzeuge wie der Server-Manager sind aber auch in Windows Server 2012 R2 Essentials verfügbar. In Kapitel 41 zeigen wir Ihnen, wie Sie auf installierten Servern mit Windows Server 2012 R2 Standard/Datacenter die Essentials-Umgebung als Serverrolle installieren. In diesem Fall können Sie die Vorteile der Edition, zum Beispiel die effiziente Datensicherung der Clients oder die Unterstützung des Dateiversionsverlaufes in Windows 8/8.1 auch auf Mitgliedsservern in Unternehmen nutzen.

Die Installation von Windows Server 2012 R2 Essentials gelingt auch ungeübten Administratoren (siehe Kapitel 2). Der Server benötigt keine Clientzugriffslizenzen und erlaubt die Anbindung von 25 Benutzern mit bis zu 50 Computern.

Die Installation erfolgt über einen angepassten Assistenten, der auch automatisch eine Active Directory-Domäne einrichtet (siehe Kapitel 2). Die Verwaltung nehmen Sie über eine speziell angepasste Verwaltungsoberfläche, dem Dashboard, vor. Clientcomputer binden sich über einen Agent an, der auch eine Sicherung der Computer direkt auf den Server ermöglicht. Auf diesem Weg können Benutzer selbst Daten wiederherstellen. Windows Server 2012 R2 erlaubt die Anbindung von Windows 7- und Windows 8/8.1-Computern. Lesen Sie sich dazu auch das Kapitel 41 durch.

Die Sicherung und Wiederherstellung spielt beim Einsatz von Windows Server 2012 R2 Essentials eine besondere Rolle und unterscheidet sich leicht von der Sicherung der anderen Editionen. Da alle wichtigen Daten des Unternehmens oder der Niederlassung/Abteilung auf einem einzelnen Server liegen, sollten Sie auf diesen Bereich ein besonderes Augenmerk legen.

Windows Server 2012 R2 Essentials enthält ein internes Sicherungsprogramm, mit dem Sie Daten der Clients sichern können. Auch eine komplette Sicherung der Clients und eine Wiederherstellung über den Server ist möglich. Der Sicherungs-Assistent der internen Sicherung von Windows Server 2012 R2 enthält noch mehr Möglichkeiten (siehe Kapitel 35), die Sie parallel oder als Ersatz zum Windows Server 2012 R2-Sicherungsprogramm verwenden können.

Windows Server 2012 R2 Essentials bietet auch die Möglichkeit, über den internen Sicherungs-Assistenten alle Daten auf den Clientcomputern zu sichern, inklusive des Betriebssystems. Mit dieser Sicherung können Sie über die Rettungs-CD von Windows Server 2012 R2 Essentials komplette Clientcomputer wiederherstellen, falls diese nicht mehr funktionieren. Außerdem kann der Dateiversionsverlauf von Windows 8/8.1 seine Daten direkt auf dem Server sichern. Das alles findet vollkommen transparent für die Anwender statt.

HINWEIS Bei der ersten Sicherung führt Windows Server 2012 R2 Essentials über die Windows Server-Sicherung für alle ausgewählten Daten eine Vollsicherung durch. Alle Sicherungen, die darauf aufbauen, sind inkrementell. Dadurch werden nur geänderte Daten gesichert, was den Sicherungszeitraum enorm verkürzt und auch die zu sichernde Menge erheblich reduziert.

Um Daten wiederherzustellen, müssen Sie aber keine Besonderheiten beachten. Der Wiederherstellungs-Assistent findet die gesicherten Daten automatisch, sodass Sie keine verschiedenen Sicherungssätze auswählen müssen.

Der Assistent zur Einrichtung im Dashboard baut auf die Windows Server-Sicherung in Windows Server 2012 R2 auf und erleichtert deutlich die Einrichtung. Lesen Sie sich daher zusätzlich zu diesem Kapitel auch das Kapitel 35 durch.

Windows Server 2012 R2 Essentials bietet im Vergleich zu anderen Editionen von Windows Server 2012 R2 die Möglichkeit, Daten von Arbeitsstationen und das Betriebssystem der Arbeitsstationen zu sichern sowie schnell und einfach wiederherzustellen. Vor allem kleine Unternehmen profitieren von diesen einfach zu bedienenden Funktionen.

Windows Server 2012 R2 Essentials bietet vor allem drei wichtige Funktionen, die für kleine Unternehmen extrem wichtig sind. Zunächst installiert der Installations-Assistent auch automatisch eine Active Directory-Gesamtstruktur, ohne dass Administratoren selbst kompliziert Hand anlegen müssen. Die Einrichtung erfolgt komplett im Hintergrund. Installieren Sie die Serverrolle für Windows Server 2012 R2 Essentials (siehe Kapitel 41), können Sie auch auf Mitgliedsservern die Funktionen

installieren. Als Benutzer auf dem Server werden dann die Anwender aus der Active Directory-Domäne angezeigt und verwaltet, in welcher der Server Mitglied ist. In diesem Fall stuft der Installations-Assistent den Server nicht zum Domänencontroller hoch.

Die zweite Funktion ist das Dashboard. Mit diesem verwalten Verantwortliche den Server auf sehr einfache Weise. Der Vorteil dabei ist, dass sich das Dashboard auch erweitern lässt und zur Verwaltung keiner großartigen Administratorkenntnisse notwendig sind.

Die dritte wichtige Funktion in Windows Server 2012 R2 Essentials ist der Agent, der auf den Arbeitsstationen installiert wird. Mit diesem können Anwender nicht nur schnell und einfach auf Freigaben des Servers zugreifen, sondern auch selbst ihre Daten sichern und wiederherstellen. Das sogenannte Launchpad auf den Computern erlaubt zusätzlich die Ausführung des Dashboards, sodass Serververantwortliche alle Einstellungen auch von ihrem Computer aus durchführen können.

Bereits während der Installation der Agent-Software lässt sich festlegen, ob der Windows-Computer aus dem Ruhezustand zur Sicherung auf den Server automatisch aufwachen soll. Die Einstellung lässt sich später auch in den Einstellungen anpassen

Datensicherung mit dem Dashboard einrichten

Um die Datensicherung mit dem Assistenten in Windows Server 2012 R2 Essentials durchzuführen, starten Sie das Dashboard und wechseln zu *Geräte*. Über das Kontextmenü des Servers konfigurieren Sie die Sicherung wie nachfolgend beschrieben. Nach der ersten Einrichtung der Sicherung können Sie diese jederzeit an Ihre Bedürfnisse anpassen.

Abbildg. 36.2 Verwalten der Computer in Windows Server 2012 R2 Essentials im Dashboard

Serversicherung einrichten

Die Sicherung und Wiederherstellung spielt beim Einsatz von Windows Server 2012 R2 Essentials eine besondere Rolle. Da alle wichtigen Daten des Unternehmens, oder zumindest einer Abteilung oder Niederlassung auf einem einzelnen Server liegen, sollten Sie auf diesen Bereich ein besonderes Augenmerk legen. Grundsätzlich ist es empfehlenswert, dass Sie ein vollwertiges Sicherungsprogramm für die Sicherung von Windows Server 2012 R2 verwenden und die Daten auf Band oder externen Datenträgern sichern (siehe auch Kapitel 35). Hier kann auch Windows Azure Online Backup interessant sein. Mehr zu diesem Thema lesen Sie in Kapitel 35.

Windows Server 2012 R2 enthält aber auch ein internes Sicherungsprogramm, mit dem Sie Daten sichern können (siehe Kapitel 35). Windows Server 2012 R2 Essentials verwendet die integrierte Sicherungsverwaltung von Windows Server 2012 R2. Wir gehen in Kapitel 35 ausführlich auf deren Verwendung ein. Nach der Einrichtung des Servers sollten Sie die Sicherung aktivieren.

Sobald Sie diesen Menübefehl anklicken, startet ein Assistent, der Sie mit wenigen Schritten durch die Einrichtung des Servers führt. Während der Einrichtung legen Sie fest, wo Sie die Daten sichern wollen, welche Daten der Assistent sichern soll und wann die Sicherung starten soll.

Auf der zweiten Seite des Assistenten sehen Sie alle Datenträger, auf denen Sie Daten sichern können. Zeigt das Fenster die Festplatte nicht an, auf der Sie die Daten sichern wollen, aktivieren Sie die Option *Alle Datenträger anzeigen, die als Sicherungsdatenträger verwendet werden können*. Die Festplatte, auf die Sie die Daten sichern, muss nicht partitioniert und formatiert sein.

Es bietet sich an, einen externen Datenträger für die Sicherung zu verwenden, am besten ein externes RAID-System oder eine Wechselfestplatte. Hier können Sie auch mehrere Festplatten verwenden und diese bei Bedarf wechseln, beispielsweise jeweils an geraden und ungeraden Wochen. Dazu verbinden Sie die Festplatten, die Sie zur Sicherung verwenden wollen, mit dem Server, und richten diese ein. Windows Server 2012 R2 verwendet dann zur Sicherung jene Festplatte, die zum Zeitpunkt der Sicherung mit dem Server verbunden ist. Sie können dazu einfach die Festplatten auswechseln; eine Konfiguration der Sicherung ist nicht notwendig.

Die Festplatten, die Sie als Sicherungsmedium verwenden, erhalten keinen Laufwerksbuchstaben, da das Sicherungsprogramm diese formatiert und nur für die Sicherung verfügbar macht. Die vollständigen und inkrementellen Sicherungen verwaltet der Server selbst. Sie müssen für die Einrichtung der Sicherungsmedien diese nur verbinden und über den Assistenten bestimmen, wann er die Sicherungen durchführen soll.

Die erste Sicherung ist eine Vollsicherung, alle weiteren sind inkrementell, laufen also sehr schnell ab. Auch wenn Sie mehrere Festplatten einsetzen und eine Festplatte defekt ist, lassen sich mit der zweiten Festplatte alle Daten wiederherstellen, da die Windows Server-Sicherung auch die Daten der Vollsicherung als Metadaten auf der zweiten Platte ablegt.

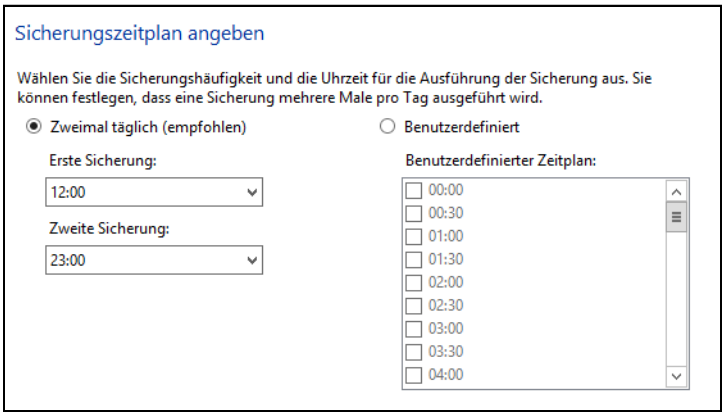
Der Assistent in Windows Server 2012 R2 Essentials ist im Vergleich zur Datensicherung in Windows Server 2012 R2 eingeschränkt und unterstützt keine genauere Konfiguration und keine Sicherung in Netzlaufwerken. Sie können im Assistenten eine beliebige externe Festplatte nutzen. Windows Server 2012 R2 unterstützt USB ab 2.0, IEEE 1394 (Firewire) oder eSATA. Zum Speichern von Datensicherungen können Sie auch mehrere externe Festplatten verwenden und diese nach Bedarf an das System anschließen oder entfernen. Sie können Daten auch auf einem internen Festplattenlaufwerk sichern, das dann aber nicht für andere Zwecke zur Verfügung steht.

ACHTUNG Der Assistent zum Konfigurieren von Serverdatensicherungen formatiert die Speicherlaufwerke bei der Konfiguration für die Datensicherung. Das heißt, alle vor der Sicherung vorhandenen Daten auf dem Laufwerk gehen verloren. Das Laufwerk ist außerdem nicht mehr im Explorer verfügbar, sondern nur noch über den Sicherungs-Assistenten.

Als Nächstes wählen Sie aus, wann der Assistent die Daten sichern soll. Sie haben die Möglichkeit, die Uhrzeiten für die Sicherung anzugeben.

Standardmäßig sichert Windows Server 2012 R2 die Daten zweimal am Tag um 12:00 Uhr und um 23:00 Uhr. Wollen Sie die Daten mehrmals sichern, wählen Sie die Option *Benutzerdefiniert* und klicken die Zeiten an, zu denen der Server sichern soll. Achten Sie aber darauf, genügend Zeit zwischen den Sicherungen zu lassen, damit die vorherige Sicherung auch tatsächlich abgeschlossen ist, bevor die neue beginnt.

Abbildg. 36.3 Auswählen des Sicherungszeitplans



Als Nächstes legen Sie fest, welche Daten der Assistent sichern soll. Wählen Sie hier alle notwendigen Daten, am besten aber alle, aus.

Auf der nächsten Seite erhalten Sie eine Zusammenfassung Ihrer Eingaben über die Sicherung angezeigt. Nach einem Klick auf *Einstellungen anwenden* formatiert der Assistent den Datenträger, den Sie für die Sicherung verwenden wollen.

Anschließend sehen Sie den Status der Datensicherung im Fenster sowie den Zeitpunkt der nächsten Sicherung. Wie Sie die Datensicherung verwalten und Daten aus dieser Sicherung wiederherstellen, lesen Sie in den folgenden Abschnitten genauer. Über das Kontextmenü des Servers im Dashboard lassen sich verschiedene Aufgaben durchführen:

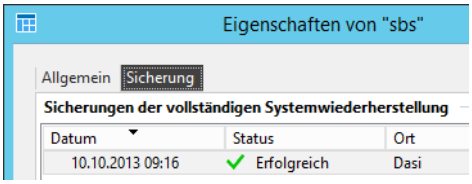
- **Sicherung für den Server starten** und **Sicherung für den Server beenden** Manuelles Starten und Beenden einer Sicherung mit den vorgegebenen Einstellungen
- **Dateien oder Ordner für den Server wiederherstellen** Aufrufen der Datensicherung und Wiederherstellen von gesicherten Daten in den Freigaben
- **Sicherung für den Server anpassen** Ändern der zu sichernden Ordner, der Sicherungszeiten und des Sicherungsmediums

Datensicherungen verwalten

Starten Sie über das Kontextmenü des Servers im Dashboard eine Sicherung, ändert sich der Status in der Spalte *Sicherungsstatus*. Hier erkennen Sie auch, ob die letzte Sicherung erfolgreich war oder nicht.

Klicken Sie doppelt auf den Server, sehen Sie auf der Registerkarte *Sicherung* ebenfalls die letzten Sicherungen und deren Status.

Abbildg. 36.4 Anzeigen des Status der letzten Sicherungen



Klicken Sie auf die Schaltfläche *Details anzeigen*, wird im Fenster der Start- und der Endzeitpunkt der Sicherung angezeigt. Im Fenster sehen Sie auch, welche Daten der Assistent erfolgreich gesichert hat und welche Datenträger nicht gesichert werden konnten.

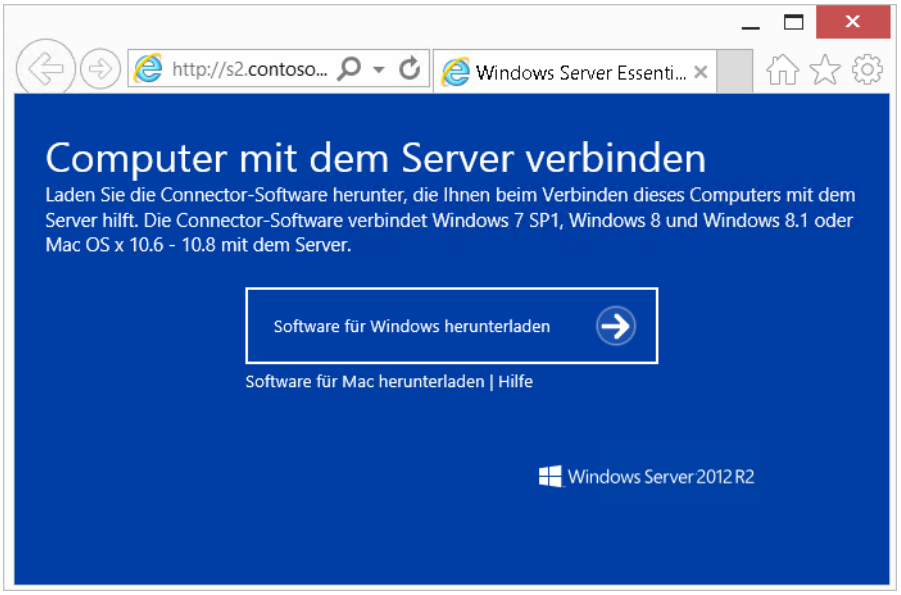
TIPP Weitere Informationen zur Sicherung erhalten Sie in der *Ereignisanzeige*, die Sie über die Programmgruppe *Verwaltung* starten. Die Datensicherung meldet ihren Status über *Anwendungs- und Dienstprotokolle/Microsoft/Windows/Backup*.

War die letzte Sicherung des Servers erfolgreich, steht in der Spalte *Sicherungsstatus* des Servers im Dashboard auch der Status *Erfolgreich*. Auch für die Clients erfasst das Dashboard den Sicherungsstatus.

Clientcomputer schnell und einfach anbinden und sichern

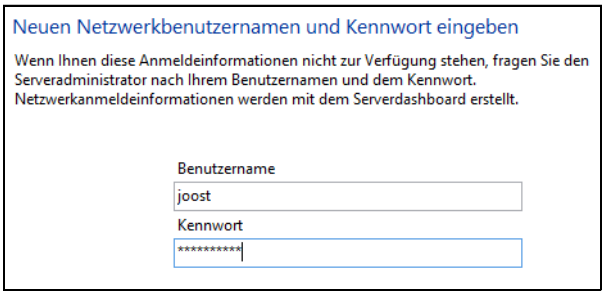
Nach der Installation des Servers (siehe Kapitel 2) verbinden sich Clients ganz einfach mit dem Server. Sie müssen dazu keine komplizierte Domänenaufnahme durchführen, sondern lediglich im Dashboard das Konto für den Benutzer anlegen. Die Anwender müssen in ihrem Browser nur die Adresse *http://<Servername>/connect* eingeben.

Abbildg. 36.5 Verbinden eines Clientcomputers mit Windows Server 2012 R2 Essentials



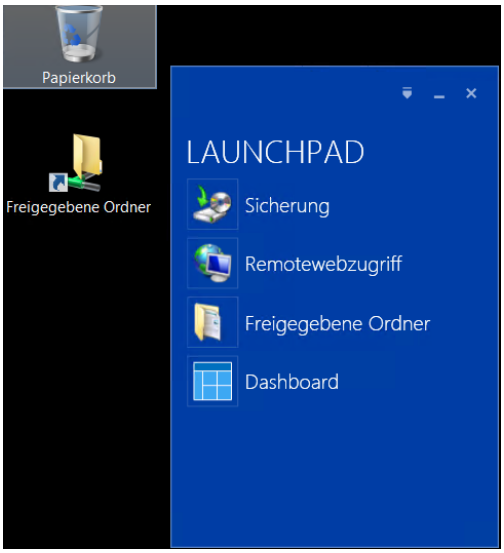
Anschließend bietet der Server den Download der Agent-Software an. Sobald Anwender den Link zur Installation angeklickt haben, startet ein Assistent, der bei der Anbindung des eigenen PCs hilft. Damit sich der Rechner anbinden lässt, muss sich der entsprechende Anwender mit der Webseite *http://<Servername>/connect* verbinden und während der Einrichtung über den Assistenten seinen Benutzernamen und Kennwort eingeben. Dieses legen Sie zuvor im Dashboard fest.

Abbildg. 36.6 Anmelden an Windows Server 2012 R2 Essentials zur Installation des Agents



Der Agent übernimmt bereits vorhandene Einstellungen und Dateien des Anwenders vom alten Profil in das neue Domänenprofil des Servers.

Abbildg. 36.7 Verwenden des Launchpads auf Clients, die an Windows Server 2012 R2 Essentials angebunden sind



Nach Abschluss der Installation befindet sich auf dem Desktop des Rechners das Launchpad. Über dieses können Anwender auf ihre Daten auf dem Server zugreifen und sogar ihren Rechner auf den Server sichern. Mit einer speziellen Wiederherstellungs-CD lassen sich komplette Rechner über den Server wiederherstellen. Benutzer können über das Launchpad Daten auf dem eigenen Rechner auf den Server sichern. Über den Agent ist auch eine Wiederherstellung möglich. Natürlich lassen sich auch einzelne Dateien über die Sicherung auf dem Server wiederherstellen, ebenfalls über das Dashboard. Diesen Vorgang müssen aber Administratoren durchführen, doch dazu später mehr.

Sobald Sie sich an der Domäne angemeldet haben, startet das Launchpad. Über dieses Launchpad greifen Anwender auf die Sicherung des Clients zu, können den Remotewebzugriff starten und direkt die Freigaben auf dem Server öffnen, für die sie berechtigt sind.

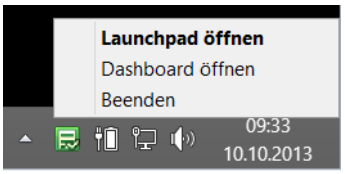
Administratoren dürfen zusätzlich noch das Dashboard aufrufen und können sich mit dem Administratorkonto direkt am Dashboard anmelden, ohne dass sich der Benutzer am PC abmelden muss. Außerdem lassen sich Meldungen für den Client im unteren rechten Bereich des Launchpads anzeigen. Hier erkennen Anwender Fehler, die auf dem Clientcomputer auftreten.

Arbeiten Sie mit Windows 8/8.1, also der kleinen Version von Windows 8/8.1 Pro/Enterprise, können Anwender zwar ebenfalls über den Connector mit den Freigaben auf dem Server arbeiten, es ist aber keine Domänenanmeldung am PC möglich wie mit Windows 8/8.1 Pro oder Enterprise. In diesem Fall müssen sich Anwender am Launchpad nach der Anmeldung am PC noch einmal explizit anmelden. Über *Optionen* lässt sich diese Anmeldung auch speichern. Nach der Anmeldung stehen die Freigaben und Funktionen im Launchpad in Windows 7 Home Edition genauso zur Verfügung wie in Windows 8/8.1 Pro oder Enterprise.

Der Connector, mit dem der Client an den Server angebunden ist, besitzt ein eigenes Symbol, welches im Infobereich der Taskleiste angezeigt wird. Über das Kontextmenü dieses Symbols starten Sie das Launchpad, zeigen Warnungen auf dem Computer an und können als Administrator das Dashboard öffnen. An der Farbe des Symbols erkennen Anwender auch, ob der Computer Fehler meldet (rotes Symbol), Warnungen findet (gelbes Symbol) oder ob alles in Ordnung ist (grünes Symbol).

Standardmäßig blendet Windows 7/8/8.1 das Symbol allerdings aus. Um es dauerhaft einzublenden, klicken Sie im Infobereich der Taskleiste auf den kleinen Pfeil und wählen *Anpassen*. Wählen Sie im neuen Fenster dann für das Symbol des Connectors die Option *Symbol und Benachrichtigungen anzeigen* aus. Sobald der Connector startet, zeigt dieser Fehler an, die auf dem Computer aufgetreten sind. Klicken Sie auf *Warnungen anzeigen*, sehen Sie detailliertere Informationen zu den Fehlern.

Abbildg. 36.8 Der Connector zeigt den Status des Computers an



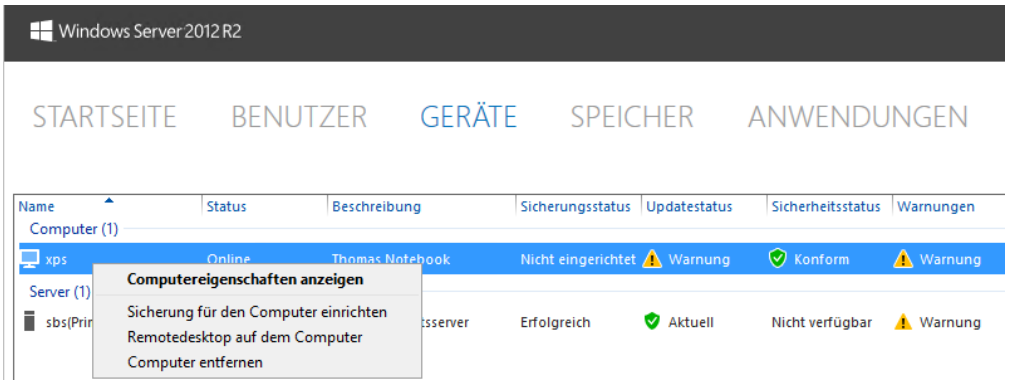
Haben Sie einen Clientcomputer mit dem Essentials-Netzwerk verbunden, sehen Sie diesen, wenn Sie im Dashboard auf *Computer und Sicherungen* klicken. Hier sind alle Computer des Netzwerks aufgelistet. Über das Kontextmenü oder die Auswahl von *Computer entfernen*, können Sie Computer von der Liste wieder löschen. In diesem Fall haben allerdings die Anwender, die sich anmelden, keine Rechte mehr, auf Freigaben zuzugreifen.

Sie sehen in diesem Bereich auch in der Spalte *Status*, ob der Computer eingeschaltet ist und ob Warnungen auf dem Computer gemeldet werden. Über das Kontextmenü oder den *Aufgaben*-Bereich sehen Sie die verschiedenen Möglichkeiten zur Verwaltung des Clients.

Clientcomputer über das Dashboard auf den Server sichern

Windows Server 2012 R2 Essentials bietet die Möglichkeit, alle Daten von Clientcomputern inklusive des Betriebssystems in die Sicherung des Servers einzubinden. So können Sie mit der Rettungs-CD eine vollständige Sicherung von Clients über das Netzwerk wiederherstellen. Sicherungen auf Clientcomputern starten und verwalten Sie vom Server aus im Dashboard über *Geräte*.

Abbildg. 36.9 Verwalten von Clientcomputern im Dashboard

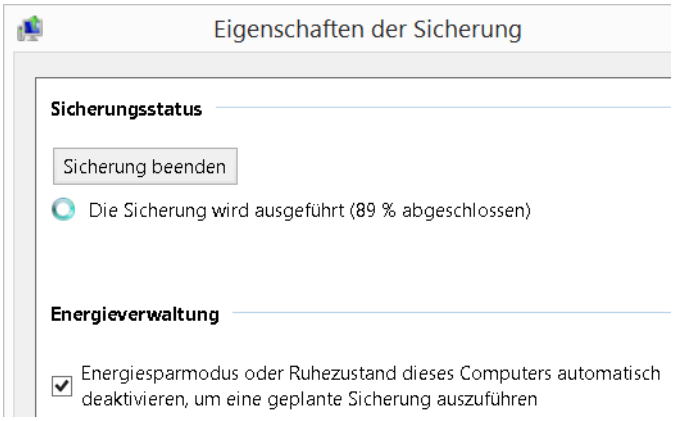


Starten Sie die Sicherung, sehen Sie über das Launchpad auf dem Client und der Auswahl von *Sicherung* den Status der Sicherung. Die Sicherung läuft im Hintergrund, sodass der Anwender weiter mit seinem Computer arbeiten kann. Ist die Sicherung abgeschlossen, wird dies an gleicher Stelle angezeigt. Über diesen Bereich starten Sie auch eine Sicherung vom Client aus auf den Server. In den Eigenschaften eines Computers sehen Sie auf der Registerkarte *Sicherung* die verschiedenen vorhandenen Sicherungen des Clients.

Die Datensicherung richten die Anwender selbst über das Launchpad ein. Nach der Anbindung an Windows Server 2012 R2 Essentials sollten Anwender daher zunächst eine erste Sicherung vornehmen. Hier ist auch der aktuelle Stand der Sicherung zu sehen.

Für eine optimale Datensicherung sollten Unternehmen auch die Daten des Servers sichern. Dazu steht im Dashboard ein eigener Einrichtungspunkt zur Verfügung, über den sich die Daten des Servers sichern lassen. Im Dashboard des Servers ist für alle angebundenen Computer, auch den Server selbst, der Status der aktuellen Datensicherung zu sehen. Sie können über diesen Bereich auch die Sicherung beenden oder eine Wiederherstellung starten.

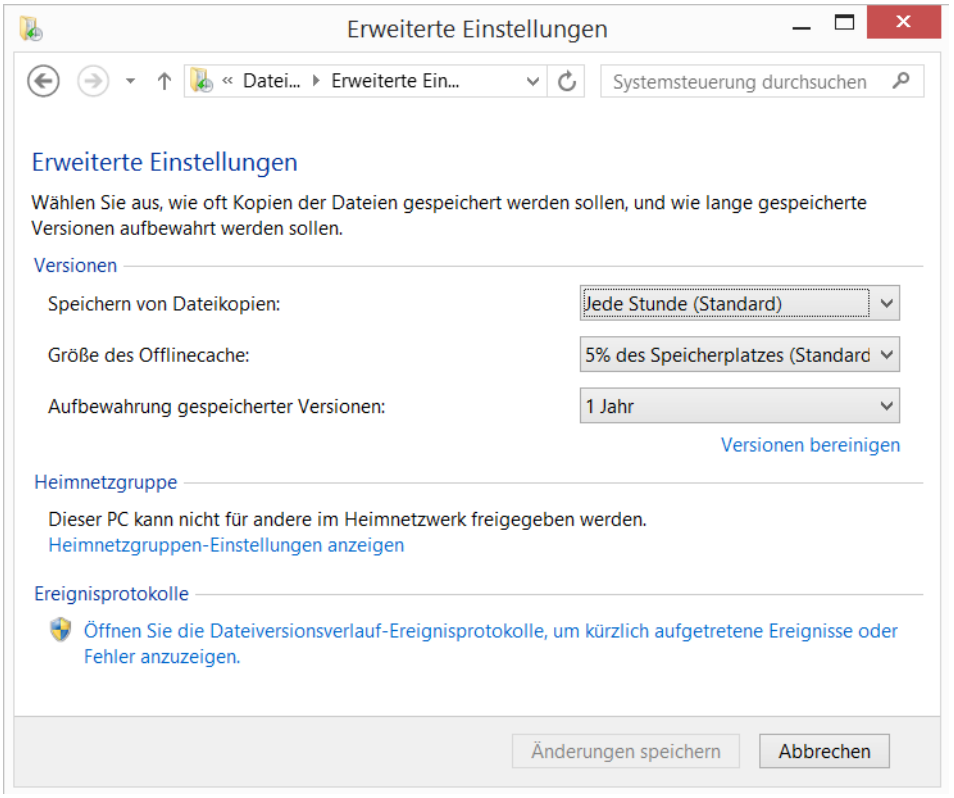
Abbildg. 36.10 Windows 8/8.1 kann seine Daten über das Launchpad auf den Server mit Windows Server 2012 R2 Essentials sichern



Neben der manuellen Sicherung von Rechnern, die Anwender über ihr Launchpad durchführen, können Sie über das Dashboard die Sicherungseinstellungen aller Clientcomputer steuern. Auf diesem Weg lassen sich zum Beispiel auch automatisierte Sicherungen erstellen.

Windows Server 2012 R2 Essentials unterstützt den Dateiversionsverlauf in Windows 8/8.1. Mit diesem können Anwender für jede Datei verschiedene Versionen schnell und einfach wiederherstellen. Die Einstellungen dazu erfolgen in den Eigenschaften des Computers im Dashboard.

Abbildg. 36.11 Die Einstellungen für den Dateiversionsverlauf sehen Sie auf dem Clientcomputer in der Systemsteuerung

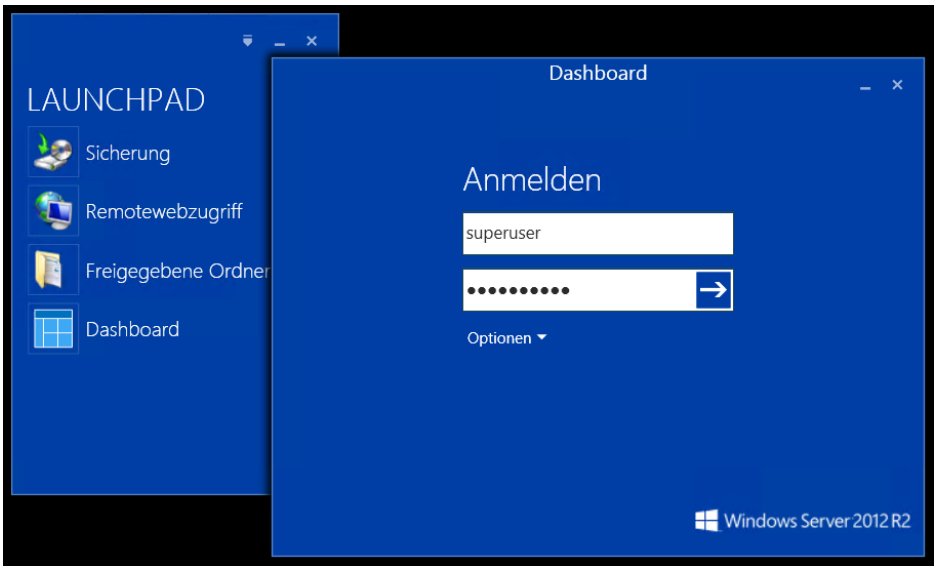


Um Dateien mit dem Dateiversionsverlauf wiederherzustellen, verwenden Anwender den Explorer in Windows 8/8.1. Eine Unterstützung durch Administratoren ist nicht notwendig. Die Sicherung erfolgt mehrmals am Tag. Die Sicherung aus dem Dateiversionsverlauf entspricht der Konfiguration in Windows 8/8.1 auch ohne Windows Server 2012 R2 Essentials. Der Unterschied besteht lediglich darin, dass der Client seine Daten nicht auf eine externe Festplatte oder ein NAS-System sichert, sondern auf den Server.

Über das Dashboard erstellen Sie einen Wiederherstellungs-USB-Stick, mit dem sich Clientcomputer booten lassen. Anwender können mit diesem Stick dann nicht nur Daten ihres PCs wiederherstellen, sondern den kompletten Computer. Im Assistenten lassen sich alle abgelegten Sicherungen auf dem Server abrufen und über das Netzwerk auf die Clients überspielen.

Sollen Dateien auf einem Computer wiederhergestellt werden, muss sich ein Anwender mit Administratorrechten über das Launchpad am Rechner das Dashboard starten. Über das Kontextmenü des Computers lassen sich dann Daten wiederherstellen. Im Rahmen der Wiederherstellung wählen Sie zunächst die Datensicherung aus, von der Anwender Daten wiederhergestellt bekommen wollen. Über einen Assistenten lässt sich dann einfach auswählen, welche Dateien wiederhergestellt werden sollen.

Abbildg. 36.12 Das Dashboard zur Serververwaltung können Administratoren auch direkt von Clients aus starten



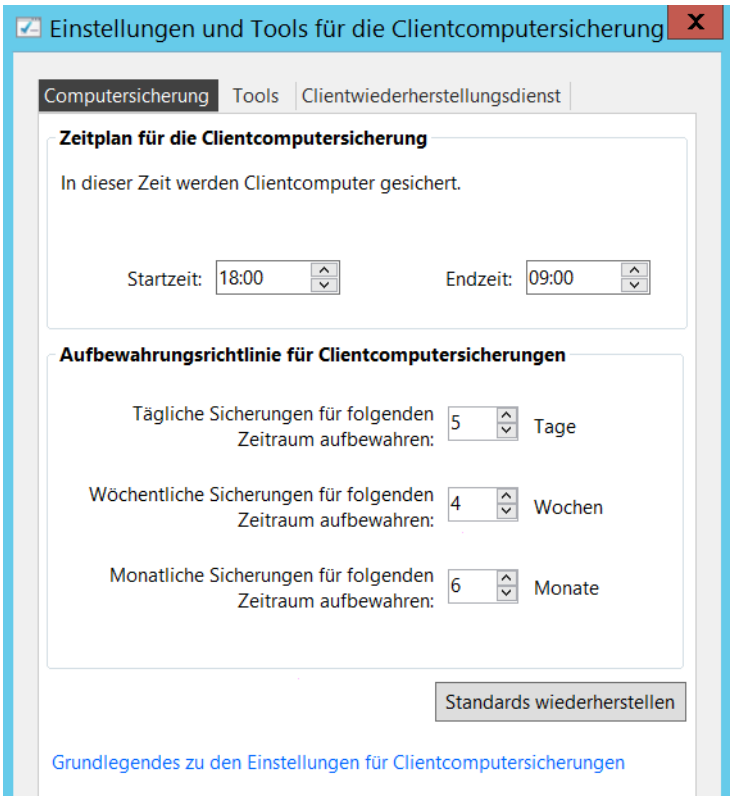
Sobald Sie eine vollständige Datensicherung des Servers durchgeführt haben, können Sie über die Windows Server 2012 R2-DVD ein vollständiges Image wiederherstellen. Dazu stellt Windows Server 2012 R2 Essentials die neue Wiederherstellungsumgebung zur Verfügung, die auch in Windows 8/8.1 integriert ist.

Clientcomputer sichern und Sicherungen verwalten

Windows Server 2012 R2 Essentials kann auch Daten auf Clientcomputern sichern. Die Sicherung erfolgt im Rahmen der normalen Datensicherung über den Connector. Damit die Sicherung funktioniert, muss der Client eingeschaltet und korrekt an den Server angebunden sein. Über Gruppenrichtlinien können Sie bei der Anbindung des Clients aber auch festlegen, dass dieser zur Zeit der Datensicherung automatisch starten und nach der Sicherung wieder herunterfahren soll.

Bevor Sie Clientcomputer sichern, sollten Sie über den Menübefehl *Clientcomputer-Sicherungsaufgaben* zunächst allgemeine Einstellungen festlegen, die der Server für die Sicherung der Clients berücksichtigen soll. Die Einstellungen gelten nur für die Sicherung der Clients, nicht für die Sicherung des Servers. Sie finden den Menübefehl im rechten Bereich des Dashboards auf der Registerkarte *Geräte*.

Abbildg. 36.13 Aufrufen der allgemeinen Einstellungen zur Sicherung von Clientcomputern



Nach der Auswahl des Menübefehls öffnet sich ein neues Fenster, über das Sie verschiedene Einstellungen vornehmen können. Auf der Registerkarte *Computersicherung* legen Sie zunächst fest, wann der Assistent die Clientcomputer sichern soll und wie lange die Sicherungen auf dem Server verfügbar sein sollen.

Mit dem Dateiversionsverlauf in Windows 8/8.1 können Anwender selbst Dateien wiederherstellen. Windows Server 2012 R2 Essentials sichert dazu notwendige Daten auf den Server. Die Anwender können über den Dateiversionsverlauf aber selbst Daten wiederherstellen. Der Dateiversionsverlauf ist nur für Windows 8/8.1 verfügbar. Wir gehen in den folgenden Abschnitten noch ausführlicher auf den Dateiversionsverlauf in Windows 8/8.1 ein.

Über die Registerkarte *Tools* können Sie defekte Sicherungen reparieren, wenn sich aus diesen keine Daten wiederherstellen lassen. Lässt sich eine Sicherung nicht reparieren und daher auch nicht zur Wiederherstellung nutzen, kann der Assistent diese Sicherung löschen.

Neu in Windows Server 2012 R2 Essentials ist die Registerkarte *Clientwiederherstellungsdienst*. Mit dieser Funktion können Sie ebenfalls Computer komplett wiederherstellen. Vorteil ist, dass Sie mit diesem Tool das Betriebssystem auf dem Client über das Netzwerk installieren können. Sie brauchen für die Funktion noch das Windows Assessement and Deployment Toolkit (WADK) von der Seite *http://go.microsoft.com/fwlink/p/?LinkId=311663* [Ms179-K36-xx].

Einrichten der Datensicherung über Dateiversionsverlauf

Microsoft hat die Datensicherung in Windows 8/8.1 komplett überarbeitet und verbessert. Die Datensicherung ist jetzt so einfach wie nie zuvor in Windows. Speichern Anwender wichtige Daten auf dem PC, sollten Administratoren auf dem Rechner den Dateiversionsverlauf einmalig einrichten und eine Sicherung der Daten auf eine externe Festplatte oder auf einer Freigabe im Netzwerk speichern. Die Vorgänge im Hintergrund sind dabei vollkommen transparent für den Anwender.

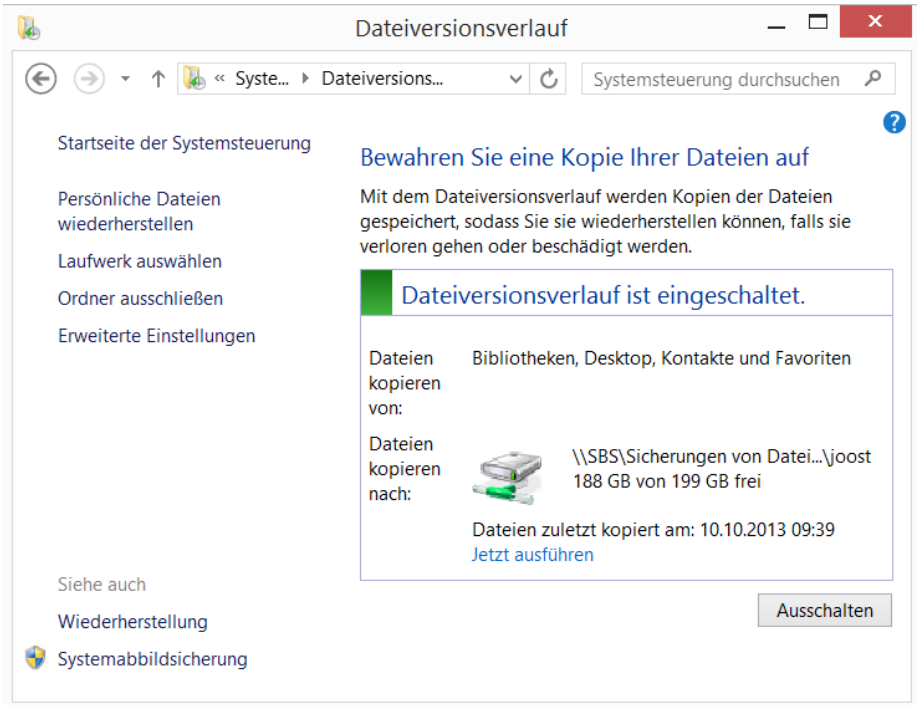
Sie können den Dateiversionsverlauf und die standardmäßige Windows-Sicherung nicht parallel einsetzen. Zuerst müssen Sie den Dateiversionsverlauf aktivieren. Ist die standardmäßige Sicherung aktiviert, müssen Sie diese zunächst deaktivieren.

Einrichten des Dateiversionsverlaufs

Um Daten schnell und einfach wiederherzustellen, lässt sich die Option in der Steuerung des Dateiversionsverlaufs auswählen. Gehen Sie zur Einrichtung folgendermaßen vor:

1. Öffnen Sie die Systemsteuerung und navigieren Sie zu *System und Sicherheit/Dateiversionsverlauf*. Klicken Sie auf *Einschalten*, um die Sicherung zu aktivieren. Setzen Sie Windows 8/8.1 zusammen mit Windows Server 2012 R2 Essentials ein, aktiviert der Agent für Windows Server 2012 R2 Essentials den Dateiversionsverlauf und speichert Dateien des Anwenders automatisch auf dem Server.
2. Sie können durch Anklicken von *Jetzt ausführen* sofort eine Sicherung der Daten durchführen.

Abbildg. 36.14 Anzeigen des Status der Dateiversionsverlaufs-Sicherung



3. Den aktuellen Status des Vorgangs sehen Sie im Fenster. Sie können eine Verknüpfung des Dateiversionsverlaufs erstellen, indem Sie das Symbol aus der Systemsteuerung auf den Desktop ziehen. Über das Kontextmenü dieses Symbols können Sie die Funktion auf der Startseite als Kachel anheften, um diese schneller zu erreichen.

Auf der externen Festplatte oder der Freigabe im Netzwerk beim Einsatz mit Windows Server 2012 R2 Essentials befindet sich ein neuer Ordner mit dem Namen des Rechners. In diesem legt Windows 8/8.1 gesicherte Dateien ab. Eine Wiederherstellung nehmen Sie aber nicht über diesen Ordner vor, sondern über den Dateiversionsverlauf und den Link *Persönliche Dateien wiederherstellen*.

Abbildg. 36.15 Daten mit dem Dateiversionsverlauf wiederherstellen

Über den Link *Erweiterte Einstellungen* in der Konfiguration des Dateiversionsverlaufs legen Sie die Einstellungen der Datensicherung fest. Über das Listenfeld *Aufbewahrung gespeicherter Versionen* definieren Sie, wie lange Windows verschiedene Versionen der Dateien aufbewahren soll. Ändern Sie eine Datei, legt Windows auch eine neue Version an.

Bei *Speichern von Dateikopien* legen Sie fest, wann Windows eine Sicherung durchführen soll. Mit *Größe des Offlinecache* steuern Sie den Zwischenspeicher für Offlinedateien auf dem lokalen Rechner.

Wollen Sie einige Dateien nicht durch den Dateiversionsverlauf sichern lassen, klicken Sie im Hauptfenster auf *Ordner ausschließen*. Standardmäßig sichert der Dateiversionsverlauf auch die Daten aller angebundenen Wechseldatenträger und externen Festplatten. Wollen Sie nur Daten der lokalen Festplatte sichern, tragen Sie bei den Ausnahmen die Laufwerksbuchstaben der externen Laufwerke ein.

Über *Laufwerk auswählen* im Hauptfenster ändern Sie das Laufwerk, in dem Windows die gesicherten Dateien aus dem Dateiversionsverlauf speichern soll.

Wiederherstellen von Dateien aus dem Dateiversionsverlauf

Um Daten mit dem Dateiversionsverlauf wiederherzustellen, öffnen Sie den Dateiversionsverlauf über die Systemsteuerung und klicken auf *Persönliche Dateien wiederherstellen*. Sie können in der Eingabeaufforderung oder der Startseite auch *filehistory* eingeben oder eine Verknüpfung zu diesem Programm erstellen, um direkt zur Wiederherstellung von Dateien zu starten.

Wählen Sie den Ordner aus, den Sie wiederherstellen wollen, oder klicken Sie doppelt auf den Ordner, um ihn zu öffnen. Setzen Sie ein Häkchen bei jenen Dateien, die Sie wiederherstellen wollen, und klicken Sie auf die Schaltfläche zur Wiederherstellung.

Über das Kontextmenü von Dateien oder Ordnern können Sie auch einen anderen Zielordner für die Wiederherstellung auswählen. Sie finden den Verlauf auch direkt im Explorer auf der Registerkarte *Start* im rechten Bereich des Menübands.

USB-Stick für die Wiederherstellung von Clientcomputern erstellen

Über die Schaltfläche *Schlüssel erstellen* über den Link *Clientcomputer-Sicherungsaufgaben* auf der Registerkarte *Geräte* im Dashboard können Sie auf der Registerkarte *Tools* einen USB-Stick so konfigurieren, dass Sie Clientcomputer über diesen USB-Stick wiederherstellen können, wenn Windows nicht mehr startet. Anschließend können Sie den entsprechenden Computer mit dem USB-Stick booten und auf diese Weise wiederherstellen.

Damit Sie den Stick erstellen können, müssen Sie diesen mit dem Server verbinden, nicht mit einem Clientcomputer. Der Stick muss eine Mindestgröße von 512 MB haben.

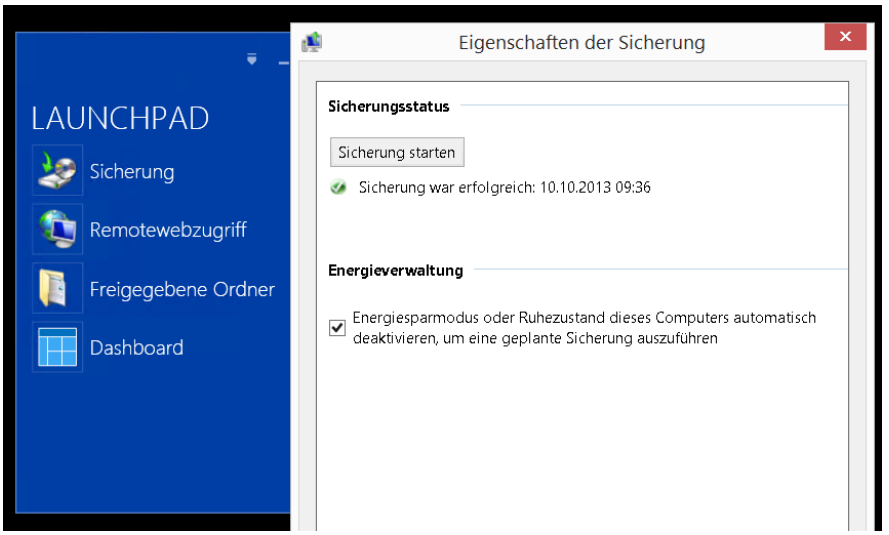
ACHTUNG Der Assistent löscht alle Daten auf dem USB-Stick und formatiert diesen neu, damit Sie Clientcomputer mit dem Stick booten können.

Clientsicherung konfigurieren und manuelle Sicherungen starten

Manuelle Sicherungen für Clientcomputer starten Sie im Dashboard auf dem Server über das Kontextmenü des Clients im Bereich *Geräte*. Wählen Sie den Menübefehl *Sicherung für den Computer starten* aus. Um die Datensicherung zu konfigurieren, wählen Sie im Kontextmenü den Befehl *Sicherung für den Computer anpassen* aus.

Den Status der letzten Datensicherung sehen Sie in der Spalte *Sicherungsstatus* des Clients. Klicken Sie doppelt auf einen Client, öffnen sich dessen Eigenschaften. Auf der Registerkarte *Sicherung* sehen Sie die jeweiligen Zeitpunkte der Sicherung.

Abbildg. 36.16 Datensicherung der Clients verwalten



Klicken Sie auf *Details anzeigen*, erhalten Sie ausführlichere Informationen zur Sicherung. Diese Hinweise sind insbesondere bei eventuell aufgetretenen Fehlern hilfreich. Auf den Clients erhalten Sie ebenfalls Daten zu den Datensicherungen. Dazu klicken Sie im Launchpad auf den Link *Sicherung*. Sie sehen im Fenster den Status der letzten Sicherung auf dem Server und können ebenfalls eine manuelle Sicherung starten.

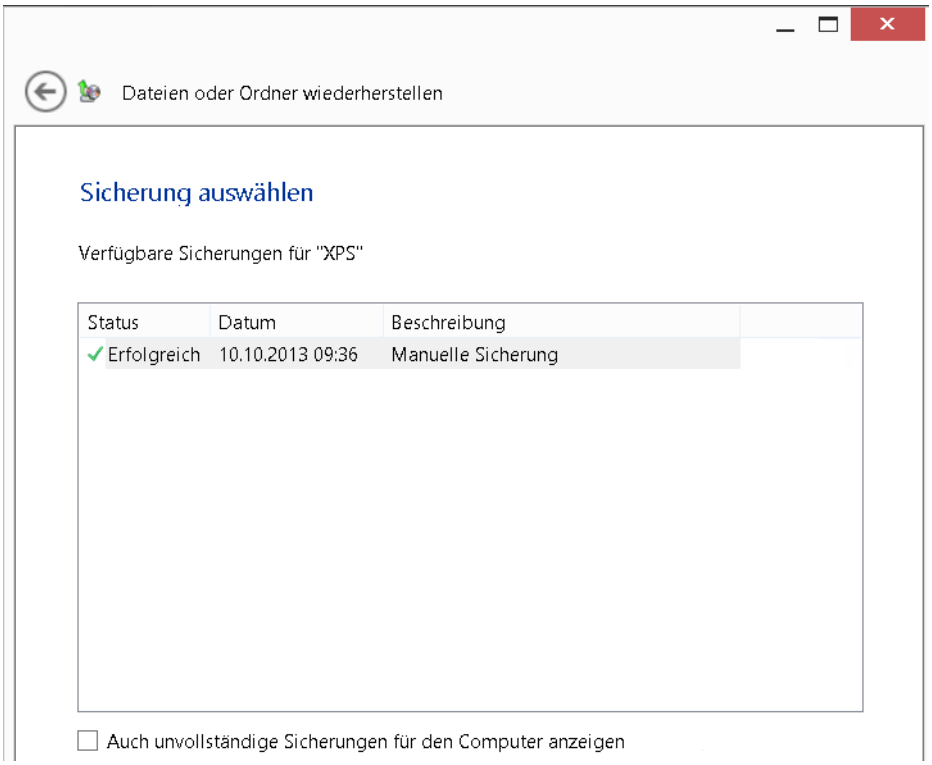
Daten auf dem Server und den Clients wiederherstellen

Haben Sie die Sicherung erfolgreich konfiguriert, können Sie über das Dashboard schnell und einfach Dateien und Ordner wiederherstellen. Wollen Sie Daten auf Clientcomputern wiederherstellen, müssen Sie das Dashboard auf dem entsprechenden Clientcomputer starten.

Daten auf dem Server wiederherstellen

Sie können Daten aus der Sicherung auch über den Assistenten wiederherstellen. Dazu müssen Sie den externen Datenträger mit dem Server verbinden, auf dem die Sicherung gespeichert ist, aus der Sie Daten wiederherstellen wollen. Wählen Sie dann im Dashboard auf der Registerkarte *Geräte* über das Kontextmenü des Computers oder des Servers die Option *Dateien oder Ordner für den Server wiederherstellen* aus. Um Daten auf Clients wiederherzustellen, müssen Sie auf dem Client das Dashboard starten und sich mit einem Administratorkonto anmelden.

Abbildg. 36.17 Wiederherstellung von Serverdateien im Dashboard starten



Zunächst wählen Sie aus, ob die Daten am ursprünglichen Ort wiederhergestellt werden sollen oder ob Sie die Daten an einem anderen Speicherort benötigen. Im nächsten Fenster legen Sie fest, ob Sie als Quelle der Wiederherstellung die aktuellste Sicherung oder eine ältere im System verfügbare Datensicherung verwenden wollen. Möchten Sie den Zeitpunkt selbst bestimmen, können Sie auswählen, welche Sicherung Sie verwenden wollen. Im Kalender sehen Sie fett markiert, wann Sicherungen verfügbar sind.

Im nächsten Schritt definieren Sie, ob Sie ein komplettes Laufwerk oder nur einzelne Dateien und Ordner wiederherstellen möchten. Abhängig von der Auswahl wählen Sie im nächsten Fenster genauer die Dateien oder Ordner aus, die Sie wiederherstellen wollen. Im nächsten Fenster geben Sie an, ob die Dateien im ursprünglichen oder in einem anderen Ordner wiederhergestellt werden sollen.

Sind bereits Dateien im Ordner vorhanden, wählen Sie in diesem Fenster auch aus, ob der Assistent alte Versionen von Dateien überschreiben soll.

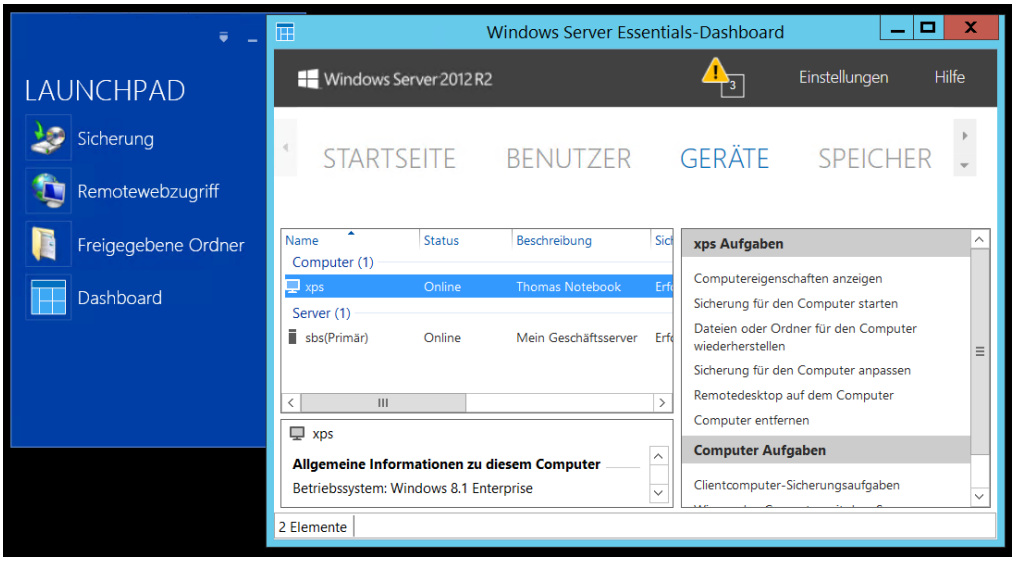
Im nächsten Fenster starten Sie die Wiederherstellung mit der Schaltfläche *Jetzt wiederherstellen*. Nach kurzer Zeit (abhängig von der Datenmenge) sind die Dateien wieder verfügbar und lassen sich erneut verwenden.

Daten auf Clientcomputern wiederherstellen

Die Datensicherung in Windows Server 2012 Essentials führt auch eine Sicherung von Daten auf den Clientcomputern aus. Um diese auf den Clients wiederherzustellen, müssen Sie sich direkt mit dem entsprechenden Computer verbinden.

Starten Sie auf dem Computer über das Launchpad das Dashboard und melden Sie sich als Administrator am Dashboard an.

Abbildg. 36.18 Starten des Dashboards über das Launchpad auf Clientcomputern



Nach dem Start des Dashboards klicken Sie auf *Geräte* und dann mit der rechten Maustaste auf den Computer, für den Sie Dateien wiederherstellen wollen. Anschließend stellt der Sicherungs-Assistent eine Verbindung mit dem Server her und Sie können die Datensicherung für den Client auswählen, aus dem Sie Dateien wiederherstellen wollen. Nach der Auswahl des Sicherungszeitraums öffnet der Assistent die entsprechende Sicherung und Sie können wählen, welche Dateien Sie wiederherstellen wollen.

Haben Sie den Ordner oder die Dateien ausgewählt, legen Sie als Nächstes fest, an welchem Ort Sie die Dateien wiederherstellen wollen. Der Assistent zeigt dabei die lokalen Laufwerke direkt auf dem Client an, nicht die Laufwerke auf dem Server. Die Wiederherstellung erfolgt also direkt auf dem Client.

Als Nächstes stellt der Assistent die Dateien wieder her. Ist der Vorgang abgeschlossen, können Sie direkt den Speicherort öffnen, weitere Dateien wiederherstellen oder den Vorgang abschließen. Wollen Sie keine Dateien mehr wiederherstellen, schließen Sie das Dashboard auf dem Clientcomputer.

Clientcomputer komplett wiederherstellen

Funktioniert ein Clientcomputer nicht mehr, können Sie diesen mit einem USB-Stick booten und aus einer Datensicherung auf dem Server wiederherstellen. Den USB-Stick dazu erstellen Sie auf dem Server. Sie können aber anstatt über den USB-Stick auch mit der Recovery-CD booten, die zum Lieferumfang von Windows Server 2012 R2 Essentials gehört. Die Vorgänge dabei sind die gleichen, nur das Booten unterscheidet sich.

Nachdem Sie den Stick erstellt haben, booten Sie den Clientcomputer mit dem USB-Stick und wählen aus, ob Sie ein 32-Bit-System oder ein 64-Bit-System wiederherstellen wollen. Anschließend startet die Wiederherstellungsumgebung über den USB-Stick.

Kann der Assistent keine Verbindung mit dem Server herstellen oder sind die lokalen Festplatten nicht verfügbar, können Sie die Treiber für die Geräte über die Schaltfläche *Treiber laden* integrieren. Dazu verbinden Sie den USB-Stick mit einem anderen Computer und kopieren die entsprechenden Treiber auf den Stick. Achten Sie aber darauf, dass Sie die Treiberdateien entpacken müssen, damit die *.inf*-Dateien der Treiber zur Verfügung stehen. Nach der erfolgreichen Anmeldung wählen Sie aus, welchen Client Sie wiederherstellen wollen.

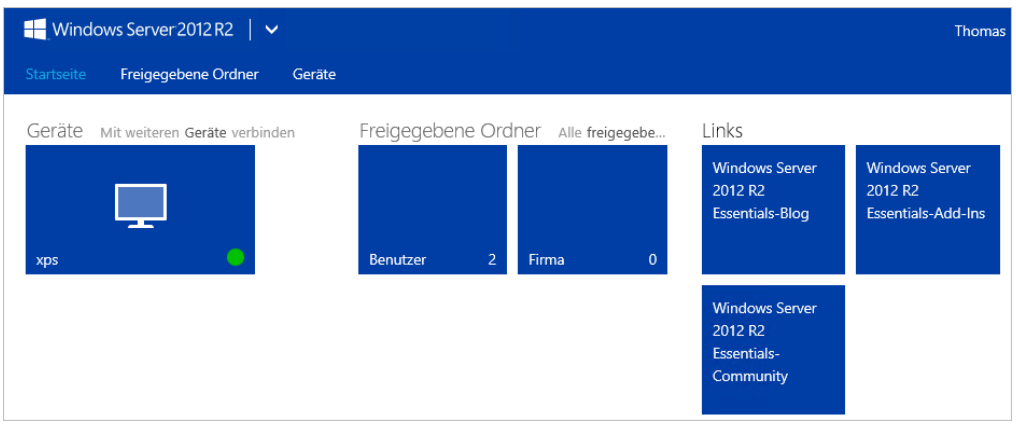
Als Nächstes bestimmen Sie, welche Sicherung der Assistent für die Wiederherstellung verwenden soll. Über *Details* können Sie sich ausführlichere Informationen zur Sicherung anzeigen lassen. Im nächsten Fenster können Sie entweder den kompletten Computer mit allen Partitionen wiederherstellen lassen oder einzelne Partitionen (Volumes) für die Wiederherstellung auswählen.

Der Remotewebzugriff

Eine weitere Besonderheit von Windows Server 2012 R2 Essentials ist der Remotewebzugriff. Diese Funktion bietet die Möglichkeit, über einen Webbrowser auf Freigaben zuzugreifen und sich per Fernwartung auf den eigenen PC oder für Administratoren auch den Server zu verbinden.

Sie können den Remotewebzugriff im Internet Explorer mit dem Link *https://<Servername>/remote* aufrufen. Nachdem die Startseite des Remotewebzugriffs aufgebaut ist, authentifizieren Sie sich in der Anmeldemaske. Es ist nicht notwendig, die Domäne einzugeben, es genügen der Benutzername und das Kennwort.

Abbildg. 36.19 Verwenden des Remotewebzugriffs in Windows Server 2012 R2 Essentials



Nach dem Verbindungsaufbau können Anwender auf ihre Dateien zugreifen und per Remotedesktop auch auf ihren Rechner, wenn dieser eingeschaltet ist. Wenn Sie sich nach der Verbindung auf den Remotewebzugriff mit dem eigenen PC verbinden wollen, klicken Sie auf der Hauptseite des Remotewebzugriffs auf den Link *Verbinden*. Administratoren können auf diesem Fenster auch eine Verbindung zum Server selbst sowie zu allen PCs im Netzwerk herstellen.

Achten Sie aber darauf, dass der Verbindungsaufbau per Remotedesktop nur dann funktioniert, wenn Sie sich mit dem Namen verbinden, den Sie auch für den Internetzugriff des Servers bei der Einrichtung festgelegt haben. Es darf keine Zertifikatwarnung beim Verbindungsaufbau auftauchen. Damit der Aufbau funktioniert, müssen Anwender das Zertifikat der Stammzertifizierungsstelle auf dem Server auf ihrem Computer installieren.

Remotewebzugriff konfigurieren

Klicken Sie im Dashboard auf *Startseite* und dann auf *Zugriff überall einrichten*. Über den Menübefehl *Klicken Sie hier, um Zugriff überall zu konfigurieren* müssen Sie diesen zunächst konfigurieren.

Beim Starten der Einrichtung können Sie auch gleich Ihren DSL-Router oder Ihre Firewall einrichten lassen. Allerdings unterstützen dies die meisten Geräte nicht, sodass Sie Portweiterleitungen des Ports TCP 443 von der Firewall zum Server manuell eintragen müssen. Bei der Einrichtung des Remotewebzugriffs müssen Sie auch einen Domänennamen eingeben. Im nächsten Schritt überprüft der Server den Namen. Wählen Sie für die Einrichtung des Domänennamens die Option *Domänenname manuell einrichten* aus.

Geben Sie im nächsten Fenster an, dass Sie den Domänennamen eingerichtet haben. Dazu müssen Sie ein DynDNS-Konto oder einen selbstregistrierten Namen besitzen. Dieser muss auf die externe IP-Adresse Ihrer Firewall zeigen und auf der Firewall haben Sie eine Weiterleitung des Ports 443 zur internen IP-Adresse des Servers hinterlegt.

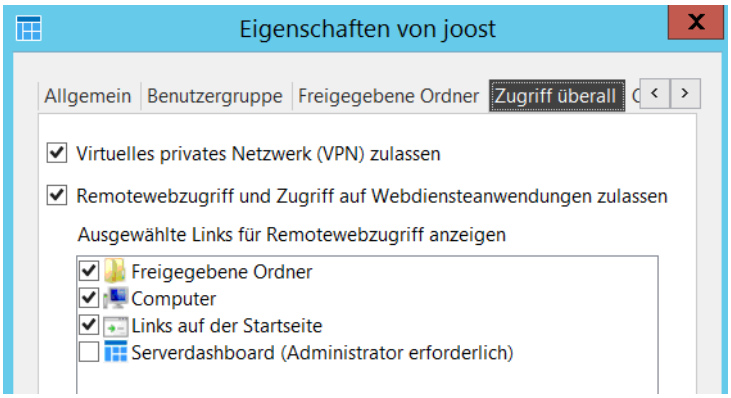
Anschließend können Sie ein Zertifikat hinterlegen, da der Zugriff über eine SSL-verschlüsselte Website erfolgt. Wie Sie dabei vorgehen, lesen Sie in Kapitel 30. Das Zertifikat hinterlegen Sie über eine CER-Datei auf dem Server.

Wollen Sie über Remotezugriff auch die Verbindung auf Computer ermöglichen, müssen Sie über den Assistenten ein öffentliches Zertifikat hinterlegen. Wollen Sie den Zugriff auf Computer über den Remotewebzugriff nur über Homeoffice-PCs zulassen, haben Sie auch die Möglichkeit, Windows Server 2012 R2 Essentials so zu konfigurieren, dass Sie mit einem internen Zertifikat auskommen, ohne das Zertifikat eines Drittanbieters zu kaufen.

Benutzereinstellungen für Remotewebzugriff

Aktivieren Sie den Remotewebzugriff, können Sie im Dashboard steuern, welche Anwender über das Internet auf den Server zugreifen dürfen. Klicken Sie dazu auf *Benutzer* und dann doppelt auf den Benutzer, für den Sie den Remotewebzugriff konfigurieren wollen.

Abbildg. 36.20 Konfigurieren des Remotezugriffs



Über die Registerkarte *Zugriff überall* stellen Sie ein, auf welche Funktionen im Remotewebzugriff der Anwender zugreifen darf.

Setzen Sie das Häkchen bei den Funktionen, die der Anwender nutzen darf. Wollen Sie den Remotewebzugriff für den Anwender deaktivieren, deaktivieren Sie das Kontrollkästchen *Remotewebzugriff und Zugriff auf Webdiensteanwendungen zulassen*.

Aktivieren Sie die Option *Computer*, darf der Anwender über den Remotewebzugriff per Remotedesktop auf die Computer zugreifen, die Sie auf der Registerkarte *Computerzugriff* aktivieren. Diese Funktion steht aber nur in Windows 7 Professional/Ultimate, Windows Vista Business/Ultimate und in Windows 8/8.1 Pro und Enterprise zur Verfügung. Der Computer muss zusätzlich an Windows Server 2012 R2 Essentials angebunden sein.

Servereinstellungen für Remotewebzugriff

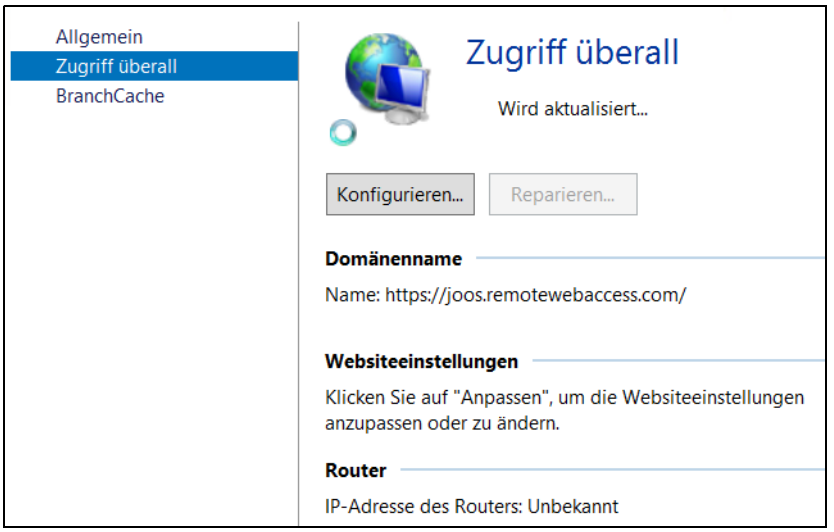
Damit der Remotewebzugriff generell funktioniert, müssen Sie ihn im Dashboard über den Menüpunkt *Einstellungen* zunächst aktivieren. Über diesen Bereich können Sie den kompletten Remotewebzugriff auch wieder deaktivieren.

Funktioniert der Zugriff nicht, obwohl Sie alle in diesem Kapitel beschriebenen Einstellungen vorgenommen haben, können Sie über die Schaltfläche *Reparieren* die Verbindung testen und anpassen. Auch wenn der Remotewebzugriff funktioniert, erscheint im Fenster oft eine Fehlermeldung, dass der Router nicht funktioniert. Testen Sie in diesem Fall zunächst, ob der Remotewebzugriff tatsächlich nicht funktioniert.

Nach der Aktivierung können Sie über die Schaltfläche *Anpassen* im Bereich *Websiteeinstellungen* verschiedene Einstellungen vornehmen, die für alle Benutzer gelten. In den Einstellungen können Sie über verschiedene Registerkarten die Einstellungen ändern.

Auf der Registerkarte *Anmeldeseite* legen Sie den Titel der Seite fest und können das Hintergrundbild und das Logo schnell und einfach ändern.

Abbildg. 36.21 Konfigurieren und Reparieren des Remotewebzugriffs



HINWEIS Das Logo darf maximal eine Größe von 32x32 Pixel haben, kleinere Logos passt die Oberfläche an. Das Hintergrundbild sieht mit einer Auflösung von 800x500 Pixel am besten aus.

Sie können Bilder im Format *.bmp, .dib, .rle, .gif, .png, .jpg* verwenden.

Auf der Registerkarte *Links auf der Startseite* legen Sie fest, welche Favoriten im Remotewebzugriff zur Verfügung stehen. Sie können die Reihenfolge der Links anpassen, die Bezeichnung ändern und beliebige Links hinzufügen oder entfernen.

Wollen Sie keine Links auf der Seite anzeigen, deaktivieren Sie einfach die Funktion in den Remotewebzugriffseinstellungen der einzelnen Benutzer.

Administratoren können im Remotewebzugriff auch direkt das Dashboard öffnen. Wollen Sie aber stattdessen lieber eine Remotedesktopverbindung öffnen, können Sie das auf der Registerkarte *Optionen zum Herstellen der Verbindung mit dem Server* aktivieren.

Fehler beim Zugriff auf den Remotewebzugriff beheben

Kann sich der Client nicht mit dem Server verbinden, liegt in den meisten Fällen ein Problem mit dem Zertifikat vor.

Stellen Sie auf jeden Fall sicher, dass der externe Name, den Anwender verwenden, auch vom Client aufgelöst werden kann und zur externen IP-Adresse Ihrer Firewall oder des DSL-Routers zeigt. Diese leitet die Anfrage von Port 443 dann bei korrekter Konfiguration an den Server weiter. Liegt ein Problem mit dem Zertifikat vor, erhalten Anwender eine Warnung im Browser. Diese lässt sich aber einfach wegklicken.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Clientcomputer an Windows Server 2012 R2 Essentials anbinden und Daten sichern oder wiederherstellen. Im Gegensatz zu anderen Editionen werden Sie bei dieser Edition von verschiedenen Assistenten und dem Dashboard unterstützt.

Im nächsten Kapitel erläutern wir Ihnen, wie Sie Patches im Netzwerk mit Windows Server Update Services verteilen.

Kapitel 37

Windows Server Update Services

In diesem Kapitel:

Wie Windows Server 2008 R2 und Windows Server 2012 verfügt auch Windows Server 2012 R2 über den Serverdienst Windows Server Update Services (WSUS). Dieser Dienst kann für Microsoft-Betriebssysteme, aber auch für alle anderen Microsoft-Produkte Updates herunterladen und im Netzwerk zur Verfügung stellen. Die Clients und Server im Netzwerk rufen Updates dann über diesen Server ab, nicht mehr über das Internet. Die Einstellungen lassen sich mit Gruppenrichtlinien steuern. Der Vorteil dabei ist die zentrale Steuerung der Updates. Außerdem müssen Unternehmen Updates nur noch einmal herunterladen, nicht für jeden Server einzeln.

Unternehmen, die mehrere Microsoft-Produkte und Clientsysteme im Netzwerk einsetzen, kommen um eine zentrale Verwaltung der Patches kaum herum. Windows Server 2012 R2 bietet dazu, wie bereits dessen Vorgänger, die Windows Server Update Services. Diese installieren Sie über den Server-Manager. Die grundlegende Funktion hat sich von Windows Server 2008 R2 zu Windows Server 2012 R2 nicht geändert. Allerdings lässt sich WSUS in Windows Server 2012 R2 jetzt auch über die PowerShell verwalten. Außerdem kann der Client besser zwischen Servern und Arbeitsstationen unterscheiden.

Microsoft empfiehlt für den Einsatz mindestens 10 GB freien Festplattenplatz, besser deutlich mehr. Unternehmen, die WSUS bereits einsetzen, können die Daten, Einstellungen und bereits gespeicherten Patches auch direkt zu Windows Server 2012 R2 migrieren. Microsoft stellt in der TechNet Anleitungen (*http://technet.microsoft.com/en-us/library/hh852352* [Ms179-K37-01]) zur Migration zur Verfügung.

Ein wichtiges Tool für die Diagnose von Clientproblemen ist das WSUS Client Diagnostics Tool von Microsoft (*http://technet.microsoft.com/en-us/wsus/bb466192.aspx* [Ms179-K37-02]). Es ermittelt, ob die Anbindung an den Server funktioniert.

Wie in Windows Server 2012 können Administratoren WSUS auch in Windows Server 2012 R2 über die PowerShell verwalten. Die Installation ist am schnellsten im Server-Manager erledigt. In diesem Fall lässt sich WSUS problemlos einrichten. Sie können in Windows Server 2012 R2 auch Windows 8.1-Clients an WSUS anbinden.

WSUS installieren

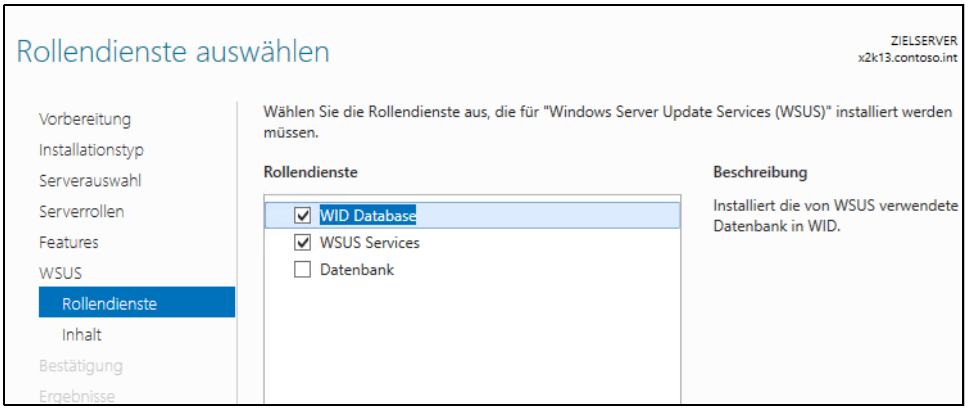
Im Server-Manager klicken Sie auf *Verwalten/Rollen und Features hinzufügen*. Als Serverrolle wählen Sie *Windows Server Updates Services* aus. Während der Installation nehmen Sie noch keine Einstellungen vor, sondern erst nachträglich. Während der Installation wählen Sie auch aus, ob auf dem Server eine interne Windows-Datenbank für WSUS installiert werden sollen (WID) oder nur der Dienst zum Verteilen von Patches. Bei der Auswahl von *Datenbank* lässt sich eine SQL Server-Datenbank hinterlegen, in der WSUS seine Daten speichern soll.

TIPP In manchen Umgebungen erscheinen Fehlermeldungen, wenn WSUS auf virtuellen Servern betrieben wird. Das liegt daran, dass die Patches auf einer virtuellen Festplatte abgespeichert werden sollen. In diesem Fall sollten Sie eine lokale Festplatte des Hyper-V-Hosts für die Patches zuteilen (siehe Kapitel 7).

Als Nächstes wählen Sie aus, wo WSUS Patches speichern soll. Diese liegen nicht in der Datenbank, sondern in einem Dateipfad. In der Datenbank liegen nur die Konfigurationsdaten von WSUS und die Berichte, die Administratoren erstellen können.

Nach Abschluss der Installation warnt der Server-Manager, dass noch eine nachträgliche Konfiguration der Dienste erfolgen muss. Diese sollten Sie nach der Installation von WSUS starten. Bei diesem Vorgang richtet der Assistent vor allem die Datenbank von WSUS ein. Danach erst starten Sie den eigentlichen Assistenten zur Einrichtung der Patches und Clients.

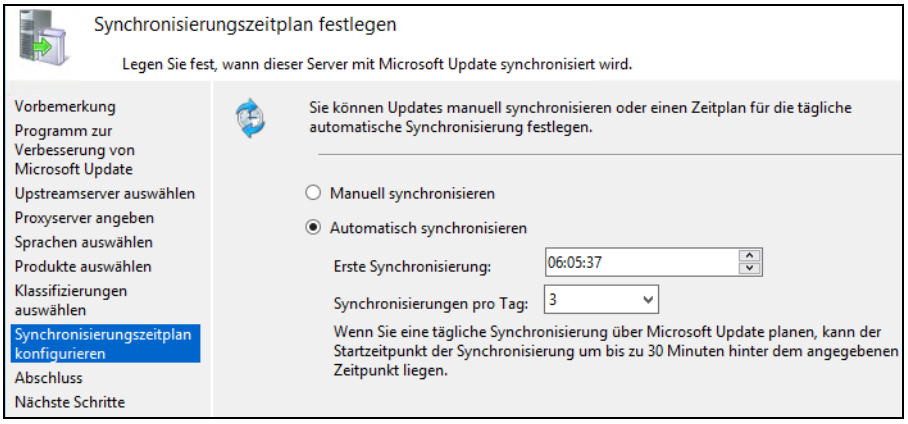
Abbildg. 37.1 Auswählen der Rollendienste



Wie für andere Serverdienste legt der Server-Manager in Windows Server 2012 R2 auch für WSUS eine eigene Gruppe an. Über das Kontextmenü des Servers im Server-Manager starten Sie den Einrichtungs-Assistenten von WSUS. Die Einrichtung unterscheidet sich nicht grundlegend von der Einrichtung eines Servers mit Windows Server 2008 R2.

Im Rahmen des Assistenten legen Sie fest, ob der Server Updates direkt bei Microsoft herunterladen soll oder von einem anderen WSUS-Server. Außerdem lassen sich die Sprachen und Produkte festlegen, die über WSUS aktualisiert werden sollen. Auch den Zeitplan der Aktualisierung legen Sie bei der Einrichtung fest.

Abbildg. 37.2 Einrichten der Synchronisierung



Nach der ersten Einrichtung lassen sich alle Einstellungen über die WSUS-Konsole anpassen, Berichte erstellen und die erste Synchronisierung starten. Über das Kontextmenü von WSUS-Servern starten Sie dann zukünftig die Verwaltungskonsole.

WSUS scannt heruntergeladene Updates und referenziert diese automatisch mit den verbundenen Clients. Einstellungen können Sie über Gruppenrichtlinien verteilen. Damit die Clients Updates installieren, müssen diese so konfiguriert sein, dass sie keine Patches aus dem Internet herunterladen, sondern den internen WSUS verwenden. Die Konfiguration der automatischen Updates in den Gruppenrichtlinien nehmen Sie in der Gruppenrichtlinienverwaltung unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Windows Update* vor. Dazu später mehr.

Über einen eigenen Menübereich in der Verwaltungskonsole lassen sich auch Berichte erstellen. So können sich Administratoren jederzeit einen Überblick verschaffen, welche Updates aktuell im Unternehmen verteilt sind und wie der Updatestatus der einzelnen Server ist.

Patchverwaltung mit WSUS

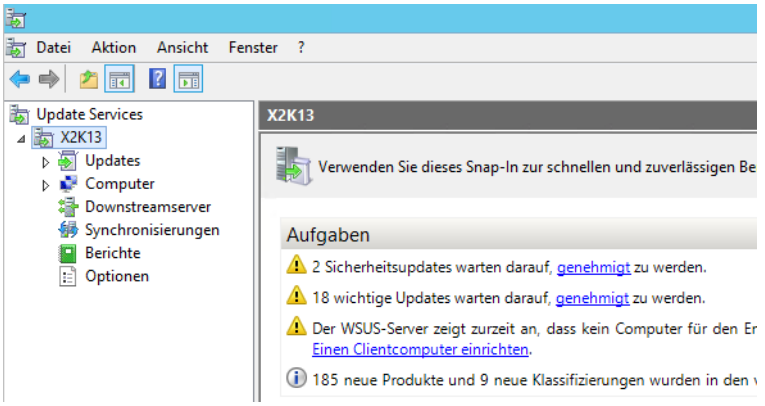
In den folgenden Abschnitten zeigen wir Ihnen, wie Sie WSUS verwalten und Clients an den Server anbinden.

TIPP Weitere Informationen, Anleitungen und Hilfen finden Sie auf den folgenden Internetseiten:

- *http://www.wsus.de* [Ms179-K37-03]
- *http://www.wsus-praxis.de* [Ms179-K37-04]
- *http://blogs.technet.com/wsus* [Ms179-K37-05]
- *http://www.wsus.info* [Ms179-K37-06]

Über den Eintrag *Synchronisierungen* in der Verwaltungskonsole sehen Sie, ob der erste Synchronisierungsvorgang erfolgreich war. Sie erfahren dann auch im oberen Bereich der Konsole, ob neue Updates zur Verfügung stehen, die Sie genehmigen müssen.

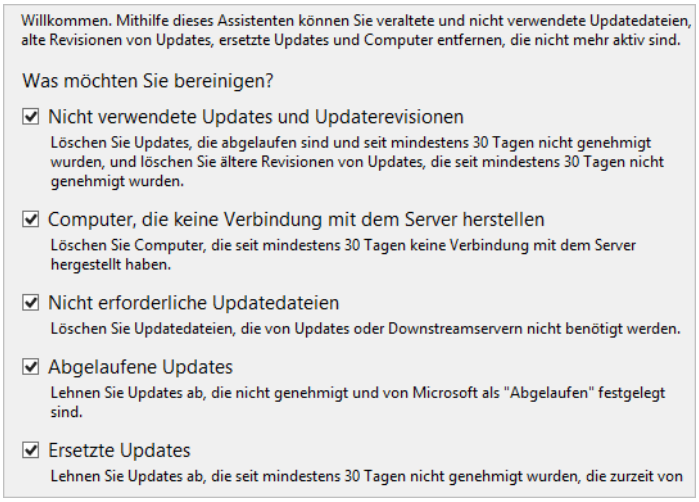
Abbildg. 37.3 Überprüfen der neuen Updates in WSUS



Mit dem *Assistenten für die Serverbereinigung* in den *Optionen* können Sie WSUS säubern. Auf diesem Weg lassen sich zum Beispiel Updates für Produkte, die Sie im Unternehmen nicht mehr einsetzen, oder alte Versionen vom Server löschen. Über den Assistenten zur Bereinigung können Sie darüber hinaus PCs aus der Datenbank löschen, 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. Diesen Assistenten starten Sie in der Konsolenstruktur über den Eintrag *Optionen* und einen Klick auf *Assistent für die Serverbereinigung*.

Abbildg. 37.4 WSUS verfügt über eine interne Reinigungsroutine, die über die Verwaltung in den Optionen gestartet werden kann



Clientcomputer über Gruppenrichtlinien anbinden

WSUS scannt heruntergeladene Updates und referenziert diese automatisch mit den verbundenen Clients. Einstellungen können Sie über Gruppenrichtlinien verteilen. Damit die Clients Updates installieren, müssen diese so konfiguriert sein, dass sie keine Patches aus dem Internet herunterladen, sondern den internen WSUS verwenden.

TIPP Wer WSUS in der PowerShell verwalten will, kann sich mit dem Befehl *Get-Command -Module UpdateServices* alle Cmdlets anzeigen lassen, mit denen sich die Windows Server Update Services verwalten lassen.

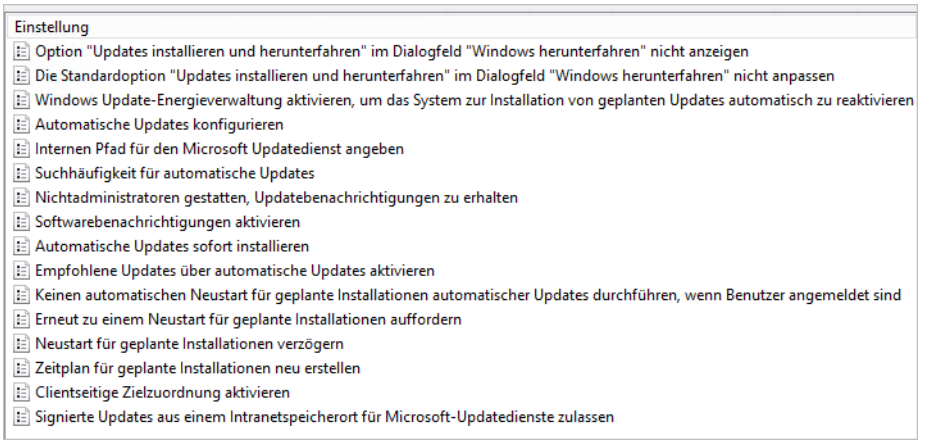
WSUS verteilt die Patches nicht automatisch an die Clients, sondern lädt die Aktualisierungen nur aus dem Internet herunter und stellt diese bereit.

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, erstellen Sie am besten spezielle Gruppenrichtlinien:

1. Starten Sie die *Gruppenrichtlinienverwaltung* über die Startseite.
2. Navigieren Sie zu *Gesamtstruktur/Domänen/<Ihre Domäne>/Gruppenrichtlinienobjekte*.
3. Klicken Sie mit der rechten Maustaste auf *Gruppenrichtlinienobjekte* und wählen Sie *Neu*.
4. Geben Sie als Name »Patchverwaltung« oder Ähnliches ein.
5. Klicken Sie auf *OK*.
6. Starten Sie über das Kontextmenü die Bearbeitung der Richtlinie. Die Konfiguration der automatischen Updates in den Gruppenrichtlinien nehmen Sie unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/Windows Update* vor.

Abbildg. 37.5 Konfigurieren von Gruppenrichtlinien für Windows Updates



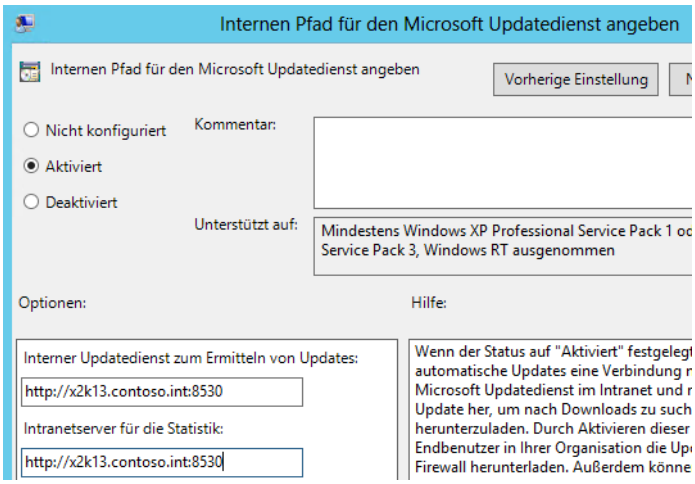
Die Arbeitsstationen lassen sich so konfigurieren, dass diese automatisch Aktualisierungen vom WSUS herunterladen und installieren. Auf diesem Weg aktualisieren Sie auch den Server. Grundsätzlich lässt sich die Konfiguration der automatischen Updates in drei Bereiche untergliedern:

- Automatisches Herunterladen der Patches vom WSUS auf den Rechner, aber keine Installation, sondern nur die Meldung anzeigen, dass Patches vorhanden ist
- Meldung anzeigen, dass neue Patches auf dem WSUS zur Verfügung stehen, aber kein Herunterladen der Patches auf den lokalen Computer
- Automatisches Herunterladen und automatische Installation der Patches. Dies ist die optimale Einstellung für Arbeitsstationen und kleine Netze.

Die erste Option ist *Internen Pfad für den Microsoft Updatedienst angeben*. Diese Option aktivieren Sie. Da WSUS eine Webapplikation ist, müssen Sie den Servernamen mit einer HTTP-Adresse angegeben: *http://<Servername>:<Port>*.

Den Port sehen Sie, wenn Sie über *Start/Verwaltung* den Internetinformationsdienste-Manager starten und auf *WSUS-Verwaltung* klicken. Im rechten Bereich sehen Sie bei *Website durchsuchen* den Port für die HTTP-Verbindung. Alternativ finden Sie den Port auch in der WSUS-Konsole im unteren Bereich.

Abbildg. 37.6 Festlegen des Pfads zum WSUS



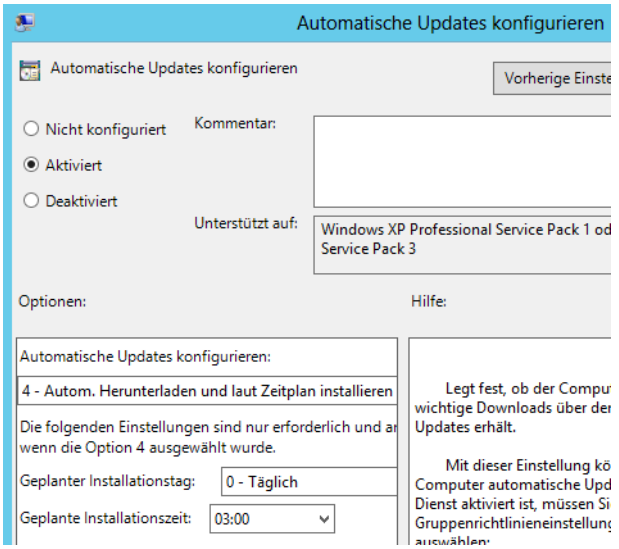
Die zweite wichtige Option ist das Updateverhalten, das Sie über *Automatische Updates konfigurieren* festlegen. Dabei stehen hauptsächlich folgende Möglichkeiten zur Verfügung:

- **Vor Herunterladen und Installation benachrichtigen** Mit dieser Option benachrichtigt Windows Administratoren vor dem Download und vor der Installation der Updates. Dazu blendet Windows ein Symbol in der Taskleiste ein.
- **Autom. Herunterladen, aber vor Installation benachrichtigen** Mit dieser Option führt der Client automatisch den Download der Updates durch, eine Installation findet aber nicht automatisch statt. Diese Einstellung ist optimal für Server.
- **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, startet Windows beim nächsten Start die Aktualisierung.
- **Lokalen Administrator ermöglichen, Einstellung auszuwählen** Mit dieser Option lassen Sie zu, dass lokale Administratoren mithilfe der Option *Automatische Updates* in der Systemsteuerung die Konfiguration selbst auswählen können.

Ebenfalls interessant ist die Funktion, die Energieverwaltung von Windows 7/8/8.1 zusammen mit der Anbindung an den WSUS über Gruppenrichtlinien zu steuern. Der PC reaktiviert sich dazu automatisch, wenn Windows Update zur automatischen Installation von Updates konfiguriert ist.

Wenn sich das System zum Zeitpunkt der geplanten Installation im Ruhezustand befindet, startet das System mit dem Windows-Energieverwaltungsfeature automatisch, um die Updates zu installieren. Wenn sich das System zum Zeitpunkt der Reaktivierung im Akkubetrieb befindet, installiert Windows aber keine Updates.

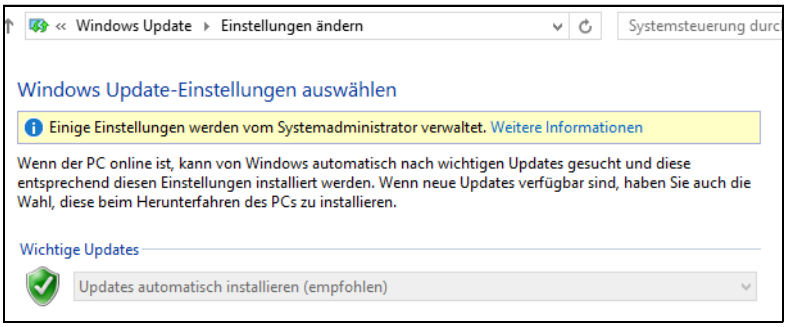
Abbildg. 37.7 Konfigurieren des Updateverhaltens der Clients



Haben Sie alle Einstellungen vorgenommen, beenden Sie die Bearbeitung der neuen Gruppenrichtlinien. Ziehen Sie anschließend die neue Gruppenrichtlinie per Ziehen/Ablegen auf den Namen Ihrer Domäne in der Gruppenrichtlinienverwaltung, damit diese verknüpft wird. Sie erhalten eine entsprechende Meldung angezeigt. Starten Sie anschließend die Computer neu und überprüfen Sie in der Windows Update-Steuerung der Systemsteuerung, ob die Anbindung erfolgreich war.

In der Systemsteuerung auf den Clients und Servern erhalten Sie Hinweise, falls Einstellungen zentral durch Gruppenrichtlinien vorgegeben sind. Sie starten die Windows Update-Verwaltung am schnellsten durch Eingabe von *wuapp* auf der Startseite. Klicken Sie auf *Einstellungen ändern*, sehen Sie, dass der Client Einstellungen von Servern erhält. Diese sind für die Änderung auf dem Client fest gesetzt und lassen sich nicht deaktivieren.

Abbildg. 37.8 Überprüfen der Einstellungen für Updates



Anwender können aber nach der Anbindung an WSUS über den Link *Online nach Updates aus Windows Update suchen* auch im Internet nach Aktualisierungen suchen, die noch nicht auf dem WSUS zur Verfügung stehen.

TIPP Nach der Konfiguration der Gruppenrichtlinie kann es einige Zeit dauern, bis die Arbeitsstationen und Server mit WSUS verbunden sind und in der Administrationsoberfläche des WSUS erscheinen.

Auf den einzelnen Rechnern können Sie in der Eingabeaufforderung durch Eingabe des Befehls *wuauclt /detectnow* eine sofortige Verbindung zum WSUS erzwingen. Ist der Client noch immer nicht angebunden, geben Sie in der Befehlszeile *Gpupdate /force* und dann *Wuauclt.exe /reportnow /detectnow* ein.

Sollten die Einstellungen in der Gruppenrichtlinie auf einem Computer noch nicht gespeichert sein, hat Windows unter Umständen die Gruppenrichtlinie noch nicht angewendet. In diesem Fall können Sie mit dem Befehl *gpupdate /force* das Aktualisieren der Gruppenrichtlinie auf dem Client erzwingen (siehe Kapitel 19). Sie benötigen dazu eine Eingabeaufforderung mit Administratorrechten.

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 sein.
5. Geben Sie in der Eingabeaufforderung den Befehl *wuauclt /detectnow* ein.

Sollte dies nicht funktionieren, können Sie noch im Registryschlüssel *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate* die Einträge für den WSUS löschen. Anschließend geben Sie den Befehl *wuauclt /detectnow /reauthorization* ein.

Updates genehmigen und bereitstellen

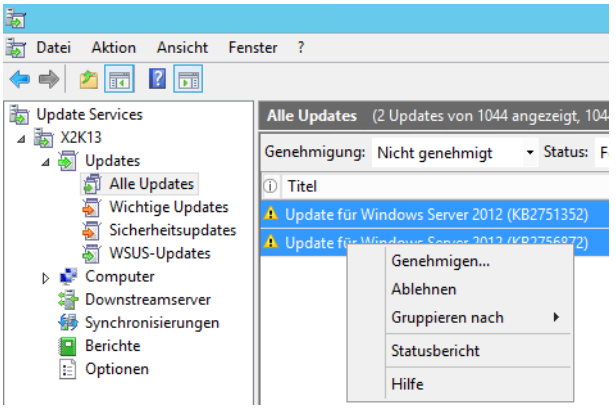
WSUS lädt die konfigurierten Updates basierend auf den vorgenommenen Spracheinstellungen, Produkten und Klassifizierungen aus dem Internet herunter, installiert diese aber nicht automatisch. Erst wenn ein Administrator einen Patch genehmigt, installiert Windows diesen Patch auf Computern. Über die Optionen in der WSUS-Verwaltung können Sie Regeln erstellen, über die Sie Updates automatisch zur Installation auf den verschiedenen Computergruppen genehmigen. Updates können Sie aber auch manuell oder in Gruppen genehmigen oder ablehnen.

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 Sie die entsprechenden Updates für andere Computergruppen oder alle Clients freigeben. Um Updates zu genehmigen, gehen Sie folgendermaßen vor:

1. Klicken Sie in der WSUS-Verwaltungskonsole auf *Updates/Alle Updates*. Anschließend sehen Sie eine Zusammenfassung der Updates, die auf dem Server verfügbar sind.
2. Wählen Sie in der Liste die Updates aus, die Sie zum Installieren genehmigen möchten. Die Ansicht können Sie entsprechend filtern. Wählen Sie ein Update aus, erhalten Sie im mittleren Bereich der Konsole ganz unten ausführliche Informationen angezeigt.

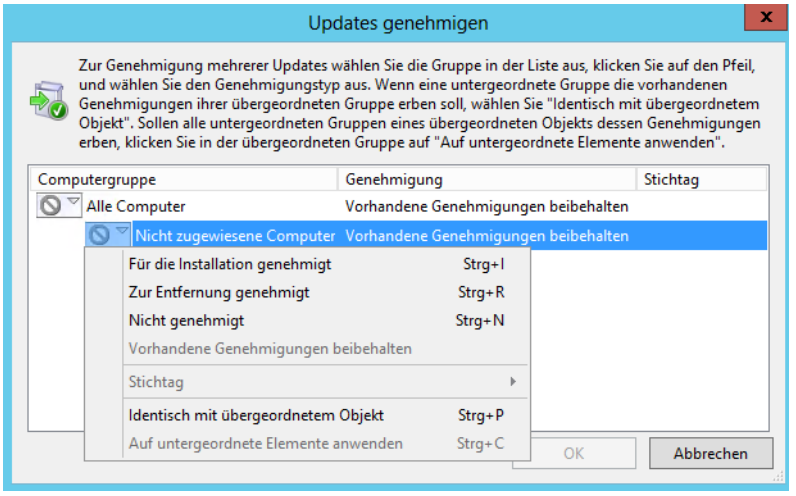
3. Klicken Sie mit der rechten Maustaste auf den oder die Patches und wählen Sie im Kontextmenü den Befehl *Genehmigen* aus. Sie können auch mehrere Updates oder mit der Tastenkombination Strg + A alle Updates auswählen und über das Kontextmenü genehmigen.

Abbildg. 37.9 Verwalten und Genehmigen von Updates



Wählen Sie die Gruppen aus und klicken Sie auf das Dreieck links neben der Gruppe. Sie können jetzt aus verschiedenen Optionen auswählen: *Für die Installation genehmigt*, *Zur Entfernung genehmigt*, *Nicht genehmigt*, *Stichtag*, *Identisch mit übergeordnetem Objekt* und *Auf untergeordnete Elemente anwenden*. Klicken Sie auf die Option *Für die Installation genehmigt* und anschließend auf *OK*. Wie Sie aus dem Menü erkennen können, kann WSUS installierte Patches auch wieder deinstallieren, wenn diese zum Beispiel mit speziellen Applikationen Probleme bereiten.

Abbildg. 37.10 Genehmigen von Updates



Berichte mit WSUS abrufen

Ab 24 Stunden nach der Freigabe von Patches können Sie in den Berichten zum WSUS überprüfen, ob die Updates auf den Computern bereitgestellt wurden. Wollen Sie mit Berichten arbeiten, muss auf dem Server das Tool Microsoft Report Viewer Redistributable 2010 (*http://www.microsoft.com/de-de/download/details.aspx?id=6442* [Ms179-K37-07]) installiert sein. 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*.
5. Berichte können Sie auch als Excel-Tabelle oder PDF-Datei speichern oder drucken. Klicken Sie dazu in der Symbolleiste auf das *Speichern*-Symbol.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie Updates mit WSUS im Netzwerk bereitstellen und WSUS verwalten. Auch die Anbindung von Windows 8/8.1 und Windows Server 2012 R2 an WSUS war Thema dieses Kapitels.

Im nächsten Kapitel lesen Sie, wie Sie Windows Server 2012 R2 überwachen und optimieren.

Kapitel 38

Diagnose und Überwachung

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, welche Bordmittel und Zusatztools Ihnen bei der Überwachung von Windows Server 2012 behilflich sein können. In Kapitel 15 sind wir bereits auf die Überwachung von Active Directory eingegangen. In diesem Kapitel erläutern wir Ihnen die Überwachung aller anderen Serverdienste in Windows Server 2012. In Kapitel 6 zeigen wir Ihnen Tools und Möglichkeiten, um den Netzwerkverkehr weiter zu analysieren.

Fehlerbehebung in Windows Server – Ereignisanzeige

Alle Fehler und Aktionen von Windows werden in den Ereignisanzeigen festgehalten und stehen Administratoren zur Verfügung, um Fehler zu beheben. 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. Sie sollten in regelmäßigen Abständen auf Datenbankservern nach Einträgen suchen, da Sie hier frühzeitig Fehler erkennen können.

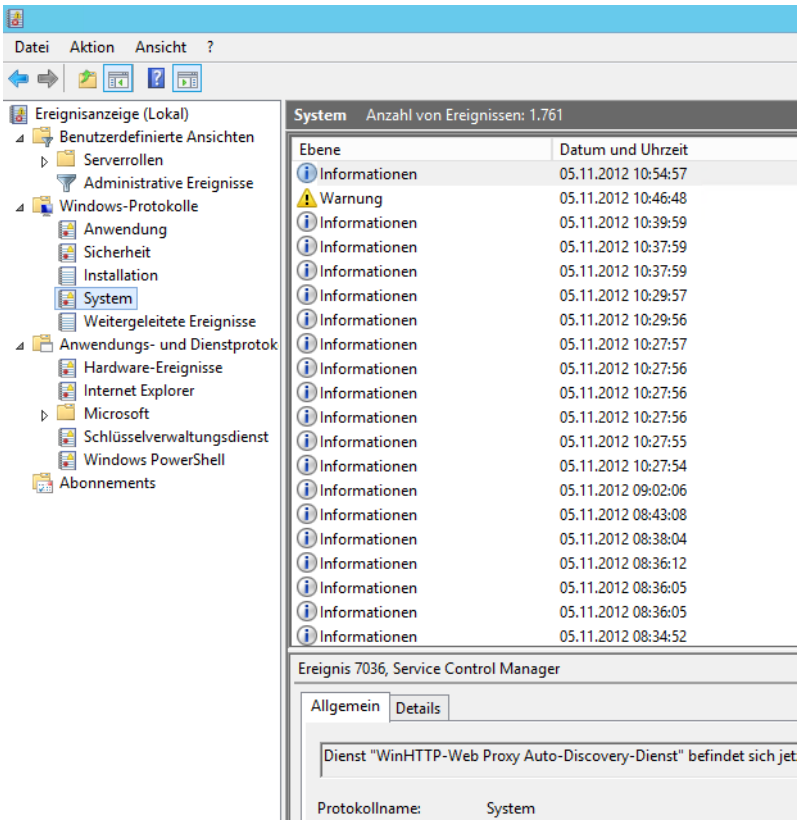
Ereignisanzeige nutzen

Sie rufen die Ereignisanzeige durch Eingabe von *eventvwr.msc* auf der Startseite auf.

HINWEIS Unter Windows Server 2012 können Sie auf der Startseite direkt mit dem Tippen von *eventvwr.msc* beginnen oder über ⊞ + R das Dialogfeld *Ausführen* aufrufen und dort den Programmnamen eingeben.

Die Ereignisanzeige sehen Sie auch unterhalb des Knotens *Diagnose* im Server-Manager. In Windows Server 2012 finden Sie die Ereignisanzeige im Menüpunkt *Tools*. Unter dem Knoten *Windows-Protokolle* ist auch weiterhin der Zugriff auf die vertrauten Anwendungs-, System- und Sicherheitsprotokolle möglich.

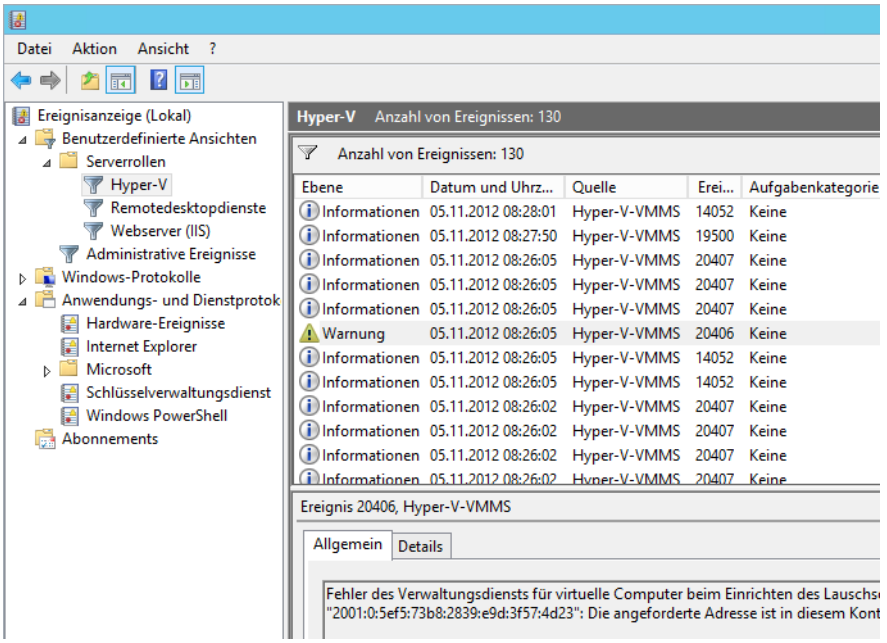
Abbildg. 38.1 Anzeigen der Ereignisprotokolle in Windows Server 2012



Klicken Sie direkt auf den Knoten *Ereignisanzeige*, sehen Sie eine Zusammenfassung aller Serverfehler im rechten Bereich. Im Knoten *Anwendungs- und Dienstprotokolle* finden Sie zahlreiche Protokolle zu den einzelnen Serverdiensten in Windows Server 2012. Viele Einträge für Serveranwendungen wie SQL Server 2012 sind im Knoten *Anwendungen* zu finden.

Über den Knoten *Benutzerdefinierte Ansichten* lassen Sie sich Filter für alle installierten Serverrollen anzeigen. Auf diese Weise können Sie auch Filter für die SQL-Instanzen erstellen lassen oder andere Serveranwendungen, die auf dem Server installiert sind.

Abbildg. 38.2 Anzeigen von Meldungen gefiltert nach Serverrollen

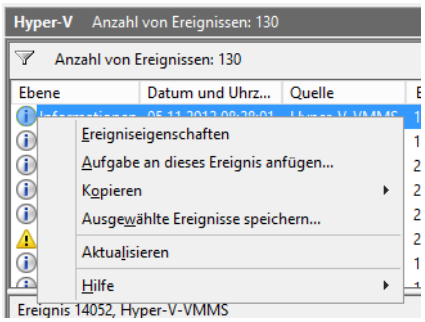


HINWEIS Der Speicherort der Standardprotokolle in der Ereignisanzeige ist *%SystemRoot%\System32\winevt\Logs*. Die Protokolldateien erhalten die Endung *.evtx*, da diese XML-basiert sind.

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 2012 bietet die Möglichkeit, weniger interessante Ereignisse herauszufiltern, sodass Sie sich auf jene Ereignisse konzentrieren können, die wichtig sind. Klicken Sie eine Meldung an, erhalten Sie im unteren Bereich ausführlichere Informationen.

Mit dem Windows-Aufgabenplaner können Sie einem Ereignis eine Aufgabe hinzufügen. Jedes Mal, wenn ein Ereignis erscheint, das der Abfrage entspricht, startet anschließend die entsprechende Aufgabe. Dazu klicken Sie mit der rechten Maustaste auf das Ereignis und wählen *Aufgabe an dieses Ereignis anfügen*. In diesem Fall startet Windows die Aufgabe immer genau dann, wenn die Datensicherung erfolgreich abgeschlossen ist.

Abbildg. 38.3 Aufgaben anhängen



Wenn Sie ein Ereignisprotokoll aufrufen, erhalten Sie im mittleren Bereich des Fensters eine Zusammenfassung aller Einträge, deren detaillierte Informationen Sie per Doppelklick auf einzelne Meldungen anzeigen lassen können. Auf Basis dieser Fehlermeldung können Sie erkennen, welche Probleme Windows Server 2012 mit einzelnen Komponenten erkannt hat. Sie sollten regelmäßig die Ereignisanzeigen auf Fehler überprüfen, da Sie hier schnell Probleme erkennen können, bevor diese gravierendere Auswirkungen haben.

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* [Ms179-K38-01] gezielt nach diesen Fehlern. Auf dieser Seite gibt es zu so gut wie jedem Eintrag der Ereignisanzeige Hinweise und mögliche Lösungsansätze.

Außerdem können Sie den Fehler in einer Suchmaschine oder in speziellen Supportseiten eingeben, wie zum Beispiel *http://www.experts-exchange.com* [Ms179-K38-02]. Auch die Suche in der Microsoft Knowledge Base unter *http://support.microsoft.com* [Ms179-K38-03] hilft oft weiter. Suchen Sie allerdings in der englischen Microsoft Knowledge Base immer nur nach englischen Begriffen, da Sie hier mehr Antworten erhalten.

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 lassen sich 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 möchten. Speichern Sie das Protokoll zuvor, entspricht dies der Option *Ereignisse speichern unter*.

- **Aktuelles Protokoll filtern** Dieser Menübefehl wird verwendet, wenn Sie keine eigene Ansicht des Protokolls erstellen möchten, 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 2012 beim Erreichen der maximalen Ereignisprotokollgröße verhalten soll
- **Aufgabe an dieses Protokoll anfügen** Mit dieser Option können Sie über die Aufgabenplanung automatisch bestimmte Aktionen und Skripts starten, wenn in den Ereignisanzeigen bestimmte Fehler auftauchen. Solche Aufgaben lassen sich auch an einzelne Ereignisse anfügen.

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. Stellen Sie fest, 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 aufgrund defekter Hardware auf, sondern meist durch Änderungen am System oder der Installation von Applikationen und Tools. Durch die Filtermöglichkeiten der Ereignisanzeige in Windows Server 2012 können Fehler oft sehr genau eingegrenzt werden.

Ereignisprotokolle im Netzwerk einsammeln

Nicht jedes Unternehmen setzt auf professionelle und teure Überwachungslösungen, um Server im Netzwerk zu überwachen. Selbst beim Einsatz solcher Lösungen kann es sinnvoll sein, zusätzlich noch Protokolldateien und Ereignisanzeigen zu überwachen. Es gibt zahlreiche kostenlose Möglichkeiten, um die Ereignisanzeigen und Protokolle der Server an einer zentralen Stelle zu sammeln und zu analysieren.

Zunächst bietet Windows Server 2012 die Möglichkeit, Ereignisse von Servern im Netzwerk zu sammeln, Abonnement genannt. Darüber hinaus gibt es Freewaretools, die ebenfalls in der Lage sind, Ereignisse in den Protokollen von Windows-Servern zu sammeln und Administratoren zentral zur Verfügung zu stellen. Nachfolgend zeigen wir Ihnen, welche Möglichkeiten es gibt. Achten Sie aber darauf, dass derartige Tools teilweise auch den Server belasten und vorsichtig eingesetzt werden sollten.

Echtzeitüberwachung der Ereignisprotokolle – EventSentry

EventSentry ist eine Monitoring-Software zur Erfassung, Analyse und Anzeige von Systemereignissen. Es besteht auch die Möglichkeit, Informationen per E-Mail zu versenden, wenn bestimmte Ereignismeldungen in den Protokollen der Server auftauchen. In der E-Mail ist die auslösende Ereignismeldung mit allen Daten enthalten. Die Lizenz der Anwendung für einen Host kostet 85 Dollar. Es gibt auch eine kostenlose, aber etwas eingeschränkte Light-Variante von EventSentry. Diese kann ebenfalls Ereignisanzeigen überwachen und E-Mails versenden, aber nicht so umfassend laufende Dienste oder Protokolldateien auf Servern überwachen. Die genauen Unterschiede finden

Sie auf der Seite des Herstellers (*http://www.eventsentry.com/downloads/full-vs-light* [Ms179-K38-04]). In vielen Fällen reichen die Funktionen der kostenlosen Light-Edition aber aus.

Der Hauptvorteil von EventSentry liegt darin, dass Sie die Ereignisanzeigen aller Ihrer Server in Echtzeit überwachen können. Abhängig von Fehlermeldungen, die in den verschiedenen Ereignisanzeigen auftreten, können Sie Aktionen durchführen lassen, zum Beispiel E-Mails an Administratoren verschicken, die den Inhalt der Ereignismeldung enthalten. Mit diesem Tool können Sie Fehler und drohende Ausfälle in Ihrem Netzwerk sehr früh erkennen. Sie können sich eine 30-Tage-Testversion oder die kostenlose Light-Version von der Seite *http://www.eventsentry.com* [Ms179-K38-05] herunterladen.

Zur Überwachung installieren Sie auf den zu überwachenden Servern das Tool mit den entsprechenden Agenten zur Überwachung. Auf einem Computer im Netzwerk installieren Sie die Verwaltungsoberfläche, auf jedem Server, den Sie überwachen möchten, den entsprechenden Agenten. Die Auswahl zur Installation nehmen Sie im Setup-Assistenten vor. Nach dem Start erscheint ein Agent, der Sie bei der Einrichtung der Anwendung unterstützt.

Im Rahmen der Einrichtung legen Sie fest, auf welche Arten von Ereignissen in den Ereignisanzeigen das Tool achten soll. In der Verwaltungsoberfläche können Sie direkt die Ereignisanzeigen *Application*, *Security* und *System* auf den angebundenen Server öffnen. Im Bereich *Packages/Event-Log Packages/Default* legen Sie fest, welche Ereignisse das Tool auf den Servern überwachen soll, auf denen der Agent installiert ist. Auf diesem Weg können Sie auch gezielt nach einzelnen IDs oder nach Ereignisquellen filtern lassen. Im Bereich *Actions* legen Sie fest, welche Aufgaben das Tool durchführen soll, wenn Ereignisse auftreten, die den konfigurierten Filtern entsprechen.

Die einzelnen Aktionen wiederum, zum Beispiel die Konfiguration der Warn-E-Mails, nehmen Sie im Bereich *Actions* im linken Abschnitt der Verwaltungsoberfläche vor. Nach der Einrichtung sollten Sie eine Test-E-Mail versenden lassen, um sicherzustellen, dass der E-Mail-Fluss funktioniert. Nach der Installation blendet EventSentry auch ein Informationsfenster ein, sobald ein Fehler auf dem Server auftaucht.

Ereignisanzeigen sammeln – PsLogList

Mit PsLogList aus der PsTools-Sammlung von Sysinternals (*http://technet.microsoft.com/de-de/sysinternals* [Ms179-K38-06]), können Sie über die Eingabeaufforderung die Ereignisanzeigen verschiedener Computer einsammeln, anzeigen und vergleichen. Wenn Sie das Tool ohne Optionen aufrufen, zeigt PsLogList alle Einträge des lokalen Systemereignisprotokolls an. Das Programm verfügt darüber hinaus über 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>
```

Tabelle 38.1 Optionen von PsLogList

Option	Auswirkung
@<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.

Tabelle 38.1 Optionen von PsLogList *(Fortsetzung)*

Option	Auswirkung
–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 angezeigt, die mit den entsprechenden Buchstaben anfangen.
–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 sie, 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 Systemereignisprotokoll. Sie können die Ereignisanzeige auswählen, wenn Sie die ersten Buchstaben oder die entsprechende Abkürzung angeben. Allerdings müssen auch auf deutschen Windows-Servern 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.

Geben Sie zum Beispiel den Befehl *psloglist system* ein, listet das Tool in der Eingabeaufforderung alle Ereignisse des Systemereignisprotokolls auf. Der Befehl *psloglist application* zeigt das Anwendungsprotokoll an. Wollen Sie nur die aktuellsten fünf Einträge sehen, verwenden Sie den Befehl *psloglist system –n 5*. Die fünf ältesten Einträge zeigen Sie mit *psloglist system –r –n 5* an.

Um effizient Daten anzuzeigen, sollten Sie die Anzeige filtern, da ansonsten zu viele Informationen auf dem Bildschirm erscheinen. Dazu verwenden Sie die Option *–f*. Wollen Sie zum Beispiel nur Fehlermeldungen erfassen, geben Sie den Befehl *psloglist system –f e* ein. Fehler und Warnungen erhalten Sie mit der Option *–f ew* angezeigt. Um nur Meldungen einer bestimmten ID anzuzeigen, verwenden Sie *–i*, gefolgt von einer kommagetrennten Liste der IDs, die Sie anzeigen wollen.

Eine weitere Möglichkeit ist das Exportieren der Ausgabe in eine *.evt*-Datei, die Sie wiederum mit der Ereignisanzeige in Windows öffnen können. Dazu verwenden Sie zusätzlich die Option *–g .\<.evt-Datei>*.

Mit PsLogList können Sie auch die Ereignisanzeigen von Computern im Netzwerk auslesen. Dazu verwenden Sie zunächst die Option *psloglist \\<Computer>* und dann die verschiedenen Optionen des Tools, um die Anzeige zu aktivieren. Dabei gehen Sie genauso vor wie bei der Abfrage lokaler Ereignisanzeigen.

Ereignisabonnements verwalten

Windows Server 2012 kann auch mit Bordmitteln die Ereignisanzeigen verschiedener Server im Netzwerk zusammentragen und anzeigen. Diese Funktion trägt die Bezeichnung *Abonnements* und lässt sich direkt in der Ereignisanzeige einrichten. Basis ist der Systemdienst *Windows-Ereignissammeldienst*. Dieser muss auf dem Server gestartet sein, der die verschiedenen Ereignisse sammeln soll, sowie auf allen beteiligten Servern. Damit die Sammlung von Ereignisanzeigen funktioniert, müssen Sie die beteiligten Computer vorbereiten, das Abonnement erstellen und dann in der Ereignisanzeige die Fehler der entsprechenden Server anzeigen.

Die Sammlung von Ereignisanzeigen basiert auf zwei Grundlagen. Es gibt einen Server, der die Daten sammelt (Sammlungscomputer) und Server, die an den Sammlungsserver angebunden sind (Quellcomputer). Die Sammlung von Ereignisanzeigen führen Sie am besten auf Servern durch, die in einer gemeinsamen Active Directory-Gesamtstruktur positioniert sind.

Im ersten Schritt müssen Sie die Remoteverwaltung auf den einzelnen Servern aktivieren. Dazu führen Sie auf jedem Quellcomputer und dem Sammlungscomputer in einer Eingabeaufforderung mit Administratorrechten (über das Kontextmenü gestartet) den Befehl *winrm quickconfig* aus. Im nächsten Schritt führen Sie noch den Befehl *wecutil qc* aus. Das Tool konfiguriert das Weiterleiten von Ereignissen über das Netzwerk zu einem Sammlungscomputer. Nehmen Sie anschließend das Computerkonto des Sammlungscomputers, auf dem Sie die Ereignisse aller angebundenen Server anzeigen wollen, in die lokalen Administratorgruppen der einzelnen Server auf.

Abbildg. 38.4 Konfigurieren der Remoteverwaltung und des Windows-Ereignissammeldienstes in Windows Server 2012

```
C:\Users\administrator.CONTOSO>wecutil qc
Der Startmodus für den Dienst wird in den Modus für verzögerten Start geändert.
Möchten Sie den Vorgang fortsetzen (J- ja oder N- nein)?j
Der Windows-Ereignissammlungsdienst wurde erfolgreich konfiguriert.
```

Die lokale Benutzerverwaltung starten Sie am schnellsten durch die Eingabe von *lusrmgr.msc* auf der Startseite. Rufen Sie die Eigenschaften der lokalen Administratorgruppe auf, klicken Sie auf die

Schaltfläche *Hinzufügen* und im daraufhin geöffneten Dialogfeld auf die Schaltfläche *Objekttypen*, um auch Computerkonten in die Gruppe aufnehmen zu können.

Wollen Sie Ereignisabonnements in Arbeitsgruppen erstellen, müssen Sie manuell eine Ausnahme in der Windows-Firewall für *Remote-Ereignisprotokollverwaltung* auf jedem Quellcomputer hinzufügen. Das Konto, mit dem Sie die Ereignisse auf den Quellcomputer sammeln, müssen Sie anschließend bei der Einrichtung des Abonnements hinterlegen. Zusätzlich ist auf dem Sammlungscomputer der folgende Befehl einzugeben:

```
winrm set winrm/config/client @{TrustedHosts="<Alle Quellcomputer, durch Komma getrennt>"}
```

Die Sammlung nehmen Sie am besten mit einem Konto vor, dass über Administratorrechte in der Domäne verfügt. Wollen Sie ein eigenes Konto dafür anlegen, müssen Sie dieses in die lokale Administratorgruppe auf allen Quellcomputern aufnehmen. Normalerweise reicht es aus, wenn nur das Computerkonto des Sammlungscomputers Mitglied der Administratorgruppe auf den Quellcomputern ist.

Haben Sie alle Vorbereitungen getroffen, starten Sie auf dem Sammlungscomputer die Ereignisanzeige und klicken auf *Abonnements*. Ist der Systemdienst *Windows-Ereignissammlungsdienst* nicht gestartet, erhalten Sie eine entsprechende Meldung. Lassen Sie in diesem Fall den Dienst starten. Anschließend klicken Sie mit der rechten Maustaste auf *Abonnements* und dann auf *Abonnement erstellen*. Alternativ können Sie auch im Menü *Aktionen* auf *Abonnement erstellen* klicken.

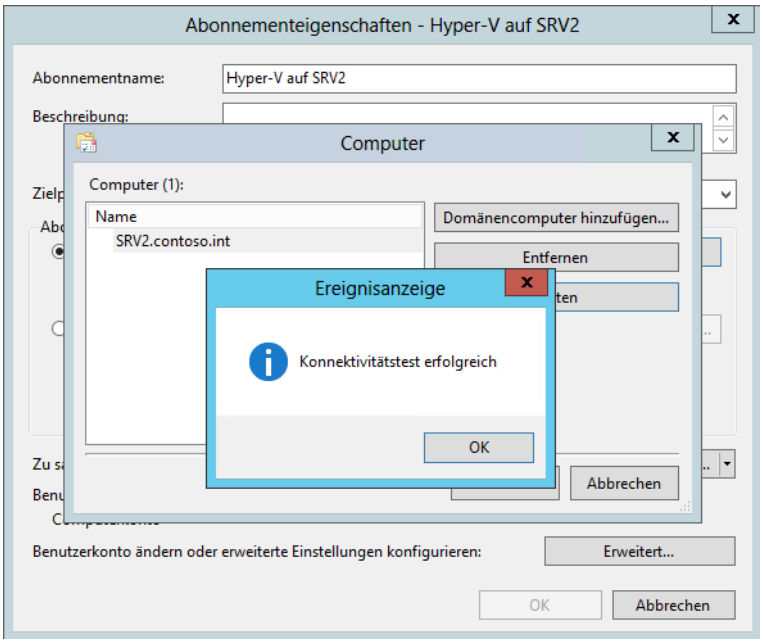
Im neuen Fenster konfigurieren Sie jetzt das Abonnement. Bei *Abonnementname* geben Sie eine Bezeichnung und auf Wunsch auch eine Beschreibung ein. Bei *Zielprotokoll* wählen Sie aus, wo auf dem Sammlungsserver die Ereignisse der Quellcomputer gesammelt werden sollen. Standardmäßig ist hier das Protokoll *Weitergeleitete Ereignisse* auswählt.

Anschließend wählen Sie die Art des Abonnements aus. Aktivieren Sie die Option *Sammlungsinitiiert* und klicken Sie auf die Schaltfläche *Computer auswählen*. Anschließend wählen Sie die Quellcomputer aus, die das Abonnement erfassen soll. Sie sollten für jeden Computer, den Sie hinzufügen, auf die Schaltfläche *Testen* klicken, um sicherzustellen, dass der Sammlungscomputer eine Verbindung aufbauen kann.

Über die Schaltfläche *Ereignisse auswählen* erstellen Sie neue Filter, über die Sie festlegen, welche Ereignisse auf den Quellcomputern der Sammlungscomputer angezeigt werden sollen. Grundsätzlich legen Sie fest, welche Ereignisse von welchen Protokollen erfasst werden sollen. Haben Sie den Filter erstellt, klicken Sie auf *OK*. Bevor Sie weitere Einstellungen vornehmen, klicken Sie auf *OK*, um das Abonnement zu überprüfen.

Nach der Erstellung muss das Abonnement als *Aktiv* gekennzeichnet sein. Auf diesem Weg können Sie auch mehrere Abonnements erstellen, die verschiedene Computer mit verschiedenen Abfragefiltern erfassen. Mit einem Doppelklick auf das Abonnement können Sie dieses jederzeit wieder anpassen.

Abbildg. 38.5 Konfigurieren eines neuen Abonnements



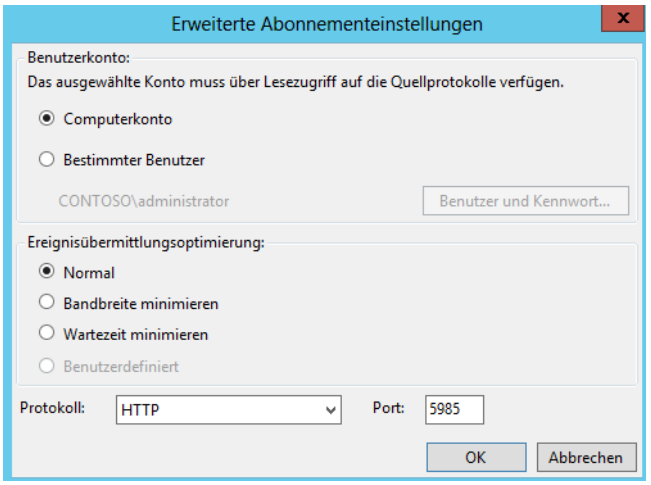
Anschließend können Sie die Ereignisse im ausgewählten Protokoll anzeigen. Haben Sie das Standardprotokoll *Weitergeleitete Ereignisse* ausgewählt, finden Sie dieses im Bereich *Windows-Protokolle*. Bis die ersten Ereignisse eintreffen, kann es allerdings eine Weile dauern. Von welchem Server die Ereignisse stammen, sehen Sie in der Spalte *Computer*.

Neben den Standardeinstellungen für Abonnements können Sie über die Schaltfläche *Erweitert* in den Eigenschaften des Abonnements einige Einstellungen ändern. Sie können an dieser Stelle zum Beispiel festlegen, dass die Abfrage der Ereignisse nicht durch das Computerkonto des Servers erfolgt, sondern mit einem speziellen Benutzerkonto, dessen Daten Sie in den erweiterten Einstellungen des Abonnements hinterlegen. Achten Sie aber darauf, dieses Konto in die lokale Administratorengruppe der Quellcomputer aufzunehmen.

Außerdem können Sie in den erweiterten Einstellungen noch festlegen, wie der Sammlungscomputer die Daten abrufen soll. Hier stehen die drei Optionen *Normal*, *Bandbreite minimieren* und *Wartezeit minimieren* zur Verfügung.

Bei der Standardeinstellung *Normal* verwendet das Abonnement den Pullzustellungsmodus. Dabei fasst das Abo immer fünf Elemente zusammen und überträgt diese vom entsprechenden Quellcomputer auf den Sammlungsserver. Die Option *Bandbreite minimieren* begrenzt die Bandbreite, die dem Abo zur Verfügung steht. Mit der Option *Wartezeit minimieren* wird sichergestellt, dass Ereignisse möglichst schnell auf dem Sammlungsserver zur Verfügung stehen.

Abbildg. 38.6 Konfigurieren von Abonnements



In den erweiterten Einstellungen legen Sie auch den Port und die Übertragungsart fest. Wenn Sie diese ändern, müssen Sie in den Firewalleinstellungen der Quellcomputer ebenfalls entsprechende Regeln definieren. In Active Directory-Umgebungen können Sie dazu auch Gruppenrichtlinien verwenden, um Regeln auf den Servern zu erstellen.

Neben den Abonnements können Sie auch mit der Standardereignisanzeige problemlos Ereignisanzeigen von Computern im Netzwerk abrufen. Sie können dazu die Ereignisanzeige selbst verwenden oder das Befehlszeilentool Wevtutil an einer Eingabeaufforderung eingeben, um Ereignisprotokolle auf einem Remotecomputer zu verwalten. Starten Sie dazu die Ereignisanzeige und klicken Sie mit der rechten Maustaste auf *Ereignisanzeige (Lokal)*. Anschließend können Sie durch Auswahl von *Verbindung mit anderem Computer herstellen* die Ereignisanzeige beliebiger Server öffnen. Wollen Sie auf diesem Weg eine Verbindung mit mehreren Servern aufbauen, müssen Sie eine neue Management Console erstellen und das Snap-In der Ereignisanzeige mehrmals integrieren.

Wollen Sie eine Verbindung mit einem anderen Benutzerkonto aufbauen, aktivieren Sie noch die Option *Verbindung unter anderem Benutzerkonto herstellen* und wählen das entsprechende Konto aus. Sie können den Benutzernamen und das Kennwort für die Verbindung festlegen.

Sie können die Ereignisanzeige eines Servers auch direkt durch Eingabe des Befehls *eventvwr<Computername>* öffnen.

Ereignisanzeige in der Systemsteuerung steuern – Wevtutil

Sie können auch in der Eingabeaufforderung eine Verbindung zur Ereignisanzeige eines anderen Servers aufbauen. Dazu verwenden Sie den folgenden Befehl:

```
wevtutil <Option> /r:<Computername> /u:<Benutzername> /p:<Kennwort>
```

Verwenden Sie die Optionen */u* und */p* nicht, verbindet Sie *wevtutil* mit dem Benutzer, mit dem Sie angemeldet sind.

Welche Optionen zur Verfügung stehen, sehen Sie, wenn Sie *wevtutil* eingeben. Das Tool dient nicht dazu, die Ereignisanzeige über das Netzwerk zu öffnen, sondern Einstellungen vorzunehmen oder das Protokoll zu löschen. Mit Aufruf *wevtutil el /r:sbs.contoso.local* lassen Sie sich zum Beispiel alle verfügbaren Protokolle auf dem Remotecomputer anzeigen. Sie können mit *wevtutil* auch Ereignisanzeigen ohne Rücksprache löschen lassen. Dazu verwenden Sie den Befehl *wevtutil cl <Name des Protokolls>*. Der Befehl *wevtutil cl System /r:sql* löscht zum Beispiel das Systemprotokoll auf dem Server *sql* ohne weitere Rücksprache. Natürlich können Sie mit dem Tool auch Protokolle über das Netzwerk auf den lokalen Computer in *.evtx*-Dateien exportieren. Dazu verwenden Sie den Befehl *wevtutil epl*.

Performance Analysis of Logs (PAL) Tool

Auf der Seite *http://pal.codeplex.com* [Ms179-K38-07] erhalten Sie das Freewaretool Performance Analysis of Logs (PAL), welches bei der Auswertung von Leistungsberichten eine gute Hilfe sein kann. Das Tool ist allerdings kein Gelegenheitstool, sondern nur geeignet, wenn Sie einen englischen Server betreiben und eine ausführliche Analyse von Logdateien durchführen wollen, die über die normalen Möglichkeiten hinausgehen.

Grundsätzlich sollten Sie das Tool nur auf Testservern installieren, nicht auf produktiven Servern. Auf der genannten Seite erhalten Sie das Tool und finden auch weiterführende Hilfe und Dokumentationen zum Thema Leistungsüberwachung von Servern. Sie benötigen für das Tool zusätzlich noch die folgenden ebenfalls frei erhältlichen Zusatzprogramme:

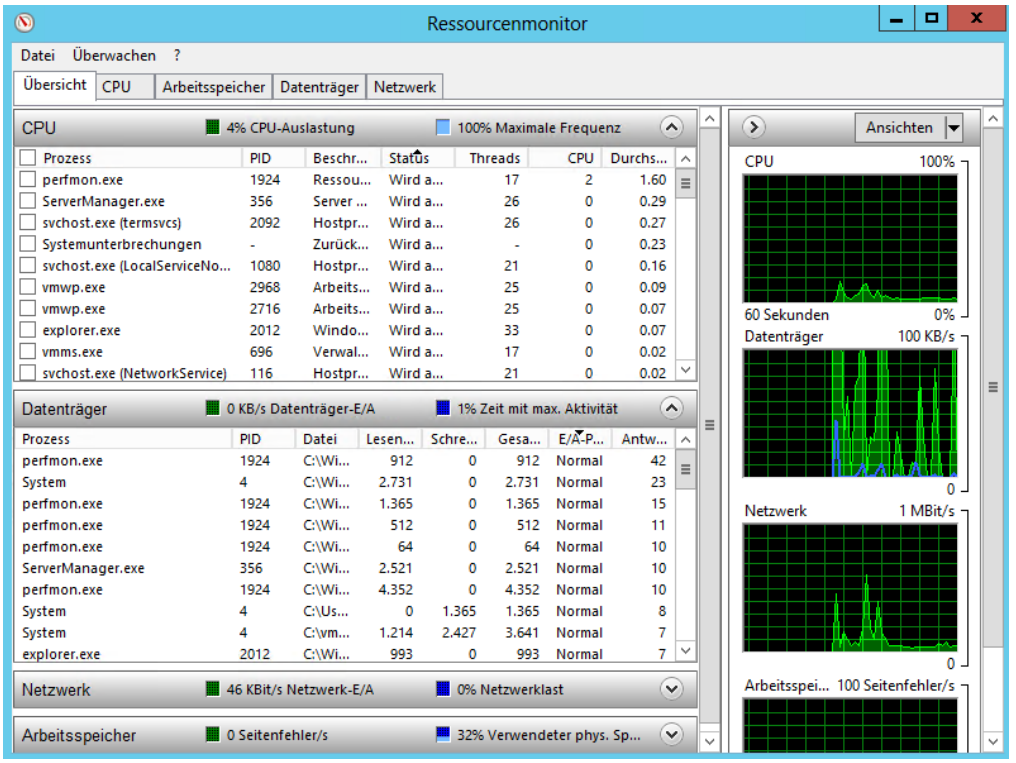
- **Log Parser 2.2** *http://www.microsoft.com/en-us/download/details.aspx?id=24659* [Ms179-K38-08]
- **Microsoft Chart Controls für Microsoft .NET Framework 3.5** *http://www.microsoft.com/de-de/download/details.aspx?id=14422* [Ms179-K38-09]
- **Office 2003-Add-In: Office Web Components** *http://www.microsoft.com/de-de/download/details.aspx?id=22276* [Ms179-K38-10]

Überwachung der Systemleistung

Über den Eintrag *Leistung* in der Konsolenstruktur des Server-Managers können Sie sich die aktuelle Systemleistung Ihres Servers mit verschiedenen Tools und Ansichten anzeigen lassen. Über den Link *Ressourcenmonitor öffnen* lässt sich eine detaillierte Ansicht des aktuellen CPU-Verbrauchs, des Arbeitsspeichers, der Datenträger und des Netzwerkverkehrs anzeigen. In Windows Server 2012 finden Sie das Programm über den Menüpunkt *Tools* im Server-Manager.

Die Gesamtleistung eines Systems wird durch verschiedene Faktoren begrenzt. Hierzu zählen etwa die Zugriffsgeschwindigkeit der physischen Datenträger, die für alle laufenden Prozesse zur Verfügung stehende Speichermenge, die Prozessorgeschwindigkeit und der Datendurchsatz der Netzwerkschnittstellen.

Abbildg. 38.7 Anzeige des Ressourcenmonitors in Windows Server 2012



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 *perfmon /res* starten. Durch Erweitern der *Ressourcenübersicht* können Sie zusätzliche Informationen anzeigen und überprüfen, welche Ressourcen von welchen Prozessen genutzt werden.

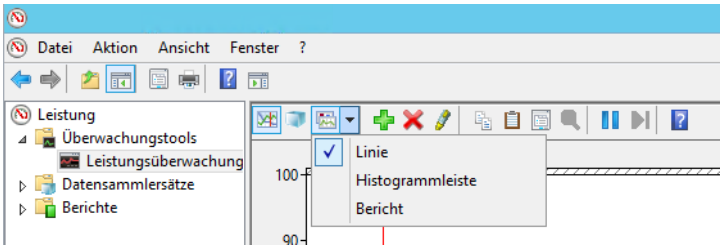
Der Bereich mit der Ressourcenübersicht enthält vier animierte Diagramme, die die Auslastung der CPU-, Datenträger-, Netzwerk- und Speicherressourcen des lokalen Computers in Echtzeit anzeigen. Unter den Diagrammen befinden sich vier erweiterbare Bereiche, in denen Einzelheiten zur jeweiligen Ressource angezeigt werden können. Klicken Sie zur Anzeige dieser Informationen auf den Abwärtspfeil rechts neben dem jeweiligen Balken.

Die Leistungsüberwachung

Klicken Sie im Server-Manager auf den Eintrag *Tools/Leistungsüberwachung*, können Sie den Server noch genauer überwachen lassen, indem Sie verschiedene Leistungsindikatoren hinzufügen. In Windows Server 2012 finden Sie das Programm im Menüpunkt *Tools*. In der Leistungsüberwachung werden die integrierten Leistungsindikatoren grafisch dargestellt. Sie können Daten in Echtzeit oder

Verlaufsdaten anzeigen und Leistungsindikatoren entweder per Ziehen/Ablegen hinzufügen oder benutzerdefinierte Datensammlergruppen (Data Collector Sets, DCS) erstellen. Die Leistungsüberwachung unterstützt verschiedene Ansichten für die visuelle Überprüfung der Daten in Leistungsprotokollen.

Abbildg. 38.8 Ändern der Ansicht in der Leistungsüberwachung



Vor allem die Auswahl *Bericht* bietet oft mehr Übersicht als die anderen Optionen in der Liste. Außerdem können Sie benutzerdefinierte Ansichten in Form von Datensammlergruppen für die Verwendung in Leistungs- und Protokollfunktionen exportieren.

Über das grüne Pluszeichen in der Symbolleiste können Sie weitere Leistungsindikatoren einblenden lassen. Für Serveranwendungen wie zum Beispiel SQL Server 2012 gibt es einige solcher Indikatoren. Das *SQLServer:Databases*-Objekt in SQL Server 2012 stellt Indikatoren zum Überwachen von Transaktionsprotokollaktivitäten zur Verfügung. Die folgenden Indikatoren sind besonders für die Überwachung der Transaktionsprotokollaktivität von Verfügbarkeitsdatenbanken interessant:

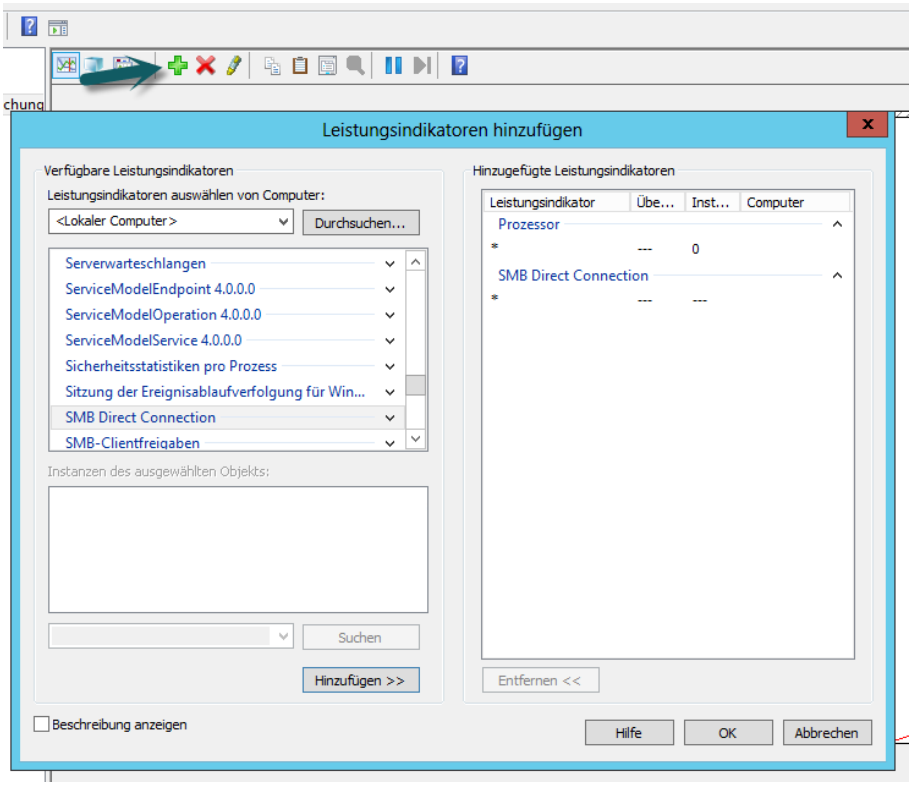
- *Schreibdauer für Protokollleerungen (ms)*
- *Protokollleerungen/Sekunde*
- *Protokollpool-Cachefehlversuche/Sekunde*
- *Protokollpool-Lesevorgänge auf dem Datenträger/Sekunde*
- *Protokollpoolanforderungen/Sekunde*

Mit den Windows-Leistungsindikatoren *Device Throughput Bytes/sec* des Objekts *SQLServer:Backup Device* und *Backup/Restore Throughput/sec* des Objekts *SQLServer:Databases* messen Sie die Übertragungsgeschwindigkeit auf das Sicherungsmedium. Auf diesem Weg können Sie die Übertragungsrate für komprimierte im Vergleich zu nicht komprimierten Sicherungen messen und auf dieser Basis entscheiden, ob die Komprimierung die höhere CPU-Last rechtfertigt.

Wählen Sie zunächst den entsprechenden Indikator aus und klicken Sie auf *Hinzufügen*. 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 Fensters. 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. 38.9 Hinzufügen von Leistungsindikatoren zur Leistungsüberwachung



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 protokolliert der Server nur die Indikatoren, die der gewählte Prozess erzeugt. Wenn Sie keine Instanz auswählen, protokolliert der Server alle Instanzen des Indikators.

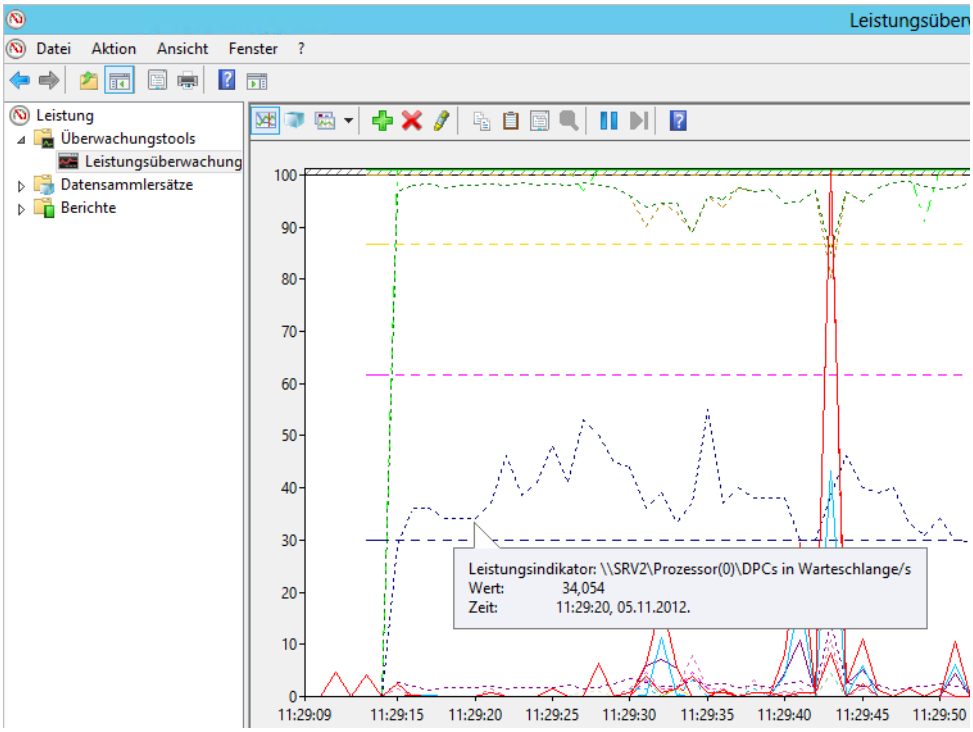
Sie können nach Instanzen eines Indikators suchen, indem Sie die Indikatorengruppe markieren oder die Gruppe erweitern und den gewünschten Indikator markieren, den Prozessnamen in das Feld unterhalb der Instanzenliste für das gewählte Objekt eingeben und auf *Suchen* klicken. Der eingegebene Prozessname wird in der Dropdownliste für eine weitere Suche angeboten.

Indikatorendaten in der Leistungsüberwachung beobachten

Standardmäßig zeigt die Leistungsüberwachung die Daten in Form eines Liniendiagramms an. 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 Dropdownlistenfeld in der Symbolleiste können Sie die Anzeige für die aktuelle Datensammlergruppe ändern.

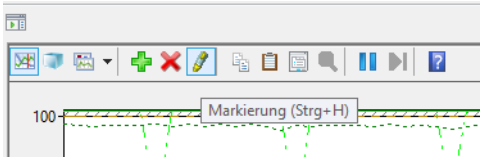
Abbildg. 38.10 Anzeigen der Überwachungsdaten



In der Histogrammansicht sehen Sie Daten ebenfalls in Echtzeit und Balkenform. 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, lässt sich 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.

Abbildg. 38.11 Markieren von Indikatoren in der Leistungsüberwachung



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 im Kontextmenü den Eintrag *Eigenschaften*. Daraufhin wird das Dialogfeld *Eigenschaften von Leistungsüberwachung* mit aktivierter Registerkarte *Daten* geöffnet. 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*. Per Klick auf die Schaltfläche *Daten aktualisieren* kann die Anzeige schrittweise durchlaufen werden.

Halten Sie die Anzeige des Liniendiagramms an und starten diese wieder, ändert sich der auf der X-Achse dargestellte Zeitraum. Die Leistungsüberwachung arbeitet mit *Objekten*, die sich beobachten lassen. 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 Multiprozessorsystem gearbeitet wird. Beim Objekt *Prozesse* wird eine Instanz für jeden aktiven Prozess definiert.

Sammlungssätze nutzen

Die Echtzeitanzeige ist nur eine Möglichkeit, die Leistungsüberwachung zu nutzen. Nachdem Sie eine Kombination aus Indikatoren zusammengestellt haben, können Sie diese als *Sammlungssätze* (Data Collector Set, DCS) speichern. 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 *Leistungsüberwachung* und rufen Sie im Kontextmenü den Untermenübefehl *Neu/ Datensammlersatz*.

Daraufhin wird der Assistent für die Erstellung einer neuen Datensammlergruppe gestartet. Die neue Datensammlergruppe enthält alle Indikatoren, die in der aktuellen Ansicht ausgewählt sind. Möchten Sie nicht den Standardbenutzer verwenden, klicken Sie im dritten Schritt des Assistenten 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. Über das Kontextmenü starten Sie einen Datensammlersatz. Nach dem Beenden erstellt der Satz einen Bericht, den Sie sich im Server-Manager anzeigen lassen können.

Ein Sammlungssatz erstellt eine Protokolldatei. Diese können Sie sich nach dem Beenden über den Bereich *Datensammlersätze/Benutzerdefiniert* aufrufen. Sie haben die Möglichkeit, für jeden Satz Speicheroptionen zu konfigurieren. Klicken Sie in der Liste des Fensters mit der rechten Maustaste auf den Namen des Sammlungssatzes und wählen Sie im Kontextmenü den Eintrag *Eigenschaften*.

Auf der Registerkarte *Allgemein* können Sie eine Beschreibung oder Schlüsselwörter für die Datensammlergruppe eingeben. Auf der Registerkarte *Verzeichnis* ist der Stammordner als Standardordner festgelegt, in dem alle Protokolldateien für die Datensammlergruppe gespeichert sind. Mit *Zeitplan* geben Sie an, wann mit der Datensammlung begonnen wird.

Auf der Registerkarte *Stoppbedingung* können Sie Kriterien für Bedingungen angeben, bei denen die Datensammlung angehalten wird. Wenn Sie auf der Registerkarte *Zeitplan* ein Ablaufdatum festgelegt haben, das nach einer auf der Registerkarte *Stoppbedingung* definierten Bedingung liegt, hat die Stoppbedingung Vorrang.

Speicherengpässe beheben

Performanceprobleme können eine Reihe unterschiedlicher Ursachen haben. Ein Problem bei der Performanceanalyse ist, dass die Beseitigung eines Engpasses oft zum nächsten Engpass führt. Dafür gibt es viele Beispiele. Wenn mehr Speicher bereit steht, 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.

Die zweite Regel besagt, dass die Auslagerungsdatei am besten auf einer anderen physischen Festplatte als der Systempartition, die Datenbankdateien und die Transaktionsprotokolle aufgehoben ist.

Auslagerungsdatei und Ressourcenmonitor

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. Falls keine physische Festplatte zur Verfügung steht, ist ein Verschieben nicht sinnvoll, da die Auslagerung auf eine Partition, die auf derselben Platte liegt, keine positiven Auswirkungen hat. Sie sollten die Auslagerungsdatei aber nicht auf Datenträger auslagern, die Datenbanken oder Transaktionsprotokolle benutzen.

In Windows Server 2012 tippen Sie auf der Startseite die Zeichenfolge *erweiterte system* ein, wechseln von *Apps* zu *Einstellungen* und klicken dann auf *Erweiterte Systemeinstellungen anzeigen.*

Auf der Registerkarte *Erweitert* klicken Sie bei *Virtueller Arbeitsspeicher* auf *Ändern*. Sie können an dieser Stelle auch eine feste Größe für die Auslagerungsdatei festlegen sowie die Laufwerke bestimmen, auf denen Auslagerungsdateien zur Verfügung stehen sollen. Klicken Sie auf *Festlegen*, nachdem Sie für das jeweilige Laufwerk die gewünschten Einstellungen vorgenommen haben. Zum Abschluss müssen Sie den Server neu starten.

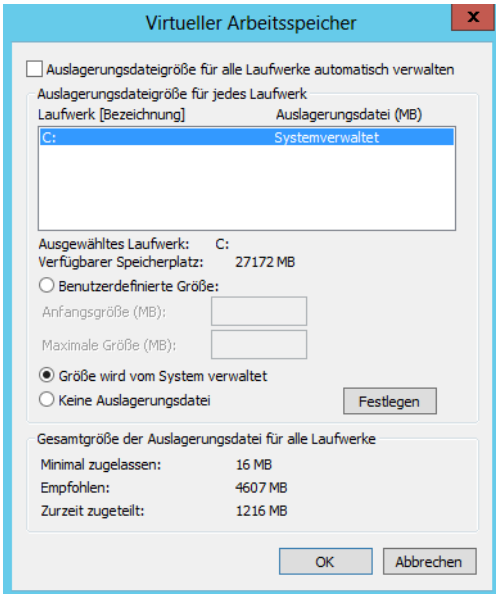
Dies hat den Vorteil, dass diese Datei nicht fragmentiert, da Windows immer auf die komplette Größe zugreifen darf. In der Vergangenheit hat sich etwa eine Größe von »Physischer Arbeitsspeicher * 2,5« als optimal herausgestellt. Sie können in der grafischen Oberfläche aber keine Auslagerungsdatei erstellen, die größer als 2 TB ist. Wenn Sie eine größere Datei verwenden wollen, müssen Sie die Einstellungen in der Eingabeaufforderung vornehmen. Wie Sie dabei vorgehen, zeigen wir Ihnen im nächsten Abschnitt.

Verwenden Sie als Speicherort am besten eine zusätzliche Festplatte und trennen Sie Betriebssystem, Datenbankdateien, Transaktionsprotokolle und die Auslagerungsdatei auf. Deaktivieren Sie dazu das Kontrollkästchen *Auslagerungsdateigröße für alle Laufwerke automatisch verwalten* und deakti-

vieren Sie die Auslagerungsdatei für alle Datenträger, auf die Serverdienste in Windows Server 2012 zugreifen müssen.

Die Auslagerungsdatei speichert Windows in der versteckten Systemdatei *pagefile.sys* im Stammordner des entsprechenden Laufwerks.

Abbildg. 38.12 Anpassen der Auslagerungsdatei



TIPP Sie können die Konfiguration der Auslagerungsdatei auch in der Eingabeaufforderung vornehmen. Dies ist zum Beispiel notwendig, wenn die Datei größer als 2 TB sein soll, oder wenn Sie die Einstellungen skripten möchten. Zum Erstellen einer Auslagerungsdatei führen Sie den folgenden Befehl aus:

```
wmic pagefileset create name="<Laufwerksbuchstabe>:\pagefile.sys"
```

Zum Festlegen der Größe der Auslagerungsdatei verwenden Sie den Befehl:

```
wmic pagefileset where name="<Laufwerksbuchstabe>:\\pagefile.sys" set
InitialSize=<MB>,MaximumSize=<MB>
```

Bitte beachten Sie den doppelten Backslash »\\«!

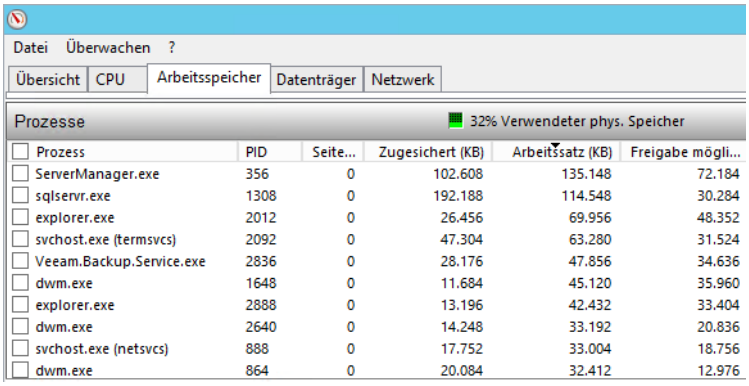
Mit dem folgenden Befehl deaktivieren Sie die Auslagerungsdatei auf einem Laufwerk:

```
wmic pagefileset where name="<Laufwerksbuchstabe>:\\pagefile.sys" delete
```

Haben Sie die Datei bereits gelöscht, erscheint die Meldung *Keine Instanzen verfügbar.* Auf diese Weise überprüfen Sie daher auch, ob auf einem Laufwerk eine Auslagerungsdatei vorhanden ist.

Im Ressourcenmonitor sehen Sie auf der Registerkarte *Arbeitsspeicher* die verschiedenen laufenden Prozesse und deren verbrauchten Arbeitsspeicher. Am schnellsten starten Sie den Ressourcenmonitor durch Eingabe von *perfmon /res* auf der Startseite von Windows Server 2012. Mit einem Klick auf die Spalte *Arbeitssatz* lassen Sie sich den Arbeitsspeicherverbrauch der Prozesse sortiert anzeigen.

Abbildg. 38.13 Überprüfen des Arbeitsspeicherverbrauchs einzelner Prozesse



Prozess	PID	Seite...	Zugesichert (KB)	Arbeitssatz (KB)	Freigabe mögli...
ServerManager.exe	356	0	102.608	135.148	72.184
sqlservr.exe	1308	0	192.188	114.548	30.284
explorer.exe	2012	0	26.456	69.956	48.352
svchost.exe (termsvcs)	2092	0	47.304	63.280	31.524
Veeam.Backup.Service.exe	2836	0	28.176	47.856	34.636
dwm.exe	1648	0	11.684	45.120	35.960
explorer.exe	2888	0	13.196	42.432	33.404
dwm.exe	2640	0	14.248	33.192	20.836
svchost.exe (netsvcs)	888	0	17.752	33.004	18.756
dwm.exe	864	0	20.084	32.412	12.976

Arbeitsspeicher mit der Leistungsüberwachung optimieren und überwachen

Die Überwachung des Arbeitsspeichers übernehmen Sie am besten ebenfalls mit der Leistungsüberwachung. Auf Servern bieten sich folgende Leistungsindikatoren an:

- **Arbeitsspeicher: Verfügbare Bytes** Gibt an, wie viele Bytes an Arbeitsspeicher derzeit für die Verwendung durch Prozesse verfügbar sind. Niedrige Werte können ein Anzeichen dafür sein, dass insgesamt zu wenig Arbeitsspeicher auf dem Server vorhanden ist oder dass eine Anwendung keinen Arbeitsspeicher freigibt.
- **Arbeitsspeicher: Seiten/s** Gibt die Anzahl der Seiten an, die wegen Seitenfehlern vom Datenträger gelesen oder auf den Datenträger geschrieben wurden, um Speicherplatz aufgrund von Seitenfehlern freizugeben. Ein hoher Wert kann auf überhöhte Auslagerungen hindeuten. Überwachen Sie noch *Seitenfehler/s*, um sicherzustellen, dass die Datenträgeraktivität nicht durch Auslagern verursacht wird.

Sinnvoll ist dies zum Beispiel beim Einsatz von SQL Server 2012 oder anderen Server. Wir erläutern die Überwachung und Optimierung nachfolgend am Beispiel des Einsatzes von SQL Server 2012. Der Manager für virtuellen Arbeitsspeicher (VMM) entnimmt Seiten von SQL Server 2012 und anderen Prozessen, um die Größen der Arbeitsspeicherbereiche dieser Prozesse anzupassen. Um festzustellen, ob die überhöhten Auslagerungen von SQL Server 2012 oder einem anderen Prozess verursacht werden, sollten Sie *Seitenfehler/s* der SQL Server-Prozessinstanz überprüfen.

In der Standardkonfiguration werden Arbeitsspeicheranforderungen von SQL Server 2012 auf Basis der verfügbaren Systemressourcen dynamisch geändert. Wenn der SQL-Server mehr Arbeitsspeicher benötigt, wird das Betriebssystem nach der Verfügbarkeit von freiem physischen Arbeitsspeicher abgefragt. Wenn SQL Server 2012 den zugeordneten Arbeitsspeicher nicht benötigt, wird der Arbeitsspeicher für das Betriebssystem freigegeben. Sie können die Option zur dynamischen Verwendung des Arbeitsspeichers jedoch mit den Serverkonfigurationsoptionen *minservermemory* und *maxservermemory* überschreiben.

Die Standardeinstellung für *minservermemory* ist 0, die für *maxservermemory* 2.147.483.647 MB (gleich 2 Petabyte). Wenn sich SQL Server 2012 nach dem Ändern der Optionen nicht starten lässt, müssen Sie den Serverdienst mit der Startoption *–f* starten. Generell ist es empfehlenswert, die dynamische Verwendung des Arbeitsspeichers beizubehalten.

Sie können die Speicheroptionen aber auch manuell festlegen und den Umfang des für SQL Server 2012 zugreifbaren Arbeitsspeichers einschränken. *minservermemory* wird dem SQL-Server nicht gleich beim Start zugeordnet. Wenn der Wert nicht benötigt wird, ruft der SQL-Server ihn auch nicht komplett ab.

Durch Sperren von Seiten im Arbeitsspeicher können Sie die Leistung eines SQL-Servers teilweise auch nach Auslagerung von Arbeitsspeicherdaten auf die Festplatte verbessern. Die SQL Server-Option *Sperren von Seiten im Speicher* wird bei SQL Server 2012 auf *ON* gesetzt, wenn dem Dienstkonto der Instanz das Windows-Benutzerrecht *Lock Pages in Memory (LPIM)* erteilt wurde. Entfernen Sie zum Deaktivieren der Option *Sperren von Seiten im Speicher* für SQL Server 2012 das Benutzerrecht *Lock Pages in Memory* für das SQL Server-Startkonto. In diesem Fall kann der Server selbst die entsprechenden Seiten nicht mehr steuern, sondern das Betriebssystem übernimmt diese Aufgabe:

Erstellen Sie für die Einstellung entweder eine Gruppenrichtlinie, die Sie den SQL-Servern zuweisen, oder nehmen Sie die Einstellungen lokal auf dem Server vor:

1. Geben Sie im Suchfeld des Startmenüs den Befehl *gpedit.msc* ein.

HINWEIS Unter Windows Server 2012 können Sie auf der Startseite direkt mit dem Tippen beginnen oder über ⊞ + R das Dialogfeld *Ausführen* aufrufen.

2. Erweitern Sie *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Zuweisen von Benutzerrechten*.
3. Klicken Sie doppelt auf *Sperren von Seiten im Speicher*.
4. Entfernen Sie das Konto des SQL-Servers in diesem Bereich, wenn es angezeigt wird.

Um die Menge des von SQL Server 2012 speziell verwendeten Arbeitsspeichers zu überwachen, überwachen Sie die folgenden Leistungsindikatoren:

- **Prozess: Arbeitsseiten** Gibt die Menge an Arbeitsspeicher an, die ein Prozess verwendet. Wenn dieser Wert konstant unter der Menge an Arbeitsspeicher liegt, die in den Serveroptionen in den Eigenschaften des SQL-Servers festgelegt sind, haben Sie den SQL-Server so konfiguriert, dass er zu viel Arbeitsspeicher beansprucht.
- **SQLServer:Buffer-Manager: Buffer cache hit ratio** Eine Rate von 90% oder höher ist hier empfohlen. Erhöhen Sie so lange Arbeitsspeicher, bis der Wert konstant über 90% liegt. Ein Wert von über 90% bedeutet, dass mehr als 90% aller Datenanforderungen vom Datencache erfüllt wurden. Aktivieren Sie zur besseren Übersicht in der Windows-Leistungsüberwachung die Ansicht *Bericht*.

Karte des Arbeitsspeichers – RAMMap und VMMap

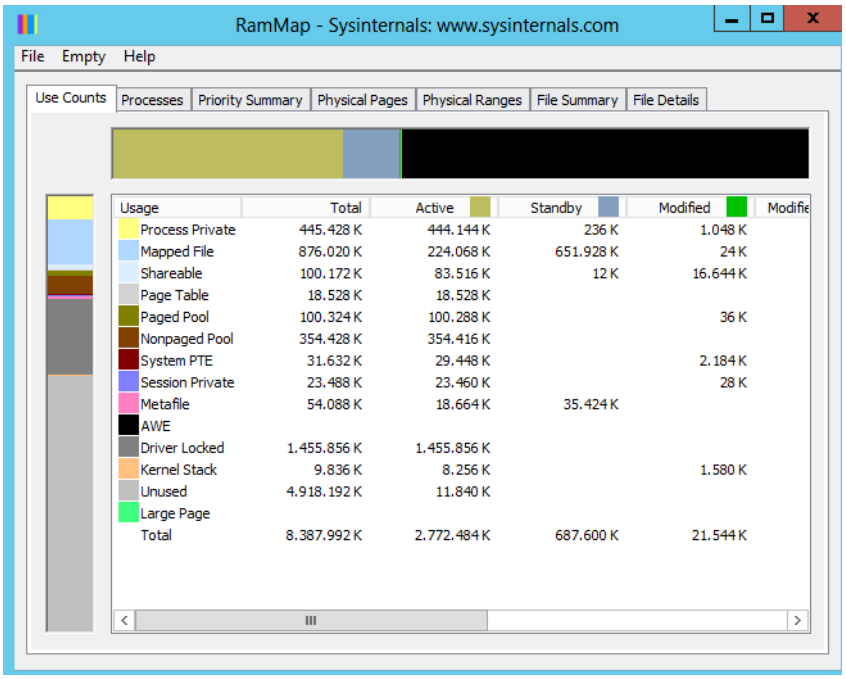
Für die Fehleranalyse oder Leistungsmessung eines Computers kann es sinnvoll sein, die aktuelle Auslastung des Arbeitsspeichers zu kennen. Das Sysinternals-Tool RAMMap (*http://technet.microsoft.com/de-de/sysinternals/ff700229* [Ms179-K38-11]) zeigt die aktuelle Zuteilung des Arbeitsspeichers in einer grafischen Oberfläche an.

Mit dem Tool erkennen Sie, wie viel Arbeitsspeicher aktuell für den Kernel reserviert sind und welchen Arbeitsspeicher die Treiber des Computers verbrauchen. Auf verschiedenen Registerkarten zeigt das Tool ausführliche Informationen zum Arbeitsspeicher an:

- **Use Counts** Zusammenfassung
- **Processes** Prozesse
- **Priority Summary** Priorisierte Standbylisten
- **Physical Pages** Seitenübersicht für den kompletten Arbeitsspeicher
- **Physical Ranges** Adressen zum Arbeitsspeicher
- **File Summary** Dateien im Arbeitsspeicher
- **File Details** Individuelle Seiten im Arbeitsspeicher nach Dateien sortiert

Das Tool hilft vor allem Technikern und Entwicklern dabei, zu verstehen, wie die aktuellen Windows-Versionen den Arbeitsspeicher verwalten und an die verschiedenen Anwendungen, Treiber und Prozesse verteilt.

Abbildg. 38.14 Anzeige der Arbeitsspeicherverteilung in Windows Server 2012



Noch ausführlicher bezüglich der Arbeitsspeicheranalyse ist VMMAP (*http://technet.microsoft.com/en-us/sysinternals/dd535533* [Ms179-K38-12]). Das Tool zeigt sehr detailliert den Arbeitsspeicherverbrauch von Prozessen an. Durch die ausführlichen Filtermöglichkeiten geht VMMap bei der Analyse also wesentlich weiter als RAMMap. Beide Tools sind nicht nur für Administratoren geeignet, sondern auch für Entwickler oder Techniker, die genau das Aufteilen der Ressourcen verstehen wollen.

VMMap hat die Möglichkeit, auch anzuzeigen, ob ein Prozess Arbeitsspeicher durch den physischen Arbeitsspeicher zugewiesen bekommt oder durch Windows in die Auslagerungsdatei ausgelagert wird. VMMap listet sehr detailliert auf, welche Daten eines Programms oder eines Prozesses in welchen Bereichen des Arbeitsspeichers oder der Auslagerungsdatei liegen. Das Tool ermöglicht auch das Erstellen von Momentaufnahmen und dadurch von Vorher-Nachher-Beobachtungen.

Durch die ausführlichen Analysemöglichkeiten kann das Tool in der grafischen Oberfläche genau anzeigen, wie viel Arbeitsspeicher einzelne Funktionen in einem Prozess benötigen. Über den Menübefehl *View/String* lässt sich anzeigen, welche Daten ein einzelner Speicherbereich enthält. Gescannte Ergebnisse lassen sich über das Menü *File* abspeichern.

Neben dem Standardformat von VMMap (*.mmp*), lassen sich die Daten auch im *.txt*-Format sowie als *.csv*-Datei abspeichern. Mit diesen Möglichkeiten können Sie also auch Analysen mit Excel durchführen. Im Gegensatz zu RAMMap können Sie VMMap aber auch unter Windows 2000, XP und Windows Server 2003 nutzen.

Diagnose des Arbeitsspeichers

Häufig sind die Probleme auf einem Server auf defekten Arbeitsspeicher zurückzuführen. In Windows Server 2012 wurde daher ein spezielles Diagnoseprogramm integriert, welches den Arbeitsspeicher ausführlich auf Fehler überprüft. Sie können das Tool über *mdsched* aufrufen. Das Tool steht auch in der Programmgruppe *Verwaltung* zur Verfügung und – wenn Sie den Server mit der DVD starten – über die *Computerreparaturoptionen*.

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.

Nachdem der Test abgeschlossen ist, startet der Server automatisch neu und meldet das Ergebnis über ein Symbol im Infobereich der Taskleiste. Über die Funktionstaste F1 gelangen Sie zu den Optionen der Überwachung und können verschiedene Überprüfungsmethoden auswählen und mit F10 starten. Ist der Test beendet, startet der Server automatisch wieder. Sie müssen daher nicht warten, bis der Test abgeschlossen ist, damit der Server wieder zur Verfügung steht.

Auf der Ultimate Boot CD (*http://www.ultimatebootcd.com* [Ms179-K38-13]) befinden sich übrigens im Bereich *Memory* ebenfalls einige Testtools für den Arbeitsspeicher.

Prozessorauslastung messen und optimieren

Auch die Prozessorleistung kann einen 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 gelegentlich 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 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. Ergänzend ist aber auch hier der Leistungsindikator *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.

Eine konstant hohe CPU-Nutzungsrate macht deutlich, dass der Prozessor eines Servers überlastet ist. Überwachen Sie in der Leistungsüberwachung von Windows Server 2012 den Leistungsindikator *Prozessor: Prozessorzeit (%)*. Dieser Leistungsindikator überwacht die Zeit, welche die CPU zur Verarbeitung eines Threads benötigt, der sich nicht im Leerlauf befindet. Ein konstanter Status von 80 bis 90 % ist zuviel. Bei Multiprozessorsystemen sollten Sie für jeden Prozessor eine eigene Instanz dieses Leistungsindikators überwachen. Dieser Wert stellt die Summe der Prozessorzeit für einen bestimmten Prozessor dar.

Zusätzlich können Sie die Prozessornutzung aber auch über *Prozessor: Privilegierte Zeit (%)* überwachen. Dieser gibt den prozentualen Zeitanteil an der Gesamtzeit an, die der Prozessor benötigt, um Windows-Kernelbefehle, wie die Verarbeitung von E/A-Anforderungen von SQL Server 2012, auszuführen. Sollte dieser Leistungsindikator bei hohen Werten für die Leistungsindikatoren *Physischer Datenträger* dauerhaft hoch sein, sollten Sie die Installation eines schnelleren oder effizienteren Datenträgers planen.

- **Prozessor: Benutzerzeit (%)** Gibt den prozentualen Zeitanteil an der Gesamtzeit an, die der Prozessor benötigt, um Benutzerprozesse wie des SQL-Server auszuführen
- **System: Prozessor-Warteschlangenlänge** Zählt die Threads, die auf Prozessorzeit warten. Ein Prozessorengpass entsteht, wenn die Threads eines Prozesses mehr Prozessorzyklen benötigen, als zur Verfügung stehen. Wenn viele Prozesse versuchen, Prozessorzeit zu beanspruchen, sollten Sie einen schnelleren Prozessor installieren.

Der Task-Manager als Analysewerkzeug

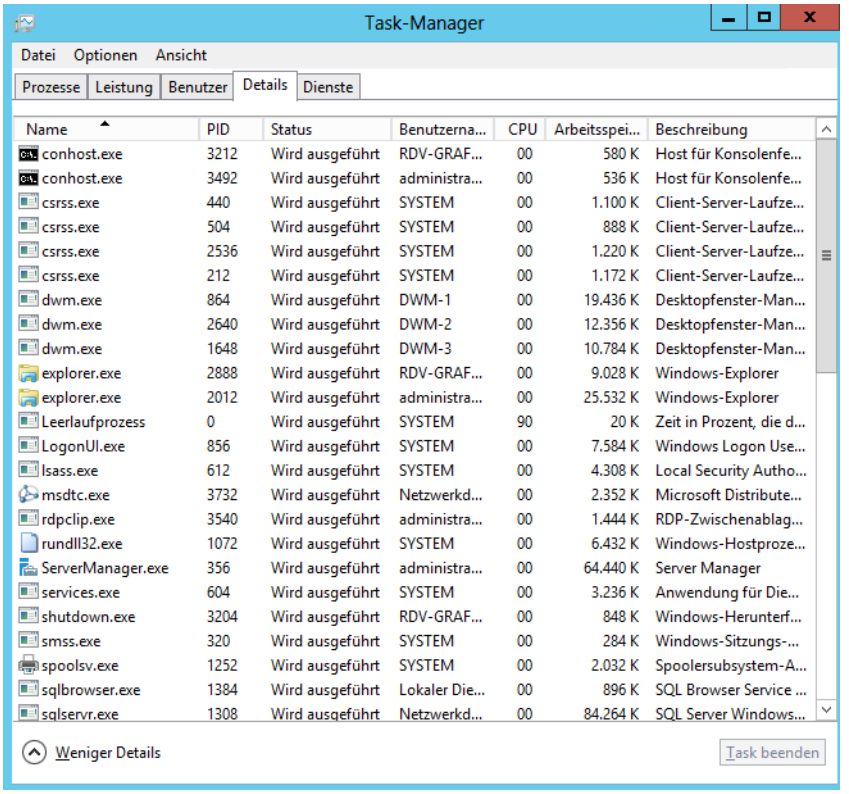
Ein weiteres wichtiges Werkzeug für die Analyse der Performance ist der Windows Task-Manager. Dieser zeichnet sich dadurch aus, dass er mit sehr wenig Aufwand genutzt werden kann. Sie können den Task-Manager durch einen Klick mit der rechten Maus auf die Taskleiste über dessen Kontextmenü aufrufen.

Alternativ können Sie den Task-Manager auch über das Menü aufrufen, das mit der Tastenkombination Strg+Alt+Entf erscheint, oder über *taskmgr* auf der Startseite. Direkt lässt sich der Task-Manager über die Tastenkombination Strg+⇧+Esc starten.

- **Prozesse** Gibt 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.

- **Leistung** Gibt einen schnellen Überblick zum aktuellen Leistungsverbrauch des Computers. Dahinter verbirgt sich ein kleiner Systemmonitor, der die wichtigsten Informationen zur Systemauslastung in grafischer Form zur Verfügung stellt. 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.
- **Benutzer** Liefert Informationen über die aktuell gestarteten Programme der angemeldeten Benutzer auf dem Computer
- **Details** 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. Mehr zu den Diensten sehen Sie auf der Registerkarte *Dienste*. 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 überwachen muss. Auch hier können Prozesse über die entsprechende Schaltfläche wieder beendet werden. Sie sollten damit allerdings sehr vorsichtig sein, da das Beenden eines Diensts dazu führen kann, dass Ihr System nicht mehr korrekt ausgeführt wird.
- **Dienste** Zeigt Informationen zu den Systemdiensten an

Abbildg. 38.15 Systemüberwachung von Windows Server 2012 mit dem Task-Manager



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.

Laufwerke und Datenträger überwachen – Leistungsüberwachung und Zusatztools

Der folgende Abschnitt geht auf Tools ein, mit denen Sie Datenträger und Laufwerke in Windows Server 2012 optimal überwachen können. Auf diesem Weg können Sie eventuellen Problemen mit den Servern vorgreifen. Sie können aber auch mit der Windows-Leistungsüberwachung, die wir in diesem Kapitel an den verschiedenen Stellen behandelt haben, ebenfalls die Datenträger im System überwachen.

SQL Server 2012 verwendet zum Beispiel Aufrufe für die Windows-Betriebssystemeingabe/-ausgabe, um Lese- und Schreibvorgänge auf dem Datenträger auszuführen. SQL Server 2012 verwaltet zwar, wann und wie Datenträger-E/A ausgeführt werden, aber das Betriebssystem führt E/A-Vorgänge aus. Das E/A-Teilsystem umfasst Systembus, Datenträgercontroller, Datenträger, CD/DVD-ROM-Laufwerk und zahlreiche andere E/A-Geräte. Datenträger-E/A ist häufig die Ursache von Engpässen in einem System, vor allem beim Einsatz von SQL-Servern.

Die folgenden zwei Leistungsindikatoren können überwacht werden, um die Datenträgeraktivität zu bestimmen:

- **Physikalischer Datenträger: Zeit (%)** Prozentsatz der Zeit, den der Datenträger für Lese-/Schreibaktivitäten benötigt. Wenn der Leistungsindikator einen hohen Wert besitzt, überprüfen Sie noch *Physikalischer Datenträger:Aktuelle Warteschlangenlänge*, um festzustellen, wie viele Anforderungen auf einen Datenträgerzugriff warten. Die Anzahl der wartenden E/A-Anforderungen sollte das Anderthalbfache bis Zweifache der Anzahl der Spindeln, aus denen sich der physische Datenträger zusammensetzt, nicht überschreiten. Wenn *Aktuelle Warteschlangenlänge* und *Zeit (%)* durchgängig sehr hoch sind, müssen Sie den Datenträger entlasten, weitere Datenträger einsetzen und die verschiedenen Datenbankdateien aufteilen, oder einen weiteren Server hinzufügen (siehe Kapitel 4).
- **Physikalischer Datenträger: Durchschnittliche Warteschlangenlänge des Datenträgers** Überwachen Sie den *Arbeitsspeicher:Seitenfehler/s*, um sicherzustellen, dass die Datenträgeraktivität nicht durch Auslagern verursacht wird. In diesem Fall liegt das Problem nicht am Datenträger, sondern an fehlendem Arbeitsspeicher.

Wenn Sie über mehr als eine logische Partition auf derselben Festplatte verfügen, sollten Sie statt den Leistungsindikatoren für physische Arbeitsspeicher die Leistungsindikatoren für logische Datenträger verwenden. Haben Sie die Datenträger mit hoher Lese-/Schreibaktivität festgestellt, können Sie zum Beispiel mit *Logischer Datenträger:Bytes geschrieben/s* den Fehler weiter eingrenzen.

Sie können zusätzlich die folgenden zwei Leistungsindikatoren überwachen, um den durch SQL Server-Komponenten erstellten E/A-Umfang zu ermitteln:

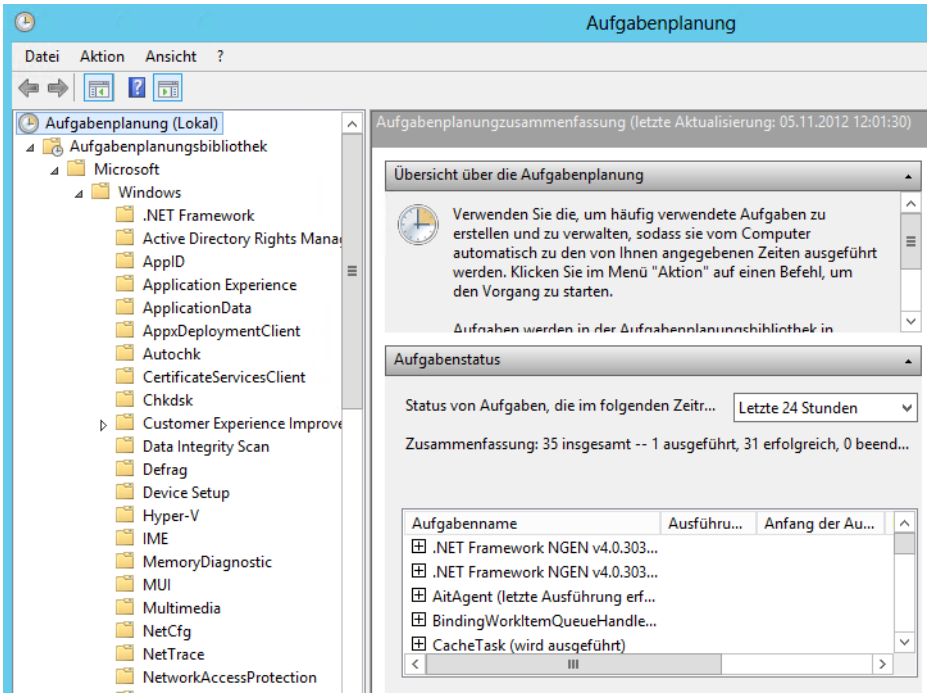
- *SQLServer:Buffer Manager:Page reads/sec*
- *SQLServer:Buffer Manager:Page writes/sec*

Sie können auch den Datenbankoptimierungsratgeber (DTA) im SQL Server Management Studio oder über die Eingabeaufforderung verwenden, um typische SQL Server-Arbeitsauslastungen zu analysieren.

Aufgabenplanung

Die Aufgabenplanung wird durch einen eigenen Menüpunkt in der Computerverwaltung konfiguriert. Sie können die Aufgabenplanung auch über *Systemsteuerung/System und Sicherheit/Verwaltung/Aufgabenplanung* oder über die Startseite durch Eintippen von *taskschd.msc* aufrufen. In Kapitel 35 sind wir bereits auf Möglichkeiten der Aufgabenplanung eingegangen.

Abbildg. 38.16 Aufgabenplanung in Windows Server 2012



Aufgabenplanung verstehen

Das Hauptfenster in der Mitte der Aufgabenplanung ist in drei Bereiche untergliedert. Sie können die einzelnen Menüs ausblenden, wenn Sie mit der Maus auf den kleinen Pfeil am Ende des Balkens klicken. Klicken Sie auf den obersten Punkt Aufgabenplanung, ändert sich der Inhalt des mittleren Fensters:

- **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 2012 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 per Doppelklick auf die einzelnen Aufgaben deren Konfiguration überprüfen und abändern. Sie sehen hier auch einige Systemaufgaben. 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 ein *Task*. Ein solcher Task besteht aus verschiedenen Startbedingungen, einschließlich Triggern, Bedingungen und Einstellungen sowie eine oder mehrere Aktionen genannte Ausführungsvorgänge:

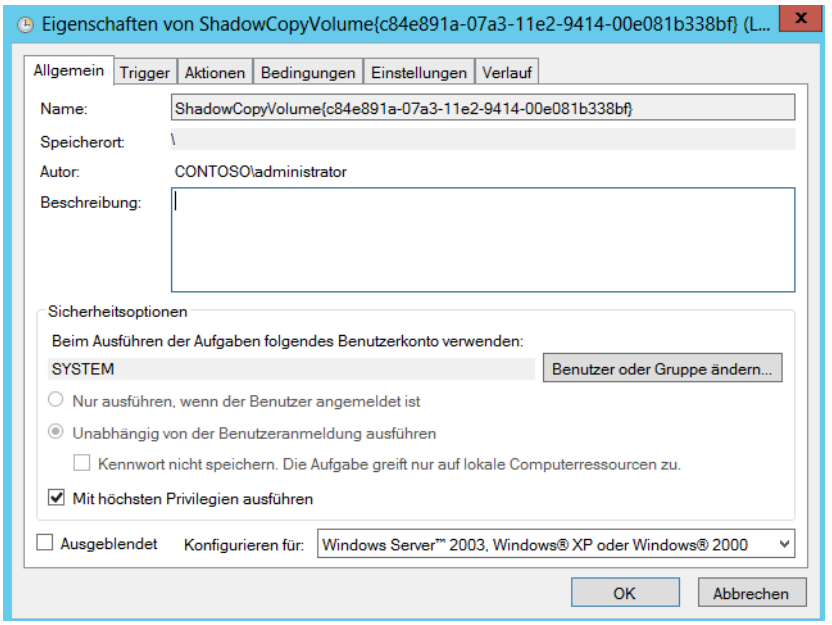
- **Trigger** Sind Kriteriensätze, bei deren Erfüllung ein Task ausgeführt wird. Sie können zeit- oder ereignisabhängig sein, und es können Parameter wie Startzeitpunkte und Wiederholungskriterien angegeben werden.
- **Bedingungen** Schränken Tasks so ein, dass sie nur ausgeführt werden, wenn sich der Computer in einem bestimmten Zustand befindet. Ein Task wird nur ausgeführt, wenn ein Trigger erfüllt ist und alle für den Task 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.
- **Einstellungen** Legen die Ausführungsoptionen fest. 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.

Wenn Sie eine Aufgabe aufgerufen haben, sehen Sie auf der rechten Seite der Managementkonsole, welche speziellen Aufgaben Sie durchführen können. Sie können zum Beispiel eine Aufgabe exportieren, um diese auf einem anderen Rechner zu importieren. Sie können Aufgaben deaktivieren, löschen oder sofort starten lassen.

In Windows Server 2012 können Sie Tasks, die abhängig vom Auftreten von Ereignissen gestartet werden sollen, sehr einfach mit dem Taskplaner-Assistent einrichten. Ein Administrator kann in der Ereignisanzeige einfach das als Trigger zu verwendende Ereignis auswählen und mit nur einem Klick den Taskplaner-Assistenten starten, um den Task einzurichten.

Durch die nahtlose Integration der Taskplaner-Benutzeroberfläche in die Ereignisanzeige können Sie einen durch ein Ereignis ausgelösten Task mit wenigen Mausklicks erstellen. Klicken Sie das Ereignis mit der rechten Maustaste an und wählen Sie die Option *Aufgabe an dieses Ereignis anfügen*. Mehr zu diesem Thema lesen Sie in Kapitel 35.

Abbildg. 38.17 Aufgaben verwalten



Über Ereignisse hinaus unterstützt der Taskplaner von Windows Server 2012 auch weitere Triggertypen, beispielsweise Trigger, die Tasks starten, wenn der Computer startet, sich ein Benutzer anmeldet oder sich der Computer im Leerlauf befindet. Mithilfe weiterer zusätzlicher Trigger können Administratoren Tasks einrichten, die abhängig vom Sitzungsstatus gestartet werden, z.B. beim Herstellen oder Trennen einer Verbindung mit einem Terminalcomputer oder beim Sperren und Entsperren einer Arbeitsstation. Mit dem Taskplaner können Sie Tasks weiterhin abhängig von Datum und Uhrzeit auslösen.

Im Taskplaner lassen sich Trigger genauer anpassen und so detailliert festlegen, wann Tasks gestartet und wie häufig sie ausgeführt werden sollen. Ein Administrator kann einem Trigger eine Verzögerung hinzufügen oder einen Task einrichten, der nach dem Auftreten des Triggers in regelmäßigen Intervallen wiederholt wird.

Für jeden Task lassen sich mehrere Bedingungen definieren. Durch Bedingungen können Sie Tasks so einschränken, dass diese nur ausgeführt werden, wenn sich der Computer in einem bestimmten Zustand befindet. Beispielsweise können Sie mit dem Taskplaner erreichen, dass ein Programm beim Eintreten eines Ereignisses nur gestartet wird, wenn das Netzwerk verfügbar ist, dass eine Aktion zu einem bestimmten Zeitpunkt nur gestartet wird, wenn der Computer im Leerlauf ist, oder dass eine Aktion beim Anmelden nur gestartet wird, wenn sich der Computer nicht im Akkubetrieb befindet.

In Windows Server 2012 können mit einem bestimmten Task mehrere Trigger verbunden werden. Beispielsweise gilt eine bestimmte Fehlerbedingung möglicherweise nur beim Auftreten von drei verschiedenen Ereignissen als erfüllt. Ein Administrator kann einfach einen Task definieren, der nur gestartet wird, wenn alle drei Ereignisse auftreten. Für Tasks können nicht nur mehrere Trigger erforderlich sein, mit einem einzelnen Task können auch mehrere Aktionen gestartet werden.

Mit dem Taskplaner müssen Sie beim aufeinander folgenden Ausführen von Tasks keine Vermutungen mehr anstellen. Ein Administrator muss 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 Tasks erforderlich: ein um 1:00 Uhr gestarteter Task zum Ausführen der Batchdatei und ein zweiter Task zum Drucken der Ergebnisse. Sie mussten die Dauer zur Ausführung des Batchprozesses schätzen und den Drucktask so einrichten, dass er 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 2012 ist dieses Szenario einfach zu verwalten. Ein einzelner Task kann definiert werden, mit dem der Batchprozess um 1:00 Uhr ausgeführt wird und nach dessen Abschluss die Ergebnisse gedruckt werden.

Der Taskplaner stellt die Ausführung von Tasks auch dann sicher, wenn sich ein Computer zum geplanten Zeitpunkt im Standbymodus befindet. Durch diese Funktionalität, durch die der Taskplaner einen Computer zum Ausführen eines Tasks aus dem Standbymodus oder Ruhezustand reaktivieren kann, können Sie die Vorteile der verbesserten Stromsparmodi von Windows Server 2012 nutzen, ohne darauf achten zu müssen, ob wichtige Tasks pünktlich ausgeführt werden.

Neben dem Reaktivieren eines Computers zum Ausführen eines Tasks können Sie nun durch eine Option festlegen, dass ein Task ausgeführt wird, sobald der Computer verfügbar ist. Wenn Sie diese Option aktivieren und der geplante Ausführungszeitpunkt eines Tasks nicht eingehalten wurde, wird der Task beim nächsten Einschalten des Computers vom Taskplaner ausgeführt.

Für Administratoren, die statt mit der grafischen Oberfläche bevorzugt mit der Eingabeaufforderung arbeiten, wurde das Befehlszeilentool Schtasks so erweitert, dass es auch die in Windows Server 2012 neu hinzugekommenen Funktionen umfasst.

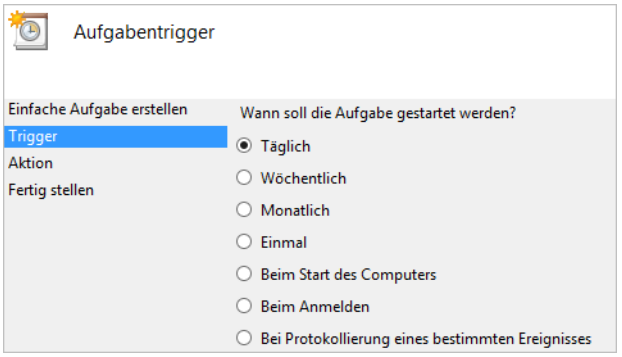
Erstellen einer neuen Aufgabe

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** Mithilfe dieser Aktion wird ein Assistent gestartet, der Sie bei der Erstellung einer neuen Aufgabe unterstützt
- **Aufgabe erstellen** Wenn Sie diese Aktion auswählen, 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 PC oder einem anderen Computer exportiert haben

Wenn Sie den Assistenten zum Erstellen einfacher Aufgaben starten, können Sie zunächst die Bezeichnung der Aufgaben sowie deren Beschreibung festlegen. Auf der nächsten Seite des Assistenten bestimmen Sie, wann diese Aufgabe durchgeführt werden soll.

Abbildg. 38.18 Festlegen des Aufgabentriggers



Abhängig von der Auswahl des Aufgabentriggers können Sie die Ausführung der Aufgabe auf dem nächsten Fenster detailliert spezifizieren. Haben Sie beispielsweise die tägliche Ausführung einer Aufgabe definiert, können Sie auf der nächsten Seite festlegen, zu welcher Uhrzeit die Aufgabe durchgeführt werden soll.

Als Nächstes legen Sie fest, welche Aktion diese Aufgabe durchführen soll. Sie können entweder ein Programm starten, was die häufigste Aufgabe ist, aber auch eine E-Mail schicken oder eine Meldung anzeigen lassen. Als ausführbares Programm können Sie zum Beispiel auch eine Batchdatei starten lassen.

Auf der nächsten Seite des Assistenten wird Ihnen nochmals eine Zusammenfassung angezeigt. Sie können sich nach der Fertigstellung die Eigenschaften der Aufgabe anzeigen lassen und alle Werte anpassen, wenn Sie nachträglich Änderungen vornehmen wollen.

Nachdem Sie die Aufgabe erstellt haben, wird diese bei den aktiven Aufgaben angezeigt. Sie können auf eine dieser Aufgaben doppelklicken, um das zugehörige Konfigurationsfenster zu öffnen. Hier lässt sich die Aufgabe konfigurieren oder sofort starten. An dieser Stelle können Aufgaben auch gelöscht oder lediglich deaktiviert werden.

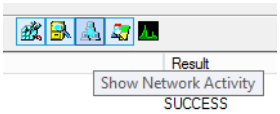
Prozesse und Dienste überwachen

Der folgende Abschnitt geht vor allem auf Tools ein, mit denen Sie die laufenden Prozesse auf dem Computer überwachen und anzeigen lassen können. Insbesondere bei der Systemdiagnose sind die folgenden Tools nützlich.

Dateisystem, Registry und Prozesse überwachen – Sysinternals Process Monitor

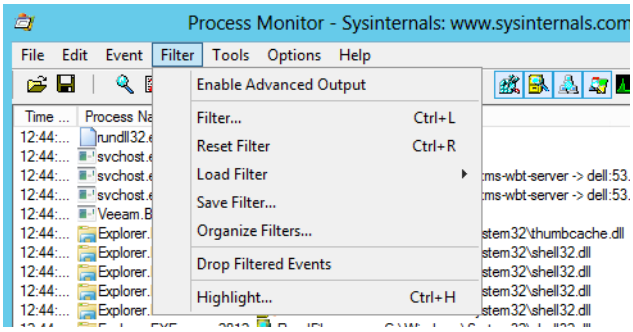
Mit dem Sysinternals-Tool Process Monitor (*http://technet.microsoft.com/de-de/sysinternals/bb896645* [Ms179-K38-14]) können Sie in einer grafischen Oberfläche ausführlich und in Echtzeit alle Aktivitäten im Dateisystem, der Registry und der Prozesse/Threads überwachen und farblich markieren. Über Schaltflächen aktivieren Sie die einzelnen Überwachungsfunktionen durch einen Klick oder schalten diese wieder aus.

Abbildg. 38.19 Aktivieren und Deaktivieren verschiedener Überwachungsmöglichkeiten im Process Monitor



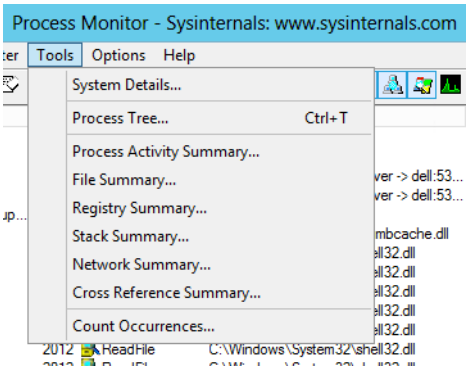
Auch der Aufbau von TCP/IP-Verbindungen und den UDP-Verkehr, also den Netzwerkverkehr des Servers, lassen sich überwachen. Allerdings speichert der Process Monitor nicht den Inhalt der TCP-Pakete, sodass sich keine Daten auslesen lassen, sondern nur die reine Funktionalität des Netzwerks. Auf Wunsch kann Process Monitor mehr Informationen zu laufenden Prozessen anzeigen, zum Beispiel die zum Prozess gehörenden DLL-Dateien. Sie können Filtern die Anzeige anpassen und unnötige Informationen ausblenden oder den Fokus auf spezielle Daten legen.

Abbildg. 38.20 Verwenden von Filtern für Process Monitor



Im Menü *Tools* stehen verschiedene Ansichten zur Verfügung. Das Tool kann auch den Bootvorgang von Servern überwachen, da es sehr früh startet. Alle Ergebnisse lassen sich dabei in eine Datei umleiten. Kann Windows nicht starten, lässt sich durch Analyse dieser Datei der Fehler schnell finden.

Abbildg. 38.21 Anpassen der Ansichten im Process Monitor

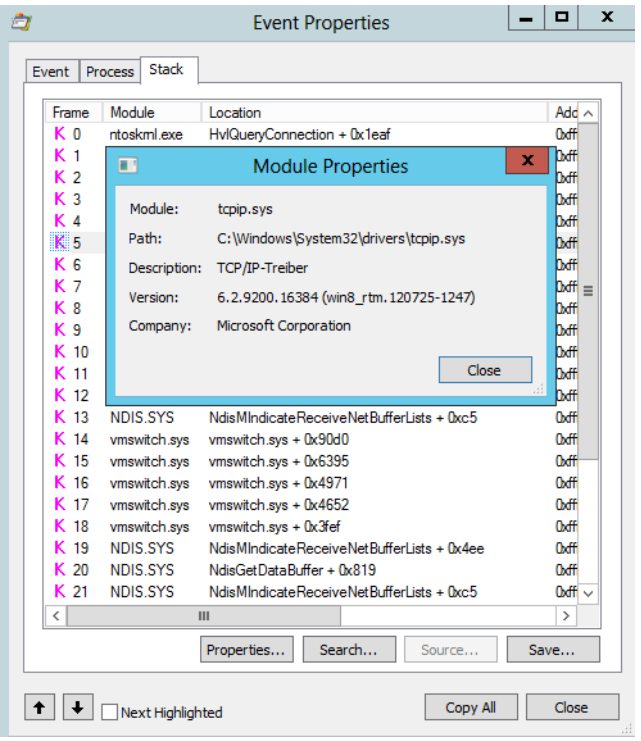


Haben Sie die Anzeige angepasst, besteht die Möglichkeit, die Daten über das Menü *File* zu speichern. Auf einem anderen Rechner können Sie die Ausgabe jederzeit über das aktuelle Fenster wieder laden und Filter setzen sowie das Ergebnis durchsuchen.

Neben der Möglichkeit, die aktuelle Ausgabe zu speichern, lassen sich über *File/Export Configuration* die Einstellungen des Tools exportieren. Die Einstellung können Sie dann auf einem anderen Rechner wieder importieren, um diese nicht neu vornehmen zu müssen. Im Menü steht dazu auch der *Import*-Befehl zur Verfügung.

Klicken Sie doppelt auf einen Eintrag, öffnet sich ein Fenster mit weiteren Informationen, die sehr detailliert die Arbeit des Prozesses und die dabei verwendeten Dateien beschreiben. Klicken Sie im Informationsfenster auf der Registerkarte *Process* oder *Stack* wiederum auf eine der beteiligten Dateien des Prozesses, können Sie von dieser Datei Informationen anzeigen lassen, zum Beispiel die Version und Speicherort.

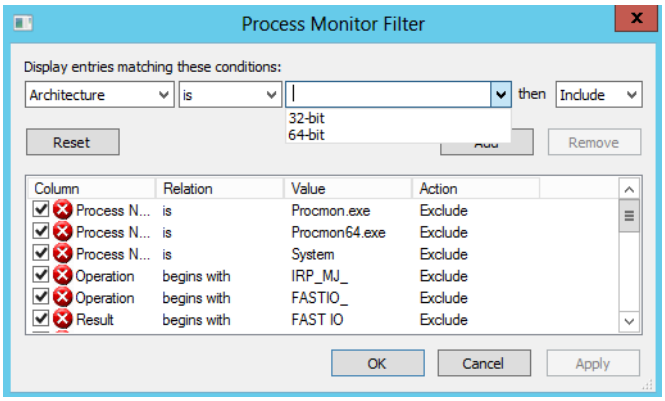
Abbildg. 38.22 Anzeigen weiterer Informationen zu Prozessen und beteiligten Dateien



Die Details eines Prozesses können Sie ebenfalls als *.csv*-Datei abspeichern, um diese später weiter zu analysieren. Wie bei *Autoruns* von Sysinternals haben Sie auch im Process Monitor die Möglichkeit, über das Kontextmenü eine Onlinesuche zum ausgewählten Prozess durchzuführen. Über das Kontextmenü können Sie einen Prozess und dessen Ausgabe auch farblich hervorheben.

Über das Kontextmenü eines Prozesses können Sie alle überwachten Vorgänge, die vor dem Prozess stattgefunden haben, ausblenden lassen, indem Sie die Option *Exclude Events Before* auswählen. Weitere Möglichkeiten im Kontextmenü sind das Einblenden nur eines einzelnen Prozesses und der Vorgänge, die dieser durchführt. Filter erstellen Sie über den Menübefehl *Filter/Filter*. Erstellen Sie komplexe Filter, können Sie diese über den Menübefehl *Filter/Save Filter* auch abspeichern und über den Menübefehl *Filter/Load Filter* jederzeit erneut aufrufen.

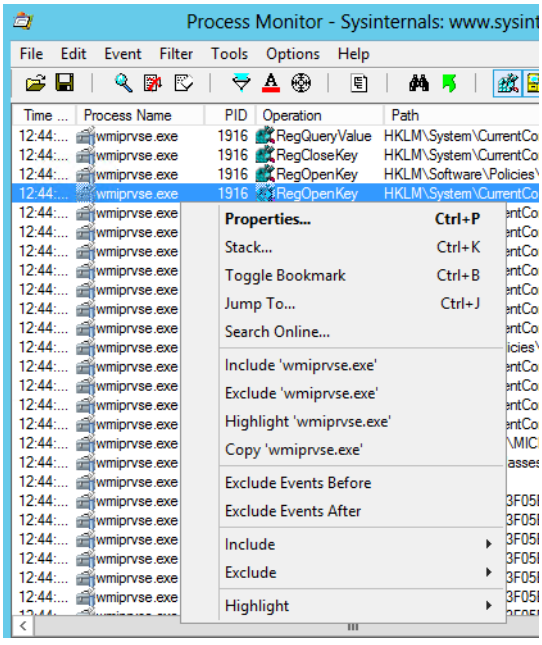
Abbildg. 38.23 Erstellen von Filtern im Process Monitor



Wollen Sie zum Beispiel nach dem Prozess filtern, der ein bestimmtes Fenster auf dem Desktop geöffnet hat, oder ein gestartetes Programm, ziehen Sie das Fadenkreuzsymbol in der Symbolleiste des Process Monitor mit der Maus auf das Fenster, dessen Prozess Sie anzeigen wollen. Anschließend erstellt Process Monitor automatisch einen Filter.

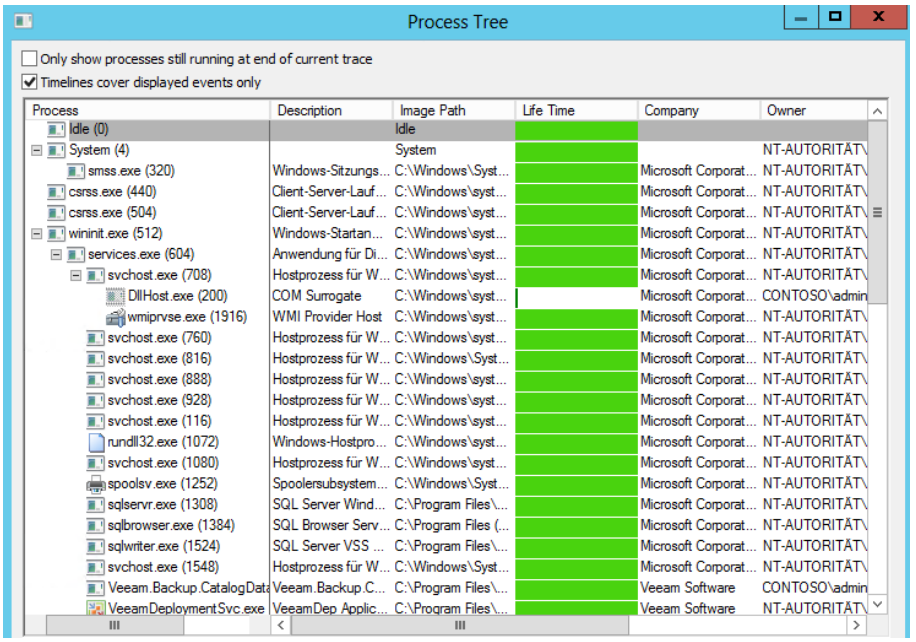
Wollen Sie den Speicherort einer Datei anzeigen oder im Registrierungs-Editor direkt zum ausgewählten Schlüssel wechseln, klicken Sie im Process Monitor den entsprechenden Eintrag mit der rechten Maustaste an und wählen im Kontextmenü den Eintrag *Jump To*.

Abbildg. 38.24 Durchführen verschiedener Aktionen über das Kontextmenü



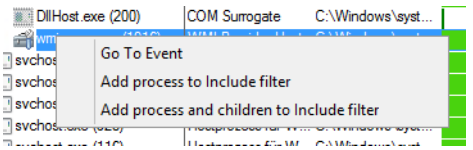
Mit der Tastenkombination Strg + T rufen Sie den Process Tree auf. Hier erhalten Sie eine ähnliche Ansicht wie mit dem Process Explorer und sehen gestartete Prozesse sowie deren Abhängigkeiten. Auch hier zeigt Process Monitor – falls möglich – das Symbol der Anwendung des Prozesses an.

Abbildg. 38.25 Aufrufen des Process Tree im Process Monitor



Klicken Sie im Process Tree mit der rechten Maustaste auf einen Tracevorgang, können Sie über das Kontextmenü und der Auswahl von *Go To Event* in Process Monitor zum aktuellen Vorgang springen, den der Prozess ausführt und den Process Monitor überwacht.

Abbildg. 38.26 Springen zum aktuellen Vorgang eines Prozesses

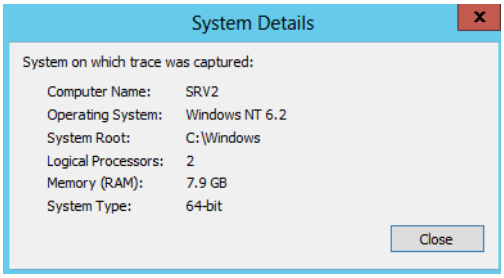


Wenn Sie Probleme mit einem Server und einem Computer haben und dabei Hilfe benötigen, ist oft ein gespeicherter Tracevorgang von Process Monitor notwendig. Dazu starten Sie Process Monitor, erstellen Filter oder arbeiten mit dem Standardfilter und speichern dann den Tracevorgang mit *File/Save* ab. Anschließend erscheint ein Fenster, in dem Sie auswählen können, welches Format Sie beim Speichern verwenden und welche Events der Speichervorgang enthalten soll.

Gespeicherte Tracevorgänge können Sie mit *File/Open* wieder öffnen und bearbeiten. Wenn Sie auf einem 32-Bit-System einen Tracevorgang speichern und auf einem 64-Bit-System öffnen wollen, müssen Sie Process Monitor (*Procmon.exe*) über die Eingabeaufforderung mit der Option */run32* starten.

Process Monitor speichert in der Datei nicht nur die Daten des Tracevorgangs, sondern auch den Namen des Computers, das Betriebssystem, die Anzahl der Prozessoren und den Arbeitsspeicher sowie den Systemtyp (32-Bit oder 64-Bit). Öffnen Sie einen gespeicherten Vorgang, können Sie diese Informationen über *Tools/System Details* öffnen.

Abbildg. 38.27 Anzeigen von Systemdetails eines Systems



Neben der Überwachung eines laufenden Systems können Sie Process Monitor so konfigurieren, dass das Tool den Bootvorgang überwachen kann. Um einen solchen Vorgang auszuführen, wählen Sie im Menü *Options* den Befehl *Enable Boot Logging*.

Bei diesem Vorgang erstellt das Tool einen Treiber, der mit dem Systemstart gestartet wird. Dieser protokolliert alle Startvorgänge von Prozessen und Dienste, die vor der Benutzeranmeldung starten und speichert die Daten im *Windows*-Ordner in der Datei *procmon.pmb*. Starten Sie Process Monitor das nächste Mal, erkennt das Tool, dass eine Protokollierung des Bootvorgangs stattgefunden hat und öffnet die entsprechende Datei.

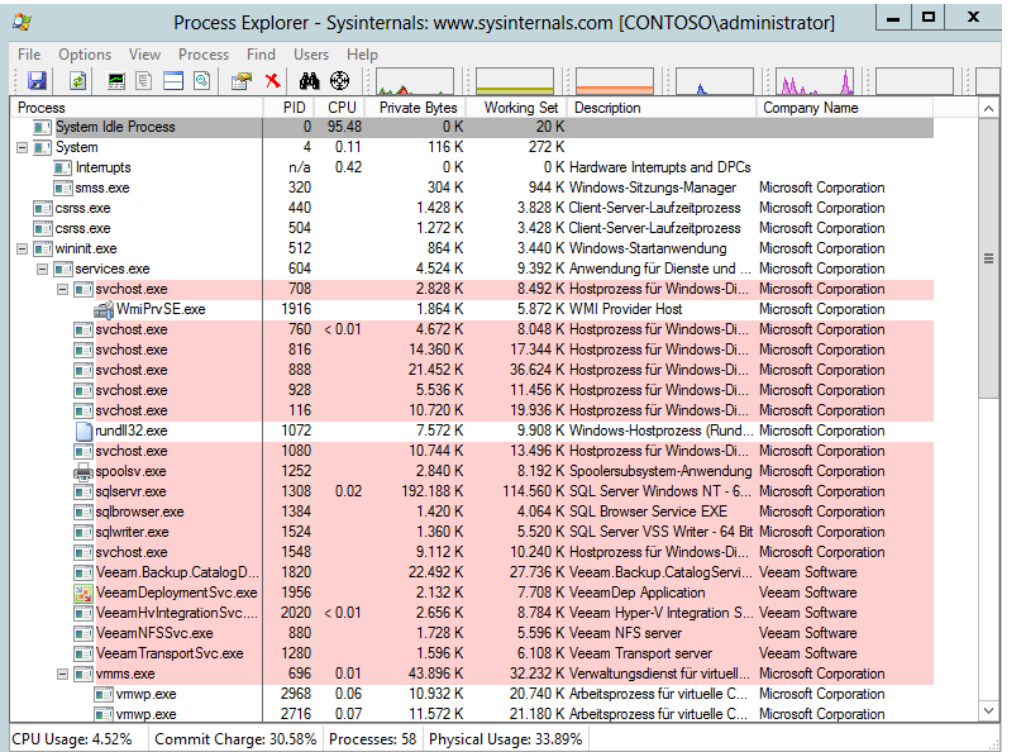
Bestandteil des Downloadpakets ist eine englischsprachige Hilfedatei, die den Umgang mit dem Tool detailliert erläutert. Funktioniert die Darstellung der Hilfe nicht, rufen Sie die Eigenschaften der Datei in *procmon.chm* auf. Wechseln Sie zur Registerkarte *Allgemein* und aktivieren ganz unten die Schaltfläche *Zulassen*.

Laufende Prozesse analysieren – Process Explorer

Ein wichtiges Tool für die Analyse der laufenden Prozesse auf einem Computer ist das Tool Process Explorer (*http://technet.microsoft.com/de-de/sysinternals/bb896653* [Ms179-K38-15]) von Sysinternals. Sie können sich entweder die ZIP-Datei herunterladen oder das Tool, wie übrigens jedes andere Tool von Sysinternals, auch direkt über den Browser starten. Dazu verwenden Sie die URL *http://live.sysinternals.com/procexp.exe* [Ms179-K38-16].

Process Explorer zeigt Prozesse in einem Fenster und darunter weitere Informationen zum aktuellen Prozess an, zum Beispiel ein aktueller Zugriff auf Ordner. Das Tool enthält wesentlich mehr Informationen als der Task-Manager in Windows. Klicken Sie auf die Messfenster im oberen Bereich, blendet der Process Explorer ein Systeminformationsfenster ein, welches ähnliche Informationen enthält wie der Task-Manager, nur diese viel umfangreicher auf verschiedenen Registerkarten darstellt.

Abbildg. 38.28 Systemüberwachung mit Process Explorer



Damit Sie alle notwendigen Daten anzeigen können, müssen Sie Process Explorer über das Kontextmenü mit Administratorrechten starten.

Das Programm zeigt Prozesse in verschiedenen Farben an. Prozesse, die im gleichen Benutzerkontext laufen wie Process Explorer selbst, stellt das Tool in hellblau dar.

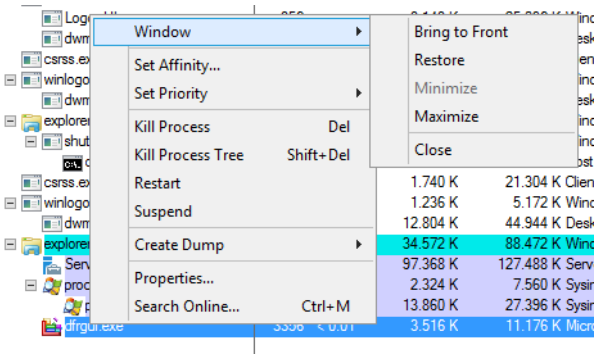
Pinkfarbene Prozesse sind Prozesse, die einen oder mehrere Windows-Dienste unterstützen. Eine weitere Farbe ist Violett. Damit werden Prozesse gekennzeichnet, die unter Umständen ausführbaren Code enthalten, um das System anzugreifen.

Viren und Trojaner verwenden solchen Code, um sich in das System einzuschleusen. Die Anzeige ist nicht immer korrekt, da es viele falsche Erkennungen gibt. Es schadet aber nicht, die einzelnen Prozesse zu überprüfen, zum Beispiel über das Kontextmenü mit dem Befehl *Search Online*.

Durch diese Auswahl startet der Browser und verwendet die hinterlegte Standardsuchmaschine im Internet, um nach dem Prozess zu suchen. Auf diese Weise finden Sie verschiedene Quellen und können den Prozess leicht identifizieren.

Über das Kontextmenü können Sie auch die Priorität von Prozessen erhöhen, um mehr Systemressourcen zuzuteilen oder Prozesse sowie ganze Prozessbäume zu beenden, zum Beispiel bei verdächtigen oder abgestürzten Prozessen. Wenn ein Prozess als aktives Fenster auf dem Desktop vorhanden ist, können Sie diesen über den Kontextmenübefehl *Window* anzeigen lassen oder minimieren.

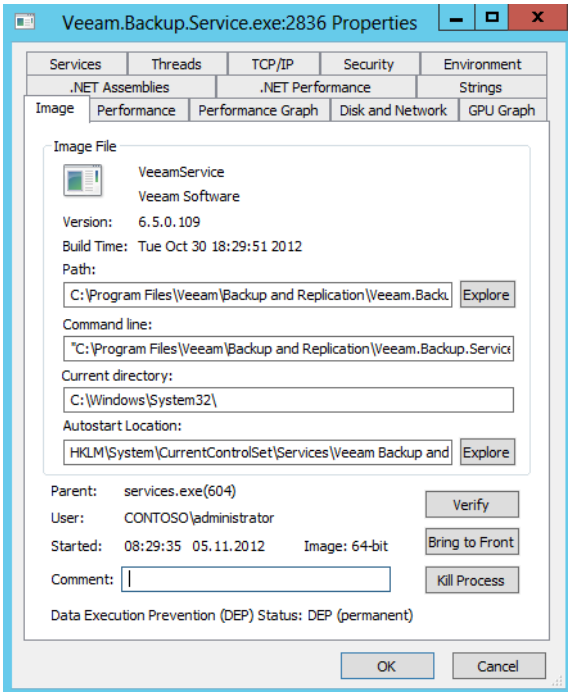
Abbildg. 38.29 Anzeigen des aktiven Fensters einen Prozesses



Mit dem Befehl *Set Affinity* im Kontextmenü eines Prozesses können Sie festlegen, welche CPUs oder CPU-Kerne der Prozess nutzen darf.

Mit dem Kontextmenübefehl *Properties* rufen Sie die Detailansicht eines Prozesses auf. Hier erhalten Sie auf verschiedenen Registerkarte ausführliche Informationen zum aktuellen Prozess und der ausführenden Datei des Prozesses angezeigt.

Abbildg. 38.30 Detailansicht eines Prozesses



Auf den verschiedenen Registerkarten sehen Sie zum Beispiel die ausführende Datei oder den Verbrauch der Systemressourcen. Auf der Registerkarte *TCP/IP* werden Ihnen die Netzwerkverbindungen oder die vom aktuellen Prozess aufgerufenen Verbindungen ins Internet angezeigt.

Mit einer braunen Farbe werden Prozesse gekennzeichnet, die durch Aufgaben in Windows ausgelöst wurden. Prozesse, die .NET Framework auf dem Rechner nutzen, stellt Process Explorer in Gelb dar. Dunkelgraue Prozesse sind aktuell pausiert, also gestartet, aber nicht aktiv.

Sie können die Farben der Anzeige anpassen. Dazu rufen Sie den Menübefehl *Options/Configure Colors* auf.

TIPP Markieren Sie eine Zeile im Sysinternals-Tool Process Explorer, können Sie diese mit der Tastenkombination Strg + C in die Zwischenablage kopieren.

Beim Starten zeigt Process Explorer zunächst die Standardspalten an.

Tabelle 38.2 Standardspalten des Process Explorer

Spalte	Beschreibung
Process	Hier sehen Sie die laufenden Prozesse und die Prozessbäume mit aufbauenden Prozessen. Falls möglich, blendet Process Explorer auch das Symbol der zugeordneten Anwendung ein.
PID	Prozess-ID des Prozesses. Diese wird vom Betriebssystem zugewiesen.
CPU	Prozentuale CPU-Zeit, die der Prozess aktuell verwendet
Private Bytes	Die Anzahl an Bytes, die der Prozess benötigt und die andere Prozesse nicht mit verwenden können
Working Set	Der dem Prozess zugeteilte Arbeitsspeicher. Die Zuteilung übernimmt in Windows der Speicher-Manager.
Description	Beschreibung, die der Entwickler der ausführenden Datei des Prozesses beigefügt hat. Diese Informationen benötigen Administratorrechte.
Company Name	Entwickler des Prozesses

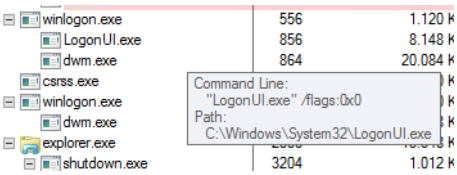
Sie können die Größe der Spalten anpassen und auch die Reihenfolge per Ziehen/Ablegen verändern. Wollen Sie Spalten ausblenden oder zusätzliche Spalten anzeigen, klicken Sie mit der rechten Maustaste auf eine Spaltenüberschrift und wählen im Kontextmenü den Eintrag *Select Columns*.

Anschließend können Sie auswählen, welche Spalten Process Explorer anzeigen soll oder welche Spalten Sie ausblenden möchten. Die Sortierreihenfolge innerhalb einer Spalte können Sie ebenfalls anpassen, indem Sie auf die entsprechende Spaltenüberschrift klicken.

Die wichtigsten Informationen über die laufenden Prozesse sehen Sie in der ersten Spalte. Process Explorer ordnet die Prozesse auch nach deren Abhängigkeiten an und zeigt an, welche Prozesse von anderen gestartet wurden. Diese Anzeige erreicht das Tool über einen Process Tree.

Einzelne Strukturen können Sie auch ein- und ausklappen, indem Sie auf das Minus- oder Pluszeichen klicken. Fahren Sie mit der Maus über einen Prozess, zeigt Process Explorer den kompletten Pfad zur ausführenden Datei an.

Abbildg. 38.31 Anzeigen des Pfads zur ausführenden Datei eines Prozesses



Auf diese Weise erhalten Sie auch mehr Informationen zu Diensten, welche die Prozesse starten. Fahren Sie mit der Maus zum Beispiel über *taskhost.exe*, sehen Sie auch die Aufgaben der Aufgabenplanung, die den aktuellen Prozess gestartet haben.

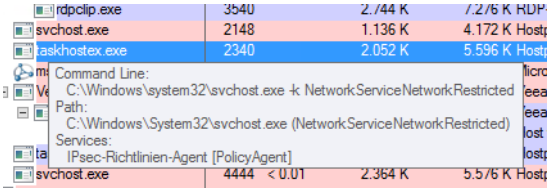
Auf diesem Weg erhalten Sie zu den einzelnen Prozessen ganz unterschiedliche Informationen über die Anwendungen, die für diesen Prozess zuständig sind. Wenn Sie zum Beispiel über den Prozess des Internet Explorers fahren, sehen Sie, welche Registerkarte im Internet Explorer aktuell von diesem Prozess genutzt wird. Der Internet Explorer öffnet für verschiedene Registerkarten (Tabs) eigene Prozesse. Fahren Sie mit der Maus über den Prozess, zeigt Process Explorer die Beschreibung der aktuell geöffneten Internetseite an.

Ein häufiger Prozess ist *svchost.exe*. Dieser ist in den meisten Fällen auch mehrmals gestartet. Die Datei *svchost.exe* gibt es seit Windows 2000; sie liegt im *System32*-Ordner 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 mithilfe 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.

Fahren Sie mit der Maus über einen Process, zeigt Process Explorer an, welche aktuellen Dienste oder Anwendungen von dieser Instanz der *svchost.exe* abhängen.

Abbildg. 38.32 Anzeigen der Dienste die Svchost benötigen



HINWEIS Über den Befehl *tasklist /svc* in der Eingabeaufforderung können Sie sich ebenfalls anzeigen lassen, welche Anwendungen auf *svchost.exe* zurückgreifen. 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. Holen Sie die Registerkarte *Details* in den Vordergrund.
3. Klicken Sie mit der rechten Maustaste auf eine Instanz von *svchost.exe* und klicken Sie dann auf *Zu Dienst(en) wechseln*. Die dem betreffenden Prozess zugeordneten Dienste werden auf der Registerkarte *Dienste* hervorgehoben.

Rufen Sie in Process Explorer über das Kontextmenü eines Prozess den Befehl *Properties* auf, sehen Sie auf der Registerkarte *Services*, für welche Dienste der Prozess zuständig ist (dies gilt auch für *svchost.exe*).

In der Symbolleiste von Process Explorer sehen Sie ein Fadenkreuz. Klicken Sie mit der Maus auf das Kreuz und ziehen es auf ein Fenster im Desktop, markiert Process Explorer automatisch den Prozess, der für dieses Fenster verantwortlich ist.

Über den Menübefehl *Options/Replace Task Manager* können Sie den Standard-Task-Manager in Windows ersetzen. Rufen Sie diesen zukünftig auf, zum Beispiel über das Kontextmenü der Taskleiste, startet direkt der Process Explorer. Auf dem gleichen Weg können Sie diese Option wieder rückgängig machen. Über den Menübefehl *View/Show Lower Pane* blenden Sie den unteren Bereich des Übersichtsfensters ein. Anschließend können Sie über den Menübefehl *View/Lower Pane View* konfigurieren, ob Sie im unteren Bereich die DLLs der Prozesse oder Handles anzeigen wollen.

Handles sind einfach ausgedrückt Zuteilungen des Betriebssystems, die Prozesse oder Anwendungen für Funktionen des Kernels erhalten, zum Beispiel der Zugriff auf den Arbeitsspeicher, Ein- oder Ausgabegeräte und so weiter. Da Prozesse und Anwendungen keinen direkten Zugriff auf den Kernel von Windows erhalten, sondern die benötigen Ressourcen zugeteilt bekommen, lassen sich diese Vorgänge überwachen. Benötigt der Prozess oder die Anwendung den Zugriff nicht mehr, wird der Handle wieder freigegeben, sodass andere Prozesse oder Anwendungen Zugriff auf die freigewordenen Ressourcen erhalten.

Über das Menü *Process* können Sie ausgewählte Prozesse beenden, neu starten oder deren Eigenschaften anzeigen. Über das Kontextmenü haben Sie aber die gleichen Möglichkeiten.

Mit der Tastenkombination Strg+F öffnen Sie ein Suchfenster. Tragen Sie hier einen Suchbegriff ein, um anzuzeigen, welche Prozesse oder DLLs dem Suchbegriff entsprechen und aktuell gestartet sind. Sie sehen, ob es sich um ein Handle oder eine DLL handelt. Auch hier können Sie die Suchergebnisse wieder über die entsprechenden Spaltenüberschriften sortieren lassen und auch die Reihenfolge ändern. Aktivieren Sie die DLL-Ansicht, werden Ihnen alle geladenen DLL-Dateien eines Prozesses angezeigt.

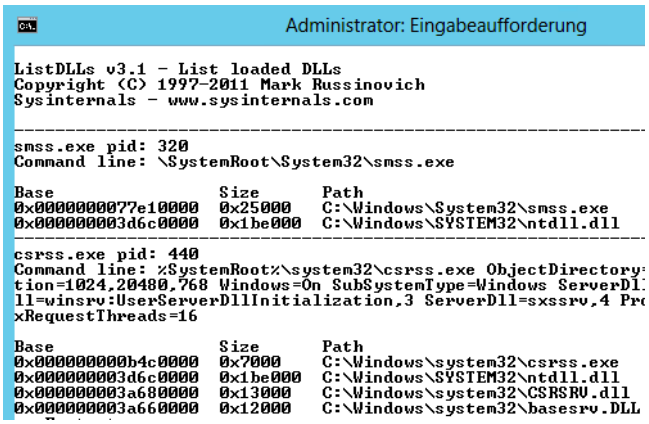
Über das Menü *View* oder das Symbol *System Information* in der Symbolleiste rufen Sie die Systeminformationen des Process Explorers auf.

Geladene DLL-Dateien anzeigen – ListDLLs

Wollen Sie auf einem Computer alle geladenen DLL (Dynamic Link Library, Dynamische Verbindungsbibliothek)-Dateien anzeigen, ist ListDLLs (*http://technet.microsoft.com/de-de/sysinternals/bb896656* [Ms179-K38-17]) von Sysinternals das aktuell beste Werkzeug dazu. Das Befehlszeilentool, welches Sie in einer Eingabeaufforderung mit Administratorrechten aufrufen müssen, zeigt Ihnen in Echtzeit alle DLL-Dateien an, die derzeit auf dem Server gestartet sind.

Sie sehen den Versionsstand der Datei sowie den genauen Speicherort. Wollen Sie die Ausgabe in eine Textdatei umleiten, verwenden Sie zum Beispiel den Befehl *listdlls >c:\temp\dll.txt*.

Abbildg. 38.33 Anzeigen der geladenen DLLs eines Computers



Sie können die Anzeige auch auf Basis geladener Prozesse anzeigen. Dazu verwenden Sie den Befehl

```
Listdlls <Name oder Teil des Prozessnamens oder dessen PID>
```

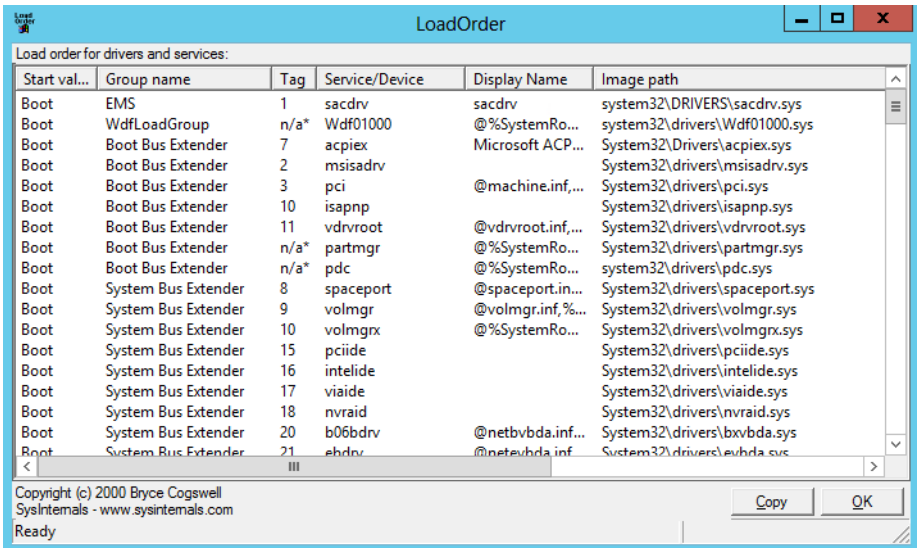
Anschließend zeigt ListDlls nur die Daten und geladenen DLLs dieses Prozesses an. Sie haben auch in der PowerShell die Möglichkeit, Prozesse zu verwalten, ohne auf Sysinternals-Tools zu setzen.

Über den Befehl *Get-Process* können Sie sich alle laufenden Prozesse eines Computers anzeigen lassen. Wollen Sie zum Beispiel nur alle Prozesse mit dem Anfangsbuchstaben »S« angezeigt bekommen, geben Sie den Befehl *Get-Process s** ein. Sollen die Prozesse zusätzlich noch sortiert werden, zum Beispiel absteigend nach der CPU-Zeit, geben Sie *Get-Process s** gefolgt von der Pipe-Option |*Sort-Object cpu –Descending* ein.

Systemtreiber anzeigen – LoadOrder

Mit dem Tool LoadOrder (*http://technet.microsoft.com/de-de/sysinternals/bb897416* [Ms179-K38-18]) lassen Sie sich die geladenen Systemdateien und die Reihenfolge des Ladens in einer grafischen Oberfläche anzeigen. Starten Sie das Tool, liest es die Startreihenfolge der geladenen Treiber ein. In neuen Windows-Betriebssystemen können natürlich weitere Plug & Play-Treiber im laufenden Betrieb dazu kommen, da Windows diese erst bei Bedarf nachlädt. LoadOrder zeigt die Treiber an, die Windows immer bei jedem Systemstart lädt.

Abbildg. 38.34 Anzeigen der Systemtreiber eines Servers und die Reihenfolge des Ladevorgangs



Sie haben die Möglichkeit, diese Liste auch in die Zwischenablage zu kopieren und dadurch zu Analysezwecken zu versenden.

Absturzanalysen für Prozesse erstellen – ProcDump

Belastet ein Prozess einen Computer zu stark und muss daher beendet werden, kann das Tool ProcDump (*http://technet.microsoft.com/de-de/sysinternals/dd996900* [Ms179-K38-19]) eine Analysedatei des Abbruchs erstellen. Der Fokus des Tools liegt darin, Verbrauchsspitzen für die CPU-Nutzung von Prozessen zu analysieren. Die Syntax des Befehls ist:

```
procdump [-64] [-b] [[-c CPU-Verbrauch] [-u] [-s Sekunden]] [-n <Anzahl>] [-e [1]] [-h]
[-m <Grenzwert >] [-ma | -mp] [-o] [-p <Trigger>] [-r] [-t] < Prozess> [<Datei>]] |
[-x <image file> <Dumpdatei> ]
```

Tabelle 38.3 Optionen von ProcDump

Option	Auswirkung
–64	Erstellt einen 64-Bit-Dump statt eines 32-Bit-Dumps
–c	Grenzwert, bei dem das Tool den Dump erstellen soll
–e	Erstellt einen Dump, wenn der Prozess abstürzt
–h	Schreibt einen Dump, wenn das Prozessfenster hängt
–m	Grenzwert für einen Dump, wenn der Prozess den Arbeitsspeichergrenzwert überschreitet
–ma	Schreibt einen Dump des kompletten Bereichs des Arbeitsspeichers, den der Prozess verbraucht

Tabelle 38.3 Optionen von ProcDump *(Fortsetzung)*

Option	Auswirkung
–mp	Erstellt einen Dump, der Threads und Handles des Prozesses enthält
–n	Anzahl der Dumps, die ProcDump erstellt, bis das Tool sich beendet
–o	Überschreibt existierende Dumps
–p	Verwendet spezielle Performance-Counter als Trigger, zum Beispiel `procdump outlook -p "\Processor(_Total)\% Processor Time" 20`
–r	Klont den Prozess zum Erstellen des Dumps (erst ab Windows 7 möglich)
–t	Erstellt einen Dump, wenn der Prozess beendet wird oder abstürzt

Wollen Sie für einen Prozess zum Beispiel fünf Dumps erstellen, wenn dieser für 60 Sekunden mehr als 50 % CPU-Last verursacht, und vorhandene Dumps überschreiben, verwenden Sie den folgenden Befehl:

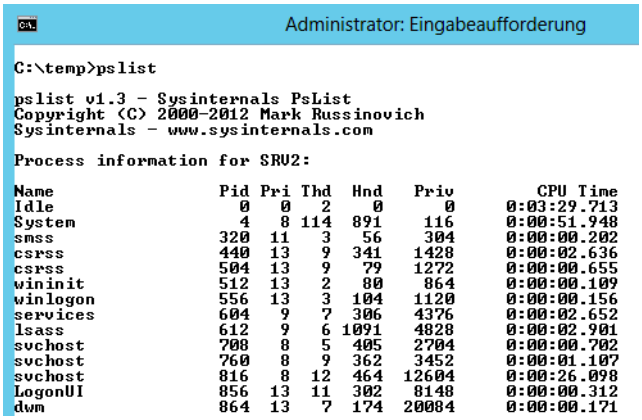
```
procdump -c 50 -s 60 -n 5 -o <Name des Prozesses> <Pfad>
```

Prozesse anzeigen und killen – PsList und PsKill

Um Prozesse in der Eingabeaufforderung anzuzeigen und zu beenden, helfen die beiden Tools PsList (*http://technet.microsoft.com/de-de/sysinternals/bb896682* [Ms179-K38-20]) und PsKill (*http://technet.microsoft.com/de-de/sysinternals/bb896683* [Ms179-K38-21]). PsList arbeitet mit PsKill zusammen.

Sie können mit PsList eine Liste von Prozesse anzeigen und die Informationen dazu nutzen, um die Prozesse mit PsKill zu beenden. Rufen Sie PsList ohne Optionen auf, zeigt das Tool bereits Informationen über die gestarteten Prozesse auf dem Computer an. Die Ausgabe enthält neben der Prozess-ID (PID) von links nach rechts die Prioritätsklasse, die Anzahl der Threads, die Anzahl der Handles, der Menge der verbrauchten CPU-Zeit und die Zeit, die dieser Prozess bereits aktiv ist. Dieses Programm braucht nicht unter einem Administratorkonto zu laufen, sondern kann auch ohne diese Berechtigung alle Informationen anzeigen.

Abbildg. 38.35 Anzeigen der geladenen Systemprozesse



Neben dem Gesamtverbrauch an virtuellem Speicher kann PsList auch Verbrauchsspitzen anzeigen. Die Option *–d* zeigt Details über die Threads an, die ein Prozess verwendet. Mit der Option *–x* ist es möglich, die Detailinformationen zum Prozess, dem Speicherverbrauch und den Threads gemeinsam auszugeben.

Die Option *–t* gibt eine Prozessstruktur aus. Dabei sind alle Prozesse zu sehen, die ein bestimmter Prozess startet. Verwenden Sie die Option *–s*, zeigt das Tool die Prozesse sortiert nach der verbrauchten CPU-Zeit an. Sie können mit dem Tool auch Prozesse auf einem Remotecomputer anzeigen lassen. Die Syntax dazu ist: *pslist* \\<*Computer*>. Wollen Sie Informationen zu speziellen Prozessen anzeigen, reicht es aus, wenn Sie einen Teil des Namens mit angeben, zum Beispiel *pslist svc*.

PsKill, ein Befehlszeilentool wie PsList, ermöglicht das Beenden von Prozessen. Mit PsKill können Sie Prozesse auf dem lokalen Computer oder auf einem Computer im Netzwerk beenden. 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.

Systemdienste im Griff – PsService

Mit PsService (*http://technet.microsoft.com/de-de/sysinternals/bb897542* [Ms179-K38-22]) können Sie Systemdienste lokal oder auf Computern im Netzwerk anzeigen, beenden und starten. Die Syntax des Programms lautet:

```
psservice [\\<Computer> [-u <Benutzername>] [-p <Kennwort>]] <Befehl> <Option>
```

Tabelle 38.4 Optionen von PsService

Option	Auswirkung
query	Zeigt den Status eines Diensts an
config	Zeigt die Einstellungen eines Diensts an
setconfig	Setzt den Starttyp des Diensts 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 Diensts

Dienste können Sie auch in der PowerShell mit *Start-Service*, *Stop-Service*, *Get-Service* und *Set-Service* starten und beenden. Auch die Befehlszeilentools *net start* und *net stop* helfen bei der Verwaltung der Systemdienste.

Am schnellsten rufen Sie die Verwaltungsoberfläche der Systemdienste in Windows durch die Eingabe von *services.msc* in der Startseite auf. In der Eingabeaufforderung sehen Sie die gestarteten Dienste über *net start*. Mit *net start >dienste.txt* werden alle gestarteten Dienste in die Datei *dienste.txt* gespeichert.

Eine weitere Möglichkeit ist der Befehl *sc query*, der deutlich mehr Informationen liefert. Dienste lassen sich, neben der grafischen Oberfläche, in der Eingabeaufforderung über *net stop <Dienstname>* stoppen und über *net start <Dienstname>* wieder starten. Der eigentliche Starttyp wird dadurch aber nicht geändert. Diesen können Sie über die Diensteverwaltungskonsole in den Eigenschaften des Diensts anpassen.

Geben Sie nur *psservice* ein, erhalten Sie Informationen zu allen Diensten auf dem lokalen System. Die Dienste eines Computers im Netzwerk zeigen Sie am schnellsten mit *psservice \\<Computername> query* an. Wollen Sie nur bestimmte Dienste anzeigen, können Sie einfach den Namen oder den Teil eines Namens hinter *query* anhängen, zum Beispiel *psservice \\dell-srv02 query wuauserv*.

Daten des Task-Mangers in Excel einlesen – TaskManager.xls

Zur Fehlersuche und Analyse reicht es nicht immer aus, die Daten im Task-Manager oder über Zusatztools einzulesen. Hier stellt die Excel-Tabelle *Taskmanager.xls* von der Seite *http://blog.didierstevens.com/2011/03/01/update-taskmanager-xls-version-0-0-3* [Ms179-K38-23] eine wertvolle Hilfe dar. Starten Sie die Tabelle in Excel, können Sie einfach die aktuellen Prozesse und deren Daten aus dem Task-Manager in Excel einlesen.

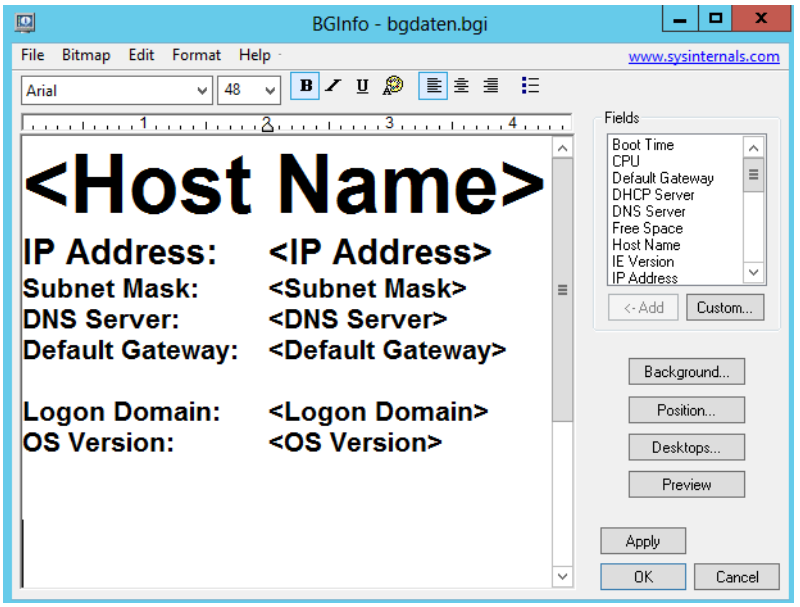
Wichtige Informationen immer im Blick – BgInfo

Administratoren, die mehrere Server oder Computer von Anwendern im Netzwerk fernwarten, haben oft das Problem, dass nicht alle Informationen über den aktuell verbundenen Computer angezeigt werden, zum Beispiel IP-Adresse, Informationen zu den Laufwerken, Rechnernamen, Bootzeit etc. Auch wenn Anwender eine Fernwartung benötigen, ist es hilfreich, wenn diese auf dem Desktop den Namen ihres Computers, die IP-Adresse und weitere Informationen auf einen Blick sehen. In vielen Fällen ist es also für Administratoren extrem hilfreich, wenn auf dem Desktop des ferngewarteten Computers nützliche Informationen angezeigt werden, allerdings ohne dass diese Informationen die Anwender stören.

Ein hilfreiches Tool für diese Zwecke ist BgInfo (*http://technet.microsoft.com/de-de/sysinternals/bb897557* [Ms179-K38-24]) von Sysinternals. Der Entwickler hält in einem eigenen Beitrag (*http://www.windowsitpro.com/article/desktop-management/bginfo.aspx* [Ms179-K38-25]) weitere Tipps zum Tool bereit. Auch im Sysinternals-Forum (*http://forum.sysinternals.com/forum5.html* [Ms179-K38-26]) erhalten Sie Informationen zu BgInfo. Allerdings ist eine Einarbeitung nicht notwendig, da das Tool sehr leicht bedienbar ist und keine Installation oder Konfiguration erfordert. BgInfo kann Informationen in verschiedenen Schriftgrößen, Farben und anderen Formatierungen auf dem Desktop anzeigen.

Neben vorgegebenen Feldern können Sie auch eigene Abfragen erstellen und Informationen einblenden lassen. Diese Anzeige lässt sich vorkonfigurieren, als Konfigurationsdatei abspeichern und per Skript oder Gruppenrichtlinie an Computer im Netzwerk verteilen. Das Tool verbraucht keinerlei Systemressourcen, sondern erstellt beim Start aus den gewünschten Informationen eine neue Desktopbitmap und beendet sich danach wieder. Im laufenden Betrieb ist das Tool daher nicht gestartet.

Abbildg. 38.36 Informationen des Servers auf dem Desktop anzeigen



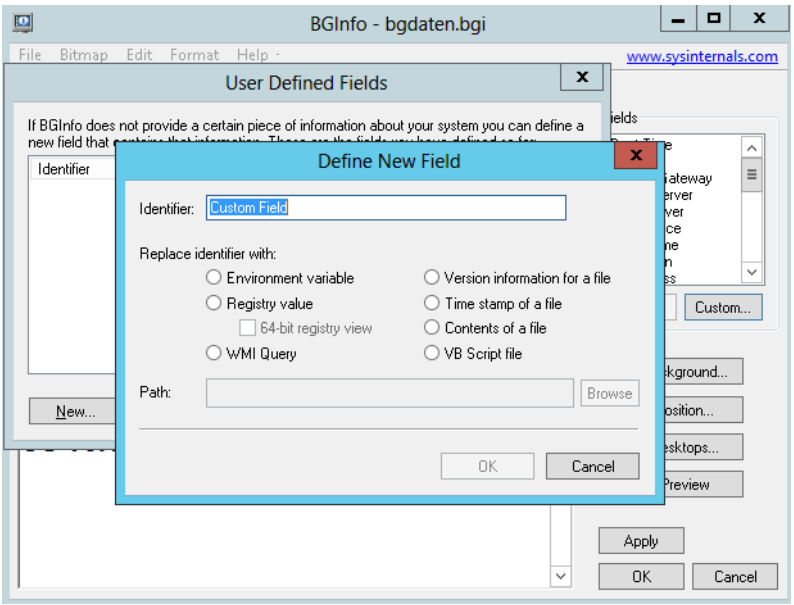
Informationen zum Computer auf dem Desktop anzeigen

Nach dem Start von BgInfo können Sie konfigurieren, welche Daten Sie zukünftig anzeigen wollen und diese als Konfigurationsdatei abspeichern. Die Konfiguration ist sehr einfach. Im Feld *Field* sehen Sie, welche Daten Sie in das Hintergrundbild einbinden können.

Klicken Sie auf ein Feld und dann auf *<–Add*, um es einzubinden. Verfügt ein Computer über mehrere Netzwerkkarten, bindet BgInfo diese mit ihren unterschiedlichen Konfigurationen wie IP-Adressen, MAC-Adressen und weitere Daten automatisch mit ein. Über die Schaltfläche *Custom* können Sie eigene Felder definieren, indem Sie mit *New* eine neue Abfrage starten.

Sie haben im neuen Fenster die Möglichkeit, Umgebungsvariablen abzufragen, einen Registrywert, eine WMI-Abfrage oder Daten einer Datei. In den meisten Fällen ist dies aber nicht notwendig, da die Standardfelder schon viele Informationen umfassen.

Abbildg. 38.37 Definieren eigener Felder in BgInfo



Felder und Zeilen, die Sie nicht benötigen, können Sie im mittleren Fenster einfach löschen. Auch Leerzeilen können Sie einfügen, wie in jeder Textverarbeitung. Einzelne Zeilen bearbeiten Sie mit den Formatierungswerkzeugen des Tools, die Sie im oberen Bereich finden. Hier können Sie die Schriftgröße und Schriftart einstellen, Farben ändern und die Ausrichtung anpassen.

Haben Sie ausgewählt, welche Felder Sie anzeigen wollen, und diese formatiert, können Sie über die Schaltfläche *Background* festlegen, welches Hintergrundbild Sie mit diesen Informationen anpassen möchten. Standardmäßig verwendet BgInfo das Hintergrundbild des Desktops, welches aktuell ausgewählt ist.

Über die Schaltfläche *Position* bestimmen Sie, an welcher Stelle des Hintergrundbilds BgInfo die Informationen aufnehmen soll. Da das Tool auch mehrere Monitore unterstützt, können Sie festlegen, auf welchem Monitor die Informationen zu sehen sein sollen. Über das Kontrollkästchen *Compensate for Taskbar position* (Ausgleich für Taskleistenposition) legen Sie die Position so fest, dass die Taskleiste den Text nicht überdeckt.

Über die Schaltfläche *Desktops* legen Sie fest, wo BgInfo die Informationen anzeigen soll. Standardmäßig sind die Daten erst ersichtlich, wenn sich ein Anwender anmeldet. Sie können noch die Einstellung *Update this wallpaper* für die Option *Logon Desktop for Console users* aktivieren. In diesem Fall werden die ausgewählten Informationen bereits am Anmeldebildschirm angezeigt, ohne dass sich Anwender anmelden müssen. Dies ist zum Beispiel für Server sinnvoll, wenn an der Konsole kein Administrator angemeldet ist.

Klicken Sie auf *Preview*, zeigt Windows eine Vorschau der Informationen an. Um diese wieder zu deaktivieren, klicken Sie noch einmal auf *Preview*. Um die Anzeige zu übernehmen, klicken Sie auf *Apply*. Mit *OK* übernehmen Sie die Einstellungen und schließen BgInfo.

Natürlich ist es nicht sinnvoll, eine Konfiguration immer wieder neu zu erstellen oder für jeden Computer einzeln anzufertigen. Aus diesem Grund haben Sie in BgInfo auch die Möglichkeit, die

von Ihnen angepassten Daten über den Menübefehl *File/Save As* als *.bgi*-Datei abzuspeichern. Sie können anschließend BgInfo so starten, dass das Tool diese *.bgi*-Datei als Konfigurationsdatei übernimmt und die ausgewählten Daten anzeigt. Dazu starten Sie BgInfo einfach mit dem Befehl:

```
bginfo <Name der .bgi-Datei> /timer:0
```

Geben Sie keine Konfigurationsdatei an, verwendet BgInfo die Standardkonfigurationsinformationen die in der Registrierung im Pfad *HKEY_CURRENT_USER\Software\Winternals\BGInfo* gespeichert sind.

Die Option */timer:0* bewirkt, dass das BgInfo-Konfigurationsfenster nicht erscheint, sondern sofort die Informationen übernommen werden. Sie können diesen Befehl in ein Anmeldeskript übernehmen und auf diese Weise auch Daten wie die Anmeldezeit oder Bootzeit des Computers erfassen. Diese Zeiten sind natürlich immer nur dann aktuell, wenn Sie BgInfo bei jedem Systemstart oder jedem Anmelden starten lassen. BgInfo aktualisiert sich niemals dynamisch, sondern verwendet immer nur die Daten, die es beim Start vorfindet. Nach der Erstellung des neuen Hintergrundbilds beendet sich BgInfo wieder. Neben Skripts können Sie BgInfo auch mit der Aufgabenplanung in Windows während des Systemstarts und im laufenden Betrieb ständig aktualisieren lassen. Das ergibt allerdings nur dann Sinn, wenn Sie auch Felder anzeigen lassen, deren Informationen sich im laufenden Betrieb ändern. Neben der Option */timer* stehen in BgInfo weitere Möglichkeiten zur Verfügung:

- **/popup** Geben Sie diese Option an, zeigt BgInfo ein Popupfenster an, welches die Informationen enthält. Dieses können Anwender schließen.
- **/taskbar** Bei dieser Option blendet BgInfo ein Symbol im Infobereich der Taskleiste bei der Uhr ein. Klicken Anwender auf das Symbol, erscheinen die gewünschten Informationen genauso wie bei der Option */popup*.
- **/all** Ändert die Daten für alle aktuell angemeldeten Benutzer (zum Beispiel auf Terminalservern). Auf diese Weise erhalten also alle angemeldeten Anwender das neue Hintergrundbild.
- **/log** Erstellt eine Protokolldatei über die Ausführung, in die das Tool auch Fehler schreibt. Diese Option ist sinnvoll, wenn Sie das Tool im laufenden Betrieb über den Aufgabenplaner häufiger starten lassen.
- **/rtf** Erstellt eine *.rtf*-Datei. Diese Datei enthält auch die Formatierungen und Farbe zur Protokollierung.

BgInfo als Inventur- und Überwachungstool verwenden

Über den Menübefehl *File/Database* können Sie in der Konfigurationsdatei eine Verbindung zu einer Datenbank vorgeben, um die Daten eines oder mehrerer Computer zu erfassen, zum Beispiel für eine Inventur. In diesem Fall ändert das Tool nicht nur das Hintergrundbild, sondern erfasst die Daten in der Datenbank oder der ausgewählten Excel-Tabelle.

Auf allen Computern, welche diese Konfigurationsdatei nutzen, muss die gleiche Version von MDAC- und JET-Datenbankunterstützung installiert sein. Microsoft empfiehlt mindestens die Versionen *MDAC 2.5* und *JET 4.0*. Sie können an dieser Stelle als Datenbank auch eine Excel-Tabelle verwenden (*.xls*). Die Datei muss verfügbar sein, das Tool kann selbst keine Excel-Dateien erstellen.

Wollen Sie mit BgInfo keine Hintergrundbilder ändern, sondern nur die Daten beim Systemstart abfragen und in die Datenbank oder Excel-Tabelle aufnehmen, können Sie in der Konfigurationsda-

tei festlegen, dass keine Änderungen stattfinden sollen. Dazu klicken Sie im Rahmen der Konfiguration auf die Schaltfläche *Desktops* und deaktivieren die Änderung der entsprechenden Desktops.

Systeminformationen in der Eingabeaufforderung anzeigen – PsInfo

Wollen Sie über einen bestimmten Computer Informationen in der Eingabeaufforderung anzeigen, zum Beispiel zur eingebauten Hardware oder installierten Service Packs und Betriebssystemständen, können Sie das kostenlose Sysinternals-Tool PsInfo aus der PsTool-Sammlung nutzen (*http://technet.microsoft.com/de-de/sysinternals/bb897550* [Ms179-K38-27]). PsInfo kann nicht nur Daten des lokalen Computers abfragen (dazu könnten Sie zum Beispiel auch *msinfo32* nutzen oder *systeminfo* in der Eingabeaufforderung), sondern auch Daten von Netzwerkcomputern.

Um Daten des lokalen Systems abzufragen, geben Sie einfach *psinfo* in der Eingabeaufforderung ein. PsInfo benötigt für die Abfrage von Remoteinformationen auch einen Remotezugriff auf die Registrierung des entsprechenden Computers, um Daten anzuzeigen. Das heißt, auf dem Computer muss der Systemdienst *Remoteregistrierung* gestartet sein. Außerdem muss das Benutzerkonto, mit dem Sie PsInfo ausführen, Zugriff auf den Remotecomputer haben.

Die Syntax des Tools lautet:

```
psinfo [[\\Computer[,Computer[,..] | @Datei [-u Benutzer [-p Kennwort]]] [-h] [-s] [-d]
[-c [-t Trennzeichen]] [Filter]
```

Tabelle 38.5 Optionen von PsInfo

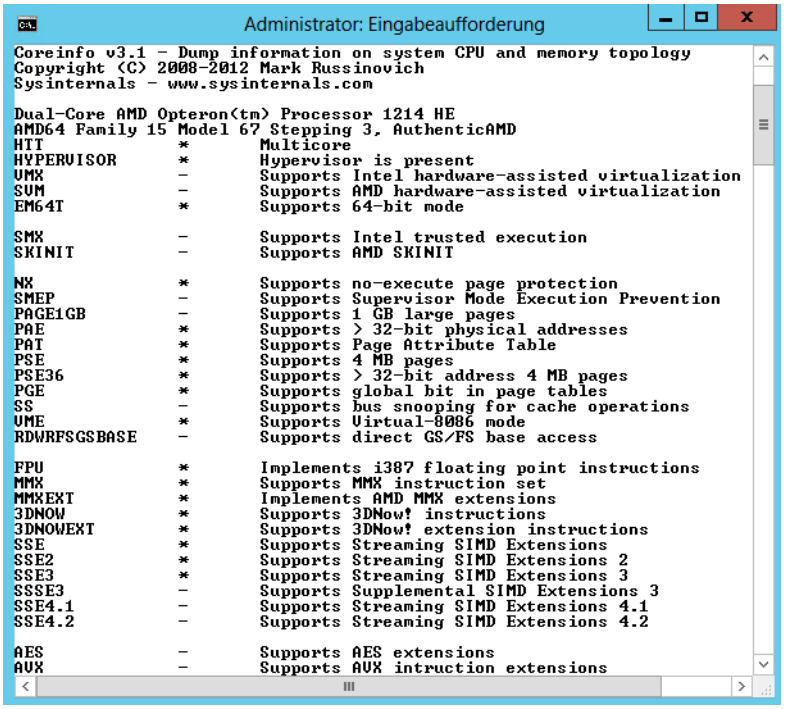
Optionen	Auswirkung
@Datei	Führt den Befehl auf allen Computern aus, die in der Textdatei angegeben sind. Schreiben Sie die einzelnen Computer jeweils in eine eigene Zeile.
–u	Benutzernamen für den Remotecomputer
–p	Kennwort für den Benutzer
–h	Liste der installierten Patches
–s	Liste der installierten Anwendungen
–d	Zeigt Informationen zu Datenträgern
–c	Ausgabe im *.csv*-Format
–t	Legt das Trennzeichen für die Ausgabe mit *–c* fest (standardmäßig Komma)
Filter	Ausgabe nach Feldern filtern, welche dem angegebenen Text entsprechen

Der Aufruf *psinfo proc* zeigt zum Beispiel nur Informationen über die Prozessoren an.

Informationen zu CPU-Kernen anzeigen – Coreinfo

Mit dem Sysinternals-Tool Coreinfo (*http://technet.microsoft.com/de-de/sysinternals/cc835722.aspx* [Ms179-K38-28]) lässt sich anzeigen, welche Kerne im Computer vorhanden sind und wie diese aktuell genutzt werden.

Abbildg. 38.38 Anzeigen von Informationen zu den Prozessoren im System



Das Tool ist vor allem nützlich, um sich den Cache des Prozessors anzeigen zu lassen. Das Tool zeigt dazu die NUMA (Non-Uniform Memory Architecture)-Daten an. Hierbei handelt es sich um die Speicherstruktur, die Mehrkernprozessoren nutzen. Bei dieser Technologie hat jeder Prozessor seinen eigenen Cache, den er aber anderen Prozessoren zur Verfügung stellen kann.

Sicherheitskonfigurations-Assistent (SCW)

Der Sicherheitskonfigurations-Assistent (Security Configuration Wizard, SCW) dient der Absicherung eines Servers über einen Assistenten, der Sicherheitsrichtlinien anwendet und die Firewall in Windows konfiguriert. Änderungen, die der SCW an einem System durchführt, können Sie leicht auch wieder rückgängig machen.

Der SCW geht Schritt für Schritt vor. Auf diese Weise steuern Sie die Einstellungen eines Servers sehr einfach. Microsoft hat in den Security Configuration Wizard eine automatische Erkennung von

Microsoft-Serverdiensten eingebaut. Zusätzliche Serverdienste binden Sie über Manifeste ein, wie im Fall von SharePoint oder Exchange. Sie können Server aber auch ohne zusätzliche Manifestdateien absichern. Der SCW besteht grundsätzlich aus drei wichtigen Komponenten:

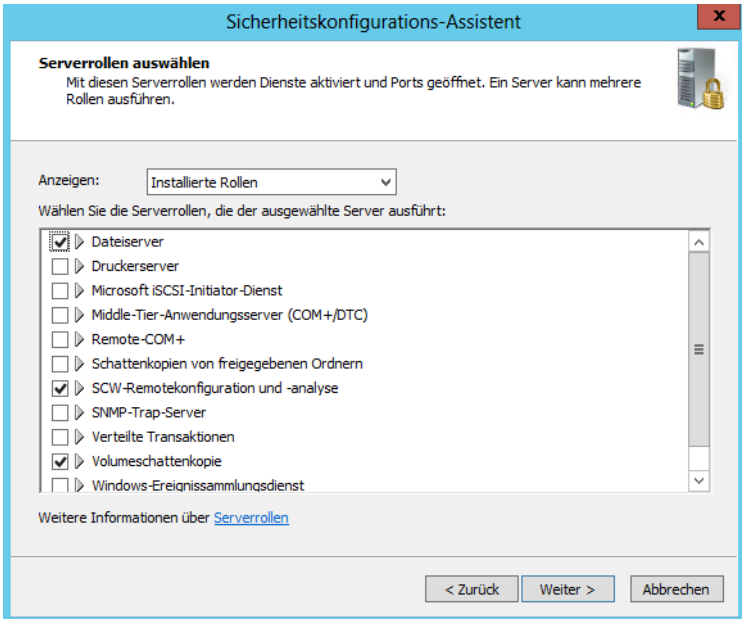
- Der grafischen Oberfläche zur Konfiguration der Sicherheitsrichtlinien
- Einer Befehlszeilenversion für das Scripting
- Der Sicherheitskonfigurationsdatenbank mit den Richtlinien

Sichern Sie einen Server mit dem SCW ab, arbeiten Sie hauptsächlich mit der grafischen Oberfläche des Programms. Dieses starten Sie am schnellsten durch die Eingabe von *scw* auf der Startseite. Das Befehlszeilentool Scwcmd dient zum Automatisieren des SCW.

Mit diesem Tool können Sie Skripts erstellen und damit mehrere Server mit einer Sicherheitsrichtlinie versorgen. Mit dem Tool lassen sich auch Richtlinien wieder rückgängig machen, falls Probleme auftreten. Sie finden im Ordner *\Windows\Security\Msscw\KBs* eine Sammlung von XML-Dateien. Diese Dateien enthalten alle wichtigen Informationen über Dienste, Serverrollen und Ports, mit deren Hilfe Sie den Server absichern können.

SCW verwendet einen rollenbasierten Mechanismus zur Absicherung eines Servers und deaktiviert die nicht benötigte Funktionalität. SCW arbeitet bei der Absicherung von Servern über Sicherheitsrichtlinien. Haben Sie auf einem Server eine Richtlinie erstellt und abgespeichert, können Sie diese Richtlinie auf einem anderen Server mithilfe des SCW importieren.

Abbildg. 38.39 Auswählen von Serverrollen für den Sicherheitskonfigurations-Assistenten



Haben Sie den SCW gestartet, fragt der Assistent nach, ob er eine bestehende Richtlinie importieren, eine neue Richtlinie erstellen, eine vorhandene Richtlinie vor dem Importieren bearbeiten oder schließlich die Durchführung der letzten Richtlinie zurücknehmen soll. Die Konfiguration der Sicherheitsrichtlinie unterteilt sich in unterschiedliche Bereiche. Sie sollten bei jedem Fenster genau

überprüfen, ob der Assistent alle Dienste und Funktionen erkannt hat. Sie können jederzeit einzelne Punkte aktivieren oder deaktivieren.

Nach dem Start erstellen Sie zunächst eine neue Sicherheitsrichtlinie, wählen den Server aus und wechseln zur Seite *Serverrollen auswählen*.

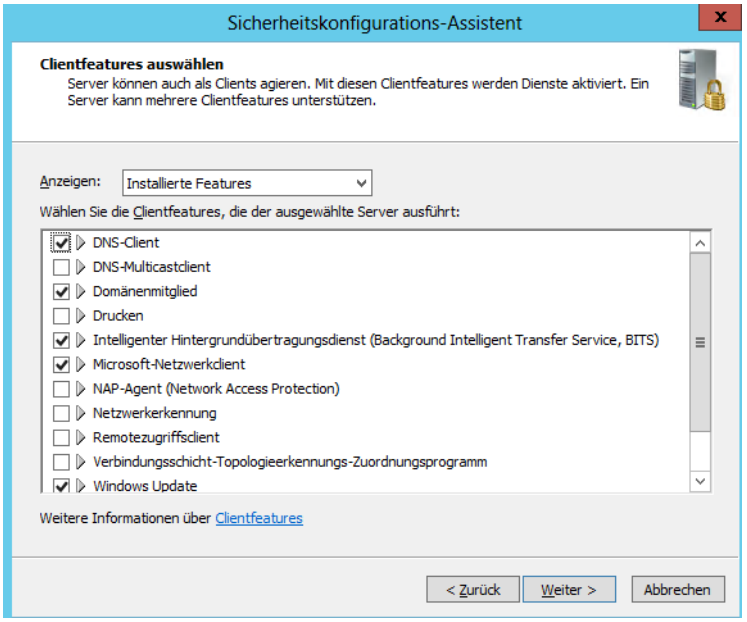
Der erste Bereich, den Sie konfigurieren, ist die rollenbasierten Konfiguration. Hier untersucht der Assistent die einzelnen Dienste und Funktionen des Servers und teilt diese den Rollen zu, die in der Sicherheitskonfigurationsdatenbank hinterlegt sind. Auch wenn Sie hier falsche Eingaben machen und diese später anwenden, sollte kein Problem auftreten, da Sie die Richtlinie jederzeit wieder deaktivieren können.

Um Administratoren bei der Auswahl von Serverrollen zu unterstützen, hat Microsoft im SCW für jede verfügbare Rolle eine Beschreibung hinterlegt, die helfen soll, entsprechende Rollen eindeutig zuzuordnen. Stellen Sie also bei der rollenbasierten Konfiguration sicher, dass alle Rollen des Servers ausgewählt sind, aber natürlich auch nicht zu viele. Manche Serverrollen sind von anderen abhängig und werden vom Assistenten notfalls automatisch hinzugefügt.

Der SCW definiert Serverrollen für verschiedene Aufgaben und erleichtert Ihnen so später die Auswahl, welches System Sie schließlich absichern wollen. Achten Sie genau darauf, welche Serverrolle Sie für einen Server anwenden, und wählen Sie immer die Rolle mit dem größten gemeinsamen Nenner aus. Es bringt nichts, wenn Sie einen Server optimal absichern, dieser aber nach dem Absicherungsvorgang nicht mehr funktioniert.

SCW aktiviert nicht nur die neue Windows-Firewall und schließt damit nicht mehr benötigte Ports, sondern deaktiviert auch Systemdienste, deaktiviert Webdienste von IIS, greift in Protokolle wie SMB und LDAP ein und definiert Sicherheitsrichtlinien. Die Basis für die erstellten Sicherheitsrichtlinien sind XML-Dateien, in denen alle Absicherungsmaßnahmen gespeichert sind.

Abbildg. 38.40 Auswählen der installierten Features



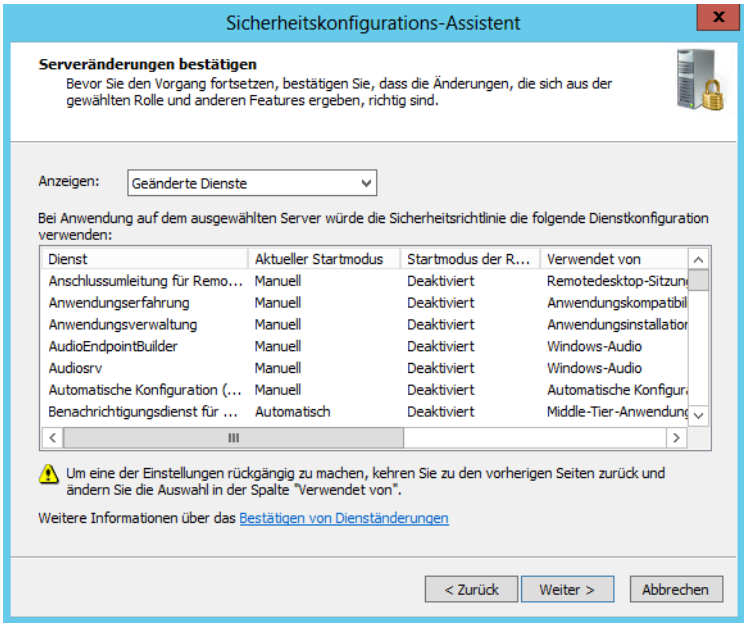
Auch notwendige Änderungen an der Registry, die der SCW durchführt, sind in dieser XML-Datei gespeichert. Haben Sie alle notwendigen Serverrollen des Servers ausgewählt, gelangen Sie mit *Weiter* zur nächsten Seite des Assistenten. Hier wählen Sie die einzelnen Features aus, die auf dem Server installiert sind.

Im nächsten Fenster können Sie noch feinere Unterscheidungen treffen. Hier wählen Sie aus, welche Optionen auf dem Server aktiviert sind und weiterhin funktionieren müssen. In diesem Fenster erhalten Sie auch Informationen über Dienste, die der Assistent nicht erkennt, und Sie können selbst entscheiden, welche Dienste der SCW deaktivieren soll und welche aktiv bleiben sollen. Da in den letzten drei Fenstern die Unterscheidungen und Konfigurationen der einzelnen Dienste immer feiner werden, sollten Sie sehr sorgfältig überlegen, welche Optionen Sie aktivieren und welche nicht.

In weiteren Fenstern können Sie festlegen, wie der Assistent mit Diensten umgehen soll, deren Funktionalität er nicht kennt. Haben Sie festgelegt, wie der SCW mit unbekannten Diensten verfahren soll, erhalten Sie im nächsten Fenster eine Zusammenfassung, welche Aktion der SCW mit den einzelnen Diensten durchführt. Bestätigen Sie dieses Fenster, ändert der SCW die angezeigten Dienständerungen in der Sicherheitsrichtlinie.

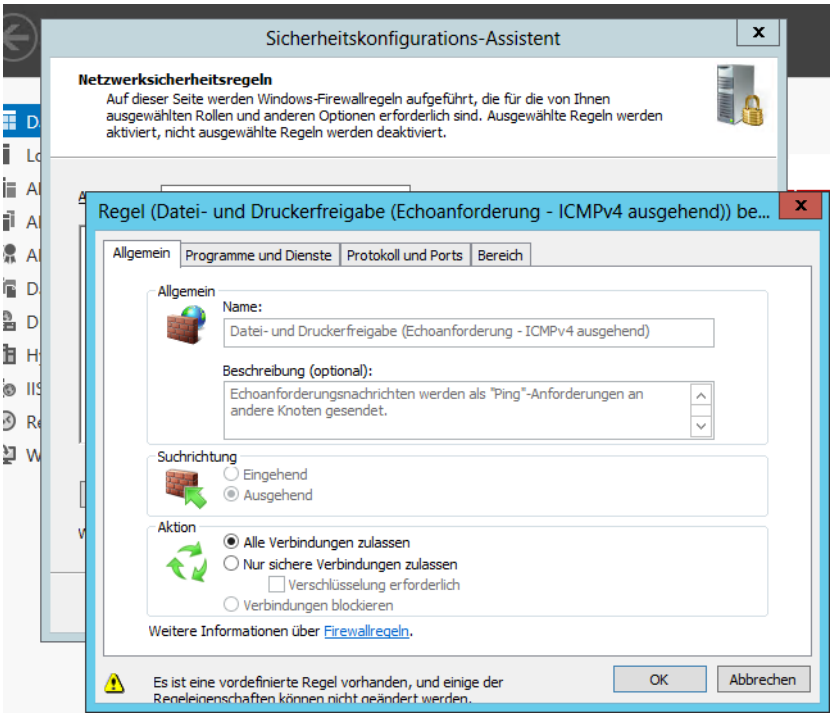
Auch an dieser Stelle erhalten Sie wieder eine Hilfe. In diesem Fenster können Sie schnell sehen, wie viele Dienste auf Ihrem Server gestartet waren, die überhaupt nicht im Einsatz sind. Je nach Anzahl von deaktivierten Diensten erreichen Sie auch eine gewisse Performancesteigerung, da jeder Dienst Arbeitsspeicher und Prozessorlast belegt. Haben Sie dieses Fenster bestätigt, ist die rollenbasierte Konfiguration abgeschlossen. Der Assistent beginnt mit der nächsten Konfigurationsmaßnahme, der Netzwerksicherheit.

Abbildg. 38.41 Ändern von Systemdiensten



Sie können diesen Abschnitt auch überspringen, wenn Sie nicht wollen, dass der SCW die Windows-Firewall aktiviert und einzelne Ports sperrt. Der Assistent zeigt Ihnen alle offenen Ports des Servers und den dazugehörigen Dienst an. Hier sehen Sie auch die einzelnen SharePoint-Dienste und können deren Zugriff steuern.

Abbildg. 38.42 Konfigurieren der Netzwerkeinstellungen



Sie können zusätzliche Ports manuell hinzufügen, offene Ports schließen lassen oder einzelne Portnummern bearbeiten. Haben Sie alle Einstellungen vorgenommen, erhalten Sie im letzten Fenster dieses Bereichs eine Zusammenfassung. Haben Sie die Konfiguration der offenen Ports abgeschlossen, wird der nächste Bereich des Assistenten angezeigt.

Hier legen Sie die Authentifizierungsmaßnahmen für LDAP und SMB sowie verschiedene Sicherheitseinstellungen fest, welche die Authentifizierung und die Registry betreffen. Abschließend erhalten Sie in einer Zusammenfassung angezeigt, welche Sicherheitseinstellungen vorgenommen werden. Auf einer weiteren Seite des Assistenten legen Sie fest, mit welcher Methode sich der Server oder dessen Dienste an externen Servern anmeldet.

Verwenden Sie zur Anmeldung nur Domänenbenutzerkonten, müssen Sie lediglich die Option *Domänenkonten* aktivieren. Auf der nächsten Seite des Assistenten legen Sie fest, ob die anderen Computer im Netzwerk mindestens unter Windows NT 4.0 SP6a laufen. Diese Option sollten Sie aktivieren. Zusätzlich könnten Sie noch die Option *Uhren, die mit der Uhr des ausgewählten Servers synchronisiert werden* aktivieren. Zum Abschluss listet der Assistent noch einmal alle Änderungen an der Registry auf, die durch die Richtlinie durchgeführt werden.

Als nächster Bereich erscheint die Überwachungskonfiguration. Hier konfigurieren Sie, welche Ereignisse der Server zukünftig in seinem Sicherheitsprotokoll speichern soll. Zum Abschluss des Assistenten müssen Sie die Einstellungen in einer XML-Datei abspeichern und können wählen, ob die konfigurierten Optionen sofort ausgeführt werden sollen oder ob Sie später die Datei laden und diese danach ausführen möchten.

Sie können die Anwendung einer Sicherheitsrichtlinie wieder zurücknehmen. Auch diesen Vorgang nehmen Sie über den SCW vor. Wenden Sie die Richtlinie sofort an, führt der SCW die XML-Datei aus und legt die eingestellten Sicherheitsvorgaben fest. Nach Abschluss der Anwendung müssen Sie den Server neu starten. Zur Anwendung von Sicherheitsrichtlinien stehen Ihnen außer der sofortigen Anwendung noch zwei andere Möglichkeiten zur Verfügung:

1. Sie können die Sicherheitsrichtlinie später einlesen, wenn Sie die grafische Oberfläche des SCW starten.
2. Sie können die Sicherheitsrichtlinie mit dem Befehlszeilentool Scwcmd gleichzeitig mehreren Servern zuweisen.

Am besten erstellen Sie eine Sicherheitsrichtlinie in einer Testumgebung und speichern diese ab. Die abgespeicherte Sicherheitsrichtlinie können Sie dann entweder manuell über die grafische Oberfläche installieren oder per Batchdatei und Befehlszeilentool Scwcmd verteilen lassen. Das Anwenden einer Sicherheitsrichtlinie ist in wenigen Sekunden abgeschlossen. Nach dem erforderlichen Neustart sind die Einstellungen sofort aktiviert.

Wollen Sie die Richtlinie später anwenden, starten Sie dazu wieder den Sicherheitskonfigurations-Assistenten. Wählen Sie als Option beim Startfenster *Vorhandene Sicherheitsrichtlinie anwenden*. Diesen Vorgang können Sie auch durchführen, wenn Sie die XML-Datei auf einen anderen Server kopieren und diese auf die gleiche Weise ausführen lassen.

Haben Sie die Option ausgewählt, können Sie mit der Schaltfläche *Durchsuchen* die XML-Datei laden lassen. Als Nächstes gelangen Sie mit *Weiter* auf die nächste Seite des Assistenten. Auf dieser Seite können Sie den Server auswählen, auf dem Sie die Sicherheitsrichtlinie anwenden wollen.

Öffnen Sie eine Eingabeaufforderung, können Sie eine Sicherheitsrichtlinie mit dem Befehlszeilentool Scwcmd anwenden. Um eine Richtlinie lokal anzuwenden, geben Sie den Befehl *scwcmd configure /p:<Pfad zur XML-Datei>* ein. Mit diesem Hilfsmittel können Sie zum Beispiel eine Batchdatei schreiben, die eine bestimmte Richtlinie anwendet.

Um eine Sicherheitsrichtlinie auf einem Remotecomputer ausführen zu können, verwenden Sie am besten das Befehlszeilentool Scwcmd. Geben Sie dazu in der Eingabeaufforderung den folgenden Befehl ein:

```
scwcmd configure /m:<IP oder Name des Remoteservers> /p: <Pfad zur XML-Datei>
```

Geben Sie in der Eingabeaufforderung *scwcmd configure* ein, erhalten Sie weitere Informationen über die Anwendung des Sicherheitskonfigurations-Assistenten über die Eingabeaufforderung.

Haben Sie auf einem Server eine Sicherheitsrichtlinie angewendet, sehen Sie zunächst keine Änderung. Eine Analyse führen Sie wieder am besten mit dem Befehlszeilentool Scwcmd durch. Geben Sie dazu in der Eingabeaufforderung den folgenden Befehl ein:

```
scwcmd analyze /m:<Server-IP oder -Name> /p:<Pfad zur Richtliniendatei> /o:<Ausgabeordner
der Analyse>
```

Die Analyse erstellt eine XML-Datei, welche die Änderung der Richtlinie enthält.

Haben Sie die Datei erstellt, können Sie entweder die XML-Datei betrachten oder über den Befehl *scwcmd view /x:<Name der erstellten XML-Datei>* die Anzeige durch den SCW formatieren und anzeigen lassen.

Wollen Sie die Ausführung einer Sicherheitsrichtlinie wieder vollständig zurücknehmen, können Sie entweder wieder über die grafische Oberfläche die Maßnahme durchführen oder über die Eingabeaufforderung die Sicherheitsrichtlinie zurücknehmen. Wollen Sie die Sicherheitsrichtlinie über die grafische Oberfläche zurücknehmen, starten Sie den Sicherheitskonfigurations-Assistenten. Wählen Sie die Option *Rollback für letzte angewendete Sicherheitsrichtlinie durchführen*. In diesem Fall wird die letzte Sicherheitsrichtlinie komplett zurückgenommen. Haben Sie zuvor keine Sicherheitsrichtlinie durchgeführt, erhalten Sie exakt den Stand vor der Einführung der Richtlinie.

Alternativ können Sie auch eine Sicherheitsrichtlinie in der Eingabeaufforderung zurücknehmen. Geben Sie dazu in der Eingabeaufforderung den folgenden Befehl ein:

```
scwcmd rollback /m:<Server-IP oder -Name>
```

Zusammenfassung

In diesem Kapitel haben wir Ihnen verschiedene Möglichkeiten in Windows Server 2012 zur Überwachung der eigenen Systemleistung aufgezeigt. Neben den Bordmitteln in Windows Server 2012 haben wir Ihnen auch verschiedene Zusatztools gezeigt, mit denen Sie Server überwachen.

Auch den Sicherheitskonfigurations-Assistenten haben wir in diesem Kapitel behandelt und die Aufgabenplanung sowie die Ereignisanzeige waren ebenfalls Thema dieses Kapitels.

Das nächste Kapitel beschäftigt sich mit den Windows-Bereitstellungsdiensten in Windows Server 2012.

Teil I

Windows-Bereitstellung und PowerShell

Kapitel 39

Windows-Bereitstellungsdienste

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen die Möglichkeiten, um Windows 8/8.1 und Windows Server 2012 R2 zentral im Unternehmen bereitzustellen. Microsoft bietet dazu einige neue Tools, zum Beispiel das Windows Assessment and Deployment Kit. Dieses arbeitet auch mit Windows Server 2012 R2 und den Windows-Bereitstellungsdiensten zusammen.

Windows Assessment and Deployment Kit (ADK)

Um Windows 8/8.1 im Unternehmen bereitzustellen, stellt Microsoft das Windows Assessment and Deployment Kit (ADK) zur Verfügung. Dieses stellt den Nachfolger des Windows Automated Installation Kit (WAIK) dar. Das Toolkit bietet neue Werkzeuge und neue Funktionen, um Windows 8/8.1 mit seinen neuen Möglichkeiten im Unternehmen zur Verfügung zu stellen.

Microsoft stellt das ADK kostenlos zur Verfügung (*http://www.microsoft.com/de-de/download/details.aspx?id=30652* [Ms179-K39-01]). Das ADK unterstützt auch die Bereitstellung von Windows Server 2012 R2, Windows Server 2008/2008 R2 und auch von Windows 7/8/8.1. Zusätzlich haben Sie die Möglichkeit, WIM-Dateien und andere Abbilder über die Windows-Bereitstellungsdienste in Windows Server 2012 R2 zu verteilen.

Grundlagen der Bereitstellung von Windows 8/8.1

Mit Windows 8/8.1 stellt Microsoft auch zahlreiche kostenlose Zusatztools zur Verfügung, über die sich das Betriebssystem effizient im Unternehmen verteilen lässt. In diesem Abschnitt zeigen wir Ihnen die wichtigsten Möglichkeiten und Techniken. Um Windows 8/8.1 in Unternehmen zu verteilen, unterstützt Microsoft Administratoren mit dem Windows Assessment and Deployment Kit (ADK), dem Nachfolger des Windows Automated Installation Kit (WAIK).

WAIK ist optimiert für Windows 7 und Windows Server 2008 R2, das ADK kann Windows 8/8.1 und Windows Server 2012 R2 bereitstellen, aber auch Windows 7/8/8.1 und Windows Server 2008/2008 R2. Dieses kostenlose Werkzeug stellt eine Umgebung bereit, mit der auch Installationen in großen Stückzahlen ausgerollt werden können.

Das Windows-Imageformat

Windows 8/8.1 arbeitet weiterhin mit dem WIM-Imageformat (Windows Imaging). Statt eines sektorbasierten Imageformats ist das WIM-Format dateibasiert. Dies hat mehrere Vorteile. WIM ist hardwareunabhängig. Das bedeutet, Administratoren müssen nur ein Image für verschiedene Hardwarekonfigurationen erstellen. Mit WIM lassen sich mehrere Images in einer zentralen Datei speichern.

Außerdem nutzt WIM eine Kompression und das Single-Instance-Verfahren, womit sich 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, sorgt Single-Instancing dafür, dass Datei A nur einmal tatsächlich gespeichert wird.

WIM-Images ermöglichen die Offlinebearbeitung von Images. So können Administratoren Betriebssystemkomponenten, Patches und Treiber hinzufügen oder löschen, ohne ein neues Image erstellen zu müssen. Windows 8/8.1 stellt eine Programmierschnittstelle (API) für das WIM-Imageformat zur Verfügung, die WIMGAPI. Auch dieses Tool ist Bestandteil des ADK.

Diese kann von Entwicklern für die Arbeit mit WIM-Imagedateien genutzt werden. In Kombination mit Windows PE lassen sich diese Images auch erweitern oder ändern, ohne dass Windows dazu komplett gestartet sein muss. So ist es beispielsweise möglich, einen Treiber auszutauschen, ohne das Administratorenimage komplett neu erstellen müssen.

Windows Systemabbild-Manager, Antwortdateien und Kataloge

Der Windows Systemabbild-Manager (Windows System Image Manager, Windows-SIM) ist ein Tool, mit dem Administratoren auf einfache Weise Antwortdateien auf XML-Basis erstellen. Das Tool ist Bestandteil des ADK. Auch Netzwerkfreigaben lassen sich so konfigurieren, dass diese Konfigurationen zur Verteilung von Windows 8/8.1 und zusätzliche Treiber enthalten.

Die Antwortdatei enthält das Grundgerüst, das Windows für die einzelnen Konfigurationsphasen benötigt. Dadurch lassen sich Eingaben wie PC-Namen, Product Keys und weitere Eingaben in einer Datei vorgeben, sodass während der Installation keinerlei Eingaben mehr notwendig sind. Die Katalogdatei eines Image (*.clg*) enthält die Einstellungen und Pakete, die in einem Image auf WIM-Basis enthalten sind.

Auch wenn die normale Installation von Windows 8/8.1 auf einem WIM-Image basiert, finden Sie auf der Windows 8/8.1-Installations-DVD im Ordner *\sources* keine *.clg*-Dateien der verschiedenen Windows-Editionen mehr. Das war in Windows 7 noch anders. Sie können aber Katalogdateien schnell und einfach mit dem Systemabbild-Manager erstellen. Die Standardinstallationsdatei *install.wim* finden Sie weiterhin in diesem Ordner, auch die Windows PE-Bootumgebung *boot.wim*.

WIM-Images haben als Dateityp die Bezeichnung *.wim*. In diesen Dateien ist festgelegt, welche Komponenten Windows 8/8.1 bei den einzelnen Windows 8/8.1-Editionen installiert. Windows 8/8.1-Antwortdateien speichern Sie am besten als *AutoUnattend.xml*. Beim Starten der Installation durchsucht Windows 8/8.1 standardmäßig den Stammordner von Laufwerken, auch USB-Sticks, nach einer Datei *AutoUnattend.xml* und verwendet die hinterlegten Antworten zur Installation.

Windows ADK – Grundlagen

Das ADK enthält kostenlose Werkzeuge, mit denen Sie automatisierte Installationspakete von Windows 8/8.1 erstellen und verteilen können. Sie können mit dem ADK aber auch Windows Server 2012 R2 sowie die Vorgängerversionen Windows 7/8/8.1 und Windows Server 2012 R2 bereitstellen. Auch Windows Server 2008 ist kompatibel mit dem ADK, allerdings nicht Windows Vista. Das Toolkit kann PCs im Netzwerke auch auf ausreichende Leistung hin untersuchen, die eine Migration zu Windows 8/8.1 ermöglichen. Bestandteil sind vor allem die folgenden Tools:

- Application Compatibility Toolkit analysiert Anwendungen im Netzwerk und den einzelnen PCs auf Kompatibilität mit Windows 8/8.1. ACT benötigt eine Datenbank. Im Download des ADK ist die kostenlose Datenbank SQL Server 2012 Express Edition integriert.

- Abbildverwaltung für die Bereitstellung (DISM), Windows System Image Manager (SIM), OSCDIMG, BCDBoot, DISMAPI, WIMGAPI und weitere Tools für das Erstellen von Images und Antwortdateien
- Windows Preinstallation Environment (Windows PE) zum Booten von Windows 8/8.1 und der anschließenden Installation
- User State Migration Tool (USMT) zur Übernahme der Benutzerprofile und Benutzerdaten auf den PCs. Im Gegensatz zu den anderen Tools kann das USMT auch Daten von Windows XP-Computern zu Windows 8/8.1 übernehmen.
- Volume Activation Management Tool (VAMT) dient der zentralen Verwaltung der Windows-Aktivierung
- Windows Assessment Toolkit hilft bei der Leistungsüberwachung von Computern
- Windows Assessment Services helfen bei der Einstellung von Images und Inventuren in Testumgebungen

Das ADK unterstützt auch den neuen UEFI-Standard, wie Windows 8/8.1 auch. Verwenden Sie in diesem Fall OSCDIMG mit der Option *–b*, um ISO-Dateien mit dem *Efisys_noprompt.bin*-Bootsektor zu verwenden (*–bC:\Efisys_noprompt.bin*).

Die Option */s* des Tools BCDBoot verwenden Sie zum Erstellen von bootfähigen USB-Sticks oder externen Festplatten. BCDBoot kopiert Bootdateien auf die EFI-Partition.

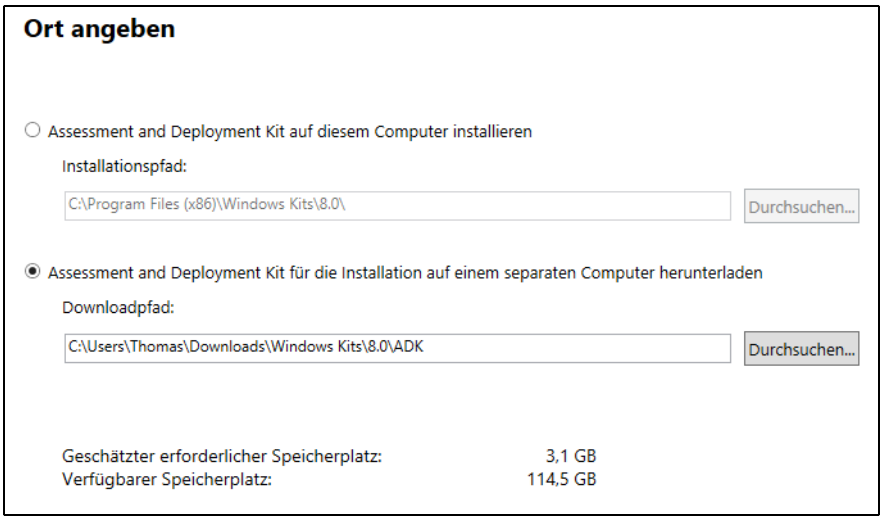
Windows Assessment and Deployment Kit installieren

Wie beim Windows Automated Installation Toolkit (WAIK) handelt es sich beim Windows Assessment and Deployment Kit (ADK) um eine Sammlung verschiedener Programme, die Administratoren dabei helfen sollen, Windows 8/8.1 für die automatisierte Bereitstellung vorzubereiten. Sie laden dazu zunächst die Installationsdatei von der Seite *http://www.microsoft.com/de-de/download/details.aspx?id=30652* [Ms179-K39-02].

Die Installationsdatei lädt weitere Dateien aus dem Internet. Das ADK benötigt .NET Framework 4.0, welches der Assistent aber automatisch auf dem entsprechenden Rechner installiert. Nach dem Download starten Sie die Datei *adksetup.exe* über einen Doppelklick. Bestätigen Sie anschließend die Fenster des Assistenten und lassen Sie die Installationsdateien herunterladen.

Starten Sie die Installation, sollten Sie aber nicht die Option *Assessment and Deployment Kit auf diesem Computer installieren* auswählen, sondern *Assessment and Deployment Kit für die Installation auf einem separatem Computer herunterladen*. Das hat den Vorteil, dass das Tool die entsprechenden Dateien herunterlädt und Sie im Benutzerprofil im *Downloads*-Ordner die vollständigen Installationsdateien des ADK vorfinden. Diese können Sie dann später jederzeit wieder installieren, ohne erneut Dateien herunterladen zu müssen. Sie können die Installation aber auch direkt starten und die Installation über das Internet durchführen lassen.

Abbildg. 39.1 Download des ADK in einen separaten Ordner



Die Installation der verschiedenen Komponenten des ADK erfordert mindestens Windows 7, besser Windows 8/8.1. Die Installation ist aber auch auf Windows Server 2012 R2 möglich.

Sie können das ADK auch skriptbasiert über die Eingabeaufforderung installieren. Dazu verwenden Sie den folgenden Befehl:

```
adksetup /quiet /installpath <Installations-Pfad> /features <ID1><ID2>
```

Um sich eine Liste aller verfügbaren IDs der verschiedenen Features anzeigen zu lassen, geben Sie in der Eingabeaufforderung den Befehl *adksetup /list*. Alle Optionen zur unbeaufsichtigten Installation finden Sie auf der Seite *http://msdn.microsoft.com/de-de/library/hh825494* [Ms179-K39-03].

Nach der Installation finden Sie die verschiedenen Programme und Tools zunächst auf der Startseite. Die Tools und Beispiele sind darüber hinaus im Ordner *C:\Programme(x86)\Windows Kits\8.0* zu finden.

Automatisierte Installation von Windows 8/8.1

Um eine Antwortdatei oder ein vorgefertigtes Bootmedium für die Installation von Windows 8/8.1 bereitzustellen, installieren Sie zunächst das Windows ADK, wie zuvor beschrieben. Auf der Startseite finden Sie die Kachel *Umgebung für Bereitstellungs- und Imageerstellungstools*. Ein Klick darauf startet eine Eingabeaufforderung mit den wichtigsten Tools. Starten Sie diese am besten über die App-Leiste mit Administratorrechten.

Vorbereiten und Erstellen einer Windows PE-CD

Wollen Sie eine Windows PE-CD erstellen, um Computer im Netzwerk mit der neuen PE-Umgebung zu booten, verwenden Sie das ADK. Mit den folgenden Schritten erstellen Sie ein Bootmedium, mit dem Sie Windows 8/8.1 installieren können:

Installieren Sie das ADK und kicken Sie auf der Startseite auf die Kachel *Umgebung für Bereitstellungs- und Imageerstellungstools*. Führen Sie den Befehl *copype.cmd <Systemvariante> <Ordner>* aus. Als Systemvariante können Sie entweder *x86* oder *amd64* verwenden, abhängig davon, welches System Sie einsetzen. Als Ordner geben Sie einen beliebigen Ordner auf der Festplatte des Admin-PC an, zum Beispiel *copype amd64 C:\winpe_amd64*. Den Ordner müssen Sie vorher nicht erstellen, der Assistent erstellt diesen automatisch und legt die Dateien im Anschluss in diesem Ordner ab.

Der nächste optionale Schritt besteht darin, die Grundstruktur der Windows PE-Version noch etwas auszubauen. Sie können in Windows PE weitere Treiber hinzufügen, es sind allerdings bereits zahlreiche Treiber in das System integriert. Dazu müssen Sie das Image öffnen und mit Daten füllen. Die Bootumgebung baut auf der Datei *boot.wim* auf. Diese findet sich im Ordner *C:\winpe_amd64\media\sources*.

Zum Öffnen und Mounten verwenden Sie das Windows-Tool DISM. Nutzen Sie dazu die bereits geöffnete Eingabeaufforderung für die Bereitstellungstools und geben Sie den folgenden Befehl ein:

```
dism /mount-image /imagefile:c:\winpe_amd64\media\sources\boot.wim /index:1 /
mountdir:C:\winpe_amd64\mount
```

Abbildg. 39.2 Mounten eines Windows PE-Images

```
C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Pr
einstallation Environment\amd64\Media\sr-latn-cs\bootmgr.efi.mui
C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Pr
einstallation Environment\amd64\Media\sv-se\bootmgr.efi.mui
C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Pr
einstallation Environment\amd64\Media\tr-tr\bootmgr.efi.mui
C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Pr
einstallation Environment\amd64\Media\uk-ua\bootmgr.efi.mui
C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Pr
einstallation Environment\amd64\Media\zh-cn\bootmgr.efi.mui
C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Pr
einstallation Environment\amd64\Media\zh-hk\bootmgr.efi.mui
C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Pr
einstallation Environment\amd64\Media\zh-tw\bootmgr.efi.mui
186 Datei(en) kopiert
        1 Datei(en) kopiert.
        1 Datei(en) kopiert.
        1 Datei(en) kopiert.

Success


C:\winpe_amd64>Dism /mount-image /imagefile:c:\winpe_amd64\media\sources\boot.wi
m /index:1 /mountdir:C:\winpe_amd64\mount

Tool zur Abbildverwaltung für die Bereitstellung


Abbild wird bereitgestellt
[==========================100.0%==========================]
Der Vorgang wurde erfolgreich beendet.

C:\winpe_amd64>_
```

Wollen Sie bestimmte Treiber in das System einbinden, geben Sie den Ordner an, in dem sich die *.inf*-Datei des Treibers befindet, zum Beispiel mit dem Befehl:

```
dism /image:C:\winpe_amd64\mount /Add-Driver /Driver:C:\Treiber\avm\fwusbn64.inf
```

Anschließend integriert der Befehl das Treiberpaket in das gemountete Image.

Abbildg. 39.3 Treiber in Images integrieren

```
C:\winpe_amd64>Dism /image:C:\winpe_amd64\mount /Add-Driver /Driver:C:\Treiber\a
vm\fwusbn64.inf

Tool zur Abbildverwaltung für die Bereitstellung



Found 1 driver package(s) to install.
Installing 1 of 1 - C:\Treiber\avm\fwusbn64.inf: The driver package was successf
ully installed.
Der Vorgang wurde erfolgreich beendet.
```

Neben Treibern können Sie aber auch weitere Pakete in Windows PE integrieren, zum Beispiel um zusätzliche Befehle und Funktionen zur Verfügung zu stellen. Hilfreich sind Komponenten aus dem ADK, um Windows 8/8.1 konfigurieren zu können. Auch das Windows Recovery Environment können Sie integrieren:

```
dism /Image:C:\winpe_amd64\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WinReCfg.cab"
dism /Image:C:\winpe_amd64\mount /Add-Package /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\de-de\WinPE-WinReCfg_de-de.cab"
```

Abbildg. 39.4 Integrieren der Windows 8/8.1-Wiederherstellungsumgebung in Windows PE

```
C:\winpe_amd64>Dism /Image:C:\winpe_amd64\mount /Add-Package /PackagePath:"C:\Pr
ogram Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Preinst
allation Environment\amd64\WinPE_OCs\WinPE-WinReCfg.cab"

Tool zur Abbildverwaltung für die Bereitstellung



Processing 1 of 1 - Adding package WinPE-WinReCfg-Package~31bf3856ad364e35~amd64

[==========================100.0%==========================]
Der Vorgang wurde erfolgreich beendet.

C:\winpe_amd64>Dism /Image:C:\winpe_amd64\mount /Add-Package /PackagePath:"C:\Pr
ogram Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Preinst
allation Environment\amd64\WinPE_OCs\de-de\WinPE-WinReCfg_de-de.cab"

Tool zur Abbildverwaltung für die Bereitstellung



Processing 1 of 1 - Adding package WinPE-WinReCfg-Package~31bf3856ad364e35~amd64

[==========================100.0%==========================]
Der Vorgang wurde erfolgreich beendet.

C:\winpe_amd64>_
```

Fügen Sie Pakete hinzu, müssen Sie immer zuerst das Paket integrieren und anschließend das entsprechende Sprachpaket.

Haben Sie alle notwendigen Pakete und Treiber integriert, schließend Sie das Image und heben die Bereitstellung auf. Im Befehl speichern Sie dann auch die von Ihnen vorgenommenen Änderungen im Image:

```
dism /unmount-image /mountdir:C:\winpe_amd64\mount /commit
```

Abbildg. 39.5 Speichern und Unmounten eines Windows 8/8.1-Images

```
C:\winpe_amd64>Dism /unmount-image /mountdir:C:\winpe_amd64\mount /commit

Tool zur Abbildverwaltung für die Bereitstellung


Abbild wird gespeichert
[==========================100.0%==========================]
Bereitstellung des Abbilds wird aufgehoben
[==========================100.0%==========================]
Der Vorgang wurde erfolgreich beendet.
```

Anschließend können Sie einen bootfähigen USB-Stick oder eine ISO-Datei erstellen. Einen USB-Stick erstellen Sie mit dem Befehl

```
MakeWinPEMedia /UFD C:\winpe_amd64 <Laufwerksbuchstabe>:
```

Um eine ISO-Datei zu erstellen, verwenden Sie:

```
MakeWinPEMedia /ISO C:\winpe_amd64 c:\winpe_amd64\winpe.iso
```

Sie können jetzt beliebige Computer mit diesem Medium booten.

Abbildg. 39.6 Erstellen einer ISO-Datei auf Basis eines Windows PE-Mediums

```
C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment
 Tools>MakeWinPEMedia /ISO C:\winpe_amd64 c:\winpe_amd64\winpe.iso
Creating c:\winpe_amd64\winpe.iso...

100% complete

Success
```

Eine interessante Neuigkeit in Windows 8/8.1 und Windows Server 2012 R2 ist die Möglichkeit, mit DISM auch virtuelle Festplatten (*.vhd* und *.vhdx*) mounten zu können. Die Syntax dazu lautet:

```
dism /Mount-Image /ImageFile:"c:\win8.vhd" /Index:1 /MountDir:"c:\temp\Mount"
```

Ebenfalls neu ist die Option */List-Image*. Diese kann den Inhalt eines Images anzeigen, also die enthaltenen Dateien und Ordner.

Zur Anzeige und zum Entfernen von installierten Paketen nutzen Sie die folgenden Aufrufe:

- dism /image:<Name> /Get-Packages Zeigt die installierten Pakete an
- dism /image:<Name> /Remove-Package /PackageName: <Paket> Entfernt installierte Pakete

Erstellen einer Antwortdatei zur automatisierten Installation von Windows 8/8.1

In diesem Abschnitt zeigen wir Ihnen in mehreren Schritten, wie Sie eine automatisierte Installation von Windows 8/8.1 über eine Antwortdatei erstellen können. Nach der Installation des ADK finden Sie Beispielantwortdateien im Ordner *C:\Program Files (x86)\Windows Kits\8.0\Assessment and*

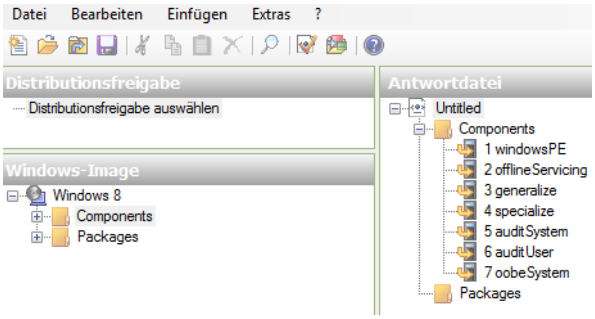
Deployment Kit\Deployment Tools\Samples\Unattend. Zunächst zeigen wir Ihnen, wie Sie eine Antwortdatei erstellen, um Windows automatisiert zu installieren:

1. Installieren Sie das ADK auf einem Computer.
2. Kopieren Sie die Datei *install.wim* von der Windows 8/8.1-DVD aus dem Ordner *\sources* in einen temporären Ordner auf der Festplatte, zum Beispiel *C:\unattend*.
3. Starten Sie über die Windows-Startseite *Windows System Image Manager*.
4. Öffnen Sie über *Datei/Windows-Abbild auswählen* die zuvor kopierte Datei *install.wim* auf der Festplatte.
5. Wählen Sie aus, welche Windows 8/8.1-Edition Sie installieren wollen.
6. Bestätigen Sie das Erstellen einer neuen Katalogdatei. Das Paket wird jetzt eingelesen und im Windows System Image Manager angezeigt. Das Erstellen des Katalogs kann einige Zeit dauern.

Abbildg. 39.7 Erstellen einer Katalogdatei und Laden eines Images

7. Anschließend starten Sie die Erstellung einer neuen Antwortdatei über *Datei/Neue Antwortdatei*.
8. Die Antwortdatei wird mit ihren verschiedenen Bereichen in der Mitte des Fensters angezeigt. Die Bereiche stellen die verschiedenen Phasen während der Installation dar.

Abbildg. 39.8 Windows System Image Manager mit eingebundenem Abbild und erstellter Antwortdatei

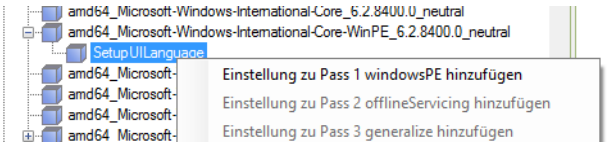


Erweitern Sie im Bereich *Windows-Image* den Knoten *Components*. Hier können Sie verschiedene Einstellungen vornehmen, um die Installation an Ihre Bedürfnisse anzupassen. Die wichtigsten Beispiele zeigen wir Ihnen in der nachfolgenden Anleitung.

Klicken Sie hierzu mit der rechten Maustaste auf die Komponente, und wählen Sie die gewünschte Konfigurationsphase aus. So wird die Komponente der Antwortdatei in der Phase der Windows-Installation hinzugefügt. Wir gehen in den nachfolgenden Beispielen von der Erstellung einer 64-Bit-Antwortdatei aus. Hier haben die Einstellungen das Präfix *amd64*. Die 32-Bit-Version von Windows 8/8.1 verwendet an dieser Stelle *x86*.

Klicken Sie unterhalb von *amd64_Microsoft-Windows-International-Core-WinPE_...* mit der rechten Maustaste auf *SetupUILanguage* und wählen Sie im Kontextmenü den Eintrag *Einstellung zu Pass 1 windowsPE* hinzufügen.

Abbildg. 39.9 Hinzufügen der ersten Komponente zur automatisierten Installation

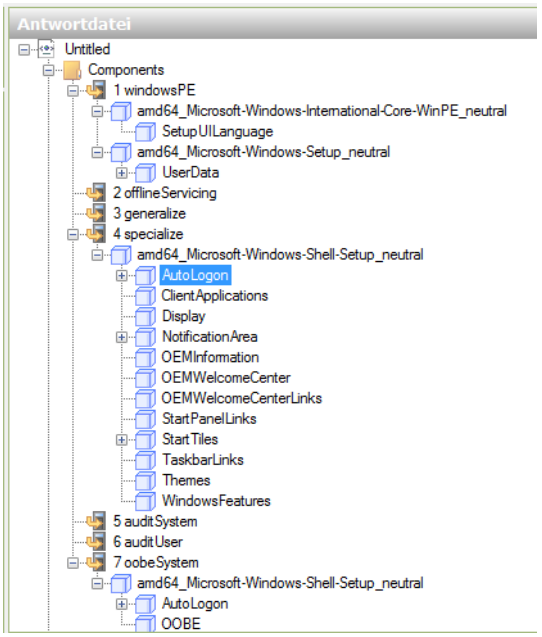


Anschließend fügen Sie noch den Bereich *amd64_Microsoft-Windows-Setup/UserData* zum gleichen Bereich hinzu.

Die drei Bereiche *amd64_Microsoft-Windows-Shell-Setup/OOBE* (zu Bereich 7), *amd64_Microsoft-Windows-Shell-Setup\AutoLogon* (zu Bereich 7) und *amd64_Microsoft-Windows-Shell-Setup* (zu Bereich 4) fügen Sie ebenfalls hinzu.

Im Bereich 4 bei der Antwortdatei können Sie über die rechte Maustaste alles unterhalb *amd64_Microsoft-Windows-Shell-Setup_neutral* löschen, den Hauptpunkt *amd64_Microsoft-Windows-Shell-Setup_neutral* aber nicht.

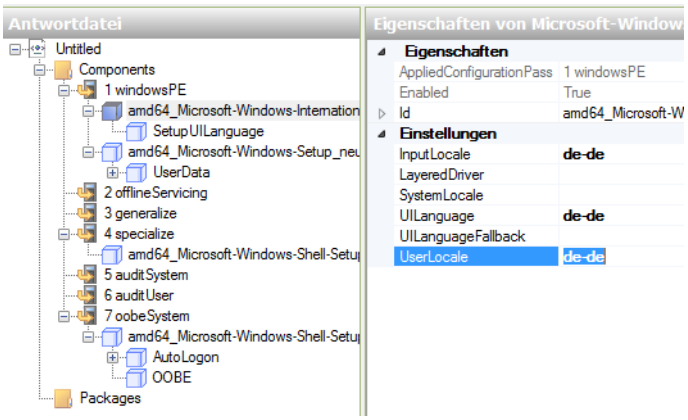
Abbildg. 39.10 Verwalten der Komponenten einer Antwortdatei



Anschließend füllen Sie die verschiedenen Bereiche der Antwortdatei mit den Daten, die für die Installation notwendig sind. Sie können auf diesem Weg weitere Optionen zur Antwortdatei hinzufügen. Wir gehen in diesem Beispiel nur auf einige wenige Möglichkeiten ein. Klicken Sie auf *amd64_Microsoft-Windows-International-Core-WinPE* in der Antwortdatei. Hier nehmen Sie jetzt Einstellungen für die Komponenten vor.

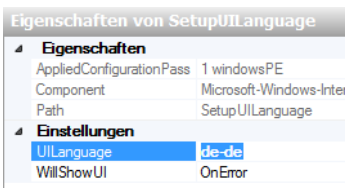
Hier werden die Spracheinstellungen unterhalb des Bereichs Einstellungen gesetzt. Dabei spielen die Werte *InputLocale* (Eingabe während der Installation), *SystemLocale* (Standardsprache der Programme), *UILanguage* (Standardsprache der Benutzeroberfläche) und *UserLocale* (Benutzereinstellung für Datum, Zeit, Währung und Zahlen) eine wichtige Rolle. Tragen Sie bei diesen Werten jeweils *de-de* ein.

Abbildg. 39.11 Einstellen der Spracheinstellungen des Betriebssystems



Klicken Sie dann im Bereich *Antwortdatei* auf den Wert *SetupUILanguage*. 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.

Abbildg. 39.12 Festlegen der Sprache während der Installation

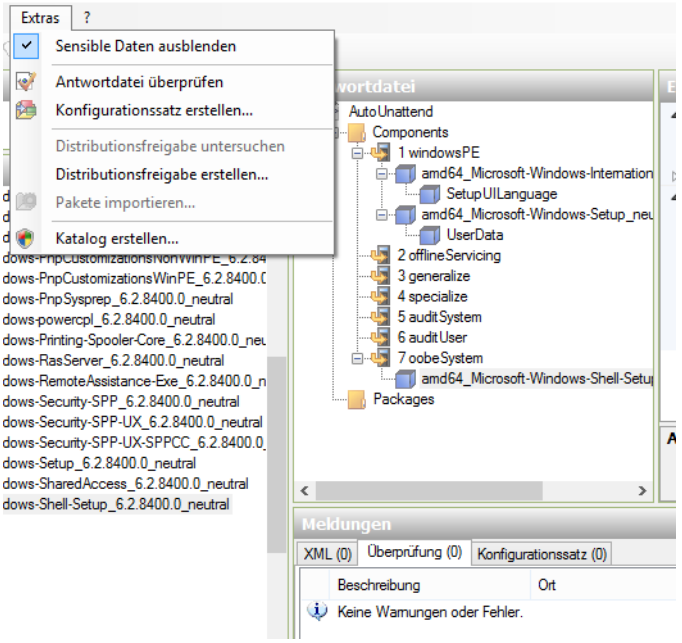


Danach passen Sie weitere Einstellungen an:

1. Klicken Sie im Bereich *Antwortdatei* auf *UserData*. 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.
2. Klicken Sie danach im Bereich *Antwortdatei* unterhalb von *UserData* auf *ProductKey*. In den Einstellungen können Sie den Produktschlüssel von Windows 8/8.1 eintragen und bei *WillShowUI* wiederum *OnError*. Klicken Sie nun auf *amd64_Microsoft-Windows-Shell-Setup_neutral* im Bereich 4. Bei *ComputerName* tragen Sie den Namen des Computers ein.

3. Klicken Sie als Nächstes auf *amd64_Microsoft-Windows-Shell-Setup_neutral* im Bereich 7. Unter *TimeZone* tragen Sie *W. Europe Standard Time* ein.
4. Klicken Sie jetzt auf *AutoLogon* im Bereich 7.
5. Bei *Enabled* tragen Sie *true* ein. Bei *LogonCount* setzen Sie den Wert mindestens auf 1. Tragen Sie hier den Wert 2 ein, werden die ersten zwei Anmeldungen automatisch durchgeführt. Bei *Username* tragen Sie *Administrator* ein.
6. Klicken Sie dann im Bereich *Antwortdatei* unterhalb von *AutoLogon* auf *Password* und geben dann im rechten Bereich das Kennwort unter *Value* an.
7. Klicken Sie im Bereich Antwortdatei auf *OOBE*. Diese Option steht für die »Out of the Box Experience«, das Verhalten des Betriebssystems direkt nach der Installation.
8. Anschließend werden die Werte für *OOBE* auf der rechten Seite gepflegt. *HideEULAPage* wird auf *true* gesetzt. Unter *NetworkLocation* (Netzwerkstandort) wählen Sie entweder *Home* oder *Work* aus.
9. Bei *ProtectYourPC* wird das Sicherheitsverhalten festgelegt (1 = Empfohlene Einstellungen, 2 = Nur automatische Updates aktivieren, 3 = Schutz deaktivieren).
10. Im Anschluss daran überprüfen Sie die Antwortdatei über *Extras/Antwortdatei überprüfen* auf eventuelle Fehler.
11. Im Bereich *Meldungen* dürfen keine Fehler erscheinen.

Abbildg. 39.13 Antwortdateien lassen sich auf Konsistenz überprüfen



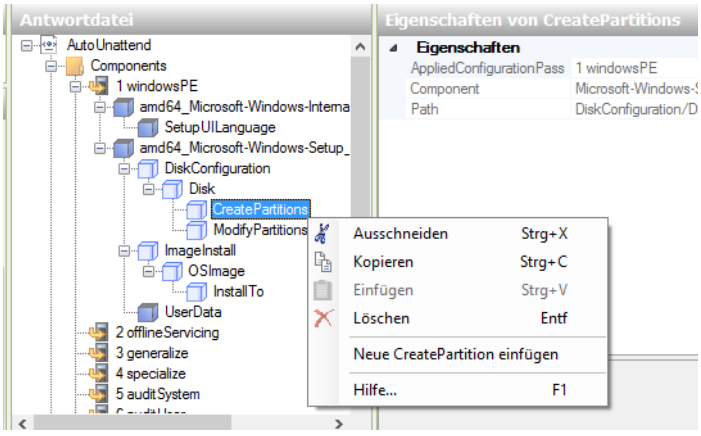
Speichern Sie Antwortdatei über *Datei/Antwortdatei speichern* als *AutoUnattend.xml* ab. Die Erstellung der Datei ist damit abgeschlossen.

Speichern Sie die Datei auf einem USB-Stick und verbinden diesen mit dem Rechner, auf dem Sie Windows 8/8.1 mit der Datei automatisiert installieren wollen. Sie können die Antwortdatei aber auch in den Windows-Bereitstellungsdiensten verwenden. Booten Sie von der Windows 8/8.1-DVD, verwendet der Setup-Assistent die Antwortdatei zur automatisierten Installation. Sie können natürlich zur Installation auch einen USB-Stick verwenden.

Wollen Sie nicht nur die Windows-Installation automatisieren, sondern auch die Partitionierung, also die Aufteilung der physischen Festplatte in mehrere logische Teile, können Sie auch diese Vorgaben in der Antwortdatei hinterlegen:

1. Öffnen Sie die erstellte Antwortdatei *AutoUnattend.xml* im Windows-Systemabbild-Manager.
2. Erweitern Sie im Bereich *Windows-Image* die Komponente *amd64_Microsoft-Windows-Setup_neutral* und dann *DiskConfiguration*.
3. Klicken Sie mit der rechten Maustaste auf *Disk*, und fügen Sie diesen Wert dem Bereich *1* hinzu.
4. Fügen Sie dann noch die Option *InstallTo* unter *amd64_Microsoft-Windows-Setup_neutral/ImageInstall/OSImage* zum Bereich 1 hinzu.
5. Die hinzugefügten Werte konfigurieren Sie jetzt wieder im Bereich *Antwortdatei*. Klicken Sie mit der rechten Maustaste auf *CreatePartitions*, und wählen Sie im Kontextmenü den Eintrag *Neue CreatePartition* einfügen aus. Den Befehl können Sie so oft wiederholen, wie Sie Windows-Partitionen auf dem Rechner automatisch erstellen wollen.

Abbildg. 39.14 Erstellen von neuen Partitionen über die Antwortdatei von Windows 8/8.1



Klicken Sie mit der rechten Maustaste auf *ModifyPartitions*, und wählen Sie im Kontextmenü den Eintrag *Neue ModifyPartition* einfügen. Den Befehl müssen Sie so oft wiederholen, wie es Partitionen auf dem Computer geben soll. Wollen Sie eine Konfiguration mit zwei Partitionen, fügen Sie der Antwortdatei eine zweite Komponente *CreatePartition* und eine zweite Komponente *ModifyPartition* hinzu, indem Sie im Bereich *Windows-Image* mit der rechten Maustaste auf die Komponente klicken und anschließend die entsprechende Konfigurationsphase auswählen:

1. Klicken Sie dann auf *DiskConfiguration* und legen für den Wert *WillShowUI* wieder *OnError* fest.
2. Klicken Sie dann auf *Disk*. Beim Wert *DiskID* tragen Sie *0* ein. Windows wird dann auf der ersten Festplatte im Computer installiert. Mit *true* bei *WillWipeDisk* wird vor der Installation der Inhalt der Festplatte gelöscht.

3. Klicken Sie im mittleren Bereich auf *CreatePartition* unterhalb von *CreatePartitions*. Mit dem Wert *Extend* legen Sie im Gegensatz zu *true* mit *false* fest, dass der Assistent die Partition nicht auf gesamte Festplattengröße erweitert. Bei *Size* geben Sie den Wert in Megabyte ein, wenn Sie nicht die ganze Festplatte bei *Extend* verwenden, also *true* eintragen. Mit *Type* legen Sie die Art der Partition fest, bei der ersten am besten *Primary*. Bei *Order* tragen Sie 1 ein.
4. Als Nächstes klicken Sie den Eintrag *ModifyPartition* unterhalb von *ModifyPartitions* an. Hier konfigurieren Sie die erstellte Partition noch genauer. Der Wert *Active* setzt mit *true* die Partition auf aktiv, nur so kann Windows 8/8.1 von der Partition starten. Wird *Extend* auf *true* gesetzt, verwendet Windows die gesamte Platte.
5. Die Option *Format* mit dem Wert *NTFS* legt das Dateisystem fest.
6. Mit *Label* können Sie den Namen des Laufwerks auf einen beliebigen Wert setzen.
7. Mit *Letter* konfigurieren Sie den Laufwerkbuchstaben, also am besten *C*.
8. *Order* auf *1* gibt die Reihenfolge an, in der die Partition angepasst werden soll, wenn Sie mehrere Partitionen erstellen lassen.
9. *PartitionID* mit dem Wert *1* legt die ID der Partition fest, welche modifiziert werden soll.
10. Nun klicken Sie im Bereich *Antwortdatei* auf *OSImage*.
11. Bei *InstallToAvaiablePartition* tragen Sie *false* ein. Dann verwendet der Assistent nicht die erste verfügbare Festplatte zur Installation des Betriebssystems, sondern die in der Antwortdatei konfigurierte Partition (siehe nächster Schritt). Bei *WillShowUI* aktivieren Sie wieder *OnError*.
12. Klicken Sie dann im Bereich *Antwortdatei* auf *InstallTo*. Hier legen Sie fest, auf welcher Festplatte Windows 8/8.1 installiert werden soll. Daher ist der Wert bei *DiskID* 0, was die erste Festplatte im PC darstellt. Tragen Sie bei *PartitionID* den Wert 1 ein, also die erste Partition auf der ersten Platte.
13. Anschließend überprüfen Sie die Antwortdatei erneut über *Extras* und speichern anschließend wieder.

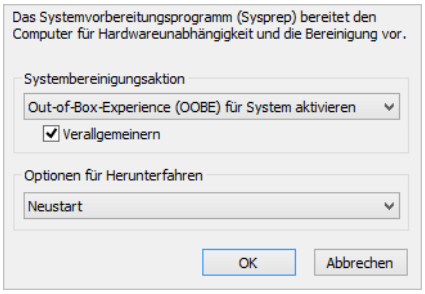
Wollen Sie Windows 8/8.1 mit der erstellten Antwortdatei installieren, benötigen Sie eine Windows 8/8.1-DVD, die Sie in das DVD-Laufwerk des Rechners einlegen, oder einen bootfähigen USB-Stick. Sie müssen sicherstellen, dass der Computer von diesem Laufwerk bootet.

Neben den beschriebenen Möglichkeiten, eine Antwortdatei zu erstellen, haben Sie bei der Verwendung eines bootfähigen USB-Sticks zur Installation noch die Möglichkeit, einen Konfigurationssatz über das Menü *Extras* im Windows-SIM zu erstellen. Dieser enthält neben der Antwortdatei noch zusätzliche Treiber und Pakete, die der Installations-Assistent später installieren soll. Wählen Sie an dieser Stelle am besten einen Ordner auf dem USB-Stick aus. Die weiteren Schritte zeigen wir Ihnen nachfolgend:

1. Schalten Sie den Computer ein, legen Sie die Windows 8/8.1-Produkt-DVD in das Laufwerk, und schließen Sie den USB-Stick an, der die Antwortdatei enthält (*AutoUnattend.xml*). Schließen Sie den USB-Stick an einem der primären USB-Anschlüsse des Computers an. Diese befinden sich meistens auf der Rückseite. Alternativ befindet sich die Antwortdatei auf dem gleichen USB-Stick wie die Installationsdateien.
2. Starten Sie den Computer. Das Windows 8/8.1-Setup startet automatisch. Standardmäßig durchsucht das Setupprogramm den Stammordner aller Wechselmedien nach einer Antwortdatei mit dem Namen *AutoUnattend.xml*.

3. Um den Computer nach der Installation klonen zu können, sollten Sie noch den Befehl *sysprep* mit der Option */generalize* sowie die Option */oobe* verwenden, um die Windows-Willkommensseite beim nächsten Neustart zu aktivieren. Wählen Sie in der Liste *Systembereinigungsaktion* die Option *Out-of-Box-Experience (OOBE) für System aktivieren* aus. Aktivieren Sie noch *Verallgemeinern* und wählen Sie die Option *Herunterfahren* aus.
4. Durch die Ausführung des Befehls werden Standardgerätetreiber aus dem Windows-Abbild entfernt. Wenn Sie während der Installation Standardgerätetreiber hinzufügen und das Windows-Abbild aufzeichnen möchten, legen Sie für die Einstellung *PersistAllDeviceInstalls* der *Komponente Microsoft-Windows-PnpSysprep* in der Antwortdatei die Option *true* fest. Bei Verwendung dieser Einstellung entfernt Sysprep die erkannten Gerätetreiber nicht.

Abbildg. 39.15 Vorbereiten eines Quellcomputers für das Klonen



Sie können Sysprep auch über eine Eingabeaufforderung ausführen, indem Sie den folgenden Befehl eingeben:

```
c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown
```

Images erstellen mit DISM

Nachdem Sie auf einem Mastercomputer Windows 8/8.1 installiert und mit Sysprep die Erstellung des Image vorbereitet haben, booten Sie den Computer mit Windows PE unter Verwendung der erstellten DVD. Anschließend können Sie ein Image der Systempartition erstellen.

Dazu geben Sie zunächst *diskpart* und dann *list disk* ein. Notieren Sie die verschiedenen Laufwerke. Sie benötigen den Laufwerksbuchstaben der Windows-Partition und den Buchstaben eines USB-Sticks oder eines externen Laufwerks, auf dem Sie das Image speichern können. Beim Booten mit Windows PE legt das Betriebssystem verschiedene Partitionen an. Um ein Image zu erstellen, verwenden Sie zum Beispiel den Befehl:

```
dism /Capture-Image /CaptureDir:D:\ /ImageFile: E:\ThinImage.wim /Name:"Contoso"
```

Um später ein Image auf einem Computer bereitzustellen, verwenden Sie den Befehl:

```
dism /Apply-Image /ImageFile:<Datei> /Index:1 /ApplyDir:<Laufwerk:\>
```

Images erstellen mit ImageX

ImageX basiert auf der Windows Imaging-Technologie (WIM) und ist das wichtigste Tool beim Rollout von Windows 7 und Windows Server 2008 R2. Auch in Windows 8/8.1 und Windows Server 2012 R2 ist das Tool noch Bestandteil, obwohl DISM in Windows 8/8.1 bevorzugt wird. Idealerweise haben Sie das Tool auf die Windows PE-CD integriert.

Das Tool befindet sich im Ordner *C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment Tools\amd64\dism* oder *\x86\dism*. Nachdem Sie auf dem Mastercomputer Windows 8/8.1 installiert und mit Sysprep die Erstellung des Image vorbereitet haben, booten Sie den Computer mit Windows PE.

Anschließend geben Sie in der Eingabeaufforderung den folgenden Befehl ein:

```
imagex /compress fast /capture C: C:\mein-image.wim <Beschreibung> /verify
```

Statt *mein-image.wim* kann eine beliebige Bezeichnung für das Image verwendet werden.

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 Image wird zum Beispiel der folgende Befehl verwendet:

```
imagex /mountrw <Pfad zum Image und zur .wim-Datei> <Pfad, in den das Image gemountet wird>
```

Mit dem folgenden Befehl werden Treiber in das Image kopiert:

```
peimg /inf=<Pfad zur .inf-Datei des Treibers> <Gemounteter Pfad>
```

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-Bereitstellungsdienste verwendet.

Wollen Sie ein Image nur auf einem einzelnen Computer ohne die Bereitstellungsdienste 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 folgenden Befehle ein:

```
diskpart
select disk 0
clean
create partition primary size=25000
select partition 1
active
format
exit
```

Im nächsten Schritt wird die Imagedatei von der Netzwerkfreigabe auf die lokale Festplatte des PC kopiert. Im Anschluss wird das Image mit dem Befehl *imagex.exe /apply C:\mein-image.wim c*: auf dem Computer installiert. Neben den beschriebenen Optionen kennt ImageX noch weitere:

- **/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
- **/scroll** Gibt alle Ausgaben am Stück aus
- **/split** Teilt 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

Grundlagen der Windows-Bereitstellungsdienste

Die Windows-Bereitstellungsdienste sind der Nachfolger der Remote Installation Services (RIS) von Windows Server 2003. WDS kann auch 64-Bit-Betriebssysteme verteilen. Der WDS-Server muss einer bestehenden Active Directory-Domäne angehören oder ein eigenständiger Domänencontroller sein.

Der WDS-Server muss außerdem Zugang zu einem aktiven DHCP-Server haben. Der Server benötigt eine separate Partition, die mit NTFS formatiert ist. In dieser speichern Sie die Abbilder zur automatisierten Installation. Die PCs im Netzwerk booten und verbinden sich anschließend mit dem Server. Dieser kopiert dann über das Netzwerk das Image auf den Server.

Virtuelle Festplatten (Virtual Hard Disks, VHDs) lassen sich über eine unbeaufsichtigte Installation bereitstellen. Multicast-Verbindung zu langsamen Clients kann ein WDS-Server automatisch trennen und so Übertragungen auf Basis der Clientgeschwindigkeit in mehrere Streams aufteilen.

Außerdem wird Multicasting in Umgebungen mit IPv6 unterstützt. Mit Transportserver sind Netzwerkstarts und Datenmulticasting im Rahmen einer erweiterten Konfiguration möglich. Transportserver ist ein eigenständiger Server der WDS der PXE, also das Booten von Computern über das Netzwerk unterstützt.

Beim Verwenden eines Transportservers für Netzwerkstarts und Multicasting sind Sie nicht auf ein Active Directory oder DNS angewiesen. WDS unterstützen Netzwerkstarts von x64-Computern mit EFI, einschließlich Funktionen zum automatischen Hinzufügen, DHCP-Verweisen zum Weiterleiten von Clients an einen bestimmten PXE-Server sowie der Fähigkeit, Startabbilder mithilfe von Multicasting bereitzustellen. Treiberpakete lassen sich jetzt direkt in Startabbilder integrieren.

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 2003/2008 als auch unter Windows Server 2012 R2 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.

Bei der Verwendung von Windows Server 2012 R2 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 Sie im Kontextmenü den Eintrag *Server konfigurieren* aus. 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 Suchabbilder genannt und erhalten vor der Generierung die Information, welcher Bereitstellungsserver verwendet werden soll. Aufzeichnungsabbilder bieten eine Alternative zum Befehlszeilentool ImageX, wenn ein mit dem Dienstprogramm Sysprep 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.

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 erfordert, dass der Benutzer beim Starten des Computers die F12-Taste drücken muss, um einen Netzwerkboot durchzuführen. Wird *PXEboot.n12* genutzt, erfolgt der Boot über das Netzwerk ohne Drücken der F12-Taste. Das Tool AbortPXE legt fest, dass ein Computer direkt das nächst verfügbare Bootmedium nutzt. Es erfolgt kein Netzwerkboot.

Wdsnbp stellt Funktionen bereit, die zur Erkennung der Architektur und zur Verwaltung von Anfragen der Bootberechtigung benötigt werden. Es wird noch vor PXEboot 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.

Wie funktioniert die automatisierte Installation von Windows über WDS?

Ein Clientcomputer wird 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 Imagegruppe existieren.

Wurde die Antwortdatei mit Informationen, wie Product Key, Sprachversion und Domänenkonto korrekt konfiguriert, läuft die Installation völlig automatisiert ab. Das Befehlszeilentool Wdsutil bietet eine erweiterte Funktionalität. Außerdem kann mit dem Tool auch ein bestehendes RIPREP-Image zu einem WIM-Image konvertiert werden.

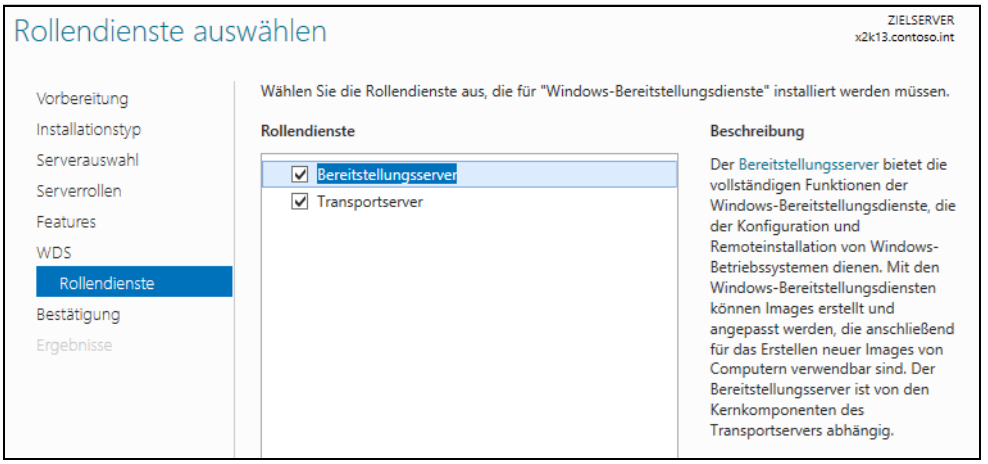
Die Windows Deployment Services bieten eine effektive Möglichkeit, Windows-Betriebssysteme ohne den Einsatz von Installationsmedien zu installieren. Durch den Einsatz von Antwortdateien lässt sich die Installation automatisieren. In Kombination mit der Lite Touch Installation (LTI) beziehungsweise der Zero Touch Installation (ZTI) 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 2012 R2 nur noch die Installation des einheitlichen Modus möglich ist. Eine Verwendung alter RIS-Abbilder ist nicht möglich.

Installieren der Windows-Bereitstellungsdienste

Die Installation besteht aus der Installation der Serverrolle und der anschließenden Ersteinrichtung des Servers. Als Erstes starten Sie den Server-Manager und installieren die Rolle *Windows-Bereitstellungsdienste* über das Menü *Verwalten* (siehe Kapitel 4). Standardmäßig wird sowohl der *Bereitstellungsserver* als auch der *Transportserver* installiert. Zur Installation gehört eine Ersteinrichtung, auch Initialisierung genannt, die über die Verwaltungskonsole der Windows-Bereitstellungsdienste durchgeführt wird.

Abbildg. 39.16 Installieren der Windows-Bereitstellungsdienste



Ersteinrichtung der Windows-Bereitstellungsdienste

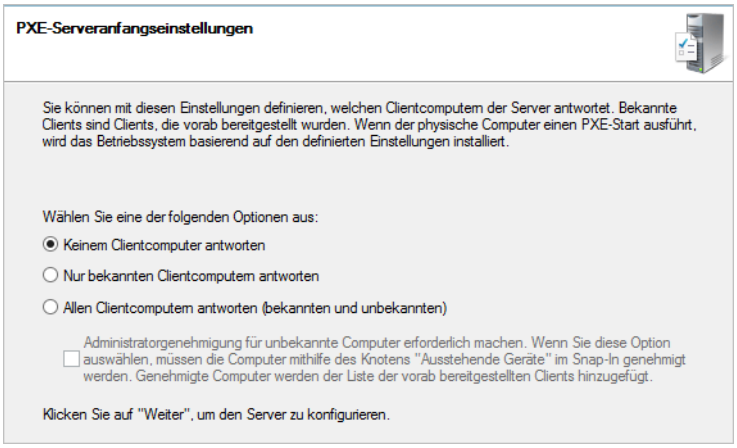
Öffnen Sie für die erste Einrichtung die Verwaltungskonsole der Windows-Bereitstellungsdienste über *Tools* im Server-Manager oder durch Eingabe von *wdsmgmt.msc* auf der Startseite. Der Server wird angezeigt, ist aber noch mit einem Warnzeichen versehen.

Über das Kontextmenü starten Sie den Befehl *Server konfigurieren*. Es startet ein Assistent, über den Sie den Server einrichten. 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. Statt über den Assistenten können Sie diesen Vorgang auch über die Eingabeaufforderung mit dem Befehl *wdsutil /initialize-server /reminst:<Ordner>* durchführen.

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 ist, diesen Server verwenden.

Damit der Server ordnungsgemäß Clients anbinden kann, sollten Sie am besten die Optionen *Allen Clientcomputern antworten (bekannten und unbekannten)* und, falls gewünscht, das Kontrollkästchen *Administratorgenehmigung für unbekannte Computer erforderlich machen* aktivieren.

Abbildg. 39.17 Konfigurieren der PXE-Anfragen an den WDS-Server

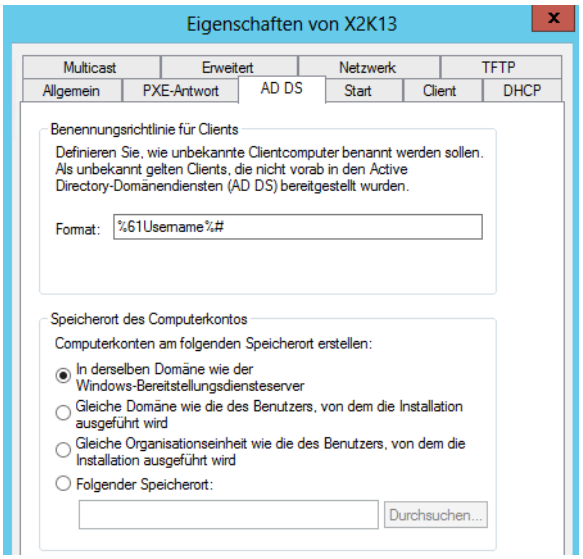


Nach der Installation können Sie diese Einstellung auch in der WDS-Konsole in den Eigenschaften des Servers auf der Registerkarte *PXE-Antworteinstellungen* konfigurieren. Anschließend ist der Server einsatzbereit für das Hinzufügen von Abbildern.

TIPP Neben der Verwaltungskonsole bieten die Windows-Bereitstellungstools auch ein Befehlszeilentool mit der Bezeichnung Wdsutil. Viele Administrationsaufgaben, zum Beispiel das Verwalten von Abbildern, lassen sich neben der grafischen Oberfläche auch mit diesem Tool durchführen. Eine ausführliche Hilfe über die Optionen erhalten Sie mit *wdsutil /?*. Bereits bei der Einrichtung des Servers kann über Wdsutil einiges automatisiert oder über Skripts abgewickelt werden.

Nach der ersten Einrichtung über den Assistenten können Sie in der WDS-Konsole über die Eigenschaften die Konfiguration des Servers anpassen.

Abbildg. 39.18 Anpassen des WDS-Servers in der WDS-Konsole



Multicast verwenden

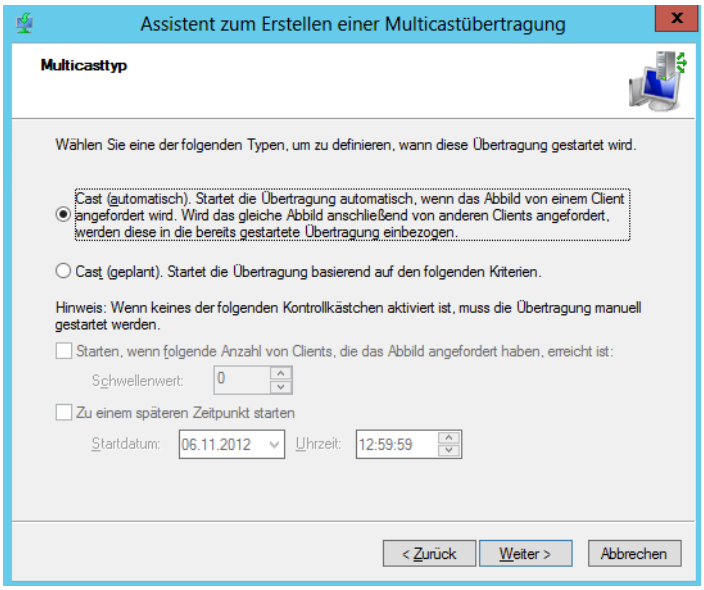
Multicast verwenden Sie, wenn sich nicht nur wenige Clients mit dem Bereitstellungsserver verbinden, sondern eine große Anzahl von Clients gleichzeitig. Beim Erstellen einer Multicastübertragung für ein Abbild werden die Daten nur einmal über das Netzwerk gesendet, wodurch eine deutliche Verringerung der verwendeten Netzwerkbandbreite erreicht werden kann.

Achten Sie aber darauf, dass diese Funktion von den Routern im Netzwerk unterstützt werden muss. 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.

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.

Abbildg. 39.19 Festlegen der Bedingungen für den Start der Übertragung



Wenn die Übertragung als geplante Umwandlung konfiguriert, mindestens ein Client verbunden und die Übertragung noch nicht gestartet ist, können Sie mit der rechten Maustaste die Übertragung anklicken und den Befehl *Starten* wählen.

Klicken Sie 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, ein Befehlszeilentool des ADK, an einer Übertragung teilnehmen. In den Eigenschaften des Servers kann auf der Registerkarte *Netzwerkeinstellungen* das Verhalten des Servers bezüglich Multicast konfiguriert werden.

TIPP Werden im Unternehmen mehrere WDS-Server für Multicast konfiguriert, sollte in den Eigenschaften jedes Servers auf der Registerkarte *Netzwerk* ein anderer Portbereich eingestellt werden, da sich sonst Datenpakete überlappen können und die Netzwerkbelastung stark ansteigt.

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, also die Installationsumgebung des Servers, laden.

Installationsabbilder sind schließlich die Abbilder, über die zum Beispiel Windows Vista oder Windows 7/8/8.1 installiert werden kann. Über die Abbilder lässt sich auch problemlos Windows Server 2008 oder Windows Server 2012 R2 installieren.

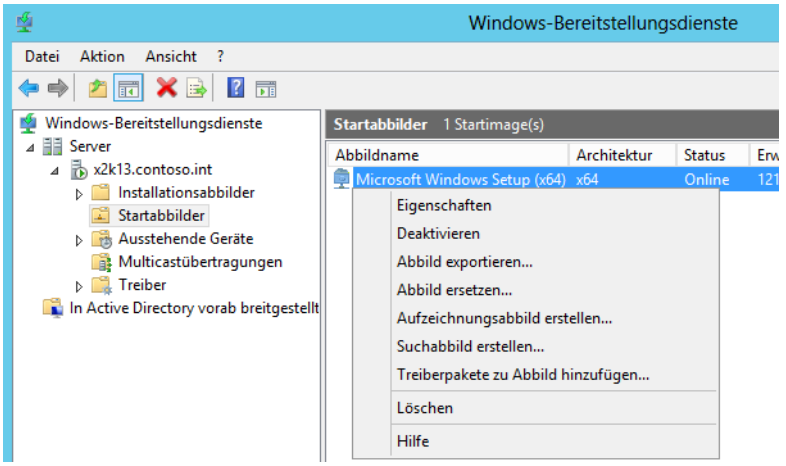
Startabbilder verwalten

Startabbilder kommen dann zum Einsatz, wenn Sie eine automatisierte Installation über Antwortdateien durchführen wollen, also wenn Anwender selbst bei der Installation den einen oder anderen Menüpunkt auswählen können.

Bei dieser Installationsmethode findet die Installation von Windows Vista oder Windows 7/8/8.1 und Windows Server 2012 R2 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 eine Antwortdatei vorgenommen.

Um ein Startabbild hinzuzufügen, starten Sie zunächst die Verwaltungsoberfläche der WDS. Als Nächstes klicken Sie den Konsoleneintrag *Startabbilder* mit der rechten Maustaste an und wählen danach im Kontextmenü den Befehl *Startabbild hinzufügen* aus.

Abbildg. 39.20 Verwalten von Startabbildern in den Windows-Bereitstellungsdiensten



Sie können entweder ein eigenes Abbild erstellen, wie bereits in diesem Kapitel besprochen, oder Sie verwenden das Standardabbild *boot.wim* aus dem Ordner *sources* auf der Windows Vista-, Windows 7/8/8.1- oder Windows Server 2012 R2-DVD.

Dieses sollten Sie vorher auf die Festplatte des Servers kopieren. Auf der nächsten Seite sehen Sie den Namen sowie die Beschreibung des Abbilds. Bestätigen Sie die restlichen Fenster, damit das Startabbild dem Server hinzugefügt wird.

Sobald das Startabbild dem Server hinzugefügt ist, sehen Sie es in der Verwaltungskonsole als Online. Über das Kontextmenü können Sie das Abbild bearbeiten oder andere Abbilder aus diesem Abbild erstellen.

Über das Kontextmenü können Sie auch zusätzliche Treiber in das Startabbild hinzufügen. Startabbilder können auch über die Eingabeaufforderung mit dem folgenden Befehl hinzugefügt werden:

```
wdsutil /Add-Image /ImageFile:<Pfad zur .wim-Datei> /ImageType:boot
```

Computer über WDS booten und Fehler beheben

Sobald die Windows-Bereitstellungsdienste installiert und konfiguriert sind und ein Startabbild oder Installationsabbilder hinzugefügt sind, können Computer über das Netzwerk gebootet werden. Achten Sie darauf, dass die Netzwerkkarte des Computers PXE beherrscht und der DHCP-Server korrekt konfiguriert ist.

HINWEIS Haben Sie WDS und DNS auf dem gleichen Server installiert, besteht die Möglichkeit, dass das Booten der Clients fehlschlägt. Das Problem liegt daran, dass der DNS-Server die Ports des WDS-Servers blockiert. Mehr Informationen zu diesem Fehler erhalten Sie auf der Internetseite *http://support.microsoft.com/kb/977512* [Ms179-K39-04].

Die Clients erhalten zwar eine IP-Adresse durch den DHCP-Server, aber können anschließend keine TFTP-Verbindung zum WDS-Server aufbauen, um Abbilder zu laden. Sie können den Fehler folgendermaßen beheben:

1. Öffnen Sie den Registrierungs-Editor und navigieren Sie zu *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WDSServer\Parameters*.
2. Öffnen Sie den Wert *UdpPortPolicy*.
3. Setzen Sie den Wert von *1* auf *0*.
4. Starten Sie den WDS-Dienst über das Kontextmenü zum Server in der WDS-Konsole neu.

Sobald sich der Computer erfolgreich mit dem WDS-Server verbindet, erhält er eine IP-Adresse zugewiesen und Windows PE wird auf diesem Computer gestartet. Nach Bestätigung des Netzwerkbootvorgangs startet der Computer mit dem Startabbild, das auf dem Computer hinterlegt worden ist.

Installationsabbilder verwenden

Installationsabbilder sind Abbilder, über die Windows Vista, Windows 7/8/8.1 oder Windows Server 2012 R2 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, Windows 7/8/8.1 oder Windows Server 2012 R2 aus dem Ordner *\sources* auf der DVD.

Installationsabbilder werden in Abbildgruppen zusammengefasst. Bei der Erstellung des ersten Installationsabbilds 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.

Im ersten Fenster wählen Sie die Abbildgruppe aus, in der Sie das Installationsabbild integrieren. Ist noch keine Abbildgruppe vorhanden, können Sie eine erstellen. Im nächsten Fenster wählen Sie die Imagedatei aus. Enthält ein Image mehrere Möglichkeiten und Windows-Editionen, legen Sie im nächsten Fenster fest, welche Edition Sie integrieren wollen. Das Installationsabbild wird in seiner Gruppe angezeigt und Sie können es nachträglich bearbeiten. Es lassen sich beliebige weitere Installationsabbilder hinzufügen, sodass bei der Betriebssystemauswahl auf dem Client weitere Optionen zur Verfügung stehen. 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 Eingabeaufforderung wird ein Installationsabbild mit dem folgenden Befehl hinzugefügt:

```
wdsutil /add-image /ImageFile:<Pfad> /ImageType:install /ImageGroup:<Abbildgruppe>
```

Mit der zusätzlichen Option */SingleImage:<Bezeichnung>* kann nur ein einzelnes Image der WIM-Datei ausgewählt werden.

TIPP Auf der Registerkarte *Client* in den Eigenschaften des WDS-Servers können Sie Antwortdateien hinterlegen, welche die Installation automatisieren, wenn das hinterlegte WIM-Abbild nicht bereits automatisiert ist.

Suchabbilder verwenden

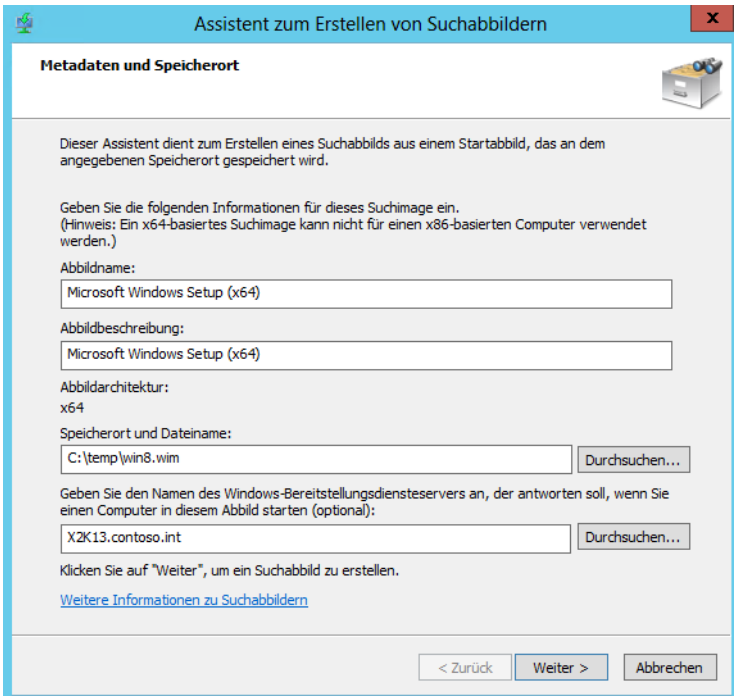
Suchabbilder sind Abbilder für Computer, die kein PXE-Boot über das Netzwerk beherrschen. Dazu wird ein Datenträger erstellt, mit dem der entsprechende Computer gebootet wird und sich mit dem WDS-Server verbinden kann.

Suchabbilder werden über ein Startabbild erstellt. Klicken Sie dazu das Startabbild mit der rechten Maustaste an und wählen Sie im Kontextmenü den Eintrag *Suchabbild erstellen* aus.

Es öffnet sich ein neues Fenster, auf dem mehrere Eingaben für das Suchabbild vorgenommen werden können. Legen Sie die Beschreibung des Abbilds fest und geben Sie den Namen und den Speicherort der zu erstellenden WIM-Datei an. Auch der WDS-Server der auf Anfragen dieses Clients antworten soll, wird hier festgelegt. Achten Sie darauf, dass für Suchabbilder immer nur ein WDS-Server konfiguriert werden kann.

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 Suchabbilds an dieser Stelle nicht viel und muss daher zunächst in eine ISO-Datei umgewandelt werden.

Abbildg. 39.21 Konfigurieren eines Suchabbilds



Aufzeichnungsabbilder 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 Suchabbilder auf Basis von Startabbildern erstellt. Klicken Sie in der WDS-Konsole mit der rechten Maustaste auf das Startabbild, auf dessen Basis Sie das Aufzeichnungsabbild erstellen wollen, und wählen *Aufzeichnungsabbild erstellen* aus. Im folgenden Fenster geben Sie den Namen des Abbilds sowie den Speicherort für die WIM-Datei des Abbilds aus.

Nachdem das Abbild erstellt ist, müssen Sie dieses noch als zusätzliches Startabbild hinzufügen. Gehen Sie dazu genauso vor wie beim Hinzufügen des ersten Startabbilds weiter vorne in diesem Kapitel. Sind mehrere Startabbilder konfiguriert, kann auf den Clientcomputern standardmäßig ausgewählt werden, welches verwendet werden soll.

Startet ein Computer über ein Aufzeichnungsstartabbild, erscheint der Assistent, mit dem ein Image des Computers erstellt und über das Netzwerk auf dem WDS-Server gespeichert werden kann.

ACHTUNG Vom Assistenten zur Abbildaufzeichnung für die Windows-Bereitstellungsdienste werden nur die mithilfe von Sysprep vorbereiteten Laufwerke angezeigt.

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 *AD DS* können Sie diese Funktion konfigurieren.

Wird die Installation nicht über eine Antwortdatei gesteuert, in der auch die Namen der Computer angegeben sind, 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.

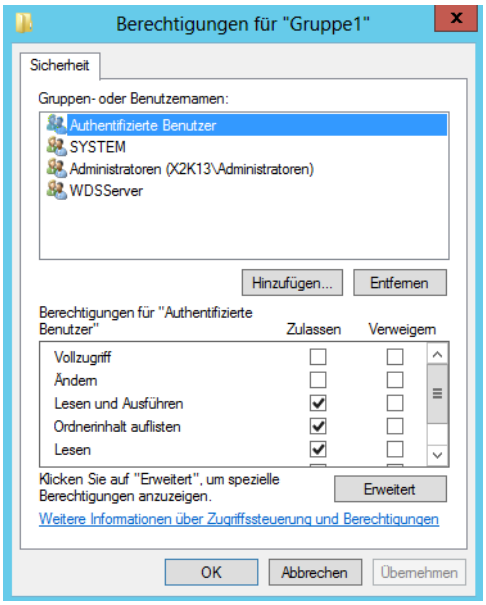
ACHTUNG Ein Computername darf aus maximal 15 Zeichen bestehen. Mit der Standardrichtlinie sind jedoch Namen mit einer Länge von bis zu 63 Zeichen möglich. Wenn ein Name mit einer Länge von mehr als 15 Zeichen generiert wird, werden alle Zeichen abgeschnitten, die auf die ersten 15 folgen, und der Computer 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. 39.22 Die Berechtigungen für Abbildgruppen lassen sich in der WDS-Konsole verwalten



Virtuelle Festplatten in WDS verwenden

Windows Server 2012 R2 und Windows 7/8/8.1 unterstützen die direkte Einbindung von VHD-Festplatten in das Betriebssystem. Die beiden Betriebssysteme lassen sich sogar von virtuellen Festplatten booten (siehe Kapitel 1 und 2). WDS in Windows Server 2012 R2 bietet die Möglichkeit, auch virtuelle Festplatten im Unternehmen bereitzustellen.

VHD-Dateien erstellen und in WDS einbinden

VHD-Dateien lassen sich genauso verteilen wie WIM-Images. Zur Einbindung benötigen Sie Wdsutil, da sich VHD-Dateien in WDS nur über die Eingabeaufforderung einbinden lassen. Damit Sie eine VHD-Datei in WDS einbinden können, muss der WDS-Server konfiguriert und mit einem Startabbild versehen sein.

HINWEIS Auf der VHD-Datei darf sich nur ein Betriebssystem und nur eine Partition befinden. GPT-Datenträger werden nicht unterstützt. Für VHD-Dateien müssen Sie eigene Abbildgruppen erstellen, WIM-Dateien und VHD-Dateien lassen sich nicht vermischen.

Um ein Image zu WDS hinzuzufügen, öffnen Sie eine Eingabeaufforderung mit Administratorrechten. Sie können die Abbildgruppe für VHD-Dateien auch in der Eingabeaufforderung mit Wdsutil erstellen. Verwenden Sie dazu den Befehl:

```
wdsutil /Add-ImageGroup /ImageGroup:<Name>
```

Anschließend können Sie mit Wdsutil VHD-Dateien, die ein Betriebssystem enthalten, in die Abbildgruppe integrieren:

```
wdsutil /Verbose /Progress /Add-Image /ImageFile:<Pfad> /ImageType:Install /
ImageGroup:<Name>
```

Verwenden Sie differenzierende Festplatten, müssen Sie den Pfad zur differenzierenden Festplatte eingeben, nicht zur übergeordneten Festplatte. Die komplette Syntax des Befehls ist:

```
wdsutil /add-Image /ImageFile:<Pfad zur VHD-Datei> [/Server:<Name>] /ImageType:install [/
ImageGroup:<Name>] [/Filename:<Neuer Dateiname des Images>] [/UnattendFile:<Pfad zur XML-
Datei>]
```

Beispiel:

```
wdsutil /Verbose /Progress /Add-Image /ImageFile:"C:\vhd\Windows8.vhd" /Server:dc02 /
ImageType:Install /ImageGroup:"VHD-Images"
```

Wollen Sie die Eigenschaften eines Images anzeigen, verwenden Sie den Befehl

```
wdsutil /Get-ImageGroup /ImageGroup:<Name> /Detailed
```

Mit dem folgenden Befehl passen Sie die Beschreibung des Images an:

```
wdsutil /Set-Image /Image:<Name> /ImageType:Install /ImageGroup:<Name> /
Description:<Beschreibung>
```

Unbeaufsichtigte Installation über eine VHD-Datei durchführen

Über zwei Antwortdateien können Sie über VHD-Images auch unbeaufsichtigte Installationen durchführen. Eine Antwortdatei automatisiert das Benutzerinterface, die andere den Rest der Installation. Beide Dateien können Sie mit Windows SIM erstellen. Dieser Vorgang nennt sich Prestaging: Ein Computerkonto wird in Active Directory mit einer vorgegebenen GUID erstellt und dann über WDS installiert und angebunden.

Mit dem folgenden Befehl können Sie einen Client, den Sie über WDS installieren, an das erstellte Konto anbinden:

```
wdsutil /Add-Device /Device:<Name> /ID:<GUID oder MAC>.
```

Beispiel:

```
wdsutil /Add-Device /Device:Client35 /ID:ACEFA3E81F20694E953EB2DAA1E8B1B6
```

Zusätzlich können Sie diesem Gerät eine Antwortdatei zuweisen:

```
wdsutil /Set-Device /Device:<Name> /WDSClientUnattend:<Pfad zur XML-Datei>.
```

Beispiel:

```
wdsutil /Set-Device /Device:Client35 /WDSClientUnattend:WDSClientUnattend\Unattend.xml
```

Bevor Computer, die Sie nicht vorbereitet haben und die daher unbekannt in den WDS sind, eine Installation über den WDS durchführen können, müssen diese für den Zugriff auf den WDS und Abbilder berechtigt sein.

Im Bereich *Ausstehende Geräte* sehen Sie solche Anfragen und können diese freischalten. In den Eigenschaften des WDS-Servers können Sie auch unbekannten Clients automatisch Zugriff gewähren. Sie steuern diese Konfiguration über die PXE-Eigenschaften des WDS-Servers. Antwortdateien lassen sich auch generell für alle Clients hinterlegen, die sich mit dem Server verbinden, also als Standard.

Treiberpakete in WDS verwenden

In Windows Server 2012 R2 können Sie in den WDS einzelnen Startabbildern Treiberpakete hinzuweisen, die Clients beim Starten automatisch laden. Sie steuern diese Funktion über das Kontextmenü von Startabbildern. Ein solches Paket kann aus mehreren verschiedenen Treibern bestehen und Sie können einen Filter festlegen, für welche Computer diese Treiber gültig sind. Achten Sie darauf, die Treiber zu extrahieren. Es darf sich nicht um *.msi-* oder *.exe*-Dateien handeln. Starten Sie die Erstellung eines Treiberpakets, können Sie bequem über einen Assistenten die Treiber hinzufügen.

Unbeaufsichtigte Installation über die Windows-Bereitstellungsdienste

Erstellte Antwortdateien lassen sich für eine unbeaufsichtigte Installation von Windows Vista oder Windows 7/8/8.1 oder Windows Server 2012 R2 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.
2. Erweitern Sie im Bereich *Components* den Eintrag *x86_Microsoft-Windows-Setup_<Nummer>_neutral*.
3. Klicken Sie den Eintrag *WindowsDeploymentServices* mit der rechten Maustaste an und wählen Sie im Kontextmenü den Befehl *Einstellung zu Pass 1 windowsPE hinzufügen* aus. Damit kann dieser Eintrag für die Antwortdatei konfiguriert werden.

Nachdem Sie den Zusatz der Antwortdatei hinzugefügt haben, können Sie diesen konfigurieren. Dazu stehen verschiedene Möglichkeiten zur Verfügung, die Sie im mittleren Bereich des Fensters sehen. 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 Installationsabbilds ein, das durch diese Antwortdatei über den WDS installiert werden soll. Hier wird nicht der Name des Abbilds, sondern der Name der entsprechenden WIM-Datei ausgewählt. Der Dateiname kann in den Eigenschaften des Installationsabbilds 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 Installationsabbilds auf dem WDS ein.
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.
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.

Nachdem die Datei bearbeitet ist, kopieren Sie diese in den Ordner *WDSClientUnattend* in den Remoteinstallationsordner 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.

Automatisieren der Installation über Abbilder

Die Automatisierung der Installation können Sie nicht nur in den Eigenschaften des WDS-Servers konfigurieren, sondern auch in den Eigenschaften des Abbilds. Auch hierzu müssen Sie die Antwortdateien für die Abbilder anpassen und für WDS optimieren.

In den Eigenschaften eines Installationsabbilds können Sie auf der Registerkarte *Allgemein* die Option *Abbildinstallation im Modus für unbeaufsichtigte Installation zulassen* aktivieren. Anschließend wählen Sie die entsprechende Antwortdatei aus. Die ausgewählte Datei wird automatisch in den Ordner *\Images\<Abbildgruppe>\install\Unattend\ImageUnattend.XML* kopiert.

Volumenaktivierungsdienste nutzen

Wollen Sie Windows 8/8.1 und Windows Server 2012 R2 über Volumenaktivierung zentral im Unternehmen aktivieren, können Sie die neuen Volumenaktivierungsdienste in Windows Server 2012 R2 nutzen. Diese installieren Sie über den Server-Manager als Serverrolle (siehe Kapitel 4).

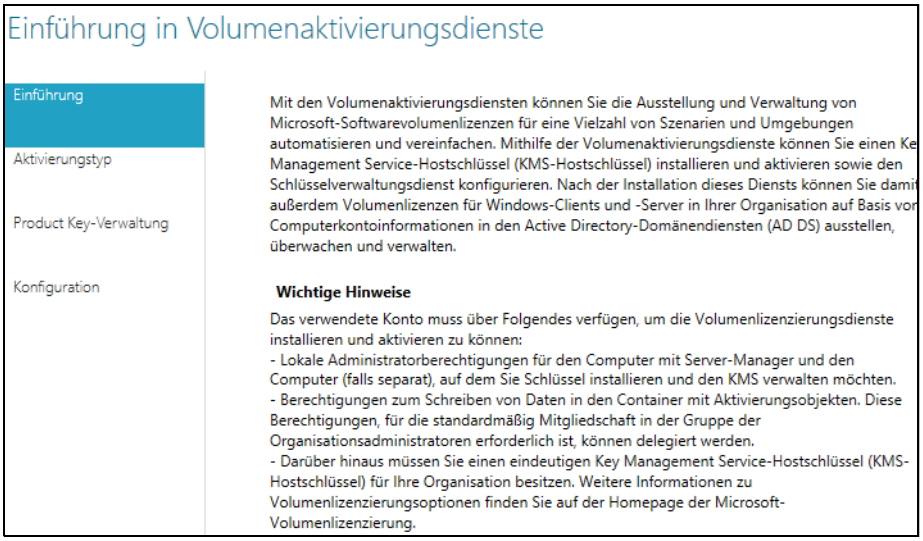
Der folgende Befehl installiert die Rolle in der PowerShell:

```
enable-windowsoptionalfeature -online -featurename VolumeActivation-Full-Role
```

Alternativ verwenden Sie *Install-WindowsFeature VolumeActivation*. Nach der Installation müssen Sie den Rollendienst noch konfigurieren:

1. Öffnen Sie im Server-Manager das *Tools*-Menü und wählen Sie den Befehl *Volumenaktivierungstools* aus.
2. Wählen Sie auf der Seite *Volumenaktivierungsmethode auswählen* die Option *Aktivierung über Active Directory* aus. Wenn das Konto, das Sie gerade verwenden, über keine Administratorberechtigungen auf Unternehmensebene verfügt, geben Sie die Anmeldeinformationen für ein Konto mit Berechtigungen zur Erstellung eines neuen Containers auf dem Domänencontroller ein und klicken Sie anschließend auf *Weiter*.
3. Geben Sie den KMS-Hostschlüssel und einen optionalen Namen für das Active Directory-Objekt ein und klicken Sie danach auf *Weiter*.

Abbildg. 39.23 Einrichten der Volumenaktivierung



Nachdem der KMS-Hostschlüssel aktiviert ist, werden Clientcomputer, die Sie der Domäne hinzufügen, automatisch aktiviert. Alle Ereignisse der Active Directory-basierten Aktivierung werden im Ereignisprotokoll der Windows-Anwendung unter der Quelle *Microsoft-Windows-Security-SPP* erfasst. Sehen Sie unter dem Ereignis 12308 nach, um die Informationen zu prüfen. Bei Clients, auf denen Windows Server 2012 R2 oder Windows 8/8.1 ausgeführt wird, sollte die Aktivierung automatisch erfolgen, wenn der Computer das nächste Mal gestartet wird und sich der Benutzer anmeldet.

HINWEIS Die Aktivierung über Active Directory funktioniert nicht bei Betriebssystemen vor Windows Server 2012 R2 oder Windows 8/8.1. Sie funktioniert zudem nicht bei Microsoft Office 2010/2013. Verwenden Sie die KMS-Volumenaktivierung, um Windows-Clients und -Anwendungen zu aktivieren, die keine Active Directory-basierte Aktivierung unterstützen.

Wählen Sie *Schlüsselverwaltungsdienst (KMS)* als Aktivierungsmethode, können Sie auch ältere Systeme und Office aktivieren. Die KMS-Volumenaktivierung erfordert einen Mindestschwellenwert von 25 Computern, bevor Aktivierungsgesuche verarbeitet werden. Der hier beschriebene

Überprüfungsprozess erhöht den Aktivierungszähler mit jedem Mal, wenn ein Clientcomputer den KMS-Host anruft. Wenn der Aktivierungsschwellenwert noch nicht erreicht ist, ergibt die Überprüfung jedoch eine Fehlermeldung.

Office 2010/2013 automatisiert installieren

Office 2010/2013 bietet die Möglichkeit, eine vollkommen automatisierte Installation durchzuführen. Über diesen Weg lassen sich auch Patches oder Servicepacks direkt in die Installation einbeziehen, auch das SP1 für Office 2010 (*http://www.microsoft.com/de-de/download/details.aspx?id=26622* [Ms179-K39-05]).

Der einfachste und bekannteste Weg ist die Installation mit dem integrierten Assistenten. Dieser trägt die Bezeichnung Office-Anpassungstool (Office Customization Tool, OCT). Das Tool steht aber nur für Office 2010/2013-Versionen zur Verfügung, die über eine Volumenlizenz verfügen. Jedoch gibt es auch für alle anderen Editionen Möglichkeiten, auf die wir nachfolgend näher eingehen.

Microsoft Office-Anpassungstool

Mit dem Microsoft Office-Anpassungstool (Office Customization Tool, OCT) passen Sie über eine grafische Oberfläche die Installation von Office 2010/2013 an und automatisieren Installation und Einstellungen für die Benutzer. Das Tool ersetzt die Office 2003-Werkzeuge zur automatischen Office-Installation, den Custom Installation Wizard und Custom Maintenance Wizard.

Änderungen, die Sie mit dem Microsoft Office-Anpassungstool am Office-Setup vornehmen, speichert das Programm in einer Setupanpassungsdatei (Setup Customization File). Die Datei erhält als Endung *.msp*. Beim Start des Office-Setupprogramms führt das Programm die Änderungen in dieser Datei automatisch aus. Die Datei muss dazu im Unterordner *\Updates* des Installationsordners gespeichert sein. Befindet sich eine *.msp*-Datei in diesem Ordner, verwendet das Office-Setup diese automatisch bei der Installation, unabhängig davon, ob es sich um eine Installationsdatei oder einen Patch handelt.

Auch Patchdateien liegen in diesem Format vor. Sie können in diesem Ordner daher mehrere Dateien speichern. Ist auf einem Computer bereits Office 2010/2013 installiert, können Sie über diese Datei auch nachträglich Anpassungen vornehmen oder Programme entfernen. Befinden sich auf einem Computer zum Beispiel Word, Excel, Access und Outlook, können Sie einzelne Komponenten über die *.msp*-Datei vom Computer entfernen lassen, indem Sie die Anpassungsdatei entsprechend konfigurieren.

Neben *.msp*-Dateien können Sie auch die Standardkonfigurationsdatei *Config.xml* von Office 2010/2013 für die Installation anpassen. Die Datei gehört zum Installationsumfang von Office 2010/2013. Allerdings stehen hier deutlich weniger Optionen zur Verfügung. Die Konfigurationsdatei können Sie dafür aber auf einfachem Weg anpassen und zur automatisierten Installation können Sie angepasste *.msp*- und *Config.xml*-Dateien parallel einsetzen. Außerdem unterstützen Office-Editionen ohne Volumenlizenz kein OCT. Hier müssen Sie den Weg über die Konfigurationsdatei zur Automatisierung wählen.

Um das Office Customization Tool zu verwenden, starten Sie das Setupprogramm mit der Option */admin*. Rufen Sie den Befehl *setup /admin* bei einer nicht kompatiblen Office-Edition auf, erscheint eine Fehlermeldung, dass Dateien fehlen. Bei kompatiblen Editionen startet das Tool und Sie können in den einzelnen Bereichen Anpassungen vornehmen.

Über die einzelnen Menüpunkte können Sie Änderungen für alle Office-Programme und die komplette Sammlung vornehmen. So besteht die Möglichkeit, direkt während der Installation bereits ein Profil für Outlook anzulegen und Konten anzugeben.

Weitere Einstellungen lassen sich über Gruppenrichtlinien durchführen. Im Downloadcenter stellt Microsoft Gruppenrichtlinienvorlagen zur Verfügung (*http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=18968* [Ms179-K39-06]), über die Sie Office 2010/2013 per Richtlinie anpassen können. Damit sich diese verwenden lassen, müssen Sie die *.admx*-Dateien nach dem Entpacken auf dem Domänencontroller in den Ordner *C:\PolicyDefinitions* kopieren.

Die Gruppenrichtlinien-Sprachdateien (*.adml*) müssen Sie aus dem jeweiligen Sprachenordner in den Ordner unter *C:\PolicyDefinitions* kopieren. So können Sie zum Beispiel in der Gruppenrichtlinienverwaltung über *Benutzerkonfiguration/Richtlinien/Administrative Vorlagen* Einstellungen für Office 2010/2013 vornehmen, 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 steuern. Für jede Einstellung finden Sie auf der Registerkarte *Erklärung* entsprechende Hilfestellungen.

Setupoptionen von Office 2010/2013

Neben den Möglichkeiten, die Office 2010/2013-Installation über *.msp*-Dateien und das Administrationsprogramm zu beeinflussen, können Sie das Setupprogramm auch mit speziellen Optionen starten. Mit der Option */adminfile <.msp-Datei>* wendet das Installationsprogramm die angegebene *.msp*-Datei an. Mit der Option */config <Konfigurationsdatei>* weisen Sie das Setupprogramm an, eine andere Konfigurationsdatei zu verwenden als bei einer normalen Installation.

Es besteht die Möglichkeit, parallel zu *.msp*-Dateien Einstellungen für die Installation per Konfigurationsdatei (*Config.xml*) mitzugeben. Die Standardkonfigurationsdatei mit der Bezeichnung *Config.xml* befindet sich im Office 2010/2013-Installationsordner im Ordner *<Edition>.ww*, also zum Beispiel *ProPlus.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.

Die Konfigurationsdatei verwenden Sie zum Beispiel, wenn Sie die Verteilung von Office über Gruppenrichtlinien durchführen oder eine Edition verwenden wollen, die das OCT nicht unterstützt. Über Konfigurationsdateien können Sie allerdings weniger Einstellungen vornehmen. Bei der Verteilung über Gruppenrichtlinien können Sie keine *.msp*-Dateien verwenden.

Das zu installierende Produkt können Sie auswählen und zusätzlich den Benutzer und die Firma angeben, auf die das Produkt registriert ist. Der Lizenzschlüssel und zusätzliche Sprachpakete können Sie ebenfalls übergeben. Im Gegensatz zur *.msp*-Datei ist der Produktschlüssel in der Datei *Config.xml* in Klartext hinterlegt, das heißt für jeden lesbar. Auch den Quellordner und den Installationsordner können Sie über *Config.xml* steuern. Die Datei können Sie mit einem normalen Editor bearbeiten. Die wichtigsten Optionen in der Datei haben wir für Sie in Tabelle 39.1 dargestellt.

Tabelle 39.1 Setupoptionen von Office 2010/2013

Element	Beschreibung
AddLanguage	Fügt der Installation ein Sprachpaket zu. Beispiel: `<AddLanguage Id="en-US" />`

Tabelle 39.1 Setupoptionen von Office 2010/2013 *(Fortsetzung)*

Element	Beschreibung
ARP	Bestimmt das Verhalten, wie Windows das Produkt in der Systemsteuerung anzeigt. Beispiel: `<ARP ARPCOMMENTS="Basisinstallation Office" />`
COMPANYNAME	Der Firmenname oder Benutzer, der das Produkt erworben hat. Beispiel: `<COMPANYNAME Value="Administrator" />`
Command	Mit diesem Element starten Sie während der Installation von Office eigene Befehle, Skripts oder Anwendungen. Beispiel: `<Command Path=\\mdt2010\Skript\Inventory.vbs />`
Display	Dieses Element legt fest, was während der Installation auf dem Bildschirm des Benutzers erscheinen 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 starten soll. Beispiel: `<DistributionPoint Location="\\mdt2010\Office" />`
INSTALLLOCATION	Diese Option legt fest, in welchen Ordner Office installiert wird. Hier können Sie auch Variablen nutzen. Geben Sie dieses Element nicht an, findet die Installation im Ordner *%ProgramFiles%\Microsoft Office* statt. Beispiel: `<INSTALLLOCATION Value="%SystemDrive%\Office2010" />`
Logging	Dieses Element bestimmt, wie der Assistent die Installation protokolliert. Beispiel: `<Logging Type="Verbose" Path="%temp%" Template="Office2010.txt" />`
OptionState	Legt die zu installierenden Komponenten der Office-Suite fest. Beispiel: `<OptionState Id="PubPrimary" State="Absent" Children="force" />`
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. 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 der Assistent nach Anpassungsdateien suchen soll. Alle in dem angegebenen Pfad befindlichen Dateien sortiert der Assistent nach Dateinamen und wendet diese in der entsprechenden Reihenfolge an. Sie können mehrere Netzwerkpfade angeben. Diese müssen Sie per Semikolon trennen. Beispiel: `<SetupUpdates CheckForUpdates="Yes" SUpdateLocation="\\mdt2010\Office\Updates" />`

Tabelle 39.1 Setupoptionen von Office 2010/2013 *(Fortsetzung)*

Element	Beschreibung
SOURCELIST	Bestimmt, wo die Installationsdateien der Office 2010/2013 Suite im Netzwerk liegen. Sie können mehrere Quellen angeben, die Sie per Semikolon trennen. Beispiel: `<SOURCELIST Value=\\mdt2010\Office;\\BACKUP\Office />`
USERINITIALS	Die Initialen des Benutzers, der mit dieser Office-Installation arbeiten soll. Beispiel: `<USERINITIALS Value="CD" />`
USERNAME	Der vollständige Name des Benutzers, der mit dieser Office-Installation arbeiten soll. Beispiel: `<USERNAME Value="Thomas Joos" />`

Alle Daten, die Sie in der Datei *Config.xml* mitgeben, müssen Sie im Installationsfenster nicht mehr eingeben. Das heißt, Sie können über diesen Weg die Installation automatisieren, indem Sie alle Optionen vorgeben. Vor allem die folgenden Zeilen sollten Sie in der Datei anpassen:

```
<Display Level="None" CompletionNotice="no" SuppressModal="yes" AcceptEula="yes" /> -->
 <PIDKEY Value="XXXXX-XXXXX-XXXXX-XXXXX-XXXXX" />
```

Tragen Sie den Product Key in die Platzhalter ein, sollte die Installation vollkommen unbeaufsichtigt ablaufen.

Patches und Service Packs in den Installationsordner integrieren

Ein wichtiger Punkt bei der Verteilung von Office 2010/2013 im Unternehmen ist die Integration von Patches und Servicepacks in den Installationsordner. Patchdateien müssen im *.msp*-Format vorliegen. Haben Sie eine *.exe*-Datei heruntergeladen, können Sie diese in den meisten Fällen entpacken und finden im Archiv anschließend die *.msp*-Dateien sowie einige andere Dateien.

Diese kopieren Sie alle in den Ordner *\Updates* des Office-Installationdatenträgers. Um das SP1 für Office 2010 zu integrieren, entpacken Sie die *.exe*-Datei und kopieren alle Dateien des Archivs in den Ordner *\Updates* der Installationsdateien von Office 2010. Genauso gehen Sie bei Patches für Office 2013 vor.

Zusammenfassung

Mit den Windows-Bereitstellungsdiensten und dem Windows Assessment and Deployment Kit (ADK) lassen sich Windows 7/8/8.1-Arbeitsstationen und Windows Server 2012 R2 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. Auch die automatisierte Installation von Office 2010/2013 haben wir in diesem Kapitel behandelt.

Im nächsten Kapitel zeigen wir Ihnen, wie Sie mit der Windows PowerShell Server mit Windows Server 2012 R2 verwalten.

Kapitel 40

Windows PowerShell

In diesem Kapitel:

Mit Windows 8.1 und Windows Server 2012 R2 veröffentlicht Microsoft auch die neue Version 4.0 der PowerShell. Diese ist standardmäßig bereits vorinstalliert. Neben den Installationen mit grafischer Benutzeroberfläche unterstützen auch Core-Server in Windows Server 2012 R2 die Cmdlets der PowerShell. Wir sind bereits in den einzelnen Kapiteln in diesem Buch auf die PowerShell eingegangen. In diesem Kapitel zeigen wir Ihnen weiterführende Informationen und den Umgang mit der PowerShell.

Wer sich in die PowerShell einarbeiten möchte, findet bei Microsoft einen mehrteiligen Onlinelernkurs (*http://www.microsoft.com/germany/msdn/aktuell/news/show.mspx?id=msdn_de_46012* [Ms179-K40-01]) zur PowerShell.

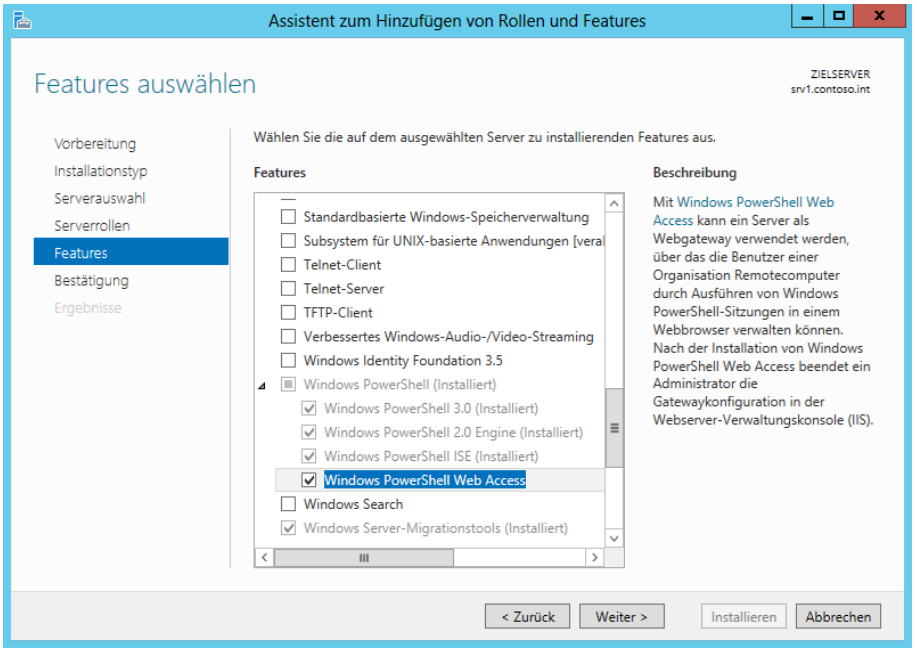
Von Microsoft Press ist das Buch *Scripting mit Windows PowerShell 3.0 – Der Workshop* (Autor: Tobias Weltner) erhältlich.

Es gibt viele Cmdlets, die Abfragen mit HTTP-Sitzungen verbinden können, zum Beispiel *Invoke-WebRequest* und *Invoke-RestMethod*. PowerShell 3.0 bietet zusätzlich noch PowerShell Web Access. Auf diese Weise lässt sich die PowerShell auch über einen Webbrowser nutzen.

In diesem Fall können Sie die PowerShell auch auf Geräten nutzen, auf denen die PowerShell nicht installiert oder die nicht kompatibel zur PowerShell sind. Die komplette Sitzung läuft dazu in einem Browser. Sie können in einer solchen Sitzung eine Verbindung zu jedem anderen Server aufbauen, wenn die PowerShell-Remoteunterstützung auf dem entsprechenden Server aktiviert ist.

Wie Sie PowerShell Web Access einrichten und nutzen, zeigt Microsoft ausführlich in der TechNet im Artikel (*http://technet.microsoft.com/de-de/library/hh831611.aspx* [Ms179-K40-03]). PowerShell Web Access müssen Sie als Serverfeature in Windows Server 2012 über den Server-Manager installieren, damit der entsprechende Server als PowerShell-Gateway zu den anderen Servern dienen kann. Mehr Informationen dazu erhalten Sie im Blogbeitrag unter *http://blog.powershell.no/tag/windows-powershell-web-access* [Ms179-K40-04]. Bei dieser Technik unterstützt Microsoft die meisten aktuellen Browser.

Abbildg. 40.1 Installieren von PowerShell Web Access in Windows Server 2012 R2



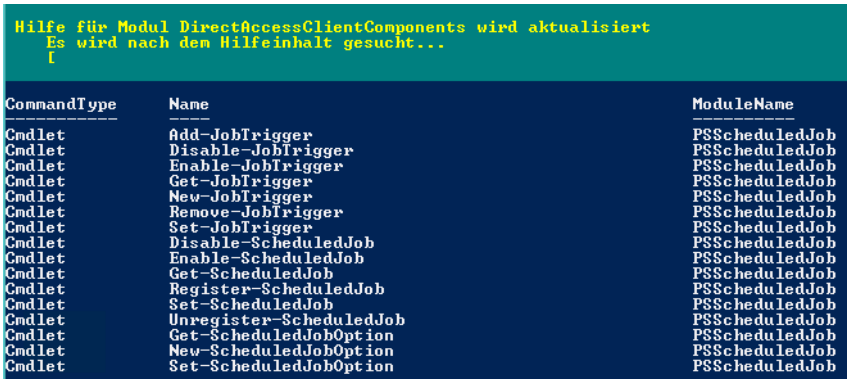
Grundsätzlich funktioniert der Zugriff auch über Smartphones und Tablet-PCs. In diesem Fall unterstützt PowerShell Web Access die folgenden Systeme und neuere. Um Ihr Gerät zu testen, versuchen Sie einfach den Verbindungsaufbau zu einer Web Access-Sitzung.

Eine wesentliche Neuerung in der PowerShell ist die einfachere Bedienung. Zunächst müssen Sie in der neuen Version keine Module mehr laden wie in der PowerShell 2.0. Alle Erweiterungen und Module, die installiert sind, erkennt die PowerShell und kann sie automatisch verwenden, sobald Sie ein Cmdlets eines bestimmten Moduls eingeben.

Die neue Version zeigt auch weniger Fehlermeldungen an, wenn eine Option eines Cmdlets fehlt. Stattdessen fragt die PowerShell nach den noch fehlenden Optionen. In der PowerShell hat Microsoft deutlich die Hilfefunktion erweitert. Rufen Sie eine Hilfe zu Cmdlets auf, kann sich die PowerShell selbstständig aktualisieren.

Das funktioniert eingeschränkt auch mit der alten PowerShell 2.0, wenn Sie für das Cmdlet *Get-Help* die Option *–Online* verwenden, zum Beispiel mit *Get-Help Get-Command –Online*. Die PowerShell bietet das neue Cmdlet *Update-Help*, welches die Hilfedateien der PowerShell aktualisieren kann. Dazu muss der Server über eine Internetverbindung verfügen. Der Befehl ruft die Hilfe direkt aus dem Internet ab.

Abbildg. 40.2 Die PowerShell bietet eine ausführlichere Hilfe als PowerShell 2.0 und kann Hilfedateien nachladen



Ebenfalls neu seit Windows Server 2012 in der PowerShell ist das Cmdlet *Show-Command*. Dieses blendet ein neues Fenster mit allen Befehlen ein, die in der PowerShell verfügbar sind. Sie können im Fenster nach Befehlen suchen und sich eine Hilfe zum Befehl sowie Beispiele anzeigen lassen.

Allerdings muss dazu die grafische Oberfläche der PowerShell ISE installiert sein. Dies ist sowohl in Windows 8.1 als auch in Windows Server 2012 R2 standardmäßig der Fall. Alle Befehle aus der normalen Eingabeaufforderung sind auch in der PowerShell verfügbar. Die Befehle werden dazu in PowerShell-Aliase übersetzt.

Unter Windows 8.1 und Windows Server 2012 R2 haben Sie den Vorteil, dass die Shell bereits in das Betriebssystem integriert und installiert ist. Die normale Eingabeaufforderung von Windows Server 2012 unterscheidet sich nicht von ihrem Pendant in Windows Server 2008 R2. Auch wenn Sie die Windows PowerShell als zusätzliche Funktion installieren, ändert sich die Eingabeaufforderung nicht, sondern Sie müssen die PowerShell über die entsprechende Verknüpfung erst starten.

In diesem Kapitel gehen wir auf Befehle und Funktionen ein, die in den anderen Kapiteln noch nicht behandelt wurden. Die meisten neuen Server-Produkte von Microsoft bauen auf die Windows PowerShell auf und ergänzen diese um weitere Befehle. Die grafischen Oberflächen dieser Produkte dienen dann nur noch dazu, Befehle zu generieren, sogenannten Cmdlets, die durch die PowerShell ausgeführt werden.

Mit dem Befehl *Get-Help <Befehl> –Detailed* erhalten Sie eine ausführliche Hilfe zu einem Befehl, Praxisbeispiele, alle Optionen und ausführliche Anleitungen. Beispiele erhalten Sie auch durch *Get-Help <Befehl> –Examples*.

Anwender mit Windows 7 SP1, Windows Server 2008 R2 SP1 und Windows Server 2012 installieren sich auf dem Rechner das Windows Management Framework 4.0 Preview (*http://www.microsoft.com/en-us/download/details.aspx?id=39347* [Ms179-K40-xx]). Ältere Versionen sind bei der PowerShell 4.0 außen vor. Wir zeigen Ihnen nachfolgend die besten Tricks speziell für die neue PowerShell 4.0. Alle Neuerungen zeigt Microsoft auch in der TechNet (*http://technet.microsoft.com/en-us/library/hh857339.aspx* [Ms179-K40-xx]).

Die PowerShell starten Sie entweder über die Verknüpfung auf der Startseite oder Sie geben *powershell* in einer Eingabeaufforderung ein. Innerhalb der PowerShell können Sie mit dem Befehl *ise* die grafische Oberfläche der PowerShell starten. Mit *cmd* gelangen Sie dann wieder zum Fenster der Eingabeaufforderung zurück.

Sie können die PowerShell auch über das Kontextmenü der *Start*-Schaltfläche starten, müssen dazu aber entsprechende Einstellungen in den Eigenschaften der Taskleiste auf der Registerkarte *Navigation* in Windows 8.1 und Windows Server 2012 R2 vornehmen.

Eine wesentliche Neuerung der PowerShell 4.0 ist die *Desired State Configuration* (DSC). Mit dieser neuen Funktion können Administratoren die Konfiguration von bestimmten Systemdiensten in Konfigurationsdateien speichern und auf Servern verteilen. Vor allem im Zusammenhang mit verschiedenen System Center-Produkten lassen sich auf diesem Weg Automatismen erstellen.

Sie können in der Datei zum Beispiel hinterlegen, dass bei der Ausführung auf einem Server bestimmte Dateien kopiert, Dienste gestartet oder installiert und Programme ausgeführt werden. Auch Systemeinstellungen wie die Aktivierung von DNS oder DHCP lassen sich in der Datei hinterlegen. Wurde die Steuerdatei erstellt, führen Sie diese mit dem neuen Cmdlet *Start-DscConfiguration* aus. Ausführliche Anleitungen zu den Möglichkeiten finden Sie in der TechNet (*http://blogs.technet.com/b/privatecloud/archive/2013/08/29/introducing-powershell-desired-state-configuration-dsc.aspx* [Ms179-K40-xx]).

Viele Hilfedaten der PowerShell sind nicht mehr auf dem Rechner gespeichert, sondern müssen aus dem Internet nachgeladen werden. Auf Rechnern ohne Internetverbindung geht das natürlich nicht. Sie haben in der PowerShell 4.0 aber die Möglichkeit, die Hilfe auf einem Rechner mit Internetverbindung zu speichern und auf einem anderen Rechner ohne Internetverbindung einzulesen. Dazu verwenden Sie das neue Cmdlet *Save-Help*.

Für die beiden Cmdlets *Register-ScheduledJob* und *Set-ScheduledJob* gibt es die neue Option *RunNow*. Entwickler müssen jetzt also keine Anfangs- und Endzeit mehr zwingend vorgeben.

In der PowerShell 4.0 ist die Ausführungsrichtlinie für Skripts jetzt standardmäßig auf *RemoteSigned* gesetzt. Diese Ausführungsrichtlinie bestimmt, ob Skripts ausgeführt werden dürfen und ob diese digital signiert sein müssen. Standardmäßig blockiert die PowerShell Skripts in PowerShell 3.0. In PowerShell 4.0 sind die Skripts erlaubt. Administratoren können die Ausführungsrichtlinie mit dem Cmdlet *Set-ExecutionPolicy* ändern und mit *Get-ExecutionPolicy* anzeigen. Dabei stehen folgende Einstellungen zur Verfügung:

- **Restricted** Standardeinstellung. Keine Skripts erlaubt.
- **AllSigned** Nur signierte Skripts sind erlaubt
- **RemoteSigned** Bei dieser Einstellung müssen Sie Skripts durch eine Zertifizierungsstelle signieren lassen
- **Unrestricted** Mit dieser Einstellung funktionieren alle Skripts

Rufen Sie in Windows 8.1 oder Windows Server 2012 R2 über das Kontextmenü der Taskleiste die Eigenschaften auf und wechseln Sie zur Registerkarte *Navigation*, lassen sich verschiedene Einstellungen vornehmen und beispielsweise festlegen, dass in Windows 8.1 der Desktop direkt nach dem Start anzeigt wird.

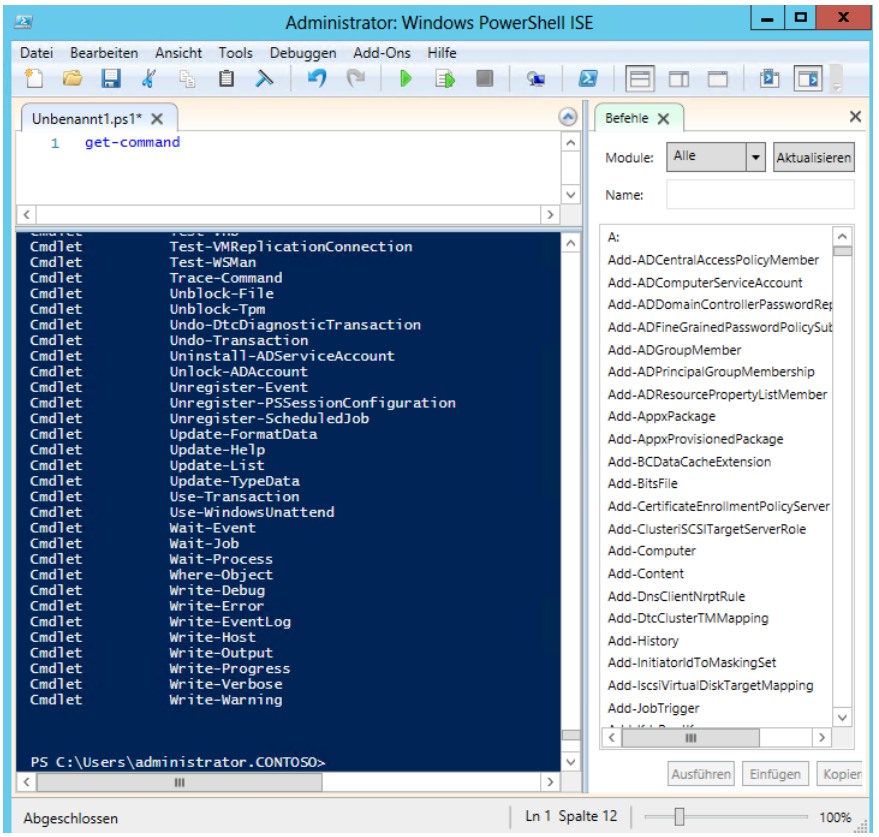
Aktivieren Sie das Kontrollkästchen *Beim Rechtsklick auf die untere linke Ecke oder beim Drücken von Windows-Taste+X "Eingabeaufforderung" im Menü durch "Windows PowerShell" ersetzen*, ersetzt Windows 8.1 die Eingabeaufforderung über das Kontextmenü der *Start*-Schaltfläche mit der Möglichkeit, die PowerShell zu starten. Die Option steht auch in Windows Server 2012 R2 zur Verfügung.

PowerShell und PowerShell ISE – Eine Einführung

Sie starten die PowerShell, indem Sie *powershell* auf der Startseite eingeben. Außerdem lässt sich die PowerShell im Explorer über die Registerkarte *Datei* öffnen. Im zugehörigen Untermenü kann die PowerShell auch mit Administratorrechten aufgerufen werden. Die herkömmliche Eingabeaufforderung mit den bekannten Befehlen steht auch weiterhin zur Verfügung. Dies gilt auch für die Unterstützung von VBScript.

Ebenfalls interessant ist die Oberfläche zur Erstellung von Skripts und Ausführung von Befehlen für die Windows PowerShell, das sogenannte Windows PowerShell Integrated Scripting Environment (ISE). Auch diese rufen Sie über die Startseite durch Eintippen von *powershell ise* auf. Die grafische Oberfläche bietet die Möglichkeit, Skripts für die Windows PowerShell in einer einheitlichen zentralen Oberfläche zu erstellen. In einer PowerShell-Sitzung starten Sie die grafische Oberfläche furch Eingabe von *ise*. Der Vorteil der PowerShell ISE ist, dass diese beim Eingeben von Befehlen bereits Vorschläge für Cmdlets unterbreitet, die Sie auswählen können. Außerdem sind die Befehle farblich besser hervorgehoben, sodass sich die einzelnen Optionen besser unterscheiden lassen.

Abbildg. 40.3 Die grafische Oberfläche der Windows PowerShell



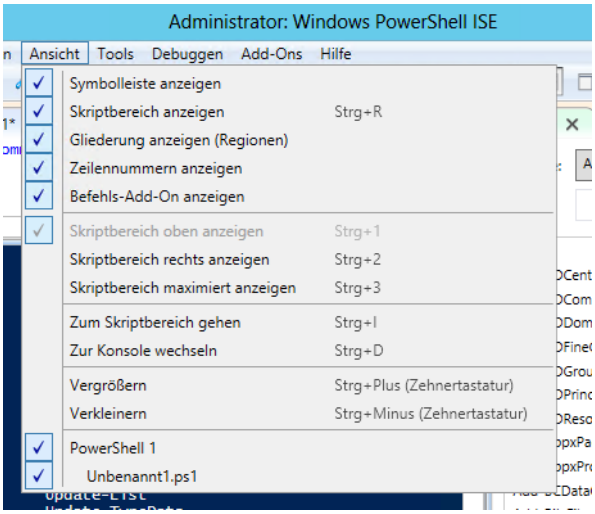
Im oberen Bereich können Sie Skriptbefehle angeben und diese dann als Skript speichern. In der Oberfläche können Sie außerdem eine PowerShell remote auf einem anderen Computer öffnen.

Verwenden Sie dazu das Menü *Datei*. Die PowerShell zeigt das ISE dann als zusätzliche Registerkarte an. Das heißt, durch diese Möglichkeiten erhalten Sie eine Oberfläche, in der Sie Befehle testen, deren Ergebnis anzeigen, Skripts schreiben und Fehler in den Skripts über den Menüpunkt *Debug* beheben können.

Geben Sie im oberen Bereich Befehle ein, werden diese nicht sofort ausgeführt, sondern wie in einem normalen Skript zunächst aufgelistet. Sind Sie fertig mit der Eingabe der Befehle, können Sie deren Ausführung starten, indem Sie auf das grüne Abspielsymbol mit der QuickInfo *Skript ausführen* klicken.

Über den Menüpunkt *Ansicht* können Sie die verschiedenen Bereiche des ISE an Ihre Bedürfnisse anpassen und die Anordnung ändern. So lässt sich zum Beispiel der Bereich zum Erstellen von Skripts an der rechten Seite anordnen.

Abbildg. 40.4 Anpassen des PowerShell ISE



Die Größe und Anzeige der verschiedenen Feldern lassen sich leicht anpassen. Skripts können Sie während der Ausführung bearbeiten und so Fehler schneller beheben. Laden Sie ein Skript über *Datei/Öffnen*, sehen Sie im Befehlsfenster dessen Bestandteile. Markieren Sie eine Zeile im Skript, können Sie über den Menüpunkt *Debuggen/Haltepunkt umschalten* eine Pause im Skript festlegen.

Generell ist der Umgang mit der PowerShell nicht sehr kompliziert. Geben Sie *Get-Command* ein, sehen Sie alle Befehle, welche die Shell zur Verfügung stellt. Die wenigsten Anwender kennen alle Cmdlets und deren verschiedenen Optionen, die Microsoft zur Verfügung stellt. Die Verwaltungsshell bietet jedoch eine ausführliche Hilfe an. Haben Sie nur den Teil eines Befehls in Erinnerung, können Sie mit dem Platzhalter * arbeiten.

Der Befehl *Get-Command *computer* zeigt zum Beispiel alle Cmdlets an, deren Namen mit »computer« endet. Ist der gesuchte Befehl nicht dabei, können Sie auch mehrere Platzhalter verwenden, zum Beispiel den Befehl *Get-Command *computer**. Dieser Befehl zeigt alle Befehle an, in denen an einer beliebigen Stelle das Wort »computer« vorkommt.

Haben Sie das gewünschte Cmdlet gefunden, unterstützt Sie die PowerShell aber mit weiteren Möglichkeiten. Für nahezu alle Cmdlets gilt die Regel, dass diese in vier Arten vorliegen: Es gibt Cmdlets mit dem Präfix New-, um etwas zu erstellen, zum Beispiel *New-Item*. Das gleiche Cmdlet gibt es dann immer noch mit Remove-, um etwas zu löschen, zum Beispiel *Remove-Item*. Wollen Sie das Objekt anpassen, gibt es das Präfix Set- zum Beispiel *Set-Item*. Als Letztes gibt es noch das Cmdlet Get-, zum Beispiel *Get-Item*, um Informationen zum Objekt abzurufen.

Neben diesen Cmdlets gibt es natürlich noch viele andere, zum Beispiel Start- und Stop- oder Export- und Import-Cmdlets. Allerdings bestehen die meisten Administrationsausgaben aus den erwähnten New-, Remove-, Set- und Get-Cmdlets. Geben Sie nur diesen Befehl ein, passiert entweder überhaupt nichts, das Cmdlet zeigt Objekte an, oder Sie werden nach der Identität des Objekts gefragt.

Mit *Get-Cmdlets* lassen Sie sich Informationen zu Objekten anzeigen. Die Option *|fl* formatiert die Ausgabe. Wollen Sie aber nicht alle Informationen, sondern nur einzelne Parameter anzeigen, können Sie diese nach der Option *|fl* anordnen. Dazu geben Sie einfach eine der Spalten an, die Sie mit dem Get-Cmdlet abgefragt haben.

Über den Menübefehl *Datei/Neue Remote-PowerShell-Registerkarte* können Sie eine PowerShell-Sitzung auf einem anderen Computer aufbauen. Wir gehen auf diese Thematik in diesem Kapitel noch genauer ein.

Damit dies funktioniert, müssen Sie auf dem Zielcomputer aber die Remoteverwaltung zunächst über die Eingabeaufforderung mit *winrm quickconfig* starten. Anschließend müssen Sie sich noch authentifizieren, wenn Sie sich mit einem anderen Benutzer als dem aktuell angemeldeten am Server anmelden wollen. Danach baut die PowerShell eine Sitzung auf und Sie können auf dem Quellserver Befehle eingeben, die auf dem Zielserver ausgeführt werden.

Damit Sie einen Computer über die PowerShell remote verwalten können, müssen Sie außerdem die Remoteverwaltung auf dem Computer aktivieren. Dazu geben Sie auf dem entsprechenden Computer noch den Befehl *Enable-PSRemoting -force* in der PowerShell ein.

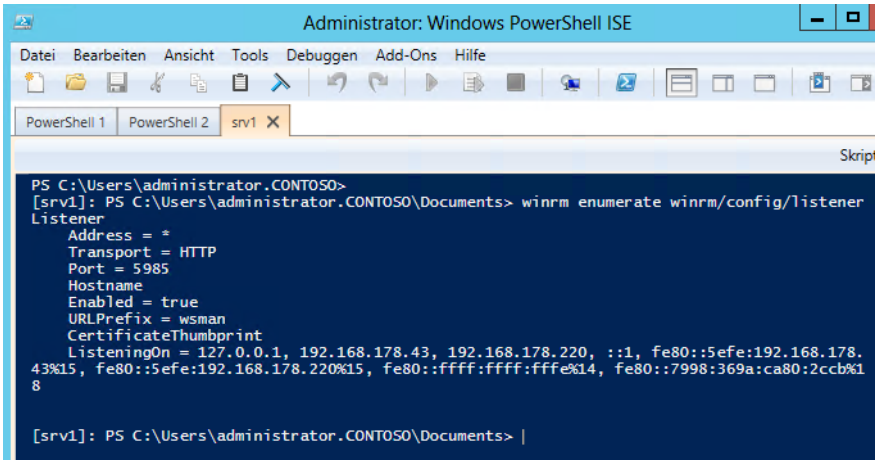
Der Befehl aktiviert auch die Ausnahmen in der Windows-Firewall. Mit *Disable-PSRemoting –Force* können Sie die Remoteverwaltung eines Computers über die PowerShell wieder deaktivieren. Sie müssen für solche administrativen Befehle die PowerShell über die App-Leiste (Klick mit der rechten Maustaste) auf der Startseite mit Administratorrechten starten.

Um den Port für die Verbindung zu überprüfen, verwenden Sie den Befehl *winrm enumerate winrm/config/listener*. Der Listener verwendet den Port 5985. Funktioniert der Zugriff nicht, können Sie auf dem Zielcomputer auch eine Liste von Computern pflegen, die Zugriff auf Remote-PowerShell-Sitzungen haben sollen. Dazu verwenden Sie den Befehl:

```
winrm set winrm/config/client @{TrustedHosts="<Alle Quellcomputer, durch Komma getrennt>"}
```

Auf Servern und Computern die Mitglied einer Domäne sind, funktionieren diese Sitzungen am besten und einfachsten.

Abbildg. 40.5 PowerShell-Remotesitzungen parallel zu lokalen Sitzungen verwenden



In Remote-PowerShell-Sitzungen verwenden Sie die gleichen Cmdlets wie auf den lokalen Computern. Allerdings erlauben nicht alle Cmdlets eine Remoteverwaltung. Sie sehen die kompatiblen Cmdlets am schnellsten, indem Sie überprüfen, ob das Cmdlet die Option *–ComputerName* unterstützt. Mit dem Befehl *Get-Help * –Parameter ComputerName* lassen Sie sich eine Liste aller dieser Cmdlets anzeigen. Hier zeigt sich auch eine Neuerung in der PowerShell.

Eine der wichtigsten Neuerungen der PowerShell ist die Unterstützung für Skriptbefehle, die sehr lange andauern, zum Beispiel zur Wartung oder der Datensicherung, sowie der Verteilung von Anwendungen. Microsoft hat dazu Funktionen der Windows Workflow Foundation (WWF) in die PowerShell integriert. Diese Technik erlaubt auch das parallele Ausführen von mehreren Befehlen. Aktionen lassen sich in Abhängigkeit voneinander setzen und mit Bedingungen konfigurieren. Allerdings ist dieser Bereich etwas komplexer zu bedienen.

Sitzungen über das Netzwerk lassen sich trennen und wieder erneut aufbauen. Dazu gibt es die beiden neuen Cmdlets *Disconnect-PSSession* und *Connect-PSSession*. Auch das Rechtemodell hat Microsoft verbessert und eine Delegierung von Berechtigungen integriert, um Benutzer mit weniger Rechten die Ausführung von Skripts zu erlauben.

In der neuen Version können Sie auch von öffentlichen Netzwerken aus zugreifen. Dazu ist die Option *–SkipNetworkProfileCheck* von *Enable-PSRemoting* und *Set-WSManQuickConfig* integriert worden. Die Option erstellt automatisch Firewallregeln, die den Zugriff erlauben.

Um eine Remotesitzung aufzubauen, verwenden Sie auch das Cmdlet *New-PSSession*. Mit *Enter-PSSession <Servername>* bauen Sie eine Verbindung auf. Mit *Exit-Session* beenden Sie diese Sitzung wieder. Neu ist die Möglichkeit, Sitzungen zu unterbrechen und erneut aufzubauen. Bei unterbrochenen Sitzungen laufen die Cmdlets weiter, auch wenn sich Administratoren vom Server getrennt haben. Dazu nutzen Sie die neuen Cmdlets *Disconnect-PSSession*, *Connect-PSSession* und *Receive-PSSession*.

Abbildg. 40.6 Erstellen einer neuen Remote-PowerShell-Sitzung

```
PS C:\Users\administrator.CONTOSO> new-pssession dc01.contoso.int

 Id Name            ComputerName    State         ConfigurationName     Availability
 -- ----            ------------    -----         -----------------     ------------
  1 Session1        dc01.contoso... Opened        Microsoft.PowerShell     Available

PS C:\Users\administrator.CONTOSO> disconnect-pssession 1

 Id Name            ComputerName    State         ConfigurationName     Availability
 -- ----            ------------    -----         -----------------     ------------
  1 Session1        dc01.contoso... Disconnected  Microsoft.PowerShell         None

PS C:\Users\administrator.CONTOSO> connect-pssession 1

 Id Name            ComputerName    State         ConfigurationName     Availability
 -- ----            ------------    -----         -----------------     ------------
  1 Session1        dc01.contoso... Opened        Microsoft.PowerShell     Available

PS C:\Users\administrator.CONTOSO> receive-pssession 1
PS C:\Users\administrator.CONTOSO> _
```

PowerShell-Aufgaben lassen sich in der PowerShell auch zeitgesteuert starten. In der PowerShell können Sie die entsprechenden Einstellungen direkt im Skript vornehmen, ohne auf die Aufgabenplanung des Betriebssystems setzen zu müssen. Dazu stellt Microsoft das neue PowerShell-Modul *PSScheduledJob* zur Verfügung. Alle verfügbaren Befehle lassen Sie sich mit *Get-Command -Module PSScheduledJob | Sort-Object Noun, Verb* anzeigen. Microsoft zeigt in einem Blogbeitrag den Umgang mit der neuen Funktion (*http://blogs.msdn.com/b/powershell/archive/2012/03/19/scheduling-background-jobs-in-windows-powershell-3-0.aspx* [Ms179-K40-05]).

Die grundsätzliche Funktionsweise der PowerShell

Grundlage der PowerShell sind die Cmdlets. Diese sind die Befehle in der Shell, auf der diese aufbaut. 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 rufen Sie mit Get-Cmdlets Daten ab, mit Set-Cmdlets erzeugen und ändern Sie Daten, mit Format-Cmdlets Daten formatieren Sie und mit Out-Cmdlets leiten Sie Ausgaben an ein angegebenes Ziel um.

Zur Anzeige einer Liste aller Befehle verwenden Sie den Befehl *Get-Command*. Über *Get-Command >C:\befehle.txt* lenken Sie alle Befehle in die Datei *C:\befehle.txt* um. Mit dem Befehl *Update-Help* lassen Sie die Hilfedateien der PowerShell über eine bestehende Internetverbindung aktualisieren.

Wenn Sie für das Cmdlet *Get-Help* die Option *–Online* verwenden, zum Beispiel mit *Get-Help Get-Command –Online*, öffnet sich ein Browserfenster mit einer ausführlichen Hilfe zum Befehl. Der Befehl *Show-Command* zeigt ein Fenster mit allen verfügbaren Befehlen in der PowerShell an.

Über die PowerShell lassen sich auch Einstellungen der Systemsteuerung öffnen, auch über das Netzwerk. Um zum Beispiel alle Tools der Systemsteuerung in der PowerShell anzuzeigen, hilft das Cmdlet *Get-ControlPanelItem*. Um ein Programm zu öffnen, verwenden Sie den Befehl *Show-ControlPanelItem*.

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 Framework auf und kann .NET-Objekte akzeptieren und zurückgeben. Diese grundlegende Änderung ermöglicht es, neue Tools und Skriptverfahren für die Verwaltung und Konfiguration von Windows zu verwenden. Standardmäßig ist die PowerShell mit der Installation von Windows 8 automatisch integriert.

Außerdem hat Microsoft zahlreiche zusätzliche Cmdlets integriert, zum Beispiel *Get-Hotfix, Send-MailMessage*, *Get-ComputerRestorePoint*, *New-WebServiceProxy*, *Debug-Process, Add-Computer, Rename-Computer, Reset-ComputerMachinePassword* oder *Get-Random*. Neu ist auch die Möglichkeit, PowerShell-Skripts als Aufgabe im Hintergrund auszuführen. Dazu hat Microsoft einige neue Cmdlets zur Verwaltung dieser Aufgaben eingebaut. Geben Sie in der PowerShell den Befehl *Get-Command *job** ein, erhalten Sie eine Liste der neuen Möglichkeiten angezeigt, um Skripts im Hintergrund laufen zu lassen.

Die PowerShell verfügt über einige neue Cmdlets, um Netzwerkeinstellungen eines Computers zu steuern oder abzufragen, zum Beispiel *Get-NetIPAddress*. Um sich eine Liste aller Cmdlets anzuzeigen, mit denen sich Netzwerkeinstellungen festlegen lassen, hilft der Befehl *Get-Command –Noun Net**.

Sie können aber nicht nur Informationen auslesen, sondern auch bearbeiten, wie die folgenden Beispiele für die Registry oder einzelne Dateien zeigen. Der Befehl *Remove-Item C:\Scripts* –Exclude *.doc* löscht alle Dateien, außer denen, die Sie mit *–Exclude* ausgeschlossen haben. *Remove-Item C:\Scripts* –Include .xls,.doc* löscht nur die Dateien hinter *–Include*.

Beide Optionen können Sie auch gemeinsam verwenden, zum Beispiel: *Remove-Item C:\Scripts* –Include *.txt –Exclude *test**. Hier löscht die PowerShell alle Textdateien im Ordner, 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*.

Statt *Remove-Item* können Sie auch *ri, rd, erase, rm, rmdir* oder *del* verwenden. Vorhandene Objekte benennen Sie mit dem Cmdlet *Rename-Item* um: *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* und kann auch den Inhalt von Registryschlüsseln anzeigen.

Mit *Get-ChildItem –Recurse* wird zusätzlich der Inhalt der Unterordner angegeben, ähnlich zu *dir /s*, nur übersichtlicher. Die Anweisung *Get-ChildItem HKLM:\SOFTWARE* zeigt den Inhalt des Registryschlüssels *HKLM\SOFTWARE* an.

Durch die PowerShell-Laufwerke können Sie alle Registryschlüssel auf diese Weise auslesen. Auch hier lässt sich mit den beiden Optionen *–Include* und *–Exclude* arbeiten: *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 Sie auch die Aliase *gci, ls* und *dir* verwenden. 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*, falls es keine solche Datei gibt. Auch hier können Sie mit Platzhaltern arbeiten.

Die Anweisung *Test-Path HKCU:\Software\Microsoft\Windows* testet, ob ein bestimmter Registryschlüssel vorhanden ist. Mit dem Cmdlet *Invoke-Item* können Sie über die Windows-PowerShell eine ausführbare Datei starten oder eine Datei öffnen: *Invoke-Item C:\Windows\System32\Calc.exe*. Statt *Invoke-Item* können Sie auch *ii* verwenden.

Mit der verbesserten *Where*-Abfrage lassen sich Informationen auch filtern. Sollen zum Beispiel alle gestoppten Systemdienste in der PowerShell angezeigt werden, geben Sie den Befehl *Get-Service | Where-Object {$_.Status –Eq "Stopped"}* ein.

Auch auf die Ereignisanzeige lässt sich zugreifen. Um zum Beispiel die *x* neuesten Fehlermeldungen in der Ereignisanzeige *System* in der PowerShell zu betrachten, geben Sie den Befehl *Get-EventLog-System –Newest 100 | Where {$_.entryType –Match "Error"}* ein.

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 bezeichnet die Shell als Windows PowerShell-Laufwerke. Eine entsprechende Liste rufen Sie mit dem Befehl *Get-PSDrive* auf.

Abbildg. 40.7 Anzeigen der Laufwerke, auf welche die PowerShell zugreifen kann

```
PS C:\Users\administrator.CONTOSO> get-psdrive

Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
Alias                                  Alias
C                 281,23         25,20 FileSystem    C:\
Cert                                   Certificate   \
D                                      FileSystem    D:\
Env                                    Environment
Function                               Function
HKCU                                   Registry      HKEY_CURRENT_USER
HKLM                                   Registry      HKEY_LOCAL_MACHINE
Variable                               Variable
WSMan                                  WSMan
```

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.

Durch die zahlreichen neuen Cmdlets in der PowerShell erhalten Sie für Anmeldeskripts deutlich mehr Möglichkeiten. In der neuen Version lassen sich jetzt auch Netzlaufwerke in Windows verbinden. Dazu verwenden Sie das Cmdlet *New-PSDrive*. Dabei hilft die neue Option *–Persist*. Alle Optionen des Cmdlets sind über *Get-Help New-PSDrive –Detailed* verfügbar.

Sie können in der PowerShell aber auch mit den echten physischen Laufwerken auf dem PC arbeiten. Um zum Beispiel die physischen Festplatten abzufragen, hilft der Befehl *Get-PhysicalDisk*. Die Ausgabe zeigt auch an, ob sich die Platte in einem neuen Speicherpool anordnen lässt (siehe Kapitel 5). Das erkennen Sie an der Option *CanPool* über den Wert *True*.

Wer genauere Informationen will, gibt *Get-PhysicalDisk |fl* ein. Durch Eingabe von Spaltenbezeichnungen nach *|fl* lassen sich erweiterte Informationen angeben und unwichtige ausblenden. Ein Beispiel dafür ist *Get-PhysicalDisk |fl FriendlyName, BusType, CanPool, Manufacturer, Healthstatus*. Das funktioniert mit allen Get-Cmdlets.

Um einen neuen Speicherpool zu erstellen, bietet es sich zum Beispiel an, Festplatten, die poolfähig sind, also bei der Option *CanPool* den Wert *True* aufweisen, in einer Variablen zu speichern. Diese Variable können Sie dann an das Cmdlet *New-StoragePool* weitergeben, um einen Speicherpool zu erstellen.

Ist erst ein Pool erstellt, können Sie virtuelle Laufwerke erstellen, die sogenannten Speicherplätze (Storage Spaces). Auch dieser Vorgang lässt sich leicht in der PowerShell durchführen. Dabei hilft das Cmdlet *New-VirtualDisk*.

Ein weiterer Vorteil der PowerShell liegt darin, dass Sie viele vertraute Tools der normalen Eingabeaufforderung nicht aufgeben müssen. Diese werden auch von der PowerShell unterstützt. Dazu gibt es für jeden Cmdlet-Befehl einen PowerShell-Alias. Die Verwendung dieser Befehle ist analog zur bisherigen Eingabeaufforderung, die natürlich noch immer parallel zur Verfügung steht. Über den Befehl *Alias* zeigt die PowerShell alle Aliase in der Eingabeaufforderung an. Mit dem Befehl *Alias <Buchstabe>** lassen Sie sich die einzelnen Aliase, die mit dem angegebenen Buchstaben beginnen, anzeigen.

Der Vorteil der Ausführung in der PowerShell ist, dass sich die Ausgabe auch filtern lässt. Geben Sie zum Beispiel *ipconfig /all* ein, erhalten Sie die gleichen Informationen wie in der Eingabeaufforderung. Es sind also keine zwei Konsolen nebeneinander notwendig.

Soll die Ausgabe gefiltert werden, hilft die Option *Select-String –Pattern "<Text>"*, zum Beispiel *ipconfig /all | Select-String –Pattern "gateway"*. Auf diesem Weg lassen sich Informationen wesentlich gezielter auslesen.

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).

Sie müssen immer einen vollqualifizierten Pfad zu der Skriptdatei angeben, auch wenn sich das Skript im aktuellen Ordner befindet. Wenn Sie auf den aktuellen Ordner verweisen wollen, 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 blockiert die PowerShell Skripts.

Sie können die Ausführungsrichtlinie mit dem Cmdlet *Set-ExecutionPolicy* ändern und mit *Get-ExecutionPolicy* anzeigen. Sie können folgende Einstellungen vornehmen:

- **Restricted** Standardeinstellung. Keine Skripts erlaubt.
- **AllSigned** Nur signierte Skripts sind erlaubt
- **RemoteSigned** Bei dieser Einstellung müssen Sie Skripts durch eine Zertifizierungsstelle signieren lassen
- **Unrestricted** Mit dieser Einstellung funktionieren alle Skripts

Nach der Eingabe von *Set-ExecutionPolicy Unrestricted* müssen Sie die Ausführung noch bestätigen. Anschließend funktionieren eigene Skripts.

Die Ausführungsrichtlinie speichert ihre Daten in der Windows-Registrierung. Mit dem Cmdlet *Start-Sleep* stoppen Sie Windows PowerShell-Aktivitäten für einen bestimmten Zeitraum. Mit dem Befehl *Start-Sleep –s 10* hält das Skript zehn Sekunden an. *Start-Sleep –m 10000* verwendet Millisekunden. Übergeben Sie die Ausgabe von Cmdlets mit der Option | *Out-Printer* an das Cmdlet *Out-Printer*, druckt die PowerShell die Ausgabe auf dem Standarddrucker aus.

Den Drucker können Sie auch in Anführungszeichen und der Bezeichnung in der Druckersteuerung angeben. Mit dem Cmdlet *Write-Warning* lassen sich eigene Warnungen in der PowerShell anzeigen. *Write-Host* schreibt Nachrichten. Beide sind farblich unterschiedlich formatiert. Farbzuweisungen lassen sich nur für *Write-Host* setzen. Die Farben konfigurieren Sie mit *–ForeGroundColor* und *–BackGroundColor* manuell. 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* starten Sie in der Windows-PowerShell ein Skript:

```
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 Befehlsreferenz anzeigen zu lassen. Über *Get-Command >C:\befehle.txt* lenken Sie alle Befehle in die Datei *C:\befehle.txt* um. Sie erhalten wie immer bei der Dateiumleitung keine Bestätigung der Ausführung.

Grundlagen zur Serververwaltung mit der PowerShell

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 Add-Computer –Detailed*. Über die Tastenkombination Strg+C können Sie innerhalb der Shell einzelne Aktionen stoppen.

Wollen Sie von einem Server mit Windows Server 2008 R2 oder Windows Server 2012 Serverdienste verwalten, die auf dem Server nicht aktiviert sind, können Sie auch hier die Verwaltungstools installieren. Dazu benötigen Sie aber keine Patches, sondern können die entsprechenden Tools direkt über den Server-Manager aktivieren. Die Installation erfolgt im Server-Manager über die Auswahl *Verwalten/Rollen und Features hinzufügen*.

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.

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 beispielsweise 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 auch möglich, per Eingabe des Befehls *$heute.ToString("MMMM")* die Ausgabe des Monats oder über *$heute.ToString("MM")* den Monat als Zahl innerhalb des Kalenderjahres zu erzwingen. 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. Sie können ermitteln, welche Art von Objekt von einem bestimmten Cmdlet abgerufen wird, indem Sie die Ergebnisse des Befehls *Get* mit einem Pipelineoperator (|) an den Befehl *Get-Member* übergeben. So können Sie mit dem Befehl *Get-Service | Get-Member* abgerufenen Objekte an *Get-Member* senden.

Mit diesem Befehl lassen sich Informationen über das .NET-Objekt anzeigen, das von einem Befehl zurückgegeben wird. Zu den Informationen zählen der Typ, die Eigenschaften und die Methoden des Objekts. Wenn Sie beispielsweise alle Eigenschaften eines Dienstobjekts anzeigen wollen, geben Sie *Get-Service | Get-Member –MemberType *property* ein.

Eine häufige Administrationsaufgabe ist die Verwaltung der laufenden Prozesse auf einem Server. Über den Befehl *Get-Process* können Sie sich alle laufenden Prozesse eines Computers anzeigen lassen. Wollen Sie aber zum Beispiel nur alle Prozesse mit dem Anfangsbuchstaben »S« angezeigt bekommen, geben Sie den Befehl *Get-Process s** ein. Sollen die Prozesse zusätzlich noch sortiert werden, zum Beispiel absteigend nach der CPU-Zeit, geben Sie *Get-Process s** gefolgt von der Pipe-Option *|Sort-Object cpu –Descending* ein.

In diesem Abschnitt zeigen wir Ihnen einige Cmdlets, die in der Praxis sehr nützlich sind und die Möglichkeiten der PowerShell im Vergleich zur herkömmlichen Eingabeaufforderung verdeutlichen. Mit dem Cmdlet *Copy-Item* kopieren Sie Dateien oder Ordner in der PowerShell. Mit dem Befehl *Copy-Item C:\Scripts\test.txt C:\Test* kopieren Sie zum Beispiel die Datei *test.txt*. Die Syntax ist ähnlich zum *Copy*-Befehl der herkömmlichen Eingabeaufforderung.

Der Befehl *Copy-Item C:\Scripts* C:\Test* kopiert alle Dateien im entsprechenden Quellordner in den Zielordner. Der Befehl *Copy-Item C:\Scripts C:\Test –Recurse* legt eine Kopie des Ordners *C:\Scripts* im Ordner *C:\Test* an. Ohne die Option *–Recurse* wird in *C:\Test* ein Ordner *Scripts* angelegt, es werden 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 können Sie wieder mit Platzhaltern arbeiten, 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* verschieben Sie Dateien und benennen diese gleichzeitig um.

Neben *Move-Item* können Sie auch mit *mi, mv* oder *move* arbeiten. Mit dem Cmdlet *New-Item* erstellen Sie neue Dateien oder Ordner. Mit dem Befehl *New-Item C:\Temp\PowerShell –Type Directory* erstellen Sie im Ordner *C:\Temp* einen neuen leeren Ordner mit der Bezeichnung *PowerShell*.

Um eine neue Datei zu erstellen, verwenden Sie die gleiche Syntax, aber den Typ *File*: *New-Item C:\Scripts\skript.txt –Type File*. Mit dem Befehl *New-Item C:\Scripts\skript.txt –Type File –Force* ersetzen Sie eine vorhandene Datei durch eine neue leere Datei. Mit dem Befehl *New-Item C:\Scripts\skript.txt –Type File –Force –Value "Text"* erstellen Sie eine neue Datei mit dem angegebenen Text als Inhalt. Statt *New-Item* können Sie auch *ni* verwenden.

Mit dem Cmdlet *Add-Content* fügen Sie Daten an eine Textdatei an: *Add-Content C:\Scripts\test.txt "Text"*. Standardmäßig fügt *Add-Content* den neuen Wert hinter dem letzten Zeichen in der Textdatei ein.

Den Inhalt einer Datei ersetzen Sie mit *Set-Content*. Das Cmdlet *Clear-Content* löscht den Inhalt einer Datei. Nach der Ausführung existiert die Datei weiterhin, hat aber keinen Inhalt mehr. Auch hier können Sie mit Platzhalterzeichen arbeiten: *Clear-Content C:\Test\e**. Neben Textdateien unterstützt das Cmdlet auch Excel-Tabellen, Word-Dokumente und andere Dateien. Statt *Clear-Content* können Sie auch *clc* verwenden. Das Cmdlet *Remove-Item* löscht Objekte: *Remove-Item C:\Scripts\test.txt*.

Mit dem Platzhalterzeichen * löschen Sie Objekte in einem angegebenen Ordner: *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 Sie mit *–Exclude* ausgeschlossen haben. *Remove-Item C:\Scripts* –Include .xls,.doc* löscht nur die Dateien hinter *–Include*. Beide Optionen können Sie auch gemeinsam verwenden, zum Beispiel: *Remove-Item C:\Scripts* –Include *.txt –Exclude *test**.

Hier löscht die PowerShell alle Textdateien im Ordner, 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*.

Statt *Remove-Item* können Sie auch *ri, rd, erase, rm, rmdir* oder *del* verwenden. Vorhandene Objekte benennen Sie mit dem Cmdlet *Rename-Item* um: *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* und kann auch den Inhalt von Registryschlüsseln anzeigen.

Mit *Get-ChildItem –Recurse* wird auch der Inhalt der Unterordner angegeben, ähnlich zu *dir /s*, nur übersichtlicher. *Get-ChildItem HKLM:\SOFTWARE* zeigt den Inhalt des Registryschlüssels HKLM an.

Durch die PowerShell-Laufwerke können Sie alle Registryschlüssel auf diese Weise auslesen. Auch hier können Sie mit den beiden Optionen *–Include* und *–Exclude* arbeiten. Diese beiden Optionen funktionieren an allen Stellen der PowerShell, auch bei der Anzeige von Informationen und Inhalten eines Ordners: *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 Sie auch die Aliase *gci, ls* und *dir* verwenden. 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 können Sie mit Platzhaltern arbeiten.

Die Anweisung *Test-Path HKCU:\Software\Microsoft\Windows* testet, ob ein bestimmter Registryschlüssel vorhanden ist. Mit dem Cmdlet *Invoke-Item* können Sie über die Windows PowerShell eine ausführbare Datei starten oder eine Datei öffnen: *Invoke-Item C:\Windows\System32\Calc.exe*. Statt *Invoke-Item* können Sie auch *ii* verwenden.

TIPP Im Internet gibt es zahlreiche Communities und Zusatzprodukte, welche den Nutzen der PowerShell weiter verbessern. 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. Wichtige Internetseiten für den Umgang mit der Windows PowerShell finden Sie unter:

- *http://www.powershell-ag.de* [Ms179-K40-06]
- *http://www.it-visions.de/scripting/powershell* [Ms179-K40-07]
- *http://www.nsoftware.com/powershell* [Ms179-K40-08]
- *http://powergui.org* [Ms179-K40-09]
- *http://gallery.technet.microsoft.com/scriptcenter* [Ms179-K40-10]
- *http://blogs.msdn.com/b/powershell* [Ms179-K40-11]

Dienste in der PowerShell und der Eingabeaufforderung steuern

Dienste können Sie in der PowerShell mit *Start-Service, Stop-Service, Get-Service* und *Set-Service* starten und beenden. Auch die Befehlszeilentools *net start* und *net stop* helfen bei der Verwaltung der Systemdienste. Am schnellsten rufen Sie die Verwaltungsoberfläche der Systemdienste in Windows durch die Eingabe von *services.msc* auf. In der Eingabeaufforderung sehen Sie die gestarteten Dienste über *net start*. Mit *net start >dienste.txt* werden alle gestarteten Dienste in die Datei *dienste.txt* gespeichert.

Eine weitere Möglichkeit ist der Befehl *sc query*, der deutlich mehr Informationen liefert. Dienste lassen sich, neben der grafischen Oberfläche, in der Eingabeaufforderung über *net stop <Dienstname>* stoppen und über *net start <Dienstname>* wieder starten.

Windows-Firewall in der PowerShell steuern

In Windows 8.1 und Windows Server 2012 R2 können Sie mit der PowerShell so gut wie alle Einstellungen vornehmen, die auch in der grafischen Oberfläche möglich sind. Vorteil bei der Verwendung der PowerShell ist die Möglichkeit, die Konfiguration zu skripten oder zu automatisieren.

Neben der PowerShell lassen sich viele Einstellungen der Windows-Firewall auch in der Eingabeaufforderung durchführen. Dazu wird der Befehl *netsh.exe* mit der Option *advfirewall* genutzt, zum Beispiel:

```
Netsh advfirewall firewall add rule name="All ICMP V4 Allow" dir=in action=allow
protocol=icmpv4
```

Verwenden Sie als Befehl *netsh firewall set opmode disable*, wird die Firewall deaktiviert. Allerdings müssen Sie diesen Befehl über das Kontextmenü als Administrator starten. Mit dem Befehl *netsh firewall set opmode enable* aktivieren Sie die Firewall wieder. Auch dazu benötigen Sie administrative Rechte.

TIPP Ändern Sie Einstellungen in der Firewall, die Sie wieder rückgängig machen wollen, aktivieren Sie für die Firewall einfach wieder die Standardeinstellungen, zum Beispiel mit dem Befehl:

```
Netsh advfirewall reset
```

Um sich eine Liste der vorhandenen Firewall-Regeln anzuzeigen, verwenden Sie den folgenden Befehl:

```
Netsh advfirewall firewall show rule name=all
```

Den Status der einzelnen Profile der Firewall lassen Sie zum Beispiel mit diesem Befehl anzeigen:

```
netsh advfirewall show allprofiles
```

Wie Sie eine Firewallregel über das Netzwerk und die PowerShell auf alle Rechner mit Windows Server 2012 R2 oder Windows 8.1 kopieren, erfahren Sie in einem Blogbeitrag im TechNet (*http://blogs.technet.com/b/heyscriptingguy/archive/2012/11/13/use-powershell-to-create-new-windows-firewall-rules.aspx* [Ms179-K40-xx]). Alle Cmdlets für die Windows-PowerShell sind ebenfalls in der TechNet zu finden (*http://technet.microsoft.com/en-us/library/jj554906.aspx* [Ms179-K40-xx]).

In aktuellen Windows-Versionen sollten Sie aber besser auf die PowerShell setzen, um die Firewall zu konfigurieren. Hier stehen mehr Möglichkeiten zur Verfügung und auch andere Einstellungen lassen sich konfigurieren. Alle verfügbaren Befehle lassen sich am besten mit dem Befehl *Get-Command -Module Netsecurity* anzeigen. Wie bei allen Cmdlets kann auch für die Cmdlets der Firewall eine Hilfe angezeigt werden. Dazu steht in der PowerShell der Befehl *Get-Help <Cmdlet>* zur Verfügung. Mit der Option *-Examples* zeigt die PowerShell Beispiele an.

Um zum Beispiel eine neue Firewallregel zu erstellen, hilft der folgende Befehl:

```
New-NetFirewallRule -DisplayName "ICMP block" -Direction Inbound -Protocol icmp4 -Action
Block
```

Remotezugriff auf Rechner in der Eingabeaufforderung erlauben

Bei Windows Server 2012 R2 kann es passieren, dass Dienste über das Netzwerk keine Verbindung mit WMI zum Quellserver aufbauen können. In diesem Fall müssen Sie die WMI-Regeln für die Windows-Firewall zunächst aktivieren, um die Kommunikation zu gestatten. Dazu verwenden Sie am besten den folgenden Befehl:

```
Netsh advfirewall firewall set rule group="Windows-Verwaltungsinstrumentation (WMI)" new
enable=yes
```

Um einen Server remote im Netzwerk zu verwalten, müssen Sie diese Zugriffe ebenfalls erst erlauben:

```
Netsh advfirewall set allprofiles settings remotemanagement enable
```

Alternativ kann der Aufruf auch folgendermaßen aussehen:

```
Netsh advfirewall firewall set rule group="remoteverwaltung" new enable=yes
```

Um testweise den kompletten Datenverkehr auf Computern freizuschalten, verwenden Sie den folgenden Befehl:

```
Netsh advfirewall set allprofiles firewallpolicy allowin-bound,allowoutbound
```

In der PowerShell nutzen Sie dazu diesen Befehl:

```
Set-NetFirewallProfile -DefaultInboundAction Block -DefaultOutboundAction Allow -
NotifyOnListen True
```

TIPP Damit Sie mit der PowerShell von einem Rechner auf den anderen zugreifen können, müssen Sie noch den Remotezugriff aktivieren. Das können Sie auf dem Rechner zum Beispiel mit dem Cmdlet *Enable-PSRemoting –force* erledigen.

Firewallregeln in der PowerShell erstellen, ändern, löschen und kopieren

Anstatt mit *New-NetFirewallRule* eine neue Firewallregel zu erstellen, ist es häufig einfacher, Firewallregeln zu kopieren. Dazu steht der Befehl *Copy-NetFirewallRule* zur Verfügung. Auch IPsec-Regeln lassen sich kopieren. Dazu wird das Cmdlet *Copy-NetIPsecRule* verwendet.

Umbenennen lassen sich Firewallregeln anschließend mit dem Cmdlet *Rename-NetFirewallRule*. Beim Kopieren können Sie einen neuen Namen angeben. Ein entsprechender Aufruf könnte beispielsweise so aussehen:

```
Copy-NetFirewallRule -DisplayName "Require Outbound Authentication" -NewName "Alternate
Require Outbound Authentication"
```

Löschen können Sie Firewallregeln mit *Remove-NetFirewallRule*.

Firewallregeln lassen sich auch mit Gruppenrichtlinien verteilen. Hier haben Sie ebenfalls die Möglichkeit, die Firewallregeln eines Domänenprofils zu kopieren, die mit einer bestimmten GPO im Unternehmen verteilt werden. Die Syntax dazu lautet:

```
Get-NetFirewallProfile -Profile Domain -PolicyStore <FQDN der Domäne>\<Name der GPO> |
Copy-NetFirewallRule -NewPolicyStore <FQDN der Domäne>\<Neue GPO>
```

Im vorangegangenen Profil ist auch das Cmdlet *Get-NetFirewallProfil* eingebunden. Mit diesem Cmdlet lassen sich Firewallregeln in der PowerShell anzeigen.

Firewall in der PowerShell steuern und Regeln aktivieren oder deaktivieren

Neben dem Erstellen und Anpassen von Firewallregeln können Sie auch die PowerShell als Ganzes steuern. Auf diesem Weg lassen sich Firewallregeln zeitweise deaktivieren (*Disable-NetFirewallRule*) und dann wieder aktivieren (*Enable-NetFirewallRule*). Die Syntax ist recht einfach:

```
Disable-NetFirewallRule –DisplayName "<Anzeigename>"
```

Mit dem folgenden Cmdlet ist es zum Beispiel möglich, alle Firewallregeln einer bestimmten Gruppenrichtlinie zu deaktivieren:

```
Disable-NetFirewallRule –Direction Outbound -PolicyStore <Domäne>\<GPO>
```

Um alle Firewallregeln eines Rechners in einer Variablen zu speichern, verwenden Sie zum Beispiel diesen Aufruf:

```
$Rules = Get-NetFirewallRule -PolicyStore ActiveStore -PolicyStoreSourceType Dynamic
```

Über diese Variable lassen sich dann alle Firewallregeln deaktivieren:

```
Disable-NetFirewallRule –InputObject $Rules
```

Anstatt das Ergebnis einer Abfrage in einer Variable zu speichern, lassen sich die Ergebnisse aber auch mit dem Pipezeichen (|) direkt an ein anderes Cmdlet übergeben:

```
Get-NetFirewallRule -PolicyStore ActiveStore -PolicyStoreSourceType Dynamic | Disable-
NetFirewallRule
```

Auf dem gleichen Weg, wie sich Firewallregeln mit *Disable-NetFirewallRule* deaktivieren lassen, können Sie die Regeln mit *Enable-NetFirewallRule* wieder aktivieren.

Firewallregeln anzeigen und Status abfragen

Der Status von Firewallregeln lässt sich mit *Get-NetFirewallRule* anzeigen. Alle Regeln eines Rechners, unabhängig von deren Status, zeigen Sie mit *Get-NetFirewallRule -All* an.

Die aktivierten Regeln zeigt die PowerShell mit *Get-NetFirewallRule -Enabled True* an. Um die aktivierten Regeln anzuzeigen, die den Datenverkehr erlauben, verwenden Sie *Get-NetFirewallRule -Enabled True -Action Allow*.

Alle Regeln eines bestimmten Profils lassen Sie sich mit *Get-NetFirewallProfile -Name Public | Get-NetFirewallRule* anzeigen. Die IPsec-Regeln lassen Sie sich am einfachsten mit *Show-NetFirewallRule* anzeigen.

Neben den Regeln können Sie auch die einzelnen Profile in der PowerShell steuern. Dazu steht das Cmdlet *Set-NetFirewallProfile* zur Verfügung. So lassen sich auf diesem Weg alle Profile und die damit verbundenen Regeln aktivieren, damit die Firewall funktioniert:

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
```

Um das Standardverhalten eines Profils zu steuern, verwenden Sie:

```
Set-NetFirewallProfile –Name Domain –DefaultInboundAction Block
```

Die globalen Einstellungen für die Windows-Firewall lassen sich mit *Set-NetFirewallSetting* steuern.

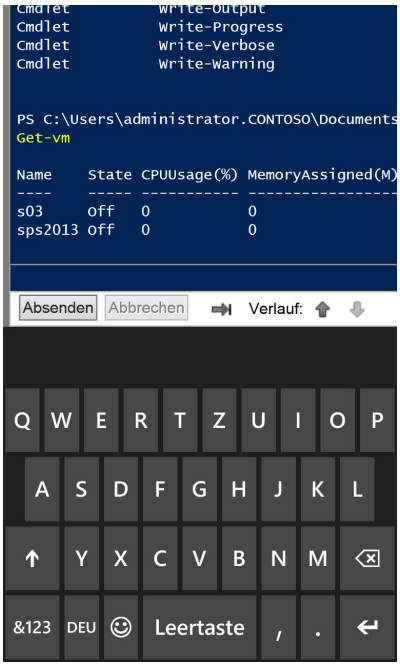
PowerShell Web Access

In diesem Abschnitt zeigen wir Ihnen, wie Sie PowerShell Web Access einrichten. Sie müssen dieses Feature nachträglich über den Server-Manager oder der PowerShell installieren und dann über die PowerShell einrichten.

Windows PowerShell Web Access stellt eine webbasierte Windows PowerShell-Konsole bereit. Auf diese Weise können Sie Windows PowerShell-Befehle und -Skripts über eine Windows PowerShell-Konsole in einem Webbrowser ausführen. Zum Verwenden sind ein Windows PowerShell Web Access-Gateway und ein Browser auf dem Clientgerät erforderlich, der JavaScript unterstützt und Cookies akzeptiert.

Nach der Installation und Konfiguration des Gateways können Benutzer mithilfe eines Webbrowsers auf eine Windows PowerShell-Konsole zugreifen. Wenn ein Benutzer die sichere Windows PowerShell Web Access-Website öffnet, kann er nach der erfolgreichen Authentifizierung eine webbasierte Windows PowerShell-Konsole ausführen.

Abbildg. 40.8 PowerShell-Sitzung über Windows Phone 8 zu Windows Server 2012 mit PowerShell Web Access



HINWEIS Sie können mit PowerShell Web Acess auch problemlos über Smartphones und Tablet-PCs remote auf die PowerShell von Servern zugreifen. Dabei können Sie alle Cmdlets nutzen, die auf dem Server verfügbar sind.

Installieren von PowerShell Web Access

PowerShell Web Access setzt voraus, dass die Internetinformationsdienste (IIS), .NET Framework 4.5 und PowerShell auf dem Server installiert sind, auf dem Sie das Gateway ausführen. Installieren Sie PowerShell Web Access mit dem Server-Manager oder in der PowerShell, werden die erforderlichen Rollen und Features automatisch hinzugefügt:

1. Starten Sie den Server-Manager und klicken Sie im Menü *Verwalten* auf *Rollen und Features hinzufügen*.
2. Wählen Sie auf der Seite *Installationstyp auswählen* die Option *Rollenbasierte oder featurebasierte Installation* aus. Klicken Sie auf *Weiter*.
3. Wählen Sie auf der Seite *Zielserver auswählen* einen Server aus dem Serverpool aus oder wählen Sie eine Offline-VHD aus. Um eine Offline-VHD als Zielserver auszuwählen, müssen Sie zuerst den Server festlegen, auf dem die VHD eingebunden werden soll. Wählen Sie danach die VHD-Datei aus.
4. Erweitern Sie auf der Seite *Features auswählen* des Assistenten *Windows PowerShell* und wählen Sie dann *Windows PowerShell Web Access* aus.
5. Sie werden aufgefordert, erforderliche Features wie .NET Framework 4.5 und Rollendienste von IIS hinzuzufügen. Fügen Sie die erforderlichen Features hinzu und setzen Sie den Vorgang fort.

HINWEIS Wenn Sie Windows PowerShell Web Access mit der PowerShell installieren, werden die Verwaltungstools für IIS nicht hinzugefügt:

```
Install-WindowsFeature -Name WindowsPowerShellWebAccess -ComputerName <Name des Servers> -
IncludeManagementTools -Restart
```

Konfigurieren des Gateways für PowerShell Web Access

Nach der Installation von PowerShell Web Access besteht der nächste Schritt in der Einrichtung des Gateways für PowerShell Web Access. Das Cmdlet *Install-PswaWebApplication* bietet eine schnelle Möglichkeit, um PowerShell Web Access zu konfigurieren. Sie können mit der Option *–UseTestCertificate* auch ein selbstsigniertes SSL-Zertifikat installieren. Verwenden Sie für eine sichere Produktionsumgebung aber besser ein gültiges SSL-Zertifikat, das von einer Zertifizierungsstelle signiert wurde (siehe Kapitel 30). Über die IIS-Manager-Konsole können Sie das Testzertifikat durch ein signiertes Zertifikat ersetzen. In Kapitel 30 finden Sie mehr zu diesem Thema.

Sie können die Konfiguration mit *Install-PswaWebApplication* oder im IIS-Manager durchführen. Standardmäßig wird durch das Cmdlet die Webanwendung *pswa* und der zugehörige Anwendungspool *pswa_pool* im Standardwebsite-Container installiert.

Der IIS-Manager bietet Konfigurationsoptionen, die für Webanwendungen verfügbar sind, zum Beispiel das Ändern der Portnummer oder des SSL-Zertifikats (Secure Sockets Layer). Um eine Testumgebung einzurichten, geben Sie in der PowerShell den Befehl *Install-PswaWebApplication –UseTestCertificate* ein. Wie Sie nachträglich Einstellungen ändern, lesen Sie in den Kapiteln 27 und 30.

Abbildg. 40.9 Aktivieren von PSA in der PowerShell

```
PS C:\Users\administrator.CONTOSO> Install-PswaWebApplication -UseTestCertificate
WARNUNG: Aus Sicherheitsgründen wird von der Verwendung eines Testzertifikats in einer Produktionsumgebung abgeraten.
Dieses Zertifikat sollte nur für interne Tests von Windows PowerShell Web Access verwendet werden. Das Testzertifikat
läuft in 90 Tagen ab.
Anwendungspool pswa_Pool wird erstellt...

Name                    State        Applications
----                    -----        ------------
pswa_Pool               Started


Webanwendung pswa wird erstellt...

Path             : /pswa
ApplicationPool  : pswa_Pool
EnabledProtocols : http
PhysicalPath     : C:\Windows\Web\PowerShellWebAccess\wwwroot


Selbstsigniertes Zertifikat wird erstellt...

HTTPS-Bindung wird erstellt...

PS C:\Users\administrator.CONTOSO>
```

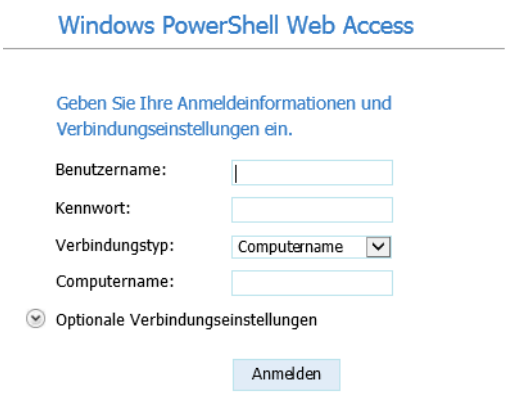
Durch die Ausführung des Cmdlets wird die PowerShell Web Access-Webanwendung im Standardwebsite-Container von IIS installiert. Die Webseite von PSWA erreichen Sie über den Link, *https://<Servername>/pswa*.

Um die Webanwendung auf einer anderen Website zu installieren, müssen Sie den Websitenamen angeben, indem Sie die Option *–WebSiteName* nutzen. Beispiel:

```
Install-PswaWebApplication –WebApplicationName <Name> –UseTestCertificate
```

Eine Anmeldung ist erst möglich, nachdem den Benutzern durch Hinzufügen von Autorisierungsregeln der Zugriff auf die Website gestattet wurde. Sie können das Zertifikat jederzeit über die Bindungen der Webseite ändern (siehe Kapitel 30).

Abbildg. 40.10 Aufrufen der Anmeldeseite für PowerShell Web Access



HINWEIS Haben Sie das Gateway eingerichtet, können Sie die Webseite öffnen, indem Sie die Adresse *http://<Servername>/pswa* eingeben. Eine Anmeldung ist aber erst möglich, nachdem den Benutzern durch Hinzufügen von Autorisierungsregeln der Zugriff auf die Website gestattet wurde.

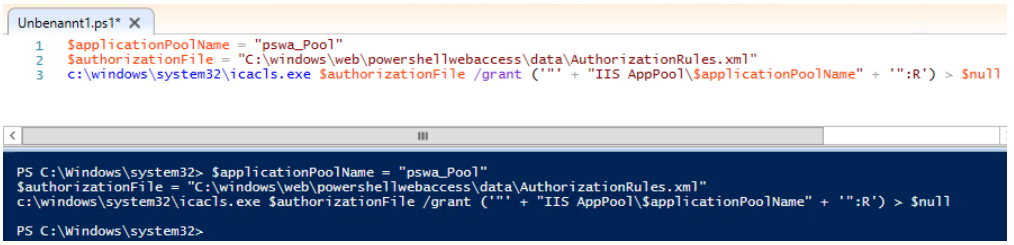
Konfigurieren der Berechtigungen für PowerShell Web Access

Nachdem Sie PowerShell Web Access installiert und das Gateway mit der Webseite und dem Zertifikat eingerichtet haben, müssen Sie Benutzern noch den Zugriff auf die PowerShell über PowerShell Web Access gestatten.

Führen Sie in einer PowerShell-Sitzung, die mit erhöhen Benutzerrechten (*Als Administrator ausführen*) geöffnet wurde, die folgenden Befehle aus:

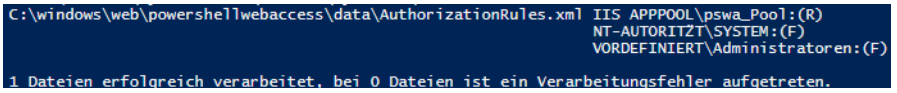
```
$applicationPoolName = "<Name des Anwendungspools für PSWA>"
$authorizationFile = "C:\windows\web\powershellwebaccess\data\AuthorizationRules.xml"
c:\windows\system32\icacls.exe $authorizationFile /grant ('"' + "IIS
AppPool\$applicationPoolName" + '":R') > $null
```

Abbildg. 40.11 Anpassen der Autorisierungsdatei für PowerShell Web Access



Anschließend lassen Sie sich mit *C:\Windows\System32\icacls.exe $authorizationFile* die gesetzten Rechte anzeigen.

Abbildg. 40.12 Anzeigen der Berechtigungen für die Autorisierungsdatei von PowerShell Web Access



PowerShell Web Access-Authentifizierungsregeln sind Positivlistenregeln. Jede Regel entspricht einer Definition einer zugelassenen Verbindung zwischen Benutzern, Zielcomputern und bestimmten Windows PowerShell-Sitzungskonfigurationen auf angegebenen Zielcomputern.

Für einen Benutzer muss nur eine Regel zutreffen, damit er Zugriff erhält. Wenn ein Benutzer über die webbasierte Konsole auf einen Computer zugreifen darf, kann sich dieser bei anderen Computern anmelden, die mit dem ersten Zielcomputer verbunden sind. Das sicherste Verfahren, um Windows PowerShell Web Access zu konfigurieren, besteht darin, Benutzern nur den Zugriff auf einge-

schränkte Sitzungskonfigurationen zu gewähren, die ihnen das Ausführen bestimmter Aufgaben ermöglichen:

- **Add-PswaAuthorizationRule** Fügt Autorisierungsregeln hinzu
- **Remove-PswaAuthorizationRule** Entfernt eine angegebene Autorisierungsregel aus PowerShell Web Access
- **Get-PswaAuthorizationRule** Zeigt die erstellten Regeln an
- **Test-PswaAuthorizationRule** Wertet Autorisierungsregeln aus

PowerShell Web Access-Benutzer müssen immer einen Benutzernamen und ein Kennwort angeben, um ihr Konto auf dem Gateway zu authentifizieren. Nachdem ein Benutzer am Gateway authentifiziert ist, werden die Autorisierungsregeln geprüft, um festzustellen, ob der Benutzer Zugriff auf den angeforderten Zielcomputer hat. Nach der erfolgreichen Autorisierung werden die Anmeldeinformationen des Benutzers an den Zielcomputer übergeben. Die Syntax für das Erstellen einer Regel ist:

```
Add-PswaAuthorizationRule -UserName <Domäne\Benutzer | Computer\Benutzer> -ComputerName
<Computername> -ConfigurationName <Sitzungskonfigurationsname>
```

Diese Autorisierungsregel erlaubt es einem bestimmten Benutzer, auf einen Computer im Netzwerk zuzugreifen. Der Zugriff ist auf eine bestimmte Sitzungskonfiguration beschränkt. Im folgenden Beispiel wird dem Benutzer *administrator* in der Domäne *Contoso* der Zugriff für die Verwaltung des Computers *srv1.contoso.int* und die Verwendung der Sitzungskonfiguration *microsoft.powershell* gestattet.

```
Add-PswaAuthorizationRule -UserName Contoso\administrator -ComputerName srv1.contoso.int -
ConfigurationName microsoft.powershell
```

Überprüfen Sie, ob die Regel erstellt wurde, indem Sie das Cmdlet *Get-PswaAuthorizationRule* ausführen. Mit *Remove-PswaAuthorizationRule –ID <Regel-ID>* löschen Sie eine Regel. Sie werden nicht aufgefordert, das Löschen der angegebenen Autorisierungsregel zu bestätigen. Die Regel wird gelöscht, sobald Sie die ↵-Taste drücken.

Für jede Windows PowerShell-Sitzung wird eine Sitzungskonfiguration verwendet. Falls für eine Sitzung keine Sitzungskonfiguration angegeben wird, verwendet Windows PowerShell die in Windows PowerShell integrierte Standardsitzungskonfiguration *Microsoft.PowerShell*. Die Standardsitzungskonfiguration schließt alle auf einem Computer verfügbaren Cmdlets ein.

Administratoren können den Zugriff auf alle Computer einschränken, indem sie eine Sitzungskonfiguration mit eingeschränktem *Runspace* (ein begrenzter Bereich von Cmdlets und Aufgaben, die die Benutzer ausführen können) definieren. Ein Benutzer, dem der Zugriff auf einen Computer gestattet wurde, kann Verbindungen mit anderen Computern herstellen, die mit dem ersten Computer verbunden sind. Durch das Definieren eines eingeschränkten Runspaces können Sie verhindern, dass Benutzer auf Computer außerhalb ihres zulässigen Windows PowerShell-Runspaces zugreifen.

Die Sitzungskonfiguration kann mit Gruppenrichtlinien an alle Computer verteilt werden, Autorisierungsregeln werden in einer XML-Datei gespeichert. Standardmäßig wird die XML-Datei unter *%WinDir%\Web\PowershellWebAccess\data\AuthorizationRules.xml* gespeichert. Der Pfad zur XML-Datei mit den Autorisierungsregeln wird in der Datei *powwa.config* gespeichert, die unter *%WinDir%\Web\PowershellWebAccess\data* gespeichert ist.

Standardmäßig ist PowerShell Web Access die Anzahl gleichzeitiger Sitzungen je Benutzer auf drei Sitzungen begrenzt. Sie können die *web.config*-Datei der Webanwendung im IIS-Manager bearbeiten, um einen anderen Wert für die Anzahl der Sitzungen pro Benutzer zu unterstützen. Die Datei *web.config* ist unter *$Env:WinDir\Web\PowerShellWebAccess\wwwroot\Web.config* gespeichert.

Standardmäßig ist der Webserver (IIS) so konfiguriert, dass der Anwendungspool neu gestartet wird, wenn Einstellungen bearbeitet werden. Der Anwendungspool wird beispielsweise neu gestartet, wenn Änderungen an der Datei *web.config* vorgenommen werden. Die Sitzungen von Benutzern, die bei PowerShell Web Access angemeldet sind, werden getrennt, wenn der Anwendungspool neu gestartet wird.

HINWEIS Nach 15-minütiger Inaktivität wird angemeldeten Benutzern eine Timeoutmeldung angezeigt. Wenn der Benutzer nicht innerhalb von fünf Minuten reagiert, wird die Sitzung beendet, und der Benutzer wird abgemeldet. Sie können die Zeitspanne für den Sitzungstimeout in den Websiteeinstellungen im IIS-Manager ändern.

Bevor Sie PowerShell Web Access auf dem Gatewayserver deinstallieren, müssen Sie die PowerShell Web Access-Website und -Webanwendungen im IIS-Manager löschen. Wählen Sie im IIS-Manager die Website aus, auf der die PowerShell Web Access-Webanwendung ausgeführt wird. Klicken Sie im *Aktionen*-Bereich unter *Website verwalten* auf *Beenden*. Danach können Sie die Seite entfernen.

Normale Eingabeaufforderung verwenden

Neben der neuen PowerShell besteht auch weiterhin die Möglichkeit, die normale Eingabeaufforderung zu nutzen. In diesem Abschnitt zeigen wir Ihnen ein paar Tipps und Tricks zur Arbeit mit der Eingabeaufforderung. In diversen Kapiteln dieses Buchs wurde bereits auf einzelne Befehle eingegangen, die ohne grafische Oberfläche in der Eingabeaufforderung eingegeben werden können.

Eine Eingabeaufforderung öffnen Sie am besten, indem Sie auf der Startseite die Zeichenfolge *cmd* eintippen. Alternativ gibt es auch hier – wie bei der PowerShell – die Möglichkeit, im Explorer die Registerkarte *Datei* zu öffnen, um hier die Eingabeaufforderung sowohl mit als auch ohne Administratorrechten aufzurufen.

Wenn Sie häufiger eine Eingabeaufforderung benötigen, können Sie zur Datei *cmd.exe* auch eine Verknüpfung auf dem Desktop erstellen oder diese an die Taskleiste anheften, zum Beispiel über die App-Leiste, die Sie auf der Startseite mit einem Klick der rechten Maustaste öffnen. Wollen Sie die Eingabeaufforderung mit Administratorrechten öffnen, können Sie dies über die Verknüpfung per Rechtsklick durchführen. Mit der Eingabeaufforderung zu arbeiten, heißt tippen: Man erteilt dem System Befehle, indem man ihren Namen per Tastatur eingibt und die Zeile mit einem Druck auf die ↵-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 Eingabeaufforderung, auch die Auswahl der zur Verfügung stehenden Befehle 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 Eingabeaufforderung schätzen zu lernen, muss man wissen, dass beim Arbeiten mit ihr immer genau ein Ordner eines Laufwerks der sogenannte aktuelle Ordner ist. Nur Dateien in diesem Ordner lassen sich ansprechen, ohne ihnen einen Pfad voranstellen zu müssen.

Zum Wechseln des aktuellen Ordners 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. 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. 40.13 Konfigurieren der Eingabeaufforderung unter Windows Server 2012

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, müssen Sie ihn nur bei gedrückter Maustaste einrahmen und dann die ↵-Taste drücken; ohne QuickEdit leitet der Befehl *Markieren* aus dem Systemmenü das Kopieren ein.

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, Ordner- oder Dateinamen einzugeben. Die wichtigsten Befehle sind nachfolgend aufgelistet:

- **APPEND** Sucht nach Dateien im Unterordner
- **ASSIGN** Verweist dem Laufwerk einen anderen Buchstaben
- **ATTRIB** Zeigt Dateiattribute an oder ändert diese
- **C:** Wechselt zum Laufwerk C:
- **CALL** Ruft einer Batchdatei aus einer anderen heraus mit Rücksprung auf
- **CD** Der Befehl *CD* zeigt Ihnen den Namen des aktuellen Ordners 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 Überprüft Datenträger
- CHOICE Erlaubt verschiedene Auswahlmöglichkeiten innerhalb von Batchdateien
- CLS Löscht den Bildschirm
- COMP Vergleicht Dateien miteinander
- COPY Kopiert Dateien
- DATE Zeigt das aktuelle Datum an oder ändert dieses
- DEL Löscht eine oder mehrere Dateien
- DELTREE Löscht komplette Verzeichnisbäume
- DIR Zeigt Inhaltsverzeichnisse an. Zeigt eine Liste der in einem Ordner enthaltenen Dateien und Unterverzeichnisse an. Wenn Sie *DIR* ohne Parameter verwenden, wird die Datenträgervolumebezeichnung und Seriennummer des Datenträgers, gefolgt von einer Liste der Ordner und Dateien auf dem Datenträger, einschließlich der entsprechenden Namen, 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 Zeigt Meldungen auf dem Bildschirm aus einer Batchdatei heraus an; schaltet die Befehlsanzeige ein bzw. aus
- EXIT Beendet das aktuelle Batchskript (mit den Parameter */b*) oder das Programm *cmd.exe* und kehrt zu dem Programm zurück, das über *cmd.exe* gestartet wurde
- EXPAND Expandiert eine oder mehrere komprimierte Dateien
- FC Vergleicht Dateien
- FIND Sucht Textstellen in Dateien
- FOR Batchbefehle zur mehrfach Wiederholung eines DOS-Befehls
- FORMAT Bereitet Festplatten vor (formatieren)
- FTP Öffnet die FTP-Verbindung
- GOTO Sprungbefehl in Batchdatei
- IF Setzt Bedingungen in Batchdateien
- LABEL Weist einen Datenträgernamen zu und ermöglicht das Ändern oder Löschen
- MD Erstellt einen Unterordner
- MENUCOLOR Legt die Farben für das Multikonfigurationsmenü fest
- MOVE Verschiebt Dateien, benennt Ordner um
- PATH Legt den Suchpfad für ausführbare MS-DOS-Befehlsdateien fest oder zeigt ihn an
- PAUSE Stoppt innerhalb von Batchdateien und wartet auf einen Tastendruck
- PING Testet eine Netzwerkverbindung
- PRINT Druckt Textdateien im Hintergrund aus
- RD Löscht einen Unterordner
- REM Fügt Kommentare in Batchdateien ein

- **REN** Benennt Dateien um
- **SUBST** Ersetzt einen Ordnernamen durch einen Laufwerkbezeichner
- **TELNET** Öffnet das Telnet-Fenster. Dazu muss aber die Funktion *Telnetclient* installiert sein
- **TIME** Zeigt die Systemzeit an und ändert diese
- **TREE** Zeigt die Ordnerstruktur eines Datenträgers grafisch an
- **TYPE** Zeigt den Inhalt einer Datei auf dem Bildschirm an
- **VOL** Zeigt den Namen und die Seriennummer eines Datenträgers an
- **XCOPY** Erweitertes Kopierprogramm mit zusätzlichen Möglichkeiten zur Übertragung von Dateien und kompletten Verzeichnisbäumen. Mit Xcopy lassen sich Dateien und Ordner einschließlich der Unterordner 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 Quellen, die neuer sind als vorhandene Dateien aus Ziel. Mit dieser Befehlsoption können Sie veränderte Dateien aktualisieren.
- **/u** Kopiert nur die Dateien aus der Quelle, die bereits im Ziel existieren
- **/s** Kopiert Ordner und Unterordner, wenn diese nicht leer sind. Wenn Sie */s* weglassen, arbeitet Xcopy nur innerhalb eines Ordners.
- **/e** Kopiert alle Unterordner, auch wenn diese leer sind
- **/t** Kopiert nur die Unterverzeichnisstruktur (Tree), keine Dateien. Um auch leere Ordner zu kopieren, müssen Sie die Befehlsoption */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

TIPP Arbeiten Sie mit der Eingabeaufforderung, können Sie schneller die verschiedenen Befehle aufrufen, wenn Sie den Anfangsbuchstaben des Ordners eingeben, zu dem Sie sich bewegen wollen, und dann die ⇆-Taste drücken. Windows vervollständigt anschließend den Befehl.

Möchten Sie zum Beispiel zum Stammordner der Partition wechseln, geben Sie den Befehl *cd* ein. Um vom Stammordner aus den Ordner *Programme* zu öffnen, reicht es auch, wenn Sie *cd P* eintippen und so lange die ⇆-Taste drücken, bis der richtige Ordner angezeigt wird.

In der Eingabeaufforderung tragen die Ordner meist englische Bezeichnungen, außer jene Ordner, die Sie selbst erstellen.

Wollen Sie aus dem Explorer direkt einen Pfad in der Eingabeaufforderung öffnen, klicken Sie auf den Ordner mit ⇧+Rechtsklick und wählen den Kontextmenübefehl *Eingabeaufforderung hier öffnen*.

Batchdateien für Administratoren

Geht es um das Skripting im Netzwerk, steht dafür meist die PowerShell an erster Stelle. Natürlich ist die PowerShell extrem mächtig und bietet umfassende Möglichkeiten, um Server und Computer zu verwalten. Es ist aber auch möglich, über die normale Eingabeaufforderung zahlreiche Verwaltungsaufgaben durchzuführen und diese in Batchdateien zusammenzufassen. Nachfolgend zeigen wir Ihnen dazu einige interessante Beispiele.

Grundlagen zu Batchdateien

Sie können die Befehle auf den nachfolgenden Seiten entweder direkt in der Eingabeaufforderung verwenden oder Sie schreiben eine Batchdatei. Dazu schreiben Sie einfach die Befehle in eine neue Textdatei und weisen dieser die Endung **.cmd* oder **.bat* zu.

Sie können auch Beschreibungen und Kommentare vor einzelne Zeilen von Batchdateien aufnehmen. Dazu verwenden Sie den Befehl *Rem* in der Zeile, zum Beispiel:

```
Rem Ab hier werden Netzlaufwerke verbunden
```

Alternativ können Sie auch einfach einen Doppelpunkt als erstes Zeichen in die Zeile schreiben. Dann lässt sich diese Zeile parallel noch als Sprungmarke nutzen, doch dazu später mehr.

Netzwerk über die Eingabeaufforderung verwalten

Wollen Sie Netzwerkeinstellungen von Computern über die Eingabeaufforderung ändern, können Sie auf das Tool *netsh.exe* zurückgreifen. Um zum Beispiel die IP-Adresse und den DNS-Server der Netzwerkschnittstelle *lan* zu ändern, verwenden Sie die drei Befehle:

```
Netsh interface ip set address "lan" static 192.168.178.99 255.255.255.0 192.168.178.4 1
Netsh interface ip delete dns "lan" 192.168.178.1
Netsh interface ip add dns "lan" 192.168.178.4
```

Die Einstellungen lassen Sie sich mit den folgenden Befehlen in der Eingabeaufforderung anzeigen:

```
Netsh interface ip show address "lan"
Netsh interface ip show dns "lan
```

Packen Sie das alles in eine Batchdatei, können Anwender selbstständig Netzwerkeinstellungen (abhängig vom Netzwerk, mit dem sie verbunden sind) einstellen.

Sie erreichen in der Eingabeaufforderung auch wesentlich schneller Konfigurationsfenster der grafischen Oberfläche der Netzwerkkartenverwaltung. Geben Sie zum Beispiel *ncpa.cpl* ein, öffnet sich das Fenster zur Verwaltung der Netzwerkeinstellungen, und mit *certlm.msc* lässt sich die Verwaltung der lokalen Zertifikate des Computers öffnen. Das ist vor allem bei der Einrichtung von Serverdiensten sinnvoll, die Zertifikate benötigen. Administratoren, die verschiedene Subnetze verwalten, können IP-Pakete mit den Befehle *pathping* oder *tracert* nachverfolgen. So lassen sich schnell Probleme auf Routern finden oder Geschwindigkeitsprobleme durch Umgehen bestimmter Routen beseitigen.

Geben Sie den Befehl *netstat -an* ein, zeigt Windows die geöffneten Ports an. Ausführlichere Informationen erhalten Sie mit *netstat -banvo*. Die Routingtabelle des Computers sehen Sie mit *netstat -r*, Statistiken zu TCP/IP zeigt das Tool mit *netstat -s* an. Auf diesem Weg können Sie also umfassende Informationen zu Netzwerkeinstellungen eines Servers abrufen.

Sprungmarken und Wartebefehle

Interessant für Batchdateien sind generell Sprungmarken, Pausezeichen und Wartebefehle. Möchten Sie zum Beispiel, dass die Ausführung einer Batchdatei zu einer bestimmten Stelle springt, schreiben Sie vor der entsprechenden Zeile einfach einen Doppelpunkt und die Bezeichnung der Sprungmarke, zum Beispiel *:Sprung1*. Wenn Sie jetzt in einer Batchdatei ein *goto Sprung1* schreiben, führt die Eingabeaufforderung die Batchdatei ab der Sprungmarke aus.

Weniger bekannt sind die Befehle zum Warten in Batchdateien. Hier bietet sich in Windows Server 2012 R2 der Befehl *timeout.exe* an. So wartet zum Beispiel der Befehl *timeout /t:5* fünf Sekunden auf eine Eingabe und macht dann mit der Batchdatei weiter. Wollen Sie das Warten erzwingen, also keine Unterbrechung per Tastendruck erlauben, verwenden Sie zusätzlich die Option */nobreak*. Mit dem Befehl *timeout /t -1* läuft kein Countdown, sondern die Batchdatei wartet, bis eine Taste gedrückt wird. Das Gleiche erreichen Sie aber auch mit dem Befehl *pause*.

Wenn/Dann-Abfragen nutzen

Interessant sind solche Sprungmarken zum Beispiel in Verbindung mit Befehlen zum Überprüfen von Bedingungen. So können Sie zum Beispiel mit *if exist c:\temp\systeminfo.txt goto sprung1* festlegen, dass die Batchdatei zur Zeile *sprung1* springt, wenn im Ordner *c:\temp* eine Datei *systeminfo.txt* existiert. Um eine Batchdatei zu beenden, verwenden Sie als Befehl *exit*. Danach schließt Windows das Fenster der Datei.

Sie können aber nicht nur die Option *exist* nutzen, um zu testen, ob eine bestimmte Datei vorhanden ist, sondern mit der Option *not exist* auch prüfen, ob die Datei explizit nicht vorhanden ist:

```
If not exist c:\temp\test.txt goto sprung1
```

Interessant ist in diesem Zusammenhang auch die Möglichkeit, zu testen, ob in einem beliebigen Ordner Dateien vorhanden sind, zum Beispiel mit *if exist c:\temp*.**. Sie können auch Ordner mit Leerzeichen verwenden, müssen in diesem Fall den Pfad aber in Anführungszeichen setzen.

Batchbefehle lassen sich problemlos miteinander verschachteln:

```
If exist c:\temp\test.bak if not exist test2.bak ren test.bak test2.bak
```

Ist die Datei *test.bak* vorhanden, die Datei *test2.bak* jedoch nicht, wird *test.bak* in *test2.bak* umbenannt.

In Batchdateien können Sie auch den Fehlerstatus eines vorangegangenen Befehls abfragen. Hat der vorherige Befehl einen Fehler verursacht, können Sie in der Batchdatei anders vorgehen als bei einer erfolgreichen Ausführung. Umgekehrt können Sie auch sicherstellen, dass der vorhergehende Befehl erfolgreich war. Ein Beispiel dazu ist:

```
Md c:\temp\test
If errorlevel 1 goto fehler
Echo Verzeichnis erstellt
:Fehler
Echo Erstellung nicht möglich
```

Der Befehl erstellt einen neuen Ordner. Ist das aus irgendwelchen Gründen nicht möglich, springt die Batchdatei zur Sprungmarke *Fehler*. *Errorlevel 0* ist die erfolgreiche Ausführung des Befehls, *Errorlevel 1* ein Fehler. Programme können aber auch unterschiedliche Werte für den Errorlevel zurückgeben. Dies testen Sie, indem Sie den entsprechenden Befehl ausführen und dann in der Eingabeaufforderung *%errorlevel%* eingeben. Sie erhalten dann den aktuellen Wert angezeigt, den Sie wiederum in einer Batchdatei verwenden können. Sie können zusätzlich zu den Wenn-Abfragen (*If*) auch Sonst-Befehle mit *else* einbauen. Wenn die Bedingung nicht eintritt, führt die Batchdatei einen anderen Befehl aus:

```
If exist c:\temp\test.bak
…
Goto weiter
…
Else if exist c:\temp\test\test.bak
…
Goto weiter2
…
```

Im vorangegangenen Befehl haben wir zwei *If*-Anfragen miteinander verknüpft, Sie können aber mit *else* jeden anderen beliebigen Befehl verwenden.

Informationen zum lokalen PC abrufen

Wenn sich Administratoren an einem PC anmelden, lassen sich viele wichtige Informationen zu einem PC in der Eingabeaufforderung wesentlich schneller und gebündelter anzeigen als in der grafischen Oberfläche und der PowerShell.

Die aktuelle IP-Adresse wird mit *ipconfig* angezeigt, mehr Informationen mit *ipconfig /all*. Der Befehl *ipconfig /displaydns* zeigt den lokalen DNS-Cache an, auch die zuletzt geöffneten Internetseiten und aufgelösten DNS-Namen. Löschen Sie den Verlauf im Browser, sind die Daten dennoch an dieser Stelle vorhanden. Sie müssen den lokalen DNS-Cache separat löschen, indem Sie den Befehl *ipconfig /flushdns* verwenden.

Den Namen des Computers sehen Sie mit *hostname*, die Version des installierten Windows mit *ver*, mit *winver* öffnet sich ein Fenster in der grafischen Oberfläche. Möchten Sie sich den angemeldeten Benutzer anzeigen lassen, zum Beispiel zur Überprüfung von Rechten, geben Sie *whoami* ein.

Ausführliche Informationen zu einem Computer erhalten Sie auch durch Eingabe von *systeminfo*. Lassen Sie die Ausgabe am besten mit *systeminfo >c:\temp\systeminfo.txt* in eine Textdatei umleiten, um alle Informationen in eine Datei zu schreiben. Das funktioniert mit allen Befehlen der Eingabeaufforderung. Der Befehl überschreibt bereits vorhandenen Text in der Datei. Möchten Sie den vorhandenen Text erhalten und den neuen Text anhängen, was zum Beispiel beim Einsatz von Batchdateien durchaus sinnvoll ist, verwenden Sie den Befehl *systeminfo >>c:\temp\systeminfo.txt*.

Über den Befehl *driverquery* im Fenster der Eingabeaufforderung können Sie sich eine Liste aller aktuell geladenen Treiber anzeigen lassen. Mit dem Befehl *driverquery >c:\treiber.txt* werden alle Treiber in die Textdatei *treiber.txt* geschrieben, die Sie mit dem Windows-Editor bearbeiten und überprüfen können. Auch hier können Sie wieder mit >> arbeiten, um den Text anzuhängen.

Um den Inhalt des aktuellen Fensters zu löschen, geben Sie den Befehl *cls* ein. In Batchdateien können Sie die Anzeige der eigentlichen Befehle ausblenden, indem Sie am Anfang der Datei *@echo off* schreiben. Wollen Sie bestimmte Nachrichten in der Eingabeaufforderung anzeigen, geben Sie *echo <Text>* ein. Der Text wird dann in der Eingabeaufforderung angezeigt. Um Leerzeilen in die Anzeige einzufügen, verwenden Sie *echo* mit einem Punkt (*echo.*).

In der Eingabeaufforderung sehen Sie Freigaben, wenn Sie den Befehl *net share* aufrufen. Mit *openfiles.exe* können Sie Dateien und Ordner, die auf einem System geöffnet sind, auflisten und trennen. Damit geöffnete Dateien angezeigt werden, müssen Sie zunächst die Einstellung *Maintain Objects List* aktivieren. Mit dem Befehl *openfiles /local on* wird das Systemflag eingeschaltet. Mit *openfiles /local off* schalten Sie das Flag wieder aus.

Wenn Sie nach dem Neustart *openfiles* eingeben, werden die geöffneten Dateien angezeigt. Möchten Sie überprüfen, welche Dateien auf einem USB-Stick geöffnet sind, empfiehlt sich der Befehl *openfiles |find /i "z:"*, wobei z: der Laufwerkbuchstabe des USB-Sticks ist. Wenn Sie offene Dateien auf Ihrem System finden und diese schließen möchten, verwenden Sie den Befehl *openfiles /disconnect /id <id>* oder *openfiles /disconnect /a <user>*. Als *<id>* wird die von *Openfiles* mitgeteilte ID eingetragen, als *<user>* die mitgeteilte Nutzerkennung.

Schleifen und Variablen

Soll es komplizierter werden, können Sie auch Schleifen in Batchdateien erstellen, also bestimmte Passagen eine bestimmte Anzahl wiederholen lassen. Dazu verwenden Sie den Befehl *for*. Die Syntax lautet *for <Variable> do (*. Nach der Klammer schreiben Sie in eigene Zeilen die Befehle und schließen dann mit einer Klammer in der letzten Zeile ab:

```
For <Variable> do (
   Befehl 1
   Befehl 2
 )
```

Sie können die Schleifen auch als Zählschleifen nutzen und eine bestimmte Anzahl lang ablaufen lassen. Dazu verwenden Sie die Option */L* und die Syntax *for /L <Variable< IN* (Startzahl, Schrittweite, Endzahl) *DO* (Aktion). Eine weitere Möglichkeit, eine Zählschleife zu erstellen, ist folgende:

```
Rem Echo ausschalten
@Echo off
Rem Setzt die Variable Wert auf 0
Set /a wert=0
Sprungmarke Start
:Start
Erhöht die Variable Wert um 1
Set /a wert=%wert+1
Rem Gibt die Variable Wert aus
Echo %wert%
Rem Überprüft ob die Variable Wert 3 erreicht hat und springt zur Sprungmarke drei
If %wert%==3 goto drei
Rem Springt zur Sprungmarke start
Goto Start
Rem Sprungmarke drei
:Drei
Echo ***Drei erreicht***
Pause
```

Auch Variablen können Sie in Batchdateien nutzen. So entspricht zum Beispiel die Variable *%1* der ausgewählten Datei, wenn Sie mit einer Batchdatei eine Datei bearbeiten wollen. Ein Beispiel dafür ist:

```
Attrib -R %1
Edit %1
Attrib +R %1
```

Speichern Sie diese Datei zum Beispiel als *test.bat* ab, können Sie mit dem Befehl *test.bat c:\temp\test.txt* den Schreibschutz einer Datei entfernen, die Datei zum Bearbeiten aufrufen und anschließend den Schreibschutz wieder setzen.

WMI-Abfragen nutzen

Sie können die Konfiguration der Auslagerungsdatei auch in der Eingabeaufforderung vornehmen. Dies ist zum Beispiel notwendig, wenn die Datei größer als 2 TB sein soll, oder wenn Sie die Einstellungen skripten möchten. Zum Erstellen einer Auslagerungsdatei führen Sie den folgenden Befehl aus:

```
Wmic.exe pagefileset create name="<Laufwerksbuchstabe>:\pagefile.sys"
```

Zum Festlegen der Größe der Auslagerungsdatei verwenden Sie den Befehl:

```
wmic.exe pagefileset where name="<Laufwerksbuchstabe>:\\pagefile.sys" set
InitialSize=<MB>,MaximumSize=<MB>
```

Bitte beachten Sie den doppelten Backslash »\\«!

Mit dem folgenden Befehl deaktivieren Sie die Auslagerungsdatei auf einem Laufwerk:

```
wmic.exe pagefileset where name="<Laufwerksbuchstabe>:\\pagefile.sys" delete
```

Haben Sie die Datei bereits gelöscht, erscheint die Meldung *Keine Instanzen verfügbar*. Auf diese Weise lässt sich daher auch überprüfen, ob auf einem Laufwerk eine Auslagerungsdatei vorhanden ist.

Wenn Sie die Daten von Servern auslesen wollen, zum Beispiel den freien Festplattenplatz oder andere Informationen, können Sie auf WMI-Befehle setzen. Dabei ist es nicht notwendig, sich mit der komplexen WMI-Problematik auseinander zu setzen, sondern über die PowerShell lassen sich diese Daten schnell und einfach ablesen. Wir zeigen Ihnen nachfolgend, wie dabei vorgegangen wird.

Um sich einen Überblick über einen Server oder eine Arbeitsstation zu verschaffen, müssen Administratoren nicht unbedingt auf Tools und die grafische Oberfläche setzen. Auch in der PowerShell oder der Eingabeaufforderung lassen sich Informationen anzeigen. Der Vorteil dabei ist, dass sich auf diesem Weg auch Skripts erstellen lassen und Informationen wesentlich schneller zur Verfügung stehen als über andere Wege. In der PowerShell gibt es dazu zahlreiche Befehle.

Mit einigen Cmdlets lassen sich direkt Festplatten abfragen, andere rufen per WMI direkt Objekte vom Betriebssystem ab. Auch hier gibt es zahlreiche Varianten. Neben Festplatteninformationen lassen sich auch Daten der Netzwerkkonfiguration abfragen. Für den Umgang mit den Befehlen muss man kein Skriptprofi sein. Die PowerShell-Befehle sind für jeden Administrator sehr leicht zu bedienen.

Das Cmdlet *Get-PhysicalDisk* listet Informationen zu Festplatten auf. Ausführliche Informationen lassen sich mit *Get-PhysicalDisk |fl* oder *Get-PhysicalDisk |ft* anzeigen. Es lassen sich auch nur einzelne Informationen abrufen, wenn nach der Option *|fl* das entsprechende Feld angefügt wird.

Ausführliche Informationen zu Festplatten lassen sich mit WMI-Befehlen abrufen. Dazu steht das Cmdlet *Get-WmiObject* zur Verfügung. Verwenden Sie die Option *Win32_LogicalDisk* lassen sich sehr ausführliche Informationen zu Festplatten anzeigen.

Um nur lokale Festplatten anzuzeigen, nutzen Sie den folgenden Befehl:

```
Get-WmiObject Win32_LogicalDisk -Filter "Drive-Type=3"
```

Soll die Anzeige zusätzlich gefiltert werden, lassen sich die gewünschten Filter direkt einblenden:

```
Get-WmiObject Win32_LogicalDisk -Filter "DriveType=3" -Computer . | Select
SystemName,DeviceID,VolumeName, Freespace
```

Es lassen sich mit der PowerShell aber auch weitere Informationen anzeigen. Eine Liste für Datenträger ist mit dem folgenden Befehl verfügbar:

```
Gwmi -list|where {$_.name -like "*disk*"}
```

Wenn Sie das installierte Betriebssystem und das Datum der Installation anzeigen lassen wollen, können Sie ebenfalls WMI und die PowerShell verwenden. Mit dem folgenden Befehl zeigen Sie die die entsprechenden Informationen an:

```
Get-WmiObject Win32_Operatingsystem | Select @{Name="Installed";
Expression={$_.ConvertToDateTime($_.InstallDate)}}, Caption
```

Auch die Bitvariante des Betriebssystems (*Get-WmiObject -Class Win32_ComputerSystem -ComputerName . | Select-Object -Property SystemType*), Domäne, Hersteller, Modell und mehr (*Get-WmiObject -Class Win32_ComputerSystem*) lassen sich anzeigen.

Informationen zur Netzwerkverbindung und zu den Netzwerkadaptern lassen sich ebenfalls anzeigen. Dabei sind die beiden Befehle *Get-WmiObject Win32_Networkadapter* und *Get-NetAdapter* interessant.

Viele dieser Befehle lassen sich auch über das Netzwerk nutzen. Zusätzlich haben Administratoren noch die Möglichkeit, die Daten von Rechnern über das Netzwerk abzufragen, zum Beispiel:

```
Get-WmiObject Win32_LogicalDisk -filter "DriveType=3" -computername 192.168.178.9
```

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie mit der neuen PowerShell und der Eingabeaufforderung umgehen. In den einzelnen Kapiteln in diesem Buch sind wir ebenfalls auf diese Bereiche eingegangen. Außerdem wurde in diesem Kapitel auch kurz die Erstellung von Skripts und Batchdateien erläutert.

Teil J

Essentials und Arbeitsnetzwerke

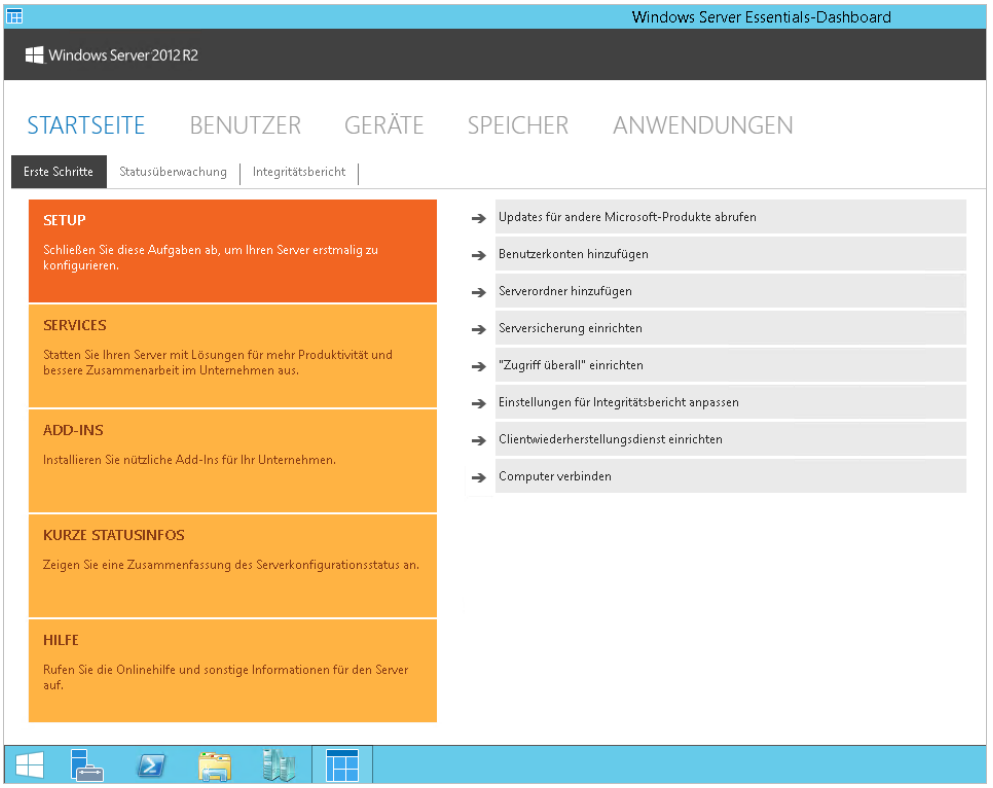
Kapitel 41

Essentials und Foundation – Windows Server 2012 R2 in kleinen Unternehmen

In diesem Kapitel:

Seit Windows Server 2012 gibt es keinen Windows Small Business Server (SBS) mehr. Der offizielle Nachfolger ist die Essentials-Edition von Windows Server 2012 R2. Diese bietet allerdings weder Exchange noch SharePoint. Unternehmen, die migrieren möchten, müssen daher einiges beachten.

Abbildg. 41.1 Windows Server 2012 R2 Essentials verfügt weiterhin über das bekannte Dashboard zur Verwaltung



In Windows Server 2012 R2 bietet die neue Edition einige Verbesserungen im Vergleich zum direkten Vorgänger in Windows Server 2012.

Unternehmen, die bisher Exchange zusammen mit Small Business Server genutzt haben, müssen bei Windows Server 2012 R2 umdenken. Dies gilt auch für Unternehmen, die SQL Server oder SharePoint im SBS-Netzwerk nutzen. Microsoft hat SBS aus dem Programm genommen und es gibt kein Serverpaket mehr, welches ein Serverbetriebssystem zusammen mit einem E-Mail- und Datenbankserver bietet. Als Alternative besteht die Möglichkeit, Windows Server 2012 R2 Essentials einzusetzen und die Exchange-Daten zu Office 365 auszulagern. Bei der Migration müssen Administratoren daher einiges beachten.

Unternehmen, die zur neuen Version wechseln möchten, sollten im ersten Schritt die lokalen Exchange-Daten von SBS zu Office 365 übertragen. Dabei spielt es keine Rolle, welche SBS-Version im Einsatz ist. Der Vorteil bei der Migration zu Office 365 ist, dass Unternehmen dadurch auch gleich Zugang zu SharePoint Online erhalten. Auch hier lassen sich die Daten des alten Companywebs übernehmen. Die Migration kann hier entweder automatisiert mit Tools oder auch manuell erfolgen, abhängig von der Anzahl der Daten, die übernommen werden sollen.

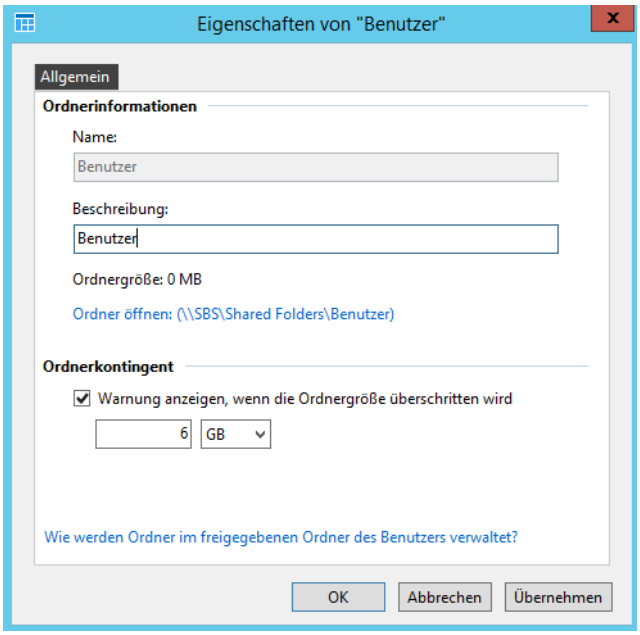
In einem ersten Schritt müssen Unternehmen die Edition von Office 365 auswählen, die zukünftig im Einsatz sein soll. Hier hilft Microsoft mit einer eigenen Website (*http://www.microsoft.com/de-de/office365/compare-plans.aspx* [Ms179-K41-01]).

Laufen Exchange und SharePoint stabil, besteht die Möglichkeit, Windows Server 2012 R2 Essentials im Netzwerk einzusetzen. Da Migrationen allerdings immer etwas Aufwand bedeuten, besteht der einfachste Weg der Übernahme in einer Neuinstallation und der anschließenden Datenübernahme.

Neuerungen in Windows Server 2012 R2 Essentials

Windows Server 2012 R2 Essentials lässt sich problemlos in bestehende Domänen integrieren, auch mehrere Server mit Windows Server 2012 R2 Essentials. Auch von anderen Niederlassungen aus können Anwender mit dem neuen Connector in Windows Server 2012 R2 Essentials auf Server zugreifen. Außerdem können Anwender den Server für die Anbindung auswählen. Installieren Sie die Serverrolle auf einem Mitgliedsserver in der Domäne, ist der Server auch danach noch Mitgliedsserver. Er wird nicht zum Domänencontroller heraufgestuft, sondern verwendet nach der Installation der Rolle die bereits verfügbaren Domänencontroller.

Abbildg. 41.2 Sie können für Ordner auf dem Server mit Windows Server 2012 R2 Essentials auch Kontingente anlegen



Ein Connector unterstützt jetzt also mehrere Server mit Windows Server 2012 R2 Essentials. Grenzwerte für die Datenspeicherung sind in der neuen Version ebenfalls mit dabei. Außerdem lassen sich im Dashboard auch Freigaben auf einem weiteren Server im Netzwerk verwalten und erstellen. Zusätz-

lich arbeitet Windows Server 2012 R2 Essentials sehr eng mit Office 365 und Windows Azure zusammen. Im Dashboard lassen sich viele Einstellungen aus Office 365 verwalten. Die vollständige Wiederherstellung von Clientcomputer kann über eine DVD erfolgen oder mit den Windows-Bereitstellungsdiensten (Windows Deployment Services, WDS) des Servers direkt über das Netzwerk.

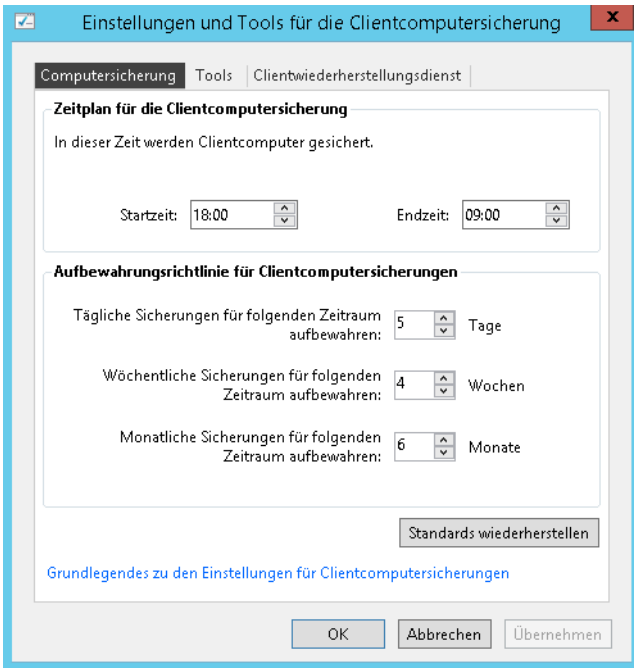
Windows Server 2012 R2 Essentials im Einsatz

Beim Einsatz von Windows Server 2012 R2 Essentials können Unternehmen bis zu 25 Benutzer und 50 Clientgeräte anbinden. Wer mehr anbinden will, kann auf Windows Server 2012 R2 Standard oder Datacenter setzen. Allerdings fällt dann die zentrale Verwaltung über das Dashboard weg, außerdem sind Clientzugriffslizenzen notwendig. Eine solche Übernahme muss ein IT-Profi vornehmen. Die Verwaltung des neuen Servers erfolgt über ein Dashboard, welches bereits von Small Business Server 2011 Essentials bekannt ist.

Windows Server 2012 Essentials gibt es in Windows Server 2012 R2 als Serverrolle für die Editionen Standard und Datacenter. Natürlich gibt es auch weiterhin die eigenständige Edition für kleinere Unternehmen. In Windows Server 2012 R2 Essentials können Sie zukünftig bis zu 100 Benutzer und 200 Geräte anbinden. Außerdem bietet Windows Server 2012 R2 Essentials Möglichkeiten zur Virtualisierung, ebenfalls auf Basis von Hyper-V 2012 R2.

Der Installations-Assistent erstellt automatisiert eine Active Directory-Domäne und nimmt notwendige Einstellungen vor. Administratoren können alle Aufgaben im Dashboard vornehmen, dem zentralen Verwaltungswerkzeug von Windows Server 2012 R2 Essentials. Zur Installation und dem Betrieb sind daher keine Profikenntnisse notwendig.

Abbildg. 41.3 Clientcomputer lassen sich mit Windows Server 2012 R2 Essentials direkt auf den Server sichern



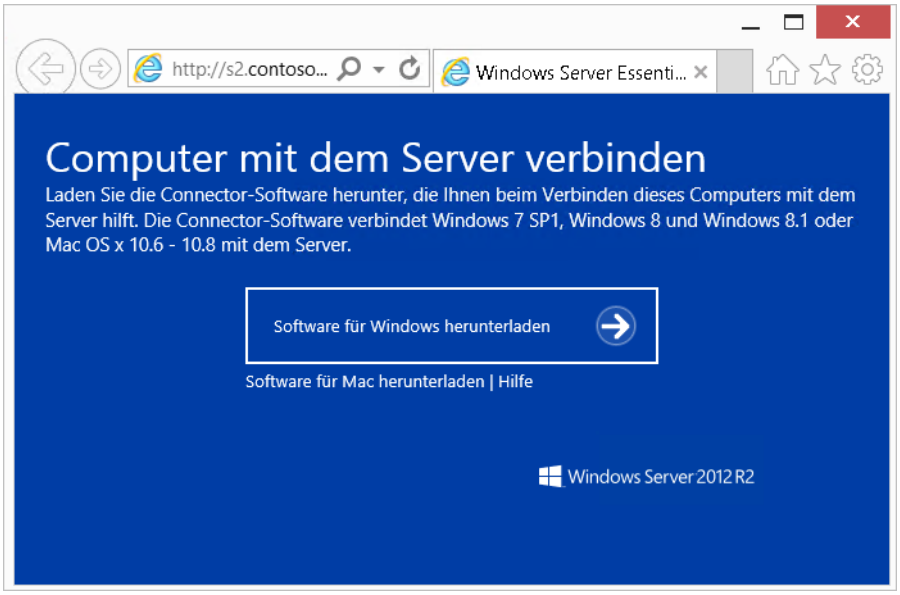
Im Gegensatz zu SBS 2011 Standard bietet Windows Server 2012 R2 Essentials aber einen wichtigen Vorteil: Clientcomputer lassen sich über einen Agent auf den Server sichern und auf einfachem Weg wiederherstellen. Diese Funktion hat Microsoft von SBS 2011 Essentials übernommen. Außerdem haben Anwender die Möglichkeit, mit Hilfe eines Webportals über das Internet mit dem Remotedesktop auf den eigenen Server zuzugreifen. Die Datensicherung und -Wiederherstellung des eigenen PCs können Anwender in einem eigenen Tool leicht selbst durchführen, das entlastet den Administrator.

Der Server benötigt keine Clientzugriffslizenzen. Der Server muss über eine mindestens 160 GB große Festplatte verfügen, davon belegt der Server aber nur etwa 20 GB, der Rest ist als Speicherplatz festgelegt. Wenn Sie den Server in einer Testumgebung mit Hyper-V installieren, dürfen Sie keine dynamische Zuordnung des Arbeitsspeichers nutzen, sondern müssen fest 2 GB Speicher zuteilen. Nach der Installation des Servers verbinden sich Clients ganz einfach mit dem Server.

Die Anwender müssen in ihrem Browser lediglich die Adresse *http://<Servername>/connect* eingeben. Anschließend bietet der Server den Download der Agent-Software an. Sobald Anwender den Link zur Installation angeklickt haben, startet ein Assistent, der sie bei der Anbindung des eigenen PCs unterstützt.

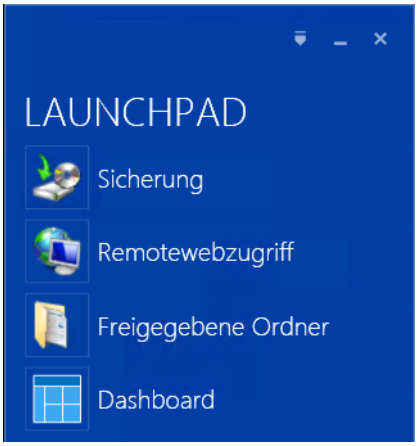
Damit sich der Rechner anbinden lässt, muss sich der jeweilige Anwender mit der Webseite verbinden und während der Einrichtung über den Assistenten seinen Benutzernamen und sein Kennwort eingeben. Dieses legt der Administrator zuvor im Dashboard fest.

Abbildg. 41.4 Die Anbindung von Clientcomputern erfolgt über einen Connector, den sich Anwender selbst installieren können.



Nach Abschluss der Installation befindet sich auf dem Desktop des Rechners das Launchpad. Über dieses können Anwender auf ihre Daten auf dem Server zugreifen und sogar ihren Rechner auf den Server sichern. Die Anbindung kann über diesen Weg auch mit Windows 8.1 ohne Domänenanbindung erfolgen. Es ist also nicht unbedingt Windows 8.1 Pro oder Enterprise notwendig.

Abbildg. 41.5 Mit dem Launchpad haben Anwender Zugriff auf die Freigaben des Servers und die Sicherungen des Rechners. Auch das Dashboard zur Verwaltung des Servers steht über das Launchpad zur Verfügung.



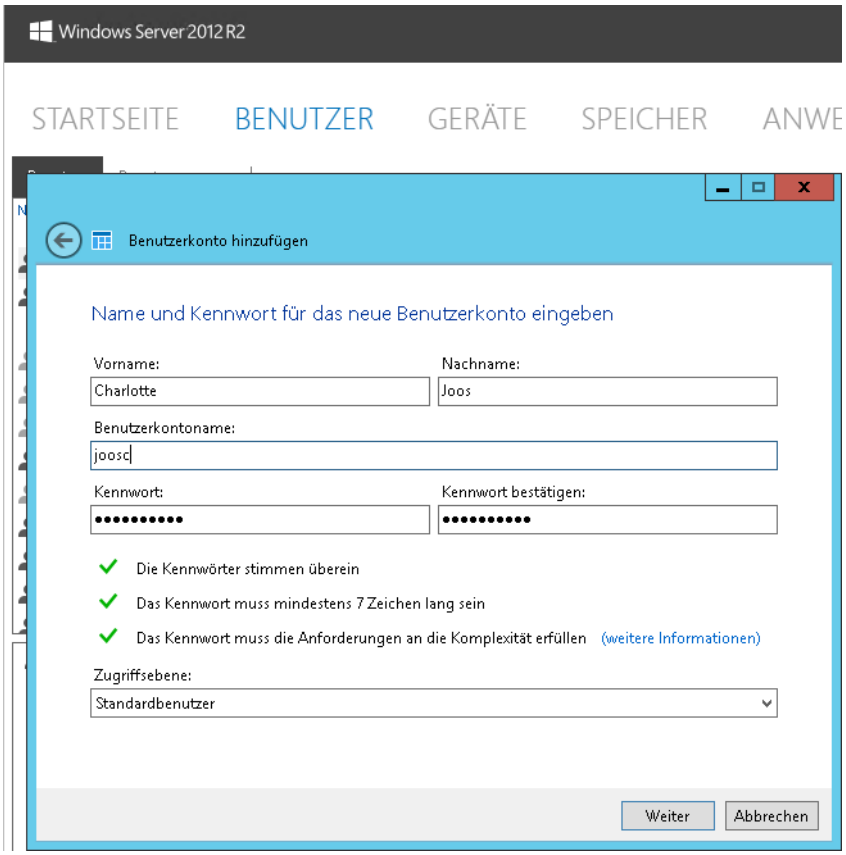
Mit einer Wiederherstellungs-CD lassen sich komplette Rechner über den Server wiederherstellen. Benutzer können über das Launchpad Daten vom eigenen Rechner auf den Server sichern. Über den Agent ist auch eine Wiederherstellung möglich. Natürlich lassen sich auch einzelne Dateien über die Sicherung auf dem Server wiederherstellen, ebenfalls über das Dashboard.

Unternehmen mit wenigen Anwendern beschäftigen keinen speziellen IT-Administrator, der eigene Server verwalten kann. Daher bietet Windows Server 2012 R2 Essentials das aus SBS 2011 Essentials bekannte Dashboard. Dieses bietet in einer angepassten Oberfläche die Möglichkeit, den Server komplett zu verwalten. Es lassen sich Benutzer anlegen, Freigaben erstellen und Zusatzanwendungen wie Backuplösungen oder Virenschutz installieren. Der Vorteil ist die leichte Bedienung. Das Dashboard können Administratoren auch von ihrer Arbeitsstation aus, ebenfalls über das Launchpad, starten. Auf diesem Weg lässt sich – die richtigen Anmeldedaten vorausgesetzt – der Server von jedem Rechner im Netzwerk aus verwalten.

Nicht nur das Anlegen von neuen Benutzern vereinfacht Windows Server 2012 R2 Essentials durch einen Assistenten, sondern auch die Zuteilung von Berechtigungen für Freigaben. Beim Anlegen von Benutzern können Sie im Assistenten exakt festlegen, auf welche Freigaben der Anwender zugreifen darf und welche Rechte er für den Zugriff hat. Legen Sie neue Freigaben an, definieren Sie auch, mit welchen Rechten die einzelnen Anwender auf die neue Freigabe zugreifen dürfen. Auch hier unterstützt wieder ein Assistent die Konfiguration, und Anwender sehen die Freigabe in ihrem Launchpad.

Zur Sicherung nutzt Windows Server 2012 R2 Essentials das in Windows Server 2012 R2 integrierte Sicherungsprogramm. Mit diesem können Administratoren die Daten des Servers auch wiederherstellen. Über das Dashboard können Unternehmen den Server zusätzlich an das Microsoft Azure Online-Backupprogramm anbinden. So lassen sich die Daten des Servers in der Cloud sichern. Dieser Dienst ist allerdings kostenpflichtig und die Preise hängen von der Größe der gesicherten Daten ab. Diese Funktion lässt sich ebenfalls direkt in das Dashboard integrieren.

Abbildg. 41.6 Neue Benutzer legen Administratoren ebenfalls im Launchpad an



Wer sich etwas tiefgründiger und ausführlicher mit dem Server auseinandersetzen möchte, kann den Server auch als Streamingserver für Windows Media Player im Netzwerk zur Verfügung stellen. Außerdem erlaubt der Server einen Zugriff über das Internet. Dazu verwenden Anwender ihren Browser oder eine VPN-Verbindung (virtuelles privates Netzwerk). Über Web Access können Sie sogar das Dashboard starten und so den Server über das Internet verwalten. Auch ein Zugriff auf Arbeitsplatzrechner ist per Remotedesktop über das Web Access möglich.

Treten Fehler auf dem Server auf, kann dieser automatisch eine Benachrichtigungs-E-Mail an Administratoren senden. Im Dashboard sehen Anwender oben rechts im Fenster noch eine Zusammenfassung von Fehlern des Servers und aller angebundenen Computer. Klicken Administratoren im Dashboard auf diesen Bereich, erhalten sie Hinweise, wie der Fehler behoben werden kann.

Über Apps binden Administratoren weitere Tools ein, welche die Verwaltung erleichtern. Die Tools lassen sich anschließend ebenfalls über das Dashboard verwalten. Die Integration erfolgt als WSSX-Datei. Diese muss nur doppelt geklickt werden, damit sich das entsprechende Programm installiert.

Bei der Migration der E-Mail-Daten hilft der Exchange Deployment Assistant (*http://technet.microsoft.com/de-de/exdeploy2010* [Ms179-K41-02]). Eigene Internetdomänen lassen sich in der Verwaltungskonsole an Office 365 einbinden. Unternehmen müssen dabei aber beachten, dass

Office 365 nicht alle Anbieter unterstützt. Vor allem die sehr kostengünstigen Angebote einiger Anbieter lassen sich nicht an Office 365 anbinden.

Die Domänen, die Administratoren an Office 365 anbinden, lassen sich im Webportal (*https://portal.microsoftonline.com* [Ms179-K41-03]) über den Administratorbereich und dann *Verwaltung/Domänen* konfigurieren. Wer keine eigene Domäne hat, kann auch mit der Domäne *<Eigener Name>.onmicrosoft.com* arbeiten. Diese gehört zum Office 365-Paket dazu. Die Migration der Daten von lokal betriebenen Exchange-Servern zu Office 365 unterstützt Microsoft ebenfalls. Sie finden diese Möglichkeiten auf der Startseite des Portals, wenn Sie auf *Optionen* im Bereich *Outlook* oder *Exchange Online* klicken. Dort steht dazu die Option *Meine Organisation/E-Mail-Migration* zur Verfügung.

Es besteht aber auch die Möglichkeit, einen zusätzlichen lokalen Exchange-Server an Windows Server 2012 R2 Essentials anzubinden. Der neue Server bietet dazu auch die Möglichkeit zur Nutzung eines Assistenten, der im Bereich E-Mail zur Verfügung steht. Generell hat die Migration der Exchange-Daten zu Office 365 nichts mit der Integration von Windows Server 2012 R2 Essentials ins Netzwerk zu tun, diese läuft unabhängig davon. Unternehmen sollten erst die Exchange-Daten vom aktuellen SBS lösen und danach den neuen Server ins Netzwerk einbinden.

Unternehmen können Daten in Windows Server 2012 R2 Essentials in der Cloud beim Microsoft Online Backup Service speichern. Auch hierzu bietet der Server einen eigenen Assistenten an. Allerdings lassen sich Daten auch noch auf herkömmlichem Weg mit Drittherstellersoftware oder auf einer lokalen Festplatte mit der Windows Server-Sicherung sichern. Administratoren können direkt vom Dashboard aus auf den internen Store für Windows Server 2012 R2 Essentials zugreifen. Über diesen lassen sich Zusatzprogramme und Add-Ins speziell für Windows Server 2012 R2 Essentials installieren. Der Vorteil dieser Add-Ins besteht darin, dass sich diese ebenfalls in das Dashboard integrieren.

Wer auf Windows Server 2012 R2 Essentials migriert, kann den Server als Neuinstallation im Netzwerk einbinden. Das ist auch der von Microsoft empfohlene Weg, da hier keine Altlasten anfallen und keine komplizierten Migrationsaufgaben notwendig sind. Anschließend legt der Administrator die Benutzerkonten neu an und kopiert die Daten in die entsprechenden Ordner. Alle Aufgaben lassen sich dann schnell und einfach im Dashboard vornehmen.

Damit Administratoren Windows Server 2012 R2 installieren können, muss der Server über 160 GB freien Speicherplatz auf der Festplatte verfügen. Das eigentliche Betriebssystem benötigt aber maximal 20 GB. Den Rest verwendet der Server als Datenpartition, wie bereits bei SBS 2011 Essentials. Freigaben und Ordner legt der Assistent automatisch an, genauso wie die Active Directory-Domäne. Weitere Systemvoraussetzungen sind:

- **CPU** 64 Bit 1,4 GHz Single-Core oder 1,3 GHz Multi-Core (Minimum)
- **Arbeitsspeicher** 2 GB (Minimum) bis 8 GB (empfohlen) oder mehr
- **Clientbetriebssysteme** Windows 7, Windows 8, Mac OS X Version 10.5 bis 10.7

Windows Server 2012 R2 Essentials virtuell installieren

Die Installation von Windows Server 2012 R2 Essentials erfolgt als normaler eigenständiger Server grundsätzlich genauso wie in den Vorgängerversionen. Es gibt allerdings Möglichkeiten zur Virtualisierung. So können Sie zum Beispiel direkt mit dem Installations-Assistenten den Server als Virtualisierungshost mit einem virtuellen Server einrichten.

Neu ist die Möglichkeit, die Funktionen von Windows Server 2012 R2 Essentials auch als Serverrolle auf einem bereits installierten Server mit Windows Server 2012 Standard oder Datacenter durchzuführen. Nach der Installation stehen in diesem Fall exakt die gleichen Verwaltungsmöglichkeiten und Funktionen zur Verfügung wie bei der Installation von einem Windows Server 2012 R2 Essentials-Datenträger.

Neu ist außerdem die Möglichkeit, Windows Server 2012 R2 Essentials komplett virtuell zu installieren. Das ist zwar technisch bereits mit Windows Server 2012 Essentials möglich gewesen, war aber lizenzrechtlich nicht erlaubt. Außerdem ist in diesem Fall eine weitere Serverlizenz für den Virtualisierungshost notwendig. Umgehen lässt sich das im Fall von Windows Server 2012 Essentials zwar mit dem kostenlosen Hyper-V Server 2012 R2. Allerdings erhalten Unternehmen bei Problemen hierfür keinerlei Support von Microsoft. Außerdem ist in diesem Fall die Installation recht kompliziert.

In Windows Server 2012 R2 Essentials ist die Virtualisierung explizit erlaubt, als Funktion integriert und sogar in die Installation des Servers über einen Assistenten eingebunden. Dazu bietet der Installations-Assistent des eigenständigen Servers auch die Möglichkeit, den Server komplett als Neuinstallation in einer virtuellen Maschine mit Hyper-V 2012 R2 einzurichten. Das heißt, in der Lizenzierung von Windows Server 2012 R2 Essentials als eigenständiger Server ist die Möglichkeit neu, den Server als Virtualisierungslösung für sich selbst und andere Server zu betreiben. Mit Windows Server 2012 Essentials ist das noch nicht möglich gewesen. Außerdem lassen sich auf dem Host zusätzlich weitere Server betreiben und virtualisieren.

Vorteil der Virtualisierung von Windows Server 2012 R2 Essentials auf einem physischen Server ist also noch die Möglichkeit, auch andere virtuelle Server auf dem Host zu installieren. So lassen sich in das Netzwerk noch mehr Server integrieren, auch mehrere Servercomputer mit Windows Server 2012 R2 Essentials. Diese müssen Unternehmen aber gesondert lizenzieren. Durch die neuen Möglichkeiten von Windows Server 2012 R2 Essentials steigt auch der Preis von etwa 400 Dollar auf etwas über 500 Dollar (die Euro-Preise standen bei Drucklegung des Buchs noch nicht fest). Angesichts des Funktionsumfangs ist das aber zu verschmerzen.

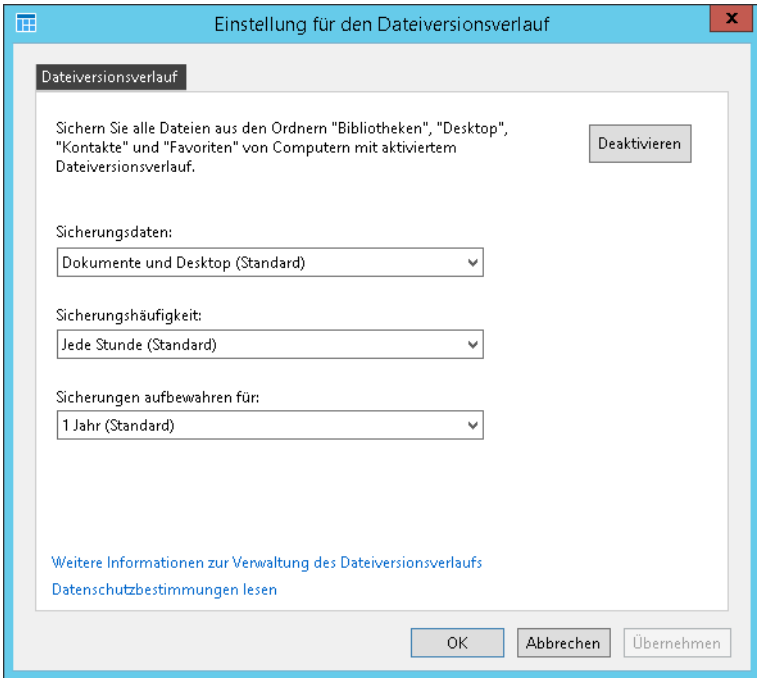
Wie schon Windows Server 2012 Essentials, erlaubt auch Windows Server 2012 R2 Essentials die Anbindung von 25 Anwendern und 50 PCs. Reichen diese Lizenzen nicht mehr aus, können Unternehmen auf die Standard oder Datacenter-Edition von Windows Server 2012 R2 wechseln.

Windows Server 2012 R2 Essentials als Serverrolle installieren

Installieren Unternehmen die Serverrolle von Windows Server 2012 R2 Essentials auf Servern mit Windows Server 2012 Standard oder Datacenter, fällt die Beschränkung von 25 Anwendern generell weg. Allerdings muss hier gesondert lizenziert werden. Außerdem können diese Server Mitglieder von größeren Active Directory-Gesamtstrukturen werden.

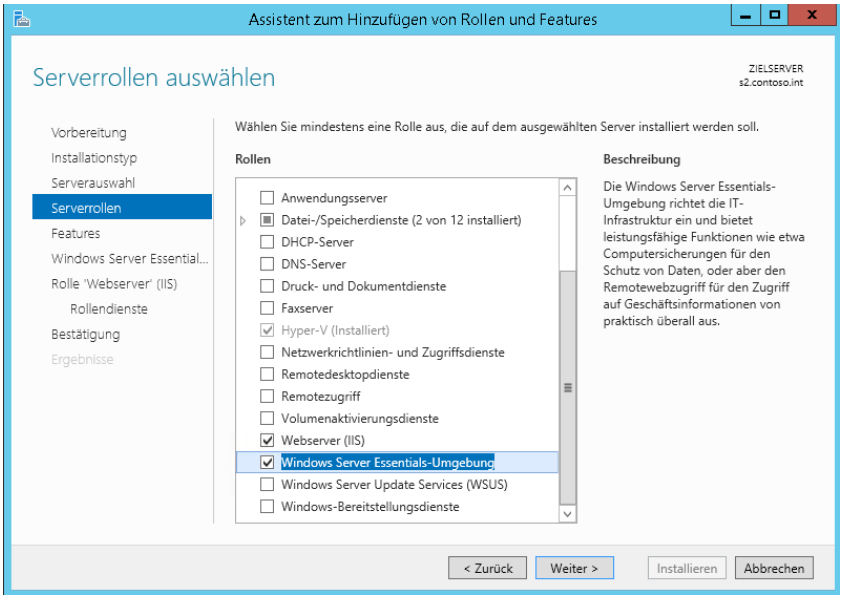
Zusätzlich können Unternehmen mehrere Server in Niederlassungen installieren. Hier gibt es generell keine Grenzen mehr. Das hat den Vorteil, dass sich die Sicherung von Clients in Niederlassungen wesentlich einfacher gestalten lässt, was einer der Hauptvorteile von Windows Server 2012 R2 Essentials ist. Da Windows Server 2012 R2 Essentials über Assistenten verfügt, um Arbeitsstationen über das Netzwerk komplett zu sichern, ist der Einsatz auch bei mittelständischen oder großen Unternehmen durchaus sinnvoll. Die neue Version arbeitet noch besser mit dem Dateiversionsverlauf von Windows 8.1 zusammen und kann Computer mit den Windows-Bereitstellungsdiensten (WDS) auf Basis von Images sichern und wiederherstellen.

Abbildg. 41.7 Windows Server 2012 R2 Essentials arbeitet mit dem Dateiversionsverlauf in Windows 8.1 zusammen



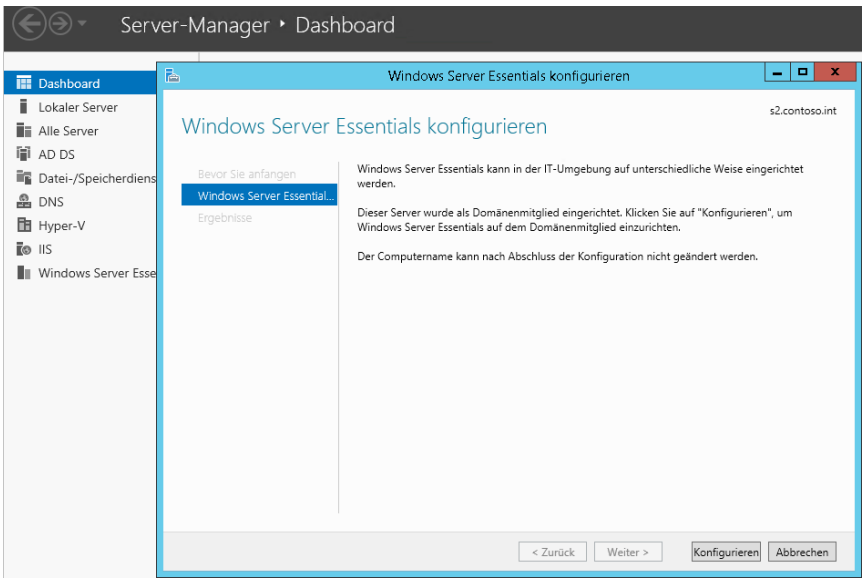
Das alles gilt nicht nur bei der Installation als Serverrolle. Wer Windows Server 2012 R2 Essentials eigenständig installiert, muss generell mit den gleichen Einschränkungen arbeiten, wie mit Windows Server 2012 Essentials. Die Installation der Funktionen für Windows Server 2012 R2 Essentials auf Servern mit Windows Server 2012 R2 Standard oder Datacenter gestaltet sich recht einfach: Sie starten den Server-Manager, rufen *Verwalten/Rollen und Features* hinzufügen auf, wählen den entsprechenden Server und anschließend die neue Serverrolle *Windows Server Essentials-Umgebung* aus.

Abbildg. 41.8 Funktionen für Windows Server 2012 R2 Essentials installieren Sie in Windows Server 2012 R2 auch als Serverrolle



Während der Installation der Serverrolle müssen Sie keinerlei Einstellungen vornehmen. Die Einrichtung der Essentials-Funktionen nehmen Sie nach dem Neustart des Servers und erst dann vor, wenn die Rolle installiert ist. Nachdem die Serverrolle installiert ist, starten Sie den Konfigurations-Assistenten für die Essentials-Umgebung.

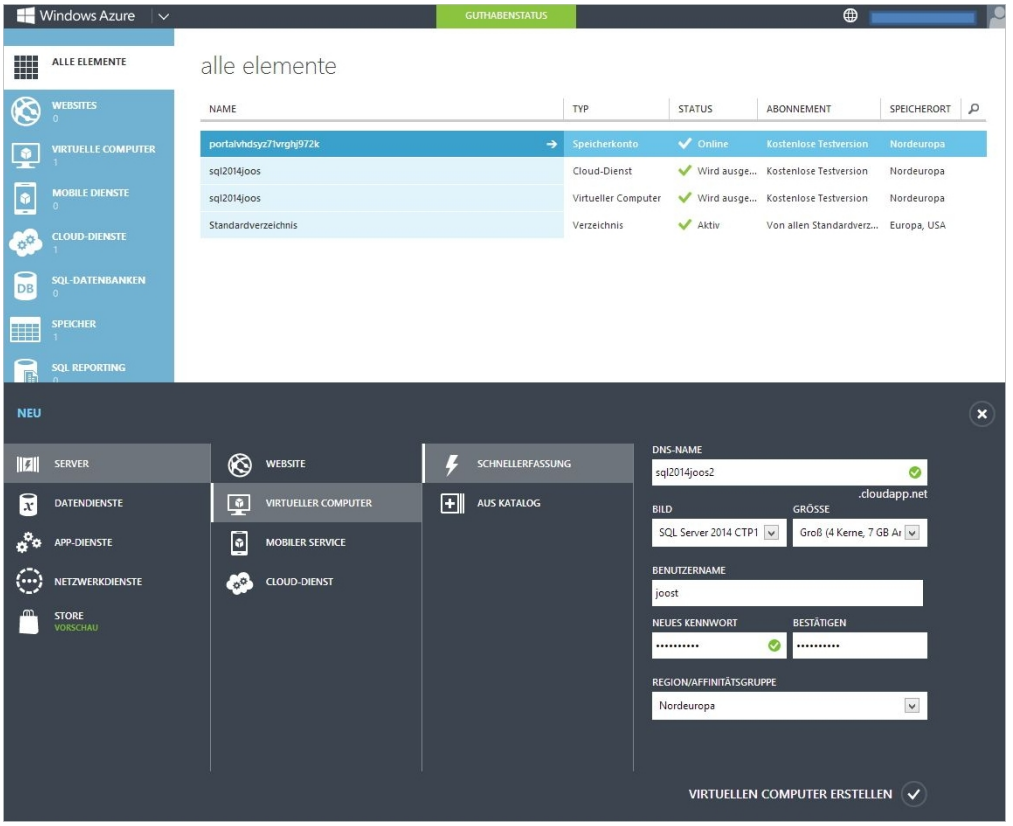
Abbildg. 41.9 Nach der Installation richten Sie Windows Server 2012 R2 Essentials über den integrierten Assistenten ein



Bei diesem Vorgang werden die notwendigen Einstellungen übernommen, Freigaben erstellt und Serverdienste eingerichtet. Die weitere Verwaltung nehmen Sie dann mit den bekannten Verwaltungswerkzeugen von Windows Server 2012 R2 oder mit dem Dashboard vor.

Durch die Möglichkeit, Windows Server 2012 R2 Essentials als Serverrolle zu betreiben, können Sie den Server auch als Image über Windows Azure Virtual Machines zur Verfügung stellen. Auch das hat große Vorteile für Unternehmen, die kleine Niederlassungen oder Abteilungen an das Netzwerk anbinden und die Funktionen von Windows Server 2012 R2 Essentials zur Verfügung stellen wollen.

Abbildg. 41.10 Virtuelle Server können Sie auch in Windows Azure erstellen. Dies gilt ebenfalls für Server mit Windows Server 2012 R2 Essentials und andere Serverdienste.



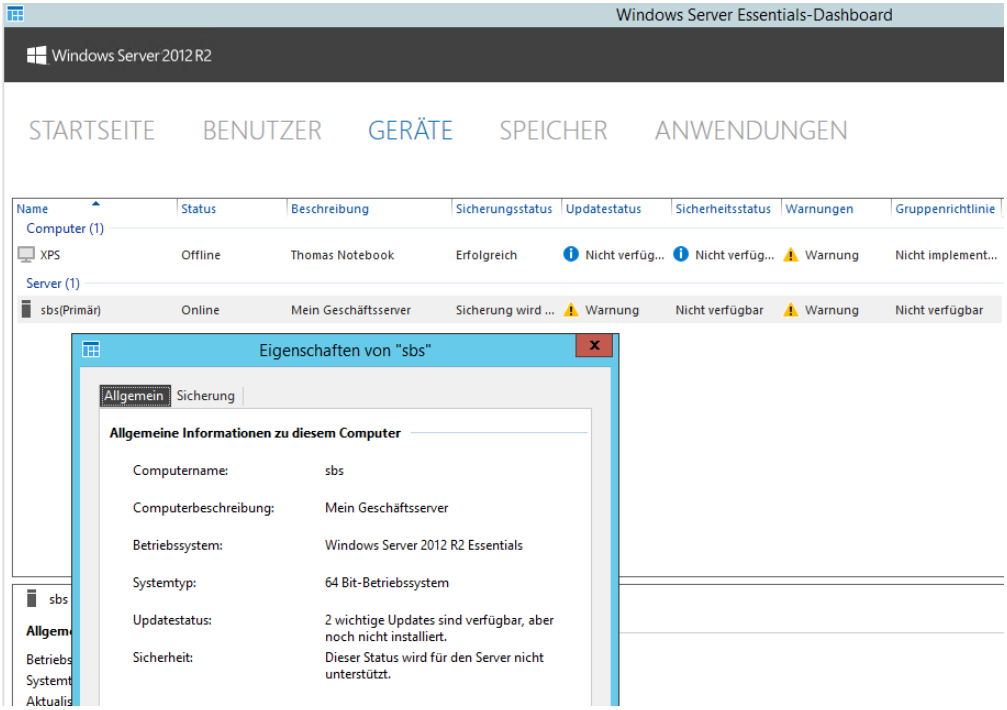
Arbeitsstationen sichern Sie auf Wunsch komplett auf den Server mit Windows Server 2012 R2 Essentials, die Daten des Servers selbst können Sie mit Windows Azure Online Backup ebenfalls in der Cloud sichern.

Windows Server 2012 R2 Essentials verwalten

Unabhängig davon, ob Sie den Server eigenständig installiert haben, als virtueller Server in Windows Azure Virtual Machines oder als Serverrolle, können Sie Einstellungen zentral mit dem Dashboard vorgeben. Hier haben Sie ähnliche Möglichkeiten wie mit SBS 2011 Essentials oder Windows Server 2012 Essentials.

Dies hat den Vorteil, dass Sie Teile der Verwaltung auch an Benutzer delegieren können. Wenn Sie Windows Server 2012 R2 Essentials als Serverrolle in eine bestehende Active Directory-Domäne aufnehmen, haben Sie im Dashboard Zugriff auf alle Benutzerkonten in der Domäne. Sie können im Dashboard dann entsprechende Einstellungen für die Benutzer definieren und Berechtigungen delegieren. Anwender können selbst eine Verbindung mit dem Server aufbauen und mit dem Dashboard arbeiten. Mit diesen Möglichkeiten lässt sich der Server als Domänencontroller oder als normaler Mitgliedsserver einsetzen.

Abbildg. 41.11 Windows Server 2012 R2 Essentials betreiben Sie auf Wunsch auch als Mitgliedsserver in vorhandenen Gesamtstrukturen



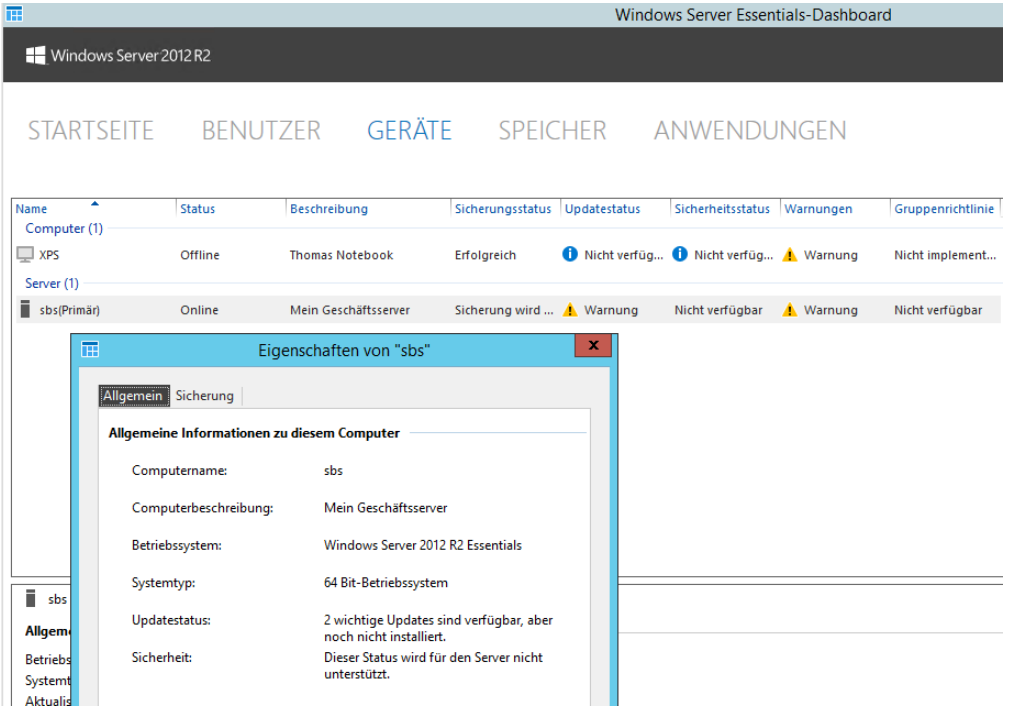
Auch bei der Installation als Serverrolle richtet der Installations-Assistent Freigaben und Sicherungen automatisch ein. Sie haben exakt die gleichen Möglichkeiten wie bei eigenständigen Installationen. Natürlich können Sie jederzeit weitere Freigaben erstellen oder Einstellungen ändern.

Mobil mit Windows Server 2012 R2 Essentials arbeiten

Bereits mit Small Business Server 2011 Essentials hat Microsoft auch für mobile Anwender die Möglichkeit geschaffen, auf den Server von unterwegs zuzugreifen. Mit Windows Server 2012 Essentials hat Microsoft diese Möglichkeiten noch verbessert. Windows Server 2012 R2 Essentials bietet darüber hinaus vor allem eine Optimierung für Smartphones und Tablet-PCs. Anwender können in Unternehmen, die BYOD (Bring Your Own Device) nutzen, optimal mit dem Server arbeiten, unabhängig davon, ob Geräte mit Windows 7/8/8.1/RT oder Windows Phone 7/8, Android oder Apple-Geräte im Einsatz sind. Dazu nutzt die neue Version nicht mehr Silverlight zur Anzeige, sondern HTML5. Das heißt, Anwender können mit jedem HTML5-kompatiblen Browser problemlos auf den Server zugreifen. Die Bedienung ist in diesem Fall auch für Touchgeräte optimiert.

Windows Server 2012 R2 Essentials unterstützt zusätzlich BranchCache. Dies bedeutet, Daten, die Anwender über Freigaben in anderen Niederlassungen auf ihren Arbeitsstationen nutzen, werden lokal zwischengespeichert. Beim nächsten Zugriff werden die Daten dem gleichen oder einem anderen Anwender noch besser und schneller zur Verfügung gestellt, ohne dass auf die ursprüngliche Remotequelle erneut zugegriffen werden muss.

Abbildg. 41.12 Windows Server 2012 R2 Essentials kann auch BranchCache nutzen



Alternative Windows Server 2012 R2 Foundation

Wer kein Dashboard und keine Assistenten sowie keinen Server benötigt, der automatisch Active Directory installiert, kann auch auf die noch günstigere Edition Windows Server 2012 R2 Foundation setzen. Diese erlaubt die Anbindung von maximal 15 Benutzern, ebenfalls ohne Clientzugriffslizenzen. Es gibt aber kein einheitliches Verwaltungswerkzeug und der Administrator, der den Server einrichtet, muss einiges an Know-how mitbringen. Auch Freigaben werden nicht automatisch angelegt, es gibt keinen Webzugriff und die Möglichkeit zur Datensicherung von Clientcomputern ist nicht vorhanden.

Die Verwaltung des Servers ist identisch mit der herkömmlichen Verwaltung von Windows Server 2012 R2. Hyper-V ist bei dieser Edition nicht integriert, aber Sie können Windows Server 2012 R2 Foundation als Hyper-V-Gast installieren. Diese Edition ist nur als OEM-Version erhältlich. Eine Lizenz ermöglicht die Installation auf einer physischen Maschine. Im Gegensatz zu den anderen Editionen dürfen Sie keine weiteren virtuellen Maschinen mit einer Lizenz installieren.

Setzen Sie die Edition als Remotedesktopserver ein, dürfen sich ebenfalls nur 15 Benutzer mit dem Server verbinden. Für diese Benutzer sind allerdings Clientzugriffslizenzen für Remotedesktopdienste notwendig, denn diese sind nicht im Betriebssystem integriert. Setzen Unternehmen Windows Server 2012 R2 Foundation in Active Directory ein, dürfen in dieser Domäne nur maximal 15 Benutzerkonten angelegt sein. Der Server darf nicht dazu verwendet werden, um untergeordnete Domänen zu erstellen. Stellt der Server Lizenzverstöße fest, fährt er automatisch herunter.

Die Version lässt sich nachträglich auf die Standard-Edition aktualisieren, ohne den Server neu installieren zu müssen. Wer sich etwas mit dem Server auseinandersetzt, kann auf den Client-PCs eine Datensicherung einrichten und diese Daten auf einer Freigabe des Servers sichern. Alle diese Funktionen müssen aber manuell eingerichtet werden.

Zusammenfassung

In diesem Kapitel haben wir Ihnen gezeigt, wie Sie mit Windows Server 2012 R2 Essentials oder Foundation Benutzer in kleinen Unternehmen oder Niederlassungen anbinden. Durch die Möglichkeit, Windows Server 2012 R2 Essentials zu virtualisieren oder als Serverrolle zu installieren, profitieren auch kleine Firmen von den Funktionen des Servers.

Kapitel 42

Active Directory-Verbunddienste und Workplace Join

In diesem Kapitel:

Mit Windows Server 2012 R2 und Windows 8.1, Windows RT 8.1 und iOS 7-Geräten haben Sie die Möglichkeit, Clients durch Active Directory-Verbunddienste (Active Directory Federation Services, AD FS) über das Internet an Unternehmensressourcen anzubinden. Im Gegensatz zu den Arbeitsplatzordnern (siehe Kapitel 5) arbeiten Anwender bei Workplace Join mit ihrer gewohnten Umgebung, können aber auf bestimmte Ressourcen im Unternehmensnetzwerk zugreifen, die ansonsten nur Domänenmitgliedern vorbehalten sind. Wir zeigen Ihnen in diesem Kapitel, wie Sie diese Funktion nutzen.

Im Rahmen der Einrichtung von Workplace Join erklären wir Ihnen auch die Einrichtung der Active Directory-Verbunddienste auf Basis einer Beispielumgebung.

Installieren und Einrichten der Active Directory-Verbunddienste

Die Active Directory-Verbunddienste (Active Directory Federation Services, AD FS) haben die Aufgabe, mehrere Gesamtstrukturen miteinander zu verbinden oder externe Anwender über eine eigene Authentifizierung an Unternehmensressourcen anzubinden. Die nachfolgende Anleitung zur Installation einer Beispielumgebung mit AD FS dient später der Einrichtung von Workplace Join zusammen mit einem Windows 8.1-Rechner.

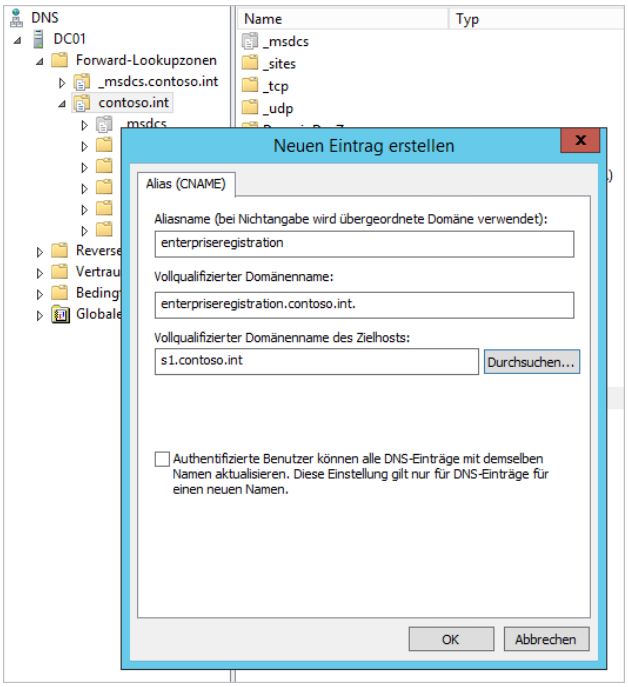
Um eine Testumgebung mit AD FS aufzubauen, brauchen Sie mindestens drei Server: einen Domänencontroller, den AD FS-Server und einen Webserver, auf den Sie zugreifen können, um die Authentifizierung zu testen. Auf allen drei Servern installieren Sie Windows Server 2012 R2. Um den Zugriff auf die Webanwendung mit Workplace Join zu testen, benötigen Sie noch einen Arbeitsplatzrechner mit Windows 8.1. Sie können zwar auch mit Windows RT 8.1 und Apple iOS 7 auf solche Ressourcen zugreifen, allerdings lässt sich die Einrichtung mit Windows 8.1 einfacher und schneller durchführen.

Vorbereitungen für die AD FS-Infrastruktur

Damit Sie eine AD FS-Infrastruktur mit einer Beispielanwendung aufbauen können, benötigen Sie eine Active Directory-Gesamtstruktur sowie einen Server mit einer internen Zertifizierungsstelle (siehe Kapitel 30). Außerdem müssen Sie verwaltete Dienstkonten anlegen (siehe Kapitel 12) sowie Servern SSL-Zertifikate zuweisen (siehe Kapitel 27). In den folgenden Abschnitten zeigen wir Ihnen auf Basis von Beispielen, wie Sie dabei vorgehen. Die nachfolgenden Schritte können Sie auch bei der Einrichtung von anderen Serverdiensten verwenden.

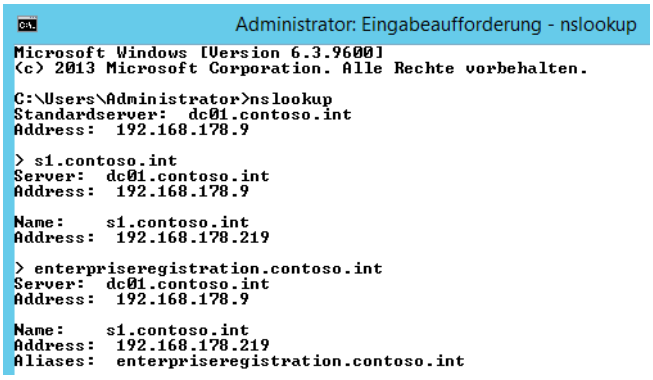
Achten Sie im ersten Schritt darauf, dass der vollqualifizierte Domänenname (FQDN) des AD FS-Servers auf den DNS-Servern korrekt eingetragen ist und aufgelöst werden kann. Da der Server Mitglied der Domäne ist, sollte das ohnehin der Fall sein. Zusätzlich sollten Sie noch den DNS-Eintrag *enterpriseregistration* erstellen. Dieser muss ein Alias (CNAME) des AD FS-Servers sein. Sie erstellen einen Alias in der DNS-Verwaltung über das Kontextmenü der Zone.

Abbildg. 42.1 Erstellen eines Alias für den AD FS-Server



Testen Sie die Namensauflösung der beiden Einträge in der Eingabeaufforderung über *Nslookup*.

Abbildg. 42.2 Überprüfen der Namensauflösung für Server in der Eingabeaufforderung



Verwaltetes Dienstkonto für AD FS einrichten

Für die Active Directory-Verbunddienste (AD FS) verwenden Sie am besten ein gruppiertes verwaltetes Dienstkonto (siehe Kapitel 12). Dieses legen Sie in der PowerShell an und geben direkt den Namen des zukünftigen AD FS-Servers mit an. Wir arbeiten zukünftig mit dem Namen *s1.contoso.int* für den AD FS-Server. Die Befehle zum Anlegen des verwalteten Dienstkontos sehen dann folgendermaßen aus:

```
Add-KdsRootKey –EffectiveTime (Get-Date).AddHours(-10)
New-ADServiceAccount adfsGmsa -DNSHostName s1.contoso.int -ServicePrincipalNames http/
s1.contoso.int
```

Sie benötigen dazu das Active Directory-Modul für die PowerShell. Auf normalen Servern müssen Sie dazu nachträglich die Remoteverwaltungstools für Active Directory installieren, auf Domänencontrollern ist das jedoch Modul automatisch verfügbar. Die Daten des angelegten Dienstkontos zeigen Sie mit dem Cmdlet *Get-ADServiceAccount adfsGmsa* an.

SSL-Zertifikate als Vorlage in Active Directory-Zertifikatdiensten festlegen

Bevor Sie AD FS als Serverrolle installieren, müssen Sie den Servercomputer, auf dem Sie AD FS installieren wollen, in die Domäne aufnehmen. Danach müssen Sie ein Zertifikat dem Server zuweisen (siehe Kapitel 30).

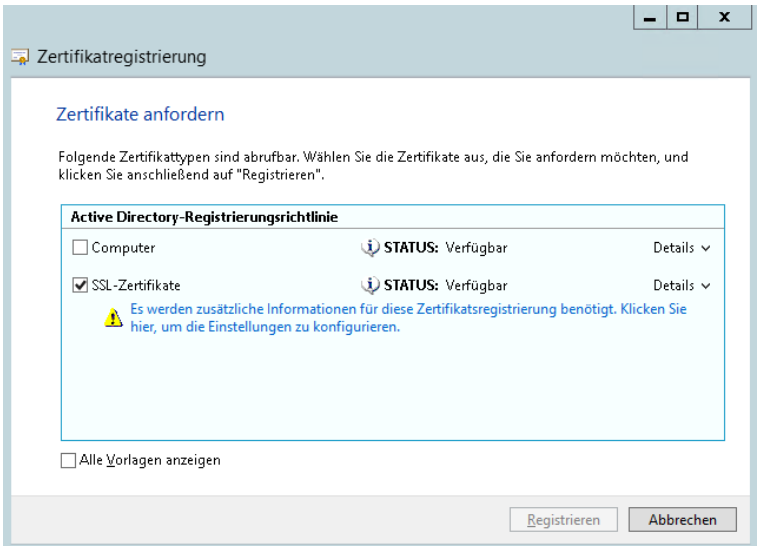
Das Zertifikat muss SSL-Verschlüsselung (Secure Sockets Layer) unterstützen. Daher benötigen Sie zunächst eine interne Zertifizierungsstelle. Wie Sie diese installieren und einrichten, lesen Sie in Kapitel 30. Im Anschluss müssen Sie auf dem Server mit der Zertifizierungsstelle eine neue Vorlage für SSL-Zertifikate bereitstellen. Auf Basis dieser Vorlage rufen Sie dann auf dem AD FS-Server ein neues SSL-Zertifikat ab. Gehen Sie dazu auf dem Zertifikatserver folgendermaßen vor:

1. Rufen Sie mit *certtmpl.msc* die Verwaltung der Vorlagen auf dem Zertifikatserver auf.
2. Klicken Sie mit der rechten Maustaste auf die Vorlage *Webserver* und wählen Sie *Duplizieren*.
3. Verwenden Sie als Namen für das neue Zertifikat auf der Registerkarte *Allgemein* die Bezeichnung »SSL-Zertifikate«.
4. Wechseln Sie zur Registerkarte *Sicherheit* und klicken Sie auf *Hinzufügen*.
5. Klicken Sie im neuen Fenster auf *Objekttypen* und wählen Sie *Computer* aus.
6. Geben Sie den Namen der AD FS-Server ein, die Sie betreiben wollen.
7. Aktivieren Sie für alle Computer das Recht *Registrieren* für die Zertifikatvorlage.
8. Klicken Sie auf *OK*.
9. Rufen Sie die Verwaltung der Zertifizierungsstelle mit *certsrv.msc* auf.
10. Klicken Sie mit der rechten Maustaste auf *Zertifikatvorlagen* und wählen Sie *Neu/Auszustellende Zertifikatvorlage*.
11. Wählen Sie die von Ihnen erstellte Vorlage aus. Die Vorlage steht jetzt in der Infrastruktur für die Zuteilung an Server bereit.

Um auf dem AD FS-Server ein Zertifikat auf Basis der von Ihnen erstellten Vorlage abzurufen, gehen Sie folgendermaßen vor:

1. Rufen Sie auf dem AD FS-Computer die Konsole *certlm.msc* auf.
2. Klicken Sie mit der rechten Maustaste auf *Eigene Zertifikate/Zertifikate* und wählen Sie *Alle Aufgaben/Neues Zertifikat anfordern*.
3. Bestätigen Sie die erste Seite der Registrierung.
4. Bestätigen Sie auf der nächsten Seite die Active Directory-Registrierungsrichtlinie.
5. Wählen Sie auf der Seite mit den Vorlagen die von Ihnen erstellte Vorlage aus. Steht diese nicht zur Verfügung, überprüfen Sie die vorangegangenen Schritte noch einmal.

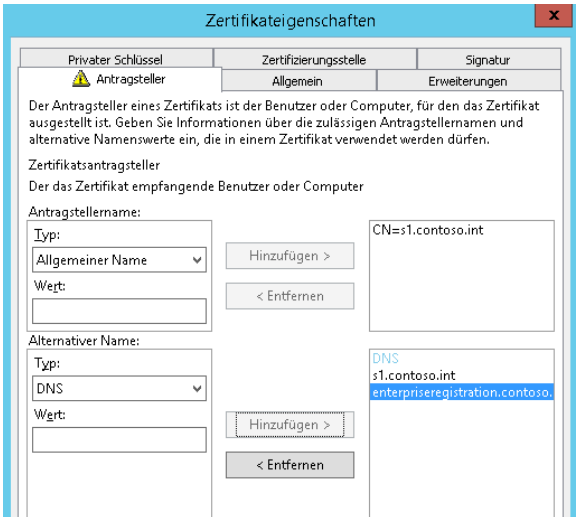
Abbildg. 42.3 Anfordern eines Zertifikats für ein Computerkonto



Im Dialogfeld müssen Sie jetzt noch auf den Link mit dem Text unterhalb der Vorlage klicken, um wichtige Daten für das Zertifikat einzugeben. Hier müssen Sie folgende Daten eingeben, bevor Sie mit *OK* bestätigen. Danach rufen Sie das Zertifikat mit *Registrieren* ab:

- *Allgemeiner Name*: *s1.contoso.int* (bei Ihnen der entsprechende Name des AD FS-Servers)

Abbildg. 42.4 Konfigurieren der korrekten Werte für ein SSL-Zertifikat des AD FS-Servers



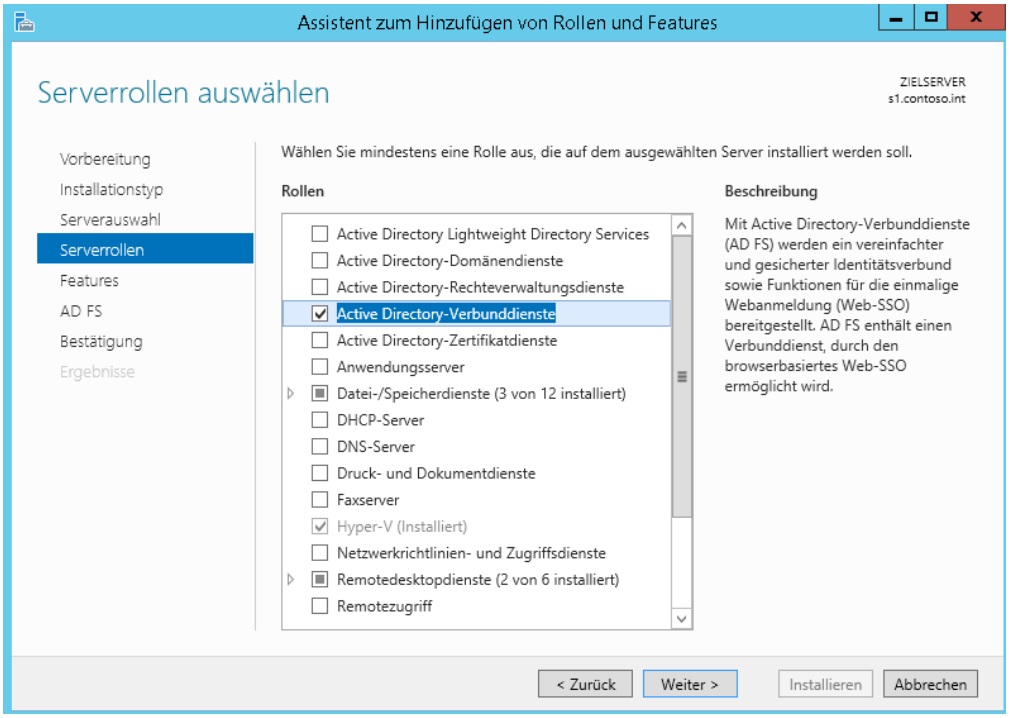
- *Alternativer Name (DNS verwenden)*:
  - *s1.contoso.int* (bei Ihnen der entsprechende Name des AD FS-Servers)
  - *enterpriseregistration.contoso.int*

AD FS als Serverrolle installieren

Haben Sie alle Vorbereitungen getroffen, installieren Sie anschließend AD FS als Serverrolle auf dem AD FS-Server. Dazu wählen Sie über *Verwalten/Rollen und Features hinzufügen* den Rollendienst *Active Directory-Verbunddienste* aus.

Während der Installation müssen Sie keine Einstellungen vornehmen, sondern wie bei den Active Directory-Domänendiensten lediglich die Systemdateien erstellen.

Abbildg. 42.5 Installieren der Active Directory-Verbunddienste



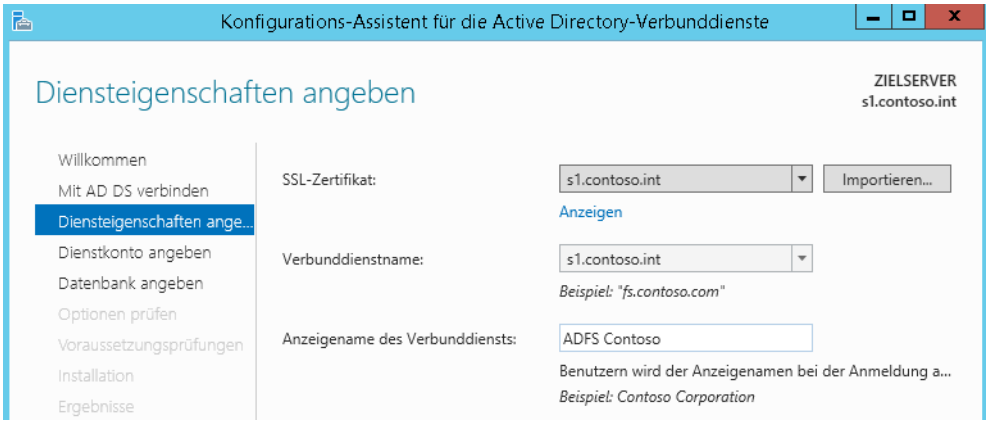
AD FS einrichten

Nachdem die Installation abgeschlossen ist, richten Sie über das Benachrichtigungscenter des Server-Managers die Infrastruktur im Netzwerk über einen Assistenten ein:

1. Bestätigen Sie die Startseite und geben Sie dann die Anmeldedaten eines Domänenadministrators ein.

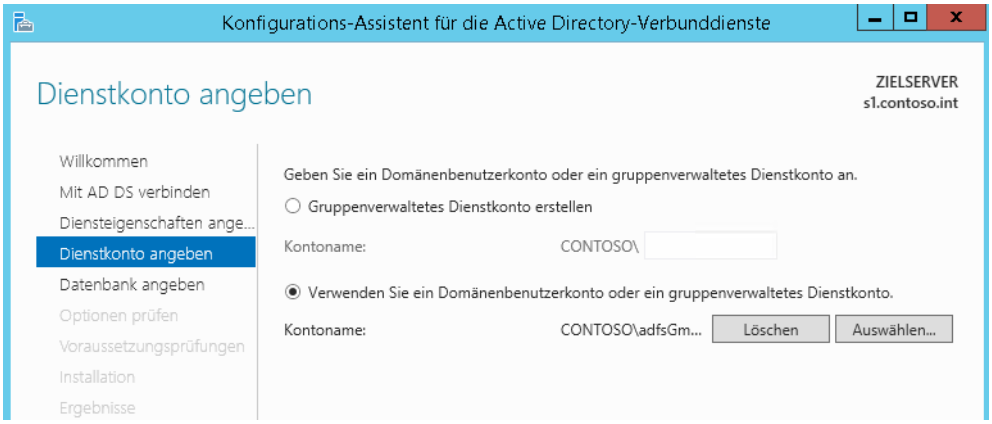
2. Wählen Sie auf der Seite *Diensteigenschaften bearbeiten* das von Ihnen installierte Zertifikat. Lassen Sie das Zertifikat anzeigen und stellen Sie sicher, dass das richtige Zertifikat verwendet wird.
3. Als Anzeigenamen können Sie einen beliebigen Namen verwenden, zum Beispiel »AD FS Contoso«.

Abbildg. 42.6 Konfigurieren der Diensteigenschaften von AD FS auf dem AD FS-Server



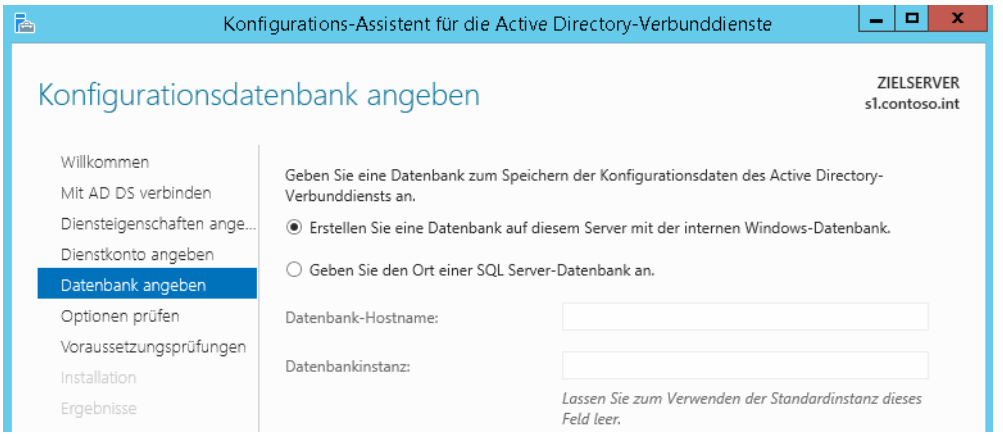
Auf der Seite *Dienstkonto angeben* aktivieren Sie die Option *Verwenden Sie ein Domänenbenutzerkonto oder ein gruppenverwaltetes Dienstkonto*. Wählen Sie dann das von Ihnen erstellte verwaltete Dienstkonto aus. Mehr zu diesem Thema erfahren Sie zu Beginn des Kapitels und in Kapitel 12.

Abbildg. 42.7 Auswählen des Dienstkontos für AD FS



Auf der Seite *Konfigurationsdatenbank angeben* aktivieren Sie die Option *Erstellen Sie eine Datenbank auf diesem Server mit der internen Windows-Datenbank*.

Abbildg. 42.8 Konfigurieren der AD FS-Datenbank



Im nächsten Fenster erhalten Sie eine Zusammenfassung Ihrer Einstellungen angezeigt. Als Nächstes werden die Voraussetzungen überprüft und dann die AD FS-Infrastruktur erstellt. Klicken Sie danach auf *Konfigurieren*, um die AD FS-Infrastruktur auf dem Server zu installieren.

Damit AD FS korrekt funktioniert, müssen Sie darauf achten, dass die Zertifikate vorhanden sind und funktionieren. Sie konfigurieren die Zertifikate in der AD FS-Verwaltung im Bereich *Dienst/Zertifikate*.

Geräteregistrierung konfigurieren

Sobald die AD FS-Infrastruktur konfiguriert ist, müssen Sie die Geräteregistrierung auf dem AD FS-Server einrichten. Dazu öffnen Sie eine PowerShell-Sitzung und geben den folgenden Befehl ein:

```
Initialize-ADDeviceRegistration
```

Sie werden nach dem Dienstkonto gefragt. Hier geben Sie die Daten des verwalteten Dienstkontos ein, zum Beispiel *contoso\adfsgmsa$*.

Danach rufen Sie den folgenden Befehl auf:

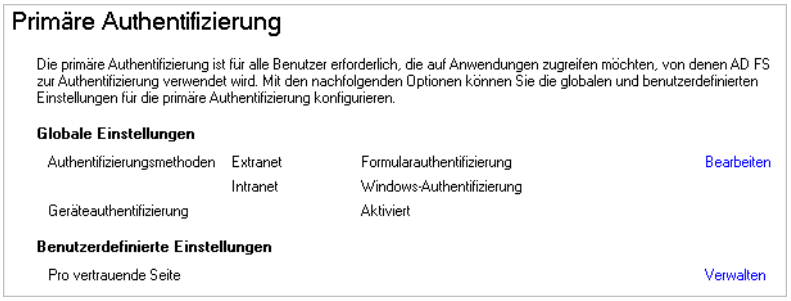
```
Enable-AdfsDeviceRegistration
```

Abbildg. 42.9 Aktivieren der Geräteregistrierung für AD FS in der PowerShell

```
PS C:\Users\administrator.CONTOSO> Initialize-ADDeviceRegistration

Cmdlet Initialize-ADDeviceRegistration an der Befehlspipelineposition 1
Geben Sie Werte für die folgenden Parameter an:
ServiceAccountName: contoso\adfsgmsa$

Mit diesem Befehl wird Active Directory für das Hosten von Device Registration Service in der aktuellen Gesamtstruktur
vorbereitet.
Möchten Sie den Vorgang fortsetzen?
[J] Ja  [A] Ja, alle  [N] Nein  [K] Nein, keine  [H] Anhalten  [?] Hilfe (Standard ist "J"): j
WARNUNG: Die Active Directory-Struktur wurde für die Geräteregistrierung vorbereitet. Führen Sie für jeden Knoten in
Ihrer AD FS-Farm das Enable-AdfsDeviceRegistration-Cmdlet aus, um AD FS Device Registration Service zu verwenden.

Message                                 Context                                 Status
-------                                 -------                                 ------
Die Konfiguration wurde erfolgreich ... DeploymentSucceeded                     Success


PS C:\Users\administrator.CONTOSO> Enable-AdfsDeviceRegistration
WARNUNG: Das SSL-Zertifikat enthält nicht alle UPN-Suffixwerte, die im Unternehmen vorhanden sind. Benutzer mit
UPN-Suffixwerten, die nicht im Zertifikat enthalten sind, können ihre Geräte nicht zum Arbeitsplatz hinzufügen. Weitere
 Informationen finden Sie unter http://go.microsoft.com/fwlink/?LinkId=311954.

Message                                 Context                                 Status
-------                                 -------                                 ------
Die Konfiguration wurde erfolgreich ... DeploymentSucceeded                     Success
```

Öffnen Sie auf dem AD FS-Server die AD FS-Verwaltungskonsole, klicken Sie mit der rechten Maustaste auf *Authentifizierungsrichtlinien* und dann in der Mitte des Fensters bei *Primäre Authentifizierung/Globale Einstellungen* auf *Bearbeiten*. Aktivieren Sie im folgenden Fenster das Kontrollkästchen *Geräteauthentifizierung aktivieren*.

Abbildg. 42.10 Aktivieren der Geräteauthentifizierung in AD FS



Einrichten einer Beispiel-Webanwendung für AD FS

Um den Nutzen von AD FS und Workplace Join von Windows 8.1 zu demonstrieren, eignet sich am besten eine Webanwendung auf einem Server mit IIS 8.5 (Internetinformationsdienste). Sie konfigurieren die Webanwendung so, dass Anwender mit Windows 8.1 auf die Webanwendung zugreifen können, auch ohne dass der entsprechende PC oder das Notebook Mitglied der Domäne ist.

Microsoft stellt eine solche Webanwendung über das Windows Identity Foundation SDK kostenlos zur Verfügung. Dieses finden Sie auf der Seite *http://www.microsoft.com/de-de/download/details.aspx?id=4451* [Ms179-K42-01]. Außerdem benötigen Sie für die Installation der notwendigen Rollen das Windows Server 2012 R2-Installationsmedium.

Webserver und notwendige Features installieren

Um den Server zu testen, müssen Sie zunächst auf einem anderen Server als den AD FS-Server die Serverrolle *Webserver* (siehe Kapitel 27) und zusätzlich *Webserver/Anwendungsentwicklung/ASP.NET 3.5* installieren. Lassen Sie auch die dazugehörigen Features installieren, die der Assistent standardmäßig vorschlägt.

Auf der Seite *Features auswählen* bei der Installation des Webservers müssen Sie noch das Serverfeature *Windows Identity Foundation 3.5* für die Installation auswählen (siehe Kapitel 4). Haben Sie alle Features festgelegt, ist auf der letzten Seite noch den Speicherort der Installationsdateien anzugeben. Dazu klicken Sie auf den Link *Alternativen Quellpfad angeben* und wählen anschließend zum Beispiel den Datenträger mit der Windows Server 2012 R2-Installations-DVD und hier den Unterordner *Sources\Sxs*, zum Beispiel *D:\Sources\Sxs*, aus.

Nach der Installation des Webservers installieren Sie als Nächstes das Windows Identity Foundation SDK (*http://www.microsoft.com/de-de/download/details.aspx?id=4451* [Ms179-K42-01]).

Anschließend installieren Sie auf dem Webserver ein SSL-Zertifikat für den Webserver (siehe Kapitel 27 und den Abschnitt »SSL-Zertifikate als Vorlage in Active Directory-Zertifikatdiensten festlegen« in diesem Kapitel). Das Zertifikat muss als CN den vollqualifizierten Domänennamen (FQDN) des Webservers aufweisen und von der internen Zertifizierungsstelle stammen.

Beispielanwendung für AD FS und Workplace Join vorbereiten

Haben Sie alle Vorbereitungen des vorherigen Abschnitts durchgeführt, kopieren Sie die Beispielanwendung aus dem Installationsordner des Windows Identity Foundation SDK (*C:\Program Files (x86)\Windows Identity Foundation SDK\v3.5\Samples\Quick Start\Web Application\PassiveRedirectBasedClaimsAwareWebApp* in den Ordner *C:\Inetpub\Claimapp*. Öffnen Sie danach die Datei *Default.aspx.cs* mit einem Texteditor.

Suchen Sie nach dem Eintrag *ExpectedClaims* und verwenden Sie die zweite gefundene Stelle. Sie müssen nun mit // die Zeilen in der Datei auskommentieren, die um die gefundene Stelle herum aufgeführt sind. Danach sollte der Bereich wie folgt aussehen:

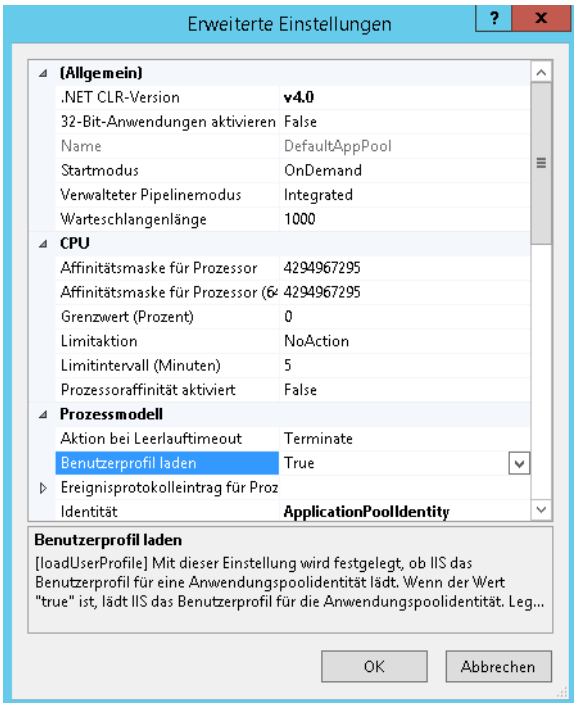
Listing 42.1 Beispiellisting einer Datei für AD FS

```
Foreach (claim claim in claimsIdentity.Claims)
{
   //Before showing the claims validate that this is an expected claim
   //If it is not in the expected claims list then don't show it
   //if (ExpectedClaims.Contains( claim.ClaimType ) )
   // {
      writeClaim( claim, table );
   //}
}
```

Speichern Sie die Datei und öffnen Sie anschließend die Datei *web.config*. Löschen Sie den gesamten Bereich *<microsoft.identityModel>* bis *</microsoft.identityModel>*, einschließlich von *<microsoft.identityModel>* und *</microsoft.identityModel>*. Speichern Sie die Datei wieder.

Öffnen Sie den IIS-Manager und klicken Sie auf *Anwendungspools* (siehe Kapitel 27). Klicken Sie mit der rechten Maustaste auf *DefaultAppPool* und wählen Sie *Erweiterte Einstellungen*. Setzen Sie den Wert *Prozessmodell/Benutzerprofil laden* auf *True*. Rufen Sie danach über das Kontextmenü die Grundeinstellungen auf und ändern Sie *.NET CLR Version* zu *NET CLR Version v2.0.50727*.

Abbildg. 42.11 Anpassen der erweiterten Einstellungen für einen Anwendungspool

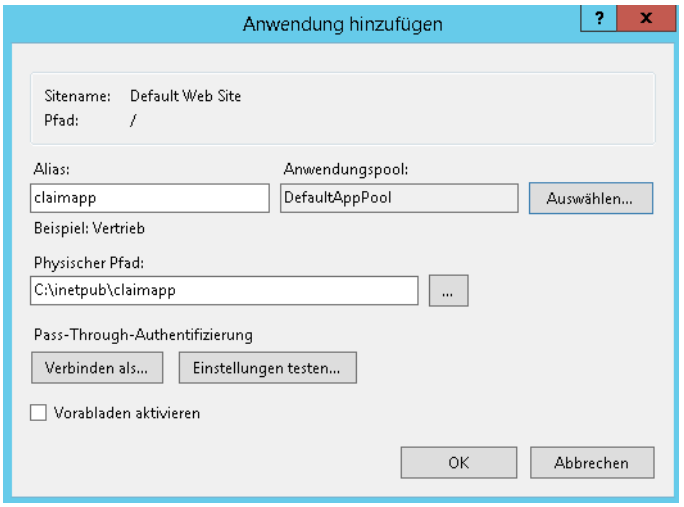


Klicken Sie danach mit der rechten Maustaste auf *Default Web Site* und wählen Sie *Bindungen bearbeiten* aus. Fügen Sie eine HTTPS-Bindung zum Port 443 hinzu und verwenden Sie das SSL-Zertifikat, das Sie auf dem Server installiert haben.

Beispielanwendung installieren

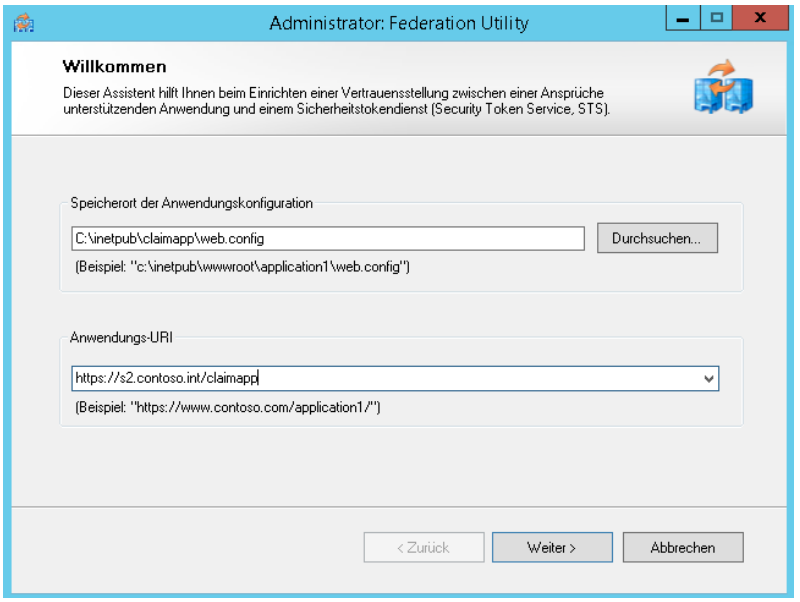
Nachdem Sie alle Vorbereitungen getroffen haben, aktivieren Sie die Beispielanwendung auf dem Webserver. Dazu klicken Sie mit der rechten Maustaste auf *Default Web Site* im IIS-Manager und wählen *Anwendung hinzufügen*. Setzen Sie den Alias auf *claimapp* und den physischen Pfad auf *C:\inetpub\claimapp*. Achten Sie darauf, dass als Anwendungspool *DefaultAppPool* ausgewählt ist.

Abbildg. 42.12 Installieren einer neuen Webanwendung in IIS 8.5



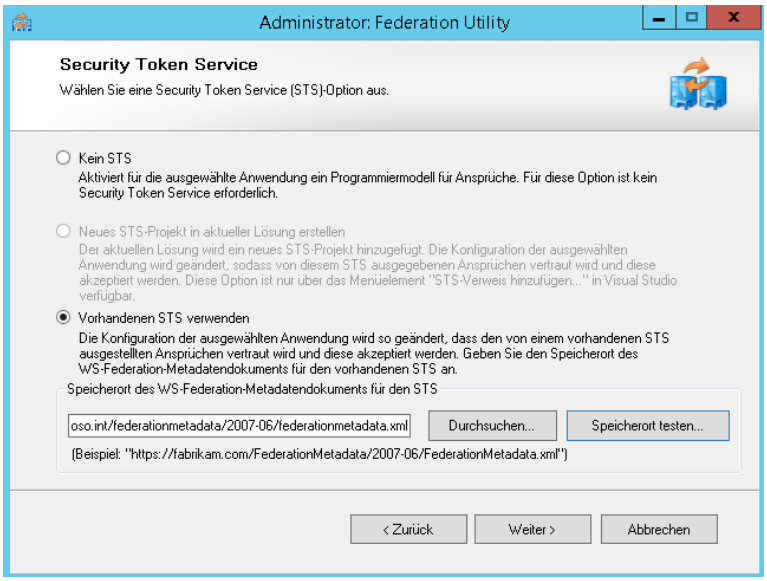
Klicken Sie danach doppelt auf die Datei *FedUtil.exe* im Ordner *C:\Program Files (x86)\Windows Identity Foundation SDK\v3.5*. Wählen Sie als *Speicherort der Anwendungskonfiguration* die Datei *web.config* im Ordner *C:\inetpub\claimapp* aus. Als URI (Uniform Resource Identifier) verwenden Sie die Adresse *https://<Webserver>/claimapp/*.

Abbildg. 42.13 Verbinden einer Webanwendung mit AD FS



Auf der nächsten Seite aktivieren Sie die Option *Vorhandenen STS verwenden*. Als Adresse verwenden Sie *https://<AD FS-Server>/federationmetadata/2007-06/federationmetadata.xml*.

Abbildg. 42.14 Einrichten des Security Token Service (STS)



Im nächsten Dialogfeld des Assistenten übernehmen Sie die Option *Zertifikatkettenüberprüfung deaktivieren* und anschließend die Option *Keine Verschlüsselung*. Auf der Seite *Angebotene Ansprüche* nehmen Sie ebenfalls keine Änderungen vor und klicken auch hier auf *Weiter*. Auf der letzten Seite aktivieren Sie die Option *Aufgabe für tägliche WS-Federationmetadatenupdates planen* und klicken auf *Fertig stellen*.

Abbildg. 42.15 Fehlermeldung nach der Einrichtung der Webanwendung für AD FS

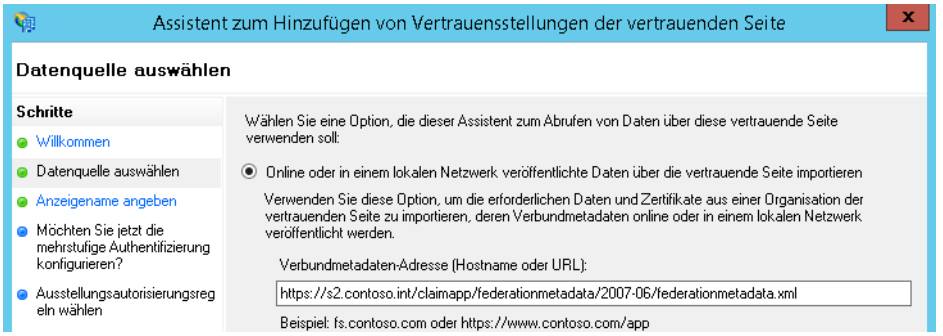
Rufen Sie nach der Einrichtung die Adresse der Claimapp auf, also *https://s2.contoso.int/claimapp* in diesem Beispiel, werden Sie auf den AD FS-Server umgeleitet und erhalten eine Fehlermeldung. Damit die Authentifizierung funktioniert, müssen Sie zunächst noch die weiteren Einstellungen vornehmen.

Vertrauensstellung zwischen Webanwendung und AD FS einrichten

Im nächsten Schritt erstellen Sie auf dem AD FS-Server Regeln für den Zugriff auf die Webanwendung. Dazu rufen Sie auf dem AD FS-Server die Verwaltungskonsole von AD FS im Server-Manager über *Tools* auf und klicken anschließend auf *Vertrauensstellungen der vertrauenden Seite* mit der rechten Maustaste. Wählen Sie *Vertrauensstellung der vertrauenden Seite hinzufügen*. Klicken Sie auf der ersten Seite auf *Start*.

Als Datenquelle wählen Sie *Online oder in einem lokalen Netzwerk veröffentlichte Daten über die vertrauende Seite importieren* und geben die Adresse *https://<Webserver>/claimapp/federationmetadata/2007-06/federationmetadata.xml* ein.

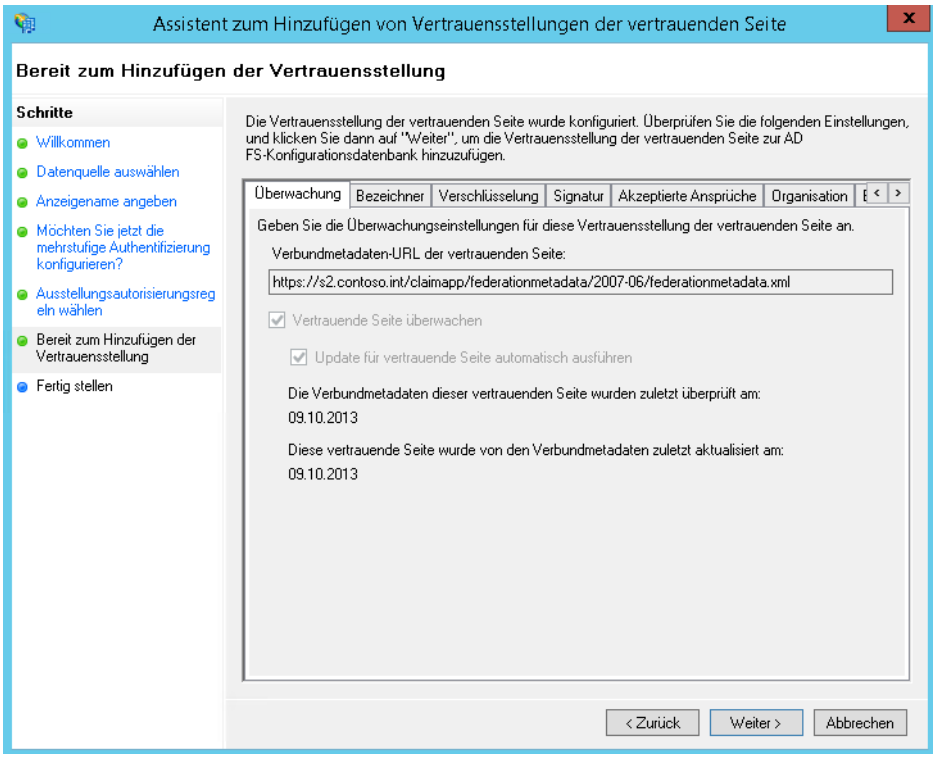
Abbildg. 42.16 Verbinden von AD FS mit der Claimapp-Webseite



Klicken Sie auf *Weiter*, überprüft der Assistent, ob die Datei vorhanden ist. Erhalten Sie einen Fehler angezeigt, überprüfen Sie im Browser, ob sich die Adresse öffnen lässt und ob die Datei vorhanden ist. Stellen Sie auch im Explorer auf dem Webserver sicher, dass die Datei existiert. Auf der nächsten Seite geben Sie den Namen für die neue Vertrauensstellung ein.

Danach legen Sie die mehrstufige Authentifizierung fest. Hier belassen Sie die Einstellung auf *Jetzt keine Einstellungen für die mehrstufige Authentifizierung konfigurieren*. Auf der Seite *Ausstellungsautorisierungsregeln* legen Sie die Option *Allen Benutzern Zugriff auf diese vertrauende Seite verweigern* fest. Danach erhalten Sie eine Zusammenfassung Ihrer Eingaben angezeigt. Auch hier klicken Sie auf *Weiter*.

Abbildg. 42.17 Anzeigen der Daten zum Hinzufügen einer Vertrauensstellung zu einer Webseite



Auf der letzten Seite belassen Sie die Einstellung auf *Nach Abschluss des Assistenten das Dialogfeld "Anspruchsregeln bearbeiten" für diese Vertrauensstellung der vertrauenden Seite öffnen* und klicken auf *Schließen*.

Klicken Sie im neuen Fenster auf *Regel hinzufügen*. Wählen Sie *Ansprüche mithilfe einer benutzerdefinierten Regel senden* aus und klicken Sie auf *Weiter*. Weisen Sie der Regel einen beliebigen Namen zu und tragen Sie bei der Regel als Text die folgenden Daten ein:

```
c:[ ]
=> issue(claim = c);
```

Klicken Sie auf *Fertig stellen* und dann auf *OK*.

Workplace Join mit Windows 8.1

Damit Sie auf Ressourcen im Netzwerk zugreifen können, verbinden Sie Ihren Windows 8.1-PC mit dem Firmennetzwerk. Es ist allerdings wichtig, dass der PC selbst kein Mitglied der Domäne ist, da Workplace Join ansonsten keinen Sinn ergibt. Außerdem müssen Sie sicherstellen, dass der PC der Zertifizierungsstelle vertraut, die Sie für den Vorgang genutzt haben. Dazu importieren Sie das Zer-

tifikat der Zertifizierungsstelle in den Speicher der Stammzertifizierungsstellen auf dem Server (siehe Kapitel 27 und 30).

Rufen Sie dann mit ⊞+C die Charms-Leiste auf und wechseln Sie zu *Einstellungen/PC-Einstellungen ändern/Netzwerk/Arbeitsplatz*. Geben Sie den Benutzerprinzipalnamen (User Principal Name, UPN) Ihres Kontos ein, zum Beispiel *mailto:joost@contoso.int*. Melden Sie sich dann am Netzwerk an. Sie erhalten daraufhin die Meldung, dass die Verbindung funktioniert. Rufen Sie die Webanwendung auf, müssen Sie sich zunächst anmelden. Wenn Sie den Browser schließen und ihn anschließend erneut starten, können Sie auch ohne Anmeldung auf den Browser zugreifen.

Funktioniert bei Ihnen die Verbindung nicht, haben Sie verschiedene Lösungsansätze. Diese werden auf folgenden Seiten beschrieben:

http://social.technet.microsoft.com/Forums/windowsserver/en-US/7c130c78-179c-4325-9377-564c47a2e4f0/error-in-adfs-during-workplace-join [Ms179-K42-02]

und

http://social.technet.microsoft.com/Forums/windows/en-US/6c401051-68d6-449c-87aa-2a2a468161e2/how-to-use-workplace-join?forum=w81previtpro [Ms179-K42-03]

Workplace Join mit iPhone/iPad

Um mit iPhones und iPads auf interne Webanwendungen zugreifen zu können, rufen Sie die Adresse *https://<AD FS-Server>/enrollmentserver/otaprofile* auf. Lassen Sie das Profil installieren und melden Sie sich mit Ihrem Benutzernamen und Kennwort an.

Zusammenfassung

In diesem Kapitel haben wir Ihnen anhand einer Beispielumgebung erklärt, wie Sie die Active Directory-Verbunddienste einrichten und Windows 8.1 oder iPhones/iPads an Ihr Netzwerk anbinden. Mit der Beispielumgebung haben Sie einen Einblick in die Möglichkeiten der neuen Technologien in Windows 8.1 und Windows Server 2012 R2 erhalten.

Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

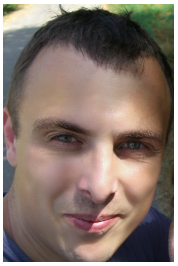
V

W

X

Z

Der Autor



Thomas Joos

ist selbstständiger IT-Consultant und seit 20 Jahren in der IT-Branche tätig. Er schreibt Fachbücher und berät Unternehmen im Mittelstands- und Enterprise-Bereich in den Themenfeldern Active Directory, Exchange Server und IT-Sicherheit. Durch seinen praxisorientierten und verständlichen Schreibstil sind seine Fachbücher für viele IT-Spezialisten eine wichtige Informationsquelle geworden. Neben vielen erfolgreichen Büchern schreibt er für zahlreiche IT-Publikationen wie z.B. *c't*, *iX*, *IT Administrator* und *tecchannel.de*.

Thomas Joos nimmt auch ständig mehrstündige Videotrainings zu Windows Server 2012/2012 R2, Windows Server 2012 R2 Essentials, Hyper-V, Windows 8.1, Exchange Server 2013 und vieles mehr auf. Einige Videos aus den Trainings stehen kostenlos zur Verfügung. Die kompletten Trainings können Sie günstig abonnieren oder als DVD kaufen. Informationen dazu finden Sie auf dem Blog des Autors: *http://thomasjoos.wordpress.com/*.