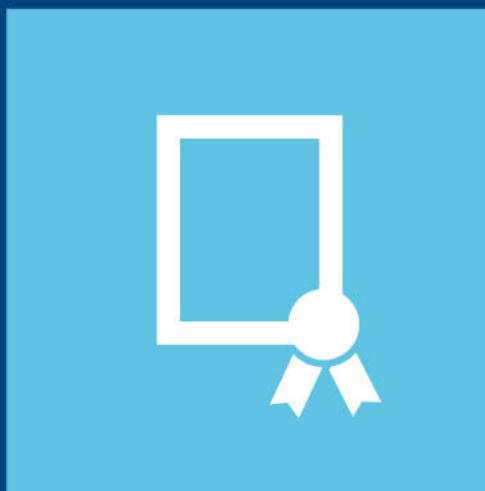


Installieren und Konfigurieren von Windows Server 2012



70-410

Original
Microsoft
Prüfungs-
Training

Installieren und Konfigurieren von Windows Server 2012

Original Microsoft Prüfungstraining

70-410

Microsoft
Press

Das deutsche Buch ist die Übersetzung von:

Craig Zacker: Exam Ref 70-410: Installing and Configuring Windows Server 2012
Veröffentlicht von Microsoft Press, A Division of Microsoft Corporation,
One Microsoft Way, Redmond, Washington 98052-6399, USA
Copyright 2012 Craig Zacker

Das in diesem Buch enthaltene Programmmaterial ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autor, Übersetzer und der Verlag übernehmen folglich keine Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programmmaterials oder Teilen davon entsteht.

Das Werk einschließlich aller Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die in den Beispielen verwendeten Namen von Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen sowie E-Mail-Adressen und Logos sind frei erfunden, soweit nichts anderes angegeben ist. Jede Ähnlichkeit mit tatsächlichen Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen, E-Mail-Adressen und Logos ist rein zufällig.

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
15 14 13

Druck-ISBN 978-3-86645-040-0
PDF-ISBN 978-3-8483-3032-4
EPUB-ISBN 978-3-8483-0166-9
MOBI-ISBN 978-3-8483-1168-2

© 2013 O'Reilly Verlag GmbH & Co. KG
Balthasarstr. 81, 50670 Köln
Alle Rechte vorbehalten

Übertragung ins Deutsche: Frank Langenau, Chemnitz
Lektorat: Florian Helmchen, florian@oreilly.de
Korrektorat: Dorothee Klein, Siegen
Satz: Gerhard Alfes, mediaService, Siegen (www.mediaservice.tv)
Umschlaggestaltung: HommerDesign GmbH, Haar (www.HommerDesign.com)
Herstellung, Druck und Bindung: Kösel, Krugzell (www.KoeselBuch.de)

Inhaltsverzeichnis

Einleitung	9
Microsoft-Zertifizierungen	10
Errata und Support für dieses Buch	10
Bleiben Sie am Ball	11
Auf die Prüfung vorbereiten	11
Kapitel 1 Server installieren und konfigurieren	13
Prüfungsziel 1.1: Server installieren	14
Eine Serverinstallation planen	14
Installationsoptionen auswählen	18
Server aktualisieren	25
Prüfungszielzusammenfassung	30
Lernzielkontrolle	30
Prüfungsziel 1.2: Server konfigurieren	32
Aufgaben nach der Installation	32
Server-Manager verwenden	41
Dienste konfigurieren	51
Serververwaltung delegieren	52
Prüfungszielzusammenfassung	54
Lernzielkontrolle	54
Prüfungsziel 1.3: Lokalen Speicher konfigurieren	56
Serverspeicher planen	56
Windows-Datenträgereinstellungen	58
Mit Datenträgern arbeiten	62
Prüfungszielzusammenfassung	80
Lernzielkontrolle	81
Kapitelzusammenfassung	82
Antworten	82
Kapitel 2 Serverrollen und -features konfigurieren	89
Prüfungsziel 2.1: Datei- und Freigabezugriff konfigurieren	90
Ordnerfreigaben erstellen	90
Berechtigungen zuweisen	96

Volumeschattenkopien konfigurieren	106
Datenträgerkontingente konfigurieren	107
Prüfungszielzusammenfassung	109
Lernzielkontrolle	109
Prüfungsziel 2.2: Druck- und Dokumentdienste konfigurieren	112
Einen Druckserver bereitstellen	112
Einen Drucker freigeben	118
Dokumente verwalten	123
Drucker verwalten	124
Die Rolle Druck- und Dokumentdienste verwenden	126
Prüfungszielzusammenfassung	132
Lernzielkontrolle	132
Prüfungsziel 2.3: Server für die Remoteverwaltung konfigurieren	135
Remoteverwaltung mit dem Server-Manager	135
Remoteserver-Verwaltungstools verwenden	143
Mit Remoteservern arbeiten	144
Prüfungszielzusammenfassung	145
Prüfungszielkontrolle	145
Antworten	147
 Kapitel 3 Hyper-V konfigurieren	 153
Prüfungsziel 3.1: Einstellungen für den virtuellen Computer erstellen und konfigurieren	154
Virtualisierungsarchitekturen	154
Hyper-V-Implementierungen	156
Hyper-V installieren	158
Hyper-V-Manager verwenden	161
Ressourcenmessung konfigurieren	175
Prüfungszielzusammenfassung	175
Lernzielkontrolle	176
Prüfungsziel 3.2: Speicher des virtuellen Computers erstellen und konfigurieren	178
Formate virtueller Festplatten	178
Virtuelle Festplatten erstellen	179
Pass-Through-Datenträger konfigurieren	186
Virtuelle Festplatten modifizieren	187
Snapshots erstellen	189
Mit einem SAN verbinden	190
Prüfungszielzusammenfassung	194
Lernzielkontrolle	195
Prüfungsziel 3.3: Virtuelle Netzwerke erstellen und konfigurieren	197
Virtuelle Switches erstellen	197
Virtuelle Netzwerkadapter erstellen	204
Konfigurationen virtueller Netzwerke erstellen	209
Prüfungszielzusammenfassung	210

Lernzielkontrolle	211
Antworten	212
 Kapitel 4 Kernnetzwerkdienste bereitstellen und konfigurieren	217
Prüfungsziel 4.1: IPv4- und IPv6-Adressierung	218
IPv4-Adressierung	218
IPv6-Adressierung	226
Einen IP-Übergang planen	231
Prüfungszielzusammenfassung	235
Lernzielkontrolle	235
Prüfungsziel 4.2: Den DHCP-Dienst bereitstellen und konfigurieren	237
DHCP	237
Einen DHCP-Server bereitstellen	243
Einen DHCP-Relay-Agenten bereitstellen	248
Prüfungszielzusammenfassung	251
Lernzielkontrolle	251
Prüfungsziel 4.3: Den DNS-Dienst bereitstellen und konfigurieren	253
Die DNS-Architektur	253
Einen DNS-Server bereitstellen	262
Lernzielzusammenfassung	270
Lernzielkontrolle	271
Antworten	272
 Kapitel 5 Active Directory installieren und verwalten	279
Prüfungsziel 5.1: Domänencontroller installieren	280
Active Directory-Domänendienste bereitstellen	280
Prüfungszielzusammenfassung	296
Lernzielkontrolle	297
Prüfungsziel 5.2: Active Directory-Benutzer und -Computer erstellen und verwalten	299
Benutzerobjekte erstellen	299
Active Directory-Objekte verwalten	313
Prüfungszielzusammenfassung	318
Lernzielkontrolle	319
Prüfungsziel 5.3: Active Directory-Gruppen und Organisationseinheiten erstellen und verwalten	321
Organisationseinheiten erstellen	322
Mit Gruppen arbeiten	325
Prüfungszielzusammenfassung	335
Lernzielkontrolle	336
Antworten	337

Kapitel 6 Gruppenrichtlinien erstellen und verwalten	343
Prüfungsziel 6.1: Gruppenrichtlinienobjekte (GPOs) erstellen	344
Gruppenrichtlinienobjekte	344
Einen zentralen Speicher konfigurieren	345
Die Konsole Gruppenrichtlinienverwaltung	346
Starter-Gruppenrichtlinienobjekte verwalten	349
Gruppenrichtlinieneinstellungen konfigurieren	350
Mehrfahe lokale Gruppenrichtlinienobjekte erstellen	351
Prüfungszielzusammenfassung	353
Lernzielkontrolle	354
Prüfungsziel 6.2: Sicherheitsrichtlinien konfigurieren	356
Lokale Richtlinien definieren	356
Benutzerkontensteuerung konfigurieren	369
Prüfungszielzusammenfassung	372
Lernzielkontrolle	373
Prüfungsziel 6.3: Richtlinien für Anwendungseinschränkungen konfigurieren	376
Richtlinien für Softwareeinschränkung	376
AppLocker verwenden	383
Prüfungszielzusammenfassung	386
Lernzielkontrolle	387
Prüfungsziel 6.4: Windows-Firewall konfigurieren	389
Windows-Firealleinstellungen	389
Mit der Windows-Firewall arbeiten	390
Die Windows-Firewall-Systemsteuerung	391
Die Konsole Windows-Firewall mit erweiterter Sicherheit	395
Prüfungszielzusammenfassung	401
Prüfungszielkontrolle	401
Antworten	403
Index	409
Der Autor	423

Einleitung

Die meisten Bücher vermitteln die grundlegenden Konzepte anhand in sich abgeschlossener Detailaufgaben. Demgegenüber betrachtet dieses Buch genau wie die Microsoft-Zertifizierungsprüfung 70-410 das Thema von einer höheren Warte aus. Es baut dabei auf Ihren vorhandenen Kenntnissen der einfachen Microsoft Windows-Systemadministration auf und erweitert Ihr Wissen in Richtung komplexerer Serverkonzepte, die für Windows Server 2012 erforderlich sind.

Kandidaten für diese Prüfung sind IT-Profis, die Kenntnisse und Erfahrungen im Betriebssystem Windows Server 2012 mitbringen und die erforderlichen Fähigkeiten und Kenntnisse für die Implementierung der Kerndienste einer Windows Server 2012-Infrastruktur nachweisen möchten.

Die Prüfung 70-410 ist die erste in einer Reihe von drei Prüfungen, die die erforderlichen Fähigkeiten und Kenntnisse bewerten, um eine Windows Server 2012-Kerninfrastruktur in eine vorhandene Unternehmensumgebung zu implementieren. Demzufolge behandelt dieses Buch die anfängliche Implementierung und Konfiguration der Windows Server 2012-Kerndienste wie zum Beispiel Active Directory und die Netzwerkdienste. Zusammen mit den beiden anderen Büchern (die sich mit den Prüfungen 70-411 und 70-412 beschäftigen) veranschaulicht dieses Buch die Fähigkeiten und Kenntnisse, die für das Implementieren, Verwalten, Warten und Bereitstellen von Diensten und der Infrastruktur in einer Windows Server 2012-Umgebung benötigt werden.

Das Buch deckt zwar die Themen jedes Prüfungsziels ab, kann aber nicht jede Prüfungsfrage behandeln. Denn nur das Microsoft Learning-Team hat Zugriff auf die Prüfungsfragen selbst und Microsoft ergänzt die Prüfung regelmäßig um neue Fragen, sodass es nicht möglich ist, mit den konkreten Fragen aufzuwarten. Betrachten Sie dieses Buch am besten als Ergänzung zu Ihrer einschlägigen Praxiserfahrung und anderen Schulungsunterlagen. Wenn Sie in diesem Buch auf ein Thema treffen, mit dem Sie sich nicht vollständig vertraut fühlen, sollten Sie sich über die im Text angegebenen Links weiterführende Informationen beschaffen und die Zeit nehmen, das Thema zu recherchieren und zu vertiefen. Auf MSDN und TechNet sowie in Blogs und Foren stehen Ihnen umfangreiche zusätzliche Informationen zur Verfügung.

Microsoft-Zertifizierungen

Microsoft-Zertifizierungen heben Sie aus der Masse heraus, da Sie damit eine breite Palette von Fertigkeiten und Erfahrung mit aktuellen Microsoft-Produkten und -Technologien nachweisen können. Die Prüfungen und entsprechenden Zertifizierungen wurden entwickelt, um Ihre Kompetenzen zu bewerten, wenn Sie Lösungen mit Microsoft-Produkten und -Technologien entwerfen und entwickeln bzw. implementieren und unterstützen. Das gilt bei lokalen Bereitstellungen (On-Premise) wie auch in der Cloud. Eine Zertifizierung bringt zahlreiche Vorteile für Bewerber, Arbeitgeber und Organisationen mit sich.



Weitere Informationen Alle Microsoft-Zertifizierungen

Weitere Informationen über die Microsoft-Zertifizierungen (einschließlich einer vollständigen Liste der Zertifizierungen, in englischer Sprache) finden Sie unter <http://www.microsoft.com/learning/en/us/certification-overview.aspx>.

Errata und Support für dieses Buch

Wir haben uns sehr um die Richtigkeit der in diesem Buch enthaltenen Informationen bemüht. Fehler, die seit der Veröffentlichung dieses englischen Buchs bekannt geworden sind, werden auf unserer Microsoft Press-Website bei oreilly.com (in englischer Sprache) aufgelistet:

<http://go.microsoft.com/fwlink/?LinkId=272595>

Sollten Sie einen Fehler finden, der noch nicht aufgeführt ist, würden wir uns freuen, wenn Sie uns auf dieser Seite darüber informieren (in englischer Sprache).

Mit Anmerkungen, Fragen oder Verbesserungsvorschlägen zu diesem Buch können Sie sich an Microsoft Press Deutschland wenden:

Per E-Mail:

mspressde@oreilly.de

Per Post:

Microsoft Press
Betreift: Prüfungstraining 70-410
Konrad-Zuse-Straße 1
85716 Unterschleißheim

Weitere Supportinformationen zu diesem Buch finden Sie gegebenenfalls auf der Support-website von Microsoft Press Deutschland unter <http://www.microsoft-press.de/support/9783866450400>.

Bitte beachten Sie, dass über unsere E-Mail-Adresse kein Software-Support angeboten wird.

Für Supportinformationen bezüglich der Softwareprodukte besuchen Sie die Microsoft-Website <http://support.microsoft.com>.

Bleiben Sie am Ball

Falls Sie News, Updates usw. von Microsoft Press erhalten möchten, wir sind auf Twitter:

http://twitter.com/mspress_de

Auf die Prüfung vorbereiten

Microsoft-Zertifizierungsprüfungen sind eine hervorragende Möglichkeit, um Ihren Lebenslauf aufzuwerten und die Welt von Ihrer Fachkompetenz wissen zu lassen. Zertifizierungsprüfungen bewerten Ihre berufliche Erfahrung und Ihre Produktkenntnisse. Auch wenn es keinen Ersatz für Berufserfahrungen gibt, kann Ihnen die Vorbereitung über Schulungen und praktische Einsätze helfen, sich auf die Prüfung vorzubereiten. Wir empfehlen, dass Sie Ihre Prüfungsvorbereitung abrunden, indem Sie eine Kombination von verfügbaren Schulungsunterlagen und Kursen nutzen. Zum Beispiel könnten Sie sich mithilfe des Training Kits und eines anderen Studienführers zu Hause vorbereiten und einen Microsoft Official Curriculum (MOC)-Kurs belegen, bei dem Sie die Atmosphäre im Schulungsraum kennenlernen. Wählen Sie die Kombination, die Ihrer Meinung nach am besten für Sie geeignet ist.

K A P I T E L 1

Server installieren und konfigurieren

Neue Server in einem Netzwerk zu installieren, ist keine Aufgabe, die nebenbei zu bewältigen wäre – Sie müssen die Installation im Voraus sehr sorgfältig planen. So haben Sie unter anderem zu entscheiden, welche Edition des Betriebssystems zu installieren ist, ob Sie die vollständige grafische Benutzeroberfläche (Graphical User Interface, GUI) oder die Server Core-Option installieren und welche Rollen Sie auf dem Server implementieren wollen. Wenn Sie Windows Server 2012 erstmals installieren, steht möglicherweise auch die Entscheidung an, ob der Server in ein Produktionsnetz einzubinden ist oder in einem Testnetz installiert werden soll.

Dieses Kapitel befasst sich mit der Installation von Windows Server 2012 – entweder als Neuinstallation oder als Server-Upgrade – und den Aufgaben für die Serverkonfiguration, die Sie unmittelbar im Anschluss an die Installation ausführen müssen. Am Ende behandelt es die Konfiguration verschiedener Arten von Festplattentechniken für den lokalen Speicher sowie die Bereitstellung von Rollen für Server im gesamten Netzwerk.

Prüfungsziele in diesem Kapitel:

- Prüfungsziel 1.1: Server installieren 14
 - Prüfungsziel 1.2: Server konfigurieren 32
 - Prüfungsziel 1.3: Lokalen Speicher konfigurieren. 56
-



Wichtig Haben Sie Seite 9 gelesen?

Dort finden Sie wichtige Informationen in Bezug auf die erforderlichen Fertigkeiten für das Bestehen der Prüfung.



Tipp Manche Prüfungsfragen sind in einem Multiple-Choice-Format gehalten, wobei die Antworten entweder richtig oder falsch sind. Wenn Sie in der Prüfung auf eine Option treffen, bei der zwei Antworten richtig zu sein scheinen, Sie aber nur eine Antwort auswählen dürfen, haben Sie höchstwahrscheinlich einen Hinweis im Fragetext übersehen, der es Ihnen erlauben würde, eine dieser Antworten zu streichen. Der Autor der Prüfungsfrage muss nämlich nicht nur gute Gründe anführen, warum eine Antwort richtig ist, sondern auch Gründe, warum die anderen Antworten unzutreffend sind. Es kann zwar passieren, dass eine schlecht formulierte Frage beim Korrekturlesen und Gegenlesen durchgerutscht ist, doch ist es wahrscheinlicher, dass Sie in einer angespannten Prüfungssituation ein entscheidendes Element übersehen haben und Sie deshalb mehrere Antworten als richtig einstufen.

Prüfungsziel 1.1: Server installieren

Die Installation ist ein Schlüsselthema und wurde in früheren Windows Server-Prüfungen ausgiebig getestet. Es gibt keinen Grund zu glauben, dass die Prüfung 70-410 anders ist. Dieses Lernziel beschäftigt sich mit der Planung einer Windows Server 2012-Installation. Dabei geht es um die Anforderungen einer Vorinstallation und wie Sie Ihre Installationshardware vorbereiten können. Außerdem werden die Serverrollen betrachtet, die Sie während der Installation implementieren können.

Das Lernziel führt Sie durch eine Neuinstallation von Windows Server Core 2012 und beschreibt, wie Sie mithilfe der Funktion *Features bei Bedarf* Ressourcen optimieren, indem alle Dateien entfernt werden, die zu einer von Ihnen zum Löschen ausgewählten Serverrolle oder einem Feature gehören. Außerdem betrachtet das Lernziel die Optionen für das Upgrade eines Windows Server 2008- oder Windows Server 2008 R2-Servers auf Windows Server 2012 und die Migration von Rollen von einem vorhandenen auf einen neuen Server.

Dieses Prüfungsziel zeigt, wie Sie

- eine Serverinstallation planen
 - Serverrollen planen
 - ein Server-Upgrade planen
 - Server Core installieren
 - die Ressourcennutzung mithilfe von *Features bei Bedarf* optimieren
 - Rollen von vorherigen Version von Windows Server migrieren
-

Eine Serverinstallation planen

In früheren Versionen von Windows Server konnte die Installationsplanung zu einer komplexen Aufgabe werden. Dabei mussten Sie von vornherein entscheiden, welche Edition des Betriebssystems zu installieren ist, ob Sie die 32-Bit- oder 64-Bit-Version installieren und

ob Sie eine Server Core-Installation durchführen oder die vollständige GUI verwenden. Alle diese Entscheidungen haben sich auf die Hardwareanforderungen ausgewirkt, zudem waren alle Entscheidungen nicht unwiderruflich. Um die Edition, die Plattform oder die Benutzeroberfläche zu ändern, müssen Sie den Server von Anfang an neu installieren.

Bei Windows Server 2012 sind die Optionen erheblich reduziert und damit auch die Installationsentscheidungen. Von Windows Server 2012 gibt es keine 32-Bit-Version, es ist lediglich ein 64-Bit-Betriebssystem verfügbar. Dies spiegelt die Tatsache wider, dass die wesentlichen Anwendungen heutzutage auf 64 Bit ausgelegt sind und dass moderne Serverkonfigurationen normalerweise auf Hardware unterstützt wird, die 64 Bit verlangt. Jetzt haben Sie lediglich die Wahl unter vier Windows Server 2012-Editionen, gegenüber sechs in Windows Server 2008 R2. Die Optionen für Server Core und vollständige Benutzeroberfläche bleiben bestehen, dazu kommt eine dritte Option namens *minimale Serverschnittstelle*. Allerdings ist es jetzt möglich, zwischen diesen Optionen zu wechseln, ohne das Betriebssystem erneut installieren zu müssen.

Eine Windows Server 2012-Edition auswählen

Microsoft veröffentlicht seine Betriebssysteme in mehreren Editionen, die Konsumenten verschiedene Preissegmente und Featuregruppen bieten. Bei der Planung einer Serverbereitstellung sollten Sie die Betriebssystem-Edition basierend auf mehreren Faktoren auswählen, unter anderem folgenden:

- Die Rollen, die Sie auf den Servern ausführen wollen
- Die Virtualisierungsstrategie, die Sie implementieren möchten
- Die vorgesehene Lizenzierungsstrategie

Gegenüber Windows Server 2008 hat Microsoft das Auswählen einer Serveredition vereinfacht, indem die verfügbaren Produkte verringert wurden. Wie bei Windows Server 2008 R2 setzt Windows Server 2012 eine 64-Bit-Prozessorarchitektur voraus. Die 32-Bit-Versionen sind komplett verschwunden und das erste Mal seit dem Windows NT Server 4.0-Release gibt es keinen Build, der Itanium-Prozessoren unterstützt. Damit bleiben die folgenden Kerneditionen von Windows Server 2012 übrig:

- **Windows Server 2012 Datacenter** Diese Edition ist für große und leistungsstarke Server mit bis zu 64 Prozessoren und Fehlertoleranzfunktionen wie zum Beispiel Unterstützung für das Hot-Add von Prozessoren konzipiert. Deshalb ist diese Edition nur über das Volumenlizenzierungsprogramm von Microsoft und von OEMs (Original Equipment Manufacturers) im Bundle mit einem Server erhältlich.
- **Windows Server 2012 Standard** Diese Edition umfasst sämtliche Windows Server 2012-Features und unterscheidet sich von der Datacenter-Edition nur in der Anzahl der VM (Virtual Machine)-Instanzen, die gemäß Lizenz erlaubt sind
- **Windows Server 2012 Essentials** Diese Edition umfasst nahezu alle Features der Standard- und Datacenter-Editionen, bis auf Server Core, Hyper-V und Active Directory Federation Services. Die Edition ist auf eine physische oder virtuelle Serverinstanz und maximal 25 Benutzer beschränkt.

- **Windows Server 2012 Foundation** Diese Edition ist eine reduzierte Version des Betriebssystems, konzipiert für kleine Unternehmen, die nur grundlegende Features wie zum Beispiel Datei- und Druckdienste und Anwendungsunterstützung benötigen. Die Edition umfasst keine Virtualisierungsrechte und ist auf 15 Nutzer beschränkt.

Die Preise der verschiedenen Editionen sind entsprechend ihren Fähigkeiten gestaltet. Administratoren, die Serverbereitstellungen planen, sind natürlich bestrebt, die preisgünstigste Version auszuwählen, die allen ihren Anforderungen genügt. Die folgenden Abschnitte untersuchen die wichtigsten Unterschiede zwischen den Windows Server 2012-Editionen.

Serverrollen unterstützen

Windows Server 2012 umfasst vordefinierte Kombinationen von Diensten – sogenannten Rollen –, die gebräuchliche Serverfunktionen implementieren. Computer, die das Windows Server 2012-Betriebssystem ausführen, können ein breites Spektrum von Aufgaben erledigen, und zwar sowohl mit der zum Produkt gehörenden Software als auch mit Anwendungen von Drittanbietern. Die von Windows Server 2012 für Netzwerkclients ausgeführten Aktivitäten werden als *Rollen* bezeichnet. Nachdem Sie das Windows Server 2012-Betriebssystem installiert haben, arbeiten Sie mit Server-Manager oder per Windows PowerShell, um dem betreffenden Computer eine oder mehrere Rollen zuzuweisen.

Einige Windows Server 2012-Editionen beinhalten sämtliche Rollen, andere dagegen nur einen Teil dieser Rollen. Die Auswahl der passenden Windows Server-Edition hatte immer damit zu tun, die Rollen, die der Computer ausführen soll, im Voraus zu ermitteln. Einst war das ein relativ einfacher Ablauf. Sie haben Ihre Serverbereitstellungen geplant, indem Sie entschieden haben, welche Server als Domänencontroller fungieren, welche als Webserver usw. Nachdem Sie diese Entscheidungen getroffen hatten, waren Sie praktisch fertig, da Serverrollen größtenteils statischen Charakter hatten.

Mit dem zunehmenden Fokus auf Virtualisierung in Windows Server 2012 sind jedoch immer mehr Administratoren gezwungen, nicht nur die Rollen zu betrachten, die ein Server zum Zeitpunkt der Bereitstellung ausführen soll, sondern auch, welche Rollen zukünftig infrage kommen.

Mithilfe von virtualisierten Servern können Sie die Serverstrategie Ihres Netzwerks nach Belieben modifizieren, um sie an geänderte Belastungen und Geschäftsanforderungen oder nicht vorhersehbare Umstände anzupassen. Demzufolge müssen Sie bei den Rollen, die ein Server ausführen soll, auch die mögliche Expansion Ihres Unternehmens und eventuelle Notfallsituationen einkalkulieren.

Servervirtualisierung unterstützen

Die Windows Server 2012-Editionen Datacenter und Standard beinhalten die Unterstützung für Hyper-V, unterscheiden sich aber in der Anzahl der VMs, die entsprechend ihrer Lizenzen erlaubt sind. Jede ausgeführte Instanz des Windows Server 2012-Betriebssystems wird als *physische Betriebssystemumgebung* (Physical Operating System Environment, POSE) oder *virtuelle Betriebssystemumgebung* (Virtual Operating System Environment, VOSE) klassifiziert. Wenn Sie eine Windows Server 2012-Lizenz kaufen, können Sie wie gehabt eine

POSE-Installation des Betriebssystems durchführen. Nachdem Sie die Hyper-V-Rolle installiert haben, können Sie VMs erzeugen und auf ihnen VOSE-Installationen durchführen. Die Anzahl der entsprechend Ihrer Lizenz erlaubten VOSE-Installationen hängt von der gekauften Edition ab, wie Tabelle 1.1 zeigt.

Tabelle 1.1 Physische und virtuelle Instanzen, die von den Windows Server 2012-Editionen unterstützt werden

Edition	POSE-Instanzen	VOSE-Instanzen
Datacenter	1	Unbeschränkt
Standard	1	2
Essentials	1 (POSE oder VOSE)	1 (POSE oder VOSE)
Foundation	1	0



Hinweis Lizenzbegrenzungen sind keine Softwarebeschränkungen

Die in Tabelle 1.1 angegebenen Beschränkungen beziehen sich auf die Lizenz, nicht auf die Software. So können Sie beispielsweise mehr als zwei virtuelle Computer für eine Kopie von Windows Server 2012 Standard anlegen, müssen dafür aber zusätzliche Lizizenzen erwerben.

Server-Lizenzierung

Microsoft bietet mehrere unterschiedliche Vertriebskanäle für Windows Server 2012-Lizenzen an, wobei nicht alle Editionen über sämtliche Kanäle verfügbar sind. Zur Lizenzierung von Windows Server 2012 gehört der Erwerb von Lizizenzen sowohl für Server als auch für Clients und es gibt für jede Form viele Optionen.

Wenn Sie bereits eine Lizenzvereinbarung mit Microsoft abgeschlossen haben, kennen Sie sicherlich die Server-Editionen, die über diese Vereinbarung zur Verfügung stehen. Andernfalls sollten Sie sich mit den verfügbaren Lizenzierungsoptionen vertraut machen, bevor Sie eine Server-Edition auswählen. Tabelle 1.2 listet die Vertriebskanäle auf, über die Sie die jeweiligen Windows Server 2012-Editionen kaufen können.

Tabelle 1.2 Verfügbarkeit der Windows Server-Vertriebskanäle nach Edition

	Einzelhandel	Volumenlizenz	OEM
Datacenter	Nein	Ja	Ja
Standard	Ja	Ja	Ja
Essentials	Ja	Ja	Ja
Foundation	Nein	Nein	Ja

Installationsanforderungen

Wenn Ihr Computer weniger als die folgenden Hardwarespezifikationen besitzt, lässt sich Windows Server 2012 nicht ordnungsgemäß (oder überhaupt nicht) installieren:

- 64-Bit-Prozessor mit 1,4-GHz
- 512 MB RAM
- 32 GB freier Festplattenplatz
- DVD-Laufwerk
- Super VGA (800 x 600) oder Monitor mit höherer Auflösung
- Tastatur und Maus (oder anderes kompatibles Zeigegerät)
- Internetzugang

Für den verfügbaren Festplattenplatz sind 32 GB als absolutes Minimum anzusehen. Auf der Systempartition ist zusätzlicher Platz erforderlich, wenn Sie das System über ein Netzwerk installieren oder wenn der Computer mit mehr als 16 GB RAM ausgestattet ist. Der zusätzliche Festplattenplatz ist für Auslagerungs-, Ruhezustands- und Sicherungsdateien erforderlich. In der Praxis dürften Sie kaum mit einem Computer zu tun haben, auf dem 512 MB RAM installiert sind und der lediglich 32 GB Festplattenplatz frei hat. Falls doch, sollten Sie mehr Festplattenplatz bereitstellen oder in zusätzliche Speicherhardware investieren.

Da Microsoft verstärkt auf Virtualisierung und Cloud-Computing in seinen Serverprodukten orientiert, wurden die maximalen Hardwarekonfigurationen für Windows Server 2012 deutlich erhöht. Tabelle 1.3 listet diese Maximalwerte auf.

Tabelle 1.3 Maximale Hardwarekonfigurationen in Windows Server-Versionen

	Windows Server 2012	Windows Server 2008 R2
Logische Prozessoren	640	256
RAM	4 TB	2 TB
Failover-Clusterknoten	64	16

Installationsoptionen auswählen

Heutzutage verwenden viele Unternehmensnetzwerke Server, die für eine bestimmte Rolle ausgelegt sind. Wenn ein Server lediglich eine einzige Rolle ausführt, sind dann überhaupt die vielen anderen Prozesse sinnvoll, die auf dem Server laufen und kaum etwas zu dieser Rolle beitragen?

Viele IT-Administratoren haben sich mittlerweile so an grafische Benutzeroberflächen (Graphical User Interfaces, GUIs) gewöhnt, dass sie sich gar nicht vorstellen können, dass es jemals etwas anderes gegeben hat, um Computer zu bedienen. Als 1993 die erste Version von Windows NT Server erschien, gab es viele Beschwerden über die Verschwendungen von Serverressourcen für grafische Anzeigen und andere Elemente, die man als unnötig erachtete.

Bis dahin waren Server-Displays üblicherweise spartanisch konzipiert, zeichenbasiert und monochrom. Tatsächlich hatten viele Server keine Display-Hardware und stützten sich stattdessen auf textbasierte Tools zur Remoteverwaltung wie zum Beispiel Telnet.

Server Core verwenden

Windows Server 2012 umfasst eine Installationsoption, die diese alten Klagen berücksichtigt. Wenn Sie die Installationsoption *Server Core* auswählen, erhalten Sie eine abgespeckte Version des Betriebssystems. Es gibt kein Start-Menü, keine Desktop-Explorer-Shell, keine Microsoft Management Console (MMC) und praktisch keine grafischen Anwendungen. Beim Starten des Computers sehen Sie lediglich ein einzelnes Fenster mit einer Eingabeaufforderung, wie es Abbildung 1.1 zeigt.



Abbildung 1.1 Die Standardoberfläche von Server Core



Hinweis Was ist Server Core?

Server Core ist weder ein separates Produkt noch eine Edition. Es handelt sich um eine Installationsoption in den Editionen Windows Server 2012 Standard und Datacenter.

Server mit Server Core zu betreiben bietet unter anderem folgende Vorteile:

- **Hardwareressourcenschonung** Server Core eliminiert einige der speicher- und prozessorintensivsten Elemente des Windows Server 2012-Betriebssystems. Somit steht die Systemhardware vorrangig für die Ausführung wichtiger Dienste zur Verfügung.
- **Geringerer Bedarf an Festplattenplatz** Server Core benötigt weniger Festplattenplatz für die installierten Elemente des Betriebssystems und weniger Platz für die Auslagerungsdatei. Dadurch ergibt sich eine maximale Nutzung der Speicherressourcen des Servers.
- **Niedrigere Patch-Häufigkeit** Die grafischen Elemente von Windows Server 2012 werden am häufigsten aktualisiert, sodass die Ausführung von Server Core die Anzahl der

Updates verringert, die Administratoren anwenden müssen. Weniger Updates bedeuten auch weniger Neustarts und geringere Ausfallzeiten des Servers.

- **Kleinere Angriffsfläche** Je weniger Software auf einem Computer läuft, desto weniger Eingangstüren gibt es, die Angreifer nutzen können. Server Core reduziert die potenzielle Angriffsfläche, die das Betriebssystem Angreifern bietet, und erhöht damit die Sicherheit insgesamt.

Als Microsoft die Option *Server Core-Installation* in Windows Server 2008 eingeführt hat, war dies ein faszinierendes Konzept, von dem allerdings nur wenige Administratoren Gebrauch machten. Das lag hauptsächlich daran, dass die meisten Serveradministratoren nicht genügend sattelfest in der Befehlszeiloberfläche waren, um einen Windows-Server ohne GUI zu verwalten.

In Windows Server 2008 und Windows Server 2008 R2 war die Entscheidung, das Betriebssystems mit *Server Core* zu installieren, unwiderruflich. Hatte man das Betriebssystem einmal mit *Server Core* installiert, gab es – abgesehen von einer kompletten Neuinstallation – keinen Weg mehr, um zur GUI zurückzukehren. In Windows Server 2012 hat sich das alles geändert. Jetzt können Sie nach Belieben mithilfe der Windows PowerShell-Befehle einen Server von der Option *Server Core-Installation* zur Option *Server mit einer grafischen Benutzeroberfläche* und wieder zurück konfigurieren.



Weitere Informationen Hin und zurück

Weitere Informationen zum Konvertieren der Option *Server Core-Installation* zur Option *Server mit einer grafischen Benutzeroberfläche* und wieder zurück finden Sie unter »Prüfungsziel 1.2: Server konfigurieren« später in diesem Kapitel.

Wenn also Administratoren zunächst eine grafische Oberfläche bevorzugen, können sie Windows Server 2012 mit dieser Option installieren, den Server mithilfe der vertrauten grafischen Tools konfigurieren und dann später zur Option *Server Core-Installation* wechseln, um von den weiter oben aufgeführten Vorzügen zu profitieren.

Server Core ist die Standardeinstellung

In Windows Server 2012 ist die Option *Server Core-Installation* die Standardeinstellung, und zwar nicht nur deshalb, weil man nach der Installation zur anderen Option wechseln kann. Microsoft versucht in Windows Server 2012, die grundsätzliche Art und Weise zu beeinflussen, wie Administratoren mit ihren Servern arbeiten. Die Option Server Core ist jetzt die Standardinstallationsoption wegen der neuen Art und Weise der Serververwaltung. Dahinter steckt die Absicht, dass Administratoren, wenn überhaupt, nur noch selten mit der Serverkonsole arbeiten müssen, weder physisch noch remote. Zwar ist Windows Server schon seit längerer Zeit für eine Remoteverwaltung eingerichtet, doch ist diese Fähigkeit immer nur Stückwerk gewesen. Bei manchen Snap-Ins der MMC (Microsoft Management Console) konnten Administratoren eine Verbindung zu Remoteservern herstellen und Windows PowerShell 2.0 hat einige Remotefunktionen von der Befehlszeile bereitgestellt, doch umfasst Windows Server 2012 erstmals umfangreiche Tools für die Remoteverwaltung, die es fast erübrigen, an der Serverkonsole zu arbeiten.

Die neue Server-Manager-Anwendung in Windows Server 2012 versetzt Administratoren in die Lage, Server aus dem gesamten Unternehmen hinzuzufügen und Servergruppen zu erstellen, um die gleichzeitige Konfiguration mehrerer Systeme zu erleichtern. Die neue Windows PowerShell 3.0-Umgebung erhöht die Anzahl der verfügbaren Cmdlets von 230 auf mehr als 2.430.

Mit derartigen Tools ist es Administratoren möglich, ihre Server mit der Option *Server Core* zu installieren, einige Befehle auszuführen, um jeden Server mit einer Active Directory-Domain Services-Domäne zu verbinden und dann niemals mehr die Serverkonsole anfassen zu müssen. Alle später auszuführenden Verwaltungsaufgaben – einschließlich der Bereitstellung von Rollen und Features – können Sie mithilfe von Server-Manager und Windows PowerShell von einer Remotearbeitsstation aus abwickeln.

Fähigkeiten von Server Core

In einer *Server Core-Installation* fällt nicht nur der größte Teil der grafischen Benutzeroberfläche weg, es verschwinden auch einige der Serverrollen, die bei der Option *Server mit einer grafischen Benutzeroberfläche* zu finden sind. Die Option *Server Core-Installation* in Windows Server 2012 umfasst allerdings 12 der 19 Rollen und zusätzlich die Unterstützung für SQL Server 2012 gegenüber nur 10 Rollen in Windows Server 2008 R2 und 9 in Windows Server 2008.

Tabelle 1.4 listet die Rollen und Features auf, die in einer Windows Server 2012-Server Core-Installation verfügbar bzw. nicht verfügbar sind.

Tabelle 1.4 Rollen in einer Server Core-Installation von Windows Server 2012

In einer Server Core-Installation verfügbare Rollen	In einer Server Core-Installation nicht verfügbar Rollen
Active Directory-Zertifikatdienste	Active Directory-Verbunddienste
Active Directory-Domäendienste	Anwendungsserver
Active Directory Lightweight Directory Services	Faxserver
Active Directory-Rechteverwaltungsdienste	Netzwerkrichtlinien- und Zugriffsdienste
DHCP-Server	Remotedesktopdienste Remotedesktopgateway Remotedesktop-Sitzungshost Web Access für Remotedesktop
DNS-Server	Volumenaktivierungsdienste
Datei- und Speicherdiene	Windows-Bereitstellungsdienste
Hyper-V	
Druck- und Dokumentdienste	
Remotezugriff	
Webserver (IIS)	
Windows Server Update Services (WSUS)	

Die minimale Serverschnittstelle verwenden

Wenn die Vorteile von Server Core so verlockend klingen, Sie aber auf einige herkömmliche Tools zur Serveradministration nicht verzichten wollen, bietet Windows Server 2012 einen Kompromiss namens *minimale Serverschnittstelle*.

Die *minimale Serverschnittstelle* ist eine Einstellung, die einige der hardwareintensivsten Elemente aus der grafischen Benutzeroberfläche entfernt. Zu diesen Elementen gehören Internet Explorer und die Komponenten der Windows-Shell, einschließlich Desktop, Datei-Explorer und die Windows 8-Desktop-Apps. Außerdem wurden die als Shell-Erweiterungen implementierten Elemente der Systemsteuerung weggelassen, einschließlich der folgenden:

- Programme und Funktionen
- Netzwerk- und Freigabecenter
- Geräte und Drucker
- Anzeige
- Windows-Firewall
- Windows Update
- Schriftarten
- Storage Spaces

In der minimalen Serverschnittstelle verbleiben nur noch Server-Manager und MMC-Anwendungen, der Gerätemanager und die gesamte Windows PowerShell-Oberfläche. Damit stehen Administratoren die meisten Tools zur Verfügung, die sie für die Verwaltung von lokalen und Remoteservern benötigen.

Möchten Sie einen Windows Server 2012-Server mit einer grafischen Benutzeroberfläche konfigurieren, der die minimale Serverschnittstelle verwendet, führen Sie folgende Schritte aus:

1. Melden Sie sich beim Server, der Windows Server 2012 ausführt, unter einem Konto an, das über Administratorrechte verfügt. Das Fenster *Server-Manager* wird geöffnet.
2. Klicken Sie auf *Verwalten/Rollen und Features entfernen*. Der Assistent zum *Entfernen von Rollen und Features* startet und zeigt die Seite *Vorbemerkungen* an.
3. Klicken Sie auf *Weiter*, um zur Seite *Zielserver auswählen* zu gelangen.
4. Wählen Sie in der Liste *Serverpool* den Server aus, den Sie modifizieren möchten, und klicken Sie auf *Weiter*. Es erscheint die Seite *Serverrollen entfernen*.
5. Klicken Sie auf *Weiter*, um die Seite *Features entfernen* zu öffnen.
6. Erweitern Sie in der Liste *Features* das Feature *Benutzeroberflächen und Infrastruktur* (siehe Abbildung 1.2).

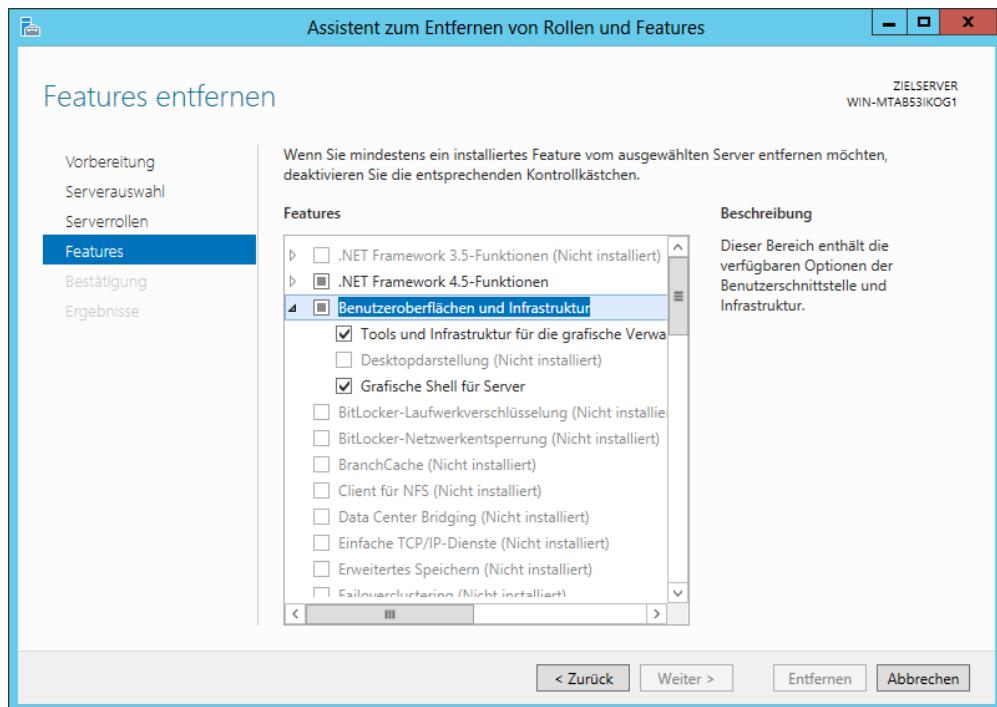


Abbildung 1.2 Das Feature *Benutzeroberflächen und Infrastruktur* im Assistenten zum Entfernen von Rollen und Features

7. Deaktivieren Sie das Kontrollkästchen *Grafische Shell für Server* und klicken Sie auf *Weiter*. Die Seite *Entfernungsauswahl bestätigen* wird geöffnet.
8. Klicken Sie auf *Entfernen*, um die Seite *Entfernungsstatus* zu öffnen.
9. Wenn das Entfernen abgeschlossen ist, klicken Sie auf *Schließen*.
10. Starten Sie den Server neu.

Die Option *Features bei Bedarf verwenden*

Während einer Windows Server 2012-Installation kopiert das Setupprogramm die Dateien für alle Betriebssystemkomponenten vom Installationsmedium in ein Verzeichnis *WinSxS*, den Side-by-Side-Komponentenspeicher. Damit sind Administratoren in der Lage, beliebige Features, die zu Windows Server 2012 gehören, zu aktivieren, ohne ein Installationsmedium bereitzustellen zu müssen.

Nachteilig bei dieser Anordnung ist, dass das Verzeichnis *WinSxS* beträchtlichen Festplattenplatz beansprucht und zwar in vielen Fällen größtenteils für Daten, die nie verwendet werden.

Da verstärkt virtuelle Computer eingesetzt werden, um Serverrollen zu verteilen, verfügen Unternehmensnetzwerke oftmals über mehrere Kopien des Serverbetriebssystems als bisher und verschwenden demzufolge mehr Festplattenplatz. Darüber hinaus schlagen sich die

heutzutage in Serverinfrastrukturen häufig eingesetzten erweiterten Speichertechnologien wie zum Beispiel Storage Area Networks (SANs) und Festkörperlaufwerke (Solid State Drives, SSDs) in erhöhten Kosten für den Speicherplatz nieder.

Die in Windows Server 2012 neue Funktion *Features bei Bedarf* verkörpert einen dritten Zustand für Betriebssystemfeatures, der Administratoren erlaubt, Festplattenplatz zu sparen, indem sie spezielle Features nicht nur deaktivieren, sondern auch aus dem *WinSxS*-Verzeichnis entfernen.

Dieser Zustand ist gedacht für Features, die Administratoren auf einem bestimmten Server nicht installieren möchten. Wollen Sie zum Beispiel das Servergrafikshell-Feature in Windows Server 2012 deaktivieren, um die Ausführung von Internet Explorer, Datei-Explorer und Desktop-Shell zu unterbinden, und die für diese Features relevanten Dateien von der Festplatte verbannen, können Sie dies mit der Option *Features bei Bedarf* realisieren. Indem Sie sämtliche Festplattendateien für alle Ihre nicht genutzten Features auf allen Ihren virtuellen Computern entfernen, erzielen Sie unter Umständen erhebliche Speicherplatz einsparungen.

Features bei Bedarf bietet einen dritten Installationsstatus für die einzelnen Features in Windows Server 2012. In vorherigen Versionen des Betriebssystems ließen sich Features aktivieren oder deaktivieren. Windows Server 2012 kennt nun die folgenden drei Zustände:

- Aktiviert
- Deaktiviert
- Deaktiviert und Nutzlast entfernt

Um diesen dritten Zustand zu implementieren, brauchen Sie das Cmdlet `Uninstall-WindowsFeature` von Windows PowerShell, das jetzt ein neues `-Remove`-Flag unterstützt. Möchten Sie beispielsweise das Servergrafikshell-Feature deaktivieren und dessen Quelldateien aus dem Verzeichnis *WinSxS* entfernen, verwenden Sie folgenden Windows PowerShell-Befehl:

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

Nachdem Sie die Quelldateien für ein Feature aus dem Ordner *WinSxS* gelöscht haben, lassen sie sich nicht wiederherstellen. Wenn Sie versuchen, das Feature erneut zu aktivieren, lädt das System die Dateien per Windows Update herunter. Alternativ ruft es sie aus einer Imagedatei ab, die Sie im Cmdlet `Install-WindowsFeature` mithilfe des Flags `-Source` spezifizieren können. Damit sind Sie in der Lage, die erforderlichen Dateien von einem Wechseldatenträger oder aus einer Imagedatei im lokalen Netzwerk abzurufen. Administratoren können auch per Gruppenrichtlinie eine Liste von Installationsquellen angeben.



Hinweis **Features bei Bedarf**

Diese Möglichkeit, Quelldateien für ein Feature von einem anderen Standort abzurufen, ist die eigentliche Funktionalität, auf die sich die Bezeichnung *Features bei Bedarf* bezieht. Microsoft verringert damit oftmals die Größe von Updates, die aus dem Internet heruntergeladen sind. Nachdem der Benutzer das Update installiert hat, lädt das Programm die erforderlichen Zusatzdateien herunter und vervollständigt die Installation.

Server aktualisieren

Ein direktes Upgrade ist die komplexeste Form der Windows Server 2012-Installation. Zudem dauert es am längsten und verursacht höchstwahrscheinlich Probleme während bei der Ausführung. Nach Möglichkeit sollten sich Administratoren an die Microsoft-Empfehlung halten und eine Neuinstallation ausführen oder stattdessen die erforderlichen Rollen, Anwendungen und Einstellungen migrieren.

Auch wenn direkte Upgrades oftmals reibungslos ablaufen, bedeutet die Komplexität des Upgradeprozesses und die große Anzahl von Variablen, dass es viele Dinge gibt, die schief laufen können. Um die Risiken zu minimieren, sollten Administratoren den Upgradeprozess unbedingt ernst nehmen, das System richtig vorbereiten und die Möglichkeit schaffen, alle eventuell auftretenden Probleme beheben zu können. Die folgenden Abschnitte beschäftigen sich ausführlich mit diesen Themen.

Upgrade-Pfade

Die Upgrade-Pfade für Windows Server 2012 sind beschränkt. Es ist in der Tat einfacher, anzugeben, wann Sie ein Upgrade durchführen können und wann nicht. Bei einem 64-Bit-System, auf dem Windows Server 2008 oder Windows Server 2008 R2 läuft, können Sie auf Windows Server 2012 aktualisieren, sofern Sie die gleiche Betriebssystemedition verwenden.

Nicht unterstützt werden von Windows Server 2012 die folgenden Upgrade-Pfade:

- Upgrades von Windows Server-Versionen vor Windows Server 2008
- Upgrades von pre-RTM-Editionen von Windows Server 2012
- Upgrades von Windows-Betriebssystemen für Arbeitsstationen
- Plattformübergreifende Upgrades wie zum Beispiel von 32-Bit-Windows Server 2008 auf 64-Bit-Windows Server 2012
- Upgrades von einer beliebigen Itanium-Edition aus
- Sprachübergreifende Upgrades wie zum Beispiel von Windows Server 2008, US English, auf Windows Server 2012, Französisch

In allen diesen Fällen lässt das Windows-Setupprogramm keine Fortsetzung des Upgrade-Vorgangs zu.

Auf das Upgrade vorbereiten

Bevor Sie sich an ein direktes Upgrade auf Windows Server 2012 heranmachen, sollten Sie eine Reihe von Vorbereitungen treffen, damit ein reibungsloser Ablauf gewährleistet ist und die Serverdaten geschützt sind.

Berücksichtigen Sie die folgenden Punkte, bevor Sie irgendein Upgrade von Windows Server 2012 ausführen:

- **Hardwarekompatibilität überprüfen** Stellen Sie sicher, dass der Server die minimalen Hardwareanforderungen für Windows Server 2012 erfüllt

- **Festplattenplatz überprüfen** Stellen Sie sicher, dass auf der Partition, auf der das alte Betriebssystem installiert ist, genügend Festplattenplatz vorhanden ist. Während des Upgradevorgangs ist genügend Festplattenplatz erforderlich, um die beiden Betriebssysteme gleichzeitig aufzunehmen. Nach Abschluss des Upgrades können Sie die alten Dateien entfernen und somit zusätzlichen Platz freigeben.
- **Von der Signierung der Software überzeugen** Die gesamte Kernelmode-Software einschließlich der Gerätetreiber muss digital signiert sein. Andernfalls lässt sich die Software nicht laden. Im Ergebnis ist mit einem abgebrochenen Upgradevorgang, Hardwareausfällen nach Abschluss des Upgrades oder einem gescheiterten Systemstart nach dem Upgrade zu rechnen. Können Sie kein signiertes Softwareupdate für die Anwendung oder den Treiber finden, sollten Sie die Anwendung bzw. den Treiber deinstallieren, bevor Sie mit der Installation fortfahren.



Wichtig Die Treibersignatur deaktivieren

Wenn ein nicht signierter Treiber den Start des Computers verhindert, können Sie die Forderung nach einer Treibersignatur deaktivieren, indem Sie während des Startvorgangs die Taste **[F8]** drücken, *Erweiterte Startoptionen* und dann *Erzwingen der Treibersignatur deaktivieren* auswählen.

- **Treiber für Massenspeicher oder Wechselmedien sichern** Wenn ein Hersteller einen eigenen Treiber für ein Gerät in Ihrem Server bereitgestellt hat, speichern Sie den Treiber auf einer CD, DVD oder einem USB-Flashlaufwerk entweder im Installationsmedien-Stammverzeichnis oder im Ordner */amd64*. Um den Treiber während des Setups bereitzustellen, klicken Sie auf *Treiber laden* oder drücken **[F6]** auf der Seite für die Datenträgerauswahl. Suchen Sie dann nach dem Speicherort des Treibers oder lassen Sie das Setupprogramm die Medien durchsuchen.
- **Anwendungskompatibilität überprüfen** Das Setupprogramm zeigt eine Seite *Kompatibilitätsbericht* an, die auf mögliche Probleme mit der Anwendungskompatibilität hinweist. Gegebenenfalls lassen sich diese Probleme beheben, wenn Sie die Anwendungen aktualisieren oder upgraden. Erstellen Sie eine Liste der auf dem Server installierten Produkte und recherchieren Sie auf den Websites der Hersteller nach Updates, Upgrades und Ankündigungen in Bezug auf die Unterstützung für Windows Server 2012. In einer Unternehmensumgebung sollten Sie alle Anwendungen auf Kompatibilität mit Windows Server 2012 testen, und zwar unabhängig von den Aussagen der Hersteller, bevor Sie Betriebssystem-Upgrades durchführen.
- **Funktionalität des Computers sicherstellen** Vergewissern Sie sich, ob Windows Server 2008 oder Windows Server 2008 R2 auf dem Computer ordnungsgemäß läuft, bevor Sie mit dem Upgrade beginnen. Da Sie ein direktes Upgrade aus dem vorhandenen Betriebssystem heraus starten müssen, können Sie nicht darauf zählen, dass Windows Server 2012 irgendwelche Probleme behebt, die den Startvorgang oder die Ausführung des Setupprogramms verhindern.
- **Eine vollständige Sicherung durchführen** Vor einem Upgrade empfiehlt es sich, das gesamte System oder zumindest die wichtigsten Datendateien zu sichern. In der Sicherung

sollten sämtliche Daten und Konfigurationsinformationen enthalten sein, die für die Funktion des Zielcomputers erforderlich sind. Achten Sie bei der Datensicherung darauf, die Boot- und Systempartitionen sowie die Daten für den Systemzustand einzuschließen. Wechselseitplatten vereinfachen diesen Vorgang, selbst wenn im Computer kein geeignetes Sicherungsgerät vorhanden ist.

- **Virenschutzprogramme deaktivieren** Derartige Programme können die Installation deutlich bremsen, da sie jede lokal auf den Computer kopierte Datei überprüfen. Sind Virenschutzprogramme installiert, deaktivieren Sie sie, bevor Sie mit dem Upgrade beginnen.
- **Den Computer von einer USV trennen** Ist Ihr Zielcomputer an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen, trennen Sie das Datenkabel, bevor Sie das Upgrade durchführen. Das Setupprogramm versucht automatisch die angeschlossenen Geräte zu erkennen, und eine USV kann dabei Probleme verursachen.
- **Erwerben Sie Windows Server 2012** Kaufen Sie die passende Windows Server 2012-Edition für das Upgrade und halten Sie den Installationsdatenträger und den Produktschlüssel bereit

Während des Upgradevorgangs bietet das Boot-Menü beim Neustart des Systems eine Option an, die vorherige Betriebssystemversion wiederherzustellen. Diese Option ist jedoch nach Abschluss des Upgrades nicht mehr verfügbar und es ist nicht möglich, Windows Server 2012 zu deinstallieren und zur alten Betriebssystemversion zurückzukehren.

Rollen migrieren

Migration ist bevorzugte Methode, einen vorhandenen Server durch einen Server, auf dem Windows Server 2012 läuft, zu ersetzen. Im Unterschied zu einem direkten Upgrade werden bei einer Migration wichtige Informationen von einem vorhandenen Server auf eine Neuinstallation von Windows Server 2012 kopiert.

Nahezu alle weiter oben aufgeführten Restriktionen in Bezug auf Upgrades gelten nicht für eine Migration. Mithilfe der Windows Server-Migrationstools und den mit Windows Server 2012 gelieferten Migrationshandbüchern können Sie Daten zwischen Servern unter den folgenden Bedingungen migrieren:

- **Zwischen Versionen** Daten lassen sich aus jeder Windows Server-Version bei Windows Server 2003 SP2 beginnend nach Windows Server 2012 migrieren. Das gilt auch für Migrationen von einem Server, auf dem Windows Server 2012 läuft, zu einem anderen Server.
- **Zwischen Plattformen** Daten können Sie von einem x86- oder x64-basierten Server auf einen x64-basierten Server, auf dem Windows Server 2012 läuft, migrieren
- **Zwischen Editionen** Daten können Sie zwischen Servern, auf denen verschiedene Windows Server-Editionen laufen, migrieren
- **Zwischen physischen und virtuellen Instanzen** Daten lassen sich von einem physischen auf einen virtuellen Server oder umgekehrt migrieren

- **Zwischen Installationsoptionen** Daten können Sie von einem Windows Server 2008 R2-Server auf einen Windows Server 2012-Server migrieren, selbst wenn der eine Server mit der Option *Server Core-Installation* und der andere mit der Option *Server mit einer grafischen Benutzeroberfläche* eingerichtet ist

Die Migration auf der Serverebene unterscheidet sich von allen Migrationen, die Sie möglicherweise auf Betriebssystemen von Arbeitsstationen durchgeführt haben. Anstatt einen einzigen Migrationslauf durchzuführen, der sämtliche Benutzerdaten vom Quell- zum Zielcomputer auf einmal kopiert, werden in einer Servermigration Rollen oder Rollendienste einzeln migriert.

Zu Windows Server 2012 gehört eine Sammlung von Migrationshandbüchern, die spezielle Anweisungen für die von Windows Server 2012 unterstützten Rollen bereitstellen. Einige dieser Rollen setzen die Verwendung der Windows Server-Migrationstools voraus, andere nicht.

Windows Server-Migrationstools installieren

Windows Server-Migrationstools ist ein Windows Server 2012-Feature, das aus Windows PowerShell-Cmdlets und Hilfedateien besteht und mit dem Administratoren bestimmte Rollen zwischen Servern migrieren können.

Bevor Sie allerdings die Migrationstools verwenden können, müssen Sie das Feature *Windows Server-Migrationstools* auf dem unter Windows Server 2012 laufenden Zielserver installieren und dann die passende Version der Tools auf den Quellserven kopieren.

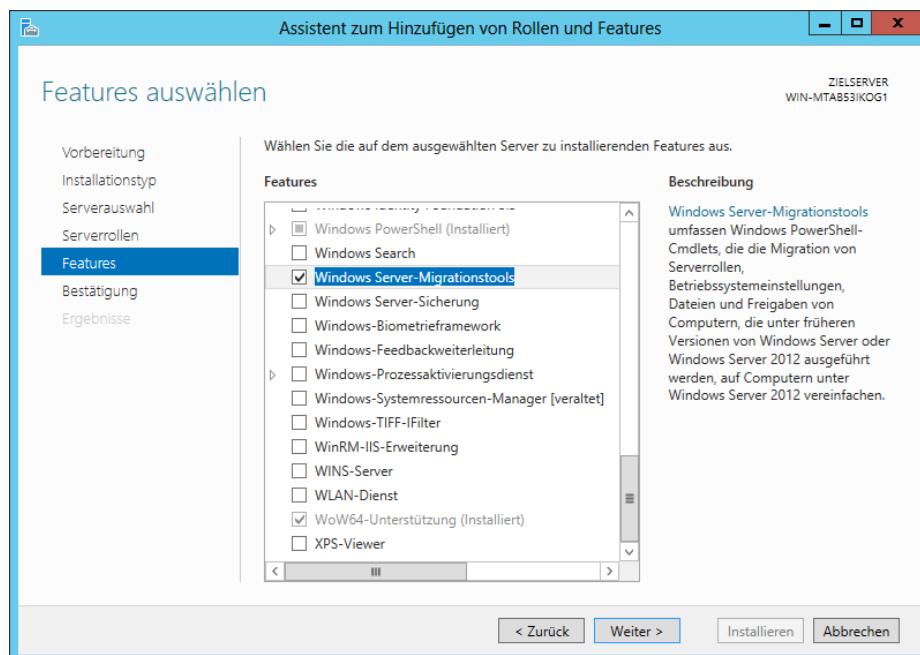


Abbildung 1.3 Die Seite *Features auswählen* des Assistenten zum Hinzufügen von Rollen und Features

Bei Windows Server-Migrationstools handelt es sich um ein Standardfeature. Um es auf Windows Server 2012 zu installieren, führen Sie im Server-Manager den Assistenten *Rollen und Features hinzufügen* (siehe Abbildung 1.3) oder das Windows PowerShell-Cmdlet `Install-WindowsFeature` aus.

Die Migrationshandbücher verwenden

Nachdem Sie die Windows Server-Migrationstools sowohl auf dem Quell- als auch dem Zielserver installiert haben, können Sie Daten zwischen den beiden Computern migrieren.

Die Migrationstools erlauben es Administratoren, bestimmte Rollen, Features, Freigaben, Betriebssystemeinstellungen und andere Daten vom Quellserver auf den Zielserver, auf dem Windows Server 2012 läuft, zu migrieren. Bei einigen Rollen sind Sie auf die Migrationstools angewiesen, bei anderen Rollen, die interne Kommunikationsfunktionen besitzen, kommen Sie ohne die Migrationstools aus.

Es gibt keine einheitliche Prozedur für die Migration sämtlicher Windows Server-Rollen, egal ob mit eigenen Migrationstools oder nicht. Stattdessen bietet Microsoft ausführliche Migrationshandbücher für einzelne Rollen und manchmal für einzelne Rollendienste innerhalb einer Rolle an.



Weitere Informationen Migrationshandbücher

Aktuelle Migrationshandbücher stehen über das Windows Server-Migrationsportal im Windows Server-TechCenter zur Verfügung (<http://technet.microsoft.com/de-de/library/jj134039>).



Gedankenexperiment Wenden Sie in diesem Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Prüfungsziels angeeignet haben. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Ralph bekommt einen neuen Server geliefert, auf dem bereits die Windows Server 2012 Datacenter-Edition mit der Option *Server mit grafischer Benutzeroberfläche* installiert ist. Ralph möchte das System als Webserver konfigurieren und sich dabei auf das absolute Minimum an Hardwareressourcen beschränken. Als Erstes installiert er mithilfe von Server-Manager die Rolle *Webserver (IIS)*.

Beantworten Sie für dieses Szenario die folgenden Fragen:

1. Mit welchem Windows PowerShell-Befehl kann Ralph die Installation mit grafischer Benutzeroberfläche in Server Core ändern?
2. Mit welchem Windows PowerShell-Befehl kann Ralph die Installationsdateien der Option *Server mit grafischer Benutzeroberfläche* vollständig aus dem System entfernen?

Prüfungszielzusammenfassung

- Microsoft veröffentlicht seine Betriebssysteme in mehreren Editionen, die Konsumenten verschiedene Preissegmente und Featuregruppen bieten
- Wenn Sie die Installationsoption *Server Core* auswählen, erhalten Sie eine abgespeckte Version des Betriebssystems
- Die minimale Serverschnittstelle ist eine Einstellung, die einige der hardwareintensivsten Elemente aus der grafischen Benutzeroberfläche entfernt
- Ein direktes Upgrade ist die komplexeste Form der Windows Server 2012-Installation. Zudem dauert es am längsten und verursacht höchstwahrscheinlich Probleme während der Ausführung. Nach Möglichkeit sollten sich Administratoren an die Microsoft-Empfehlung halten und eine Neuinstallation ausführen oder stattdessen die erforderlichen Rollen, Anwendungen und Einstellungen migrieren.
- Migration ist die bevorzugte Methode, einen vorhandenen Server durch einen Server, auf dem Windows Server 2012 läuft, zu ersetzen. Im Unterschied zu einem direkten Upgrade werden bei einer Migration wichtige Informationen von einem vorhandenen Server auf eine Neuinstallation von Windows Server 2012 kopiert.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Rollen implementiert das, was in die Kategorie Infrastrukturdienste fällt? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. DNS
 - B. Web Server (IIS)
 - C. DHCP
 - D. Remote Desktop Services
2. Welcher der folgenden Upgradepfade ist für Windows Server 2012 gültig?
 - A. Windows Server 2003 Standard zu Windows Server 2012 Standard
 - B. Windows Server 2008 Standard zu Windows Server 2012 Standard
 - C. Windows Server 2008 R2 32-Bit zu Windows Server 2012 64-bit
 - D. Windows 7 Ultimate zu Windows Server 2012 Essentials

3. Welches Feature müssen Sie einer Windows Server 2012 Server-Core-Installation hinzufügen, um sie zur minimalen Serverschnittstelle zu konvertieren?
 - A. Tools und Infrastruktur für die grafische Verwaltung
 - B. Grafische Shell für Server
 - C. Windows PowerShell
 - D. Microsoft Management Console
4. Wie heißt das Verzeichnis, in dem Windows alle Betriebssystemmodule speichert, die das System gegebenenfalls später noch installieren muss?
 - A. Windows
 - B. System32
 - C. bin
 - D. WinSxS
5. Aus welchen Gründen sollten Administratoren ihre Windows Server 2012-Server mit der Option *Server Core* installieren? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Eine Server Core-Installation lässt sich in die Option *Server mit grafischer Benutzeroberfläche* konvertieren, ohne das Betriebssystem neu installieren zu müssen.
 - B. Die Windows PowerShell 3.0-Oberfläche in Windows Server 2012 umfasst mehr als 10-Mal so viele Cmdlets wie die Version Windows PowerShell 2.0.
 - C. Mit dem neuen Server-Manager in Windows Server 2012 ist es erheblich einfacher, Server remote zu verwalten.
 - D. Eine Windows Server 2012-Lizenz für die Option Server Core-Installation kostet deutlich weniger als eine Lizenz für die Option Server mit grafischer Benutzeroberfläche.

Prüfungsziel 1.2: Server konfigurieren

Unmittelbar nach der Installation ist ein Server selten so konfiguriert, dass er alle Aufgaben ausführt, die Sie für ihn geplant haben. In der Regel ist eine gewisse Konfiguration im Anschluss an die Installation notwendig. Und ist der Server erst einmal in Betrieb, können sich noch weitere Konfigurationsänderungen ergeben.

Dieses Prüfungsziel zeigt, wie Sie

- Server Core konfigurieren
 - die Administration delegieren
 - Features in Offlineabbildern hinzufügen und entfernen
 - Rollen auf Remoteservern bereitstellen
 - den Server von der Option *Server Core-Installation* zur Option *Server mit grafischer Benutzeroberfläche* konvertieren und umgekehrt
 - Dienste konfigurieren
 - den NIC-Teamvorgang konfigurieren
-

Aufgaben nach der Installation

Im Rahmen der verstärkten Orientierung auf Cloud-basierte Dienste in Windows-Netzwerken enthält Windows Server 2012 eine breite Palette von überarbeiteten Tools mit Funktionen für eine erleichterte Verwaltung von Remoteservern.

Zum Beispiel versetzt der neue Server-Manager Administratoren in die Lage, Windows-Server komplett zu verwalten, ohne mit der Server-Konsole direkt – weder physisch noch remote – interagieren zu müssen. Allerdings gibt es einige Aufgaben, die Administratoren unmittelbar im Anschluss an die Betriebssysteminstallation ausführen und dafür direkt auf die Server-Konsole zugreifen müssen. Zu diesen Aufgaben gehören unter anderem:

- Die Netzwerkverbindung konfigurieren
- Die Zeitzone festlegen
- Remotedesktop aktivieren
- Den Computer umbenennen
- Einer Domäne beitreten

Tools der grafischen Benutzeroberfläche verwenden

In Windows Server 2012 bietet die Kachel *Eigenschaften* des Server-Managers (siehe Abbildung 1.4) die gleiche Funktionalität wie das Fenster *Aufgaben der Erstkonfiguration* in vorherigen Windows Server-Versionen. Eine oder alle Konfigurationsaufgaben nach der Installation in einer Windows Server 2012-Installation mit grafischer Benutzeroberfläche

können Sie mit den Tools in der Kachel *Eigenschaften* abschließen. Dabei arbeiten Sie entweder direkt an der Serverkonsole oder mithilfe von Remotedesktop, um auf den Server von einem anderen Computer aus zuzugreifen.

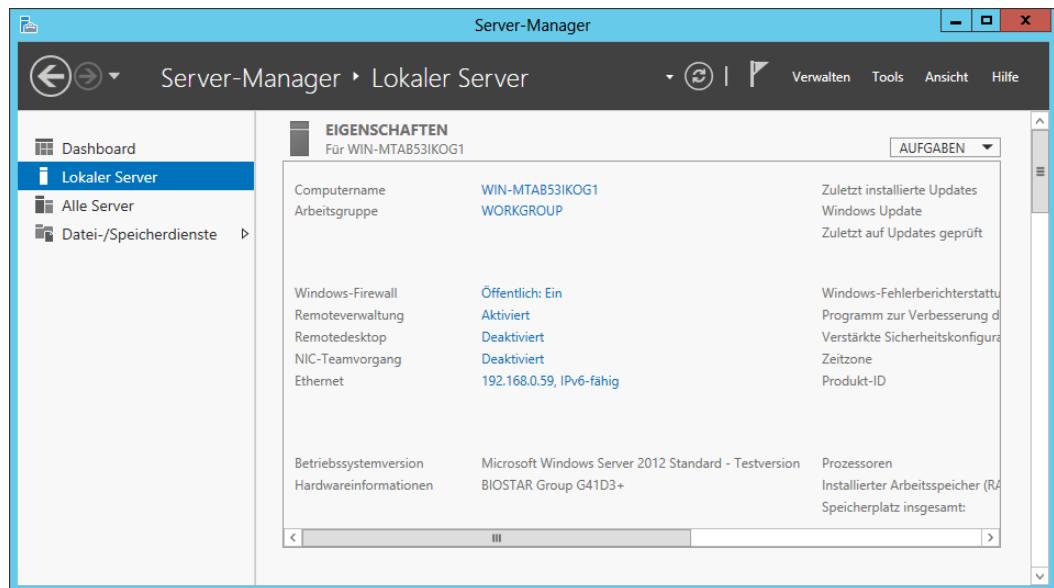


Abbildung 1.4 Die Kachel *Eigenschaften* des lokalen Servers im Server-Manager

Der Eintrag *Ethernet* in der Kachel *Eigenschaften* gibt den aktuellen Status für die Netzwerkschnittstelle des Computers an. Gibt es im Netzwerk einen DHCP (Dynamic Host Configuration Protocol)-Server, hat der Server bereits eine IP-Adresse und andere Einstellungen abgerufen und konfiguriert damit die Schnittstelle. Befindet sich kein DHCP-Server im Netzwerk oder müssen Sie den Computer mit einer statischen IP-Adresse konfigurieren, klicken Sie auf den *Ethernet*-Hyperlink, um das Fenster *Netzwerkverbindungen* aus der Systemsteuerung anzuzeigen. Damit können Sie das Dialogfeld *Eigenschaften von Ethernet* und das Dialogfeld *Eigenschaften von Internetprotokoll Version (TCP/IPv4)* öffnen und dort den TCP/IP-Client konfigurieren.

Für die Kommunikation der Active Directory-Domänen-Dienste ist eine genaue Computerzeit wichtig. Steht der Server in einer anderen Zeitzone als der (für Deutschland) standardmäßigen Zone (*UTC+0100*) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien, klicken Sie auf den *Zeitzone*-Hyperlink, um das Dialogfeld *Datum und Uhrzeit* zu öffnen und die Einstellung anzupassen.

Standardmäßig lässt Windows Server 2012 keine Remotedesktopverbindungen zu. Um sie zu aktivieren, klicken Sie auf den *Remotedesktop*-Hyperlink. Daraufhin gelangen Sie zum Dialogfeld *Systemeigenschaften* mit der Registerkarte *Remote*.

In einer manuellen Betriebssysteminstallation weist das Windows-Setupprogramm dem Computer einen eindeutigen Namen zu, der mit »WIN-« beginnt. Möchten Sie den

Computernamen ändern und einer Domäne beitreten, klicken Sie auf den *Computername-Hyperlink* und gelangen damit zum Dialogfeld *Systemeigenschaften* mit der Registerkarte *Computername*. Klicken Sie hier auf die Schaltfläche *Ändern*, um das Dialogfeld *Ändern des Computernamens bzw. der Domäne* zu öffnen.

Falls es aufgrund des begrenzten physischen Zugriffs auf den Server erforderlich ist, können Sie sich darauf beschränken, die Netzwerkverbindung zu konfigurieren und Remotedesktop zu aktivieren. Dann verbinden Sie sich per Remotedesktop mit dem Server und konfigurieren alles andere.

Die Befehlszeilentools verwenden

Wenn Sie bei der Installation von Windows Server 2012 die Option *Server Core* gewählt haben, können Sie die gleichen Aufgaben nach der Installation von der Befehlszeile aus ausführen. Dabei müssen Sie mindestens den Computer umbenennen und einer Domäne beitreten. Hierfür ist das Programm *Netdom.exe* vorgesehen.

Um einen Computer umzubenennen, führen Sie *Netdom.exe* mit der folgenden Syntax aus (siehe auch Abbildung 1.5):

```
netdom renamecomputer %ComputerName% /NewName: <NewComputerName>
```

```
C:\> Administrator: Eingabeaufforderung
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Administrator>netdom renamecomputer %ComputerName% /NewName:YAC
Durch diesen Vorgang wird der Computer WIN-MTAB53IKOG1
in YAC umbenannt.

Von bestimmten Diensten wie der Zertifizierungsstelle werden feste Computernamen
verwendet. Werden Dienste dieses Typs auf WIN-MTAB53IKOG1 ausgeführt,
zieht eine Änderung des Computernamens negative Auswirkungen nach sich.

Möchten Sie den Vorgang fortsetzen (Ja oder Nein)?
j
Zum Abschließen des Vorgangs muss der Computer neu gestartet werden.

Der Befehl wurde ausgeführt.

C:\Users\Administrator>
```

Abbildung 1.5 Umbenennen eines Computers von der Befehlszeile aus

Entsprechend der Anweisung ist der Computer neu zu starten. Führen Sie dazu den folgenden Befehl aus:

```
shutdown /r
```

Dann verbinden Sie den Computer mit einer Domäne. Die Syntax dieses Befehls lautet:

```
netdom join %ComputerName% /domain: <DomainName> /userd: <UserName> /passwordd:*
```

Das Sternchen (*) im Parameter */passwordd* bewirkt, dass das Programm das Kennwort für das angegebene Benutzerkonto abfragt.

Diese Befehle setzen voraus, dass der TCP/IP-Client des Computers bereits durch einen DHCP-Server eingerichtet ist. Andernfalls müssen Sie ihn manuell konfigurieren, bevor Sie einer Domäne beitreten können. Möchten Sie einem Computer mit Server Core eine statische IP-Adresse zuweisen, können Sie dazu das Programm *Netsh.exe* oder den über Windows PowerShell bereitgestellten WMI (Windows Management Instrumentation)-Zugriff verwenden.

Remotedesktopverbindungen zum Server aktivieren Sie mit dem folgenden Cmdlet:

```
Set-RemoteDesktop -Enable
```

Zwischen grafischer Benutzeroberfläche und Server Core konvertieren

In Windows Server 2012 können Sie einen Computer, der mit der Option *Server mit grafischer Benutzeroberfläche* eingerichtet ist, in die Option *Server Core* konvertieren und einem Server Core-Computer die grafische Benutzeroberfläche hinzufügen. Der Nutzwert von Server Core ist damit erheblich höher, verglichen mit der Version in Windows Server 2008 R2, wo sich die Oberfläche nur ändern ließ, wenn das gesamte Betriebssystem neu installiert wurde.

Diese Fähigkeit erlaubt es Administratoren, Server mit grafischer Benutzeroberfläche zu installieren, das anfängliche Setup mithilfe der grafischen Tools zu absolvieren und dann die Server zur Option Server Core zu konvertieren, um die Systemressourcen zu schonen. Sollte es sich später erforderlich machen, lassen sich die GUI-Komponenten erneut installieren.

Der folgende Ablauf zeigt, wie Sie von einer vollständigen Installation mit grafischer Benutzeroberfläche mithilfe von Server-Manager zu einer Server Core-Installation wechseln.

1. Melden Sie sich unter einem Konto mit Administratorrechten an dem Server an, auf dem Windows Server 2012 läuft. Das Fenster *Server-Manager* erscheint.
2. Im Menü *Verwalten* wählen Sie *Rollen und Features entfernen* aus. Daraufhin startet der Assistent zum Entfernen von Rollen und Features und zeigt die Seite *Vorbemerkungen* an.
3. Klicken Sie auf *Weiter*. Es erscheint die Seite *Zielserver auswählen*.
4. Wählen Sie den Server aus, auf dem Sie zu Server Core wechseln möchten, und klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Serverrollen entfernen*.
5. Klicken Sie auf *Weiter*. Es erscheint die Seite *Features entfernen*.
6. Scrollen Sie in der Liste nach unten und erweitern Sie das Feature *Benutzeroberflächen und Infrastruktur*, wie in Abbildung 1.6 gezeigt.
7. Deaktivieren Sie die Kontrollkästchen für die folgenden Komponenten:
 - Tools und Infrastruktur für die grafische Verwaltung
 - Grafische Shell für Server

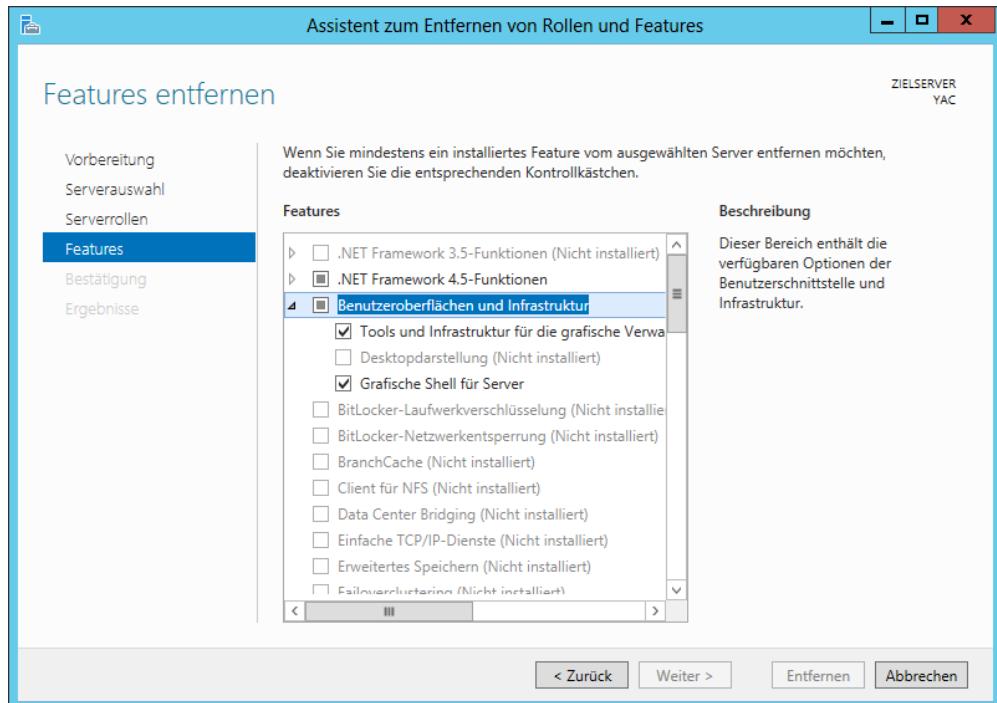


Abbildung 1.6 Die Seite *Features entfernen* in Server-Manager

8. Es erscheint das Dialogfeld *Möchten Sie die Features entfernen, für die "Tools und Infrastruktur für die grafische Verwaltung" erforderlich ist?* mit einer Liste der abhängigen Features, die deinstalliert werden müssen. Klicken Sie auf *Features entfernen*.
9. Klicken Sie auf *Weiter*, um die Seite *Entfernungsauswahl* bestätigen zu öffnen.
10. Aktivieren Sie das Kontrollkästchen *Zielserver bei Bedarf automatisch neu starten* und klicken Sie auf *Entfernen*. Während der Assistent das Feature entfernt, erscheint die Seite *Entfernungsstatus*.
11. Klicken Sie auf *Schließen*. Sobald das Entfernen abgeschlossen ist, startet der Computer neu.

Um einem Server Core-Computer die grafische Benutzeroberfläche hinzuzufügen, müssen Sie per Windows PowerShell dieselben Features installieren, die Sie in der vorhergehenden Prozedur entfernt haben. Mit dem folgenden Windows PowerShell-Befehl wandeln Sie eine Server Core-Installation von Windows Server 2012 in eine vollständige Installation mit grafischer Benutzeroberfläche um:

```
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart
```

Um eine vollständige Installation mit grafischer Benutzeroberfläche in eine Server Core-Installation umzuwandeln, verwenden Sie folgenden Befehl:

```
Uninstall-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart
```

NIC-Teamvorgang konfigurieren

Der Netzwerkadapter (NIC)-Teamvorgang ist ein neues Feature in Windows Server 2012. Damit können Administratoren die Bandbreite von mehreren Netzwerkadapters zusammenfassen und somit eine erhöhte Performance und Fehlertoleranz gewährleisten. Durch Virtualisierung sind Administratoren in der Lage, entscheidende Netzwerkfunktionen auf verschiedenen Systemen zu realisieren, ohne für jede Funktion einen eigenen physischen Computer anschaffen zu müssen. Nachteilig bei dieser Praxis ist aber, dass ein einzelner Server, der mehrere virtuelle Computer hostet, trotzdem noch einen Single Point of Failure (svw. das schwächste Glied in der Kette) für alle von ihnen darstellt. Ein einziger nicht funktionierender Netzwerkadapter, ein fehlerhafter Switch oder selbst ein nicht richtig eingestecktes Kabel können zum Ausfall eines Hostservers und aller seiner virtuellen Computer führen.

Der auch als *Lastenausgleich und Failover* (Load Balancing and Failover, LBFO) oder *Bandbreitenaggregation* bezeichnete NIC-Teamvorgang ist eine Technik, die schon einige Zeit existiert, jedoch immer an spezifische Hardwareimplementierungen gebunden war. In Windows Server 2012 ist die Funktion des NIC-Teamvorgangs hardwareunabhängig und erlaubt es, mehrere physische Netzwerkadapter zu einer einzigen Schnittstelle zusammenzufassen. Das Ergebnis ist eine höhere Performance, da der Durchsatz der Adapter kombiniert wird, und ein Schutz gegen Adapтерausfälle, weil der gesamte Datenverkehr auf die funktionierenden Netzwerkadapter verteilt wird.

Das Feature *NIC-Teamvorgang* in Windows Server 2012 unterstützt zwei Modi:

- **Switchunabhängiger Modus** Die Netzwerkadapter sind an verschiedene Switches angeschlossen, sodass alternative Routen durch das Netzwerk zur Verfügung stehen
- **Switchabhängiger Modus** Alle Netzwerkadapter sind mit demselben Switch verbunden, was eine einzelne Schnittstelle mit zusammengefasster Bandbreite ergibt

Im switchunabhängigen Modus können Sie zwischen zwei Konfigurationen wählen. Bei der Konfiguration aktiv/aktiv bleiben alle Netzwerkadapter funktional, was einen erhöhten Durchsatz gewährleistet. Fällt ein Adapter aus, wird der gesamte Datenverkehr auf die verbleibenden Adapter rangiert. In der Konfiguration aktiv/Standby bleibt ein Adapter offline und fungiert als Failover, falls der aktive Adapter ausfällt. Im Modus aktiv/aktiv führt ein Adapтерausfall zu einer verringerten Performance, im Modus aktiv/Standby bleibt die Performance nach einem Adapтерausfall gleich.

Im switchabhängigen Modus können Sie zwischen statischem und dynamischem Teamvorgang wählen. Der statische Teamvorgang gleicht den Datenverkehr zwischen den Adapters im Team aus; der dynamische Teamvorgang verwendet LACP (Link Aggregation Control Protocol, in IEEE 802.3ax definiert), sofern Ihr Equipment dies unterstützt.

Der NIC-Teamvorgang weist eine wichtige Beschränkung auf. Besteht der Datenverkehr aus großen TCP-Sequenzen, wie zum Beispiel einer Hyper-V-Livemigration, vermeidet das System die Verwendung mehrerer Adapter für diese Sequenzen, um die Anzahl verlorener und Out-of-Order-TCP-Segmente zu minimieren. Demzufolge werden Sie keine Performanceverbesserungen bei großen Dateiübertragungen per TCP feststellen.

NIC-Teams erstellen und verwalten Sie mithilfe von Server-Manager oder per Windows PowerShell. Führen Sie die folgenden Schritte aus, um ein NIC-Team mit Server-Manager zu erzeugen:

1. Melden Sie sich bei dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Es erscheint das Fenster *Server-Manager*.
2. Klicken Sie im Navigationsbereich auf *Lokaler Server*. Es erscheint die Startseite *Lokaler Server*.
3. Klicken Sie in der Kachel *Eigenschaften* auf *NIC-Teamvorgang*. Das Fenster *NIC-Teamvorgang* wird geöffnet (siehe Abbildung 1.7).

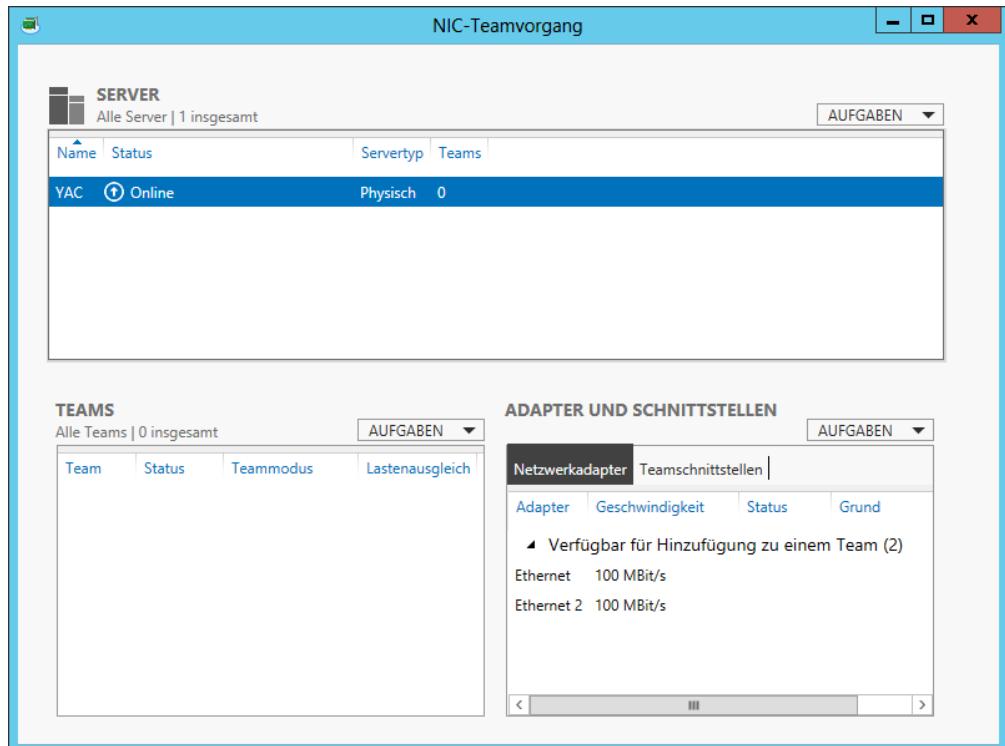


Abbildung 1.7 Das Fenster *NIC-Teamvorgang* in Server-Manager

4. In der Kachel *Teams* klicken Sie auf *Aufgaben* und wählen *Neues Team* aus, um die Seite *Neues Team* zu öffnen.
5. Klicken Sie auf den Pfeil *Weitere Eigenschaften*, um das Fenster zu erweitern, wie Abbildung 1.8 zeigt.

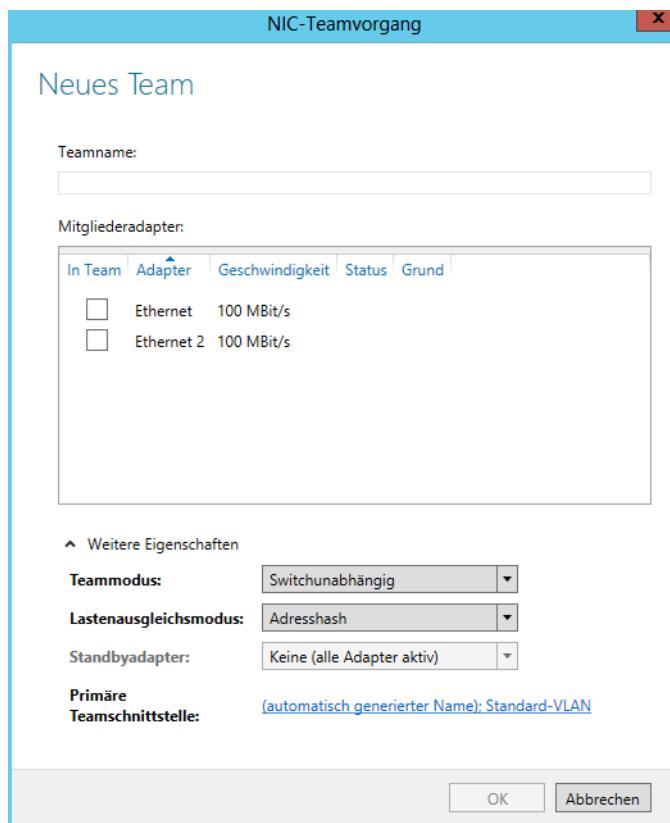


Abbildung 1.8 Die Seite *Neues Team* in Server-Manager

6. Tragen Sie in das Textfeld *Teamname* den Namen ein, den Sie dem Team zuweisen möchten.
7. Wählen Sie im Feld *Mitgliederadapter* die Netzwerkadapter aus, die Sie dem Team hinzufügen möchten.
8. Wählen Sie in der Dropdownliste *Teammodus* eine der folgenden Optionen aus:
 - Statischer Teamvorgang
 - Switchunabhängig
 - LACP
9. Wählen Sie in der Dropdownliste *Lastenausgleichsmodus* eine der folgenden Optionen aus:
 - Adresshash
 - Hyper-V-Port

10. Haben Sie sich beim Teammodus für *Switchunabhängig* entschieden, wählen Sie jetzt in der Dropdownliste *Standbyadapter* einen der Adapter aus, die Sie dem Team hinzugefügt haben, der dann als Offline-Standby fungiert.
11. Klicken Sie auf *OK*. Das neue Team erscheint in der Kachel *Teams*, wie in Abbildung 1.9 gezeigt.

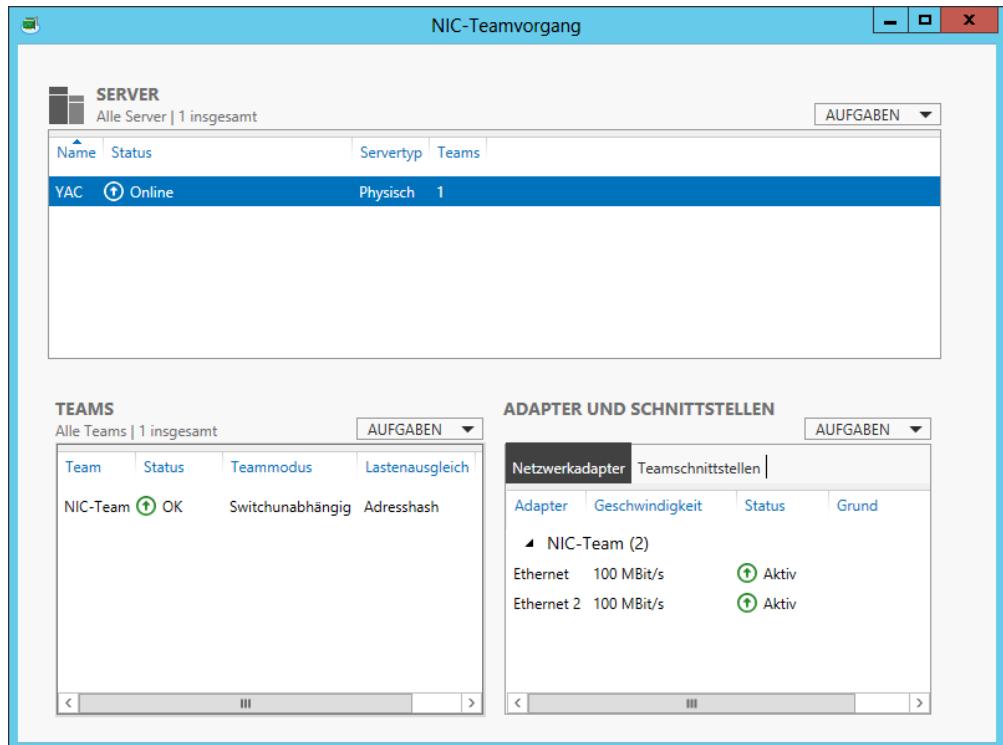


Abbildung 1.9 Im Fenster *NIC-Teamvorgang* des Server-Managers angelegtes neues NIC-Team

Nachdem Sie ein NIC-Team erstellt haben, lässt sich im Fenster *NIC-Teamvorgang* der Status des Teams und der erzeugten Teamschnittstelle überwachen. Anhand der Statusindikatoren für das Team selbst und für die einzelnen Adapter können Sie erkennen, ob ein Adapter offline gegangen ist.

Falls dies passiert, wechselt der Indikator des fehlerhaften Adapters sofort in den Status *Verbindung getrennt*, wie in Abbildung 1.10 zu sehen. Je nach gewähltem Teammodus kann sich auch der Status des anderen Adapters ändern.

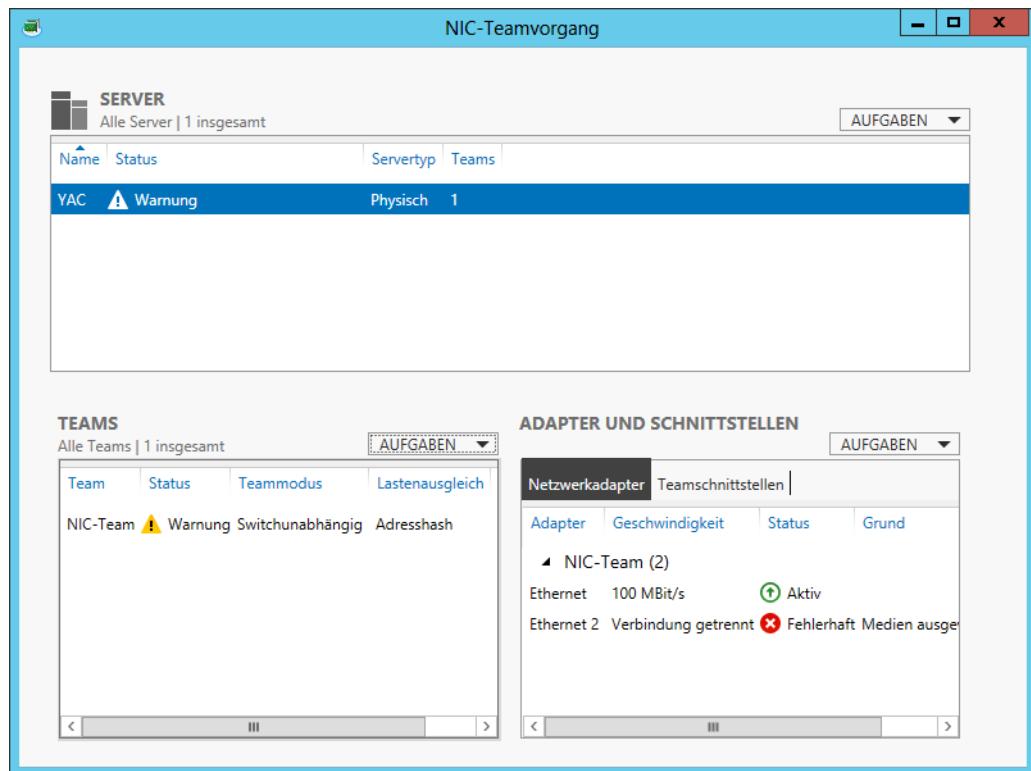


Abbildung 1.10 Ein NIC-Team mit einem ausgefallenen Adapter

Server-Manager verwenden

Das Tool *Server-Manager* in Windows Server 2012 ist eine neue Anwendung, die den ersten und offensichtlichsten Beweis für eine wesentliche Paradigmenverschiebung in der Windows Server-Administration liefert. In vorherigen Versionen von Windows Server musste ein Administrator, der eine Rolle mithilfe der grafischen Benutzeroberfläche installieren wollte, an der Serverkonsole arbeiten, und zwar entweder physisch von der Tastatur aus oder über eine Verbindung mithilfe der *Remotedesktopdienste* (vormals Terminaldienste genannt). Dagegen kann der Server-Manager von Windows Server 2012 Rollen und Features auf jedem beliebigen Server im Netzwerk installieren.

Server hinzufügen

Der Server-Manager in Windows Server 2012 unterscheidet sich von vorhergehenden Versionen vor allem durch die Möglichkeit, mehrere Server auf einmal hinzuzufügen und zu verwalten. Wenn Sie sich an einer vollständigen Installation mit grafischer Benutzeroberfläche von Windows Server 2012 mit einem Administratorkonto anmelden, startet der Server-Manager automatisch und zeigt die *Willkommen*-Kachel an.

Die Benutzeroberfläche von Server-Manager besteht aus einem Navigationsbereich auf der linken Seite mit Symbolen, die verschiedene Ansichten von Serverressourcen darstellen. Die Auswahl eines Symbols zeigt eine Startseite im rechten Bereich an, die aus einer Anzahl von Kacheln mit Informationen über die Ressource besteht. Die *Dashboard*-Seite, die standardmäßig erscheint, enthält neben der *Willkommen*-Kachel auch Miniaturansichten. Diese fassen die anderen Ansichten zusammen, die im Server-Manager verfügbar sind, wie es Abbildung 1.11 zeigt. Dazu gehören eine Seite für den lokalen Server, eine für alle Server sowie andere für Servergruppen und Rollengruppen.

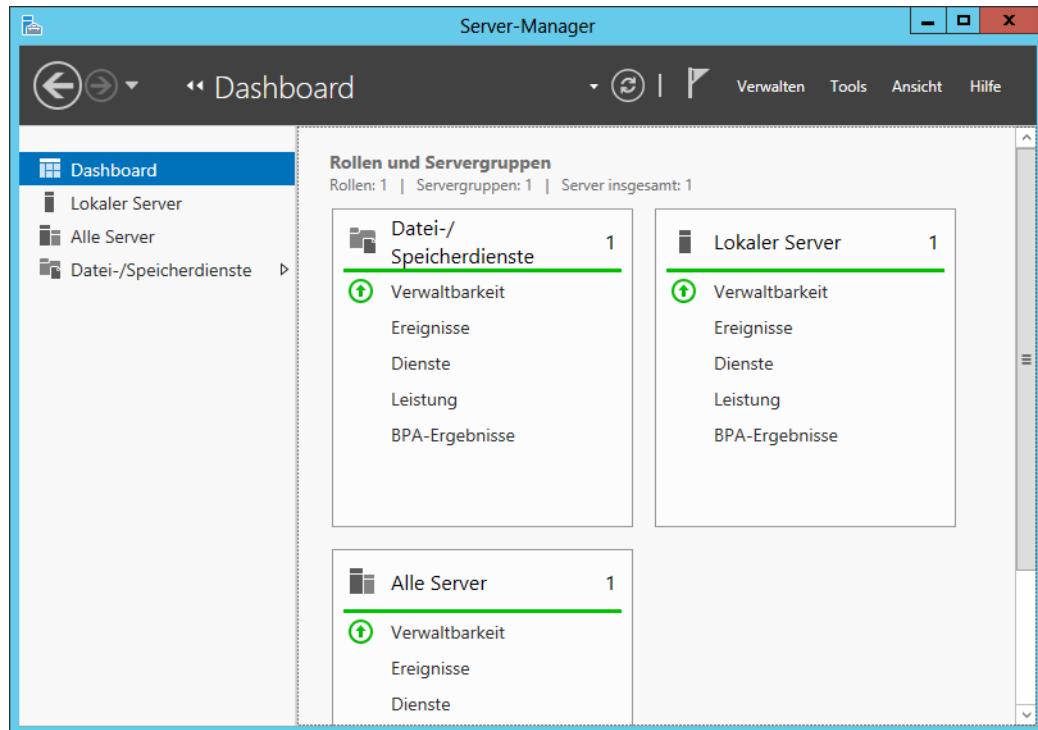


Abbildung 1.11 Dashboard-Miniaturansichten im Server-Manager

Beim ersten Start von Server-Manager erscheint zwar nur der lokale Server, doch können Sie weitere Server hinzufügen, um diese gemeinsam zu verwalten. Die hinzugefügten Server können physische oder virtuelle Server sein und jeweils eine beliebige Version von Windows Server ab Windows Server 2003 aufwärts ausführen. Nachdem Sie der Benutzeroberfläche Server hinzugefügt haben, können Sie Gruppen mit Sammlungen von Servern anlegen, wie zum Beispiel Server an einem bestimmten Standort oder Server, die eine bestimmte Funktion realisieren. Diese Gruppen sind im Navigationsbereich zu sehen und lassen sich als einzelne Entität administrieren.

Führen Sie die folgenden Schritte aus, um Server in Server-Manager hinzuzufügen:

1. Melden Sie sich bei dem Server, der Windows Server 2012 ausführt, unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Klicken Sie im Navigationsbereich auf *Alle Server*. Daraufhin erscheint die Startseite *Alle Server*, wie sie Abbildung 1.12 zeigt.

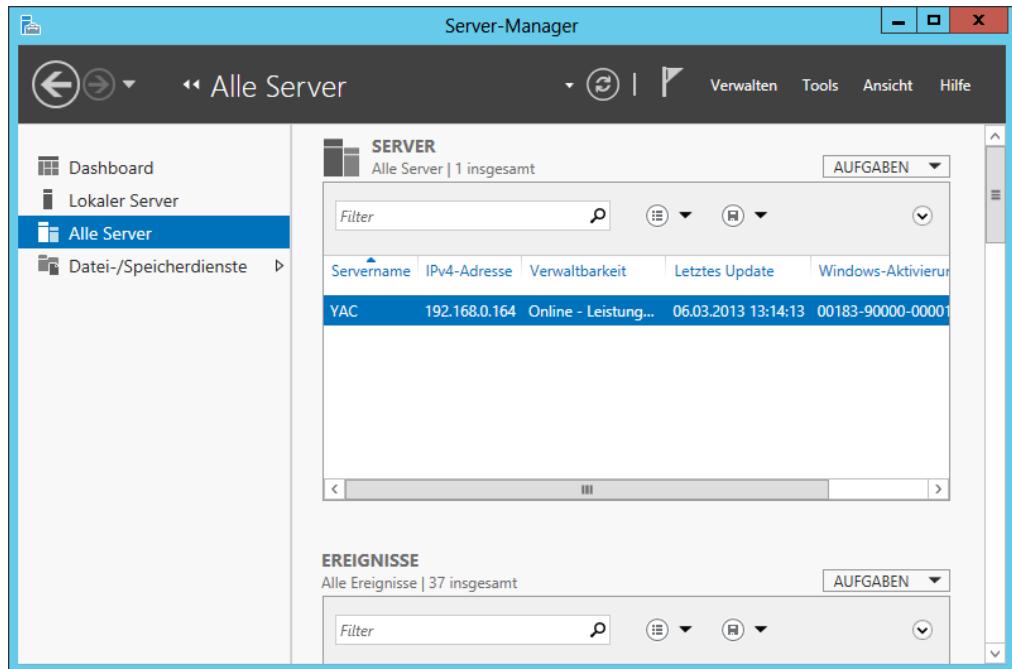


Abbildung 1.12 Die Startseite *Alle Server* in Server-Manager

3. Wählen Sie im Menü *Verwalten* den Befehl *Server hinzufügen*. Es erscheint das Dialogfeld *Server hinzufügen*, das in Abbildung 1.13 zu sehen ist.
4. Wählen Sie eine der folgenden Registerkarten aus, um festzulegen, wie Sie die hinzuzufügenden Server suchen möchten:
 - **Active Directory** Erlaubt die Suche nach Computern, die bestimmte Betriebssysteme an bestimmten Standorten in einer Active Directory-Domänen Dienst-Domäne ausführen
 - **DNS** Erlaubt die Suche nach Servern in Ihrem derzeit konfigurierten DNS (Domain Name System)-Server
 - **Importieren** Ermöglicht es, eine Textdatei mit den Namen der hinzuzufügenden Server anzugeben

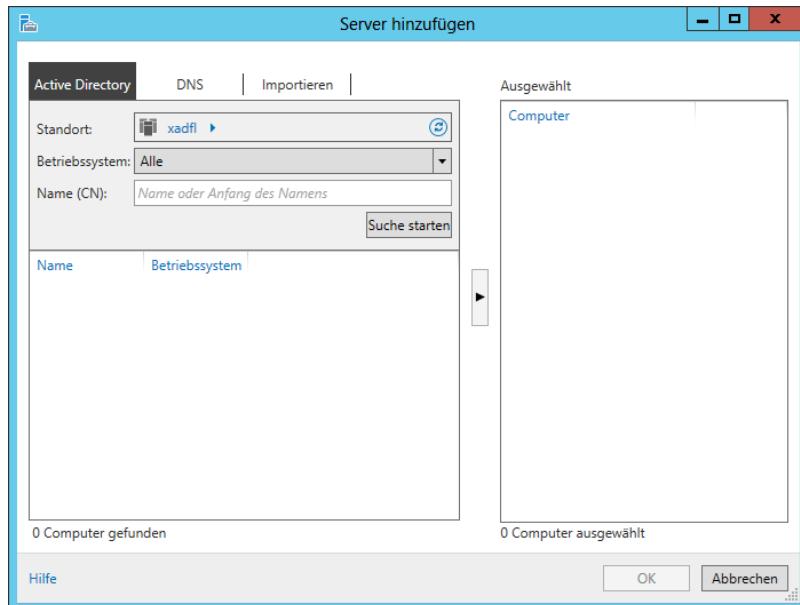


Abbildung 1.13 Das Dialogfeld *Server hinzufügen* in Server-Manager

5. Initiiieren Sie eine Suche oder laden Sie eine Textdatei hoch, um eine Liste der verfügbaren Server wie in Abbildung 1.14 anzuseigen.

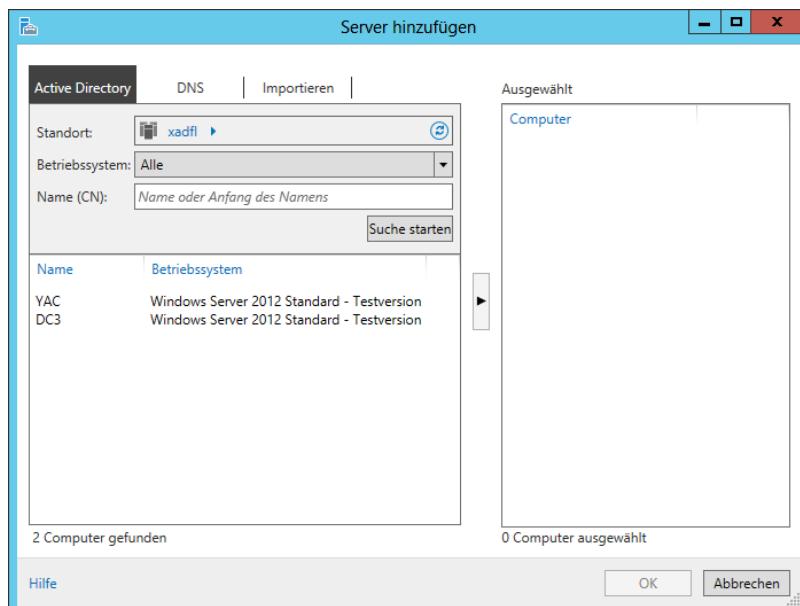


Abbildung 1.14 Suchen nach Servern in Server-Manager

6. Wählen Sie die Server aus, die Sie hinzufügen möchten, und klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil, um sie in die Liste *Ausgewählt* zu übernehmen.
7. Klicken Sie auf *OK*. Die ausgewählten Server werden der Startseite *Alle Server* hinzugefügt.

Nachdem Sie Remote-Server in die Benutzeroberfläche von Server-Manager hinzugefügt haben, gibt es verschiedene Möglichkeiten, auf sie zuzugreifen, unter anderem mit den standardmäßigen MMC-Verwaltungstools, der Konsole *Computerverwaltung* und einer Windows PowerShell-Remotesitzung.

Administratoren von Unternehmensnetzwerken müssen gegebenenfalls eine große Anzahl von Servern in Server-Manager hinzufügen. Um nicht mit einer langen Auswahlliste von Servern arbeiten zu müssen, können Sie Servergruppen basierend auf Serverstandorten, Funktionen oder anderen organisatorischen Paradigmen einrichten.

Rollen und Features hinzufügen

Windows Server 2012 fasst im *Server-Manager* mit dem Assistenten zum Hinzufügen von Rollen und Features das zusammen, was bisher für diese Aufgaben in eigenen Assistenten realisiert wurde. Nachdem Sie der Server-Manager-Benutzeroberfläche mehrere Server hinzugefügt haben, sind sie in den Assistenten zum Hinzufügen von Rollen und Features integriert, sodass Sie Rollen und Features auf jedem Ihrer Server bereitstellen können.

Führen Sie die folgenden Schritte aus, um Rollen und Features mithilfe von Server-Manager zu installieren:

1. Melden Sie sich bei dem Server, der Windows Server 2012 ausführt, unter einem Konto mit Administratorrechten an. Das Fenster Server-Manager wird geöffnet.
2. Wählen Sie im Menü *Verwalten* den Eintrag *Rollen und Features hinzufügen*. Der Assistent zum Hinzufügen von Rollen und Features startet und zeigt die Seite *Vorbemerkungen* an.
3. Klicken Sie auf *Weiter*, um die Seite *Installationstyp auswählen* wie in Abbildung 1.15 gezeigt zu öffnen.
4. Lassen Sie die Option *Rollenbasierte oder featurebasierte Installation* ausgewählt und klicken Sie auf *Weiter*. Daraufhin gelangen Sie zur Seite *Zielserver auswählen*, wie in Abbildung 1.16 zu sehen.

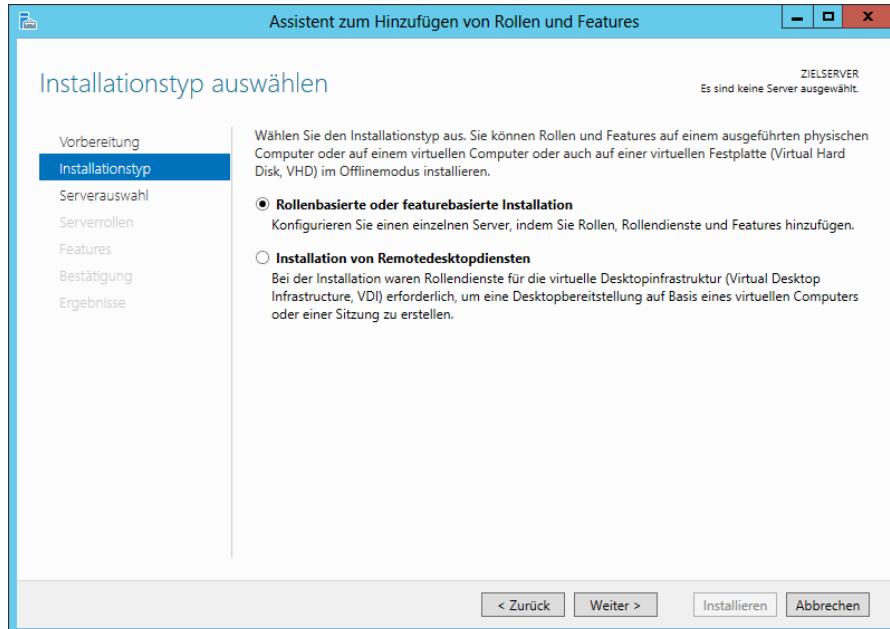


Abbildung 1.15 Die Seite *Installationstyp auswählen* im Assistenten zum Hinzufügen von Rollen und Features

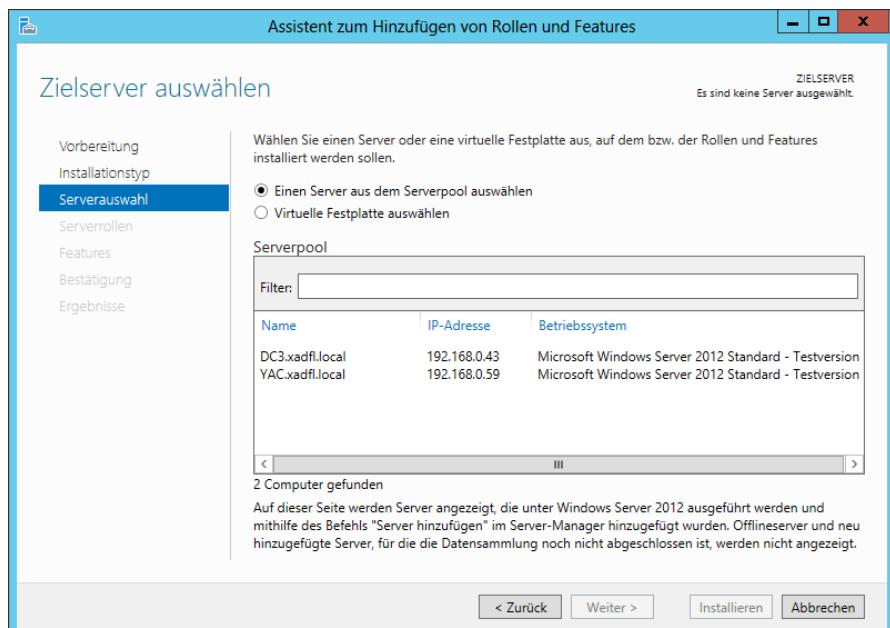


Abbildung 1.16 Die Seite *Zielserver auswählen* im Assistenten zum Hinzufügen von Rollen und Features

5. Wählen Sie den Server aus, auf dem Sie die Rollen oder Features installieren möchten. Enthält der Serverpool eine große Anzahl von Servern, können Sie mithilfe des Textfelds *Filter* eine Teilmenge des Pools basierend auf einer Textzeichenfolge anzeigen. Haben Sie den Server ausgewählt, klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Serverrollen auswählen*, die Abbildung 1.17 zeigt.

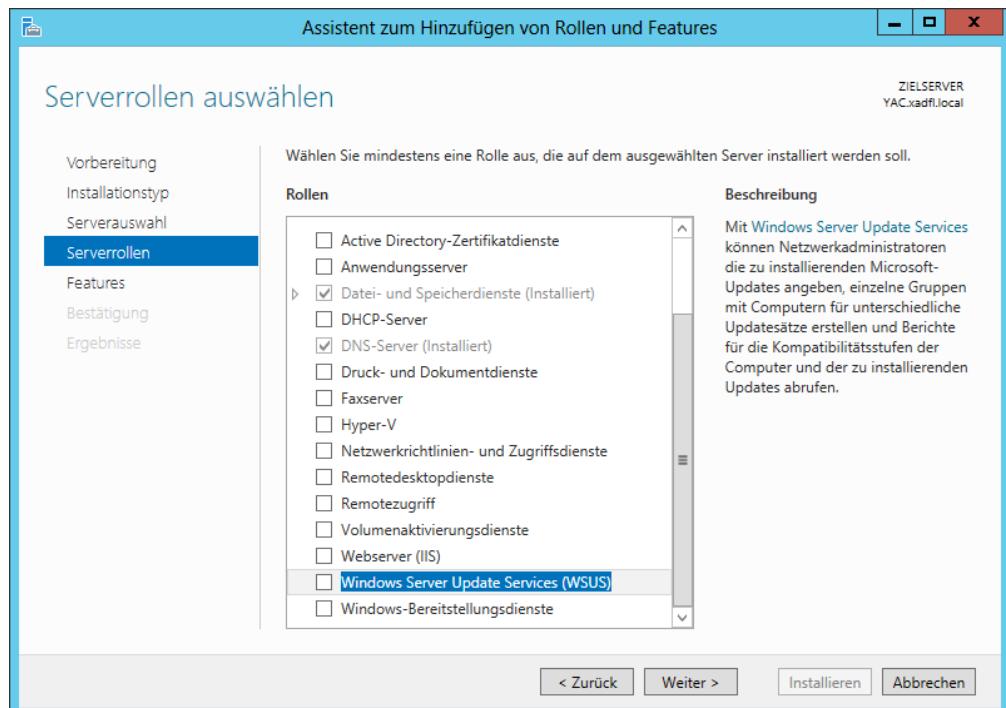


Abbildung 1.17 Die Seite *Serverrollen auswählen* im Assistenten zum Hinzufügen von Rollen und Features



Hinweis Komponenten auf mehreren Servern installieren

Mit dem Assistenten zum Hinzufügen von Rollen und Features können Sie zwar Komponenten auf einem beliebigen Server, den Sie Server-Manager hinzugefügt haben, installieren, es ist aber nicht möglich, Komponenten auf mehreren Servern auf einmal zu installieren. Allerdings lässt sich dies mithilfe von Windows PowerShell bewerkstelligen.

6. Wählen Sie die Rolle(n) aus, die Sie auf dem ausgewählten Server installieren möchten. Besitzen die ausgewählten Rollen andere Rollen- oder Featureabhängigkeiten, erscheint ein Dialogfeld *Sollen für <Rolle> erforderliche Features hinzugefügt werden?*



Hinweis Alle Rollen und Features auswählen

Im Unterschied zu vorherigen Versionen von Server-Manager erlaubt es die Version von Windows Server 2012, alle Rollen und Features für eine bestimmte Serverkonfiguration auf einmal auszuwählen, anstatt den Assistenten mehrmals ausführen zu müssen.

7. Klicken Sie auf *Features hinzufügen*, um die Abhängigkeiten zu akzeptieren, und klicken Sie dann auf *Weiter*. Damit gelangen Sie zur Seite *Features auswählen*, die in Abbildung 1.18 zu sehen ist.

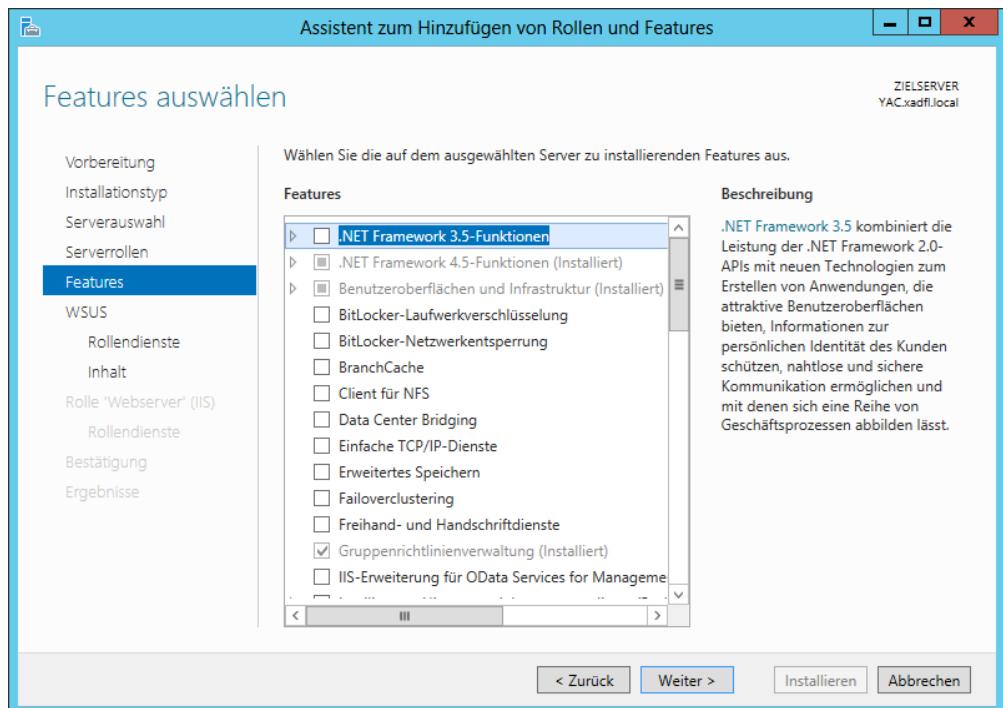


Abbildung 1.18 Die Seite *Features auswählen* im Assistenten zum Hinzufügen von Rollen und Features

8. Markieren Sie alle Features, die Sie auf dem ausgewählten Server installieren möchten, und klicken Sie auf *Weiter*. Für die ausgewählten Features können wiederum Abhängigkeiten erscheinen.
9. Der Assistent zeigt dann Seiten je nach den ausgewählten Rollen oder Features an. Die meisten Rollen haben eine Seite *Rollendienste auswählen*, auf der Sie die zu installierenden Elemente für die jeweilige Rolle festlegen können. Vervollständigen Sie die einzelnen rollen- oder featurespezifischen Seiten und klicken Sie auf *Weiter*. Abschließend erscheint eine Seite *Installationsauswahl bestätigen*.
10. Sie können die folgenden optionalen Funktionen auswählen:

- **Zielserver bei Bedarf automatisch neu starten** Bewirkt, dass der Server nach Abschluss der Installation automatisch neu startet, sofern die ausgewählten Rollen und Features dies erfordern.
- **Konfigurationseinstellungen exportieren** Erzeugt ein XML-Skript, das die über den Assistenten ausgeführten Abläufe dokumentiert. Mithilfe dieses Skripts und Windows PowerShell können Sie dann die gleiche Konfiguration auf einem anderen Server installieren.
- **Alternativen Quellpfad angeben** Legt den Speicherort einer Imagedatei fest, die die erforderliche Software für die Installation der ausgewählten Rollen und Features enthält.

11. Klicken Sie auf *Installieren*. Daraufhin erscheint die Seite *Installation Installationsstatus*. Je nach den installierten Rollen und Features zeigt der Assistent gegebenenfalls Hyperlinks zu den Tools an, die für Aufgaben nach der Installation auszuführen sind. Klicken Sie nach Abschluss der Installation auf *Schließen*, um den Assistenten fertig zu stellen.



Hinweis Eine exportierte Konfigurationsdatei verwenden

Möchten Sie eine exportierte Konfigurationsdatei verwenden, um Rollen und Features auf einem anderen Windows Server 2012-Computer zu installieren, können Sie das mit dem folgenden Befehl in einer Windows PowerShell-Sitzung mit erhöhten Rechten bewerkstelligen:

```
Install-WindowsFeature -ConfigurationFilePath <ExportedConfig.xml>
```

Wenn Sie Rollen auf Ihren Servern installiert haben, erscheinen die Rollen als Symbole im Navigationsbereich. Diese Symbole stellen eigentlich Rollengruppen dar. Jede Rollengruppe enthält sämtliche Instanzen dieser Rolle, die auf beliebigen Ihrer hinzugefügten Server zu finden ist. Deshalb können Sie die Rolle über alle Server hinweg verwalten, auf denen Sie sie installiert haben.

Rollen auf virtuellen Festplatten bereitstellen

Der Server-Manager erlaubt es Administratoren nicht nur, Rollen und Features auf Servern im Netzwerk zu installieren, sondern auch auf virtuellen Computern, die sich momentan im Offline-Status befinden. Zum Beispiel könnten Sie einen virtuellen Computer als Offline-Webserver auf einem Backup-Hostserver einrichten, für den Fall, dass der Computer, der den primären virtuellen Computer für den Webserver hostet, ausfallen sollte. Im Server-Manager ist es möglich, eine VHD-Datei (VHD – Virtual Hard Disk, virtuelle Festplatte) auszuwählen und darauf Rollen und Features zu installieren oder zu entfernen, ohne die VM starten zu müssen.

Führen Sie die folgenden Schritte aus, um Rollen oder Features auf einer Offline-VHD-Datei zu installieren:

1. Melden Sie sich auf dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Es erscheint das Fenster *Server-Manager*.

2. Wählen Sie im Menü *Verwalten* den Eintrag *Rollen und Features hinzufügen* aus. Daraufhin startet der Assistent zum Hinzufügen von Rollen und Features und zeigt die Seite *Vorbemerkungen* an.
3. Klicken Sie auf *Weiter*, um die Seite *Installationstyp auswählen* zu öffnen.
4. Lassen Sie die Option *Rollenbasierte oder featurebasierte Installation* ausgewählt und klicken Sie auf *Weiter*. Es erscheint die Seite *Zielserver auswählen*.
5. Wählen Sie die Option *Virtuelle Festplatte auswählen* aus. Am unteren Rand der Seite erscheint ein Textfeld *Virtuelle Festplatte*.
6. Geben Sie in das Textfeld *Virtuelle Festplatte* den Speicherort der VHD-Datei ein, die Sie ändern möchten (oder suchen Sie den Speicherort über *Durchsuchen*).
7. Wählen Sie im Feld *Serverpool* den Server aus, auf dem der Assistent die VHD-Datei bereitstellen soll (siehe Abbildung 1.19), und klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Serverrollen auswählen*.

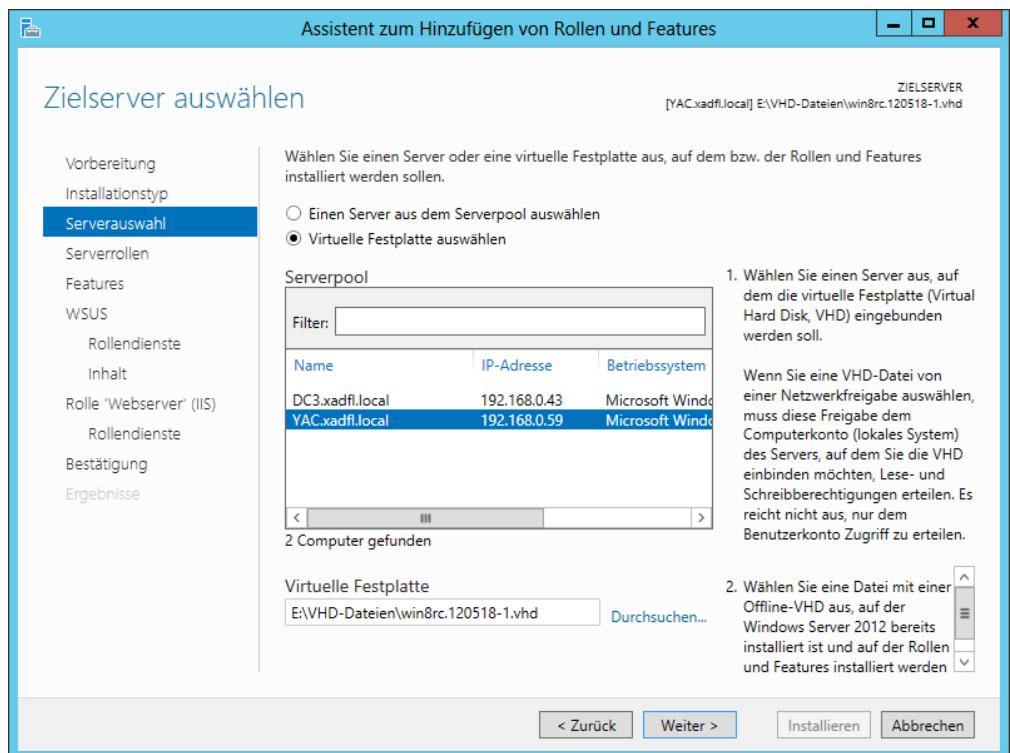


Abbildung 1.19 Die Seite *Zielserver auswählen* im Assistenten zum Hinzufügen von Rollen und Features



Hinweis Was bedeutet es, die VHD-Datei bereitzustellen?

Der Assistent muss die VHD-Datei auf dem ausgewählten Server bereitstellen (mounten), um sie zu inspizieren und zu ermitteln, welche Rollen und Features bereits installiert und welche für eine Installation verfügbar sind. Durch das Bereitstellen wird eine VHD-Datei lediglich über das Dateisystem des Computers zugänglich gemacht; das ist nicht dasselbe wie das Starten des virtuellen Computers mithilfe der VHD-Datei.

8. Wählen Sie die Rolle(n) aus, die Sie auf dem ausgewählten Server installieren möchten, und fügen Sie bei Bedarf die erforderlichen Abhängigkeiten hinzu. Klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Features auswählen*.
9. Wählen Sie alle Features aus, die Sie auf dem ausgewählten Server installieren möchten, und klicken Sie auf *Weiter*. Je nach ausgewählten Features kann die Seite für die Abhängigkeiten erscheinen.
10. Der Assistent zeigt dann Seiten an, die für die gewählten Rollen oder Features spezifisch sind. Hier können Sie Rollendienste auswählen und andere Einstellungen konfigurieren. Vervollständigen Sie die einzelnen rollen- oder featurespezifischen Seiten und klicken Sie auf *Weiter*. Es erscheint eine Bestätigungsseite.
11. Klicken Sie auf *Installieren*. Die Seite *Installationsstatus* wird geöffnet. Klicken Sie nach Abschluss der Installation auf *Schließen*, um die Bereitstellung der VHD aufzuheben und den Assistanten fertigzustellen.

Dienste konfigurieren

Die meisten Rollen und viele der Features von Windows Server umfassen Dienste, d.h. Programme, die ständig im Hintergrund laufen und normalerweise darauf warten, dass ein Clientprozess ihnen eine Anforderung sendet. Server-Manager bietet Zugriff auf Dienste, die auf Servern im gesamten Netzwerk ausgeführt werden.

Auf der Startseite des lokalen Servers im Server-Manager finden Sie unter anderem eine Kachel *Dienste*, wie Abbildung 1.20 zeigt. Diese Kachel listet alle Dienste auf, die auf dem Server installiert sind, und spezifiziert ihre Betriebsstatus sowie ihren Starttyp. Wenn Sie mit der rechten Maustaste auf einen Dienst klicken, bietet das Kontextmenü Befehle, mit denen sich der Dienst starten, beenden, neu starten, anhalten und fortsetzen lässt.

Die Kachel *Dienste* in der Anzeige des Server-Managers ähnelt dem herkömmlichen MMC-Snap-In *Dienste*, wie Sie es aus vorherigen Versionen von Windows Server kennen. Allerdings können Sie einen Dienst im Server-Manager zwar starten und beenden, nicht jedoch seinen Starttyp ändern, der angibt, ob der Dienst automatisch mit dem Betriebssystem gestartet werden soll. Dazu müssen Sie auf das MMC-Snap-In *Dienste* zurückgreifen.

Außerdem erscheint die Kachel *Dienste* im Server-Manager von Windows Server 2012 an verschiedenen Stellen in Server-Manager und zeigt jeweils eine Liste von Diensten für einen anderen Kontext an. Dies ist ein gutes Beispiel für das Organisationsprinzip der neuen Version

des Server-Managers. Dieselben Tools bieten an verschiedenen Stellen eine einheitliche Verwaltungsoberfläche für unterschiedliche Gruppen von Komponenten.

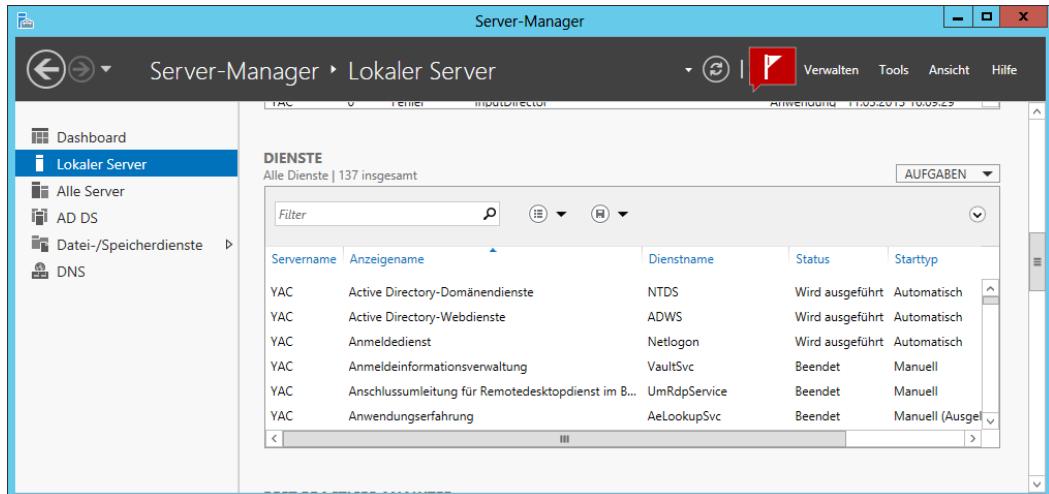


Abbildung 1.20 Die Kachel *Dienste* in Server-Manager

Wenn Sie zum Beispiel das Symbol *Alle Server* im Navigationsbereich auswählen, erscheint zuerst wie üblich die Kachel *Server* mit allen Servern, die Sie der Server-Manager-Konsole hinzugefügt haben. Wählen Sie einige oder alle Server aus und scrollen in der Kachel *Dienste* nach unten, sehen Sie die gleiche Anzeige wie zuvor, die aber jetzt alle Dienste für alle ausgewählten Computer enthält. Damit ist es möglich, die Dienste auf allen Servern gleichzeitig zu überwachen.

Bei Auswahl eines der Rollengruppensymbole können Sie auf die gleiche Weise aus den Servern auswählen, die diese Rolle ausführen, und die Kachel *Dienste* enthält dann nur die Dienste, die dieser Rolle für die ausgewählten Server zugeordnet sind.

Um andere Serverkonfigurationseinstellungen zu bearbeiten, benötigen Sie das MMC-Snap-In *Dienste*, wie bereits oben erwähnt. Allerdings können Sie dieses wie auch viele andere Snap-Ins mithilfe von Server-Manager aufrufen.

Nachdem Sie einen Server aus dem Fensterbereich *Server* einer Gruppenstartseite ausgewählt haben, klicken Sie auf das Menü *Tools*, um eine Liste der serverspezifischen Dienstprogramme und MMC-Snap-Ins (einschließlich des Snap-Ins *Dienste*) anzuzeigen, die für den ausgewählten Server gelten.

Serververwaltung delegieren

Mit zunehmendem Umfang der Netzwerke steigt auch die Anzahl der Verwaltungsaufgaben, die regelmäßig durchzuführen sind, sowie die Anzahl der erforderlichen IT-Mitarbeiter, die diese Aufgaben wahrzunehmen haben. Verwaltungsaufgaben an bestimmte Personen zu delegieren, ist ein selbstverständlicher Bestandteil der Serververwaltung im Unternehmen.

Dabei sind auch die erforderlichen Berechtigungen, die diese Personen für die Ausführung der Aufgaben benötigen – und zwar nur die notwendigen Berechtigungen – zuzuweisen.



Hinweis Berechtigungen delegieren

Weitere Informationen zum Delegieren von Druckerberechtigungen finden Sie im Prüfungsziel 2.2, »Druck- und Dokumentdienste konfigurieren«. Einzelheiten zum Delegieren der Verwaltungskontrolle via Active Directory behandelt das Prüfungsziel 5.3, »Active Directory-Gruppen und Organisationseinheiten erstellen«.

In kleineren Netzwerken mit wenigen IT-Mitarbeitern läuft die Aufgabendelegierung eher leger ab und jeder in der IT-Abteilung erhält vollen Zugriff auf das gesamte Netzwerk. Dagegen erweist sich diese Praxis in größeren Netzwerken mit vielen IT-Mitarbeitern zunehmend als untauglich. Zum Beispiel werden Sie es den neuen Mitarbeitern in der IT-Abteilung zugestehen, neue Benutzerkonten anzulegen, jedoch nicht, Ihre Active Directory-Struktur neu zu gestalten oder das Kennwort des Geschäftsführers zu ändern.

Mithilfe von Delegierung gewähren Administratoren anderen Benutzern eine Teilmenge der Berechtigungen, die sie selbst besitzen. In diesem Sinne ist Delegierung ebenso eine Angelegenheit, Berechtigungen einzuschränken wie sie zu gewähren. Zum einen sollen die betreffenden Personen die benötigten Berechtigungen erhalten, zum anderen sind vertrauliche Informationen und eine empfindliche Infrastruktur zu schützen.



Gedankenexperiment Wenden Sie in diesem Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Dem IT-Mitarbeiter Deepak wurde die Aufgabe übertragen, einen neuen Server unter Windows Server 2012 namens ServerA mit der Option *Server Core* zu konfigurieren. Dieser Computer soll an eine Zweigstelle der Firma ausgeliefert werden. Der Server ist als Dateiserver mit Unterstützung für das verteilte Dateisystem (Distributed File System, DFS), als Druckerserver mit Unterstützung für Internet- und UNIX-Druckvorgänge sowie als gesicherter Intranet-Web-/FTP-Server für Domänenbenutzer zu konfigurieren.

Beantworten Sie für dieses Szenario die folgenden Fragen:

1. Mit welchem Windows PowerShell-Befehl sollte Deepak die erforderlichen Rollen auf den Servern installieren?
2. Mit welchem Windows PowerShell-Befehl kann Deepak die Kurznamen für die Rollen erhalten, wie sie Windows PowerShell verwendet.
3. Listen Sie die Befehle auf, die Deepak auf dem neuen Server ausführen muss, um die erforderlichen Module zu installieren.

Prüfungszielzusammenfassung

- Der neue Server-Manager versetzt Administratoren in die Lage, Windows-Server komplett zu verwalten, ohne mit der Server-Konsole – weder physisch noch remote – interagieren zu müssen
- Es gibt einige Aufgaben, die Administratoren unmittelbar im Anschluss an die Betriebssysteminstallation ausführen und dafür direkt auf die Server-Konsole zugreifen müssen
- Wenn Sie bei der Installation von Windows Server 2012 die Option *Server Core* gewählt haben, können Sie die Aufgaben nach der Installation von der Befehlszeile aus ausführen
- In Windows Server 2012 bietet die Kachel *Eigenschaften* des Server-Managers die gleiche Funktionalität wie das Fenster *Aufgaben der Erstkonfiguration* in vorherigen Windows Server-Versionen
- In Windows Server 2012 können Sie einen Computer, der mit der Option *Server mit grafischer Benutzeroberfläche* eingerichtet ist, in die Option *Server Core* konvertieren und einem Server Core-Computer die grafische Benutzeroberfläche hinzufügen
- Der NIC-Teamvorgang ist ein neues Feature in Windows Server 2012. Damit können Administratoren die Bandbreite von mehreren Netzwerkadapters zusammenfassen und somit eine erhöhte Performance und Fehlertoleranz gewährleisten.
- Administratoren von Unternehmensnetzwerken müssen gegebenenfalls eine große Anzahl von Servern in Server-Manager hinzufügen. Um nicht mit einer langen Auswahlliste von Servern arbeiten zu müssen, können Sie Servergruppen basierend auf Serverstandorten, Funktionen oder anderen organisatorischen Paradigmen einrichten.
- Server-Manager erlaubt es Administratoren nicht nur, Rollen und Features auf Servern im Netzwerk zu installieren, sondern auch auf virtuellen Computern, die sich momentan im Offline-Status befinden

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche Features müssen Sie aus einer vollständigen Installation von Windows Server 2012 mit grafischer Benutzeroberfläche entfernen, um sie in eine Server Core-Installation umzuwandeln? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI)
 - B. Benutzeroberflächen und Infrastruktur
 - C. Desktopdarstellung (Desktop Experience)
 - D. Grafische Shell für Server

2. Welche der folgenden Modi des NIC-Teamvorgangs bieten Fehlertoleranz und Bandbreitenzusammenfassung?
 - A. Hyper-V-Livemigration
 - B. Switchunabhängiger Modus
 - C. Switchabhängiger Modus
 - D. LACP (Link Aggregation Control Protocol)
3. Mit welchen der folgenden Befehlszeilentools verknüpfen Sie einen Computer mit einer Domäne?
 - A. Net.exe
 - B. Netsh.exe
 - C. Netdom.exe
 - D. Ipconfig.exe
4. Welche der folgenden Aussagen ist für den Server-Manager nicht richtig?
 - A. Der Server-Manager kann Rollen auf mehreren Servern auf einmal bereitstellen.
 - B. Der Server-Manager kann Rollen auf VHDs bereitstellen, wenn diese offline sind.
 - C. Der Server-Manager kann Rollen und Features gleichzeitig installieren.
 - D. Der Server-Manager kann Rollen und Features auf jedem Windows Server 2012-Server im Netzwerk installieren.
5. Welche der folgenden Operationen können Sie mithilfe von Server-Manager nicht für einen Dienst ausführen?
 - A. Einen laufenden Dienst beenden
 - B. Einen beendeten Dienst starten
 - C. Einen Dienst deaktivieren
 - D. Einen Dienst so konfigurieren, dass er beim Starten des Computers startet

Prüfungsziel 1.3: Lokalen Speicher konfigurieren

Windows Server 2012 ist zwar für Remotespeicherung und Cloud-Computing ausgelegt, doch spielt die Konfiguration des lokalen Speichers immer noch eine wichtige Rolle.

Dieses Prüfungsziel zeigt, wie Sie:

- Speicherplatz konzipieren
 - Basis- und dynamische Datenträger konfigurieren
 - MBR- und GPT-Datenträger konfigurieren
 - Volumes verwalten
 - Virtuelle Festplatten erstellen und bereitstellen
 - Speicherpools und Festplattenpools konfigurieren
-

Serverspeicher planen

Ein Windows-Server kann seine Aufgaben möglicherweise mit demselben Speichertyp wie eine Arbeitsstation ausführen, d.h. dass eine oder mehrere Standardfestplatten an eine standardmäßige Laufwerkschnittstelle wie zum Beispiel Serial ATA (SATA) angeschlossen sind. Allerdings unterscheiden sich Server und Arbeitsstationen hinsichtlich der E/A-Lasten und ein standardmäßiges Speichersubsystem kann leicht durch Dateianforderungen von Dutzenden oder Hunderten von Benutzern überfordert werden. Darüber hinaus bieten Standardfestplatten keine Fehlertoleranz und sind nur begrenzt skalierbar.

Es gibt eine breite Palette von Speichertechniken, die für den Servereinsatz besser geeignet sind. Der konzeptionelle Entwurf einer Speicherlösung hängt unter anderem von folgenden Faktoren ab:

- Speicherkapazität, die der Server benötigt
- Anzahl der Benutzer, die gleichzeitig auf den Server zugreifen
- Vertraulichkeit der Daten, die auf dem Server zu speichern sind
- Wichtigkeit der Daten für das Unternehmen

Die folgenden Abschnitte untersuchen diese Faktoren und die Techniken, die Sie bei der Planung von Netzwerkspeicherlösungen einbeziehen können.

Wie viele Server sind erforderlich?

Ist ein großer Dateiserver gegenüber mehreren kleineren vorzuziehen? Bei der Planung einer Serverbereitstellung wird oftmals die Frage gestellt, ob ein großer Server besser geeignet ist als mehrere kleine. In der Vergangenheit haben Sie vielleicht die Vor- und Nachteile erörtert, ob Sie mehrere Serverrollen auf einem Server ausführen oder sie auf kleinere Server aufteilen sollen. Heute liegt die Betonung auf Virtualisierung: Obwohl Sie eventuell verschiedene

Rollen auf vielen virtuellen Computern ausführen, können die virtuellen Computer alle auf einem einzigen großen physischen Server laufen.

Wenn Sie große physische Server ins Auge fassen oder wenn die Speicheranforderungen Ihrer Organisation besonders groß sind, müssen Sie auch die Speichergrenzen berücksichtigen, die Windows Server 2012 auferlegt.

Die Anzahl der Standorte, die Ihr Unternehmensnetzwerk umfasst, und die Technologien, die Sie für die Netzwerkkommunikation zwischen diesen Standorten einsetzen, können ebenfalls Ihre Planung beeinflussen. Wenn zum Beispiel Ihre Organisation weltweit mehrere Zweigstellen betreibt und relativ ausgedehnte WAN (Wide Area Network)-Verbindungen zu ihnen unterhält, ist es wahrscheinlich wirtschaftlicher, an jedem Standort einen eigenen Server zu installieren, als sämtliche Benutzer über die WAN-Verbindungen auf einen einzigen Server zugreifen zu lassen.

An den einzelnen Standorten hängt die Anzahl der erforderlichen Server davon ab, wie häufig Ihre Benutzer mit den gleichen Ressourcen arbeiten und wie viel Fehlertoleranz und Hochverfügbarkeit Sie in das System einbauen möchten. Arbeitet zum Beispiel jede Abteilung in Ihrer Organisation mit eigenen Anwendungen und Dokumenten, wobei nur selten Zugriffe auf andere Abteilungen erforderlich sind, ist die Bereitstellung individueller Server für jede Abteilung möglicherweise vorzuziehen. Wenn dagegen alle Mitarbeiter im Unternehmen mit dem gleichen Satz von Ressourcen arbeiten, stellen zentralisierte Server sicherlich die bessere Wahl dar.

Speicheranforderungen abschätzen

Die in einem Server benötigte Speicherkapazität hängt von vielen Faktoren ab, nicht nur von den anfänglichen Anforderungen Ihrer Anwendungen und Benutzer. Für einen Anwendungsserver weisen Sie zunächst die Größe des Speichers zu, der für die Anwendungsdateien selbst erforderlich ist, sowie anderen Speicher, den die Anwendungen entsprechend den Empfehlungen der Entwickler benötigen. Wenn Benutzer die Dokumente auf dem Server speichern, weisen sie einen bestimmten Betrag des Speichers für jeden Benutzer zu, den der Server unterstützt. Dann kalkulieren Sie das mögliche Wachstum Ihrer Organisation und des Netzwerks ein, und zwar sowohl in Bezug auf zusätzliche Benutzer und den zusätzlich von jedem Benutzer benötigten Speicher als auch auf Datendateien und Updates für die Anwendungen selbst.

Storage Spaces verwenden

Windows Server 2012 führt mit den sogenannten *Storage Spaces* (Speicherplätzen) eine neue Datenträgervirtualisierungstechnik ein. Server können damit die Speicherkapazität von einzelnen physischen Datenträgern verketten und diesen Platz zuordnen, um virtuelle Datenträger jeder beliebigen Größe, die von der Hardware unterstützt wird, zu schaffen.

Diese Art der Virtualisierung ist ein Feature, das oftmals in SAN (Storage Area Network)- und NAS (Network Attached Storage)-Techniken zu finden ist, die beträchtliche Investitionen in spezialisierte Hardware und administrative Fertigkeiten verlangen. Storage Spaces bieten

ähnliche Fähigkeiten, indem sie direkt angeschlossene Standardfestplatten oder einfache externe JBOD (»Just a Bunch Of Disks)-Arrays verwenden.

Storage Spaces erstellen Speicherpools aus nicht zugeordnetem Festplattenplatz auf Serverlaufwerken. Ein *Speicherpool* kann sich unsichtbar über mehrere Laufwerke erstrecken und liefert eine akkumulierte Speicherressource. Administratoren können diese bei Bedarf erweitern oder verringern, indem sie Datenträger in den Pool einfügen oder daraus entfernen. Mit dem Platz im Pool sind Administratoren in der Lage, *virtuelle Datenträger* beliebiger Größe einzurichten.

Nachdem ein virtueller Datenträger erstellt ist, verhält er sich genau wie ein physischer Datenträger, außer dass die eigentlichen Daten auf einer beliebigen Anzahl physischer Laufwerke im System gespeichert sein können. Virtuelle Datenträger können auch eine Fehlertoleranz realisieren, indem sie auf den physischen Festplatten im Speicherpool gespiegelte oder Paritätsdaten speichern.

Auf einem virtuellen Datenträger können Sie Volumes einrichten, genauso wie Sie es von einer physischen Festplatte her kennen. Server-Manager stellt die erforderlichen Tools bereit, mit denen sich Speicherpools und virtuelle Datenträger erstellen und verwalten lassen. Mit gewissen Einschränkungen ist es auch möglich, Volumes und Dateifreigaben zu erstellen.

Windows-Datenträgereinstellungen

Bei der Installation von Windows Server 2012 führt das Setupprogramm automatisch alle Vorbereitungsarbeiten für den primären Datenträger im System durch. Wenn Sie jedoch zusätzliche Festplattenlaufwerke auf einem Server installieren oder Einstellungen verwenden möchten, die von den Systemstandardwerten abweichen, müssen Sie die folgenden Aufgaben manuell erledigen:

- **Einen Partitionsstil auswählen** Windows Server 2012 unterstützt zwei Datenträgerpartitionsstile: MBR (Master Boot Record) und GPT (GUID Partition Table). Es ist nicht möglich, beide Stile auf demselben Laufwerk zu verwenden – Sie müssen sich für einen der beiden Partitionsstile entscheiden.
- **Einen Datenträgertyp auswählen** Windows Server 2012 unterstützt zwei Datenträgertypen: Basis und dynamisch. Es ist nicht möglich, beide Typen auf demselben Laufwerk zu verwenden. Im selben Computer können Sie jedoch beide Typen gemischt einsetzen.
- **Den Datenträger in Partitionen oder Volumes unterteilen** Obwohl viele Profis die Begriffe Partition und Volume gleichberechtigt verwenden, ist es korrekt, von Partitionen auf Basisdatenträgern und von Volumes auf dynamischen Datenträgern zu sprechen
- **Die Partitionen oder Volumes mit einem Dateisystem formatieren** Windows Server 2012 unterstützt die Dateisysteme NTFS, FAT (einschließlich der Varianten FAT16, FAT32 und exFAT) und das neue ReFS

Die folgenden Abschnitte befassen sich mit den Optionen für jede dieser Aufgaben.

Einen Partitionsstil auswählen

Der Begriff *Partitionsstil* bezieht sich auf die Methode, nach der das Windows-Betriebssystem die Partitionen auf der Festplatte organisiert. Server, die Windows Server 2012 ausführen, können einen der beiden folgenden Datenträgerpartitionsstile verwenden:

- **MBR** Diesen Partitionsstil gab es schon vor Windows und er ist für x86- und x64-basierte Computer immer noch gebräuchlich
- **GPT** Dieser Partitionsstil existiert seit Ende der 1990er Jahre, wird aber von keiner x86-Version von Windows vor Windows Server 2008 und Windows Vista unterstützt. Heute wird GPT von den meisten Betriebssystemen einschließlich Windows Server 2012 unterstützt.

Vor Windows Server 2008 und Windows Vista haben alle x86-basierten Windows-Computer ausschließlich den MBR-Partitionsstil verwendet. Computer, die auf der x64-Plattform basierten, konnten entweder den MBR- oder den GPT-Partitionsstil verwenden, sofern es sich beim GPT-Datenträger nicht um den Bootdatenträger handelte.

Das Booten von einer GPT-Festplatte ist nur möglich, wenn die Architektur des Computers eine EFI (Extensible Firmware Interface)-basierte Bootpartition unterstützt. Andernfalls muss das Systemlaufwerk ein MBR-Datenträger sein und GPT können Sie nur auf separaten Festplatten, die nicht bootfähig sind, zur Datenspeicherung verwenden.

Wenn Sie einen Datenträger in Windows Server 2012 mithilfe von Server-Manager initialisieren, wird der GPT-Partitionsstil verwendet, egal ob es sich um einen physischen oder einen virtuellen Datenträger handelt. Server-Manager besitzt keine Steuerelemente, die MBR unterstützen, zeigt aber den Partitionsstil in der Kachel *Datenträger* an.

Datenträgertypen

Die meisten Personalcomputer verwenden Basisfestplatten, da sie am einfachsten zu verwalten sind. Erweiterte Volumetypen setzen dynamische Festplatten voraus. Auf einer *Basisfestplatte* mit dem MBR-Partitionsstil lassen sich primäre und erweiterte Partitionen sowie logische Laufwerke einrichten, um Daten zu organisieren. Eine *primäre Partition* stellt sich für das Betriebssystem wie eine physisch separate Festplatte dar. Sie kann ein Betriebssystem hosten und wird in diesem Fall als die *aktive Partition* bezeichnet.

In Windows Server 2012 können Sie auf MBR-Basisfestplatten drei Volumes im Format primärer Partitionen erstellen. Wenn Sie das vierte Volume anlegen, erzeugt das System eine erweiterte Partition mit einem logischen Laufwerk der angegebenen Größe. Bleibt noch Platz auf der Festplatte frei, weist das System ihn der erweiterten Partition zu (siehe Abbildung 1.21), wo Sie zusätzliche logische Laufwerke einrichten können.

(C:) 97,66 GB NTFS Fehlerfrei (System, Start)	(D:) 48,83 GB NTFS Fehlerfrei (Primäre Par)	(E:) 48,83 GB NTFS Fehlerfrei (Primäre Par)	Volume (G:) 39,06 GB NTFS Fehlerfrei (Logisches)	231,04 GB Freier Speicherplatz
---	---	---	--	--------------------------------

Abbildung 1.21 Primäre und erweiterte Partitionen auf einer Basisfestplatte mit MBR

Haben Sie den GPT-Partitionsstil ausgewählt, erscheint der Datenträger immer noch als Basisfestplatte, doch können Sie jetzt bis zu 128 Volumes als primäre Partitionen erstellen (siehe Abbildung 1.22). Auf GPT-Datenträgern gibt es weder erweiterte Partitionen noch logische Laufwerke.

Volume (H:) 9,77 GB NTFS Fehlerfrei (Primä)	Volume (I:) 9,77 GB NTFS Fehlerfrei (Primä)	Volume (J:) 9,77 GB NTFS Fehlerfrei (Primä)	Volume (K:) 9,77 GB NTFS Fehlerfrei (Primä)	Volume (L:) 9,77 GB NTFS Fehlerfrei (Primä)	100,10 GB Nicht zugeordnet
---	---	---	---	---	-------------------------------

Abbildung 1.22 Primäre Partitionen auf einem Basisdatenträger mit GPT

Die Alternative zur Basisfestplatte ist eine *dynamische Festplatte*. Wenn Sie eine Basisfestplatte in eine dynamische Festplatte konvertieren, wird eine einzige Partition erstellt, die den gesamten Datenträger einnimmt. Aus dem Speicherplatz in dieser Partition können Sie dann eine unbegrenzte Anzahl von Volumes erzeugen. Dynamische Festplatten unterstützen mehrere unterschiedliche Volumetypen, wie sie der nächste Abschnitt beschreibt.

Volumetypen

Eine dynamische Festplatte kann eine unbegrenzte Anzahl von Volumes enthalten, die ähnlich wie primäre Partitionen auf einer Basisfestplatte arbeiten. Allerdings lässt sich eine vorhandene dynamische Festplatte nicht als aktiv markieren. Wenn Sie ein Volume auf einer dynamischen Festplatte mit dem Snap-In *Datenträgerverwaltung* in Windows Server 2012 erstellen, stehen Ihnen die folgenden fünf Volumetypen zur Auswahl:

- **Einfaches Volume** Besteht aus dem Speicherplatz einer einzigen Festplatte. Nachdem Sie ein einfaches Volume eingerichtet haben, können Sie es auf mehrere Datenträger erweitern, um ein übergreifendes oder Stripesetvolume zu erstellen, sofern es sich nicht um ein System- oder Startvolume handelt. Außerdem können Sie ein einfaches Volume zu beliebigem angrenzenden nicht zugeordneten Speicherplatz auf derselben Festplatte erweitern oder – mit gewissen Einschränkungen – das Volume verkleinern, indem Sie die Zuordnung von ungenutztem Speicherplatz im Volume aufheben.
- **Übergreifendes Volume** Besteht aus dem Speicherplatz von 2 bis 32 physischen Festplatten, bei denen es sich durchweg um dynamische Festplatten handeln muss. Ein übergreifendes Volume ist praktisch eine Methode, um den Platz von mehreren dynamischen Festplatten zu einem einzigen großen Volume zusammenzufassen. Windows Server 2012 schreibt auf das übergreifende Volume, indem zunächst der gesamte Platz auf der ersten Festplatte gefüllt wird und dann nacheinander die zusätzlichen Festplatten belegt werden. Ein übergreifendes Volume lässt sich jederzeit durch zusätzlichen Festplattenplatz erweitern. Mit einem übergreifenden Volume wird weder die Lese-/Schreibperformance der Festplatte erhöht noch Fehlertoleranz realisiert. In der Konsequenz gehen alle Daten im gesamten Volume verloren, wenn eine physische Festplatte im übergreifenden Volume ausfällt.
- **Stripesetvolume** Besteht aus dem Speicherplatz von 2 bis 32 physischen Festplatten, bei denen es sich durchweg um dynamische Festplatten handeln muss. Der Unterschied zu

einem übergreifenden Volume besteht darin, dass das System bei einem Stripesetvolume die Daten streifenweise auf die aufeinanderfolgenden Festplatten im Volume schreibt. Diese Technik verbessert die Performance, da jede Festplatte im Array die Zeit hat, den nächsten Ort ihres nächsten Stripes zu suchen, während die anderen Festplatten schreiben. Stripesetvolumes bieten allerdings keine Fehlertoleranz und sie lassen sich nach dem Erstellen auch nicht erweitern. Fällt eine einzige physische Festplatte im Stripesetvolume aus, gehen sämtliche Daten im gesamten Volume verloren.

- **Gespiegeltes Volume** Besteht aus gleich großen Speicherbereichen auf zwei physischen Festplatten, die beide dynamische Festplatten sein müssen. Das System führt alle Lese- und Schreiboperationen auf beiden Festplatten gleichzeitig durch, sodass die auf dem Volume gespeicherten Daten doppelt vorhanden sind. Fällt eine der Festplatten aus, stellt die andere Festplatte den Zugriff auf das Volume sicher, bis die ausgefallene Festplatte repariert oder ersetzt worden ist.
- **RAID-5-Volume** Belegt Speicherplatz auf drei oder mehr physischen Festplatten, bei denen es sich durchweg um dynamische Festplatten handeln muss. Das System schreibt Daten und Paritätsinformationen streifenweise über alle Festplatten hinweg, sodass sich bei Ausfall einer physischen Festplatte die fehlenden Daten anhand der Paritätsinformationen auf den anderen Festplatten wiederherstellen lassen. RAID-5-Volumes bieten aufgrund der Stripetechnik eine höhere Leseperformance, wohingegen die Schreibleistung wegen der erforderlichen Paritätsberechnungen leidet.

Dateisysteme

Um Daten oder Programme auf einer Festplatte zu speichern und zu organisieren, ist ein *Dateisystem* zu installieren. Ein Dateisystem bildet die zugrundeliegende Laufwerkstruktur, die es erlaubt, Informationen auf dem Computer zu speichern. Ein Dateisystem installieren Sie, indem Sie eine Partition oder ein Volume auf der Festplatte formatieren.

In Windows Server 2012 sind fünf Dateisystemoptionen verfügbar: NTFS, FAT32, exFAT, FAT (auch als FAT16 bekannt) und ReFS. NTFS ist das bevorzugte Dateisystem für einen Server. Gegenüber FAT bietet es den Vorteil, größere Festplattenlaufwerke zu unterstützen. Zudem bietet es bessere Sicherheit in Form von Verschlüsselung und Berechtigungen, die den Zugriff durch nicht autorisierte Benutzer einschränken.

Da dem FAT-Dateisystem die Sicherheitsmechanismen des NTFS-Dateisystems fehlen, kann jeder Benutzer, der Zugang zum Computer hat, jede beliebige Datei ohne Einschränkung lesen. Darüber hinaus weisen FAT-Dateisysteme Beschränkungen hinsichtlich der Festplattengröße auf: FAT32 kommt nur mit Partitionen bis zu 32 GB oder Dateien bis zu 4 GB zurecht. FAT ist nicht für Festplatten größer als 4 GB oder Dateien größer als 2 GB geeignet. Aufgrund dieser Beschränkungen ist FAT16 oder FAT32 praktisch nur erforderlich, um einen Dual-Boot des Computers mit einem Nicht-Windows-Betriebssystem oder einer vorherigen Windows-Version, die kein NTFS unterstützt, zu ermöglichen. Für einen Server kommt eine derartige Konfiguration höchstwahrscheinlich nicht in Betracht.

ReFS ist ein neues Dateisystem, das mit Windows Server 2012 eingeführt wurde und praktisch unbegrenzte Datei- und Verzeichnisgrößen erlaubt und wesentlich robuster ist, was Fehlerprüfungstools wie zum Beispiel *Chkdsk.exe* überflüssig macht. Allerdings bringt ReFS keine

Unterstützung für NTFS-Features wie zum Beispiel Dateikomprimierung, verschlüsseltes Dateisystem (Encrypted File System, EFS) und Datenträgerkontingente mit. Außerdem lassen sich ReFS-Datenträger nicht von Betriebssystemen lesen, die älter als Windows Server 2012 bzw. Windows 8 sind.

Mit Datenträgern arbeiten

Windows Server 2012 umfasst Tools, mit denen Sie Datenträger grafisch oder von der Eingabeaufforderung verwalten können. Alle Windows Server 2012-Installationen enthalten die Rolle *Datei- und Speicherdiene*s. Diese ist dafür zuständig, dass der Server-Manager ein Untermenü anzeigt, wenn Sie auf das Symbol im Navigationsbereich klicken, wie Abbildung 1.23 zeigt. Das Untermenü bietet Verweise auf Startseiten, wo Administratoren Volumes, Datenträger, Speicherpools, Freigaben und iSCSI-Geräte verwalten können.

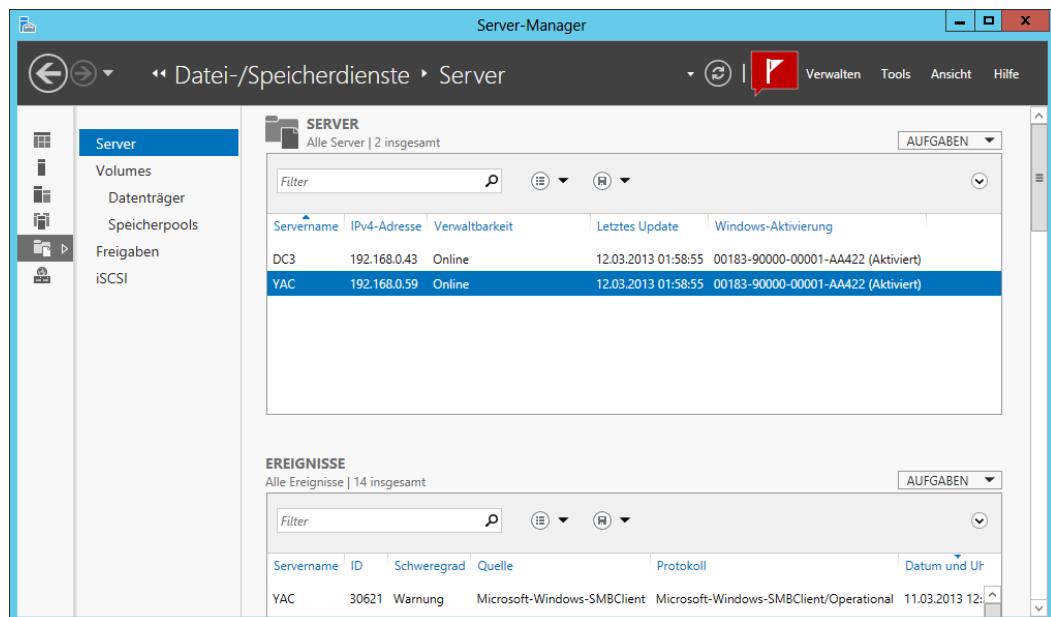


Abbildung 1.23 Das Untermenü *Datei-/Speicherdiene* in Server-Manager

Server-Manager ist das einzige grafische Tool, das Speicherpools verwalten und virtuelle Festplatten erzeugen kann. Außerdem ist es in der Lage, einige – wenn auch nicht alle – Datenträger- und Volume-Verwaltungsoperationen auf physischen Festplatten durchzuführen. Wie die anderen Startseiten von Server-Manager ermöglicht es die Seite *Datei-/Speicherdiene*, Aufgaben auf beliebigen Servern durchzuführen, die Sie der Benutzeroberfläche hinzugefügt haben.

Das MMC-Snap-In *Datenträgerverwaltung* ist das herkömmliche Tool, mit dem sich datenträgerbezogene Aufgaben erledigen lassen. Um auf dieses Snap-In zuzugreifen, öffnen Sie die Konsole *Computerverwaltung* und wählen *Datenträgerverwaltung* aus. Außerdem

können Sie Festplatten und Volumes von der Befehlszeile aus mit dem Dienstprogramm *DiskPart.exe* verwalten.

Eine neue physische Festplatte hinzufügen

Wenn Sie einem Windows Server 2012-Computer eine neue Festplatte hinzufügen, müssen Sie den Datenträger formatieren, bevor Sie auf seinen Speicherplatz zugreifen können. Um eine neue sekundäre Festplatte hinzuzufügen, fahren Sie den Computer herunter und bauen die neue physische Festplatte den Herstelleranweisungen entsprechend ein. Eine neu hinzugefügte physische Festplatte erscheint im Server-Manager in der Kachel *Datenträger*, wie Abbildung 1.24 zeigt, wobei der Status auf *Offline* gesetzt und der Partitionsstil mit *Unbekannt* angegeben ist.

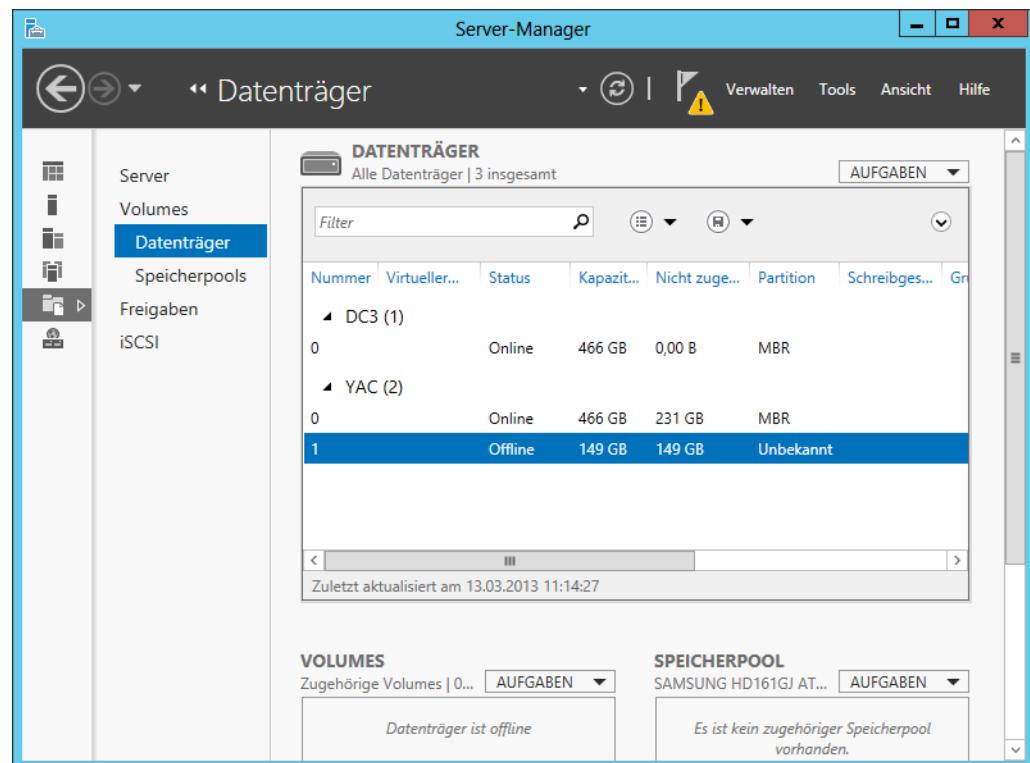


Abbildung 1.24 Eine neue physische Festplatte in Server-Manager

Damit Sie auf die Festplatte zugreifen können, müssen Sie sie zuerst in den Onlinestatus versetzen. Klicken Sie dazu mit der rechten Maustaste in der Kachel *Datenträger* und wählen Sie im Kontextmenü den Befehl *Online schalten*. Nachdem Sie die Aktion bestätigt haben und der Festplattenstatus *Online* zeigt, klicken Sie mit der rechten Maustaste darauf und wählen *Initialisieren*.

Im Unterschied zum Snap-In *Datenträgerverwaltung* ist es im Server-Manager nicht möglich, den Partitionsstil für die Festplatte auszuwählen. Es erscheint ein Fenster *Aufgabenstatus*. Ist

der Vorgang abgeschlossen, klicken Sie auf *Schließen*. Daraufhin erscheint die Festplatte in der Liste mit dem auf *GPT* gesetzten Partitionsstil.

Den Partitionsstil einer Festplatte können Sie jederzeit (im Snap-In *Datenträgerverwaltung*) wechseln. Klicken Sie dazu mit der rechten Maustaste auf die betreffende Festplatte und wählen Sie im Kontextmenü den Befehl *Zu GPT-Datenträger konvertieren* bzw. *Zu MBR-Datenträger konvertieren*. Seien Sie sich aber bewusst, dass das Konvertieren des Partitionsstils ein destruktiver Vorgang ist. Die Konvertierung können Sie nur auf einem nicht zugeordneten Datenträger durchführen. Enthält also die zu konvertierende Festplatte bereits Daten, müssen Sie sie sichern und dann alle vorhandenen Partitionen oder Volumes löschen, bevor Sie mit der Konvertierung beginnen.

Virtuelle Festplatten erzeugen und bereitstellen

Hyper-V stützt sich auf das VHD-Format, um virtuelle Datenträgerdaten in Dateien zu speichern, die sich leicht von einem Computer auf einen anderen übertragen lassen. Mit dem Snap-In *Datenträgerverwaltung* in Windows Server 2012 können Sie VHD-Dateien erzeugen und sie auf dem Computer bereitstellen. Danach können Sie sie genau wie physische Datenträger behandeln und darauf Daten speichern. Wenn Sie die Bereitstellung einer virtuellen Festplatte aufheben, werden die gespeicherten Daten in der Datei gepackt, sodass Sie sie bei Bedarf kopieren oder verschieben können.

Führen Sie die folgenden Schritte aus, um eine virtuelle Festplatte in der *Datenträgerverwaltung* zu erstellen:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Daraufhin erscheint das Fenster *Server-Manager*.
2. Klicken Sie auf *Tools/Computerverwaltung*. Die Konsole *Computerverwaltung* wird geöffnet.
3. Klicken Sie auf *Datenträgerverwaltung*, um das gleichnamige Snap-In zu öffnen.
4. Im Menü *Aktion* wählen Sie *Virtuelle Festplatte erstellen*. Daraufhin erscheint das Dialogfeld *Virtuelle Festplatte erstellen und anfügen*, wie es Abbildung 1.25 zeigt.
5. Geben Sie im Textfeld *Ort* den Pfad und Dateinamen für die Datei an, die Sie erstellen möchten.
6. Im Feld *Größe der virtuellen Festplatte* legen Sie die maximale Größe der zu erstellenden Festplatte fest.
7. Wählen Sie eine der folgenden Optionen für *Format der virtuellen Festplatte*:
 - **VHD** Das ursprüngliche und kompatiblere Format, das Dateien bis zu 2.040 GB unterstützt
 - **VHDX** Eine neue Version des Formats, das Dateien bis zu 64 TB unterstützt, das sich jedoch nur auf Windows Server 2012-Computern lesen lässt

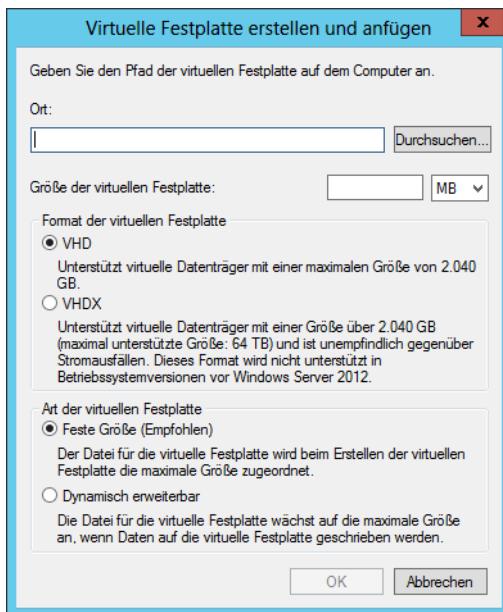


Abbildung 1.25 Das Dialogfeld *Virtuelle Festplatte erstellen und anfügen*

8. Wählen Sie eine der folgenden Optionen für *Art der virtuellen Festplatte*:
 - **Feste Größe (Empfohlen)** Ordnet den gesamten Festplattenplatz für die VHD-Datei sofort zu
 - **Dynamisch erweiterbar** Ordnet Festplattenplatz der VHD-Datei hinzu, wenn Sie neue Daten auf die virtuelle Festplatte schreiben
9. Klicken Sie auf *OK*. Das System erstellt die VHD-Datei und fügt sie an, sodass sie im Snap-In als Datenträger erscheint.

Wenn Sie die virtuelle Festplatte erstellt und angefügt haben, erscheint sie im Snap-In *Datenträgerverwaltung* und im Server-Manager als nicht initialisierte Festplatte. Mit beiden Tools können Sie die Festplatte initialisieren und Volumes darauf erstellen, genau wie bei einer physischen Festplatte. Nachdem Sie Daten auf den Volumes gespeichert haben, können Sie die virtuelle Festplatte trennen und sie an einen anderen Standort verschieben oder auf einem virtuellen Computer unter Hyper-V bereitstellen.

Einen Speicherpool erstellen

Nachdem Sie Ihre physischen Festplatten installiert haben, können Sie deren Speicherplatz in einem Speicherpool verketten, aus dem sich virtuelle Festplatten beliebiger Größe erstellen lassen.

Führen Sie die folgenden Schritte aus, um mithilfe von Server-Manager einen Speicherpool zu erstellen:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Es erscheint das Fenster *Server-Manager*.
2. Klicken Sie auf das Symbol *Datei-/Speicherdienste* und in dem erscheinenden Unter-menü auf *Speicherpools*. Damit gelangen Sie zur Seite *Speicherpools*, wie sie Abbildung 1.26 zeigt.

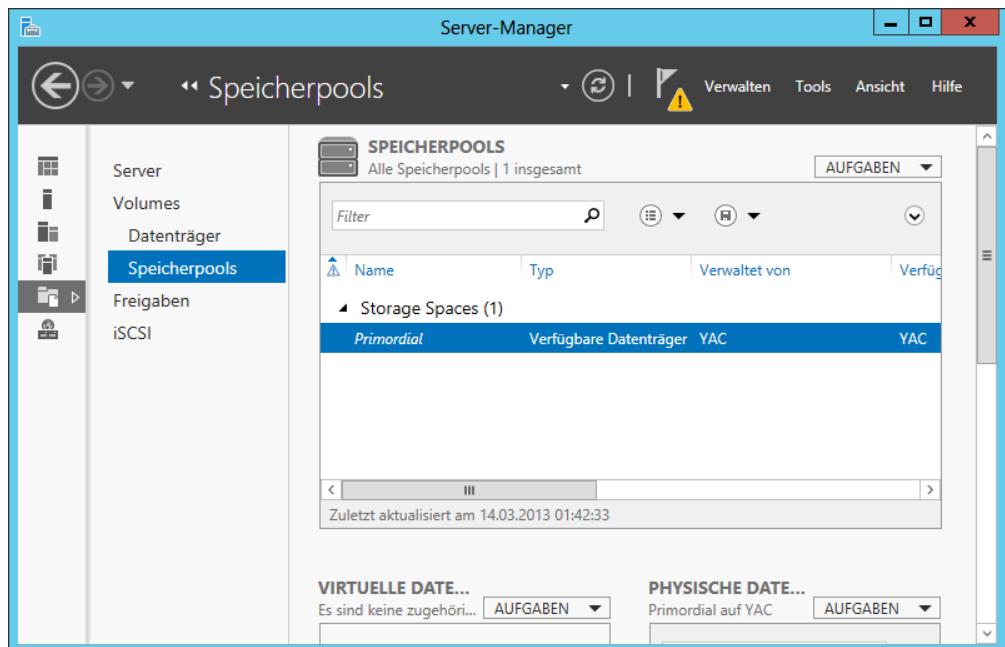


Abbildung 1.26 Die Startseite *Speicherpools*

3. In der Kachel *Speicherpools* wählen Sie den ursprünglichen Platz (*Primordial*) auf dem Server, wo Sie den Pool erstellen möchten, und im Menü *Aufgaben* wählen Sie dann *Neuer Speicherpool*. Nun startet der Assistent für neue Speicherpools und zeigt die Seite *Vorbemerkungen* an.
4. Klicken Sie auf *Weiter*. Es erscheint die Seite *Name und Subsystem für Speicherpool angeben*, wie sie in Abbildung 1.27 zu sehen ist.
5. Geben Sie in das Feld *Name* den Namen ein, den Sie dem Speicherpool zuweisen möchten. Wählen Sie dann den Server aus, auf dem der Pool erstellt werden soll, und klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Physische Laufwerke für den Speicherpool auswählen* (siehe Abbildung 1.28).

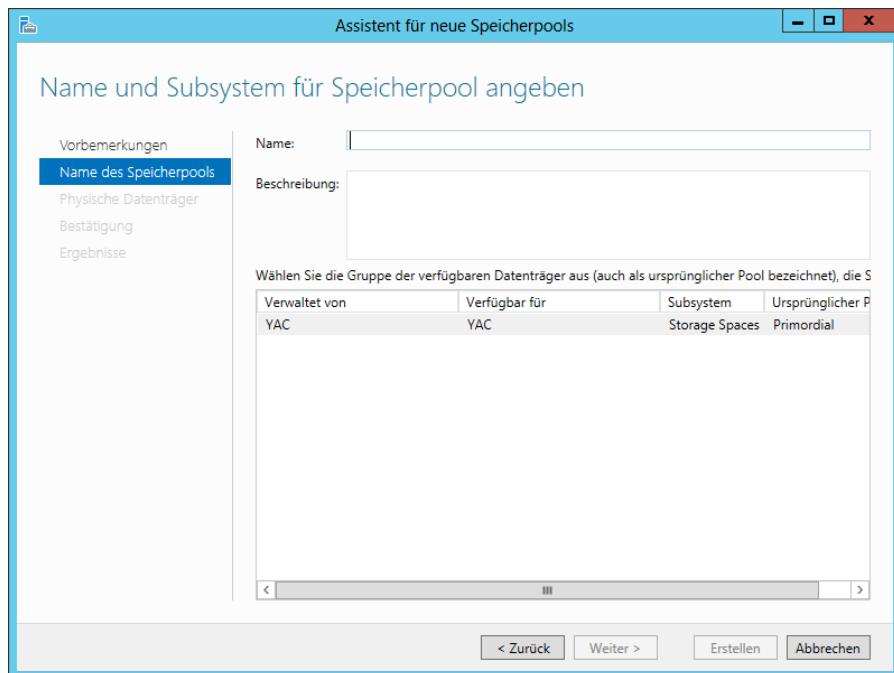


Abbildung 1.27 Die Seite *Name und Subsystem für Speicherpool angeben*

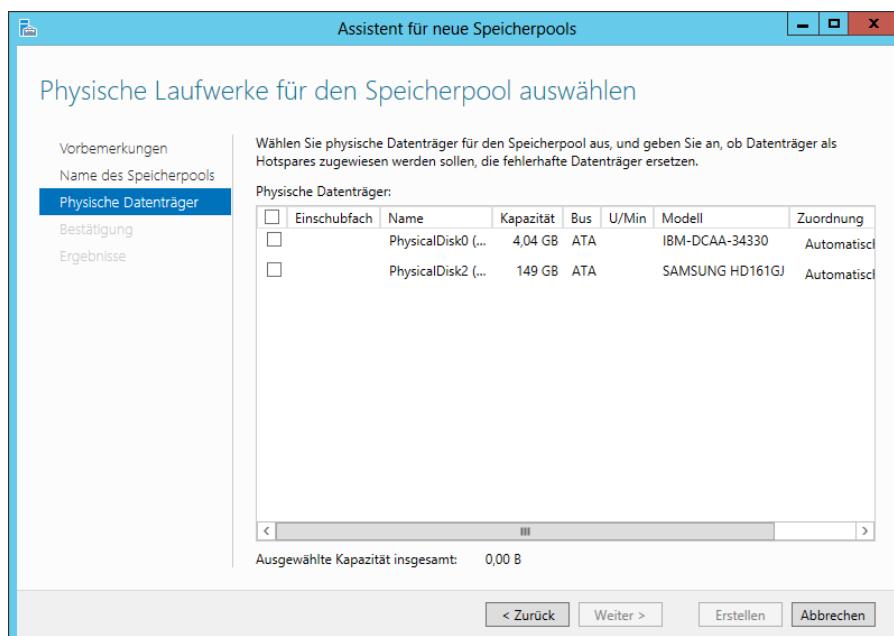


Abbildung 1.28 Die Seite *Physische Laufwerke für den Speicherpool auswählen*



Hinweis Der Assistent zeigt nur geeignete Festplatten an

Der Assistent zeigt nur diejenigen Festplatten an, die sich in den Pool hinzufügen lassen. Festplatten, die bereits Partitionen oder Volumes enthalten, erscheinen nicht.

6. Aktivieren Sie die Kontrollkästchen für die Festplatten, die Sie dem Pool hinzufügen möchten, und klicken Sie auf *Weiter*. Es erscheint die Seite *Auswahl bestätigen*.
7. Klicken Sie auf *Erstellen*. Der Assistent erstellt den neuen Speicherpool und öffnet die Seite *Ergebnisse anzeigen*.
8. Klicken Sie auf *Schließen*. Der Assistent wird beendet und der neue Pool erscheint auf der Startseite *Speicherpools*, wie Abbildung 1.29 zeigt.

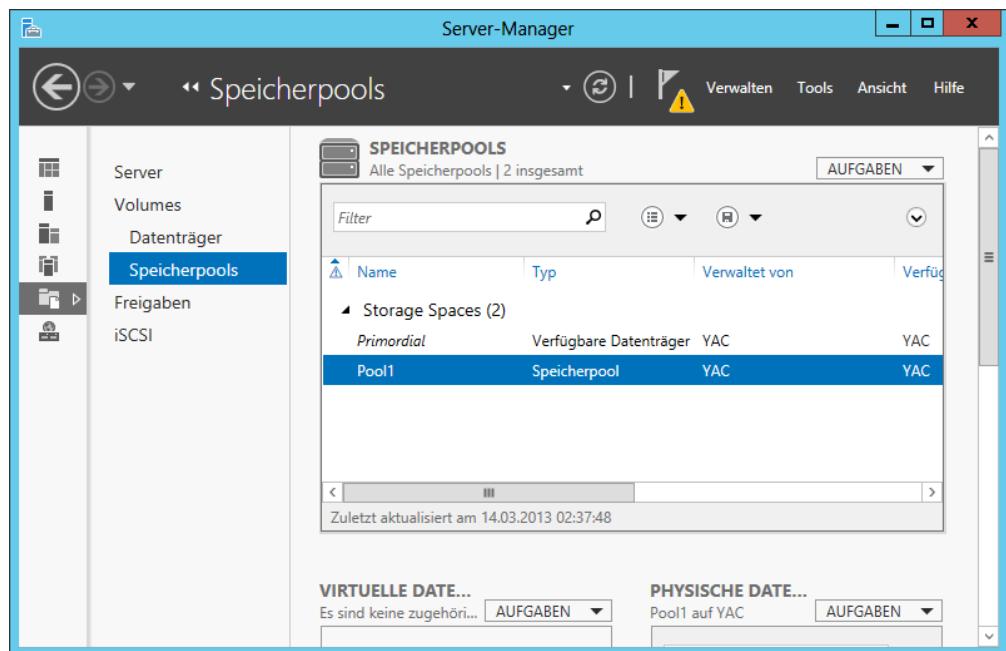


Abbildung 1.29 Ein neuer Pool auf der Startseite *Speicherpools*

9. Schließen Sie das Fenster *Server-Manager*.

Wenn Sie einen Speicherpool erstellt haben, können Sie physische Festplatten hinzufügen oder entfernen, um die Kapazität des Pools zu ändern. Das Menü *Aufgaben* in der Kachel *Physische Datenträger* auf der Startseite *Speicherpools* enthält die folgenden Optionen:

- **Physischen Datenträger hinzufügen** Fügt dem Pool eine physische Festplatte hinzu, sofern sie initialisiert ist und keine Volumes enthält
- **Datenträger zurücksetzen** Bereitet eine physische Festplatte zum Entfernen aus dem Speicherpool vor, indem alle darauf enthaltenen Daten auf die anderen physischen

Festplatten im Pool verschoben werden. Dadurch kann der Status von virtuellen Festplatten, die Spiegel- oder Paritätsfehlertoleranz verwenden, auf *Warnung* zurückgesetzt werden, wenn die Anzahl der physischen Festplatten im Pool wegen der Zurücksetzung unter das erforderliche Minimum fällt.

- **Datenträger entfernen** Entfernt den Platz, den eine physische Festplatte bereitstellt, aus dem Speicherpool. Diese Option erscheint nur, wenn bereits sämtliche Daten von der Festplatte entfernt wurden.

Einen neuen Speicherpool können Sie auch per Windows PowerShell erstellen. Verwenden Sie dazu das Cmdlet `New-StoragePool` mit der folgenden grundlegenden Syntax:

```
New-StoragePool -FriendlyName <Poolname> -StorageSubSystemFriendlyName <Name des Subsystems>
-PhysicalDisks <Datenträgernamen>
```

Mit den Cmdlets `Get-StorageSubsystem` und `Get-PhysicalDisk` lassen sich die richtigen Bezeichner für das Speichersubsystem und die physischen Festplatten abrufen.

Virtuelle Festplatten erzeugen

Den Speicherplatz des erstellten Speicherpools können Sie nun verwenden und je nach Bedarf beliebig viele virtuelle Festplatten erzeugen.

Führen Sie die folgenden Schritte aus, um mithilfe von Server-Manager eine virtuelle Festplatte zu erstellen:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Es erscheint das Fenster *Server-Manager*.
2. Klicken Sie auf das Symbol *Datei- und Speicherdiene* und im eingeblendeten Unter- menü auf *Speicherpools*. Die Startseite *Speicherpools* erscheint.
3. Scrollen Sie (falls erforderlich) nach unten bis zur Kachel *Virtuelle Datenträger* und wählen Sie im Menü *Aufgaben* den Befehl *Neuer virtueller Datenträger*. Daraufhin startet der Assistent für neue virtuelle Datenträger und zeigt die Seite *Vorbemerkungen* an.
4. Klicken Sie auf *Weiter*, um die Seite *Speicherpool auswählen* zu öffnen.
5. Wählen Sie den Pool aus, in dem Sie eine virtuelle Festplatte erstellen möchten, und klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Geben Sie den Namen des virtuellen Datenträgers an*.
6. Geben Sie in das Textfeld *Name* einen Namen für die virtuelle Festplatte ein und klicken Sie auf *Weiter*. Es wird die Seite *Wählen Sie die Speicheranordnung aus* geöffnet, die in Abbildung 1.30 zu sehen ist.

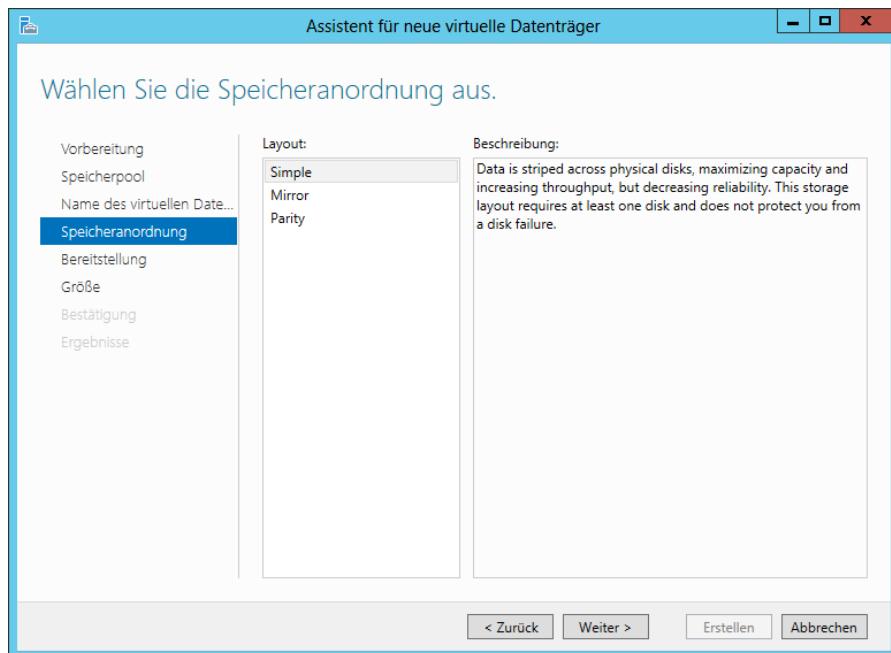


Abbildung 1.30 Die Seite *Wählen Sie die Speicheranordnung aus*

7. Wählen Sie eine der folgenden Layoutoptionen aus und klicken Sie auf *Weiter*:
 - **Simple (Einfach)** Setzt voraus, dass der Pool mindestens eine physische Festplatte enthält, und bietet keine Fehlertoleranz. Stehen mehrere physische Festplatten zur Verfügung, verteilt das System die Daten in Stripes über den Festplatten.
 - **Mirror (Spiegel)** Setzt voraus, dass der Pool mindestens zwei physische Festplatten enthält, und realisiert Fehlertoleranz, indem identische Kopien jeder Datei gespeichert werden. Zwei physische Festplatten bieten Schutz gegen einen einzelnen Festplattenausfall; bei fünf physischen Festplatten ist der Schutz für den Ausfall von zwei Festplatten gegeben.
 - **Parity (Parität)** Setzt voraus, dass der Pool mindestens drei physische Festplatten enthält, und realisiert Fehlertoleranz, indem Paritätsinformationen zusammen mit den Daten in Form von Stripesets gespeichert werden.



Wichtig Fehlertoleranz auf Festplattenebene

Die in Storage Spaces integrierte Fehlertoleranz wird auf der Festplattenebene realisiert, nicht auf der Volumeebene, wie im Snap-In *Datenträgerverwaltung*. Theoretisch können Sie über die Datenträgerverwaltung gespiegelte oder RAID-5-Volumes aus virtuellen Festplatten heraus erstellen, doch würde das dem Zweck ihrer Erstellung von vornherein zuwiderlaufen, da sich die virtuellen Festplatten auf derselben physischen Festplatte befinden können.

8. Es wird die Seite *Geben Sie den Bereitstellungstyp an* geöffnet, die Abbildung 1.31 zeigt.

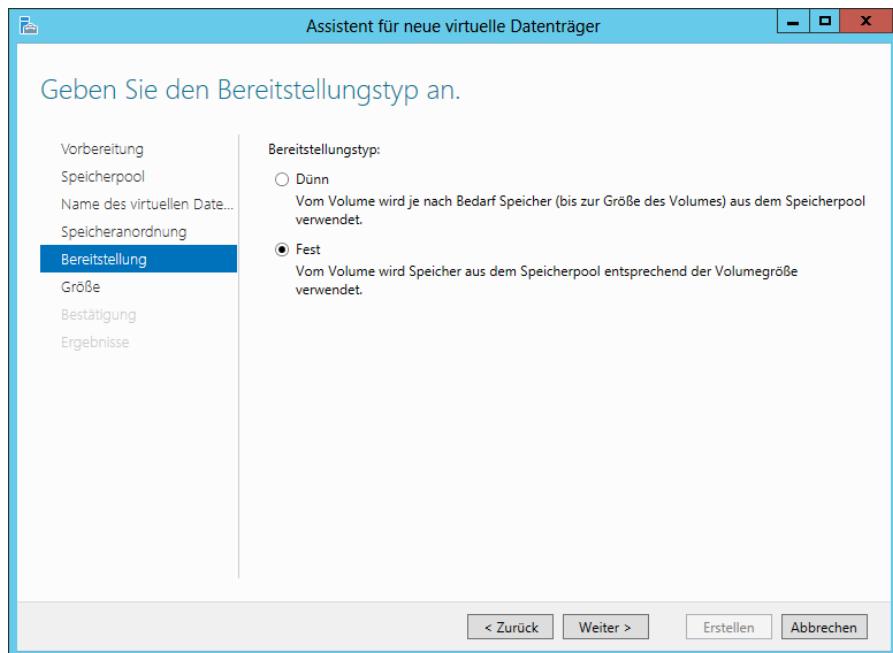


Abbildung 1.31 Die Seite *Geben Sie den Bereitstellungstyp an*

9. Wählen Sie eine der folgenden Bereitstellungstypoptionen aus und klicken Sie auf **Weiter:**
 - **Dünn** Das System ordnet den Speicherplatz aus dem Speicherpool der Festplatte nach Bedarf bis zur maximal festgelegten Größe zu
 - **Fest** Das System ordnet der Festplatte den Speicherplatz in der maximal spezifizierten Größe sofort beim Erstellen zu

Es erscheint die Seite *Geben Sie die Größe des virtuellen Datenträgers an* (siehe Abbildung 1.32).

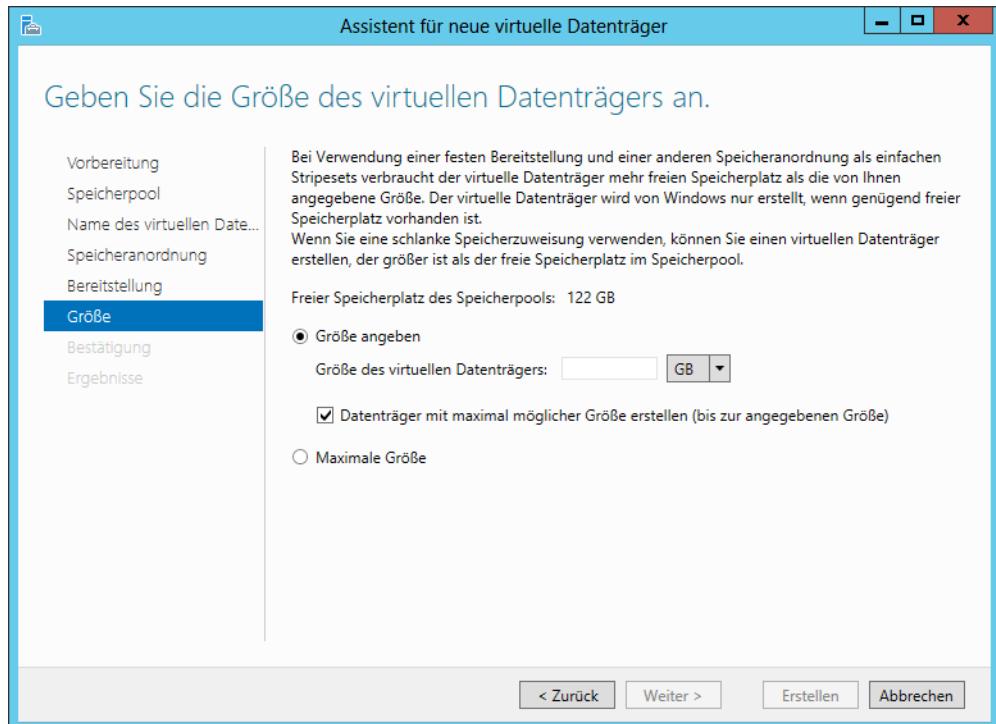


Abbildung 1.32 Die Seite *Geben Sie die Größe des virtuellen Datenträgers an*

10. Geben Sie im Textfeld *Größe des virtuellen Datenträgers* die Größe des Datenträgers an, den Sie erstellen möchten, und klicken Sie auf *Weiter*. Daraufhin gelangen Sie zur Seite *Auswahl bestätigen*.
11. Klicken Sie auf *Erstellen*. Wenn der Assistent den Datenträger anlegt, erscheint die Seite *Ergebnisse anzeigen*.
12. Klicken Sie auf *Schließen*. Der Assistent wird beendet und die neue Festplatte erscheint in der Kachel *Virtuelle Datenträger*, wie Abbildung 1.33 zeigt.
13. Schließen Sie das Fenster *Server-Manager*.

Standardmäßig startet der Assistent für neue Volumes, wenn Sie eine neue virtuelle Festplatte anlegen. Zu diesem Zeitpunkt ist die Festplatte ein virtuelles Äquivalent einer neu installierten physischen Festplatte. Sie enthält nichts weiter als nicht zugeordneten Speicherplatz und Sie müssen mindestens ein Volume erstellen, bevor Sie Daten auf der Festplatte speichern können.

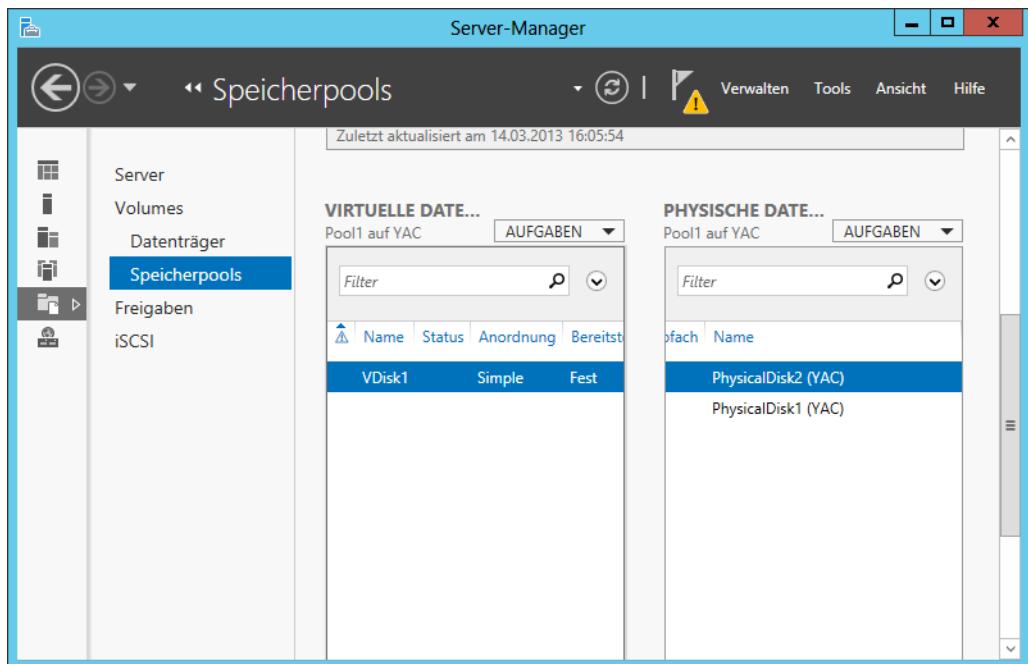


Abbildung 1.33 Eine neue Festplatte in der Kachel *Virtuelle Datenträger* von Server-Manager

Ein einfaches Volume erstellen

Aus technischer Sicht erstellen Sie Partitionen auf Basisfestplatten und Volumes auf dynamischen Festplatten. Dies ist keine willkürliche Unterscheidung in der Terminologie. Das Konvertieren einer Basisfestplatte in eine dynamische Festplatte erzeugt letztlich eine große Partition, die den gesamten Speicherplatz auf der Festplatte einnimmt. Die Volumes, die Sie auf der dynamischen Festplatte erstellen, sind logische Unterteilungen innerhalb dieser einzigen Partition.

Die Windows-Versionen vor 2008 verwenden die korrekte Terminologie im Snap-In *Datenträgerverwaltung*. Über die Menüs können Sie Partitionen auf Basisfestplatten und Volumes auf dynamischen Festplatten erstellen. Windows Server 2012 verwendet den Begriff *Volume* für beide Datenträgertypen und erlaubt es, jeden verfügbaren Volumetyp zu erzeugen, egal, ob es sich um eine Basis- oder dynamische Festplatte handelt. Wird der ausgewählte Volumetyp auf einer Basisfestplatte nicht unterstützt, konvertiert der Assistent sie in eine dynamische Festplatte im Rahmen des Volume-Erstellungsvorgangs.

Auch wenn in den Menüs bei Basispartitionen von Volumes die Rede ist, bleiben die herkömmlichen Regeln für Basisfestplatten in Kraft. Der Menübefehl *Neues einfaches Volume* legt auf Basisfestplatten bis zu drei primäre Partitionen an. Wenn Sie ein viertes Volume erstellen, erzeugt der Assistent eine erweiterte Partition und ein logisches Laufwerk mit der von Ihnen angegebenen Größe. Falls noch Platz auf der Festplatte frei bleibt, können Sie zusätzliche logische Laufwerke in der erweiterten Partition einrichten.



Wichtig Vorsicht mit dem Dienstprogramm DiskPart.exe!

Wenn Sie mit dem zu Windows Server 2012 gehörenden Befehlszeilendienstprogramm *DiskPart.exe* Basisfestplatten verwalten, können Sie vier primäre Partitionen oder drei primäre Partitionen und eine erweiterte Partition erstellen. Das Dienstprogramm *DiskPart.exe* enthält eine Obermenge der Befehle, die das Snap-In *Datenträgerverwaltung* unterstützt. Anders ausgedrückt, beherrscht *DiskPart* alles, was Sie mit der *Datenträgerverwaltung* ausführen können, und darüber hinaus noch weitere Befehle. Während aber das Snap-In *Datenträgerverwaltung* Sie daran hindert, unbeabsichtigte Aktionen aufzurufen, die zu einem Datenverlust führen können, bringt *DiskPart* keine derartigen Sicherheitsmechanismen mit und unterbindet keine solchen Aktionen. Deshalb empfiehlt Microsoft, dass nur erfahrene Benutzer mit *DiskPart* arbeiten und das Dienstprogramm mit Vorsicht einsetzen sollten.

Führen Sie die folgenden Schritte aus, um ein neues einfaches Volume auf einer Basis- oder dynamischen Festplatte mithilfe des Snap-Ins *Datenträgerverwaltung* zu erstellen:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Es erscheint das Fenster *Server-Manager*.
2. Klicken Sie auf *Tools/Computerverwaltung*. Daraufhin wird die Konsole *Computerverwaltung* geöffnet.
3. Klicken Sie auf *Datenträgerverwaltung*, um das gleichnamige Snap-In zu starten.
4. Klicken Sie mit der rechten Maustaste in der grafischen Ansicht auf einen nicht zugeordneten Bereich der Festplatte, auf der Sie ein Volume erstellen möchten, und wählen Sie im Kontextmenü *Neues einfaches Volume*, um den Assistenten zum Erstellen neuer einfacher Volumes zu starten.
5. Klicken Sie auf *Weiter*, um die *Willkommen*-Seite zu verlassen und zur Seite *Volumegröße festlegen* zu gehen (siehe Abbildung 1.34).

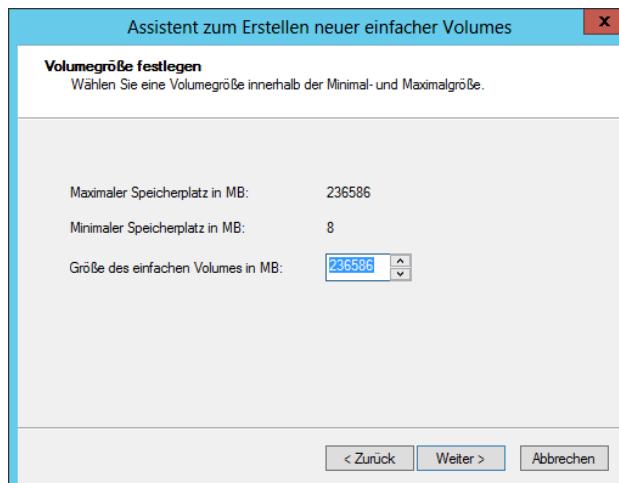


Abbildung 1.34 Die Seite *Volumegröße festlegen*

6. Legen Sie die Größe für die neue Partition oder das neue Volume innerhalb der auf der Seite genannten Grenzen im Drehfeld *Größe des einfachen Volumes in MB* fest. Klicken Sie auf *Weiter*. Als Nächstes erscheint die Seite *Laufwerkbuchstaben oder -pfad zuordnen*, die in Abbildung 1.35 dargestellt ist.

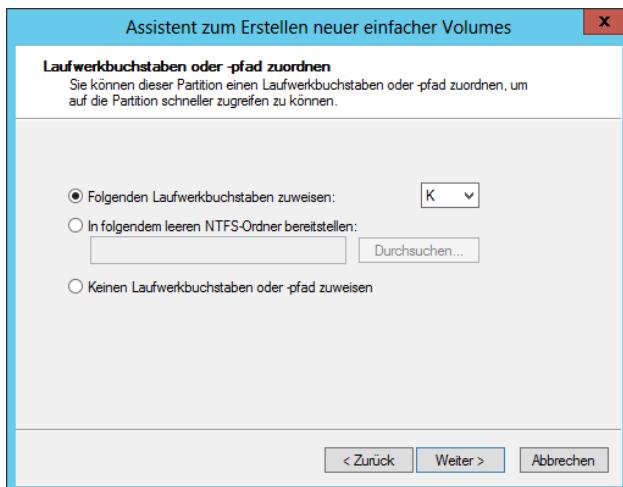


Abbildung 1.35 Die Seite *Laufwerkbuchstaben oder -pfad zuordnen*

7. Konfigurieren Sie eine der folgenden drei Optionen:
 - **Folgenden Laufwerkbuchstaben zuweisen** Klicken Sie bei dieser Option auf die zugeordnete Dropdownliste und wählen Sie den Laufwerkbuchstaben aus, den Sie dem Laufwerk zuweisen möchten
 - **In folgendem leeren NTFS-Ordner bereitstellen** Bei dieser Option geben Sie entweder den Pfad zu einem vorhandenen NTFS-Ordner ein oder klicken auf *Durchsuchen*, um nach dem Ordner zu suchen oder einen neuen Ordner zu erstellen. Der gesamte Inhalt des neuen Laufwerks erscheint dann im angegebenen Ordner.
 - **Keinen Laufwerkbuchstaben oder -pfad zuweisen** Wählen Sie diese Option, wenn Sie die Partition zwar erstellen möchten, aber noch nicht bereit sind, sie zu verwenden. Wenn Sie keinen Volume- oder Laufwerkbuchstaben oder -pfad zuweisen, wird das Laufwerk nicht bereitgestellt und ist nicht zugänglich. Möchten Sie das Laufwerk für eine Verwendung bereitstellen, weisen Sie ihm einen Laufwerkbuchstaben oder -pfad zu.
8. Klicken Sie auf *Weiter*, um die Seite *Partition formatieren* zu öffnen, die Abbildung 1.36 zeigt.

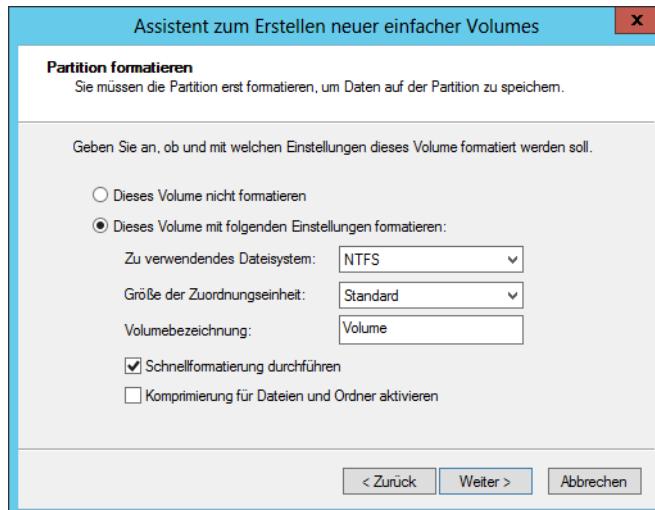


Abbildung 1.36 Die Seite *Partition formatieren*

9. Geben Sie an, ob der Assistent das Volume formatieren soll. Legen Sie in diesem Fall auch fest, wie. Wenn Sie das Volume noch nicht formatieren möchten, wählen Sie die Option *Dieses Volume nicht formatieren*. Möchten Sie das Volume formatieren, wählen Sie die Option *Dieses Volume mit folgenden Einstellungen formatieren* und konfigurieren die zugeordneten Optionen wie folgt:
 - **Zu verwendendes Dateisystem** Wählen Sie das gewünschte Dateisystem aus. Die verfügbaren Optionen hängen von der Größe des Volumes ab und können ReFS, NTFS, exFAT, FAT32 und FAT umfassen.
 - **Größe der Zuordnungseinheit** Legen Sie die Clustergröße des Dateisystems fest. Die Clustergröße kennzeichnet die Basiseinheit in Byte, mit der das System den Festplattenplatz zuordnet. Das System berechnet die standardmäßige Größe der Zuordnungseinheit basierend auf der Größe des Volumes. Diesen Wert können Sie überschreiben, indem Sie auf die zugeordnete Dropdownliste klicken und einen der Einträge auswählen. Verwendet Ihr Client beispielsweise durchweg kleine Dateien, können Sie die Größe der Zuordnungseinheit auf eine kleinere Clustergröße setzen.
 - **Volumebezeichnung** Geben Sie einen Namen für die Partition oder das Volume ein. Den Standardnamen *Volume* können Sie beliebig ändern.
 - **Schnellformatierung durchführen** Ist dieses Kontrollkästchen aktiviert, formatiert Windows den Datenträger ohne Fehlerprüfung. Diese schnellere Formatierungsme- thode wird allerdings von Microsoft nicht empfohlen. Bei einer Fehlerprüfung sucht das System nach defekten Sektoren auf der Festplatte und markiert diese, damit Ihre Clients diese Bereiche der Festplatte nicht verwenden.
 - **Komprimierung für Dateien und Ordner aktivieren** Ist dieses Kontrollkästchen aktiviert, wird die Ordnerkomprimierung für die Festplatte eingeschaltet. Diese Option ist nur für Volumes verfügbar, die mit dem Dateisystem NTFS formatiert sind.

10. Klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Fertigstellen des Assistenten*.
11. Kontrollieren Sie die Einstellungen in Bezug auf die gewählten Optionen und klicken Sie dann auf *Fertig stellen*. Der Assistent erstellt das Volume entsprechend Ihrer Spezifikationen.
12. Schließen Sie die Konsole, die das Snap-In *Datenträgerverwaltung* enthält.

Nachdem Sie ein einfaches Volume erstellt haben, können Sie dessen Eigenschaften mit dem Snap-In *Datenträgerverwaltung* ändern, d.h. erweitern oder verkleinern, wie es dieses Kapitel später noch beschreibt.

Diese Prozedur kann Volumes auf physischen oder virtuellen Festplatten erzeugen. Mit einem ähnlichen Assistenten in Server-Manager lassen sich auch einfache Volumes erstellen.

Wenn Sie den Assistenten für neue Volumes im Server-Manager – von den Startseiten *Volumes* oder *Datenträger* aus – starten, präsentiert der Assistent Optionen, die mit denen im Assistenten zum Erstellen neuer einfacher Volumes der *Datenträgerverwaltung* nahezu identisch sind.

Der wesentliche Unterschied besteht darin, dass der Assistent für neue Volumes wie alle Assistenten von Server-Manager eine Seite enthält, auf der Sie den Server und die Festplatte auswählen können, wo Sie das Volume erstellen möchten (siehe Abbildung 1.37). Demzufolge ist dieser Assistent geeignet, Volumes auf einer beliebigen Festplatte auf jedem Ihrer Server zu erstellen.

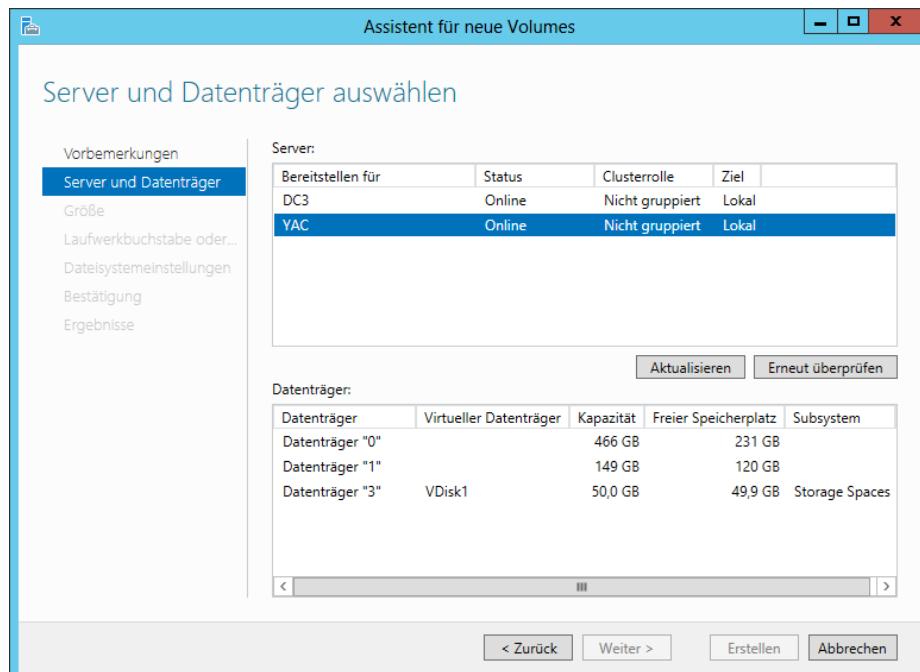


Abbildung 1.37 Die Seite *Server und Datenträger auswählen* im Assistenten für neue Volumes des Server-Managers

Ein Stripeset-, übergreifendes, gespiegeltes oder RAID-5-Volume erstellen

Ein Stripeset-, übergreifendes, gespiegeltes oder RAID-5-Volume lässt sich in fast den gleichen Schritten wie ein einfaches Volume erstellen, außer dass die Seite *Volumegröße festlegen* durch die Seite *Datenträger auswählen* ersetzt wird.

Führen Sie die folgenden Schritte aus, um ein Stripeset-, übergreifendes, gespiegeltes oder RAID-5-Volume zu erstellen:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Es erscheint das Fenster *Server-Manager*.
2. Klicken Sie auf *Tools/Computerverwaltung*. Die Konsole *Computerverwaltung* wird geöffnet.
3. Klicken Sie auf *Datenträgerverwaltung*, um das gleichnamige Snap-In zu öffnen.
4. Klicken Sie mit der rechten Maustaste auf einen nicht zugeordneten Bereich der Festplatte und wählen Sie dann aus dem Kontextmenü den Befehl für den Typ des Volumes, das Sie erstellen möchten. Daraufhin startet ein Assistent, mit dem Titel *Neues Volume* plus dem ausgewählten Volumetyp.
5. Klicken Sie auf *Weiter*, um die *Willkommen*-Seite zu verlassen und zur Seite *Datenträger auswählen* zu gelangen (siehe Abbildung 1.38).

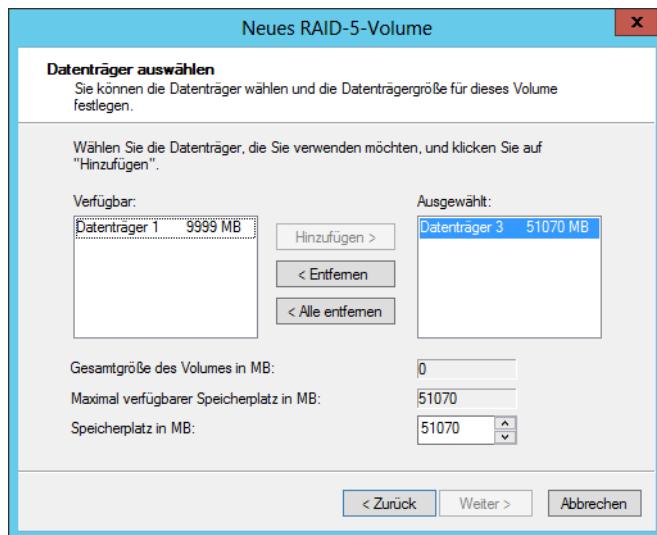


Abbildung 1.38 Die Seite *Datenträger auswählen*

6. Wählen Sie auf der Seite *Datenträger auswählen* aus dem Listenfeld *Verfügbar* die Festplatten aus, die Sie für das neue Volume verwenden möchten, und klicken Sie dann auf *Hinzufügen*. Der Assistent verschiebt die ausgewählten Festplatten in die Liste *Ausgewählt* und verbindet sie mit der ursprünglichen Festplatte, die Sie beim Starten des Assistenten ausgewählt haben. Für ein Stripeset-, übergreifendes oder gespiegeltes Volume

müssen Sie mindestens zwei Festplatten in die Liste *Ausgewählt* übernehmen, bei einem RAID-5-Volume sind es mindestens drei.

7. Legen Sie mit dem Drehfeld *Speicherplatz in MB* die Größe des Speicherplatzes fest, den Sie auf jeder Festplatte belegen möchten.
 - Wenn Sie ein übergreifendes Volume erstellen, müssen Sie jede Festplatte in der Liste *Ausgewählt* anklicken und die Größe des Speicherplatzes für diese Festplatte spezifizieren. Der Standardwert ist die Größe des nicht zugeordneten Platzes auf der jeweiligen Festplatte.
 - Bei einem Stripeset-, gespiegelten oder RAID-5-Volume brauchen Sie nur einen Wert festzulegen, da diese Volumes auf jeder Festplatte den gleichen Platz belegen. Der Standardwert ist die Größe des nicht zugeordneten Platzes auf der Festplatte mit dem kleinsten freien Speicherplatz.
8. Legen Sie fest, ob Sie einen Laufwerkbuchstaben oder -pfad zuweisen möchten, und klicken Sie dann auf *Weiter*. Es erscheint die Seite *Partition formatieren*.
9. Geben Sie an, ob oder wie Sie das Volume formatieren möchten. Klicken Sie dann auf *Weiter*, um zur Seite *Fertigstellen des Assistenten* zu gelangen.
10. Kontrollieren Sie die Einstellungen in Bezug auf die gewählten Optionen und klicken Sie dann auf *Fertig stellen*. Befinden sich unter den ausgewählten Festplatten, mit denen Sie das Volume erstellen möchten, Basisfestplatten, warnt eine Meldung der *Datenträgerverwaltung*, dass die Basisfestplatten beim Erstellen des Volumes in dynamische Festplatten konvertiert werden.
11. Klicken sie auf *Ja*. Der Assistent erstellt das Volume entsprechend Ihren Spezifikationen.



Weitere Informationen Zusätzliche Optionen

Im Abschnitt »Ein einfaches Volume erstellen« weiter vorn in diesem Kapitel finden Sie weitere Informationen in Bezug auf die Optionen der Seiten *Laufwerkbuchstaben oder -pfad zuordnen* und *Partition formatieren*.

12. Schließen Sie das Snap-In *Datenträgerverwaltung*.

Die Befehle im Kontextmenü einer Festplatte hängen von der Anzahl der im Computer installierten Festplatten und des nicht zugeordneten Speicherplatzes auf ihnen ab. Zum Beispiel müssen mindestens zwei Festplatten mit nicht zugeordnetem Speicherplatz verfügbar sein, um ein Stripeset-, übergreifendes oder gespiegeltes Volume zu erstellen, und mindestens drei Festplatten bei einem RAID-5-Volume.



Gedankenexperiment Wenden Sie in diesem Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Auf einem neuen Server, auf dem Windows Server 2012 läuft, richtet Morris einen Speicherpool aus zwei physischen Laufwerken mit einer Kapazität von jeweils 1 TB ein.

Dann erstellt er aus dem Platz im Speicherpool drei einfache virtuelle Festplatten. Anschließend erzeugt er mit dem Snap-In *Datenträgerverwaltung* aus den drei virtuellen Festplatten ein RAID-5-Volume.

Beantworten Sie für dieses Szenario die folgenden Fragen:

1. Inwiefern ist die Speicherplanung von Morris hinsichtlich der Fehlertoleranz ineffektiv?
 2. Weshalb lässt sich die Fehlertoleranz des Speicherplans mit einer dritten Festplatte für den Speicherpool nicht verbessern?
 3. Wie kann Morris den Speicherplan ändern, um ihn fehlertolerant zu gestalten?
-

Prüfungszielzusammenfassung

- Windows Server 2012 unterstützt zwei Datenträgerpartitionsstile (MBR und GPT), zwei Datenträgertypen (Basis und dynamisch), fünf Volumetypen (einfach, Stripset, übergreifend, gespiegelt und RAID-5) und drei Dateisysteme (ReFS, NTFS und FAT)
- Das Snap-In *Datenträgerverwaltung* kann Festplatten auf dem lokalen Computer initialisieren, partitionieren und formatieren. Server-Manager kann die gleichen Aufgaben für Server im gesamten Netzwerk durchführen.
- Ein Windows-Server kann seine Aufgaben möglicherweise mit demselben Speichertyp wie eine Arbeitsstation ausführen. Allerdings unterscheiden sich Server und Arbeitsstationen hinsichtlich der E/A-Lasten und ein standardmäßiges Speichersubsystem kann leicht durch Dateianforderungen von Dutzenden oder Hunderten von Benutzern überfordert werden. Darüber hinaus bieten Standardfestplatten keine Fehlertoleranz und sind nur begrenzt skalierbar.
- Windows Server 2012 führt mit den sogenannten Storage Spaces (Speicherplätzen) eine neue Datenträgervirtualisierungstechnik ein. Server können damit die Speicherkapazität von einzelnen physischen Datenträgern verketten und diesen Platz zuordnen, um virtuelle Datenträger jeder beliebigen Größe, die von der Hardware unterstützt wird, zu schaffen.
- Alle Windows Server 2012-Installationen enthalten die Rolle *Datei- und Speicherdiene*ste. Diese ist dafür zuständig, dass Server-Manager ein Untermenü anzeigt, wenn Sie auf das Symbol im Navigationsbereich klicken. Das Untermenü bietet Verweise auf Startseiten, wo Administratoren Volumes, Datenträger, Speicherpools, Freigaben und iSCSI-Geräte verwalten können.
- Mit dem Snap-In *Datenträgerverwaltung* in Windows Server 2012 können Sie VHD-Dateien erzeugen und sie auf dem Computer bereitstellen
- Nachdem Sie Ihre physischen Festplatten installiert haben, können Sie deren Speicherplatz in einem Speicherpool verketten, aus dem sich virtuelle Festplatten beliebiger Größe erstellen lassen. Den Speicherplatz des erstellten Speicherpools können Sie nun verwenden und je nach Bedarf beliebig viele virtuelle Festplatten erzeugen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Aussagen gelten für Stripesetvolumes? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Stripesetvolumes bieten eine bessere Performance als einfache Volumes.
 - B. Stripesetvolumes bieten eine höhere Fehlertoleranz als einfache Volumes.
 - C. Stripesetvolumes lassen sich nach dem Erstellen erweitern.
 - D. Fällt eine physische Festplatte im Stripesetvolume aus, sind sämtliche Daten im gesamten Volume verloren.
2. Welche der folgenden Anforderungen gelten für das Erweitern eines Volumes auf einer dynamischen Festplatte? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Wenn Sie ein einfaches Volume erweitern wollen, können Sie nur den verfügbaren Platz auf derselben Festplatte verwenden, wenn das Volume einfach bleiben soll.
 - B. Auf dem Volume muss ein Dateisystem eingerichtet sein (Rohvolume), bevor sich ein einfaches oder übergreifendes Volume erweitern lässt.
 - C. Ein einfaches oder übergreifendes Volume können Sie erweitern, wenn Sie es mit dem Dateisystem FAT oder FAT32 formatieren.
 - D. Ein einfaches Volume können Sie über zusätzliche Festplatten erweitern, wenn es kein System- oder Startvolume ist.
3. Welche der folgenden Volumetypen, die Windows Server 2012 unterstützt, bieten Fehler-toleranz? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Stripeset
 - B. Übergreifend
 - C. Gespiegelt
 - D. RAID-5
4. Für welche der folgenden Techniken ist ein JBOD-Laufwerksarray eine Alternative?
 - A. SAN
 - B. SCSI
 - C. RAID
 - D. iSCSI

Kapitelzusammenfassung

- Wenn Sie die Installationsoption Windows Server Core wählen, erhalten Sie eine abgespeckte Version des Betriebssystems
- Die minimale Serverschnittstelle ist eine Einstellung, die einige der hardwareintensivsten Elemente aus der grafischen Benutzeroberfläche entfernt
- Migration ist die bevorzugte Methode, um einen vorhandenen Server durch einen Server mit Windows Server 2012 zu ersetzen. Im Unterschied zu einem direkten Upgrade werden bei der Migration wichtige Informationen von einem vorhandenen Server zu einer Neuinstallation von Windows Server 2012 kopiert.
- Auf einem Windows Server 2012-Computer können Sie von einer vollständigen Installation mit grafischer Benutzeroberfläche zu einer Server Core-Installation wechseln und einen Server Core-Computer in eine vollständige Installation mit grafischer Benutzeroberfläche umwandeln
- Der NIC-Teamvorgang ist ein neues Feature in Windows Server 2012. Damit können Administratoren die Bandbreite von mehreren Netzwerkadapters zusammenfassen und somit eine erhöhte Performance und Fehlertoleranz gewährleisten.
- Windows Server 2012 unterstützt zwei Datenträgerpartitionsstile (MBR und GPT), zwei Datenträgertypen (Basis und dynamisch), fünf Volumetypen (einfach, Stripset, übergreifend, gespiegelt und RAID-5) und drei Dateisysteme (ReFS, NTFS und FAT)
- Nachdem Sie Ihre physischen Festplatten installiert haben, können Sie deren Speicherplatz zu einem Speicherpool verketten und daraus virtuelle Festplatten in beliebiger Anzahl und Größe erstellen

Antworten

Dieser Abschnitt enthält die Lösungen für die Gedankenexperimente und Antworten auf die Fragen der Prüfungszielkontrollen in diesem Kapitel.

Prüfungsziel 1.1: Gedankenexperiment

```
Uninstall-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart  
Uninstall-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Remove
```

Prüfungsziel 1.1: Kontrolle

1. **Richtige Antworten:** A, C
 - A. **Richtig:** DNS ist ein Infrastrukturdienst.
 - B. **Falsch:** Web Server (IIS) ist ein Anwendungsdienst und kein Infrastrukturdienst.
 - C. **Richtig:** DHCP ist ein Infrastrukturdienst.
 - D. **Falsch:** Remotedesktopdienste stellt einen Anwendungsdienst und keinen Infrastrukturdienst dar.

2. Richtige Antwort: B

- A. **Falsch:** Von keiner Version von Windows Server 2003 Standard ist ein Upgrade auf Windows Server 2012 Standard möglich.
- B. **Richtig:** Von Windows Server 2008 Standard können Sie ein Upgrade auf Windows Server 2012 Standard ausführen.
- C. **Falsch:** Weder für die 32-Bit-Version von Windows Server 2008 R2 noch für jede andere 32-Bit-Version ist ein Upgrade auf Windows Server 2012 (64 Bit) möglich.
- D. **Falsch:** Von Windows 7 Ultimate oder irgendeinem Arbeitsstationsbetriebssystem ist kein Upgrade auf Windows Server 2012 möglich.

3. Richtige Antwort: A

- A. **Richtig:** Das Installieren des Moduls *Tools und Infrastruktur für die grafische Verwaltung* – und nur dieses Moduls – auf einer Server Core-Installation resultiert in der minimalen Serverschnittstelle.
- B. **Falsch:** Das Installieren der Features *Server Graphical Shell* und *Tools und Infrastruktur für die grafische Verwaltung* konvertiert eine Server Core-Installation in eine vollständige Installation mit grafischer Benutzeroberfläche.
- C. **Falsch:** Windows PowerShell ist eine Befehlszeilenoberfläche, die keine Auswirkung auf die minimale Serverinstallation hat.
- D. **Falsch:** MMC ist eine der grafischen Anwendungen, die in der minimalen Serverinstallation zur Verfügung stehen, die Sie aber nicht einzeln installieren.

4. Richtige Antwort: D

- A. **Falsch:** Das *Windows*-Verzeichnis enthält aktive Betriebssystemdateien und nicht die Installationsdateien.
- B. **Falsch:** Das *System32*-Verzeichnis enthält aktive Betriebssystemdateien und nicht die Installationsdateien.
- C. **Falsch:** Es gibt kein *bin*-Verzeichnis, das mit dem Windows-Betriebssystem verbunden ist.
- D. **Richtig:** Windows speichert sämtliche Module für die Betriebssysteminstallation im Verzeichnis *WinSxS*.

5. Richtige Antworten: A, B, C

- A. **Richtig:** Es ist möglich, auf einem unter Windows Server 2012 laufenden Computer bei Bedarf zwischen der Server Core-Installation und der vollständigen Installation mit grafischer Benutzeroberfläche zu wechseln.
- B. **Richtig:** Die Windows PowerShell 3.0-Benutzeroberfläche in Windows Server 2012 bringt deutlich mehr Cmdlets mit als Windows PowerShell 2.0.
- C. **Richtig:** Server-Manager bindet in viele Assistenten eine Benutzeroberfläche zur Serverauswahl ein.
- D. **Falsch:** Es gibt keine unterschiedlichen Lizenzen für die Windows Server 2012-Versionen Server Core-Installation und vollständige Installation mit grafischer Benutzeroberfläche.

Prüfungsziel 1.2: Gedankenexperiment

1. Install-WindowsFeature
2. Get-WindowsFeature
Install-WindowsFeature FS-FileServer
Install-WindowsFeature FS-DFS-Namespace
Install-WindowsFeature FS-DFS-Replication
Install-WindowsFeature FS-NFS-Service
Install-WindowsFeature Print-Services -allsubfeatures
Install-WindowsFeature Web-Server
Install-WindowsFeature Web-Windows-Auth
Install-WindowsFeature Web-Ftp-Service

Prüfungsziel 1.2: Kontrolle

1. **Richtige Antworten:** B, D
 - A. **Falsch:** WMI (Windows Management Instrumentation) ist ein Satz von Treibererweiterungen, die oftmals zusammen mit Windows PowerShell verwendet werden. Diese Komponenten müssen Sie nicht entfernen, um zu einer Server Core-Installation wechseln zu können.
 - B. **Richtig:** Es ist erforderlich, das Feature *Tools und Infrastruktur für die grafische Verwaltung* zu entfernen, um zu einer Server Core-Installation wechseln zu können.
 - C. **Falsch:** Bei einer vollständigen Installation mit grafischer Benutzeroberfläche oder einer Server Core-Installation wird die Desktopdarstellung standardmäßig nicht installiert.
 - D. **Richtig:** Das Servergrafikshell-Feature bietet Unterstützung für MMC, Server-Manager und einen Teil der Systemsteuerung. Um zu einer Server Core-Installation zu wechseln, müssen Sie das Feature entfernen.
2. **Richtige Antwort:** B
 - A. **Falsch:** Hyper-V-Livemigration ist kein Modus des NIC-Teamvorgangs.
 - B. **Richtig:** Im switchunabhängigen Modus werden die Netzwerkadapter des Teams mit verschiedenen Switches verbunden, sodass alternative Pfade durch das Netz zur Verfügung stehen.
 - C. **Falsch:** Im switchabhängigen Modus sind die Netzwerkadapter des Teams mit denselben Switches verbunden, sodass zwar Bandbreitenaggregation, jedoch keine Fehlertoleranz gegeben ist.
 - D. **Falsch:** Das LACP (Link Aggregation Control Protocol) ist kein Modus des NIC-Teamvorgangs.

3. Richtige Antwort: C

- A. **Falsch:** Das Windows-Befehlszeilentool *Net.exe* stellt zwar viele verschiedene Funktionen bereit, kann jedoch einen Computer nicht mit einer Domäne verbinden.
- B. **Falsch:** Mit dem Netzwerk-Shellprogramm *Netsh.exe* können Sie die Netzwerkschnittstelle konfigurieren, jedoch nicht einen Computer mit einer Domäne verbinden.
- C. **Richtig:** *Netdom.exe* ist die Windows-Befehlszeilenanwendung *Domain Manager*.
- D. **Falsch:** *Ipconfig.exe* kann Netzwerkkonfigurationseinstellungen anzeigen, jedoch nicht einen Computer mit einer Domäne verbinden.

4. Richtige Antwort: A

- A. **Richtig:** Server-Manager kann Rollen nicht auf mehreren Servern gleichzeitig bereitstellen.
- B. **Falsch:** Server-Manager kann Offline-VHD-Dateien bereitstellen sowie Rollen und Features auf ihnen installieren.
- C. **Falsch:** Server-Manager kombiniert die Rollen- und Featureinstallationsprozesse in einem einzigen Assistenten.
- D. **Falsch:** Server-Manager kann Rollen und Features auf jedem Windows Server 2012-Server im Netzwerk installieren.

5. Richtige Antworten: C, D

- A. **Falsch:** Einen laufenden Dienst können Sie mithilfe von Server-Manager beenden.
- B. **Falsch:** Einen beendeten Dienst können Sie mithilfe von Server-Manager starten.
- C. **Richtig:** Ein Dienst lässt sich mit Server-Manager nicht deaktivieren.
- D. **Richtig:** Mit Server-Manager ist es nicht möglich, einen Dienst für den automatischen Start beim Starten des Computers zu konfigurieren.

Prüfungsziel 1.3: Gedankenexperiment

1. Morris hat ein RAID-5-Volume aus den virtuellen Festplatten erstellt, die aus einem Speicherpool stammen, der lediglich zwei physische Festplatten umfasst. Ein RAID-5-Volume kann nur dann Fehlertoleranz bieten, wenn die Daten auf drei physischen Festplatten gespeichert werden.
2. Eine zusätzliche dritte Festplatte garantiert keine Fehlertoleranz, da es nicht sicher ist, ob jede der drei virtuellen Festplatten auf einer separaten einzelnen Festplatte existiert.
3. Um den Plan fehlertolerant zu machen, sollte Morris die drei einfachen virtuellen Festplatten löschen und eine neue virtuelle Festplatte entweder mit der Spiegel- oder der Paritätslayoutoption erstellen.

Prüfungsziel 1.3: Kontrolle

1. Richtigige Antworten: A, D

- A. **Richtig:** Stripesets bieten verbesserte Performance, da jedes Laufwerk in der Gruppe Zeit hat, den Ort des nächsten Stripes zu suchen, während die anderen Laufwerke schreiben.
- B. **Falsch:** Stripesetvolumes enthalten keine redundanten Daten und bieten demzufolge keine Fehlertoleranz.
- C. **Falsch:** Stripesetvolumes lassen sich nach dem Erstellen nicht erweitern, ohne dabei die auf ihnen gespeicherten Daten zu zerstören.
- D. **Richtig:** Fällt eine einzelne physische Festplatte im Stripesetvolume aus, gehen sämtliche Daten im gesamten Volume verloren.

2. Richtigige Antworten: A, D

- A. **Richtig:** Wenn Sie ein einfaches Volume erweitern, können Sie nur den verfügbaren Platz auf derselben Festplatte verwenden. Wenn Sie das Volume auf eine andere Festplatte erweitern, ist es kein einfaches Volume mehr.
- B. **Falsch:** Sie können ein einfaches oder übergreifendes Volume erweitern, selbst wenn es kein Dateisystem besitzt (Rohvolume).
- C. **Falsch:** Ein Volume können Sie erweitern, wenn Sie es mit dem Dateisystem NTFS formatiert haben. Volumes mit den Dateisystemen FAT oder FAT32 lassen sich nicht erweitern.
- D. **Richtig:** Ein einfaches Volume können Sie über zusätzliche Festplatten hinweg erweitern, wenn es sich nicht um ein System- oder ein Startvolume handelt.

3. Richtigige Antworten: C, D

- A. **Falsch:** Ein Stripesetvolume verteilt die Daten auf mehrere Festplatten, schreibt die Daten aber nur einmal. Demzufolge bietet es keine Fehlertoleranz.
- B. **Falsch:** Ein übergreifendes Volume nutzt den Platz auf mehreren Laufwerken, schreibt die Daten aber nur einmal. Demzufolge bietet es keine Fehlertoleranz.
- C. **Richtig:** Ein gespiegeltes Volume schreibt Duplikate aller Daten auf zwei oder mehrere Festplatten und bietet dadurch Fehlertoleranz.
- D. **Richtig:** Ein RAID-5-Volume schreibt Daten und Paritätsinformationen auf mehrere Festplatten und bietet dadurch Fehlertoleranz.

4. Richtigige Antwort: C

- A. **Falsch:** Ein SAN ist ein separates Netzwerk, das für Speicherung vorgesehen ist, und JBOD ist eine Datenträgergruppe, die sich auf einem SAN oder einem Standardnetzwerk installieren lässt.
- B. **Falsch:** SCSI ist eine Datenträgerschnittstelle und kein Typ einer Datenträgergruppe.

- C. **Richtig:** Eine JBOD-Datenträgergruppe ist eine Alternative zu einer RAID-Datenträgergruppe, die jede Festplatte als unabhängiges Volume behandelt.
- D. **Falsch:** Eine JBOD-Datenträgergruppe ist keine Alternative zu iSCSI. Dies ist ein Protokoll, das für SAN-Kommunikation verwendet wird.

K A P I T E L 2

Serverrollen und -features konfigurieren

Dieses Kapitel beschäftigt sich mit einigen der grundlegenden Dienste, die die meisten Windows-Server ausführen. In der Geschäftswelt war die Datei- und Druckerfreigabe der ausschlaggebende Grund, Computer in einem Netzwerk zu betreiben, und mit Windows Server 2012 ist die Remoteverwaltung zu einem entscheidenden Element der Serveradministration geworden.

Prüfungsziele in diesem Kapitel:

- Prüfungsziel 2.1: Datei- und Freigabezugriff konfigurieren 90
- Prüfungsziel 2.2: Druck- und Dokumentdienste konfigurieren 112
- Prüfungsziel 2.3: Server für die Remoteverwaltung konfigurieren 135

Prüfungsziel 2.1: Datei- und Freigabezugriff konfigurieren

Zu den wichtigsten Funktionen der Routinearbeiten von Serveradministratoren gehört die Entscheidung, wo Benutzer ihre Dateien speichern sollen und wer darauf zugreifen darf.

Dieses Prüfungsziel zeigt, wie Sie

- Freigaben erstellen und konfigurieren
 - Freigabeberechtigungen konfigurieren
 - Offlinedateien konfigurieren
 - NTFS-Berechtigungen konfigurieren
 - Zugriffsbasierter Aufzählung konfigurieren
 - Volumeschattenkopie-Dienst konfigurieren
 - NTFS-Kontingente konfigurieren
-

Ordnerfreigaben erstellen

Ordner werden freigegeben, um sie für Netzwerkbenutzer zugänglich zu machen. Nachdem Sie die Festplatten auf einem Dateiserver konfiguriert haben, müssen Sie Freigaben einrichten, damit Netzwerkbenutzer auf diese Festplatten zugreifen können. Wie Kapitel 1 beim Thema Planung angemerkt hat, brauchen Sie von vornherein eine Freigabestrategie. Daraus sollte hervorgehen

- welche Ordner Sie freigeben
- welche Namen Sie den Freigaben zuweisen
- welche Berechtigungen Sie den Benutzern der Freigaben erteilen
- welche Offlinedatei-Einstellungen Sie für die Freigaben verwenden

Wenn Sie der Ersteller-Besitzer eines Ordners sind, können Sie ihn auf einem Windows Server 2012-Computer freigeben. Dazu klicken Sie in einem Dateiexplorer-Fenster mit der rechten Maustaste auf den Ordner, wählen im Kontextmenü *Freigeben für/Bestimmte Personen* und folgen den Anweisungen im Dialogfeld *Dateifreigabe* (siehe Abbildung 2.1).

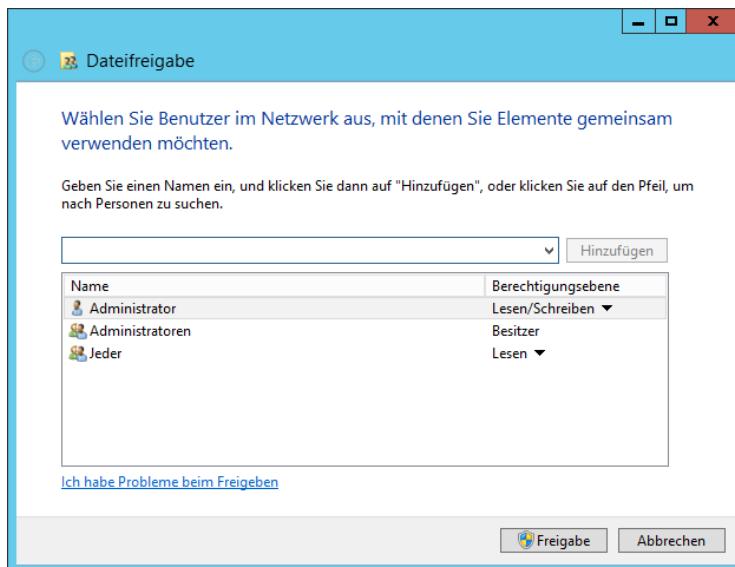


Abbildung 2.1 Das Dialogfeld *Dateifreigabe*

Bei dieser Methode zum Erstellen von Freigaben bietet die vereinfachte Oberfläche nur wenig Kontrolle über Elemente, wie zum Beispiel Freigabeberechtigungen. Sie legen lediglich fest, dass die Benutzer Lese- oder Lese-/Schreibberechtigungen für die Freigabe erhalten. Sind Sie nicht der Ersteller-Besitzer des Ordners, können Sie stattdessen auf die Registerkarte *Freigabe* des Blatts *Eigenschaften* für den Ordner zugreifen. Wenn Sie auf die Schaltfläche *Freigabe* klicken, erscheint das gleiche Dialogfeld, über die Schaltfläche *Erweiterte Freigabe* gelangen Sie zum Dialogfeld *Erweiterte Freigabe*, das Abbildung 2.2 zeigt und mehr Kontrolle über Freigabeberechtigungen bietet.

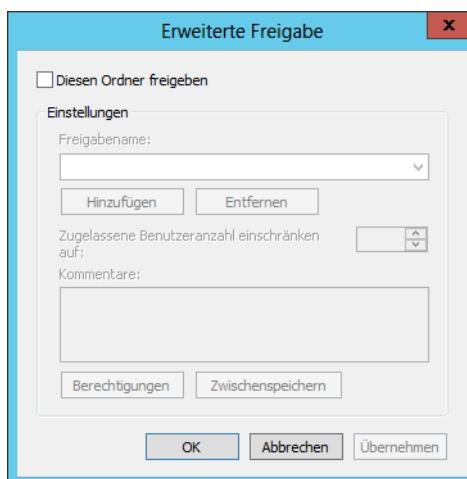


Abbildung 2.2 Das Dialogfeld *Erweiterte Freigabe*



Hinweis Netzwerkerkennung

Damit die Benutzer im Netzwerk die Freigaben sehen können, die Sie auf dem Dateiserver erstellen, müssen Sie im Netzwerk- und Freigabecenter der Systemsteuerung die Einstellungen für Netzwerkerkennung und Dateifreigabe aktivieren.

Über die Startseite *Datei- und Speicherdiene*s des Server-Managers haben Sie die Möglichkeit, die Freigaben auf allen Festplatten in sämtlichen Servern zu kontrollieren und deren Eigenschaften feinstufig zu beeinflussen.

Windows Server 2012 unterstützt zwei Arten von Ordnerfreigaben:

- **SMBs (Server Message Blocks)** Dies ist das standardmäßige Dateifreigabeprotokoll, das alle Versionen von Windows verwenden
- **NFS (Network File System)** NFS ist das standardmäßige Dateifreigabeprotokoll, das die meisten UNIX- und Linux-Distributionen verwenden

Bei der Installation von Windows Server 2012 installiert das Setupprogramm standardmäßig den Rollendienst *Speicherdiene*s in der Rolle *Datei- und Speicherdiene*s. Bevor Sie jedoch SMB-Freigaben mit dem Server-Manager erstellen und verwalten können, müssen Sie den Rollendienst *Dateiserver* installieren, und um NFS-Freigaben zu erstellen, den Rollendienst *Server für NFS*.

Führen Sie die folgenden Schritte aus, um eine Ordnerfreigabe mithilfe des Server-Managers zu erstellen:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Daraufhin erscheint das Fenster *Server-Manager*.
2. Klicken Sie auf das Symbol *Datei- und Speicherdiene*s und im eingeblendeten Unter- menü auf *Freigaben*, um die Startseite *Freigaben* zu öffnen.
3. Im Menü *Aufgaben* wählen Sie *Neue Freigabe*. Der Assistent für neue Freigaben startet und zeigt die Seite *Profil für die Freigabe auswählen* an, die in Abbildung 2.3 zu sehen ist.
4. Wählen Sie eine der folgenden Optionen aus der Liste *Dateifreigabeprofil*:
 - **SMB-Freigabe – Schnell** Bietet einfache SMB-Freigabe mit vollen Freigabe- und NTFS-Berechtigungen
 - **SMB-Freigabe – Erweitert** Bietet SMB-Freigabe mit vollen Freigabe- und NTFS- Berechtigungen und Zugriff auf Dienste, die der Ressourcen-Manager für Dateiserver bereitstellt
 - **SMB-Freigabe – Anwendungen** Bietet SMB-Freigabe mit Einstellungen, die für Hyper-V und andere Anwendungen geeignet sind
 - **NFS-Freigabe – Schnell** Bietet einfache NFS-Freigabe mit Authentifizierung und Berechtigungen

- **NFS-Freigabe – Erweitert** Bietet NFS-Freigabe mit Authentifizierung und Berechtigungen sowie Zugriff auf Dienste, die der Ressourcen-Manager für Dateiserver bereitstellt

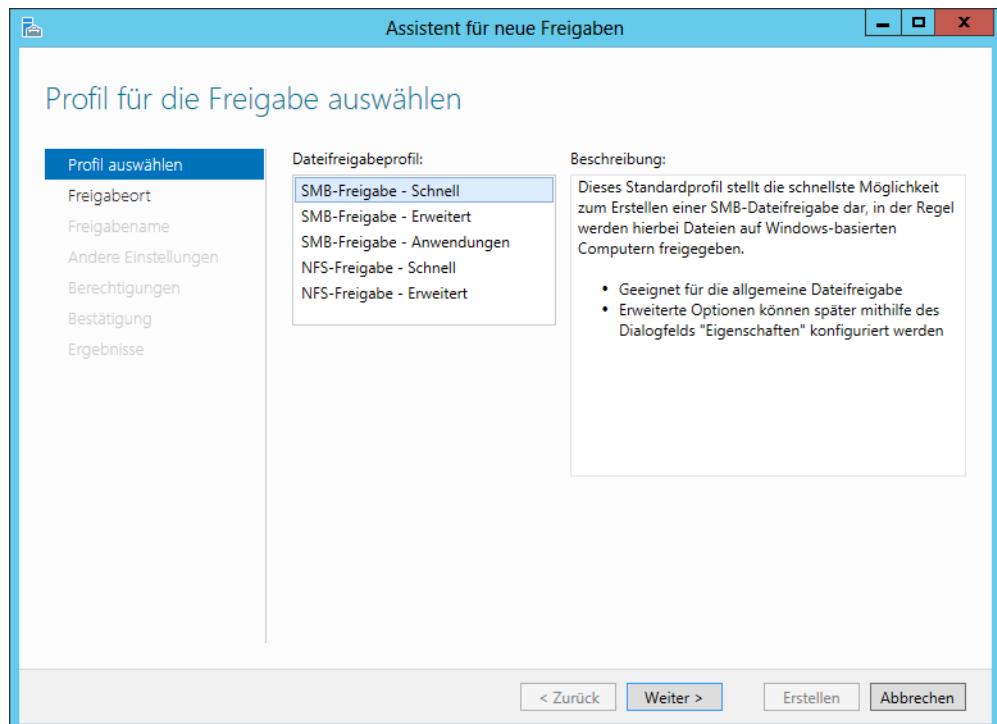


Abbildung 2.3 Die Seite *Profil für die Freigabe auswählen* im Assistenten für neue Freigaben

5. Klicken Sie auf *Weiter*. Die Seite *Server und Pfad für diese Freigabe auswählen* erscheint.
6. Wählen Sie den Server aus, auf dem Sie die Freigabe erstellen möchten, und wählen Sie entweder ein Volume auf dem Server aus oder geben Sie einen Pfad zu dem freizugebenden Ordner an. Klicken Sie auf *Weiter*. Es erscheint die Seite *Freigabename angeben*.



Weitere Informationen NFS-Freigaben

Bei Auswahl eines der NFS-Freigabeprofile präsentiert der Assistent zwei zusätzliche Seiten: *Authentifizierungsmethoden angeben* und *Freigabeberechtigungen angeben*. Über diese beiden Seiten können Sie auf Funktionen zugreifen, die der Rollendienst *Server für NFS* implementiert, wie sie das Prüfungsziel »Konfigurieren der Advanced File Services« in der Zertifizierungsprüfung 70-412, »Configuring Advanced Windows Server 2012 Services« behandelt.

7. Geben Sie im Textfeld *Freigabename* den Namen an, den Sie der Freigabe zuweisen möchten, und klicken Sie auf *Weiter*. Daraufhin erscheint die Seite *Freigabeeinstellungen konfigurieren* (siehe Abbildung 2.4).

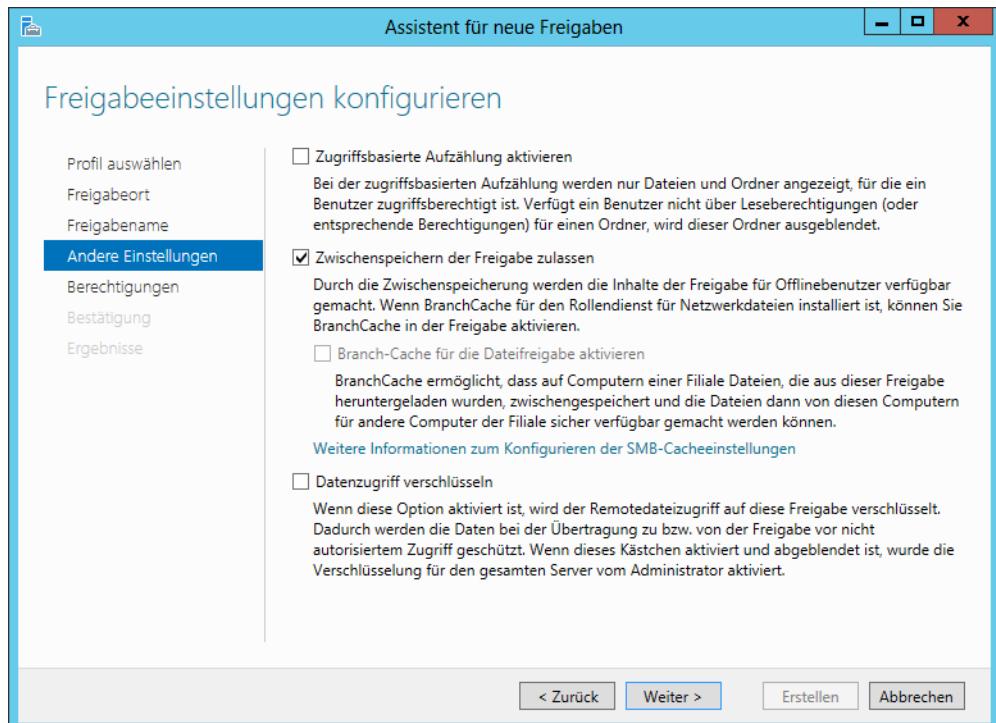


Abbildung 2.4 Die Seite *Freigabeeinstellungen konfigurieren* des Assistenten für neue Freigaben

8. Wählen Sie unter den folgenden Optionen aus (eine oder mehrere):
- **Zugriffsbasierte Aufzählung aktivieren** Verhindert, dass Benutzer Dateien und Ordner einsehen können, für die sie keine Zugriffsberechtigungen besitzen
 - **Zwischenspeichern der Freigabe zulassen** Ermöglicht Offline-Benutzern, auf den Inhalt dieser Freigabe zuzugreifen
 - **Branch-Cache für die Dateifreigabe aktivieren** Erlaubt es BranchCache-Servern, Dateien zwischenzuspeichern, auf die von dieser Freigabe aus zugegriffen wird
 - **Datenzugriff verschlüsseln** Bewirkt, dass der Server den Remotedateizugriff auf diese Freigabe verschlüsselt



Hinweis Zugriffsbasierte Aufzählung

Das in Windows Server 2003 R2 eingeführte Feature *Zugriffsbasierte Aufzählung* (Access-based Enumeration, ABE) wendet Filter auf freigegebene Ordner basierend auf den Berechtigungen einzelner Benutzer auf die Dateien und Unterordner in der Freigabe an. Kurz gesagt sehen Benutzer, die auf eine bestimmte freigegebene Ressource nicht zugreifen können, diese Ressource auch nicht im Netzwerk. Dieses Feature verhindert, dass Benutzer Dateien und Ordner durchsuchen, auf die sie nicht zugreifen dürfen. Die zugriffsbasierte Aufzählung lässt sich jederzeit für eine Freigabe aktivieren bzw. deaktivieren, indem Sie das Blatt *Eigenschaften* in der Konsole *Freigabe und Speicherverwaltung* öffnen und auf *Erweitert* klicken. Daraufhin gelangen Sie zum gleichen Dialogfeld *Erweitert*, das auch der Assistent zum Bereitstellen eines freigegebenen Ordners anzeigt.



Hinweis Offlinedateien

Das auch als *clientseitige Zwischenspeicherung* bezeichnete Feature *Offlinedateien* ermöglicht es Clientsystemen, lokale Kopien der Dateien zu verwalten, auf die sie von Serverfreigaben zugreifen. Wenn ein Client die Option *Immer offline verfügbar* für serverbasierte Dateien, Ordner oder Freigaben auswählt, kopiert das Clientsystem die ausgewählten Daten auf den lokalen Datenträger und aktualisiert sie regelmäßig, sodass der Clientbenutzer immer darauf zugreifen kann, selbst wenn der Server offline ist. Damit Clients das Feature *Offlinedateien* verwenden können, muss für die Freigabe das Kontrollkästchen *Zwischenspeichern der Freigabe zulassen* aktiviert sein. Windows Server 2012 und Windows 8 verfügen zudem für das Feature *Offline-dateien* über den neuen Modus *Immer offline*. Clients verwenden dann immer die zwischengespeicherte Kopie der Serverdateien, was in einer besseren Performance resultiert. Um diesen Modus zu implementieren, müssen Sie auf dem Client die Gruppenrichtlinieneinstellung *Modus für langsame Verbindungen konfigurieren* auf den Wert 1 Millisekunde setzen.

9. Klicken Sie auf *Weiter*, um zur Seite *Berechtigungen zur Zugriffssteuerung angeben* weiterzugehen.
 10. Modifizieren Sie die Standardfreigabe- und NTFS-Berechtigungen nach Bedarf und klicken Sie auf *Weiter*. Die Seite *Auswahl bestätigen* erscheint.
-



Hinweis Erweiterte Freigabeprofile

Wenn Sie eines der erweiterten Freigabeprofile auswählen, zeigt der Assistent zwei zusätzliche Seiten an: *Ordnerverwaltungseigenschaften angeben* und *Kontingent auf einen Ordner oder auf ein Volume anwenden*. Über beide Seiten erreichen Sie Funktionen der Anwendung *Ressourcen-Manager für Dateiserver*, wie sie das Prüfungsziel »Ressourcen-Manager für Dateiserver konfigurieren« in der Zertifizierungsprüfung 70-411, »Administering Windows Server 2012«, beschreibt.

11. Klicken Sie auf *Erstellen*. Der Assistent erstellt die Freigabe und zeigt die Seite *Ergebnisse anzeigen* an.
12. Schließen Sie den Assistenten für neue Freigaben.

Nachdem Sie mithilfe des Assistenten eine Freigabe erstellt haben, erscheint die neue Freigabe im Server-Manager auf der Startseite *Freigaben* in der Kachel *Freigaben*. Jetzt können Sie über diese Kachel eine Freigabe verwalten, indem Sie mit der rechten Maustaste darauf klicken und ihr Blatt *Eigenschaften* öffnen oder auf *Freigabe beenden* klicken.

Berechtigungen zuweisen

Weiter vorn in diesem Kapitel haben Sie gelernt, wie Sie den Zugriff auf einen Dateiserver steuern, indem Sie den Netzwerkbenutzern den benötigten Zugriff gewähren und gleichzeitig andere Dateien gegenüber mögliche – gewollte oder ungewollte – Eingriffe und Schäden sichern. Diese Zugriffssteuerung implementiert Windows Server 2012 mithilfe von *Berechtigungen*.

Berechtigungen sind Privilegien, die bestimmten Systementitäten gewährt werden, beispielsweise Benutzern, Gruppen oder Computern, und diese in die Lage versetzen, eine Aufgabe durchzuführen oder auf eine Ressource zuzugreifen. Zum Beispiel können Sie eine bestimmte Benutzerberechtigung gewähren, um eine Datei zu lesen, und gleichzeitig demselben Benutzer die Berechtigungen verweigern, die Datei zu ändern oder zu löschen.

Windows Server 2012 verfügt über mehrere Berechtigungsgruppen, die unabhängig voneinander wirken. In Bezug auf die Dateifreigabe sollten Sie mit der Funktionsweise der folgenden Berechtigungssysteme vertraut sein:

- **Freigabeberechtigungen** Steuern den Zugriff auf Ordner über ein Netzwerk. Um auf eine Datei über ein Netzwerk zuzugreifen, benötigt ein Benutzer die passenden Freigabeberechtigungen (und passende NTFS-Berechtigungen, wenn sich der freigegebene Ordner auf einem NTFS-Volume befindet).
- **NTFS-Berechtigungen** Steuern den Zugriff auf die Dateien und Ordner von Datenträgervolumes, die mit dem NTFS-Dateisystem formatiert sind. Um auf eine Datei – entweder auf dem lokalen System oder über ein Netzwerk – zuzugreifen, benötigt der Benutzer die passenden NTFS-Berechtigungen.

Diese Berechtigungssysteme arbeiten unabhängig voneinander und greifen manchmal ineinander, um für eine bestimmte Ressource einen erhöhten Schutz zu bieten. Damit Netzwerkbenutzer auf einen freigegebenen Ordner auf einem NTFS-Laufwerk zugreifen können, müssen Sie ihnen sowohl Freigabeberechtigungen als auch NTFS-Berechtigungen gewähren. Wie bereits weiter vorn gezeigt, können Sie diese Berechtigungen bereits während der Freigabeerstellung zuweisen, aber auch im Nachhinein modifizieren.

Die Windows-Berechtigungsarchitektur verstehen

Um die Berechtigungen zu speichern, besitzt jedes dieser Elemente eine *Zugriffssteuerungsliste* (Access Control List, ACL). Eine ACL ist eine Auflistung von einzelnen Berechtigungen in Form von *Zugriffssteuerungseinträgen* (Access Control Entries, ACEs). Jeder ACE besteht aus einem Sicherheitsprinzipal (d.h. dem Namen des Benutzers, der Gruppe oder des Computers, dem/der die Berechtigungen gewährt werden) und den spezifischen Berechtigungen, die diesem Sicherheitsprinzipal zugewiesen sind. Wenn Sie Berechtigungen in einem der

Windows Server 2012-Berechtigungssysteme verwalten, erstellen und modifizieren Sie praktisch ACEs in einer ACL.

Berechtigungen in Windows Server 2012 verwalten Sie über eine Registerkarte auf dem Blatt *Eigenschaften* des geschützten Elements (siehe Abbildung 2.5), auf dem die Sicherheitsprinzipale oben und die zugeordneten Berechtigungen unten aufgelistet sind. Freigabeberechtigungen sind normalerweise auf einer Registerkarte *Freigabeberechtigungen* zu finden und NTFS-Berechtigungen auf einer Registerkarte *Sicherheit*. Alle Windows-Berechtigungssysteme verwenden die gleiche grundlegende Benutzeroberfläche, auch wenn sich die Berechtigungen an sich unterscheiden. Auch der Server-Manager bietet Zugriff auf NTFS- und Freigabeberechtigungen, allerdings mit einer leicht abgewandelten Benutzeroberfläche.

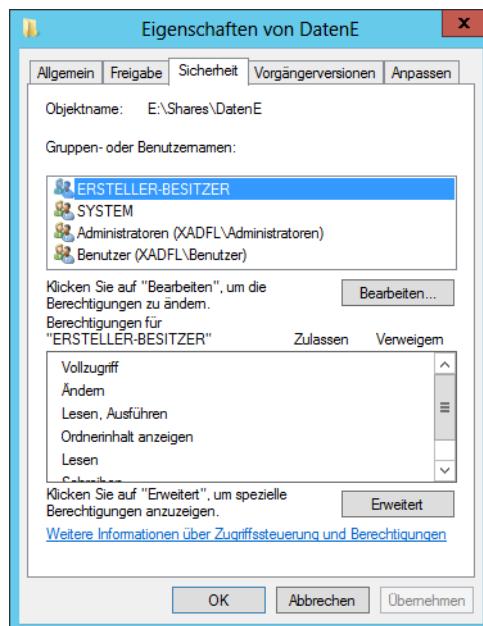


Abbildung 2.5 Die Registerkarte *Sicherheit* eines Dialogfelds *Eigenschaften*

Grundlegende und erweiterte Berechtigungen

Die Berechtigungen, die ein bestimmtes Systemelement schützen, sind nicht mit Schlüsseln zu einem Schloss vergleichbar, die entweder vollen oder überhaupt keinen Zugang bieten. Vielmehr sind Berechtigungen granular konzipiert, sodass Sie den Sicherheitsprinzipalen einen bestimmten Grad von Zugriff gewähren können.

Um diese Granularität zu realisieren, besitzt jedes Windows-Berechtigungssystem eine Kollektion von Berechtigungen, die Sie in beliebiger Kombination einem Sicherheitsprinzipal zuweisen können. Je nach dem Berechtigungssystem, mit dem Sie arbeiten, stehen möglicherweise Dutzende von unterschiedlichen Berechtigungen für ein einzelnes Systemelement zur Verfügung.

Windows bringt vordefinierte Berechtigungskombinationen mit, die für die gebräuchlichsten Zugriffssteuerungsszenarios geeignet sind. Auf der Registerkarte *Sicherheit* des Eigenschaftenblatts für ein Systemelement sind die NTFS-Eigenschaften unter der Bezeichnung *grundlegende Berechtigungen* aufgeführt. Dabei handelt es sich eigentlich um Kombinationen von erweiterten Berechtigungen, die die feinstufigste Steuerung über das Element bieten.



Tipp Vor Windows Server 2012 wurden grundlegende Berechtigungen als Standardberechtigungen und erweiterte Berechtigungen als spezielle Berechtigungen bezeichnet. Prüfungskandidaten sollten sich auch die alternativen Begriffe einprägen.

Zum Beispiel verfügt das NTFS-Berechtigungssystem über 14 erweiterte Berechtigungen, die Sie einem Order oder einer Datei zuweisen können. Allerdings gibt es auch sechs grundlegende Berechtigungen, die verschiedene Kombinationen der 14 erweiterten Berechtigungen verkörpern. In den meisten Fällen arbeiten Administratoren ausschließlich mit grundlegenden Berechtigungen und nur selten, wenn überhaupt, direkt mit erweiterten Berechtigungen.

Falls es Ihnen sinnvoll erscheint, direkt mit erweiterten Berechtigungen zu arbeiten – Windows macht es möglich. Wenn Sie auf die Schaltfläche *Erweitert* der Registerkarte *Sicherheit* eines Eigenschaftenblatts klicken, erscheint ein Dialogfeld *Erweiterte Sicherheitseinstellungen* (siehe Abbildung 2.6), in dem Sie direkt auf die ACEs für das ausgewählte Element zugreifen können. Vom System-Manager aus gelangen Sie über das Eigenschaftenblatt einer Freigabe zum gleichen Dialogfeld.

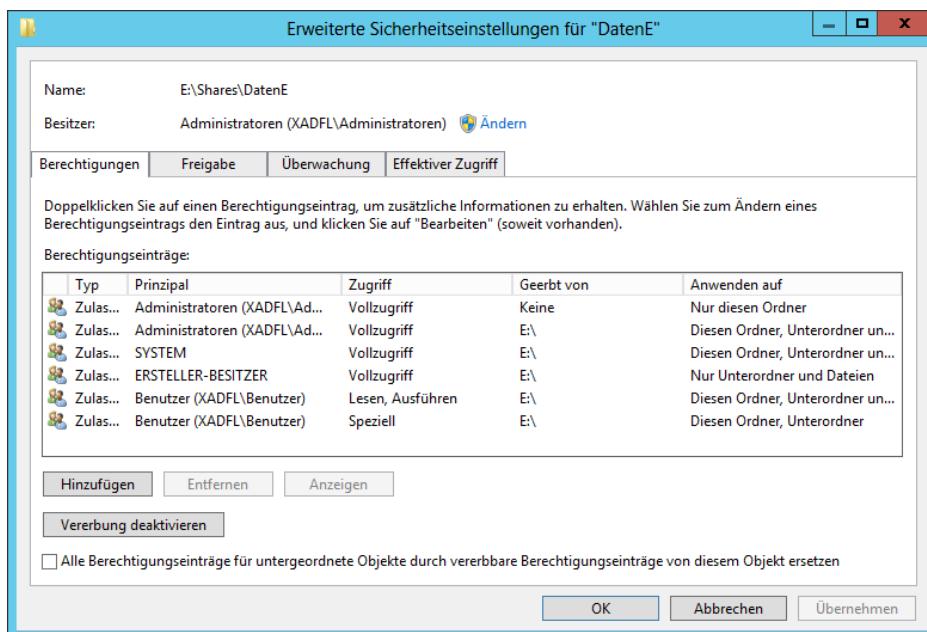


Abbildung 2.6 Das Dialogfeld *Erweiterte Sicherheitseinstellungen*

Berechtigungen erteilen und verweigern

Wenn Sie einem Systemelement Berechtigungen zuweisen, erstellen Sie letztlich einen neuen ACE in der ACL des Elements. Man unterscheidet zwei grundlegende ACE-Typen: *Zulassen* und *Verweigern*. Somit kann man sich der Berechtigungsverwaltung aus zwei Richtungen nähern:

- **Additiv** Ohne Berechtigungen beginnen und dann *Zulassen*-Berechtigungen an einzelne Sicherheitsprinzipale vergeben, um ihnen den benötigten Zugriff zu ermöglichen
- **Subtraktiv** Zunächst einzelnen Sicherheitsprinzipalen alle möglichen *Zulassen*-Berechtigungen gewähren, wodurch sie vollständige Kontrolle über das Systemelement erhalten, und ihnen dann *Verweigern*-Berechtigungen gewähren für die Zugriffe, die Sie ihnen nicht erlauben möchten

Die meisten Administratoren bevorzugen den additiven Ansatz, da Windows standardmäßig versucht, den Zugriff auf wichtige Systemelemente zu beschränken. In einer zweckmäßig gestalteten Berechtigungshierarchie sind *Verweigern*-Berechtigungen oftmals unnötig. Viele Administratoren missbilligen deren Verwendung, da es bei kombinierten *Zulassen*- und *Verweigern*-Berechtigungen in einer Hierarchie schwierig sein kann, die effektiven Berechtigungen für ein bestimmtes Systemelement zu ermitteln.

Berechtigungen vererben

Als wichtigstes Prinzip in der Berechtigungsverwaltung gilt, dass Berechtigungen in einer Hierarchie normalerweise nach unten weitergegeben werden. Das ist die sogenannte *Vererbung von Berechtigungen*. Wenn Sie zum Beispiel Alice die *Zulassen*-Berechtigungen für das Stammverzeichnis des Laufwerks D erteilen, erben sämtliche Ordner und Unterordner auf dem Laufwerk D diese Berechtigungen und Alice kann darauf zugreifen.

Das Prinzip der Vererbung vereinfacht das Zuweisen von Berechtigungen erheblich. Ohne Vererbung müssten Sie den Sicherheitsprinzipalen einzeln die *Zulassen*-Berechtigungen für jede Datei, jeden Ordner, jede Freigabe, jedes Objekt und jeden Schlüssel gewähren, für die sie Zugriff benötigen. Mit Vererbung lässt sich der Zugriff für ein ganzes Dateisystem gewähren, indem Sie einen Satz von *Zulassen*-Berechtigungen erstellen.

In den meisten Fällen – ob bewusst oder nicht – berücksichtigen Systemadministratoren die Vererbung, wenn sie die Struktur ihrer Dateisysteme und Active Directory-Domänen-dienste konzipieren. Der Speicherort eines Systemelements in einer Hierarchie basiert oftmals darauf, wie die Administratoren Berechtigungen zuweisen möchten.

In manchen Situationen wird es ein Administrator unterbinden wollen, dass untergeordnete Elemente die Berechtigungen ihrer übergeordneten Elemente erben. Hierfür gibt es zwei Möglichkeiten:

- **Vererbung deaktivieren** Wenn Sie erweiterte Berechtigungen zuweisen, können Sie einen ACE so konfigurieren, dass er seine Berechtigungen nicht an die untergeordneten Elemente weitergibt. Damit blockieren Sie praktisch den Vererbungsvorgang.
- **Berechtigungen verweigern** Wenn Sie einem Systemelement eine *Verweigern*-Berechtigung zuweisen, überschreibt sie jegliche *Zulassen*-Berechtigungen, die das Element gegebenenfalls von seinen übergeordneten Objekten geerbt hat

Effektiver Zugriff

Einem Sicherheitsprinzipal können Berechtigungen auf viele Arten erteilt werden und ein Administrator muss verstehen, wie diese Berechtigungen zusammenwirken. Die Kombination von *Zulassen-* und *Verweigern-*Berechtigungen, die einem Sicherheitsprinzipal für ein bestimmtes Systemelement – ob explizit zugewiesen, vererbt oder über eine Gruppenmitgliedschaft – erteilt werden, ist der sogenannte *effektive Zugriff* für dieses Element. Da einem Sicherheitsprinzipal Berechtigungen aus verschiedenen Quellen erteilt werden können, ist es nicht ungewöhnlich, dass diese Berechtigungen miteinander kollidieren. Die folgenden Regeln definieren, wie die Berechtigungen zusammenwirken, um den effektiven Zugriff bilden:

- **Zulassen-Berechtigungen sind kumulativ** Werden einem Sicherheitsprinzipal *Zulassen-*Berechtigungen aus mehreren Quellen erteilt, bilden die zusammengefassten Berechtigungen die effektiven Zugriffsberichtigungen
- **Verweigern-Berechtigungen überschreiben Zulassen-Berechtigungen** Werden einem Sicherheitsprinzipal *Zulassen-*Berechtigungen – ob explizit, durch Vererbung oder aus einer Gruppe – erteilt, können Sie diese Berechtigungen überschreiben, indem Sie dem Prinzipal *Verweigern-*Berechtigungen desselben Typs erteilen
- **Explizite Berechtigungen haben Vorrang gegenüber geerbten Berechtigungen** Werden einem Sicherheitsprinzipal Berechtigungen durch Vererbung von einem übergeordneten Objekt oder von Gruppenmitgliedschaften erteilt, können Sie diese Berechtigungen überschreiben, indem Sie dem Sicherheitsprinzipal selbst explizit sich widersprechende Berechtigungen zuweisen

Anstatt alle möglichen Berechtigungsquellen zu untersuchen und auszuwerten, können Sie selbstverständlich auch das Dialogfeld *Erweiterte Sicherheitseinstellungen* öffnen und auf die Registerkarte *Effektiver Zugriff* gehen. Diese Registerkarte erlaubt es, einen Benutzer, eine Gruppe oder ein Gerät auszuwählen und dessen effektiven Zugriff anzuzeigen, mit oder ohne den Einfluss spezifischer Gruppen.

Freigabeberechtigungen festlegen

Unter Windows Server 2012 besitzen freigegebene Ordner ihr eigenes Berechtigungssystem, das unabhängig von den anderen Windows-Berechtigungssystemen ist. Damit Netzwerkbenutzer auf Freigaben auf einem Dateiserver zugreifen können, müssen Sie ihnen die passenden Freigabeberechtigungen erteilen. Standardmäßig wird der speziellen Identität *Jeder* die Freigabeberechtigung *Vollzugriff* für jede neue Freigabe erteilt, die Sie erstellen. Möchten Sie die Freigabeberechtigungen für eine vorhandene Freigabe mittels Dateiexplorer ändern, öffnen Sie das Eigenschaftenblatt für den freigegebenen Ordner, wechseln zur Registerkarte *Freigabe*, klicken auf die Schaltfläche *Erweiterte Freigabe* und dann auf die Schaltfläche *Berechtigungen*. Daraufhin gelangen Sie zur Registerkarte *Freigabeberechtigungen*, wie sie Abbildung 2.7 zeigt.

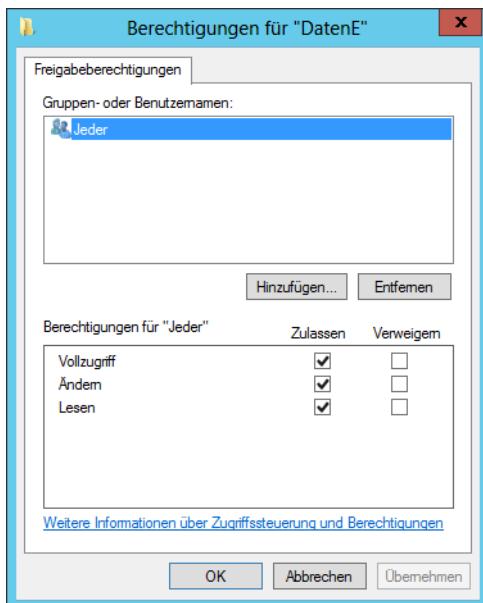


Abbildung 2.7 Die Registerkarte *Freigabeberechtigungen* für einen freigegebenen Ordner

Über diese Benutzeroberfläche können Sie Sicherheitsprinzipale hinzufügen und ihnen die drei Freigabeberechtigungen erteilen oder entziehen. Führen Sie die folgenden Schritte aus, um Freigabeberechtigungen mithilfe des Server-Managers festzulegen (entweder wenn Sie eine Freigabe erstellen oder wenn Sie eine vorhandene Freigabe modifizieren):

1. Melden Sie sich bei Windows Server 2012 an und starten Sie den Server-Manager.
2. Klicken Sie auf das Symbol *Datei- und Speicherdiene* und im daraufhin eingeblendeten Untermenü auf *Freigaben*, um die Startseite *Freigaben* zu öffnen.
3. Klicken Sie mit der rechten Maustaste in der Kachel *Freigaben* auf eine Freigabe und wählen Sie im Kontextmenü den Befehl *Eigenschaften*, um das Eigenschaftenblatt für die Freigabe zu öffnen.
4. Klicken Sie auf *Berechtigungen*. Es erscheint die Seite *Berechtigungen*.
5. Klicken Sie auf *Berechtigungen anpassen*, um das Dialogfeld *Erweiterte Sicherheitseinstellungen* für die Freigabe zu öffnen.
6. Wechseln Sie zur Registerkarte *Freigabe*. Damit gelangen Sie zu der Benutzeroberfläche, die in Abbildung 2.8 zu sehen ist.

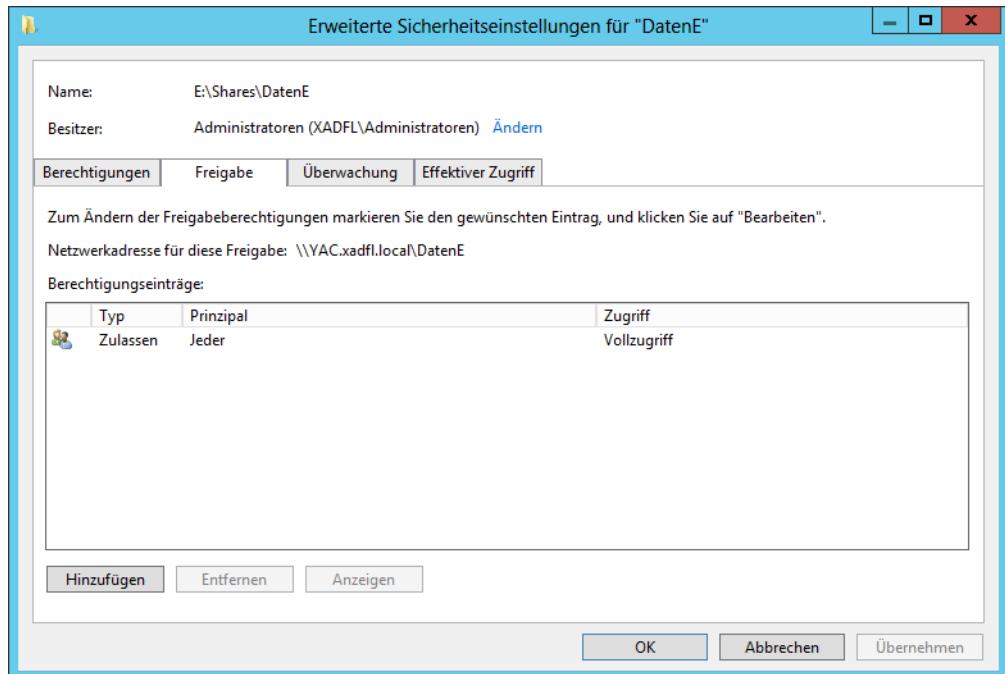


Abbildung 2.8 Die Registerkarte *Freigabe* des Dialogfelds *Erweiterte Sicherheitseinstellungen* für eine Freigabe im Server-Manager

7. Klicken Sie auf *Hinzufügen*, um das Dialogfeld *Berechtigungseintrag* für die Freigabe zu öffnen.
8. Klicken Sie auf den Link *Prinzipal auswählen*. Daraufhin wird das Dialogfeld *Benutzer, Computer, Dienstkonto oder Gruppe auswählen* angezeigt.
9. Geben Sie den Namen ein oder suchen Sie nach dem Sicherheitsprinzipal, dem Sie Freigabeberechtigungen erteilen möchten, und klicken Sie auf *OK*. Der angegebene Sicherheitsprinzipal erscheint im Dialogfeld *Berechtigungseintrag*.
10. Wählen Sie den Typ der zuzuweisenden Berechtigungen aus (*Zulassen* oder *Verweigern*).
11. Aktivieren Sie die Kontrollkästchen für die Berechtigungen, die Sie zuweisen möchten, und klicken Sie auf *OK*.
12. Der eben erstellte neue ACE erscheint im Dialogfeld *Erweiterte Sicherheitseinstellungen*.



Hinweis Freigabeberechtigungen umgehen

Wie diese Lektion später noch erläutert, behalten viele Dateiserveradministratoren die Berechtigung *Vollzugriff* für die spezielle Identität *Jeder* einfach bei, umgehen damit praktisch das Freigabeberechtigungssystem und stützen sich ausschließlich auf NTFS-Berechtigungen, um einen feinstufigen Schutz für das Dateisystem zu realisieren.

13. Klicken Sie auf *OK*, um das Dialogfeld *Erweiterte Sicherheitseinstellungen* zu schließen.
14. Klicken Sie auf *OK*, um das Eigenschaftenblatt der Freigabe zu schließen.
15. Schließen Sie das Fenster *Server-Manager*.

NTFS-Autorisierung

Die Mehrheit der heutigen Windows-Installationen verwendet die NTFS- und ReFS-Dateisysteme im Unterschied zu FAT32. Zu den wesentlichen Vorteilen von NTFS und ReFS gehört, dass sie Berechtigungen unterstützen, was bei FAT32 nicht der Fall ist. Wie bereits weiter vorn in diesem Kapitel erläutert, besitzt jede Datei und jeder Ordner auf einem NTFS- oder ReFS-Laufwerk eine ACL, bestehend aus ACEs, von denen jeder einen Sicherheitsprinzipal und die diesem Prinzipal zugewiesenen Berechtigungen enthält.

Im NTFS-Berechtigungssystem, das auch ReFS unterstützt, sind die Sicherheitsprinzipale Benutzer und Gruppen, die Windows unter ihren Sicherheitsbezeichnern (Security Identifier, SID) anspricht. Wenn ein Benutzer auf eine NTFS-Datei oder einen NTFS-Ordner zugreifen möchte, liest das System das Sicherheitszugriffstoken des Benutzers. Es enthält die SIDs für das Benutzerkonto und alle Gruppen, zu denen der Benutzer gehört. Dann vergleicht das System diese SIDs mit denen, die in den ACEs der Datei oder des Ordners gespeichert sind, um die Zugriffsrechte des Benutzers zu ermitteln. Dieser Vorgang heißt *Autorisierung*.

Grundlegende NTFS-Berechtigungen zuweisen

Die meisten Dateiserveradministratoren arbeiten ausschließlich mit grundlegenden NTFS-Berechtigungen, da es bei den gebräuchlichen Aufgaben der Zugriffssteuerung nicht notwendig ist, direkt mit erweiterten Berechtigungen zu arbeiten.

Um einem freigegebenen Ordner grundlegende NTFS-Berechtigungen zuzuweisen, stehen praktisch die gleichen Optionen wie bei Freigabeberechtigungen zur Verfügung. Öffnen Sie dazu das Eigenschaftenblatt des Ordners im Dateiexplorer und gehen Sie auf die Registerkarte *Sicherheit* oder öffnen Sie das Eigenschaftenblatt der Freigabe im Server-Manager, wie es der folgende Ablauf beschreibt.

1. Melden Sie sich bei Windows Server 2012 an und starten Sie den Server-Manager.
2. Öffnen Sie die Startseite *Freigaben*.



Hinweis NTFS-Berechtigungen

NTFS-Berechtigungen sind nicht auf freigegebene Ordner beschränkt. Auf einem NTFS-Volume besitzt jede Datei und jeder Ordner Berechtigungen. Diese Prozedur beschreibt zwar, wie Sie einem freigegebenen Ordner Berechtigungen zuweisen, doch können Sie auch das Eigenschaftenblatt für einen beliebigen Ordner in einem Dateiexplorerfenster öffnen, auf die Registerkarte *Sicherheit* wechseln und hier auf die gleiche Weise die NTFS-Berechtigungen des Ordners bearbeiten.

3. Öffnen Sie das Eigenschaftenblatt für eine Freigabe und klicken Sie auf *Berechtigungen*, um zur Seite *Berechtigungen* zu gelangen.



Hinweis Der Assistent für neue Freigaben

Der Assistent für neue Freigaben zeigt auf seiner Seite *Berechtigungen zur Zugriffssteuerung angeben* die gleiche *Berechtigungen*-Oberfläche an. Die weiteren Schritte in dieser Prozedur gelten also gleichermaßen für diese Seite und deren darauffolgende Dialogfelder.

4. Klicken Sie auf *Berechtigungen anpassen*, um das Dialogfeld *Erweiterte Sicherheitseinstellungen* für die Freigabe mit der Registerkarte *Berechtigungen* zu öffnen, wie Abbildung 2.9 zeigt. Dieses Dialogfeld gibt den Inhalt einer ACL wieder, soweit es mit der grafischen Benutzeroberfläche von Windows machbar ist.

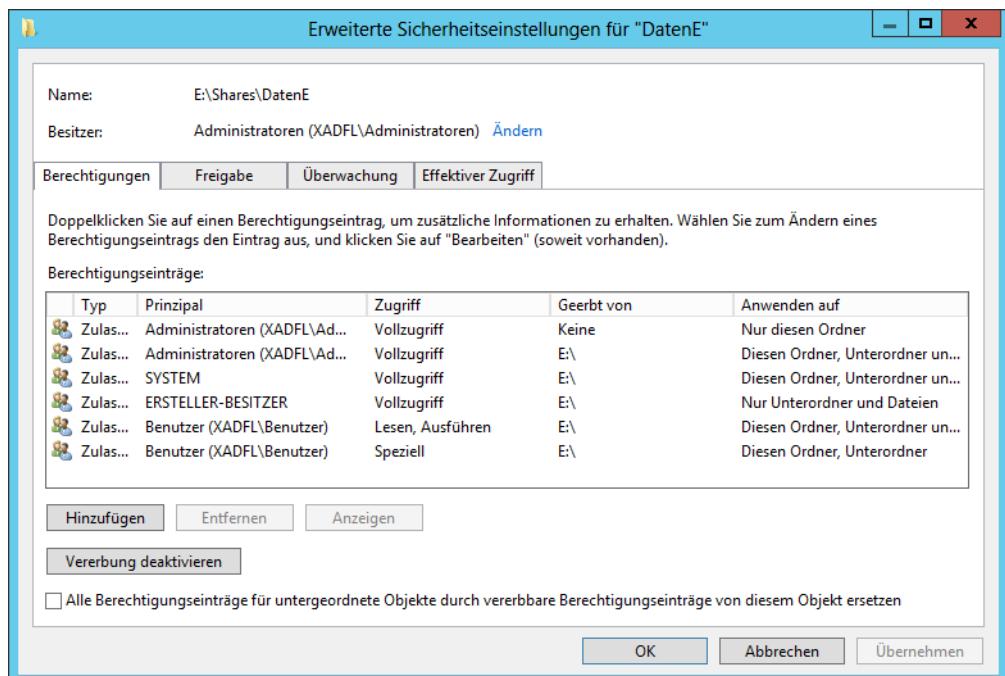


Abbildung 2.9 Das Dialogfeld *Erweiterte Sicherheitseinstellungen* für eine Freigabe im Server-Manager

5. Klicken Sie auf *Hinzufügen*. Daraufhin erscheint das Dialogfeld *Berechtigungseintrag* für die Freigabe.
6. Klicken Sie auf den Link *Prinzipal auswählen*, um das Dialogfeld *Benutzer, Computer, Dienstkonto oder Gruppe auswählen* zu öffnen.
7. Geben Sie den Namen des Sicherheitsprinzipals, dem Sie Freigabeberechtigungen zuweisen möchten, ein (oder suchen Sie nach dem Namen) und klicken Sie auf *OK*. Der angegebene Sicherheitsprinzipal erscheint im Dialogfeld *Berechtigungseintrag*.

8. Wählen Sie in der Dropdownliste *Typ* den Typ der zuzuweisenden Berechtigung (*Zulassen* oder *Verweigern*) aus.
9. Legen Sie in der Dropdownliste *Anwenden auf* fest, welche Unterordner und Dateien die zugewiesenen Berechtigungen erben sollen.
10. Aktivieren Sie die Kontrollkästchen für die grundlegenden Berechtigungen, die Sie zuweisen möchten, und klicken Sie auf *OK*. Der eben erstellte neue ACE erscheint im Dialogfeld *Erweiterte Sicherheitseinstellungen*.
11. Klicken Sie zweimal auf *OK*, um das Dialogfeld *Erweiterte Sicherheitseinstellungen* und das Eigenschaftenblatt zu schließen.
12. Schließen Sie das Fenster *Server-Manager*.

Erweiterte NTFS-Berechtigungen zuweisen

In Windows Server 2012 lassen sich auch die erweiterten Berechtigungen in derselben Benutzeroberfläche verwalten, die Sie auch für die grundlegenden Berechtigungen verwenden.

Wenn Sie im Dialogfeld *Berechtigungseintrag* auf den Link *Erweiterte Berechtigungen anzeigen* klicken, tritt an die Stelle der Liste mit grundlegenden Berechtigungen eine Liste mit erweiterten Berechtigungen. Dann können Sie erweiterte Berechtigungen in beliebiger Kombination zuweisen, genau wie Sie es bereits von den grundlegenden Berechtigungen her kennen.

Freigabe- und NTFS-Berechtigungen kombinieren

Für Dateiserveradministratoren ist es wichtig zu wissen, dass die NTFS- und Freigabeberechtigungssysteme vollkommen getrennt voneinander sind und dass Netzwerkbenutzer sowohl die richtigen NTFS- als auch die richtigen Freigabeberechtigungen besitzen müssen, damit sie auf die Dateien eines freigegebenen NTFS-Laufwerks zugreifen können.

Die einer Datei oder einem Ordner zugewiesenen Freigabe- und NTFS-Berechtigungen können allerdings kollidieren. Wenn zum Beispiel ein Benutzer die NTFS-Berechtigungen *Schreiben* und *Ändern* für einen Ordner besitzt, jedoch keine *Ändern*-Berechtigungen für die Freigabe, ist dieser Benutzer nicht in der Lage, eine Datei in diesem Ordner zu modifizieren.

Das Freigabeberechtigungssystem ist das einfachste der Windows-Berechtigungssysteme und bietet nur grundlegenden Schutz für freigegebene Netzwerkressourcen. Für Freigabeberechtigungen sind lediglich drei Zugriffsebenen definiert, im Unterschied zu dem weit komplexeren System der NTFS-Berechtigungen. Im Allgemeinen bevorzugen Netzwerkadministratoren entweder die NTFS-Berechtigungen oder die Freigabeberechtigungen, verwenden jedoch nicht beide Systeme.

Freigabeberechtigungen bieten begrenzten Schutz, doch kann dieser insbesondere bei kleinen Netzwerken durchaus genügen. Freigabeberechtigungen können auch auf einem Computer mit FAT32-Laufwerken die einzige Option sein, da das FAT-Dateisystem kein eigenes Berechtigungssystem mitbringt.

In einem Netzwerk, das bereits mit einem zweckmäßig gestalteten System von NTFS-Berechtigungen ausgestattet ist, sind Freigabeberechtigungen wirklich nicht notwendig. In diesem Fall können Sie gefahrlos die Freigabeberechtigung *Vollzugriff für Jeder* unverändert übernehmen, die standardmäßige *Lesen*-Berechtigung überschreiben und Sicherheit mit NTFS-Berechtigungen gewährleisten. Wenn Sie Freigabeberechtigungen hinzufügen, verkompliziert sich der Administrationsprozess, ohne irgendwelche zusätzliche Sicherheit zu bringen.

Volumeschattenkopien konfigurieren

Das Windows Server 2012-Feature *Volumeschattenkopien* versetzt Sie in die Lage, vorherige Versionen von Dateien auf einem Server zu verwalten, sodass Benutzer auf eine Kopie zugreifen können, falls sie eine Datei versehentlich gelöscht oder überschrieben haben. Volumeschattenkopien lassen sich nur für ein gesamtes Volume implementieren; es ist nicht möglich, bestimmte Freigaben, Order oder Dateien auszuwählen.

Führen Sie die folgenden Schritte aus, um ein Windows Server 2012-Volume zu konfigurieren und Schattenkopien zu erstellen:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an.
2. Öffnen Sie den Datei-Explorer. Das Fenster *Datei-Explorer* erscheint.
3. Erweitern Sie in der Liste *Ordner* den Container *Computer*, klicken Sie mit der rechten Maustaste auf ein Volume und wählen Sie im Kontextmenü *Schattenkopien konfigurieren*. Daraufhin wird das Dialogfeld *Schattenkopien* geöffnet, das Abbildung 2.10 zeigt.

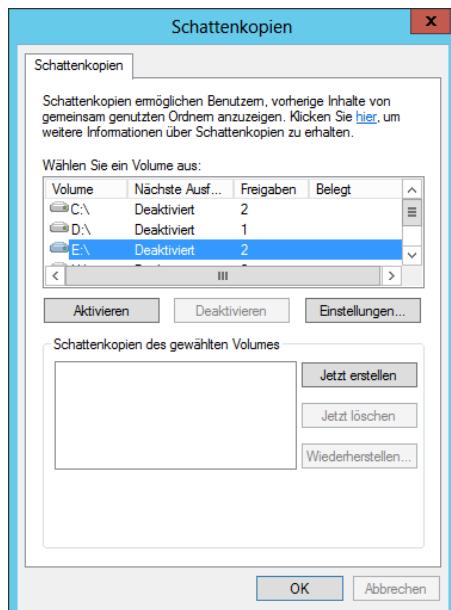


Abbildung 2.10 Das Dialogfeld *Schattenkopien*

4. Legen Sie im Feld *Wählen Sie ein Volume aus* das Volume fest, für das Sie Schattenkopien aktivieren möchten. Wenn Sie Schattenkopien für ein Volume aktivieren, verwendet das System folgende Standardeinstellungen:
 - Das System speichert die Schattenkopien auf dem ausgewählten Volume
 - Das System reserviert mindestens 300 MB Festplattenplatz für die Schattenkopien
 - Das System erzeugt Schattenkopien wöchentlich von Montag bis Freitag jeweils um 7:00 Uhr
5. Möchten Sie die Standardparameter ändern, klicken Sie auf *Einstellungen*.
6. Legen Sie im Dialogfeld *Einstellungen* im Feld *Speicherbereich* das Volume fest, wo die Schattenkopien gespeichert werden sollen.
7. Legen Sie die maximale Größe für den Speicherbereich fest oder wählen Sie die Option *Unbegrenzt*. Wenn der Speicherbereich voll ist, löscht das System jeweils die ältesten Schattenkopien.
8. Klicken Sie auf *Zeitplan*. Mit den Steuerelementen auf der Registerkarte *Zeitplan* können Sie je nach den Anforderungen Ihrer Benutzer die vorhandenen Aufgaben für Schattenkopien ändern, löschen oder neue Aufgaben erstellen.
9. Klicken Sie jeweils auf *OK*, um die Dialogfelder *Zeitplan* und *Einstellungen* zu schließen.
10. Klicken Sie auf *Aktivieren*. Das System aktiviert das Feature *Schattenkopien* für das ausgewählte Volume und erstellt die erste Kopie im angegebenen Speicherbereich.
11. Schließen Sie den Datei-Explorer.

Nachdem Sie diese Schritte abgeschlossen haben, können Sie vorherige Versionen von Dateien auf den ausgewählten Volumes über die Registerkarte *Vorgängerversionen* oder jedes Eigenschaftenblatt einer Datei oder eines Ordners wiederherstellen.

Datenträgerkontingente konfigurieren

Die Verwaltung von Festplattenplatz gehört zu den ständigen Aufgaben von Serveradministratoren. Mithilfe von *Datenträgerkontingenten* (Quotas) lässt sich verhindern, dass Benutzer den ganzen Speicherplatz an sich reißen. Windows Server 2012 unterstützt zwei Typen von Datenträgerkontingenten. Die aufwendigere Variante ist als Teil des FSRM (File Server Resource Manager) implementiert. Die zweite und einfachere Option ist über NTFS-Datenträgerkontingente realisiert.

Administratoren können mithilfe von NTFS-Datenträgerkontingenten für Benutzer eines bestimmten Volumes ein Speicherlimit festlegen. Je nachdem, wie Sie die Datenträgerkontingente konfigurieren, kann Benutzern, die das Limit überschreiten, entweder der Festplattenplatz verweigert oder eine Warnung gesendet werden. Der von einzelnen Benutzern konsumierte Speicherplatz wird anhand der Größe der Dateien ermitteln, die sie besitzen oder erstellen.

NTFS-Datenträgerkontingente sind in dem Sinne recht beschränkt, da sich Limits nur auf der Volumeebene festlegen lassen. Außerdem ist das Feature in Bezug auf die Aktionen beschränkt, die man als Reaktion auf die Überschreitung des Limits durch einen Benutzer unternehmen kann. Dagegen sind die Datenträgerkontingente im Ressourcen-Manager für Dateiserver (File Server Resource Manager) wesentlich flexibler hinsichtlich der festlegbaren Limits und der Reaktionen des Programms, das E-Mail-Benachrichtigungen senden und Befehle ausführen sowie Berichte generieren und Ereignisse protokollieren kann.

Führen Sie die folgenden Schritte aus, um NTFS-Datenträgerkontingente für ein Volume zu konfigurieren:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an.
2. Öffnen Sie den Datei-Explorer.
3. Im Fenster *Datei-Explorer* erweitern Sie in der Liste *Ordner* den Container *Computer*, klicken mit der rechten Maustaste auf ein Volume und wählen *Eigenschaften* aus dem Kontextmenü.
4. Klicken Sie im Eigenschaftenblatt für das Volume auf die Registerkarte *Kontingent*. Es erscheint die in Abbildung 2.11 gezeigte Benutzeroberfläche.

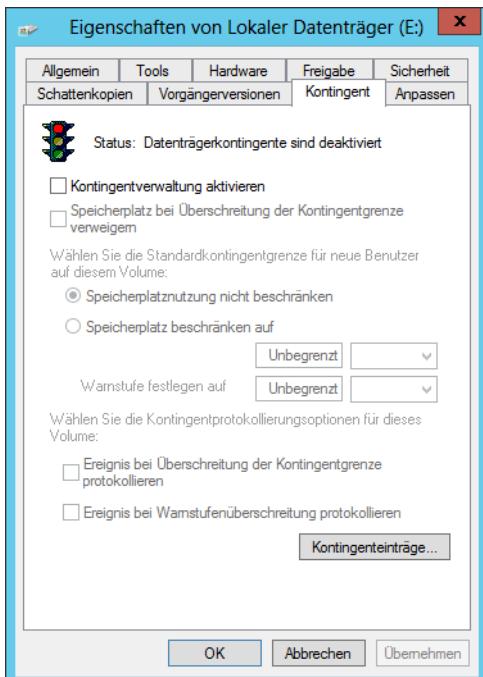


Abbildung 2.11 Die Registerkarte *Kontingent* im Eigenschaftenblatt eines Volumes

5. Setzen Sie das Kontrollkästchen *Kontingentverwaltung aktivieren*, um die übrigen Steuerelemente zu aktivieren.
6. Möchten Sie verhindern, dass Benutzer mehr als ihr Datenträgerkontingent verbrauchen, aktivieren Sie das Kontrollkästchen *Speicherplatz bei Überschreitung der Kontingentgrenze verweigern*.
7. Wählen Sie die Option *Speicherplatz beschränken auf* und legen Sie die Werte für das Kontingentlimit und die Warnstufe fest.
8. Aktivieren Sie die Kontrollkästchen *Ereignis protokollieren*, falls bei Überschreitung der angegebenen Limits durch die Benutzer Protokolleinträge generiert werden sollen.
9. Klicken Sie auf *OK*, um die Kontingente einzurichten und das Eigenschaftenblatt zu schließen.
10. Schließen Sie den Datei-Explorer.

Prüfungszielzusammenfassung

- Ordnerfreigaben machen die auf den Datenträgern eines Dateiservers gespeicherten Daten für Netzwerkbenutzer zugänglich
- Mit NTFS-Berechtigungen steuern Sie den Zugriff auf Dateien und Ordner. Dazu spezifizieren Sie die Aufgaben, die die einzelnen Benutzer auf den Dateien und Ordnern ausführen dürfen. Freigabeberechtigungen bieten elementare Zugriffssteuerung für alle Dateien auf einer Netzwerksfreigabe. Netzwerkbenutzer müssen über die passenden Freigabe- und NTFS-Berechtigungen verfügen, um auf Freigaben von Dateiservern zugreifen zu können.
- Zugriffsbasierte Aufzählung (Access-based Enumeration, ABE) wendet Filter auf freigegebene Ordner basierend auf den Berechtigungen einzelner Benutzer auf die Dateien und Unterordner in der Freigabe an. Kurz gesagt sehen Benutzer, die auf eine bestimmte freigegebene Ressource nicht zugreifen können, diese Ressource auch nicht im Netzwerk.
- Das Feature *Offlinedateien* ermöglicht es Clientsystemen, lokale Kopien der Dateien zu verwalten, auf die sie von Serverfreigaben aus zugreifen
- Das Windows Server 2012-Feature *Volumeschattenkopien* versetzt Sie in die Lage, vorherige Versionen von Dateien auf einem Server zu verwalten, sodass Benutzer auf eine Kopie zugreifen können, falls sie eine Datei versehentlich gelöscht oder überschrieben haben
- Administratoren können mithilfe von NTFS-Datenträgerkontingenzen für Benutzer eines bestimmten Volumes ein Speicherlimit festlegen

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahl-

möglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Wie viele Schattenkopien kann ein Windows Server 2012-System für jedes Volume maximal verwalten?
 - A. 8
 - B. 16
 - C. 64
 - D. 128
2. Welcher der folgenden Begriffe beschreibt den Vorgang, Benutzern den Zugriff auf Freigaben von Dateiservern zu erteilen, indem ihre Berechtigungen gelesen werden?
 - A. Authentifizierung
 - B. Autorisierung
 - C. Aufzählung
 - D. Zuweisung
3. Welche der folgenden Aufgaben können Sie mithilfe der Datenträgerkontingente im Resourcen-Manager für Dateiserver durchführen, jedoch nicht mithilfe von NTFS-Datenträgerkontingenzen? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Eine E-Mail-Nachricht an einen Administrator senden, wenn Benutzer ihre Limits überschreiten.
 - B. Für jeden Benutzer unterschiedliche Speicherlimits festlegen.
 - C. Benutzer daran hindern, Speicherbereich auf einem Volume über das zugestandene Limit hinaus zu verbrauchen.
 - D. Warnungen an Benutzer generieren, wenn sie sich ihrem zugestandenen Speicherlimit nähern.
4. Im NTFS-Berechtigungssystem sind Kombinationen von erweiterten Berechtigungen auch als _____ Berechtigungen bekannt. (Wählen Sie alle zutreffenden Antworten aus.)
 - A. spezielle
 - B. grundlegende
 - C. Freigabe-
 - D. Standard-

5. Welche der folgenden Aussagen definiert am besten die Rolle des Sicherheitsprinzips bei Berechtigungszuweisungen im Dateisystem?
 - A. Die einzige Person, die auf eine Datei zugreifen kann, der keine Berechtigungen zugewiesen wurden.
 - B. Die Person, die für das Erstellen von Berechtigungsrichtlinien verantwortlich ist.
 - C. Die Person, die Berechtigungen zuweist.
 - D. Die Person, der Berechtigungen zugewiesen werden.



Gedankenexperiment Wenden Sie in diesem Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Sie arbeiten am Helpdesk für ein Unternehmensnetzwerk und erhalten einen Anruf von einem Benutzer Leo, der Zugriff auf die Dateien für ein neu klassifiziertes Projekt namens Contoso verlangt. Die Contoso-Dateien sind in einem freigegebenen Ordner auf einem Dateiserver gespeichert, der abgesperrt in einem gesicherten unterirdischen Datenspeicherzentrum steht. Nachdem Sie sich davon überzeugt haben, dass der Benutzer die erforderlichen Unbedenklichkeitsbescheinigungen besitzt, erstellen Sie eine neue Gruppe CONTOSO_USERS auf dem Dateiserver und fügen das Benutzerkonto von Leo dieser Gruppe hinzu.

Dann nehmen Sie die Gruppe CONTOSO_USERS in die Zugriffsteuerungsliste für den Ordner *Trinity* auf dem Dateiserver auf und weisen der Gruppe die folgenden NTFS-Berechtigungen zu:

- Zulassen Ändern
- Zulassen Lesen & Ausführen
- Zulassen Ordnerinhalt anzeigen
- Zulassen Lesen
- Zulassen Schreiben

Später ruft Leo Sie zurück und teilt Ihnen mit, dass er zwar auf den Contoso-Ordner zugreifen und die dort gespeicherten Dateien lesen kann, er aber nicht in der Lage ist, Änderungen zurück auf den Server zu speichern.

Worin liegt höchstwahrscheinlich die Ursache für das Problem?

Prüfungsziel 2.2: Druck- und Dokumentdienste konfigurieren

Wie die im vorherigen Abschnitt behandelten Funktionen für die Dateifreigabe gehört die Freigabe von Druckdiensten zu den grundlegendsten Anwendungen, für die lokale Netzwerke konzipiert sind.

Dieses Prüfungsziel zeigt, wie Sie

- den Easy Print-Druckertreiber konfigurieren
 - die Druckverwaltung des Unternehmens konfigurieren
 - Treiber konfigurieren
 - Druckerpools konfigurieren
 - Druckerprioritäten konfigurieren
 - Druckerberechtigungen konfigurieren
-

Einen Druckerserver bereitstellen

Es ist relativ einfach, einen einzelnen Netzwerkdruckerdienst zu installieren, freizugeben, zu überwachen und zu verwalten, doch wenn Sie für Dutzende oder sogar Hunderte von Druckdiensten in einem großen Unternehmensnetzwerk zuständig sind, können diese Aufgaben zu einer echten Herausforderung werden.

Die Windows-Druckerarchitektur

In Bezug auf die Komponenten der Netzwerkdruckerarchitektur ist es wichtig, die von Microsoft verwendeten Termini zu verstehen. Beim Drucken in Microsoft Windows sind normalerweise die folgenden vier Komponenten beteiligt:

- **Druckgerät** Dies ist die eigentliche Hardware, die Dokumente auf Papier oder anderen Druckmedien erzeugt. Windows Server 2012 unterstützt sowohl lokale Druckgeräte, die direkt an Computerports angeschlossen sind, als auch Druckgeräte mit Netzwerkschnittstelle, die über Netzwerk entweder direkt oder über einen anderen Computer angeschlossen sind.
- **Drucker** In Windows versteht man unter einem Drucker die Softwareschnittstelle, über die ein Computer mit einem Druckgerät kommuniziert. Windows Server 2012 unterstützt zahlreiche physische Schnittstellen, einschließlich USB (Universal Serial Bus)-, IEEE 1394 (FireWire)-, parallele (LPT), serielle (COM), IrDA (Infrared Data Access)- und Bluetooth-Anschlüsse sowie Netzwerkdruckerdienste wie zum Beispiel lpr-, IPP (Internet Printing Protocol)- und Standard-TCP/IP-Anschlüsse.
- **Druckerserver** Hierbei handelt es sich um einen Computer (oder ein eigenständiges Gerät), das Druckaufträge von Clients entgegennimmt und sie an Druckgeräte sendet, die entweder lokal angeschlossen oder über das Netzwerk verbunden sind

- **Druckertreiber** Dies ist ein Gerätetreiber, der die von Anwendungen generierten Druckaufträge in eine geeignete Befehlssequenz für ein bestimmtes Druckgerät konvertiert. Druckertreiber werden für bestimmte Druckgeräte entworfen und bieten Anwendungen den Zugriff auf sämtliche Features des jeweiligen Druckgeräts.



Hinweis Nomenklatur für Drucker

Die Begriffe »Drucker« und »Druckgerät« werden im Windows-Druckervokabular am häufigsten falsch verwendet. Offenbar beziehen sich viele Quellen mit »Drucker« auf die Druckerhardware. In Windows jedoch sind Drucker und Druckgerät nicht gleichbedeutend. Zum Beispiel können Sie einem Windows Server 2012-Computer einen Drucker hinzufügen, ohne dass ein physisches Druckgerät vorhanden ist. Der Computer kann dann den Drucker, Druckerserver und Druckertreiber hosten. Diese drei Komponenten versetzen den Computer in die Lage, Druckaufträge zu verarbeiten und sie in einer Druckwarteschlange zu speichern, bis das Druckgerät verfügbar ist.

Das Drucken unter Windows

Die vier genannten Komponenten wirken zusammen, um die von Windows-Anwendungen erzeugten Druckaufträge zu verarbeiten und sie in gedruckte Dokumente zu überführen, wie Abbildung 2.12 zeigt.

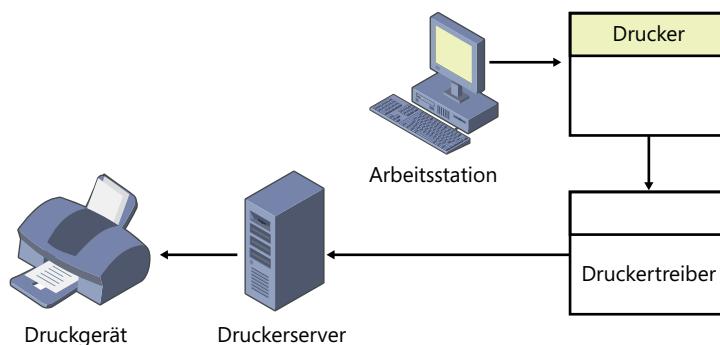


Abbildung 2.12 Die Windows-Druckerarchitektur

Bevor Sie in Windows Dokumente drucken können, müssen Sie mindestens einen Drucker installieren. Dazu sind folgende Schritte erforderlich:

- Hersteller und Modell des jeweiligen Druckgeräts auswählen
- Den Anschluss (oder eine andere Schnittstelle) spezifizieren, über die der Computer auf das Druckgerät zugreift
- Einen Druckertreiber bereitstellen, der speziell für dieses Druckgerät geschrieben ist

Wenn Sie aus einer Anwendung heraus ein Dokument drucken, wählen Sie den Drucker aus, der als Ziel für den Druckauftrag fungiert.

Dem Drucker ist ein Druckertreiber zugeordnet, der die von der Anwendung generierten Befehle übernimmt und sie in eine Druckersteuerungssprache (Printer Control Language, PCL) – d.h. eine Sprache, die der Drucker versteht – konvertiert. Es gibt standardisierte PCLs, wie zum Beispiel die Sprache PostScript, und proprietäre Sprachen, wie sie vom Druckerhersteller entwickelt wurden.

Der Druckertreiber erlaubt es Ihnen, den Druckauftrag entsprechend den verschiedenen Fähigkeiten des Druckgeräts zu konfigurieren. Diese Fähigkeiten sind normalerweise auf dem Eigenschaftenblatt des Druckers aufgeführt. Zum Beispiel weiß Ihre Textverarbeitung nicht, ob das Druckgerät farbig oder monochrom druckt oder ob es Duplexdrucken unterstützt. Der Druckertreiber realisiert derartige Features für das Druckgerät.

Nachdem der Drucker einen Druckauftrag verarbeitet hat, speichert er ihn in einer als *Spooler* bezeichneten Druckwarteschlange. Je nach Einrichtung der Druckkomponenten können gespoolte Aufträge im PCL-Format vorliegen, sodass sie bereit sind für die Weitergabe an das Druckgerät, oder in einem Zwischenformat, wobei der Druckertreiber die gespoolten Aufträge in das PCL-Format übersetzen muss, bevor sie an das Gerät gesendet werden. Wenn noch andere Druckaufträge anstehen, muss ein neuer Auftrag gegebenenfalls eine Zeit lang im Spooler warten. Hat der Server schließlich den Auftrag an das Druckgerät gesendet, liest das Gerät die PCL-Befehle und erzeugt einen Dokumentausdruck.

Flexibilität beim Drucken unter Windows

Die Flexibilität der Windows-Druckerarchitektur manifestiert sich in den verschiedenen Arten, wie Sie die vier Druckerkomponenten bereitstellen können. Ein einzelner Computer kann sämtliche Rollen ausführen (selbstverständlich mit Ausnahme des Druckgeräts) oder Sie können sie im Netzwerk verteilen. Die folgenden Abschnitte beschreiben vier grundlegende Konfigurationen, die die Basis der meisten Druckerbereitstellungen unter Windows bilden. Diese Konfigurationen lassen sich skalieren, um sie an Netzwerke praktisch jeder Größe anzupassen.

Direktes Drucken

Die einfachste Druckerarchitektur besteht aus einem einzigen Druckgerät, das an einen Computer angeschlossen ist. Man spricht von einem lokal angeschlossenen Druckgerät, wie in Abbildung 2.13 dargestellt. Wenn Sie ein Druckgerät direkt mit einem Windows Server 2012-Computer verbinden und aus einer auf diesem System laufenden Anwendung drucken, realisiert der Computer den Drucker, den Druckertreiber und die Druckserverfunktionen.

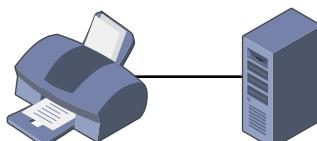


Abbildung 2.13 Ein lokal angeschlossenes Druckgerät

Freigeben lokal angeschlossener Drucker

Es ist nicht nur möglich, aus einer auf diesem Computer laufenden Anwendung zu drucken, Sie können den Drucker (und das Druckgerät) für andere Nutzer im selben Netzwerk freigeben. In dieser Anordnung fungiert der Computer mit dem lokal angeschlossenen Druckgerät als Druckerserver. Abbildung 2.14 zeigt die anderen Drucker im Netzwerk, die Druckclients.

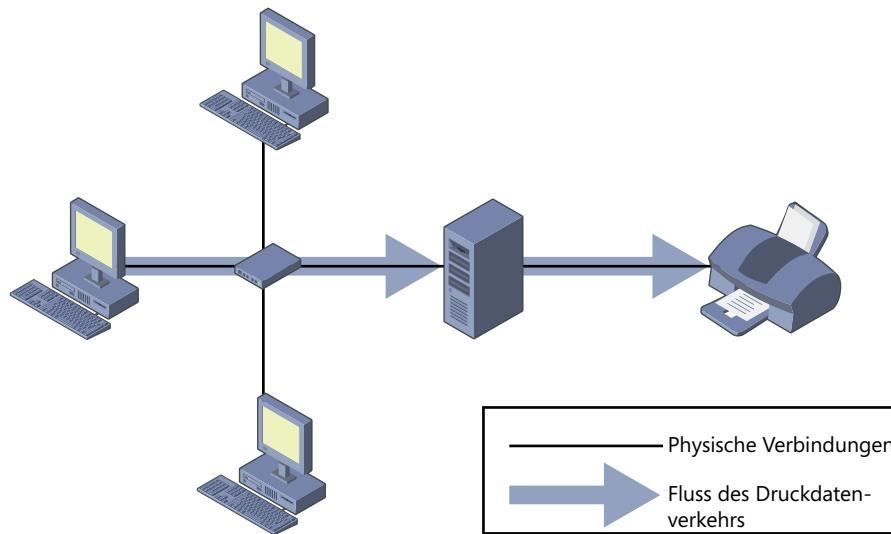


Abbildung 2.14 Freigabe eines lokal angeschlossenen Druckers

In der standardmäßigen Windows Server 2012-Konfiguration für die Druckerfreigabe verwendet jeder Client seinen eigenen Drucker und Druckertreiber. Wie zuvor sendet die auf dem Clientcomputer laufende Anwendung den Druckauftrag an den Drucker und der Druckertreiber rendert den Auftrag je nach den Fähigkeiten des Druckgeräts.

Diese Druckanordnung hat vor allem den Vorteil, dass mehrere Benutzer von unterschiedlichen Orten des Netzwerks aus Druckaufträge an ein einzelnes Druckgerät senden können, das mit einem als Druckerserver fungierenden Computer verbunden ist. Nachteilig ist, dass eine beträchtliche Belastung des Druckerservers entsteht, wenn Druckaufträge für viele Benutzer zu verarbeiten sind. Obwohl jeder Windows-Computer als Druckerserver fungieren kann, sollten Sie für diesen Zweck nur dann eine Arbeitsstation verwenden, wenn Sie nicht mehr als eine Handvoll Druckerclients zu unterstützen haben oder mit einem sehr geringen Druckaufkommen zu rechnen ist.

Drucken über Netzwerkdrucker

Bei den bisher beschriebenen Druckerlösungen sind die Druckgeräte direkt an einen Computer über einen USB- oder anderen Port angeschlossen. Allerdings müssen Druckgeräte nicht unbedingt an Computer angeschlossen sein. Stattdessen ist es auch möglich, ein Druckgerät direkt mit dem Netzwerk zu verbinden. Viele Modelle von Druckgeräten sind mit Netzwerkschnittstellenadapters ausgestattet, sodass sich die Verbindung über ein

Standardnetzwerkabel herstellen lässt. Manche Druckgeräte besitzen Erweiterungssteckplätze, in denen Sie einen separat erworbenen Netzwerkdruckeradapter installieren können. Schließlich sind für Druckgeräte ohne Netzwerkfähigkeiten eigenständige Druckerserver erhältlich, die sich mit dem Netzwerk verbinden lassen und an das Sie ein oder mehrere Druckgeräte anschließen können. Derartig ausgestattete Druckgeräte besitzen eigene IP-Adressen und verfügen in der Regel über eine eingebettete webbasierte Konfigurationsoberfläche.

Bei Druckgeräten, die mit dem Netzwerk verbunden sind, muss der Administrator in Bezug auf die Bereitstellung vor allem entscheiden, welchen Computer er als Druckerserver einsetzt. Eine einfache (wenn auch oftmals unpraktische) Option ist es, jeden Druckerclient als seinen eigenen Druckerserver fungieren zu lassen, wie Abbildung 2.15 zeigt. Jeder Client verarbeitet und spooft seine eigenen Druckaufträge, stellt die Verbindung zum Druckgerät über einen TCP (Transmission Control Protocol)-Port her und sendet die Aufträge direkt an das Gerät, um einen Ausdruck zu erzeugen.

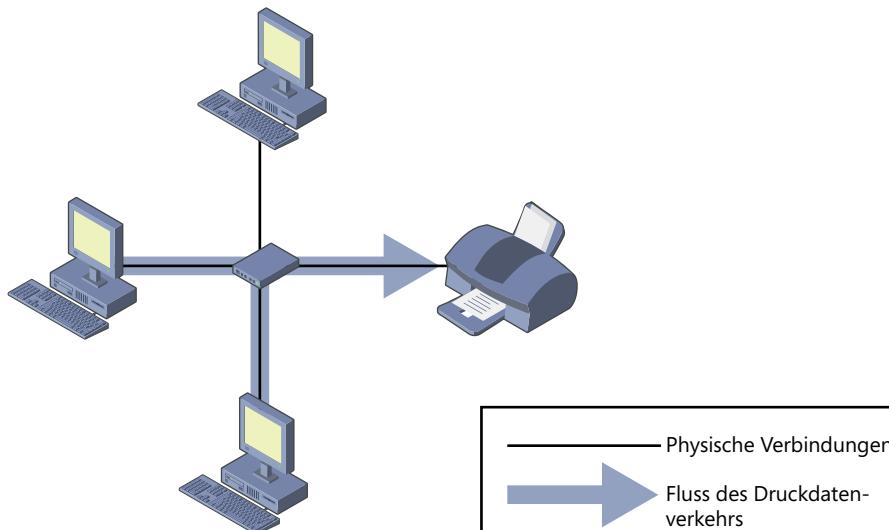


Abbildung 2.15 Ein an das Netzwerk angeschlossenes Druckgerät mit mehreren Druckerservern

Selbst für einzelne Endbenutzer ohne administrative Hilfe dürfte diese Anordnung einfach einzurichten sein. Allerdings sind auch folgende Nachteile zu nennen:

- Benutzer, die die Druckwarteschlange inspizieren, sehen ausschließlich ihre Druckaufträge
- Benutzer nehmen die anderen Benutzer, die auf das Druckgerät zugreifen, nicht wahr. Es gibt für sie keine Möglichkeit, in Erfahrung zu bringen, welche anderen Aufträge an das Druckgerät gesendet wurden oder wie lange es dauert, bis das Druckgerät ihre Aufträge fertig gestellt hat.

- Administratoren sind nicht in der Lage, die Druckwarteschlange zentral zu verwalten, weil jeder Client seine eigene Druckwarteschlange besitzt
- Administratoren können keine erweiterten Druckerfeatures implementieren, beispielsweise Druckerpools oder Remoteverwaltung
- Fehlermeldungen erscheinen nur auf dem Computer, der den vom Druckgerät momentan bearbeiteten Druckauftrag ausgelöst hat
- Druckaufträge werden komplett vom Clientcomputer verarbeitet und auch nicht teilweise auf einen externen Druckerserver ausgelagert

Aus diesen Gründen eignet sich diese Anordnung nur für kleine Arbeitsgruppennetzwerke, in denen es keine dedizierten Administratoren gibt, die für die Netzwerkpflege zuständig wären.

Freigabe von Netzwerkdruckern

Eine weit beliebtere Option für das Drucken mit Netzwerkdruckern ist es, einen Computer als Druckerserver zu bestimmen und ihn alle Druckerclients im Netzwerk bedienen zu lassen. Dazu installieren Sie einen Drucker auf einem Computer – dem Druckerserver – und konfigurieren ihn so, dass er auf das Druckgerät direkt über einen TCP-Port zugreift. Dann geben Sie den Drucker frei, wie Sie es bei einem lokal angeschlossenen Druckgerät tun würden, und konfigurieren die Clients für den Zugriff auf die Druckerfreigabe.

Wie Abbildung 2.16 zeigt, ist die physische Konfiguration die gleiche wie in der vorherigen Anordnung, doch unterscheidet sich der logische Pfad, den die Druckaufträge bis zum Druckgerät nehmen. Anstatt unmittelbar zum Druckgerät zu gehen, gelangen die Druckaufträge zum Druckerserver, der sie spoolet und nacheinander an das Druckgerät sendet.

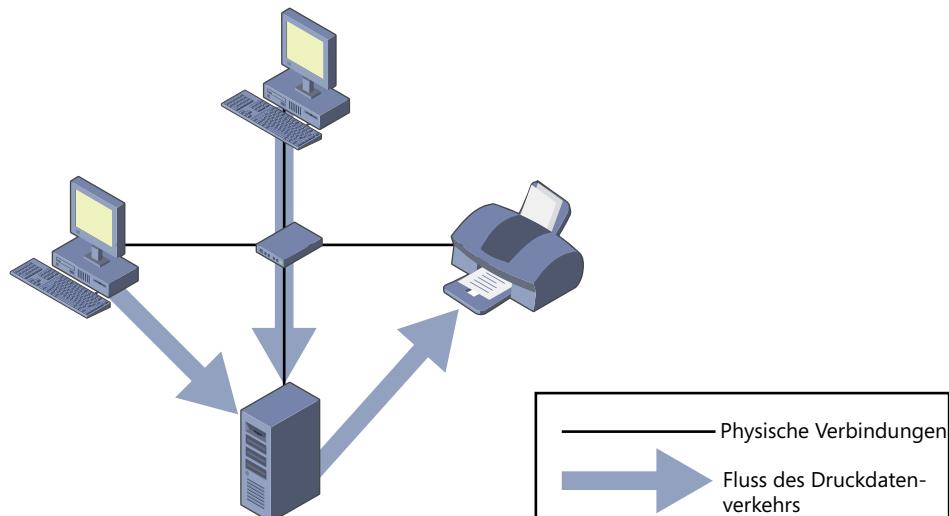


Abbildung 2.16 Ein an das Netzwerk angeschlossenes Druckgerät mit einem einzelnen freigegebenen Druckerserver

Bei dieser Anordnung werden praktisch alle Nachteile der Anordnung mit mehreren Druckerservern zu Vorteilen:

- Alle Clientdruckaufträge kommen in eine einzige Druckwarteschlange, sodass Benutzer und Administratoren eine vollständige Liste der wartenden Druckaufträge sehen können
- Ein Teil der Belastung durch das Rendern der Druckaufträge wird auf den Druckerserver verlagert, sodass der Benutzer die Kontrolle über den Clientcomputer schneller zurück erhält
- Administratoren können sämtliche in der Warteschlange stehenden Aufträge von einem Remotestandort aus verwalten
- Druckerfehlermeldungen erscheinen auf allen Clientcomputern
- Administratoren können Druckerpools und andere erweiterte Druckerfeatures einrichten
- Administratoren sind in der Lage, Sicherheits-, Überwachungs- und Protokollfunktionen von einem zentralen Ort aus zu verwalten

Erweiterte Druckerkonfigurationen

Die in den vorherigen Abschnitten beschriebenen vier Konfigurationen können Administratoren als Bausteine heranziehen, um Druckerlösungen für ihre Netzwerk zu erstellen. Es gibt viele mögliche Variationen, um eine Netzwerkarchitektur einzurichten, die den Ansprüchen Ihrer Organisation genügt. Zu den komplexeren Möglichkeiten gehören unter anderem folgende:

- Ein einzelner Drucker lässt sich an mehrere Druckgeräte anschließen, wodurch ein sogenannter *Druckerpool* entsteht. In einem stark ausgelasteten Netzwerk mit vielen Druckerclients kann der Druckerserver eine große Anzahl von eintreffenden Druckaufträgen auf mehrere identische Druckgeräte aufteilen, um kürzere Bedienungszeiten und eine bessere Fehlertoleranz zu bieten.
- An einen einzigen Drucker kann man mehrere Druckgeräte anschließen, die verschiedene Formate und Papiergrößen unterstützen. Der Drucker verteilt die Aufträge mit unterschiedlichen Anforderungen an die passenden Druckgeräte.
- Mit einem einzelnen Druckgerät lassen sich mehrere Drucker verbinden. Wenn Sie mehrere Drucker einrichten, können Sie unterschiedliche Prioritäten, Sicherheitseinstellungen und Überwachungsparameter für verschiedene Benutzer konfigurieren. Zum Beispiel ist es möglich, einen Drucker mit hoher Priorität für die Leitungsebene der Firma und einen Drucker mit geringerer Priorität für Mitarbeiter einzurichten. Damit ist gewährleistet, dass die Druckaufträge der Leitungsebene zuerst gedruckt werden, selbst wenn die Server mit demselben Druckgerät verbunden sind.

Einen Drucker freigeben

Ein Windows Server 2012-Druckerserver kann einfach oder komplex sein, je nachdem, wie viele Clients der Server unterstützen muss und wie hoch das Druckaufkommen ist. Für ein Heim- oder kleines Unternehmensnetzwerk, in dem eine Handvoll Benutzer gelegentlich den

Drucker nutzt, ist keine besondere Vorbereitung erforderlich. Wenn jedoch der Computer ein erhebliches Druckaufkommen zu bewältigen hat, machen sich gegebenenfalls Hardware-aufrüstungen wie zum Beispiel zusätzlicher Festplattenplatz oder mehr Systemspeicher notwendig.

Den Computer können Sie auch als dedizierten Druckerserver betrachten. Neben mehr Speicher und Festplattenplatz benötigt ein Windows Server 2012-Computer als Druckerserver mehr Prozessorzeit, wie es bei jeder anderen Anwendung der Fall ist. Auf einem Server, der sehr viele Druckaufgaben verarbeitet, erfahren andere Rollen und Anwendungen höchst-wahrscheinlich wesentliche Leistungseinbußen. Wenn Sie einen derartigen Server benötigen, empfiehlt es sich, den Computer ausschließlich für Druckerveraufgaben einzurichten und andere Rollen und Anwendungen auf anderen Servern unterzubringen.

Auf einem Windows Server 2012-Computer können Sie einen Drucker gleich bei der Installation oder auch erst später freigeben. Für ältere Drucker leiten Sie die Installation ein, indem Sie über die Systemsteuerung den Druckerinstallations-Assistenten aufrufen.

Allerdings verwenden die meisten Druckgeräte, die heute auf dem Markt sind, entweder eine USB-Verbindung zu einem Computer oder eine Ethernet-Verbindung zu einem Netzwerk.

Bei einem USB-Drucker stecken Sie das Druckgerät am USB-Port des Computers an und schalten es ein, um den Installationsvorgang zu starten. Ein manuelles Eingreifen ist nur erforderlich, wenn Windows Server 2012 keinen Treiber für das Druckgerät mitbringt.

Für Druckgeräte, die in ein Netzwerk integriert sind, sucht ein Installationsprogramm, das mit dem Produkt geliefert wird, das Druckgerät im Netzwerk, installiert die korrekten Treiber, erstellt einen Drucker auf dem Computer und konfiguriert den Drucker mit der richtigen IP-Adresse und anderen Einstellungen.

Nachdem der Drucker auf dem Windows Server 2012-Computer, der als Ihr Druckerserver fungiert, installiert ist, können Sie ihn für die Netzwerkclients wie folgt freigeben:

1. Melden Sie sich bei Windows Server an.
2. Öffnen Sie in der Systemsteuerung *Geräte und Drucker*.
3. Klicken Sie im Fenster *Geräte und Drucker* mit der rechten Maustaste auf das Symbol für den Drucker, den Sie freigeben möchten, und wählen Sie im Kontextmenü *Drucker-eigenschaften*. Das Eigenschaftenblatt für den Drucker erscheint.



Hinweis Eigenschaften

Das Kontextmenü bietet für jeden Drucker zwei Eigenschaftenblätter. Der Menübefehl *Druckereigenschaften* öffnet das Eigenschaftenblatt für den Drucker und der Menübefehl *Eigenschaften* das Eigenschaftenblatt für das Druckgerät.

4. Gehen Sie auf die Registerkarte *Freigabe*.
5. Aktivieren Sie das Kontrollkästchen *Diesen Drucker freigeben*. Der Druckername erscheint im Textfeld *Freigabename*. Den Standardnamen können Sie beibehalten oder einen eigenen Namen eingeben.

6. Aktivieren Sie eines oder beide der folgenden optionalen Kontrollkästchen:
 - **Druckauftragsaufbereitung auf Clientcomputern durchführen** Minimiert die Ressourcennutzung auf dem Druckerserver, indem den Druckerclients der Hauptteil der Druckverarbeitung übertragen wird
 - **Im Verzeichnis anzeigen** Erstellt ein neues Druckerobjekt in der Datenbank der Active Directory-Domänen-Dienste (AD DS). Damit sind Domänenbenutzer in der Lage, den Drucker durch eine Suche im Verzeichnis zu lokalisieren. Diese Option erscheint nur, wenn der Computer Mitglied einer AD DS-Domäne ist.
7. Klicken Sie auf *Zusätzliche Treiber*, um das gleichnamige Dialogfeld zu öffnen. Hier haben Sie die Möglichkeit, Druckertreiber für andere Windows-Plattformen wie zum Beispiel Itanium und x86 zu laden. Wenn Sie die alternativen Treiber installieren, stellt der Druckerserver sie automatisch den Clients zur Verfügung, die unter den jeweiligen Betriebssystemversionen laufen.
8. Aktivieren Sie entsprechend Ihren Anforderungen die verfügbaren Kontrollkästchen und klicken Sie auf *OK*. Für jedes aktivierte Kontrollkästchen zeigt Windows Server 2012 ein Dialogfeld *Druckertreiber* an.
9. Legen Sie in jedem *Druckertreiber*-Dialogfeld den Standort der Druckertreiber für das ausgewählte Betriebssystem fest (durch Eingabe oder Suche des Standorts) und klicken Sie dann auf *OK*.
10. Klicken Sie auf *OK*, um das Dialogfeld *Zusätzliche Treiber* zu schließen.
11. Klicken Sie auf *OK*, um das Eigenschaftenblatt für den Drucker zu schließen. Das Druckersymbol in der Systemsteuerung *Geräte und Drucker* enthält nun ein Symbol, das den freigegebenen Drucker kennzeichnet.
12. Schließen Sie die Systemsteuerung.

Der Drucker steht nun den Clients im Netzwerk zur Verfügung.

Druckertreiber verwalten

Druckertreiber versetzen Computer in die Lage, die Fähigkeiten der Druckgeräte zu verwalten. Wenn Sie einen Drucker auf einem Windows Server 2012-Server installieren, dann installieren Sie auch einen Treiber, den andere Windows-Computer verwenden können.

Über die Windows-Funktion Point-and-Print können Clients auf die Drucker zugreifen, die auf Druckservern installiert sind. Ein Benutzer auf einer Arbeitsstation wählt einen Drucker auf einem Server aus und Windows installiert automatisch den Treiber, den der Client benötigt, um seine Druckaufträge zu verarbeiten und sie an diesen Drucker zu schicken.

Die Druckertreiber, die Sie unter Windows Server 2012 installieren, sind die gleichen Treiber, die Windows-Arbeitsstationen und andere Serverversionen verwenden, wobei jedoch eine Besonderheit zu beachten ist: Als 64-Bit-Plattform verwendet Windows Server 2012 64-Bit-Gerätetreiber, die für andere Computer mit 64-Bit-Versionen von Windows geeignet sind.

Wenn Sie jedoch 32-Bit-Windows-Systeme in Ihrem Netzwerk betreiben, müssen Sie auf dem Server einen 32-Bit-Treiber installieren, der diesen Systemen zur Verfügung steht.

Das Dialogfeld *Zusätzliche Treiber*, das Sie über die Registerkarte *Freigabe* des Eigenschaftenblatts eines Druckers erreichen, lassen sich Treiber für andere Prozessorplattformen installieren. Allerdings müssen Sie diese Treiber von einem Computer aus installieren, der auf der alternativen Plattform läuft. Anders ausgedrückt: Um einen 32-Bit-Treiber für einen Drucker auf einem Windows Server 2012-Server zu installieren, müssen Sie auf das Eigenschaftenblatt des Druckers von einem unter einer 32-Version von Windows laufenden Computer zugreifen. Das ist möglich, indem Sie auf den Drucker direkt über das Netzwerk mithilfe von Datei-Explorer zugreifen oder das Snap-In *Druckverwaltung* auf dem 32-Bit-System ausführen und über dieses Ihren Windows Server 2012-Druckerserver verwalten.



Hinweis Treiber installieren

Damit der Server Treiber für unterschiedliche Plattformen von Clientcomputern bereitstellt, müssen Sie bei der Installation der Treiber für dasselbe Druckgerät sicherstellen, dass sie identische Namen haben. Zum Beispiel behandelt Windows Server 2012 »HP LaserJet 5200 PCL6« und HP LaserJet 5200 PCL 6« als zwei verschiedene Treiber. Die Namen müssen identisch sein, damit der Server sie korrekt anwendet.

Remotezugriff via Easy Print

Verbindet sich ein Remotedesktopdienste-Client mit einem Server, führt er Anwendungen auf der Hardware (Prozessor(en), Speicher) des Servers aus. Wenn aber dieser Client ein Dokument aus einer dieser Anwendungen heraus drucken möchte, soll der Druckauftrag zum Druckgerät gehen, das mit dem Clientcomputer verbunden ist.

Die Komponente, die Remotedesktop-Clients in die Lage versetzt, auf ihre lokalen Druckgeräte zu drucken, wird als *Easy Print* bezeichnet. Easy Print hat die Form eines Druckertreibers, der auf dem Server zusammen mit dem Rollendienst für den Remotedesktop-Sitzungshost installiert wird.

Der Easy Print-Druckertreiber für Remotedesktop erscheint automatisch im Snap-In *Druckverwaltung*, ist aber keinem bestimmten Druckgerät zugeordnet. Stattdessen fungiert der Treiber als Redirector, der den Server in der Lage versetzt, die Drucker an den verbundenen Clients anzusprechen.

Easy Print benötigt keine Konfiguration außer der Installation der Rolle *Remotedesktopdienste*. Nachdem er aber betriebsbereit ist, bietet er dem Serveradministrator zusätzlichen Zugriff auf die Drucker an den Remotedesktopclients.

Wenn sich ein Remotedesktopclient mit einem Server über das Programm *Remotedesktopverbindung* oder die Site Web Access für Remotedesktop verbindet, werden die auf dem Clientsystem installierten Drucker zum Server umgeleitet und erscheinen im Snap-In *Druckverwaltung* als umgeleitete Serverdrucker, wie Abbildung 2.17 zeigt.

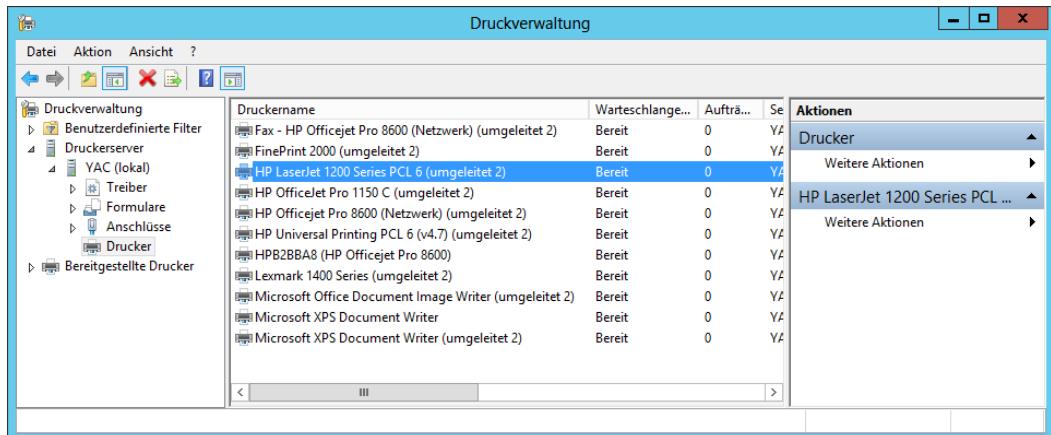


Abbildung 2.17 Durch Easy Print umgeleitete Drucker auf einem Remotedesktopserver

Ein Client, der eine Anwendung auf dem Server ausführt, kann demzufolge auf einem lokalen Druckgerät mithilfe des umgeleiteten Druckers drucken. Administratoren können auch das Eigenschaftenblatt für den umgeleiteten Drucker in der üblichen Weise öffnen und dessen Einstellungen bearbeiten.

Druckersicherheit konfigurieren

Wie bei Ordnerfreigaben müssen Clients über die erforderlichen Berechtigungen verfügen, um auf einen freigegebenen Drucker zugreifen zu können. Druckerberechtigungen sind wesentlich einfacher als NTFS-Berechtigungen; sie geben an, ob Benutzer den Drucker verwenden, an den Drucker geschickte Dokumente verwalten oder die Eigenschaften des Druckers selbst verwalten dürfen. Führen Sie die folgenden Schritte aus, um Berechtigungen für einen Drucker zuzuweisen:

1. Melden Sie sich bei Windows Server 2012 unter einem Domänenkonto mit Administratorrechten an.
2. Öffnen Sie die Systemsteuerung und wählen Sie *Hardware/Geräte und Drucker*.
3. Klicken Sie mit der rechten Maustaste im Fenster *Geräte und Drucker* auf eines der Druckersymbole und wählen Sie im Kontextmenü den Befehl *Druckereigenschaften*. Es erscheint das Eigenschaftenblatt des Druckers.
4. Wechseln Sie zur Registerkarte *Sicherheit*. In der oberen Hälfte sind alle Sicherheitsprinzipals aufgelistet, die derzeit Berechtigungen für den ausgewählten Drucker besitzen. In der unteren Hälfte finden Sie die Berechtigungen, die dem ausgewählten Sicherheitsprinzipal zugeordnet sind.
5. Klicken Sie auf *Hinzufügen*. Es erscheint das Dialogfeld *Benutzer, Computer, Dienstkonten oder Gruppen auswählen*.

6. In das Textfeld *Geben Sie die zu verwendenden Objektnamen ein* geben Sie einen Benutzer- oder Gruppennamen ein und klicken dann auf *OK*. Der Benutzer oder die Gruppe erscheint in der Liste *Gruppen- oder Benutzernamen*.
7. Wählen Sie den Sicherheitsprinzipal aus, den Sie hinzugefügt haben, und aktivieren/deaktivieren Sie die Kontrollkästchen in der unteren Hälfte der Anzeige, um dem Benutzer die entsprechenden grundlegenden Berechtigungen zu erteilen oder zu verweigern.
8. Klicken Sie auf *OK*, um das Eigenschaftenblatt zu schließen.
9. Schließen Sie die Systemsteuerung.

Wie bei NTFS-Berechtigungen gibt es zwei Arten von Druckerberechtigungen: grundlegende und erweiterte. Die drei grundlegenden Berechtigungen bestehen jeweils aus einer Kombination von erweiterten Berechtigungen.

Dokumente verwalten

Standardmäßig weisen alle Drucker die Berechtigung *Zulassen Drucken* der speziellen Identität *Jeder* zu, sodass alle Benutzer auf den Drucker zugreifen und ihre eigenen Dokumente verwalten können. Benutzer, die die Berechtigung *Zulassen Dokumente verwalten* besitzen, können die Dokumente beliebiger Benutzer verwalten.

Verwalten von Dokumenten heißt, die momentan in einer Druckwarteschlange wartenden Dokumente anhalten, fortsetzen, neu starten und abbrechen. Windows Server 2012 stellt für jeden Drucker ein Fenster *Druckwarteschlange* bereit, in dem Benutzer die Druckaufträge anzeigen können, die momentan auf einen Ausdruck warten. Führen Sie die folgenden Schritte aus, um Dokumente zu verwalten:

1. Melden Sie sich bei Windows Server 2012 an.
2. Öffnen Sie die Systemsteuerung und wählen Sie *Hardware/Geräte und Drucker* aus.
3. Klicken Sie mit der rechten Maustaste im Fenster *Geräte und Drucker* auf eines der Druckersymbole und wählen Sie aus dem Kontextmenü den Befehl *Druckaufträge anzeigen*. Es erscheint ein Fenster für die Druckwarteschlange mit dem Namen des jeweiligen Druckers, wie es Abbildung 2.18 zeigt.

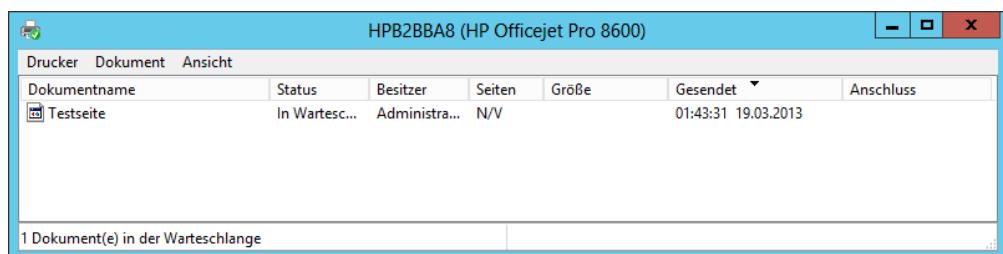


Abbildung 2.18 Windows Server 2012-Fenster einer Druckwarteschlange

4. Wählen Sie einen der Menübefehle aus, um die zugeordnete Funktion auszuführen.

5. Schließen Sie das Fenster für die Druckwarteschlange.
6. Schließen Sie die Systemsteuerung.

Drucker verwalten

Benutzer mit der *Zulassen*-Berechtigung *Diesen Drucker verwalten* können nicht nur Dokumente in der Warteschlange bearbeiten, sondern auch den Drucker selbst neu konfigurieren. Das Verwalten eines Druckers heißt, die Betriebsparameter zu verändern, die sich auf alle Benutzer auswirken, und den Zugriff auf den Drucker zu steuern.

Im Allgemeinen handelt es sich bei den meisten softwarebasierten Aufgaben, die sich auf das Verwalten eines Druckers beziehen, um diejenigen Aufgaben, die Sie einmalig durchführen, während Sie den Drucker erstmals einrichten. Zu den Routineaufgaben der Druckerverwaltung gehören eher Aufgaben der physischen Wartung, wie zum Beispiel Papierstaus beseitigen, Papier nachladen und Tonerkartuschen bzw. Tintenpatronen wechseln. Die folgenden Abschnitte beschäftigen sich jedoch mit einigen typischen Konfigurationsaufgaben der Druckerverwaltung.

Druckerprioritäten festlegen

In manchen Fällen möchten Sie bestimmten Benutzern in Ihrer Organisation vorrangigen Zugriff auf ein Druckgerät erteilen, sodass bei starkem Druckaufkommen deren Druckaufträge vor denen anderer Benutzer verarbeitet werden. Hierzu müssen Sie mehrere Drucker erstellen, sie demselben Druckgerät zuordnen und dann die einzelnen Prioritäten ändern, wie die folgenden Schritte beschreiben:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit der Berechtigung *Drucker verwalten* an.
2. Öffnen Sie die Systemsteuerung und wählen Sie *Hardware | Geräte und Drucker*.
3. Klicken Sie im Fenster *Geräte und Drucker* mit der rechten Maustaste auf eines der Druckersymbole und wählen Sie aus dem Kontextmenü den Befehl *Druckereigenschaften*. Es erscheint das Eigenschaftenblatt für den jeweiligen Drucker.
4. Gehen Sie auf die Registerkarte *Erweitert*, wie in Abbildung 2.19 gezeigt.
5. Setzen Sie das Drehfeld *Priorität* auf eine Zahl, die die höchste Priorität für den Drucker angibt. Größere Zahlen bedeuten höhere Prioritäten. Der größtmögliche Wert für die Priorität ist 99.



Hinweis Druckerprioritäten

Die Werte im Drehfeld *Priorität* haben keine absolute Bedeutung, sondern stehen für relative Prioritäten der Drucker untereinander. Wenn ein Drucker einen höheren Prioritätswert als ein anderer hat, verarbeitet der Server die Druckaufträge des Druckers mit dem höheren Wert zuerst. Mit anderen Worten spielt es keine Rolle, ob der höhere Prioritätswert 9 oder 99 ist, solange die niedrigere Priorität einen kleineren Wert aufweist.

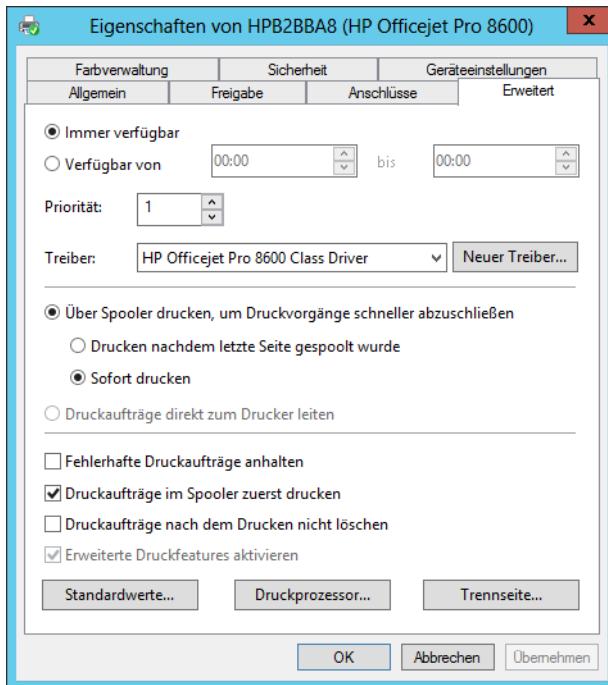


Abbildung 2.19 Die Registerkarte *Erweitert* im Eigenschaftenblatt eines Druckers

6. Wechseln Sie zur Registerkarte *Sicherheit*.
 7. Fügen Sie die Benutzer oder Gruppen hinzu, denen Sie den Zugriff mit hoher Priorität auf den Drucker gewähren möchten, und weisen Sie ihnen die *Zulassen*-Berechtigung *Drucken* zu.
 8. Entziehen Sie der speziellen Identität *Jeder* die die *Zulassen*-Berechtigung *Drucken*.
 9. Klicken Sie auf *OK*, um das Eigenschaftenblatt zu schließen.
 10. Erstellen Sie einen identischen Drucker mit demselben Druckertreiber und ordnen Sie ihn demselben Druckgerät zu. Behalten Sie die Prioritätseinstellung mit dem Standardwert 1 bei und übernehmen Sie auch die Standardberechtigungen.
 11. Benennen Sie die Drucker um, wobei aus den Namen die Priorität hervorgehen sollte, die Sie den Druckern zugewiesen haben.
 12. Schließen Sie die Systemsteuerung.
- Informieren Sie die privilegierten Benutzer, dass sie ihre Druckaufträge an den Drucker mit der höheren Priorität schicken. Sämtliche an diesen Drucker gesendeten Druckaufträge werden verarbeitet vor denen, die an den anderen Drucker mit der niedrigeren Priorität gesendet werden.

Einen Druckerpool erstellen

Wie bereits erwähnt, erhöht ein Druckerpool das Leistungsvermögen eines einzelnen Druckers, indem man ihn an mehrere Druckgeräte anschließt. Wenn Sie einen Druckerpool erstellen, sendet der Druckerserver jeden eingehenden Druckauftrag an das erste Druckgerät, das derzeit nicht belegt ist. Damit werden die Druckaufträge effizient auf die verfügbaren Druckgeräte verteilt und Benutzer schneller bedient.

Einen Druckerpool konfigurieren Sie in folgenden Schritten:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit der Berechtigung *Drucker verwalten* an.
2. Öffnen Sie die Systemsteuerung und wählen Sie *Hardware | Geräte und Drucker*.
3. Klicken Sie im Fenster *Geräte und Drucker* mit der rechten Maustaste auf die Druckersymbole und wählen Sie aus dem Kontextmenü den Befehl *Druckereigenschaften*. Es erscheint das Eigenschaftenblatt für den Drucker.
4. Wechseln Sie zur Registerkarte *Anschlüsse*.
5. Wählen Sie alle Anschlüsse aus, mit denen die Druckgeräte verbunden sind.
6. Aktivieren Sie das Kontrollkästchen *Druckerpool aktivieren* und klicken Sie dann auf *OK*.
7. Schließen Sie die Systemsteuerung.

Damit Sie einen Druckerpool erstellen können, brauchen Sie mindestens zwei identische Druckgeräte oder zumindest zwei Druckgeräte, die den gleichen Druckertreiber verwenden. Die Druckgeräte müssen sich am selben Standort befinden, da es sich nicht feststellen lässt, welches Druckgerät ein bestimmtes Dokument verarbeitet. Außerdem müssen Sie alle Druckgeräte im Pool mit demselben Druckerserver verbinden. Handelt es sich beim Druckerserver um einen Windows Server 2012-Computer, können Sie die Druckgeräte mit beliebigen Anschlüssen verbinden, die praktikabel sind.

Die Rolle Druck- und Dokumentdienste verwenden

Die in den vorherigen Abschnitten beschriebenen Fähigkeiten zur Druckerfreigabe und -verwaltung stehen auf jedem Windows Server 2012-Computer in seiner standardmäßigen Installationskonfiguration zur Verfügung. Wenn Sie aber die Rolle *Druck- und Dokumentdienste* auf dem Computer installieren, sind zusätzliche Tools verfügbar, die vor allem für Administratoren nützlich sind, die Netzwerkdrucker auf Unternehmensebene betreuen.

Bei der Installation der Rolle *Druck- und Dokumentdienste* mit dem Assistenten zum Hinzufügen von Rollen und Features des Server-Managers können Sie auf der Seite *Rollendienste* aus den folgenden Optionen auswählen:

- **Druckerserver** Installiert das MMC-Snap-In *Druckverwaltung*, über das Administratoren Drucker im gesamten Unternehmen bereitstellen, überwachen und verwalten können

- **Server für verteilte Scanvorgänge** Versetzt Computer in der Lage, Dokumente von netzwerkbasierten Scannern entgegenzunehmen und sie an die entsprechenden Benutzer weiterzuleiten
- **Internetdrucken** Erstellt eine Website, die es Benutzern im Internet ermöglicht, Druckaufträge an freigegebene Windows-Drucker zu senden
- **LPD-Dienst** Ermöglicht UNIX-Clients, die den LPR (Line Printer Remote)-Dienst ausführen, ihre Druckaufträge an Windows-Drucker zu senden

Wie üblich fügt Windows Server 2012 ein neues Symbol im Navigationsbereich des Server Managers hinzu, wenn Sie eine Rolle installieren. Die Startseite *Druckdienste* enthält eine gefilterte Ansicht mit Protokolleinträgen von druckerbezogenen Ereignissen, eine Statusanzeige für die rollenbezogenen Systemdienste und Rollendienste sowie Leistungsindikatoren.

Das MMC-Snap-In *Druckverwaltung* ist ein administratives Tool, das die Steuerelemente für die Druckerkomponenten des gesamten Unternehmensbereichs in einer einzigen Konsole vereint. Über dieses Tool können Sie auf die Druckwarteschlangen und Eigenschaftenblätter für alle Netzwerkdrucker im Unternehmen zugreifen, Drucker für Clientcomputer mithilfe einer Gruppenrichtlinie bereitstellen und benutzerdefinierte Ansichten anlegen. Diese Ansichten erleichtern es, Druckgeräte zu identifizieren, die aufgrund von Fehlern oder erschöpfter Verbrauchsmaterialien Aufmerksamkeit erfordern.

Windows Server 2012 installiert die Konsole *Druckverwaltung*, wenn Sie dem Computer die Rolle *Druck- und Dokumentdienste* hinzufügen. Die Konsole lässt sich aber auch ohne die Rolle installieren. Dazu fügen Sie das Feature *Tools für Druck- und Dokumentdienste* hinzu, das Sie im Assistenten zum Hinzufügen von Rollen und Features unter *Remoteserver-Verwaltungstools | Rollenverwaltungstools* finden.

Die folgenden Abschnitte erläutern einige der Verwaltungsaufgaben, die Sie mit der Konsole *Druckverwaltung* durchführen können.

Druckerserver hinzufügen

Standardmäßig zeigt die Konsole *Druckverwaltung* in der Liste der Druckerserver nur den lokalen Computer an. Wie Abbildung 2.20 zeigt, gibt es unter jedem Druckerserver die vier Knoten *Treiber*, *Formulare*, *Anschlüsse* und *Drucker*, die dem jeweiligen Server zugeordnet sind.

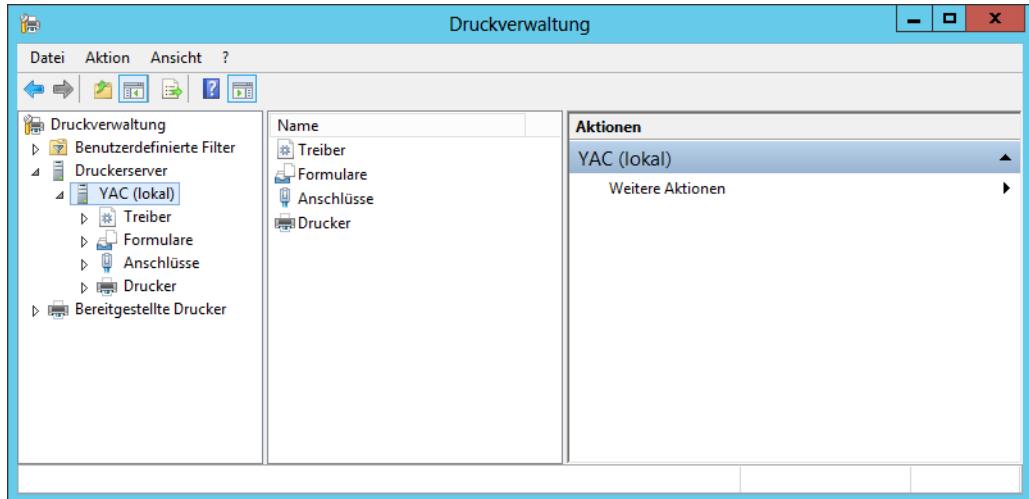


Abbildung 2.20 In der Konsole *Druckverwaltung* angezeigter Druckerserver

Um andere Druckerserver und deren Drucker verwalten zu können, müssen Sie sie der Konsole hinzufügen. Das geschieht in folgenden Schritten:

1. Melden Sie sich bei Windows Server 2012 an und starten Sie den Server-Manager.
2. Klicken Sie auf *Tools/Druckverwaltung*, um die Konsole *Druckverwaltung* zu öffnen.
3. Klicken Sie mit der rechten Maustaste auf den Knoten *Druckerserver* und klicken Sie im Kontextmenü auf *Server hinzufügen/entfernen*. Daraufhin erscheint das Dialogfeld *Server hinzufügen/entfernen*.
4. Klicken Sie im Abschnitt *Druckerserver angeben* auf *Durchsuchen*. Daraufhin erscheint das Dialogfeld *Druckerserver auswählen*.
5. Wählen Sie den Druckerserver aus, den Sie der Konsole hinzufügen möchten, und klicken Sie auf *Server auswählen*. Im Dialogfeld *Server hinzufügen/entfernen* erscheint dann der ausgewählte Server im Textfeld *Server hinzufügen*.
6. Klicken Sie auf *Zur Liste hinzufügen*. Der ausgewählte Server erscheint nun in der Liste *Druckerserver*.
7. Klicken Sie auf *OK*. Der Server ist nun unter dem Knoten *Druckerserver* aufgeführt.
8. Schließen Sie die Systemsteuerung.

Jetzt können Sie die Drucker verwalten, die dem Server zugeordnet sind, den Sie der Konsole hinzugefügt haben.

Drucker anzeigen

Für Druckeradministratoren in großen Unternehmensnetzwerken ist es schwierig, Dutzende oder Hunderte von Druckgeräten, die häufig im Einsatz sind und regelmäßige Aufmerksamkeit

erfordern, im Auge zu behalten. Ob es sich bei einer notwendigen Wartung um eine größere Reparatur handelt, eine Tintenpatrone oder Tonerkartusche zu ersetzen ist oder der Papier- schacht gefüllt werden muss – Druckgeräte erhalten die benötigte Aufmerksamkeit erst, wenn ein Administrator das Problem wahrnimmt.

Die Konsole *Druckverwaltung* bietet mehrere Möglichkeiten, die mit den Druckerservern im Netzwerk verbundenen Druckerkomponenten anzuzeigen. Um Ansichten zu erstellen, wendet die Konsole auf die vollständige Liste der Drucker verschiedene Filter an, die die anzuzeigenden Drucker auswählen. Unter dem Knoten *Benutzerdefinierte Filter* sind bereits die folgenden vier Standardfilter zu finden:

- **Alle Drucker** Enthält eine Liste mit sämtlichen Druckern aller Druckerserver, die Sie der Konsole hinzugefügt haben
- **Alle Treiber** Enthält eine Liste sämtlicher Druckertreiber auf allen Druckerservern, die Sie der Konsole hinzugefügt haben
- **Drucker nicht bereit** Enthält eine Liste aller Drucker, die keinen *Bereit*-Status melden
- **Drucker mit Aufträgen** Enthält eine Liste aller Drucker, für die momentan Druckaufträge in der Druckwarteschlange stehen

Mit Ansichten wie *Drucker nicht bereit* können Administratoren schnell und einfach die Drucker identifizieren, die Aufmerksamkeit verlangen, ohne einzelne Druckerserver durchsuchen oder sich durch eine lange Liste aller Drucker im Netzwerk arbeiten zu müssen. Neben diesen Standardfiltern können Sie eigene benutzerdefinierte Filter einrichten.

Drucker und Druckerserver verwalten

Nachdem Sie mithilfe gefilterter Ansichten die zu untersuchenden Drucker isoliert haben, können Sie einen Drucker auswählen, um dessen Status, die Anzahl der momentan in seiner Druckwarteschlange stehenden Druckaufträge und den Namen des Druckerservers, der den Drucker hostet, anzuzeigen. Wenn Sie im Bereichsfenster mit der rechten Maustaste klicken und im Kontextmenü *Erweiterte Ansicht einblenden* auswählen, erscheint ein weiterer Bereich mit dem Inhalt der Warteschlange des ausgewählten Druckers. Die in der Warteschlange befindlichen Druckaufträge können Sie hier genauso bearbeiten wie im Fenster *Druckwarteschlange* der Konsole *Druckserver*.

Die Konsole *Druckverwaltung* erlaubt es Administratoren auch, auf die Konfigurations- oberfläche für die in den Anzeigen der Konsole sichtbaren Drucker oder Druckerserver zuzugreifen. Wenn Sie mit der rechten Maustaste auf einen Drucker oder Druckerserver in der Konsolenbenutzeroberfläche klicken und dann *Eigenschaften* im Kontextmenü auswählen, wird das gleiche Eigenschaftenblatt angezeigt, wie Sie es auf dem Druckerserver selbst sehen würden. Administratoren können dann Drucker und Druckerserver konfigurieren, ohne sich zum Standort des Druckerservers begeben oder eine Remotedesktopverbindung zum Druckerserver herstellen zu müssen.

Drucker mit einer Gruppenrichtlinie bereitstellen

Um einen Druckerclient für den Zugriff auf einen freigegebenen Drucker zu konfigurieren, müssen Sie lediglich das Netzwerk oder die AD DS-Struktur durchsuchen und den Drucker auswählen. Wenn Sie aber Hunderte oder Tausende von Druckerclients zu konfigurieren haben, sieht das Ganze komplizierter aus. Hier greifen Ihnen AD DS unter die Arme. Drucker lassen sich damit ganz einfach für eine große Anzahl von Clients bereitstellen.

Durch das Veröffentlichen von Druckern in der AD DS-Datenbank sind Benutzer und Administratoren in der Lage, Drucker nach Name, Standort oder Modell zu suchen (falls Sie die Felder *Standort* und *Modell* im Druckerobjekt ausgefüllt haben). Um ein Druckerobjekt in der AD DS-Datenbank zu erstellen, können Sie entweder das Kontrollkästchen *In Verzeichnis anzeigen* aktivieren, während Sie den Drucker freigeben, oder mit der rechten Maustaste in der Konsole *Druckverwaltung* auf einen Drucker klicken und *In Verzeichnis anzeigen* aus dem Kontextmenü auswählen.

Möchten Sie mithilfe von AD DS Drucker für Clients bereitstellen, müssen Sie die entsprechenden Richtlinien in einem Gruppenrichtlinienobjekt (Group Policy Object, GPO) konfigurieren. Ein GPO können Sie mit beliebigen Domänen, Standorten oder organisatorischen Einheiten (Organizational Unit, OU) in der AD DS-Struktur verknüpfen. Wenn Sie ein GPO konfigurieren, um einen Drucker bereitzustellen, empfangen alle Benutzer oder Computer in dieser Domäne, diesem Standort oder dieser OU die Druckerverbindung standardmäßig, wenn sie sich anmelden. Drucker stellen Sie über eine Gruppenrichtlinie in folgenden Schritten bereit:

1. Melden Sie sich bei Windows Server 2012 unter einem Domänenkonto mit Administratorenrechten an. Es erscheint das Fenster *Server-Manager*.
2. Öffnen Sie die Konsole *Druckverwaltung*.
3. Klicken Sie mit der rechten Maustaste im Bereichsfenster der Konsole auf einen Drucker und wählen Sie im Kontextmenü den Befehl *Mit Gruppenrichtlinie bereitstellen*. Daraufhin erscheint das Dialogfeld *Mit Gruppenrichtlinie bereitstellen*, wie es in Abbildung 2.21 zu sehen ist.
4. Klicken Sie auf *Durchsuchen*, um das Dialogfeld *Gruppenrichtlinienobjekt suchen* zu öffnen.
5. Wählen Sie das Gruppenrichtlinienobjekt (Group Policy Object, GPO) aus, über das Sie den Drucker bereitstellen möchten, und klicken Sie auf *OK*. Das ausgewählte Gruppenrichtlinienobjekt erscheint im Feld *Name des Gruppenrichtlinienobjekts*.

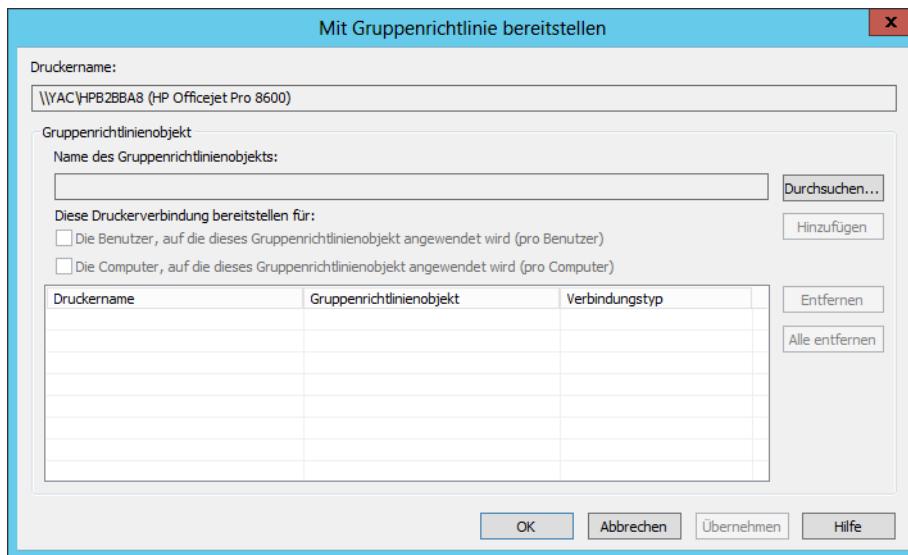


Abbildung 2.21 Das Dialogfeld *Mit Gruppenrichtlinie bereitstellen*

6. Aktivieren Sie das zutreffende Kontrollkästchen, um festzulegen, ob der Drucker für die Benutzer und/oder die Computer, auf die dieses Gruppenrichtlinienobjekte angewendet wird, bereitgestellt werden soll, und klicken Sie dann auf *Hinzufügen*. Die neuen Drucker-GPO-Zuordnungen erscheinen in der Tabelle.

Bereitstellen des Druckers für die Benutzer heißt, dass alle dem GPO zugeordneten Benutzer die Druckerverbindung erhalten, unabhängig davon, an welchem Computer sie sich anmelden. Eine Bereitstellung für die Computer bedeutet, dass sämtliche dem GPO zugeordneten Computer die Druckerverbindung erhalten, unabhängig davon, wer sich an den Computern anmeldet.

7. Klicken Sie auf *OK*. Ein Meldungsfeld der Druckverwaltung informiert Sie darüber, dass die Operation erfolgreich verlaufen ist.
8. Klicken Sie auf *OK* und dann noch einmal auf *OK*, um das Dialogfeld *Mit Gruppenrichtlinie bereitstellen* zu schließen.
9. Schließen Sie die Systemsteuerung.

Wenn sich Benutzer, die auf einem Computer ab Windows Server 2008 oder ab Windows Vista arbeiten und denen das GPO zugeordnet ist, ihre Richtlinien aktualisieren oder den Computer neu starten, empfangen sie die neuen Einstellungen und der Drucker erscheint in der Systemsteuerung unter *Drucker*.



Hinweis Pushprinterconnections.exe

Clients, die mit älteren Windows-Versionen, einschließlich Windows XP und Windows Server 2003 arbeiten, unterstützenrichtlinienbasierte Druckerbereitstellungen nicht automatisch. Um das GPO für eine Druckerbereitstellung auf diesen Computern zu aktivieren, müssen Sie die Systeme so konfigurieren, dass sie das Dienstprogramm *PushPrinterConnections.exe* ausführen. Am zweckmäßigsten hierfür ist es, dasselbe GPO, das Sie für die Druckerbereitstellung verwendet haben, so zu konfigurieren, dass das Programm von einem Benutzeranmeldedeskript oder einem Maschinenskript gestartet wird.

Prüfungszielzusammenfassung

- Beim Drucken in Microsoft Windows sind normalerweise die folgenden vier Komponenten beteiligt: Druckgerät, Drucker, Druckerserver und Druckertreiber
- Die einfachste Druckerarchitektur besteht aus einem einzigen Druckgerät, das an einen Computer angeschlossen ist. Man spricht von einem lokal angeschlossenen Druckgerät. Diesen Drucker (und das Druckgerät) können Sie für andere Nutzer im selben Netzwerk freigeben.
- Bei Druckgeräten, die mit dem Netzwerk verbunden sind, muss der Administrator in Bezug auf die Bereitstellung vor allem entscheiden, welchen Computer er als Druckerserver einsetzt
- Der Treiber Easy Print für Remotedesktop ermöglicht Remotedesktopclients, die Anwendungen auf einem Server ausführen, ihre Druckaufträge zu ihren lokalen Druckgeräten umzuleiten
- Druckerberechtigungen sind wesentlich einfacher als NTFS-Berechtigungen; sie geben an, ob Benutzer den Drucker verwenden, an den Drucker geschickte Dokumente verwalten oder die Eigenschaften des Druckers selbst verwalten dürfen
- Das MMC-Snap-In *Druckverwaltung* ist ein administratives Tool, das die Steuerelemente für die Druckerkomponenten des gesamten Unternehmensbereichs in einer einzigen Konsole vereint

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welcher der folgenden Begriffe beschreibt die Softwareschnittstelle, über die ein Computer mit einem Druckgerät kommuniziert?
 - A. Drucker
 - B. Druckerserver

- C. Druckertreiber
 - D. Snap-In *Druckverwaltung*
2. Auf einem unter Windows Server 2012 laufenden Computer richten Sie einen Druckerpool ein. Der Druckerpool enthält drei identische Druckgeräte. Sie öffnen das Eigenschaftendialogfeld für den Drucker und wählen auf der Registerkarte *Anschlüsse* die Option *Druckerpool aktivieren*. Was müssen Sie als Nächstes tun?
 - A. Den Anschluss LPT1 konfigurieren, um drei Drucker zu unterstützen.
 - B. Die den drei Druckern zugeordneten Anschlüsse auswählen oder erstellen.
 - C. Auf der Registerkarte *Geräteeinstellungen* die installierbaren Optionen konfigurieren, um zwei zusätzliche Druckgeräte zu unterstützen.
 - D. Auf der Registerkarte *Erweitert* die Priorität für jedes Druckgerät konfigurieren, damit die Druckaufträge unter den drei Druckgeräten verteilt werden.
 3. Eines Ihrer Druckgeräte arbeitet nicht einwandfrei und Sie möchten vorübergehend verhindern, dass Benutzer Druckaufträge an den Drucker senden, der dieses Gerät bedient. Was unternehmen Sie?
 - A. Die Freigabe des Druckers beenden.
 - B. Den Drucker aus dem Active Directory entfernen.
 - C. Den Druckeranschluss ändern.
 - D. Die Freigabe umbenennen.
 4. Sie verwalten einen Computer unter Windows Server 2012, der als Druckerserver konfiguriert ist. Benutzer in der *Marketing*-Gruppe beschweren sich, dass sie nicht in der Lage sind, Dokumente mit einem Drucker auf dem Server zu drucken. Daraufhin inspizieren Sie die Berechtigungen im Dialogfeld *Eigenschaften* des Druckers. Der *Marketing*-Gruppe wurde die *Zulassen*-Berechtigung *Dokumente verwalten* erteilt. Warum können Benutzer auf dem Drucker nicht drucken?
 - A. Der Gruppe *Jeder* muss die Berechtigung *Dokumente verwalten* erteilt werden.
 - B. Der Gruppe *Administratoren* muss die Berechtigung *Drucker verwalten* erteilt werden.
 - C. Der *Marketing*-Gruppe muss die Berechtigung *Drucken* erteilt werden.
 - D. Der *Marketing*-Gruppe muss die Berechtigung *Drucker verwalten* erteilt werden.
 5. Sie verwalten einen Druckerserver, der unter Windows Server 2012 läuft, und möchten ein Druckgerät warten, das physisch mit dem Druckerserver verbunden ist. In der Druckwarteschlange stehen mehrere Dokumente. Sie wollen verhindern, dass die Dokumente auf dem Drucker ausgedruckt werden, doch Sie möchten auch nicht, dass Benutzer die Dokumente erneut an den Drucker senden müssen. Wie gehen Sie am besten vor?
 - A. Das Dialogfeld *Eigenschaften* des Druckers öffnen und auf der Registerkarte *Freigabe* die Option *Drucker nicht freigeben* wählen.
 - B. Das Dialogfeld *Eigenschaften* des Druckers öffnen und einen Anschluss auswählen, der keinem Druckgerät zugeordnet ist.

- C. Das Warteschlangenfenster des Druckers öffnen, das erste Dokument auswählen und dann im Menü *Dokument* den Befehl *Anhalten* wählen.
- D. Das Warteschlangenfenster des Druckers öffnen und im Menü *Drucken* den Befehl *Drucker anhalten* wählen.



Gedankenexperiment Wenden Sie in diesem Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Als Mitarbeiter für den technischen Support sind Sie für eine Anwaltskanzlei mit einer Gruppe von 10 Gerichtssekreteränen tätig, die Verwaltungsarbeiten für die Rechtsanwälte ausführen. Alle Sekretäre verwenden einen einzigen freigegebenen Hochgeschwindigkeits-laserdrucker, der an einen dedizierten Windows-Druckerserver angeschlossen ist. Die Sekretäre müssen regelmäßig mehrere Kopien großer Dokumente drucken und obwohl der Laserdrucker schnell ist, läuft er nahezu ständig. Manchmal müssen die Sekretäre 20 Minuten oder noch länger warten, nachdem sie einen Druckauftrag für ihre Dokumente abgeschickt haben, bevor er in der Druckwarteschlange an die Spitze gelangt ist. Der Büroleiter hat angeboten, zusätzliche Drucker für die Abteilung anzuschaffen. Allerdings haben sich die Sekretäre daran gewöhnt, einfach auf *Drucken* zu klicken, und sie scheuen die Vorstellung, mehrere Druckwarteschlangen inspizieren zu müssen, um diejenige mit den wenigsten Druckaufträgen herauszufinden, bevor sie ein Dokument abschicken.

Beantworten Sie für dieses Szenario die folgenden Frage:

Wie können Sie für das Büro eine Druckerlösung einrichten, bei der die Sekretäre zusätzliche Drucker möglichst effizient nutzen können?

Prüfungsziel 2.3: Server für die Remoteverwaltung konfigurieren

Windows Server 2012 ist für eine einfache Remoteserververwaltung konzipiert, sodass Administratoren nur selten, wenn überhaupt, direkt an der Serverkonsole arbeiten müssen. Dies spart Serverressourcen, die sich besser den Anwendungen zuteilen lassen.

Dieses Prüfungsziel zeigt, wie Sie

- WinRM konfigurieren
 - die Verwaltung von Servern mit einer Vorgängerversion konfigurieren
 - Server für laufende Verwaltungsaufgaben konfigurieren
 - Mehrserververwaltung konfigurieren
 - Server Core konfigurieren
 - die Windows-Firewall konfigurieren
-

Remoteverwaltung mit dem Server-Manager

Der Server-Manager ist schon seit Windows Server 2003 das Hauptinstrument für die Serveradministration von Windows Server. Die auffälligste Verbesserung, die der Server-Manager in Windows Server 2012 erfahren hat, ist die Fähigkeit, administrative Aufgaben sowohl auf Remoteservern als auch auf dem lokalen System durchführen zu können.

Wenn Sie sich bei einer vollständigen Installation von Windows Server 2012 mit grafischer Benutzeroberfläche unter einem Administratorkonto anmelden, startet der Server-Manager automatisch und zeigt die Kachel *Willkommen* an. Die Server-Manager-Benutzeroberfläche besteht aus dem Navigationsbereich auf der linken Seite mit den Symbolen, die verschiedene Ansichten von Serverressourcen darstellen. Wenn Sie ein Symbol auswählen, erscheint im rechten Bereich eine Startseite, die aus einer Reihe von Kacheln mit Informationen über die Ressource besteht. Die standardmäßig angezeigte *Dashboard*-Seite enthält in Ergänzung zur Kachel *Willkommen* Miniaturansichten, die die anderen Ansichten von Server-Manager im Überblick zeigen. Zu diesen anderen Ansichten gehören eine Seite für den lokalen Server, eine Seite für alle Server sowie weitere für Servergruppen und Rollengruppen.

Server hinzufügen

Der Server-Manager von Windows Server 2012 unterscheidet sich gegenüber vorherigen Versionen vor allem durch die Fähigkeit, mehrere Server auf einmal hinzufügen und verwalten zu können. Zwar erscheint beim ersten Start nur der lokale Server im Server-Manager, doch können Sie weitere Server hinzufügen und sie dann gemeinsam verwalten. Es lassen sich Server hinzufügen, die physisch oder virtuell sind und jede Windows Server-Version von Windows Server 2003 an aufwärts ausführen. Nachdem Sie der Benutzeroberfläche Server hinzugefügt haben, können Sie Gruppen mit Auflistungen von Servern erstellen, wie zum Beispiel Server an einem bestimmten Standort oder Server, die eine besondere Funktion

ausführen. Diese Gruppen sind im Navigationsbereich zu sehen, sodass Sie sie als einzelne Entität verwalten können.

Führen Sie die folgenden Schritte aus, um Server im Server-Manager hinzuzufügen:

1. Melden Sie sich beim Server, der Windows Server 2012 ausführt, unter einem Konto mit Administratorrechten an. Es erscheint das Fenster *Server-Manager*.
2. Klicken Sie im Navigationsbereich auf das Symbol *Alle Server*, um die Startseite *Alle Server* zu öffnen.
3. Im Menü *Verwalten* wählen Sie *Server hinzufügen*. Daraufhin erscheint das Dialogfeld *Server hinzufügen*.
4. Gehen Sie auf eine der folgenden Registerkarten, um festzulegen, wie Sie die hinzuzufügenden Server suchen möchten:
 - **Active Directory** Erlaubt eine Suche nach Computern, die bestimmte Betriebssysteme an bestimmten Standorten in der lokalen AD DS-Domäne ausführen
 - **DNS** Erlaubt eine Suche nach Servern in Ihrem momentan konfigurierten DNS (Domain Name System)-Server
 - **Importieren** Erlaubt es, eine Textdatei mit den Namen oder IP-Adressen der hinzuzufügenden Server bereitzustellen
5. Leiten Sie eine Suche ein oder laden Sie eine Textdatei hoch, um eine Liste der verfügbaren Server anzuzeigen.

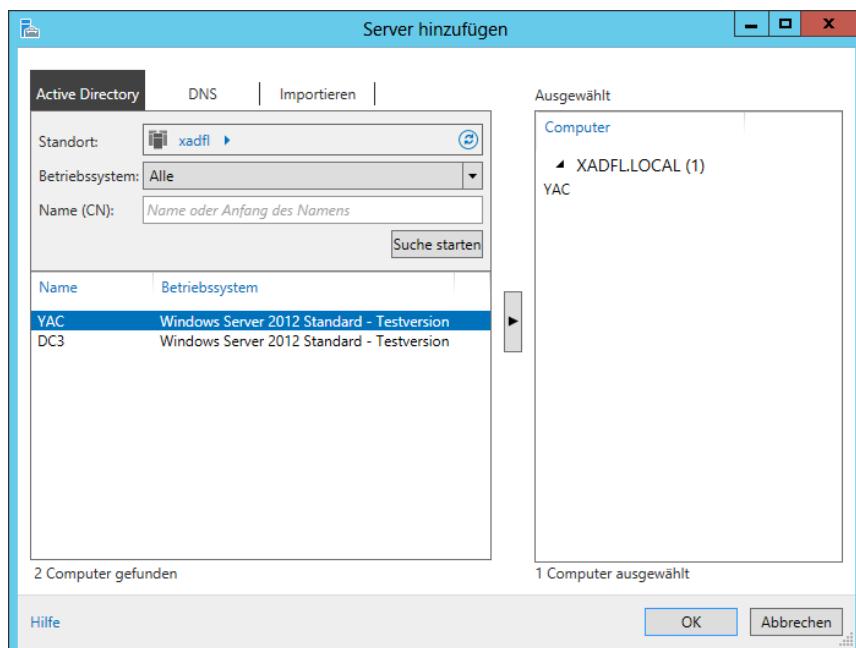


Abbildung 2.22 Ausgewählte Server im Server-Manager

6. Wählen Sie die hinzuzufügenden Server aus und klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil, um sie in die Liste *Ausgewählt* zu übernehmen, wie es in Abbildung 2.22 zu sehen ist.
7. Klicken Sie auf *OK*. Die ausgewählten Server sind jetzt auf der Startseite *Alle Server* aufgeführt.
8. Schließen Sie die Server-Manager-Konsole.

Nachdem Sie der Server-Manager-Benutzeroberfläche Remoteserver hinzugefügt haben, erscheinen diese auf der Startseite *Alle Server*. Dann können Sie auf sie in verschiedener Weise zugreifen, und zwar je nach Windows-Version, die der Remoteserver ausführt.

Windows Server 2012-Server verwalten

Wenn Sie Server, die unter Windows Server 2012 laufen, im Server-Manager hinzufügen, können Sie sofort den Assistenten zum Hinzufügen von Rollen und Features aufrufen, um Rollen und Features auf den hinzugefügten Servern zu installieren.

Es lassen sich auch andere Verwaltungsaufgaben durchführen, beispielsweise NIC-Teamvorgänge konfigurieren und den Server neu starten, da die Windows-Remoteverwaltung (Windows Remote Management, WinRM) auf Windows Server 2012 standardmäßig aktiviert ist.

WinRM konfigurieren

WinRM erlaubt es Administratoren, einen Computer von einem Remotestandort aus zu verwalten, und zwar mithilfe von Tools, die auf WMI (Windows Management Instrumentation) und Windows PowerShell basieren. Die WinRM-Einstellungen können Sie über die Server-Manager-Benutzeroberfläche anpassen.

Auf der Startseite *Lokaler Server* zeigt in der Kachel *Eigenschaften* ein Indikator für die Remoteverwaltung den aktuellen WinRM-Status des Servers an. Möchten Sie den WinRM-Status ändern, klicken Sie auf den Hyperlink *Remoteverwaltung*, um das Dialogfeld *Remoteverwaltung konfigurieren* zu öffnen. Wenn Sie das Kontrollkästchen *Remoteverwaltung dieses Servers von anderen Computern aktivieren* ausschalten, wird WinRM deaktiviert, wenn Sie es setzen, aktiviert.



Hinweis Windows PowerShell

Um WinRM von einer Windows PowerShell-Sitzung aus zu verwalten, wie es bei einem Computer mit einer Server Core-Installation der Fall ist, verwenden Sie den folgenden Befehl:

`Configure-SMRemoting.exe -Get|-Enable|-Disable`

- `-Get` zeigt den aktuellen WinRM-Status an
 - `-Enable` aktiviert WinRM
 - `-Disable` deaktiviert WinRM
-

Windows-Firewall konfigurieren

Wenn Sie MMC-Snap-Ins starten, die sich auf einen Remoteserver beziehen, wie zum Beispiel die Konsole *Computerverwaltung*, ernten Sie eine Fehlermeldung aufgrund der standardmäßigen Windows-Firewall-Einstellungen in Windows Server 2012. MMC verwendet DCOM (Distributed Component Object Model) für die Remoteverwaltung anstelle von WinRM, und diese Einstellungen sind standardmäßig nicht aktiviert.

Um dieses Problem zu beseitigen, müssen Sie die folgenden eingehenden Regeln der Windows-Firewall auf dem Remoteserver aktivieren, den Sie verwalten möchten:

- COM+-Netzwerkzugriff (DCOM-In)
- Remote-Ereignisprotokollverwaltung (NP eingehend)
- Remote-Ereignisprotokollverwaltung (RPC)
- Remote-Ereignisprotokollverwaltung (RPC-EPMAP)

Die Firewall-Regeln auf dem Remotesystem können Sie nach einer der folgenden Methoden ändern:

- Das MMC-Snap-In *Windows-Firewall mit erweiterte Sicherheit* auf dem Remoteserver öffnen (falls es sich um eine vollständige Installation mit grafischer Benutzeroberfläche handelt)
- Den Befehl `Netsh AdvFirewall` von einer Eingabeaufforderung mit Administratorrechten ausführen
- Das `NetSecurity`-Modul in Windows PowerShell verwenden
- Ein Gruppenrichtlinienobjekt mit den entsprechenden Einstellungen erstellen und es auf den Remoteserver anwenden



Hinweis Windows PowerShell

Die für die Remoteserververwaltung mithilfe von DCOM erforderlichen Windows-Firewall-Regeln auf einer Server Core-Installation können Sie mit der folgenden Windows PowerShell-Syntax konfigurieren:

```
Set-NetFirewallRule -name <rule name> -enabled True
```

Mit dem Befehl `Get-NetFirewallRule` erhalten Sie die Windows PowerShell-Namen für die vorkonfigurierten Regeln in der Windows-Firewall. Die entsprechenden Befehle, um die vier Regeln zu aktivieren, lauten wie folgt:

```
Set-NetFirewallRule -name  
ComPlusNetworkAccess-DCOM-In -enabled True  
Set-NetFirewallRule -name  
RemoteEventLogSvc-In-TCP -enabled True  
Set-NetFirewallRule -name RemoteEventLogSvc-NP-In-TCP  
-enabled True  
Set-NetFirewallRule -name  
RemoteEventLogSvc-RPCSS-In-TCP  
-enabled True
```

Für die Administratoren, die an Lösungen zur Remoteverwaltung interessiert sind, bietet die Gruppenrichtlinienmethode deutliche Vorteile. Damit können Sie nicht nur die Firewall auf dem Remotesystem konfigurieren, ohne auf die Serverkonsole direkt zuzugreifen, sondern auch die Firewall auf Server Core-Installationen konfigurieren, ohne von der Befehlszeile arbeiten zu müssen. Schließlich – und das ist bei großen Netzwerken wahrscheinlich am wichtigsten – können Sie mithilfe einer Gruppenrichtlinie die Firewall auf allen Servern, die Sie verwalten möchten, auf einmal konfigurieren.

Führen Sie die folgenden Schritte aus, um Windows-Firewall-Einstellungen mithilfe einer Gruppenrichtlinie zu konfigurieren. Dieser Ablauf setzt voraus, dass der Server einer AD DS-Domäne angehört und auf ihm das Feature *Gruppenrichtlinienverwaltung* installiert ist.

1. Melden Sie sich am Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* erscheint.
2. Öffnen Sie die Konsole *Gruppenrichtlinienverwaltung* und erstellen Sie ein neues Gruppenrichtlinienobjekt mit einem Namen wie zum Beispiel **Server-Firewall-Konfiguration**.
3. Öffnen Sie dieses Gruppenrichtlinienobjekt mit dem Gruppenrichtlinienverwaltungs-Editor.



Weitere Informationen Gruppenrichtlinienobjekte

Ausführliche Informationen, wie Sie Gruppenrichtlinienobjekte erstellen und sie mit anderen Objekten verknüpfen, finden Sie im Prüfungsziel 6.1, »Gruppenrichtlinienobjekte (GPOs) erstellen«.

4. Gehen Sie zum Knoten *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Windows-Firewall mit erweiterter Sicherheit\Windows-Firewall mit erweiterter Sicherheit\Eingehende Regeln*.
5. Klicken Sie mit der rechten Maustaste auf *Eingehende Regeln* und wählen Sie im Kontextmenü den Befehl *Neue Regel*. Der Assistent für neue eingehende Regel startet und zeigt die Seite *Regeltyp* an.
6. Wählen Sie die Option *Vordefiniert* und in der Dropdownliste den Eintrag *COM+-Netzwerkzugriff*. Klicken Sie auf *Weiter*. Der Assistent zeigt die Seite *Vordefinierte Regeln* an.
7. Klicken Sie auf *Weiter*, um zur Seite *Aktion* zu gelangen.
8. Lassen Sie die Option *Verbindung zulassen* ausgewählt und klicken Sie auf *Fertig stellen*. Die Regel erscheint in der Konsole *Gruppenrichtlinienverwaltungs-Editor*.
9. Öffnen Sie den Assistenten für neue eingehende Regel erneut.
10. Wählen Sie die Option *Vordefiniert* und in der Dropdownliste den Eintrag *Remote-Ereignisprotokollverwaltung*. Klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Vordefinierte Regeln*, die die drei Regeln in der Gruppe *Remote-Ereignisprotokollverwaltung* anzeigt.

11. Lassen Sie die drei Regeln ausgewählt und klicken Sie auf *Weiter*, um die Seite *Aktion* zu öffnen.
12. Lassen Sie die Option *Verbindung zulassen* ausgewählt und klicken Sie auf *Fertig stellen*. Die drei Regeln erscheinen in der Konsole *Gruppenrichtlinienverwaltungs-Editor*.
13. Schließen Sie die Konsole *Gruppenrichtlinienverwaltungs-Editor*.
14. In der Konsole *Gruppenrichtlinienverwaltung* verknüpfen Sie das eben erstellte Gruppenrichtlinienobjekt **Server-Firewall-Konfiguration** mit Ihrer Domäne.
15. Schließen Sie die Konsole *Gruppenrichtlinienverwaltung*.

Die Einstellungen in dem von Ihnen erstellten Gruppenrichtlinienobjekt werden im nächsten Durchlauf oder Neustart auf Ihren Remoteservern bereitgestellt und Sie können darauf mit MMC-Snap-Ins wie zum Beispiel *Computerverwaltung* und *Datenträgerverwaltung* zugreifen.

Server mit einer Vorgängerversion verwalten

Die Windows-Firewallregeln, die Sie für Remoteserver unter Windows Server 2012 aktiviert haben, sind auf Computern, die vorherige Versionen von Windows Server ausführen, standardmäßig deaktiviert. Deshalb müssen Sie sie auf derartigen Servern explizit aktivieren.

Im Unterschied zu Windows Server 2012 fehlt aber vorherigen Versionen des Betriebssystems die erforderliche WinRM-Unterstützung, um sie mithilfe des neuen Server-Managers verwalten zu können.

Wenn Sie Server mit Windows Server 2008 oder Windows Server 2008 R2 im Server-Manager von Windows Server 2012 hinzufügen, erscheinen sie standardmäßig mit dem Verwaltbarkeitsstatus »Online – Stellen Sie sicher, dass der WinRM 3.0-Dienst installiert ist, ausgeführt wird und die erforderlichen Firewallports geöffnet sind.« Um die WinRM-Unterstützung für Server unter Windows Server 2008 oder Windows Server 2008 R2 hinzuzufügen, müssen Sie die folgenden Updates herunterladen und installieren:

- .NET Framework 4.0
- Windows Management Framework 3.0

Diese Updates stehen im Microsoft Download Center unter den folgenden URLs zum Download bereit:

- <http://www.microsoft.com/en-us/download/details.aspx?id=17718>
- <http://www.microsoft.com/en-us/download/details.aspx?id=34595>

Nachdem Sie die Updates installiert haben, startet das System zwar automatisch den Dienst *Windows-Remoteverwaltung*, doch müssen Sie auf dem Remoteserver noch die folgenden Aufgaben abschließen:

- Die Regeln *Windows-Remoteverwaltung (HTTP eingehend)* in der Windows-Firewall aktivieren, wie Abbildung 2.23 zeigt

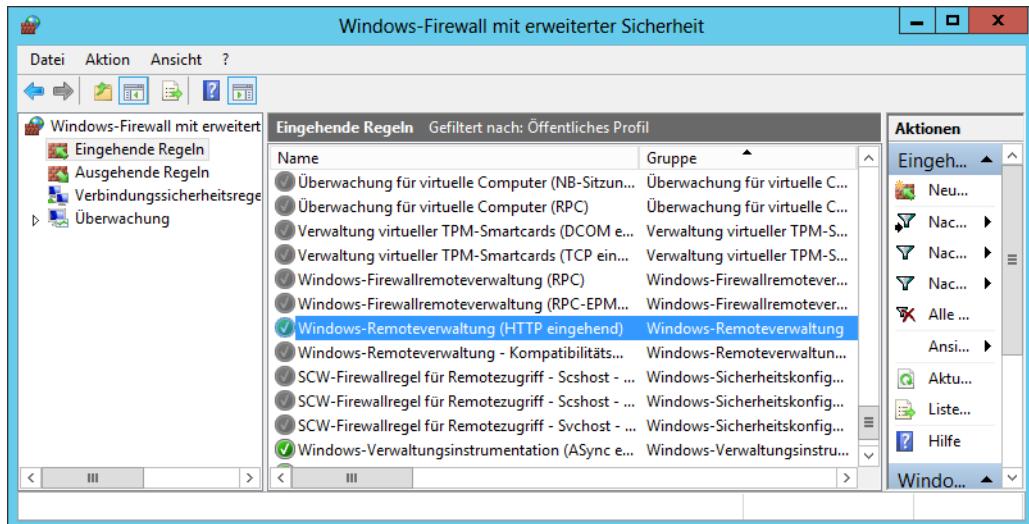


Abbildung 2.23 Die Regeln *Windows-Remoteverwaltung* in der Konsole *Windows-Firewall mit erweiterter Sicherheit*

- Einen WinRM-Listener erstellen, indem der Befehl `winrm quickconfig` an einer Eingabeaufforderung mit Administratorrechten ausgeführt wird
- Die Regeln *COM+-Netzwerkzugriff* und *Remote-Ereignisprotokollverwaltung* in der Windows-Firewall aktivieren, wie es der vorherige Abschnitt beschrieben hat

Nachdem Sie die genannten Updates installiert haben, bestehen immer noch Beschränkungen hinsichtlich der Verwaltungsaufgaben, die Sie bei früheren Windows Server-Versionen von einem Remotestandort durchführen können. Zum Beispiel ist es nicht möglich, mit dem Assistenten zum Hinzufügen von Rollen und Features im Server-Manager auf früheren Windows Server-Versionen Rollen und Features zu installieren. Diese Server erscheinen auf der Seite *Zielserver auswählen* nicht im Serverpool.

Allerdings können Sie mithilfe von Windows PowerShell auf Servern, die unter Windows Server 2008 oder Windows Server 2008 R2 laufen, Rollen und Features remote installieren, wie der folgende Ablauf beschreibt:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Es erscheint das Fenster *Server-Manager*.
2. Öffnen Sie eine Windows PowerShell-Sitzung mit Administratorrechten.
3. Richten Sie mit dem folgenden Befehl eine Windows PowerShell-Sitzung mit dem Remotecomputer ein:
`Enter-PSSession <Remoteservername> -credential <Benutzername>`
4. Geben Sie das Kennwort ein, das zum angegebenen Benutzernamen gehört, und drücken Sie **[Enter]**.

5. Mit dem folgenden Befehl zeigen Sie eine Liste von Rollen und Features auf dem Remoteserver an:
`Get-WindowsFeature`
6. Installieren Sie die Komponente. Verwenden Sie dazu den Kurznamen der Rolle oder des Diensts, wie er in der Get-WindowsFeature-Anzeige erscheint, mit dem folgenden Befehl:
`Add-WindowsFeature <Featurename>`
7. Verwenden Sie den folgenden Befehl, um die Sitzung mit dem Remoteserver zu schließen:
`Exit-PSSession`
8. Schließen Sie das Windows PowerShell-Fenster.



Hinweis Windows PowerShell

Wenn Sie eine Rolle oder ein Feature per Windows PowerShell auf einem Remoteserver installieren, bindet die Installation keine Verwaltungstools für die Rolle ein, wie es bei einer Assistenten-basierten Installation der Fall wäre. Allerdings können Sie die Tools zusammen mit der Rolle oder dem Feature installieren, wenn Sie auf der `Install-WindowsFeature`-Befehlszeile den Parameter `IncludeManagementTools` angeben. Achten Sie aber bei der Option *Server Core-Installation* darauf, dass trotz dieses Parameters weder MMC-Snap-Ins noch andere grafische Tools installiert werden.

Servergruppen erstellen

Administratoren von Unternehmensnetzwerken müssen gegebenenfalls eine große Anzahl von Servern in Server-Manager hinzufügen. Damit Sie sich nicht durch lange Listen von Servern durcharbeiten müssen, können Sie Servergruppen basierend auf Serverstandorten, Funktionen oder anderen organisatorischen Paradigmen erstellen.

Wenn Sie eine Servergruppe anlegen, erscheint sie als Symbol im Navigationsbereich. Dann können Sie die Server in der Gruppe genauso wie in der Gruppe *Alle Server* verwalten.

Eine Servergruppe erstellen Sie in folgenden Schritten:

1. Melden Sie sich bei Windows Server 2012 an und starten Sie den Server-Manager.
2. Klicken Sie im Navigationsbereich auf das Symbol *Alle Server*. Die Startseite *Alle Server* erscheint.
3. Wählen Sie im Menü *Verwalten* den Befehl *Servergruppe erstellen*. Damit gelangen Sie zum Dialogfeld *Servergruppe erstellen*, das Abbildung 2.24 zeigt.
4. Geben Sie in das Textfeld *Servergruppenname* den Namen ein, den Sie der Servergruppe zuweisen möchten.
5. Legen Sie auf einer der vier Registerkarten eine Methode für die Auswahl von Servern fest.

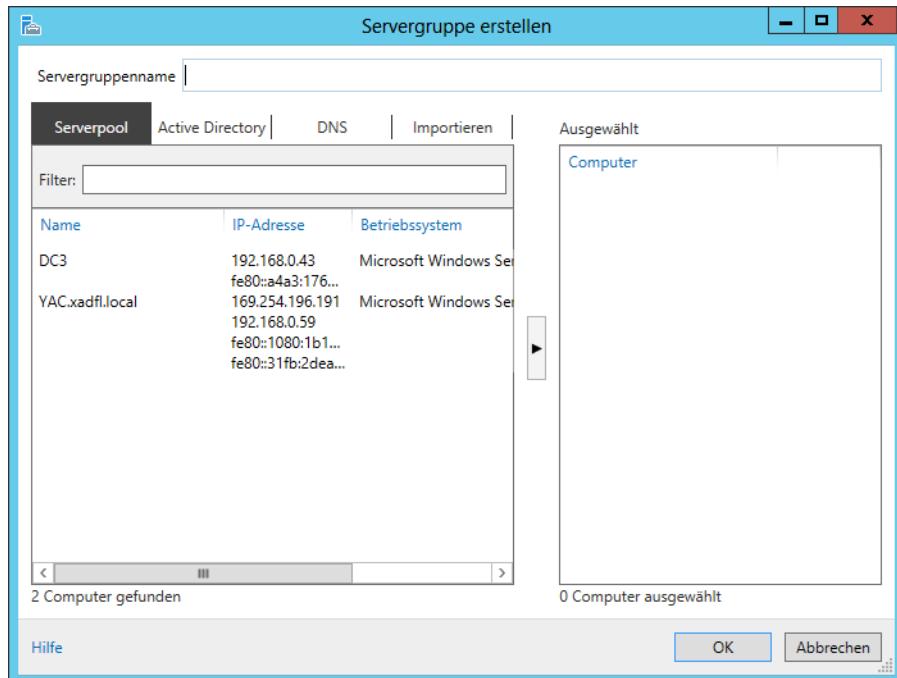


Abbildung 2.24 Das Dialogfeld *Servergruppe erstellen* im Server-Manager

6. Markieren Sie die Server, die Sie der Gruppe hinzufügen möchten, und klicken Sie auf die Schaltfläche mit dem nach rechts weisenden Pfeil, um sie in das Feld *Ausgewählt* zu übernehmen.
7. Klicken Sie auf *OK*. Im Navigationsbereich erscheint ein neues Servergruppensymbol mit dem angegebenen Namen.
8. Schließen Sie die Konsole *Server-Manager*.

Das Erstellen von Servergruppen wirkt sich nicht auf die Funktionen aus, die sich auf ihnen ausführen lassen. Zum Beispiel sind keine Aktionen für komplett Servergruppen möglich. Die Gruppierungen sind lediglich dazu gedacht, eine große Anzahl von Servern zu organisieren und sie leicht auffinden zu können.

Remoteserver-Verwaltungstools verwenden

Remoteserver können Sie von jedem Computer, der unter Windows Server 2012 läuft, verwalten. Die erforderlichen Tools werden standardmäßig installiert. Allerdings legt die von Microsoft propagierte neue Verwaltungsmethode den Administratoren nahe, die Server wegzuschließen und sie an einem Remotestandort von einer Arbeitsstation aus zu verwalten.

Damit Sie Windows-Server von einer Arbeitsstation aus verwalten können, müssen Sie das Paket *Remoteserver-Verwaltungstools* für die Windows-Version installieren, die auf Ihrer

Arbeitsstation läuft. Das Paket steht im Microsoft Download Center unter <http://www.microsoft.com/download> zum Download bereit.

Die Remoteserver-Verwaltungstools sind in einer Microsoft-Updatedatei mit der Erweiterung *.msu* gepackt, sodass Sie sie ganz einfach vom Datei-Explorer, von der Eingabeaufforderung oder per Software Distribution in einem Gruppenrichtlinienobjekt bereitstellen können. Wenn Sie Remoteserver-Verwaltungstools auf einer Arbeitsstation unter Windows 8 installieren, sind sämtliche Tools standardmäßig aktiviert. Im Gegensatz dazu war es in vorherigen Versionen erforderlich, die Tools über die Systemsteuerungsoption *Windows-Funktionen* explizit zu aktivieren. Allerdings können Sie weiterhin ausgewählte Features über die Systemsteuerung zuschalten.

Wenn Sie den Server-Manager auf einer Windows-Arbeitsstation starten, gibt es keinen lokalen Server und keine Remoteserver zu verwalten, bis Sie diese hinzugefügt haben. Das geschieht nach den gleichen Schritten, wie sie weiter vorn in diesem Lernziel beschrieben wurden.

Der Zugriff auf die Server hängt vom Konto ab, mit dem Sie sich bei der Arbeitsstation anmelden. Erscheint eine Meldung »Zugriff verweigert«, können Sie sich mit dem Server über ein anderes Konto verbinden. Klicken Sie dann mit der rechten Maustaste auf den Server und wählen Sie im Kontextmenü den Befehl *Verwalten als*, um ein Standarddialogfeld *Windows-Sicherheit* anzuzeigen, in dem Sie alternative Anmeldeinformationen angeben können.

Mit Remoteservern arbeiten

Nachdem Sie im Server-Manager Remoteserver hinzugefügt haben, können Sie auf sie mithilfe verschiedener Remoteverwaltungstools zugreifen.

Server-Manager bietet die folgenden drei grundlegenden Methoden, um mit Remoteservern zu arbeiten:

- **Kontextabhängige Aufgaben** Wenn Sie in einer Server-Kachel an beliebiger Stelle im Server-Manager mit der rechten Maustaste klicken, erscheint ein Kontextmenü mit Tools und Befehlen, die auf den ausgewählten Server verweisen. Dazu gehören Befehle, die der Server-Manager auf dem Remoteserver ausführt, beispielsweise *Server neu starten* und *Windows PowerShell*. Andere Befehle starten Tools auf dem lokalen System und dirigieren sie zum Remoteserver, zum Beispiel MMC-Snap-Ins und der Assistent zum Installieren von Rollen und Features. Wieder andere beziehen sich auf den Server-Manager selbst, etwa Befehle, die Server aus der Benutzeroberfläche entfernen. Für spezielle Bereiche erscheinen weitere kontextabhängige Aufgaben in den *Aufgaben*-Menüs.
- **Kontextunabhängige Aufgaben** Die Menüleiste am oberen Rand der Server-Manager-Konsole bietet Zugriff auf interne Aufgaben. Unter anderem starten Sie von hier aus die Assistenten zum Hinzufügen von Servern und zum Installieren von Rollen und Features oder öffnen das Dialogfeld *Server-Manager-Eigenschaften*, in dem Sie das Aktualisierungsintervall der Konsole festlegen können.

- **Kontextunabhängige Tools** Das Menü *Tools* der Konsole bietet Zugriff auf externe Programme, wie zum Beispiel MMC-Snap-Ins und die Windows PowerShell-Oberfläche, die sich auf das lokale System beziehen

Prüfungszielzusammenfassung

- Windows Server 2012 ist für eine einfache Remoteserververwaltung konzipiert, sodass Administratoren nur selten, wenn überhaupt, direkt an der Serverkonsole arbeiten müssen. Dies spart Serverressourcen, die sich besser den Anwendungen zuteilen lassen.
- Wenn Sie Server, die unter Windows Server 2012 laufen, im Server-Manager hinzufügen, können Sie sofort den Assistenten zum Hinzufügen von Rollen und Features aufrufen, um Rollen und Features auf den hinzugefügten Servern zu installieren
- Die Windows-Firewall-Regeln, die Sie für Remoteserver unter Windows Server 2012 aktiviert haben, sind auf Computern, die vorherige Versionen von Windows Server ausführen, standardmäßig deaktiviert. Deshalb müssen Sie sie auf derartigen Servern explizit aktivieren.
- Administratoren von Unternehmensnetzwerken müssen gegebenenfalls eine große Anzahl von Servern in Server-Manager hinzufügen. Damit Sie sich nicht durch lange Listen von Servern durcharbeiten müssen, können Sie Servergruppen basierend auf Serverstandorten, Funktionen oder anderen organisatorischen Paradigmen erstellen.
- Remoteserver können Sie von jedem Computer, der unter Windows Server 2012 läuft, verwalten. Die erforderlichen Tools werden standardmäßig installiert. Allerdings legt die von Microsoft propagierte neue Verwaltungsmethode den Administratoren nahe, die Server wegzuschließen und sie an einem Remtestandort von einer Arbeitsstation aus zu verwalten.

Prüfungszielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Prüfungsziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Aufgaben müssen Sie erledigen, bevor Sie mit dem Snap-In *Computerverwaltung* einen unter Windows Server 2012 laufenden Remoteserver verwalten können?
 - A. WinRM auf dem Remoteserver aktivieren.
 - B. Die Regel *COM+-Netzwerkzugriff* auf dem Remoteserver aktivieren.
 - C. Die Regeln *Remote-Ereignisprotokollverwaltung* auf dem Remoteserver aktivieren.
 - D. Die Remoteserver-Verwaltungstools auf dem Remoteserver installieren.

2. Mit welchem der folgenden Windows PowerShell-Cmdlets können Sie die vorhandenen Windows-Firewall-Regeln auf einem Windows Server 2012-Computer auflisten? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Get-NetFirewallRule
 - B. Set-NetFirewallRule
 - C. Show-NetFirewallRule
 - D. New-NetFirewallRule
3. Welche der folgenden Aufgaben können Sie für einen Windows Server 2008-Server NICHT remote ausführen?
 - A. Rollen mithilfe des Server-Managers installieren.
 - B. Rollen mithilfe von Windows PowerShell installieren.
 - C. Über das Snap-In Computerverwaltung die Verbindung zum Remoteserver herstellen.
 - D. Ereignisprotokolleinträge überwachen.
4. Welche der folgenden Updates müssen Sie auf einem unter Windows Server 2008 laufenden Server installieren, bevor Sie über den Windows Server 2012-Server-Manager eine Verbindung zu ihm herstellen können? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. .NET Framework 3.5
 - B. .NET Framework 4.0
 - C. Windows Management Framework 3.0
 - D. Windows Server 2008 R2
5. Welche der folgenden Elemente erscheinen NICHT in der Standardanzeige, wenn Sie Server-Manager von einer Windows 8-Arbeitsstation aus mithilfe der Remoteserver-Verwaltungstools ausführen?
 - A. Das Dashboard
 - B. Die Startseite *Lokaler Server*
 - C. Die Startseite *Alle Server*
 - D. Die Kachel *Willkommen*



Gedankenexperiment Wenden Sie in diesem Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Ralph ist verantwortlich für die 24 Server, die eine bestimmte Anwendung ausführen und die im gesamten Unternehmensnetzwerk seiner Firma verstreut sind. Er möchte auf seiner Windows 8-Arbeitsstation mithilfe von Server-Manager diese Server verwalten und die auf

ihnen auftretenden Ereignisse überwachen. Dazu muss er die eingehenden Regeln *COM+-Netzwerzugriff* und *Remote-Ereignisprotokollverwaltung* in der Windows-Firewall auf den Servern aktivieren.

Da er nicht sämtliche Standorte aller Server aufsuchen kann und das IT-Personal an vielen Standorten recht unzuverlässig arbeitet, hat sich Ralph dafür entschieden, die Windows-Firewall auf allen Servern über eine Gruppenrichtlinie zu konfigurieren. Die Active Directory Domänendienste-Struktur ist nach geografischen Aspekten organisiert mit der Konsequenz, dass sich die Server von Ralph an vielen verschiedenen OUs unter einer einzigen Domäne befinden.

Beantworten Sie für dieses Szenario die folgende Frage:

Wie kann Ralph über eine Gruppenrichtlinie die erforderlichen Regeleinstellungen für die Windows-Firewall auf seinen 24 Servern – und nur auf diesen Servern – bereitstellen?

Antworten

Dieser Abschnitt enthält die Lösungen für die Gedankenexperimente und Antworten auf die Fragen der Prüfungszielkontrollen in diesem Kapitel.

Prüfungsziel 2.1: Kontrolle

1. Richtige Antwort: C

- A. **Falsch:** Windows Server 2012 kann mehr als 8 Volumeschattenkopien verwalten.
- B. **Falsch:** Windows Server 2012 kann mehr als 16 Volumeschattenkopien verwalten.
- C. **Richtig:** Windows Server 2012 kann bis zu 64 Volumeschattenkopien verwalten, bevor die jeweils ältesten Daten gelöscht werden.
- D. **Falsch:** Windows Server 2012 kann nicht 128 Volumeschattenkopien verwalten.

2. Richtige Antwort: B

- A. **Falsch:** Authentifizierung heißt, die Identität des Benutzers zu überprüfen.
- B. **Richtig:** Autorisierung ist der Vorgang, durch den ein Benutzer Zugriff auf bestimmte Ressourcen gewährt wird, und zwar basierend auf den Berechtigungen, die er besitzt.
- C. **Falsch:** Das Windows-Feature *Zugriffsbasierte Aufzählung* hindert Benutzer daran, Ressourcen zu sehen, für die sie keine Berechtigungen besitzen.
- D. **Falsch:** Zuweisung beschreibt das Erteilen von Berechtigungen, jedoch nicht das Lesen.

3. Richtige Antworten: A, B

- A. **Richtig:** Über den Ressourcen-Manager für Dateiserver können Sie Administratoren mit E-Mail-Nachrichten darüber informieren, wenn Benutzer den ihnen zugewiesenen Speicherplatz überschreiten.

- B. **Richtig:** Mit dem Ressourcen-Manager für Dateiserver können Sie für einzelne Benutzer Datenträgerkontingente erstellen, die unterschiedliche Speicherlimits festlegen.
- C. **Falsch:** Mithilfe von NTFS-Datenträgerkontingenzen können Sie Benutzer daran hindern, den Speicherplatz auf einem Volume über deren zugeteiltes Limit hinaus zu verbrauchen.
- D. **Falsch:** Mithilfe von NTFS-Datenträgerkontingenzen können Sie Warnungen für Benutzer generieren, wenn sie sich ihrem zugeteilten Speicherlimit nähern.
4. **Richtige Antworten:** B, D
- A. **Falsch:** In den Windows Server-Versionen vor Windows Server 2012 werden spezielle Berechtigungen kombiniert, um Standardberechtigungen zu bilden.
- B. **Richtig:** Grundlegende Berechtigungen werden aus verschiedenen Kombinationen von erweiterten Berechtigungen gebildet.
- C. **Falsch:** Freigabeberechtigungen sind ein System, das vom NTFS-Berechtigungssystem getrennt ist.
- D. **Richtig:** In Windows Server-Versionen vor Windows Server 2012 werden Standardberechtigungen aus verschiedenen Kombinationen von speziellen Berechtigungen gebildet.
5. **Richtige Antwort:** D
- A. **Falsch:** Der Besitzer ist die einzige Person, die auf eine Datei zugreifen kann, der keine Berechtigungen zugewiesen wurden.
- B. **Falsch:** Der Sicherheitsprinzipal ist nicht dafür zuständig, die Berechtigungsrichtlinien einer Organisation zu erstellen.
- C. **Falsch:** Der Sicherheitsprinzipal empfängt Berechtigungen, er erstellt sie nicht.
- D. **Richtig:** Der Sicherheitsprinzipal ist der Benutzer oder Computer, dem Berechtigungen zugewiesen werden.

Prüfungsziel 2.1: Gedankenexperiment

Die wahrscheinlichste Ursache für das Problem ist, dass Leo nicht genügend Freigabeberechtigungen für den Lese-/Schreibzugriff auf die Contoso-Dateien besitzt. Wenn der Gruppe **CONTOSO_USERS** die Freigabeberechtigung **Vollzugriff Zulassen** erteilt wird, sollte Leo in der Lage sein, seine Änderungen in den Contoso-Dateien zu speichern.

Prüfungsziel 2.2: Kontrolle

1. **Richtige Antwort:** A
- A. **Richtig:** In Windows versteht man unter einem Drucker die Softwareschnittstelle, über die ein Computer mit einem Druckgerät kommuniziert.

- B. **Falsch:** Ein Druckerserver ist ein Gerät, das Druckaufträge von Clients entgegennimmt und sie an Druckgeräte sendet, die entweder lokal oder über das Netzwerk angeschlossen sind.
- C. **Falsch:** Ein Druckertreiber ist ein Gerätetreiber, der die von Anwendungen generierten Druckaufträge in eine geeignete Befehlssequenz für ein bestimmtes Druckgerät konvertiert.
- D. **Falsch:** Das Snap-In *Druckverwaltung* ist ein Tool, mit dem Administratoren Drucker im gesamten Netzwerk verwalten.
2. **Richtige Antwort: B**
- A. **Falsch:** Jeder Drucker muss mit einem eigenen Anschluss verbunden sein, egal ob die Drucker in einem Pool zusammengefasst sind oder nicht.
- B. **Richtig:** Um einen Druckerpool einzurichten, setzen Sie das Kontrollkästchen *Druckerpool aktivieren* und wählen dann die Anschlüsse entsprechend den Druckern aus, die Teil des Pools sein werden (oder erstellen diese Anschlüsse).
- C. **Falsch:** Um einen Druckerpool zu erstellen, verwenden Sie nicht die Einstellungen der installierbaren Optionen.
- D. **Falsch:** Prioritäten haben mit Druckerpools nichts zu tun.
3. **Richtige Antwort: A**
- A. **Richtig:** Wenn Sie die Freigabe des Druckers beenden, sind Benutzer nicht mehr in der Lage, das Druckgerät zu verwenden.
- B. **Falsch:** Wenn Sie den Drucker aus Active Directory entfernen, können Benutzer den Drucker zwar nicht mehr über eine Suche auffinden, aber immer noch darauf zugreifen.
- C. **Falsch:** Wenn Sie den Druckeranschluss ändern, können Benutzer keine Druckaufträge mehr an das Druckgerät senden, doch sind sie weiterhin in der Lage, Aufträge an den Drucker zu schicken.
- D. **Falsch:** Wenn Sie die Freigabe umbenennen, ist es möglicherweise schwierig für die Benutzer, den Drucker zu finden, aber sie können ihn verwenden, falls sie ihn doch finden.
4. **Richtige Antwort: C**
- A. **Falsch:** Die Berechtigung *Dokumente verwalten* erlaubt es Benutzern nicht, Aufträge an den Drucker zu senden.
- B. **Falsch:** Die Berechtigung *Drucker verwalten* erlaubt es Benutzern nicht, Aufträge an den Drucker zu senden.
- C. **Richtig:** Die Berechtigung *Drucken* ermöglicht es Benutzern, Dokumente an den Drucker zu senden, die Berechtigung *Dokumente verwalten* dagegen nicht.
- D. **Falsch:** Die Berechtigung *Dokumente verwalten* erlaubt es Benutzern nicht, Aufträge an den Drucker zu senden.

5. Richtige Antwort: D

- A. **Falsch:** Ein nicht freigegebener Drucker arbeitet die Aufträge noch ab, die bereits in der Warteschlange stehen.
- B. **Falsch:** Wenn Sie den Anschluss ändern, müssen Benutzer die bereits in der Warteschlange befindlichen Druckaufträge erneut senden.
- C. **Falsch:** Wird das erste Dokument in der Warteschlange angehalten, verhindert das nicht, dass die anderen Druckaufträge in der Warteschlange gedruckt werden.
- D. **Richtig:** Wenn Sie die Option *Drucker anhalten* auswählen, bleiben die Dokumente in der Druckwarteschlange, bis Sie das Drucken fortsetzen. Diese Option gilt für alle Dokumente in der Warteschlange.

Prüfungsziel 2.2: Gedankenexperiment

Installieren Sie zusätzliche, identische Drucker, verbinden Sie sie mit demselben Windows Server 2012-Druckerserver und erstellen Sie einen Druckerpool, indem Sie das entsprechende Kontrollkästchen auf der Registerkarte *Anschlüsse* im Eigenschaftenblatt des Druckers aktivieren.

Prüfungsziel 2.3: Kontrolle

1. Richtige Antwort: B

- A. **Falsch:** WinRM ist auf einem Windows Server 2012-Server standardmäßig aktiviert.
- B. **Richtig:** Die Regel *COM+-Netzwerkzugriff* ist auf dem Remoteserver zu aktivieren, damit die MMC-Snap-Ins eine Verbindung herstellen können.
- C. **Falsch:** Die *Remote-Ereignisprotokollverwaltung*-Regeln sind nicht erforderlich, um die Verbindung zu einem Remoteserver über ein MMC-Snap-In herstellen zu können.
- D. **Falsch:** PTR-Datensätze enthalten die erforderlichen Informationen, damit der Server Reverse-Lookups von Namen durchführen kann.

2. Richtige Antworten: A, C

- A. **Richtig:** Das Cmdlet `Get-NetFirewallRule` zeigt eine Liste aller Regeln auf einem System an, das Windows-Firewall ausführt.
- B. **Falsch:** Das Cmdlet `Set-NetFirewallRule` ist dafür vorgesehen, spezifische Regeln zu verwalten, und nicht, sie aufzulisten.
- C. **Richtig:** Das Cmdlet `Show-NetFirewallRule` zeigt eine Liste aller Regeln auf einem System an, das Windows-Firewall ausführt.
- D. **Falsch:** Das Cmdlet `New-NetFirewallRule` ist dafür vorgesehen, Regeln zu erstellen, und nicht, sie aufzulisten.

3. Richtige Antwort: A

- A. **Richtig:** Mit Server-Manager lassen sich keine Rollen auf einem Remoteserver installieren, der unter Windows Server 2008 läuft.
- B. **Falsch:** Mit Windows PowerShell können Sie Rollen auf einem Remoteserver installieren, der unter Windows Server 2008 läuft.
- C. **Falsch:** Über die Konsole *Computerverwaltung* können Sie sich nicht mit einem Windows Server 2008-Computer verbinden, außer wenn Sie die Regel *COM+Netzwerkzugriff* aktivieren.
- D. **Falsch:** Ereignisprotokolleinträge können Sie auf einem Remoteserver, der unter Windows Server 2008 läuft, überwachen, sofern Sie die *Remote-Ereignisprotokollverwaltung*-Regeln aktivieren.

4. Richtige Antworten: B, C

- A. **Falsch:** .NET Framework 3.5 ist nicht erforderlich, damit Server-Manager eine Verbindung zu Windows Server 2008 herstellen kann.
- B. **Richtig:** .NET Framework 4.0 ist erforderlich, damit Server-Manager eine Verbindung zu Windows Server 2008 herstellen kann.
- C. **Richtig:** Windows Management Framework 3.0 ist erforderlich, damit Server-Manager eine Verbindung zu Windows Server 2008 herstellen kann.
- D. **Falsch:** Es ist nicht erforderlich, ein Upgrade auf Windows Server 2008 R2 durchzuführen, damit sich Server-Manager mit Windows Server 2008 verbinden kann.

5. Richtige Antwort: B

- A. **Falsch:** Das Dashboard erscheint in der standardmäßigen Server-Manager-Anzeige.
- B. **Richtig:** Die Startseite *Lokaler Server* erscheint nicht, da es sich beim lokalen System um eine Arbeitsstation und nicht um einen Server handelt.
- C. **Falsch:** Die Startseite *Alle Server* erscheint in der standardmäßigen Server-Manager-Anzeige.
- D. **Falsch:** Die Kachel *Willkommen* erscheint in der standardmäßigen Server-Manager-Anzeige.

Prüfungsziel 2.3: Gedankenexperiment

Nachdem Ralph ein Gruppenrichtlinienobjekt mit den erforderlichen Windows-Firewall-Einstellungen eingerichtet hat, sollte er eine Sicherheitsgruppe mit allen 24 Computerobjekten anlegen, die seine Server darstellen. Dann sollte er das Gruppenrichtlinienobjekt mit der Firmendomäne verknüpfen und mithilfe der Sicherheitsfilterung den Gültigkeitsbereich des Gruppenrichtlinienobjekts auf die von ihm erstellte Gruppe einschränken.

K A P I T E L 3

Hyper-V konfigurieren

Das Konzept der Virtualisierung von Servern hat sich im Lauf der letzten Jahre von einem neuartigen Experiment zu einem komfortablen Labor- und Testwerkzeug gemausert und ist mittlerweile eine seriöse Bereitstellungsstrategie für Produktionsserver. Windows Server 2012 umfasst die Rolle *Hyper-V*, mit der Administratoren virtuelle Computer (Virtual Machines, VMs) erstellen können, die jeweils in ihrer eigenen isolierten Umgebung laufen. Virtuelle Computer sind eigenständige Einheiten, die Administratoren ganz leicht von einem physischen Computer auf einen anderen verschieben können. Dadurch vereinfacht sich das Bereitstellen von Netzwerkanwendungen und Diensten erheblich.

Dieses Kapitel behandelt einige der grundlegenden Aufgaben von Administratoren, um Hyper-V-Server und virtuelle Computer einzurichten und bereitzustellen.

Prüfungsziele in diesem Kapitel:

- Prüfungsziel 3.1: Einstellungen für den virtuellen Computer erstellen und konfigurieren 154
- Prüfungsziel 3.2: Speicher des virtuellen Computers erstellen und konfigurieren .. 178
- Prüfungsziel 3.3: Virtuelle Netzwerke erstellen und konfigurieren 197

Prüfungsziel 3.1: Einstellungen für den virtuellen Computer erstellen und konfigurieren

Servervirtualisierung in Windows Server 2012 basiert auf dem sogenannten Hypervisor-Modul. Der auch als Monitortreiber für virtuelle Computer (Virtual Machine Monitor, VMM) bezeichnete Hypervisor ist dafür zuständig, die physische Hardware des Computers zu abstrahieren und mehrere virtualisierte Hardwareumgebungen – die virtuellen Computer – zu schaffen. Jeder virtuelle Computer besitzt seine eigene (virtuelle) Hardwarekonfiguration und kann eine eigene Kopie eines Betriebssystems ausführen. Genügend physische Hardware und die korrekte Lizenzierung vorausgesetzt, kann somit ein einzelner Windows Server 2012-Computer, auf dem die Hyper-V-Rolle installiert ist, mehrere virtuelle Computer unterstützen, die Administratoren genauso verwalten können wie eigenständige Computer.

Dieses Prüfungsziel zeigt, wie Sie

- dynamischen Speicher konfigurieren
 - Smart Paging konfigurieren
 - Ressourcenmessung konfigurieren
 - Integrationsdienste konfigurieren
-

Virtualisierungsarchitekturen

Virtualisierungsprodukte können mehrere unterschiedliche Architekturen verwenden, um die Hardwareressourcen eines Computers unter den virtuellen Computern gemeinsam zu nutzen. Der frühe Typ der Virtualisierungsprodukte, zu denen auch Microsoft Windows Virtual PC und Microsoft Virtual Server gehören, setzt die Installation eines Standardbetriebssystems auf einem Computer voraus. Dieses wird zum »Host«-Betriebssystem. Dann installieren Sie das Virtualisierungsprodukt, das die Hypervisor-Komponente hinzufügt. Der Hypervisor führt praktisch das Hostbetriebssystem aus, wie es Abbildung 3.1 veranschaulicht, sodass Sie so viele virtuelle Computer erstellen können, wie es die Hardware des Computer erlaubt.

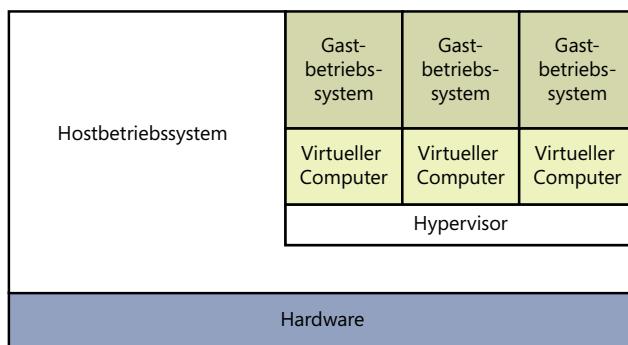


Abbildung 3.1 Ein hybrider VMM, der sich den Hardwarezugriff mit einem Hostbetriebssystem teilt

Diese Anordnung, bei der der Hypervisor über einem Hostbetriebssystem läuft, wird als Typ-2-Virtualisierung bezeichnet. Mithilfe des Typ-2-Hypervisors lässt sich für jeden virtuellen Computer eine virtuelle Hardwareumgebung schaffen. So können Sie festlegen, wie viel Speicher jeder virtuelle Computer erhalten soll, virtuelle Festplattenlaufwerke mit dem Festplattenplatz auf den physischen Laufwerken des Computers erstellen und Zugriff auf Peripheriegeräte bieten. Dann installieren Sie auf jedem virtuellen Computer ein »Gastbetriebssystem«, genauso als würden Sie einen neuen Computer bereitstellen. Das Hostbetriebssystem teilt sich dann den Zugriff auf den Prozessor des Computers mit dem Hypervisor, wobei sich jede Komponente die benötigten Taktzyklen nimmt und die Steuerung des Prozessors an die andere übergibt.

Typ-2-Virtualisierung kann eine adäquate VM-Leistung bereitstellen, insbesondere in Schulungsraum- und Laborumgebungen, doch bietet sie keine Leistung, die mit separaten physischen Computern vergleichbar wäre. Deshalb empfiehlt sie sich im Allgemeinen nicht für stark belastete Server in Produktionsumgebungen.

Die in Windows Server 2012 integrierte Virtualisierungsfunktionalität Hyper-V verwendet eine andere Art von Architektur, und zwar Typ-1-Virtualisierung. Hier bildet der Hypervisor eine Abstraktionsebene, die direkt mit der physischen Hardware des Computers interagiert – d.h. ohne Zutun eines Hostbetriebssystems. Der Begriff *Hypervisor* soll die Ebene über dem Term *Supervisor* symbolisieren, bezogen auf die Zuständigkeit, die Prozessortaktzyklen eines Computers zuzuteilen.

Der Hypervisor erstellt mit sogenannten *Partitionen* individuelle Umgebungen, die jeweils ihr eigenes Betriebssystem installieren und auf die Hardware des Computers über den Hypervisor zugreifen. Im Unterschied zur Typ-2-Virtualisierung teilt sich kein Betriebssystem Prozessorzeit mit dem Hypervisor. Stattdessen markiert der Hypervisor die erste von ihm erstellte Partition als übergeordnete Partition und alle darauffolgenden Partitionen als untergeordnete Partitionen, wie Abbildung 3.2 veranschaulicht.

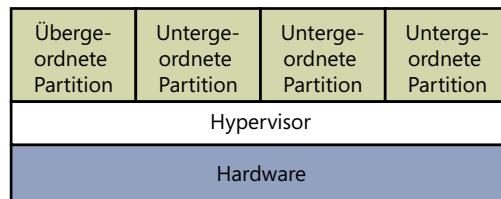


Abbildung 3.2 Eine VMM vom Typ 1, bei der der Hypervisor den gesamten Hardwarezugriff realisiert

Die übergeordnete Partition greift über den Hypervisor auf die Systemhardware zu, genau wie auch die untergeordneten Partitionen. Der einzige Unterschied besteht darin, dass die übergeordnete Partition den Virtualisierungsstack ausführt, der die untergeordneten Partitionen erstellt und verwaltet. Die übergeordnete Partition ist auch für die Subsysteme zuständig, die direkt die Performance der physischen Hardware des Computers beeinflussen, beispielsweise Plug&Play, Energieverwaltung und Fehlerbehandlung. Diese Subsysteme laufen ebenfalls in den Betriebssystemen auf den untergeordneten Partitionen, doch arbeiten sie nur mit virtueller Hardware, während die übergeordnete oder Root-Partition die eigentliche Hardware anspricht.



Hinweis Hyper-V

Es mag so aussehen, als ob die Hyper-V-Rolle in Windows Server 2012 Typ-1-Virtualisierung bereitstellt, da sie voraussetzt, dass das Windows Server-Betriebssystem installiert ist und läuft. Die hinzugefügte Hyper-V-Rolle konvertiert jedoch die installierte Instanz von Windows Server 2012 in die übergeordnete Partition und veranlasst das System, den Hypervisor vor dem Betriebssystem zu laden.

Hyper-V-Implementierungen

Windows Server 2012 enthält die Hyper-V-Rolle nur in den Editionen Standard und Datacenter. Die Hyper-V-Rolle ist für das Betriebssystem erforderlich, um als primäre Partition eines Computers fungieren und somit andere virtuelle Computer hosten zu können. Damit ein Betriebssystem als Gastbetriebssystem in einem virtuellen Computer funktioniert, ist keine spezielle Software erforderlich. Demzufolge ist Windows Server 2012 Essentials in der Lage, als Gastbetriebssystem zu arbeiten, obwohl es die Hyper-V-Rolle nicht mitbringt. Zu den anderen Gastbetriebssystemen, die Hyper-V unterstützt, gehören Betriebssysteme von Windows-Arbeitsstationen und viele andere Nicht-Microsoft-Server- und Arbeitsstationsprodukte.

Hyper-V-Lizenzerung

Hinsichtlich Hyper-V besteht der Unterschied zwischen den Editionen Standard und Datacenter von Windows Server 2012 vor allem in der Anzahl der virtuellen Computer, die die Versionen unterstützen. Wenn Sie eine Windows Server 2012-Instanz auf einem virtuellen Computer installieren, benötigen Sie eine Lizenz für das Betriebssystem, genau wie wenn Sie es auf einem physischen Computer installieren. Mit dem Kauf der Datacenter-Edition berechtigt Sie die Lizenz, eine unbegrenzte Anzahl von virtuellen Computern anzulegen, die Windows Server 2012 auf diesem einen physischen Computer ausführen. Die Standard-Lizenz erlaubt nur zwei virtuelle Instanzen von Windows Server 2012.



Hinweis Lizenzerung

Die Lizenzerungseinschränkungen der Editionen Windows Server 2012 Standard und Datacenter regeln nicht, wie viele virtuelle Computer Sie erstellen können, sondern schreiben lediglich vor, welches Betriebssystem Sie auf den virtuellen Computern installieren dürfen. Zum Beispiel können Sie eine Lizenz für die Standard-Edition nutzen, um zwei virtuelle Instanzen von Windows Server 2012 einzurichten, doch können Sie auch jede Anzahl von virtuellen Computern erstellen, die eine kostenlose Linux-Distribution ausführen.

Hardwareeinschränkungen von Hyper-V

In der Windows Server 2012-Version von Hyper-V wurde die Skalierbarkeit gegenüber vorherigen Versionen erheblich verbessert. Ein Windows Server 2012-Hyper-V-Hostsystem kann bis zu 320 logische Prozessoren enthalten und unterstützt bis zu 2048 virtuelle CPUs sowie bis zu 4 TB physischen Arbeitsspeicher.

Ein Server kann 1024 aktive virtuelle Computer hosten und auf jedem virtuellen Computer sind bis zu 64 virtuelle CPUs und bis zu 1 TB Arbeitsspeicher möglich.

Außerdem ist Hyper-V in der Lage, Cluster mit bis zu 64 Knoten und 8000 virtuellen Computern zu unterstützen.



Hinweis Windows PowerShell

Eine weitere wichtige Verbesserung in der Windows Server 2012-Version von Hyper-V ist die Integration eines Hyper-V-Moduls für Windows PowerShell. Es umfasst mehr als 160 neue Cmdlets, mit denen sich der Hyper-V-Dienst und dessen virtuelle Computer erstellen und verwalten lassen.

Hyper-V Server

Außer der Implementierung von Hyper-V in Windows Server 2012 bietet Microsoft ein dediziertes Hyper-V Server-Produkt, das eine Teilmenge von Windows Server 2012 ist. Hyper-V Server beinhaltet die Hyper-V-Rolle, die das Produkt während der Betriebssysteminstallation standardmäßig installiert. Mit Ausnahme einiger begrenzter Datei- und Speicherdienste sowie Remotedesktop-Funktionen umfasst das Betriebssystem keine anderen Rollen, wie Abbildung 3.3 zeigt.

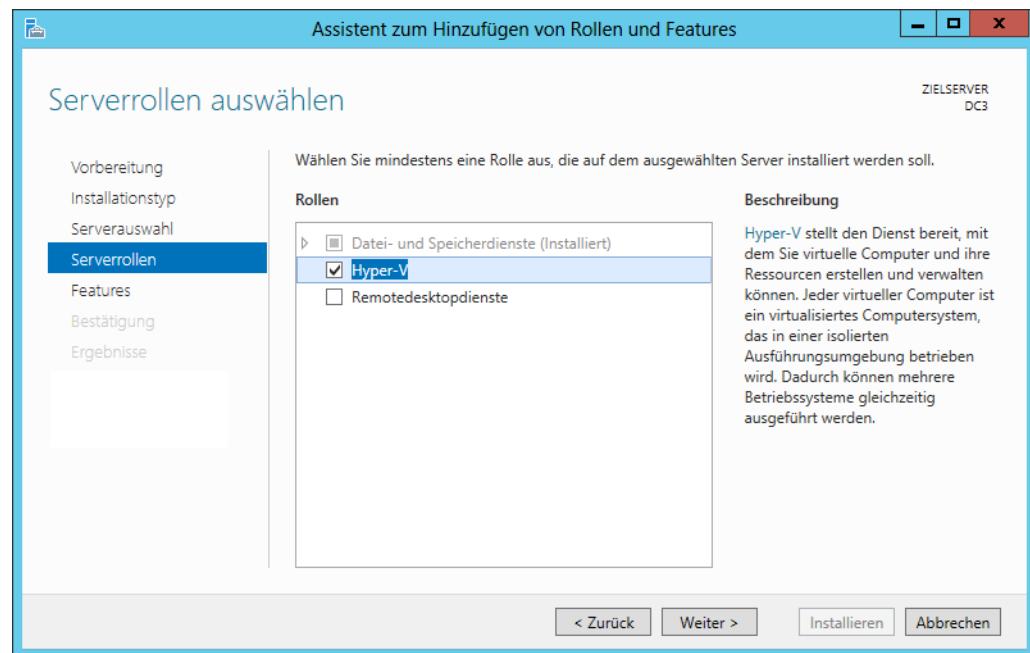


Abbildung 3.3 Die in Hyper-V Server verfügbaren Rollen

Der Hyper-V Server ist zudem auf die Server Core-Benutzeroberfläche beschränkt, enthält allerdings auch eine einfache skriptbasierte Konfigurationsbenutzeroberfläche, wie sie

Abbildung 3.4 zeigt, Hyper-V Server lässt sich remote über Server-Manager und Hyper-V-Manager verwalten, genau wie es bei jeder anderen Server Core-Installation möglich ist.

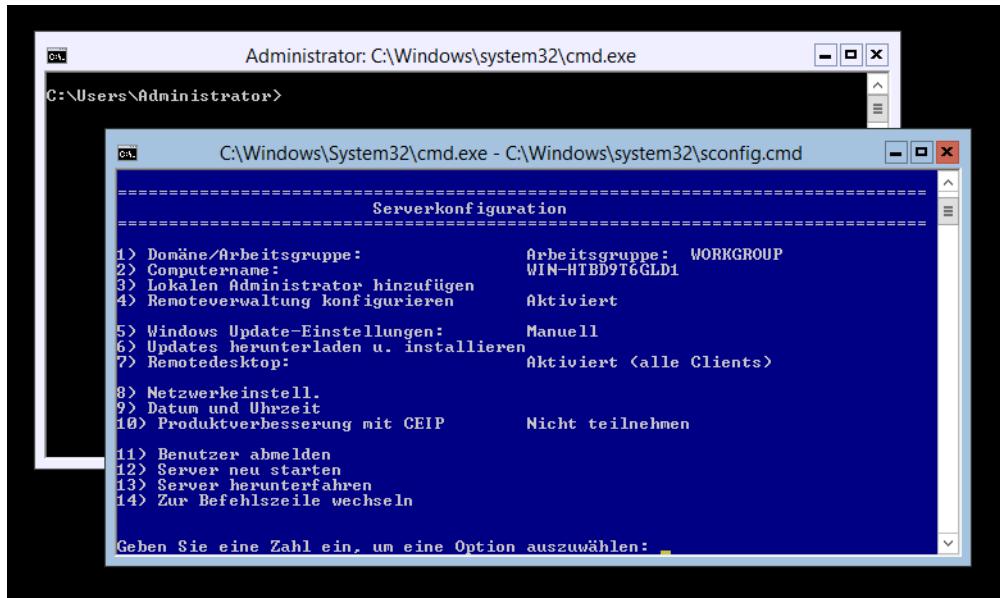


Abbildung 3.4 Die Server Core-Oberfläche in Hyper-V Server

Im Unterschied zu Windows Server 2012 ist Hyper-V Server ein kostenloses Produkt, das auf der Microsoft-Website zum Download bereitsteht. Allerdings umfasst Hyper-V Server keinerlei Lizenzen für virtuelle Instanzen. Alle Betriebssysteme, die Sie auf den erstellten virtuellen Computern installieren, müssen Sie selbst erwerben und lizenzieren.

Hyper-V installieren

Wenn Sie über die geeignete Hardware und die erforderlichen Lizenzen verfügen, können Sie wie jede andere Rolle auch die Hyper-V-Rolle über den Server-Manager zu Windows Server 2012 hinzufügen. Dabei installiert die Hyper-V-Rolle die Hypervisor-Software und im Falle einer vollständigen Installation von Windows Server 2012 mit grafischer Benutzeroberfläche auch die Verwaltungstools. Die Hyper-V-Manager-Konsole ist das wichtigste Werkzeug, um virtuelle Computer und deren Komponenten auf Hyper-V-Servern zu erstellen und zu verwalten. Hyper-V-Manager stellt Administratoren eine Liste aller virtuellen Computer auf Windows Server 2012-Systemen bereit und ermöglicht ihnen, die Umgebungen sowohl der Server als auch der einzelnen virtuellen Computer zu konfigurieren. Außerdem gibt es einen Satz von Hyper-V-Cmdlets für Windows PowerShell, sodass Sie die vollständige Kontrolle über virtuelle Computer mithilfe dieser Benutzeroberfläche ausüben können.

Microsoft empfiehlt, mit Hyper-V keine anderen Rollen zu installieren. Falls der physische Computer andere Rollen ausführen soll, ist es besser, sie in einem der virtuellen Computer zu installieren, die Sie per Hyper-V erstellt haben. Zudem sollten Sie Hyper-V auf einem

Computer mit der Option Server Core installieren. Dadurch minimieren Sie den Overhead, der auf der Partition aufzuwenden ist. Wie bei anderen Rollen schließt das Installieren von Hyper-V auf Server Core die Verwaltungstools aus. Diese müssen Sie separat als Feature auf einem anderen Computer installieren.

Damit Sie die Hyper-V-Rolle auf einem Windows Server 2012-Server installieren können, benötigen Sie die geeignete Hardware, die den folgenden Anforderungen genügen muss:

- 64-Bit-Prozessor mit hardwareunterstützter Virtualisierung, zum Beispiel Prozessoren mit einer Virtualisierungsoption wie der Intel Virtualization Technology (Intel VT) und der AMD Virtualization (AMD-V)-Technik
- Ein System-BIOS, das die Virtualisierungshardware unterstützt, auf der die Virtualisierungsfunktion aktiviert wurde
- Per Hardware forcierte Datenausführungsverhinderung (Data Execution Prevention, DEP), die Intel als *eXecute Disable (XD)* und AMD als *No eXecute (NX)* beschreibt. Diese Prozessortechnik teilt den Arbeitsspeicher in Bereiche auf, die entweder Prozessoranweisungen oder Daten speichern. Insbesondere müssen Sie bei Intel das XD-Bit und bei AMD das NX-Bit aktivieren.

Die Hyper-V-Rolle installieren Sie in folgenden Schritten:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorenrechten an. Das Fenster *Server-Manager* erscheint.
2. Im Menü *Verwalten* wählen Sie *Rollen und Features hinzufügen*. Daraufhin startet der Assistent zum Hinzufügen von Rollen und Features und zeigt die Seite *Vorbemerkungen* an.
3. Klicken Sie auf *Weiter*, um die Seite *Installationstyp auswählen* zu öffnen.
4. Lassen Sie die Option *Rollenbasierte oder featurebasierte Installation* ausgewählt und klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Zielserver auswählen*.
5. Wählen Sie den Server aus, auf dem Sie Hyper-V installieren möchten, und klicken Sie auf *Weiter*. Die Seite *Serverrollen auswählen* wird geöffnet.
6. Wählen Sie die Hyper-V-Rolle aus. Es erscheint das Dialogfeld *Sollen für Hyper-V erforderliche Features hinzugefügt werden?*
7. Klicken Sie auf *Features hinzufügen*, um die Abhängigkeiten zu bestätigen, und klicken Sie dann auf *Weiter*, um die Seite *Features auswählen* zu öffnen.
8. Klicken Sie auf *Weiter*. Es erscheint die Seite *Hyper-V*.
9. Klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Virtuelle Switches erstellen* (siehe Abbildung 3.5).

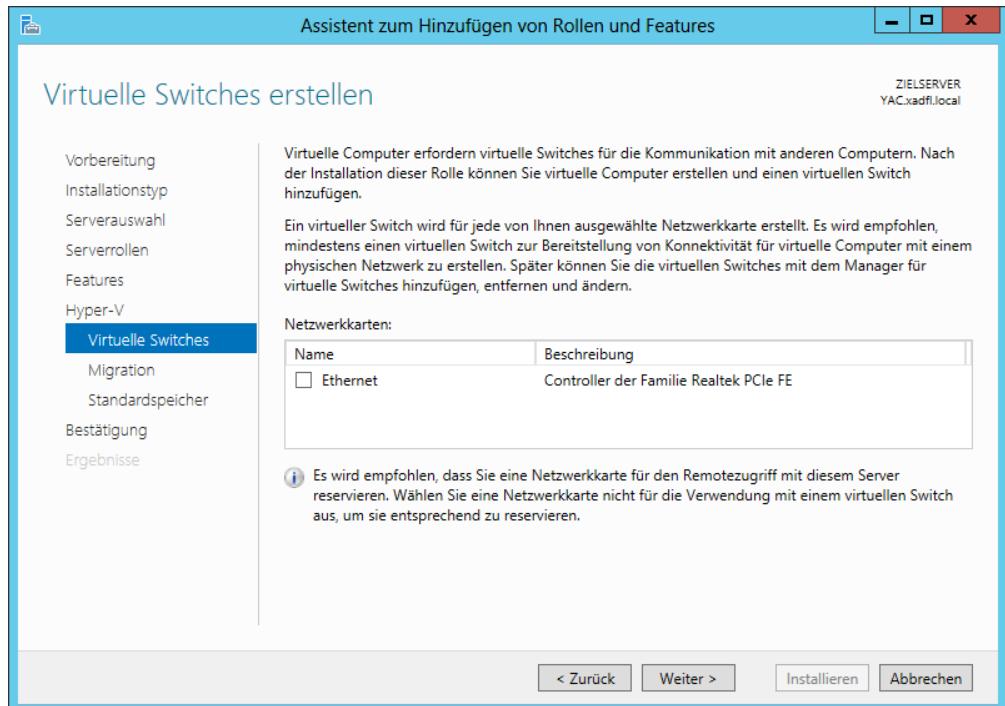


Abbildung 3.5 Die Seite *Virtuelle Switches erstellen* des Assistenten zum Hinzufügen von Rollen und Features

10. Aktivieren Sie das entsprechende Kontrollkästchen für einen Netzwerkadapter und klicken Sie auf *Weiter*. Die Seite *Migration eines virtuellen Computers* wird geöffnet (siehe Abbildung 3.6).
11. Klicken Sie auf *Weiter*, um die Seite *Standardspeicher* zu öffnen.
12. Geben Sie bei Bedarf Alternativen zu den Standardspeicherorten für VHD-Dateien und Konfigurationsdateien für den virtuellen Computer an und klicken Sie auf *Weiter*. Die Seite *Installationsauswahl bestätigen* wird geöffnet.
13. Klicken Sie auf *Installieren*. Der Assistent zeigt darauf die Seite *Installationsstatus* an, während die Rolle installiert wird.
14. Klicken Sie auf *Schließen*, um den Assistenten zu beenden.
15. Starten Sie den Server neu.

Durch die installierte Rolle wird die Windows Server 2012-Startprozedur geändert, damit der neu installierte Hypervisor die Systemhardware direkt ansprechen und dann darauf aufsetzend das Betriebssystem als primäre Partition laden kann.

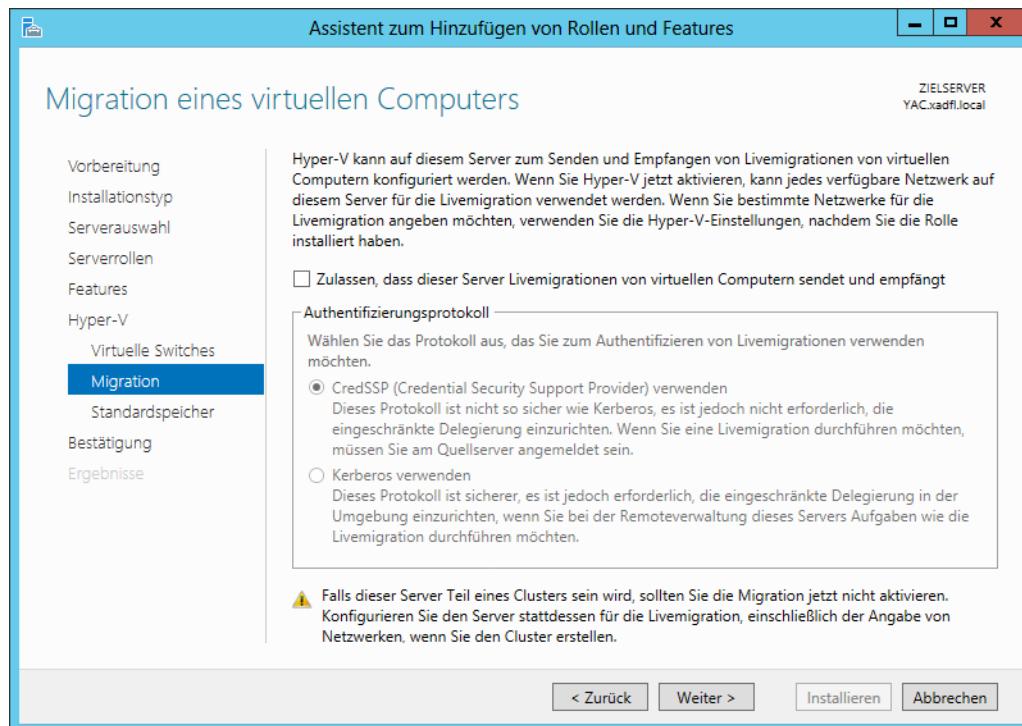


Abbildung 3.6 Die Seite *Migration eines virtuellen Computers* des Assistenten zum Hinzufügen von Rollen und Features



Hinweis Windows PowerShell

Die Hyper-V-Rolle können Sie auch mit dem Cmdlet `Install-WindowsFeature` installieren. Verwenden Sie dazu die folgende Syntax:

```
Install-WindowsFeature -Name Hyper-V  
-ComputerName <name> -IncludeManagementTools -Restart
```

Hyper-V-Manager verwenden

Wenn Sie die Hyper-V-Rolle installiert und den Computer neu gestartet haben, können Sie virtuelle Computer erstellen und Betriebssysteme darauf bereitstellen. Die Konsole *Hyper-V-Manager* ist das wichtigste grafische Werkzeug, mit dem Sie virtuelle Computer erstellen und verwalten. Erreichbar ist die Konsole über das Menü *Tools* im Server-Manager, wo Sie auch die anderen Server- und Active Directory-Verwaltungstools finden.

Wie mit den meisten Windows Server 2012-Verwaltungstools (einschließlich Server-Manager selbst) können Sie mit der Hyper-V-Manager-Konsole virtuelle Computer auf mehreren Servern erstellen und verwalten. Administratoren haben damit die vollständige Kontrolle über ihre Server von einem zentralen Standort aus.

Um Hyper-V-Manager auf einem Server auszuführen, der nicht über die Hyper-V-Rolle verfügt, müssen Sie das Feature *Hyper-V-Verwaltungstools* installieren. Diese Tools sind auch im Paket *Remoteserver-Verwaltungstools* für Windows 8 enthalten.

Nachdem Sie die Hyper-V-Manager-Konsole installiert und gestartet haben, können Sie der Anzeige Server hinzufügen. Klicken Sie dazu mit der rechten Maustaste auf den Knoten *Hyper-V-Manager* im linken Bereich und wählen Sie *Verbindung mit dem Server herstellen*. Daraufhin erscheint das Dialogfeld *Computer auswählen*, in dem Sie den Namen eines Hyper-V-Servers eingeben oder suchen können.

Die Hyper-V-Manager-Konsole listet für den ausgewählten Server alle virtuellen Computer zusammen mit Statusinformationen auf, wie Abbildung 3.7 zeigt.

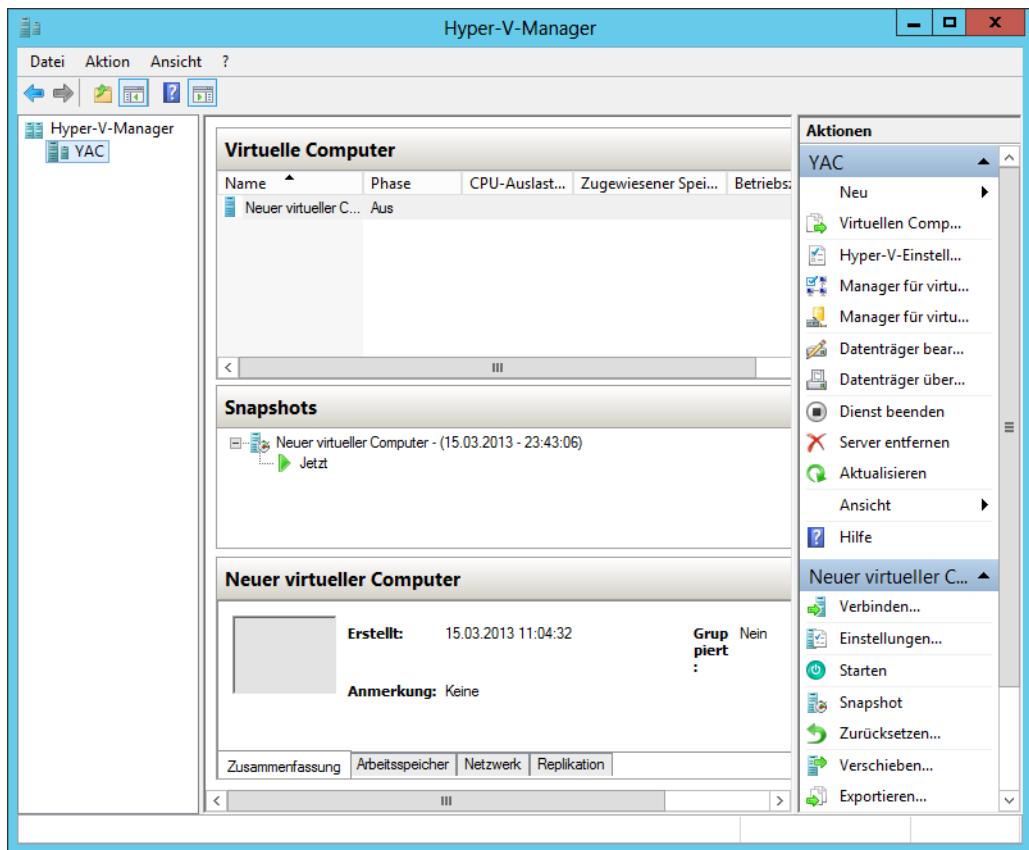


Abbildung 3.7 Die Hyper-V-Manager-Konsole

Einen virtuellen Computer erstellen

Haben Sie Hyper-V installiert und den Hyper-V-Manager konfiguriert, können Sie virtuelle Computer erstellen und darauf jeweils das Betriebssystem installieren. Mit Hyper-V-Manager richten Sie neue virtuelle Computer ein und definieren Hardwareressourcen, die das System

ihnen zuordnen soll. Abhängig von der physischen Hardware des Computers und den Einschränkungen des Gastbetriebssystems können Administratoren in den Einstellungen für einen bestimmten virtuellen Computer die Anzahl der Prozessoren und die Arbeitsspeicherkapazität angeben, virtuelle Netzwerkadapter installieren und virtuelle Datenträger nach verschiedenen Techniken einschließlich SANs (Storage Area Networks) einrichten.

In der Standardeinstellung speichert Hyper-V die Dateien, die die virtuellen Computer ausmachen, in den Ordner, die Sie während der Installation auf der Seite *Standardspeicher* angegeben haben. Jeder virtuelle Computer verwendet die folgenden Dateien:

- Eine Konfigurationsdatei für den virtuellen Computer im XML-Format (Erweiterung *.xml*) mit sämtlichen Konfigurationsinformationen des virtuellen Computers einschließlich aller seiner Einstellungen
- Eine oder mehrere VHD-Dateien (Erweiterung *.vhd* oder *.vhdx*), um das Gastbetriebssystem, Anwendungen und Daten für den virtuellen Computer zu speichern

Darüber hinaus kann ein virtueller Computer eine Datei für den gesicherten Zustand (Erweiterung *.vsv*) verwenden, falls der Computer in einen gesicherten Zustand versetzt worden ist.

Einen neuen virtuellen Computer erstellen Sie in folgenden Schritten:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Hyper-V-Manager*, um die *Hyper-V-Manager*-Konsole zu öffnen.
3. Wählen Sie im linken Bereich einen Hyper-V-Server aus.
4. Im Menü *Aktion* wählen Sie *Neu/Virtueller Computer*. Der Assistent für neue virtuelle Computer startet und zeigt die Seite *Vorbemerkungen* an.
5. Klicken Sie auf *Weiter*, um die Seite *Name und Pfad angeben* zu öffnen.
6. Geben Sie in das Textfeld *Name* einen Namen für den virtuellen Computer ein. Denken Sie dabei daran, dass das System diesen Namen auch heranzieht, um Dateien und Ordner für den virtuellen Computer zu erstellen. Möchten Sie die Dateien des virtuellen Computers an einem anderen als dem Standardspeicherort erstellen, aktivieren Sie das Kontrollkästchen *Virtuellen Computer an einem anderen Speicherort speichern* und geben im Textfeld *Pfad* einen alternativen Pfad ein. Klicken Sie dann auf *Weiter*. Damit gelangen Sie zur Seite *Speicher zuweisen*.



Weitere Informationen **Arbeitsspeicher**

Weitere Informationen, wie Hyper-V Hauptspeicher verwendet, finden Sie im Abschnitt »Speicher reservieren« später in diesem Kapitel.

- Geben Sie in das Textfeld *Startspeicher* die Größe des Hauptspeichers ein, den Sie für den virtuellen Computer vorgesehen haben, und klicken Sie auf *Weiter*. Es wird die Seite *Netzwerk konfigurieren* geöffnet, die in Abbildung 3.8 zu sehen ist.

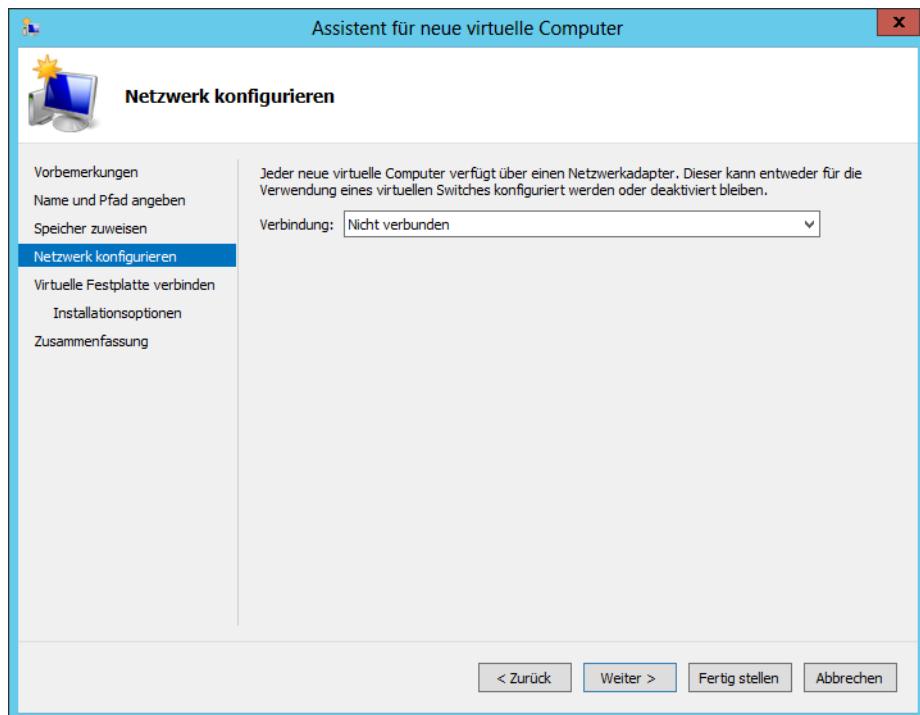


Abbildung 3.8 Die Seite *Netzwerk konfigurieren* des Assistenten für neue virtuelle Computer

- Wählen Sie in der Dropdownliste *Verbindung* einen virtuellen Switch aus und klicken Sie auf *Weiter*. Die Seite *Virtuelle Festplatte verbinden* wird geöffnet (siehe Abbildung 3.9).



Weitere Informationen Netzwerke

Weitere Informationen zu virtuellen Switches und virtuellen Computern im Netzwerk finden Sie in »Prüfungsziel 3.3: Virtuelle Netzwerke erstellen und konfigurieren« später in diesem Kapitel.

- Lassen Sie die Option *Virtuelle Festplatte erstellen* ausgewählt und geben Sie Werte für die folgenden Felder ein:
 - **Name** Legt den Dateinamen für die VHD fest, wobei das mit Windows Server 2012 eingeführte .vhdx-Format verwendet wird
 - **Pfad** Spezifiziert einen Speicherort für die VHD abweichend vom Standard, den Sie auf der Seite *Name und Pfad angeben* festgelegt haben
 - **Größe** Gibt die maximale Größe der VHD an

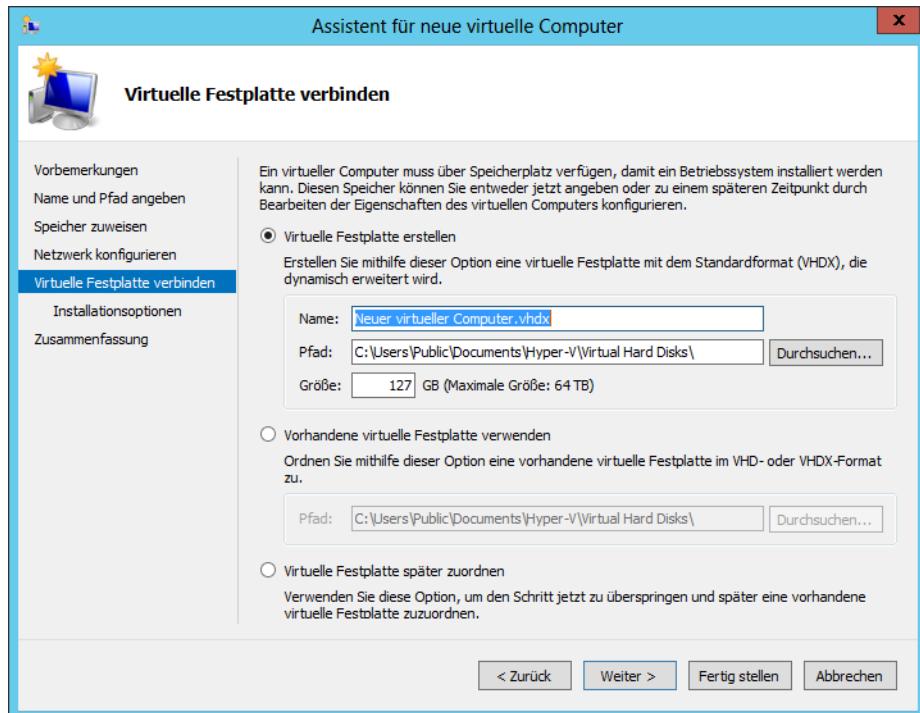


Abbildung 3.9 Die Seite *Virtuelle Festplatte verbinden* des Assistenten für neue virtuelle Computer



Weitere Informationen Speicher

Standardmäßig erstellt der Assistent eine zunächst kleine VHD-Datei, die dynamisch bis zu dem von Ihnen festgelegten Maximum erweitert wird. Weitere Informationen zum Hyper-V-Speicher enthält der Abschnitt »Prüfungsziel 3.2: Speicher des virtuellen Computers erstellen und konfigurieren« später in diesem Kapitel.

10. Klicken Sie auf *Weiter*. Die Seite *Installationsoptionen* wird geöffnet.
11. Lassen Sie die Option *Betriebssystem zu einem späteren Zeitpunkt installieren* ausgewählt und klicken Sie auf *Weiter*. Es erscheint die Seite *Abschließen des Assistenten für neue virtuelle Computer*.
12. Klicken Sie auf *Fertig stellen*. Der Assistent erstellt den neuen virtuellen Computer und fügt ihn zur Liste der virtuellen Computer in Hyper-V-Manager hinzu.

Der nach diesem Ablauf erstellte virtuelle Computer ist einem fabrikneuen Computer äquivalent. Er besitzt die gesamte (virtuelle) Hardware, die für den Betrieb erforderlich ist, jedoch keine Software.



Hinweis Windows PowerShell verwenden

Um mithilfe von Windows PowerShell einen neuen virtuellen Computer zu erstellen, verwenden Sie das Cmdlet `New-VM` mit der folgenden grundlegenden Syntax:

```
New-VM -Name "VM name" -MemoryStartupBytes <memory>
```

```
-NewVHDSizeBytes <Datenträgergröße>
```

Zum Beispiel erstellt der folgende Befehl einen neuen virtuellen Computer namens *ServerA* mit 1 GB Arbeitsspeicher und einem neuen 60-GB-VHD-Laufwerk:

```
New-VM -Name "ServerA" -MemoryStartupBytes 1GB
```

```
-NewVHDSizeBytes 60GB
```

Für das Cmdlet `New-VM` gibt es viele weitere Parameter, die Sie über das Cmdlet `Get-Help` erkunden können.

Bei jedem virtuellen Computer auf einem Hyper-V-Server spezifiziert eine Auflistung von Einstellungen die Hardwareressourcen im Computer und die Konfigurationseinstellungen, die diese Ressourcen steuern. Die entsprechenden Werte können Sie über die Seite *Einstellungen* für den jeweiligen virtuellen Computer verwalten und ändern.

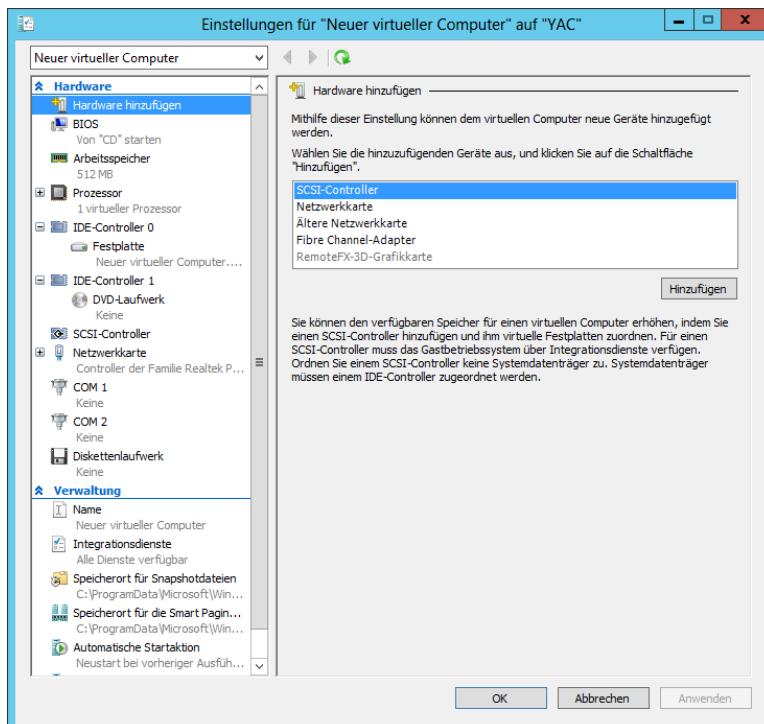


Abbildung 3.10 Das Dialogfeld *Einstellungen* für einen virtuellen Computer

Wenn Sie einen virtuellen Computer aus der Liste im Hyper-V-Manager auswählen, erscheint eine Reihe von Symbolen im Bereich *Aktionen*. Durch Klicken auf das Symbol *Einstellungen* wird das Dialogfeld *Einstellungen* geöffnet (siehe Abbildung 3.10), das die vorrangige Konfigurationsoberfläche für diesen virtuellen Computer darstellt. Hier können Sie alle Einstellungen ändern, die der Assistent für neue virtuelle Computer für Sie konfiguriert hat.

Ein Betriebssystem installieren

Wenn Sie einen virtuellen Computer erstellt haben, können Sie darauf ein Betriebssystem installieren, genau wie bei einem fabrikneuen Computer. Hyper-V in Windows Server 2012 unterstützt die folgenden Betriebssysteme, die sich auf virtuellen Computern installieren lassen:

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Home Server 2011
- Windows Small Business Server 2011
- Windows Server 2003 R2
- Windows Server 2003 SP2
- Windows 8
- Windows 7 Enterprise und Ultimate
- Windows Vista Business, Enterprise und Ultimate SP2
- Windows XP Professional SP3
- Windows XP x64 Professional SP2
- CentOS 6.0 – 6.2
- Red Hat Enterprise Linux 6.0 – 6.2
- SUSE Linux Enterprise Server 11 SP2



Hinweis Gastbetriebssysteme

Dies ist die offizielle Liste von unterstützten Gastbetriebssystemen der RTM-Version. Andere Betriebssysteme können durchaus funktionieren, sind aber nicht umfassend getestet worden.

Eine Softwareinstallation auf virtuellen Computern hat unter anderem den Vorteil, dass es mehrere Möglichkeiten gibt, auf die Installationsdateien zuzugreifen. Ein virtueller Computer verfügt standardmäßig über ein DVD-Laufwerk, das selbst physisch oder virtuell sein kann.

Wenn Sie im Dialogfeld *Einstellungen* eines virtuellen Computers das DVD-Laufwerk in der Hardwareliste auswählen, erscheint die in Abbildung 3.11 gezeigte Benutzeroberfläche. Im Abschnitt *Medien* können Sie eine der folgenden Optionen für das Laufwerk auswählen:

- **Keine** Gleichbedeutend mit einem Laufwerk, in das kein Datenträger eingelegt ist
- **Abbilddatei** Verweist auf eine Festplatten-Imagedatei mit der Erweiterung *.iso*, die auf einem Laufwerk des Hostcomputers oder auf einem freigegebenen Netzwerklaufwerk gespeichert ist
- **Physisches CD/DVD-Laufwerk** Verknüpft das virtuelle DVD-Laufwerk mit einem physischen DVD-Laufwerk im Hostcomputer

Die Möglichkeit, eine Abbilddatei (Imagedatei) für ein virtuelles DVD-Laufwerk bereitzustellen, ist insbesondere für Administratoren nützlich, die Betriebssystemdateien als Festplattenimages herunterladen. Nachdem Sie einen Installationsdatenträger – entweder physisch oder virtuell – bereitgestellt haben, können Sie im Bereich *Aktionen* auf *Starten* klicken, was gleichbedeutend mit dem Einschalten des virtuellen Computers ist.

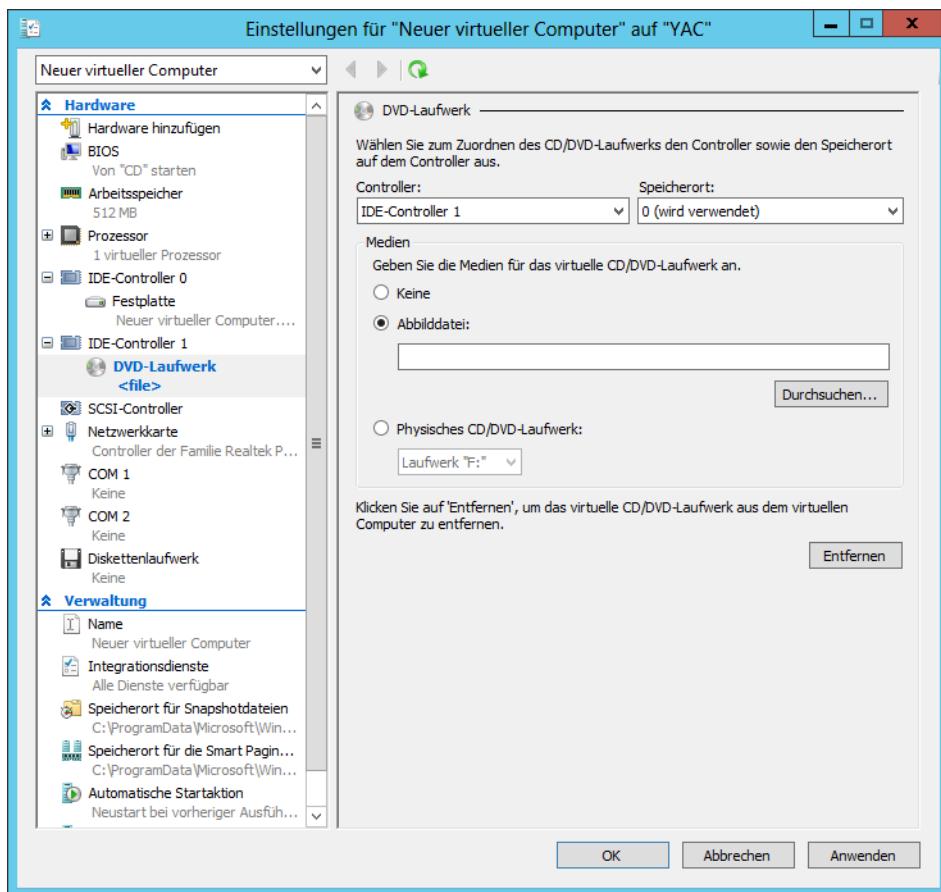


Abbildung 3.11 Einstellungen für das DVD-Laufwerk eines virtuellen Computers

Wenn Sie einen virtuellen Computer starten, aktivieren Sie im Hyper-V-Manager die Miniaturansicht, die den Inhalt des Computerbildschirms anzeigt. Um die Aktivität des

virtuellen Computers in voller Größe darzustellen, klicken Sie im Bereich *Aktionen* auf *Verbinden* und öffnen damit ein neues Fenster für den virtuellen Computer. Dann können Sie über dieses Fenster mit dem virtuellen Computer interagieren, genauso als würden Sie an einer physischen Konsole des Computers sitzen.

Wenn der virtuelle Computer von der bereitgestellten Festplatte bootet, läuft die Betriebssysteminstallation genauso ab, als würden Sie einen physischen Computer verwenden. Während der Installation können Sie mit dem VHD-Laufwerk genauso wie mit einem physischen Laufwerk arbeiten, d.h. Partitionen verschiedener Größen erstellen und eine Partition für das Betriebssystem auswählen. Ist die Installation abgeschlossen, startet der virtuelle Computer neu. Dann können Sie sich an diesem Computer anmelden und ihn in gewohnter Weise verwenden.

Integrationsdienste konfigurieren

In manchen Fällen funktionieren bestimmte Hyper-V-Gastbetriebssystemfeatures mit den betriebssystemeigenen Gerätetreibern nicht ordnungsgemäß. Deshalb bringt Hyper-V mit den *Integrationsdiensten* ein Softwarepaket mit, das Sie auf Ihren virtuellen Computern aus Kompatibilitätsgründen installieren können.

Das Paket *Integrationsdienste* stellt unter anderem folgende Funktionen bereit:

- **Herunterfahren des Betriebssystems** Ermöglicht es der Hyper-V-Manager-Konsole, ein Gastbetriebssystem kontrolliert herunterzufahren, sodass sich ein Administrator nicht erst anmelden und das System manuell herunterfahren muss
- **Zeitsynchronisierung** Ermöglicht Hyper-V, die Betriebssystemtakte in übergeordneten und untergeordneten Partitionen zu synchronisieren
- **Datenaustausch** Ermöglicht es den Windows-Betriebssystemen in den übergeordneten und untergeordneten Partitionen, Informationen auszutauschen, beispielsweise Betriebssystem-Versionsinformationen und vollständig qualifizierte Domänennamen
- **Takt** Implementiert einen Dienst, in dem die übergeordnete Partition regelmäßige Taktsignale an die untergeordneten Partitionen sendet, von denen eine Reaktion in gleicher Weise erwartet wird. Wenn eine untergeordnete Partition nicht antwortet, weist das darauf hin, dass das Gastbetriebssystem eingefroren ist oder Fehlfunktionen zeigt.
- **Sicherung** Ermöglicht eine Sicherung der virtuellen Windows-Computer mithilfe der Volumeschattenkopie-Dienste

In den Betriebssystemen Windows Server 2012 und Windows 8 sind die neuesten Integrationsdienste bereits enthalten und es ist nicht erforderlich, das Paket auf virtuellen Computern, die diese Betriebssysteme ausführen, als Gast zu installieren. Ältere Windows-Versionen besitzen frühere Versionen des Pakets Integrationsdienste, die jedoch aktualisiert werden müssen, und einige Windows-Versionen verfügen überhaupt nicht über das Paket.



Hinweis Linux

Für Linux-Gastbetriebssysteme müssen Sie das neueste Release der Linux Integration Services Version 3.2 für Hyper-V vom Microsoft Download Center herunterladen. Die neueste Version 3.4 (Anfang 2013) steht unter <http://www.microsoft.com/de-de/download/details.aspx?id=28188> zum Download bereit.

Auf einem Windows-Gastbetriebssystem aktualisieren Sie die Integrationsdienste wie folgt:

1. Melden Sie sich auf dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Hyper-V-Manager*. Daraufhin startet die Hyper-V-Manager-Konsole.
3. Wählen Sie im linken Bereich einen Hyper-V-Server aus.
4. Starten Sie im Bereich *Aktionen* den virtuellen Computer, auf dem Sie die Integrationsdienste installieren möchten, und klicken Sie auf *Verbinden*. Es erscheint ein Fenster *Verbindung mit virtuellen Computern*.
5. Wählen Sie im Fenster *Verbindung mit virtuellen Computern* im Menü *Aktion* den Befehl *Installationsdatenträger für Integrationsdienste einlegen*. Hyper-V stellt ein Image des Integrationsdienste-Datenträgers auf einem virtuellen Festplattenlaufwerk bereit und es erscheint ein Fenster *Automatische Wiedergabe*.
6. Klicken Sie auf *Hyper-V-Integrationsdienste installieren*. Ein Meldungsfeld zeigt daraufhin die Frage an, ob Sie die vorhandene Installation aktualisieren möchten.
7. Klicken Sie auf *OK*. Das System installiert das Paket und fordert Sie auf, den Computer neu zu starten.
8. Klicken Sie auf *Ja*, um den Computer neu zu starten.

Wenn Sie die Integrationsdienste installiert bzw. aktualisiert haben, können Sie die einzelnen Funktionen aktivieren oder deaktivieren. Öffnen Sie dazu das Dialogfeld *Einstellungen* für den virtuellen Computer und wählen Sie die Seite *Integrationsdienste* aus, wie Abbildung 3.12 zeigt.

Nun sind Sie bereit, den virtuellen Computer zu konfigurieren und zu verwalten, genauso als würden Sie an einem physischen Server arbeiten. Unter anderem können Sie das Netzwerk konfigurieren, den Remotedesktop aktivieren, die gewünschten Rollen und Features laden und Anwendungen installieren.

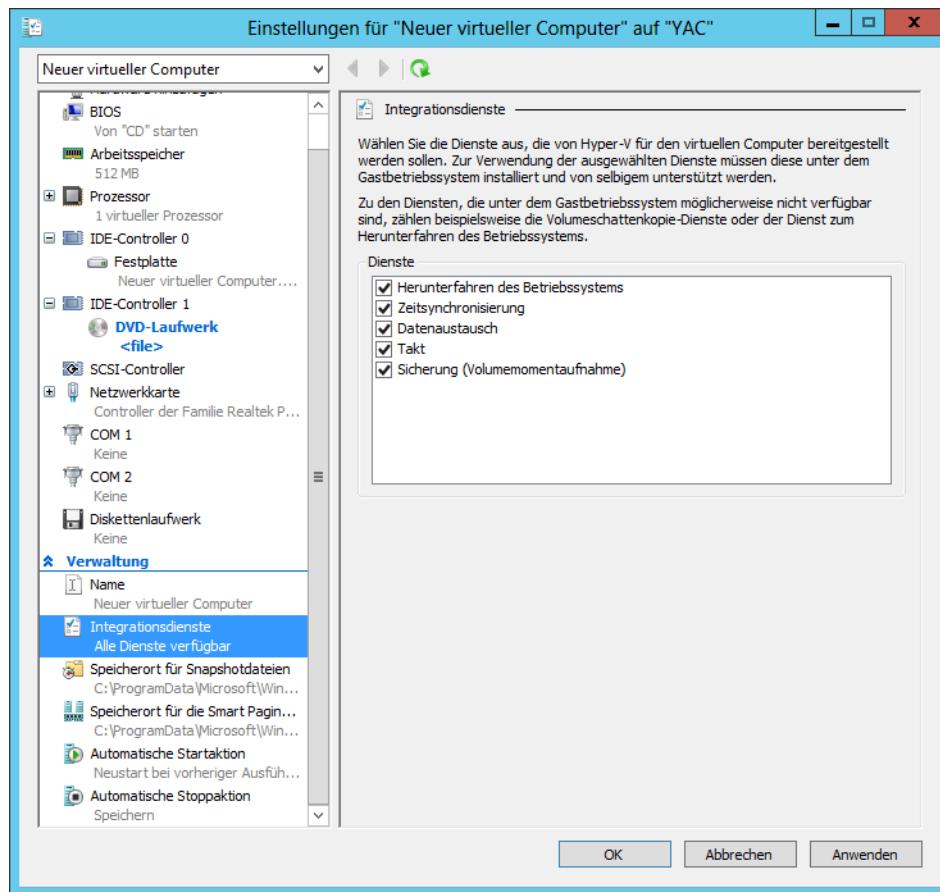


Abbildung 3.12 Einstellungen der Integrationsdienste für einen virtuellen Computer

Speicher reservieren

Mithilfe von dynamischem Speicher kann Hyper-V die Größe des RAMs anpassen, der für virtuelle Computer je nach ihren laufenden Anforderungen reserviert wird. Manche Computerkomponenten lassen sich virtualisieren. So können Sie mit einem Teil des Datenträgerplatzes ein virtuelles Festplattenlaufwerk erstellen oder eine Imagedatei verwenden und ein virtuelles DVD-Laufwerk einrichten. Außerdem ist es möglich, virtuelle Netzwerkadapter und andere Komponenten zu erstellen, die in einem virtuellen Computer wie die echte (physische) Komponente erscheinen. Anders liegen die Dinge jedoch beim Systemspeicher. Für Arbeitsspeicher gibt es keinen Ersatz, sodass Hyper-V lediglich den im Computer installierten physischen Arbeitsspeicher auf die verschiedenen virtuellen Computer aufteilen kann.

Wenn Sie einen virtuellen Computer mit dem Assistenten für neue virtuelle Computer einrichten, legen Sie auf der Seite *Speicher zuweisen* fest, wie viel Arbeitsspeicher der virtuelle Computer erhalten soll. Es liegt auf der Hand, dass die nutzbare Speicherkapazität vom physischen Arbeitsspeicher abhängt, der im Computer installiert ist.

Nachdem Sie den virtuellen Computer erstellt haben, können Sie die ihm zugeteilte Speicherkapazität anpassen. Dazu fahren Sie den virtuellen Computer herunter, öffnen dessen Dialogfeld *Einstellungen* und ändern auf der Seite *Speicher* den Wert für *Arbeitsspeicher beim Start*, wie Abbildung 3.13 zeigt. Somit haben Sie auch die Möglichkeit, mit verschiedenen Speichergrößen zu experimentieren und das optimale Performanceniveau für das System festzulegen.

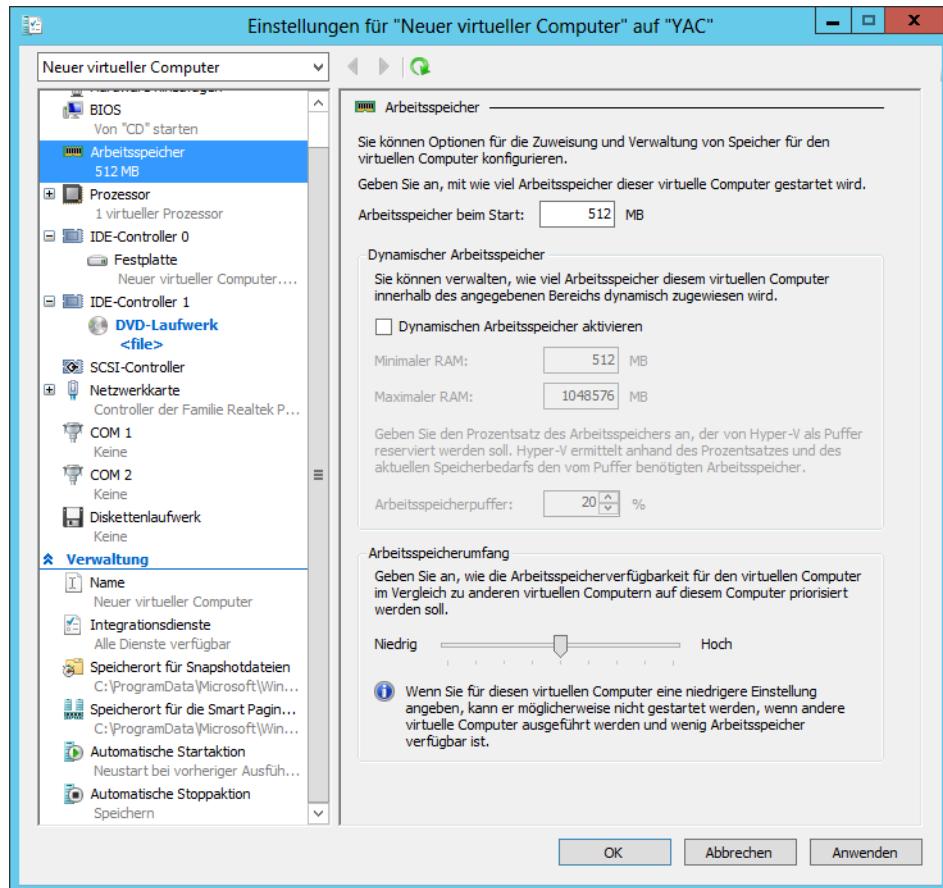


Abbildung 3.13 Speichereinstellungen für einen virtuellen Computer

Dynamischen Arbeitsspeicher verwenden

In den ersten Versionen von Hyper-V ließ sich die Speicherreservierung nur ändern, wenn der virtuelle Computer heruntergefahren wurde. Dagegen können Sie in der Windows Server 2012-Version auf das Feature *Dynamischer Arbeitsspeicher* zurückgreifen, um dem virtuellen Computer automatisch Speicher aus einem gemeinsamen Pool neu zuzuordnen, falls sich der Speicherbedarf des virtuellen Computers ändern sollte. Ist zum Beispiel ein virtualisierter Server mit starkem Clientdatenverkehr konfrontiert, kann Hyper-V die Speicherkapazität

erhöhen, die für das System reserviert ist, und sie wieder verringern, wenn der Datenverkehr zurückgeht.

Um dynamischen Speicher zu verwenden, müssen Sie ihn aktivieren. Schalten Sie dazu im Dialogfeld *Einstellungen* des virtuellen Computers auf der Seite *Speicher* das Kontrollkästchen *Dynamischen Arbeitsspeicher aktivieren* ein und konfigurieren Sie dann die folgenden Einstellungen:

- **Arbeitsspeicher beim Start** Gibt die Menge des Speichers an, den Sie dem virtuellen Computer beim Starten reservieren möchten. Wenn Sie dynamischen Speicher verwenden, können Sie hier die minimale Größe angeben, die für den Startvorgang des Systems erforderlich ist.
- **Minimaler RAM** Gibt die kleinste Speichermenge an, die der virtuelle Computer zu jedem Zeitpunkt verwenden kann. Betriebssysteme benötigen unter Umständen für den Startvorgang mehr Speicher als für die Ausführung, sodass dieser Wert kleiner als der Wert für *Arbeitsspeicher beim Start* sein kann.
- **Maximaler RAM** Gibt die größte Speichermenge an, die der virtuelle Computer jederzeit verwenden darf. Der Bereich für diesen Wert kann sich von einer Untergrenze wie für *Arbeitsspeicher beim Start* festgelegt bis zu 64 GB erstrecken.
- **Arbeitsspeicherpuffer** Gibt einen Prozentwert an, mit dem Hyper-V berechnet, wie viel Speicher für den virtuellen Computer zu reservieren ist. Dieser Wert ergibt sich aus der tatsächlichen Nutzung des Speichers auf Basis der Leistungsindikatoren. Ist zum Beispiel der Wert für den Arbeitsspeicherpuffer auf 20 Prozent gesetzt, erhält ein virtueller Computer, der mit Anwendungen und Betriebssystem 1 GB Speicher benötigt, eine dynamische Reservierung von 1,2 GB.
- **Arbeitsspeicherumfang** Gibt einen relativen Wert für die Priorität dieses virtuellen Computers im Vergleich zu anderen virtuellen Computern auf demselben Computer an. Wenn der physische Arbeitsspeicher im Computer nicht ausreicht, um die volle Kapazität für den Arbeitsspeicherpuffer jedes virtuellen Computers zuzuordnen, erhalten die virtuellen Computer mit den größeren Werten für den Arbeitsspeicherumfang höhere Prioritäten.



Hinweis RAM

Sie können jederzeit den Wert für *Minimaler RAM* verringern, den Wert für *Maximaler RAM* erhöhen oder die Werte für *Arbeitsspeicherpuffer* und *Speichergewichtung* ändern. Um aber dynamischen Speicher zu aktivieren bzw. zu deaktivieren, müssen Sie den virtuellen Computer herunterfahren.

Neben der Konfiguration der Einstellungen für den virtuellen Computer ist es für die Verwendung von dynamischem Speicher erforderlich, dass der virtuelle Gastcomputer mindestens Windows Vista oder mindestens Windows Server 2003 SP2 ausführt und die Windows Server 2012-Integrationsdienste installiert sind.



Hinweis Windows PowerShell

Die Speichereinstellungen für einen virtuellen Computer lassen sich auch mit dem Cmdlet Set-VMMemory entsprechend der folgenden grundlegenden Syntax konfigurieren:

```
Set-VMMemory <VM name> -DynamicMemoryEnabled $true  
-MinimumBytes <memory> -StartupBytes <memory>  
-MaximumBytes <memory> -Priority <value> -Buffer <percentage>
```

Zum Beispiel können Sie mit dem folgenden Befehl die Speichereinstellungen für den virtuellen Computer *ServerA* konfigurieren, dynamischen Speicher aktivieren und die Werte für alle dafür relevanten Einstellungen festlegen:

```
Set-VMMemory ServerA -DynamicMemoryEnabled $true  
-MinimumBytes 64MB
```

Smart Paging konfigurieren

Dynamischer Arbeitsspeicher wurde bereits mit Hyper-V in Windows Server 2008 R2 eingeführt, doch Windows Server 2012 verbessert das Konzept mit der zusätzlichen Einstellung *Minimaler RAM*. Dadurch ist Hyper-V in der Lage, den von einem virtuellen Computer verwendeten Arbeitsspeicher auf ein Niveau zu verringern, das für den Start des Systems genügt, wodurch der frei werdende Speicher für andere Zwecke zur Verfügung steht.

Bei Werten für *Minimaler RAM*, die geringer sind als die Werte für *Arbeitsspeicher beim Start*, kann das Problem auftreten, dass der physische Speicher aufgebraucht wird, wenn zu viele virtuelle Computer gleichzeitig mit den Werten für *Minimaler RAM* arbeiten. Sollte ein virtueller Computer in einem derartigen Fall einen Neustart durchführen müssen, kann er den Startvorgang nicht abschließen, da ihm nicht genügend Speicher zur Verfügung steht, um seine Speicherreservierung vom Wert *Minimaler RAM* auf seinen Wert *Arbeitsspeicher beim Start* zu erhöhen.

Für derartige Fälle ist in Hyper-V das Feature *Smart Paging* vorgesehen. Wenn ein virtueller Computer neu starten muss und es nicht mehr genügend Speicher gibt, um die Speicherreservierung auf den Wert *Arbeitsspeicher beim Start* zu erhöhen, gleicht das System die Differenz mithilfe von Festplattenplatz aus und lagert Speicherinhalte auf der Festplatte aus.

Da Festplattenzugriffe länger dauern als Speicherzugriffe, bedeutet Smart Paging eine ernsthafte Leistungseinbuße. Allerdings benötigt der virtuelle Computer die Auslagerung nur während des Neustarts und kehrt dann zu seiner minimalen RAM-Reservierung zurück.

Hyper-V setzt Smart Paging unter besonderen Bedingungen ein: wenn ein virtueller Computer neu starten muss, es keinen freien Arbeitsspeicher gibt und keine anderen Möglichkeiten bestehen, den benötigten Arbeitsspeicher freizugeben.

Einen Speicherort für die Auslagerungsdatei können Sie im Dialogfeld *Einstellungen* des virtuellen Computers auf der Seite *Speicherort für die Smart Paging-Datei* auswählen.

Ressourcenmessung konfigurieren

Die Ressourcenmessung ist ein neues Windows PowerShell-basiertes Feature in Hyper-V von Windows Server 2012. Administratoren haben damit die Möglichkeit, die Nutzung von virtuellen Computern nach verschiedenen Kriterien zu dokumentieren. Es gibt eine Reihe von Gründen, warum Organisationen die Nutzung von virtuellen Computern verfolgen möchten. Bei großen Unternehmen kann dies eine Frage der internen Abrechnung und die Kontrolle der laufenden Ausgaben sein, wie zum Beispiel für die WAN (Wide Area Network)-Bandbreite. Bei Serviceprovidern ist es möglicherweise erforderlich, Kunden basierend auf den von ihnen genutzten Ressourcen von virtuellen Computern abzurechnen.

Ressourcenmessung stützt sich auf Windows PowerShell-Cmdlets, um unter anderem folgende Leistungskennziffern für einzelne virtuelle Computer zu verfolgen:

- CPU-Nutzung
- Minimale, maximale und durchschnittliche Arbeitsspeichernutzung
- Nutzung von Festplattenplatz
- Eingehender und ausgehender Netzwerkdatenverkehr

Die statistischen Daten bei der Ressourcenmessung bleiben konsistent, selbst wenn Sie virtuelle Computer mithilfe von Livemigration zwischen Hostsystemen übertragen oder VHD-Dateien zwischen virtuellen Computern verschieben.

Eine Ressourcenmessung setzt voraus, dass Sie sie zuerst für den konkreten virtuellen Computer aktivieren, den Sie überwachen möchten. Hierzu führen Sie das Cmdlet `Enable-VMResourceMetering` mit der folgenden Syntax aus:

```
Enable-VMResourceMetering -VMName <name>
```

Nachdem Sie die Messung aktiviert haben, können Sie jederzeit mit dem Cmdlet `Measure-VM` einen statistischen Bericht anzeigen. Die Syntax lautet:

```
Measure-VM -VMName <name>
```

Neben der Ressourcenmessung für komplett virtuelle Computer können Administratoren auch mithilfe von Ressourcenpools spezifische Komponenten von virtuellen Computern überwachen, beispielsweise Prozessoren, Arbeitsspeicher, Netzwerkadapter und VHD-Dateien. Einen Ressourcenpool erstellen Sie mit dem Cmdlet `New-VMResourcePool` und aktivieren dann die Messung für den Pool mithilfe von `Enable-VMResourceMetering`.

Mit Techniken wie Pipelining können Administratoren über die Cmdlets für die Ressourcenmessung Daten zur Performance von virtuellen Computern erfassen und sie in Anwendungen oder Datendateien exportieren.

Prüfungszielzusammenfassung

- Virtualisierung bildet eine zusätzliche Abstraktionsebene zwischen der eigentlichen physischen Hardware und dem System, das die Hardware verwendet. Anstatt den Server direkt auf die Hardware des Computers zugreifen zu lassen, erzeugt eine

zwischengeschaltete Komponente, der Hypervisor, eine Umgebung für virtuelle Computer, und das Serverbetriebssystem läuft in dieser Umgebung.

- Durch Virtualisierung werden mehrere Instanzen eines Betriebssystems, die sogenannten virtuellen Computer, auf einem einzelnen Computer bereitgestellt und verwaltet
- Microsoft Hyper-V ist ein Hypervisor-basiertes Virtualisierungssystem für x64-Computer, das mit Windows Server 2008 eingeführt wurde. Der Hypervisor wird zwischen der Hardware und dem Betriebssystem installiert. Er verkörpert die Hauptkomponente, die die virtuellen Computer verwaltet.
- Aus lizenzerrechtlichen Gründen bezeichnet Microsoft jeden virtuellen Computer, den Sie auf einem Hyper-V-Server erstellen, als virtuelle Instanz. Jede Windows Server 2012-Version beinhaltet eine Anzahl von virtuellen Instanzen. Um zusätzliche Instanzen zu erstellen, müssen Sie entsprechende Lizenzen erwerben.
- Im Sinne eines schlanken Systems mit minimalem Overhead enthält Hyper-V Server nur den Windows-Hypervisor, das Windows Server-Treibermodell und die Virtualisierungs-komponenten

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Aussagen zu den Virtualisierungstypen 1 und 2 sind richtig? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Bei Typ-1-Virtualisierung setzt der Hypervisor auf einem Hostbetriebssystem auf.
 - B. Bei Typ-1-Virtualisierung läuft der Hypervisor direkt auf der Computerhardware.
 - C. Bei Typ-2-Virtualisierung setzt der Hypervisor auf einem Hostbetriebssystem auf.
 - D. Bei Typ-2-Virtualisierung läuft der Hypervisor direkt auf der Computerhardware.
2. Welcher der folgenden Typen der Servervirtualisierung bietet die beste Performance für stark frequentierte Server in Produktionsumgebungen?
 - A. Typ-1-Virtualisierung
 - B. Typ-2-Virtualisierung
 - C. Präsentationsvirtualisierung
 - D. RemoteApp

3. Welches der folgenden Microsoft-Betriebssysteme enthält eine Lizenz, die Ihnen erlaubt, eine unbegrenzte Anzahl von virtuellen Instanzen zu erstellen?
 - A. Hyper-V Server
 - B. Windows Server 2012 Datacenter
 - C. Windows Server 2012 Standard
 - D. Windows Server 2012 Foundation
4. Welche der folgenden Hyper-V-Funktionen ermöglichen es einem virtuellen Computer, mit einem Wert für Minimaler RAM, der geringer als der Wert *Arbeitsspeicher beim Start* ist, zu funktionieren? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Smart Paging
 - B. Dynamischer Arbeitsspeicher
 - C. Speichergewichtung
 - D. Integrationsdienste
5. In welches Systemelement wird die Instanz des Betriebssystems, auf dem Sie die Hyper-V-Rolle installiert haben, konvertiert, wenn Sie die Hyper-V-Rolle auf einem Windows Server 2012 installieren?
 - A. Den Hypervisor
 - B. Den Monitordienst für virtuelle Computer
 - C. Die übergeordnete Partition
 - D. Eine untergeordnete Partition



Gedankenexperiment Wenden Sie im folgenden Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Alice hat einen Windows Server 2012-Computer mit 8 GB installiertem Hauptspeicher als Hyper-V-Server konfiguriert. Nachdem sie acht virtuelle Computer mit dem Assistenten für neue virtuelle Computer erstellt und jeweils 1024 MB als Wert für *RAM bei Start* festgelegt hat, erweist es sich als problematisch, alle acht virtuellen Computer hochzufahren. Welche Einstellungen kann Alice modifizieren, um das Problem zu lösen, ohne den Wert für *RAM bei Start* zu ändern?

Prüfungsziel 3.2: Speicher des virtuellen Computers erstellen und konfigurieren

Bei einem virtuellen Computer, den Sie in Windows Server 2012-Hyper-V erstellen, emulieren Sie sämtliche Standardkomponenten, die ein physischer Computer normalerweise enthält. Wie Prüfungsziel 3.1 erläutert hat, nehmen Sie beim Virtualisieren von Arbeitsspeicher einen Teil des physischen Speichers im Computer und weisen ihn einem virtuellen Computer zu. Das Gleiche gilt für Festplattenplatz. Hyper-V nutzt ein spezialisiertes VHD-Format, um einen Teil des Platzes auf einem physischen Datenträger zu packen und ihn für den virtuellen Computer wie ein physisches Festplattenlaufwerk erscheinen zu lassen.

Wenn Sie einen neuen virtuellen Computer in Hyper-V mit dem Assistenten für neue virtuelle Computer einrichten, erzeugt der Assistent ein virtuelles Speichersubsystem, das aus zwei IDE-Controllern und einem SCSI-Controller besteht. Der IDE-Controller hostet das Systemlaufwerk und das DVD-Laufwerk des virtuellen Computers. Wie ihre physischen Pendants kann jeder IDE-Controller zwei Geräte hosten, sodass Sie zwei zusätzliche virtuelle Laufwerke erstellen und sie dem System hinzufügen können.

In der Standardkonfiguration des virtuellen Computers ist der SCSI-Controller nicht belegt. Diesem Controller können Sie also neu erstellte Laufwerke hinzufügen, um den virtuellen Computer mit zusätzlichem Speicherplatz zu versorgen. Außerdem lassen sich weitere SCSI-Controller einrichten, denen Sie dann Laufwerke hinzufügen können. Durch diese Möglichkeiten lassen sich mit Hyper-V virtuelle Speichersubsysteme konstruieren, die praktisch jede vorstellbare physische Speicherlösung nachbilden.

Dieses Prüfungsziel zeigt, wie Sie

- VHDs und VHDX erstellen
 - verschiedenartige Laufwerke konfigurieren
 - VHDs modifizieren
 - Pass-Through-Datenträger konfigurieren
 - Snapshots verwalten
 - einen virtuellen Fibre Channel-Adapter implementieren
-

Formate virtueller Festplatten

Windows Server 2012 Hyper-V unterstützt die ursprüngliche VHD-Festplatten-Imagedatei und das neue VHDX-Format. Das ursprüngliche VHD-Format stammt von der Firma Connectix, die es für das eigene Produkt Virtual PC entwickelt hat. Später hat Microsoft das Produkt erworben und das VHD-Format für alle darauffolgenden eigenen Virtualisierungsprodukte eingesetzt, Hyper-V eingeschlossen. Es gibt die folgenden drei Typen von VHD-Dateien:

- **Festes Festplattenimage** Eine Imagedatei festgelegter Größe, bei der bereits beim Anlegen der Datei der gesamte Festplattenplatz reserviert wird, der für das Erstellen des Images erforderlich ist. Feste Festplattenimages sind hinsichtlich der Speicherplatznutzung verschwenderisch, da sie große Mengen leeren Platz enthalten können. Vom Standpunkt der Verarbeitung aus gesehen sind sie aber auch effizient, weil es keinen Overhead wegen dynamischer Erweiterung gibt.
- **Dynamisches Festplattenimage** Eine Imagedatei mit einer festgelegten Maximalgröße. Die Datei ist anfangs klein und wird bei Bedarf erweitert, um sich den Daten anzupassen, die das System in das Image schreibt.
- **Differenzierendes Festplattenimage** Eine untergeordnete Imagedatei, die mit einer bestimmten übergeordneten Imagedatei verbunden ist. Das System schreibt alle Änderungen an den Daten in der übergeordneten Imagedatei in das untergeordnete Image, um den Festplattenplatz zu verwalten oder zu einem späteren Zeitpunkt einen Rollback zu ermöglichen.

VHD-Images sind auf eine maximale Größe von 2 TB begrenzt und mit allen Versionen von Hyper-V und Microsoft-Hypervisor-Produkten des Typs 2 kompatibel, beispielsweise mit Virtual Server und Virtual PC. Windows Server 2012 hat eine aktualisierte Version des Formats eingeführt, das die Dateinamenerweiterung .vhdx verwendet.

VHDX-Imagedateien dürfen bis zu 64 TB groß sein und unterstützen logische Sektorgrößen von 4 KB, um kompatibel mit neuen Laufwerkstypen zu sein, die native 4 KB-Sektoren verwenden. Außerdem können VHDX-Dateien Blockgrößen bis zu 256 MB verwenden, sodass Administratoren das Performanceniveau von virtuellen Speichersubsystemen für bestimmte Anwendungen und Datendateitypen optimieren können. Allerdings sind VHDX-Dateien nicht abwärtskompatibel und lassen sich nur von Windows Server 2012- und Windows 8-Hyper-V-Servern lesen. Wenn die Möglichkeit besteht, dass Sie Ihre virtuellen Computer von Windows Server 2012 auf eine ältere Version von Hyper-V migrieren, sollten Sie weiterhin das VHD-Dateiformat verwenden.

Virtuelle Festplatten erstellen

Windows Server 2012-Hyper-V bietet verschiedene Möglichkeiten, um virtuelle Festplattendateien zu erstellen. So können Sie sie als Teil eines virtuellen Computers anlegen oder sie zu einem anderen Zeitpunkt erzeugen und sie einem virtuellen Computer hinzufügen. Über die grafische Benutzeroberfläche im Hyper-V-Manager lassen sich die meisten VHD-Parameter bearbeiten. Die feinstufigste Kontrolle über das Datenträgerimage-Format ist jedoch mit den neuen Windows PowerShell-Cmdlets in Windows Server 2012 gegeben.

Eine virtuelle Festplatte mit einem virtuellen Computer erstellen

Der Assistent für neue virtuelle Computer enthält eine Seite *Virtuelle Festplatte verbinden*, auf der Sie eine einzelne Festplatte in Ihren neuen virtuellen Computer hinzufügen können. Die Optionen für diese Festplatte sind recht begrenzt:

- **Virtuelle Festplatte erstellen** Erlaubt es, Name, Speicherort und Größe einer neuen VHD anzugeben. Dabei können Sie nur eine dynamisch erweiterbare Festplatte mit dem VHDX-Format erstellen.

- **Vorhandene virtuelle Festplatte verwenden** Hier können Sie den Speicherort einer vorhandenen VHD- oder VHDX-Festplatte angeben, die der virtuelle Computer voraussichtlich als Systemdatenträger verwenden wird
- **Virtuelle Festplatte später zuordnen** Verhindert, dass der Assistent irgendwelche virtuellen Festplatten zur Konfiguration des virtuellen Computers hinzufügt. Es wird davon ausgegangen, dass Sie eine Festplatte später manuell hinzufügen, bevor Sie den virtuellen Computer starten.

Diese Assistantenseite ist dafür vorgesehen, die Festplatte zu erstellen, auf der Sie das Betriebssystem des virtuellen Computers installieren, oder eine vorhandene Festplatte auszuwählen, auf der ein Betriebssystem bereits installiert ist. Der Assistent erstellt immer eine dynamisch erweiterbare Festplatte, die am IDE-Controller 0 angeschlossen ist.



Hinweis VHDs

Microsoft ist dazu übergegangen, die Evaluierungskopien seiner Produkte als Alternative zu den herkömmlichen installierbaren Festplattenimages in Form vorinstallierter VHD-Dateien zu veröffentlichen. Nachdem Sie diese Dateien heruntergeladen haben, können Sie einen virtuellen Computer auf einem Hyper-V-Server erstellen und über die Option *Vorhandene virtuelle Festplatte verwenden* festlegen, die VHD als sein Systemlaufwerk bereitzustellen.

Eine neue virtuelle Festplatte erstellen

Mit dem Assistenten für neue virtuelle Festplatten können Sie in Hyper-V-Manager jederzeit eine VHD-Datei erstellen, auch ohne sie einem virtuellen Computer hinzuzufügen. Führen Sie dazu die folgenden Schritte aus:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorenrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Wählen Sie im Menü *Tools* den Befehl *Hyper-V-Manager*.
3. Wählen Sie im linken Bereich der Konsole *Hyper-V-Manager* einen Hyper-V-Server aus.
4. Im Menü *Aktion* wählen Sie *Neu/Festplatte*, um den Assistenten für neue virtuelle Festplatten zu starten, der die Seite *Vorbemerkungen* anzeigen.
5. Klicken Sie auf *Weiter*, um die Seite *Datenträgerformat auswählen* zu öffnen.
6. Wählen Sie eine der folgenden Optionen für das Datenträgerformat aus:
 - **VHD** Erstellt ein Image nicht größer als 2 TB im kompatiblen VHD-Format
 - **VHDX** Erstellt ein Image bis zu 64 TB im neuen VHDX-Format
7. Klicken Sie auf *Weiter*, um die Seite *Datenträgertyp auswählen* zu öffnen.
8. Wählen Sie eine der folgenden Optionen für den Datenträgertyp aus:
 - **Feste Größe** Erzeugt eine Festplatte der angegebenen Größe und reserviert den gesamten Speicherplatz auf einmal

- **Dynamisch erweiterbar** Erzeugt eine Festplatte, die bis zu der von Ihnen angegebenen Maximalgröße erweitert wird, wenn Sie Daten hinzufügen
- **Differenzierung** Erstellt ein untergeordnetes Laufwerk, das die Änderungen aufnimmt, die Sie im angegebenen übergeordneten Laufwerk vornehmen

9. Klicken Sie auf *Weiter*. Es erscheint die Seite *Name und Pfad angeben*.
10. Geben Sie einen Namen für das Festplattenimage in das Textfeld *Name* ein und bei Bedarf einen Pfad für die Datei, falls er vom Standardpfad für den Server abweicht. Klicken Sie auf *Weiter*, um die Seite *Datenträger konfigurieren* zu öffnen.
11. Für feste und dynamisch erweiterbare Festplatten wählen Sie eine der folgenden Optionen aus und konfigurieren sie:
 - **Neue virtuelle Festplatte ohne Inhalt erstellen** Legt die Größe (oder die Maximalgröße) des zu erstellenden Festplattenimages fest
 - **Inhalt der angegebenen physischen Festplatte kopieren** Ermöglicht es, eine der physischen Festplatten im Computer auszuwählen und ihren Inhalt in das neue Festplattenimage zu kopieren
 - **Inhalt der angegebenen virtuellen Festplatte kopieren** Ermöglicht es, ein virtuelle Festplattendatei auszuwählen und ihren Inhalt in das neue Festplattenimage zu kopieren
12. Klicken Sie auf *Weiter*. Es erscheint die Seite *Abschließen des Assistenten für neue virtuelle Festplatten*.
13. Klicken Sie auf *Fertigstellen*.

Der Assistent erstellt die neue Imagefestplatte und speichert sie am angegebenen Speicherort.



Hinweis Windows PowerShell

Neue VHD-Dateien können Sie auch per Windows PowerShell erstellen. Dabei haben Sie mehr Kontrolle als über die grafische Benutzeroberfläche. Verwenden Sie das Cmdlet `New-VHD` mit der folgenden grundlegenden Syntax, um ein neues Festplattenimage zu erstellen:

```
New-VHD -Path c:\filename.vhd|c:\filename.vhdx  
-Fixed|-Dynamic|-Differencing -SizeBytes <size>  
[-BlockSizeBytes <block size>]  
[-LogicalSectorSizeBytes 512|4096] [-ParentPath <pathname>]
```

Wenn Sie ein Festplattenimage mit dem Cmdlet erstellen, bestimmt die angegebene Dateinaemerweiterung das Format (VHD oder VHDX). Dabei können Sie die Blockgröße und die logische Sektorgröße für das Image festlegen – zwei Dinge, die in der grafischen Benutzeroberfläche nicht möglich sind. Zum Beispiel erstellt der folgende Befehl eine VHDX-Image-datei mit der festen Größe 400 GB und einer logischen Sektorgröße von 4 KB:

```
New-VHD -Path c:\diskfile.vhdx -Fixed  
-SizeBytes 400GB -LogicalSectorSizeBytes 4096
```

Virtuelle Festplatten zu virtuellen Computern hinzufügen

Da sich virtuelle Festplattendateien separat erstellen lassen, können Administratoren mehr Kontrolle über deren Fähigkeiten ausüben. Nach dem Erstellen der VHD- oder VHDX-Dateien müssen Sie sie jedoch einem virtuellen Computer hinzufügen, damit sie nutzbar sind.

Einem physischen Computer fügen Sie ein Festplattenlaufwerk hinzu, indem Sie es an einen Controller anschließen. Das Gleiche gilt für einen virtuellen Computer in Hyper-V. Wenn Sie das Dialogfeld *Einstellungen* für einen virtuellen Computer in seiner Standardkonfiguration öffnen, finden Sie drei Controller vor, die mit *IDE-Controller 0*, *IDE-Controller 1* und *SCSI-Controller* bezeichnet sind. Diese entsprechen den Controllern, wie sie in einem typischen physischen Servercomputer realisiert sind.

Jeder IDE-Controller kann zwei Geräte unterstützen. Die Standardkonfiguration eines virtuellen Computers verwendet einen Kanal an IDE-Controller 0 für die Systemfestplatte und einen Kanal an IDE-Controller 1 für das DVD-Laufwerk des Systems. Haben Sie im Assistenten für neue virtuelle Computer keine virtuelle Festplatte erstellt – also die Option *Virtuelle Festplatte später zuordnen* gewählt –, müssen Sie ein Festplattenimage zu IDE-Controller 0 hinzufügen, um es als Systemlaufwerk zu verwenden. Vom SCSI-Controller aus kann der virtuelle Computer nicht booten.

Einem virtuellen Computer fügen Sie ein vorhandenes virtuelles Systemlaufwerk in folgenden Schritten hinzu:

1. Melden Sie sich bei dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Hyper-V-Manager*, um die Konsole *Hyper-V-Manager* zu öffnen.
3. Wählen Sie im linken Bereich einen Hyper-V-Server aus.
4. Wählen Sie einen virtuellen Computer aus und klicken Sie im Bereich *Aktionen* auf *Einstellungen*. Es erscheint das Dialogfeld *Einstellungen* für den virtuellen Computer.
5. Wählen Sie *IDE-Controller 0* aus, wie Abbildung 3.14 zeigt.

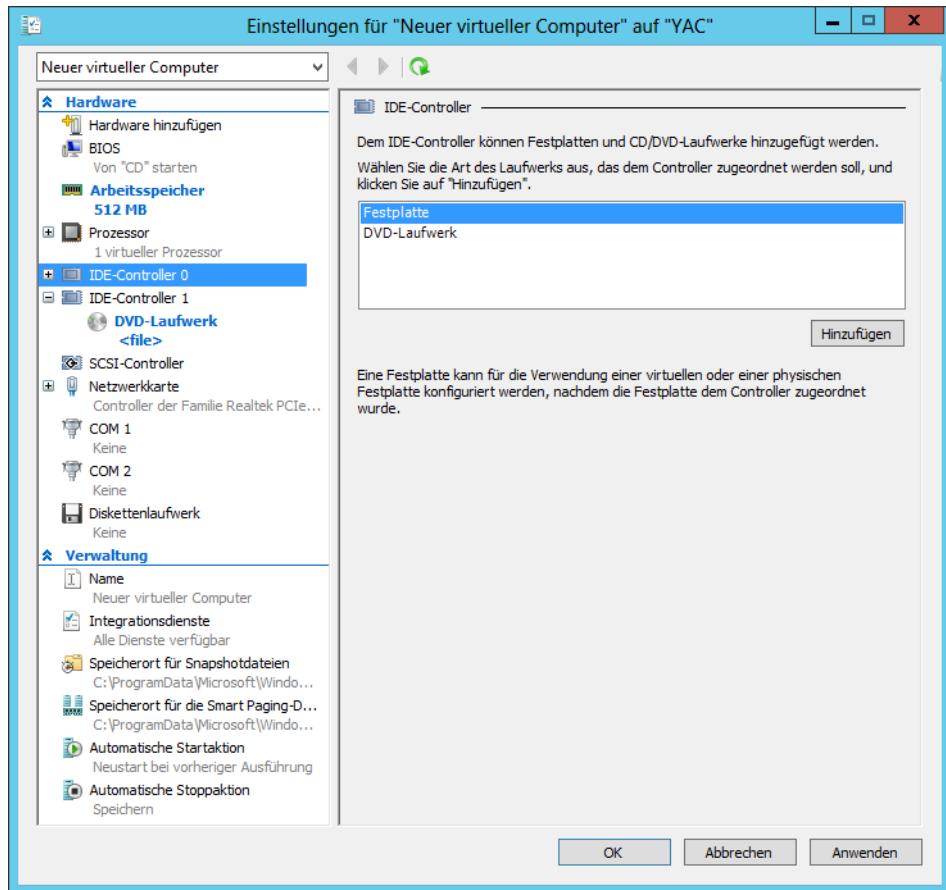


Abbildung 3.14 Die Benutzeroberfläche für IDE-Controller im Dialogfeld *Einstellungen*

6. Wählen Sie im Abschnitt *IDE-Controller* den Eintrag *Festplatte* aus und klicken Sie auf *Hinzufügen*. Daraufhin erscheint die Seite *Festplatte*, wie in Abbildung 3.15 gezeigt.
7. Wählen Sie in den Listen *Controller* und *Speicherort* den IDE-Controller und den Kanal für die Festplatte aus.
8. Klicken Sie bei ausgewählter Option *Virtuelle Festplatte* auf *Durchsuchen* und wählen Sie die Festplatten-Imagedatei aus, die Sie hinzufügen möchten.

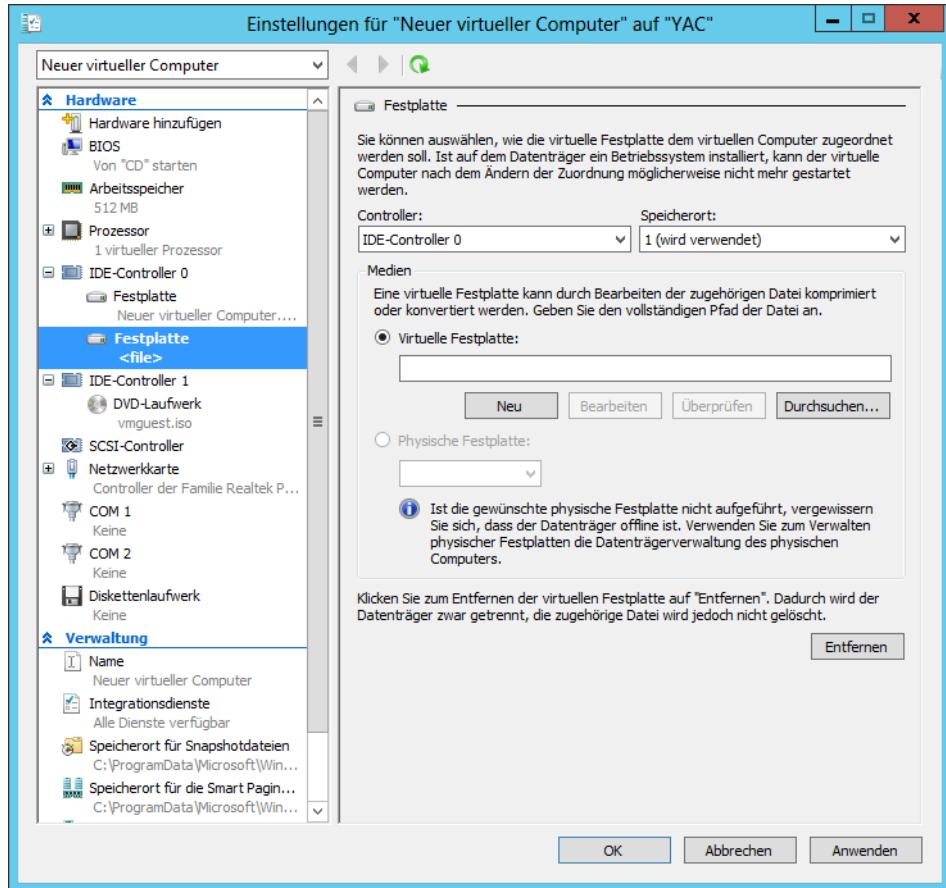


Abbildung 3.15 Die Benutzeroberfläche für eine Festplatte im Dialogfeld *Einstellungen*

9. Klicken Sie auf *OK*, um das Dialogfeld *Einstellungen* zu schließen.

In einem virtuellen Computer können Sie zwar kein SCSI-Laufwerk als Systemlaufwerk verwenden, doch ist es möglich, dem SCSI-Controller virtuelle Datenfestplatten zuzuordnen. Im Unterschied zu den IDE-Anschlüssen, die jeweils nur zwei Geräte unterstützen, lassen sich an einem SCSI-Anschluss bis zu 64 Laufwerke betreiben. Außerdem können Sie einen virtuellen Computer mit weiteren SCSI-Controllern ausstatten, sodass eine fast unbegrenzte Skalierbarkeit für das virtuelle Speichersubsystem gegeben ist.

Differenzierende Festplatten erstellen

Mit einer differenzierenden Festplatte können Sie eine vorhandene virtuelle Festplatten-Imagedatei in ihrem ursprünglichen Zustand bewahren und sie gleichzeitig in einem Betriebssystem bereitstellen und sogar ihren Inhalt verändern. Wenn Sie zum Beispiel ein Labor-Setup aufbauen, können Sie ein Grundsystem erstellen, indem Sie eine neue Kopie eines Betriebssystems auf einer neuen virtuellen Festplatte installieren und die Umgebung

Ihren Anforderungen entsprechend konfigurieren. Dann können Sie eine neue untergeordnete differenzierende Festplatte erstellen, wobei Ihr Grundimage als übergeordnete Festplatte dient. Alle darauffolgenden Änderungen am System werden dann auf die differenzierende Festplatte geschrieben, während die übergeordnete Festplatte unangetastet bleibt. Mit dem Testsystem können Sie nun nach Belieben experimentieren, da der Rückweg offen steht und Sie zu Ihrer Grundkonfiguration zurückkehren können, indem Sie einfach eine neue differenzierende Festplatte anlegen.

Es lassen sich mehrere differenzierende Festplatten anlegen, die auf dasselbe übergeordnete Image zeigen, sodass Sie ein Labornetzwerk mit beliebig vielen virtuellen Computern entsprechend Ihren Anforderungen einrichten können. Dies spart Festplattenplatz und eine wiederholte Installation des Betriebssystems erübrigert sich.

Führen Sie die folgenden Schritte aus, um eine geklonte Version einer Grundinstallation mit einer differenzierenden Festplatte zu erstellen:

1. Installieren und konfigurieren Sie den als Basis dienenden virtuellen Computer. Legen Sie einen neuen virtuellen Computer mit einer neuen Festplatten-Imagedatei an und installieren Sie darauf ein Gastbetriebssystem. Konfigurieren Sie das Betriebssystem entsprechend Ihren Anforderungen und installieren Sie alle Rollen, Features, Anwendungen und Dienste, die Sie benötigen.
2. Verallgemeinern Sie das übergeordnete Image. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten auf dem Grundsystem und führen Sie das Dienstprogramm *Sysprep.exe* aus. Sysprep konfiguriert das System, um sich selbst eine neue eindeutige Sicherheits-ID (SID) zuzuweisen, wenn der Computer das nächste Mal startet. Dadurch ist es möglich, mehrere geklonte Systeme von einem einzigen Festplattenimage zu erstellen.
3. Legen Sie ein übergeordnetes Festplattenimage an. Nachdem Sie die Grundinstallation verallgemeinert haben, brauchen Sie den ursprünglichen virtuellen Computer nicht mehr. Somit können Sie alles löschen mit Ausnahme der VHD- oder VHDX-Datei, die das Festplattenimage enthält. Dieses wird zu Ihrem übergeordneten Image. Öffnen Sie das Eigenschaftenblatt für die Imagedatei und setzen Sie das Flag *Schreibgeschützt*. Damit verhindern Sie Änderungen am Grundimage.
4. Legen Sie eine differenzierende Festplatte an. Erstellen Sie mit dem Assistenten für neue virtuelle Festplatten oder mit dem Windows PowerShell-Cmdlet *New-VHD* eine neue differenzierende Festplatte, die auf das Grundimage zeigt, das Sie vorher als übergeordnetes Image erstellt und vorbereitet haben.
5. Richten Sie einen geklonten virtuellen Computer ein. Erstellen Sie einen neuen virtuellen Computer und ordnen Sie ihm auf der Seite *Virtuelle Festplatte verbinden* mit ausgewählter Option *Vorhandene virtuelle Festplatte verwenden* die differenzierende Festplatte zu, die Sie eben erstellt haben.

Nun können Sie weitere geklonte virtuelle Computer mit differenzierenden Festplatten einrichten, die alle dieselbe übergeordnete Festplatte verwenden. Jeder virtuelle Computer kann eigenständig arbeiten und die übergeordnete Festplatte bleibt unverändert.

Wenn Sie einen differenzierenden Datenträger mit dem Assistenten für neue virtuelle Festplatten erstellen und auf der Seite *Datenträgertyp auswählen* die Option *Differenzierung* aktivieren, sieht die Seite *Datenträger konfigurieren* wie in Abbildung 3.16 gezeigt aus. Geben Sie im Textfeld *Pfad* den Namen der Datei an, die Sie für das übergeordnete Image verwenden möchten.

Ähnlich verhält es sich, wenn Sie die differenzierende Festplatte per Windows PowerShell erstellen. Hier rufen Sie das Cmdlet `New-VHD` mit den Parametern `-Differencing` und `-ParentPath` auf, wobei Sie im zweiten Parameter den Speicherort der übergeordneten Festplatte angeben.

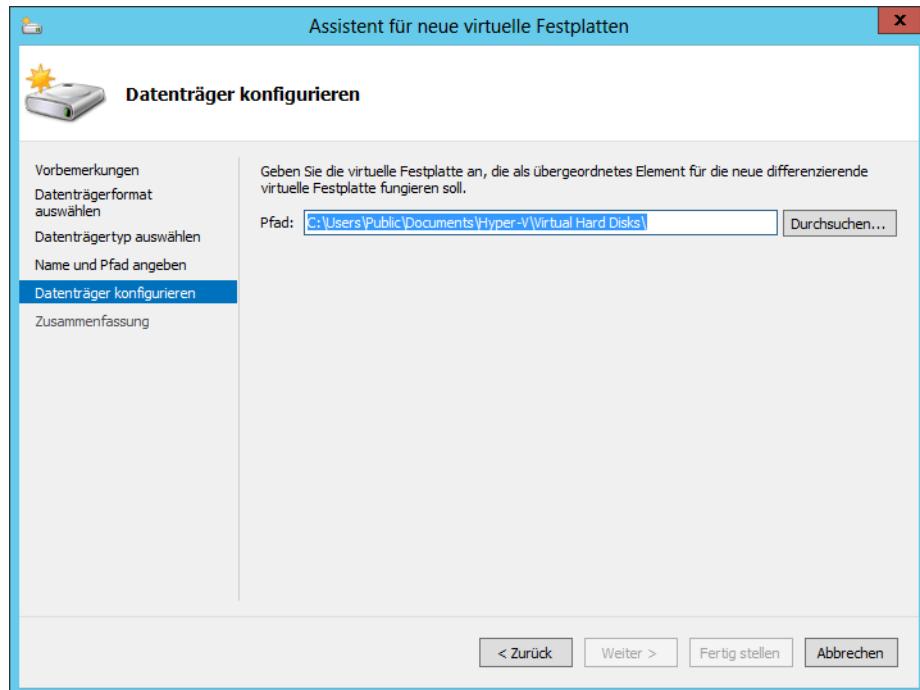


Abbildung 3.16 Die Seite *Datenträger konfigurieren* im Assistenten für neue virtuelle Festplatten, wenn Sie eine differenzierende Festplatte erstellen

Pass-Through-Datenträger konfigurieren

Bislang ging es im Rahmen dieses Prüfungsziels hauptsächlich um VHDs, Bereiche von Speicherplatz auf einem physischen Festplattenlaufwerk, das virtuellen Computern zugeordnet wird. Es ist aber auch möglich, dass virtuelle Computer auf physische Festplatten direkt zugreifen.

Ein Pass-Through-Datenträger (Durchleitungslaufwerk) ist eine Art virtuelle Festplatte, die nicht auf einen Speicherbereich einer physischen Festplatte verweist, sondern auf ein physisches Festplattenlaufwerk, das auf dem Hostcomputer installiert ist. Wenn Sie eine Festplatte mit einem der Controller in einem virtuellen Computer verbinden, können Sie sich zwischen einer physischen Festplatte im Unterschied zu einer virtuellen Festplatte entscheiden.

Um eine physische Festplatte mit einem virtuellen Computer zu verbinden, muss der virtuelle Computer exklusiv darauf zugreifen können. Das heißt, dass Sie zuerst die Festplatte im übergeordneten Betriebssystem über das Snap-In *Datenträgerverwaltung* (siehe Abbildung 3.17) oder das Dienstprogramm *Diskpart.exe* offline schalten müssen. Nachdem sich die Festplatte im Offline-Zustand befindet, erscheint sie in der Dropdownliste *Physische Festplatte* und lässt sich auswählen.

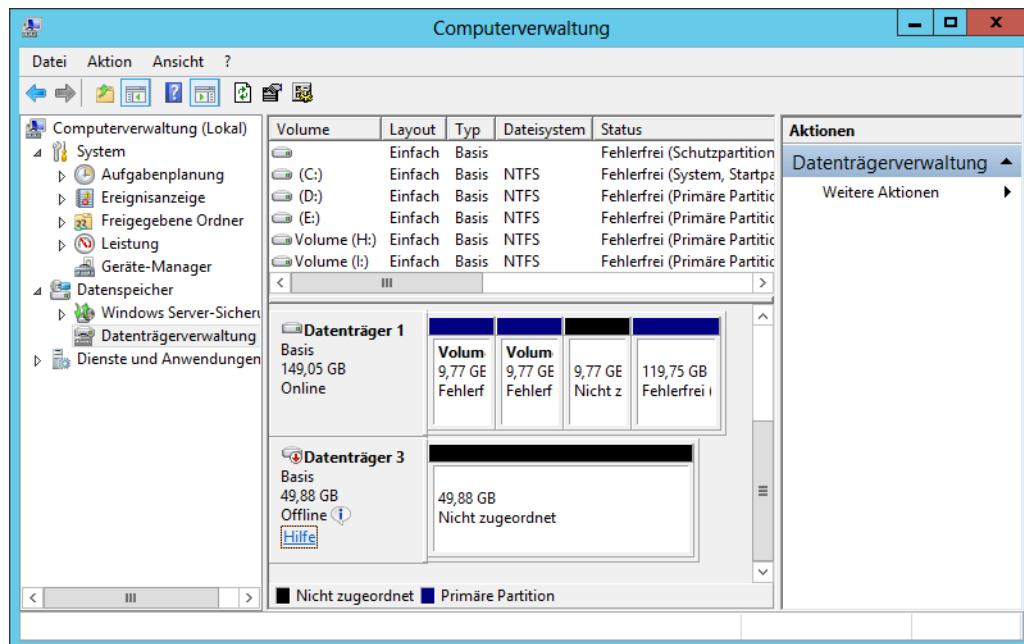


Abbildung 3.17 Ein Offlinedatenträger im Snap-In *Datenträgerverwaltung*

Virtuelle Festplatten modifizieren

In Windows Server 2012 und Hyper-V haben Administratoren verschiedene Möglichkeiten, VHD-Images zu verwalten und zu manipulieren, ohne sie in einem virtuellen Computer bereitzustellen. Nachdem Sie eine VHD erstellt haben, können Sie sie mit dem Assistenten zum Bearbeiten virtueller Festplatten im Hyper-V-Manager verwalten. Um eine vorhandene VHD- oder VHDX-Datei zu bearbeiten, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorenrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Wählen Sie im Menü *Tools* den Befehl *Hyper-V-Manager*, um die Konsole *Hyper-V-Manager* zu öffnen.
3. Wählen Sie im linken Fensterbereich einen Hyper-V-Server aus.

4. Wählen Sie im Fensterbereich *Aktionen* den Eintrag *Datenträger bearbeiten*. Daraufhin startet der Assistent zum Bearbeiten virtueller Festplatten und zeigt die Seite *Vorbemerkungen* an.
5. Klicken Sie auf *Weiter*, um zur Seite *Virtuelle Festplatte suchen* zu gelangen.
6. Geben Sie den Namen der VHD- oder VHDX-Datei ein, die Sie öffnen möchten (oder arbeiten Sie mit *Durchsuchen*), und klicken Sie auf *Weiter*. Es erscheint die Seite *Aktion auswählen*.
7. Wählen Sie eine der folgenden Funktionen aus:
 - **Komprimieren** Verringert die Größe einer dynamisch erweiterbaren oder differenzierenden Festplatte, indem der freie Speicherplatz gelöscht wird, wobei die Kapazität der Festplatte unverändert bleibt
 - **Konvertieren** Ändert den Formattyp einer Festplatte, indem die Daten in eine neue Festplatten-Imagedatei kopiert werden
 - **Erweitern** Vergroßert die Kapazität der Festplatte, indem freier Speicherplatz an die Imagedatei angefügt wird
 - **Verkleinern** Verringert die Kapazität der Festplatte, indem freier Speicherplatz aus der Datei gelöscht wird
 - **Zusammenführen** Fasst die Daten auf einer differenzierenden Festplatte mit den Daten der übergeordneten Festplatte zusammen, um eine einzelne zusammengesetzte Imagedatei zu bilden
8. Klicken Sie auf *Weiter*, um die Seite *Abschließen des Assistenten zum Bearbeiten virtueller Festplatten* zu öffnen.
9. Füllen Sie die neuen Seiten aus, die der Assistent im Ergebnis Ihrer Auswahl anzeigt, und klicken Sie dann auf *Fertig stellen*.

Die Optionen, die auf der Seite *Aktion auswählen* des Assistenten erscheinen, hängen vom aktuellen Status der ausgewählten Imagedatei ab. Zum Beispiel ist die Option *Zusammenführen* nur für eine differenzierende Festplatte vorhanden und die Option *Verkleinern* nur, wenn genügend freier Speicherplatz zur Verfügung steht, den der Assistent löschen kann.

Neben diesen Festplattenbearbeitungsfunktionen des Hyper-V-Managers ist es auch mit dem Snap-In *Datenträgerverwaltung* auf dem Hyper-V-Host möglich, eine VHD- oder VHDX-Datei bereitzustellen und auf deren Inhalt zuzugreifen, als würde es sich um eine physische Festplatte handeln.

Eine VHD-Datei stellen Sie in folgenden Schritten bereit:

1. Melden Sie sich bei dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Computerverwaltung* aus, um die Konsole *Computerverwaltung* zu öffnen.

3. Wählen Sie im linken Fensterbereich *Datenträgerverwaltung* aus. Das Snap-In *Datenträgerverwaltung* wird geöffnet.
4. Im Menü *Aktion* wählen Sie *Virtuelle Festplatte anfügen*. Daraufhin erscheint das Dialogfeld *Virtuelle Festplatte anfügen*.
5. Geben Sie in das Textfeld *Ort* die Imagedatei ein, die Sie anfügen möchten (oder arbeiten Sie mit *Durchsuchen*), und klicken Sie auf *OK*. Die Festplatte wird in der *Datenträgerverwaltung* angezeigt.
6. Schließen Sie die Konsole *Computerverwaltung*.

Nun können Sie mit der virtuellen Festplatte und ihrem Inhalt mithilfe der Standardtools genauso wie mit einem physischen Festplattenlaufwerk arbeiten. Die virtuelle Festplatte trennen Sie nach dem gleichen Verfahren, wobei Sie im Menü *Aktion* den Eintrag *Virtuelle Festplatte trennen* auswählen.

Snapshots erstellen

In Hyper-V stellt ein Snapshot ein erfasstes Image des Zustands, der Daten und der Hardwarekonfiguration eines virtuellen Computers zu einem bestimmten Zeitpunkt dar. Snapshots zu erstellen ist eine komfortable Möglichkeit für Administratoren, bei Bedarf zu einem vorherigen Zustand eines virtuellen Computers zurückzukehren. Wenn Sie beispielsweise bei einer kniffligen Systemaktualisierung einen Snapshot erstellen, bevor Sie das Update durchführen, können Sie den Snapshot anwenden, um den virtuellen Computer in den Zustand zurückzuversetzen, in dem er sich vor Anwenden des Updates befunden hat.

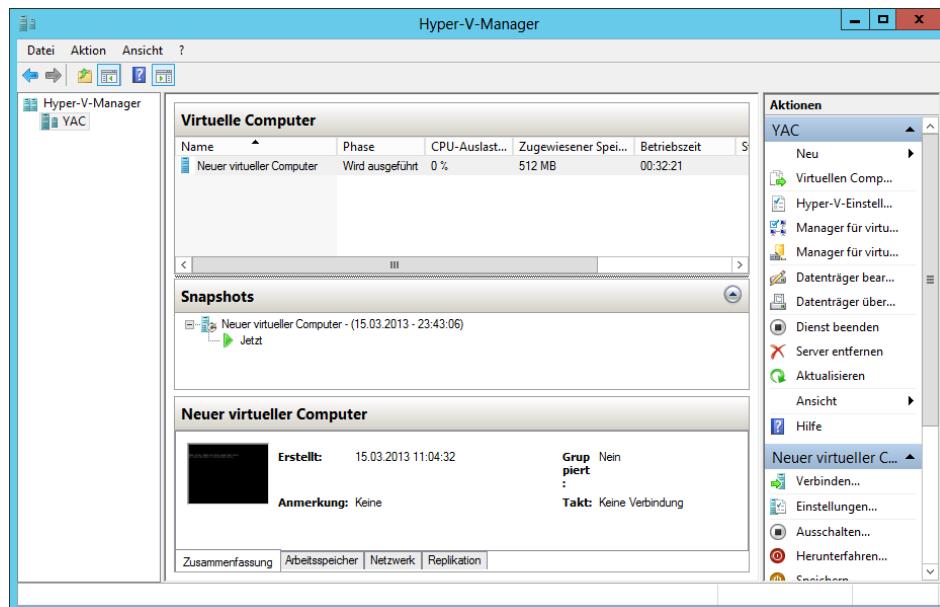


Abbildung 3.18 Ein Snapshot in Hyper-V-Manager

Snapshots lassen sich ganz leicht erstellen. Wählen Sie einfach im Hyper-V-Manager einen laufenden virtuellen Computer und im Fensterbereich *Aktionen* den Eintrag *Snapshot* aus. Das System erstellt eine Snapshot-Datei mit der Erweiterung *.avhd* oder *.avhdx* im selben Ordner wie die VHD-Datei und fügt den Snapshot in die Anzeige des Hyper-V-Managers ein, wie Abbildung 3.18 zeigt.

Snapshots sind in der Hand das Administrators ein nützliches Tool, um eine Umgebung in Hyper-V zu testen, doch empfiehlt es sich nicht für ausgiebigen Einsatz in Produktionsumgebungen. Neben dem zusätzlichen Verbrauch von Festplattenplatz kann die Anwesenheit von Snapshots die Gesamtleistung des Festplattensubsystems eines virtuellen Computers beeinträchtigen.

Mit einem SAN verbinden

Ein SAN (Storage Area Network) ist im Wesentlichen einfach ein Netzwerk, das für Hochgeschwindigkeitsverbindungen zwischen Servern und Speichergeräten ausgelegt ist. Anstatt Festplattenlaufwerke in Servern zu installieren oder sie über einen externen SCSI-Bus anzuschließen, besteht ein SAN aus einem oder mehreren Laufwerken mit Netzwerkadapters, die Sie mit Ihren Servern über normale verdrillte (Twisted Pair) oder fiberoptische Kabel verbinden. Demzufolge besitzt ein SAN, das mit einem Server verbunden ist, mindestens zwei Netzwerkadapter – einen für die normale LAN (Local Area Network)-Verbindung und einen für das SAN (siehe Abbildung 3.19).

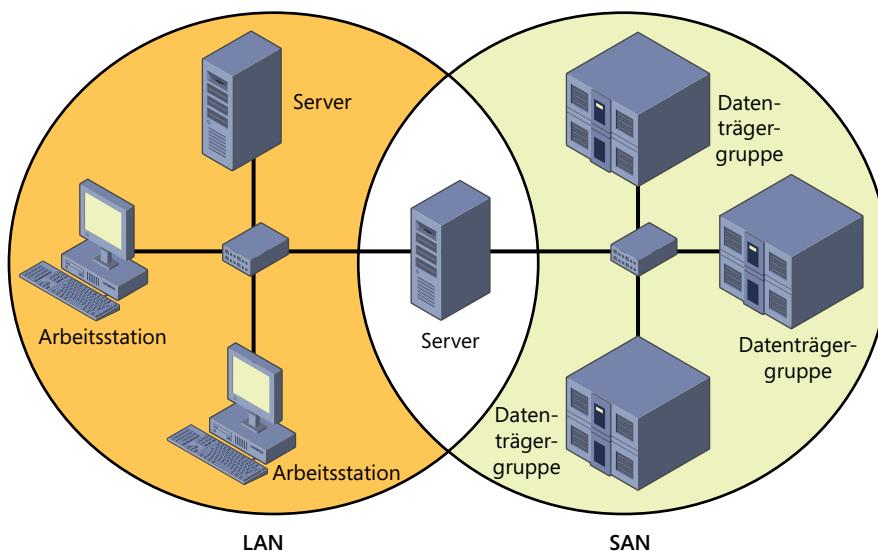


Abbildung 3.19 Ein Server, der an ein SAN angeschlossen ist

SANs bieten vielfältige Vorteile. Weil die Speichergeräte mit einem Netzwerk statt mit den Servern selbst verbunden sind, vermeiden Sie die Beschränkungen aufgrund der maximalen Anzahl von Geräten, die Sie an einen Computer direkt anschließen können. Außerdem sind

SANs flexibler in Bezug auf ihre Kommunikationsfähigkeiten. Da jedes Gerät in einem SAN mit jedem anderen Gerät im selben SAN kommunizieren kann, sind Hochgeschwindigkeitsdatenübertragungen auf folgende Arten möglich:

- **Server zu Speicher** Server können über das SAN auf Speichergeräte so zugreifen, als wären sie direkt am Computer angeschlossen
- **Server zu Server** Server können das SAN verwenden, um direkt miteinander bei hohen Geschwindigkeiten zu kommunizieren, um das LAN mit dem Datenverkehr zu überlasten
- **Speicher zu Speicher** Speichergeräte können ohne Servermitwirkung untereinander kommunizieren, um beispielsweise ein Medium auf einem anderen zu sichern oder Laufwerke auf andere Datenträgergruppen zu spiegeln

Ein SAN ist an sich keine Technik für Hochverfügbarkeit. Diese Eigenschaft lässt sich aber erreichen, wenn Sie redundante Server im selben Netzwerk verbinden, wie Abbildung 3.20 veranschaulicht. Damit sind diese in der Lage, auf dieselben Datenspeichergeräte zuzugreifen. Falls ein Server ausfällt, kann ein anderer dessen Rollen übernehmen, indem er auf dieselben Daten zugreift. Eine derartige Anordnung bezeichnet man als Servercluster.

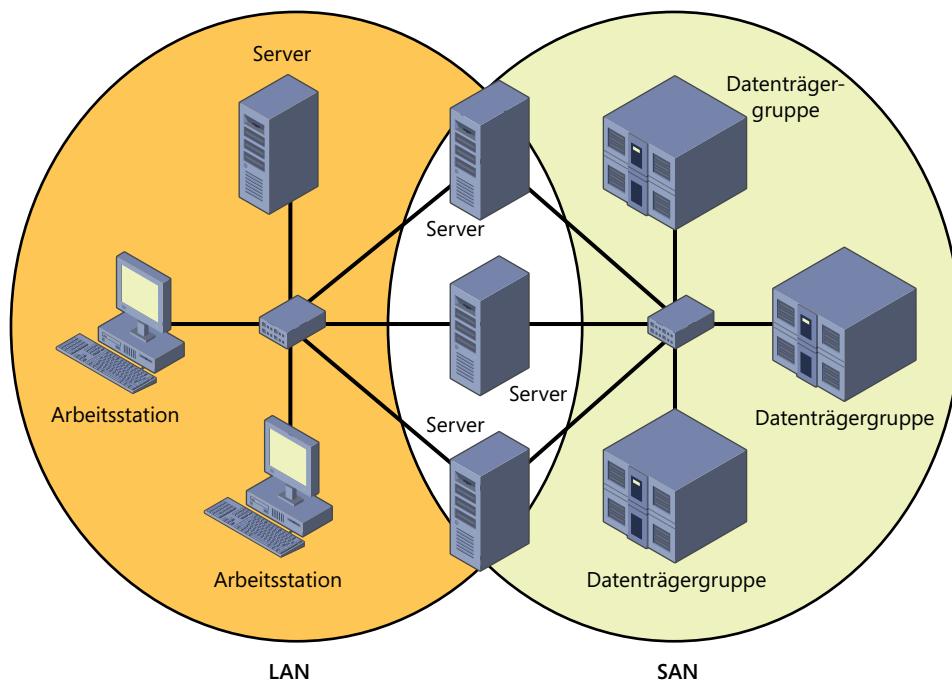


Abbildung 3.20 Mehrere Server, die an ein SAN angeschlossen sind

Da SANs mit Standardnetzwerktechniken arbeiten, lassen sich auch die Entferungen zwischen Servern und Speichergeräten erheblich ausdehnen. So können Sie ein SAN konzipieren, das sich genau wie ein normales Computernetzwerk über verschiedene Räume, Etagen oder sogar Gebäude erstreckt.

Im Unterschied zu einem direkten Anschluss über ein SCSI-Kabel können Server und Speichergeräte über eine SAN-Verbindung keine SCSI-Befehle austauschen. Um über ein SAN zu kommunizieren, bilden Server und Speichergeräte ihre SCSI-Kommunikation auf ein anderes Protokoll wie zum Beispiel SCSI-Fibre Channel ab.

Das Fibre Channel-Protokoll

Fibre Channel ist eine universelle SAN-Kommunikationstechnik, die verschiedenartige Netzwerkmedien, Übertragungsgeschwindigkeiten, Topologien und Protokolle auf oberer Ebene unterstützt. Nachteilig ist in erster Linie, dass Spezialhardware erforderlich ist, die recht teuer sein kann.

Die Installation eines Fibre Channel-SANs hat zur Konsequenz, ein vollständig neues Netzwerk mit eigenen speziellen Medien, Switches und Netzwerkkadapters aufzubauen. Neben den Hardwarekosten, die leicht das 10-fache eines herkömmlichen Ethernet-Netzwerks betragen können, sind auch Ausgaben für Installation und Wartung zu berücksichtigen. Fibre Channel ist eine recht esoterische Technik mit relativ wenigen Experten auf diesem Gebiet. Um ein Fibre Channel-SAN zu installieren und zu verwalten, muss eine Organisation entweder erfahrene Mitarbeiter einstellen oder die vorhandenen Mitarbeiter für diese neue Technik ausbilden.

Virtuelle Computer mit einem SAN verbinden

Die spezialisierten Netzwerktechniken für den Aufbau von Fibre Channel-SANs haben es in der Vergangenheit erschwert, diese Technik mit virtualisierten Servern einzusetzen. Windows Server 2012-Hyper-V unterstützt nun aber das Einrichten von virtuellen Fibre Channel-Adaptoren.

Ein Hyper-V-Fibre Channel-Adapter ist praktisch ein Pass-Through-Gerät, das einem virtuellen Computer den Zugriff auf einen physischen Fibre Channel-Adapter, der im Computer installiert ist, und darüber den Zugriff auf die an das SAN angeschlossenen Ressourcen erlaubt. Damit können Anwendungen, die auf virtuellen Computern laufen, auf Datendateien zugreifen, die auf SAN-Geräten gespeichert sind, und Administratoren sind in der Lage, Servercluster mit virtuellen Computern und gemeinsamen Speichersubsystem einzurichten.

Um die Fibre Channel-Konnektivität zu unterstützen, müssen die Treiber der physischen Fibre Channel-Hostbusadapter im Hostcomputer die virtuelle Fibre Channel-Technik explizit unterstützen. Bei Veröffentlichung von Windows Server 2012 war diese Unterstützung noch recht spärlich gesät, doch ist davon auszugehen, dass immer mehr Hersteller ihre Treiber aktualisieren, um die erforderliche Unterstützung zu bieten. Außerdem muss Ihr SAN in der Lage sein, die angeschlossenen Ressourcen mithilfe von logischen Gerätenummern (Logical Unit Numbers, LUNs) anzusprechen.

Unter der Voraussetzung, dass Sie die passende Hard- und Software auf dem Hostcomputer installiert haben, implementieren Sie die Fibre Channel-Funktionen in Hyper-V, indem Sie zuerst ein virtuelles SAN über den Manager für virtuelle SANs erstellen, der vom Hyper-V-Manager aus erreichbar ist. Wenn Sie das virtuelle SAN einrichten, erscheinen die WWNNs

(World Wide Node Names) und WWPNs (World Wide Port Names) Ihres Hostbusadapters, wie Abbildung 3.21 zeigt.

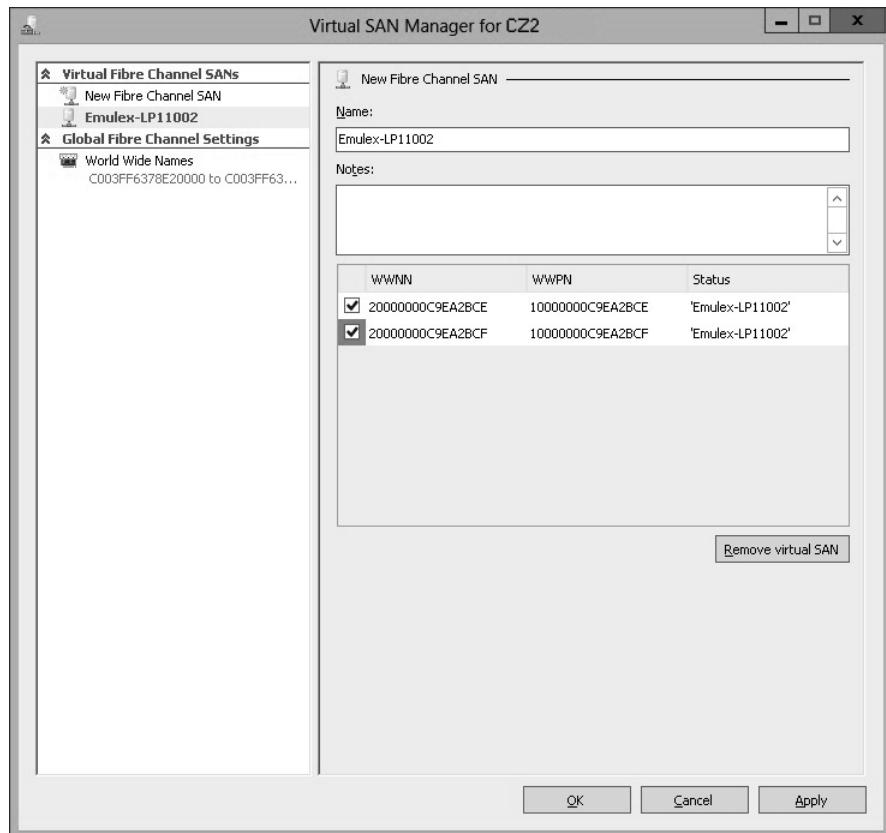


Abbildung 3.21 WWNNs und WWPNs in einem virtuellen SAN

Im nächsten Schritt fügen Sie über das Dialogfeld *Einstellungen* auf der Seite *Hardware hinzufügen* einem virtuellen Computer einen Fibre Channel-Adapter hinzu. Das vorher erstellte virtuelle SAN ist dann auf der Seite *Fibre Channel-Adapter* verfügbar (siehe Abbildung 3.22). Hyper-V virtualisiert das SAN und macht die WWNNs und WWPNs für den virtuellen Computer verfügbar.

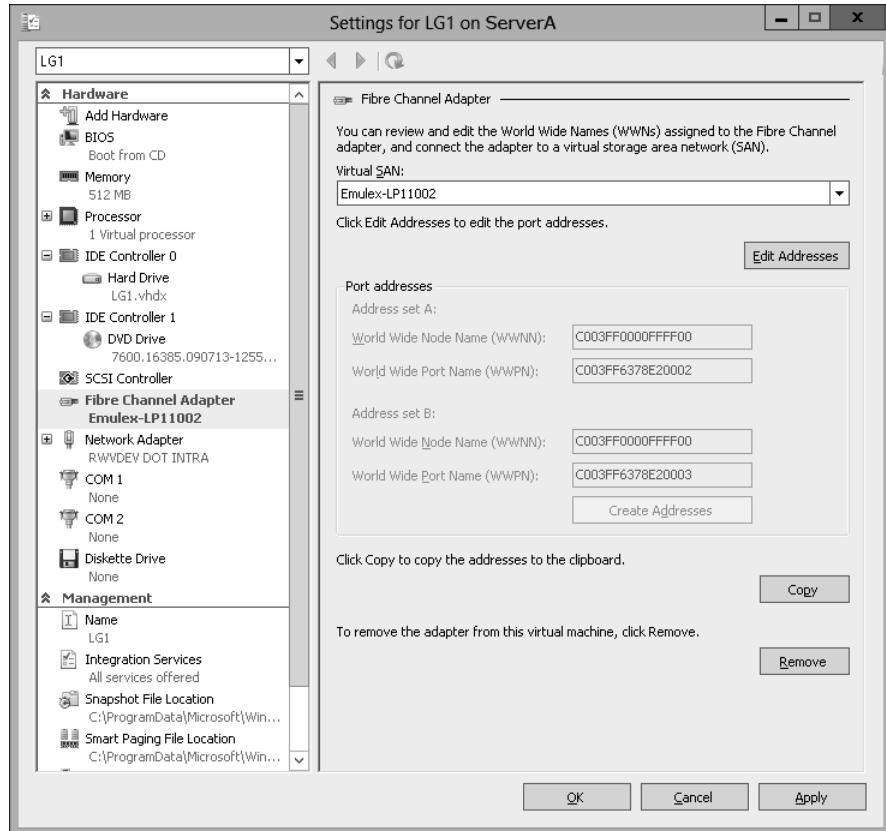


Abbildung 3.22 Ein Fibre Channel-Adapter in einem virtuellen Computer

Prüfungszielzusammenfassung

- Hyper-V nutzt ein spezialisiertes VHD-Format, um einen Teil des Platzes auf einem physischen Datenträger zu packen und ihn für den virtuellen Computer wie ein physisches Festplattenlaufwerk erscheinen zu lassen
- Ein dynamisches Festplattenimage ist eine Imagedatei mit einer festgelegten Maximalgröße. Die Datei ist anfangs klein und wird bei Bedarf erweitert, um sich den Daten anzupassen, die das System in das Image schreibt.
- Ein differenzierendes Festplattenimage ist eine untergeordnete Imagedatei, die mit einer bestimmten übergeordneten Imagedatei verbunden ist. Das System schreibt alle Änderungen an den Daten in der übergeordneten Imagedatei in das untergeordnete Image, um zu einem späteren Zeitpunkt einen Rollback zu ermöglichen.
- VHDX-Imagedateien dürfen in Windows Server 2012 bis zu 64 TB groß sein und unterstützen logische Sektorgrößen von 4 KB, um kompatibel mit neuen Laufwerkstypen zu sein, die native 4 K-Sektoren verwenden

- Ein Pass-Through-Datenträger ist eine Art virtuelle Festplatte, die nicht auf einen Speicherbereich einer physischen Festplatte verweist, sondern auf ein physisches Festplattenlaufwerk, das auf dem Hostcomputer installiert ist
- In Hyper-V stellt ein Snapshot ein erfasstes Image des Zustands, der Daten und der Hardwarekonfiguration eines virtuellen Computers zu einem bestimmten Zeitpunkt dar
- Die spezialisierten Netzwerktechniken für den Aufbau von Fibre Channel-SANs haben es in der Vergangenheit erschwert, diese Technik mit virtualisierten Servern einzusetzen. Windows Server 2012-Hyper-V unterstützt nun aber das Einrichten von virtuellen Fibre Channel-Adaptoren.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Aussagen über VHDX-Dateien ist nicht richtig?
 - A. VHDX-Dateien dürfen maximal 64 TB groß sein.
 - B. VHDX-Dateien lassen sich nur von Computern öffnen, die Windows Server 2012 ausführen.
 - C. VHDX-Dateien unterstützen größere Blockgrößen als VHD-Dateien.
 - D. VHDX-Dateien unterstützen logische Sektoren mit 4 KB.
2. Welche der folgenden Punkte müssen für einen Pass-Through-Datenträger gelten?
 - A. Ein Pass-Through-Datenträger muss im Gastbetriebssystem, das auf ihn zugreift, offline gesetzt sein.
 - B. Ein Pass-Through-Datenträger muss in der übergeordneten Partition des Hyper-V-Servers offline gesetzt sein.
 - C. Ein Pass-Through-Datenträger lässt sich nur an einen SCSI-Controller anschließen.
 - D. Ein Pass-Through-Datenträger muss einem virtuellen Computer über das Snap-In *Datenträgerverwaltung* hinzugefügt werden.
3. Unter welchen Bedingungen erscheint die Funktion *Zusammenführen* im Assistenten zum Bearbeiten virtueller Festplatten?
 - A. Wenn Sie eine VHDX-Datei zur Bearbeitung auswählen.
 - B. Wenn Sie zwei oder mehrere Festplatten zur Bearbeitung auswählen.
 - C. Wenn Sie eine Festplatte auswählen, auf der freier Speicherplatz vorhanden ist.
 - D. Wenn Sie eine differenzierende Festplatte zur Bearbeitung auswählen.

4. Welche der folgenden Gründe sprechen dagegen, Snapshots von virtuellen Computern aufzunehmen? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Snapshots können große Mengen Festplattenplatz belegen.
 - B. Jeder Snapshot setzt eine separate Kopie der Speicherreservierung im virtuellen Computer voraus.
 - C. Es kann mehrere Stunden dauern, bis ein Snapshot erstellt ist.
 - D. Die Anwesenheit von Snapshots kann die Leistung eines virtuellen Computers herabsetzen.
5. Welche der folgenden Voraussetzungen müssen nicht erfüllt sein, um einem virtuellen Computer mit Hyper-V einen Fibre Channel-Adapter hinzuzufügen?
 - A. Es muss ein virtuelles Fibre Channel-SAN eingerichtet werden.
 - B. Im Hostcomputer muss ein physischer Fibre Channel-Adapter installiert sein.
 - C. Es ist ein Fibre Channel-Adapter erforderlich, der virtuelle Netzwerke unterstützt.
 - D. Der Fibre Channel-Adapter muss mit den Speichergeräten über SCSI-Kabel verbunden sein.



Gedankenexperiment Wenden Sie im folgenden Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Ed möchte auf seinem Hyper-V-Server eine neue VHD-Datei per Windows PowerShell erstellen. Er führt das Cmdlet Get-Disk aus und erhält die folgenden Ergebnisse:

Number	Friendly Name	Operational Status	Total Size	Partition Style
0	WDC WD5003ABYX-18WERA0	Online	465.76 GB	MBR
1	WDC WD1002FAEX-00Z3A0	Online	931.51 GB	GPT

Mit welchem Befehl kann Ed eine neue VHD mit einer festen Größe von 500 GB für seinen virtuellen Computer *ServerA* im Windows Server 2012-Format erstellen, wobei er die Daten von der 465-GB-Festplatte auf seinem Computer und eine Sektorgröße von 4096 Byte verwenden will?

Prüfungsziel 3.3: Virtuelle Netzwerke erstellen und konfigurieren

Netzwerke stellen einen entscheidenden Bestandteil in einer Infrastruktur mit virtuellen Computern dar. Je nach Ihrem Netzwerkplan können die virtuellen Computer, die Sie auf einem Windows Server 2012-Hyper-V-Server einrichten, eine Kommunikation mit anderen virtuellen Computern, mit den Computern in Ihrem physischen Netzwerk und mit dem Internet erfordern.

Wenn Sie ein Netzwerk aus physischen Computern aufbauen, installieren Sie in jedem Computer einen Netzwerkadapter und verbinden ihn mit dem Hardwareswitch. Das gleiche Prinzip gilt auch in einer Hyper-V-Umgebung, außer dass Sie es mit virtuellen statt mit physischen Komponenten zu tun haben. Jeder virtuelle Computer, den Sie erstellen, besitzt mindestens einen virtuellen Netzwerkadapter. Diesen Adapter können Sie mit einem virtuellen Switch verbinden. Dadurch sind Sie in der Lage, sich mit den virtuellen Computern auf Ihrem Hyper-V-Server zu verbinden, und zwar in verschiedenen Netzwerkkonfigurationen, die die Systeme in Ihrem physischen Netzwerk einbinden oder ausschließen.

Auf einem Hyper-V-Server können Sie mehrere virtuelle Switches und in jedem virtuellen Computer mehrere Netzwerkadapter anlegen. Somit lässt sich eine flexible Netzwerkumgebung gestalten, die für unterschiedliche Aufgaben gerüstet ist – angefangen bei einem Labor- oder Schulungsnetzwerk bis hin zu einer Produktionsumgebung. Darüber hinaus erlaubt es Windows Server 2012, Erweiterungen für virtuelle Switches hinzuzufügen, sodass sich deren Funktionalität von Softwareentwicklern verbessern lässt.

Dieses Prüfungsziel zeigt, wie Sie

- Hyper-V-Netzwerkvirtualisierung implementieren
 - virtuelle Hyper-V-Switches konfigurieren
 - die Netzwerkperformance optimieren
 - MAC-Adressen konfigurieren
 - Netzwerkséparation konfigurieren
 - synthetische und ältere Netzwerkadapter konfigurieren
-

Virtuelle Switches erstellen

Ein virtueller Switch ist wie sein physisches Gegenstück ein Gerät, das auf der Schicht 2 des OSI (Open Systems Interconnect)-Referenzmodells arbeitet. Ein Switch besitzt eine Reihe von Ports (Anschlüssen), die jeweils mit dem Netzadapter eines Computers verbunden sind. Jeder mit dem Switch verbundene Computer kann Daten auf jeden anderen Computer, der mit demselben Switch verbunden ist, übertragen.

Im Unterschied zu physischen Switches können virtuelle Switches, die durch Hyper-V erstellt wurden, eine unbegrenzte Anzahl von Ports besitzen. Administratoren brauchen sich also keine Gedanken zu machen um Dinge wie die Verbindung von Switches oder um Uplink- und Crossover-Schaltungen.

Den virtuellen Standardswitch erstellen

Beim Installieren der Hyper-V-Rolle mit dem Windows Server 2012-Assistenten zum Hinzufügen von Rollen und Features haben Sie Gelegenheit, virtuelle Switches zu erstellen. Installieren Sie Hyper-V auf einem Server, der Windows Server 2012 ausführt, können Sie auf der Seite *Virtuelle Switches erstellen* einen virtuellen Switch für die einzelnen physischen Netzwerkadapter, die im Hostcomputer installiert sind, erstellen. Mithilfe dieser Switches können virtuelle Computer an den Netzwerken teilnehmen, mit denen die physischen Adapter verbunden sind.

Wenn Sie einen virtuellen Switch auf diese Weise erstellen, ändert sich die Netzwerkkonfiguration im Hostbetriebssystem auf der übergeordneten Partition. Der neue virtuelle Switch erscheint im Fenster *Netzwerkverbindungen* und bei dessen Eigenschaften ist zu sehen, dass der Switch an den TCP/IP-Client des Betriebssystems gebunden ist, wie Abbildung 3.23 zeigt.

Zwischenzeitlich ändert auch Hyper-V die Eigenschaften der ursprünglichen Netzwerkverbindung, die den physischen Netzwerkadapter im Computer darstellen. Der physische Netzwerkadapter ist jetzt nur an den virtuellen Switch gebunden (siehe Abbildung 3.24).

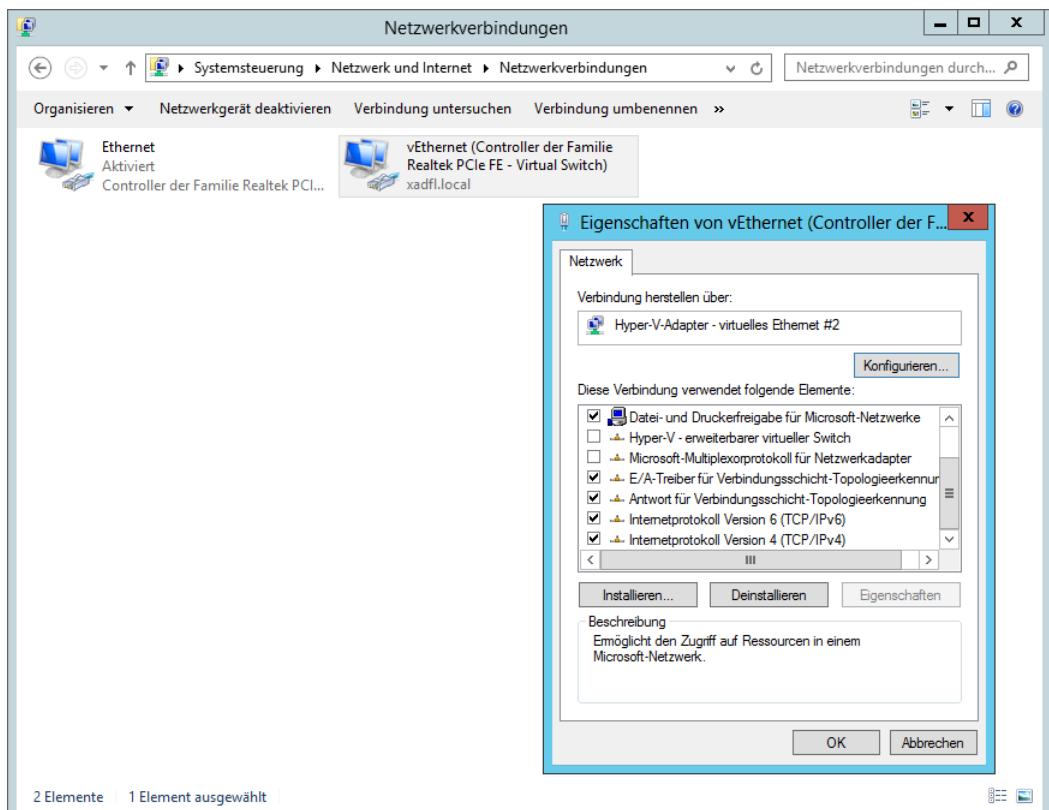


Abbildung 3.23 Im Hostbetriebssystem angezeigter virtueller Switch und dessen Eigenschaften

Letztlich wird die physische Netzwerkkonfiguration, in der der Netzwerkadapter mit einem externen physischen Switch verbunden ist, durch die von Hyper-V erzeugte virtuelle Netzwerkkonfiguration überlagert. In dieser virtuellen Konfiguration ist der virtuelle Switch mit dem physischen Switch und der Netzwerkadapter im Hostbetriebssystem mit dem virtuellen Switch verbunden. Das interne virtuelle Netzwerk und das externe physische Netzwerk werden zu einem einzigen LAN verknüpft, genauso als würden Sie zwei physische Switches verbinden.

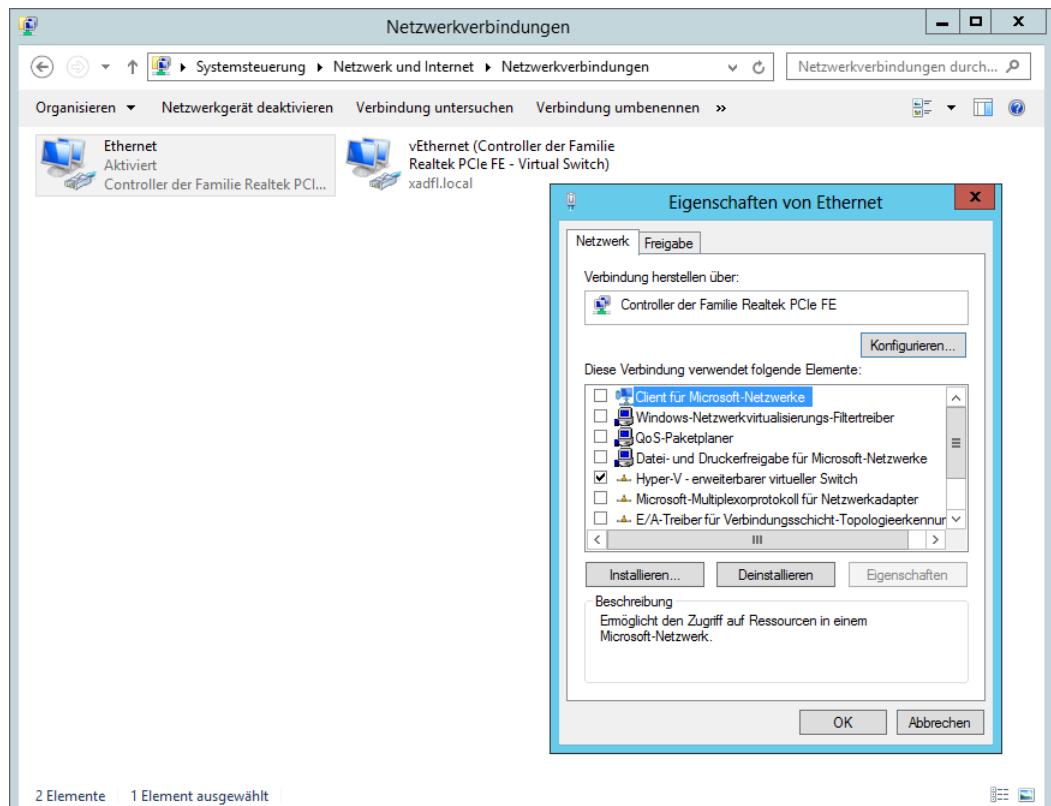


Abbildung 3.24 Ein Netzwerkadapter im Hostbetriebssystem, der an einen virtuellen Switch gebunden ist

Nachdem Hyper-V den virtuellen Switch erstellt und diese Konfigurationsänderungen vorgenommen hat, werden alle neuen virtuellen Computer, die Administratoren für eine Verbindung zum virtuellen Switch auswählen, Bestandteil dieses vereinigten Netzwerks, wie es bei physischen Computern der Fall ist, die mit einem physischen Netzwerk über einen externen Switch verbunden sind.

In der Hyper-V-Terminologie ist ein derartiger virtueller Switch ein externer Netzwerkswitch, da er Verbindungen bereitstellt, die extern zur Hyper-V-Umgebung sind. Dies ist normaler-

weise die bevorzugte Anordnung für ein Produktionsnetzwerk, in der virtuelle Hyper-V-Computer Dienste für das gesamte Netzwerk bereitstellen und nutzen.

Zum Beispiel erhält ein virtueller Computer, der mit diesem Switch verbunden ist, automatisch eine IP-Adresse von einem DHCP (Dynamic Host Configuration Protocol)-Server im physischen Netzwerk, sofern es dort einen derartigen Server gibt. Als Alternative könnten Sie einen virtuellen Computer als DHCP-Server konfigurieren und ihn Adressen für alle Systeme – virtuelle und physische – im Netzwerk bereitstellen lassen.

Vielleicht noch wichtiger ist, dass in dieser Anordnung die virtuellen Computer auch auf das Internet über die Router und DNS-Server im externen Netzwerk zugreifen können. Die virtuellen Computer können dann Betriebssystemaktualisierungen von den Windows Update-Servern im Internet herunterladen, genau wie es regelmäßig bei externen Computern geschieht.

Es gibt aber auch Situationen, in denen ein derartiger virtueller Switch nicht geeignet ist. Wenn Sie ein Labornetzwerk für Produkttests oder ein Netzwerk für den Schulungsraum aufbauen, soll das Netzwerk weder vom externen Netzwerk aus zugänglich sein noch darauf zugreifen können. In diesen Fällen müssen Sie mit dem Manager für virtuelle Switches im Hyper-V-Manager eine andere Art von virtuellem Switch erstellen.

Einen neuen virtuellen Switch erstellen

Hyper-V in Windows Server 2012 unterstützt drei Switch-Typen, die Sie im Manager für virtuelle Switches erstellen müssen, bevor Sie sie verwenden können.

Einen neuen virtuellen Switch erstellen Sie in folgenden Schritten:

1. Melden Sie sich bei dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Hyper-V-Manager*, um die Konsole *Hyper-V-Manager* zu öffnen.
3. Wählen Sie im linken Fensterbereich einen Hyper-V-Server aus.
4. Im Bereich *Aktionen* wählen Sie *Manager für virtuelle Switches* aus. Daraufhin wird für den Hyper-V-Server das in Abbildung 3.25 gezeigte Dialogfeld *Manager für virtuelle Switches* geöffnet.
5. Im Abschnitt *Virtuellen Switch erstellen* wählen Sie einen der folgenden Switch-Typen:
 - **Extern** Der virtuelle Switch wird an den Netzwerkprotokollstack im Hostbetriebssystem gebunden und im Hyper-V-Server an einen physischen Netzwerkadapter angegeschlossen. Virtuelle Computer, die auf den über- und untergeordneten Partitionen laufen, können auf das physische Netzwerk zugreifen, mit dem der physische Adapter verbunden ist.

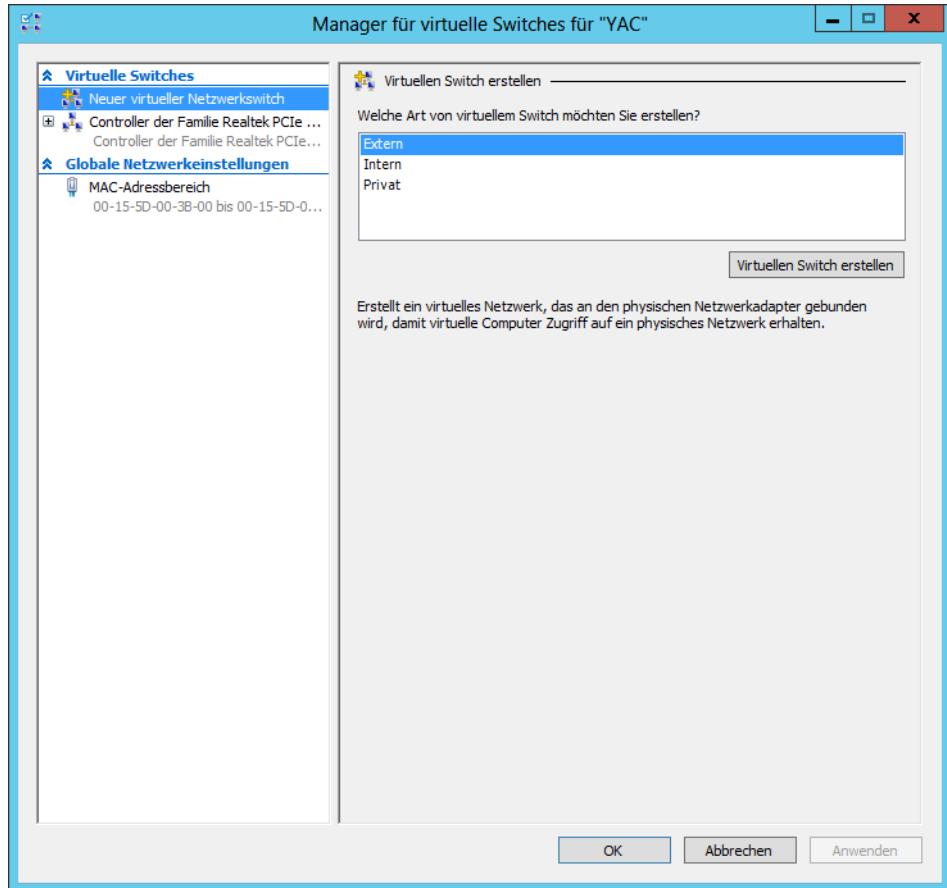


Abbildung 3.25 Das Dialogfeld *Manager für virtuelle Switches*

- **Intern** Ein interner Netzwerkswitch wird an eine separate Instanz des Netzwerkprotokoll-Stacks im Hostbetriebssystem gebunden, und zwar unabhängig vom physischen Netzwerkadapter und dessen angeschlossenem Netzwerk. Virtuelle Computer, die auf den über- und untergeordneten Partitionen laufen, können auf das virtuelle Netzwerk zugreifen, das durch den virtuellen Switch implementiert wird; das Hostbetriebssystem auf der übergeordneten Partition kann auf das physische Netzwerk über den physischen Netzwerkadapter zugreifen. Dagegen sind die virtuellen Computer auf den untergeordneten Partitionen nicht in der Lage, auf das physische Netzwerk über den physischen Adapter zuzugreifen.
- **Privat** Ein privater Netzwerkswitch existiert nur im Hyper-V-Server und ist nur den virtuellen Computern zugänglich, die auf den untergeordneten Partitionen laufen. Das Hostbetriebssystem auf der übergeordneten Partition kann über den physischen Netzwerkadapter auf das physische Netzwerk zugreifen, jedoch nicht auf das virtuelle Netzwerk, das durch den virtuellen Switch erstellt wurde.

6. Klicken Sie auf *Virtuellen Switch erstellen*, um die Seite *Eigenschaften für virtuelle Switches* zu öffnen.
7. Konfigurieren Sie bei Bedarf die folgenden Optionen:
 - **Gemeinsames Verwenden dieses Netzwerkadapters für das Verwaltungsbetriebssystem zulassen** Diese Option ist standardmäßig ausgewählt, wenn Sie einen externen virtuellen Switch erstellen. Wird dieses Kontrollkästchen deaktiviert, wird das Hostbetriebssystem vom physischen Netzwerk ausgeschlossen, während der Zugriff auf die untergeordneten virtuellen Computer erlaubt wird.
 - **SR-IOV (Single-Root I/O Virtualization) aktivieren** Ermöglicht es, einen externen virtuellen Switch mit einem physischen Netzwerkadapter, der SR-IOV unterstützen kann, zu erstellen. Diese Option ist nur verfügbar, wenn Sie einen neuen virtuellen Switch erstellen; ein vorhandener virtueller Switch lässt sich mit dieser Option nicht modifizieren.
 - **Identifizierung virtueller LANs für das Verwaltungsbetriebssystem aktivieren** Wenn Ihr Hostcomputer mit einer physischen Switch-basierten Infrastruktur verbunden ist, die mithilfe virtueller LANs (VLANs) getrennte Subnetze erstellt, können Sie dieses Kontrollkästchen aktivieren und einen VLAN-Bezeichner eingeben, um auf den virtuellen Switch mit einem bestimmten VLAN in Ihrem physischen Netzwerk zuzugreifen.
8. Klicken Sie auf *OK*. Der neue virtuelle Switch erscheint im linken Fensterbereich in der Liste der virtuellen Switches. Bei Bedarf können Sie weitere virtuelle Switches erstellen. Zwar können Sie für jeden physischen Netzwerkadapter im Computer jeweils nur einen externen Switch erstellen, doch lassen sich mehrere interne oder private Switches anlegen, um je nach Anforderung beliebig viele Netzwerke einzurichten.



Hinweis Windows PowerShell

Einen neuen virtuellen Switch können Sie per Windows PowerShell mit dem Cmdlet `New-VMSwitch` und der folgenden grundlegenden Syntax erstellen:

```
New-VMSwitch <switch name> -NetAdapterName <adapter name>
[-SwitchType Internal|Private]
```

Zum Beispiel erstellen Sie mit dem folgenden Befehl einen externen Switch namens *LAN Switch*:

```
New-VMSwitch "LAN Switch" -NetAdapterName "Ethernet"
```

MAC-Adressen konfigurieren

Jeder Netzwerkadapter besitzt eine MAC (Media Access Control)-Adresse – manchmal auch als *Hardwareadresse* bezeichnet –, die das Gerät im Netzwerk eindeutig kennzeichnet. Bei physischen Netzwerkadapters weist der Hersteller die MAC-Adresse zu und hinterlegt sie permanent in der Firmware des Adapters. Die MAC-Adresse ist ein hexadezimaler 6-Byte-Wert. Die ersten drei Bytes enthalten eine Herstellerkennung (Organizationally Unique Identifier, OUI) und die letzten drei Bytes kennzeichnen den Adapter selbst.

Da die MAC-Adresse für den Betrieb eines LANs entscheidend ist, müssen auch die virtuellen Netzwerkadapter auf einem Hyper-V-Server eine MAC-Adresse erhalten. Der Server verfügt über mindestens eine echte MAC-Adresse, die durch seinen physischen Netzwerkadapter gegeben ist. Hyper-V kann aber nicht nur diese eine Adresse für alle virtuellen Adapter verwenden, die die virtuellen Computer mit dem Netzwerk verbinden.

Stattdessen erzeugt Hyper-V während der Installation der Rolle einen Pool von MAC-Adressen und weist dann Adressen aus diesem Pool den virtuellen Computern zu, wenn Sie diese erstellen. Um den Pool der MAC-Adressen für den Hyper-V-Server anzuzeigen oder zu ändern, öffnen Sie den Manager für virtuelle Switches und wählen unter *Globale Netzwerkeinstellungen* den Eintrag *MAC-Adressbereich*, wie Abbildung 3.26 zeigt.

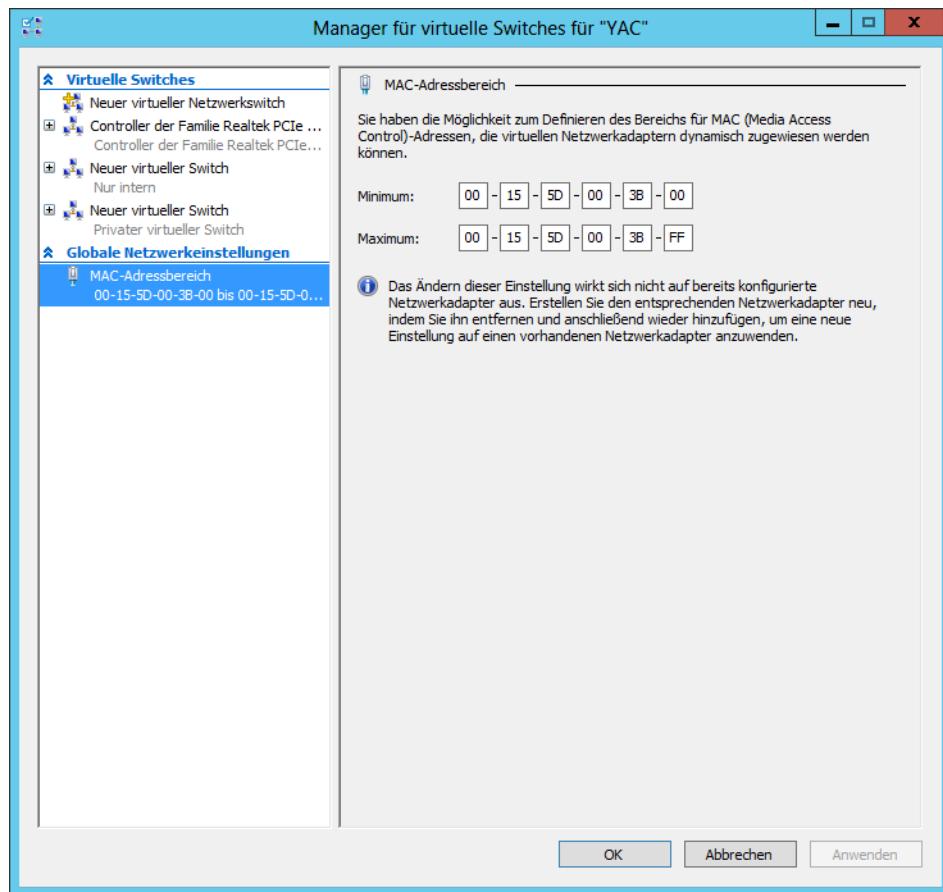


Abbildung 3.26 Der MAC-Adressbereich im Manager für virtuelle Switches

Die ersten drei Bytes des MAC-Adressbereichs lauten immer 00-15-5D. Dabei handelt es sich um eine OUI, die von Microsoft registriert wurde. Die vierten und fünften Bytes der MAC-Adresse geben die beiden letzten Bytes der – in das Hexadezimalformat konvertierten – IP-Adresse an, die dem physischen Netzwerkadapter des Servers zugeordnet wurde. Das sechste

und letzte Byte der MAC-Adresse enthält einen Wert im Bereich von 00 bis FF. Damit stehen 256 Adressen zur Verfügung.

Der Hyper-V-Server weist die MAC-Adressen den Netzwerkadapters in virtuellen Computern zu, wenn Administratoren die Adapter erstellen. Die Adapter behalten ihre MAC-Adressen permanent bei oder bis der Adapter aus dem virtuellen Computer entfernt wird. Der Server nimmt die nicht verwendeten Adressen entgegen und verwendet sie wieder. Der Standardpool von 256 Adressen dürfte für die meisten Hyper-V-Konfigurationen mit virtuellen Computern ausreichen. Andernfalls können Sie die Werte *Minimum* und *Maximum* ändern und den Pool vergrößern. Damit keine doppelten Adressen auftreten, sollten Sie nur das vorletzte Byte ändern, wodurch sich ein Adressbereich entsprechend dem letzten Byte ergibt. Zum Beispiel umfasst der in Abbildung 3.26 gezeigte Bereich 256 Adressen mit den folgenden Werten:

00-15-1D-00-3B-00 bis 00-15-1D-00-3B-FF

Wenn Sie nur die niederwertigste Stelle des vorletzten Bytes ändern, vergrößern Sie den Pool von 256 auf ($16 * 256 =$) 4096 Adressen:

00-15-1D-00-30-00 to 00-15-1D-00-3F-FF



Achtung MAC-Adressen

Gibt es weitere Hyper-V-Server in Ihrem Netzwerk, müssen Sie bei Änderungen des MAC-Adresspools darauf achten, dass keine Möglichkeit zur Vergabe doppelter MAC-Adressen entsteht. Andernfalls ist mit Netzwerkproblemen zu rechnen.

Virtuelle Netzwerkadapter erstellen

Mit den virtuellen Switches, die Sie im Hyper-V-Manager erstellt haben, können Sie virtuelle Computer anschließen, indem Sie virtuelle Netzwerkadapter erstellen und konfigurieren.

Wenn Sie einen neuen virtuellen Computer erstellen, umfasst die Standardkonfiguration einen virtuellen Netzwerkadapter. Auf der Seite *Netzwerk konfigurieren* des Assistenten für neue virtuelle Computer können Sie einen der virtuellen Switches auswählen, die Sie erstellt haben.

Wenn Sie beim Installieren von Hyper-V nur den standardmäßigen externen virtuellen Switch erstellt haben und sich ein virtueller Computer mit diesem Switch verbindet, wird das System mit dem physischen Netzwerk verknüpft. Möchten Sie zusätzliche Netzwerkadapter in Ihren virtuellen Computern erstellen, müssen Sie die folgenden Schritte ausführen:

1. Melden Sie sich bei dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Hyper-V-Manager*, um die Konsole *Hyper-V-Manager* zu öffnen.
3. Wählen Sie im linken Fensterbereich einen Hyper-V-Server aus.
4. Wählen Sie in der Liste *Virtuelle Computer* einen virtuellen Computer aus und klicken Sie im Fensterbereich *Aktionen* auf *Einstellungen*. Es erscheint das Dialogfeld *Einstellungen* für den virtuellen Computer.

5. In der Liste *Hardware hinzufügen* wählen Sie *Netzwerkadapter* aus und klicken auf *Hinzufügen*. In der Liste *Hardware* erscheint ein neuer Adapter, wie Abbildung 3.27 zeigt.

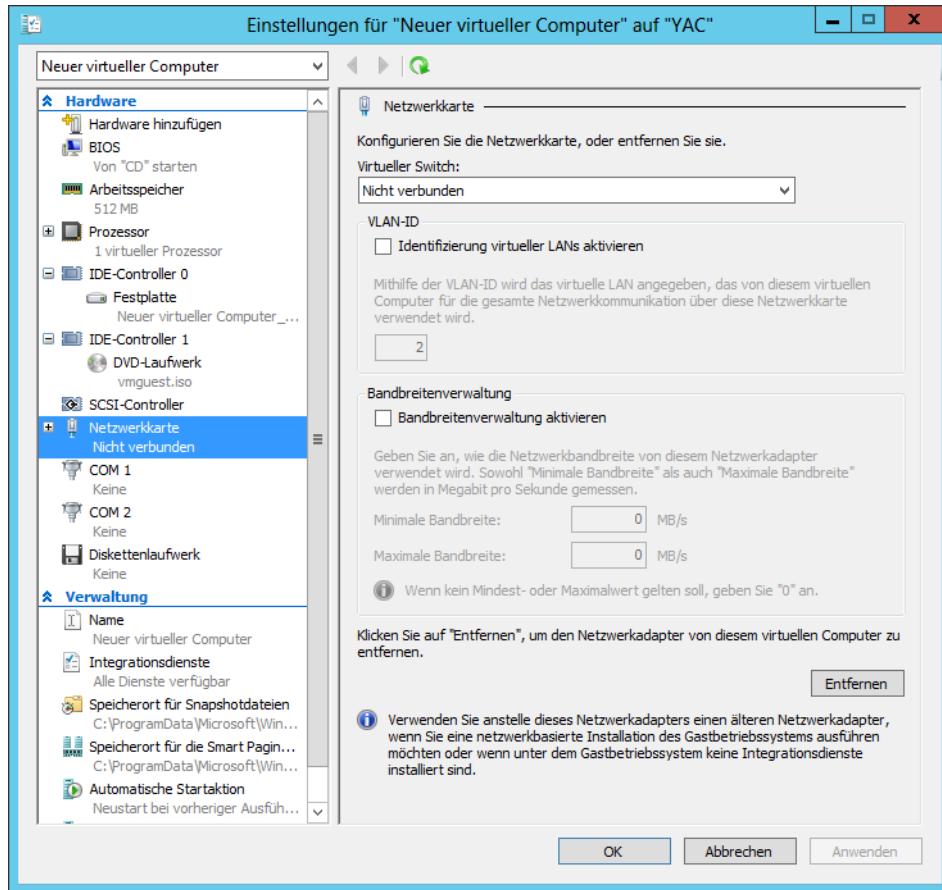


Abbildung 3.27 Ein neuer Netzwerkadapter im Dialogfeld *Einstellungen*

6. Wählen Sie in der Liste *Virtueller Switch* den Switch aus, den Sie mit dem Netzwerkadapter verbinden möchten.
7. Wenn Ihr Hostcomputer mit einer physischen Switch-Infrastruktur verbunden ist, die mithilfe von VLANs separate Subnetze erstellt, können Sie das Kontrollkästchen *Identifizierung virtueller LANs aktivieren* setzen und einen VLAN-Bezeichner eingeben, um den Netzwerkadapter einem bestimmten VLAN in Ihrem physischen Netzwerk zuzuordnen.
8. Um die Netzwerkbandbreite festzulegen, die für den Netzwerkadapter reserviert wird, setzen Sie das Kontrollkästchen *Bandbreitenverwaltung aktivieren* und geben die Werte für die Einstellungen *Minimale Bandbreite* und *Maximale Bandbreite* ein.
9. Klicken Sie auf *OK*. Die Einstellungen werden in der Konfiguration des virtuellen Computers gespeichert.

Auf einem Windows Server 2012-Hyper-V-Server lassen sich bis zu 12 Netzwerkadapter einrichten: 8 synthetische und 4 emulierte.

Synthetische und emulierte Adapter

Wenn Sie auf der Seite *Hardware hinzufügen* die Option *Netzwerkadapter* auswählen, wird ein Adapter erstellt, der in der Hyper-V-Terminologie als *synthetischer Netzwerkadapter* bezeichnet wird. Hyper-V unterstützt zwei Arten von Netzwerk- und Speicheradapters: synthetische und emulierte (manchmal auch als *ältere Adapter* bezeichnet).

Ein synthetischer Adapter ist ein rein virtuelles Gerät, das keinem realen Produkt entspricht. Synthetische Geräte in einem virtuellen Computer, die auf einer untergeordneten Partition ausgeführt werden, kommunizieren mit der übergeordneten Partition über einen Hochgeschwindigkeitskanal, den sogenannten *VMBus*.

Die virtuellen Switches, die Sie in Hyper-V anlegen, residieren in der übergeordneten Partition und sind Bestandteil einer als Dienstanbieter für Netzwerkvirtualisierung (Virtualization Service Provider, VSP) bezeichneten Komponente. Der synthetische Netzwerkadapter in der untergeordneten Partition ist ein Virtualisierungsdienstclient (Virtualization Service Client, VSC). Sowohl VSP als auch VSC sind mit dem VMBus verbunden, sodass die Kommunikation zwischen Partitionen möglich ist (siehe Abbildung 3.28). Der VSP (in der übergeordneten Partition) bietet dem VSC (in der untergeordneten Partition) Zugriff auf die physische Hardware im Hostcomputer – sprich den physischen Netzwerkadapter.

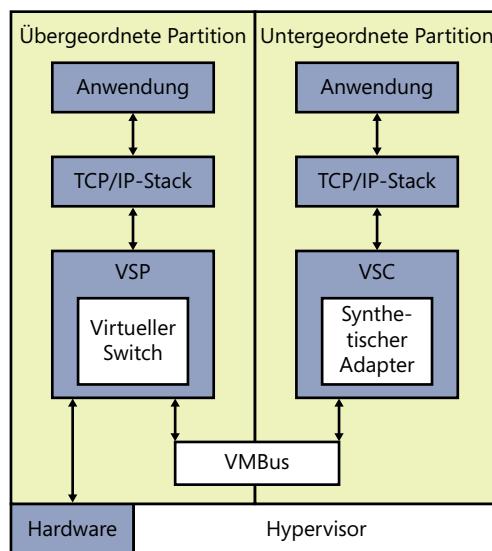


Abbildung 3.28 Synthetische Netzwerkadapter kommunizieren über den VMBus

Da synthetische Adapter über den VMBus auf die Hardware zugreifen können, gewährleisten sie ein wesentlich höheres Leistungs niveau als die alternativen emulierten Adapter.

Synthetische Adapter werden im Rahmen der Integrationsdienste implementiert, die auf den

unterstützten Gastbetriebssystemen laufen. Nachteilig bei synthetischen Netzwerkadapters ist vor allem, dass sie erst funktionsfähig sind, wenn das Betriebssystem auf dem virtuellen Computer geladen ist.

Bei einem emulierten Adapter – auch »älterer Adapter« genannt – handelt es sich um einen Standardnetzwerkadaptertreiber. Er kommuniziert mit der übergeordneten Partition über direkte Aufrufe zum Hypervisor, der extern zu den Partitionen ist (siehe Abbildung 3.29). Dieses Kommunikationsverfahren ist beträchtlich langsamer als der VMBus, den synthetische Netzwerkadapter verwenden, und demzufolge auch weniger erstrebenswert.

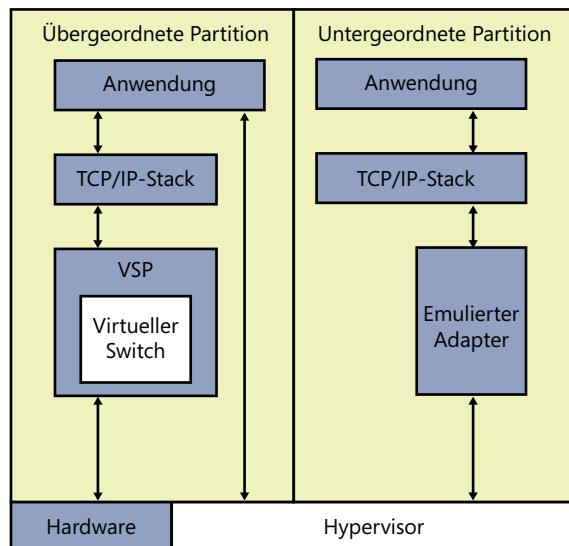


Abbildung 3.29 Emulierte Netzwerkadapter kommunizieren mithilfe des Hypervisors

Einen emulierten Adapter installieren Sie nach dem gleichen Verfahren, wie es weiter oben beschrieben wurde, außer dass Sie in der Liste *Hardware hinzufügen* den Eintrag *Ältere Netzwerkkarte* auswählen. Im Unterschied zu synthetischen Adapters laden emulierte Adapter ihre Treiber vor dem Betriebssystem. Deshalb ist es möglich, den virtuellen Computer mithilfe von PXE (Preboot eXecution Environment) zu booten und ein Betriebssystem über das Netzwerk bereitzustellen.

Dies ist eines der beiden Szenarios, in denen ein emulierter Adapter einem synthetischen Adapter vorzuziehen ist. Im anderen Szenario installieren Sie ein Betriebssystem auf Ihren virtuellen Computern, für die kein Integrationsdienste-Paket verfügbar ist.

Einstellungen zur Hardwarebeschleunigung konfigurieren

Manche physischen Netzwerkadapters besitzen Features, die die Performance verbessern sollen. Dazu werden bestimmte Funktionen vom Systemprozessor auf Komponenten ausgelagert, die im Adapter selbst realisiert sind. Hyper-V beherrscht einige dieser Features, solange die Hardware im physischen Netzwerkadapter sie ordnungsgemäß unterstützt.

Wenn Sie im Dialogfeld *Einstellungen* eines virtuellen Computers einen Netzwerkadapter erweitern, können Sie die Seite *Hardwarebeschleunigung* öffnen. Hier lassen sich die folgenden Einstellungen für die Hardwarebeschleunigung konfigurieren:

- **Warteschlange für virtuelle Computer aktivieren** Eine Warteschlange für virtuelle Computer (Virtual Machine Queue, VMQ) speichert eingehende Pakete, die für virtuelle Computer vorgesehen sind, in separaten Warteschlangen auf dem physischen Netzwerkadapter und liefert sie direkt an die virtuellen Computer. Diese Technik umgeht die Verarbeitung, die normalerweise der virtuelle Switch auf der übergeordneten Partition durchführt.
- **IPSec-Taskabladung aktivieren** Verwendet die Komponenten im Netzwerkadapter, um kryptografische Funktionen zu realisieren, wie sie für IPSec erforderlich sind. Außerdem können Sie die maximale Anzahl von Sicherheitszuordnungen festlegen, die der Adapter berechnen können soll.
- **E/A-Virtualisierung mit Einzelstamm** Aktiviert den virtuellen Adapter, um von den Vorteilen der SR-IOV-Funktionen des physischen Adapters zu profitieren

Erweiterte Features von Netzwerkadapters konfigurieren

Die Seite *Erweiterte Features* bietet unter anderem folgende zusätzliche Optionen für Funktionen von Netzwerkadapters:

- **MAC-Adresse** Standardmäßig weist der Hyper-V-Server virtuellen Netzwerkadapters eine MAC-Adresse dynamisch zu. Mit der Option *Statisch* können Sie aber festlegen, dass eine statische MAC-Adresse erstellt wird. Dabei ist lediglich zu gewährleisten, dass kein anderer – virtueller oder physischer – Adapter im selben Netzwerk dieselbe Adresse verwendet.
- **Spoofing von MAC-Adressen aktivieren** Ist diese Einstellung aktiviert, kann der Port im virtuellen Switch, an den der virtuelle Netzwerkadapter angeschlossen ist, Pakete senden und empfangen, die eine beliebige MAC-Adresse enthalten. Der virtuelle Switch-Port kann auch neue MAC-Adressen lernen und sie in seine Weiterleitungstabelle aufnehmen.
- **DHCP-Wächter aktivieren** Verhindert, dass der Adapter Nachrichten verarbeitet, die von nicht autorisierten DHCP-Servern gesendet werden
- **Portspiegelung** Bei dieser Einstellung kann der Adapter alle Pakete, die er über das Netzwerk empfängt, an einen anderen virtuellen Computer weiterleiten, um sie beispielsweise durch eine Anwendung wie den Netzwerkmonitor analysieren zu lassen
- **NIC-Teamvorgang** Ermöglicht dem Adapter, seine Bandbreite zu der anderer Adapter im selben Gastbetriebssystem in einer NIC-Teamvorgang-Struktur hinzuzufügen

Konfigurationen virtueller Netzwerke erstellen

Mit Hyper-V lässt sich nahezu jede vorhandene physische Netzwerkkonfiguration in ihren virtuellen Raum erweitern oder ein vollkommen separates und isoliertes Netzwerk innerhalb der Hyper-V-Umgebung einrichten.

Die grundlegende Standardkonfiguration eines virtuellen Hyper-V-Computers verbindet dessen Netzwerkadapter mit einem externen virtuellen Switch und somit das Gastbetriebssystem des virtuellen Computers mit dem äußeren Netzwerk. Der virtuelle Computer kann dann von den Diensten profitieren, die im äußeren Netzwerk laufen, und Daten über Router an andere Netzwerke einschließlich des Internets senden.

Mit einer derartigen Anordnung können Administratoren viele physische Server in virtuellen Computern auf einem einzigen Hyper-V-Server zusammenfassen und ihnen somit den Zugriff auf das gesamte Netzwerk erlauben. Es gibt hier keinen Unterschied zwischen dem physischen Netzwerk und der virtuellen Variante im Hyper-V-Raum.

Ein Produktionsnetzwerk in den virtuellen Raum erweitern

In einem Hyper-V-Server können mehrere physische Netzwerkadapter installiert sein, die mit verschiedenen Netzwerken verbunden sind, um den Datenverkehr zu trennen, oder mit demselben Netzwerk, um die verfügbare Bandbreite zu erhöhen. Gegebenenfalls gibt es auch Adapter, die SAN-Verbindungen für freigegebenen Speicher und Servercluster zugeordnet sind.

Microsoft empfiehlt, in einem Hyper-V-Server mindestens zwei physische Netzwerkadapter einzusetzen, wobei der eine Adapter die übergeordnete Partition bedient und der andere mit den untergeordneten Partitionen verbunden ist. Besitzt der Server mehr als zwei physische Adapter, können Sie separate externe virtuelle Netzwerkswitches für die physischen Adapter einrichten und jeden mit einem eigenen virtuellen Computer verbinden.

Ein isoliertes Netzwerk erstellen

Für Test- und Evaluierungszwecke oder für Schulungsraumsituationen ist es zweckmäßig, isolierte Netzwerkumgebungen zu schaffen. Mit internen oder privaten virtuellen Switches können Sie ein Netzwerk aufbauen, das nur innerhalb des Hyper-V-Raums existiert, wobei die übergeordnete Partition eingebunden sein kann oder nicht.

Die Stärken eines derartig isolierten Netzwerks sind gleichzeitig seine Schwächen. Wenn Sie die Gastbetriebssysteme über die Windows-Bereitstellungsdienste installieren oder die virtuellen Computer mithilfe von DHCP konfigurieren möchten, müssen Sie diese Dienste in Ihrem privaten Netzwerk installieren und konfigurieren. Zudem haben die Gastbetriebssysteme keinen Zugriff auf das Internet, sodass sie auch keine Betriebssystemupdates herunterladen können. In diesem Fall müssen Sie passende Ersatzlösungen im privaten Netzwerk bereitstellen.

Die Systeme lassen sich mit Updates versorgen, wenn Sie zwei Netzwerkadapter auf jedem Ihrer virtuellen Computer installieren, wobei Sie einen an einen privaten Switch anschließen

und den anderen an einen externen Switch. Damit sind die virtuellen Computer in der Lage, sowohl auf das Internet als auch auf das private Netzwerk zuzugreifen.

Ein isoliertes Netzwerk können Sie auch mit VLANs erstellen. Dies ist insbesondere hilfreich, wenn virtuelle Computer auf verschiedenen Hyper-V-Servern residieren, die Sie dem isolierten Netzwerk hinzufügen möchten. Indem Sie die Netzwerkadapter mit einem externen Switch verbinden und sie mit demselben VLAN-Bezeichner konfigurieren, können Sie ein Netzwerk innerhalb eines Netzwerks einrichten, das das VLAN gegenüber anderen Computern isoliert. Zum Beispiel können Sie einen DHCP-Server in Ihrem VLAN bereitstellen, ohne dass Konflikte mit den anderen DHCP-Servern in Ihrer Produktionsumgebung auftreten.

Prüfungszielzusammenfassung

- Netzwerke stellen einen entscheidenden Bestandteil in einer Infrastruktur mit virtuellen Computern dar. Je nach Ihrem Netzwerkplan können die virtuellen Computer, die Sie auf einem Windows Server 2012-Hyper-V-Server einrichten, eine Kommunikation mit anderen virtuellen Computern, mit den Computern in Ihrem physischen Netzwerk und mit dem Internet erfordern.
- Ein virtueller Switch ist wie sein physisches Gegenstück ein Gerät, das auf der Schicht 2 des OSI (Open Systems Interconnect)-Referenzmodells arbeitet. Ein Switch besitzt eine Reihe von Ports (Anschlüssen), die jeweils mit dem Netzadapter eines Computers verbunden sind. Jeder mit dem Switch verbundene Computer kann Daten auf jeden anderen Computer, der mit demselben Switch verbunden ist, übertragen.
- Hyper-V in Windows Server 2012 unterstützt drei Arten von Switches: externe, interne und private. Diese müssen Sie im Manager für virtuelle Switches erstellen, bevor Sie virtuelle Computer mit ihnen verbinden können
- Jeder Netzwerkadapter besitzt eine MAC-Adresse – manchmal auch als *Hardwareadresse* bezeichnet –, die das Gerät im Netzwerk eindeutig kennzeichnet
- Nachdem Sie in Hyper-V-Manager virtuelle Switches erstellt haben, können Sie virtuelle Computer mit ihnen verbinden, indem Sie virtuelle Netzwerkadapter erstellen und konfigurieren
- Wenn Sie auf der Seite *Hardware hinzufügen* die Option *Netzwerkadapter* auswählen, wird ein Adapter erstellt, der in der Hyper-V-Terminologie als *synthetischer Netzwerkadapter* bezeichnet wird. Hyper-V unterstützt zwei Arten von Netzwerk- und Speicheradapters: synthetische und emulierte (auch als *ältere Netzwerkadapter* bezeichnet).

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Gründe sprechen dafür, einen emulierten Netzwerkadapter statt eines synthetischen zu verwenden? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Sie möchten das Gastbetriebssystem mithilfe eines Windows-Bereitstellungsdienst-Servers installieren.
 - B. Für das geplante Gastbetriebssystem ist kein Integrationsdienste-Paket verfügbar.
 - C. Der Hersteller Ihres physischen Netzwerkadapters hat noch keinen synthetischen NetzwerkadAPTERtreiber bereitgestellt.
 - D. Der emulierte Netzwerkadapter bietet eine bessere Performance.
2. Welche der folgenden Aussagen trifft auf synthetische Netzwerkadapter nicht zu?
 - A. Synthetische Adapter kommunizieren mit der übergeordneten Partition über den VMBus.
 - B. Synthetische Adapter setzen voraus, dass das Integrationsdienste-Paket auf dem Gastbetriebssystem installiert ist.
 - C. Synthetische Adapter bieten eine bessere Performance als emulierte Adapter.
 - D. Synthetische Adapter können den untergeordneten virtuellen Computer über einen PXE-Netzwerkboot starten.
3. Wie viele Ports werden von einem virtuellen Hyper-V-Switch maximal unterstützt?
 - A. 8
 - B. 256
 - C. 4096
 - D. Unbegrenzt
4. Welche der folgenden virtuellen Switch-Typen erlauben es Gastbetriebssystemen nicht, mit der übergeordneten Partition zu kommunizieren?
 - A. Extern
 - B. Intern
 - C. Privat
 - D. Isoliert

5. Wie viele dynamisch zugewiesene MAC-Adressen kann ein Hyper-V-Server standardmäßig bereitstellen?
 - A. 8
 - B. 256
 - C. 4096
 - D. Unbegrenzt



Gedankenexperiment Wenden Sie im folgenden Gedankenexperiment die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Ralph hat einen Windows Server 2012-Hyper-V-Server mit einem physischen Netzwerkadapter und einem externen Switch, der an diesen Adapter angeschlossen ist. Bei dieser Anordnung können die virtuellen Computer auf dem Server Betriebssystemupdates automatisch aus dem Internet herunterladen. Allerdings möchte Ralph die virtuellen Computer auf dem Hyper-V-Server einsetzen, um ein isoliertes Testnetzwerk einzurichten, in dem er neue Softwareprodukte evaluieren kann. Das Testnetzwerk muss seinen eigenen DHCP-Server besitzen, der keine Konflikte mit den DHCP-Servern im Produktionsnetzwerk verursacht.

Wie kann Ralph das benötigte Testnetzwerk aus seinen virtuellen Computern konstruieren, ohne die Konfiguration zu ändern, die den Computern den Zugang zum Internet ermöglichen?

Antworten

Dieser Abschnitt enthält die Lösungen für die Gedankenexperimente und Antworten auf die Fragen der Lernzielkontrollen in diesem Kapitel.

Prüfungsziel 3.1: Kontrolle

1. **Richtige Antworten:** B, C
 - A. **Falsch:** Bei Typ-1-Virtualisierung wird der Hypervisor nicht unter einem Hostbetriebssystem ausgeführt.
 - B. **Richtig:** Ein Typ-1-Hypervisor wird direkt auf der Computerhardware ausgeführt.
 - C. **Richtig:** Ein Typ-2-Hypervisor wird unter einem Hostbetriebssystem ausgeführt.
 - D. **Falsch:** Bei Typ-2-Virtualisierung wird der Hypervisor nicht direkt auf der Computerhardware ausgeführt.
2. **Richtige Antwort:** A
 - A. **Richtig:** Typ-1-Virtualisierung bietet die beste Performance, da der Hypervisor direkt auf der Computerhardware ausgeführt wird und der Overhead eines Hostbetriebssystems entfällt.

- B. **Falsch:** Bei Typ-2-Virtualisierung ist die Performance geringer als bei Typ 1, da die Prozessorzeit mit dem Hostbetriebssystem geteilt werden muss.
- C. **Falsch:** Der Begriff Präsentationsvirtualisierung beschreibt die Funktionalität der Remotedesktopdienste unter Windows und hat nichts mit der Virtualisierung von Servern zu tun.
- D. **Falsch:** RemoteApp ist eine Technologie, um einzelne Anwendungen zu virtualisieren und sie mithilfe der Remotedesktopdienste bereitzustellen.
3. **Richtige Antwort: B**
- A. **Falsch:** Hyper-V Server umfasst keine Lizenz für virtuelle Instanzen.
- B. **Richtig:** Windows Server 2012 Datacenter Edition umfasst eine Lizenz, die es Ihnen erlaubt, eine unbegrenzte Anzahl von virtuellen Instanzen zu erstellen.
- C. **Falsch:** Windows Server 2012 Standard Edition umfasst eine Lizenz, die es Ihnen erlaubt, zwei virtuelle Instanzen zu erstellen.
- D. **Falsch:** Windows Server 2012 Foundation Edition bietet keine Unterstützung für Hyper-V.
4. **Richtige Antworten: A, B, D**
- A. **Richtig:** Smart Paging ermöglicht den Neustart eines virtuellen Computers, selbst wenn die als Startwert festgelegte RAM-Größe nicht zur Verfügung steht. Bei Smart Paging verwendet das System Festplattenplatz als temporären Ersatz für den Hauptspeicher während eines Systemneustarts.
- B. **Richtig:** Dynamischer Speicher erlaubt es Ihnen, einen Wert für *Minimaler RAM* anzugeben, der kleiner als der Wert für *Arbeitsspeicher beim Start* ist, wobei aber Smart Paging dafür sorgt, dass das System mit diesen Parameter funktioniert.
- C. **Falsch:** Mit der Einstellung *Arbeitsspeicherumfang* steuert Windows die Reservierung von Speicher für die einzelnen virtuellen Computer, beeinflusst aber nicht die Startfähigkeit eines Systems.
- D. **Richtig:** Ein Gastbetriebssystem benötigt die *Integrationsdienste*, um dynamischen Arbeitsspeicher verwenden zu können.
5. **Richtige Antwort: C**
- A. **Falsch:** Die Instanz des Betriebssystems, auf dem Sie Hyper-V installieren, wird nicht zum Hypervisor.
- B. **Falsch:** Die Instanz des Betriebssystems, auf dem Sie Hyper-V installieren, wird nicht zum VMM.
- C. **Richtig:** Die Instanz des Betriebssystems, auf dem Sie die Hyper-V-Rolle installieren, wird zur übergeordneten Partition.
- D. **Falsch:** Die Instanz des Betriebssystems, auf dem Sie die Hyper-V-Rolle installieren, wird nicht zur untergeordneten Partition.

Prüfungsziel 3.1: Gedankenexperiment

Alice kann dynamischen Speicher auf jedem der acht virtuellen Computer aktivieren und den Wert *Minimaler RAM* jedes Computers auf 512 MB setzen. Damit kann jeder virtuelle Computer mit 1024 MB Hauptspeicher starten und dann seinen Speicherbedarf verringern, was den Start des nächsten Computers ermöglicht.

Prüfungsziel 3.2: Kontrolle

1. **Richtige Antwort:** B
 - A. **Falsch:** VHDX-Dateien können bis zu 64 TB groß sein, während VHD-Dateien auf 2 TB begrenzt sind.
 - B. **Richtig:** Sowohl Windows Server 2012 als auch Windows 8 können VHDX-Dateien öffnen.
 - C. **Falsch:** VHDX-Dateien unterstützen Blockgrößen bis zu 256 MB.
 - D. **Falsch:** VHDX-Dateien können die 4096-Blockgrößen unterstützen, die auf manchen neueren Laufwerken gegeben sind.
2. **Richtige Antwort:** B
 - A. **Falsch:** Ein Pass-Through-Datenträger muss sich im Gastbetriebssystem, das auf ihn zugreift, im Onlinestatus befinden.
 - B. **Richtig:** Ein Pass-Through-Datenträger muss sich im übergeordneten Container im Offlinestatus befinden, damit das Gastbetriebssystem exklusiv darauf zugreifen kann.
 - C. **Falsch:** Ein Pass-Through-Datenträger lässt sich mit beliebigen Controllertypen verbinden.
 - D. **Falsch:** Einen Pass-Through-Datenträger fügen Sie einem virtuellen Computer nicht mit dem Snap-In *Datenträgerverwaltung* hinzu, sondern mithilfe von Hyper-V-Manager.
3. **Richtige Antwort:** D
 - A. **Falsch:** VHD- oder VHDX-Dateien können Sie zusammenführen.
 - B. **Falsch:** Zur Bearbeitung können Sie nur eine Festplatte auswählen.
 - C. **Falsch:** Für das Zusammenführen eines Datenträgers gibt es keine Anforderungen in Bezug auf freien Speicherplatz.
 - D. **Richtig:** Die Funktion *Zusammenführen* erscheint nur, wenn Sie eine differenzierende Festplatte zur Bearbeitung auswählen. Die Funktion hat das Ziel, die Daten der differenzierenden Festplatte mit den Daten der übergeordneten Festplatte zusammenzufassen.
4. **Richtige Antworten:** A, D
 - A. **Richtig:** Snapshots verbrauchen Festplattenplatz, der sich besser für andere Zwecke verwenden ließe.
 - B. **Falsch:** Snapshots setzen keine doppelte Speicherreservierung voraus.

- C. **Falsch:** Unter typischen Bedingungen dauert es nicht mehrere Stunden, bis Snapshots erstellt sind.
- D. **Richtig:** Der Hyper-V-Server muss Snapshots jedes Mal suchen und verarbeiten, wenn er auf die Festplattenlaufwerke eines virtuellen Computers zugreift, wodurch seine Leistung sinkt.
5. **Richtige Antwort:** D
- A. **Falsch:** Bevor Sie einem virtuellen Computer einen Fibre Channel-Adapter hinzufügen können, müssen Sie erst ein Fibre Channel-SAN einrichten.
- B. **Falsch:** Bevor Sie virtuelle Fibre Channel-Komponenten erstellen können, müssen Sie über einen physischen Fibre Channel-Adapter verfügen.
- C. **Falsch:** Der Treiber für Ihren physischen Fibre Channel-Adapter muss virtuelle Netzwerke unterstützen.
- D. **Richtig:** SCSI-Kabel sind für Fibre Channel-Installationen nicht erforderlich.

Prüfungsziel 3.2: Gedankenexperiment

Ed sollte die VHD-Datei mit dem folgenden Windows PowerShell-Befehl erstellen:

```
New-VHD -Path c:\servera.vhdx -Fixed -SizeBytes 500GB -LogicalSectorSizeBytes 4096 -SourceDisk 0
```

Prüfungsziel 3.3: Kontrolle

1. **Richtige Antworten:** A, B
- A. **Richtig:** Eine Windows-Bereitstellungsserver-Installation erfordert einen Adapter, um PXE zu unterstützen, was zwar emulierte Adapter beherrschen, synthetische Adapter jedoch nicht.
- B. **Richtig:** Treiber für synthetische Adapter werden im Rahmen des Integrationsdienst-Pakets installiert. Ist für das Gastbetriebssystem kein Paket verfügbar, gibt es keine synthetischen Treiber.
- C. **Falsch:** Treiber für synthetische Adapter werden von Hardwareherstellern nicht bereitgestellt.
- D. **Falsch:** Synthetische Adapter bieten eine bessere Performance als emulierte Adapter.
2. **Richtige Antwort:** D
- A. **Falsch:** Synthetische Adapter verwenden den schnelleren VMBus, um mit der übergeordneten Partition zu kommunizieren; emulierte Adapter müssen Aufrufe zum Hypervisor ausführen.
- B. **Falsch:** Treiber synthetischer Adapter werden im Rahmen des Integrationsdienst-Pakets auf dem Gastbetriebssystem installiert.

- C. **Falsch:** Wegen ihrer effizienteren Kommunikation mit der übergeordneten Partition schneiden synthetische Adapter leistungsmäßig besser ab als emulierte Adapter.
- D. **Richtig:** Synthetische Netzwerkadapter werden mit den Integrationsdiensten auf dem Gastbetriebssystem geladen und können demnach keine PXE unterstützen.
3. **Richtige Antwort: D**
- A. **Falsch:** Auf acht Verbindungen beschränkte Switches erweisen sich in vielen Hyper-V-Installationen als unzureichend.
- B. **Falsch:** Hyper-V-Switches sind nicht auf 256 Verbindungen beschränkt.
- C. **Falsch:** Hyper-V-Switches sind nicht auf 4096 Verbindungen beschränkt.
- D. **Richtig:** Virtuelle Hyper-V-Switches können eine unbeschränkte Anzahl von Verbindungen unterstützen.
4. **Richtige Antwort: C**
- A. **Falsch:** Externe Switches ermöglichen den Gastbetriebssystemen, mit dem äußeren Netzwerk und der übergeordneten Partition zu kommunizieren.
- B. **Falsch:** Interne Switches ermöglichen den Gastbetriebssystemen, mit der übergeordneten Partition zu kommunizieren, jedoch nicht mit dem äußeren Netzwerk.
- C. **Richtig:** Private Switches ermöglichen den Gastbetriebssystemen, miteinander zu kommunizieren, nicht jedoch mit dem äußeren Netzwerk oder mit der übergeordneten Partition.
- D. **Falsch:** Isoliert ist kein technischer Begriff, der sich auf einen virtuellen Switch-Typ bezieht.
5. **Richtige Antwort: B**
- A. **Falsch:** Ein Pool von acht MAC-Adressen dürfte für viele Hyper-V-Installationen unzureichend sein.
- B. **Richtig:** Ein Hyper-V-Server stellt standardmäßig einen Pool von 256 MAC-Adressen bereit. Indem Sie den Standardadressbereich bearbeiten, können Sie diese Anzahl auch vergrößern.
- C. **Falsch:** Hyper-V reserviert standardmäßig lediglich ein Byte der MAC-Adresse für einen dynamischen Wert. Dies genügt nicht, um 4096 Adressen zu unterstützen.
- D. **Falsch:** Hyper-V erzeugt einen endlichen Pool von MAC-Adressen, indem minimale und maximale Adresswerte spezifiziert werden.

Prüfungsziel 3.3: Gedankenexperiment

Ralph kann eine isolierte Testumgebung einrichten, ohne die Konfiguration der virtuellen Switches zu ändern. Dazu setzt er in jedem virtuellen Computer das Kontrollkästchen *Identifizierung virtueller LANs aktivieren* für den Netzwerkadapter und weist allen virtuellen Computern, die er in das Testnetzwerk aufnehmen möchte, dieselben VLAN-Bezeichner zu.

K A P I T E L 4

Kernnetzwerkdienste bereitstellen und konfigurieren

Dieses Kapitel beschäftigt sich mit den lebenswichtigen Infrastrukturdiensten, die nahezu jedes Netzwerk implementieren muss. Jeder Computer in einem TCP/IP-Netzwerk muss mindestens über eine IP (Internet Protocol)-Adresse verfügen und die meisten der heutigen Netzwerke verwenden das DHCP (Dynamic Host Configuration Protocol), um diese Adressen zuzuweisen. Damit TCP/IP-Computer auf Ressourcen im Internet zugreifen und Active Directory-Domänendienste (AD DS)-Domänencontroller finden können, müssen sie auf einen DNS (Domain Name System)-Server zugreifen können. Windows Server 2012 beinhaltet alle diese Dienste und liefert die Tools mit, um sie zu verwalten.

Prüfungsziele in diesem Kapitel:

- Prüfungsziel 4.1: IPv4- und IPv6-Adressierung 218
- Prüfungsziel 4.2: Den DHCP-Dienst bereitstellen und konfigurieren 237
- Prüfungsziel 4.3: Den DNS-Dienst bereitstellen und konfigurieren 253

Prüfungsziel 4.1: IPv4- und IPv6-Adressierung

Serveradministratoren müssen mit den Grundprinzipien der IPv4- und IPv6-Adressräume vertraut sein. Dieser Abschnitt untersucht diese Prinzipien und beschreibt den üblichen Ablauf, um IPv4- und IPv6-Adressierungsstrategien zu konzipieren.

Dieses Prüfungsziel zeigt, wie Sie

- IP-Adressoptionen konfigurieren
 - Subnetze konfigurieren
 - Supernetze konfigurieren
 - Interoperabilität zwischen IPv4 und IPv6 konfigurieren
 - ISATAP konfigurieren
 - Teredo konfigurieren
-

IPv4-Adressierung

Wie Sie wahrscheinlich wissen, besteht der IPv4-Adressraum aus 32-Bit-Adressen, die in Form von vier 8-Bit-Dezimalwerten von 0 bis 255 durch Punkte getrennt geschrieben werden, wie zum Beispiel 192.168.43.100. In dieser sogenannten punktierten Dezimalschreibweise bezeichnet man die einzelnen 8-Bit-Dezimalwerte als *Oktette* oder *Bytes*.

Jede Adresse besteht aus Netzwerkbits, die ein Netzwerk identifizieren, und Hostbits, die ein bestimmtes Gerät in diesem Netzwerk kennzeichnen. Um die Netzwerkbits von den Hostbits zu unterscheiden, ist für jede Adresse eine Subnetzmaske erforderlich.

Eine Subnetzmaske ist ebenfalls ein 32-Bit-Wert, der aus 1- und 0-Bits besteht. Bezogen auf eine IP-Adresse entsprechen die 1-Bits in der Maske den Netzwerkbits und die 0-Bits den Hostbits. Wenn also die weiter oben genannte IP-Adresse 192.168.43.100 eine Subnetzmaske von 255.255.255.0 (in binärer Form 11111111.11111111.11111111.00000000) besitzt, kennzeichnen die ersten drei Oktette (192.168.43) das Netzwerk und das letzte Oktett (100) den Host.

Klassenorientierte IPv4-Adressierung

Da sich die Subnetzmaske, die den IP-Adressen zugeordnet ist, ändern kann, variiert gegebenenfalls auch die Anzahl der Bits, die das Netzwerk und den Host identifizieren.

Der ursprüngliche IP-Standard definiert drei Klassen von IP-Adressen, die Netzwerke unterschiedlicher Größen unterstützen, wie Abbildung 4.1 veranschaulicht.

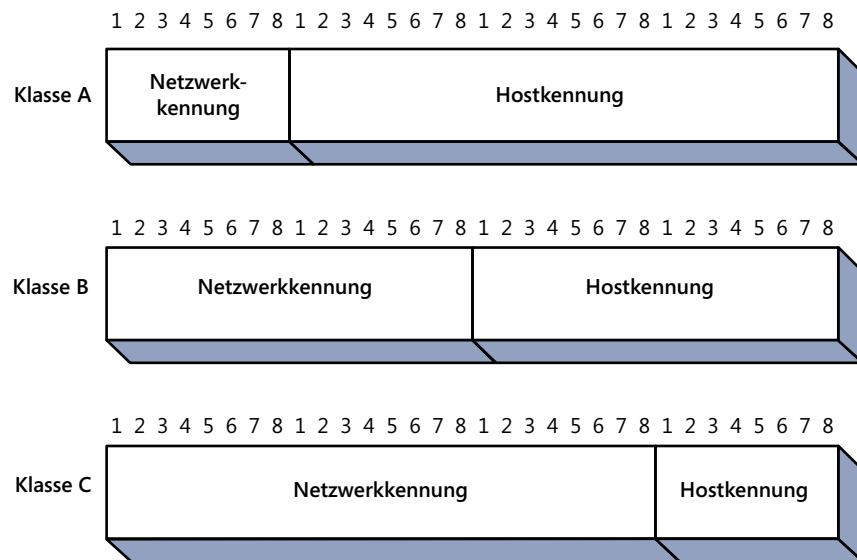


Abbildung 4.1 Die drei IPv4-Adressklassen

Tabelle 4.1 listet die Anzahl der unterstützten Netzwerke und Hosts auf, die von den jeweiligen Adressklassen unterstützt werden.

Tabelle 4.1 IPv4-Adressklassen

IP-Adressklasse	Klasse A	Klasse B	Klasse C
Erste Bitwerte (binär)	0	10	110
Erste Bitwerte (dezimal)	0 – 127	128 – 191	192 – 223
Anzahl der Netzwerksbits	8	16	24
Anzahl der Hostbits	24	16	8
Anzahl der möglichen Netzwerke	126	16.384	2.097.152
Anzahl der möglichen Hosts	16.777.214	65.534	254



Hinweis Zusätzliche Klassen

Der IP-Standard definiert neben den Klassen A, B und C noch zwei weitere Klassen: D und E. Adressen der Klasse D beginnen mit den Bitwerten 1110 und Adressen der Klasse E mit den Werten 11110. Die IANA (Internet Assigned Numbers Authority) hat Adressen der Klasse D für Multicast-Kennungen reserviert. Eine Multicast-Adresse identifiziert eine Gruppe von Computern in einem Netzwerk, die ähnliche Merkmale besitzen. Mithilfe von Multicast-Adressen sind TCP/IP-Anwendungen in der Lage, Daten an Computer zu senden, die spezifische Funktionen ausführen (beispielsweise an alle Router im Netzwerk), selbst wenn sie sich in verschiedenen Subnetzen befinden. Adressen der Klasse E sind für experimentelle Zwecke vorgesehen und bislang nicht in Gebrauch.

Die Zeile »Erste Bitwerte« in Tabelle 4.1 gibt die Werte an, die das erste, die ersten beiden oder die ersten drei Bits einer Adresse in jeder Klasse haben müssen. Frühe TCP/IP-Implementierungen haben anhand dieser Bits anstelle einer Subnetzmaske die Klasse einer Adresse bestimmt. Die Binärwerte der ersten Bits jeder Adressklasse begrenzen den möglichen Bereich der Dezimalwerte für das erste Byte der Adresse. Da zum Beispiel das erste Bit einer Adresse der Klasse A 0 sein muss, erstrecken sich die möglichen Binärwerte des ersten Bytes in einer Adresse der Klasse A von 00000000 bis 01111111 oder dezimal von 1 bis 127. Wenn Sie also eine IP-Adresse sehen, in der das erste Byte eine Zahl von 1 bis 127 ist, wissen Sie, dass es sich um eine Adresse der Klasse A handelt.

In einer Adresse der Klasse A stehen die ersten acht Bit der Adresse für die Netzwerkkennung und die verbleibenden 24 Bit für die Hostkennung. Folglich gibt es nur 126 mögliche Netzwerke der Klasse A (die Netzwerkkennung 127 ist für Diagnosezwecke reserviert), wobei aber in jedem Netzwerk bis zu 16.777.214 Netzwerkadapter adressierbar sind. Adressen der Klassen B und C verwenden mehr Bits für die Netzwerkkennung und unterstützen somit eine größere Anzahl von Netzwerken, wodurch aber weniger Bits für die Hostkennung verbleiben. Dieser Kompromiss verringert die Anzahl der Hosts, die sich in jedem Netzwerk ansprechen lassen.

Die Werte in Tabelle 4.1 für die Anzahl der Hosts, die jede Adressklasse unterstützt, scheinen zu klein zu sein. Zum Beispiel kann eine 8-Bit-Binärzahl 256 (d.h. 2⁸) mögliche Werte annehmen und nicht 254, wie es in der Tabelle für die Anzahl der Hosts bei einer Adresse der Klasse C angegeben ist. Der Wert 254 wird verwendet, weil der ursprüngliche Standard der IP-Adressierung feststellt, dass sich einzelnen Hosts keine Adressen mit »nur Nullen« oder »nur Einsen« zuweisen lassen. Die nur aus Nullen bestehende Adresse kennzeichnet das Netzwerk und keinen bestimmten Host, während die Kennung »nur Einsen« immer eine Broadcast-Adresse anzeigt. Für beide Werte gilt, dass Sie sie einem einzelnen Host nicht zuweisen dürfen. Die Anzahl der möglichen Netzwerk- oder Hostadressen, die sich mit einer gegebenen Anzahl von Bits erzeugen lassen, berechnen Sie also mit der Formel $2^x - 2$, wobei x die Anzahl der Bits angibt.

Klassenloses domänenübergreifendes Routing

Als das Internetprotokoll (IP) entwickelt wurde, konnte sich noch niemand vorstellen, dass der 32-Bit-Adressraum jemals erschöpft sein würde. In den frühen 1980er Jahren gab es keine

Netzwerke, die 65.536 Computer umfassten, geschweige denn 16 Millionen, und niemand kümmerte sich um die verschwenderische Zuteilung von IP-Adressen basierend auf diesen Klassen.

Wegen dieser Verschwendungen geriet die klassenorientierte Adressierung langsam außer Mode und wurde durch eine Reihe von Methoden mit Subnetzen – einschließlich der Subnetzmaskeierung mit variabler Länge (VLSM) und schließlich durch klassenloses domänenübergreifendes Routing (Classless Inter-Domain Routing, CIDR) abgelöst. CIDR ist eine Subnetzmethode, bei der Administratoren die Netzwerkbits von den Hostbits an beliebiger Position in der Adresse und nicht nur zwischen Oktetten trennen können. Dadurch lassen sich Netzwerke von nahezu jeder Größe aufbauen.

Außerdem führt CIDR eine neue Notation für Netzwerkadressen ein. An eine Adresse in der standardmäßigen punktierten Dezimalschreibweise schließt sich ein Schrägstrich und eine Zahl an, die die Größe des Präfixes für die Netzwerkennung angibt. Zum Beispiel stellt 192.168.43.0/24 eine einzelne Adresse der Klasse C dar, die eine 24-Bit-Netzwerkennung und die übrigen 8 Bit für bis zu 254 Hostkennungen verwendet. Jeder dieser Hosts erhält eine Adresse aus dem Bereich von 192.168.43.1 bis 192.168.43.254, wobei die Subnetzmaske 255.255.255.0 verwendet wird.

Mithilfe von CIDR kann der Administrator allerdings diese Adresse in weitere Subnetze gliedern, indem er einige der Hostbits reserviert, um Subnetze zu erstellen. Möchte der Administrator zum Beispiel Subnetze für vier Büros einrichten, kann er zwei der Hostkennungsbits heranziehen. Damit ändert sich die Netzwerkadresse in CIDR-Notation zu 192.168.43.0/26. Da die Netzwerkennung nun 26 Bit umfasst, lautet die Subnetzmaske für alle vier Netzwerke 11111111.11111111.11111111.11000000 in binärer Form oder 255.255.255.192 in der Standarddezimaldarstellung. Jedes der vier Netzwerke kann bis zu 62 Hosts umfassen, wobei die in Tabelle 4.2 gezeigten IP-Adressbereiche verwendet werden.

Tabelle 4.2 Beispiel für CIDR-Netzwerke mit der Adresse 192.168.43.0/26

Netzwerkadresse	erste IP-Adresse	letzte IP-Adresse	Subnetzmaske
192.168.43.0	192.168.43.1	192.168.43.62	255.255.255.192
192.168.43.64	192.168.43.65	192.168.43.126	255.255.255.192
192.168.43.128	192.168.43.129	192.168.43.190	255.255.255.192
192.168.43.192	192.168.43.193	192.168.43.254	255.255.255.192

Falls der Administrator mehr als vier Subnetze benötigt, ändert er die Adresse in 192.168.43.0/28 und fügt damit der Netzwerkadresse zwei Bits hinzu. Damit lassen sich dann maximal 16 Subnetze bilden, von denen jedes bis zu 14 Hosts unterstützen kann. Die Subnetzmaske für diese Netzwerke lautet demnach 255.255.255.240.

Öffentliche und private IPv4-Adressierung

Damit ein Computer aus dem Internet zugänglich ist, muss er über eine IP-Adresse verfügen, die sowohl registriert als auch eindeutig ist. Alle Webserver im Internet besitzen registrierte Adressen, genau wie alle anderen Arten von Internetservern.

Die IANA ist die oberste Quelle für alle registrierten Adressen. Diese von der ICANN (Internet Corporation for Assigned Names and Numbers) verwaltete Organisation reserviert Adressblöcke für RIRs (Regional Internet Registrys), die ihrerseits kleinere Blöcke an ISPs (Internet Service Provider) zuteilen. Möchte eine Organisation einen Server im Internet hosten, erhält sie eine registrierte Adresse normalerweise von einem ISP.

Für Arbeitsstationen, die lediglich auf Ressourcen im Internet zugreifen, sind registrierte IP-Adressen nicht erforderlich. Wenn Organisationen für alle ihre Arbeitsstationen registrierte Adressen verwendet hätten, wäre der IPv4-Adressraum schon vor langer Zeit erschöpft gewesen. Stattdessen verwenden Organisationen normalerweise private IP-Adressen für ihre Arbeitsstationen. Private IP-Adressen sind Adressblöcke, die speziell für private Netzwerkverwendung reserviert sind. Diese Adressen darf jeder verwenden, ohne sie zu registrieren, doch sind sie nicht dafür geeignet, Computer aus dem Internet zugänglich zu machen, ohne eine spezielle Technik wie zum Beispiel Netzwerkadressübersetzung (Network Address Translation, NAT) zu verwenden.

Die folgenden drei Adressblöcke sind für die private Nutzung reserviert:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Die meisten Unternehmensnetzwerke verwenden Adressen aus diesen Blöcken für ihre Arbeitsstationen. Es spielt keine Rolle, ob mehrere Organisationen auf die gleichen Adressen zurückgreifen, da die Arbeitsstationen niemals direkt mit demselben Netzwerk verbunden sind.

IPv4-Subnetze

Unternehmensadministratoren greifen in den meisten Fällen auf Adressen in einem der privaten IP-Adressbereiche zurück, um die benötigten Subnetze einzurichten. Wenn Sie ein Unternehmensnetzwerk von Grund auf neu erstellen, können Sie sich frei für einen der privaten Adressblöcke entscheiden und sich die Arbeit erleichtern, indem Sie die Subnetze an den Oktettgrenzen teilen.

Zum Beispiel können Sie mit dem privaten IP-Adressbereich 10.0.0.0/8 arbeiten und das komplette zweite Oktett als Subnetz-ID heranziehen. Es lassen sich also bis zu 256 Subnetze mit jeweils 65.536 Hosts bilden. Die Subnetzmaske für alle Adressen in den Subnetzen lautet 255.255.0.0 und es ergeben sich folgende Netzwerkadressen:

- 10.0.0.0/16
- 10.1.0.0/16
- 10.2.0.0/16

- 10.3.0.0/16
- ...
- 10.255.0.0/16

In einem vorhandenen Netzwerk scheint die Subnetzbildung schwieriger zu sein. Zum Beispiel könnten Sie einen relativ kleinen Adressbereich zugeteilt bekommen und gebeten werden, daraus eine bestimmte Anzahl von Subnetzen zu erstellen. Dabei gehen Sie wie folgt vor:

1. Bestimmen Sie, wie viele Bits für die Subnetzkennung erforderlich sind, um die verlangte Anzahl von Subnetzen zu erstellen.
2. Subtrahieren Sie die benötigten Subnetzbits von den Hostbits und addieren Sie sie zu den Netzwerksbits.
3. Berechnen Sie die Subnetzmaske, indem Sie die Netzwerk- und Subnetzbits in binärer Form addieren und den Binärwert in die Dezimaldarstellung umwandeln.
4. Nehmen Sie das niederwertigste Subnetzbit und die Hostbits in binärer Form und konvertieren Sie sie in einen Dezimalwert.
5. Inkrementieren Sie die Netzwerk kennung (einschließlich der Subnetzbits) um den berechneten Dezimalwert, um die Netzwerkadressen für Ihre neuen Subnetze zu ermitteln.

Wenn Sie bei dem weiter vorn in diesem Kapitel angegebenen Beispiel die Adresse 192.168.43.0/24 nehmen und zwei zusätzliche Bits für die Subnetzkennung reservieren, erhalten Sie für die Subnetzmaske einen binären Wert von 11111111.11111111.11111111.11000000 (255.255.255.192 im Dezimalformat, wie oben erwähnt).

Das niederwertigste Subnetzbit plus die Hostbits ergeben den Binärwert 1000000, der dem Dezimalwert 64 entspricht. Wenn Sie also wissen, dass die Netzwerkadresse Ihres ersten Subnetzes 192.168.43.0 lautet, muss das zweite Subnetz 192.168.43.64 sein, das dritte 192.168.43.128 und das vierte 192.168.43.192, wie aus Tabelle 4.2 hervorgeht.

Supernetting

CIDR vereinfacht nicht nur die Netzwerknotation, sondern erlaubt auch eine als Zusammenfassung von IP-Adressen oder Supernetting bezeichnete Technik, durch die sich die Größe der Internet-Routingtabellen reduzieren lässt. Ein Supernetz ist eine Kombination von zusammenhängenden Netzwerken, die sämtlich ein gemeinsames CIDR-Präfix enthalten. Besitzt eine Organisation mehrere zusammenhängende Netzwerke, die als Supernetz darstellbar sind, lassen sich diese Netzwerke in einer Routingtabelle auflisten, indem man nur einen Eintrag statt vieler verwendet.

Sind zum Beispiel in einer Organisation die folgenden fünf Subnetze vorhanden, würde man standardmäßig für jedes Subnetz einen separaten Tabelleneintrag anlegen:

- 172.16.43.0/24
- 172.16.44.0/24

- 172.16.45.0/24
- 172.16.46.0/24
- 172.16.47.0/24

Um ein Supernetz zu erstellen, das alle fünf Netzwerke umfasst, sind die gemeinsamen Bits der Netzwerke zu isolieren. Wenn Sie die Netzwerkadressen aus der Dezimal- in die Binärdarstellung umwandeln, erhalten Sie die folgenden Werte:

172.16.43.0	10101100.00010000.00101011.00000000
172.16.44.0	10101100.00010000.00101100.00000000
172.16.45.0	10101100.00010000.00101101.00000000
172.16.46.0	10101100.00010000.00101110.00000000
172.16.47.0	10101100.00010000.00101111.00000000

In der Binärdarstellung ist zu sehen, dass alle fünf Adressen die gleichen ersten 21 Bits aufweisen. Diese 21 Bits werden wie folgt zur Netzwerkkennung der Supernetzadresse:

10101100.00010000.00101

Wenn Sie die Hostbits auf null setzen, um die Netzwerkadresse zu bilden, und die Binärzahl in das dezimale Format zurückkonvertieren, erhalten Sie die Supernetzadresse 172.16.40.0/21:

10101100.00010000.00101000.00000000

172.16.40.0/21

Diese eine Netzwerkadresse ersetzt die ursprünglichen fünf Adressen in Routingtabellen, die im gesamten Internet dupliziert werden. Dies ist lediglich ein Beispiel für eine Technik, mit der Administratoren Dutzende oder sogar Hunderte von Subnetzen zu einzelnen Routingtabelleneinträgen zusammenfassen können.

IPv4-Adressen zuweisen

Ein Netzwerkadministrator muss nicht nur damit vertraut sein, wie die IP-Adressierung funktioniert, sondern auch die Methoden kennen, um IP-Adressen für die Computer in einem Netzwerk bereitzustellen.

Es gibt prinzipiell drei Methoden, um IPv4-Adressen zuzuweisen:

- Manuelle Konfiguration
- DHCP (Dynamic Host Configuration Protocol)
- APIPA (Automatic Private IP Addressing)

Die folgenden Abschnitte erörtern die Vor- und Nachteile dieser Methoden.

Manuelle IPv4-Adresskonfiguration

Es ist weder schwierig noch zeitaufwendig, einen TCP/IP-Client manuell zu konfigurieren. Die meisten Betriebssysteme bieten eine grafische Benutzeroberfläche, in der Sie eine IPv4-Adresse, eine Subnetzmaske und verschiedene andere TCP/IP-Konfigurationsparameter eingeben können. In Windows Server 2012 konfigurieren Sie die IP-Adresseinstellungen auf dem Eigenschaftenblatt *Internetprotokoll Version 4 (TCP/IPv4)*, wie Abbildung 4.2 zeigt.

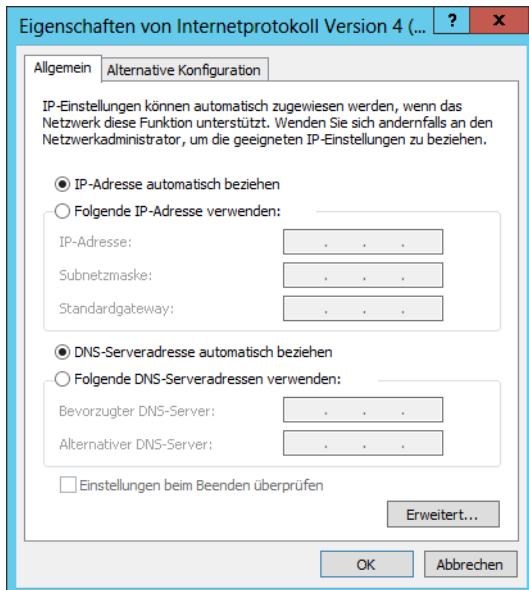


Abbildung 4.2 Das Eigenschaftenblatt *Internetprotokoll Version 4 (TCP/IPv4)*

Wenn Sie die Option *Folgende IP-Adresse verwenden* wählen, können Sie folgende Optionen für die IP-Adresse konfigurieren:

- **IP-Adresse** Legt die IP-Adresse im lokalen Subnetz fest, die die Netzwerkschnittstelle im Computer identifiziert
- **Subnetzmaske** Legt die Maske fest, die dem lokalen Subnetz zugeordnet ist
- **Standardgateway** Legt die IP-Adresse eines Routers im lokalen Subnetz fest, über den das System auf Ziele in anderen Netzwerken zugreift
- **Bevorzugter DNS-Server** Gibt die IP-Adresse des DNS-Servers an, den das System verwendet, um Hostnamen zu IP-Adressen aufzulösen

Das Hauptproblem bei manueller Konfiguration ist darin zu sehen, dass die Konfiguration, die für eine Arbeitsstation etwa zwei Minuten in Anspruch nimmt, bei 100 Servern schon mehrere Stunden und bei 1000 Computern mehrere Tage dauert. Außer bei kleinen Netzwerken ist das manuelle Konfigurieren nicht praktikabel. Und das hat nicht nur mit dem Zeitaufwand zu tun. Sie müssen nämlich auch die zugewiesenen IPv4-Adressen verfolgen und sicherstellen, dass jedes System eine eindeutige Adresse erhält. Da sich dies zu einem logistischen Albtraum ausweiten kann, entscheiden sich nur wenige Netzwerkadministratoren für diese Methode.

Das Protokoll für dynamische Hostkonfiguration (DHCP)

Bei DHCP handelt es sich um eine Anwendung und ein Protokoll auf der Anwendungsschicht. Beides zusammen versetzt Administratoren in die Lage, IP-Adressen dynamisch aus einem Pool zuzuweisen. Computer, die mit DHCP-Clients ausgestattet sind, kontaktieren beim

Startvorgang automatisch einen DHCP-Server, der ihnen eindeutige Adressen und alle anderen Konfigurationsparameter zuweist, die der TCP/IP-Client benötigt.

Der DHCP-Server vermietet gewissermaßen (»least«) den Clients die Adressen. Nach einer festgelegten Zeitspanne erneuern die Clients ihre Adressen oder geben sie an den Server zurück, der sie dann neu zuweisen kann. DHCP automatisiert nicht nur die Adressenzuweisung, sondern merkt sich auch die zugewiesenen Adressen, sodass keine doppelten Adressen im Netzwerk auftauchen.

Automatische private IP-Adressierung (APIPA)

APIPA ist die Bezeichnung von Microsoft für einen DHCP-Failover-Mechanismus, den alle aktuellen Microsoft Windows-Betriebssysteme verwenden. Auf Windows-Computern ist der DHCP-Client standardmäßig aktiviert. Wenn ein System nach mehreren Versuchen keinen DHCP-Server im Netzwerk finden kann, übernimmt APIPA und weist dem Computer automatisch eine Adresse im Netzwerk 169.254.0.0/16 zu.

Für ein kleines Netzwerk, das nur aus einem einzigen LAN (Local Area Network) besteht, ist APIPA eine einfache und effektive Alternative zur Installation eines DHCP-Servers. Bei Installationen mit mehreren LANs, die durch Router miteinander verbunden sind, müssen Administratoren jedoch mehr Kontrolle über die Zuweisung der IP-Adressen ausüben können. Das heißt normalerweise, einen oder mehrere DHCP-Server bereitzustellen.

IPv6-Adressierung

Wie die meisten Administratoren wissen, ist IPv6 dafür konzipiert, den IP-Adressraum zu vergrößern und somit Adressen für erheblich mehr Geräte als IPv4 bereitzustellen. Die IPv6-Adressbreite von 128 Bit ermöglicht 2128 Adressen – d.h. über 54 Millionen Adressen für jeden Quadratmeter Erdoberfläche.

IPv6 bietet aber nicht nur mehr Adressen, sondern verringert auch die Größe der Routingtabellen in den Routern, die über das Internet verteilt sind. Das ergibt sich daraus, dass der Umfang der Adressen mehr als die beiden Subnetzebenen bietet, die derzeit mit IPv4 möglich sind.

Einführung in IPv6

IPv6-Adressen unterscheiden sich außer ihrer Länge in mehreren Punkten von IPv4-Adressen. Anstelle der vier 8-Bit-Dezimalzahlen, die durch Punkte getrennt sind, werden IPv6 Adressen in Form von acht 16-Bit-Hexadezimalzahlen geschrieben und durch Doppelpunkte getrennt:

XX:XX:XX:XX:XX:XX:XX:XX

Jedes X steht hier für acht Bit (oder ein Byte), was in Hexadezimalschreibweise durch zwei Zeichen wie im folgenden Beispiel dargestellt wird:

21cd:0053:0000:0000:e8bb:04f2:003c:c394

IPv6-Adressen kürzen

Besteht eine IPv6-Adresse aus zwei oder mehr aufeinanderfolgenden 8-Bit-Blöcken aus Nullen, können Sie diese wie folgt durch einen doppelten Doppelpunkt ersetzen:

21cd:0053::e8bb:04f2:003c:c394

Dabei ist zu beachten, dass der doppelte Doppelpunkt in einer IPv6-Adresse nur einmal auftreten darf.

Außerdem können Sie die führenden Nullen in jedem Block wie folgt löschen:

21cd:53::e8bb:4f2:3c:c394

IPv6-Netzwerkadressen ausdrücken

In IPv6 gibt es keine Subnetzmasken. Netzwerkadressen verwenden die gleiche Notation wie CIDR, um die Netzwerksbits zu identifizieren. Im Beispiel wird die Netzwerkadresse wie folgt geschrieben:

21cd:53::/64

Dies ist die komprimierte Form für die folgende Netzwerkadresse:

21cd:0053:0000:0000:0000:0000:0000:0000/64

IPv6-Adresstypen

Im Unterschied zu IPv4 gibt es in IPv6 keine Broadcast-Übertragungen und demzufolge keine Broadcast-Adressen. IPv6 unterstützt die folgenden drei Arten von Übertragungen:

- **Unicast** Bietet einen 1:1-Übertragungsdienst zu einzelnen Schnittstellen, einschließlich Serverfarmen, die eine gemeinsame Adresse verwenden
- **Multicast** Bietet einen 1:n-Übertragungsdienst zu Gruppen von Schnittstellen, die durch eine einzelne Multicast-Adresse identifiziert werden
- **Anycast** Bietet einen 1:1:n-Übertragungsdienst zu Gruppen von Schnittstellen, wobei nur die nächstgelegene (gemessen durch die Anzahl der dazwischen liegenden Router) die Übertragung empfängt



Hinweis IPv6-Adressbereiche

In IPv6 bezieht sich der Bereich einer Adresse auf die Größe ihres funktionalen Gebiets. Zum Beispiel ist der Bereich einer globalen Unicast-Adresse unbeschränkt, umfasst also das gesamte Internet. Der Bereich einer verbindungslokalen Unicast-Adresse (Link Local Unicast) ist die unmittelbare Verbindung (Link), d.h. das lokale Netzwerk. Der Bereich einer eindeutigen lokalen Unicast-Adresse (Unique Local Unicast) umfasst alle Subnetze innerhalb einer Organisation.

Darüber hinaus unterstützt IPv6 mehrere Adresstypen, wie sie in den folgenden Abschnitten beschrieben werden.

Globale Unicast-Adressen

Eine globale Unicast-Adresse entspricht einer registrierten IPv4-Adresse, die weltweit routingfähig und im Internet eindeutig ist.

Verbindungslokale Unicast-Adressen

In IPv6 erzeugen Systeme, die sich selbst eine Adresse zuweisen, automatisch eine verbindungslokale Unicast-Adresse (Link Local Unicast), die praktisch einer APIPA-Adresse in IPv4 gleichzusetzen ist. Alle verbindungslokalen Adressen besitzen dieselbe Netzwerkkennung: ein 10-Bit-Präfix 11111110 010, gefolgt von 54 Nullen, was die folgende Netzwerkadresse ergibt:

fe80:0000:0000:0000/64

In der kompakten Schreibweise sieht die verbindungslokale Netzwerkadresse so aus:

fe80::/64

Da alle verbindungslokalen Adressen im selben Netzwerk liegen, sind sie nicht routingfähig, und Systeme, die sie verarbeiten, können nur mit anderen Systemen über dieselbe Verbindung kommunizieren.

Eindeutige lokale Unicast-Adressen

Eindeutige lokale Unicast-Adressen (Unique Local Unicast) sind das IPv6-Äquivalent der privaten IPv4-Netzwerkadressen 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16. Wie die privaten IPv4-Adressen sind eindeutige lokale Adressen routingfähig innerhalb einer Organisation. Administratoren können bei Bedarf auch Subnetze einrichten, um eine Organisation beliebiger Größe zu unterstützen.



Hinweis Veraltete IPv6-Adressen

Viele Quellen von IPv6-Informationen listen weiterhin standortlokale Unicast-Adressen (Site Local Addresses) als gültigen Unicast-Typ auf, und zwar mit einer Funktion, die der einer privaten IPv4-Netzwerkadresse ähnelt. Aus verschiedenen Gründen wurden standortlokale Unicast-Adressen verworfen und obwohl ihre Verwendung nicht verboten ist, wurde ihre Funktionalität durch eindeutige lokale Unicast-Adressen ersetzt.

Multicast-Adressen

Multicast-Adressen beginnen immer mit dem Wert 11111111 (binär) bzw. FF (hexadezimal).

Anycast-Adressen

Eine Anycast-Adresse identifiziert die Router in einem gegebenen Adressbereich und sendet die Daten an den nächsten Router, wie er durch die lokalen Routing-Protokolle bestimmt wird. Organisationen können mithilfe von Anycast-Adressen eine bestimmte Gruppe von Routern im Unternehmen identifizieren, beispielsweise diejenigen, die den Zugang zum Internet realisieren. Um Anycast-Adressen verwenden zu können, müssen die Router für die Erkennung derartiger Adressen konfiguriert sein.

IPv6-Adressen zuweisen

Das Verfahren, mit dem Administratoren den Netzwerkcomputern IPv6-Adressen zuweisen, ähnelt dem für IPv4-Adressen. Wie bei IPv4 kann ein Windows-Computer eine IPv6-Adresse nach drei möglichen Methoden erhalten:

- **Manuelle Zuweisung** Ein Benutzer oder Administrator stellt manuell eine Adresse und andere Informationen für jede Netzwerkschnittstelle bereit
- **Selbstzuweisung** Der Computer erzeugt seine eigene Adresse mithilfe einer zustandslosen Adress-Autokonfiguration
- **Dynamische Zuweisung** Der Computer erbittet und empfängt eine Adresse von einem DHCPv6-Server im Netzwerk

Manuelle IPv6-Adresszuweisung

Für den Unternehmensadministrator ist die manuelle Adresszuweisung in IPv6 wegen der Adresslänge noch unpraktischer als in IPv4. Dennoch ist sie möglich und das Verfahren ist in Windows Server 2012 das gleiche wie das für IPv4, außer dass Sie das Eigenschaftenblatt *Internetprotokoll Version 6 (TCP/IPv6)* öffnen, das Abbildung 4.3 zeigt.

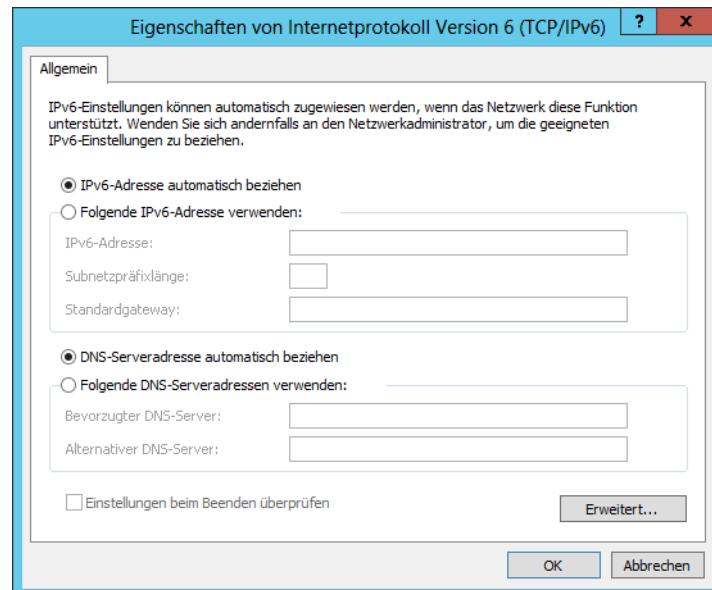


Abbildung 4.3 Das Eigenschaftenblatt *Internetprotokoll Version 6 (TCP/IPv6)*

Da es recht mühsam ist, IPv6-Adressen manuell zu bearbeiten, sind die beiden folgenden Optionen weitaus stärker verbreitet.

Zustandslose IPv6-Adressenautokonfiguration

Ein Windows-Computer initiiert beim Startvorgang die zustandslose Adressenautokonfiguration, während der er jeder Schnittstelle eine verbindungslokale Unicast-Adresse zuweist. Diese Zuweisung findet selbst dann statt, wenn die Schnittstelle später eine globale Unicast-Adresse empfängt. Die verbindungslokale Adresse ermöglicht dem System, mit dem Router in der Verbindung zu kommunizieren, was zusätzliche Anweisungen liefert.

Die Schritte der zustandslosen Adressenautokonfiguration sehen folgendermaßen aus:

1. **Verbindungslokale Adresserzeugung** Die IPv6-Implementierung auf dem System erzeugt für jede Schnittstelle eine verbindungslokale Adresse. Dazu wird die Netzwerk-adresse fe80::/64 verwendet und eine Schnittstellenkennung entweder aus der MAC-Adresse der Schnittstelle oder durch einen Pseudozufallsgenerator erzeugt.
2. **Erkennung doppelter Adressen** Nach dem IPv6-ND (Neighbor Discovery)-Protokoll ermittelt das System durch Senden einer Nachbaranfrage-Nachricht, ob ein anderer Computer in der Verbindung die gleiche Adresse verwendet, und hört auf eine Nachbarankündigungs-Nachricht, die als Antwort gesendet wird. Bleibt eine Antwort aus, betrachtet das System die Adresse als eindeutig für die Verbindung. Trifft dagegen eine Antwort ein, muss das System eine neue Adresse generieren und den Ablauf wiederholen.
3. **Verbindungslokale Adresszuweisung** Stellt das System fest, dass die verbindungslo-
kale Adresse eindeutig ist, konfiguriert es die Schnittstelle so, dass es diese Adresse ver-
wendet. In einem kleinen Netzwerk, das nur aus einem Segment oder einer Verbindung
besteht, kann dies bereits die permanente Adresszuweisung der Schnittstelle sein. In
einem Netzwerk mit mehreren Subnetzen hat die verbindungslokale Adresszuweisung
vor allem die Aufgabe, die Kommunikation des Systems mit einem Router in der Verbin-
dung zu ermöglichen.
4. **Routerankündigungsge-
such** Das System verwendet das ND-Protokoll, um Routeran-
frage-Nachrichten an die Multicast-Adresse für alle Router zu senden. Diese Nachrichten
fordern die Router auf, die Routerankündigungs-Nachrichten häufiger zu senden.
5. **Routerankündigung** Der Router in der Verbindung verwendet das ND-Protokoll, um
Routerankündigungs-Nachrichten an das System zu senden. Diese Nachrichten enthalten
Informationen, wie die Autokonfiguration weiter ablaufen soll. Die Routerankündigungs-
Nachrichten liefern normalerweise ein Netzwerkpräfix, das das System zusammen mit
seiner vorhandenen Schnittstellenkennung verwendet, um eine globale oder eindeutige
lokale Unicast-Adresse zu erzeugen. Die Nachrichten können das System auch anweisen,
eine zustandsbehaftete Autokonfiguration einzuleiten, indem es einen bestimmten
DHCPv6-Server kontaktiert. Gibt es in der Verbindung keinen Router, was das System
durch fehlenden Empfang von Routerankündigungs-Nachrichten feststellt, muss das
System versuchen, eine zustandslose Autokonfiguration einzuleiten.
6. **Globale oder eindeutige lokale Adresskonfiguration** Mit den vom Router empfan-
genen Daten generiert das System eine geeignete Adresse, die entweder global oder inner-
halb des Unternehmens routingfähig ist, und konfiguriert die Schnittstelle so, dass sie
diese Adresse verwendet. Wenn das System dazu aufgefordert wird, kann es auch eine
zustandsbehaftete Autokonfiguration einleiten, indem es den vom Router angegebenen

DHCPv6 kontaktiert und eine globale oder eindeutige lokale Adresse sowie andere Konfigurationseinstellungen von diesem Server bezieht

DHCPv6

Als Unternehmensadministrator eines Netzwerks mit mehreren Segmenten müssen Sie gegebenenfalls eindeutige lokale oder globale Adressen für die netzwerkübergreifende Kommunikation verwenden. Deshalb brauchen Sie entweder Router, die die passenden Netzwerkpräfixe ankündigen, oder DHCPv6-Server, die Adressen mit den korrekten Präfixen bereitstellen können.

Die Remotezugriffsrolle in Windows Server 2012 unterstützt IPv6-Routing und -Ankündigung, die DHCP-Serverrolle unterstützt die IPv6-Adresszuweisung.

Einen IP-Übergang planen

Viele Unternehmensadministratoren sind so mit IPv4-Adressen vertraut, dass sie nur zögerlich an einen Wechsel denken. Netzwerkadressübersetzung (Network Address Translation, NAT) und CIDR dienen seit Jahren als ausgezeichnete Lückenbüßer in Bezug auf die Erschöpfung des 32-Bit-IP-Adressraums und viele würden die IPv4-Adressen gern beibehalten. Doch nun nähert sich der lange Zeit als Gespenst am Horizont wahrnehmbare IPv6-Übergang mit erschreckender Geschwindigkeit und Administratoren, die mit den neuen Technologien noch nicht vertraut sind, sollten hier schleunigst nachziehen.

Die Netzwerkindustrie und insbesondere das Internet haben riesige Summen in IPv4-Technologien investiert. Diese Technik wurde bisher nur zögerlich durch IPv6 ersetzt. In der Tat ist dies ein allmäßlicher Vorgang, der eigentlich schon vor über 10 Jahren ernsthaft beginnen sollte. Allerdings behandeln viele Administratoren ihre IPv4-Ausrüstung wie Haushaltsgeräte: Solange sie ordnungsgemäß arbeiten, gibt es keinen Grund, sie zu ersetzen. Leider kommt der Tag, wenn diese Gerätschaften nicht mehr funktionieren werden, rasant näher. Auch wenn es noch nicht an der Zeit sein mag, ausschließlich mit IPv6 zu arbeiten, sollten Administratoren den Übergang im Auge haben, wenn sie ihre Netzerke konzipieren und ihre Kaufentscheidungen treffen.



Hinweis IPv4-Adresserschöpfung

Der von der IANA noch nicht zugewiesene Adresspool war am 31. Januar 2011 erschöpft. Bei einem der RIRs, dem APNIC (Asia Pacific Network Information Center), waren am 15. April 2011 die Adressen aufgebraucht, bei den anderen RIRs dürfte dieser Zustand bald erreicht sein.

Unternehmensadministratoren können innerhalb des Unternehmens selbst nach ihren Vorstellungen verfahren. Wenn alle Netzwerkgeräte in der Organisation IPv6 unterstützen, können sie jederzeit auf IPv6-Adressen übergehen. Das Internet ist jedoch immer noch stark auf IPv4 basiert und dies wird voraussichtlich noch mehrere Jahre anhalten. Demzufolge muss der Übergang von IPv4 auf IPv6 schrittweise erfolgen – ein Projekt also, das für einen gewissen Zeitraum noch beide IP-Versionen unterstützt.

Jetzt und in der nahen Zukunft müssen Administratoren unter der Annahme arbeiten, dass die übrige Welt IPv4 verwendet. Implementieren Sie deshalb einen Mechanismus für die Übertragung Ihres IPv6-Datenverkehrs über eine IPv4-Verbindung. Letztlich wird sich die Lage umkehren. Der größte Teil der Welt wird IPv6 ausführen und die verbliebenen IPv4-Technologien müssen ihren älteren Datenverkehr über neue Verbindungen übertragen.

Einen dualen IP-Stack verwenden

Für den Übergang von IPv4 zu IPv6 ist es am einfachsten und naheliegendsten, beide Versionen zu betreiben. In diesem Sinne verfahren alle aktuellen Versionen von Windows, bis zurück zu Windows Server 2008 und Windows Vista.

Standardmäßig installieren diese Betriebssysteme beide IP-Versionen und verwenden sie gleichzeitig. Selbst wenn Sie bis heute noch nichts von IPv6 gehört hätten – Ihre Computer verwenden höchstwahrscheinlich diese Version und verfügen über verbindungslokale IPv6-Adressen. Diese können Sie sich mit dem Befehl `ipconfig /all` anzeigen lassen.

Die Implementierungen auf der Netzwerkschicht sind in Windows getrennt, sodass Sie sie separat konfigurieren können. Sowohl für IPv4 als auch für IPv6 können Sie die Adresse und andere Einstellungen manuell festlegen oder auf die Autokonfiguration zurückgreifen.

Da Windows beide IP-Versionen unterstützt, können die Computer mit TCP/IP-Ressourcen kommunizieren, die IPv4 oder IPv6 ausführen. In einem Unternehmensnetzwerk sind allerdings weitere Geräte – vornehmlich Router – vorhanden, die möglicherweise noch kein IPv6 beherrschen. Zudem ist das Internet fast vollständig auf IPv4 aufgebaut.

Administratoren sollten bereits jetzt darauf achten, dass die für die Netzwerkschicht anzuschaffenden Gerätschaften auch IPv6 unterstützen. Andernfalls gilt es als fast sicher, dass die Kosten für neue Hardware später erneut zu Buche schlagen.

Tunnel

Im Augenblick gibt es viele Netzwerkdienste, die ausschließlich auf IPv4 ausgerichtet sind, und vergleichbar wenige, die IPv6 voraussetzen. Allerdings sind diese IPv6-Dienste im Kommen.

Das DirectAccess-Feature für Remotenetzwerke in Windows Server 2012 und Windows 8 ist ein Beispiel für eine reine IPv6-Technik und ein großer Teil seiner Komplexität ist der Notwendigkeit geschuldet, IPv6-Verbindungen über das IPv4-Internet einzurichten.

Der IPv6-Datenverkehr wird über ein IPv4-Netzwerk hauptsächlich durch das sogenannte Tunneling abgewickelt. In diesem Fall ist Tunneling der Vorgang, mit dem ein System ein IPv6-Datagramm in einem IPv4-Paket kapselt, wie es Abbildung 4.4 veranschaulicht. Das System kann dann das IPv4-Paket an seinen Zielort senden, wobei keines der dazwischen liegenden Systeme den Inhalt des Pakets erkennen kann.

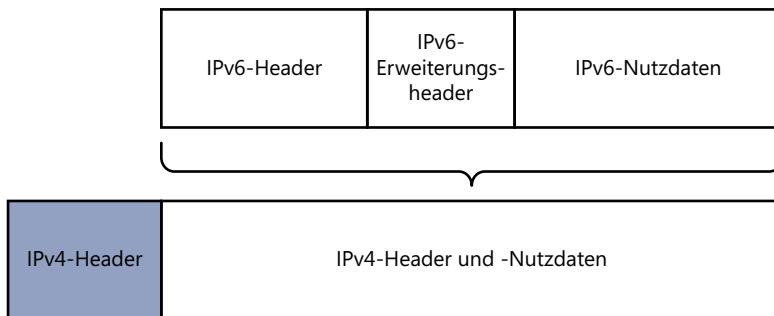


Abbildung 4.4 IPv6-Datenverkehr, der in einem IPv4-Datagramm gekapselt ist

Tunneling kann je nach der Netzwerkinfrastruktur in verschiedensten Konfigurationen arbeiten. Dazu gehören Verbindungen von Router zu Router, von Host zu Host, von Router zu Host und von Host zu Router. Am gebräuchlichsten ist allerdings die Router-zu-Router-Konfiguration, wie bei einer reinen IPv4-Verbindung zwischen einer IPv6-Niederlassung und dem IPv6-Hauptsitz, wie Abbildung 4.5 zeigt.

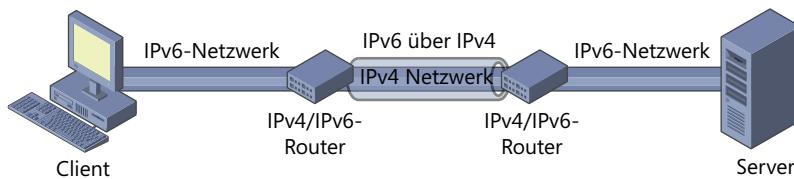


Abbildung 4.5 Zwei IPv6-Netzwerke, die durch einen IPv4-Tunnel verbunden sind

Die beiden Router unterstützen sowohl IPv4 als auch IPv6 und die lokalen Netzwerke an jedem Standort verwenden IPv6. Die Verbindung zwischen den beiden Standorten ist allerdings auf reines IPv4 ausgerichtet. Indem ein Tunnel zwischen den Routern in den beiden Büros eingerichtet wird, lässt sich bei Bedarf IPv6-Datenverkehr mithilfe ihrer IPv4-Schnittstellen übertragen. Die Computer an dem einen Standort können IPv6-Datenverkehr an den anderen Standort senden, und die Router sind dafür zuständig, die IPv6-Daten in IPv4-Pakete für den Weg durch den Tunnel zu kapseln. Windows unterstützt verschiedene – sowohl manuelle als auch automatische – Tunneling-Verfahren, wie sie die folgenden Abschnitte beschreiben.

Tunnel manuell konfigurieren

Semipermanente Tunnel, die IPv6-Datenverkehr über ein reines IPv4-Netzwerk übertragen, lassen sich auch manuell erstellen. Wenn ein Computer unter Windows Server 2012 oder Windows 8 als ein Endpunkt des Tunnels fungiert, können Sie den folgenden Befehl verwenden:

```
netsh interface ipv6 add v6v4tunnel "interface" localaddress remoteaddress
```

In diesem Befehl ist `interface` ein Klartextname, den Sie dem zu erstellenden Tunnel zuweisen möchten, `localaddress` und `remoteaddress` bezeichnen die IPv4-Adressen, die die beiden Endpunkte des Tunnels bilden. Der folgende Befehl gibt ein Beispiel an:

```
netsh interface ipv6 add v6v4tunnel "tunnel" 206.73.118.19 157.54.206.43
```

Tunnel automatisch konfigurieren

Es gibt auch eine Reihe von Mechanismen, die Tunnel über IPv4-Verbindungen automatisch erstellen. Diese Verfahren sind als temporäre Lösungen für die Übergangsphase von IPv4 zu IPv6 gedacht. Alle bieten einen Mechanismus, um eine IPv4-Adresse im IPv6-Format auszudrücken. Die folgenden Abschnitte beschreiben die von Windows unterstützten IPv4-zu-IPv6-Übergangstechniken.

6to4

Der 6to4-Mechanismus bindet im Wesentlichen die IPv4-Verbindungen in einem Netzwerk in die IPv6-Infrastruktur ein. Dazu definiert er eine Methode, um IPv4-Adressen im IPv6-Format auszudrücken und den IPv6-Datenverkehr in IPv4-Paketen zu kapseln.

ISATAP

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) ist ein automatisches Tunneling-Protokoll, mit dem Betriebssysteme von Windows-Arbeitsstationen eine IPv6-Verbindung mithilfe eines IPv4-Netzwerks emulieren.

Außerdem konvertiert ISATAP die IPv4-Adressen in das Adressformat der IPv6-Verbindungs-schicht, verwendet dabei aber eine andere Methode als 6to4. Da ISATAP kein Multicasting unterstützt, kann das Protokoll keine Router in der üblichen Art mithilfe des ND-Protokolls lokalisieren. Stattdessen stellt das System eine Liste möglicher Router (Potential Routers List, PRL) anhand von DNS-Abfragen zusammen und sendet regelmäßig ICMPv6 (Internet Control Message Protocol version 6)-Suchnachrichten an die Router.

Teredo

Um 6to4-Tunneling zu verwenden, müssen beide Endpunkte des Tunnels eine registrierte IPv4-Adresse besitzen. In den meisten Netzwerken befindet sich aber das System, das als Endpunkt fungieren würde, hinter einem NAT-Router und hat demnach eine nicht registrierte Adresse. In einem derartigen Fall wird die einzige registrierte Adresse dem NAT-Router selbst zugewiesen. Und sofern der Router kein 6to4 unterstützt (was auf viele Produkte zutrifft), lässt sich der Tunnel nicht einrichten.

Teredo räumt nun dieses Manko aus dem Weg und versetzt Nicht-IPv6-NAT-Router in die Lage, als Tunnelendpunkte zu fungieren. Dazu kapselt Teredo die IPv6-Pakete in UDP (User Datagram Protocol)-Datagrammen auf der Transportschicht und nicht wie bei 6to4 IPv4-Datagramme auf der Netzwerkschicht.

Damit ein Teredo-Client als Tunnelendpunkt fungieren kann, benötigt er Zugriff auf einen Teredo-Server, mit dem er Routeranfrage- und Routerankündigungs-Nachrichten austauscht und daraus ermittelt, ob sich der Client hinter einem NAT-Router befindet.

Um eine Kommunikation einzuleiten, tauscht ein Teredo-Client Null-Pakete – sogenannte Bubbles – mit dem gewünschten Ziel aus, wobei die Teredo-Server an jedem Endpunkt als Zwischenstationen dienen. Die Bubble-Nachrichten haben die Aufgabe, Zuordnungen für beide Computer in den gegenseitigen NAT-Routern anzulegen.

Prüfungszielzusammenfassung

- Der IPv4-Adressraum besteht aus 32-Bit-Adressen, die in Form von vier 8-Bit-Dezimalwerten von 0 bis 255 durch Punkte getrennt geschrieben werden, wie zum Beispiel 192.168.43.100. In dieser sogenannten punktierten Dezimalschreibweise bezeichnet man die einzelnen 8-Bit-Dezimalwerte als Oktette oder Bytes.
- Da sich die Subnetzmaske, die den IP-Adressen zugeordnet ist, ändern kann, variiert gegebenenfalls auch die Anzahl der Bits, die das Netzwerk und den Host identifizieren. Der ursprüngliche IP-Standard definiert drei Klassen von IP-Adressen für Netzwerkuzuweisungen, die eine unterschiedliche Anzahl von Netzwerken und Hosts unterstützen.
- Wegen ihrer Verschwendungen geriet die klassenorientierte Adressierung langsam außer Mode und wurde durch eine Reihe von Methoden mit Subnetzen – einschließlich der Subnetzmaskierung mit variabler Länge (VLSM) und schließlich durch klassenloses domänenübergreifendes Routing (Classless Inter-Domain Routing, CIDR) abgelöst.
- Ein Windows-Computer initiiert beim Startvorgang die zustandslose IPv6-Adressenautokonfiguration, während er jeder Schnittstelle eine verbindungslokale Unicast-Adresse zuweist.
- Für den Übergang von IPv4 zu IPv6 ist es am einfachsten und naheliegendsten, beide Versionen zu betreiben. In diesem Sinne verfahren alle aktuellen Versionen von Windows.
- Der IPv6-Datenverkehr wird über ein IPv4-Netzwerk hauptsächlich durch das sogenannte Tunneling abgewickelt. Tunneling ist der Vorgang, mit dem ein System ein IPv6-Datagramm in einem IPv4-Paket kapselt.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Techniken wird vorrangig verwendet, um IPv6-Datenverkehr über ein IPv4-Netzwerk zu übertragen?
 - A. Subnetze
 - B. Tunneling
 - C. Supernetze
 - D. Zusammenziehen

2. Welche der folgenden Adressen ist das IPv6-Äquivalent zu einer privaten IPv4-Adresse?
 - A. Verbindungslokale Unicast-Adresse
 - B. Global eindeutige Unicast-Adresse
 - C. Eindeutige lokale Unicast-Adresse
 - D. Anycast-Adresse
3. Welches der folgenden Protokolle ist ein automatisches Tunneling-Protokoll, das Windows-Betriebssysteme verwenden, die sich hinter NAT-Routern befinden?
 - A. Teredo
 - B. 6to4
 - C. ISATAP
 - D. APIPA
4. Welche Art von IP-Adresse muss ein System besitzen, damit es vom Internet aus sichtbar ist?
 - A. Registriert
 - B. Binär
 - C. Klasse B
 - D. In Subnetze aufgeteilt
5. Welche der folgenden Werte für Subnetzmasken verwenden Sie, wenn Sie einen TCP/IP-Client mit einer IPv4-Adresse im Netzwerk 172.16.32.0/19 konfigurieren?
 - A. 255.224.0.0
 - B. 255.240.0.0
 - C. 255.255.224.0
 - D. 255.255.240.0
 - E. 255.255.255.240



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Der Unternehmensadministrator hat Arthur die Netzwerkadresse 172.16.8.0/25 für das von ihm aufzubauende Zweigstellennetzwerk zugewiesen. Arthur berechnet, dass er über 126 (d.h. $2^8 - 2$) IP-Adressen verfügt, was für sein Netzwerk zwar genügt, doch er hat ermittelt, dass er sechs Subnetze mit mindestens jeweils 10 Hosts benötigt.

Beantworten Sie für dieses Szenario die folgenden Fragen:

1. Wie kann Arthur die ihm zugeteilte Adresse in Subnetze aufteilen, um seinen Anforderungen zu entsprechen?
2. Welche IP-Adressen und Subnetzmasken verwenden die Computer in seinem Zweigstellennetzwerk?

Prüfungsziel 4.2: Den DHCP-Dienst bereitstellen und konfigurieren

Ein Server ist selten von Anfang an bereit, alle für ihn vorgesehenen Aufgaben unmittelbar nach der Installation ausführen zu können. Normalerweise macht sich eine Konfiguration im Anschluss an die Installation erforderlich und weitere Konfigurationsänderungen fallen möglicherweise an, nachdem der Server in Betrieb ist.

Dieses Prüfungsziel zeigt, wie Sie

- Bereiche erstellen und konfigurieren
 - eine DHCP-Reservierung konfigurieren
 - DHCP-Optionen konfigurieren
 - Client und Server für PXE-Start konfigurieren
 - DHCP-Relay-Agent konfigurieren
 - DHCP-Server autorisieren
-

DHCP

DHCP ist ein Dienst, der automatisch die IP-Adresse und andere TCP/IP-Einstellungen auf Netzwerkcomputern konfiguriert. Dabei weist er Adressen aus einem Pool (einem sogenannten *Bereich*) zu und gibt sie wieder frei, wenn sie nicht mehr verwendet werden.

Das manuelle Konfigurieren von TCP/IP-Clients ist nicht nur eine zeitaufwendige Angelegenheit, sondern kann auch infolge von Eingabefehlern zu Adressierungskonflikten führen, die die Netzwerkkommunikation lahmlegen. DHCP verhindert derartige Fehler und bietet viele andere Vorteile. Dazu gehören die automatische Zuweisung neuer Adressen, wenn Computer von einem Subnetz in ein anderes verschoben werden, und das automatische Freigeben von Adressen, die nicht mehr in Gebrauch sind.

DHCP besteht aus den folgenden drei Komponenten:

- Einer DHCP-Serveranwendung, die auf Clientanforderungen nach TCP/IP-Konfigurationseinstellungen reagiert
- Einem DHCP-Client, der Anfragen an Server auslöst und die empfangenen TCP/IP-Konfigurationseinstellungen auf den lokalen Computer anwendet
- Einem DHCP-Kommunikationsprotokoll, das die Formate und Abläufe des Meldungsaustauschs zwischen DHCP-Clients und -Servern definiert

Sämtliche Microsoft Windows-Betriebssysteme bringen DHCP-Clientfunktionen mit und alle Serverbetriebssysteme (einschließlich Windows Server 2012) enthalten den Microsoft DHCP-Server.

Die DHCP-Standards definieren drei verschiedene Methoden der IP-Adresszuweisung:

- **Dynamische Zuweisung** Der DHCP-Server weist einem Clientcomputer eine IP-Adresse aus einem Bereich für eine festgelegte Zeitspanne zu. Jeder Client muss periodisch die Lease erneuern, um die Adresse weiterzuverwenden. Erlaubt der Client, dass die Lease abläuft, wird die Adresse an den Bereich zurückgegeben, um sie einem anderen Client neu zuweisen zu können.
- **Automatische Zuweisung** Der DHCP-Server weist einem Clientcomputer eine IP-Adresse permanent aus einem Bereich zu. Nachdem der DHCP-Server dem Client die Adresse zugewiesen hat, lässt sie sich nur ändern, wenn der Computer manuell neu konfiguriert wird.
- **Manuelle Zuweisung** Der DHCP-Server weist einem bestimmten Computer im Netzwerk eine spezifische IP-Adresse permanent zu. In Windows Server 2012-DHCP-Server werden manuell zugewiesene Adressen als Reservierungen bezeichnet.

Außer IP-Adressen kann DHCP den Clients Werte für andere Parameter bereitstellen, die für die Konfiguration eines TCP/IP-Clients erforderlich sind, einschließlich Subnetzmaske, Standardgateway und DNS-Serveradressen. Ziel ist es, jegliche manuelle TCP/IP-Konfiguration auf einem Clientsystem überflüssig zu machen. Zum Beispiel kann der Microsoft DHCP-Server mehr als 50 Konfigurationsparameter zusammen mit der IP-Adresse bereitstellen, selbst wenn Windows-Clients nur eine Teilmenge dieser Parameter verwenden können.

Bei DHCP-Kommunikationen gibt es acht verschiedene Meldungstypen, die alle das gleiche grundlegende Paketformat verwenden. Der DHCP-Datenverkehr wird in standardmäßigen UDP/IP- Datagrammen übertragen, und zwar über Port 67 am Server und Port 68 am Client.

DHCP-Optionen

Das DHCP-Optionsfeld ist ein allgemeiner Abschnitt, der dafür vorgesehen ist, die verschiedenen Parameter (bis auf die IP-Adresse) für die Konfiguration des TCP/IP-Stacks eines Clientsystems zu übertragen. Da Sie einen DHCP-Server so konfigurieren können, dass er viele Optionen an Clients liefert, wäre es nicht zweckmäßig, einzelne Felder für jede Option zu definieren.

Die Option DHCP-Meldungstyp

Die Option DHCP-Meldungstyp identifiziert die Gesamtfunktion der DHCP-Meldung und ist in allen DHCP-Paketen erforderlich. Das DHCP-Kommunikationsprotokoll definiert 8 verschiedene Meldungstypen:

- **DHCPDISCOVER** Von Clients verwendet, um Konfigurationsparameter von einem DHCP-Server anzufordern
- **DHCPOFFER** Von Servern verwendet, um anfragenden Clients IP-Adressen anzubieten
- **DHCPREQUEST** Von Clients verwendet, um eine IP-Adresszuweisung zu akzeptieren oder zu erneuern
- **DHCPDECLINE** Von Clients verwendet, um eine angebotene IP-Adresse abzuweisen

- **DHCPACK** Von Servern verwendet, um zu bestätigen, dass der Client eine angebotene IP-Adresse akzeptiert hat
- **DCHPNAK** Von Servern verwendet, um die Zusage des Clients für eine angebotene IP-Adresse abzulehnen
- **DHCPRELEASE** Von Clients verwendet, um die Lease einer IP-Adresse zu beenden
- **DHCPIINFORM** Von Clients verwendet, um zusätzliche TCP/IP-Konfigurationsparameter von einem Server abzurufen

Herstellerspezifische BOOTP-Erweiterungen

Zu diesen Optionen gehören viele grundlegende TCP/IP-Konfigurationsparameter, die von den meisten Clientsystemen verwendet werden:

- **Subnetzmaske** Spezifiziert, welche Bits der IP-Adresse das Hostsystem und welche Bits das Netzwerk, in dem sich das Hostsystem befindet, identifizieren
- **Router** Legt die IP-Adresse des Routers (oder des Standardgateways) im lokalen Netzwerksegment fest, die der Client für Datenübertragungen an Systeme in anderen Netzwerksegmenten verwenden soll
- **Domain Name Server** Gibt die IP-Adressen der Server an, die der Client für die DNS-Namensauflösung verwendet
- **Hostname** Gibt den DNS-Hostnamen an, den der Client verwendet
- **Domänenname** Gibt den Namen der DNS-Domäne an, in der sich das System befindet

DHCP-Erweiterungen

Über diese Optionen lassen sich Parameter angeben, die das Aushandeln der DHCP-Leases und Erneuerungsvorgänge regeln:

- **Angeforderte IP-Adresse** Vom Client verwendet, um eine bestimmte IP-Adresse vom Server anzufordern
- **IP-Adressen-Leasezeitraum** Legt den Leasezeitraum für eine dynamisch zugewiesene IP-Adresse fest
- **Serverkennung** Gibt die IP-Adresse des Servers an, der an einer DHCP-Transaktion beteiligt ist; vom Client für Unicast-Meldungen an den Server verwendet
- **Parameteranforderungsliste** Vom Client verwendet, um eine Liste der angeforderten Konfigurationsoptionen (die durch ihre Codenummern identifiziert werden) an den Server zu senden
- **Meldung** Dient dazu, eine Fehlermeldung vom Server an den Client in einer DCHPNAK-Meldung zu übertragen
- **Erneuerungszeitraum (T1)** Spezifiziert die Zeitspanne, die verstrichen sein muss, bevor die Lease einer IP-Adresse in den Erneuerungsstatus übergeht
- **Neueinbindungszeitraum (T2)** Spezifiziert die Zeitspanne, die verstrichen sein muss, bevor die Lease einer IP-Adresse in den Neueinbindungsstatus übergeht

DHCP-Kommunikationen

Um eine DHCP-Strategie für ein Unternehmensnetzwerk zu entwerfen und ordnungsgemäß umzusetzen, müssen Sie wissen, wie die Kommunikation zwischen DHCP-Clients und -Servern abläuft. Auf Windows-Computern ist der DHCP-Client standardmäßig aktiviert, auch wenn er in der Benutzeroberfläche namentlich nicht erwähnt wird. Die Option *IP-Adresse automatisch beziehen* im Eigenschaftenblatt *Internetprotokoll Version 4 (TCP/IPv4)* und die Option *IPv6-Adresse automatisch beziehen* im Eigenschaftenblatt *Internetprotokoll Version 6 (TCP/IPv6)* steuern die Aktivierung des Clients für IPv4 bzw. IPv6.

Aushandeln der DHCP-Lease

Eine DHCP-Kommunikation wird immer durch den Client eingeleitet, wie Abbildung 4.6 zeigt.

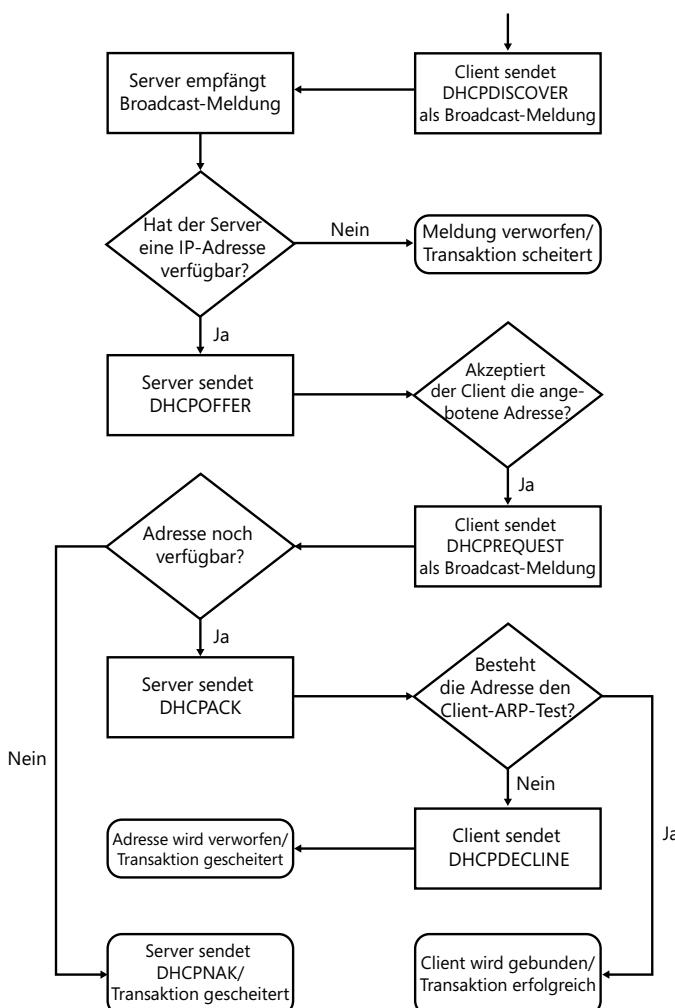


Abbildung 4.6 Ablauf der IP-Adresszuweisung per DHCP

Der Ablauf sieht folgendermaßen aus:

1. Startet ein Computer erstmalig, wobei der DHCP-Client aktiv ist, generiert der Client eine Reihe von DHCPDISCOVER-Meldungen, um eine IP-Adresszuweisung von einem DHCP-Server zu erbitten, und sendet sie als Broadcast-Meldung im lokalen Netzwerk.
2. Alle DHCP-Server, die die DHCPDISCOVER-Broadcast-Meldungen empfangen, generieren DHCPOFFER-Meldungen, die eine IP-Adresse und andere TCP/IP-Konfigurationsparameter enthalten, und senden sie an den Client.
3. Nach einer festgelegten Zeitspanne sendet der Client keine Broadcasting-Meldungen mehr und signalisiert die Annahme einer der angebotenen Adressen, indem er eine DHCPREQUEST-Meldung generiert mit der Adresse des Servers, dessen Angebot er angenommen hat, und sendet sie als Broadcast im lokalen Netzwerk.
4. Empfängt der Server, der die angenommene IP-Adresse angeboten hat, die DHCPREQUEST-Meldung, fügt er die angebotene IP-Adresse zusammen mit anderen Einstellungen in seine Datenbank ein.
5. Der Server sendet dann eine DHCPACK-Meldung an den Client und bestätigt damit den Abschluss des Vorgangs. Kann der Server die Zuweisung nicht fertig stellen, sendet er eine DHCPNAK-Meldung an den Client und der Vorgang beginnt von Neuem.
6. Als abschließenden Test sendet der Client die angebotene IP-Adresse in einer Broadcast-Meldung per ARP (Address Resolution Protocol), um sich davon zu überzeugen, dass kein anderes System im Netzwerk dieselbe Adresse verwendet. Wenn der Client keine Antwort auf seine ARP-Broadcast-Meldung erhält, ist die DHCP-Transaktion abgeschlossen. Antwortet ein anderes System auf die ARP-Meldung, verwirft der Client die IP-Adresse und sendet eine DHCPDECLINE-Meldung an den Server, um die Transaktion zu annullieren. Dann startet der Client den Vorgang von Neuem.

DHCP-Leaseerneuerung

In der Standardeinstellung verwendet der DHCP-Server in Windows Server 2012 eine dynamische Zuordnung, wobei die Clients die IP-Adressen mit einem Leasezeitraum von acht Tagen erhalten. Während dieses Leasezeitraums versucht der Client in regelmäßigen Abständen, den Server zu kontaktieren, um die Lease zu erneuern, wie Abbildung 4.7 zeigt.

Der Ablauf sieht folgendermaßen aus:

1. Wenn der DHCP-Client die 50-Prozentmarke des Leasezeitraums erreicht (der sogenannte Erneuerungszeitraum oder T1-Wert), generiert der Client DHCPREQUEST-Meldungen und sendet sie als Unicast-Meldungen an den DHCP-Server, der die Lease ausgibt.
2. Reagiert der Server nicht bis zu dem Zeitpunkt, zu dem der Client die 87,5-Prozentmarke des Leasezeitraums erreicht hat (den sogenannten Neueinbindungszeitraum oder T2-Wert), sendet der Client seine DHCPREQUEST-Meldungen als Broadcasts und versucht damit, eine IP-Adresszuweisung von einem beliebigen DHCP-Server im Netzwerk zu erbitten.

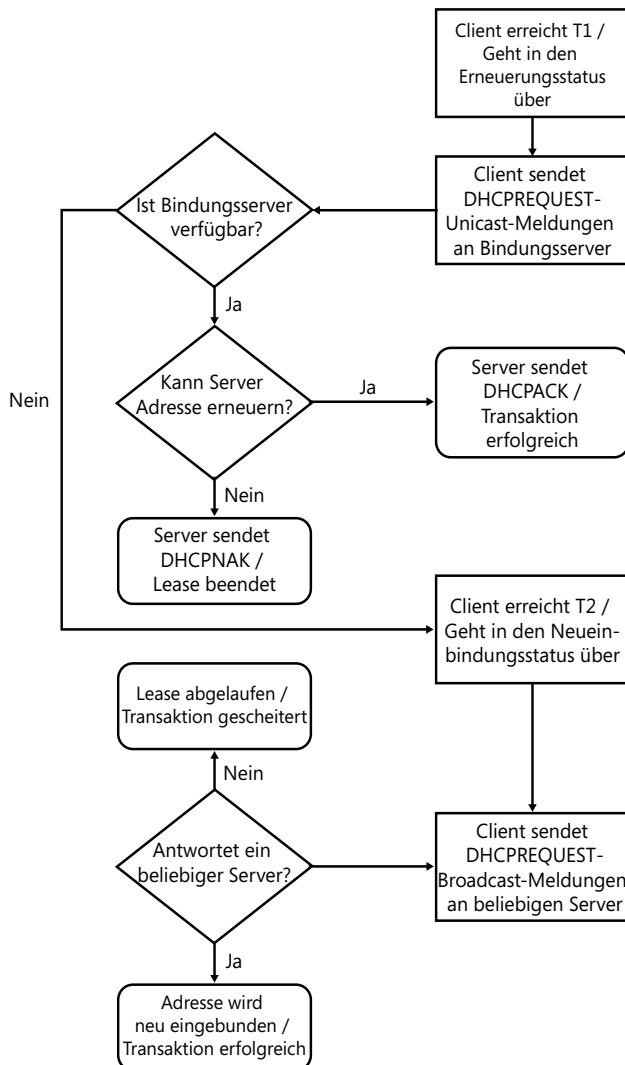


Abbildung 4.7 Erneuerung der DHCP-IP-Adresse

- Wenn der Client die DHCPREQUEST-Meldung sendet, erhält er eine DHCPACK-Meldung, die die Leaserneuerungsanforderung bestätigt, oder eine DHCPNAK-Meldung, die die Lease beendet. Empfängt der Client keine Antworten auf seine DHCPREQUEST-Meldungen, bis die Lease abläuft, oder empfängt er eine DHCPNAK-Meldung, gibt der Client seine IP-Adresse wieder frei. Die gesamte TCP/IP-Kommunikation wird dann eingestellt, außer der Übertragung von DHCPDISCOVER-Broadcasts.

Einen DHCP-Server bereitstellen

Da DHCP-Server unabhängig voneinander arbeiten, müssen Sie den Dienst auf jedem Computer, der als DHCP-Server fungieren soll, installieren und Bereiche konfigurieren. Der DHCP-Serverdienst ist in Windows Server 2012 als Rolle verpackt. Diese Rolle installieren Sie über den Assistenten zum Hinzufügen und Rollen und Features, der von der Server-Manager-Konsole aus zugänglich ist.

Wenn Sie die DHCP-Serverrolle auf einem Computer installieren, der einer Active Directory-Domänen-Dienste-Domäne angehört, wird der DHCP-Server automatisch autorisiert, um IP-Adressen an Clients zuzuweisen, die Mitglieder derselben Domäne sind. Wenn der Server beim Installieren der Rolle noch keiner Domäne angehört und Sie ihn erst später mit einer Domäne verknüpfen, müssen Sie den DHCP-Server in der Domäne manuell autorisieren. Klicken Sie dazu in der DHCP-Konsole mit der rechten Maustaste auf den Serverknoten und wählen Sie aus dem Kontextmenü den Befehl *Autorisieren*.

Nachdem Sie die DHCP-Serverrolle installiert haben, müssen Sie den Dienst konfigurieren, indem Sie einen Bereich erstellen. Erst dann kann der Server Clients bedienen.

Einen Bereich erstellen

Ein Bereich umfasst IP-Adressen in einem bestimmten Subnetz, die für die Zuweisung durch einen DHCP-Server ausgewählt wurden. In Windows Server-Versionen vor Windows Server 2012 können Sie einen Bereich einrichten, während Sie die DHCP-Serverrolle installieren. In Windows Server 2012 sind dies dagegen zwei separate Abläufe. Um einen Bereich mit dem MMC-Snap-In *DHCP* zu erstellen, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Klicken Sie auf *Tools / DHCP*. Daraufhin erscheint die DHCP-Konsole.
3. Erweitern Sie den Serverknoten und den *IPv4*-Knoten.
4. Klicken Sie mit der rechten Maustaste auf den *IPv4*-Knoten und wählen Sie *Neuer Bereich*. Der Bereichserstellungs-Assistent startet und zeigt die Seite *Willkommen* an.
5. Klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Bereichsname*.
6. Geben Sie in das Textfeld *Name* einen Namen für den Bereich ein und klicken Sie auf *Weiter*. Es wird die Seite *IP-Adressbereich* geöffnet, wie sie in Abbildung 4.8 zu sehen ist.
7. Geben Sie in das Textfeld *Start-IP-Adresse* die erste Adresse im Adressbereich ein, die Sie zuweisen möchten. In das Feld *End-IP-Adresse* tragen Sie die letzte Adresse im Bereich ein.

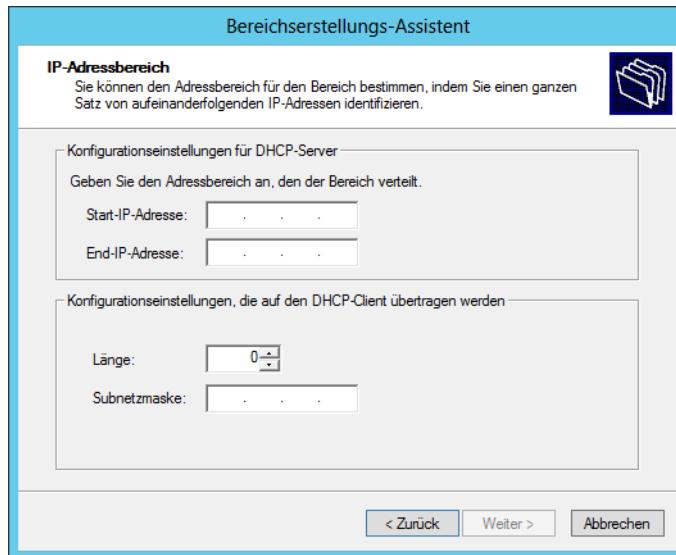


Abbildung 4.8 Die Seite *IP-Adressbereich* in der DHCP-Konsole

8. In das Textfeld *Subnetzmase* geben Sie den Maskenwert für das Subnetz ein, in dem der Bereich operiert. Klicken Sie auf *Weiter*. Es erscheint die Seite *Ausschlüsse und Verzögerung hinzufügen*.
9. In den Textfeldern *Start-IP-Adresse* und *End-IP-Adresse* spezifizieren Sie den IP-Adressbereich, den Sie ausschließen möchten. Außerdem können Sie eine Zeitspanne festlegen, mit der der Server nach dem Empfang von DHCPDISCOVER-Meldungen die DHCPOFFER-Meldungen verzögert sendet. Klicken Sie dann auf *Weiter*, um die Seite *Leasedauer* zu öffnen.
10. Geben Sie die Länge der Leases für die Adressen im Bereich an und klicken Sie auf *Weiter*. Es erscheint die Seite *DHCP-Optionen konfigurieren*.
11. Wählen Sie *Ja, diese Optionen jetzt konfigurieren* und klicken Sie auf *Weiter*. Daraufhin erscheint die Seite *Router (Standardgateway)*, die Abbildung 4.9 zeigt.
12. Geben Sie im Textfeld *IP-Adresse* die Adresse eines Routers im Subnetz an, der vom Bereich bedient wird. Klicken Sie auf *Hinzufügen* und dann auf *Weiter*. Die Seite *Domänenname und DNS-Server* wird geöffnet.
13. Geben Sie in das Textfeld *Servername* den Namen eines DNS-Servers im Netzwerk ein und klicken Sie auf *Auflösen* oder geben Sie die Adresse eines DNS-Servers in das Textfeld *IP-Adresse* ein. Klicken Sie auf *Hinzufügen* und dann auf *Weiter*. Es erscheint die Seite *WINS-Server*.
14. Klicken Sie auf *Weiter*, um die Seite *Bereich aktivieren* zu öffnen.

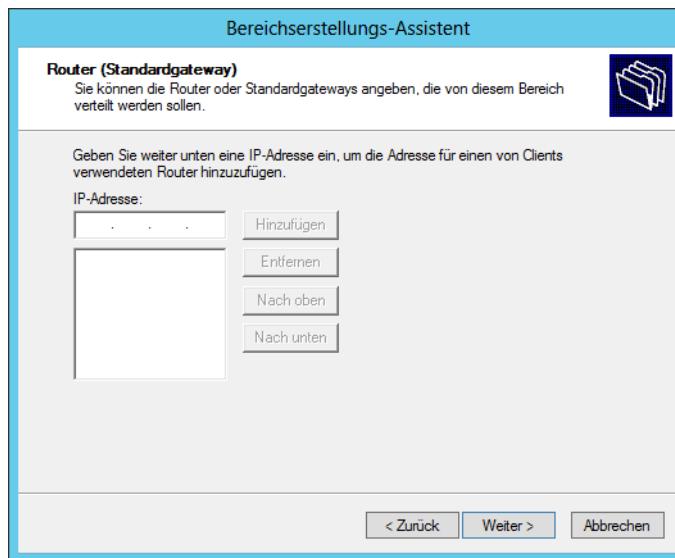


Abbildung 4.9 Die Seite *Router (Standardgateway)* in der DHCP-Konsole

15. Wählen Sie *Ja, diesen Bereich jetzt aktivieren* und klicken Sie auf *Weiter*. Die Seite *Fertigstellen des Assistenten* wird geöffnet.
16. Klicken Sie auf *Fertig stellen*, um den Assistenten zu schließen.
17. Schließen Sie die DHCP-Konsole.

Nachdem die Rolleninstallation abgeschlossen ist, können alle DHCP-Clients im Subnetz, das Sie im erzeugten Bereich identifiziert haben, ihre IP-Adressen und andere TCP/IP-Konfigurationseinstellungen via DHCP beziehen. Mithilfe der DHCP-Konsole können Sie auch zusätzliche Bereiche für andere Subnetze erstellen.

DHCP-Optionen konfigurieren

Mit dem Bereichserstellungs-Assistenten können Sie lediglich die am häufigsten verwendeten DHCP-Optionen konfigurieren, wenn Sie einen neuen Bereich erstellen. Die vielen anderen Optionen lassen sich aber jederzeit zu einem späteren Zeitpunkt konfigurieren.

Der Windows DHCP-Server unterstützt zwei Arten von Optionen:

- **Bereichsoptionen** Optionen, die nur an DHCP-Clients übermittelt werden, die Adressen aus einem bestimmten Bereich empfangen
- **Serveroptionen** Optionen, die allen DHCP-Clients übermittelt werden, die Adressen vom Server empfangen

Die Router-Option ist ein typisches Beispiel für eine Bereichsoption, da die Standardgatewayadresse eines DHCP-Clients im selben Subnetz wie seine IP-Adresse liegen muss. Die DNS-Server-Option ist normalerweise eine Serveroption, da DNS-Server nicht im

selben Subnetz liegen müssen und Netzwerke oftmals dieselben DNS-Server für alle ihre Clients verwenden.

Alle Optionen, die der Windows DHCP-Server unterstützt, können entweder Bereichs- oder Serveroptionen sein. Ihre Konfiguration läuft prinzipiell bei beiden gleich ab. Um eine Bereichsoption zu konfigurieren, klicken Sie mit der rechten Maustaste auf den Knoten *Bereichsoptionen* und wählen im Kontextmenü *Optionen konfigurieren*. Abbildung 4.10 zeigt das Dialogfeld *Optionen – Bereich*, das die Steuerelemente für die verfügbaren Optionen enthält.

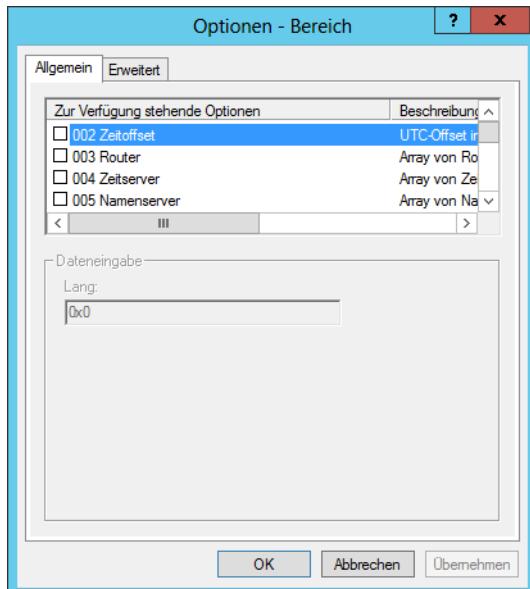


Abbildung 4.10 Das Dialogfeld *Optionen – Bereich*

Wenn Sie mit der rechten Maustaste auf den Knoten *Serveroptionen* klicken, können Sie das Dialogfeld *Serveroptionen* öffnen, das gleich aufgebaut ist.

Eine Reservierung erstellen

Obwohl DHCP eine ausgezeichnete TCP/IP-Konfigurationslösung für die meisten Computer in einem Netzwerk darstellt, gibt es auch einige, für die das nicht zutrifft. Domänencontroller, Internet-Webserver und DHCP-Server selbst brauchen statische IP-Adressen.

Da die dynamische DHCP-Zuweisungsmethode einkalkuliert, dass sich die IP-Adresse eines Computers ändern kann, ist sie für diese speziellen Aufgaben nicht geeignet. Allerdings ist es per DHCP auch möglich, diesen Computern die Adressen manuell anstatt statisch zuzuweisen.

In einem Windows DHCP-Server wird eine manuell zugewiesene Adresse als *Reservierung* bezeichnet. Um eine Reservierung zu erstellen, erweitern Sie den Bereichsknoten, klicken mit der rechten Maustaste auf den Knoten *Reservierungen* und wählen im Kontextmenü den

Befehl *Neue Reservierung*. Daraufhin wird das Dialogfeld *Neue Reservierung* geöffnet, das in Abbildung 4.11 zu sehen ist.

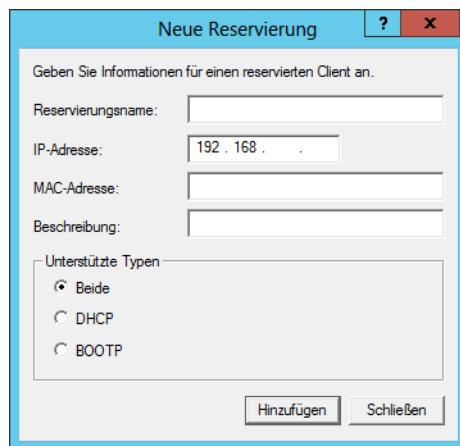


Abbildung 4.11 Das Dialogfeld *Neue Reservierung* eines DHCP-Servers

In diesem Dialogfeld geben Sie die IP-Adresse an, die Sie dem Clientcomputer zuweisen und mit seiner MAC-Adresse, die in seinem Netzwerkadapter fest codiert ist, verknüpfen möchten.

Es ist auch möglich, den TCP/IP-Client des Computers manuell zu konfigurieren, doch stellt eine DHCP-Reservierung sicher, dass alle Ihre IP-Adressen von Ihren DHCP-Servern verwaltet werden. In einem großen Unternehmen, in dem verschiedene Administratoren mit DHCP- und TCP/IP-Konfiguration zu tun haben, könnte die von einem Administrator manuell zugewiesene IP-Adresse bereits in einem DHCP-Bereich eingeschlossen sein, den ein anderer Administrator eingerichtet hat – Adresskonflikte sind dann vorprogrammiert. Reservierungen erzeugen eine permanente Aufzeichnung der IP-Adresszuweisung auf dem DHCP-Server.

PXE verwenden

Das Windows-Betriebssystem bringt einen DHCP-Client mit, der die IP-Adresse und andere TCP/IP-Einstellungen von Computern konfigurieren kann, bei denen bereits ein Betriebssystem installiert ist. Allerdings ist es auch für einen komplett neuen Computer möglich – d.h. einen Computer ohne installiertes Betriebssystem –, DHCP zu verwenden.

Die in vielen Netzwerkadapters von Haus aus eingebaute Funktion PXE (Preboot eXecution Environment) ermöglicht solchen Computern, sich mit einem DHCP-Server über das Netzwerk zu verbinden und TCP/IP-Cienteinstellungen zu beziehen, selbst wenn auf dem Computer kein Betriebssystem vorhanden ist. Administratoren verwenden normalerweise diese Funktion, um die Bereitstellung des Betriebssystems bei umfangreichen Flotten von Arbeitsstationen zu automatisieren.

Außer dem Konfigurieren der IP-Adresse und anderer TCP/IP-Cienteinstellungen auf dem Computer kann der DHCP-Server der Arbeitsstation eine Option anbieten, die den Standort einer Boot-Datei angibt. Diese kann das Dateisystem herunterladen und für den Start des

Computers verwenden sowie eine Windows-Betriebssysteminstallation einleiten. Ein mit PXE ausgerüstetes System lädt Startdateien herunter, und zwar mithilfe des TFTP (Trivial File Transfer Protocol), einer vereinfachten Version des FTP-Protokolls, die keine Authentifizierung erfordert.

Mithilfe der Rolle *Windows-Bereitstellungsdienste* (Windows Deployment Services, WDS) von Windows Server 2012 können Administratoren Imagedateien (Abbilddateien) verwalten, die es erlauben, Remotearbeitsstationen zu starten und Windows zu installieren. Damit ein PXE-Adapter auf WDS-Images zugreifen kann, muss für den DHCP-Server im Netzwerk eine benutzerdefinierte PXEClient-Option (Option 60) mit dem Standort des WDS-Servers im Netzwerk konfiguriert sein.

Der PXE-Client auf der Arbeitsstation benötigt normalerweise keine Konfiguration, außer dass gegebenenfalls die Boot-Reihenfolge zu ändern ist, damit der Computer zuerst versucht, über das Netzwerk zu starten, bevor er auf die lokalen Geräte zugreift.

In einer ordnungsgemäß konfigurierten WDS-Installation von Windows 8 läuft die Bereitstellung des Clientbetriebssystems wie folgt ab:

1. Der Clientcomputer startet, findet kein lokales Boot-Gerät und versucht, einen Netzwerkstart durchzuführen.
2. Der Clientcomputer verbindet sich mit einem DHCP-Server im Netzwerk, von dem er eine DHCPOFFER-Meldung mit einer IP-Adresse und anderen TCP/IP-Konfigurationsparametern bekommt. Dazu kommt die 060 PXEClient-Option, die den Namen eines WDS-Servers enthält.
3. Der Client verbindet sich mit dem WDS-Server und erhält eine Startabbilddatei, die er per TFTP herunterlädt.
4. Der Client lädt Windows PE und den WDS-Client aus der Imagedatei auf eine RAM-Disk (eine virtuelle Festplatte, die im Arbeitsspeicher eingerichtet wird) und zeigt ein Startmenü mit einer Liste der vom WDS-Server verfügbaren Installationsabbilder an.
5. Der Benutzer auf dem Clientcomputer wählt ein Installationsimage aus dem Startmenü aus und die Installation des Betriebssystems beginnt. Von hier an läuft der Setupvorgang genau wie eine manuelle Installation.

Einen DHCP-Relay-Agenten bereitstellen

Wenn Sie sich für eine zentralisierte oder hybride DHCP-Infrastruktur entscheiden, brauchen Sie einen DHCP-Relay-Agenten in jedem Subnetz, in dem kein DHCP-Server vorhanden ist. Viele Router können die Funktionen eines DHCP-Relay-Agenten wahrnehmen. Sollte das nicht der Fall sein, lassen sich die Funktionen eines Relay-Agenten auf einem Windows Server 2012-Computer konfigurieren. Gehen Sie dazu folgendermaßen vor:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.

2. Installieren Sie über den Assistenten zum Hinzufügen von Rollen und Features die Remotezugriffsrolle einschließlich des Routing-Rollendienstes.
3. Klicken Sie auf *Assistent für erste Schritte öffnen*. Daraufhin wird der Assistent *Remotezugriff konfigurieren* geöffnet.
4. Klicken Sie auf *Nur VPN bereitstellen*. Es erscheint die Konsole *Routing und RAS*.
5. Klicken Sie mit der rechten Maustaste auf den Serverknoten und wählen Sie aus dem Kontextmenü *Routing und RAS konfigurieren und aktivieren*. Daraufhin erscheint der Setup-Assistent für den Routing- und RAS-Server.
6. Klicken Sie auf *Weiter*, um die Seite *Willkommen* zu verlassen und zur Seite *Konfiguration* zu gehen, die in Abbildung 4.12 zu sehen ist.

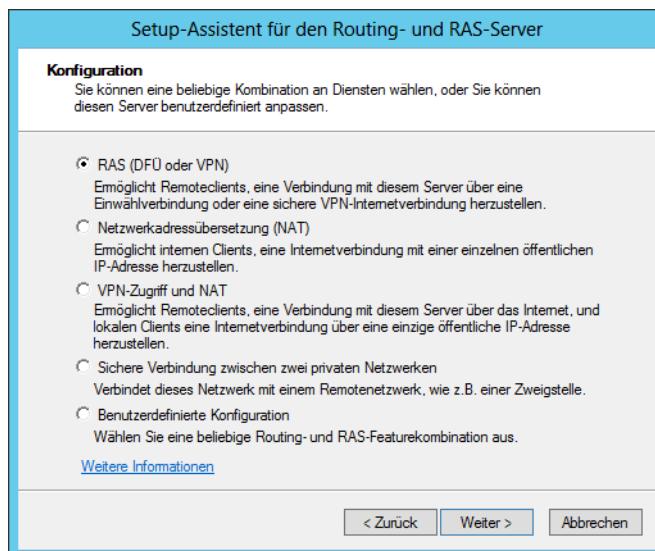


Abbildung 4.12 Die Seite *Konfiguration* im Setup-Assistenten für den Routing- und RAS-Server

7. Wählen Sie die Option *Benutzerdefinierte Konfiguration* und klicken Sie auf *Weiter*. Die Seite *Benutzerdefinierte Konfiguration* erscheint.
8. Aktivieren Sie das Kontrollkästchen *LAN-Routing* und klicken Sie auf *Weiter*. Die Seite *Fertigstellen des Assistenten* wird geöffnet.
9. Klicken Sie auf *Fertig stellen*. Es erscheint ein Routing- und RAS-Meldungsfeld mit der Aufforderung, den Dienst zu starten.
10. Klicken Sie auf *Dienst starten*.
11. Erweitern Sie den *IPv4*-Knoten. Klicken Sie dann mit der rechten Maustaste auf den Knoten *Allgemein* und wählen Sie im Kontextmenü den Befehl *Neues Routingprotokoll* aus. Das Dialogfeld *Neues Routingprotokoll* erscheint.

12. Wählen Sie den Eintrag *DHCP-Relay-Agent* aus und klicken Sie auf *OK*. Es erscheint ein Knoten *DHCP-Relay-Agent*, der dem *IPv4-Knoten* untergeordnet ist.
13. Klicken Sie mit der rechten Maustaste auf den *DHCP-Relay-Agent*-Knoten und wählen Sie im Kontextmenü den Befehl *Neue Schnittstelle*. Daraufhin erscheint das Dialogfeld *Neue Schnittstelle für DHCP-Relay-Agent*.
14. Wählen Sie die Schnittstelle zum Subnetz aus, auf der Sie den Relay-Agenten installieren wollen, und klicken Sie auf *OK*. Das Dialogfeld *Eigenschaften von DHCP-Relay-Eigenschaften* für die Schnittstelle erscheint.
15. Lassen Sie das Kontrollkästchen *DHCP-Pakete weiterleiten* ausgewählt und konfigurieren Sie bei Bedarf die folgenden Einstellungen:
 - **Schwellenwert des Abschnittszählers** Gibt die maximale Anzahl von Relay-Agenten an, über die DHCP-Meldungen laufen können, bevor sie verworfen werden. Der Standardwert ist 4 und der Maximalwert 16. Diese Einstellung verhindert, dass DHCP-Meldungen endlos im Netzwerk weitergeleitet werden.
 - **Neustart-Schwellenwert (Sekunden)** Gibt die Zeitspanne an, die der Relay-Agent wartet, bevor er eine empfangene DHCP-Meldung weiterleitet. Der Standardwert beträgt 4 Sekunden. Mit dieser Einstellung können Sie steuern, welcher DHCP-Server die Clients für ein bestimmtes Subnetz verarbeitet.
16. Klicken Sie auf *OK*.
17. Klicken Sie mit der rechten Maustaste auf den *DHCP-Relay-Agent*-Knoten und wählen Sie im Kontextmenü den Befehl *Eigenschaften*. Es erscheint das Dialogfeld *Eigenschaften von DHCP-Relay-Agent* (siehe Abbildung 4.13).

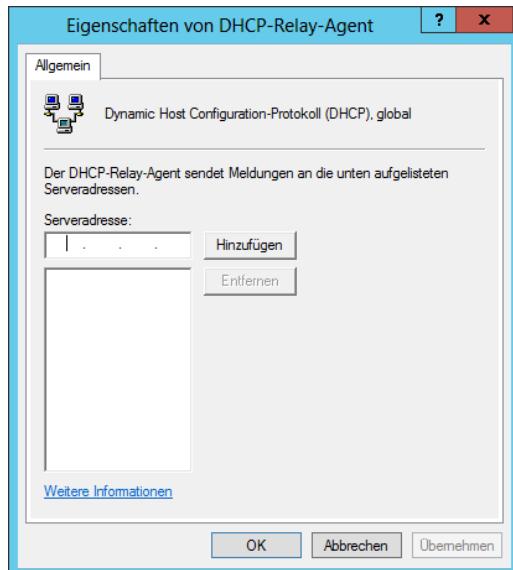


Abbildung 4.13 Das Dialogfeld *Eigenschaften von DHCP-Relay-Agent*

18. Geben Sie die IP-Adresse des DHCP-Servers ein, zu dem der Agent die Meldungen weiterleiten soll, und klicken Sie auf *Hinzufügen*. Wiederholen Sie bei Bedarf diesen Schritt, um weitere Server hinzuzufügen.
19. Klicken Sie auf *OK*.
20. Schließen Sie die Routing- und RAS-Konsole.

Der Server ist nun dafür konfiguriert, DHCP-Meldungen an die festgelegten Serveradressen weiterzuleiten.

Prüfungszielzusammenfassung

- DHCP ist ein Dienst, der automatisch die IP-Adresse und andere TCP/IP-Einstellungen auf Netzwerkcomputern konfiguriert. Dabei weist er Adressen aus einem Pool (einem sogenannten Bereich) zu und gibt sie wieder frei, wenn sie nicht mehr verwendet werden.
- DHCP besteht aus drei Komponenten: einer DHCP-Serveranwendung, einem DHCP-Client und einem DHCP-Kommunikationsprotokoll
- Die DHCP-Standards definieren drei verschiedene Methoden der IP-Adresszuweisung: dynamische, automatische und manuelle Zuweisung

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welcher der folgenden Begriffe bezeichnet die Komponente, die DHCP-Clients in die Lage versetzt, mit DHCP-Servern in anderen Subnetzen zu kommunizieren?
 - A. Weiterleitung
 - B. Resolver
 - C. Bereich
 - D. Relay-Agent
2. Welcher der folgenden Meldungstypen wird während einer erfolgreichen DHCP-Adresszuweisung nicht verwendet?
 - A. DHCPDISCOVER
 - B. DHCPREQUEST
 - C. DHCPACK
 - D. DHCPINFORM

3. Welcher der folgenden Arten von DHCP-Adresszuweisung ist in Windows Server 2012 einer Reservierung äquivalent?
 - A. Dynamische Zuweisung
 - B. Automatische Zuweisung
 - C. Manuelle Zuweisung
 - D. Hybride Zuweisung
4. Welche der folgenden Netzwerkkomponenten sind normalerweise in der Lage, als DHCP-Relay-Agenten zu fungieren?
 - A. Windows 8-Computer
 - B. Router
 - C. Switches
 - D. Windows Server 2012-Computer
5. Welcher der folgenden TCP/IP-Parameter wird normalerweise als Bereichsoption in DHCP bereitgestellt?
 - A. DNS-Server
 - B. Subnetzmaske
 - C. Leasedauer
 - D. Standardgateway



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Nachdem Ralph als Leiter der IT-Abteilung bei Contoso, Ltd., eine große Anzahl von WLAN-Laptops im Netzwerk bereitgestellt hat, entscheidet er sich für DHCP, damit die Laptop-Benutzer von einem Subnetz zu einem anderen wechseln können, ohne ihre IP-Adressen manuell neu zu konfigurieren. Allerdings bemerkt Ralph kurz nach der DHCP-Bereitstellung, dass einige der IP-Adressbereiche erschöpft sind, wodurch sich manche Computer nicht mit einem neuen Subnetz verbinden können.

Beantworten Sie für dieses Szenario die folgende Frage:

Wie kann Ralph dieses Problem lösen, ohne das Subnetzkonzept des Netzwerks zu ändern?

Prüfungsziel 4.3: Den DNS-Dienst bereitstellen und konfigurieren

DNS ist ein entscheidendes Element sowohl für die Internet- als auch für die Active Directory-Kommunikation. Die gesamte TCP/IP-Kommunikation basiert auf IP-Adressen. Jeder Computer in einem Netzwerk besitzt mindestens eine Netzwerkschnittstelle, die im TCP/IP-Sprachgebrauch als Host bezeichnet wird, und jeder Host verfügt über eine IP-Adresse, die in diesem Netzwerk eindeutig ist. Jedes durch ein TCP/IP-System übertragene Datagramm enthält die IP-Adresse des sendenden Computers und die IP-Adresse des vorgesehenen Empfängers. Wenn aber Benutzer auf einen freigegebenen Ordner im Netzwerk oder auf eine Website im Internet zugreifen, geben sie einen Hostnamen an und keine IP-Adresse. Das hängt damit zusammen, dass sich Namen wesentlich leichter merken lassen als IP-Adressen.

Dieses Prüfungsziel zeigt, wie Sie

- Active Directory-Integration von Primärzonen konfigurieren
 - Weiterleitungen konfigurieren
 - Stammhinweise konfigurieren
 - DNS-Cache verwalten
 - A- und PTR-Ressourceneinträge erstellen
-

Die DNS-Architektur

Damit TCP/IP-Systeme diese verständlichen Hostnamen verwenden können, müssen sie die dem Namen zugeordnete IP-Adresse herausfinden können. In der Anfangszeit der TCP/IP-Netzwerke besaß jeder Computer eine Liste der Namen und ihrer äquivalenten IP-Adressen – eine sogenannte *Hosttabelle*. Zu jener Zeit war es wegen der geringen Anzahl von Computern im sich gerade entwickelnden Internet noch praktikabel, eine einzige Hosttabelle zu verwalten und zu verteilen.

Heute gibt es im Internet Millionen von Computern und die Vorstellung von Wartung und Verteilung einer einzigen Datei, die sämtliche Namen dafür enthält, ist absurd. Anstelle einer Hosttabelle, die auf jedem Computer gespeichert ist, verwenden heutige TCP/IP-Netzwerke DNS-Server, um Hostnamen in IP-Adressen umzuwandeln. Diese Umwandlung wird als *Namensauflösung* bezeichnet.

Im Kern ist das DNS immer noch eine Liste von Namen und ihren äquivalenten IP-Adressen, doch unterscheiden sich die Methoden, um diese Namen zu erstellen, zu speichern und abzurufen, erheblich von denen in einer Hosttabelle. Das DNS besteht aus drei Elementen:

- **DNS-Namespace** Die DNS-Standards definieren einen baumartig strukturierten Namespace, in dem jeder Zweig des Baums eine Domäne identifiziert. Jede Domäne enthält eine Auflistung von Ressourceneinträgen, die Hostnamen, IP-Adressen und andere Informationen enthalten. Abfrageoperationen sind Versuche, bestimmte Ressourceneinträge von einem bestimmten Domänennamen abzurufen.

- **Namenserver** Ein DNS-Server ist eine Anwendung, die auf einem Servercomputer läuft und Informationen über die Domänenbaumstruktur verwaltet sowie (üblicherweise) Autorisierungsinformationen über eine oder mehrere spezifische Domänen in dieser Struktur enthält. Die Anwendung ist in der Lage, auf Abfragen nach Informationen über die Domänen zu reagieren, für die es die Autorität verkörpert, und auch Abfragen über andere Domänen an andere Namenserver weiterzuleiten. Somit kann jeder DNS-Server auf Informationen über jede Domäne in der Baumstruktur zugreifen.
- **Resolver** Ein Resolver ist ein Clientprogramm, das DNS-Abfragen generiert und sie an einen DNS-Server zur Ausführung sendet. Ein Resolver hat direkten Zugriff auf wenigstens einen DNS-Server und kann auch Weiterleitungen verarbeiten, um seine Abfragen bei Bedarf an andere Server zu richten

In der grundlegendsten Form besteht die DNS-Namensauflösung aus einem Resolver, der eine Namensauflösungsanforderung an seinen designierten Server sendet. Wenn der Server keine Informationen über den angeforderten Namen besitzt, leitet er die Anforderung an einen anderen DNS-Server im Netzwerk weiter. Der zweite Server generiert eine Antwort mit der IP-Adresse des angeforderten Namens und gibt sie an den ersten Server zurück, der die Informationen an den Resolver weiterleitet, wie Abbildung 4.14 zeigt. In der Praxis kann die DNS-Namensauflösung jedoch wesentlich komplexer sein, wie die nächsten Abschnitte erläutern.

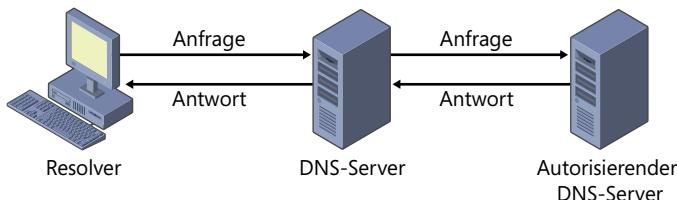


Abbildung 4.14 DNS-Server leiten Anfragen und Antworten an andere DNS-Server weiter

DNS-Kommunikation

Auch wenn sämtliche Internet-Anwendungen per DNS Hostnamen zu IP-Adressen auflösen, lässt sich diese Namensauflösung am einfachsten verfolgen, wenn Sie mit einem Webbrower auf eine Internet-Site zugreifen. Wenn Sie in das Adressfeld des Browsers eine URL mit einem DNS-Namen (zum Beispiel www.microsoft.com) eingeben und die -Taste drücken, sehen Sie möglicherweise für einen kurzen Augenblick eine Meldung mit etwa dem Wortlaut: »Suche Site: www.microsoft.com.« Einige Sekunden später erscheint dann eine Meldung »Verbinden mit«, gefolgt von einer IP-Adresse. In dieser Zeitspanne findet die DNS-Namensauflösung statt.

Aus dem Blickwinkel des Clients besteht die Prozedur, die während dieser wenigen Sekunden stattfindet, aus der Anwendung, die eine Abfragenachricht mit dem aufzulösenden Namen an ihren designierten DNS-Server sendet. Der Server antwortet daraufhin mit einer Nachricht, die die IP-Adresse für diesen Namen enthält. Mit der bereitgestellten Adresse kann die Anwendung dann eine Nachricht an das vorgesehene Ziel senden. Wie komplex der Vorgang wirklich ist, können Sie nur sehen, wenn Sie dabei die Rolle des DNS-Servers untersuchen.

Um die Beziehungen zwischen den DNS-Servern für verschiedene Domänen im Namespace besser erläutern zu können, zeigt der folgende Ablauf den Vorgang der Internet-Namensauflösung.

1. Ein Benutzer auf einem Clientsystem gibt den DNS-Namen eines Internet-Servers in einer Anwendung wie zum Beispiel einem Webbrowser ein. Die Anwendung generiert einen API (Application Programming Interface)-Aufruf zum Resolver auf dem Client-System und der Resolver erzeugt eine rekursive DNS-Abfragenachricht mit dem Servernamen und sendet sie zu dem DNS-Server, der in der TCP/IP-Konfiguration des Computers verzeichnet ist (siehe Abbildung 4.15).

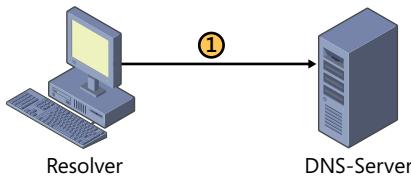


Abbildung 4.15 Der Client-Resolver sendet eine Abfrage zur Namensauflösung an seinen DNS-Server

2. Der DNS-Server des Clients empfängt die Abfrage und überprüft dann anhand seiner Ressourceneinträge, ob er die autorisierende Quelle für die Zone ist, die den angeforderten Servernamen enthält. Trifft das nicht zu (der typische Fall), generiert der Server eine iterative Abfrage und übermittelt sie an einen der *Stammnamenserver* (siehe Abbildung 4.16). Der Stammnamenserver untersucht den vom DNS-Server des Clients angeforderten Namen und sieht in seinen Ressourceneinträgen nach, um die autorisierenden Server für die Toplevel-Domäne (Domäne der obersten Ebene) des Namens zu ermitteln. Dann sendet der Stammnamenserver eine Antwort an den DNS-Server des Clients mit einer Referenz auf die Adressen der Server der Toplevel-Domäne.

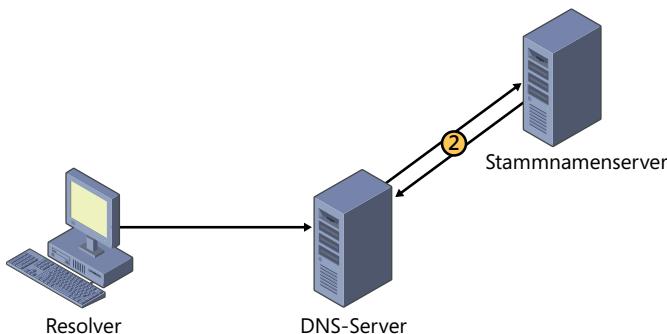


Abbildung 4.16 Der DNS-Server des Clients leitet die Anfrage an einen Stammnamenserver weiter

3. Der DNS-Server des Clients, der jetzt im Besitz der Serveradresse der Toplevel-Domäne für den angeforderten Namen ist, generiert eine neue iterative Abfrage und sendet sie an den Server der Toplevel-Domäne, wie Abbildung 4.17 zeigt. Der Server der Toplevel-Domäne untersucht die Domäne der zweiten Ebene im angeforderten Namen und sendet ein Referenz mit den Adressen der autorisierenden Server für diese Domäne der zweiten Ebene zurück an den DNS-Server des Clients.

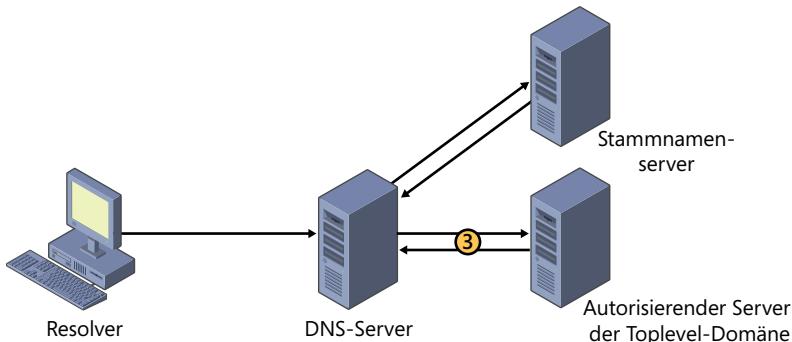


Abbildung 4.17 Der DNS-Server des Clients leitet die Anfrage an einen Server der Toplevel-Domäne weiter



Hinweis Zusammengefasste Schritte

Bei der eben beschriebenen DNS-Namensaüflösung wird die Auflösung der Namen in den Domänen der obersten und zweiten Ebenen in Form separater Schritte dargestellt, was oftmals nicht der Realität entspricht. Die gebräuchlichsten Toplevel-Domänen wie zum Beispiel *com*, *net* und *org* werden tatsächlich von den Stammnamenserven gehostet. Damit entfällt eine Weiterleitung bei der Namensaüflösung.

4. Der DNS-Server des Clients generiert eine weitere iterative Abfrage und sendet sie an den Server in der Domäne der zweiten Ebene, wie Abbildung 4.18 zeigt. Ist der Server in der Domäne der zweiten Ebene die Autorität für die Zone, die den angeforderten Namen enthält, konsultiert er seine Ressourceneinträge, um die IP-Adresse des anfordernden Systems zu ermitteln, und sendet sie in einer Antwortnachricht zurück an den DNS-Server dieses Clients.

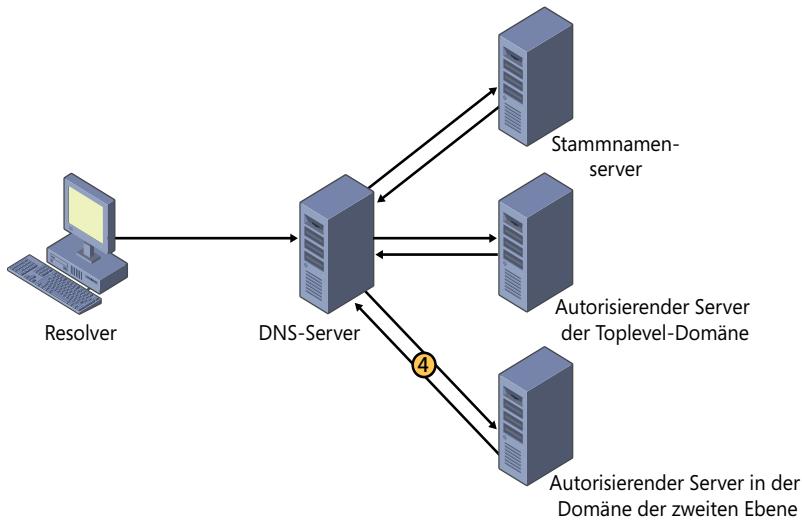


Abbildung 4.18 Der DNS-Server des Clients leitet die Anforderung an einen Server in der Domäne der zweiten Ebene

5. Der DNS-Server des Clients empfängt die Antwort vom autorisierenden Server und sendet die IP-Adresse zurück an den Resolver auf dem Clientsystem (siehe Abbildung 4.19). Der Resolver leitet die Adresse an die Anwendung weiter, die dann eine IP-Kommunikation mit dem vom Benutzer angegebenen System einleiten kann.

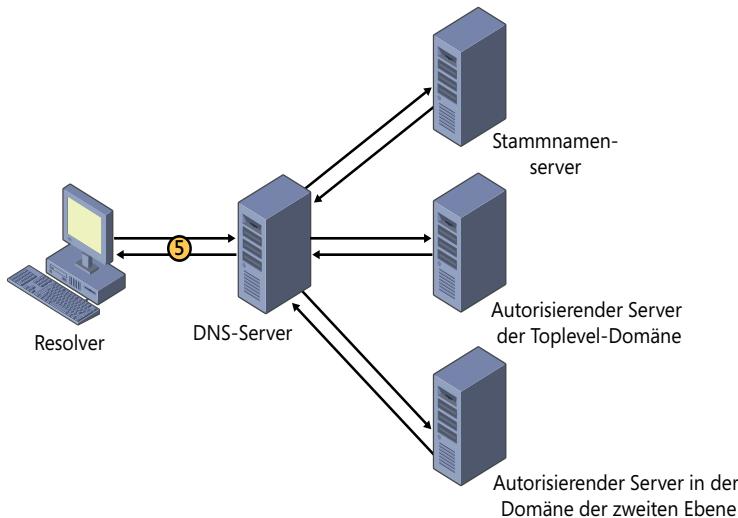


Abbildung 4.19 Der DNS-Server des Clients antwortet dem Client-Resolver

Abhängig vom Namen, den der Client aufzulösen versucht, kann dieser Vorgang einfacher oder auch beträchtlich komplexer sein, als hier dargestellt. Ist andererseits der DNS-Server des

Clients die Autorität für die Domäne, in der der angeforderte Name liegt, sind weder andere Server noch iterative Abfragen erforderlich. Enthält aber der angeforderte Name drei oder mehr Domänenebenen, können zusätzliche iterative Abfragen anfallen.

Diese Prozedur setzt auch eine erfolgreiche Fertigstellung der Namensauflösung voraus. Wenn irgendeiner der abgefragten autoritativen DNS-Server eine Fehlermeldung an den DNS-Server des Clients zurückgibt, die zum Beispiel besagt, dass eine der Domänen im Namen nicht existiert, wird diese Fehlermeldung zurück an den Client geleitet und die Namensauflösung gilt als gescheitert.

DNS-Server-Caching

Die DNS-Namensauflösung mag lang und komplex erscheinen, doch in vielen Fällen braucht der DNS-Server des Clients keine Abfragen an die Server zu schicken, die im angeforderten DNS-Namen angegeben sind. Das hängt damit zusammen, dass DNS-Serer in der Lage sind, die Informationen zu behalten, die sie über den DNS-Namespace im Verlauf der Namensauflösungen in Erfahrung gebracht haben, und sie auf dem lokalen Laufwerk zu speichern.

Beispielsweise speichert ein DNS-Server, der Anforderungen von Clients empfängt, die Adressen der angeforderten Systeme und die Adressen für autorisierende Server der jeweiligen Domänen. Wenn der Client beim nächsten Mal die Auflösung eines bereits aufgelösten Namens anfordert, kann der Server unmittelbar mit den zwischengespeicherten Daten antworten. Und wenn ein Client einen anderen Namen in einer dieser Domänen anfordert, kann der Server eine Abfrage direkt an einen autoritativen Server für die jeweilige Domäne senden und muss nicht erst einen Stammnamenserver kontaktieren. Somit lassen sich die Namen in häufig aufgerufenen Domänen im Allgemeinen schnell auflösen, da einer der Server auf den dazwischen liegenden Stationen bereits Informationen über die Domäne im Cache stehen hat, während Namen in »finsternen Domänenecken« länger benötigen, da der ganze Anforderungs-/Weiterleitungsprozess notwendig ist.

Caching ist ein entscheidendes Element der DNS-Architektur, denn es verringert die Anzahl der Anfragen, die an die Stammnamen- und Toplevel-Domänen-Server zu senden sind. Diese Server, die ja an der Spitze der DNS-Struktur stehen, kommen am wahrscheinlichsten als Engpass für das Gesamtsystem infrage. Allerdings müssen Caches schließlich freigemacht werden und es gibt eine feine Linie zwischen effektivem und ineffektivem Caching.

Da DNS-Server in ihren Caches Ressourceneinträge behalten, kann es Stunden oder sogar Tage dauern, bis sich Änderungen bei einem autorisierenden Server über das Internet verbreitet haben. Während dieses Zeitraums erhalten Benutzer möglicherweise fehlerhafte Informationen als Antwort auf eine Abfrage. Wenn Informationen zu lange in Servercaches verbleiben, vergeht zu viel Zeit, bis sich die Änderungen, die Administratoren an den Daten in ihren DNS-Servern vorgenommen haben, im Internet verbreitet haben. Werden Caches zu schnell geleert, steigt die Anzahl der Anforderungen, die an die Stammnamen- und Toplevel-Domänen-Server gesendet werden, steil an.

Die Zeitspanne, für die DNS-Daten auf einem Server im Cache verbleiben, wird als *Time to Live (TTL)* bezeichnet. Im Unterschied zu den meisten Datencaches wird der TTL-Wert nicht vom Administrator des Servers, auf dem der Cache gespeichert ist, vorgegeben. Stattdessen

legen die Administratoren jedes autorisierenden DNS-Servers fest, wie lange die Daten für die Ressourceneinträge in ihren Domänen oder Zonen in dem Server, wo sie zwischengespeichert werden, aufzubewahren sind. Damit können Administratoren einen TTL-Wert basierend auf der Volatilität ihrer Serverdaten spezifizieren. In einem Netzwerk, in dem häufig Änderungen an IP-Adressen auftreten oder neue Ressourceneinträge hinzukommen, erhöht ein geringerer TTL-Wert die Wahrscheinlichkeit, dass Clients aktuelle Daten erhalten. Wenn in einem Netzwerk relativ selten Änderungen vorkommen, lässt sich mit einem höheren TTL-Wert die Anzahl der Anfragen verringern, die an die übergeordneten Server Ihrer Domäne oder Zone gesendet werden.

Um den TTL-Wert für eine Zone auf einem Windows Server 2012-DNS-Server zu ändern, klicken Sie mit der rechten Maustaste auf die Zone, öffnen das Eigenschaftenblatt und gehen auf die Registerkarte *Autoritätsursprung (SOA)*, die in Abbildung 4.20 zu sehen ist. Auf dieser Registerkarte können Sie den TTL-Wert für diese Eintragseinstellung auf einen vom Standardwert (1 Stunde) abweichenden Wert setzen.

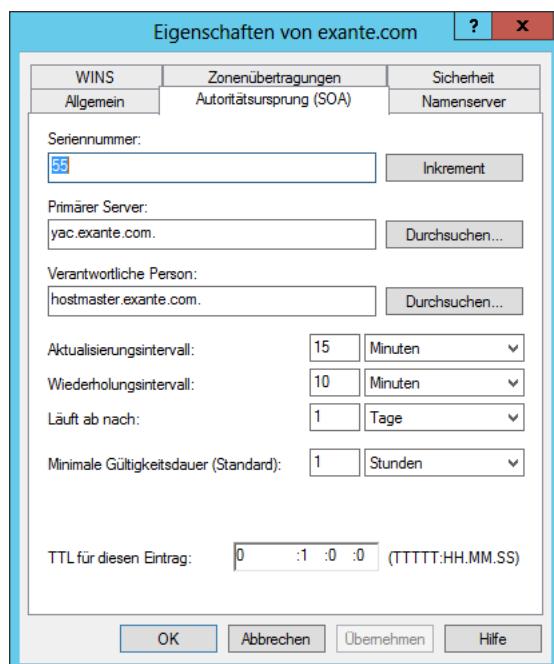


Abbildung 4.20 Die Registerkarte *Autoritätsursprung (SOA)* auf dem Eigenschaftenblatt eines DNS-Servers

DNS-Referrals und -Abfragen

Der Vorgang, bei dem der eine DNS-Server eine Anforderung zur Namensauflösung an einen anderen DNS-Server sendet, wird als *Referral* bezeichnet. Referrals sind für die DNS-Namensauflösung entscheidend.

Wie Ihnen sicherlich in dem weiter vorn beschriebenen Prozess aufgefallen ist, hat der Client nur insofern mit der Namensauflösung zu tun, als dass er eine Abfrage sendet und eine Antwort empfängt. Der DNS-Server des Clients muss gegebenenfalls Referrals an mehrere Server senden, bevor er denjenigen Server erreicht, der die benötigten Informationen besitzt.

DNS-Server erkennen die folgenden zwei Arten von Namensauflösungsanforderungen:

- **Rekursive Abfrage** Bei einer rekursiven Abfrage übernimmt der DNS-Server, der die Namensauflösungsanforderung empfängt, die volle Verantwortung für die Namensauflösung. Wenn der Server Informationen zum angeforderten Namen besitzt, antwortet er sofort dem Anfordernden. Besitzt der Server keine Informationen zum Namen, sendet er Referrals an andere DNS-Server, bis er die benötigten Informationen erhält. TCP/IP-Client-Resolver senden immer rekursive Abfragen an ihre vorgesehenen DNS-Server.
- **Iterative Abfrage** In einer iterativen Abfrage antwortet der Server, der die Namensauflösungsanforderung empfängt, sofort mit den besten Informationen, die er zu diesem Zeitpunkt besitzt. DNS-Server verwenden iterative Abfragen, wenn sie miteinander kommunizieren. In den meisten Fällen wäre es unzweckmäßig, einen DNS-Server so zu konfigurieren, dass er eine rekursive Abfrage an einen anderen DNS-Server sendet. Iterative Abfragen sendet ein DNS-Server nur an einen anderen Server, wenn es sich um einen speziellen Servertyp – eine sogenannte *Weiterleitung (Forwarder)* – mit einer besonderen Konfiguration handelt, um mit anderen Servern auf diese Art und Weise zu interagieren.

DNS-Weiterleitungen

DNS-Server senden rekursive Abfragen unter anderem dann an andere Server, wenn Sie einen Server für die Funktion *Weiterleitung* konfigurieren. Wenn in einem Netzwerk mehrere DNS-Server laufen, sollen sicherlich nicht alle Server Abfragen an andere DNS-Server im Internet senden. Besteht beispielsweise nur eine relativ langsame Verbindung zwischen Netzwerk und Internet, könnten mehrere Server zu viel Bandbreite beanspruchen, wenn sie alle wiederholt Abfragen senden.

Um dies zu verhindern, erlauben es die meisten DNS-Implementierungen, einen Server als Weiterleitung für alle Internetabfragen zu konfigurieren, die von den anderen Servern im Netzwerk erzeugt werden. Muss ein Server den DNS-Namen eines Internetsystems auflösen und kann er die erforderlichen Informationen in seinem Cache nicht finden, sendet er eine rekursive Abfrage an den Weiterleitungsserver, der dann dafür zuständig ist, seine eigenen iterativen Abfragen über die Internetverbindung zu senden. Nachdem der Weiterleitungsserver den Namen aufgelöst hat, sendet er eine Antwort zurück an den ursprünglichen DNS-Server, der sie an den Client weiterleitet.

Um Weiterleitungen auf einem Windows Server 2012-DNS-Server zu konfigurieren, klicken Sie mit der rechten Maustaste auf den Serverknoten, öffnen das Eigenschaftenblatt und gehen auf die Registerkarte *Weiterleitungen*, wie sie Abbildung 4.21 zeigt. Auf dieser Registerkarte können Sie die Namen und Adressen der Server hinzufügen, die Ihr Server als Weiterleitungen verwenden soll.

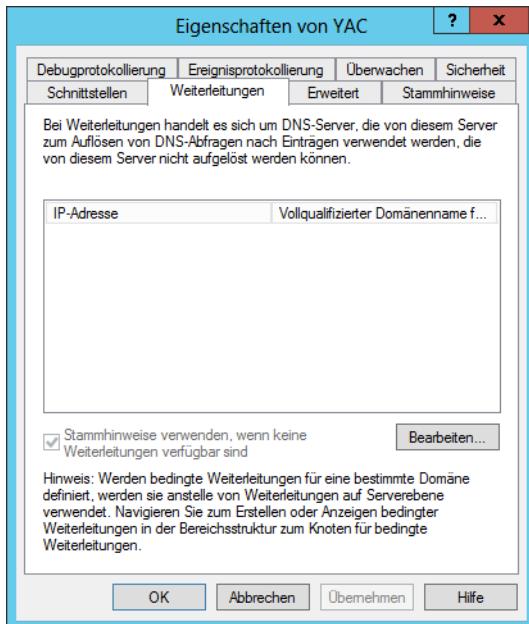


Abbildung 4.21 Die Registerkarte *Weiterleitungen* auf dem Eigenschaftenblatt eines DNS-Servers

Reversenamenauflösung

Der weiter vorn beschriebene Prozess der Namensauflösung hat die Aufgabe, DNS-Namen in IP-Adressen umzuwandeln. Allerdings kann es auch vorkommen, dass ein Computer eine IP-Adresse in einen DNS-Namen umwandeln muss. Dies wird als *Reversenamenauflösung* (Reverse-Lookup von Namen) bezeichnet.

Da die Domänenhierarchie nach Domänennamen gegliedert ist, gibt es keinen augenscheinlichen Weg, eine IP-Adresse mithilfe von iterativen Abfragen in einen Namen aufzulösen, außer die Anforderung der Reversenamenauflösung an jeden DNS-Server im Internet weiterzuleiten, um die angeforderte Adresse zu suchen – ein offenbar nicht praktikabler Weg.

Um diesem Problem zu begegnen, haben die Entwickler des DNS eine spezielle Domäne geschaffen, die *in-addr.arpa*, die speziell für die Reversenamenauflösung konzipiert ist. Die Domäne der zweiten Ebene *in-addr.arpa* enthält vier zusätzliche Ebenen von Subdomänen. Jede der vier Ebenen besteht aus Subdomänen, die mit den Zahlenwerten von 0 bis 255 benannt sind. Zum Beispiel gibt es unterhalb von *in-addr.arpa* 256 Domänen der dritten Ebene, die die Namen von *0.in-addr.arpa* bis *255.in-addr.arpa* tragen. Unter diesen 256 Domänen der dritten Ebene gibt es jeweils 256 Domänen der vierten Ebene, die ebenfalls von 0 bis 255 nummeriert sind, und jede Domäne der vierten Ebene führt zu 256 Domänen der fünften Ebene (siehe Abbildung 4.22). Jede Domäne dieser fünften Ebene kann bis zu 256 Hosts enthalten, die ebenfalls von 0 bis 255 nummeriert sind.

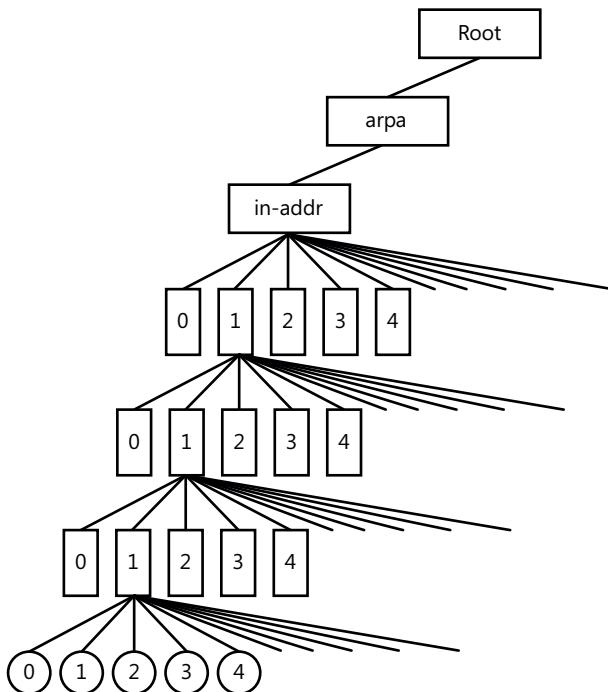


Abbildung 4.22 Die DNS-Reverse-Lookupdomäne

Mithilfe dieser Hierarchie von Subdomänen ist es möglich, die ersten drei Bytes einer IP-Adresse als DNS-Domänenname auszudrücken und einen Ressourceneintrag zu erstellen, der nach dem vierten Byte in der jeweiligen Domäne der fünften Ebene benannt ist. Um zum Beispiel die IP-Adresse 192.168.89.34 in einen Namen aufzulösen, würde ein DNS-Server eine Domäne namens `89.168.192.in-addr.arpa` in der üblichen Weise suchen und den Inhalt des Ressourceneintrags namens `34` in dieser Domäne lesen.



Hinweis Reverse-Lookup-Adressen

In der Domäne `in-addr.arpa` ist die IP-Adresse im Domänennamen umgekehrt, weil bei IP-Adressen das unwichtigste Bit (d.h. die Hostkennung) rechts steht, bei vollqualifizierten DNS-Domänennamen (FQDNs) der Host jedoch links erscheint.

Einen DNS-Server bereitstellen

Um einen DNS-Server auf einem Windows Server 2012-Computer bereitzustellen, genügt es, die DNS-Serverrolle mit dem Assistenten zum Hinzufügen von Rollen und Features im Server-Manager zu installieren. Die eigentliche Installation verlangt keine weiteren Eingaben, es gibt keine zusätzlichen Seiten im Assistenten und es sind keine Rollendienste auszuwählen.

Sobald Sie die DNS-Serverrolle installiert haben, ist der Computer bereit, reine auf Caching orientierte Namensauflösungsdienste für alle Clients, die auf ihn zugreifen können,

durchzuführen. Die Rolle installiert auch die DNS-Manager-Konsole, mit der Sie die anderen Funktionen des DNS-Servers konfigurieren. Die folgenden Abschnitte erläutern, wie Sie den Server für andere Dienste konfigurieren.

Zonen erstellen

Eine Zone ist eine administrative Entität, die Sie auf einem DNS-Server einrichten, um einen separaten Teil des DNS-Namespace darzustellen. Normalerweise gliedern Administratoren den DNS-Namespace in Zonen, um sie auf verschiedenen Servern zu speichern und ihre Verwaltungsaufgaben an andere Personen zu delegieren. Zonen bestehen immer aus ganzen Domänen oder Subdomänen. Es lässt sich auch eine Zone einrichten, die mehrere Domänen enthält, sofern diese Domänen im DNS-Namespace zusammenhängend sind. Zum Beispiel können Sie eine Zone aus einer übergeordneten Domäne und ihrer untergeordneten Domäne bilden, weil sie direkt miteinander verbunden sind. Dagegen können Sie keine Zone aus zwei untergeordneten Domänen ohne ihre gemeinsame übergeordnete Domäne erstellen, weil die beiden untergeordneten Domänen nicht direkt miteinander verbunden sind (siehe Abbildung 4.23).

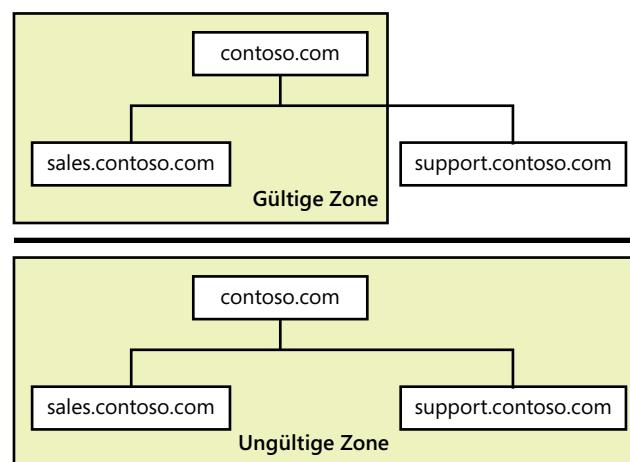


Abbildung 4.23 Gültige Zonen müssen aus zusammenhängenden Domänen bestehen

Bei Bedarf können Sie den DNS-Namespace in mehrere Zonen gliedern und sie auf ein und demselben DNS-Server hosten, auch wenn es keinen überzeugenden Grund dafür gibt. Der DNS-Server in Windows Server 2012 kann bis zu 200.000 Zonen auf einem einzelnen Server unterstützen. Allerdings lässt sich nur schwer ein Szenario vorstellen, das so viele Zonen verlangen würde. In der Regel richtet ein Administrator mehrere Zonen auf einem Server ein und delegiert dann die meisten davon auf andere Server, die dann dafür zuständig sind, die Zonen zu hosten.

Jede Zone besteht aus einer Zonendatenbank, die die Ressourceneinträge für die Domänen in dieser Zone enthält. Der DNS-Server in Windows Server 2012 unterstützt die folgenden drei Zonentypen, die festlegen, wo der Server die Zonendatenbank speichert und welche Art von Informationen sie enthält:

- **Primäre Zone** Erzeugt eine primäre Zone, die die Masterkopie der Zonendatenbank enthält, wo Administratoren alle Änderungen an den Ressourceneinträgen der Zone vornehmen. Wenn das Kontrollkästchen *Zone in Active Directory speichern (DNS-Server muss als schreibbarer Domänencontroller eingerichtet sein)* deaktiviert ist, erstellt der Server eine primäre Masterzonendatenbankdatei auf dem lokalen Laufwerk. Dabei handelt es sich um eine einfache Textdatei, die mit den meisten Nicht-Windows-DNS-Server-Implementierungen kompatibel ist.
- **Sekundäre Zone** Erzeugt ein Duplikat einer primären Zone auf einem anderen Server. Die sekundäre Zone enthält eine Sicherungskopie der primären Masterzonendatenbankdatei, die als identische Textdatei auf dem lokalen Laufwerk des Servers gespeichert wird. Die Ressourceneinträge in einer sekundären Zone lassen sich nur aktualisieren, wenn Sie die primäre Masterzonendatenbankdatei durch eine sogenannte Zonenübertragung replizieren.
- **Stubzone** Erzeugt eine Kopie einer primären Zone mit den Schlüsselressourceninträgen, die die autorisierenden Server für die Zone identifizieren. Die Stubzone leitet Anfragen weiter oder referenziert sie. Wenn Sie eine Stubzone erstellen, konfigurieren Sie sie mit der IP-Adresse des Servers, der die Zone hostet, von der Sie den Stub erstellt haben. Empfängt der Server, der die Stubzone hostet, eine Anfrage nach einem Namen in dieser Zone, leitet er entweder die Anforderung an den Host der Zone weiter oder antwortet mit einer Referral zu diesem Host. Das hängt davon ab, ob die Anfrage rekursiv oder iterativ ist.

DNS wurde schon lange vor Active Directory entworfen, sodass sich der größte Teil des Internets auf primäre und sekundäre Zonen mithilfe von textbasierten Datenbankdateien stützt. Die gebräuchlichste DNS-Server-Implementierung im Internet ist ein UNIX-Programm namens BIND, das diese Datenbanken verwendet.

Für DNS-Server, die interne Domänen – und insbesondere AD DS-Domänen – unterstützen, wird empfohlen, mit dem Windows DNS-Server eine primäre Zone zu erstellen und sie in Active Directory zu speichern. Wenn Sie die Zone in der AD DS-Datenbank speichern, brauchen Sie keine sekundären Zonen zu erstellen oder Zonenübertragungen vorzunehmen, da es AD DS übernimmt, die Daten zu replizieren. Außerdem werden die DNS-Daten geschützt, egal welche Sicherungslösung Sie verwenden, um Active Directory zu schützen.



Prüfungstipp Die Prüfung 70-410 deckt nur das Erstellen einer primären Zone ab, die in Active Directory gespeichert ist. Die Abläufe für das Erstellen textbasierter primärer und sekundärer Zonen und die Konfiguration von Zonenübertragungen sind Gegenstand der Zertifizierungsprüfung 70-411, »Administering Windows Server 2012«, im Lernziel »Configure DNS Zones«.

Active Directory-integrierte Zonen

Wenn Sie den DNS-Server-Dienst auf einem Computer ausführen, der als Active Directory-Domändienste-Domänencontroller konfiguriert ist und Sie das Kontrollkästchen *Zone in Active Directory speichern (DNS-Server muss als schreibbarer Domänencontroller*

eingerichtet sein) aktivieren, während Sie eine Zone im Assistenten zum Erstellen neuer Zonen konfigurieren, legt der Server keine Zonendatenbankdatei an. Stattdessen speichert der Server die DNS-Ressourceneinträge für die Zone in der AD DS-Datenbank. Ist die DNS-Datenbank in Active Directory gespeichert, ergeben sich eine Reihe von Vorteilen, so unter anderem eine einfachere Administration, Erhaltung der Netzwerkbandbreite und erhöhte Sicherheit.

In Active Directory-integrierten Zonen wird die Zonendatenbank automatisch auf andere Domänencontroller zusammen mit allen anderen Active Directory-Daten repliziert. Active Directory verwendet ein Mehrfach-Master-Replikationssystem, sodass Kopien der Datenbank auf allen Domänencontrollern in der Domäne aktualisiert werden. Die DNS-Ressourcen-einträge können Sie auf jedem Domänencontroller modifizieren, der eine Kopie der Zonen-datenbank hostet. Active Directory aktualisiert automatisch alle anderen Domänencontroller. Es ist nicht erforderlich, sekundäre Zonen zu erstellen oder Zonenübertragungen manuell zu konfigurieren, da Active Directory sämtliche Aktivitäten der Datenbankreplikation durchführt.

Standardmäßig repliziert Windows Server 2012 die Datenbank für eine primäre Zone, die in Active Directory gespeichert ist, auf alle anderen Domänencontroller, die den DNS-Server in der AD DS-Domäne ausführen, wo sich der primäre Domänencontroller befindet. Außerdem können Sie den Bereich der Zonendatenbankreplikation modifizieren, um Kopien auf allen Domänencontrollern im gesamten Unternehmen oder auf allen Domänencontrollern in der AD DS-Domäne zu behalten, unabhängig davon, ob sie den DNS-Server ausführen. Weiterhin ist es möglich, einen benutzerdefinierten Replikationsbereich zu erstellen, der die Zonendaten-bank auf die angegebenen Domänencontroller kopiert.

Active Directory erhält die Netzwerkbandbreite, indem es nur die DNS-Daten repliziert, die sich seit der letzten Replikation geändert haben, und die Daten vor der Übertragung über das Netzwerk komprimiert. Darüber hinaus nutzen Zonenübertragungen die vollen Sicherheitsfunktionen von Active Directory, die beträchtlich robuster sind als diejenigen von dateibasierten Zonenübertragungen.

Eine Active Directory-Zone erstellen

Um eine neue primäre Zone zu erstellen und sie in Active Directory zu speichern, gehen Sie wie folgt vor:

1. Melden Sie sich bei dem Windows Server 2012-Domänencontroller unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Klicken Sie auf *Tools / DNS*, um die *DNS-Manager*-Konsole zu öffnen.
3. Erweitern Sie den Serverknoten und wählen Sie den Ordner *Forward-Lookupzonen* aus.
4. Klicken Sie mit der rechten Maustaste auf den Ordner *Forward-Lookupzonen* und wählen Sie im Kontextmenü den Befehl *Neue Zone*. Der Assistent zum Erstellen neuer Zonen startet.
5. Klicken Sie auf *Weiter*, um die Seite *Willkommen* zu verlassen und die Seite *Zonentyp* zu öffnen.

6. Lassen Sie die Option *Primäre Zone* und das Kontrollkästchen *Zone in Active Directory speichern (DNS-Server muss als schreibbarer Domänencontroller eingerichtet sein)* ausgewählt und klicken Sie auf *Weiter*. Daraufhin erscheint die Seite *Active Directory-Zonenreplikationsbereich*.
7. Klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Zonenname*.
8. Geben Sie in das Textfeld *Zonenname* den Namen ein, den Sie der Zone zuweisen möchten, und klicken Sie auf *Weiter*. Die Seite *Dynamisches Update* wird geöffnet.
9. Wählen Sie eine der folgenden Optionen aus:
 - *Nur sichere dynamische Updates zulassen*
 - *Nicht sichere und sichere dynamische Updates zulassen*
 - *Dynamische Updates nicht zulassen*
10. Klicken Sie auf *Weiter*. Die Seite *Fertigstellen des Assistenten* wird geöffnet.
11. Klicken Sie auf *Fertig stellen*. Der Assistent erstellt die neue Zone.
12. Schließen Sie die *DNS-Manager*-Konsole.

Nachdem Sie eine primäre Zone erstellt haben, können Sie weitere Ressourceneinträge anlegen, die die Namen der Hosts im Netzwerk und deren äquivalente IP-Adressen spezifizieren.

Ressourceneinträge erstellen

Wenn Sie Ihren eigenen DNS-Server betreiben, erstellen Sie einen Ressourceneintrag für jeden Hostnamen, der vom übrigen Netzwerk aus zugänglich sein soll.

DNS-Server verwenden verschiedene Typen von Ressourceneinträgen. Die wichtigsten sind:

- **SOA (Autoritätsursprung)** Zeigt an, dass der Server die beste autorisierende Quelle für Daten ist, die die Zone betreffen. Jede Zone muss genau einen SOA-Eintrag besitzen.
- **NS (Namenserver)** Kennzeichnet einen DNS-Server, der als Autorität für die Zone fungiert. Jeder DNS-Server in der Zone (ob primärer oder sekundärer) muss durch einen NS-Eintrag dargestellt werden.
- **A (Adresse)** Gibt eine Name/Adresse-Zuordnung an, die eine IPv4-Adresse für einen bestimmten DNS-Namen liefert. Dieser Eintragstyp steht für die primäre Funktion des DNS: Namen in Adressen umwandeln.
- **AAAA (Adresse)** Gibt eine Name/Address-Zuordnung an, die eine IPv6-Adresse für einen bestimmten DNS-Namen liefert. Dieser Eintragstyp steht für die primäre Funktion des DNS: Namen in Adressen umwandeln.
- **PTR (Zeiger)** Gibt eine Adress/Name-Zuordnung an, die einen DNS-Namen für eine bestimmte Adresse in der Domäne *in-addr.arpa* liefert. Dieser Eintrag ist dem A-Eintrag funktionell entgegengesetzt und wird nur für Reverse-Lookups verwendet.

- **CNAME (Kanonischer Name)** Erstellt einen Alias, der auf den kanonischen Namen (d.h. den »wahren« Namen) eines Hosts zeigt, der durch einen A-Eintrag identifiziert wird. Administratoren stellen mithilfe von CNAME-Einträgen alternative Namen bereit, über die sich Systeme identifizieren lassen.
- **MX (Mail-Exchanger)** Kennzeichnet ein System, das E-Mail-Verkehr, der an eine Adresse in der Domäne gesendet wird, an den individuellen Empfänger, ein E-Mail-Gateway oder einen anderen Mailserver leitet



Prüfungstipp Die Prüfung 70-410 deckt nur das Erstellen von A- und PTR-Ressourceneinträgen ab. Die Abläufe für das Erstellen anderer Typen von Ressourceneinträgen sind Gegenstand der Zertifizierungsprüfung 70-411, »Administering Windows Server 2012«, im Prüfungsziel »Configure DNS Records«.

Um einen neuen Adressen-Ressourceneintrag zu erstellen, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Klicken Sie auf *Tools / DNS*, um die *DNS-Manager*-Konsole zu öffnen.
3. Erweitern Sie den Serverknoten und wählen Sie den Ordner *Forward-Lookupzonen* aus.
4. Klicken Sie mit der rechten Maustaste auf die Zone, in der Sie den Eintrag erstellen möchten, und wählen Sie im Kontextmenü den Befehl *Neuer Host (A oder AAAA)*. Daraufhin erscheint das Dialogfeld *Neuer Host*, das Abbildung 4.24 zeigt.

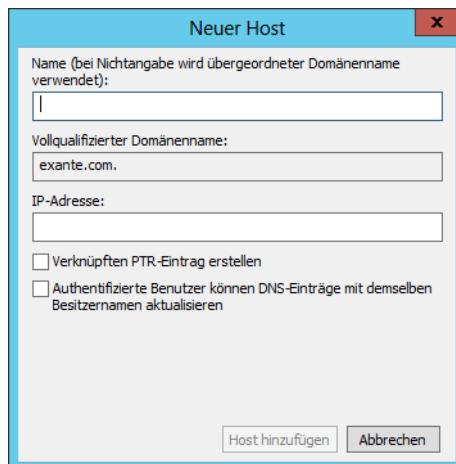


Abbildung 4.24 Das Dialogfeld *Neuer Host*

5. Geben Sie in das Textfeld *Name* den Hostnamen für den neuen Eintrag ein. Der FQDN für den Eintrag wird angezeigt.

6. Geben Sie in das Textfeld *IP-Adresse* die IPv4- oder IPv6-Adresse ein, die mit dem Hostnamen verknüpft ist.
7. Aktivieren Sie bei Bedarf die folgenden Kontrollkästchen:
 - **Verknüpften PTR-Eintrag erstellen** Erstellt einen Eintrag für Reverse-Lookups von Namen für den Host in der Domäne *in-addr.arpa*
 - **Authentifizierte Benutzer können DNS-Einträge mit demselben Besitzernamen aktualisieren** Erlaubt es Benutzern, ihre eigenen Ressourceneinträge zu modifizieren
8. Klicken Sie auf *Host hinzufügen*. Der neue Ressourceneintrag wird in der ausgewählten Zone erstellt.
9. Schließen Sie die *DNS-Manager*-Konsole.

Um einen PTR-Eintrag für einen neuen Host zu erstellen, aktivieren Sie im Dialogfeld *Neuer Host* das Kontrollkästchen *Verknüpften PTR-Eintrag erstellen*. Diese Einstellung ist aber nur wirksam, wenn auf dem Server bereits eine Reverse-Lookupzone vorhanden ist. Um die Zone zu erstellen, gehen Sie wie weiter oben beschrieben vor, wählen aber dieses Mal den Ordner *Reverse-Lookupzonen* aus.

Wenn Sie eine IPv4-Reverse-Lookupzone erstellen möchten, gelangen Sie auf die Seite *Name der Reverse-Lookupzone*, die in Abbildung 4.25 zu sehen ist. Hier können Sie die Netzwerk-kennung eingeben, mit der der Assistent die Zone erstellt.

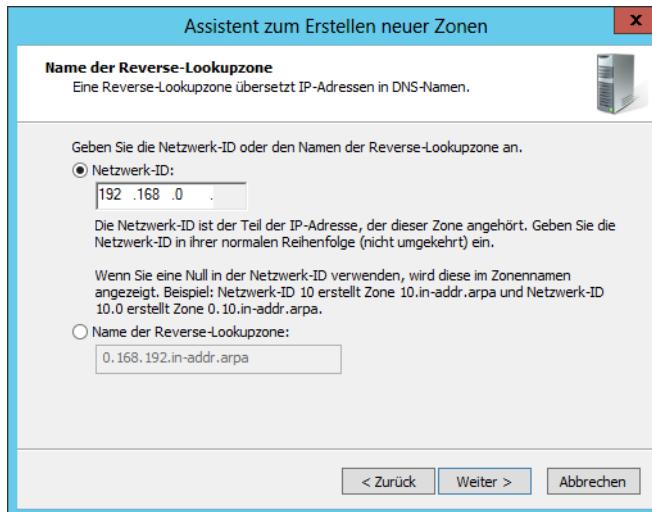


Abbildung 4.25 Die Seite *Name der Reverse-Lookupzone* im Assistenten zum Erstellen neuer Zonen

Nachdem die Zone erstellt ist, können Sie entweder PTR-Einträge zusammen mit A- oder AAAA-Einträgen oder einen neuen PTR-Eintrag über das Dialogfeld *Neuer Ressourcen-eintrag* erstellen.

DNS-Server-Einstellungen konfigurieren

Haben Sie einen DNS-Server installiert und darauf Zonen sowie Ressourceneinträge erstellt, können Sie mit verschiedenen Einstellungen das Verhalten anpassen. Die folgenden Abschnitte beschreiben einige dieser Einstellungen.

Active Directory-DNS-Replikation konfigurieren

Um den Replikationsbereich für eine Active Directory-integrierte Zone zu ändern, öffnen Sie das Eigenschaftenblatt der Zone in der *DNS-Manager-Konsole*, gehen auf die Registerkarte *Allgemein* und klicken auf die Schaltfläche *Ändern* neben *Replikation: Alle DNS-Server in dieser Domäne*, um das Dialogfeld *Bereich der Zonenreplikation ändern* zu öffnen (siehe Abbildung 4.26). Die Optionen sind die gleichen wie im Assistenten zum Erstellen neuer Zonen.

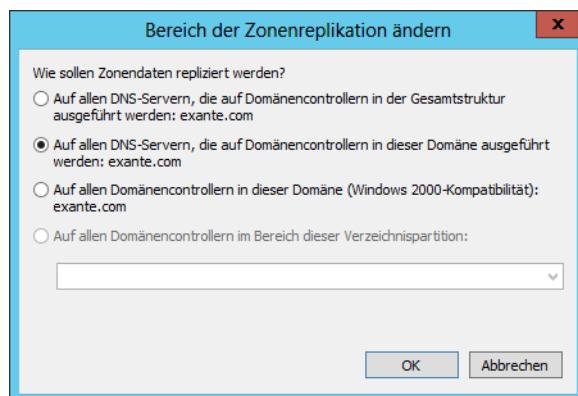


Abbildung 4.26 Das Dialogfeld *Bereich der Zonenreplikation ändern*

Stammhinweise konfigurieren

Jeder DNS-Server muss in der Lage sein, den Stammnamenserver zu kontaktieren, um die Namensauflösung einzuleiten. Die meisten Serverimplementierungen, einschließlich Microsoft DNS-Server, sind mit den Namen und Adressen von mehreren Stammnamenservern vorkonfiguriert. Dies sind die sogenannten *Stammhinweise*.

Die Namen der 13 Stammnamenserver befinden sich in einer Domäne namens *root-servers.net* und sind mit den Buchstaben des Alphabets benannt. Die Server stehen auf der ganzen Welt verteilt in verschiedenen Subnetzen, um Fehlertoleranz zu gewährleisten.

Um die Stammhinweise auf einem Windows Server 2012-DNS-Server zu modifizieren, klicken Sie mit der rechten Maustaste auf den Serverknoten, öffnen das Eigenschaftenblatt und gehen auf die Registerkarte *Stammhinweise*, die Abbildung 4.27 zeigt. Hier können Sie Stammhinweise in der Liste hinzufügen, bearbeiten oder entfernen.

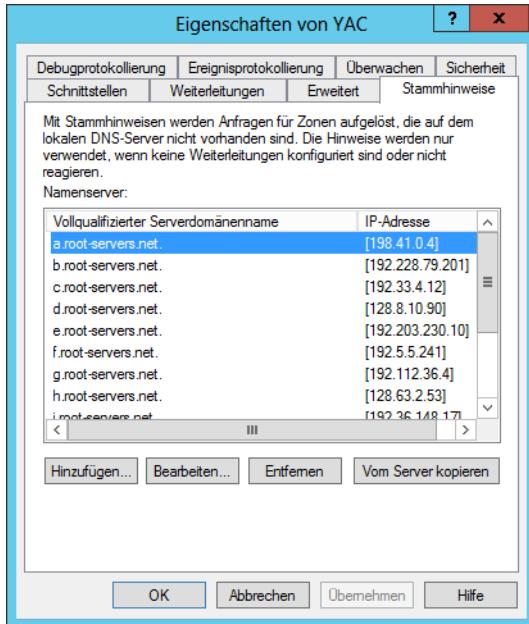


Abbildung 4.27 Die Registerkarte *Stammhinweise* auf dem Eigenschaftenblatt eines DNS-Servers

Lernzielzusammenfassung

- DHCP ist ein Dienst, der automatisch die IP-Adresse und andere TCP/IP-Einstellungen auf Netzwerkcomputern konfiguriert. Dabei weist er Adressen aus einem Pool (einem sogenannten Bereich) zu und gibt sie wieder frei, wenn sie nicht mehr verwendet werden.
- Heutige TCP/IP-Netzwerke verwenden DNS-Server, um Hostnamen in IP-Adressen umzuwandeln. Diese Umwandlung wird als *Namensauflösung* bezeichnet.
- DNS besteht aus drei Elementen: DNS-Namespace, Namenserver und Resolver
- Der hierarchische Aufbau des DNS-Namespace soll es jedem DNS-Server im Internet ermöglichen, die autorisierende Quelle für jeden Domänenamen mit möglichst wenigen Anfragen zu lokalisieren.
- Bei einer rekursiven Abfrage übernimmt der DNS-Server, der die Namensauflösungsanforderung empfängt, die volle Verantwortung für die Namensauflösung. In einer iterativen Abfrage antwortet der Server, der die Namensauflösungsanforderung empfängt, sofort mit den besten Informationen, die er zu diesem Zeitpunkt besitzt.
- Für die Internet-Namensauflösung muss der DNS-Server lediglich die Fähigkeit besitzen, eingehende Anfragen von Resolvern zu verarbeiten und seine eigenen Anfragen an andere DNS-Server im Internet zu senden

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welcher der folgenden Typen von Ressourceneinträgen enthält die Informationen, die ein DNS-Server benötigt, um Reverse-Lookups von Namen durchzuführen?
 - A. A
 - B. CNAME
 - C. SOA
 - D. PTR
2. Welche der folgenden Adressen ist der korrekte FQDN für einen Ressourceneintrag in einer Reverse-Lookupzone, wenn die IP-Adresse des Computers 10.75.143.88 lautet?
 - A. 88.143.75.10.in-addr.arpa
 - B. 10.75.143.88.in-addr.arpa
 - C. in-addr.arpa.88.143.75.10
 - D. arpa.in-addr.10.75.143.88
3. Welche der folgenden Komponenten gehört nicht zu den Elementen des DNS?
 - A. Resolver
 - B. Relay-Agenten
 - C. Namenserver
 - D. Namespace
4. In welcher der folgenden DNS-Transaktionen generiert das Abfragesystem eine rekursive Abfrage?
 - A. Ein DNS-Client sendet den Servernamen www.adatum.com von einer URL zu seinem designierten DNS-Server zur Auflösung.
 - B. Der DNS-Server eines Clients sendet eine Anforderung zu einem Stammdomänen-server, um den autorisierenden Server für die Toplevel-Domäne *com* zu suchen.
 - C. Der DNS-Server eines Clients sendet eine Anforderung zum Server der Toplevel-Domäne *com*, um den autorisierenden Server für die Domäne *adatum.com* zu suchen.
 - D. Der DNS-Server eines Clients sendet eine Anforderung an den Server der Domäne *adatum.com*, um die IP-Adresse zu suchen, die mit dem Servernamen *www* verknüpft ist.

5. Welche der folgenden Benutzeroberflächen enthält die Steuerelemente, mit denen sich die Zwischenspeicherung von DNS-Namen modifizieren lässt?
 - A. Die Registerkarte *Weiterleitungen* auf dem Eigenschaftenblatt eines Servers.
 - B. Die Registerkarte *Autoritätsursprung (SOA)* auf dem Eigenschaftenblatt einer Zone.
 - C. Die Registerkarte *Stammhinweise* auf dem Eigenschaftenblatt eines Servers.
 - D. Der Assistent zum Erstellen neuer Zonen.



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Alice ist Unternehmensadministrator für die Firma Wingtip Toys, die kürzlich ihre Kundendienstabteilung mit 100 Arbeitsstationen erweitert hat. Alle Arbeitsstationen im Firmennetzwerk sind so konfiguriert, dass sie einen Server im Umkreisnetzwerk als ihren primären DNS-Server und einen Server im Netzwerk ihres ISPs als sekundären Server verwenden.

Im Ergebnis der Erweiterung hat sich die Internet-Performance spürbar verschlechtert und eine Netzwerkmonitor-Ablaufverfolgung zeigt einen auffallend starken DNS-Datenverkehr auf der Verbindung zwischen dem Umkreisnetzwerk und dem ISP-Netzwerk an.

Beantworten Sie für dieses Szenario die folgende Frage:

Wie kann Alice den Umfang des DNS-Datenverkehrs über die Internet-Verbindung verringern? (Geben Sie zwei Möglichkeiten an.)

Antworten

Dieser Abschnitt enthält die Lösungen für die Gedankenspiele und Antworten auf die Fragen der Lernzielkontrollen in diesem Kapitel.

Lernziel 4.1: Kontrolle

1. **Richtige Antwort: B**
 - A. **Falsch:** Das Einrichten von Subnetzen ist eine Technik, um ein Netzwerk verwaltungsmäßig zu gliedern; sie überträgt keinen IPv6-Verkehr über ein IPv4-Netzwerk.
 - B. **Richtig:** Tunneling ist eine Methode, um IPv6-Verkehr in IPv4-Datagrammen zu kapseln.
 - C. **Falsch:** Das Einrichten von Supernetzen ist eine Methode, um zusammenhängende Subnetze zu einer Einheit zusammenzufassen.
 - D. **Falsch:** Zusammenziehen ist eine Methode, um IPv6-Adressen zu kürzen.

2. Richtige Antwort: C

- A. **Falsch:** Verbindungslokale Unicast-Adressen werden von IPv6-Systemen selbst zugewiesen. Demzufolge sind sie APIPA-Adressen in IPv4 äquivalent.
- B. **Falsch:** Eine globale Unicast-Adresse ist einer registrierten IPv4-Adresse äquivalent, die weltweit routungsfähig und im Internet eindeutig ist.
- C. **Richtig:** Eindeutige lokale Unicast-Adressen sind das IPv6-Äquivalent der privaten Netzwerkadressen 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16 in IPv4.
- D. **Falsch:** Die Funktion einer Anycast-Adresse ist es, die Router in einem gegebenen Adressbereich zu identifizieren und Verkehr an den nächsten Router zu senden.

3. Richtige Antwort: A

- A. **Richtig:** Teredo ist ein Mechanismus, der Geräten hinter Nicht-IPv6-NAT-Routern ermöglicht, als Tunnelendpunkte zu fungieren.
- B. **Falsch:** 6to4 bindet die IPv4-Verbindungen eines Netzwerks in die IPv6-Infrastruktur ein. Dazu wird eine Methode definiert, um IPv4-Adressen im IPv6-Format auszudrücken und IPv6-Verkehr in IPv4-Paketen zu kapseln.
- C. **Falsch:** ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) ist ein automatisches Tunneling-Protokoll, das eine IPv6-Verbindung mithilfe eines IPv4-Netzwerks emuliert und von Betriebssystemen auf Windows-Arbeitsstationen verwendet wird.
- D. **Falsch:** APIPA ist ein Verfahren, das IPv4-Adressen automatisch selbst zuweist. Es hat nichts zu tun mit Tunneling.

4. Richtige Antwort: A

- A. **Richtig:** Damit eine Adresse vom Internet aus sichtbar ist, muss sie bei der IANA registriert sein.
- B. **Falsch:** Die binäre Schreibweise von Adressen dient lediglich dazu, die Host- und Netzwerkkennungen leichter identifizieren zu können.
- C. **Falsch:** Alle Adressklassen können im Internet sichtbar oder unsichtbar sein.
- D. **Falsch:** Adressen in Subnetzen können im Internet sichtbar oder unsichtbar sein.

5. Richtige Antwort: C

- A. **Falsch:** Die Maske 255.224.0.0 entspricht der Binärdarstellung 11111111.11100000.00000000.00000000 und enthält nur 11 Bits für die Netzwerkkennung.
- B. **Falsch:** Die Maske 255.240.0.0 entspricht der Binärdarstellung 11111111.11110000.00000000.00000000 und enthält nur 12 Bits für die Netzwerkkennung.

- C. **Richtig:** Die Maske 255.255.224.0 entspricht der Binärdarstellung 11111111.11111111.11100000.00000000 und enthält 19 Bits für die Netzwerkkennung.
- D. **Falsch:** Die Maske 255.255.240.0 entspricht der Binärdarstellung 11111111.11111111.11110000.00000000 und enthält 20 Bits für die Netzwerkkennung.
- E. **Falsch:** Die Maske 255.255.255.240 entspricht der Binärdarstellung 11111111.11111111.11111111.11110000 und enthält 28 Bits für die Netzwerkkennung.

Lernziel 4.1: Gedankenspiel

Arthur kann die ihm zugeteilte Adresse in einem Subnetz einsetzen, indem er drei Hostbits verwendet, die acht Subnetze bis zu jeweils 16 Hosts erlauben. Die Subnetzmaske der Computer lautet dann 255.255.255.240 und es sind folgende IP-Adressbereiche möglich:

192.16.8.1 - 192.16.8.14
192.16.8.17 - 192.16.8.30
192.16.8.33 - 192.16.8.46
192.16.8.49 - 192.16.8.62
192.16.8.65 - 192.16.8.78
192.16.8.81 - 192.16.8.94
192.16.8.97 - 192.16.8.110
192.16.8.113 - 192.16.8.126
192.16.8.129 - 192.16.8.142
192.16.8.145 - 192.16.8.158
192.16.8.161 - 192.16.8.174
192.16.8.177 - 192.16.8.190
192.16.8.193 - 192.16.8.206
192.16.8.209 - 192.16.8.222
192.16.8.225 - 192.16.8.238
192.16.8.241 - 192.16.8.254

Lernziel 4.2: Kontrolle

1. **Richtige Antwort:** D
 - A. **Falsch:** Eine Weiterleitung ist ein DNS-Server, der rekursive Anfragen von anderen Servern entgegennimmt.
 - B. **Falsch:** Ein Resolver ist eine DNS-Clientkomponente.
 - C. **Falsch:** Ein Bereich besteht aus mehreren IP-Adressen, die von einem entsprechend konfigurierten DHCP-Server zugewiesen werden können.
 - D. **Richtig:** Ein Relay-Agent ist ein Softwaremodul, das DHCP-Broadcast-Meldungen empfängt und sie an einen DHCP-Server in einem anderen Subnetz weiterleitet.

2. Richtige Antwort: D

- A. **Falsch:** Die DHCP-Adresszuweisung beginnt, wenn der DHCP-Client DHCPDISCOVER-Meldungen generiert und sie als Broadcasts im lokalen Netzwerk sendet.
- B. **Falsch:** Der Client beendet schließlich das Senden von Broadcast-Meldungen und signalisiert mit einer DHCPREQUEST-Meldung, dass er eine der ihm angebotenen Adressen akzeptiert.
- C. **Falsch:** Wenn der Server, der die akzeptierte IP-Adresse angeboten hat, die DHCPREQUEST-Meldung empfängt, sendet er dem Client eine DHCPACK-Meldung und bestätigt damit den Abschluss des Vorgangs.
- D. **Richtig:** Der DHCPINFORM-Meldungstyp wird bei einer IP-Adresszuweisung nicht verwendet.

3. Richtige Antwort: C

- A. **Falsch:** Eine dynamische Zuweisung liegt vor, wenn der DHCP-Server eine IP-Adresse an einen Clientcomputer aus einem Bereich für eine festgelegte Zeitdauer zuweist.
- B. **Falsch:** Eine automatische Zuweisung liegt vor, wenn der DHCP-Server eine IP-Adresse an einen Clientcomputer aus einem Bereich dauerhaft zuweist.
- C. **Richtig:** Manuelle Zuweisung liegt vor, wenn der DHCP-Server eine bestimmte IP-Adresse an einen bestimmten Computer im Netzwerk dauerhaft zuweist. Im DHCP-Server von Windows Server 2012 werden manuell zugewiesene Adressen als Reservierungen bezeichnet.
- D. **Falsch:** Hybrid ist ein DHCP-Infrastrukturtyp und nicht ein Adresszuweisungstyp.

4. Richtige Antworten: B, D

- A. **Falsch:** Windows 8 kann nicht als LAN-Router und demzufolge nicht als DHCP-Relay-Agent fungieren.
- B. **Richtig:** In den meisten IP-Routern sind Funktionen für einen DHCP-Relay-Agenten integriert. Sind die Router, die Ihre Subnetze miteinander verbinden, so ausgestattet, können Sie sie als Relay-Agenten nutzen und brauchen keinen DHCP-Server in jedem Subnetz.
- C. **Falsch:** Switches sind Geräte der Datenverbindungsschicht und dafür vorgesehen, mit Geräten im selben Subnetz zu kommunizieren. Ein DHCP-Relay-Agent muss auf zwei Subnetze zugreifen können.
- D. **Richtig:** Sind Ihre Router nicht in der Lage, als DHCP-Relay-Agenten zu arbeiten, können Sie auf die Relay-Agent-Funktionen zurückgreifen, die in Windows-Serverbetriebssystemen integriert sind. In Windows Server 2012 ist die DHCP-Relay-Agent-Funktionalität in der Remotezugriffsrolle untergebracht.

5. Richtige Antwort: D

- A. **Falsch:** In den meisten Fällen verwenden alle Computer in einem Netzwerk denselben DNS-Server, sodass es komfortabler ist, seine Adresse nur einmal über eine Serveroption und nicht als Bereichsoption in jedem Bereich bereitzustellen.
- B. **Falsch:** Die Subnetzmaske ist in jede Adresslease automatisch eingeschlossen und muss demzufolge weder als Bereichs- noch als Serveroption bereitgestellt werden.
- C. **Falsch:** Die Leasedauer-Option wird automatisch in jede Adresslease eingeschlossen und muss demzufolge weder als Bereichs- noch als Serveroption bereitgestellt werden.
- D. **Richtig:** Das Standardgateway muss ein Router im selben Subnetz sein wie die IP-Adressen, die der DHCP zuweist. Demzufolge ist die Gatewayadresse für jeden Bereich unterschiedlich und muss als Bereichsoption bereitgestellt werden.

Lernziel 4.2: Gedankenspiel

Ralph kann die Dauer der IP-Addressleases in seinen Bereichen verringern, sodass aufgegebene Adressen den Clients schneller zur Verfügung stehen.

Lernziel 4.3: Kontrolle

1. Richtige Antwort: D

- A. **Falsch:** Ein Ressourceneintrag enthält Informationen für Forward- und nicht für Reverse-Lookups von Namen.
- B. **Falsch:** CNAME-Ressourceneinträge enthalten Alias-Informationen für A-Einträge. Für Reverse-Lookups von Namen werden sie nicht verwendet.
- C. **Falsch:** SOA-Einträge legen fest, dass ein Server für eine Zone autorisierend ist. Für Reverse-Lookups von Namen werden sie nicht verwendet.
- D. **Richtig:** PTR-Einträge enthalten die erforderlichen Informationen für den Server, damit er Reverse-Lookups von Namen durchführen kann.

2. Richtige Antwort: A

- A. **Richtig:** Um die IP-Adresse 10.75.143.88 in einen Namen aufzulösen, sucht ein DNS-Server eine Domäne *143.75.10.in-addr:arpa* in der üblichen Weise und liest den Inhalt eines Ressourceneintrags namens 88 in dieser Domäne.
- B. **Falsch:** Die unwichtigsten Bits in der IP-Adresse (d.h. 88) sollten im FQDN zuerst erscheinen.
- C. **Falsch:** Die für Reverse-Lookups verwendete Domäne der obersten Ebene ist *arpa*. Demzufolge muss *arpa* der letzte und wichtigste Name in einem FQDN für Reverse-Lookups sein.
- D. **Falsch:** Die für Reverse-Lookups verwendete Domäne der obersten Ebene ist *arpa*. Demzufolge muss *arpa* der letzte und wichtigste Name in einem FQDN für Reverse-Lookups sein.

3. Richtige Antwort: B

- A. **Falsch:** Resolver sind Clientprogramme, die DNS-Anfragen generieren und sie an einen DNS-Server zur Ausführung senden.
- B. **Richtig:** Relay-Agenten sind Router, die es DHCP-Clients ermöglichen, mit Servern in anderen Netzwerken zu kommunizieren.
- C. **Falsch:** Namenserver sind Anwendungen, die auf Servercomputern laufen und Informationen über die Domänenstruktur verwalten.
- D. **Falsch:** DNS besteht aus einem baumartig strukturierten Namespace, in dem jeder Zweig des Baums eine Domäne identifiziert.

4. Richtige Antwort: A

- A. **Richtig:** Wenn ein Client eine Anfrage zur Namensauflösung an seinen DNS-Server sendet, verwendet er eine rekursive Abfrage, sodass der Server die Verantwortung dafür übernimmt, den Namen aufzulösen.
- B. **Falsch:** Ein DNS-Server, der nach dem Server für eine Domäne der obersten Ebene sucht, verwendet iterative Anfragen und keine rekursiven.
- C. **Falsch:** Ein DNS-Server, der nach dem Server für eine Domäne der zweiten Ebene sucht, verwendet iterative Anfragen und keine rekursiven.
- D. **Falsch:** Ein DNS-Server, der eine Servernamensauflösung von einem autorisierenden Server anfordert, verwendet iterative und keine rekursiven Anfragen.

5. Richtige Antwort: B

- A. **Falsch:** Die Adressen von Servern mit den rekursiven Anfragen Ihres Servers legen Sie auf der Registerkarte *Weiterleitungen* fest.
- B. **Richtig:** Die Registerkarte *Autoritätsursprung (SOA)* auf dem Eigenschaftenblatt einer Zone enthält die Einstellung *Minimale Gültigkeitsdauer (Standard)*, die das Zwischenspeichern der DNS-Namen für die Zone steuert.
- C. **Falsch:** Die Adressen der Stammnamenserver im Internet legen Sie auf der Registerkarte *Stammhinweise* fest.
- D. **Falsch:** Der Assistent zum Erstellen neuer Zonen ermöglicht es Ihnen nicht, Einstellungen für das Zwischenspeichern von Namen zu ändern.

Lernziel 4.3: Gedankenspiel

1. Alice kann den DNS-Server im Umkreisnetzwerk so konfigurieren, dass er den DNS-Server des ISPs als Weiterleitung verwendet.
2. Alice kann die Arbeitsstationen so konfigurieren, dass sie den DNS-Server des ISPs als ihren primären DNS-Server verwenden.

K A P I T E L 5

Active Directory installieren und verwalten

Ein Verzeichnisdienst ist ein Repository mit Informationen über die Ressourcen – Hardware, Software und Mitarbeiter –, die mit einem Netzwerk verbunden sind. Benutzer, Computer und Anwendungen können von allen Punkten des Netzwerks aus unterschiedlichsten Beweggründen auf das Repository zugreifen. Dazu gehören Authentifizierung, Konfiguration des Datenspeichers und selbst eine simple Suche nach Informationen. Active Directory-Domäendienste (Active Directory Domain Services, AD DS) ist der Verzeichnisdienst, den Microsoft mit Windows Server 2000 eingeführt und in jeder Nachfolgeversion des Serverbetriebssystems bis einschließlich Windows Server 2012 aktualisiert hat.

Dieses Kapitel beschreibt einige der grundlegenden Aufgaben von Administratoren, um die AD DS zu installieren und zu verwalten.

Prüfungsziele in diesem Kapitel:

- Prüfungsziel 5.1: Domänencontroller installieren 280
- Prüfungsziel 5.2: Active Directory-Benutzer und -Computer erstellen und verwalten 299
- Prüfungsziel 5.3: Active Directory-Gruppen und Organisationseinheiten erstellen und verwalten. 321

Prüfungsziel 5.1: Domänencontroller installieren

Die AD DS verkörpern einen Verzeichnisdienst, mit dem Administratoren organisatorische Gliederungen – sogenannte Domänen – einrichten können. Eine Domäne ist ein logischer Container von Netzwerkkomponenten, die von mindestens einem als Domänencontroller designierten Server gehostet werden. Die Domänencontroller für jede Domäne replizieren ihre Daten untereinander, um Fehlertoleranz und Lastenausgleich zu realisieren.

Dieses Prüfungsziel zeigt, wie Sie

- einen Domänencontroller in eine Domäne hinzufügen und daraus entfernen
 - einen Domänencontroller aktualisieren
 - Active Directory-Domänendienste (AD DS) auf einer Server Core-Installation installieren
 - einen Domänencontroller per »Installieren von Medium« installieren
 - Probleme bei DNS-SRV-Einträgen lösen
 - einen globalen Katalogserver konfigurieren
-

Active Directory-Domänendienste bereitstellen

Nachdem Sie ein Active Directory-Konzept erstellt haben, ist es an der Zeit, über den eigentlichen Bereitstellungsvorgang nachzudenken. Wie bei den meisten großen Netzwerktechnologien empfiehlt es sich, die AD DS auf einem Testnetzwerk zu installieren, bevor Sie es in die Produktion überführen.

Es gibt viele Variablen, die die Leistung einer Active Directory-Installation beeinflussen können, einschließlich der Hardware, die Sie für Ihre Domänencontroller auswählen, der Fähigkeiten Ihres Netzwerks und der Art der WAN (Wide Area Network)-Verbindungen zu Ihren Remotestandorten. In vielen Fällen sieht ein Active Directory-Konzept zwar auf dem Papier gut aus, funktioniert aber in der konkreten Umgebung nicht wie vorgesehen, und Sie werden den Entwurf modifizieren müssen, bevor Sie zur eigentlichen Bereitstellung übergehen.

Active Directory gehört zu den am schwersten zu testenden Technologien, da es eine isolierte Laborumgebung nicht erlaubt, die vielen Faktoren zu emulieren, die auf die Leistung eines Verzeichnisdiensts einwirken. Die meisten Testumgebungen können das Muster des Netzwerkverkehrs einer Produktionsumgebung nicht duplizieren und nur wenige verfügen über die notwendigen WAN-Verbindungen, um ein reales Netzwerk mit mehreren Standorten zu simulieren. Wo es möglich ist, sollten Sie Ihren Entwurf unter realen Bedingungen testen und dabei Ihre vorhandenen LAN (Local Area Network)- und WAN-Technologien einsetzen, dabei jedoch für die Domänencontroller und die AD DS-Clients nur auf Laborcomputer zurückgreifen.

Um eine neue Gesamtstruktur einer neuen Domäne zu erstellen oder einen Domänencontroller in eine vorhandene Domäne einzufügen, müssen Sie die Rolle *Active Directory-Domänen-*

dienste auf einem Windows Server 2012-Computer installieren und dann den Konfigurationsassistenten für die Active Directory-Domänendienste ausführen.

Wenn Sie einen Windows Server 2012-Computer als Domänencontroller einsetzen möchten, müssen Sie ihn mit statischen IP-Adressen konfigurieren und nicht mit Adressen, die ein DHCP-Server bereitstellt. Und wenn Sie eine Domäne in einer vorhandenen Gesamtstruktur erstellen oder einen Domänencontroller in eine vorhandene Domäne einbinden, müssen Sie den Computer so konfigurieren, dass er den DNS-Server verwendet, der die vorhandene Gesamtstruktur oder Domäne hostet. Das gilt zumindest für die Phase der Active Directory-Installation.

Die Rolle Active Directory-Domänendienste installieren

Das Installieren der Rolle *Active Directory-Domänendienste* wandelt den Computer zwar noch nicht in einen Domänencontroller um, doch es bereitet ihn darauf vor.

Führen Sie die folgenden Schritte aus, um die Rolle *Active Directory-Domänendienste* zu installieren:

1. Melden Sie sich am Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Verwalten* wählen Sie *Rollen und Features hinzufügen*. Daraufhin startet der Assistent zum Hinzufügen von Rollen und Features und zeigt die Seite *Vorbemerkungen* an.
3. Klicken Sie auf *Weiter*. Die Seite *Installationstyp auswählen* erscheint.
4. Lassen Sie die Option *Rollenbasierte oder featurebasierte Installation* ausgewählt und klicken Sie auf *Weiter*, um die Seite *Zielserver auswählen* zu öffnen.
5. Wählen Sie den Server aus, den Sie zu einem Domänencontroller heraufstufen möchten, und klicken Sie auf *Weiter*. Damit gelangen Sie zur Seite *Serverrollen auswählen*.
6. Wählen Sie die Rolle *Active Directory-Domänendienste* aus. Das Dialogfeld *Sollen für Active Directory-Domänendienste erforderliche Features hinzugefügt werden?* wird geöffnet.
7. Klicken Sie auf *Features hinzufügen*, um die Abhängigkeiten zu akzeptieren, und klicken Sie dann auf *Weiter*. Es erscheint die Seite *Features auswählen*.
8. Klicken Sie auf *Weiter*. Die Seite *Active Directory-Domänendienste* erscheint und zeigt Informationen über die Rolle an.
9. Klicken Sie auf *Weiter*. Die Seite *Installationsauswahl bestätigen* wird geöffnet.
10. Wählen Sie bei Bedarf aus den folgenden Funktionen aus, die optional sind:
 - **Zielserver bei Bedarf automatisch neu starten** Bewirkt, dass der Server automatisch neu startet, wenn die Installation abgeschlossen ist, sofern es für die ausgewählten Rollen und Features erforderlich ist

- **Konfigurationseinstellungen exportieren** Erstellt ein XML-Skript, das die vom Assistenten durchgeführten Prozeduren dokumentiert. Dieses Skript können Sie mit Windows PowerShell verwenden, um die gleiche Konfiguration auf einem anderen Server zu installieren.
 - **Alternativen Quellpfad angeben** Spezifiziert den Standort einer Imagedatei mit der erforderlichen Software, um die ausgewählten Rollen und Features zu installieren
11. Klicken Sie auf *Installieren*. Daraufhin wird die Seite *Installationsstatus* angezeigt. Nachdem die Rolle installiert ist, erscheint ein Link *Server zu einem Domänencontroller heraufstufen*.
 12. Lassen Sie den Assistenten geöffnet.



Hinweis *Dcpromo.exe*

Das Programm *Dcpromo.exe* aus früheren Versionen von Windows Server wurde zugunsten der Domänencontrollerinstallation per Server-Manager verworfen, wie die folgenden Abschnitte beschreiben. Allerdings ist es immer noch möglich, AD DS-Installationen zu automatisieren, indem Sie *Dcpromo.exe* mit einer Antwortdatei ausführen.

Wenn Sie die Rolle installiert haben, können Sie den Assistenten zum Installieren von Active Directory-Domänendiensten aufrufen. Die Abläufe im Assistenten hängen von der Funktion ab, welche der neue Domänencontroller ausführen soll. Die folgenden Abschnitte beschreiben die Abläufe für die gebräuchlichsten Arten von Domänencontrollerinstallationen.

Eine neue Gesamtstruktur erstellen

Bei einer neuen AD DS-Installation ist im ersten Schritt eine neue Gesamtstruktur aufzubauen. Dazu erstellen Sie die erste Domäne in der Gesamtstruktur – die *Gesamtstruktur-Stammdomäne*.

Eine neue Gesamtstruktur erstellen Sie in den folgenden Schritten:

1. Melden Sie sich bei dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an und installieren Sie die Rolle *Active Directory-Domänendienste*, wie weiter oben beschrieben.
2. Am Ende des Installationsvorgangs für die Rolle *Active Directory-Domänendienste* klicken Sie auf der Seite *Installationsstatus* auf den Hyperlink *Server zu einem Domänencontroller heraufstufen*. Daraufhin startet der Konfigurations-Assistent für die Active Directory-Domänendienste und zeigt die Seite *Bereitstellungskonfiguration* an.
3. Wählen Sie die Option *Neue Gesamtstruktur hinzufügen* (siehe Abbildung 5.1) und geben Sie in das Textfeld *Name der Stammdomäne* den Namen der Domäne ein, die Sie erstellen möchten.

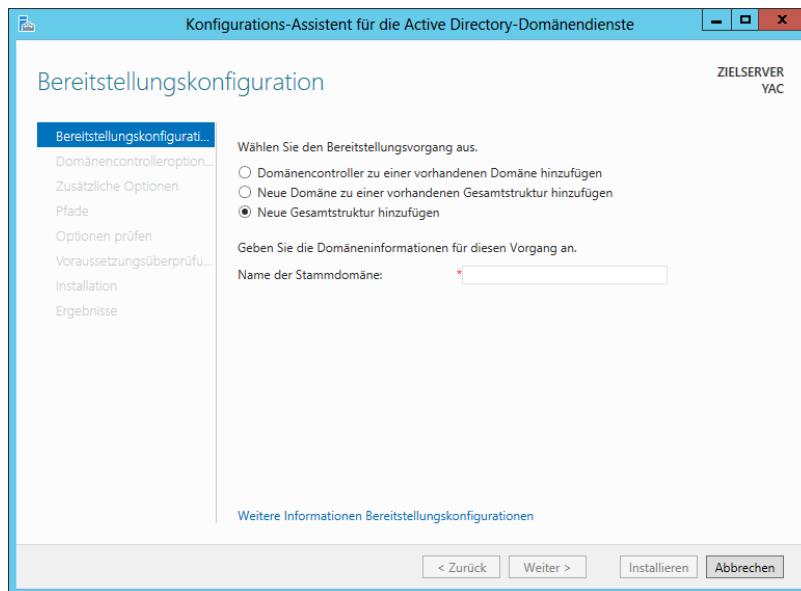


Abbildung 5.1 Die Seite *Bereitstellungskonfiguration* des Konfigurations-Assistenten für die Active Directory-Domänendienste

4. Klicken Sie auf *Weiter*. Es wird die Seite *Domänencontrolleroptionen* geöffnet, die Abbildung 5.2 zeigt.

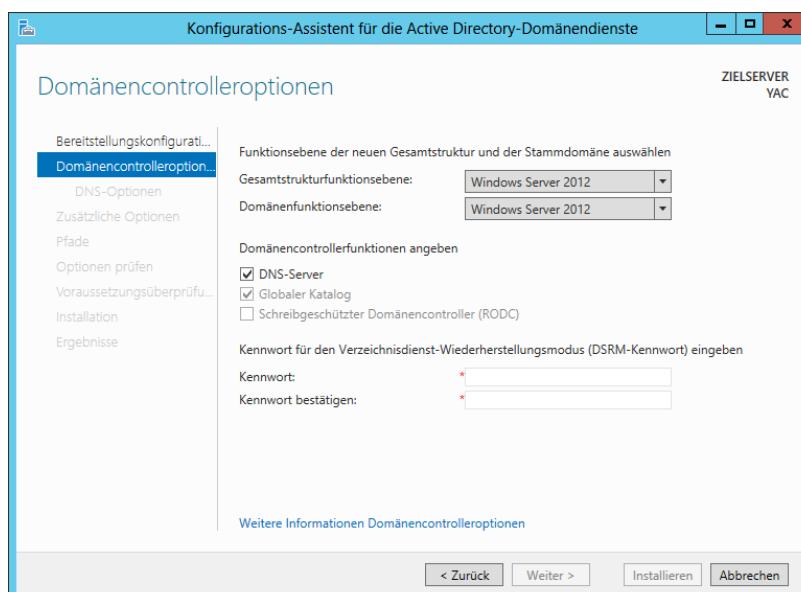


Abbildung 5.2 Die Seite *Domänencontrolleroptionen* des Konfigurations-Assistenten für die Active Directory-Domänendienste

5. Wenn Sie dieser Gesamtstruktur Domänencontroller hinzufügen möchten, die unter älteren Versionen von Windows Server laufen, wählen Sie aus der Dropdownliste *Gesamtstrukturfunktionsebene* die älteste Windows-Version aus, die Sie voraussichtlich installieren werden.
6. Möchten Sie dieser Domäne Domänencontroller hinzufügen, die unter älteren Versionen von Windows Server laufen, wählen Sie aus der Dropdownliste *Domänenfunktionsebene* die älteste Windows-Version aus, die Sie voraussichtlich installieren werden.
7. Haben Sie keinen DNS-Server in Ihrem Netzwerk installiert, lassen Sie das Kontrollkästchen *Domänennamenserver (DNS)* aktiviert. Wenn es bereits einen DNS-Server im Netzwerk gibt und der Domänencontroller so konfiguriert ist, dass er diesen Server für DNS-Dienste verwendet, deaktivieren Sie das Kontrollkästchen.



Hinweis Domänencontrolleroptionen

Die Optionen *Globaler Katalog (GC)* und *Schreibgeschützter Domänencontroller (RODC)* sind nicht verfügbar, weil der erste Domänencontroller in einer neuen Gesamtstruktur ein globaler Katalogserver sein muss und kein schreibgeschützter Domänencontroller sein darf.

8. Geben Sie in die Textfelder *Kennwort* und *Kennwort bestätigen* das Kennwort ein, das Sie für die Verzeichnisdienstwiederherstellung (Directory Services Restore Mode, DSRM) verwenden möchten. Klicken Sie auf *Weiter*, um zur Seite *DNS-Optionen* weiterzugehen. Hier erscheint eine Warnung, dass eine Delegierung für den DNS-Server nicht erstellt werden kann, da der DNS-Serverdienst noch nicht installiert ist.
9. Klicken Sie auf *Weiter*, um die Seite *Zusätzliche Optionen* zu öffnen, die die NetBIOS-Entsprechung des angegebenen Domänenamens anzeigt.
10. Ändern Sie bei Bedarf den Namen und klicken Sie auf *Weiter*, um die Seite *Pfade* zu öffnen.
11. Ändern Sie bei Bedarf die Standardspeicherorte für die AD DS-Dateien und klicken Sie auf *Weiter*. Es erscheint die Seite *Optionen prüfen*.
12. Klicken Sie auf *Weiter*, um zur Seite *Voraussetzungsüberprüfung* zu gehen, die in Abbildung 5.3 zu sehen ist.
13. Der Assistent führt eine Reihe von Umgebungstests aus, um zu ermitteln, ob das System als Domänencontroller arbeiten kann. Die Ergebnisse können als Warnungen erscheinen, die eine Fortsetzung der Prozedur ermöglichen, oder als Fehler, bei denen Sie erst bestimmte Aktionen durchführen müssen, bevor sich der Server heraufstufen lässt. Klicken Sie auf *Installieren*, wenn das System alle Voraussetzungsüberprüfungen bestanden hat. Der Assistent erstellt die neue Gesamtstruktur und konfiguriert den Server als Domänencontroller.

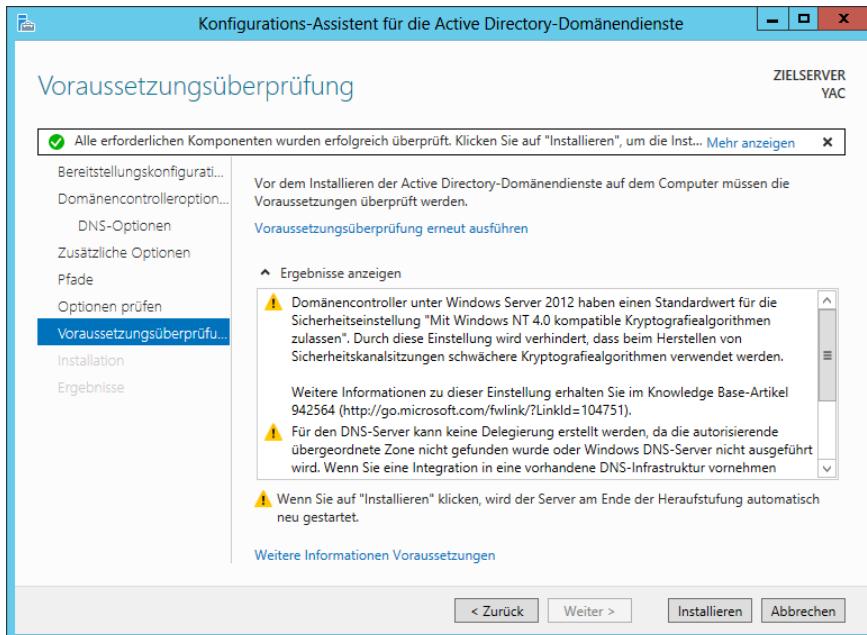


Abbildung 5.3 Die Seite *Voraussetzungsüberprüfung* des Konfigurations-Assistenten für die Active Directory-Domänendienste

14. Der Computer wird automatisch neu gestartet.

Mit der einsatzbereiten Gesamtstruktur-Stammdomäne können Sie nun zusätzliche Domänencontroller in dieser Domäne erstellen oder neue Domänen in die Gesamtstruktur einfügen.

Einen Domänencontroller in eine vorhandene Domäne hinzufügen

Jede Active Directory-Domäne sollte mindestens zwei Domänencontroller besitzen.

Um einen Domänencontroller in eine vorhandene Windows Server 2012-Domäne einzufügen, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorenrechten an und installieren Sie die Rolle *Active Directory-Domänendienste*, wie weiter oben in diesem Prüfungsziel beschrieben.
2. Am Ende des Installationsvorgangs für die Rolle *Active Directory-Domänendienste* klicken Sie auf der Seite *Installationsstatus* auf den Hyperlink *Server zu einem Domänencontroller heraufstufen*. Daraufhin startet der Konfigurations-Assistent für die Active Directory-Domänendienste und zeigt die Seite *Bereitstellungskonfiguration* an.
3. Wählen Sie die Option *Domänencontroller zu einer vorhandenen Domäne hinzufügen* und klicken Sie auf *Auswählen*.

4. Falls Sie nicht an einer vorhandenen Domäne in der Gesamtstruktur angemeldet sind, öffnet sich das Dialogfeld *Anmeldeinformationen für die Bereitstellung*, in dem Sie die Administratoranmeldeinformationen für die Domäne eingeben müssen, um fortfahren zu können. Nachdem Sie authentifiziert sind, erscheint das Dialogfeld *Domäne aus der Gesamtstruktur auswählen*.
5. Wählen Sie die Domäne aus, der Sie einen Domänencontroller hinzufügen möchten, und klicken Sie auf *OK*. Der Name der ausgewählten Domäne erscheint im Feld *Domäne*.
6. Klicken Sie auf *Weiter*. Die in Abbildung 5.4 gezeigte Seite *Domänencontrolleroptionen* wird geöffnet.

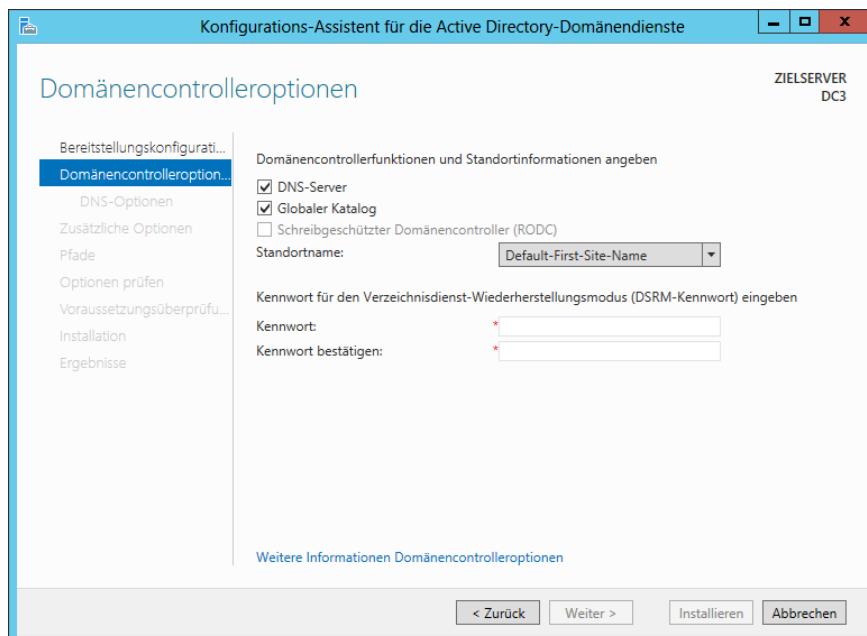


Abbildung 5.4 Die Seite *Domänencontrolleroptionen* im Konfigurations-Assistenten für die Active Directory-Domänendienste

7. Möchten Sie den DNS-Serverdienst auf dem Computer installieren, lassen Sie das Kontrollkästchen *DNS-Server* aktiviert. Andernfalls wird die Domäne auf dem DNS-Server gehostet, für den der Computer konfiguriert ist.
8. Lassen Sie das Kontrollkästchen *Globaler Katalog* (GC) aktiviert, wenn der Computer als globaler Katalogserver fungieren soll. Dies ist wichtig, wenn Sie den neuen Domänencontroller an einem Standort bereitstellen, der noch nicht über einen GC-Server verfügt.
9. Aktivieren Sie das Kontrollkästchen *Schreibgeschützter Domänencontroller (RODC)*, um einen Domänencontroller zu erstellen, den Administratoren nicht verwenden können, um AD DS-Objekte zu modifizieren.

10. Wählen Sie in der Dropdownliste *Standortname* den Standort aus, wo der Domänencontroller eingerichtet wird.
11. Geben Sie in die Textfelder *Kennwort* und *Kennwort bestätigen* das Kennwort ein, das Sie für die Verzeichnisdienstwiederherstellung (Directory Services Restore Mode, DSRM) verwenden möchten. Klicken Sie auf *Weiter*, um zu der in Abbildung 5.5 gezeigten Seite *Zusätzliche Optionen* zu gelangen.

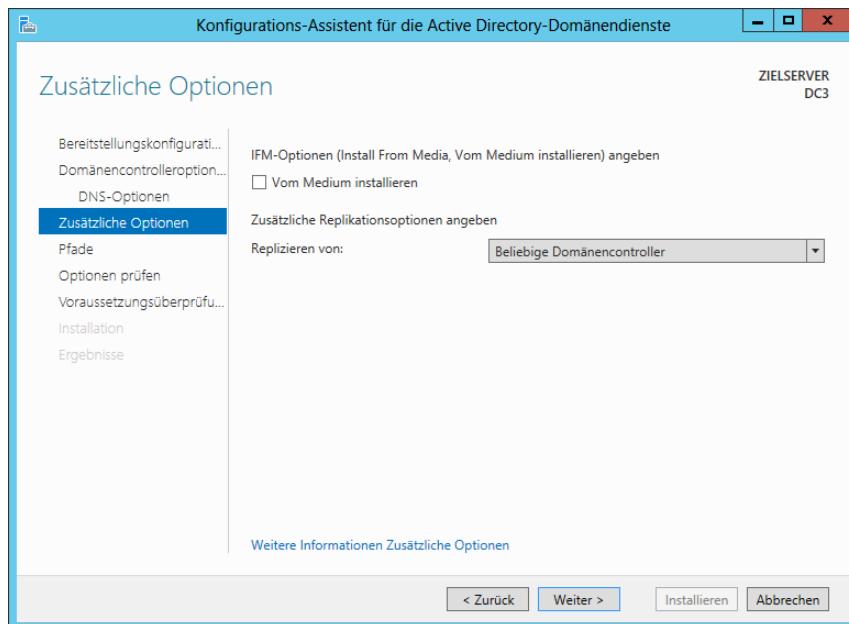


Abbildung 5.5 Die Seite *Zusätzliche Optionen* des Konfigurations-Assistenten für die Active Directory-Domänendienste

12. Um die Option *Installieren von Medium* zu verwenden, aktivieren Sie das entsprechende Kontrollkästchen.
13. Wählen Sie in der Dropdownliste *Replizieren von* den vorhandenen Domänencontroller aus, den der Server als Datenquelle verwenden soll. Klicken Sie dann auf *Weiter*, um die Seite *Pfade* zu öffnen.
14. Modifizieren Sie bei Bedarf die Standardspeicherorte für die AD DS-Dateien und klicken Sie auf *Weiter*. Es erscheint die Seite *Optionen prüfen*.
15. Klicken Sie auf *Weiter*, um zur Seite *Voraussetzungsüberprüfung* zu gehen.
16. Nachdem das System alle Voraussetzungsüberprüfungen bestanden hat, klicken Sie auf *Installieren*. Der Assistent konfiguriert die Funktion des Servers als Domänencontroller.
17. Starten Sie den Computer neu.

Der Domänencontroller ist nun dafür konfiguriert, die vorhandene Domäne zu bedienen. Befindet sich der neue Domänencontroller am selben Standort wie ein anderer Domänencontroller, beginnt die AD DS-Replikation zwischen beiden automatisch.

Eine neue untergeordnete Domäne in einer Gesamtstruktur erstellen

Wenn Sie über eine Gesamtstruktur mit mindestens einer Domäne verfügen, können Sie eine untergeordnete Domäne unterhalb jeder vorhandenen Domäne hinzufügen. Eine neue untergeordnete Domäne erstellen Sie fast in der gleichen Weise wie eine neue Gesamtstruktur, außer dass Sie auf der Seite *Bereitstellungskonfiguration* des Konfigurations-Assistenten für die Active Directory-Domänendienste die übergeordnete Domäne angeben müssen, unter der Sie eine untergeordnete Domäne erstellen wollen (siehe Abbildung 5.6).

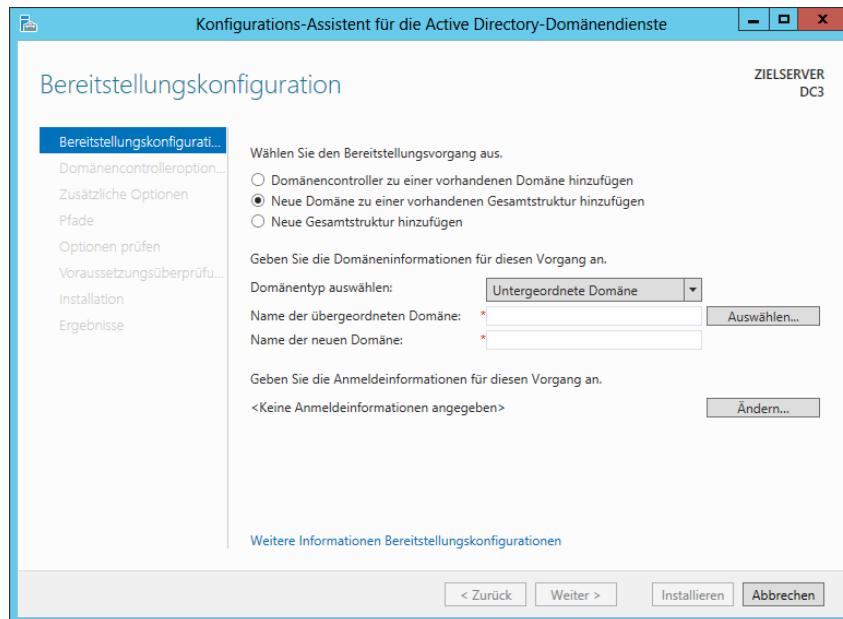


Abbildung 5.6 Die Seite *Bereitstellungskonfiguration* des Konfigurations-Assistenten für die Active Directory-Domänendienste



Hinweis Strukturdomänen

Der Assistent bietet auch die Möglichkeit, eine Strukturdomäne zu erstellen. Dabei handelt es sich um eine neue Domäne, die keiner vorhandenen Domäne in der Gesamtstruktur untergeordnet ist.

Active Directory-Domänendienste auf Server Core installieren

In Windows Server 2012 ist es jetzt möglich, Active Directory-Domänendienste auf einem Computer mit der Option *Server Core-Installation* zu installieren und das System zu einem

Domänencontroller heraufzustufen. Dies lässt sich alles per Windows PowerShell bewerkstelligen.

In Windows Server 2008 und Windows Server 2008 R2 war es üblich, die Active Directory-Domänendienste auf einem Computer mit der Option *Server Core-Installation* mithilfe einer Antwortdatei, die von der Eingabeaufforderung über das Programm *Dcpromo.exe* mit dem Parameter */unattend* geladen wurde, zu installieren.

Führt man in Windows Server 2012 das Programm *Dcpromo.exe* ohne Parameter aus, startet es nicht mehr den Konfigurations-Assistenten für die Active Directory-Domänendienste. Dennoch können Administratoren, die bereits beträchtliche Zeit in die Entwicklung von Antwortdateien für unbeaufsichtigte Installationen von Domänencontrollern gesteckt haben, diese weiterhin von der Eingabeaufforderung aus ausführen, auch wenn die Warnung erscheint: »Der unbeaufsichtigte Vorgang "dcpromo" wurde durch das Modul "ADDSDeployment" für Windows PowerShell ersetzt.«

Windows PowerShell ist für Installationen der Active Directory-Domänendienste auf Server Core nun die bevorzugte Methode. Wie bei der Assistenten-basierten Installation läuft die Windows PowerShell-Prozedur in zwei Phasen ab: Zuerst müssen Sie die Rolle Active Directory-Domänendienste installieren und anschließend den Server zu einem Domänencontroller heraufstufen.

Das Installieren der Rolle Active Directory-Domänendienste sieht mit Windows PowerShell nicht anders aus, als das Installieren jeder anderen Rolle. In einer Windows PowerShell-Sitzung mit erhöhten Rechten führen Sie den folgenden Befehl aus:

```
Install-WindowsFeature -name AD-Domain-Services  
-IncludeManagementTools
```

Wie andere Rolleninstallationen mit Windows PowerShell installiert das Cmdlet *Install-WindowsFeature* keine Verwaltungstools für die Rolle, wie zum Beispiel *Active Directory-Verwaltungscenter* und *Active Directory-Benutzer und -Computer*, sofern Sie nicht den Parameter *-IncludeManagementTools* im Befehl angeben.

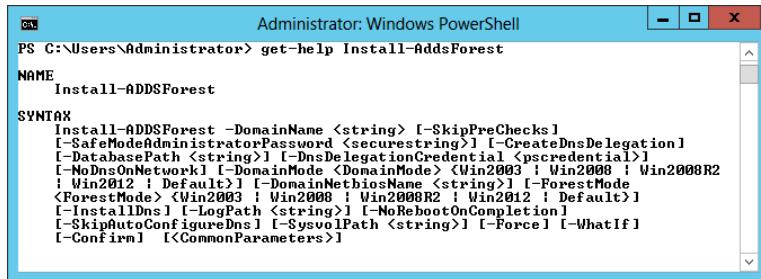
Nachdem Sie die Rolle installiert haben, ist es etwas komplizierter, den Server zu einem Domänencontroller heraufzustufen. Das Modul *ADDSDeployment* für Windows PowerShell umfasst eigene Cmdlets für die drei Bereitstellungskonfigurationen, die die vorherigen Abschnitte beschrieben haben:

- `Install-AddForest`
- `Install-AddDomainController`
- `Install-AddDomain`

Jedes dieser Cmdlets unterstützt mit vielen möglichen Parametern die zahlreichen Konfigurationsoptionen, die Sie im Konfigurations-Assistenten für die Active Directory-Domänen-dienste finden. In der einfachsten Form installiert der folgende Befehl einen Domänencontroller für eine neue Gesamtstruktur *adatum.com*:

```
Install-AddForest -DomainName "adatum.com"
```

Die Standardwerte für alle anderen Parameter des Cmdlets sind die gleichen wie im Konfigurations-Assistenten für die Active Directory-Domänendienste. Wenn Sie das Cmdlet ohne Parameter aufrufen, arbeitet es die einzelnen Optionen schrittweise nacheinander ab und fordert Sie zur Eingabe der Werte auf. Außerdem können Sie mit dem Befehl `Get-Help` grundlegende Syntaxinformationen aufrufen, wie Abbildung 5.7 zeigt.



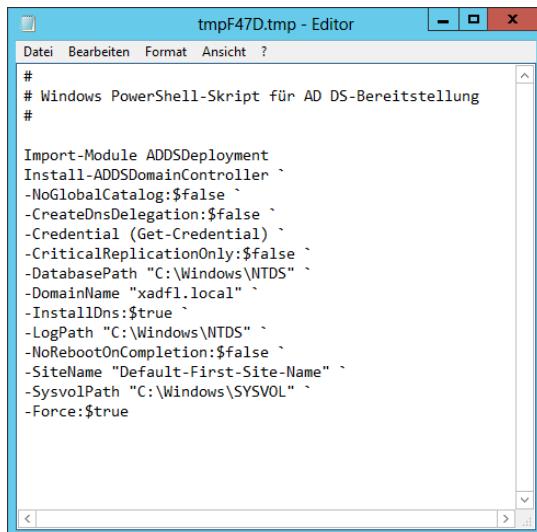
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> get-help Install-AddForest

NAME
  Install-AddForest

SYNTAX
  Install-AddForest [-DomainName <string>] [-SkipPreChecks]
  [-SafeModeAdministratorPassword <securestring>] [-CreateDnsDelegation]
  [-DatabasePath <string>] [-DnsDelegationCredential <pscredential>]
  [-NoDnsOnNetwork] [-DomainMode <Win2003 | Win2008 | Win2008R2
  | Win2012 | Default>] [-DomainNameSuffix <string>] [-ForestMode
  <ForestMode> <Win2003 | Win2008R2 | Win2012 | Default>]
  [-InstallDns] [-LogPath <string>] [-NoRebootOnCompletion]
  [-SkipDnsConfigureDns] [-SysvolPath <string>] [-Force] [-WhatIf]
  [-Confirm] [<CommonParameters>]
```

Abbildung 5.7 Syntax für das Cmdlet *Install-AddForest* in Windows PowerShell

Eine komplexe Installation ist mit Windows PowerShell auch möglich, wenn Sie auf einem Windows Server 2012-Computer mit der Option *Server mit grafischer Benutzeroberfläche* ein Skript generieren. Starten Sie zunächst den Konfigurations-Assistenten für die Active Directory-Domänendienste und konfigurieren Sie alle Optionen mit Ihren geplanten Einstellungen. Wenn Sie die Seite *Optionen prüfen* erreichen, klicken Sie auf *Skript anzeigen*, um den Windows PowerShell-Code für das passende Cmdlet anzuzeigen (siehe Abbildung 5.8).



```
tmpF47D.tmp - Editor
Datei Bearbeiten Format Ansicht ?
#
# Windows PowerShell-Skript für AD DS-Bereitstellung
#
Import-Module ADDSDeployment
Install-ADDSDomainController `
-NoGlobalCatalog:$false `
-CreateDnsDelegation:$false `
-Credential (Get-Credential) `
-CriticalReplicationOnly:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainName "xadfl.local" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SiteName "Default-First-Site-Name" `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

Abbildung 5.8 Ein Installationsskript, das der Konfigurations-Assistent für die Active Directory-Domänendienste generiert hat

Dieses Feature funktioniert, weil Server-Manager tatsächlich auf Windows PowerShell basiert. Das Skript enthält damit die Cmdlets und Parameter, die ausgeführt werden, wenn der Assistent eine Installation durchführt. Außerdem können Sie diese Skripting-Funktionen mit dem Cmdlet `Install-AddDomainController` verwenden, um mehrere Domänencontroller für dieselbe Domäne bereitzustellen.

Installieren von Medium (IFM)

Weiter vorn wurde in diesem Prüfungsziel beim Installieren eines replizierten Domänencontrollers erwähnt, dass die Seite *Zusätzliche Optionen* des Konfigurations-Assistenten für die Active Directory-Domäendienste ein Kontrollkästchen *Installieren von Medium* (Install from Media, IFM) enthält. Durch diese Option können Administratoren die Bereitstellung von replizierten Domänencontrollern auf Remotestandorten effizienter gestalten.

Normalerweise legt die Installation eines Domänencontrollers in einer vorhanden Domäne die AD DS-Datenbankstruktur an, doch stehen erst dann Daten darin, wenn der Server Replikationsdatenverkehr von den anderen Domänencontrollern empfangen kann. Sind die Domänencontroller für eine bestimmte Domäne gut vernetzt, beispielsweise durch LAN-Verbindungen, findet die Replikation praktisch sofort nach der Installation des neuen Domänencontrollers statt und geschieht vollkommen automatisch.

Wenn Sie einen Domänencontroller jedoch an einem Remotestandort installieren, läuft die Verbindung zu den anderen Domänencontrollern höchstwahrscheinlich über eine WAN-Verbindung, die in der Regel langsamer und teurer als eine LAN-Verbindung ist. In diesem Fall kann sich die anfängliche Replikation mit den anderen Domänencontrollern wesentlich problematischer gestalten. Aufgrund der geringen Geschwindigkeit der WAN-Verbindung dauert die Replikation recht lange und die Verbindung kann überflutet werden, was den normalen Datenverkehr verzögert. Befinden sich die Domänencontroller an verschiedenen AD DS-Standorten, findet eine Replikation erst statt, wenn ein Administrator die erforderlichen Standortverknüpfungen erstellt und konfiguriert.



Hinweis Replikation

Die erste Replikation, die nach der Installation eines neuen Domänencontrollers stattfindet, ist die einzige, bei der die Server eine vollständige Kopie der AD DS-Datenbanken austauschen. In darauffolgenden Replikationen tauschen die Domänencontroller nur Informationen über die Objekte und Attribute aus, die sich seit der letzten Replikation geändert haben.

Mit dem Befehlszeilentool `Ntdsutil.exe` können Administratoren diese Probleme vermeiden. Dazu erstellen sie Installationsmedien für Domänencontroller, die eine Kopie der AD DS-Datenbank beinhalten. Mit diesen Medien werden die Daten bei der Installation eines Remotedomänencontrollers zusammen mit der Datenbankstruktur installiert und es ist keine anfängliche Replikation erforderlich.

Um IFM-Medien zu erstellen, führen Sie das Programm `Ntdsutil.exe` auf einem Domänencontroller aus, auf dem die gleiche Windows-Version läuft, die Sie bereitstellen wollen. Das Programm ist interaktiv und verlangt von Ihnen die Eingabe einer Folge von Befehlen wie die folgende:

- **Ntdsutil** Startet das Programm
- **Activate instance ntds** Fokussiert das Programm auf die installierte AD DS-Instanz
- **Ifm** Schaltet das Programm in den IFM-Modus
- **Create Full|RODC <Pfadname>** Erstellt Medien entweder für einen vollständigen Lese-/Schreib-Domänencontroller oder für einen schreibgeschützten Domänencontroller und speichert sie im Ordner, der durch die Variable *Pfadname* angegeben ist



Hinweis Parameter von Ntdsutil.exe

Der Befehl `create` des Programms *Ntdsutil.exe* unterstützt auch Parameter, die den Inhalt des SYSVOL-Volumes in die AD DS-Daten einbinden. Die Windows Server 2012-Version des Programms bringt außerdem einen Parameter `nodefrag` mit, der die Defragmentierung überfährt und damit den Erstellungsvorgang der Medien beschleunigt.

Wenn Sie diese Befehle ausführen, erstellt das Programm *Ntdsutil.exe* einen Snapshot der AD DS-Datenbank, stellt ihn als Volume bereit, um ihn zu defragmentieren, und speichert ihn dann im angegebenen Ordner zusammen mit einer Kopie der Windows-Registrierung (siehe Abbildung 5.9).

```
C:\>Administrator: Eingabeaufforderung - ntdsutil
Administrator: Eingabeaufforderung - ntdsutil
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Aktive Instanz wurde auf "ntds" festgelegt.
ntdsutil: ifm
IFM: create full c:\ifm
Snapshot wird erstellt...
Der Snapshotsatz <1068caf2-7976-4ed7-ae5d-0eadbebda844> wurde erfolgreich generiert.
Der Snapshot <48d9b3a7-0cbe-4edc-8cac-37473a33a840> wird als C:\$SNAP_201303111524_VOLUMEC\$ bereitgestellt.
Snapshot <48d9b3a7-0cbe-4edc-8cac-37473a33a840> ist bereits bereitgestellt.
Defragmentierungsmodus wird initialisiert...
Quelldatenbank: C:\$SNAP_201303111524_VOLUMEC$\Windows\NTDS\ntds.dit
Zieldatenbank: c:\ifm\Active Directory\ntds.dit

Defragmentation Status <% complete>
0   10  20  30  40  50  60  70  80  90  100
-----
```

Registrierungsdateien werden kopiert...
c:\ifm\registry\SYSTEM wird kopiert
c:\ifm\registry\SECURITY wird kopiert
Die Bereitstellung des Snapshots <48d9b3a7-0cbe-4edc-8cac-37473a33a840> wurde aufgehoben.
IFM-Medien wurden erfolgreich in "c:\ifm" erstellt.
IFM:

Abbildung 5.9 Eine Befehlssequenz des Programms *Ntdsutil.exe*

Nachdem Sie die IFM-Medien erstellt haben, können Sie sie mit zweckmäßigen Mitteln zu den Servern bringen, die Sie als Domänencontroller bereitstellen möchten. Um die Medien zu verwenden, starten Sie wie gewohnt den Konfigurations-Assistenten für die Active Directory-Domäendienste, aktivieren das Kontrollkästchen *Installieren von Medien* und geben den Pfad zum Speicherort des Ordners an.

Active Directory-Domänendienste aktualisieren

Verglichen mit vorherigen Versionen des Betriebssystems ist es jetzt wesentlich einfacher, Windows Server 2012 in eine vorhandene AD DS-Installation einzubinden.

Eine AD DS-Infrastruktur lässt sich auf zwei Wegen aktualisieren: Sie können die vorhandenen Vorgängerversionen der Domänencontroller auf Windows Server 2012 aktualisieren oder einen neuen Windows Server 2012-Domänencontroller in Ihre vorhandene Installation einfügen.

Auf Windows Server 2012 gibt es mehrere Upgradepfade: Einen Windows Server 2008- oder Windows Server 2008 R2-Domänencontroller können Sie auf Windows Server 2012 aktualisieren, frühere Versionen sind jedoch nicht aktualisierbar.

Wenn Sie in der Vergangenheit einen neuen Domänencontroller in eine vorhandene AD DS-Installation basierend auf vorherigen Windows-Versionen hinzufügen wollten, mussten Sie das Programm *Adprep.exe* ausführen, um die Domänen und Gesamtstrukturen zu aktualisieren. Je nach Komplexität der Installation muss sich der Administrator bei verschiedenen Domänencontrollern mit unterschiedlichen Anmeldeinformationen anmelden, nach verschiedenen Versionen von *Adprep.exe* suchen und das Programm mehrmals mit dem Parameter */domainprep* für jede Domäne und dem Parameter */forestprep* für die Gesamtstruktur ausführen.

In Windows Server 2012 ist die Funktionalität von *Adprep.exe* vollständig in Server-Manager und im Konfigurations-Assistenten für die Active Directory-Domänendienste eingeflossen. Wenn Sie einen neuen Windows Server 2012-Domänencontroller installieren, brauchen Sie nur die entsprechenden Anmeldeinformationen bereitzustellen – der Assistent erledigt den Rest.



Hinweis Gruppenmitgliedschaft

Um den ersten Windows Server 2012-Domänencontroller auf einer AD DS-Vorgängerinstallation zu installieren, müssen Sie die Anmeldeinformationen für einen Benutzer angeben, der Mitglied der Gruppen *Organisations-Admins* und *Schema-Admins* sowie Mitglied der Gruppe *Domänen-Admins* in der Domäne ist, die den Schemamaster hostet.

Adprep.exe ist immer noch Bestandteil des Betriebssystems und unterstützt die alte Vorbereitungsmethode. Allerdings gibt es keinen triftigen Grund, diese Methode zu verwenden.

Einen Domänencontroller entfernen

Da *Dcpromo.exe* aufgegeben wurde, hat sich das Herabstufen eines Domänencontrollers geändert und ist nicht mehr auf Anhieb intuitiv.

Um einen Domänencontroller aus einer AD DS-Installation zu entfernen, müssen Sie zunächst den Assistenten zum Entfernen von Rollen und Features aufrufen, wie es der folgende Ablauf zeigt.

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorenrechten an. Die *Server-Manager*-Konsole wird geöffnet.

2. Starten Sie den Assistenten zum Entfernen von Rollen und Features und entfernen Sie die Rolle *Active Directory-Domänendienste* und ihre dazugehörigen Features. Es erscheint ein Dialogfeld *Validierungsergebnisse*, das in Abbildung 5.10 zu sehen ist.

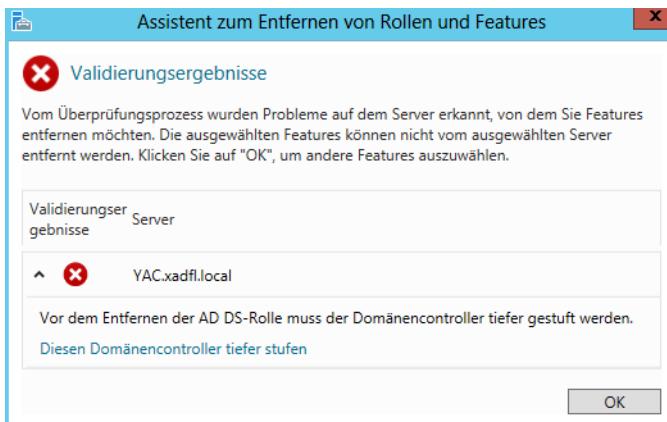


Abbildung 5.10 Das Dialogfeld *Validierungsergebnisse* des Assistenten zum Entfernen von Rollen und Features

3. Klicken Sie auf den Hyperlink *Diesen Domänencontroller tiefer stufen*. Daraufhin startet der Konfigurations-Assistent für die Active Directory-Domänendienste und zeigt die Seite *Anmeldeinformationen* an.
4. Aktivieren Sie das Kontrollkästchen *Entfernen dieses Domänencontrollers erzwingen* und klicken Sie auf *Weiter*, um die Seite *Neues Administratorkennwort* zu öffnen.
5. Geben Sie in die Textfelder *Kennwort* und *Kennwort bestätigen* das Kennwort ein, das der Server für das lokale Administratorkonto nach dem Tieferstufen verwenden soll. Klicken Sie dann auf *Weiter*. Es erscheint die Seite *Optionen prüfen*.
6. Klicken Sie auf *Tiefer stufen*. Der Assistent stuft den Domänencontroller herab und startet das System neu.
7. Melden Sie sich mit dem oben eingegebenen lokalen Administratorkennwort an.
8. Starten Sie erneut den Assistenten zum Entfernen von Rollen und Features und wiederholen Sie den Vorgang, um die Rolle *Active Directory-Domänendienste* und die dazugehörigen Features zu entfernen.
9. Schließen Sie den Assistenten und starten Sie den Server neu.



Hinweis Windows PowerShell

Einen Domänencontroller können Sie auch mit dem folgenden Windows PowerShell-Befehl tiefer stufen:

```
Uninstall-ADDSDomainController -ForceRemoval  
-LocalAdministratorPassword <password> -Force
```

Den globalen Katalog konfigurieren

Der globale Katalog ist ein Index aller AD DS-Objekte in einer Gesamtstruktur, sodass Systeme keine Suchoperationen über mehrere Domänencontroller durchführen müssen. Wie wichtig der globale Katalog tatsächlich ist, hängt von der Größe Ihres Netzwerks und dessen Standortkonfiguration ab.

Besteht zum Beispiel Ihr Netzwerk aus einer einzigen Domäne und sind die Domänencontroller alle am selben Standort untergebracht und über schnelle Verbindungen verknüpft, nützt der globale Katalog wenig, von universellen Gruppensuchen abgesehen. Wenn Sie möchten, können Sie alle Ihre Domänencontroller zu globalen Katalogservern machen. Suchoperationen erfolgen mit Lastenausgleich und der Replikationsdatenverkehr dürfte das Netzwerk kaum überlasten.

Wenn jedoch Ihr Netzwerk mehrere Domänen umfasst und die Domänencontroller an mehreren Standorten über WAN-Verbindungen verknüpft sind, ist die Konfiguration des globalen Katalogs entscheidend. Nach Möglichkeit sollten Benutzer keine AD DS-Suchen über langsame und teure WAN-Verbindungen ausführen müssen, die Domänencontroller an anderen Standorten kontaktieren. In diesem Fall empfiehlt es sich, an jedem Standort einen globalen Katalogserver vorzusehen. Die anfängliche Replikation mag zwar Unmengen von Datenverkehr erzeugen, doch auf lange Sicht sind die Einsparungen sicher erheblich.

Beim Heraufstufen eines Servers zu einem Domänencontroller haben Sie die Möglichkeit, den Domänencontroller zu einem globalen Katalogserver zu machen. Möchten Sie dies nicht, können Sie auch jeden anderen Domänencontroller zu einem globalen Katalogserver machen. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich bei dem Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Die *Server-Manager*-Konsole wird geöffnet.
2. Im Menü *Tools* wählen Sie *Active Directory-Standorte und -Dienste*. Daraufhin wird die Konsole *Active Directory-Standorte und -Dienste* geöffnet.
3. Erweitern Sie den Standort des Domänencontrollers, der als globaler Katalogserver dienen soll. Erweitern Sie dann den Ordner *Server* und wählen Sie den zu konfigurierenden Server aus.
4. Klicken Sie mit der rechten Maustaste auf den Knoten *NTDS-Einstellungen* für den Server und wählen Sie aus dem Kontextmenü *Eigenschaften*, um das Eigenschaftenblatt *NTDS-Einstellungen* zu öffnen.
5. Aktivieren Sie das Kontrollkästchen *Globaler Katalog* und klicken Sie auf *OK*.
6. Schließen Sie die Konsole *Active Directory-Standorte und -Dienste*.

Problembehebung bei DNS-SRV-Einträgen

DNS ist für den Betrieb der Active Directory-Domänen Dienste entscheidend. Um Verzeichnisdiensten wie zum Beispiel den AD DS Rechnung zu tragen, wurde ein spezieller DNS-Ressourceneintrag geschaffen, der es Clients ermöglicht, Domänencontroller und andere wichtige AD DS-Dienste zu finden.

Wenn Sie einen neuen Domänencontroller erstellen, ist die Registrierung des Servers im DNS einer der wichtigsten Bestandteile des Vorgangs. Diese automatische Registrierung ist der Grund, warum ein AD DS-Netzwerk Zugriff auf einen DNS-Server benötigt, der den Standard *Dynamische Updates* wie im RFC (Request for Comments) 2136 beschrieben unterstützt.

Scheitert der DNS-Registrierungsprozess, sind die Computer im Netzwerk nicht in der Lage, diesen Domänencontroller zu finden. Das hat gegebenenfalls schwerwiegende Konsequenzen. Computer können diesen Domänencontroller nicht verwenden, um der Domäne beizutreten, vorhandene Domänenmitglieder können sich nicht anmelden und die Replikation zwischen diesem und anderen Domänencontrollern ist nicht möglich.

In den meisten Fällen sind DNS-Probleme auf allgemeine Netzwerkfehler oder Konfigurationsfehler bei DNS-Clients zurückzuführen. Als Erstes sollten Sie deshalb versuchen, einen Ping auf den DNS-Server auszuführen, und kontrollieren, ob in der Clientkonfiguration die richtigen Adressen für die zu verwendenden DNS-Server eingetragen sind.

Um sich zu vergewissern, dass ein Domänencontroller im DNS registriert ist, öffnen Sie eine Eingabeaufforderung mit Administratorrechten und geben den folgenden Befehl ein:

```
dcdiag /test:registerindns /dnsdomain:<Domäne> /v
```

Prüfungszielzusammenfassung

- Ein Verzeichnisdienst ist ein Repository mit Informationen über die Ressourcen – Hardware, Software und Personal –, die mit einem Netzwerk verbunden sind. Active Directory ist der Verzeichnisdienst, den Microsoft mit Windows Server 2000 eingeführt und in jeder Nachfolgeversion des Serverbetriebssystems bis einschließlich Windows Server 2012 aktualisiert hat.
- Wenn Sie Ihre erste Domäne in einem Active Directory-Netzwerk einrichten, erstellen Sie praktisch den Stamm einer Domänenstruktur. Die Struktur können Sie dann mit zusätzlichen Domänen bestücken, solange sie Bestandteil desselben zusammenhängenden Namespaces sind.
- Bei einer neuen AD DS-Installation ist im ersten Schritt eine neue Gesamtstruktur aufzubauen. Dazu erstellen Sie die erste Domäne in der Gesamtstruktur – die Gesamtstruktur-Stammdomäne.
- In Windows Server 2012 ist es jetzt möglich, Active Directory-Domänenendienste auf einem Computer mit der Option Server Core-Installation zu installieren und das System zu einem Domänencontroller heraufzustufen. Dies lässt sich alles per Windows PowerShell bewerkstelligen.
- Installieren von Medium (IFM) ist ein Feature, durch das Administratoren die Bereitstellung von replizierten Domänencontrollern auf Remotestandorten rationeller gestalten können
- Eine AD DS-Infrastruktur lässt sich auf zwei Wegen aktualisieren: Sie können die vorhandenen Vorgängerversionen der Domänencontroller auf Windows Server 2012

aktualisieren oder einen neuen Windows Server 2012-Domänencontroller in Ihre vorhandene Installation einfügen

- Der globale Katalog ist ein Index aller AD DS-Objekte in einer Gesamtstruktur, sodass Systeme keine Suchoperationen über mehrere Domänencontroller durchführen müssen
- DNS ist für den Betrieb der Active Directory-Domänendienste entscheidend. Um Verzeichnisdiensten wie zum Beispiel den AD DS Rechnung zu tragen, wurde ein spezieller DNS-Ressourceneintrag geschaffen, der es Clients ermöglicht, Domänencontroller und andere wichtige AD DS-Dienste zu finden.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Elemente können nicht mehrere Active Directory-Domänen enthalten?
 - A. Organisationseinheiten
 - B. Standorte
 - C. Strukturen
 - D. Gesamtstrukturen
2. Wie lauten die beiden grundlegenden Klassen von Active Directory-Objekten?
 - A. Ressource
 - B. Endknoten
 - C. Domäne
 - D. Container
3. Welche der folgenden Aussagen trifft nicht auf die Attribute eines Objekts zu?
 - A. Administratoren müssen Informationen für bestimmte Attribute manuell bereitstellen.
 - B. Zu jedem Containerobjekt gehört ein Attribut mit einer Liste aller anderen Objekte, die es enthält.
 - C. Endknotenobjekte enthalten keine Attribute.
 - D. Active Directory erstellt den global eindeutigen Bezeichner (Globally Unique Identifier, GUID) automatisch.

4. Welche der folgenden Aussagen stellt keinen Grund dar, warum man eine Active Directory-Infrastruktur mit möglichst wenig Domänen entwerfen sollte.
 - A. Zusätzliche Domänen erhöhen den Verwaltungsaufwand der Installation.
 - B. Jede zusätzlich erstellte Domäne vergrößert die Hardwarekosten der Active Directory-Bereitstellung.
 - C. Manche Anwendungen haben eventuell Probleme damit, in einer Gesamtstruktur mit mehreren Domänen zu arbeiten
 - D. Für jede Domäne, die Sie erstellen, müssen Sie eine Lizenz von Microsoft erwerben.
5. Welche der folgenden Komponenten verwendet ein Active Directory-Client, um Objekte in einer anderen Domäne zu suchen?
 - A. DNS
 - B. Globaler Katalog
 - C. DHCP
 - D. Standortverknüpfung



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Robert konzipiert eine neue Active Directory-Domänendienste-Infrastruktur für die Firma Litware, Inc., die ihren Stammsitz in New York hat und zwei Büros in London und Tokio unterhält. Das Londoner Büro besteht nur aus Vertriebs- und Marketingmitarbeitern; eine eigene IT-Abteilung gibt es nicht. Das Büro in Tokio ist größer und beherbergt Vertreter aller Firmenabteilungen, einschließlich einer kompletten IT-Mannschaft.

Mit dem Stammsitz in Tokio kommuniziert das Büro über eine 64-KBit/s-Einwählverbindung und das Londoner Büro verfügt über eine 512-KBit/s-Frame-Relay-Verbindung. Die Firma hat den Domänennamen *litware.com* registriert und Robert hat eine Subdomäne *inside.litware.com* für Active Directory erstellt.

Entwerfen Sie anhand dieser Angaben eine möglichst wirtschaftliche Active Directory-Infrastruktur für Litware, Inc., und geben Sie an, wie viele Domänen zu erstellen sind, welche Namen sie erhalten sollen, wie viele Domänencontroller installiert werden müssen und wo ihre Installation erfolgen soll. Erläutern Sie jede Ihrer Entscheidungen.

Prüfungsziel 5.2: Active Directory-Benutzer und -Computer erstellen und verwalten

Benutzer und Computer sind die grundlegenden Endknotenobjekte, die die Zweige des AD DS-Baums besetzen. Das Erstellen und Verwalten dieser Objekte gehört für die meisten AD DS-Administratoren zum Alltagsgeschäft.

Dieses Prüfungsziel zeigt, wie Sie

- das Erstellen von Active Directory-Konten automatisieren
 - Benutzer und Computer erstellen, kopieren, konfigurieren und löschen
 - Vorlagen konfigurieren
 - Active Directory-Massenoperationen durchführen
 - Benutzerrechte konfigurieren
 - einer Domäne offline beitreten
 - inaktive und deaktivierte Konten verwalten
-

Benutzerobjekte erstellen

Das Benutzerkonto ist das Hauptinstrument, über das Personen in einem AD DS-Netzwerk auf Ressourcen zugreifen. Der Ressourcenzugriff für Einzelpersonen findet über ihre individuellen Benutzerkonten statt. Um Zugriff auf das Netzwerk zu erhalten, müssen sich angehende Netzwerkbenutzer gegenüber dem Netzwerk mit einem bestimmten Benutzerkonto authentifizieren.

Authentifizierung ist der Vorgang, bei dem die Identität eines Benutzers mithilfe eines bekannten Werts wie zum Beispiel einem Kennwort, einer Smartcard oder einem Fingerabdruck bestätigt wird. Gibt ein Benutzer einen Namen und ein Kennwort ein, validiert der Authentifizierungsprozess die Anmeldeinformationen gegenüber den Daten, die in der AD DS-Datenbank gespeichert sind. Im Unterschied zur Authentifizierung bestätigt die *Autorisierung*, dass ein authentifizierter Benutzer über die korrekten Berechtigungen verfügt, um auf eine oder mehrere Netzwerkressourcen zuzugreifen.

Systeme unter Windows Server 2012 unterschieden die beiden folgenden Arten von Benutzerkonten:

- **Lokale Benutzer** Diese Konten können nur auf Ressourcen auf dem lokalen Computer zugreifen und sind in der SAM-Datenbank (Security Account Manager, Sicherheitskontenverwaltung) auf dem Computer gespeichert, auf dem die Konten angelegt wurden. Lokale Konten werden niemals auf andere Computer repliziert und bieten keinen Domänenzugriff. Ein lokales Konto, das auf dem einen Server konfiguriert ist, kann also nicht auf Ressourcen auf einem zweiten Server zugreifen; für diesen Fall wäre ein zweites lokales Konto zu konfigurieren.

- **Domänenbenutzer** Diese Konten können auf AD DS- oder networkbasierte Ressourcen wie zum Beispiel freigegebene Ordner und Drucker zugreifen. Die Kontodaten für diese Benutzer werden in der AD DS-Datenbank gespeichert und auf alle Domänencontroller in derselben Domäne repliziert. Eine Teilmenge der Domänenbenutzerdaten wird in den globalen Katalog repliziert, der dann seinerseits auf andere globale Katalogserver in der Gesamtstruktur repliziert wird.

Auf einem Windows Server 2012-Computer werden standardmäßig zwei integrierte Benutzerkonten erstellt: *Administrator* und *Gast*. Integrierte Benutzerkonten können lokale Konten oder Domänenkonten sein, je nachdem, ob der Server als eigenständiger Server oder als Domänencontroller konfiguriert ist. Bei einem eigenständigen Server sind die integrierten Konten lokale Konten auf dem Server selbst. Auf einem Domänencontroller handelt es sich bei den integrierten Konten um Domänenkonten, die auf jeden Domänencontroller repliziert werden.

Auf einem Mitgliedsserver oder eigenständigen Server hat das integrierte lokale Administrator-Konto Vollzugriff auf alle Dateien und vollständige Verwaltungsberechtigungen für den lokalen Computer. Auf einem Domänencontroller hat das integrierte Administratorkonto, das in Active Directory erstellt wird, Vollzugriff auf die Domäne, in der es erstellt wurde. Standardmäßig gibt es nur ein integriertes Administrator-Konto pro Domäne. Weder das lokale Administratorkonto auf einem Mitgliedsserver oder einem eigenständigen Server noch ein Domänenadministratorkonto können gelöscht werden; allerdings lassen sie sich umbenennen.

Die folgende Liste fasst verschiedene Sicherheitsrichtlinien zusammen, die Sie in Bezug auf das Administratorkonto beachten sollten:

- **Das Administratorkonto umbenennen** Diese Maßnahme wehrt Angriffe ab, die sich speziell auf den Administrator-Benutzernamen auf einem Server oder einer Domäne richten. Allerdings schützt dies nur gegen recht simple Angriffe, sodass Sie sich nicht ausschließlich darauf verlassen sollten, um das Netzwerk zu schützen.
- **Ein starkes Kennwort festlegen** Achten Sie darauf, dass das Kennwort mindestens sieben Zeichen lang ist und aus einer Mischung von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen besteht
- **Die Administratorkennwörter nur wenigen Personen bekanntmachen** Wenn Administratorkennwörter nur einem engen Personenkreis bekannt sind, verringert sich die Gefahr von Sicherheitsverletzungen, die durch die Verwendung dieses Kontos entstehen
- **Das Administratorkonto nicht für tägliche Routinearbeiten ohne administrativen Bezug verwenden** Microsoft empfiehlt ein nicht-administratives Benutzerkonto für die normale Arbeit und den Befehl *Ausführen als*, wenn Verwaltungsaufgaben wahrgenommen sind

Das integrierte Gastkonto bietet Benutzern wie zum Beispiel Handelsvertretern oder vorübergehend Beschäftigten einen zeitlich begrenzten Zugriff auf das Netzwerk. Wie das Administratorkonto lässt sich auch das Gastkonto nicht löschen, kann und sollte aber umbenannt werden. Das Gastkonto ist standardmäßig deaktiviert und ihm ist kein Standardkennwort zugeordnet. In den meisten Umgebungen ist es besser, spezielle Konten für temporäre

Benutzer einzurichten, anstatt auf das Gastkonto zurückzugreifen. Somit lässt sich gewährleisten, dass das Konto auch den Firmensicherheitsrichtlinien für temporäre Benutzer entspricht. Wenn Sie jedoch das Gastkonto verwenden möchten, sollten Sie die folgenden Richtlinien beherzigen:

- **Das Gastkonto umbenennen, nachdem es aktiviert wurde** Wie beim Administratorkonto erwähnt, verweigert diese Maßnahme Eindringlingen einen Benutzernamen, der schon die Hälfte der erforderlichen Informationen offenbaren würde, um auf Ihre Domäne zugreifen zu können
- **Ein starkes Kennwort festlegen** Das Gastkonto wird standardmäßig mit einem leeren Kennwort konfiguriert. Aus Sicherheitsgründen sollten Sie niemals ein leeres Kennwort zulassen. Achten Sie darauf, dass das Kennwort mindestens sieben Zeichen lang ist und aus einer Mischung von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen besteht.

Tools zum Erstellen von Benutzern

Zu den häufigsten Aufgaben von Administratoren gehört es, Active Directory-Benutzerobjekte zu erstellen. Windows Server 2012 bringt hierfür mehrere Tools mit. Welches Tool Sie konkret einsetzen, hängt davon ab, um wie viele Objekte es sich handelt, welcher Zeitrahmen für das Erstellen dieser Gruppen zur Verfügung steht und ob besondere Umstände zu berücksichtigen sind, wie etwa das Importieren von Benutzern aus einer vorhandenen Datenbank.

Ist lediglich ein einzelner Benutzer zu erstellen, bietet sich das Active Directory-Verwaltungscenter oder die Konsole *Active Directory-Benutzer und -Computer* an. Müssen Sie jedoch mehrere Benutzer in einem engen Zeitfenster erstellen oder verfügen Sie über eine Datenbank, aus der diese Objekte zu importieren sind, brauchen Sie ein effizienteres Tool. In Windows Server 2012 können Sie aus einer Reihe von Tools auswählen, abhängig davon, welche Aufgaben zu erledigen sind. Die folgende Liste beschreibt die gebräuchlichsten Methoden, um mehrere Benutzer und Gruppen zu erstellen. Ausführlich werden diese Tools in den nächsten Abschnitten beschrieben.

- **Dsadd.exe** ist das Standardbefehlszeilentool zum Erstellen von AD DS-Endknotenobjekten. Es eignet sich in Verbindung mit Batchdateien, um AD DS-Objekte in Massen zu erstellen.
- **Windows PowerShell** ist das derzeit anerkannte Windows-Wartungstool, mit dem Sie Skripts zum Erstellen von Objekten mit nahezu unbeschränkter Komplexität schreiben können
- **CSV-Verzeichnisaustausch (CSVDE.exe)** ist ein Befehlszeilendienstprogramm, das neue AD DS-Objekte erstellen kann, indem es Informationen aus einer durch Trennzeichen getrennten (.csv) Datei importiert
- **LDAP Data Interchange Format Directory Exchange (LDIFDE.exe)** ist wie CSVDE ein Dienstprogramm, das AD DS-Informationen importieren und damit Objekte hinzufügen, löschen oder modifizieren kann. Bei Bedarf ist es zudem möglich, das Schema zu ändern.

Diese Tools haben ihren Platz in der Netzwerkverwaltung und es liegt beim Administrator, das jeweils am besten geeignete Tool entsprechend seinen Fertigkeiten und der konkreten Situation auszuwählen. Wenn zum Beispiel zwei Tools für eine Aufgabe infrage kommen, könnten Sie sich für das Tool entscheiden, mit dem Sie am meisten vertraut sind, oder für dasjenige, das die Aufgabe in weniger Zeit bewältigt.

Die folgenden Abschnitte untersuchen verschiedene Szenarios für den Einsatz dieser Tools, um Benutzerobjekte zu erstellen.

Einzelne Benutzer erstellen

Für manche Administratoren gehört es zum Tagesgeschäft, einzelne Benutzer einzurichten, und es gibt hierzu viele Möglichkeiten. In Windows Server 2012 wurde die mit Windows Server 2008 R2 eingeführte Anwendung *Active Directory-Verwaltungscenter* (ADAC) überarbeitet, um neue Features wie zum Beispiel den Active Directory-Papierkorb und abgestimmte Kennwortrichtlinien vollständig einzubinden. Mit diesem Tool können Sie auch AD DS-Benutzerkonten erstellen und verwalten.

Führen Sie die folgenden Schritte aus, um mit dem Active Directory-Verwaltungscenter einen einzelnen Benutzer zu erstellen:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorenrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Active Directory-Verwaltungscenter* aus. Die *Active Directory-Verwaltungscenter*-Konsole wird geöffnet.
3. Suchen Sie im linken Fensterbereich die Domäne, in der Sie das Benutzerobjekt erstellen möchten, und wählen Sie einen Container in dieser Domäne aus.
4. Klicken Sie im Aufgabenbereich unterhalb des Containernamens auf *Neu / Benutzer*, um das Fenster *Benutzer erstellen* zu öffnen, wie Abbildung 5.11 zeigt.
5. Geben Sie in das Feld *Vollständiger Name* den Namen des Benutzers und in das Feld *SamAccountName-Anmeldung von Benutzer* einen Kontonamen ein.
6. Geben Sie in die Felder *Kennwort* und *Kennwort bestätigen* ein Anfangskennwort für den Benutzer ein.
7. Füllen Sie bei Bedarf auch die optionalen Felder auf der Seite aus.
8. Klicken Sie auf *OK*. Das Benutzerobjekt erscheint im Container.

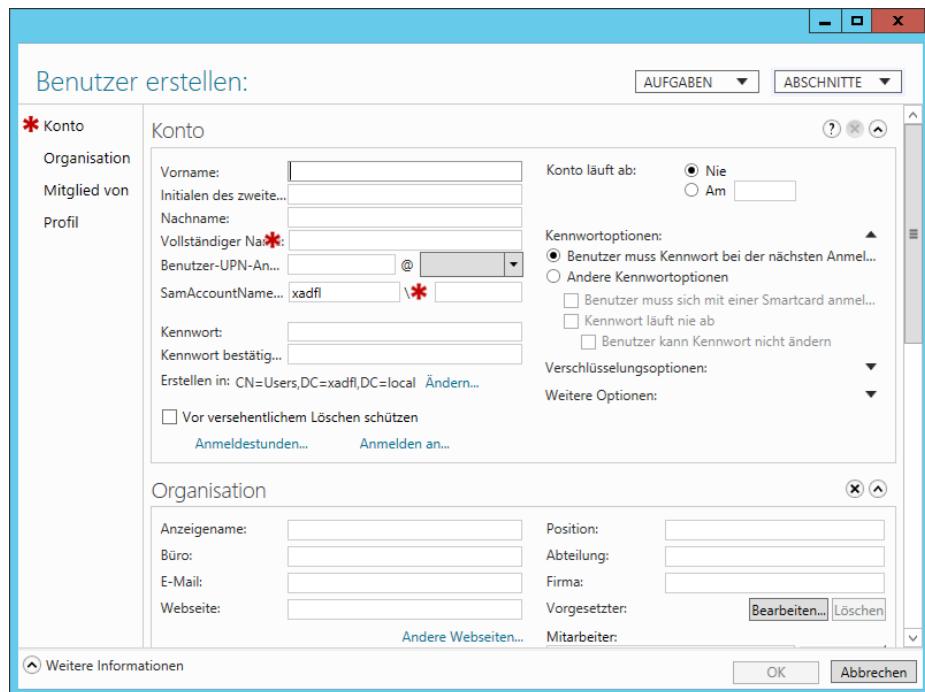


Abbildung 5.11 Das Fenster *Benutzer erstellen* in der Active Directory-Verwaltungcenter-Konsole

9. Schließen Sie die Active Directory-Verwaltungcenter-Konsole.

Administratoren, die mit der Konsole *Active Directory-Benutzer und -Computer* vertrauter sind, können diese weiterhin verwenden und Benutzer über den Assistenten *Neues Objekt – Benutzer* anlegen, wie Abbildung 5.12 zeigt.

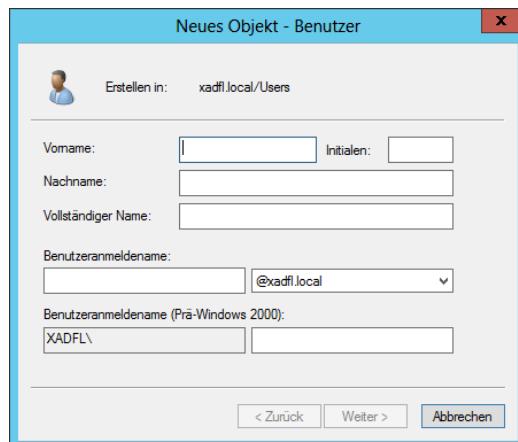
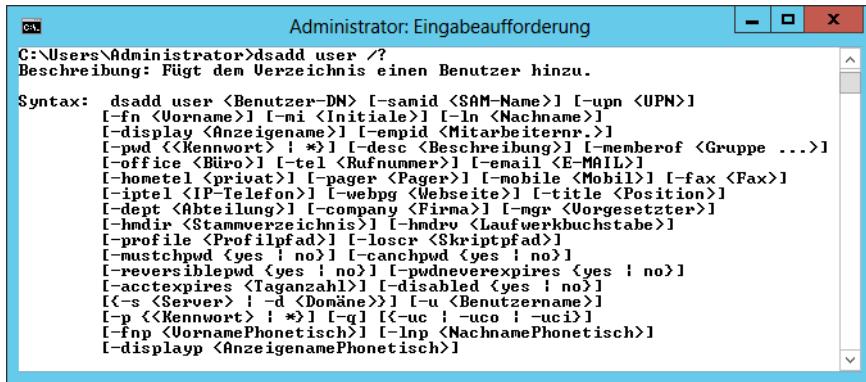


Abbildung 5.12 Der Assistent *Neues Objekt – Benutzer* in der Konsole *Active Directory-Benutzer und -Computer*

Administratoren, die auf Server Core-Installationen arbeiten oder denen die Befehlszeile lieber ist, können Benutzerobjekte auch ohne grafische Benutzeroberfläche erstellen.

Dsadd.exe

Das Programm *Dsadd.exe* eignet sich für Administratoren, die mit der herkömmlichen Eingabeaufforderung vertrauter sind. Es kann neue Benutzerobjekte erstellen, wobei die in Abbildung 5.13 gezeigte Syntax verwendet wird.



```
C:\>Administrator: Eingabeaufforderung
C:\Users\Administrator>dsadd user /?
Beschreibung: Fügt dem Verzeichnis einen Benutzer hinzu.

Syntax: dsadd user <Benutzer-DN> [-samid <SAM-Name>] [-upn <UPN>]
        [-fn <Vorname>] [-mi <Initiale>] [-ln <Nachname>]
        [-display <Anzeigename>] [-empid <Mitarbeiternr.>]
        [-pwd <>] [-desc <Beschreibung>] [-memberof <Gruppe ...>]
        [-office <Büro>] [-tel <Rufnummer>] [-email <E-MAIL>]
        [-hometel <privat>] [-pager <Pager>] [-mobile <Mobil>] [-fax <Fax>]
        [-iptel <IP-Telefon>] [-webpg <Webseite>] [-title <Position>]
        [-dept <Abteilung>] [-company <Firma>] [-mgr <Vorgesetzter>]
        [-hmdir <Stammverzeichnis>] [-hmdirv <Laufwerkbuchstabe>]
        [-profile <Profilpfad>] [-loscr <Skriptpfad>]
        [-mustchpwd <yes | no>] [-canchpwd <yes | no>]
        [-reversiblepwd <yes | no>] [-pwdneverexpires <yes | no>]
        [-acctexpires <Taganzahl>] [-disabled <yes | no>]
        [-s <Server>] [-d <Domäne>] [-u <Benutzername>]
        [-p <>] [-q1 [-u1 ; -uc1]] [-q2 [-u2 ; -uc2]]
        [-fnp <VornamePhonetisch>] [-lnp <NachnamePhonetisch>]
        [-display <AnzeigenamePhonetisch>]
```

Abbildung 5.13 Syntax des Programms *Dsadd.exe*

Um einen Benutzer mit dem Dienstprogramm *Dsadd.exe* zu erstellen, müssen Sie den definierten Namen (Distinguished Name, DN) für den Benutzer und seine Anmelde-ID kennen, was in den AD DS auch als *SAM-Kontonamenattribut* bezeichnet wird. Der definierte Name eines Objekts kennzeichnet seine Position in der Active Directory-Struktur. Im definierten Namen *cn=Elizabeth Andersen,ou=Research,dc=adatum,dc=com* bezieht sich *cn* auf den allgemeinen Namen für das Benutzerkonto von *Elizabeth Andersen*, das sich in der OU *Research* befindet, die zur Domäne *adatum.com* gehört.

Jedes Objekt besitzt einen eindeutigen DN, doch kann sich dieser DN ändern, wenn Sie das Objekt an andere Standorte innerhalb der Active Directory-Struktur verschieben. Wenn Sie zum Beispiel eine zusätzliche Ebene von OUs einführen, die Büros in verschiedenen Städten darstellen, könnte sich der oben angegebene DN in *cn=Elizabeth Andersen,ou=Research,ou=Baltimore,dc=adatum,dc=com* ändern, obwohl es sich um dasselbe Benutzerobjekt mit denselben Rechten und Berechtigungen handelt.

Der SAM-Kontoname bezieht sich auf den Anmeldenamen jedes Benutzers – den Teil links vom @ in einem Benutzerprinzipalnamen – der *eander* ist in *eander@adatum.com*. Der SAM-Kontoname muss in der gesamten Domäne eindeutig sein.

Wenn Sie über diese beiden Elemente verfügen, können Sie mit dem Dienstprogramm *Dsadd.exe* einen Benutzer gemäß der folgenden Syntax erstellen:

```
dsadd user <Benutzer-DN> -samid <SAM-Name>
```

In der einfachsten Form können Sie zum Beispiel das weiter oben erwähnte Konto für Elizabeth Andersen wie folgt erstellen:

```
dsadd user
cn="Elizabeth Andersen,ou=Research,dc=adatum,dc=com"
-samid eander
```

Mit dem Tool *Dsadd.exe* lassen sich auch Attributwerte hinzufügen. Der folgende Befehl fügt dem Benutzerobjekt einige der gebräuchlichsten Attribute hinzu:

```
Dsadd.exe User
"CN=Elizabeth Andersen,OU=Research,DC=adatum,DC=local"
-samid "eander"
-fn "Elizabeth"
-ln "Andersen"
-disabled no
-mustchpwd yes
-pwd "Pa$$w0rd"
```

Windows PowerShell

Da Microsoft verstärkt auf Windows PowerShell als Serververwaltungstool orientiert, gibt es natürlich auch ein Cmdlet *New-ADUser*, mit dem Sie ein Benutzerkonto erstellen und die dazugehörenden Attribute konfigurieren können. Die zahlreichen Parameter des Cmdlets *New-ADUser* (siehe Abbildung 5.14) ermöglichen den Zugriff auf sämtliche Attribute eines Benutzerobjekts.

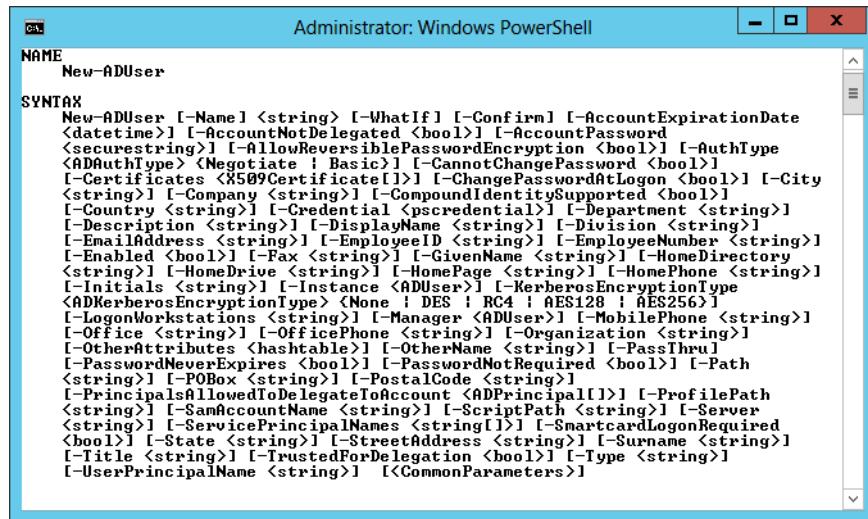


Abbildung 5.14 Syntax des Cmdlets *New-ADUser*

Um zum Beispiel ein neues Benutzerobjekt für Elizabeth Andersen in einer Organisationseinheit (OU) *Research* zu erstellen, rufen Sie das Cmdlet *New-ADUser* mit den folgenden Parametern auf:

```
new-ADUser
-Name "Elizabeth Andersen"
-SamAccountName "eander"
-GivenName "Elizabeth"
-SurName "Andersen"
-path 'OU=Research,DC=adatum,dc=local'
-Enabled $true
-AccountPassword "Pa$$w0rd"
-ChangePasswordAtLogon $true
```

Die Parameter `-Name` und `-SamAccountName` sind erforderlich, um das Objekt zu kennzeichnen, der Parameter `-path` spezifiziert die Position des Objekts in der AD DS-Hierarchie und der Parameter `-Enabled` stellt sicher, dass das Konto aktiv ist.

Benutzervorlagen erstellen

Manchmal müssen Administratoren regelmäßig einzelne Benutzer erstellen, doch enthalten die Benutzerkonten so viele Attribute, dass es zu zeitaufwändig wäre, diese einzeln festzulegen. Komplexe Benutzerobjekte lassen sich schneller erstellen, wenn man die Befehle für das Cmdlet oder das Programm Dsadd.exe in einem Skript oder einer Batchdatei hinterlegt. Bevorzugen Sie allerdings eine grafische Benutzeroberfläche, können Sie mit einer Benutzervorlage etwa das Gleiche bewerkstelligen.

Eine Benutzervorlage ist ein Standardbenutzerobjekt, das Textbausteine für Attributeinstellungen enthält. Möchten Sie einen neuen Benutzer mit diesen Einstellungen anlegen, kopieren Sie einfach die Vorlage in ein neues Benutzerobjekt und ändern den Namen und alle anderen Attribute, die speziell für diesen Benutzer gelten.

Über die Konsole *Active Directory-Benutzer und -Computer* erstellen Sie eine Benutzervorlage in folgenden Schritten:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Erstellen Sie ein Benutzerobjekt mit dem Namen *Standardvorlage*, wobei Sie das Kontrollkästchen *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* deaktivieren und das Kontrollkästchen *Konto ist deaktiviert* setzen.
3. Öffnen Sie das Eigenschaftenblatt des Benutzers und ändern Sie die Attribute auf den verschiedenen Registerkarten in die Werte, die allen Benutzern gemeinsam sind, die Sie erstellen werden.
4. Schließen Sie die Konsole *Active Directory-Benutzer und -Computer*.

Um die Vorlage zu verwenden, klicken Sie mit der rechten Maustaste auf das Benutzerobjekt *Standardvorlage* und wählen im Kontextmenü den Befehl *Kopieren*. Daraufhin startet der Assistent *Objekt kopieren – Benutzer*, den Abbildung 5.15 zeigt.

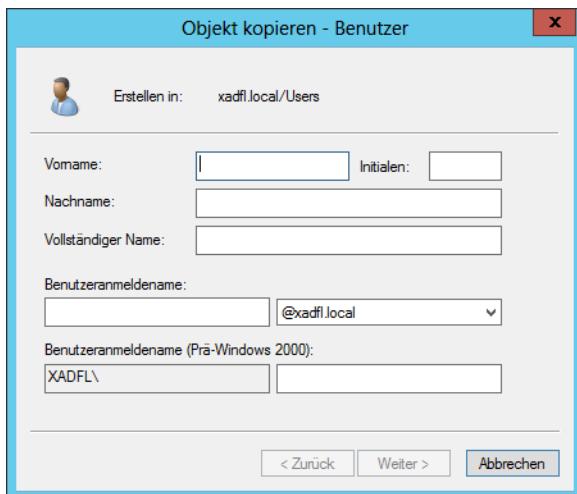


Abbildung 5.15 Der Assistent *Objekt kopieren – Benutzer*

Geben Sie die erforderlichen eindeutigen Informationen für den Benutzer ein und löschen Sie das Kontrollkästchen *Konto ist deaktiviert*, bevor Sie auf *OK* klicken. Der Assistent erstellt ein neues Benutzerobjekt mit sämtlichen Attributen, die Sie in der Vorlage konfiguriert haben.

Mehrere Benutzer erstellen

Zuweilen müssen Administratoren Hunderte oder Tausende von Benutzerobjekten anlegen, sodass die Verfahren zum Erstellen einzelner Objekte nicht praktikabel sind. Die vorherigen Abschnitte haben Methoden beschrieben, wie Sie einzelne Benutzer und Gruppenobjekte über die grafische Benutzeroberfläche und über die in Windows Server 2012 vorhandenen Befehlszeilentools anlegen. Die nächsten Abschnitte untersuchen einige der Mechanismen, um große Mengen von Active Directory-Objekten zu erstellen.

CSVDE.exe

Anwendungen wie zum Beispiel Microsoft Excel können Listen von Benutzern zusammen mit dazugehörenden Informationen erzeugen, die sich dann in die AD DS-Datenbank aufnehmen lassen. In diesen Fällen können Sie Daten aus den Anwendungen exportieren, indem Sie sie in einer Datei im CSV-Format speichern. Das CSV-Format eignet sich auch, um Daten in Anwendungen von Drittanbietern zu importieren und daraus zu exportieren.

Eine CSV-Datei ist eine reine Textdatei, in der jede Zeile einen Eintrag darstellt. Die Einträge sind in Felder unterteilt, die durch Kommas voneinander getrennt sind (CSV – Comma Separated Value). Dieses Format ist geeignet, um Datenbankinformationen auf universelle Art im Klartext zu speichern.

Mit dem Befehlszeilendienstprogramm *CSVDE.exe* können Administratoren Active Directory-Objekte importieren und exportieren. Das Programm verwendet eine CSV-Datei, in der ein Kopfeintrag die Attribute angibt, die in den einzelnen kommagetrennten Feldern

enthalten sind. Der Kopfeintrag ist nichts weiter als die erste Zeile der Textdatei, die die korrekten Attributnamen angibt. Um eine CSV-Datei in die AD DS importieren zu können, müssen die Attributnamen in der Datei mit den Attributen übereinstimmen, wie sie im Active Directory-Schema definiert sind. Nehmen Sie zum Beispiel eine Liste mit Personen und Telefonnummern, die Sie als Benutzer in die Active Directory-Datenbank importieren möchten. Zu diesem Zweck müssen Sie einen Kopfeintrag erstellen, der die zu erzeugenden Objektnamen und Attribute genau widerspiegelt. Für Benutzerkonten sind die folgenden Attribute gebräuchlich:

- **dn** Gibt den definierten Namen des Objekts an, sodass sich das Objekt ordnungsgemäß in Active Directory platzieren lässt
- **samAccountName** Füllt das SAM-Kontofeld
- **objectClass** Gibt den Typ des zu erstellenden Objekts an, beispielsweise Benutzer, Gruppe oder OU
- **telephoneNumber** Füllt das Feld *Telefonnummer*
- **userPrincipalName** Füllt das Feld *Benutzerprinzipalname*

In der CSV-Datei müssen Sie die Daten in der Reihenfolge angeben, wie sie durch die Attribute im Kopfeintrag vorgegeben ist. Falls die Zuordnung von Feldern und Daten nicht stimmt, tritt entweder ein Fehler auf, wenn Sie das Programm *CSVDE.exe* ausführen, oder die erstellten Objekte enthalten unkorrekte Ergebnisse. Das folgende Beispiel für einen Kopfeintrag verwendet die oben aufgeführten Attribute, um ein Benutzerobjekt zu erstellen:

```
dn,samAccountName,userPrincipalName,telephoneNumber,objectClass
```

Ein Eintrag, der diesem Kopfeintrag entspricht, sieht dann beispielsweise so aus:

```
"cn=Elizabeth Andersen,ou=Research,dc=adatum,dc=com",eander,eander@adatum.com,586-555-1234,user
```

Nachdem Sie einen Eintrag für jedes zu erstellende Konto hinzugefügt haben, speichern Sie die Datei mit der Dateierweiterung *.csv*. Mit dem folgenden Befehl können Sie dann das Programm *CSVDE.exe* starten und die Datei importieren:

```
csvde.exe -i -f <filename.csv>
```

Am Schalter *-i* erkennt *CSVDE.exe*, dass diese Operation Daten importiert. Der Schalter *-f* gibt die *.csv*-Datei an, in der die zu importierenden Datensätze stehen.

LDIFDE.exe

Das Dienstprogramm *LDIFDE.exe* besitzt die gleiche Basisfunktionalität wie *CSDVE.exe* und erlaubt es, vorhandene Datensätze in Active Directory zu modifizieren. Deshalb ist *LDIFDE.exe* eine flexiblere Option. Nehmen Sie zum Beispiel an, Sie müssen 200 neue Benutzer in Ihre AD DS-Struktur importieren. Dies lässt sich sowohl mit *CSVDE.exe* als auch mit *LDIFDE.exe* erledigen. Allerdings können Sie mit *LDIFDE.exe* die Objekte später modifizieren oder löschen, während *CSVDE.exe* diese Option nicht bietet.

Die *LDIFDE.exe*-Eingabedateien sind entsprechend dem Standard LDAP-Datenaustauschformat (LDIF) formatiert und lassen sich mit jedem Texteditor erstellen. Das Format für die

Datendatei mit den zu erstellenden Objektdatensätzen unterscheidet sich erheblich von dem Format für *CSVDE.exe*. Das folgende Beispiel zeigt die Syntax für eine Datendatei, um das gleiche Benutzerkonto wie im oben angegebenen *CSVDE.exe*-Beispiel zu erstellen:

```
dn: "cn=Elizabeth Andersen,ou=Research,dc=adatum,dc=com"
changetype: add
ObjectClass: user
SAMAccountName: eander
UserPrincipalName: eander@adatum.com
telephoneNumber: 586-555-1234
```

Bei *LDIFDE.exe* können Sie eine von drei Aktionen angeben, die mit den Datensätzen in der LDIF-Datei durchgeführt werden:

- **Add** Erstellt neue Objekte
- **Modify** Modifiziert vorhandene Objektattribute
- **Delete** Löscht vorhandene Objekte

Nachdem Sie die Datendatei erstellt und mit der Dateierweiterung *.ldf* gespeichert haben, führen Sie das Programm *LDIFDE.exe* mit der folgenden Syntax aus:

```
ldifde -i -f <filename.ldf>
```

Das nächste Beispiel veranschaulicht die LDIF-Syntax, um die Telefonnummer eines vorhandenen Benutzerobjekts zu ändern. Beachten Sie in der letzten Zeile den Bindestrich. Er ist erforderlich, damit die Datei ordnungsgemäß funktioniert.

```
dn: "cn=Elizabeth Andersen,ou=Research,dc=adatum,dc=com"
changetype: modify
replace: telephoneNumber
telephoneNumber: 586-555-1111
-
```

Windows PowerShell

Benutzerobjekte können Sie auch per Windows PowerShell anhand von CSV-Dateien erstellen. Das Cmdlet `Import-Csv` liest die Daten aus der Datei und leitet sie an das Cmdlet `New-ADUser` weiter. Um die Daten aus der Datei in die richtigen Benutzerobjektattribute einzufügen, verweisen Sie in den Parametern des Cmdlets `New-ADUser` auf die Feldnamen im Kopfeintrag der CSV-Datei.

Ein Beispiel für das Massenerzeugen von Benutzerobjekten sieht so aus:

```
Import-Csv users.csv | foreach
{New-ADUser -SamAccountName $_.SamAccountName
-Name $_.Name -Surname $_.Surname
-GivenName $_.GivenName -Path "OU=Research,DC=adatum,DC=COM" -AccountPassword Pa$$w0rd
-Enabled $true}
```

Computerobjekte erstellen

Da ein AD DS-Netzwerk mit einem zentralisierten Verzeichnis arbeitet, müssen sich die Computer, die der Domäne angehören, auf irgendeine Art und Weise verfolgen lassen. Active Directory verwendet hierzu die Computerkonten, die in Form von Computerobjekten in der Active Directory-Datenbank realisiert sind. Wenn Sie über ein gültiges Active Directory-Benutzerkonto und ein Kennwort verfügen, Ihr Computer jedoch nicht durch ein Computerobjekt dargestellt wird, können Sie sich in der Domäne nicht anmelden.

Computerobjekte werden in der Active Directory-Hierarchie genau wie Benutzerobjekte gespeichert und sie besitzen viele der gleichen Fähigkeiten, wie zum Beispiel:

- Computerobjekte bestehen aus Eigenschaften, die den Namen des Computers, seinen Standort und wer sie verwalten darf angeben
- Computerobjekte erben Gruppenrichtlinieneinstellungen von Containerobjekten wie Domänen, Standorten und Organisationseinheiten
- Computerobjekte können Mitglieder von Gruppen sein und Berechtigungen von Gruppenobjekten erben

Wenn sich ein Benutzer bei einer Active Directory-Domäne anmeldet, richtet der Clientcomputer eine Verbindung zu einem Domänencontroller ein, um die Identität des Benutzers zu authentifizieren. Bevor eine Benutzeroauthentifizierung stattfindet, führen die beiden Computer eine vorläufige Authentifizierung mithilfe ihrer jeweiligen Computerobjekte durch, um sicherzustellen, dass beide Systeme Teil der Domäne sind. Der auf dem Clientcomputer laufende Dienst *NetLogon* verbindet sich mit dem gleichen Dienst auf dem Domänencontroller und jeder prüft dann, ob das andere System über ein gültiges Computerkonto verfügt. Ist diese Validierung abgeschlossen, richten beide Systeme einen sicheren Kommunikationskanal zwischen sich ein, über den sie dann mit der Benutzeroauthentifizierung beginnen können.

Die Computerkontoverifikation zwischen dem Client und dem Domänencontroller ist ein originaler Authentifizierungsprozess mit Kontonamen und Kennwörtern, so wie er stattfindet, wenn sich ein Benutzer bei der Domäne authentifiziert. Der Unterschied besteht darin, dass die von den Computerkonten verwendeten Kennwörter automatisch generiert und versteckt gehalten werden. Administratoren können Computerkonten zurücksetzen, doch müssen sie keine Kennwörter für sie bereitstellen.

Für Administratoren heißt das, dass sie nicht nur Benutzerkonten in der Domäne erstellen, sondern auch sicherstellen müssen, dass die Netzwerkcomputer Teil der Domäne sind. Einer AD DS-Domäne fügen Sie einen Computer in zwei Schritten hinzu:

- **Ein Computerkonto erstellen** Hierzu legen Sie ein neues Computerobjekt im Active Directory an und weisen ihm den Namen eines realen Computers im Netzwerk zu
- **Den Computer mit der Domäne verknüpfen** Wenn Sie einen Computer in die Domäne aufnehmen, kontaktiert das System einen Domänencontroller, richtet eine vertrauenswürdige Beziehung mit der Domäne ein, sucht (oder erstellt) ein Computerobjekt, das dem Namen des Computers entspricht, passt seine Sicherheitskennung (SID) an die des Computerobjekts an und modifiziert seine Gruppenmitgliedschaften

Wie diese Schritte durchgeführt werden und wer sie ausführt, hängt von der Art und Weise ab, in der Sie Computer in Ihrem Netzwerk bereitstellen. Es gibt verschiedene Möglichkeiten, neue Computerobjekte zu erstellen, und wie Administratoren an diese Aufgabe herangehen, hängt von mehreren Faktoren ab, unter anderem, wie viele Objekte sie erzeugen müssen, wo sie sich befinden, wenn sie die Objekte erstellen, und welche Tools sie bevorzugen.

Allgemein ausgedrückt, erstellen Sie Computerobjekte, wenn Sie neue Computer in der Domäne bereitstellen. Nachdem ein Computer durch ein Objekt dargestellt und der Domäne beigetreten ist, kann sich jeder Benutzer in der Domäne von diesem Computer aus anmelden. Zum Beispiel brauchen Sie keine neuen Computerobjekte zu erstellen oder Computer erneut mit der Domäne zu verknüpfen, wenn Mitarbeiter die Firma verlassen und neu eingestellte Mitarbeiter ihre Tätigkeit an ihren Computern beginnen. Wenn Sie jedoch das Betriebssystem auf einem Computer neu installieren, müssen Sie ein neues Computerobjekt dafür anlegen (oder das vorhandene zurücksetzen), da der neu installierte Computer eine andere SID erhält.

Ein Computerobjekt muss immer erstellt werden, bevor der entsprechende Computer der Domäne beitreten kann, auch wenn es möglicherweise nicht so aussehen mag. Es gibt die folgenden beiden grundlegenden Strategien, um Active Directory-Computerobjekte zu erstellen:

- Die Computerobjekte vorab mit einem Active Directory-Tool erstellen, sodass die Computer die vorhandenen Objekte finden können, wenn sie der Domäne beitreten
- Mit dem Beitreten zur Domäne beginnen und den Computer sein eigenes Computerobjekt erstellen lassen

In beiden Fällen existiert das Computerobjekt bereits, bevor der Beitritt stattfindet. Zwar scheint bei der zweiten Strategie der Beitritt zuerst stattzufinden, doch der Computer erstellt das Objekt, bevor der eigentliche Beitrittsvorgang beginnt.

Sind mehrere Computer – insbesondere an verschiedenen Standorten – bereitzustellen, ziehen es die meisten Administratoren vor, die Computerobjekte im Voraus anzulegen. Bei einer großen Anzahl von Computern ist es sogar möglich, den Erstellungsvorgang von Computerobjekten mit Befehlszeilertools und Batchdateien zu automatisieren. Die folgenden Abschnitte untersuchen die Tools, die Sie für das Erstellen von Computerobjekten einsetzen können.

Computerobjekte per Active Directory-Benutzer und -Computer erstellen

Wie Benutzerobjekte können Sie Computerobjekte über die Konsole Active Directory-Benutzer und -Computer erstellen. Um Computerobjekte in einer Active Directory-Domäne mithilfe der Konsole *Active Directory-Benutzer und -Computer* oder mit irgendeinem anderen Tool zu erstellen, brauchen Sie die geeigneten Berechtigungen für den Container, in dem die Objekte untergebracht werden.

Standardmäßig verfügt die Gruppe *Administratoren* über die Berechtigungen, Objekte überall in der Domäne zu erstellen, und die Gruppe *Konten-Operatoren* verfügt über spezielle Berechtigungen, um Computerobjekte im Container *Computer* anzulegen und daraus zu löschen sowie von allen neuen OUs, die Sie anlegen. Da die Gruppen *Domänen-Admins* und *Organisations-Admins* Mitglieder der Gruppe *Administratoren* sind, können Mitglieder dieser

Gruppen Computerobjekte überall erstellen. Außerdem kann ein Administrator die Kontrolle von Containern explizit an bestimmte Benutzer oder Gruppen delegieren und sie damit in die Lage versetzen, Computerobjekte in diesen Containern zu erstellen.

Das Erstellen eines Computerobjekts in *Active Directory-Benutzer und -Computer* ist dem Erstellen eines Benutzerobjekts ähnlich. Sie wählen den Container aus, in dem Sie das Objekt unterbringen möchten, und wählen aus dem Menü *Aktion* den Befehl *Neu / Computer*. Daraufhin startet der Assistent *Neues Objekt – Computer*, wie Abbildung 5.16 zeigt.

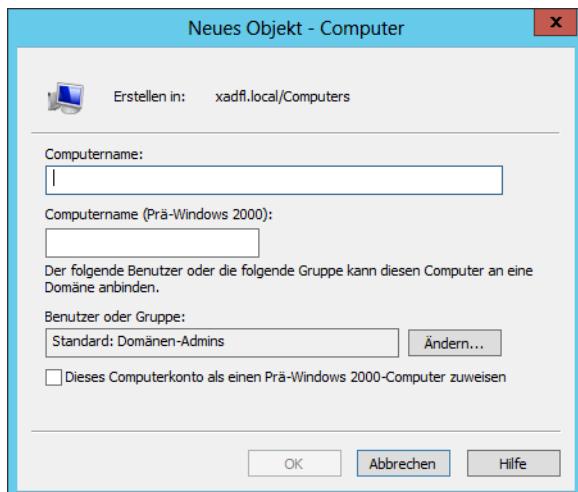


Abbildung 5.16 Der Assistent *Neues Objekt – Computer*

Computerobjekte besitzen relativ wenige Attribute und in den meisten Fällen geben Sie wahrscheinlich nur einen Namen ein, der bis zu 64 Zeichen lang sein kann. Dieser Name muss mit dem Namen des Computers übereinstimmen, der mit dem Objekt verknüpft wird.

Computerobjekte mit dem Active Directory-Verwaltungscenter erstellen

Wie Benutzerobjekte können Sie auch Computerobjekte im Active Directory-Verwaltungscenter erstellen. Wählen Sie dazu einen Container aus und wählen Sie dann *Neu / Computer* in der Aufgabenliste, um das Dialogfeld *Computer erstellen* zu öffnen.

Computer per Dsadd.exe erstellen

Wie für Benutzerobjekte gilt, dass sich die grafischen Tools von Windows Server 2012 zwar gut eignen, um einzelne Objekte zu erstellen und zu verwalten, doch wenn es um mehrere Objekte geht, wenden sich viele Administratoren der Befehlszeile zu.

Das Dienstprogramm *Dsadd.exe* ermöglicht es, Computerobjekte von der Befehlszeile aus zu erstellen, so wie Sie die Benutzerobjekte weiter vorn in diesem Kapitel angelegt haben. Außerdem können Sie mithilfe einer Batchdatei aus *Dsadd.exe*-Befehlen mehrere Objekte auf

einmal generieren. Die grundlegende Syntax für das Erstellen eines Computerobjekts per *Dsadd.exe* lautet:

```
dsadd computer <Computer-DN>
```

Der Parameter <Computer-DN> spezifiziert einen definierten Namen für das neu zu erstellende Gruppenobjekt. Die definierten Namen (DN) verwenden das gleiche Format wie in CSV-Dateien, die weiter oben beschrieben wurden.

Computerobjekte mit Windows PowerShell erstellen

Mit dem Windows PowerShell-Cmdlet `New-ADComputer` können Sie Computerobjekte gemäß der folgenden grundlegenden Syntax erstellen:

```
new-ADComputer -Name <Computername> -path <DN>
```

Dieses Cmdlet erstellt Computerobjekte, verknüpft sie aber nicht mit einer Domäne.

Active Directory-Objekte verwalten

Nachdem Sie Benutzer- und Computerobjekte erstellt haben, können Sie sie in vielerlei Hinsicht mit den gleichen Mitteln verwalten und modifizieren, mit denen Sie sie erstellt haben.

Wenn Sie im *Active Directory-Verwaltungscenter* oder in der Konsole *Active Directory-Benutzer und -Computer* auf ein Objekt doppelklicken, erscheint das Eigenschaftenblatt für dieses Objekt. Das Fenster sieht etwas anders aus, enthält aber die gleichen Informationen und bietet die gleichen Möglichkeiten, um die Objektattribute zu bearbeiten.

Mehrere Benutzer verwalten

Wenn Sie Domänenbenutzerkonten verwalten, kommt es sicherlich hin und wieder vor, dass die gleichen Änderungen an mehreren Benutzerobjekten vorzunehmen sind. Müsste man sie einzeln ändern, wäre das recht umständlich.

In diesen Situationen ist es möglich, über das *Active Directory-Verwaltungscenter* oder die Konsole *Active Directory-Benutzer und -Computer* die Eigenschaften von mehreren Benutzerkonten gleichzeitig zu modifizieren. Wählen Sie einfach mehrere Benutzerobjekte aus, indem Sie die `Strg`-Taste gedrückt halten und auf die einzelnen Benutzer klicken. Haben Sie alle Benutzer markiert, wählen Sie *Eigenschaften*. Es erscheint ein Eigenschaftenblatt mit den Attributen, die Sie für die ausgewählten Objekte gleichzeitig bearbeiten können (siehe Abbildung 5.17).

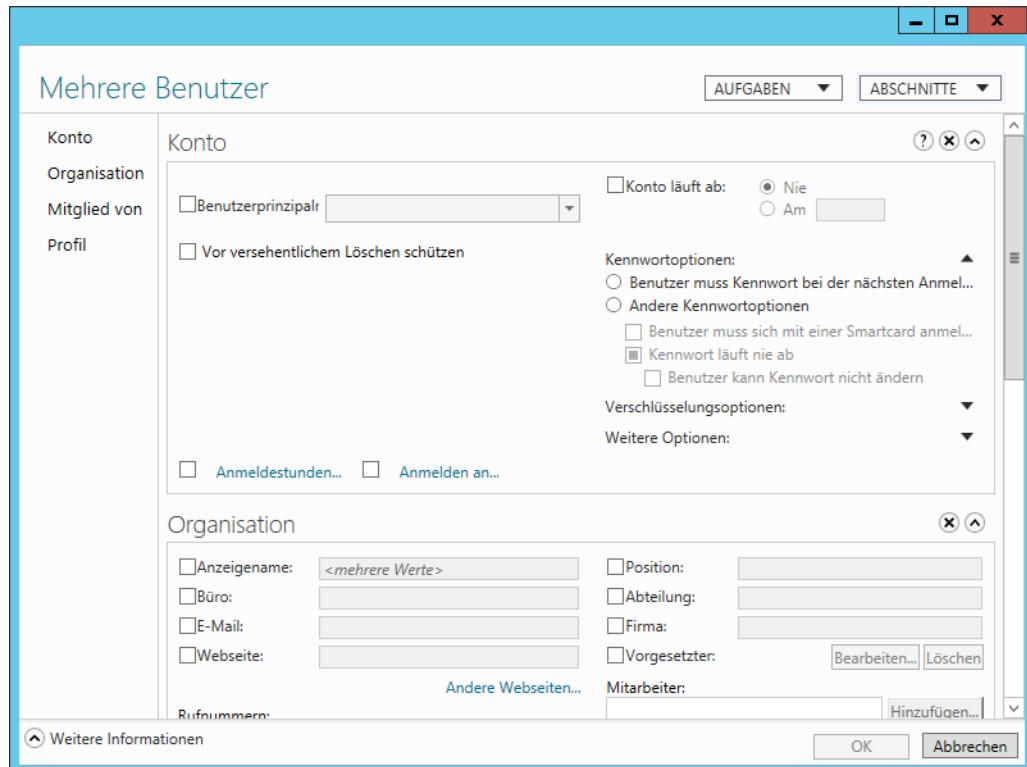


Abbildung 5.17 Ein Eigenschaftenblatt *Mehrere Benutzer* im Active Directory-Verwaltungcenter

Beitreten eines Computers zu einer Domäne

Das Beitreten eines Computers zu einer Domäne muss auf dem Computer selbst erfolgen und ist durch ein Mitglied der lokalen Administratorgruppe des Computers durchzuführen. Nach dem Anmelden verknüpfen Sie einen Windows Server 2012-Computer mit einer Domäne auf dem Blatt *Systemeigenschaften* über die Registerkarte *Computername*. Das Blatt *Systemeigenschaften* ist vom Server-Manager aus erreichbar. Klicken Sie dazu auf der Kachel *Eigenschaften* des Servers auf den Hyperlink neben *Computername* oder *Domäne*.

Auf einem Computer, der noch keiner Domäne beigetreten ist, zeigt die Registerkarte *Computername* den Namen an, der dem Computer während der Betriebssysteminstallation zugewiesen wurde, und den Namen der Arbeitsgruppe (in der Standardeinstellung *WORKGROUP*), zu der das System derzeit gehört. Um den Computer mit der Domäne zu verknüpfen, klicken Sie auf *Ändern*. Daraufhin erscheint das Dialogfeld *Ändern des Computernamens bzw. der Domäne* (siehe Abbildung 5.18).

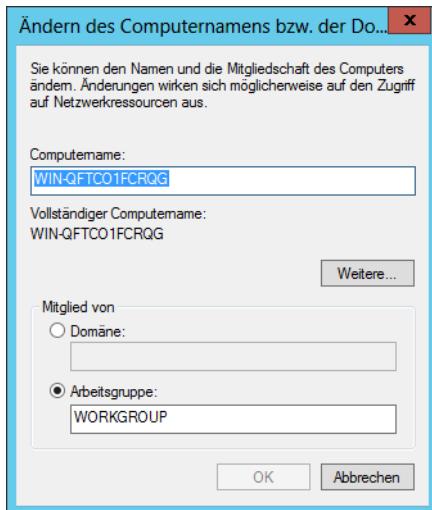


Abbildung 5.18 Das Dialogfeld Ändern des Computernamens bzw. der Domäne

In diesem Dialogfeld können Sie im Feld *Computername* den Namen ändern, der dem Computer während der Installation zugewiesen wurde. Abhängig davon, ob Sie bereits ein Computerobjekt erstellt haben, sind die folgenden Vorsichtsmaßnahmen zu berücksichtigen:

- Um einer Domäne beizutreten, in der Sie bereits ein Computerobjekt für das System in den AD DS erstellt haben, muss der Name dieses Felds mit dem Namen des Objekts genau übereinstimmen
- Wenn Sie ein Computerobjekt während des Beitrittsvorgangs erstellen wollen, darf der Name in diesem Feld noch nicht in der Domäne existieren

Wenn Sie die Option *Domäne* auswählen und den Namen der Domäne eingeben, der der Computer beitreten soll, kontaktiert der Computer einen Domänencontroller für die Domäne und es erscheint ein zweites Dialogfeld *Ändern des Computernamens bzw. der Domäne* mit der Abfrage von Name und Kennwort eines Domänenbenutzerkontos mit der Berechtigung, den Computer in die Domäne aufzunehmen.

Nachdem Sie beim Domänencontroller authentifiziert sind, wird der Computer in der Domäne begrüßt und Sie erhalten die Aufforderung, den Computer neu zu starten.

Einer Domäne mit Netdom.exe beitreten

Es ist auch möglich, mit dem Befehlszeilendienstprogramm *Netdom.exe* einen Computer mit einer Domäne zu verknüpfen. Die Syntax für den Befehl lautet:

```
netdom join <Computername> /Domain:<Domänenname>
[/UserD:<Benutzer> /PasswordD:<Benutzerkennwort>] [/OU:OU DN]
```

Computerobjekte während des Beitriffs erstellen

Einen Computer können Sie einer Domäne anschließen, unabhängig davon, ob Sie bereits ein Computerobjekt für ihn erstellt haben. Nachdem der Computer beim Domänencontroller authentifiziert ist, durchsucht der Domänencontroller die Active Directory-Datenbank nach einem Computerobjekt mit demselben Namen wie der Computer. Findet er kein übereinstimmendes Objekt, erstellt der Computer ein Objekt im Container *Computer* mit dem vom Computer gelieferten Namen.

Damit sich das Computerobjekt auf diese Weise automatisch erstellen lässt, würde man erwarten, dass das bei der Verbindung zum Domänencontroller angegebene Benutzerkonto über Rechte zur Objekterstellung für den Container *Computer* verfügen muss, beispielsweise als Mitgliedschaft in der Administratorgruppe. Allerdings ist dies nicht immer der Fall.

Domänenbenutzer können Computerobjekte auch über einen interessanten, indirekten Prozess erstellen. Das Gruppenrichtlinienobjekt (GPO) *Standarddomänencontroller-Richtlinie* gewährt der speziellen Identität *Authentifizierte Benutzer* das Benutzerrecht *Hinzufügen von Arbeitsstationen zur Domäne*, wie Abbildung 5.19 zeigt. Das heißt, dass jeder Benutzer, der in Active Directory erfolgreich authentifiziert wurde, das Recht erhält, bis zu 10 Arbeitsstationen zur Domäne hinzuzufügen und 10 dazugehörige Computerobjekte zu erstellen, selbst wenn der Benutzer keine expliziten Berechtigungen zum Erstellen von Objekten besitzt.

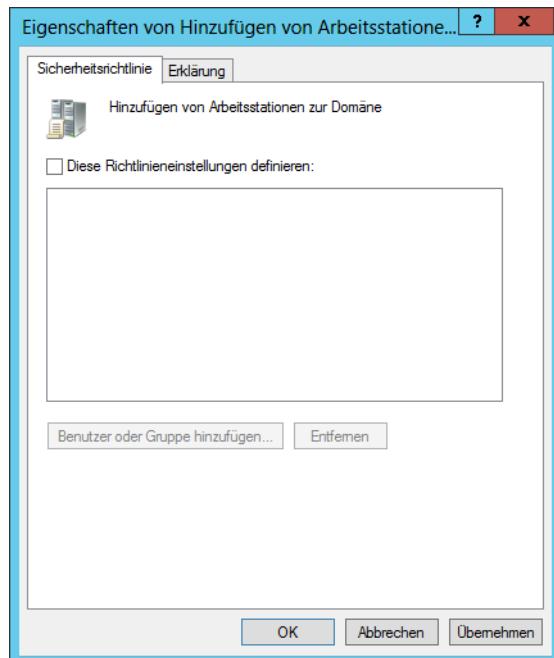


Abbildung 5.19 Die Zuweisungen der Benutzerrechte *Standarddomänencontroller-Richtlinie*



Hinweis Benutzerrechte zuweisen

Benutzerrechte sind Gruppenrichtlinieneinstellungen, die Benutzer in die Lage versetzen, bestimmte systembezogene Aufgaben durchzuführen. Zum Beispiel erfordert das lokale Anmelden an einem Domänencontroller, dass einem Benutzer entweder das Recht *Lokal anmelden* erteilt wurde oder sein Konto ein Mitglied der Gruppe *Konten-Operatoren*, *Administratoren*, *Sicherungs-Operatoren*, *Druck-Operatoren* oder *Server-Operatoren* auf dem Domänencontroller ist. Ähnliche Einstellungen, die in dieser Auflistung enthalten sind, beziehen sich auf Benutzerrechte, die mit Herunterfahren des Betriebssystems, Besitzübernahme von Datei- oder Objektrechten und Synchronisieren von Verzeichnisdienstdaten verbunden sind. Weitere Informationen zur Zuweisung von Benutzerrechten finden Sie in Kapitel 6 im Prüfungsziel 6.2.

Im Offline-Status einer Domäne beitreten

Administratoren verknüpfen Computer mit Domänen normalerweise dann, wenn die Computer mit dem Netzwerk verbunden sind und auf einen Domänencontroller zugreifen können. Es gibt jedoch Situationen, in denen Administratoren Computer einrichten möchten, ohne dass Zugriff auf einen Domänencontroller besteht. Das ist beispielsweise bei einer Neuinstallation in einer Zweigniederlassung der Fall. Unter diesen Umständen ist es möglich, einen Beitritt zur Domäne im Offline-Status durchzuführen. Dies lässt sich mit dem Befehlszeilenprogramm *Djoin.exe* bewerkstelligen. Der Offline-Domänenbeitritt erfordert, dass Sie das Programm *Djoin.exe* zweimal ausführen – zuerst auf einem Computer mit Zugriff auf einen Domänencontroller und dann auf dem Computer, der der Domäne beitreten soll. Wenn die Verbindung zum Domänencontroller besteht, holt das Programm Metadaten des Computerkontos für das anzuschließende System und speichert sie in einer Datei. Die Syntax für diese Phase lautet:

```
djoin /provision /domain <Domäne>
/machine <Computername> /savefile <Dateiname.txt>
```

Dann bringen Sie die Metadatendatei zum Computer, der der Domäne beitreten soll, und führen dort *Djoin.exe* erneut aus, wobei Sie den Namen der Datei angeben. Das Programm speichert die Metadaten aus der Datei auf dem Computer, sodass das System automatisch der Domäne angeschlossen wird, sobald es auf einen Domänencontroller zugreifen kann. Die Syntax für diese zweite Phase sieht folgendermaßen aus:

```
djoin /requestODJ /loadfile <Dateiname.txt>
/windowspath %SystemRoot% /localos
```

Deaktivierte Konten verwalten

Ein deaktiviertes Benutzerkonto kann niemand verwenden, um sich an der Domäne anzumelden, bis ein Administrator mit den passenden Berechtigungen es wieder aktiviert. Benutzerkonten können Sie manuell deaktivieren, um ihre Verwendung zu verhindern, dabei aber sämtliche Attribute der Konten zu bewahren. Es ist allerdings auch möglich, dass ein System sie automatisch deaktiviert. Zum Beispiel können wiederholte Verletzungen von Kennwortrichtlinieneinstellungen ein Konto deaktivieren, um Angreifer daran zu hindern, weitere Angriffsversuche zu unternehmen.

Um ein Benutzerkonto im *Active Directory-Verwaltungscenter* oder in der Konsole *Active Directory-Benutzer und -Computer* zu deaktivieren oder zu aktivieren, klicken Sie mit der rechten Maustaste auf das Objekt und wählen im Kontextmenü den Befehl *Deaktivieren* bzw. *Aktivieren*. Es ist auch möglich, mehrere Konten auf einmal zu deaktivieren/aktivieren. Markieren Sie dazu alle gewünschten Objekte und klicken Sie dann mit der rechten Maustaste.

Ein Benutzer- oder Computerkonto lässt sich auch per Windows PowerShell mit der folgenden Cmdlet-Syntax deaktivieren bzw. aktivieren:

```
Disable-ADAccount -Identity <Kontoname>
```

```
Enable-ADAccount -Identity <Kontoname>
```

Prüfungszielzusammenfassung

- Das Benutzerkonto ist das Hauptinstrument, über das Personen in einem AD DS-Netzwerk auf Ressourcen zugreifen
- Zu den häufigsten Aufgaben von Administratoren gehört es, Active Directory-Benutzerobjekte zu erstellen. Windows Server 2012 bringt hierfür mehrere Tools mit.
- In Windows Server 2012 wurde die mit Windows Server 2008 R2 eingeführte Anwendung *Active Directory-Verwaltungscenter* (ADAC) überarbeitet, um neue Features wie zum Beispiel den Active Directory-Papierkorb und abgestimmte Kennwortrichtlinien vollständig einzubinden. Mit diesem Tool können Sie auch AD DS-Benutzerkonten erstellen und verwalten.
- Microsoft Excel und Microsoft Exchange sind zwei gängige Anwendungen, in denen Sie eine Reihe von Benutzern zusammen mit ihren dazugehörenden Informationen speichern können, um sie der AD DS-Datenbank hinzuzufügen. In diesen Fällen können Sie Daten aus den Anwendungen exportieren, indem Sie sie in einer Datei im CSV-Format speichern.
- Das Dienstprogramm *LDIFDE.exe* besitzt die gleiche Basisfunktionalität wie *CSDVE.exe* und erlaubt es, vorhandene Datensätze in Active Directory zu modifizieren
- Da ein AD DS-Netzwerk mit einem zentralisierten Verzeichnis arbeitet, müssen sich die Computer, die der Domäne angehören, auf irgendeine Art und Weise verfolgen lassen. Active Directory verwendet hierzu die Computerkonten, die in Form von Computerobjekten in der Active Directory-Datenbank realisiert sind.
- Das Beitreten eines Computers zu einer Domäne muss auf dem Computer selbst erfolgen und ist durch ein Mitglied der lokalen Administratorgruppe des Computers durchzuführen
- Es ist möglich, einen Beitritt zur Domäne im Offline-Status durchzuführen. Dies lässt sich mit dem Befehlszeilenprogramm *Djoin.exe* bewerkstelligen.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Mit welchem Tool kann man Objekte in Active Directory hinzufügen, löschen oder modifizieren und zudem bei Bedarf das Schema ändern?
 - A. DCPROMO
 - B. LDIFDE
 - C. CSVDE
 - D. NSLOOKUP
2. Wie heißt die erste Zeile der Textdatei mit den passenden Attributnamen, wenn Sie mit CSVDE arbeiten?
 - A. Kopfzeile
 - B. Kopfeintrag
 - C. Namenszeile
 - D. Namenseintrag
3. Mit welchem der folgenden Dienstprogramme können Sie einen Computer im Offline-Status einer Domäne anschließen?
 - A. net join
 - B. join
 - C. djoin
 - D. dconnect
4. Bei welchem der folgenden Konten handelt es sich nicht um einen Benutzerkontentyp, der sich in Windows Server 2012 konfigurieren lässt?
 - A. Lokale Konten
 - B. Domänenkonten
 - C. Netzwerkkonten
 - D. Integrierte Konten
5. Welche der folgenden Konten sind die beiden integrierten Benutzerkonten, die auf einem Windows Server 2012-Computer automatisch erstellt werden?
 - A. Netzwerk
 - B. Interaktiv
 - C. Administrator
 - D. Gast



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Als Netzwerkadministrator bauen Sie ein Active Directory-Netzwerk für eine Firma Fabrikam, Inc., auf und müssen Benutzerobjekte für die 75 Benutzer der Abteilung *Innendienst* erstellen. Hierfür haben Sie bereits die Domäne *fabrikam.com* und eine Organisationsseinheit *Innendienst* eingerichtet. Die Personalabteilung hat Ihnen eine Liste der Benutzer übergeben und Sie angewiesen, die Kontonamen aus dem Anfangsbuchstaben des Vornamens und aus dem Nachnamen zu bilden. Außerdem muss jedes Benutzerobjekt den Wert *Innendienst* in der Eigenschaft *Abteilung* (*dept*) und *Fabrikam, Inc.* in der Eigenschaft *Firma* (*company*) enthalten. Welches der folgenden Befehlszeilenformate erlaubt es, die 75 Benutzerobjekte mit den geforderten Eigenschaftswerten zu erstellen, wenn Sie als Beispiel den ersten Namen in der Liste, Oliver Cox, annehmen?

- A: dsadd "Oliver Cox" -company "Fabrikam, Inc." -dept "Innendienst"
 - B: dsadd user CN=Oliver Cox,CN=Innendienst,DC=fabrikam,DC=com -company Fabrikam, Inc. -dept Innendienst
 - C: dsadd -company "Fabrikam, Inc." -dept "Innendienst" "CN=Oliver Cox,CN=Innendienst,DC=fabrikam,DC=com"
 - D: dsadd user "CN=Oliver Cox,CN=Innendienst,DC=fabrikam,DC=com" -company "Fabrikam, Inc." -dept "Innendienst"
-

Prüfungsziel 5.3: Active Directory-Gruppen und Organisationseinheiten erstellen und verwalten

Organisationseinheiten (OUs) lassen sich strukturell verschachteln, sodass Administratoren von der oben erwähnten Vererbung profitieren können. Allerdings sollten Sie die Anzahl der Verschachtelungsebenen bei Organisationseinheiten begrenzen, da zu viele Ebenen die Reaktion auf Ressourcenanfragen bremsen und die Anwendung von Gruppenrichtlinien-einstellungen verkomplizieren können.

Wenn Sie Active Directory-Domäendienste erstmals installieren, gibt es in der Domäne standardmäßig nur eine Organisationseinheit: die OU *Domänencontroller*. Alle anderen Organisationseinheiten muss ein Domänenadministrator einrichten.



Hinweis Organisationseinheiten und Berechtigungen

Organisationseinheiten gelten nicht als Sicherheitsprinzipale. Folglich können Sie einer Resource, die auf der Mitgliedschaft in einer OU basiert, keine Zugriffsberechtigungen zuweisen. Hierin liegt der Unterschied zwischen Organisationseinheiten und globalen, domänenlokalen und universalen Gruppen. Gruppen werden verwendet, um Zugriffsberechtigungen zuzuweisen, während Organisationseinheiten dazu dienen, Ressourcen zu organisieren und Berechtigungen zu delegieren.

In einer Domäne gibt es noch einen anderen Typ von Containerobjekt, das tatsächlich als *Container* bezeichnet wird. Zum Beispiel enthält eine neu erstellte Domäne mehrere Containerobjekte. Dazu gehören das Objekt *Users*, das die vordefinierten Benutzer und Gruppen der Domäne enthält, und das Objekt *Computers* mit den Computerobjekten für alle Systeme, die der Domäne beigetreten sind.

Im Unterschied zu Organisationseinheiten können Sie Containerobjekten weder Gruppenrichtlinieneinstellungen zuweisen noch deren Administration delegieren. Zudem ist es mit den Active Directory-Standardverwaltungstools wie zum Beispiel mit der Konsole *Active Directory-Benutzer und -Computer* nicht möglich, neue Containerobjekte zu erstellen. Containerobjekte lassen sich zwar per Skript erstellen, doch gibt es keinen triftigen Grund, so zu verfahren. Eine Domäne gliedert man vorzugsweise mithilfe von Organisationseinheiten.

Dieses Prüfungsziel zeigt, wie Sie

- Gruppenverschachtelung konfigurieren
- Gruppen konvertieren (einschließlich Sicherheit, Verteiler, universal, domänenlokal und domänenglobal)
- Gruppenmitgliedschaft mithilfe von Gruppenrichtlinien verwalten
- Gruppenmitgliedschaft aufzählen
- das Erstellen und Verwalten von Active Directory-Objekten delegieren
- Active Directory-Standardcontainer verwalten
- Gruppen und Organisationseinheiten erstellen, kopieren, konfigurieren und löschen

Organisationseinheiten erstellen

Organisationseinheiten stellen den einfachsten Objekttyp dar, der sich in der AD DS-Hierarchie erstellen lässt. Hierfür müssen Sie lediglich einen Namen für das Objekt angeben und seine Position in der Active Directory-Struktur definieren.

Im *Active Directory-Verwaltungscenter* erstellen Sie ein OU-Objekt in folgenden Schritten:

1. Melden Sie sich am Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen sie *Active Directory-Verwaltungscenter*, um die Konsole *Active Directory-Verwaltungscenter* zu öffnen.
3. Klicken Sie mit der rechten Maustaste im linken Fensterbereich auf das Objekt, unter dem Sie die neue Organisationseinheit erstellen möchten, und wählen Sie im Kontextmenü *Neu / Organisationseinheit*. Daraufhin erscheint das in Abbildung 5.20 gezeigte Fenster *Organisationseinheit erstellen*.

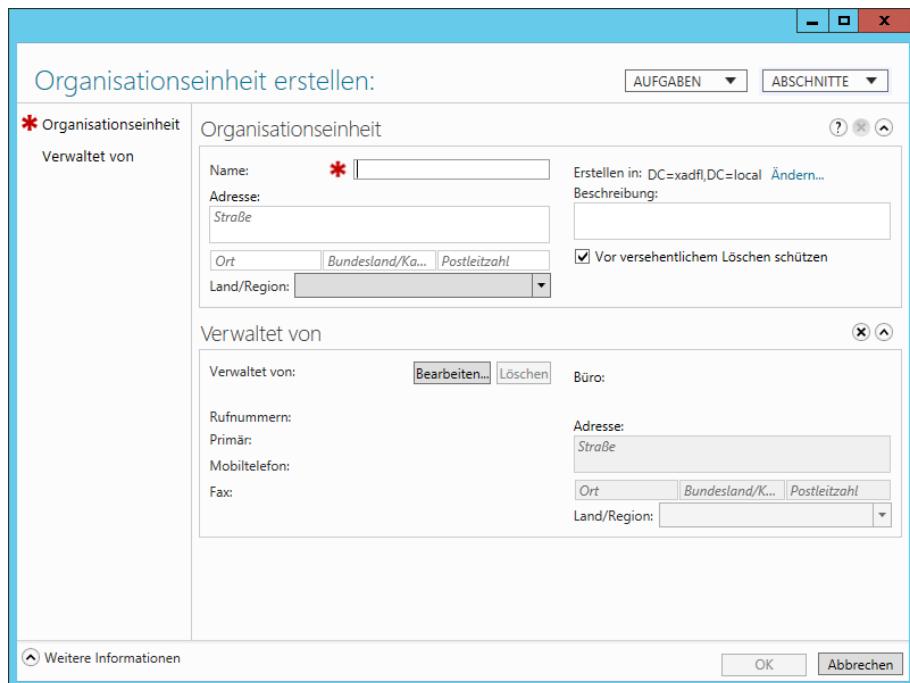


Abbildung 5.20 Das Fenster *Organisationseinheit erstellen* im *Active Directory-Verwaltungscenter*

4. Geben Sie in das Feld *Name* einen Namen für die Organisationseinheit ein und fügen Sie bei Bedarf optionale Informationen hinzu.
5. Klicken Sie auf *OK*. Das OU-Objekt erscheint im Container.
6. Schließen Sie die Konsole *Active Directory-Verwaltungscenter*.

In der Konsole *Active Directory-Benutzer und -Computer* erstellen Sie eine Organisationseinheit fast in der gleichen Weise, auch wenn das Dialogfeld *Neues Objekt – Organisationseinheit* anders aussieht. Nachdem Sie eine Organisationseinheit erstellt haben, können Sie darauf doppelklicken, um ihr Eigenschaftenblatt zu öffnen und ihre Attribute zu bearbeiten, oder mit der rechten Maustaste darauf klicken und *Verschieben* wählen, um das Dialogfeld *Verschieben* zu öffnen, das in Abbildung 5.21 zu sehen ist.

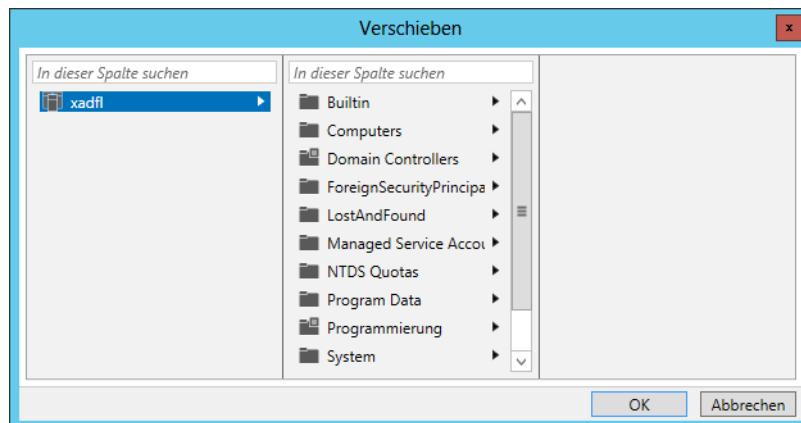


Abbildung 5.21 Das Dialogfeld *Verschieben* im *Active Directory-Verwaltungszentrum*

Active Directory-Verwaltungsaufgaben mithilfe von Organisationseinheiten delegieren

Mithilfe von Organisationseinheiten lässt sich ein dezentralisiertes Verwaltungsmodell implementieren, in dem andere Administratoren Teile der AD DS-Hierarchie verwalten, ohne die übrige Struktur zu beeinflussen.

Wenn Sie die Autorität auf Standortebene delegieren, wirkt sich das auf alle Domänen und Benutzer an diesem Standort aus. Eine Delegierung auf Domänenebene beeinflusst die gesamte Domäne. Wenn Sie jedoch die Autorität auf der Ebene der Organisationseinheit delegieren, sind davon nur diese Organisationseinheit sowie alle ihre untergeordneten Objekte betroffen. Indem Sie die Verwaltungsautorität für eine OU-Struktur im Unterschied zu einer gesamten Domäne oder einem Standort gewähren, bieten sich Ihnen die folgenden Vorteile:

- **Geringste Anzahl von Administratoren mit globalen Berechtigungen** Mit einer Hierarchie von Verwaltungsebenen schränken Sie den Personenkreis ein, der globalen Zugriff benötigt
- **Begrenzter Fehlerbereich** Verwaltungstechnische Fehler wie zum Beispiel das Löschen eines Container- oder Gruppenobjekts beeinflussen nur die jeweilige OU-Struktur

Der Assistent zum Zuweisen der Objektverwaltung bietet eine einfache Benutzeroberfläche, in der Sie Berechtigungen für Domänen, Organisationseinheiten und Container delegieren können. Die AD DS besitzen ihr eigenes Berechtigungssystem, das dem von NTFS und Druckern ähnelt. Der Assistent zum Zuweisen der Objektverwaltung ist praktisch eine

Frontend-Oberfläche, die komplexe Kombinationen von Berechtigungen je nach konkreten Verwaltungsaufgaben bildet.

Über die Benutzeroberfläche des Assistenten lassen sich Benutzern oder Gruppen Verwaltungsberechtigungen und die spezifischen Aufgaben, die sie ausführen dürfen, zuweisen. Dabei können Sie vordefinierte Aufgaben delegieren oder benutzerdefinierte Aufgaben erstellen, falls Sie spezifischere Zuweisungen benötigen.

Um die Objektverwaltung über eine Organisationseinheit zu delegieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich am Windows Server 2012-Server unter einem Konto mit Administratorrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Öffnen Sie die Konsole *Active Directory-Benutzer und -Computer*, klicken Sie mit der rechten Maustaste auf das Objekt, dem Sie die Verwaltung zuweisen möchten, und klicken Sie auf *Objektverwaltung zuweisen*. Der Assistent zum Zuweisen der Objektverwaltung startet und zeigt die Seite *Willkommen* an.
3. Klicken Sie auf *Weiter*, um zur Seite *Benutzer oder Gruppen* zu gehen.
4. Klicken Sie auf *Hinzufügen zu*, um das Dialogfeld *Benutzer, Computer oder Gruppen auswählen* zu öffnen.
5. Geben Sie den Namen des Benutzers oder der Gruppe ein, dem/der Sie die Objektverwaltung zuweisen möchten, und klicken Sie auf *OK*. Der Benutzer oder die Gruppe erscheint in der Liste *Ausgewählte Benutzer und Gruppen*.
6. Klicken Sie auf *Weiter*. Die Seite *Zuzuweisende Aufgaben* enthält die folgenden Optionen:
 - **Folgende allgemeine Aufgaben zuweisen** Bei dieser Option können Sie aus einer Liste von vordefinierten Aufgaben auswählen
 - **Benutzerdefinierte Aufgaben zum Zuweisen erstellen** Bei dieser Option haben Sie die Möglichkeit, spezifischere Festlegungen für eine zuzuweisende Aufgabe zu treffen.
7. Wählen Sie *Benutzerdefinierte Aufgaben zum Zuweisen erstellen* und klicken Sie auf *Weiter*. Daraufhin zeigt die Seite *Active Directory-Objekttyp* die folgenden Optionen an:
 - **Diesem Ordner, bestehenden Objekten in diesem Ordner und neuen Objekten in diesem Ordner** Diese Option weist die Objektverwaltung dem Container einschließlich aller seiner aktuellen und zukünftigen Objekte zu
 - **Folgenden Objekten im Ordner** Bei dieser Option lassen sich spezifische Objekte auswählen, denen die Verwaltung zugewiesen werden soll. Mit *Gewählte Objekte in diesem Ordner erstellen* lassen Sie das Erstellen der ausgewählten Objekttypen zu, bei *Gewählte Objekte in diesem Ordner löschen* dürfen die ausgewählten Objekttypen gelöscht werden.

8. Wählen Sie die Option *Diesem Ordner, bestehenden Objekten in diesem Ordner und neuen Objekten in diesem Ordner* und klicken Sie auf *Weiter*. Die Seite *Berechtigungen* wird geöffnet.
9. Legen Sie die zugewiesenen Berechtigungen entsprechend Ihren Anforderungen für den Benutzer oder die Gruppe fest, dem/der Sie die Verwaltung zuweisen möchten. Die Berechtigungen können Sie aus den folgenden drei Optionen kombinieren:
 - **Allgemein** Zeigt allgemeine Berechtigungen an. Diese entsprechen den Berechtigungen auf der Registerkarte *Sicherheit* in den Eigenschaften eines Objekts.
 - **Eigenschaftenspezifisch** Zeigt Berechtigungen an, die sich auf bestimmte Attribute oder Eigenschaften eines Objekts beziehen
 - **Erstellen/Löschen der Berechtigungen von bestimmten untergeordneten Objekten** Zeigt Berechtigungen an, die für die Berechtigungen zum Erstellen und Löschen von festgelegten Objekttypen gelten
10. Klicken Sie auf *Weiter*. Es erscheint die Seite *Fertigstellen des Assistenten*.
11. Klicken Sie auf *Fertig stellen*.
12. Schließen Sie die Konsole *Active Directory-Benutzer und -Computer*.

Mit diesen Schritten haben Sie einem bestimmten Administrator oder einer Gruppe von Administratoren Berechtigungen für einen Teil des Active Directory erteilt. Mit dem Assistenten zum Zuweisen der Objektverwaltung können Sie Berechtigungen zwar erteilen, jedoch weder ändern noch entfernen. Für diese Aufgaben müssen Sie auf die Registerkarte *Sicherheit* im Eigenschaftenblatt des AD DS-Objekts zurückgreifen.



Hinweis Erweiterte Ansicht

In der Konsole *Active Directory-Benutzer und -Computer* ist die Registerkarte *Sicherheit* im Eigenschaftenblatt einer Organisationseinheit standardmäßig nicht zu sehen. Um die Registerkarte anzuzeigen, müssen Sie im Menü *Ansicht* der Konsole den Befehl *Erweiterte Features* wählen.

Mit Gruppen arbeiten

Seit den frühen Tagen der Microsoft-Serverbetriebssysteme haben Administratoren Gruppen verwendet, um Netzwerkberechtigungen zu verwalten. Mithilfe von Gruppen lassen sich Berechtigungen an mehrere Benutzer gleichzeitig zuweisen. Eine Gruppe kann man als Sammlung von Benutzer- oder Computerkonten definieren, die als Sicherheitsprinzipal fungieren, was weitgehend der Funktion eines Benutzers ähnelt.

Wenn sich ein Benutzer in Windows Server 2012 bei Active Directory anmeldet, wird ein Zugriffstoken erstellt, das den Benutzer und die Gruppenmitgliedschaften dieses Benutzers kennzeichnet. Domänencontroller verifizieren anhand dieses Zugriffstokens die Berechtigungen eines Benutzers, wenn dieser auf eine lokale oder Netzwerkressource zugreifen möchte. Mithilfe von Gruppen können Administratoren mehreren Benutzern dieselbe

Berechtigungsebene für Ressourcen im Netzwerk erteilen. Wenn zum Beispiel 25 Benutzer in der Grafikabteilung Zugang zu einem Farbdrucker haben müssen, können Sie entweder jedem Benutzer die entsprechenden Berechtigungen für den Drucker zuweisen oder eine Gruppe, die die 25 Benutzer enthält, erstellen und die passenden Berechtigungen der Gruppe zuweisen. Wenn der Zugriff auf eine Ressource über ein Gruppenobjekt erfolgt, haben Sie Folgendes erreicht:

- Wenn Benutzer auf den Drucker zugreifen müssen, genügt es, sie der Gruppe hinzuzufügen. Damit erhalten die Benutzer sämtliche Berechtigungen, die dieser Gruppe zugewiesen sind. Analog können Sie Benutzer aus der Gruppe entfernen, wenn Sie ihnen den Zugriff auf den Drucker entziehen möchten.
- Administratoren brauchen eine Änderung nur einmal vorzunehmen, um die Zugriffsebene auf den Drucker für alle Benutzer zu modifizieren. Werden die Berechtigungen der Gruppe geändert, ändert sich auch die Berechtigungsebene für alle Gruppenmitglieder. Ohne die Gruppe müssen Sie alle 25 Benutzerkonten einzeln modifizieren.



Hinweis Zugriffstoken

Zugriffstoken werden für Benutzer nur generiert, wenn sie sich erstmals im Netzwerk von ihrer Arbeitsstation aus anmelden. Wenn Sie Benutzer einer Gruppe hinzufügen, müssen sich die Benutzer abmelden und dann wieder anmelden, damit diese Änderung in Kraft tritt.

Benutzer können Mitglieder von mehreren Gruppen sein. Zudem können Gruppen andere Active Directory-Objekte wie zum Beispiel Computer und andere Gruppen aufnehmen. Diese als *Gruppenverschachtelung* bezeichnete Technik beschreibt den Vorgang, eine oder mehrere Gruppen als Mitglieder einer anderen Gruppe zu konfigurieren. Nehmen Sie als Beispiel eine Firma mit zwei Gruppen an: *Marketing* und *Grafikdesign*. Die Mitglieder der Gruppe *Grafikdesign* haben Zugriff auf einen hochauflösenden Farblaserdrucker. Wenn die Mitglieder der Gruppe *Marketing* nun ebenfalls diesen Drucker benötigen, können Sie einfach der Gruppe *Grafikdesign* die Gruppe *Marketing* als Mitglied hinzufügen. Damit erhalten die Mitglieder der Gruppe *Marketing* dieselben Berechtigungen für den Farblaserdrucker wie die Mitglieder der Gruppe *Grafikdesign*.

Gruppentypen

In Windows Server 2012 gibt es zwei Gruppenklassifizierungen: *Gruppentyp* und *Gruppenbereich*. Der Gruppentyp definiert, wie eine Gruppe in Active Directory verwendet wird.

Windows Server 2012 unterscheidet zwei Gruppentypen:

- **Verteilergruppen** Nicht auf Sicherheit bezogene Gruppen, die für die Informationsverteilung an eine oder mehrere Personen erstellt werden
- **Sicherheitsgruppen** Sicherheitsbezogene Gruppen, die für das Erteilen von Ressourcenzugriffsberichtigungen an mehrere Benutzer erstellt werden

Auf Active Directory ausgerichtete Anwendungen können *Verteilergruppen* für nicht auf Sicherheit bezogene Funktionen einsetzen. Zum Beispiel verwendet Microsoft Exchange

Verteilergruppen, um Nachrichten an mehrere Benutzer zu senden. Nur Anwendungen, die für die Zusammenarbeit mit Active Directory ausgelegt sind, können Verteilergruppen in dieser Weise verwenden.

Gruppen, mit denen Sie Berechtigungen an Ressourcen zuweisen, werden als Sicherheitsgruppen bezeichnet. Administratoren machen mehrere Benutzer, die auf dieselbe Ressource zugreifen müssen, zu Mitgliedern einer Sicherheitsgruppe. Dann erteilen sie der Gruppe die Berechtigung, auf die Ressource zuzugreifen. Nachdem Sie eine Gruppe erstellt haben, können Sie sie jederzeit von einer Sicherheitsgruppe in eine Verteilergruppe konvertieren und umgekehrt.

Gruppenbereiche

Neben den Sicherheits- und Verteilungsgruppentypen sind in Active Directory mehrere Gruppenbereiche verfügbar. Der Gruppenbereich steuert, welche Objekte die Gruppe enthalten kann, wobei die Objekte auf dieselbe Domäne eingeschränkt oder Objekte aus Remote-domänen zugelassen werden. Außerdem bestimmt der Gruppenbereich die Position in der Domäne oder Gesamtstruktur, wo die Gruppe verwendet werden kann. Zu den Gruppenbereichen, die in einer Active Directory-Domäne verfügbar sind, gehören domänenlokale, globale und universale Gruppen.

Domänenlokale Gruppen

Domänenlokale Gruppen können die folgenden Mitglieder enthalten:

- Benutzerkonten
- Computerkonten
- Globale Gruppen aus einer beliebigen Domäne in der Gesamtstruktur
- Universale Gruppen
- Domänenlokale Gruppen aus derselben Domäne

Mithilfe domänenlokaler Gruppen weisen Sie den Ressourcen in derselben Domäne wie die domänenlokale Gruppe Berechtigungen zu. Domänenlokale Gruppen können die Berechtigungszuweisung und Verwaltung vereinfachen.

Globale Gruppen

Globale Gruppen können die folgenden Mitglieder enthalten:

- Benutzerkonten
- Computerkonten
- Andere globale Gruppen aus derselben Domäne

Mit globalen Gruppen können Sie jeder Ressource, die sich in einer beliebigen Domäne in der Gesamtstruktur befindet, Berechtigungen erteilen oder verweigern. Dazu fügen Sie die globale Gruppe als Mitglied einer domänenlokalen Gruppe hinzu, die die gewünschten Berechtigungen besitzt. Globale Gruppenmitgliedschaften werden nur auf Domänencontroller in

derselben Domäne repliziert. Benutzer mit allgemeinen Ressourcenanforderungen sollten Mitglieder einer globalen Gruppe sein, um die Zuweisung von Berechtigungen an Ressourcen zu erleichtern. Die Mitgliedschaft der globalen Gruppe können Sie so häufig wie nötig ändern, um Benutzer mit den erforderlichen Ressourcenberechtigungen zu versehen.

Universale Gruppen

Universale Gruppen können die folgenden Mitglieder enthalten:

- Benutzerkonten
- Computerkonten
- Globale Gruppen aus einer beliebigen Domäne in der Gesamtstruktur
- Andere universale Gruppen

Existiert eine gesamtstrukturübergreifende Vertrauensstellung, können universale Gruppen gleichartige Konten aus einer vertrauenswürdigen Gesamtstruktur enthalten. Universale Gruppen können wie globale Gruppen Benutzer entsprechend ihren Anforderungen an den Ressourcenzugriff organisieren. Mit ihnen können Sie den Zugriff auf Ressourcen realisieren, die sich in einer beliebigen Domäne in der Gesamtstruktur befinden, indem Sie domänenlokale Gruppen verwenden.

Außerdem eignen sich universale Gruppen, um Gruppen und Konten zusammenzufassen, die sich entweder über mehrere Domänen oder über die komplette Gesamtstruktur erstrecken. Ein wichtiger Aspekt bei der Anwendung und Auslastung von universalen Gruppen ist, dass sich Gruppenmitgliedschaften in universellen Gruppen nicht häufig ändern sollten, da universale Gruppen im globalen Katalog gespeichert werden. Änderungen an Mitgliedslisten von universalen Gruppen werden auf alle globalen Katalogserver überall in der Gesamtstruktur repliziert. Treten diese Änderungen häufig auf, kann der Replikationsprozess beträchtliche Bandbreite verbrauchen, was insbesondere für relativ langsame und teure WAN-Verbindungen gilt.

Gruppen verschachteln

Wie bereits weiter oben erwähnt, spricht man von Gruppenverschachtelung, wenn Gruppen als Mitglieder zu anderen Gruppen hinzugefügt werden. Wenn Sie zum Beispiel eine globale Gruppe zu einem Mitglied einer universalen Gruppe machen, sagt man, dass die globale Gruppe in der universalen Gruppe verschachtelt ist.

Gruppenverschachtelung verringert die Anzahl der erforderlichen Berechtigungszuweisungen an Benutzer in verschiedenen Domänen in einer Gesamtstruktur mit mehreren Domänen.

Wenn zum Beispiel Ihre AD DS-Hierarchie mehrere untergeordnete Domänen besitzt und die Benutzer in jeder Domäne auf eine Unternehmensdatenbankanwendung in der übergeordneten Domäne zugreifen müssen, lässt sich der Zugriff auf diese Anwendung am einfachsten wie folgt einrichten:

1. In jeder Domäne globale Gruppen erstellen mit allen Benutzern, die auf die Unternehmensdatenbank zugreifen müssen.

2. In der übergeordneten Domäne eine universale Gruppe erstellen. Die globale Gruppe jedes Standorts als Mitglied einschließen.
3. Die universale Gruppe zur erforderlichen domänenlokalen Gruppe hinzufügen, um die benötigte Berechtigung für den Zugriff auf die Unternehmensdatenbank zuzuweisen.

Diesen herkömmlichen Ansatz der Gruppenverschachtelung in den AD DS bezeichnet man oftmals auch mit dem Akronym AGUDLP (Account, Global, Universal, Domain Local, Permission – Konto, global, universal, domänenlokal, Berechtigung), d.h., man fügt Konten zu globalen Gruppen hinzu, fügt diese globalen Gruppen in universale Gruppen ein, fügt universale Gruppen in lokale Gruppen ein und weist schließlich den domänenlokalen Gruppen Berechtigungen zu.

Die gleiche Strategie können Sie auf Ihr Verwaltungsmodell anwenden. Zum Beispiel sehen Sie im Container *Builtin*, wie die standardmäßigen domänenlokalen Gruppen auf Verwaltungsaufgaben aufgebaut sind.

Administratoren können mit der gleichen Methode ihre eigenen domänenlokalen Gruppen erstellen, an die sie Verwaltungsaufgaben und Benutzerrechte für bestimmte Organisationseinheiten delegieren. Sind die globalen Gruppen (oder die universalen Gruppen für gesamtstrukturweite Zuweisungen) eingerichtet und in die domänenlokalen Gruppen eingefügt, ist die Struktur einsatzbereit.

Gruppen erstellen

Im *Active Directory-Verwaltungscenter* oder in der Konsole *Active Directory-Benutzer und -Computer* erstellen Sie Gruppen fast genauso, wie Sie es von Organisationseinheiten kennen. Wenn Sie eine Gruppe anlegen, geben Sie einen Namen für das Gruppenobjekt an. Der gewählte Name darf eine Länge von 64 Zeichen haben und muss in der Domäne eindeutig sein. Außerdem wählen Sie einen Gruppentyp und einen Gruppenbereich aus. Abbildung 5.22 zeigt das Fenster *Gruppe erstellen* im *Active Directory-Verwaltungscenter*.

Das Dialogfeld *Neues Objekt – Gruppe* in *Active Directory-Benutzer und -Computer* sieht etwas anders aus, enthält aber die gleichen grundlegenden Steuerelemente.

Obwohl die grafischen AD DS-Dienstprogramme zweckmäßig sind, um Gruppen einzeln zu erstellen und zu verwalten, stellen sie nicht die effizienteste Methode dar, um eine größere Anzahl von Sicherheitsprinzipalen einzurichten. Mit den Befehlszeilentools von Windows Server 2012 können Sie über Batchdateien oder andere Arten von Skripts Gruppen in großer Anzahl erstellen und verwalten. Die folgenden Abschnitte gehen auf einige dieser Tools näher ein.

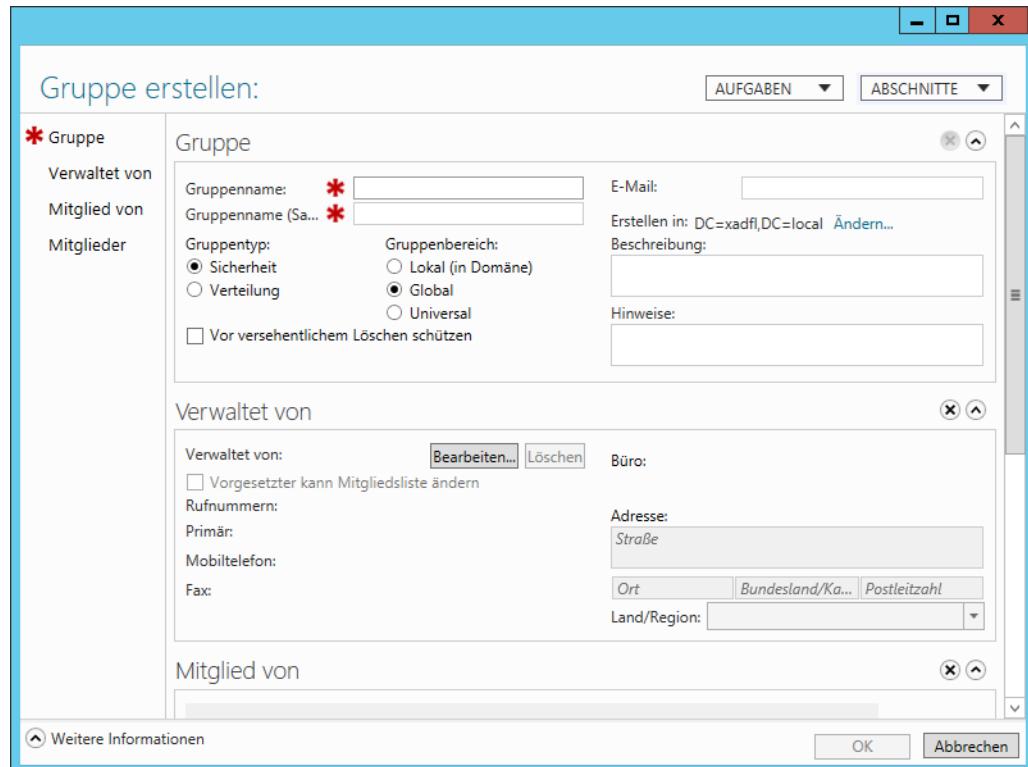


Abbildung 5.22 Im Active Directory-Verwaltungszentrum eine Gruppe erstellen

Gruppen von der Befehlszeile aus erstellen

Das Programm *Dsadd.exe* eignet sich nicht nur, um neue Benutzerobjekte zu erstellen, sondern auch, um Gruppenobjekte einzurichten. Die grundlegende Syntax für das Erstellen von Gruppenobjekten mit *Dsadd.exe* sieht folgendermaßen aus:

```
dsadd group <GroupDN> [Parameter]
```

Der Parameter *<GroupDN>* ist ein definierter Name (DN) für das neu anzulegende Gruppenobjekt. Für die definierten Namen gilt das gleiche Format wie in CSV-Dateien.

Zwar erstellt *Dsadd.exe* standardmäßig globale Sicherheitsgruppen, doch lassen sich Befehlszeilenparameter angeben, um Gruppen mit anderen Typen und Bereichen zu erstellen sowie Mitglieder und Mitgliedschaften für die Gruppen und andere Gruppenobjekteigenschaften anzugeben. Am gebräuchlichsten sind die folgenden Befehlszeilenparameter:

- **-secgrp yes | no** Gibt an, ob das Programm eine Sicherheitsgruppe (yes) oder eine Verteilergruppe (no) erstellen soll. Der Standardwert ist yes.
- **-scope 1 | g | u** Gibt an, ob das Programm eine domänenlokale (1), globale (g) oder universale (u) Gruppe erstellen soll. Der Standardwert ist g.

- **-samid <SAM-Name>** Gibt den SAM-Namen für das Gruppenobjekt an
- **-desc <Beschreibung>** Gibt eine Beschreibung für das Gruppenobjekt an
- **-memberof <Gruppe ...>** Gibt die definierten Namen einer oder mehrerer Gruppen an, in denen die neue Gruppe Mitglied sein soll
- **-members <Mitglied ...>** Gibt die definierten Namen eines oder mehrerer Objekte an, die Mitglieder der neuen Gruppe sein sollen

Zum Beispiel erstellen Sie mit dem folgenden Befehl eine neue Gruppe *Vertrieb* im Container *Users* und legen den Benutzer *Administrator* als Mitglied fest:

```
dsadd group "CN=Vertrieb,CN=Users,DC=adatum,DC=com" -member "CN=Administrator,CN=Users,DC=a datum,DC=com"
```

Um per Windows PowerShell ein neues Gruppenobjekt zu erstellen, verwenden Sie das Cmdlet *New-ADGroup* mit der folgenden Syntax:

```
New-ADGroup  
-Name <Gruppenname>  
-SamAccountName <SAM-Name>  
-GroupCategory <Distribution | Security>  
-GroupScope <DomainLocal | Global | Universal>  
-Path <definierter Name>
```

Zum Beispiel erstellen Sie mit dem folgenden Befehl eine globale Sicherheitsgruppe *Vertrieb* in der Organisationseinheit *Chicago*:

```
New-ADGroup -Name Vertrieb -SamAccountName Vertrieb  
-GroupCategory Security -GroupScope Global  
-Path "OU=Chicago,DC=Adatum,DC=Com"
```

Gruppenmitgliedschaften verwalten

Während Sie im *Active Directory-Verwaltungszentrum* die Mitglieder einer Gruppe bereits angeben können, wenn Sie die Gruppe erstellen, müssen Sie in der Konsole *Active Directory-Benutzer und -Computer* zuerst das Gruppenobjekt erstellen und ihm dann die Mitglieder hinzufügen.

Die einer Gruppe hinzuzufügenden Mitglieder markieren Sie in der Konsole, öffnen dann über *Aktion / Eigenschaften* das Eigenschaftenblatt der Gruppe und gehen zur Registerkarte *Mitglieder*.

Auf der Registerkarte *Mitglieder* können Sie der Mitgliedsliste der Gruppe Objekte hinzufügen und auf der Registerkarte *Mitglied von* die Gruppe in die Mitgliedsliste einer anderen Gruppe aufnehmen. Bei beiden Aufgaben wählen Sie die Objekte im Standarddialogfeld *Benutzer, Kontakte, Computer, Dienstkonten oder Gruppen auswählen* aus.

Nachdem Sie die gewünschten Objekte eingegeben oder gesucht haben, klicken Sie auf *OK*, um das Eigenschaftenblatt zu schließen und die Objekte in die Mitgliedsliste der Gruppe hinzuzufügen.

Gruppenmitgliedschaft per Gruppenrichtlinie verwalten

Die Gruppenmitgliedschaften lassen sich auch mit Gruppenrichtlinien steuern. Wenn Sie eine Richtlinie *Eingeschränkte Gruppen* erstellen, können Sie die Mitgliedschaft für eine Gruppe angeben und erzwingen, sodass niemand Mitglieder hinzufügen oder entfernen kann.

Um eine Richtlinie *Eingeschränkte Gruppen* zu erstellen, gehen Sie folgendermaßen vor:

1. Melden Sie sich beim Windows Server 2012-Server unter einem Konto mit Administratorenrechten an. Das Fenster *Server-Manager* wird geöffnet.
2. Öffnen Sie die Konsole *Gruppenrichtlinienverwaltung*. Erstellen Sie ein neues Gruppenrichtlinienobjekt und verknüpfen Sie es mit Ihrer Domäne.
3. Öffnen Sie das Gruppenrichtlinienobjekt im Gruppenrichtlinienverwaltungs-Editor und gehen Sie zum Ordner *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Eingeschränkte Gruppen* (siehe Abbildung 5.23).

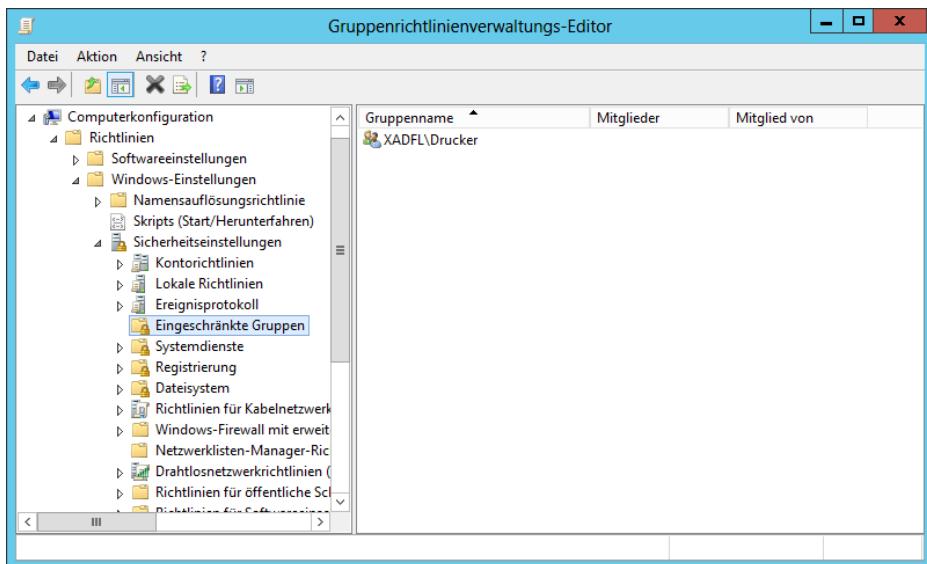


Abbildung 5.23 Der Ordner *Eingeschränkte Gruppen* im Gruppenrichtlinienobjekt

4. Klicken Sie mit der rechten Maustaste auf den Ordner *Eingeschränkte Gruppen* und wählen Sie im Kontextmenü *Gruppe hinzufügen*, um das Dialogfeld *Gruppe hinzufügen* zu öffnen.
5. Geben Sie das hinzuzufügende Gruppenobjekt ein (oder suchen Sie es) und klicken Sie auf *OK*. Die Gruppe erscheint im Ordner *Eingeschränkte Gruppen* und für die Richtlinie wird ein Eigenschaftenblatt geöffnet (siehe Abbildung 5.24).

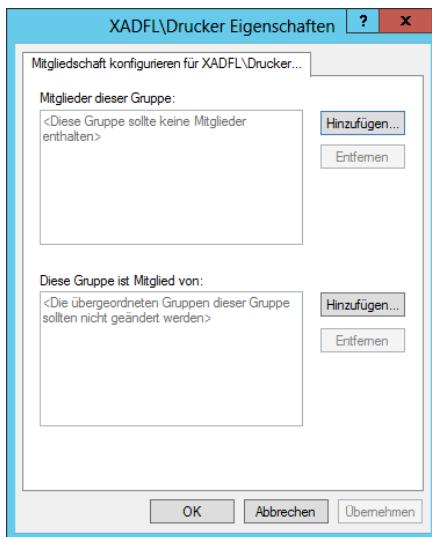


Abbildung 5.24 Das Eigenschaftenblatt für eine Richtlinie *Eingeschränkte Gruppen*

6. Klicken Sie auf eine oder beide *Hinzufügen*-Schaltflächen, um Objekte als Mitglieder der Gruppe oder anderer Gruppen, zu der die Gruppe gehören soll, hinzuzufügen.
7. Klicken Sie auf *OK*.
8. Schließen Sie die Konsolen *Gruppenrichtlinienverwaltungs-Editor* und *Gruppenrichtlinienverwaltung*.

Die Mitglieder, die Sie mit einer Richtlinie *Eingeschränkte Gruppen* für eine Gruppe festgelegt haben, sind nun die einzigen Mitglieder, die in dieser Gruppe verbleiben dürfen. Zwar hindert die Richtlinie Administratoren nicht daran, die Gruppenmitgliedschaft mit anderen Tools zu modifizieren, doch wird die Gruppenmitgliedsliste durch die Richtlinie überschrieben, sobald das System seine Gruppenrichtlinieneinstellungen aktualisiert.

Gruppenobjekte mit Dsmod.exe verwalten

Mit dem Programm *Dsmod.exe* lassen sich die Eigenschaften vorhandener Gruppenobjekte von der Windows Server 2012-Eingabeaufforderung aus ändern. Das Programm erlaubt es unter anderem, Mitglieder zu einer Gruppe hinzuzufügen und daraus zu entfernen sowie Typ und Bereich der Gruppe zu ändern. Die grundlegende Syntax für *Dsmod.exe* lautet:

```
dsmod group <Gruppen-DN> [Parameter]
```

Die gebräuchlichsten Befehlszeilenparameter für *Dsmod.exe* sind:

- **-secgrp yes | no** Setzt den Gruppentyp auf Sicherheitsgruppe (yes) oder Verteilergruppe (no)
- **-scope l | g | u** Setzt den Gruppenbereich auf domänenlokal (l), global (g) oder universal (u)

- **-addmbr <Mitglied ...>**: Fügt der Gruppe Mitglieder hin. Ersetzen Sie <Mitglied ...> durch die definierten Namen eines oder mehrerer Objekte.
- **-rmmbr <Mitglied ...>** Entfernt Mitglieder aus der Gruppe. Ersetzen Sie <Mitglied ...> durch die definierten Namen eines oder mehrerer Objekte.
- **-chmbr <Mitglied ...>** Ändert (ersetzt) die gesamte Liste von Gruppenmitgliedern. Ersetzen Sie <Mitglied ...> durch die definierten Namen eines oder mehrerer Objekte.

Zum Beispiel fügen Sie mit dem folgenden Befehl den Benutzer *Administrator* der Gruppe *Guests* hinzu:

```
dsmod group "CN=Guests,CN=BuiltIn,DC=adatum,DC=com" -addmbr "CN=Administrator,CN=Users,D C=adatum,DC=com"
```

Gruppen konvertieren

Wenn sich Gruppenfunktionen ändern, müssen Sie gegebenenfalls den Typ eines Gruppenobjekts ändern. Öffnen Sie dazu das Eigenschaftenblatt der Gruppe in der Konsole *Active Directory-Verwaltungscenter* oder *Active Directory-Benutzer und -Computer*. Modifizieren Sie auf der Registerkarte *Allgemein* die Option *Gruppentyp* und klicken Sie dann auf *OK*.

Den Bereich der Gruppe ändern Sie in der gleichen Weise, außer dass Sie auf der Registerkarte *Allgemein* eine der Gruppenbereichsoptionen auswählen. Mit den AD DS-Dienstprogrammen können Sie nur zulässige Bereichsänderungen durchführen, wie sie in Tabelle 5.1 aufgeführt sind.

Tabelle 5.1 Einschränkungen bei der Konvertierung von Active Directory-Gruppenbereichen

	In domänenlokale	In global	In universal
Von domänenlokal	Nicht zutreffend	Unzulässig	Nur zulässig, wenn die domänenlokale Gruppe keine anderen domänenlokalen Gruppen als Mitglieder enthält
Von global	Unzulässig	Nicht zutreffend	Nur zulässig, wenn die globale Gruppe kein Mitglied einer anderen globalen Gruppe ist
Von universal	Keine Einschränkungen	Nur zulässig, wenn die universale Gruppe keine anderen universalen Gruppen als Mitglieder enthält	Nicht zutreffend

Eine Gruppe löschen

Wie bei Benutzeroberjekten besitzt jede Gruppe, die Sie in den AD DS erstellen, eine eindeutige und nicht wieder verwendbare SID. Windows Server 2012 identifiziert anhand der SID die Gruppe und die ihr zugewiesenen Berechtigungen.

Wenn Sie eine Gruppe löschen, verwendet Windows Server 2012 dieselbe SID für diese Gruppe nicht noch einmal, selbst wenn Sie eine neue Gruppe mit demselben Namen wie die gelöschte Gruppe erstellen. Demzufolge können Sie Zugriffsberechtigungen, die Sie Ressourcen zugewiesen haben, nicht erneut zuweisen, indem Sie ein gelöschtes Gruppenobjekt wiederherstellen. Stattdessen müssen Sie die wiederhergestellte Gruppe als Sicherheitsprinzipal in die Zugriffssteuerungsliste (ACL, Access Control List) erneut eintragen.

Beim Löschen einer Gruppe löschen Sie nur das Gruppenobjekt sowie die Berechtigungen und die Rechte, die diese Gruppe als den Sicherheitsprinzipal spezifizieren. Die Objekte, die Mitglieder der Gruppe sind, werden nicht gelöscht.

Prüfungszielzusammenfassung

- Nachdem Sie ein Konzept für Ihre Active Directory-Domänen sowie die Strukturen und Gesamtstrukturen, die darüber liegen, erstellt haben, sollten Sie sich mit der Hierarchie befassen, die Sie in jeder Domäne einrichten wollen
- Organisationseinheiten lassen sich in eine Active Directory-Hierarchie einfacher einfügen als Domänen; es ist keine zusätzliche Hardware erforderlich und Sie können eine Organisationseinheit bei Bedarf leicht verschieben oder löschen
- Möchten Sie mehreren Benutzern die Berechtigung für den Zugriff auf eine Netzwerkressource wie zum Beispiel eine Freigabe im Dateisystem oder einen Drucker erteilen, müssen Sie eine Sicherheitsgruppe verwenden. Einer Organisationseinheit lassen sich keine Berechtigungen zuweisen. Obwohl es sich bei Gruppen um Containerobjekte handelt, sind sie nicht in der gleichen Weise wie Domänen und Organisationseinheiten Bestandteil der Active Directory-Hierarchie.
- Organisationseinheiten stellen den einfachsten Objekttyp dar, der sich in der AD DS-Hierarchie erstellen lässt. Hierfür müssen Sie lediglich einen Namen für das Objekt angeben und seine Position in der Active Directory-Struktur definieren.
- Mithilfe von Organisationseinheiten lässt sich ein dezentralisiertes Verwaltungsmodell implementieren, in dem andere Administratoren Teile der AD DS-Hierarchie verwalten, ohne die übrige Struktur zu beeinflussen
- Mithilfe von Gruppen lassen sich Berechtigungen an mehrere Benutzer gleichzeitig zuweisen. Eine Gruppe kann man als Sammlung von Benutzer- oder Computerkonten definieren, die als Sicherheitsprinzipal fungieren, was weitgehend der Funktion eines Benutzers ähnelt.
- In Active Directory gibt es zwei Gruppentypen: Sicherheits- und Verteilergruppen. Außerdem werden drei Gruppenbereiche unterschieden: domänenlokal, global und universal.
- Von Gruppenverschachtelung spricht man, wenn Gruppen als Mitglieder zu anderen Gruppen hinzugefügt werden
- Gruppenmitgliedschaften lassen sich mit Gruppenrichtlinien steuern. Wenn Sie eine Richtlinie *Eingeschränkte Gruppen* erstellen, können Sie die Mitgliedschaft für eine Gruppe angeben und erzwingen, sodass niemand Mitglieder hinzufügen oder entfernen kann.

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Gruppen verwenden Sie, um Gruppen und Konten zusammenzufassen, die sich entweder über mehrere Domänen oder über die komplette Gesamtstruktur erstrecken?
 - A. Global
 - B. Domänenlokal
 - C. Integriert
 - D. Universal
2. Welche der folgenden Begründungen ist für das Erstellen einer Organisationseinheit kein korrekter Grund?
 - A. Um einen permanenten Container zu erstellen, der sich weder verschieben noch umbenennen lässt.
 - B. Um die Abteilungen in Ihrer Organisation nachzubilden.
 - C. Um Verwaltungsaufgaben zu delegieren.
 - D. Um verschiedene Gruppenrichtlinieneinstellungen an eine bestimmte Gruppe von Benutzern oder Computern zuzuweisen.
3. Welche der folgenden Gruppenbereichsänderungen sind niemals zulässig? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Global zu universal
 - B. Global zu domänenlokal
 - C. Universal zu global
 - D. Domänenlokal zu universal
4. Welche der folgenden Sicherheitsprinzipale können in einer Domäne, die auf der Windows Server 2012-Domänenfunktionsebene läuft, Mitglieder einer globalen Gruppe sein? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Benutzer
 - B. Computer
 - C. Universale Gruppen
 - D. Globale Gruppen

5. In der Konsole *Active Directory-Benutzer und -Computer* möchten Sie eine globale Sicherheitsgruppe löschen, doch die Konsole lässt Sie die Aufgabe nicht fertig stellen. Welche der folgenden Ursachen kommen möglicherweise für das Scheitern infrage? (Wählen Sie alle zutreffenden Antworten aus.)
- A. Die Gruppe enthält immer noch Mitglieder.
 - B. Ein Mitglied der Gruppe hat die Gruppe als seine primäre Gruppe festgelegt.
 - C. Sie besitzen nicht die geeigneten Berechtigungen für den Container, in dem sich die Gruppe befindet.
 - D. Von der Konsole *Active Directory-Benutzer und -Computer* können Sie globale Gruppen nicht löschen.

Antworten

Dieser Abschnitt enthält die Lösungen für die Gedankenspiele und Antworten auf die Fragen der Lernzielkontrollen in diesem Kapitel.

Prüfungsziel 5.1: Kontrolle

1. **Richtige Antwort:** A
 - A. **Richtig:** In den AD DS können Sie eine Domäne in Organisationseinheiten untergliedern und mit Objekten füllen, jedoch keine Domänen innerhalb von Organisationseinheiten erstellen.
 - B. **Falsch:** Ein Standort kann mehrere Domänen enthalten.
 - C. **Falsch:** Eine Struktur kann mehrere Domänen enthalten.
 - D. **Falsch:** Eine Gesamtstruktur kann mehrere Domänen enthalten.
2. **Richtige Antworten:** B, D
 - A. **Falsch:** Es gibt keine Objektklasse namens *Ressource*.
 - B. **Richtig:** Es gibt zwei Basisklassen von Objekten: Containerobjekte und Endknotenobjekte. Ein Endknotenobjekt kann keine untergeordneten Objekte enthalten.
 - C. **Falsch:** Eine Domäne ist ein spezifischer Objekttyp und keine allgemeine Klassifizierung.
 - D. **Richtig:** Es gibt zwei Basisklassen von Objekten: Containerobjekte und Endknotenobjekte. Ein Containerobjekt kann andere, untergeordnete Objekte enthalten.
3. **Richtige Antworten:** A, B, C
 - A. **Richtig:** Manche Attribute werden automatisch erstellt, für andere Attribute muss der Administrator die Informationen manuell angeben.

- B. **Richtig:** Ein Containerobjekt besitzt als eines seiner Attribute eine Liste aller anderen Objekte, die es enthält.
- C. **Richtig:** Endknotenobjekte besitzen Attribute, die Informationen über die jeweilige Ressource enthalten, die das Objekt darstellt.
- D. **Falsch:** Manche Attribute werden automatisch erstellt. Ein Beispiel hierfür ist der global eindeutige Bezeichner (GUID), den der Domänencontroller jedem Objekt zuweist, wenn er es erstellt.
4. **Richtige Antwort:** D
- A. **Falsch:** Jede Domäne in einer Active Directory-Installation ist eine separate Verwaltungseinheit. Je mehr Domänen Sie erstellen, desto größer ist die Anzahl der anfallenden Verwaltungsaufgaben, die Sie durchführen müssen.
- B. **Falsch:** Jede Domäne benötigt ihre eigenen Domänencontroller, sodass jede zusätzliche Domäne, die Sie anlegen, die Gesamtkosten für Hardware und Wartung der Bereitstellung erhöht.
- C. **Falsch:** In einer Gesamtstruktur mit mehreren Domänen könnten Anwendungen möglicherweise nicht ordnungsgemäß ausgeführt werden.
- D. **Richtig:** Für Domänen sind keine gesonderten Microsoft-Lizenzen erforderlich.
5. **Richtige Antwort:** B
- A. **Falsch:** DNS wird für Suchen in einer Domäne verwendet.
- B. **Richtig:** Um ein Objekt in einer anderen Domäne zu finden, suchen Active Directory-Clients zuerst im globalen Katalog. Diese Suche liefert dem Client die benötigten Informationen, um nach dem Objekt in der jeweiligen Domäne zu suchen, die es enthält.
- C. **Falsch:** DHCP bietet keine Suchfunktionen.
- D. **Falsch:** Standortverknüpfungsobjekte bieten keine Suchfunktionen.

Prüfungsziel 5.1: Gedankenspiel

Robert sollte Active Directory auf einem Domänencontroller im New Yorker Stammsitz installieren und dabei eine Gesamtstruktur-Stammdomäne namens *hq.inside.litware.com* erstellen. Da das Londoner Büro über hervorragende Netzwerkverbindungen verfügt, jedoch keine eigenen IT-Mitarbeiter hat, kann er dort einen schreibgeschützten Domänencontroller für die Domäne *hq.inside.litware.com* installieren, sodass sich die Londoner Benutzer über einen lokalen Domänencontroller authentifizieren können. Für das Büro in Tokio, das über schlechtere Netzwerkverbindungen verfügt und eigene IT-Mitarbeiter beschäftigt, sollte das Konzept zwei Domänencontroller vorsehen, die eine separate Domäne namens *tokyo.inside.litware.com* in derselben Gesamtstruktur hosten. Die Benutzer in Tokio erhalten dadurch Zugriff auf einen lokalen Domänencontroller und es verringert sich der Replikationsdatenverkehr, der über die Einwahlverbindung zwischen den Büros in New York und Tokio läuft.

Prüfungsziel 5.2: Kontrolle

1. **Richtige Antwort:** B
 - A. **Falsch:** Das in Windows Server 2012 verworfene Tool *Dcpromo* dient dazu, Active Directory-Domänencontroller herauf- und herabzustufen.
 - B. **Richtig:** Wie *CSVDE.exe* lässt sich das LDAP Data Interchange Format Directory Exchange (*LDIFDE.exe*)-Dienstprogramm verwenden, um Active Directory-Daten zu importieren oder zu exportieren. Außerdem eignet es sich, um Objekte in Active Directory hinzuzufügen, zu löschen oder zu modifizieren. Bei Bedarf kann auch das Schema modifiziert werden.
 - C. **Falsch:** *CSVDE.exe* kann Active Directory-Objekte aus Informationen in CSV-Dateien erstellen, vorhandene Objekte jedoch nicht modifizieren.
 - D. **Falsch:** NSLOOKUP ist ein Dienstprogramm für die DNS-Namensauflösung. Es kann keine AD DS-Objekte erstellen.
2. **Richtige Antwort:** B
 - A. **Falsch:** Die erste Zeile der CSV-Datei ist der Kopfeintrag und nicht die Kopfzeile.
 - B. **Richtig:** Mit dem Befehlszeilendienstprogramm CSVDE kann ein Administrator AD DS-Objekte importieren oder exportieren. Das Programm verwendet eine CSV-Datei basierend auf einem Kopfeintrag, der jeden Teil der Daten beschreibt. Ein Kopfeintrag ist lediglich die erste Textzeile, die geeignete Attributnamen verwendet.
 - C. **Falsch:** Die erste Zeile der CSV-Datei ist der Kopfeintrag, nicht die Namenszeile.
 - D. **Falsch:** Die erste Zeile der CSV-Datei ist der Kopfeintrag, nicht der Namenseintrag.
3. **Richtige Antwort:** C
 - A. **Falsch:** Mit dem Befehl *net join* können Sie keinen Offline-Domänenbeitritt durchführen.
 - B. **Falsch:** Mit dem Befehl *join* können Sie keinen Offline-Domänenbeitritt durchführen.
 - C. **Richtig:** Auf einem Windows Server 2012-Computer können Sie mit dem Dienstprogramm *Djoin.exe* einen Offline-Domänenbeitritt durchführen.
 - D. **Falsch:** Mit dem Befehl *dconnect* können Sie keinen Offline-Domänenbeitritt durchführen.
4. **Richtige Antwort:** C
 - A. **Falsch:** In Windows Server 2012 können lokale Konten erstellt und konfiguriert werden.
 - B. **Falsch:** In Windows Server 2012 können Domänenkonten erstellt und konfiguriert werden.
 - C. **Richtig:** In Windows Server 2012 können drei Typen von Benutzerkonten erstellt und konfiguriert werden: lokale Konten, Domänenkonten und integrierte Benutzerkonten.

D. **Falsch:** In Windows Server 2012 können integrierte Konten erstellt und konfiguriert werden.

5. **Richtige Antworten:** C, D

A. **Falsch:** In Windows Server 2012 gibt es kein Konto *Netzwerk*.

B. **Falsch:** In Windows Server 2012 gibt es kein Konto *Interaktiv*.

C. **Richtig:** Die beiden auf einem Windows Server 2012-Computer standardmäßig erstellten integrierten Benutzerkonten sind das Administratorkonto und das Gastkonto.

D. **Richtig:** Die beiden auf einem Windows Server 2012-Computer standardmäßig erstellten integrierten Benutzerkonten sind das Administratorkonto und das Gastkonto.

Prüfungsziel 5.2: Gedankenspiel

Richtige Antwort: D. Antwort A ist falsch, weil der Befehl `user` fehlt und weil der Name des Benutzers nicht im Format eines definierten Namens (DN) ausgedrückt wird. Antwort B ist falsch, da die Werte der Befehlszeilenvariablen, die Leerzeichen enthalten, nicht in Anführungszeichen eingeschlossen sind. Antwort C ist falsch, da der Befehl `user` fehlt und da die Parameter `-company` und `-dept` vor dem definierten Namen erscheinen.

Prüfungsziel 5.3: Kontrolle

1. **Richtige Antwort:** D

A. **Falsch:** Globale Gruppen dürfen keine Benutzer aus anderen Domänen enthalten.

B. **Falsch:** Domänenlokale Gruppen können keine Berechtigungen für Ressourcen in anderen Domänen haben.

C. **Falsch:** Integrierte Gruppen besitzen keine inhärenten domänenübergreifenden Eigenschaften.

D. **Richtig:** Universale Gruppen werden wie lokale Gruppen eingesetzt, um Benutzer entsprechend ihren Anforderungen auf Ressourcenzugriffe zu organisieren. Mithilfe von domänenlokalen Gruppen können Sie diese Gruppen verwenden, um den Zugriff auf Ressourcen zu ermöglichen, die sich in beliebigen Domänen in der Gesamtstruktur befinden. Universale Gruppen eignen sich auch, um Gruppen und Konten zusammenzufassen, die sich entweder über mehrere Domänen oder über die komplette Gesamtstruktur erstrecken.

2. **Richtige Antwort:** A

A. **Richtig:** Organisationseinheiten werden unter anderem erstellt, um die organisatorische Gliederung nachzubilden, Gruppenrichtlinieneinstellungen zuzuweisen und die Verwaltung zu delegieren. Falls erforderlich, können Sie eine Organisationseinheit ganz einfach verschieben oder umbenennen.

- B. **Falsch:** Das Nachbilden der organisatorischen Gliederung ist ein triftiger Grund, um eine Organisationseinheit zu erstellen.
- C. **Falsch:** Das Delegieren von Verwaltungsaufgaben ist ein triftiger Grund, um eine Organisationseinheit zu erstellen.
- D. **Falsch:** Das Zuweisen von Gruppenrichtlinieneinstellungen ist ein triftiger Grund, um eine Organisationseinheit zu erstellen.
3. **Richtige Antwort:** B
- A. **Falsch:** Umwandlungen von globalen zu universalen Gruppen sind manchmal zulässig.
- B. **Richtig:** Umwandlungen von globalen zu domänenlokalen Gruppen sind niemals zulässig.
- C. **Falsch:** Umwandlungen von universalen zu globalen Gruppen sind manchmal zulässig.
- D. **Falsch:** Umwandlungen von domänenlokalen zu universalen Gruppen sind manchmal zulässig.
4. **Richtige Antworten:** A, B, D
- A. **Richtig:** Benutzer können Sicherheitsprinzipale in einer globalen Gruppe sein.
- B. **Richtig:** Computer können Sicherheitsprinzipale in einer globalen Gruppe sein.
- C. **Falsch:** Universale Gruppen können keine Sicherheitsprinzipale in einer globalen Gruppe sein.
- D. **Richtig:** Globale Gruppen können Sicherheitsprinzipale in einer globalen Gruppe sein.
5. **Richtige Antworten:** B, C
- A. **Falsch:** Es ist möglich, eine Gruppe zu löschen, die Mitglieder enthält.
- B. **Richtig:** Wenn irgendein Mitglied die Gruppe als seine primäre Gruppe festgelegt hat, erlaubt das System nicht, die Gruppe zu löschen.
- C. **Richtig:** Sie benötigen die geeigneten Active Directory-Berechtigungen für den Container, in dem sich die Gruppe befindet, um sie zu löschen.
- D. **Falsch:** Mit der Konsole *Active Directory-Benutzer und -Computer* ist es möglich, Gruppen zu löschen.

K A P I T E L 6

Gruppenrichtlinien erstellen und verwalten

Mit dem Mechanismus der Gruppenrichtlinien lassen sich Betriebssystemeinstellungen für Computer im gesamten Netzwerk steuern und bereitstellen. Gruppenrichtlinien bestehen aus Benutzer- und Computereinstellungen für die verschiedenen Microsoft Windows-Betriebssysteme, die die Systeme beim Hoch- und Herunterfahren des Computers sowie bei der Benutzeran- und -abmeldung implementieren. Hierfür können Sie ein oder mehrere Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) konfigurieren und sie dann mit konkreten AD DS (Active Directory-Domäendienste)-Objekten verknüpfen. Wenn Sie ein GPO mit einem Containerobjekt verknüpfen, erhalten alle Objekte in diesem Container die Einstellungen, die Sie im GPO konfiguriert haben. Es ist möglich, mehrere GPOs mit einem einzelnen AD DS-Container zu verknüpfen oder ein GPO mit mehreren Containern in der gesamten AD DS-Hierarchie.

Dieses Kapitel behandelt einige der grundlegenden Aufgaben von Administratoren, um Gruppenrichtlinieneinstellungen einzurichten und bereitzustellen.

Prüfungsziele in diesem Kapitel:

- Prüfungsziel 6.1: Gruppenrichtlinienobjekte (GPOs) erstellen 344
- Prüfungsziel 6.2: Sicherheitsrichtlinien konfigurieren. 356
- Prüfungsziel 6.3: Richtlinien für Anwendungseinschränkungen konfigurieren 376
- Prüfungsziel 6.4: Windows-Firewall konfigurieren 389

Prüfungsziel 6.1: Gruppenrichtlinienobjekte (GPOs) erstellen

Obwohl die Bezeichnung Gruppenrichtlinienobjekt impliziert, dass Richtlinien direkt mit Gruppen verknüpft werden, trifft das nicht zu. Gruppenrichtlinien lassen sich mit Standorten, Domänen und Organisationseinheiten (OUs) verknüpfen, um die jeweiligen Einstellungen auf alle Benutzer und Computer in diesen AD DS-Containern anzuwenden. Allerdings erlaubt es eine spezielle Technik namens *Sicherungsfilterung*, GPO-Einstellungen nur auf einen oder mehrere Benutzer oder Gruppen innerhalb eines Containers anzuwenden, indem selektiv die Berechtigung *Gruppenrichtlinie übernehmen* auf einem oder mehreren Benutzern oder Sicherheitsgruppen erteilt wird.

Die verwaltungstechnischen Vorteile von Gruppenrichtlinien sind wahrscheinlich ihr größter Beitrag zur Netzwerkeffizienz. Die Implementierung von Gruppenrichtlinien hilft Administratoren, eine zentralisierte Verwaltung zu erreichen. Unter anderem bieten sich dadurch folgende Vorteile:

- Administratoren haben die Kontrolle über die zentralisierte Konfiguration von Benutzeinstellungen, die Installation von Anwendungen und die Desktopkonfiguration
- Durch eine zentralisierte Verwaltung von Benutzerdateien muss man nicht mehr versuchen, Dateien von einem beschädigten Laufwerk wiederherzustellen. Die eventuellen Aufwendungen dafür entfallen.
- Wegen der schnellen Bereitstellung von neuen Einstellungen über Gruppenrichtlinien sind weniger manuelle Sicherheitsänderungen auf jedem Computer durchzuführen

Dieses Prüfungsziel zeigt, wie Sie

- einen zentralen Speicher konfigurieren
 - Starter-Gruppenrichtlinienobjekte verwalten
 - Verknüpfungen von Gruppenrichtlinienobjekten konfigurieren
 - mehrere lokale Gruppenrichtlinien konfigurieren
 - Sicherungsfilterung konfigurieren
-

Gruppenrichtlinienobjekte

Gruppenrichtlinienobjekte enthalten sämtliche Gruppenrichtlinieneinstellungen, die Administratoren für Benutzer- und Computer an einem Standort, in einer Domäne oder in einer Organisationseinheit bereitstellen wollen. Um ein Gruppenrichtlinienobjekt bereitzustellen, muss ein Administrator es dem Container zuordnen, für den es bereitgestellt wird. Diese Zuordnung wird erreicht, indem das Gruppenrichtlinienobjekt mit dem gewünschten AD DS-Objekt verknüpft wird. Zu den Verwaltungsaufgaben für Gruppenrichtlinien gehört es auch, Gruppenrichtlinienobjekte zu erstellen, ihren Speicherort festzulegen und die AD DS-Verknüpfungen zu verwalten.

Es gibt drei Typen von Gruppenrichtlinienobjekten: lokale, nichtlokale und Starter-Gruppenrichtlinienobjekte.

Lokale Gruppenrichtlinienobjekte

Alle Windows-Betriebssysteme unterstützen lokale Gruppenrichtlinienobjekte und die Windows-Versionen seit Windows Server 2008 R2 und Windows Vista können mehrfache lokale Gruppenrichtlinienobjekte unterstützen. Administratoren haben damit die Möglichkeit, unterschiedliche lokale Gruppenrichtlinienobjekte für Administratoren und spezifische Gruppenrichtlinienobjekteinstellungen für einen oder mehrere lokale Benutzer, die an einer Arbeitsstation konfiguriert sind, einzurichten. Dies ist besonders interessant für Computer an öffentlichen Orten wie zum Beispiel Bibliotheken und Kioske, die nicht Bestandteil einer Active Directory-Infrastruktur sind. Ältere Windows-Releases können nur ein lokales Gruppenrichtlinienobjekt unterstützen und die Einstellungen in diesem lokalen Gruppenrichtlinienobjekt gelten für alle Benutzer, die sich am Computer anmelden.

Lokale Gruppenrichtlinienobjekte enthalten weniger Optionen als Domänen-Gruppenrichtlinienobjekte. Sie unterstützen weder Ordnerumleitung noch Gruppenrichtlinien für die Softwareinstallation. Außerdem sind weniger Sicherheitseinstellungen verfügbar. Wenn ein lokales und ein nichtlokales (Active Directory-basiertes) Gruppenrichtlinienobjekt in Konflikt stehende Einstellungen aufweisen, überschreiben die Einstellungen des nichtlokalen Gruppenrichtlinienobjekts die Einstellungen des lokalen Gruppenrichtlinienobjekts.

Nichtlokale Gruppenrichtlinienobjekte

Nichtlokale Gruppenrichtlinienobjekte werden in AD DS erstellt und mit Standorten, Domänen und Organisationseinheiten verknüpft. Nachdem sie mit einem Container verknüpft sind, werden die Einstellungen im Gruppenrichtlinienobjekt standardmäßig auf alle Benutzer und Computer in diesem Container angewendet.

Starter-Gruppenrichtlinienobjekte

Starter-Gruppenrichtlinienobjekte wurden mit Windows Server 2008 eingeführt. Es handelt sich dabei praktisch um eine Vorlage für das Erstellen von Domänen-Gruppenrichtlinienobjekten basierend auf einer Standardauflistung von Einstellungen. Wenn Sie ein neues Gruppenrichtlinienobjekt aus einem Starter-Gruppenrichtlinienobjekt erstellen, werden alle Richtlinien im Starter-Gruppenrichtlinienobjekt automatisch auf das neue Gruppenrichtlinienobjekt als dessen Standardeinstellungen kopiert

Einen zentralen Speicher konfigurieren

In Windows Server 2008 und Windows Vista hat Microsoft die tokenbasierten administrativen Vorlagendateien (ADM) älterer Versionen von Gruppenrichtlinien durch ein XML-basiertes Format (ADMX) ersetzt. Administrative Vorlagendateien definieren die registrierungsbasierten Einstellungen, die in Gruppenrichtlinienobjekten erscheinen.

Frühere Windows-Versionen haben eine Kopie der ADM-Dateien für jedes von Administratoren erstellte Gruppenrichtlinienobjekt angelegt und sie im SYSVOL-Volume eines

Domänencontrollers gespeichert. Eine große Active Directory-Installation konnte leicht Dutzende von Gruppenrichtlinienobjekten haben und jede Kopie der ADM-Dateien belegte 4 MB Speicherplatz. Das Ergebnis war ein als SYSVOL Bloat (»Aufblähen von SYSVOL«) bezeichneter Zustand, in dem Hunderte von Megabytes redundanter Informationen in SYSVOL-Volumes gespeichert waren, die auf alle Domänencontroller für die Domäne repliziert werden mussten.

Um diesem Problem zu begegnen, können die Gruppenrichtlinientools nun auf die ADMX-Dateien in einem zentralen Speicher zugreifen, d.h. auf eine einzige Kopie der ADMX-Dateien, die auf einem Domänencontroller gespeichert sind. Um einen zentralen Speicher zu verwenden, müssen Sie den entsprechenden Ordner im SYSVOL-Volume eines Domänencontrollers erstellen.

Standardmäßig speichern Tools wie die Konsole *Gruppenrichtlinienverwaltung* die ADMX-Dateien im Ordner `\%systemroot%\PolicyDefinitions`, auf den meisten Computern also in `C:\Windows\PolicyDefinitions`. Um einen zentralen Speicher einzurichten, müssen Sie den gesamten *PolicyDefinitions*-Ordner an denselben Speicherort wie die Gruppenrichtlinienvorlagen kopieren, d.h. `%systemroot%\SYSVOL\sysvol\<Domänenname>\Policies` oder in UNC (Universal Naming Convention)-Notation `\<Domänenname>\SYSVOL\<Domänenname>\Policies`.

Die Konsole Gruppenrichtlinienverwaltung

Die Konsole *Gruppenrichtlinienverwaltung* ist das MMC-Snap-In, mit dem Administratoren Gruppenrichtlinienobjekte erstellen und ihre Bereitstellung in AD DS-Objekten verwalten. Der Gruppenrichtlinienverwaltungs-Editor ist ein eigenes Snap-In, das Gruppenrichtlinienobjekte öffnet und es erlaubt, deren Einstellungen zu modifizieren.

Es gibt verschiedene Möglichkeiten, mit diesen beiden Tools zu arbeiten, abhängig davon, was Sie erreichen möchten. So können Sie ein Gruppenrichtlinienobjekt erstellen und es dann mit einer Domäne, einem Standort oder einer Organisationseinheit verknüpfen, oder Sie erstellen ein Gruppenrichtlinienobjekt und verknüpfen es in einem einzigen Schritt. Windows Server 2012 implementiert die Tools als Feature *Gruppenrichtlinienverwaltung* und installiert sie automatisch mit der *AD DS*-Rolle. Mit dem Assistenten zum Hinzufügen von Rollen und Features, der ebenfalls im Paket *Remoteserver-Verwaltungstools* für Windows-Arbeitsstationen enthalten ist, können Sie das Feature manuell auf einem Server installieren.

Nichtlokale Gruppenrichtlinienobjekte erstellen und verknüpfen

Wenn Sie die standardmäßigen Gruppenrichtlinienobjekte unverändert lassen und eigene benutzerdefinierte Gruppenrichtlinien bereitstellen wollen, erstellen Sie zunächst ein oder mehrere neue Gruppenrichtlinienobjekte und verknüpfen sie mit den geeigneten AD DS-Objekten.

Gehen Sie folgendermaßen vor, um über die Konsole *Gruppenrichtlinienverwaltung* ein neues Gruppenrichtlinienobjekt zu erstellen und es mit einem OU-Objekt in AD DS zu verknüpfen:

1. Melden Sie sich bei einem Windows Server 2012-Domänencontroller unter einem Konto mit Domänenadministratorrechten an. Die Konsole *Server-Manager* wird geöffnet.

2. Öffnen Sie das *Active Directory-Verwaltungscenter* und erstellen Sie in Ihrer Domäne eine Organisationseinheit *Vertrieb*.
3. Wählen Sie im Server-Manager im Menü *Tools* den Befehl *Gruppenrichtlinienverwaltung*. Die Konsole *Gruppenrichtlinienverwaltung* erscheint (siehe Abbildung 6.1).

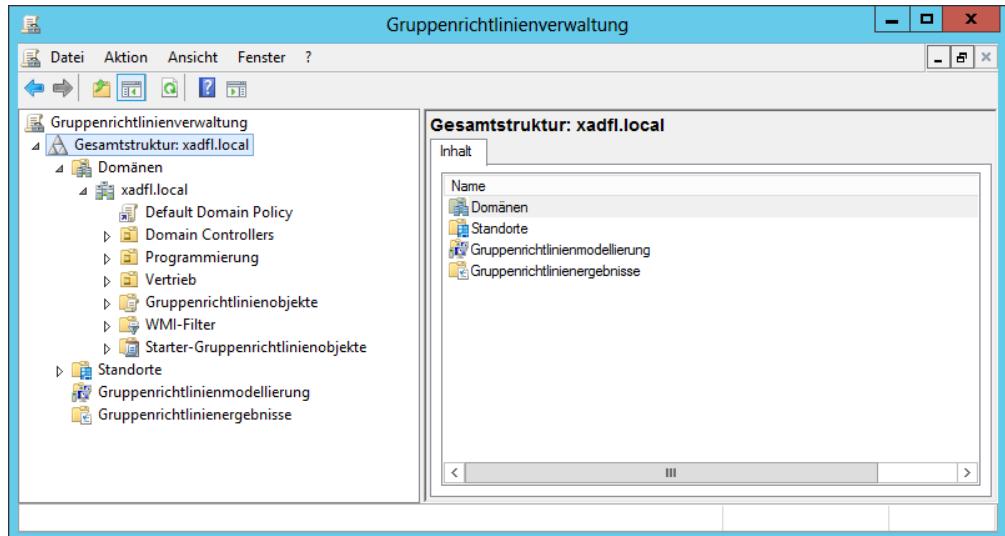


Abbildung 6.1 Die Konsole *Gruppenrichtlinienverwaltung*

4. Erweitern Sie den Gesamtstrukturcontainer und gehen Sie zu Ihrer Domäne. Erweitern Sie dann den Domänencontainer und wählen Sie den Ordner *Gruppenrichtlinienobjekte* aus. Die derzeit in der Domäne vorhandenen Gruppenrichtlinienobjekte erscheinen auf der Registerkarte *Inhalt*.
5. Klicken Sie mit der rechten Maustaste auf den Ordner *Gruppenrichtlinienobjekte* und wählen Sie im Kontextmenü *Neu*. Das Dialogfeld *Neues Gruppenrichtlinienobjekt* erscheint.
6. Geben Sie in das Textfeld *Name* einen Namen für das neue Gruppenrichtlinienobjekt ein und klicken Sie auf *OK*. Das neue Gruppenrichtlinienobjekt erscheint in der Liste *Inhalt*.
7. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf das Domänen-, Standort- oder OU-Objekt, mit dem Sie das neue Gruppenrichtlinienobjekt verknüpfen möchten, und wählen Sie im Kontextmenü *Vorhandenes Gruppenrichtlinienobjekt verknüpfen*. Das Dialogfeld *Gruppenrichtlinienobjekt auswählen* erscheint.
8. Wählen Sie das Gruppenrichtlinienobjekt aus, das Sie mit dem Objekt verknüpfen wollen, und klicken Sie auf *OK*. Das Gruppenrichtlinienobjekt erscheint auf der Registerkarte *Verknüpfte Gruppenrichtlinienobjekte* des Objekts, wie Abbildung 6.2 zeigt.

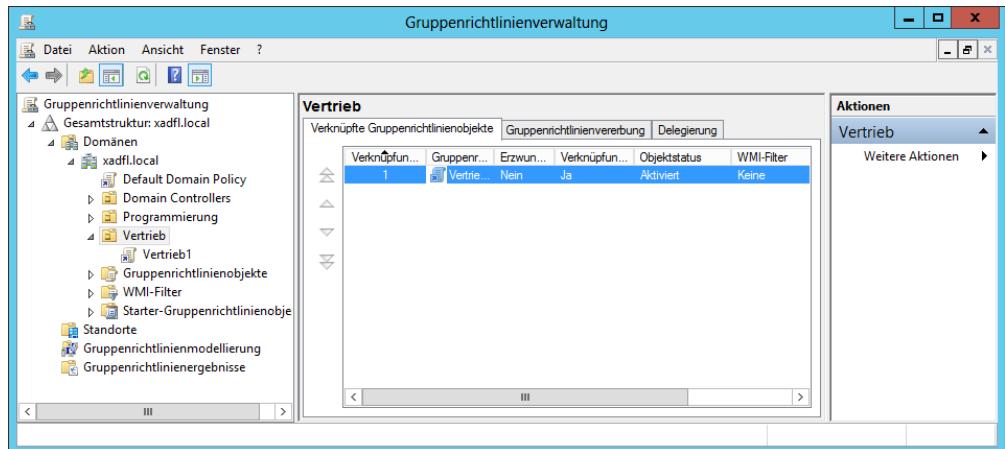


Abbildung 6.2 Die Registerkarte *Verknüpfte Gruppenrichtlinienobjekte*

9. Schließen Sie die Konsole *Gruppenrichtlinienverwaltung*.

Ein Gruppenrichtlinienobjekt können Sie auch in einem einzigen Schritt erstellen und mit einem Active Directory-Container verknüpfen. Klicken Sie dazu mit der rechten Maustaste auf ein Objekt und wählen Sie im Kontextmenü *Gruppenrichtlinienobjekt hier erstellen und verknüpfen*.

Wenn Sie ein Gruppenrichtlinienobjekt mit einem Domänenobjekt verknüpfen, wird es auf alle Benutzer und Computer in der Domäne angewendet. Und wenn Sie ein Gruppenrichtlinienobjekt mit einem Standort verknüpfen, der mehrere Domänen enthält, gelten die Gruppenrichtlinieneinstellungen für alle Domänen und die ihnen untergeordneten Objekte. Dieser Vorgang wird als *Vererbung von Gruppenrichtlinienobjekten* bezeichnet.

Sicherheitsfilterung verwenden

Beim Verknüpfen eines Gruppenrichtlinienobjekts mit einem Container erhalten standardmäßig alle Benutzer und Computer in diesem Container die Gruppenrichtlinienobjekteinstellungen. Das hängt damit zusammen, dass das Erstellen der Verknüpfung die Berechtigungen *Gruppenrichtlinie lesen* und *Gruppenrichtlinie übernehmen* für das Gruppenrichtlinienobjekt den Benutzern und Computern im Container erteilt.

Genauer gesagt erteilt das System die Berechtigungen der speziellen Identität *Authentifizierte Benutzer*, die sämtliche Benutzer und Computer im Container umfasst. Mit der sogenannten *Sicherheitsfilterung* lassen sich aber die standardmäßigen Berechtigungszuweisungen modifizieren, sodass nur bestimmte Benutzer und Computer die Berechtigungen und folglich die Einstellungen im Gruppenrichtlinienobjekt erhalten.

Um die Standardkonfiguration der Sicherheitsfilterung für ein Gruppenrichtlinienobjekt zu modifizieren, wählen Sie es im linken Fensterbereich der Konsole *Gruppenrichtlinienverwaltung* aus, wie Abbildung 6.3 zeigt. Im Bereich *Sicherheitsfilterung* können Sie über die Schaltflächen *Hinzufügen* und *Entfernen* die spezielle Identität *Authentifizierte Benutzer* durch

bestimmte Benutzer, Computer oder Gruppenobjekte ersetzen. Von den Benutzern und Computern im Container, mit dem das Gruppenrichtlinienobjekt verknüpft ist, erhalten nur diejenigen die Einstellungen vom Gruppenrichtlinienobjekt, die Sie im Bereich *Sicherheitsfilterung* ausgewählt haben.

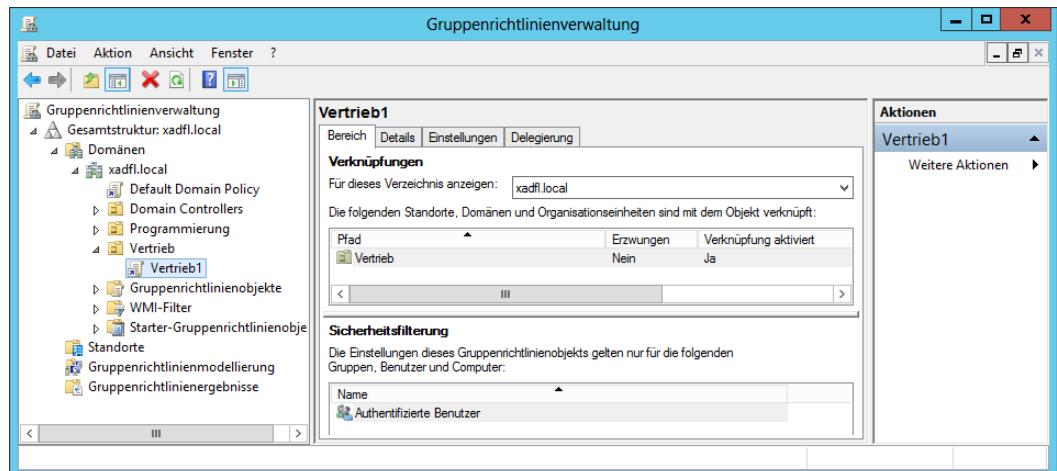


Abbildung 6.3 Sicherheitsfilterung in der Konsole *Gruppenrichtlinienverwaltung*

Starter-Gruppenrichtlinienobjekte verwalten

Starter-Gruppenrichtlinienobjekte sind im Wesentlichen Vorlagen, nach denen Sie mehrere Gruppenrichtlinienobjekte mit demselben Satz an Grundeinstellungen von administrativen Vorlagen erstellen können. Derartige Starter-Gruppenrichtlinienobjekte erstellen und bearbeiten Sie genau wie jedes andere Gruppenrichtlinienobjekt. Klicken Sie in der Konsole *Gruppenrichtlinienverwaltung* mit der rechten Maustaste auf den Ordner *Starter-Gruppenrichtlinienobjekte* und wählen Sie aus dem Kontextmenü *Neu*, um ein leeres Starter-Gruppenrichtlinienobjekt zu erstellen. Dann können Sie das Starter-Gruppenrichtlinienobjekt im Gruppenrichtlinienverwaltungs-Editor öffnen und alle Einstellungen konfigurieren, die Sie neu zu erstellenden Gruppenrichtlinienobjekten übertragen möchten.



Hinweis Starter-Gruppenrichtlinienobjekte

Wenn Sie sich in der Konsole *Gruppenrichtlinienverwaltung* den Knoten *Starter-Gruppenrichtlinienobjekte* erstmals ansehen, erscheint eine Meldung mit der Aufforderung, den Ordner für Starter-Gruppenrichtlinienobjekte zu erstellen, indem Sie auf die entsprechende Schaltfläche klicken.

Aus den fertig bearbeiteten Starter-Gruppenrichtlinienobjekten können Sie neue Gruppenrichtlinienobjekte nach zwei Methoden erstellen: (1.) Sie klicken mit der rechten Maustaste auf ein Starter-Gruppenrichtlinienobjekt und wählen im Kontextmenü *Neues Gruppenrichtlinienobjekt aus Starter-Gruppenrichtlinienobjekt* oder (2.) Sie erstellen ein neues Gruppenrichtlinienobjekt in der üblichen Weise wie weiter vorn beschrieben und wählen das

gewünschte Starter-Gruppenrichtlinienobjekt aus der Dropdownliste *Quell-Starter-Gruppenrichtlinienobjekt* aus. Dabei werden die Einstellungen vom Starter-Gruppenrichtlinienobjekt auf das neue Gruppenrichtlinienobjekt kopiert, das Sie dann weiter bearbeiten können.

Gruppenrichtlinieneinstellungen konfigurieren

Über die Gruppenrichtlinieneinstellungen können Sie die Konfiguration von Desktop, Umgebung und Sicherheitseinstellungen eines Benutzers anpassen. Diese Einstellungen sind in zwei Teilkategorien gegliedert: *Computerkonfiguration* und *Benutzerkonfiguration*. Die Teilkategorien werden als *Gruppenrichtlinienknoten* bezeichnet. Ein Knoten ist einfach eine übergeordnete Struktur, die alle verwandten Einstellungen aufnimmt. Hier ist der Knoten speziell für Computerkonfigurationen und Benutzerkonfigurationen eingerichtet.

Gruppenrichtlinienknoten bieten eine Möglichkeit, die Einstellungen danach zu organisieren, worauf sie angewendet werden. Die in einem Gruppenrichtlinienobjekt definierten Einstellungen lassen sich auf Clientcomputer, Benutzer oder Mitgliedsserver sowie Domänencontroller anwenden. Welche Einstellungen worauf angewendet werden, hängt vom Container ab, mit dem Sie das Gruppenrichtlinienobjekt verknüpfen. Standardmäßig werden alle Objekte im Container, mit dem das Gruppenrichtlinienobjekt verknüpft ist, durch die Einstellungen des Gruppenrichtlinienobjekts beeinflusst.

Die Knoten *Computerkonfiguration* und *Benutzerkonfiguration* enthalten die folgenden drei Teilknoten oder Erweiterungen, die die verfügbaren Gruppenrichtlinieneinstellungen weiter untergliedern:

- **Softwareeinstellungen** Unter dem Knoten *Computerkonfiguration* werden die Einstellungen für Softwareinstallationen in diesem Ordner auf alle Benutzer angewendet, die sich an einer Domäne von einem Computer anmelden, der vom Gruppenrichtlinienobjekt beeinflusst wird. Unter dem Knoten *Benutzerkonfiguration* werden die Einstellungen für Softwareinstallationen in diesem Ordner auf alle Benutzer angewendet, auf die sich die Gruppenrichtlinie bezieht, unabhängig vom Computer, von dem aus sie sich anmelden.
- **Windows-Einstellungen** Unter dem Knoten *Computerkonfiguration* werden die Sicherheitseinstellungen und Skripts in diesem Ordner auf alle Benutzer angewendet, die sich bei AD DS von diesem konkreten Computer aus anmelden. Unter dem Knoten *Benutzerkonfiguration* enthält dieser Ordner Einstellungen für Ordnerumleitungen, Sicherheitseinstellungen und Skripts, die für bestimmte Benutzer gelten.
- **Administrative Vorlagen** Windows Server 2012 umfasst Tausende Richtlinien in administrativen Vorlagen, die sämtlich registrierungsbasierte Richtlinieneinstellungen enthalten. Administrative Vorlagen sind Dateien mit der Erweiterung *.admx* und werden verwendet, um die Benutzeroberfläche für die Gruppenrichtlinieneinstellungen zu generieren, die Sie mithilfe des Gruppenrichtlinienverwaltungs-Editors festlegen können.

Um mit den Einstellungen von administrativen Vorlagen zu arbeiten, müssen Sie die Funktion der folgenden drei Status jeder Richtlinieneinstellung kennen:

- **Nicht konfiguriert** Als Ergebnis der Richtlinie tritt keine Änderung an der Registrierung gegenüber ihrem Standardstatus auf. Dies ist auch die Standardeinstellung bei der Mehrheit der Gruppenrichtlinienobjekteinstellungen. Verarbeitet ein System ein Gruppenrichtlinienobjekt mit einer Einstellung *Nicht konfiguriert*, wird der von der Einstellung betroffene Registrierungsschlüssel weder modifiziert noch überschrieben, und zwar unabhängig von seinem aktuellen Wert.
- **Aktiviert** Die Richtlinienfunktion wird in der Registrierung explizit aktiviert, unabhängig von ihrem vorherigen Zustand
- **Deaktiviert** Die Richtlinienfunktion wird in der Registrierung explizit deaktiviert, unabhängig von ihrem vorherigen Zustand

Diese Zustände sind insbesondere wichtig, wenn Sie mit Gruppenrichtlinienvererbung und mehreren Gruppenrichtlinienobjekten arbeiten. Ist eine Richtlinieneinstellung in der Registrierung standardmäßig deaktiviert und Sie haben ein Gruppenrichtlinienobjekt mit einer niedrigeren Priorität, das diese Einstellung aktiviert, müssen Sie ein Gruppenrichtlinienobjekt mit höherer Priorität konfigurieren, um die Einstellung zu deaktivieren, falls Sie ihren Standardwert wiederherstellen wollen. Wenn Sie den Status *Nicht konfiguriert* anwenden, bleibt die Einstellung unverändert, d.h. im Status *aktiviert*.

Mehrfache lokale Gruppenrichtlinienobjekte erstellen

Computer, die Mitglieder einer AD DS-Domäne sind, profitieren von einer sehr flexiblen Gruppenrichtlinienkonfiguration. Eigenständige (Nicht-AD DS)-Systeme können einen gewissen Grad dieser Flexibilität erreichen, wenn Sie mindestens unter Windows Vista oder Windows Server 2008 R2 ausgeführt werden. Unter diesen Betriebssystemen haben Administratoren die Möglichkeit, mehrfache lokale Gruppenrichtlinienobjekte zu erstellen, die verschiedene Einstellungen für verschiedene Benutzer basierend auf deren Identitäten bieten.

Windows-Systeme, die mehrfache lokale Gruppenrichtlinienobjekte unterstützen, besitzen die folgenden drei Ebenen der Gruppenrichtlinienunterstützung:

- **Richtlinien der lokalen Gruppe** Identisch mit dem einzelnen lokalen Gruppenrichtlinienobjekt, das von älteren Betriebssystemversionen unterstützt wird. Diese Ebene besteht sowohl aus Computer- als auch Benutzereinstellungen und wird auf alle Systembenutzer angewendet, ob administrativ oder nicht. Dies ist das einzige lokale Gruppenrichtlinienobjekt, das Computereinstellungen umfasst. Um also Richtlinien der Computerkonfiguration anzuwenden, müssen Sie dieses Gruppenrichtlinienobjekt verwenden.
- **Administratoren- und Nicht-Administratoren-Gruppenrichtlinie** Diese Ebene besteht aus zwei Gruppenrichtlinienobjekten: eines gilt für Mitglieder der lokalen Administratorengruppe und eines für alle Benutzer, die keine Mitglieder der lokalen Administratorengruppe sind. Im Unterschied zum Gruppenrichtlinienobjekt *Richtlinien der lokalen Gruppe* umfasst diese Ebene keine Sicherheitseinstellungen.

- **Benutzerspezifische Gruppenrichtlinie** Die Gruppenrichtlinienobjekte in dieser Ebene werden auf bestimmte lokale Benutzerkonten angewendet, die auf dem Computer erstellt wurden. Die Gruppenrichtlinienobjekte können sich nur auf einzelne Benutzer und nicht auf lokale Gruppen beziehen. Außerdem besitzen diese Gruppenrichtlinienobjekte keine Computerkonfigurationsseinstellungen.

Windows wendet die lokalen Gruppenrichtlinienobjekte in der hier aufgeführten Reihenfolge an. Die Einstellungen für *Richtlinien der lokalen Gruppe* werden zuerst angewendet, dann folgen entweder Administrator- oder Nichtadministrator-Gruppenrichtlinienobjekte und schließlich alle benutzerspezifischen Gruppenrichtlinienobjekte. Wie bei nichtlokalen Gruppenrichtlinienobjekten können die später verarbeiteten Einstellungen alle früheren Einstellungen, mit denen sie in Konflikt stehen, überschreiben.

Bei einem System, das auch Mitglied einer Domäne ist, kommen die drei Ebenen der lokalen Gruppenrichtlinienobjektverarbeitung zuerst an die Reihe, gefolgt von der nichtlokalen Gruppenrichtlinienanwendung in Standardreihenfolge.

Lokale Gruppenrichtlinienobjekte erstellen Sie mit dem Gruppenrichtlinienobjekt-Editor, der als MMC-Snap-In auf allen Windows-Computern insbesondere für die Verwaltung von lokalen Gruppenrichtlinienobjekten zur Verfügung steht. Gehen Sie wie folgt vor:

1. Melden Sie sich an einem Windows-Computer unter einem Konto mit Administratorrechten an. Die Konsole *Server-Manager* wird geöffnet.
2. Öffnen Sie das Dialogfeld *Ausführen*, geben Sie in das Textfeld *Öffnen* den Befehl **mmc** ein und klicken Sie auf *OK*. Es erscheint eine leere MMC-Konsole.
3. Klicken Sie auf *Datei / Snap-In hinzufügen/entfernen*, um das Dialogfeld *Snap-In hinzufügen/entfernen* zu öffnen.

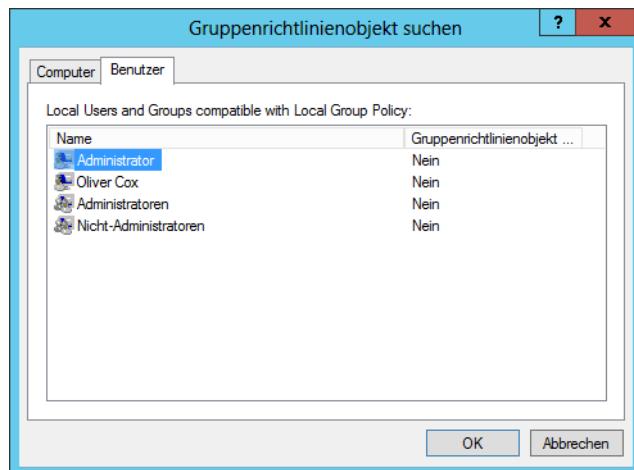


Abbildung 6.4 Die Registerkarte *Benutzer* im Dialogfeld *Gruppenrichtlinienobjekt suchen*

4. Markieren Sie in der Liste *Verfügbare Snap-Ins* den Eintrag *Gruppenrichtlinienobjekt-Editor* und klicken Sie auf *Hinzufügen*. Es erscheint die Seite *Gruppenrichtlinienobjekt auswählen*.
5. Um das Gruppenrichtlinienobjekt *Lokaler Computer* zu erstellen, klicken Sie auf *Fertig stellen*. Um ein sekundäres oder tertiäres Gruppenrichtlinienobjekt anzulegen, klicken Sie auf *Durchsuchen*. Es erscheint das Dialogfeld *Gruppenrichtlinienobjekt suchen*.
6. Gehen Sie auf die Registerkarte *Benutzer* (siehe Abbildung 6.4).



Hinweis Mehrere lokale Gruppenrichtlinienobjekte

Bei Windows-Computern, die mehrere lokale Gruppenrichtlinienobjekte nicht unterstützen, fehlt die Registerkarte *Benutzer* im Dialogfeld *Gruppenrichtlinienobjekte suchen*. Hierzu gehören Domänencontroller und Computer, die Windows-Versionen vor Windows Vista und Windows Server 2008 R2 ausführen.

7. Um ein sekundäres Gruppenrichtlinienobjekt zu erstellen, wählen Sie entweder *Administrator* oder *Nichtadministrator* und klicken auf *OK*. Um ein tertiäres Gruppenrichtlinienobjekt zu erstellen, wählen Sie einen Benutzer aus und klicken auf *OK*. Das Gruppenrichtlinienobjekt erscheint auf der Seite *Gruppenrichtlinienobjekt auswählen*.
8. Klicken Sie auf *Fertig stellen*. Das Snap-In erscheint im Dialogfeld *Snap-Ins hinzufügen/entfernen*.
9. Klicken Sie auf *OK*. Das Snap-In ist nun in der MMC-Konsole enthalten.
10. Klicken Sie auf *Datei / Speichern unter*, um das Kombinationsfeld *Speichern unter* zu öffnen.
11. Geben Sie einen Namen für die Konsole ein und speichern Sie sie in der Programmgruppe *Verwaltung*.
12. Schließen Sie die MMC-Konsole.

Diese Konsole können Sie nun immer dann öffnen, wenn Sie die Einstellungen im erstellten Gruppenrichtlinienobjekt konfigurieren müssen. Ein Gruppenrichtlinienobjekt *Richtlinien der lokalen Gruppe* besitzt sowohl Computerkonfigurations- als auch Benutzerkonfigurations-einstellungen, während die sekundären und tertiären Gruppenrichtlinienobjekte nur über Benutzerkonfigurationseinstellungen verfügen.

Prüfungszielzusammenfassung

- Gruppenrichtlinien bestehen aus Benutzer- und Computereinstellungen, die beim Hoch- und Herunterfahren des Computers implementiert werden können. Mit diesen Einstellungen ist es möglich, die Benutzerumgebung anzupassen, Sicherheitsrichtlinien zu implementieren und die Benutzer- und Desktopverwaltung zu erleichtern.
- Gruppenrichtlinien in AD DS können Standorten, Domänen und Organisationseinheiten zugewiesen werden. Standardmäßig gibt es eine lokale Richtlinie pro Computer. Lokale

Richtlinieneinstellungen werden von Active Directory-Richtlinieneinstellungen überschrieben.

- Mithilfe der Konsole *Gruppenrichtlinienverwaltung* erstellen und modifizieren Sie Gruppenrichtlinienobjekte und deren Einstellungen

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Auf welche der folgenden Dateitypen greifen die Gruppenrichtlinientools in einem zentralen Speicher standardmäßig zu?
 - A. ADM-Dateien
 - B. ADMX-Dateien
 - C. Gruppenrichtlinienobjekte
 - D. Sicherheitsvorlagen
2. Welches der folgenden lokalen Gruppenrichtlinienobjekte hat auf einem System mit mehreren lokalen Gruppenrichtlinienobjekten Vorrang?
 - A. Richtlinien der lokalen Gruppe
 - B. Richtlinien der Administratorgruppe
 - C. Richtlinien der Nichtadministratorgruppe
 - D. Benutzerspezifische Gruppenrichtlinie
3. Mit welcher der folgenden Techniken können Sie Gruppenrichtlinienobjekteinstellungen auf eine bestimmte Gruppe von Benutzern in einer Organisationseinheit anwenden?
 - A. Gruppenrichtlinienobjektverknüpfung
 - B. Administrative Vorlagen
 - C. Sicherheitsfilterung
 - D. Starter-Gruppenrichtlinienobjekte
4. Welche der folgenden Aussagen beschreibt am besten die Funktion eines Starter-Gruppenrichtlinienobjekts?
 - A. Ein Starter-Gruppenrichtlinienobjekt fungiert als Vorlage für das Erstellen eines neuen Gruppenrichtlinienobjekts.
 - B. Ein Starter-Gruppenrichtlinienobjekt ist das erste Gruppenrichtlinienobjekt, das auf alle Active Directory-Clients angewendet wird.

- C. Ein Starter-Gruppenrichtlinienobjekt verwendet eine vereinfachte Benutzeroberfläche für Privatbenutzer.
- D. Ein Starter-Gruppenrichtlinienobjekt enthält alle Einstellungen, die im standardmäßigen Domänenrichtlinien-Gruppenrichtlinienobjekt enthalten sind.
5. Wie lautet das Ergebnis, wenn Sie ein Gruppenrichtlinienobjekt mit dem Wert *Nicht konfiguriert* für eine bestimmte Einstellung auf ein System anwenden, auf dem die gleiche Einstellung deaktiviert ist?
- A. Die Einstellung bleibt deaktiviert.
- B. Die Einstellung wird in *Nicht konfiguriert* geändert.
- C. Die Einstellung wird in *Aktiviert* geändert.
- D. Die Einstellung erzeugt einen Konfliktfehler.



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Nach einem jüngsten Vorfall, bei dem ein Mitarbeiter mit einem beträchtlichen Umfang an vertraulichen Daten die Firma verließ, hat der Leiter der IT-Abteilung Alice damit beauftragt, Gruppenrichtlinieneinstellungen zu implementieren, die alle Benutzer mit Ausnahme der Administratoren und Mitglieder der Gruppe *Geschäftsleitung* daran hindern, USB-Geräte zu installieren.

Alice erstellt für diesen Zweck ein Gruppenrichtlinienobjekt *Geräteeinschränkungen* und verknüpft es mit dem einzigen Domänenobjekt der Firma. Das Gruppenrichtlinienobjekt enthält die folgenden Einstellungen aus dem Ordner *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Geräteinstallation\Einschränkungen bei der Geräteinstallation*:

- Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallation" erlauben – Aktiviert
- Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind – Aktiviert

Was muss Alice sonst noch tun, um die ihr gestellte Aufgabe zu erfüllen?

Prüfungsziel 6.2: Sicherheitsrichtlinien konfigurieren

Gruppenrichtlinien zielen in erster Linie darauf ab, eine zentralisierte Verwaltung von Sicherheitseinstellungen für Benutzer und Computer zu bieten. Die meisten Einstellungen, die sich auf Sicherheit beziehen, sind im Ordner *Windows-Einstellungen* im Knoten *Computerkonfiguration* eines Gruppenrichtlinienobjekts untergebracht. Mithilfe der *Sicherheitseinstellungen* können Sie steuern, wie Benutzer im Netzwerk authentifiziert werden, welche Ressourcen sie verwenden dürfen, welche Richtlinien für Gruppenmitgliedschaften gelten und welche Ereignisse in Bezug auf Benutzer- und Gruppenaktionen in den Ereignisprotokollen aufgezeichnet werden. Richtlinieneinstellungen im Knoten Computerkonfiguration gelten für einen Computer, wobei es keine Rolle spielt, wer sich an diesem Computer anmeldet. Es gibt mehr Einstellungen für die Computerkonfiguration als Einstellungen, die Sie auf einen bestimmten Benutzer anwenden können.

Dieses Prüfungsziel zeigt, wie Sie

- das Zuweisen von Benutzerrechten konfigurieren
 - Einstellungen von Sicherheitsoptionen konfigurieren
 - Sicherheitsvorlagen konfigurieren
 - Überwachungsrichtlinien konfigurieren
 - lokale Benutzer und Gruppen konfigurieren
 - die Benutzerkontensteuerung konfigurieren
-

Lokale Richtlinien definieren

Mithilfe lokaler Richtlinien können Administratoren auf dem lokalen Computer Benutzerrechte festlegen, die regeln, was Benutzer auf dem Computer tun dürfen, und bestimmen, ob das System Benutzeraktivitäten in einem Ereignisprotokoll aufzeichnen soll. Ereignisse auf dem lokalen Computer zu verfolgen – die sogenannte *Überwachung* –, ist ein wichtiger Bestandteil der Überwachung und Verwaltung von Aktivitäten auf einem Windows Server 2012-Computer.

Der unter *Sicherheitseinstellungen* liegende Knoten *Lokale Richtlinien* eines Gruppenrichtlinienobjekts besitzt drei untergeordnete Knoten: *Überwachungsrichtlinie*, *Zuweisen von Benutzerrechten* und *Sicherheitsoptionen*. Wie die folgenden Abschnitte erläutern, sollten Sie im Hinterkopf behalten, dass lokale Richtlinien lokal zu einem Computer sind. Als Bestandteil eines Gruppenrichtlinienobjekts in Active Directory beeinflussen sie die lokalen Sicherheitseinstellungen von Computerkonten, auf die das Gruppenrichtlinienobjekt angewendet wird.

Eine Überwachungsrichtlinie planen und konfigurieren

Der Abschnitt *Überwachungsrichtlinie* eines Gruppenrichtlinienobjekts erlaubt es Administratoren, erfolgreiche und gescheiterte Sicherheitsereignisse zu protokollieren, beispielsweise

Anmeldeereignisse, Kontozugriffe und Objektzugriffe. Mithilfe der Überwachung können Sie sowohl Benutzer- als auch Systemaktivitäten verfolgen. Wenn Sie eine Überwachung planen, müssen Sie die zu überwachenden Computer und die Art der zu verfolgenden Ereignisse bestimmen.

In Bezug auf die zu überwachenden Ereignisse – wie zum Beispiel Kontoanmeldeereignisse – müssen Sie entscheiden, ob Sie erfolgreiche Anmeldeversuche, gescheiterte Anmeldeversuche oder beides überwachen wollen. Indem Sie erfolgreiche Ereignisse verfolgen, können Sie ermitteln, wie oft Benutzer auf Netzwerkressourcen zugreifen. Diese Informationen liefern wichtige Hinweise für die Planung der Ressourcennutzung und die Budgetierung neuer Ressourcen. Wenn Sie gescheiterte Ereignisse verfolgen, können Sie stattgefundene oder versuchte Sicherheitsverletzungen erkennen. Stellen Sie zum Beispiel fest, dass gescheiterte Anmeldeversuche gehäuft bei einem bestimmten Benutzerkonto auftreten, sollten Sie diesbezüglich weitere Nachforschungen anstellen. Abbildung 6.5 zeigt die Richtlinieneinstellungen, die für eine Überwachung zur Verfügung stehen.

Tritt ein überwachtes Ereignis auf, schreibt Windows Server 2012 ein Ereignis in das Sicherheitsprotokoll auf dem Domänencontroller oder auf dem Computer, wo das Ereignis stattgefunden hat. Handelt es sich um einen Anmeldeversuch oder ein anderes Active Directory-bezogenes Ereignis, wird das Ereignis in das Ereignisprotokoll auf dem Domänencontroller geschrieben. Bei einem Computerereignis wie etwa dem Zugriff auf ein Diskettenlaufwerk kommt das Ereignis in das Ereignisprotokoll des lokalen Computers.

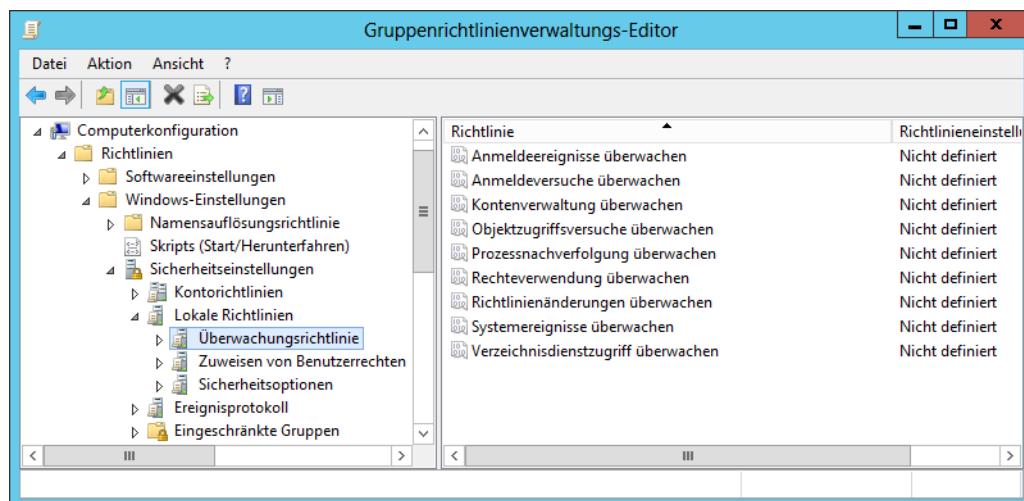


Abbildung 6.5 Überwachungsrichtlinien in der standardmäßigen Domänenrichtlinie

Sie müssen entscheiden, welche Computer, Ressourcen und Ereignisse Sie überwachen möchten. Wichtig dabei ist, die notwendige Überwachung gegen die mögliche Informationsüberflutung abzuwägen, die entstehen kann, wenn Sie jeden möglichen Ereignistyp überwachen. Die folgenden Orientierungspunkte sollen Ihnen helfen, Ihre Überwachungsrichtlinie zu planen:

- **Nur relevante Elemente überwachen** Bestimmen Sie die Ereignisse, die Sie überwachen wollen, und entscheiden Sie, ob es wichtiger ist, Erfolg oder Scheitern dieser Ereignisse zu verfolgen. Planen Sie für die Überwachung nur Ereignisse ein, die Ihnen dabei helfen, Netzwerkinformationen zusammenzutragen.
- **Sicherheitsprotokolle archivieren, um einen dokumentierten Verlauf zu erhalten** Wenn Sie den Verlauf der aufgetretenen Ereignisse dokumentieren, können Sie auf diese Dokumentation zurückgreifen, um beispielsweise den Bedarf an zusätzlichen Ressourcen basierend auf der bisherigen Nutzung zu ermitteln
- **Die Größe der Sicherheitsprotokolle sorgfältig konfigurieren** Die Größe Ihrer Sicherheitsprotokolle sollten Sie nach der Anzahl von Ereignissen festlegen, die Sie voraussichtlich protokollieren werden. Die Richtlinieneinstellungen für Ereignisprotokolle lassen sich unter dem Knoten *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Ereignisprotokoll* eines Gruppenrichtlinienobjekts konfigurieren.

Die Umsetzung Ihres Plans setzt voraus, dass Sie die zu überwachenden Kategorien angeben und bei Bedarf die Objekte für eine Überwachung konfigurieren. Gehen Sie wie folgt vor, um eine Überwachungsrichtlinie zu konfigurieren:

1. Melden Sie sich an einem Windows Server 2012-Domänencontroller unter einem Konto mit Domänenadministratorrechten an. Die Konsole *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Gruppenrichtlinienverwaltung*, um die Konsole *Gruppenrichtlinienverwaltung* zu öffnen.
3. Erweitern Sie den Gesamtstrukturcontainer und suchen Sie Ihre Domäne auf. Erweitern Sie dann den Domänencontainer und wählen Sie den Ordner *Gruppenrichtlinienobjekte* aus. Auf der Registerkarte *Inhalt* erscheinen die Gruppenrichtlinienobjekte, die derzeit in der Domäne vorhanden sind.
4. Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt *Default Domain Policy* (Standarddomänenrichtlinie) und klicken Sie im Kontextmenü auf *Bearbeiten*. Für diese Richtlinie wird nun ein Fenster *Gruppenrichtlinienverwaltungs-Editor* geöffnet.
5. Gehen Sie zum Knoten *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien* und wählen Sie *Überwachungsrichtlinie* aus. Im rechten Fensterbereich erscheinen nun die Überwachungsrichtlinieneinstellungen.
6. Doppelklicken Sie auf die Überwachungsrichtlinieneinstellung, die Sie modifizieren wollen. Es erscheint das Eigenschaftenblatt für die ausgewählte Richtlinie (siehe Abbildung 6.6).
7. Aktivieren Sie das Kontrollkästchen *Diese Richtlinieneinstellungen definieren*.
8. Aktivieren Sie die passenden Kontrollkästchen, um erfolgreiche und/oder gescheiterte Versuche zu überwachen.

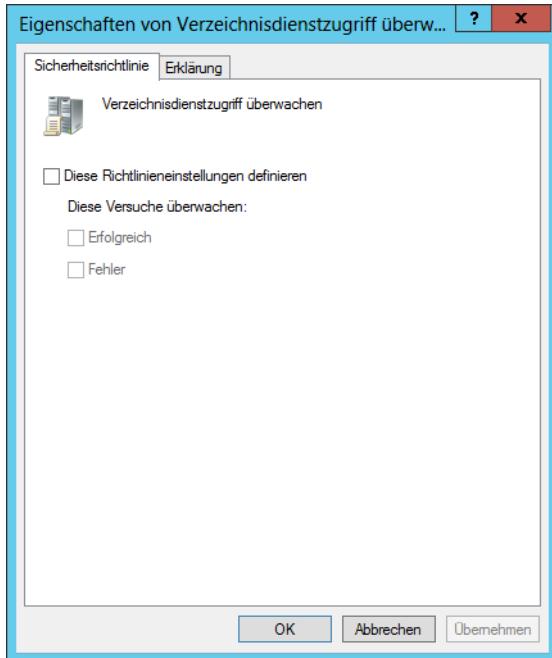


Abbildung 6.6 Das Eigenschaftenblatt für eine Richtlinieneinstellung

9. Klicken Sie auf *OK*, um das Eigenschaftenblatt der Einstellung zu schließen.
10. Schließen sie den Gruppenrichtlinienverwaltungs-Editor und die Gruppenrichtlinienverwaltungskonsole.

Nunmehr haben Sie eine Überwachungsrichtlinie im Gruppenrichtlinienobjekt der Standarddomänenrichtlinie konfiguriert. Diese wird dann bei der nächsten Richtlinienaktualisierung auf alle Computer in der Domäne weitergeleitet.

Die Objekte sind für eine Überwachung zu konfigurieren, falls Sie eine der beiden folgenden Ereigniskategorien konfiguriert haben:

- **Verzeichnisdienstzugriff überwachen** Diese Ereigniskategorie protokolliert Benutzerzugriffe auf Active Directory-Objekte wie zum Beispiel andere Benutzerobjekte oder Organisationseinheiten
- **Objektzugriffsversuche überwachen** Diese Ereigniskategorie protokolliert Benutzerzugriffe auf Dateien, Ordner, Registrierungsschlüssel und Drucker

Jede dieser Ereigniskategorien erfordert zusätzliche Setupschritte. Dabei öffnen Sie das Eigenschaftenblatt für das zu überwachende Objekt und spezifizieren die Sicherheitsprinzipale oder die Dateien und Ordner, für die Sie den Zugriff überwachen möchten.



Hinweis Überwachungsoptionen

Seit Windows Server 2008 gibt es für die AD DS-Überwachung neue Optionen, die anzeigen, ob eine Änderung aufgetreten ist, und den alten und den neuen Wert bereitstellen. Wenn Sie zum Beispiel die Beschreibung eines Benutzers von *Marketing* in *Training* ändern, zeichnet das Ereignisprotokoll der Verzeichnisdienste zwei Ereignisse auf, die den ursprünglichen Wert und den neuen Wert enthalten.

Benutzerrechte zuweisen

Wie Abbildung 6.7 zeigt, sind die Einstellungen für das Zuweisen von Benutzerrechten in Windows Server 2012 umfangreich und enthalten auch Einstellungen, die Benutzer benötigen, um systembezogene Aufgaben durchzuführen.

Richtlinie	Richtlinieneinstellung
[1] Ändern der Systemzeit	Nicht definiert
[2] Ändern der Zeitzone	Nicht definiert
[3] Anheben der Zeitplanungspriorität	Nicht definiert
[4] Anmelden als Batchauftrag verweigern	Nicht definiert
[5] Anmelden als Dienst	Nicht definiert
[6] Anmelden als Dienst verweigern	Nicht definiert
[7] Anmelden als Stapelverarbeitungsauftrag	Nicht definiert
[8] Anmelden über Remotedesktopdienste verweigern	Nicht definiert
[9] Anmelden über Remotedesktopdienste zulassen	Nicht definiert
[10] Annehmen der Clientidentität nach Authentifizierung	Nicht definiert
[11] Anpassen von Speicherkontingenten für einen Prozess	Nicht definiert
[12] Arbeitsatz eines Prozesses vergrößern	Nicht definiert
[13] Auf Anmeldeinformations-Manager als vertrauenswürdig...	Nicht definiert
[14] Auf diesen Computer vom Netzwerk aus zugreifen	Nicht definiert
[15] Auslassen der durchsuchenden Überprüfung	Nicht definiert
[16] Debuggen von Programmen	Nicht definiert
[17] Durchführen von Volumewartungsaufgaben	Nicht definiert
[18] Einsetzen als Teil des Betriebssystems	Nicht definiert
[19] Entfernen des Computers von der Dockingstation	Nicht definiert
[20] Ermöglichen, dass Computer- und Benutzerkonten für Dele...	Nicht definiert
[21] Ersetzen eines Tokens auf Prozessebene	Nicht definiert
[22] Erstellen einer Auslagerungsdatei	Nicht definiert

Abbildung 6.7 Einstellungen für die Zuweisung von Benutzerrechten in einem Gruppenrichtlinienobjekt

Zum Beispiel muss dem Konto eines Benutzers, der sich lokal an einem Domänencontroller anmeldet, das Recht *Lokal anmelden zulassen* zugewiesen sein oder er muss Mitglied einer der folgenden AD DS-Gruppen sein: *Konten-Operatoren*, *Administratoren*, *Sicherungs-Operatoren*, *Druck-Operatoren* oder *Server-Operatoren*.

Diese Gruppenmitgliedschaften ermöglichen es Benutzern, sich lokal anzumelden, weil Windows Server 2012 diesen Gruppen standardmäßig das Benutzerrecht *Lokal anmelden zulassen* im Objekt der Standarddomänencontrollerrichtlinie zuweist.

Andere ähnliche Einstellungen in dieser Sammlung beziehen sich auf Benutzerrechte, die dem Herunterfahren des Systems, dem Übernehmen der Besitzrechte von Dateien oder Objekten, dem Wiederherstellen von Dateien und Verzeichnissen sowie der Synchronisierung von Verzeichnisdienstdaten zugeordnet sind.

Sicherheitsoptionen konfigurieren

Wie Abbildung 6.8 zeigt, umfasst der Knoten *Sicherheitsoptionen* in einem Gruppenrichtlinienobjekt Sicherheitseinstellungen, die sich auf interaktive Anmeldung, digitales Signieren von Daten, Beschränkungen beim Zugriff auf Disketten und CD-ROM-Laufwerke, Verhalten bei der Installation von nichtsignierten Treibern und Verhalten von Anmeldedialogfeldern beziehen.

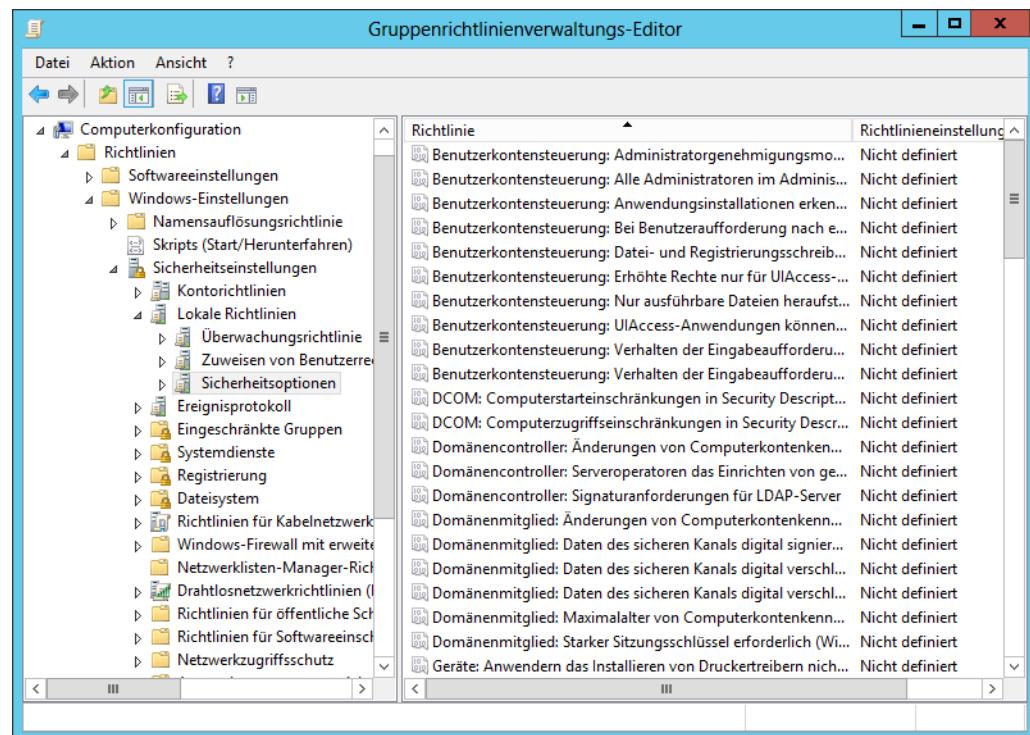


Abbildung 6.8 Der Knoten *Sicherheitsoptionen* in einem Gruppenrichtlinienobjekt

Die Kategorie *Sicherheitsoptionen* schließt auch Optionen ein, um Authentifizierung und Kommunikationssicherheit innerhalb von Active Directory zu konfigurieren.

Sicherheitsvorlagen verwenden

Eine *Sicherheitsvorlage* ist eine Sammlung von Konfigurationseinstellungen, die als Textdatei mit der Erweiterung *.inf* gespeichert sind. Sicherheitsvorlagen können viele der gleichen Sicherheitsparameter wie Gruppenrichtlinienobjekte enthalten. Allerdings stellen Sicherheitsvorlagen diese Parameter in einer vereinheitlichten Benutzeroberfläche dar, sodass Sie Ihre Konfigurationen als Dateien speichern können, und erleichtern es, diese bereitzustellen, wann und wo sie benötigt werden.

Die Einstellungen, die Sie mithilfe von Sicherheitsvorlagen bereitstellen können, umfassen viele der Sicherheitsrichtlinien, die in diesem Prüfungsziel behandelt wurden, einschließlich Überwachungsrichtlinien, Zuweisungen von Benutzerrechten, Sicherheitsoptionen, Richtlinien für Ereignisprotokolle und eingeschränkte Gruppen. Eine Sicherheitsvorlage ist an sich ein komfortables Mittel, um die Sicherheit eines Einzelsystems zu konfigurieren. In Verbindung mit Gruppenrichtlinien oder Skripting erlauben sie Administratoren, die Sicherheit von Netzwerken zu verwalten, die aus Hunderten oder Tausenden von Computern bestehen, die unter verschiedenen Versionen von Microsoft Windows laufen.

Mit diesen Tools können Administratoren komplexe Sicherheitskonfigurationen schaffen und diese Konfigurationen für die verschiedenen Rollen, die Computer in ihren Organisationen erfüllen, anpassen. Wenn Sie Sicherheitsvorlagen über ein Netzwerk bereitstellen, sind Sie in der Lage, konsistente, skalierbare und reproduzierbare Sicherheitseinstellungen im gesamten Unternehmen zu realisieren.

Die Konsole Sicherheitsvorlagen

Sicherheitsvorlagen sind Textdateien, die Sicherheitseinstellungen in einem breiten Spektrum von Formaten enthalten, abhängig vom Wesen der jeweiligen Einstellungen. Es ist zwar möglich, Sicherheitsvorlagen in einem Texteditor direkt zu bearbeiten, doch bietet Windows Server 2012 eine grafische Benutzeroberfläche, die das Ganze erleichtert.

Sicherheitsvorlagen lassen sich mit dem MMC-Snap-In *Sicherheitsvorlagen* erstellen und verwalten. Im Menü für die Verwaltungstools von Windows Server 2012 ist allerdings keine MMC mit diesem enthalten, sodass Sie eine Konsole mit dem Snap-In in eigener Regie über das MMC-Dialogfeld *Snap-Ins hinzufügen bzw. entfernen* einrichten müssen. Wenn Sie eine neue Vorlage erstellen, zeigt die Konsole eine Benutzeroberfläche, wie sie in Abbildung 6.9 zu sehen ist.

Der linke Fensterbereich des Snap-Ins *Sicherheitsvorlagen* zeigt auf einen Ordner, in dem die Konsole standardmäßig die von Ihnen erstellten Vorlagendateien speichert. Das Snap-In interpretiert jede Datei mit einer *.inf*-Erweiterung in diesem Ordner als Sicherheitsvorlage, selbst wenn die Erweiterungen nicht in der Konsole zu sehen sind.

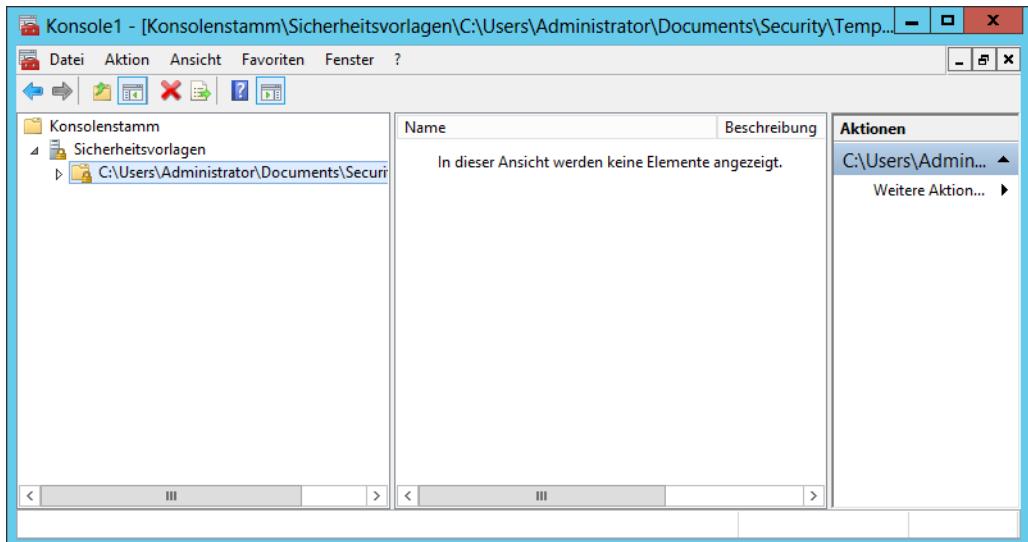


Abbildung 6.9 Das Snap-In *Sicherheitsvorlagen*

Wenn Sie in der Konsole eine neue Vorlage erstellen, sehen Sie eine hierarchische Anzeige der Richtlinien in der Vorlage und ihre aktuellen Einstellungen. Viele der Richtlinien sind mit denen in einem Gruppenrichtlinienobjekt identisch, und zwar sowohl hinsichtlich Erscheinung als auch Funktion. Und genau wie in einem Gruppenrichtlinienobjekt können Sie die Richtlinien in jeder Vorlage modifizieren.

Sicherheitsvorlagen erstellen

Um eine neue Sicherheitsvorlage von Grund auf neu zu erstellen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich an einem Windows-Computer unter einem Konto mit Administratorrechten an. Die Konsole *Server-Manager* wird geöffnet.
2. Öffnen Sie das Dialogfeld *Ausführen*, geben Sie in das Textfeld *Öffnen* den Befehl **mmc** ein und klicken Sie auf *OK*. Es erscheint eine leere MMC-Konsole.
3. Klicken Sie auf *Datei/Snap-In hinzufügen/entfernen*, um das Dialogfeld *Snap-In hinzufügen bzw. entfernen* zu öffnen.
4. Markieren Sie in der Liste *Verfügbare Snap-Ins* den Eintrag *Sicherheitsvorlagen* und klicken Sie auf *Hinzufügen*. Das Snap-In wird in die Liste *Ausgewählte Snap-Ins* übernommen.
5. Klicken Sie auf *OK*. Das Snap-In erscheint in der MMC.
6. Klicken Sie auf *Datei/Speichern unter*. Es erscheint ein Kombinationsfeld *Speichern unter*.

7. Geben Sie einen Namen für die Konsole ein und speichern Sie sie in der Programmgruppe *Verwaltungstools*.
8. Erweitern Sie den Knoten *Sicherheitsvorlagen*.
9. Klicken Sie mit der rechten Maustaste auf den Suchpfad der Sicherheitsvorlage und wählen Sie im Kontextmenü den Befehl *Neue Vorlage*. Ein Dialogfeld wird geöffnet.
10. Geben Sie in das Feld *Vorlage* einen Namen für die Vorlage ein und klicken Sie auf *OK*. Die neue Vorlage erscheint in der Konsole. Lassen Sie die Konsole geöffnet.

Wenn Sie eine leere Sicherheitsvorlage erstellen, sind noch keine Richtlinien in ihr definiert. Das Anwenden einer leeren Vorlage auf einen Computer hat keine Wirkung auf ihn.

Mit Einstellungen von Sicherheitsvorlagen arbeiten

Sicherheitsvorlagen enthalten viele der gleichen Einstellungen wie Gruppenrichtlinienobjekte, sodass Sie bereits mit einigen Elementen einer Vorlage vertraut sind. Zum Beispiel enthalten Sicherheitsvorlagen die gleichen lokalen Richtlinieneinstellungen, die dieses Kapitel weiter vorn beschrieben hat; die Vorlagen sind nur eine andere Methode, diese Richtlinien zu konfigurieren und bereitzustellen. Außerdem bieten Sicherheitsvorlagen ein Instrument für das Konfigurieren der Berechtigungen, die Dateien, Ordner, Registrierungseinträgen und Diensten zugeordnet sind.

Gegenüber der Richtlinie für *Lokaler Computer* besitzen Sicherheitsvorlagen mehr Einstellungen, da eine Vorlage auch Optionen sowohl für eigenständige Computer einschließt als auch für Computer, die in einer Domäne teilnehmen.

Sicherheitsvorlagen in Gruppenrichtlinienobjekte importieren

Um eine Sicherheitsvorlage auf mehreren Computern gleichzeitig bereitzustellen, ist es am einfachsten, die Vorlage in ein Gruppenrichtlinienobjekt zu importieren. Nachdem Sie die Vorlage importiert haben, wird sie zum Bestandteil des Gruppenrichtlinienobjekts und die Domänencontroller des Netzwerks stellen sie auf allen Computern bereit, die von diesem Gruppenrichtlinienobjekt beeinflusst werden. Wie bei jeder Gruppenrichtlinienbereitstellung können Sie ein Gruppenrichtlinienobjekt mit jedem Domänen-, Standort- oder OU-Objekt in der Active Directory-Gesamtstruktur verknüpfen. Die Einstellungen im Gruppenrichtlinienobjekt werden dann von allen Container- und Endknotenobjekten geerbt, die dem ausgewählten Objekt untergeordnet sind.

Eine Sicherheitsvorlage importieren Sie in folgenden Schritten in ein Gruppenrichtlinienobjekt:

1. Melden Sie sich an einem Windows Server 2012-Domänencontroller unter einem Konto mit Domänenadministratorrechten an. Die Konsole *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Gruppenrichtlinienverwaltung*. Es erscheint die Konsole *Gruppenrichtlinienverwaltung*.
3. Erweitern Sie den Gesamtstrukturcontainer und gehen Sie zu Ihrer Domäne. Erweitern Sie dann den Domänencontainer und wählen Sie den Ordner *Gruppenrichtlinienobjekte*

aus. Die momentan in der Domäne vorhandenen Gruppenrichtlinienobjekte erscheinen auf der Registerkarte *Inhalt*.

4. Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, in das Sie die Vorlage importieren möchten, und klicken Sie auf *Bearbeiten*. Daraufhin wird für diese Richtlinie ein Fenster *Gruppenrichtlinienverwaltungs-Editor* geöffnet.
5. Gehen Sie zum Knoten *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen*. Klicken Sie mit der rechten Maustaste auf den Knoten *Sicherheitseinstellungen* und wählen Sie im Kontextmenü den Befehl *Richtlinie importieren*. Das Dialogfeld *Richtlinie importieren von* erscheint.
6. Gehen Sie zur Sicherheitsvorlage, die Sie importieren wollen, und klicken Sie auf *Öffnen*. Die Richtlinieneinstellungen der Vorlage werden in das Gruppenrichtlinienobjekt kopiert.
7. Schließen Sie den *Gruppenrichtlinienverwaltungs-Editor* und die Konsole *Gruppenrichtlinienverwaltung*.

Lokale Benutzer und Gruppen konfigurieren

Windows Server 2012 bringt zwei separate Benutzeroberflächen mit, um lokale Benutzerkonten zu erstellen und zu verwalten: die Systemsteuerungsoption *Benutzerkonten* und das MMC-Snap-In *Lokale Benutzer und Gruppen*. Beide Oberflächen bieten Zugriff auf dieselbe Sicherheitskontenverwaltung (Security Account Manager, SAM), wo die Benutzer- und Gruppeninformationen gespeichert sind, sodass sämtliche Änderungen, die Sie in einer Oberfläche durchführen, auch in der anderen erscheinen.

Da Microsoft die Systemsteuerungsoption *Benutzerkonten* und das Snap-In *Lokale Benutzer und Gruppen* für Computernutzer mit unterschiedlicher Fachkompetenz konzipiert hat, bieten diese beiden Komponenten auf unterschiedlichen Niveaus Zugriff auf die Sicherheitskontenverwaltung:

- **Benutzerkonten** Stellt eine vereinfachte Benutzeroberfläche mit äußerst beschränktem Zugriff auf Benutzerkonten bereit. Über diese Oberfläche können Sie lokale Benutzerkonten erstellen und deren Basisattribute ändern, doch ist es nicht möglich, Gruppen zu erstellen oder Gruppenmitgliedschaften zu verwalten (abgesehen von der Gruppe *Administratoren*).
- **Lokale Benutzer und Gruppen** Bietet vollständigen Zugriff auf lokale Benutzer und Gruppen sowie alle ihre Attribute

Die Systemsteuerungsoption Benutzerkonten

Windows Server 2012 erstellt während der Betriebssysteminstallation zwei lokale Benutzerkonten: die Konten *Administrator* und *Gast*. Für das Administratorkonto fordert das Setupprogramm zur Eingabe eines Kennworts auf, das Gastkonto wird standardmäßig deaktiviert.

Nach Abschluss der Installation startet das System neu. Da nur das Administratorkonto zur Verfügung steht, findet die Anmeldung am Computer mit diesem Konto statt. Es besitzt

Administratorrechte, sodass Sie jetzt zusätzliche Benutzerkonten erstellen oder vorhandene modifizieren können.



Hinweis Lokale Benutzer erstellen

Auf Windows Server 2012-Computern, die einer Arbeitsgruppe angehören, können Sie neue Benutzerkonten nur in der Systemsteuerung erstellen. Wenn Sie einen Computer an eine AD DS-Domäne anschließen, müssen Sie das Snap-In *Lokale Benutzer und Gruppen* verwenden, um neue lokale Benutzerkonten einzurichten. Domänencontroller haben keine lokalen Benutzer- oder Gruppenkonten.

Die Systemsteuerungsoption *Benutzerkonten* erstellt Standardkonten. Um einem lokalen Benutzer die Rechte eines Administrators zu erteilen, müssen Sie den Kontotyp über die in Abbildung 6.10 gezeigte Benutzeroberfläche ändern.

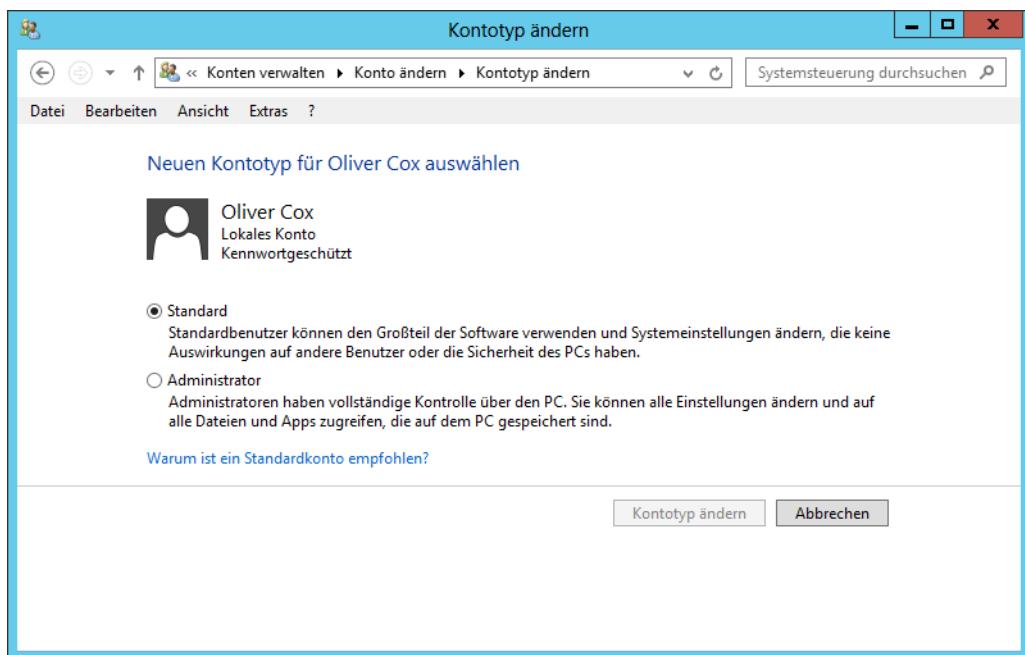


Abbildung 6.10 Das Fenster *Kontotyp ändern*

Was in der Systemsteuerungsoption *Benutzerkonten* als Kontotyp bezeichnet wird, ist tatsächlich eine Gruppenmitgliedschaft. Die Option *Standard* fügt das Benutzerkonto zur lokalen Benutzergruppe hinzu, während die Option *Administrator* das Konto in die Administratorengruppe aufnimmt.

Das Snap-In Lokale Benutzer und Gruppen

Über die Systemsteuerungsoption *Benutzerkonten* sind lokale Benutzerkonten nur teilweise zugänglich und Gruppen (bis auf *Benutzer* und *Administratoren*) gar nicht. Im Unterschied

dazu bietet das Snap-In *Lokale Benutzer und Gruppen* kompletten Zugriff auf alle lokalen Benutzer- und Gruppenkonten auf dem Computer.

Standardmäßig ist das Snap-In *Lokale Benutzer und Gruppen* Bestandteil der *Computer-Management-Konsole*. Allerdings können Sie das Snap-In an sich laden oder eine eigene MMC mit den Snap-Ins Ihrer Wahl zusammenstellen.

Um ein lokales Benutzerkonto mit dem Snap-In *Lokale Benutzer und Gruppen* zu erstellen, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Die Konsole *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Computerverwaltung*, um die Konsole *Computerverwaltung* zu öffnen.
3. Erweitern Sie den Knoten *Lokale Benutzer und Gruppen* und klicken Sie auf *Benutzer*, um eine Liste der aktuellen lokalen Benutzer anzuzeigen.
4. Klicken Sie mit der rechten Maustaste auf den Ordner *Benutzer* und wählen Sie im Kontextmenü *Neuer Benutzer*. Das in Abbildung 6.11 gezeigte Dialogfeld *Neuer Benutzer* erscheint.

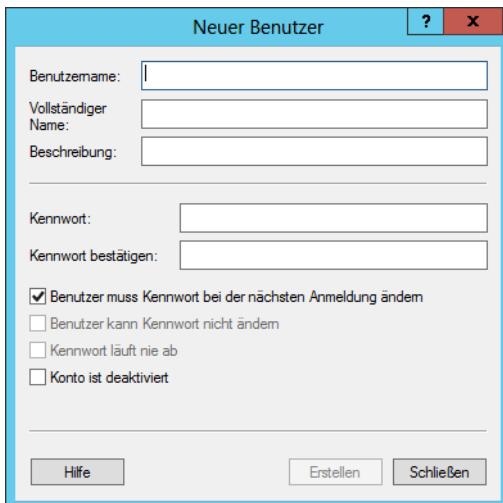


Abbildung 6.11 Das Dialogfeld *Neuer Benutzer*

5. Geben Sie in das Textfeld *Benutzername* den Namen ein, den Sie dem neuen Benutzerkonto zuweisen möchten. Dies ist die einzige erforderliche Eingabe in diesem Dialogfeld.
6. Geben Sie (optional) einen vollständigen Namen und eine Beschreibung für das Konto an.
7. Geben Sie in die Textfelder *Kennwort* und *Kennwort bestätigen* ein Kennwort für das Konto ein (optional).

8. Aktivieren oder deaktivieren Sie die vier Kontrollkästchen, um die folgenden Funktionen zu steuern:
 - **Benutzer muss Kennwort bei der nächsten Anmeldung ändern** Bei aktiviertem Kontrollkästchen ist der neue Benutzer gezwungen, das Kennwort zu ändern, sobald er sich das erste Mal angemeldet hat
 - **Benutzer kann Kennwort nicht ändern** Bei aktiviertem Kontrollkästchen hat der Benutzer keine Möglichkeit, das Kennwort für das Konto zu ändern
 - **Kennwort läuft nie ab** Ist dieses Kontrollkästchen aktiviert, bleibt das vorhandene Kennwort auf unbegrenzte Zeit bestehen
 - **Konto ist deaktiviert** Wenn Sie dieses Kontrollkästchen aktivieren, wird das Benutzerkonto deaktiviert, sodass sich niemand unter diesem Konto anmelden kann
9. Klicken Sie auf *Erstellen*. Das neue Konto wird der Benutzerliste hinzugefügt, die Konsole setzt die Eingabefelder auf leere Werte zurück und das Dialogfeld ist wieder bereit, um ein weiteres Benutzerkonto zu erstellen.
10. Klicken Sie auf *Schließen*.
11. Schließen Sie die Konsole *Computerverwaltung*.

Eine lokale Gruppe erstellen

Um eine lokale Gruppe mit dem Snap-In *Lokale Benutzer und Gruppen* zu erstellen, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei Windows Server 2012 unter einem Konto mit Administratorrechten an. Die Konsole *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Computerverwaltung*, um die Konsole *Computerverwaltung* zu öffnen.
3. Erweitern Sie den Knoten *Lokale Benutzer und Gruppen* und klicken Sie auf *Gruppen*, um eine Liste der lokalen Gruppen anzuzeigen.
4. Klicken Sie mit der rechten Maustaste auf den Ordner *Gruppen* und wählen Sie dann im Kontextmenü *Neue Gruppe*. Das Dialogfeld *Neue Gruppe* wird geöffnet.
5. Geben Sie in das Textfeld *Gruppenname* den Namen ein, den Sie der Gruppe zuweisen möchten. Dies ist die einzige erforderliche Eingabe im Dialogfeld. Tragen Sie falls gewünscht eine Beschreibung für die Gruppe ein.
6. Klicken Sie auf *Hinzufügen*. Das Dialogfeld *Benutzer, Computer, Dienstkonten oder Gruppen auswählen* wird geöffnet.
7. Geben Sie in das Textfeld die Namen der Benutzer (jeweils durch Semikolon getrennt) ein, die Sie in die Gruppe aufnehmen möchten, und klicken Sie dann auf *OK*. Die Benutzer werden der Mitgliedsliste hinzugefügt. Sie können auch den Benutzernamen nur teilweise eintippen und auf *Namen überprüfen* klicken, um den Namen vervollständigen zu lassen, oder auf *Erweitert* klicken, um nach Benutzern zu suchen.

8. Klicken Sie auf *Erstellen*, um die Gruppe zu erstellen und sie mit den angegebenen Benutzern zu füllen. Die Konsole setzt dann die Eingabefelder zurück und das Dialogfeld ist für das Erstellen einer weiteren Gruppe bereit.
9. Klicken Sie auf *Schließen*.
10. Schließen Sie die Konsole *Computerverwaltung*.

Lokale Gruppen besitzen außer einer Mitgliedsliste keine anderen Attribute. Wenn Sie also eine vorhandene Gruppe öffnen, können Sie Mitglieder hinzufügen oder entfernen, sonst aber keine Änderungen vornehmen. Wie bereits weiter vorn in diesem Kapitel erwähnt, dürfen lokale Gruppen keine anderen lokalen Gruppen als Mitglieder aufnehmen. Doch wenn der Computer Mitglied einer Windows-Domäne ist, kann eine lokale Gruppe Domänenbenutzer und Domänengruppen als Mitglieder enthalten.

Benutzerkontensteuerung konfigurieren

Eines der häufigsten Windows-Sicherheitsprobleme geht auf den Umstand zurück, dass viele Benutzer ihre alltäglichen Aufgaben am Computer mit mehr Systemzugriff als tatsächlich erforderlich durchführen. Wenn sich ein Benutzer als Administrator oder als Benutzer, der Mitglieder der Administratorengruppe ist, anmeldet, erhält er vollständigen Zugriff auf alle Bereiche des Betriebssystems. Für viele Anwendungen und Aufgaben, mit denen Benutzer jeden Tag zu tun haben, ist ein Systemzugriff auf einer solchen Ebene gar nicht erforderlich; er wird nur für bestimmte administrative Funktionen benötigt, etwa um systemweite Software zu installieren oder Systemparameter zu konfigurieren.

Für die meisten Benutzer ist es reine Bequemlichkeit, sich immer mit Administratorrechten anzumelden. Entsprechend einer Microsoft-Empfehlung sollten Sie sich normalerweise als Standardbenutzer anmelden und Administratorrechte nur verwenden, wenn Sie sie tatsächlich benötigen. Viele Fachleute, die so vorgehen, finden sich jedoch häufig in Situationen wieder, in denen sie administrativen Zugriff benötigen. Es gibt eine überraschend große Anzahl von allgemeinen, ja selbst banalen, Windows-Aufgaben, die administrativen Zugriff verlangen. Und wenn Benutzer diese Aufgaben nicht durchführen können, wirkt sich das gegebenenfalls negativ auf ihre Produktivität aus.

Microsoft hat sich dieses Problems angenommen, indem alle Windows Server 2012-Benutzer von Systemzugriffen mit Administratorrechten abgehalten werden, außer wenn diese Rechte erforderlich sind, um die unmittelbar anstehende Aufgabe durchzuführen. Die hierfür zuständigen Mechanismen werden als Benutzerkontensteuerung (User Account Control, UAC) bezeichnet.

Administrative Aufgaben durchführen

Wenn sich ein Benutzer bei Windows Server 2012 anmeldet, gibt das System ein Token aus, das die Zugriffsebene des Benutzers anzeigt. Autorisiert das System den Benutzer, eine bestimmte Aktivität durchzuführen, fragt er das Token ab, ob der Benutzer über die erforderlichen Rechte verfügt.

In den Windows-Versionen vor Windows Server 2008 und Windows Vista haben Standardbenutzer Standardtokens und Mitglieder der Administratorengruppe administrative Token erhalten. Jede von einem administrativen Benutzer durchgeführte Aufgabe wurde demzufolge mithilfe des administrativen Tokens autorisiert, was zu den weiter oben geschilderten Problemen führte.

Auf einem Windows Server 2012-Computer mit Benutzerkontensteuerung erhält ein Standardbenutzer weiterhin ein Standardtoken, doch ein administrativer Benutzer erhält zwei Token: eines für Standardbenutzerzugriff und eines für den Zugriff mit Administratorrechten. Standardmäßig verwenden sowohl die Standard- als auch die administrativen Benutzer meistens das Standardbenutzertoken.

Wenn ein Standardbenutzer eine Aufgabe ausführen möchte, die Administratorrechte voraussetzt, zeigt das System eine Aufforderung zur Eingabe von Anmeldeinformationen an (siehe Abbildung 6.12), das vom Benutzer den Namen und das Kennwort für ein Konto mit Administratorrechten abfragt.

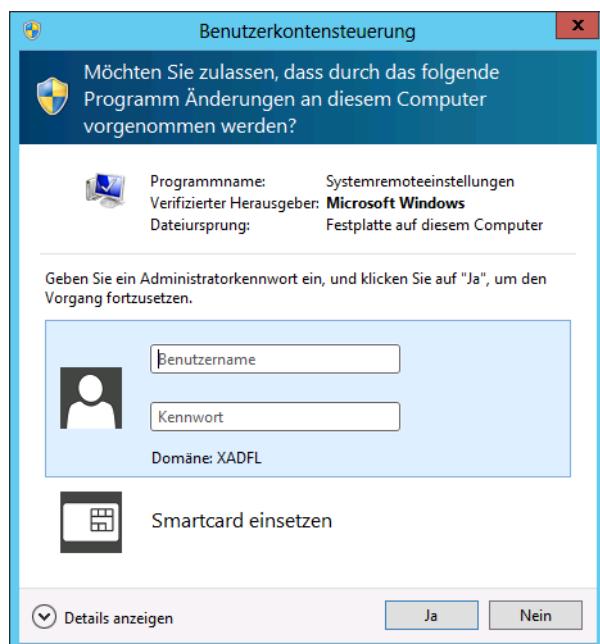


Abbildung 6.12 Eine Aufforderung der Benutzerkontensteuerung zur Eingabe von Anmeldeinformationen

Versucht ein Administrator, eine Aufgabe auszuführen, die administrative Zugriff erfordert, schaltet das System das Konto vom Standardbenutzertoken auf das administrative Token um. Dies ist der sogenannte *Administratorbestätigungsmodus*.

Bevor das System dem Benutzer erlaubt, das administrative Token zu nutzen, kann es vom menschlichen Benutzer eine Bestätigung verlangen, dass er tatsächlich eine administrative Aufgabe ausführen will. Dazu generiert das System eine Anhebungsaufforderung, wie sie

Abbildung 6.13 zeigt. Diese Bestätigung verhindert, dass nicht autorisierte Prozesse, wie sie beispielsweise durch Malware initiiert werden, auf das System mit Administratorrechten zugreifen.

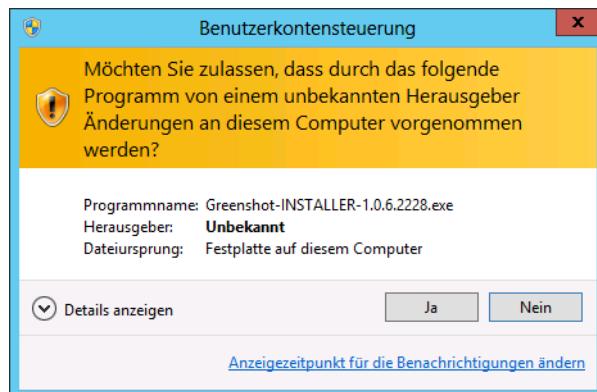


Abbildung 6.13 Eine Anhebungsaufforderung der Benutzerkontensteuerung

Sicherer Desktop

Wenn Windows Server 2012 eine Anhebungsaufforderung oder eine Aufforderung zur Eingabe von Anmeldeinformationen anzeigt, geschieht das standardmäßig über den sicheren Desktop.

Der sichere Desktop ist eine Alternative zum interaktiven Benutzerdesktop, den Windows normalerweise anzeigt. Generiert Windows Server 2012 eine Anhebungsaufforderung oder Aufforderung zur Eingabe von Anmeldeinformationen, wechselt das System zum sicheren Desktop, der alle anderen Desktopsteuerelemente deaktiviert und nur Windows-Prozesse erlaubt, die mit der Eingabeaufforderung interagieren. Dies soll verhindern, dass Malware automatisch eine Antwort auf die Anhebungsaufforderung oder Aufforderung zur Eingabe von Anmeldeinformationen geben kann und dadurch die menschliche Antwort umgehen würde.

Benutzerkontensteuerung konfigurieren

Windows Server 2012 aktiviert die Benutzerkontensteuerung standardmäßig, doch ist es möglich, ihre Eigenschaften zu konfigurieren und sie sogar vollständig zu deaktivieren. Über das Wartungscenter in der Systemsteuerung sind in Windows Server 2012 die folgenden vier Einstellungen für die Benutzerkontensteuerung verfügbar (siehe auch Abbildung 6.14):

- Immer benachrichtigen
- Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden
- Nur benachrichtigen, wenn Änderungen am Computer von Programmen vorgenommen werden (Desktop nicht abblenden)
- Nie benachrichtigen

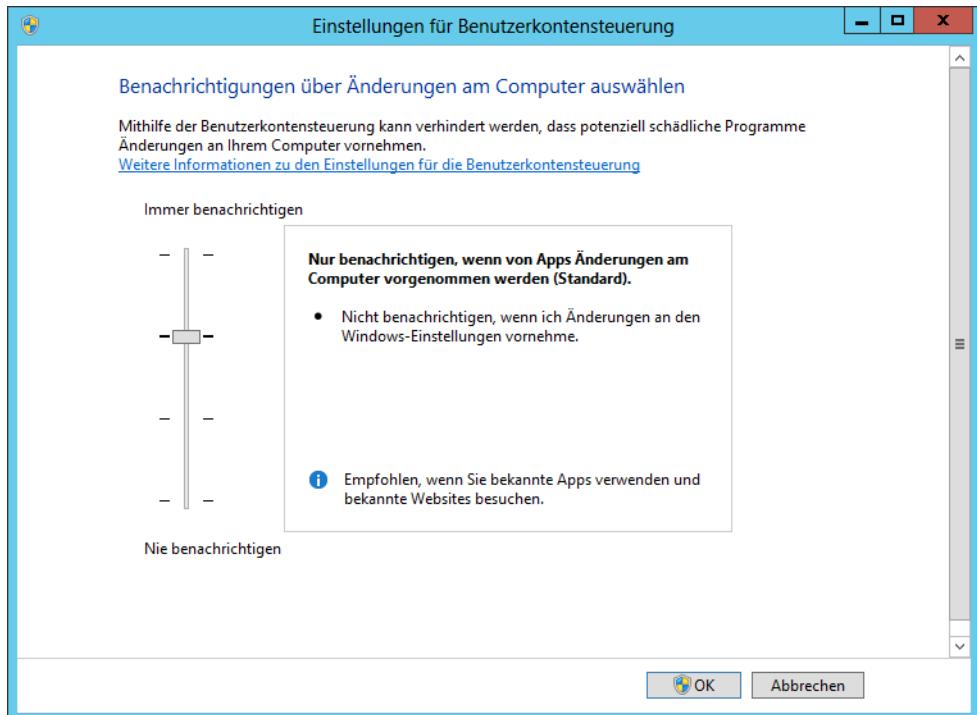


Abbildung 6.14 Das Dialogfeld *Einstellungen für Benutzerkontensteuerung*

Die Systemsteuerung erlaubt nur eine grobe Kontrolle der Benutzerkontensteuerung, eine feinstufige Anpassung der Eigenschaften für die Benutzerkontensteuerung ist über den Knoten *Sicherheitsoptionen* in *Gruppenrichtlinie* und *Lokale Sicherheitsrichtlinie* gegeben.

Prüfungszielzusammenfassung

- Die meisten Einstellungen, die sich auf Sicherheit beziehen, sind im Ordner *Windows-Einstellungen* im Knoten *Computerkonfiguration* eines Gruppenrichtlinienobjekts untergebracht
- Lokale Richtlinien regeln, welche Aktionen Benutzer auf einem bestimmten Computer ausführen dürfen, und bestimmen, ob die Aktionen in einem Ereignisprotokoll aufgezeichnet werden
- Überwachung lässt sich für erfolgreiche Anmeldeversuche, gescheiterte Anmeldeversuche oder beides konfigurieren
- Administratoren können mithilfe von Sicherheitsvorlagen lokale Richtlinien, Gruppenmitgliedschaften, Einstellungen für die Ereignisprotokollierung und andere Richtlinien konfigurieren

- Wenn ein Standardbenutzer eine Aufgabe ausführen möchte, die Administratorrechte voraussetzt, zeigt das System eine Aufforderung zur Eingabe von Anmeldeinformationen an, die vom Benutzer den Namen und das Kennwort für ein Konto mit Administratorrechten abfragt
- Die Benutzerkontensteuerung ist in allen Windows Server 2012-Installationen standardmäßig aktiviert, doch ist es möglich, über Gruppenrichtlinien ihre Eigenschaften zu konfigurieren und sie sogar vollständig zu deaktivieren

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Mit welchen der folgenden Tools stellen Sie die Einstellungen in einer Sicherheitsvorlage allen Computern in einer AD DS-Domäne bereit?
 - A. Active Directory-Benutzer und -Computer
 - B. Snap-In Sicherheitsvorlagen
 - C. Gruppenrichtlinienobjekt-Editor
 - D. Konsole *Gruppenrichtlinienverwaltung*
2. Welche der folgenden Gruppen sind lokale Gruppen, denen Sie über die Windows-Systemsteuerung Benutzer hinzufügen können? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Benutzer
 - B. Hauptbenutzer
 - C. Administratoren
 - D. Nichtadministratoren
3. Mit welchen der folgenden Tools ändern Sie die Eigenschaften in einer Sicherheitsvorlage?
 - A. Active Directory-Benutzer und -Computer
 - B. Snap-In *Sicherheitsvorlagen*
 - C. Gruppenrichtlinienobjekt-Editor
 - D. Konsole *Gruppenrichtlinienverwaltung*

4. Über welche der folgenden Mechanismen erhalten die integrierten lokalen Gruppen auf einem Windows Server 2012-Server ihre speziellen Fähigkeiten?
 - A. Sicherheitsoptionen
 - B. Windows-Firewall-Regeln
 - C. NTFS-Berechtigungen
 - D. Benutzerrechte
5. Was müssen Sie tun, bevor ein Windows Server 2012-Computer Anmeldeversuche bei Active Directory protokolliert, nachdem Sie die Richtlinie *Verzeichnisdienstzugriff überwachen* konfiguriert und bereitgestellt haben?
 - A. Über die Konsole *Active Directory-Benutzer und -Computer* müssen Sie die Active Directory-Objekte auswählen, die Sie überwachen möchten.
 - B. Sie müssen warten, bis die Überwachungsrichtlinieneinstellungen auf alle Domänencontroller im Netzwerk weitergeleitet sind.
 - C. Sie müssen das Eigenschaftenblatt *Verzeichnisdienstzugriff überwachen* öffnen und alle Active Directory-Objekte auswählen, die Sie überwachen möchten.
 - D. Dem Namen jedes Active Directory-Objekts, das Sie überwachen möchten, müssen Sie einen Unterstrich hinzufügen.



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Als Netzwerkadministrator planen Sie die Bereitstellung einer Sicherheitsvorlage in einem Netzwerk, das aus 100 Arbeitsstationen besteht. Die Arbeitsstationen laufen alle unter verschiedenen Versionen von Microsoft Windows mit folgender Aufteilung:

- Windows 7: 30 Arbeitsstationen
- Windows XP Professional: 40 Arbeitsstationen
- Windows XP Home Edition: 20 Arbeitsstationen
- Windows 2000 Professional: 10 Arbeitsstationen

In der Vergangenheit waren einige Computer im Netzwerk beeinträchtigt, da Endbenutzer die Sicherheitskonfigurationen ihrer Arbeitsstationen geändert hatten. Nun besteht Ihre Aufgabe darin, auf den Arbeitsstationen Ihre Sicherheitsvorlagen so bereitzustellen, dass Endbenutzer sie nicht mehr modifizieren können. Um dieses Ziel zu erreichen, wollen Sie die Vorlagen mithilfe einer Gruppenrichtlinie auf einem AD DS-OU-Objekt bereitstellen, das alle Arbeitsstationen enthält.

Beantworten Sie für das geschilderte Szenario die folgenden Fragen:

1. Wie viele Arbeitsstationen können ihre Einstellungen der Sicherheitsvorlage von einem Gruppenrichtlinienobjekt, das mit einem AD DS-Container verknüpft ist, nicht erhalten?
2. Mit welchen der folgenden Methoden können Sie Ihre Sicherheitsvorlagen auf den Arbeitsstationen bereitstellen, die keine Gruppenrichtlinien unterstützen, und trotzdem Ihre zugewiesenen Ziele erreichen?
 - A. Alle Computer, die keine Gruppenrichtlinien unterstützen, auf Windows 7 aktualisieren.
 - B. Das Snap-In *Sicherheitsvorlagen* auf jedem Computer ausführen und die passende Sicherheitsvorlage laden.
 - C. Ein Anmeldeskript erstellen, das mithilfe von *Secedit.exe* die Sicherheitsvorlage auf jedem Computer importiert.
 - D. Das Snap-In *Sicherheitskonfiguration und -analyse* auf jedem Computer ausführen und damit die passende Sicherheitsvorlage importieren.

Prüfungsziel 6.3: Richtlinien für Anwendungseinschränkungen konfigurieren

Die Optionen im Knoten *Richtlinien für Softwareeinschränkung* bieten Organisationen eine bessere Kontrolle, um die Ausführung von möglicherweise gefährlichen Anwendungen zu verhindern. Softwareeinschränkungsrichtlinien sind dafür konzipiert, Software zu erkennen und ihre Ausführung zu steuern. Zudem können Administratoren steuern, wer von den Richtlinien beeinflusst wird.

Dieses Prüfungsziel zeigt, wie Sie

- Regelerzwingung konfigurieren
 - AppLocker-Regeln konfigurieren
 - Richtlinien für Softwareeinschränkung konfigurieren
-

Richtlinien für Softwareeinschränkung

Der Knoten *Richtlinien für Softwareeinschränkung* befindet sich im Knoten *Windows-Einstellungen\Sicherheitseinstellungen* unter dem Knoten *Benutzerkonfiguration* oder *Computerkonfiguration* eines Gruppenrichtlinienobjekts. Standardmäßig ist der Ordner *Richtlinien für Softwareeinschränkung* leer. Wenn Sie eine neue Richtlinie definieren, erscheinen zwei Unterordner: *Sicherheitsstufen* und *Zusätzliche Regeln*. Im Ordner *Sicherheitsstufen* können Sie das Standardverhalten definieren, von dem alle Regeln erstellt werden. Die Kriterien für jedes ausführbare Programm werden im Ordner *Zusätzliche Regeln* definiert.

In den folgenden Abschnitten lernen Sie, wie Sie die Sicherheitsstufe für eine Softwareeinschränkungsrichtlinie festlegen und wie Sie Regeln definieren, die die Ausführung von Programmdateien steuern.

Einschränkungen erzwingen

Bevor Sie irgendwelche Regeln erstellen, die die Einschränkung oder die Zulassung von ausführbaren Dateien steuern, müssen Sie wissen, wie die Regeln standardmäßig arbeiten. Wenn eine Richtlinie keine Einschränkungen erzwingt, starten ausführbare Dateien basierend auf den Berechtigungen, die Benutzer oder Gruppen im NTFS-Dateisystem besitzen.

In Bezug auf die Verwendung von Richtlinien für Softwareeinschränkung müssen Sie Ihr Konzept bestimmen, um Einschränkungen zu erzwingen. Hierfür gibt es die drei folgenden grundlegenden Strategien:

- **Nicht eingeschränkt** Erlaubt die Ausführung aller Anwendungen mit Ausnahme derjenigen, die speziell ausgeschlossen werden
- **Nicht erlaubt** Verhindert die Ausführung aller Anwendungen mit Ausnahme derjenigen, die speziell zugelassen werden

- **Standardbenutzer** Verhindert die Ausführung aller Anwendungen, die Administratorenrechte benötigen, lässt aber die Ausführung von Programmen zu, die nur Ressourcen erfordern, die für normale Benutzer zugänglich sind

Für welches Konzept Sie sich entscheiden, hängt von den Anforderungen der jeweiligen Organisation ab. In der Voreinstellung enthält der Bereich *Richtlinien für Softwareeinschränkung* den Wert *Nicht eingeschränkt* für die Einstellung *Standardsicherheitsstufe*.

Zum Beispiel werden Sie in einer Hochsicherheitsumgebung nur bestimmte Anwendungen zur Ausführung zulassen wollen. In diesem Fall setzen Sie die Standardsicherheitsstufe auf *Nicht erlaubt*. Im Unterschied dazu dürften in einem weniger sicheren Netzwerk alle ausführbaren Dateien zugelassen sein, sofern Sie nichts anderes festlegen. Hier wäre der Wert der Standardsicherheitsstufe auf *Nicht eingeschränkt* zu belassen und Sie müssten eine Regel erstellen, um eine Anwendung zu identifizieren, bevor Sie sie deaktivieren könnten. Die Standardsicherheitsstufe können Sie modifizieren, um die Einstellung *Nicht erlaubt* wiederzuspiegeln. Da das System bei der Einstellung *Nicht erlaubt* davon ausgeht, dass alle Programme abgelehnt werden, sofern keine spezifische Regel ihre Ausführung erlaubt, kann diese Einstellung administrative Probleme bereiten, wenn sie nicht gründlich getestet ist. Deshalb sollten Sie alle Anwendungen testen, die Sie ausführen möchten, um sich von ihrer ordnungsgemäßen Funktion zu überzeugen.

Um die Einstellung *Standardsicherheitsstufe* auf *Nicht erlaubt* zu setzen, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei einem Windows Server 2012-Server unter einem Konto mit Domänenadministratorrechten an. Die Konsole *Server-Manager* wird geöffnet.
2. Im Menü *Tools* wählen Sie *Gruppenrichtlinienverwaltung*, um die Konsole *Gruppenrichtlinienverwaltung* zu öffnen.
3. Erweitern Sie den Gesamtstrukturcontainer und gehen Sie zu Ihrer Domäne. Erweitern Sie dann den Domänencontainer und wählen Sie den Ordner *Gruppenrichtlinienobjekte* aus. Auf der Registerkarte *Inhalt* erscheinen die Gruppenrichtlinienobjekte, die momentan in der Domäne vorhanden sind.
4. Klicken Sie mit der rechten Maustaste auf ein Gruppenrichtlinienobjekt und wählen Sie *Bearbeiten*. Ein Fenster *Gruppenrichtlinienverwaltungs-Editor* wird geöffnet.
5. Gehen Sie unter *Computerkonfiguration* oder *Benutzerkonfiguration* zum Knoten *Richtlinien für Softwareeinschränkung*.
6. Klicken Sie mit der rechten Maustaste auf *Richtlinien für Softwareeinschränkung* und wählen Sie *Neue Richtlinien für Softwareeinschränkung erstellen*. Es erscheinen die Ordner, die neue Richtlinien enthalten.
7. Doppelklicken Sie im Detailbereich auf *Sicherheitsstufen*. Das Kontrollhäkchen auf dem Symbol *Nicht eingeschränkt* weist auf die Standardeinstellung hin.
8. Klicken Sie mit der rechten Maustaste auf die Sicherheitsstufe *Nicht erlaubt* und wählen Sie im Kontextmenü den Eintrag *Als Standard*. Es erscheint ein Meldungsfeld *Richtlinien*

für Softwareeinschränkung mit einer Warnung in Bezug auf die Aktion, die Sie durchführen möchten.

9. Klicken Sie auf *Ja* und schließen Sie dann den *Gruppenrichtlinienverwaltungs-Editor* und die *Konsole Gruppenrichtlinienverwaltung*.

Damit haben Sie die Standardsicherheitsstufe für eine Softwareeinschränkungsrichtlinie geändert.

Regeln für Softwareeinschränkung konfigurieren

Die Funktionalität der Softwareeinschränkungsrichtlinien hängt in erster Linie von den Regeln ab, die Software identifizieren, und dann von den Regeln, die deren Nutzung steuern. Wenn Sie eine neue Richtlinie für Softwareeinschränkung erstellen, erscheint der Unterordner *Zusätzliche Regeln*. Hier lassen sich Regeln mit Bedingungen erstellen, unter denen Programme ausgeführt oder verweigert werden können. Diese Regeln setzen bei Bedarf die Einstellung für die Standardsicherheitsstufe außer Kraft.

Um eigene Regeln im Ordner *Zusätzliche Regeln* zu erstellen, verwenden Sie ein Dialogfeld wie es Abbildung 6.15 zeigt.

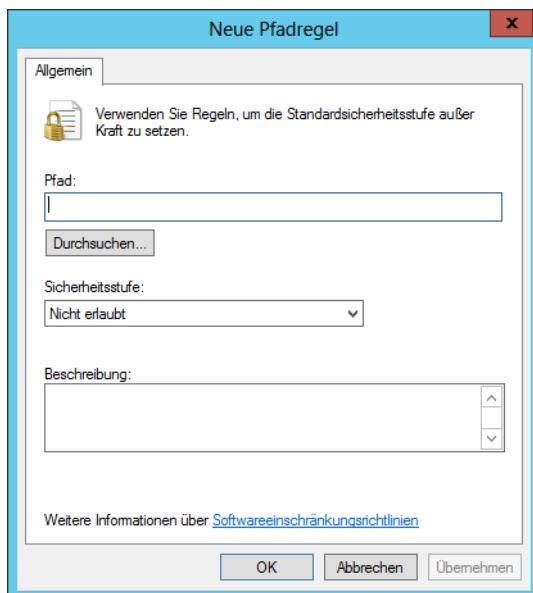


Abbildung 6.15 Das Dialogfeld *Neue Pfadregel*

Mit den folgenden vier Typen von Softwareeinschränkungsregeln können Sie festlegen, welche Programme in Ihrem Netzwerk ausgeführt werden dürfen oder nicht:

- Hashregeln
- Zertifikatregeln

- Pfadregeln
- Netzwerkzonenregeln

Daneben gibt es noch einen fünften Regeltyp – die Standardregel. Diese Regel wird wirksam, wenn eine Anwendung keiner der anderen Regeln, die Sie erstellt haben, entspricht. Um die Standardregel zu konfigurieren, wählen Sie eine der Richtlinien im Ordner *Sicherheitsstufen* aus und klicken auf deren Eigenschaftenblatt auf *Als Standard*.

Die folgenden Abschnitte erläutern die oben genannten vier Regeltypen.

Hashregeln

Ein Hashwert ist eine Folge von Bytes mit einer festen Länge, die ein Programm oder eine Datei eindeutig kennzeichnet. Generiert wird ein Hashwert durch einen Algorithmus, der quasi einen Fingerabdruck der Datei erzeugt und es nahezu unmöglich macht, dass ein anderes Programm den gleichen Hashwert liefert. Wenn Sie eine Hashregel erstellen und ein Benutzer ein von der Regel betroffenes Programm auszuführen versucht, vergleicht das System den Hashwert der ausführbaren Datei mit dem Hashwert, der in der Softwareeinschränkungsrichtlinie gespeichert ist. Stimmen beide überein, wird die Richtlinieneinstellung angewendet. Demzufolge verhindern Sie mit einem Hashwert für die ausführbare Datei einer Anwendung, dass die Anwendung bei nicht korrektem Hashwert ausgeführt wird. Da der Hashwert auf der Datei selbst basiert, funktioniert die Datei weiterhin, wenn Sie sie von einem Speicherort zu einem anderen verschieben. Wird aber die ausführbare Datei in irgendeiner Weise verändert, beispielsweise durch einen Wurm oder einen Virus modifiziert oder ersetzt, verhindert die Hashregel in der Softwareeinschränkungsrichtlinie die Ausführung der Datei.

Zertifikatregeln

Eine Zertifikatregel verwendet ein digitales Zertifikat, das mit einer Anwendung verknüpft ist, um ihre Rechtmäßigkeit zu bestätigen. Mithilfe von Zertifikatregeln können Sie die Ausführung von Software zulassen, wenn sie von einer vertrauenswürdigen Quelle kommt, oder verhindern, wenn sie aus einer nicht vertrauenswürdigen Quelle stammt. Außerdem lassen sich Zertifikatregeln verwenden, um Programme in nicht zugelassenen Bereichen des Betriebssystems auszuführen.

Pfadregeln

Eine Pfadregel identifiziert Software über den Verzeichnispfad, in dem die Anwendung im Dateisystem gespeichert ist. Mithilfe von Pfadregeln lassen sich Ausnahmen definieren, die die Ausführung einer Anwendung erlauben, wenn die Standardsicherheitsstufe für Softwareeinschränkungsrichtlinien auf *Nicht erlaubt* gesetzt ist. Oder Sie verhindern damit die Ausführung einer Anwendung, wenn die Standardsicherheitsstufe für Softwareeinschränkungsrichtlinien auf *Nicht eingeschränkt* gesetzt ist.

Pfadregeln können entweder einen Speicherort im Dateisystem spezifizieren, wo Anwendungsdateien gespeichert sind, oder eine Registrierungspfadeinstellung. Registrierungspfadregeln gewährleisten, dass die ausführbare Datei einer Anwendung gefunden wird. Wenn zum Beispiel ein Administrator mit einer Pfadregel einen Dateisystemspeicherort für eine

Anwendung definiert und die Anwendung an einen neuen Speicherort verschoben wird, wie es beispielsweise bei der Umstrukturierung eines Netzwerks vorkommt, ist der ursprüngliche Pfad in der Pfadregel nicht mehr gültig. Besagt die Pfadregel, dass die Anwendung nur dann funktioniert, wenn sie sich in einem bestimmten Pfad befindet, lässt sich das Programm von seinem neuen Speicherort nicht mehr ausführen. Dies könnte eine erhebliche Sicherheitsverletzung nach sich ziehen, wenn das Programm auf vertrauliche Informationen verweist.

Wenn Sie dagegen in der Pfadregel den Speicherort eines Registrierungsschlüssels angeben, wirkt sich ein geänderter Speicherort der Anwendungsdateien nicht auf das Ergebnis der Regel aus. Denn wenn Sie eine Anwendung verschieben, wird der Registrierungsschlüssel, der auf die Dateien der Anwendung verweist, automatisch aktualisiert.

Netzwerkzonenregeln

Netzwerkzonenregeln gelten nur für Windows Installer-Pakete, die eine Installation von einer festgelegten Zone versuchen, beispielsweise von einem lokalen Computer, einem lokalen Intranet, vertrauenswürdigen Sites, eingeschränkten Sites oder aus dem Internet. Mit diesem Regeltyp können Sie für Windows Installer-Pakete festlegen, dass sie nur installiert werden, wenn sie aus einem vertrauenswürdigen Bereich des Netzwerks kommen. Zum Beispiel könnte eine Netzwerkzonenregel verhindern, dass Windows Installer-Pakete aus dem Internet oder anderen Netzwerkstandorten heruntergeladen und installiert werden.

Mehrere Regeln verwenden

Eine Softwareeinschränkungsregel lässt sich mithilfe mehrerer Regeltypen definieren, um die Programmausführung zuzulassen bzw. nicht zuzulassen. Indem Sie mehrere Regeltypen einsetzen, können Sie die verschiedensten Sicherheitsstufen realisieren. Zum Beispiel können Sie mit einer Pfadregel verhindern, dass Programme aus dem freigegebenen Ordner `\Server\Accounting` ausgeführt werden, und mit einer weiteren Pfadregel die Ausführung von Programmen aus dem freigegebenen Ordner `\Server\Application` erlauben. Außerdem können Sie Zertifikateregeln und Hashregeln in Ihre Richtlinie einbinden. Wenn Sie mehrere Regeltypen implementieren, wenden die Systeme die Regeln entsprechend der folgenden Rangfolge an:

1. Hashregeln
2. Zertifikateregeln
3. Netzwerkzonenregeln
4. Pfadregeln

Tritt ein Konflikt zwischen den Regeltypen auf, etwa zwischen einer Hashregel und einer Pfadregel, setzt sich die Hashregel durch, da sie in der Rangfolge höher steht. Bei Konflikten zwischen zwei Regeln desselben Typs und den gleichen Identifizierungseinstellungen – beispielsweise zwei Pfadregeln, die Software aus demselben Verzeichnis identifizieren – wird die restriktivere Einstellung angewendet. Wenn in diesem Fall die eine Pfadregel auf *Nicht eingeschränkt* und die andere auf *Nicht erlaubt* gesetzt ist, wird die Richtlinie mit der Einstellung *Nicht erlaubt* erzwungen.

Eigenschaften von Softwareeinschränkung konfigurieren

Im Ordner *Richtlinien für Softwareeinschränkung* können Sie drei spezifische Eigenschaften konfigurieren, um zusätzliche Einstellungen bereitzustellen, die bei der Implementierung für alle Richtlinien gelten. Diese drei Eigenschaften – *Erzwingen*, *Designierte Dateitypen* und *Vertrauenswürdige Herausgeber* – werden in den folgenden Abschnitten beschrieben.

Erzwingen

Wie Abbildung 6.16 zeigt, können Sie im Dialogfeld *Eigenschaften von Erzwingen* festlegen, ob die Richtlinien auf alle Dateien angewendet oder ob Bibliotheksdateien wie zum Beispiel DLLs ausgeschlossen werden sollen. Die Standardeinstellung schließt DLLs aus. Dies ist die praktischste Methode für Erzwingen. Ist zum Beispiel die Standardsicherheitsstufe für die Richtlinie auf *Nicht erlaubt* und die *Eigenschaften von Erzwingen* auf *Alle Softwaredateien* gesetzt, müssten Sie eine Regel definieren, die jede DLL prüft, bevor sich das Programm zulassen oder ablehnen ließe. Wenn Sie dagegen die Standardeinstellung für *Eigenschaften von Erzwingen* übernehmen und DLLs ausschließen, braucht kein Administrator individuelle Regeln für jede DLL-Datei zu definieren.

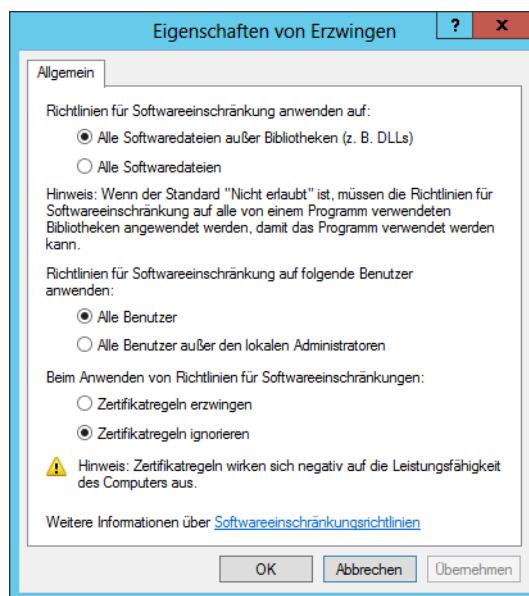


Abbildung 6.16 Eigenschaften von Erzwingen konfigurieren

Designierte Dateitypen

Die *Eigenschaften von Designierte Dateitypen* im Ordner *Richtlinien für Softwareeinschränkung* geben die Dateitypen an, die als ausführbar betrachtet werden (siehe Abbildung 6.17). Dateitypen, die als ausführbare Dateien oder Programmdateien designiert sind, werden von allen Regeln gemeinsam verwendet, obwohl Sie auch eine Liste für eine Computerrichtlinie angeben können, die sich von einer Liste für eine Benutzerrichtlinie unterscheidet.

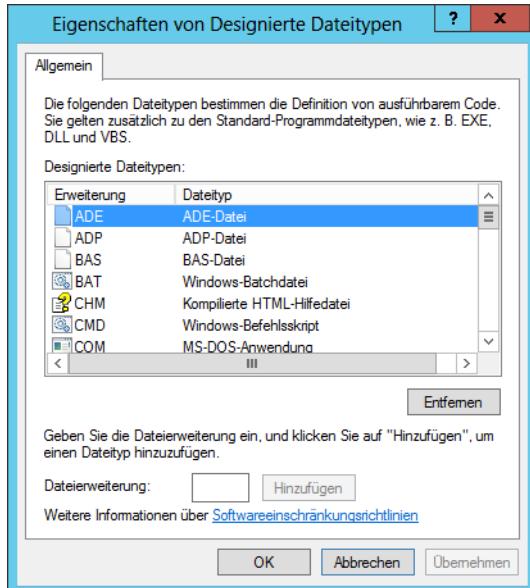


Abbildung 6.17 Eigenschaften von Designierte Dateitypen konfigurieren

Vertrauenswürdige Herausgeber

Schließlich kann der Administrator mit den *Eigenschaften von Vertrauenswürdigen Herausgebern* steuern, wie das System Zertifikatsregeln verarbeitet. Im Dialogfeld *Eigenschaften von Vertrauenswürdigen Herausgebern* (siehe Abbildung 6.18) legen Sie mit der ersten Einstellung fest, welche Benutzer die vertrauenswürdigen Zertifikatquellen verwalten dürfen. In der Standardeinstellung haben Administratoren des lokalen Computers das Recht, vertrauenswürdige Herausgeber auf dem lokalen Computer anzugeben, und Organisationsadministratoren dürfen vertrauenswürdige Herausgeber in einer Organisationseinheit festlegen. Unter dem Aspekt der Sicherheit sollte es Benutzern in einem Hochsicherheitsnetzwerk nicht erlaubt sein, die Quellen auszuwählen, von denen Zertifikate bezogen werden können.

Im Dialogfeld *Eigenschaften von Vertrauenswürdige Herausgeber* können Sie auch eine Überprüfung aktivieren, ob ein Zertifikat widerrufen wurde. Bei einem widerrufenen Zertifikat sollte es dem Benutzer nicht erlaubt werden, auf Netzwerkressourcen zuzugreifen. Als Optionen können Sie den Herausgeber oder den Zeitstempel des Zertifikats überprüfen lassen, um festzustellen, ob es widerrufen wurde.

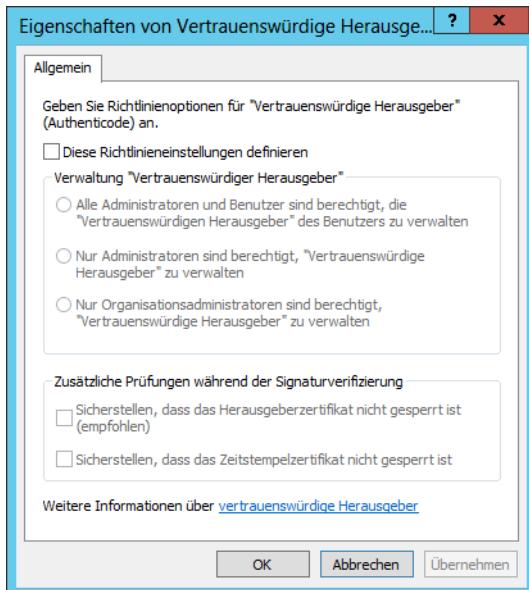


Abbildung 6.18 Eigenschaften von Vertrauenswürdige Herausgeber konfigurieren

AppLocker verwenden

Richtlinien für Softwareeinschränkung sind zwar recht leistungsfähig, können aber auch jede Menge zusätzlichen Verwaltungsaufwand erfordern. Wenn Sie alle Anwendungen verbieten wollen, außer denjenigen, die den erstellten Regeln entsprechen, haben Sie es mit vielen Programmen in Windows Server 2012 zu tun, die selbst Regeln benötigen. Dazu kommen noch die Anwendungen, die Sie installieren möchten. Administratoren müssen die Regeln manuell definieren, was eine beschwerliche Arbeit bedeuten kann.

Das Windows-Feature AppLocker, auch als Anwendungssteuerungsrichtlinien bezeichnet, ist prinzipiell eine aktualisierte Version des Konzepts, das in Richtlinien für Softwareeinschränkung implementiert ist. Zwar stützt sich AppLocker ebenfalls auf Regeln, die Administratoren zu verwalten haben, doch ist das Erstellen der Regeln dank einer assistentenbasierten Oberfläche wesentlich einfacher.

Zudem ist AppLocker flexibler als die Richtlinien für Softwareeinschränkung. Sie können AppLocker-Regeln auf bestimmte Benutzer und Gruppen anwenden und auch Regeln erstellen, die alle zukünftigen Versionen einer Anwendung unterstützen. Nachteilig bei AppLocker ist vor allem, dass sich die Richtlinien nur auf Computer unter Windows 7 und Windows Server 2008 R2 oder neuer anwenden lassen.

Regeltypen von AppLocker

Die AppLocker-Einstellungen sind in Gruppenrichtlinienobjekten untergebracht, und zwar im Container *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Anwendungssteuerungsrichtlinien\AppLocker*, wie Abbildung 6.19 zeigt.

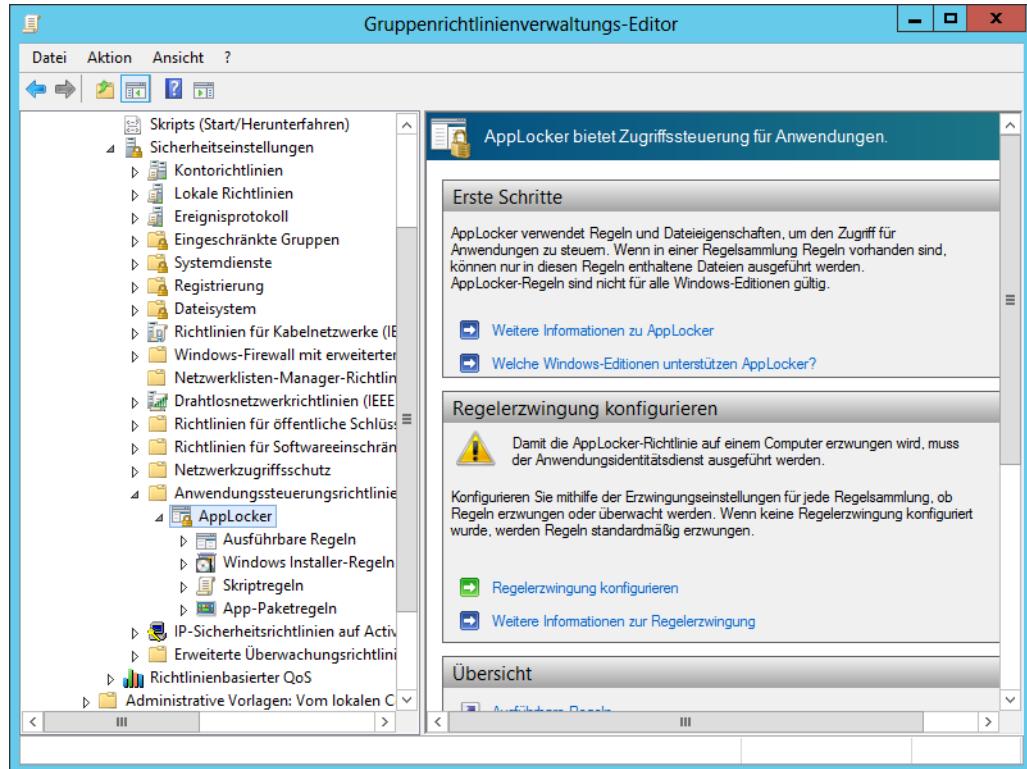


Abbildung 6.19 Der *AppLocker*-Container in einem Gruppenrichtlinienobjekt

Der *AppLocker*-Container enthält vier Knoten mit den folgenden grundlegenden Regeltypen:

- **Ausführbare Regeln** Enthält Regeln, die auf Dateien mit den Erweiterungen *.exe* und *.com* angewendet werden
- **Windows Installer-Regeln** Enthält Regeln, die auf Windows Installer-Pakete mit den Erweiterungen *.msi* und *.msp* angewendet werden
- **Skriptregeln** Enthält Regeln, die auf Skriptdateien mit den Erweiterungen *.ps1*, *.bat*, *.cmd*, *.vbs* und *.js* angewendet werden
- **App-Paketregeln** Enthält Regeln, die auf Anwendungen, die über den Windows Store gekauft wurden, angewendet werden

Jede Regel, die Sie in den einzelnen Containern erstellen, kann den Zugriff auf bestimmte Ressourcen abhängig von den folgenden Kriterien zulassen oder blockieren:

- **Herausgeber** Identifiziert codesignierte Anwendungen anhand einer digitalen Signatur, die aus einer Anwendungsdatei extrahiert wird. Es lassen sich auch Herausgeberregeln erstellen, die auf alle zukünftigen Versionen einer Anwendung angewendet werden.

- **Pfad** Identifiziert Anwendungen anhand eines Datei- oder Ordnernamens. Das potenzielle Sicherheitsrisiko dieses Regeltyps besteht darin, dass jede Datei der Regel entsprechen kann, solange es sich um den korrekten Namen oder Speicherort handelt.
- **Dateihash** Identifiziert Anwendungen anhand eines digitalen Fingerabdrucks, der auch gültig bleibt, selbst wenn sich der Name oder der Speicherort der ausführbaren Datei ändert. Dieser Regeltyp funktioniert ähnlich wie sein Äquivalent in Richtlinien für Softwareeinschränkung. Allerdings ist es in AppLocker wesentlich einfacher, Regeln zu erstellen und Dateihashes zu generieren.

Standardregeln erstellen

Normalerweise blockiert AppLocker alle ausführbaren Dateien, Installer-Pakete und Skripts mit Ausnahme derjenigen, für die *Zulassen*-Regeln definiert sind. Um also AppLocker einzusetzen, müssen Sie Regeln erstellen, die Benutzer in die Lage versetzen, auf die Dateien zuzugreifen, die für die Ausführung von Windows- und die installierten Anwendungen des Systems erforderlich sind. Am einfachsten lässt sich das bewerkstelligen, wenn Sie mit der rechten Maustaste auf jeden der vier Regelcontainer klicken und im Kontextmenü den Eintrag *Standardregeln erstellen* wählen.

Die Standardregeln für jeden Container können Sie bei Bedarf replizieren, modifizieren oder löschen. Außerdem haben Sie die Möglichkeit, eigene Regeln zu erstellen, solange Sie genau darauf achten, den Zugriff auf alle Ressourcen zu gewähren, die der Computer für die Ausführung von Windows benötigt.



Wichtig AppLocker-Richtlinien anwenden

Für die Funktion von AppLocker setzt Windows Server 2012 voraus, dass der Dienst *Anwendungsidentität* ausgeführt wird. In der Voreinstellung verwendet dieser Typ den *Starttyp Manuell*, sodass Sie den Dienst in der Konsole *Dienste* selbst starten müssen, bevor Windows die AppLocker-Richtlinien anwenden kann.

Regeln automatisch erstellen

Der größte Vorteil von AppLocker gegenüber Richtlinien für Softwareeinschränkung ist die Fähigkeit, Regeln automatisch erstellen zu lassen. Wenn Sie mit der rechten Maustaste auf einen der Regelcontainer klicken und im Kontextmenü *Regeln automatisch generieren wählen*, startet der Assistent zum automatischen Generieren von Regeln.

Nachdem Sie den zu analysierenden Ordner und die Benutzer oder Gruppen, auf die die Regeln angewendet werden sollen, festgelegt haben, erscheint eine Seite *Regeleinstellungen*, auf der Sie die Typen der zu erstellenden Regeln spezifizieren können. Der Assistent zeigt dann eine Zusammenfassung seiner Ergebnisse auf der Seite *Regeln prüfen* an und fügt die Regeln in den Container ein.

Regeln manuell erstellen

Regeln können Sie nicht nur automatisch erstellen lassen, sondern auch manuell über eine assistentenbasierte Oberfläche definieren. Wählen Sie dazu im Kontextmenü für einen der Regelcontainer den Eintrag *Neue Regel erstellen*.

Der Assistent fragt die folgenden Informationen ab:

- **Aktion** Gibt an, ob Sie dem Benutzer oder der Gruppe den Zugriff auf die Ressource gewähren oder verweigern wollen. In AppLocker überschreiben explizite *Verweigern*-Regeln immer die *Zulassen*-Regeln.
- **Benutzer oder Gruppe** Gibt den Namen des Benutzers oder der Gruppe an, auf den/die die Richtlinie angewendet werden soll
- **Bedingungen** Gibt an, ob Sie eine Herausgeber-, Pfad- oder Dateihashregel erstellen möchten. Der Assistent generiert eine zusätzliche Seite für die gewählte Option, auf der Sie deren Parameter konfigurieren können.
- **Ausnahmen** Erlaubt es, Ausnahmen für die zu erstellende Regel anzugeben, wobei Sie eine der drei Bedingungen *Herausgeber*, *Pfad* oder *Dateihash* verwenden können

Prüfungszielzusammenfassung

- Richtlinien für Softwareeinschränkung erlauben es, den ausführbaren Code der Software zu identifizieren und seine Ausführung im Netzwerk entweder zuzulassen oder zu verbieten
- Die drei Standardsicherheitsstufen in den Richtlinien für Softwareeinschränkung sind *Nicht eingeschränkt*, bei der alle Anwendungen basierend auf Benutzerberechtigungen funktionieren, *Nicht erlaubt*, bei der die Ausführung aller Anwendungen unabhängig von den Benutzerberechtigungen verweigert wird, und *Standardbenutzer*, die die Ausführung nur derjenigen ausführbaren Dateien ermöglicht, die sich von normalen Benutzern ausführen lassen
- In einer Richtlinie für Softwareeinschränkung lassen sich vier Regeltypen definieren. In der Prioritätsreihenfolge sind das Hash-, Zertifikat-, Internetzonen- und Pfadregeln. Die für eine bestimmte Regel festgelegte Sicherheitsstufe setzt die Standardsicherheitsstufe der Richtlinie außer Kraft.
- Richtlinien für Softwareeinschränkung sind Gruppenrichtlinieneinstellungen, für die Administratoren mit Regeln verschiedener Typen steuern können, welche Programme auf Arbeitsstationen ausgeführt werden dürfen
- Mithilfe von AppLocker können Administratoren Regeln für die Anwendungseinschränkung wesentlich einfacher als bisher erstellen

Lernzielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Lernziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welche der folgenden Regeln gehört nicht zu den Regeltypen für Softwareeinschränkung, die von Windows Server 2012 unterstützt werden?
 - A. Hashregeln
 - B. Zertifikatregeln
 - C. Pfadregeln
 - D. Firewallregeln
2. Welche der folgenden Strategien zum Erzwingen von Softwareeinschränkung verhindern die Ausführung aller ausführbaren Dateien, außer denjenigen, die ein Administrator explizit zugelassen hat?
 - A. Standardbenutzer
 - B. Nicht erlaubt
 - C. Hauptbenutzer
 - D. Nicht eingeschränkt
3. Unter welchen der folgenden Bedingungen wird eine Hashregel in einer Richtlinie für Softwareeinschränkung nicht mehr funktionieren? (Wählen Sie alle zutreffenden Antworten aus.)
 - A. Wenn Sie die Datei, auf der der Hashwert basiert, in einen anderen Ordner verschieben.
 - B. Wenn Sie die Datei, auf der der Hashwert basiert, auf eine neue Version aktualisieren.
 - C. Wenn die Datei, auf der der Hashwert basiert, durch einen Virus modifiziert wird.
 - D. Wenn Sie die Berechtigungen für die Datei, auf der der Hashwert basiert, ändern.
4. Welche der folgenden Regeltypen betrifft Dateien mit der Erweiterung *.msi*?
 - A. Ausführbare Regeln
 - B. Windows Installer-Regeln
 - C. Skriptregeln
 - D. App-Paketregeln

5. Welchen der folgenden Dienste müssen Sie manuell starten, bevor Windows die AppLocker-Richtlinien anwenden kann?
 - A. Anwendungsidentität
 - B. Anwendungsverwaltung
 - C. Anmeldeinformationsverwaltung
 - D. Netzwerkkonnektivitäts-Assistent



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Lernziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Sophie hat vor, per AppLocker den Zugriff auf Anwendungen in einem neuen Netzwerk zu steuern, das sie für die Abteilung *Forschung und Entwicklung* eines großen Luft- und Raumfahrtunternehmens eingerichtet hat. Die Softwareentwickler in der Abteilung haben kürzlich eine neue Anwendung namens Virtual Wind Tunnel bereitgestellt, die auf einem Regierungsprojekt beruht und dementsprechend klassifiziert ist. Alle vollbeschäftigte Mitarbeiter besitzen eine Unbedenklichkeitsbescheinigung, um mit der Anwendung zu arbeiten, die Praktikanten in der Abteilung jedoch nicht. Sophie hat die Benutzerkonten aller Personen der Abteilung in eine Sicherheitsgruppe *ResDev* gestellt. Die Praktikanten sind außerdem Mitglieder der Gruppe *RDint*.

Wie kann Sophie AppLocker einsetzen, um jedem in der Abteilung den Zugriff auf die Anwendung Virtual Wind Tunnel zu gewähren, ohne die Gruppenmitgliedschaften zu ändern und ohne Richtlinien auf einzelne Benutzer anwenden zu müssen?

Prüfungsziel 6.4: Windows-Firewall konfigurieren

Vielleicht haben Sie die Tür zum Rechenzentrum verschlossen, in dem die Server stehen, doch die Computer sind immer noch mit dem Netzwerk verbunden. Ein Netzwerk ist wie eine andere Art von Tür, oder vielmehr wie eine Folge von Türen, durch die Daten herein- und hinausgehen. Um Ihren Benutzern Dienste anbieten zu können, müssen diese Türen zumindest zeitweise geöffnet sein, doch haben die Serveradministratoren zu gewährleisten, dass nur die richtigen Türen geöffnet bleiben.

Eine Firewall ist ein Programm, das einen Computer oder ein Netzwerk schützt, indem es bestimmte Arten von Netzwerkdatenverkehr vom und zum System durchlässt und anderen Datenverkehr blockiert. Praktisch realisiert eine Firewall eine Reihe von Filtern, die den Inhalt von Paketen und die Muster des Datenverkehrs vom und zum Netzwerk untersuchen, um zu ermitteln, welche Pakete passieren dürfen.

Ziel einer Firewall ist es, sämtlichen Datenverkehr, den legitime Benutzer für die ihnen zugewiesenen Aufgaben benötigen, zu erlauben und alles andere zu sperren. Wenn Sie mit Firewalls arbeiten, haben Sie mit Themen wie Authentifizierung und Autorisierung nichts zu tun. Diese Mechanismen steuern, wer durch die geöffneten Servertüren gehen darf. Dagegen bestimmt die Firewall, welche Türen geöffnet bleiben sollen und welche dichtzuhalten sind.

Dieses Prüfungsziel zeigt, wie Sie

- Regeln für mehrere Profile per Gruppenrichtlinie konfigurieren
 - Verbindungssicherheitsregeln konfigurieren
 - die Windows-Firewall konfigurieren, um Anwendungen, Bereiche, Ports und Benutzer zuzulassen oder zu verweigern
 - authentifizierte Firewallausnahmen konfigurieren
 - Einstellungen importieren und exportieren
-

Windows-Firealleinstellungen

Windows Server 2012 bringt ein Firewallprogramm namens Windows-Firewall mit, das auf allen Systemen standardmäßig aktiviert ist. In der Standardkonfiguration sperrt die Windows-Firewall den meisten eingehenden Datenverkehr des Computers. Firewalls untersuchen den Inhalt jedes Pakets, das den Computer erreicht oder verlässt, und vergleichen die gefundenen Informationen mit einer Reihe von Regeln. Diese Regeln legen fest, welche Pakete die Firewall passieren dürfen und welche gesperrt werden.

Windows-Systeme kommunizieren über das Protokoll TCP/IP (Transmission Control Protocol/Internet Protocol). Dabei werden Anwendungsdaten über eine Reihe von geschichteten Protokollen gepackt, die definieren, woher die Daten kommen und wohin sie gehen. In den Firewallregeln lassen sich vor allem die folgenden drei Kriterien verwenden:

- **IP-Adressen** IP-Adressen identifizieren bestimmte Hosts im Netzwerk. Eine Firewall lässt sich auf Basis der IP-Adressen so konfigurieren, dass nur der Datenverkehr von und zu bestimmten Computern oder Netzwerken passieren darf.
- **Protokollnummern** Protokollnummern geben an, ob das Paket TCP- oder UDP (User Datagram Protocol)-Daten enthält. Wenn Sie einen Filter nach Protokollnummern einrichten, können Sie Pakete sperren, die bestimmte Arten von Datenverkehr enthalten. Windows-Computer verwenden in der Regel UDP für einen kurzen Nachrichtenaustausch, wie er beispielsweise bei DNS (Domain Name System)- und DHCP (Dynamic Host Configuration Protocol)-Transaktionen vorkommt. TCP-Pakete übertragen normalerweise größere Datenmengen, wie beispielsweise beim Datenaustausch mit Web-, Datei- und Druckservern.
- **Portnummern** Portnummern identifizieren bestimmte Anwendungen, die auf dem Computer laufen. Die gebräuchlichsten Firewallregeln spezifizieren mit Portnummern die Arten des Anwendungsdatenverkehrs, den der Computer senden und empfangen darf. Zum Beispiel empfängt ein Webserver die eingehenden Pakete normalerweise auf Port Nummer 80. Sofern die Firewall keine Regel hat, die Port 80 für eingehenden Datenverkehr öffnet, kann der Webserver in seiner Standardkonfiguration nicht funktionieren.

Firewallregeln können auf zwei Arten wie folgt funktionieren:

- Den gesamten Datenverkehr zulassen, bis auf den, der den angewendeten Regeln entspricht
- Den gesamten Datenverkehr sperren, bis auf den, der den angewendeten Regeln entspricht

Im Allgemeinen ist es sicherer, den gesamten Datenverkehr standardmäßig zu sperren. Vom Standpunkt des Serveradministrators aus beginnen Sie mit einem vollkommen gesperrten System und fangen dann an, Ihre Anwendungen zu testen. Funktioniert eine Anwendung nicht ordnungsgemäß, weil der Netzwerkzugriff gesperrt ist, können Sie mit einer Regel die Ports öffnen, die die Anwendung für die Kommunikation benötigt. Die ist die Methode, die die Windows-Firewall standardmäßig für eingehenden Netzwerkdatenverkehr verwendet. In der Firewall sind Standardregeln vorkonfiguriert, die den Datenverkehr zulassen, den standardmäßige Windows-Netzwerkfunktionen verwenden, beispielsweise die Datei- und Druckerfreigabe. Für ausgehenden Netzwerkdatenverkehr verwendet die Windows-Firewall die zweite Methode, lässt also den gesamten Datenverkehr die Firewall passieren, bis auf den, der einer Regel entspricht.

Mit der Windows-Firewall arbeiten

Die Windows-Firewall ist ein einzelnes Programm mit einem Satz von Regeln. Es gibt aber zwei unterschiedliche Benutzeroberflächen, über die Sie die Firewall verwalten und überwachen können. Die Windows-Firewall-Systemsteuerung bietet eine vereinfachte Benutzeroberfläche, bei der sich Administratoren nicht mit den Details von Regeln und Portnummern befassen müssen. Möchten Sie lediglich die Firewall aktivieren oder deaktivieren (was normalerweise beim Testen oder bei der Problembehebung der Fall ist) oder mit Firewalleinstellungen für eine bestimmte Windows-Rolle oder ein Windows-Feature

arbeiten, genügt die Version der Systemsteuerung. Für einen vollständigen Zugriff auf Firewallregeln und komplexere Funktionen müssen Sie die Konsole *Windows-Firewall mit erweiterter Sicherheit* verwenden. Dazu später mehr.

In vielen Fällen brauchen Administratoren niemals mit der Windows-Firewall direkt zu arbeiten. Viele Rollen und Features von Windows Server 2012 öffnen bei ihrer Installation automatisch die geeigneten Firewallports. In anderen Situationen warnt das System Sie in Bezug auf Firewallprobleme.

Wenn Sie zum Beispiel den Datei-Explorer zum ersten Mal öffnen und versuchen, auf das Netzwerk zuzugreifen, erscheint eine Warnung mit dem Hinweis, dass Netzwerkerkennung und Dateifreigabe deaktiviert sind und Sie daran hindern, das Netzwerk zu durchsuchen.

Die Netzwerkerkennung ist lediglich ein Satz von Firewallregeln, die die Ports regulieren, die Windows für die Suche im Netzwerk verwendet, konkret die Ports 137, 138, 1900, 2869, 3702, 5355, 5357 und 5358. Standardmäßig deaktiviert Windows Server 2012 eingehende Regeln, die mit diesen Ports verknüpft sind, sodass die Ports geschlossen sind und den gesamten Datenverkehr durch sie sperren. Wenn Sie auf die Warnung klicken und im Kontextmenü *Netzwerkerkennung und Dateifreigabe aktivieren* wählen, aktivieren Sie praktisch diese Firewallregeln und öffnen dabei die damit verknüpften Ports.

Außer mit den Menübefehlen, die über die Warnung zugänglich sind, können Sie die Regeln für Netzwerkerkennung und Dateifreigabe auch auf andere Art steuern. Das *Netzwerk- und Freigabecenter* der Systemsteuerung bietet auf der Seite *Erweiterte Freigabeeinstellungen* Optionen, über die Sie Netzwerkerkennung, Dateifreigabe und andere grundlegende Netzwerkfunktionen ein- und ausschalten.

Die Windows-Firewall-Systemsteuerung enthält den Link *Eine App oder ein Feature durch die Windows-Firewall zulassen*, der zum Dialogfeld *Zugelassene Apps* führt. Über das Kontrollkästchen *Netzwerkerkennung* in diesem Dialogfeld können Sie den gleichen Satz von Regeln steuern wie über die Netzwerkerkennung der Systemsteuerung im *Netzwerk- und Freigabecenter*.

Schließlich können Sie über die Konsole *Windows-Firewall mit erweiterter Sicherheit* direkt auf einzelne Regeln der Netzwerkerkennung zugreifen. Wenn Sie den Knoten *Eingehende Regeln* auswählen und in der Liste nach unten scrollen, finden Sie neun verschiedene Netzwerkerkennungsregeln.

Wie ein näherer Blick auf die Regeln in der Konsole zeigt, ist die Netzwerkerkennung eine komplexe Windows-Funktion, die nur schwer in den Griff zu bekommen wäre, wenn Sie durch Ausprobieren die verwendeten Ports ermitteln müssten. Deshalb umfasst die Windows-Firewall eine umfangreiche Regelsammlung, um die Ports zu verwalten, die Anwendungen und Dienste des Betriebssystems für einen ordnungsgemäßen Ablauf benötigen.

Die Windows-Firewall-Systemsteuerung

Die Windows-Firewall-Systemsteuerung bietet den einfachsten und sichersten Zugriff auf die Steuerelemente der Firewall. Für die meisten Serveradministratoren sind diese Steuerelemente normalerweise ausreichend, sofern das System keine speziellen Anforderungen stellt oder Sie mit speziellen Serveranwendungen arbeiten.

Wenn Sie das Fenster *Windows-Firewall* über die Systemsteuerung öffnen (siehe Abbildung 6.20), erfahren Sie

- ob der Computer mit einem Domänen-, privaten oder öffentlichen Netzwerk verbunden ist,
- ob der Dienst *Windows-Firewall* derzeit eingeschaltet ist,
- ob eingehende und ausgehende Verbindungen blockiert sind,
- den Namen des derzeit aktiven Netzwerks und
- ob Benutzer benachrichtigt werden, wenn ein Programm blockiert wird.

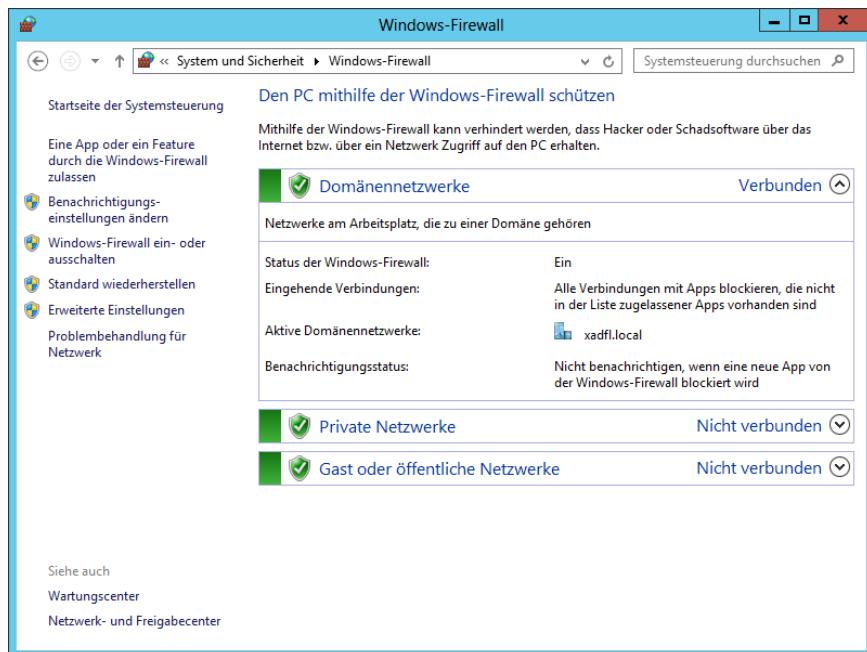


Abbildung 6.20 Die Windows-Firewall-Systemsteuerung

Die Links im linken Fensterbereich bieten die folgenden Funktionen:

- **Eine App oder ein Feature durch die Windows-Firewall zulassen** Öffnet das Dialogfeld *Zugelassene Apps*, in dem Sie die Anwendungen auswählen können, die Datenverkehr durch die Firewall senden dürfen
- **Benachrichtigungseinstellungen ändern** Öffnet das Dialogfeld *Einstellungen anpassen*, indem Sie die Benachrichtigungseinstellungen für jedes der drei Profile bearbeiten können
- **Windows-Firewall ein- oder ausschalten** Öffnet das Dialogfeld *Einstellungen anpassen*, in dem Sie den Status der Firewall in jedem der drei Profile aktivieren bzw. deaktivieren können

- **Standard wiederherstellen** Setzt sämtliche Firewalleinstellungen auf ihre Installationswerte zurück
- **Erweiterte Einstellungen** Startet die Konsole *Windows-Firewall mit erweiterter Sicherheit*
- **Problembehandlung für Netzwerk** Startet die *Problembehandlung – Netzwerk und Internet*

Einstellungen anpassen

Mehrere Links im Fenster *Windows-Firewall* verweisen auf denselben Platz: ein Dialogfeld *Einstellungen anpassen* mit den Steuerelementen für einige der Basisfunktionen der Firewall.

Abbildung 6.21 zeigt das Dialogfeld *Einstellungen anpassen*, das in drei Bereiche gegliedert ist, die den drei Profilen auf einem Windows-Computer entsprechen. Die Windows-Firewall stellt anhand dieser Profile den Typ des Netzwerks dar, mit dem der Server verbunden ist. Folgende Profile sind definiert:

- **Öffentlich** Das öffentliche (oder Gast-) Profil ist für Server vorgesehen, die für nicht authentifizierte oder vorübergehende Benutzer zugänglich sind, beispielsweise Computer in einem öffentlichen Labor oder Informationskiosk

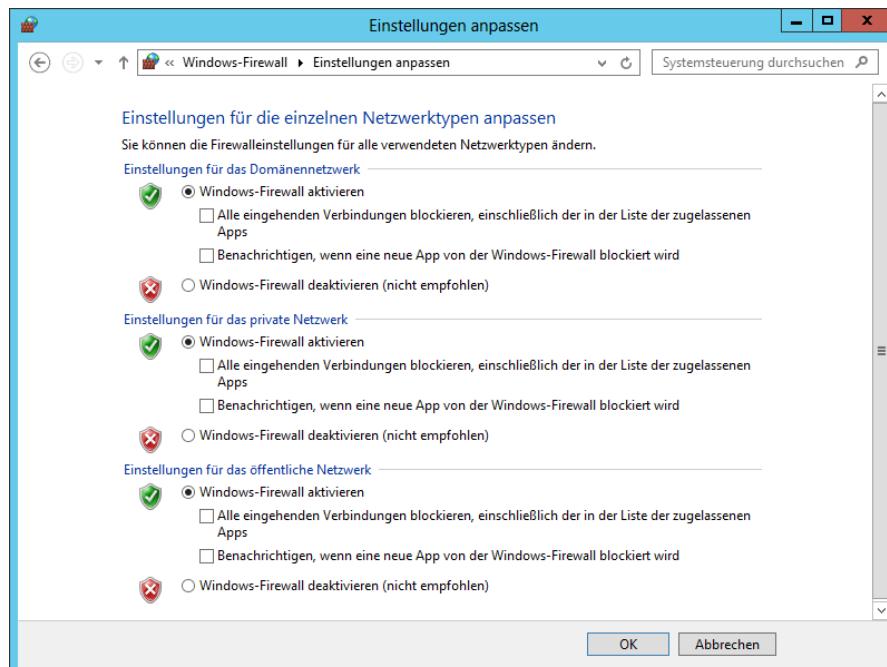


Abbildung 6.21 Das Dialogfeld *Einstellungen anpassen* für die Windows-Firewall

- **Privat** Dieses Profil ist für Server in einem internen Netzwerk vorgesehen, das nur für autorisierte Benutzer zugänglich ist

- **Domäne** Dieses Profil wird auf Server angewendet, die Mitglieder einer AD DS-Domäne sind, in der alle Benutzer identifiziert und authentifiziert werden

In der Windows-Firewall sind die drei Profile im Wesentlichen getrennte Regelmengen, die auf Computer angewendet werden, die mit dem designierten Netzwerktyp verbunden sind. Administratoren können die Umgebung der Netzwerktypen steuern, indem sie für jeden Netzwerktyp separate Regeln und Einstellungen für jedes Profil konfigurieren. Das Dialogfeld *Einstellungen anpassen* enthält die folgenden Steuerelemente für jedes der drei Netzwerkprofile:

- **Windows-Firewall aktivieren/deaktivieren** Schaltet die Windows-Firewall für das ausgewählte Profil ein bzw. aus
- **Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Apps** Erhöht die Sicherheit des Systems, indem alle unerwünschten Verbindungsversuche auf den Computer blockiert werden
- **Benachrichtigen, wenn eine neue App von der Windows-Firewall blockiert wird** Ist diese Option aktiviert, benachrichtigt das System den Benutzer beim gescheiterten Versuch einer Anwendung, Datenverkehr durch die Firewall zu senden

Anwendungen zulassen

Bisweilen müssen Administratoren die Firewalleinstellungen auf andere Weise modifizieren, was normalerweise damit zusammenhängt, dass eine bestimmte Anwendung Zugriff auf einen Port benötigt, der von den Standardregeln der Firewall nicht erfasst wird.

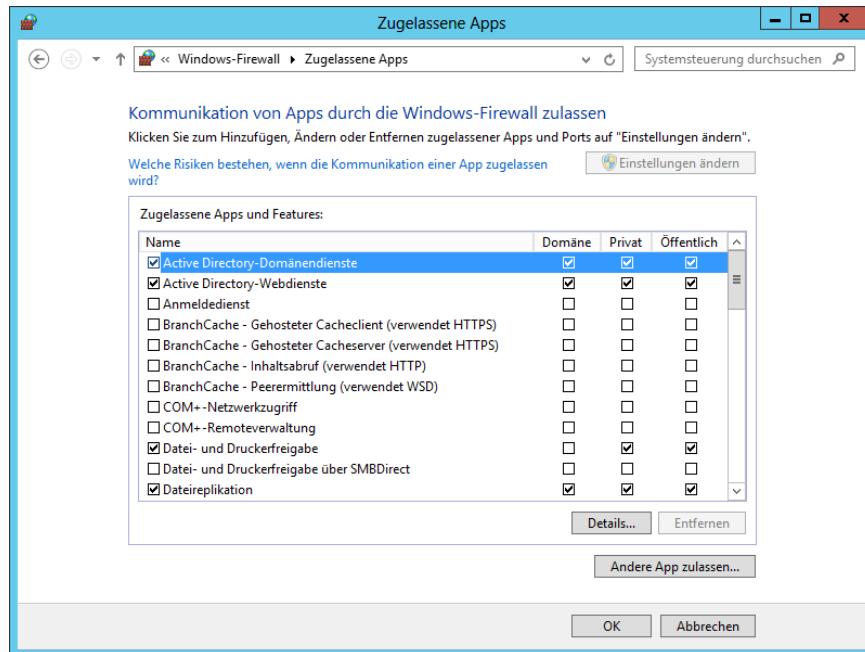


Abbildung 6.22 Das Dialogfeld *Zugelassene Apps* für Windows-Firewall

Hierzu können Sie in der Windows-Firewall-Systemsteuerung das Dialogfeld *Zugelassene Apps* verwenden, das Abbildung 6.22 zeigt.

Einen Port in der Firewall eines Servers zu öffnen, ist grundsätzlich eine gefährliche Aktivität. Je mehr Türen Sie geöffnet halten, desto größer ist die Wahrscheinlichkeit, dass Angreifer eindringen. Die Windows-Firewall bietet zwei grundlegende Methoden, um einen Durchgang in der Firewall zu öffnen: einen Port öffnen und eine Anwendung zulassen. Ein Risiko ist bei beiden Methoden gegeben, bei der zweiten ist es aber geringer. Denn wenn Sie in der Konsole *Windows-Firewall mit erweiterter Sicherheit* einen Port mithilfe einer Regel öffnen, bleibt der Port ständig geöffnet. Wenn Sie dagegen über die Systemsteuerung die Firewall für eine Anwendung öffnen, ist der angegebene Port nur geöffnet, solange das Programm läuft. Sobald Sie das Programm beenden, schließt die Firewall den Port.



Prüfungstipp Frühere Versionen von Windows führen zugelassene Anwendungen unter Ausnahmen. Dem liegt die Ansicht zugrunde, dass diese Anwendungen als Ausnahmen zu den allgemeinen Firewallregeln zu betrachten sind, die sämtliche Ports des Computers gegen Eindringversuche sperrt. Prüfungskandidaten sollten auf Fragen vorbereitet sein, die noch den älteren Terminus enthalten.

Das Dialogfeld *Zulässige Apps* listet die Anwendungen nach den Rollen und Features auf, die auf dem Server installiert sind. Jede aufgeführte Anwendung entspricht einer oder mehreren Firewallregeln, die die Systemsteuerung bei Bedarf aktiviert und deaktiviert.

Im Unterschied zu früheren Versionen bietet die Windows Server 2012-Version der Windows-Firewall-Systemsteuerung keinen direkten Zugriff auf Portnummern. Für eine genauere Kontrolle über die Firewall müssen Sie die Konsole *Windows-Firewall mit erweiterter Sicherheit* verwenden. Klicken Sie dazu in der Windows-Firewall-Systemsteuerung auf *Erweiterte Einstellungen* oder rufen Sie sie im Server-Manager über das Menü *Tools* auf.

Die Konsole Windows-Firewall mit erweiterter Sicherheit

Konzeptionell soll die Windows-Firewall-Systemsteuerung Administratoren und fortgeschrittenen Benutzern ermöglichen, die grundlegenden Firewalleinstellungen zu verwalten. Für einen Vollzugriff auf die Windows-Firewall-Konfigurationseinstellungen ist das MMC-Snap-In *Windows-Firewall mit erweiterter Sicherheit* vorgesehen.

Um die Konsole zu öffnen, starten Sie den Server-Manager und wählen im Menü *Tools* den Eintrag *Windows-Firewall mit erweiterter Sicherheit*. Daraufhin wird die Konsole *Windows-Firewall mit erweiterter Sicherheit* geöffnet, die in Abbildung 6.23 zu sehen ist.

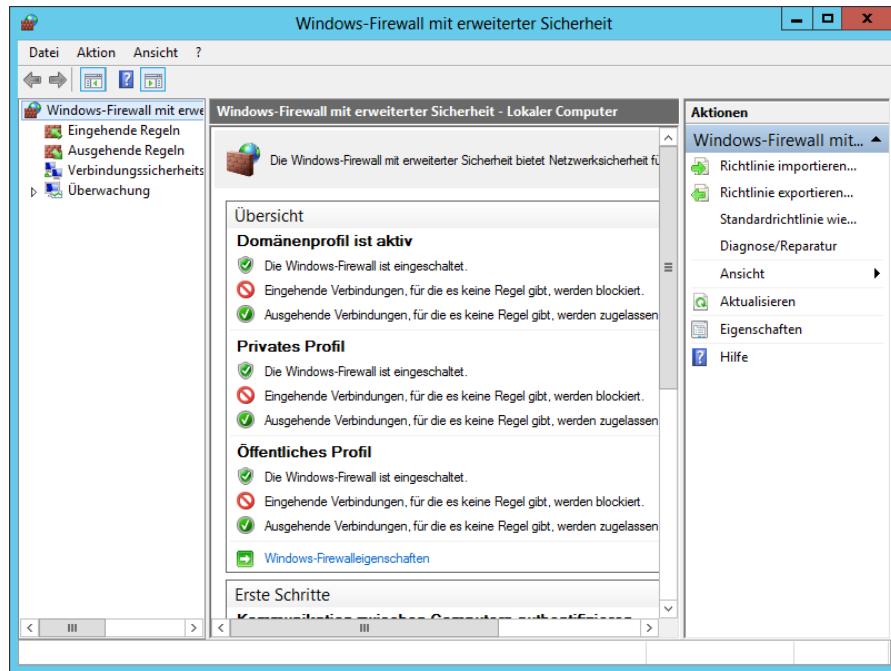


Abbildung 6.23 Die Konsole *Windows-Firewall mit erweiterter Sicherheit*

Profileinstellungen konfigurieren

Die Konsole *Windows-Firewall mit erweiterter Sicherheit* zeigt im mittleren Fensterbereich oben im Abschnitt *Übersicht* die Status für die drei Netzwerkstandortprofile des Computers an. Wenn Sie den Computer mit einem anderen Netzwerk verbinden (was bei einem Server zugegebenermaßen kaum vorkommen wird), kann die Windows-Firewall ein anderes Profil und einen anderen Satz von Regeln laden.

Die Standardkonfiguration der Windows-Firewall verlangt nach den gleichen grundlegenden Einstellungen für alle drei Profile wie folgt:

- Die Firewall ist eingeschaltet
- Eingehender Datenverkehr wird geblockt, außer wenn er einer Regel entspricht
- Ausgehender Datenverkehr ist zugelassen, außer wenn er einer Regel entspricht

Möchten Sie dieses Standardverhalten ändern, klicken Sie auf den Link *Windows-Firewall-eigenschaften*. Daraufhin wird das Dialogfeld *Windows-Firewall mit erweiterter Sicherheit* für den lokalen Computer angezeigt.

In diesem Dialogfeld ist jedem der drei Netzwerkstandortprofile eine Registerkarte mit identischen Steuerelementen zugeordnet, auf denen sich die Standardprofileinstellungen bearbeiten lassen. Zum Beispiel können Sie die Firewall vollkommen deaktivieren, wenn die Verbindung zu einem Domänenetzwerk besteht, und die Firewall mit ihren Einstellungen für

die höchste Sicherheitsstufe einschalten, wenn Sie den Computer mit einem öffentlichen Netzwerk verbinden. Außerdem haben Sie hier die Möglichkeit, die Benachrichtigungsoptionen der Firewall, das Protokollierungsverhalten und die Reaktion bei Regelkonflikten zu konfigurieren.

Regeln erstellen

Die zugelassenen Anwendungen, die Sie in der Windows-Firewall-Systemsteuerung konfigurieren können, sind eine relativ komfortable Methode, um mit Firewallregeln zu arbeiten. In der Konsole Windows-Firewall mit erweiterter Sicherheit können Sie mit den Regeln in ihrer Ursprungsform arbeiten.

Wenn Sie im linken Fensterbereich entweder *Eingehende Regeln* oder *Ausgehende Regeln* auswählen, erscheint im mittleren Fensterbereich eine Liste aller Regeln, die in der ausgewählten Richtung operieren (siehe Abbildung 6.24). Die derzeit aktiven Regeln sind mit einem Kontrollhäkchen in einem grünen Kreis neben der Regel gekennzeichnet und die außer Kraft gesetzten Regeln sind als nicht verfügbar dargestellt.

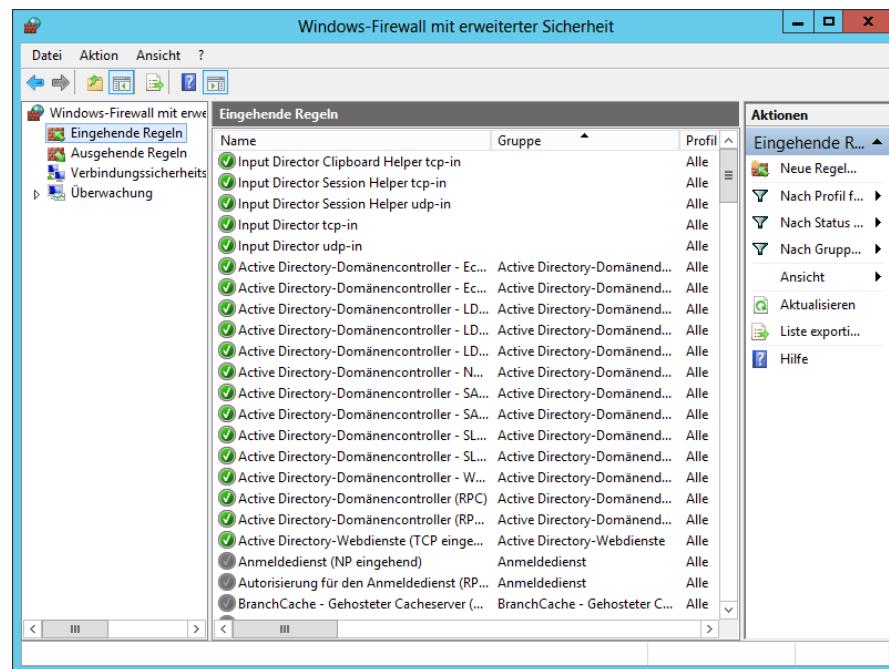


Abbildung 6.24 Die Liste *Eingehende Regeln* in der Konsole *Windows-Firewall mit erweiterter Sicherheit*

Neue Regeln können Sie über diese Benutzeroberfläche wesentlich flexibler erstellen als mit der Windows-Firewall-Systemsteuerung. Wenn Sie mit der rechten Maustaste auf den Knoten *Eingehende Regeln* (oder *Ausgehende Regeln*) klicken und im Kontextmenü *Neue Regel*

wählen, führt Sie der Assistent für neue eingehende (ausgehende) Regel durch die erforderlichen Schritte, um die folgenden Parameter zu konfigurieren:

- **Regeltyp** Hier wählen Sie aus, ob Sie eine Programmregel, eine Portregel, eine Variante einer vordefinierten Regel oder eine benutzerdefinierte Regel erstellen möchten. Diese Auswahl bestimmt, welche der folgenden Seiten der Assistent anzeigt.
- **Programm** Spezifiziert, ob die Regel auf alle Programme, auf ein bestimmtes Programm oder einen bestimmten Dienst anzuwenden ist. Dies ist äquivalent damit, in der Windows-Firewall-Systemsteuerung eine zugelassene Anwendung zu definieren, außer dass Sie den genauen Pfad zur Anwendung angeben müssen.
- **Protokoll und Ports** Gibt das Protokoll für die Netzwerk- oder Transportschicht an oder die lokalen und Remoteports, auf die die Regel angewendet wird. Damit können Sie die genauen Typen des Datenverkehrs spezifizieren, den die Regel blockieren oder zulassen soll. Um Regeln auf diese Weise zu erstellen, müssen Sie mit den Protokollen und Ports vertraut sein, über die eine Anwendung an beiden Endpunkten der Verbindung kommuniziert.
- **Vordefinierte Regeln** Gibt an, welche vordefinierten Regeln, die spezifische Anforderungen an die Netzwerkkonnektivität definieren, der Assistent erstellen soll
- **Bereich** Spezifiziert die IP-Adressen der lokalen und Remotesysteme, auf die die Regel angewendet wird. Damit können Sie den Datenverkehr zwischen bestimmten Computern blockieren oder zulassen.
- **Aktion** Legt die Aktion fest, die die Firewall ausführen soll, wenn ein Paket der Regel entspricht. Die Regel konfigurieren Sie, um standardmäßig blockierten Datenverkehr zu erlauben oder standardmäßig erlaubten Datenverkehr zu blockieren. Außerdem lässt sich für die Regel festlegen, dass sie Datenverkehr nur zulässt, wenn die Verbindung zwischen den kommunizierenden Computern mithilfe von IPSec gesichert wird.
- **Profil** Legt die Profile fest, auf die die Regel anzuwenden ist: Domäne, privat oder öffentlich
- **Name** Legt einen Namen und eine (optionale) Beschreibung für die Regel fest

Mit dem Assistenten lassen sich Regeln erstellen, die von einfachen Programmregeln (wie denen, die Sie über die Windows-Firewall-Systemsteuerung definieren können) bis hin zu hochkomplexen und spezifischen Regeln reichen, die nur bestimmte Typen des Datenverkehrs zwischen bestimmten Computern blockieren oder zulassen. Je komplizierter die Regeln jedoch werden, desto mehr müssen Sie über die TCP/IP-Kommunikation im Allgemeinen und das Verhalten Ihrer Anwendungen im Speziellen wissen. Es ist zwar recht einfach, die Standardeinstellungen der Firewall an bestimmte Anwendungen anzupassen, doch ist es eine gewaltige Aufgabe, eine vollkommen neue Firewallkonfiguration aus dem Boden zu stampfen.

Regeln importieren und exportieren

Es kann recht zeitaufwendig sein, Regeln in der Konsole *Windows-Firewall mit erweiterter Sicherheit* zu erstellen und zu modifizieren, vor allem wenn Sie diesen Prozess für mehrere

Computer wiederholen müssen. Deshalb bietet die Konsole die Möglichkeit, Regeln und Einstellungen, die Sie erstellt haben, zu speichern, indem Sie sie in eine Richtliniendatei exportieren.

Eine Richtliniendatei mit der Erweiterung *.wfw* enthält sämtliche Eigenschaftseinstellungen in einer Windows-Firewall-Installation und ihre sämtlichen Regeln, einschließlich der vordefinierten Regeln und der Regeln, die Sie erstellt oder modifiziert haben. Um eine Richtliniendatei zu erstellen, wählen Sie in der Konsole *Windows-Firewall mit erweiterter Sicherheit* im Menü *Aktion* den Befehl *Richtlinie exportieren* und geben dann einen Namen und den Speicherort für die Datei an.

Dann können Sie die Regeln und Einstellungen auf einen anderen Computer duplizieren, indem Sie die Datei kopieren und den Inhalt über die Funktion *Richtlinie importieren* einlesen.



Hinweis Richtlinien importieren

Wenn Sie Richtlinien aus einer Datei importieren, warnt die Konsole Sie, dass alle vorhandenen Regeln und Einstellungen überschrieben werden. Wenn Sie also auf einem Computer benutzerdefinierte Regeln erstellen, dürfen Sie nicht erwarten, mithilfe einer Richtliniendatei weitere Regeln importieren zu können.

Regeln per Gruppenrichtlinie erstellen

Über die Konsole *Windows-Firewall mit erweiterter Sicherheit* lassen sich zwar komplexe Konfigurationen für die Firewall erstellen, doch ist die Windows-Firewall immer noch eine Anwendung, die einen einzelnen Computer gegen Eindringlinge schützen soll. Bei einer großen Anzahl von Windows Server 2012-Servern ist es ziemlich langwierig, eine komplexe Firewallkonfiguration auf jedem Computer manuell zu erstellen. Wie bei den meisten Windows-Konfigurationsaufgaben können Administratoren deshalb die Firewalleteinstellungen mithilfe einer Gruppenrichtlinie im gesamten Netzwerk auf andere Computer verteilen.

Wenn Sie ein Gruppenrichtlinienobjekt bearbeiten und zum Knoten *Computerkonfiguration\Gruppenrichtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Windows-Firewall mit erweiterter Sicherheit* gehen, sehen Sie eine Benutzeroberfläche, die nahezu identisch mit der Konsole *Windows-Firewall mit erweiterter Sicherheit* ist.

Wie in der Konsole können Sie die Windows-Firewalleteigenschaften konfigurieren sowie eingehende, ausgehende und Verbindungssicherheitsregeln erstellen. Der Unterschied besteht darin, dass Sie diese Einstellungen dann auf Computern an beliebigen Standorten im Netzwerk bereitstellen können, indem Sie das Gruppenrichtlinienobjekt mit einem AD DS-Objekt verknüpfen.

Wenn Sie ein neues Gruppenrichtlinienobjekt öffnen, enthält die Windows-Firewall mit erweiterter Sicherheit keine Regeln – auch nicht die vorkonfigurierten Regeln, die Sie auf jedem Windows Server 2012-Computer finden. Sie können neue Regeln von Grund auf neu erstellen, um sie im Netzwerk bereitzustellen, oder Sie können Einstellungen aus einer Richtliniendatei importieren, genau wie es in der Konsole *Windows-Firewall mit erweiterter Sicherheit* möglich ist.

Im Unterschied zum Importieren einer Richtliniendatei überschreiben Gruppenrichtlinien nicht die gesamte Konfiguration der Windows-Firewall. Wenn Sie Firewallregeln und -einstellungen mit einer Gruppenrichtlinie bereitstellen, werden die Regeln im Gruppenrichtlinienobjekt mit den vorhandenen Regeln auf den Zielcomputern kombiniert. Die einzige Ausnahme bilden Regeln mit identischen Namen wie vorhandene Regeln. In diesem Fall überschreiben die Gruppenrichtlinienobjekt-Einstellungen die auf den Zielcomputern vorhandenen Regeln.

Verbindungssicherheitsregeln erstellen

Windows Server 2012 bringt auch ein Feature mit, das den IPsec-Datenschutz in die Windows-Firewall einbindet. Die IPSec (IP Security)-Standards sind eine Sammlung von Dokumenten, die eine Methode für das Sichern von Daten definieren, wenn sie über ein TCP/IP-Netzwerk übertragen werden. IPsec umfasst eine Routine zum Einrichten einer Verbindung, bei der sich die Computer einander authentifizieren, bevor Daten übertragen werden, und eine als Tunneln bezeichnete Technik, die Datenpakete zu ihrem Schutz in anderen Paketen kapselt.

Außer eingehenden und ausgehenden Regeln können Sie in der Windows-Firewall mit erweiterter Sicherheit auch Verbindungssicherheitsregeln erstellen. Hierfür greift Ihnen der Assistent für neue Verbindungssicherheitsregel unter die Arme. Verbindungssicherheitsregeln definieren den Typ des Schutzes, den Sie auf die Kommunikation entsprechend den Windows-Firewallregeln anwenden wollen.

Wenn Sie mit der rechten Maustaste auf den Knoten Verbindungssicherheitsregeln klicken und im Kontextmenü den Eintrag *Neue Regel* wählen, führt Sie der Assistent für neue Verbindungssicherheitsregel durch die Schritte, in denen Sie die folgenden Parameter konfigurieren:

- **Regeltyp** Gibt die grundlegende Funktion der Regel an: Computer basierend auf Authentifizierungskriterien isolieren, bestimmte Computer (wie zum Beispiel Infrastrukturserver) von der Authentifizierung ausnehmen, zwei bestimmte Computer oder Gruppen von Computern authentifizieren oder die Kommunikation zwischen zwei Computern über einen Tunnel durchführen. Außerdem können Sie benutzerdefinierte Regeln erstellen, um diese Funktionen zu kombinieren.
- **Endpunkte** Legt die IP-Adressen der Computer fest, die eine sichere Verbindung einrichten, bevor Daten übertragen werden
- **Anforderungen** Gibt an, ob die Authentifizierung zwischen zwei Computern in jeder Richtung angefordert werden soll oder erforderlich ist
- **Authentifizierungsmethode** Gibt den Typ der Authentifizierung an, den die Computer beim Einrichten einer Verbindung verwenden sollen
- **Profil** Legt die Profile fest, auf die die Regel anzuwenden ist: Domäne, privat, öffentlich oder eine Kombination dieser Profile
- **Name** Gibt einen Namen und eine (optionale) Beschreibung für die Regel an

Prüfungszielzusammenfassung

- Eine Firewall ist ein Programm, das einen Computer oder ein Netzwerk schützt, indem es bestimmte Arten von Netzwerkdatenverkehr vom und zum System durchlässt und anderen Datenverkehr blockiert
- Praktisch realisiert eine Firewall eine Reihe von Filtern, die den Inhalt von Paketen und die Muster des Datenverkehrs vom und zum Netzwerk untersuchen, um zu ermitteln, welche Pakete passieren dürfen
- In der Firewall sind Standardregeln vorkonfiguriert, die den Datenverkehr zulassen, den standardmäßige Windows-Netzwerkfunktionen verwenden, beispielsweise die Datei- und Druckerfreigabe. Für ausgehenden Netzwerkdatenverkehr lässt die Windows-Firewall den gesamten Datenverkehr die Firewall passieren, bis auf den, der einer Regel entspricht.
- Die Windows-Firewall-Systemsteuerung soll es Administratoren ermöglichen, grundlegende Konfigurationsaufgaben durchzuführen
- Für einen Vollzugriff auf die Windows-Firewall-Konfigurationseinstellungen ist das MMC-Snap-In *Windows-Firewall mit erweiterter Sicherheit* vorgesehen

Prüfungszielkontrolle

Mit den folgenden Fragen können Sie Ihr Wissen zu den Informationen in diesem Prüfungsziel testen. Die Antworten auf diese Fragen mit Erklärungen, warum die jeweiligen Auswahlmöglichkeiten richtig oder falsch sind, finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

1. Welcher der folgenden Mechanismen wird am häufigsten in Firewallregeln verwendet, um Datenverkehr im Netzwerk zu erlauben?
 - A. Hardwareadressen
 - B. IP-Adressen
 - C. Protokollnummern
 - D. Portnummern
2. Welche der folgenden Sicherheitsmechanismen werden von den Verbindungssicherheitsregeln für den Netzwerkverkehr, der die Firewall passieren darf, vorausgesetzt?
 - A. EFS
 - B. IPsec
 - C. Benutzerkontensteuerung (UAC)
 - D. Kerberos
3. Welche der folgenden Aktionen können Sie in der Windows-Firewall-Systemsteuerung nicht durchführen?
 - A. Eine Anwendung in allen drei Profilen durch die Firewall zulassen.

- B. Alle eingehenden Verbindungen für ein beliebiges der drei Profile blockieren.
 - C. Firewallausnahmen basierend auf Portnummer für alle drei Profile erstellen.
 - D. Windows-Firewall für alle drei Profile ausschalten.
4. Welche der folgenden Tools sind nicht in der Lage, die Firewallregeln für die Netzwerk-erkennung zu aktivieren und zu deaktivieren?
- A. Datei-Explorer
 - B. Netzwerk- und Freigabecenter
 - C. Wartungscenter
 - D. Dialogfeld *Zugelassene Apps*
5. Welche der folgenden Aussagen über die Windows-Firewall sind nicht richtig? (Wählen Sie alle zutreffenden Antworten aus.)
- A. Per Gruppenrichtlinie angewendete Firewallregeln überschreiben alle Firewallregeln auf dem Zielcomputer.
 - B. Bei per Gruppenrichtlinie angewendeten Firewallregeln werden die neu bereitgestellten Regeln mit den bereits vorhandenen Regeln kombiniert.
 - C. Importiert man Firewallregeln, die auf einem anderen Computer gespeichert wurden, werden alle Regeln auf dem Zielsystem überschrieben.
 - D. Importiert man Firewallregeln, die auf einem anderen Computer gespeichert wurden, werden beide Sätze von Einstellungen miteinander kombiniert.



Gedankenexperiment Wenden Sie im folgenden Gedankenspiel die Kenntnisse an, die Sie sich im Rahmen dieses Prüfungsziels angeeignet haben, um die erforderlichen Schritte zu nennen. Die Antworten auf diese Fragen finden Sie im Abschnitt »Antworten« am Ende dieses Kapitels.

Ralph ist angehender Netzwerkadministrator bei Wingtip Toys. Er hat in der IT-Abteilung Bereitschaftsdienst, während alle anderen zu einer Konferenz in der Stadt unterwegs sind. Der beste Kunde der Firma meldet sich telefonisch bei Ralph und berichtet, dass er nicht in der Lage ist, Bestellungen über die Website der Firma aufzugeben. Als Ralph die Protokolle für den Windows-Webserver inspiziert, fällt im ein großes Aufkommen an eingehendem Datenverkehr auf, das am Morgen begonnen hat.

Ralph vermutet, dass der Server Ziel eines DoS (Denial of Service)-Angriffs ist, hat aber keinen Zugriff auf die Firewall des Netzwerks und weiß auch nichts über die Firewall-konfiguration, die die Firma verwendet. Allerdings kann Ralph auf die Windows-Firewall zugreifen, die auf dem Webserver läuft. Welche temporären Modifikationen kann er an dieser Firewall vornehmen, um den Angriff zu blockieren und dem Kunden zu ermöglichen, seine Bestellungen wie gewohnt aufzugeben?

Antworten

Dieser Abschnitt enthält die Lösungen für die Gedankenspiele und Antworten auf die Fragen der Prüfungszielkontrollen in diesem Kapitel.

Prüfungsziel 6.1: Kontrolle

1. Richtige Antwort: B

- A. **Falsch:** Gruppenrichtlinientools, die mit den älteren administrativen Vorlagendateien (ADM) arbeiten, suchen diese nicht im zentralen Speicher.
- B. **Richtig:** Gruppenrichtlinientools suchen standardmäßig nach XML-basierten administrativen Vorlagendateien (ADMX) im zentralen Speicher.
- C. **Falsch:** Gruppenrichtlinienobjekte werden in der Active Directory-Datenbank gespeichert, nicht im zentralen Speicher.
- D. **Falsch:** Sicherheitsvorlagen befinden sich nicht im zentralen Speicher.

2. Richtige Antwort: D

- A. **Falsch:** Lokale Gruppenrichtlinienobjekte werden zuerst angewendet, dann folgen Administrator-, Nichtadministrator- und benutzerspezifische lokale Gruppenrichtlinienobjekte.
- B. **Falsch:** Gruppenrichtlinienobjekte lokaler Administratoren werden nach lokalen Gruppenrichtlinienobjekten und vor benutzerspezifischen lokalen Gruppenrichtlinienobjekten angewendet.
- C. **Falsch:** Gruppenrichtlinienobjekte lokaler Nichtadministratoren werden nach lokalen Gruppenrichtlinienobjekten und vor benutzerspezifischen lokalen Gruppenrichtlinienobjekten angewendet.
- D. **Richtig:** Von den lokalen Gruppenrichtlinienobjekttypen werden benutzerspezifische lokale Gruppenrichtlinienobjekte zuletzt angewendet.

3. Richtige Antwort: C

- A. **Falsch:** Gruppenrichtlinienobjektverknüpfungen wenden Gruppenrichtlinieneinstellungen auf den gesamten Inhalt eines AD DS-Containers an.
- B. **Falsch:** Administrative Vorlagen definieren die registrierungsbasierten Einstellungen, die in Gruppenrichtlinienobjekten erscheinen.
- C. **Richtig:** Sicherheitsfilterung ist ein Gruppenrichtlinienfeature, mit dem sich die Verteilung von Gruppenrichtlinieneinstellungen auf bestimmte Benutzer und Gruppen innerhalb eines AD DS-Containers einschränken lässt.
- D. **Falsch:** Starter-Gruppenrichtlinienobjekte sind Vorlagen, um neue Gruppenrichtlinienobjekte zu erstellen.

4. Richtige Antwort: A

- A. **Richtig:** Starter-Gruppenrichtlinienobjekte sind Vorlagen, mit denen Sie mehrere Gruppenrichtlinienobjekte mit demselben Satz grundlegender Einstellungen von administrativen Vorlagen erstellen können.

- B. **Falsch:** Starter-Gruppenrichtlinienobjekte werden nicht durch Clients angewendet.
 - C. **Falsch:** Starter-Gruppenrichtlinienobjekte verwenden die gleiche Benutzeroberfläche wie Standardgruppenrichtlinienobjekte.
 - D. **Falsch:** Starter-Gruppenrichtlinienobjekte enthalten nicht alle Einstellungen, die im Gruppenobjekt für die Standarddomänenrichtlinie vorhanden sind.
5. **Richtige Antwort:** A
- A. **Richtig:** Eine Richtlinieneinstellung *Nicht konfiguriert* hat keine Wirkung auf die vorhandene Einstellung dieser Richtlinie.
 - B. **Falsch:** Eine Einstellung *Deaktiviert* bleibt deaktiviert, wenn Sie ein Gruppenrichtlinienobjekt mit dem Wert *Nicht konfiguriert* für dieselbe Einstellung anwenden.
 - C. **Falsch:** Eine Einstellung *Nicht konfiguriert* ändert die Einstellung *Deaktiviert* nicht in *Aktiviert*.
 - D. **Falsch:** Konflikte bei Richtlinieneinstellungen führen zu überschriebenen Einstellungen, jedoch nicht zu Fehlern.

Prüfungsziel 6.1: Gedankenspiel

Alice muss ein anderes Gruppenrichtlinienobjekt mit der folgenden Einstellung anlegen, es mit der Domäne verknüpfen und seine Sicherheitsfilterung modifizieren, indem die Gruppe *Geschäftsleitung* hinzugefügt und die Gruppe *Authentifizierte Benutzer* entfernt wird. Das Gruppenrichtlinienobjekt muss Vorrang vor dem Gruppenrichtlinienobjekt *Geräte-einstellungen* haben.

- Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind – Deaktiviert

Prüfungsziel 6.2: Kontrolle

1. **Richtige Antwort:** D
- A. **Falsch:** Mit Active Directory-Benutzer und -Computer ist es nicht möglich, eine Sicherheitsvorlage auf eine Domäne anzuwenden.
 - B. **Falsch:** Mit dem Snap-In *Sicherheitsvorlagen* ist es nicht möglich, eine Sicherheitsvorlage auf eine Domäne anzuwenden.
 - C. **Falsch:** Mit dem Gruppenrichtlinienobjekt-Editor ist es nicht möglich, eine Sicherheitsvorlage auf eine Domäne anzuwenden.
 - D. **Richtig:** Nachdem Sie die Sicherheitsvorlage in ein Gruppenrichtlinienobjekt importiert haben, können Sie es mit einem Domänenobjekt verknüpfen und die Vorlage-einstellungen bereitstellen.

2. Richtige Antworten: A, C

- A. **Richtig:** Wenn Sie in der Windows-Systemsteuerung einen Standardbenutzer erstellen, fügen Sie das Konto in die lokale Benutzergruppe ein.
- B. **Falsch:** Mit der Windows-Systemsteuerung ist es nicht möglich, einen Benutzer in die Gruppe *Hauptbenutzer* hinzuzufügen.
- C. **Richtig:** Wenn Sie in der Windows-Systemsteuerung einem Benutzer administrative Rechte erteilen, wird das Konto in die lokale Administratorengruppe hinzugefügt.
- D. **Falsch:** In Windows gibt es keine lokale Gruppe *Nichtadministratoren*.

3. Richtige Antwort: B

- A. **Falsch:** Mit Active Directory-Benutzer und -Computer ist es nicht möglich, die Einstellungen einer Sicherheitsvorlage zu modifizieren.
- B. **Richtig:** Die Einstellungen in einer Sicherheitsvorlage ändern Sie mit dem Snap-In *Sicherheitsvorlagen*.
- C. **Falsch:** Mit dem *Gruppenrichtlinienobjekt-Editor* ist es nicht möglich, die Einstellungen in einer Sicherheitsvorlage zu modifizieren.
- D. **Falsch:** Mit der Konsole *Gruppenrichtlinienverwaltung* ist es nicht möglich, die Einstellungen in einer Sicherheitsvorlage zu modifizieren.

4. Richtige Antwort: D

- A. **Falsch:** Sicherheitsoptionen können nicht die Fähigkeiten liefern, die integrierten lokalen Gruppen gewährt werden.
- B. **Falsch:** Windows-Firewallregeln können nicht die Fähigkeiten liefern, die integrierten lokalen Gruppen gewährt werden.
- C. **Falsch:** NTFS-Berechtigungen können nicht die Fähigkeiten liefern, die integrierten lokalen Gruppen gewährt werden.
- D. **Richtig:** Auf einem Windows Server 2012-Server erhalten integrierte lokale Gruppen ihre speziellen Fähigkeiten über Benutzerrechte.

5. Richtige Antwort: A

- A. **Richtig:** Die Richtlinie *Verzeichnisdienstzugriff überwachen* überwacht nur die Objekte, die Sie in der Konsole *Active Directory-Benutzer und -Computer* ausgewählt haben.
- B. **Falsch:** Es ist nicht erforderlich zu warten, bis die Richtlinieneinstellungen auf alle Domänencontroller weitergeleitet wurden.
- C. **Falsch:** Die zu überwachenden Objekte konfigurieren Sie in der Konsole *Active Directory-Benutzer und -Computer* und nicht in der Richtlinie selbst.
- D. **Falsch:** Es hat keinen Einfluss, wenn Sie die Objektnamen ändern.

Prüfungsziel 6.2: Gedankenspiel

1. 20. Von den aufgeführten Betriebssystemen sind nur Windows 7, Windows XP Professional und Windows 2000 Professional in der Lage, Gruppenrichtlinien zu verwenden.
2. A. Dass Endbenutzer die Sicherheitseinstellungen auf ihren Computern nicht ändern, lässt sich einzig dadurch sicherstellen, dass sie per Gruppenrichtlinie bereitgestellt werden. Da setzt aber voraus, dass Sie das Betriebssystem aktualisieren. Bei den Antworten C und D wären Sie zwar in der Lage, Sicherheitsvorlagen auf den Computern bereitzustellen, doch könnten die Benutzer die Einstellungen im Nachhinein modifizieren.

Prüfungsziel 6.3: Kontrolle

1. **Richtige Antwort:** D
 - A. **Falsch:** Hashregeln gehören zu den Regeltypen für Softwareeinschränkung.
 - B. **Falsch:** Zertifikatregeln gehören zu den Regeltypen für Softwareeinschränkung.
 - C. **Falsch:** Pfadregeln gehören zu den Regeltypen für Softwareeinschränkung.
 - D. **Richtig:** Firewallregeln gehören nicht zu den Regeltypen für Softwareeinschränkung.
2. **Richtige Antwort:** B
 - A. **Falsch:** Die Strategie *Standardbenutzer* verhindert die Ausführung von Anwendungen, die Administratorrechte erfordern, erlaubt aber die Ausführung von Programmen, die nur Ressourcen benötigen, die normalen Benutzern zugänglich sind.
 - B. **Richtig:** Die Strategie *Nicht erlaubt* verhindert die Ausführung aller Anwendungen, außer denen, die speziell zugelassen sind.
 - C. **Falsch:** Es gibt keine Strategie *Hauptbenutzer*, um Softwareeinschränkungen zu erzwingen.
 - D. **Falsch:** Die Strategie *Nicht eingeschränkt* erlaubt die Ausführung aller Anwendungen, außer denen, die speziell ausgeschlossen sind.
3. **Richtige Antworten:** B, C
 - A. **Falsch:** Der Hashwert basiert auf der Datei und nicht auf deren Speicherort, sodass es sich nicht auf die Funktionalität auswirkt, wenn Sie die Datei verschieben.
 - B. **Richtig:** Wird die Datei durch eine andere Version ersetzt, wird der Hashwert unbrauchbar.
 - C. **Richtig:** Wird die Datei in irgendeiner Form verändert, wird der Hashwert unbrauchbar.
 - D. **Falsch:** Geänderte Dateiberechtigungen wirken sich auf die Datei selbst nicht aus, sodass der Hashwert weiterhin funktioniert.
4. **Richtige Antwort:** B
 - A. **Falsch:** Ausführbare Regeln werden auf Dateien mit den Erweiterungen *.exe* und *.com* angewendet.
 - B. **Richtig:** Windows Installer-Regeln werden auf Pakete mit den Erweiterungen *.msi* und *.msp* angewendet.

- C. **Falsch:** Skriptregeln werden auf Skriptdateien mit den Erweiterungen *.ps1*, *.bat*, *.cmd*, *.vbs* und *.js* angewendet.
- D. **Falsch:** App-Paketregeln werden auf Anwendungen angewendet, die über den Windows Store gekauft wurden.
5. **Richtige Antwort:** A
- A. **Richtig:** Um AppLocker verwenden zu können, setzt Windows Server 2012 voraus, dass der Dienst *Anwendungsidentität* läuft.
- B. **Falsch:** Der Dienst *Anwendungsverwaltung* ist nicht erforderlich, damit Windows AppLocker-Richtlinien anwendet.
- C. **Falsch:** Der Dienst *Anmeldeinformationsverwaltung* ist nicht erforderlich, damit Windows AppLocker-Richtlinien anwendet.
- D. **Falsch:** Der Netzwerkkonnektivitäts-Assistent ist nicht erforderlich, damit Windows AppLocker-Richtlinien anwendet.

Prüfungsziel 6.3: Gedankenspiel

Sophie hat zwei Regeln zu erstellen: eine *Zulassen*-Regel, die der Gruppe *ResDev* den Zugriff auf die Anwendung gewährt, und eine *Verweigern*-Regel die nur auf die Gruppe *RDint* angewendet wird. Da die *Verweigern*-Regeln gegenüber den AppLocker-Regeln Vorrang haben, sind die Praktikanten nicht in der Lage, auf die Anwendung zuzugreifen.

Prüfungsziel 6.4: Kontrolle

1. **Richtige Antwort:** D
- A. **Falsch:** Es ist zwar denkbar, dass Firewalls den Netzwerkdatenverkehr mithilfe von Hardwareadressen filtern, doch ist diese Lösung kaum praktikabel.
- B. **Falsch:** Firewalls filtern normalerweise bestimmte Arten des Netzwerkdatenverkehrs und nicht komplett IP-Adressen.
- C. **Falsch:** Beim Filtern nach Protokollnummer ist normalerweise nicht die erforderliche Feinabstufung möglich, um eine effiziente Firewallkonfiguration zu erstellen.
- D. **Richtig:** Firewalls verwenden normalerweise Portnummern, um den Datenverkehr im Netzwerk zuzulassen.
2. **Richtige Antwort:** B
- A. **Falsch:** Das verschlüsselnde Dateisystem (EFS) bietet Sicherheit nur für das Speichermedium, nicht aber für den Netzwerkdatenverkehr.
- B. **Richtig:** Verbindungssicherheitsregeln setzen voraus, dass der Netzwerkdatenverkehr, der die Firewall passieren darf, IPsec für Sicherheit verwendet.
- C. **Falsch:** Die Benutzerkontensteuerung kann den Netzwerkdatenverkehr nicht einschränken.

D. **Falsch:** Kerberos ist ein Authentifizierungsprotokoll. Es kann den Netzwerddatenverkehr nicht einschränken.

3. **Richtige Antwort: C**

A. **Falsch:** In der Windows-Firewall-Systemsteuerung können Sie einer Anwendung die Firewall für alle drei Profile öffnen.

B. **Falsch:** In der Windows-Firewall-Systemsteuerung können Sie alle eingehenden Verbindungen für alle drei Profile blockieren.

C. **Richtig:** In der Windows-Firewall-Systemsteuerung ist es nicht möglich, den Netzwerddatenverkehr nach Portnummern für alle drei Profile zu blockieren.

D. **Falsch:** In der Windows-Firewall-Systemsteuerung können Sie die Firewall für jedes der drei Profile ein- und ausschalten.

4. **Richtige Antwort: C**

A. **Falsch:** Der Datei-Explorer zeigt einen Link an, der die Netzwerkerkennungsregeln aktiviert.

B. **Falsch:** Das Netzwerk- und Freigabecenter der Systemsteuerung enthält einen Link, der Zugriff auf die Steuerelemente für die Tools zur Netzwerkerkennung bietet.

C. **Richtig:** Das Wartungscenter der Systemsteuerung enthält keine Steuerelemente für die Netzwerkerkennung.

D. **Falsch:** Das Dialogfeld *Zugelassene Apps* enthält Steuerelemente für die Netzwerkerkennungsregeln.

5. **Richtige Antworten: B, C**

A. **Falsch:** Per Gruppenrichtlinie angewendete Firewallregeln werden mit den vorhandenen Regeln kombiniert.

B. **Richtig:** Per Gruppenrichtlinie angewendete Firewallregeln werden mit den vorhandenen Regeln kombiniert.

C. **Richtig:** Importiert man Windows-Firewallregeln von einem anderen System, werden alle vorhandenen Regeln überschrieben.

D. **Falsch:** Das Importieren von Regeln überschreibt die vorhandenen Regeln; die importierten Regeln werden nicht mit den vorhandenen kombiniert.

Prüfungsziel 6.4: Gedankenspiel

Als vorübergehende Maßnahme könnte der Administrator eine Windows-Firewallregel auf Basis von IP-Adressen erstellen, die den Datenverkehr vom Computer des Kunden zulässt und jeglichen anderen Datenverkehr blockiert. Damit wird verhindert, dass das System die DoS-Dateien verarbeitet.

Index

.avhd 190
.avhdx 190
.iso 168
.msu 144
.vhd 163
.vhdx 163, 179
.vsv 163
.xml 163
6to4 234

A

A (Adresse) 266
AAAA (Adresse) 266
Abbildungseien 168
Abfragen
 iterative 260
 rekursive 260
Access Control Entry (ACE) 96
Access Control Entry (ACE) *siehe* Zugriffssteuerungseintrag
Access Control List (ACL) *siehe* Zugriffssteuerungsliste
ACE (Access Control Entry) 96
Active Directory
 DNS-Replikation 269
 Domänendienste installieren 281
 LDIFDE.exe 308
 Zone erstellen 265
 Zugriffstoken 325
Active Directory Domain Services (AD DS) *siehe* Active Directory-Domänendienste
Active Directory-Benutzer und -Computer
 Benutzervorlage 306
 Computerobjekte 311
 mehrere Benutzer verwalten 313
 Objekte verwalten 313

Active Directory-Domänendienste 279–280

 Windows PowerShell 289

Active Directory-integrierte Zonen 264

Active Directory-Verwaltungscenter 302

 Computerobjekte 312

 mehrere Benutzer verwalten 313

 Objekte verwalten 313

 OU-Objekt erstellen 322

AD DS

 aktualisieren 293

 Domänencontroller entfernen 293

 Rolle 346

AD DS *siehe* Active Directory-Domänendienste

Adapter

 emulierter 207

 Netzwerk- 220

 PXE- 248

 synthetischer 206

ADDSDeployment 289

Add-WindowsFeature 142

ADM 345

Administrator 300

 Bestätigungsmodus 370

ADMX 345

 Gruppenrichtlinientools 346

Adressen

 Bereiche 227

 Bereiche (MAC) 203

 DHCP 200

 Hardware- 202

 Hyper-V 204

 Klassen 218

 MAC- 202

Adressen *siehe auch* IP-Adressen

Aggregation 37

AGUDLP 329

- Aktionen 398
Anhebungsaufforderung 370
Anwendungsidentität 385
Anwendungssteuerungsrichtlinien 383
Anycast 227–228
APIPA 226
AppLocker 383
 Anwendungsidentität 385
 Regel automatisch erstellen 385
 Regel manuell erstellen 386
 Regeltypen 383
 Standardregel 385
App-Paketregeln 384
Arbeitsspeicher
 beim Start 173
 dynamischer 173
 Puffer 173
 Smart Paging 174
 Umfang 173
 virtuelle Computer 171
Arbeitsspeicher *siehe auch* RAM
ARP (Address Resolution Protocol) 241
Assistenten
 Bereichserstellungs- 243
 für erste Schritte 249
 für neue ausgehende Regel 397
 für neue eingehende Regel 139, 397
 für neue Freigaben 92
 für neue Speicherpools 66
 für neue Verbindungssicherheitsregel 400
 für neue virtuelle Computer 163, 182
 für neue virtuelle Datenträger 69
 für neue virtuelle Festplatten 180
 für neue Volumes 72
 Neues Objekt ? Benutzer 303
 Neues Objekt ? Computer 312
 Objekt kopieren ? Benutzer 306
 Remotezugriff konfigurieren 249
 zum automatischen Generieren von Regeln 385
 zum Bearbeiten virtueller Datenträger 188
 zum Bearbeiten virtueller Festplatten 187
 zum Bereitstellen eines freigegebenen Ordners 95
 zum Erstellen neuer einfacher Volumes 74
 zum Hinzufügen von Rollen und Features 159
 zum Installieren von Active Directory-
 Domändiensten 282
 zum Zuweisen der Objektverwaltung 323
ausführbare Regeln 384
Authentifizierung 299
 Methoden 400
Autorisierung 103, 299
- ## B
- Bandbreite
 Aggregation 37
 Hyper-V 175
 zusammenfassen 37
Basisfestplatten 59
Benutzer
 Domänen- 300
 erstellen 302
 lokale 299
 mehrere erstellen 307
 Rechte zuweisen 360
Benutzerkonfiguration 350
Benutzerkonten 299, 365
 Administrator 300
 Gast 300
 lokale 365
Benutzerkontensteuerung 369
Benutzeroberfläche
 grafische 18
 minimale Serverschnittstelle 22
Benutzerrechte 317
Benutzervorlagen 306
Berechtigungen 96
 Autorisierung 103
 Dokumente verwalten 123
 Drucker 123
 Drucker verwalten 124
 effektiver Zugriff 100
 erteilen 99
 erweiterte 97–98
 grundlegende 97–98
 Gruppenrichtlinie übernehmen 344
 Jeder 100
 kombinieren 105
 spezielle 98
 Standard- 98
 Vererbung 99
 verweigern 99
 Zugriffssteuerung 95
 Zugriffssteuerungsliste 96

- Bereiche 237, 398
erstellen 243
- Bereichserstellungs-Assistent 243
- Betriebssystemumgebung
POSE / VOSE 16
- BIND 264
- Booten
GPT-Partition 59
- BOOTP 239
- BranchCache 94
- ## C
- Chkdsk.exe 61
- CIDR
(Classless Inter-Domain Routing) 221
- Classless Inter-Domain Routing (CIDR) 221
- clientseitige Zwischen speicherung 95
- Cmdlets
Add-WindowsFeature 142
Enable-VMResourceMetering 175
Enter-PSSession 141
Exit-PSSession 142
Get-WindowsFeature 142
Import-Csv 309
Install-WindowsFeature 142
New-ADComputer 313
New-ADGroup 331
New-ADUser 305
New-VHD 181
New-VM 166
New-VMResourcePool 175
New-VMSwitch 202
Remotedesktopverbindungen 35
Set-NetFirewallRule 138
Set-RemoteDesktop 35
Set-VMMemory 174
Uninstall-WindowsFeature 24
- CNAME (Kanonischer Name) 267
- Computer
Beitreten zu Domäne 314
Name ändern 314
umbenennen 34
- Computerkonfiguration 350
- Computername 33
- Computerobjekte 310
- Container 321
- Controller
IDE 178
SCSI 178
- CSV 307
- CSVDE.exe 307
- ## D
- Dashboard 42
- Datei- und Speicherdi enste 62, 92
- Dateien
Abbild- 168
für gespeicherten Zustand 163
- Dateifreigabeprofil 92
- Dateikomprimierung 61
- Dateisysteme 61
Volume formatieren 76
- Datenausführungsverhinderung 159
- Datenträger
Datei- und Speicherdi enste 62
dynamische Festplatten 60
Einstellungen 58
entfernen 69
hinzufügen 68
Kontingente 61, 107
konvertieren 64
Partitionsstile 59
Pass-Through- 186
virtueller 58
zurücksetzen 68
- Datenträger *siehe auch* Festplatten
- Datenträgerverwaltung
DiskPart.exe 74
Festplatte offline schalten 187
VHD-Dateien 64
- dcdiag 296
- Dcpromo.exe 282
- Desktop
sicherer 371
- DHCP 225, 237
Adresszuweisung 237
ARP (Address Resolution Protocol) 241
Bereich erstellen 243
- Bereiche 237
- Erweiterungen 239
- Kommunikation 240
- Meldungstyp 238

- DHCP (*Fortsetzung*)
 Optionen 238, 245
 Relay-Agent 248
 Reservierungen 246
 Server bereitstellen 243
 virtuelle Switches 200
- DHCPACK 239
- DHCPDECLINE 238
- DHCPDISCOVER 238
- DHCPIFORM 239
- DHCPNAK 239
- DHCPOFFER 238
- DHCPRELEASE 239
- DHCPREQUEST 238
- Dienstanbieter für Netzwerkvirtualisierung 206
- Dienste
 Active Directory-Domänen- 280
 Anwendungsidentität 385
 konfigurieren 51
 NetLogon 310
 Windows-Firewall 392
 Windows-Remoteverwaltung 140
- Dienstprogramme
 CSVDE.exe 301
 DiskPart.exe 62, 74
 Diskpart.exe 187
 Dsadd.exe 304, 312
 LDIFDE.exe 301
 Netdom.exe 315
 PushPrinterConnections.exe 132
 Sysprep.exe 185
- Differenzierung 181
- Directory Services Restore Mode (DSRM) 287
- Directory Services Restore Mode, DSRM *siehe*
 Verzeichnisdienstwiederherstellung
- DiskPart.exe 62, 74
- Diskpart.exe 187
- Djoin.exe 317
- dn 308
- DNS
 BIND 264
 Caching 258
 Kommunikation 254
 Replikation 269
 Ressourceneinträge 266
 SRV-Einträge 295
 Stammhinweise 269
 Weiterleitungen 260
- Dokumente
 verwalten 123
- Domänen 280
 beitreten 34
 Computer beitreten 314
 Container 321
 der obersten Ebene 255
 Toplevel 255
- Domänencontroller 280
 AD DS-Datenbank 291
 einfügen in Domäne 285
 herabstufen 293
 heraufstufen 282
 Nttsutil.exe 291
 Registrierung im DNS 296
 Replikation 291
 schreibgeschützter 284
- Domänencontrolleroptionen 283
- Domänenfunktionsebene 284
- Druck- und Dokumentdienste 126
- Drucken
 direktes 114
 Netzwerkdrucker 115
 Spooler 114
- Drucker 112
 anzeigen 128
 Berechtigungen 123
 Dokumente verwalten 123
 Easy Print 121
 erweiterte Konfiguration 118
 Filter 128
 freigeben 118
 Gruppenrichtlinien 130
 Nomenklatur 113
 Prioritäten 124
 Sicherheit 122
- Druckerarchitektur 112
- Druckerpools 118, 126
- Druckerserver 112, 126
- Druckertreiber 113
 Easy Print 121
 installieren 121
 verwalten 120
- Druckgerät 112
- Druckverwaltung 127, 129
 Druckerserver hinzufügen 127
- Druckwarteschlange 113–114

Dsadd.exe 304
 Computerobjekte 312
 Gruppenobjekt erstellen 330
 Dsmod.exe 333
 DSRM (Directory Services Restore Mode) 284, 287
 Dynamische Updates 296
 RFC 2136 296

E

Easy Print 121
 Editionen 15
 EFI (Extensible Firmware Interface) 59
 Einfaches Volume 60
 Eingabeaufforderung 19
 Einschränkungen 376
 Einstellungen
 Sicherheitsvorlagen 364
 Software- 350
 Windows- 350
 Enable-VMResourceMetering 175
 Encrypted File System (EFS) 61
 Enter-PSSession 141
 EPS (Encrypted File System) 61
 Erneuerungszeitraum 239
 Erweiterte Freigabeeinstellungen 391
 Erweiterungen
 .avhd 190
 .avhdx 190
 .iso 168
 .msu 144
 .vhd 163
 .vhdx 163
 .vsv 163
 .xml 163
 DHCP 239
 herstellerspezifische 239
 Shell- 22
 Erzwingen 381
 Ethernet 33
 eXecute Disable (XD) 159
 exFAT 61
 Exit-PSSession 142

F

FAT 61
 FAT16 61
 FAT32 61

Features
 AppLocker 383
 Dynamischer Arbeitsspeicher 172
 Gruppenrichtlinienverwaltung 346
 NIC-Teamvorgang 37
 Smart Paging 174
 Volumeschattenkopie 106
 Windows Server-Migrationstools 28

Features bei Bedarf 14, 23

Fehlertoleranz 70

Festplatten
 Basis- 59
 dynamische 60
 Formate virtueller 178
 geeignet für Speicherpools 68
 hinzufügen 63
 virtuelle 64, 179

Festplatten *siehe auch* Datenträger

File Server Resource Manager *siehe* Ressourcen-Manager für Dateiserver

Filter

Drucker 128

Firewall

Netzwerkerkennung 391
 Problembehandlung 393

Freigabeberechtigungen 100

Freigaben

BranchCache 94
 Drucker 118
 Netzwerkdrucker 117
 Ordner 90
 Profil 92
 Verschlüsselung 94

G

Gast 300
 Gesamtstruktur
 Stammdomäne 282, 338
 Strukturdomäne 288
 Gesamtstrukturfunktionsebene 284
 Gespiegeltes Volume 61
 Get-NetFirewallRule 138
 Get-StorageSubsystem 69
 Get-WindowsFeature 142
 Globaler Katalog 284
 globaler Katalog
 universale Gruppe 328

- GPT 59
Group Policy Objects (GPOs) *siehe* Gruppenrichtlinienobjekte
Gruppe
 domänenlokale 327
 globale 327
 konvertieren 334
 SID 334
 universale 328
Gruppen
 erstellen 329
 lokale 368
 Mitgliedschaft verwalten 331
 Organisationseinheiten 321
Gruppenbereich 326
Gruppenobjekt
 Dsmod.exe 333
Gruppenrichtlinien
 Benutzerrechte 317
 Drucker bereitstellen 130
 Firewall 399
 Gruppenmitgliedschaft 332
 Regeln 399
 übernehmen 344
Gruppenrichtlinieneinstellungen 350
Gruppenrichtlinienknoten 350
Gruppenrichtlinienobjekte 344
 lokale 345
 mehrfache lokale 345, 351
 Sicherheitsvorlagen importieren 364
 Standarddomänencontrollerrichtlinie 316
 Starter- 345, 349
 Vererbung 348
Gruppenrichtlinienobjekt-Editor 352
Gruppenrichtlinientools
 ADMX 346
Gruppenrichtlinienverwaltung 346
Gruppenrichtlinienverwaltungs-Editor 332, 346
 öffnen 377
Gruppentyp 326
Gruppenverschachtelung 326, 328
- H**
- HardwareAdresse 202
Hardwarebeschleunigung 208
Hardwarekompatibilität 25
Hashregel 379
- Hashwert 379
Heraufstufen
 Domänencontroller 282
Herausgeber
 Organisationsadministrator 382
Herstellerkennung 202
Hosttabelle 253
Hyper-V 153
 Adressen 204
 dynamischer Arbeitsspeicher 172
 Hardwareeinschränkungen 156
 Implementierungen 156
 Integrationsdienste 169
 Lizenziierung 156
 Manager für virtuelle Switches 200
 Ressourcenmessung 175
 Server 157
 Smart Paging 174
 Snapshot 189
Hypervisor 154
 Partitionen 155
 Virtual Machine Monitor (VMM) 154
Hyper-V-Manager 161
 Manager für virtuelle SANs 192
Hyper-V-Verwaltungstools 162
- I**
- IANA (Internet Assigned Numbers Authority) 220
ICANN (Internet Corporation for Assigned Names and Numbers) 222
ICMPv6 (Internet Control Message Protocol version 6) 234
IDE 178
IFM
 Installieren von Medium 291
Import-CSV 309
in-addr.arpa 261
Install from Media (IFM) 291
Install-AddsDomain 289
Install-AddsDomainController 289, 291
Install-AddsForest 289
Installation
 Anforderungen 18
 Dateisystem 61
 Edition auswählen 15
 Optionen 18
 planen 14

- Installation (*Fortsetzung*)
 - Server 14
 - Server Core 19
 - Server konfigurieren 32
 - Signierung 26
 - Upgrade 25
 - WinSxS 23
 - Installieren von Medium 291
 - Install-WindowsFeature 289
 - Hyper-V-Rolle 161
 - Tools installieren 142
 - Windows Server-Migrationstools 29
 - Integrationsdienste 169
 - Internetdrucken 127
 - IP-Adresse
 - DHCP 237
 - Leasezeitraum 239
 - Multicast 220
 - Oktett 218
 - private 222
 - punktierte Dezimalschreibweise 218
 - registrierte 222
 - Supernetting 223
 - IP-Adressen 33, 115
 - Klasse 218
 - öffentliche 222
 - private 222
 - statische 246
 - Typen 227
 - Windows-Firewall 390
 - zuweisen 224
 - ipconfig 232
 - IPv6 226
 - ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) 234
- J**
- JBOD 57
 - Jeder 100
- K**
- Knoten
 - Gruppenrichtlinien 350
 - Kommunikation
 - DNS 254
- Kompatibilitätsbericht 26
 - Komprimierung 61, 76
 - Konfiguration
 - Benutzerkontensteuerung 369
 - Datenträgerkontingente 107
 - Desktop 350
 - Druckerpools 126
 - Einstellungen exportieren 49
 - erweiterte Drucker- 118
 - Gruppenrichtlinieneinstellungen 350
 - Lokale Benutzer und Gruppen 365
 - Profileinstellungen 396
 - Regeln für Softwareeinschränkung 378
 - Server 237
 - Sicherheitseinstellungen 350
 - Sicherheitsoptionen 361
 - Sicherheitsvorlagen 362
 - Tunnel 233
 - Umgebung 350
 - Windows-Firewall 138, 389
 - Konten
 - Administrator 300
 - deaktivierte 317
 - Gast 300
 - integrierte 300
 - Kontingente 107
 - Konvertieren
 - Datenträger 64
 - Kopfeintrag 307
- L**
- LAN (Local Area Network) 280
 - Lastenausgleich und Failover (LBFO) 37
 - Laufwerkbuchstaben
 - zuweisen 75
 - LDAP-Datenaustauschformat (LDIF) 308
 - LDIFDE.exe 308
 - Leasedauer 244
 - Leasezeitraum 239
 - Link Local Unicast 227
 - Lizenzyierung 17
 - Hyper-V 156
 - Lokale Benutzer und Gruppen 366
 - LPD-Dienst 127

M

MAC

(Media Access Control) 202
Adressbereiche 203
doppelte Adressen 204

MAC-Adressen

Spoofing 208
statische 208
Weiterleitungstabelle 208

Manager

für virtuelle SANs 192
für virtuelle Switches 200

MBR 59

Measure-VM 175

Medien 167

mehrfache lokale Gruppenrichtlinienobjekte 351

Meldungen

DHCP 239
Microsoft Management Console (MMC) 19
Migration 27
Windows Server-Migrationstools 28

Migrationshandbücher 29

minimale Serverschnittstelle 15, 22

Mitgliedsliste 331

MMC (Microsoft Management Console) 19

Multicast 220, 227–228

MX (Mail-Exchanger) 267

N

Namensauflösung 253

Namenserver 254

Namespace 253

NAT

Router 234
NAT (Network Address Translation) 222

Ndtsutil.exe 291

Netdom.exe 34, 315

NetLogon 310

Network Address Translation (NAT) 222

Netzwerk- und Freigabecenter 391

Netzwerkadapter

Bandbreite zusammenfassen 37
Erweiterte Features 208
Hardwarebeschleunigung 207
synthetischer 206
virtuelle 204

Netzwerkadressübersetzung 222, 231

Netzwerkdrucker 115

Freigabe 117

Netzwerke

Erweitern in virtuellen Raum 209
isolierte 209
Konfigurationen 209
virtuelle 197

Netzwerkerkennung 92, 391

Netzwerkmonitor 208

Netzwerkzonenregel 380

Netzwerkzonenregeln

Windows Installer 380

Neueinbindungszeitraum 239

New-ADComputer 313

New-ADGroup 331

New-ADUser 305

New-StoragePool 69

New-VHD 181, 186

New-VM 166

New-VMResourcePool 175

New-VMSwitch 202

NFS

(Network File System) 92

Freigaben 92

NIC-Teamvorgang 37

No eXecute (NX) 159

nodefrag 292

NS (Namenserver) 266

Ntdsutil.exe

nodefrag 292

NTFS 61

O

objectClass 308

Offlinedateien 95

Offline-Domänenbeitritt 317

Oktett 218

Optionen

DHCP 245

Ordner

Freigaben 90

Organisationsadministrator 382

Organisationseinheiten

erstellen 322

Gruppen 321

Sicherheitsprinzipale 321

verschachteln 321

Verwaltung delegieren 323

Organizationally Unique Identifier (OUI) 202

OSI

(Open Systems Interconnect) 197

Switch, virtueller 197

OSI (Open Systems Interconnect) 197

OUI (Organizationally Unique Identifier) 202

P

Partitionen 155

aktive 59

primäre 59

Stile 59

Pass-Through-Datenträger 186

Pfadregel 379

physische Betriebssystemumgebung 16

Point-and-Print 120

PolicyDefinitions 346

Portnummern 390

Portspiegelung 208

POSE (Physical Operating System Environment) 16

Potential Routers List (PRL) 234

Prioritäten

Drucker 124

virtueller Computer 173

Problembehandlung

Netzwerk und Internet 393

Profile 398, 400

Windows-Firewall 393

Protokolle

DHCP 225, 238

Ereignis- 356

FTP 247

ISATAP 234

Routing- 249

SCSI-Fibre Channel 192

Sicherheits- 357

TCP/IP 224, 240, 389

TFTP 247

Tunneling 234

Protokollnummern

Windows-Firewall 390

PTR (Zeiger) 266

PushPrinterConnections.exe 132

PXE (Preboot eXecution Environment) 207, 247

Q

Quell-Starter-Gruppenrichtlinienobjekt 349

Quota *siehe* Datenträgerkontingent

R

RAID-5-Volume 61

RAM

minimaler/maximaler 173

RAM *siehe auch* Arbeitsspeicher

Referrals 259

ReFS 61

Regeln

AppLocker 385

App-Paket- 384

ausführbare 384

Gruppenrichtlinien 399

Hash- 379

importieren/exportieren 398

Internetzonen- 380

manuell erstellen 386

Pfad- 379

Skript- 384

Standardregeln 379

Verbindungssicherheit 400

vordefinierte 398

Windows Installer- 384

Zertifikat- 379

Relay-Agent 248

Remotedesktopdienste 41, 121

Remotedesktopverbindung 121

Remotedesktopverbindungen 35

Remoteserver 144

Remoteserver-Verwaltungstools 143, 346

Remoteverwaltung

Windows-Firewall 138

Remotezugriff 249

-Remove 24

Replikation 291

Reservierungen 246

Resolver 254

Ressourceneinträge 253, 266

Ressourcen-Manager für Dateiserver 92, 95

Ressourcenmessung 175

Reverse-Lookups 261

Reversenamenauflösung 261

- RFC
 2136 (Dynamische Updates) 296
- Richtlinien
 importieren 399
 lokale 356
 Lokaler Computer 364
 Softwareeinschränkung 376
- Richtliniendateien
 Assistenten 399
- RIR (Regional Internet Registry) 222
- Rollen 16
 Active Directory-Domänendienste 281
 AD DS 346
 Datei- und Speicherdiene 62, 92
 DHCP 243
 DHCP-Server 231
 Dienste konfigurieren 51
 Druck- und Dokumentdiene 126
 Hyper-V 153
 migrieren 27
 Remotedesktopdiene 121
 Remotezugriff 231, 249
 virtuelle Festplatten 49
 Windows-Bereitstellungsdienste 248
- Rollendienste
 Dateiserver 92
 Server für NFS 92
 Speicherdiene 92
- Router
 NAT 234
- Routing
 klassenloses domänenübergreifendes 220
- Routing und RAS
 Konsole 249
- S**
- samAccountName 308
 SAM-Kontonamenattribut 304
- SAN
 (Storage Area Network) 190
 SCSI-Fibre Channel 192
- Schattenkopien 106
- Schnellformatierung 76
- SCSI 178
 Fibre Channel 192
- Server
 aktualisieren 25
 Anzahl 56
- für NFS 92
 für verteilte Scanvorgänge 127
 hinzufügen 41, 135
 installieren 14
 Konfiguration 237
 konfigurieren 32
 Lizenzierung 17
 Speicher planen 56
 Verwaltung delegieren 52
 Virtualisierung 16, 56
- Server Core 19
 Fähigkeiten 21
- Servergruppen
 erstellen 142
- Server-Manager 21, 41, 135
 Eigenschaften 144
 Rollen und Features hinzufügen 45
 Server hinzufügen 41, 135
 Servergruppe erstellen 142
- Set-RemoteDesktop 35
- Set-VMMemory 174
- sicherer Desktop 371
- Sicherheit
 Drucker 122
- Sicherheitseinstellungen 356
 effektiver Zugriff 100
- Sicherheitsfilterung 348
- Sicherheitsgruppe 326
- Sicherheitsoptionen
 konfigurieren 361
- Sicherheitsprinzipale 96
 Organisationseinheiten 321
- Sicherheitsstufen
 Standardregeln 379
- Sicherheitsvorlagen 362
 Einstellungen 364
 erstellen 363
 importieren in Gruppenrichtlinienobjekte 364
- Sicherungsfilterung 344
- SID
 Gruppe 334
- Signierung 26
- Single Point of Failure 37
- Skriptregeln 384
- Smart Paging 174
- SMB
 (Server Message Blocks) 92
 Freigaben 92

- SMRemoting 137
 Snap-Ins
 Druckverwaltung 127
 Gruppenrichtlinienverwaltung 346
 Gruppenrichtlinienverwaltungs-Editor 346
 Lokale Benutzer und Gruppen 365
 Sicherheitsvorlagen 362
 Windows-Firewall mit erweiterter Sicherheit 395
 Snapshot 189
 SOA (Autoritätsursprung) 266
 Software Distribution 144
 Softwareeinschränkung 376
 Eigenschaften 381
 Hashregel 379
 Netzwerkzonenregel 380
 Pfadregel 379
 Regeln 378
 Zertifikatregel 379
 Softwareeinstellungen 350
 Speicher
 Anforderungen 57
 dynamischer 172
 lokaler 56
 planen 56
 reservieren 171
 Speicherplätze *siehe* Storage Spaces
 Speicherpools 58
 erstellen 65
 Festplatten, geeignete 68
 New-StoragePool 69
 Spoofing 208
 Spooler 114
 SRV-Einträge 295
 Stammhinweise 269
 Stammnamenserver 255
 Standarddomänencontrollerrichtlinie 316
 Standardregeln 379
 AppLoker 385
 Starter-Gruppenrichtlinienobjekte 345, 349
 Storage Spaces
 JBOD 57
 Stripesetvolume 60
 Strukturdomäne 288
 Stubzonen 264
 Subnetze 222
 Subnetzmarske 218
 IPv6 227
 Supernetting 223
 Supervisor 155
 Switches
 virtuelle 197
 Sysprep.exe 185
 Systemeigenschaften
 Remotedesktop 33
 Systemsteuerung
 Benutzerkonten 365
 Netzwerk- und Freigabecenter 391
 Windows-Firewall- 391
- T**
- telephoneNumber 308
 Telnet 18
 Teredo 234
 Terminaldienste 41
 TFTP (Trivial File Transfer Protocol) 247
 Time to Live (TTL) 258
 Tools
 Benutzer erstellen 301
 Toplevel-Domäne 255
 Treibersignatur 26
 TTL
 ändern 259
 Time to Live 258
 Tunnel 232
- U**
- Übergreifendes Volume 60
 Überwachung 356
 Richtlinie konfigurieren 358
 UDP
 (User Datagram Protocol) 390
 Unicast 227
 standortlokale Adressen 228
 Uninstall-WindowsFeature 24
 Unique Local Unicast 227
 Upgrade 25
 Upgrade-Pfade 25
 userPrincipalName 308
 USV (Unterbrechungsfreie Stromversorgung) 27

V

Verbindungssicherheitsregeln 400
Vererbung
 Berechtigungen 99
 Gruppenrichtlinienobjekte 348
Verschlüsselung
 Freigaben 94
Verteilergruppe 326
Verwaltung
 delegieren 52
Verzeichnisdienst 280
Verzeichnisdienstwiederherstellung 284, 287
Virtual Machine Monitor (VMM) 154
Virtual Machines (VMs) *siehe* virtuelle Computer
Virtual PC 178
Virtualisierung 16, 56
 Architektur 154
 Hypervisor 154
 Storage Spaces 57
 Typen 155
Virtualisierungsdienstclient 206
Virtualization Service Client (VSC) 206
Virtualization Service Provider (VSP) 206
virtuelle Computer 153
 Abbildungseiten 168
 Arbeitsspeicher 171
 Betriebssystem installieren 167
 erstellen 162
 Medien 167
virtueller Datenträger 58
VLAN-Bezeichner 202
VLSM 221
VMBus 206
VMM (Virtual Machine Monitor) 154
VMs (Virtual Machines) *siehe* virtuelle Computer
Volumes
 Bezeichnung 76
 einfaches erstellen 73
Volumeschattenkopie 106
Volumetypen 60
Vorgängerversionen 107
Vorlagen
 administrative 350
 Benutzer 306
Vorlagendateien, administrative (ADM) 345
VOSE (Virtual Operating System Environment) 16
VSC (Virtualization Service Client) 206

VSP

Virtualization Service Provider 206

W

WAN (Wide Area Network) 280
Weiterleitungen 260
Weiterleitungstabelle 208
Windows Deployment Services (WDS) 248
Windows Installer
 Netzwerkzonenregel 380
 Regeln 384
Windows PowerShell
 Active Directory-Domäendienste 289
 ADDSDeployment 289
 Add-WindowsFeature 142
 Arbeitsspeicher 174
 Benutzer anlegen 305
 Benutzerobjekt erstellen 309
 Computerobjekte 313
 Domänencontroller tiefer stufen 294
 Enable-VMResourceMetering 175
 Enter-PSSession 141
 Exit-PSSession 142
 Firewall-Regeln 138
 Get-NetFirewallRule 138
 Get-WindowsFeature 142
 Hyper-V installieren 161
 Install-AddDomain 289
 Install-AddDomainController 289, 291
 Install-AddForest 289
 Install-WindowsFeature 142, 161, 289
 Measure-VM 175
 New-ADComputer 313
 New-ADGroup 331
 New-ADUser 305
 New-VHD 181, 186
 New-VM 166
 New-VMResourcePool 175
 New-VMSwitch 202
 Ressourcenmessung 175
 Set-NetFirewallRule 138
 Set-VMMemory 174
 SMRemoting 137
 virtuellen Computer erstellen 166
 virtuellen Switch erstellen 202
 WinRM 137
 WinRM konfigurieren 137

-
- Windows Server-Migrationtools 28
 - Windows-Bereitstellungsdienste 248
 - Windows-Einstellungen 350
 - Windows-Firewall 389
 - Anwendungen zulassen 394
 - mit erweiterter Sicherheit 390, 395
 - Profile 393
 - Profileinstellungen 396
 - Remoteverwaltung 138
 - Systemsteuerung 391
 - Windows-Firewall *siehe auch* Firewall
 - WindowsPowerShell
 - Set-RemoteDesktop 35
 - Speicherpool erstellen 69
 - Uninstall-WindowsFeature 24
 - Windows-Remoteverwaltung (WinRM) 137
 - WinRM
 - (Windows Remote Management) 137
 - Listener 141
 - winrm quickconfig 141
 - WinSxS 23
- WMI
 - (Windows Management Instrumentation) 35, 137
 - WinRM konfigurieren 137
 - WWNNs (World Wide Node Names) 192
 - WWPNs (World Wide Port Names) 192
- ## Z
- Zeitzone 33
 - Zertifikatregel 379
 - Zonen 264
 - erstellen 263
 - sekundäre 264
 - Stub- 264
 - Zonenübertragung 264
 - Zugriff
 - effektiver 100
 - Zugriffsbasierte Aufzählung 95
 - Zugriffssteuerungseintrag 96
 - Zugriffssteuerungseinträge 96
 - Zugriffssteuerungsliste 96
 - Zugriffstoken 325
 - Zwischenspeicherung
 - clientseitige 95

Der Autor

Craig Zacker ist Autor und Co-Autor dutzender Bücher, Artikel und Websites zu den Themen Betriebssysteme, Netzwerke und PC-Hardware, u.a. *Windows Small Business Server 2011 Administrator's Pocket Consultant* und *MCITP Self-Paced Training Kit for Exam 70-686: Windows 7 Desktop Administrator* (beide für Microsoft Press, USA). Außerdem war er bereits Lehrbeauftragter für Englisch, Netzwerkadministrator, Webmaster, Schulungsleiter, Fotolaborant, Bibliotheksangestellter, Student und Zeitungsjunge. Er wohnt in einem kleinen Haus zusammen mit seiner wunderbaren Frau und einer neurotischen Katze.

Nutzungsbedingungen; Haftungsbeschränkungen

1. Ihr Exemplar wird Ihnen ausschließlich für Ihre persönliche, nichtgewerbliche Nutzung zur Verfügung gestellt, wobei Einschränkungen gemäß diesen Nutzungsbedingungen und dem Urheberrecht Deutschlands sowie anderer Länder gelten.
2. Sie dürfen die nachfolgenden Handlungen weder selbst vornehmen noch von anderen vornehmen lassen:
 - (a) Ihr Exemplar ganz oder in Teilen verändern, veröffentlichen, übertragen oder öffentlich wiedergeben oder davon abhängige eigene Werke erstellen, soweit dies nicht ausdrücklich nach diesen Nutzungsbedingungen oder den Schranken des Urheberrechts gemäß §§ 44a ff. UrhG erlaubt ist.
 - (b) Das Exemplar ins Usenet oder auf eine externe Internetseite hochladen oder das Exemplar Dritten auf andere Weise zur Verfügung stellen, etwa über ein Intranet, einen öffentlichen oder privaten Hostingdienst, einem peer-to-peer Netzwerk, oder über RSS-Feeds, soweit dies nicht ausdrücklich von diesen Nutzungsbedingungen oder gemäß §§ 44a ff. UrhG erlaubt ist; und/oder
 - (c) Dritten die Ihnen nach diesen Nutzungsbedingungen eingeräumten Rechte ganz oder teilweise übertragen, lizenziieren oder in anderer Form weitergeben.
3. Soweit dies nicht ausdrücklich in diesen Nutzungsbedingungen oder den Schranken des Urheberrechts gemäß §§ 44a ff. UrhG erlaubt ist, darf Ihr Exemplar nicht gespeichert, vervielfältigt oder auf beliebige Art und Weise übertragen werden, ohne dass der Urheberrechtsinhaber dies im Vorwege ausdrücklich schriftlich erlaubt hat. Der Händler und seine Zulieferer behalten sich sämtliche Rechte vor, die nicht ausdrücklich in diesen Nutzungsbedingungen eingeräumt werden. Der Händler oder seine Zulieferer sind Inhaber sämtlicher Ansprüche, urheberrechtlicher Nutzungsrechte und sonstiger geistiger Eigentumsrechte am Exemplar. Sie dürfen Urheberrechts-hinweise oder andere Herkunftshinweise, die sich am Exemplar befinden, weder entfernen noch sonst unkenntlich machen.
4. Vorbehaltlich der Regelungen in Ziffer 6 bestätigen Sie, dass Sie Ihr Exemplar und dessen Inhalt auf eigene Gefahr verwenden und dass das Exemplar „wie besehen“ zur Verfügung gestellt wird, ohne jegliche zusätzliche Versicherung oder Garantie irgendwelcher Art, ausdrücklich oder konkludent (sei es gewohnheitsrechtlich, gesetzlich oder auf sonstiger Grundlage). Soweit dies rechtlich möglich ist, schließen der Händler und seine Zulieferer jegliche Bedingungen, Versicherungen, Bestätigungen und Garantien aus (insbesondere auch konkludente Garantien bezüglich der Qualität oder der Eignung des Exemplars oder seines Inhalts für einen bestimmten Zweck).
5. Unbeschadet der Regelungen in Ziffer 6 bestätigen Sie und stimmen Sie zu, dass der Händler und seine Zulieferer nicht für folgende Ansprüche haftbar ist:
 - (a) Direkte Verluste, Ansprüche, Schäden oder Verletzungen;
 - (b) Indirekte Verluste, Ansprüche oder Schäden, oder jegliche Buszahlungen, atypische Schäden, beiläufig entstandene Schäden oder Folgeschäden jeder Art, die nicht unmittelbar mit dem Vorgang im Zusammenhang stehen, der Ihren Anspruch begründet hat;
 - (c) Entgangene Gewinne oder Ersparnisse;
 - (d) Verlust oder Beschädigung von Daten oder Informationen;
 - (e) Verlust von Vertragsbeziehungen, Geschäft oder geschäftlichen Gelegenheiten oder
 - (f) Schäden am Ruf oder Reputation;dies geltend in jedem Fall, unabhängig davon, ob unmittelbare oder mittelbare Schäden geltend gemacht werden und unabhängig davon, ob Ansprüche aus Vertrag, unerlaubter Handlung (insbesondere wegen Fahrlässigkeit), Gefährdungshaftung oder aus anderen Gründen hergeleitet werden, soweit sie im Zusammenhang mit diesem Exemplar oder dessen Inhalt und/oder jeglicher Nutzung derselben entstehen, auch soweit der Händler oder seine Zulieferer im Vorwege gewarnt wurden oder sich der Möglichkeit derartiger Verluste oder Schäden bewusst waren.
6. Keine Regelung dieser Nutzungsbedingungen verringert oder beseitigt eine Haftung seitens des Händlers oder dessen Zulieferer für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder für sonstige Schäden, die auf einer grob fahrlässigen Pflichtverletzung, auf Vorsatz oder einer arglistigen Täuschung seitens der jeweils haftenden Partei oder deren Erfüllungsgehilfen beruht oder für sonstige Haftungsansprüche, die nach deutschem Recht nicht ausgeschlossen oder eingeschränkt werden können.