

William R. Stanek

Microsoft Windows 8 Ratgeber für Administratoren



Der praktische Begleiter
für die tägliche Arbeit

Microsoft
Press

William R. Stanek

Microsoft Windows 8 – Ratgeber für Administratoren

Microsoft
Press

Dieses Buch ist die deutsche Übersetzung von:
William R. Stanek: *Windows 8 Administration – Pocket Consultant*
Microsoft Press, Redmond, Washington 98052-6399
Copyright 2012 by Microsoft Corporation

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. Die in diesem Buch erwähnten Software- und Hardwarebezeichnungen sind in den meisten Fällen auch eingetragene Marken und unterliegen als solche den gesetzlichen Bestimmungen. Der Verlag richtet sich im Wesentlichen nach den Schreibweisen der Hersteller.

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
14 13 12

ISBN 978-3-86645-690-7, PDF-E-Book-ISBN 978-3-84834-003-3

Copyright der deutschen Ausgabe:
© 2013 O'Reilly Verlag GmbH & Co. KG
Balthasarstr. 81, 50670 Köln
Alle Rechte vorbehalten

Übersetzung: Detlef Johannis, Kempten, Michael Ringel, Bonn
Korrektorat: Claudia Mantel-Rehbach, Entraching
Fachlektorat und Satz: Günter Jürgensmeier, München
Umschlaggestaltung: Hommer Design, Haar (www.HommerDesign.com)
Layout und Gesamtherstellung: Kösel, Krugzell (www.KoeselBuch.de)

*Für meine Frau – viele Jahre, durch viele Bücher, Millionen
von Wörtern und Abertausende von Seiten hindurch war
sie für mich da, half mir durch Unterstützung und
Ermutigung und machte jeden Ort, an dem wir lebten, zu
einem Zuhause.*

*Für meine Kinder – sie halfen mir, die Welt mit neuen
Augen zu sehen, zeigten außergewöhnliche Geduld und
endlose Liebe und machten jeden Tag zu einem Abenteuer.*

*Für Karen, Martin, Lucinda, Juliana und viele andere, die
viel oder auch nur ein wenig geholfen haben.*

William R. Stanek

Inhaltsverzeichnis

Einführung	17
Für wen ist dieser Ratgeber konzipiert?	18
Wie ist dieses Buch aufgebaut?	19
In diesem Buch verwendete Konventionen	19
Support	20
1 Einführung in die Windows 8-Administration	21
Überblick über Windows 8	22
Grundlagen der 64-Bit-Architektur	26
Bereitstellen von Windows 8	28
Verwenden von DISM	30
Grundlagen von Windows-Abbildern	31
Verwalten des Zugriffs und Vorabbereitstellen von Computern	33
Anpassen von Windows-Abbildern	35
Installieren von Windows 8	37
Vorbereiten der Windows 8-Installation	38
Installieren von Windows 8	39
Ausführen von Windows 8	44
Arbeiten mit dem Wartungscenter und Aktivieren von Windows	45
Verwenden von Windows 8 in Gruppen und Domänen	46
Energiesparpläne, Ruhezustände und Herunterfahren	52
Architektur von Windows 8	54
2 Konfigurieren von Windows 8-Computern	59
Support für Windows 8-Computer	60
Arbeiten mit der Konsole <i>Computerverwaltung</i>	61
Ermitteln von Grunddaten über System und Leistung	64
Abrufen von ausführlicheren Systeminformationen	68
Arbeiten mit der WMI-Steuerung	70
Verwenden von Systemprogrammen	72
Arbeiten mit der Datenträgerbereinigung	73
Überprüfen von Systemdateien mit der Dateisignaturverifizierung	75
Verwalten der Systemkonfiguration und der Systemstartoptionen	76
Verwalten der Systemeigenschaften	82
Die Registerkarte <i>Computername</i>	83
Die Registerkarte <i>Hardware</i>	83
Die Registerkarte <i>Erweitert</i> : Leistungsoptionen	84
Die Registerkarte <i>Erweitert</i> : Umgebungsvariablen	88
Die Registerkarte <i>Erweitert</i> : Systemstart und Wiederherstellung	91
Die Registerkarte <i>Computerschutz</i>	94
Die Registerkarte <i>Remote</i>	97

Konfigurieren der Energieverwaltung	97
Verwalten von Energieoptionen in der Befehlszeile	98
Verwenden von Energieplänen	100
Einstellen und Optimieren von Energieplänen	104
Erstellen von Energiesparplänen	106
Einstellen der Netzschalteroptionen und des Kennwortschutzes bei Reaktivierung	108
Verwalten von Energieoptionen mit Richtlinieneinstellungen	109
Einstellen der Aktionen bei niedrigen Akkuladezuständen	110

3 Anpassen von Desktop und Benutzeroberfläche	113
Optimieren der PC-Einstellungen	114
Die Seite <i>Anpassen</i>	114
Die Seite <i>Benutzer</i>	116
Die Seite <i>Benachrichtigungen</i>	116
Die Seiten <i>Suche</i> , <i>Teilen</i> und <i>Datenschutz</i>	116
Die Seite <i>Einstellungen synchronisieren</i>	117
Arbeiten mit Desktops und Autostartanwendungen	118
Erstellen von Verknüpfungen für Desktops und Autostart	118
Hinzufügen oder Entfernen von Autostartprogrammen	121
Anpassen der Taskleiste	122
Funktionsweise der Taskleiste	122
Verknüpfungen an die Taskleiste anheften	123
Ändern der Größe und Position der Taskleiste	123
Automatisches Ausblenden, Fixieren und Steuern der Sichtbarkeit der Taskleiste	123
Steuern der Anwendungen im Infobereich	124
Optimieren der Symbolleisten	125
Anzeigen von Symbolleisten	125
Erstellen persönlicher Symbolleisten	126
Verwenden von Designs	127
Anwenden und Entfernen von Designs	127
Anpassen und Erweitern von Designs	128
Löschen benutzerdefinierter Designs	129
Optimieren der Desktopumgebung	129
Einstellen des Desktophintergrunds	129
Verwenden der Standarddesktopsymbole	131
Bildschirmschoner	133
Konfigurieren eines Bildschirmschoners mit Kennwortschutz	133
Verringern der Ressourcenbelastung durch Bildschirmschoner	134
Einstellen der Energiesparoptionen für Monitore	135
Ändern des Erscheinungsbilds und der Grafikeinstellungen	136
Konfigurieren von Fensterfarbe und -darstellung	136
Optimieren der Lesbarkeit	138
Konfigurieren von Grafikeinstellungen	139
Beseitigen von Anzeige Problemen	146

4 Verwalten von Firmware, Startkonfiguration und Systemstart	149
Firmwareoptionen	150
Firmwareschnittstellentypen und Systemstartdaten	150
Systemstartdienste, Laufzeitdienste und andere Elemente	151
UEFI	152
Start- und Energiemodi	154
Arbeiten mit Firmwareschnittstellen	155
Aufbau der Firmwareschnittstellen	156
Energiesparmodi und Energieverwaltung	159
Analysieren und Beseitigen von Startproblemen	162
Problembehebung in der Startphase 1	163
Problembehebung in der Startphase 2	164
Problembehebung in der Startphase 3	166
Problembehebung in der Startphase 4	166
Problembehebung in der Startphase 5	167
Verwalten der Systemstartkonfiguration	168
Einstellen von Start- und Wiederherstellungsoptionen	168
Verwalten der Systemstartkonfiguration	169
Arbeiten mit dem BCD-Editor	171
Verwalten des BCD-Speichers	172
Anzeigen von BCD-Einträgen	173
Erstellen und Auswählen des BCD-Speichers	176
Importieren und Exportieren des BCD-Speichers	177
Erstellen, Kopieren und Löschen von BCD-Einträgen	177
Einstellen der Werte von BCD-Einträgen	178
Ändern der Optionen für DEP und PAE	182
Anpassen der Reihenfolge, in der Betriebssysteme angezeigt werden	183
Ändern des Eintrags für das Standardbetriebssystem	183
Ändern des Standardzeitlimits	184
Die Startreihenfolge kurzzeitig ändern	184
5 Konfigurieren von Benutzer- und Computerrichtlinien	185
Grundlagen von Gruppenrichtlinien	186
Bearbeiten und Benutzen der lokalen Gruppenrichtlinien	187
Öffnen und Benutzen von Richtlinien für Standorte, Domänen und Organisationseinheiten	190
Konfigurieren von Richtlinien	192
Anzeigen von Richtlinien und Vorlagen	193
Aktivieren, Deaktivieren und Konfigurieren von Richtlinien	194
Hinzufügen oder Entfernen von Vorlagen	195
Arbeiten mit Datei- und Datenverwaltungsrichtlinien	195
Konfigurieren von Datenträgerkontingentrichtlinien	196
Konfigurieren von Systemwiederherstellungsrichtlinien	197
Konfigurieren von Offlinedatei richtlinien	198
Verwenden von Zugriffs- und Verbindungsrichtlinien	202
Konfigurieren von Netzwerkrichtlinien	202
Konfigurieren von Remoteunterstützungsrichtlinien	204

Verwenden von Computer- und Benutzerskriptrichtlinien	205
Steuern der Skriptausführung durch Richtlinien	206
Zuweisen von Computerskripts für das Starten und Herunterfahren	208
Zuweisen von Benutzerskripts für An- und Abmeldung	208
Verwenden von Anmelde- und Startrichtlinien	209
Einstellen der Autostartrichtlinien	209
Deaktivieren von Ausführungslisten durch Gruppenrichtlinien	210
6 Automatisieren der Windows 8-Konfiguration	213
Grundlagen von Gruppenrichtlinieneinstellungen	214
Konfigurieren von Gruppenrichtlinieneinstellungen	216
Arbeiten mit Verwaltungsaktionen	216
Arbeiten mit Bearbeitungszuständen	217
Arbeiten mit alternativen Aktionen und Zuständen	219
Verwalten von Einstellungselementen	220
Erstellen und Verwalten eines Einstellungselements	220
Konfigurieren von Optionen auf der Registerkarte <i>Gemeinsame Optionen</i>	222
7 Verwalten von Benutzerzugriff und Sicherheit	225
Grundlagen von Benutzer- und Gruppenkonten	226
Grundlagen von lokalen Benutzerkonten	227
Grundlagen von Gruppenkonten	229
Domänenanmeldung und lokale Anmeldung	231
Benutzerkontensteuerung und Anhebungsaufforderungen	232
Ein zweiter Blick auf Standardbenutzer- und Administratorkonten	232
Optimieren von Benutzerkontensteuerung und Administratorgenehmigungsmodus	234
Verwalten der lokalen Anmeldung	237
Erstellen lokaler Benutzerkonten in einer Heimnetzgruppe oder Arbeitsgruppe	238
Gewähren der lokalen Anmeldung bei vorhandenem Domänenkonto	240
Ändern des Typs eines lokalen Benutzerkontos	241
Wechseln zwischen synchronisierten und normalen Konten	242
Festlegen von Kennwörtern für lokale Benutzerkonten	242
Wiederherstellen der Kennwörter von lokalen Benutzerkonten	243
Kontrollieren der Anmeldung	244
Löschen von Konten und Sperren des lokalen Zugriffs auf Arbeitsstationen	246
Verwalten gespeicherter Anmeldeinformationen	246
Hinzufügen von Windows- oder generischen Anmeldeinformationen	247
Hinzufügen von zertifikatbasierten Anmeldeinformationen	249
Bearbeiten von Anmeldeinformationen	250
Sichern und Wiederherstellen von Anmeldeinformationen	250
Löschen von Anmeldeinformationen	251
Verwalten lokaler Benutzerkonten und Gruppen	251
Erstellen von lokalen Benutzerkonten	252
Erstellen lokaler Gruppen für Arbeitsstationen	254
Verwalten der Mitglieder lokaler Gruppen	256
Aktivieren und Deaktivieren lokaler Benutzerkonten	257
Erstellen eines sicheren Gastkontos	258
Umbenennen lokaler Benutzerkonten und Gruppen	259
Löschen lokaler Benutzerkonten und Gruppen	259

Verwalten des Remotezugriffs auf Arbeitsstationen	260
Konfigurieren der Remoteunterstützung	261
Konfigurieren des Remotedesktopzugriffs	263
Herstellen von Remotedesktopverbindungen	266
8 Installieren und Verwalten von Programmen	269
Verwalten von Desktop-Apps	270
Arbeiten mit Apps: Die Grundlagen	270
Konfigurieren von vertrauenswürdigen Apps und Windows Store-Zugang	271
Verbessern der Sicherheit für Apps und Außerkraftsetzen der Standardeinstellungen	271
Verbessern der Netzwerksicherheit für Apps	273
Verwalten der Anwendungsvirtualisierung und der Ausführungsebenen	273
Zugriffstoken und Ortsvirtualisierung	274
Anwendungsintegrität und Ausführungsebenen	275
Festlegen der Ausführungsebenen	277
Optimieren der Virtualisierung und die Anhebungsaufforderung bei Installationen	279
Programminstallation: Die Grundlagen	280
Verwenden von Autorun	281
Anwendungsinallation und Kompatibilität	281
Bereitstellen von Anwendungen für ausgewählte Benutzer oder für alle Benutzer	283
Bereitstellen von Anwendungen mithilfe von Gruppenrichtlinien	285
Konfigurieren der Programmkompatibilität	286
Besonderheiten bei der Installation von 16-Bit- und MS-DOS-Programmen	286
Erzwingen der Programmkompatibilität	287
Verwalten von installierten und laufenden Programmen	290
Verwalten aktuell ausgeführter Programme	291
Verwalten, Reparieren und Deinstallieren von Programmen	292
Festlegen der Standardprogramme	293
Verwalten des Befehlspaths	295
Verwalten von Dateierweiterungen und Dateiverknüpfungen	297
Einstellen der automatischen Wiedergabe	299
Hinzufügen und Entfernen von Windows-Funktionen	300
9 Verwalten von Hardwaregeräten und Treibern	303
Arbeiten mit dem automatischen Hilfesystem	304
Benutzen von <i>Hilfe und Support</i>	304
Anpassen von <i>Hilfe und Support</i>	310
Arbeiten mit den Supportdiensten	317
Verwalten von Diensten mithilfe von Richtlinieneinstellungen	322
Installieren und Warten von Geräten: Die Grundlagen	323
Installieren vorhandener Geräte	324
Installieren von internen Geräten, USB-, FireWire- und eSATA-Geräten	326
Installieren von Drahtlosnetzwerk-, Netzwerk- und Bluetooth-Geräten	329
Installieren von lokalen und Netzwerkdruckern	331
Einführung in den Geräte-Manager	335
Arbeiten mit Gerätetreibern	337
Grundlagen der Gerätetreiber	337
Verwenden von signierten und nichtsignierten Gerätetreibern	338

Überprüfen der Treiberinformationen	338
Installieren und Aktualisieren von Gerätetreibern	339
Aktivieren und Deaktivieren bestimmter Gerätetypen	342
Einschränken der Geräteinstallation durch Gruppenrichtlinien	343
Wiederherstellen der Vorversion eines Treibers	344
Entfernen der Gerätetreiber für ausgebaute Geräte	345
Deinstallieren, erneutes Installieren und Deaktivieren von Gerätetreibern	345
Aktivieren und Deaktivieren von Hardwaregeräten	346
Beseitigen von Hardwareproblemen	346

10 Erledigen von Wartungs- und Supportaufgaben	351
Verwalten automatischer Updates	352
Windows Update: Die Grundlagen	352
Wiederherstellen von Windows-Binärdateien und -Komponenten via Windows Update	354
Konfigurieren der automatischen Updates	355
Suchen nach Updates	359
Anzeigen des Updateverlaufs und der installierten Updates	359
Entfernen von Updates zur Problembehebung	360
Ausblenden verfügbarer Updates	360
Wiederherstellen abgelehnter Updates	360
Verwenden der Remoteunterstützung zur Problembehebung	361
Funktionsweise der Remoteunterstützung	361
Erstellen von Remoteunterstützungseinladungen	363
Anbieten von Remoteunterstützung oder Beantworten einer Remoteunterstützungseinladung	365
Erkennen und Beheben von Windows 8-Fehlern	366
Verwenden der Ereignisprotokolle zur Fehlerüberprüfung und Fehlerdiagnose	366
Anzeigen und Verwalten der Ereignisprotokolle	367
Planen von Wartungsarbeiten	368
Funktionsweise der Aufgabenplanung	368
Anzeigen und Verwalten von Aufgaben auf lokalen und Remotesystemen	370
Erstellen von geplanten Aufgaben	371
Problembehandlung für geplante Aufgaben	372
Sichern und Wiederherstellen eines Computers	373
Sichern und Wiederherstellen von Dateien und Ordnern mit Vorgängerversionen	373
Wiederherstellen nach einem fehlgeschlagenen Start	374
Wiederherstellen nach einer fehlgeschlagenen Reaktivierung	375
Reparieren eines Computers, um den Systemstart zu ermöglichen	375
Sichern und Wiederherstellen des Systemzustands mit der Systemwiederherstellung	377
Erstellen und Verwenden des Dateiversionsverlaufs	381
Wiederherstellen persönlicher Daten	385
Problembehandlung für Systemstart und Herunterfahren	385
Behebung von Problemen beim Neustart und dem Herunterfahren des Systems	385
STOP-Fehler und ihre Bedeutung	386

11 Arbeiten mit TPM und BitLocker-Laufwerkverschlüsselung	389
Einrichten von TPM	390
TPM: Die Grundlagen	390
TPM: Verwaltung und Richtlinien	392
Aktivieren von TPM	395
Initialisieren und Vorbereiten eines TPM für den ersten Einsatz	396
Ein- und Ausschalten eines initialisierten TPM	399
Löschen des TPM	399
Ändern des TPM-Besitzerkennworts	401
BitLocker-Laufwerkverschlüsselung: Grundlagen	402
Funktionsweise der BitLocker-Laufwerkverschlüsselung	402
Hardwareverschlüsselung, sicherer Start und Netzwerkentsperrung	405
Bereitstellen der BitLocker-Laufwerkverschlüsselung	408
Verwalten der BitLocker-Laufwerkverschlüsselung	412
Vorbereiten der BitLocker-Laufwerkverschlüsselung	413
Aktivieren von BitLocker auf anderen Volumes als dem Systemvolume	415
Aktivieren von BitLocker auf USB-Flashlaufwerken	417
Aktivieren von BitLocker auf Systemvolumes	419
Verwalten von BitLocker und Beseitigen von Problemen	423
12 Verwalten von Festplattenlaufwerken und Dateisystemen	427
Grundlagen der Datenträgerverwaltung	428
Verwenden der Computerkonsole	431
Verwenden der Datenträgerverwaltung	433
Verwenden von FSUtil und DiskPart	435
Optimieren der Laufwerksleistung	436
Funktionsweise und Verwendung von Windows-ReadyBoost	436
Aktivieren und Konfigurieren von ReadyBoost	437
Funktionsweise und Verwendung von Windows-ReadyDrive	438
Funktionsweise und Verwendung von Windows-SuperFetch	439
Basisdatenträger und dynamische Datenträger	441
Verwenden von Basisdatenträgern und dynamischen Datenträgern	444
Bedeutung der Laufwerksbezeichnungen	444
Installieren und Initialisieren neuer Festplattenlaufwerke	446
Ändern der Partitionstabellenart bei einem Datenträger	447
Kennzeichnen einer Partition als aktiv	447
Konvertieren eines Basisdatenträgers in einen dynamischen Datenträger, und umgekehrt	448
Verwenden von Datenträgern, Partitionen und Volumes	450
Partitionieren und Vorbereiten von Festplattenlaufwerken	452
Erstellen von Partitionen, logischen Laufwerken und einfachen Volumes	452
Erstellen von übergreifenden und Stripesetvolumes	455
Erweitern und Verkleinern von Volumes	457
Formatieren von Partitionen und Volumes	458
Zuweisen, Ändern oder Entfernen von Laufwerksbuchstaben und Laufwerkspfad	459
Zuweisen, Ändern oder Löschen einer Volumebezeichnung	461
Löschen von Partitionen, Volumes und logischen Laufwerken	461
Konvertieren eines Volumes nach NTFS	462

Wiederherstellen eines einfachen, übergreifenden oder Stripesetvolumes	464
Wiederherstellen eines Stripesets mit Parität	464
Verwenden der Datenträgerspiegelung	465
Erstellen von gespiegelten Volumes	465
Aufheben der Spiegelung	466
Entfernen eines Spiegelsatzes	466
Einbauen eines dynamischen Datenträgers in einen anderen Computer	467
Beseitigung auftretender Datenträgerprobleme	468
Reparieren von Fehlern und Inkonsistenzen auf Datenträgern	471
Prüfen auf Laufwerksfehler	472
Defragmentieren von Datenträgern	475
Neusynchronisieren und Reparieren eines Spiegelsatzes	477
Reparieren eines gespiegelten Systemvolumes, um den Systemstart zu ermöglichen	478
Arbeiten mit Wechselmediengeräten	479
Arbeiten mit Daten-CDs und -DVDs	481
Brennen von Medien: Die Grundlagen	481
Bereitstellen von ISO-Abbildern	482
ISO-Abbilder auf Disk brennen	482
Gemasterte Disks brennen	483
Disks mit Livedateisystemen brennen	484
Ändern der Standardbrennoptionen	485
Verwalten von Datenträgerkomprimierung und Dateiverschlüsselung	485
Komprimieren von Datenträgern und Daten	485
Verschlüsseln von Laufwerken und Daten	488

13 Verwalten der Dateisicherheit und Ressourcenfreigabe	493
Optionen für die Dateisicherheit und Dateifreigabe	494
Kontrollieren des Zugriffs auf Dateien und Ordner mit NTFS-Berechtigungen	499
Bedeutung und Verwendung der Standardberechtigungen	499
Zuweisen von speziellen Berechtigungen	504
Zuweisen von anspruchsbasierten Berechtigungen	508
Dateibesitz und Berechtigungszuweisung	510
Vererben von Berechtigungen	511
Ermitteln der effektiven Berechtigungen und Problembehebung	514
Freigeben von Dateien und Ordnern im Netzwerk	516
Kontrollieren des Zugriffs auf Netzwerkfreigaben	516
Erstellen einer freigegebenen Ressource	517
Erstellen und Verwalten von freigegebenen Ordnern mit Gruppenrichtlinien	522
Verwenden von freigegebenen Ressourcen	523
Verwenden von freigegebenen Ordnern zur Administration	527
Problembehebung in der Dateifreigabe	528
Verwenden und Konfigurieren der Freigabe öffentlicher Ordner	530
Verwenden der Freigabe in öffentlichen Ordnern	530
Konfigurieren der Freigabe öffentlicher Ordner	531
Überwachen von Datei- und Ordnerzugriff	532
Aktivieren der Überwachung für Dateien und Ordner	532
Konfigurieren und Analysieren der Überwachung	532

14 Verwalten von Datenzugriff und Verfügbarkeit	537
Konfigurieren von Datei-Explorer-Optionen	538
Anpassen des Datei-Explorers	538
Konfigurieren erweiterter Datei-Explorer-Optionen	541
Verwalten von Offlinedateien	544
Grundlagen der Offlinedateien	544
Dateien und Ordner offline verfügbar machen	546
Verwalten der Offlinedateisynchronisierung	548
Konfigurieren von Datenträgnutzungslimits für Offlinedateien	553
Verwalten der Verschlüsselung für Offlinedateien	554
Sperren der Offlineverwendung von Dateien	554
Konfigurieren von Datenträgerkontingenten	555
Verwenden von Datenträgerkontingenten	555
Aktivieren von Datenträgerkontingenten auf NTFS-Volumes	557
Anzeigen von Datenträgerkontingenteinträgen	558
Erstellen von Datenträgerkontingenteinträgen	559
Aktualisieren und Anpassen von Datenträgerkontingenteinträgen	560
Löschen von Datenträgerkontingenteinträgen	560
Exportieren und Importieren von Datenträgerkontingenteinträgen	561
Deaktivieren von Datenträgerkontingenten	562
Verwenden von BranchCache	563
15 Konfigurieren und Problembehandlung von TCP/IP-Netzwerken	567
Überblick über die Netzwerkfunktionen von Windows 8	568
Netzwerkerkennung und Netzwerkkategorien	568
Verwenden des Netzwerk-Explorers	570
Verwenden des Netzwerk- und Freigabecenters	571
Installieren der Netzwerkkomponenten	572
Verwenden von TCP/IP und des dualen IP-Stacks	572
Installieren von Netzwerkadaptern	575
Installieren der Netzwerkdienste (TCP/IP)	575
Konfigurieren von Netzwerkverbindungen	576
Konfigurieren statischer IP-Adressen	577
Konfigurieren dynamischer und alternativer IP-Adressen	579
Konfigurieren mehrerer Gateways	580
Konfigurieren der DNS-Auflösung	581
Konfigurieren der WINS-Namenszuordnung	583
Verwalten von Netzwerkverbindungen	585
Aktivieren und Deaktivieren von Netzwerkverbindungen	585
Überprüfen von Status, Geschwindigkeit und Aktivität von Netzwerkverbindungen	586
Anzeigen der Netzwerkkonfiguration	587
Umbenennen von Netzwerkverbindungen	588
Problembehandlung und Testen von Netzwerkeinstellungen	588
Diagnostizieren und Beheben von Netzwerkverbindungsproblemen	588
Diagnostizieren und Beheben von Internetverbindungsproblemen	589
Durchführen von einfachen Standardtests	590
Beheben von IP-Adressierungsproblemen	591

Freigeben und Erneuern der DHCP-Zuweisung	592
Registrieren von DNS-Einträgen und Leeren des DNS-Auflösungscaches	593
16 Verwalten von mobilen Netzwerken und Remotezugriff	595
Konfigurieren des Netzwerks auf mobilen Geräten	596
Verwenden des Windows-Mobilitätscenters	597
Konfigurieren von dynamischen IP-Adressen	598
Konfigurieren von alternativen privaten IP-Adressen	599
Verbinden mit Netzwerkprojektoren	601
Mobile Netzwerke und Remotezugriff	602
Erstellen von Verbindungen für den Remotezugriff	604
Erstellen einer Wählverbindung	605
Erstellen einer Breitbandverbindung zum Internet	611
Erstellen einer VPN-Verbindung	612
Einstellen der Verbindungseigenschaften	613
Einstellen der automatischen oder manuellen Verbindungen	614
Einstellen des Proxys für mobile Verbindungen	615
Einstellen der Verbindungsanmeldungsinformationen	618
Einstellen der automatischen Verbindungstrennung	619
Einstellen der Wählregeln für eine Verbindung	619
Einstellen der bevorzugten und der alternativen Rufnummern	620
Einstellen der Identitätsprüfung	621
Einstellen der Netzwerkprotokolle und -komponenten	621
Aktivieren und Deaktivieren der Windows-Firewall für Netzwerkverbindungen	623
Herstellen von Verbindungen	624
Verbinden mit Wählverbindungen	624
Verbinden mit Breitbandverbindungen	625
Verbinden mit VPN	626
Drahtlosnetzwerke	628
Drahtlosgeräte und Drahtlostechnologien	628
Sicherheit im Drahtlosnetzwerk	629
Installieren und Konfigurieren eines Drahtlosadapters	631
Verwenden von Drahtlosnetzwerken und Drahtlosverbindungen	631
Verbinden mit Drahtlosnetzwerken	634
Verwalten und Problembehandlung von Drahtlosnetzwerken	635
Stichwortverzeichnis	636
Der Autor	672

Einführung

Das Schreiben von *Microsoft Windows 8 – Ratgeber für Administratoren* war mit viel Spaß, aber auch mit viel Arbeit verbunden. Als ich mit der Arbeit an diesem Buch begann, wollte ich als Erstes herausfinden, was sich in Windows 8 gegenüber den Vorgängerversionen von Windows geändert hat und welche neuen Funktionen und Optionen zur Verfügung stehen. Wie bei jedem neuen Betriebssystem waren umfangreiche Recherchen und eine intensive Beschäftigung mit den Interna des Systems nötig, bis ich herausgefunden hatte, wie die Dinge genau funktionieren.

Für jemanden, der von einer älteren Windows-Version auf Windows 8 wechselt, zählt die tiefgreifende Änderung der Benutzeroberfläche zu den wesentlichsten Änderungen des Betriebssystems. Windows 8 unterstützt nun zusätzlich zur herkömmlichen Bedienung mit Maus und Tastatur eine Bedienung durch Streif- und Tippbewegungen auf Touchscreens. Wenn Sie auf einem Computer arbeiten, der über einen Touchscreen verfügt, können Sie die auf dem Bildschirm angezeigten Elemente in einer Weise bearbeiten, die auf herkömmlichen Computern nicht möglich war. Zu den Streif- und Tippbewegungen gehören zum Beispiel:

- **Antippen** Tippen Sie ein Element mit dem Finger an. Das einfache oder doppelte Antippen eines Elements auf dem Bildschirm wirkt im Allgemeinen genauso wie ein einfacher beziehungsweise doppelter Mausklick.
- **Drücken und Halten** Drücken Sie mit Ihrem Finger auf ein Element und halten Sie es einige Sekunden fest. Das Drücken und Halten von Elementen auf dem Bildschirm wirkt normalerweise genauso wie ein Klick mit der rechten Maustaste.
- **Streifen zum Auswählen** Schieben Sie ein Element ein kurzes Stück entgegengesetzt zur Richtung, in der die Seite geblättert wird. Dadurch wählen Sie die Elemente aus, in manchen Fällen öffnen Sie auch zugehörige Befehle. Falls sich die Befehle und Optionen für ein Element nicht durch Drücken und Festhalten öffnen lassen, können Sie stattdessen das Streifen zum Auswählen probieren.
- **Streifen vom Rand** Streifen oder wischen Sie vom Rand des Bildschirms nach innen. Wenn Sie vom rechten Rand aus streifen, öffnet sich der Charms-Bereich. Beim Streifen vom linken Rand werden die offenen Apps angezeigt, zwischen denen Sie dann einfach umschalten können. Wenn Sie vom oberen oder unteren Rand her streifen, werden Befehle für das aktive Element angezeigt.
- **Finger zusammenführen** Berühren Sie ein Element mit mehreren Fingern und ziehen Sie dann die Finger näher zueinander. Mit dieser Geste zoomen Sie aus einer Darstellung hinaus oder zeigen weniger Details an.
- **Finger spreizen** Berühren Sie ein Element mit mehreren Fingern und ziehen Sie dann die Finger auseinander. Mit dieser Geste zoomen Sie in eine Darstellung hinein oder zeigen mehr Details an.

Außerdem können Sie auch mit einer Bildschirmtastatur Text eingeben. Die Änderungen in der Benutzeroberfläche sind zwar beträchtlich, aber die umfangreichsten Änderungen am Betriebssystem wurden hinter den Kulissen vorgenommen, wo sie sich zum Teil auch auf die Architektur auswirken. Einige der neuen Funktionen sind so durchgreifend, dass sie für immer die Art und Weise ändern werden, in der wir Windows benutzen.

Ein Ratgeber sollte ein kompaktes Format haben und gut zu lesen sein. Er sollte ein Buch sein, mit dem sich Probleme lösen und Aufgaben bewältigen lassen, unabhängig davon, wo sich der Leser gerade befindet. Unter dieser Vorgabe habe ich den Text nochmals sorgfältig durchgesehen, um sicherzustellen, dass alle wichtigen Bereiche der Windows 8-Administration beschrieben werden. Das Ergebnis meiner Arbeit liegt nun vor Ihnen, und ich hoffe, Sie werden ebenso wie ich finden, dass es sich um einen der besten und praktischsten Ratgeber für Windows 8 handelt. Dieses Buch enthält alles, was Sie brauchen, um die Grundkonfiguration, Optimierungen und Wartungsarbeiten durchzuführen.

Mein Ziel bestand darin, umfangreiche Informationen in Form eines handlichen Ratgebers bereitzustellen. Auf diese Weise müssen Sie sich nicht durch Hunderte von Seiten irrelevanter Daten kämpfen, um die benötigten Informationen zu finden. Stattdessen erhalten Sie genau die Informationen, die Sie benötigen, um eine bestimmte Aufgabe durchzuführen oder ein konkretes Problem zu lösen. Kurz gesagt: Das vorliegende Buch soll die Referenz sein, in der Sie nachschlagen, wenn Sie Fragen in Bezug auf die Windows 8-Konfiguration und Wartung haben. Daher werden in diesem Ratgeber täglich anfallende Arbeiten, häufig eingesetzte Verfahren, dokumentierte Beispiele und Optionen aufgegriffen, die repräsentativ, aber ohne Anspruch auf Vollständigkeit sind.

Ein weiteres Ziel bestand darin, den Inhalt dieses Buchs übersichtlich zu halten, damit dieser Ratgeber kompakt und leicht zu handhaben ist und gleichzeitig möglichst viele Informationen bereithält, die ihn zu einer wertvollen Informationsquelle machen. Statt einer dicken 1000-seitigen Dokumentation oder einer leichten 100-seitigen Kurzreferenz erhalten Sie einen nützlichen Ratgeber, der Ihnen bei häufig durchzuführenden Aufgaben, bei der Problemlösung und der täglichen Arbeit schnelle und einfache Hilfe bietet.

Für wen ist dieser Ratgeber konzipiert?

Microsoft Windows 8 – Ratgeber für Administratoren behandelt die Standard-, Professional- und Enterprise-Editionen von Windows 8. Er wurde für folgende Zielgruppen konzipiert:

- Erfahrene Benutzer, die Windows 8 konfigurieren und warten möchten
- Windows-Systemadministratoren und Support-Mitarbeiter
- Administratoren, die ein Upgrade von Vorgängerversionen auf Windows 8 durchführen
- Administratoren, die bisher auf anderen Plattformen gearbeitet haben

Um so viele Informationen wie möglich zur Verfügung zu stellen, wird davon ausgegangen, dass Sie Grundkenntnisse im Bereich des Netzwerkbetriebs besitzen und über ein grundlegendes Verständnis von Windows-Betriebssystemen verfügen. Deswegen werden den allgemeinen Windows-Grundlagen, der Windows-Architektur oder den Grundlagen der Vernetzung von Windows-Computern keine ganzen Kapitel gewidmet. Dagegen werden Themenbereiche wie die Anpassung des Desktops, Vernetzung von mobilen Computern, TCP/IP-Konfiguration, Benutzerprofile und Systemoptimierung erläutert. Im Bereich der Problembehandlung ist das Buch sehr ausführlich, wobei ich versucht habe sicherzustellen, dass der Haupttext in jedem Kapitel (sofern sinnvoll) durch Richtlinien und Erläuterungen zur Problembehandlung ergänzt wird. Ratschläge zur Problembehandlung werden von Anfang an in die Kapitel des Buchs integriert, statt sie als Nachtrag in einem separat angehängten Problembehandlungskapitel zusammenzufassen. Ich hoffe, dass Sie den Computer, nachdem Sie diese Kapitel gelesen und sich mit den Details beschäftigt haben, für Ihre Benutzer zu einem besseren, leistungsfähigeren und angenehmeren Arbeitsgerät machen und Ausfallzeiten verringern können.

Wie ist dieses Buch aufgebaut?

Microsoft Windows 8 – Ratgeber für Administratoren konzentriert sich auf die bei der Konfiguration, Optimierung und Wartung anfallenden Arbeiten und ist daher eher aufgabenbezogen als nach Windows 8-Funktionen geordnet. Die Bücher aus der Ratgeber-Reihe sollen nicht unterhalten oder bilden, sondern nützlich sein.

Schnelle Informationsvermittlung und einfache Handhabung stellen wesentliche Merkmale des vorliegenden Ratgebers dar. Das Buch verfügt über ein ausführliches Inhaltsverzeichnis und einen umfangreichen Index, um bei der Problemlösung schnelle Hilfe zu bieten. Ebenso wurde eine große Anzahl weiterer Referenzinformationen eingefügt, wie Schrittanweisungen, Listen, Tabellen mit Kurzinformationen und umfangreiche Querverweise.

In diesem Buch verwendete Konventionen

Ich habe versucht, den Text klar und leicht lesbar zu halten. Befehle, Code und Listings werden im Text in kursiver Schrift dargestellt, in Listings in *nichtproportionaler* Schrift:

Code und Listings

Wenn Sie aufgefordert werden, einen Befehl einzugeben, erscheint der Befehl in **Fettformatierung**. Menüs und andere Elemente der Benutzeroberfläche werden *kursiv* geschrieben. Bei der Einführung und Definition neuer Begriffe werden diese ebenfalls *kursiv* hervorgehoben.

Des Weiteren werden folgende Arten von Hinweisen verwendet:

ACHTUNG Warnt vor eventuell auftretenden Problemen.

EMPFOHLENE VORGEHENSWEISE Beschreibt die optimale Vorgehensweise bei der Arbeit mit komplizierteren Konfigurations- und Administrationskonzepten.

HINWEIS Liefert Details zu Punkten, die einer weiteren Erklärung bedürfen.

PRAXISTIPP Liefert praxisbezogene Tipps bei der Erörterung weiterführender Themen.

SICHERHEIT Bietet Hinweise oder zusätzliche Informationen zu Sicherheitsfragen.

TIPP Stellt hilfreiche Hinweise oder zusätzliche Informationen zur Verfügung.

WEITERE INFORMATIONEN Bietet weitere Informationen zu einem Thema.

WICHTIG Weist auf wichtige Konzepte oder potenzielle Probleme hin.

Ich hoffe, dass *Microsoft Windows 8 – Ratgeber für Administratoren* Ihnen sämtliche Informationen bietet, die Sie zur schnellen und effizienten Ausführung aller wesentlichen Arbeiten an Windows 8-Computern benötigen. Anregungen und Kritik sind immer willkommen und können an folgende E-Mail-Adresse gesendet werden: williamstanek@aol.com. Vielen Dank.

Support

Wir haben uns sehr um die Richtigkeit der in diesem Buch sowie auf der Begleit-CD enthaltenen Informationen bemüht. Mit Anmerkungen, Fragen oder Verbesserungsvorschlägen können Sie sich an Microsoft Press wenden:

Per E-Mail:

mspressde@oreilly.de

Per Post:

Microsoft Press

Betrifft: *Microsoft Windows 8 – Ratgeber für Administratoren*

Konrad-Zuse-Straße 1

85716 Unterschleißheim

Supportinformationen zu diesem Buch und der beiliegenden CD finden Sie auf der Supportwebsite von Microsoft Press unter <http://www.microsoft-press.de/support.asp?s110=690>.

Fehler, die seit der Veröffentlichung dieses Buchs in der englischsprachigen Originalausgabe bekannt geworden sind, werden auf unserer Microsoft Press-Website bei www.oreilly.com aufgeführt:

<http://shop.oreilly.com/product/0790145345486.do>

Falls Sie einen Fehler finden, der noch nicht beschrieben wurde, können Sie uns auf derselben Seite darüber informieren (in englischer Sprache).

Falls Sie weitere Unterstützung benötigen, können Sie sich mit einer E-Mail (in englischer Sprache) an den Microsoft Press Book Support unter mspinput@microsoft.com wenden.

Beachten Sie, dass unter den oben angegebenen Adressen kein Support für Microsoft-Software geleistet wird.

Bleiben Sie am Ball

Falls Sie neuste Nachrichten, Aktualisierungen usw. von Microsoft Press erhalten möchten, wir sind auf Twitter: http://twitter.com/mspress_de.

Kapitel 1

Einführung in die Windows 8-Administration

In diesem Kapitel:

Überblick über Windows 8	22
Grundlagen der 64-Bit-Architektur	26
Bereitstellen von Windows 8	28
Installieren von Windows 8	37
Ausführen von Windows 8	44
Architektur von Windows 8	54

Windows 8 wurde als Betriebssystem für Clientdienste entworfen. Dieses Kapitel beschreibt, wie Sie Windows 8 installieren und welche Arbeiten bei der Verwaltung von Windows 8 anfallen. Im Verlauf dieses Kapitels und des ganzen Buchs wird immer wieder ausführlich von den Änderungen die Rede sein, die praktisch alle Aspekte der Computerverwaltung und der Sicherheit verbessern. Der Schwerpunkt dieses Buchs liegt zwar auf der Windows 8-Verwaltung, aber die beschriebenen Tipps und Vorgehensweisen sind für jeden von Nutzen, der für Windows 8 Support leistet, dafür Software entwickelt oder damit arbeitet.

Beachten Sie bitte, dass dieses Buch für die gemeinsame Verwendung mit *Microsoft Windows Server 2012 – Ratgeber für Administratoren* (Microsoft Press, 2012) ausgelegt ist. Neben vielen Administrationsarbeiten beschreiben die Ratgeber für die Windows Server-Betriebssysteme die Verwaltung der Verzeichnisdienste, der Daten und des Netzwerks. Dieses Buch konzentriert sich hingegen auf die Benutzer- und Systemadministration. Folgende Themen werden ausführlich behandelt:

- Anpassen des Betriebssystems und der Windows-Umgebung
- Konfigurieren der Hardware und der Netzwerkgeräte
- Verwalten des Benutzerzugriffs und globaler Einstellungen
- Konfigurieren des mobilen Netzwerkzugriffs
- Verwenden der Remoteverwaltung und Remoteunterstützung
- Beheben von Systemproblemen

In diesem Zusammenhang ist wichtig, dass Sie praktisch alle Konfigurationsoptionen des Betriebssystems Windows über Gruppenrichtlinien steuern können. Statt bei jeder Beschreibung darauf hinzuweisen, dass Feature A oder B nur konfiguriert werden kann, wenn die gültigen Gruppenrichtlinien dies erlauben, setze ich voraus, dass Sie bereits wissen, welche Auswirkungen Gruppenrichtlinien auf Systemkonfiguration und Verwaltung haben. Außerdem gehe ich davon aus, dass Sie mit der Befehlszeile und Windows PowerShell vertraut sind. Auf diese Weise kann ich mich auf die wirklich wichtigen Administrationsaufgaben konzentrieren.

Überblick über Windows 8

Windows 8 ist die neueste Version des Windows-Betriebssystems für Clientcomputer. Windows 8 lässt sich von Haus aus auf der Basis von Abbildern installieren und bereitstellen. Windows 8, Windows 8 Pro und Windows 8 Enterprise unterstützen 32-Bit-x86- und 64-Bit-x64-Prozessoren für PCs und Tablets. Windows 8 RT unterstützt ARM-Prozessoren. Viele höhere Funktionen wie BitLocker, das verschlüsselnde Dateisystem, der Beitritt zu einer Domäne, Gruppenrichtlinien und der Remotedesktophost setzen die Verwendung von Windows 8 Pro oder Windows 8 Enterprise voraus.

Für die 32-Bit- und 64-Bit-Versionen von Windows 8 werden separate Installationsmedien zur Verfügung gestellt. Um die 32-Bit-Version von Windows 8 auf einem x86-Computer zu installieren, müssen Sie das 32-Bit-Installationsmedium verwenden. Wollen Sie dagegen die 64-Bit-Version von Windows 8 auf einem x64-Computer installieren, brauchen Sie das 64-Bit-Installationsmedium. Wenn Sie bereits ein 32-Bit-Betriebssystem verwenden und stattdessen ein 64-Bit-Betriebssystem installieren wollen (sofern die Hardware beide Architekturen unterstützt), müssen Sie den Computer herunterfahren und vom 64-Bit-Installationsmedium neu starten. Dasselbe gilt, wenn Sie ein 32-Bit-Betriebssystem auf einem Computer installieren wollen, der bisher unter einem 64-Bit-Betriebssystem läuft.

HINWEIS Windows RT ist für Geräte mit ARM-Prozessoren gedacht und unterscheidet sich beträchtlich von den anderen Editionen von Windows 8.

Die Unabhängigkeit von bestimmten Sprachen und die Möglichkeit zur schnellen und flexiblen Installation von Windows 8 wurden durch eine entsprechende Modularisierung und durch Laufwerkabbilder erreicht. Jede Komponente des Betriebssystems wurde als unabhängiges Modul konzipiert, das leicht hinzugefügt oder entfernt werden kann. Das ist die Basis für die Konfigurierbarkeit von Windows 8. Der erforderliche Speicherplatz auf den Installationsmedien wird durch die Komprimierung der Dateien und durch eine Eininstanzspeicherung beträchtlich reduziert. Die Laufwerkabbilder auf den Installationsmedien liegen im WIM-Format (Windows Imaging) vor.

Die Windows-Vorinstallationsumgebung 4.0 (Windows PE 4.0) ersetzt MS-DOS als Vorinstallationsumgebung und bietet eine startfähige Betriebssystemumgebung für die Installation, Bereitstellung, Wiederherstellung und Problembehebung. Die Windows-Startumgebung enthält einen Startmanager, mit dem Sie die Startanwendung auswählen können, die das Betriebssystem hochfahren soll. Sind auf einem Computer mehrere Betriebssysteme nebeneinander installiert, erreichen Sie ältere Betriebssysteme als Windows Vista in der Startumgebung unter dem Eintrag *Frühere Windows-Version*.

Die Benutzerkontensteuerung verbessert durch die Trennung von Standard- und Administratorkonten die Sicherheit des Computers. Sie bewirkt, dass alle Anwendungen mit den geringstmöglichen Berechtigungen ausgeführt werden. Bei Bedarf erscheint ein Bestätigungsdialogfeld, wenn eine Anwendung Administratorrechte erfordert. Die Funktionsweise dieses Dialogfelds wird durch die Gruppenrichtlinieneinstellungen festgelegt. Wenn Sie sich mit dem integrierten Administratorkonto anmelden, werden gewöhnlich keine Bestätigungsdialogfelder zur Anhebung der Berechtigungen angezeigt.

Windows 8 verwendet in der Benutzeroberfläche folgende wichtige Elemente:

- Startbildschirm
- Charmleiste
- Suchfeld
- Desktopeinstellungsbereich
- PC-Einstellungsbildschirm
- Apps-Bildschirm (auch *Alle Apps* genannt)

In Windows 8 ersetzt ein Startbildschirm das herkömmliche *Start*-Menü. *Start* ist ein Fenster, kein Menü. Programme können im *Start*-Fenster durch *Kacheln* dargestellt werden. Durch das Antippen oder Anklicken einer Kachel wird das betreffende Programm gestartet. Wenn Sie eine Kachel gedrückt halten oder mit der rechten Maustaste anklicken, wird statt eines Kontextmenüs eine Optionsleiste angezeigt.

In *Start* lässt sich ein Programm zum Beispiel schnell öffnen, indem man die WINDOWS-Taste drückt, den Dateinamen des Programms eingibt und dann auf die EINGABETASTE drückt. Das funktioniert, solange das *Apps*-Suchfeld im Eingabefokus liegt (gewöhnlich ist dies der Fall).

Ein Druck auf die WINDOWS-Taste führt zu einem Wechsel zwischen dem Startbildschirm und dem Desktop, oder zwischen *Start* und *PC-Einstellungen*, falls Sie mit *PC-Einstellungen* arbeiten. Auf *Start* gibt es eine *Desktop*-Kachel, die Sie antippen oder anklicken können, um den Desktop anzuzeigen. Auch mit der Tastenkombination WINDOWS-Taste+D erreichen Sie den Desktop. Falls Sie nur kurz einen Blick auf den Desktop werfen möchten, halten Sie die Kombination WINDOWS-Taste+, gedrückt (also die WINDOWS-Taste und die Komma-Taste).

Die Charmleiste ist eine Optionsleiste für *Start*, *Desktop* und *PC-Einstellungen*. Auf einem Touch-Bildschirm lässt sich die Charmleiste durch eine Streifbewegung vom rechten Bildschirmrand öffnen. Mit der Maus öffnen Sie die Charmleiste, indem Sie den Mauszeiger über eine der verborgenen Schaltflächen bewegen, die sich in der oberen und unteren rechten Ecke der Bildschirme *Start*, *Desktop* oder *PC-Einstellungen* befinden. Auch mit der Tastenkombination WINDOWS-Taste+C lässt sich die Leiste öffnen.

Die Charmleiste zeigt fünf Charms:

- **Suchen** Tippen oder klicken Sie auf den Charm *Suchen*, wenn Sie die Suchleiste öffnen möchten. Jeder Text, der auf dem Startbildschirm eingegeben wird, wird automatisch ins Suchfeld der Suchleiste eingetragen. Das Suchfeld lässt sich auf *Apps*, *Einstellungen* oder *Dateien* einstellen. Durch die Einstellung auf *Apps* lassen sich installierte Programme schnell finden. Nach der Einstellung auf *Einstellungen* fördert die Suche schnell alle entsprechenden Einstellungen und Optionen in der Systemsteuerung zutage. Eine Einstellung auf *Dateien* ermöglicht die schnelle Suche von Dateien.
- **Teilen** Tippen oder klicken Sie den Charm *Teilen* an, wenn Sie bestimmte Objekte für andere freigeben möchten. Wenn Sie zum Beispiel mit der Anwendung *Karten* arbeiten, werden gewöhnlich Optionen zum Teilen der Karte angezeigt, mit der Sie arbeiten.
- **Start** Tippen oder klicken Sie den Charm *Start* an, um zwischen Desktop und Startbildschirm zu wechseln, oder zwischen *Start* und *PC-Einstellungen*, falls Sie mit *PC-Einstellungen* arbeiten.
- **Geräte** Tippen oder klicken Sie den Charm *Geräte* an, wenn Sie mit angeschlossenen Geräten arbeiten möchten, beispielsweise mit einem zweiten Monitor.
- **Einstellungen** Tippen oder klicken Sie den Charm *Einstellungen* an, wenn Sie die Einstellungsleiste öffnen möchten. Diese Leiste bietet den Zugang zu wichtigen Optionen, beispielsweise zu den Optionen *Energie sparen*, *Herunterfahren* und *Neu starten*.

TIPP Die Standardeinstellung ist die Suche nach Anwendungen. Daher können Sie ein Programm auf dem *Start*-Bildschirm schnell öffnen, indem Sie einfach den Programmnamen eingeben und dann die EINGABETASTE drücken.

Mit der Kombination WINDOWS-Taste+I können Sie ebenfalls die Einstellungsleiste öffnen. Mit den angebotenen Optionen können Sie:

- Netzwerkverbindungen und den Netzwerkstatus anzeigen
- Die Lautstärkeeinstellung anzeigen und ändern
- Die Helligkeit des Bildschirms einstellen (nur auf portablen Geräten)
- Benachrichtigungen für eine bestimmte Zeit ausblenden
- Den Computer herunterfahren, neu starten oder in den Energiesparmodus versetzen
- Die Bildschirmtastatur anzeigen (nur auf Geräten mit Touch-Bildschirm)
- Den Bildschirm *PC-Einstellungen* öffnen (durch einen Klick auf *PC-Einstellungen ändern*)

Die Einstellungsleisten der Bildschirme *Start*, *Desktop* und *PC-Einstellungen* sind ähnlich aufgebaut, aber nicht gleich. Die *Start*-Einstellungsleiste weist die Option *Kacheln* auf, die Sie antippen oder anklicken können, um die Optionen zum Hinzufügen von Verwaltungstoolkacheln zum Startbildschirm und zum Löschen von persönlichen Informationen aus Kacheln anzuzeigen.

Die Einstellungsleiste *Desktop* weist eine größere Zahl von Verknüpfungen auf:

- **Systemsteuerung** zum Öffnen der Systemsteuerung
- **Anpassung** zum Öffnen der Anpassungseinstellungen in der Systemsteuerung
- **PC-Info** zum Öffnen der Seite *System* der Systemsteuerung
- **Hilfe** zum Öffnen von *Windows-Hilfe und Support*

Bei der Arbeit mit dem Desktop lässt sich die Systemsteuerung also mit der Tastenkombination **WINDOWS-Taste+I** und dem anschließenden Klick auf die Option *Systemsteuerung* der Einstellungsleiste schnell öffnen.

Der Datei-Explorer ist standardmäßig auf der Taskleiste des Desktops zu finden. Das bedeutet, dass Sie die Systemsteuerung auch auf folgende Weise erreichen:

1. Öffnen Sie den Datei-Explorer, indem Sie das entsprechende Symbol auf der Taskleiste antippen oder anklicken.
2. Tippen oder klicken Sie auf den nach oben gerichteten Pfeil links neben der Adressleiste.
3. Tippen oder klicken Sie auf *Systemsteuerung*.

Außerdem sollten Sie wissen, wie Sie den Anwendungsbildschirm *Apps* erreichen, der die installierten Anwendungen in der Kategorie *Apps* in alphabetischer Reihenfolge auflistet.

Der Anwendungsbildschirm wird automatisch angezeigt, wenn Sie nach einer Anwendung suchen. Falls die Einstellungsleiste auf dem Anwendungsbildschirm angezeigt wird, tippen oder klicken Sie in einen freien Bereich des Anwendungsbildschirms, damit die Einstellungsleiste verschwindet. Vom *Start*-Fenster oder vom Desktop aus lässt sich der Anwendungsbildschirm mit der Tastenkombination **WINDOWS-Taste+Q** erreichen. Eine weitere Methode zur Anzeige des Anwendungsbildschirms besteht darin, eine *Apps*-Suche zu beginnen und dann in einen freien Bereich des Anwendungsbildschirms zu tippen oder zu klicken, um das Suchfeld verschwinden zu lassen.

Auf dem Anwendungsbildschirm werden einige Anwendungen, die man bei der Verwaltung des Computers häufig braucht, in der Kategorie *Windows-System* angezeigt, beispielsweise *Eingabeaufforderung*, *Computer*, *Systemsteuerung*, *Task-Manager*, *Explorer* und *Windows PowerShell*.

HINWEIS In Windows 8 Pro und Windows 8 Enterprise ist Windows PowerShell normalerweise bereits enthalten. Von *Start* aus erreichen Sie Windows PowerShell am einfachsten, indem Sie **powershell** eingeben und die **EINGABETASTE** drücken. Das funktioniert, solange Windows PowerShell der erste Treffer für das Schlüsselwort »powershell« ist. Gibt es mehrere Übereinstimmungen, drücken Sie nicht die **EINGABETASTE**, sondern tippen oder klicken auf die Anwendung, die ausgeführt werden soll.

TIPP Vielleicht möchten Sie einige Elemente aus dem Anwendungsbildschirm zur Taskleiste von *Start* oder *Desktop* hinzufügen. Dazu halten Sie das Element gedrückt oder klicken es mit der rechten Maustaste an und tippen oder klicken nach Bedarf auf *An »Start« anheften* oder auf *An Taskleiste anheften*. Zur Vereinfachung der Verwaltung würde ich empfehlen, die Elemente *Eingabeaufforderung*, *Computer*, *Systemsteuerung* und *Windows PowerShell* an die Taskleiste anzuhängen.

Vielleicht möchten Sie Windows PowerShell als Standardeingabeaufforderung verwenden, um Windows-Standardbefehle und Windows PowerShell-Befehle einzugeben. Im Prinzip lässt sich zwar alles, was in einer herkömmlichen Eingabeaufforderung eingegeben werden kann, auch in einer Windows PowerShell-Eingabeaufforderung eingeben, weil Windows PowerShell im Rahmen seiner Arbeit nach externen Befehlen und Hilfsprogrammen sucht. Sofern der externe Befehl oder das externe Hilfsprogramm in einem

Verzeichnis zu finden ist, das in der Umgebungsvariablen *Path* genannt wird, wird der Befehl oder das Hilfsprogramm ausgeführt. Vergessen Sie aber nicht, dass sich die Ausführungsreihenfolge in Windows PowerShell darauf auswirken kann, wie ein Befehl ausgeführt wird. Die Ausführungsreihenfolge für Windows PowerShell lautet: 1.) alternative integrierte oder profildefinierte Aliase, 2.) integrierte oder profildefinierte Funktionen, 3.) Cmdlets oder Schlüsselwörter der Sprache, 4.) Skripts mit der Namens-erweiterung *.ps1* und 5.) externe Befehle, Hilfsprogramme und Dateien. Wenn also ein Element in den Schritten 1 bis 4 der Ausführungsreihenfolge denselben Namen wie in Befehl hat, wird dieses Element ausgeführt, und nicht der erwartete Befehl.

Windows 8 enthält Windows PowerShell. Wenn Sie Windows PowerShell für den Remotezugriff konfiguriert haben, haben Sie mehrere Möglichkeiten, Befehle auf Remotecomputern auszuführen. Beispielsweise können Sie eine Remotesitzung mit den Computern aufbauen, mit denen Sie arbeiten wollen. Das folgende Beispiel und der Ausschnitt der Ausgabe zeigen, wie Sie prüfen, welche Windows-Edition auf den Remotecomputern jeweils läuft:

```
$s = new-pssession -computername engpc15, hrpc32, cserpc28
invoke-command -session $s {dism.exe /online /get-currentedition}
```

Die folgenden Zeilen zeigen das gekürzte Ergebnis:

```
Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7600.16385
Abbildversion: 6.1.7600.16385
Aktuelle Edition : Ultimate
Der Vorgang wurde erfolgreich beendet.
```

Die interne Versionsnummer von Windows 7 ist 6.1 und die interne Versionsnummer von Windows 8 lautet 6.2. Das Ergebnis lässt also erkennen, dass auf dem Computer Windows 7 Ultimate verwendet wird und noch keine Aktualisierung auf Windows 8 erfolgt ist.

HINWEIS

Beim Befehl *New-PSSession* legen Sie mit dem Argument *-ComputerName* fest, mit welchen Remotecomputern Sie arbeiten; dabei können Sie die Zielcomputer anhand des DNS-Namens, des NetBIOS-Namens oder der IP-Adresse angeben. Wenn Sie mit mehreren Remotecomputern gleichzeitig arbeiten, müssen Sie die Computernamen oder IP-Adressen durch Kommas voneinander trennen. Weitere Informationen zur Arbeit mit Windows PowerShell und dem Remotezugriff finden Sie in Kapitel 6, »Using Sessions, Jobs, and Remoting«, des Buchs *Windows PowerShell 2.0 Administrator's Pocket Consultant* (Microsoft Press, 2009).

Grundlagen der 64-Bit-Architektur

Seit die 64-Bit-Architektur für die Windows-Betriebssysteme eingeführt wurde, hat sie sich entscheidend verändert. Computer, auf denen 64-Bit-Versionen von Windows laufen, bieten nicht nur bessere Leistung und höhere Geschwindigkeit als ihre 32-Bit-Gegenstücke, sie sind auch besser skalierbar, weil sie mehr Daten pro Taktzyklus verarbeiten, mehr Arbeitsspeicher ansprechen und numerische Berechnungen schneller durchführen.

Es gibt zwei unterschiedliche 64-Bit-Architekturen:

- **x64** Diese Architektur basiert auf den 64-Bit-Erweiterungen für den x86-Befehlssatz, wie sie in AMD Opteron-Prozessoren (AMD64), Intel Xeon-Prozessoren mit 64-Bit-Erweiterungstechnologie und anderen Prozessoren implementiert sind. Diese Architektur bietet native 32-Bit-Verarbeitung und zusätzlich 64-Bit-Verarbeitung über die Erweiterungen, sodass 32-Bit- und 64-Bit-Anwendungen parallel ausgeführt werden können.

- **IA64** Diese Architektur basiert auf der Prozessorarchitektur EPIC (Explicitly Parallel Instruction Computing), die in Intel Itanium- (IA64) und anderen Prozessoren implementiert ist. Diese Architektur bietet native 64-Bit-Verarbeitung, sodass 64-Bit-Anwendungen optimale Leistung erzielen.

Die vorherrschende Architektur ist x64. Sie ist die wichtigste 64-Bit-Architektur für PCs und Tablets, die von Windows 8 unterstützt wird. Die 64-Bit-Verarbeitung wurde mit dem Ziel entworfen, Operationen ausführen zu können, die viel Arbeitsspeicher benötigen und aufwendige numerische Berechnungen erfordern. Bei der 64-Bit-Verarbeitung können Anwendungen große Datengruppen vollständig in den Arbeitsspeicher (also das RAM) laden, sodass keine Speicherseiten auf die Festplatte ausgelagert werden müssen. Die Leistung verbessert sich dadurch ganz erheblich.

Die momentan relevanten Firmwareschnittstellen sind:

- BIOS (Basic Input/Output System)
- EFI (Extensible Firmware Interface)
- UEFI (Unified Extensible Firmware Interface)

Itanium-Computer unterscheiden sich in vielen grundlegenden Punkten von Computern, die auf Basis der x86- und x64-Spezifikationen entwickelt wurden. Während Itanium-Computer für die Start- und Systemvolumes EFI und den Festplattentyp GPT (GUID Partition Table) nutzen, verwenden x86-Computer für die Start- und Systemvolumes ein BIOS und MBR-Festplatten (Master Boot Record). x64-Computer wiederum arbeiten mit UEFI, das auf BIOS oder EFI aufsetzt; mehr dazu im Abschnitt »Firmwareoptionen« in Kapitel 4, »Verwalten von Firmware, Startkonfiguration und Systemstart«. Daher gibt es Unterschiede bei der Verwaltung von Computern mit diesen Architekturen, insbesondere in den Bereichen Setup und Festplattenkonfiguration. Weil sich UEFI aber zunehmend durchsetzt und Windows 8 in der Lage ist, unabhängig vom Firmwaretyp sowohl MBR- als auch GPT-Datenträger zu nutzen, hängt es nicht mehr unbedingt von der jeweiligen Prozessorarchitektur ab, welchen Firmwaretyp und welche Festplatten ein Computer einsetzt. Diese Entscheidung wird von den Hardwareherstellern getroffen.

HINWEIS Techniken für die Benutzung von MBR- und GPT-Datenträgern sind in Kapitel 12, »Verwalten von Festplattenlaufwerken und Dateisystemen«, beschrieben. Im Allgemeinen verwenden BIOS-basierte Computer MBR für Systemstart- und für Datenfestplatten, GPT dagegen nur vereinzelt für Datenfestplatten. EFI-basierte Computer können sowohl mit GPT- als auch MBR-Datenträgern arbeiten, aber Sie brauchen dann mindestens eine GPT-Festplatte mit der EFI-Systempartition (EFI System Partition, ESP) sowie eine primäre Partition oder ein einfaches Volume, von dem das Betriebssystem gestartet wird.

In den meisten Fällen ist 64-Bit-Hardware kompatibel zu 32-Bit-Anwendungen. Allerdings ist die Leistung von 32-Bit-Anwendungen besser, wenn sie auf 32-Bit-Hardware laufen. Die 64-Bit-Editionen von Windows unterstützen sowohl 64-Bit- als auch 32-Bit-Anwendungen; dazu verwenden sie eine x86-Emulationsschicht namens Windows on Windows 64 (WOW64). Dieses WOW64-Subsystem isoliert 32-Bit-Anwendungen von 64-Bit-Anwendungen. Das verhindert Probleme mit Dateisystem und Registrierung. Das Betriebssystem bietet Interoperabilität über die 32-Bit/64-Bit-Grenze hinweg, damit COM (Component Object Model) und einfache Operationen wie Ausschneiden, Kopieren und Einfügen über die Zwischenablage funktionieren. 32-Bit-Prozesse können aber keine 64-Bit-DLLs (Dynamic-Link Library) laden, und 64-Bit-Prozesse umgekehrt auch keine 32-Bit-DLLs.

Wenn Sie auf die 64-Bit-Architektur umrüsten, werden Sie wahrscheinlich feststellen wollen, welche Computer im Unternehmen 64-Bit-Betriebssysteme unterstützen und auf welchen bereits 64-Bit-Betriebssysteme laufen. Mit Windows PowerShell können Sie folgende Informationen ermitteln:

- Feststellen, ob auf einem Computer ein 64-Bit-Betriebssystem installiert ist. Dazu fragen Sie die Eigenschaft *OSArchitecture* des Objekts *Win32_OperatingSystem* ab. Hier ein Beispiel:

```
get-wmiobject -class win32_operatingsystem | format-list osarchitecture
```

Das Ergebnis lautet:

```
osarchitecture : 32-Bit
```

- Feststellen, ob ein Computer ein 64-Bit-Betriebssystem unterstützt. Dazu werten Sie die Eigenschaften *Name* und *Description* des Objekts *Win32_Prozessor* aus:

```
get-wmiobject -class win32_processor | format-list name, description
```

```
name           : Intel(R) Core(TM)2 Quad CPU           @ 2.66GHz
description    : x64 Family 6 Model 15 Stepping 7
```

Das erste Beispiel verrät Ihnen, dass auf dem Computer momentan eine 32-Bit-Version von Windows läuft. Die Ausgabe im zweiten Beispiel zeigt, dass der Computer einen x64-Prozessor hat. Folglich können Sie bei diesem Computer ein Upgrade auf eine 64-Bit-Version von Windows 8 durchführen.

Statt jeden Computer einzeln zu überprüfen, können Sie auch ein Skript verwenden, das diese Aufgabe erledigt. Beispielskripts und vollständige Anleitungen finden Sie in Kapitel 8, »Inventorying and Evaluating Windows Systems«, des Buchs *Windows PowerShell 2.0 Administrator's Pocket Consultant* (Microsoft Press, 2009).

Bereitstellen von Windows 8

Mit Windows 8 können Sie benutzerdefinierte Versionen des Betriebssystems (Builds) auf Computern bereitstellen. Dafür stehen sowohl manuelle als auch automatisierte Prozesse zur Verfügung. Wollen Sie Windows mithilfe eines manuellen Verfahrens bereitstellen, müssen Sie die erforderlichen Start- und Installationsabbilder sowie optional Wiederherstellungsabbilder erstellen. Wenn Sie den Bereitstellungsprozess dagegen automatisieren wollen, müssen Sie die Windows-Bereitstellungsdienste installieren. Unabhängig davon, ob Sie einen vollständig manuellen Prozess, einen vollständig automatisierten Prozess oder irgendeine Kombination der beiden verwenden, führen Sie in allen Fällen ähnliche Verwaltungsarbeiten zur Vorbereitung durch. Für diese Arbeiten müssen Sie das Windows ADK (Windows Assessment and Deployment Kit) für Windows 8 und die Windows-Bereitstellungsdienste kennen und verwenden.

Das Windows Assessment and Deployment Kit für Windows 8 ist im Microsoft-Downloadcenter (<http://download.microsoft.com/>) erhältlich und enthält folgende Tools für die Bereitstellung von Windows-Abbildern:

- Anwendungskompatibilitäts-Toolkit (Application Compatibility Toolkit, ACT)
- Bereitstellungstools
- User State Migration Tool (USMT)
- Volumenaktivierungsverwaltungstool (Volume Activation Management Tool, VAMT)
- Windows-Bewertungsdienste
- Windows-Bewertungstoolkit
- Windows Performance Toolkit (WPT)
- Windows-Vorinstallationsumgebung (Windows Preinstallation Environment, Windows PE)

Zur Bereitstellung von Windows 8 über ein Netzwerk können Sie die Windows-Bereitstellungsdienste verwenden. Sie können die Rolle *Windows-Bereitstellungsdienste* zu jedem Server hinzufügen, auf dem Windows Server 2012 ausgeführt wird.

Windows 8 und Windows Server 2012 benutzen Windows PE 4.0. Windows PE 4.0 ist eine startfähige Umgebung, die Betriebssystemfunktionen für folgende Aufgaben zur Verfügung stellt:

- **Installation** Wenn Sie Windows 8 installieren, laufen die grafischen Tools, die während der Setupphase Systeminformationen sammeln, innerhalb von Windows PE.
- **Bereitstellung** Wenn ein neuer Computer einen Netzwerkstart ausführt, kann der eingebaute PXE-Client (Preboot Execution Environment) eine Verbindung zu einem Windows-Bereitstellungsdiensteserver herstellen, ein Windows PE-Abbild über das Netzwerk herunterladen und dann innerhalb dieser Umgebung Bereitstellungsskripts ausführen.
- **Wiederherstellung** Mit Windows PE können Sie auf das Systemstartreparaturtool zugreifen und es ausführen, falls Windows 8 aufgrund einer beschädigten Systemdatei nicht starten kann.
- **Problembehandlung** Sie können Windows PE von Hand starten, um eine Problembehandlung oder eine Diagnose auszuführen, wenn in Windows 8 Probleme auftreten, die sich mit anderen Mitteln nicht diagnostizieren lassen.

Windows PE ist modular und erweiterbar und bietet vollständigen Zugriff auf Partitionen, die mit den Dateisystemen FAT oder NTFS formatiert sind. Weil Windows PE aus einer Untermenge der Windows-Komponenten besteht, können Sie viele Windows-Anwendungen ausführen, mit Hardwaregeräten arbeiten und über IP-Netzwerke kommunizieren. In Windows PE stehen unter anderem folgende Befehlszeilentools zur Verfügung:

- **BCDBoot** Initialisiert den Startkonfigurationsdatenspeicher (Boot Configuration Data, BCD) und ermöglicht Ihnen, die Startumgebungsdateien in die Systempartition zu kopieren.
- **Bootsect** Ein Tool zum Erstellen und Bearbeiten von Systemstartsektoren auf Festplatten und Flashlaufwerken
- **Copype** Ein Tool zum Erstellen einer Verzeichnisstruktur für Windows PE-Dateien und zum Kopieren der Windows PE-Mediendateien. Die Ausführung dieses Tools dient zur Vorbereitung der Erstellung von startfähigen Windows PE-Medien.
- **DiskPart** Ein Tool zum Erstellen und Bearbeiten von Datenträgern, Partitionen und Volumes
- **DISM** Ein leistungsfähiges Tool zum Bearbeiten und Verwalten von Abbildern
- **Drvload** Ein Unterstützungstool, mit dem Sie Gerätetreiber hinzufügen und dynamisch einen Treiber laden können, nachdem Windows PE gestartet wurde
- **ImageX** Ein Tool zum Aufzeichnen und Anwenden von Windows-Abbildern
- **Lpksetup** Ein Tool zum Hinzufügen und Entfernen von Sprachpaketen
- **Makewinpmedia** Ein Tool zum Erstellen startfähiger Windows PE-Medien
- **Net** Eine Sammlung von Befehlen, mit denen Sie lokale Benutzer verwalten, Dienste starten und beenden sowie Verbindungen zu freigegebenen Ordnern herstellen können
- **Netcfg** Ein Tool, das den Netzwerkzugriff konfiguriert
- **Oscdimg** Ein Tool zum Erstellen von CD- und DVD-ISO-Abbilddateien
- **Wpeinit** Ein Tool, das Windows PE jedes Mal initialisiert, wenn es gestartet wird

Copype und Makewinpemedia sind neue Tools, mit denen sich startfähige Windows PE-Medien leichter erstellen lassen. Sie können Copype zur Einrichtung der Windows PE-Buildumgebung verwenden. Nach der Optimierung des Builds können Sie das startfähige Medium mit Makewinpemedia erstellen. Bei dem Medium kann es sich um eine CD, eine DVD, ein USB-Flashlaufwerk oder um ein externes USB-Festplattenlaufwerk handeln.

Verwenden von DISM

Die Abbildverwaltung für die Bereitstellung (Deployment Image Servicing and Management, DISM) ist eins der wichtigsten Bereitstellungstools. In Windows 8 Pro und Windows 8 Enterprise ist es bereits enthalten.

Mit DISM können Sie Online- und Offlineabbilder des Betriebssystems Windows verwalten, darunter Abbilder für die Bereitstellung und für virtuelle Computer. Für die Bereitstellung von Windows 8 werden Windows-Abbilddateien (.wim) eingesetzt, für virtuelle Computer dagegen Dateien für virtuelle Festplatten (.vhd). WIM- und VHD-Dateien werden mit denselben Befehlen verwaltet.

Mit DISM können Sie folgende Aufgaben erledigen:

- Hinzufügen und Entfernen von Paketen; solche Pakete sind beispielsweise Language Packs, Patches oder Dienstprogramme.
- Aktivieren und Deaktivieren von Windows-Funktionen
- Hinzufügen und Entfernen von Gerätetreibern, die von anderen Herstellern zur Verfügung gestellt werden

Sie können DISM in einer Eingabeaufforderung mit Administratorrechten auszuführen:

1. Auf dem Anwendungsbildschirm wird die Eingabeaufforderung in der Kategorie *Windows-System* aufgelistet. Oder geben Sie **cmd** ein, falls Sie mit *Start* arbeiten.
2. Halten Sie die das Symbol für die Eingabeaufforderung auf dem Anwendungsbildschirm gedrückt oder klicken Sie es mit der rechten Maustaste an. Tippen oder klicken Sie dann auf *Als Admin ausführen*.

Falls eine Eingabeaufforderung der Benutzerkontensteuerung angezeigt wird, müssen Sie wie üblich fortfahren, um die Anwendung mit Administratorrechten auszuführen.

3. Geben Sie im Eingabeaufforderungsfenster den Befehl **dism /?** ein, um die verfügbaren Optionen für DISM anzuzeigen.
4. Welche Befehle für die Verwaltung von Onlineabbildern zur Verfügung stehen, zeigt der Befehl **dism /online /?** an.

DISM wurde zwar in erster Linie für die Arbeit mit Offlineabbildern und bereitgestellten Abbildern entwickelt, aber mit einigen DISM-Befehlen können Sie auch wichtige Informationen über das aktuell auf einem Computer laufende Betriebssystem abrufen. Tabelle 1.1 beschreibt die Unterbefehle aus dem *online*-Kontext von DISM, mit denen Sie laufende Betriebssysteme verwalten. Zum Beispiel zeigt der folgende Befehl eine Liste der Windows-Editionen an, auf die Sie bei Ihrem Computer ein Upgrade vornehmen können:

```
dism /online /get-targeteditions
```

Tabelle 1.1 Unterbefehle aus dem *online*-Kontext von DISM für laufende Betriebssysteme

Unterbefehl	Beschreibung
<code>/Disable-Feature</code> <code>/featurename:Funktionsname</code>	Deaktiviert die angegebene Funktion. Bei den Namen der Funktionen wird zwischen Groß- und Kleinschreibung unterschieden.
<code>/Enable-Feature</code> <code>/featurename:Funktionsname</code>	Aktiviert die angegebene Funktion. Bei den Namen der Funktionen wird zwischen Groß- und Kleinschreibung unterschieden.
<code>/Get-CurrentEdition</code>	Zeigt an, welche Edition von Windows momentan installiert ist.
<code>/Get-DriverInfo</code> <code>/driver:Treibername.inf</code>	Zeigt Informationen über den angegebenen Fremdherstellertreiber an, der im Treiberspeicher installiert ist. Bei den Treibernamen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
<code>/Get-Drivers</code>	Zeigt Informationen über alle Fremdherstellertreiber an, die im Treiberspeicher installiert sind.
<code>/Get-FeatureInfo</code> <code>/featurename:Funktionsname</code>	Zeigt Informationen über die angegebene Funktion an. Bei den Namen der Funktionen wird zwischen Groß- und Kleinschreibung unterschieden.
<code>/Get-Features</code>	Zeigt Informationen über die installierten Windows-Funktionen an.
<code>/Get-Intl</code>	Zeigt Informationen über die Standardsprache für die Benutzeroberfläche, Systemregion, Standardzeitzone, Tastatursprache und installierte Sprachen an.
<code>/Get-PackageInfo</code> <code>/packagename:Paketname</code>	Zeigt Informationen über das angegebene Paket an. Bei den Paketnamen wird zwischen Groß- und Kleinschreibung unterschieden.
<code>/Get-Packages</code>	Zeigt Informationen über die installierten Windows-Pakete an.
<code>/Get-TargetEditions</code>	Listet die Windows-Editionen auf, auf die ein Betriebssystemupgrade durchgeführt werden kann.

Grundlagen von Windows-Abbildern

Wenn Sie Windows 8 aktualisieren, indem Sie Features hinzufügen oder entfernen, Hotfixes einspielen oder Service Packs installieren, ändern Sie im Prinzip nur den Bestand an verfügbaren Modulen. Und weil diese Module voneinander unabhängig sind, können Sie solche Änderungen vornehmen, ohne dass dies Auswirkungen auf das System als Ganzes hat. Weil auch Sprachpakete (Language Packs) separate Module sind, können Sie ganz einfach andere Sprachkonfigurationen einrichten, ohne für jede Sprache eine eigene Installation zu benötigen.

Microsoft liefert Windows 8 auf Medien mit Datenträgerabbildern im WIM-Format (Windows Imaging Format) aus. WIM nutzt Komprimierung und die Eininstanzspeicherung (Single Instance Storage, SIS), um die Größe der Abbilddateien deutlich zu verringern. Die Komprimierung verringert die Größe des Abbilds in ähnlicher Weise wie Zip-Komprimierung bei Datendateien. Die Verwendung von SIS führt zu einer Verringerung der Abbildgröße, weil nur ein Exemplar einer Datei tatsächlich gespeichert wird, wenn sich mehrere Kopien der Datei im Laufwerkabbild befinden. Da WIM hardwareunabhängig ist, kann Microsoft eine Binärdatei für 32-Bit-Architekturen und eine für 64-Bit-Architekturen ausliefern. Für Windows 8 RT steht eine weitere Binärdatei zur Verfügung.

Windows 8 kann entweder automatisiert oder interaktiv installiert werden. Sie haben verschiedene Möglichkeiten, die Installation von Windows 8 zu automatisieren, zum Beispiel:

- **Erstellen einer Antwortdatei für die unbeaufsichtigte Installation** Windows 8 verwendet eine standardkonforme Antwortdatei. Diese Datei namens *Unattend.xml* ist in XML geschrieben, sodass es einfach ist, sie mit Standardtools zu bearbeiten. Indem Sie eine benutzerdefinierte Antwortdatei erstellen und Setup dann mit dieser Antwortdatei ausführen, können Sie unbeaufsichtigte Installationen von Windows 8 durchführen. Das Setupprogramm installiert das Betriebssystem dabei von einer Distributionsfreigabe oder von einem Medium.

- **Durchführen der Installation mit Abbildern, die mit Sysprep vorbereitet wurden** In diesem Fall müssen Sie das Befehlszeilentool für die Systemvorbereitung (*Sysprep.exe*) auf einem Computer ausführen, den Sie als Vorlage für die Bereitstellung verwenden wollen, und dann ein Datenträgerabbild mit der Konfiguration dieses Computers erstellen. Sysprep liegt im Ordner %SystemRoot%\System32\Sysprep. Das Windows Automated Installation Kit (Windows AIK) enthält den Windows-Systemabbild-Manager und ImageX, die dabei helfen, Bereitstellungen mit Sysprep vorzubereiten. Im Windows-Systemabbild-Manager erstellen Sie Antwortdateien für unbeaufsichtigte Installationen. Mit ImageX erstellen und verwalten Sie Datenträgerabbilder.

Weil ImageX WIM als Datenträgerabbildformat verwendet und die Vorteile des modularen Entwurfs von Windows 8 ausnutzt, müssen deutlich weniger Datenträgerabbilder verwaltet werden. Sie brauchen nicht mehr zahlreiche hardware- oder sprachabhängige Datenträgerabbilder zu pflegen. Gewöhnlich reicht es, wenn Sie sich auf ein einziges Datenträgerabbild für jede Prozessorarchitektur beschränken, die in Ihrer Organisation eingesetzt wird. Dann passen Sie die Betriebssysteminstallation mithilfe von unterschiedlichen Installationsskripts an die jeweiligen Anforderungen an.

WIM bietet gegenüber älteren Datenträgerabbildformaten noch weitere Vorteile. Sie können mit WIM Datenträgerabbilder offline ändern und verwalten. Das bedeutet, dass Sie optionale Komponenten und Treiber hinzufügen oder entfernen sowie Updates einspielen können, ohne ein neues Datenträgerabbild erstellen zu müssen. Dazu stellen Sie das Datenträgerabbild als Ordner im Dateisystem bereit und verwenden dann den Datei-Explorer oder andere Tools, um Dateien nach Bedarf zu aktualisieren, zu verwalten oder zu entfernen.

Der Windows-Systemabbild-Manager, ImageX und Sysprep stellen mehrere unterschiedliche Methoden zur Verfügung, um die Bereitstellung zu automatisieren. Im Prinzip gehen Sie dabei immer so vor:

1. Richten Sie Windows 8 auf einem Computer ein, der nicht für den normalen Betrieb benutzt wird, und konfigurieren Sie das Betriebssystem. Installieren und konfigurieren Sie anschließend alle benötigten Komponenten und Anwendungen.
2. Führen Sie Sysprep aus, um den Computer für die Aufzeichnung vorzubereiten. Sysprep löscht alle eindeutigen Kennungen vom Computer und markiert ihn als Masterbereitstellungscomputer. Nach Abschluss dieses Vorgangs enthält der Computer keine Kennungen mehr, die es ermöglichen würden, den Computer an einer Domäne oder Arbeitsgruppe anzumelden und dort zu benutzen.
3. Rufen Sie ImageX mit dem Argument */capture* auf, um das Datenträgerabbild aufzuzeichnen und dieses Abbild auf einem Medium oder in einer Distributionsfreigabe zu speichern. Sie können das Abbild offline verwalten, indem Sie es mit *imagex /mount* im Lese-/Schreib-Modus im Dateisystem bereitstellen und dann die gewünschten Änderungen vornehmen. Mit dem Befehl *imagex /unmount* heben Sie die Bereitstellung des Abbilds im Dateisystem wieder auf, wenn Sie fertig sind.

Sie können Abbilder auch mit *dism /mount-wim* im Dateisystem bereitstellen und die Bereitstellung mit *dism /unmount-wim* wieder aufheben. DISM bietet Funktionen zum Bearbeiten von Abbildern. Sie können damit Product Keys festlegen, Upgrades durchführen, Treiber hinzufügen oder entfernen, Sprach- und Gebietsschemadaten festlegen, Pakete sowie Features hinzufügen oder entfernen und Abbilder aufräumen.

4. Erstellen Sie mit dem Windows-Systemabbild-Manager Ihre Antwortdateien für die unbeaufsichtigte Installation. Anschließend können Sie Bereitstellungsskripts entwickeln, die den Computer konfigurieren, Setup unter Benutzung der Antwortdatei ausführen und das Datenträgerabbild anwenden, das Sie vorher erstellt haben.
5. Führen Sie Ihr Bereitstellungsskript aus, um den Computer zu konfigurieren und das Betriebssystem zu installieren.

Verwalten des Zugriffs und Vorabbereitstellen von Computern

Abbilder können Sie mit DISM und den bereits beschriebenen Verfahren verwalten. Sie haben folgende Möglichkeiten, um zu verhindern, dass nichtautorisierte Benutzer Abbilder installieren:

- Führen Sie eine Vorabbereitstellung der Computer durch und erlauben Sie die Bereitstellung nur für bekannte Computer.
- Ändern Sie die Sicherheitseinstellungen der Abbilddateien, sodass nur berechtigtes Personal darauf zugreifen darf.
- Aktivieren Sie die Administratorgenehmigung für Clientinstallationen.

Vorabbereitstellen von Computern

Beim Vorabbereitstellen (engl. prestaging) von Computern legen Sie Computerkonten in Active Directory an, bevor Sie die entsprechenden Computer benutzen. Mithilfe der Vorabbereitstellung können Sie genau kontrollieren, welche Clients und Server miteinander kommunizieren dürfen. Bevor Sie die Vorabbereitstellung von Computern beginnen, sollten Sie sicherstellen, dass die Windows-Bereitstellungsdienste so konfiguriert sind, dass sie nur Anforderungen von bekannten Computern annehmen. Gehen Sie dazu folgendermaßen vor:

1. Erweitern Sie in der Konsole *Windows-Bereitstellungsdienste* den Knoten *Server*. Halten Sie das Symbol des Servers gedrückt, mit dem Sie arbeiten möchten, oder klicken Sie es mit der rechten Maustaste an, und wählen Sie den Befehl *Eigenschaften*.
2. Wählen Sie auf der Registerkarte *PXE-Antwort* die Option *Nur bekannten Clientcomputern antworten* aus und tippen oder klicken Sie auf *OK*.

Für die Vorabbereitstellung eines Computers müssen Sie die GUID (Globally Unique Identifier) des Computers kennen. Die GUID eines Computers leitet sich aus der aktiven Netzwerkkarte dieses Computers ab und muss im Format {dddddddd-dddd-dddd-dddd-dddddddddddd} eingegeben werden, wobei d eine Hexadezimalziffer ist, zum Beispiel {AEFED345-BC13-22CD-ABCD-11BB11342112}.

Sie haben mehrere Möglichkeiten, die benötigten GUIDs zu ermitteln. In manchen Fällen bringen die Hersteller einen Aufkleber mit der GUID auf dem Computer an. Vergessen Sie in so einem Fall aber nicht, dass die GUID nur gültig ist, solange die Netzwerkkarte benutzt wird, die ursprünglich im Computer eingebaut war. Falls Sie die Netzwerkkarte austauschen, erhält die neue Karte eine andere GUID.

Sie können die GUID für die installierte Netzwerkkarte auch über die Firmware des Computers in Erfahrung bringen. Läuft ein Remotecomputer bereits, können Sie den folgenden Befehl an einer Windows PowerShell-Eingabeaufforderung eingeben:

```
get-wmiobject win32_networkadapter | format-list guid
```

Schreiben Sie die GUID der Netzwerkkarte auf, die mit dem LAN (Local Area Network) verbunden ist, oder kopieren Sie sie über die Zwischenablage.

Gehen Sie folgendermaßen vor, um die Vorabbereitstellung eines Computers durchzuführen:

1. Klicken Sie in der Konsole *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf die Organisationseinheit oder den Container, in dem der Computer abgelegt wird, oder halten Sie das Symbol gedrückt. Tippen oder klicken Sie auf *Neu* und dann auf *Computer*.
2. Geben Sie einen Namen für den Computer ein und tippen oder klicken Sie auf *Weiter*. Stattdessen können Sie auch auf *Ändern* tippen oder klicken und einen Benutzer oder eine Gruppe auswählen, der/die berechtigt ist, diesen Computer zur Domäne hinzuzufügen, und anschließend auf *Weiter* tippen oder klicken.

3. Aktivieren Sie auf der Seite *Verwalteter Computer* das Kontrollkästchen *Verwalteter Computer*, geben Sie die GUID des Computers ein und tippen oder klicken Sie auf *Weiter*. Die GUID finden Sie in der Systemfirmware, manchmal ist sie auch auf dem Computergehäuse vermerkt.
4. Wählen Sie auf der Seite *Hostserver* den Windows-Bereitstellungsdiensteserver aus, der diesen Client bedient. Tippen oder klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

Anpassen der Sicherheitseinstellungen für die Abbilddatei

Die Sicherheitseinstellungen für eine Abbilddatei ändern Sie im Datei-Explorer. Klicken Sie mit der rechten Maustaste auf die Abbilddatei oder halten Sie das entsprechende Symbol gedrückt, und wählen Sie den Befehl *Eigenschaften*. Nun können Sie im Eigenschaftendialogfeld auf der Registerkarte *Sicherheit* die gewünschten Sicherheitseinstellungen konfigurieren. Stattdessen können Sie die Sicherheitseinstellungen auch für den Abbildgruppenordner konfigurieren, in dem die Abbilddatei gespeichert ist. Diese Einstellungen werden dann an alle Abbilder in diesem Abbildgruppenordner vererbt.

Anfordern der Genehmigung von einem Administrator

Statt eine Vorabbereitstellung der Computer durchzuführen oder die Sicherheitseinstellungen der Abbilddatei zu verändern, können Sie es auch von der Genehmigung eines Administrators abhängig machen, ob Computer mithilfe eines Abbilds eingerichtet werden. Gehen Sie folgendermaßen vor, um einzustellen, dass die Genehmigung eines Administrators eingeholt wird, statt die Sicherheitseinstellungen für Abbilddateien zu verändern:

1. Erweitern Sie in der Konsole *Windows-Bereitstellungsdienste* den Knoten *Server*. Klicken Sie mit der rechten Maustaste auf den Server, mit dem Sie arbeiten wollen, oder halten Sie dessen Symbol gedrückt, und tippen oder klicken Sie auf *Eigenschaften*.
2. Wählen Sie auf der Registerkarte *PXE-Antwort* die Option *Allen Clientcomputern antworten (bekannten und unbekannten)*.
3. Aktivieren Sie das Kontrollkästchen *Administratorgenehmigung für unbekannte Computer erforderlich machen* und tippen oder klicken Sie auf *OK*.

Werden nun Computer über das Netzwerk gestartet, befinden Sie sich erst einmal in einem Wartezustand. Bevor die Installation fortgesetzt wird, kann ein Administrator die Anforderung genehmigen oder ablehnen.

Gehen Sie folgendermaßen vor, um eine Anforderung zu genehmigen:

1. Wählen Sie in der Konsole *Windows-Bereitstellungsdienste* den Server aus, mit dem Sie arbeiten wollen. Tippen oder klicken Sie auf den Ordner *Ausstehende Geräte* des Servers, um ihn auszuwählen und eine Liste aller Computer anzuzeigen, die auf eine Genehmigung warten.
2. Klicken Sie mit der rechten Maustaste auf den Computer oder halten Sie dessen Symbol gedrückt, und wählen Sie im Kontextmenü den Befehl *Genehmigen*.

Gehen Sie folgendermaßen vor, um eine Anforderung abzulehnen:

1. Wählen Sie in der Konsole *Windows-Bereitstellungsdienste* den Server aus, mit dem Sie arbeiten wollen. Tippen oder klicken Sie auf den Ordner *Ausstehende Geräte* des Servers, um ihn auszuwählen und eine Liste aller Computer anzuzeigen, die auf eine Genehmigung warten.
2. Klicken Sie mit der rechten Maustaste auf den Computer oder halten Sie dessen Symbol gedrückt, und wählen Sie im Kontextmenü den Befehl *Ablehnen*.

Anpassen von Windows-Abbildern

Mit dem Dienstprogramm DISM können Sie ein bereitgestelltes Start- oder Installationsabbild anpassen. Tabelle 1.2 fasst die verfügbaren Befehle für DISM zusammen. Alle Komponenten in einem Abbild werden über den Komponentenspeicher verwaltet.

Tabelle 1.2 Wichtige Befehle für das Dienstprogramm DISM

Befehlstyp/Befehl	Beschreibung
Allgemeine Befehle	
<code>/Cleanup-Wim</code>	Löscht alle Ressourcen im Zusammenhang mit bereitgestellten Windows-Abbildern, die beschädigt sind.
<code>/Commit-Wim</code>	Speichert die Änderungen in einem bereitgestellten Windows-Abbild.
<code>/Get-MountedWimInfo</code>	Zeigt Informationen über bereitgestellte Windows-Abbilder an.
<code>/Get-WimInfo</code>	Zeigt Informationen über die Abbilder in einer Windows-Abbilddatei an.
<code>/Image</code>	Legt den Pfad zum Stammverzeichnis eines Offline-Windows-Abbilds fest.
<code>/Mount-Wim</code>	Stellt ein Abbild aus einer Windows-Abbilddatei im Dateisystem bereit.
<code>/Online</code>	Legt das laufende Betriebssystem als Ziel fest.
<code>/Remount-Wim</code>	Stellt ein verwaistes Windows-Bereitstellungsverzeichnis wieder her.
<code>/Unmount-Wim</code>	Hebt die Bereitstellung eines bereitgestellten Windows-Abbilds im Dateisystem wieder auf.
Zusätzliche Argumente	
<code>/English</code>	Zeigt die Befehlszeilenausgabe in englischer Sprache an.
<code>/Format</code>	Legt das Berichtsausgabeformat fest.
<code>/LogLevel</code>	Legt fest, welche Ausgabebene im Protokoll aufgezeichnet wird (1–4).
<code>/LogPath</code>	Gibt den Protokolldateipfad an.
<code>/NoRestart</code>	Unterdrückt automatische Neustarts und Aufforderungen, einen Neustart durchzuführen.
<code>/Quiet</code>	Unterdrückt alle Ausgaben außer Fehlermeldungen.
<code>/ScratchDir</code>	Gibt den Pfad für ein Entwurfsverzeichnis an.
<code>/SysDriveDir</code>	Legt den Pfad für die Systemladefile <i>BootMgr</i> fest.
<code>/WinDir</code>	Gibt den Pfad zum Windows-Verzeichnis an.

Sobald Sie ein Abbild im Dateisystem bereitgestellt haben, können Sie die Unterbefehle von *dism /image* benutzen, um das bereitgestellte Abbild zu bearbeiten. Tabelle 1.3 führt die verfügbaren Unterbefehle auf. Mithilfe dieser Unterbefehle können Sie beim Abbild ein Upgrade auf eine höhere Edition vornehmen, Gerätetreiber hinzufügen und entfernen, Zeitzonen und Benutzeroberflächensprache auswählen, Patches und installierte MSI-Anwendungen (Message Signaled Interrupt) anzeigen, Pakete hinzufügen oder entfernen und vieles mehr.

Tabelle 1.3 Wichtige Unterbefehle für bereitgestellte und Offlineabbilder

Unterbefehl	Beschreibung
<code>/Add-Driver</code>	Fügt Treiberpakete zu einem Offlineabbild hinzu.
<code>/Add-Package</code>	Fügt Pakete zum Abbild hinzu.
<code>/Apply-Unattend</code>	Wendet die Datei <i><Antwortdatei>.xml</i> auf ein Abbild an. ►

Unterbefehl	Beschreibung
<i>/Check-AppPatch</i>	Zeigt Informationen an, wenn MSP-Dateien (Multiple Customization Patches) auf das bereitgestellte Abbild angewendet werden können.
<i>/Cleanup-Image</i>	Führt Aufräum- und Wiederherstellungsoperationen für das Abbild aus.
<i>/Disable-Feature</i>	Deaktiviert eine bestimmte Funktion im Abbild.
<i>/Enable-Feature</i>	Aktiviert eine bestimmte Funktion im Abbild.
<i>/Gen-LangIni</i>	Generiert eine neue <i>Lang.ini</i> -Datei.
<i>/Get-AppInfo</i>	Zeigt Informationen über eine bestimmte installierte MSI-Anwendung an.
<i>/Get-AppPatches</i>	Zeigt Informationen über alle angewendeten MSP-Patches für alle installierten Anwendungen an.
<i>/Get-AppPatchInfo</i>	Zeigt Informationen über installierte MSP-Patches an.
<i>/Get-Apps</i>	Zeigt Informationen über alle installierten MSI-Anwendungen an.
<i>/Get-CurrentEdition</i>	Zeigt die Edition des angegebenen Abbilds an.
<i>/Get-DriverInfo</i>	Zeigt Informationen über einen bestimmten Treiber in einem Offlineabbild oder einem laufenden Betriebssystem an.
<i>/Get-Drivers</i>	Zeigt Informationen über alle Treiber in einem Offlineabbild oder einem laufenden Betriebssystem an.
<i>/Get-FeatureInfo</i>	Zeigt Informationen über eine bestimmte Funktion an.
<i>/Get-Features</i>	Zeigt Informationen über alle Funktionen in einem Paket an.
<i>/Get-Intl</i>	Zeigt Informationen über die Gebietseinstellungen und Sprachen an.
<i>/Get-PackageInfo</i>	Zeigt Informationen über ein bestimmtes Paket an.
<i>/Get-Packages</i>	Zeigt Informationen über alle Pakete im Abbild an.
<i>/Get-TargetEditions</i>	Zeigt eine Liste der Windows-Editionen an, auf die bei einem Abbild ein Upgrade durchgeführt werden kann.
<i>/Remove-Driver</i>	Löscht Treiberpakete aus einem Offlineabbild.
<i>/Remove-Package</i>	Löscht Pakete aus dem Abbild.
<i>/Set-AllIntl</i>	Konfiguriert alle Regionaleinstellungen im bereitgestellten Offlineabbild.
<i>/Set-Edition</i>	Führt beim Windows-Abbild ein Upgrade auf eine höhere Edition durch.
<i>/Set-InputLocale</i>	Legt die verwendeten Eingabegeräte und Tastaturlayouts im bereitgestellten Offlineabbild fest.
<i>/Set-LayeredDriver</i>	Legt die überlagerten Tastaturtreiber fest.
<i>/Set-ProductKey</i>	Fügt den Product Key in das Offlineabbild ein.
<i>/Set-SetupUILang</i>	Legt die Standardsprache für das Setup fest.
<i>/Set-SKUIntlDefaults</i>	Setzt alle Regionaleinstellungen im bereitgestellten Offlineabbild auf die Standardwerte für die angegebene SKU-Sprache.
<i>/Set-SysLocale</i>	Legt die Sprache für Nicht-Unicode-Programme (das Systemgebietsschema) und Schrifteinstellungen im bereitgestellten Offlineabbild fest.
<i>/Set-TimeZone</i>	Legt die Standardzeitzone im bereitgestellten Offlineabbild fest.
<i>/Set-UILang</i>	Legt die Standardsprache für die verwendete Systembenutzeroberfläche im bereitgestellten Offlineabbild fest.
<i>/Set-UILangFallback</i>	Legt die zweite Standardsprache für die verwendete Systembenutzeroberfläche im bereitgestellten Offlineabbild fest.
<i>/Set-UserLocale</i>	Legt das Benutzergebietsschema im bereitgestellten Offlineabbild fest.

Das Tool zur Abbildverwaltung für die Bereitstellung stellt Befehle zum Arbeiten mit WIM-Abbildern zur Verfügung. Abbilder werden mit der folgenden Syntax im Dateisystem bereitgestellt:

```
dism /mount-wim /wimfile:Pfad /index:Index /mountdir:Bereitstellungspfad
```

Dabei sind *Pfad* der vollständige Pfad zum WIM-Abbild, *Index* die Nummer des gewünschten Abbilds innerhalb der *.wim*-Datei und *Bereitstellungspfad* der Verzeichnisspeicherort, an dem Sie das Abbild bereitstellen wollen. Hier ein Beispiel:

```
dism /mount-wim /wimfile:c:\winpe_x86\iso\sources\boot.wim /index:1 /mountdir:c:\Win8
```

Nun können Sie das Abbild nach Ihren Wünschen anpassen. Dabei können Sie die Änderungen jederzeit speichern, indem Sie *dism /commit-wim* ausführen, wie in diesem Beispiel:

```
dism /commit-wim /mountdir:c:\Win8
```

Hier speichern Sie die Änderungen in den WIM-Abbildern, die Sie im Verzeichnis *C:\Win8* bereitgestellt haben.

Mit *dism /unmount-wim* heben Sie die Bereitstellung einer WIM-Datei im Dateisystem wieder auf. Ein Beispiel:

```
dism /unmount-wim /mountdir:c:\Win8
```

In diesem Beispiel heben Sie die Bereitstellung des WIM-Abbilds auf, das im Verzeichnis *C:\Win8* bereitgestellt und dort verändert wurde. Haben Sie Änderungen vorgenommen, die noch nicht gespeichert wurden, müssen Sie diese Änderungen speichern oder verwerfen, wenn Sie die Bereitstellung des WIM-Abbilds im Dateisystem aufheben. Fügen Sie das Argument */Commit* hinzu, um die Änderungen zu speichern, oder */Discard*, um sie zu verwerfen. Dies wirkt sich nur auf Änderungen aus, die Sie noch nicht vorher gespeichert haben.

Installieren von Windows 8

Die Editionen Windows 8 Pro und Enterprise sind für den Einsatz in Active Directory-Domänen gedacht. Wenn Sie Windows 8 auf einem Computer installieren, der bereits ein Betriebssystem hat, haben Sie die Wahl, entweder eine Neuinstallation oder ein Upgrade auszuführen. Die wesentlichen Unterschiede zwischen einer Neuinstallation und einem Upgrade sind:

- **Neuinstallation** Bei einer Neuinstallation ersetzt das Windows-Setupprogramm das vorherige Betriebssystem auf dem Computer vollständig. Alle Benutzer- und Anwendungseinstellungen gehen verloren. Eine Neuinstallation sollten Sie durchführen, wenn kein Upgrade des Betriebssystems möglich ist, wenn das System mehrere Betriebssysteme starten soll, wenn eine standardisierte Konfiguration benötigt wird oder wenn noch kein Betriebssystem installiert ist.
- **Upgradeinstallation** Bei einem Upgrade bleiben Benutzerkonten, Benutzerdateien und Benutzereinstellungen erhalten, vorhandene Anwendungen und deren Einstellungen werden beibehalten und eine grundlegende Systemkonfiguration braucht nicht zu erfolgen. Eine Upgradeinstallation sollten Sie durchführen, wenn Ihre Computer unter einer Windows-Version laufen, die das Upgrade auf Windows 8 unterstützt, und wenn Sie die Arbeitsunterbrechung so kurz wie möglich halten wollen. Auf diese Weise bleiben die vorhandenen Einstellungen, Benutzerdaten und Anwendungskonfigurationen erhalten.

Auf welche Weise das Upgrade abläuft, hängt davon ab, welches Betriebssystem aktualisiert wird. Wenn Sie von Windows 7 aus ein Upgrade durchführen, nimmt Windows Setup eine direkte Aktualisierung (In-Place-Upgrade) vor, die so funktioniert, wie bereits beschrieben. Unter Windows Vista und Windows XP wird eine direkte Aktualisierung in-place anders durchgeführt. Mit Windows Vista können Sie Be-

nutzerkonten, Benutzerdateien und Benutzereinstellungen beibehalten, ebenso die grundlegende Systemkonfiguration, aber Windows Setup bewahrt nicht die vorhandenen Anwendungen und deren Einstellungen. Mit Windows XP können Sie ebenfalls Benutzerkonten, Benutzerdateien und Benutzereinstellungen beibehalten, aber Windows Setup bewahrt nicht die grundlegende Systemkonfiguration und auch nicht die vorhandenen Anwendungen und deren Einstellungen.

Vorbereiten der Windows 8-Installation

Bei der Installation von Windows 8 haben Sie die Möglichkeit, vom Windows-Installationsmedium zu starten, Setup aus Ihrem aktuellen Windows-Betriebssystem heraus zu starten, eine Befehlszeileninstallation auszuführen oder eine der automatischen Installationsmöglichkeiten zu verwenden.

Es gibt für die Installation von Windows 8 zwei grundlegende Ansätze: interaktiv oder automatisiert. Die meisten Leute sind mit der interaktiven Installation vertraut; dabei gehen Sie den Setupprozess schrittweise durch und geben etliche Informationen ein. Diesen Prozess führen Sie mit dem Installationsmedium aus (indem Sie entweder vom Installationsmedium starten oder Windows Setup in einer Befehlszeile aufrufen). Wenn Sie von einer im Handel gekauften Windows 8-DVD starten, läuft der interaktive Installationsprozess ab, bei dem Sie während des Vorgangs mehrmals aufgefordert werden, Konfigurationsinformationen einzugeben.

Für das automatisierte Setup stehen mehrere Arten zur Auswahl, bei denen der Administrator festlegt, wie viel Benutzerinteraktion erforderlich ist. Die simpelste Form des automatisierten Setups ist eine unbeaufsichtigte Installation, bei der ausschließlich Antwortdateien verwendet werden. Eine Antwortdatei enthält entweder alle oder einen Teil der Konfigurationsdaten, die Sie bei einem Standardinstallationsprozess von Hand eingeben. Antwortdateien für die unbeaufsichtigte Installation erstellen Sie mit dem Windows-Systemabbild-Manager, der im Windows Assessment and Deployment Kit (ADK), herunterzuladen unter <http://download.microsoft.com/>, enthalten ist. Mithilfe der Windows-Bereitstellungsdienste können Sie das unbeaufsichtigte Setup noch weiter automatisieren.

Das Standardsetupprogramm für Windows 8 ist *Setup.exe*. Sie starten *Setup.exe* aus einer vorhandenen Version des Betriebssystems Windows, um ein Upgrade durchzuführen, oder Sie starten den Computer vom Vertriebsmedium, um Windows 8 neu zu installieren. Wenn Sie mit Windows 8 auf einem x86-System arbeiten, müssen Sie die speziellen Laufwerksabschnitte kennen, die vom Betriebssystem benutzt werden:

- **Aktiv** Die aktive Partition beziehungsweise das aktive Volume ist der Laufwerksabschnitt für Systemcache und Systemstartcode. Auch manche Wechseldatenträger werden unter den Laufwerken aufgelistet, die eine aktive Partition haben.
- **Start** Die Startpartition beziehungsweise das Startvolume enthält das Betriebssystem und die zugehörigen Dateien. System- und Startpartition beziehungsweise -volume können identisch sein.
- **System** Die Systempartition beziehungsweise das Systemvolume enthält die hardwarespezifischen Dateien, die gebraucht werden, um das Betriebssystem zu laden. Da Systempartition oder Systemvolume einen Teil der Softwarekonfiguration bilden, können sie nicht in einem Stripeset oder in einem übergreifenden Volume liegen.

Partitionen und Volumes sind im Wesentlichen dasselbe. Es werden allerdings zwei unterschiedliche Begriffe verwendet, weil Sie Partitionen auf einem Basisdatenträger anlegen, Volumes dagegen auf einem dynamischen Datenträger. Auf einem x86-Computer verwenden Sie das Snap-In *Datenträgerverwaltung*, um eine Partition als aktiv zu markieren.

Beim aktiven Volume, dem Startvolume und dem Systemvolume kann es sich zwar um dasselbe Volume handeln, aber alle drei Typen werden benötigt. Wenn Sie Windows 8 installieren, analysiert das Setup-

programm alle Festplattenressourcen, die zur Verfügung stehen. Gewöhnlich legt Windows 8 Start- und Systemdateien auf dasselbe Laufwerk und dieselbe Partition und markiert diese Partition als aktive Partition. Diese Konfiguration hat den Vorteil, dass Sie nicht mehrere Laufwerke für das Betriebssystem brauchen und die Betriebssystempartitionen auf einem zusätzlichen Laufwerk spiegeln können.

Bei der Installation auf einer EFI-Hardwareplattform gibt es einige Unterschiede. Das Extended Firmware Interface (EFI) der IA64-Plattform lädt beim Systemstart zuerst ein Startmenü, das in der Firmware definiert ist. EFI-Datenträger haben gewöhnlich eine Partitionsstruktur, die als GUID-Partitionstabelle (Globally Unique Identifier) oder GPT (GUID Partition Table) bezeichnet wird. Diese Partitionsstruktur unterscheidet sich grundlegend von den MBR-Partitionen einer 32-Bit-Plattform.

GPT-Datenträger haben zwei obligatorische Partitionen und optional bis zu 128 weitere Partitionen, die als OEM- oder Datenpartitionen bezeichnet werden:

- EFI-Systempartition (EFI System Partition, ESP)
- Microsoft-reservierte Partition (Microsoft Reserved Partition, MSR)
- Mindestens eine Datenpartition

Das EFI-Startmenü bietet mehrere Optionen an, eine davon ist die EFI-Shell. Die EFI-Shell stellt eine Betriebsumgebung zur Verfügung, in der die Dateisysteme FAT und FAT32 sowie Konfigurations- und Dateiverwaltungsbefehle unterstützt werden. Der Befehl *Map* zeigt die Liste der Partitionen auf einem EFI-Computer an. In der Ausgabe des Befehls *Map* sind unter *blk* die Partitionsblöcke und unter *fs#* die lesbaren Dateisysteme aufgeführt. Sie wechseln in eine andere Partition, indem Sie die Blocknummer der Partition gefolgt von einem Doppelpunkt eingeben. Der Befehl *dir* listet die Dateien in der Partition auf. EFI enthält einen Systemstartwartungsmanager (engl. boot maintenance manager), mit dem Sie das Startmenü konfigurieren können.

Wenn Sie Windows 8 installieren, erstellt das Setupprogramm automatisch eine Partition für die Windows-Wiederherstellungsumgebung (Windows Recovery Environment, Windows RE) und installiert darin zusätzliche Komponenten, die bei Wiederherstellung und Problembehandlung zum Einsatz kommen. Daher stehen die Windows-Wiederherstellungstools auf einem Windows 8-Computer immer zur Verfügung. Weitere Informationen finden Sie im Abschnitt »Wiederherstellen nach einem fehlgeschlagenen Start« von Kapitel 10, »Erledigen von Wartungs- und Supportaufgaben«.

Als Administrator können Sie diese Tools einsetzen, um Computer wiederherzustellen. Gelingt es einem Benutzer an einem anderen Standort nicht, Windows zu starten, können Sie ihm beschreiben, wie er Windows RE startet und die Wiederherstellung einleitet. Dazu erklären Sie dem Benutzer, wie er auf das Menü *Erweiterte Startoptionen* zugreift, wie im Abschnitt »Wiederherstellen nach einem fehlgeschlagenen Start« von Kapitel 10, »Erledigen von Wartungs- und Supportaufgaben«, beschrieben.

Installieren von Windows 8

Bevor Sie Windows 8 auf einem Computer installieren, sollten Sie überprüfen, ob die vorliegende Hardware die Anforderungen erfüllt, die an den verfügbaren Arbeitsspeicher, die Rechenleistung und die Leistungsfähigkeit der Grafikkarte gestellt werden. Microsoft hat eine Mindestanforderung und eine Empfehlung formuliert. Die Anforderungen an das Grafiksystem und den Speicher werden in Megabyte (MByte) und Gigabyte (GByte) gemessen, die Anforderungen an Prozessoren in Gigahertz (GHz).

Der Einsatz von Windows 8 setzt folgende Ausstattung voraus:

- Ein 32-Bit- (x86) oder 64-Bit-Prozessor (x64) mit mindestens 1 GHz
- Mindestens 1 GByte RAM (32-Bit-System) beziehungsweise 2 GByte RAM (64 Bit)

- Ein DirectX-9-fähiger Grafikchip mit einem Treiber, der mindestens WDDM 1.0 unterstützt
- Eine Touch-Benutzeroberfläche erfordert ein multitouchfähiges Tablet oder einen entsprechenden Monitor.

HINWEIS Microsoft empfiehlt, dass auf dem Computer mindestens 16 GByte (32-Bit-Version) beziehungsweise 20 GByte (64-Bit-Version) Festplattenplatz frei sein sollte. Durch verschiedene Windows 8-Funktionen kann der Platzbedarf der Installation schnell ansteigen, beispielsweise durch Systemschutzpunkte, mit denen alte Versionen von geänderten Dateien und Ordnern aufbewahrt werden. Damit die Festplatte immer optimale Leistung liefert, sollten stets 15 Prozent ihrer Kapazität frei bleiben und genug Platz für die Auslagerungsdatei zur Verfügung stehen, die doppelt so groß werden kann wie das RAM des Computers. Sofern Sie ein In-Place-Upgrade durchführen, speichert außerdem der Ordner *Windows.old* die Ordner und Dateien der vorherigen Installation.

Ein Computer, der diese Hardwarevoraussetzungen erfüllt oder übertrifft, kann Windows 8 ausführen. Eine Neuinstallation von Windows 8 führen Sie mit folgenden Schritten durch:

1. Schalten Sie den Computer ein und legen Sie den Windows 8-Datenträger ins DVD-ROM-Laufwerk des Computers ein. Wenn Sie dazu aufgefordert werden, drücken Sie eine Taste, um das Setupprogramm von der DVD zu starten. Falls keine Aufforderung erscheint, eine Taste zu drücken, um den Computer von der DVD zu starten, müssen Sie wahrscheinlich die Boot- oder Startoptionen in der Firmware ändern.
2. Sie werden aufgefordert, Einstellungen für die Sprache, die Zeit, das Währungsformat und die Tastatur vorzunehmen. Tippen oder klicken Sie anschließend auf *Weiter* und dann auf *Jetzt installieren*.
3. Bei den Einzelhandelsversionen von Windows 8 müssen Sie gewöhnlich einen Product Key eingeben. Tun Sie dies, wenn Sie dazu aufgefordert werden. Tippen Sie auf die Schaltfläche *Bildschirmtastatur*, falls Sie auf einem Gerät ohne Tastatur arbeiten, und geben Sie den Product Key dann mit der Bildschirmtastatur ein.

HINWEIS Wenn das Setupprogramm den Product Key nicht akzeptiert, überprüfen Sie, ob Sie die einzelnen Buchstaben und Ziffern korrekt eingegeben haben. Die Bindestriche brauchen Sie nicht einzugeben. Manchmal ist es einfacher, den Product Key neu einzugeben, statt nach dem falschen Wert in der Zeichenfolge zu suchen.

4. Lesen Sie die Lizenzbedingungen. Wenn Sie einverstanden sind, tippen oder klicken Sie auf *Ich akzeptiere die Lizenzbedingungen* und dann auf *Weiter*.
5. Die Seite *Wählen Sie eine Installationsart aus* wird angezeigt und ermöglicht Ihnen die Wahl zwischen einer Upgrade- und einer benutzerdefinierten Installation. Wählen Sie *Benutzerdefiniert: nur Windows installieren (für fortgeschrittene Benutzer)*, um mit der Neuinstallation fortzufahren.
6. Wählen Sie die Laufwerkspartition aus, auf der Sie das Betriebssystem installieren wollen, und tippen oder klicken Sie auf *Weiter*.

TIPP Auf der Seite *Wo möchten Sie Windows installieren* können Sie während der Installation eine Eingabeaufforderung öffnen, indem Sie die Tastenkombination UMSCHALT+F10 drücken. Daraufhin startet eine MinWinPC-Umgebung, die Setup benutzt, um das Betriebssystem zu installieren. Hier haben Sie Zugriff auf viele Befehlszeilentools, die auch in einer Standardinstallation von Windows 8 verfügbar sind.

7. Sofern es auf der Laufwerkspartition, die Sie ausgewählt haben, bereits eine Windows-Installation gibt, erscheint eine Meldung, in der Sie darauf hingewiesen werden, dass die vorhandenen Benutzer- und Anwendungseinstellungen in einen Ordner namens *Windows.old* verschoben werden und dass Sie zwar auf die Dateien zugreifen, die vorige Windows-Version aber nicht benutzen können. Tippen oder klicken Sie auf *OK*.
8. Nun beginnt Setup mit der Installation. Im Verlauf dieses Vorgangs kopiert Setup das Laufwerkabbild von Windows 8 auf das Laufwerk, das Sie ausgewählt haben, und entpackt es. Anschließend installiert Setup auf der Basis der Computerkonfiguration und der erkannten Hardware die gewünschten Funktionen. Sobald Setup die Installation abschließt, wird das Betriebssystem geladen und für die erste Benutzung eingerichtet. Nach der Vorbereitung des Systems startet Setup den Computer erneut.
9. Wählen Sie auf der Seite *Anpassen* eine Hintergrundfarbe für die *Start*-Seite und den Desktop aus. Geben Sie einen Computernamen ein und tippen oder klicken Sie auf *Weiter*.
10. Falls Sie dazu aufgefordert werden, wählen Sie Ihr Land oder Ihre Region, Zeit- und Währungsformat sowie Ihr Tastaturlayout aus. Klicken Sie dann auf *Weiter*.
11. Bei Drahtlosverbindungen müssen Sie die Drahtlosverbindung auswählen, die verwendet werden soll. Wenn Sie auf *Verbinden* tippen oder klicken, können Sie ein Kennwort für das Drahtlosnetzwerk eingeben. Anschließend müssen Sie erneut auf *Verbinden* tippen oder klicken. Wenn der Computer über eine herkömmliche Kabelverbindung zum Internet verfügt, sollte dies nicht erforderlich sein.
12. Auf der Seite *Einstellungen* können Sie auf *Express-Einstellungen verwenden* tippen oder klicken, um die Expresseinstellungen zu übernehmen, oder auf *Anpassen*, falls Sie die Einstellungen selbst vornehmen möchten. Die Expresseinstellungen geben bestimmte Standardeinstellungen vor:
 - Aktivierung der Freigabe und Verbindung mit Geräten. In Heim- und Arbeitsplatznetzwerken kann diese Einstellung sinnvoll sein, aber nicht zwangsläufig auch in Domänenumgebungen.
 - Automatische Installation von wichtigen und empfohlenen Updates, ebenso von Updates für Geräte
 - Aktivierung des SmartScreen-Filters für den Internet Explorer und Windows zum Schutz des PCs vor unsicheren Inhalten, Dateien und Websites
 - Verwendung der Windows-Fehlerberichterstattung für die Suche nach Lösungen für Probleme
 - Zur Lösung von Kompatibilitätsproblemen mit Websites werden im Internet Explorer Kompatibilitätslisten verwendet.
 - Desktop-Anwendungen können Ihren Namen und Ihr Kontenbild verwenden.
 - Die Plattform für Windows-Position (Windows Location Platform) wird aktiviert, damit Desktop-Anwendungen Benutzer nach ihrem Standort fragen können.
13. Wenn der Computer über eine Internetverbindung verfügt, haben Sie auf der Seite *Am PC anmelden* die Wahl zwischen der Einrichtung eines Microsoft-Kontos oder eines lokalen Computerkontos. Andernfalls lässt sich nur ein lokales Computerkonto erstellen. Da in einer Domäne oder Arbeitsgruppe gewöhnlich ein lokales Konto gewünscht wird, klicken oder tippen Sie auf *Ohne Microsoft-Konto anmelden* und bestätigen Ihre Wahl, indem Sie *Lokales Konto* anklicken oder antippen. Geben Sie dann einen Benutzernamen ein. Geben Sie ein Kennwort ein und bestätigen Sie es. Geben Sie außerdem einen Kennworthinweis ein. Tippen oder klicken Sie dann auf *Fertig stellen*.

14. Anschließend bereitet Windows 8 den Desktop des Computers vor.

Eine Aktualisierung eines vorhandenen Computers auf Windows 8 führen Sie mit folgenden Schritten durch:

1. Starten Sie den Computer und melden Sie sich mit einem Administratorkonto an. Legen Sie die Windows 8-DVD in das DVD-ROM-Laufwerk des Computers ein. Das Setupprogramm von Windows 8 sollte automatisch starten. Ist dies nicht der Fall, wechseln Sie im Datei-Explorer auf das DVD-Laufwerk und tippen oder klicken *Setup.exe* doppelt an.

HINWEIS Bei der Installation ist nur die aktuell im Betriebssystem konfigurierte Tastatur verfügbar. Das kann zur Folge haben, dass Sie vielleicht unerwartete Zeichen sehen, wenn Sie eine Windows 8-Edition mit einer abweichenden Tastatureinstellung und Sprache installieren.

2. Setup kopiert temporäre Dateien und beginnt dann mit der Arbeit. Wenn Ihr Computer mit dem Internet verbunden ist, können Sie angeben, ob die erforderlichen Updates bereits bei der Installation heruntergeladen werden. Tippen oder klicken Sie entweder auf *Online gehen, um jetzt Updates zu installieren* oder auf *Nein danke*.

TIPP Sie brauchen bei der Installation noch keine Updates herunterzuladen. Das können Sie mit Windows Update auch später nachholen. Ich ziehe es allerdings vor, die Updates bereits bei der Installation herunterzuladen, damit der Computer auf einem aktuellen Stand ist, wenn ich das Betriebssystem installiert habe.

3. Bei den Einzelhandelsversionen von Windows 8 müssen Sie gewöhnlich einen Product Key eingeben. Tun Sie dies, wenn Sie dazu aufgefordert werden. Tippen Sie auf die Schaltfläche *Bildschirmtastatur*, falls Sie auf einem Gerät ohne Tastatur arbeiten, und geben Sie den Product Key dann mit der Bildschirmtastatur ein. Wenn Sie das nächste Mal eine Verbindung herstellen, führt der Computer automatisch eine Aktivierung von Windows durch. Tippen oder klicken Sie auf *Weiter*.

HINWEIS Wenn das Setupprogramm den Product Key nicht akzeptiert, überprüfen Sie, ob Sie die einzelnen Buchstaben und Ziffern korrekt eingegeben haben. Die Bindestriche brauchen Sie nicht einzugeben. Manchmal ist es einfacher, den Product Key neu einzugeben, statt nach dem falschen Wert in der Zeichenfolge zu suchen.

4. Lesen Sie die Lizenzbedingungen. Wenn Sie einverstanden sind, tippen oder klicken Sie auf *Ich akzeptiere die Lizenzbedingungen* und dann auf *Weiter*.
5. Welche Optionen Sie auf der Seite sehen, auf der festgelegt wird, was beibehalten werden soll, hängt davon ab, welche Windows-Version derzeit auf Ihrem Computer läuft. Die Aktualisierungsoptionen betreffen folgende Bereiche:
 - **Windows-Einstellungen** Ist dieser Punkt verfügbar und ausgewählt, versucht Setup, die Grundeinstellungen zu bewahren, beispielsweise die Einstellungen für den Desktophintergrund, den Monitor, die Internetfavoriten, den Internetverlauf und die Bedienung. Nicht alle Einstellungen werden nach Windows 8 übertragen und sind dort verfügbar.
 - **Persönliche Dateien** Wenn dieser Punkt verfügbar und ausgewählt ist, speichert Setup persönliche Dateien aus dem Ordner des Benutzers. Das bedeutet, dass persönliche Dateien aus den Ordnern *Dokumente*, *Musik*, *Bilder*, *Videos* und aus anderen Ordnern verschoben und unter Windows 8 verfügbar gemacht werden.

- **Anwendungen** Ist dieser Punkt verfügbar und ausgewählt, speichert Setup Einstellungen für Desktopanwendungen, damit sie nach dem Upgrade verfügbar sind. Desktopprogramme und einige Desktopanwendungen müssen neu installiert werden.
- **Nichts** Ist dieser Punkt ausgewählt, verschiebt Setup Ordner und Dateien aus der vorigen Windows-Installation in einen Ordner namens *Windows.old* und die vorige Windows-Installation ist nicht mehr lauffähig.

SICHERHEIT Wenn Sie ein Upgrade durchführen und zur Anmeldung ein Fingerabdruckleser oder ein anderes biometrisches Gerät benutzen, müssen Sie Ihr Kennwort notieren. Bei der ersten Anmeldung an Windows 8 müssen Sie den Benutzernamen und das Kennwort eingeben.

6. Tippen oder klicken Sie auf *Weiter* und dann auf *Installieren*. Fahren Sie mit den Schritten 8 bis 14 der bereits beschriebenen Prozedur fort.

Es kann aus verschiedenen Gründen vorkommen, dass bei der Installation von Windows 8 Probleme auftreten. Hier kurz einige Lösungen für öfters vorkommende Probleme:

- **Sie können nicht vom Windows 8-Installationsmedium starten** Die meisten Computer können zwar von DVD starten, aber manchmal ist diese Möglichkeit in der Firmware deaktiviert. Stellen Sie die Startreihenfolge in der Firmware so ein, dass das DVD-Laufwerk vor den Festplattenlaufwerken und anderen startfähigen Medien aufgelistet ist. Weitere Informationen finden Sie in Kapitel 4, »Verwalten von Firmware, Startkonfiguration und Systemstart«.
- **Sie können während des Setups keine Festplatte auswählen** Das Windows 8-Installationsmedium enthält zwar Treiber für die meisten Festplattencontroller, aber unter Umständen haben Sie einen Controller, zu dem kein Standardtreiber verfügbar ist. Legen Sie das Medium ein, auf dem die erforderlichen Treiber gespeichert sind, und tippen oder klicken Sie auf der Seite *Wo möchten Sie Windows installieren* auf *Treiber laden*. Befindet sich der Treiber auf einem internen Festplattenlaufwerk, können Sie auch die Tastenkombination UMSCHALT+F10 drücken, um eine Eingabeaufforderung zu öffnen, und dann mit Xcopy die Treiberdateien auf einen USB-Speicherstick oder einen anderen Wechseldatenträger kopieren. Klicken Sie dann auf *Treiber laden*, um die Treiber von diesem Medium einzulesen.
- **Sie haben vergessen, als Vorbereitung auf die Installation die Festplattenkonfiguration zu ändern** Tippen oder klicken Sie auf der Seite *Wo möchten Sie Windows installieren* auf *Laufwerkoptionen (erweitert)*. Mit den nun angebotenen Optionen können Sie nach Bedarf Partitionen erstellen, löschen und formatieren. Falls Sie eine Partition verkleinern oder vergrößern wollen (auch während eines Upgrades), können Sie mit der Tastenkombination UMSCHALT+F10 eine Eingabeaufforderung öffnen und dann mit dem Dienstprogramm DiskPart die Partition bearbeiten. Sie können Partitionen auf diese Weise vergrößern und verkleinern, ohne sie zu löschen. Außerdem bietet DiskPart die Möglichkeit, den Laufwerkstyp und den Partitionstyp zu ändern. Weitere Informationen zu DiskPart finden Sie in den Kapiteln 10, 11 und 12 des Buchs *Windows Command-Line Administrator's Pocket Consultant, Second Edition* (Microsoft Press, 2008).

Ausführen von Windows 8

Nach dem Start des Betriebssystems können Sie sich anmelden und auf den Desktop zugreifen. Standardmäßig speichert Windows 8 Benutzerprofile unter `%SystemDrive%\Users\%UserName%`. Im Ordner der Benutzerprofile wird für jeden Benutzer, der sich auf dem System anmeldet, ein persönlicher Ordner angelegt, in dem sich etliche Unterordner befinden. Diese Ordner sind die Standardspeicherorte für bestimmte Daten- und Dateitypen. Die wichtigsten Unterordner sind:

- **AppData** Benutzerspezifische Anwendungsdaten (in einem ausgeblendeten Ordner)
- **Desktop** Der Desktop des Benutzers
- **Downloads** Programme und Daten, die aus dem Internet heruntergeladen wurden
- **Eigene Bilder** Die Bilder des Benutzers
- **Eigene Dokumente** Die Dokumentdateien des Benutzers
- **Eigene Musik** Die Musikdateien des Benutzers
- **Eigene Videos** Die Videodateien des Benutzers
- **Favoriten** Die Internetfavoriten des Benutzers
- **Gespeicherte Spiele** Die gespeicherten Spielstände des Benutzers
- **Kontakte** Kontakte und Kontaktgruppen
- **Links** Die Internetlinks des Benutzers
- **Suchvorgänge** Die gespeicherten Suchvorgänge des Benutzers

HINWEIS `%SystemDrive%` und `%UserName%` stehen für die Umgebungsvariablen `SystemDrive` und `UserName`. Im Betriebssystem Windows gibt es viele Umgebungsvariablen, die für den Zugriff auf benutzer- oder systemspezifische Werte verwendet werden. Wenn in diesem Buch der aktuelle Wert einer Umgebungsvariablen verwendet werden soll, gebe ich die Variable mit folgender Syntax an: `%Variablenname%`. Falls Sie eine ältere Windows-Version auf Windows 8 aktualisiert haben, enthält der persönliche Ordner eines Benutzers auch symbolische Links (die wie Verknüpfungen aussehen) zu den Ordnern und Einstellungen, die in dieser älteren Version verwendet wurden. Ein *symbolischer Link* ist ein Zeiger auf eine Datei oder einen Ordner. Ein solcher Link wird oft erstellt, um die Abwärtskompatibilität für Anwendungen zu gewährleisten, die an einem bestimmten Speicherort, der verschoben wurde, nach einem Ordner oder einer Datei suchen. Sie erstellen symbolische Verknüpfungen mit dem Befehlszeilenprogramm `Mklink`. Geben Sie in einer Eingabeaufforderung den Befehl `mklink /?` ein, um sich die verfügbaren Optionen anzeigen zu lassen.

Neben den persönlichen Ordnern verwendet Windows 8 auch persönliche Bibliotheken. Eine solche Bibliothek ist lediglich eine Sammlung mehrerer Dateien und Ordner, die zusammengefasst und in einer gemeinsamen Ansicht aufgelistet werden. Es gibt folgende Standardbibliotheken:

- **Dokumente** Vereinigt die Daten aus dem Ordner *Eigene Dokumente* des Benutzers und dem Ordner *Öffentliche Dokumente*.
- **Musik** Vereinigt die Daten aus dem Ordner *Eigene Musik* eines Benutzers und dem Ordner *Öffentliche Musik*.
- **Bilder** Vereinigt die Daten aus dem Ordner *Eigene Bilder* eines Benutzers und dem Ordner *Öffentliche Bilder*.
- **Videos** Vereinigt die Daten aus dem Ordner *Eigene Videos* eines Benutzers und dem Ordner *Öffentliche Videos*.

Sie können neue Bibliotheken anlegen, die verschiedene Datensammlungen anzeigen. Klicken Sie dazu im Datei-Explorer mit der rechten Maustaste auf den Knoten *Bibliotheken*, oder halten Sie ihn gedrückt, wählen Sie *Neu* und dann *Bibliothek*.

WICHTIG

Wenn Sie mit Bibliotheken arbeiten, dürfen Sie nicht vergessen, dass es sich dabei lediglich um Auflistungen der gesammelten Daten handelt. Windows 8 erstellt zusammengefasste Ansichten aller Dateien und Ordner, die Sie zu Bibliotheken hinzufügen. Die Bibliotheken selbst enthalten keinerlei Daten. Alle Aktionen, die Sie mit einer Datei oder einem Ordner innerhalb einer Bibliothek ausführen, wirken auf die Quelldatei beziehungsweise den Quellordner.

Windows 8 stellt Designs zur Verfügung, mit denen Sie ganz einfach das Aussehen von Menüs, Fenstern und Desktop anpassen können. Sie wählen ein Design aus, indem Sie in der Systemsteuerung unter *Darstellung und Anpassung* auf den Link *Design ändern* tippen oder klicken und das gewünschte Design auswählen. Die Windows-Standard-Designs sehen gut aus und stellen ausgefeilte dynamische Effekte für die Benutzeroberfläche zur Verfügung. Reicht die Leistung des Anzeigegeräts nicht aus, sollten Sie gegebenenfalls ein Design mit hohem Kontrast wählen. Ob ein anspruchsvolleres Benutzeroberflächendesign auf einem Computer verwendet werden kann, hängt allerdings davon ab, welche Windows 8-Edition installiert ist und welche Hardwareleistung der Computer bietet.

Arbeiten mit dem Wartungscenter und Aktivieren von Windows

In der Standardeinstellung zeigt das Betriebssystem nach der Anmeldung im Infobereich der Taskleiste eine weiße Fahne als Symbol für das Wartungscenter an. Das Wartungscenter ist ein Programm, das den Status wichtiger Sicherheits- und Wartungsbereiche überwacht. Ändert sich der Status eines überwachten Elements, ändert das Wartungscenter das Benachrichtigungssymbol, sodass es den Schweregrad der Warnung widerspiegelt. Wenn Sie das Symbol antippen oder anklicken, zeigt Windows ein Dialogfeld mit einer Zusammenfassung aller Warnungen oder Elemente an, die Ihre Aufmerksamkeit benötigen. Tippen oder klicken Sie auf den Link einer Warnung, um die dazugehörige Lösung zu starten. Tippen oder klicken Sie auf den Link *Wartungscenter öffnen*, um das Wartungscenter anzuzeigen.

Falls Sie die Benachrichtigungen des Wartungscenters in der Taskleiste deaktiviert haben, können Sie das Wartungscenter folgendermaßen starten:

1. Klicken Sie in *Systemsteuerung* auf den Kategorielink *System und Sicherheit*.
2. Tippen oder klicken Sie auf *Wartungscenter*.

Das Wartungscenter (Abbildung 1.1) bietet einen Überblick über den Status des Computers und listet alle Probleme auf, die beseitigt werden müssen. Nach der Installation von Windows 8 werden Sie im Wartungscenter vielleicht darauf hingewiesen, dass Gerätetreiber verfügbar sind und installiert werden müssen. Tippen oder klicken Sie auf die Aktionsschaltfläche, um die Treiberinstallation zu starten. Ausführlichere Informationen über die Arbeit mit dem Wartungscenter finden Sie im Abschnitt »Benutzen von *Hilfe und Support*« von Kapitel 9, »Verwalten von Hardwaregeräten und Treibern«.

Für die Editionen Windows 8 Pro und Enterprise werden Volumenlizenzen angeboten. Windows 8-Versionen, für die Volumenlizenzen verfügbar sind, müssen unter Umständen nicht aktiviert werden und benötigen keinen Product Key, aber die Handelsversionen von Windows 8 müssen aktiviert werden und brauchen einen Product Key. Ob Windows 8 aktiviert ist, stellen Sie in der Systemsteuerung fest. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*. Lesen Sie auf der Seite *System* den Text unter *Windows-Aktivierung*. Dieser Eintrag gibt an, ob Sie das Betriebssystem aktiviert haben. Wurde Windows 8 noch nicht aktiviert, können Sie, sofern Sie mit dem Internet verbunden sind, *Details in der Windows-Aktivierung anzeigen* wählen und dann auf *Aktivieren* tippen oder klicken.

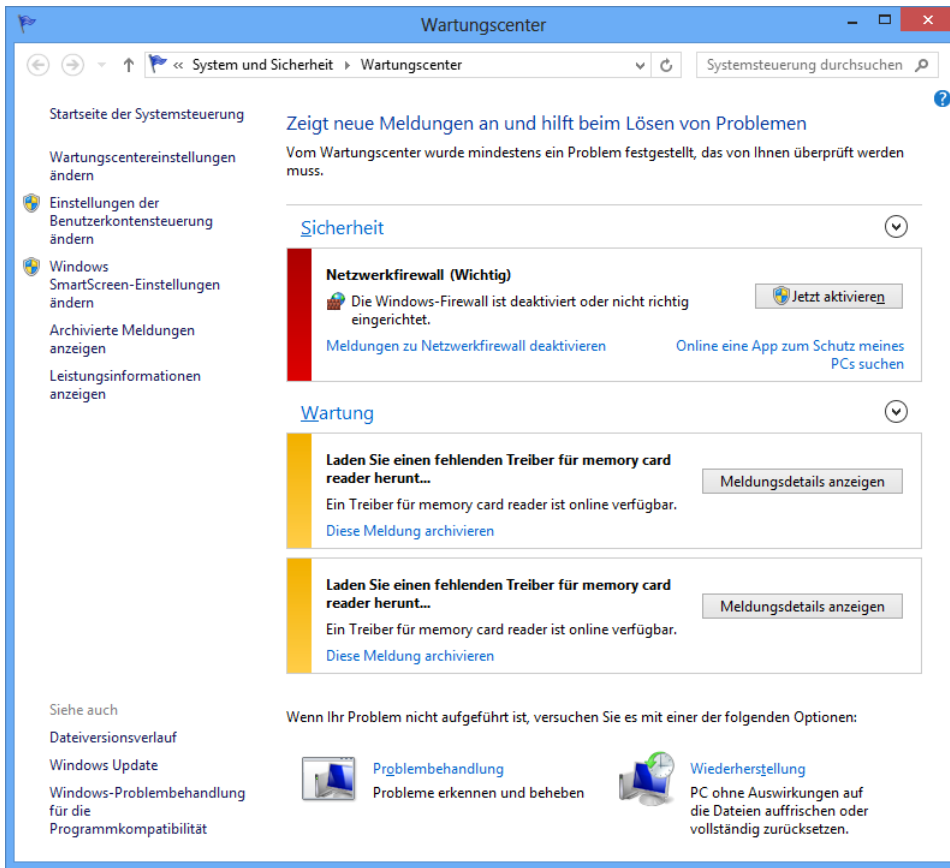


Abbildung 1.1 Das Wartungscenter

Verwenden von Windows 8 in Gruppen und Domänen

Computer, die unter Windows 8 laufen, können Mitglieder einer Heimnetzgruppe, einer Arbeitsgruppe oder einer Domäne sein. Eine Heimnetzgruppe ist eine lose zusammengefasste Gruppe von Computern in einem Heimnetzwerk. Die Computer in einer Heimnetzgruppe geben Daten frei, auf die mit einem Kennwort zugegriffen werden kann, das allen Benutzern der jeweiligen Heimnetzgruppe zugewiesen wurde. Sie legen das Kennwort der Heimnetzgruppe fest, wenn Sie die Heimnetzgruppe einrichten. Bei Bedarf können Sie es später jederzeit ändern.

Eine Arbeitsgruppe ist eine lockere Verbindung von Computern, die separat verwaltet werden. Eine Domäne ist eine Gruppe von Computern, die mithilfe von Domänencontrollern als Gruppe verwaltet werden. Domänencontroller sind Windows-Server, die den Zugang zum Netzwerk, zur Verzeichnisdatenbank und zu gemeinsamen Ressourcen verwalten und kontrollieren.

Heimnetzgruppen stehen nur zur Verfügung, wenn ein Windows 8-Computer mit einem Heimnetzwerk verbunden ist. Genauso sind Arbeitsgruppen und Domänen nur dann verfügbar, wenn der Windows 8-Computer mit einem Unternehmensnetzwerk verbunden ist. Wie Sie Netzwerke und Netzwerkverbindungen verwalten, erfahren Sie in Kapitel 15, »Konfigurieren und Problembehandlung von TCP/IP-Netzwerken«.

Bestimmte Funktionen von Windows 8 hängen davon ab, ob der Computer Mitglied einer Heimnetzgruppe, einer Arbeitsgruppe oder einer Domäne ist. Die folgenden Abschnitte beschreiben die Unterschiede, die sich für die Benutzerkontensteuerung, die Anmeldung, die schnelle Benutzerumschaltung und die Kennwortverwaltung ergeben.

Grundlagen der Benutzerkontensteuerung in Windows 8

Ist ein Windows 8-Computer Mitglied einer Heimnetz- oder Arbeitsgruppe, hat er nur lokale Konten. In einer Domäne dagegen verfügt ein Computer, auf dem Windows 8 ausgeführt wird, über lokale Konten und Domänenkonten. In Windows 8 gibt es zwei Haupttypen von lokalen Benutzerkonten:

- **Standard** Standardbenutzerkonten können den größten Teil der Software benutzen und Systemeinstellungen ändern, die sich nicht auf andere Benutzer oder auf die Sicherheit des Systems auswirken.
- **Administrator** Administratorkonten bieten vollständigen Zugriff auf den Computer und können alle benötigten Änderungen vornehmen.

Außerdem gibt es in Windows 8 einen speziellen lokalen Benutzerkontentyp, der *Microsoft-Konto* genannt wird und auf älteren Windows-Versionen nicht zur Verfügung steht. Microsoft-Konten kann man sich als synchronisierte lokale Konten vorstellen. Sie werden im Abschnitt »Grundlagen von Benutzer- und Gruppenkonten« von Kapitel 7, »Verwalten von Benutzerzugriff und Sicherheit«, ausführlicher beschrieben.

Windows 8 enthält zur Verbesserung der Sicherheit des Computers die *Benutzerkontensteuerung* (User Account Control, UAC), die dafür sorgt, dass es eine strenge Trennung zwischen Standardbenutzerkonten und Administratorkonten gibt. Wegen der Benutzerkontensteuerung werden alle Anwendungen in Windows 8 entweder mit Standardbenutzerrechten oder mit Administratorrechten ausgeführt. Wenn Sie sich als Standardbenutzer oder als Administrator anmelden, erhalten Sie eine Sicherheitsmeldung, sobald Sie eine Anwendung ausführen, die Administratorrechte erfordert. Wie die Sicherheitsmeldung erfolgt, hängt von den entsprechenden Gruppenrichtlinieneinstellungen ab (siehe den Abschnitt »Optimieren von Benutzerkontensteuerung und Administratorgenehmigungsmodus« in Kapitel 7) und davon, ob Sie sich mit einem Standardbenutzerkonto oder mit einem Administratorkonto angemeldet haben.

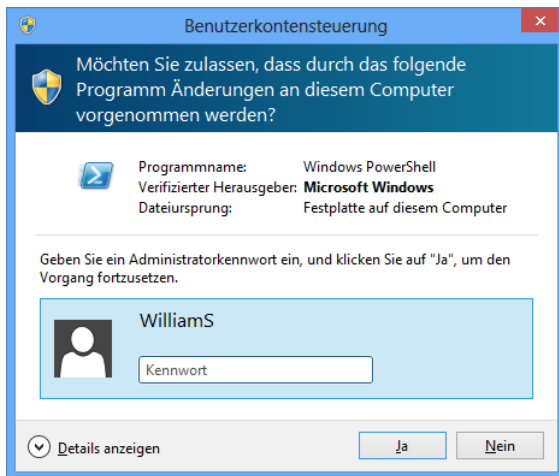


Abbildung 1.2 Anfordern von Administratorrechten

Wenn Sie mit einem Standardbenutzerkonto angemeldet sind, werden Sie aufgefordert, ein Kennwort für ein Administratorkonto anzugeben (Abbildung 1.2). In einer Heimnetzgruppe oder Arbeitsgruppe wer-

den die lokalen Administratorkonten mit Namen aufgeführt. Um fortzufahren, klicken Sie das Konto an, geben das dazugehörige Kennwort ein und tippen oder klicken auf *Ja*.

In einer Domäne listet das Dialogfeld *Benutzerkontensteuerung* keine Administratorkonten auf, daher können Sie nur fortfahren, wenn Sie Benutzername und Kennwort eines Administratorkontos in der Standarddomäne (der Anmeldedomäne) oder in einer vertrauenswürdigen Domäne kennen. Geben Sie auf die Aufforderung von Windows hin den Namen des Kontos sowie das zugehörige Kennwort ein und tippen oder klicken Sie auf *Ja*. Wenn das Konto zur Standarddomäne gehört, brauchen Sie den Namen der Domäne nicht anzugeben. Liegt das Konto dagegen in einer anderen Domäne, müssen Sie den Namen der Domäne und des Kontos im Format *Domäne\Benutzername* angeben, also beispielsweise *cpandl\williams*.

Wenn Sie sich mit einem Administratorkonto angemeldet haben, müssen Sie bestätigen, dass Sie fortfahren möchten (Abbildung 1.3). Sie können die Durchführung der betreffenden Aufgabe mit Klicken oder Tippen auf *Ja* erlauben oder mit *Nein* abbrechen. Nach dem Klicken oder Tippen auf *Details anzeigen* können Sie den Pfadnamen des Programms lesen, das ausgeführt werden soll.

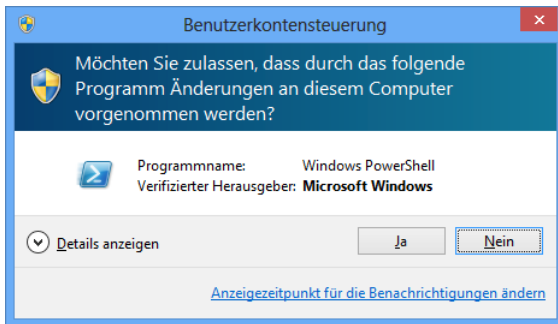


Abbildung 1.3 Nachfrage, ob eine Änderung durchgeführt werden darf

Die Erhöhung der Rechte ermöglicht die Ausführung einer Standardbenutzeranwendung mit Administratorrechten. Mit folgenden Schritten können Sie Anwendungen mit erhöhten Rechten ausführen:

1. Klicken Sie mit der rechten Maustaste auf die Kachel oder das Symbol der Anwendung, oder halten Sie es gedrückt, und wählen Sie dann *Als Admin ausführen*.
2. Wenn Sie die Meldung der Benutzerkontensteuerung zur Erhöhung der Rechte sehen, fahren Sie wie gewohnt fort und führen die Anwendung mit den erhöhten Rechten aus.

HINWEIS

Wenn Sie Verwaltungsaufgaben über die Befehlszeile ausführen wollen, müssen Sie die Eingabeaufforderung mit erhöhten Rechten ausführen. Ohne Erhöhung der Rechte erhalten Sie eine Fehlermeldung, sobald Sie ein Verwaltungsprogramm ausführen oder etwas tun, wofür Administratorrechte erforderlich sind.

Anmelden an Windows 8

Nach dem Start zeigt Windows 8 einen Sperrbildschirm an. Wenn Sie den Sperrbildschirm anklicken, erscheint der Willkommenbildschirm. Das Verhalten des Willkommenbildschirms hängt von den Gruppenrichtlinieneinstellungen und davon ab, ob der Computer zu einer Heimnetzgruppe, einer Arbeitsgruppe oder einer Domäne gehört.

Beachten Sie Folgendes:

- In einer Heimnetzgruppe oder Arbeitsgruppe zeigt der Willkommenbildschirm eine Liste der Konten an, die es auf dem Computer gibt. Wenn Sie sich mit einem dieser Konten anmelden möchten, tippen oder klicken Sie auf das Konto und geben bei Bedarf das dazugehörige Kennwort ein.
- In einer Domäne wird standardmäßig der Name des Benutzers auf dem Willkommenbildschirm angezeigt, der sich zuletzt angemeldet hat. Um sich mit diesem Konto anzumelden, geben Sie das erforderliche Kennwort ein. Sie können sich auch als ein anderer Benutzer anmelden. Dazu klicken Sie auf die Schaltfläche *Benutzer wechseln*, wählen eines der aufgeführten Konten aus und geben das dazugehörige Kennwort ein. Oder Sie klicken auf *Anderer Benutzer*, um den Namen und das Kennwort des zu benutzenden Kontos anzugeben. Die Schaltfläche *Benutzer wechseln* wird links neben dem Kontenbild als nach links gerichteter Pfeil in einem Kreis dargestellt.

Standardmäßig wird das letzte Konto, mit dem eine Anmeldung am Computer erfolgte, im Format *Computer\Benutzername* oder *Domäne\Benutzername* angezeigt. Zur Anmeldung mit diesem Konto geben Sie das Kennwort ein und tippen oder klicken auf die OK-Schaltfläche. Diese Schaltfläche ist Teil des Eingabefelds *Kennwort* und zeigt einen nach rechts gerichteten Pfeil. Zur Anmeldung mit einem anderen Konto tippen oder klicken Sie auf die Schaltfläche *Benutzer wechseln*, drücken gegebenenfalls STRG+ALT+ENTF und klicken dann auf *Anderer Benutzer*. Welche Informationen Sie zur Anmeldung eingeben müssen, hängt von der Art des Kontos ab, das Sie auswählen.

- Gehört das Konto zur aktuellen Domäne, geben Sie den Benutzernamen und das Kennwort ein und tippen oder klicken dann auf die Pfeilschaltfläche.
- Gehört das Konto zu einer anderen Domäne, müssen Sie den Domänennamen und den Kontonamen im Format *Domäne\Benutzername* angeben, wie beispielsweise *cpandl\williams*.
- Wenn Sie sich auf dem lokalen Computer anmelden möchten, geben Sie *.\<Benutzername>* ein, wobei *<Benutzername>* der Name des lokalen Kontos ist, wie beispielsweise *.\williams*.

Wenn Sie angemeldet sind, können Sie den Anmeldebildschirm mit der Tastenkombination STRG+ALT+ENTF anzeigen. Dieser Bildschirm ermöglicht eine Sperrung des Computers, das Wechseln des Benutzers, die Abmeldung, die Änderung des Kennworts oder den Aufruf des Task-Managers. Die Schaltfläche zum Herunterfahren befindet sich in der unteren rechten Ecke. Wenn Sie diese Schaltfläche antippen oder anklicken, erscheinen die Optionen *Energie sparen*, *Herunterfahren* und *Neu starten*. Da *Herunterfahren* und *Neu starten* auch Optionen des *Ein/Aus*-Schalters sind, können Sie einen Computer auch folgendermaßen herunterfahren oder neu starten:

1. Führen Sie eine Streifbewegung vom rechten Bildschirmrand durch oder drücken Sie die WINDOWS-Taste+C.
2. Tippen oder klicken Sie auf *Einstellungen* und tippen oder klicken Sie auf *Ein/Aus*.
3. Tippen oder klicken Sie nach Bedarf auf *Herunterfahren* oder *Neu starten*.

HINWEIS

Windows 8 unterstützt in Domänen, Heimnetzgruppen und Arbeitsgruppen die schnelle Benutzerumschaltung. Ist auf einem Windows 8-Computer bereits ein Benutzer angemeldet, können Sie mithilfe der schnellen Benutzerumschaltung einem anderen Benutzer die Anmeldung ermöglichen, ohne dass sich der aktuelle Benutzer abmelden muss. Zur Umschaltung der Benutzer drücken Sie STRG+ALT+ENTF und tippen oder klicken dann auf die Schaltfläche *Benutzer wechseln*.

Verwalten der Benutzerkontenkennwörter in Windows 8

Windows 8 bietet schnelle und einfache Wege zur Verwaltung von Benutzerkontenkennwörtern. Sie können auf einfache Weise folgende Aufgaben erledigen:

- Ändern des Kennworts des aktuellen Benutzers
- Ändern des Kennworts eines Kontos aus einer anderen Domäne oder eines Kontos auf dem lokalen Computer
- Erstellen einer Kennwörterücksetzdiskette
- Zurücksetzen des Kennworts eines Benutzers

Diese Aufgaben werden in den folgenden Abschnitten ausführlicher beschrieben.

Ändern des Kennworts des aktuellen Benutzers

Gehen Sie folgendermaßen vor, um das Kennwort des aktuellen Benutzers zu ändern:

1. Drücken Sie STRG+ALT+ENTF und klicken Sie dann auf die Option *Kennwort ändern*.

HINWEIS In einer Domäne wird der Name des Domänenkontos des aktuellen Benutzers im Format *Domäne\Benutzername* angezeigt. In einer Heimnetzgruppe oder Arbeitsgruppe wird der Name des lokalen Benutzerkontos des aktuellen Benutzers angezeigt.

2. Geben Sie im Textfeld *Altes Kennwort* das aktuelle Kennwort des Kontos ein.
3. Geben Sie im Textfeld *Neues Kennwort* das neue Kennwort für das Konto ein und bestätigen Sie es durch die erneute Eingabe im Textfeld *Kennwort bestätigen*.
4. Tippen oder klicken Sie auf die Pfeilschaltfläche, um die Änderung zu bestätigen.

Ändern der Kennwörter anderer Konten

Das Kennwort eines Domänenkontos oder eines lokalen Benutzerkontos, das nicht dem Konto des aktuellen Benutzers entspricht, können Sie mit folgenden Schritten ändern:

1. Drücken Sie STRG+ALT+ENTF und klicken Sie dann auf die Option *Kennwort ändern*.
2. Tippen oder klicken Sie in das Textfeld *Benutzername* und geben Sie dann den Namen des Kontos ein.

HINWEIS Für ein Domänenkonto geben Sie den Domänennamen und den Kontonamen im Format *Domäne\Benutzername* an, wie beispielsweise *cpandl\williams*. Für ein Konto auf dem lokalen Computer geben Sie *.\<Benutzername>* ein, wobei *<Benutzername>* der Name des lokalen Kontos ist, wie beispielsweise *.\williams*.

3. Geben Sie im Textfeld *Altes Kennwort* das aktuelle Kennwort des Kontos ein.
4. Geben Sie im Textfeld *Neues Kennwort* das neue Kennwort für das Konto ein und bestätigen Sie es durch die erneute Eingabe im Textfeld *Kennwort bestätigen*.
5. Tippen oder klicken Sie auf die Pfeilschaltfläche, um die Änderung zu bestätigen.

Erstellen und Verwenden einer Kennwörterücksetzdiskette

Kennwörter für Domänenbenutzer und lokale Benutzer werden unterschiedlich verwaltet. In Domänen verwalten Administratoren die Kennwörter von Domänenbenutzerkonten. Administratoren können vergessene Kennwörter in der Konsole *Active Directory-Benutzer und -Computer* zurücksetzen.

In Heimnetzgruppen und Arbeitsgruppen lassen sich Kennwörter für lokale Konten in einer sicheren, verschlüsselten Datei auf einer Kennwörterücksetzdiskette speichern, die auf einer Diskette oder einem USB-Speicherstick abgelegt wird. Gehen Sie folgendermaßen vor, um eine Kennwörterücksetzdiskette für den aktuellen Benutzer zu erstellen:

1. Drücken Sie STRG+ALT+ENTF und klicken Sie dann auf die Option *Kennwort ändern*.
2. Tippen oder klicken Sie auf *Kennwörterücksetzdiskette erstellen*, um den Assistenten für vergessene Kennwörter zu starten.
3. Lesen Sie im Assistenten für vergessene Kennwörter den Einführungstext und tippen oder klicken Sie auf *Weiter*.
4. Sie können Ihre verschlüsselte Kennwortdatei auf einer Diskette oder auf einem USB-Speicherstick ablegen. Wenn Sie eine Diskette verwenden wollen, müssen Sie eine leere, formatierte Diskette in Laufwerk A einlegen und dann in der Laufwerksliste den Eintrag *Diskettenlaufwerk (A:)* auswählen. Wollen Sie dagegen einen USB-Speicherstick verwenden, wählen Sie das gewünschte Gerät in der Laufwerksliste aus. Klicken Sie anschließend auf *Weiter*.
5. Geben Sie das aktuelle Kennwort für den angemeldeten Benutzer in das entsprechende Textfeld ein und tippen oder klicken Sie auf *Weiter*.
6. Warten Sie, bis der Assistent fertig ist, klicken Sie dann auf *Weiter*, entfernen Sie den Datenträger und tippen oder klicken Sie auf *Fertig stellen*.

Achten Sie darauf, dass Sie die Kennwörterücksetzdiskette an einem sicheren Ort lagern, denn jeder, der diese Diskette hat, kann sich Zugriff auf die Daten des betreffenden Benutzers verschaffen. Kann sich ein Benutzer nicht mehr anmelden, weil er sein Kennwort vergessen hat, können Sie mithilfe der Kennwörterücksetzdiskette ein neues Kennwort festlegen und sich mit dem neuen Kennwort am betreffenden Konto anmelden.

PRAXISTIPP

Mit BitLocker To Go können Sie USB-Speichersticks und andere Wechseldatenträger schützen und verschlüsseln. Ist ein Benutzer angemeldet, kann der geschützte Datenträger mit einem Kennwort oder mit einer Smartcard und der zugehörigen PIN entsperrt werden. Während kein Benutzer angemeldet ist, ist es aber nicht möglich, auf das geschützte Laufwerk zuzugreifen. Daher sollten Sie eine Kennwörterücksetzdiskette nicht mit BitLocker To Go schützen. Weitere Informationen finden Sie in Kapitel 11, »Arbeiten mit TPM und BitLocker-Laufwerkverschlüsselung«.

Rücksetzen des Kennworts eines Benutzers

Administratoren können vergessene Kennwörter in der Konsole *Active Directory-Benutzer und -Computer* zurücksetzen. In Heimnetzgruppen und Arbeitsgruppen können Sie ein Kennwort folgendermaßen zurücksetzen:

1. Tippen oder klicken Sie auf der Willkommenseite auf die Pfeilschaltfläche, ohne ein Kennwort anzugeben, und tippen oder klicken Sie dann auf *OK*. Nun sollte die Option *Kennwort zurücksetzen* angezeigt werden. Hat der Benutzer bereits ein falsches Kennwort angegeben, wird die Option *Kennwort zurücksetzen* möglicherweise schon angezeigt.
2. Legen Sie die Diskette ein oder stecken Sie den USB-Speicherstick an, auf dem die Kennwortwiederherstellungsdatei gespeichert ist, und tippen oder klicken Sie auf *Kennwort zurücksetzen*, um den Kennwörterücksetz-Assistenten zu starten.
3. Lesen Sie auf der ersten Seite des Kennwörterücksetz-Assistenten den Einführungstext und tippen oder klicken Sie auf *Weiter*.

4. Wählen Sie das Gerät, das Sie verwenden wollen, in der Laufwerksliste aus und tippen oder klicken Sie auf *Weiter*.
5. Geben Sie auf der Seite *Benutzerkontokennwort zurücksetzen* ein neues Kennwort für den Benutzer ein und bestätigen Sie es durch erneute Eingabe.
6. Geben Sie einen Kennworthinweis ein und tippen oder klicken Sie auf *Weiter*. Tippen oder klicken Sie auf *Fertig stellen*.

Energiesparpläne, Ruhezustände und Herunterfahren

In der Standardeinstellung verwendet ein Windows 8-Computer den Energiesparplan *Ausbalanciert*. Dieser Energiesparplan schaltet den Monitor aus und versetzt den Computer automatisch in den Standbymodus, wenn eine bestimmte, einstellbare Zeit lang keine Benutzeraktivität festgestellt wurde.

Beim Übergang in den Standbymodus speichert das Betriebssystem automatisch den Zustand des Computers, schaltet den Monitor aus und versetzt den Computer in den Standbymodus. Der Standbymodus ist ein Betriebsmodus mit geringem Stromverbrauch, bei dem der Zustand des Computers im Arbeitsspeicher erhalten bleibt und die Lüfter und Festplatten des Computers ausgeschaltet werden.

Da Windows 8 den Computerzustand vor dem Übergang in den Standbymodus speichert, brauchen Sie die Programme vor dem Wechsel in den Standbymodus nicht zu schließen. Weil der Computer im Standbymodus nur wenig Strom verbraucht, brauchen Sie sich auch keine Gedanken über Energieverschwendung zu machen.

TIPP Wie der Standbymodus im Detail funktioniert, hängt von der Art des Computers ab. Sie können viele mobile Computer ein- und ausschalten, indem Sie den Deckel öffnen oder schließen. Wenn Sie den Deckel schließen, geht der Laptop in den Standbymodus über, und sobald Sie den Deckel öffnen, wird der Laptop aus dem Standbymodus heraus wieder aktiviert. Falls die Spannung des Akkus unter eine kritische Grenze fällt oder sich der Computer über eine bestimmte Zeit hinaus im Standbymodus befindet, wird der Zustand des Computers auf der Festplatte gespeichert und der Computer vollständig heruntergefahren. Dieser letzte Zustand ähnelt dem Ruhezustand von älteren Windows-Versionen.

Um die Standardenergieoptionen anzuzeigen oder zu ändern, öffnen Sie zuerst die Systemsteuerung. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann unter *Energieoptionen* auf *Energiesparmodus ändern*. Wie in Abbildung 1.4 zu sehen, können Sie über die verfügbaren Optionen für den aktiven Energiesparplan einstellen, wann und wie weit der Bildschirm heruntergeregt oder ganz ausgeschaltet wird und wann der Computer in den Energiesparmodus versetzt wird. Tippen oder klicken Sie auf *Änderungen speichern*, damit Ihre Einstellungen angewendet werden. Auf Desktopcomputern können Sie nur einstellen, wann der Bildschirm ausgeschaltet und der Computer in den Energiesparmodus versetzt wird. Tippen oder klicken Sie auf *Änderungen speichern*, um Ihre Änderungen zu speichern.

Die meisten Computer können Sie direkt in den Standbymodus versetzen, indem Sie auf den Charm *Einstellungen* tippen oder klicken, dann auf *Ein/Aus* und schließlich auf *Energie sparen*. Sie wecken den Computer aus diesem Modus wieder auf, indem Sie auf den Touchscreen drücken und den Punkt gedrückt halten, die Maus bewegen oder irgendeine Taste auf der Tastatur drücken. Beachten Sie, dass manche Computer getrennte Schalter zum Ein-/Ausschalten und für die Energiespartaste haben. Welche Funktion diese Schalter haben, können Sie in den Energieoptionen einstellen.

Es gibt Umstände, die verhindern, dass ein Computer in den Standbymodus versetzt werden kann. Die Systemhardware, der Zustand und die Konfiguration können sich darauf auswirken, wie die Schalter für Ein/Aus und Standbymodus funktionieren. Manche Computerhardware unterstützt den Standbymodus

nicht. In diesem Fall kann der Computer nicht in den Standbymodus versetzt werden. Das ist auch der Fall, wenn Updates auf dem Computer installiert wurden, die einen Neustart erfordern, oder wenn Sie Programme installiert haben, die einen Neustart erfordern. Und wenn ein Administrator die Konfiguration der Energieoptionen auf dem Computer geändert und dabei die Funktion des Ein-/Ausschalters, der Energiespartaste oder beider Schalter anders zugewiesen hat, führt der Computer diese neuen Aktionen aus, statt den Computer wie in der Standardeinstellung auszuschalten oder in den Standbymodus zu versetzen.

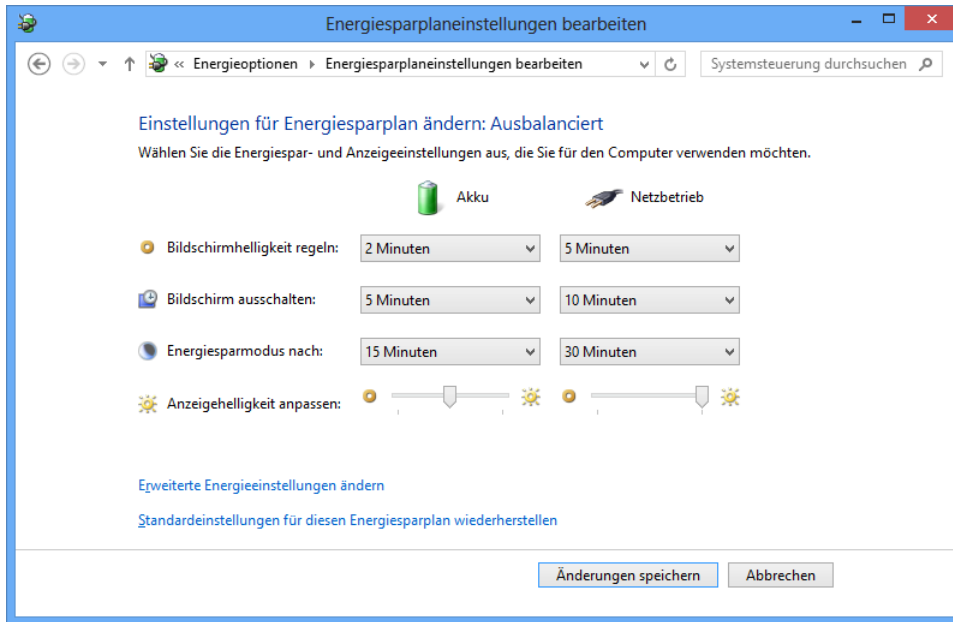


Abbildung 1.4 Konfigurieren der Energieoptionen

ACHTUNG Bei Arbeiten an einem Computer, der sich im Standbymodus befindet, dürfen Sie keinesfalls vergessen, dass immer noch Strom fließt. Sie dürfen niemals neue Hardware im Computer installieren oder Geräte an den Computer anschließen, während er sich im Standbymodus befindet. Um Fehler zu vermeiden, sollten Sie einen Windows 8-Computer grundsätzlich vom Stromnetz trennen, bevor Sie interne Geräte installieren. Externe Geräte sind die Ausnahme von der Regel. Sie können Geräte mit USB-, IEEE 1394- (FireWire) oder eSATA-Anschlüssen auch anschließen, ohne den Computer zuvor herunterzufahren und vom Stromnetz zu trennen.

Zur Änderung der Standardeinstellung für den Ein-/Ausschalter öffnen Sie die Systemsteuerung, tippen oder klicken dann auf *System und Sicherheit* und schließlich unter *Energieoptionen* auf *Netzschaltverhalten ändern*. Wie zuvor hängt es von der Art des Computers ab, welche Optionen verfügbar sind. Bei Mobilcomputern können Sie für die unterschiedliche Stromversorgung über Akku oder Stromnetz wahrscheinlich verschiedene Einstellungen vornehmen, mit denen Sie festlegen, was beim Druck auf den Ein-/Ausschalter oder auf die Energiespartaste oder beim Schließen des Deckels geschehen soll. Bei Bedarf können Sie auch auf *Einige Einstellungen sind momentan nicht verfügbar* klicken und folgendes tun:

- Wählen Sie *Kennwort ist erforderlich*, damit bei der Reaktivierung aus dem Energiesparmodus die Eingabe eines Kennworts verlangt wird.

- Wählen Sie *Schnellstart aktivieren*, damit beim Herunterfahren des Computers Systeminformationen in einer Datei auf dem Systemlaufwerk gespeichert werden. Beim nächsten Start wird diese Datei eingelesen, um den Startvorgang zu beschleunigen. Beim erneuten Starten eines laufenden Computers wird der Schnellstart nicht verwendet.
- Wählen Sie die Optionen aus, die im Energiemenü und im Menü des Profilsbilds angezeigt werden sollen.

Tippen oder klicken Sie auf *Änderungen speichern*, damit Ihre Einstellungen wirksam werden.

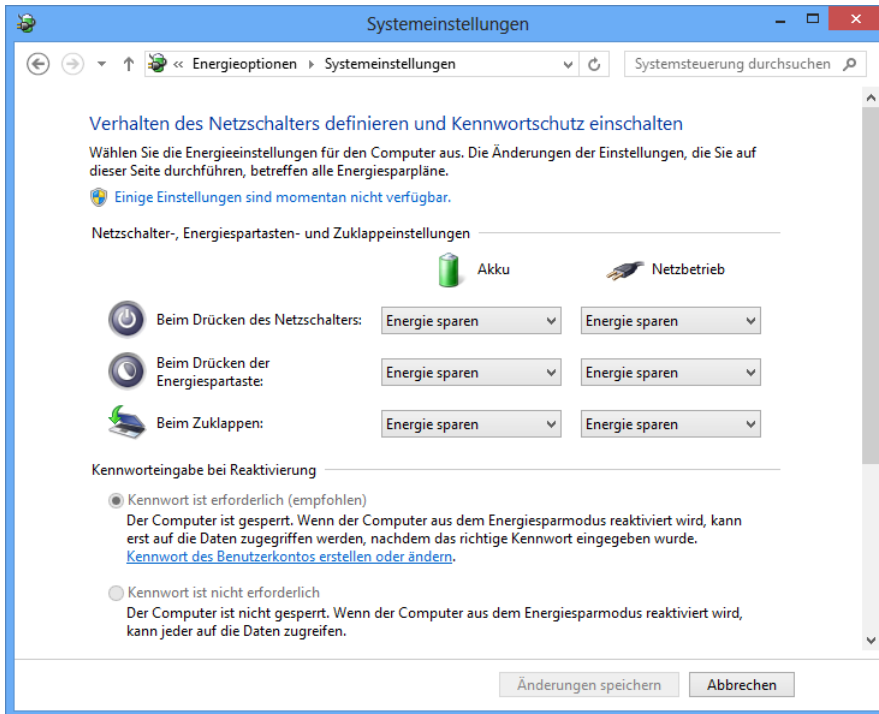


Abbildung 1.5 Konfigurieren der Optionen für Ein-/Ausschalter und Energiespartaste

Architektur von Windows 8

Wenn Sie wirklich wissen wollen, wie Windows 8 arbeitet und was unter der Haube vorgeht, müssen Sie sich genauer mit der internen Funktionsweise des Betriebssystems beschäftigen. Windows 8 startet nicht von einer Initialisierungsdatei, vielmehr benutzt es den Windows-Start-Manager, um das Betriebssystem zu initialisieren und zu starten.

Die Startumgebung (engl. boot environment) verändert den Ablauf des Betriebssystemstarts ganz gewaltig. Die Startumgebung wurde von Microsoft entwickelt, um mehrere lästige Probleme bezüglich der Startintegrität, der Betriebssystemintegrität und der Firmwareabstraktion zu lösen. Die Startumgebung wird noch vor dem Betriebssystem geladen, sie ist somit eine eigenständige Umgebung, die unabhängig vom Betriebssystem läuft. Daher kann die Startumgebung eingesetzt werden, um die Integrität des Startvorgangs und des Betriebssystems selbst zu überprüfen, bevor das Betriebssystem tatsächlich gestartet wird.

Die Startumgebung ist eine erweiterbare Abstraktionsschicht, die es dem Betriebssystem erlaubt, mit unterschiedlichen Arten von Firmwareschnittstellen zusammenzuarbeiten, ohne dass das Betriebssystem speziell auf die Zusammenarbeit mit diesen Firmwareschnittstellen abgestimmt sein muss. Statt jedes Mal, wenn eine neue Firmwareschnittstelle entwickelt wird, das Betriebssystem zu aktualisieren, verwenden die Entwickler einer Firmwareschnittstelle die Standardprogrammierschnittstellen der Startumgebung, um dem Betriebssystem die erforderliche Kommunikation mit den Firmwareschnittstellen zu ermöglichen.

Die Abstraktion der Firmwareschnittstelle ist die erste spezielle Zutat, die es Windows 8 ermöglicht, auf identische Weise mit BIOS- und EFI-basierten Computern zu arbeiten. Dies ist auch einer der Hauptgründe, warum Windows 8 Hardwareunabhängigkeit erreicht. Über die Startumgebung erfahren Sie in den Kapiteln 2 und 4 mehr.

Die nächste spezielle Zutat für die Hardwareunabhängigkeit ist WIM (Windows Imaging Format). Microsoft liefert Windows 8 auf Datenträgern mit Laufwerkabbildern aus, die im WIM-Format vorliegen. WIM setzt Komprimierung und SIS (Single Instance Storage) ein und erreicht dadurch eine erstaunliche Verringerung der Dateigröße. Die Komprimierung verringert die Größe des Abbilds in ähnlicher Weise wie Zip-Komprimierung bei Datendateien. Die Verwendung von SIS führt zu einer Verringerung der Abbildgröße, weil nur ein Exemplar einer Datei tatsächlich gespeichert wird, wenn sich mehrere Kopien der Datei im Laufwerkabbild befinden.

Die letzte spezielle Zutat für die Hardwareunabhängigkeit von Windows 8 ist die Modularisierung. Windows 8 nutzt einen modularen Komponentenentwurf, bei dem jede Komponente des Betriebssystems als separate, unabhängige Einheit (oder Modul) definiert ist. Weil Module wiederum andere Module enthalten können, lassen sich mehrere wichtige Features des Betriebssystems unabhängig von anderen wichtigen Features zusammenfassen und beschreiben. Und weil die Module voneinander unabhängig sind, können sie hinzugefügt oder entfernt werden, um die Betriebssystemumgebung anzupassen.

Windows 8 enthält eine umfangreiche Supportarchitektur. Den Kern dieser Architektur bildet die eingebaute Diagnose und Problembehandlung. Microsoft hat sie so entworfen, dass sie Probleme nach Möglichkeit selbst erkennt und beseitigt. Wo das nicht möglich ist, versucht sie zumindest, dem Benutzer bei der Diagnose der Probleme Hilfestellung zu bieten.

Windows 8 enthält Features für die Netzwerkauswertung und die Netzwerkerkennung. Die Netzwerkauswertung verfolgt Änderungen an der Netzwerkkonfiguration und der Konnektivität. Die Netzwerkerkennung steuert die Fähigkeit eines Computers, andere Computer und Geräte in einem Netzwerk zu erkennen.

Dank der Netzwerkauswertung ist Windows 8 in der Lage, die aktuelle Netzwerkkonfiguration und den Konnektivitätsstatus zu ermitteln. Das ist wichtig, weil viele Netzwerk- und Sicherheitseinstellungen davon abhängen, mit welcher Art Netzwerk der Windows 8-Computer verbunden ist. Windows 8 verwaltet separate Netzwerkkonfigurationen für Domänennetze, private Netze und öffentliche Netze. Es erkennt folgende Ereignisse:

- Wenn Sie eine Netzwerkverbindung ändern
- Ob der Computer Verbindung zum Internet hat
- Ob der Computer über das Internet eine Verbindung zum Unternehmensnetzwerk herstellen kann

In Windows 8 unterstützt die Windows-Firewall Verbindungen mit mehreren Netzwerken gleichzeitig sowie mehrere aktive Firewallprofile. Deshalb hängt das für eine Verbindung aktive Firewallprofil von der Art der Verbindung ab.

Wenn Sie einen Computer von einem Netzwerk-Switch oder -Hub trennen und an einen anderen Netzwerk-Switch oder -Hub anschließen, nimmt der Computer unter Umständen an, dass er nun mit einem

anderen Netzwerk verbunden ist. Abhängig von der Konfiguration der Gruppenrichtlinien führt das möglicherweise dazu, dass der Computer in einen besonders geschützten Modus schaltet, in dem zusätzliche Netzwerksicherheitseinstellungen angewendet werden. Wie in Abbildung 1.6 gezeigt, können Sie sich den Status der Netzwerkverbindungen im Netzwerk- und Freigabecenter ansehen. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Netzwerkstatus und -aufgaben anzeigen*, um diese Verwaltungskonsolle zu öffnen.



Abbildung 1.6 Ermitteln des Netzwerkstatus

TIPP Mithilfe eines Features namens DirectAccess können Windows 8-Computer jetzt unabhängig vom eigenen Standort direkt auf Unternehmensnetzwerke zugreifen, solange sie Zugriff auf das Internet haben. Erfreuliche Nachricht für Benutzer: Sie brauchen dazu keine VPN-Verbindung mehr zu öffnen. Das Feature greift auf DirectAccess-Server zurück, die im Unternehmensnetzwerk konfiguriert werden; außerdem muss DirectAccess in den Gruppenrichtlinien aktiviert sein. Weitere Informationen finden Sie in Kapitel 16, »Verwalten von mobilen Netzwerken und Remotezugriff«.

Windows 8 verfolgt den Identifizierungsstatus aller Netzwerke, mit denen der Computer verbunden ist. Während Windows 8 ein Netzwerk analysiert, zeigt das Netzwerk- und Freigabecenter als Status *Netzwerkidentifizierung* an. Das ist ein temporärer Status für ein Netzwerk, das gerade identifiziert wird. Sobald Windows 8 ein Netzwerk identifiziert, wird es zu einem identifizierten Netzwerk und unter seinem Netzwerk- oder Domännennamen im Netzwerk- und Freigabecenter aufgelistet.

Gelingt es Windows 8 nicht, das Netzwerk zu identifizieren, wird es unter dem Status *Nicht identifiziertes Netzwerk* im Netzwerk- und Freigabecenter angezeigt. In den Gruppenrichtlinien können Sie für jeden Netzwerkstatus und für alle Netzwerke den Standardstandorttyp und die Benutzerberechtigungen festlegen; öffnen Sie dazu die Richtlinien für die Computerkonfiguration unter *Windows-Einstellungen\Sicherheitseinstellungen\Netzwerklisten-Manager-Richtlinien*.

Wenn Sie im Netzwerk- und Freigabecenter arbeiten, können Sie versuchen, mit der Windows-Netzwerkdiagnose, einer weiteren Schlüsselkomponente innerhalb des Diagnose- und Problembehandlungsframeworks, einen Warnungsstatus zu diagnostizieren. Zur Durchführung der Diagnose tippen oder klicken Sie auf *Probleme beheben*, dann auf *Internetverbindungen* und schließlich auf *Weiter*. Die Windows-Netzwerkdiagnose versucht daraufhin, das Netzwerkproblem zu identifizieren und eine mögliche Lösung anzubieten.

Die Diagnose- und Problembehandlungsinfrastruktur von Windows 8 bietet verbesserte Diagnoseanleitungen, zusätzliche Fehlerberichterstattungsdetails, erweiterte Ereignisprotokollierung und umfangreiche Wiederherstellungsrichtlinien. Ältere Windows-Versionen enthalten zwar bereits einige Hilfe- und Diagnosefeatures, aber diese Features ermöglichen größtenteils keine automatische Reparatur oder Diagnose. Windows kann nun viele Arten von Hardware-, Arbeitsspeicher- und Leistungsproblemen erkennen und automatisch beseitigen oder den Benutzer durch den Problembehandlungsprozess führen. Weitere Informationen finden Sie im Abschnitt »Arbeiten mit dem automatischen Hilfesystem« von Kapitel 9, »Verwalten von Hardwaregeräten und Treibern«.

Auch die Fehlererkennung für Geräte und Festplattenlaufwerke wurde automatisiert. Treten bei einem Gerät Probleme auf, erkennt die Hardwarediagnose die Fehlerbedingungen und repariert das Problem entweder automatisch oder leitet den Benutzer durch den Wiederherstellungsvorgang. Bei Festplattenlaufwerken kann die Hardwarediagnose mithilfe von Fehlerberichten, die von den Festplattenlaufwerken bereitgestellt werden, potenzielle Defekte erkennen und Sie vorbeugend warnen. Die Hardwarediagnose leitet Sie auch durch den Datensicherungsprozess, wenn sie meldet, dass eine Festplatte möglicherweise bald ausfällt.

Windows 8 kann Leistungsprobleme automatisch erkennen. Dazu gehören langsamer Anwendungsstart, langsamer Systemstart, langsames Schalten in den Ruhezustand beziehungsweise Aufwachen aus dem Ruhezustand sowie langsames Herunterfahren. Zeigt ein Computer schlechte Leistung, kann die Windows-Diagnose das Problem erkennen und mögliche Lösungen vorschlagen. Bei komplexeren Leistungsproblemen können Sie die relevanten Leistungs- und Zuverlässigkeitsdaten in der Konsole *Leistungsüberwachung* verfolgen, die zu den Verwaltungsprogrammen gehört.

Windows 8 kann auch Probleme erkennen, die durch Speicherlecks und RAM-Defekte ausgelöst werden. Wenn Sie vermuten, dass bei einem Computer ein Problem mit dem RAM vorliegt, das nicht automatisch erkannt wird, können Sie die Windows-Speicherdiagnose folgendermaßen von Hand starten:

1. Geben Sie im *Start*-Bildschirm **mdsched.exe** ein und drücken Sie die EINGABETASTE. Der Text, den Sie in *Start* eingeben, wird normalerweise automatisch in das Suchfeld *Apps* übertragen.
2. Wählen Sie aus, ob Sie den Computer neu starten und das Tool sofort ausführen oder das Tool erst beim nächsten planmäßigen Start ausführen wollen (Abbildung 1.7).

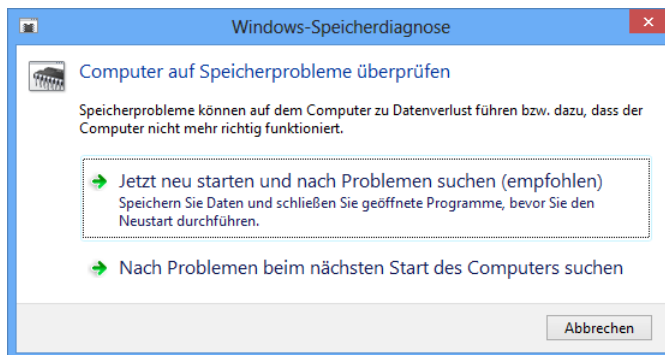


Abbildung 1.7 Überprüfen auf Speicherprobleme

3. Die Windows-Speicherdiagnose läuft automatisch, sobald der Computer neu gestartet wird, und führt dabei einen Standardtest des Arbeitsspeichers aus. Sie können weniger oder mehr Tests ausführen, indem Sie die Taste F1 drücken, mit den Pfeiltasten die Testmischung *Minimal*, *Standard* oder

Erweitert auswählen und schließlich F10 drücken, um die gewünschten Einstellungen anzuwenden und den Test fortzusetzen.

4. Sobald der Test abgeschlossen ist, startet der Computer neu. Sie bekommen die Testergebnisse angezeigt, wenn Sie sich anmelden.

Wenn ein Computer aufgrund von defektem Arbeitsspeicher abstürzt und die Speicherdiagnose das erkennt, werden Sie aufgefordert, einen Arbeitsspeichertest durchzuführen, sobald der Computer das nächste Mal gestartet wird.

Kapitel 2

Konfigurieren von Windows 8-Computern

In diesem Kapitel:

Support für Windows 8-Computer	60
Verwenden von Systemprogrammen	72
Verwalten der Systemeigenschaften	82
Konfigurieren der Energieverwaltung	97

Eine Ihrer Hauptaufgaben als Administrator ist die Verwaltung der Betriebssystemkonfiguration. Windows 8 weist viele einzigartige Eigenschaften auf, darunter folgende:

- Windows 8 hat eine modulare Architektur, und seine Binärdateien werden in Form von Laufwerkabbildern ausgeliefert, die im Windows-Abbilddateiformat (Windows Imaging, WIM) vorliegen. Daher können Sie das Tool zur Abbildverwaltung für die Bereitstellung (Deployment Image Servicing and Management, DISM) benutzen, um Pakete, Treiber, Features und Regionsschemaeinstellungen in Windows-Abbilddateien (.wim) oder Dateien für virtuelle Festplatten (.vhd) zu verwalten. Die Datenträgerverwaltung und DiskPart wurden so aktualisiert, dass sie mit .vhd-Dateien umgehen können.
- Eine Vorstartumgebung, in der der Windows-Start-Manager eingesetzt wird, um den Systemstart zu steuern und die ausgewählte Startanwendung zu laden. Windows 8 benutzt im Gegensatz zu älteren Windows-Versionen also nicht mehr *Ntldr* und *Boot.ini*, um das Betriebssystem zu laden. Außerdem gibt es zusätzliche Startoptionen. Zum Beispiel können Sie auf einem Computer ein Betriebssystem starten, das sich in einer .vhd-Datei befindet. Dazu können Sie beispielsweise ein einfaches Startabbild erstellen, das die benötigte .vhd-Datei mit Xcopy beim Systemstart auf das angegebene Laufwerk kopiert.
- Ein Kontrollprogramm für Benutzerrechte und Zugriffssteuerung, die Benutzerkontensteuerung (User Account Control, UAC), legt fest, welche Prozesse ausgeführt werden dürfen und wie Anwendungen mit dem Betriebssystem zusammenarbeiten. Deswegen geht Windows 8 anders mit Benutzerprivilegien und Zugriffssteuerung um als ältere Windows-Versionen. Wie Sie in Kapitel 7, »Verwalten von Benutzerzugriff und Sicherheit«, erfahren, können Sie die UAC-Eingabeaufforderungen anpassen oder ausschalten, aber auch dann bleiben andere UAC-Features aktiv, etwa die Anwendungsvirtualisierung.

Außerdem müssen Sie die Tools und Optionen kennen, die Sie für die Konfiguration von Windows 8 brauchen. Um dieses Thema geht es in diesem Kapitel. Viele der benötigten Tools befinden sich auf dem Anwendungsbildschirm *Apps*, der mit der Tastenkombination WINDOWS-Taste+Q leicht zu erreichen ist. Wenn Sie mit einem Touchscreen arbeiten, führen Sie eine Streifbewegung vom rechten Bildschirmrand durch und tippen dann auf *Suche*, um den Anwendungsbildschirm anzuzeigen (die *Apps*-Suche ist normalerweise die Standardeinstellung). Wenn Sie meinen Rat aus Kapitel 1, »Einführung to Windows 8 Administration« befolgt haben, haben Sie die wichtigsten Tools für die tägliche Arbeit vielleicht schon auf *Start* oder auf der Taskleiste des Desktops angeheftet, um sie schnell erreichen zu können.

Support für Windows 8-Computer

Um erfolgreich einen Computer verwalten, Fehler beheben und Probleme lösen zu können, müssen Sie wissen, wie der Computer konfiguriert ist. Zu den Hilfsprogrammen, mit denen Sie die Konfiguration eines Computers ermitteln können, gehören:

- **Computerverwaltung** Bietet Zugang zu wichtigen Tools für die System-, Dienst- und Datenträgerverwaltung.
- **Leistungsüberwachung** Hier überwachen Sie die Systemleistung und stellen fest, ob Leistungsprobleme auftreten.
- **Ressourcenmonitor** Zeigt detaillierte Auslastungsinformationen zu Systemressourcen wie Prozessoren, Arbeitsspeicher, Datenträgern und Netzwerk an. Verwenden Sie den Ressourcenmonitor, wenn Sie genauere Daten brauchen, als der Task-Manager liefert.

- **System** Zeigt Basisinformationen über einen Computer an und verwaltet wichtige Systemeigenschaften.
- **Systeminformationen** Zeigt ausführliche Informationen über die Konfiguration des Systems und die Verfügbarkeit der Ressourcen an. Sie können die Systeminformationen auch zur Problembehebung verwenden.
- **Task-Manager** Zeigt Auslastungsinformationen zu Systemressourcen an.

In diesem Abschnitt beschreibe ich, wie Sie mit diesen Tools effizient arbeiten. Zuerst sollten Sie die Verwaltungsprogramme zum Startbildschirm hinzufügen. Auf der Seite *Start* wählen Sie dazu eine der folgenden Methoden:

- Auf einem Touchscreen führen Sie eine Streifbewegung vom rechten Bildschirmrand durch, tippen auf *Einstellungen*, dann auf *Kacheln* und schließlich auf *Verwaltungstools anzeigen*.
- Bewegen Sie auf einem herkömmlichen Computer den Mauszeiger auf die verborgene Schaltfläche in der unteren rechten Ecke des Bildschirms, um die Charmsleiste anzuzeigen. Klicken Sie auf der Charmsleiste auf *Einstellungen*, dann auf *Kacheln* und schließlich auf *Verwaltungstools anzeigen*.

Ein Tippen oder Klicken auf den Schalter unter *Verwaltungstools anzeigen* führt zur Umschaltung zwischen *Ja* und *Nein*. Das bedeutet, dass die Tools entweder angezeigt werden oder nicht. Wenn Sie *Start* das nächste Mal öffnen, sind die Tools entweder zu sehen oder nicht, je nach der Einstellung.

Start und *Desktop* verfügen über ein praktisches Menü, das Sie öffnen können, indem Sie in die untere linke Ecke des *Start*- oder *Desktop*-Bildschirms tippen und diese Stelle gedrückt halten, oder indem Sie diese Ecke mit der rechten Maustaste anklicken. Nützlich auf Computern mit Maus und Tastatur, eine echte Erleichterung auf Computern mit Touchscreen. In diesem Kontextmenü gibt es Optionen für die Systemsteuerung, die Computerverwaltung, Energieoptionen, Suchen, System, Task-Manager, Explorer und so weiter.

WEITERE INFORMATIONEN

Auf *Start* zeigt die verborgene Schaltfläche in der unteren linken Ecke eine Miniaturansicht des Desktops, wenn sie aktiviert wird, und ein Tippen oder Klicken auf die Miniaturansicht öffnet den Desktop. Auf *Desktop* zeigt die verborgene Schaltfläche in der unteren linken Ecke eine Miniaturansicht von *Start*, wenn sie aktiviert wird, und ein Tippen oder Klicken auf die Miniaturansicht öffnet *Start*. Wenn Sie diese Miniaturansicht gedrückt halten oder mit der rechten Maustaste anklicken, öffnet sich das Kontextmenü.

Arbeiten mit der Konsole *Computerverwaltung*

Die Konsole *Computerverwaltung* dient zur Durchführung von wichtigen Verwaltungsarbeiten auf dem lokalen Computer oder auf einem Remotesystem. Wenn Sie die Verwaltungstools zu *Start* hinzugefügt haben, können Sie die Konsole *Computerverwaltung* starten, indem Sie auf die entsprechende Kachel tippen oder klicken. Sie können die Konsole *Computerverwaltung* auch starten, indem Sie im Suchfeld *Apps compmgmt.msc* eingeben und die EINGABETASTE drücken.

Wie Abbildung 2.1 zeigt, besteht das Hauptfenster aus mehreren Anzeigebereichen, ähnlich dem Datei-Explorer. Mit der Konsolenstruktur im linken Anzeigebereich können Sie navigieren und das gewünschte Tool herausuchen. Das Aktionsfeld auf der rechten Seite ähnelt dem Kontextmenü, das angezeigt wird, wenn Sie ein Objekt mit der rechten Maustaste anklicken oder es antippen und gedrückt halten. Um das Aktionsfeld zu öffnen oder zu schließen, tippen oder klicken Sie auf der Symbolleiste der Konsole auf die Schaltfläche *Aktionsbereich ein-/ausblenden*. Die Tools sind in drei Hauptkategorien aufgeteilt:

- **System** Allgemeine Tools zur Systemverwaltung und zur Anzeige von Informationen über das System
- **Datenspeicher** Tools zur Verwaltung der Datenträger
- **Dienste und Anwendungen** Tools zum Anzeigen und Verwalten von Eigenschaften der Dienste und Anwendungen, die auf dem Computer installiert sind

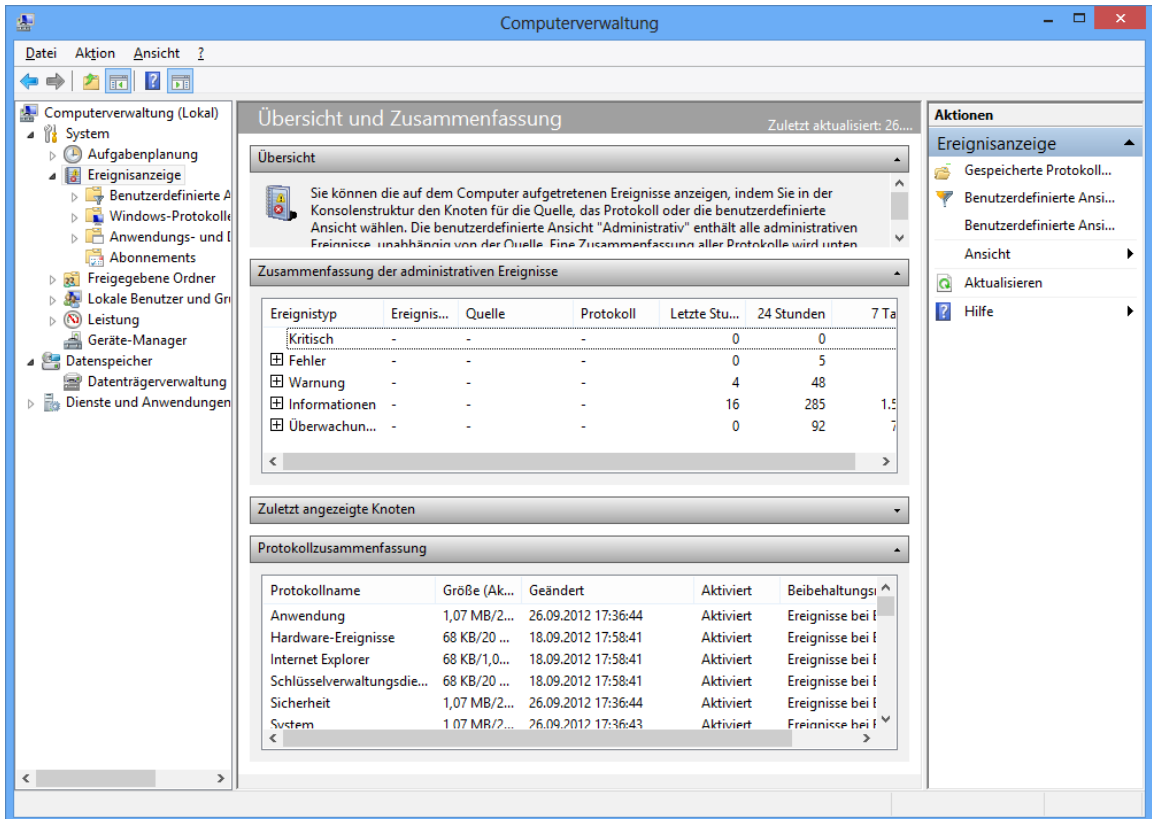


Abbildung 2.1 Mit der Konsole *Computerverwaltung* können Sie Computer und Ressourcen verwalten

In diesen Kategorien sind folgende Tools verfügbar:

- **Aufgabenplanung** Anzeige und Verwaltung geplanter Aufgaben. Geplante Aufgaben dienen zur Automatisierung von Prozessen, beispielsweise zur Bereinigung oder Überprüfung von Datenträgern. Geplante Aufgaben und Automation werden in Kapitel 10, »Erledigen von Wartungs- und Supportaufgaben«, besprochen.
- **Ereignisanzeige** Anzeige der Ereignisprotokolle des ausgewählten Computers. Ereignisprotokolle zeichnen wichtige Ereignisse auf, die auf dem Computer eingetreten sind, und können zur Überprüfung verwendet werden, ob der betreffende Computer Konfigurations- oder sonstige Probleme hat. Ereignisse und Ereignisprotokolle werden in Kapitel 10 beschrieben.
- **Freigegebene Ordner** Anzeigen und Verwalten freigegebener Ordner sowie der zugehörigen Sitzungen und offenen Dateien. Freigegebene Ordner werden in Kapitel 13, »Verwalten der Dateisicherheit und Ressourcenfreigabe«, genauer beschrieben.

- **Lokale Benutzer und Gruppen** Verwaltung lokaler Benutzer und lokaler Benutzergruppen auf dem ausgewählten Computer. Auf jedem Clientcomputer gibt es lokale Benutzer und lokale Benutzergruppen, nicht zu verwechseln mit Domänenbenutzern und Domänengruppen. Die Arbeit mit lokalen Benutzern und Gruppen wird in Kapitel 7 beschrieben.
- **Leistung** Tools zur Überwachung und Berichterstattung, mit denen Sie die aktuelle Leistung eines Computers und die Leistungsentwicklung über einen längeren Zeitraum hinweg verfolgen können.
- **Geräte-Manager** Dient als zentraler Ort für die Überprüfung der Zustände aller Geräte, die in einem Computer installiert sind, und zur Aktualisierung der dazugehörigen Gerätetreiber. Sie können den Geräte-Manager auch zur Behebung von Geräteproblemen verwenden. Die Verwaltung von Geräten wird in Kapitel 9, »Verwalten von Hardwaregeräten und Treibern«, besprochen.
- **Datenträgerverwaltung** Verwaltung von Festplatten, Laufwerkspartitionen und Volumes. Windows 8 unterstützt laufwerksübergreifende Volumes, Stripes (Datenstreifen), Stripes mit Parität und die Spiegelung von Laufwerken. Laufwerksübergreifende Volumes sind nicht auf ein Festplattenlaufwerk beschränkt, sondern können sich über mehrere Laufwerke erstrecken. Durch die Aufteilung von Volumes in Stripes können Sie Datenstripes auf mehrere Laufwerke verteilen, damit sich im Durchschnitt ein schnellerer Datenzugriff ergibt. Allerdings bietet keine dieser Methoden einen zusätzlichen Schutz vor Fehlern. Wenn also eine der Festplatten ausfällt, die Teil eines übergreifenden oder in Stripes aufgeteilten Volumes ist, fällt das ganze Volume aus.
- **Dienste** Anzeige und Verwaltung der Systemdienste, die auf einem Computer vorhanden sind. In Windows 8 hat jeder Dienst eine Wiederherstellungsrichtlinie. Fällt ein Dienst aus, versucht Windows 8 automatisch, den Dienst neu zu starten. Es berücksichtigt dabei automatisch die Abhängigkeiten zwischen Diensten und auch anderen Komponenten. Alle erforderlichen Dienste und Systemkomponenten werden gestartet, bevor der Versuch unternommen wird, einen nicht erfolgreich gestarteten Dienst erneut zu starten. Die Arbeit mit Diensten wird in Kapitel 9 besprochen.
- **WMI-Steuerung** Anzeige und Verwaltung der Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI). WMI erfasst Systeminformationen, überwacht den Zustand des Systems und verwaltet Systemkomponenten. Weitere Informationen finden Sie weiter unten in diesem Kapitel im Abschnitt »Arbeiten mit der WMI-Steuerung«.

In der Computerverwaltung können Sie mit folgenden Schritten auch einen Remotecomputer auswählen und verwalten:

1. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Knoten *Computerverwaltung*, oder halten Sie den Knoten gedrückt, und wählen Sie dann *Verbindung mit anderem Computer herstellen*. Dadurch öffnet sich das Dialogfeld *Computer auswählen*.
2. Wählen Sie *Anderen Computer* und geben Sie dann den vollqualifizierten Namen des Computers ein, mit dem Sie arbeiten möchten, beispielsweise *cspc85.microsoft.com*, wobei *cspc85* der Name des Computers und *microsoft.com* der Name der Domäne ist. Oder Sie tippen oder klicken auf *Durchsuchen*, um den Computer auszuwählen, mit dem Sie arbeiten möchten.
3. Tippen oder klicken Sie auf *OK*.

Wenn Sie die Remoteverwaltung von Windows 8-Computern mit dem WS-Verwaltungsprotokoll ermöglichen möchten, geben Sie in einer Eingabeaufforderung mit erhöhten Rechten **WinRM quickconfig** ein. Geben Sie bei jeder Bestätigungsaufforderung *y* ein. Dadurch wird der Windows-Remoteverwaltungsdienst (WinRM) gestartet und so konfiguriert, dass er WSM-Verwaltungsanfragen auf jeder IP-Adresse annimmt. Außerdem wird eine Windows-Firewallausnahme für die Windows-Remoteverwaltung erstellt und *LocalAccountTokenFilterPolicy* so konfiguriert, dass für die Remoteverwaltung die entsprechenden Administratorrechte gewährt werden.

Andere Arten von Remoteverwaltungszugriffen hängen von anderen Ausnahmen in Windows-Firewall ab. Merken Sie sich Folgendes:

- **Remotedesktop** wird getrennt von der Remoteverwaltung aktiviert oder deaktiviert. Wenn jemand mit Remotedesktop eine Verbindung zum lokalen Server herstellen soll, müssen Sie ihm die entsprechenden Verbindungen zum Computer erlauben und den Zugriff konfigurieren, wie in Kapitel 16, »Verwalten von mobilen Netzwerken und Remotezugriff«, besprochen.
- Die Remote-Ereignisprotokollverwaltung muss in Windows-Firewall als zulässige Anwendung konfiguriert werden, damit sich die Ereignisprotokolle eines Computers remote verwalten lassen. In der Windows-Firewall mit erweiterter Sicherheit gibt es einige entsprechende Regeln, die eine Verwaltung über benannte Pipes (Named Pipes, NP) und Remoteprozeduraufrufe (Remote Procedure Call, RPC) ermöglichen.
- Die Remoteverwaltung geplanter Aufgaben muss in Windows-Firewall als zulässige Anwendung konfiguriert werden, damit sich die geplanten Aufgaben eines Computers remote verwalten lassen. In der Windows-Firewall mit erweiterter Sicherheit gibt es einige entsprechende Regeln, die eine Verwaltung über RPC ermöglichen.
- Die Remotedienstverwaltung muss in Windows-Firewall als zulässige Anwendung konfiguriert werden, damit sich die Dienste eines Computers remote verwalten lassen. In der Windows-Firewall mit erweiterter Sicherheit gibt es einige entsprechende Regeln, die eine Verwaltung über NP und RPC ermöglichen.
- Die Remotevolumeverwaltung muss in Windows-Firewall als zulässige Anwendung konfiguriert werden, damit sich die Volumes eines Computers remote verwalten lassen. In der Windows-Firewall mit erweiterter Sicherheit gibt es einige Regeln, die eine Verwaltung des Dienstes für virtuelle Datenträger und des Ladeprogramms des Dienstes für virtuelle Datenträger ermöglichen.

Ermitteln von Grunddaten über System und Leistung

Mit der Konsole *System* können Sie Systemeigenschaften anzeigen und verwalten. Zugang zu dieser Konsole erhalten Sie, indem Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System* tippen oder klicken. Wie Abbildung 2.2 zeigt, ist die Konsole *System* in vier Bereiche aufgeteilt, die Links zur Durchführung häufiger durchzuführender Arbeiten enthalten und eine Übersicht über das System bieten. Diese Bereiche sind:

- **Windows-Edition** Zeigt Edition und Version des Betriebssystems.
- **System** Nennt den Prozessor, den Arbeitsspeicher, die Leistungseinstufung und die Art des installierten Betriebssystems. Der Typ des Betriebssystems wird als 32- oder 64-Bit-Betriebssystem angegeben.
- **Einstellungen für Computernamen, Domäne und Arbeitsgruppe** Zeigt den Computernamen, eine Beschreibung sowie die Domäne, Heimnetzgruppe oder Arbeitsgruppe. Wenn Sie diese Angaben ändern möchten, tippen oder klicken Sie auf *Einstellungen ändern* und dann im Dialogfeld *Systemeigenschaften* auf die Schaltfläche *Netzwerk-ID* oder *Ändern*.
- **Windows-Aktivierung** Zeigt, ob Sie den Product Key eingegeben und das Betriebssystem bereits aktiviert haben. Falls Windows 8 noch nicht aktiviert wurde, können Sie auf den angezeigten Link tippen oder klicken und die Aktivierung durchführen. Folgen Sie einfach den Anweisungen.

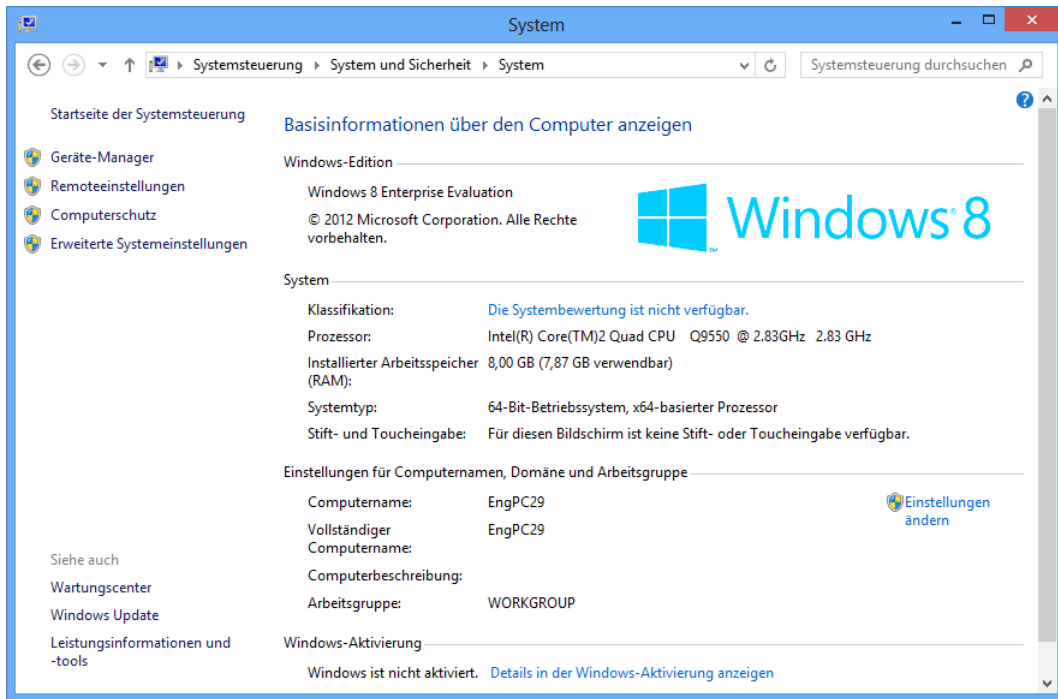


Abbildung 2.2 Systemeigenschaften können Sie in der *System*-Konsole anzeigen und verwalten

Auf der linken Seite der *System*-Konsole werden wichtige Supporttools aufgelistet, auf die Sie rasch zugreifen können:

- *Geräte-Manager*
- *Remoteeinstellungen*
- *Computerschutz*
- *Erweiterte Systemeinstellungen*

Ein Klick auf *Einstellungen ändern* unter *Einstellungen für Computernamen, Domäne und Arbeitsgruppe* öffnet das Dialogfeld *Systemeigenschaften*. Wie sich die Computerkonfiguration mithilfe der *Systemeigenschaften* einstellen lässt, wird weiter unten in diesem Kapitel im Abschnitt »Verwalten der Systemeigenschaften« besprochen.

Die Bewertung eines Computers mit dem Windows-Leistungsindex ist ein wichtiger Anhaltspunkt für die Einschätzung, welche Systemfunktionen er in akzeptabler Geschwindigkeit und Qualität ausführen kann. In den meisten Fällen bewertet das Windows-Setupprogramm die Leistung eines Computers, sobald die Installation abgeschlossen ist. Sie erhalten ausführlichere Informationen über die Bewertung eines Computers, indem Sie unter *System* auf den Link *Windows-Leistungsindex* tippen oder klicken, um *Leistungsinformationen und -tools* zu öffnen (Abbildung 2.3).

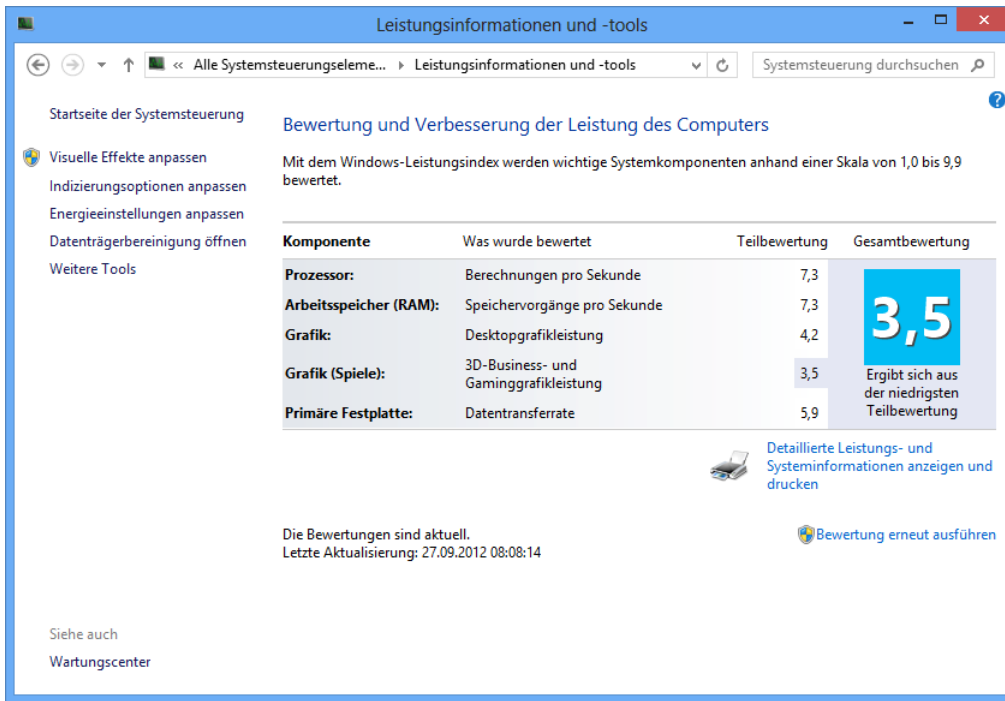


Abbildung 2.3 Verwenden Sie die Konsole *Leistungsinformationen und -tools* zur Bewertung der Leistung des Computers

PRAXISTIPP

Falls Ihr Computer nach der Installation nicht automatisch bewertet wurde, ist noch kein Leistungsindex errechnet worden. In diesem Fall können Sie auf den Link *Die Systembewertung ist nicht verfügbar* tippen oder klicken, um die Konsole *Leistungsinformationen und -tools* zu öffnen und das System zu bewerten. Die Bewertung eines Computers verändert sich unter Umständen, wenn Sie neue Hardware installieren. Wenn Windows Änderungen an der Hardwarekonfiguration erkennt, erhalten Sie die Meldung »Der Windows-Leistungsindex muss aktualisiert werden«. Tippen oder klicken Sie in diesem Fall auf den angezeigten Link, um *Leistungsinformationen und -tools* zu öffnen, und tippen oder klicken Sie dann auf *Aktualisieren* oder *Bewertung erneut ausführen*, um die Leistungsbewertung neu berechnen zu lassen.

Die Seite *Leistungsinformationen und -tools* zeigt die Gesamteinstufung des Systems und listet die Bewertung der installierten Hardware in fünf Kategorien auf:

- *Prozessor*
- *Arbeitsspeicher (RAM)*
- *Grafik*
- *Grafik (Spiele)*
- *Primäre Festplatte*

Windows 8 verwendet die Gesamt- und Detailbewertung des Computers zur Entscheidung, welche der verfügbaren Funktionen konfiguriert werden sollen. Ist die Leistung des Computers zu gering, empfiehlt Windows 8 die Abschaltung einiger Funktionen, um die Gesamtleistung zu verbessern. Anhand des Leistungsverhaltens kann Windows 8 auch die Abschaltung oder Änderung von anderen Funktionen vorschlagen, um die Gesamtleistung zu optimieren.

TIPP Verschiedene Faktoren können die Leistungsbewertung negativ beeinflussen, wie zum Beispiel mangelnder Speicherplatz auf der primären Festplatte. Wenn Sie einen Computer mit neuer Hardware ausstatten oder versuchen, Leistungsprobleme zu beheben, die sich auf die Bewertung des Computers auswirken, können Sie auf *Aktualisieren* oder *Bewertung erneut ausführen* tippen oder klicken, um die aktuelle Leistungsbewertung des Computers zu erstellen.

Der linke Fensterabschnitt in *Leistungsinformationen und -tools* bietet schnellen Zugriff auf mehrere nützliche Konfigurationsbereiche:

- **Visuelle Effekte anpassen** Öffnet das Dialogfeld *Leistungsoptionen*, in dem Sie visuelle Effekte, Prozessorzeitplanung, virtuellen Arbeitsspeicher und Datenausführungsverhinderung verwalten können.
- **Indizierungsoptionen anpassen** Öffnet das Dialogfeld *Indizierungsoptionen*, in dem Sie einstellen, welche Speicherorte indiziert werden und welche Indexeinstellungen dabei verwendet werden.
- **Energieeinstellungen anpassen** Öffnet das Dialogfeld *Energieoptionen*, in dem Sie Energiesparpläne verwalten, die Funktion der Schalter am Computergehäuse konfigurieren und Wartezeiten bis zum Abschalten des Bildschirms und dem Aktivieren des Standbymodus festlegen.

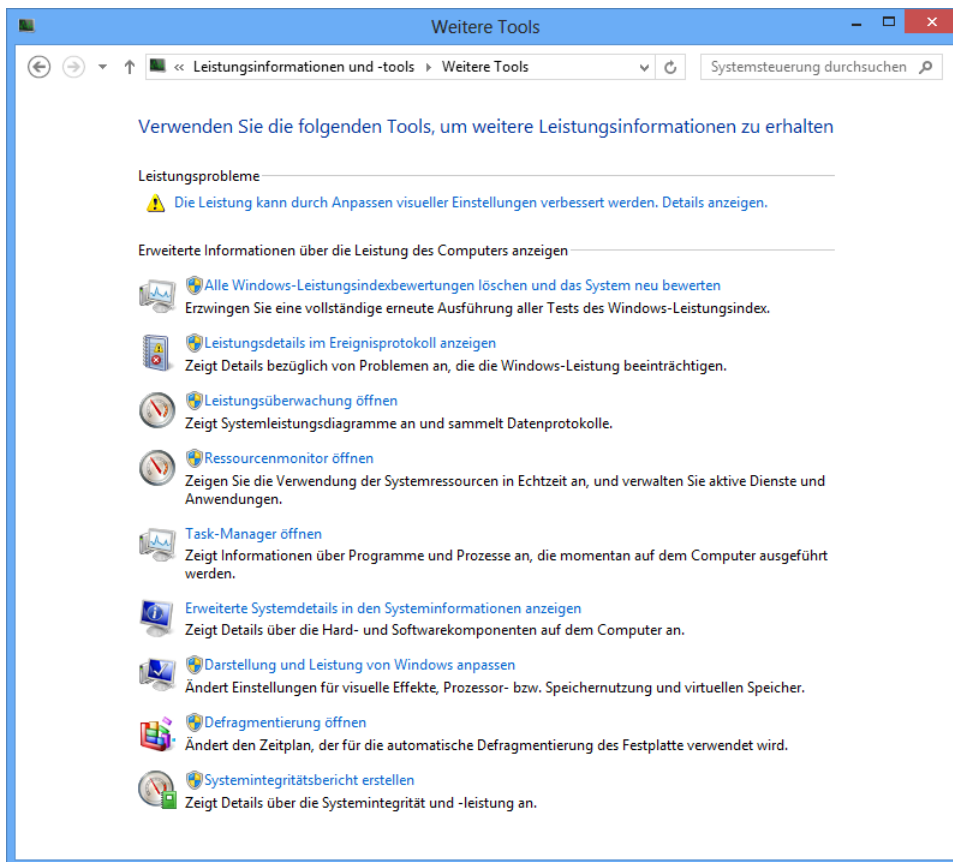


Abbildung 2.4 Zugriff auf weitere Tools zum Verwalten des Computers

Eine der nützlichsten Optionen in *Leistungsinformationen und -tools* ist der Link *Weitere Tools* im linken Fensterabschnitt. Wenn Sie ihn antippen oder anklicken, wird die Seite aus Abbildung 2.4 geöffnet. Hier haben Sie schnellen Zugriff auf Systemwartungstools, darunter folgende:

- Task-Manager, der normalerweise mit der Tastenkombination STRG+ALT+ENTF geöffnet wird
- Ressourcenmonitor, der normalerweise mit der Schaltfläche *Ressourcenmonitor* im Task-Manager geöffnet wird
- Erweiterte Systemdetails in den Systeminformationen, die normalerweise durch Ausführen von *Msinfo32* geöffnet werden
- Systemintegritätsbericht, der normalerweise nur im Rahmen einer erweiterten Diagnose generiert wird

Sofern Sie als Administrator angemeldet sind, können Sie einen Systemintegritätsbericht generieren, indem Sie auf *Systemintegritätsbericht erstellen* tippen oder klicken. Das Erstellen dieses Berichts dauert etwa 1 Minute. Der Bericht führt Einzelheiten zum Status von Hardwareressourcen, Systemreaktionszeiten und Prozessen auf dem Computer auf, außerdem Systeminformationen und Konfigurationsdaten (Abbildung 2.5). Der Bericht enthält auch Vorschläge, wie sich Probleme beseitigen lassen und die Leistung optimieren lässt. Sie können den Bericht als HTML-Dokument speichern, indem Sie den Menübefehl *Datei/Speichern unter* wählen und dann im Dialogfeld *Speichern unter* den Speicherort und den Dateinamen für den Bericht angeben. Sie können den Bericht auch als Anhang in einer E-Mail-Nachricht versenden, indem Sie den Menübefehl *Datei/Senden an* wählen.

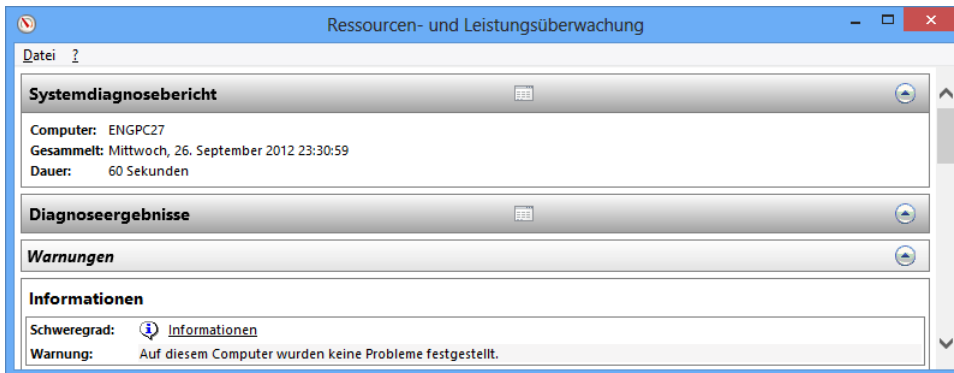


Abbildung 2.5 Der Diagnosebericht hilft beim Beseitigen von Leistungsproblemen

Abrufen von ausführlicheren Systeminformationen

Wenn Sie ausführliche Angaben über das System brauchen oder Remotesysteme überprüfen möchten, verwenden Sie das Programm Systeminformationen (*Msinfo32.exe*). Tippen oder klicken Sie im Anwendungsbildschirm auf *Systeminformationen* oder geben Sie im *Apps*-Suchfeld *msinfo32* ein und drücken Sie die EINGABETASTE. Wie in Abbildung 2.6 gezeigt, können Sie sich durch die Wahl des Knotens *Systemübersicht* einen Überblick über das System verschaffen. Die Konfigurationsdaten werden mit dem Dienst Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI) erfasst.

Das Programm Systeminformationen zeigt ausführliche Informationen über viele wichtige Bereiche des Betriebssystems an:

- **Hardwareressourcen** Bietet ausführliche Informationen über Ein-/Ausgabe (E/A), Unterbrechungsanforderungen (IRQs), Speicher, direkte Speicherzugriffe (DMA) sowie Plug & Play-Geräte. Ein

Schlüsselbereich, den Sie überprüfen sollten, wenn es im System Probleme mit einem Gerät gibt, ist der Knoten *Konflikte/Gemeinsame Nutzung*. Dieser Bereich bietet eine Übersicht über Geräte, die Ressourcen gemeinsam benutzen oder Konflikte im System verursachen.

- **Komponenten** Bietet ausführliche Informationen über installierte Komponenten, angefangen bei den Audiocodern bis hin zu den USB-Controllern. Ein Schlüsselbereich, den Sie überprüfen sollten, wenn es Probleme mit einer Komponente des Systems gibt, ist der Knoten *Problemgeräte*. Unter diesem Knoten finden Sie Informationen über Komponenten, bei denen es zu Fehlern kommt.
- **Softwareumgebung** Bietet ausführliche Informationen über die Ausführungsumgebung des Betriebssystems. Wenn Sie versuchen, Probleme auf einem Remotesystem zu beheben, wird Ihnen der Bereich *Softwareumgebung* sehr von Nutzen sein. Neben Treibern, Umgebungsvariablen, Druckaufträgen und Netzwerkverbindungen können Sie auch aktive Tasks, Dienste, Programmgruppen und Autostartprogramme überprüfen.

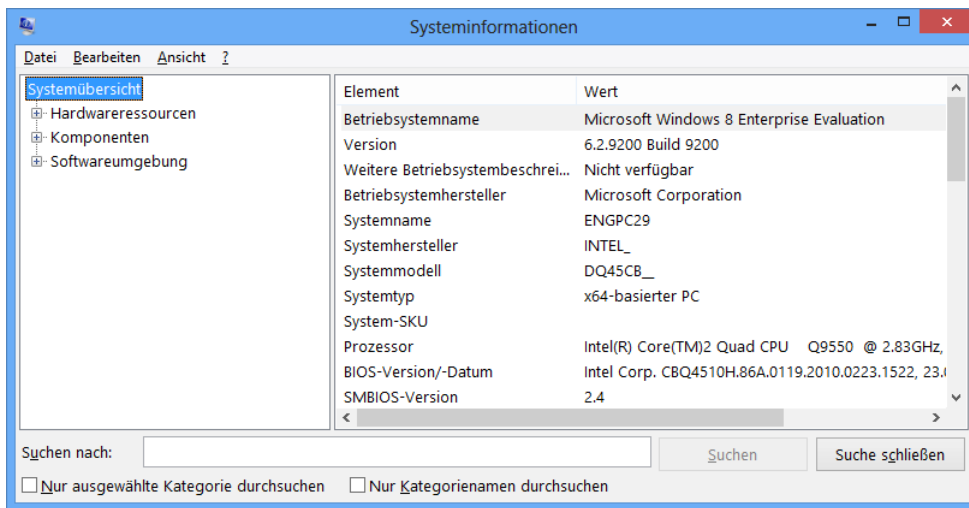


Abbildung 2.6 Ausführliche Systeminformationen können Ihnen bei der Behebung von Problemen mit der Systemkonfiguration helfen

Wenn Sie die Konfiguration eines Remotecomputers überprüfen möchten, gehen Sie folgendermaßen vor:

1. Starten Sie das Programm Systeminformationen. Wählen Sie im *Ansicht*-Menü *Remotecomputer*. Dadurch wird das Dialogfeld *Remotecomputer* geöffnet.
2. Wählen Sie im Dialogfeld *Remotecomputer* die Option *Remotecomputer im Netzwerk*.
3. Geben Sie den Namen des Computers im entsprechenden Textfeld ein und tippen oder klicken Sie auf *OK*.

Das Konto, das Sie verwenden, muss über die erforderlichen Administratorrechte für den lokalen Computer oder die Domäne verfügen. Wenn Sie keine Informationen vom Remotesystem erhalten, müssen Sie vielleicht den Namespace überprüfen, den der WMI-Dienst verwendet, wie im nächsten Abschnitt dieses Kapitels beschrieben. Dass Sie Systeminformationen über einen Remotecomputer sehen, erkennen Sie daran, dass der Knoten *Systemübersicht* den Computernamen in Klammern anzeigt.

Arbeiten mit der WMI-Steuerung

Die Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI) ist eine Schlüsselkomponente des Betriebssystems Windows 8. Sie dient zur Erfassung von Informationen über das System, zur Überwachung des Systemzustands und zur Verwaltung von Systemkomponenten. Damit sie funktionieren kann, ist WMI auf den WMI-Dienst angewiesen. Dieser Dienst muss ausgeführt werden und für die Umgebung konfiguriert sein.

Sie können die Einstellung des WMI-Dienstes mit der WMI-Steuerung überprüfen, die Sie auf dem lokalen System oder auf einem Remotesystem folgendermaßen öffnen:

1. Öffnen Sie vom Anwendungsbildschirm aus die Computerverwaltung (oder vom Startbildschirm aus, sofern Sie die Verwaltungstools hinzugefügt haben).
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *Computerverwaltung* oder halten Sie den Knoten gedrückt, und wählen Sie dann *Verbindung mit anderem Computer herstellen*. Nun können Sie das System auswählen, dessen Dienste Sie verwalten möchten.
3. Erweitern Sie den Knoten *Dienste und Anwendungen*, indem Sie auf das Symbol vor dem Knoten tippen oder klicken. Tippen oder klicken Sie dann auf *WMI-Steuerung*. (Das ist erforderlich, damit die Steuerung eingelesen wird.) Klicken Sie mit der rechten Maustaste auf *WMI-Steuerung* oder halten Sie den Knoten gedrückt, und wählen Sie dann *Eigenschaften*. Nun können Sie WMI im Dialogfeld *Eigenschaften von WMI-Steuerung* konfigurieren.

Wie aus Abbildung 2.7 hervorgeht, verfügt das Dialogfeld *Eigenschaften von WMI-Steuerung* über folgende Registerkarten:

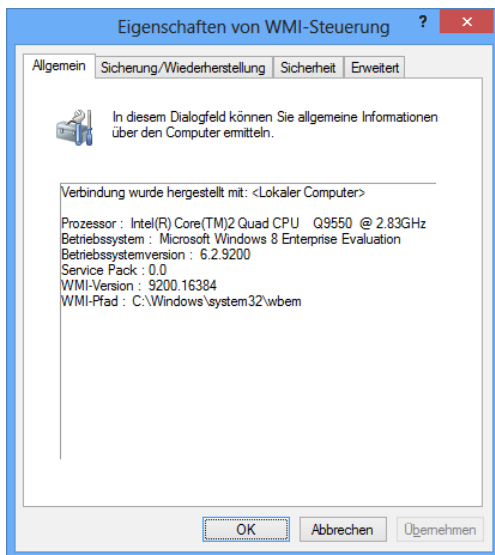


Abbildung 2.7 Die *WMI-Steuerung* dient zur Konfiguration des WMI-Dienstes

- **Allgemein** Die Felder auf dieser Registerkarte geben einen Überblick über das System und WMI. WMI verwendet die Anmeldeinformationen des aktuellen Benutzers, um die Systeminformationen abzurufen.

- **Sicherung/Wiederherstellung** Die Werte, die WMI ermittelt, werden in einer Datenbank abgelegt. Standardmäßig liegt diese Datenbank im Verzeichnis `%SystemRoot%\System32\Wbem\Repository`. Die Werte werden standardmäßig in regelmäßigen Abständen gesichert. Mit den Schaltflächen *Jetzt sichern* oder *Wiederherstellen* dieser Registerkarte können Sie die Datenbank manuell sichern oder wiederherstellen.
- **Sicherheit** Sicherheitseinstellungen bestimmen, wer Zugang zu den verschiedenen Ebenen der WMI-Daten erhält. Standardmäßig erhalten Administratoren den vollen Zugriff auf WMI, und die Gruppe *Authentifizierte Benutzer* ist berechtigt, Methoden auszuführen, Konten zu aktivieren und die erfassten Zahlen zu speichern.
- **Erweitert** Die Einstellung legt den Standardnamespace für WMI fest. Der Standardnamespace wird in WMI-Skripts verwendet, wenn der Namespace eines WMI-Objekts nicht vollständig angegeben wurde. Sie können die Standardeinstellung ändern, indem Sie auf *Ändern* tippen oder klicken, einen neuen Standardnamespace festlegen und dann auf *OK* tippen oder klicken.

HINWEIS WMI führt Fehlerprotokolle, die zur Behebung von Problemen mit dem WMI-Dienst verwendet werden können. Standardmäßig werden diese Protokolle unter `%SystemRoot%\System32\Wbem\Logs` gespeichert. WMI-Verwaltung, Dateien, Protokolle und Datenbanken können einen beträchtlichen Teil der Festplatte beanspruchen. Im Durchschnitt belegen diese Dateien auf meinen Testsystemen etwa 65 MByte. Der größte Teil davon (40 bis 50 MByte) wird für die Datenbankdateien gebraucht.

Die von WMI gesammelten Informationen werden in einer Gruppe von Systemdateien gespeichert, die als *Repository* bezeichnet werden. Standardmäßig werden die Repositorydateien unter `%SystemRoot%\System32\Wbem\Repository` gespeichert. Das Repository ist das Kernstück von WMI und den Hilfe- und Supportdiensten. Informationen werden mithilfe einer Stagingdatei übertragen. Wenn die Repositorydaten oder die Stagingdatei beschädigt wird, funktioniert WMI vielleicht nicht richtig. Gewöhnlich dauert dieser Zustand nur eine begrenzte Zeit, aber Sie können sich davor schützen, indem Sie manuell eine Sicherungskopie der Repositorydateien erstellen.

Zur manuellen Sicherung des WMI-Repositorys gehen Sie folgendermaßen vor:

1. Öffnen Sie das Dialogfeld *Eigenschaften von WMI-Steuerung* und tippen oder klicken Sie auf die Registerkarte *Sicherung/Wiederherstellen*.
2. Tippen oder klicken Sie auf *Jetzt sichern*. Geben Sie im Dialogfeld *Einen Namen für die Sicherungsdatei angeben* einen Namen für die WMI-Sicherungsdatei und den Speicherort an. Klicken Sie dann auf *Speichern*.
3. Während der Erstellung der Sicherungsdatei wird das Dialogfeld *Sicherung wird ausgeführt* angezeigt. Die Namenserverweiterung der Sicherungsdatei lautet *.rec* und die Größe der Datei liegt ungefähr zwischen 20 und 30 MByte, je nach der gespeicherten Datenmenge.

Wenn Sie das WMI-Repository später wiederherstellen müssen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Dialogfeld *Eigenschaften von WMI-Steuerung* und tippen oder klicken Sie auf die Registerkarte *Sicherung/Wiederherstellen*.
2. Tippen oder klicken Sie auf *Wiederherstellen*. Geben Sie im Dialogfeld *Einen Namen für die Sicherungsdatei zum Wiederherstellen angeben* den Ort und den Namen der betreffenden Sicherungsdatei an. Tippen oder klicken Sie dann auf *Öffnen*.
3. Für eine gewisse Zeit wird das Dialogfeld *Wiederherstellung wird ausgeführt* angezeigt. Dann wird eine Warnung angezeigt. Tippen oder klicken Sie auf *OK*.

4. Ihre Verbindung zur WMI-Steuerung ist unterbrochen. Sobald die Wiederherstellung abgeschlossen ist, können Sie die Verbindung zum Computer wieder aufnehmen. Dazu schließen Sie das Dialogfeld *Eigenschaften von WMI-Steuerung* und öffnen es erneut. Dadurch wird die WMI-Steuerung veranlasst, die Verbindung zum lokalen Computer oder zum Remotecomputer wiederherzustellen. Erfolgreich kann dieser Versuch aber erst dann sein, wenn die Wiederherstellung abgeschlossen ist.

HINWEIS

Wenn sich keine Verbindung herstellen lässt, bedeutet dies gewöhnlich, dass die WMI-Steuerung noch mit der Wiederherstellung der Datenbank beschäftigt ist. Warten Sie noch eine halbe oder eine Minute und versuchen Sie es erneut.

Verwenden von Systemprogrammen

Zum Lieferumfang von Windows 8 gehören eine ganze Reihe von Systemprogrammen, darunter folgende:

- **Datensicherung (*Sdclt.exe*)** Öffnet das Tool *Windows 7-Datienwiederherstellung*, in dem Sie Benutzer- und Systemdateien sichern und wiederherstellen können. Weitere Informationen finden Sie in Kapitel 10.
- **Integrierte Diagnoseprogramme** Die integrierten Diagnoseprogramme durchsuchen das System und überprüfen die Hardware und die Softwareeinstellungen nach Problemen. Diese Programme eignen sich zur Diagnose von Problemen und zur Behebung von Leistungs- und Konfigurationsproblemen. Die Verwendung der Diagnoseprogramme wird in diesem Kapitel, aber auch in mehreren weiteren Kapiteln dieses Buchs beschrieben.
- **DirectX-Diagnoseprogramm (*Dxdiag.exe*)** Ein integriertes Diagnoseprogramm, das Sie bei der Lösung von Problemen mit Microsoft DirectX unterstützt. DirectX dient zur Leistungsverbesserung von Anwendungen, sofern die Hardware des Systems DirectX unterstützt.
- **Datenträgerbereinigung (*Cleanmgr.exe*)** Das Dienstprogramm Datenträgerbereinigung durchsucht Laufwerke nach Dateien, die nicht mehr gebraucht werden. Standardmäßig berücksichtigt die Datenträgerbereinigung temporäre Dateien, den Papierkorb und verschiedene Offlinedateien, wenn sie nach Dateien sucht, die gelöscht werden können.
- **Defragmentierung (*Dfrgui.exe*)** Das Laufwerkoptimierungsprogramm untersucht Laufwerke auf Fragmentierung und kann zur Defragmentierung der Dateien eingesetzt werden. Durch eine starke Fragmentierung von Dateien kann die Leistung des Systems sinken. Weitere Informationen über dieses Programm finden Sie in Kapitel 12, »Verwalten von Festplattenlaufwerken und Dateisystemen«.
- **Dateisignaturverifizierung (*Sigverif.exe*)** Dient zur Überprüfung der digitalen Signaturen von Betriebssystemdateien. Alle kritischen Dateien, die nicht digital signiert sind, werden in einer Ergebnisliste angezeigt. Eine vollständige Liste aller überprüften Dateien finden Sie in der Protokolldatei *Sigverif.txt* (im Ordner *Dokumente*).
- **Remoteunterstützungsanbieter** Ermöglichen es Ihnen, einem Benutzer Remoteunterstützung anzubieten. Nimmt ein Benutzer das Angebot an, können Sie versuchen, auf seinem System Probleme zu beheben, wie das in Kapitel 10 besprochen wird.
- **Remoteunterstützung** Ermöglicht es Ihnen, eine Einladung zur Remoteunterstützung zu erstellen, mit der Sie zum Beispiel Hilfe von einem Techniker anfordern können. Remoteunterstützung wird in Kapitel 10 ausführlich besprochen.

- **Systemkonfigurationsprogramm (*Msconfig.exe*)** Ermöglicht Ihnen die Verwaltung von Informationen über die Systemkonfiguration. Sie können auch einen normalen Systemstart, einen Diagnose-systemstart oder einen benutzerdefinierten Systemstart festlegen.
- **Systemwiederherstellung (*Rstrui.exe*)** Mit dem Systemprogramm Systemwiederherstellung können Sie Wiederherstellungspunkte erstellen oder das System auf einen bestimmten Wiederherstellungspunkt zurückführen. Das Systemwiederherstellungsprogramm wird in Kapitel 10 besprochen.

Zu den Programmen, die Sie sich an dieser Stelle etwas näher ansehen sollten, gehören die Datenträgerbereinigung, die Dateisignaturverifizierung und das Systemkonfigurationsprogramm.

Arbeiten mit der Datenträgerbereinigung

Die Datenträgerbereinigung überprüft Laufwerke auf Dateien, die nicht mehr gebraucht werden. Wenn Sie die Datenträgerbereinigung einsetzen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Datenträgerbereinigung, indem Sie auf dem Anwendungsbildschirm die entsprechende Option antippen oder anklicken, oder indem Sie im Suchfeld *Apps cleanmgr* eingeben und die EINGABETASTE drücken.
2. Sofern der Computer mehrere Laufwerke aufweist, wird das Dialogfeld *Datenträgerbereinigung: Laufwerksauswahl* angezeigt. Wählen Sie in der Dropdownliste *Laufwerk* das Laufwerk aus, das Sie aufräumen möchten, und tippen oder klicken Sie auf OK.

Die Datenträgerbereinigung überprüft das ausgewählte Laufwerk und sucht dabei nach temporären Benutzerdateien, die gelöscht werden können, sowie nach Benutzerdateien, die möglicherweise gelöscht werden können. Je mehr Dateien auf dem Laufwerk liegen, desto länger dauert die Suche.

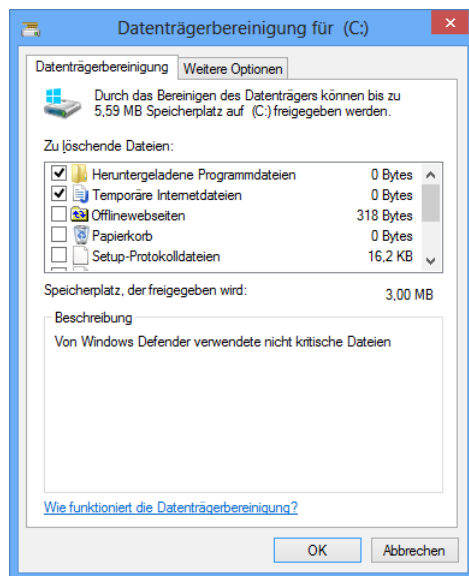


Abbildung 2.8 Mit der Datenträgerbereinigung finden Sie Dateien, die gelöscht werden können

Wenn die Datenträgerbereinigung ihren ersten Durchlauf abgeschlossen hat, können Sie temporäre Systemdateien, die gelöscht werden können, und Systemdateien hinzufügen, die unter Umständen gelöscht werden dürfen. Klicken Sie dazu auf *Systemdateien bereinigen*, wählen Sie ein Systemlaufwerk aus, das untersucht werden soll, und tippen oder klicken Sie auf *OK*. Sie erhalten nun einen Bericht angezeigt, der ähnlich wie in Abbildung 2.8 aussieht. In diesem Bericht werden je nach Bedarf mehrere Dateikategorien genannt, darunter folgende:

- **Heruntergeladene Programmdateien** Betrifft Programme, die vom Browser heruntergeladen wurden, wie ActiveX-Steuerelemente und Java-Applets. Dabei handelt es sich um temporäre Dateien, die gelöscht werden können.
- **Beim Windows-Upgrade verworfene Dateien** Betrifft Dateien, die bei einem vorherigen Upgrade nicht als Windows-Systemdateien eingestuft wurden. Nachdem Sie alle benötigten Daten von früheren Windows-Installationen einschließlich der Benutzerdaten gesichert haben, können Sie diese Option verwenden, um die betreffenden Dateien zu löschen.
- **Ruhezustandsdateibereinigung** Betrifft die Daten über den Zustand des Computers beim Eintritt in den Ruhezustand. Wenn der Computer nicht mehr in den Ruhezustand übergehen soll, können Sie diese Datei löschen.
- **Temporäre Office-Dateien** Betrifft temporäre Dateien und Protokolle, die von Microsoft Office benutzt werden. Diese Dateien können gelöscht werden.
- **Offlinedateien** Betrifft lokale Kopien von Netzwerkdateien, die Sie für die Offlineverwendung gekennzeichnet haben. Diese Dateien wurden lokal gespeichert, um offline verfügbar zu sein, und können gelöscht werden.
- **Offlinewebsites** Enthält lokale Kopien von Webseiten, die Sie für die Offlineverwendung gekennzeichnet haben. Diese Dateien wurden lokal gespeichert, um den Offlinezugriff zu ermöglichen. Sie können gelöscht werden.
- **Vorherige Windows-Installation(en)** Damit sind Dateien aus früheren Windows-Installationen gemeint, die unter *%SystemDrive%\Windows.old* gespeichert wurden. Nachdem Sie alle benötigten Daten aus den früheren Windows-Installationen gesichert haben, einschließlich der Benutzerdaten, können Sie die betreffenden Dateien mit dieser Option löschen.
- **Temporäre Offlinedateien** Betrifft temporäre Daten und Arbeitskopien von kürzlich benutzten Netzwerkdateien. Diese Dateien wurden lokal gespeichert, um offline zugänglich zu sein, und können gelöscht werden.
- **Papierkorb** Der Papierkorb enthält Dateien, die zwar gelöscht, aber noch nicht vom Computer entfernt wurden. Erst bei der Leerung des Papierkorbs werden diese Dateien tatsächlich vom Computer entfernt.
- **Temporäre Dateien** Betrifft Dateien im Ordner *Temp*. Dabei handelt es sich hauptsächlich um temporäre Dateien oder Arbeitsdateien von Anwendungen.
- **Temporäre Internetdateien** Betrifft Webseiten, die der Browser zwischengespeichert hat. Diese Dateien sind temporär und können gelöscht werden.
- **Miniaturansichten** Betrifft Miniaturansichten von Bildern, Videos und Dokumenten, die von Windows 8 erstellt wurden. Wenn Sie das erste Mal auf einen Ordner zugreifen, erstellt Windows 8 Miniaturansichten der darin enthaltenen Bilder, Videos und Dokumente. Diese Miniaturansichten werden gespeichert, damit sie beim nächsten Zugriff auf den Ordner schnell angezeigt werden können. Wenn Sie die Miniaturansichten löschen, werden sie beim nächsten Zugriff auf den betreffenden Ordner wieder erstellt.

3. Markieren Sie mit den Kontrollkästchen in der Liste *Zu löschende Dateien* die Dateikategorien, die gelöscht werden sollen. Klicken Sie dann auf OK. Wenn Sie zur Bestätigung der Aktion aufgefordert werden, tippen oder klicken Sie auf *Dateien löschen*.

Überprüfen von Systemdateien mit der Dateisignaturverifizierung

Kritische Dateien, die vom Betriebssystem verwendet werden, sind digital signiert. Digitale Signaturen dienen dazu, die Authentizität der Dateien zu beweisen und leichter Manipulationen erkennbar zu machen, durch die Probleme auf dem System entstehen könnten. Wenn Sie es mit Problemen zu tun haben, für die es anscheinend keine plausible Erklärung gibt, sollten Sie überprüfen, ob vielleicht kritische Systemdateien geändert wurden. Das ist zum Beispiel sinnvoll, wenn ein System nach der Installation einer Anwendung instabil wird. Diese Überprüfung können Sie mit der Dateisignaturverifizierung vornehmen.

Die ausführbare Datei der Dateisignaturverifizierung ist *Sigverif.exe*. Sie können die Dateisignaturverifizierung mit folgenden Schritten starten und verwenden:

1. Geben Sie im Suchfeld *Apps* **sigverif** ein und drücken Sie die EINGABETASTE. Dadurch wird die Dateisignaturverifizierung gestartet (Abbildung 2.9).



Abbildung 2.9 Die Dateisignaturverifizierung hilft beim Überprüfen von Systemdateien

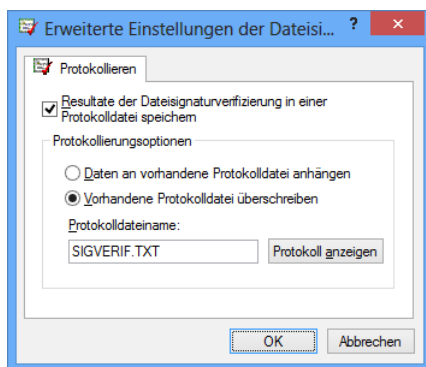


Abbildung 2.10 Ändern der Protokollierungsoptionen

2. Standardmäßig zeigt die Dateisignaturverifizierung eine Liste der Systemdateien an, die nicht digital signiert sind, und speichert ein Protokoll in der Datei *Sigverif.txt* (im Ordner *Öffentliche Dokumente*). Bevor Sie Dateisignaturen überprüfen, sollten Sie die Protokollierungsoptionen festlegen. Klicken Sie dazu auf *Erweitert*. Wie in Abbildung 2.10 gezeigt, werden die Verifizierungsergebnisse in der Standardeinstellung in einer Protokolldatei gespeichert. Alle Ergebnisse, die Sie generieren, überschreiben bereits vorher erstellte Ergebnisse, und die Ergebnisse werden in einer Protokolldatei namens *Sigverif.txt* gespeichert. Um Änderungen an Dateien gut zu erkennen, sollten Sie die Ergebnisse nicht überschreiben, sondern anhängen. Bei dieser Einstellung sind Änderungen einfacher zu sehen. Tippen oder klicken Sie auf *OK*, wenn Sie die Protokollierungsoptionen wie gewünscht eingestellt haben. Sie kehren damit wieder zum Hauptfenster zurück.
3. Tippen oder klicken Sie auf *Starten*, um die Dateisignaturverifizierung auszuführen. In den Resultaten finden Sie die Liste der Dateien, die im Bericht der Dateisignaturverifizierung angezeigt werden. Diese Dateien sind nicht digital signiert und könnten vielleicht in böswilliger Absicht durch andere Programme desselben Namens ersetzt worden sein. Tippen oder klicken Sie auf *Schließen*, um zum Hauptfenster zurückzukehren. Wenn Sie ein Problem vermuten, sollten Sie die Ereignisprotokolle und andere Fehlerprotokolle daraufhin überprüfen, ob diese Dateien in den Fehlerberichten auftauchen.
4. Sie können sich das Verifizierungsprotokoll ansehen, indem Sie auf *Erweitert* und dann auf *Protokoll anzeigen* klicken. Sie können das Verifizierungsprotokoll stattdessen auch im Microsoft Editor öffnen. Die Protokolldatei *Sigverif.txt* liegt standardmäßig im Ordner *Öffentliche Dokumente*. Sehen Sie das Protokoll durch und prüfen Sie, ob Dateien aufgeführt sind, die sich verändert haben, seit sie installiert wurden. Die Dateien werden anhand ihres Status aufgelistet, zum Beispiel als »Signiert« und »Nicht signiert«. Sehen Sie sich das Änderungsdatum und die Version der Datei an. Wenn bei einem Computer seit einem bestimmten Datum Probleme auftreten und wichtige Dateien an diesem Tag geändert wurden, ist das möglicherweise die Ursache der Probleme. Es ist beispielsweise möglich, dass ein Programm installiert wurde, das eine wichtige Datei durch eine ältere Version überschrieben hat.

Verwalten der Systemkonfiguration und der Systemstartoptionen

Ob Sie die Systemkonfigurationsdateien aktualisieren oder Probleme beheben möchten, die beim Systemstart auftreten, das Programm Systemkonfiguration ist in solchen Fällen das Werkzeug der Wahl. Es ist ein integriertes Programm zur Verwaltung von Systemkonfigurationsdaten. Mit diesem Programm können Sie folgende Elemente verwalten:

- Startoptionen des Betriebssystems
- Autostartanwendungen
- Dienststartoptionen

Die folgenden Abschnitte beschreiben die wichtigsten Arbeiten, die Sie mit dem Systemkonfigurationsprogramm durchführen können. Die ausführbare Datei des Systemkonfigurationsprogramms ist *Msconfig.exe*. Sie können das Programm starten, indem Sie im Suchfeld *Apps* **msconfig** eingeben und dann die EINGABETASTE drücken.

HINWEIS

Das Systemkonfigurationsprogramm finden Sie auch auf dem Anwendungsbildschirm, und zwar im Abschnitt *Verwaltung*.

Startmodi und Behebung von Problemen mit dem Systemstart

Mit dem Programm Systemkonfiguration können Sie den Startmodus eines Computers festlegen. Folgende drei Startmodi sind verfügbar:

- **Normaler Systemstart** Wird für den Normalbetrieb benutzt. In diesem Modus lädt das Betriebssystem alle Systemkonfigurationsdateien und Gerätetreiber. Außerdem startet es alle Autostartanwendungen und alle aktivierten Dienste.
- **Diagnosesystemstart** Der Diagnosesystemstart dient zur Behebung von Systemproblemen. Im Diagnosemodus lädt das Betriebssystem nur die wichtigsten Gerätetreiber und die unverzichtbaren Dienste. Nachdem Sie das System im Diagnosemodus gestartet haben, können Sie die Systemeinstellungen ändern, um die Konfigurationsprobleme zu beheben.
- **Benutzerdefinierter Systemstart** Der benutzerdefinierte Systemstart dient zur Eingrenzung von Problembereichen in der Konfiguration. Hier können Sie eine geänderte Startkonfiguration wählen und selektiv die Systemdienste und Startelemente aussuchen. Auf diese Weise können Sie die Einstellungen ermitteln, die Probleme verursachen, und sie nach Bedarf korrigieren.

Der Normalfall ist der normale Systemstart. Wenn bei einem Computer Probleme auftreten und Sie einen anderen Startmodus verwenden möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Systemkonfigurationsprogramm, indem Sie im Suchfeld *Apps* **msconfig** eingeben und dann die EINGABETASTE drücken, oder indem Sie auf dem Anwendungsbildschirm auf die entsprechende Option tippen oder klicken.

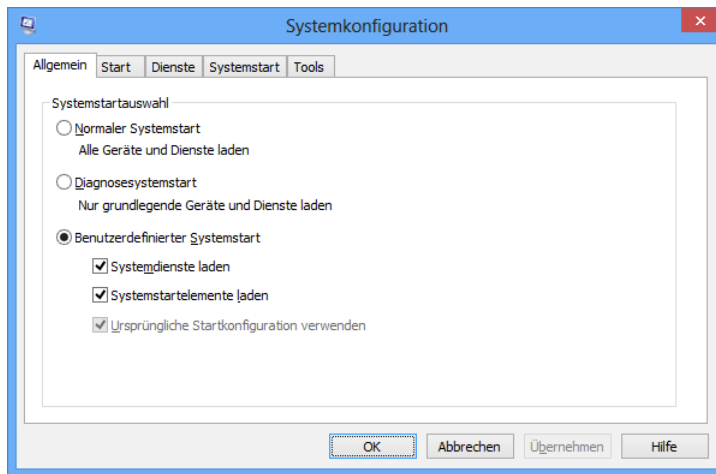


Abbildung 2.11 Auf der Registerkarte *Allgemein* des Programms *Systemkonfiguration* können Sie die Art des Systemstarts einstellen

2. Auf der Registerkarte *Allgemein* (Abbildung 2.11) wählen Sie entweder *Diagnosesystemstart* oder *Benutzerdefinierter Systemstart*. Wenn Sie sich für *Benutzerdefinierter Systemstart* entscheiden, können Sie die Elemente auswählen, die das System verwenden soll:
 - **Systemdienste laden** Weist das System an, beim Start die Windows-Dienste zu laden. Wenn Sie diese Option wählen, können Sie auf der Registerkarte *Dienste* festlegen, welche Dienste gestartet werden sollen.

- **Systemstartelemente laden** Weist das System an, beim Start die dafür vorgesehenen Anwendungen zu starten. Wenn Sie diese Option wählen, können Sie auf der Registerkarte *Systemstart* die Autostartanwendungen aktivieren oder deaktivieren.
- **Ursprüngliche Startkonfiguration verwenden** Weist das System an, beim Start die ursprüngliche Startkonfiguration zu verwenden statt der neuen Konfiguration, die Sie im Systemkonfigurationsprogramm durch die Änderung der Einstellungen erstellt haben.

HINWEIS Wenn Sie auf den Registerkarten *Start*, *Dienste* oder *Systemstart* Änderungen vornehmen, werden auf der Registerkarte *Allgemein* automatisch die Option *Benutzerdefinierter Systemstart* und die zugehörigen Unteroptionen ausgewählt.

3. Wenn Sie fertig sind, tippen oder klicken Sie auf *OK* und starten dann das System neu. Sollten sich beim Systemstart Probleme ergeben, starten Sie erneut im abgesicherten Modus und wiederholen diese Prozedur. Nach einem fehlgeschlagenen Start erscheint der abgesicherte Modus automatisch als Startoption.

Ändern der Startoptionen

Windows 8 verwendet zum Start des Betriebssystems den Windows-Start-Manager und eine Startanwendung. Es benutzt in der Standardkonfiguration weder *Boot.ini* noch andere Startdateien. Zur Fehlerbehebung können Sie mit den Optionen auf der *Start*-Registerkarte des Systemkonfigurationsprogramms die Startpartition, Startmethode und Startoptionen für das Betriebssystem festlegen.

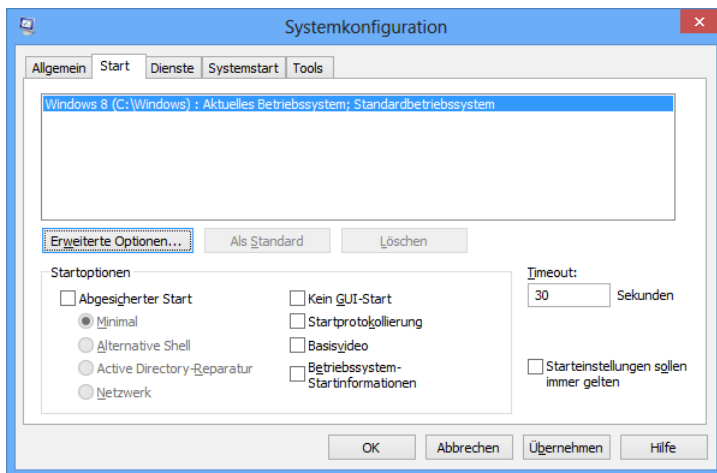


Abbildung 2.12 Die Steuerelemente auf der Registerkarte *Start* legen die Startpartition, die Startmethode und die Startoptionen fest, die das Betriebssystem benutzt

Wie aus Abbildung 2.12 hervorgeht, werden die startfähigen Betriebssysteme des Computers aufgelistet, wenn Sie das Systemkonfigurationsprogramm starten und auf die Registerkarte *Start* klicken. Wenn Sie festlegen möchten, dass ein anderes als das aktuelle Betriebssystem verwendet werden soll, klicken Sie einfach auf den entsprechenden Eintrag. Bei der Bearbeitung der Betriebssystemeinträge haben Sie die Wahl unter folgenden Optionen:

- **Als Standard** Legt die aktuell gewählte Startpartition als Standardpartition fest. Die Standardpartition wird automatisch gewählt, wenn Sie vor Ablauf des Zeitlimits keine andere Partition auswählen.
- **Timeout** Legt fest, wie lange der Computer wartet, bevor er die Standardstartpartition verwendet.
- **Löschen** Löscht einen Betriebssystemeintrag. Der Eintrag kann nicht so einfach wiederhergestellt werden. Löschen Sie einen Eintrag also nur, wenn es unbedingt erforderlich ist.

HINWEIS Ist auf einem Computer nur ein Betriebssystem vorhanden, werden die Schaltflächen *Als Standard* und *Löschen* abgeblendet dargestellt, weil es kein anderes Betriebssystem gibt, das ausgewählt oder gelöscht werden könnte. Wenn Sie das Standardbetriebssystem auswählen, steht *Als Standard* nicht zur Verfügung. Und wenn Sie das aktuelle Betriebssystem auswählen, ist die Schaltfläche *Löschen* deaktiviert.

Außerdem können Sie folgende Startoptionen festlegen:

- **Abgesicherter Start** Startet den Computer im abgesicherten Modus mit zusätzlichen Flags für minimale, alternative oder Netzwerkshell und den Verzeichnisdienstreparaturstatus (*DsRepair*). Nach dem erfolgreichen Start im abgesicherten Modus können Sie die Systemeinstellungen ändern, um Konfigurationsprobleme zu lösen.
- **Kein GUI-Start** Startet den Computer bis zur Windows-Eingabeaufforderung, ohne die grafischen Komponenten des Betriebssystems zu laden. Der Start bis zur Eingabeaufforderung ist sinnvoll, wenn Sie mit den Grafikkomponenten von Windows 8 Probleme haben.
- **Startprotokollierung** Schaltet die Startprotokollierung ein, damit die wichtigsten Ereignisse beim Systemstart in eine Protokolldatei geschrieben werden.
- **Basisvideo** Schaltet den Computer in den VGA-Modus (Video Graphics Array). Verwenden Sie diesen Modus, wenn Sie Probleme mit der Grafikeinstellung beheben müssen und beispielsweise ein Modus eingestellt ist, den der Monitor nicht anzeigen kann.
- **Betriebssystem-Startinformationen** Startet den Computer mit ausführlichen Kommentaren, damit Sie überprüfen können, was vor dem Laden der Grafikkomponenten von Windows alles geschieht.

Alle Änderungen, die Sie vornehmen, werden vom Systemkonfigurationsprogramm als geänderte Startkonfigurationsdaten gespeichert. Wenn Sie alle erforderlichen Änderungen vorgenommen haben und auf OK klicken, können Sie den Computer neu starten, damit die Änderungen wirksam werden. Nachdem Sie dann die erforderlichen Änderungen vorgenommen haben, können Sie zu einem normalen Systemstart zurückgehen, indem Sie auf der Registerkarte *Allgemein* die Option *Normaler Systemstart* wählen und dann auf OK klicken. Auch dann müssen Sie den Computer neu starten, damit die neue Einstellung wirksam wird.

Wenn Sie auf der Registerkarte *Start* auf die Schaltfläche *Erweiterte Optionen* tippen oder klicken, können Sie im Dialogfeld *Erweiterte Startoptionen* (Abbildung 2.13) die Startoptionen für Prozessoren, maximalen Arbeitsspeicher, PCI-Lock und Debuggen einstellen. Verwenden Sie diese Optionen für die Problembehandlung. Wenn Sie beispielsweise vermuten, dass ein Problem dadurch verursacht wird, dass mehrere Prozessoren verfügbar sind, können Sie die Prozessoranzahl auf 1 setzen. Und wenn Sie vermuten, dass ein Problem durch Arbeitsspeicher ausgelöst wird, der über die ersten 4 GByte hinausgeht, können Sie in *Maximaler Speicher* die Größe 4.096 MByte einstellen. Sobald Sie mit der Problembehandlung fertig sind, sollten Sie diese Optionen wieder löschen, um den normalen Betrieb wieder aufzunehmen.

Wenn eine der erweiterten oder Standardstartoptionen auf der Registerkarte *Start* dauerhaft wirken soll, markieren Sie das Kontrollkästchen *Starteinstellungen sollen immer gelten*, bevor Sie auf OK klicken. In den meisten Fällen werden Sie nicht wollen, dass Optionen zur Problembehebung oder für das Debuggen dauerhaft werden. Achten Sie also darauf, dass Sie diese Optionen vorher löschen.

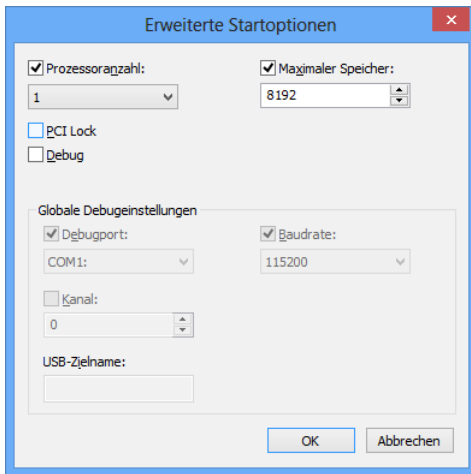


Abbildung 2.13 Einstellen der erweiterten Startoptionen im Rahmen der Problembehandlung

Aktivieren und Deaktivieren von Autostartanwendungen zur Problembehebung

Wenn Sie vermuten, dass eine der Anwendungen, die beim Systemstart geladen werden, ein Problem verursacht, können Sie das sehr leicht überprüfen. Sperren Sie den automatischen Start der Anwendungen und starten Sie das System dann neu. Tritt das Problem nicht mehr auf, haben Sie die Ursache vermutlich gefunden und können versuchen, die Anwendung oder Anwendungen zu ermitteln, die Probleme verursachen, und den automatischen Start dieser Anwendungen sperren.

Um Autostartanwendungen zu deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Systemkonfigurationsprogramm, indem Sie im Suchfeld *Apps msconfig* eingeben und dann die EINGABETASTE drücken oder indem Sie auf dem Anwendungsbildschirm auf die entsprechende Option tippen oder klicken.
2. Sorgen Sie auf der Registerkarte *Allgemein* dafür, dass *Benutzerdefinierter Systemstart* gewählt ist, und löschen Sie das Kontrollkästchen *Systemstartelemente laden*.
3. Tippen oder klicken Sie auf *OK*. Sie müssen das System neu starten, damit die Änderungen wirksam werden. Starten Sie den Computer also neu. Wenn das Problem nicht mehr auftritt, haben Sie die möglichen Ursachen auf die Autostartanwendungen eingegrenzt.

Die Option *Benutzerdefinierter Systemstart* wird automatisch gelöscht. Wenn Sie den Computer das nächste Mal starten, werden die Startanwendungen also wieder geladen. Nun müssen Sie mit dem Task-Manager das Programm ermitteln, das die Probleme bereitet. Zum Start des Task-Managers können Sie STRG+ALT+ENTF drücken oder im Suchfeld *Apps taskmgr* eingeben. Sie können auch die untere linke Ecke des Bildschirms gedrückt halten oder mit der rechten Maustaste anklicken und im Kontextmenü, das dann erscheint, auf *Task-Manager* tippen oder klicken.

Der Task-Manager zeigt auf der Registerkarte *Autostart* die Anwendungen an, die für einen automatischen Start konfiguriert wurden. Sie können die Anwendungen der Reihe nach deaktivieren und jeweils den Computer neu starten, um zu überprüfen, ob das Problem behoben ist. Um eine Anwendung zu deaktivieren, tippen oder klicken Sie den Eintrag der Anwendung im Task-Manager mit der rechten Maustaste an oder halten ihn gedrückt, und tippen oder klicken dann auf *Deaktivieren*. Wenn Sie kein Programm als Fehlerquelle ermitteln können, ist vielleicht eine Windows-Komponente, ein Dienst oder ein Gerätetreiber die Ursache des Problems.

ACHTUNG

Deaktivieren Sie nur die Programme, die Sie als potenzielle Probleme einstufen, und tun Sie das nur dann, wenn Sie wissen, welche Aufgabe das Programm hat. Wenn Sie nicht wissen, was ein Programm tut, deaktivieren Sie es nicht. Manchmal kann man mehr über ein Autostartprogramm in Erfahrung bringen, indem man seinen Befehlspfad überprüft und seinen Installationsordner untersucht.

Aktivieren und Deaktivieren von Diensten zur Problembehebung

So wie automatisch gestartete Anwendungen in einem System Probleme verursachen können, so können dies auch automatisch gestartete Dienste. Um Probleme mit Diensten einzugrenzen, können Sie bestimmte Dienste zeitweilig mit dem Systemkonfigurationsprogramm deaktivieren, das System neu starten und dann überprüfen, ob das Problem noch auftritt. Ist das nicht mehr der Fall, haben Sie vermutlich den Verursacher gefunden. Dann können Sie den betreffenden Dienst dauerhaft deaktivieren oder beim Hersteller anfragen, ob eine aktualisierte Version des Dienstes verfügbar ist.

Zur temporären Deaktivierung eines Dienstes gehen Sie folgendermaßen vor:

1. Öffnen Sie das Systemkonfigurationsprogramm, indem Sie im Suchfeld *Apps* **msconfig** eingeben und dann die EINGABETASTE drücken, oder indem Sie auf dem Anwendungsbildschirm auf die entsprechende Option tippen oder klicken.
2. Tippen oder klicken Sie auf die Registerkarte *Dienste*. Wie in Abbildung 2.14 zu sehen, zeigt diese Registerkarte eine Liste aller Dienste an, die auf dem Computer installiert sind. In dieser Liste sind der Status des Dienstes, etwa *Wird ausgeführt* oder *Beendet*, und der Hersteller aufgeführt. Dienste, die nicht von Microsoft stammen, finden Sie leichter, wenn Sie das Kontrollkästchen *Alle Microsoft-Dienste ausblenden* aktivieren.

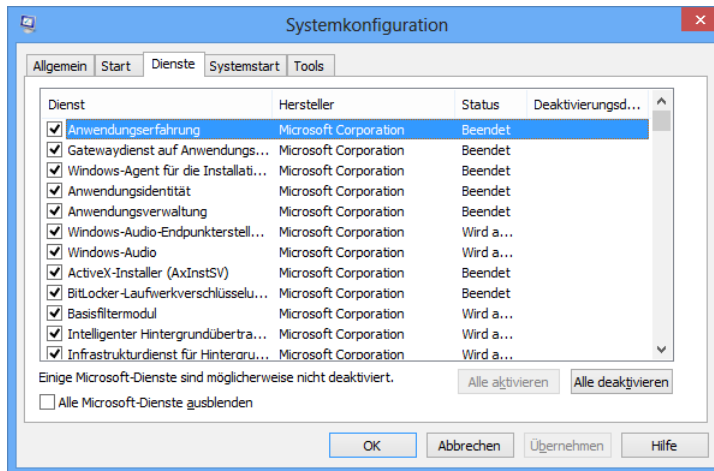


Abbildung 2.14 Verwenden Sie die Registerkarte *Dienste* zur Behebung von Problemen mit Windows-Diensten

3. Löschen Sie das Kontrollkästchen neben jedem Dienst, der beim nächsten Systemstart nicht ausgeführt werden soll.

ACHTUNG Deaktivieren Sie nur solche Dienste, die Sie als potenzielle Problemverursacher eingestuft haben. Tun Sie dies nur dann, wenn Sie wissen, welche Bedeutung der Dienst für das Betriebssystem hat. Wenn Sie nicht wissen, was ein Dienst tut, deaktivieren Sie ihn nicht. Auf der Registerkarte *Dienste* des Systemkonfigurationsprogramms erfahren Sie keine weiteren Einzelheiten über Dienste. Welche Aufgaben ein Dienst hat, können Sie mit dem *Dienste*-Programm, das Teil der Computerverwaltung ist, in Erfahrung bringen. Wählen Sie in diesem Programm einen Dienst aus und sehen Sie sich auf der Registerkarte *Erweitert* die dazugehörige Beschreibung an. Oder tippen oder klicken Sie den betreffenden Dienst doppelt an und lesen die Beschreibung auf der Registerkarte *Allgemein* des dazugehörigen Eigenschaftendialogfelds durch.

4. Tippen oder klicken Sie auf *OK*. Sie müssen das System neu starten, damit die Änderungen wirksam werden. Tippen oder klicken Sie also auf *Neu starten*, wenn Sie aufgefordert werden, das System neu zu starten. Oder starten Sie das System manuell neu.
5. Wiederholen Sie diese Prozedur, bis Sie den Dienst gefunden haben, der das Problem verursacht. Wenn Sie keinen Dienst als Fehlerquelle ermitteln können, ist vielleicht eine Windows-Komponente, eine Startanwendung oder ein Gerätetreiber die Ursache des Problems.

Verwalten der Systemeigenschaften

Zum Verwalten der Systemeigenschaften verwenden Sie das Dialogfeld *Systemeigenschaften*. Die folgenden Abschnitte beschreiben Schlüsselbereiche des Betriebssystems, die mit dem Dialogfeld *Systemeigenschaften* konfiguriert werden können.

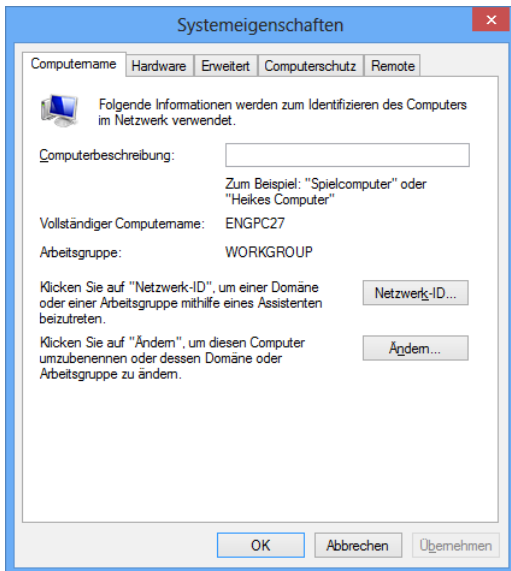


Abbildung 2.15 Mit der Registerkarte *Computernamen* können Sie die Systemidentifikation anzeigen und konfigurieren

Die Registerkarte *Computername*

Die Netzwerkidentifikation eines Computers kann mit der Registerkarte *Computername* des Dialogfelds *Systemeigenschaften* angezeigt und geändert werden (Abbildung 2.15). Wie aus der Abbildung hervorgeht, zeigt die Registerkarte *Computername* den vollständigen Computernamen des Systems und die Domänenmitgliedschaft an. Der vollständige Computernamen ist der DNS-Name (Domain Name System) des Computers, der auch den Platz des Computers in der Active Directory-Hierarchie angibt.

Um das Dialogfeld *Systemeigenschaften* zu öffnen, halten Sie die verborgene Schaltfläche in der unteren linken Ecke des *Start*- oder *Desktop*-Bildschirms gedrückt oder klicken sie mit der rechten Maustaste an, wählen im Kontextmenü *System* und tippen oder klicken dann auf die Verknüpfung *Einstellungen ändern*. Oder geben Sie im *Apps*-Suchfeld `sysdm.cpl` ein und drücken Sie dann die EINGABETASTE.

Mit den Optionen auf der Registerkarte *Computername* können Sie:

- **Einen Computer zu einer Domäne hinzufügen** Tippen oder klicken Sie auf *Netzwerk-ID*, um den Assistenten *Einer Domäne oder Arbeitsgruppe beitreten* zu öffnen, der Sie durch die erforderlichen Änderungen der Netzwerkzugangsinformationen führt.
- **Einen Computernamen ändern** Tippen oder klicken Sie auf *Ändern*, um den Computernamen und die Zugehörigkeit des Computers zu einer Domäne oder Gruppe zu ändern.

PRAXISTIPP

Bevor Sie versuchen, einen Computer zu einer Domäne hinzuzufügen, müssen Sie sicherstellen, dass die IP-Adressenkonfiguration (inklusive der DNS-Einstellungen) für das Netzwerk richtig sind, an das der Computer angeschlossen ist. Damit Clientcomputer DNS sinnvoll nutzen können, sollte der Computer einen passenden Computernamen und ein korrekt konfiguriertes primäres DNS-Suffix erhalten. Statt mehr oder weniger raffinierter oder zufälliger Namen sollten Sie sich für eine Namensgebung entscheiden, die für beide Benutzergruppen verständlich ist, nämlich für Benutzer und Administratoren. Im DNS dient der Computernamen als Hostname, und das primäre DNS-Suffix gibt die Domäne an, zu welcher der Computer gehört. Wird auf einem Computer nur ein Hostname ohne DNS-Suffix benutzt, dient das primäre DNS-Suffix zur Zuordnung des Namens. Nehmen wir zum Beispiel an, Sie sind auf einem Computer angemeldet, dessen primäres DNS-Suffix *tech.cpandl.com* lautet, und Sie senden auf einer Befehlszeile einen Ping an *Corpsvr28*. Der Computer leitet die Anfrage an *corpsvr28.tech.cpandl.com* weiter.

Standardmäßig gibt das primäre DNS-Suffix die Domäne an, deren Mitglied der Computer ist. Sie können das primäre DNS-Suffix eines Computers bei Bedarf ändern. Wenn das primäre DNS-Suffix eines Computers zum Beispiel *seattle.tech.cpandl.com* lautet, könnten Sie es auf *cpandl.com* umstellen, um die Namensauflösung in dieser umfangreichen DNS-Hierarchie zu vereinfachen. Zur Änderung des primären DNS-Suffixes tippen oder klicken Sie auf der Registerkarte *Computername* auf *Ändern* und dann auf *Weitere*. Geben Sie im entsprechenden Textfeld das primäre DNS-Suffix ein und schließen Sie dann alle geöffneten Dialogfelder, indem Sie auf die entsprechende Schaltfläche *OK* oder *Schließen* klicken.

Die Registerkarte *Hardware*

Die Registerkarte *Hardware* des Dialogfelds *Systemeigenschaften* bietet Zugriff auf den Geräte-Manager und die Geräteinstallationseinstellungen.

Um das Dialogfeld *Systemeigenschaften* zu öffnen, halten Sie die verborgene Schaltfläche in der unteren linken Ecke des *Start*- oder *Desktop*-Bildschirms gedrückt oder klicken sie mit der rechten Maustaste an, wählen im Kontextmenü *System* und tippen oder klicken dann auf die Verknüpfung *Erweiterte Systemeinstellungen*. Die wichtigsten Optionen, mit denen Sie auf der Registerkarte *Hardware* arbeiten werden, sind die Geräteinstallationseinstellungen.

Wenn Sie ein neues Gerät anschließen, sucht Windows 8 mit Windows Update automatisch nach neuen Treibern. Wenn Sie nicht möchten, dass der Computer automatisch nach neuen Treibern sucht, tippen

oder klicken Sie auf die Schaltfläche *Geräteinstallationseinstellungen*, wählen dann entweder *Ja, automatisch ausführen* oder *Nein, zu installierende Software selbst auswählen* und klicken auf *Änderungen speichern* und OK.

HINWEIS

Die Schaltfläche *Geräte-Manager* öffnet den Geräte-Manager in einer MMC (Microsoft Management Console). Der Geräte-Manager ist auch in der Computerverwaltungskonsolle als MMC-Snap-In enthalten und wird in Kapitel 9 besprochen.

Die Registerkarte *Erweitert*: Leistungsoptionen

Die Registerkarte *Erweitert* des Dialogfelds *Systemeigenschaften* bietet Zugang zu vielen Schlüsselfunktionen des Windows-Betriebssystems, wie beispielsweise die Leistung von Anwendungen, die Größe des virtuellen Speichers, Benutzerprofile, Umgebungsvariablen und das Verhalten beim Starten und Wiederherstellen.

Die Leistungsoptionen sind eine Teilmenge der erweiterten Konfigurationseinstellungen, die im Dialogfeld *Leistungsoptionen* zugänglich sind. Dieses Dialogfeld erreichen Sie auf folgende Weise:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie in der Konsole *System* auf *Einstellungen ändern* oder im linken Teil der Seite auf *Erweiterte Systemeinstellungen*.
3. Um das Dialogfeld *Leistungsoptionen* zu öffnen, tippen oder klicken Sie im Dialogfeld *Systemeigenschaften* auf die Registerkarte *Erweitert* und dann unter *Leistung* auf *Einstellungen*.

Um das Dialogfeld *Leistungsoptionen* direkt zu öffnen, geben Sie im Suchfeld *Apps* **SystemPropertiesPerformance** ein und drücken die EINGABETASTE.

Einstellen der Windows-Leistung

Die Oberfläche von Windows 8 wurde um viele grafische Elemente erweitert. Zu diesen Erweiterungen zählen zahlreiche visuelle Effekte für Menüs, Symbolleisten, Fenster und die Taskleiste. Im Dialogfeld *Leistungsoptionen* können Sie die Leistung von Windows genauer einstellen.

Die Registerkarte *Visuelle Effekte* ist im Dialogfeld *Leistungsoptionen* standardmäßig vorgewählt. Zur Steuerung der visuellen Effekte stehen Ihnen folgende Optionen zur Verfügung:

- **Optimale Einstellung automatisch auswählen** Ermöglicht es dem Betriebssystem, die Leistungseinstellung an der verfügbaren Hardware auszurichten. Bei einem neueren Computer entspricht das Ergebnis wahrscheinlich der Option *Für optimale Darstellung anpassen*. Der maßgebliche Unterschied ist aber, dass Windows bei der Entscheidung die Leistungsfähigkeit der verfügbaren Hardware berücksichtigt.
- **Für optimale Darstellung anpassen** Um Windows für die optimale Darstellung zu optimieren, aktivieren Sie alle visuellen Effekte für alle grafischen Benutzeroberflächen. Menüs und die Taskleiste verwenden Überblendungen und Schatten. Die Ränder der Schriftzeichen werden bei der Darstellung auf dem Bildschirm geglättet. Listenfelder führen einen weichen Bildlauf durch. Ordner zeigen ihre Inhalte mit Webansichten, und so weiter.
- **Für optimale Leistung anpassen** Durch die Leistungsoptimierung schalten Sie ressourcenintensive visuelle Effekte ab, beispielsweise Überblendungen und geglättete Ränder bei der Schriftdarstellung. Eine gewisse Grundmenge an visuellen Effekten bleibt aber erhalten.

- **Benutzerdefiniert** Sie können die gewünschten visuellen Effekte detailliert einstellen, indem Sie die entsprechenden Kontrollkästchen im Dialogfeld *Leistungsoptionen* aktivieren oder deaktivieren. Wenn Sie alle Kontrollkästchen deaktivieren, verwendet Windows keine visuellen Effekte.

Wenn Sie die gewünschten visuellen Effekte eingestellt haben, tippen oder klicken Sie auf *Übernehmen*. Schließen Sie alle offenen Dialogfelder jeweils durch tippen oder klicken auf OK.

Einstellen der Anwendungsleistung

Die Leistung der Anwendungen hängt davon ab, wie viel Laufzeit Windows 8 den entsprechenden Threads zuteilt. Von der Laufzeitzuteilung ist auch die Reaktionsfähigkeit interaktiver Anwendungen abhängig (im Gegensatz zu Anwendungen, die beispielsweise als Dienste im Hintergrund ausgeführt werden). Sie können die Anwendungsleistung mit den Optionen auf der Registerkarte *Erweitert* des Dialogfelds *Leistungsoptionen* einstellen. Dieses Dialogfeld können Sie zum Beispiel öffnen, indem Sie im Apps-Suchfeld **SystemPropertiesPerformance** eingeben und die EINGABETASTE drücken.

Im Bereich *Prozessorzeitplanung* stehen Ihnen auf der Registerkarte *Erweitert* des Dialogfelds *Leistungsoptionen* folgende Optionen zur Verfügung:

- **Programme** Wenn die aktive Anwendung die beste Reaktionszeit aufweisen und den größten Anteil an den verfügbaren Ressourcen erhalten soll, wählen Sie *Programme*. Das ist die Standardoption für alle Windows 8-Arbeitsstationen.
- **Hintergrunddienste** Wenn Hintergrundanwendungen bessere Reaktionszeiten als die aktive Anwendung erhalten sollen, wählen Sie *Hintergrunddienste*. Im Allgemeinen ist das die bevorzugte Einstellung für Windows 8-Computer, die als Server eingesetzt werden (damit ist gemeint, dass sie Aufgaben eines Servers übernehmen und nicht als Windows 8-Arbeitsstationen eingesetzt werden). Beispielsweise kann ein Windows 8-Computer als Druckserver der Abteilung eingesetzt werden.

Wenn Sie die Leistungseinstellung ändern, tippen oder klicken Sie anschließend auf *Übernehmen*.

Konfigurieren des virtuellen Arbeitsspeichers

Mithilfe von virtuellem Speicher ist es möglich, Speicherplatz von einem Laufwerk als Erweiterung des verfügbaren Arbeitsspeichers (RAM) zu verwenden. Für diese Funktion ist eine Auslagerung von nicht benötigten Speicherseiten auf einen Datenträger erforderlich. Dafür wird eine spezielle Datei bereitgestellt, die Auslagerungsdatei genannt wird und eine zuvor festgelegte Größe annehmen kann, beispielsweise 4096 MByte. Bei Bedarf können ausgelagerte Seiten später wieder aus der Auslagerungsdatei eingelesen werden. Eine erste Auslagerungsdatei wird automatisch auf dem Laufwerk angelegt, auf dem das Betriebssystem installiert wird. Auf anderen Laufwerken werden keine Auslagerungsdateien erstellt und müssen bei Bedarf manuell erstellt werden. Wenn Sie manuell eine Auslagerungsdatei erstellen, geben Sie eine Anfangsgröße und eine maximale Größe an. Auslagerungsdateien erhalten den Namen *Pagefile.sys*.

PRAXISTIPP

Gewöhnlich macht Windows 8 die Auslagerungsdatei anfangs mindestens so groß, wie es der auf dem Computer installierten Speichermenge entspricht. Auf diese Weise wird verhindert, dass die Auslagerungsdateien fragmentieren, was zu einer schlechten Systemleistung führen könnte. Wenn Sie den virtuellen Arbeitsspeicher von Hand verwalten wollen, können Sie die Fragmentierung gering halten, indem Sie für die Auslagerungsdatei eine Anfangsgröße einstellen, die mindestens der Gesamtgröße des RAM entspricht. In Computern mit 4 GByte oder weniger RAM sollten Sie die maximale Größe mindestens auf das Doppelte des gesamten RAM setzen. Bei Computern, die über 4 GByte RAM haben, sollten Sie die maximale Größe mindestens auf das 1,5-Fache des gesamten RAM setzen (oder auf die Größe, die der Hersteller des Computers empfiehlt). Das hilft dabei, die Auslagerungsdatei konsistent zu halten, sodass fortlaufende Blöcke geschrieben werden können (sofern möglich angesichts der Kapazität auf dem Volume).

Gehen Sie folgendermaßen vor, um den virtuellen Arbeitsspeicher von Hand zu konfigurieren:

1. Öffnen Sie das Dialogfeld *Leistungsoptionen*, beispielsweise indem Sie im *Apps*-Suchfeld **SystemPropertiesPerformance** eingeben und die **EINGABETASTE** drücken.
2. Tippen oder klicken Sie auf der Registerkarte *Erweitert* auf **Ändern**, um das Dialogfeld *Virtueller Arbeitsspeicher* zu öffnen (Abbildung 2.16). Folgende Informationen werden angezeigt:
 - **Laufwerk [Bezeichnung] und Auslagerungsdatei (MB)** Zeigt die Größe der Auslagerungsdateien, die derzeit auf dem System konfiguriert sind. Jedes Laufwerk wird mit seiner Auslagerungsdatei angezeigt, sofern vorhanden. Für manuell erstellte Auslagerungsdateien werden die festgelegte Anfangsgröße und die maximale Größe angezeigt.
 - **Gesamtgröße der Auslagerungsdatei für alle Laufwerke** Gibt eine Empfehlung für die Größe der Auslagerungsdatei auf dem System und gibt die aktuell zugeteilte Größe der Auslagerungsdatei an. Falls Sie das erste Mal eine Auslagerungsdatei konfigurieren, beachten Sie bitte, dass die empfohlene Dateigröße in den meisten Fällen bereits auf dem Systemlaufwerk reserviert wurde, was auch unter der vom System verwalteten Größe angezeigt wird.

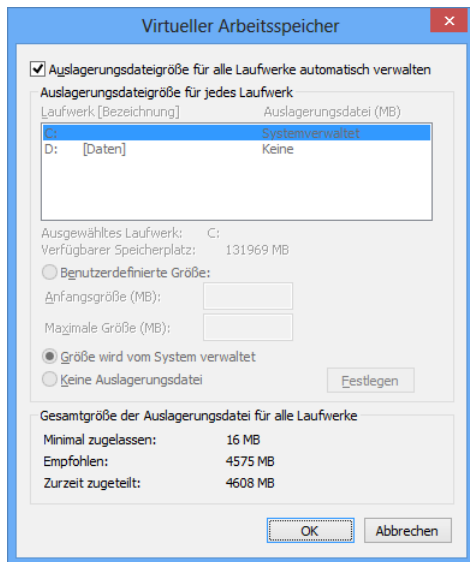


Abbildung 2.16 Der virtuelle Arbeitsspeicher erweitert die Menge des tatsächlich installierten Arbeitsspeichers

3. Standardmäßig verwaltet Windows 8 die Größen der Auslagerungsdateien auf allen Laufwerken. Wenn Sie die Auslagerungsdateien manuell konfigurieren möchten, deaktivieren Sie das Kontrollkästchen *Auslagerungsdateigröße für alle Laufwerke automatisch verwalten*.
4. Wählen Sie in der Liste *Laufwerk* das Laufwerk aus, mit dem Sie arbeiten möchten.
5. Wählen Sie *Benutzerdefinierte Größe* und legen Sie dann eine Anfangsgröße und eine maximale Größe fest.
6. Tippen oder klicken Sie auf *Festlegen*, um die Änderungen zu speichern.
7. Wiederholen Sie die Schritte 4 bis 6 für jedes Laufwerk, das Sie konfigurieren möchten.

8. Tippen oder klicken Sie auf *OK*. Wenn Sie gefragt werden, ob Sie eine vorhandene Datei *Pagefile.sys* überschreiben möchten, tippen oder klicken Sie auf *Ja*.
9. Wenn Sie Einstellungen für eine Auslagerungsdatei ändern, die gerade benutzt wird, erscheint eine Meldung, die Sie darüber informiert, dass Sie das System neu starten müssen, damit die Änderungen wirksam werden. Tippen oder klicken Sie auf *OK*.
10. Tippen oder klicken Sie zweimal auf *OK*, um die offenen Dialogfelder zu schließen. Wenn Sie das Dienstprogramm *System* schließen, wird eine Meldung mit dem Hinweis angezeigt, dass die Änderungen erst bei einem Neustart des Computers wirksam werden.

Sie können Windows 8 mit folgenden Schritten so einstellen, dass es die Auslagerungsdateien automatisch verwaltet:

1. Tippen oder klicken Sie auf der Registerkarte *Erweitert* auf *Ändern*, um das Dialogfeld *Virtueller Arbeitsspeicher* zu öffnen.
2. Wählen Sie das Kontrollkästchen *Auslagerungsdateigröße für alle Laufwerke automatisch verwalten*.
3. Schließen Sie alle geöffneten Dialogfelder, indem Sie jeweils auf *OK* klicken.

TIPP Es ist eine empfohlene Sicherheitsmaßnahme, beim Herunterfahren des Systems die Auslagerungsdatei zu löschen. Das können Sie durch die Aktivierung der Richtlinie *Herunterfahren: Auslagerungsdatei des virtuellen Arbeitsspeichers löschen* unter *Lokale Richtlinien\Sicherheitsoptionen* erreichen.

Konfigurieren der Datenausführungsverhinderung

Die Datenausführungsverhinderung (Data Execution Prevention, DEP) ist eine Speicherschutztechnologie. Sie weist den Prozessor des Computers an, alle Speicherbereiche in einer Anwendung als nicht ausführbar zu kennzeichnen, sofern der betreffende Bereich nicht ausdrücklich ausführbaren Code enthält. Wenn Code auf einer Speicherseite ausgeführt werden soll, die als nicht ausführbar gekennzeichnet ist, kann der Prozessor eine Ausnahme auslösen und die Ausführung verhindern. Das hindert bösartigen Code wie beispielsweise einen Virus in den meisten Speicherbereichen daran, sich selbst in den betreffenden Bereich einzufügen, denn nur bestimmte Bereiche des Speichers sind so gekennzeichnet, dass sie ausführbaren Code enthalten können.

HINWEIS 32-Bit-Versionen von Windows unterstützen die Datenausführungsverhinderung, wie sie von Prozessoren der Firma Advanced Micro Devices (AMD) ermöglicht wird, die einen No-Execute-Speicherseitenschutz (NX) bieten. Solche Prozessoren unterstützen die entsprechenden Befehle und müssen im PAE-Modus (Physical Address Extension) arbeiten, um große Speicherkonfigurationen zu unterstützen. Auch 64-Bit-Versionen von Windows unterstützen die NX-Prozessorfunktion, sie brauchen aber nicht PAE, um große Arbeitsspeicherkonfigurationen zu unterstützen.

Um zur Datenausführungsverhinderung kompatibel zu sein, müssen Anwendungen in der Lage sein, Speicher explizit mit der Execute-Berechtigung zu kennzeichnen. Anwendungen, die das nicht können, sind nicht zur NX-Prozessorfunktion kompatibel. Wenn bei der Ausführung von Anwendungen Probleme auftreten, die mit dem Speicher zu tun haben, sollten Sie diese Anwendungen als Ausnahmen konfigurieren, statt den Ausführungsschutz vollständig abzuschalten. Auf diese Weise bleiben Ihnen die Vorteile des Speicherschutzes erhalten und Sie können ihn selektiv für die Anwendungen abschalten, die mit der NX-Prozessorfunktion nicht ordnungsgemäß arbeiten.

Der Ausführungsschutz wird auf Benutzermodus- und Kernelmodusprogramme angewendet. Kommt es im Benutzermodus zu einer Ausführungsschutzverletzung, wird eine `STATUS_ACCESS_VIOLATION`-Ausnahme ausgelöst. In den meisten Fällen wird diese Ausnahme wahrscheinlich nicht behandelt und hat die Beendigung des betreffenden Prozesses zur Folge. Das ist auch das gewünschte Verhalten, denn die meisten Programme, die sich nicht an die Regeln halten, wie beispielsweise Viren oder Würmer, sind von bösartiger Natur.

Anders als bei den Anwendungen lässt sich der Ausführungsschutz für Kernelmodus Gerätetreiber nicht selektiv aktivieren oder deaktivieren. Außerdem wirkt der Ausführungsschutz auf konformen 32-Bit-Systemen standardmäßig auf den Stapel. Auf konformen 64-Bit-Systemen wirkt der Ausführungsschutz auf den Stapel, den ausgelagerten Pool und den Sitzungspool. Eine Ausführungsschutzverletzung im Kernelmodus, die in einem Gerätetreiber auftritt, führt zu der Ausnahme `ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY`.

Ob ein Computer die Datenausführungsverhinderung unterstützt, können Sie mit dem Programm *System* ermitteln. Sofern er die Datenausführungsverhinderung unterstützt, können Sie die Datenausführungsverhinderung mit folgenden Schritten einstellen:

1. Öffnen Sie das Dialogfeld *Leistungsoptionen*, beispielsweise indem Sie im *Apps*-Suchfeld **SystemPropertiesPerformance** eingeben und die `ENTER` drücken.
2. Aus dem Text im unteren Teil der Registerkarte *Datenausführungsverhinderung* geht hervor, ob der Computer die Datenausführungsverhinderung unterstützt.
3. Wenn ein Computer die Datenausführungsverhinderung unterstützt und entsprechend eingestellt ist, können Sie die Datenausführungsverhinderung mit folgenden Optionen konfigurieren:
 - **Datenausführungsverhinderung nur für erforderliche Windows-Programme und -Dienste einschalten** Aktiviert die Datenausführungsverhinderung nur für Dienste, Programme und Komponenten des Betriebssystems. Das ist die standardmäßige und empfohlene Option für Computer, welche die Datenausführungsverhinderung unterstützen und entsprechend eingestellt sind.
 - **Datenausführungsverhinderung für alle Programme und Dienste mit Ausnahme der ausgewählten einschalten** Aktiviert die Datenausführungsverhinderung und lässt Ausnahmen zu. Wählen Sie diese Optionsschaltfläche und klicken Sie dann auf *Hinzufügen*, um die Programme anzugeben, die ohne Datenausführungsverhinderung ausgeführt werden sollen. Auf diese Weise wirkt die Datenausführungsverhinderung bei allen Programmen, mit Ausnahme der hier aufgeführten Programme.
4. Tippen oder klicken Sie auf *OK*.

Die Registerkarte *Erweitert*: Umgebungsvariablen

System- und Benutzerumgebungsvariablen werden im Dialogfeld *Umgebungsvariablen* eingestellt (Abbildung 2.17). So öffnen Sie dieses Dialogfeld:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie im linken Bereich der Konsole *System* auf *Erweiterte Systemeinstellungen*.
3. Tippen oder klicken Sie auf der Registerkarte *Erweitert* des Dialogfelds *Systemeigenschaften* auf *Umgebungsvariablen*.

HINWEIS

Wenn Sie im Suchfeld *Apps* **SystemPropertiesAdvanced** eingeben und dann die `ENTER` drücken, öffnen Sie das Dialogfeld *Systemeigenschaften* mit aufgeschlagener Registerkarte *Erweitert* und können dann auf *Umgebungsvariablen* tippen oder klicken.

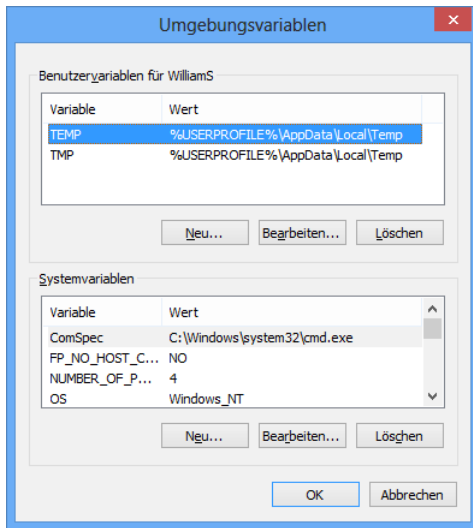


Abbildung 2.17 Das Dialogfeld *Umgebungsvariablen* ermöglicht die Einstellung von System- und Benutzerumgebungsvariablen

Erstellen einer Umgebungsvariablen

Wenn Sie eine Systemumgebungsvariable erstellen oder ändern, wird die Änderung erst nach dem Neustart des Computers wirksam. Erstellen oder ändern Sie eine Benutzerumgebungsvariable, so wird die Änderung bei der nächsten Anmeldung des betreffenden Benutzers auf dem Computer wirksam.

Gehen Sie folgendermaßen vor, um eine Umgebungsvariable zu erstellen:

1. Öffnen Sie das Dialogfeld *Umgebungsvariablen*, wie bereits beschrieben.
2. Tippen oder klicken Sie je nach Bedarf unter *Benutzervariablen* oder unter *Systemvariablen* auf *Neu*. Dadurch öffnet sich das Dialogfeld *Neue Benutzervariable* oder *Neue Systemvariable*.
3. Geben Sie im Feld *Name der Variablen* den Namen der Variablen ein. Geben Sie dann im Feld *Wert der Variablen* den Variablenwert ein. Tippen oder klicken Sie auf *OK*.

PRAXISTIPP

Der Befehlspfad für ausführbare Dateien wird über die Variable *Path* verwaltet. Wie Sie diese Variable bearbeiten, um den Befehlspfad zu ändern, wird im Abschnitt »Verwalten des Befehlspfads« in Kapitel 8 beschrieben.

WEITERE INFORMATIONEN

Benutzerprofile enthalten globale Benutzereinstellungen und Konfigurationsdaten. Sie werden erstellt, wenn sich ein Benutzer das erste Mal an einem lokalen Computer oder an einer Domäne anmeldet. Die Benutzerprofile von lokalen Konten unterscheiden sich von den Benutzerprofilen von Domänenkonten. Das Profil eines Benutzers speichert beispielsweise die Desktopeinstellung eines Benutzers, damit der Desktop jedes Mal wiederhergestellt werden kann, wenn sich der Benutzer anmeldet. Eine ausführliche Beschreibung der Benutzerprofile finden Sie in Kapitel 11, »Managing Existing User and Group Accounts«, des Buchs *Microsoft Windows Server 2012 – Ratgeber für Administratoren* (Microsoft Press, 2012).

Gehen Sie folgendermaßen vor, um die Gruppenrichtlinien zu öffnen und mithilfe eines Einstellungselements auf mehreren Computern in einer ganzen Domäne eine Umgebungsvariable zu erstellen:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und dann *Umgebung* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und *Umgebung* auswählen.
2. Halten Sie den Knoten *Umgebung* gedrückt oder klicken Sie ihn mit der rechten Maustaste an, und wählen Sie im Kontextmenü den Befehl *Neu/Umgebungsvariable*. Daraufhin öffnet sich das Dialogfeld *Neue Umgebungseigenschaften*.
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Erstellen* aus. Wählen Sie anschließend die Option *Benutzervariable* aus, wenn Sie eine Benutzervariable erstellen wollen, oder *Systemvariable*, um eine Systemvariable zu erstellen.
4. Geben Sie im Textfeld *Name* den Namen der Variablen ein und im Textfeld *Wert* den Variablenwert.
5. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsame Optionen* fest, wie die Einstellungen angewendet werden. In den meisten Fällen soll die Variable einfach nur einmal erstellt werden. Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmalig anwenden*.
6. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Bearbeiten einer Umgebungsvariablen

Vorhandene Umgebungsvariablen können Sie folgendermaßen bearbeiten:

1. Öffnen Sie das Dialogfeld *Umgebungsvariablen*, wie bereits beschrieben.
2. Wählen Sie je nach Typ der Variablen eine Variable aus der Liste *Benutzervariablen* oder *Systemvariablen* aus.
3. Tippen oder klicken Sie unter der entsprechenden Liste *Benutzervariablen* oder *Systemvariablen* auf *Bearbeiten*. Dadurch öffnet sich das Dialogfeld *Benutzervariable bearbeiten* oder *Systemvariable bearbeiten*.
4. Geben Sie im Feld *Wert der Variablen* den neuen Variablenwert ein und tippen oder klicken Sie auf *OK*.

Gehen Sie folgendermaßen vor, um die Gruppenrichtlinien zu öffnen und mithilfe eines Einstellungselements auf mehreren Computern in einer ganzen Domäne eine Umgebungsvariable zu aktualisieren:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt zum Bearbeiten. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und dann *Umgebung* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und *Umgebung* auswählen.
2. Halten Sie den Knoten *Umgebung* gedrückt oder klicken Sie ihn mit der rechten Maustaste an, und wählen Sie im Kontextmenü den Befehl *Neu/Umgebungsvariable*. Daraufhin öffnet sich das Dialogfeld *Neue Umgebungseigenschaften*.
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Aktualisieren* aus, wenn Sie die Variable ändern wollen, oder den Eintrag *Ersetzen*, um die Variable zu löschen und danach neu zu erstellen. Wählen

Sie anschließend die Option *Benutzervariable* aus, wenn Sie eine Benutzervariable erstellen wollen, oder *Systemvariable*, um eine Systemvariable zu erstellen.

4. Geben Sie im Textfeld *Name* den Namen der Variablen ein, die aktualisiert werden soll, und im Textfeld *Wert* den Variablenwert.
5. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. In den meisten Fällen soll die Variable nur einmal geändert werden. Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmalig anwenden*.
6. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Löschen einer Umgebungsvariablen

Wenn Sie im Dialogfeld *Umgebungsvariablen* arbeiten, können Sie eine Umgebungsvariable löschen, indem Sie sie aus der Liste auswählen und auf *Löschen* tippen oder klicken. Um eine Umgebungsvariable auf den Computern einer Domäne zu löschen, verwenden Sie Gruppenrichtlinien:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt zum Bearbeiten. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und dann *Umgebung* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und *Umgebung* auswählen.
2. Sie haben nun folgende Möglichkeiten:
 - Wenn bereits ein Einstellungselement für die Variable vorhanden ist, können Sie den Variablennamen doppelt antippen oder anklicken, um das entsprechende Eigenschaftendialogfeld zu öffnen. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Löschen*. Wählen Sie auf der Registerkarte *Gemeinsam* die gewünschten Optionen aus, zum Beispiel *Nur einmalig anwenden*, und tippen oder klicken Sie auf *OK*.
 - Wenn es noch kein Einstellungselement für die Variable gibt, die Sie von den Computern entfernen möchten, müssen Sie eines anlegen. Wie das geht, wurde weiter oben beschrieben. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Löschen* aus und stellen Sie auf der Registerkarte *Gemeinsam* die gewünschten Optionen ein.

Die Registerkarte *Erweitert*: Systemstart und Wiederherstellung

Die Eigenschaften für Systemstart und Wiederherstellung werden im Dialogfeld *Starten und Wiederherstellen* eingestellt (Abbildung 2.18). So öffnen Sie dieses Dialogfeld:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie in der Konsole *System* auf *Einstellungen ändern* oder im linken Bereich der Konsole auf *Erweiterte Systemeinstellungen*.
3. Um das Dialogfeld *Starten und Wiederherstellen* zu öffnen, tippen oder klicken Sie im Dialogfeld *Systemeigenschaften* auf die Registerkarte *Erweitert* und dann unter *Starten und Wiederherstellen* auf die Schaltfläche *Einstellungen*.

HINWEIS Wenn Sie im Suchfeld Apps **SystemPropertiesAdvanced** eingeben und dann die EINGABETASTE drücken, öffnen Sie das Dialogfeld *Systemeigenschaften* mit aufgeschlagener Registerkarte *Erweitert* und können dann auf *Umgebungsvariablen* tippen oder klicken.

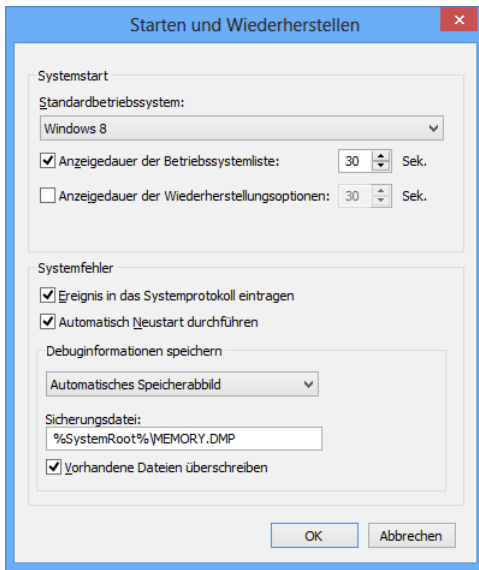


Abbildung 2.18 Im Dialogfeld *Starten und Wiederherstellen* können Sie verschiedene Eigenschaften für den Systemstart und das Wiederherstellen einstellen

Einstellen der Startoptionen

Der Bereich *Systemstart* des Dialogfelds *Starten und Wiederherstellen* steuert den Systemstart. Sind auf einem Computer mehrere startfähige Betriebssysteme installiert, können Sie das Standardbetriebssystem in der Dropdownliste *Standardbetriebssystem* auswählen. Diese Änderung wirkt sich auf die Konfiguration aus, die der Windows-Start-Manager verwendet.

Beim Start eines Computers, auf dem mehrere startfähige Betriebssysteme installiert sind, zeigt Windows 8 standardmäßig für 30 Sekunden ein Startmenü mit einer Betriebssystemliste an. Das können Sie auf verschiedene Weise beeinflussen:

- Den sofortigen Start des Standardbetriebssystems erreichen Sie durch das Deaktivieren des Kontrollkästchens *Anzeigedauer der Betriebssystemliste*.
- Die Anzeige der verfügbaren Optionen für eine bestimmte Zeitdauer erreichen Sie, indem Sie das Kontrollkästchen *Anzeigedauer der Betriebssystemliste* aktivieren und dann die gewünschte Zeitspanne (in Sekunden) festlegen.

Gewöhnlich ist auf den meisten Systemen ein Wert von 3 bis 5 Sekunden sinnvoll. Das ist lang genug, um bei Bedarf eine Auswahl zu treffen, und noch kurz genug, um den Systemstart nicht unnötig zu verzögern.

Wird ein System im Wiederherstellungsmodus gestartet, kann eine Liste mit Wiederherstellungsoptionen angezeigt werden. Wie bei den Standardstartoptionen können Sie auch hier das Startverhalten unterschiedlich festlegen. Durch die Deaktivierung des Kontrollkästchens *Anzeigedauer der Wiederherstellungsoptionen* erreichen Sie, dass der Computer mit der Standardwiederherstellungsoption sofort gestartet wird. Oder Sie aktivieren das Kontrollkästchen *Anzeigedauer der Wiederherstellungsoptionen* und legen dann eine Zeitspanne (in Sekunden) für die Anzeige der Optionen fest.

Einstellen der Wiederherstellungsoptionen

Die Bereiche *Systemfehler* und *Debuginformationen speichern* des Dialogfelds *Starten und Wiederherstellen* steuern die Systemwiederherstellung. Wiederherstellungsoptionen erlauben den Administratoren genau zu steuern, was beim Auftreten eines schwerwiegenden Systemfehlers (auch als Abbruchfehler oder STOP-Fehler bekannt) geschehen soll. Im Bereich *Systemfehler* sind folgende Optionen verfügbar:

- **Ereignis in das Systemprotokoll eintragen** Fehler werden ins Systemprotokoll eingetragen. Das ermöglicht es einem Administrator, die Fehlermeldung zu einem späteren Zeitpunkt in der Ereignisanzeige nachzulesen.
- **Automatisch Neustart durchführen** Aktivieren Sie diese Option, wenn das System nach einem schwerwiegenden Fehler automatisch einen Neustart versuchen soll.

HINWEIS

Die Konfiguration von automatischen Neustarts ist nicht immer eine gute Sache. Manchmal ist es besser, wenn ein System einfach stehen bleibt, statt neu zu starten, damit es vor einem Neustart überprüft werden kann. Sonst erfahren Sie vielleicht nur durch eine Überprüfung des Systemprotokolls, dass ein Neustart stattgefunden hat, oder wenn Sie beim Neustart zufällig vor dem Monitor des Computers sitzen.

Die Auswahlliste *Debuginformationen speichern* ermöglicht Ihnen die Auswahl der Art der Debuginformationen, die in eine Speicherabbilddatei geschrieben werden sollen. Die Speicherabbilddatei wiederum kann zur Untersuchung des Systemfehlers verwendet werden. Folgende Optionen stehen zur Verfügung:

- **Kein** Wählen Sie diese Einstellung, wenn keine Debuginformationen geschrieben werden sollen.
- **Kleines Speicherabbild** Wählen Sie diese Einstellung, wenn das physische Speichersegment gespeichert werden soll, in dem der Fehler aufgetreten ist. Die Größe des Abbilds beträgt 256 KByte.
- **Kernelspeicherabbild** Wählen Sie diese Einstellung, wenn der Bereich des physischen Arbeitsspeichers gespeichert werden soll, der vom Windows-Systemkern benutzt wird. Wie groß die Datei wird, hängt von der Größe des Windows-Systemkerns ab.
- **Vollständiges Speicherabbild** Wählen Sie diese Einstellung, wenn der gesamte physische Speicher gespeichert werden soll. Wie groß die Datei wird, hängt davon ab, wie stark der physische Speicher ausgelastet ist. Die Datei kann durchaus so groß werden, wie es der installierten RAM-Größe entspricht.
- **Automatisches Speicherabbild** Wählen Sie diese Einstellung, wenn Windows selbst ermitteln soll, welches Speicherabbild am besten geeignet ist, und die Datei entsprechend anlegen soll.

Wenn eine Speicherabbilddatei geschrieben werden soll, müssen Sie auch einen Speicherort dafür festlegen. Die Standardorte sind `%SystemRoot%\Minidump` für kleine Speicherabbilder und `%SystemRoot%\Memory.dmp` für alle anderen Speicherabbilder. Im Normalfall werden Sie auch das Kontrollkästchen *Vorhandene Dateien überschreiben* aktivieren. Diese Option sorgt dafür, dass vorhandene Speicherabbilddateien überschrieben werden, falls ein neuer Abbruchfehler auftritt.

EMPFOHLENE VORGEHENSWEISE

Eine Speicherabbilddatei kann nur erstellt werden, wenn das System entsprechend konfiguriert ist. Das Systemlaufwerk muss über eine hinreichend große Auslagerungsdatei verfügen (sie wird auf der Registerkarte *Erweitert* für den virtuellen Arbeitsspeicher eingestellt), und auf dem Laufwerk, auf dem die Speicherabbilddatei gespeichert werden soll, muss ebenfalls genügend freier Platz verfügbar sein. Für eine Kernel-Speicherabbilddatei werden 35 bis 50 Prozent des verfügbaren RAM benötigt. Wenn ein System also mit 16 GByte RAM ausgerüstet ist, müssen auf dem Laufwerk etwa 6 bis 8 GByte frei sein, damit eine Abbilddatei des Betriebssystemkerns geschrieben werden kann.

Die Registerkarte *Computerschutz*

Die Registerkarte *Computerschutz* des Dialogfelds *Systemeigenschaften* (Abbildung 2.19) ermöglicht die Konfiguration der Systemwiederherstellung. Sie erreichen diese Registerkarte folgendermaßen:

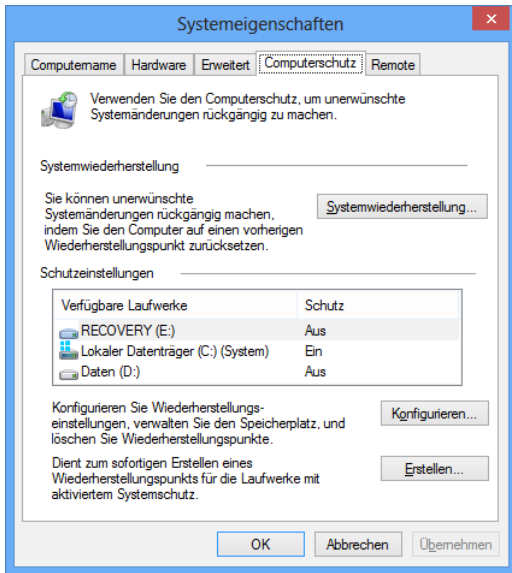


Abbildung 2.19 Das System verwaltet für jedes Laufwerk separate Wiederherstellungspunkte

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie in der Konsole *System* auf *Einstellungen ändern* oder im linken Bereich der Konsole auf *Erweiterte Systemeinstellungen*.
3. Tippen oder klicken Sie im Dialogfeld *Systemeigenschaften* auf die Registerkarte *Computerschutz*.

Sie können die Registerkarte *Computerschutz* des Dialogfelds *Systemeigenschaften* auch öffnen, indem Sie im Suchfeld Apps **SystemPropertiesProtection** eingeben und die EINGABETASTE drücken.

Im Gegensatz zu Windows 7 gehört die Komponente Vorgängerversionen nicht mehr zur Systemwiederherstellung. In Windows 8 stellen Sie ältere Versionen von persönlichen Dateien aus Dateiversionsverlaufsicherungen wieder her. Die folgenden Abschnitte beschreiben die Verwendung und Konfiguration der Systemwiederherstellung. Die Verwendung von Wiederherstellungspunkten zur Wiederherstellung eines Computers und von Dateiversionsverlaufsicherungen wird in Kapitel 10 besprochen.

PRAXISTIPP

Dateiserver, auf denen Windows Server 2012 ausgeführt wird, verfügen noch über die Funktion *Vorgängerversionen*. Vorgängerversionen stammen aus Schattenkopien und werden für Ordner erstellt, die im Netzwerk freigegeben wurden. Im Datei-Explorer weist das Eigenschaftendialogfeld für einen freigegebenen Ordner, der mit einem Netzlaufwerk verknüpft ist, die Registerkarte *Vorgängerversionen* auf. Verwenden Sie die Optionen auf dieser Registerkarte, um in einem freigegebenen Ordner eines Dateiservers Vorgängerversionen von Dateien wiederherzustellen.

Der Computerschutz

Bei aktivierter Systemwiederherstellung fertigt der Computer regelmäßig Abbilder der Systemkonfiguration an. Diese Abbilder heißen *Wiederherstellungspunkte*. Ein Wiederherstellungspunkt umfasst Windows-Einstellungen, eine Liste der installierten Programme und so weiter. Arbeitet ein Computer nicht richtig oder kann er wegen einer Änderung der Systemkonfiguration nicht richtig starten, können Sie das System mithilfe eines Wiederherstellungspunkts in den Zustand zurückversetzen, in dem er sich zu dem Zeitpunkt befand, an dem der Wiederherstellungspunkt aufgezeichnet wurde. Nehmen wir an, Ihr System arbeitet einwandfrei und Sie installieren ein neues Service Pack für Microsoft Office. Anschließend treten Fehler auf und die Office-Anwendungen laufen nicht. Sie versuchen, das Update zu deinstallieren, aber das nützt nichts. Also entschließen Sie sich zur Systemwiederherstellung. Mithilfe der Systemwiederherstellung können Sie das System in den Zustand zurückversetzen, der vor dem Update aufgezeichnet wurde.

HINWEIS

Die Systemwiederherstellung kennt verschiedene Arten von Wiederherstellungspunkten. Eine Art, der Systemwiederherstellungspunkt, wird vom Betriebssystem geplant und in regelmäßigen Abständen erstellt. Eine andere Art Wiederherstellungspunkt, der Installationswiederherstellungspunkt, wird automatisch erstellt, wenn Sie Anwendungen installieren. Andere Wiederherstellungspunkte, die manuellen Wiederherstellungspunkte, werden von den Benutzern erstellt. Sie sollten Benutzern empfehlen, vor der Durchführung einer Operation, die zu Problemen führen könnte, manuell einen Wiederherstellungspunkt zu erstellen.

Die Systemwiederherstellung verwaltet Wiederherstellungspunkte auf Laufwerksbasis. Jedes Laufwerk mit kritischen Anwendungen und Systemdateien sollte auf Konfigurationsänderungen überwacht werden. Standardmäßig ist die Systemwiederherstellung nur für das Systemlaufwerk aktiviert. Sie können die Konfiguration der Systemwiederherstellung ändern und nach Bedarf die Überwachung anderer Laufwerke aktivieren. Wenn ein Laufwerk nicht für die Überwachung durch die Systemwiederherstellung konfiguriert ist, werden Konfigurationsänderungen auf diesem Laufwerk nicht aufgezeichnet und das Laufwerk kann nicht in einen früheren Zustand zurückversetzt werden, falls Probleme auftreten.

HINWEIS

Systemschutzpunkte werden täglich für alle Laufwerke erstellt, die von der Systemwiederherstellung überwacht werden. Vorgängerversionen werden nicht als Teil eines automatisch oder manuell erstellten Systemschutzpunkts eines Laufwerks erstellt. Verwenden Sie stattdessen Dateiversionsverlaufsicherungen.

Konfigurieren der Systemwiederherstellung

Wie die Systemwiederherstellung arbeitet, können Sie auf der Registerkarte *Computerschutz* des Dialogfelds *Systemeigenschaften* festlegen. Der Systemprozess, der für die Überwachung von Änderungen in der Konfiguration und bei den Anwendungen zuständig ist, ist der Systemwiederherstellungsdienst. Dieser Dienst wird für den automatischen Start konfiguriert und mit dem lokalen Systemkonto ausgeführt. Die Systemwiederherstellung funktioniert nicht richtig, wenn der Dienst nicht ausgeführt wird oder nicht richtig konfiguriert wurde.

Die Systemwiederherstellung speichert Systemwiederherstellungspunktinformationen für alle überwachten Laufwerke und erfordert auf dem Systemlaufwerk mindestens 300 MByte freien Speicherplatz zur Speicherung von Wiederherstellungspunkten. Die Systemwiederherstellung reserviert bei Bedarf zusätzlichen Platz für Wiederherstellungspunkte, und zwar bis zu 100 Prozent der Laufwerkskapazität. Aber dieser zusätzliche Platz ist immer für die Speicherung durch Benutzer und Anwendungen verfügbar. Die Systemwiederherstellung gibt bei Bedarf zusätzlichen Speicherplatz für Sie frei. Wenn die Systemwieder-

herstellung nicht mehr genügend freien Speicherplatz findet, überschreibt das Betriebssystem zuvor erstellte Wiederherstellungspunkte.

Wie viel Platz die Systemwiederherstellung verwendet, können Sie konfigurieren. In der Standardeinstellung reserviert die Systemwiederherstellung mindestens 1 Prozent der gesamten Laufwerkskapazität zum Speichern von Wiederherstellungspunkten. Zum Beispiel reserviert die Systemwiederherstellung auf einer Festplatte mit einer Gesamtkapazität von 930 GByte standardmäßig 9,3 GByte.

Gehen Sie folgendermaßen vor, um die Systemwiederherstellung für jedes Laufwerk zu konfigurieren:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie im linken Fensterabschnitt der Konsole *System* auf *Computerschutz*.
3. Konfigurieren Sie die Systemwiederherstellung für ein Volume, indem Sie das gewünschte Volume in der Liste *Schutzeinstellungen* auswählen und auf *Konfigurieren* tippen oder klicken. Daraufhin öffnet sich das Dialogfeld *Systemschutz für* (Abbildung 2.20).

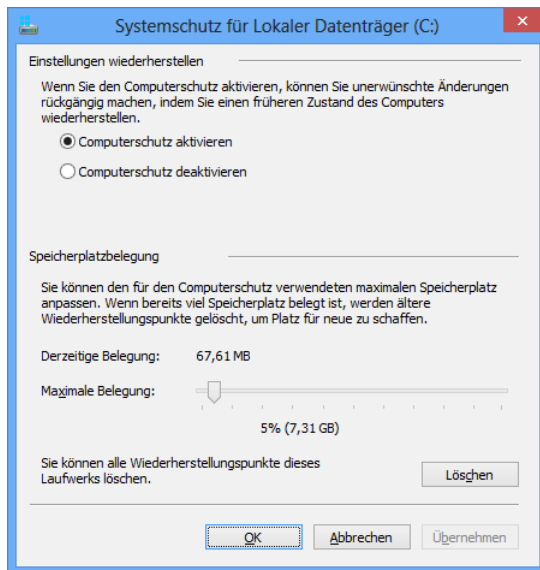


Abbildung 2.20 Konfigurieren der Systemwiederherstellung für ein bestimmtes Laufwerk

4. Wählen Sie eine der folgenden Optionen aus:
 - **Computerschutz aktivieren** Wählen Sie diese Option, wenn Sie Kopien der Systemeinstellungen aufbewahren möchten. Diese Option wird für das Systemvolume empfohlen, weil auf diese Weise sichergestellt ist, dass Sie den Computer wiederherstellen können.
 - **Computerschutz deaktivieren** Wählen Sie diese Option, um die Systemwiederherstellung auszuschaalten. Diese Option wird für das Systemvolume nicht empfohlen, weil es dann nicht möglich ist, den Computer nach Konfigurationsänderungen wiederherzustellen.
5. Wenn Sie den Systemschutz aktiviert haben, können Sie mit dem Schieberegler im Bereich *Speicherplatzbelegung* einstellen, wie viel Festplattenplatz die Systemwiederherstellung höchstens verwenden darf. Ist die Maximalgröße erreicht, löscht die Systemwiederherstellung ältere Wiederherstellungspunkte, um Platz für neue zu schaffen.

6. Tippen oder klicken Sie auf *OK*. (Falls Sie den Systemschutz deaktiviert haben, löscht Windows alle gespeicherten Systemeinstellungen und Sie müssen dies durch Antippen oder Anklicken von *Ja* bestätigen. Tippen oder klicken Sie gegebenenfalls auf *Schließen*, sobald Windows mit dem Löschen der Wiederherstellungspunkte fertig ist.)

Wenn Sie einen Computer mithilfe der Systemwiederherstellung schützen und absolut sicher sind, dass sich das System in stabilem Zustand befindet, können Sie alle gespeicherten Systemeinstellungen löschen, um Platz auf dem Datenträger frei zu machen oder sicherzustellen, dass Benutzer keinen ungeeigneten Wiederherstellungspunkt anwenden. Gehen Sie dazu folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie in der Konsole *System* im linken Fensterabschnitt auf *Computerschutz*.
3. Wählen Sie in der Liste *Schutzeinstellungen* das Volume aus, das Sie bearbeiten wollen, und tippen oder klicken Sie auf *Konfigurieren*.
4. Tippen oder klicken Sie auf *Löschen* und dann auf *Fortsetzen*, um zu bestätigen, dass Sie tatsächlich alle gespeicherten Systemeinstellungen entfernen wollen.
5. Warten Sie, bis Windows alle Wiederherstellungspunkte gelöscht hat, und tippen oder klicken Sie dann auf *Schließen*.

Die Registerkarte *Remote*

Die Registerkarte *Remote* des Dialogfelds *Systemeigenschaften* steuert Remoteunterstützungs- und Remotedesktopverbindungen. Diese Optionen werden in Kapitel 7 im Abschnitt »Verwalten des Remotezugriffs auf Arbeitsstationen« besprochen.

Konfigurieren der Energieverwaltung

Die Energieoptionen wirken sich darauf aus, wie sich ein Computer in verschiedenen Versorgungs- und Belastungssituationen verhält, beispielsweise bei Netz- oder bei Akkubetrieb. Im Prinzip sollten zwar alle Computer so eingestellt werden, dass sie möglichst wenig Strom verbrauchen, aber für Laptops ist dies besonders wichtig, zumal es einen Zusammenhang zwischen Leistung und Betriebsdauer gibt. In bestimmten Situationen nehmen Sie es vielleicht in Kauf, dass der Laptop nicht die volle Leistung bringt und langsamer reagiert, wenn er dafür mit einer Akkuladung länger betrieben werden kann. In anderen Situationen ziehen Sie vielleicht eine mittlere Leistung und eine mittlere Betriebsdauer pro Akkuladung vor. Oder Sie wollen alles an Leistung, was der Computer hergibt, auch wenn die Akkus dadurch schneller entladen werden.

Die wichtigsten Energieoptionen werden mit sogenannten Energieplänen verwaltet. Damit sind Zusammenstellungen von Energieeinstellungen gemeint, mit denen die Leistungsaufnahme und der Energieverbrauch gesteuert werden. Ein Computer kann über mehrere Energiepläne verfügen, von denen aber stets nur einer aktiv sein kann. Neben den Energieplänen wird auf den meisten Computern auch noch eingestellt, was geschehen soll, wenn der Netzschalter oder die Energiespartaste gedrückt werden. Beim Schließen des Deckels geht ein Laptop gewöhnlich in einen Energiesparmodus über, während ein längerer Druck auf den Netzschalter zum Herunterfahren des Computers führt und ein Druck auf die Energiespartaste ihn in einen Energiesparmodus versetzt. Durch systemweit geltende Einstellungen der Energieoptionen können Sie das Verhalten bei einem Druck auf den Netzschalter und den Kennwortschutz bei der Reaktivierung nach den Vorstellungen einzelner Benutzer oder Benutzergruppen einstellen.

Verwalten von Energieoptionen in der Befehlszeile

In Windows 8 gibt es ein Programm namens *Powercfg.exe*, mit dem sich Energieoptionen auf der Befehlszeile verwalten lassen. Sie können sich ansehen, welche Optionen für dieses Programm zur Verfügung stehen, indem Sie in einer Eingabeaufforderung **powercfg /?** eingeben. Zu den Parametern, die Sie am häufigsten verwenden werden, gehören:

- **-a** Listet die auf dem Computer verfügbaren Energiesparmodi und gegebenenfalls die Gründe auf, warum bestimmte Energiesparmodi nicht unterstützt werden.
- **-d [guid]** Löscht den Energiesparplan, der durch die GUID (Globally Unique Identifier) angegeben wird.
- **-devicequery all_devices** Listet detaillierte Informationen zur Energieverwaltung für alle Geräte des Computers auf. Leiten Sie die Ausgabe in eine Datei um, diese Liste ist nämlich sehr lang und ausführlich.
- **-energy** Prüft, ob auf dem System öfter vorkommende Konfigurations-, Geräte- und Akkuprobleme gibt, und generiert einen HTML-Bericht im aktuellen Arbeitsverzeichnis.
- **-h** Schaltet die Ruhezustandsfunktion ein oder aus.
- **-l** Listet die Energiesparpläne des Computers mit Namen und GUID auf.
- **-q [guid]** Zeigt den Inhalt des Energiesparplans an, der durch die GUID angegeben wird. Wenn Sie keine GUID angeben, wird der Inhalt des aktiven Energiesparplans aufgelistet.
- **-requests** Zeigt alle Energieverwaltungsanforderungen an, die von Gerätetreibern gesendet wurden. Gibt es ausstehende Anforderungen für den Bildschirm, verhindern diese Anforderungen, dass der Computer die Monitore automatisch abschaltet. Werden ausstehende Anforderungen für irgendein Gerät (inklusive Bildschirm) aufgeführt, verhindern diese Anforderungen, dass der Computer automatisch in einen stromsparenden Energiesparmodus wechselt.
- **-s [guid]** Macht den Energiesparplan, der durch die GUID angegeben wird, zum aktiven Energiesparplan.
- **-x [Einstellung] [Wert]** Setzt die angegebene Einstellung im aktiven Energiesparplan auf den angegebenen Wert.

HINWEIS Standardmäßig verwendet Windows 8 einen Hybridmodus und nicht den Ruhezustand. Der Ruhezustand sollte erst nach einer Überprüfung der Kompatibilität konfiguriert werden. Beachten Sie auch, dass Befehle für das Energiekonfigurationsprogramm (Powercfg) mit einem Bindestrich (-) oder mit einem Schrägstrich (/) angegeben werden können. Ich ziehe den Bindestrich wegen seiner Position auf der (amerikanischen) Tastatur vor.

Die folgenden Zeilen wurden nach der Eingabe des Befehls **powercfg -l** auf einer Befehlszeile angezeigt:

Bestehende Energieschemen (* Aktiv)

GUID des Energieschemas: 381b4222-f694-41f0-9685-ff5bb260df2e (Ausbalanciert)
 GUID des Energieschemas: 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c (Höchstleistung)
 GUID des Energieschemas: a1841308-3541-4fab-bc81-f71556f20b4a (Energiesparmodus)
 GUID des Energieschemas: c1d97820-3148-42a9-a587-75d618a9bb2b (Grafikabteilung) *

Der aktive Plan wird durch ein Sternchen gekennzeichnet. An dieser Liste können Sie ablesen, dass es auf dem Computer vier Energiesparpläne gibt und dass der Energiesparplan der Grafikabteilung der aktive Plan ist.

Wenn Sie mit `Powercfg` einen Energiesparplan einstellen oder ändern möchten, müssen Sie die Eingabeaufforderung mit erhöhten Rechten öffnen. Falls die Angabe einer GUID erforderlich ist, erhalten Sie den entsprechenden Wert am einfachsten, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten **`powercfg -l`** eingeben und dann den Wert des entsprechenden Energiesparplans kopieren. Soll beispielsweise der Plan *Ausbalanciert* aus dem obigen Beispiel der Standardplan für den Computer werden, geben Sie in einer Eingabeaufforderung mit erhöhten Rechten Folgendes ein:

```
powercfg -s 381b4222-f694-41f0-9685-ff5bb260df2e
```

Welche Energiesparmodi ein Computer unterstützt, erfahren Sie, indem Sie **`powercfg -a`** in einer Eingabeaufforderung eingeben. `Powercfg` listet detailliert auf, welche Modi unterstützt werden und welche nicht. Ein Beispiel:

Die folgenden Standbymodusfunktionen sind auf diesem System verfügbar:

Standby (S1 S3)

Ruhezustand

Hybrider Standbymodus

Die folgenden Standbymodusfunktionen sind auf diesem System nicht verfügbar:

Standby (S2)

Dieser Standbyzustand wird von der Systemfirmware nicht unterstützt.

Treten Probleme auf, wenn ein Computer versucht, in den Energiesparmodus oder den Ruhezustand zu schalten, können Sie unter Umständen mit `powercfg -a` feststellen, was die Ursache ist. Wenn die Firmware einen bestimmten Modus nicht unterstützt, hilft es manchmal, die Firmware zu aktualisieren, damit die Unterstützung für einen Modus nachgerüstet wird. Wird das Problem von einem Gerät verursacht, das einen bestimmten Modus nicht unterstützt, können Sie dieses Gerät vielleicht ausbauen und durch ein kompatibles Gerät ersetzen.

Sie können jederzeit die Energiesparkonfiguration und Gerätekompatibilität eines Computers auswerten, indem Sie einen Energieeffizienzdiagnosebericht erstellen. Geben Sie dazu in einer Eingabeaufforderung den Befehl **`powercfg -energy`** ein. Dann wird der Bericht als HTML-Dokument unter dem Namen *Energy-Report.html* generiert. Der Bericht listet auf, wie die Energieverwaltungscompatibilität der Geräte aussieht. Jedes Gerät, das keine ausreichende Unterstützung für die Energieverwaltung bietet, wird zusammen mit einer detaillierten Fehlerliste aufgeführt. Wenn beispielsweise ein USB-Gerät nicht richtig in den Standbymodus schaltet, erhalten Sie in diesem Bericht detaillierte Informationen über die aufgetretenen Fehler und die Gerätekonfiguration. Wurde eine Energieverwaltungsfähigkeit aufgrund eines Kompatibilitätsproblems deaktiviert, werden Sie darauf hingewiesen. Wenn zum Beispiel das Feature »PCI Express Active-State Power Management« von der Hardware nicht unterstützt wird und daher deaktiviert wurde, finden Sie einen entsprechenden Eintrag im Bericht. Auch Warnungen und zusätzliche Informationen über Geräte und Kompatibilität sind enthalten, darunter Details zu den unterstützten Energiesparmodi und den Energieverwaltungsfähigkeiten des Prozessors.

PRAXISTIPP

Bei Notebooks werden wichtige Informationen zur Akkuladung und der Akkulebensdauer gemeldet. Nähert sich ein Akku dem Ende seiner Lebensdauer, merken Sie das daran, dass die Betriebsdauer mit einer vollen Akkuladung immer kürzer wird. In diesem Fall zeigen die Akkuinformationen, dass der Akku nicht mehr so viel Kapazität besitzt, wie er sollte. Dann ist es gegebenenfalls sinnvoll, den Akku des Notebooks zu ersetzen.

Wenn Sie sich noch ausführlicher mit Energieverwaltungsproblemen beschäftigen müssen, können Sie sich umfassende Details zur Energieverwaltungsunterstützung bei jedem einzelnen Gerät des Computers besorgen, indem Sie folgenden Befehl eingeben:

```
powercfg -devicequery all_devices > power.txt
```

Die Informationen werden in der Datei *Power.txt* im aktuellen Arbeitsverzeichnis gespeichert.

Wenn Sie Windows PowerShell für die Remoteausführung konfiguriert haben, können Sie Powercfg ganz einfach auf mehreren Remotecomputern starten. Tragen Sie dazu die Namen aller Remotecomputer, die überprüft werden sollen, jeweils in einer eigenen Zeile in eine Datei namens *Computers.txt* ein und speichern Sie diese Datei. Öffnen Sie nun eine PowerShell-Eingabeaufforderung mit Administratorrechten und geben Sie folgende Befehle ein:

```
$comp = get-content c:\computers.txt
$s = new-ssession -computername $comp
invoke-command -session $s { powercfg.exe -energy }
```

Hier wurde die Datei mit den Computernamen als *C:\Computers.txt* bereitgestellt. Passen Sie diesen Pfad an, wenn Sie die Datei an einem anderen Ort gespeichert haben. Nun wird auf jedem Computer eine Datei namens *Energy-Report.html* erstellt und im Standardverzeichnis des Benutzerkontos gespeichert, unter dem Sie auf den Computer zugreifen. Wenn Sie das HTML-Dokument nicht von jedem einzelnen Computer abrufen wollen, können Sie den Bericht in eine Freigabe schreiben und den Computernamen in den Berichtsnamen einarbeiten, wie im folgenden Beispiel gezeigt:

```
$comp = get-content c:\computers.txt
$s = new-ssession -computername $comp
invoke-command -session $s { powercfg.exe -energy -output "\\fileserver46\data\$env:computername.html" }
```

Hier schreiben Sie den Bericht in die Freigabe *\\fileserver46\data* und setzen den Dateinamen mit dem Wert der Umgebungsvariablen *ComputerName* zusammen. Beachten Sie, dass Sie die Dateierweiterung *.exe* nach dem Programmnamen angeben müssen, wenn Sie mit PowerShell arbeiten und Befehle aufrufen, die als ausführbare Dateien vorliegen.

Verwenden von Energieplänen

Auf mobilen Computern zeigt die Taskleiste in ihrem Infobereich ein Energieversorgungssymbol. Ein Tippen oder Klicken auf dieses Symbol bewirkt die Anzeige des Ladezustands des Akkus und des verwendeten Energiesparplans. Durch das Antippen oder Anklicken der Verknüpfungen aus dem Benachrichtigungsdialogfeld lässt sich die Seite *Energieoptionen* der Systemsteuerung öffnen. Die meisten Konfigurationen von Windows 8 verfügen über drei bevorzugte Energiepläne:

- **Ausbalanciert** Ein Energieplan, der einen Kompromiss zwischen Energieverbrauch und Systemleistung schließt. Der Prozessor wird schneller, wenn mehr Rechenleistung gebraucht wird, und wieder langsamer, wenn eine geringere Rechenleistung erforderlich ist. Das ist der Standardenergieplan. Verwenden Sie diesen Plan für Benutzer, die mit unterschiedlichen Anwendungen arbeiten, beispielsweise mit Microsoft PowerPoint, das mittlere Ansprüche an die Grafikleistung stellt, und mit Microsoft Word oder Microsoft Outlook, deren Ansprüche an die Grafikleistung nicht sonderlich hoch sind.
- **Höchstleistung** Ein Energieplan, der die Leistung des Computers optimiert, ohne Rücksicht auf die Akkus zu nehmen. Dieser Plan sorgt dafür, dass Sie immer genügend Rechenleistung für grafikintensive Programme oder Multimediaspiele zur Verfügung haben. Verwenden Sie diesen Plan, wenn die Leistung des Computers im Vordergrund steht und die Benutzer hauptsächlich mit grafikintensiven Anwendungen oder mit Anwendungen arbeiten, die komplexe Berechnungen durchführen. Wahrscheinlich müssen Sie auf *Weitere Energiesparpläne einblenden* tippen oder klicken, um diesen Plan zu sehen.

- **Energiesparmodus** Ein Energieplan, der für einen geringen Energieverbrauch ausgelegt ist. Dieser Plan sorgt dafür, dass der Prozessor langsamer läuft, um die Akkus zu schonen. Verwenden Sie diesen Plan für Benutzer, die hauptsächlich Anwendungen wie Microsoft Word und Microsoft Outlook verwenden, die keine hohen Ansprüche an die Grafikleistung stellen.

Die Energieeinstellungen lassen sich in zwei allgemeine Kategorien aufteilen: Grundeinstellungen und erweiterte Einstellungen. Die Grundeinstellungen legen fest, wann ein Computer seinen Monitor abblendet oder abschaltet und wann er in den Energiesparmodus wechselt. Wichtig ist, dass mobile Computer über zwei verschiedene Sätze an Einstellungen verfügen, die sich unabhängig voneinander konfigurieren lassen, nämlich einen Satz für den Batteriebetrieb und einen zweiten für den Betrieb mit Netzstrom. Sie können einen Computer zum Beispiel so einstellen, dass der Monitor bei Batteriebetrieb nach 2 Minuten Inaktivität abgeblendet wird, während dies bei Betrieb mit Netzstrom erst nach 5 Minuten erfolgt.

Mit den erweiterten Energieeinstellungen lässt sich genauer festlegen, ob und wann die Komponenten eines Computers, deren Energieverbrauch sich steuern lässt, heruntergefahren werden und wie diese Komponenten unter Leistungsgesichtspunkten eingestellt werden. Welche erweiterten Energieeinstellungen zur Verfügung stehen, hängt von der Konfiguration des Computers ab. Wichtige Energieeinstellungen sind:

- **Akku\Akkustand für Reservestrom** Legt fest, bei wie viel Prozent Akkukapazität der Reservestrommodus eingeleitet wird. Der Standardwert ist 7 Prozent, das heißt, dass der Computer in den Reservestrommodus schaltet, sobald nur noch 7 Prozent Akkukapazität übrig sind. Sie können zwar einen beliebigen Prozentwert eintragen, aber im Allgemeinen ist ein Reservestand von 5 bis 18 Prozent sinnvoll.
- **Bildschirm\Bildschirm ausschalten nach** Bestimmt, ob und wann ein Computermonitor abgeschaltet wird, um Strom zu sparen. Wenn Sie diese Funktion abschalten möchten, wählen Sie die Einstellung *Nie*. Geben Sie an, nach wie vielen Minuten der Bildschirm ausgeschaltet wird, wenn der Computer nicht benutzt wird.
- **Desktophintergrundeinstellungen\Diashow** Legt fest, ob das Diashowfeature für den Desktophintergrund verfügbar ist oder unterbrochen wird. Die Standardeinstellung ist *Verfügbar*. Wenn Sie diese Option auf *Angehalten* setzen, wird eine Diashow, die als Desktophintergrund angezeigt wird, deaktiviert.
- **Drahtlosadaptoreinstellungen\Energiesparmodus** Gibt den Energiesparmodus an, der verwendet werden soll, wenn Drahtlosnetzwerkadapter an den Computer angeschlossen sind. Zulässige Werte sind *Höchstleistung*, *Minimaler Energiesparmodus*, *Mittlerer Energiesparmodus*, *Maximaler Energiesparmodus*.
- **Energie sparen\Hybriden Standbymodus zulassen** Gibt an, ob der Computer den hybriden Standbymodus nach Art von Windows 8 verwendet oder den Ruhezustand früherer Windows-Versionen. Sie können diesen Wert auf *Ein* oder *Aus* stellen. Der hybride Standbymodus von Windows 8 versetzt den Computer in einen Zustand niedriger Energieaufnahme, bis der Benutzer den Computer wieder aktiviert. Wird der Computer mit einem Akku betrieben, verbraucht er auch im Standbymodus noch Strom, allerdings nur sehr wenig. Wird der Akku leer, während sich der Computer noch im Standbymodus befindet, wird die aktuelle Arbeitsumgebung auf der Festplatte gespeichert. Anschließend wird der Computer vollständig ausgeschaltet. Dieser Endzustand ähnelt dem Ruhezustand von Windows XP.
- **Energie sparen\Ruhezustand nach** Legt fest, ob und wann ein Computer in den Ruhezustand übergeht, um Strom zu sparen. Wenn ein Computer in den Ruhezustand übergeht, wird ein Abbild der aktuellen Arbeitsumgebung des Benutzers und des Betriebssystems auf dem Laufwerk gespeichert.

Sobald der Benutzer den Computer wieder einschaltet, werden die Arbeitsumgebung und das Betriebssystem aus dem gespeicherten Abbild wiederhergestellt. In Windows 8 wird diese Einstellung normalerweise nicht als Standard verwendet. Die Standardeinstellung ist, nach einer bestimmten Phase der Inaktivität in einen Standbymodus zu wechseln. Die Einstellung *Nie* deaktiviert diese Funktion. Sie können die Zeitspanne in Minuten angeben, nach der der Computer automatisch in den Ruhezustand übergeht, wenn er nicht benutzt wird.

- **Energie sparen\Standbymodus nach** Legt fest, ob und wann ein Computer in einen Standbymodus übergeht, um Strom zu sparen. Mit der Einstellung *Nie* können Sie diese Funktion deaktivieren. Sie können festlegen, nach wie viel Minuten der Computer in einen Standbymodus wechselt, wenn er unbenutzt bleibt.
- **Energie sparen\Zeitgeber zur Aktivierung zulassen** Legt fest, ob es erlaubt ist, dass der Computer aufgrund von Zeitgeberereignissen aus dem Energiesparmodus aufgeweckt wird. Wenn Sie diese Option auf *Deaktivieren* setzen, wecken Zeitgeberereignisse den Computer nicht auf. Setzen Sie die Option dagegen auf *Aktivieren*, können Zeitgeberereignisse den Computer aufwecken.
- **Festplatte\Festplatte ausschalten nach** Legt fest, ob und wann das Festplattenlaufwerk eines Computers ausgeschaltet wird, um Strom zu sparen. Durch die Einstellung auf *Nie* bleibt die Festplatte eingeschaltet, solange der Computer läuft. Sie können festlegen, nach wie viel Minuten die Festplatte abgeschaltet wird, wenn der Computer unbenutzt bleibt. Windows 8 zeigt ein spezielles Eingabefeld zur Festlegung des numerischen Werts an. Durch Tippen oder Klicken auf einen der beiden nach oben und unten gerichteten Pfeile können Sie den Wert ändern, und wenn Sie die Maustaste gedrückt halten, geht das sehr schnell. Wenn Sie den Wert 1 noch einmal verringern, lautet die nächste Einstellung *Nie*. Sie können den gewünschten Wert auch direkt eingeben. Wenn Sie eine 0 eingeben, wird sie als *Nie* interpretiert.
- **Multimediaeinstellungen\Bei der Freigabe von Medien** Legt fest, was der Computer tut, wenn ein Gerät oder ein anderer Computer Medien von diesem Computer abspielt. Wenn Sie diese Option auf *Wechseln in den Modus "Abwesend" zulassen* setzen, schaltet der Computer nicht in den Energiesparmodus, wenn Sie Medien für andere Geräte oder Computer freigeben. Verwenden Sie die Einstellung *Der Computer kann in den Energiesparmodus wechseln*, darf der Computer in den Energiesparmodus schalten, wenn einige Zeit kein Benutzer an diesem Computer gearbeitet hat, und zwar unabhängig davon, ob er Medien für andere Computer oder Geräte freigibt. Wenn Sie diese Option auf *Wechseln in den Energiesparmodus bei Inaktivität verhindern* setzen, wechselt der Computer, der Medien für andere Geräte oder Computer freigibt, nur dann in den Energiesparmodus, wenn der Benutzer den Energiesparmodus explizit aktiviert.
- **Multimediaeinstellungen\Bei der Videowiedergabe** Legt fest, welcher Energiesparmodus beim Abspielen von Videos benutzt wird. Wenn Sie diese Option auf *Videoqualität optimieren* stellen, nutzt der Computer die bestmögliche Wiedergabequalität für Videos. Verwenden Sie die Einstellung *Ausbalanciert*, wendet der Computer einen ausgewogenen Ansatz an, bei dem er die Wiedergabequalität ein wenig verringert, um Strom zu sparen. Und wenn Sie die Option auf *Energieeinsparung optimieren* setzen, passt der Computer die Wiedergabequalität aktiv an, um Strom zu sparen.
- **Netzschalter und Zuklappen\Energiespartastenaktion** Legt fest, was geschehen soll, wenn jemand die Energiespartaste drückt. Mit dieser Einstellung können Sie die Standardaktion des Computers ändern. Sie können diesen Wert auf *Nichts unternehmen*, *Energie sparen* oder *Ruhezustand* einstellen. Allerdings können Sie keine Einstellung verwenden, die nicht vom Computer unterstützt wird.
- **Netzschalter und Zuklappen\Standardaktion für Beenden** Legt fest, was geschehen soll, wenn jemand den Netzschalter eines Computers drückt. Sie können diese Option auf *Energie sparen*, *Ruhezustand*, *Herunterfahren* und auf *Nichts unternehmen* einstellen.

- **PCI Express\Verbindungszustand-Energieverwaltung** Legt den Energiesparmodus fest, der für PCI-Express-Geräte verwendet wird, die an den Computer angeschlossen sind (PCI steht für Peripheral Component Interconnect). Diesen Wert können Sie auf *Aus*, *Mittlere Energieeinsparungen* und *Maximale Energieeinsparungen* einstellen.
- **<Planname>\Kennwort bei Reaktivierung anfordern** Legt fest, ob bei der Reaktivierung aus einem Energiesparmodus ein Kennwort erforderlich ist. Sie können diese Option auf *Ja* oder *Nein* einstellen. Bei Domänencomputern hat diese Option den Wert *Ja* und kann nur über Gruppenrichtlinien geändert werden.
- **Prozessorenergieverwaltung\Maximaler Leistungszustand des Prozessors** Legt die höchste Leistung des Mikroprozessors fest. Um Strom zu sparen, können Sie die höchste Leistung des Prozessors herabsetzen. Aber die Energieersparnis geht direkt zu Lasten der Reaktionsfähigkeit und der Rechenleistung. Die Herabsetzung der maximalen Leistung des Prozessors auf 50 Prozent oder weniger ist zwar eine erhebliche Einschränkung der Rechenleistung und Reaktionsfähigkeit, kann aber auch eine beträchtliche Energieersparnis bewirken.
- **Prozessorenergieverwaltung\Minimaler Leistungszustand des Prozessors** Legt die minimale Leistung des Mikroprozessors fest. Wenn Sie Strom sparen möchten, setzen Sie die erlaubte minimale Leistung herunter. Allerdings wirkt sich diese Herabsetzung direkt auf die Reaktionsfähigkeit und Rechengeschwindigkeit aus. Ein Wert von 5 Prozent würde zum Beispiel die Reaktionszeit auf Anfragen und die Datenverarbeitung verlangsamen, aber eine beträchtliche Energieeinsparung bedeuten. Ein Wert um 50 Prozent dürfte ein vernünftiger Kompromiss zwischen Reaktionsfähigkeit und Rechenleistung des Computers und einer gewissen Energieersparnis sein. Der Wert 100 Prozent bedeutet die beste Reaktionsfähigkeit, die höchste Rechenleistung und den größten Energieverbrauch.
- **Prozessorenergieverwaltung\Systemkühlungsrichtlinie** Legt fest, ob das Betriebssystem die Lüftergeschwindigkeit erhöht, bevor es den Prozessor verlangsamt. Wenn Sie diese Option auf *Passiv* setzen, wird diese Funktion eingeschränkt, sodass der Prozessor möglicherweise heißer wird als üblich. Setzen Sie diese Option auf *Aktiv*, ist die Funktion aktiviert und hilft, den Prozessor zu kühlen.
- **USB-Einstellungen\Einstellung für selektives USB-Energiesparen** Legt fest, ob das Feature für selektives USB-Energiesparen verfügbar ist. Wenn Sie diese Option auf *Deaktiviert* setzen, wird der selektive Energiesparmodus nicht für USB-Geräte benutzt. Setzen Sie die Option dagegen auf *Aktiviert*, kann der selektive Energiesparmodus für USB-Geräte benutzt werden.

Wie Sie sehen, lässt sich mit den erweiterten Energieeinstellungen praktisch jeder Aspekt der Energieverwaltung steuern. Die entscheidenden Unterschiede in den erweiterten Einstellungen sind die zwischen den Energiesparplänen. Während der Plan *Höchstleistung* zum Beispiel dafür sorgt, dass der Mikroprozessor des Computers immer mit voller Leistung laufen kann, sorgen die Pläne *Energiesparmodus* und *Ausbalanciert* für einen niedrigeren Stromverbrauch, indem sie den Prozessor so einstellen, dass er mindestens 5 und höchstens 100 Prozent der maximalen Leistung verbraucht.

Achten Sie bei der Einstellung der Energiesparpläne darauf, dass alle Komponenten nach einer gewissen Phase der Inaktivität abgeschaltet werden. Die Abschaltung von Komponenten ermöglicht es dem Computer, schrittweise in den Ruhezustand überzugehen. Wenn sich der Computer im Standbymodus befindet, sind alle Geräte, die über eine Energiesteuerung verfügen, ausgeschaltet, damit der Laptop weniger Strom verbraucht. Wird der Computer aus dem Standbymodus heraus reaktiviert, werden die Komponenten wieder eingeschaltet, wie zum Beispiel der Monitor und die Festplatten, und die Arbeitsumgebung des Benutzers wird wiederhergestellt. Sie sollten den Standbymodus so einstellen, dass ein Laptop ziemlich schnell in einen Energiesparmodus übergeht, wenn der Benutzer nicht mehr am Laptop arbeitet, etwa nach 20 bis 30 Minuten.

Da es auf einem Computer mehrere Energiesparpläne geben kann, lässt sich für jede Art der Benutzung ein spezieller Plan erstellen. Sie können für die verschiedenen Situationen mehrere Pläne vorbereiten. Zu Hause oder im Büro brauchen Laptops vielleicht eine andere Energieeinstellung als bei einer Präsentation. In einem Fall möchten Sie den Laptop vielleicht so einstellen, dass er möglichst wenig Strom verbraucht, weil er auf Akku läuft. In einem anderen Fall ist es Ihnen vielleicht wichtig, dass der Laptop nicht sein Festplattenlaufwerk oder seinen Drahtlosnetzwerkadapter ausschaltet.

Einstellen und Optimieren von Energieplänen

Computer können zwar über mehrere Energiepläne verfügen, aber zu einem bestimmten Zeitpunkt kann immer nur ein Energieplan aktiv sein. Zur Auswahl oder Optimierung eines Energieplans gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Energieoptionen*.
2. Wie aus Abbildung 2.21 hervorgeht, können Sie den Energiesparplan, der verwendet werden soll, aus der Liste *Bevorzugte Energiesparpläne* auswählen.

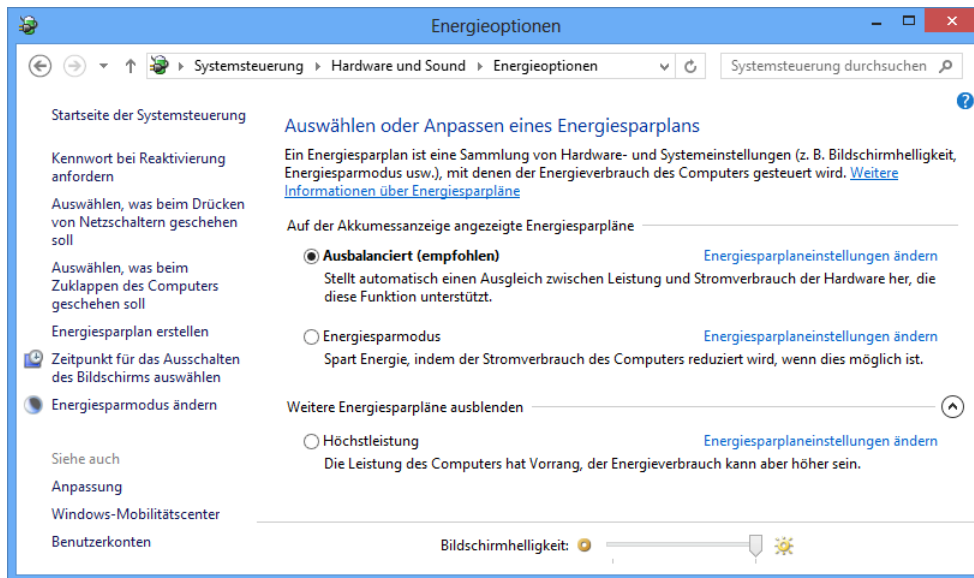


Abbildung 2.21 Auswählen eines Energiesparplans

3. Tippen oder klicken Sie unter dem Plan, den Sie bearbeiten möchten, auf *Energiesparplaneinstellungen ändern*. Dadurch öffnet sich die Seite *Energiesparplaneinstellungen bearbeiten* (Abbildung 2.22). Mobilgeräte weisen für Akku- und Netzbetrieb separate Einstellungen auf.
4. Auf einem Mobilgerät können Sie mit der Liste *Bildschirmhelligkeit regeln* festlegen, ob und nach welcher Zeitspanne der Monitor dunkler gestellt wird. Wenn Sie diese Funktion deaktivieren möchten, wählen Sie die Einstellung *Niemals*.
5. Mit der Liste *Bildschirm ausschalten* legen Sie fest, ob und nach welcher Zeitspanne der Bildschirm des Computers automatisch ausgeschaltet wird. Wenn Sie diese Funktion deaktivieren möchten, wählen Sie die Einstellung *Niemals*.

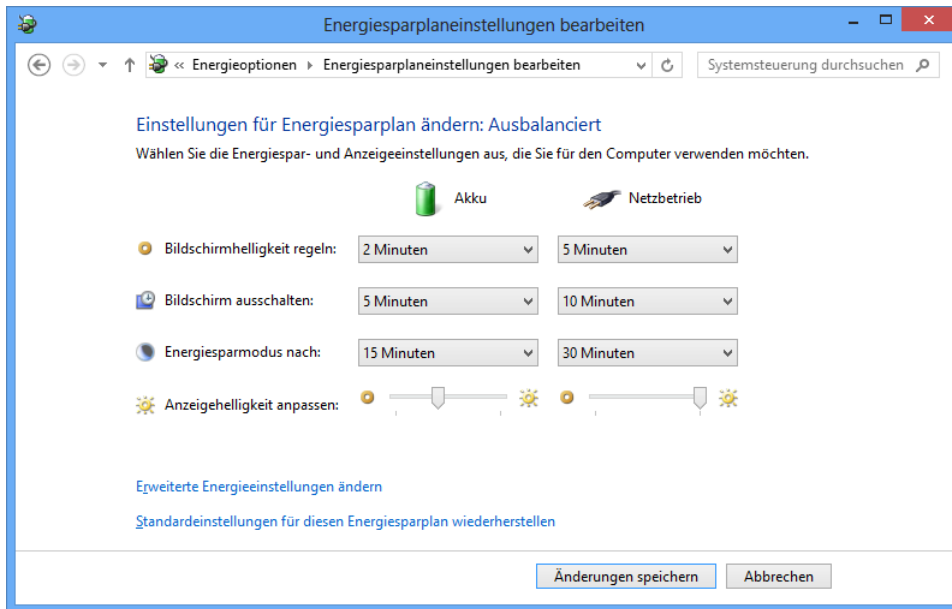


Abbildung 2.22 Konfigurieren der Einstellungen eines Energiesparplans

6. Mit der Liste *Energiesparmodus nach* können Sie festlegen, ob und nach welcher Zeitspanne der Computer automatisch in einen Energiesparmodus wechselt. Wenn Sie diese Funktion deaktivieren möchten, wählen Sie die Einstellung *Niemals*.

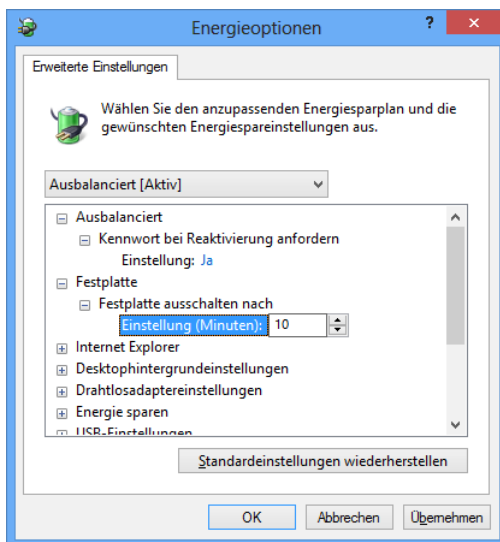


Abbildung 2.23 Im Dialogfeld *Energieoptionen* stellen Sie erweiterte Energieoptionen ein

7. Wenn Sie erweiterte Einstellungen vornehmen möchten, tippen oder klicken Sie auf *Erweiterte Energieeinstellungen ändern*. Nehmen Sie im Dialogfeld *Energieoptionen* (Abbildung 2.23) die gewünsch-

ten Einstellungen vor. Tippen oder klicken Sie auf *OK*, um die vorgenommenen Änderungen zu speichern.

8. Tippen oder klicken Sie auf *Änderungen speichern*, wenn Sie etwas in den Dropdownlisten *Bildschirm ausschalten* oder *Energiesparmodus nach* geändert haben.

In Gruppenrichtlinien können die Energiesparpläne auf mehreren Computern einer Domäne mithilfe eines Einstellungselements optimieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Energieoptionen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Energieoptionen* auswählen.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Energieoptionen* oder halten Sie den Knoten gedrückt, und wählen Sie im Kontextmenü den Befehl *Neu/Energiesparplan* (mindestens Windows 7). Daraufhin öffnet sich das Eigenschaftendialogfeld für die Energieoptionen.
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Aktualisieren* aus, wenn Sie die Energiesparplaneinstellungen ändern wollen, oder den Eintrag *Ersetzen*, um den Energiesparplan zu löschen und danach in der konfigurierten Form neu zu erstellen.
4. Wählen Sie in der Auswahlliste den Energiesparplan, den Sie verwenden wollen, zum Beispiel *Ausbalanciert*.
5. Machen Sie einen Plan zum aktiven Plan, indem Sie das Kontrollkästchen *Als aktiven Energiesparplan festlegen* aktivieren.
6. Verwenden Sie die verfügbaren Optionen, um die Einstellungen für den Energiesparplan zu konfigurieren.
7. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Erstellen von Energiesparplänen

Zusätzlich zu den bevorzugten Energieplänen von Windows 8 können Sie bei Bedarf eigene Energiesparpläne erstellen. Dazu gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Energieoptionen*.
2. Tippen oder klicken Sie im linken Fensterabschnitt auf *Energiesparplan erstellen*. Dadurch öffnet sich die Seite *Energiesparplan erstellen* (Abbildung 2.24).
3. Wählen Sie den bevorzugten Energiesparplan aus, der Ihren Vorstellungen am besten entspricht, um eine Ausgangsbasis für weitere Änderungen zu haben.
4. Geben Sie im Feld *Energiesparplanname* einen Namen für den Energiesparplan ein und tippen oder klicken Sie dann auf *Weiter*. Dadurch öffnet sich die Seite *Energiesparplaneinstellungen bearbeiten*.
5. Auf einem Mobilgerät können Sie mit der Liste *Bildschirmhelligkeit regeln* festlegen, ob und nach welcher Zeitspanne der Monitor dunkler gestellt wird. Wenn Sie diese Funktion deaktivieren möchten, wählen Sie die Einstellung *Niemals*.

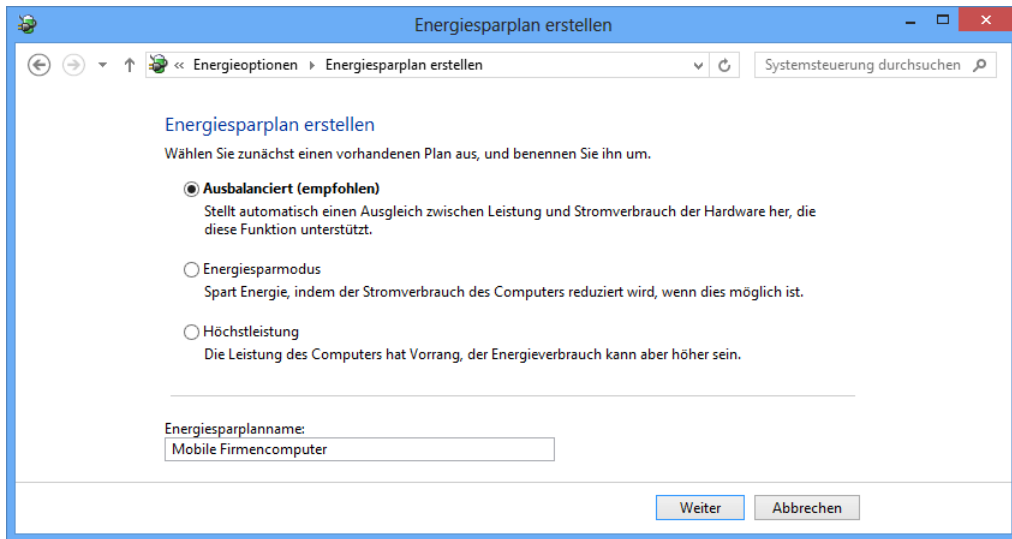


Abbildung 2.24 Erstellen eines Energiesparplans

6. Mit der Liste *Bildschirm ausschalten* können Sie festlegen, ob und nach welcher Zeitspanne der Bildschirm des Computers automatisch ausgeschaltet wird. Wenn Sie diese Funktion deaktivieren möchten, wählen Sie die Einstellung *Niemals*.
7. Mit der Liste *Energiesparmodus nach* können Sie festlegen, ob und nach welcher Zeitspanne der Computer automatisch in einen Energiesparmodus wechselt. Wenn Sie diese Funktion deaktivieren möchten, wählen Sie die Einstellung *Niemals*.
8. Tippen oder klicken Sie auf *Erstellen*, um den Plan zu erstellen. Die Seite *Energieoptionen* wird mit dem von Ihnen erstellen Plan als neuem bevorzugtem Energiesparplan angezeigt, der den Plan ersetzt, den Sie als Ausgangsbasis gewählt haben. Diesen ursprünglichen Plan finden Sie nun unter *Weitere Energiesparpläne*. Sollte der Plan ausgeblendet sein, tippen oder klicken Sie auf die kleine Schaltfläche rechts neben der Überschrift *Weitere Energiesparpläne einblenden*, um den Plan anzuzeigen.
9. Der Plan, den Sie erstellt haben, wird standardmäßig vorgewählt. Klicken Sie unter diesem Plan auf *Energiesparplaneinstellungen ändern*, um die Seite *Energiesparplaneinstellungen bearbeiten* anzuzeigen, und tippen oder klicken Sie dann auf *Erweiterte Energieeinstellungen ändern*, um das Dialogfeld *Energieoptionen* zu öffnen.
10. Nachdem Sie die erweiterten Energieeinstellungen nach Wunsch vorgenommen haben, tippen oder klicken Sie auf *OK*, um die Änderungen zu speichern, die Sie vorgenommen haben.

Gehen Sie folgendermaßen vor, um die Gruppenrichtlinien zu öffnen und mithilfe eines Einstellungselements auf mehreren Computern in einer gesamten Domäne Energiesparpläne zu erstellen:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Energieoptionen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Energieoptionen* auswählen.

2. Klicken Sie mit der rechten Maustaste auf den Knoten *Energieoptionen* oder halten Sie den Knoten gedrückt, und wählen Sie im Kontextmenü den Befehl *Neu/Energiesparplan* (mindestens Windows 7). Daraufhin öffnet sich das Eigenschaftendialogfeld für die Energieoptionen.
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Erstellen* aus. Wählen Sie den bevorzugten Energiesparplan aus, der Ihren Vorstellungen am besten entspricht, um eine Ausgangsbasis für weitere Änderungen zu haben. Tippen oder klicken Sie anschließend in die Auswahlliste und geben Sie einen Namen für Ihren neuen Plan ein.
4. Wählen Sie in der Auswahlliste den Energiesparplan, den Sie verwenden wollen, zum Beispiel *Ausbalanciert*.
5. Machen Sie einen Plan zum aktiven Plan, indem Sie das Kontrollkästchen *Als aktiven Energiesparplan festlegen* aktivieren.
6. Verwenden Sie die verfügbaren Optionen, um die Einstellungen für den Energiesparplan zu konfigurieren.
7. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Einstellen der Netzschalteroptionen und des Kennwortschutzes bei Reaktivierung

Durch systemweit gültige Einstellungen für die Energieoptionen können Sie festlegen, wie der Netzschalter funktionieren soll und ob alle Benutzer, die sich am Computer anmelden, bei der Reaktivierung erneut das Kennwort eingeben müssen. Sie können den Netzschalter so einstellen, dass ein Druck darauf das System in einen Standbymodus oder in den Ruhezustand versetzt oder herunterfährt. Außerdem können Sie den Computer so einstellen, dass nach seiner Reaktivierung aus einem Energiesparmodus ein Kennwort erforderlich ist, um die Bildschirmsperre aufzuheben, oder nicht.

Gehen Sie folgendermaßen vor, um die systemweiten Energieeinstellungen zu konfigurieren:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Energieoptionen*.
2. Tippen oder klicken Sie im linken Fensterabschnitt auf *Auswählen, was beim Drücken von Netzschaltern geschehen soll*.
3. Wählen Sie in der Dropdownliste *Beim Drücken des Netzschalters* aus, ob der Computer nichts tun, herunterfahren oder in den Energiesparmodus oder in den Ruhezustand wechseln soll, wenn der Netzschalter gedrückt wird. Sie können hier allerdings keine Option auswählen, die nicht vom Computer unterstützt wird.
4. Wählen Sie in der Dropdownliste *Beim Drücken der Energiespartaste* aus, ob der Computer in den Energiesparmodus oder in den Ruhezustand wechseln oder nichts tun soll, wenn die Energiespartaste betätigt wird. Auch hier gilt, dass Sie nur Optionen auswählen können, die auf dem Computer unterstützt werden.
5. Wenn sie verfügbar ist, legen Sie mit der Liste *Beim Zuklappen* fest, ob der Computer in den Energiesparmodus oder in den Ruhezustand wechseln oder nichts tun soll, wenn der Deckel des Laptops zugeklappt wird. Wieder gilt, dass Sie nur Optionen auswählen können, die auf dem Computer unterstützt werden.

6. Wenn die Optionen unter *Kennworteingabe bei Reaktivierung* und *Einstellungen für das Herunterfahren* nicht angezeigt werden, müssen Sie auf *Zurzeit nicht verfügbare Einstellungen ändern* klicken.
7. Wählen Sie die Option *Kennwort ist erforderlich* aus, wenn Sie möchten, dass die Benutzer ein Kennwort eingeben müssen, sobald der Computer aus einem Energiesparmodus aufwacht. Diese Einstellung empfiehlt sich, um die Sicherheit des Systems zu verbessern.
8. Wählen Sie *Schnellstart aktivieren*, damit beim Herunterfahren des Computers Systeminformationen in einer Datei auf dem Systemlaufwerk gespeichert werden. Beim nächsten Start wird diese Datei eingelesen, um den Startvorgang zu beschleunigen. Beim erneuten Starten eines laufenden Computers wird der Schnellstart nicht verwendet.
9. Wählen Sie die Energieoptionen aus, die beim Antippen oder Anklicken des Ein-/Ausschalters angezeigt werden sollen.
10. Tippen oder klicken Sie auf *Änderungen speichern*, wenn Sie die gewünschten Änderungen vorgenommen haben.

Verwalten von Energieoptionen mit Richtlinienereinstellungen

In den Gruppenrichtlinien finden Sie die Richtlinienereinstellungen zum Verwalten der Energieoptionen unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Energieverwaltung*. Es gibt hier fünf Unterknoten:

- **Benachrichtigungseinstellungen** Enthält Richtlinien zum Einstellen von Benachrichtigungen und Aktionen bei kritischem Akkuzustand.
- **Festplatteneinstellungen** Enthält Richtlinien, mit denen eingestellt wird, wann Festplatten im Netz- und im Akkubetrieb ausgeschaltet werden.
- **Schaltflächeneinstellungen** Umfasst Richtlinien zum Einstellen der Funktionen von Netzschalter, Energiespartaste und Notebookdeckel, jeweils im Netz- und im Akkubetrieb. Hier steuern Sie auch, wie der Netzschalter im Tasks-Bildschirm arbeitet, den Sie mit STRG+ALT+ENTF öffnen.
- **Standbymoduseinstellungen** Umfasst Richtlinien zum Einstellen der Energiesparmodi, die für Geräte und Anwendungen erlaubt sind.
- **Video- und Anzeigeeinstellungen** Enthält Richtlinien, mit denen eingestellt wird, wann der Monitor ausgeschaltet, die Bildschirmhelligkeit verringert und die Diashow auf dem Desktophintergrund deaktiviert werden, jeweils für den Netz- und den Akkubetrieb.

Damit eine Richtlinie wirksam wird, aktivieren Sie sie und legen dann die gewünschte Aktion fest.

In den Gruppenrichtlinien können Sie auch den aktiven Energiesparplan festlegen. Wie die Einstellung erfolgt, hängt davon ab, ob Sie einen Standardplan verwenden, einen aktualisierten bevorzugten Plan oder einen benutzerdefinierten Plan, den Sie selbst erstellt haben. Wenn alle Computer, für die eine bestimmte Richtlinie gilt, einen der Standardenergiepläne von Windows 8 verwenden sollen, gehen Sie folgendermaßen vor:

1. Nachdem Sie das Gruppenrichtlinienobjekt geöffnet haben, mit dem Sie arbeiten möchten, erweitern Sie den Knoten *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Energieverwaltung*.
2. Tippen oder klicken Sie *Aktiven Energiesparplan auswählen* doppelt an.
3. Wählen Sie *Aktiviert* und dann in der Liste *Aktiver Energiesparplan* den Plan, der verwendet werden soll. Verfügbar sind die Einstellungen *Höchstleistung*, *Energiesparmodus* und *Automatisch*. Wenn Sie *Automatisch* wählen, verwendet Windows 8 in den meisten Fällen den Plan *Ausbalanciert*.
4. Tippen oder klicken Sie auf *OK*.

Wenn alle Computer, für die eine bestimmte Richtlinie gilt, einen aktualisierten bevorzugten Plan oder einen benutzerdefinierten Plan verwenden sollen, den Sie selbst erstellt haben, gehen Sie folgendermaßen vor:

1. Nachdem Sie das Gruppenrichtlinienobjekt geöffnet haben, mit dem Sie arbeiten möchten, erweitern Sie den Knoten *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Energieverwaltung*.
2. Tippen oder klicken Sie *Benutzerdefinierten aktiven Energiesparplan festlegen* doppelt an.
3. Wählen Sie *Aktiviert* und geben Sie im Textfeld *Benutzerdefinierter aktiver Energiesparplan (GUID)* die GUID des zu verwendenden Energiesparplans ein.
4. Tippen oder klicken Sie auf *OK*.

TIPP Sie erhalten eine Liste der GUIDs der Energiesparpläne, die auf einem Computer zur Verfügung stehen, wenn Sie in einer Eingabeaufforderung mit erhöhten Rechten **powercfg -l** eingeben.

Einstellen der Aktionen bei niedrigen Akkuladezuständen

Ob ein Laptop ein akustisches Signal gibt oder eine Meldung anzeigt, wenn der Akkuladezustand auf eine bestimmte Stufe fällt, hängt von seiner Einstellung ab. Sie können drei Ladezustände und die zugehörigen Benachrichtigungen einstellen:

- **Benachrichtigung bei niedriger Akkukapazität** Mit der Benachrichtigung bei niedriger Restkapazität soll der Benutzer darauf hingewiesen werden, dass der Akku bald leer ist. Dieser Zustand bedeutet, dass der Akku nur noch 10 Prozent oder weniger seiner vollen Kapazität aufweist. Bei einem Akku mit insgesamt 8 Stunden Betriebsdauer entsprechen 10 Prozent etwa 48 Minuten Betriebszeit.
- **Benachrichtigung bei kritischer Akkukapazität** Die Benachrichtigung bei kritischem Ladezustand soll den Benutzer darauf hinweisen, dass der Computer bald wegen Strommangels ausfallen wird. Als kritisch wird der Ladezustand eingestuft, wenn der Akku nur noch 3 Prozent oder weniger seiner vollen Kapazität aufweist. Bei einem Akku mit insgesamt 8 Stunden Betriebsdauer entsprechen 3 Prozent etwa 14 Minuten Betriebszeit.
- **Reservestromalarm** Die Benachrichtigung bei Reservestrom soll den Benutzer warnen, wenn der Akku auf Reservestrom läuft. Der Reservestromzustand wird standardmäßig aktiviert, wenn der Akku nur noch 1 Prozent oder weniger seiner vollen Kapazität aufweist. Bei einem Akku mit insgesamt 8 Stunden Betriebsdauer entspricht 1 Prozent etwa 5 Minuten Betriebszeit.

Mit der Aktion, die Sie mit den Alarmen für niedrige und kritische Akkukapazität verknüpfen, legen Sie fest, welche Aktionen das Betriebssystem ausführt, wenn die entsprechende Alarmstufe erreicht ist. Beispielsweise können Sie in diesem Fall den Computer herunterfahren, in den Standbymodus schalten oder den Ruhezustand aktivieren. Seit Windows Vista können Sie die Benachrichtigungen über niedrige Akkukapazität abschalten, indem Sie die Richtlinie *Benutzerbenachrichtigung bei niedriger Akkukapazität deaktivieren* aktivieren. In Windows 7 wurde die Warnung für Reservestrom hinzugefügt, um die Benutzer zu warnen, wenn die Akkus so gut wie leer sind. Da bei der Einstellung der Benachrichtigungsstufen unterschiedliche Dinge berücksichtigt werden müssen, möchte ich die Stufen in den folgenden Abschnitten separat besprechen.

Einstellen der Benachrichtigung und Aktionen bei niedriger Akkukapazität

Wie bereits erwähnt, ist die Benachrichtigung bei niedriger Akkukapazität für den Benutzer ein Hinweis darauf, dass dem Computer in absehbarer Zeit der Strom ausgeht. Wenn dieser Zustand eintritt, informiert das System den Benutzer entweder nur mit einer entsprechenden Meldung oder mit einer Kombination von Meldung und akustischem Signal. Vielleicht möchten Sie das System auch so einstellen, dass es noch einen Schritt weiter geht und statt eines Alarms oder zusätzlich dazu in einen Energiesparmodus wechselt.

Um die Benachrichtigung und Aktion für den niedrigen Akkuladezustand einzustellen, gehen Sie folgendermaßen vor:

1. Nachdem Sie das Gruppenrichtlinienobjekt geöffnet haben, mit dem Sie arbeiten möchten, erweitern Sie den Knoten *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Energieverwaltung/Benachrichtigungseinstellungen*.
2. Zur Einstellung der Aktion bei niedrigem Ladezustand tippen oder klicken Sie *Aktion zur Benachrichtigung bei niedriger Akkukapazität* doppelt an. Wählen Sie *Aktiviert* und dann im Kombinationsfeld *Aktion zur Benachrichtigung bei niedriger Akkukapazität* die gewünschte Aktion, beispielsweise *Standbymodus*. Tippen oder klicken Sie auf *OK*.
3. Wenn Sie einstellen möchten, welche Restkapazität als niedriger Ladezustand gewertet wird, tippen oder klicken Sie *Benachrichtigungsebene für niedrige Akkukapazität* doppelt an. Wählen Sie *Aktiviert* und legen Sie dann im Feld *Benachrichtigungsebene für niedrige Akkukapazität* eine passende Stufe fest. Tippen oder klicken Sie auf *OK*.

TIPP Der Standardwert für die Einstufung des niedrigen Ladezustands hängt von der Betriebsdauer mit einer Akkuladung ab und liegt gewöhnlich bei 10 Prozent dieser Zeit. Auf den meisten Systemen ist das ein sinnvoller Wert. Allerdings hatte ich es auch schon mit Systemen zu tun, auf denen dieser Wert keineswegs ausreichte. Besonders bei schlechten Akkus ist das nicht genug. Ich stelle dann meistens Werte zwischen 12 und 15 Prozent ein. Im Gegensatz dazu ist die Standardeinstellung auf energieeffizienten Systemen oder auf Computern, die mit zwei Akkus ausgerüstet sind, häufig viel zu hoch. Dann stelle ich die Stufe so ein, dass der Benutzer informiert wird, wenn noch ungefähr 20 Minuten Betriebsdauer übrig sind.

Einstellen der Benachrichtigung bei kritischer Akkukapazität

Die Konfiguration einer Aktion bei einem kritischen Ladezustand des Akkus soll dafür sorgen, dass das System einen definierten Betriebszustand einnehmen kann, bevor die Energieversorgung ausfällt. Sobald der kritische Ladezustand des Akkus eintritt, benachrichtigt das System den Benutzer und geht in den Ruhezustand über. Im Ruhezustand werden die Komponenten des Computers, deren Energiezustände sich steuern lassen, weitgehend abgeschaltet, um Strom zu sparen. Häufig stelle ich die Aktion bei niedriger Akkukapazität so ein, dass der Computer in einen Energiesparmodus übergeht. Dann stelle ich die Aktion bei kritischer Akkukapazität so ein, dass der Computer in den Ruhezustand wechselt oder ganz heruntergefahren wird. Durch diesen Wechsel der Energieverwaltung in den nächsten Zustand wird für eine Sicherung des Systemzustands gesorgt, bevor der **Strom ausfällt**.

Um die Benachrichtigung und Aktion für den kritischen Akkuladezustand einzustellen, gehen Sie folgendermaßen vor:

1. Nachdem Sie das Gruppenrichtlinienobjekt geöffnet haben, mit dem Sie arbeiten möchten, erweitern Sie den Knoten *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Energieverwaltung/Benachrichtigungseinstellungen*.

2. Zur Einstellung der Aktion bei kritischem Ladezustand tippen oder klicken Sie *Aktion zur Benachrichtigung bei kritischer Akkukapazität* doppelt an. Wählen Sie *Aktiviert* und dann im Kombinationsfeld *Aktion zur Benachrichtigung bei kritischer Akkukapazität* die gewünschte Aktion, beispielsweise *Standbymodus*. Tippen oder klicken Sie auf *OK*.
3. Wenn Sie einstellen möchten, welche Restkapazität als kritischer Ladezustand gewertet wird, tippen oder klicken Sie *Benachrichtigungsebene für kritische Akkukapazität* doppelt an. Wählen Sie *Aktiviert* und legen Sie dann im Feld *Benachrichtigungsebene für kritische Akkukapazität* eine passende Stufe fest. Tippen oder klicken Sie auf *OK*.

TIPP

Der Standardwert für die Einstufung des kritischen Ladezustands hängt von der Betriebsdauer ab, die sich mit einer Akkuladung erreichen lässt, und liegt gewöhnlich bei 3 Prozent dieser Zeit. Auf den meisten Systemen ist das ein sinnvoller Wert. Wenn der Computer in den Ruhezustand wechseln oder herunterfahren soll, ist Ihnen dieser Wert vielleicht noch zu hoch. Außerdem sollten Sie die übliche Betriebsdauer berücksichtigen, die das Gerät mit einer Akkuladung erreicht. Kann man im Akkubetrieb lange auf dem Computer arbeiten, ist der Standardwert gewöhnlich zu hoch. Reicht eine Akkuladung nicht lange, ist der Wert vermutlich nicht hoch genug. Gewöhnlich stelle ich die Benachrichtigung für kritische Akkukapazität so ein, dass sie erfolgt, wenn noch eine Betriebsdauer von 6 bis 8 Minuten übrig ist.

Konfigurieren des Reservestrommodus

Der Reservestrommodus soll Benutzer warnen, dass der Akku so gut wie leer ist. Gehen Sie folgendermaßen vor, um die Benachrichtigung für den Reservestrommodus einzustellen:

1. Nachdem Sie das Gruppenrichtlinienobjekt geöffnet haben, mit dem Sie arbeiten möchten, erweitern Sie den Knoten *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Energieverwaltung/Benachrichtigungseinstellungen*.
2. Stellen Sie ein, wann der Reservestromalarm ausgelöst wird, indem Sie doppelt auf *Benachrichtigungsebene für Reservestrom* tippen oder klicken. Wählen Sie *Aktiviert* aus und stellen Sie dann im Kombinationsfeld *Benachrichtigungsebene für Reservestrom* den gewünschten Prozentwert ein. Tippen oder klicken Sie auf *OK*.

Kapitel 3

Anpassen von Desktop und Benutzeroberfläche

In diesem Kapitel:

Optimieren der PC-Einstellungen	114
Arbeiten mit Desktops und Autostartanwendungen	118
Anpassen der Taskleiste	122
Optimieren der Symbolleiste	125
Verwenden von Designs	127
Optimieren der Desktopumgebung	129
Bildschirmschoner	133
Ändern des Erscheinungsbilds und der Grafikeinstellungen	136

Als Administrator werden Sie von Benutzern oft gebeten, ihnen bei der Anpassung des Desktops und der Profildaten zu helfen. Windows 8 bietet viele Optionen für die Desktop- und Bildschirmanpassung. Diese Optionen sind zwar nützlich, können aber auch Probleme nach sich ziehen, die Sie dann vermutlich wieder lösen sollen. Vielleicht stellen Sie auch fest, dass Benutzer doch ziemlich viel Zeit darauf verwenden, diese Probleme selbst zu lösen, und bieten dann Ihre Hilfe an. Dieses Kapitel beschäftigt sich mit der Konfiguration und Problembeseitigung in folgenden Bereichen:

- PC-Einstellungen, Taskleiste und Symbolleisten
- Desktopdesigns und Hintergrundbilder
- Benutzerdefinierte Desktops
- Bildschirmschoner
- Erscheinungsbild und Konfiguration des Bildschirms

Optimieren der PC-Einstellungen

Der Bildschirm *PC-Einstellungen* und die dazugehörigen Seiten wurden so entworfen, dass sie einen einfachen Zugang zu den Einstellungen für die Benutzeroberfläche und die Anwendungen ermöglichen. Der Bildschirm *PC-Einstellungen* lässt sich auf verschiedene Arten öffnen:

- Bei einer Touch-UI führen Sie eine Streifbewegung vom rechten Bildschirmrand durch, tippen auf *Einstellungen* und dann auf *PC-Einstellungen ändern*.
- Mit Maus und Tastatur drücken Sie die Tastenkombination WINDOWS-Taste+I und tippen oder klicken dann auf *PC-Einstellungen ändern*.

Abbildung 3.1 zeigt ein Beispiel für den Bildschirm *PC-Einstellungen*. Um zwischen den Seiten zu wechseln, tippen oder klicken Sie den Namen der gewünschten Seite an. Jeder Benutzer, der sich am Computer anmeldet, erhält seinen eigenen Satz an Einstellungen.

In den folgenden Abschnitten werden die wichtigsten Bereiche des Betriebssystems beschrieben, die sich mit diesen Seiten und Optionen konfigurieren lassen. Berücksichtigen Sie dabei aber, dass sich die Seiten und Optionen, die Sie auf Ihrem Computer sehen werden, durchaus etwas von den Abbildungen in diesem Buch unterscheiden können.

HINWEIS

In diesem Abschnitt verwende ich für Desktop-Anwendungen überwiegend den Begriff *Apps*. Weitere Informationen über Apps finden Sie in Kapitel 8, »Installieren und Verwalten von Programmen«.

Die Seite *Anpassen*

Auf der Seite *Anpassen* konfigurieren Sie den Sperrbildschirm, die Startseite und das Profilbild. Um zwischen den Konfigurationsbereichen zu wechseln, tippen oder klicken Sie nach Bedarf auf *Sperrbildschirm*, *Startseite* oder *Profilbild*.

Anpassen des Sperrbildschirms

Im Bereich *Sperrbildschirm* können Sie durch einfaches Antippen oder Anklicken ein Bild auswählen, das als Hintergrund angezeigt werden soll. Wenn Sie ein Bild von einem anderen Speicherort verwenden möchten, tippen oder klicken Sie auf *Durchsuchen*, verwenden die angezeigten Optionen zur Navigation und wählen das gewünschte Bild aus.

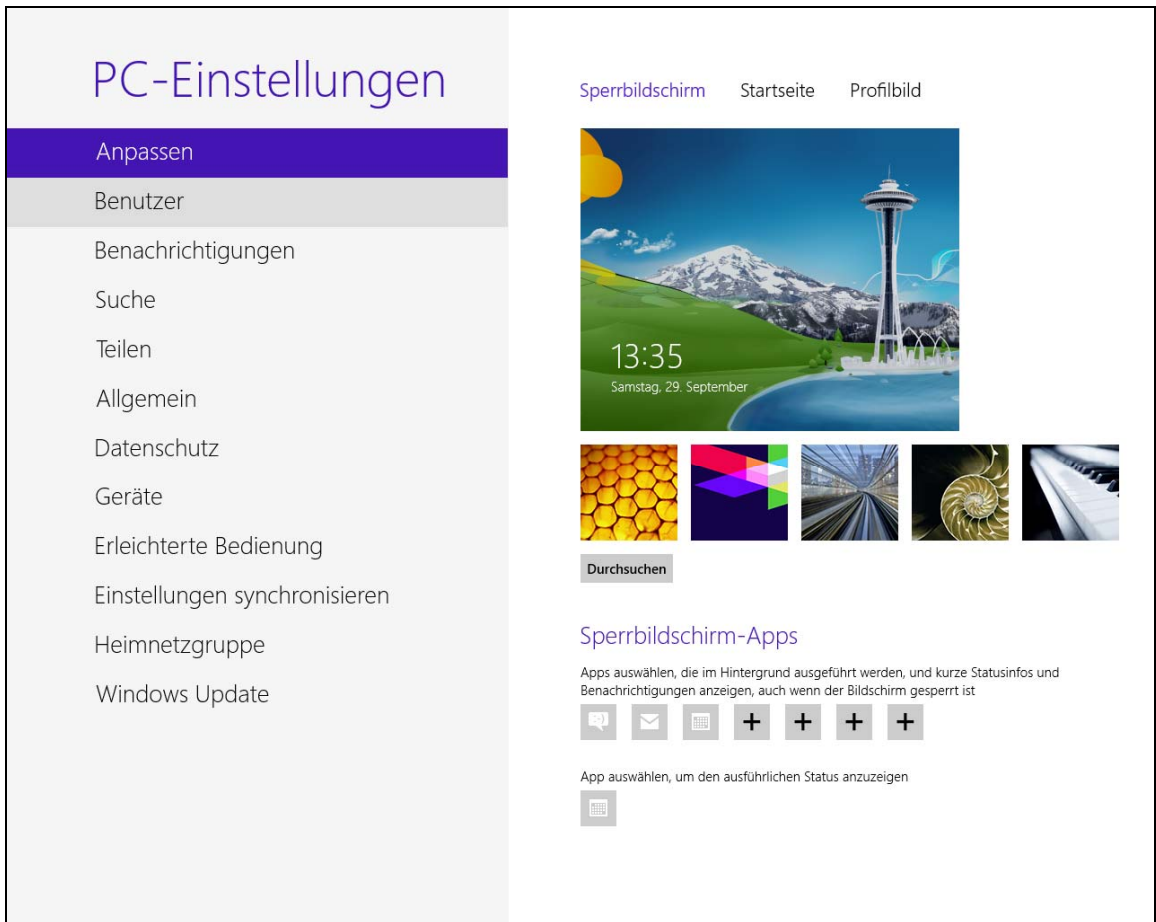


Abbildung 3.1 Die Benutzeroberfläche lässt sich mit den PC-Einstellungen anpassen

Einige Anwendungen, die *Sperrbildschirm-Apps* genannt werden, können im Hintergrund ausgeführt werden und auch bei gesperrtem Bildschirm kurze Statusinformationen und Benachrichtigungen anzeigen. Standardmäßig werden zum Beispiel die Apps *Nachrichten*, *Mail* und *Kalender* entsprechend konfiguriert. Andere auf dem Computer installierte Anwendungen sind vielleicht ebenfalls in der Lage, auf dem Sperrbildschirm kurze Statusangaben und Benachrichtigungen anzuzeigen. Tippen oder klicken Sie in diesem Fall auf die Option *Hinzufügen* (sie wird als Pluszeichen angezeigt) und tippen oder klicken Sie die Anwendung an, die Sie hinzufügen möchten. Um eine Sperrbildschirm-App zu entfernen, tippen oder klicken Sie die Anwendung an und tippen oder klicken auf *Hier keine kurzen Statusinfos anzeigen*.

Einige Apps wie *Kalender* und *Wetter* können auf dem Sperrbildschirm ausführliche Statusinformationen anzeigen, aber im Normalfall kann zu jedem Zeitpunkt immer nur eine dieser Anwendungen ihre Informationen anzeigen. Sie wird unter *App auswählen, um den ausführlichen Status anzuzeigen* angezeigt. Wenn noch keine Anwendung zur ausführlichen Statusanzeige hinzugefügt wurde, tippen oder klicken Sie auf die Option *Hinzufügen* (sie wird als Pluszeichen angezeigt) und tippen oder klicken dann auf die Anwendung, die hinzugefügt werden soll. Um eine Anwendung aus der ausführlichen Statusanzeige zu entfernen, tippen oder klicken Sie die Anwendung an und tippen oder klicken dann auf *Keinen detaillierten Status auf dem Sperrbildschirm anzeigen*.

Anpassen der Startseite und des Profilbilds

Im Bereich *Startseite* können Sie die Gestaltung des Hintergrunds ändern, indem Sie auf das gewünschte Muster tippen oder klicken. Außerdem können Sie eine Farbe für den Hintergrund der Startseite festlegen.

Als Profilbild kann ein beliebiges Bild verwendet werden. Standardmäßig wird eine sehr einfache Grafik angezeigt, die nach der Art eines Passfotos einen Menschen darstellt. Wenn Sie ein Bild von einem anderen Speicherort verwenden möchten, tippen oder klicken Sie auf *Durchsuchen*, navigieren mit den verfügbaren Optionen zum gewünschten Speicherort und suchen das Bild heraus.

Sofern Ihr Computer mit einer Kamera ausgerüstet ist, können Sie ein Profilbild erstellen, indem Sie auf *Kamera* klicken und der Anleitung folgen.

Die Seite *Benutzer*

Auf der Seite *Benutzer* wird das Konto des angemeldeten Benutzers verwaltet. Handelt es sich dabei um ein Microsoft-Konto, können Sie mit den angezeigten Optionen zu einem lokalen Konto wechseln. Handelt es sich bei dem Konto, mit dem sich der aktuelle Benutzer angemeldet hat, um ein lokales Konto, können Sie mit den angezeigten Optionen zu einem Microsoft-Konto wechseln.

Mit den *Anmeldeoptionen* können Sie ein Kennwort für den angemeldeten Benutzer erstellen oder es ändern, sofern die Gruppenrichtlinien dies zulassen. Außerdem können Sie festlegen, ob ein Benutzer bei der Reaktivierung des Computers ein Kennwort eingeben muss.

In einer Arbeits- oder Heimnetzgruppe stehen zwei weitere Anmeldeinformationen zur Verfügung. Sie können einen Bildcode für den angemeldeten Benutzer erstellen. Sie können für den angemeldeten Benutzer auch eine PIN erstellen oder ändern. Weitere Informationen über die Arbeit mit Benutzerkonten finden Sie in Kapitel 7, »Verwalten von Benutzerzugriff und Sicherheit«.

Die Seite *Benachrichtigungen*

Viele Apps können Benachrichtigungen anzeigen. Diese Benachrichtigungen lassen sich auf der Seite *Benachrichtigungen* steuern. Im oberen Bereich finden Sie folgende Benachrichtigungssteuerelemente:

- **App-Benachrichtigungen anzeigen** Legt fest, ob Apps auf der Startseite und auf dem Desktop Benachrichtigungen anzeigen können.
- **App-Benachrichtigungen auf dem Sperrbildschirm anzeigen** Legt fest, ob Apps auf dem Sperrbildschirm Benachrichtigungen anzeigen können.
- **Benachrichtigungstöne wiedergeben** Legt fest, ob Apps Benachrichtigungstöne wiedergeben können.

Tippen oder klicken Sie auf das Steuerelement, um die entsprechenden Benachrichtigungen ein- oder auszuschalten. Außerdem können Sie Benachrichtigungen für einzelne Apps ein- oder ausschalten.

Die Seiten *Suche*, *Teilen* und *Datenschutz*

Die Seite *Suche* ermöglicht die Anpassung der Suche. Windows 8 führt Buch über den Verlauf Ihrer Suchaktionen und kann diese Daten verwenden, um die Apps, nach denen Sie am häufigsten suchen, am Anfang der Ergebnisliste anzuzeigen und um Suchen als zukünftige Suchvorschläge zu speichern. Mit den Suchverlaufsoptionen können Sie diese Mechanismen abschalten und die Verlaufsdaten löschen.

Bei der Suche nach Apps sucht Windows nicht nur nach den Apps, sondern auch nach darin gespeicherten Daten. Bestimmte Apps wie *Mail*, *Musik*, *Fotos* und *News* sind für die Suche konfiguriert. Die Suche

lässt sich für diese Anwendungen separat ein- oder ausschalten. Tippen oder klicken Sie einfach auf die dazugehörige Schaltfläche, um die Suche ein- oder auszuschalten.

In ähnlicher Weise sind bestimmte Anwendungen für ein einfaches Teilen konfiguriert und ermöglichen es Ihnen, Fotos, Dokumente und andere Dinge auf einfache Weise mit anderen Benutzern zu teilen. Auf der Seite *Teilen* können Sie einstellen, wie das Teilen funktioniert. Windows 8 merkt sich, welche Anwendungen Sie zum Teilen verwenden, und kann diese Anwendungen in einer priorisierten Liste anzeigen. Standardmäßig erscheinen bis zu fünf Apps in dieser Liste. Tippen oder klicken Sie auf *Elemente in der Liste*, wenn Sie eine andere Zahl festlegen möchten. Wenn Sie die Liste löschen möchten, tippen oder klicken Sie auf *Liste löschen*.

Bestimmte Apps wie *Mail* und *Kontakte* sind so eingestellt, dass sie automatisch teilen. Das Teilen lässt sich für jede App separat ein- oder ausstellen. Tippen oder klicken Sie einfach auf das dazugehörige Symbol, um das Teilen ein- oder auszuschalten.

Apps können auch Ihren Standort, Ihren Namen und Ihr Profilbild verwenden. Die entsprechenden Einstellungen nehmen Sie auf der Seite *Datenschutz* vor. Tippen oder klicken Sie einfach auf die entsprechende Schaltfläche, um festzulegen, ob diese Informationen in den Apps verfügbar sein sollen.

TIPP Auf der Seite *Allgemein* können Sie unter *App-Wechsel* einstellen, ob ein Benutzer zwischen den zuletzt verwendeten Apps wechseln kann. Wenn dieser Wechsel zwischen den Apps zugelassen ist, führt Windows 8 eine Verlaufsliste über die zuletzt verwendeten Apps. Um diesen Verlauf zu löschen, tippen oder klicken Sie auf *Verlauf löschen*.

Die Seite *Einstellungen synchronisieren*

Wenn der aktuelle Benutzer über ein Microsoft-Konto verfügt, können Sie auf der Seite *Einstellungen synchronisieren* festlegen, wie Einstellungen zwischen Geräten synchronisiert werden. Zu den Einstellungen, die sich synchronisieren lassen, gehören:

- Die Einstellungen des Benutzers von der Seite *Anpassen*
- Die Desktop-Einstellungen für Designs, die Taskleiste und mehr
- Kennwörter für einige Apps, Websites, Netzwerke und Heimnetzgruppen
- Einstellungen für die erleichterte Bedienung und Spracheinstellungen
- Browsereinstellungen, Browserverlauf und Browserfavoriten
- Andere Windows-Einstellungen für den Explorer, die Maus und mehr

Das Hauptsteuerelement ist *Einstellungen auf diesem PC synchronisieren*. Wenn Sie nicht möchten, dass Einstellungen zwischen Geräte synchronisiert werden, schalten Sie diese Option aus. Sollen dagegen einige oder alle Einstellungen zwischen Geräten synchronisiert werden, schalten Sie diese Option ein.

Wenn die Synchronisation zugelassen ist, können Sie mit den Optionen unter *Zu synchronisierende Einstellungen* festlegen, welche Einstellungen synchronisiert werden. Da Windows 8 auch erkennt, wenn ein Computer eine getaktete Verbindung benutzt, beispielsweise ein Mobiltelefonnetz, können Sie die Synchronisation über getaktete Verbindungen ein- oder ausschalten und festlegen, ob eine Synchronisation erfolgen darf, wenn die getaktete Verbindung nicht servergespeichert ist.

Arbeiten mit Desktops und Autostartanwendungen

Im Betriebssystem Windows werden alle Elemente auf dem Desktop und Autostartanwendungen mit Verknüpfungen konfiguriert. Dabei legt der Speicherort der Verknüpfung fest, auf welche Weise sie benutzt wird. Wenn Sie zum Beispiel Autostartanwendungen für alle Benutzer konfigurieren wollen, fügen Sie Verknüpfungen zum Ordner `%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp` hinzu. Diese Anwendungen werden dann automatisch gestartet, sobald sich ein Benutzer lokal am System anmeldet. Wenn Sie für einen bestimmten Benutzer Autostartprogramme einrichten möchten, können Sie Verknüpfungen zum Ordner `%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\StartUp` hinzufügen.

Erstellen von Verknüpfungen für Desktops und Autostart

Im Datei-Explorer erstellen Sie Verknüpfungen für den Desktop, Ordner und Autostartanwendungen für einzelne Benutzer, indem Sie sich am Computer anmelden und Verknüpfungen an den richtigen Speicherorten erstellen. Auch in Gruppenrichtlinien können Sie Verknüpfungen für Desktops, Autostartanwendungen und andere Elemente erstellen. Dazu konfigurieren Sie Richtlinieneinstellungen für Verknüpfungen. Diese Einstellungselemente werden automatisch auf alle Benutzer und Computer angewendet, die das jeweilige Gruppenrichtlinienobjekt verarbeiten.

Gehen Sie folgendermaßen vor, um Einstellungen für Verknüpfungen zu konfigurieren:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und dann *Verknüpfungen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und *Verknüpfungen* auswählen.

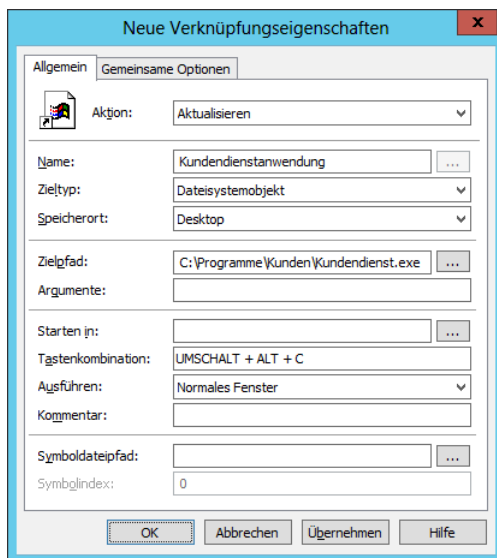


Abbildung 3.2 Erstellen einer Verknüpfung mithilfe eines Einstellungselements

2. Klicken Sie mit der rechten Maustaste auf den Knoten *Verknüpfungen* oder halten Sie den Knoten gedrückt, und wählen Sie den Befehl *Neu/Verknüpfung*. Daraufhin öffnet sich das Eigenschaftendialogfeld der neuen Verknüpfung (Abbildung 3.2).
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Erstellen*, *Aktualisieren* oder *Ersetzen* aus. Konfigurieren Sie nun die anderen Optionen, wie in diesem Abschnitt beschrieben.
4. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsame Optionen* fest, wie die Einstellungen angewendet werden. In vielen Fällen ist es sinnvoll, eine Verknüpfung nur ein einziges Mal anzuwenden. Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmal anwenden*.
5. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

In der Dropdownliste *Speicherort* sind die Spezialordner aufgeführt, in denen Sie Ihre Verknüpfung ablegen können. Tabelle 3.1 fasst diese Ordner zusammen.

Verknüpfungen können auf lokale oder Netzwerkdateien sowie auf Internetressourcen verweisen. Die Verknüpfungen für lokale oder Netzwerkdateien werden als *Linkverknüpfungen* bezeichnet, die Verknüpfungen mit Internetressourcen als *URL-Verknüpfungen*.

Linkverknüpfungen dienen normalerweise dazu, Anwendungen zu starten oder Dokumente zu öffnen; sie öffnen keine URL in einem Browser. Daher haben Linkverknüpfungen andere Eigenschaften als URL-Verknüpfungen. Diese Eigenschaften sind in Tabelle 3.2 zusammengefasst. Wenn Sie irgendeine Eigenschaft falsch einstellen oder eine Eigenschaft zuweisen, die nicht von einer verknüpften Anwendung unterstützt wird, kann es sein, dass die Verknüpfung nicht erstellt wird oder nicht wie erwartet funktioniert. In diesem Fall müssen Sie das Problem beseitigen und erneut versuchen, die Verknüpfung anzulegen.

Tabelle 3.1 Spezielle Ordner für Verknüpfungen

Spezielle Ordner	Verwendung
<i>Alle Benutzer – Desktop</i>	Desktopverknüpfungen für alle Benutzer
<i>Alle Benutzer – Menü "Start"</i>	Optionen im Startmenü für alle Benutzer
<i>Alle Benutzer – Programme</i>	Menüoptionen in <i>Alle Programme</i> für alle Benutzer
<i>Alle Benutzer – Starten</i>	Autostartanwendungen für alle Benutzer
<i>Alle Benutzer – Explorer-Favoriten</i>	Explorer-Favoriten für alle Benutzer
<i>Desktop</i>	Desktopverknüpfungen für einen bestimmten Benutzer
<i>Explorer-Favoriten</i>	Verknüpfungen im Menü <i>Favoriten</i> für einen bestimmten Benutzer
<i>Explorer-Links</i>	Linkfavoriten für einen bestimmten Benutzer
<i>Netzwerkumgebung</i>	Netzwerkverknüpfungen für einen bestimmten Benutzer
<i>Programme</i>	Optionen im Menü <i>Alle Programme</i> für einen bestimmten Benutzer
<i>Schnellstart-Symbolleiste</i>	Symbolleistenordner mit Verknüpfungen für einen bestimmten Benutzer
<i>Senden an</i>	Verknüpfungen im Menü <i>Senden an</i> für einen bestimmten Benutzer
<i>Start</i>	Autostartanwendungen für einen bestimmten Benutzer
<i>Startmenü</i>	Startmenüverknüpfungen für einen bestimmten Benutzer
<i>Zuletzt verwendet</i>	Verknüpfungen der zuletzt verwendeten Dokumente für einen bestimmten Benutzer

Tabelle 3.2 Eigenschaften von Linkverknüpfungen

Eigenschaft	Beschreibung	Beispielwert
<i>Argumente</i>	Argumente, die an eine Anwendung übergeben werden, die über die Verknüpfung gestartet wird	<i>C:\Gettingstarted.doc</i>
<i>Ausführen</i>	Der Fensterstil der Anwendung, die von der Verknüpfung gestartet wird. Zur Auswahl stehen die Stile <i>Normales Fenster</i> , <i>Minimiert</i> und <i>Maximiert</i> .	Normales Fenster
<i>Kommentar</i>	Eine aussagekräftige Beschreibung für die Verknüpfung	Öffnet das Erste-Schritte-Dokument
<i>Name</i>	Der Name der Verknüpfung	Erste Schritte
<i>Speicherort</i>	Gibt an, wo die Verknüpfung erstellt werden soll.	Desktop
<i>Starten in</i>	Das Arbeitsverzeichnis der Anwendung, die von der Verknüpfung gestartet wird	<i>C:\Working</i>
<i>Symboldateipfad</i>	Der Speicherort eines Symbols (Icon) für die Verknüpfung. Falls diese Eigenschaft keinen Wert zugewiesen hat, wird ein Standardsymbol verwendet.	<i>C:\Program Files\Internet Explorer\IEXPLORE.EXE</i>
<i>Symbolindex</i>	Der Index des Symbols für die Verknüpfung. Nur wenige Anwendungen haben mehrere Symbole, daher ist der Index fast immer 0.	0
<i>Tastenkombination</i>	Ein Tastenkürzel, das die Verknüpfung ausführt. Diese Eigenschaft kann nur für Desktopverknüpfungen und Startmenüoptionen benutzt werden.	ALT+UMSCHALT+Z
<i>Zielpfad</i>	Der Pfad der Datei, die ausgeführt wird	<i>%WinDir%\Notepad.exe</i>
<i>Zieltyp</i>	Der Typ der Verknüpfung, die Sie erstellen. Wählen Sie <i>Dateisystemobjekt</i> für Linkverknüpfungen, <i>URL</i> für URL-Verknüpfungen und <i>Shellobjekt</i> für Explorer-Shellverknüpfungen.	Dateisystemobjekt

Eine der nützlichsten Optionen ist die Eigenschaft *Argumente*. Mithilfe dieser Eigenschaft können Sie Argumente festlegen, die an die gestartete Anwendung übergeben werden. Auf diese Art können Sie beispielsweise eine Verknüpfung anlegen, die Microsoft Office Word startet und ein bestimmtes Dokument öffnet. Dazu tragen Sie den Zielpfad für Word ein und übergeben als Argument das Dokument, das geöffnet werden soll.

Wenn Sie Verknüpfungen zum Desktop oder zu Menüs hinzufügen, können Sie ein Tastenkürzel festlegen, das die Verknüpfung aufruft. Tastenkürzel müssen mindestens eine Zusatztaste und eine Haupttaste haben. Folgende Zusatztasten stehen zur Auswahl:

- **ALT** Die ALT-Taste
- **STRG** Die STRG-Taste
- **UMSCHALT** Die UMSCHALT-Taste

Zusatztasten können Sie beliebig kombinieren, zum Beispiel ALT+STRG oder UMSCHALT+STRG, aber die Kombination sollte keine Tastenkürzel ergeben, die bereits für andere Verknüpfungen verwendet werden. Haupttasten sind die Buchstaben A–Z und die Ziffern 0–9, außerdem ENDE, POS1, BILD-AUF und BILD-AB. Zum Beispiel können Sie eine Verknüpfung definieren, die das Tastenkürzel UMSCHALT+ALT+G verwendet.

Wenn Sie Verknüpfungen für Anwendungen anlegen, haben die Anwendungen normalerweise ein Standardsymbol, das in der Verknüpfung angezeigt wird. Erstellen Sie etwa eine Verknüpfung für den Internet Explorer, wird das Standardsymbol mit dem blauen »e« angezeigt. Wenn Sie Verknüpfungen mit Dokumentdateien erstellen, wird in den meisten Fällen das Windows-Standardsymbol verwendet.

Wollen Sie ein anderes Symbol als das Standardsymbol benutzen, können Sie die Eigenschaft *Symbol-dateipfad* einstellen. Normalerweise ist das Symbol in derselben Datei gespeichert wie die Anwendung, zum Beispiel *Iexplore.exe* oder *Notepad.exe*, und der Symbolindex ist 0. Windows muss in der Lage sein, die ausführbare Datei zu finden. Wird die ausführbare Datei nicht im Pfad gefunden, kann das Symbol nicht ausgelesen werden. Achten Sie daher darauf, dass Sie den vollständigen Pfad zur ausführbaren Datei eintragen.

Das Arbeitsverzeichnis legt das Standardverzeichnis für eine Anwendung fest. Dieses Verzeichnis wird verwendet, wenn ein Benutzer zum ersten Mal Dateien öffnet oder speichert.

URL-Verknüpfungen öffnen Internetdokumente in einer geeigneten Anwendung. Beispielsweise werden Webseiten im Standardbrowser geöffnet, etwa dem Internet Explorer. Für URL-Verknüpfungen stehen die Eigenschaften *Argumente*, *Starten in*, *Ausführen* und *Kommentar* nicht zur Verfügung.

Hinzufügen oder Entfernen von Autostartprogrammen

Vom Administrator oder Benutzer installierte Programme, die im Hintergrund ausgeführt werden, können mit dem *StartUp*-Ordner verwaltet werden. Autostartprogramme, die nur für den aktuell angemeldeten Benutzer gestartet werden, sind im *StartUp*-Ordner aus den Profildaten dieses Benutzers gespeichert (unter *%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs*). Autostartprogramme, die für alle Benutzer verfügbar sind, die sich am Computer anmelden, werden im *Startup*-Ordner für alle Benutzer gespeichert (unter *%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs*).

Mit folgenden Schritten können Sie Autostartprogramme für alle Benutzer hinzufügen oder entfernen:

1. Wechseln Sie im Datei-Explorer in den verborgenen Ordner *%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu*. Wenn die verborgenen Elemente nicht angezeigt werden, tippen oder klicken Sie auf *Ansicht* und aktivieren in der Gruppe *Ein-/ausblenden* dann das Kontrollkästchen *Ausgeblendete Elemente*.
2. Tippen oder klicken Sie im linken Fensterabschnitt unter dem Ordner *Startmenü* auf den Ordner *Programme* und dann auf *Autostart*.
3. Nun können Sie Autostartprogramme für alle Benutzer hinzufügen oder entfernen. Wenn Sie ein Autostartprogramm hinzufügen möchten, erstellen Sie eine Verknüpfung mit dem Programm, das gestartet werden soll. Um ein Autostartprogramm zu entfernen, löschen Sie seine Verknüpfung aus dem *Autostart*-Ordner.

Mit folgenden Schritten können Sie Autostartprogramme für einen bestimmten Benutzer hinzufügen oder entfernen:

1. Melden Sie sich als der Benutzer an, dessen Autostartanwendungen Sie verwalten wollen. Wechseln Sie im Datei-Explorer in den verborgenen Ordner *%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu*.
2. Tippen oder klicken Sie im linken Fensterabschnitt unter *Startmenü* auf den Ordner *Programme* und dann auf *Autostart*.
3. Nun können Sie Autostartprogramme für diesen Benutzer hinzufügen oder entfernen. Wenn Sie ein Autostartprogramm hinzufügen möchten, erstellen Sie eine Verknüpfung mit dem Programm, das gestartet werden soll. Um ein Autostartprogramm zu entfernen, löschen Sie seine Verknüpfung aus dem *Autostart*-Ordner.

HINWEIS

Genau genommen brauchen Sie sich nicht als der Benutzer anzumelden, dessen Autostartanwendungen Sie verwalten möchten, aber es erleichtert die Arbeit. Wenn Sie sich nicht als dieser Benutzer anmelden können, wechseln Sie in den Ordner *Benutzer (Users)* auf dem Systemlaufwerk und arbeiten sich nach unten bis in die Ordner vor, in denen das Benutzerprofil des betreffenden Benutzers gespeichert ist. Die Benutzerprofile werden nach Kontennamen getrennt.

In Gruppenrichtlinieneinstellungen legen Sie fest, welche Anwendungen automatisch nach dem Anmelden eines Benutzers gestartet werden sollen, indem Sie Verknüpfungen in den Ordnern *Alle Benutzer – Starten* und *Start* erstellen. Der Ordner *Alle Benutzer – Starten* enthält die Autostartanwendungen für alle Benutzer, die sich am System anmelden. Der Ordner *Start* legt die Autostartanwendungen für den aktuellen Benutzer fest.

Wenn Sie eine Verknüpfung für eine Autostartanwendung erstellen, brauchen Sie gewöhnlich nur die Optionen *Name*, *Zieltyp*, *Speicherort* und *Pfad* zu konfigurieren. Gelegentlich ist es außerdem sinnvoll, ein Arbeitsverzeichnis für eine Anwendung einzutragen oder Argumente zu übergeben.

Falls Sie eine Autostartanwendung später wieder entfernen wollen, können Sie dazu eine Richtlinieneinstellung erstellen, bei der als Aktion der Eintrag *Löschen* ausgewählt ist.

Anpassen der Taskleiste

Die Taskleiste bietet einen schnellen Zugriff auf oft benötigte Informationen und aktive Anwendungen. Sie können das Verhalten und die Eigenschaften der Taskleiste auf vielfältige Weise ändern. Dieser Abschnitt beschreibt die wichtigsten Methoden.

Funktionsweise der Taskleiste

Die Taskleiste ist einer der am wenigsten beachteten Bereiche des Windows-Desktops. Benutzer und Administratoren neigen dazu, ihrer Einstellung nur wenig Aufmerksamkeit zu schenken, obwohl wir sie Tag für Tag verwenden und uns darauf verlassen, dass sie für den schnellen Zugriff auf praktisch alles zur Verfügung steht, was wir im Windows-Betriebssystem tun. Wenn Sie feststellen, dass Benutzer öfters Probleme mit dem Zugriff auf bestimmte Windows-Funktionen oder der Ausführung von Anwendungen haben, können Sie das ändern, indem Sie die Taskleiste an die Bedürfnisse der Benutzer anpassen. Die Windows-Taskleiste kann mehrere Symbolleisten enthalten, die den Benutzer auf unterschiedlichste Arten unterstützen können.

Manchmal ergeben sich erstaunliche Produktivitätssteigerungen dadurch, dass man ein häufig benutztes Element auf der Taskleiste unterbringt. Die meisten Leute verbringen zum Beispiel viel Zeit damit, Dokumente zu suchen und zu lesen. Sie wühlen im Internet oder im Intranet der Organisation herum, um die neusten Informationen zu finden. Sie öffnen Dokumente in Microsoft Word, Excel, PowerPoint und anderen Anwendungen, suchen nach einzelnen Dokumenten und starten einzelne Anwendungen, um diese einzelnen Dokumente zu lesen. Nach dem Hinzufügen einer Adressleiste zur Taskleiste können Benutzer direkt auf Dokumente zugreifen und die zuständige Anwendung automatisch öffnen. Sie brauchen nur den Pfadnamen des Dokuments einzugeben und die EINGABETASTE zu drücken. Mit der Zeit erscheinen mehr und mehr der häufiger verwendeten Dokumente in der Verlaufsliste der Adressleiste, was dem Benutzer das Auffinden der gewünschten Information weiter erleichtert.

Verknüpfungen an die Taskleiste anheften

Windows 8 hat keine Schnellstartleiste. Stattdessen können Sie in Windows 8 häufig benutzte Programme direkt auf der Taskleiste anheften oder fixieren. Diese Möglichkeit haben Sie zum Beispiel, wenn Sie mit dem Startbildschirm arbeiten. Klicken Sie einfach mit der rechten Maustaste auf ein Element, das Sie zur Taskleiste hinzufügen möchten, oder halten Sie es gedrückt, und wählen Sie den Befehl *An Taskleiste anheften*. Sobald Sie ein Element an der Taskleiste angeheftet haben, können Sie die Position des Elements in der Taskleiste ändern, indem Sie sein Symbol antippen oder anklicken und ziehen (oder verschieben). Wollen Sie ein Element wieder aus der Taskleiste entfernen, klicken Sie mit der rechten Maustaste auf das Element oder halten es gedrückt und wählen den Befehl *Dieses Programm von der Taskleiste lösen*.

Ändern der Größe und Position der Taskleiste

Standardmäßig erscheint die Taskleiste am unteren Bildschirmrand und ist in der Größe so eingestellt, dass eine Zeile mit Optionen sichtbar ist. Solange die Position der Taskleiste nicht fixiert ist, können Sie sie aber an jeder Kante des Windows-Desktops andocken und ihre Größe nach Bedarf einstellen. Zum Verschieben der Taskleiste tippen oder klicken Sie sie einfach an und ziehen sie zu einer anderen Kante des Desktops. Während Sie die Taskleiste verschieben, wird sie am Rand des Windows-Desktops angezeigt. Sobald Sie die Maustaste oder die Taskleiste loslassen, erscheint die Taskleiste an ihrer neuen Position. Zur Größeneinstellung der Taskleiste bewegen Sie den Mauszeiger auf die der Bildschirmmitte zugewandte Kante und ziehen sie auf die gewünschte Größe.

Automatisches Ausblenden, Fixieren und Steuern der Sichtbarkeit der Taskleiste

Wenn Sie die Sichtbarkeit der Taskleiste kontrollieren möchten, stehen mehrere Optionen zur Wahl. Sie können die Taskleiste so einstellen, dass sie automatisch ausgeblendet wird, wenn sie nicht benutzt wird. Sie können die Taskleiste fixieren, damit sich weder ihre Größe noch ihre Position verändern lässt. Sie können die Taskleiste auch an einer bestimmten Position und in einer bestimmten Form anzeigen. Sobald die Größe und Position der Taskleiste so eingestellt ist, wie der Benutzer sie haben will, sollten Sie die Taskleiste fixieren. Auf diese Weise hat sie eine feste Position und der Benutzer muss nicht erst nach ihr suchen. Gehen Sie folgendermaßen vor, um die Taskleiste zu konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf die Taskleiste oder halten Sie sie gedrückt, und wählen Sie den Befehl *Eigenschaften*.
2. Wählen Sie auf der Registerkarte *Taskleiste* die gewünschten Optionen für Aussehen und Verhalten. Sie können die Taskleiste fixieren oder dafür sorgen, dass sie automatisch ausgeblendet wird oder kleine Symbole verwendet.
3. Legen Sie in der Dropdownliste *Position der Taskleiste auf dem Bildschirm* die Anordnung der Taskleiste auf dem Desktop fest. Es stehen *Unten*, *Links*, *Rechts* und *Oben* zur Wahl.
4. Stellen Sie in der Dropdownliste *Schaltflächen der Taskleiste* ein, ob Taskleistenschaltflächen zusammengefasst und Beschriftungen ausgeblendet werden sollen. Wählen Sie *Immer gruppieren*, *Beschriftungen ausblenden*, wenn Schaltflächen desselben Typs zusammengefasst und ihre Beschriftungen ausgeblendet werden sollen. Wählen Sie *Gruppieren*, wenn die Taskleiste voll ist, um Schaltflächen nur dann zusammenzufassen, wenn kein Platz mehr auf der Taskleiste ist. Wenn die Schaltflächen niemals zusammengefasst werden sollen, können Sie *Nie gruppieren* auswählen.
5. Tippen oder klicken Sie auf *OK*.

TIPP Die Fixierung der Taskleiste ist eine der nützlichsten Taskleistenoptionen. Wenn Sie die Taskleiste nach der optimalen Einstellung fixieren, haben Benutzer weniger Probleme mit versehentlichen Änderungen der Taskleistenoptionen. Die Fixierung hindert Benutzer nicht daran, die Taskleiste absichtlich anders einzustellen. Wenn Benutzer tatsächlich die Taskleiste ändern möchten, brauchen sie sie nur mit der rechten Maustaste anzuklicken oder gedrückt zu halten und dann das Kontrollkästchen *Taskleiste fixieren* zu deaktivieren.

Steuern der Anwendungen im Infobereich

Der Infobereich (oder der Systembereich) ist der Bereich am rechten Ende der Taskleiste, in dem die Systemuhr und Benachrichtigungssymbole von Anwendungen angezeigt werden. Die zwei Standardbenachrichtigungssymbole sind das Wartungscenter und die Netzwerkkonsole. Wenn Sie auf die Symbole im Infobereich zeigen, wird ein kleines Feld mit Informationen über die betreffende Anwendung angezeigt. Um eine Anwendung in diesem Bereich zu bedienen, klicken Sie das Anwendungssymbol mit der rechten Maustaste an oder halten es gedrückt, um ein Menü mit den verfügbaren Optionen zu öffnen. Jede Anwendung bietet andere Menüoptionen an, von denen die meisten für den schnellen Zugriff auf Standardfunktionen gedacht sind.

Sie können den Infobereich auf verschiedene Weise optimieren, indem Sie die Eigenschaften des Infobereichs einstellen, von denen es abhängt, ob Systemsymbole wie die Uhr, die Lautstärkeeinstellung und die Netzwerkverbindung angezeigt werden und ob Anwendungssymbole generell angezeigt werden oder nicht.

Steuern der Symbolanzeige im Infobereich

Der Infobereich zeigt Anwendungs- und Systemsymbole an. Anwendungssymbole werden aus verschiedenen Gründen im Infobereich angezeigt. Manche Programme, wie beispielsweise das Wartungscenter, werden von Windows selbst verwaltet. Ihre Symbole erscheinen immer dann, wenn dem Benutzer Benachrichtigungen mitgeteilt werden müssen. Andere Programme werden beim Betriebssystemstart geladen und im Hintergrund ausgeführt, wie zum Beispiel ein Antivirenprogramm. Gewöhnlich können Sie dann in der Anwendung oder im Installationsprogramm für die Anwendung festlegen, ob im Infobereich Symbole angezeigt werden sollen oder nicht. Windows 8 bietet eine allgemeine Schnittstelle zur Steuerung der Symbolanzeige im Infobereich. Sie können für jede Anwendung individuell festlegen, ob und wie Symbole angezeigt werden sollen.

Zur Steuerung der Anzeige von Anwendungssymbolen im Infobereich gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Taskleiste oder halten Sie die Taskleiste gedrückt, und wählen Sie den Befehl *Eigenschaften*.
2. Tippen oder klicken Sie auf der Registerkarte *Taskleiste* unter *Infobereich* auf die Schaltfläche *Anpassen*, um die Seite *Infobereichsymbole* zu öffnen (Abbildung 3.3).
3. Wenn Sie wollen, dass alle Symbole angezeigt werden, brauchen Sie nur das Kontrollkästchen *Immer alle Symbole und Benachrichtigungen auf der Taskleiste anzeigen* zu aktivieren und auf *OK* zu tippen oder zu klicken. Überspringen Sie in diesem Fall die restlichen Schritte.
4. Deaktivieren Sie das Kontrollkästchen *Immer alle Symbole und Benachrichtigungen auf der Taskleiste anzeigen*, wenn Sie die Anzeige der Symbole einzeln anpassen wollen. Nun können Sie das Benachrichtigungsverhalten optimieren. Zu jedem Eintrag in der linken Spalte gibt es in der rechten Spalte ein Auswahlménü mit folgenden Optionen:

- **Symbol und Benachrichtigungen ausblenden** Das Symbol und die Benachrichtigungen werden nie angezeigt.
 - **Nur Benachrichtigungen anzeigen** Es werden nur Benachrichtigungen angezeigt.
 - **Symbol und Benachrichtigungen anzeigen** Es werden immer das Symbol und Benachrichtigungen angezeigt.
5. Tippen oder klicken Sie zweimal auf OK, wenn Sie die Benachrichtigungseinträge konfiguriert haben.

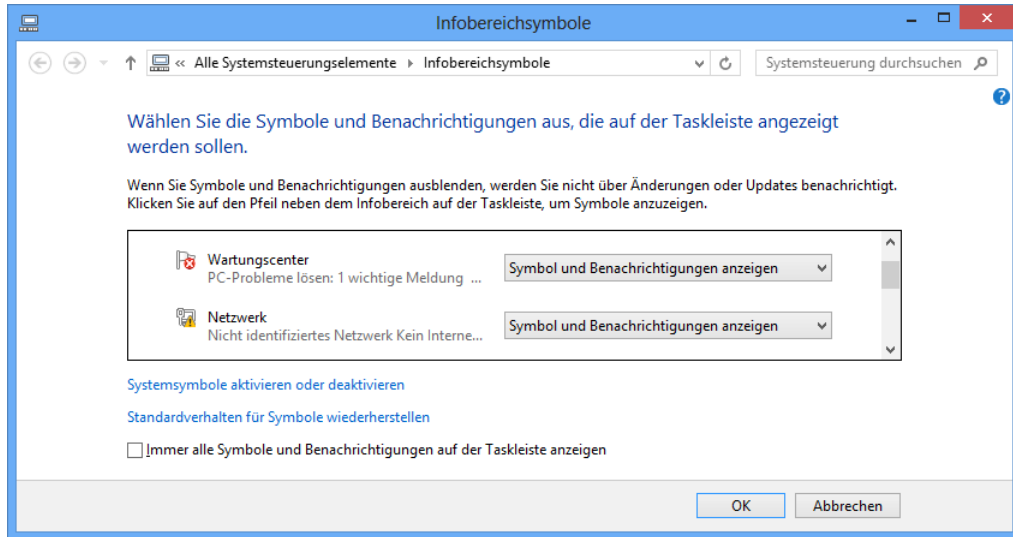


Abbildung 3.3 Konfigurieren der Benachrichtigungssymbole

Optimieren der Symbolleisten

Für die Taskleiste sind mehrere Symbolleisten verfügbar. Den meisten Benutzern dürfte die Symbolleiste *Schnellstart* bekannt sein (in älteren Windows-Versionen, aber nicht mehr in Windows 8), die den schnellen Zugriff auf oft benutzte Anwendungen und den Windows-Desktop ermöglichte. Die Taskleiste kann mehrere Symbolleisten anzeigen, die in Windows 8 enthalten sind. Außerdem können Benutzer auch selbst Symbolleisten erstellen.

Anzeigen von Symbolleisten

Für die Taskleiste stehen folgende Symbolleisten zur Verfügung:

- **Adresse** Zeigt ein Adresseingabefeld, in dem Sie URLs (Uniform Resource Locators) und andere Adressen eingeben können, auf die Sie zugreifen möchten, sei es im Internet, im lokalen Netzwerk oder auf dem lokalen Computer. Wenn Sie einen vollständigen Pfadnamen angeben, wird automatisch die zuständige Anwendung gestartet, um die angegebene Datei zu öffnen.
- **Links** Bietet Zugang zum Ordner *Links* aus dem Menü *Favoriten* des Internet Explorers. Um Verknüpfungen mit Dateien, Internetseiten oder anderen Ressourcen hinzuzufügen, ziehen Sie eine passende Verknüpfung auf die *Links*-Symbolleiste. Zum Entfernen einer Verknüpfung klicken Sie die Verknüpfung mit der rechten Maustaste an oder halten sie gedrückt, und wählen *Löschen*. Wenn Sie dazu aufgefordert werden, bestätigen Sie den Vorgang mit *Ja*.

- **Desktop** Bietet Zugriff auf alle Verknüpfungen, die auf dem lokalen Desktop liegen. Sie brauchen also weder die Anwendungsfenster zu minimieren noch die Schaltfläche *Desktop anzeigen* rechts auf der Taskleiste anzuklicken, um auf diese Verknüpfungen zuzugreifen.
- **Bildschirmtastatur** Bietet schnellen Zugang zur Bildschirmtastatur.

Um Symbolleisten anzuzeigen oder auszublenden, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Taskleiste oder halten Sie sie gedrückt, um das Kontextmenü zu öffnen.
2. Zeigen Sie auf *Symbolleisten* und klicken Sie dann in der Liste auf den Namen der gewünschten Symbolleiste. Dadurch wird die Symbolleiste ein- oder ausgeschaltet.

TIPP Standardmäßig werden alle Symbolleisten mit einem Namen angezeigt. Sie können die Anzeige des Namens abschalten, indem Sie die Symbolleiste mit der rechten Maustaste anklicken und dann auf *Titel anzeigen* klicken, um diesen Befehl zu deaktivieren. Wenn die Taskleiste fixiert ist, müssen Sie die Fixierung zuvor aufheben, indem Sie im Kontextmenü auf *Taskleiste fixieren* klicken.

Erstellen persönlicher Symbolleisten

Sie können auch neue Symbolleisten für Benutzer erstellen. Auch selbsterstellte Symbolleisten haben einen Ordner als Basis, und ihre Schaltflächen hängen vom Inhalt dieses Ordners ab. Die meisten Symbolleisten, die Sie erstellen werden, verweisen wahrscheinlich auf freigegebene Netzwerkordner. Wenn zum Beispiel alle Benutzer Zugriff auf den freigegebenen Ordner *CorpData* haben, in dem Firmendaten gespeichert werden, und auf einen Ordner *UserData*, in dem persönliche Informationen liegen, können Sie die Taskleiste durch Symbolleisten ergänzen, die auf diese Ordner verweisen. Will der Benutzer auf einen dieser Ordner zugreifen, tippt oder klickt er einfach die entsprechende Schaltfläche an.

Neue Symbolleisten können Sie auf folgende Weise erstellen:

1. Klicken Sie mit der rechten Maustaste auf die Taskleiste oder halten Sie die Taskleiste gedrückt, um das Kontextmenü zu öffnen. Zeigen Sie auf *Symbolleisten* und tippen oder klicken Sie auf *Neue Symbolleiste*. Daraufhin öffnet sich das Dialogfeld *Neue Symbolleiste – Ordner auswählen*, das dem üblichen *Öffnen*-Dialogfeld ähnelt.
2. Wechseln Sie in den Ordner, in dem Sie Ihre neue Symbolleiste aufbauen wollen.
3. Wenn Sie auf *Ordner auswählen* tippen oder klicken, wird der Ordner auf der Taskleiste als neue Symbolleiste angezeigt. Wenn Sie nun Verknüpfungen zu diesem Ordner hinzufügen, erscheinen sie auch als Elemente auf der Symbolleiste. Und wenn Sie die Verknüpfungen aus dem Ordner löschen, verschwinden sie auch von der Symbolleiste.

HINWEIS Was selbstdefinierte Symbolleisten betrifft, gibt es eine gute und eine schlechte Nachricht. Die gute Nachricht lautet, dass die meisten Benutzer sie für nützlich halten. Die schlechte Nachricht ist folgende: Sollte ein Benutzer eine selbstdefinierte Symbolleiste schließen, muss die Leiste neu erstellt werden, bevor sie sich wieder auf der Taskleiste anzeigen lässt.

Verwenden von Designs

Mit »Design« ist eine Kombination von Hintergrund und Sounds, Symbolen und anderen Elementen gemeint, mit denen sich der Desktop und die Betriebssystemumgebung an die persönlichen Vorlieben anpassen lassen. Administratoren tendieren dazu, Designs zu hassen, während Benutzer dazu neigen, Designs zu mögen. In diesem Abschnitt erfahren Sie, was es mit Designs auf sich hat, wie man einzelne Details anpasst, und natürlich wie man Designs löscht.

Anwenden und Entfernen von Designs

Es sind verschiedene vorgefertigte Designs verfügbar. Manche Designs werden bei der Installation des Betriebssystems installiert. Um ein Design anzuwenden, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten sie dort eine Stelle gedrückt, und wählen Sie *Anpassen*. Dadurch wird die Konsole *Anpassung* der Systemsteuerung geöffnet (Abbildung 3.4).

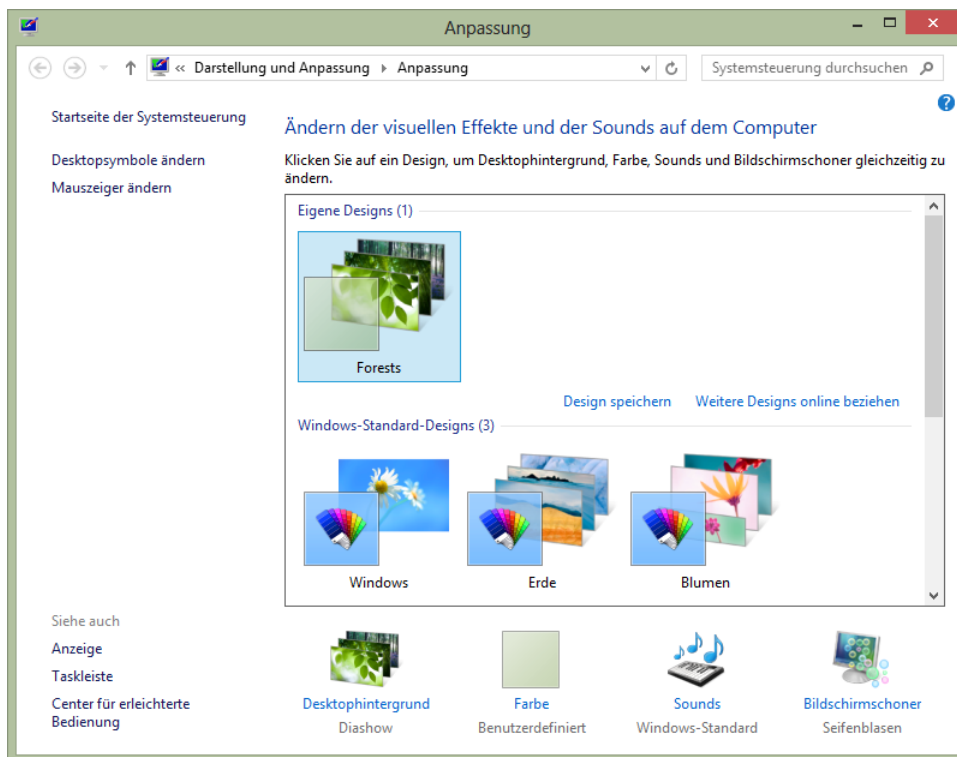


Abbildung 3.4 In der Konsole *Anpassung* können Sie verschiedene Dialogfelder zur Einstellung des Designs, der Anzeige und anderer Dinge öffnen

2. Wählen Sie in der Liste das gewünschte Design aus. Sie können ein Design von der Microsoft-Website verwenden, indem Sie auf *Weitere Designs online beziehen* klicken, woraufhin sich die Microsoft-Website in Ihrem Standardbrowser öffnet. Sie verwenden ein Onlinedesign, indem Sie es auswählen und auf *Speichern* tippen oder klicken. Wählen Sie einen Speicherort aus, wenn Sie dazu aufgefordert

werden. Warten Sie, bis der Download beendet ist, und tippen oder klicken Sie dann im Dialogfeld *Download abgeschlossen* auf *Öffnen*. Das Design ist nun verfügbar und kann angewendet werden.

3. Im unteren Teil der Konsole *Anpassung* finden Sie einige Optionen für das ausgewählte Design. Tippen oder klicken Sie auf eines dieser Elemente, um es zu ändern.

Zur Wiederherstellung des ursprünglichen Designs gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten sie dort eine Stelle gedrückt, und wählen Sie *Anpassen*.
2. Wählen Sie *Windows* als Design aus.

TIPP Da die Anzeige des Designs vom Designdienst (*Themes*) gesteuert wird, können Sie diesen Dienst anhalten, wenn Sie das Design zum Beispiel im Rahmen einer Fehlersuche schnell ausschalten möchten, ohne die Designeinstellung zu ändern. Mit folgendem Befehl können Sie den Designdienst in einer Eingabeaufforderung mit erhöhten Rechten anhalten: **net stop themes**. Um den Designdienst neu zu starten, geben Sie in einer Eingabeaufforderung mit erhöhten Rechten folgenden Befehl ein: **net start themes**.

Anpassen und Erweitern von Designs

Wenn Sie ein Design auf den Windows-Desktop anwenden, können davon viele verschiedene Einstellungen betroffen sein. Oft ist es so, dass den Benutzern ein bestimmtes Design im Prinzip gefällt, bis auf ein paar Dinge wie beispielsweise der Sound. Um dieses Problem zu lösen, können Sie die Systemeinstellungen ändern, die dem Benutzer nicht gefallen, und das aktualisierte Design speichern, damit der Benutzer es später wiederherstellen kann.

Sie verwalten Designs in der Konsole *Anpassung*, die Sie öffnen, indem Sie mit der rechten Maustaste auf einen freien Bereich des Desktops klicken oder diese Stelle gedrückt halten und den Befehl *Anpassen* wählen. Die wichtigsten Einstellungen in der Konsole *Anpassung*, auf die sich ein Design auswirken kann, sind folgende:

- **Bildschirmschoner** Zur Einstellung des Bildschirmschoners tippen oder klicken Sie auf *Bildschirmschoner*. Wählen Sie im Dialogfeld *Bildschirmschonereinstellungen* einen Bildschirmschoner aus oder wählen Sie (*Kein*), wenn Sie keinen Bildschirmschoner wünschen. Tippen oder klicken Sie anschließend auf *OK*.
- **Sounds** Zur Änderung des Sounds tippen oder klicken Sie auf *Sounds*. Wählen Sie aus der Liste *Soundschema* des Dialogfelds *Sound* eine andere Zusammenstellung an Programmereignisgeräuschen aus. Zur Wiederherstellung der Standardvorgabe wählen Sie *Windows-Standard*. Um die Geräusche abzuschalten, wählen Sie *Keine Sounds*. Tippen oder klicken Sie auf *OK*. Wenn Sie die Sounds abschalten, empfiehlt es sich, auch das Kontrollkästchen *Windows-Startsound wiedergeben* zu deaktivieren.
- **Mauszeiger** Sie ändern die Mauszeiger, indem Sie im linken Fensterabschnitt auf *Mauszeiger ändern* tippen oder klicken. Wählen Sie im Dialogfeld *Eigenschaften von Maus* auf der Registerkarte *Zeiger* im Feld *Schema* einen anderen Satz Mauszeiger aus. Tippen oder klicken Sie auf *OK*.
- **Desktophintergrund** Sie ändern den Desktophintergrund, indem Sie auf *Desktophintergrund* tippen oder klicken. Wählen Sie in der Liste *Bildpfad* den Speicherort der Bilder aus, die Sie als Hintergrund anzeigen wollen. Tippen oder klicken Sie auf *Durchsuchen*, um das Dialogfeld *Ordner suchen* zu öffnen. Sie können auch Windows-Desktophintergründe aus dem Ordner `%SystemRoot%\Web\Wallpaper` auswählen, in dem die mit Windows 8 gelieferten Standardhintergrundbilder abgelegt sind.

Tippen oder klicken Sie auf den Hintergrund, den Sie verwenden wollen, legen Sie die Bildposition fest und tippen oder klicken Sie auf *Änderungen speichern*.

- **Farbschema** Tippen oder klicken Sie auf *Farbe*, um das Farbschema zu ändern. Tippen oder klicken Sie auf die Farbe, die Sie verwenden möchten, und dann auf *Änderungen speichern*.

Löschen benutzerdefinierter Designs

Designs, die Benutzer aus anderen Quellen importieren, können auf der Festplatte viel Platz einnehmen. Um ein Design und die dazugehörigen Dateien zu löschen, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Anpassen*.
2. Klicken Sie unter *Eigene Designs* mit der rechten Maustaste auf das Design, das Sie löschen wollen, oder halten Sie es gedrückt, und wählen Sie den Befehl *Design löschen*. Windows löscht die Definitionsdatei des Designs und alle zugehörigen Mediendateien.

TIPP Gewöhnlich liegen Definitionsdateien für Designs, die Windows installiert, im Ordner `%WinDir%\Resources\Themes`, während vom Benutzer erstellte Designs in den Profildaten des Benutzers gespeichert werden. Wenn Sie herausfinden möchten, wie viel Platz die Designs belegen, überprüfen Sie diese Ordner und ihre Unterordner. Sie sollten in diesen Ordnern aber keine Dateien direkt löschen, sondern auf die gerade beschriebenen Methoden zurückgreifen.

Optimieren der Desktopumgebung

Wenn Sie Anwendungen oder Ordner öffnen, erscheinen sie auf dem Desktop. Sie können geöffnete Anwendungen und Ordner auf dem Desktop in bestimmter Weise anordnen, indem Sie einen leeren Bereich der Taskleiste mit der rechten Maustaste anklicken oder gedrückt halten und dann nach Bedarf einen der Befehle *Fenster überlappen*, *Fenster gestapelt anzeigen* oder *Fenster nebeneinander anzeigen* wählen. Wenn Sie auf *Desktop anzeigen* klicken, minimiert Windows alle geöffneten Fenster und der Desktop wird sichtbar. Die Wahl von *Geöffnete Fenster anzeigen* versetzt die minimierten Fenster wieder in ihre vorigen Zustände.

Sie können Dateien, Ordner und Verknüpfungen auf dem Desktop ablegen. Jede Datei und jeder Ordner, den Sie auf dem Desktop speichern, erscheint auf dem Desktop. Jede Datei und jeder Ordner, den Sie von einem Datei-Explorer-Fenster auf den Desktop ziehen, bleibt auf dem Desktop liegen. Um eine Verknüpfung mit einer Datei oder einem Ordner auf dem Desktop abzulegen, klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, zeigen auf *Senden an* und wählen dann *Desktop (Verknüpfung erstellen)*.

Neben diesen Grundtechniken bietet Windows 8 noch viele andere Wege zur Optimierung der Desktopumgebung. Sie können beispielsweise ein Firmenlogo oder ein anderes Symbol in den Standarddesktop aufnehmen. Das ist besonders bei verliehenen Laptops sinnvoll. Sie könnten zum Beispiel ein Logo mit dem Hinweis »Leihgabe der Technikabteilung« erstellen. Außerdem können Sie mit den Windows-Minianwendungen benutzerdefinierte Inhalte direkt auf dem Desktop ablegen.

Einstellen des Desktophintergrunds

Windows 8 bietet mehrere Sätze an Hintergrundbildern und fasst diese Bilder anhand der Ordner zusammen, in denen die Bilddateien gespeichert sind. Hintergrundbilder werden auf der Festplatte des Computers in Unterordnern von `%WinDir%\Web\Wallpaper` gespeichert. Jeder Ordner dient als Name

für eine neue Gruppe. So werden zum Beispiel Bilder aus dem Ordner *Landschaften* in der *Landschaften*-Gruppe der Hintergrundbilder angezeigt.

Hintergrundbilder können in den Formaten *.bmp*, *.gif*, *.jpg*, *.jpeg*, *.dib* und *.png* vorliegen. Wenn Sie ein Bild in einem dieser Formate in einem Unterordner von *%WinDir%\Web\Wallpaper* hinzufügen, wird das Bild als Teil der betreffenden Gruppe verfügbar. Wenn Sie eine neue Gruppe definieren möchten, erstellen Sie einfach einen Ordner innerhalb von *%WinDir%\Web\Wallpaper* und speichern die gewünschten Bilder dort ab.

Zur Auswahl eines Hintergrundbilds für den Desktop gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie dann *Anpassen*. Tippen oder klicken Sie in der Konsole *Anpassung* auf *Desktophintergrund*. Dadurch öffnet sich die Konsole *Desktophintergrund* (Abbildung 3.5).

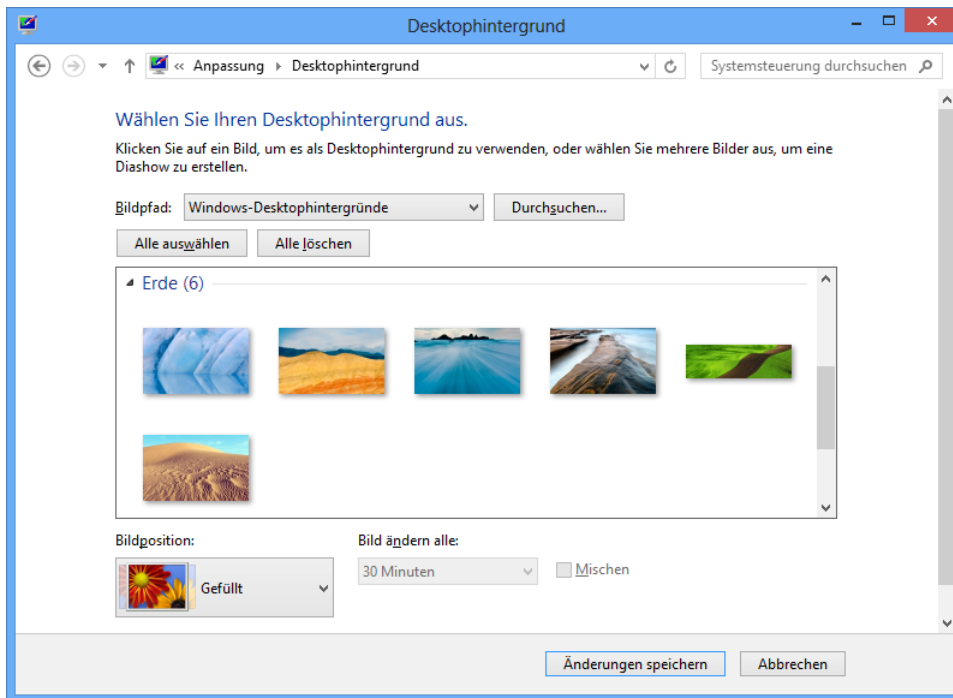


Abbildung 3.5 Wählen Sie das gewünschte Hintergrundbild aus

2. Wenn Sie *Windows-Desktophintergründe* als *Bildpfad* festlegen, fasst Windows 8 Hintergrundbilder zu Gruppen gleichartiger Bilder zusammen, wie zum Beispiel *Erde* oder *Blumen*.
3. Tippen oder klicken Sie auf das Bild, das Sie als Hintergrundbild verwenden möchten. Wenn Sie kein Hintergrundbild finden, das Ihnen gefällt, tippen oder klicken Sie auf die Schaltfläche *Durchsuchen*, um im Dateisystem oder im Netzwerk nach einem passenden Bild zu suchen.
4. Stellen Sie in der Dropdownliste *Bildposition* ein, wie das Hintergrundbild angezeigt werden soll. Es stehen folgende Optionen zur Auswahl:
 - **Zentriert** Zentriert das Bild auf dem Desktophintergrund. Alle Bereiche, die das Bild nicht abdeckt, verwenden die aktuelle Desktopfarbe.

- **Gefüllt** Füllt den Desktophintergrund mit dem Bild aus. Die Seiten des Bilds werden unter Umständen abgeschnitten.
 - **Angepasst** Passt das Bild auf den Desktophintergrund an. Das richtige Seitenverhältnis wird beibehalten. Das ist eine gute Option für Fotos und große Bilder, die Sie ansehen wollen, ohne dass sie gedehnt oder gestaucht werden.
 - **Gestreckt** Streckt das Bild, sodass es den Desktophintergrund ausfüllt. Das richtige Seitenverhältnis wird so weit wie möglich beibehalten, aber die Höhe wird angepasst, um verbleibende Lücken zu füllen.
 - **Nebeneinander** Legt das Bild so oft neben- und untereinander, dass es den ganzen Bildschirm ausfüllt. Das ist eine gute Wahl für kleine Bilder und Symbole.
5. Tippen oder klicken Sie auf *Änderungen speichern*, wenn Sie mit dem Einstellen des Hintergrunds fertig sind.

Verwenden der Standarddesktopsymbole

In der Standardeinstellung wird nur das Papierkorbsymbol zum Desktop hinzugefügt. Doppeltes Antippen oder Anklicken des Symbols *Papierkorb* öffnet ein Fenster, in dem Sie sich Dateien und Ordner ansehen können, die Sie als gelöscht markiert haben. Indem Sie auf *Verwalten* tippen oder klicken und dann *Papierkorb leeren* wählen, können Sie alle Elemente aus dem Papierkorb endgültig löschen. Wenn Sie auf *Verwalten* tippen oder klicken und dann *Eigenschaften des Papierkorbs* wählen, können Sie einstellen, wie der Papierkorb verwendet wird. In jedem Volume eines internen Festplattenlaufwerks gibt es einen Papierkorbordner. Wenn Sie einen Ordner antippen oder anklicken, können Sie die Maximalgröße des Papierkorbs auf diesem Volume einstellen oder festlegen, dass Dateien aus diesem Volume sofort endgültig gelöscht und nicht erst in den Papierkorb verschoben werden.

Darüber hinaus können Sie folgende Symbole zum Desktop hinzufügen:

- **Benutzerdateien** Doppeltes Antippen oder Anklicken des Symbols der Benutzerdateien öffnet Ihren persönlichen Ordner.
- **Computer** Doppeltes Antippen oder Anklicken des Symbols öffnet ein Fenster, in dem Sie auf Festplattenlaufwerke und auf Geräte mit Wechselmedien zugreifen können. Ein Klick mit der rechten Maustaste auf das *Computer*-Symbol oder das Gedrückthalten dieses Symbols öffnet ein Kontextmenü. Die Wahl des Befehls *Verwalten* in diesem Kontextmenü öffnet die Konsole *Computerverwaltung*. Die Wahl des Befehls *Netzlaufwerk verbinden* in diesem Kontextmenü ermöglicht es Ihnen, eine Verbindung mit einem freigegebenen Netzwerkordner herzustellen. Durch die Wahl des Befehls *Netzlaufwerk trennen* lässt sich die Verbindung mit einem freigegebenen Netzlaufwerk wieder trennen.
- **Netzwerk** Doppeltes Antippen oder Anklicken des Symbols *Netzwerk* öffnet ein Fenster, in dem Sie auf die Computer und Geräte in Ihrem Netzwerk zugreifen können. Ein Klick mit der rechten Maustaste auf das Symbol *Netzwerk* oder das Gedrückthalten dieses Symbols öffnet ein Kontextmenü. Die Wahl des Befehls *Netzlaufwerk verbinden* in diesem Kontextmenü ermöglicht Ihnen die Herstellung von Verbindungen mit freigegebenen Netzwerkordnern. Der Befehl *Netzlaufwerk trennen* in diesem Kontextmenü ermöglicht die Trennung der Verbindung zu einem freigegebenen Netzwerkordner.
- **Systemsteuerung** Doppeltes Antippen oder Anklicken des Symbols *Systemsteuerung* öffnet die Systemsteuerung, die Zugang zu Systemkonfigurations- und Systemverwaltungsprogrammen bietet.

Mit folgenden Schritten können Sie einige nützliche Desktopsymbole hinzufügen oder entfernen:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Anpassen*. Dadurch öffnet sich die Konsole *Anpassung*.
2. Tippen oder klicken Sie im linken Bereich auf *Desktopsymbole ändern*. Es öffnet sich das Dialogfeld *Desktopsymboleinstellungen* (Abbildung 3.6).

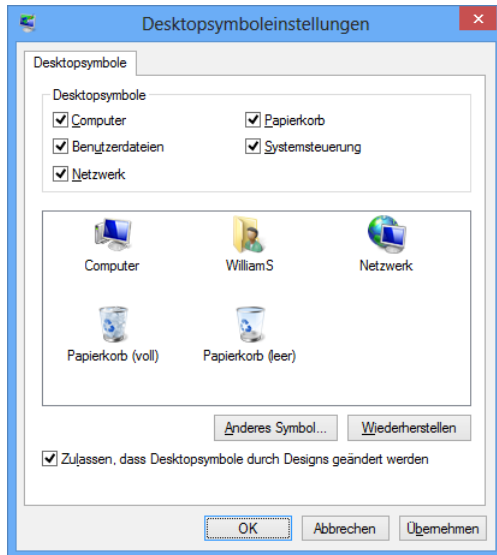


Abbildung 3.6 Im Dialogfeld *Desktopsymboleinstellungen* können Sie die anzuzeigenden Desktopsymbole auswählen und einstellen

3. Das Dialogfeld *Desktopsymboleinstellungen* weist für alle Standardsymbole Kontrollkästchen auf. Deaktivieren Sie das entsprechende Kontrollkästchen, um ein Symbol zu entfernen. Aktivieren Sie ein Kontrollkästchen, um das Symbol hinzuzufügen.
4. Tippen oder klicken Sie auf *OK*.

Sie können alle Desktopsymbole verbergen, indem Sie mit der rechten Maustaste einen freien Bereich des Desktops anklicken oder die Stelle gedrückt halten, auf *Ansicht zeigen* und *Desktopsymbole anzeigen* wählen. Wenn Sie dies wiederholen und ein zweites Mal *Desktopsymbole anzeigen* wählen, erscheinen alle verborgenen Desktopsymbole wieder.

Wenn Sie ein Symbol oder eine Verknüpfung nicht mehr auf dem Desktop sehen wollen, klicken Sie das Element mit der rechten Maustaste an oder halten es gedrückt und wählen dann *Löschen*. Sobald Sie dazu aufgefordert werden, bestätigen Sie den Vorgang durch Tippen oder Klicken auf *Ja*. Wenn Sie ein Symbol, das für eine Datei oder einen Ordner steht, vom Desktop löschen, wird auch die Datei beziehungsweise der Ordner (samt Inhalt) gelöscht.

Bildschirmschoner

Bildschirmschoner sollen automatisch anspringen, wenn der Benutzer für eine gewisse Zeit keine Eingaben mehr gemacht hat. Ursprünglich sollten Bildschirmschoner durch einen ständigen Wechsel des Bildes verhindern, dass sich ein Bild, das lange Zeit ohne Veränderung angezeigt wird, in die Leuchtstoffschichten der damaligen Bildröhren einbrannte. Bei den heutigen Flachbildschirmen ist das zwar kein Problem mehr, aber Bildschirmschoner gibt es immer noch. Wichtigster Vorteil eines Bildschirmschoners ist heute, dass sich ein Computer automatisch mit einem Kennwortschutz versehen lässt, wenn ein Bildschirmschoner aktiv wird.

Konfigurieren eines Bildschirmschoners mit Kennwortschutz

Der Kennwortschutz eines Bildschirmschoners kann nichtautorisierte Benutzer davon abhalten, einen Computer zu benutzen. Dadurch werden die persönlichen Daten des Benutzers und das geistige Eigentum der Organisation besser geschützt. Als Administrator sollten Sie dafür sorgen, dass die Computer, für die Sie zuständig sind, mit aktiviertem kennwortgeschütztem Bildschirmschoner betrieben werden.

Den Kennwortschutz durch einen Bildschirmschoner erreichen Sie folgendermaßen:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Anpassen*.
2. Tippen oder klicken Sie auf *Bildschirmschoner*, um das Dialogfeld *Bildschirmschonereinstellungen* zu öffnen (Abbildung 3.7).

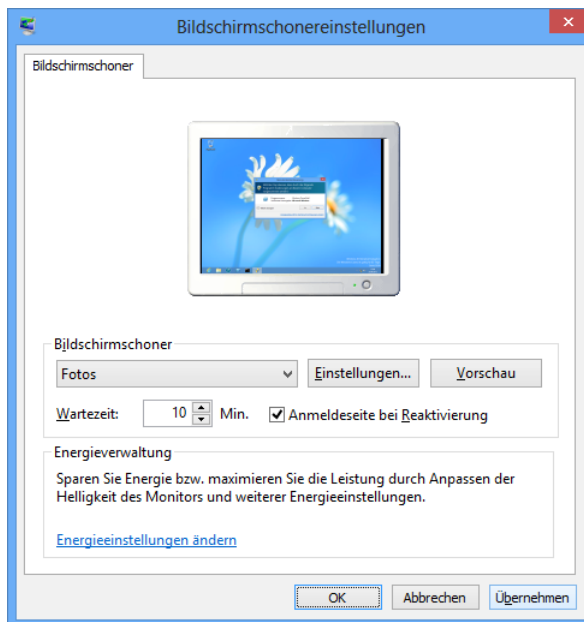


Abbildung 3.7 Stellen Sie einen Bildschirmschoner mit Kennwortschutz ein, um die Daten des Benutzers und der Organisation besser zu schützen

3. Wählen Sie in der Liste *Bildschirmschoner* einen Bildschirmschoner aus. Falls Sie den Bildschirmschoner deaktivieren möchten, wählen Sie (*Kein*) und überspringen die restlichen Schritte.

PRAXISTIPP

Leider können Bildschirmschoner einen beträchtlichen Teil der Ressourcen eines Computers beanspruchen und nicht nur die Auslastung des Speichers und des Prozessors erhöhen, der ohne Bildschirmschoner vermutlich nichts zu tun hätte, sondern auch den Energieverbrauch. Manche Darstellungen sind sehr komplex, und der Computer muss viele Berechnungen durchführen, um das Bild aufzubauen und zu aktualisieren. Hinweise auf eine Verringerung der Ressourcenbelastung durch Bildschirmschoner finden Sie in den Abschnitten »Verringern der Ressourcenauslastung durch Bildschirmschoner« und »Einstellen der Energiesparoptionen für Monitore« weiter unten in diesem Kapitel.

4. Aktivieren Sie das Kontrollkästchen *Anmeldeseite bei Reaktivierung*.
5. Geben Sie im Feld *Wartezeit* die Zeitspanne ein, die nach der letzten Bedienung des Computers durch den Benutzer verstreichen muss, bevor der Bildschirmschoner aktiviert wird. In den meisten Fällen sind Einstellungen zwischen 10 und 15 Minuten sinnvoll.
6. Tippen oder klicken Sie auf *OK*.

HINWEIS

Einer der besten Bildschirmschoner ist *Fotos*. Er zeigt standardmäßig eine Diashow aller Fotos in der Bibliothek *Bilder*, Sie können aber auch einen anderen Ordner auswählen. Mithilfe der Einstellungen können Sie die Geschwindigkeit der Diashow ändern und wählen, ob die Bilder in der Original- oder in zufälliger Reihenfolge angezeigt werden.

Verringern der Ressourcenbelastung durch Bildschirmschoner

Ein Computer, der Windows 8 ausführt und zudem Hintergrundaufgaben oder bestimmte Aufgaben im Netzwerk übernimmt, beispielsweise Druckdienste, sollte nicht zusätzlich mit einem komplexen Bildschirmschoner wie 3D-Text belastet werden. Stattdessen sollte ein einfacher Bildschirmschoner gewählt werden, der zum Beispiel einen leeren Bildschirm zeigt. Außerdem können Sie die Einstellungen eines komplexeren Bildschirmschoners so ändern, dass sein Ressourcenbedarf kleiner wird. Gewöhnlich erreichen Sie dies durch die Verringerung von Auflösung oder Aktualisierungsrate des Bildschirmschoners. Zur Verringerung des Ressourcenbedarfs eines Bildschirmschoners gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Anpassen*.
2. Tippen oder klicken Sie auf den Link *Bildschirmschoner*, um das Dialogfeld *Bildschirmschonereinstellungen* zu öffnen.
3. Wenn Sie einfach nur einen Bildschirmschoner einstellen möchten, der weniger Ressourcen beansprucht, wählen Sie in der Liste *Bildschirmschoner* einen einfacheren Bildschirmschoner aus, beispielsweise *Leer*.
4. Wenn Sie *3D-Text* oder einen anderen komplexen Bildschirmschoner verwenden, aber dessen Ressourcenbedarf einschränken möchten, wählen Sie den gewünschten Bildschirmschoner aus und tippen oder klicken dann auf *Einstellungen*. Verringern Sie mit den Optionen des Dialogfelds die Werte für Auflösung, Größe, Rotationsgeschwindigkeit oder ähnliche Felder, von denen die Berechnung und Aktualisierung der Darstellung beeinflusst wird.
5. Schließen Sie die geöffneten Dialogfelder, indem Sie jeweils *OK* antippen oder anklicken.

Einstellen der Energiesparoptionen für Monitore

Die meisten neueren Monitore verfügen über Energiesparoptionen, die sie dazu veranlassen, nach einem gewissen Zeitraum, in dem kein Benutzer am Computer arbeitet, abzuschalten. Die Aktivierung dieser Funktion kann sich durchaus auf die Stromrechnung einer Organisation auswirken, weil eingeschaltete Monitore einiges an Strom verbrauchen. Auf manchen Systemen wird diese Funktion bei der Installation des Betriebssystems automatisch aktiviert. Das hängt allerdings davon ab, ob das Betriebssystem den Monitor erkennen und die erforderlichen Treiber installieren kann.

Auf einem Laptop, der mit Akkus betrieben wird, ist ein möglichst geringer Energieverbrauch noch wichtiger. Wenn Sie den Monitor so einstellen, dass er ausgeschaltet wird, wenn der Computer nicht benutzt wird, können Sie die Betriebsdauer bei Akkubetrieb verlängern.

Zur Einstellung der Energieoptionen eines Monitors gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Anpassen*.
2. Tippen oder klicken Sie auf *Bildschirmschoner*, um das Dialogfeld *Bildschirmschonereinstellungen* zu öffnen.
3. Tippen oder klicken Sie auf *Energieeinstellungen ändern*. Dadurch öffnet sich die Konsole *Energieoptionen* der Systemsteuerung.
4. Tippen oder klicken Sie im linken Fensterabschnitt auf *Zeitpunkt für das Ausschalten des Bildschirms auswählen*.
5. Legen Sie mit der Auswahlliste eine Zeitspanne fest, nach welcher der Monitor abgeschaltet werden soll, um Strom zu sparen. Mobile Computer haben vielleicht separate Optionen für Akku- und Netzbetrieb.
6. Tippen oder klicken Sie auf *Änderungen speichern*.

HINWEIS Falls der Computer mit einem Monitor verbunden ist, der das Energiesparen nicht unterstützt, sind einige Energiesparoptionen vielleicht nicht zugänglich. Falls Sie den Computer nicht vor Ort konfigurieren und einen anderen Monitor als der Benutzer verwenden, sollten Sie sich vielleicht ein ähnliches Monitormodell beschaffen, wie es der Benutzer verwendet, und den Vorgang wiederholen.

PRAXISTIPP Meistens ist es sinnvoll, den Monitor nach einer Leerlaufphase von 15 bis 20 Minuten abzuschalten. Mein Bürocomputer schaltet nach 7 Minuten Leerlauf den Bildschirmschoner ein und nach 15 Minuten den Monitor aus. Mein Laptop schaltet nach 5 Minuten Leerlauf den Bildschirmschoner ein und nach 10 Minuten den Monitor aus.

Ändern des Erscheinungsbilds und der Grafikeinstellungen

Die Einstellungen für das allgemeine Erscheinungsbild und den Bildschirm wirken sich sehr stark auf das Aussehen und Verhalten des Windows 8-Desktops und seiner grafischen Elemente aus. Die Einstellung des Erscheinungsbilds betrifft Fenster, Bedienelemente, Farben und Schriften. Von den Grafikeinstellungen hängen Bildschirmauflösung, Farbqualität, Bildwiederholrate, Hardwarebeschleunigung und Farbverwaltung ab.

Konfigurieren von Fensterfarbe und -darstellung

Windows Aero ist eine verbesserte Benutzerschnittstelle, die Features wie einen transparenten Taskleistenthintergrund, Livevorschau, geschmeidiges Ziehen von Fenstern, animiertes Schließen und Öffnen von Fenstern und viel mehr bietet. Im Rahmen der Installation führt Windows 8 einen Leistungstest aus und prüft, ob der Computer die grundlegenden Anforderungen für Windows Aero erfüllt. Dazu gehören:

- Unterstützung für das Windows Display Driver Model (WDDM). WDDM 1.0 wurde in Windows Vista eingeführt. In Windows 7 und höher bieten Anzeigetreiber, die WDDM 1.1 unterstützen, verbesserte Leistung. Gleichzeitig verringert sich der Arbeitsspeicher pro Fenster um bis zu 50 Prozent.
- Unterstützung für DirectX bei Grafikprozessoren (Graphics Processing Unit, GPU) mit mindestens 128 MByte Grafikspeicher. WDDM 1.1 unterstützt DirectX 11, das gegenüber seinen Vorgängern weitere Verbesserungen und Leistungsoptimierungen bietet.

PRAXISTIPP

Mit *Leistungsinformationen und -tools* können Sie schnell feststellen, wie viel Grafikspeicher verfügbar ist und ob die Grafikkarte eines Computers WDDM unterstützt. Wählen Sie auf der Startseite der Systemsteuerung in der Dropdownliste *Anzeige* entweder *Kleine Symbole* oder *Große Symbole*, um alle Systemsteuerungselemente anzuzeigen, tippen oder klicken Sie auf *Leistungsinformationen und -tools* und dann auf *Detaillierte Leistungs- und Systeminformation anzeigen und drucken*. In der Liste der Komponenten sind unter *Grafik* der Grafikkartentyp und die WDDM-Unterstützung aufgelistet. In der erweiterten Liste unter *Grafik* finden Sie zusätzliche Details, darunter die Größe des dedizierten Grafikspeichers und die unterstützte DirectX-Version.

Auf geeigneten Systemen verwendet Windows 8 standardmäßig das Aero-Design, um erweiterte Anzeigefunktionen zu bieten, beispielsweise die Andockfunktion, mit der sich Fenster nebeneinander anordnen lassen, und das »Schütteln«, wodurch sich alle offenen Fenster mit Ausnahme des aktiven Fensters verbergen lassen. Um ein aktives Fenster mit der Tastatur an eine Seite des Desktops anzudocken, drücken Sie entweder die **WINDOWS-Taste+NACH-LINKS** oder **WINDOWS-Taste+NACH-RECHTS**. Beim »Schütteln« klicken Sie auf die Titelleiste eines Fensters und bewegen es bei gedrückter Maustaste schnell hin und her. Um die minimierten Fenster wieder anzuzeigen, schütteln Sie das offene Fenster erneut.

So stellen Sie die Farboptionen für den Monitor ein:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Anpassen*.
2. Tippen oder klicken Sie auf *Farbe*, um die Seite *Farbe und Darstellung* zu öffnen (Abbildung 3.8).
3. Durch das Antippen oder Anklicken einer der verfügbaren Farben können Sie die Grundfarbe der Fenster ändern. Wenn Sie selbst eine Farbe definieren möchten, tippen oder klicken Sie auf *Farbmixer einblenden* und versuchen dann, mit den Schiebereglern *Farbton*, *Sättigung* und *Helligkeit* eine passende Farbe zu finden.

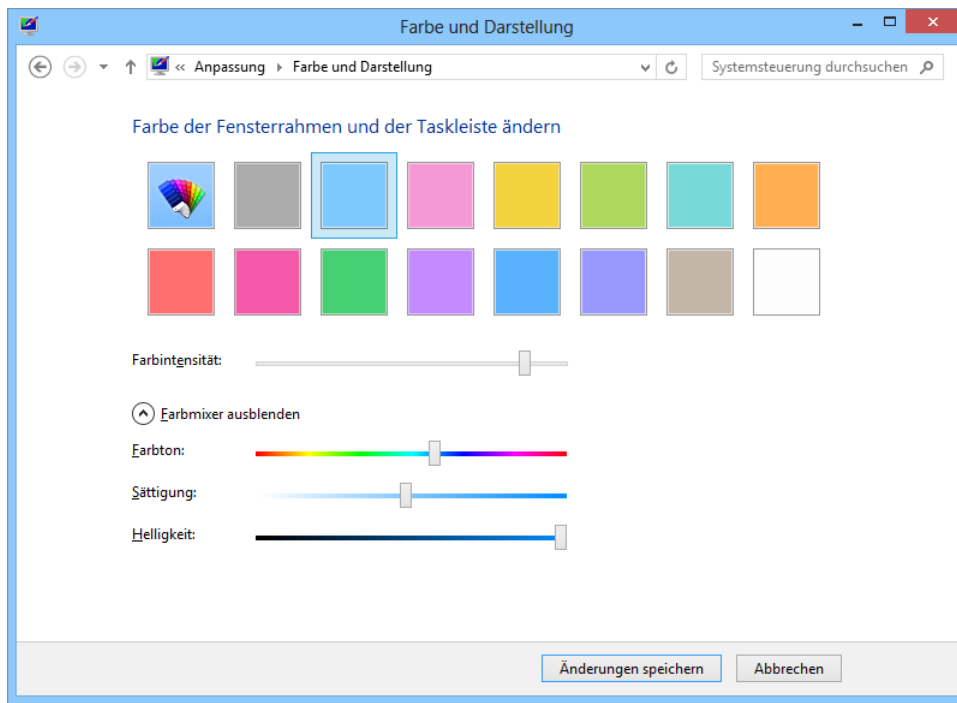


Abbildung 3.8 Konfigurieren der Darstellung mit den Optionen der Seite *Farbe und Darstellung*

4. Stellen Sie mit dem Schieberegler *Farbintensität* die Farbintensität ein, von der auch die Transparenz abhängt. Durch eine Erhöhung der Intensität werden die Farben leuchtender und deckender. Durch eine Verringerung der Intensität werden sie schwächer und durchscheinender.
5. Tippen oder klicken Sie auf *Änderungen speichern*.

Zur besseren Unterstützung von Benutzern mit Sehschwächen bietet Windows 8 einige Designs mit hohem Kontrast, nämlich *Kontrast Nr. 1*, *Kontrast Nr. 2*, *Kontrast Schwarz* und *Kontrast Weiß*. Wenn Sie eines dieser Designs verwenden, ändern sich die Optionen auf der Seite *Farbe und Darstellung*. Außerdem können Sie die Standardfarbeinstellungen für einzelne Grafikelemente ändern, beispielsweise die Fensterhintergrundfarbe, die Textfarbe und die Farbe des aktiven Fensters. Dazu gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Anpassen*.
2. Tippen oder klicken Sie auf *Farbe* und legen Sie dann die Farben für die Schnittstellenelemente fest. Für die Darstellung des Titels des aktiven Fensters können Sie zum Beispiel die Vordergrund- und Hintergrundfarbe festlegen.
3. Tippen oder klicken Sie auf *OK* und dann auf *Änderungen speichern*.

Optimieren der Lesbarkeit

Unabhängig davon, ob Benutzer 27-Zoll-Breitbildmonitore oder 19-Zoll-Monitore haben, gibt es gelegentlich einige, denen es schwerfällt, Text auf dem Bildschirm zu lesen. Die Lesbarkeit von Text auf dem Bildschirm verschlechtert sich, wenn Sie die Bildschirmauflösung erhöhen, weil der Text auf dem Bildschirm dadurch kleiner wird. Um diese Auswirkung zu verstehen, müssen Sie wissen, wie die Auflösung funktioniert und was der Begriff DPI bedeutet.

Wenn Sie Dokumente auf einem Drucker ausgeben, legt die Zahl der Punkte pro Zoll (Dots Per Inch, DPI) die Druckqualität fest. Im Allgemeinen gilt: Je höher die DPI, desto besser die Qualität des ausgedruckten Dokuments, weil Bilder und Text schärfer aussehen, wenn mehr Punkte pro Zoll verwendet werden. So sieht ein hochauflösendes Bild, das mit 1200×600 DPI in seiner normalen Größe ausgedruckt wird, gewöhnlich viel besser aus als dasselbe Bild bei 300×300 DPI. Wenn Sie allerdings ein Bild vergrößern und zum Beispiel ein 2×3 Zoll großes Bild auf 6×9 Zoll ausdrucken, lässt das Ergebnis oft zu wünschen übrig, weil das skalierte Bild pixelig aussieht.

Bei Windows-Computern ist 96 DPI der Standard für die meisten Monitore. Windows 8 zeigt alle Benutzeroberflächenelemente (User Interface, UI), auch den Text, standardmäßig mit 96 DPI an. Wenn Sie die Anzeigeauflösung ändern, verändern Sie auch die Skalierung, mit der UI-Elemente angezeigt werden. Wenn ein Monitor beispielsweise eine optimale Auflösung von 1920×1200 hat und Sie die Anzeigeauflösung 800×600 benutzen, sehen die UI-Elemente groß, aber grob aus, weil Sie die Anzeige von 800×600 Bildpunkten auf eine Fläche strecken, die für 1920×1200 Bildpunkte optimiert ist.

Im Allgemeinen können Sie die optimale Auflösung ermitteln, indem Sie die Breite und die Höhe des Monitors (in der Einheit Zoll) jeweils mit 96 multiplizieren. Nehmen wir als Beispiel einen 24-Zoll-Breitformatmonitor, dessen Bildschirm 20 Zoll breit und 12,5 Zoll hoch ist. In diesem Fall beträgt die optimale Anzeigeauflösung 1920×1200 . Bei dieser Größe sehen Text und UI-Elemente auf dem Bildschirm aber unter Umständen sehr klein aus, sodass Sie Anpassungen vornehmen müssen, um die Lesbarkeit zu verbessern. Eine Möglichkeit ist, dies innerhalb einer Anwendung zu tun. So können die Benutzer in Microsoft Word den Text mit dem Kombinationsfeld *Zoom* auf eine gut lesbare Größe skalieren.

Windows ermöglicht es, die Textgröße für bestimmte Elemente der Benutzeroberfläche zu ändern, nämlich für die Titelleisten von Dialogfeldern, Menüs, Meldungsfelder, Palettentitel, Symbole und QuickInfos. Durch eine Vergrößerung oder Verkleinerung der Textgröße in einem bestimmten Teil der Benutzeroberfläche lässt sich die Lesbarkeit verbessern. Für jedes Konto eines Computers lässt sich die Textgröße einstellen. So legen Sie die Textgröße für Elemente der Benutzeroberfläche fest:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Darstellung und Anpassung*. Tippen oder klicken Sie unter der Überschrift *Anzeige* auf *Text und weitere Elemente vergrößern oder verkleinern*.
2. Klicken Sie auf die Auswahlliste unter *Nur die Textgröße ändern* und wählen Sie das gewünschte Element aus, beispielsweise *Menüs*.
3. Wählen Sie in der Schriftgrößenliste die gewünschte Schriftgröße für das ausgewählte Element aus. Bei Bedarf aktivieren Sie das Kontrollkästchen *Fett*, damit der Text entsprechend angezeigt wird.
4. Wiederholen Sie die Schritte 2 und 3, um die Textgröße für weitere Elemente der Benutzeroberfläche festzulegen. Wenn Sie fertig sind, tippen oder klicken Sie auf *Übernehmen*.
5. Der Benutzer muss sich abmelden und wieder anmelden, damit die Änderungen wirksam werden.

Windows bietet Ihnen auch die Möglichkeit, mithilfe der Skalierung die Größe von Text und anderen Elementen auf dem Bildschirm anzupassen. Wenn Sie die Skalierung auf diese Weise einsetzen, vergrößert Windows Text und UI-Elemente um den Faktor, den Sie einstellen. Jedes Konto auf einem Computer

hat eigene Einstellungen für die Skalierung. Sie stellen folgendermaßen ein, welche Skalierung für Text und UI-Elemente benutzt wird:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Darstellung und Anpassung* und dann unter *Anzeige* auf *Text und weitere Elemente vergrößern oder verkleinern*.
2. Mit den Standardskalierungsoptionen können Sie die Werte 100 Prozent (Standardwert), 125 Prozent oder 150 Prozent auswählen. Wählen Sie die gewünschte Skalierungsoption aus und tippen oder klicken Sie auf *Übernehmen*.
3. Sie können auch eine benutzerdefinierte Einstellung zwischen 100 und 500 Prozent verwenden. Tippen oder klicken Sie dazu auf *Benutzerdefinierte Optionen für die Größenanpassung* und stellen Sie dann im Kombinationsfeld des Dialogfelds *Benutzerdefinierte Optionen für die Größenanpassung* den gewünschten Skalierungswert ein.
4. Der Benutzer muss sich ab- und dann wieder anmelden, damit die Änderungen wirksam werden.

WICHTIG Wenn Sie eine höhere Einstellung als 200 Prozent verwenden, werden UI-Elemente und Text unter Umständen so groß, dass Sie nicht mehr mit dem Computer arbeiten können. Möglicherweise ist es nicht einmal mehr möglich, erneut die Systemsteuerung zu öffnen und darin die ursprüngliche Skalierung wiederherzustellen. Wenn Sie ein Skalierungsproblem haben, können Sie in einer Eingabeaufforderung oder im *Apps*-Suchfeld **dpiscaling** eingeben. Daraufhin öffnet sich direkt die Seite *Anzeige*, wo Sie die Skalierung zurücksetzen können.

PRAXISTIPP Wenn Sie die Skalierung aktiviert haben und der Text in einer Anwendung verschwommen oder unlesbar ist, ist es sinnvoll, die Anzeigeskalierung für diese Anwendung gezielt zu deaktivieren. Tippen oder klicken Sie dazu mit der rechten Maustaste auf die Verknüpfung der Anwendung oder halten Sie sie gedrückt und wählen Sie den Befehl *Eigenschaften*. Aktivieren Sie auf der Registerkarte *Kompatibilität* das Kontrollkästchen *Skalierung bei hohem DPI-Wert deaktivieren* und tippen oder klicken Sie auf *OK*.

Konfigurieren von Grafikeinstellungen

Die Grafikeinstellungen betreffen Bildschirmauflösung, Farbqualität, Bildwiederholrate, Hardwarebeschleunigung und Farbverwaltung. Dieser Abschnitt soll Ihnen bei der Optimierung verschiedener Grafikeinstellungen helfen. Überprüfen Sie zuerst, ob Windows 8 die Grafikkarte und den Monitor korrekt erkannt hat.

Überprüfen des Grafikadapters und des Monitors

Jeder Computer hat einen Monitor- und einen Grafikkartentreiber. Der Monitortreiber teilt Windows mit, welche Fähigkeiten der Monitor besitzt, der Grafikkartentreiber gibt Windows Auskunft über die Fähigkeiten der Grafikkarte.

Eine optimale Darstellung setzt voraus, dass der Computer mit den richtigen Daten für die Grafikkarte und den Monitor arbeitet. Je nach den Grafikkarten und Monitormodellen, die Windows 8 erkannt zu haben glaubt, werden unterschiedliche Gerätetreiber installiert. Diese Treiber sind bei der Bestimmung der verfügbaren und der für das System passenden Bildschirmauflösungen, Farbtiefen und Bildwiederholraten von entscheidender Bedeutung. Werden die Grafikkarte und der Monitor nicht korrekt erkannt und eingestellt, kann Windows 8 ihre Leistung nicht richtig nutzen.

Falsche aktuelle Einstellungen der Grafikkarte oder des Monitors können viele Ursachen haben. Manchmal erkennt der Plug & Play-Mechanismus das Gerät nicht und es wird ein allgemeiner Treiber verwendet. Manchmal erkennt Windows 8 das Gerät falsch und geht beispielsweise von einem anderen Modell

aus. In solchen Fällen wird der verwendete Gerätetreiber vermutlich funktionieren, aber nicht alle Funktionen bieten, die eigentlich verfügbar sein sollten.

Gehen Sie zur Überprüfung der aktuellen Grafikkarte und des Monitors folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Bildschirmauflösung*.
2. Auf der Seite *Bildschirmauflösung* (Abbildung 3.9) werden alle momentan erkannten Monitore in der Liste *Anzeige* aufgeführt. Auflösung und Ausrichtung werden in den gleichnamigen Listen aufgeführt. Falls nicht der richtige Monitor angezeigt wird oder Sie die Monitoreinstellungen genauer untersuchen wollen, sollten Sie im Abschnitt »Ändern des Monitors« weiter unten in diesem Kapitel weiterlesen.

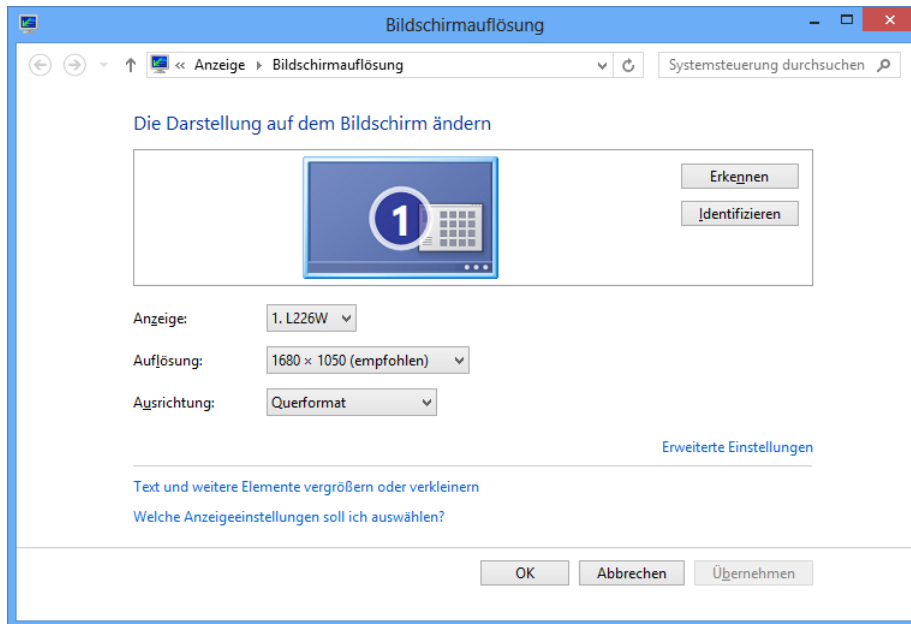


Abbildung 3.9 Überprüfen der Konfiguration von Monitor und Grafikkarte

3. Wählen Sie in der Liste *Anzeige* einen Monitor aus und tippen oder klicken Sie auf *Erweiterte Einstellungen*. Die Grafikkarte für den Monitor wird aufgelistet. Wenn nicht die richtige Grafikkarte angezeigt wird oder wenn Sie die Treibereinstellungen genauer überprüfen möchten, fahren Sie mit dem Abschnitt »Wechseln des Grafiktreibers« weiter unten in diesem Kapitel fort.
4. Tippen oder klicken Sie zweimal auf *OK*.

Wechseln des Grafiktreibers

Wenn Sie der obigen Anleitung gefolgt sind und nicht die Grafikkarte angezeigt wird, die im Computer installiert ist, können Sie versuchen, einen anderen Treiber zu installieren. Ist auf dem Computer beispielsweise ein allgemeiner S3-Grafikkartentreiber installiert und Sie sind sich sicher, dass eine NVIDIA GeForce FX 5200 installiert ist, sollten Sie vermutlich den Grafikkartentreiber wechseln.

Um herauszufinden, ob die Einstellungen für die Grafikkarte richtig sind, müssen Sie wissen, welche Hardware im System verfügbar ist. Aus der Systemdokumentation sollte hervorgehen, welche Grafikkarte installiert ist. Andere Administratoren sind normalerweise ebenfalls gute Informationsquellen. Gewöhn-

lich kann Ihnen jemand aus der Technikabteilung sofort sagen, welche Grafikkarte in einem bestimmten Computertyp installiert ist. Falls Sie aber nicht auf einfache Weise herausfinden, um welche Grafikkarte es sich handelt, bieten sich mehrere Alternativen an. Falls die aktuellen Einstellungen funktionieren, brauchen Sie sie eigentlich nicht zu ändern. Sie können auch mit einer der folgenden Methoden herauszufinden versuchen, mit welcher Grafikkarte Sie es zu tun haben:

- Fahren Sie den Computer herunter und schalten Sie ihn anschließend wieder ein. (Verwenden Sie dazu aber nicht den Befehl *Neu starten*, denn manche Computer führen in diesem Fall keine vollständige Initialisierung durch.) Beobachten Sie den Bildschirm genau, wenn der Computer eingeschaltet wird. Normalerweise müsste kurz der Name der Grafikkarte angezeigt werden, bevor Windows 8 geladen wird.
- Fahren Sie den Computer herunter, trennen Sie ihn vom Stromnetz und öffnen Sie das Gehäuse. Suchen Sie nach der Bezeichnung der Grafikkarte. Wenn der Monitor noch angeschlossen ist, ist die Grafikkarte leicht zu erkennen. Es ist die Steckkarte, mit der das Monitorkabel verbunden ist.
- Ist der Grafikchip bereits auf dem Mainboard installiert (es gibt also keinen separaten Grafikadapter), sehen Sie nach, ob Sie auf dem Mainboard einen Chip finden, der mit Grafikchipdaten bedruckt ist. Oder schreiben Sie sich die Modellnummer des Mainboards auf und sehen Sie auf der Website des Herstellers nach, ob dort die gesuchten Informationen zu bekommen sind.

Wenn Sie die genaue Bezeichnung der Grafikkarte kennen, sehen Sie auf der Website des Herstellers nach, ob Sie dort einen passenden Treiber finden. Manche Grafikkarten werden mit Installationsdatenträger verkauft, auf dem Sie vielleicht ein Installationsprogramm finden. Starten Sie dieses Programm und installieren Sie die Grafikkartentreiber. Enthält der Datenträger zwar die Treiber, aber kein Installationsprogramm, müssen Sie die Treiber manuell installieren.

Sobald Sie bereit sind, den Grafiktreiber zu installieren, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Bildschirmauflösung*.
2. Wenn Ihr System mehrere Monitore oder Grafikkarten hat, müssen Sie in der Liste *Anzeige* den Monitor auswählen, den Sie bearbeiten wollen.

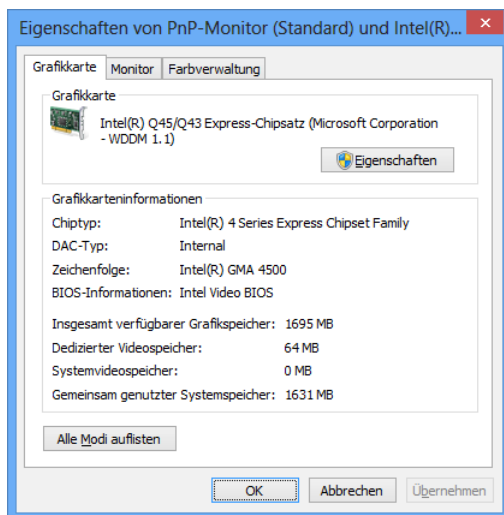


Abbildung 3.10 Aktuelle Informationen zur Grafikkarte

3. Tippen oder klicken Sie auf *Erweiterte Einstellungen*. Lesen Sie auf der Registerkarte *Grafikkarte* (Abbildung 3.10) die aktuellen Informationen zum Grafikkartentyp und die Informationen zur Grafikkarte. Tippen oder klicken Sie auf *Eigenschaften*.
4. Tippen oder klicken Sie auf der Registerkarte *Treiber* auf *Treiber aktualisieren*. Dadurch wird der Assistent *Treibersoftware aktualisieren* gestartet.
5. Wählen Sie aus, ob automatisch nach dem Treiber gesucht werden soll oder ob Sie ihn selbst auf dem Computer suchen wollen.
6. Wenn Sie den Treiber automatisch suchen lassen, sucht Windows 8 nach einer neueren Version des Treibers und installiert sie, sofern er sich finden lässt. Ist keine neuere Version des Treibers verfügbar, behält Windows 8 den aktuellen bei. Tippen oder klicken Sie in beiden Fällen auf *Schließen*, um den Vorgang abzuschließen, und überspringen Sie die restlichen Schritte.
7. Wenn Sie den Treiber selbst suchen, haben Sie folgende Alternativen:
 - **Den Treiber suchen** Wenn Sie nach dem Treiber suchen möchten, tippen oder klicken Sie auf *Durchsuchen*. Suchen Sie im Dialogfeld *Ordner suchen* den Startordner für die Suche aus und klicken Sie dann auf *OK*. Da alle Unterordner des ausgewählten Ordners automatisch in die Suche einbezogen werden, können Sie auch ein Stammverzeichnis auswählen, beispielsweise C:, wenn ein ganzes Laufwerk durchsucht werden soll. Wenn die Unterordner nicht durchsucht werden sollen, löschen Sie das Kontrollkästchen *Unterordner einbeziehen*.
 - **Den Treiber auswählen** Wenn Sie den zu installierenden Treiber selbst auswählen möchten, tippen oder klicken Sie auf *Aus einer Liste von Gerätetreibern auf dem Computer auswählen*. Der Assistent zeigt dann eine Liste mit kompatibler Hardware. Tippen oder klicken Sie auf das Gerät, das Ihrer Grafikkarte entspricht. Wenn Sie eine größere Auswahl wünschen, deaktivieren Sie das Kontrollkästchen *Kompatible Hardware anzeigen*; es erscheint eine Liste aller Hersteller, die Grafikkarten produzieren. Suchen Sie aus der Liste den Hersteller Ihrer Grafikkarte oder des Grafikchips heraus und wählen Sie dann auf der rechten Seite das passende Modell.
8. Nach der Wahl des Gerätetreibers setzen Sie die Installation fort, indem Sie auf *Weiter* tippen oder klicken. Tippen oder klicken Sie auf *Schließen*, sobald die Installation des Treibers abgeschlossen ist. Falls der Assistent keinen passenden Treiber finden kann, müssen Sie einen besorgen und diese Prozedur wiederholen. Vergessen Sie nicht, dass Sie in manchen Fällen das System neu starten müssen, damit der neu installierte oder aktualisierte Treiber verwendet wird.

Ändern des Monitors

Die Qualität des Bilds auf dem Monitor ist von der Kombination aus Grafikkarte und Monitor abhängig. Die meisten Computer verfügen über mindestens einen Monitoranschluss. Dabei werden unter anderem folgende Anschlusstypen unterstützt:

- **HDMI (High-Definition Multimedia Interface)** ist der aktuelle Digitalstandard für den Anschluss von Videogeräten. HDMI kann für Computermonitore eingesetzt werden, eignet sich aber besser für andere High-End-Videogeräte. Es ist zwar möglich, HDMI an DVI-Verbindungen (Digital Video Interface) anzuschließen, aber die meisten Computer, die einen HDMI-Anschluss haben, verfügen auch über mindestens eine DVI-Buchse.
- **DVI (Digital Video Interface)** ist der Digitalstandard für computergenerierte Texte und Grafik. Es gibt mehrere Formate für DVI. DVI-I und DVI-A können an VGA angeschlossen werden, bei DVI-D ist das nicht möglich. Dual-Link-DVI unterstützt Monitore mit hoher Auflösung; es wird benötigt, um das Bild auf einigen sehr großen Monitoren in optimaler Qualität anzuzeigen. Weil DVI-Kabel je

nach Bauart mehrere dieser Typen gleichzeitig unterstützen können oder auch nicht, sollten Sie Ihre Kabel sorgfältig überprüfen und sicherstellen, dass Sie die richtigen verwenden.

- 15-poliges VGA (Video Graphics Array) ist der analoge Standard zum Anschließen von Monitoren an Computer. Es gibt auch 9-polige VGA-Kabel, die zum 15-poligen Anschluss kompatibel sind. Sehr viele Monitore haben nach wie vor eine solche Buchse, aber Sie sollten aufgrund der besseren Qualität neuere Verbindungen wie DVI und HDMI verwenden, wenn sie zur Verfügung stehen.

HINWEIS Viele Computermonitore werden mit einem angeschlossenen VGA-Kabel geliefert. Wenn dies nicht der optimale Verbindungstyp ist und das Kabel abgezogen werden kann, sollten Sie es entfernen.

TIPP Viele Computer haben Anschlüsse für DisplayPort-Adapter. Ein DisplayPort-Adapter unterstützt die automatische Anpassung an VGA, DVI oder HDMI, je nachdem, an was für einen Monitor der Ausgang angeschlossen wird und welcher Adaptertyp zwischen dem Monitoreingang und dem Ausgang am Computer eingesetzt wird.

Ist an der Grafikkarte ein Plug & Play-Monitor angeschlossen, hat Windows 8 ihn wahrscheinlich erkannt und korrekt installiert. Vielleicht hat Windows 8 aber nur einen ähnlichen Treiber installiert und nicht genau den Treiber, der eigentlich für das Monitormodell vorgesehen ist. Um eine optimale Bildqualität sicherzustellen, sollte Windows 8 den Treiber verwenden, der für den betreffenden Monitor vorgesehen ist. Andernfalls passen Anzeigemodus, Farbtiefe, Bildwiederholrate und Farbabstimmung vielleicht nicht zum verwendeten Monitor.

Zur Änderung der Monitorinstallation gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Bildschirmauflösung*.
2. Wenn Ihr System mehrere Monitore oder Grafikkarten hat, müssen Sie in der Liste *Anzeige* den Monitor auswählen, den Sie bearbeiten wollen.
3. Tippen oder klicken Sie auf *Erweiterte Einstellungen* und dann auf der Registerkarte *Monitor* auf *Eigenschaften*.
4. Tippen oder klicken Sie auf der Registerkarte *Treiber* auf *Treiber aktualisieren*. Dadurch wird der Assistent *Treibersoftware aktualisieren* gestartet.
5. Aktualisieren Sie den Treiber, wie in den Schritten 5 bis 8 der vorherigen Anleitung beschrieben.

Konfigurieren mehrerer Monitore

Die meisten modernen Computer sind mit einer Grafikkarte ausgestattet, die zwei Monitore unterstützt. Das erkennen Sie daran, dass die Grafikkarte mehrere Monitoranschlüsse hat. An solche Computer können Sie mehrere Monitore anschließen und den Desktop des Benutzers über alle Monitore verteilen, damit der Benutzer mehr Informationen gleichzeitig im Blick hat. Wenn Sie mehrere Monitore an einen Computer anschließen, zeigt die Seite *Bildschirmauflösung* für jeden Monitor ein eigenes Symbol an. Der erste Monitor trägt die Nummer 1, der zweite die Nummer 2 und so weiter. Wenn Sie das Symbol eines Monitors antippen oder anklicken, können Sie diesen Monitor genauso bearbeiten, als würden Sie ihn aus der Liste *Anzeige* auswählen.

Wird zu einem Monitor, den Sie angeschlossen haben, kein Symbol angezeigt, sollten Sie das Monitorkabel überprüfen und den Monitor einschalten. Wenn Sie nun auf die Schaltfläche *Erkennen* tippen oder klicken, müsste Windows den Monitor automatisch erkennen.

Haben Sie mehrere Monitore angeschlossen, ist nicht immer ohne Weiteres zu erkennen, welcher Monitor welchem Symbol entspricht. Tippen oder klicken Sie in diesem Fall auf die Schaltfläche *Identifizieren*, um auf jedem Monitor die entsprechende Nummer anzuzeigen. Die Nummer wird als große weiße Zahl angezeigt. Wenn sich herausstellt, dass die Monitore anders angeordnet sind, als die entsprechenden Symbole auf der Seite *Bildschirmauflösung* konfiguriert sind, können Sie die Monitorsymbole verschieben, damit ihre Position der tatsächlichen Anordnung der Bildschirme entspricht.

Nachdem Sie die Monitore konfiguriert haben, können Sie die Anzeige über alle Monitore ausdehnen. Tippen oder klicken Sie dazu auf das Symbol des zweiten Monitors (oder wählen Sie den zweiten Monitor in der Liste *Anzeige* aus) und wählen Sie in der Liste *Mehrere Anzeigen* den Eintrag *Diese Anzeigen erweitern* aus. Im Allgemeinen sollten Sie den Monitor mit der Nummer 1 mit *Dies ist zurzeit die Hauptanzeige* markieren.

Nach der Konfiguration der Monitore lässt sich die Konfiguration mit der Tastenkombination **WINDOWS-Taste+P** leicht ändern. Nach der Eingabe dieser Tastenkombination können Sie eine der folgenden Optionen auswählen:

- Wählen Sie *Nur PC-Bildschirm*, wenn Sie nur den Hauptmonitor des Computers oder den integrierten Bildschirm eines Laptops verwenden möchten.
- Wählen Sie *Duplizieren*, wenn der zweite Monitor genau das anzeigen soll, was auch auf dem Hauptmonitor oder auf dem integrierten Monitor eines Laptops zu sehen ist.
- Wählen Sie *Erweitern*, um die Anzeige auf den zweiten Monitor zu erweitern.
- Wählen Sie *Nur zweiter Bildschirm*, wenn die Daten nur auf dem externen Monitor oder Projektor angezeigt werden sollen.

Auf einem Touchscreen erreichen Sie diese Optionen, indem Sie eine Streifbewegung vom rechten Bildschirmrand durchführen, auf *Geräte* tippen und dann auf *Zweiter Bildschirm* tippen.

Auflösung, Farbqualität und Bildwiederholrate sind die wichtigsten Faktoren für die Bilddarstellung. Die Auflösung beschreibt die Zahl der Bildpunkte (oder Pixel, für Picture Elements), aus denen sich ein Bild zusammensetzt. Die Farbqualität hängt von der Zahl der Farben ab, die gleichzeitig angezeigt werden können. Die Bildwiederholrate gibt an, wie oft das Bild in der Sekunde angezeigt wird.

Windows 8 optimiert die Einstellungen für jeden Monitor automatisch und wählt nach der Durchführung der Tests eine passende Bildschirmauflösung, Farbqualität und Bildwiederholrate. Normalerweise eignen sich die Werte sehr gut, die Windows wählt, aber sie sind vielleicht nicht die optimalen Einstellungen für Ihren Computer.

Welche Auflösung die beste ist, hängt von der Größe des Monitors und auch davon ab, was der Benutzer am Computer tun will. Designer und Entwickler, die eine großflächige Anzeige brauchen, ziehen höhere Auflösungen vor, beispielsweise 1920×1200 . Dann können sie mehr von den Objekten sehen, an denen sie arbeiten. Benutzer, die überwiegend E-Mails lesen oder mit Word-Dokumenten arbeiten, ziehen vielleicht eine geringere Auflösung vor, etwa 1280×1024 . Bei dieser Auflösung sind die Bedienelemente leichter zu erkennen und die Augen werden nicht so angestrengt. Auf einem Breitformatmonitor sollten Sie eine Auflösung wählen, die auf Breitformatanzeigen abgestimmt ist.

Die Farbqualität hängt indirekt von der Bildauflösung ab. Die meisten aktuellen Grafikkarten können zwar bei verschiedenen Auflösungen 32-Bit-Farben anzeigen, aber nicht jede Karte ist auch bei der größten Auflösung noch dazu in der Lage. Manche Grafikkarten zeigen weniger Farben an, wenn Sie eine höhere Auflösung einstellen. Meistens ist es besser, eine höhere Farbtiefe zu wählen. Die Speichermenge, die erforderlich ist, um ein Bild im Speicher zu halten, berechnet sich aus der Zahl der Bildpunkte multipliziert mit der Zahl der Bits, die für jeden Bildpunkt erforderlich sind. Die Zahl der Bildpunkte hängt von der Auflösung ab, die Zahl der Bits pro Bildpunkt von der Farbtiefe. Welche Kombinationen von

Bildauflösung und Farbtiefe zulässig sind, hängt von der Menge des verfügbaren Speichers auf der Grafikkarte ab.

Bildauflösung und Farbtiefe können Sie folgendermaßen einstellen:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Bildschirmauflösung*.
2. Wenn Ihr System mehrere Monitore oder Grafikkarten hat, müssen Sie in der Liste *Anzeige* den Monitor auswählen, den Sie bearbeiten wollen.
3. Tippen oder klicken Sie auf die Dropdownliste *Auflösung* und stellen Sie die Bildschirmgröße mit dem Schieberegler ein, zum Beispiel 1024 × 768. Falls diese Option abgeblendet dargestellt wird, können Sie die Auflösung nicht ändern.
4. Tippen oder klicken Sie auf *Erweiterte Einstellungen*, um die Anzeigemodi anzuzeigen, die sich für 32-Bit-Farben eignen. Tippen oder klicken Sie auf der Registerkarte *Grafikkarte* auf *Alle Modi auflisten*. Achten Sie auf die Auflösungen, die sich für 32-Bit-Farben eignen.
5. Tippen oder klicken Sie zweimal auf *OK*.

Auch wenn dem Auge das Flackern nicht direkt auffällt, können niedrige Bildwiederholraten (unter 72 Hz) bei Röhrenmonitoren auf die Dauer sehr anstrengend für die Augen sein.

Zur Überprüfung oder Einstellung der Bildwiederholrate einer Grafikkarte gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Bildschirmauflösung*.
2. Wenn Ihr System mehrere Monitore oder Grafikkarten hat, müssen Sie in der Liste *Anzeige* den Monitor auswählen, den Sie bearbeiten wollen.
3. Tippen oder klicken Sie auf *Erweiterte Einstellungen* und dann auf der Registerkarte *Grafikkarte* auf *Alle Modi auflisten*. Es werden alle Auflösungen und Bildwiederholraten aufgelistet, die für die Grafikkarte zulässig sind.
4. Wählen Sie auf der Registerkarte *Monitor* im Listenfeld *Bildschirmaktualisierungsrate* die gewünschte Bildwiederholrate aus.

ACHTUNG In vielen Fällen ist das Kontrollkästchen *Modi ausblenden, die von diesem Monitor nicht angezeigt werden* gesperrt und kann nicht gewählt werden. Falls Sie dieses Kontrollkästchen löschen können, vergessen Sie bitte nicht, dass kein brauchbares Bild zustande kommt, wenn die gewählte Bildwiederholrate die Fähigkeiten des Monitors oder der Grafikkarte übersteigt. Außerdem können Grafikkarte und Monitor beschädigt werden, wenn sie auf höhere Bildwiederholraten eingestellt werden, als sie bewältigen.

Farbprofile ermöglichen es, die Farben für die Benutzer genauer einzustellen. Vielleicht ist es für Ihre Arbeit erforderlich, dass die auf dem Bildschirm angezeigten Farben genauer mit den Farben im Druck übereinstimmen. Ein entsprechendes Farbprofil kann Sie dabei unterstützen. Wenn Sie das Farbprofil erhalten haben, müssen Sie es auf folgende Weise separat auf jedem Monitor installieren:

1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops oder halten Sie dort eine Stelle gedrückt, und wählen Sie den Befehl *Bildschirmauflösung*. Standardmäßig ist die Anzeige 1 vorgewählt. Tippen oder klicken Sie auf 2, wenn Sie die Einstellungen für den zweiten Monitor ändern möchten.

2. Tippen oder klicken Sie auf *Erweiterte Einstellungen*. Tippen oder klicken Sie auf der Registerkarte *Farbverwaltung* auf *Farbverwaltung*.
3. Wählen Sie im Dialogfeld *Farbverwaltung* die Registerkarte *Alle Profile*, um Informationen über die installierten Farbprofile zu erhalten. Tippen oder klicken Sie auf *Hinzufügen*.
4. Suchen Sie im Dialogfeld *Profil installieren* das Profil heraus, das Sie verwenden möchten, und tippen oder klicken Sie auf *Hinzufügen*.
5. Wählen Sie im Dialogfeld *Farbverwaltung* die Registerkarte *Geräte*. Tippen oder klicken Sie auf das neue Profil und dann auf *Als Standardprofil festlegen*.

Wenn Sie nicht über ein Farbprofil verfügen, können Sie die Anzeigefarben auf dem Monitor mit dem Tool Bildschirm-Farbkalibrierung nach Bedarf anpassen. Um dieses Tool zu öffnen, geben Sie im Suchfeld *Apps Dccw.exe* ein und drücken die EINGABETASTE.

Beseitigen von Anzeigeproblemen

Wie bereits erwähnt, hat jeder Computer einen Monitor- und einen Grafikkartentreiber. Der Monitor-treiber teilt Windows die Fähigkeiten des Monitors mit, der Grafikkartentreiber die Fähigkeiten der Grafikkarte.

Ganz offensichtlich spielen Monitor- und Grafikkartentreiber eine wichtige Rolle auf einem Computer. Wenn Sie Anzeigekomponenten installieren oder einen Computer aufrüsten, sollten Sie sicher sein, dass der Computer über Treiber verfügt, die in Ihrer Umgebung getestet wurden und sich als zuverlässig erwiesen haben. Wenn Sie ein Problem mit den Treibern vermuten, sollten Sie sie möglichst bald aktualisieren. Wenn Sie vermuten, dass das Problem durch die Konfiguration des Computers verursacht wird, sollten Sie den Computer im abgesicherten Modus starten und dann die Standardeinstellungen ändern.

Bevor Sie mit der detaillierten Diagnose und Problembehandlung beginnen, sollten Sie untersuchen, welche Programme der Benutzer ausgeführt hat. Programme, die für ältere Windows-Versionen als Windows XP entwickelt wurden, verursachen manchmal Kompatibilitätsprobleme. Schließen Sie alle laufenden Programme und überprüfen Sie verdächtige Programme, um festzustellen, welchen Anzeigemodus sie verwenden. Wenn ein Programm einen anderen Anzeigemodus benötigt und das Hin- und Herschalten des Anzeigemodus Probleme verursacht, können Sie unter Umständen die Kompatibilitätseinstellungen so konfigurieren, dass das Problem beseitigt wird. Klicken Sie dazu mit der rechten Maustaste auf die Verknüpfung der Anwendung oder halten Sie die Verknüpfung gedrückt und wählen Sie den Befehl *Eigenschaften*. Wählen Sie im Eigenschaftendialogfeld die Registerkarte *Kompatibilität* aus. Aktivieren Sie im Feld *Einstellungen* die passenden Optionen, zum Beispiel *In Bildschirmauflösung 640x480 ausführen*. Wenn Sie sich nicht sicher sind, welche Kompatibilitätseinstellungen Sie verwenden müssen, können Sie mit der rechten Maustaste auf die Verknüpfung der Anwendung klicken oder die Verknüpfung gedrückt halten, den Befehl *Behandeln von Kompatibilitätsproblemen* wählen und dann den Anweisungen des Programmkompatibilitäts-Assistenten folgen.

Viele Probleme im Zusammenhang mit Monitoren haben mit der Verbindung zwischen Monitor und Computer zu tun. Wird das Monitorbild durch Flecken, Farbverschiebungen, diagonale Linien, horizontale Balken oder andere Probleme verunstaltet, sollten Sie zuerst die Monitorverbindung überprüfen. Wenn Sie sicher sind, dass die Verkabelung in Ordnung ist, können Sie den Monitor für mindestens 10 Sekunden ausschalten und dann wieder einschalten. Wenn das Problem weiterhin besteht und Sie den Verdacht haben, dass es am Monitor selbst liegt, können Sie versuchen, das Problem im Rahmen einer detaillierten Fehlerbehandlung zu lösen.

Ist das Bild des Monitors nicht stabil (Flackern, Zittern, Wackeln), können Konfigurationsprobleme oder ein ungeeigneter Standort die Ursache sein. Verursacht die Aktualisierungsrate des Monitors das Problem, können Sie es beseitigen, indem Sie die Einstellungen der Aktualisierungsrate ändern, wie weiter oben im Abschnitt »Ändern der Bildwiederholrate« beschrieben. Ist der Standort die Ursache für das Problem, können Sie möglicherweise die Kabel und Geräte verschieben, die elektromagnetische Störungen verursachen. Verdächtig sind in einem solchen Fall Stromkabel anderer Geräte, große Lautsprecher oder Schreibtischlampen. Besteht das Problem weiter, sollten Sie sicherstellen, dass der Monitor geschirmte Kabel hat und nicht zu nah an Klimaanlage, großen Leuchtstofflampen oder ähnlichen Störquellen steht.

Wenn der Monitor Bedienelemente eingebaut hat, können Sie nach einer Möglichkeit suchen, die automatische Feinabstimmung oder Einstellung zu aktivieren. Dafür gibt es oft eine separate Taste; sobald Sie diese Taste drücken, passt sich der Monitor automatisch an das Signal an.

Falls Flecken, Farbverschiebungen oder Linien auftreten und sich das Problem durch das Überprüfen und Korrigieren der Verbindungen nicht beseitigen lässt, müssen Sie den Monitor unter Umständen entmagnetisieren (engl. degauss). Bei diesem Vorgang werden magnetische Felder beseitigt, die sich im Lauf der Zeit um einen Röhrenmonitor aufbauen können und das Bild beeinträchtigen. Manche Monitore führen automatisch eine Entmagnetisierung durch, wenn Sie den Monitor aus- und dann wieder einschalten, bei anderen Modellen gibt es eine Option oder eine Taste für diesen Zweck, manchmal werden auch beide Varianten kombiniert. Möglicherweise finden Sie am Monitor eine Taste, die mit *Degauss* beschriftet ist, oder im internen Menü des Monitors gibt es eine entsprechende Option. Während der Monitor entmagnetisiert wird, wird der Bildschirm kurzzeitig verzerrt. Das ist während des Entmagnetisierungsvorgangs normal. Wenn Sie die Entmagnetisierung von Hand auslösen, sollten Sie 15 bis 20 Minuten warten, bevor Sie den Vorgang wiederholen.

Wenn die Probleme immer noch nicht beseitigt sind, sollten Sie sicherstellen, dass der Monitor direkt an den Computer angeschlossen ist. Entfernen Sie alle Verlängerungskabel, die zwischen Monitor und Grafikkarte hängen. Entfernen Sie auch alle Entspiegelungsmechanismen oder ähnliche Geräte, die den Bildschirm des Monitors überdecken. Prüfen Sie, ob einzelne Pins am Monitorkabel verbogen oder gebrochen sind oder ganz fehlen. Einige Pins sind zwar nicht verdrahtet, aber wenn andere Pins fehlen oder verbogen sind, kann das Anzeigeprobleme auslösen. Wenn Pins verbogen sind und sich der Stecker reparieren lässt, sollten Sie den Monitor ausschalten, das Netzkabel des Monitors abziehen und die Pins mithilfe einer Pinzette oder einer Zange gerade biegen.

Kapitel 4

Verwalten von Firmware, Startkonfiguration und Systemstart

In diesem Kapitel:

Firmwareoptionen	150
Start- und Energiemodi	154
Analysieren und Beseitigen von Startproblemen	162
Verwalten der Systemstartkonfiguration	168
Verwalten des BCD-Speichers	172

Wenn bei einem Computer der Start fehlschlägt oder ein Abbruchfehler auftritt, der das Betriebssystem zum Absturz bringt, wird bei der Suche nach der Fehlerursache seltsamerweise oft das grundlegendste Element für den Start von Computer und Betriebssystem übersehen: die Firmware. Das passiert, weil die meisten Leute sich sofort auf die Problembehandlung von Windows stürzen, ohne die Firmware zu beachten. Dieser Ansatz ist so fatal, weil viele Computerprobleme ihre Ursache in der Firmware haben, entweder weil die Firmware selbst fehlerhaft ist oder weil sie falsch konfiguriert ist. Um zwischen Problemen in der Firmware und Problemen im Betriebssystem unterscheiden zu können, müssen Sie wissen, wie der Startvorgang funktioniert und was während seiner einzelnen Phasen passiert. Außerdem müssen Sie die Firmware selbst kennenlernen. Wenn Sie sich mit diesen Elementen gut auskennen, sind Sie besser in der Lage, entsprechende Probleme zu diagnostizieren und zu beseitigen.

Firmwareoptionen

Am Startvorgang sind Firmware, Firmwareschnittstellen und ein Betriebssystem beteiligt. Während des Systemstarts ist die Firmware der erste Code, der ausgeführt wird. Die Firmware führt eine Grundinitialisierung des Computers durch und stellt die Dienste bereit, die es einem Computer ermöglichen, ein Betriebssystem zu laden.

Plattformfirmware ist in Chipsätzen des Mainboards implementiert. Alle Computer, ob es sich nun um Tablets, Desktops oder Laptops handelt, verfügen auf ihren Mainboards über spezielle Chips mit Firmware. Es gibt viele unterschiedliche Arten dieser Mainboardchipsätze. Ältere Mainboardchipsätze können unter Umständen nicht aktualisiert werden, aber die meisten neuen Modelle ermöglichen ein Firmwareupdate. Die Chipsatzfirmware ist klar von der zugrunde liegenden Firmwareschnittstelle des Computers getrennt.

Windows für die Prozessorarchitektur ARM (auch Windows On Arm oder WOA genannt) wurde ebenfalls für die Verwendung von Plattformfirmware entworfen, die in einem Mainboardchipsatz gespeichert ist. Allerdings kann man das Mainboard mit WOA auch als eine Reihe von Silikon-Schichten betrachten, die in einem sehr kleinen Formfaktor zusammengepackt wurden – ein »System on Chip« (SoC).

HINWEIS

WOA ist für Firmware, Startkonfiguration und Systemstart ein Sonderfall. Ich habe zwar versucht, einige WOA- und Windows RT-Aspekte in diesem Kapitel anzusprechen, aber nicht alles, was in diesem Kapitel beschrieben wird, gilt auch für WOA oder Windows RT.

Firmwareschnittstellentypen und Systemstartdaten

Jeder Computer hat eine Firmware, aber es ist die Schnittstelle zwischen der Plattformfirmware und dem Betriebssystem, die den Startvorgang erledigt. Auf welche Weise eine Firmwareschnittstelle arbeitet und welche Aufgaben sie ausführt, hängt von der Art der Firmwareschnittstelle ab. Momentan sind folgende Firmwareschnittstellen in Gebrauch:

- BIOS (Basic Input/Output System)
- EFI (Extensible Firmware Interface)
- UEFI (Unified Extensible Firmware Interface)

BIOS, EFI oder UEFI eines Computers stellen die Hardwareschnittstelle zwischen Hardwarekomponenten und Software bereit. Wie Chipsätze selbst können auch BIOS, EFI und UEFI aktualisiert werden. Die meisten technischen Dokumente bezeichnen die Firmwareschnittstelle eines Computers einfach als Firmware. Zum Beispiel steht in der Dokumentation gewöhnlich, dass Sie »diese und jene Änderung in der

Firmware vornehmen« oder »die Firmware prüfen« sollen. Genau genommen nehmen Sie die Änderung aber in der Firmwareschnittstelle vor, und die Firmwareschnittstelle führt dann die Änderung in der Firmware durch.

UEFI ist sowohl eine Firmwareschnittstelle als auch ein Industriestandard. Als Firmwareschnittstelle ist UEFI modular. Es erfüllt unter Umständen einen anderen Zweck als BIOS oder EFI, und es bietet möglicherweise eine andere Funktionalität. Der Standard UEFI ist so aufgebaut, dass er erweiterbare und testbare Schnittstellen zur Verfügung stellt. Für WOA ist UEFI die unterste Schicht des Systems. Wie bei anderen Chiparchitekturen bietet UEFI die Dienste an, die für das Laden des Betriebssystems erforderlich sind. Außerdem unterstützt WOA zur Verschlüsselung von Laufwerken TPM.

Außerdem ist wichtig zu wissen, dass BIOS, EFI und UEFI auf ganz unterschiedliche Weise arbeiten. BIOS basiert auf dem 16-Bit-Realmodus der x86-Architektur und wurde ursprünglich entworfen, um einen Computer nach dem Einschalten der Stromversorgung zu starten. Aus diesem Grund bildet das BIOS die Schnittstelle zwischen Firmware und Betriebssystem und initialisiert die Plattform.

Windows 8 benutzt unabhängig vom Firmwareschnittstellentyp eine Vor-Betriebssystem-Startumgebung. Diese Startumgebung ist eine erweiterbare Abstraktionsschicht, die es dem Betriebssystem ermöglicht, mit mehreren Arten von Firmwareschnittstellen zusammenzuarbeiten, ohne dass das Betriebssystem speziell auf die Ansteuerung dieser Firmwareschnittstellen abgestimmt sein muss. Innerhalb der Startumgebung wird der Systemstart mithilfe von Parametern im Startkonfigurationsdatenspeicher (Boot Configuration Data, BCD) gesteuert.

Alle Computer, die unter Windows Vista und höher laufen, haben einen BCD-Speicher. Der BCD-Speicher liegt in einer Datei, die als BCD-Registrierung (engl. BCD registry) bezeichnet wird. Der Speicherort dieser Registrierung hängt von der Firmware des Computers ab:

- In BIOS-basierten Betriebssystemen liegt die BCD-Registrierungsdatei im Verzeichnis `\Boot\Bcd` der aktiven Partition.
- In EFI-basierten Betriebssystemen ist die BCD-Registrierungsdatei in der EFI-Systempartition gespeichert.

Die Einträge im BCD-Speicher legen fest, welcher Startmanager während des Systemstarts benutzt wird und welche Startanwendungen zur Verfügung stehen. Der Standardstartmanager ist der Windows-Start-Manager. Der Windows-Start-Manager steuert die Abläufe beim Systemstart und ermöglicht Ihnen auszuwählen, welche Startanwendung ausgeführt wird. Systemstartanwendungen laden ein bestimmtes Betriebssystem oder eine bestimmte Betriebssystemversion. Die Startanwendung für Windows 8 ist beispielsweise das Windows-Startladeprogramm. Daher können Sie BIOS-basierte und EFI-basierte Computer auf praktisch dieselbe Weise starten.

Im Allgemeinen können Sie während des Starts des Betriebssystems die Tasten F8 oder F12 drücken, um das Menü *Erweiterte Startoptionen* zu öffnen. In diesem Menü können Sie einen der verfügbaren erweiterten Startmodi auswählen, darunter *Abgesicherter Modus*, *Startprotokollierung aktivieren* und *Erzwingen der Treibersignatur deaktivieren*. Diese erweiterten Modi ändern temporär den Ablauf des Betriebssystemstarts, um Ihnen die Gelegenheit zu bieten, Probleme zu diagnostizieren und zu beseitigen. Sie nehmen aber keine dauerhaften Änderungen an der Systemstartkonfiguration oder dem BCD-Speicher vor.

Systemstartdienste, Laufzeitdienste und andere Elemente

Das BIOS verwaltet den Datenfluss, der vor dem Start zwischen Betriebssystem und angeschlossenen Geräten wie Grafikkarte, Tastatur, Maus und Festplatte hin- und herläuft. Wenn das BIOS einen Computer initialisiert, stellt es zuerst fest, ob alle angeschlossenen Geräte verfügbar sind und funktionieren. Anschließend beginnt es damit, das Betriebssystem zu laden.

Im Lauf der Jahre wurden diese grundlegenden Funktionen des BIOS immer stärker erweitert und umfassen inzwischen folgende Elemente:

- **Systemstartdienste** Unter diesem Begriff werden etliche Schnittstellen und Protokolle zusammengefasst, die in der Startumgebung zur Verfügung stehen. Die Dienste stellen auf jeden Fall einen Betriebssystemlader mit Zugriff auf Plattformfähigkeiten bereit, die gebraucht werden, um den Start des Betriebssystems abzuschließen. Diese Dienste stehen auch Treibern und Anwendungen zur Verfügung, die Zugriff auf Plattformfähigkeiten benötigen. Systemstartdienste werden beendet, sobald das Betriebssystem die Kontrolle über den Computer übernimmt.
- **Laufzeitdienste** Dies sind die Schnittstellen, die Zugriff auf zugrunde liegende plattformspezifische Hardware bieten, beispielsweise auf Timer, die während der Betriebssystemausführung nützlich sind. Diese Dienste stehen während des Startprozesses zur Verfügung, aber auch später noch, nachdem der Betriebssystemlader die Systemstartdienste beendet hat.
- **Advanced Configuration and Power Interface (ACPI)** Eine tabellenbasierte Schnittstelle zum Mainboard, die es dem Betriebssystem ermöglicht, Energieverwaltung und Systemkonfiguration zu steuern.
- **Dienste für System Management BIOS (SMBIOS)** Eine tabellenbasierte Schnittstelle, die für die WMB-Spezifikation (Wired für Management Baseline) benötigt wird. Sie wird benutzt, um plattform-spezifische Verwaltungsdaten an das Betriebssystem oder einen vom Betriebssystem ausgeführten Verwaltungsagenten weiterzugeben.

Computer mit BIOS benutzen im Allgemeinen Festplatten, die MBR-Partitionen (Master Boot Record) haben. Um die 16-Bit-Wurzeln des BIOS hinter sich zu lassen, entwickelte Intel EFI als neue Firmwareimplementierung für seine 64-Bit-Itanium-Prozessoren. EFI basiert auf dem 64-Bit-Realmodus der x64-Architektur. Wie das BIOS stellt auch EFI die Schnittstelle zwischen Firmware und Betriebssystem bereit, erledigt die Plattforminitialisierung und einige andere Funktionen. Bei der Einführung von EFI stellte Intel auch eine neue Tabellenarchitektur für Festplatten bereit, die auf den Namen GPT (GUID Partition Table) getauft wurde.

UEFI

Als Intel mit der Entwicklung von EFI begann, wurde Entwicklern bei Intel und anderen Herstellern bewusst, dass die enge Verknüpfung zwischen Firmware und Prozessorarchitektur aufgehoben werden musste. Das führte zur Entwicklung von UEFI. Die Spezifikation wurde im Januar 2006 als UEFI 2.0 verabschiedet und erreichte im April 2011 den Stand UEFI 2.3.1. Die UEFI-Spezifikationen definieren ein Modell für die Schnittstelle zwischen Betriebssystemen und Plattformfirmware. Diese Schnittstelle besteht aus Datentabellen, die plattformbezogene Daten sowie Systemstart- und Laufzeitdienstaufrufe enthalten, die dem Betriebssystem und seinen Ladeprogrammen zur Verfügung stehen. Die Schnittstelle ist von der Prozessorarchitektur unabhängig. Weil UEFI die Prozessorarchitektur abstrahiert, arbeitet es mit Computern, die eine x86-, x64-, ARM- oder eine beliebige andere Architektur haben. Wie bei EFI benutzen Computer mit UEFI im Allgemeinen Festplatten, die GPT-Partitionen haben. UEFI ersetzt allerdings nicht den gesamten Funktionsumfang von BIOS oder EFI, sondern erweitert BIOS oder EFI lediglich.

PRAXISTIPP

Die UEFI-2.3.1-Spezifikation ist über 2.200 Seiten lang. Um Ihnen die nicht immer spannende Lektüre zu ersparen, habe ich das Wichtigste hier zusammengefasst.

In UEFI ist die SAL (System Abstraction Layer) die Firmware, die Unterschiede in der Plattformimplementierung abstrahiert und die grundlegende Schnittstelle zu allen höheren Softwareschichten bereitstellt. UEFI definiert Systemstartdienste und Laufzeitdienste.

Zu den UEFI-Systemstartdiensten gehören:

- Ereignis-, Zeitgeber- und Aufgabenprioritätsdienste, die Ereignisse erstellen, auf Ereignisse warten, Ereignisse signalisieren, prüfen und abschließen, Zeitgeber einrichten und die Priorität von Aufgaben anheben oder wiederherstellen
- Speicherzuweisungsdienste, die Arbeitsspeicherseiten reservieren oder freigeben, Arbeitsspeicherzuordnungen abrufen und gepoolten Arbeitsspeicher reservieren oder freigeben
- Treibermodellsystemstartdienste, die Protokollschnittstellen für Geräte verwalten, Protokollströme öffnen oder schließen und Verbindungen zu Controllern aufbauen oder trennen
- Abbilddienste, die Abbilder laden, starten und freigeben
- Verschiedene Dienste, die Watchdog-Zeitgeber einrichten, Arbeitsspeicher kopieren und füllen, Konfigurationstabellen installieren und CRC-Berechnungen (Cyclic Redundancy Checking) ausführen

Wichtige UEFI-Laufzeitdienste sind:

- Variablendienste, die Variablen abrufen, ändern und abfragen
- Zeitdienste, die die Uhrzeit ermitteln und ändern sowie die Aufwachzeit ermitteln und festlegen
- Dienste für virtuellen Arbeitsspeicher, die Zuordnungen für virtuelle Adressen festlegen und Arbeitsspeicherzeiger konvertieren
- Verschiedene Dienste, die den Computer zurücksetzen, Leistungsindikatoren liefern und Informationen an die Firmware übergeben

UEFI definiert architekturunabhängige Modelle für Abbilder, die mit EFI geladen werden, Gerätepfade, Gerätetreiber, Treibersignierung und sicheren Systemstart. Außerdem definiert es folgende Elemente:

- Konsolenunterstützung, die einfache Text- und Grafikausgabe ermöglicht
- Unterstützung für eine HI-Infrastruktur (Human Interface), die grundlegende Mechanismen für die Verwaltung von Benutzereingaben beschreibt und zugehörige Protokolle, Funktionen und Typdefinitionen definiert, mit deren Hilfe sich Benutzereingaben abstrahieren lassen
- Medienunterstützung, die E/A-Zugriff auf Dateisysteme, Dateien und Mediengeräte ermöglicht
- Unterstützung für die Bustypen PCI (Peripheral Component Interconnect), SCSI (Small Computer System Interface) und iSCSI (Internet Small Computer System Interface), die E/A-Zugriff über einen PCI-, SCSI- oder iSCSI-Bus sowie einen Systemstart von SCSI oder iSCSI erlaubt
- USB-Unterstützung (Universal Serial Bus), die E/A-Zugriff über USB-Hostcontroller, -Busse und -Geräte zur Verfügung stellt
- Komprimierungsunterstützung, die Algorithmen zum Komprimieren und Dekomprimieren von Daten bereitstellt
- Unterstützung für ACPI-Tabellen, die das Installieren oder Entfernen einer ACPI-Tabelle erlaubt
- Unterstützung für virtuelle Computer mit EFI-Bytecode, die es erlaubt, EFI-Gerätetreiber zu laden und auszuführen
- Netzwerkprotokollunterstützung, die die Protokolle SNP (Simple Network Protocol), PXE (Preboot Execution Environment) und BIS (Boot Integrity Services) definiert. SNP stellt eine Paketebenenschnittstelle zu Netzwerkkarten bereit. PXE wird für Netzwerkzugriff und Netzwerkstart eingesetzt. Mit BIS wird die digitale Signatur eines Datenblocks anhand eines digitalen Zertifikats geprüft, um

die Integrität und Autorisierung sicherzustellen. PXE greift auf BIS zurück, um heruntergeladene Netzwerkstartabbilder zu überprüfen, bevor sie ausgeführt werden.

- Unterstützung für verwaltete Netzwerke, mit denen MNSBP (Managed Network Service Binding Protocol) und MNP (Managed Network Protocol) definiert werden. Diese Dienste ermöglichen es mehreren ereignisgesteuerten Treibern und Anwendungen, parallel auf Netzwerkschnittstellen zuzugreifen. MNSBP wird benutzt, um Kommunikationsgeräte zu suchen, die von einem MNP-Laufwerk unterstützt werden, und um Instanzen von Protokolltreibern zu verwalten. MNP wird von Treibern und Anwendungen benutzt, um asynchrone Netzwerk-E/A für Paketrohdaten durchzuführen.
- Unterstützung für Netzwerkadressprotokolle, die folgende Protokolle definiert: ARPSBP (Address Resolution Protocol Service Binding Protocol), ARP (Address Resolution Protocol), DHCPv4, DHCPv4-Dienstbindung, DHCPv6 und DHCPv6-Dienstbindung
- Unterstützung für diverse andere Netzwerkprotokolle, die folgende Protokolle definiert: Virtuelle LAN-Konfiguration, EAP/EAP-Verwaltung, TCPv4, TCPv4-Dienstbindung, TCPv6, TCPv6-Dienstbindung, IPv4, IPv4-Dienstbindung und -Konfiguration, IPv6, IPv6-Dienstbindung und -Konfiguration, IPSec- und IPSec2-Konfiguration, FTPv4, FTPv4-Dienstbindung, UDPv4, UDPv4-Dienstbindung, UDPv6, UDPv6-Dienstbindung, Multicast-TFTPv4 und Multicast-TFTPv6

HINWEIS

Mit WOA wird ACPI beim Start zur Aufzählung von Plug & Play-Geräten verwendet (Touchcontroller, Anzeige und so weiter), und außerhalb des SoC zur Energieverwaltung von Geräten. Ansonsten gibt es keinen Gerätebaum oder die Möglichkeit herauszufinden, was mit einem SoC verbunden ist oder wie das SoC verbunden ist.

Noch einmal, weil dieser Punkt wichtig ist: UEFI soll BIOS oder EFI nicht vollständig ersetzen. Während UEFI eine andere Schnittstelle für Systemstartdienste und Laufzeitdienste benutzt, müssen manche Plattformfirmwareimplementierungen die Funktionen ausführen, die BIOS und EFI für Systemkonfiguration und Setup benötigen, weil UEFI diese Funktionen nicht zur Verfügung stellt. Aus diesem Grund wird UEFI oft so implementiert, dass es auf einem herkömmlichen BIOS oder EFI aufsetzt. In einem solchen Fall übernimmt UEFI die Funktion des Einstiegspunkts in BIOS oder EFI, der für die Initialisierung aufgerufen wird.

Start- und Energiemodi

Wird ein Computer neu gestartet, nachdem der Strom abgeschaltet war, aktiviert die Firmwareschnittstelle die ganze Hardware, die der Computer für den Systemstart braucht. Dazu gehören:

- Mainboardchipsätze
- Prozessoren und Prozessorcaches
- Systemarbeitsspeicher
- Grafik- und Audiocontroller
- Interne Laufwerke
- Interne Erweiterungskarten

Sobald die Firmwareschnittstelle diesen Vorgang abgeschlossen hat, übergibt sie die Kontrolle über den Computer an das Betriebssystem. Die Implementierung der Firmwareschnittstelle bestimmt, was als Nächstes passiert:

- Bei einem BIOS-basierten Computer, der unter Windows XP oder älteren Windows-Versionen läuft, werden *Ntldr* und *Boot.ini* benutzt, um das Betriebssystem zu starten. *Ntldr* übernimmt die Aufgabe, das Betriebssystem zu laden, und *Boot.ini* enthält die Parameter, die den Startvorgang ermöglichen, beispielsweise die Identität der Startpartitionen. Mithilfe der Parameter in *Boot.ini* können Sie Optionen hinzufügen, die steuern, auf welche Weise das Betriebssystem startet, die Computerkomponenten eingesetzt werden und die Betriebssystemfeatures benutzt werden.
- Bei BIOS-basierten Computern, die unter Windows Vista oder neueren Windows-Versionen laufen, werden der Windows-Start-Manager und das Windows-Startladeprogramm benutzt, um das Betriebssystem zu starten. Der Windows-Start-Manager initialisiert das Betriebssystem, indem er das Windows-Startladeprogramm ausführt, das dann wiederum das Betriebssystem mithilfe von Informationen im BCD-Speicher startet. Über die BCD-Parameter können Sie Optionen hinzufügen, die steuern, auf welche Weise das Betriebssystem startet, die Computerkomponenten eingesetzt werden und die Betriebssystemfeatures benutzt werden.
- Bei Itanium-Computern werden *Ia64ldr.efi*, *Diskpart.efi* und *Nvrboot.efi* benutzt, um das Betriebssystem zu starten. *Ia64ldr.efi* hat die Aufgabe, das Betriebssystem zu laden, während *Diskpart.efi* die Startpartitionen identifiziert. Mit *Nvrboot.efi* konfigurieren Sie die Parameter, die den Start ermöglichen.
- Bei anderen EFI-basierten Computern verwaltet *Bootmgfw.efi* den Startprozess und übergibt die Kontrolle an das Windows-Startladeprogramm. Über *Bcdedit.exe* konfigurieren Sie die Parameter, die den Start ermöglichen.
- Bei UEFI stellen die UEFI-Systemstartdienste eine Abstraktionsschicht zur Verfügung. Momentan setzt diese Abstraktionsschicht auf BIOS oder EFI auf. Ein Computer mit BIOS als zugrunde liegender Architektur benutzt einen BIOS-basierten Ansatz, um das Betriebssystem zu starten. Ein Computer mit EFI als zugrunde liegender Architektur nutzt entsprechend einen EFI-basierten Ansatz für den Start des Betriebssystems.
- Mit WOA stellen die UEFI-Systemstartdienste eine Abstraktionsschicht zur Verfügung. Der Windows-Start-Manager initialisiert das Betriebssystem, indem er das Windows-Startladeprogramm ausführt, das dann wiederum das Betriebssystem mithilfe von Informationen im BCD-Speicher startet. Die für die Konfiguration des Geräts benötigten Informationen werden in Tabellen gespeichert.

Arbeiten mit Firmwareschnittstellen

Wenn Sie einen Computer einschalten, können Sie bei den meisten Modellen die Firmwareschnittstelle aufrufen, indem Sie eine bestimmte Taste drücken. Welche Taste das ist, wird auf dem Startbildschirm angezeigt. Beispielsweise müssen Sie bei vielen Computern während der ersten Sekunden nach dem Einschalten F2 oder ENTF drücken, um die Firmwareschnittstelle zu öffnen. Die Firmwareschnittstellen stellen Steuerungsoptionen bereit, mit denen Sie bestimmte Hardwarefunktionen einstellen können. Unter anderem können Sie folgende Elemente konfigurieren:

- Ändern der Monitorhelligkeit (bei Notebooks)
- Anpassen der Festplattenlautstärke
- Einstellen, wie viele Kerne der Prozessor benutzt und wie schnell sie getaktet werden
- Ändern der Startreihenfolge
- Ändern von Datum und Uhrzeit im CMOS (Complementary Metal Oxide Semiconductor)
- Zurücksetzen der Firmwareschnittstelle auf die Standardkonfiguration
- Ein- und Ausschalten modularer Zusatzgeräte

Firmwareschnittstellen sind in der Lage, grundlegende Konfigurationsinformationen aufzulisten, darunter Daten über folgende Elemente:

- Netzteilkapazität (bei Notebooks)
- Ladezustand und Verfassung des Akkus (bei Notebooks)
- Monitortyp und Hardwareauflösung (bei Notebooks)
- Firmwareversion
- Arbeitsspeicher
- Prozessoren
- Speichergeräte
- Grafikkhipsatz

In den meisten Firmwareschnittstellen können Sie Kennwörter für Administratoren, normale Benutzer und/oder allgemeine Benutzer festlegen, auf die das Betriebssystem keinen Zugriff hat. Ist ein Administrator Kennwort (meist als »supervisor« bezeichnet) eingetragen, müssen Sie dieses Kennwort eingeben, bevor Sie die Firmwarekonfiguration ändern dürfen. Ist dagegen ein Benutzerkennwort eingetragen, müssen Sie das Kennwort jedes Mal beim Start eingeben, bevor der Computer das Betriebssystem lädt. Vergessen Sie diese Kennwörter, können Sie unter Umständen nicht mit dem Computer arbeiten oder seine Firmwareeinstellungen ändern, bis Sie die vergessenen Kennwörter gelöscht haben. Beim Löschen der Kennwörter gehen im Allgemeinen auch alle Einstellungen verloren, die Sie in der Firmwareschnittstelle geändert haben.

Ein Update der Firmwareschnittstelle löst oft Probleme oder erweitert die Firmwareschnittstelle des Computers durch neue Features. Sofern beim Betrieb des Computers keine Probleme auftreten und Sie keine neuen Features in der Firmwareschnittstelle benötigen, können Sie gewöhnlich darauf verzichten, die Firmwareschnittstelle des Computers auf die neuste Version zu aktualisieren. Ein Update der Firmwareschnittstelle ist nicht ganz ungefährlich: Kommt es dabei zu einem Fehler, startet der Computer möglicherweise gar nicht mehr.

Aufbau der Firmwareschnittstellen

Welche Informationen und Konfigurationsoptionen in der Firmwareschnittstelle angeboten werden, hängt von dem Computer ab, mit dem Sie arbeiten, vom Typ der Firmwareschnittstelle und von der Version der Firmwareschnittstelle. Die meisten Desktopcomputer haben mehr Konfigurationsoptionen als Notebooks.

Eine momentan weit verbreitete Firmwareschnittstelle ist Phoenix SecureCore. Auf meinem Notebook stellt diese Schnittstelle mehrere Menüseiten mit Informationen und Einstellmöglichkeiten zur Verfügung, darunter *Main*, *Advanced*, *Security* und *Boot*.

HINWEIS

Die Firmwareschnittstellen sind bei vielen Computern nur in englischer Sprache verfügbar, nur in seltenen Fällen auf Deutsch. In den folgenden Abschnitten wurden daher bei den Menüs die englischen Bezeichnungen beibehalten.

Auf der Seite *Main* werden wichtige Daten zur Konfiguration des Computers aufgeführt, darunter:

- Systemuhrzeit und Datum
- Größe des Systemarbeitsspeichers
- Größe des erweiterten Arbeitsspeichers

- Speichergeschwindigkeit, beispielsweise 1.333 MHz
- CPU-Typ, zum Beispiel Intel Core i5-2430
- CPU-Geschwindigkeit, beispielsweise 2,4 GHz
- CPU-Cachegrößen für den L1-Cache, L2-Cache und L3-Cache
- Typ und Modell der Festplatte, zum Beispiel WDC WD5000BPVT-75HXZ
- Typ und Modell des optischen Laufwerks, zum Beispiel PLDS DVD +/- RW DU 8A-(S1) ATAPI
- System-BIOS-Version, zum Beispiel A02
- Stromversorgungsadaptertyp, beispielsweise 65 Watt
- Seriennummer
- Inventarnummer
- Produktname

Auf der Seite *Main* können Sie mit den verfügbaren Optionen das Systemdatum und die Systemzeit einstellen. Die Seite *Advanced* bietet zusätzliche Konfigurationsinformationen und ermöglicht die Verwaltung von wichtigen Einstellungen. Auf dieser Seite können Sie folgende Angaben anzeigen oder festlegen:

- Systemuhrzeit
- Systemdatum
- Größe des Systemarbeitsspeichers
- Größe des erweiterten Arbeitsspeichers
- Größe des Grafikarbeitsspeichers

Außerdem können Sie folgende Elemente ansehen oder ändern:

- *Intel Multiple Monitor*-Status als *Enabled* oder *Disabled*. Ist diese Einstellung deaktiviert, zeigt der Computer während des Starts den Diagnosebildschirm an. Wenn diese Einstellung aktiviert ist, können die integrierte Grafikkarte des Computers und eine zusätzliche Grafikkarte gegebenenfalls im Betriebssystem zusammenarbeiten. Ist sie deaktiviert, kann im Betriebssystem nur eine Grafikkarte verwendet werden, entweder die integrierte Karte oder die Zusatzkarte.
- *Intel SpeedStep*-Status als *Enabled* oder *Disabled*. Ist diese Einstellung aktiviert, kann die CPU in mehreren Leistungsstufen arbeiten. Eine Deaktivierung hindert den Computer daran, die Leistung des Prozessors zu regeln.
- *Intel Virtualization*-Status als *Enabled* oder *Disabled*. Wenn diese Einstellung aktiviert ist, können virtuelle Computer die Hardwarevirtualisierung verwenden.
- *Intel Turbo Boost*-Status als *Enabled* oder *Disabled*. Ist diese Einstellung aktiviert, können Prozessorkerne schneller laufen, als es ihrer Standardarbeitsfrequenz entspricht, sofern sie die Grenzen für Temperatur, Strom- und Leistungsaufnahme noch nicht erreichen.
- *USB PowerShare*-Status als *Enabled* oder *Disabled*. Wenn diese Einstellung aktiviert ist, können Benutzer den USB-PowerShare-Anschluss verwenden, um selbst dann externe Geräte mit dem Systemakku zu laden, wenn der Computer ausgeschaltet ist.
- *USB Emulation*-Status als *Enabled* oder *Disabled*. Ist diese Einstellung aktiviert, kann die Firmware USB-Geräte bei der POST-Bearbeitung berücksichtigen (bevor das Betriebssystem hochfährt).
- *USB Wake Support*-Status als *Enabled* oder *Disabled*. Wenn diese Einstellung aktiviert ist, können USB-Geräte den Computer aufwecken.

Auf der Seite *Security* legen Sie die Administrator-, Benutzer- und Festplattenkennwörter fest. Die Statusinformationen zeigen den aktuellen Status für jedes Kennwort an. Wurden noch keine Kennwörter festgelegt, sieht die Anzeige so aus:

- *Supervisor Password Is: Clear*
- *User Password Is: Clear*
- *Hard Disk Password Status: Clear*

Mit den folgenden zusätzlichen Konfigurationsoptionen können Sie die Kennwörter verwalten:

- **Set Supervisor Password** Das Administratorkennwort kontrolliert den Zugriff auf die Firmwareschnittstelle.
- **Set User Password** Das Benutzerkennwort kontrolliert den Zugriff auf den Computer.
- **Set Hard Disk Password** Das Festplattenkennwort kontrolliert den Zugriff auf die Festplatte des Computers.

Sie legen ein Kennwort fest, indem Sie den Menüpunkt auswählen und die EINGABETASTE drücken. Geben Sie auf Anforderung das neue Kennwort ein und bestätigen Sie es durch eine zweite Eingabe. Drücken Sie die EINGABETASTE.

Im Bereich der Startreihenfolge können Sie ansehen und einstellen, in welcher Reihenfolge die Startgeräte durchprobiert werden. Die folgende Liste stammt von einem Dell-Desktopcomputer:

1. *Hard disk*
2. *USB hard disk*
3. *CD/DVD*
4. *USB CD/DVD*
5. *USB Floppy*
6. *Network*

Wenn Sie den Computer einschalten, versucht er von dem Gerät zu starten, das in der Liste an erster Stelle steht. Gelingt das nicht, versucht es der Computer mit dem zweiten Startgerät und so weiter. Sie können ein Gerät mit den Pfeiltasten auswählen und es dann mit den Tasten + oder – in der Liste nach oben oder unten verschieben.

Auf der Seite *Exit* können Sie die Firmwareschnittstelle verlassen und den Startvorgang des Computers fortsetzen. Wie bei den meisten Firmwareschnittstellen bekommen Sie hier mehrere Optionen zur Auswahl:

- **Exit Saving Changes** Verlässt die Firmwareschnittstelle und speichert Ihre Änderungen.
- **Exit Discarding Changes** Verlässt die Firmwareschnittstelle und verwirft Ihre Änderungen.
- **Discard Changes** Verwirft Ihre Änderungen, ohne die Firmwareschnittstelle zu verlassen.
- **Save Changes** Speichert Ihre Änderungen, ohne die Firmwareschnittstelle zu verlassen.

Auf allen Menüseiten stehen einige Optionen zur Verfügung, die in den meisten Firmwareschnittstellen gleich sind:

- Die Taste F1 zeigt einen Hilfetext an.
- Drücken Sie die Taste PFEIL-NACH-OBEN oder PFEIL-NACH-UNTEN, um ein Element auszuwählen.
- Drücken Sie die EINGABETASTE, um die aktuelle Option in einem Untermenü auszuwählen.

- Drücken Sie die Tasten PFEIL-NACH-LINKS oder PFEIL-NACH-RECHTS, um eine Menüseite auszuwählen.
- Drücken Sie + oder –, um die Werte zu ändern.
- Drücken Sie F9, um die Standardeinstellungen wiederherzustellen. (Sie müssen diesen Vorgang bestätigen, wenn Sie dazu aufgefordert werden.)
- Drücken Sie ESC, um die Firmwareschnittstelle zu verlassen (und wählen Sie dann aus, ob Sie Ihre Änderungen speichern oder verwerfen wollen).
- Drücken Sie die EINGABETASTE, um eine Einstellung zu wählen oder einen Befehl auszuführen.
- Drücken Sie F10, um Ihre Änderungen zu speichern und die Firmwareschnittstelle zu verlassen. (Wenn Sie aufgefordert werden, den Vorgang zu bestätigen, ist bereits die Option *Yes* ausgewählt. Drücken Sie einfach die EINGABETASTE, wenn Sie die Änderungen speichern und die Firmwareschnittstelle verlassen wollen. Drücken Sie die LEERTASTE, um die Option *No* auszuwählen, und dann die EINGABETASTE, um in der Firmwareschnittstelle zu bleiben.)

Wie Sie sehen, stehen hier nicht allzu viele Konfigurationsoptionen zur Verfügung. Dagegen bieten viele Desktopcomputer eine überwältigende Zahl von Optionen und Detail Einstellungen. Wenn Sie mit einem Desktopcomputer arbeiten, werden Sie wahrscheinlich Optionen finden, die ähnliche Aufgaben erfüllen. Weil sich die unterschiedlichen Hersteller der Firmwareschnittstellen kaum auf gemeinsame Standards und Konventionen geeinigt haben, haben die Optionen eventuell andere Bezeichnungen und Werte.

Energiesparmodi und Energieverwaltung

Damit Sie die Hardwareaspekte, die für Systemstartprobleme oft sehr wichtig sind, besser verstehen, müssen wir uns genauer mit ACPI (Advanced Configuration and Power Interface) beschäftigen. Der Mainboardchipsatz des Computers, die Firmware und das Betriebssystem müssen ACPI unterstützen, damit die entsprechenden Energiesparfeatures funktionieren. ACPI-fähige Komponenten verfolgen den Energiezustand des Computers. Ein ACPI-fähiges Betriebssystem kann eine Anforderung generieren, dass das System in einen anderen ACPI-Modus geschaltet wird, woraufhin die Firmwareschnittstelle den gewünschten ACPI-Modus aktiviert.

Wie in Tabelle 4.1 gezeigt, gibt es sechs unterschiedliche Energiezustände, von S0 (das System ist vollständig angeschaltet und betriebsbereit) bis S5 (das System ist vollständig ausgeschaltet). Die Zustände S1, S2, S3 und S4 werden als *Energiesparmodi* (engl. sleep states) bezeichnet. In diesen Zuständen scheint es, als wäre das System ausgeschaltet, weil es nur noch wenig Strom verbraucht, aber das System hält die Hardware dabei in einem Zustand, der es erlaubt, später weiterzuarbeiten, ohne dass das System neu gestartet werden muss.

Mainboardchipsätze unterstützen bestimmte, aber nicht immer alle Energiezustände. Zum Beispiel könnte ein Mainboard die Energiezustände S0, S1, S4 und S5 unterstützen, aber nicht S2 und S3. Windows-Betriebssysteme bieten die Möglichkeit, einen laufenden Computer in einen Standby- oder Ruhezustand zu versetzen und umgekehrt ein System aus dem Standby- oder Ruhezustand wieder aufzuwecken. Mithilfe der Standby- und Ruhezustandsmodi können die Benutzer ihr System viel schneller ein- und ausschalten als bei den normalen Ausschalt- und Startvorgängen.

Ein Computer wacht also auf, wenn er vom ausgeschalteten Zustand (S5) oder irgendeinem Ruhezustand (S1–S4) in den eingeschalteten Zustand (S0) wechselt. Im umgekehrten Fall wechselt der Computer vom eingeschalteten Zustand (S0) in den ausgeschalteten Zustand (S5) oder in einen der Ruhezustände (S1–S4). Ein Computer kann nicht direkt von einem Ruhezustand in einen anderen schalten; er muss sich im eingeschalteten Zustand befinden, bevor er in einen anderen Ruhezustand wechselt.

Tabelle 4.1 Energiezustände für ACPI in Firmware und Hardware

Zustand	Typ	Beschreibung
S0	Eingeschaltet	Das System ist vollständig betriebsbereit, alle Komponenten werden mit Strom versorgt und der Kontext wird lückenlos beibehalten (zum Beispiel flüchtige Register, Arbeitsspeichercaches und RAM).
S1	Standbymodus	Das System verbraucht weniger Strom als im Zustand S0. Alle Hardware- und Prozessorkontexte werden beibehalten.
S2	Standbymodus	Das System verbraucht weniger Strom als im Zustand S1. Der Prozessor wird nicht mehr mit Strom versorgt, daher gehen Prozessorkontext und Inhalt des Caches verloren.
S3	Standbymodus	Das System verbraucht weniger Strom als im Zustand S2. Prozessor- und Hardwarekontexte, Cacheinhalt und Chipsatzkontext gehen verloren. Der Inhalt des Systemarbeitsspeichers bleibt erhalten.
S4	Ruhezustand	Das System verbraucht weniger Strom als alle anderen Standbymodi, es ist beinahe vollständig ausgeschaltet. Die Kontextdaten werden auf die Festplatte geschrieben, in der Hardware selbst bleiben keine Kontextdaten mehr erhalten. Das System kann unter Benutzung der Kontextdaten gestartet werden, die auf Festplatte gespeichert sind.
S5	Ausgeschaltet	Das System ist ausgeschaltet und verwaltet keine Kontextdaten mehr. Um das System in Betrieb zu nehmen, muss es einen vollständigen Startvorgang durchlaufen.

Wenn Sie mit Firmware arbeiten, können Sie auf einer Seite, die meist *Advanced/Power Management* oder ähnlich heißt, ACPI und die zugehörigen Einstellungen verwalten. Hier finden Sie unter anderem folgende Energieeinstellungen:

- **Restore AC Power Loss oder AC Recovery** Legt fest, in welchen Betriebsmodus der Computer wieder anläuft, nachdem der Strom abgeschaltet war. Mögliche Werte sind *Stay Off*, *Last State* oder *Power On*. Die Einstellung *Stay Off* (oder *Power off*) bedeutet, dass das System ausgeschaltet bleibt, wenn der Strom wieder eingeschaltet wird. Bei *Last State* wird das System in den Zustand geschaltet, den es hatte, bevor der Strom ausgeschaltet wurde. Und *Power On* bedeutet, dass das System eingeschaltet wird, sobald der Strom wieder eingeschaltet ist.
- **Wake On LAN From S4/S5 oder Auto Power On** Legt fest, welche Aktion ausgeführt wird, wenn ein Aufwachereignis der PCI-Energieverwaltung auftritt, während das System ausgeschaltet ist. Mögliche Einstellungen sind auch hier *Power On* oder *Power Off*. Auch Einstellungen wie *Enabled* oder *Disabled* sind möglich.
- **ACPI Suspend State oder Suspend Mode** Legt den Modus des Standbyzustands fest. Normalerweise stellen Sie hier den Zustand S1 oder S3 ein.

HINWEIS

In dieser Beschreibung gebe ich jeweils zwei Bezeichnungen für jede Einstellung an, weil die Firmware Ihres Computers unter Umständen nicht genau dieselben Texte verwendet. Es hängt von der Firmwareversion ab, welche Bezeichnungen für Systemstart-, Standby- und andere Einstellungen verwendet werden.

Intel und AMD setzen unterschiedliche Techniken ein, um die Start- und Aufwachphasen zu beschleunigen. Bei einem Computer mit Intel-Prozessor finden Sie beispielsweise Energieeinstellungen wie diese:

- **Enhanced Intel SpeedStep Technologie (EIST)** Kann entweder aktiviert oder deaktiviert sein.
- **Intel Quick Resume Technology Driver (QRTD)** Kann entweder aktiviert oder deaktiviert sein.

EIST (auch SpeedStep genannt) ermöglicht dem System, die Prozessorspannung und den Kerntakt dynamisch anzupassen, was den Stromverbrauch und die Wärmeentwicklung senkt. Ist EIST oder eine ähnliche Technik aktiviert, bekommen Sie auf der Seite *System* in der Systemsteuerung zwei unterschied-

liche Prozessorgeschwindigkeiten angezeigt. Die erste ist die Nenngeschwindigkeit des Prozessors, die zweite die aktuelle Betriebsgeschwindigkeit, die oft kleiner ist als der erste Wert. Ist EIST ausgeschaltet, sind beide Prozessorgeschwindigkeiten gleich. Auch die erweiterten Einstellungen für die Prozessor-energieverwaltung unter *Energieoptionen* können Auswirkungen auf die Funktionsweise dieser Technik haben.

QRTD erlaubt einem Computer, der auf Intel Viiv-Technologie basiert, sich wie ein Unterhaltungselektronikgerät zu verhalten, das nach einem einmal erfolgten Start sofort ein- und ausgeschaltet werden kann. Intel QRTD verwaltet dieses Verhalten über den sogenannten Quick-Resume-Modus des Intel Viiv-Chipsatzes. Wenn Sie den Einschaltknopf am Computer oder auf einer Fernbedienung drücken, schaltet der Computer in den Quick-Sleep-Modus, aus dem Sie den Computer wieder in den Quick-Resume-Modus aufwecken, indem Sie die Maus bewegen, eine Ein-/Ausschalttaste auf der Tastatur drücken (sofern vorhanden) oder die Standbytaste auf der Fernbedienung drücken. Der Quick-Sleep-Modus unterscheidet sich vom normalen Standbymodus eines Computers, weil die Grafikkarte des Computers im Quick-Sleep-Modus keine Daten mehr an das Anzeigegerät sendet, der Ton stummgeschaltet ist und die Monitorlampe den Standbymodus anzeigt, dabei aber wichtige Komponenten des Systems weiterhin mit Strom versorgt werden, etwa Prozessor, Lüfter und so weiter. Diese Technologie wurde ursprünglich für Windows XP Media Center Edition entwickelt, sie sollte im Allgemeinen nicht für Windows 8 benutzt werden. (In vielen Fällen funktioniert sie nicht in Windows Vista. Unter Umständen müssen Sie dieses Feature in der Firmware deaktivieren, damit Standby und Aufwachen des Computers einwandfrei funktionieren.)

Wenn Sie die Energieeinstellungen des Computers in der Firmware konfiguriert haben, sollten Sie sich die Systemstarteinstellungen in der Firmware ansehen. Meist können Sie folgende Starteinstellungen in der Firmware konfigurieren:

- **Boot Drive Order** Legt die Startreihenfolge für Systemstartgeräte fest.
- **Boot To Hard Disk Drive** Legt fest, ob der Computer von einem fest eingebauten Datenträger starten kann. Mögliche Werte sind *Disabled* oder *Enabled*.
- **Boot To Removable Devices** Legt fest, ob der Computer von einem Wechseldatenträger starten kann. Mögliche Werte sind *Disabled* oder *Enabled*.
- **Boot To Network** Legt fest, ob der Computer einen Netzwerkstart durchführen kann. Mögliche Werte sind *Disabled* oder *Enabled*.
- **USB Boot** Legt fest, ob der Computer von einem USB-Speicherstick starten kann. Mögliche Werte sind *Disabled* oder *Enabled*.

Auf einigen Computern wird einfach nur eine Liste der startfähigen Geräte angezeigt und Sie können das gewünschte Gerät auswählen.

Wie bei den Energieeinstellungen gilt auch hier, dass die genauen Bezeichnungen bei Ihrem Computer unter Umständen anders lauten; sie sind aber meist sehr ähnlich. Sie müssen diese Einstellungen anpassen, damit Sie Ihren Computer wie vorgesehen starten können. Wenn Sie BitLocker-Laufwerkverschlüsselung einsetzen, sollten Sie *Boot To Removable Devices*, *USB Boot* oder beide aktivieren, damit sichergestellt ist, dass der Computer während des Startprozesses das USB-Flashlaufwerk mit dem Verschlüsselungsschlüssel erkennt.

Analysieren und Beseitigen von Startproblemen

Damit Sie Startprobleme diagnostizieren und beseitigen können, müssen Sie wissen, in welcher Reihenfolge die Ereignisse ablaufen, wenn Sie die Einschalttaste eines Computers drücken. In diesem Fall passiert Folgendes:

1. Die Firmwareschnittstelle führt die Systemkonfiguration durch. Dies wird als POST (Power-On Self Test) bezeichnet.
2. Die Firmwareschnittstelle richtet den Computer ein, auch als Initialisierung des Computers bezeichnet.
3. Die Firmwareschnittstelle übergibt die Kontrolle an den Betriebssystemlader, den sogenannten Startmanager.
4. Der Startmanager führt das Startladeprogramm aus. Das Startladeprogramm greift auf die Systemstartdienste der Firmwareschnittstelle zurück, um den Betriebssystemstart auszuführen und das Betriebssystem zu laden. Der Ladevorgang des Betriebssystems besteht aus folgenden Schritten:
 - a. Laden (aber nicht Ausführen) des Betriebssystemkerns, gewöhnlich *Ntoskrnl.exe*
 - b. Laden (aber nicht Ausführen) der Hardware Abstraction Layer (HAL), gewöhnlich *Hal.dll*
 - c. Laden der Registrierungsstruktur *HKEY_LOCAL_MACHINE\System* in den Arbeitsspeicher (aus *%SystemRoot%\System32\Config\System*)
 - d. Durchsuchen des Schlüssels *HKEY_LOCAL_MACHINE\System\Services* nach Gerätetreibern und Laden (aber nicht Initialisieren) der Treiber, die für die Startklasse konfiguriert sind, in den Arbeitsspeicher. Treiber sind ebenfalls Dienste (daher werden sowohl Gerätetreiber als auch Systemdienste vorbereitet).
 - e. Aktivieren der Arbeitsspeicherauslagerung
5. Das Startladeprogramm übergibt die Kontrolle an den Betriebssystemkern.
6. Systemkern und HAL initialisieren den Windows-Executive, der wiederum die Konfigurationsinformationen verarbeitet, die im Zweig *HKEY_LOCAL_MACHINE\System\CurrentControlSet* gespeichert sind, und dann die Gerätetreiber und Systemdienste startet.
7. Der Systemkern startet den Sitzungs-Manager (*Smss.exe*), der seinerseits folgende Schritte ausführt:
 - a. Er initialisiert die Systemumgebung, indem er Systemumgebungsvariablen anlegt.
 - b. Er startet das Win32-Subsystem (*Csrss.exe*). Hier schaltet Windows die Anzeigerausgaben vom Textmodus in den Grafikmodus um.
 - c. Er startet den Windows-Anmelde-Manager (*Winlogon.exe*), der wiederum den Dienststeuerungs-Manager (*Services.exe*) und die lokale Sicherheitsautorität (*Lsass.exe*) startet und darauf wartet, dass sich ein Benutzer anmeldet.
 - d. Er legt zusätzliche Auslagerungsdateien an, sofern sie gebraucht werden.
 - e. Bei Bedarf schließt er die Umbenennung von gesperrten Dateien ab, die in der vorherigen Sitzung aktualisiert wurden.
8. Der Windows-Anmelde-Manager wartet, bis sich ein Benutzer anmeldet. Der Anmeldebildschirm und der Standardanmeldeinformationsanbieter nehmen Benutzernamen und Kennwort entgegen und übergeben diese Daten zur Authentifizierung an die lokale Sicherheitsautorität.

9. Der Windows-Anmelde-Manager führt *Userinit.exe* und die Datei-Explorer-Shell aus. *Userinit.exe* initialisiert die Benutzerumgebung, indem es Benutzerumgebungsvariablen anlegt, Autostartprogramme ausführt und andere wichtige Aufgaben durchführt.

Diese Abfolge gilt für einen Kaltstart des Computers und erstreckt sich vom Einschalten des Stroms bis zur Benutzeranmeldung. Wird der Computer dagegen aus einem Standby- oder Ruhezustand wieder aufgeweckt, ist die Abfolge der Ereignisse etwas anders. Auch wenn Sie ein anderes Betriebssystem als Windows oder ein anderes Windows-Betriebssystem als Windows Vista oder höher starten, unterscheiden sich die Vorgänge in einigen Details.

TIPP Bei WOA ist die Abfolge der Ereignisse ähnlich, aber etwas anders. Hier stellt UEFI die für das Laden des Betriebssystems erforderlichen Dienste bereit. Der Windows-Start-Manager initialisiert das Betriebssystem, indem er das Startladeprogramm lädt, das wiederum das Betriebssystem startet, wobei es Informationen aus dem BCD-Speicher verwendet. Das Startladeprogramm übergibt die Kontrolle an den Betriebssystemkern. Der Systemkern und die HAL initialisieren den Windows-Executive. Die Informationen, die für die Konfiguration von WOA erforderlich sind, werden in Tabellen gespeichert, damit das Betriebssystem die Tabelle lesen und WOA konfigurieren kann. Um die Gerätetreiber zu laden und den Startvorgang fortzuführen, initialisiert der Windows-Executive die einfachen Peripheriebusse (eine Reihe von seriellen Bussen mit geringem Leistungsverbrauch) und dann die Gerätetreiber, die Verbindungen über diese Busse unterstützen. Dann kann der Systemkern den Sitzungs-Manager starten, der wiederum den Rest des Systems hochfährt.

Manchmal lässt sich die Ursache eines Startproblems dadurch aufspüren, dass Sie genau herausfinden, an welcher Stelle innerhalb des Startvorgangs ein Fehler auftritt. Tabelle 4.2 listet die verschiedenen Startphasen auf und beschreibt mögliche Ursachen für Probleme, die in der jeweiligen Phase auftreten. Die Nummerierung dient lediglich dazu, in den nächsten Abschnitten auf die verschiedenen Phasen zu verweisen.

Tabelle 4.2 Problembehandlung für den Systemstart

Phase	Name der Phase	Mögliche Ursachen für das Problem
1	Systemkonfiguration, Power-On Self Test	Hardwaredefekt oder fehlendes Gerät
2	Setup, Initialisierung	Firmwarekonfiguration, Laufwerkssystem oder Dateisystem
3	Betriebssystemlader, Startmanager	BCD-Einträge, falsche Auswahl für das zu ladende Betriebssystem oder ungültiges Startladeprogramm
4	Kernel, HAL, Windows-Executive	Konfiguration von Treiber oder Dienst; Dienstabhängigkeiten
5	Sitzungs-Manager	Grafikmodus, Systemumgebung oder Komponentenkonfiguration

Problembehebung in der Startphase 1

Wenn Sie einen vorher vollständig ausgeschalteten Computer einschalten, wird zuerst die Systemkonfiguration (Power-On Self Test) durchgeführt. Während dieser Phase führt die Firmware erste Prüfungen der Hardware durch, stellt fest, ob alle benötigten Geräte vorhanden sind, und liest die Systemkonfigurationseinstellungen aus dem nichtflüchtigen Speicher des Mainboards ein. Der nichtflüchtige Speicher kann als EEPROM (Electrically Erasable Programmable Read-Only Memory), Flashspeicher oder batteriegepuffertes RAM vorliegen. Meist handelt es sich um Flashspeicher, dessen Inhalt auch dann erhalten bleibt, wenn Sie den Computer herunterfahren und vom Strom trennen.

Sobald die Mainboardfirmware ihre Tests durchgeführt und die Einstellungen gelesen hat, führen Add-On-Geräte, die eigene Firmware haben, ihre Tests durch und laden ihre Einstellungen. Solche Geräte sind beispielsweise Grafikkarten und Hostcontrollerkarten. Schlägt der Start in dieser Phase fehl, hat der Computer wahrscheinlich einen Hardwaredefekt. Es kann auch sein, dass ein benötigtes Gerät fehlt, etwa Tastatur, Maus oder Festplatte. In den meisten Fällen zeigt die Firmwareschnittstelle eine Fehlermeldung an, die das Problem genauer beschreibt. Falls die Bildschirmausgabe nicht funktioniert, zeigt die Firmwareschnittstelle das Problem unter Umständen durch eine bestimmte Abfolge von Piepstönen an.

Ein Problem mit Tastatur, Maus oder Bildschirmausgabe können Sie beseitigen, indem Sie die Verbindung des Geräts zum Computer überprüfen. Verursacht ein anderes Gerät das Problem, können Sie den Fehler möglicherweise dadurch beheben, dass Sie die Gerätekonfiguration in der Firmwareschnittstelle ändern; vielleicht müssen Sie das Gerät auch austauschen.

Problembehebung in der Startphase 2

Sobald die Systemkonfiguration abgeschlossen ist, geht der Computer in die Setup- oder Initialisierungsphase über. Einstellungen der Firmwareschnittstelle legen fest, welche Geräte der Computer benutzt, um das Betriebssystem zu starten. Wie der Startvorgang abläuft, hängt von der Startreihenfolge und dem jeweiligen Status der verschiedenen Geräte ab. Wie bereits beschrieben, versucht der Computer zuerst, von dem Gerät zu starten, das am Anfang der Liste steht. Gelingt das nicht, probiert der Computer den Start vom zweiten Gerät und so weiter. Kann von keinem der konfigurierten Geräte gestartet werden, erhalten Sie eine Fehlermeldung, die etwa so aussieht:

Non-system disk oder disk error

Replace and press any key when ready to continue

In diesem Fall sollten Sie die Startreihenfolge überprüfen, sie muss richtig eingestellt sein. Falls Sie versuchen, von DVD zu starten, sollten Sie prüfen, ob das Medium richtig eingelegt ist und der Start vom DVD-Laufwerk aktiviert ist. Versuchen Sie, von einer Festplatte zu starten, muss der Start von Festplatte aktiviert sein, und die Festplatte muss vor allen USB- oder anderen Wechseldatenträgern aufgelistet sein, die Sie angeschlossen haben. Wenn Sie vor Kurzem eine neue Festplatte installiert haben, sollten Sie den Computer ausschalten, den Stromstecker abziehen und dann prüfen, ob alle Kabel richtig angeschlossen und die Steckbrücken richtig konfiguriert sind.

Weil es nicht immer ganz einleuchtend ist, wie die Startoptionen in der Firmware konfiguriert werden müssen, beschreibe ich hier einige Beispiele anhand einiger Computer von verschiedenen Herstellern. Auf einem HP-Notebook befinden sich die Systemstarteinstellungen auf der Seite *System Configuration* in den Untermenüs *Boot Options* und *Boot Order*. Das Untermenü *Boot Options* enthält folgende Optionen:

- **F10 And F12 Delay (sec)** Legt fest, wie lange der Benutzer beim Start Gelegenheit erhält, die Tasten F10 oder F12 zu drücken. Auf diesem Laptop führen F10 und F12 zu den Startoptionen und zu den erweiterten Startoptionen.
- **DVD Boot** Aktiviert oder deaktiviert den Start von DVD.
- **Floppy Boot** Aktiviert oder deaktiviert den Systemstart von Diskette.
- **Internal Network Adapter Boot** Aktiviert oder deaktiviert den Systemstart über das Netzwerk.

Wählen Sie eine Option mit den Tasten PFEIL-NACH-OBEN und PFEIL-NACH-UNTEN aus und drücken Sie die EINGABETASTE, um die möglichen Einstellungen anzuzeigen und zu ändern.

Im Untermenü *Boot Order* ist die Startreihenfolge folgendermaßen aufgelistet:

1. *USB Floppy*
2. *ATAPI CD/DVD ROM Drive*
3. *Notebook Hard Drive*
4. *USB Diskette On Key*
5. *USB Hard Drive*
6. *Network Adapter* (nur wenn *Internal Network Adapter Boot* aktiviert ist)

Hier können Sie mit den Tasten PFEIL-NACH-OBEN und PFEIL-NACH-UNTEN ein Gerät auswählen und dann F5 oder F6 drücken, um das Gerät in der Liste nach oben oder unten zu verschieben. Dieser Computer unterscheidet (wie viele neuere Modelle) zwischen USB-Flashsticks (als *USB Diskette On Key* bezeichnet) und USB-Laufwerken (*USB Hard Drive*). Für die Computerbenutzer ist praktisch kein Unterschied zwischen diesen beiden Typen sichtbar.

Auf einem Dell Inspiration-Laptop verwalten Sie die Systemstarteinstellungen auf der Seite *System* im Untermenü *Boot Sequence*. Hier ist die Startreihenfolge folgendermaßen aufgelistet:

1. *Hard disk*
2. *USB hard disk*
3. *CD/DVD*
4. *USB CD/DVD*
5. *USB Floppy*
6. *Network*

Zur Navigation in der Startgeräteleiste dienen die Tasten PFEIL-NACH-OBEN und PFEIL-NACH-UNTEN. Drücken Sie die EINGABETASTE, um einen Eintrag zur Bearbeitung zu öffnen und das Gerät auszuwählen, das an dieser Stelle stehen soll. Um den betreffenden Gerätetyp zu deaktivieren, wählen Sie *Disabled*.

Viele Desktopcomputer werden mit Controllern für Hardware-RAID (Redundant Array of Independent Disks) ausgeliefert. Auf meinem Dell-Computer wird die Option *SATA Operation* des Untermenüs *Drives* verwendet, um den Hardware-RAID-Controller zu aktivieren oder zu deaktivieren. RAID-Controller für Desktopcomputer unterstützen üblicherweise RAID 0 und RAID 1. RAID 0 bietet keinen Schutz für Daten, es erweitert lediglich ein logisches Datenträgervolume über mehrere physische Datenträger. RAID 1 schützt die Daten dadurch, dass sie auf zwei Datenträger gespiegelt werden. Bei dieser Spiegelkonfiguration sehen zwei physische Datenträger wie ein einziger Datenträger aus, wobei beide Datenträger genau dieselben Daten enthalten.

PRAXISTIPP

Ein Computer mit Hardware-RAID-Controller startet vielleicht nicht, wenn eines der Laufwerke, das für den RAID-Betrieb erforderlich ist, aus dem Computer entfernt wird und Hardware-RAID aktiviert bleibt. Sofern das verbleibende Laufwerk startfähig ist, deaktivieren Sie RAID im BIOS und starten dann den Computer erneut, damit das Betriebssystem hochgefahren werden kann.

Problembehebung in der Startphase 3

Nach dem Setup übergibt die Firmwareschnittstelle die Kontrolle an den Startmanager, der dann seinerseits das Startladeprogramm ausführt.

Computer, die ein BIOS haben, lesen Daten aus dem MBR (Master Boot Record). Normalerweise ist der MBR der erste Datensektor auf der Festplatte. Er enthält Startbefehle und eine Partitionstabelle, in der die Festplattenpartitionen definiert sind. Die aktive Partition, auch als Startpartition (engl. boot partition) bezeichnet, enthält ebenfalls Startcode in ihrem ersten Datensektor. Diese Daten liefern Informationen über das Dateisystem auf der Partition, sodass die Firmware in der Lage ist, das Stubprogramm *Bootmgr* im Stammverzeichnis der Startpartition zu finden und zu starten. *Bootmgr* schaltet den Prozess vom Realmodus in den geschützten 32-Bit- oder 64-Bit-Modus um und lädt den 32-Bit- oder 64-Bit-Windows-Start-Manager (der in der Stubdatei selbst liegt). Der Windows-Start-Manager sucht und startet daraufhin das Windows-Startladeprogramm (*Winload*).

Probleme können auftreten, wenn es keine aktive Startpartition gibt oder irgendwelche Startsektordaten fehlen oder beschädigt sind. In diesem Fall erhalten Sie Fehlermeldungen wie:

```
Error loading operating system
```

und

```
Invalid partition table
```

In solchen Fällen können Sie die Funktion oft mit dem Tool Systemstartreparatur wiederherstellen.

Dagegen haben Computer, die mit EFI arbeiten, einen eingebauten Startmanager. Wenn Sie Windows installieren, fügt Windows einen Eintrag zum EFI-Startmanager hinzu. Dieser Eintrag heißt *Windows-Start-Manager* und verweist auf die ausführbare Datei des Startmanagers in der EFI-Systempartition (*\Efi\Microsoft\Boot\Bootmgfw.efi*). Der Startmanager übergibt die Kontrolle an das Windows-Startladeprogramm.

Probleme können auftreten, wenn Sie ein anderes Betriebssystem installieren oder die Einstellungen des EFI-Startmanagers verändern. In vielen Fällen gelingt es, die Funktion mit dem Tool Systemstartreparatur wiederherzustellen. Oft reicht es auch aus, die Einstellungen des EFI-Startmanagers zu ändern.

Problembehebung in der Startphase 4

Das Startladeprogramm greift auf die Systemstartdienste der Firmwareschnittstelle zurück, um den Start des Betriebssystems abzuschließen. Dabei lädt das Startladeprogramm den Betriebssystemkern (*Ntoskrnl.exe*) und dann die HAL (Hardware Abstraction Layer) aus der Datei *Hal.dll*. Anschließend lädt das Startladeprogramm die Registrierungsstruktur *HKEY_LOCAL_MACHINE\System* in den Arbeitsspeicher (aus *%SystemRoot%\System32\Config\System*) und sucht darin im Schlüssel *HKEY_LOCAL_MACHINE\System\Services* nach Gerätetreibern. Es lädt dabei alle Treiber in den Arbeitsspeicher, die für die Systemstartklasse konfiguriert sind.

Sobald das Startladeprogramm die Kontrolle an den Betriebssystemkern übergeben hat, initialisieren Systemkern und HAL den Windows-Executive, der daraufhin die Konfigurationsdaten verarbeitet, die im Zweig *HKEY_LOCAL_MACHINE\System\CurrentControlSet* gespeichert sind, und anschließend die Gerätetreiber und Systemdienste startet. Treiber und Dienste werden entsprechend ihrem Starttyp ausgeführt. Dieser Wert steht im Unterschlüssel *Start* des Zweigs *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\<Name>*, wobei *<Name>* für den Namen des Geräts oder Dienstes steht. Gültige Werte sind 0 (Systemstarttreiber), 1 (Systemtreiber), 2 (automatisch geladener Treiber oder Dienst), 3 (bei Bedarf geladener Treiber oder Dienst), 4 (deaktivierter und nicht gestarteter Treiber oder Dienst) und 5 (verzögert gestarteter Dienst). Treiber werden in folgender Reihenfolge gestartet: Systemstarttrei-

ber, Systemtreiber, automatisch geladene Treiber, bei Bedarf geladene Treiber und ganz zuletzt verzögert gestartete Dienste.

Die meisten Probleme in dieser Phase sind auf ungültige Treiber- und Dienstkonfigurationen zurückzuführen. Manche Treiber und Dienste hängen von anderen Komponenten und Diensten ab. Auch wenn abhängige Komponenten oder Dienste nicht verfügbar oder falsch konfiguriert sind, kann das Startprobleme auslösen.

Während des Systemstarts werden Unterschlüssel von *HKEY_LOCAL_MACHINE\System* ausgewertet, um Geräte und Dienste zu konfigurieren. Der Unterschlüssel *Select* enthält mehrere Werte, die für diese Aufgabe wichtig sind:

- Der Wert *Current* ist ein Zeiger auf den *ControlSet*-Unterschlüssel, in dem die aktuelle Konfiguration für alle Geräte und Dienste definiert ist.
- Der Wert *Default* ist ein Zeiger auf den *ControlSet*-Unterschlüssel, in dem die Konfigurationsdefinition gespeichert ist, die der Computer beim nächsten Systemstart benutzt, sofern kein Fehler auftritt und Sie keine alternative Konfiguration verwenden.
- Der Wert *Failed* ist ein Zeiger auf den *ControlSet*-Unterschlüssel mit einer Konfigurationsdefinition, mit der Windows nicht geladen werden konnte.
- Der Wert *LastKnownGood* ist ein Zeiger auf den *ControlSet*-Unterschlüssel, in dem die Konfiguration definiert ist, die für die letzte erfolgreiche Anmeldung benutzt wurde.

Bei einem normalen Start benutzt der Computer den Konfigurationssatz aus *Default*. Sofern beim Start keine Fehler auftreten und Sie nicht die letzte als funktionierend bekannte Konfiguration auswählen, verweisen die Werte *Default*, *Current* und *LastKnownGood* auf denselben *ControlSet*-Unterschlüssel, zum Beispiel *ControlSet001*. Wenn dagegen beim Start Fehler aufgetreten sind und Sie in den erweiterten Startoptionen die letzte als funktionierend bekannte Konfiguration ausgewählt haben, wird der Eintrag *Failed* so aktualisiert, dass er auf die Konfigurationsdefinition verweist, mit der der Systemstart fehlgeschlagen ist. Wenn der Systemstart erfolgreich war und Sie nicht die letzte als funktionierend bekannte Konfiguration aufgerufen haben, wird in den Wert *LastKnownGood* ein Verweis auf die aktuelle Konfigurationsdefinition eingetragen.

Problembehebung in der Startphase 5

In der abschließenden Phase des Systemstarts führt der Systemkern den Sitzungs-Manager (*Smss.exe*) aus. Der Sitzungs-Manager initialisiert die Systemumgebung, indem er Systemumgebungsvariablen anlegt und das Win32-Subsystem (*Csrss.exe*) startet. An diesem Punkt schaltet Windows die Anzeige vom Textmodus in den Grafikmodus um. Falls die Grafikkarte defekt oder nicht richtig eingebaut ist, zeigt der Computer weder im Text- noch im Grafikmodus etwas an. Ist die Grafikkarte dagegen falsch konfiguriert, macht sich das oft bemerkbar, sobald der Computer in den Grafikmodus umschaltet. Ist die Grafikkarte falsch konfiguriert, kommt es unter Umständen zu Darstellungsfehlern, wie im Abschnitt »Beseitigen von Anzeige Problemen« in Kapitel 3 beschrieben.

Die Bildschirmanzeige ist nur eine von mehreren Komponenten, bei denen sich in dieser späten Phase des Systemstarts unter Umständen Probleme bemerkbar machen. Sollte der Systemstart in dieser Phase fehlschlagen, können Sie die verursachende Komponente mithilfe der Startprotokollierung aufspüren. Tritt in dieser Phase ein Abbruchfehler beim Computer auf, können Sie anhand der Informationen, die in der Abbruchmeldung aufgeführt sind, die Komponente identifizieren.

Der Sitzungs-Manager startet den Windows-Anmelde-Manager (*Winlogon.exe*), der dann seinerseits den Dienststeuerungs-Manager (*Services.exe*) und die lokale Sicherheitsautorität (*Lsass.exe*) startet und war-

tet, bis sich ein Benutzer anmeldet. Sobald sich ein Benutzer anmeldet, führt der Windows-Anmelde-Manager das Programm *Userinit.exe* und die Datei-Explorer-Shell aus. *Userinit.exe* initialisiert die Benutzerumgebung, indem es Benutzerumgebungsvariablen anlegt, Autostartprogramme ausführt und andere wichtige Aufgaben durchführt. Die Datei-Explorer-Shell stellt Desktop, Taskleiste und Menüsystem zur Verfügung.

Falls während oder nach der Anmeldung Startprobleme auftreten, liegt das Problem wahrscheinlich bei einem falsch konfigurierten Dienst oder einer Autostartanwendung. Im Rahmen der Problembehandlung können Sie Dienste und Autostartanwendungen zeitweise deaktivieren, wie im Abschnitt »Verwalten der Systemstartkonfiguration« weiter unten in diesem Kapitel beschrieben.

Verwalten der Systemstartkonfiguration

Während das Betriebssystem startet, können Sie F8 oder F12 drücken, um das Menü *Erweiterte Startoptionen* aufzurufen. In diesem Menü haben Sie die Möglichkeit, einen von verschiedenen erweiterten Startmodi auszuwählen. Diese erweiterten Modi nehmen keine dauerhaften Änderungen an der Systemstartkonfiguration oder dem BCD-Speicher vor. Zu den Tools, mit denen Sie die Systemstartkonfiguration anpassen und den BCD-Speicher verwalten können, gehören das Dialogfeld *Starten und Wiederherstellen*, das Systemkonfigurationsprogramm und der BCD-Editor. Die folgenden Abschnitte beschreiben, wie Sie diese Tools einsetzen.

Einstellen von Start- und Wiederherstellungsoptionen

Das Dialogfeld *Starten und Wiederherstellen* steuert die grundlegenden Optionen für das Betriebssystem während des Systemstarts. Über diese Optionen können Sie festlegen, welches Standardbetriebssystem verwendet wird, wie lange die Liste der verfügbaren Betriebssysteme angezeigt wird und wie lange bei Bedarf die Wiederherstellungsoptionen angezeigt werden. Unabhängig davon, ob Sie einen Computer mit anderen Betriebssystemen starten, sollten Sie diese Einstellungen optimieren, um die Wartezeit während des Systemstarts möglichst kurz zu halten und den Startvorgang zu beschleunigen.

Gehen Sie folgendermaßen vor, um das Dialogfeld *Starten und Wiederherstellen* zu öffnen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*, um das Fenster *System* zu öffnen.
2. Tippen oder klicken Sie im linken Fensterabschnitt des Fensters *System* auf *Erweiterte Systemeinstellungen*, um das Dialogfeld *Systemeigenschaften* anzuzeigen.
3. Tippen oder klicken Sie auf der Registerkarte *Erweitert* des Dialogfelds *Systemeigenschaften* unter *Starten und Wiederherstellen* auf die Schaltfläche *Einstellungen*. Daraufhin öffnet sich das Dialogfeld *Starten und Wiederherstellen* (Abbildung 4.1).
4. Wenn Ihr Computer mehrere Betriebssysteme hat, können Sie in der Dropdownliste *Standardbetriebssystem* auswählen, welches Betriebssystem als Standardeinstellung gestartet wird.
5. Legen Sie fest, wie lange die Betriebssystemliste angezeigt wird, indem Sie das Kontrollkästchen *Anzeigedauer der Betriebssystemliste* aktivieren und die Dauer in der Einheit Sekunden eintragen. Um den Startvorgang zu beschleunigen, können Sie beispielsweise den Wert 5 Sekunden verwenden.
6. Legen Sie fest, wie lange die Liste der Wiederherstellungsoptionen angezeigt wird, indem Sie das Kontrollkästchen *Anzeigedauer der Wiederherstellungsoptionen* aktivieren und die Dauer in der Einheit Sekunden angeben. Auch hier können Sie den Wert 5 Sekunden verwenden, um den Startvorgang zu beschleunigen.

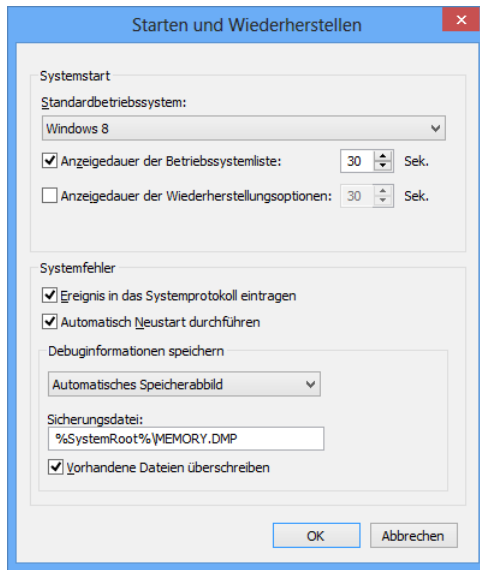


Abbildung 4.1 Konfigurieren der Systemstartoptionen

7. Aktivieren Sie unter *Systemfehler* das Kontrollkästchen *Ereignis in das Systemprotokoll eintragen*, wenn Ereignisse, die mit Systemfehlern zusammenhängen, protokolliert werden sollen. Aktivieren Sie *Automatisch Neustart durchführen*, wenn Sie wollen, dass der Computer nach einem Fehler automatisch neu gestartet wird.
8. Tippen oder klicken Sie auf *OK*, um Ihre Einstellungen zu speichern.

Verwalten der Systemstartkonfiguration

Im Programm *Systemkonfiguration* (*Mscconfig.exe*) können Sie den Startvorgang des Computers in allen Einzelheiten optimieren. Meist setzen Sie dieses Dienstprogramm bei der Problembehandlung und Diagnose ein. Beispielsweise können Sie im Rahmen einer Problembehandlung den Computer so konfigurieren, dass er einen Diagnosestart ausführt, bei dem nur unverzichtbare Geräte und Dienste geladen werden.

In der Systemsteuerung finden Sie das Systemkonfigurationsprogramm unter *System und Sicherheit/Verwaltung*. Sie können es auch starten, indem Sie die WINDOWS-Taste drücken, **msconfig.exe** eingeben (das Wort wird automatisch in das Suchfeld *Apps* eingetragen) und dann die EINGABETASTE drücken. Wie Abbildung 4.2 zeigt, verfügt dieses Hilfsprogramm über einige Registerkarten mit Optionen.

Mit den Optionen der Registerkarte *Allgemein* legen Sie fest, auf welche Weise das System gestartet wird. Dies ist oft der Ausgangspunkt für Problembehandlung und Diagnose. Mit diesen Optionen können Sie auswählen, ob ein normaler Systemstart, ein Diagnosesystemstart oder ein benutzerdefinierter Systemstart ausgeführt wird. Starten Sie nun den Computer neu und beseitigen Sie die Probleme. Anschließend öffnen Sie das Systemkonfigurationsprogramm wieder, wählen auf der Registerkarte *Allgemein* die Option *Normaler Systemstart* und tippen oder klicken auf *OK*.

Mit den Optionen auf der Registerkarte *Start* legen Sie fest, wie die verschiedenen Prozesse des Startvorgangs arbeiten. Sie können den Computer so konfigurieren, dass er in einem der sicheren Systemstartmodi hochfährt, und zusätzliche Optionen einstellen, zum Beispiel *Kein GUI-Start*. Sollten Sie nach der Problembehandlung feststellen, dass Sie diese Einstellungen beibehalten wollen, können Sie das Kontroll-

kästchen *Starteinstellungen sollen immer gelten* aktivieren, um die Einstellungen im Eintrag der Systemstartkonfiguration zu speichern.

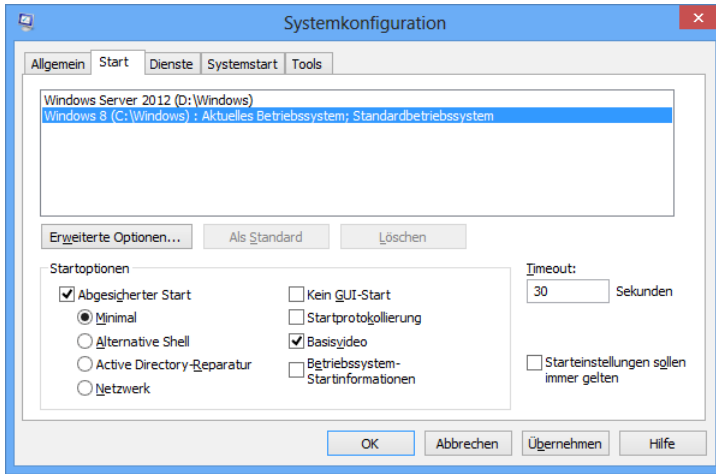


Abbildung 4.2 Das Systemkonfigurationsprogramm ist nützlich für die Problembehandlung

Wenn Sie auf der Registerkarte *Start* auf die Schaltfläche *Erweiterte Optionen* tippen oder klicken, wird das Dialogfeld *Erweiterte Startoptionen* geöffnet (Abbildung 4.3). Hier können Sie die Kontrollkästchen *PCI Lock* und *Debug* aktivieren und außerdem folgende erweiterte Optionen einstellen:

- Festlegen, wie viele Prozessoren das Betriebssystem benutzen soll. Dabei ist es egal, ob es sich bei den Prozessoren um separate CPUs in eigenen Sockeln oder Kerne innerhalb einer Mehrkern-CPU handelt. Diese Möglichkeit sollten Sie nutzen, wenn Sie vermuten, dass ein Problem durch die zusätzlich verfügbaren Prozessoren ausgelöst wird, und feststellen wollen, ob das Problem tatsächlich mit der Mehrprozessorkonfigurationen oder der Parallelausführung zu tun hat. Sehen wir als Beispiel einen Computer an, der eine CPU mit vier Prozessorkernen enthält. Eine selbstentwickelte Anwendung, die im Unternehmen für die Inventarverwaltung eingesetzt wird, ist sehr langsam, wenn sie auf diesem Computer läuft. Auf Computern, die nur einen einzigen Prozessorkern haben, ist die Geschwindigkeit dagegen völlig ausreichend. Sie konfigurieren den Computer nun so, dass er nur mit einem Prozessor startet, und stellen fest, dass sich die Leistung der Anwendung verbessert. Sie aktivieren wieder alle Prozessoren und melden dem Softwareentwicklungsteam, dass die Anwendung bei der Parallelausführung auf mehreren Prozessorkernen Schwächen zeigt.
- Einstellen der Höchstmenge des Arbeitsspeichers, der vom Betriebssystem benutzt wird. Verwenden Sie diese Einstellmöglichkeit, wenn Sie den Verdacht haben, dass ein Problem durch zusätzlichen Arbeitsspeicher verursacht wird, den Sie in einem Computer installiert haben. Auch hier wieder ein Beispiel: Ein Computer hatte bei der Auslieferung 8 GByte RAM, später haben Sie ihn mit weiteren 8 GByte RAM aufgerüstet. Nun stellt sich heraus, dass der Computer nicht mehr startet. Sie können das neue RAM als Fehlerursache ausschließen, indem Sie den Computer auf 8.192 MByte Arbeitsspeicher beschränken.

Wenn Sie vermuten, dass die Dienste, die auf einem Computer installiert sind, Startprobleme verursachen, können Sie das schnell überprüfen, indem Sie auf der Registerkarte *Allgemein* den Diagnose- oder benutzerdefinierten Systemstart auswählen. Stellen Sie dabei fest, dass tatsächlich bestimmte Dienste die Startprobleme verursachen, können Sie diese Dienste zeitweise auf der Registerkarte *Dienste* deaktivieren und den Computer dann neu starten, um zu prüfen, ob das Problem damit beseitigt ist. Ist das der Fall, haben

Sie die Ursache wahrscheinlich gefunden. Sie können den Dienst nun dauerhaft deaktivieren oder beim Hersteller des Dienstes nachfragen, ob eine aktualisierte Version verfügbar ist. Sie deaktivieren einen Dienst, indem Sie das zugehörige Kontrollkästchen auf der Registerkarte *Dienste* ausschalten.

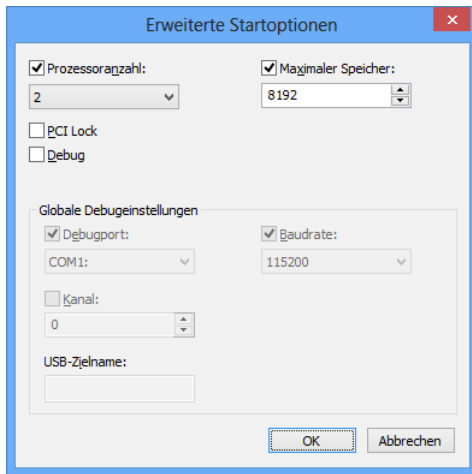


Abbildung 4.3 Die erweiterten Startoptionen helfen bei der Lösung bestimmter Probleme

Auch wenn Sie vermuten, dass Anwendungen, die beim Systemstart automatisch ausgeführt werden, Probleme verursachen, können Sie das schnell überprüfen, indem Sie auf der Registerkarte *Systemstart* auf *Task-Manager öffnen* tippen oder klicken. Sie deaktivieren eine Autostartanwendung, indem Sie die Anwendung auf der Registerkarte *Autostart* auswählen und dann auf *Deaktivieren* tippen oder klicken. Tritt das Problem anschließend nicht mehr auf, haben Sie wahrscheinlich die Ursache aufgespürt. Anschließend können Sie die Autostartanwendung dauerhaft deaktivieren oder beim Softwarehersteller nachfragen, ob er eine aktualisierte Version anbietet.

Wenn Sie das Systemkonfigurationsprogramm für Problembehandlung und Diagnose einsetzen, dürfen Sie nicht vergessen, die ausgewählten Startoptionen später wieder zu entfernen. Öffnen Sie dazu wieder das Programm *Systemkonfiguration*, nachdem Sie den Computer neu gestartet und alle Probleme beseitigt haben, stellen Sie die ursprünglichen Einstellungen wieder her und tippen oder klicken Sie auf *OK*.

Arbeiten mit dem BCD-Editor

Der BCD-Speicher enthält mehrere Einträge. Auf einem BIOS-basierten Computer finden Sie folgende Einträge:

- Einen Eintrag für den Windows-Start-Manager. Es gibt nur einen Startmanager, daher ist auch nur ein entsprechender Eintrag vorhanden.
- Einen oder mehrere Einträge für das Windows-Startladeprogramm. Es gibt jeweils einen Eintrag für jede Instanz von Windows 8, Windows 7 oder Windows Vista, die auf dem Computer installiert ist. Wenn Sie Windows Server 2008 oder höher installiert haben, gibt es auch für jede dieser Installationen Einträge.

Auf einem Computer mit anderen Betriebssystemen gibt es zusätzlich diese Einträge:

- Ein Eintrag für ein Legacy-Betriebssystem. Der Legacy-Eintrag verweist nicht auf eine Startanwendung. Er dient dazu, *Ntldr* und *Boot.ini* aufzurufen, um Windows XP oder älter zu starten. Wenn es auf dem Computer mehrere Instanzen von Windows XP oder älter gibt, können Sie das gewünschte Betriebssystem auswählen, nachdem Sie den Menüeintrag für das Legacy-Betriebssystem gewählt haben.

Der Windows-Start-Manager ist selbst ein Startladeprogramm. Daneben gibt es weitere Startladeprogramme, zum Beispiel:

- Ladeprogramm für Legacy-Betriebssysteme, eingetragen als *Ntldr*
- Lader für Windows Vista oder neuere Betriebssysteme, eingetragen als *Osloader*
- Windows-Startsektor Anwendung, eingetragen als *Bootsector*
- Firmware-Startmanager, eingetragen als *Fwbootmgr*
- Windows-Ladeprogrammfortsetzung, eingetragen als *Resume*

Sie können den BCD-Speicher im BCD-Editor (*Bcdedit.exe*) ansehen und bearbeiten. Der BCD-Editor ist ein Befehlszeilenprogramm. Gehen Sie folgendermaßen vor, um sich die Einträge im BCD-Speicher mit dem BCD-Editor anzusehen:

1. Geben Sie im Suchfeld *Apps* **Cmd.exe** ein. Dazu können Sie zum Beispiel die WINDOWS-Taste drücken und dann **Cmd.exe** eingeben.
2. Klicken Sie mit der rechten Maustaste auf *Eingabeaufforderung* oder halten Sie das Symbol gedrückt und wählen Sie den Befehl *Als Admin ausführen*.
3. Geben Sie in der Eingabeaufforderung **bcdedit** ein.

Tabelle 4.3 fasst die Befehle zusammen, die Sie verwenden können, wenn Sie mit dem BCD-Speicher arbeiten. Diese Befehle ermöglichen folgende Aktionen:

- Erstellen, Importieren, Exportieren und Identifizieren des gesamten BCD-Speichers
- Erstellen, Löschen und Kopieren einzelner Einträge im BCD-Speicher
- Ändern oder Löschen der Werte eines Eintrags im BCD-Speicher
- Steuern der Systemstartreihenfolge und des Startmanagers
- Konfigurieren und Steuern der Notfallverwaltungsdienste (Emergency Management Services, EMS)
- Konfigurieren und Steuern des Systemstartdebuggers und des Hypervisordebuggers

Verwalten des BCD-Speichers

Der BCD-Editor ist ein leistungsfähiges Befehlszeilentool, mit dem Sie die Konfiguration der Startumgebung, die vor dem Betriebssystem ausgeführt wird, anzeigen und bearbeiten können. In den folgenden Abschnitten erkläre ich zwar, wie Sie den BCD-Speicher verändern, aber Sie sollten das nur versuchen, wenn Sie IT-Experte mit ausreichender Erfahrung auf diesem Gebiet sind. Zur Sicherheit sollten Sie auf jeden Fall eine vollständige Datensicherung des Computers anlegen, bevor Sie irgendwelche Änderungen am BCD-Speicher vornehmen. Warum? Wenn Sie einen Fehler machen, lässt sich Ihr Computer unter Umständen gar nicht mehr starten, sodass Ihnen nur die Möglichkeit der Wiederherstellung bleibt.

Tabelle 4.3 Befehle für den BCD-Editor

Befehl	Beschreibung
<code>/bootdebug</code>	Aktiviert oder deaktiviert das Systemstartdebugging für eine Startanwendung.
<code>/bootems</code>	Aktiviert oder deaktiviert die Notfallverwaltungsdienste für eine Startanwendung.
<code>/bootsequence</code>	Legt die einmalige Startreihenfolge für den Startmanager fest.
<code>/copy</code>	Kopiert Einträge im Speicher.
<code>/create</code>	Erstellt neue Einträge im Speicher.
<code>/createstore</code>	Erstellt einen neuen (leeren) Startkonfigurationsdatenspeicher.
<code>/dbgsettings</code>	Legt die globalen Debugparameter fest.
<code>/debug</code>	Aktiviert oder deaktiviert das Kerneldebugging für einen Betriebssystemeintrag.
<code>/default</code>	Legt den Standardeintrag fest, den der Startmanager benutzt.
<code>/delete</code>	Löscht Einträge aus dem Speicher.
<code>/deletevalue</code>	Löscht Eintragsoptionen aus dem Speicher.
<code>/displayorder</code>	Legt fest, in welcher Reihenfolge der Startmanager die Einträge des Startmenüs anzeigt.
<code>/ems</code>	Aktiviert oder deaktiviert die Notfallverwaltungsdienste für einen Betriebssystemeintrag.
<code>/emssettings</code>	Legt die globalen Parameter für die Notfallverwaltungsdienste fest.
<code>/enum</code>	Listet die Einträge im Speicher auf.
<code>/export</code>	Exportiert den Inhalt des Systemspeichers in eine Datei. Diese Datei kann später benutzt werden, um den Zustand des Systemspeichers wiederherzustellen.
<code>/hypervisorsettings</code>	Legt die Parameter für den Hypervisor fest.
<code>/import</code>	Stellt den Zustand des Systemspeichers aus einer Sicherungsdatei wieder her, die mit dem Befehl <code>/export</code> erstellt wurde.
<code>/mirror</code>	Erstellt eine gespiegelte Version der Einträge im Speicher.
<code>/set</code>	Legt Eintragsoptionswerte im Speicher fest.
<code>/store</code>	Gibt den BCD-Speicher an, der verwendet werden soll. Fehlt diese Angabe, wird der Systemspeicher verwendet.
<code>/sysstore</code>	Legt das Systemspeichergerät fest. Diese Einstellung wirkt sich nur auf EFI-Systeme aus.
<code>/timeout</code>	Legt das Zeitlimit für den Startmanager fest.
<code>/toolsdisplayorder</code>	Legt fest, in welcher Reihenfolge der Startmanager die Einträge des Toolmenüs anzeigt.
<code>/v</code>	Aktiviert die Ausgabe ausführlicher Meldungen.

Anzeigen von BCD-Einträgen

Ein Computer kann einen System- und einen Nicht-System-BCD-Speicher haben. Der System-BCD-Speicher enthält die Starteinträge für Betriebssysteme und die zugehörigen Systemstarteinstellungen. Wenn Sie den BCD-Editor benutzen, arbeiten Sie immer mit diesem System-BCD-Speicher.

Auf einem Computer, der nur ein einziges Betriebssystem hat, sehen die BCD-Einträge ähnlich aus wie in Listing 4.1. Wie das Listing zeigt, enthält der BCD-Speicher des Beispielcomputers zwei Einträge: einen für den Windows-Start-Manager und einen für das Windows-Startladeprogramm. In diesem Fall ruft der Windows-Start-Manager das Startladeprogramm auf, und das Startladeprogramm seinerseits *Winload.exe*, um Windows 8 zu starten.

Listing 4.1 Einträge im BCD-Speicher auf einem Computer mit einem einzigen Betriebssystem

```

Windows Boot Manager
-----
identifizier      {bootmgr}
device            partition=\Device\HarddiskVolume1
description       Windows Boot Manager
locale            en-US
inherit           {globalsettings}
integrityservices Enable
default           {current}
resumeobject      {16b857b4-9e02-11e0-9c17-b7d085eb0682}
displayorder      {current}
                  {16b857ad-9e02-11e0-9c17-b7d085eb0682}
toolsdisplayorder {memdiag}
timeout           30
custom:26000025   Yes

Windows Boot Loader
-----
identifizier      {current}
device            partition=C:
path              \Windows\system32\winload.exe
description       Windows 8
locale            en-US
inherit           {bootloadersettings}
recoverysequence  {16b857b6-9e02-11e0-9c17-b7d085eb0682}
integrityservices Enable
recoveryenabled   Yes
allowedinmemorysettings 0x15000075
osdevice          partition=C:
systemroot        \Windows
resumeobject      {16b857b4-9e02-11e0-9c17-b7d085eb0682}
nx                OptIn
bootmenupolicy    Standard

```

Die BCD-Einträge für den Windows-Start-Manager und das Windows-Startladeprogramm haben ähnliche Eigenschaften. Tabelle 4.4 fasst diese Eigenschaften zusammen.

Wenn Sie mit dem BCD-Speicher und dem BCD-Editor arbeiten, finden Sie Verweise auf bekannte Kennungen, die in Tabelle 4.5 aufgelistet sind, und auf GUIDs. Wird eine GUID benutzt, hat sie folgendes Format, wobei jedes N für eine Hexadezimalziffer steht:

```
{NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN}
```

Ein Beispiel:

```
{16b857ad-9e02-11e0-9c17-b7d085eb0682}
```

Die Bindestriche, mit denen die verschiedenen Abschnitte der GUID voneinander getrennt werden, müssen an den gezeigten Stellen eingefügt werden. Sowohl bekannte Kennungen als auch GUIDs sind in geschweifte Klammern eingeschlossen.

Tabelle 4.4 Eigenschaften von BCD-Einträgen

Eigenschaft	Beschreibung
Description	Eine aussagekräftige Beschreibung, die dabei hilft, den Eintragstyp zu interpretieren
Device	Der Pfad des Geräts. Bei einer Partition auf einer physischen Festplatte lautet dieser Eintrag beispielsweise <i>partition=C:</i> .
FileDevice	Der Pfad zu einem Dateigerät, zum Beispiel <i>partition=C:</i>
FilePath	Der Dateipfad zu einer benötigten Datei, zum Beispiel <i>\Hiberfil.sys</i>
Identifier	Eine Kennung für den Eintrag. Dies kann ein Startladeprogramm sein, zum Beispiel <i>Bootmgr</i> oder <i>Ntldr</i> , ein Verweis auf den aktuellen Betriebssystemeintrag oder die GUID (Globally Unique Identifier) eines bestimmten Objekts. Tabelle 4.5 listet einige bekannte Kennungen auf.
Inherit	Die Liste der Einträge, die durch Vererbung übernommen werden
Locale	Die Gebietsschemaeinstellung des Computers, zum Beispiel <i>de-DE</i> . Die Gebietsschemaeinstellung legt fest, welche Sprache in der Benutzeroberfläche (User Interface, UI) verwendet wird. Der Ordner <i>\Boot</i> enthält Unterordner für jedes unterstützte Gebietsschema, und jeder dieser Unterordner enthält die sprachspezifischen UI-Elemente für den Windows-Start-Manager und das Dienstprogramm Windows-Speicherdiagnose (<i>Memdiag.exe</i>).
OsDevice	Der Pfad zum Betriebssystemgerät, zum Beispiel <i>partition=C:</i>
Path	Der tatsächliche Dateipfad zum Startladeprogramm, beispielsweise <i>\Windows\System32\Winload.exe</i>

Sind auf einem Computer weitere Instanzen von Windows Vista oder höher installiert, enthält der BCD-Speicher für jedes dieser zusätzlichen Betriebssysteme weitere Einträge. Zum Beispiel enthält der BCD-Speicher zu jedem Betriebssystem jeweils einen Eintrag für den Windows-Start-Manager und einen Eintrag für das Windows-Startladeprogramm.

Ist auf einem Computer ein älteres Betriebssystem installiert, beispielsweise Windows XP, enthält der BCD-Speicher drei Einträge: einen für den Windows-Start-Manager, einen für das Windows-Legacybetriebssystem-Ladeprogramm und einen für das Windows-Startladeprogramm. Der Eintrag für das Windows-Legacybetriebssystem-Ladeprogramm sieht meist ähnlich wie in Listing 4.2 aus.

Windows-Start-Manager, Windows-Legacybetriebssystem-Ladeprogramm und Windows-Startladeprogramm sind zwar die wichtigsten Eintragstypen für den Systemstart, der BCD-Speicher enthält aber auch Informationen über Systemstarteinstellungen und Dienstprogramme für den Systemstart. Der Eintrag für das Windows-Startladeprogramm kann Parameter umfassen, die den Status der Systemstarteinstellungen festlegen, beispielsweise ob die NX-Richtlinie (No Execute) aktiviert oder deaktiviert ist. Außerdem kann der Eintrag des Windows-Startladeprogramms Informationen über die verfügbaren Systemstart-Dienstprogramme enthalten, etwa die Windows-Speicherdiagnose.

Sie brauchen die tatsächlichen Werte der GUIDs, um Einträge im BCD-Speicher zu verändern. Diese Werte ermitteln Sie, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten `bcdedit /v` eingeben.

Listing 4.2 Beispieleintrag für das Legacybetriebssystem-Ladeprogramm

```
Windows-Legacybetriebssystem-Ladeprogramm
-----
identifizier:      {ntldr}
device:           partition=C:
path:             \ntldr
description:      Frühere Windows-Version
```

Tabelle 4.5 Bekannte Kennungen

Kennung	Beschreibung
<i>{badmemory}</i>	Enthält die globale RAM-Defektliste, die an jeden Startanwendungseintrag vererbt werden kann.
<i>{bootloadersettings}</i>	Enthält die Sammlung der globalen Einstellungen, die an alle Einträge für das Windows-Startladeprogramm vererbt werden sollen.
<i>{bootmgr}</i>	Verweist auf den Eintrag des Windows-Start-Managers.
<i>{current}</i>	Eine virtuelle Kennung, die für den Betriebssystem-Starteintrag für das momentan laufende Betriebssystem steht
<i>{dbgsettings}</i>	Enthält die globalen Debuggereinstellungen, die an jeden Startanwendungseintrag vererbt werden können.
<i>{default}</i>	Eine virtuelle Kennung, die für den Eintrag des Standardstartmanagers steht
<i>{emssettings}</i>	Enthält die Einstellungen für die globalen Notfallverwaltungsdienste, die an jeden Startanwendungseintrag vererbt werden können.
<i>{fwbootmgr}</i>	Der Eintrag für den Firmware-Startmanager. Dieser Eintrag wird auf EFI-Systemen benutzt.
<i>{globalsettings}</i>	Die Sammlung der globalen Einstellungen, die an alle Startanwendungseinträge vererbt werden sollen
<i>{hypervisorsettings}</i>	Die Hypervisoreinstellungen, die an jeden Betriebssystemladereintrag vererbt werden können
<i>{memdiag}</i>	Der Anwendungseintrag für die Speicherdiagnose
<i>{ntldr}</i>	Das Windows-Legacybetriebssystem-Ladeprogramm (<i>Ntldr</i>), mit dem ältere Windows-Betriebssysteme als Windows Vista gestartet werden.
<i>{ramdiskoptions}</i>	Enthält die zusätzlichen Optionen, die der Startmanager für RAM-Laufwerksgeräte benötigt.
<i>{resumeloadersettings}</i>	Enthält die Sammlung der globalen Einstellungen, die an alle Anwendungseinträge vererbt werden sollen, mit denen Windows aus dem Ruhezustand aufgeweckt wird.

Erstellen und Auswählen des BCD-Speichers

Sie können im BCD-Editor einen Nicht-System-BCD-Speicher anlegen, indem Sie den folgenden Befehl ausführen:

```
bcdedit /createstore Speicherpfad
```

Dabei ist *Speicherpfad* der Ordnerpfad des Speicherorts, in dem Sie den Nicht-System-Speicher erstellen wollen, zum Beispiel:

```
bcdedit /createstore c:\non-sys\bcd
```

Auf einem EFI-System können Sie das Systemspeichergerät mit dem Befehl */sysstore* zeitweise umstellen. Verwenden Sie dazu folgende Syntax:

```
bcdedit /sysstore Speichergerät
```

Dabei steht *Speichergerät* für die Gerätekennung des tatsächlichen Systemspeichers. Ein Beispiel:

```
bcdedit /sysstore c:
```

Das Gerät muss eine Systempartition sein. Beachten Sie, dass diese Einstellung nicht über mehrere Neustarts hinweg erhalten bleibt; sie wird nur benutzt, wenn das Systemspeichergerät nicht eindeutig definiert ist.

Importieren und Exportieren des BCD-Speichers

Der BCD-Editor stellt getrennte Befehle zum Importieren und Exportieren des BCD-Speichers bereit. Mit dem Befehl `/export` exportieren Sie eine Kopie des System-BCD-Speichers in den angegebenen Ordner. Verwenden Sie die folgende Befehlssyntax:

```
bcdedit /export Speicherpfad
```

Dabei ist *Speicherpfad* der tatsächliche Ordnerpfad, in den Sie die Kopie des Systemspeichers exportieren wollen. Ein Beispiel:

```
bcdedit /export c:\backup\bcd
```

Mit dem Befehl `/import` stellen Sie eine vorher exportierte Kopie des Systemspeichers wieder her. Verwenden Sie dazu folgende Befehlssyntax:

```
bcdedit /import Importpfad
```

wobei *Importpfad* der tatsächliche Ordnerpfad ist, aus dem Sie den Systemspeicher importieren. Wiederrum ein Beispiel:

```
bcdedit /import c:\backup\bcd
```

Auf einem EFI-System können Sie `/clean` zum Befehl `/import` hinzufügen, um festzulegen, dass alle vorhandenen Firmwarestarteinträge gelöscht werden sollen. Hier ein Beispiel:

```
bcdedit /import c:\backup\bcd /clean
```

Erstellen, Kopieren und Löschen von BCD-Einträgen

Der BCD-Editor kennt mehrere Befehle zum Erstellen, Kopieren und Löschen von Einträgen im BCD-Speicher. Mit dem Befehl `/create` erstellen Sie Kennungs-, Anwendungs- und Vererbungseinträge im BCD-Speicher.

Wie in Tabelle 4.5 weiter oben beschrieben, kennt der BCD-Editor viele bekannte Kennungen, darunter `{dbgsettings}`, mit der ein Eintrag für Debuggereinstellungen erstellt wird, `{ntldr}` zum Erstellen eines Eintrags für ein älteres Windows-Betriebssystem und `{ramdiskoptions}` für einen Eintrag mit zusätzlichen Optionen für ein RAM-Laufwerk. Sie erstellen Kennungseinträge mit folgender Syntax:

```
bcdedit /create Kennung /d "Beschreibung"
```

Dabei steht *Kennung* für eine bekannte Kennung des Eintrags, den Sie erstellen wollen. Ein Beispiel:

```
bcdedit /create {ntldr} /d "Ladeprogramm für älteres Windows-Betriebssystem"
```

Sie können auch Einträge für bestimmte Startladeprogrammanwendungen erstellen, beispielsweise:

- **Bootsector** Eine Realmodus-Startsektoranwendung. Wird benutzt, um den Startsektor für eine Realmodus-Anwendung festzulegen.
- **Osloader** Eine Betriebssystemladeranwendung. Wird benutzt, um Windows Vista oder neuer zu laden.
- **Resume** Eine Anwendung für die Windows-Ladeprogrammfortsetzung. Wird benutzt, um das Betriebssystem aus dem Ruhezustand aufzuwecken.
- **Startup** Eine Realmodus-Anwendung. Wird benutzt, um eine Realmodus-Anwendung auszuwählen.

Verwenden Sie die folgende Befehlssyntax:

```
bcdedit /create /application Anwendungstyp /d "Beschreibung"
```

wobei *Anwendungstyp* einer der vorher aufgelisteten Anwendungstypen ist. Ein vollständiges Beispiel:

```
bcdedit /create /application osloader /d "Windows Vista"
```

Sie können Einträge im Systemspeicher mit dem Befehl */delete* und der folgenden Syntax löschen:

```
bcdedit /delete Kennung
```

Wenn Sie versuchen, eine bekannte Kennung zu löschen, müssen Sie das Argument */f* angeben, um das Löschen zu erzwingen:

```
bcdedit /delete {ntldr} /f
```

Die Option */cleanup* wird bei der Verwendung des Befehls */delete* automatisch verwendet. Das bedeutet, dass der BCD-Editor auch alle anderen Verweise auf den gelöschten Eintrag entfernt. So ist sichergestellt, dass der Datenspeicher keine ungültigen Verweise auf eine gelöschte Kennung enthält. Weil die Einträge auch aus der Anzeigereihenfolge entfernt werden, führt das unter Umständen dazu, dass ein anderes Standardbetriebssystem eingestellt ist. Wenn Sie den Eintrag löschen und dabei alle Verweise außer dem Eintrag für die Anzeigereihenfolge automatisch entfernen wollen, können Sie das Argument */nocleanup* verwenden.

Einstellen der Werte von BCD-Einträgen

Sobald Sie einen Eintrag erstellt haben, müssen Sie ihm die zugehörigen Optionswerte zuweisen. Die grundlegende Syntax zum Festlegen von Werten lautet:

```
bcdedit /set Kennung Option Wert
```

Dabei sind *Kennung* die Kennung des Eintrags, der geändert werden soll, *Option* die Option, die Sie festlegen wollen, und *Wert* der gewünschte Optionswert. Ein Beispiel:

```
bcdedit /set {current} device partition=d:
```

Sie können Optionen und ihre Werte wieder löschen, indem Sie den Befehl */deletevalue* mit dieser Syntax aufrufen:

```
bcdedit /deletevalue Kennung Option
```

Dabei stehen *Kennung* für die Kennung des Eintrags, der geändert werden soll, und *Option* für die Option, die Sie löschen wollen. Hier ein Beispiel:

```
bcdedit /deletevalue {current} badmemorylist
```

Wenn Sie mit Optionen arbeiten, haben Sie mehrere Möglichkeiten, boolesche Werte einzugeben. Für *True* können Sie *1*, *On*, *Yes* oder *True* angeben, und für *False* die Angaben *0*, *Off*, *No* oder *False*. Wenn Sie in einer Eingabeaufforderung mit erhöhten Rechten **bcdedit /enum all /v** ausführen, werden die BCD-Einträge für alle Systemstartdienstprogramme und die zugehörigen Werte der Einstellungen angezeigt. Dieser Befehl listet alle BCD-Einträge unabhängig von ihrem aktuellen Status auf; die Einträge werden dabei im ausführlichen Modus ausgegeben. Jeder dieser zusätzlichen Einträge hat eine ganz bestimmte Aufgabe und listet die Werte auf, die Sie ändern können. Wichtige Einträge sind:

- **Wiederaufnahme aus dem Ruhezustand** Der Eintrag *Wiederaufnahme aus dem Ruhezustand* zeigt die aktuelle Konfiguration für das Aufwecken des Computers aus dem Ruhezustand an. Das Dienstprogramm, das vor dem Betriebssystem gestartet wird und das Fortsetzen des Betriebssystems steuert, ist *Winresume.exe*. In diesem Beispiel liegt es im Ordner *C:\Windows\System32*. Die Ruhezustandsdaten sind, wie im Parameter *FilePath* festgelegt, in der Datei *Hiberfil.sys* im Stammordner von *OS-Device* (hier in *C:*) gespeichert. Weil das Aufwachen aus dem Ruhezustand anders funktioniert, wenn beim Computer PAE (Physical Address Extension) und Debugging aktiviert sind, werden diese Optionen über die Parameter *Pae* und *DebugOptionEnabled* berücksichtigt.

- **Windows-Speichertestprogramm** Der Eintrag *Windows-Speichertestprogramm* zeigt die aktuelle Konfiguration für das Dienstprogramm Windows-Speicherdiagnose. Als Dienstprogramm für die Speicherdiagnose wird *Memtest.exe* vor dem Betriebssystem gestartet. Weil die Windows-Speicherdiagnose dazu dient, defekten Arbeitsspeicher aufzuspüren, ist der Parameter *BadMemoryAccess* standardmäßig auf *Yes* gesetzt. Sie können diese Funktion ausschalten, indem Sie **bcdedit /set {memdiag} badmemoryaccess NO** eingeben. In der Speicherdiagnose können Sie die Zahl der Durchgänge mit *Passcount* festlegen und die Testmischung im Parameter *Testmix* als *Basic* oder *Extended* einstellen. Hier ein Beispiel: **bcdedit /set {memdiag} passcount 2 testmix basic**.
- **Windows-Legacybetriebssystem-Ladeprogramm** Der Eintrag *Windows-Legacybetriebssystem-Ladeprogramm* zeigt die aktuelle Konfiguration für das Laden älterer Windows-Versionen an. Der Parameter *Device* legt fest, welche Standardpartition benutzt wird (beispielsweise C:), und der Parameter *Path* enthält den Standardpfad zum Ladeprogramm, etwa *Ntldr*.
- **EMS-Einstellungen** Der Eintrag *EMS-Einstellungen* zeigt die Konfiguration an, die beim Starten der Notfallverwaltungsdienste verwendet wird. Die einzelnen Einträge des Windows-Startladeprogramms legen jeweils fest, ob die Notfallverwaltungsdienste aktiviert sind. Wenn das BIOS Notfallverwaltungsdienste zur Verfügung stellt und Sie die BIOS-Einstellungen benutzen wollen, können Sie **bcdedit /emssettings bios** eingeben. Sie können auch einen Port und eine Baudrate für die Notfallverwaltungsdienste festlegen. Hier ein Beispiel: **bcdedit /emssettings EMSPORT:2 EMSBAUDRATE:115200**. Sie aktivieren oder deaktivieren die Notfallverwaltungsdienste für eine Startanwendung, indem Sie nach der Kennung der Startanwendung das Argument */bootems* angeben, gefolgt vom gewünschten Modus, also *On* oder *Off*.
- **Debuggereinstellungen** Der Eintrag *Debuggereinstellungen* zeigt die Konfiguration, die verwendet wird, wenn das System bei aktiviertem Debugger gestartet wird. Die einzelnen Einträge des Windows-Startladeprogramms legen jeweils fest, ob der Debugger aktiviert ist. Sie können sich die Hypervisor-Debuggereinstellungen ansehen, indem Sie **bcdedit /dbgsettings** eingeben. Ist der Debuggerstart aktiviert, legt *DebugType* den Typ des Debuggers als *SERIAL*, *1394* oder *USB* fest. Bei der Einstellung *SERIAL* gibt *DebugPort* an, welche serielle Schnittstelle als Debuggerport verwendet wird, und *BaudRate* legt die Baudrate für die Debugsitzung fest. Ist die Einstellung *1394* ausgewählt, können Sie über *Channel* den Debuggerkanal festlegen. Und bei der Einstellung *USB* können Sie mit *TargetName* den USB-Zielnamen eintragen, der für das Debuggen verwendet wird. Bei allen Debuggertypen können Sie mit dem Argument */Noumex* festlegen, dass Benutzermodusausnahmen ignoriert werden. Hier einige Beispiele, wie Sie den Debugmodus einstellen:


```
bcdedit /dbgsettings SERIAL DEBUGPORT:1 BAUDRATE:115200
bcdedit /dbgsettings 1394 CHANNEL:23
bcdedit /dbgsettings USB TARGETNAME:DEBUGGING
```
- **Hypervisoreinstellungen** Der Eintrag *Hypervisoreinstellungen* zeigt die Konfiguration an, die verwendet wird, wenn der Hypervisor bei eingeschaltetem Debugger benutzt wird. Die einzelnen Einträge des Windows-Startladeprogramms legen jeweils fest, ob der Debugger aktiviert ist. Sie können sich die Hypervisor-Debuggereinstellungen ansehen, indem Sie **bcdedit /hypervisorsettings** eingeben. Wenn der Start mit Hypervisordebugging aktiviert ist, legt der Parameter *HypervisorDebugType* den Typ des Debuggers fest, der Parameter *HypervisorDebugPort* die serielle Schnittstelle, die als Debuggerport benutzt wird, und *HypervisorBaudRate* die Baudrate für die Debuggersitzung. Diese Parameter funktionieren genauso wie bei den Debuggereinstellungen. Ein Beispiel: **bcdedit /hypervisorsettings SERIAL DEBUGPORT:1 BAUDRATE:115200**. Sie können den Hypervisordebugger auch über FireWire steuern. In diesem Fall müssen Sie den Parameter *CHANNEL* mit einem Doppelpunkt von der verwendeten Kanalnummer trennen: **bcdedit /hypervisorsettings 1394 CHANNEL:23**.

Tabelle 4.6 fasst wichtige Optionen zusammen, die für Startanwendungseinträge (Bootapp) gelten. Weil Windows-Start-Manager, Windows-Speicherdiagnose, Windows-Betriebssystemlader und Windows-Ladeprogrammfortsetzung Startanwendungen sind, gelten diese Optionen auch für die entsprechenden Einträge.

Tabelle 4.7 fasst wichtige Optionen zusammen, die in Einträgen für Windows-Betriebssystemlader-Anwendungen (Osloader) zur Verfügung stehen.

Tabelle 4.6 Wichtige Optionen für Startanwendungseinträge

Option	Beschreibung
<i>BadMemoryAccess</i>	Wenn dieser Wert <i>True</i> ist, darf eine Anwendung Arbeitsspeicher verwenden, der in der Liste des defekten Arbeitsspeichers aufgeführt ist. Ist der Wert dagegen <i>False</i> , wird verhindert, dass Anwendungen auf Arbeitsspeicher zugreifen, der in der Liste des defekten Arbeitsspeichers aufgeführt ist.
<i>BadMemoryList</i>	Eine Liste mit den Nummern der defekten Seitenrahmen im Arbeitsspeicher des Systems
<i>BaudRate</i>	Eine Zahl, mit der die Baudrate für den seriellen Debugger eingestellt wird
<i>BootDebug</i>	Ein boolescher Wert, der den Systemstartdebugger aktiviert oder deaktiviert
<i>BootEMS</i>	Ein boolescher Wert, der die Notfallverwaltungsdienste aktiviert oder deaktiviert
<i>Channel</i>	Ein Integerwert, der den Kanal für den 1394-Debugger festlegt.
<i>ConfigAccessPolicy</i>	Legt die Zugriffsrichtlinie auf <i>DEFAULT</i> oder <i>DISALLOWMMCONFIG</i> fest.
<i>DebugAddress</i>	Ein Integerwert, der die Adresse einer seriellen Schnittstelle für den Debugger angibt
<i>DebugPort</i>	Ein Integerwert, der die Nummer einer seriellen Schnittstelle für den seriellen Debugger festlegt
<i>DebugStart</i>	Mögliche Werte sind <i>ACTIVE</i> , <i>AUTOENABLE</i> oder <i>DISABLE</i> .
<i>DebugType</i>	Mögliche Werte sind <i>SERIAL</i> , <i>1394</i> oder <i>USB</i> .
<i>EMSBAudRate</i>	Definiert die Baudrate für die Notfallverwaltungsdienste.
<i>EMSPort</i>	Legt die Nummer der seriellen Schnittstelle für die Notfallverwaltungsdienste fest.
<i>FirstMegaBytePolicy</i>	Legt die Richtlinie für die Verwendung des ersten MByte des Speichers fest. Mögliche Werte sind <i>USENONE</i> , <i>USEALL</i> oder <i>USEPRIVATE</i> .
<i>GraphicsModeDisabled</i>	Ein boolescher Wert, der den Grafikmodus aktiviert oder deaktiviert
<i>GraphicsResolution</i>	Definiert die Grafikauflösung, zum Beispiel 1024 × 768 oder 800 × 600.
<i>Locale</i>	Legt das Gebietsschema der Startanwendung fest.
<i>Noumex</i>	Wenn <i>Noumex</i> den Wert <i>True</i> hat, werden Benutzermodusausnahmen ignoriert. Hat <i>Noumex</i> dagegen den Wert <i>False</i> , werden Benutzermodusausnahmen nicht ignoriert.
<i>NoVESA</i>	Ein boolescher Wert, der die Verwendung der VESA-Bildschirmmodi (Video Electronics Standards Association) aktiviert oder deaktiviert
<i>RecoveryEnabled</i>	Ein boolescher Wert, der die Verwendung einer Wiederherstellungsabfolge aktiviert oder deaktiviert
<i>RecoverySequence</i>	Definiert die benutzte Wiederherstellungsabfolge.
<i>TargetName</i>	Gibt den Zielnamen für den USB-Debugger als Zeichenfolge an.
<i>TestSigning</i>	Ein boolescher Wert, der die Verwendung von Signaturzertifikaten für Testcode aktiviert oder deaktiviert
<i>TruncateMemory</i>	Gibt die physische Speicheradresse an, ab der Arbeitsspeicher ignoriert wird.

Tabelle 4.7 Wichtige Optionen für Windows-Betriebssystemladeanwendungen

Option	Beschreibung
<i>AdvancedOptions</i>	Ein boolescher Wert, der erweiterte Optionen aktiviert oder deaktiviert
<i>BootLog</i>	Ein boolescher Wert, der das Systemstartinitialisierungsprotokoll aktiviert oder deaktiviert
<i>BootStatusPolicy</i>	Legt die Systemstartstatusrichtlinie fest. Mögliche Werte sind <i>DisplayAllFailures</i> , <i>IgnoreAllFailures</i> , <i>IgnoreShutdownFailures</i> und <i>IgnoreBootFailures</i> .
<i>ClusterModeAddressing</i>	Legt fest, wie viele Prozessoren höchstens in einem einzigen APIC-Cluster (Advanced Programmable Interrupt Controller) zusammengefasst werden.
<i>ConfigFlags</i>	Legt prozessorspezifische Konfigurationsflags fest.
<i>DbgTransport</i>	Gibt den Dateinamen für einen privaten Debuggertransport an.
<i>Debug</i>	Ein boolescher Wert, der den Kerneldebugger aktiviert oder deaktiviert
<i>DriverLoadFailurePolicy</i>	Legt die Richtlinie für Fehler beim Laden von Treibern fest. Mögliche Werte sind <i>Fatal</i> oder <i>UseErrorControl</i> .
<i>Ems</i>	Ein boolescher Wert, der die Kernel-Notfallverwaltungsdienste aktiviert oder deaktiviert
<i>Hal</i>	Legt den Dateinamen für eine private HAL fest.
<i>HalBreakPoint</i>	Ein boolescher Wert, der den speziellen HAL-Haltepunkt aktiviert oder deaktiviert
<i>HypervisorLaunchType</i>	Konfiguriert den Hypervisor-Starttyp. Möglich sind <i>Off</i> und <i>Auto</i> .
<i>IncreaseUserVA</i>	Ein Integerwert (in der Einheit MByte), der den verfügbaren virtuellen Adressraum für Benutzermodusprozesse vergrößert
<i>Kernel</i>	Legt den Dateinamen für einen privaten Systemkern fest.
<i>LastKnownGood</i>	Ein boolescher Wert, der den Start der letzten als funktionierend bekannten Konfiguration aktiviert oder deaktiviert
<i>MaxProc</i>	Ein boolescher Wert, der die Anzeige der Höchstzahl von Prozessoren im System aktiviert oder deaktiviert
<i>Msi</i>	Legt fest, welcher MSI (Message Signaled Interrupt) benutzt wird. Mögliche Werte sind <i>Default</i> oder <i>ForceDisable</i> .
<i>NoCrashAutoReboot</i>	Ein boolescher Wert, der den automatischen Neustart nach einem Absturz aktiviert oder deaktiviert
<i>NoLowMem</i>	Ein boolescher Wert, der die Nutzung von Arbeitsspeicher aus niedrigen Adressbereichen aktiviert oder deaktiviert
<i>NumProc</i>	Legt fest, wie viele Prozessoren beim Systemstart benutzt werden.
<i>Nx</i>	Steuert den NX-Schutz (No-Execute). Mögliche Werte sind <i>OptIn</i> , <i>OptOut</i> , <i>AlwaysOn</i> und <i>AlwaysOff</i> .
<i>OneCPU</i>	Ein boolescher Wert, der festlegt, ob erzwungen wird, dass nur die Systemstart-CPU benutzt wird
<i>OptionsEdit</i>	Ein boolescher Wert, der den Optionseditor aktiviert oder deaktiviert
<i>OSDevice</i>	Gibt an, welches Gerät den Systemstamm enthält.
<i>Pae</i>	Steuert die PAE. Mögliche Werte sind <i>Default</i> , <i>ForceEnable</i> oder <i>ForceDisable</i> .
<i>PerfMem</i>	Legt die Größe (in MByte) des Puffers fest, der für die Leistungsdatenprotokollierung reserviert wird.
<i>RemoveMemory</i>	Ein Integerwert (in MByte), der angibt, wie viel Arbeitsspeicher vom gesamten verfügbaren Arbeitsspeicher entfernt wird, der vom Betriebssystem benutzt werden kann
<i>RestrictAPICCluster</i>	Legt fest, wie viele APIC-Cluster höchstens vom System benutzt werden.
<i>ResumeObject</i>	Legt die Kennung für das Resume-Objekt fest, das mit diesem Betriebssystemobjekt verknüpft ist.
<i>SafeBoot</i>	Gibt an, dass der Computer einen sicheren Startmodus verwendet. Mögliche Werte sind <i>Minimal</i> , <i>Network</i> und <i>DsRepair</i> .



Option	Beschreibung
<i>SafeBootAlternateShell</i>	Ein boolescher Wert, der die Verwendung der alternativen Shell aktiviert oder deaktiviert, wenn im abgesicherten Modus gestartet wird
<i>Sos</i>	Ein boolescher Wert, der die Anzeige zusätzlicher Systemstartdaten aktiviert oder deaktiviert
<i>SystemRoot</i>	Definiert den Pfad zum Systemstamm
<i>UseFirmwarePCISettings</i>	Ein boolescher Wert, der die Verwendung von PCI-Ressourcen aktiviert oder deaktiviert, die im BIOS konfiguriert sind
<i>UsePhysicalDestination</i>	Ein boolescher Wert, der festlegt, ob die Nutzung des physischen APIC erzwungen wird
<i>Vga</i>	Ein boolescher Wert, der festlegt, ob die Nutzung des VGA-Bildschirmtreibers erzwungen wird
<i>WinPE</i>	Ein boolescher Wert, der den Start der Windows-Vorinstallationsumgebung (Windows PE) aktiviert oder deaktiviert

Ändern der Optionen für DEP und PAE

Die Datenausführungsverhinderung (Data Execution Prevention, DEP) ist eine Technik, die dazu dient, den Arbeitsspeicher zu schützen. Ist DEP aktiviert, markiert der Prozessor des Computers den gesamten Arbeitsspeicherbereich einer Anwendung als nicht ausführbar (engl. nonexecutable), sofern nicht explizit angegeben ist, dass die entsprechende Stelle ausführbaren Code enthält. Wird nun versucht, Code auszuführen, der sich in einer als nicht ausführbar markierten Arbeitsspeicherseite befindet, kann der Prozessor eine Ausnahme melden und verhindern, dass dieser Code ausgeführt wird. Dieses Verhalten verhindert, dass böswilliger Anwendungscode, zum Beispiel Viren, sich selbst in bestimmte Bereiche des Arbeitsspeichers einschmuggeln.

Bei Computern, deren Prozessoren die NX-Seitenschutzfunktion (Non-Execute) unterstützen, können Sie das Betriebssystem so konfigurieren, dass es den NX-Schutz nur für sich selbst verwendet. Dazu setzen Sie den Parameter *nx* auf den Wert *OptIn*. Soll das Betriebssystem den NX-Schutz auch anderen Anwendungen zur Verfügung stellen, können Sie dem Parameter *nx* dagegen den Wert *OptOut* zuweisen. Hier ein Beispiel:

```
bcdedit /set {current} nx optout
```

Wenn Sie den NX-Schutz als *OptIn* konfigurieren, wird DEP nur für wichtige Windows-Programme und -Dienste verwendet. Dies ist die Standardeinstellung. Konfigurieren Sie den NX-Schutz dagegen als *OptOut*, verwenden alle Programme und Dienste DEP, also nicht nur die Windows-Standardprogramme und -dienste. Programme, die DEP nicht nutzen sollen, müssen explizit ausgeschlossen werden, wie im Abschnitt »Konfigurieren der Datenausführungsverhinderung« von Kapitel 2, »Konfigurieren von Windows 8-Computern«, beschrieben. Sie können den NX-Schutz auch so konfigurieren, dass er immer an oder immer aus ist. Verwenden Sie dazu die Werte *AlwaysOn* und *AlwaysOff*, zum Beispiel so:

```
bcdedit /set {current} nx alwayson
```

Prozessoren, die den NX-Schutz unterstützen, müssen im PAE-Modus laufen, damit NX benutzt werden kann. Sie konfigurieren PAE, indem Sie den Parameter *Pae* auf *Default*, *ForceEnable* oder *ForceDisable* setzen. Hat *Pae* den Wert *Default*, benutzt das Betriebssystem die Standardkonfiguration für PAE. Setzen Sie *Pae* auf *ForceEnable*, benutzt das Betriebssystem PAE. Und wenn Sie *Pae* auf den Wert *ForceDisable* setzen, benutzt das Betriebssystem PAE nicht. Hier ein Beispiel:

```
bcdedit /set {current} pae default
```

Anpassen der Reihenfolge, in der Betriebssysteme angezeigt werden

Mit dem Befehl `/displayorder` können Sie die Reihenfolge ändern, in der die Startmanager für eine bestimmte Installation von Windows Vista, Windows 7 oder Windows 8 aufgelistet werden. Die Syntax lautet:

```
bcdedit /displayorder id1 id2 ... idn
```

Dabei ist *id1* die Kennung des ersten angezeigten Betriebssystems, *id2* die Kennung des zweiten und so weiter. Nehmen wir an, Sie wollen die Anzeigereihenfolge der Betriebssysteme ändern, die durch folgende BCD-Einträge identifiziert werden:

Windows-Startladeprogramm

```
-----
identifizier          {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

Windows-Startladeprogramm

```
-----
identifizier          {14504de-e96b-11cd-a51b-89ace9305d5e}
```

Windows-Startladeprogramm

```
-----
identifizier          {8b78e48f-02d0-11dd-af92-a72494804a8a}
```

Dazu verwenden Sie folgenden Befehl:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a}
{16b857b4-9e02-11e0-9c17-b7d085eb0682}
{14504de-e96b-11cd-a51b-89ace9305d5e}
```

Indem Sie `/displayorder` mit `/addfirst` verwenden, machen Sie das angegebene Betriebssystem zum ersten Eintrag der Liste:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a} /addfirst
```

Entsprechend wird das angegebene Betriebssystem zum letzten Eintrag der Liste, wenn Sie `/displayorder` zusammen mit `/addlast` verwenden:

```
bcdedit /displayorder {8b78e48f-02d0-11dd-af92-a72494804a8a} /addlast
```

Ändern des Eintrags für das Standardbetriebssystem

Der Befehl `/default` ändert den Eintrag für das Standardbetriebssystem. Die Syntax dieses Befehls lautet:

```
bcdedit /default id
```

wobei *id* die Betriebssystemkennung im Startladeprogrammeintrag ist. Nehmen wir wieder als Beispiel ein Betriebssystem, das durch diesen BCD-Eintrag identifiziert wird:

Windows-Startladeprogramm

```
-----
identifizier          {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

Mit dem folgenden Befehl machen Sie dieses Betriebssystem zum Standardbetriebssystem:

```
bcdedit /default {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

Wenn Sie ein älteres Betriebssystem als Windows 8 als Standard verwenden wollen, müssen Sie die Kennung des Windows-Legacybetriebssystem-Ladeprogramms verwenden. Der entsprechende BCD-Eintrag sieht so aus:

Windows-Legacybetriebssystem-Ladeprogramm

```
-----  
identifizier      {466f5a88-0af2-4f76-9038-095b170dc21c}  
device            partition=C:  
path              \ntldr  
description        Älteres Microsoft Windows-Betriebssystem
```

In diesem Fall können Sie *Ntldr* als Standard festlegen, indem Sie diesen Befehl verwenden:

```
bcdedit /default {466f5a88-0af2-4f76-9038-095b170dc21c}
```

Ändern des Standardzeitlimits

Mit dem Befehl */timeout* können Sie festlegen, wie lange gewartet wird, bevor das Standardbetriebssystem startet. Geben Sie mit dem Befehl */timeout* an, wie viele Sekunden Sie warten wollen:

```
bcdedit /timeout 30
```

Wenn Sie als Zeitlimit den Wert von 0 Sekunden angeben, wird das Standardbetriebssystem sofort gestartet.

Die Startreihenfolge kurzzeitig ändern

Gelegentlich ist es nützlich, ein einziges Mal ein bestimmtes Betriebssystem zu starten, danach aber wieder die Standardstartreihenfolge zu verwenden. Dafür gibt es den Befehl */bootsequence*. Geben Sie nach dem Befehl die Kennung des Betriebssystems an, das nach dem nächsten Neustart des Computers verwendet werden soll, zum Beispiel:

```
bcdedit /bootsequence {975a8204-9658-11dd-993e-9aea7965e9da}
```

Sobald Sie nun den Computer neu starten, verwendet der Computer für diesen einen Start das angegebene Betriebssystem als Vorgabe. Wenn Sie den Computer danach wieder starten, gilt wieder die ursprüngliche Standardstartreihenfolge.

Kapitel 5

Konfigurieren von Benutzer- und Computerrichtlinien

In diesem Kapitel:

Grundlagen von Gruppenrichtlinien	186
Konfigurieren von Richtlinien	192
Arbeiten mit Datei- und Datenverwaltungsrichtlinien	195
Verwenden von Zugriffs- und Verbindungsrichtlinien	202
Verwenden von Computer- und Benutzerskriptrichtlinien	205
Verwenden von Anmelde- und Startrichtlinien	209

Gruppenrichtlinien sind ein Satz Regeln, die Sie anwenden können, um Benutzer und Computer einfacher zu verwalten. In Windows 8 umfassen die Gruppenrichtlinien verwaltete Richtlinieneinstellungen (kurz Richtlinien, im Englischen auch als »policy settings« bezeichnet) und unverwaltete Richtlinieneinstellungen (kurz Einstellungen, im englischen »policy preferences«). Mit verwalteten Richtlinieneinstellungen steuern Sie die Konfiguration des Betriebssystems und seiner Komponenten, während Sie mit unverwalteten Richtlinieneinstellungen Betriebssystem- und Anwendungseinstellungen konfigurieren, bereitstellen und verwalten. Der Hauptunterschied zwischen verwalteten und unverwalteten Richtlinieneinstellungen besteht darin, wie sie durchgesetzt werden. Verwaltete Richtlinieneinstellungen werden von den Gruppenrichtlinien strikt erzwungen, unverwaltete Richtlinieneinstellungen dagegen nicht. In diesem Kapitel zeige ich Ihnen, wie Sie verwaltete Richtlinieneinstellungen benutzen. Das nächste Kapitel beschreibt die Benutzung unverwalteter Richtlinieneinstellungen.

Grundlagen von Gruppenrichtlinien

Mit verwalteten Richtlinieneinstellungen steuern Sie die Konfiguration des Betriebssystems und deaktivieren in der Benutzeroberfläche die Optionen und Steuerelemente für die Einstellungen, die von den Gruppenrichtlinien verwaltet werden. Die meisten Richtlinieneinstellungen sind in separaten Zweigen der Registrierung gespeichert. Das Betriebssystem und die Anwendungen prüfen diese Registrierungszweige, um festzustellen, ob und wie verschiedene Aspekte des Betriebssystems gesteuert werden.

Es gibt zwei Arten von Gruppenrichtlinien: lokale Gruppenrichtlinien und Active Directory-Gruppenrichtlinien. Lokale Gruppenrichtlinien dienen allein zur Verwaltung des lokalen Computers. Dagegen verwalten Active Directory-Gruppenrichtlinien die Einstellungen der Computer an Standorten, in Domänen und in Organisationseinheiten (Organizational Unit, OU). Gruppenrichtlinien vereinfachen die Verwaltung, weil sie den Administratoren eine zentrale Kontrolle der Rechte, Berechtigungen und Möglichkeiten von Benutzern und Computern erlauben. Ein sorgfältiger Umgang mit den Gruppenrichtlinien ist für eine einwandfreie Funktion des Systems entscheidend. Richtlinieneinstellungen lassen sich in zwei Kategorien aufteilen, nämlich in Richtlinien, die für Computer gelten, und in Richtlinien, die für Benutzer gelten. Computerrichtlinien werden gewöhnlich beim Systemstart angewendet und Benutzerrichtlinien bei der Anmeldung.

Während des Systemstarts und bei der Anmeldung werden die Richtlinien in einer genau festgelegten Reihenfolge angewendet. Diese Reihenfolge spielt auch bei der Problembehebung eine wichtige Rolle. Sind mehrere Richtlinien konfiguriert, werden sie in folgender Reihenfolge angewendet:

1. Lokale Richtlinien
2. Standortrichtlinien
3. Domänenrichtlinien
4. Gruppenrichtlinien der Organisationseinheit
5. Gruppenrichtlinien von untergeordneten Organisationseinheiten

Wenn es Konflikte zwischen den Richtlinieneinstellungen gibt, hat die später angewendete Einstellung Vorrang und setzt die vorher geltende Einstellung außer Kraft. Daher haben beispielsweise Richtlinien einer Organisationseinheit Vorrang vor den Gruppenrichtlinien der Domäne. Wie Sie sicher erwarten, gibt es Ausnahmen von dieser Vorrangregelung, die es Administratoren ermöglicht, Richtlinien zu blockieren, zu überwachen und zu deaktivieren.

Der Gruppenrichtlinienclientdienst isoliert die Benachrichtigung und Verarbeitung der Gruppenrichtlinien vom Windows-Anmeldevorgang, was den Ressourcenverbrauch für die Hintergrundverarbeitung der Richtlinie verringert, die Gesamtleistung verbessert und es ermöglicht, neue Gruppenrichtlinien-

dateien im Rahmen des Aktualisierungsvorgangs auszuliefern und anzuwenden, ohne dass ein Neustart erforderlich ist. Dank der Erkennung der Netzwerkstandortkategorie (Network Location Awareness, NLA) können die Gruppenrichtlinienclients den Computerstatus, den Netzwerkstatus und die verfügbare Netzwerkbandbreite ermitteln, um langsame Verbindungen zu erkennen. Folglich hat der Gruppenrichtlinienclient einen besseren Überblick über die Betriebsumgebung und ist besser in der Lage festzulegen, welche Richtlinien wann angewendet werden sollten.

Ereignismeldungen zu Gruppenrichtlinien werden in das Systemprotokoll eines Computers eingetragen. Außerdem stehen zur Problembeseitigung noch weitere Mittel zur Verfügung. Sie können die ausführlichen Ereignismeldungen aus dem Betriebsprotokoll verwenden. In der Ereignisanzeige finden Sie das Betriebsprotokoll unter *Anwendungs- und Dienstprotokolle\Microsoft\Windows\GroupPolicy\Betriebsbereit*. Außerdem können Sie mit *gpupdate.exe* dafür sorgen, dass die neusten Einstellungen angewendet werden. Gewöhnlich wird dieses Befehlszeilentool zwar auf dem Computer verwendet, auf dem Probleme behoben werden sollen, aber Windows Server 2012 ermöglicht die Ausführung von *gpupdate.exe* und damit die Aktualisierung der Gruppenrichtlinien auf Remotecomputern auch nach Zeitplan. Weitere Informationen finden Sie in Kapitel 4, »Automatisieren von Aufgaben, Richtlinien und Prozeduren«, in *Windows Server 2012 – Ratgeber für Administratoren* (Microsoft Press, 2012).

Bearbeiten und Benutzen der lokalen Gruppenrichtlinien

Lokale Gruppenrichtlinien werden auf alle Benutzer oder Administratoren angewendet, die sich an einem Computer anmelden, der Mitglied einer Arbeitsgruppe ist, sowie auf alle Benutzer oder Administratoren, die sich lokal an einem Computer anmelden, der Mitglied einer Domäne ist.

Wie bei Windows 7 kann auch ein Computer, auf dem Windows 8 ausgeführt wird, mit mehreren lokalen Richtlinienobjekten verknüpft sein. Lokale Gruppenrichtlinien werden über das lokale Gruppenrichtlinienobjekt (Group Policy Object, GPO) verwaltet. Das lokale GPO ist auf jedem Computer im Ordner *%SystemRoot%\System32\GroupPolicy* gespeichert. Zusätzliche benutzer- und gruppenspezifische lokale GPOs liegen im Ordner *%SystemRoot%\System32\GroupPolicyUsers*.

Wenn Sie Computer statt in einer Domänenkonfiguration als eigenständige Computer verwenden, ist es unter Umständen sinnvoll, mehrere lokale GPOs zu verwenden. Sie können beispielsweise ein lokales GPO für Administratoren und ein anderes für Nicht-Administratoren einrichten. Auf diese Weise brauchen Sie keine Einstellungen, die Konflikte bei der Verwaltung des Computers verursachen, explizit zu deaktivieren oder zu entfernen, bevor Sie Administratortasken durchführen. In einer Domänenkonfiguration ist es dagegen kaum sinnvoll, mehrere lokale GPOs zu benutzen. In Domänen werden auf die meisten Computer und Benutzer bereits mehrere GPOs angewendet. Fügen Sie dann noch mehrere lokale GPOs zu dieser Mischung hinzu, wird die Verwaltung der Gruppenrichtlinien sehr unübersichtlich.

Windows 8 hat drei Schichten lokaler GPOs:

- **Lokale Gruppenrichtlinien** Die lokalen Gruppenrichtlinien sind das einzige lokale GPO, in dem sowohl Computerkonfigurations- als auch Benutzerkonfigurationseinstellungen auf alle Benutzer des Computers angewendet werden.
- **Lokale Gruppenrichtlinien für Administratoren und Nicht-Administratoren** Die lokalen Gruppenrichtlinien für Administratoren und Nicht-Administratoren enthalten nur Benutzerkonfigurationseinstellungen. Welche Richtlinie angewendet wird, hängt davon ab, ob das verwendete Benutzerkonto Mitglied der lokalen Gruppe *Administratoren* ist.
- **Benutzerspezifische lokale Gruppenrichtlinien** Die benutzerspezifischen lokalen Gruppenrichtlinien enthalten ausschließlich Benutzerkonfigurationseinstellungen. Diese Richtlinie wird auf einzelne Benutzer und Gruppen angewendet.

Diese Schichten der lokalen GPOs werden in folgender Reihenfolge verarbeitet: lokale Gruppenrichtlinien, lokale Gruppenrichtlinien für Administratoren beziehungsweise Nicht-Administratoren, benutzerspezifische lokale Gruppenrichtlinien.

Weil in allen lokalen GPOs dieselben Benutzerkonfigurationseinstellungen verfügbar sind, kann es vorkommen, dass eine Einstellung in einem GPO einen Konflikt mit der Einstellung in einem anderen GPO verursacht. Windows 8 löst solche Konflikte in den Einstellungen auf, indem es alle vorherigen Einstellungen durch die zuletzt eingelesene und aktuelle Einstellung überschreibt. Windows 8 verwendet also die letzte Einstellung. Wenn Windows 8 Konflikte auflöst, ist dabei nur von Bedeutung, ob die Einstellung aktiviert oder deaktiviert ist. Die Einstellung *Nicht konfiguriert* hat keine Auswirkung auf den Zustand einer Einstellung, die aus einer vorher angewendeten Richtlinie stammt. Um die Domänenadministration zu vereinfachen, können Sie die Verarbeitung der lokalen GPOs auf Windows 8-Computern deaktivieren, indem Sie in einem Gruppenrichtlinienobjekt der Domäne die Richtlinieneinstellung *Verarbeitung lokaler Gruppenrichtlinienobjekte deaktivieren* aktivieren. Sie finden diese Einstellung in den Gruppenrichtlinien unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Gruppenrichtlinie*.

HINWEIS

Lokale GPOs werden immer verarbeitet, wenn sie aktiviert sind. Sie haben aber den niedrigsten Rang, was bedeutet, dass ihre Einstellungen von den Einstellungen für Standort, Domäne und Organisationseinheit überschrieben werden.

Das einzige lokale Richtlinienobjekt, das auf einem Computer standardmäßig vorhanden ist, ist das lokale GPO. Weitere lokale Richtlinienobjekte können Sie im Gruppenrichtlinienobjekt-Editor erstellen und verwalten. Weil die lokalen Gruppenrichtlinien lediglich eine Untermenge der Gruppenrichtlinien sind, gibt es viele Dinge, die Sie nicht lokal konfigurieren können, sondern nur in einer Domänenumgebung. Erstens können Sie keinerlei unverwaltete Richtlinieneinstellungen verwalten. Zweitens können Sie nur einen Teil der verwalteten Richtlinieneinstellungen konfigurieren. Abgesehen von diesen grundlegenden Unterschieden werden lokale Gruppenrichtlinien und Active Directory-Gruppenrichtlinien auf dieselbe Weise verwaltet.

Um mit lokalen GPOs zu arbeiten, brauchen Sie ein Administratorkonto. Am schnellsten greifen Sie auf das oberste lokale GPO des lokalen Computers zu, indem Sie im Suchfeld oder in einer Eingabeaufforderung den folgenden Befehl eingeben:

```
gpedit.msc /gpcomputer: "%ComputerName%"
```

Dieser Befehl startet den Gruppenrichtlinienobjekt-Editor in einer Microsoft Management Console (MMC), wobei als Ziel der lokale Computer eingestellt ist.

Außerdem können Sie das oberste lokale GPO auf einem Computer auch folgendermaßen bearbeiten:

1. Öffnen Sie die MMC. Dazu können Sie zum Beispiel die WINDOWS-Taste drücken, **mmc** eingeben und die EINGABETASTE drücken.
2. Wählen Sie in der Microsoft Management Console den Menübefehl *Datei* und dann *Snap-In hinzufügen/entfernen*.
3. Tippen oder klicken Sie im Dialogfeld *Snap-Ins hinzufügen bzw. entfernen* auf *Gruppenrichtlinienobjekt-Editor* und dann auf *Hinzufügen*.
4. Tippen oder klicken Sie im Dialogfeld *Gruppenrichtlinienobjekt auswählen* auf *Fertig stellen* (der lokale Computer ist das Standardobjekt). Tippen oder klicken Sie auf *OK*.

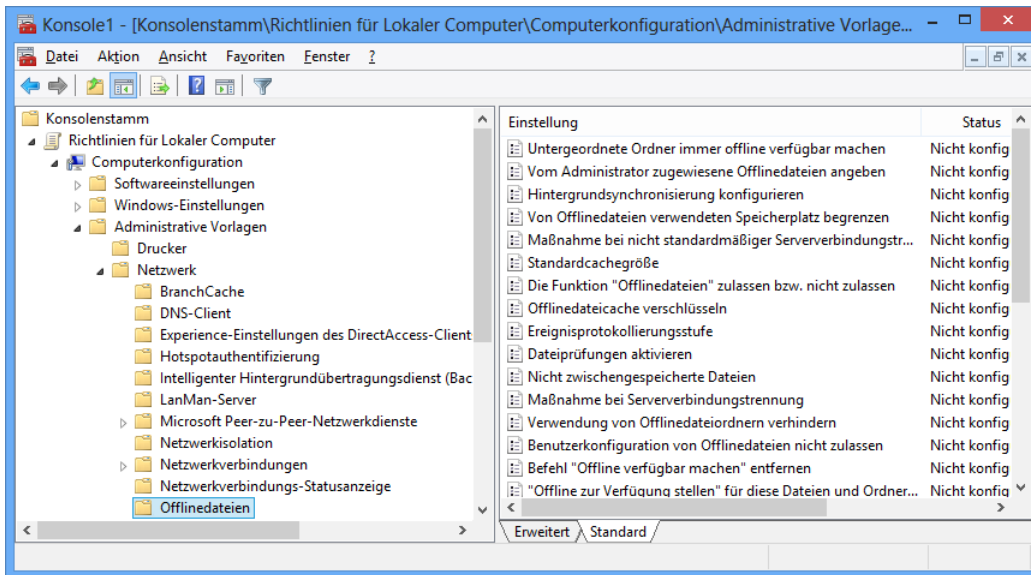


Abbildung 5.1 Zugreifen auf das oberste lokale GPO

Wie in Abbildung 5.1 gezeigt, können Sie nun im Konsolenfenster die lokalen Gruppenrichtlinieneinstellungen verwalten. Weil die lokalen Gruppenrichtlinien keine unverwalteten Richtlinieneinstellungen umfassen, gibt es unter *Computerkonfiguration* und *Benutzerkonfiguration* keine getrennten Knoten für *Richtlinien* und *Einstellungen*.

Sie können bei Bedarf auch andere lokale Richtlinienobjekte anlegen und verwalten. Gehen Sie folgendermaßen vor, um weitere lokale GPOs zu erstellen und zu bearbeiten:

1. Tippen oder klicken Sie in der MMC auf *Datei* und anschließend auf *Snap-In hinzufügen/entfernen*.
2. Tippen oder klicken Sie im Dialogfeld *Snap-Ins hinzufügen bzw. entfernen* auf *Gruppenrichtlinienobjekt-Editor* und dann auf *Hinzufügen*.
3. Tippen oder klicken Sie im Dialogfeld *Gruppenrichtlinienobjekt auswählen* auf *Durchsuchen*. Tippen oder klicken Sie im Dialogfeld *Gruppenrichtlinienobjekt suchen* auf die Registerkarte *Benutzer*.
4. Auf der Registerkarte *Benutzer* (Abbildung 5.2) zeigen die Einträge in der Spalte *Gruppenrichtlinienobjekt ist vorhanden*, ob ein bestimmtes lokales Richtlinienobjekt bereits erstellt wurde. Sie haben nun folgende Möglichkeiten:
 - Wählen Sie *Administratoren* aus, um das lokale GPO für Administratoren zu erstellen. Sie verwenden hier die Gruppe *Administratoren* statt des Benutzers *Administrator*, um sicherzustellen, dass die Richtlinie auf alle lokalen Administratoren angewendet wird.
 - Wählen Sie *Nicht-Administratoren* aus, um das lokale GPO für Nicht-Administratoren anzulegen und zu öffnen.
 - Wählen Sie den lokalen Benutzer aus, dessen benutzerspezifisches lokales GPO Sie erstellen oder öffnen wollen.
5. Tippen oder klicken Sie auf *OK*, dann auf *Fertig stellen* und schließlich wieder auf *OK*. Sofern das ausgewählte Objekt noch nicht vorhanden ist, wird es nun erstellt. Andernfalls öffnen Sie das Objekt, damit Sie es ansehen und bearbeiten können.

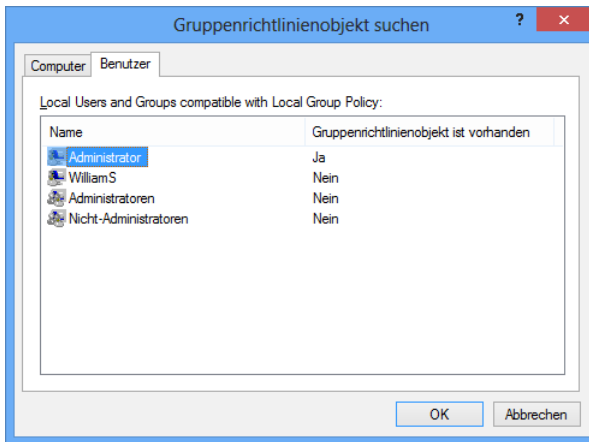


Abbildung 5.2 Zugreifen auf weitere lokale GPOs

Öffnen und Benutzen von Richtlinien für Standorte, Domänen und Organisationseinheiten

In Active Directory kann jeder Standort, jede Domäne und jede Organisationseinheit jeweils eine oder mehrere eigene Gruppenrichtlinien haben. Wenn Sie mit Active Directory-Gruppenrichtlinien arbeiten wollen, müssen Sie die Konsole *Gruppenrichtlinienverwaltung* (Group Policy Management Console, GPMC) verwenden, um diese GPOs anzuzeigen und zu bearbeiten. Außerdem brauchen Sie ein Administratorkonto, um auf diese GPOs zuzugreifen.

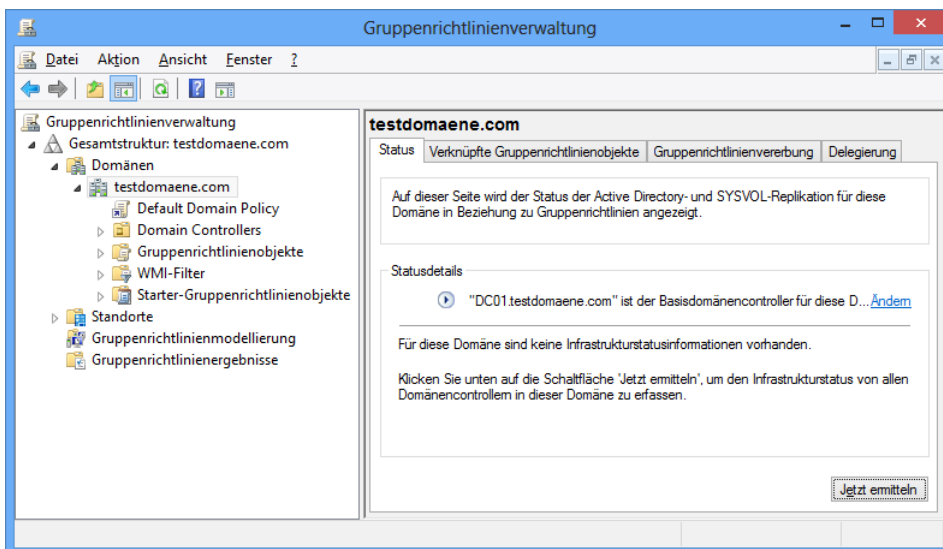


Abbildung 5.3 Zugreifen auf Gruppenrichtlinienobjekte für Domänen, Standorte und Organisationseinheiten

Auf einem Computer, der unter einer Server-Edition von Windows läuft, steht die Konsole *Gruppenrichtlinienverwaltung* als Teil der Standardinstallation zur Verfügung. Auf einem Computer, der unter einer Desktopedition von Windows läuft, können Sie die Konsole *Gruppenrichtlinienverwaltung* einspielen,

indem Sie die Remoteserver-Verwaltungstools (Remote Server Administration Tools, RSAT) installieren. RSAT für Windows 8 können Sie vom Microsoft Download Center herunterladen (<http://download.microsoft.com/>).

Nachdem Sie die Konsole *Gruppenrichtlinienverwaltung* als Teil von RSAT installiert haben, können Sie sie im Server-Manager starten. Tippen oder klicken Sie im Server-Manager auf *Tools* und dann auf *Gruppenrichtlinienverwaltung*.

Wie in Abbildung 5.3 gezeigt, enthält der linke Fensterabschnitt der Konsole *Gruppenrichtlinienverwaltung* auf den oberen Ebenen standardmäßig zwei Knoten: *Gruppenrichtlinienverwaltung* (der Konsolenstamm) und *Gesamtstruktur* (ein Knoten für die aktuelle Gesamtstruktur, mit der Sie momentan verbunden sind; der Name ergibt sich aus der Gesamtstruktur-Stammdomäne dieser Gesamtstruktur). Wenn Sie den Knoten *Gesamtstruktur* erweitern, sehen Sie folgende Knoten:

- **Domänen** Bietet Zugang zu den Richtlinieneinstellungen der Domänen in der dazugehörigen Gesamtstruktur. Standardmäßig sind Sie mit der Domäne verbunden, bei der Sie sich angemeldet haben, und können Verbindung zu anderen Domänen aufnehmen. Wenn Sie den Knoten einer Domäne erweitern, können Sie auf das GPO der Standarddomänenrichtlinie (*Default Domain Policy*), auf die Organisationseinheit *Domain Controllers* (und das dazugehörige GPO *Default Domain Controllers Policy*) und auf die Gruppenrichtlinienobjekte zugreifen, die in der Domäne definiert wurden.
- **Standorte** Bietet Zugang zu den Richtlinieneinstellungen für Standorte in der Gesamtstruktur. Standardmäßig werden Standorte verborgen.
- **Gruppenrichtlinienmodellierung** Bietet Zugang zum Gruppenrichtlinienmodellierungs-Assistenten, der Sie bei der Planung der Richtlinien unterstützt und die Richtlinien zu Testzwecken simuliert. Auch alle gespeicherten Richtlinienmodelle stehen hier zur Verfügung.
- **Gruppenrichtlinienergebnisse** Bietet Zugang zum Gruppenrichtlinienergebnis-Assistenten. Sie haben die Gruppenrichtlinienobjekte und Organisationseinheiten aus allen Domänen, mit denen Sie verbunden sind, zur Bearbeitung an einem Ort zur Verfügung.

Die Gruppenrichtlinienobjekte, die in der Konsole *Gruppenrichtlinienverwaltung* in Containern für Domänen, Standorte und Organisationseinheiten aufgeführt werden, sind in Wirklichkeit Gruppenrichtlinienobjekt-Verknüpfungen und nicht die Gruppenrichtlinienobjekte selbst. Die tatsächlichen Gruppenrichtlinienobjekte befinden sich im Gruppenrichtlinienobjekte-Container der ausgewählten Domäne. Beachten Sie auch, dass die Symbole für Gruppenrichtlinienobjekt-Verknüpfungen mit einem kleinen Pfeil in der linken unteren Ecke markiert sind, ähnlich wie Verknüpfungssymbole. Sie öffnen ein Gruppenrichtlinienobjekt zum Bearbeiten, indem Sie es gedrückt halten oder mit der rechten Maustaste anklicken und im Kontextmenü den Befehl *Bearbeiten* wählen.

Nachdem Sie ein Gruppenrichtlinienobjekt für die Bearbeitung ausgewählt oder neu erstellt haben, können Sie die Bearbeitung mit dem Gruppenrichtlinienverwaltungs-Editor durchführen. Wie aus Abbildung 5.4 hervorgeht, zeigt der Gruppenrichtlinienverwaltungs-Editor zwei Hauptknoten an:

- **Computerkonfiguration** Ermöglicht Ihnen die Festlegung von Richtlinien, die unabhängig vom angemeldeten Benutzer für Computer gelten.
- **Benutzerkonfiguration** Ermöglicht Ihnen die Festlegung von Richtlinien, die für bestimmte Benutzer gelten, und zwar unabhängig davon, an welchem Computer sie sich anmelden.

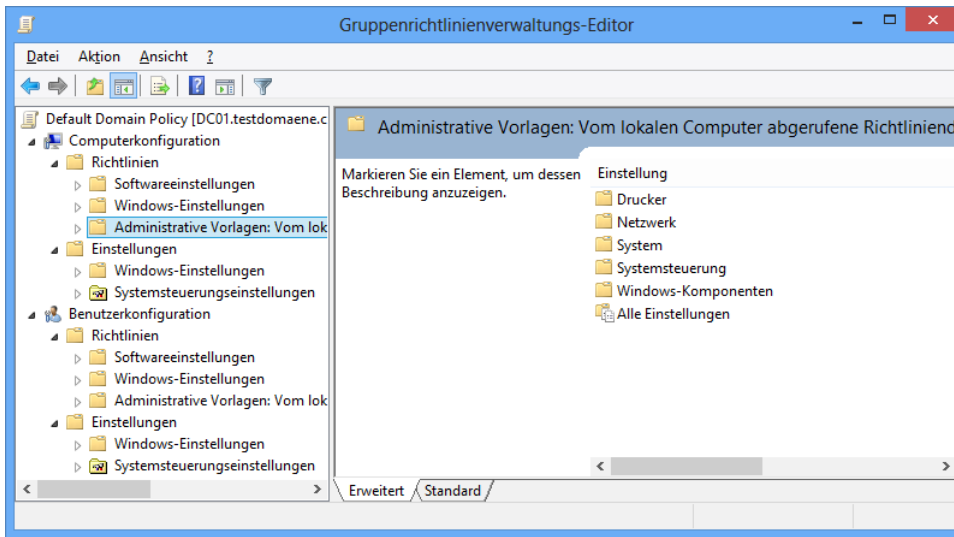


Abbildung 5.4 Die Gruppenrichtlinienoptionen hängen vom Gruppenrichtlinienobjekt ab, das Sie erstellen, und von den installierten Add-Ons

HINWEIS

Vergessen Sie nicht, dass Benutzerkonfigurationseinstellungen, die in lokalen Gruppenrichtlinienobjekten vorgenommen werden, nur auf den Computern gelten, auf denen die Optionen konfiguriert sind. Wenn Sie möchten, dass die Einstellungen auf allen Computern gelten, die der Benutzer vielleicht verwendet, müssen Sie die Gruppenrichtlinien der Domäne, der Organisationseinheit oder des Standorts verwenden.

Unter *Computerkonfiguration* und *Benutzerkonfiguration* finden Sie jeweils die separaten Knoten *Richtlinien* und *Einstellungen*. Wenn Sie mit verwalteten Richtlinieneinstellungen arbeiten, verwenden Sie den Knoten *Richtlinien*. Welche Optionen unter einem Richtlinienknoten zur Verfügung stehen, hängt davon ab, welche Add-Ons installiert sind und welche Art von Richtlinie Sie erstellen. Gewöhnlich finden Sie in beiden Knoten folgende untergeordnete Knoten:

- **Softwareeinstellungen** Legt Richtlinien für Softwareeinstellungen und die Softwareinstallation fest. Wenn Sie Software installieren, können unter *Softwareeinstellungen* untergeordnete Knoten hinzugefügt werden.
- **Windows-Einstellungen** Legt Richtlinien für Ordnerumleitung, Skripts und Sicherheit fest.
- **Administrative Vorlagen** Legt Richtlinien für Betriebssystem, Windows-Komponenten und Programme fest. Diese Richtlinien, die im Verlauf dieses Kapitels näher besprochen werden, gelten für Benutzer und Computer.

Konfigurieren von Richtlinien

Zur Verwaltung von Benutzern und Computern verwenden Sie die Richtlinien aus den administrativen Vorlagen. Diese Richtlinien bieten einen einfachen Zugang zu den Richtlinieneinstellungen der Registrierung, die das Betriebssystem, Windows-Komponenten und Programme steuern. Ältere Windows-Versionen, in denen es Gruppenrichtlinien gibt, verwenden ADM-Dateien (Administrative Template) mit einer speziellen Sprache, um Richtlinieneinstellungen auf Registrierungsbasis zu speichern. Windows 8 verwendet dagegen ein Dateiformat, das ADMX genannt wird und auf dem XML-Standard beruht. Im

Gegensatz zu ADM-Dateien, die in dem Gruppenrichtlinienobjekt gespeichert werden, zu dem sie gehören, werden ADMX-Dateien in einem zentralen Datenspeicher verwaltet. In Domänen lassen sich ADMX-Dateien durch die zentrale Speicherung leichter bearbeiten und verwalten.

Anzeigen von Richtlinien und Vorlagen

Wie aus Abbildung 5.5 hervorgeht, können Sie die aktuell konfigurierten Vorlagen im Knoten *Administrative Vorlagen* des Gruppenrichtlinienverwaltungs-Editors anzeigen. Er enthält Richtlinien, die für lokale Systeme, Organisationseinheiten, Domänen und Standorte konfiguriert werden können. Die Vorlagen unter *Computerkonfiguration* und *Benutzerkonfiguration* sind verschieden. Im Gruppenrichtlinienverwaltungs-Editor und bei der Installation neuer Windows-Komponenten können Sie Vorlagen mit neuen Richtlinien hinzufügen.

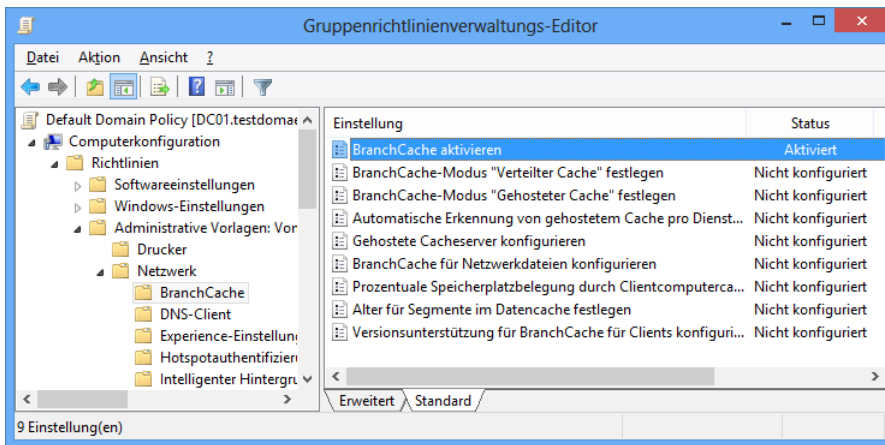


Abbildung 5.5 Festlegen von Benutzer- und Computerrichtlinien mithilfe administrativer Vorlagen

Alle Änderungen, die Sie an den Richtlinien aus den administrativen Vorlagen vornehmen, werden in der Registrierung gespeichert. Computerkonfigurationen werden in *HKEY_LOCAL_MACHINE* gespeichert und Benutzerkonfigurationen in *HKEY_USER*. Wenn Sie im Gruppenrichtlinienverwaltungs-Editor ein wenig im Knoten *Administrative Vorlagen* herumstöbern, lernen Sie die verschiedenen Richtlinien der administrativen Vorlagen am schnellsten kennen. Sie werden feststellen, dass sich Richtlinien gewöhnlich in einem von drei Zuständen befinden:

- **Nicht konfiguriert** Die Richtlinie wird nicht verwendet und ihre Einstellung hat keinen Einfluss auf die Konfiguration des Computers.
- **Aktiviert** Die Richtlinie ist aktiv und ihre Einstellungen werden in der Registrierung gespeichert.
- **Deaktiviert** Die Richtlinie ist nicht aktiv. Sie kann ein bestimmtes Verhalten aufweisen, das im Gegensatz zu der Einstellung für den aktiven Zustand steht. Die Einstellungen werden in der Registrierung gespeichert.

Aktivieren, Deaktivieren und Konfigurieren von Richtlinien

Im Gruppenrichtlinienverwaltungs-Editor finden Sie administrative Vorlagen in zwei Knoten: *Computerkonfiguration* und *Benutzerkonfiguration*. In den meisten Fällen überschneiden sich die Richtlinien nicht und stehen auch nicht im Widerspruch zueinander. Sollte sich ein Konflikt ergeben, haben die Computerrichtlinien Vorrang. Das bedeutet, dass die Computerrichtlinie die Richtlinie ist, die gilt und die durchgesetzt wird. Im Verlauf dieses Kapitels werden die häufig verwendeten Richtlinien und ihre Anwendung genauer beschrieben.

Bevor Sie Richtlinien bearbeiten können, müssen Sie den Gruppenrichtlinienverwaltungs-Editor für den Standort, die Domäne oder die Organisationseinheit öffnen, mit der Sie arbeiten wollen. Gehen Sie folgendermaßen vor, um auf ein Gruppenrichtlinienobjekt für eine Domäne oder eine Organisationseinheit zuzugreifen:

1. Erweitern Sie in der Konsole *Gruppenrichtlinienverwaltung* den Knoten der Gesamtstruktur, mit der Sie arbeiten wollen, und dann den untergeordneten Knoten *Domänen*.
2. Erweitern Sie den Knoten der Domäne, mit der Sie arbeiten wollen, und dann den untergeordneten Knoten *Gruppenrichtlinienobjekte*.
3. Klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt, mit dem Sie arbeiten wollen, oder halten Sie es gedrückt, und wählen Sie den Befehl *Bearbeiten*. Daraufhin wird das Gruppenrichtlinienobjekt zur Bearbeitung im Gruppenrichtlinienverwaltungs-Editor geöffnet.

Nachdem Sie das GPO im Gruppenrichtlinienverwaltungs-Editor geöffnet haben, können Sie Richtlinien folgendermaßen aktivieren, deaktivieren und konfigurieren:

1. Erweitern Sie den Ordner *Administrative Vorlagen* unter *Computerkonfiguration* oder *Benutzerkonfiguration*, je nach der gesuchten Richtlinie.
2. Tippen oder klicken Sie in der Strukturdarstellung auf den Ordner, in dem die gewünschte Richtlinie liegt. Dadurch werden die enthaltenen Richtlinien im rechten Konsolenbereich angezeigt.
3. Tippen oder klicken Sie die gewünschte Richtlinie doppelt oder mit der rechten Maustaste an oder halten Sie die Richtlinie gedrückt, und wählen Sie *Bearbeiten*, um die Richtlinie im Bearbeitungsdialogfeld zu öffnen.
4. Um unteren rechten Bereich finden Sie im Textfeld *Hilfe* eine Beschreibung der Richtlinie, sofern eine Beschreibung verfügbar ist.
5. Zur Einstellung der Richtlinie dienen die Optionsschaltflächen im oberen linken Bereich des Dialogfelds:
 - **Nicht konfiguriert** Die Richtlinie ist nicht konfiguriert.
 - **Aktiviert** Die Richtlinie ist aktiv.
 - **Deaktiviert** Die Richtlinie ist nicht aktiv.
6. Wenn Sie die Richtlinie aktivieren, nehmen Sie im Bereich *Optionen* alle zusätzlichen Einstellungen vor, die erforderlich sind, und tippen oder klicken dann auf *Übernehmen*.
7. Mit den Schaltflächen *Vorherige Einstellung* und *Nächste Einstellung* erreichen Sie die anderen Richtlinien, die im Ordner verfügbar sind. Nehmen Sie die gewünschten Einstellungen vor, wie in den Schritten 4 bis 6 beschrieben.
8. Tippen oder klicken Sie auf *OK*, wenn Sie fertig sind.

Hinzufügen oder Entfernen von Vorlagen

Sie können im Gruppenrichtlinienverwaltungs-Editor Vorlagenordner hinzufügen und entfernen. Gehen Sie folgendermaßen vor:

1. Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor für den Standort, die Domäne oder die Organisationseinheit, mit der Sie arbeiten möchten.
2. Tippen oder klicken Sie unter *Computerkonfiguration* oder *Benutzerkonfiguration* mit der rechten Maustaste auf den Ordner *Administrative Vorlagen* und wählen Sie *Vorlagen hinzufügen/entfernen*. Dadurch öffnet sich das Dialogfeld *Vorlagen hinzufügen/entfernen*.
3. Um neue Vorlagen hinzuzufügen, tippen oder klicken Sie auf *Hinzufügen*. Anschließend wählen Sie im Dialogfeld *Richtlinienvorlagen* die Vorlage aus, die Sie hinzufügen möchten, und tippen oder klicken auf *Öffnen*.
4. Um eine vorhandene Vorlage zu entfernen, wählen Sie die Vorlage aus und tippen oder klicken dann auf *Entfernen*.
5. Wenn Sie keine Vorlagen mehr hinzufügen oder entfernen möchten, tippen oder klicken Sie auf *Schließen*.

Arbeiten mit Datei- und Datenverwaltungsrichtlinien

Jeder Systemadministrator sollte sich mit den Richtlinien zur Datei- und Datenverwaltung auskennen. Sie legen fest, welche Datenmenge ein Benutzer auf einem Computer speichern kann, wie Offlinedateien verwendet werden und ob die Systemwiederherstellungsfunktion aktiviert ist.

Tabelle 5.1 Richtlinien für Datenträgerkontingente

Richtlinienname	Beschreibung
Datenträgerkontingente ermöglichen	Aktiviert oder deaktiviert Datenträgerkontingente für alle NTFS-Volumes des Computers und hindert Benutzer daran, die Einstellung zu ändern.
Datenträgerkontingentsgrenze erzwingen	Gibt an, ob Datenträgerkontingente durchgesetzt werden. Ist dies der Fall, erhalten Benutzer keinen zusätzlichen Speicherplatz, wenn ihr Kontingent erschöpft ist. Diese Einstellung hat Vorrang vor der Einstellung auf der Registerkarte <i>Kontingent</i> des NTFS-Volumes.
Ereignis protokollieren, wenn die Datenträgerkontingentsgrenze überschritten wird	Gibt an, ob ein Ereignis protokolliert wird, wenn Benutzer ihre Kontingentsgrenze erreichen. Hindert Benutzer an der Änderung ihrer Protokolloptionen.
Ereignis protokollieren, wenn die Kontingentwarnstufe überschritten wird	Gibt an, ob ein Ereignis protokolliert wird, wenn Benutzer die Warnstufe erreichen.
Richtlinie auf austauschbare Datenträger anwenden	Legt fest, ob Kontingentrichtlinien auf NTFS-Volumes von Wechselmedien erweitert werden. Wenn Sie diese Richtlinie nicht aktivieren, gelten Kontingente nur für fest installierte Festplatten.
Standarddatenträgerkontingent und Warnstufe festlegen	Legt ein Standarddatenträgerkontingent und eine Warnstufe für alle Benutzer fest. Diese Einstellung hat Vorrang vor allen anderen Einstellungen und gilt nur für neue Benutzer eines Volumes.

Konfigurieren von Datenträgerkontingentrichtlinien

Richtlinien, die Datenträgerkontingente kontrollieren, gelten für den ganzen Computer. Sie finden diese Richtlinien unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Datenträgerkontingente*. Tabelle 5.1 listet die verfügbaren Richtlinien auf.

Wenn Sie mit Datenträgerkontingenten arbeiten, werden Sie vermutlich auf allen Systemen einheitliche Richtlinien verwenden. Im Normalfall werden Sie aber nicht alle verfügbaren Richtlinien einsetzen. Stattdessen aktivieren Sie selektiv die erforderlichen Richtlinien und verwenden dann die NTFS-Standardfunktionen zur Kontrolle der Kontingente auf den verschiedenen Volumes. Wenn Sie Datenträgerkontingente festlegen möchten, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor für den Standort, die Domäne oder die Organisationseinheit, mit der Sie arbeiten möchten. Die Datenträgerkontingentrichtlinien finden Sie unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Datenträgerkontingente*.
2. Tippen oder klicken Sie doppelt auf *Datenträgerkontingente ermöglichen*. Wählen Sie die Option *Aktiviert* aus und tippen oder klicken Sie auf *OK*.
3. Tippen oder klicken Sie doppelt auf *Datenträgerkontingentsgrenze erzwingen*. Wenn Sie auf allen NTFS-Volumes des Computers Datenträgerkontingente durchsetzen wollen, wählen Sie *Aktiviert*. Andernfalls wählen Sie *Deaktiviert* und legen dann auf Volumebasis die gewünschten Grenzen fest, wie in Kapitel 14 beschrieben. Tippen oder klicken Sie auf *OK*.

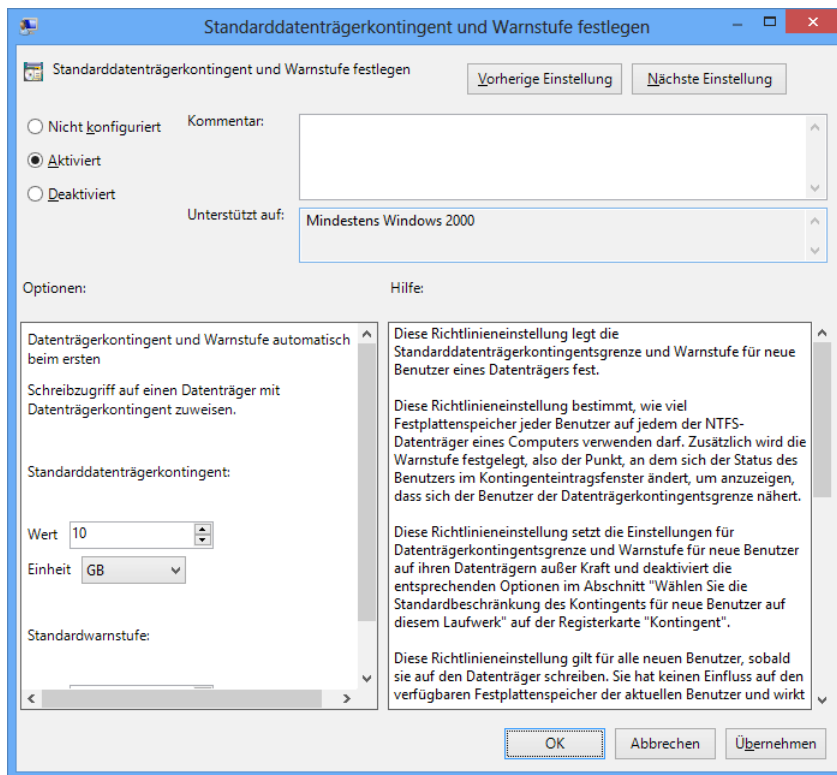


Abbildung 5.6 Mit dem Eigenschaftendialogfeld *Standarddatenträgerkontingent und Warnstufe festlegen* legen Sie Werte für Datenträgerkontingente fest

4. Tippen oder klicken Sie *Standarddaten trägerkontingent und Warnstufe festlegen* doppelt an. Das Dialogfeld *Eigenschaften von Standarddaten trägerkontingent und Warnstufe* öffnet sich (Abbildung 5.6). Wählen Sie *Aktiviert*.
5. Blättern Sie gegebenenfalls im Optionsfeld nach unten. Legen Sie unter *Standarddaten trägerkontingent* das Kontingent fest, das neuen Benutzern bei ihrem ersten Schreibzugriff auf das kontingentierte Volume zugestanden wird. Das Kontingent gilt nicht für aktuelle Benutzer und wirkt sich nicht auf aktuelle Kontingente aus. 1 bis 5 GByte sind in einer Organisation oft ein brauchbarer Wert, beispielsweise für ein freigegebenes Verzeichnis, das von den Mitgliedern einer Arbeitsgruppe verwendet wird. Welche Einstellung sinnvoll ist, hängt natürlich von der Datenmenge ab, mit der es die Benutzer routinemäßig zu tun haben. Grafikdesigner und Ingenieure werden vermutlich wesentlich mehr Platz brauchen.
6. Blättern Sie im Optionsfeld nach unten, bis Sie die Warnstufe einstellen können. 90 Prozent des Standarddaten trägerkontingents sind ein guter Wert. Wenn Sie also ein Standarddaten trägerkontingent von 10 GByte festlegen, dann stellen Sie die Warnstufe auf 9 GByte ein. Tippen oder klicken Sie auf *OK*.
7. Tippen oder klicken Sie *Ereignis protokollieren, wenn die Daten trägerkontingentsgrenze überschritten wird* doppelt an. Wählen Sie *Aktiviert*, damit alle Kontingentereignisse im Anwendungsprotokoll erfasst werden. Tippen oder klicken Sie auf *OK*.
8. Tippen oder klicken Sie *Ereignis protokollieren, wenn die Kontingentwarnstufe überschritten wird* doppelt an. Wählen Sie *Aktiviert*, damit alle Kontingentwarnungen im Anwendungsprotokoll erfasst werden. Tippen oder klicken Sie auf *OK*.
9. Tippen oder klicken Sie *Richtlinie auf austauschbare Datenträger anwenden* doppelt an. Wählen Sie *Deaktiviert*, damit die Kontingente nur für fest im Computer installierte Volumes gelten. Tippen oder klicken Sie auf *OK*.

Konfigurieren von Systemwiederherstellungsrichtlinien

Die Systemwiederherstellung dient dazu, den Zustand der Systemvolumes zu speichern und Benutzer in die Lage zu versetzen, ein System im Fall eines Problems wiederherzustellen. Es ist zwar für den durchschnittlichen Benutzer eine durchaus sinnvolle Funktion, aber sie kann auch einen beträchtlichen Teil des Speicherplatzes beanspruchen. Wie in Kapitel 2, »Konfigurieren von Windows 8-Computern«, beschrieben, können Sie die Systemwiederherstellung für ausgewählte Laufwerke oder für alle Laufwerke eines Computers abschalten.

Im Gruppenrichtlinienverwaltungs-Editor finden Sie die Systemwiederherstellungsrichtlinien unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Systemwiederherstellung*. Mit den Systemwiederherstellungsrichtlinien können Sie diese Funktion verwalten und deaktivieren. Folgende Richtlinien sind verfügbar:

- **Systemwiederherstellung deaktivieren** Wenn Sie diese Richtlinie aktivieren, wird die Systemwiederherstellung abgeschaltet und lässt sich auch nicht mehr in der *System*-Konsole oder mit dem Systemwiederherstellungs-Assistenten verwalten. Wenn Sie diese Richtlinie aktivieren, wird die Systemwiederherstellung durchgesetzt und lässt sich nicht abschalten.
- **Konfiguration deaktivieren** Wenn Sie diese Richtlinie aktivieren, verhindern Sie die Konfiguration der Systemwiederherstellungsfunktion. Benutzer können nicht auf die Registerkarte *Computerschutz* zugreifen. Wenn Sie diese Richtlinie deaktivieren, können Benutzer auf die Registerkarte *Computerschutz* zugreifen, sie aber nicht zur Konfiguration der Systemwiederherstellung benutzen.

Zur Einstellung der Systemwiederherstellungsrichtlinien gehen Sie folgendermaßen vor:

1. Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor für den Standort, die Domäne oder die Organisationseinheit, mit der Sie arbeiten möchten. Tippen oder klicken Sie dann auf den Ordner *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Systemwiederherstellung*.
2. Zur Aktivierung oder Deaktivierung der Systemwiederherstellung klicken Sie doppelt auf *Systemwiederherstellung deaktivieren*. Wählen Sie die Option *Aktiviert* oder *Deaktiviert*. Tippen oder klicken Sie auf *OK*.
3. Zur Aktivierung oder Deaktivierung der Konfiguration der Systemwiederherstellung klicken Sie doppelt auf *Konfiguration deaktivieren*. Wählen Sie die Option *Aktiviert* oder *Deaktiviert*. Tippen oder klicken Sie auf *OK*.

Konfigurieren von Offlinedateirichtlinien

Offlinedateirichtlinien werden auf Computer- und Benutzerebene festgelegt. Es gibt auf beiden Ebenen Richtlinien mit gleichen Namen. Wenn Sie auf beiden Ebenen mit Richtlinien gleichen Namens arbeiten, vergessen Sie bitte nicht, dass Computerrichtlinien Vorrang vor Benutzerrichtlinien haben und dass diese Richtlinien zu unterschiedlichen Zeitpunkten angewendet werden.

Tabelle 5.2 beschreibt die wichtigsten Richtlinien. Wie aus der Tabelle hervorgeht, betreffen die meisten Offlinedateirichtlinien den Zugriff, die Synchronisation, die Zwischenspeicherung und die Verschlüsselung. Sie finden Offlinedateirichtlinien unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Offlinedateien* und *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Offlinedateien*.

Einstellen von Richtlinien für die Offlinedateikonfiguration

Sie können als Administrator kontrollieren, welche Dateien und Ordner für die Offlineverwendung zur Verfügung stehen. Gewöhnlich ist das auf Dateiservern und anderen Systemen erforderlich, die freigegebene Ressourcen im Netzwerk anbieten. Sie können auf verschiedene Weise kontrollieren, welche Ressourcen offline zur Verfügung stehen.

Gehen Sie zur Einstellung der Offlinedateirichtlinien folgendermaßen vor:

1. Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor für den Standort, die Domäne oder die Organisationseinheit, mit der Sie arbeiten möchten. Die meisten Offlinedateirichtlinien lassen sich im entsprechenden *Offlinedateien*-Ordner als Computer- oder Benutzerrichtlinien einstellen, wobei Computerrichtlinien standardmäßig Vorrang haben. Sie finden die Richtlinien für Offlinedateien unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Offlinedateien* oder *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Offlinedateien*, sofern es im Folgenden nicht anders angegeben wird.
2. Zur Zuweisung der Ressourcen, die automatisch offline verfügbar sein sollen, tippen oder klicken Sie *Vom Administrator zugewiesene Offlinedateien angeben* doppelt an. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie dann auf *Anzeigen*. Geben Sie im Dialogfeld *Inhalt anzeigen* die Ressourcen mit ihrem UNC-Pfad an, wie zum Beispiel *\\Corpservers23\Data*. Abbildung 5.7 zeigt eine Liste von Ressourcen, die im Dialogfeld *Inhalt anzeigen* eingetragen wurden. Schließen Sie alle geöffneten Dialogfelder, indem Sie jeweils *OK* antippen oder anklicken.

Tabelle 5.2 Offlinedatei richtlinien

Richtlinientyp	Richtlinienname	Beschreibung
Computer	Die Funktion "Offline-dateien" zulassen bzw. nicht zulassen	Aktiviert oder deaktiviert die Offlinedateifunktion und kann nicht durch Benutzer außer Kraft gesetzt werden. Ermöglicht die administrative Kontrolle der Offlinedateieinstellungen eines Systems.
Computer	Hintergrundsynchronisierung konfigurieren	Steuert die Hintergrundsynchronisierung bei langsamen Verbindungen. Aktiviert: Die Hintergrundsynchronisierung wird regelmäßig durchgeführt, um Dateien in freigegebenen Ordnern zwischen dem Client und dem Server zu synchronisieren. Deaktiviert: Es wird das Standardverhalten für die Hintergrundsynchronisierung benutzt.
Computer	Modus für langsame Verbindungen konfigurieren	Steuert, wie langsame Verbindungen verwendet werden. Aktiviert: Für jeden freigegebenen Ordner, für den der Offlinedateicache verwendet wird, wird der Modus für langsame Verbindungen eingestellt. Deaktiviert: Für Offlinedateien wird nicht der Modus für langsame Verbindungen verwendet.
Computer	Dateiprüfungen aktivieren	Legt fest, welche Dateitypen sich nicht in einem Offlineordner speichern lassen. Aktiviert: Benutzer können keine Dateien mit bestimmten Dateinamenserweiterungen erstellen. Deaktiviert: Benutzer können in Offlineordnern beliebige Dateitypen erstellen.
Computer	Dateisynchronisierung für kostenbezogene Netzwerke aktivieren	Legt fest, ob Offlinedateien über langsame Netzwerke im Hintergrund synchronisiert werden, wenn dadurch zusätzliche Kosten entstehen. Aktiviert: Eine Synchronisierung kann erfolgen, wenn der Benutzer ein Roaming-Netzwerk verwendet und das Datenlimit für dieses Netzwerk beinahe erreicht oder überschritten ist. Deaktiviert: Es erfolgt keine Synchronisierung im Hintergrund.
Computer	Transparentes Zwischenspeichern aktivieren	Steuert die Zwischenspeicherung von Netzwerkdateien über langsame Verbindungen. Aktiviert: Optimiert die Zwischenspeicherung auf dem Client, damit möglichst wenig Übertragungen über langsame Verbindungen notwendig sind. Deaktiviert: Die transparente Zwischenspeicherung wird nicht benutzt.
Computer	Offlinedateicache verschlüsseln	Legt fest, ob Offlinedateien zur Erhöhung der Sicherheit verschlüsselt werden.
Computer	Nicht zwischengespeicherte Dateien	Nennt die Dateitypen (Dateinamenserweiterungen), die nicht offline verwendet werden können.
Computer	Von Offlinedateien verwendeten Speicherplatz begrenzen	Begrenzt den Festplattenplatz, der zum Speichern von Offlinedateien benutzt werden darf.
Computer	Wirtschaftliche Verwendung der vom Administrator zugewiesenen Offlinedateien konfigurieren	Bestimmt, wie vom Administrator zugewiesene Offlinedateien bei der Anmeldung synchronisiert werden. Aktiviert: Nur neue Dateien und Ordner werden bei der Anmeldung synchronisiert. Deaktiviert: Alle Dateien und Ordner werden bei der Anmeldung synchronisiert.
Computer/ Benutzer	Befehl "Offline verfügbar machen" entfernen	Verhindert, dass Benutzer Dateien offline verfügbar machen.
Computer/ Benutzer	Befehl "Offline arbeiten" entfernen	Entfernt die Option "Offline arbeiten" aus dem Datei-Explorer, damit Benutzer nicht manuell einstellen können, ob sich Offlinedateien im Offline- oder Onlinemodus befinden.
Computer/ Benutzer	Vom Administrator zugewiesene Offlinedateien angeben	Gibt mit UNC-Pfaden (Universal Naming Convention) die Dateien und Ordner an, die immer offline verfügbar sind.

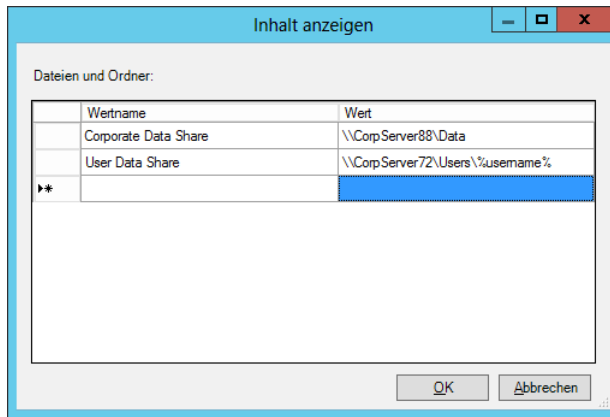


Abbildung 5.7 Verwenden Sie das Dialogfeld *Inhalt anzeigen*, um den UNC-Pfad der Ressourcen anzugeben, die automatisch offline verfügbar sein sollen

ACHTUNG Sie sollten sorgfältig abwägen, welche Ressourcen automatisch offline verfügbar gemacht werden. Je mehr Ressourcen auf diese Weise zugewiesen werden, desto mehr Datenübertragungen sind im Netzwerk erforderlich, um die Offlinedateizwischenspeicher zu aktualisieren.

3. Um zu verhindern, dass Benutzer Dateien und Ordner offline verfügbar machen, tippen oder klicken Sie *Befehl "Offline verfügbar machen" entfernen* doppelt an. Wählen Sie *Aktiviert* und tippen oder klicken Sie dann auf *OK*. Sobald diese Richtlinie in Kraft tritt, können Benutzer keine Dateien mehr für die Offlineverwendung aussuchen.
4. Um festzulegen, welche Dateitypen nicht in Offlineordnern erstellt werden können, tippen oder klicken Sie *Dateiprüfungen aktivieren* doppelt an. Wählen Sie *Aktiviert*. Geben Sie im Textfeld *Erweiterungen* die Dateinamenserweiterungen, die ausgeschlossen werden sollen, durch Semikolons getrennt ein und tippen oder klicken Sie dann auf *OK*. Erweiterungen müssen mit einem Sternchen und einem Punkt anfangen, wie *.vbs oder *.js. Wenn diese Richtlinie in Kraft tritt, können Benutzer in Offlineordnern keine Dateien mit den angegebenen Erweiterungen mehr erstellen.
5. Unter Windows 8 und höher können Sie *Befehl "Offline arbeiten" entfernen* doppelt antippen oder anklicken und dann *Aktiviert* wählen. Sobald diese Option in Kraft tritt, können Benutzer nicht mehr manuell ändern, welche Offlinedateien sich im Offline- oder Onlinemodus befinden. Allerdings können sie weiterhin Offlinedateien verwenden.

In Windows Vista und höher werden Offlinedateien automatisch synchronisiert, wobei immer die Hintergrundsynchonisierung benutzt wird, während der Computer mit einem langsamen Netzwerk verbunden ist. Als langsames Netzwerk wird unter Windows 8 und höher ein Netzwerk eingestuft, das eine Latenz von mehr als 35 Millisekunden aufweist. Gewöhnlich wird ein Netzwerk mit einer Latenz von mehr als 80 Millisekunden als langsam betrachtet.

Sie können verhindern, dass ein Computer, auf dem Windows Vista oder höher ausgeführt wird, in den Modus für langsame Verbindungen wechselt und somit die Hintergrundsynchonisierung nutzt, indem Sie die Richtlinie *Modus für langsame Verbindungen konfigurieren* deaktivieren. Wenn Sie diese Richtlinie aktivieren, können Sie auf der Basis von Latenz und Datendurchsatz festlegen, wann die Verbindungen als langsam eingestuft werden sollen.

So konfigurieren Sie langsame Verbindungen:

1. Öffnen Sie den Gruppenrichtlinienverwaltungs-Editor für den Standort, die Domäne oder die Organisationseinheit, mit der Sie arbeiten möchten. Erweitern Sie dann den Knoten *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Offlinedateien*.
2. Um die Schwellenwerte für die Einstufung einer Verbindung als langsame Verbindung einzustellen, tippen oder klicken Sie doppelt auf *Modus für langsame Verbindungen konfigurieren*. Wählen Sie *Aktiviert* und tippen oder klicken Sie auf *Anzeigen* (wahrscheinlich müssen Sie im Feld *Optionen* einen Bildlauf durchführen, um *Anzeigen* zu sehen). Geben Sie im Dialogfeld *Inhalt anzeigen* unter *Wertname* die zu verwaltenden Ressourcen an und unter *Wert* die Einstellungen für Durchsatz und Latenz. Berücksichtigen Sie dabei Folgendes:
 - In *Wertname* können Sie die UNC-Pfade einzelner Server angeben. Geben Sie zum Beispiel `\\corpserver172\*` ein, um die Schwellenwerte für alle Freigaben auf CorpServer172 festzulegen, oder `\\corpserver85\data\*`, um die Schwellenwerte für Dateien und Ordner im Ordner *Data* von CorpServer85 festzulegen.
 - In *Wertname* können Sie Werte festlegen, die für alle Server aus dem Wirkungsbereich der Richtlinie gelten, indem Sie ein Sternchen (*) eingeben.
 - In *Wert* können Sie Schwellenwerte für den Durchsatz (in Bit pro Sekunde) angeben, für die Latenz (in Millisekunden) oder für beides. Geben Sie zum Beispiel **Durchsatz=1024** ein, wenn der Modus für langsame Verbindungen verwendet werden soll, falls der Durchsatz kleiner ist als 1024 Bit pro Sekunde. Geben Sie **Latenz=60** ein, wenn der Modus für langsame Verbindungen verwendet werden soll, wenn die Netzwerklatenz über 60 Millisekunden liegt, oder geben Sie **Durchsatz=1024, Latenz=60** ein, wenn beide Schwellenwerte gelten sollen.

Abbildung 5.8 zeigt eine Liste der Ressourcen, die im Dialogfeld *Inhalt anzeigen* eingetragen wurden. Tippen oder klicken Sie auf *OK*, bis alle offenen Dialogfelder geschlossen sind.

ACHTUNG

Sie sollten sorgfältig prüfen, welche Ressourcen automatisch offline verfügbar gemacht werden sollen. Je mehr Ressourcen Sie auf diese Weise verfügbar machen, desto mehr Datenverkehr ist im Netzwerk erforderlich, um die Zwischenspeicher für Offlinedateien zu aktualisieren.

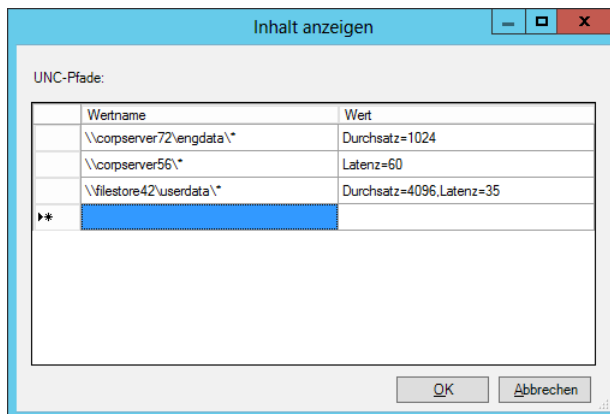


Abbildung 5.8 Legen Sie im Dialogfeld *Inhalt anzeigen* die Schwellenwerte für den Modus für langsame Verbindungen fest.

4. Standardmäßig führt Windows die Synchronisierung beim Modus für langsame Verbindungen im Hintergrund durch. Sie erfolgt jeweils nach etwa 6 Stunden. Zur genaueren Einstellung der Hintergrundsynchonisierung tippen oder klicken Sie doppelt auf *Hintergrundsynchronisierung konfigurieren*. Wählen Sie *Aktiviert*, nehmen Sie die erforderlichen Einstellungen vor und tippen oder klicken Sie dann auf *OK*. Berücksichtigen Sie bei der Konfiguration der Hintergrundsynchonisierung folgendes:
 - *Synchronisierungsintervall* und *Synchronisierungsabweichung* werden zusammen verwendet, um das Aktualisierungsintervall festzulegen. Standardmäßig beträgt das Synchronisierungsintervall 360 Minuten, mit einer Synchronisierungsabweichung bis zu 60 Minuten, um zu verhindern, dass viele Clients zur selben Zeit das Netzwerk und die Server belasten.
 - Sorgen Sie mit *Maximal zulässige Zeit ohne Synchronisierung* dafür, dass alle Netzwerkordner regelmäßig aktualisiert werden. Der Wert wird in Minuten festgelegt. Wenn Sie also sicherstellen möchten, dass Netzwerkordner mindestens einmal am Tag aktualisiert werden, geben Sie den Wert **1440** ein.
 - Mit *Startzeit der Sperre* und *Dauer der Sperre* können Sie erreichen, dass zu bestimmten Tageszeiten keine Aktualisierung erfolgt. Als Startzeit wird die Uhrzeit angegeben, während die Dauer in Minuten angegeben wird. Wenn Sie also erreichen möchten, dass die Netzwerkordner zwischen 14 und 18 Uhr nicht aktualisiert werden, geben Sie die Startzeit **1400** und die Dauer **240** ein.
4. Unter Windows 8 und höher können Sie mit *Dateisynchronisierung für kostenbezogene Netzwerke aktivieren* steuern, ob eine Hintergrundsynchonisierung über Mobiltelefonnetze und andere Netze erfolgen darf, wenn dadurch zusätzliche Kosten durch wechselnde Standorte oder durch das Überschreiten von Datenlimits entstehen. Standardmäßig ist die Synchronisierung über kostenbezogene Netzwerke deaktiviert. Um sie zu aktivieren, tippen oder klicken Sie doppelt auf *Dateisynchronisierung für kostenbezogene Netzwerke aktivieren*, wählen *Aktiviert* und tippen oder klicken dann auf *OK*.

Verwenden von Zugriffs- und Verbindungsrichtlinien

Zugriffs- und Verbindungsrichtlinien kontrollieren Netzwerkverbindungen, Wählverbindungen und Remoteunterstützungskonfigurationen. Diese Richtlinien haben Einfluss auf die Verbindung eines Systems mit dem Netzwerk und auf den Remotezugriff auf das System.

Konfigurieren von Netzwerkrichtlinien

Es gibt viele Richtlinien für Netzwerke. Netzwerkrichtlinien, die gemeinsame Internetverbindungen, Internetverbindungsfirewall, Windows-Firewall und Netzwerkbridge kontrollieren, werden auf Computerebene konfiguriert. Netzwerkrichtlinien, die LAN-Verbindungen, die TCP/IP-Konfiguration und den Remotezugriff kontrollieren, werden auf Benutzerebene konfiguriert. Tabelle 5.3 beschreibt die wichtigsten Richtlinien. Sie finden Netzwerkrichtlinien unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Netzwerkverbindungen* und *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Netzwerkverbindungen*.

Tabelle 5.3 Netzwerkrichtlinien

Richtlinientyp	Richtliniename	Beschreibung
Benutzer	Ändern von Eigenschaften einer für alle Benutzer gültigen RAS-Verbindung zulassen	Legt fest, ob Benutzer die Eigenschaften von RAS-Verbindungen anzeigen und ändern können, die für alle Benutzer des Computers verfügbar sind.
Benutzer	Löschen von RAS-Verbindungen nicht zulassen	Legt fest, ob Benutzer RAS-Verbindungen löschen können.
Computer	Gesamten Datenverkehr über das interne Netzwerk weiterleiten	Wird im Zusammenhang mit DirectAccess benutzt. Legt fest, ob Remotecomputer über das interne Unternehmensnetzwerk oder über ihre eigene Internetverbindung auf das Internet zugreifen.
Computer	Höhere Rechte von Domänenbenutzern beim Festlegen einer Netzwerkadresse anfordern	Legt fest, ob eine Anhebungsaufforderung angezeigt wird, bevor der Netzwerkstandort eingestellt werden darf.
Computer	Installation und Konfiguration der Netzwerkbridge im eigenen DNS-Domänen-netzwerk nicht zulassen	Legt fest, ob Benutzer Netzwerkbrücken installieren und konfigurieren können. Diese Richtlinie gilt nur in der Domäne, in der sie konfiguriert wird.

Wie aus Tabelle 5.3 hervorgeht, wurden die Netzwerkrichtlinien für Computer so konzipiert, dass sie Vorgänge im Netzwerk einer Organisation einschränken. Wenn Sie diese Richtlinien durchsetzen, werden Benutzer in den entsprechenden Domänen davon abgehalten, Dinge wie zum Beispiel gemeinsame Internetverbindungen zu nutzen. Das hat den Sinn, die Sicherheit des Firmennetzwerks zu schützen, hindert aber zum Beispiel Benutzer von Laptops nicht daran, ihre Computer mit nach Hause zu nehmen und diese Funktionen dort zu verwenden. Um diese Beschränkungen zu aktivieren oder zu deaktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie dann *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk* und tippen oder klicken Sie auf *Netzwerkverbindungen*.
2. Tippen oder klicken Sie die Richtlinie, die Sie konfigurieren möchten, doppelt an. Auf der Registerkarte *Einstellung* wählen Sie nach Bedarf *Aktiviert* oder *Deaktiviert*. Tippen oder klicken Sie auf dann OK.

Benutzerrichtlinien für Netzwerkverbindungen verhindern gewöhnlich den Zugang zu bestimmten Funktionen, beispielsweise zur erweiterten Einstellung von TCP/IP-Verbindungen. Diese Richtlinien konfigurieren Sie folgendermaßen:

1. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie dann *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk* und tippen oder klicken Sie auf *Netzwerkverbindungen*.
2. Tippen oder klicken Sie die Richtlinie, die Sie konfigurieren möchten, doppelt an. Auf der Registerkarte *Einstellung* wählen Sie nach Bedarf *Aktiviert* oder *Deaktiviert*. Tippen oder klicken Sie dann auf OK.

Konfigurieren von Remoteunterstützungsrichtlinien

Remoteunterstützungsrichtlinien eignen sich, um Remoteunterstützung auf Computern zuzulassen oder zu verhindern. Wenn Sie Remoteunterstützungsrichtlinien konfigurieren, möchten Sie vermutlich unerbetene Remoteunterstützungsangebote verhindern und angeforderte Unterstützungsangebote zulassen. Sie können mit den Richtlinien auch eine bestimmte Gültigkeitsdauer für Einladungen durchsetzen, statt die Einstellungen auf jedem Computer im Dialogfeld *Systemeigenschaften* vorzunehmen. Zur Verbesserung der Sicherheit können Sie Einladungen auch mit starker Verschlüsselung schützen. Allerdings schränkt diese Erweiterung den Kreis der potenziellen Helfer, die auf eine Remoteunterstützungseinladung antworten können, auf die Benutzer von Windows Vista oder höher ein.

Zur Einstellung der Richtlinien gehen Sie folgendermaßen vor:

1. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie dann *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Remoteunterstützung*.
2. Tippen oder klicken Sie *"Angeforderte Remoteunterstützung" konfigurieren* doppelt an und wählen Sie die Option *Aktiviert*. Ist die Richtlinie aktiviert, erlaubt sie autorisierten Benutzern die Antwort auf Remoteunterstützungseinladungen.

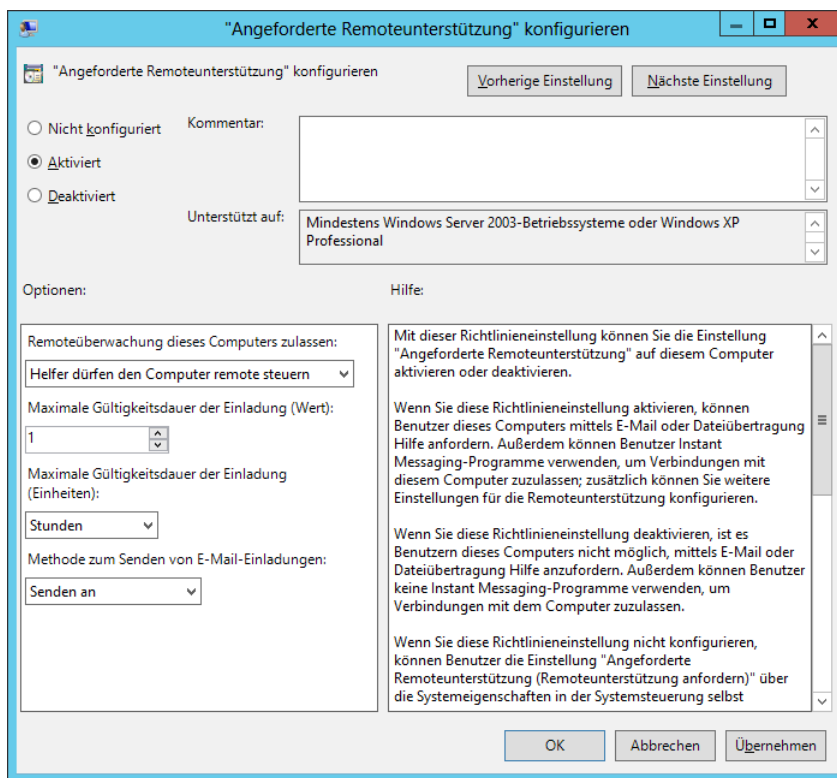


Abbildung 5.9 Legen Sie die Gültigkeitsdauer für Remoteunterstützungseinladungen fest

3. Nun können Sie die Zugriffsebene für Helfer festlegen. In der Auswahlliste *Remoteüberwachung dieses Computers zulassen* gibt es zwei Optionen:
 - **Helfer dürfen den Computer remote steuern** Erlaubt die Einsichtnahme und die Fernsteuerung des Computers.
 - **Helfer dürfen den Computer nur ansehen** Lässt nur eine Einsichtnahme zu. Helfer können nicht die Steuerung übernehmen, um Änderungen durchzuführen.
4. Dann legen Sie in den Feldern *Maximale Gültigkeitsdauer der Einladung (Wert)* und *Maximale Gültigkeitsdauer der Einladung (Einheiten)* die Gültigkeitsdauer von Remoteunterstützungseinladungen fest (Abbildung 5.9). Standardwert für die maximale Gültigkeitsdauer ist 1 Stunde. Tippen oder klicken Sie auf OK.

PRAXISTIPP

Für die Übermittlungsmethode für E-Mail-Einladungen stehen *Senden an* oder *Einfaches MAPI* zur Auswahl. Mit *Senden an* ist eine Mailübermittlungsmethode auf Browserbasis gemeint, bei welcher der Empfänger der Einladung über einen Internetlink eine Verbindung herstellt. Sie können auch *Einfaches MAPI* einstellen, um die E-Mail-Einladung mit MAPI (Messaging Application Programming Interface) zu versenden. In diesem Fall wird die Einladung als Anhang einer Einladungs-E-Mail versendet. Solange beide beteiligten Computer über Port 80 eine Verbindung herstellen können und Sie für Ihre E-Mail ein Standardprogramm verwenden wie Microsoft Outlook oder Windows Mail, werden Sie vermutlich *Senden an* verwenden.

5. Tippen oder klicken Sie *"Remoteunterstützung anbieten" konfigurieren* doppelt an. Im Dialogfeld *"Remoteunterstützung anbieten" konfigurieren* wählen Sie *Deaktiviert*. Die Deaktivierung dieser Richtlinie verhindert unerbetene Unterstützungsangebote. Tippen oder klicken Sie auf OK.
6. Wenn Sie eine starke Verschlüsselung einsetzen und Verbindungen auf Computer beschränken möchten, auf denen Windows Vista, Windows 7, Windows 8 oder höher ausgeführt wird, tippen oder klicken Sie *Nur Verbindungen von Computern mit Windows Vista oder höher zulassen* doppelt an. Im Dialogfeld *Nur Verbindungen von Computern mit Windows Vista oder höher zulassen* wählen Sie *Aktiviert*. Tippen oder klicken Sie auf OK.

Um Remoteunterstützung und Remotesteuerung zu sperren, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Remoteunterstützung*.
2. Tippen oder klicken Sie *"Angeforderte Remoteunterstützung" konfigurieren* doppelt an. Wählen Sie die Option *Deaktiviert* und klicken Sie auf *Nächste Einstellung*.
3. Im Dialogfeld *"Remoteunterstützung anbieten" konfigurieren* wählen Sie *Deaktiviert* und tippen oder klicken auf OK.

Verwenden von Computer- und Benutzerskriptrichtlinien

Skriptrichtlinien steuern die Ausführung und Verwendung von Computer- und Benutzerskripts. Es lassen sich vier Arten von Skripten konfigurieren:

- **Startskripts** Werden während des Starts des Computers ausgeführt.
- **Skripts zum Herunterfahren** Werden vor dem Herunterfahren des Computers ausgeführt.
- **Anmeldeskripts** Werden bei der Anmeldung eines Benutzers ausgeführt.
- **Abmeldeskripts** Werden bei der Abmeldung eines Benutzers ausgeführt.

Sie können diese Skripts als Batchdatei für die Eingabeaufforderung, als Windows-Skripts oder als Windows PowerShell-Skripts schreiben. Batchskripts verwenden die Befehlssprache der Shell. Windows-Skripts verwenden den Windows Script Host (WSH) und werden in einer Skriptsprache wie VBScript (Microsoft Visual Basic, Scripting Edition) oder Microsoft JScript geschrieben. Windows PowerShell-Skripts sind in der PowerShell-Sprache geschrieben. Beachten Sie, dass unverwaltete Richtlinieneinstellungen die Ausführung von Computer- und Benutzerskripten in vielen Fällen überflüssig machen.

Steuern der Skriptausführung durch Richtlinien

Richtlinien zur Steuerung der Skriptausführung finden sich unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Skripts* und *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\System\Skripts*. Mit den entsprechenden Richtlinien können Sie die Ausführung der Startskripts, der Skripts zum Herunterfahren, der Anmelde- und Abmeldeskripts steuern. Tabelle 5.4 beschreibt die wichtigsten Richtlinien. Sie sehen, es gibt eine ganze Reihe von Optionen zur Steuerung der Skriptausführung.

Tabelle 5.4 Computer- und Benutzerskriptrichtlinien

Richtlinientyp	Richtlinienname	Beschreibung
Benutzer	Anweisungen in Abmeldeskripts während der Ausführung anzeigen	Zeigt Abmeldeskripts und ihre Befehle bei ihrer Ausführung an.
Benutzer	Anweisungen in Anmeldeskripts während der Ausführung anzeigen	Zeigt Anmeldeskripts und ihre Befehle bei ihrer Ausführung an.
Benutzer	Legacy-Anmeldeskripts im Hintergrund ausführen	Blendet Anmeldeskripts aus, die unter Windows NT 4 mit dem Systemrichtlinien-Editor konfiguriert wurden.
Computer	Maximale Wartezeit für Gruppenrichtlinienskripts angeben	Legt die Zeitspanne fest, die das System maximal darauf wartet, dass die Ausführung eines Skripts beendet wird. Der Standardwert ist 600 Sekunden (10 Minuten).
Computer	Anweisungen in Abmeldeskripts während der Ausführung anzeigen	Zeigt die Skripts zum Herunterfahren und ihre Befehle bei ihrer Ausführung an.
Computer	Anweisungen in Startskripts während der Ausführung anzeigen	Zeigt Startskripts und ihre Befehle bei ihrer Ausführung an.
Computer	Startskripts asynchron ausführen	Mit dieser Einstellung können Skripts auch gleichzeitig ausgeführt werden statt nacheinander.
Computer	Windows-PowerShell-Skripts beim Starten und Herunterfahren des Computers zuerst ausführen	Legt fest, ob Windows PowerShell-Skripts beim Starten und Herunterfahren des Systems vor anderen Skripttypen ausgeführt werden.
Computer/ Benutzer	Anmeldeskripts gleichzeitig ausführen	Sorgt dafür, dass das System wartet, bis die Ausführung der Anmeldeskripts abgeschlossen ist, bevor es die Windows-Benutzeroberfläche anzeigt.
Computer/ Benutzer	Windows-PowerShell-Skripts beim Anmelden und Abmelden des Benutzers zuerst ausführen	Legt fest, ob Windows PowerShell-Skripts beim An- und Abmelden vor anderen Skripttypen ausgeführt werden.

Es lassen sich zwar viele Richtlinienkombinationen konfigurieren, aber die üblichen Einstellungen sind folgende:

- Windows PowerShell-Skripts sollen zuerst ausgeführt werden.
- Anmelde- und Startskripts sollen gleichzeitig ausgeführt werden (zumindest in den meisten Fällen).
- Kein Skript soll bei der Ausführung sichtbar sein.
- Das System soll gewöhnlich nicht länger als 1 Minute darauf warten, dass die Ausführung eines Skripts beendet wird.

Zur Einstellung dieses Verhaltens gehen Sie folgendermaßen vor:

1. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie dann *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Skripts*.
2. Tippen oder klicken Sie doppelt auf *Windows-PowerShell-Skripts beim Starten und Herunterfahren des Computers zuerst ausführen*. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie auf OK.
3. Tippen oder klicken Sie doppelt auf *Windows-PowerShell-Skripts beim Anmelden und Abmelden des Benutzers zuerst ausführen*. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie auf OK.
4. Tippen oder klicken Sie doppelt auf *Anmeldeskripts gleichzeitig ausführen*. Wählen Sie die Option *Deaktiviert* und tippen oder klicken Sie auf OK.
5. Tippen oder klicken Sie doppelt auf *Startskripts asynchron ausführen*. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie auf OK.
6. Tippen oder klicken Sie doppelt auf *Anweisungen in Startskripts während der Ausführung anzeigen*. Wählen Sie die Option *Deaktiviert* und tippen oder klicken Sie auf OK.
7. Tippen oder klicken Sie doppelt auf *Anweisungen in Abmeldeskripts während der Ausführung anzeigen*. Wählen Sie die Option *Deaktiviert* und tippen oder klicken Sie auf OK.
8. Tippen oder klicken Sie doppelt auf *Maximale Wartezeit für Gruppenrichtlinienskripts angeben*. Wählen Sie die Option *Aktiviert* und geben Sie im Feld *Sekunden* den Wert 60 ein. Tippen oder klicken Sie auf OK.
9. Erweitern Sie *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\System\Skripts*.
10. Tippen oder klicken Sie doppelt auf *Legacy-Anmeldeskripts im Hintergrund ausführen*. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie auf OK.
11. Tippen oder klicken Sie doppelt auf *Anweisungen in Anmeldeskripts während der Ausführung anzeigen*. Wählen Sie die Option *Deaktiviert* und tippen oder klicken Sie auf OK.
12. Tippen oder klicken Sie doppelt auf *Anweisungen in Abmeldeskripts während der Ausführung anzeigen*. Wählen Sie die Option *Deaktiviert* und tippen oder klicken Sie auf OK.
13. Tippen oder klicken Sie doppelt auf *Windows-PowerShell-Skripts beim Anmelden und Abmelden des Benutzers zuerst ausführen*. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie auf OK.

Zuweisen von Computerskripts für das Starten und Herunterfahren

Computerskripts für das Starten und Herunterfahren lassen sich über Gruppenrichtlinien zuweisen. Auf diese Weise führt ein Computer – oder alle Computer, die Mitglieder des Standorts, der Domäne oder der Organisationseinheit sind – die Skripts automatisch aus, wenn er gestartet oder heruntergefahren wird.

Um Computerskripts zuzuweisen, gehen Sie so vor:

1. Kopieren Sie die Skripts, die Sie verwenden möchten, in den Ordner *Scripts\Startup* oder *Scripts\Shutdown* der entsprechenden Richtlinie, damit sie sich leichter verwalten lassen. Auf Domänencontrollern werden Skripts im Ordner *%SystemRoot%\sysvol\sysvol\%UserDnsDomain%\Policies\GUID\Machine* gespeichert und auf Windows 8-Arbeitsstationen im Ordner *%WinDir%\System32\GroupPolicy\Machine*.
2. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie dann *Computerkonfiguration\Windows-Einstellungen\Skripts*.
3. Wenn Sie Startskripts bearbeiten möchten, klicken Sie das Element *Starten* mit der rechten Maustaste an oder halten es gedrückt und wählen dann *Eigenschaften*. Um Skripts für das Herunterfahren zu bearbeiten, klicken Sie das Element *Herunterfahren* mit der rechten Maustaste an oder halten es gedrückt und wählen *Eigenschaften*. Tippen oder klicken Sie dann auf *Dateien anzeigen*. Sofern Sie die Computerskripts in den richtigen Ordner kopiert haben, sollten Sie die Skripts sehen, die Sie zuweisen wollen.
4. Tippen oder klicken Sie auf *Hinzufügen*, um ein Skript zuzuweisen. Dadurch öffnet sich das Dialogfeld *Hinzufügen eines Skripts*. Geben Sie im Textfeld *Skriptname* den Namen des Skripts ein, das Sie in den Ordner *Scripts\Startup* oder *Scripts\Shutdown* der Richtlinie kopiert haben. Im Textfeld *Skriptparameter* geben Sie die Parameter und Argumente ein, die an das Befehlszeilenskript oder an den Scripting Host für ein WSH-Skript übergeben werden sollen. Wiederholen Sie diesen Schritt für alle weiteren Skripts.
5. Die Skripts werden beim Start oder beim Herunterfahren in der Reihenfolge ausgeführt, in der sie im *Eigenschaften*-Dialogfeld aufgelistet werden. Wählen Sie ein Skript aus und tippen oder klicken Sie nach Bedarf auf *Nach oben* oder *Nach unten*, um die Reihenfolge zu ändern.
6. Wenn Sie später den Skriptnamen oder die Parameter ändern möchten, wählen Sie das Skript in der Skriptliste aus und tippen oder klicken auf *Bearbeiten*.
7. Um ein Skript zu löschen, wählen Sie das Skript in der Skriptliste aus und tippen oder klicken dann auf *Entfernen*.

Zuweisen von Benutzerskripts für An- und Abmeldung

Benutzerskripts lassen sich über Gruppenrichtlinien zuweisen. Auf diese Weise führen alle Benutzer, die auf einen Computer zugreifen oder Mitglieder des Standorts, der Domäne oder der Organisationseinheit sind, die Skripts automatisch aus, wenn sie sich an- oder abmelden.

Um Benutzerskripts zuzuweisen, gehen Sie folgendermaßen vor:

1. Kopieren Sie die Skripts, die Sie verwenden möchten, in die Ordner *Scripts\Logon* oder *Scripts\Logoff* der entsprechenden Richtlinie. Auf Domänencontrollern werden Skripts im Ordner *%SystemRoot%\sysvol\sysvol\%UserDnsDomain%\Policies\GUID\User* gespeichert und auf Windows 8-Arbeitsstationen im Ordner *%WinDir%\System32\GroupPolicy\User*.

2. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie dann *Benutzerkonfiguration\Windows-Einstellungen\Skripts*.
3. Wenn Sie Anmeldeskripts bearbeiten möchten, klicken Sie das Element *Anmelden* mit der rechten Maustaste an oder halten es gedrückt und wählen dann *Eigenschaften*. Um Abmeldeskripts zu bearbeiten, klicken Sie das Element *Abmelden* mit der rechten Maustaste an oder halten es gedrückt und wählen *Eigenschaften*. Tippen oder klicken Sie dann auf *Dateien anzeigen*. Sofern Sie die Benutzer-skripts in den richtigen Ordner kopiert haben, sollten Sie die Skripts sehen, die Sie zuweisen wollen.
4. Tippen oder klicken Sie auf *Hinzufügen*, um ein Skript zuzuweisen. Dadurch öffnet sich das Dialogfeld *Hinzufügen eines Skripts*. Geben Sie im Textfeld *Skriptname* den Namen des Skripts ein, das Sie in den Ordner *Scripts\Logon* oder *Scripts\Logoff* der Richtlinie kopiert haben. Im Textfeld *Skriptparameter* geben Sie die Parameter und Argumente ein, die an das Befehlszeilenskript oder an den Scripting Host für ein WSH-Skript übergeben werden sollen. Wiederholen Sie diesen Schritt für alle weiteren Skripts.
5. Die Skripts werden bei der An- oder Abmeldung in der Reihenfolge ausgeführt, in der sie im *Eigenschaften*-Dialogfeld aufgelistet werden. Wählen Sie einen Skriptnamen aus und tippen oder klicken Sie nach Bedarf auf *Nach oben* oder *Nach unten*, um die Reihenfolge zu ändern.
6. Wenn Sie später den Skriptnamen oder die Parameter ändern möchten, wählen Sie das Skript in der Skriptliste aus und tippen oder klicken dann auf *Bearbeiten*.
7. Um ein Skript zu löschen, wählen Sie es in der Skriptliste aus und tippen/klicken dann auf *Entfernen*.

Verwenden von Anmelde- und Startrichtlinien

Windows 8 bietet eine Reihe von Richtlinien, mit denen Sie den Anmeldevorgang kontrollieren können. Mit einigen dieser Richtlinien können Sie auch die Ausführung von Anwendungen bei der Anmeldung steuern. Das macht sie insofern mit Anmeldeskripts vergleichbar, als sie bei der Anmeldung bestimmte Arbeiten durchführen können. Andere Richtlinien wirken sich auf die Darstellung der Willkommenseite und des Anmeldebildschirms aus. Die wichtigsten Anmelde- und Startrichtlinien finden Sie unter *Computerkonfiguration* und *Benutzerkonfiguration* jeweils in *Administrative Vorlagen\System\Anmelden*, Tabelle 5.5 fasst diese Richtlinien zusammen.

Einstellen der Autostartrichtlinien

Benutzer können ihre Autostartanwendungen zwar separat konfigurieren, aber in Unternehmen, in denen bestimmte Benutzergruppen mit denselben Anwendungen arbeiten, ist es gewöhnlich sinnvoller, dies durch Richtlinien zu erledigen. Wenn Sie erreichen möchten, dass bestimmte Programme bei der Anmeldung automatisch gestartet werden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie dann *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Anmelden*.
2. Tippen oder klicken Sie doppelt auf *Diese Programme bei der Benutzeranmeldung ausführen* und wählen Sie die Option *Aktiviert* aus.
3. Tippen oder klicken Sie auf *Anzeigen*. Geben Sie im Dialogfeld *Inhalt anzeigen* die vollständigen UNC-Pfade der Anwendungen an, wie zum Beispiel *C:\Program Files (x86)\Internet Explorer\explore.exe* oder *\\DCServ01\Apps\Stats.exe*.
4. Schließen Sie alle offenen Dialogfelder.

Tabelle 5.5 Anmelde- und Startrichtlinien

Richtlinientyp	Richtliniename	Beschreibung
Computer	Anmeldung mit Bildcode deaktivieren	Wenn Sie diese Richtlinieneinstellung aktivieren, können Domänenbenutzer keinen Bildcode einrichten und sich nicht mit ihm anmelden.
Computer	Anwendungsbenachrichtigungen auf gesperrtem Bildschirm deaktivieren	Verhindert, dass auf dem gesperrten Bildschirm Anwendungsbenachrichtigungen angezeigt werden.
Computer	Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten	Legt fest, dass der Computer wartet, bis das Netzwerk vollständig initialisiert ist. Beim Start werden dann die aktuellen Richtlinien und Daten verwendet und keine zwischengespeicherten Daten. Das bedeutet zum Beispiel für die Anmeldung, dass kein zwischengespeichertes Benutzerkonto verwendet wird, sondern dass die Authentifizierung beim Domänencontroller durchgeführt werden muss.
Computer	Immer benutzerdefinierten Anmeldehintergrund verwenden	Erlaubt es, einen benutzerdefinierten Hintergrund für die Anmeldeseite zu verwenden.
Computer	Immer klassische Anmeldung verwenden	Tauscht unter Windows 7 und älter den einfachen Standardanmeldebildschirm gegen den Anmeldebildschirm aus, der aus früheren Windows-Versionen bekannt ist.
Computer	Lokale Benutzer auf Computern, die der Domäne angehören, auflisten	Ermöglicht es, lokale Benutzer auf dem Anmeldebildschirm aufzulisten.
Computer	Verbundene Benutzer auf Computern, die der Domäne angehören, nicht auflisten	Verhindert, dass verbundene Benutzer auf dem Anmeldebildschirm aufgelistet werden.
Computer	PIN-Anmeldung aktivieren	Ermöglicht Domänenbenutzern die Anmeldung mit einer PIN.
Computer/ Benutzer	Diese Programme bei der Benutzeranmeldung ausführen	Legt Programme fest, die bei der Benutzeranmeldung automatisch gestartet werden sollen. Geben Sie den vollständigen Pfadnamen an (sofern das Programm nicht in %SystemRoot% liegt).
Computer/ Benutzer	Einmalige Ausführungsliste nicht verarbeiten	Zwingt das System dazu, benutzerdefinierte einmalige Ausführungslisten zu ignorieren.
Computer/ Benutzer	Herkömmliche Ausführungsliste nicht verarbeiten	Ignoriert alle Autostartanwendungen bis auf die, die unter Windows NT 4 mit dem Systemrichtlinien-Editor festgelegt wurden.

Deaktivieren von Ausführungslisten durch Gruppenrichtlinien

Durch Richtlinien können Sie die alten Ausführungslisten ebenso deaktivieren wie Listen für die einmalige Ausführung (Run-Once-Listen). Ausführungslisten sind in der Registrierung unter *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* und *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run* gespeichert.

Listen für die einmalige Ausführung können von Administratoren erstellt werden und geben Programme an, die beim nächsten Systemstart einmal ausgeführt werden sollen, aber bei den darauf folgenden Systemstarts nicht mehr. Listen für die einmalige Ausführung sind in der Registrierung unter *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce* und *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce* gespeichert.

Gehen Sie folgendermaßen vor, um Ausführungslisten zu deaktivieren:

1. Öffnen Sie das Gruppenrichtlinienobjekt, das Sie verwenden möchten, im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie dann *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Anmelden* oder *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\System\Anmelden*.
2. Tippen oder klicken Sie doppelt auf *Einmalige Ausführungsliste nicht verarbeiten*. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie auf OK.
3. Tippen oder klicken Sie doppelt auf *Herkömmliche Ausführungsliste nicht verarbeiten*. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie auf OK.

Kapitel 6

Automatisieren der Windows 8-Konfiguration

In diesem Kapitel:

Grundlagen von Gruppenrichtlinieneinstellungen	214
Konfigurieren von Gruppenrichtlinieneinstellungen	216
Verwalten von Einstellungselementen	220

Mit unverwalteten Gruppenrichtlinieneinstellungen können Sie Betriebssystem- und Anwendungseinstellungen automatisch konfigurieren, bereitstellen und verwalten. Dazu gehören unter anderem Einstellungen für Datenquellen, zugeordnete Laufwerke, Umgebungsvariablen, Netzwerkfreigaben, Ordneroptionen und Verknüpfungen. Wenn Sie Computer bereitstellen und einrichten, werden Sie feststellen, dass es einfacher ist, Gruppenrichtlinieneinstellungen zu verwenden, als dieselben Einstellungen auf jedem einzelnen Computer von Hand zu konfigurieren, in Windows-Abbildern einzurichten oder durch Start-, Anmelde-, Herunterfahren- und Abmeldeskripts festzulegen.

In diesem Kapitel beschreibe ich, was Sie unbedingt wissen müssen, um Gruppenrichtlinieneinstellungen zu verwalten. In den nächsten Kapiteln zeige ich Ihnen, wie Sie bestimmte Richtlinieneinstellungen nutzen, um die Konfiguration Ihrer Windows-Computer zu automatisieren, unabhängig davon, ob Sie in einem kleinen, mittleren oder großen Unternehmen arbeiten.

Grundlagen von Gruppenrichtlinieneinstellungen

Sie konfigurieren unverwaltete Richtlinieneinstellungen in Active Directory-Gruppenrichtlinien. In lokalen Gruppenrichtlinien gibt es keine unverwalteten Einstellungen. Die Gruppenrichtlinien setzen die unverwalteten Richtlinieneinstellungen nicht immer strikt durch, sie speichern die Einstellungen auch nicht in den entsprechenden Zweigen der Registrierung. Stattdessen schreiben die Gruppenrichtlinien die Einstellungen an dieselben Stellen innerhalb der Registrierung, an denen auch eine Anwendung oder ein Betriebssystemfeature die entsprechende Konfiguration ablegt. Dank dieses Ansatzes können Sie Einstellungen für Anwendungen und Betriebssystemfeatures verwenden, die keine Gruppenrichtlinien auswerten.

Durch Einstellungen lassen sich keine Anwendungs- oder Betriebssystemfeatures in der Benutzeroberfläche deaktivieren, damit der Benutzer sie nicht mehr verwenden kann. Die Benutzer können weiterhin Einstellungen ändern, die Sie mit unverwalteten Richtlinieneinstellungen konfiguriert haben. Aber diese Einstellungen überschreiben die vorhandene Konfiguration, und es gibt keine Möglichkeit, die ursprüngliche Konfiguration wiederherzustellen.

Wie bei verwalteten Richtlinieneinstellungen aktualisieren die Gruppenrichtlinien auch die unverwalteten Einstellungen in regelmäßigen Abständen, in der Standardeinstellung beträgt das Intervall 90 bis 120 Minuten. Das bedeutet, dass die Richtlinieneinstellungen, die Sie konfiguriert haben, regelmäßig erneut auf den Computer eines Benutzers angewendet werden. Statt eine solche Aktualisierung zu erlauben, können Sie auch verhindern, dass die Gruppenrichtlinien einzelne Einstellungen verändern; dazu stellen Sie ein, dass die Einstellungen lediglich ein einziges Mal angewendet werden.

Auf welche Weise Sie unverwaltete Richtlinieneinstellungen benutzen, hängt davon ab, ob Sie das konfigurierte Element erzwingen wollen oder nicht. Wollen Sie ein Element konfigurieren, ohne es zu erzwingen, können Sie unverwaltete Richtlinieneinstellungen verwenden und dann die automatische Aktualisierung deaktivieren. Wenn Sie dagegen ein Element konfigurieren und die gewählte Konfiguration erzwingen wollen, müssen Sie verwaltete Richtlinieneinstellungen verwenden oder unverwaltete Einstellungen konfigurieren und dann die automatische Aktualisierung aktivieren.

Weil Einstellungen sowohl für Computerkonfigurations- als auch Benutzerkonfigurationseinstellungen gelten, finden Sie unter *Computerkonfiguration* und *Benutzerkonfiguration* jeweils einen eigenen Knoten namens *Einstellungen*, der wiederum zwei Unterknoten enthält:

- **Windows-Einstellungen** Verwaltet allgemeine Betriebssystem- und Anwendungseinstellungen.
- **Systemsteuerungseinstellungen** Verwaltet Systemsteuerungseinstellungen.

Tabelle 6.1 bietet einen Überblick über die verfügbaren Einstellungen und gibt an, wo sie in den Konfigurationszweigen und den Unterknoten angeordnet sind.

Tabelle 6.1 Konfigurierbare Einstellungen in den Gruppenrichtlinien

Einstellungstyp	Ort	Richtlinien-konfigurationszweig
Anwendungen, Anwendung	Windows-Einstellungen	Benutzer
Dateien, Datei	Windows-Einstellungen	Computer und Benutzer
Datenquelle, Benutzerdatenquellen	Systemsteuerungseinstellungen	Benutzer
Datenquellen, Datenquelle	Systemsteuerungseinstellungen	Computer und Benutzer
Dienste, Dienst	Systemsteuerungseinstellungen	Computer
Drucker, freigegebener Drucker	Systemsteuerungseinstellungen	Benutzer
Drucker, lokaler Drucker	Systemsteuerungseinstellungen	Computer und Benutzer
Drucker, TCP/IP-Drucker	Systemsteuerungseinstellungen	Computer und Benutzer
Energieoptionen, Energieoptionen (Windows XP)	Systemsteuerungseinstellungen	Computer und Benutzer
Energieoptionen, Energieschema (Windows XP)	Systemsteuerungseinstellungen	Computer und Benutzer
Energieoptionen, Energiesparplan (mindestens Windows 7)	Systemsteuerungseinstellungen	Computer und Benutzer
Geplante Aufgaben, geplante Aufgabe (mindestens Windows 7)	Systemsteuerungseinstellungen	Computer und Benutzer
Geplante Aufgaben, geplante Aufgabe (Windows XP)	Systemsteuerungseinstellungen	Computer und Benutzer
Geplante Aufgaben, sofortige Aufgabe (mindestens Windows 7)	Systemsteuerungseinstellungen	Computer und Benutzer
Geplante Aufgaben, sofortiger Task (Windows XP)	Systemsteuerungseinstellungen	Computer und Benutzer
Geräte, Gerät	Systemsteuerungseinstellungen	Computer und Benutzer
INI-Dateien, INI-Datei	Windows-Einstellungen	Computer und Benutzer
Internet Explorer, Microsoft Internet Explorer 10	Systemsteuerungseinstellungen	Benutzer
Internet Explorer, Microsoft Internet Explorer 5 und 6	Systemsteuerungseinstellungen	Benutzer
Internet Explorer, Microsoft Internet Explorer 7	Systemsteuerungseinstellungen	Benutzer
Internet Explorer, Microsoft Internet Explorer 8 und 9	Systemsteuerungseinstellungen	Benutzer
Laufwerkzuordnungen, zugeordnetes Laufwerk	Windows-Einstellungen	Benutzer
Lokale Benutzer und Gruppen, lokale Gruppe	Systemsteuerungseinstellungen	Computer und Benutzer
Lokale Benutzer und Gruppen, lokaler Benutzer	Systemsteuerungseinstellungen	Computer und Benutzer
Netzwerkfreigaben, Netzwerkfreigabe	Windows-Einstellungen	Computer
Netzwerkoptionen, Einwahlverbindung	Systemsteuerungseinstellungen	Computer und Benutzer
Netzwerkoptionen, VPN-Verbindung	Systemsteuerungseinstellungen	Computer und Benutzer
Ordner, Ordner	Windows-Einstellungen	Computer und Benutzer
Ordneroptionen, Dateityp	Systemsteuerungseinstellungen	Computer
Ordneroptionen, Öffnen mit	Systemsteuerungseinstellungen	Benutzer
Ordneroptionen, Ordneroptionen (mindestens Windows Vista)	Systemsteuerungseinstellungen	Benutzer
Ordneroptionen, Ordneroptionen (Windows XP)	Systemsteuerungseinstellungen	Benutzer
Regionale Einstellungen	Systemsteuerungseinstellungen	Benutzer
Registrierung, Registrierungs-Assistent	Windows-Einstellungen	Computer und Benutzer
Registrierung, Registrierungselement	Windows-Einstellungen	Computer und Benutzer ►

Einstellungstyp	Ort	Richtlinien-konfigurationszweig
Registrierung, Sammlungselement	Windows-Einstellungen	Computer und Benutzer
Startmenü, Startmenü (mindestens Windows Vista)	Systemsteuerungseinstellungen	Benutzer
Startmenü, Startmenü (Windows XP)	Systemsteuerungseinstellungen	Benutzer
Umgebung, Umgebungsvariable	Windows-Einstellungen	Computer und Benutzer
Verknüpfungen, Verknüpfung	Windows-Einstellungen	Computer und Benutzer

Konfigurieren von Gruppenrichtlinieneinstellungen

Unverwaltete Richtlinieneinstellungen werden anders konfiguriert und gepflegt als verwaltete Richtlinien. Sie definieren Einstellungen, indem Sie eine Verwaltungsaktion, einen Bearbeitungszustand oder beides festlegen.

Arbeiten mit Verwaltungsaktionen

In den verschiedenen Einstellungsbereichen können Sie gewöhnlich Aktionen festlegen, die angeben, wie die Einstellung angewendet werden soll. Die meisten Einstellungen unterstützen folgende Verwaltungsaktionen:

- **Erstellen** Erstellt ein Einstellungselement auf dem Computer eines Benutzers. Das Einstellungselement wird nur erstellt, wenn es noch nicht vorhanden ist.
- **Ersetzen** Erstellt ein Einstellungselement, sofern es noch nicht vorhanden ist, oder löscht ein vorhandenes Einstellungselement und erstellt es neu. Bei den meisten Einstellungen gibt es weitere Optionen, mit denen Sie genau steuern können, wie der Ersetzungsvorgang abläuft. Abbildung 6.1 zeigt ein Beispiel.

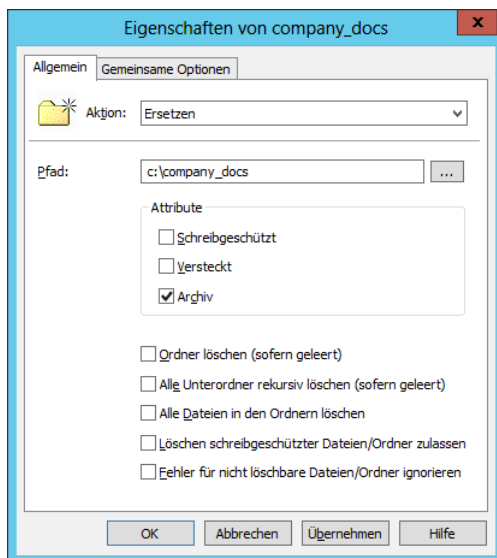


Abbildung 6.1 Auswählen der Verwaltungsaktion

- **Aktualisieren** Ändert bestimmte Konfigurationen in einem Einstellungselement. Diese Aktion unterscheidet sich von *Ersetzen* dadurch, dass sie nur Werte innerhalb des Einstellungselements ändert. Alle anderen Werte bleiben gleich. Falls noch kein entsprechendes Einstellungselement vorhanden ist, wird es bei der Aktion *Aktualisieren* erstellt.
- **Löschen** Löscht ein Einstellungselement vom Computer eines Benutzers. Bei den meisten Einstellungen stehen zusätzliche Optionen zur Verfügung, mit denen Sie genau steuern können, wie der Löschvorgang abläuft. Diese zusätzlichen Optionen sind in vielen Fällen dieselben wie bei der Aktion *Ersetzen*.

Die Verwaltungsaktion legt fest, wie das Einstellungselement angewendet oder ob das Element gelöscht wird, wenn es nicht mehr gebraucht wird. Verwaltungsaktionen werden unter anderem von den Einstellungen unterstützt, die folgende Elemente konfigurieren:

- Anwendungen
- Datenquellen
- Laufwerkzuordnungen
- Umgebung
- Dateien
- Ordner
- INI-Dateien
- Lokale Benutzer und Gruppen
- Netzwerkooptionen
- Netzwerkfreigaben
- Drucker
- Registrierungselemente
- Geplante Aufgaben
- Verknüpfungen

Arbeiten mit Bearbeitungszuständen

Ein kleinerer Teil der Einstellungen unterstützt Bearbeitungszustände, die grafische Benutzeroberflächen aus Dienstprogrammen der Systemsteuerung anzeigen. Bei dieser Art Einstellung wird das Element so angewendet, wie es der Bearbeitungszustand jedes Werts in der zugehörigen Benutzeroberfläche festlegt. Der einmal angewendete Bearbeitungszustand kann nicht rückgängig gemacht werden, und es gibt keinen Befehl, um den Bearbeitungszustand wieder zu entfernen, wenn er nicht mehr angewendet wird.

Bearbeitungszustände werden unter anderem von den Einstellungen unterstützt, die folgende Elemente konfigurieren:

- Ordneroptionen
- Interneteinstellungen
- Energieoptionen
- Regionale Einstellungen
- Startmenü

HINWEIS

Nur Standardordneroptionen unterstützen Bearbeitungszustände.

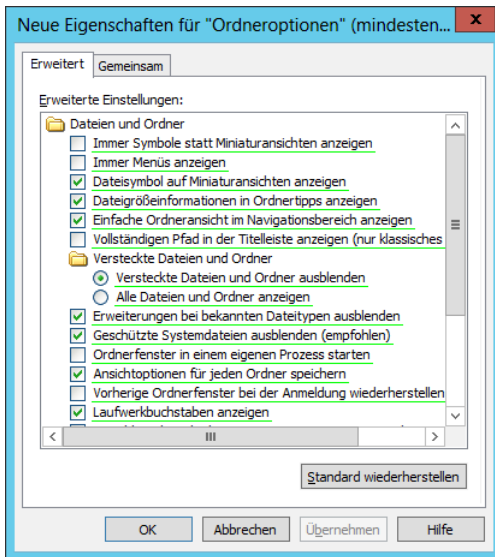


Abbildung 6.2 Anzeige des Bearbeitungszustands als Linien

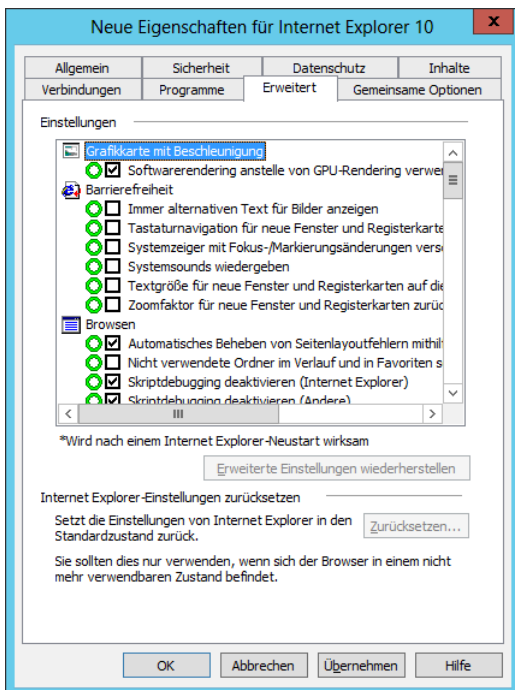


Abbildung 6.3 Andere Darstellung des Bearbeitungszustands

Weil jede Version einer Anwendung und des Betriebssystems Windows eine andere Benutzeroberfläche haben kann, sind die entsprechenden Optionen mit einer ganz bestimmten Version verbunden. Zum Beispiel müssen Sie die Einstellungselemente für Ordneroption für die Internet Explorer 8 und 9 separat von den Einstellungselementen für den Internet Explorer 10 konfigurieren.

Wenn Sie mit dieser Art Einstellung arbeiten, wird in der Standardeinstellung jeder Wert der Benutzeroberfläche vom Clientcomputer verarbeitet und angewendet, selbst wenn Sie den zugehörigen Wert gar nicht explizit konfigurieren. Somit werden alle vorhandenen Werte auf diese Benutzeroberfläche angewendet. Wie in Abbildung 6.2 zu sehen, wird der Bearbeitungszustand aller zugehörigen Optionen grafisch angezeigt:

- Eine durchgezogene grüne Linie bedeutet, dass der Wert ausgeliefert und auf dem Client verarbeitet wird.
- Eine gestrichelte rote Linie bedeutet, dass der Wert weder ausgeliefert noch auf dem Client verarbeitet wird.

Reicht der Platz in der Benutzeroberfläche nicht aus, um die Linien zu zeichnen, wird statt der durchgezogenen grünen Linie ein grüner Kreis angezeigt (das heißt, dass der Wert ausgeliefert und auf dem Client verarbeitet wird) und statt der gestrichelten roten Linie ein roter Kreis (das heißt, dass der Wert nicht ausgeliefert und nicht auf dem Client verarbeitet wird). Die Abbildungen 6.2 und 6.3 zeigen Beispiele für Einstellungselemente, die Bearbeitungszustände verwenden.

Sie können die folgenden Funktionstasten verwenden, um den Bearbeitungszustand von Optionen zu verwalten:

- **F5** Aktiviert die Verarbeitung aller Werte auf der ausgewählten Registerkarte. Das ist nützlich, wenn Sie die Verarbeitung einiger Werte deaktiviert haben und später wieder möchten, dass alle Optionen auf einer Registerkarte verarbeitet werden.
- **F6** Aktiviert die Verarbeitung der momentan ausgewählten Option auf der ausgewählten Registerkarte. Das ist nützlich, wenn Sie eine Option deaktiviert haben und später entscheiden, dass sie doch verarbeitet werden soll.
- **F7** Deaktiviert die Verarbeitung der momentan ausgewählten Option auf der ausgewählten Registerkarte. Das ist nützlich, wenn Sie verhindern wollen, dass eine Option auf dem Client verarbeitet wird.
- **F8** Deaktiviert die Verarbeitung aller Optionen auf der ausgewählten Registerkarte. Das ist nützlich, wenn Sie möchten, dass keine der Optionen auf einer Registerkarte auf dem Client verarbeitet wird. Außerdem ist diese Funktion praktisch, wenn Sie nur einige ausgewählte Optionen aktivieren wollen.

HINWEIS Denken Sie daran, dass der Wert, der mit einer Option verknüpft ist, vom Bearbeitungszustand unabhängig ist. Indem Sie eine Option einstellen oder löschen, ändern Sie nicht den Bearbeitungszustand.

Arbeiten mit alternativen Aktionen und Zuständen

Einige wenige Einstellungen unterstützen weder Verwaltungsaktionen noch Bearbeitungszustände. Dazu gehören beispielsweise die Einstellungen zum Konfigurieren von Geräten, sofortigen Tasks und Diensten. Bei den Geräten (Abbildung 6.4) verwenden Sie die Dropdownliste *Aktion*, um bestimmte Geräteklassen und Gerätetypen zu aktivieren oder zu deaktivieren. Bei den sofortigen Tasks erstellt die zugehörige Einstellung eine Aufgabe, die ausgeführt und dann automatisch gelöscht wird. Und bei den Diensten konfigurieren Sie in der zugehörigen Einstellung einen vorhandenen Dienst.



Abbildung 6.4 Auswählen der Aktion zum Aktivieren oder Deaktivieren des Geräts

Verwalten von Einstellungselementen

Um unverwaltete Einstellungen anzusehen und zu bearbeiten, müssen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten öffnen, wie in Kapitel 5, »Konfigurieren von Benutzer- und Computerrichtlinien«, beschrieben. Dann haben Sie folgende Möglichkeiten, um die Einstellungen für Computer oder Benutzer zu verwalten:

- Wenn Sie Einstellungen konfigurieren wollen, die auf Computer unabhängig davon angewendet werden, wer angemeldet ist, müssen Sie doppelt auf den Knoten *Computerkonfiguration* tippen oder klicken, dann doppelt auf den Knoten *Einstellungen* tippen oder klicken und schließlich den Einstellungsbereich auswählen, den Sie bearbeiten wollen.
- Wenn Sie Einstellungen konfigurieren wollen, die auf Benutzer unabhängig davon angewendet werden, an welchem Computer sie sich anmelden, müssen Sie doppelt auf den Knoten *Benutzerkonfiguration* tippen oder klicken, dann doppelt auf den Knoten *Einstellungen* tippen oder klicken und schließlich den Einstellungsbereich auswählen, den Sie bearbeiten wollen.

Erstellen und Verwalten eines Einstellungselements

Sie verwalten Einstellungselemente, indem Sie den gewünschten Einstellungsbereich auswählen und dann die zugehörigen Einstellungselemente in der Detailansicht bearbeiten. Während ein bestimmter Bereich ausgewählt ist und angezeigt wird, können Sie ein zugehöriges Element erstellen, indem Sie mit der rechten Maustaste in der Detailansicht auf einen leeren Bereich klicken oder diese Stelle gedrückt halten, auf *Neu* zeigen und dann den Elementtyp auswählen, den Sie erstellen wollen. Im Kontextmenü werden nur Elemente für den gerade ausgewählten Bereich angeboten. Arbeiten Sie beispielsweise in *Drucker* unterhalb des Knotens *Computerkonfiguration*, bekommen Sie die Möglichkeit angeboten, eine Einstellung für einen TCP/IP-Drucker oder einen lokalen Drucker zu erstellen, wenn Sie mit der rechten Maustaste auf den Knoten klicken oder ihn gedrückt halten und im Kontextmenü auf *Neu* zeigen.

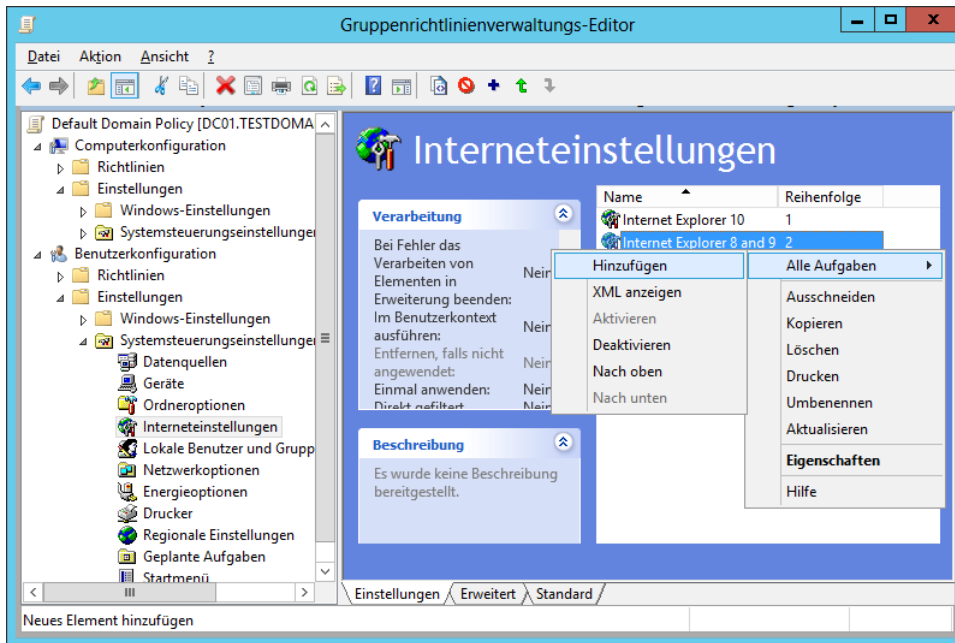


Abbildung 6.5 Verwalten von Einstellungselementen mit dem Gruppenrichtlinienverwaltungs-Editor und den Befehlen des Kontextmenüs

Nachdem Sie Elemente für einen Einstellungsbereich erstellt haben, können Sie mit der rechten Maustaste auf ein einzelnes Element klicken oder es gedrückt halten, um ein Kontextmenü zu öffnen, in dem Befehle zum Verwalten dieses Elements zur Verfügung stehen. Abbildung 6.5 zeigt ein Beispiel.

In der Symbolleiste werden ähnliche Optionen angezeigt, wenn Sie ein Element auswählen. Statt mit der rechten Maustaste auf ein Element zu klicken oder es gedrückt zu halten und im Kontextmenü den Befehl *Eigenschaften* zu wählen, um sein Eigenschaftendialogfeld zu öffnen, können Sie auch doppelt auf das Einstellungselement tippen oder klicken. Anschließend können Sie im Eigenschaftendialogfeld die Optionen für das Einstellungselement ansehen oder ändern.

Auf Clientcomputern verarbeitet der Gruppenrichtlinienclient die Einstellungselemente entsprechend ihrer Vorrangreihenfolge. Das Einstellungselement mit dem niedrigsten Rang (es steht in der Liste ganz unten) wird zuerst verarbeitet, gefolgt vom Einstellungselement mit dem zweitniedrigsten Rang und so weiter, bis das Einstellungselement mit dem höchsten Rang (das am Anfang der Liste steht) verarbeitet ist.

Die Verarbeitung wird in der Reihenfolge des Vorrangs ausgeführt, um sicherzustellen, dass Einstellungselemente mit höherer Vorrangstufe Priorität gegenüber Einstellungselementen mit geringerer Vorrangstufe haben. Treten irgendwelche Konflikte zwischen den Optionen auf, die in den Einstellungselementen angewendet werden, werden die Werte verwendet, die zuletzt geschrieben werden. Sie können die Vorrangreihenfolge ändern, indem Sie einen Einstellungsbereich in der Konsolenstruktur auswählen und in der Detailansicht auf das Einstellungselement klicken, das Sie bearbeiten wollen. In der Symbolleiste werden nun zusätzliche Befehle angezeigt, darunter:

- *Ausgewähltes Element nach oben verschieben*
- *Ausgewähltes Element nach unten verschieben*

Tippen oder klicken Sie auf *Ausgewähltes Element nach unten verschieben*, um die Vorrangstufe des ausgewählten Elements zu verringern. Wenn Sie dagegen auf *Ausgewähltes Element nach oben verschieben* klicken, heben Sie die Vorrangstufe des ausgewählten Elements an.

Konfigurieren von Optionen auf der Registerkarte *Gemeinsame Optionen*

Alle Einstellungselemente haben eine Registerkarte namens *Gemeinsame Optionen*, auf der Sie Optionen finden, die für alle Einstellungselemente gelten. Die genaue Liste der gemeinsamen Optionen unterscheidet sich zwar von Element zu Element, aber die meisten Einstellungselemente haben die Optionen, die Sie in Abbildung 6.6 sehen.

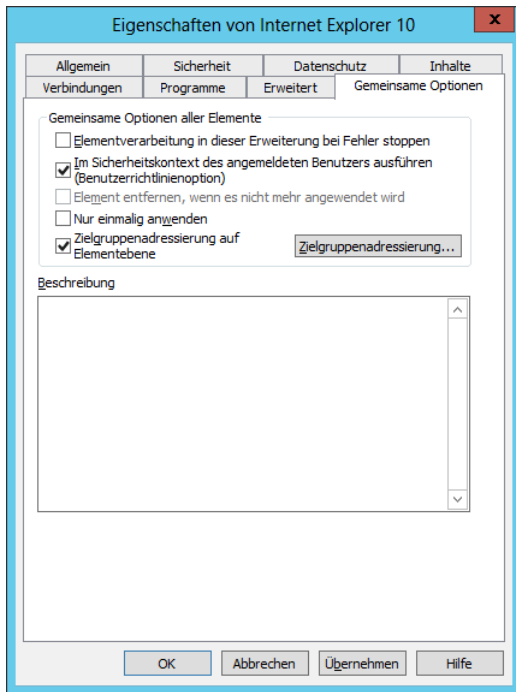


Abbildung 6.6 Konfigurieren zusätzlicher Verarbeitungsoptionen auf der Registerkarte *Gemeinsame Optionen*

Die gemeinsamen Optionen werden folgendermaßen benutzt:

- **Elementverarbeitung in dieser Erweiterung bei Fehler stoppen** Tritt bei der Verarbeitung eines Einstellungselements ein Fehler auf, wird in der Standardeinstellung die Verarbeitung der anderen Einstellungselemente fortgesetzt. Dieses Verhalten können Sie ändern, indem Sie *Elementverarbeitung in dieser Erweiterung bei Fehler stoppen* aktivieren. Ist dieses Kontrollkästchen aktiviert, verhindert ein Einstellungselement, dessen Verarbeitung fehlschlägt, dass die übrigen Einstellungselemente innerhalb der Erweiterung für ein bestimmtes Gruppenrichtlinienobjekt verarbeitet werden. Diese Option hat keine Auswirkung auf die Verarbeitung in anderen **Gruppenrichtlinienobjekten**.

- **Im Sicherheitskontext des angemeldeten Benutzers ausführen** In der Standardeinstellung verarbeitet der Gruppenrichtlinienclient, der auf einem Computer läuft, die Benutzereinstellungen innerhalb des Sicherheitskontexts des Winlogon-Kontos (bei Computern mit älteren Windows-Versionen als Windows Vista) oder des Systemkontos (bei Computern mit Windows Vista oder neuer). In diesem Kontext bleibt eine Einstellungserweiterung auf die Umgebungsvariablen und Systemressourcen beschränkt, die auf dem Computer verfügbar sind. Stattdessen kann der Client die Benutzereinstellungen auch im Sicherheitskontext des angemeldeten Benutzers verarbeiten. Auf diese Weise kann die Einstellungserweiterung auf Ressourcen unter der Identität des Benutzers statt als Systemdienst zugreifen. Das ist manchmal notwendig, wenn beispielsweise Laufwerkzuordnungen oder andere Einstellungen benutzt werden, für die der Computer keine ausreichenden Berechtigungen für den Ressourcenzugriff besitzt oder die mit Benutzerumgebungsvariablen arbeiten müssen.
- **Element entfernen, wenn es nicht mehr angewendet wird** Wenn die Richtlinieneinstellungen in einem Gruppenrichtlinienobjekt nicht mehr auf einen Benutzer oder Computer angewendet werden, werden diese Richtlinieneinstellungen in der Standardeinstellung gelöscht, weil sie nicht mehr im Gruppenrichtlinienbereich der Registrierung gesetzt werden. Standardeinstellungselemente werden allerdings nicht automatisch entfernt, wenn ein Gruppenrichtlinienobjekt nicht mehr auf einen Benutzer oder Computer angewendet wird. Dieses Verhalten können Sie ändern, indem Sie dieses Kontrollkästchen für ein Einstellungselement aktivieren. Ist das Kontrollkästchen aktiviert, entscheidet die Einstellungserweiterung, ob ein Einstellungselement, das bisher angewendet wurde, nun nicht mehr relevant ist. Wird das Einstellungselement als nicht mehr relevant eingestuft, löscht die Einstellungserweiterung alle Werte, die mit diesem Einstellungselement verknüpft sind.

PRAXISTIPP

Im Allgemeinen können Einstellungen, die Verwaltungsaktionen unterstützen, entfernt werden, sobald sie nicht mehr angewendet werden. Dagegen können Einstellungen, die Bearbeitungszustände unterstützen, in einem solchen Fall nicht entfernt werden. Wenn Sie *Element entfernen, wenn es nicht mehr angewendet wird* aktivieren, wird die Verwaltungsaktion auf *Ersetzen* gestellt. Daher führt die Einstellungserweiterung während der Gruppenrichtlinienverarbeitung eine Löschoperation aus, gefolgt von einer Erstelloperation. Sofern das Einstellungselement anschließend nicht mehr für den Benutzer oder Computer relevant ist (also nicht mehr angewendet wird), werden die Ergebnisse des Einstellungselements gelöscht (aber nicht neu erstellt). Auch die Zielfestlegung auf ein bestimmtes Element kann dazu führen, dass ein Einstellungselement nicht mehr angewendet wird.

- **Nur einmalig anwenden** Die Gruppenrichtlinien schreiben Einstellungen in den Speicherort der Registrierung, in dem auch eine Anwendung oder ein Betriebssystemfeature die entsprechende Option speichert. Daher können Benutzer Werte ändern, die mithilfe unverwalteter Richtlinieneinstellungen konfiguriert wurden. In der Standardeinstellung werden die Ergebnisse der Einstellungselemente allerdings jedes Mal neu geschrieben, wenn die Gruppenrichtlinien aktualisiert werden. So ist sichergestellt, dass Einstellungselemente so angewendet werden, wie die Administratoren es vorsehen. Sie können dieses Verhalten ändern, indem Sie dieses Kontrollkästchen aktivieren. Ist dieses Kontrollkästchen aktiviert, wendet die Einstellungserweiterung die Ergebnisse des Einstellungselements nur ein einziges Mal an und danach nicht mehr.
- **Zielgruppenadressierung auf Elementebene** Mit der Zielgruppenadressierung auf Elementebene können Sie die Anwendung eines Einstellungselements filtern, damit dieses Einstellungselement nur auf ausgewählte Benutzer oder Computer angewendet wird. Wenn der Gruppenrichtlinienclient eine bestimmte Einstellung auswertet, berechnet er zu jedem Element den Wert *Wahr* oder *Falsch*. Ist das Ergebnis *Wahr*, wird das Einstellungselement angewendet; in diesem Fall wird es verarbeitet. Ist das Ergebnis dagegen *Falsch*, wird das Einstellungselement nicht angewendet und folglich nicht verarbei-

tet. Wenn dieses Kontrollkästchen aktiviert ist, können Sie auf die Schaltfläche *Zielgruppenadressierung* klicken, um den Zielgruppenadressierungseeditor zu öffnen und dort zu konfigurieren, auf welche Ziele die Einstellung angewendet wird.

PRAXISTIPP Die Zielgruppenadressierung von Elementen wird als logischer Ausdruck ausgewertet. Dieser logische Ausdruck kann auch Umgebungsvariablen umfassen, sofern die Umgebungsvariablen im Kontext des aktuellen Benutzers verfügbar sind. Wenn Sie Ihren logischen Ausdruck erstellen, müssen Sie sicherstellen, dass er Sinn ergibt. Und wenn Sie einen festen Wert eintragen, statt eine Umgebungsvariable zu benutzen, funktioniert die Zielgruppenadressierung nicht wie erwartet.

Kapitel 7

Verwalten von Benutzerzugriff und Sicherheit

In diesem Kapitel:

Grundlagen von Benutzer- und Gruppenkonten	226
Benutzerkontensteuerung und Anhebungsaufforderungen	232
Verwalten der lokalen Anmeldung	237
Verwalten gespeicherter Anmeldeinformationen	246
Verwalten lokaler Benutzerkonten und Gruppen	251
Verwalten des Remotezugriffs auf Arbeitsstationen	260

Windows 8-Computer können Mitglieder einer Heimnetzgruppe, einer Arbeitsgruppe oder einer Domäne sein. Wenn eine Arbeitsstation Mitglied einer Heimnetzgruppe oder Arbeitsgruppe ist, werden Zugriff und Sicherheit direkt auf der Arbeitsstation konfiguriert. Ist die Arbeitsstation dagegen Mitglied einer Domäne, werden Zugriff und Sicherheit auf zwei Ebenen konfiguriert, nämlich auf der Ebene des lokalen Systems und auf Domänenebene. Benutzerzugriffe für einzelne Computer können auf der Ebene des lokalen Systems konfiguriert werden, während Einstellungen, die für mehrere Computer und Ressourcen gelten, in der aktuellen Active Directory-Gesamtstruktur vorgenommen werden.

In diesem Kapitel erfahren Sie, wie lokale Systemzugriffe und lokale Konten verwaltet werden. Eine ausführliche Beschreibung der Konfiguration von Zugriffen und Berechtigungen in einer Domäne finden Sie in dem Buch *Microsoft Windows Server 2012 – Ratgeber für Administratoren* (Microsoft Press, 2012). Denken Sie bitte daran, dass jede Aufgabe, die in diesem Kapitel (wie auch im gesamten Buch) beschrieben wird, entweder mit lokaler Anmeldung oder über eine Remotedesktopverbindung durchgeführt werden kann.

Grundlagen von Benutzer- und Gruppenkonten

Windows 8 kennt Benutzerkonten und Gruppenkonten, wobei Benutzer auch Mitglieder von Gruppen sein können. Benutzerkonten sind für einzelne Benutzer vorgesehen. Gruppenkonten, kurz »Gruppen« genannt, dienen zur Vereinfachung der Verwaltung von vielen Benutzern. Sie können sich mit einem Benutzerkonto anmelden, aber nicht mit einem Gruppenkonto.

In Windows 8 gibt es zwei allgemeine Arten von Benutzerkonten:

- **Lokale Benutzerkonten** Benutzerkonten, die auf einem lokalen Computer angelegt werden, heißen *lokale Benutzerkonten*. Diese Konten eignen sich nur für den Zugriff auf den lokalen Computer. Sie können lokale Benutzerkonten mit der Option *Benutzerkonten* der Systemsteuerung oder mit der Konsole *Lokale Benutzer und Gruppen* anlegen und löschen. Die Konsole *Lokale Benutzer und Gruppen* ist unter dem Knoten *System* in der Computerverwaltung verfügbar, bei der es sich ebenfalls um ein Snap-In der Microsoft Management Console (MMC) handelt.
- **Domänenbenutzerkonten** In Active Directory definierte Benutzerkonten werden *Domänenbenutzerkonten* genannt. Mit einmaligem Anmelden (Single-Sign On) eignen sich diese Konten für den Zugriff auf Ressourcen aus der ganzen Gesamtstruktur. Wenn ein Computer Mitglied einer Active Directory-Domäne ist, können Sie Domänenbenutzerkonten mit *Active Directory-Benutzer und -Computer* anlegen. Diese MMC-Konsole ist im Menü *Tools* des Server-Managers verfügbar, wenn Sie auf Ihrem Windows 8-Computer die Remote Server Administration Tools installiert haben.

Lokale Benutzerkonten und Domänenbenutzerkonten können als Standardbenutzerkonten oder als Administratorkonten konfiguriert werden. Ein Standardbenutzerkonto verfügt auf einem lokalen Computer nur über beschränkte Rechte, während ein Administratorkonto auf einem lokalen Computer über mehr Rechte verfügt.

In Windows 8 gibt es einen neuen speziellen Typ eines lokalen Kontos, der *Microsoft-Konto* genannt wird und in älteren Windows-Versionen nicht verfügbar ist. Microsoft-Konten kann man sich als synchronisierte lokale Konten vorstellen, die folgendermaßen funktionieren:

- Ein Benutzer meldet sich mit einer E-Mail-Adresse als Anmeldename und einem Kennwort, das für sein Online-Microsoft-Konto gilt, auf einem Computer an.
- Da der Benutzer eine Verbindung zu seinem Microsoft-Konto hergestellt hat, kann er auch die verschiedenen eingebundenen Funktionen dieses Kontos verwenden.

Eine Synchronisierung des Kontos ermöglicht es den Benutzern, im Windows Store Anwendungen und andere Inhalte für ihre Computer zu kaufen. Außerdem lassen sich synchronisierte Inhalte (Dateien, Fotos und mehr) und bestimmte Profileinstellungen auf SkyDrive speichern, damit sie auch verfügbar sind, wenn sich der Benutzer auf einem anderen Windows 8-Computer anmeldet. Diese synchronisierten Inhalte sind für Benutzer praktisch immer in der gleichen Weise zugänglich, unabhängig davon, auf welchem Computer sie sich anmelden. In allen anderen Aspekten funktionieren synchronisierte Konten genauso wie herkömmliche lokale Konten.

Ein herkömmliches lokales Konto lässt sich jederzeit in ein synchronisiertes Konto konvertieren. Umgekehrt lässt sich auch ein synchronisiertes Konto jederzeit in ein herkömmliches Konto konvertieren.

PRAXISTIPP

Auf Firmen-PCs möchten Sie vielleicht verhindern, dass Benutzer Microsoft-Konten erstellen oder sich mit solchen Konten anmelden können. Sie können Microsoft-Konten in den Gruppenrichtlinien blockieren, indem Sie die Richtlinie *Konten: Microsoft-Konten blockieren* aktivieren. Diese Richtlinie ist in den Sicherheitsoptionen für die Computerkonfiguration unter *Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien* zu finden. Verwenden Sie die Einstellung *Benutzer können keine Microsoft-Konten hinzufügen*, um Benutzer an der Erstellung von Microsoft-Konten zu hindern. Um Benutzer daran zu hindern, Microsoft-Konten zu erstellen oder sich mit solchen Konten anzumelden, wählen Sie die Einstellung *Benutzer können keine Microsoft-Konten hinzufügen oder sich damit anmelden*.

Grundlagen von lokalen Benutzerkonten

Alle Benutzerkonten werden anhand eines Anmeldenamens identifiziert. In Windows 8 besteht dieser Anmelde-name aus zwei Teilen:

- **Benutzername** Der Name des Kontos in Textform
- **Benutzercomputer oder -domäne** Der Computer oder die Domäne, zu der das Konto gehört

Für den Benutzer *WilliamS*, dessen Konto auf dem Computer *ENGPC85* angelegt wurde, lautet der vollständige Anmelde-name unter Windows 8 *ENGPC85\WilliamS*. Mit einem lokalen Computerkonto kann sich *WilliamS* auf seiner lokalen Arbeitsstation anmelden und lokale Ressourcen verwenden, aber nicht auf Ressourcen zugreifen, die zur Domäne gehören.

Wenn Sie für einen Benutzer ein Microsoft-Konto erstellen, verwendet Windows 8 die Namensinformationen, die Sie angeben, als Anmeldenamen. Vor- und Nachname des Benutzers werden im Anzeigetext verwendet. Die vollständige E-Mail-Adresse dient als Anmelde-name, weil diese Adresse lokal auf dem Computer gespeichert wird. Wenn sich der Benutzer anmeldet und sein Computer mit dem Internet verbunden ist, können die Einstellungen und Inhalte des Benutzers synchronisiert und aktualisiert werden. Ist der Computer nicht mit dem Internet verbunden, werden die Einstellungen und Inhalte wie bei herkömmlichen Benutzerkonten aus seinem Profil ausgelesen.

Bei der Arbeit mit Domänen kann der vollständige Anmelde-name auf zweierlei Art und Weise angegeben werden:

- Der Benutzerkontenname und der vollständige Domänenname werden durch ein At-Zeichen (@) voneinander getrennt. Der vollständige Anmelde-name für den Benutzernamen *Williams* in der Domäne *technology.microsoft.com* wäre zum Beispiel *Williams@technology.microsoft.com*.
- Der Benutzerkontenname und der Domänenname werden durch einen umgekehrten Schrägstrich (\) voneinander getrennt. Der vollständige Anmelde-name für *Williams* aus der Domäne *technology* wäre *technology\Williams*.

Windows zeigt bei der Beschreibung von Rechten und Berechtigungen zwar Benutzernamen an, aber das entscheidende Kennzeichen für Konten sind Sicherheitskennungen (Security Identifiers, SIDs). SIDs sind eindeutige Kennungen, die bei der Erstellung von Sicherheitsprinzipalen erstellt werden. Jede SID besteht aus einem Computer- oder Domänensicherheitskennungspräfix und einer relativen Kennung für den Benutzer. Windows 8 verwendet diese Kennungen zur Verwaltung der Konten, die dadurch von Benutzernamen unabhängig werden. SIDs haben viele Aufgaben, aber die beiden wichtigsten sind, Ihnen zu ermöglichen, auf einfache Weise Benutzernamen zu ändern und Konten zu löschen, ohne sich Gedanken darüber machen zu müssen, ob sich vielleicht jemand Zugang zu Ressourcen verschafft, indem er einfach ein Konto neu erstellt.

Wenn Sie einen Kontonamen ändern, geben Sie Windows 8 den Auftrag, mit einer bestimmten SID einen neuen Namen zu verknüpfen. Wenn Sie ein Konto löschen, teilen Sie Windows 8 mit, dass eine bestimmte SID nicht mehr gilt. Selbst wenn Sie später ein Konto mit demselben Benutzernamen erstellen, verfügt das neue Konto nicht automatisch über dieselben Rechte und Berechtigungen wie das alte Konto, weil das neue Konto eine neue SID hat.

Benutzer können auch mit Kennwörtern und Zertifikaten geschützt werden. Kennwörter sind Authentifizierungszeichenfolgen für ein Konto. Zertifikate identifizieren einen Benutzer durch eine Kombination aus einem öffentlichen und einem geheimen Schlüssel. Mit einem Kennwort melden Sie sich interaktiv an, während ein Zertifikat mit seinem geheimen Schlüssel auf einer Smartcard gespeichert und von einem Smartcardleser gelesen wird.

Wenn Sie Windows 8 installieren, legt das Betriebssystem Standardkonten an. Sie werden einige vordefinierte Konten vorfinden, die ähnliche Aufgaben wie die Konten haben, die in Windows-Domänen angelegt werden. Die wichtigsten Konten sind folgende:

- **Administrator** Das Konto *Administrator* ist ein vordefiniertes Konto, das den Vollzugriff auf Dateien, Verzeichnisse, Dienste und andere Ressourcen bietet. Sie können dieses Konto weder löschen noch deaktivieren. In Active Directory hat das Administratorkonto domänenweiten Zugriff und domänenweite Berechtigungen. Auf einer lokalen Arbeitsstation hat das Administratorkonto nur Zugriff auf den lokalen Computer.
- **Gast** Das Konto *Gast* ist für Benutzer vorgesehen, die nur einmal oder gelegentlich am Computer arbeiten. Obwohl Gäste nur über beschränkte Rechte verfügen, müssen Sie sehr sorgfältig mit diesem Konto umgehen, weil es potenzielle Sicherheitsprobleme für das System mit sich bringt. Das Risiko ist so hoch, dass das Konto nach der Installation von Windows 8 standardmäßig deaktiviert ist.

In der Standardeinstellung sind diese Konten Mitglieder mehrerer Gruppen. Bevor Sie eines der vordefinierten Konten ändern, sollten Sie sich die genauen Einstellungen und die Gruppenmitgliedschaften notieren. Diese Gruppenmitgliedschaften gewähren dem Benutzer den Zugang zu bestimmten Systemressourcen oder schränken diesen Zugang ein. So ist *Administrator* zum Beispiel ein Mitglied der Gruppe *Administratoren*, und *Gast* ist ein Mitglied der Gruppe *Gäste*. Mitglied einer Gruppe zu sein bedeutet für ein Konto, die Privilegien und Rechte dieser Gruppe in Anspruch nehmen zu dürfen.

Neben den vordefinierten Konten verfügt Windows 8 über einige Pseudokonten, die vom Betriebssystem zur Durchführung bestimmter Aufgaben verwendet werden. Diese Pseudokonten sind nur auf dem lokalen System verfügbar. Sie können die Einstellungen dieser Konten nicht mit den Benutzerverwaltungsprogrammen ändern. Benutzer können sich mit diesen Konten auch nicht am Computer anmelden. Zu den Pseudokonten zählen:

- **SYSTEM** Das Konto *SYSTEM* (oft einfach als lokales Systemkonto bezeichnet) ist ein Pseudokonto zum Ausführen von Systemprozessen und Durchführen von Aufgaben auf Systemebene. Dieses Konto gewährt das Anmelderecht *Anmelden als Dienst*. Die meisten Dienste werden mit dem Konto *SYS-*

TEM ausgeführt. In manchen Fällen haben diese Dienste die Berechtigung zur Interaktion mit dem Desktop. Dienste, die weniger Berechtigungen oder Anmelderechte benötigen, werden mit den Konten *LOKALER DIENST* oder *NETZWERKDIENST* ausgeführt. Zu den Diensten, die als *SYSTEM* ausgeführt werden, gehören *Intelligenter Hintergrundübertragungsdienst*, *Computerbrowser*, *Gruppenrichtlinienclient*, *Anmeldedienst*, *Netzwerkverbindungen*, *Druckwarteschlange* und *Benutzerprofildienst*.

- **LOKALER DIENST** Das Konto *LOKALER DIENST* ist ein Pseudokonto für die Ausführung von Diensten, die auf einem lokalen System weniger Berechtigungen und Anmelderechte benötigen. Dienste, die unter diesem Konto ausgeführt werden, erhalten standardmäßig das Recht *Anmelden als Dienst* und die Privilegien *Anpassen von Speicherkontingenten für einen Prozess*, *Auslassen der durchsuchenden Überprüfung*, *Ändern der Systemzeit*, *Zeitzone ändern*, *Erstellen globaler Objekte*, *Generieren von Sicherheitsüberwachungen*, *Annehmen der Clientidentität nach Authentifizierung* und *Ersetzen eines Tokens auf Prozessebene*. Zu den Diensten, die als *LOKALER DIENST* ausgeführt werden, gehören *Gatewaydienst auf Anwendungsebene*, *Remoteregistrierung*, *Smartcard*, *SSDP-Ermittlungsdienst*, *TCP/IP-NetBIOS-Hilfsdienst* und *WebClient*.
- **NETZWERKDIENST** Das Konto *NETZWERKDIENST* wird für die Ausführung von Diensten benutzt, die auf einem lokalen System weniger Privilegien und Anmelderechte benötigen, aber auf Netzwerkressourcen zugreifen müssen. Wie bei *LOKALER DIENST* erhalten Dienste, die unter diesem Konto ausgeführt werden, das Recht *Anmelden als Dienst* und die Privilegien *Anpassen von Speicherkontingenten für einen Prozess*, *Auslassen der durchsuchenden Überprüfung*, *Erstellen globaler Objekte*, *Generieren von Sicherheitsüberwachungen*, *Annehmen der Clientidentität nach Authentifizierung* und *Ersetzen eines Tokens auf Prozessebene*. Dienste, die als *NETZWERKDIENST* ausgeführt werden, sind *BranchCache*, *Distributed Transaction Coordinator*, *DNS-Client*, *Remotedesktopdienste* und *Remoteprozeduraufruf (RPC)*. *NETZWERKDIENST* kann sich gegenüber Remotesystemen auch als das Computerkonto authentifizieren.

Grundlagen von Gruppenkonten

Windows 8 bietet auch Gruppenkonten. Sie dienen zur Vereinfachung der Kontenverwaltung und sind dafür vorgesehen, vergleichbaren Benutzern gleiche Rechte und Berechtigungen zu geben. Wenn ein Benutzer Mitglied einer Gruppe ist, die auf eine bestimmte Ressource zugreifen darf, kann der Benutzer ebenfalls diese Ressource verwenden. Daher können Sie einem Benutzer Zugang zu verschiedenen Netzwerkressourcen verschaffen, indem Sie ihn einfach zum Mitglied der richtigen Gruppe machen. Beachten Sie bitte, dass Sie sich zwar mit einem Benutzerkonto auf einem Computer anmelden können, aber nicht mit einem Gruppenkonto. Da es in verschiedenen Active Directory-Domänen oder auf lokalen Computern Gruppen mit gleichen Namen geben kann, werden Gruppen oft in der Form *Domäne\Gruppenname* oder *Computer\Gruppenname* angegeben (zum Beispiel *Technology\GMarketing* für die Gruppe *GMarketing* in der Domäne oder auf dem Computer *Technology*).

Windows 8 verwendet folgende drei Arten von Gruppen:

- **Lokale Gruppen** Lokale Gruppen werden auf einem lokalen Computer definiert und nur auf dem lokalen Computer verwendet. Sie können lokale Gruppen mit der Konsole *Lokale Benutzer und Gruppen* erstellen.
- **Sicherheitsgruppen** Sicherheitsgruppen können mit Sicherheitsdeskriptoren verknüpft sein. Sicherheitsgruppen definieren Sie in Domänen mit *Active Directory-Benutzer und -Computer*.
- **Verteilerguppen** Werden für E-Mail-Verteilerlisten verwendet. Mit ihnen sind keine Sicherheitsdeskriptoren verknüpft. Sie definieren Verteilergruppen in Domänen mit *Active Directory-Benutzer und -Computer*.

Wie Benutzerkonten werden auch Gruppenkonten durch eindeutige SIDs unterschieden. Wenn Sie ein Gruppenkonto löschen und wieder neu erstellen, können Sie also nicht davon ausgehen, dass das neue Konto über dieselben Rechte und Berechtigungen verfügt wie das alte Konto. Die neue Gruppe hat eine neue SID und die Rechte und Berechtigungen der alten Gruppe sind verloren.

Wenn Sie Benutzerzugriffsebenen festlegen, können Sie den Benutzer zu einem Mitglied der folgenden integrierten oder vordefinierten Gruppen machen:

- **Administratoren** Mitglieder dieser Gruppe sind lokale Administratoren und haben Vollzugriff auf die Arbeitsstation. Sie können Konten anlegen, Gruppenmitgliedschaften ändern, Drucker installieren, freigegebene Ressourcen verwalten und so weiter. Da dieses Konto Vollzugriff bietet, sollten Sie sehr sorgfältig mit der Auswahl der Benutzer sein, die Sie dieser Gruppe zuordnen.
- **Benutzer** Benutzer erledigen den größten Teil ihrer Arbeit auf einer bestimmten Windows 8-Arbeitsstation. Deswegen haben Mitglieder der Gruppe *Benutzer* mehr Beschränkungen als Rechte. Mitglieder dieser Gruppe können sich lokal auf einer Windows 8-Arbeitsstation anmelden, ein lokales Profil benutzen, die Arbeitsstation sperren und sie herunterfahren.
- **Ereignisprotokollleser** Die Mitglieder dieser Gruppe können sich die Ereignisprotokolle auf dem lokalen Computer ansehen.
- **Gäste** Gäste sind Benutzer mit stark eingeschränkten Rechten. Mitglieder dieser Gruppe können per Remotezugriff auf das System und seine Ressourcen zugreifen, aber kaum etwas anderes tun.
- **Hauptbenutzer** In früheren Versionen von Windows wurde diese Gruppe zur Vergabe zusätzlicher Privilegien eingesetzt, beispielsweise die, Computereinstellungen zu verändern und Programme zu installieren. In Windows 8 gibt es diese Gruppe nur noch aus Gründen der Abwärtskompatibilität mit dem vorhandenen Programmbestand.
- **Hyper-V-Administratoren** Mitglieder dieser Gruppe können alle Funktionen von Hyper-V verwalten. Virtualisierungstechnologien sind in Windows 8 integriert und werden auf 64-Bit-Hardware mit Adressübersetzung der zweiten Ebene (Second Level Address Translation, SLAT) unterstützt.
- **Kryptografie-Operatoren** Mitglieder dieser Gruppe verwalten die Konfiguration der Verschlüsselung, IPsec (Internet Protocol Security), digitale IDs und Zertifikate.
- **Leistungsprotokollbenutzer** Mitglieder dieser Gruppe können Leistungsindikatoren verwalten und anzeigen. Sie können auch die Leistungsprotokollierung verwalten.
- **Leistungsüberwachungsbenutzer** Mitglieder dieser Gruppe können Leistungsindikatoren und Leistungsprotokolle anzeigen.
- **Netzwerkkonfigurations-Operatoren** Mitglieder dieser Gruppe können die Netzwerkeinstellungen der Arbeitsstation verwalten. Sie können auch TCP/IP-Einstellungen ändern und andere allgemeine Netzwerkeinstellungen vornehmen.
- **Remotedesktopbenutzer** Mitglieder dieser Gruppe können sich mit den Remotedesktopdiensten an der Arbeitsstation anmelden. Sobald Mitglieder dieser Gruppe auf dem Computer angemeldet sind, bestimmen die anderen Gruppen, in denen sie Mitglieder sind, ihre Privilegien auf der Arbeitsstation. Ein Benutzer, der Mitglied der Gruppe *Administratoren* ist, erhält dieses Privileg automatisch. (Allerdings müssen Remoteanmeldungen aktiviert werden, bevor sich ein Administrator remote an einer Arbeitsstation anmelden kann.)
- **Remoteverwaltungsbenutzer** Mitglieder dieser Gruppe können über Verwaltungsprotokolle auf WMI-Ressourcen zugreifen.

- **Replikations-Operator** Mitglieder dieser Gruppe können die Dateireplikation auf dem lokalen Computer verwalten. Dateireplikation wird hauptsächlich in Active Directory-Domänen und auf Windows-Servern verwendet.
- **Sicherungs-Operatoren** Mitglieder dieser Gruppe können Dateien und Verzeichnisse der Arbeitsstation sichern und wiederherstellen. Sie können sich am lokalen Computer anmelden, Dateien sichern oder wiederherstellen und den Computer herunterfahren. Wegen der Art, wie ihr Konto konfiguriert ist, können sie Dateien unabhängig davon sichern, ob sie über Schreib- oder Lesezugriff auf die Dateien verfügen. Allerdings können sie die Zugriffsberechtigungen der Dateien nicht ändern und auch keine anderen Verwaltungsarbeiten durchführen.
- **WindowsRMRemoteWMIUsers_** Mitglieder dieser Gruppe können über die Windows-Remoteverwaltung auf WMI-Ressourcen zugreifen.
- **Zugriffssteuerungs-Unterstützungsoperatoren** Mitglieder dieser Gruppe können remote Autorisierungsattribute und -berechtigungen für Ressourcen auf dem Computer abfragen.

HINWEIS

In Windows gibt es mehrere Operatorgruppen. Standardmäßig sind keine anderen Gruppen oder Benutzerkonten Mitglieder dieser Gruppe. Dadurch ist sichergestellt, dass Sie den Zugriff explizit gewähren müssen.

In den meisten Fällen legen Sie den Benutzerzugriff mit den Gruppen *Benutzer* oder *Administratoren* fest. Sie können die Benutzer- und Administratorzugriffsebenen einstellen, indem Sie als Kontentyp *Standardbenutzer* oder *Administrator* wählen. Diese einfachen Aufgaben können Sie zwar mit den Benutzerkontenoptionen der Systemsteuerung erledigen, aber um einen Benutzer zum Mitglied einer Gruppe zu machen, müssen Sie *Lokale Benutzer und Gruppen* in der Konsole *Computerverwaltung* verwenden.

Domänenanmeldung und lokale Anmeldung

Wenn Computer Mitglieder einer Domäne sind, geben Sie zur Anmeldung auf einem Computer und bei der Domäne gewöhnlich ein Domänenkonto an. Alle Administratoren einer Domäne haben Zugriff auf die Ressourcen der lokalen Arbeitsstationen, die Mitglieder der Domäne sind. Benutzer können dagegen nur die lokalen Arbeitsstationen verwenden, an denen sie sich anmelden dürfen. Standardmäßig kann sich in einer Domäne jeder Benutzer mit einem gültigen Domänenkonto auf jedem Computer anmelden, der Mitglied der Domäne ist. Einmal auf einem Computer angemeldet, hat der Benutzer Zugang zu allen Ressourcen, die er mit den Berechtigungen seines Kontos oder der Gruppen, zu denen das Konto gehört, verwenden darf, sei es direkt oder indirekt über forderungsbasierte Zugriffsrichtlinien. Dazu gehören Ressourcen aus der Domäne ebenso wie Ressourcen des lokalen Computers.

Mit *Active Directory-Benutzer und -Computer* können Sie die Anmeldung jedes einzelnen Benutzers auf bestimmte Arbeitsstationen der Domäne beschränken. Tippen oder klicken Sie in *Active Directory-Benutzer und -Computer* mit der rechten Maustaste auf das Benutzerkonto oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*. Tippen oder klicken Sie auf der Registerkarte *Konto* des Dialogfelds *Eigenschaften* auf *Anmelden an* und legen Sie dann mit den Optionen des Dialogfelds *Anmeldearbeitsstationen* fest, bei welchen Arbeitsstationen sich der Benutzer anmelden darf. Allerdings müssen Sie sich nicht zwangsläufig an einer Domäne anmelden, wenn Sie mit Windows 8 arbeiten. Computer, die für Arbeitsgruppen konfiguriert sind, verfügen nur über lokale Konten. Vielleicht müssen Sie sich auch auf einem Computer, der Mitglied einer Domäne ist, lokal anmelden, um bestimmte Verwaltungsarbeiten durchzuführen. Nur Benutzer, die über ein lokales Benutzerkonto verfügen, können sich lokal anmelden. Wenn Sie sich lokal anmelden, haben Sie Zugang zu allen Ressourcen, die Sie mit den Berechtigungen Ihres Kontos oder der Gruppen, zu denen das Konto gehört, verwenden dürfen.

PRAXISTIPP

Verwechseln Sie die Beschränkungen der Anmeldearbeitsstationen nicht mit primären Computern. Von primären Computern ist in der Richtlinie *Ordner nur auf primären Computern umleiten* die Rede, die in den administrativen Vorlagen der Computerkonfiguration unter *System\Ordnerumleitung* zu finden ist. Mit dieser Richtlinie können Administratoren festlegen, von welchen Computern Benutzer Zugriff auf Roamingprofile und umgeleitete Ordner haben. Ziel dieser Richtlinie ist es, persönliche Daten und Firmendaten zu schützen, wenn sich Benutzer auf anderen Computern als denen anmelden, auf denen sie gewöhnlich arbeiten. Die Datensicherheit wird verbessert, indem diese Daten auf den Computern, die normalerweise nicht verwendet werden, nicht heruntergeladen und zwischengespeichert werden. Im Kontext dieser Richtlinie ist ein primärer Computer ein Computer, für den die Arbeit mit umgeleiteten Daten ausdrücklich zugelassen wurde. Dazu ist es erforderlich, die erweiterten Eigenschaften eines Benutzers oder einer Gruppe in Active Directory zu bearbeiten und die Namen der zugelassenen Computer in der Eigenschaft *msDS-PrimaryComputer* festzulegen.

Benutzerkontensteuerung und Anhebungsaufforderungen

Die Benutzerkontensteuerung (User Account Control, UAC) wirkt sich auf die Berechtigungen aus, die Standardbenutzern und Administratoren zur Verfügung stehen, auf die Installation und die Ausführung von Programmen, und so weiter. In diesem Abschnitt möchte ich die Beschreibung aus Kapitel 1, »Einführung in die Windows 8-Administration«, wieder aufgreifen und ausführlicher schildern, wie sich die Benutzerkontensteuerung auf Benutzer- und Administratorkonten auswirkt. Für die Verwaltung von Windows 8-Systemen zählt dies zum unverzichtbaren Grundlagenwissen.

HINWEIS

Die Funktionsweise der Benutzerkontensteuerung zu verstehen hilft Ihnen, ein besserer Administrator zu werden. Zur Unterstützung der Benutzerkontensteuerung mussten viele Details des Windows-Betriebssystems überarbeitet werden. Einige der weitreichendsten Änderungen haben mit der Art und Weise zu tun, wie Anwendungen installiert und ausgeführt werden. In Kapitel 8, »Installieren und Verwalten von Programmen«, finden Sie eine ausführliche Beschreibung der Auswirkungen der Architekturänderungen auf die Ausführung von Anwendungen unter Windows 8.

Ein zweiter Blick auf Standardbenutzer- und Administratorkonten

Unter Windows XP und früheren Windows-Versionen konnten böswillige Softwareprogramme die Tatsache ausnutzen, dass die meisten Benutzerkonten als Mitglieder der Gruppe der lokalen Administratoren konfiguriert sind. Das ermöglicht es der Schadsoftware nicht nur, sich selbst zu installieren, sondern auch, mit diesen weitreichenden Rechten Unheil auf dem Computer anzurichten, denn Programme, die von Administratoren installiert werden, können Bereiche des Dateisystems und der Registrierung überschreiben, die sonst sicher sind.

Um der wachsenden Bedrohung durch bösartige Software zu begegnen, gehen die Betroffenen zunehmend dazu über, den Zugang zu den Computern zu beschränken und den Benutzern die Anmeldung mit Standardbenutzerkonten vorzuschreiben. Administratoren müssen dann *Ausführen als* benutzen, um Verwaltungsarbeiten durchführen zu können. Leider können sich solche Änderungen in der Verfahrensweise stark auf die Produktivität auswirken. Wer unter Windows XP als Standardbenutzer angemeldet ist, kann manche der einfachsten Arbeiten nicht mehr durchführen. Beispielsweise kann er die Uhr oder das Datum nicht einstellen und weder die Zeitzone des Computers noch die Energieoptionen ändern. Viele Softwareprogramme, die für Windows XP entwickelt wurden, funktionieren ohne Administratorrechte einfach nicht mehr richtig. Solche Programme verwenden die Rechte der lokalen Administratoren beispielsweise bei der Installation und der späteren Benutzung für Schreibzugriffe auf Systembereiche. Außerdem sagt

Ihnen Windows XP nicht vor einer Operation, ob Sie zur Durchführung Administratorrechte brauchen oder nicht.

Die Benutzerkontensteuerung versucht, die Arbeit mit dem Computer zu erleichtern und gleichzeitig die Sicherheit zu verbessern, indem sie neu definiert, wie Standardbenutzerkonten und Administratorkonten verwendet werden. Die Benutzerkontensteuerung stellt eine grundlegende Änderung dar, weil sie ein Grundgerüst vorgibt, das die Verwendung der Administratorrechte einschränkt und verlangt, dass alle Anwendungen in einem bestimmten Benutzermodus ausgeführt werden. Auf diese Weise verhindert die Benutzerkontensteuerung ungewollte Änderungen der Systemeinstellung und hindert nichtautorisierte Anwendungen daran, sich zu installieren oder böswillige Aktionen durchzuführen.

Wegen der Benutzerkontensteuerung definiert Windows 8 zwei Arten von Benutzerkonten: Standard und Administrator. Außerdem definiert Windows 8 zwei Modi (Ausführungsstufen) für Anwendungen: Standardbenutzermodus und Administratormodus. Der größte Teil der Software kann mit Standardbenutzerkonten ausgeführt werden und Systemeinstellungen ändern, die sich weder auf andere Benutzer noch auf die Sicherheit des Computers auswirken. Administratorkonten ermöglichen den vollständigen Zugriff auf den Computer und die Durchführung aller gewünschten Änderungen. Wenn ein Administrator eine Anwendung startet, gelten sein Zugriffstoken und die damit verbundenen Administratorrechte für die Anwendung, die somit über alle Rechte und Berechtigungen eines lokalen Computeradministrators verfügt. Startet ein Standardbenutzer eine Anwendung, gelten auch sein Zugriffstoken und die damit verbundenen Rechte zur Laufzeit für die Anwendung, die somit auf die Rechte und Berechtigungen eines Standardbenutzers beschränkt bleibt. Außerdem werden alle Anwendungen bei der Installation so konfiguriert, dass sie in einem bestimmten Modus laufen. Alle Arbeiten, die von Standardmodusanwendungen durchgeführt werden und Administratorrechte erfordern, werden nicht nur beim Setup erkannt, sondern müssen auch vom Benutzer genehmigt werden.

In Windows 8 verfügen Standardbenutzerkonten über folgende Berechtigungen:

- Installieren von Schriftarten, Anzeigen der Systemuhr und des Kalenders, Einstellen der Zeitzone
- Ändern der Einstellungen der Anzeige und der Energieoptionen
- Hinzufügen von Druckern und anderen Geräten (sofern die erforderlichen Treiber bereits auf dem Computer installiert sind oder von einem IT-Administrator installiert werden)
- Herunterladen und Installieren von Updates (sofern die Updates benutzerkontensteuerungskompatible Installationsprogramme verwenden)
- Erstellen und Konfigurieren von VPN-Verbindungen (Virtuelles Privates Netzwerk). VPN-Verbindungen dienen dazu, über das öffentliche Internet hinweg sichere Verbindungen zu privaten Netzwerken herzustellen.
- Installieren von WEP (Wired Equivalent Privacy) für die Verbindung mit gesicherten Drahtlosnetzwerken. Das WEP-Sicherheitsprotokoll verleiht Drahtlosnetzwerken eine höhere Sicherheit.
- Zugreifen auf den Computer über das Netzwerk und Herunterfahren des Computers.

Windows 8 definiert auch zwei Ausführungsebenen für Anwendungen: Standard und Administrator. Windows 8 ordnet den meisten Anwendungen und Prozessen ein Sicherheitstoken zu, mit dessen Hilfe es erkennt, ob ein Benutzer erhöhte Rechte braucht, um eine Anwendung auszuführen. Wenn eine Anwendung über ein Standardtoken verfügt oder nicht als Administratoranwendung identifiziert werden kann, sind zur Ausführung der Anwendung keine erhöhten Rechte erforderlich und Windows 8 startet die Anwendung als Standardanwendung. Verfügt die Anwendung über ein Administratortoken, so sind zur Ausführung der Anwendung erhöhte Rechte erforderlich und Windows 8 holt vom Benutzer die Erlaubnis oder Bestätigung ein, bevor es mit der Ausführung der Anwendung beginnt.

Der Vorgang, vor der Ausführung einer Anwendung im Administratormodus und vor der Durchführung von Änderungen an der Systemkonfiguration eine Genehmigung einzuholen, gehört zur *Anhebung der Rechte* (auch als Erhöhung der Rechte bezeichnet). Diese Art der Rechteanhebung verbessert die Sicherheit und verringert die Chancen bösartiger Software, weil Benutzer informiert werden, bevor etwas geschieht, das sich auf die Systemeinstellung auswirken kann, und weil Anwendungen keine Administratorrechte erhalten, ohne dass zuerst ein Benutzer darüber informiert wird. Die Erhöhung der Rechte schützt auch Administratoranwendungen vor Angriffen durch Standardanwendungen. Weitere Informationen über die Erhöhung der Rechte und die Arbeitsweise der Benutzerkontensteuerung finden Sie in Kapitel 8.

In der Standardeinstellung schaltet Windows 8 auf den sicheren Desktop um, bevor es die Anhebungseingabeaufforderung anzeigt. Der sichere Desktop schränkt den Zugriff für Programme und Prozesse auf die Desktopumgebung ein, was die Möglichkeit verhindert, dass ein böswilliges Programm oder ein böswilliger Benutzer sich Zugriff auf den Prozess verschaffen, dessen Rechte erhöht werden. Sollten Sie nicht wollen, dass Windows 8 auf den sicheren Desktop umschaltet, bevor es eine Anhebungseingabeaufforderung anzeigt, können Sie Einstellungen konfigurieren, die dafür sorgen, dass statt des sicheren Desktops der Standarddesktop verwendet wird. Dadurch wird der Computer aber verwundbarer gegenüber Malware und Angriffen.

Optimieren von Benutzerkontensteuerung und Administratorgenehmigungsmodus

Jeder Computer hat ein integriertes lokales Administratorkonto. Dieses vordefinierte Konto wird nicht durch die Benutzerkontensteuerung geschützt. Wenn Sie daher dieses Konto für die Administration verwenden, setzen Sie Ihren Computer unter Umständen einer Gefahr aus. Um die Computer in Umgebungen zu schützen, in denen Sie ein lokales Administratorkonto für die Administration einsetzen, sollten Sie ein neues lokales Administratorkonto anlegen und dieses Konto für die Administration verwenden.

Die Benutzerkontensteuerung kann für jedes Benutzerkonto individuell konfiguriert oder deaktiviert werden. Wenn Sie die Benutzerkontensteuerung für ein Benutzerkonto deaktivieren, verlieren Sie die zusätzlichen Sicherheitsmechanismen, die von der Benutzerkontensteuerung zur Verfügung gestellt werden, und setzen den Computer Gefahren aus. Wenn Sie die Benutzerkontensteuerung deaktivieren oder wieder aktivieren, nachdem sie deaktiviert wurde, müssen Sie den Computer neu starten, damit die Änderung wirksam wird. Der Administratorgenehmigungsmodus ist die Schlüsselkomponente der Benutzerkontensteuerung, die darüber entscheidet, ob und wie Administratoren zur Bestätigung aufgefordert werden, wenn sie Administratoranwendungen ausführen. Normalerweise funktioniert der Administratorgenehmigungsmodus folgendermaßen:

- Alle Administratorkonten, auch das vordefinierte lokale Administratorkonto, werden im Administratorgenehmigungsmodus ausgeführt und unterliegen ihm.
- Da alle Administratorkonten im Administratorgenehmigungsmodus ausgeführt werden und diesem unterliegen, sehen alle Administratoren, einschließlich des vordefinierten lokalen Administratorkontos, eine Anhebungsaufforderung, wenn sie Administratoranwendungen ausführen.

Wenn Sie als Administrator angemeldet sind, können Sie die Funktionsweise der Benutzerkontensteuerung für alle Benutzer ändern. Gehen Sie dazu folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann unter *Wartungszentrum* auf *Einstellungen der Benutzerkontensteuerung ändern*.
2. Stellen Sie im Dialogfeld *Einstellungen für Benutzerkontensteuerung* (Abbildung 7.1) mit dem Schieberegler ein, wann die Benutzer über Änderungen am Computer informiert werden, und tippen oder klicken Sie auf *OK*. Tabelle 7.1 fasst die verfügbaren Optionen zusammen.

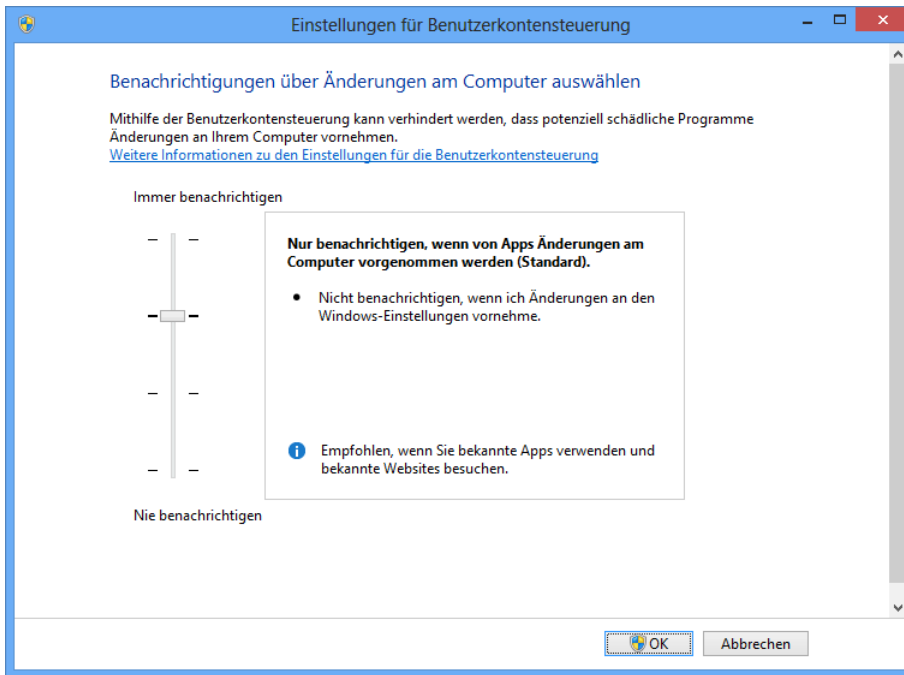


Abbildung 7.1 Das Dialogfeld *Einstellungen für Benutzerkontensteuerung*

Tabelle 7.1 Einstellungen für Benutzerkontensteuerung

Option	Beschreibung	Empfohlene Verwendung	Sicherer Desktop?
<i>Immer benachrichtigen</i>	Benachrichtigt den aktuellen Benutzer immer, wenn Programme versuchen, Software zu installieren oder Änderungen am Computer vorzunehmen, und wenn der Benutzer Windows-Einstellungen ändert.	Verwenden Sie diese Option, wenn ein Computer höchstmögliche Sicherheit braucht und die Benutzer häufig Software installieren und unbekannte Websites besuchen.	Ja
<i>Nur benachrichtigen, wenn ... (Standard)</i>	Benachrichtigt den aktuellen Benutzer nur, wenn Programme versuchen, Änderungen am Computer vorzunehmen, aber nicht, wenn der Benutzer Windows-Einstellungen ändert.	Verwenden Sie diese Option, wenn ein Computer hohe Sicherheit benötigt und Sie die Zahl der angezeigten Benachrichtigungsmeldungen verringern wollen.	Ja
<i>Nur benachrichtigen, wenn ... (Desktop nicht abblenden)</i>	Wie die Einstellung <i>Standard</i> , verhindert aber zusätzlich, dass die Benutzerkontensteuerung auf den sicheren Desktop umschaltet.	Stellen Sie diese Option ein, wenn die Benutzer in einer vertrauenswürdigen Umgebung mit vertrauten Anwendungen arbeiten und keine ungewöhnlichen Websites besuchen.	Nein
<i>Nie benachrichtigen</i>	Schaltet alle Eingabeaufforderungen der Benutzerkontensteuerung ab.	Wählen Sie diese Option, wenn die Sicherheit nicht von großer Bedeutung ist und die Benutzer in einer vertrauenswürdigen Umgebung mit Programmen arbeiten, die nicht für Windows 8 zertifiziert sind, weil sie die Benutzerkontensteuerung nicht unterstützen.	Nein

In den Gruppenrichtlinien können Sie den Administratorgenehmigungsmodus und die Anzeige von Anhebungsaufforderungen mit den Einstellungen im Zweig *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen* verwalten. Hier stehen unter anderem folgende Richtlinien zur Verfügung:

- *Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administratorkonto* Legt fest, ob Benutzer und Prozesse, die als das vordefinierte lokale Administratorkonto laufen, dem Administratorgenehmigungsmodus unterliegen. In der Standardeinstellung ist diese Funktion deaktiviert, das bedeutet, dass das vordefinierte lokale Administratorkonto nicht dem Administratorgenehmigungsmodus unterliegt und auch bezüglich Anhebungseingabeaufforderungen nicht denselben Beschränkungen unterliegt wie Administratoren im Administratorgenehmigungsmodus. Wenn Sie diese Einstellung deaktivieren, unterliegen Benutzer und Prozesse, die als das vordefinierte lokale Administratorkonto laufen, nicht mehr dem Administratorgenehmigungsmodus und damit auch nicht mehr bezüglich der Anhebungseingabeaufforderungen dem Verhalten, das für Administratoren im Administratorgenehmigungsmodus gilt.
- *Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern* Legt fest, ob Programme für Eingabehilfen in der Benutzeroberfläche (UIAccess-Anwendungen) den sicheren Desktop automatisch für Anhebungsaufforderungen deaktivieren, die von einem Standardbenutzer verwendet werden. Wenn Sie diese Einstellung aktivieren, können UIAccess-Programme, darunter auch die Windows-Remoteunterstützung, den sicheren Desktop für Anhebungsaufforderungen deaktivieren.
- *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorgenehmigungsmodus* Legt fest, ob Administratoren, die dem Administratorgenehmigungsmodus unterliegen, eine Anhebungseingabeaufforderung angezeigt bekommen, wenn sie Administratoranwendungen ausführen. Außerdem steuert diese Richtlinie, wie die Anhebungseingabeaufforderung arbeitet. In der Standardeinstellung werden Administratoren auf dem sicheren Desktop nach ihrer Genehmigung gefragt, wenn Administratoranwendungen gestartet werden. Sie können diese Richtlinie so konfigurieren, dass Administratoren ohne den sicheren Desktop nach ihrer Genehmigung gefragt werden, zur Eingabe von Anmeldeinformationen mit oder ohne sicheren Desktop aufgefordert werden (wie Standardbenutzer) oder nur nach ihrer Genehmigung gefragt werden, wenn es sich um Windows-fremde Programmdateien handelt. Sie können die Richtlinie auch so einstellen, dass Administratoren überhaupt nicht nach ihrer Genehmigung gefragt werden; in diesem Fall werden die Rechte des Administrators automatisch angehoben. Keine dieser Einstellungen verhindert, dass ein Administrator mit der rechten Maustaste auf eine Anwendungsverknüpfung klickt oder sie gedrückt hält und den Befehl *Als Admin ausführen* wählt.
- *Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer* Bestimmt, ob Benutzer, die mit einem Standardbenutzerkonto angemeldet sind, eine Anhebungsaufforderung sehen, wenn sie Administratoranwendungen ausführen. Gewöhnlich wird von Benutzern, die mit einem Standardbenutzerkonto angemeldet sind, auf dem sicheren Desktop die Eingabe der Anmeldeinformationen eines Administrators verlangt, wenn sie Administratoranwendungen ausführen oder Administrationsaufgaben erledigen. Sie können diese Richtlinie auch so einstellen, dass die Benutzer statt auf dem sicheren Desktop auf dem Standarddesktop zur Eingabe der Anmeldeinformationen aufgefordert werden. Und Sie können die Anhebungsanforderungen automatisch ablehnen, damit die Benutzer gar nicht zu dieser Eingabe aufgefordert werden. In diesem Fall können Benutzer auch nicht die Rechte anheben, indem sie die Anmeldeinformationen eines Administrators eingeben. Das verhindert aber nicht, dass Benutzer die Verknüpfung zu einer Anwendung mit der rechten Maustaste anklicken oder sie gedrückt halten und *Als Admin ausführen* wählen können.

- *Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind* Legt fest, ob Anwendungen signiert und überprüft sein müssen, damit die Anhebung durchgeführt wird. Ist diese Richtlinie aktiviert, werden die Rechte ausführbarer Dateien nur angehoben, wenn sie die Signaturprüfung bestehen und entsprechende Zertifikate im Speicher für vertrauenswürdige Herausgeber eingetragen sind. Verwenden Sie diese Möglichkeit nur, wenn höchstmögliche Sicherheit gebraucht wird und Sie geprüft haben, dass alle benutzten Anwendungen signiert und gültig sind.
- *Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind* Legt fest, ob UIAccess-Programme an einem sicheren Speicherort im Dateisystem liegen müssen, damit die Anhebung durchgeführt wird. Ist diese Richtlinie aktiviert, müssen UIAccess-Programme unter %SystemRoot%\Program Files, %SystemRoot%\Program Files (x86) oder %SystemRoot%\Windows\System32 liegen.
- *Benutzerkontensteuerung: Alle Administratoren im Administratorgenehmigungsmodus ausführen* Entscheidet darüber, ob Benutzer, die mit einem Administratorkonto angemeldet sind, dem Administratorgenehmigungsmodus unterliegen. Standardmäßig ist diese Funktion aktiviert. Das bedeutet, dass Administratoren dem Administratorgenehmigungsmodus unterliegen und dass für sie auch die Anhebungsbestätigung gilt, wie sie für Administratoren im Administratorgenehmigungsmodus festgelegt ist. Wenn Sie diese Einstellung deaktivieren, unterliegen Benutzer, die mit einem Administratorkonto angemeldet sind, nicht mehr dem Administratorgenehmigungsmodus und daher auch nicht mehr der Anhebungsaufforderung, die für Administratoren im Administratorgenehmigungsmodus festgelegt ist.

PRAXISTIPP Die entsprechenden Benutzerkontensteuerungseinstellungen für Geräte werden in Kapitel 8 beschrieben. Im Abschnitt »Optimieren der Virtualisierung und die Anhebungsaufforderung bei Installationen« finden Sie weitere Informationen.

In einer Domänenumgebung können Sie die gewünschten Sicherheitseinstellungen für eine bestimmte Computergruppe in der Weise vornehmen, wie es in Active Directory üblich ist. Mit den lokalen Sicherheitsrichtlinien können Sie diese Einstellungen auch für einzelne lokale Computer vornehmen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie die Konsole *Lokale Sicherheitsrichtlinie*. Dazu können Sie zum Beispiel die WINDOWS-Taste drücken, **Secpol.msc** eingeben und dann die Eingabetaste drücken.
2. Erweitern Sie in der Konsolenstruktur den Knoten *Lokale Richtlinien* unter *Sicherheitseinstellungen* und wählen Sie dann *Sicherheitsoptionen*, wie in Abbildung 7.2 gezeigt.
3. Tippen oder klicken Sie die gewünschte Richtlinie doppelt an, führen Sie die erforderlichen Änderungen durch und tippen oder klicken Sie dann auf **OK**. Wiederholen Sie diesen Schritt nach Bedarf, um andere Richtlinien zu ändern.

Verwalten der lokalen Anmeldung

Alle lokalen Computerkonten sollten durch Kennwörter geschützt sein. Wird ein Konto ohne Kennwort erstellt, ist das Konto ungeschützt und jeder kann sich lokal anmelden. Allerdings kann ein lokales Konto ohne Kennwort nicht für einen Remotezugriff auf einen Computer verwendet werden.

Die folgenden Abschnitte beschreiben die Erstellung und Einrichtung von lokalen Benutzerkonten. Auf jeder Arbeitsstation gibt es lokale Computerkonten, unabhängig davon, ob der Computer Mitglied einer Heimnetzgruppe, Arbeitsgruppe oder Domäne ist.

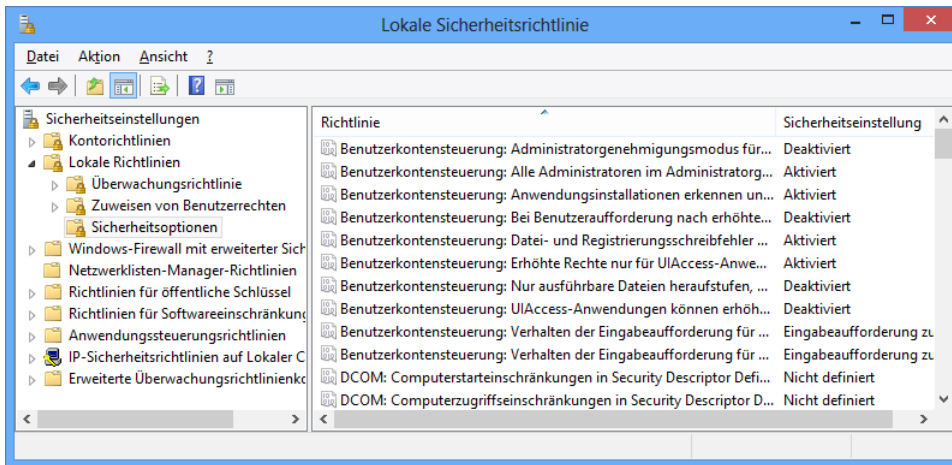


Abbildung 7.2 Die Konsole *Lokale Sicherheitsrichtlinie*

Erstellen lokaler Benutzerkonten in einer Heimnetzgruppe oder Arbeitsgruppe

Windows 8 bietet zwei Arten von lokalen Benutzerkonten: normal und synchronisiert. Wenn ein Computer Mitglied einer Heimnetzgruppe oder Arbeitsgruppe ist, können Sie mit folgenden Schritten ein normales lokales Benutzerkonto auf dem Computer erstellen:

1. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *Benutzerkonten und Family Safety* auf *Kontotyp ändern*. Dadurch öffnet sich die Seite *Konten verwalten*.

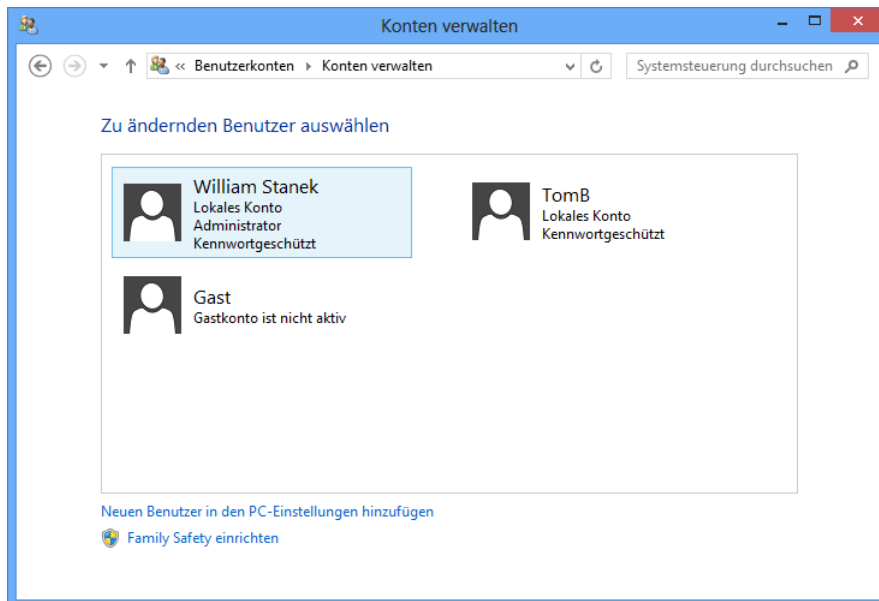


Abbildung 7.3 In einer Heimnetzgruppe oder Arbeitsgruppe verwenden Sie die Seite *Konten verwalten* aus der Systemsteuerung, um lokale Benutzerkonten anzuzeigen

Wie aus Abbildung 7.3 hervorgeht, listet die Seite *Konten verwalten* alle konfigurierbaren Benutzerkonten des lokalen Computers nach Kontentyp und mit Konfigurationsdetails auf. Verfügt ein Konto über ein Kennwort, wird es als kennwortgeschützt aufgeführt. Wurde ein Konto deaktiviert, wird es als nicht aktiv aufgeführt.

2. Tippen oder klicken Sie auf *Neuen Benutzer in den PC-Einstellungen hinzufügen*. Dadurch öffnet sich die Seite *Neues Konto erstellen*. Klicken Sie auf der Seite *Benutzer* unter *Weitere Benutzer* auf *Benutzer hinzufügen*. Dadurch öffnet sich die Seite *Benutzer hinzufügen*.
3. Wenn keine Verbindung mit dem Internet besteht, können Sie standardmäßig nur ein normales lokales Benutzerkonto erstellen. Im anderen Fall müssen Sie die Verknüpfung *Ohne Microsoft-Konto anmelden* antippen oder anklicken.
4. Wenn der Computer mit dem Internet verbunden ist, tippen oder klicken Sie auf *Lokales Konto*. Das ist nicht erforderlich, wenn der Computer nicht mit dem Internet verbunden ist.
5. Geben Sie den Namen des lokalen Kontos ein. Legen Sie gegebenenfalls ein Kennwort fest, bestätigen Sie es durch eine erneute Eingabe und geben Sie außerdem noch einen Kennworthinweis an.
6. Tippen oder klicken Sie auf *Weiter* und dann auf *Fertig stellen*. Das Konto wird standardmäßig als Standardbenutzerkonto erstellt. Um dem Benutzer alle Berechtigungen für den lokalen Computer zu geben, müssen Sie den Kontentyp in ein Administratorkonto ändern, wie später in diesem Kapitel unter der Überschrift »Ändern des Typs eines lokalen Benutzerkontos« beschrieben.

Ein synchronisiertes Konto ist ein Microsoft-Konto. Auf einem Computer, der Mitglied einer Heimnetzgruppe oder Arbeitsgruppe ist, können Sie mit folgenden Schritten ein Microsoft-Konto erstellen.

1. Öffnen Sie die *PC-Einstellungen*. Dazu können Sie zum Beispiel die WINDOWS-Taste+I drücken und dann auf *PC-Einstellungen ändern* tippen oder klicken.
2. Tippen oder klicken Sie auf der Seite *Benutzer* auf *Benutzer hinzufügen* und folgen Sie der Anleitung, um das Benutzerkonto zu erstellen.

Um ein Microsoft-Konto zu erstellen, muss der Computer mit dem Internet verbunden sein. Wenn Sie ein Microsoft-Konto erstellen, stellt Windows 8 eine Verbindung zum Microsoft Store her und überprüft, ob für die E-Mail-Adresse, die Sie angeben, bereits ein Konto eingerichtet wurde. Ist dies nicht der Fall, werden Sie dazu aufgefordert, dieses Konto einzurichten. Dazu geben Sie die E-Mail-Adresse und das Kennwort für das Konto ein sowie den Vor- und Zunamen des Benutzers, Land oder Region und den ZIP-Code oder die Postleitzahl.

Anschließend werden Sie aufgefordert, Sicherheitsinformationen hinzuzufügen, beispielsweise eine Telefonnummer, damit man Ihnen den Code für das Rücksetzen des Kontokennwords als Textnachricht oder automatischen Anruf, eine andere E-Mail-Adresse für die Zusendung einer Nachricht zum Rücksetzen des Kennworts und eine geheime Frage mit Antwort übermitteln kann, um gegebenenfalls die Identität des Benutzers zu überprüfen.

Schließlich müssen Sie noch den Geburtstag und das Geschlecht des Benutzers angeben und einen Überprüfungstext eingeben. Wenn Sie auf *Fertig stellen* klicken, wird das Microsoft-Konto online und auf dem lokalen Computer erstellt.

HINWEIS

Wenn der Computer nicht mit dem Internet verbunden ist und Sie versuchen, ein Microsoft-Konto zu erstellen, können Sie nur ein lokales Konto erstellen. Sobald wieder eine Verbindung mit dem Internet besteht, müssen Sie sich dann als dieser Benutzer auf dem Computer anmelden, in den *PC-Einstellungen* die Seite *Benutzer* aufschlagen und auf *Zu einem Microsoft-Konto wechseln* tippen oder klicken. Anschließend werden Sie durch die Kontenerstellung geführt.

Die Synchronisierung eines Kontos ermöglicht es, Anwendungseinstellungen, Profildaten und einige Profilinhalte auf den verschiedenen Geräten, die der Benutzer verwendet, synchron zu halten. Welche Einstellungen synchronisiert werden und welche nicht, wird in den *PC-Einstellungen* mit den Optionen auf der Seite *Einstellungen synchronisieren* festgelegt.

Gewähren der lokalen Anmeldung bei vorhandenem Domänenkonto

Wenn sich ein Benutzer lokal auf einem Computer anmelden muss und bereits über ein Domänenkonto verfügt, können Sie ihm mit folgenden Schritten die Berechtigung zur lokalen Anmeldung geben:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Benutzerkonten* auf die Verknüpfung *Kontotyp ändern*. Daraufhin öffnet sich das Dialogfeld *Benutzerkonten*. Wie Abbildung 7.4 zeigt, listet das Dialogfeld *Benutzerkonten* alle konfigurierbaren Benutzerkonten auf dem lokalen Computer unter Angabe der Domäne und der Gruppenmitgliedschaft auf.

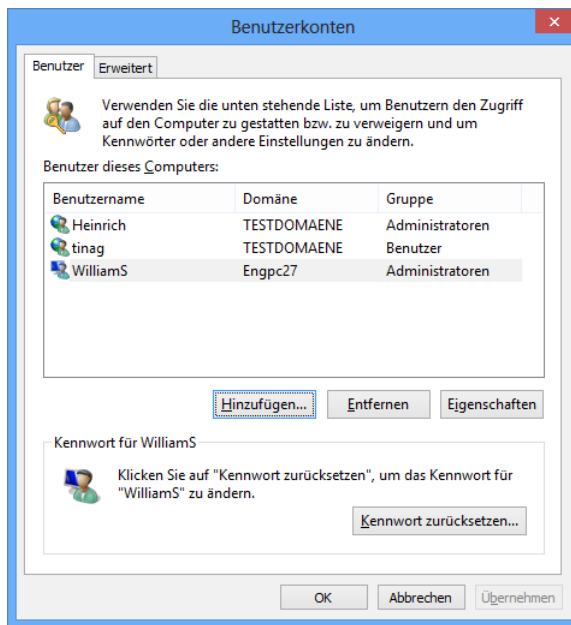


Abbildung 7.4 Im Dialogfeld *Benutzerkonten* verwalten Sie lokale Benutzerkonten auf einem Computer, der Mitglied einer Domäne ist

2. Tippen oder klicken Sie auf *Hinzufügen*. Dadurch wird der Assistent zum Hinzufügen von Benutzern gestartet.
3. Sie erstellen ein lokales Computerkonto für einen Benutzer, der bereits über ein Domänenkonto verfügt. Geben Sie in den Eingabefeldern den Domänenkontennamen des Benutzers und die Domäne ein oder tippen oder klicken Sie auf *Durchsuchen*, um im Dialogfeld *Benutzer auswählen* nach einem Benutzerkonto zu suchen. Klicken Sie auf *Weiter*.
4. Ein Standardbenutzerkonto wird als Mitglied der lokalen Gruppe *Benutzer* angelegt. Soll der Benutzer die üblichen Berechtigungen eines normalen Benutzers erhalten, wählen Sie *Standard*.
5. Ein Administratorkonto wird als Mitglied der lokalen Gruppe *Administratoren* erstellt. Wenn der Benutzer das volle Zugriffsrecht auf einen Computer erhalten soll, wählen Sie *Administrator*.

6. Das Konto *Andere* wird als Mitglied der Gruppe erstellt, die Sie auswählen. Wenn der Benutzer die Berechtigungen einer bestimmten Gruppe erhalten soll, wählen Sie *Andere* und dann die gewünschte Gruppe.
7. Tippen oder klicken Sie auf *Weiter* und dann auf *Fertig stellen*. Wenn Sie andere Berechtigungen festlegen oder den Benutzer zu anderen lokalen Gruppen hinzufügen müssen, folgen Sie der Beschreibung im Abschnitt »Verwalten lokaler Benutzerkonten und Gruppen« weiter hinten in diesem Kapitel.

Ändern des Typs eines lokalen Benutzerkontos

Das Programm *Benutzerkonten* aus der Systemsteuerung ermöglicht auf einfache Weise die Änderung der Kontentypen für lokale Benutzer. Sie können sehr schnell einen der vordefinierten Kontentypen *Standard* und *Administrator* festlegen. Für eine genauere Einstellung müssen Sie allerdings auf die Konsole *Lokale Benutzer und Gruppen* zurückgreifen und die Gruppenmitgliedschaften individuell festlegen. (Weitere Informationen zu diesem Thema finden Sie im Abschnitt »Verwalten der Mitglieder lokaler Gruppen« weiter hinten in diesem Kapitel.)

In einer Heimnetzgruppe oder Arbeitsgruppe können Sie den Kontentyp für einen lokalen Computerbenutzer folgendermaßen von *Standard* auf *Administrator* und umgekehrt ändern:

1. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *Benutzerkonten* auf *Kontotyp ändern*. Es öffnet sich die Seite *Konten verwalten*.
2. Tippen oder klicken Sie auf das Konto, das Sie ändern möchten, und dann auf *Kontotyp ändern*.
3. Legen Sie auf der Seite *Kontotyp ändern* durch die Wahl von *Standard* oder *Administrator* die Zugriffsebene für den Benutzer fest und tippen oder klicken Sie dann auf *Kontotyp ändern*.

HINWEIS

Der Kontotyp des letzten auf einem Computer verbleibenden Administratorkontos lässt sich nicht ändern. Auf einem Computer muss es mindestens einen lokalen Administrator geben.

In einer Domäne können Sie den Kontentyp für einen lokalen Computerbenutzer folgendermaßen ändern:

1. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *Benutzerkonten* auf *Kontotyp ändern*. Es öffnet sich das Dialogfeld *Benutzerkonten*.
2. Tippen oder klicken Sie auf der Registerkarte *Benutzer* das Konto an, das Sie bearbeiten möchten, und tippen oder klicken Sie dann auf *Eigenschaften*.
3. Wählen Sie im *Eigenschaften*-Dialogfeld die Registerkarte *Gruppenmitgliedschaft*.
4. Wählen Sie als Kontentyp *Standardbenutzer* oder *Administrator*. Oder wählen Sie *Andere* und dann die gewünschte Gruppe.
5. Tippen oder klicken Sie zweimal auf *OK*.

Wechseln zwischen synchronisierten und normalen Konten

Mit dem Hilfsprogramm *PC-Einstellungen* können Sie auf einfache Weise synchronisierte auf normale Konten umstellen, und umgekehrt. In einer Heimnetzgruppe oder Arbeitsgruppe können Sie mit folgenden Schritten ein normales lokales Konto in ein Microsoft-Konto umwandeln, und umgekehrt:

1. Melden Sie sich als der betreffende Benutzer an und öffnen Sie die *PC-Einstellungen*. Dazu können Sie zum Beispiel die Tastenkombination **WINDOWS-Taste+I** drücken und dann auf *PC-Einstellungen ändern* tippen oder klicken.
2. Tippen oder klicken Sie auf der Seite *Benutzer* auf *Zu einem lokalen Konto wechseln* oder auf *Zu einem Microsoft-Konto wechseln*, je nach den Gegebenheiten, und folgen Sie dann der Anleitung.

Sie müssen mit dem Internet verbunden sein, um zu einem Microsoft-Konto zu wechseln.

Festlegen von Kennwörtern für lokale Benutzerkonten

In einer Heimnetzgruppen- oder Arbeitsgruppenkonfiguration werden lokale Benutzerkonten standardmäßig ohne Kennwörter erstellt. Das bedeutet, dass sich Benutzer auf der Willkommenseite standardmäßig mit einem simplen Klick auf ihren Kontennamen anmelden können. Zur Erhöhung der Sicherheit sollten alle lokalen Konten mit Kennwörtern versehen werden.

Am einfachsten erreichen Sie das, indem Sie sich mit jedem Konto anmelden, das ein Kennwort erhalten soll, und dem Konto dann mit dem Programm *Benutzerkonten* aus der Systemsteuerung ein Kennwort zuweisen. Wenn Sie bei der Zuweisung des Kennworts als der Benutzer angemeldet sind, dessen Konto das Kennwort erhält, brauchen Sie sich keine Gedanken darüber zu machen, ob Sie dadurch verschlüsselte Daten verlieren. Wenn Sie ein Kennwort zuweisen, ohne als der betreffende Benutzer angemeldet zu sein, verliert der Benutzer den Zugang zu seinen verschlüsselten Dateien, verschlüsselten E-Mails, persönlichen Zertifikaten und gespeicherten Kennwörtern. Das ist so, weil der Hauptschlüssel des Benutzers, der für den Zugriff auf das persönliche Verschlüsselungszertifikat und zur Entschlüsselung der Daten erforderlich ist, mit einem Hashwert verschlüsselt wurde, der auf einem leeren Kennwort basiert. Wenn Sie dann ein Kennwort zuweisen, stimmen die Hashwerte nicht überein und der Benutzer hat keinen Zugriff mehr auf seine eigenen Daten. Die einzige Lösung dieses Problems ist, durch die Löschung des Kontenkennworts die ursprüngliche Einstellung wiederherzustellen. Dann sollte der Benutzer eigentlich wieder Zugriff auf seine verschlüsselten Dateien haben. Wie bereits erwähnt, tritt dieses Problem nur bei den lokalen Konten für Computer und nicht bei Domänenbenutzerkonten auf.

TIPP

Nur das Programm *Benutzerkonten* ermöglicht Ihnen die Zuweisung eines Kennworthinweises, der sich als nützlich erweisen kann, wenn der Benutzer sein Kennwort vergessen hat. Ein anderes Mittel zur Wiederherstellung eines Kennworts ist eine Kennwörterücksetzdiskette, bei der es sich um eine Diskette oder ein USB-Flashlaufwerk handeln kann. Bei der Zuweisung von Kennwörtern dürfen Sie aber nicht vergessen, dass dies die einzigen Verfahren zur Wiederherstellung von Kennwörtern für lokale Benutzerkonten sind, wenn Sie keinen Datenverlust riskieren wollen. Warum? Sie können zwar für ein Benutzerkonto ein Kennwort erstellen, zurücksetzen oder löschen, aber dadurch werden alle persönlichen Zertifikate und gespeicherten Kennwörter gelöscht, die mit dem Konto verbunden sind. Das Ergebnis ist, dass der Benutzer nicht mehr auf seine verschlüsselten Dateien oder privaten E-Mails zugreifen kann, die er mit seinem geheimen Schlüssel verschlüsselt hat. Außerdem verliert er die gespeicherten Kennwörter für Websites und Netzwerkressourcen. Wichtig ist außerdem, dass dieses Problem nur bei lokalen Benutzerkonten auftritt. Administratoren können die Kennwörter von Domänenbenutzern ändern oder zurücksetzen, ohne dadurch den Zugriff auf verschlüsselte Daten zu gefährden.

Auf folgende Weise können Sie einem lokalen Benutzerkonto ein Kennwort zuweisen:

1. Melden Sie sich als der Benutzer an, für dessen Konto Sie ein Kennwort festlegen möchten. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *Benutzerkonten* auf *Kontotyp ändern*. Es öffnet sich die Seite *Konten verwalten*, und es erscheint die Seite *Konten verwalten*.

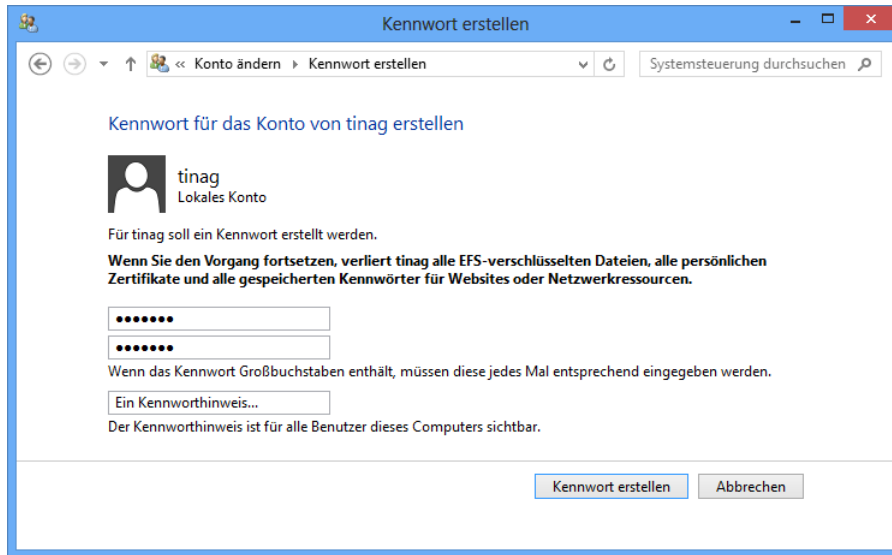


Abbildung 7.5 Erstellen eines Kennworts mit einem Kennwordhinweis

2. Tippen oder klicken Sie das Konto an, für das Sie ein Kennwort festlegen möchten. Um Datenverluste zu verhindern, muss es dasselbe Konto sein, mit dem Sie gerade angemeldet sind. Jedes Konto, das bereits über ein Kennwort verfügt, wird als kennwortgeschützt aufgelistet. Ein Konto ohne diese Kennzeichnung hat noch kein Kennwort.
3. Tippen oder klicken Sie auf *Kennwort erstellen*. Geben Sie ein Kennwort ein und bestätigen Sie es durch eine erneute Eingabe, wie in Abbildung 7.5 illustriert. Geben Sie anschließend einen Kennwordhinweis ein. Ein Kennwordhinweis ist ein Wort oder eine Phrase, die Ihnen helfen soll, sich an das Kennwort zu erinnern. Der Hinweis ist für alle sichtbar, die den Computer benutzen.
4. Tippen oder klicken Sie auf *Kennwort erstellen*.

Wiederherstellen der Kennwörter von lokalen Benutzerkonten

Wie bereits erwähnt, ist es bei Verlust eines Kennworts vorzuziehen, das Kennwort wiederherzustellen statt es zu ändern oder zu löschen, damit der Zugang zu den verschlüsselten Daten und gespeicherten Kennwörtern des Benutzers nicht verloren geht.

Windows 8 bietet zwei Wege zur Wiederherstellung von Benutzerkennwörtern:

- **Kennwordhinweis** Kennwordhinweise können auf der Willkommenseite gelesen werden. Gewöhnlich wird die Willkommenseite nach dem Hochfahren des Computers angezeigt, wenn noch niemand angemeldet ist. Falls bereits jemand an der Arbeitsstation angemeldet ist, bitten Sie ihn, sich abzumelden. Tippen oder klicken Sie auf den Benutzernamen, damit die Aufforderung zur Eingabe des Kennworts erscheint, und dann auf die blaue Eingabeschaltfläche, damit der Kennwordhinweis ange-

zeigt wird. Vielleicht hilft der Kennworthinweis dem Benutzer, sich an das Kennwort zu erinnern. Ist das nicht der Fall, brauchen Sie die Kennworrücksetzdiskette.

- **Kennworrücksetzdiskette** Kennworrücksetzdisketten können für jedes kennwortgeschützte lokale Benutzerkonto erstellt werden. Sie versetzen jeden in die Lage, das Kennwort des dazugehörigen lokalen Kontos zurückzusetzen, ohne das alte Kennwort zu kennen. Da jeder, der Zugang zu diesen Disketten hat, Kontenkennwörter ändern kann, sollten Sie die Kennworrücksetzdiskette an einem sicheren Ort aufbewahren. Sofern Sie den Benutzern erlauben, eine eigene Kennworrücksetzdiskette zu erstellen, sollten Sie dafür sorgen, dass die Benutzer verstehen, wie wichtig diese Disketten sind.

HINWEIS

Die Kennwörter für Domänenbenutzer und für lokale Benutzer werden unterschiedlich verwaltet. In Domänen verwalten Administratoren die Kennwörter von Domänenbenutzerkonten und können vergessene Kennwörter in der Konsole *Active Directory-Benutzer und -Computer* zurücksetzen.

Kennwörter für lokale Computerkonten können in einer sicheren, verschlüsselten Datei auf einer Kennworrücksetzdiskette gespeichert werden, bei der es sich um eine Diskette oder einen USB-Speicherstick handeln kann. Wie Sie eine Kennworrücksetzdiskette für den aktuellen Benutzer erstellen, wurde im Abschnitt »Erstellen und Verwenden einer Kennworrücksetzdiskette« in Kapitel 1 beschrieben. Und im Abschnitt »Rücksetzen des Kennworts eines Benutzers« in Kapitel 1 ist beschrieben, wie Sie das Kennwort für ein lokales Computerkonto zurücksetzen.

Kontrollieren der Anmeldung

Windows 8 zeigt standardmäßig einen Sperrbildschirm und einen Willkommensbildschirm an, unabhängig davon, ob ein Computer zu einer Heimnetzgruppe, einer Arbeitsgruppe oder einer Domäne gehört. Der Unterschied zwischen dem Sperrbildschirm und dem Willkommensbildschirm ist sehr wichtig.

Der Sperrbildschirm wird angezeigt, wenn niemand angemeldet ist. In *PC-Einstellungen* tippen oder klicken Sie auf *Anpassen* und dann auf *Sperrbildschirm*, um die entsprechenden Einstellungen vorzunehmen. Sie können ein Bild für den Sperrbildschirm auswählen und angeben, welche Anwendungen im Hintergrund laufen dürfen. Außerdem können Sie noch festlegen, ob und wie diese Anwendungen kurze Statusinfos und Meldungen anzeigen. Standardmäßig zeigen die Anwendungen Nachrichten, Kalender und Mail kurze Statusinfos und Meldungen an. Als Administrator können Sie diese Einstellungen in den Gruppenrichtlinien ändern, indem Sie die Richtlinie *Anwendungsbenachrichtigungen auf gesperrtem Bildschirm deaktivieren* aktivieren, die Sie in den administrativen Vorlagen der Computerkonfiguration unter *System\Anmelden* finden.

Wenn Sie den Sperrbildschirm antippen oder anklicken, sehen Sie den Willkommensbildschirm. In einer Domäne wird standardmäßig der Name des letzten Benutzers angezeigt, der sich auf dem Computer angemeldet hat. Sie können sich mit diesem Konto anmelden, indem Sie das erforderliche Kennwort eingeben. Sie können sich auch als ein anderer Benutzer anmelden. Achten Sie auf dem Willkommensbildschirm auf die Schaltfläche links neben dem Benutzerbild. Das ist die Schaltfläche *Benutzer wechseln*. Tippen oder klicken Sie auf *Benutzer wechseln*, wählen Sie eines der angezeigten Konten aus und geben Sie das Kennwort für dieses Konto ein, oder tippen oder klicken Sie auf *Anderer Benutzer*, um einen Benutzernamen und ein Kennwort für das zu benutzende Konto einzugeben.

Auf dem Willkommensbildschirm von Computern, die zu einer Heimnetzgruppe oder Arbeitsgruppe gehören, sehen Sie eine Liste der Konten, die zur Anmeldung auf dem Computer zur Verfügung stehen. Wenn Sie sich mit einem dieser Konten anmelden möchten, tippen oder klicken Sie das gewünschte Konto an und geben das dazugehörige Kennwort ein, sofern erforderlich. Allerdings werden nicht alle

Konten angezeigt, die auf dem Computer vorhanden sind. Manche Konten werden automatisch verborgen, beispielsweise das Konto *Administrator*.

Der Willkommenbildschirm ist sehr bequem, erleichtert aber auch Versuche, sich unberechtigt Zugang zum Computer zu verschaffen. Daher können Sie die Konten in Heimnetzgruppen, Arbeitsgruppen und Domänen verbergen und vom Benutzer verlangen, dass er einen Anmeldenamen eingibt. Das Verbergen des Namens des letzten Benutzers erhöht die Sicherheit, weil Benutzer dann einen gültigen Kontennamen kennen müssen. Den Benutzernamen verbergen Sie durch die Aktivierung der Gruppenrichtlinie *Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen*, die Sie in der Computerkonfiguration unter *Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen* finden.

Standardmäßig können Domänenbenutzer keine PIN-Kennwörter verwenden, sie können jedoch Bildcodes verwenden. Die folgenden Richtlinien aus den administrativen Vorlagen der Computerkonfiguration unter *System\Anmelden* ermöglichen Ihnen die Änderung dieses Verhaltens: *PIN-Anmeldung aktivieren* und *Anmeldung mit Bildcode deaktivieren*.

In einer Domänenumgebung können Sie die gewünschte Sicherheitskonfiguration mit den Active Directory-Gruppenrichtlinien für eine ganze Gruppe von Computern vornehmen. Mit den lokalen Sicherheitsrichtlinien können Sie diese Einstellung auch für einzelne Computer vornehmen. So konfigurieren Sie die lokalen Richtlinien auf einem Heimnetzgruppen- oder Arbeitsgruppencomputer:

1. Öffnen Sie den Editor für lokale Gruppenrichtlinien. Das können Sie zum Beispiel tun, indem Sie die WINDOWS-Taste DRÜCKEN, **Gpedit.msc** eingeben und dann die EINGABETASTE drücken.
2. Erweitern Sie im Editor unter *Computerkonfiguration* die Knoten *Windows-Einstellungen*, *Sicherheits-einstellungen*, *Lokale Richtlinien* und wählen Sie dann *Sicherheitsoptionen* (Abbildung 7.6).

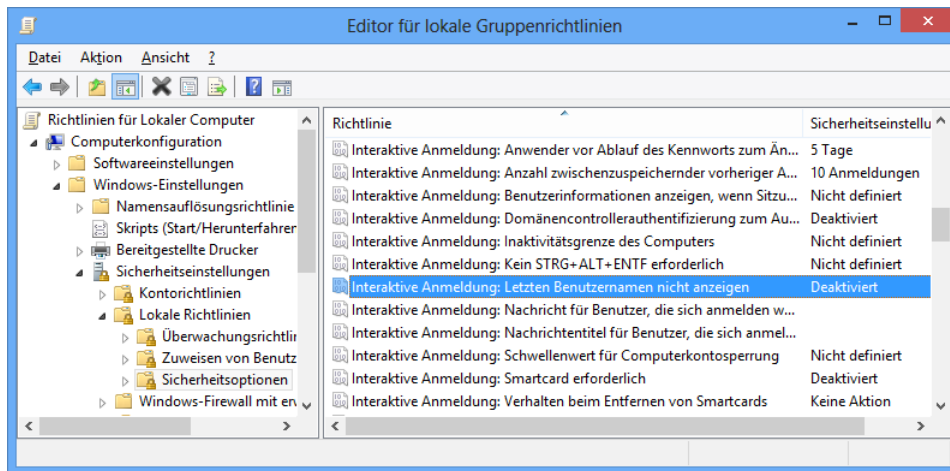


Abbildung 7.6 Deaktivieren Sie die Kontennamenanzeige als Sicherheitsmaßnahme

3. Tippen oder klicken Sie doppelt auf *Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen*.
4. Wählen Sie die Option *Aktiviert* und tippen oder klicken Sie auf *OK*.
5. Erweitern Sie dann *Computerkonfiguration*, *Administrative Vorlagen*, *System*, *Anmelden* und konfigurieren Sie alle weiteren erforderlichen Richtlinien.

Löschen von Konten und Sperren des lokalen Zugriffs auf Arbeitsstationen

Domänenadministratoren erhalten automatisch Zugang zu den lokalen Ressourcen von Arbeitsstationen. Andere Benutzer erhalten nur die Berechtigung für den Zugriff auf Ressourcen, die auf den Computern liegen, an denen sie sich anmelden dürfen. Wenn Arbeitsstationen im Unternehmen weitergegeben werden, ergibt sich vielleicht die Situation, dass die vorherigen Besitzer einer Arbeitsstation immer noch Zugang zu ihren Ressourcen haben oder dass Benutzer, die eigentlich nur für eine gewisse Zeit Zugang zu einer Arbeitsstation erhalten sollten, nie aus der Benutzerliste gestrichen wurden.

In einer Domäne können Sie mit dem Eigenschaftendialogfeld eines Kontos in *Active Directory-Benutzer und -Computer* kontrollieren, an welchen Arbeitsstationen sich der betreffende Benutzer anmelden kann. Tippen oder klicken Sie das Konto doppelt an, um das Dialogfeld *Eigenschaften* zu öffnen. Tippen oder klicken Sie auf der Registerkarte *Konto* auf die Schaltfläche *Anmelden an*.

In einer Heimnetzgruppe oder Arbeitsgruppe können Sie das Konto eines Benutzers mit folgenden Schritten löschen und dem betreffenden Benutzer die Anmeldung verweigern:

1. Melden Sie sich als Benutzer mit lokalen Administratorrechten an. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *Benutzerkonten* auf *Kontotyp ändern*. Dadurch öffnet sich die Seite *Konten verwalten*.
2. Tippen oder klicken Sie auf das Konto, das Sie entfernen möchten.
3. Tippen oder klicken Sie auf *Konto löschen*.
4. Bevor das Konto gelöscht wird, haben Sie die Gelegenheit, den Inhalt des Desktops und des Ordners *Dokumente* des Benutzers in einen Ordner zu kopieren, der auf dem Desktop des aktuellen Benutzers liegt. Um die Dokumente des Benutzers zu speichern, tippen oder klicken Sie auf *Dateien behalten*. Um die Dateien zu löschen, tippen oder klicken Sie auf *Dateien löschen*.
5. Bestätigen Sie die Löschung des Kontos, indem Sie auf *Konto löschen* tippen oder klicken.

Vergessen Sie nicht, dass der Benutzer in einer Domäne immer noch in der Lage sein könnte, mit einem Domänenkonto auf die Arbeitsstation zuzugreifen, wenn nicht weitere Einschränkungen bezüglich der Anmeldung an Arbeitsstationen in Kraft sind.

Verwalten gespeicherter Anmeldeinformationen

In Windows 8 können Sie die Anmeldeinformationsverwaltung benutzen, um Anmeldeinformationen zu speichern, die dann nach Möglichkeit verwendet werden, um die Benutzer automatisch bei Servern, Websites und Programmen anzumelden. Anmeldeinformationen werden im Profil des Benutzers gespeichert. Wenn Sie feststellen, dass ein Benutzer häufig Probleme mit der Anmeldung bei kennwortgeschützten Ressourcen hat, beispielsweise im firmeneigenen Intranet oder auf einer externen Internet-Site, können Sie für diesen Benutzer gespeicherte Anmeldeinformationen für alle benötigten Ressourcen erstellen.

Die Anmeldeinformationsverwaltung unterstützt vier Arten gespeicherter Anmeldeinformationen:

- **Webanmeldeinformationen** Anmeldeinformationen für eine Website. Sie enthalten den Speicherort der Ressource sowie Namen und Kennwort des Anmeldekontos.
- **Windows-Anmeldeinformationen** Anmeldeinformationen für Windows-Standardauthentifizierung (NTLM oder Kerberos). Sie enthalten den Speicherort der Ressource sowie Namen und Kennwort des Anmeldekontos.

- **Zertifikatbasierte Anmeldeinformationen** Diese Anmeldeinformationen umfassen einen Ressourcenspeicherort und verwenden für die Authentifizierung ein Zertifikat, das im Speicher für eigene Zertifikate in der Zertifikatverwaltung abgelegt ist.
- **Generische Anmeldeinformationen** Anmeldeinformationen, die einfache oder benutzerdefinierte Authentifizierungstechniken nutzen. Sie umfassen einen Ressourcenspeicherort sowie Namen und Kennwort des Anmeldekontos.

Die folgenden Abschnitte stellen die Techniken für die Arbeit mit gespeicherten Anmeldeinformationen vor.

PRAXISTIPP Wenn Sie ein Microsoft-Konto erstellen, werden generische Anmeldeinformationen für Windows Live erstellt und gespeichert. Diese Windows Live-Anmeldeinformationen werden für den Zugriff auf den Microsoft Store, SkyDrive und andere Microsoft-Dienste verwendet. Normalerweise sollten Sie diese Anmeldeinformationen nicht bearbeiten oder löschen. Wenn die Live-Anmeldeinformationen und die gespeicherten Anmeldeinformationen aber aus irgendeinem Grund voneinander abweichen, müssen Sie hier die E-Mail-Adresse und das Kennwort bearbeiten, das vom Benutzer für den Zugriff auf Microsoft-Dienste verwendet wird.

Hinzufügen von Windows- oder generischen Anmeldeinformationen

Jedes Benutzerkonto verfügt über eigene Anmeldeinformationen. Die Anmeldeinformationen werden in den Profildaten des Benutzers gespeichert und enthalten Angaben, die für die Anmeldung bei kennwortgeschützten Ressourcen erforderlich sind. Wenn Sie bei der Erstellung der Anmeldeinformationen mit einem Domänenkonto angemeldet sind und das Konto über ein servergespeichertes Profil verfügt (ein »Roamingprofil«, also kein lokales oder verbindliches Profil), sind die Anmeldeinformationen überall verfügbar, unabhängig davon, auf welchem Computer der Domäne Sie sich anmelden. Andernfalls sind die Anmeldeinformationen nur auf dem speziellen Computer verfügbar, auf dem Sie die Einträge vorgenommen haben.

PRAXISTIPP Wenn Ihre Organisation Computer hat, die keine Domänenmitglieder sind, sondern in Arbeitsgruppen oder Heimnetzgruppen organisiert sind, werden Sie feststellen, dass alle Benutzer durch die gespeicherten Anmeldeinformationen eine Menge Zeit sparen. Nehmen wir an, Ted benutzt für seine tägliche Arbeit einen Computer, der Mitglied einer Arbeitsgruppe ist, braucht aber Zugriff auf mehrere unterschiedliche Server an unterschiedlichen Standorten oder in unterschiedlichen Domänen. Das können Sie für Ted wesentlich einfacher machen, indem Sie für jede Ressource Windows-Anmeldeinformationen erstellen. Unabhängig davon, wie Ted auf die Server zugreift, wird er nun automatisch authentifiziert, ohne dass er alternative Anmeldeinformationen eingeben muss. Wenn Ted beispielsweise ein Netzlaufwerk für *FileServer84* einrichtet und Sie Anmeldeinformationen für diesen Server eingetragen haben, braucht Ted nicht die Option *Verbindung mit anderen Anmeldeinformationen herstellen* zu verwenden und dann alternative Anmeldeinformationen einzugeben.

So fügen Sie einen Eintrag zu den Anmeldeinformationen des angemeldeten Benutzers hinzu:

1. Melden Sie sich als der Benutzer an, dessen Anmeldeinformationen Sie verwalten wollen. Tippen oder klicken Sie in der Systemsteuerung auf *Benutzerkonten* und dann unter *Anmeldeinformationsverwaltung* auf *Windows-Anmeldeinformationen verwalten*.

Auf der Seite *Anmeldeinformationsverwaltung* (Abbildung 7.7) sehen Sie eine Liste der aktuellen Einträge, die nach dem Anmeldeinformationstyp sortiert sind (sofern bereits Anmeldeinformationen vorhanden sind).

HINWEIS Der Einfachheit halber nenne ich häufig nur die kurze Überschrift *Benutzerkonten* aus der Systemsteuerung. Beachten Sie, dass diese kurze Überschrift nur auf Domänencomputern in der Systemsteuerung angezeigt wird, während sie auf Computern aus Arbeitsgruppen und Heimnetzwerken *Benutzerkonten* und *Family Safety* lautet.

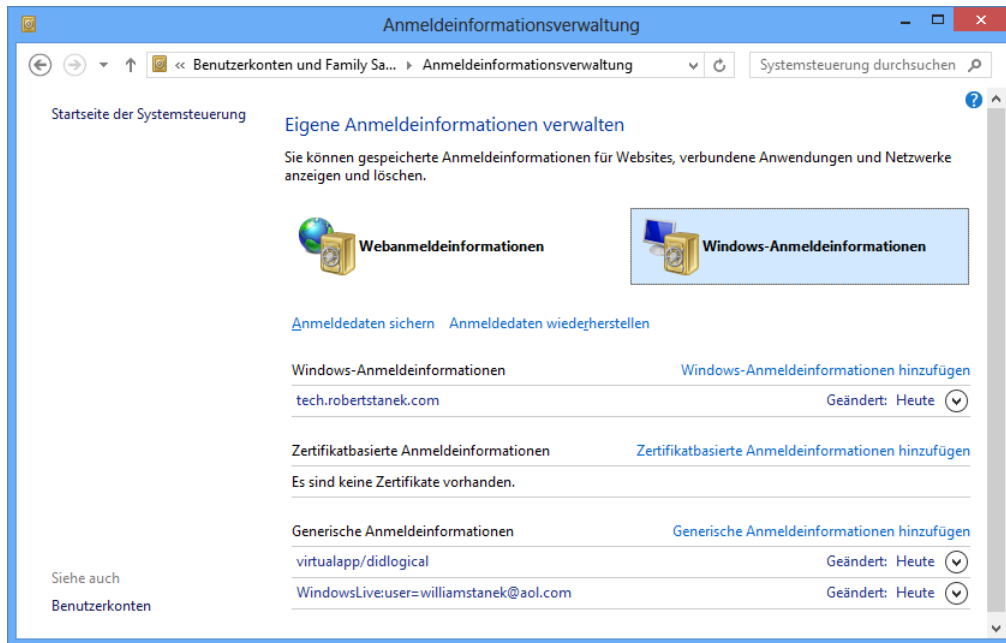


Abbildung 7.7 Anzeigen der momentan verfügbaren Anmeldeinformationen und -optionen

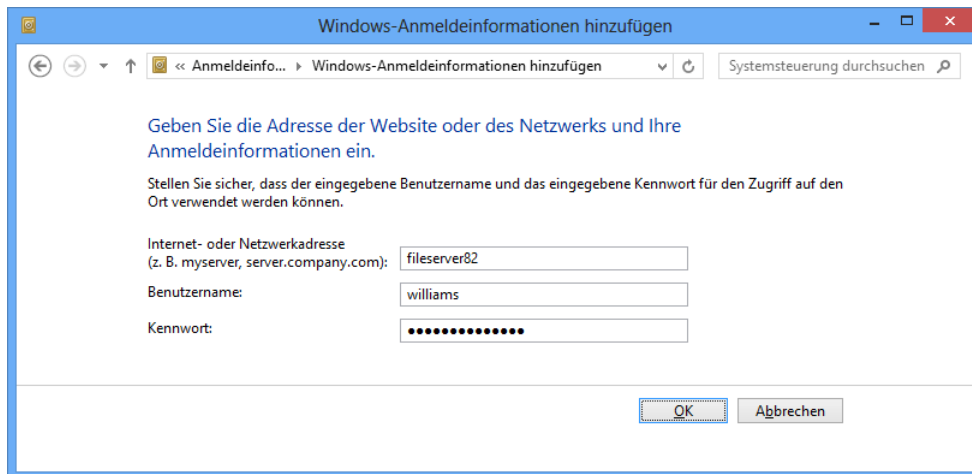


Abbildung 7.8 Erstellen von gespeicherten Anmeldeinformationen

2. Tippen oder klicken Sie auf *Windows-Anmeldeinformationen hinzufügen* oder *Generische Anmeldeinformationen hinzufügen*, je nachdem, welchen Typ Anmeldeinformationen Sie erstellen wollen. Geben Sie dann die Daten ein, die Sie brauchen, um die Anmeldeinformationen zu konfigurieren (Abbildung 7.8).

Es stehen folgende Optionen zur Verfügung:

- **Internet- oder Netzwerkadresse** Die Netzwerk- oder Internetressource, für die Sie den Eintrag vornehmen. Dabei kann es sich um den Namen eines Servers handeln, beispielsweise *Fileserver86*, den vollqualifizierten Domänennamen einer Internetressource, etwa *www.microsoft.com*, oder um eine Adresse mit einem Platzhalter, wie zum Beispiel **.microsoft.com*. Wenn Sie einen Servernamen oder vollqualifizierten Domänennamen angeben, wird dieser Eintrag für den Zugriff auf einen bestimmten Server oder Dienst verwendet. Wenn Sie einen Platzhalter verwenden, wird der Eintrag für jeden Server aus der angegebenen Domäne verwendet. So könnte zum Beispiel der Eintrag **.microsoft.com* für den Zugriff auf *www.microsoft.com*, *ftp.microsoft.com*, *smtp.microsoft.com* und *extranet.microsoft.com* verwendet werden.
- **Benutzername** Der Benutzername, der für den Server benötigt wird. Der Name muss auch alle erforderlichen Domänenangaben umfassen. Wenn Sie für eine Ressource die Standarddomäne verwenden, brauchen Sie nur den Benutzernamen einzugeben, zum Beispiel *Williams*. Bei einer anderen Domäne geben Sie den vollständigen Domänenkontennamen ein, wie zum Beispiel *technology\Williams*. Für einen Internetdienst geben Sie den vollständigen Dienstkontennamen an, wie zum Beispiel *Williams@msn.com*.
- **Kennwort** Das Kennwort, das der Server verlangt. Die meisten Benutzer vergessen, dass sie auch das Kennwort in ihren Anmeldeinformationen ändern müssen, wenn sie ihr Kennwort auf dem Server oder Dienst ändern. Und wenn ein Benutzer vergisst, das Kennwort in den Anmeldeinformationen zu ändern, können die wiederholten erfolglosen Anmelde- oder Verbindungsversuche mit dem Server oder Dienst dazu führen, dass das betreffende Konto gesperrt wird.

3. Tippen oder klicken Sie auf *OK*, um die Anmeldeinformationen zu speichern.

Hinzufügen von zertifikatbasierten Anmeldeinformationen

Der Zertifikatspeicher *Eigene Zertifikate* im Profil eines Benutzers enthält Zertifikate, die ausgestellt wurden, um diesen Benutzer zu authentifizieren. Sobald Sie ein Zertifikat für den Benutzer hinzugefügt haben, können Sie Anmeldeinformationen erstellen, die mit einem Zertifikat auf eine Ressource zugreifen.

Gehen Sie folgendermaßen vor, um einen Eintrag für zertifikatbasierte Anmeldeinformationen zu den gespeicherten Anmeldeinformationen des momentan angemeldeten Benutzers hinzuzufügen:

1. Melden Sie sich als der Benutzer an, dessen Anmeldeinformationen Sie verwalten wollen. Tippen oder klicken Sie in der Systemsteuerung auf *Benutzerkonten* und dann unter *Anmeldeinformationsverwaltung* auf *Windows-Anmeldeinformationen verwalten*.
2. Auf der Seite *Anmeldeinformationsverwaltung* sehen Sie eine Liste der aktuellen Einträge, die nach dem Anmeldeinformationstyp sortiert sind (sofern bereits Anmeldeinformationen vorhanden sind).
3. Tippen oder klicken Sie auf *Zertifikatbasierte Anmeldeinformationen hinzufügen*. Geben Sie im Feld *Internet- oder Netzwerkadresse* den Namen des Netzwerks oder der Internetressource ein, für die Sie die Anmeldeinformationen einrichten. Das kann ein Servername, ein vollqualifizierter Domänenname für eine Internetressource oder eine Adresse mit einem Platzhalter sein.
4. Tippen oder klicken Sie auf *Zertifikat auswählen*. Tippen oder klicken Sie im Dialogfeld *Zertifikat auswählen* auf das Zertifikat, das Sie für die Ressource verwenden wollen, und tippen oder klicken Sie dann auf *OK*.
5. Tippen oder klicken Sie erneut auf *OK*, um die Anmeldeinformationen zu speichern.

Bearbeiten von Anmeldeinformationen

Sie können Anmeldeinformationen jederzeit bearbeiten. Vergessen Sie aber nicht, dass lokale Anmeldeinformationseinträge nur auf dem Computer sichtbar sind, auf dem sie erstellt werden. Wenn Sie einen Eintrag ändern möchten, müssen Sie sich also auf der lokalen Arbeitsstation anmelden, auf der der Eintrag erstellt wurde. Eine Ausnahme sind Benutzer mit servergespeicherten Profilen. Verwendet ein Benutzer ein servergespeichertes Profil, lassen sich Anmeldeinformationseinträge auf jedem Computer ändern, auf dem sich der Benutzer bei der Domäne anmeldet.

Gehen Sie folgendermaßen vor, um die Anmeldeinformationseinträge eines Benutzers zu bearbeiten:

1. Melden Sie sich als der Benutzer an, dessen Anmeldeinformationseinträge Sie verwalten wollen. Tippen oder klicken Sie in der Systemsteuerung auf *Benutzerkonten* und dann unter *Anmeldeinformationsverwaltung* auf *Windows-Anmeldeinformationen verwalten*.
Auf der Seite *Anmeldeinformationsverwaltung* sehen Sie eine Liste der aktuellen Einträge, die nach dem Anmeldeinformationstyp sortiert sind.
2. Tippen oder klicken Sie auf die Anmeldeinformationen, die Sie bearbeiten wollen.
3. Tippen oder klicken Sie auf *Bearbeiten*.
4. Geben Sie die gewünschten neuen Werte für Benutzername und Kennwort ein oder wählen Sie das Zertifikat aus, das mit den Anmeldeinformationen verknüpft sein soll. Tippen oder klicken Sie auf *Speichern*.

Sichern und Wiederherstellen von Anmeldeinformationen

Sie können die gespeicherten Anmeldeinformationen eines Benutzers getrennt von seinen anderen Computerdaten sichern. Verfügen Sie über eine Datensicherung der Anmeldeinformationen, können Sie die Anmeldeinformationen später wiederherstellen oder auf einen neuen Computer übertragen, indem Sie die Informationen wiederherstellen. Normalerweise sollten Sie die Anmeldeinformationen auf einen Wechseldatenträger sichern.

Gehen Sie folgendermaßen vor, um die Anmeldeinformationen eines Benutzers zu sichern:

1. Melden Sie sich als der Benutzer an, dessen Anmeldeinformationseinträge Sie verwalten wollen. Tippen oder klicken Sie in der Systemsteuerung auf *Benutzerkonten* und dann unter *Anmeldeinformationsverwaltung* auf *Windows-Anmeldeinformationen verwalten*.
Auf der Seite *Anmeldeinformationsverwaltung* sehen Sie eine Liste der aktuellen Einträge, die nach dem Anmeldeinformationstyp sortiert sind.
2. Tippen oder klicken Sie auf *Anmeldedaten sichern*.
3. Tippen oder klicken Sie im Dialogfeld *Gespeicherte Benutzernamen und Kennwörter* auf *Durchsuchen*. Wählen Sie im Dialogfeld *Sicherungsdatei speichern* unter einen Speicherort aus und geben Sie einen Namen für die Datensicherungsdatei der Anmeldeinformationen ein. Sicherungsdateien für Anmeldeinformationen werden mit der Dateinamenserweiterung *.crd* gespeichert. Tippen oder klicken Sie auf *Speichern*.
4. Tippen oder klicken Sie auf *Weiter*. Drücken Sie die Tastenkombination STRG+ALT+ENTF, um auf den sicheren Desktop umzuschalten. Geben Sie ein Kennwort für die Sicherungsdatei der Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden.
5. Tippen oder klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

Gehen Sie folgendermaßen vor, um die Anmeldeinformationen eines Benutzers auf demselben oder einem anderen Computer wiederherzustellen:

1. Melden Sie sich als der Benutzer an, dessen Anmeldeinformationseinträge Sie verwalten wollen. Tippen oder klicken Sie in der Systemsteuerung auf *Benutzerkonten* und dann unter *Anmeldeinformationsverwaltung* auf *Windows-Anmeldeinformationen verwalten*.
2. Tippen oder klicken Sie auf der Seite *Anmeldeinformationsverwaltung* auf *Anmeldedaten wiederherstellen*.
3. Tippen oder klicken Sie im Dialogfeld *Gespeicherte Benutzernamen und Kennwörter* auf *Durchsuchen*. Wählen Sie im Dialogfeld *Sicherungsdatei öffnen* die Sicherungsdatei für die Anmeldeinformationen aus und tippen oder klicken Sie auf *Öffnen*.
4. Tippen oder klicken Sie auf *Weiter*. Drücken Sie die Tastenkombination STRG+ALT+ENTF, um auf den sicheren Desktop umzuschalten, und geben Sie das Kennwort für die Sicherungsdatei der Anmeldeinformationen ein.
5. Tippen oder klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

Löschen von Anmeldeinformationen

Braucht ein Benutzer einen Anmeldeinformationseintrag nicht mehr, sollten Sie diesen Eintrag löschen. Gehen Sie folgendermaßen vor, um einen Anmeldeinformationseintrag eines Benutzers zu löschen:

1. Melden Sie sich als der Benutzer an, dessen Anmeldeinformationseinträge Sie verwalten wollen. Tippen oder klicken Sie in der Systemsteuerung auf *Benutzerkonten* und dann unter *Anmeldeinformationsverwaltung* auf *Windows-Anmeldeinformationen verwalten*.
Auf der Seite *Anmeldeinformationsverwaltung* sehen Sie eine Liste der aktuellen Einträge, die nach dem Anmeldeinformationstyp sortiert sind.
2. Tippen oder klicken Sie auf die Anmeldeinformationen, die Sie löschen wollen.
3. Tippen oder klicken Sie auf *Entfernen*. Bestätigen Sie die Nachfrage, ob der Eintrag tatsächlich gelöscht werden soll, indem Sie auf *Ja* tippen oder klicken.

Wie bereits erwähnt, können lokale Anmeldeinformationseinträge nur auf dem Computer gelöscht werden, auf dem sie erstellt wurden. Verwendet ein Benutzer allerdings ein servergespeichertes Profil, können Anmeldeinformationseinträge auf jedem Computer gelöscht werden, an dem der Benutzer angemeldet ist.

Verwalten lokaler Benutzerkonten und Gruppen

Lokale Benutzerkonten und Gruppenkonten werden ähnlich verwaltet wie Domänenkonten. Sie können Konten erstellen, ihre Eigenschaften verwalten, gesperrte oder deaktivierte Konten zurücksetzen und so weiter. Sie können lokale Benutzerkonten nicht nur mit der Systemsteuerung erstellen, sondern auch in der Konsole *Lokale Benutzer und Gruppen* oder durch unverwaltete Richtlinieneinstellungen. Sie sollten diese Möglichkeiten folgendermaßen nutzen:

- Verwenden Sie *Lokale Benutzer und Gruppen*, um lokale Benutzerkonten auf einem Computer zu verwalten.
- Verwenden Sie unverwaltete Richtlinieneinstellungen, um lokale Benutzerkonten auf mehreren Computern in einer Domäne zu verwalten.

Wenn Sie mit unverwalteten Richtlinieneinstellungen arbeiten, können Sie Benutzer und Gruppen über Einträge in den Zweigen *Computerkonfiguration* oder *Benutzerkonfiguration* verwalten. Nehmen Sie *Computerkonfiguration*, wenn Sie Einstellungen konfigurieren wollen, die auf Computer unabhängig davon angewendet werden sollen, wer sich daran anmeldet. Verwenden Sie dagegen *Benutzerkonfiguration*, wenn Sie Einstellungen konfigurieren, die auf bestimmte Benutzer angewendet werden sollen, und zwar unabhängig davon, an welchen Computern sie sich anmelden.

Erstellen von lokalen Benutzerkonten

Gehen Sie folgendermaßen vor, um die Konsole *Lokale Benutzer und Gruppen* zu öffnen und ein Benutzerkonto anzulegen:

1. Öffnen Sie die Computerverwaltung. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen Sie im Kontextmenü *Verbindung mit anderem Computer herstellen*. Nun können Sie die Windows 8-Arbeitsstation angeben, deren lokale Konten Sie verwalten möchten. (Domänencontroller haben keine lokalen Benutzer und Gruppen.)
2. Tippen oder klicken Sie im Knoten *System* doppelt auf *Lokale Benutzer und Gruppen*, um den Knoten aufzuklappen, und wählen Sie dann *Benutzer* aus. In der Detailansicht müsste jetzt eine Liste der momentan definierten Benutzerkonten angezeigt werden.
3. Klicken Sie mit der rechten Maustaste auf den Knoten *Benutzer* oder halten Sie ihn gedrückt, und wählen Sie dann *Neuer Benutzer*. Dadurch öffnet sich das Dialogfeld *Neuer Benutzer* (Abbildung 7.9).

Abbildung 7.9 Mit dem Dialogfeld *Neuer Benutzer* können Sie in *Lokale Benutzer und Gruppen* neue Benutzerkonten anlegen

Die Felder dieses Dialogfelds haben folgende Bedeutungen:

- **Benutzername** Der Anmeldename für das Benutzerkonto. Der Name sollte den Richtlinien für lokale Benutzernamen entsprechen.
- **Vollständiger Name** Der vollständige Name des Benutzers, beispielsweise William R. Stanek.

- **Beschreibung** Eine Beschreibung des Benutzers. Im Normalfall gibt man die Berufsbezeichnung des Benutzers an, zum Beispiel Webmaster. Sie können auch die Berufsbezeichnung und die Abteilung des Benutzers angeben.
 - **Kennwort** Das Kennwort für das Konto. Dieses Kennwort sollte Ihre Kennwortrichtlinien einhalten.
 - **Kennwort bestätigen** Das Kennwort für das Konto. Dieses Textfeld soll sicherstellen, dass das Kennwort korrekt zugewiesen wird. Geben Sie das Kennwort einfach noch einmal ein, um es zu bestätigen.
 - **Benutzer muss Kennwort bei der nächsten Anmeldung ändern** Wenn dieses Kontrollkästchen gewählt ist, muss der Benutzer bei der nächsten Anmeldung sein Kennwort ändern.
 - **Benutzer kann Kennwort nicht ändern** Wenn dieses Kontrollkästchen gewählt ist, kann der Benutzer sein Kennwort nicht ändern.
 - **Kennwort läuft nie ab** Wenn dieses Kontrollkästchen gewählt ist, läuft das Kennwort des Kontos nie ab. Diese Einstellung hat Vorrang vor der lokalen Kontorichtlinie.
 - **Konto ist deaktiviert** Wenn dieses Kontrollkästchen gewählt ist, ist das Konto deaktiviert und kann nicht verwendet werden. Benutzen Sie diese Option, wenn die Verwendung eines Kontos für eine bestimmte Zeit verhindert werden soll.
4. Tippen oder klicken Sie auf *Erstellen*, wenn Sie alle Eingaben und Einstellungen für das neue Konto vorgenommen haben.

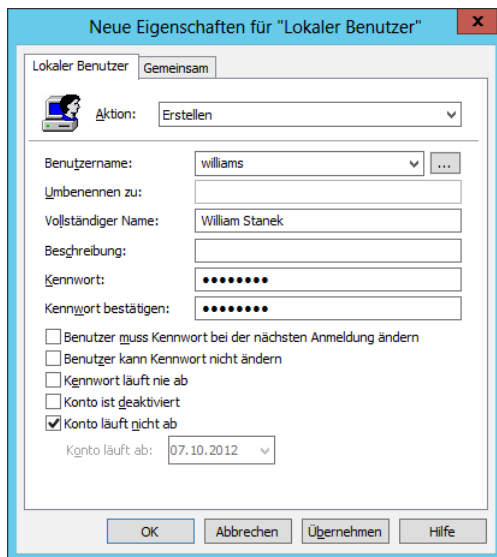


Abbildung 7.10 Konfigurieren von neuen lokalen Benutzerkonten in den Gruppenrichtlinien

Gehen Sie folgendermaßen vor, um die Gruppenrichtlinien zu bearbeiten und mit einem Einstellungselement ein Benutzerkonto anzulegen:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Wenn Sie die Einstellungen für Computer konfigurieren wollen, müssen Sie *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann

Lokale Benutzer und Gruppen auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Lokale Benutzer und Gruppen* auswählen.

2. Klicken Sie mit der rechten Maustaste auf den Knoten *Lokale Benutzer und Gruppen* oder halten Sie ihn gedrückt, und wählen Sie im Kontextmenü den Befehl *Neu/Lokaler Benutzer*. Daraufhin öffnet sich das Dialogfeld *Neue Eigenschaften für "Lokaler Benutzer"* (Abbildung 7.10).
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Erstellen* aus. Die übrigen Felder im Dialogfeld sind dieselben wie in der letzten Anleitung.
4. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. In den meisten Fällen legen Sie das neue Konto nur einmal an. Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmal anwenden*.
5. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es in dem Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Erstellen lokaler Gruppen für Arbeitsstationen

Lokale Gruppen erstellen Sie mit der Konsole *Lokale Benutzer und Gruppen* oder mit Gruppenrichtlinien. Sie können die Konsole *Lokale Benutzer und Gruppen* mit folgenden Schritten öffnen und eine Gruppe erstellen:

1. Öffnen Sie die Computerverwaltung. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen Sie *Verbindung mit anderem Computer herstellen*. Nun können Sie die Windows 8-Arbeitsstation angeben, deren lokale Konten Sie verwalten möchten. (Domänencontroller haben keine lokalen Benutzer und Gruppen.)
2. Tippen oder klicken Sie unter dem Knoten *System* doppelt auf *Lokale Benutzer und Gruppen*, um den Knoten aufzuklappen, und wählen Sie dann *Gruppen* aus. In der Detailansicht müsste nun eine Liste der momentan definierten Gruppenkonten angezeigt werden.

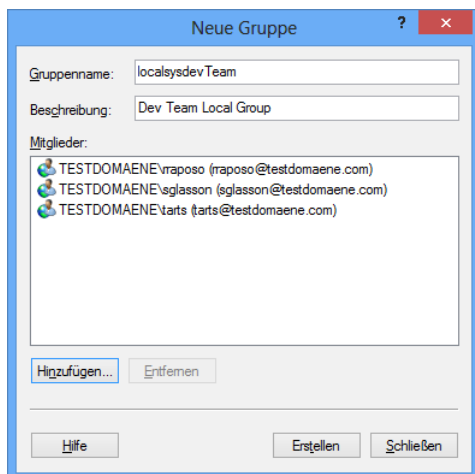


Abbildung 7.11 Das Dialogfeld *Neue Gruppe* ermöglicht Ihnen auf einer Windows 8-Arbeitsstation die Definition neuer lokaler Gruppen

3. Klicken Sie mit der rechten Maustaste auf den Knoten *Gruppen* oder halten Sie ihn gedrückt, und wählen Sie im Kontextmenü den Befehl *Neue Gruppe*. Daraufhin öffnet sich das Dialogfeld *Neue Gruppe* (Abbildung 7.11).
4. Nachdem Sie einen Namen und eine Beschreibung der Gruppe eingegeben haben, tippen oder klicken Sie auf die Schaltfläche *Hinzufügen*, um Mitglieder zur Gruppe hinzuzufügen. Dadurch öffnet sich das Dialogfeld *Benutzer auswählen*.
5. Im Dialogfeld *Benutzer auswählen* tippen oder klicken Sie auf *Pfade*, um den Computer oder die Domäne auszuwählen, in der die gewünschten Benutzerkonten liegen.
6. Geben Sie im Textfeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen eines Benutzers ein und klicken Sie dann auf *Namen überprüfen*. Werden Übereinstimmungen gefunden, wählen Sie das gewünschte Konto aus und tippen oder klicken auf *OK*. Werden keine passenden Konten gefunden, korrigieren Sie den Namen, den Sie eingegeben haben, und wiederholen die Suche. Wiederholen Sie diesen Vorgang so oft wie nötig und tippen oder klicken Sie auf *OK*, wenn Sie fertig sind.
7. Das Dialogfeld *Neue Gruppe* wurde aktualisiert und zeigt Ihre Auswahl an. Falls Sie einen Fehler gemacht haben, wählen Sie den betreffenden Namen aus und entfernen ihn durch antippen oder anklicken von *Entfernen*.
8. Tippen oder klicken Sie auf *Erstellen*, wenn Sie die Auswahl der Gruppenmitglieder beendet haben.

Gehen Sie folgendermaßen vor, um Gruppenrichtlinien zum Bearbeiten zu öffnen und mit einem Einstellungselement eine lokale Gruppe anzulegen:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Wenn Sie die Einstellungen für Computer konfigurieren wollen, müssen Sie *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Lokale Benutzer und Gruppen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Lokale Benutzer und Gruppen* auswählen.

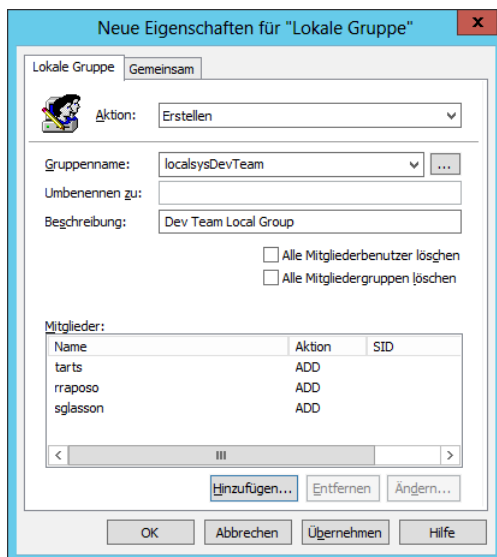


Abbildung 7.12 Konfigurieren neuer lokaler Gruppenkonten in Gruppenrichtlinien

2. Klicken Sie mit der rechten Maustaste auf den Knoten *Lokale Benutzer und Gruppen* oder halten Sie ihn gedrückt, und wählen Sie im Kontextmenü den Befehl *Neu/Lokale Gruppe*. Daraufhin öffnet sich das Dialogfeld *Neue Eigenschaften für "Lokale Gruppe"* (Abbildung 7.12).
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Erstellen* aus. Geben Sie einen Namen und eine Beschreibung für die Gruppe ein.
4. Tippen oder klicken Sie auf *Hinzufügen*, um Mitglieder zur Gruppe hinzuzufügen. Tippen oder klicken Sie im Dialogfeld *Lokales Gruppenmitglied* auf die *Durchsuchen*-Schaltfläche (die Schaltfläche mit den drei Punkten). Wählen Sie im Dialogfeld *Benutzer, Computer oder Gruppe auswählen* einen Benutzer oder eine Gruppe aus, der/die zur lokalen Gruppe hinzugefügt werden soll, und tippen oder klicken Sie zweimal auf *OK*. Wiederholen Sie diesen Schritt so oft wie nötig.
5. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. In den meisten Fällen legen Sie das neue Konto nur einmal an. Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmal anwenden*.
6. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Element angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Element definiert haben.

Verwalten der Mitglieder lokaler Gruppen

Mit der Konsole *Lokale Benutzer und Gruppen* können Sie Mitglieder zu lokalen Gruppen hinzufügen oder löschen. Gehen Sie folgendermaßen vor:

1. Öffnen Sie den Knoten *Lokale Benutzer und Gruppen* in der Computerverwaltung und wählen Sie dann den Ordner *Gruppen*. Tippen oder klicken Sie die Gruppe, die Sie bearbeiten möchten, doppelt an.
2. Wenn Sie Benutzerkonten zur Gruppe hinzufügen möchten, tippen oder klicken Sie auf die Schaltfläche *Hinzufügen*. Es öffnet sich das Dialogfeld *Benutzer auswählen*. Im Textfeld *Geben Sie die zu verwendenden Objektnamen ein* des Dialogfelds *Benutzer auswählen* geben Sie den Namen des gewünschten Benutzers ein und tippen oder klicken auf *Namen überprüfen*. Werden Übereinstimmungen gefunden, wählen Sie das gewünschte Konto aus und tippen oder klicken auf *OK*. Werden keine passenden Konten gefunden, korrigieren Sie den Namen, den Sie eingegeben haben, und wiederholen die Suche. Wiederholen Sie diesen Vorgang so oft wie nötig und tippen oder klicken Sie auf *OK*, wenn Sie fertig sind.
3. Um Benutzerkonten aus der Gruppe zu entfernen, verwenden Sie die Schaltfläche *Entfernen*. Wählen Sie einfach das Konto aus, das aus der Gruppe entfernt werden soll, und tippen oder klicken Sie dann auf *Entfernen*.
4. Tippen oder klicken Sie auf *OK*, wenn Sie fertig sind.

Gehen Sie folgendermaßen vor, um die Gruppenrichtlinien zu bearbeiten und mit einem Element Mitglieder in einer lokalen Gruppe hinzuzufügen oder zu entfernen:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Wenn Sie die Einstellungen für Computer konfigurieren wollen, müssen Sie *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Lokale Benutzer und Gruppen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Lokale Benutzer und Gruppen* auswählen.

2. Klicken Sie mit der rechten Maustaste auf den Knoten *Lokale Benutzer und Gruppen* oder halten Sie ihn gedrückt, und wählen Sie im Kontextmenü den Befehl *Neu/Lokale Gruppe*. Daraufhin öffnet sich das Dialogfeld *Neue Eigenschaften für "Lokale Gruppe"*.
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Aktualisieren* aus, um die Einstellungen der Gruppe zu verändern, oder *Ersetzen*, um die Gruppe zu löschen und dann genau so neu zu erstellen, wie Sie sie definieren. Wenn Sie eine Gruppe aktualisieren, können Sie einen neuen Namen im Feld *Umbenennen zu* eingeben.
4. Legen Sie fest, ob der aktuelle Benutzer als Mitglied zur Gruppe hinzugefügt oder daraus entfernt werden soll. Stattdessen können Sie auch *Aktuellen Benutzer nicht konfigurieren* wählen.
5. Wählen Sie aus, ob alle vorhandenen Mitgliederbenutzer, alle vorhandenen Mitgliedergruppen oder beide gelöscht werden sollen.
6. Tippen oder klicken Sie auf *Hinzufügen*, um Mitglieder zur Gruppe hinzuzufügen. Wählen Sie im Dialogfeld *Lokales Gruppenmitglied* in der Dropdownliste *Aktion* den Eintrag *Dieser Gruppe hinzufügen* aus, wenn Sie ein Mitglied hinzufügen wollen, oder den Eintrag *Aus dieser Gruppe entfernen*, wenn Sie ein Mitglied löschen. Tippen oder klicken Sie auf die *Durchsuchen*-Schaltfläche (die Schaltfläche mit den drei Punkten). Wählen Sie im Dialogfeld *Benutzer, Computer oder Gruppe auswählen* einen Benutzer oder eine Gruppe aus, der/die in der lokalen Gruppe hinzugefügt beziehungsweise gelöscht werden soll, und tippen oder klicken Sie zweimal auf *OK*. Wiederholen Sie diesen Schritt so oft wie nötig.
7. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden, und tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Aktivieren und Deaktivieren lokaler Benutzerkonten

Lokale Benutzerkonten können aus verschiedenen Gründen deaktiviert worden sein. Vergisst ein Benutzer sein Kennwort und versucht, es zu erraten, überschreitet er vielleicht die Kontenrichtlinie für fehlgeschlagene Anmeldeversuche. Vielleicht hat ein anderer Administrator das Konto des Benutzers deaktiviert, weil der Benutzer im Urlaub war. Wurde ein Konto deaktiviert oder gesperrt, können Sie es mit den folgenden Methoden wieder aktivieren.

Wenn das Konto deaktiviert ist, gehen Sie folgendermaßen vor, um es auf einem lokalen Computer wieder zu aktivieren:

1. Erweitern Sie in der Konsole *Computerverwaltung* den Knoten *Lokale Benutzer und Gruppen* und wählen Sie im linken Fensterabschnitt den Ordner *Benutzer* aus.
2. Tippen oder klicken Sie im rechten Fensterabschnitt doppelt auf den Kontonamen des Benutzers und deaktivieren Sie das Kontrollkästchen *Konto ist deaktiviert*.
3. Tippen oder klicken Sie auf *OK*.

Ist ein Konto gesperrt, können Sie es folgendermaßen auf einem lokalen Computer wieder aktivieren:

1. Wählen Sie im Knoten *Lokale Benutzer und Gruppen* im linken Fensterabschnitt den Ordner *Benutzer* aus.
2. Tippen oder klicken Sie im rechten Fensterabschnitt doppelt auf den Kontonamen des Benutzers und deaktivieren Sie das Kontrollkästchen *Konto ist gesperrt*.
3. Tippen oder klicken Sie auf *OK*.

Gehen Sie folgendermaßen vor, um mit unverwalteten Richtlinieneinstellungen Konten zu aktivieren oder zu deaktivieren und andere Kontooptionen zu konfigurieren:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Wenn Sie die Einstellungen für Computer konfigurieren wollen, müssen Sie *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Lokale Benutzer und Gruppen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Lokale Benutzer und Gruppen* auswählen.
2. Tippen oder klicken Sie im rechten Fensterabschnitt doppelt auf den Kontonamen eines Benutzers, um das zugehörige Eigenschaftendialogfeld zu öffnen.
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Aktualisieren* aus. Nehmen Sie die erforderlichen Änderungen vor und tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Erstellen eines sicheren Gastkontos

In manchen Umgebungen müssen Sie vielleicht ein Gastkonto für Besucher einrichten. Dann empfiehlt es sich, das Gastkonto für die Verwendung auf einem bestimmten Computer oder einer bestimmten Computergruppe zu konfigurieren und sorgfältig zu kontrollieren, wofür das Konto benutzt werden kann. Zur Einrichtung eines sicheren Gastkontos empfehle ich, folgende Arbeiten durchzuführen:

- **Aktivieren des Gastkontos** Standardmäßig ist das Gastkonto deaktiviert. Daher müssen Sie es zuerst aktivieren, damit es verwendet werden kann. Dazu öffnen Sie den Knoten *Lokale Benutzer und Gruppen* in der Computerverwaltung und wählen dann den Ordner *Benutzer*. Tippen oder klicken Sie *Gast* doppelt an und löschen Sie das Kontrollkästchen *Konto ist deaktiviert*. Tippen oder klicken Sie auf *OK*.
- **Festlegen eines sicheren Kennworts für das Gastkonto** Standardmäßig wird dem Gastkonto kein Kennwort zugewiesen. Um die Sicherheit des Computers zu verbessern, sollten Sie ein Kennwort festlegen. Tippen oder klicken Sie *Gast* in *Lokale Benutzer und Gruppen* mit der rechten Maustaste an oder halten Sie das Konto gedrückt, und wählen Sie dann *Kennwort festlegen*. In der Warnmeldung tippen oder klicken Sie auf *Fortsetzen*. Geben Sie das neue Kennwort ein und bestätigen Sie es. Tippen oder klicken Sie auf *OK*.
- **Sicherstellen, dass das Gastkonto nicht über das Netzwerk verwendet werden kann** Das Gastkonto sollte von anderen Computern aus nicht zugänglich sein. Wäre es verwendbar, könnten sich Benutzer von anderen Computern über das Netzwerk als Gäste anmelden. Um das zu verhindern, starten Sie die Konsole *Lokale Sicherheitsrichtlinie* aus dem Menü *Tools* des Server-Managers oder geben in einer Befehlszeile *secpol.msc* ein. Erweitern Sie *Lokale Richtlinien*, *Zuweisen von Benutzerrechten* und sorgen Sie dafür, dass *Gast* in der Richtlinie *Zugriff vom Netzwerk auf diesen Computer verweigern* als beschränktes Konto aufgeführt wird.
- **Verhindern, dass das Gastkonto den Computer herunterfahren kann** Wenn ein Computer herunter- oder hochgefahren wird, wäre es denkbar, dass sich ein Gast (oder jeder andere Benutzer mit lokalem Zugriff) nichtautorisierten Zugriff auf den Computer verschafft. Um das möglichst zu verhindern, sollten Sie dafür sorgen, dass das Gastkonto nicht über das Benutzerrecht *Herunterfahren des Systems* verfügt. Erweitern Sie in der Konsole *Lokale Sicherheitsrichtlinie* die Knoten *Lokale Richtlinien*, *Zuweisen von Benutzerrechten* und sorgen Sie dafür, dass das Konto *Gast* nicht in der Richtlinie *Herunterfahren des Systems* aufgeführt wird.

- **Verhindern, dass das Gastkonto Ereignisprotokolle anzeigen kann** Um die Sicherheit des Systems nicht zu beeinträchtigen, sollte dem Gastkonto nicht erlaubt werden, Ereignisprotokolle einzusehen. Um dafür zu sorgen, starten Sie den Registrierungs-Editor, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten *regedit* eingeben und den Schlüssel *HKLM\System\CurrentControlSet\Services\Eventlog* herausuchen. Dort finden Sie drei wichtige Unterschlüssel: *Application*, *Security* und *System*. Sorgen Sie dafür, dass es unter jedem dieser Unterschlüssel einen *DWORD*-Wert namens *Restrict-GuestAccess* gibt, der den Wert 1 hat.

Umbenennen lokaler Benutzerkonten und Gruppen

Wenn Sie ein Konto umbenennen, ändern Sie damit nur die Beschriftung. Da die SID für das Konto unverändert bleibt, ändern sich auch nicht die Berechtigungen oder sonstige Eigenschaften des Kontos. Gehen Sie folgendermaßen vor, um ein Konto umzubenennen, während Sie auf einen lokalen Computer zugreifen:

1. Wählen Sie in *Lokale Benutzer und Gruppen* nach Bedarf den Ordner *Benutzer* oder *Gruppen*.
2. Klicken Sie den Kontonamen mit der rechten Maustaste an oder halten Sie ihn gedrückt, und wählen Sie *Umbenennen*. Geben Sie einen neuen Kontonamen ein und tippen oder klicken Sie dann auf einen anderen Eintrag.

Gehen Sie folgendermaßen vor, um ein Konto mithilfe von Gruppenrichtlinien umzubenennen:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Wenn Sie die Einstellungen für Computer konfigurieren wollen, müssen Sie *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Lokale Benutzer und Gruppen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Lokale Benutzer und Gruppen* auswählen.
2. Sie haben jetzt folgende Möglichkeiten:
 - Wenn es bereits ein Einstellungselement für den Benutzer oder die Gruppe gibt, können Sie doppelt auf den Benutzer- oder Gruppennamen tippen oder klicken, um das zugehörige Eigenschaftendialogfeld zu öffnen. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Aktualisieren* aus. Geben Sie im Feld *Umbenennen zu* den neuen Kontonamen ein und tippen oder klicken Sie auf *OK*.
 - Ist noch kein Einstellungselement für den Benutzer oder die Gruppe vorhanden, müssen Sie eines anlegen. Wie das geht, wurde bereits weiter oben beschrieben. Weil Sie den Benutzer oder die Gruppe umbenennen wollen, müssen Sie in der Dropdownliste *Aktion* den Eintrag *Aktualisieren* wählen und dann den neuen Kontonamen im Feld *Umbenennen zu* eingeben.

Löschen lokaler Benutzerkonten und Gruppen

Durch seine Löschung wird ein Konto endgültig entfernt. Nachdem Sie ein Konto gelöscht haben, können Sie nicht einfach ein neues Konto mit demselben Namen anlegen und dann erwarten, dass die Einstellungen des gelöschten Kontos automatisch für das neue Konto gelten, denn das neue Konto hat eine andere SID erhalten.

Da die Löschung eines vordefinierten Kontos weitreichende Auswirkungen auf die Arbeitsstation hätte, lässt Windows 8 es nicht zu, dass Sie eines der vordefinierten Benutzer- oder Gruppenkonten löschen. Andere Konten können Sie in *Lokale Benutzer und Gruppen* löschen, indem Sie ein Konto auswählen und die ENTF-Taste drücken oder indem Sie ein Konto mit der rechten Maustaste anklicken oder es gedrückt

halten und *Löschen* wählen. Wenn Sie zur Bestätigung des Vorgangs aufgefordert werden, tippen oder klicken Sie auf *Ja*.

HINWEIS

Wenn Sie mit *Lokale Benutzer und Gruppen* ein Konto löschen, löscht Windows 8 nicht die Profildaten, die persönlichen Dateien oder das Stammverzeichnis des Benutzers. Sollen auch diese Dateien und Ordner gelöscht werden, müssen Sie das selbst übernehmen.

Gehen Sie folgendermaßen vor, um ein Konto mithilfe von Gruppenrichtlinien zu löschen:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Wenn Sie die Einstellungen für Computer konfigurieren wollen, müssen Sie *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Lokale Benutzer und Gruppen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Lokale Benutzer und Gruppen* auswählen.
2. Sie haben jetzt folgende Möglichkeiten:
 - Wenn es bereits ein Einstellungselement für den Benutzer oder die Gruppe gibt, können Sie doppelt auf den Benutzer- oder Gruppennamen tippen oder klicken, um das zugehörige Eigenschaftendialogfeld zu öffnen. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Löschen* aus. Legen Sie auf der Registerkarte *Gemeinsam* die gewünschten Optionen fest, beispielsweise *Nur einmal anwenden*, und tippen oder klicken Sie auf *OK*.
 - Ist noch kein Einstellungselement für den Benutzer oder die Gruppe vorhanden, müssen Sie eines anlegen. Wie das geht, wurde bereits weiter oben beschrieben. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Löschen* aus und legen Sie auf der Registerkarte *Gemeinsam* die gewünschten Optionen fest.

Verwalten des Remotezugriffs auf Arbeitsstationen

Windows 8 bietet einige Funktionen, die auf Remoteverbindungen basieren. Mit der *Remoteunterstützung* können Benutzer Remoteunterstützungsanforderungen an Supporttechniker senden, die dann einen Computer im Remotezugriff warten können. Mit dem *Remotedesktop* können Benutzer eine Remoteverbindung mit einem Computer herstellen und auf seine Ressourcen zugreifen. Dieser Abschnitt beschreibt, wie Sie Remoteunterstützung und Remotedesktop konfigurieren. Normalerweise ist weder Remoteunterstützung noch Remotedesktop aktiviert, Sie müssen diese Funktionen also manuell aktivieren.

Remoteunterstützung und Remotedesktop funktionieren durch Firewalls hindurch, die Netzwerkadressübersetzung (Network Address Translation, NAT) verwenden. Remoteunterstützung bietet zudem integrierte Diagnosefunktionen. Um bei Bedarf eine gründliche Problemsuche und die einfache Weitergabe von Informationen über das Problem zu ermöglichen, können zwei Supportmitarbeiter gleichzeitig eine Verbindung mit einem Remotecomputer aufnehmen. Wenn die Problembehebung einen Neustart des Computers erfordert, werden die Remoteunterstützungssitzungen nach dem Neustart des betreffenden Computers automatisch wiederhergestellt.

Bevor ein Benutzer Remoteunterstützung anfordert, ist es sinnvoll, wenn er mithilfe der Problemaufzeichnung Schritt für Schritt festhält, wie das Problem aussieht. Die Problemaufzeichnung ist ganz einfach zu benutzen. Gehen Sie folgendermaßen vor, um die Problemaufzeichnung zu starten und zu verwenden:

1. Bringen Sie den Benutzer dazu, die Problemaufzeichnung zu starten. Dazu kann er zum Beispiel die WINDOWS-Taste drücken, **psr** eingeben und die EINGABETASTE drücken. Sobald das Tool läuft, kann der Benutzer die Umgebung vorbereiten und dann damit beginnen, das Problem aufzuzeichnen.
2. Um mit der Aufzeichnung zu beginnen, tippt oder klickt der Benutzer auf *Aufzeichnung starten*. Sobald die Aufzeichnung läuft, führt der Benutzer die Aktionen durch, bei denen das Problem auftritt. Dabei kann er auf *Kommentar hinzufügen* tippen oder klicken, um Kommentare einzufügen, während er arbeitet.
3. Wenn der Benutzer das Problem reproduziert hat und die zugehörigen Fehlermeldungen angezeigt wurden, beendet er die Aufzeichnung, indem er auf *Aufzeichnung beenden* klickt oder tippt.
4. Wenn der Benutzer die Aufzeichnung beendet, zeigt die Problemaufzeichnung alle Schritte, die der Benutzer unternommen hat, während die Aufzeichnung lief. Der Benutzer kann dann auf *Speichern* tippen oder klicken, um das Dialogfeld *Speichern unter* zu öffnen. Hier wählt der Benutzer den Speicherort und einen Namen für die Zip-Datei aus, die die Aufzeichnung des Problems in Form einer *.mhtml*-Datei enthält.
5. Der Benutzer kann die Zip-Datei nun in einer E-Mail-Nachricht an einen Supporttechniker senden oder sie in eine Dateifreigabe kopieren. Der Supporttechniker sieht sich die Aufzeichnung des Problems an, indem er doppelt auf die Zip-Datei klickt oder tippt, um ihren Inhalt im Datei-Explorer anzuzeigen, und dann doppelt auf die enthaltene *.mht*-Datei, um sie im Internet Explorer anzusehen.
6. Der Supporttechniker bekommt nun die Bildschirmausgabe für alle Schritte angezeigt, die der Benutzer durchgeführt hat, während das Problem aufgezeichnet wurde. Hinter den jeweiligen Bildschirmfotos werden zusätzliche Details zu jedem Schritt aufgeführt, die automatisch generiert worden sind. Anhand dieser Informationen und der Kommentare des Benutzers kann der Supporttechniker nun über das weitere Vorgehen bei der Problembehandlung entscheiden.

Konfigurieren der Remoteunterstützung

Remoteunterstützung ist eine nützliche Funktion, wenn es um die Unterstützung und Beratung von Benutzern geht, sei es durch Mitarbeiter des Unternehmens oder durch externe Berater. Ein Benutzer kann es dem Berater erlauben, ihm bei der Arbeit zuzusehen oder die Kontrolle über den Computer zu übernehmen. Diese Funktion kann dazu verwendet werden, um den Benutzer zum Beispiel durch einen komplexen Ablauf zu führen oder Systemeinstellungen vorzunehmen, während er die Änderungen an seinem Monitor verfolgt. Entscheidend für die Remoteunterstützung ist die Zugriffsebene, die Sie dem Berater gewähren.

Standardmäßig ist die Remoteunterstützung so eingestellt, dass sie dem Berater die Beobachtung und Steuerung des Computers ermöglicht, sofern sie aktiviert wird. Da Benutzer die Remoteunterstützungseinladung an interne und externe Berater senden können, ist dies natürlich ein Aspekt, der unter Sicherheitsgesichtspunkten sorgfältig durchdacht werden muss. Um potenzielle Sicherheitsrisiken zu begrenzen, können Sie die Möglichkeiten des Beraters auf die Einsichtnahme beschränken und ihm die Steuerung des Computers verweigern. Für Windows 8 lässt sich auch festlegen, dass nur Verbindungen mit Windows Vista-Computern oder höher zulässig sind. Diese Option ist sinnvoll, um Kompatibilitätsprobleme zu vermeiden und sicherzustellen, dass die verbesserten Sicherheitsmechanismen von Windows Vista oder höher auch für Remoteunterstützungssitzungen gelten.

Ein weiterer wichtiger Aspekt der Remoteunterstützung, den Sie kontrollieren können, ist die Zeitbeschränkung für die Gültigkeitsdauer der Einladungen. Die Standardgültigkeitsdauer beträgt 6 Stunden, die maximale Gültigkeitsdauer, die Sie einstellen können, ist 30 Tage. Sinn einer mehrtätigen Gültigkeitsdauer ist zwar, den Beratern Zeit für eine Antwort zu lassen, aber sie bedeutet auch, dass diese Berater im

Extremfall über einen Zeitraum von 30 Tagen hinweg auf einen Computer zugreifen können. Nehmen wir beispielsweise an, Sie senden einem Techniker eine Einladung mit einem 30-Tage-Limit und der Techniker löst das Problem bereits am ersten Tag. Dann hat er noch weitere 29 Tage lang Zugang zum Computer. Unter Sicherheitsaspekten ist das nicht wünschenswert. Um das Risiko für Ihre Systeme zu beschränken, sollten Sie normalerweise wesentlich kürzere Gültigkeitszeiträume wählen, zum Beispiel 1 Stunde. Ist das Problem in diesem Zeitraum nicht zu lösen, können Sie eine weitere Einladung versenden.

Gehen Sie folgendermaßen vor, um die Remoteunterstützung zu konfigurieren:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*. Tippen oder klicken Sie unter der Überschrift *System* auf *Remotezugriff zulassen*. Dadurch öffnet sich das Dialogfeld *Systemeigenschaften* mit vorgewählter Registerkarte *Remote*, wie in Abbildung 7.13 gezeigt.

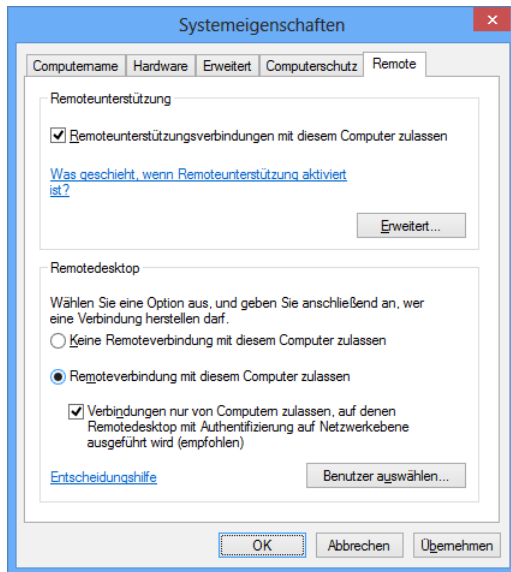


Abbildung 7.13 Verwenden Sie die Optionen der Registerkarte *Remote* zur Einrichtung der Remoteunterstützung für den Computer

2. Um die Remoteunterstützung zu deaktivieren, löschen Sie das Kontrollkästchen *Remoteunterstützungsverbindungen mit diesem Computer zulassen* und tippen oder klicken auf *OK*. Überspringen Sie die restlichen Schritte.
3. Um die Remoteunterstützung zu aktivieren, aktivieren Sie das Kontrollkästchen *Remoteunterstützungsverbindungen mit diesem Computer zulassen*.
4. Tippen oder klicken Sie auf *Erweitert*. Es öffnet sich das Dialogfeld *Remoteunterstützungseinstellungen* (Abbildung 7.14).
5. Die Option *Remotesteuern dieses Computers zulassen* hebt eine wichtige Einschränkung für die Remoteunterstützung auf. Ist sie gewählt, kann der Berater den Computer nicht nur einsehen, sondern auch kontrollieren. Wenn sein Einfluss auf die Einsichtnahme beschränkt werden soll, löschen Sie dieses Kontrollkästchen.
6. Mit den Einladungsoptionen lässt sich das Zeitfenster festlegen, in dem eine Einladung gültig sein soll. Sie können einen Wert im Bereich von Minuten, Stunden oder bis zu 30 Tagen festlegen. (Das

Dialogfeld lässt zwar auch Angaben bis zu 99 Tagen zu, aber jeder Wert, der 30 Tage übersteigt, wird auf 30 zurückgesetzt, sobald Sie auf OK tippen oder klicken.) Wenn Sie zum Beispiel eine Gültigkeitsdauer von 10 Tagen festlegen, kann ein Benutzer keine Einladungen versenden, die länger als 10 Tage gelten. Die Standardvorgabe für die Gültigkeitsdauer einer Einladung ist 6 Stunden.

- 7. Tippen oder klicken Sie auf die OK-Schaltflächen der beiden geöffneten Dialogfelder, wenn Sie mit dem Einstellen der Remoteunterstützungsoptionen fertig sind.

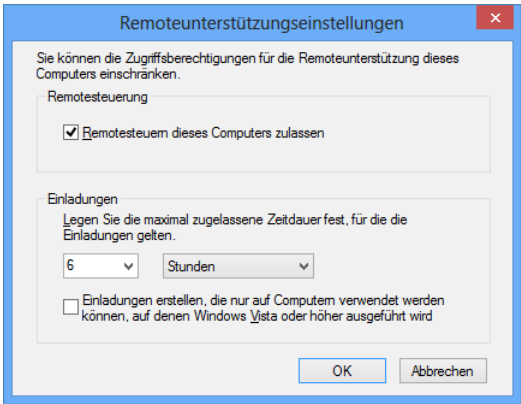


Abbildung 7.14 Das Dialogfeld *Remoteunterstützungseinstellungen* dient zur gezielten Einschränkung der Remoteunterstützung

In den Gruppenrichtlinien können Sie die Remoteunterstützung mithilfe der Richtlinieneinstellungen verwalten, die in Tabelle 7.2 aufgelistet sind. Diese Einstellungen befinden sich unter den angegebenen Pfaden in *Computerkonfiguration/Richtlinien/Administrative Vorlagen*.

Tabelle 7.2 Richtlinieneinstellungen zum Verwalten der Remoteunterstützung

Einstellung	Pfad
"Angeforderte Remoteunterstützung" konfigurieren	\System\Remoteunterstützung
Nur Verbindungen von Computern mit Windows Vista oder höher zulassen	\System\Remoteunterstützung
"Remoteunterstützung anbieten" konfigurieren	\System\Remoteunterstützung
Sitzungsprotokollierung aktivieren	\System\Remoteunterstützung

Konfigurieren des Remotedesktopzugriffs

Im Gegensatz zur Remoteunterstützung, die im Wesentlichen eine Darstellung des aktuellen Desktops des Benutzers ermöglicht, bietet Remotedesktop mehrere Zugriffsebenen:

- Wenn ein Benutzer aktuell auf dem lokalen Desktop angemeldet ist und dann von einem anderen Computer aus versucht, sich remote anzumelden, wird der lokale Desktop automatisch gesperrt und der Benutzer kann alle seine laufenden Anwendungen benutzen, als würde er vor Ort an der Tastatur sitzen. Diese Funktion ist besonders für Benutzer geeignet, die von zu Hause oder von anderen Orten aus weiterarbeiten möchten. Sie können an Anwendungen und Dokumenten weiterarbeiten, mit denen sie vor dem Verlassen des Büros gearbeitet haben.

- Wenn ein Benutzer in der Remotezugriffsliste einer Arbeitsstation eingetragen und nicht anderweitig angemeldet ist, kann er eine neue Windows-Sitzung einleiten. Die Windows-Sitzung verhält sich so, als würde der Benutzer vor Ort an der Tastatur sitzen. Das funktioniert sogar dann, wenn noch weitere Benutzer am Computer angemeldet sind. Auf diese Weise können sich mehrere Benutzer eine Arbeitsstation teilen und ihre Ressourcen benutzen.

Remotedesktop ist nicht standardmäßig aktiviert. Sie müssen die Funktion explizit aktivieren und dadurch den Remotezugriff auf die Arbeitsstation zulassen. Ist Remotedesktop aktiviert, können alle Mitglieder der Administratorgruppe eine Verbindung mit der Arbeitsstation herstellen. Andere Benutzer müssen zuvor in eine Remotezugriffsliste eingetragen werden, um Zugriff auf die Arbeitsstation zu erhalten. Gehen Sie zur Einstellung des Remotezugriffs folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie im linken Anzeigebereich der Seite *System* auf *Remoteeinstellungen*. Dadurch öffnet sich das Dialogfeld *Systemeigenschaften* mit vorgewählter Registerkarte *Remote*.
3. Zur Deaktivierung von Remotedesktop wählen Sie *Keine Remoteverbindung mit diesem Computer zulassen* und tippen oder klicken auf *OK*. Überspringen Sie die restlichen Schritte.
4. Zur Aktivierung von Remotedesktop gibt es zwei Optionen:
 - Wählen Sie *Remoteverbindungen mit diesem Computer zulassen*, um Verbindungen von jeder Windows-Version zuzulassen.
 - Wählen Sie außerdem *Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird*, um nur Verbindungen von Windows Vista-Computern oder höher zuzulassen (und von Computern mit sicherer Netzwerkauthentifizierung).
5. Tippen oder klicken Sie auf *Benutzer auswählen*. Dadurch öffnet sich das Dialogfeld *Remotedesktopbenutzer* (Abbildung 7.15).

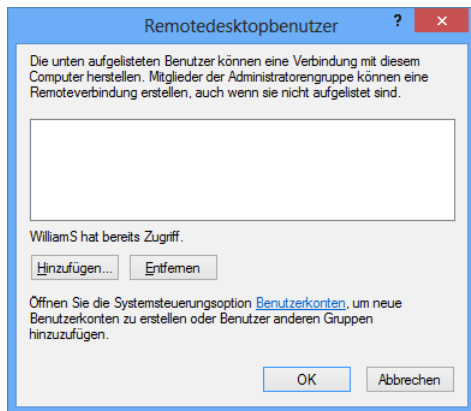


Abbildung 7.15 Geben Sie weitere Benutzer an, die Remotedesktopverbindungen herstellen dürfen

6. Um einem Benutzer Remotedesktopzugriff zu gewähren, tippen oder klicken Sie auf *Hinzufügen*. Dadurch öffnet sich das Dialogfeld *Benutzer auswählen*. Im Dialogfeld *Benutzer auswählen* tippen oder klicken Sie auf *Pfade*, um den Computer oder die Domäne auszuwählen, in der die gewünschten Benutzerkonten liegen. Geben Sie im Textfeld *Geben Sie die zu verwendenden Objektnamen ein* den Namen eines Benutzers ein und klicken Sie dann auf *Namen überprüfen*. Werden Übereinstimmun-

gen gefunden, wählen Sie das gewünschte Konto aus und tippen oder klicken dann auf *OK*. Werden keine passenden Konten gefunden, korrigieren Sie den Namen, den Sie eingegeben haben, und wiederholen die Suche. Wiederholen Sie diesen Vorgang so oft wie nötig und tippen oder klicken Sie auf *OK*, wenn Sie fertig sind.

7. Um die Zugriffsberechtigung für ein Konto aufzuheben, wählen Sie das Konto aus und tippen oder klicken dann auf *Entfernen*.
8. Tippen oder klicken Sie auf *OK* in den beiden geöffneten Dialogfeldern, wenn Sie fertig sind.

Tabelle 7.3 Richtlinieneinstellungen zum Verwalten des Remotedesktops

Einstellung	Pfad unter Computerkonfiguration
	Pfade unter Windows-Komponenten\Remotedesktopdienste
Anzahl Überwachungen beschränken (gemeint sind Monitore)	\Remotedesktopsitzungs-Host\Umgebung für Remotesitzung
Abmelden von Administratoren in Konsolensitzung verweigern	\Remotedesktopsitzungs-Host\Verbindungen
Automatisch erneut verbinden	\Remotedesktopsitzungs-Host\Verbindungen
Bei der Verbindungsherstellung immer zur Kennworteingabe auffordern	\Remotedesktopsitzungs-Host\Sicherheit
Berechtigungsanpassung für lokale Administratoren nicht zulassen	\Remotedesktopsitzungs-Host\Sicherheit
Gesamtgröße des Caches für servergespeicherte Benutzerprofile begrenzen	\Remotedesktopsitzungs-Host\Profile
Gleichmäßige CPU-Zeitplanung deaktivieren	\Remotedesktopsitzungs-Host\Verbindungen
Maximale Bildschirmauflösung begrenzen	\Remotedesktopsitzungs-Host\Umgebung für Remotesitzung
Maximale Farbtiefe einschränken	\Remotedesktopsitzungs-Host\Umgebung für Remotesitzung
Netzwerkerkennung auf dem Server auswählen	\Remotedesktopsitzungs-Host\Verbindungen
RDP-Dateien von gültigen Herausgebern und standardmäßige RDP-Einstellungen des Benutzers zulassen	\Remotedesktopverbindungs-Client
RDP-Dateien von unbekannten Herausgebern zulassen	\Remotedesktopverbindungs-Client
RDP-Transportprotokolle auswählen	\Remotedesktopsitzungs-Host\Verbindungen
Serverauthentifizierung für Client konfigurieren	\Remotedesktopverbindungs-Client
SHA1-Fingerabdrücke von Zertifikaten angeben, die vertrauenswürdige RDP-Herausgeber darstellen	\Remotedesktopverbindungs-Client
Speichern von Kennwörtern nicht zulassen	\Remotedesktopverbindungs-Client
Verschlüsselungsstufe der Clientverbindung festlegen	\Remotedesktopsitzungs-Host\Sicherheit
Verwendung einer bestimmten Sicherheitsstufe für Remoteverbindungen (RDP) ist erforderlich	\Remotedesktopsitzungs-Host\Sicherheit
	andere Pfade
Remotedesktopfreigabe deaktivieren	\Windows-Komponenten\NetMeeting
Windows-Firewall: Eingehende Remotedesktopausnahmen zulassen	\Netzwerk\Netzwerkverbindungen\Windows-Firewall\Domänenprofil
Windows-Firewall: Eingehende Remotedesktopausnahmen zulassen	\Netzwerk\Netzwerkverbindungen\Windows-Firewall\Standardprofil

Windows-Firewall muss so konfiguriert sein, dass sie Ausnahmen für eingehende Remotedesktopverbindungen zulässt. Die Konfiguration können Sie auf jedem Computer einzeln in der Windows-Firewall für das Domänenprofil und das Standardprofil vornehmen. In den Gruppenrichtlinien stehen die Richtlinien-einstellungen aus Tabelle 7.3 zur Verfügung, um diese Ausnahme einzurichten und den Remotedesktop zu konfigurieren. Sie finden diese Einstellungen im angegebenen Pfad unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen*.

Herstellen von Remotedesktopverbindungen

Als Administrator können Sie Remotedesktopverbindungen mit Windows-Servern und Windows-Arbeitsstationen herstellen. Für Remotedesktopverbindungen mit Servern, auf denen Windows 2000 Server ausgeführt wird, installieren Sie die Terminaldienste und konfigurieren die Dienste für den Remotezugriffsmodus. Unter Windows XP Professional und Nachfolgern wird Remotedesktop zwar automatisch installiert, aber normalerweise nicht automatisch aktiviert. Das müssen Sie explizit durchführen, wie im vorigen Abschnitt dieses Kapitels beschrieben. Sobald Remotedesktop auf einem Computer aktiviert ist, haben alle Administratoren Remotezugriff auf den Computer. Anderen Benutzern kann nach Bedarf die Berechtigung für den Remotezugriff gewährt werden.

Zur Herstellung einer Remotedesktopverbindung mit einem Server oder einer Arbeitsstation gehen Sie folgendermaßen vor:

1. Geben Sie auf einer Befehlszeile **mstsc** ein oder drücken Sie die WINDOWS-Taste, geben Sie **mstsc** ein und drücken Sie die EINGABETASTE.
2. Tippen oder klicken Sie auf die Schaltfläche *Optionen einblenden*. Dadurch werden die Registerkarten des Dialogfelds *Remotedesktopverbindung* sichtbar (Abbildung 7.16).



Abbildung 7.16 Geben Sie im Dialogfeld *Remotedesktopverbindung* den Namen des Computers ein, mit dem Sie eine Verbindung herstellen möchten, und tippen oder klicken Sie auf *Verbinden*

3. Geben Sie im Textfeld *Computer* den Namen des Computers ein, mit dem Sie eine Verbindung herstellen möchten. Wenn Sie den Namen des Computers nicht kennen, verwenden Sie die Dropdownliste und wählen einen verfügbaren Computer aus. Oder Sie wählen in der Dropdownliste *Nach weiteren Computern suchen*, um eine Liste der Domänen und dazugehörigen Computer anzuzeigen.
4. Stellen Sie bei Bedarf weitere Optionen ein. Falls Sie gespeicherte Anmeldeinformationen für den Computer konfiguriert haben, werden diese Anmeldeinformationen automatisch benutzt. Sie können die Anmeldeinformationen bei Bedarf bearbeiten oder löschen.
5. Tippen oder klicken Sie auf *Verbinden*. Sofern Sie vorher noch keine Anmeldeinformationen für den Computer gespeichert haben, erscheint ein Anmeldedialogfeld, in dem Sie Ihre Anmeldeinformationen eingeben und dann auf *OK* klicken müssen. Sofern die Verbindung aufgebaut werden kann, sehen Sie das Remotedesktopfenster des ausgewählten Computers und können mit den Ressourcen des Computers arbeiten. Sollte die Verbindung nicht zustande kommen, überprüfen Sie die Angaben, die Sie gemacht haben, und versuchen es erneut.

HINWEIS Antippen oder Anklicken der Schaltfläche *Optionen anzeigen* des Dialogfelds *Remotedesktopverbindung* führt zur Anzeige zusätzlicher Optionen für die Konfiguration der Verbindung und die Speicherung der Verbindungseinstellungen. Mit diesen Optionen können Sie die Anzeigegröße des Remotedesktops einstellen, Programme bei der Verbindungsherstellung automatisch starten, die lokale Zwischenspeicherung und die Datenkomprimierung aktivieren oder deaktivieren sowie Verbindungen mit den lokalen Ressourcen verwalten, wie zum Beispiel Druckern, seriellen Schnittstellen und Laufwerken.

Kapitel 8

Installieren und Verwalten von Programmen

In diesem Kapitel:

Verwalten von Desktop-Apps	270
Verwalten der Anwendungsvirtualisierung und der Ausführungsebenen	273
Programminstallation: Die Grundlagen	280
Bereitstellen von Anwendungen mithilfe von Gruppenrichtlinien	285
Konfigurieren der Programmkompatibilität	286
Verwalten von installierten und laufenden Programmen	290

Desktopprogramme sind Anwendungen, die Sie installieren und konfigurieren können. Die meisten Desktopprogramme verwenden den Windows-Installer, um die Verwaltung der Anwendungen zu erleichtern. Meistens installieren und konfigurieren Administratoren und Supportmitarbeiter die Programme, die auf Desktopcomputern eingesetzt werden. Zu den üblichen Arbeiten gehört es, Programme vor der Auslieferung neuer Computer zu installieren und zu konfigurieren, auf Anforderung neue Programme auf vorhandenen Computern zu installieren und vorhandene Programme zu aktualisieren, sobald neue Versionen verfügbar sind. Wenn Benutzer zusätzliche Programme installieren, werden Sie vielleicht auch zur Fehlerbehebung oder zur Deinstallation der Programme gerufen.

Die meisten Installationsprobleme sind ziemlich einfach zu lösen, wenn man weiß, worauf man achten muss. Andere Probleme können sich als sehr hartnäckig erweisen und erfordern manchmal mehr Arbeit, als man vermutet. Dieses Kapitel beschreibt, wie sich die Benutzerkontensteuerung auf die Installation und Verwendung von Anwendungen auswirkt und wie man Anwendungen installiert, wartet und deinstalliert. Außerdem erfahren Sie, wie Desktop-Apps installiert und konfiguriert werden. Mit den Bezeichnungen *Anwendungen* und *Software* sind in diesem Buch zwar im allgemeinen Desktop-Programme und Desktop-Apps gemeint, wobei eine App ein Programm im weitesten Sinne ist, aber es ist nun wichtig, zwischen Desktop-Programmen und Desktop-Apps zu unterscheiden.

Der Schwerpunkt dieses Kapitels liegt auf Programmen. Mit der Bezeichnung *App* sind in diesem Kapitel Desktop-Apps gemeint. Ich werde mit der Beschreibung der Apps beginnen, um den Rahmen für den Rest dieses Kapitels abzustecken.

Verwalten von Desktop-Apps

Apps sind in Windows 8 neu. Apps können im Windows Store gekauft und über das Internet installiert werden. Sie können Apps auch selbst entwickeln oder durch andere entwickeln lassen und mit Gruppenrichtlinien bereitstellen. Apps werden zwar so ähnlich wie Desktop-Programme verwaltet, weisen aber einige spezielle Eigenschaften auf.

Arbeiten mit Apps: Die Grundlagen

In Windows 8 ersetzt der Startbildschirm das herkömmliche Startmenü. Desktop-Apps werden bei der Installation automatisch zu *Start* hinzugefügt und erhalten dort auch eine Kachel. Eine *Start*-Kachel erleichtert es, die App zu starten und zu verwalten. Sie können mit der rechten Maustaste auf die Kachel klicken oder die Kachel gedrückt halten, um Verwaltungsoptionen anzuzeigen. Welche Verwaltungsoptionen verfügbar sind, hängt von der Art der Kachel ab. Live-Kacheln können ihre Inhalte aktualisieren und diese Aktualisierungen lassen sich ein- und ausschalten. Einige Kacheln können in verschiedenen Größen angezeigt werden. Solche Kacheln können Sie vielleicht vergrößern oder verkleinern. Wenn eine Kachel nicht mehr auf *Start* angezeigt werden soll, können Sie die Option *Von "Start" lösen* wählen.

Apps, die Sie von *Start* lösen, können Sie auf verschiedene Arten starten und verwalten. Ein Weg führt über die Liste *Alle Apps*. In Windows 8 entspricht *Alle Apps* dem Menü *Alle Programme* der älteren Windows-Versionen. Vom Startbildschirm aus können Sie *Alle Apps* anzeigen, indem Sie einen leeren Bereich des Startbildschirms mit der rechten Maustaste anklicken oder die Stelle gedrückt halten und dann *Alle Apps* wählen.

HINWEIS

Desktop-Programme werden vielleicht nicht automatisch zu *Start* oder *Alle Apps* hinzugefügt. Weitere Informationen finden Sie weiter hinten in diesem Kapitel im Abschnitt »Bereitstellen von Anwendungen für ausgewählte Benutzer oder für alle Benutzer«.

Für die Arbeit mit Apps und Kacheln gibt es einige praktische Tastenkombinationen, die sich auch für Desktop-Programme verwenden lassen:

- **WINDOWS-Taste+NACH-LINKS oder NACH-RECHTS** Schaltet die Andockfunktion um. Beim Andocken wird der Bildschirm aufgeteilt. Wenn eine App also normal angezeigt wird, dockt sie durch WINDOWS+NACH-LINKS links an und durch WINDOWS+NACH-RECHTS rechts.
- **WINDOWS-Taste+NACH-OBEN** Zeigt die App im Vollbildmodus.
- **WINDOWS-Taste+NACH-UNTEN** Beendet den Vollbildmodus und zeigt die App wieder mit ihrer ursprünglichen Fenstergröße.

Konfigurieren von vertrauenswürdigen Apps und Windows Store-Zugang

Gewöhnlich werden Apps über ein Netzwerk oder das Internet installiert und aktualisiert. Standardmäßig kann ein Windows 8-Computer nur vertrauenswürdige App-Pakete installieren, die vom Windows Store stammen. Wenn Sie vertrauenswürdige Apps installieren möchten, die von Ihnen oder anderen entwickelt wurden, müssen Sie die Richtlinie *Installation aller vertrauenswürdigen Apps zulassen* aktivieren, die in den administrativen Vorlagen der Computerkonfiguration unter *Windows-Komponenten\Bereitstellung von App-Paketen* zu finden ist.

Den Zugang der Benutzer zu Windows Store können Sie auf verschiedene Arten steuern:

- Sie können durch die Aktivierung der Richtlinie *Konten: Microsoft-Konten blockieren* die Verwendung von Microsoft-Konto auf einem Computer kontrollieren. Diese Richtlinie finden Sie in den Sicherheitsoptionen der Computerkonfiguration unter *Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien*. Wenn Sie diese Richtlinie aktivieren, stehen zwei Optionen zur Wahl. Sie können die Einstellung *Benutzer können keine Microsoft-Konten hinzufügen* verwenden, um Benutzer an der Erstellung von Microsoft-Konten zu hindern. Oder Sie verwenden *Benutzer können keine Microsoft-Konten hinzufügen oder sich damit anmelden*, um Benutzer daran zu hindern, Microsoft-Konten zu erstellen oder sich mit Microsoft-Konten anzumelden.
- Sie können Benutzer am Zugang zu Windows Store hindern, indem Sie die Richtlinie *Store-Anwendung deaktivieren* in den administrativen Vorlagen der Computerkonfiguration unter *Windows-Komponenten\Store* aktivieren.
- Sie können verhindern, dass Computer automatisch App-Updates herunterladen, indem Sie die Richtlinie *Automatisches Herunterladen von Updates deaktivieren* in den administrativen Vorlagen der Computerkonfiguration unter *Windows-Komponenten\Store* aktivieren.

Verbessern der Sicherheit für Apps und Außerkraftsetzen der Standardeinstellungen

Apps laufen in einem separaten Kontext und haben eine niedrigere Integritätseinstufung als Desktop-Programme. Die niedrigere Integritätsebene kann Apps trotzdem nicht davon abhalten, Aufgaben auszuführen, die sich negativ auf die Sicherheit auswirken, weil Sie andernfalls zustimmen müssten, damit der Vorgang durchgeführt wird, während Sie in diesen Fällen bei den Apps nicht zustimmen müssen. Apps können zum Beispiel standardmäßig eine Datei in einem Desktop-Programm öffnen. Bei einem unbekannten Dateityp oder Protokoll sehen die Benutzer ein Dialogfeld *Öffnen mit* und können eine lokale Anwendung auswählen, um den unbekannten Dateityp oder das unbekannte Protokoll zu öffnen, oder sie können den Store-Dienst verwenden, um eine Anwendung zu suchen, die das leistet.

Es gibt einige Richtlinien, mit denen sich die Sicherheit verbessern und solche Verhaltensweisen verhindern lassen:

- Um eine App daran zu hindern, automatisch ein Desktop-Programm zu öffnen, das mit einem Dateityp verknüpft ist, aktivieren Sie in den administrativen Vorlagen der Benutzerkonfiguration unter *Windows-Komponenten\App-Laufzeit* die Richtlinie *Starten von einer Datei zugeordneten Desktop-Apps verhindern*.
- Um eine App daran zu hindern, automatisch ein Desktop-Programm zu öffnen, das mit einem Protokoll verknüpft ist, aktivieren Sie in den administrativen Vorlagen der Benutzerkonfiguration unter *Windows-Komponenten\App-Laufzeit* die Richtlinie *Starten von Desktop-Apps, die einem Protokoll zugeordnet sind, verhindern*.
- Um die Option *Im Store nach einer App suchen* aus dem Dialogfeld *Öffnen mit* zu entfernen, aktivieren Sie in den administrativen Vorlagen der Computerkonfiguration unter *System\Internetkommunikationsverwaltung\Internetkommunikationseinstellungen* die Richtlinie *Zugriff auf den Store deaktivieren*.

Außerdem ist folgender Punkt wichtig: Einige Apps können auf dem Sperrbildschirm kurze Benachrichtigungen anzeigen, deren Verlauf standardmäßig protokolliert wird. Dieser Benachrichtigungsverlauf ermöglicht es, genau die Kachel nach einer Wiederanmeldung zu sehen, die bei ihrer letzten Abmeldung zu sehen war. Um Benachrichtigungen auf dem Sperrbildschirm zu sperren, aktivieren Sie in den administrativen Vorlagen der Computerkonfiguration unter *System\Anmelden* die Richtlinie *Anwendungsbenachrichtigungen auf gesperrtem Bildschirm deaktivieren*. Um den Benachrichtigungsverlauf zu löschen, wenn sich ein Benutzer abmeldet, aktivieren Sie in den administrativen Vorlagen der Benutzerkonfiguration unter *Startmenü und Taskleiste* die Richtlinie *Beim Beenden die Liste der Kachelbenachrichtigungen leeren*.

Anwendungen erhalten Benachrichtigungen über den Windows-Pushbenachrichtigungsdienst (Windows Push Notification Service, WNS). Live-Apps verwenden WNS, um die Darstellung auf ihren Kacheln zu aktualisieren, um Benachrichtigungen anzuzeigen und um Benachrichtigungen zu empfangen. Mit den administrativen Vorlagen für die Benutzerkonfiguration unter *Startmenü und Taskleiste\Benachrichtigungen* können Sie die Verwendung von WNS steuern:

- Um in Windows die Anzeige von Benachrichtigungen zu sperren, die ungefragt auf dem Bildschirm erscheinen (Popupbenachrichtigungen), aktivieren Sie die Richtlinie *Popupbenachrichtigungen deaktivieren*. Diese Einstellung wirkt sich nicht auf die Sprechblasen der Taskleiste aus.
- Um die Anzeige von Benachrichtigungen zu sperren, die auf dem Sperrbildschirm erscheinen, aktivieren Sie die Richtlinie *Popupbenachrichtigungen auf dem gesperrten Bildschirm deaktivieren*.
- Um die Aktualisierung von Kacheln und Kachelsignalen auf dem Startbildschirm zu sperren, aktivieren Sie die Richtlinie *Kachelbenachrichtigungen deaktivieren*.
- Um Apps daran zu hindern, Benachrichtigungen und Aktualisierungen zu versenden, aktivieren Sie die Richtlinie *Netzwerkverwendung für Benachrichtigungen deaktivieren*. Durch die Aktivierung dieser Richtlinie wird die Verbindung zwischen Windows und dem Windows-Pushbenachrichtigungsdienst deaktiviert.

PRAXISTIPP

Microsoft erfasst die Verwendung von Apps auf verschiedene Arten. Sie können diese Erfassung mit den Richtlinien aus den administrativen Vorlagen der Benutzerkonfiguration unter *Windows-Komponenten\Rand-UI* steuern.

Verbessern der Netzwerksicherheit für Apps

Windows 8 bietet einige neue Netzwerkfunktionen für Anwendungen im Allgemeinen und Apps im Besonderen. Windows 8 verwendet ein Feature namens Windows-Netzwerkisolation, um Proxys und private Netzwerkhosts automatisch zu erkennen, wenn ein Computer mit einer Domäne verbunden wird. Standardmäßig wird jeder erkannte Proxy als autorisierend eingestuft und jeder Netzwerkhost kann in den privaten Subnetzen erkannt werden, die für den Computer zugänglich sind.

Die Proxyerkennung und die Ermittlung privater Netzwerkhosts sind separate Funktionen. Die Proxyerkennung steuern Sie mit den Richtlinien aus den administrativen Vorlagen der Computerkonfiguration unter *Netzwerk\Netzwerkisolation*. Aktivieren Sie die Richtlinie *Internetproxyserver für Apps* und geben Sie eine durch Kommas getrennte Liste der IP-Adressen für Internetproxyserver an, die Anwendungen auf Computern der Domäne für den Zugriff auf das Internet verwenden können. Standardmäßig wird die Liste der Proxys mit der Liste der automatisch erkannten Proxys zusammengeführt. Wenn nur die von Ihnen angegebenen Proxys verwendet werden sollen, aktivieren Sie *Proxydefinitionen sind verbindlich*.

Mit der Richtlinie *Intranetproxyserver für Apps* geben Sie die zulässigen privaten Netzwerkproxyserver an. Aktivieren Sie diese Richtlinie und geben Sie eine durch Kommas getrennte Liste der Proxys an, die den Zugriff auf Intranetressourcen ermöglichen. Wenn nur die von Ihnen angegebenen Proxys verwendet werden sollen, aktivieren Sie *Proxydefinitionen sind verbindlich*.

Mit den Richtlinien aus den administrativen Vorlagen der Computerkonfiguration unter *Netzwerk\Netzwerkisolation* lässt sich auch die Ermittlung privater Netzwerkhosts steuern. Hosts, die auf diese Weise erkannt werden, werden als privat eingestuft. Normalerweise geht die Ermittlung privater Netzwerkhosts nicht über Subnetzgrenzen hinaus.

Sie können den Suchbereich erweitern, indem Sie die Richtlinie *Adressbereich des privaten Netzwerks für Apps* aktivieren und eine durch Kommas getrennte Liste der IPv4- und IPv6-Subnetze Ihrer Firma eingeben. Auf diese Weise erfährt Windows, welche Subnetze verfügbar sind und zur Ermittlung privater Netzwerkhosts verwendet werden können. Standardmäßig wird die Liste der Subnetze mit der Liste der automatisch erkannten Subnetze zusammengeführt. Wenn Sie *Subnetzdefinitionen sind verbindlich* aktivieren, werden nur Netzwerkhosts aus den in der Richtlinie angegebenen Adressbereichen gesucht und als privat eingestuft.

Verwalten der Anwendungsvirtualisierung und der Ausführungsebenen

Die Benutzerkontensteuerung (User Account Control, UAC) wirkt sich stark darauf aus, wie Anwendungen installiert und ausgeführt werden, wo sie Daten schreiben und welche Rechte Anwendungen haben. In diesem Abschnitt möchte ich Ihnen einen Überblick darüber geben, was die Benutzerkontensteuerung für die Installation von Anwendungen bedeutet, angefangen bei Sicherheitstoken über Datei- und Registrierungsvirtualisierung bis hin zu den Ausführungsebenen. Das gehört zum Grundlagenwissen, wenn man für die Installation und Wartung von Anwendungen in Windows 8 zuständig ist.

Zugriffstoken und Ortsvirtualisierung

Alle Anwendungen, die unter Windows 8 ausgeführt werden, lassen sich einer von zwei allgemeinen Gruppen zuordnen:

- **UAC-konform** Jede Anwendung, die speziell für Windows Vista oder Windows 8 entwickelt wurde, wird als konforme Anwendung betrachtet. Anwendungen, die als konform mit der neuen Windows 8-Architektur zertifiziert wurden, tragen das Logo »UAC-compliant«.
- **Altbestand** Alle Anwendungen, die für Windows XP oder eine ältere Windows-Version entwickelt wurden, gelten als Altbestand (oder Legacyanwendungen).

Die Unterscheidung zwischen UAC-konformen und Legacyanwendungen ist wegen der Architekturänderung wichtig, die zur Unterstützung der Benutzerkontensteuerung erforderlich war. UAC-konforme Anwendungen verwenden die Benutzerkontensteuerung, um die Angriffsfläche des Betriebssystems zu verkleinern. Das erfolgt dadurch, dass nichtautorisierte Anwendungen daran gehindert werden, sich ohne Zustimmung des Benutzers zu installieren oder zur Ausführung zu bringen. Außerdem werden die Standardberechtigungen eingeschränkt, die Anwendungen gewährt werden. Das erschwert es böswilliger Software, einen Computer zu übernehmen.

HINWEIS

Die Windows 8-Komponente, die für die Benutzerkontensteuerung zuständig ist, ist der Dienst *Anwendungsinformationen*. Dieser Dienst ermöglicht die Ausführung von interaktiven Anwendungen mit einem Administratorzugriffstoken. Den Unterschied zwischen einem Administratorzugriffstoken und einem gewöhnlichen Benutzerzugriffstoken können Sie sich ansehen, indem Sie zwei Eingabeaufforderungsfenster öffnen, eines als Standardbenutzer und eines mit erhöhten Rechten (klicken Sie das Programmsymbol des Eingabeaufforderungsfensters mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie *Als Admin ausführen*). Geben Sie in jedem Fenster den Befehl **whoami /all** ein und vergleichen Sie die Ergebnisse. Beide Zugriffstoken verfügen über dieselbe Sicherheitskennung (SID), aber das Administratorzugriffstoken verfügt über mehr Berechtigungen als das normale Benutzerzugriffstoken.

Alle Anwendungen, die unter Windows 8 ausgeführt werden, erhalten ihren Sicherheitskontext durch das Zugriffstoken des aktuellen Benutzers. Die Benutzerkontensteuerung macht aus allen Benutzern standardmäßig Standardbenutzer, selbst wenn es sich um Mitglieder der Administratorengruppe handelt. Hat ein Administrator zugestimmt, seine Administratorrechte anzuwenden, wird für ihn ein neues Zugriffstoken erstellt. Es umfasst alle Rechte des Benutzers. Dieses Zugriffstoken – und nicht das Standardzugriffstoken – wird für den Start einer Anwendung oder eines Prozesses verwendet.

In Windows 8 können die meisten Anwendungen mit dem Benutzerzugriffstoken ausgeführt werden. Ob eine Anwendung mit den Standardberechtigungen auskommt oder auf Administratorrechte angewiesen ist, hängt davon ab, was sie tut. Anwendungen, die auf Administratorrechte angewiesen sind (*Administratoranwendungen*), unterscheiden sich auf folgende Weise von Anwendungen, für deren Ausführung die Rechte eines Standardbenutzers ausreichen (*Benutzeranwendungen*):

- **Administratoranwendungen** erfordern erhöhte Rechte, um ausgeführt zu werden und ihre Kernaufgaben durchführen zu können. Nachdem sie mit erhöhten Rechten gestartet wurde, kann eine Anwendung mit dem Zugriffstoken eines Administrators Aufgaben durchführen, für die Administratorrechte erforderlich sind. Sie kann auch Schreibzugriffe auf Systembereiche der Registrierung und des Dateisystems durchführen.
- **Benutzeranwendungen** sind nicht auf erhöhte Rechte angewiesen, um ausgeführt zu werden und ihre Hauptaufgaben zu erfüllen. Wurde eine Anwendung im Benutzermodus gestartet und verfügt daher nur über ein gewöhnliches Benutzerzugriffstoken, muss sie erhöhte Rechte anfordern, um Administrationsaufgaben durchführen zu können. Für alle anderen Arbeiten sollte die Anwendung keine

erhöhten Rechte verwenden. Außerdem darf die Anwendung Schreibzugriffe auf die Registrierung und das Dateisystem nur in Bereichen durchführen, die nicht dem Betriebssystem vorbehalten sind.

Anwendungen, die nicht für Windows 8 entwickelt wurden, werden mit einem gewöhnlichen Benutzer-token ausgeführt. Zur Unterstützung der Benutzerkontensteuerungsarchitektur werden diese Anwendungen in einem speziellen Kompatibilitätsmodus ausgeführt. Sie setzen eine spezielle Virtualisierung des Dateisystems und der Registrierung ein und erhalten »virtualisierte« Ansichten der Registrierung und des Dateisystems. Versucht eine Anwendung einen Schreibzugriff auf einen Bereich, der dem System vorbehalten ist, gibt Windows 8 der Anwendung eine private Kopie der Datei oder des Registrierungswertes. Änderungen werden dann in dieser privaten Kopie gespeichert. Die private Kopie wiederum wird in den Profildaten des Benutzers gespeichert. Benutzt die Anwendung später erneut diesen Ort, der dem System vorbehalten ist, für Lese- oder Schreibzugriffe, erhält sie die private Kopie aus den Profildaten des Benutzers. Tritt bei der Bearbeitung solcher virtualisierten Daten ein Fehler auf, wird in der Fehlermeldung und im Fehlerprotokoll der virtualisierte Ort angegeben, und nicht das Original, das die Anwendung bearbeiten wollte.

Anwendungsintegrität und Ausführungsebenen

Die Ausrichtung auf die Aufteilung in Benutzer- und Administratorrechte wirkt sich auch auf die Rechte aus, die zur Installation und Ausführung von Anwendungen erforderlich sind. In Windows XP und älteren Windows-Versionen hatten Mitglieder der Hauptbenutzergruppe bei der Installation und Ausführung von Anwendungen bestimmte Administrationsrechte zur Ausführung von Arbeiten am System. Anwendungen, die für Windows 8 entwickelt wurden, kommen ohne Hauptbenutzergruppe aus. In Windows 8 gibt es diese Gruppe nur noch aus Gründen der Kompatibilität mit Legacyanwendungen.

Windows 8 erkennt im Rahmen der Benutzerkontensteuerung die Installation von Anwendungen und fordert standardmäßig vom Benutzer eine Erhöhung der Rechte an, um die Installation fortsetzen zu können. Installationspakete von UAC-konformen Anwendungen beschreiben die erforderlichen Rechte in einer speziellen Datei, die *Manifest* genannt wird. Ein Anwendungsmanifest beschreibt die für die Anwendung erforderlichen Berechtigungen folgendermaßen:

- **RunAsInvoker** Führt die Anwendung mit denselben Rechten aus, über die auch der Benutzer verfügt. Jeder Benutzer kann die Anwendung ausführen. Die Anwendung wird für Standardbenutzer und für Administratoren mit dem Standardzugriffstoken ausgeführt. Mit erhöhten Rechten wird die Anwendung nur ausgeführt, wenn der übergeordnete Prozess, der die Anwendung startet, über ein Administratorzugriffstoken verfügt. Wenn Sie beispielsweise eine Eingabeaufforderung mit erhöhten Rechten öffnen und in diesem Fenster eine Anwendung starten, wird diese Anwendung mit einem Administratorzugriffstoken ausgeführt.
- **RunAsHighest** Führt die Anwendung mit den höchsten Berechtigungen des Benutzers aus. Die Anwendung kann von Administratoren und von Standardbenutzern gestartet werden. Welche Aufgaben die Anwendung durchführen kann, hängt von den Rechten des Benutzers ab. Handelt es sich um einen Standardbenutzer, verwendet die Anwendung ein Standardzugriffstoken. Ist der Benutzer Mitglied einer Gruppe mit zusätzlichen Berechtigungen, wie zum Beispiel *Sicherungs-*, *Server-* oder *Konten-Operatoren*, wird die Anwendung mit einem partiellen Administratorzugriffstoken ausgeführt, das nur die Berechtigungen gewährt, über die der Benutzer verfügt. Ist der Benutzer Mitglied der Gruppe *Administratoren*, wird die Anwendung mit einem vollwertigen Administratorzugriffstoken ausgeführt.

- **RunAsAdmin** Die Anwendung wird mit Administratorrechten ausgeführt. Nur Administratoren können die Anwendung starten. Für Standardbenutzer oder Benutzer, die Mitglieder von Gruppen mit zusätzlichen Berechtigungen sind, wird die Anwendung nur ausgeführt, wenn vom Benutzer die Anmeldeinformationen angefordert werden können, die für eine Ausführung mit erhöhten Rechten erforderlich sind, oder wenn die Anwendung von einem Prozess mit erhöhten Rechten gestartet wird, beispielsweise von einem mit erhöhten Rechten ausgeführten Eingabeaufforderungsfenster. Für einen Benutzer, der zur Gruppe der Administratoren gehört, wird die Anwendung mit dem Administratorzugriffstoken ausgeführt.

Zum Schutz von Anwendungsprozessen kennzeichnet Windows 8 sie mit Integritätseinstufungen (Integritätsebenen) von niedrig bis hoch. Anwendungen, die Systemdaten ändern können, wie beispielsweise die Datenträgerverwaltung, werden auf eine hohe Integritätsebene eingestuft, während Anwendungen, die das Betriebssystem potenziell gefährden können, wie der Windows Internet Explorer 8 von Windows 8, nur eine niedrige Einstufung erreichen. Anwendungen von tieferen Integritätsebenen können Daten in Anwendungen von höheren Integritätsebenen nicht ändern.

Windows 8 identifiziert den Herausgeber jeder Anwendung, die versucht, mit dem vollen Administratorzugriffstoken ausgeführt zu werden. Je nach Herausgeber kennzeichnet Windows 8 die Anwendung und ordnet sie einer der folgenden drei Kategorien zu:

- Windows Vista oder höher
- Herausgeber verifiziert (signiert)
- Herausgeber nicht verifiziert (nicht signiert)

Damit Sie schnell das potenzielle Sicherheitsrisiko bei der Installation oder Ausführung der Anwendung erkennen, zeigt die farbkodierte Anhebungsaufforderung je nach der Kategorie, zu der die Anwendung gehört, eine entsprechende Meldung an:

- Stammt die Anwendung von einem Herausgeber, der blockiert wurde, oder wird sie durch entsprechende Gruppenrichtlinien blockiert, erscheint die Anhebungsaufforderung mit rotem Hintergrund und einer Meldung wie »Das Ausführen von Software auf dem Computer wurde für diesen Herausgeber geblockt«.
- Handelt es sich um ein Verwaltungsprogramm (beispielsweise um die Computerverwaltung), hat die Anhebungsaufforderung einen blaugrünen Hintergrund und zeigt eine Meldung wie »Möchten Sie zulassen, dass durch das folgende Programm Änderungen an diesem Computer vorgenommen werden?«
- Wurde die Anwendung mit Authenticode signiert und vom lokalen Computer als vertrauenswürdig akzeptiert, hat die Anhebungsaufforderung einen grauen Hintergrund und zeigt eine Meldung wie »Zur Fortsetzung des Programms ist Ihre Zustimmung erforderlich«.
- Ist die Anwendung nicht signiert (oder ist sie signiert, aber ihr wird nicht vertraut), hat die Anhebungsaufforderung einen gelben Hintergrund und ein rotes Schildsymbol und zeigt eine Meldung wie »Ein nicht identifiziertes Programm möchte auf den Computer zugreifen«.

Der Wechsel zum sicheren Desktop, auf den nur Kernprozesse von Windows Zugriff haben, sichert den Vorgang der Anhebung weiter ab. Der sichere Desktop schützt den Anhebungsprozess, weil er verhindert, dass die Anhebungseingabeaufforderung gefälscht werden kann. Der sichere Desktop wird standardmäßig in den Gruppenrichtlinien aktiviert, wie im Abschnitt »Optimieren von Benutzerkontensteuerung und Administratorgenehmigungsmodus« von Kapitel 7 beschrieben.

Festlegen der Ausführungsebenen

Standardmäßig werden nur Anwendungen, die mit einem Administratorzugriffstoken ausgeführt werden, mit erhöhten Rechten ausgeführt. Manchmal erleichtert es die Arbeit, wenn auch eine Anwendung mit erhöhten Rechten ausgeführt werden kann, die nur mit einem Standardzugriffstoken ausgeführt wird. Vielleicht möchten Sie beispielsweise ein Eingabeaufforderungsfenster mit erhöhten Rechten ausführen, damit Sie Administrationsarbeiten durchführen können.

Neben den bereits besprochenen Anwendungsmanifesten bietet Windows 8 zwei verschiedene Wege zur Festlegung der Ausführungsebene von Anwendungen:

- Sie führen eine Anwendung einmal als Administrator aus.
- Sie führen eine Anwendung immer als Administrator aus.

Um eine Anwendung einmal als Administrator auszuführen, klicken Sie die Verknüpfung oder den Menüeintrag der Anwendung mit der rechten Maustaste an oder halten ihn gedrückt und wählen *Als Administrator ausführen*. Wenn Sie ein Standardkonto verwenden und die Anhebungsaufforderung aktiviert ist, werden Sie vor dem Start der Anwendung um Ihre Zustimmung gebeten. Wenn Sie ein Standardkonto verwenden und die Anhebungsaufforderung deaktiviert ist, kann die Anwendung nicht gestartet werden. Wenn Sie ein Administratorkonto verwenden und die Anhebungsaufforderung aktiviert ist, werden Sie vor dem Start der Anwendung um Ihre Zustimmung gebeten.

Windows 8 ermöglicht es Ihnen, eine Anwendung so zu kennzeichnen, dass sie immer mit Administratorrechten ausgeführt wird. Auf diese Weise lassen sich zum Beispiel Kompatibilitätsprobleme mit Legacyanwendungen lösen, die Administratorrechte erfordern. Außerdem ist das bei UAC-konformen Anwendungen sinnvoll, die normalerweise im Standardmodus ausgeführt werden, mit denen Sie aber Verwaltungsarbeiten durchführen. Betrachten Sie folgende Beispiele:

- Eine Standardanwendung, die für Windows 8 entwickelt wurde, wird routinemäßig mit erhöhten Rechten ausgeführt und für Verwaltungsaufgaben verwendet. Damit es nicht mehr vor jedem Programmstart erforderlich ist, mit der rechten Maustaste auf die Programmverknüpfung zu klicken oder sie gedrückt zu halten und *Als Administrator ausführen* zu wählen, beschließen Sie, die Anwendung so zu kennzeichnen, dass sie immer mit Administratorrechten ausgeführt wird.
- Eine Anwendung, die für Windows XP oder eine ältere Windows-Version entwickelt wurde, erfordert Administratorrechte. Da dieses Programm unter Windows 8 standardmäßig so konfiguriert wird, dass es den Standardmodus verwendet, arbeitet es nicht korrekt und verursacht zahlreiche Fehler. Um dieses Kompatibilitätsproblem zu lösen, erstellen Sie mit Windows-Application Compatibility Toolkit (ACT) Version 5.5 oder neuer ein Anwendungskompatibilitäts-Shim. Als kurzfristige Lösung können Sie die Anwendung auch so markieren, dass sie immer mit dem Administratorkonto ausgeführt wird.

HINWEIS

Sie können keine Systemanwendungen oder Prozesse so kennzeichnen, dass sie immer mit Administratorprivilegien ausgeführt werden. Nur Anwendungen und Prozesse, die nicht zum Betriebssystem gehören, können so gekennzeichnet werden, dass sie immer auf dieser Ebene laufen.

PRAXISTIPP

Das Windows Application Compatibility Toolkit (ACT) ist eine Lösung für Administratoren, bei der nicht in die Programmierung der Anwendung eingegriffen werden muss. Das ACT hilft Ihnen, häufig auftretende Kompatibilitätsprobleme zu beseitigen. Zum Beispiel laufen einige Anwendungen nur unter einem bestimmten Betriebssystem oder wenn der Benutzer ein Administrator ist. Mit dem ACT können Sie ein Shim erstellen (das ist in diesem Fall eine zusätzliche Software-Schicht für den Ausgleich von kleinen Unterschieden, eine Art Software-Adapter). Das Shim antwortet auf Anfragen der

Anwendung bezüglich des Betriebssystems oder der Benutzerebene mit dem Wert *True*, damit die Anwendung läuft. Das ACT hilft Ihnen außerdem dabei, komplexere Lösungen für Anwendungen zu entwickeln, die versuchen, in geschützte Bereiche des Betriebssystems zu schreiben, oder erhöhte Privilegien benutzen, wenn das gar nicht nötig ist. Sie können das ACT im Microsoft Download Center herunterladen (<http://download.microsoft.com>).

Mit folgenden Schritten können Sie ein Programm so kennzeichnen, dass es immer mit Administrator-rechten ausgeführt wird:

1. Suchen Sie auf dem Desktop oder im Explorer die Anwendung, die Sie immer mit Administrator-rechten ausführen möchten.
2. Klicken Sie mit der rechten Maustaste auf die Verknüpfung der Anwendung oder halten Sie sie gedrückt, und tippen oder klicken Sie dann auf *Eigenschaften*.
3. Wählen Sie im *Eigenschaften*-Dialogfeld die Registerkarte *Kompatibilität* (Abbildung 8.1).

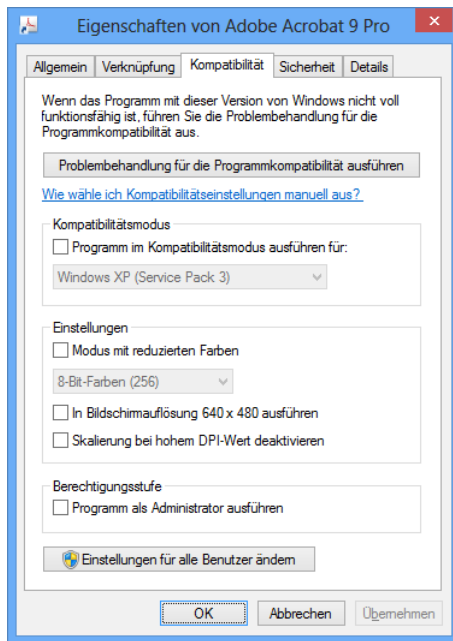


Abbildung 8.1 Die Registerkarte *Kompatibilität*

4. Sie haben jetzt folgende Möglichkeiten:
 - Wenn die Einstellung nur für den momentan angemeldeten Benutzer gelten soll, können Sie das Kontrollkästchen *Programm Als Administrator ausführen* aktivieren und auf *OK* tippen oder klicken.
 - Wenn die Einstellung für alle Benutzer des Computers und unabhängig davon gelten soll, über welche Verknüpfung die Anwendung gestartet wird, müssen Sie auf *Einstellungen für alle Benutzer ändern* tippen oder klicken. Daraufhin öffnet sich das Eigenschaftendialogfeld für die .exe-Datei der Anwendung. Aktivieren Sie hier das Kontrollkästchen *Programm Als Administrator ausführen* und tippen oder klicken Sie zweimal auf *OK*.

HINWEIS Wenn das Kontrollkästchen *Programm Als Administrator ausführen* nicht zugänglich ist, bedeutet dies, dass die ständige Ausführung der Anwendung mit erhöhten Rechten gesperrt ist, dass die Anwendung keine erhöhten Rechte erfordert oder dass Sie nicht als Administrator angemeldet sind.

Nun wird das Programm immer mit einem Administratorzugriffstoken ausgeführt. Vergessen Sie nicht, dass das Programm nicht ausgeführt wird, wenn Sie ein Standardkonto verwenden und die Anhebungsaufforderung deaktiviert ist.

Optimieren der Virtualisierung und die Anhebungsaufforderung bei Installationen

Was Anwendungen betrifft, lassen sich einige Bereiche der Benutzerkontensteuerung anpassen, darunter:

- Automatische Erkennung von Installationen und Anhebungsaufforderung
- Virtualisierung von Schreibzugriffen

In den Gruppenrichtlinien steuern Sie diese Features unter *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen*. Hier stehen folgende Sicherheitseinstellungen zur Verfügung:

- **Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern** Legt fest, ob Windows 8 automatisch die Installation von Anwendungen erkennt und den Benutzer um eine Anhebung der Rechte oder um Zustimmung bittet. (Diese Einstellung ist in Windows 8 standardmäßig aktiviert.) Wenn Sie diese Einstellung deaktivieren, erhalten Benutzer keine Anhebungsaufforderung und sind daher auch nicht in der Lage, die Rechte anzuheben, indem sie die Anmeldeinformationen eines Administrators angeben.
- **Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren** Bestimmt, ob die Virtualisierung von Schreibzugriffen auf bestimmte geschützte Dateien und Registrierungswerte aktiviert ist oder nicht. Da diese Einstellung standardmäßig aktiviert ist, werden Schreibzugriffe auf bestimmte Dateien und Registrierungswerte an die virtuellen Orte umgeleitet, statt an den von der Anwendung angesprochenen geschützten Orten zu erfolgen. Wenn Sie diese Einstellung deaktivieren, wird der Schreibzugriff auf geschützte Ordner oder geschützte Registrierungsbereiche ohne weitere Fehlermeldung fehlschlagen.

HINWEIS Andere Einstellungen für die Benutzerkontensteuerung wurden bereits im Kapitel 7 besprochen, im Abschnitt »Optimieren von Benutzerkontensteuerung und Administratorgenehmigungsmodus«.

In einer Domäne können Sie die gewünschte Sicherheitseinstellung für eine bestimmte Computergruppe mit Active Directory-Gruppenrichtlinien vornehmen. Mit den lokalen Gruppenrichtlinien können Sie die Einstellungen auch für jeden Computer einzeln vornehmen. Dazu gehen Sie so vor:

1. Öffnen Sie die Konsole *Lokale Sicherheitsrichtlinie*. Dazu können Sie zum Beispiel die WINDOWS-Taste drücken, **Secpol.msc** eingeben und die EINGABETASTE drücken. Wenn Sie für *Start* die Option *Verwaltungstools anzeigen* aktiviert haben, werden Sie auf dem Startbildschirm auch eine entsprechende Kachel finden.
2. Erweitern Sie in der Konsolenstruktur den Knoten *Lokale Richtlinien* unter *Sicherheitseinstellungen* und wählen Sie dann *Sicherheitsoptionen*.
3. Tippen oder klicken Sie die gewünschte Richtlinie doppelt an, führen Sie die erforderlichen Änderungen durch und klicken Sie dann auf **OK**.

Programminstallation: Die Grundlagen

Die Installation von Programmen ist ziemlich einfach. Nicht so einfach ist es, die vielen Dinge zu erkennen und zu beheben, die danebengehen können. Um die Probleme beheben zu können, die sich vielleicht ergeben, müssen Sie den Installationsvorgang verstehen. Eine typische Installation beginnt gewöhnlich damit, dass der Autorun-Mechanismus ausgelöst wird. Autorun wiederum startet ein Installationsprogramm. Sobald das Installationsprogramm gestartet ist, kann die Installation beginnen. Im Rahmen der Installation werden auch die Anmeldeinformationen des Benutzers überprüft, um sicherzustellen, dass er über das Recht zur Installation von Programmen verfügt. Wenn das nicht der Fall ist, wird er um die Anhebung der Rechte gebeten. Im Rahmen der Installation müssen Sie vielleicht auch entscheiden, ob das Programm nur für bestimmte Benutzer oder für alle Benutzer eines Computers zugänglich sein soll.

Es kommt gelegentlich vor, dass Windows die erforderlichen Installationsberechtigungen nicht richtig erkennt. Das kann passieren, wenn das Installationsmanifest für das Programm eine *RequestedExecutionLevel*-Einstellung eingebettet hat, deren Wert auf *RequireAdministrator* gesetzt ist. Weil die *RequestedExecutionLevel*-Einstellung Vorrang vor dem hat, was der Installer in Windows erkennt, schlägt der Installationsvorgang jedes Mal fehl, wenn Sie den Installer mit Standardbenutzerberechtigungen ausführen. Sie lösen dieses Problem, indem Sie die fehlgeschlagene Installation verlassen, das Setup abbrechen oder eine andere geeignete Aktion durchführen. Suchen Sie anschließend die ausführbare Datei des Installers. Klicken Sie mit der rechten Maustaste auf diese Datei oder halten Sie sie gedrückt, und wählen Sie den Befehl *Als Administrator ausführen*, um den Installationsvorgang mit Administratorprivilegien noch einmal auszuführen.

Anwendungssteuerungsrichtlinien ersetzen die Richtlinien für Softwareeinschränkung. Die Richtlinien für Softwareeinschränkung legen fest, welche Anwendungen Benutzer in Windows 2000, Windows XP und Windows Vista installieren und ausführen dürfen. Anwendungssteuerungsrichtlinien legen dagegen fest, welche Anwendungen die Benutzer in Windows 7 und höher installieren und ausführen dürfen, sowie in Windows Server 2008 Release 2 und höher. Dabei sind folgende Punkte wichtig:

- Wenn Sie ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) bearbeiten, können Sie Richtlinien für Softwareeinschränkung, die für Computer gelten sollen, unter *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für Softwareeinschränkung* erstellen und verwalten. Die Einstellungen für Benutzer verwalten Sie entsprechend unter *Benutzerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für Softwareeinschränkung*. Erzwingungseinstellungen steuern, wie Einschränkungen angewendet werden. Dafür vorgesehene Dateitypen legen fest, was als ausführbare Datei gilt und was nicht.
- Wenn Sie ein Gruppenrichtlinienobjekt bearbeiten, können Sie Anwendungssteuerungsrichtlinien, die für Computer gelten sollen, unter *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Anwendungssteuerungsrichtlinien* erstellen und verwalten. Hier können Sie separate Regeln für ausführbare Dateien, Windows Installer-Dateien und Skriptdateien konfigurieren. Regeln können auf Basis des Herausgebers, des Dateipfads oder des Dateihashes angewendet werden. Eine Herausgeberregel bietet am meisten Flexibilität; Sie können damit genau angeben, welche Produkte und Versionen erlaubt sind. Zum Beispiel können Sie auf diese Weise Microsoft Word 2007 oder neuer erlauben.

Verwenden von Autorun

Wenn Sie eine Anwendungs-CD oder -DVD einlegen, sucht Windows 8 nach einer Datei namens *Autorun.inf*. Ist sie vorhanden, legt *Autorun.inf* die Aktion fest, die das Betriebssystem durchführen soll, und kann auch weitere Installationsparameter angeben. *Autorun.inf* ist eine Textdatei, die sich in jedem Standardtexteditor öffnen lässt. Ein Beispiel:

```
[autorun]
OPEN=SETUP.EXE AUTORUN=1
ICON=SETUP.EXE,4
SHELL=OPEN
DisplayName=Microsoft Digital Image Suite 9
ShortName=PIS
PISETUP=PIP\pisetup.exe
```

Diese *Autorun.inf*-Datei öffnet eine Datei namens *Setup.exe*, wenn die CD- oder DVD in ein Laufwerk eingelegt wird. Da es sich bei *Setup.exe* um ein Programm handelt, wird das Programm gestartet. Die *Autorun.inf*-Datei gibt auch ein Programmsymbol an, den Status der Systemshell, den Anzeigenamen des Programms, einen kurzen Namen für das Programm und einen zusätzlichen Parameter, bei dem es sich in diesem Fall um ein weiteres Installationsprogramm handelt, das gestartet werden soll.

Bei der zu öffnenden Datei muss es sich nicht zwangsläufig um ein Programm handeln. Betrachten Sie folgendes Beispiel:

```
[autorun]
OPEN=Autorun\ShellExec default.htm
```

Diese *Autorun.inf*-Datei führt eine Systemshell aus und öffnet eine Datei namens *Default.htm*. Wichtig ist, dass das im Webbrowser geöffnete Dokument in diesem Fall Links auf ein Installationsprogramm enthält.

TIPP Wenn eine Anwendungs-CD oder -DVD im Laufwerk liegt, können Sie den Autorun-Vorgang jederzeit einleiten. Öffnen Sie einfach kurz das Laufwerk und schließen Sie es wieder.

Anwendungsinstallation und Kompatibilität

Die meisten Anwendungen verwenden zur Installation ein Installationsprogramm auf der Basis von InstallShield, Wise Install oder Windows Installer. Wenn Sie das Installationsprogramm starten, organisiert es den Ablauf der Installation und es sollte auch erlauben, das Programm bei Bedarf wieder zu deinstallieren. Wenn Sie eine ältere Anwendung installieren, wird vielleicht eine ältere Version dieser Installationsprogramme verwendet. Das kann bedeuten, dass das Programm bei der Deinstallation nicht vollständig vom Computer entfernt wird.

Selbst wenn Sie sicher sind, dass eine Anwendung mit einem aktuellen Installationsprogramm installiert wird, müssen Sie die Möglichkeit in Betracht ziehen, dass Sie vielleicht das System wiederherstellen müssen, falls bei der Installation etwas danebengeht. Um sicherzustellen, dass Sie Ihr System wiederherstellen können, sollten Sie prüfen, ob die Systemwiederherstellung für das Laufwerk aktiviert ist, auf dem Sie das Programm installieren, damit die Systemwiederherstellung einen automatischen Prüfpunkt anlegen kann, bevor das Programm installiert wird.

Die Installationsprogramme der meisten aktuellen Programme lösen automatisch die Erstellung eines Wiederherstellungspunkts aus, bevor irgendwelche Änderungen am Computer durchgeführt werden, aber für die Installationsprogramme älterer Programme gilt das nicht immer. Wie Sie einen Wiederher-

stellungspunkt manuell erstellen, wird in Kapitel 10, »Erledigen von Wartungs- und Supportaufgaben«, beschrieben. Sollten sich anschließend Probleme ergeben, können Sie die Anwendung deinstallieren und mit der Systemwiederherstellung das System in den Zustand zurückversetzen, in dem es sich vor der Installation der Anwendung befand.

Vor der Installation einer Anwendung sollten Sie überprüfen, ob die Anwendung zu Windows 8 kompatibel ist. Um das zu prüfen, können Sie Folgendes tun:

- Überprüfen Sie die Verpackung der Software, auf der die Kompatibilität angegeben sein sollte. Achten Sie auf das Windows 8-Logo.
- Suchen Sie auf der Website des Softwareherstellers nach einer Liste der kompatiblen Betriebssysteme.

HINWEIS

Suchen Sie im Rahmen der Kompatibilitätsüberprüfung auch nach Updates oder Patches für das Programm. Installieren Sie die Updates oder Patches, sofern verfügbar, nach der Installation des Programms.

Windows 8 versucht, potenzielle Kompatibilitätsprobleme zu erkennen, bevor Sie Anwendungen installieren. Entdeckt es ein Problem, öffnet sich möglicherweise ein Dialogfeld des Programmkompatibilitäts-Assistenten, sobald Sie die Installation des Programms starten. Dieses Dialogfeld enthält oft Informationen über bekannte Kompatibilitätsprobleme mit dem Programm. In vielen Fällen zeigt es auch gleich eine mögliche Lösung an. So werden Sie beispielsweise gebeten, das neueste Service Pack für das Programm zu installieren, bevor Sie das Programm auf dem Computer ausführen. In manchen Fällen zeigt der Programmkompatibilitäts-Assistent die Meldung »Dieses Programm wurde aufgrund von Kompatibilitätsproblemen geblockt«. Das Programm wurde in einem solchen Fall geblockt, weil bekannt ist, dass es Stabilitätsprobleme unter Windows verursacht, und sich das Problem nicht unmittelbar umgehen lässt. Sie haben dann nur die Möglichkeit, die Schaltflächen *Online nach Lösungen suchen* oder *Abbrechen* anzutippen oder anzuklicken. Wenn Sie online nach Lösungen suchen, wird meistens empfohlen, eine aktualisierte Version des Programms zu kaufen. Wenn Sie abbrechen, beenden Sie den Installationsvorgang, ohne nach möglichen Lösungen zu suchen.

Wenn die Installation weiterläuft, aber aus irgendeinem Grund fehlschlägt, bevor sie vollständig abgeschlossen ist (oder bevor das Betriebssystem darüber benachrichtigt wird, dass der Vorgang abgeschlossen ist), bekommen Sie ebenfalls ein Dialogfeld des Programmkompatibilitäts-Assistenten angezeigt. Ist das Programm in diesem Fall richtig installiert, können Sie auf *Das Programm wurde richtig installiert* tippen oder klicken. Wurde das Programm dagegen nicht richtig installiert, sollten Sie auf *Erneut mit den empfohlenen Einstellungen installieren* tippen oder klicken, damit der Programmkompatibilitäts-Assistent versuchen kann, bestimmte Kompatibilitätsreparaturen vorzunehmen und das Installationsprogramm dann erneut auszuführen.

Wenn Sie Programme starten, nimmt Windows 8 mit dem Programmkompatibilitäts-Assistenten bei bekannten Kompatibilitätsproblemen automatische Änderungen vor. Wenn der Programmkompatibilitäts-Assistent bei der Ausführung einer Anwendung ein bekanntes Kompatibilitätsproblem erkennt, informiert er Sie über dieses Problem und bietet Lösungen an. Sie können dem Programmkompatibilitäts-Assistenten dann erlauben, die Anwendung für Sie neu zu konfigurieren, oder Sie können manuell versuchen, die Kompatibilität herzustellen, wie im Abschnitt »Konfigurieren der Programmkompatibilität« weiter unten in diesem Kapitel beschrieben.

Die Richtlinien in den administrativen Vorlagen der Computerkonfiguration unter *Windows-Komponenten\Anwendungskompatibilität* werden auch zur Steuerung der Kompatibilitätseinstellungen verwendet. Dazu gehören:

- **Zugriff auf 16-Bit-Anwendungen verhindern** Ist diese Richtlinie aktiviert, kann das MS-DOS-Subsystem nicht auf Computern ausgeführt werden. Das bedeutet auch, dass 32-Bit-Programme mit 16-Bit-Installationsprogrammen oder anderen 16-Bit-Komponenten nicht lauffähig sind.
- **Programmkompatibilitäts-Eigenschaftenseite entfernen** Wenn diese Richtlinie aktiviert ist, ist die Registerkarte *Kompatibilität* nicht im Eigenschaftendialogfeld von Programmen verfügbar.
- **Programmkompatibilitätsmodul deaktivieren** Ist diese Richtlinie aktiviert, überprüft Windows beim Start von Anwendungen nicht mehr die Kompatibilitätsdatenbank auf bekannte Probleme. Dadurch verbessert sich zwar die Geschwindigkeit beim Start von Anwendungen, aber es können sich auch vermeidbare Stoppfehler oder Blue Screens ergeben, wenn inkompatible Anwendungen auf dem System ausgeführt werden und nicht richtig konfiguriert sind.
- **Programmkompatibilitäts-Assistenten deaktivieren** Wenn Sie diese Richtlinie aktivieren, laufen Legacyanwendungen ohne Switchback-Schutz. Switchback ist eine Kompatibilitätsfunktion, die allgemeine Kompatibilitätsprobleme beheben soll, die bei Legacyanwendungen auf den aktuellen Windows-Versionen bekanntermaßen auftreten. Dadurch kann sich zwar die Leistung etwas verbessern, aber Anwendungen mit Inkompatibilitäten reagieren vielleicht nicht mehr oder verursachen andere Probleme auf dem Computer.

Bereitstellen von Anwendungen für ausgewählte Benutzer oder für alle Benutzer

In Windows 8 ersetzt *Start* das herkömmliche Menüsystem. Desktop-Apps werden bei der Installation automatisch zu *Start* hinzugefügt und erhalten eine *Start*-Kachel. Eine *Start*-Kachel erleichtert den Start und die Verwaltung der App. Um die Verwaltungsfunktionen anzuzeigen, halten Sie die Kachel gedrückt oder klicken sie mit der rechten Maustaste an.

Welche Verwaltungsoptionen verfügbar sind, hängt von der Art der Kachel ab. Live-Kacheln können ihre Inhalte aktualisieren und diese Aktualisierungen lassen sich ein- und ausschalten. Einige Kacheln können in verschiedenen Größen angezeigt werden. Solche Kacheln können Sie vielleicht vergrößern oder verkleinern. Wenn eine Kachel nicht mehr auf *Start* angezeigt werden soll, können Sie die Option *Von "Start" lösen* wählen.

Nach der Installation sollten die meisten Desktop-Programme auf dem Startbildschirm über Kacheln verfügen und auf der *Alle Apps*-Leiste ihre Optionen anzeigen. Das ist so, weil die Verknüpfungen mit dem Programm für alle Benutzer im entsprechenden Unterordner des Ordners *Startmenü/Programme* (%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs) gespeichert werden, damit alle Benutzer, die sich auf einem System anmelden, Zugang zu dem Programm erhalten. Manche Programme fragen Sie bei der Installation, ob das Programm für alle Benutzer oder nur für den aktuell angemeldeten Benutzer installiert werden soll. Andere Programme installieren sich einfach nur für den aktuellen Benutzer.

Wenn das Installationsprogramm die Anwendung nur für den aktuellen Benutzer installiert und Sie möchten, dass auch andere Benutzer Zugang zur Anwendung erhalten, können Sie Folgendes tun:

- Melden Sie sich mit den Konten der Benutzer an, die Zugriff auf die Anwendung erhalten sollen, und installieren Sie die Anwendung jeweils neu, damit die Anwendung selektiv für bestimmte Benutzer zugänglich wird. Sie müssen die Installation erneut durchführen, wenn ein neues Benutzerkonto auf dem Computer eingerichtet wird und der betreffende Benutzer ebenfalls Zugang zur Anwendung erhalten soll.

- Wenn die Anwendung nicht darauf angewiesen ist, dass in der Registrierung benutzerbezogene Einstellungen vorgenommen werden, können Sie die Anwendung in manchen Fällen für alle Benutzer eines Computers verfügbar machen, indem Sie die entsprechenden Verknüpfungen im Ordner *Startmenü/Programme* für alle Benutzer speichern. Kopieren oder verschieben Sie die Programmverknüpfungen vom Profil des aktuellen Benutzers in den Ordner *Startmenü/Programme* für alle Benutzer.

Wenn Sie ein Programm für alle Benutzer eines Computers verfügbar machen möchten, können Sie die Verknüpfungen des Programms mit folgenden Schritten kopieren oder verschieben:

1. Wechseln Sie im Datei-Explorer zum Ordner *Programme* des momentan angemeldeten Benutzers. Dies ist ein ausgeblendeter Unterordner von `%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu`. Wenn die verborgenen Elemente nicht angezeigt werden, tippen oder klicken Sie im Datei-Explorer auf *Ansicht* und aktivieren in der Gruppe *Ein-/ausblenden* das Kontrollkästchen *Ausgeblendete Elemente*.
2. Klicken Sie im Ordner *Programme* mit der rechten Maustaste auf den Ordner für die Programmgruppe oder die Verknüpfung, die Sie bearbeiten wollen, oder halten Sie das entsprechende Symbol gedrückt, und wählen Sie den Befehl *Kopieren* oder *Ausschneiden*.
3. Wechseln Sie nun zum Ordner *Startmenü/Programme* für alle Benutzer. Dies ist ein ausgeblendeter Unterordner von `%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu`.
4. Tippen oder klicken Sie im Ordner *Programme* mit der rechten Maustaste auf einen leeren Bereich oder halten Sie die entsprechende Stelle gedrückt, und wählen Sie den Befehl *Einfügen*. Die Programmgruppe oder Verknüpfung müsste jetzt allen Benutzern des Computers zur Verfügung stehen.

Wenn ein Programm nicht für alle Benutzer des Computers, sondern nur für den aktuell angemeldeten Benutzer zugänglich sein soll, können Sie die Verknüpfungen des Programms folgendermaßen verschieben:

1. Wechseln Sie im Datei-Explorer zum Ordner *Startmenü* für alle Benutzer. Dies ist ein ausgeblendeter Unterordner von `%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu`.
2. Klicken Sie im Ordner *Programme* mit der rechten Maustaste auf den Ordner für die Programmgruppe oder die Programmverknüpfung, die Sie bearbeiten wollen, oder halten Sie das entsprechende Symbol gedrückt, und wählen Sie im Kontextmenü den Befehl *Ausschneiden*.
3. Wechseln Sie im Datei-Explorer zum Ordner *Programme* des momentan angemeldeten Benutzers. Dies ist ein ausgeblendeter Unterordner von `%UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu`.
4. Klicken Sie im Ordner *Programme* mit der rechten Maustaste auf einen leeren Bereich oder halten Sie die entsprechende Stelle gedrückt, und wählen Sie den Befehl *Einfügen*. Die Programmgruppe oder Verknüpfung dürfte jetzt nur noch dem momentan angemeldeten Benutzer zur Verfügung stehen.

HINWEIS

Die Verschiebung der Programmgruppe oder Verknüpfung verbirgt nur die Tatsache, dass das Programm auf dem Computer verfügbar ist, sie hindert andere Benutzer nicht daran, das Programm über das *Apps*-Suchfeld, das Dialogfeld *Ausführen* oder den Datei-Explorer zu starten.

Bereitstellen von Anwendungen mithilfe von Gruppenrichtlinien

Mithilfe von Gruppenrichtlinien können Sie Anwendungen für Benutzer im Netzwerk verfügbar machen. Wenn Sie die Gruppenrichtlinien zur Installation von Anwendungen verwenden, haben Sie zwei Alternativen:

- Weisen Sie Benutzern oder Computern die Anwendung zu. Wird eine Anwendung einem Computer zugewiesen, so wird sie beim nächsten Start des Computers installiert und ist für alle Benutzer des Computers verfügbar, sobald sich die Benutzer nach der Installation das nächste Mal anmelden. Wird eine Anwendung einem Benutzer zugewiesen, so wird sie vollständig installiert, sobald sich der Benutzer das nächste Mal am Netzwerk anmeldet. Eine zugewiesene Anwendung kann auch so konfiguriert werden, dass sie bei der ersten Verwendung installiert wird. Bei dieser Konfiguration wird die Anwendung durch Verknüpfungen auf dem Desktop oder im *Start*-Bildschirm des Benutzers zugänglich gemacht. Ist die Installation bei der ersten Verwendung konfiguriert, wird die Anwendung installiert, sobald der Benutzer die Anwendung durch Tippen oder Klicken auf die Verknüpfung starten will.
- Veröffentlichen Sie die Anwendung und stellen Sie sie zur Installation bereit. Wenn Sie eine Anwendung veröffentlichen, können Sie sie durch Aktivierung der Namenserverweiterung verfügbar machen. Ist die Aktivierung der Namenserverweiterung konfiguriert, wird das Programm installiert, sobald ein Benutzer eine Datei mit der entsprechenden Namenserverweiterung öffnet. Klickt oder tippt ein Benutzer beispielsweise eine Datei doppelt an, deren Namenserverweiterung *.doc* oder *.docx* lautet, könnte automatisch Microsoft Word installiert werden.

Sie können Anwendungen für Computer mit einem Windows Installer-Paket (eine *.msi*-Datei) und den Richtlinien unter *Computerkonfiguration\Richtlinien\Softwareeinstellungen\Softwareinstallation* automatisch bereitstellen. Anwendungen für Benutzer stellen Sie mit einem Windows Installer-Paket (*.msi*-Datei) und den Richtlinien in *Benutzerkonfiguration\Richtlinien\Softwareeinstellungen\Softwareinstallation* bereit. Die Schritte zur Bereitstellung von Anwendungen durch Gruppenrichtlinien sind folgende:

1. Damit das Windows Installer-Paket zugänglich ist, muss es in einem freigegebenen Verzeichnis liegen. Kopieren Sie also das betreffende Windows Installer-Paket (*.msi*-Datei) in ein freigegebenes Verzeichnis, das für die Zielgruppe zugänglich ist.
2. Öffnen Sie das Gruppenrichtlinienobjekt, in dem Sie die Anwendung bereitstellen möchten, im Gruppenrichtlinienverwaltungs-Editor. Nach der Bereitstellung ist die Anwendung für alle Clients verfügbar, für die das Gruppenrichtlinienobjekt gilt. Das bedeutet, dass die Anwendung für Benutzer und Computer in der betreffenden Domäne, in der Organisationseinheit oder im Standort verfügbar ist.
3. Erweitern Sie den Knoten *Computerkonfiguration\Richtlinien\Softwareeinstellungen* oder *Benutzerkonfiguration\Richtlinien\Softwareeinstellungen*, klicken Sie den Knoten *Softwareinstallation* mit der rechten Maustaste an oder halten Sie ihn gedrückt, zeigen Sie auf *Neu* und wählen Sie dann *Paket*.
4. Suchen Sie im Dialogfeld *Öffnen* das Windows Installer-Paket (*.msi*-Datei) der Anwendung und klicken Sie dann auf *Öffnen*. Anschließend können Sie unter den drei Bereitstellungsmethoden *Veröffentlicht*, *Zugewiesen* und *Erweitert* wählen.
5. Um das Programm zu veröffentlichen oder zuzuweisen, wählen Sie entsprechend *Veröffentlicht* oder *Zugewiesen* und tippen oder klicken dann auf *OK*. Wenn Sie eine Computerrichtlinie konfigurieren, ist das Programm beim nächsten Start des Computers verfügbar, für den das GPO gilt. Wenn Sie eine

Benutzerrichtlinie konfigurieren, ist das Programm für den Benutzer aus der Domäne, der Organisationseinheit oder dem Standort verfügbar, sobald er sich das nächste Mal anmeldet. Aktuell angemeldete Benutzer müssen sich abmelden und wieder anmelden, damit die Änderung wirksam wird.

6. Wenn Sie zusätzliche Bereitstellungsoptionen für das Programm festlegen möchten, wählen Sie *Erweitert*. Anschließend können Sie die Einstellungen nach Bedarf vornehmen.

Konfigurieren der Programmkompatibilität

Wenn Sie 16-Bit- oder MS-DOS-Programme installieren möchten, müssen Sie einige Besonderheiten berücksichtigen. Außerdem müssen Sie vielleicht die Kompatibilitätsoptionen anpassen, um ältere Programme ausführen zu können. Die folgenden Abschnitte beschreiben solche Situationen.

Besonderheiten bei der Installation von 16-Bit- und MS-DOS-Programmen

Viele 16-Bit- und MS-DOS-Programme, die keine direkten Hardwarezugriffe durchführen, können ohne Probleme unter Windows 8 installiert und benutzt werden. Allerdings verstehen die meisten 16-Bit- und MS-DOS-Programme keine langen Dateinamen. Um die Kompatibilität sicherzustellen, kümmert sich Windows 8 um die Zuordnung von langen und kurzen Dateinamen. Dadurch werden lange Dateinamen geschützt, falls sie durch ein 16-Bit- oder MS-DOS-Programm geändert werden. Außerdem darf man nicht vergessen, dass manche 16-Bit- und MS-DOS-Programme 16-Bit-Treiber brauchen, die unter Windows 8 nicht unterstützt werden. Folglich werden solche Programme nicht ausgeführt.

Die meisten vorhandenen 16-Bit- und MS-DOS-Programme wurden ursprünglich für Windows 3.0 oder Windows 3.1 geschrieben. Windows 8 führt diese alten Programme in einer virtuellen Maschine aus, die den erweiterten 386-Modus von Windows 3.0 und Windows 3.1 nachahmt. Anders als in älteren Windows-Versionen wird in Windows 8 jedes 16-Bit- oder MS-DOS-Programm auf einem Thread in derselben virtuellen Maschine ausgeführt. Das bedeutet, dass sich alle Programme denselben Speicherraum teilen, wenn Sie mehrere 16-Bit- oder MS-DOS-Programme ausführen. Wenn eines dieser Programme nicht mehr reagiert oder »hängt«, bedeutet dies leider meistens, dass die anderen Programme ebenfalls hängen.

Sie können verhindern, dass ein 16-Bit- oder MS-DOS-Programm andere Anwendungen stört, indem Sie jedes dieser Programme in einem separaten Speicherraum verwenden. Um das zu erreichen, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Programmverknüpfung oder halten Sie sie gedrückt, und wählen Sie dann *Eigenschaften*. Falls es noch keine Verknüpfung für das Programm gibt, erstellen Sie eine und öffnen dann das *Eigenschaften*-Dialogfeld der Verknüpfung.
2. Tippen oder klicken Sie auf der Registerkarte *Verknüpfung* auf die Schaltfläche *Erweitert*. Dadurch öffnet sich das Dialogfeld *Erweiterte Eigenschaften*.
3. Wählen Sie das Kontrollkästchen *In getrenntem Speicherbereich ausführen*.
4. Tippen oder klicken Sie auf die OK-Schaltflächen der beiden geöffneten Dialogfelder, um die Dialogfelder zu schließen und die Änderungen zu speichern.

HINWEIS Die Ausführung einer Anwendung in einem separaten Speicherbereich beansprucht zusätzlichen Speicher. Gewöhnlich werden Sie aber feststellen, dass die Anwendung schneller reagiert. Außerdem haben Sie dadurch den Vorteil, mehrere Instanzen der Anwendung verwenden zu können, solange alle Instanzen in ihren eigenen Speicherräumen ausgeführt werden.

TIPP Die Eingabeaufforderung (*Cmd.exe*) ist eine 32-Bit-Eingabeaufforderung. Wenn Sie eine 16-Bit-Eingabeaufforderung wünschen, wie sie in MS-DOS üblich war, können Sie *Command.com* verwenden. Geben Sie dazu im Dialogfeld *Ausführen* den Befehl **command** ein.

Erzwingen der Programmkompatibilität

Manche Programme lassen sich nicht auf Windows 8 installieren oder ausführen, obwohl sie auf früheren Versionen von Windows funktioniert haben. Wenn Sie versuchen, ein Programm zu installieren, das bekannte Kompatibilitätsprobleme hat, sollte Windows 8 eine entsprechende Warnung mit einem Hinweis auf das Kompatibilitätsproblem anzeigen. In den meisten Fällen werden Sie kein Programm installieren wollen, das Kompatibilitätsprobleme hat. Das gilt besonders für Systemhilfsprogramme, beispielsweise für ein Antivirusprogramm oder ein Datenträgerverwaltungsprogramm. Die Verwendung inkompatibler Systemhilfsprogramme kann ernste Probleme nach sich ziehen. Auch andere Arten von inkompatiblen Programmen können Probleme verursachen, wenn sie zum Beispiel in geschützte Bereiche des Datenträgers schreiben, die für das System reserviert sind.

Aber unabhängig davon können Sie ein Programm, das sich unter Windows 8 nicht installieren oder ausführen lässt, durch eine entsprechende Kompatibilitätseinstellung vielleicht doch noch verwendungsfähig machen. Windows 8 bietet zwei Mechanismen zur Verwaltung der Kompatibilitätseinstellungen. Sie können den Programmkompatibilitäts-Assistenten verwenden, oder Sie bearbeiten die Kompatibilitätseinstellungen direkt im Eigenschaftendialogfeld des Programms. Das Ergebnis ist dasselbe. Allerdings ist die Verwendung des Programmkompatibilitäts-Assistenten die einzige Methode zur Kompatibilitätseinstellung von Programmen, die sich auf freigegebenen Netzlaufwerken, auf CDs, DVDs und anderen Wechselmedien befinden. Unter dem Strich bleibt festzuhalten, dass Sie ein Programm, das sich nicht anders installieren und ausführen lässt, manchmal unter Verwendung des Programmkompatibilitäts-Assistenten installieren und ausführen müssen.

Verwenden des Programmkompatibilitäts-Assistenten

Sie können nur Kompatibilitätseinstellungen für Programme konfigurieren, die Sie bereits installiert haben. Für die Programme, die im Betriebssystem enthalten sind, können Sie keine Kompatibilitätseinstellungen konfigurieren. Gehen Sie folgendermaßen vor, wenn Sie versuchen wollen, Kompatibilitätsprobleme automatisch vom Programmkompatibilitäts-Assistenten erkennen zu lassen.

1. Suchen Sie die Programmverknüpfung heraus. Klicken Sie mit der rechten Maustaste auf die Programmverknüpfung oder halten Sie sie gedrückt, und wählen Sie den Befehl *Behandeln von Kompatibilitätsproblemen*. Daraufhin wird die Problembehandlung bei der Programmkompatibilität gestartet (Abbildung 8.2).
2. Der Assistent versucht, Kompatibilitätsprobleme automatisch zu erkennen. Sie können das Programm, das Sie untersuchen, versuchsweise mit den empfohlenen Einstellungen ausführen, indem Sie auf *Empfohlene Einstellungen testen* tippen oder klicken. Sehen Sie sich anschließend an, welche Einstellungen angewendet werden, und tippen oder klicken Sie auf *Programm testen*.

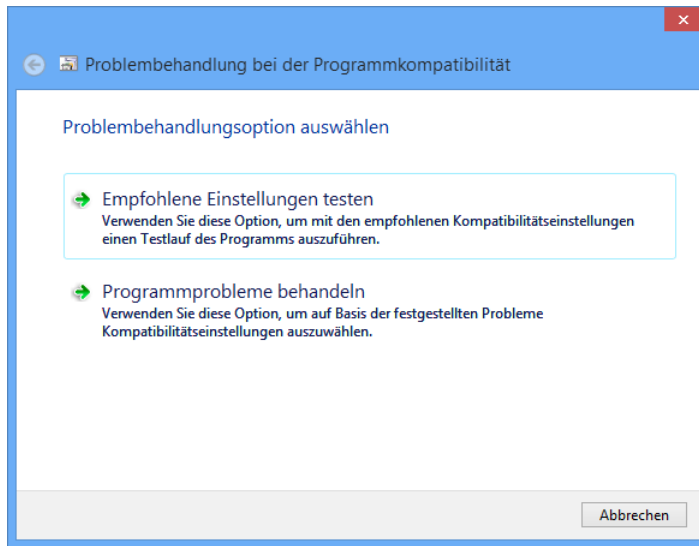


Abbildung 8.2 Untersuchen von Kompatibilitätsproblemen

3. Warten Sie, bis das Programm ausgeführt worden ist, und tippen oder klicken Sie auf *Weiter*. Sie haben jetzt folgende Möglichkeiten:
 - Tippen oder klicken Sie auf *Ja, diese Einstellungen für dieses Programm speichern*, wenn die Kompatibilitätseinstellungen das Problem beseitigen und Sie die Einstellungen beibehalten wollen.
 - Tippen oder klicken Sie auf *Nein, mit anderen Einstellungen wiederholen*, wenn das Problem durch die Kompatibilitätseinstellungen nicht beseitigt wurde und Sie den Prozess noch einmal ganz von vorne beginnen wollen.
 - Tippen oder klicken Sie auf *Nein, Problem an Microsoft senden und online nach einer Lösung suchen*, wenn die Kompatibilitätseinstellungen das Problem nicht beseitigt haben und Sie online nach einer Lösung suchen möchten.
 - Tippen oder klicken Sie auf *Abbrechen*, wenn Sie die Kompatibilitätseinstellungen verwerfen und den Assistenten verlassen wollen.

Gehen Sie folgendermaßen vor, um eine erweiterte Problembehandlung einzuleiten und im Programmkompatibilitäts-Assistenten festzulegen, welche Kompatibilitätseinstellungen verwendet werden sollen:

1. Suchen Sie die Programmverknüpfung im Datei-Explorer heraus. Programmverknüpfungen liegen unter `%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs`. Klicken Sie mit der rechten Maustaste auf die Programmverknüpfung oder halten Sie sie gedrückt, und wählen Sie den Befehl *Behandeln von Kompatibilitätsproblemen*. Dadurch wird der Programmkompatibilitäts-Assistent gestartet.
2. Tippen oder klicken Sie auf *Programmprobleme behandeln*. Geben Sie auf der Seite *Welche Probleme sind Ihnen aufgefallen?* an, welche Probleme Sie beobachtet haben. Welche Assistentenseiten in den nächsten Schritten nach dem Antippen oder Anklicken von *Weiter* angezeigt werden, hängt davon ab, welche Kontrollkästchen Sie hier auswählen. Verfügbare Einstellungen sind:
 - **Das Programm war in früheren Versionen von Windows funktionsfähig, kann nun aber nicht mehr installiert oder ausgeführt werden** Wenn Sie dieses Kontrollkästchen aktivieren, werden Sie auf einer der nächsten Assistentenseiten gefragt, unter welcher Version das Programm funk-

tioniert hat. Weil Ihre Angabe den Kompatibilitätsmodus festlegt, sollten Sie das Betriebssystem wählen, für das dieses Programm entwickelt wurde. Wenn Windows 8 das Programm ausführt, simuliert es die Umgebung des angegebenen Betriebssystems.

- **Das Programm wird zwar geöffnet, aber nicht ordnungsgemäß angezeigt** Wenn Sie versuchen, ein Spiel, ein Lernprogramm oder ein anderes Programm auszuführen, das bestimmte Anzeigeeinstellungen voraussetzt, zum Beispiel ein Programm, das für Microsoft Windows 98 entwickelt wurde, können Sie dieses Kontrollkästchen aktivieren und anschließend angeben, welche Art von Anzeigeproblem auftritt. Ihre Angabe schränkt die Grafikanzeige ein: Wenn Sie 256 Farben, die Bildschirmauflösung 640 × 480 oder beides benutzen, schränkt Windows die Grafikanzeige ein. Das hilft manchmal bei Programmen, die bei höheren Bildschirmauflösungen und größerer Farbtiefe nicht laufen. Sie können auch einstellen, dass Designs, Desktopgestaltung (die spezielle optische Effekte auf dem Desktop ermöglicht) und Anzeigeskalierung für hohe DPI-Werte deaktiviert werden.
 - **Für das Programm sind zusätzliche Berechtigungen erforderlich** Wenn Sie dieses Kontrollkästchen aktivieren, wird das Programm so konfiguriert, dass es mit Administratorprivilegien läuft.
 - **Mein Problem wird nicht aufgeführt** Wenn Sie dieses Kontrollkästchen aktivieren, zeigt der Assistent optionale Seiten für das Betriebssystem und die Auswahl von Anzeigeproblemen an. Außerdem richtet der Assistent das Programm so ein, dass es als Administrator ausgeführt wird. Wenn Sie diese Option verwenden, hat das letztlich dieselbe Wirkung, als hätten Sie alle drei anderen Kontrollkästchen aktiviert.
3. Sehen Sie sich an, welche Kompatibilitätseinstellungen angewendet werden. Wenn Sie diese Einstellungen doch nicht verwenden wollen, können Sie auf *Abbrechen* tippen oder klicken und den Vorgang wiederholen, um andere Optionen auszuwählen. Wollen Sie diese Einstellungen anwenden, brauchen Sie nur auf *Programm starten* zu tippen oder zu klicken; der Assistent startet das Programm daraufhin mit den Kompatibilitätseinstellungen, die Sie angegeben haben.
4. Warten Sie, bis das Programm ausgeführt wurde, und tippen oder klicken Sie dann auf *Weiter*. Sie werden nun gefragt, ob das Problem durch die Änderungen beseitigt wurde. Sie haben jetzt folgende Möglichkeiten:
- Tippen oder klicken Sie auf *Ja, diese Einstellungen für dieses Programm speichern*, wenn die Kompatibilitätseinstellungen das Problem beseitigt haben und Sie die Einstellungen beibehalten wollen.
 - Tippen oder klicken Sie auf *Nein, mit anderen Einstellungen wiederholen*, wenn das Problem durch die Kompatibilitätseinstellungen nicht beseitigt wurde und Sie den Prozess noch einmal ganz von vorne beginnen wollen.
 - Tippen oder klicken Sie auf *Nein, Problem an Microsoft senden und online nach einer Lösung suchen*, wenn die Kompatibilitätseinstellungen das Problem nicht beseitigt haben und Sie online nach einer Lösung suchen möchten.
 - Tippen oder klicken Sie auf *Abbrechen*, wenn Sie die Kompatibilitätseinstellungen verwerfen und den Assistenten verlassen wollen.

HINWEIS Wenn Sie alternative Anzeigeeinstellungen für ein Programm konfigurieren, schaltet dieses Programm jedes Mal, wenn Sie es starten, in den alternativen Anzeigemodus. Die ursprünglichen Anzeigeeinstellungen werden wiederhergestellt, sobald Sie das Programm beenden.

Direktes Einstellen der Kompatibilitätsoptionen

Wenn ein Programm, das Sie bereits installiert haben, nicht richtig funktioniert, möchten Sie die Kompatibilitätseinstellungen vielleicht direkt vornehmen und nicht mit dem Assistenten. Gehen Sie folgendermaßen vor.

1. Klicken Sie mit der rechten Maustaste auf das Verknüpfungssymbol des Programms oder halten Sie es gedrückt, und wählen Sie den Befehl *Eigenschaften*.
2. Tippen oder klicken Sie im Eigenschaftendialogfeld auf die Registerkarte *Kompatibilität*. Alle Optionen, die Sie hier auswählen, werden für den momentan angemeldeten Benutzer auf die Anwendungsverknüpfung angewendet. Wenn die Einstellungen für alle Benutzer des Computers und unabhängig davon gelten sollen, über welche Verknüpfung das Programm gestartet wird, müssen Sie auf *Einstellungen für alle Benutzer ändern* tippen oder klicken. Daraufhin öffnet sich das Eigenschaftendialogfeld für die *.exe*-Datei der Anwendung. Wählen Sie hier die gewünschten Kompatibilitätseinstellungen, die für alle Benutzer gelten sollen, sie sich am Computer anmelden.

HINWEIS Programme, die zum Betriebssystem Windows 8 gehören, können nicht im Kompatibilitätsmodus ausgeführt werden. Deswegen sind die Optionen auf der Registerkarte *Kompatibilität* bei solchen Programmen auch nicht verfügbar.

3. Wählen Sie das Kontrollkästchen *Programm im Kompatibilitätsmodus ausführen für* und wählen Sie dann das Betriebssystem aus der Liste aus, für das die Anwendung entwickelt wurde.
4. Sofern erforderlich, schränken Sie die Grafikdarstellung des Programms mit den Optionen aus dem Bereich *Einstellungen* ein. Wählen Sie nach Bedarf 256 Farben, die Bildschirmauflösung 640 × 480 oder beides.
5. Wenn es erforderlich ist, können Sie auch Designs, die Desktopgestaltung und hohe DPI-Werte deaktivieren.
6. Tippen oder klicken Sie auf *OK*. Starten Sie das Programm, indem Sie doppelt auf die Verknüpfung tippen oder klicken, und probieren Sie die Kompatibilitätseinstellungen aus. Wenn sich bei der Ausführung des Programms immer noch Probleme ergeben, müssen Sie die Kompatibilitätseinstellungen vielleicht noch einmal ändern.

Verwalten von installierten und laufenden Programmen

Windows 8 bietet einige Verwaltungsprogramme für Anwendungen. Dazu gehören:

- **Task-Manager** Bietet Optionen für die Anzeige und Verwaltung von ausgeführten Programmen sowie Optionen zur Anzeige der Ressourcenbelegung und der Leistung.
- **Programme** Zeigt die installierten Programme an, unterstützt Sie beim Hinzufügen und Entfernen von Programmen, zeigt installierte Updates an und so weiter.
- **Standardprogramme** Unterstützt Sie bei der Verwaltung und Konfiguration von globalen Standardprogrammen für den Computer und von persönlichen Standardprogrammen für die einzelnen Benutzer, bei den Einstellungen für die automatische Wiedergabe für Multimedia und bei der Verknüpfung von Dateitypen mit Anwendungen.
- **Windows-Funktionen** Bietet die Anzeige und Verwaltung der Windows-Komponenten, die auf dem Computer installiert sind.

- **Assoc** Hilft Ihnen beim Anzeigen und Verwalten von Dateitypverknüpfungen.
- **Ftype** Hilft Ihnen beim Anzeigen und Verwalten von Dateitypdefinitionen.

Diese Tools und die zugehörigen Konfigurationsoptionen werden in den nächsten Abschnitten genauer beschrieben.

Verwalten aktuell ausgeführter Programme

In Windows 8 können Sie die Programme, die aktuell auf einem Computer ausgeführt werden, mit dem Task-Manager anzeigen und bearbeiten. Sie starten den Task-Manager, indem Sie die Tastenkombination STRG+ALT+ENTF drücken und dann *Task-Manager* auswählen. Oder tippen oder klicken Sie in die linke untere Ecke des Bildschirms und wählen Sie dann im Kontextmenü den *Task-Manager* aus.

Standardmäßig zeigt der Task-Manager eine einfache Liste der laufenden Anwendungen an (Abbildung 8.3). Wenn Sie eine Anwendung aus der Liste antippen oder anklicken, können Sie sie verwalten. Um eine Anwendung zu beenden, weil sie zum Beispiel nicht mehr reagiert, tippen oder klicken Sie erst in der Taskliste auf die Anwendung und dann auf *Task beenden*. Um andere Verwaltungsoptionen anzuzeigen, klicken Sie die Anwendung in der Taskliste mit der rechten Maustaste an oder halten sie gedrückt.

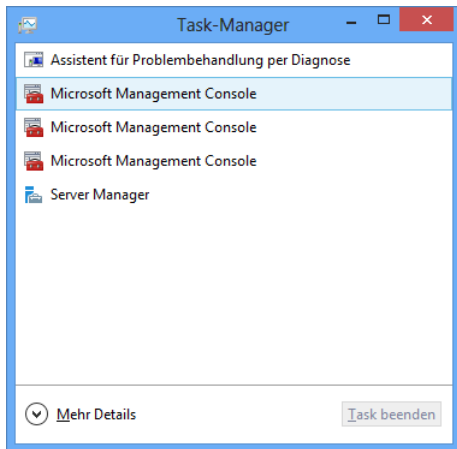


Abbildung 8.3 In der einfachen Listendarstellung gibt Ihnen der Task-Manager einen schnellen Überblick über die laufenden Anwendungen

Wenn Sie in der Übersichtsdarstellung arbeiten, können Sie auf *Mehr Details* tippen oder klicken, um den Task-Manager ganz zu öffnen. Dann sehen Sie ausführliche Angaben über die laufenden Anwendungen und Prozesse (Abbildung 8.4). Die Registerkarte *Prozesse* listet alle Anwendungen und Prozesse auf, die auf dem Computer laufen. Bei den Einträgen unter der Überschrift *Apps* handelt es sich um Anwendungen, die Sie gestartet haben. Prozesse, die von Windows im Hintergrund ausgeführt werden, werden unter *Hintergrundprozesse* aufgelistet. Alle anderen Prozesse, die auf dem Computer laufen, werden unter *Windows-Prozesse* aufgelistet.

Jede Anwendung und jeder Prozess wird mit Namen, Status, Prozessorauslastung, Speicherbelegung, Festplattenverwendung und Netzwerkverwendung aufgeführt. Ein leeres Statusfeld bedeutet, dass sich die Anwendung oder der Prozess in einem normalen Zustand befindet. Wie bei der Kurzübersicht können Sie eine Anwendung oder einen laufenden Prozess beenden, indem Sie die Anwendung oder den Prozess in der Taskliste antippen oder anklicken und dann auf *Task beenden* tippen oder klicken.

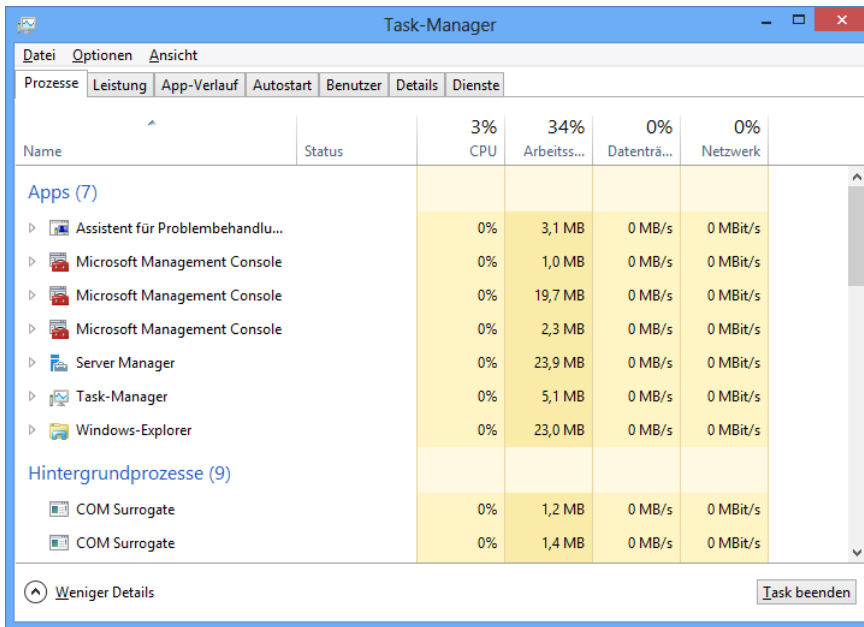


Abbildung 8.4 In der detaillierten Darstellung zeigt der Task-Manager einen ausführlichen Überblick über die laufenden Anwendungen und Prozesse

Durch doppeltes Antippen oder Anklicken einer Anwendung oder eines Prozesses wird das dazugehörige Fenster oder der Prozess angezeigt. Um zusätzliche Verwaltungsoptionen anzuzeigen, klicken Sie die Anwendung oder den Prozess in der Taskliste mit der rechten Maustaste an oder halten den Listeneintrag gedrückt. Unter anderem stehen Befehle wie *Dateipfad öffnen* (öffnet den Ordner, in dem die ausführbare Datei des Prozesses liegt, im Datei-Explorer), *Abbilddatei erstellen* (erstellt eine Speicherabbilddatei des ausgewählten Prozesses), *Zu Details wechseln* (öffnet die Registerkarte *Details* mit dem ausgewählten Prozess) und *Eigenschaften* (öffnet das Eigenschaftendialogfeld für die ausführbare Datei) zur Verfügung.

Verwalten, Reparieren und Deinstallieren von Programmen

Windows 8 betrachtet jedes Programm, das Sie auf einem Computer installiert oder für eine Netzwerkinstallation verfügbar gemacht haben, als ein installiertes Programm. In Windows XP und älteren Windows-Versionen haben Sie Programme mit dem Programm Software aus der Systemsteuerung installiert und verwaltet. In Windows 8 installieren Sie Anwendungen mit den Setupprogrammen der Anwendungen und verwalten sie auf der Seite *Programme und Features* der Systemsteuerung.

Sie können die Seite *Programme und Features* auf folgende Weise zum Anzeigen, Entfernen oder Reparieren von installierten Programmen verwenden:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Programme* und dann auf *Programme und Features*. Nun sollten Sie eine Liste der installierten Programme sehen.
2. Klicken Sie in der Spalte *Name* mit der rechten Maustaste auf das Programm, das Sie bearbeiten möchten, oder halten Sie es gedrückt. Welche Optionen verfügbar sind, hängt von dem Programm ab, mit dem Sie arbeiten:

- *Deinstallieren* zur Deinstallation des Programms
- *Deinstallieren/ändern* zur Änderung oder Deinstallation des Programms
- *Ändern* zur Änderung der Programmkonfiguration
- *Reparieren* zur Reparatur des Programms (sofern verfügbar)

Wenn Sie Programme deinstallieren, sollten Sie folgende Punkte beachten:

- Windows warnt Sie, wenn Sie versuchen, ein Programm zu deinstallieren, während andere Benutzer angemeldet sind. Im Allgemeinen sollten Sie sicherstellen, dass alle anderen Benutzer abgemeldet sind, bevor Sie Programme deinstallieren. Andernfalls kann es passieren, dass andere Benutzer Daten verlieren oder mit anderen Problemen konfrontiert werden.
- Windows erlaubt Ihnen nur die Programme zu deinstallieren, die mit einem Windows-kompatiblen Setupprogramm installiert wurden. Die meisten Anwendungen verwenden zwar ein Setupprogramm, das auf InstallShield, Wise Install oder Windows Installer zurückgreift, aber ältere Programme verwenden unter Umständen ein separates Dienstprogramm für die Deinstallation. Manche ältere Programme kopieren einfach ihre Datendateien in einen Programmordner. In einem solchen Fall müssen Sie das Programm deinstallieren, indem Sie den entsprechenden Ordner löschen.
- Viele Deinstallationsprogramme lassen versehentlich oder absichtlich Daten zurück. Folglich finden Sie oft Ordner für diese Anwendungen im Ordner *Program Files*. Sie könnten diese Ordner natürlich löschen, aber möglicherweise enthalten sie wichtige Datendateien oder benutzerdefinierte Einstellungen, die wiederverwendet werden, wenn Sie das Programm später erneut installieren.
- Gelegentlich schlägt der Deinstallationsprozess fehl. Solche Probleme lassen sich oft dadurch beseitigen, dass Sie das Deinstallationsprogramm einfach noch einmal ausführen. Manchmal müssen Sie auch von Hand aufräumen, nachdem der Deinstallationsprozess abgeschlossen ist. Dabei müssen Sie vielleicht Programmdateien entfernen und Überbleibsel des Programms in der Windows-Registrierung löschen. Ein Programm namens Fixit-portable hilft Ihnen dabei, die Registrierung aufzuräumen. Weitere Informationen zu diesem Dienstprogramm und eine Downloadmöglichkeit für die Software finden Sie unter http://support.microsoft.com/mats/Program_Install_and_Uninstall/. Wählen Sie auf der Microsoft-Website nicht *Jetzt ausführen*, sondern klicken Sie auf *Erweitert* und dann auf *Download*, um die ausführbare Datei zu speichern. Starten Sie die ausführbare Datei nach dem Herunterladen und folgen Sie der Anleitung, um das Programm zu installieren.

Festlegen der Standardprogramme

Durch Standardprogramme wird festgelegt, welche Programme für welche Dateiart verwendet werden und wie Windows mit Dateien auf CDs, DVDs und portablen Geräten umgeht. Sie konfigurieren Standardprogramme auf der Basis der Dateiarten, die von diesen Programmen bearbeitet werden können. Die Wahl zum Standardprogramm kann sich auf den aktuell angemeldeten Benutzer beschränken oder für alle Benutzer des Computers gelten. Einstellungen für einzelne Benutzer haben Vorrang vor globalen Einstellungen. Wenn Sie zum Beispiel Windows Media Player als allgemeines Standardprogramm für alle Dateiarten verwenden, die das Programm unterstützt, würden alle Benutzer des Computers zum Abspielen der Audio- und Videodateien, die das Programm unterstützt, Windows Media Player verwenden. Möchte ein Benutzer stattdessen Apple iTunes als Standardabspieler für Audio- und Videodateien verwenden, können Sie iTunes als seinen Standardabspieler für die Mediendateien einrichten, die das Programm unterstützt.

Mit folgenden Schritten können Sie allgemeine Standardprogramme für alle Benutzer eines Computers einrichten:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Programme*, dann auf *Standardprogramme* und schließlich auf *Programmmzugriff und Computerstandards festlegen*. Daraufhin öffnet sich das Dialogfeld aus Abbildung 8.5.

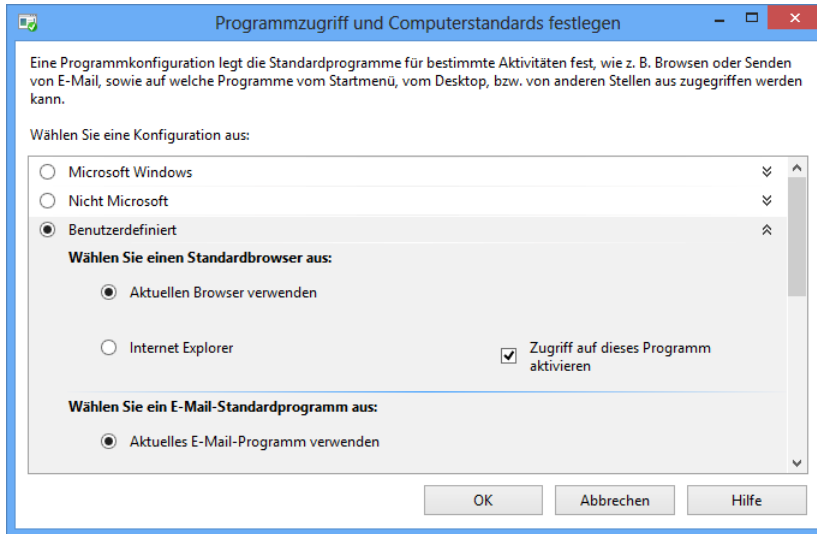


Abbildung 8.5 Festlegen einer globalen Standardkonfiguration

2. Wählen Sie eine der folgenden Konfigurationen aus:
 - **Microsoft Windows** Legt die aktuell installierten Windows-Programme als Standard für das Browsen im Web, den Versand von E-Mails, die Wiedergabe von Mediendateien und so weiter fest.
 - **Nicht Microsoft** Legt die aktuell installierten Programme als Standard für das Browsen im Web, den Versand von E-Mails, die Wiedergabe von Mediendateien und so weiter fest.
 - **Benutzerdefiniert** Ermöglicht Ihnen die Auswahl von Standardprogrammen für das Browsen im Web, den Versand von E-Mails, die Wiedergabe von Mediendateien und so weiter.
3. Tippen oder klicken Sie auf **OK**, um die Einstellungen zu speichern.

Um die allgemeinen Vorgaben zu ändern, können Sie für einzelne Benutzer andere Standardprogramme festlegen. Gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Programme*, dann auf *Standardprogramme* und schließlich auf *Standardprogramme festlegen*.
2. Wählen Sie aus der Liste *Programme* ein Programm aus, mit dem Sie arbeiten möchten.
3. Wenn Sie das Programm als Standardprogramm für alle Dateiformate verwenden möchten, die es unterstützt, tippen oder klicken Sie auf *Dieses Programm als Standard festlegen*.
4. Wenn Sie das Programm nur für bestimmte Dateiformate und Protokolle verwenden möchten, tippen oder klicken Sie auf *Standards für dieses Programm auswählen*. Wählen Sie die Dateinamenserweiterungen aus, für die das Programm als Standardprogramm verwendet werden soll, und tippen oder klicken Sie dann auf *Speichern*.

Verwalten des Befehlspfads

Windows braucht den Befehlspfad, um ausführbare Dateien zu finden. Sie können sich den aktuellen Befehlspfad für ausführbare Dateien mit dem Befehl *Path* ansehen. Geben Sie in einer Eingabeaufforderung **path** in eine neue Zeile ein und drücken Sie die EINGABETASTE. In einer Windows PowerShell-Konsole müssen Sie **\$env:path** in einer neuen Zeile eingeben und die EINGABETASTE drücken. Wie Sie in beiden Fällen in der Ausgabe sehen, trennt Windows die einzelnen Pfade durch ein Semikolon (;), um kenntlich zu machen, wo ein Dateipfad endet und der nächste beginnt.

Der Befehlspfad wird bei der Anmeldung festgelegt. Dabei werden System- und Benutzerumgebungsvariablen ausgewertet. Der Pfad, der in der Systemvariablen *PATH* definiert ist, legt den Basispfad fest. Und der Pfad, der in der Benutzervariablen *PATH* definiert ist, wird mit folgender Syntax an den Basispfad angehängt:

```
%PATH%;WeiterePfade
```

Hier weist *%PATH%* Windows an, die aktuellen Systempfade einzufügen, und *WeiterePfade* steht für die zusätzlichen benutzerspezifischen Pfade, die verwendet werden sollen.

ACHTUNG Ein falsch eingestellter Pfad kann schwere Probleme verursachen. Sie sollten einen geänderten Befehlspfad immer testen, bevor Sie ihn in einer Produktivumgebung verwenden. Der Befehlspfad wird während der Anmeldung festgelegt. Daher müssen Sie sich ab- und wieder anmelden, um die Auswirkungen des geänderten Pfads zu beobachten.

Vergessen Sie nicht, welche Suchreihenfolge Windows benutzt. Pfade werden in der Reihenfolge durchsucht, in der sie aufgeführt sind. Der letzte Pfad aus der Benutzervariablen *PATH* wird also als letzter durchsucht. Das kann manchmal dazu führen, dass sich die Ausführung Ihrer Programme und Skripts verzögert. Soll Windows Ihre Programme und Skripts schneller finden, ist es unter Umständen sinnvoll, den entsprechenden Pfad weiter vorne in der Suchreihenfolge einzutragen.

Passen Sie auf, wenn Sie den Befehlspfad festlegen. Es ist schnell passiert, dass Sie versehentlich sämtliche Pfaddaten überschreiben. Vergessen Sie beispielsweise, *%Path%* anzugeben, wenn Sie den Benutzerpfad festlegen, löschen Sie alle anderen Pfadinformationen. Sie können sicherstellen, dass sich der Befehlspfad wiederherstellen lässt, indem Sie ihn in eine Datei kopieren.

- Wenn Sie in der Eingabeaufforderung arbeiten, können Sie den aktuellen Befehlspfad in eine Datei schreiben, indem Sie **path > orig_path.txt** eingeben. Denken Sie daran, dass Sie nicht in geschützte Systemspeicherorte schreiben können, wenn Sie eine Standardeingabeaufforderung statt einer Administratoreingabeaufforderung verwenden. In diesem Fall können Sie in ein Unterverzeichnis schreiben, auf das Sie Zugriff haben, oder in Ihr eigenes Profil. Wenn Sie einfach **path** eingeben, schreiben Sie den Befehlspfad in das Eingabeaufforderungsfenster.
- Wenn Sie in der PowerShell-Konsole arbeiten, können Sie den aktuellen Befehlspfad in eine Datei schreiben, indem Sie den Befehl **\$env:path > orig_path.txt** verwenden. Wenn Sie eine Standardkonsole statt einer Administratorkonsole verwenden, können Sie nicht in geschützte Systemspeicherorte schreiben. In diesem Fall können Sie in ein Unterverzeichnis schreiben, auf das Sie Zugriff haben, oder in Ihr eigenes Profil. Wenn Sie einfach **\$env:path** eingeben, wird der Befehlspfad im PowerShell-Fenster ausgegeben.

In der Eingabeaufforderung oder dem PowerShell-Fenster können Sie den Befehlspfad mit dem Dienstprogramm *Setx.exe* bearbeiten. Außerdem können Sie den Befehlspfad folgendermaßen anpassen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie auf der Seite *System* auf *Einstellungen ändern* oder im linken Fensterabschnitt auf *Erweiterte Systemeinstellungen*.
3. Tippen oder klicken Sie auf der Registerkarte *Erweitert* des Dialogfelds *Systemeigenschaften* auf die Schaltfläche *Umgebungsvariablen*.
4. Wählen Sie in der Liste *Systemvariablen* die Variable *PATH* aus. Tippen oder klicken Sie unter *Systemvariablen* auf die Schaltfläche *Bearbeiten*.
5. Der Wert der Variablen *PATH* ist standardmäßig ausgewählt. Drücken Sie die Taste PFEIL-NACH-RECHTS, ohne eine andere Taste zu drücken. Damit müsste die Auswahl aufgehoben werden und der Cursor am Ende des Variablenwerts stehen.
6. Tippen Sie ein Semikolon und dann den gewünschten Pfad ein. Wiederholen Sie diesen Schritt so oft wie nötig und klicken Sie schließlich dreimal auf *OK*.

In den Gruppenrichtlinien können Sie ein Einstellungselement verwenden, um den Befehlspfad anzupassen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und dann *Umgebung* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Windows-Einstellungen* erweitern und *Umgebung* auswählen.
2. Halten Sie den Knoten *Umgebung* gedrückt oder klicken Sie ihn mit der rechten Maustaste an, und wählen Sie im Kontextmenü den Befehl *Neu/Umgebungsvariable*. Daraufhin öffnet sich das Eigenschaftendialogfeld für die neue Umgebungsvariable.
3. Wählen Sie in der Liste *Aktion* den Eintrag *Aktualisieren* aus, wenn Sie die Variable *PATH* aktualisieren wollen, oder den Eintrag *Ersetzen*, um die Variable *PATH* zu löschen und dann neu zu erstellen. Wählen Sie anschließend die Option *Benutzervariable* aus.
4. Geben Sie im Feld *Name* den Variablennamen **Path** ein und im Feld *Wert* den Variablenwert. Gewöhnlich geben Sie dabei erst **%Path%** ein, gefolgt von den Pfaden, die Sie hinzufügen wollen. Trennen Sie die Pfade jeweils durch Semikolons. Ist auf den betreffenden Computern bereits eine *PATH*-Benutzervariable definiert, müssen Sie die entsprechenden Pfade mit aufnehmen, damit diese Pfade erhalten bleiben.
5. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. In den meisten Fällen werden Sie die Variable *PATH* nur einmal erstellen wollen (damit die Gruppenrichtlinien die Variable nicht jedes Mal neu erstellen, wenn die Richtlinie aktualisiert wird). Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmalig anwenden*.
6. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

ACHTUNG Ein falsch konfigurierter Pfad kann schwere Probleme verursachen. Bevor Sie einen aktualisierten Pfad auf mehreren Computern bereitstellen, sollten Sie die Konfiguration testen. Dazu können Sie beispielsweise ein Gruppenrichtlinienobjekt in Active Directory anlegen, das nur auf einen isolierten Testcomputer angewendet wird. Erstellen Sie dann ein Einstellungselement für dieses Gruppenrichtlinienobjekt und warten Sie, bis die Richtlinie aktualisiert wird, oder wenden Sie die Richtlinie mit GPOupdate sofort an. Wenn Sie am betreffenden Computer angemeldet sind, müssen Sie sich ab- und dann wieder anmelden, bevor Sie die Ergebnisse überprüfen können.

Verwalten von Dateierweiterungen und Dateiverknüpfungen

Dateierweiterungen und Dateiverknüpfungen sind ebenfalls wichtige Elemente bei der Entscheidung, wie Programme ausgeführt werden. Welche Dateitypen Windows als ausführbare Dateien einstuft, wird durch die Dateierweiterungen für ausführbare Dateien festgelegt. Dateierweiterungen ermöglichen es den Benutzern, einen Befehl allein durch Angabe des Befehlsnamens auszuführen. Und Dateiverknüpfungen ermöglichen es den Benutzern, doppelt auf eine Datei zu tippen oder zu klicken, damit diese Datei automatisch in der passenden Anwendung geöffnet wird. Es werden zwei Dateierweiterungstypen benutzt:

- **Dateierweiterungen für ausführbare Dateien** Ausführbare Dateien (engl. executable) werden über die Umgebungsvariable `%PATHEXT%` definiert. Sie können im Dialogfeld *Umgebungsvariablen* oder mit Einstellungselementen von Gruppenrichtlinien festgelegt werden, ähnlich wie die Variable `PATH`. Sie können sich die aktuellen Einstellungen ansehen, indem Sie in der Befehlszeile `set pathext` beziehungsweise in der PowerShell-Eingabeaufforderung `$env:pathext` eingeben. Der Standard ist `PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC`. Dank dieser Einstellung weiß die Befehlszeile, welche Dateien ausführbare Dateien sind und welche nicht. Daher brauchen Sie in der Befehlszeile keine Dateierweiterung anzugeben.
- **Dateierweiterungen für Anwendungen** Dateierweiterungen für Anwendungen werden auch als Dateiverknüpfungen bezeichnet. Dateiverknüpfungen machen es möglich, Argumente an ausführbare Dateien zu übergeben und Dokumente, Arbeitsblätter oder andere Anwendungsdateien durch doppeltes Antippen oder Anklicken des Dateisymbols zu öffnen. Jede bekannte Erweiterung in einem System hat eine Dateiverknüpfung, die Sie sich in der Eingabeaufforderung ansehen können, indem Sie `assoc` eingeben, gefolgt von der Erweiterung, beispielsweise `assoc .doc` oder `assoc .docx`. Jede Dateiverknüpfung gibt wiederum den Dateityp für die Dateierweiterung an. Das können Sie sich ansehen, indem Sie in einer Eingabeaufforderung `ftype` mit der Dateiverknüpfung eingeben, also `ftype Word.Document.8` oder `ftype Word.Document.12`.

HINWEIS `Assoc` und `Ftype` sind interne Befehle der Eingabeaufforderung (`Cmd.exe`). Wenn Sie `Assoc` in PowerShell verwenden wollen, müssen Sie `cmd /c assoc` eingeben, gefolgt von der Erweiterung, zum Beispiel `cmd /c assoc .doc`. Und wenn Sie `Ftype` in PowerShell ausführen wollen, müssen Sie entsprechend `cmd /c ftype` eingeben, gefolgt von der Dateiverknüpfung, also `cmd /c ftype Word.Document.8`.

Bei ausführbaren Dateien bestimmt die Reihenfolge der Dateierweiterungen in der Variablen `%PATH-EXT%` die Suchreihenfolge, die von der Befehlszeile für jedes Verzeichnis individuell ausgewertet wird. Enthält ein bestimmtes Verzeichnis im Befehlspfad also mehrere ausführbare Dateien, die zum angegebenen Befehlsnamen passen, wird eine `.com`-Datei vor einer `.exe`-Datei ausgeführt und so weiter.

Jede bekannte Dateierweiterung in einem System hat eine entsprechende Dateiverknüpfung und einen entsprechenden Dateityp. Das gilt sogar bei Erweiterungen für ausführbare Dateien. In manchen Fällen ist der Dateityp der Erweiterungstext ohne den Punkt, gefolgt vom Schlüsselwort *file*, zum Beispiel `cmd-file`, `exefile` oder `batfile`. Die Dateiverknüpfung gibt in diesem Fall an, dass das erste Argument, das über-

geben wird, der Befehlsname ist, und dass weitere Argumente an die Anwendung weitergeleitet werden sollen. Tippen Sie beispielsweise **assoc .exe** ein, um sich die Dateiverknüpfungen für ausführbare Dateien vom Typ **.exe** anzusehen, müssen Sie anschließend **ftype exe file** eingeben. Wie sich zeigt, ist die Dateiverknüpfung folgendermaßen konfiguriert:

```
exefile="%1" %*
```

Wenn Sie also eine **.exe**-Datei ausführen, weiß Windows, dass der erste Wert der Befehl ist, den Sie ausführen wollen, und alles andere Argumente sind, die einfach weitergeleitet werden sollen.

Dateiverknüpfungen und -typen werden in der Windows-Registrierung verwaltet und können mit den Befehlen **Assoc** und **Ftype** geändert werden. Sie erstellen eine Dateiverknüpfung in der Befehlszeile, indem Sie **assoc** eingeben, gefolgt von der Erweiterungseinstellung, zum Beispiel **assoc .pl=perlfile**. Den Dateityp erstellen Sie in der Befehlszeile, indem Sie die Zuordnung zwischen Datei und Typ inklusive der Aufrufparameter festlegen, die zusammen mit dem Befehlsnamen übergeben werden, zum Beispiel **ftype perlfile=C:\Perl\Bin\Perl.exe "%1" %***.

Sie können einen Dateityp oder ein Protokoll auch mit einem bestimmten Programm verknüpfen, indem Sie folgendermaßen vorgehen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Programme*. Tippen oder klicken Sie auf *Standardprogramme* und dann auf *Dateityp oder Protokoll einem Programm zuordnen*.
2. Auf der Seite *Dateizuordnungen festlegen* werden die aktuellen Dateiverknüpfungen nach ihren Dateierweiterungen und dem aktuellen Standard für die jeweilige Erweiterung aufgelistet. Tippen oder klicken Sie auf die Dateierweiterung und dann auf *Programm ändern*, um die Dateiverknüpfung für eine Erweiterung zu ändern.
3. Sie haben jetzt folgende Möglichkeiten:
 - Das Dialogfeld *Wie soll dieser Dateityp geöffnet werden* zeigt Programme an, die im Betriebssystem als Programme registriert sind, die Dateien mit der ausgewählten Erweiterung unterstützen. Tippen oder klicken Sie auf ein empfohlenes Programm, um es als Standard für die ausgewählte Erweiterung festzulegen.
 - Um andere verfügbare Programme anzuzeigen, die möglicherweise ebenfalls die ausgewählte Erweiterung unterstützen, tippen oder klicken Sie auf *Weitere Optionen*. Tippen oder klicken Sie auf ein Programm, um es als Standard für die ausgewählte Erweiterung festzulegen. Stattdessen können Sie auch auf eine der *Nach einer App suchen*-Optionen klicken, um ein anderes Programm zu suchen, das Sie als Standard verwenden wollen.

In den Gruppenrichtlinien können Sie mit einem Einstellungselement neue Dateitypen und Dateiverknüpfungen definieren. Gehen Sie folgendermaßen vor, um ein Einstellungselement für einen neuen Dateityp zu erstellen:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie den Zweig *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* und wählen Sie *Ordneroptionen* aus.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Ordneroptionen* oder halten Sie ihn gedrückt, und wählen Sie im Kontextmenü den Befehl *Neu/Dateityp*. Daraufhin öffnet sich das Eigenschaftendialogfeld für den neuen Dateityp.
3. Wählen Sie in der Liste *Aktion* den Eintrag *Erstellen*, *Aktualisieren*, *Ersetzen* oder *Löschen* aus. Wie diese Aktionen funktionieren, wurde bereits in Kapitel 6, »Automatisieren der Windows 8-Konfiguration«, beschrieben. Wenn Sie ein Einstellungselement erstellen möchten, das einen vorhandenen Dateityp löscht, wählen Sie die Aktion *Löschen*.

4. Geben Sie im Feld *Dateierweiterung* die Namenserverweiterung des Dateityps ohne den Punkt ein, zum Beispiel **pl**.
5. Wählen Sie in der Dropdownliste *Zugeordnete Klasse* eine registrierte Klasse aus, die Sie mit dem Dateityp verknüpfen wollen.
6. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Gewöhnlich ist es sinnvoll, die neue Variable nur einmal zu erstellen. Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmal anwenden*.
7. Tippen oder klicken Sie auf **OK**. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Gehen Sie folgendermaßen vor, um ein Einstellungselement für eine neue Dateiverknüpfung zu erstellen:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* und wählen Sie *Ordneroptionen* aus.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Ordneroptionen* oder halten Sie ihn gedrückt, und wählen Sie im Kontextmenü den Befehl *Neu/Öffnen mit*. Dadurch öffnet sich das Dialogfeld *Neue Eigenschaften für "Öffnen mit"*.
3. Wählen Sie in der Liste *Aktion* den Eintrag *Erstellen, Aktualisieren, Ersetzen* oder *Löschen* aus.
4. Geben Sie im Feld *Dateierweiterung* die Namenserverweiterung des Dateityps ohne den Punkt ein, zum Beispiel **pl**.
5. Tippen oder klicken Sie auf die *Durchsuchen*-Schaltfläche rechts neben dem Textfeld *Zugeordnetes Programm* und wählen Sie im Dialogfeld *Öffnen* das Programm aus, das Sie mit dem Dateityp verknüpfen wollen.
6. Optional können Sie das Kontrollkästchen *Als Standard* aktivieren, um das zugehörige Programm zum Standard für Dateien mit der angegebenen Dateierweiterung zu machen.
7. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Gewöhnlich ist es sinnvoll, die neue Variable nur einmal zu erstellen. Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmal anwenden*.
8. Tippen oder klicken Sie auf **OK**. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Einstellen der automatischen Wiedergabe

In Windows 8 lässt sich mit den Optionen für die automatische Wiedergabe (AutoPlay) einstellen, wie Windows mit Dateien von CDs, DVDs und tragbaren Geräten umgeht. Sie können für jede Art von CD, DVD und Medien, die Ihr Computer bearbeiten kann, die automatische Wiedergabe separat einstellen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Programme*. Tippen oder klicken Sie auf *Standardprogramme* und dann auf *Einstellungen für automatische Wiedergabe ändern*. Dadurch öffnet sich die Seite *Automatische Wiedergabe* in der Systemsteuerung.
2. Verwenden Sie die Medienauswahlliste (Abbildung 8.6), um die Standardoptionen für die automatische Wiedergabe der verschiedenen Medienarten nach Bedarf festzulegen.

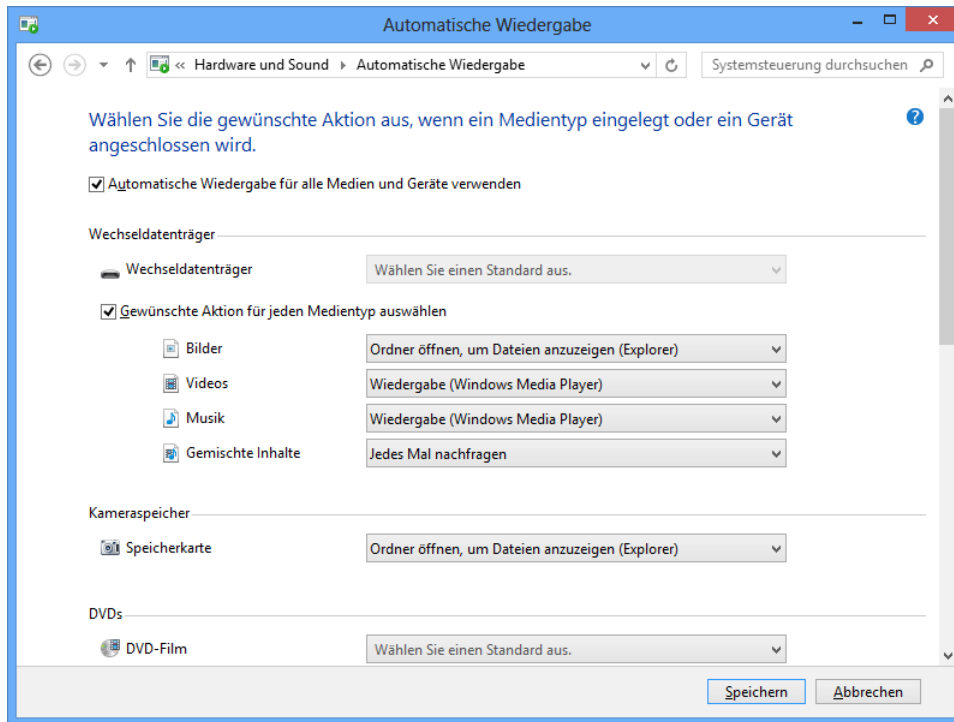


Abbildung 8.6 Legen Sie die Optionen für die automatische Wiedergabe von CDs, DVDs und Dateien auf portablen Geräten fest

Den Standard für Wechseldatenträger (USB-Speichersticks und so weiter) können Sie so festlegen, dass er für alle Medientypen gilt oder für jeden Medientyp separat. Um einen allgemeinen Standard festzulegen, löschen Sie das Kontrollkästchen *Gewünschte Aktion für jeden Medientyp auswählen* und legen den Standard fest. Um separate Standards festzulegen, wählen Sie das Kontrollkästchen *Gewünschte Aktion für jeden Medientyp auswählen* und legen dann für jeden Medientyp separat den Standard fest.

4. Tippen oder klicken Sie auf *Speichern*, um die Einstellungen zu speichern.

Hinzufügen und Entfernen von Windows-Funktionen

In Windows XP und älteren Windows-Versionen haben Sie Komponenten des Betriebssystems mit der Option *Windows-Komponenten hinzufügen/entfernen* des Programms *Software* aus der Systemsteuerung installiert und verwaltet. Inzwischen werden Betriebssystemkomponenten als Windows-Funktionen (oder Features) betrachtet, die ein- und ausgeschaltet statt hinzugefügt und entfernt werden.

Mit folgenden Schritten können Sie Windows-Funktionen aktivieren oder deaktivieren:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Programme*. Tippen oder klicken Sie unter *Programme und Features* auf *Windows-Features aktivieren oder deaktivieren*. Daraufhin öffnet sich das Dialogfeld *Windows-Features* (Abbildung 8.7).
2. Aktivieren Sie die Kontrollkästchen der Funktionen, um sie zu aktivieren, oder deaktivieren Sie Kontrollkästchen, um Funktionen auszuschalten.
3. Tippen oder klicken Sie auf *OK*. Windows 8 konfiguriert nun die Komponenten entsprechend den Einstellungen, die Sie vorgenommen haben.

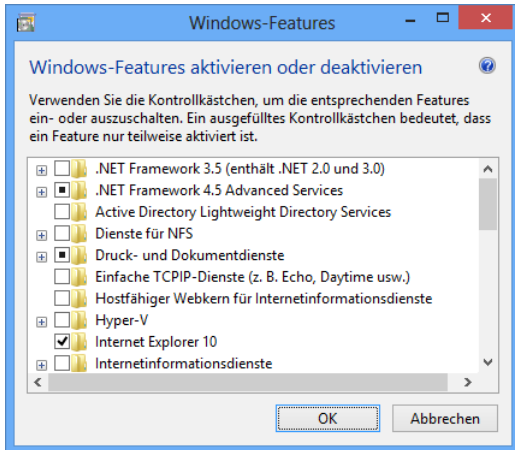


Abbildung 8.7 Hinzufügen oder Entfernen von Betriebssystemkomponenten

Kapitel 9

Verwalten von Hardwaregeräten und Treibern

In diesem Kapitel:

Arbeiten mit dem automatischen Hilfesystem	304
Installieren und Warten von Geräten: Die Grundlagen	323
Einführung in den Geräte-Manager	335
Arbeiten mit Gerätetreibern	337

Die Verwaltung der Hardwarekonfiguration von Computern bedeutet im Wesentlichen die Installation und Konfiguration von Betriebssystemkomponenten, Hardwaregeräten und Gerätetreibern. Allerdings unterscheidet sich die Verwaltung der Hardwarekonfiguration von Windows 7- und Windows 8-Computern stark von der Konfigurationsverwaltung bei Computern, die unter Windows XP oder älteren Windows-Versionen laufen. Viele Teile von Windows 8 werden automatisch überwacht und aktualisiert. Sie müssen nicht wie in früheren Windows-Versionen konfiguriert und gepflegt werden. Windows 8 setzt folgende Mittel ein:

- Eine automatische Wartung, die vom Betriebssystem erkannte Probleme behebt oder im Wartungszentrum über die Probleme berichtet
- SmartScreen zur Warnung der Benutzer, bevor sie unbekannte Apps aus dem Internet verwenden
- Integrierte Überwachung der Hardwaregeräte, des Arbeitsspeichers, der Vernetzung und der Leistung
- Problemberichte zur automatischen Behebung von Konfigurations- und Leistungsproblemen
- Problem Diagnosen mit Lösungsvorschlägen zur Behebung von Problemen, die sich nicht automatisch beseitigen lassen
- Automatische Updates, um die Betriebssystemkomponenten auf dem neusten Stand zu halten
- Treiberaktualisierung zur Beschaffung der erforderlichen Treiber und Treiberupdates für erkannte Hardwaregeräte
- Eine verbesserte automatische Diagnose für Kompatibilitätsprobleme in Anwendungen und Laufwerken

Ab dem Moment, in dem Sie Windows 8 installieren, sind diese Komponenten wirksam und unterstützen Sie bei der Überwachung und Verwaltung. Als Administrator können Sie diese Komponenten zur Unterstützung bei der Konfiguration und Wartung der Systeme einsetzen. Für verschiedene Bereiche sind separate Überwachungsprogramme verfügbar, mit denen sich aktuelle Leistungsdaten für die Hardware, die Speicherauslastung und die Netzauslastung erfassen lassen.

Zur Konfiguration und Wartung von Hardwaregeräten und Treibern können Sie den Geräte-Manager, *Geräte und Drucker* oder den Assistenten zum Hinzufügen von Geräten und Druckern verwenden. Diese Programme unterstützen Sie bei der Installation und Deinstallation von Hardwaregeräten sowie bei der Behebung von Problemen mit den Geräten und Treibern. Zur Verwaltung von bestimmten Hardwaregeräten sind spezielle Programme verfügbar, wie zum Beispiel zur Einstellung der Tastatur oder der Soundkarte. Für die automatische Aktualisierung des Systems und für die Treiberaktualisierung verwenden Sie Windows Update, für das es in der Systemsteuerung ein eigenes Konfigurationsprogramm gibt.

Arbeiten mit dem automatischen Hilfesystem

Die vielen Verbesserungen in *Hilfe und Support* von Windows 8 ändern grundlegend die Funktionsweise des Betriebssystems und den Ablauf Ihres Supports. Als Administrator müssen Sie unbedingt wissen, wie das Hilfesystem funktioniert und wie es konfiguriert wird.

Benutzen von *Hilfe und Support*

Windows 8 stützt sich auf eine umfangreiche Diagnose- und Problembehebungsarchitektur, deren Grundlage schon für Windows 7 entwickelt wurde. Ältere Windows-Versionen boten zwar auch Diagnosefunktionen an, aber die Diagnosen gingen nur selten so weit, dass man von Selbstdiagnose oder einem selbstkorrigierenden System sprechen konnte. Dagegen kann das aktuelle Framework viele Arten

von Hardware-, Speicher- und Leistungsproblemen erkennen und automatisch beheben oder den Benutzer durch die Problembehebungsprozedur führen.

Windows bietet nun zuverlässigere und leistungsfähigere Gerätetreiber, die einen Teil der üblichen Ursachen für Hänger und Abstürze verhindern. Eine verbesserte Abbruchmöglichkeit von Ein-/Ausgabeoperationen der Gerätetreiber sorgt dafür, dass sich das System leichter von blockierenden Aufrufen erholen kann und dass es weniger blockierende Ein-/Ausgabeoperationen bei Laufwerken gibt.

Um Ausfallzeiten und die Zahl der Neustarts zu verringern, die zur Installation von Anwendungen und Updates erforderlich sind, kann Windows 8 den Updateprozess verwenden, um in Gebrauch befindliche Dateien für die Aktualisierung vorzumerken und diese Dateien automatisch zu ersetzen, wenn die Anwendung das nächste Mal gestartet wird. In bestimmten Fällen kann Windows 8 die Anwendungsdaten speichern, die Anwendung schließen, die in Gebrauch befindlichen Dateien aktualisieren und die Anwendung dann neu starten. Um die Gesamtleistung und Reaktionsfähigkeit des Systems zu verbessern, verwendet Windows den Speicher effizienter, sorgt für eine geordnete Ausführung von Threadgruppen und bietet mehrere Laufzeitzuteilungsmechanismen für Prozesse. Durch die Optimierung des Speichers und der Laufzeitzuteilung sorgt Windows 8 dafür, dass sich Hintergrundprozesse weniger stark auf die Systemleistung auswirken.

Windows überwacht standardmäßig Apps, die aus dem Internet heruntergeladen werden, mit SmartScreen. Bevor unbekannte Apps aus dem Internet gestartet werden können, ist die Genehmigung durch einen Administrator erforderlich. Wenn Sie das nicht möchten, stellen Sie SmartScreen so ein, dass stattdessen eine Warnung angezeigt wird, oder Sie schalten SmartScreen ganz ab.

Windows bietet zudem eine bessere Unterstützung bei der Ursachenforschung in Problembereichen. Mit zusätzlichen Details im Fehlereintrag im Ereignisprotokoll erleichtert Windows die Identifizierung und Behebung von Problemen. Windows 8 kann sich auch nach dem Ausfall eines Dienstes besser erholen als seine Vorgänger. Beim Neustart eines ausgefallenen Dienstes berücksichtigt Windows Abhängigkeiten unter den Diensten ebenso wie Abhängigkeiten von anderen Komponenten. Alle erforderlichen Dienste und Systemkomponenten, von denen der ausgefallene Dienst abhängig ist, werden vor dem ausgefallenen Dienst gestartet.

In älteren Windows-Versionen wurde eine abgestürzte oder hängende Anwendung als nicht reagierend gekennzeichnet. Dann war es Sache des Benutzers, die Anwendung zu beenden und neu zu starten. Windows versucht nun, das Problem mit nicht reagierenden Anwendungen durch einen Programmkompatibilitäts-Assistenten (Program compatibility Assistant, PCA) und einen Neustart-Manager zu lösen. Der PCA erkennt, wenn wegen Kompatibilitätsproblemen Installationen fehlschlagen, Laufzeitfehler auftreten und Treiber blockieren. Zur Behebung dieser Probleme bietet der PCA an, eine Anwendung im Kompatibilitätsmodus zu betreiben oder Online-Hilfe von einer Microsoft-Website anzufordern. Der Neustart-Manager kann nicht reagierende Anwendungen automatisch schließen und neu starten. Dank des Neustart-Managers brauchen Sie Probleme mit eingefrorenen Anwendungen möglicherweise nicht mehr selbst zu lösen.

HINWEIS Der Diagnoserichtliniendienst und der Programmkompatibilitäts-Assistent-Dienst müssen laufen und richtig konfiguriert sein, damit die automatische Diagnose und die Unterstützung bei Kompatibilitätsproblemen funktionieren. In der Konsole *Computerverwaltung* können Sie diese Dienste unter dem Knoten *Dienste und Anwendungen/Dienste* konfigurieren. Um die Computerverwaltung zu öffnen, können Sie zum Beispiel die WINDOWS-Taste drücken, **compmgmt.msc** eingeben und dann die EINGABETASTE drücken. Diese Methode funktioniert, solange das Suchfeld *Apps* im Eingabefokus liegt.

PRAXISTIPP

Aus technischer Sicht sind die Hauptknoten in der Computerverwaltung Snap-In-Erweiterungen, die zur Microsoft Management Console (MMC) hinzugefügt wurden, um die Konsole zusammenzustellen. Möchten Sie sich davon überzeugen? Geben Sie in einer Eingabeaufforderung MMC ein. Verwenden Sie *Snap-In hinzufügen/entfernen*, um die Computerverwaltung zur MMC hinzuzufügen. Wählen Sie im Dialogfeld *Snap-Ins hinzufügen bzw. entfernen* unter *Ausgewählte Snap-Ins* den Eintrag *Computerverwaltung* aus und klicken Sie auf *Erweiterungen bearbeiten*. Sie sehen die einzelnen Snap-In-Erweiterungen – und wie Microsoft die Konsole zusammengestellt hat.

Fehlgeschlagene Installationen und hängende Anwendungen und Treiber werden auch im Wartungszentrum verfolgt. In diesen Fällen sind die integrierten Diagnosemechanismen manchmal in der Lage, eine Lösung für das Problem anzubieten. Folgendermaßen zeigen Sie eine Liste der aktuellen Probleme an:

- Tippen oder klicken Sie im Infobereich der Taskleiste auf das Symbol *Wartungszentrum* und dann auf *Wartungszentrum öffnen*.
- Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *System und Sicherheit* auf *Status des Computers überprüfen*.

Im Wartungszentrum (Abbildung 9.1) finden Sie eine Liste der Probleme, die in zwei Kategorien untergliedert ist: Sicherheit und Wartung.

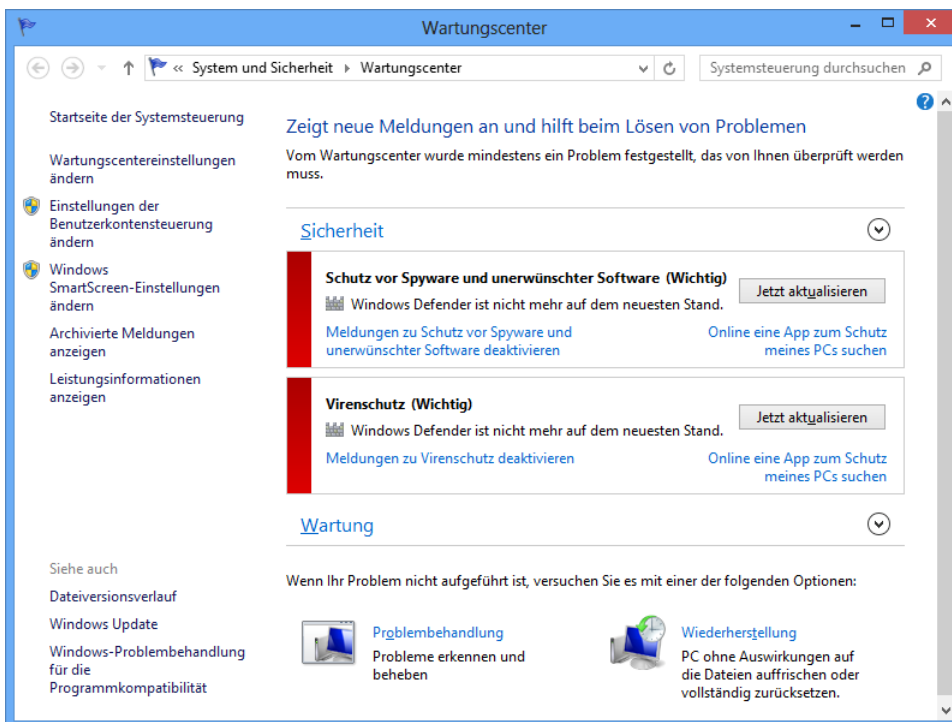


Abbildung 9.1 Im Wartungszentrum erfahren Sie, ob momentan Probleme vorliegen

Die Probleme sind mit Farben markiert:

- Rot sind Warnungen zu einem bedeutsamen Problem, das Ihrer Aufmerksamkeit bedarf. Hat der Computer beispielsweise keine Antivirensoftware, ist das eine rote Warnung.

- Orange sind Warnungen zu einem Problem, das Sie bei Gelegenheit überprüfen sollten. Wurde der Computer etwa seit einiger Zeit nicht mehr mit Windows-Defender untersucht, ist das eine orange Warnung.

Wenn Sie auf die Kategorieüberschriften *Sicherheit* oder *Wartung* tippen oder klicken, wird der jeweilige Abschnitt erweitert und zeigt detailliertere Informationen an. Wenn Sie den Bereich *Sicherheit* erweitern, werden Informationen zu folgenden Elementen angezeigt:

- Status von Netzwerkfirewall, Windows Update, Virenschutz und Schutz vor Spyware und unerwünschter Software
- Konfiguration von Internetsicherheitseinstellungen, Benutzerkontensteuerung, Windows SmartScreen, Netzwerkzugriffsschutz und Windows-Aktivierung

Wenn Sie den Bereich *Wartung* erweitern, werden Informationen über folgende Elemente angezeigt:

- Verknüpfungen zum Verwalten der Konfiguration von Problembereichen
- Status des Dateiversionsverlaufs und der Laufwerke des Computers
- Status der automatischen Wartung und Verknüpfungen für die Einstellung der Wartung

Wenn Sie einen Computer frisch eingerichtet haben und nun prüfen wollen, ob Probleme bestehen, oder wenn Sie den Verdacht haben, dass Probleme bei diesem Computer auftreten, die noch nicht diagnostiziert wurden, können Sie die automatische Problemerkennung folgendermaßen einleiten:

1. Tippen oder klicken Sie im Wartungscenter auf die Bereichsüberschrift *Wartung* und blättern Sie gegebenenfalls nach unten.
2. Unter der Liste der aktuellen Probleme finden Sie den Abschnitt *Nach Lösungen für Problembereiche suchen*, der eine Reihe von Verknüpfungen enthält. Tippen oder klicken Sie auf *Nach Lösungen suchen*, um den automatisierten Problembereichterstattungsprozess zu starten. Sobald dieser Prozess abgeschlossen ist, aktualisiert das Wartungscenter die Anzeige und führt alle neu erkannten Probleme sowie die bekannten Lösungen auf.

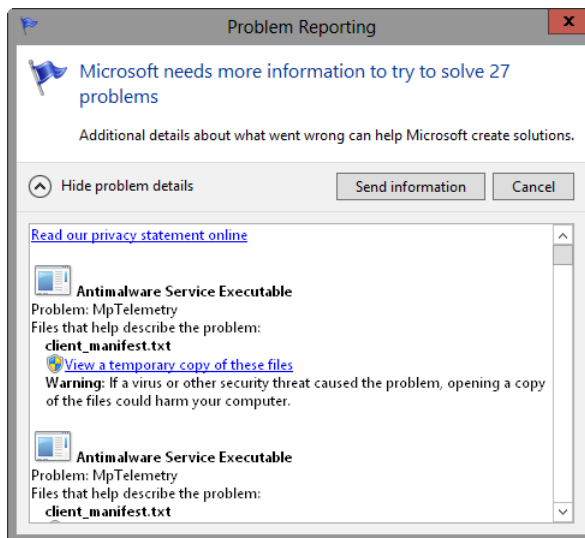


Abbildung 9.2 Überprüfen erkannter Probleme, zu denen keine Lösungen verfügbar sind

3. Erkennt die automatisierte Diagnose Probleme, zu denen sie keine Lösungen anbieten kann, können Sie sich zusätzliche Informationen über die Probleme ansehen. Tippen oder klicken Sie im Dialogfeld *Problembereichte und -lösungen* (Abbildung 9.2) auf *Problemdetails anzeigen*, um weitere Informationen über die erkannten Probleme zu erhalten. Wenn Sie Ihre eigene Problembehandlung durchführen wollen, können Sie auf die angezeigten Links tippen oder klicken, um die Daten zu extrahieren, die Sie später zum Analysieren der Probleme brauchen. Die so extrahierten Daten werden im Ordner *Temp* im Profil des angemeldeten Benutzers gespeichert. Sie müssen diese Daten kopieren, bevor Sie fortfahren.
4. Tippen oder klicken Sie im Dialogfeld *Problembereichte und -lösungen* auf *Informationen senden*, um die Daten an Microsoft zu senden, oder auf *Abbrechen*, um *Problembereichte und -lösungen* zu schließen, ohne die Informationen an Microsoft zu senden. Wenn Sie sich dazu entscheiden, die Informationen an Microsoft zu senden, werden die Problembehandlungsdaten in den Ordner *Temp* im Profil des angemeldeten Benutzers extrahiert, an Microsoft übertragen und dann aus dem Verzeichnis *Temp* gelöscht. Dabei können erhebliche Mengen an Daten extrahiert und gesendet werden.

Erkannte Probleme, zu denen Lösungen bekannt sind, können Sie folgendermaßen im Wartungscenter beseitigen:

1. Bei jedem Problem finden Sie eine Lösungsschaltfläche oder eine Verknüpfung. Handelt es sich um ein Sicherheitsproblem, können Sie gewöhnlich Programme online suchen oder den Computer mit Schutzsoftware durchsuchen. Bei Wartungsproblemen tippen oder klicken Sie meist auf die Schaltfläche *Antwort zum Problem anzeigen*, um eine Seite zu öffnen, die ausführlichere Informationen zum Problem liefert.
2. Auf der Seite *Weitere Informationen* gibt es mehrere Möglichkeiten: Wird ein Problem durch einen Treiber oder Software verursacht, finden Sie einen Link, über den Sie den neusten Treiber oder ein Softwareupdate herunterladen und installieren können. Ist dagegen ein Konfigurationsproblem die Ursache, finden Sie eine Beschreibung des Problems und eine Schritt-für-Schritt-Anleitung, wie Sie die Konfiguration so ändern, dass das Problem beseitigt ist.
3. Sobald Sie ein Problem beseitigt haben, indem Sie einen Treiber oder ein Softwareupdate installieren, können Sie die Meldung für künftige Analysen archivieren. Aktivieren Sie dazu das Kontrollkästchen *Diese Meldung archivieren*, bevor Sie die Seite *Weitere Informationen* mit OK schließen.

Sie haben im Wartungscenter die Möglichkeit, einen Zuverlässigkeitsbericht für den Computer erstellen zu lassen, um den bisherigen Verlauf der Hardware- und Softwareprobleme zu überprüfen. Anhand dieses Verlaufs können Sie feststellen, wie stabil der Computer ist und welche Geräte oder Programme in der Vergangenheit Probleme verursacht haben. Gehen Sie folgendermaßen vor, um die Zuverlässigkeitsüberwachung zu öffnen und zu benutzen:

1. Tippen oder klicken Sie im Wartungscenter auf die Bereichsüberschrift *Wartung* und blättern Sie nach unten.
2. Unter der Liste der aktuellen Probleme finden Sie den Abschnitt *Nach Lösungen für Problembereichte suchen*, der eine Reihe von Links enthält. Tippen oder klicken Sie auf *Zuverlässigkeitsverlauf anzeigen*.
3. Wie in Abbildung 9.3 gezeigt, erhalten Sie eine grafische Darstellung, die über die Stabilität des Computers Auskunft gibt. Hier können Sie den Verlauf über mehrere Tage oder Wochen verfolgen. Die Standardansicht ist *Tage*. Wenn Sie sich mehrere Wochen ansehen wollen, müssen Sie neben *Anzeige* auf die Option *Wochen* tippen oder klicken. Die Stabilität des Computers wird in Form von Werten gemessen, die von 0 (geringe Zuverlässigkeit) bis 10 (hervorragende Zuverlässigkeit) reichen.
4. Ereignisse, die sich unter Umständen auf die Stabilität auswirken, werden mit Informations- oder Warnsymbolen unten im Diagramm angezeigt. Wenn Sie auf ein solches Symbol tippen oder klicken,

werden ausführliche Informationen zum Ereignis in der Liste *Zuverlässigkeitsdetails* angezeigt. Wie Sie in der Abbildung sehen, werden zu den Ereignissen die Spalten *Quelle*, *Zusammenfassung* und *Datum* angezeigt. Unter *Aktion* finden Sie einen Link. Falls Windows das Problem automatisch lösen konnte, ist dies der Link *Antwort zum Problem anzeigen*. Wenn Sie auf den Link tippen oder klicken, wird angezeigt, wie Windows das Problem beseitigt hat. In anderen Fällen ist der Link *Technische Details anzeigen* aufgeführt. Tippen oder klicken Sie diesen Link an, um weitere Informationen über das Stabilitätsproblem zu erhalten (Abbildung 9.4).

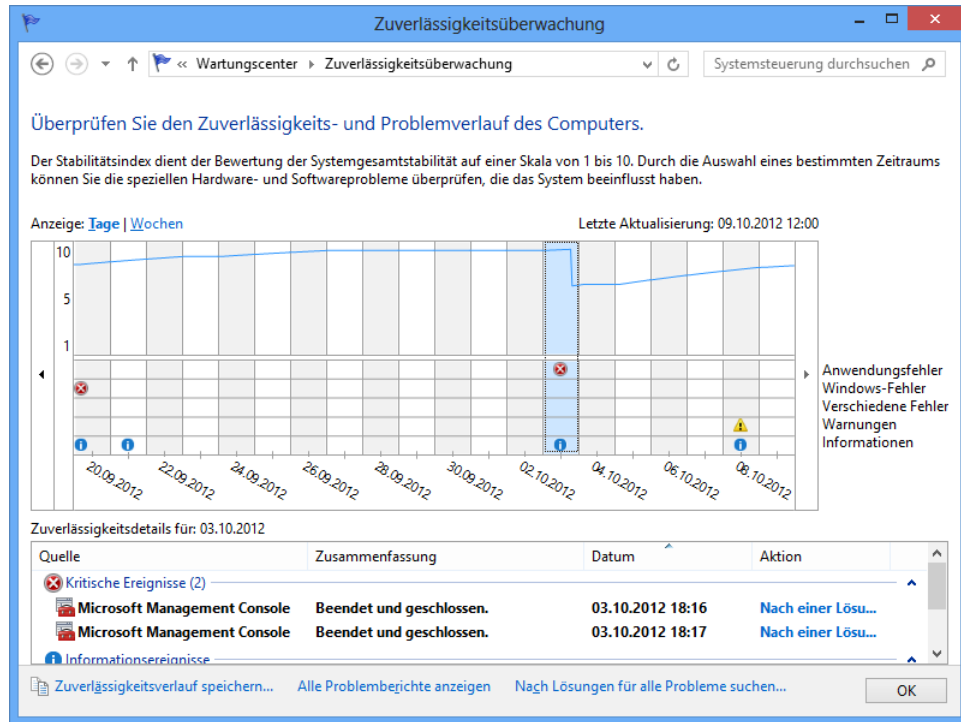


Abbildung 9.3 Grafische Darstellung der Stabilität eines Computers

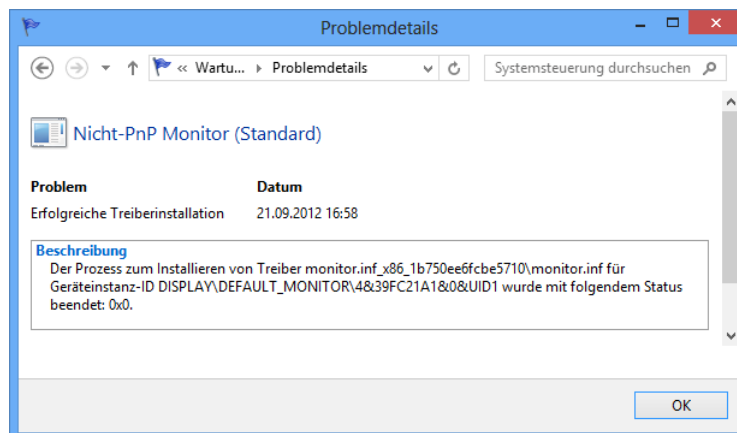


Abbildung 9.4 Anzeigen von Berichtsdetails, die weitere Informationen liefern

5. Am unteren Rand des Fensters *Zuverlässigkeitsüberwachung* stehen weitere Optionen zur Verfügung:
- **Zuverlässigkeitsverlauf speichern** Hier können Sie die vollständigen Details zur Stabilität des Computers für die künftige Verwendung speichern. Diese Informationen werden in Form eines Zuverlässigkeitsüberwachungsberichts gespeichert, der als XML formatiert ist. Tippen oder klicken Sie auf *Zuverlässigkeitsverlauf speichern* und wählen Sie dann im angezeigten Dialogfeld einen Speicherort und den Dateinamen für den Bericht. Sie können sich den Bericht im Internet Explorer ansehen, indem Sie die Datei doppelt antippen oder anklicken.
 - **Alle Problemberichte anzeigen** Öffnet die Seite *Problemberichte*, die eine Liste aller Probleme anzeigt, die bisher erkannt wurden. Hier wird auch der Status der Probleme gemeldet. Durch Tippen oder Klicken auf *Alle Problemberichte löschen* können Sie alle Berichte entfernen.
 - **Nach Lösungen für alle Probleme suchen** Startet den automatisierten Problemberichterstattungsprozess. Sobald dieser Prozess abgeschlossen ist, aktualisiert das Wartungscenter die Anzeige und führt alle neu entdeckten Probleme und die zugehörigen Lösungen auf (sofern bekannt).

Anpassen von *Hilfe und Support*

Windows 8 stellt viele Möglichkeiten zur Verfügung, die Funktionsweise des Hilfe- und Supportsystems anzupassen. Auf der einfachsten Ebene können Sie steuern, welche Benachrichtigungsarten im Wartungscenter angezeigt werden. Dieses Feature können Sie noch weiter optimieren, indem Sie kontrollieren, wie Problemberichterstattung und Problembehandlung arbeiten.

Jeder Benutzer, der sich an einem Computer anmeldet, hat individuelle Benachrichtigungseinstellungen. Gehen Sie folgendermaßen vor, um festzulegen, welche Arten von Benachrichtigungen im Wartungscenter angezeigt werden:

1. Tippen oder klicken Sie im linken Fensterabschnitt des Wartungscenters auf *Wartungscentereinstellungen ändern*.

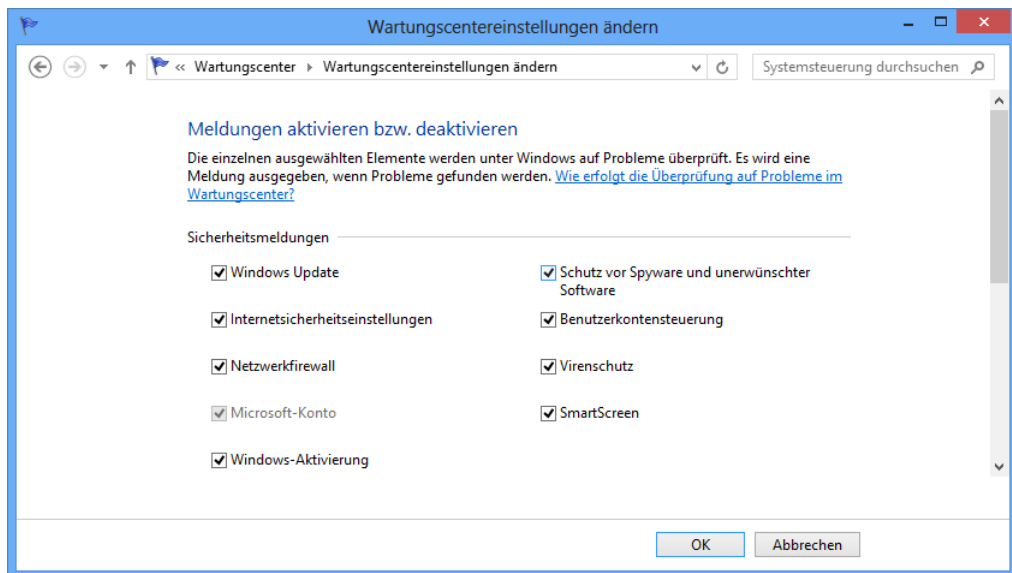


Abbildung 9.5 Konfigurieren von Sicherheitsmeldungen im Wartungscenter

2. Aktivieren Sie auf der Seite *Wartungscentereinstellungen ändern* (Abbildung 9.5) die Kontrollkästchen der Benachrichtigungen, die der Benutzer angezeigt bekommen soll, und deaktivieren Sie die Kontrollkästchen der Benachrichtigungen, die nicht angezeigt werden sollen.
3. In der Standardeinstellung werden im Rahmen des Programms zur Verbesserung der Benutzerfreundlichkeit Nutzungsinformationen an Microsoft gesendet. Wenn Sie nicht an diesem Programm teilnehmen wollen, können Sie auf den Link *Einstellungen für das Programm zur Verbesserung der Benutzerfreundlichkeit* klicken, die Option *Nein, ich möchte nicht am Windows-Programm zur Verbesserung der Benutzerfreundlichkeit teilnehmen* wählen und auf *Änderungen speichern* klicken.
4. Tippen oder klicken Sie auf *OK*.

In einer Standardkonfiguration hat jeder Benutzer, der sich an einem Computer anmeldet, individuelle Einstellungen für die Problemberichterstattung. Administratoren können aber auch festlegen, dass für alle Benutzer dieselben Berichtseinstellungen gelten. So legen Sie fest, wie die Problemberichterstattung für den momentan angemeldeten Benutzer oder für alle Benutzer funktioniert:

1. Tippen oder klicken Sie im linken Fensterabschnitt des Wartungscenters auf *Wartungscentereinstellungen ändern*.
2. Tippen oder klicken Sie auf der Seite *Wartungscentereinstellungen ändern* unter *Verwandte Einstellungen* auf *Einstellungen für Problemberichterstattung*.
3. Sie bekommen nun die aktuelle Konfiguration der Problemberichterstattung für den angemeldeten Benutzer angezeigt. Ist es möglich, die Einstellungen zu verändern, dann ist der Computer so konfiguriert, dass jeder Benutzer seine Problemberichteinstellungen selbst wählen kann. Wenn es dagegen nicht möglich ist, die Einstellungen zu verändern, ist der Computer so konfiguriert, dass für alle Benutzer dieselben Problemberichteinstellungen gelten.
4. Sofern der Computer so konfiguriert ist, dass die Problemberichteinstellungen für jeden Benutzer individuell verwaltet werden, können Sie die Problemberichteinstellungen wählen, die Sie für den momentan angemeldeten Benutzer verwenden möchten, und *OK* klicken, um die Einstellungen zu speichern. Es stehen folgende Optionen zur Wahl:
 - *Automatisch nach Lösungen suchen*
 - *Automatisch nach Lösungen suchen und gegebenenfalls zusätzliche Berichtsdaten senden*
 - *Bei Problemen erst Bestätigung anfordern, bevor nach Lösungen gesucht wird*
 - *Nie nach Lösungen suchen*
5. Werden die Problemberichteinstellungen für den gesamten Computer festgelegt, müssen Sie auf *Berichtseinstellungen für alle Benutzer ändern* klicken, die Problemberichteinstellungen wählen, die für alle Benutzer gelten sollen, und auf *OK* klicken, um die Einstellungen zu speichern. Es stehen folgende Optionen zur Auswahl:
 - *Automatisch nach Lösungen suchen*
 - *Automatisch nach Lösungen suchen und gegebenenfalls zusätzliche Daten senden*
 - *Bei Problemen erst Bestätigung anfordern, bevor nach Lösungen gesucht wird*
 - *Nie nach Lösungen suchen*
 - *Jeder Benutzer darf Einstellungen auswählen*

Wenn die Problemberichterstattung aktiviert ist, können Sie Programme aus der Problemberichterstattung ausschließen. Gehen Sie dazu so vor:

1. Tippen oder klicken Sie im linken Fensterabschnitt des Wartungscenters auf *Wartungscentereinstellungen ändern*.

2. Tippen oder klicken Sie auf der Seite *Wartungszentereinstellungen ändern* unter *Verwandte Einstellungen* auf *Einstellungen für Probleberichterstattung*. Tippen oder klicken Sie anschließend auf *Aus Berichterstattung auszuschließende Programme auswählen*.
3. Auf der Seite *Erweiterte Einstellungen für die Probleberichterstattung* wird eine Liste aller Programme angezeigt, die momentan ausgeschlossen sind. Sie haben nun folgende Möglichkeiten:
 - Fügen Sie Programme hinzu, um sie aus der Berichterstattung auszuschließen. Tippen oder klicken Sie auf *Hinzufügen*, wählen Sie im Dialogfeld die ausführbare Datei (.exe) des gewünschten Programms aus und tippen oder klicken Sie auf *Öffnen*.
 - Entfernen Sie Programme aus der Liste, damit sie nicht mehr von der Berichterstattung ausgeschlossen sind. Markieren Sie das Programm dazu in der Liste und tippen oder klicken Sie auf *Entfernen*.

Für jeden Benutzer, der sich an einem Computer anmeldet, gelten individuelle Windows SmartScreen-Einstellungen. So stellen Sie SmartScreen ein:

1. Tippen oder klicken Sie im linken Fensterabschnitt des Wartungszenters auf *Windows SmartScreen-Einstellungen ändern*.
2. Legen Sie im Dialogfeld *Windows SmartScreen* fest, wie mit unbekannten Apps verfahren werden soll. Standardmäßig zeigt Windows vor der Ausführung unbekannter Apps aus dem Internet ein Meldungsfeld an, in dem die Genehmigung eines Administrators angefordert wird. Wenn Sie auf die Genehmigung eines Administrators verzichten, können Sie stattdessen auch eine Warnung anzeigen oder SmartScreen deaktivieren.
3. Tippen oder klicken Sie auf *OK*.

Für jeden Benutzer, der sich an einem Computer anmeldet, gelten individuelle Einstellungen für die automatische Wartung. So stellen Sie die Wartung ein:

1. Tippen oder klicken Sie im Wartungszenters auf die Überschrift *Wartung* und führen Sie gegebenenfalls einen Bildlauf durch.
2. Unter der Liste der aktuellen Probleme gibt es einen Abschnitt mit der Überschrift *Automatische Wartung*. Tippen oder klicken Sie auf *Wartungseinstellungen ändern*.

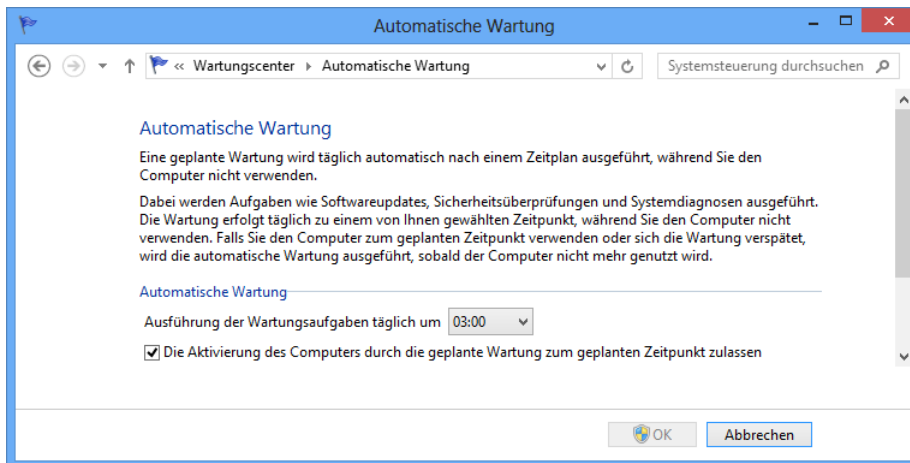


Abbildung 9.6 Festlegen der Wartungseinstellungen

3. Auf der Seite *Automatische Wartung* sehen Sie die aktuellen Einstellungen für die Wartung (Abbildung 9.6).
4. Legen Sie in der Dropdownliste *Ausführung der Wartungsaufgaben täglich um* die gewünschte Anfangszeit für die tägliche Wartung fest.
5. Damit Windows den Computer für die Wartung aus dem Energiesparmodus reaktivieren kann, wählen Sie das entsprechende Kontrollkästchen.
6. Tippen oder klicken Sie auf OK.

Die automatische Wartung stützt sich auf die Windows-Diagnoseinfrastruktur. Windows führt routinemäßig um 3 Uhr nachts Wartungsarbeiten durch, sofern der Computer am Stromnetz angeschlossen ist und das Betriebssystem sonst nichts zu tun hat. Andernfalls beginnt die Wartung, wenn der Computer das nächste Mal wieder mit Netzstrom betrieben wird und das Betriebssystem sonst nichts zu tun hat. Da die Wartung nur erfolgt, wenn sich das Betriebssystem im Leerlauf befindet, darf sie im Hintergrund bis zu 3 Tage laufen. Das ermöglicht Windows auch die Durchführung von komplexen Wartungsarbeiten.

Im Wartungscenter zeigt der Abschnitt *Automatische Wartung* den Status der automatischen Wartung an und bietet auch Verwaltungsoptionen. Zu den Statusinformationen gehört das Datum der letzten Ausführung. Außerdem wird es angegeben, wenn Korrekturen erforderlich sind. Während die Wartung durchgeführt wird, lautet die Statusangabe *Wartung wird durchgeführt*. Ergibt sich bei der Wartung ein Problem, sehen Sie auch dies. Um die Wartung manuell zu starten, tippen oder klicken Sie auf *Wartung starten*.

Die automatische Wartung wird als geplante Aufgabe durchgeführt. In der Aufgabenplanung finden Sie diese Aufgabe in der Aufgabenplanungsbibliothek unter *Microsoft\Windows\Diagnosis*. Ausführliche Angaben über die durchgeführten Wartungsläufe finden Sie auf der Registerkarte *Verlauf*.

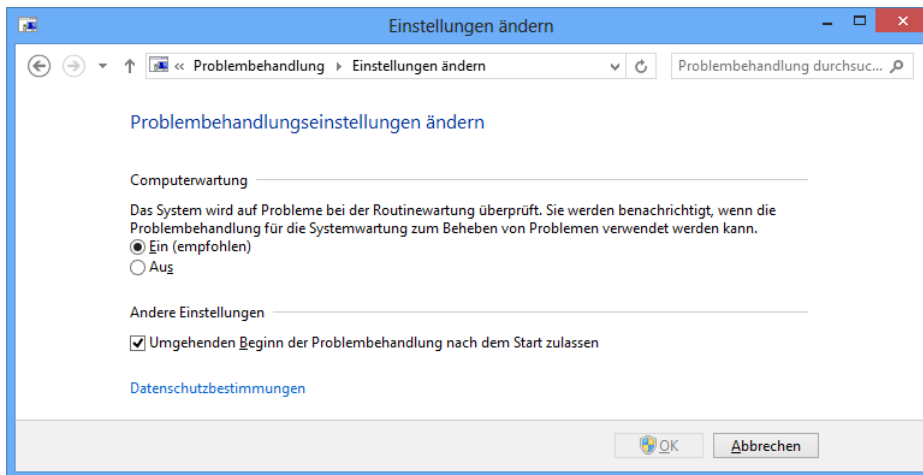


Abbildung 9.7 Einstellen, wie die Problembehandlung arbeitet

Für jeden Benutzer, der sich an einem Computer anmeldet, gelten individuelle Problembehandlungseinstellungen. So stellen Sie ein, wie die Problembehandlung arbeitet:

1. Tippen oder klicken Sie im Wartungscenter auf die Bereichsüberschrift *Wartung* und blättern Sie nach unten.

2. Tippen oder klicken Sie am unteren Ende der Seite auf *Problembehandlung*. Tippen oder klicken Sie auf der linken Seite des Fensters *Problembehandlung* auf *Einstellungen ändern*.
3. Auf der Seite *Einstellungen ändern* (Abbildung 9.7) sind die aktuellen Einstellungen für die Problembehandlung aufgeführt. In der Standardeinstellung prüft Windows in regelmäßigen Abständen, ob häufig vorkommende Wartungsprobleme vorliegen, und zeigt Erinnerungen an, wenn das Problembehandlungsmodul des Systems in der Lage ist, Probleme zu beseitigen. Zum Beispiel benachrichtigt das Problembehandlungsmodul den Benutzer, wenn es unbenutzte Dateien und Verknüpfungen gibt, die entfernt werden können.
4. Sobald der Benutzer ein Problembehandlungsmodul startet, wird die Problembehandlung in der Standardeinstellung automatisch eingeleitet. Möchten Sie, dass der Benutzer den Start der Problembehandlung bestätigen muss, können Sie das Kontrollkästchen *Umgehenden Beginn der Problembehandlung nach dem Start zulassen* deaktivieren.
5. Tippen oder klicken Sie auf *OK*, um Ihre Einstellungen zu speichern.

Die Problembehandlungsmodule unterstützen die automatische Identifizierung und Behebung von Problemen mit dem Betriebssystem. Die automatische Problembehandlung ist auf Windows PowerShell und zugehörige Systemdienste angewiesen. Solange PowerShell installiert ist (das ist standardmäßig der Fall) und die benötigten Dienste verfügbar sind, müsste die automatische Problembehandlung funktionieren. Es stehen folgende Standardproblembehandlungsmodule zur Verfügung:

- **DirectAccess** Diagnostiziert und beseitigt Probleme, die verhindern, dass der Computer mit DirectAccess eine Verbindung mit dem Arbeitsplatz herstellt.
- **Hardware und Geräte** Diagnostiziert und beseitigt Probleme, die verhindern, dass der Computer ein Gerät richtig benutzen kann.
- **Heimnetzgruppe** Diagnostiziert und beseitigt Probleme, die verhindern, dass der Computer andere Computer oder freigegebene Dateien aus einer Heimnetzgruppe findet.
- **Eingehende Verbindungen** Diagnostiziert und beseitigt Probleme, die eingehende Verbindungen blockieren.
- **Internetverbindungen** Diagnostiziert und beseitigt Probleme, die verhindern, dass der Computer eine Verbindung zum Internet herstellt und auf das Web zugreift.
- **Leistung von Internet Explorer** Diagnostiziert und behebt Probleme, die sich auf die Leistung des Internet Explorers auswirken.
- **Internet Explorer-Sicherheit** Erkennt Probleme in den Einstellungen, die eventuell die Sicherheit des Computers und des Benutzers gefährden, wenn er im Web surft.
- **Netzwerkkarte** Diagnostiziert und beseitigt Probleme in den Bereichen von Ethernet-, WLAN- und anderen Netzwerkkarten.
- **Wiedergeben von Audiodateien** Diagnostiziert und beseitigt Probleme, die verhindern, dass der Computer Audiodateien abspielt.
- **Energieverwaltung** Diagnostiziert und beseitigt Probleme, die sich auf die Energieverwaltung des Computers auswirken.
- **Drucker** Diagnostiziert und beseitigt Probleme, die verhindern, dass der PC einen Drucker benutzt.
- **Programmkompatibilität** Diagnostiziert und beseitigt Probleme, die verhindern, dass ältere Programme auf dem Computer laufen.
- **Aufzeichnen von Audiodateien** Diagnostiziert und beseitigt Probleme, die verhindern, dass der Computer Audiodateien aufzeichnet.

- **Suche und Indizierung** Diagnostiziert und behebt Probleme mit den Such- und Indizierungsfunktionen von Windows.
- **Freigegebene Ordner** Diagnostiziert und behebt Probleme mit dem Zugriff auf freigegebene Dateien und Ordner, die auf anderen Computern liegen.
- **Systemwartung** Führt Routinewartungen aus, wenn der Benutzer dies nicht erledigt.
- **Windows Update** Diagnostiziert und beseitigt Probleme, die den Computer an der Verwendung von Windows Update hindern.

TIPP Administratoren können in den Gruppenrichtlinien Richtlinien für die Unterstützung nach Fehlern des Typs "Zugriff verweigert" konfigurieren, um Benutzern bei der Suche nach Ansprechpartnern zu helfen, wenn sie Schwierigkeiten mit dem Zugriff auf Dateien haben, und um benutzerdefinierte Fehlermeldungen anzuzeigen. Verwenden Sie die Richtlinie *Unterstützung nach "Zugriff verweigert" auf Client für alle Dateitypen aktivieren*, um diese Unterstützung zu aktivieren. Wie die Unterstützung funktionieren soll, legen Sie mit *Meldung für Fehler vom Typ "Zugriff verweigert" anpassen* fest. Diese Richtlinien sind in den administrativen Vorlagen der Computerkonfiguration unter *System\Unterstützung nach "Zugriff verweigert"* zu finden.

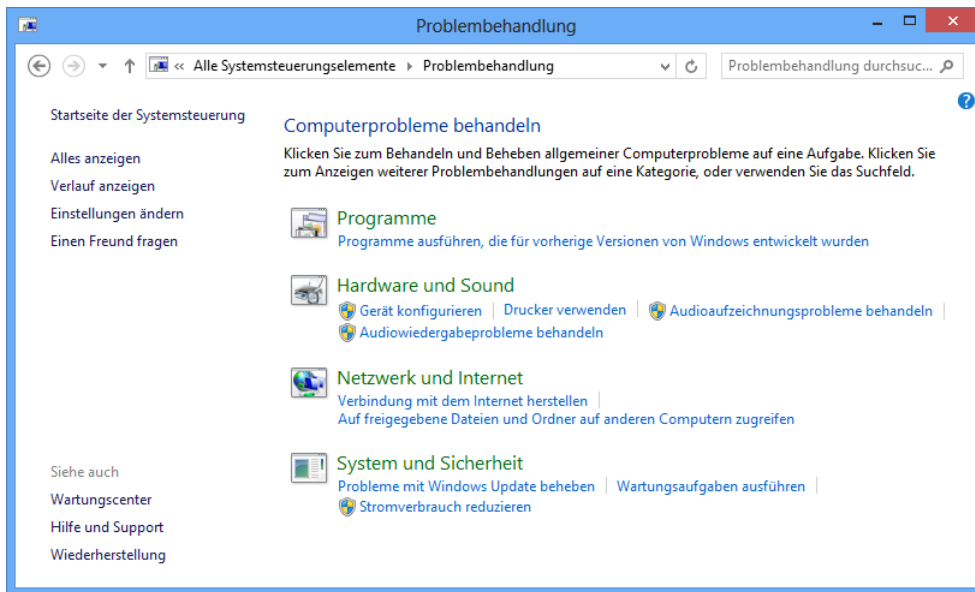


Abbildung 9.8 Anzeigen und Starten der Problembehandlungsmodule

Sie greifen im Wartungscenter auf die verfügbaren Problembehandlungsmodule zu, indem Sie nach unten blättern und dann auf *Problembehandlung* klicken. Wie in Abbildung 9.8 zu sehen, sind die Problembehandlungsmodule in Kategorien eingeteilt. Es stehen folgende Kategorien zur Verfügung:

- **Programme** Für die Behandlung von Kompatibilitätsproblemen bei Anwendungen, die für ältere Windows-Versionen entwickelt wurden
- **Hardware und Sound** Für die Behandlung von Problemen bei Hardwaregeräten, Audioaufzeichnung und Audiowiedergabe
- **Netzwerk und Internet** Für die Behandlung von Problemen mit Netzwerkverbindungen und dem Zugriff auf freigegebene Ordner auf anderen Computern

- **System und Sicherheit** Für die Behandlung von Problemen mit Windows Update, Energieverwaltung und Leistung. Tippen oder klicken Sie auf *Wartungsaufgaben ausführen*, um unbenutzte Dateien und Verknüpfungen zu entfernen und andere Routinewartungsaufgaben zu erledigen.

Tabelle 9.1 listet die Richtlinien aus dem Bereich *Administrative Vorlagen* auf, mit denen sich das Wartungscenter und damit zusammenhängende Funktionen verwalten lassen. In den Gruppenrichtlinien können Sie im Zweig *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Problembehandlung und Diagnose* konfigurieren, wie die automatische Problembehandlung und Diagnose arbeiten.

Tabelle 9.1 Richtlinien zum Verwalten des Wartungscenters und der zugehörigen Features

Richtliniennamen	Beschreibung	Zweig in <i>Administrative Vorlagen</i>
<i>Problembehandlung: Benutzerzugriff auf Onlineinhalte zur Problembehandlung auf Microsoft-Servern über die Systemsteuerung für die Problembehandlung zulassen</i>	Wenn Sie diese Richtlinie aktivieren oder nicht konfigurieren, können Benutzer, die mit dem Internet verbunden sind, auf Problembehandlungsinhalte zugreifen und danach suchen. Benutzer können auf solche Inhalte zugreifen, indem sie auf <i>Ja</i> tippen oder klicken, wenn sie im Wartungscenter aufgefordert werden, die neusten Problembehandlungsinhalte abzurufen.	<i>Computerkonfiguration</i> unter <i>System\Problembehandlung und Diagnose\Skriptdiagnose</i>
<i>Problembehandlung: Zugriff und Ausführung von Problembehandlungs-Assistenten durch Benutzer zulassen</i>	Wenn Sie diese Richtlinie aktivieren oder nicht konfigurieren, können Benutzer auf die Problembehandlungswerkzeuge im Wartungscenter zugreifen und sie ausführen.	<i>Computerkonfiguration</i> unter <i>System\Problembehandlung und Diagnose\Skriptdiagnose</i>
<i>Wartungscentersymbol entfernen</i>	Wenn Sie diese Richtlinie aktivieren, wird das Symbol des Wartungscenters nicht im Infobereich der Taskleiste angezeigt. Das verhindert allerdings nicht, dass Benutzer über die Systemsteuerung auf das Wartungscenter zugreifen. Andernfalls wird das Symbol des Wartungscenters angezeigt.	<i>Benutzerkonfiguration</i> unter <i>Startmenü und Taskleiste</i>
<i>Programm zur Verbesserung der Benutzerfreundlichkeit deaktivieren</i>	Wenn diese Richtlinie aktiviert ist, nehmen die Benutzer nicht am Programm teil. Ist diese Richtlinie deaktiviert, nehmen die Benutzer am Programm teil.	<i>Computerkonfiguration</i> unter <i>System\Internetkommunikationsverwaltung\Internetkommunikationseinstellungen</i>
<i>Zugriff auf den Bereich "Lösungen zu Leistungsproblemen" deaktivieren</i>	Wenn diese Richtlinie aktiviert ist, können die Benutzer nicht auf Lösungen zu Leistungsproblemen zugreifen. Andernfalls ist dieser Zugriff für die Benutzer möglich.	<i>Benutzer- und Computerkonfiguration</i> unter <i>System\Systemsteuerung – Leistung</i>
<i>Über blockierte Treiber benachrichtigen</i>	Wenn diese Richtlinie aktiviert oder nicht konfiguriert ist, benachrichtigt Windows die Benutzer, wenn Treiber aufgrund von Kompatibilitätsproblemen blockiert werden.	<i>Computerkonfiguration</i> unter <i>System\Problembehandlung und Diagnose\Anwendungskompatibilitätsdiagnose</i>
<i>Durch veraltete COM-Objekte verursachte Anwendungsfehler erkennen</i>	Wenn Sie diese Richtlinie aktivieren oder nicht konfigurieren, erkennt Windows, wenn Programme versuchen, veraltete COM-Objekte zu erstellen. In diesem Fall wird der Benutzer benachrichtigt.	<i>Computerkonfiguration</i> unter <i>System\Problembehandlung und Diagnose\Anwendungskompatibilitätsdiagnose</i>
<i>Durch veraltete Windows-DLLs verursachte Anwendungsfehler erkennen</i>	Wenn Sie diese Richtlinie aktivieren oder nicht konfigurieren, erkennt Windows, wenn Programme veraltete DLLs benutzen. In diesem Fall wird der Benutzer benachrichtigt.	<i>Computerkonfiguration</i> unter <i>System\Problembehandlung und Diagnose\Anwendungskompatibilitätsdiagnose</i> ►

Richtliniename	Beschreibung	Zweig in <i>Administrative Vorlagen</i>
<i>Kompatibilitätsprobleme für Anwendungen und Geräte erkennen</i>	Wenn Sie diese Richtlinie aktivieren oder nicht konfigurieren, erkennt Windows, wenn es wegen Kompatibilitätsproblemen zu Installationsfehlern, Laufzeitfehlern und blockierten Treibern kommt, und informiert die Benutzer.	<i>Computerkonfiguration</i> unter <i>System\Problembehandlung und Diagnose\Anwendungskompatibilitätsdiagnose</i>
<i>Programmkompatibilitätsmodul deaktivieren</i>	Wenn diese Richtlinie aktiviert ist, prüft Windows nicht die Kompatibilitätsdatenbank, bevor es Anwendungen startet.	<i>Computerkonfiguration</i> unter <i>Windows-Komponenten\Anwendungskompatibilität</i>
<i>Programmkompatibilitäts-Assistenten deaktivieren</i>	Wenn diese Richtlinie aktiviert ist, überwacht Windows vom Benutzer gestartete Programme während der Laufzeit nicht auf bekannte Kompatibilitätsprobleme.	<i>Benutzer- und Computerkonfiguration</i> unter <i>Windows-Komponenten\Anwendungskompatibilität</i>
<i>Berichtwarteschlange konfigurieren</i>	Wenn diese Richtlinie aktiviert und konfiguriert ist, kann ein Administrator die Warteschlange und die Benachrichtigungen im Zusammenhang mit der Fehlerberichterstattung konfigurieren.	<i>Benutzer- und Computerkonfiguration</i> unter <i>Windows-Komponenten\Windows-Fehlerberichterstattung\Erweiterte Einstellungen für Fehlerberichterstattung</i>
<i>Windows-Fehlerberichterstattung deaktivieren</i>	Wenn diese Richtlinie aktiviert ist, sendet die Windows-Fehlerberichterstattung keinerlei Informationen an Microsoft. Andernfalls sendet die Windows-Fehlerberichterstattung Daten.	<i>Benutzer- und Computerkonfiguration</i> unter <i>Windows-Komponenten\Windows-Fehlerberichterstattung</i>

Arbeiten mit den Supportdiensten

Zur Unterstützung der automatischen Diagnose und Problembehebung bietet Windows 8 verschiedene Komponenten und Tools für die Verwaltung der Diagnoseergebnisse, die Problembenachrichtigung und die Unterstützung des Benutzers an. Diese Komponenten sind alle auf die Verfügbarkeit der Supportdienste angewiesen, die mit dem Betriebssystem installiert wurden. Wenn Sie im Verwaltungsprogramm *Computerverwaltung* unter *Dienste und Anwendungen* den Knoten *Dienste* öffnen, finden Sie ein ganzes Bündel an Diensten für den Systemsupport vor.

Tabelle 9.2 bietet einen Überblick über die wichtigsten Supportdienste in Windows 8. Die Funktionen zur Problemerkennung, Fehlerbehebung und Problemlösung werden weitgehend von den Diensten *Diagnoserichtliniendienst* und *Diagnosesystemhost* unterstützt. Ein dritter Dienst, der *Diagnosediensthost*, wird nur bei Bedarf gestartet.

Wie Sie schon an der Zahl der Supportdienste erkennen können, ist das integrierte automatische Hilfesystem von Windows 8 recht vielschichtig. Das System wurde so konzipiert, dass es automatisch den Zustand des Computersystems überwacht, vorbeugende Maßnahmen ergreift und Probleme meldet, damit sie behoben werden können. Im Systemmonitor und der Zuverlässigkeitsüberwachung werden weitere Leistungs- und Zuverlässigkeitsdaten verfolgt.

Supportdienste sind die Grundlage der erweiterten Supportfunktionen von Windows 8. Wenn wichtige Dienste nicht ausgeführt werden oder falsch konfiguriert sind, können sich Probleme bei der Verwendung bestimmter Supportfunktionen ergeben.

Sie können diese und andere Dienste in der Computerverwaltung überprüfen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit*, dann auf *Verwaltung* und schließlich doppelt auf *Computerverwaltung*.

Tabelle 9.2 Supportdienste in Windows 8

Name	Beschreibung
<i>Anwendungserfahrung</i>	Verarbeitet Anwendungs-kompatibilitäts-Cacheanforderungen beim Start von Anwendungen.
<i>Anwendungsinformationen</i>	Erleichtert das Ausführen von interaktiven Anwendungen mit zusätzlichen Administratorrechten.
<i>Anwendungsverwaltung</i>	Verarbeitet Installations-, Deinstallations- und Auflistungsanforderungen für Software, die über Gruppenrichtlinien bereitgestellt wird.
<i>Aufgabenplanung</i>	Ermöglicht einem Benutzer, automatische Aufgaben auf diesem Computer zu konfigurieren und zu planen.
<i>Benachrichtigungsdienst für Systemereignisse</i>	Überwacht Systemereignisse und bietet Benachrichtigungsdienste.
<i>Benutzerprofildienst</i>	Ist zuständig für das Laden und Entladen von Benutzerprofilen.
<i>Designs</i>	Ermöglicht dem Computer, Designs zu verwenden, und stellt die Benutzeroberfläche zum Verwalten der Designs bereit.
<i>Diagnosediensthos</i>	Ermöglicht Diagnosefunktionen, die im Kontext von <i>LOKALER DIENST</i> ausgeführt werden müssen.
<i>Diagnoserichtliniendienst</i>	Ermöglicht die Problemerkennung, Problembehandlung und Lösung für Windows-Komponenten.
<i>Diagnosesystemhos</i>	Ermöglicht Diagnosefunktionen, die im Kontext von <i>SYSTEM</i> ausgeführt werden müssen.
<i>Intelligenter Hintergrundübertragungsdienst</i>	Überträgt Dateien im Hintergrund unter Verwendung von ungenutzter Netzwerkbandbreite.
<i>Programmkompatibilitäts-Assistent-Dienst</i>	Bietet Unterstützung für den Programmkompatibilitäts-Assistenten.
<i>Sekundäre Anmeldung</i>	Ermöglicht das Starten von Prozessen mit verschiedenen Anmeldeinformationen.
<i>Superfetch</i>	Verwaltet und verbessert die Systemleistung durch das Vorabladen von Komponenten und Anwendungsdaten anhand des Verwendungsmusters.
<i>Unterstützung in der Systemsteuerung unter Lösungen für Probleme</i>	Unterstützt das Anzeigen, Senden und Löschen von Problembereichen auf Systemebene.
<i>Windows Modules Installer</i>	Unterstützt Windows-Updates von empfohlenen und optionalen Komponenten.
<i>Windows Update</i>	Ermöglicht die automatische Aktualisierung von Windows-Komponenten und anderen Programmen.
<i>Windows-Ereignisprotokoll</i>	Ist zuständig für die Protokollierung von Ereignissen.
<i>Windows-Fehlerberichterstattungsdienst</i>	Ermöglicht die Berichterstattung über Fehler bei nicht mehr reagierenden Programmen und die Angabe von Lösungen.
<i>Windows-Remoteverwaltung (WS-Verwaltung)</i>	Ermöglicht den Remotebetrieb in der Windows PowerShell und aktiviert das Protokoll WS-Verwaltung für die Remoteverwaltung.
<i>Windows-Verwaltungsinstrumentation</i>	Bietet den Zugriff auf Systemverwaltungsinformationen.
<i>Windows-Zeitgeber</i>	Synchronisiert die Systemzeit mit Greenwich Mean Time.

2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Verbindung mit anderem Computer herstellen*. Nun können Sie auswählen, auf welchem System Sie die Dienste verwalten wollen.
3. Erweitern Sie den Knoten *Dienste und Anwendungen*, indem Sie auf das zugehörige Dreiecksymbol tippen oder klicken. Wählen Sie *Dienste* aus (Abbildung 9.9). Sie müssten nun eine vollständige Liste aller Dienste angezeigt bekommen, die auf dem System installiert sind. Diese Liste ist standardmäßig nach dem Dienstnamen sortiert.

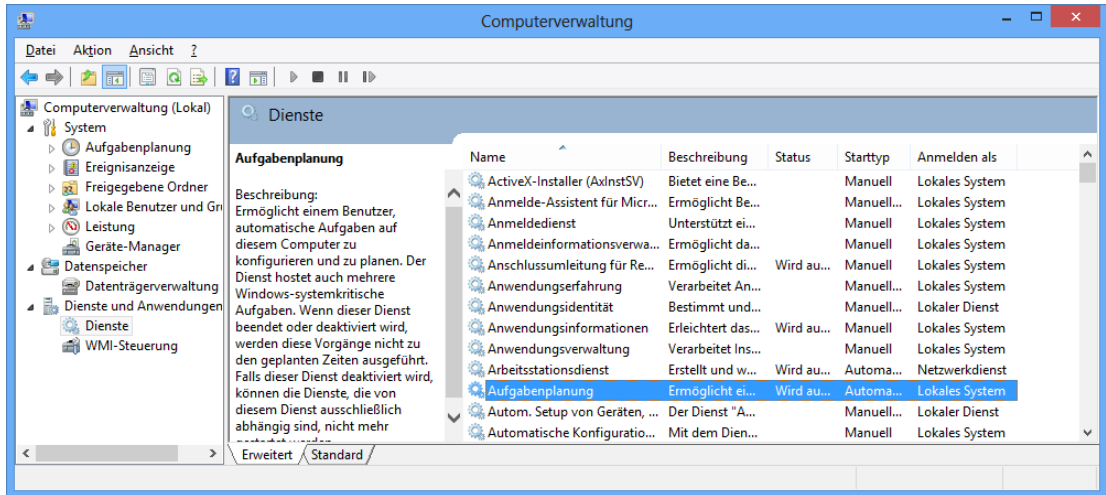


Abbildung 9.9 Verwalten von Diensten in Windows 8

Die wichtigsten Spalten in dieser Liste sind:

- **Name** Der Name des Dienstes. Hier werden nur Dienste aufgeführt, die auf dem System installiert sind. Tippen oder klicken Sie doppelt auf einen Eintrag, um seine Startoptionen zu konfigurieren.
 - **Beschreibung** Eine kurze Beschreibung des Dienstes und seiner Aufgaben.
 - **Status** Gibt an, ob der Dienst läuft, angehalten oder beendet wurde. (Wurde der Dienst beendet, zeigt das Feld keinen Text an.)
 - **Starttyp** Die Starttypeinstellung für den Dienst. Automatische Dienste werden beim Systemstart ausgeführt. Benutzer oder andere Dienste starten manuelle Dienste. Deaktivierte Dienste sind ausgeschaltet und können nicht gestartet werden, während sie deaktiviert sind.
 - **Anmelden als** Das Konto, unter dem sich der Dienst anmeldet. Das Standardkonto ist in den meisten Fällen *SYSTEM*.
4. Das Fenster *Dienste* hat zwei Ansichten: *Erweitert* und *Standard*. Sie schalten die Ansicht mit den Registerkarten unten im Fenster *Dienste* um. In der erweiterten Ansicht werden Verknüpfungen zum Verwalten der Dienste angezeigt. Tippen oder klicken Sie auf *starten*, um einen beendeten Dienst zu starten. Tippen oder klicken Sie auf *neu starten*, um einen Dienst zu beenden und anschließend neu zu starten. Wenn Sie einen Dienst in der erweiterten Ansicht auswählen, wird außerdem eine Dienstbeschreibung angezeigt, in der die Aufgaben des Dienstes zusammengefasst sind.

Starten, Beenden und Anhalten von Diensten

Als Administrator müssen Sie Windows 8-Dienste häufig starten, beenden oder anhalten. Gehen Sie dazu wie folgt vor:

1. Erweitern Sie in der Computerverwaltung den Knoten *Dienste und Anwendungen*, indem Sie auf das zugehörige Dreiecksymbol klicken, und wählen Sie den Knoten *Dienste* aus.
2. Klicken Sie mit der rechten Maustaste auf den Dienst, den Sie verwalten wollen, oder halten Sie ihn gedrückt, und wählen Sie *Starten*, *Beenden* oder *Anhalten*.

HINWEIS

Sie können auch *Neu starten* wählen, damit Windows den Dienst beendet und nach einer kurzen Pause wieder startet. Falls Sie einen Dienst angehalten haben, können Sie mit dem Befehl *Fortsetzen* seine normale Ausführung wiederaufnehmen. Wenn Dienste ausfallen, die automatisch gestartet werden sollen, wird im Statusfeld ein leerer Eintrag angezeigt, und Sie erhalten gewöhnlich eine Benachrichtigung. Dienstaussfälle können auch in den Ereignisprotokollen des Systems aufgeführt werden. In Windows 8 lassen sich Aktionen zur automatischen Behandlung von Dienstaussfällen konfigurieren. Beispielsweise kann Windows 8 versuchen, den Dienst für Sie neu zu starten.

Konfigurieren des Dienststartmodus

Sie können festlegen, ob Windows 8 Dienste manuell oder automatisch startet. Sie können Dienste durch Deaktivieren auch dauerhaft ausschalten. Zum Konfigurieren des Dienststarts gehen Sie wie folgt vor:

1. Erweitern Sie in der Computerverwaltung den Knoten *Dienste und Anwendungen*, indem Sie auf das zugehörige Dreiecksymbol klicken, und wählen Sie den Knoten *Dienste* aus.
2. Klicken Sie mit der rechten Maustaste auf den Dienst, den Sie konfigurieren wollen, oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Eigenschaften*.
3. Wählen Sie auf der Registerkarte *Allgemein* in der Dropdownliste *Starttyp* eine Startoption aus und tippen oder klicken Sie auf *OK*. Es stehen folgende Einträge zur Auswahl:
 - **Automatisch** Der Dienst wird beim Systemstart gestartet.
 - **Automatisch (Verzögerter Start)** Mit dem Starten des Dienstes nach dem Systemstart wird gewartet, bis alle unverzögerten Dienste gestartet wurden.
 - **Manuell** Der Dienst kann manuell gestartet werden.
 - **Deaktiviert** Schaltet den Dienst aus.

Konfigurieren der Dienstanmeldung

Sie können festlegen, dass sich Windows 8-Dienste unter einem Systemkonto oder als bestimmte Benutzer anmelden. Gehen Sie dazu jeweils wie folgt vor:

1. Erweitern Sie in der Computerverwaltung den Knoten *Dienste und Anwendungen*, indem Sie auf das zugehörige Dreiecksymbol klicken, und wählen Sie den Knoten *Dienste* aus.
2. Klicken Sie mit der rechten Maustaste auf den Dienst, den Sie konfigurieren wollen, oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Eigenschaften*.
3. Wählen Sie die Registerkarte *Anmelden* aus. Nehmen Sie eine der folgenden Einstellungen vor und klicken Sie danach auf *OK*.
 - Wählen Sie **Lokales Systemkonto** aus, wenn sich der Dienst unter Verwendung des Systemkontos anmelden soll (die Standardeinstellung bei den meisten Diensten). Verwendet der Dienst eine Benutzerschnittstelle, über die Eingaben vorgenommen werden können, wählen Sie **Datenaus-**

tausch zwischen Dienst und Desktop zulassen, um Benutzern die Steuerung über die Schnittstelle des Dienstes zu ermöglichen.

- Wählen Sie *Dieses Konto* aus, wenn sich der Dienst unter einem bestimmten Benutzerkonto anmelden soll. Vergessen Sie nicht, in die vorhandenen Textfelder Kontoname und Kennwort einzugeben. Suchen Sie mit der Schaltfläche *Durchsuchen* gegebenenfalls nach einem Benutzerkonto. Tippen oder klicken Sie auf *OK*.

Konfigurieren der Dienstwiederherstellung

Während der Installation konfiguriert Windows 8 für kritische Systemdienste eine automatische Wiederherstellung. In den meisten Fällen sind kritische Dienste daher so konfiguriert, dass sie automatisch neu gestartet werden, falls der Dienst unerwartet beendet wird. Sie können diese Einstellungen nicht ändern, weil sie im entsprechenden Dialogfeld abgeblendet sind.

Gehen Sie folgendermaßen vor, um die Wiederherstellungsoptionen für andere Dienste zu konfigurieren:

1. Erweitern Sie in der Computerverwaltung den Knoten *Dienste und Anwendungen*, indem Sie auf das zugehörige Dreiecksymbol klicken, und wählen Sie den Knoten *Dienste* aus.
2. Klicken Sie mit der rechten Maustaste auf den Dienst, den Sie konfigurieren wollen, oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Eigenschaften*.
3. Tippen oder klicken Sie auf die Registerkarte *Wiederherstellung*.
4. Nun können Sie Wiederherstellungsoptionen für den ersten, den zweiten und weitere Fehler konfigurieren. Es sind folgende Optionen verfügbar:
 - **Keine Aktion durchführen** Das Betriebssystem unternimmt bei diesem Fehler keinen Versuch zur Wiederherstellung. Bei vorherigen oder Folgefehlern wird allerdings eventuell weiterhin eine Wiederherstellung versucht.
 - **Dienst neu starten** Beendet den Dienst und startet ihn nach einer kurzen Pause neu.
 - **Ein Programm ausführen** Ermöglicht bei Auftreten eines Fehlers das Ausführen eines Programms oder Skripts. Bei diesem Skript kann es sich um eine Batchdatei oder ein Windows-Skript handeln. Bei Auswahl dieser Option geben Sie den vollständigen Pfad des auszuführenden Programms an und legen alle erforderlichen Befehlszeilenparameter fest, die beim Programmstart übergeben werden sollen.
 - **Computer neu starten** Fährt den Computer herunter und startet ihn anschließend neu. Vor der Auswahl dieser Option sollten Sie die Start- und Wiederherstellungsoptionen prüfen. Das System sollte die Standardeinstellungen schnell und automatisch wählen.

TIPP

Wenn Sie Wiederherstellungsoptionen für kritische Dienste konfigurieren, können Sie versuchen, bei den ersten beiden Versuchen den Dienst und beim dritten Versuch den Computer neu zu starten.

5. Konfigurieren Sie die weiteren Optionen so, wie es für die bisher ausgewählten Wiederherstellungsoptionen erforderlich ist, und tippen oder klicken Sie auf *OK*. Wenn Sie als Wiederherstellungsoption die Ausführung eines Programms gewählt haben, müssen Sie im Bereich *Programm ausführen* die Optionen festlegen. Wenn Sie den Neustart des Dienstes gewählt haben, müssen Sie die Verzögerung des Neustarts festlegen. Windows 8 wartet nach Beendigung des Dienstes die angegebene Zeit, bevor versucht wird, den Dienst neu zu starten. In den meisten Fällen sollte eine Verzögerung von 1 bis 2 Minuten genügen.

Deaktivieren nicht benötigter Dienste

Als Administrator sind Sie für die Computer- und Netzwerksicherheit verantwortlich, und nicht benötigte Dienste stellen ein potenzielles Sicherheitsrisiko dar. In vielen Organisationen finden sich beispielsweise Computer, auf denen die Publishingdienste World Wide Web (WWW), Simple Mail Transfer Protocol (SMTP) und File Transfer Protocol (FTP) ausgeführt werden, obwohl sie nicht benötigt werden. Die Dienste ermöglichen jedoch den Zugriff auf den Computer durch anonyme Benutzer und können Computer für Angriffe anfällig machen, falls sie nicht ordnungsgemäß konfiguriert wurden.

Falls bestimmte Dienste nicht benötigt werden, haben Sie verschiedene Möglichkeiten. Wenn nicht benötigte Dienste über Features installiert wurden, können Sie das zugehörige Feature entfernen, um die unnötige Komponente und ihre zugehörigen Dienste zu entfernen. Oder Sie deaktivieren einfach die nicht verwendeten Dienste.

Gehen Sie folgendermaßen vor, um einen Dienst zu deaktivieren:

1. Erweitern Sie in der Computerverwaltung den Knoten *Dienste und Anwendungen*, indem Sie auf das zugehörige Dreiecksymbol klicken, und wählen Sie den Knoten *Dienste* aus.
2. Klicken Sie mit der rechten Maustaste auf den Dienst, den Sie konfigurieren wollen, oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Eigenschaften*.
3. Wählen Sie auf der Registerkarte *Allgemein* im Dropdownlistenfeld *Starttyp* die Option *Deaktiviert* aus.

Das Deaktivieren eines Dienstes führt nicht dazu, dass ein zurzeit ausgeführter Dienst angehalten wird. Es wird lediglich verhindert, dass der Dienst beim nächsten Computerstart gestartet wird. Zur Beseitigung dieses Sicherheitsrisikos tippen oder klicken Sie auf der Registerkarte *Allgemein* des Eigenschaftendialogfelds auf *Beenden* und anschließend auf *OK*.

Verwalten von Diensten mithilfe von Richtlinieneinstellungen

Statt Dienste auf einzelnen Computern zu verwalten, können Sie auch Elemente in Gruppenrichtlinien einsetzen, um die Dienste auf allen Computern zu konfigurieren, die ein bestimmtes Gruppenrichtlinienobjekt (Group Policy Object, GPO) verarbeiten. Wenn Sie einen Dienst über Richtlinieneinstellungen konfigurieren, ist der Standardwert in den meisten Fällen *Keine Änderung*, das heißt, dass die Einstellung nur geändert wird, wenn Sie einen anderen Wert zuweisen. Ähnlich wie bei der manuellen Verwaltung von Diensten haben Sie folgende Möglichkeiten, wenn Sie dafür Gruppenrichtlinieneinstellungen verwenden:

- Starten, Beenden und Neustarten von Diensten
- Einstellen des Starttyps auf *Manuell*, *Automatisch*, *Automatisch (Verzögerter Start)* oder *Deaktiviert*
- Auswählen des verwendeten Anmeldekontos
- Einrichten der Wiederherstellungsoptionen, um auf Dienstaussfälle zu reagieren

Gehen Sie folgendermaßen vor, um ein Element zu erstellen, mit dem Sie einen Dienst steuern:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie den Knoten *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen*.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Dienste* oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Neu/Dienst*. Daraufhin öffnet sich das Eigenschaftendialogfeld für den neuen Dienst (Abbildung 9.10).

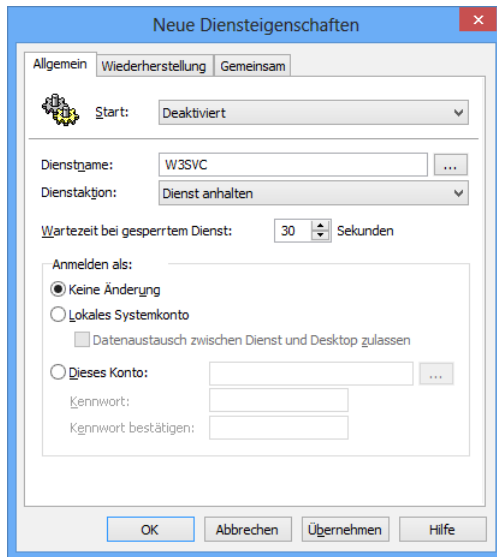


Abbildung 9.10 Anpassen eines Dienstes mit einem Gruppenrichtlinienobjekt

3. Geben Sie im Feld *Dienstname* den Namen des Dienstes ein, den Sie konfigurieren wollen. Der Dienstname unterscheidet sich vom Anzeigenamen des Dienstes. Wenn Sie nicht sicher sind, wie der Name eines Dienstes lautet, können Sie auf die Schaltfläche rechts neben dem Textfeld tippen oder klicken und den Dienst dann aus der Liste der verfügbaren Dienste auf Ihrem Verwaltungscomputer auswählen. Denken Sie daran, dass manche Dienste, die auf Ihrem Verwaltungscomputer laufen, unter Umständen nicht auf den Computern der Benutzer zur Verfügung stehen, und umgekehrt.
4. Konfigurieren Sie den Dienst mit den verfügbaren Optionen so, wie er auf den Computern der Benutzer eingerichtet werden soll. Es werden nur Einstellungen verarbeitet, in denen Sie einen anderen Wert als *Keine Änderung* auswählen.
5. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Meist ist es am sinnvollsten, die Dienstkonfiguration nur einmal anzuwenden. Aktivieren Sie in diesem Fall das Kontrollkästchen *Nur einmal anwenden*.
6. Tippen oder klicken Sie auf **OK**. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Installieren und Warten von Geräten: Die Grundlagen

Viele verschiedene Arten von Geräten können in Computer eingebaut oder mit Computern verbunden werden. Die wichtigsten Gerätearten sind folgende:

- **Erweiterungskarten/Adapter** Karten und Adapter werden innerhalb des Computergehäuses in Erweiterungssteckplätze des Mainboards eingesteckt, oder im Fall eines Laptops in Erweiterungssteckplätze an den Seiten des Gehäuses. Viele Karten und Adapter haben weitere Steckverbinder, an die andere Geräte angeschlossen werden können.

- **Interne Laufwerke** Viele unterschiedliche Laufwerksarten lassen sich installieren, von DVD-Laufwerken bis hin zu Festplattenlaufwerken. Interne Laufwerke werden gewöhnlich mit zwei Kabeln angeschlossen. Eines wird mit dem Mainboard verbunden und sorgt für die Datenübertragung und Steuerung, das andere für den Strom.
- **Externe Laufwerke und Geräte** Externe Laufwerke und Geräte werden über die entsprechenden Anschlüsse mit dem Computer verbunden. Dabei kann es sich um Anschlüsse aus den Anfangszeiten des PCs handeln, wie LPT1 oder COM1, um einen Anschluss, den Sie mit einer speziellen Erweiterungskarte in den Computer eingebaut haben, oder um einen seriellen Hochleistungsanschluss wie einen USB-Anschluss (Universal Serial Bus), eSata, oder um einen IEEE-1394-Anschluss, gewöhnlich FireWire genannt. Drucker, Scanner, USB-Flashlaufwerke, Smartphones und die meisten Digitalkameras lassen sich als externe Geräte anschließen.
- **Speicher** Speicherchips werden benutzt, um den physischen Arbeitsspeicher im Computer zu erweitern. Speicher kann zum Mainboard oder einem bestimmten Gerät hinzugefügt werden, etwa einer Grafikkarte. Am häufigsten wird Speicher in Form von RAM (Random Access Memory) benutzt.

Die Konfiguration von Hardwaregeräten wird in Windows 8 nicht in derselben Weise verwaltet wie in Windows XP und älteren Windows-Versionen. Geräte, die bereits im Computer installiert sind, aber bei einer Aktualisierung oder Installation des Betriebssystems nicht erkannt werden, werden anders konfiguriert als neu installierte Geräte.

Installieren vorhandener Geräte

Windows 8 erkennt automatisch Geräte, die bei einer Aktualisierung oder Installation des Betriebssystems nicht installiert wurden. Wurde ein Gerät nicht installiert, weil Windows 8 keinen passenden Treiber zur Verfügung stellen konnte, erkennt das integrierte Hardwarediagnosetool in vielen Fällen trotzdem die Hardware und verwendet dann das automatische Updatesystem, um den passenden Treiber das nächste Mal anzufordern, wenn Windows Update ausgeführt wird. Das geht natürlich nur, wenn Windows Update aktiviert ist und Sie nicht nur die Aktualisierung des Betriebssystems zugelassen haben, sondern auch die Aktualisierung von Treibern.

Treiberupdates können zwar automatisch über Windows Update heruntergeladen werden, sie werden dann aber nicht automatisch installiert. Nach der Aktualisierung oder Installation des Betriebssystems sollten Sie nach Treiberupdates suchen und sie installieren, bevor Sie andere Methoden zur Installation von Gerätetreibern ausprobieren. Eine ausführlichere Besprechung der automatischen Aktualisierung erfolgt zwar erst in Kapitel 10, »Erledigen von Wartungs- und Supportaufgaben«, aber die Grundschrirte sind folgende:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*.
2. Tippen oder klicken Sie in *Windows Update* auf die Schaltfläche *Nach Updates suchen*.

Typische Gerätetreiberupdates werden als optionale Updates eingestuft. Ausnahmen sind unverzichtbare Treiber, wie Video-, Sound- und Festplattentreiber. Daher ist es sinnvoll, alle verfügbaren Updates zu berücksichtigen, und nicht nur die wichtigen, wenn es um verfügbare Treiber geht. Zur Installation der verfügbaren Treiberupdates gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*.

- Tippen oder klicken Sie im linken Fensterabschnitt von Windows Update auf *Nach Updates suchen*. Wenn Windows 8 die Updateprüfung beendet hat, wird vielleicht angezeigt, dass nicht nur wichtige Updates verfügbar sind, sondern auch optionale Updates (Abbildung 9.11). Tippen oder klicken Sie auf *Updates installieren*, um die wichtigen Updates zu installieren.

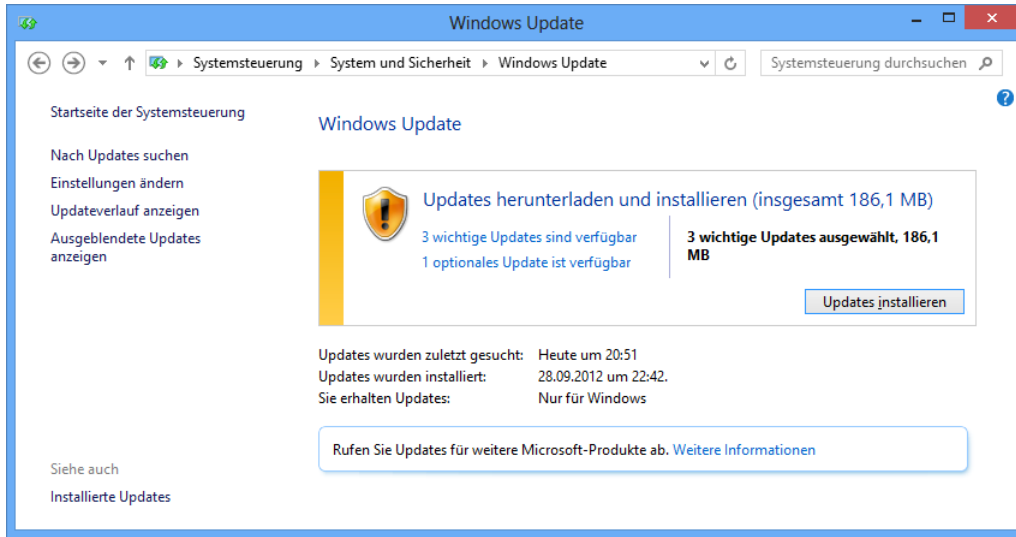


Abbildung 9.11 Nach Updates suchen

- Weil Treiberupdates normalerweise als optional aufgelistet werden, sollten Sie prüfen, ob irgendwelche optionalen Updates zur Verfügung stehen. Ist das der Fall, können Sie auf den zugehörigen Link tippen oder klicken (Abbildung 9.12). Möglicherweise stellt sich dann heraus, dass es sich bei dem optionalen Update um ein Treiberupdate handelt.

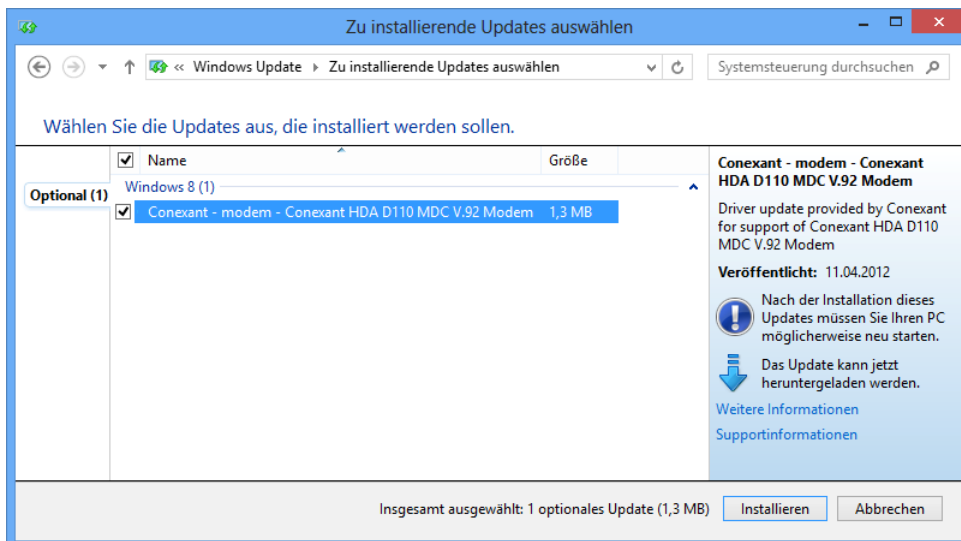


Abbildung 9.12 Auswählen eines Updates, das installiert werden soll

4. Standardmäßig werden optionale Updates nicht zur Installation vorgewählt. Wenn Sie sicherstellen möchten, dass ein bestimmtes Update installiert wird, aktivieren Sie das entsprechende Kontrollkästchen. Tippen oder klicken Sie dann auf OK, um die ausgewählten Updates herunterzuladen und zu installieren.

Nach der Installation des Gerätetreibers sollte Windows 8 die Hardware innerhalb weniger Minuten automatisch erkennen und das Gerät installieren. Kann Windows 8 das Gerät zwar erkennen, aber nicht automatisch installieren, wird unter Umständen eine Lösung im Wartungszentrum aufgeführt. Dann können Sie die gefundene Lösung überprüfen.

Installieren von internen Geräten, USB-, FireWire- und eSATA-Geräten

Die meisten neuen Geräte sind Plug & Play-kompatibel. Das bedeutet, dass sich das neue Gerät mit einer der folgenden Methoden sehr einfach installieren lassen sollte:

- Lesen Sie bei einem internen Gerät die Installationsanleitung des Hardwareherstellers. Unter Umständen müssen Sie die Gerätetreibersoftware installieren, bevor Sie das Gerät anschließen. Dann fahren Sie den Computer herunter und trennen ihn vom Stromnetz, bauen das Gerät in den vorgesehenen Steckplatz ein oder verbinden es mit dem Computer, schalten den Computer wieder ein und lassen Windows 8 das Gerät automatisch erkennen.
- Handelt es sich um ein USB-, FireWire- oder eSATA-Gerät, verbinden Sie es einfach an einem passenden Anschluss mit dem Computer und überlassen die automatische Erkennung des Geräts Windows 8.

HINWEIS Windows 8 erwartet, dass USB-, FireWire- und eSATA-Geräte Plug & Play-kompatibel sind. Ist das bei einem Gerät nicht der Fall, gelingt es möglicherweise, das Gerät mithilfe von Software zu installieren, die der Hersteller zur Verfügung stellt.

Je nach Gerät sollte Windows 8 das neue Gerät automatisch erkennen und einen passenden Treiber aus seinem Vorrat installieren. Benachrichtigungen erfolgen nur, wenn es ein Problem gibt. Normalerweise erfolgt die Installation im Hintergrund.

Anschließend sollte das Gerät ohne Probleme funktionieren. Das ist zumindest der Grundgedanke, aber es läuft nicht immer alles ganz so einfach. Die automatische Erkennung und Installation kann nur erfolgreich sein, wenn das Gerät Plug & Play-kompatibel ist und ein passender Gerätetreiber zur Verfügung steht.

Windows 8 enthält in seiner Standardkonfiguration viele Gerätetreiber. Wenn sich einer dieser Treiber eignet, sollte das Gerät automatisch installiert werden. Ist eine Aktualisierung der Treiber mit Windows Update zulässig, überprüft Windows 8 mit Windows Update automatisch, ob neue Treiber verfügbar sind, sobald Sie ein neues Gerät anschließen oder Windows das Gerät erstmals erkennt. Da Windows Update Gerätetreiber nicht automatisch installiert, müssen Sie selbst überprüfen, ob neue Gerätetreiber verfügbar sind, die Sie installieren können.

HINWEIS Einzelheiten über die Verwendung von Windows Update zur automatischen Suche nach Gerätetreibern finden Sie im Abschnitt »Die Registerkarte Hardware« von Kapitel 2, »Konfigurieren von Windows 8-Computern«. Wie in Kapitel 10 beschrieben, muss Windows Update aktiviert sein, damit diese Suche erfolgen kann.

Dass ein Gerät installiert wurde, wissen Sie normalerweise, weil sie es verwenden können. Von der Verfügbarkeit des Geräts können Sie sich auch in *Geräte und Drucker* überzeugen. Um *Geräte und Drucker* zu öffnen, tippen oder klicken in der Systemsteuerung unter der Überschrift *Hardware und Sound* auf *Geräte und Drucker anzeigen*.

Es kommt gelegentlich vor, dass Windows 8 das neue Gerät automatisch erkennt, aber bei der Gerätetreiberinstallation Probleme auftreten. Wenn das geschieht, schlägt die Installation ohne Meldung fehl. Dass die Installation nicht richtig erfolgt ist, erkennen Sie daran, dass das Gerät nicht verfügbar ist. In *Geräte und Drucker* sollten Sie Warnsymbole für den Computer und das Gerät sehen (Abbildung 9.13). In diesem Fall sehen Sie wahrscheinlich eine Fehlermeldung wie die folgende, wenn Sie das Gerät antippen oder die Maus über das Gerätesymbol schieben:

Gerätestatus: Treiber ist nicht verfügbar

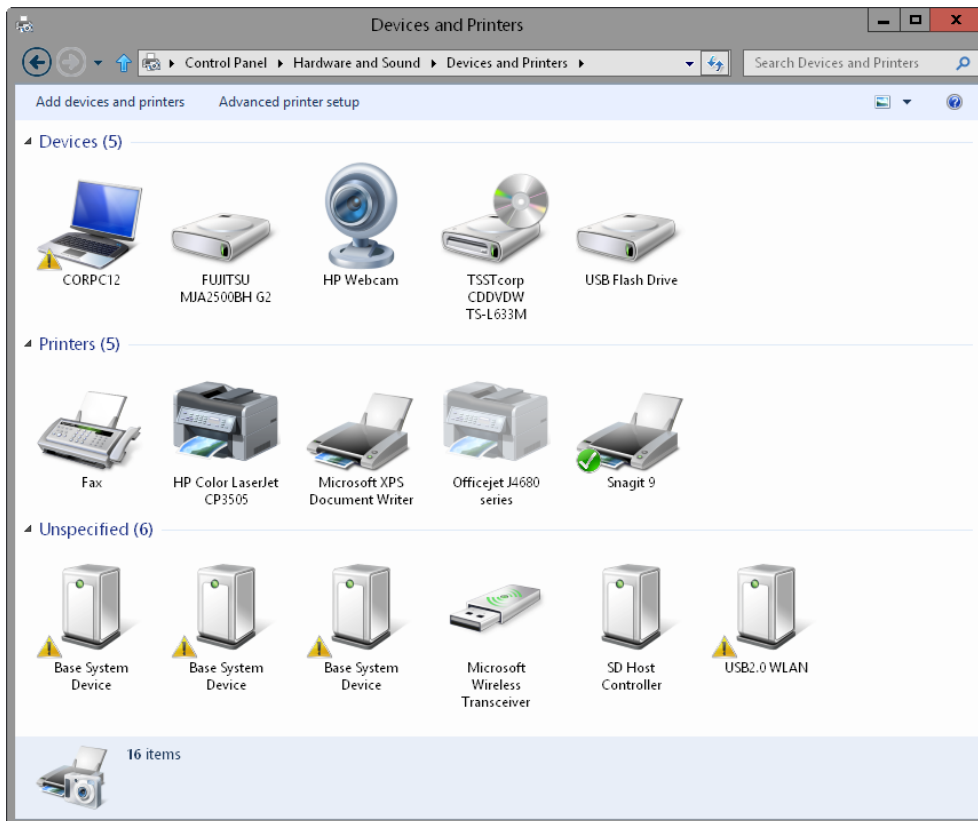


Abbildung 9.13 Beim Installieren des Geräts ist ein Fehler aufgetreten

Wenn Sie den Computer antippen oder anklicken, erscheint im Detailbereich außerdem die Statusanzeige *Problembehandlung erforderlich*.

Dasselbe können Sie auch bei den Geräten machen, die Sie zu installieren versuchen. Wenn Sie das Computersymbol antippen oder die Maus darüber schieben, sehen Sie eine Fehlermeldung. Wenn Sie das Gerät antippen oder anklicken, erscheint im Detailbereich die Statusanzeige *Problembehandlung erforderlich*. Außerdem sehen Sie vielleicht eine Statusmeldung wie die folgende:

Status: Installation unvollständig. Verbindung mit dem Internet herstellen.

Um mit der Problembeseitigung zu beginnen, tippen oder klicken Sie auf *Problembeseitigung*. Diese Option ist oben im Fenster *Geräte und Drucker* zu sehen, wenn Sie den Computer oder das Gerät auswählen. Die Problembeseitigung führt Sie Schritt für Schritt durch die Prozedur. Der wahrscheinlichste Grund für eine fehlgeschlagene Geräteinstallation ist es wohl, dass der Gerätetreiber noch aus dem Internet heruntergeladen und installiert werden muss. Die Problembeseitigung sollte dies relativ schnell erkennen und Sie auffordern, den Treiber zu installieren (Abbildung 9.14).

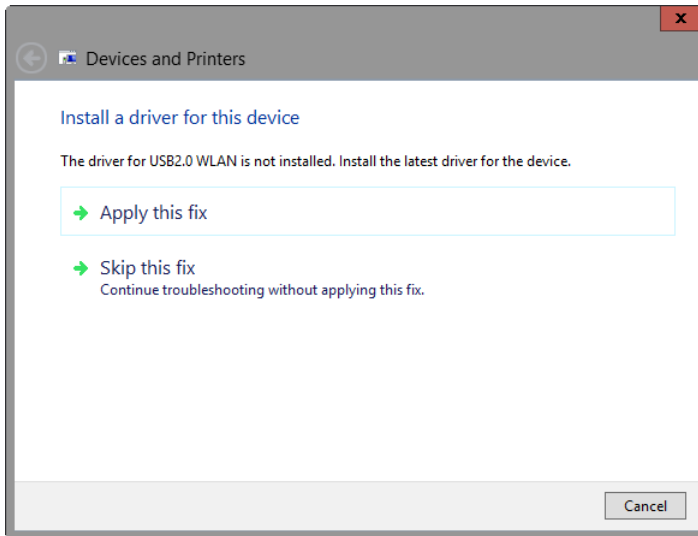


Abbildung 9.14 Windows zeigt im Wartungszentrum eine mögliche Lösung an

Falls Windows 8 das Gerät nicht erkennt und installiert, sollten Sie auf der Website des Herstellers nach kompatibler Installationssoftware suchen. Haben Sie Installationssoftware für das Gerät gefunden, können Sie die Software ausführen und dann den angezeigten Anweisungen folgen. Dann müsste das Gerät einwandfrei installiert werden.

HINWEIS Wenn Windows das Gerät nicht installieren kann, liegt vielleicht ein Problem damit oder mit dem Treiber vor, oder ein Konflikt mit vorhandener Hardware. Weitere Einzelheiten über die Problembeseitigung finden Sie im Abschnitt »Beseitigen von Hardwareproblemen« weiter unten in diesem Kapitel.

Nachdem Sie ein Gerät erfolgreich installiert haben, fallen in gewissen Abständen Wartungsarbeiten für das Gerät und seine Treiber an. Wenn ein neuer Treiber für ein Gerät veröffentlicht wird, ist es sinnvoll, den Treiber erst in einer Entwicklungs- oder Testumgebung auszuprobieren, um zu überprüfen, ob er die Probleme löst, von denen Benutzer berichtet haben. Lässt sich der Treiber problemlos installieren und weist er tatsächlich nicht mehr die alten Probleme auf, wäre der nächste Schritt, ihn auf den Computern zu installieren, die mit dem betreffenden Gerät ausgerüstet sind. Es empfiehlt sich, die Treiberaktualisierung folgendermaßen durchzuführen:

1. Überprüfen Sie auf jedem System, welches Gerät/welcher Treiber installiert sind, bevor Sie den neuen Treiber installieren. Notieren Sie sich Speicherort, Version und Dateinamen des vorhandenen Treibers.
2. Erstellen Sie einen Systemwiederherstellungspunkt, wie in Kapitel 10 im Abschnitt »Sichern und Wiederherstellen des Systemzustands mit der Systemwiederherstellung« besprochen.

3. Installieren Sie den neuen Treiber und starten Sie den Computer bei Bedarf neu. Wenn der Computer und das Gerät nach dem Neustart einwandfrei funktionieren, können Sie die Aktualisierung als erfolgreich ansehen.
4. Weisen der Computer oder das Gerät nach der Installation des Treibers Fehlfunktionen auf, führen Sie das System mit den Werkzeugen des Geräte-Managers auf den zuvor installierten Treiber zurück. Lässt sich der Computer nicht starten und der Treiber nicht wiederherstellen, können Sie das System in die letzte als funktionierend bekannte Konfiguration zurückversetzen und es dann mithilfe des Systemwiederherstellungspunkts, den Sie in Schritt 2 erstellt haben, wiederherstellen.

Installieren von Drahtlosnetzwerk-, Netzwerk- und Bluetooth-Geräten

Sie können die meisten Drahtlos-, Netzwerk- und Bluetooth-Geräte an einen Computer anschließen, etwa Drahtlosnetzwerke, externe Festplatten, Telefone, Tastaturen, Mäuse und Media-Extender-Geräte. Diese Geräte bringen oft Installationssoftware mit, aber bevor Sie diese Installationssoftware starten, sollten Sie prüfen, ob sie zu Windows 8 kompatibel ist. Sollte das nicht der Fall sein, müssen Sie auf der Website des Herstellers nach aktualisierter Software suchen.

Manche Geräte werden direkt an einen Computer angeschlossen. Andere verbinden sich über ein Netzwerk mit einem Computer. Gehen Sie folgendermaßen vor, um ein Drahtlos- oder Bluetooth-Gerät direkt an einen Computer anzuschließen:

1. Die meisten Drahtlos- und Bluetooth-Geräte setzen voraus, dass Sie einen Empfänger an den Computer anschließen. Manche Geräte nutzen einen gemeinsamen Empfänger. Wenn Sie beispielsweise ein Paket mit Funktastatur und -maus kaufen, müssen Sie gewöhnlich nur einen gemeinsamen Empfänger am USB-Anschluss des Computers einstecken.
2. Stellen Sie Computer und Empfänger so auf, dass sich der Empfänger in Reichweite des Geräts befindet, zu dem Sie eine Verbindung herstellen wollen. So sollte eine typische Tastatur oder Maus höchstens 2 Meter Abstand zum Empfänger haben, ein Drahtlosadapter dagegen kann durchaus 30 Meter vom Drahtlosrouter entfernt sein.
3. Konfigurieren Sie die benötigten Geräteeinstellungen und stellen Sie sicher, dass das Gerät eingeschaltet ist. Wenn Sie versuchen, ein Drahtlosnetzwerkgerät hinzufügen, muss es für Ihr Drahtlosnetzwerk konfiguriert sein, bevor Sie es zu einem Computer hinzufügen können. Manche Drahtlosnetzwerkgeräte müssen in einen speziellen Modus namens WPS (Wireless Protected Setup) geschaltet werden, damit sie erkannt werden.
4. Das Gerät müsste nun erkannt und automatisch installiert werden. Wird das Gerät nicht erkannt und installiert, öffnen Sie *Geräte und Drucker*. Stellen Sie in *Geräte und Drucker* sicher, dass das Gerät noch nicht als verfügbar aufgelistet wird. Wenn das Gerät tatsächlich nicht verfügbar ist, können Sie auf *Gerät hinzufügen* tippen oder klicken und dann den Anweisungen folgen.
5. Wenn beim Anschließen des Geräts Probleme auftreten, können Sie im Rahmen der Problembehandlung Folgendes versuchen:
 - Stellen Sie sicher, dass das Gerät nicht ausgeschaltet ist, der Akku nicht leer ist und das Gerät nicht im Standbymodus ist. Manche Drahtlosgeräte haben eine Taste, die Sie drücken müssen, um das Herstellen einer Verbindung zu erzwingen. Andere, etwa Bluetooth-Telefone, haben oft eine Einstellung im internen Menü, die Sie aktivieren müssen, damit eine Verbindung hergestellt wird. Auch am Empfänger eines Geräts gibt es unter Umständen eine Taste, die Sie drücken können, damit der Empfänger nach kompatiblen Drahtlosgeräten sucht.

- Sind Drahtlos- und Bluetooth-Funktionen in den Computer integriert, sollten Sie sicherstellen, dass der Drahtlos- oder Bluetooth-Sender eingeschaltet ist. Manche Notebooks haben einen Schalter, mit dem der Sender ein- und ausgeschaltet werden kann.
- Wenn Sie den Verdacht haben, dass sich das Gerät nicht in Reichweite befindet, sollten Sie es versuchsweise näher an den Computer stellen. Befindet sich eine Wand zwischen Gerät und Computer, können Sie Gerät und Computer in denselben Raum bringen.
- Ist der Standort das Problem, können Sie versuchen, Kabel und Geräte zu verschieben, die möglicherweise elektromagnetische Störungen verursachen. Bei den Störquellen kann es sich um Stromkabel für andere Geräte, große Lautsprecher oder Schreibtischlampen handeln. Besteht das Problem weiterhin, sollten Sie sicherstellen, dass das Gerät nicht zu nah bei Klimaanlage, Mikrowellenherden oder ähnlichen Geräten steht.

Gehen Sie folgendermaßen vor, wenn Sie ein Kabel- oder Drahtlosgerät über ein Netzwerk an den Computer anschließen wollen:

1. Verbinden Sie das Gerät mit dem Netzwerk und schalten Sie es ein. Konfigurieren Sie nun die Grundeinstellungen des Geräts so, dass sie zum Netzwerk passen. Beispielsweise müssen Sie die TCP/IP-Einstellungen oft so konfigurieren, dass DHCP (Dynamic Host Configuration Protocol) benutzt wird. Manchmal müssen Sie auch eine statische IP-Adresse vergeben.
2. Warten Sie etwa 90 Sekunden, bis das Gerät erkannt wird. Das Gerät müsste nun erkannt und automatisch installiert werden. Wird das Gerät nicht erkannt und installiert, sollten Sie *Geräte und Drucker* öffnen. Stellen Sie in *Geräte und Drucker* sicher, dass das Gerät noch nicht als verfügbar aufgelistet wird. Wenn das Gerät tatsächlich nicht verfügbar ist, können Sie auf *Gerät hinzufügen* klicken und dann den Anweisungen folgen.
3. Wenn beim Anschließen des Geräts Probleme auftreten, können Sie im Rahmen der Problembehandlung Folgendes versuchen:
 - Stellen Sie sicher, dass keine Firewall die Verbindung zum Gerät blockiert. Sie müssen unter Umständen einen Firewallport öffnen, um die Kommunikation zwischen Computer und Gerät zu ermöglichen.
 - Stellen Sie sicher, dass das Gerät eingeschaltet ist und mit demselben Netzwerk wie der Computer verbunden ist. Besteht Ihr Netzwerk aus mehreren verbundenen Subnetzen, können Sie versuchen, das Gerät an dasselbe Netzwerksubnetz anzuschließen. An welchem Subnetz ein Computer angeschlossen ist, erkennen Sie an seiner IP-Adresse.
 - Stellen Sie sicher, dass das Gerät so konfiguriert ist, dass es sich selbst über Broadcast im Netzwerk bekannt macht. Die meisten Netzwerkgeräte sind automatisch so eingerichtet.
 - Stellen Sie sicher, dass das Netzwerkgerät eine gültige IP-Adresse und richtige Netzwerkeinstellungen hat. Wird DHCP verwendet, weisen Netzwerkrouter die IP-Adressen automatisch zu, sobald sich Geräte mit dem Netzwerk verbinden.

HINWEIS

Nicht alle erkannten Geräte können zum Computer hinzugefügt werden. Ob ein Gerät tatsächlich mit Ihrem Computer verbunden werden kann, erfahren Sie aus den Handbüchern, die dem Gerät beiliegen, oder auf der Website des Herstellers.

PRAXISTIPP Die Netzwerkerkennung hat Auswirkungen darauf, ob Ihr Computer andere Computer und Geräte im Netzwerk findet und ob andere Computer im Netzwerk Ihren Computer finden. In der Standardeinstellung blockiert die Windows-Firewall die Netzwerkerkennung, aber Sie können sie folgendermaßen aktivieren:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet*.
2. Tippen oder klicken Sie auf *Netzwerk- und Freigabecenter*.
3. Tippen oder klicken Sie im linken Fensterabschnitt auf *Erweiterte Freigabeeinstellungen ändern*.
4. Wählen Sie je nach Bedarf für das Domänenprofil oder andere Profile unter *Netzwerkerkennung* die Option *Netzwerkerkennung einschalten* aus, und tippen oder klicken Sie auf *Änderungen speichern*.

Installieren von lokalen und Netzwerkdruckern

Es gibt unterschiedliche Wege, Drucker mit Computern zu verbinden. Welche Möglichkeit Sie wählen, hängt vom Drucker ab. Manche Drucker werden direkt an einen Computer angeschlossen; sie werden als *lokale Drucker* bezeichnet. Andere verbinden sich über ein Netzwerk mit dem Computer, dies sind die *Netzwerkdrucker*. Zur Klasse der Netzwerkdrucker gehören alle Drucker in einem Netzwerk, etwa Bluetooth- und WLAN-Drucker, sowie Drucker, die an einen anderen Computer angeschlossen und im Netzwerk freigegeben sind.

Die meisten Drucker haben Installationssoftware, die Sie ausführen, um den Drucker erstmals zu konfigurieren. Bei einem Drucker, der direkt an den Computer angeschlossen ist, führen Sie diese Software gewöhnlich nur einmal aus. Die Software richtet dabei den Drucker auf dem Computer ein und konfiguriert eine Verbindung zum Drucker, damit er benutzt werden kann. Bei einem Netzwerkdrucker führen Sie die Software meist einmal auf Ihrem Verwaltungscomputer aus, um den Drucker für die Nutzung vorzubereiten. Dann erstellen Sie auf jedem Computer, auf dem der Drucker zur Verfügung stehen soll, Verbindungen zum Drucker.

Einrichten eines lokalen Druckers

Einen Drucker mit USB-Anschluss verbinden Sie direkt mit dem Computer, woraufhin Windows ihn automatisch erkennen und installieren sollte. Wird Ihr Drucker über eine serielle oder parallele Schnittstelle angeschlossen, müssen Sie ihn möglicherweise von Hand installieren. Gehen Sie folgendermaßen vor, um einen Drucker von Hand zu installieren:

1. Schalten Sie den Drucker ein. Prüfen Sie in *Geräte und Drucker*, ob der Drucker noch nicht als verfügbar aufgelistet wird. Wenn der Drucker noch nicht verfügbar ist, müssen Sie die weiteren Schritte dieser Anleitung durcharbeiten, um ihn zu installieren.
2. Tippen oder klicken Sie in *Geräte und Drucker* auf *Drucker hinzufügen*. Der Druckerinstallations-Assistent versucht, den Drucker automatisch zu erkennen. Wenn er den Drucker findet, mit dem Sie arbeiten möchten, tippen oder klicken Sie den Drucker in der angezeigten Liste an, folgen der Anleitung und überspringen die restlichen Schritte in dieser Beschreibung. Wenn der Assistent den Drucker nicht findet, tippen oder klicken Sie auf *Der gesuchte Drucker ist nicht aufgeführt*.
3. Tippen oder klicken Sie auf *Lokalen Drucker oder Netzwerkdrucker mit manuellen Einstellungen hinzufügen* und dann auf *Weiter*.
4. Wählen Sie in der Dropdownliste *Vorhandenen Anschluss verwenden* den Anschluss aus, mit dem der Drucker verbunden ist, und tippen oder klicken Sie auf *Weiter*.

5. Nun können Sie folgendermaßen fortfahren:

- Wählen Sie Hersteller und Modell des Druckers aus und tippen oder klicken Sie auf *Weiter*.
- Wenn der Drucker nicht aufgelistet wird, Sie aber ein Installationsmedium haben, können Sie auf *Datenträger* klicken und dann zu dem Ordner wechseln, in dem der Druckertreiber gespeichert ist. Weitere Informationen finden Sie im Handbuch des Druckers.
- Haben Sie kein Installationsmedium, können Sie auf *Windows Update* tippen oder klicken, damit Windows nach verfügbaren Treibern sucht.

6. Gehen Sie die übrigen Schritte im Assistenten durch und tippen oder klicken Sie auf *Fertig stellen*. Ob der Drucker funktioniert, können Sie feststellen, indem Sie eine Testseite drucken.

Sie können lokale Drucker auch über Gruppenrichtlinieneinstellungen verwalten. Ich empfehle diesen Ansatz nur in Fällen, wo es möglich ist, bestimmte Computer gezielt auszuwählen, damit nur Computer konfiguriert werden, an die tatsächlich ein lokaler Drucker angeschlossen ist.

Gehen Sie folgendermaßen vor, um ein Einstellungselement anzulegen, mit dem Sie lokale Drucker erstellen, aktualisieren, ersetzen oder löschen:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Drucker* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, erweitern Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* und wählen Sie *Drucker* aus.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Drucker* oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Neu/Lokaler Drucker*. Daraufhin öffnet sich das Eigenschaftendialogfeld für den neuen lokalen Drucker.
3. Wählen Sie im Eigenschaftendialogfeld für den neuen lokalen Drucker in der Dropdownliste *Aktion* den Eintrag *Erstellen, Aktualisieren, Ersetzen* oder *Löschen* aus.
4. Geben Sie im Textfeld *Name* den Namen des Druckers ein. Wenn Sie einen Drucker erstellen, wird dieser Name für den neuen lokalen Drucker verwendet. Wenn Sie einen Drucker aktualisieren, ersetzen oder löschen, muss dieser Name genau dem lokalen Drucker entsprechen, den Sie verwalten wollen.
5. Wählen Sie in der Dropdownliste *Port* den Anschluss aus, mit dem der lokale Drucker verbunden ist.
6. Geben Sie im Textfeld *Druckerpfad* den UNC-Pfad eines freigegebenen Druckers ein, der vom selben Typ ist wie der lokale Drucker, den Sie konfigurieren. Das Einstellungselement verwendet diesen Pfad als Installationsquelle für den Druckertreiber.
7. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Weil Sie in diesem Fall eine Einstellung erzwingen, ist es sinnvoll, die Einstellung jedes Mal anzuwenden, wenn die Gruppenrichtlinien aktualisiert werden. Deaktivieren Sie daher das Kontrollkästchen *Nur einmalig anwenden*.
8. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Gehen Sie folgendermaßen vor, um ein Einstellungselement zu erstellen, mit dem Sie einen freigegebenen lokalen Drucker verwalten:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie den Knoten *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* und wählen Sie *Drucker* aus.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Drucker* oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Neu/Freigegebener Drucker*. Daraufhin öffnet sich das Eigenschaftendialogfeld für die neue Druckerfreigabe.
3. Wählen Sie im Eigenschaftendialogfeld für die neue Druckerfreigabe in der Dropdownliste *Aktion* den Eintrag *Erstellen*, *Aktualisieren*, *Ersetzen* oder *Löschen* aus. Wenn Sie eine Richtlinieneinstellung mit der Aktion *Löschen* erstellen, können Sie festlegen, dass alle freigegebenen Druckerverbindungen gelöscht werden. Stellen Sie dazu die Aktion auf *Löschen* und aktivieren Sie das Kontrollkästchen *Alle freigegebenen Druckerverbindungen löschen*.
4. Geben Sie im Textfeld *Freigabepfad* den UNC-Pfad des freigegebenen Druckers ein. Wählen Sie bei Bedarf einen lokalen Anschluss aus, dem Sie die freigegebene Verbindung zuordnen. Wenn Sie die Aktion *Löschen* verwenden, wird der freigegebene Drucker, der mit diesem lokalen Anschluss verknüpft ist, gelöscht. Stattdessen können Sie mit der Aktion *Löschen* auch die Zuordnungen aller lokalen Anschlüsse aufheben.
5. Optional können Sie den Drucker zum Standarddrucker machen. Wenn Sie eine freigegebene Druckerverbindung erstellen, aktualisieren oder ersetzen und wollen, dass die Verbindung jedes Mal zur Verfügung stehen, wenn sich der Benutzer anmeldet, können Sie das Kontrollkästchen *Verbindung wiederherstellen* aktivieren.
6. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Weil Sie in diesem Fall eine Einstellung erzwingen, ist es sinnvoll, die Einstellung jedes Mal anzuwenden, wenn die Gruppenrichtlinien aktualisiert werden. Deaktivieren Sie daher das Kontrollkästchen *Nur einmalig anwenden*.
7. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Einrichten eines Drahtlos-, Bluetooth- oder Netzwerkdruckers

Wenn ein Drucker eine Drahtlos- oder Bluetooth-Verbindung benutzt, richten Sie den Computer und den Drucker genauso ein wie andere ähnliche Geräte. Gehen Sie vor, wie weiter vorne in diesem Kapitel im Abschnitt »Installieren von Drahtlosnetzwerk-, Netzwerk- und Bluetooth-Geräten« beschrieben, allerdings müssen Sie den Drucker diesmal genauso verbinden wie einen Netzwerkdrucker.

Sorgen Sie dafür, dass der Drucker eingeschaltet ist und sich in einem Modus befindet, in dem er erkannt werden kann. Vielleicht müssen Sie die Drahtlos- oder Bluetooth-Funktionen des Druckers manuell einschalten. Falls der Drucker mit einem Kabel angeschlossen ist, lassen sich seine integrierten Funktionen für die dynamische Adressierung vielleicht nicht verwenden. In diesem Fall müssen Sie die TCP/IP-Einstellungen des Druckers manuell vornehmen.

Stellen Sie in *Geräte und Drucker* sicher, dass der Drucker noch nicht als verfügbar aufgelistet wird. Wenn der Drucker noch nicht verfügbar ist, können Sie die Verbindung folgendermaßen herstellen:

1. Tippen oder klicken Sie in *Geräte und Drucker* auf *Drucker hinzufügen*. Der Druckerinstallations-Assistent versucht, den Drucker automatisch zu erkennen. Wenn er den Drucker findet, mit dem Sie arbeiten möchten, tippen oder klicken Sie den Drucker in der angezeigten Liste an, folgen der Anlei-

tung und überspringen die restlichen Schritte in dieser Beschreibung. Wenn der Assistent den Drucker nicht findet, tippen oder klicken Sie auf *Der gesuchte Drucker ist nicht aufgeführt*.

2. Tippen oder klicken Sie im Druckerinstallations-Assistenten auf *Bluetooth, Funk- oder Netzwerkdrucker hinzufügen*.
3. Wählen Sie in der Liste der verfügbaren Drucker den Drucker aus, den Sie benutzen wollen, und tippen oder klicken Sie auf *Weiter*.
4. Installieren Sie den Druckertreiber auf Ihrem Computer, wenn Sie dazu aufgefordert werden.
5. Gehen Sie die übrigen Schritte im Assistenten durch und tippen oder klicken Sie auf *Fertig stellen*. Ob der Drucker funktioniert, können Sie feststellen, indem Sie eine Testseite drucken.
6. Wenn es nicht gelingt, die Verbindung zum Drucker herzustellen, können Sie im Rahmen der Problembehandlung Folgendes versuchen:
 - Stellen Sie sicher, dass keine Firewall die Verbindung zum Drucker blockiert. Sie müssen unter Umständen einen Firewallport öffnen, um die Kommunikation zwischen Computer und Drucker zu ermöglichen.
 - Stellen Sie sicher, dass der Drucker eingeschaltet ist und mit demselben Netzwerk wie der Computer verbunden ist. Besteht Ihr Netzwerk aus mehreren verbundenen Subnetzen, können Sie versuchen, den Drucker an dasselbe Netzwerksubnetz anzuschließen. An welchem Subnetz ein Computer angeschlossen ist, erkennen Sie an seiner IP-Adresse.
 - Stellen Sie sicher, dass der Drucker so konfiguriert ist, dass er sich selbst über Broadcast im Netzwerk bekannt macht. Die meisten Netzwerkdrucker sind automatisch so eingerichtet.
 - Stellen Sie sicher, dass der Drucker eine gültige IP-Adresse und richtige Netzwerkeinstellungen hat. Wird DHCP verwendet, weisen Netzwerkrouter die IP-Adressen automatisch zu, sobald sich Drucker mit dem Netzwerk verbinden.

Sie können Netzwerkdrucker auch über Gruppenrichtlinieneinstellungen verwalten. Gehen Sie folgendermaßen vor, um eine Verbindung zu einem Netzwerkdrucker zu erstellen, zu aktualisieren, zu ersetzen oder zu löschen:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Drucker* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und *Drucker* auswählen.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Drucker* oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Neu/TCP/IP-Drucker*. Daraufhin öffnet sich das Eigenschaftendialogfeld für den neuen TCP/IP-Drucker.
3. Wählen Sie im Eigenschaftendialogfeld für den neuen TCP/IP-Drucker in der Dropdownliste *Aktion* den Eintrag *Erstellen, Aktualisieren, Ersetzen* oder *Löschen* aus.
4. Sie haben jetzt folgende Möglichkeiten:
 - Wenn Sie die Verbindung zum Drucker mit seiner IP-Adresse herstellen wollen, können Sie die IP-Adresse im Feld *IP-Adresse* eintippen.
 - Wenn Sie die Verbindung zum Drucker mit seinem DNS-Namen herstellen wollen, können Sie das Kontrollkästchen *DNS-Name verwenden* aktivieren und dann den vollqualifizierten Domännennamen des Druckers eingeben.

5. Geben Sie im Textfeld *Lokaler Name* den Namen des Druckers ein. Wenn Sie eine Druckerverbindung erstellen, wird dieser Name auf den Computern der Benutzer angezeigt. Wenn Sie eine Drucker-Verbindung aktualisieren, ersetzen oder löschen, muss dieser Name genau dem Drucker entsprechen, den Sie verwalten wollen.
6. Geben Sie im Textfeld *Druckerpfad* den UNC-Pfad eines freigegebenen Druckers ein, der vom selben Typ ist wie der Netzwerkdrucker, den Sie konfigurieren. Das Einstellungselement verwendet diesen Drucker als Installationsquelle für den Druckertreiber.
7. Optional können Sie den Drucker zum Standarddrucker machen.
8. Stellen Sie mit den Optionen auf der Registerkarte *Porteinstellungen* das Protokoll, die Portnummer und andere Optionen für den Drucker ein.
9. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Weil Sie in diesem Fall eine Einstellung erzwingen, ist es sinnvoll, die Einstellung jedes Mal anzuwenden, wenn die Gruppenrichtlinien aktualisiert werden. Deaktivieren Sie daher das Kontrollkästchen *Nur einmalig anwenden*.
10. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Einführung in den Geräte-Manager

Sie können den Geräte-Manager zur Anzeige und Konfiguration von Hardwaregeräten verwenden. Als Administrator werden Sie dieses Programm vermutlich ziemlich oft verwenden. Daher sollten Sie es kennenlernen, bevor Sie vor Ort mit Geräten arbeiten.

Um den Geräte-Manager zu öffnen und eine ausführliche Liste der Hardware anzuzeigen, die in einem Computer installiert ist, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit*, dann auf *Verwaltung* und schließlich doppelt auf *Computerverwaltung*.

HINWEIS

Wenn Sie mit einem Remotecomputer arbeiten möchten, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten ihn gedrückt, und wählen dann *Verbindung mit anderem Computer herstellen*. Wählen Sie *Verbindung mit anderem Computer herstellen* und geben Sie dann den vollqualifizierten Namen des Computers ein, mit dem Sie arbeiten möchten, oder tippen oder klicken Sie auf *Durchsuchen*, um den Computer auszuwählen, mit dem Sie arbeiten möchten. Tippen oder klicken Sie auf *OK*.

2. Erweitern Sie in der Konsole *Computerverwaltung* den Knoten *System* und wählen Sie dann *Geräte-Manager* aus. Sie müssten nun eine vollständige Liste der Geräte angezeigt bekommen, die auf dem System installiert sind (Abbildung 9.15). Diese Liste ist standardmäßig nach dem Gerätetyp sortiert. Mit den Optionen aus dem Menü *Ansicht* können Sie die Darstellung auch so einstellen, dass Geräte nach Verbindung, Ressourcen nach Typ oder Ressourcen nach Verbindung sortiert dargestellt werden.
3. Tippen oder klicken Sie auf das Dreiecksymbol vor einem Gerätetyp, wenn Sie sich ansehen möchten, welche Geräte des betreffenden Typs installiert sind. Wählen Sie das Gerät aus, das Sie bearbeiten wollen.

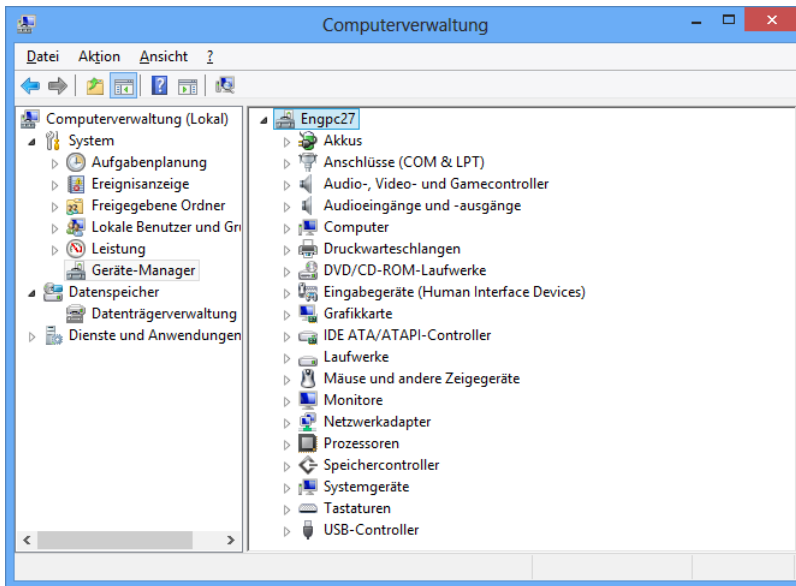


Abbildung 9.15 Verwalten von Hardwaregeräten im Geräte-Manager

Nachdem Sie den Geräte-Manager geöffnet haben, können Sie jedes der installierten Geräte bearbeiten. Wenn Sie einen Geräteeintrag mit der rechten Maustaste anklicken oder gedrückt halten, erscheint ein Kontextmenü. Welche der folgenden Optionen darin verfügbar sind, hängt vom Gerätetyp ab:

- **Eigenschaften** Zeigt das Eigenschaftendialogfeld für das Gerät an.
- **Deinstallieren** Deinstalliert das Gerät und seine Treiber.
- **Deaktivieren** Deaktiviert das Gerät, aber deinstalliert es nicht.
- **Aktivieren** Aktiviert ein Gerät, sofern es deaktiviert ist.
- **Treibersoftware aktualisieren** Startet den Hardwareaktualisierungsassistenten, mit dessen Hilfe Sie den Gerätetreiber aktualisieren können.
- **Nach geänderter Hardware suchen** Weist Windows 8 an, die Hardwarekonfiguration zu überprüfen und herauszufinden, ob sich Änderungen ergeben haben.

TIPP Die Geräteliste weist Warnsymbole auf, falls es mit einem Gerät Probleme gibt. Ein gelbes Warnsymbol mit einem Ausrufezeichen weist auf ein Problem mit einem Gerät hin. Ein rotes X bedeutet, dass ein Gerät falsch installiert oder aus irgendeinem Grund vom Benutzer oder Administrator deaktiviert wurde. Ein weißer Kreis mit einem nach unten gerichteten Pfeil deutet an, dass ein Gerät aus irgendeinem Grund von einem Benutzer oder Administrator deaktiviert wurde.

Mit den Optionen des *Ansicht*-Menüs der Computerverwaltungskonsolle können Sie festlegen, ob Geräte oder Ressourcen angezeigt werden und in welcher Weise die Anzeige erfolgt. Folgende Optionen stehen zur Verfügung:

- **Geräte nach Typ** Die Anzeige der Geräte erfolgt nach dem Gerätetyp, wie zum Beispiel Laufwerk oder Drucker. Unter dem Typ wird der Gerätenamen angezeigt. Das ist die Standardansicht.
- **Geräte nach Verbindung** Die Anzeige der Geräte erfolgt nach dem Verbindungstyp, wie zum Beispiel Geräte, die an den PCI-Bus des Computers angeschlossen sind.

- **Ressourcen nach Typ** Zeigt den Status der belegten Ressourcen nach den Typen der Geräte an, von denen die Ressourcen benutzt werden. Bei den Ressourcentypen handelt es sich um Arbeitsspeicher, direkte Speicherzugriffe (DMA), Ein-/Ausgabeanschlüsse und Interruptanforderungen (IRQ).
- **Ressourcen nach Verbindung** Zeigt den Status der belegten Ressourcen nach dem Verbindungstyp an statt nach dem Gerätetyp. In dieser Ansicht können Sie überprüfen, welche Ressourcen für Geräte mit Verbindung zum PCI-Bus, Stammbus und so weiter verbraucht werden.
- **Ausgeblendete Geräte anzeigen** Fügt ausgeblendete Geräte zu den Standardansichten hinzu. Zeigt Nicht-Plug & Play-Geräte sowie Geräte an, die zwar aus dem Computer ausgebaut wurden, aber deren Treiber noch installiert sind.

Arbeiten mit Gerätetreibern

Zu jeder Hardwarekomponente, die in einem Computer installiert ist, gehört ein Gerätetreiber. Aufgabe des Gerätetreibers ist es, die Verbindung zwischen der Hardwareabstraktionsschicht (Hardware Abstraction Layer, HAL) und der Hardwarekomponente herzustellen. Die Hardwareabstraktionsschicht betreibt auf einer niedrigen Ebene die Kommunikation zwischen dem Betriebssystem und einer Hardwarekomponente. Bei der Installation einer Hardwarekomponente im Betriebssystem teilen Sie dem Betriebssystem mit, welchen Treiber das Gerät benutzt. Anschließend wird der Gerätetreiber automatisch geladen und als Teil des Betriebssystems ausgeführt.

Grundlagen der Gerätetreiber

Windows 8 enthält eine umfangreiche Gerätetreiberbibliothek. In der Grundinstallation des Betriebssystems werden diese Treiber im Treiberspeicher gespeichert. Manche Service Packs, die Sie installieren, werden auch Updates für den Treiberspeicher enthalten. Auf 32-Bit-Computern befindet sich der 32-Bit-Treiberspeicher im Ordner `%SystemRoot%\System32\DriverStore`. Auf 64-Bit-Computern liegt der 64-Bit-Treiberspeicher in `%SystemRoot%\System32\DriverStore` und der 32-Bit-Treiberspeicher im Ordner `%SystemRoot%\SysWOW64\DriverStore`. Der Ordner `DriverStore` enthält auch Unterordner für lokalisierte Treiberinformationen. Sie werden für jede Sprache, die auf dem System konfiguriert worden ist, einen Unterordner vorfinden. Für die lokalisierte Treiberinformation für die USA wird beispielsweise ein Unterordner namens *en-US* angelegt. Für die deutschen Treiberinformationen heißt der Unterordner *de-DE*.

Jeder Treiber aus dem Treiberspeicher ist vollständig zu Windows 8 kompatibel und wurde von Microsoft digital signiert, damit sich das Betriebssystem von der Echtheit des Treibers überzeugen kann. Wenn Sie ein neues Plug & Play-kompatibles Gerät installieren, sucht Windows 8 im Treiberspeicher nach einem kompatiblen Treiber. Ist einer vorhanden, installiert das Betriebssystem das Gerät automatisch.

Zu jedem Gerätetreiber gehört eine Setupinformationsdatei. Der Name dieser Datei endet auf *.inf*. Es handelt sich um eine Textdatei mit ausführlichen Informationen über das zu installierende Gerät. In der Setupinformationsdatei werden auch alle Quelldateien genannt, die vom Treiber verwendet werden. Quelldateien haben die Namensendung *.sys*. Es gibt auch *.pnf*- und *.dll*-Dateien für Treiber, und manche Treiber sind mit einer Komponentenmanifestdatei (*.amx*) verknüpft. Die Manifestdatei liegt im XML-Format vor und enthält Einzelheiten über die digitale Signatur des Treibers. Sie kann auch Plug & Play-Informationen enthalten, die vom Gerät zur automatischen Einstellung verwendet werden.

Für jeden auf einem System installierten Treiber gibt es im Ordner *Drivers* eine Quelldatei (*.sys*). Wenn Sie einen neuen Gerätetreiber installieren, wird der Treiber in einen Unterordner von *Drivers* kopiert und die Konfigurationseinstellungen werden in die Registrierung eingetragen. Die *.inf*-Datei des Treibers dient zur Steuerung der Installation und der Registrierungseinträge. Ist der Treiber noch nicht im Treiber-

speicher vorhanden, gibt es im System noch keine *.inf*-Datei oder eine andere mit ihm verknüpfte Datei. In diesem Fall werden die *.inf*-Datei des Treibers und andere dazugehörige Dateien in einem Unterordner von *DriverStore\FileRepository* gespeichert, wenn Sie das Gerät installieren.

Verwenden von signierten und nichtsignierten Gerätetreibern

Jeder Treiber im Treiberspeicher ist digital signiert. Die Signatur bestätigt, dass der Treiber einen ausführlichen Test im Windows Hardware Quality Lab durchlaufen hat. Ein Gerätetreiber mit einer digitalen Signatur von Microsoft sollte eigentlich nicht dazu führen, dass Ihr System instabil wird oder abstürzt. Die digitale Signatur von Microsoft stellt zudem sicher, dass der Gerätetreiber nicht absichtlich oder versehentlich verändert wurde. Wenn ein Gerätetreiber nicht von Microsoft digital signiert wurde, ist er nicht offiziell auf seine Tauglichkeit getestet worden oder seine Dateien wurden vielleicht durch ein anderes Programm verändert. Das bedeutet, dass nichtsignierte Treiber mit einer höheren Wahrscheinlichkeit als alle anderen Anwendungen, die Sie installiert haben, einen Absturz des Computers oder ein Hängen des Systems verursachen können.

Um Probleme mit nichtsignierten Treibern möglichst zu vermeiden, warnt Windows 8 Sie standardmäßig, wenn Sie versuchen, einen nichtsignierten Treiber zu installieren. Windows lässt sich auch so konfigurieren, dass die Installation bestimmter Gerätetypen grundsätzlich verhindert wird. Um die Treibereinstellungen der Computer in einer ganzen Organisation einheitlich zu gestalten, können Sie Gruppenrichtlinien verwenden. Wenn Sie das tun, legt die Gruppenrichtlinie fest, ob und wie Geräte installiert werden dürfen.

Sie können die Geräteinstallationseinstellungen für mehrere Computer unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Geräteinstallation* konfigurieren.

TIPP Wenn Sie beim Versuch, ein Gerät zu installieren, feststellen, dass dies nicht funktioniert, sind möglicherweise Geräteinstallationseinschränkungen in den Gruppenrichtlinien aktiv. Sie müssen die Gruppenrichtlinien außer Kraft setzen, um das Gerät zu installieren.

Überprüfen der Treiberinformationen

Für jeden Treiber, der auf einem System benutzt wird, gibt es auch eine Datei mit dem ausführbaren Code des Treibers. Mit folgenden Schritten können Sie herausfinden, wo diese Datei liegt:

1. Starten Sie die Computerverwaltung. Erweitern Sie in der Konsole *Computerverwaltung* den Knoten *System*.
2. Wählen Sie *Geräte-Manager* aus. Sie müssten nun eine vollständige Liste der Geräte angezeigt bekommen, die auf dem System installiert sind. Diese Liste ist standardmäßig nach dem Gerätetyp sortiert.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie bearbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*. Das Eigenschaftendialogfeld für das Gerät öffnet sich.
4. Tippen oder klicken Sie auf der Registerkarte *Treiber* auf *Treiberdetails*, um das Dialogfeld *Treiberdetails* zu öffnen. Wie aus Abbildung 9.16 hervorgeht, werden folgende Informationen angezeigt:
 - **Treiberdateien** Die Pfadnamen der Treiberdateien
 - **Anbieter** Der Hersteller des Treibers
 - **Dateiversion** Die Dateiversion

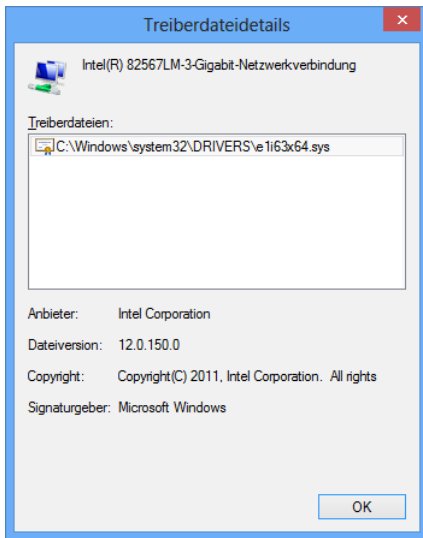


Abbildung 9.16 Das Dialogfeld *Treiberdateidetails* zeigt den Pfadnamen der Treiberdatei, den Anbieter und die Dateiversion an

Installieren und Aktualisieren von Gerätetreibern

Damit die Geräte reibungslos arbeiten, ist es wichtig, die Gerätetreiber auf dem neusten Stand zu halten. Sie können Treiber mit den Assistenten *Neue Hardware gefunden*, *Hardware-* und *Treibersoftwareupdate* installieren und aktualisieren. Standardmäßig können diese Assistenten an folgenden Orten nach aktuellen Gerätetreibern suchen:

- Auf dem lokalen Computer
- Auf der Hardware-Installations-CD
- Auf der Windows Update-Website oder auf dem Windows Update-Server Ihrer Organisation

In den Gruppenrichtlinien gibt es mehrere Richtlinien, die festlegen, wie Informationen über Geräte ermittelt werden und wie Windows nach Treibern sucht:

- **Zugriff auf alle Windows Update-Funktionen deaktivieren unter Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Internetkommunikationsverwaltung\Internetkommunikationseinstellungen** Wenn diese Richtlinie aktiviert ist, sind alle Windows Update-Funktionen gesperrt und den Benutzern nicht zugänglich. Benutzer können auch nicht auf die Windows Update-Website zugreifen.
- **Suche nach Gerätetreibern auf Windows Update deaktivieren unter Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Internetkommunikationsverwaltung\Internetkommunikationseinstellungen** Standardmäßig ist die Windows Update-Suche bei der Installation eines Geräts optional. Wenn Sie diese Einstellung aktivieren, wird Windows Update bei der Installation eines neuen Geräts nicht durchsucht. Wenn Sie diese Einstellung deaktivieren, wird Windows Update bei der Installation eines neuen Geräts immer durchsucht, sofern lokal kein Treiber verfügbar ist.
- **Suchreihenfolge für Quellspeicherorte für Gerätetreiber festlegen unter Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Geräteinstallation** Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, können Sie die Reihenfolge für die Speicherorte festlegen, in

denen auf jedem Computer nach Gerätetreibern gesucht wird. Wenn Sie diese Richtlinie aktivieren, können Sie festlegen, dass Windows Update zuerst, zuletzt oder überhaupt nicht durchsucht werden soll, wenn während der Geräteinstallation nach Treibersoftware gesucht wird.

- **Zeitlimit für Geräteinstallation festlegen unter Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Geräteinstallation** Wenn Sie diese Richtlinie deaktivieren oder nicht konfigurieren, wartet Windows 5 Minuten, ob die Geräteinstallation abgeschlossen werden kann, bevor es die Installation abbricht. Wenn Sie diese Richtlinie aktivieren, können Sie festlegen, wie lange Windows 8 wartet, bevor es die Installation abbricht.
- **Abrufen von Gerätemetadaten aus dem Internet verhindern unter Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Geräteinstallation** Wenn Sie diese Richtlinie deaktivieren oder nicht konfigurieren, ruft Windows 8 Gerätemetadaten zu installierten Geräten aus dem Internet ab und nutzt diese Informationen, um die Geräte auf dem neusten Stand zu halten. Wenn Sie diese Richtlinieneinstellung aktivieren, ruft Windows 8 keine Gerätemetadaten für installierte Geräte aus dem Internet ab.

Gerätetreiber können Sie folgendermaßen installieren und aktualisieren:

1. Starten Sie die Computerverwaltung. Erweitern Sie in der Konsole *Computerverwaltung* den Knoten *System*.
2. Wählen Sie in der Konsole *Computerverwaltung* den Knoten *Geräte-Manager* aus. Sie müssten nun eine vollständige Liste der Geräte angezeigt bekommen, die auf dem System installiert sind. Diese Liste ist standardmäßig nach dem Gerätetyp sortiert.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie bearbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Treibersoftware aktualisieren*. Dadurch wird der Treibersoftwareupdate-Assistent gestartet.

EMPFOHLENE VORGEHENSWEISE

Aktualisierte Treiber können den Funktionsumfang eines Geräts erweitern, die Leistung verbessern und Probleme beheben. Allerdings sollten Sie nicht einfach den neusten Treiber auf einem Arbeitscomputer installieren, ohne ihn zuvor in einer Testumgebung überprüft zu haben. Die Grundregel lautet: erst testen, dann installieren.

4. Wie Abbildung 9.17 zeigt, können Sie wählen, ob die Treibersoftware automatisch gesucht werden soll oder ob Sie den Treiber selbst an einem bestimmten Ort suchen oder manuell aus einer Liste auswählen.
5. Wenn Sie sich für die automatische Installation entscheiden, sucht Windows 8 nach einer neueren Version des Gerätetreibers und installiert diese Version, sofern es sie gibt. Ist keine neuere Version des Treibers verfügbar, behält Windows 8 den aktuellen Treiber bei. In beiden Fällen tippen oder klicken Sie auf *Schließen*, um den Vorgang abzuschließen. Überspringen Sie die restlichen Schritte.
6. Wenn Sie sich zur manuellen Installation des Treibers entschließen, haben Sie immer noch die Wahl zwischen zwei Alternativen:
 - **Suchen des Treibers** Tippen oder klicken Sie auf *Auf dem Computer nach Treibersoftware suchen*. Tippen oder klicken Sie auf *Durchsuchen* und suchen Sie im Dialogfeld *Ordner suchen* den Startordner für die Suche aus. Tippen oder klicken Sie dann auf *OK*. Wenn Sie *Unterordner einbeziehen* aktiviert lassen, werden auch die Unterordner des ausgewählten Ordners in die Suche einbezogen und Sie können ein Stammverzeichnis auswählen, beispielsweise C:, wenn ein ganzes Laufwerk durchsucht werden soll.

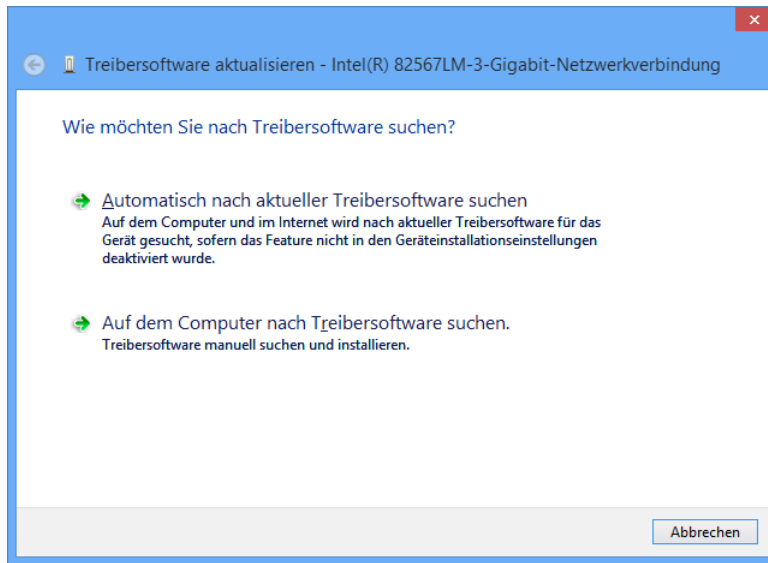


Abbildung 9.17 Wählen Sie, ob die Treiberinstallation automatisch oder manuell erfolgen soll

- **Auswählen des Treibers** Tippen oder klicken Sie auf *Aus einer Liste von Gerätetreibern auf dem Computer auswählen*. Der Assistent zeigt dann eine Liste mit kompatibler Hardware. Tippen oder klicken Sie auf das Gerät, das Ihrer Hardware entspricht. Wenn Sie eine größere Auswahl wünschen, deaktivieren Sie das Kontrollkästchen *Kompatible Hardware anzeigen*. Dann sehen Sie eine vollständige Liste der Hersteller für die Art von Gerät, mit dem Sie arbeiten. Wie aus Abbildung 9.18 hervorgeht, suchen Sie in der Herstellerliste nach dem Hersteller und auf der rechten Seite nach dem Gerät.

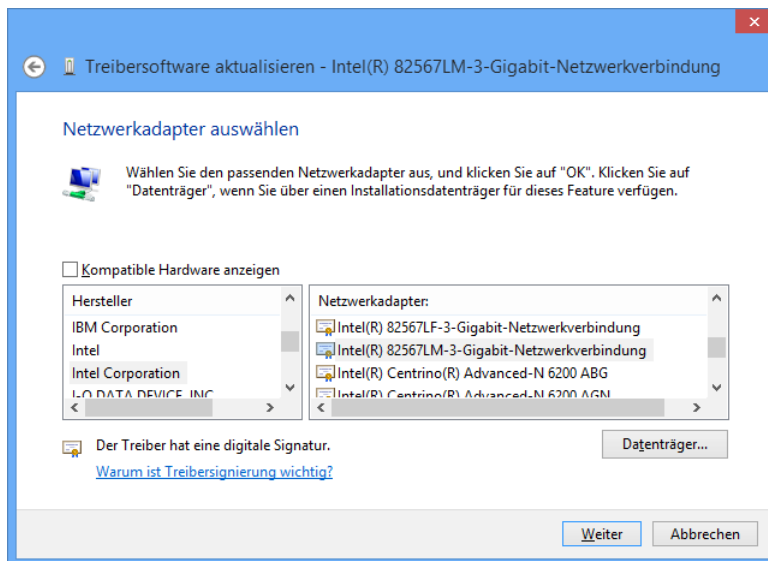


Abbildung 9.18 Wählen Sie den passenden Gerätetreiber für das Gerät aus, das Sie hinzufügen

HINWEIS

Wenn der Hersteller oder das Gerät, das Sie verwenden möchten, nicht aufgeführt ist, legen Sie Ihren Datenträger mit dem Gerätetreiber ins Laufwerk ein und tippen oder klicken dann auf die Schaltfläche *Datenträger*. Befolgen Sie die Anweisungen.

7. Nachdem Sie den Gerätetreiber durch eine automatische Suche oder eine manuelle Auswahl ausgewählt haben, tippen oder klicken Sie auf *Weiter* und durchlaufen die nächsten Schritte des Installationsprozesses. Tippen oder klicken Sie auf *Schließen*, wenn die Treiberinstallation abgeschlossen ist. Wenn der Assistent keinen passenden Treiber finden kann, müssen Sie einen passenden Treiber beschaffen und diese Prozedur dann wiederholen. Vergessen Sie bitte nicht, dass Sie in manchen Fällen das System neu starten müssen, um den neu installierten oder aktualisierten Gerätetreiber zu aktivieren.

Aktivieren und Deaktivieren bestimmter Gerätetypen

Mit Gruppenrichtlinieneinstellungen können Sie verwalten, welche Hardwaregeräte auf den Computern benutzt werden dürfen, auf die ein Gruppenrichtlinienobjekt angewendet wird. Sie haben folgende Möglichkeiten, um festzulegen, welche Geräte benutzt werden dürfen:

- **Geräteklasse** Eine Geräteklasse umfasst einen weiten Bereich ähnlicher Geräte, beispielsweise alle DVD-Laufwerke.
- **Gerätetyp** Ein Gerätetyp bezeichnet bestimmte Geräte innerhalb einer Geräteklasse, zum Beispiel das Laufwerk NEC DVD-ROM RW ND-3530A ATA.

HINWEIS

Wenn Sie Geräte anhand des Typs verwalten wollen, müssen Sie einen Verwaltungscomputer mit den Geräten ausstatten, die Sie bearbeiten wollen. Dann erstellen Sie die Einstellungselemente auf diesem Computer. Ein Verwaltungscomputer ist ein Computer, auf dem die Verwaltungstools installiert sind, beispielsweise die Remote Server Administration Tools (RSAT).

Gehen Sie folgendermaßen vor, um ein Einstellungselement zu erstellen, mit dem Sie Geräte anhand von Klasse oder Typ aktivieren oder deaktivieren:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Geräte* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* und *Geräte* auswählen.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Geräte* oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Neu/Gerät*. Daraufhin öffnet sich das Eigenschaftendialogfeld für das neue Gerät.
3. Wählen Sie im Eigenschaftendialogfeld für das neue Gerät in der Dropdownliste *Aktion* einen der folgenden Einträge aus:
 - **Gerät verwenden (aktivieren)** Wählen Sie diese Option, wenn Sie Geräte anhand ihrer Klasse oder ihres Typs aktivieren wollen.
 - **Gerät nicht verwenden (deaktivieren)** Wählen Sie diese Option, wenn Sie Geräte anhand ihrer Klasse oder ihres Typs deaktivieren wollen.

4. Tippen oder klicken Sie auf die Schaltfläche rechts neben *Gerätekategorie*. Sie haben jetzt zwei Möglichkeiten:
 - Wählen Sie eine Gerätekategorie aus, um die Geräte anhand der Kategorie zu verwalten.
 - Erweitern Sie einen Gerätekategorienknoten und wählen Sie einen Gerätetyp aus, um die Geräte anhand ihres Typs zu verwalten.
5. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Weil Sie in diesem Fall eine Einstellung erzwingen, ist es sinnvoll, die Einstellung jedes Mal anzuwenden, wenn die Gruppenrichtlinien aktualisiert werden. Deaktivieren Sie daher das Kontrollkästchen *Nur einmalig anwenden*.
6. Tippen oder klicken Sie auf OK. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Einschränken der Geräteinstallation durch Gruppenrichtlinien

Gruppenrichtlinieneinstellungen können nicht nur benutzt werden, um Einstellungen für die Codesignatur und Sucheinschränkungen festzulegen, Sie können damit auch die Installation bestimmter Geräte, die anhand der Gerätekategorie identifiziert werden, erlauben oder verhindern. Geräte, die auf dieselbe Weise eingerichtet und konfiguriert werden, werden zu einer Gerätesetupklasse zusammengefasst. Jede Gerätesetupklasse hat eine bestimmte GUID (Globally Unique Identifier). Damit Sie die Geräteinstallation über Gruppenrichtlinien einschränken können, müssen Sie die GUID für die gewünschte Gerätesetupklasse kennen.

Die Registrierung enthält für jede Standardgerätesetupklasse einen Schlüssel unter *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class*. Die Namen der Registrierungsschlüssel entsprechen der Klassen-GUID. Wenn Sie den Registrierungsschlüssel einer Klassen-GUID auswählen, gibt der Wert *Class* die Gerätesetupklasse an, die von dieser GUID identifiziert wird. Wählen Sie beispielsweise *{4d36e965-e325-11ce-bfc1-08002be10318}* aus, erkennen Sie, dass es sich um die Gerätesetupklasse für CD-ROM-Geräte handelt.

Die Richtlinieneinstellungen zum Verwalten der Geräteinstallation liegen im Zweig *Computerkonfiguration\Richtlinien\Administrative Vorlagen\System\Geräteinstallation\Einschränkungen bei der Geräteinstallation*. Es gibt folgende Richtlinien:

- *Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallation" erlauben*
- *Installation von Geräten mit diesen Geräte-IDs zulassen*
- *Installation von Geräten mit Treibern zulassen, die diesen Gerätesetupklassen entsprechen*
- *Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind*
- *Installation von Geräten mit diesen Geräte-IDs verhindern*
- *Installation von Wechselgeräten verhindern*
- *Zeit (in Sekunden) bis zum Erzwingen eines Neustarts, wenn dieser für das Inkrafttreten von Richtlinienänderungen erforderlich ist*

Sie können diese Richtlinien folgendermaßen konfigurieren:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor.
2. Erweitern Sie *Computerkonfiguration*, *Administrative Vorlagen*, *System*, *Geräteinstallation* und *Einschränkungen bei der Geräteinstallation*.
3. Tippen oder klicken Sie die gewünschte Richtlinie doppelt an, um ihr Eigenschaftendialogfeld zu öffnen.
4. Stellen Sie die Richtlinie auf *Nicht konfiguriert*, wenn sie nicht angewandt werden soll, auf *Aktiviert*, wenn sie gelten soll, oder auf *Deaktiviert*, wenn die Richtlinie gesperrt werden soll (sofern es die Gruppenrichtlinieneinstellungen zulassen).
5. Wenn Sie eine Richtlinie aktivieren, die über eine *Anzeigen*-Option verfügt, tippen oder klicken Sie die *Anzeigen*-Schaltfläche an und geben im *Inhalt anzeigen*-Dialogfeld die Geräte-IDs an, die von dieser Richtlinie betroffen sind. Tippen oder klicken Sie anschließend auf *OK*. Im Registrierungs-Editor besteht die GUID für eine Gerätesetupklasse aus dem gesamten Schlüsselnamen einschließlich der geschweiften Klammern. Sie können den Schlüsselnamen folgendermaßen kopieren und in das Dialogfeld *Inhalt anzeigen* einfügen:
 - a. Öffnen Sie den Registrierungs-Editor, indem Sie die *WINDOWS*-Taste drücken, **regedit** eingeben und die *EINGABETASTE* drücken. Diese Methode funktioniert, solange das Suchfeld *Apps* im Eingabefokus liegt.
 - b. Klicken Sie im Registrierungs-Editor mit der rechten Maustaste auf den Schlüsselnamen oder halten Sie ihn gedrückt und wählen Sie den Befehl *Schlüsselnamen kopieren*.
 - c. Tippen oder klicken Sie im Dialogfeld *Inhalt anzeigen* des Gruppenrichtlinienverwaltungs-Editors zweimal in das Textfeld *Wert*, damit ein Einfügekursor angezeigt wird. Halten Sie das Textfeld gedrückt oder klicken Sie es mit der rechten Maustaste an und wählen Sie den Befehl *Einfügen*.
 - d. Löschen Sie den Pfad, der vor der GUID steht. Sie sollten also den Teil *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class* löschen.
 - e. Sie können die GUIDs für weitere Gerätesetupklassen hinzufügen, indem Sie die Schritte b bis d wiederholen.
6. Tippen oder klicken Sie auf *OK*.

Wiederherstellen der Vorversion eines Treibers

Es kann vorkommen, dass ein Gerätetreiber, den Sie installierten, praktisch den Ausfall des Geräts oder andere Probleme auf dem Computer zur Folge hat. Keine Sorge: Sie können das System auf den zuvor installierten Gerätetreiber zurückführen. Dazu gehen Sie folgendermaßen vor:

1. Wenn Sie mit dem Systemstart Probleme haben, müssen Sie den Computer im abgesicherten Modus starten, wie im Abschnitt »Problembehandlung für Systemstart und Herunterfahren« in Kapitel 10 beschrieben.
2. Starten Sie die Computerverwaltung. Erweitern Sie in der Konsole *Computerverwaltung* den Knoten *System*.
3. Wählen Sie in der Konsole *Computerverwaltung* den Knoten *Geräte-Manager* aus. Sie müssten nun eine vollständige Liste der Geräte angezeigt bekommen, die auf dem System installiert sind. Diese Liste ist standardmäßig nach dem Gerätetyp sortiert.

4. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie bearbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*. Dadurch wird das Eigenschaftendialogfeld für das Gerät geöffnet.
5. Tippen oder klicken Sie auf die Registerkarte *Treiber* und dann auf *Vorheriger Treiber*. Wenn Sie aufgefordert werden, den Vorgang zu bestätigen, tippen oder klicken Sie auf *Ja*.
6. Tippen oder klicken Sie auf *OK*, um das Eigenschaftendialogfeld des Treibers zu schließen.

HINWEIS Falls der Gerätetreiber noch nicht aktualisiert wurde, ist auch keine Vorgängerversion des Treibers verfügbar. In diesem Fall ist die Schaltfläche *Vorheriger Treiber* deaktiviert.

Entfernen der Gerätetreiber für ausgebaute Geräte

Wenn Sie ein Gerät aus einem Computer ausbauen, erkennt Windows 8 gewöhnlich diesen Vorgang und entfernt automatisch die Gerätetreiber für das Gerät. Manchmal erkennt Windows 8 die Veränderung aber nicht und Sie müssen die Treiber manuell entfernen. Dazu gehen Sie folgendermaßen vor:

1. Starten Sie die Computerverwaltung. Erweitern Sie in der Konsole *Computerverwaltung* den Knoten *System*.
2. Wählen Sie in der Konsole *Computerverwaltung* den Knoten *Geräte-Manager* aus.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie entfernen möchten, oder halten Sie es gedrückt, und wählen Sie dann *Deinstallieren*.
4. Wenn Sie aufgefordert werden, den Vorgang zu bestätigen, tippen oder klicken Sie auf *OK*.

Deinstallieren, erneutes Installieren und Deaktivieren von Gerätetreibern

Durch das Deinstallieren eines Gerätetreibers ist das betreffende Gerät nicht mehr im System verfügbar. Wenn ein Gerät nicht richtig arbeitet, lässt sich das Problem manchmal lösen, indem man das Gerät aus dem System entfernt, das System neu startet und den Gerätetreiber dann erneut installiert. Sie können ein Gerät folgendermaßen deinstallieren und erneut installieren:

1. Starten Sie die Computerverwaltung. Erweitern Sie in der Konsole *Computerverwaltung* den Knoten *System*.
2. Wählen Sie in der Konsole *Computerverwaltung* den Knoten *Geräte-Manager* aus. Sie müssten nun eine vollständige Liste der Geräte angezeigt bekommen, die auf dem System installiert sind. Diese Liste ist standardmäßig nach dem Gerätetyp sortiert.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie bearbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Deinstallieren*.
4. Wenn Sie aufgefordert werden, den Vorgang zu bestätigen, tippen oder klicken Sie auf *OK*.
5. Starten Sie das System neu. Windows 8 sollte das Vorhandensein des Geräts erkennen und automatisch den erforderlichen Gerätetreiber installieren. Wenn das Gerät nicht automatisch installiert wird, installieren Sie es manuell, wie im Abschnitt »Installieren und Aktualisieren von Gerätetreibern« weiter oben in diesem Kapitel beschrieben.

Wenn Sie verhindern möchten, dass ein Gerät automatisch neu installiert wird, deinstallieren Sie das Gerät nicht, sondern deaktivieren es nur. Sie deaktivieren ein Gerät, indem Sie es im Geräte-Manager mit der rechten Maustaste anklicken oder es gedrückt halten und *Deaktivieren* wählen.

Aktivieren und Deaktivieren von Hardwaregeräten

Wenn ein Gerät nicht richtig arbeitet, kann es sinnvoll sein, es zu deaktivieren oder zu deinstallieren. Durch die Deinstallation wird der Treiber des betreffenden Geräts entfernt, was den Anschein erweckt, als sei das Gerät aus dem System entfernt worden. Beim nächsten Start des Systems wird Windows 8 wahrscheinlich versuchen, das Gerät neu zu installieren. Gewöhnlich installiert Windows 8 Plug & Play-Geräte automatisch, Nicht-Plug & Play-Geräte aber nicht.

Durch eine Deaktivierung wird ein Gerät abgeschaltet und nicht mehr von Windows 8 benutzt. Da ein deaktiviertes Gerät keine Systemressourcen beansprucht, können Sie davon ausgehen, dass es im System keinen Konflikt mehr verursachen kann.

Sie können ein Gerät folgendermaßen deinstallieren oder deaktivieren:

1. Starten Sie die Computerverwaltung. Erweitern Sie in der Konsole *Computerverwaltung* den Knoten *System*.
2. Wählen Sie in der Konsole *Computerverwaltung* den Knoten *Geräte-Manager* aus. Sie müssten nun eine vollständige Liste der Geräte angezeigt bekommen, die auf dem System installiert sind. Diese Liste ist standardmäßig nach dem Gerätetyp sortiert.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie bearbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann eine der folgenden Optionen:
 - *Deinstallieren*
 - *Deaktivieren*
4. Wenn Sie aufgefordert werden, den Vorgang zu bestätigen, tippen oder klicken Sie je nach Vorgang auf *Ja* oder *OK*.

Beseitigen von Hardwareproblemen

Die integrierte Hardwarediagnose von Windows 8 kann viele Probleme mit Hardwaregeräten erkennen. Wird ein Problem erkannt, sehen Sie vielleicht eine Problemberichtsprechblase, die Sie auf das Problem hinweist. Ein Klick auf diese Sprechblase sollte das Wartungscenter öffnen. Sie können das Wartungscenter auch öffnen, indem Sie in der Systemsteuerung auf *System und Sicherheit* klicken und dann auf *Wartungscenter*.

Wenn ein Gerät falsch installiert wurde oder ein anderes Problem aufweist, zeigt der Geräte-Manager mit einem Warnsymbol an, dass das Gerät ein Problem hat. Wenn Sie das Gerät doppelt anklicken oder antippen, wird auf der Registerkarte *Allgemein* des Eigenschaftendialogfelds des betreffenden Geräts ein Fehlercode angezeigt. Wie aus Tabelle 9.3 hervorgeht, kann dieser Fehlercode bei der Behebung des Fehlers sehr hilfreich sein. Die meisten Lösungsvorschläge in dieser Tabelle setzen voraus, dass Sie die Registerkarte *Allgemein* des Eigenschaftendialogfelds gewählt haben.

Tabelle 9.3 Übliche Gerätefehler und ihre Behebung

Fehlermeldung	Was ist zu tun?
Das Gerät ist nicht richtig konfiguriert. (Code 1)	Beschaffen Sie einen passenden Treiber für das Gerät und tippen oder klicken Sie auf der Registerkarte <i>Treiber</i> auf <i>Treiber aktualisieren</i> , um den Treibersoftwareupdate-Assistenten zu starten.
Der Treiber für dieses Gerät ist entweder beschädigt, oder es stehen nicht genügend Arbeitsspeicher oder andere Ressourcen zur Verfügung. (Code 3)	Tippen oder klicken Sie auf der Registerkarte <i>Treiber</i> auf die Schaltfläche <i>Treiber aktualisieren</i> , um den Treibersoftwareupdate-Assistenten zu starten. Vermutlich werden Sie beim Start die Meldung »Nicht genügend Arbeitsspeicher« erhalten.
Das Gerät kann nicht gestartet werden. (Code 10)	Tippen oder klicken Sie auf der Registerkarte <i>Treiber</i> auf die Schaltfläche <i>Treiber aktualisieren</i> , um den Treibersoftwareupdate-Assistenten zu starten. Versuchen Sie nicht, automatisch einen Treiber zu finden. Wählen Sie stattdessen die manuelle Installation und wählen Sie das Gerät aus.
Dieses Gerät kann keine ausreichenden freien Ressourcen finden, die verwendet werden können. (Code 12)	Durch die Ressourcenzuweisung für dieses Gerät ergibt sich ein Konflikt mit einem anderen Gerät, oder die Firmware wurde falsch konfiguriert. Überprüfen Sie die Firmware und sehen Sie auf der Registerkarte <i>Ressourcen</i> des Eigenschaftendialogfelds des Geräts nach, ob Gerätekonflikte bestehen.
Sie müssen den Computer neu starten, damit dieses Gerät ordnungsgemäß funktioniert. (Code 14)	In diesem Fall ist das Gerät gewöhnlich korrekt installiert, aber erst nach einem Neustart des Computers einsatzbereit.
Windows konnte nicht alle Ressourcen identifizieren, die dieses Gerät verwendet. (Code 16)	Prüfen Sie, ob ein signierter Treiber für das Gerät zur Verfügung steht. Wenn einer verfügbar ist und Sie ihn bereits installiert haben, müssen Sie vielleicht die Ressourceneinstellung für das Gerät ändern. Überprüfen Sie die Registerkarte <i>Ressourcen</i> im Eigenschaftendialogfeld des Geräts.
Die Treiber für dieses Gerät müssen erneut installiert werden. (Code 18)	Nach einer Aktualisierung müssen Sie sich vielleicht als Administrator anmelden, um die Installation beenden zu können. Wenn das nicht der Fall ist, tippen oder klicken Sie auf der Registerkarte <i>Treiber</i> auf <i>Treiber aktualisieren</i> , um den Treiber erneut zu installieren.
Die Registrierung ist eventuell beschädigt. (Code 19)	Entfernen Sie das Gerät und installieren Sie es neu. Dadurch sollten falsche oder widersprüchliche Registrierungseinträge korrigiert werden.
Windows entfernt dieses Gerät. (Code 21)	Das System entfernt das Gerät. Die Registrierung ist vielleicht beschädigt. Wenn das Gerät weiterhin diese Meldung anzeigt, starten Sie den Computer erneut.
Das Gerät wurde deaktiviert. (Code 22)	Das Gerät wurde im Geräte-Manager deaktiviert. Um es zu aktivieren, wählen Sie im Eigenschaftendialogfeld des Geräts auf der Registerkarte <i>Allgemein</i> unter <i>Gerätestatus</i> die Schaltfläche <i>Gerät aktivieren</i> .
Dieses Gerät ist entweder nicht vorhanden, funktioniert nicht ordnungsgemäß, oder es wurden nicht alle Treiber installiert. (Code 24)	Das kann ein Hinweis auf einen fehlerhaften Treiber oder ein fehlerhaftes Gerät sein. Der Fehlercode kann auch bei alten Geräten auftreten. Aktualisieren Sie den Treiber.
Die Treiber für dieses Gerät wurden nicht installiert. (Code 28)	Beschaffen Sie einen passenden Treiber für das Gerät und klicken Sie dann auf <i>Treiber aktualisieren</i> , um den Treibersoftwareupdate-Assistenten zu starten.
Dieses Gerät funktioniert nicht ordnungsgemäß, da die Firmware des Geräts die erforderlichen Ressourcen nicht zur Verfügung stellt. (Code 29)	Überprüfen Sie in der Gerätedokumentation, wie die Ressourcen zugewiesen werden müssen. Vielleicht müssen Sie die Firmware aktualisieren oder das Gerät in der Firmware des Systems aktivieren.



Fehlermeldung	Was ist zu tun?
Das Gerät funktioniert nicht ordnungsgemäß, da Windows die für das Gerät erforderlichen Treiber nicht laden kann. (Code 31)	Vielleicht ist der Gerätetreiber nicht zu Windows 8 kompatibel. Beschaffen Sie einen passenden Treiber für das Gerät und tippen oder klicken Sie auf <i>Treiber aktualisieren</i> , um den Treibersoftwareupdate-Assistenten zu starten.
Ein Treiber für dieses Gerät wird nicht gebraucht und wurde deaktiviert. (Code 32)	Ein Dienst, von dem das Gerät abhängig ist, wurde deaktiviert. Überprüfen Sie die Ereignisprotokolle, um herauszufinden, welche Dienste aktiviert und gestartet werden müssen.
Die für dieses Gerät erforderlichen Ressourcen konnten nicht bestimmt werden. (Code 33)	Das kann ein Hinweis auf ein defektes Gerät oder defekte Hardware sein. Der Fehler kann auch bei alten Geräten auftreten. Aktualisieren Sie den Treiber und/oder überprüfen Sie in der Gerätedokumentation, wie die Ressourcen eingestellt werden müssen.
Die Einstellungen für das Gerät können nicht bestimmt werden. (Code 34)	Das alte Gerät muss manuell konfiguriert werden. Überprüfen Sie die Jumpereinstellungen des Geräts und die Firmwareeinstellungen und stellen Sie dann auf der Registerkarte <i>Ressourcen</i> des Eigenschaftendialogfelds des Geräts die Ressourcenverwendung ein.
Die Systemfirmware enthält nicht genügend Informationen, um das Gerät richtig zu konfigurieren und zu verwenden. (Code 35)	Dieser Fehler tritt in Multiprozessorsystemen auf. Aktualisieren Sie die Firmware. Suchen Sie nach einer Firmwareoption zur Verwendung der Multiprozessor-Spezifikation (MPS) 1.1 oder MPS 1.4. Gewöhnlich brauchen Sie MPS 1.4.
Das Gerät fordert einen PCI-Interrupt an, obwohl es für einen ISA-Interrupt konfiguriert ist (oder umgekehrt). (Code 36)	Interrupts von alten Geräten können nicht von mehreren Geräten verwendet werden. Wenn sich ein Gerät in einem PCI-Steckplatz befindet, aber der Steckplatz in der Firmware für ein Legacygerät reserviert wird, kann dieser Fehler auftreten. Ändern Sie die Firmwareeinstellung.
Der Gerätetreiber für diese Hardware kann nicht initialisiert werden. (Code 37)	Starten Sie den Treibersoftwareupdate-Assistenten, indem Sie auf der Registerkarte <i>Treiber</i> auf die Schaltfläche <i>Treiber aktualisieren</i> klicken.
Der Gerätetreiber für diese Hardware kann nicht geladen werden, weil sich eine Vorgängerinstanz des Gerätetreibers noch im Arbeitsspeicher befindet. (Code 38)	Ein im Arbeitsspeicher befindlicher Gerätetreiber führt zu einem Konflikt. Starten Sie den Computer neu.
Der Gerätetreiber für diese Hardware kann nicht geladen werden. Der Treiber ist möglicherweise beschädigt oder nicht vorhanden. (Code 39)	Überprüfen Sie, ob das Hardwaregerät ordnungsgemäß installiert und verbunden wurde und mit Strom versorgt wird. Ist dies der Fall, dann suchen Sie nach einem neuen Treiber oder installieren den vorhandenen Treiber erneut.
Auf die Hardware kann nicht zugegriffen werden, weil die Dienstschlüsselinformationen in der Registrierung fehlen oder nicht richtig eingetragen wurden. (Code 40)	Der Registrierungseintrag für den Gerätetreiber ist ungültig. Installieren Sie den Treiber erneut.
Der Gerätetreiber wurde für die Hardware geladen, aber das Gerät wurde nicht gefunden. (Code 41)	Wenn das Gerät entfernt wurde, können Sie den Treiber deinstallieren, das Gerät neu installieren und dann im Menü <i>Aktion</i> des Geräte-Managers auf <i>Nach geänderter Hardware suchen</i> tippen oder klicken, um den Treiber erneut zu installieren. Wenn das Gerät nicht entfernt wurde oder nicht Plug & Play-fähig ist, brauchen Sie einen neuen oder aktualisierten Treiber für das Gerät. Verwenden Sie den Hardware-Assistenten, um Geräte zu installieren, die nicht Plug & Play-fähig sind. Tippen oder klicken Sie im Geräte-Manager auf das Menü <i>Aktion</i> und dann auf <i>Legacyhardware hinzufügen</i> . ►

Fehlermeldung	Was ist zu tun?
Der Gerätetreiber kann für diese Hardware nicht geladen werden, weil dasselbe Gerät bereits auf dem Computer ausgeführt wird. (Code 42)	Es wurde ein Gerät entdeckt, das zweimal vorhanden ist. Dieser Fehler tritt auf, wenn ein Bustreiber fälschlicherweise zwei gleich benannte Geräte erkennt oder wenn ein Gerät mit derselben Seriennummer am neuen Ort erkannt wird, bevor es vom alten Ort entfernt wurde. Starten Sie den Computer neu, um dieses Problem zu beseitigen.
Dieses Gerät wurde angehalten, weil es Fehler gemeldet hat. (Code 43)	Das Gerät wurde vom Betriebssystem gestoppt. Sie müssen es vielleicht deinstallieren und dann erneut installieren. Vielleicht hat das Gerät ein Problem mit der No-Execute-Funktion des Prozessors. Suchen Sie in diesem Fall nach einem neuen Treiber.
Dieses Hardwaregerät wurde von einer Anwendung oder einem Dienst deaktiviert. (Code 44)	Das Gerät wurde vom Betriebssystem gestoppt. Starten Sie den Computer neu. Vielleicht hat das Gerät ein Problem mit der No-Execute-Funktion des Prozessors. Suchen Sie in diesem Fall nach einem neuen Treiber.
Dieses Hardwaregerät ist zurzeit nicht an den Computer angeschlossen. (Code 45)	Wenn Sie den Geräte-Manager starten, während die Umgebungsvariable <code>DEVMGR_SHOW_NONPRESENT_DEVICES</code> auf den Wert 1 gesetzt ist, werden alle vorher angeschlossenen Geräte, die nicht mehr vorhanden sind, in der Geräteliste angezeigt und bekommen diesen Fehlercode zugewiesen. Sie können diese Meldung löschen, indem Sie das Gerät an den Computer anschließen oder den Geräte-Manager starten, ohne dass diese Umgebungsvariable gesetzt ist.
Windows kann auf dieses Hardwaregerät nicht zugreifen, weil das Betriebssystem gerade heruntergefahren wird. (Code 46)	Das Gerät ist nicht verfügbar, weil der Computer gerade herunterfährt. Sobald der Neustart des Computers abgeschlossen ist, müsste das Gerät wieder verfügbar sein.
Dieses Hardwaregerät kann nicht verwendet werden, weil es für "Sicheres Entfernen" konfiguriert, aber noch nicht vom Computer getrennt wurde. (Code 47)	Wenn Sie eine Auswurf Taste gedrückt haben, erhalten Sie diesen Fehler, wenn das Gerät entfernt werden kann. Sie können das Gerät erneut benutzen, indem Sie es abstecken und dann wieder anstecken oder den Computer neu starten.
Die Software für dieses Gerät wurde nicht initialisiert, weil sie auf Windows Fehler verursacht. Wenden Sie sich an den Hardwarehersteller, um einen neuen Treiber zu erhalten. (Code 48)	Der Treiber für dieses Gerät ist inkompatibel zu Windows, daher wurde er nicht geladen. Besorgen und installieren Sie einen neuen oder aktualisierten Treiber vom Hardwarehersteller.
Die neuen Hardwaregeräte können nicht gestartet werden, da die Systemstruktur zu groß ist (die Struktur überschreitet die Registrierungsgrößenbeschränkung). (Code 49)	Die Systemstruktur der Registrierung hat ihre Maximalgröße überschritten. Neue Geräte funktionieren erst wieder, wenn die Größe verringert wird. Möglicherweise wird dieser Fehler durch Geräte verursacht, die nicht mehr an den Computer angeschlossen, aber noch im Systemzweig der Registrierung eingetragen sind. Versuchen Sie, alle Hardwaregeräte zu deinstallieren, die Sie nicht mehr benutzen.

Kapitel 10

Erledigen von Wartungs- und Supportaufgaben

In diesem Kapitel:

Verwalten automatischer Updates	352
Verwenden der Remoteunterstützung zur Problembehebung	361
Erkennen und Beheben von Windows 8-Fehlern	366
Planen von Wartungsarbeiten	368
Sichern und Wiederherstellen eines Computers	373
Problembehandlung für Systemstart und Herunterfahren	385

In diesem Buch habe ich an mehreren Stellen Support- und Problembehandlungstechniken beschrieben, die Ihnen bei der Administration von Windows 8 helfen. In diesem Kapitel lernen Sie Techniken kennen, mit denen Sie den Support für Computer verbessern, auf die Sie keinen direkten Zugriff haben, und mit denen Sie bestimmte Problemarten beseitigen. Ich beginne mit einer Beschreibung der automatischen Updates und zeige dann, wie Sie mit der Remoteunterstützung Probleme auch dann beseitigen können, wenn Sie nicht selbst vor dem Computer des Benutzers sitzen. Vergessen Sie in diesem Zusammenhang nicht die Problemaufzeichnung (*Psr.exe*). Wie in Kapitel 7, »Verwalten von Benutzerzugriff und Sicherheit«, beschrieben, können Sie mit diesem Tool Details über ein Problem aufzeichnen, das bei einem Benutzer auftritt; dazu brauchen Sie selbst keinen Zugriff auf den Computer des Benutzers.

Verwalten automatischer Updates

Die Standardfunktion von Windows 8 für automatische Updates heißt *Windows Update*. Windows Update wird nicht nur zur Aktualisierung des Betriebssystems verwendet, sondern auch zur Aktualisierung der Programme, die zum Lieferumfang des Betriebssystems gehören, und zur Aktualisierung von Gerätetreibern. Die folgenden Abschnitte beschreiben, wie Windows Update funktioniert und wie es Sie dabei unterstützt, den Computer auf dem neusten Stand zu halten.

Windows Update: Die Grundlagen

Windows Update ist eine Clientkomponente, die regelmäßig einen dafür vorgesehenen Server kontaktiert und ihn auf Updates überprüft. Sind Updates verfügbar, kann Windows Update sie je nach Konfiguration automatisch herunterladen und installieren oder Benutzer und Administratoren darüber informieren, dass Updates verfügbar sind. Die Serverkomponente, mit der Windows Update Kontakt aufnimmt, ist entweder die Windows Update-Website von Microsoft (<http://windowsupdate.microsoft.com/>) oder ein dafür vorgesehener Windows-Updatedienstserver, der von Ihrer Organisation eingerichtet und betrieben wird.

Windows Update unterstützt die Verteilung und Installation folgender Updatetypen:

- **Kritische Updates** Updates, die als entscheidend für die Stabilität und den Schutz eines Computers eingestuft werden
- **Sicherheitsupdates** Updates, die das System sicherer machen sollen
- **Update-Rollups** Updates, die andere Updates enthalten
- **Service Packs** Ein umfassendes Update des Betriebssystems und seiner Komponenten, gewöhnlich mit kritischen Updates, Sicherheitsupdates und Update-Rollups
- **Optionale Updates** Updates, die möglicherweise nützlich sind, beispielsweise Updates für Treiber

HINWEIS

Windows Update lädt Updates für Treiber standardmäßig von der Windows Update-Website herunter. Sie können auch festlegen, dass Windows Update die verwalteten WSUS-Server (Windows Server Update Services) nach Treiberupdates durchsuchen soll, oder dass diese Server zuerst durchsucht werden sollen und die Suche nur dann in Windows Update fortgesetzt werden soll, wenn dort keine Updates zu finden sind. Dazu aktivieren und konfigurieren Sie die Richtlinie *Suchserver für Gerätetreiberupdates festlegen* in den administrativen Vorlagen der Computerkonfiguration unter *System\Geräteinstallation*. Wählen Sie nach Bedarf *Verwalteten Server und anschließend Windows Update durchsuchen*.

Ein wichtiger Teil der Erweiterung besteht darin, dass Windows Update Downloads priorisieren kann, damit Updates in der Reihenfolge ihrer Wichtigkeit angewendet werden. Die wichtigsten Updates können also zuerst heruntergeladen und installiert werden, bevor die weniger wichtigen folgen. Außerdem können Sie einstellen, wie ein Computer überprüft, ob Updates vorliegen und wie er Updates installiert. Üblich ist eine Prüfung in Abständen von 22 Stunden. In den Gruppenrichtlinien können Sie dieses Intervall ändern. Standardmäßig installieren Computer täglich nachts um 3 Uhr Ortszeit die Updates, die sie heruntergeladen haben. Sie können bei Bedarf die Installationszeit ändern und die Installation so einstellen, dass Sie informiert werden.

Windows 8 reduziert die Anzahl der nach Updates erforderlichen Neustarts, indem es zulässt, dass eine neue Version einer aktualisierten Datei installiert wird, während die alte Datei noch von einer Anwendung oder einer Betriebssystemkomponente benutzt wird. Dabei kennzeichnet Windows 8 die betreffende Datei für die Aktualisierung und ersetzt sie beim nächsten Start der Anwendung automatisch. Bei einigen Anwendungen und Komponenten kann Windows 8 die Daten der Anwendung speichern, die Anwendung schließen, die Datei aktualisieren und die Anwendung dann wieder starten. Insgesamt hat der Aktualisierungsvorgang also weniger direkte Auswirkungen auf Benutzer.

PRAXISTIPP

Bei der automatischen Aktualisierung wird zur Übertragung der Dateien der intelligente Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS) verwendet. BITS ist ein Dienst, der im Hintergrund Dateien übertragen kann und in der Lage ist, unterbrochene Übertragungen wieder aufzunehmen. BITS Version 4.0, das in Windows 8 vorliegt, verbessert den Übertragungsmechanismus so, dass die verfügbare Bandbreite effizienter genutzt wird. Das bedeutet auch, dass insgesamt weniger Daten übertragen werden und die Übertragung schneller erfolgt. Durch Gruppenrichtlinien lässt sich BITS so einstellen, dass Updates nur zu bestimmten Zeiten heruntergeladen werden und die verwendete Bandbreite begrenzt wird. Sie konfigurieren diese und andere Einstellungen mit der Richtlinie *Arbeitszeitplan zur Beschränkung der für BITS-Übertragungen im Hintergrund verwendeten maximalen Netzwerkbandbreite einrichten*, zu finden in den Gruppenrichtlinien unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Intelligenter Hintergrundübertragungsdienst*. Außerdem kann Windows 8 Updates mit BITS 4.0 von vertrauenswürdigen Partnern aus dem LAN (Local Area Network), von einem Updateserver oder direkt von Microsoft anfordern. Sobald ein anderer Computer im Netzwerk (ein »Peer«) über eine Kopie eines Updates verfügt, können andere Computer im LAN dies automatisch erkennen und das Update direkt von diesem Peer herunterladen. Das erforderliche Update braucht also im Prinzip nur einmal über das WAN (Wide Area Network) übertragen zu werden, und nicht Dutzende oder Hunderte Male.

Sie können automatische Updates auf verschiedene Weise benutzen. Das System lässt sich folgendermaßen einstellen:

- **Updates automatisch installieren** Bei dieser Einstellung ruft das Betriebssystem in einem einstellbaren Intervall (standardmäßig alle 22 Stunden) die verfügbaren Updates ab und installiert sie nach Zeitplan, standardmäßig nachts um 3 Uhr. Dieses Verhalten wurde gegenüber Windows XP geändert, denn es ist nicht mehr erforderlich, dass Benutzer die Updates akzeptieren müssen, bevor sie installiert werden. Stattdessen werden Updates automatisch heruntergeladen und dann nach Zeitplan installiert. Als Zeitplan lässt sich die tägliche Installation zu einem bestimmten Zeitpunkt oder die Installation an einem bestimmten Wochentag zu einem bestimmten Zeitpunkt einstellen.
- **Updates herunterladen, aber Installation manuell durchführen** Bei dieser Einstellung (der Standardeinstellung) ruft das Betriebssystem alle Updates ab, sobald sie verfügbar sind, und informiert den Benutzer, wenn sie zur Installation bereit sind. Der Benutzer kann die Updates dann annehmen oder ablehnen. Angenommene Updates werden installiert. Abgelehnte Updates werden zwar nicht installiert, bleiben aber auf dem System und können bei Bedarf später installiert werden.

- **Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen** Bei dieser Einstellung informiert das Betriebssystem den Benutzer, bevor es Updates abrufen. Entscheidet sich der Benutzer für das Herunterladen eines Updates, erhält er noch die Gelegenheit, es anzunehmen oder abzulehnen. Angenommene Updates werden installiert. Abgelehnte Updates werden zwar nicht installiert, bleiben aber auf dem System und können bei Bedarf später installiert werden.
- **Nie nach Updates suchen** Wenn automatische Updates deaktiviert sind, werden Benutzer nicht über Updates informiert. Allerdings können Sie Updates manuell von der Windows Update-Website herunterladen.

Wenn Windows Update so konfiguriert ist, dass es Updates automatisch herunterlädt und installiert, werden die Benutzer nur beiläufig über die Verfügbarkeit oder Installation der Updates benachrichtigt. Wenn Sie eine Benachrichtigung in der Taskleiste antippen oder anklicken, erhalten Sie ausführlichere Informationen über ein Update.

Wiederherstellen von Windows-Binärdateien und -Komponenten via Windows Update

Windows kann Windows Update auch für andere Zwecke nutzen:

- Windows Update wird zur Wiederherstellung von gelöschten Windows-Binärdateien verwendet.
- Windows Update wird zur erneuten Installation beschädigter Komponenten verwendet.

Binärdateien, die zur Installation von Windows-Funktionen erforderlich sind, werden in den Richtlinien *Nutzlastdateien* (engl. Payloads) genannt. Auf Computern, auf denen Windows Server 2012 verwendet wird, können Sie ein optionales Feature nicht nur deinstallieren, sondern auch die dazugehörigen Binärdateien deinstallieren und entfernen. Dazu verwenden Sie das Cmdlet *Uninstall-WindowsFeature* mit dem Parameter *Remove*.

Mit dem Cmdlet *Install-WindowsFeature* können Sie ein Feature installieren und die dazugehörigen Binärdateien wiederherstellen. Standardmäßig werden diese Binärdateien über Windows Update wiederhergestellt. Um andere Quelldateipfade anzugeben, aktivieren und konfigurieren Sie die Richtlinie *Einstellungen für die Installation optionaler Komponenten und die Reparatur von Komponenten angeben* in den administrativen Vorlagen der Computerkonfiguration unter *System*. Mit der Richtlinie können Sie auch festlegen, dass keine Binärdateien für Betriebssystemfeatures (also »Nutzlastdateien«) von Windows Update heruntergeladen werden sollen.

Als alternative Dateiquellpfade eignen sich freigegebene Ordner oder WIM-Dateien (Windows Imaging). Trennen Sie die Pfade durch Semikolons voneinander. Für WIM-Dateien geben Sie mit folgender Syntax den UNC-Pfad (Universal Naming Convention) zum freigegebenen Ordner an, der die WIM-Datei enthält, und den Index des zu verwendenden Abbilds:

```
wim:\\ServerName\FreigabeName\\AbbildDateiName.wim:Index
```

Darin ist *ServerName* der Name des Servers, *FreigabeName* der Name des freigegebenen Ordners, *Abbild-DateiName.wim* der Name der WIM-Datei und *Index* der Index des zu verwendenden Abbilds, wie in:

```
wim:\\CorpServer62\\Images\\install.wim:2
```

Wenn eine Betriebssystemkomponente beschädigt ist und Windows 8 dies erkennt, lässt sich der für die Reparatur der Komponente erforderliche Inhalt von Windows Update herunterladen. Standardmäßig erfolgt das Komponentenupdate über WSUS (Windows Server Update Services), sofern verfügbar. Durch die Aktivierung und Konfiguration der Richtlinie *Einstellungen für die Installation optionaler Komponenten und die Reparatur von Komponenten angeben* können Sie einen anderen Quelldateipfad angeben. Sie

können auch festlegen, dass Windows Update das Update direkt von der Windows Update-Website herunterladen soll statt von WSUS.

Konfigurieren der automatischen Updates

Windows 8 unterteilt Updates in folgende Kategorien:

- **Wichtige Updates** Umfasst kritische Updates, Sicherheitsupdates, Update-Rollups und Service Packs für das Betriebssystem und für Programme, die zum Lieferumfang des Betriebssystems gehören.
- **Empfohlene Updates** Umfasst Updates für Treiber, die mit dem Betriebssystem ausgeliefert werden, sowie empfohlene optionale Updates.
- **Updates für Microsoft-Produkte** Umfasst Updates für andere Microsoft-Produkte, die auf dem Computer installiert sind, sowie neue optionale Microsoft-Software.
- **Point-and-Print-Treiber** Umfasst Updates für Treiber, die clientseitiges Rendering ermöglichen.

HINWEIS In der Standardeinstellung umfasst Windows Update auch Updates aus Webkompatibilitätslisten von Microsoft. Die aufgelisteten Sites werden in der Kompatibilitätsansicht automatisch angezeigt. Sie können dies in *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Windows-Komponenten\Internet Explorer\Kompatibilitätsansicht* konfigurieren.

PRAXISTIPP Wenn Sie die Standardedition von Windows 8 einsetzen, setzt Windows Update die Suche nach kompatiblen Point-and-Print-Treibern auch dann fort, wenn es auf dem Computer selbst und auf der Windows Update-Site keine findet. Findet der Computer keinen geeigneten Treiber, versucht er, eine Verbindung mit irgendeinem verfügbaren Treiber herzustellen, der die Hardware unterstützt. Wenn Sie allerdings die Enterprise-Editionen von Windows 8 verwenden, müssen Sie explizit die Richtlinie *Point-and-Print-Verbindung auf die Suche in Windows Update ausdehnen* aktivieren, damit dieses Verhalten angewendet wird. Sie finden diese Richtlinie unter *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Drucker*.

In der Standardeinstellung ist Windows 8 so konfiguriert, dass es wichtige Updates automatisch installiert. Gehen Sie folgendermaßen vor, um die automatischen Updates auf einem bestimmten Computer individuell zu konfigurieren:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann unter *Windows Update* auf *Automatische Updates aktivieren oder deaktivieren*.
2. Stellen Sie mit der Auswahlliste ein, ob und wie Updates eingespielt werden sollen (Abbildung 10.1).
3. Aktivieren Sie das Kontrollkästchen *Empfohlene Updates auf die gleiche Weise wie wichtige Updates bereitstellen*, wenn Sie Updates aktiviert haben und Treiber sowie optionale Updates installieren wollen.
4. Tippen oder klicken Sie auf *OK*.

Mit einer Erweiterungskomponente namens Microsoft Update können Sie Windows Update erweitern, damit auch Updates für andere auf dem Computer installierte Microsoft-Produkte sowie neue optionale Microsoft-Software eingeschlossen werden. Wenn Sie Microsoft-Produkte installieren, kann Microsoft Update automatisch im Rahmen der Installation heruntergeladen und installiert werden.

Ob ein Computer Microsoft Update verwendet, können Sie folgendermaßen überprüfen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*.
2. Wenn der Computer für die Verwendung von Windows Update konfiguriert ist, sehen Sie im unteren Teil der Seite folgende Angabe:

Sie erhalten Updates: Für Windows und andere Produkte von Microsoft Update.

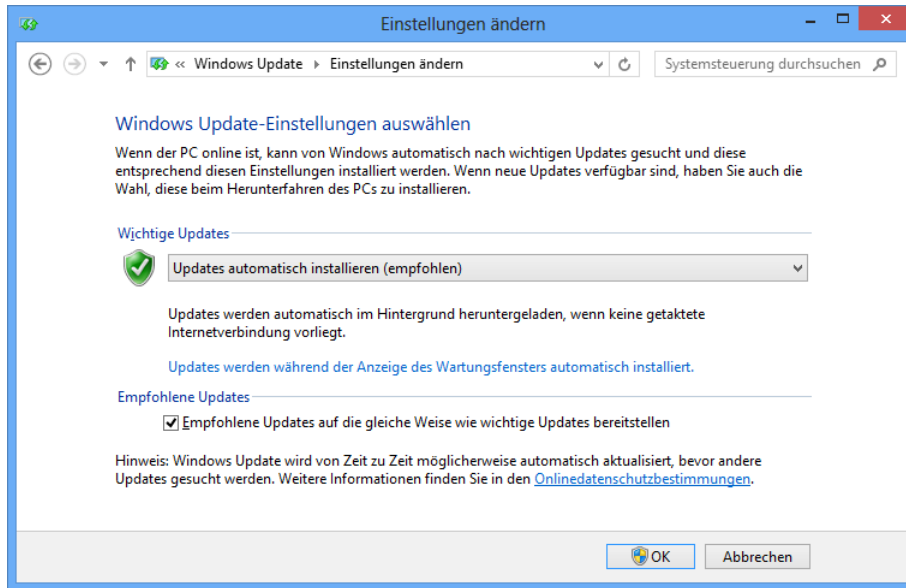


Abbildung 10.1 Konfigurieren von Windows Update

So installieren Sie Microsoft Update:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*.
2. Tippen oder klicken Sie unten in dem Kästchen mit der Beschriftung *Rufen Sie Updates für weitere Microsoft-Produkte ab* auf *Weitere Informationen*. Dadurch öffnet sich die Windows Update-Seite von der Microsoft-Website im Standardbrowser.
3. Lesen Sie den Text über Microsoft Update, wählen Sie *Ich stimme den Nutzungsbedingungen von Microsoft Update zu* und tippen oder klicken Sie dann auf *Installieren*.
4. Solange automatische Updates aktiviert sind, erhält der Computer im Rahmen der automatischen Aktualisierung auch Updates für Microsoft-Produkte. Wenn Sie nun mit Windows Update arbeiten, können Sie auf *Einstellungen ändern* tippen oder klicken und Microsoft Updates aktivieren oder deaktivieren, indem Sie das Kontrollkästchen *Updates für andere Microsoft-Produkte bereitstellen, wenn ein Windows-Update ausgeführt wird* aktivieren oder deaktivieren.

Standardmäßig wird Windows Update im Rahmen der automatischen Wartung täglich nachts um 3 Uhr ausgeführt, aber der Computer wird zu diesem Zweck nicht extra reaktiviert. Ist der Computer zur vorgesehenen Zeit ausgeschaltet, erfolgt die automatische Wartung das nächste Mal, wenn der Computer eingeschaltet ist und sich im Leerlauf befindet. Die automatische Wartung erfolgt auch, wenn der Computer eingeschaltet ist, sich im Leerlauf befindet und die Wartung hinter dem Zeitplan liegt.

So können Sie dieses Verhalten ändern:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann unter *Windows Update* auf *Automatische Updates aktivieren oder deaktivieren*.
2. Tippen oder klicken Sie auf die Verknüpfung *Updates werden während der Anzeige des Wartungsfensters automatisch installiert*. Verwenden Sie die Auswahlliste für die Festlegung der gewünschten Wartungszeit, beispielsweise 5 Uhr morgens (Abbildung 10.2).

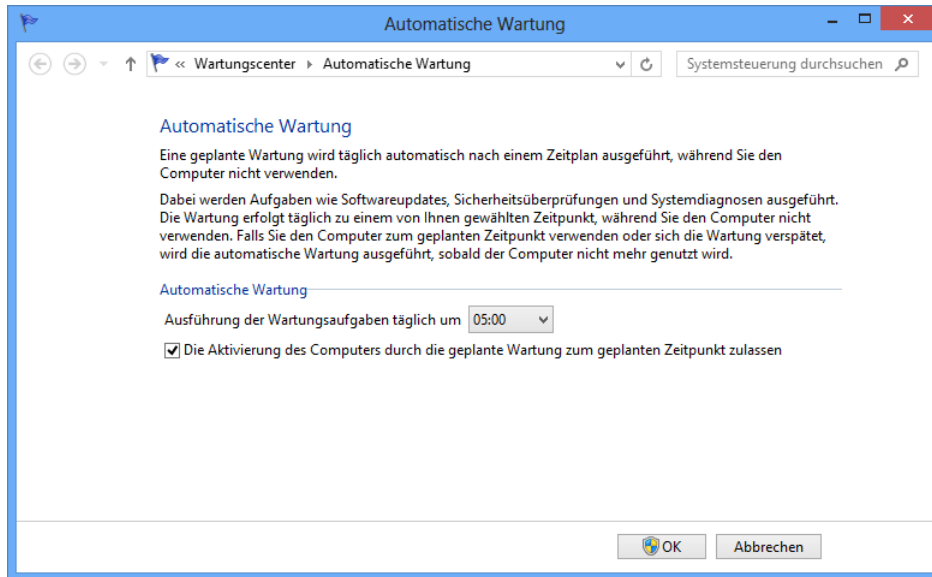


Abbildung 10.2 Verwalten des geplanten Wartungsfensters

3. Wenn der Computer am Stromnetz angeschlossen ist, können Sie auch festlegen, dass er für die geplanten Wartungsarbeiten aktiviert wird. Aktivieren Sie dazu das entsprechende Kontrollkästchen.
4. Tippen oder klicken Sie auf *OK*.

In einer Active Directory-Domäne können Sie automatische Updates mit den Gruppenrichtlinien in *Richtlinien\Administrative Vorlagen\Windows-Komponenten\Windows Update* unter *Computerkonfiguration* zentral konfigurieren und verwalten. Tabelle 10.1 fasst die wichtigsten Richtlinien zusammen, wobei eine der Richtlinien unter *Benutzerkonfiguration\Windows-Komponenten* zu finden ist.

TIPP Mit den Richtlinien aus den administrativen Vorlagen der Computerkonfiguration unter *Windows-Komponenten\Wartungszeitplan* können Sie die Ausführung der automatischen Wartung steuern. Die Aktivierungszeitgrenze ist die vorge-sehene Zeit für den täglichen Start der automatischen Wartung. Für virtuelle Maschinen, die auf einem Computer laufen, fügt Windows noch eine zufällige Verzögerung von bis zu 30 Minuten hinzu. Auch diese Verzögerung lässt sich Einstellen.

Tabelle 10.1 Richtlinien zum Verwalten von automatischen Updates

Richtlinie	Funktion
<i>Automatische Updates konfigurieren</i>	Mit dieser Einstellung konfigurieren Sie Automatische Updates, wobei Sie ähnliche Optionen zur Verfügung haben, wie in diesem Abschnitt beschrieben. Sie können auch die Installation im Rahmen der geplanten Wartungen durchführen (sofern sie aktiviert ist). Aktivieren und konfigurieren Sie zu diesem Zweck die Richtlinien unter <i>Computerkonfiguration\Windows-Komponenten\Wartungszeitplan</i> .
<i>Automatische Updates sofort installieren</i>	Wenn diese Einstellung aktiviert ist, werden Updates, die weder Windows-Dienste unterbrechen noch Neustarts des Computers erfordern, sofort nach dem Herunterladen installiert.
<i>Clientseitige Zielzuordnung aktivieren</i>	Wenn sie aktiviert ist und Sie einen Ort für einen Microsoft-Updatedienst im Intranet angegeben haben, ermöglicht diese Einstellung einem Administrator die Definition einer Zielgruppe für das aktuelle Gruppenrichtlinienobjekt. Durch die Einführung clientseitiger Zielgruppen können Administratoren kontrollieren, welche Updates auf bestimmten Computergruppen installiert werden. Bevor ein Update bereitgestellt wird, muss es für eine bestimmte Zielgruppe zugelassen werden. Die Einstellung gilt nur, wenn Sie im Intranet einen Microsoft-Updatedienst verwenden.
<i>Empfohlene Updates über Automatische Updates aktivieren</i>	Ist diese Richtlinie aktiviert, werden neben den wichtigen Updates auch empfohlene Updates und andere optionale Updates installiert, einschließlich Treiberupdates.
<i>Erneut zu einem Neustart für geplante Installationen auffordern</i>	Ist diese Einstellung aktiviert und Automatische Updates auf die Installation von Updates nach Zeitplan eingestellt, sorgt diese Einstellung dafür, dass der angemeldete Benutzer nach einer gewissen Zeit erneut auf den erforderlichen Neustart hingewiesen wird, falls er den letzten Hinweis ignoriert hat. Ist diese Einstellung deaktiviert oder nicht konfiguriert, beträgt das Standardintervall für den erneuten Hinweis 10 Minuten.
<i>Internen Pfad für den Microsoft Updatedienst angeben</i>	Ist diese Einstellung aktiviert, können Sie den vollständigen Domännennamen des Microsoft Updateservers angeben, der von Ihrer Organisation eingerichtet und betrieben wird, sowie den dazugehörigen Statistikserver. Beide Dienste können auf demselben Server ausgeführt werden.
<i>Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind</i>	Mit dieser Einstellung können Sie festlegen, dass der Computer nach der Installation von Updates, die einen Neustart erfordern, nicht neu gestartet wird, falls ein Benutzer angemeldet ist. Stattdessen wird der Benutzer darüber informiert, dass ein Neustart erforderlich ist. Nach dem Neustart des Computers wird die Installation des Updates abgeschlossen.
<i>Neustart für geplante Installationen verzögern</i>	Ist nach der Installation eines Updates ein Neustart des Computers erforderlich, wird der Computer mit einer Verzögerung von 15 Minuten neu gestartet. Um eine andere Verzögerung einzustellen, aktivieren Sie diese Richtlinie und legen dann die Verzögerungszeit fest.
<i>Nichtadministratoren gestatten, Updatebenachrichtigungen zu erhalten</i>	Ist diese Einstellung aktiviert, kann jeder Benutzer, der auf dem Computer angemeldet ist, Updatebenachrichtigungen erhalten, sofern dies in der Konfiguration der automatischen Updates vorgesehen ist. Ist diese Einstellung deaktiviert oder nicht konfiguriert, erhalten nur Administratoren Updatebenachrichtigungen.
<i>Suchhäufigkeit für automatische Updates</i>	Diese Einstellung legt das Intervall fest, in dem eine Überprüfung auf neue Updates erfolgt. Standardmäßig prüfen Computer alle 22 Stunden, ob neue Updates vorliegen. Wenn Sie diese Richtlinie aktivieren und ein anderes Intervall einstellen, wird dieses Intervall mit einer zufällig gewählten Abweichung von bis zu 20 Prozent übernommen. Wenn Sie also ein Intervall von 10 Stunden einstellen, hängt das tatsächlich verwendete Intervall vom Computer ab und liegt ungefähr zwischen 8 und 12 Stunden.
<i>Windows Update-Energieverwaltung aktivieren, um das System zur Installation von geplanten Updates automatisch zu reaktivieren</i>	Wenn diese Richtlinie aktiviert ist und der Computer für die automatisierte Installation von Updates nach einem Zeitplan konfiguriert ist, verwendet Windows Update die Energieverwaltungsfunktionen des Computers, um den Computer zur geplanten Updatezeit aus dem Energiesparmodus aufzuwecken und dann die Updates zu installieren. Dieser Prozess findet nicht statt, wenn der Computer im Akkubetrieb läuft. ►

Richtlinie	Funktion
<i>Zeitplan für geplante Installationen neu erstellen</i>	Ist diese Einstellung aktiviert, gibt sie an, wie lange nach einem Systemstart gewartet wird, bis eine noch ausstehende Installation durchgeführt wird.
<i>Zugriff auf alle Windows Update-Funktionen entfernen</i>	Wenn Sie diese Einstellung aktivieren, werden alle Windows Update-Komponenten aus der Benutzerschnittstelle entfernt. Automatische Updates werden deaktiviert und Benutzer können nicht auf Windows Update zugreifen (eine Richtlinie aus der Benutzerkonfiguration).

Suchen nach Updates

Die Hauptseite *Windows Update* zeigt an, wann der Computer oder ein Benutzer die letzte Überprüfung auf neue Updates vorgenommen hat, wann das letzte Mal Updates installiert wurden und ob die automatischen Updates konfiguriert sind. Mit folgenden Schritten können Sie die Nutzungsdaten überprüfen oder eine manuelle Prüfung auf neue Updates vornehmen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*. Sie sehen Angaben über die letzte Prüfung auf Updates, die letzte Installation von Updates (auch wenn sie vielleicht nicht erfolgreich war) und die aktuelle Updatekonfiguration.
2. Wenn Sie manuell eine Suche nach Updates durchführen möchten, tippen oder klicken Sie auf *Nach Updates suchen*.
3. Wenn Sie optionale Updates installieren wollen, die möglicherweise verfügbar sind, können Sie die Verknüpfung anklicken, die zeigt, wie viele optionale Updates verfügbar sind.
4. Wählen Sie auf der Seite *Zu installierende Updates auswählen* die Updates aus, die Sie installieren wollen, und tippen oder klicken Sie auf *OK*.

Anzeigen des Updateverlaufs und der installierten Updates

Der Downloadmanager von Windows Update trägt erfolgreiche und fehlgeschlagene Updates in ein Updateprotokoll ein. Sie können dieses Protokoll folgendermaßen einsehen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*.
2. Tippen oder klicken Sie im linken Anzeigebereich auf *Updateverlauf anzeigen*. Dadurch öffnet sich die Seite *Updateverlauf anzeigen*.

Updates, die auf der Seite *Updateverlauf anzeigen* mit dem Status *Erfolgreich* angezeigt werden, wurden heruntergeladen und installiert. Updates, die mit dem Status *Fehlgeschlagen* angezeigt werden, wurden zwar heruntergeladen, konnten aber nicht installiert werden. Vielleicht sehen Sie auch Statusangaben wie *Neustart ausstehend* oder *Abgebrochen*. Einige Updates können nur in der Startphase des Betriebssystems durchgeführt werden. Es sind solche Updates, die den Status *Neustart ausstehend* erhalten. Nach dem Neustart des Computers und der Installation des Updates ändert sich der Status entsprechend. Das Herunterladen von Updates kann aus verschiedenen Gründen abgebrochen werden. Benutzer können das Herunterladen von Updates zum Beispiel in Windows Update abbrechen. Auch der Neustart eines Computers kann zum Abbruch des Herunterladens eines Updates führen.

Wenn Sie ein Update entfernen möchten, tippen oder klicken Sie auf der Seite *Updateverlauf anzeigen* auf *Installierte Updates*. Klicken Sie dann auf der Seite *Installierte Updates* mit der rechten Maustaste auf das Update, das Sie nicht haben wollen, oder halten Sie es gedrückt, und wählen Sie *Deinstallieren*.

Entfernen von Updates zur Problembehebung

Machen Sie sich keine Sorgen, wenn ein automatisches Update auf einem System Probleme verursacht. Sie können ein Update in derselben Weise entfernen, wie Sie andere Programme entfernen. Gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*.
2. Tippen oder klicken Sie auf *Updateverlauf anzeigen* und dann auf *Installierte Updates*.
3. Um ein Update zu entfernen, wählen Sie es in der Liste aus und tippen oder klicken dann auf *Deinstallieren*.

Ausblenden verfügbarer Updates

Im Lauf der Zeit sammeln sich bei einem Benutzer möglicherweise eine Reihe von Updates an, die absichtlich nicht installiert wurden, aber dennoch in der Liste der Updates aufgeführt werden, die für eine Installation zur Verfügung stehen. Wenn Sie oder der Benutzer ein Update geprüft haben und entscheiden, es nicht zu installieren, können Sie es folgendermaßen ausblenden:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*.
2. Tippen oder klicken Sie auf den Link, der angibt, wie viele Updates verfügbar sind.
3. Tippen oder klicken Sie auf der Seite *Zu installierende Updates auswählen* mit der rechten Maustaste auf das Update, das Sie nicht installieren wollen, oder halten Sie es gedrückt, und wählen Sie den Befehl *Update ausblenden*.

Wiederherstellen abgelehnter Updates

Wenn ein Benutzer ein Update ablehnt, er nicht über Updates benachrichtigt werden möchte oder er Updates nicht automatisch installieren will, können Sie die Updates wiederherstellen, damit sie manuell installiert werden können. Gehen Sie dazu folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *Windows Update*.
2. Tippen oder klicken Sie auf *Ausgeblendete Updates anzeigen*.
3. Wählen Sie auf der Seite *Ausgeblendete Updates anzeigen* ein Update aus, das Sie installieren möchten, und tippen oder klicken Sie auf *Wiederherstellen*.
4. Windows 8 stellt abgelehnte Updates so wieder her, dass sie mit dem üblichen Benachrichtigungs- und Installationsprozess gewählt und installiert werden können.

Verwenden der Remoteunterstützung zur Problembehebung

Remoteunterstützung ermöglicht es den Supportmitarbeitern, den Desktop eines Benutzers einzusehen und zeitweilig die Kontrolle zu übernehmen, um bestimmte Probleme zu lösen oder den Benutzer durch komplexe Aufgaben zu führen. Sobald die Remoteunterstützung lokal konfiguriert ist, wie in Kapitel 7 beschrieben, oder über Gruppenrichtlinien eingerichtet wurde, wie in Kapitel 5, »Konfigurieren von Benutzer- und Computerrichtlinien«, besprochen, können Sie mit dieser Funktion arbeiten.

Funktionsweise der Remoteunterstützung

Remoteunterstützung ist unter Windows XP und neueren Windows-Versionen verfügbar. Nur Benutzer, die diese Betriebssysteme verwenden, können Remoteunterstützungseinladungen versenden und darauf reagieren. Im Unternehmen ist es am einfachsten, wenn Sie nach dem folgenden Prinzip mit der Remoteunterstützung arbeiten:

1. Stellen Sie sicher, dass Sie mit einem Benutzerkonto arbeiten, das Mitglied der lokalen Gruppe *Remoteunterstützungsanbieter* ist (oder einer Gruppe, die Mitglied dieser Gruppe ist).
2. Stellen Sie sicher, dass Windows-Firewallausnahmen für die ausführbaren Dateien *Msra.exe* und *Raserver.exe* eingerichtet sind und TCP-Port 135 für DCOM geöffnet ist. Normalerweise werden diese Einstellungen über Gruppenrichtlinien standardmäßig konfiguriert.
3. Stellen Sie sicher, dass der andere Computer so konfiguriert ist, dass er Remoteunterstützung erlaubt, und stellen Sie dann eine Verbindung zu diesem Computer her, indem Sie seinen Computernamen oder die IP-Adresse angeben.

WEITERE INFORMATIONEN

Windows 8 erkennt es, wenn eine Firewall Remoteunterstützungsverbindungen blockiert. Ist dies der Fall und ein Benutzer versucht, eine Unterstützungseinladung zu versenden, erhält er in der Windows-Remoteunterstützung eine Meldung, die besagt, dass der Computer nicht für den Versand von Einladungen eingerichtet ist. Er kann auf *Reparieren* tippen oder klicken, damit die Windows-Netzwerkd Diagnose das Problem untersuchen kann. Anschließend kann er versuchen, die angebotenen Reparaturmaßnahmen umzusetzen, sofern er über die Berechtigungen eines Administrators verfügt, und das Diagnoseprogramm schließen.

In einer Unternehmensumgebung gewähren Sie folgendermaßen Remoteunterstützung:

1. Öffnen Sie die Windows-Remoteunterstützung, zum Beispiel indem Sie die WINDOWS-Taste drücken, *msra.exe* eingeben und die EINGABETASTE drücken.
2. Tippen oder klicken Sie im Assistenten *Windows-Remoteunterstützung* auf *Einem Benutzer, von dem Sie eingeladen wurden, Hilfe anbieten*.
3. Tippen oder klicken Sie auf die Verknüpfung *Erweiterte Verbindungsoption für Helpdesk*.
4. Geben Sie den Namen oder die IP-Adresse des Computers ein, dem Sie helfen wollen, und tippen oder klicken Sie auf *Weiter*, um die Verbindung zu diesem Computer aufzubauen.

Benutzer leiten eine Remoteunterstützungssitzung ein, indem sie eine Einladung versenden. Das Supportpersonal leitet Sitzungen ein, indem es Benutzern Hilfe anbietet. Nachdem eine Sitzung zustande gekommen ist, können Helfer mit Benutzern kommunizieren, deren Arbeit auf dem Monitor verfolgen und, sofern es ihnen erlaubt wird, die Kontrolle über die Computer übernehmen. Remoteunterstützungseinladungen lassen sich in Dateiform erstellen oder als E-Mail versenden:

- **E-Mail-Einladung** E-Mail-Einladungen werden als E-Mails an die Adresse des Empfängers gesendet. Ein Anhang in der Nachricht dient zur Einleitung der Remoteunterstützungssitzung. Sie können eine Standardadresse für die E-Mails einrichten, wie zum Beispiel *RemoteAssist@name_ihrer_firma.com*, damit Benutzer leichter ihre Hilferufe an das Supportteam absetzen können. Wenn diese Adresse in Microsoft Exchange Server als eine Verteilerliste konfiguriert ist, über die Einladungen an Mitglieder des Supportteams gelangen, oder als zusätzliche Mailbox für bestimmte Teammitglieder, kann das Supportpersonal Anfragen effizienter bearbeiten und die Benutzer verfügen über einen standardisierten Weg, Hilfe anzufordern.
- **Dateieinladung** Einladungen in Dateiform werden als Microsoft Remote Control Incident-Dateien (*.msrcincident*) gespeichert. Doppeltes Tippen oder Klicken auf den Dateinamen leitet die Remoteunterstützungssitzung ein. Sie können Dateieinladungen verwenden, wenn Sie E-Mails versenden und die Einladung separat hinzufügen müssen. Sie können auch einen freigegebenen Ordner einrichten, der Benutzern automatisch als Netzlaufwerk zur Verfügung gestellt wird und auch für das Supportpersonal zugänglich ist. Geben Sie der Freigabe einen Namen, der auf die Verwendung für Hilfeanforderungen hinweist, beispielsweise *Hilfeanforderungen* oder *Unterstützungseinladungen*.
- **Easy Connect-Einladung** Benutzt PNRP (Peer Name Resolution Protocol), um eine Einladung zur Remoteunterstützung über das Internet zu senden. Easy Connect generiert automatisch ein Zugriffskennwort, das es dem Helfer ermöglicht, direkt eine Verbindung zum Computer herzustellen. Die Kontaktinformationen des Helfers werden gespeichert, damit sie künftig ohne Kennworteingabe erneut verwendet werden können. (Diese Technik funktioniert nur, wenn sowohl der Helfer als auch der Benutzer, der Unterstützung benötigt, mit Windows 8 oder einer neueren Windows-Version arbeiten.)

Unter Windows 8 müssen Einladungen mit einem Kennwort erstellt werden. Das ist gegenüber früheren Windows-Versionen eine Änderung, die zur Erhöhung der Sicherheit beiträgt. Das Kennwort stellt in der Remoteunterstützungseinstellung einen zusätzlichen Sicherheitsfaktor dar, mit dem sich überprüfen lässt, ob die betreffenden Benutzer tatsächlich zur Remoteunterstützung autorisiert sind, weil sie das Kennwort kennen müssen. Sie sollten eine offizielle Richtlinie einführen, in der die Verwendung von Kennwörtern vorgeschrieben wird. Um den Vorgang zu beschleunigen, könnten Sie bestimmte Kennwörter definieren, die für Unterstützungseinladungen verwendet werden. Kennwörter sollten regelmäßig geändert werden. Außerdem sollten Sie erwägen, den verschiedenen Gruppen einer Organisation unterschiedliche Kennwörter zuzuweisen.

Damit die Remoteunterstützung funktioniert, muss eine Netzwerkverbindung zwischen dem Computer des Benutzers und dem Computer des Helfers vorhanden sein. Die Remoteunterstützung benutzt für die Kommunikation UPnP, SSDP, PNRP und Teredo. Weil die meisten Firewalls diese Kommunikation standardmäßig nicht erlauben, verhindert unter Umständen eine Firewall zwischen den beiden Computern die Unterstützungssitzung. Damit die Remoteunterstützung funktioniert, muss in diesem Fall eine Ausnahme für ausgehende Kommunikation vom Computer des Helfers zum Computer des Benutzers erstellt werden. Gehen Sie folgendermaßen vor, um die benötigte Windows-Firewallausnahme für Remoteunterstützung einzurichten:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit*. Tippen oder klicken Sie unter *Windows-Firewall* auf *Apps über die Windows-Firewall kommunizieren lassen*.
2. Blättern Sie im Fenster *Zugelassene Programme* nach unten, bis Sie *Remoteunterstützung* finden. Stellen Sie sicher, dass das Kontrollkästchen *Remoteunterstützung* aktiviert ist.
3. Es gibt Kontrollkästchen für die Netzwerktypen *Domäne*, *Privat* und *Öffentlich*. Wählen Sie aus, für welche Netzwerktypen die Remoteunterstützung erlaubt sein soll, und tippen oder klicken Sie auf *OK*.

Die Remoteunterstützung funktioniert auch über NAT-Firewalls (Network Address Translation). Wenn Sie mit Remoteunterstützungssitzungen Support leisten, finden Sie integrierte Diagnoseprogramme vor, die Sie durch Antippen oder Anklicken starten können. Ist eine intensivere Betreuung nötig, können zwei Supporttechniker gleichzeitig eine Verbindung mit einem Computer aufnehmen. Dank der automatischen Wiederverbindung nach dem Start des Computers können Sie auch in einer Remoteunterstützungssitzung einen Neustart des Computers vornehmen, den Sie betreuen, und brauchen die Verbindung nicht manuell wiederherzustellen. Sobald der Computer hochgefahren ist, wird die Remoteunterstützungssitzung automatisch wiederhergestellt.

Erstellen von Remoteunterstützungseinladungen

Um eine Remoteunterstützungseinladung für E-Mail zu erstellen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung unter *System und Sicherheit* auf *Probleme erkennen und beheben*. Tippen oder klicken Sie im linken Fensterabschnitt des Fensters *Problembehandlung* auf *Einen Freund fragen*.
2. Tippen oder klicken Sie im Remoteunterstützungs-Assistenten auf *Laden Sie eine Person ein, die Ihnen hilft* und dann auf *Einladung per E-Mail senden*.
3. Wenn Sie dazu aufgefordert werden, geben Sie ein sicheres Kennwort für die Verbindung mit Ihrem Computer ein und bestätigen es. Dieses Kennwort wird von der Person benutzt, die Sie einladen, und gilt nur für die Remoteunterstützungssitzung.
4. Wenn Sie auf *Weiter* klicken, startet Windows 8 Ihr Standardmailprogramm und erstellt eine E-Mail mit der Einladung. Geben Sie im Textfeld *An* die E-Mail-Adresse der Person ein, die Sie einladen, und tippen oder klicken Sie dann auf *Senden*.

Wenn Sie eine Remoteunterstützungseinladung erstellen und in einer Datei speichern möchten, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung unter *System und Sicherheit* auf *Probleme erkennen und beheben*. Tippen oder klicken Sie im linken Fensterabschnitt des Fensters *Problembehandlung* auf *Einen Freund fragen*.
2. Tippen oder klicken Sie im Remoteunterstützungs-Assistenten auf *Laden Sie eine Person ein, die Ihnen hilft* und dann auf *Einladung als Datei speichern*.
3. Geben Sie einen Pfad und einen Dateinamen für die Einladung ein. Wenn Sie einen Pfad angeben, der auf einen Netzwerkordner verweist, ist die Einladung für einen Administrator, der Zugriff auf diesen Ordner hat, leicht zugänglich.
4. Übergeben Sie Ihrem Helfer die Einladungsdatei und das automatisch generierte Kennwort. Dieses Kennwort wird von der Person benutzt, die Sie einladen, und gilt nur für die Remoteunterstützungssitzung.

Gehen Sie folgendermaßen vor, um eine Einladung zur Remoteunterstützung mit Easy Connect zu erstellen:

1. Tippen oder klicken Sie in der Systemsteuerung unter *System und Sicherheit* auf *Probleme erkennen und beheben*. Tippen oder klicken Sie im linken Fensterabschnitt des Fensters *Problembehandlung* auf *Einen Freund fragen*.
2. Tippen oder klicken Sie im Remoteunterstützungs-Assistenten auf *Laden Sie eine Person ein, die Ihnen hilft* und dann auf *Easy Connect verwenden*.

- Teilen Sie Ihrem Helfer das Easy Connect-Kennwort mit. Dieses Kennwort wird automatisch generiert und gilt nur für diese Remoteunterstützungssitzung.

Standardmäßig gelten Remoteunterstützungseinladungen maximal 6 Stunden und ermöglichen es dem Helfer, einen Computer fernzusteuern. Diese Einstellungen können Sie im Dialogfeld *Systemeigenschaften* ändern, wie in Kapitel 7 im Abschnitt »Konfigurieren der Remoteunterstützung« besprochen. Nachdem Sie die E-Mail mit der Einladung gesendet oder die Einladungsdatei erstellt haben, wird das Dialogfeld *Windows-Remoteunterstützung* angezeigt (Abbildung 10.3). Welche Optionen hier zur Verfügung stehen, hängt davon ab, ob die Verbindung bereits besteht oder nicht:

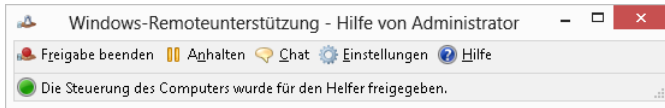


Abbildung 10.3 Verwalten von Remoteunterstützungssitzungen

- **Steuerung anfordern/Freigabe beenden** Fordert die Steuerung an oder beendet die Freigabe des Computers. Wenn Sie die Steuerung anfordern, erhält die Person, der Sie helfen, eine Meldung mit der Aufforderung zur Bestätigung.
- **An Bildschirm anpassen/Tatsächliche Größe** Passt die Größe der Darstellung des anderen Bildschirms an die Größe Ihres Fensters an.
- **Chat** Öffnet ein Chat-Fenster für die Übermittlung von Nachrichten zwischen dem Helfer und dem aktuellen Benutzer des Computers.
- **Einstellungen** Ermöglicht die Konfiguration der Sitzungseinstellungen. Standardmäßig wird ein Protokoll der Remoteunterstützungssitzung im Ordner `%UserProfile%\Documents\Remote Assistance Logs` des Computers gespeichert, der die Remoteunterstützung anfordert.

Der Helfer kann die Sitzung beenden, indem er das Fenster *Windows-Remoteunterstützung* schließt.

Wenn Sie als Helfer die Steuerung anfordern, erscheint bei der Person, der Sie helfen, eine Bestätigungsaufforderung, mit der sie bestätigen kann, ob sie dem Helfer die Kontrolle über den Desktop gewähren möchte. Die Person, der geholfen wird, muss auf *Ja* tippen oder klicken, um die Steuerung zu teilen. Zuvor ist es aber vielleicht erforderlich, dass sie ihnen erlaubt, die Benutzerkontensteuerung zu verwenden. Diese Berechtigung ist erforderlich, um auf dem Remotecomputer Administratöraufgaben durchzuführen.

Für die Person, der geholfen wird, hat das Dialogfeld *Windows-Remoteunterstützung* folgende Optionen:

- **Pause/Fortsetzen** Hält die Remoteunterstützungssitzung an. Der Helfer kann den Remotedesktop nicht mehr sehen. Die Person, der geholfen wird, muss dann auf *Fortsetzen* klicken, um die Remoteunterstützungssitzung wieder aufzunehmen.
- **Freigabe beenden** Beendet das Teilen des Computers und die Remoteunterstützungssitzung.
- **Einstellungen** Ermöglicht die Konfiguration der Sitzungseinstellungen. Welche Einstellungen verfügbar sind, hängt von dem Computer ab, der Hilfe erhält. Mit der ESC-Taste kann die gemeinsame Steuerung des Computers beendet werden, wenn die entsprechende Einstellung vorgenommen wurde. Es wird eine Protokolldatei der Remoteunterstützungssitzung gespeichert, und die Bandbreite wird so beschränkt, dass kein Ziehen von Fenstern möglich ist, kein Desktophintergrund übertragen wird und keine Schriftglättung erfolgt. Mit dem Schieberegler *Bandbreitenverwendung* können Sie die übertragene Datenmenge an die Übertragungsleistung der Verbindung anpassen.

HINWEIS

Standardmäßig wird ein Protokoll der Remoteunterstützungssitzung im Ordner `%UserProfile%\Documents\Remote Assistance Logs` des Computers gespeichert, der die Remoteunterstützung anfordert, ebenso auf dem Computer des Helfers.

- **Chat** Öffnet ein Chat-Fenster für die Übermittlung von Nachrichten zwischen dem Helfer und dem aktuellen Benutzer des Computers.

Anbieten von Remoteunterstützung oder Beantworten einer Remoteunterstützungseinladung

Wenn Sie wissen, dass ein Benutzer Probleme mit seinem Computer hat, können Sie mit folgenden Schritten Remoteunterstützung anbieten, statt auf die Einladung oder das Easy Connect-Kennwort des Benutzers zu warten:

1. Öffnen Sie die Windows-Remoteunterstützung, zum Beispiel indem Sie die WINDOWS-Taste drücken, `msra.exe` eingeben und die EINGABETASTE drücken.
2. Tippen oder klicken Sie im Assistenten *Windows-Remoteunterstützung* auf *Einem Benutzer, von dem Sie eingeladen wurden, Hilfe anbieten*.
3. Tippen oder klicken Sie auf den Link *Erweiterte Verbindungsoptionen für Helpdesk*.
4. Geben Sie den Namen oder die IP-Adresse des Computers ein, dem Sie helfen wollen, und tippen oder klicken Sie auf *Weiter*, um die Verbindung zu diesem Computer herzustellen.

Wenn jemand bereits eine Einladung erstellt hat, können Sie sie beantworten, indem Sie den betreffenden Anhang in der E-Mail oder die Einladungsdatei doppelt anklicken. Außerdem können Sie eine Einladung, die in einer Datei gespeichert wurde, folgendermaßen beantworten:

1. Öffnen Sie die Windows-Remoteunterstützung, zum Beispiel indem Sie die WINDOWS-Taste drücken, `msra.exe` eingeben und die EINGABETASTE drücken.
2. Tippen oder klicken Sie im Assistenten *Windows-Remoteunterstützung* auf *Einem Benutzer, von dem Sie eingeladen wurden, Hilfe anbieten*.
3. Tippen oder klicken Sie auf *Einladungsdatei verwenden* und wählen Sie dann im Dialogfeld *Öffnen* die Einladung aus. Tippen oder klicken Sie auf *Öffnen*.
4. Geben Sie das Kennwort für die Einladung ein, wenn Sie dazu aufgefordert werden.
5. Tippen oder klicken Sie auf *OK*. Sie werden nun mit dem Computer des Benutzers verbunden, der Hilfe benötigt, sofern dieser Benutzer die Einladung nicht widerrufen hat, die Einladung nicht abgelaufen ist und die Remoteunterstützung erlaubt ist.

Wenn jemand Easy Connect verwendet und Ihnen das Kennwort geschickt hat, beantworten Sie die Einladung so:

1. Öffnen Sie die Windows-Remoteunterstützung, zum Beispiel indem Sie die WINDOWS-Taste drücken, `msra.exe` eingeben und die EINGABETASTE drücken.
2. Tippen oder klicken Sie im Assistenten *Windows-Remoteunterstützung* auf *Einem Benutzer, von dem Sie eingeladen wurden, Hilfe anbieten*.
3. Tippen oder klicken Sie auf *Easy Connect verwenden*. Geben Sie das Kennwort für die Einladung ein, wenn Sie dazu aufgefordert werden.
4. Tippen oder klicken Sie auf *OK*. Sie werden nun mit dem Computer des Benutzers verbunden, der Hilfe benötigt.

Erkennen und Beheben von Windows 8-Fehlern

Auf einem Computer können Dutzende, in manchen Fällen Hunderte von verschiedenen Komponenten, Diensten und Anwendungen konfiguriert sein. Diese Komponenten alle am Laufen zu halten, kann durchaus schwierig werden. Die integrierten Diagnosefunktionen, die bisher in diesem Buch beschrieben wurden, sind bereits eine große Hilfe bei der Diagnose häufiger auftretender Probleme und deren Behebung. Wie in Kapitel 9, »Verwalten von Hardwaregeräten und Treibern«, beschrieben, werden bekannte Probleme in der Konsole *Problembenachrichtigungen und -lösungen* erfasst. Wie die integrierten Diagnosefunktionen versucht auch diese Konsole, Lösungen für Probleme zu finden, sofern dies möglich ist. Aber nicht alle Probleme lassen sich automatisch erkennen und lösen. Das ist der Punkt, an dem die Protokolle über Fehler, die von Windows-Komponenten, Anwendungen und Hardwaregeräte gemeldet werden, nützlich werden.

Verwenden der Ereignisprotokolle zur Fehlerüberprüfung und Fehlerdiagnose

Windows 8 speichert Fehlermeldungen von Prozessen, Diensten, Anwendungen und Hardwaregeräten in Protokolldateien. Es werden zwei Arten von Protokolldateien verwendet:

- **Windows-Protokolle** Diese Protokolldateien werden vom Betriebssystem zur Aufzeichnung von allgemeinen Ereignissen aus den Bereichen Anwendungen, Sicherheit, Installation und Systemkomponenten verwendet.
- **Anwendungs- und Dienstprotokolle** Diese Protokolldateien werden von bestimmten Anwendungen oder Diensten zur Aufzeichnung von anwendungs- oder dienstspezifischen Ereignissen verwendet.

Einträge in einer Protokolldatei werden mit einer Warnstufe erfasst, mit der sich verschiedene Ereignistypen unterscheiden lassen, zum Beispiel Fehlermeldungen und Meldungen, die nur zur Information dienen. Sie werden folgende Arten von Einträgen vorfinden:

- **Informationen** Ein Informationsereignis, das im Allgemeinen auf eine erfolgreich durchgeführte Aktion hinweist
- **Überwachung erfolgreich** Ein Ereigniseintrag, der die erfolgreiche Ausführung einer Aktion beschreibt
- **Überwachungsfehler** Ein Ereigniseintrag, der die gescheiterte Ausführung einer Aktion beschreibt
- **Warnung** Eine Warnung, deren Informationen dazu dienen können, zukünftige Probleme zu vermeiden
- **Fehler** Eine Fehlermeldung, beispielsweise über einen fehlgeschlagenen Versuch, einen Dienst zu starten

Neben Warnstufe, Datum und Uhrzeit bieten die Übersicht- und Detaildarstellungen der Ereigniseinträge folgende Informationen:

- **Quelle** Die Anwendung, der Dienst oder die Komponente, die das Ereignis protokolliert hat
- **Ereignis-ID** Eine Kennung für das betreffende Ereignis
- **Aufgabenkategorie** Eine Ereigniskategorie, die manchmal verwendet wird, um die dazugehörige Aktion zu beschreiben

- **Benutzer** Das Benutzerkonto, dessen Anmeldeinformationen verwendet wurden. Wenn ein Systemprozess oder ein Dienst das Ereignis ausgelöst hat, ist der Benutzername gewöhnlich eine der Spezialidentitäten, beispielsweise *NETZWERKDIENTST*, *LOKALER DIENST* oder *SYSTEM*.
- **Computer** Der Name des Computers, auf dem das Ereignis eingetreten ist
- **Details** In der Detaildarstellung steht hier eine Beschreibung des Ereignisses, gefolgt von dazugehörigen Daten oder Fehleranzeigen.

Anzeigen und Verwalten der Ereignisprotokolle

In der Computerverwaltung können Sie unter dem Knoten *Ereignisanzeige* auf Ereignisprotokolle zugreifen. Um die Computerverwaltung zu öffnen, tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit*, *Verwaltung* und dann auf *Computerverwaltung*. Sie können die Computerverwaltung auch öffnen, indem Sie die WINDOWS-Taste drücken, **compmgmt.msc** eingeben und die EINGABETASTE drücken. Auf die Ereignisprotokolle können Sie folgendermaßen zugreifen:

1. Öffnen Sie die Computerverwaltung. Standardmäßig sind Sie mit dem lokalen Computer verbunden. Wenn Sie die Protokolle eines Remotecomputers einsehen möchten, klicken Sie in der Konsolenstruktur (im linken Anzeigebereich) mit der rechten Maustaste auf den Eintrag *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* geben Sie dann den Namen des Computers ein, auf den Sie zugreifen möchten, und tippen oder klicken auf *OK*.
2. Erweitern Sie den Knoten *Ereignisanzeige* und dann den Knoten *Windows-Protokolle* oder *Anwendungs- und Dienstprotokolle* oder beide, um die verfügbaren Protokolle anzuzeigen.
3. Wählen Sie ein Protokoll aus, das Sie näher untersuchen möchten (Abbildung 10.4).

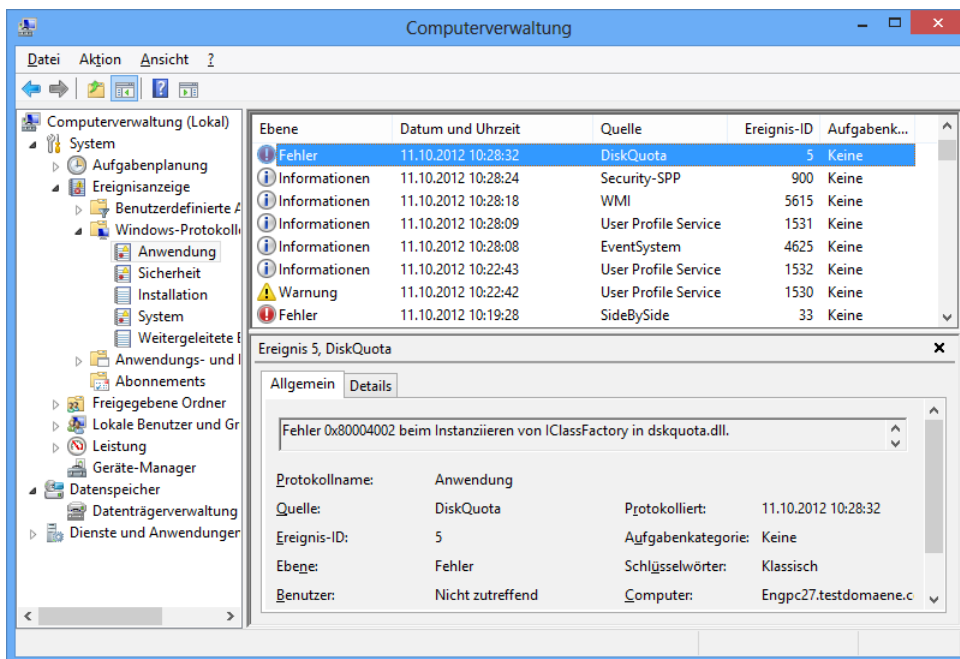


Abbildung 10.4 Die *Ereignisanzeige* zeigt die Ereignisse an, die im gewählten Protokoll aufgezeichnet wurden

WEITERE INFORMATIONEN

Mit der Tastenkombination WINDOWS-Taste+X lässt sich ein Kontextmenü öffnen, in dem häufig verwendete Tools verfügbar sind, darunter die Computerverwaltung und die Ereignisanzeige. Wenn Sie die Ereignisanzeige geöffnet haben, können Sie eine Verbindung mit einem anderen Computer herstellen, indem Sie den Eintrag *Ereignisanzeige* in der Konsolenstruktur auf der linken Seite des Fensters mit der rechten Maustaste anklicken oder ihn gedrückt halten und dann auf *Verbindung mit anderem Computer herstellen* tippen oder klicken.

Warnungen und Fehlermeldungen sind die beiden wichtigsten Ereignisarten, die Sie sich näher ansehen sollten. Wenn solche Ereignisse protokolliert werden und Sie die Ursache nicht kennen, tippen oder klicken Sie den betreffenden Eintrag doppelt an. Dann öffnet sich das Dialogfeld *Ereigniseigenschaften* mit einer genaueren Beschreibung des Ereignisses. Achten Sie auf die Fehlerursache und versuchen Sie, das Problem mit den Methoden zu beheben, die in diesem Buch beschrieben werden. Um mehr über die Fehlerursache und die Methoden zur Fehlerbehebung zu erfahren, können Sie bei Bedarf auf den Link *Onlinehilfe* tippen oder klicken, der in der Fehlerbeschreibung angegeben ist, oder die Microsoft Knowledge Base nach der Ereignis-ID oder nach Stichwörtern aus der Fehlerbeschreibung durchsuchen.

Planen von Wartungsarbeiten

Wenn Sie Desktop- oder Laptopsysteme verwalten, haben Sie viel mit Routinearbeiten zu tun, die in mehr oder weniger regelmäßigen Abständen anfallen. Dann können Sie den Aufgabenplanungsdienst verwenden, um einmal oder regelmäßig anfallende Arbeiten automatisch auszuführen. Zur Automatisierung von Arbeiten verwenden Sie Befehlsskripts, WSH-Skripts (Windows Script Host) oder Anwendungen, die die gewünschten Arbeiten durchführen. Im Gegensatz zu früheren Windows-Versionen gibt es in Windows 8 bereits eine umfangreiche Bibliothek mit vordefinierten Aufgaben. Damit lassen sich sehr viele Arbeiten automatisieren, angefangen bei der Deinstallation eines Bluetooth-Geräts über das Defragmentieren von Laufwerken bis hin zum Überprüfen des Systems mit Windows-Defender.

Funktionsweise der Aufgabenplanung

Windows 8 bietet mehrere Programme für die automatische Ausführung von Aufgaben, wie zum Beispiel die Aufgabenplanung, das Befehlszeilenprogramm Sctasks (*sctasks.exe*) und einige Windows PowerShell-Cmdlets. Sie können jedes dieser Tools zur Planung von Aufgaben auf dem lokalen Computer und auf Remotecomputern verwenden. Die Aufgabenplanung umfasst mehrere Assistenten, mit denen Sie Aufgaben planen. In diesen Assistenten richten Sie die Aufgaben in einer grafischen Benutzeroberfläche mit der Maus ein. Sctasks ist dagegen ein Befehlszeilenprogramm. Zu den neuen Windows PowerShell-Cmdlets gehören *New-ScheduledTask*, *New-ScheduledTaskAction*, *Set-ScheduledTask*, *Start-ScheduledTask* und *Stop-ScheduledTask*.

Alle diese Planungstools verwenden den Aufgabenplanungsdienst, um die Systemuhr abzulesen und dann zur vorgesehenen Zeit mit der Ausführung der geplanten Aufgabe zu beginnen. Der Aufgabenplanungsdienst meldet sich standardmäßig mit dem Konto *LOKALES SYSTEM* an. Dieses Konto verfügt gewöhnlich nicht über die Berechtigungen, die für Verwaltungsarbeiten erforderlich sind. Zur Lösung dieses Problems lässt sich jede Aufgabe so einrichten, dass sie mit dem Konto eines bestimmten Benutzers durchgeführt wird. Bei der Definition der Aufgabe legen Sie den Benutzernamen und das Kennwort fest. Achten Sie darauf, ein Konto zu verwenden, das über die erforderlichen Berechtigungen und Zugriffsrechte verfügt, um die vorgesehene Arbeit durchführen zu können.

HINWEIS Der Schwerpunkt dieses Abschnitts liegt auf der Aufgabenplanung, in Windows 8-Computern das wichtigste Programm zum Ausführen geplanter Aufgaben. Wenn Sie mehr über Schtasks erfahren möchten, geben Sie in einer Befehlszeile **schtasks /?** ein oder lesen Kapitel 8, »Scheduling Tasks to Run Automatically«, in dem Buch *Windows Command-Line Administrator's Pocket Consultant, Second Edition* (Microsoft Press, 2008).

In Windows 8 gibt es zwei verschiedene Arten von geplanten Aufgaben:

- **Standardaufgaben** Sie dienen zur Automatisierung von Routinearbeiten und zur Systempflege. Diese Aufgaben sind für Benutzer sichtbar und können bei Bedarf geändert werden.
- **Ausgeblendete Aufgaben** Sie dienen zur Automatisierung spezieller Systemaufgaben. Diese Aufgaben sind für den Benutzer normalerweise nicht zu sehen und sollten normalerweise auch nicht geändert werden. Manche ausgeblendeten Aufgaben werden durch ein dazugehöriges Programm erstellt und verwaltet, beispielsweise von Windows-Defender.

Unter Windows 8 ist die Erstellung und Verwaltung von Aufgaben wesentlich weiter entwickelt als zuvor. Jede Aufgabe lässt sich so konfigurieren, dass sie:

- Nur ausgeführt wird, wenn ein Benutzer angemeldet ist, oder dass sie unabhängig davon ausgeführt wird, ob ein Benutzer angemeldet ist oder nicht.
- Mit Standardbenutzerrechten ausgeführt wird oder mit den höchsten erforderlichen Rechten (einschließlich Administratorberechtigungen).

Da Aufgaben, die unter Windows 8 definiert werden, nicht zu anderen Windows-Versionen kompatibel sind, können Sie eine Windows 8-Aufgabe nicht einfach auf eine ältere Windows-Version kopieren und erwarten, dass sie funktioniert. Allerdings können Sie bei der Definition einer Aufgabe angeben, ob die Definition so erfolgen soll, dass sie zu früheren Windows-Versionen kompatibel ist. Dann könnten Sie die Aufgabe auf anderen Computern benutzen, auf denen frühere Windows-Versionen ausgeführt werden.

Aufgaben verfügen über viele Eigenschaften, wie zum Beispiel:

- **Trigger** Trigger legen die Umstände fest, unter denen die Ausführung einer Aufgabe beginnt und endet. Sie können eine Aufgabe beginnen nach Zeitplan, durch die Anmeldung eines Benutzers, durch den Start des Computers oder dadurch, dass sich der Prozessor im Leerlauf befindet. Die Ausführung einer Aufgabe kann auch ausgelöst werden durch Ereignisse, durch die Verbindung eines Benutzers mit einer Terminalserversitzung oder durch die Trennung dieser Verbindung, oder dadurch, dass ein Benutzer eine Arbeitsstation sperrt oder die Sperrung aufhebt. Aufgaben mit Ereignissen als Auslöser können sehr wichtig sein, weil sie die Möglichkeit bieten, automatisch auf Fehler und Warnungen zu reagieren.
- **Aktionen** Aktionen legen fest, was geschehen soll, wenn die Ausführung der Aufgabe ausgelöst wird. Es können Programme oder Skripts gestartet, E-Mails versendet oder Meldungen angezeigt werden.
- **Bedingungen** Damit können Sie die Bedingungen festlegen, unter denen die Ausführung einer Aufgabe begonnen oder eine begonnene Ausführung beendet wird. Sie können Bedingungen verwenden, um den Computer zur Ausführung einer Aufgabe zu aktivieren oder die Aufgabe nur auszuführen, wenn eine bestimmte Netzwerkverbindung verfügbar ist. Sie können Bedingungen verwenden, um eine Aufgabe auszuführen, zu beenden oder erneut zu starten, wenn sich der Prozessor im Leerlauf befindet. Vielleicht möchten Sie, dass mit der Ausführung einer Aufgabe nur begonnen wird, wenn sich der Prozessor seit mindestens 10 Minuten im Leerlauf befindet, dass sie beendet wird, wenn sich der Prozessor nicht mehr im Leerlauf befindet, und dass sie erneut begonnen wird,

wenn sich der Prozessor wieder im Leerlauf befindet. Sie können durch Bedingungen auch festlegen, dass eine Aufgabe nur dann ausgeführt wird, wenn der Computer an der Steckdose betrieben wird, und dass die Ausführung beendet wird, sobald der Computer auf Akkubetrieb wechselt.

Anzeigen und Verwalten von Aufgaben auf lokalen und Remotesystemen

Die aktuellen Aufgaben, die auf einem Computer konfiguriert sind, sind in der Computerverwaltung unter dem Knoten *Aufgabenplanung* zugänglich. Aufgaben werden mit der bekannten Ordnerstruktur verwaltet und gruppiert. Die entsprechenden Basisordner haben Namen, die den Betriebssystemfunktionen, Tools und Konfigurationsbereichen entsprechen, für die die Aufgaben erstellt wurden. In einem Basisordner finden Sie gewöhnlich eine oder mehrere Aufgaben.

Sie können die für einen Computer geplanten Aufgaben mit folgenden Schritten einsehen und verwalten:

1. Öffnen Sie die Computerverwaltung. Standardmäßig sind Sie mit dem lokalen Computer verbunden. Wenn Sie die Aufgabenplanung eines Remotecomputers einsehen möchten, klicken Sie in der Konsolenstruktur (im linken Anzeigebereich) mit der rechten Maustaste auf den Eintrag *Computerverwaltung* oder halten ihn gedrückt, und wählen *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* geben Sie dann den Namen des Computers ein, auf den Sie zugreifen möchten, und tippen oder klicken auf *OK*.
2. Erweitern Sie den Knoten *Aufgabenplanung*, dann den Knoten *Aufgabenplanungsbibliothek* und nach Bedarf die entsprechenden untergeordneten Knoten.
3. Wenn Sie in der Konsolenstruktur einen Aufgabenordner auswählen, wird die erste Aufgabe im Ordner standardmäßig ausgewählt. Wenn in dem Ordner mehrere Aufgaben liegen und Sie mit einer anderen Aufgabe arbeiten möchten, wählen Sie die betreffende Aufgabe aus.
4. Wenn Sie die Aufgabe ausgewählt haben, mit der Sie arbeiten möchten, können Sie sich deren Eigenschaften auf den verschiedenen Registerkarten ansehen (Abbildung 10.5). Wenn Sie die Aufgabe bearbeiten möchten, klicken Sie im Hauptbereich des Fensters mit der rechten Maustaste auf die Aufgabe oder halten Sie sie gedrückt:
 - Löschen Sie eine Aufgabe, indem Sie *Löschen* wählen.
 - Deaktivieren Sie die Aufgabe, indem Sie auf *Deaktivieren* tippen oder klicken.
 - Bearbeiten Sie die Eigenschaften der Aufgabe, indem Sie auf *Eigenschaften* tippen oder klicken, im Eigenschaftendialogfeld die gewünschten Änderungen vornehmen und dann auf *OK* klicken.
 - Exportieren Sie eine Aufgabe in eine Datei, die auf einem anderen Computer importiert werden kann, indem Sie *Exportieren* wählen. Nachdem Sie die Aufgabe exportiert haben, stellen Sie in der Computerverwaltung eine Verbindung mit einem anderen Computer her, klicken mit der rechten Maustaste auf den Knoten *Aufgabenplanungsbibliothek* oder halten ihn gedrückt, und wählen dann *Aufgabe importieren*. Dann können Sie im Dialogfeld *Öffnen* die Aufgabendatei auf dem anderen Computer herausuchen und öffnen.
 - Leiten Sie die Ausführung einer Aufgabe ein, indem Sie auf *Ausführen* tippen oder klicken.
 - Sofern die Aufgabe ausgeführt wird, können Sie sie durch Antippen oder Anklicken von *Beenden* abbrechen.

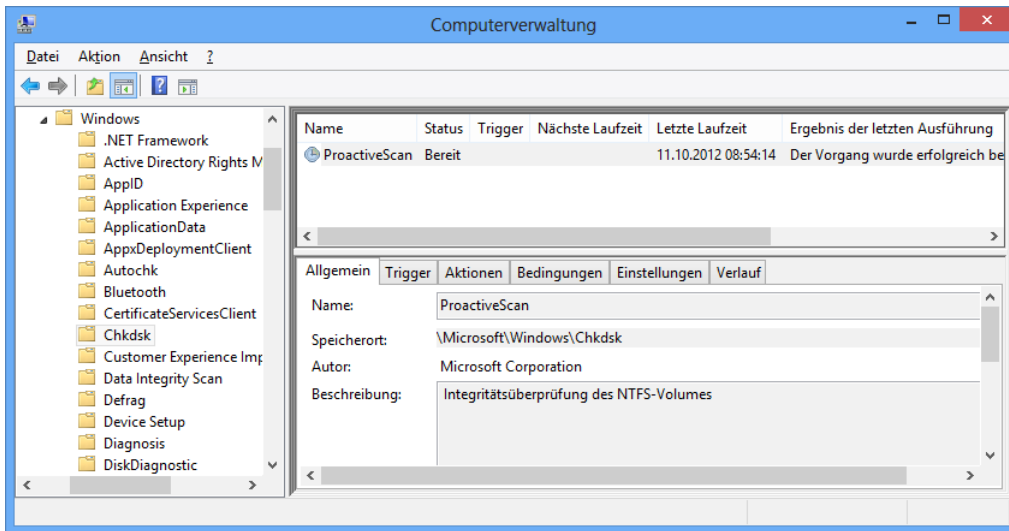


Abbildung 10.5 Anzeigen und Verwalten geplanter Aufgaben

HINWEIS

Sie können zwar benutzerdefinierte Aufgaben ändern oder löschen, aber die meisten Aufgaben, die vom Betriebssystem erstellt werden, lassen sich weder konfigurieren noch löschen. Werden Betriebssystemaufgaben nicht angezeigt, können Sie diese Aufgaben sichtbar machen, indem Sie im Menü *Ansicht* den Befehl *Ausgeblendete Aufgaben einblenden* wählen. Wenn Sie Aufgaben exportieren, legt die Einstellung *Konfigurieren für* fest, in welchen Betriebssystemen die Aufgabe benutzt werden kann.

Welche geplanten Aufgaben auf einem Computer ausgeführt werden, können Sie folgendermaßen überprüfen:

1. Öffnen Sie die Computerverwaltung. Standardmäßig sind Sie mit dem lokalen Computer verbunden. Wenn Sie die Aufgabenplanung eines Remotecomputers einsehen möchten, klicken Sie in der Konsolenstruktur (im linken Anzeigebereich) mit der rechten Maustaste auf den Eintrag *Computerverwaltung* oder halten ihn gedrückt, und wählen *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* geben Sie dann den Namen des Computers ein, auf den Sie zugreifen möchten, und tippen oder klicken auf *OK*.
2. Wählen Sie den Knoten *Aufgabenplanung* aus. Klicken Sie mit der rechten Maustaste auf den Knoten *Aufgabenplanung* oder halten Sie ihn gedrückt, und wählen Sie dann *Alle aktiven Aufgaben anzeigen*.

Erstellen von geplanten Aufgaben

Gehen Sie folgendermaßen vor, um eine geplante Aufgabe zu erstellen:

1. Öffnen Sie die Computerverwaltung. Standardmäßig sind Sie mit dem lokalen Computer verbunden. Wenn Sie die Aufgabenplanung eines Remotecomputers einsehen möchten, klicken Sie in der Konsolenstruktur (im linken Anzeigebereich) mit der rechten Maustaste auf den Eintrag *Computerverwaltung* oder halten ihn gedrückt, und wählen *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* geben Sie dann den Namen des Computers ein, auf den Sie zugreifen möchten, und tippen oder klicken auf *OK*.

2. Wählen Sie den Knoten *Aufgabenplanung*, klicken Sie diesen Knoten mit der rechten Maustaste an oder halten Sie ihn gedrückt, und wählen Sie *Aufgabe erstellen*. Dadurch wird das Dialogfeld *Aufgabe erstellen* geöffnet.
3. Geben Sie den Namen der Aufgabe auf der Registerkarte *Allgemein* ein und legen Sie dann die Sicherheitsoptionen für die Ausführung der Aufgabe fest.
 - Wenn die Aufgabe mit dem Konto eines anderen Benutzers ausgeführt werden soll, also nicht mit dem Konto des aktuellen Benutzers, tippen oder klicken Sie auf *Benutzer oder Gruppe ändern*. Wählen Sie im Dialogfeld *Benutzer oder Gruppe auswählen* den Benutzer oder die Gruppe aus, deren Konto für die Durchführung der Aufgabe verwendet werden soll, und geben Sie später die entsprechenden Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden.
 - Nehmen Sie mit den verfügbaren Optionen die erforderlichen Einstellungen vor. Standardmäßig werden Aufgaben nur automatisch ausgeführt, wenn ein Benutzer angemeldet ist. Soll die Aufgabe unabhängig davon ausgeführt werden, ob ein Benutzer angemeldet ist oder nicht, wählen Sie *Unabhängig von der Benutzeranmeldung ausführen*. Sie können auch festlegen, dass die Aufgabe mit den höchsten Berechtigungen ausgeführt wird, und die Aufgabe für ältere Windows-Versionen konfigurieren. Um die Aufgabe für Windows 7 und Windows 8 zu konfigurieren, wählen Sie *Windows 7, Windows Server 2008 R2*.
4. Erstellen Sie auf der Registerkarte *Trigger* die gewünschten Auslöser. Um einen Trigger zu erstellen, tippen oder klicken Sie auf *Neu*, konfigurieren den Trigger mit den verfügbaren Optionen und tippen oder klicken dann auf *OK*.
5. Definieren Sie auf der Registerkarte *Aktionen* die Aktionen, die durchgeführt werden sollen. Um eine Aktion zu definieren, tippen oder klicken Sie auf *Neu*, konfigurieren die Aktion mit den verfügbaren Optionen und tippen oder klicken dann auf *OK*.
6. Geben Sie auf der Registerkarte *Bedingungen* die Bedingungen an, die für Start oder Beendigung der Aufgabe gelten.
7. Nehmen Sie auf der Seite *Einstellungen* weitere Einstellungen vor, soweit sie für die Aufgabe erforderlich sind.
8. Tippen oder klicken Sie auf *OK*, um die Aufgabe zu erstellen.

Problembehandlung für geplante Aufgaben

Wenn Sie Aufgaben definieren, die auf einem Computer automatisch ausgeführt werden sollen, können sich verschiedene Probleme ergeben. Manche Aufgaben werden nicht zum vorgesehenen Zeitpunkt ausgeführt. Andere Aufgaben werden gestartet und hören gar nicht mehr auf. Um den Status einer Aufgabe zu überprüfen, wählen Sie die Aufgabe in der Aufgabenplanung aus und überprüfen die Angaben unter *Status*, *Letzte Laufzeit* und *Ergebnis der letzten Ausführung*. Lautet der Status der Aufgabe *In Warteschlange*, dann wartet sie darauf, nach Zeitplan ausgeführt zu werden. Hat sie den Status *Bereit*, dann ist sie bereit zur nächsten Ausführung. Soll eine Aufgabe automatisch ausgeführt werden, aber unter *Letzte Laufzeit* wird *Nie* angegeben, sollten Sie die Eigenschaften der Aufgabe überprüfen, um herauszufinden, warum sie nicht ausgeführt wird. Steht unter *Letzte Laufzeit* eine Fehlermeldung, müssen Sie das angegebene Problem beheben, damit die Aufgabe normal ausgeführt werden kann.

Überprüfen Sie die Eigenschaften einer Aufgabe, indem Sie ihren Eintrag in der Aufgabenplanung antippen oder anklicken. Die Registerkarte *Verlauf* bietet ausführliche Informationen über die Aufgabe, von der Erstellung bis hin zur letzten Ausführung. Verwenden Sie diese Angaben zur Behebung des Problems.

Eine Aufgabe, die als *Wird ausgeführt* gelistet wird, hängt vielleicht. Ob es sich um einen Prozess handelt, der hängt, können Sie mit der *Letzten Laufzeit* überprüfen, die angibt, wann mit der Ausführung der Aufgabe begonnen wurde. Läuft die Ausführung bereits länger als einen Tag, ist das normalerweise ein Hinweis auf ein Problem. Vielleicht wartet ein Skript auf eine Eingabe, vielleicht gibt es Probleme mit Schreib- oder Lesezugriffen auf Dateien, oder es ist einfach ein Fehler aufgetreten und die Ausführung der Aufgabe muss beendet werden. Um die Ausführung zu beenden, klicken Sie den Eintrag in der Aufgabenplanung mit der rechten Maustaste an oder halten ihn gedrückt, und wählen *Beenden*.

Sichern und Wiederherstellen eines Computers

Windows 8 sieht die Konsole *Sichern und Wiederherstellen* als zentrale Konsole zum Sichern und Wiederherstellen eines Computers vor. Sie können diese Konsole in der *Systemsteuerung* öffnen, indem Sie unter der Überschrift *System und Sicherheit* auf *Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern* klicken. Ältere Versionen von Dateien und Ordnern finden Sie vielleicht auf den freigegebenen Ordnern im Netzwerk. Andere Hilfsmittel zum Sichern und Wiederherstellen der Daten eines Computers sind die Tools Systemstartreparatur, Windows-Ladeprogrammfortsetzung und die Systemwiederherstellung. Diese Tools werden in den folgenden Abschnitten beschrieben.

Sichern und Wiederherstellen von Dateien und Ordnern mit Vorgängerversionen

Auf Dateiservern, die unter Windows Server 2012 betrieben werden, sind Vorgängerversionen verfügbar. Vorgängerversionen kommen aus Schattenkopien und werden für Ordner erstellt, die auf Dateiservern liegen und im Netzwerk freigegeben sind. Vorgängerversionen sind zwar kein Ersatz für eine vollständige Sicherung des Systems, aber sie eignen sich zur automatischen Erstellung von Sicherungskopien von Dateien und Ordnern, die sich auf den überwachten Laufwerken ändern. Wird eine überwachte Datei oder ein überwachter Ordner versehentlich gelöscht oder geändert, können Sie die Vorgängerversion der Datei oder des Ordners wiederherstellen.

Wenn Sie im Datei-Explorer mit der rechten Maustaste auf eine Datei oder einen Ordner klicken, der auf einem Dateiserver freigegeben wurde, oder das entsprechenden Symbol gedrückt halten, und *Eigenschaften* wählen, sehen Sie die Registerkarte *Vorgängerversionen*. Wenn Sie diese Registerkarte wählen, werden verfügbare Vorgängerversionen der Datei oder des Ordners aufgelistet, sofern vorhanden. Nachdem Sie eine Vorgängerversion ausgewählt haben, können Sie:

- die Schaltfläche *Öffnen* antippen oder anklicken, um eine Vorgängerversion zu öffnen.
- die Schaltfläche *Kopieren* antippen oder anklicken, um eine Vorgängerversion zu kopieren
- die Schaltfläche *Wiederherstellen* verwenden, um die Datei oder den Ordner auf die gewünschte Version zurückzuführen.

Wenn Sie auf Ihrem Computer keine Vorgängerversionen sehen, kann es dafür verschiedene Gründe geben:

- Vielleicht handelt es sich bei der Datei um eine Offlinedatei. Offlinedateien sind Kopien von Netzwerkdateien. Clientcomputer erstellen keine Vorgängerversionen von Offlinedateien. Allerdings können auf dem Server, auf dem die Datei gespeichert ist, Vorgängerversionen verfügbar sein.
- Vielleicht handelt es sich um eine Systemdatei. Von Systemdateien werden keine Vorgängerversionen erstellt.

- Vielleicht wurde der Ordner gelöscht, in dem die Datei gespeichert war. In diesem Fall müssen Sie das Eigenschaftendialogfeld des Ordners öffnen, der den gelöschten Ordner enthielt. Verwenden Sie die Registerkarte *Vorgängerversionen* dieses Ordners, um den gelöschten Ordner wiederherzustellen, und verwenden Sie den wiederhergestellten Ordner, um die gewünschte Vorgängerversion der Datei wiederherzustellen.
- Es wurde vielleicht noch keine Schattenkopie erstellt, seit die Datei erstellt und gespeichert wurde.

Wiederherstellen nach einem fehlgeschlagenen Start

Wenn ein Windows 8-Computer startet und nicht aus einem Energiesparmodus oder dem Ruhezustand reaktiviert wird, initialisiert der Windows-Start-Manager das Betriebssystem, indem er das Windows-Startladeprogramm startet, das wiederum anhand der Informationen aus dem BCD-Speicher das Betriebssystem startet. Schlägt der Start von Windows 8 fehl, sehen Sie beim nächsten Neustart des Computers einen Wiederherstellungsbildschirm. Auf diesem Bildschirm können Sie *PC neu starten* wählen, um den Computer herunterzufahren und neu zu starten, oder *Erweiterte Reparaturoptionen anzeigen*, um zusätzliche Optionen zur Reparatur des Computers anzuzeigen.

Zu den erweiterten Reparaturoptionen gehören:

- **Fortsetzen** Das Reparaturmenü wird verlassen und das Betriebssystem wird geladen.
- **Anderes Betriebssystem** Das Reparaturmenü wird verlassen und Sie erhalten die Gelegenheit, das zu ladende Betriebssystem auszuwählen.
- **PC ausschalten** Das Reparaturmenü wird verlassen und der Computer wird heruntergefahren.
- **Problembehandlung** Zeigt das Problembehandlungsmenü.

Das Problembehandlungsmenü hat drei Optionen:

- **PC auffrischen** PC auffrischen ist eine neue Funktion von Windows 8, die Windows 8 aus dem Betriebssystemabbild, das auf dem Computer gespeichert ist, erneut installiert und dabei persönliche Dateien, Konten und persönliche Einstellungen beibehält. Desktop-Apps und die dazugehörigen Einstellungen sind nach dem Auffrischen zwar verfügbar, aber andere Programme, die zuvor installiert wurden, sind nicht mehr verfügbar.
- **Originaleinstellung wiederherstellen** Die Wiederherstellung der Originaleinstellungen ist eine neue Funktion von Windows 8, die Windows 8 aus dem Betriebssystemabbild, das auf dem Computer gespeichert ist, erneut installiert und die Installation auf ihren "fabrikneuen" Zustand zurücksetzt. Nach der Wiederherstellung sind keine persönlichen Dateien, Konten oder Einstellungen verfügbar und Sie müssen Desktop-Apps und Desktop-Programme neu installieren.
- **Erweiterte Optionen** Zeigt das Menü *Erweiterte Optionen* an.

Das Menü *Erweiterte Optionen* hat fünf Optionen:

- **System wiederherstellen** Ermöglicht die Verwendung von auf dem Computer gespeicherten Wiederherstellungspunkten, um Windows wiederherzustellen, wie unten in diesem Kapitel im Abschnitt »Sichern und Wiederherstellen des Systemzustands mit der Systemwiederherstellung« beschrieben.
- **Systemimage-Wiederherstellung** Ermöglicht Ihnen die Wiederherstellung des Computers aus einer Systemabbilddatei. Der Vorgang ähnelt dem Rücksetzen des Computers in einen vorigen Zustand, nur wählen Sie dabei die Abbilddatei aus, die zur Wiederherstellung verwendet werden soll, und diese Datei kann von einem Remotecomputer stammen. Nach der Wiederherstellung sind keine persönlichen Dateien, Konten und Einstellungen verfügbar und Sie müssen Desktop-Apps und Desktop-Programme erneut installieren (abgesehen von denen, die bereits zum Systemabbild gehören).

- **Automatische Reparatur** Ermöglicht den Start des Tools *Automatische Reparatur*, das Startprobleme beheben kann, beispielsweise fehlerhafte Einträge im Startkonfigurationsdatenspeicher (Boot Configuration Data, BCD), beschädigte Systemdateien und beschädigte Start-Manager. Normalerweise wird dieses Tool automatisch gestartet, wenn Windows ein behebbares Problem erkennt.
- **Eingabeaufforderung** Ermöglicht den Zugang zu einer Eingabeaufforderung und die Arbeit mit den Befehlen und Tools, die in der Wiederherstellungsumgebung verfügbar sind.
- **Starteinstellungen** Ermöglicht die Änderung des Startverhaltens von Windows 8. Dies ermöglicht Ihnen den Neustart des Computers, damit Sie das Erzwingen der Treibersignatur, früh startende Schadsoftwareschutzprogramme und den automatischen Neustart bei einem Systemversagen deaktivieren können. Außerdem können Sie einen Grafikmodus mit niedriger Auflösung, den Debug-Modus, die Startprotokollierung und den abgesicherten Modus aktivieren.

Wiederherstellen nach einer fehlgeschlagenen Reaktivierung

Wenn ein Computer, auf dem Windows 8 ausgeführt wird, in einen Energiesparmodus oder in den Ruhezustand übergeht, wird ein Abbild des aktuellen Zustands des Computers erstellt. Bei einem Energiesparmodus bleibt dieses Abbild im Speicher und wird verwendet, wenn der Benutzer den Computer reaktiviert. Für den Ruhezustand wird dieses Abbild auf einen Datenträger geschrieben und dann vom Datenträger wieder eingelesen, wenn der Benutzer den Computer reaktiviert. Für beide Vorgänge ist die Windows-Ladeprogrammfortsetzung (Windows Resume Loader) zuständig.

Probleme mit der Reaktivierung können sich aus verschiedenen Gründen ergeben. Das Abbild kann fehlerhaft sein, der Arbeitsspeicher kann Fehler aufweisen und der Datenträger natürlich auch. Ergeben sich bei der Reaktivierung des Systems aus einem Energiesparmodus Probleme, geht die Windows-Ladeprogrammfortsetzung zu einem herkömmlichen Systemstart über und das Betriebssystem wird ohne die Energiesparmodusdaten geladen. Ergeben sich bei der Reaktivierung des Systems nach dem Ruhezustand Probleme, geht die Windows-Ladeprogrammfortsetzung wieder zu einem herkömmlichen Systemstart über und das Betriebssystem wird ohne die Ruhezustandsdaten geladen.

In beiden Fällen bedeutet dies den Verlust von Daten, die nicht gespeichert wurden, bevor der Computer in den Energiesparmodus oder Ruhezustand wechselte. Allerdings sind die meisten aktuellen Anwendungen so eingerichtet, dass sie ihren Zustand automatisch speichern, wenn der Computer in einen Energiesparmodus wechselt. Daher kann es durchaus sein, dass Wiederherstellungsdaten vorliegen, wenn Sie eine der betreffenden Anwendungen neu starten.

Nach einer fehlgeschlagenen Reaktivierung kann die Automatische Reparatur die zuletzt durchgeführten Konfigurationsänderungen am Energiesparmodus und Ruhezustand untersuchen und gegebenenfalls rückgängig machen. Wenn Sie den aktuellen Energiesparplan zum Beispiel so geändert haben, dass der Computer automatisch in den Ruhezustand wechselt, wenn er sich eine bestimmte Zeit in einem Energiesparmodus befunden hat, kann die Automatische Reparatur diese Änderung rückgängig machen.

Reparieren eines Computers, um den Systemstart zu ermöglichen

Um das Betriebssystem ordnungsgemäß starten zu können, müssen Windows 8-Computer auf bestimmte Systemdateien zugreifen können. Lässt sich ein Computer nicht starten, weil eine bestimmte Systemdatei beschädigt ist oder fehlt, können Sie die Datei mit dem Tool Automatische Reparatur wiederherstellen. Manchmal reicht die Reparatur einer beschädigten oder fehlenden Datei aber nicht aus, um die Probleme des Computers zu beseitigen. Dann müssen Sie die Fehlersuche fortsetzen und versuchen, das eigentliche Problem zu erkennen.

Die meisten Startprobleme treten auf, weil etwas im System geändert wurde, beispielsweise wurde vielleicht ein Gerät falsch installiert. Die Systemkonfiguration oder die Registrierung wurde vielleicht falsch aktualisiert, sodass sich Konflikte ergeben. Oft lassen sich Startprobleme beheben, indem man das System im abgesicherten Modus startet und die Änderungen genauer untersucht, die zuletzt vorgenommen wurden. Wenn Sie die Arbeit im abgesicherten Modus abgeschlossen haben, überprüfen Sie das Ergebnis, indem Sie den Computer anschließend im Normalmodus starten. Dann sollten Sie wieder so mit dem Computer arbeiten können, wie Sie es gewohnt sind.

Im abgesicherten Modus lädt Windows 8 nur die wichtigsten Dateien, Dienste und Treiber. Zu den Treibern, die geladen werden, gehören die Treiber für Maus, Monitor, Tastatur, Massenspeicher und Basisvideo. Der Monitortreiber ist für die Grundeinstellungen und Modi des Monitors zuständig, der Basisvideotreiber stellt die Grundparameter und den Anzeigemodus für die Grafikkarte des Computers ein. Netzwerkdienste oder -treiber werden nicht geladen, sofern Sie nicht den abgesicherten Modus mit Netzwerktreibern wählen. Da im abgesicherten Modus nur eine Teilmenge der Konfigurationsdaten geladen wird, eignet sich dieser Modus gut zur Fehlersuche.

Mit folgenden Schritten können Sie einen Windows 8-Computer im abgesicherten Modus starten:

1. Wenn der Computer nicht normal startet, wird in der Startphase der Wiederherstellungsbildschirm angezeigt. Tippen oder klicken Sie auf dem Wiederherstellungsbildschirm auf *Erweiterte Reparaturoptionen anzeigen* und dann auf *Problembehandlung*.
2. Tippen oder klicken Sie auf dem Problembehandlungsbildschirm auf *Erweiterte Optionen* und dann auf *Starteinstellungen*.
3. Tippen oder klicken Sie auf dem Starteinstellungsbildschirm auf *Neu starten*.
4. Wenn Sie mehrere Betriebssysteme nebeneinander installiert haben und das herkömmliche Startmenü erscheint, wählen Sie mit den PFEILTASTEN den gewünschten abgesicherten Modus aus und drücken Sie dann die EINGABETASTE. Haben Sie nur Windows 8 installiert, erscheint der Bildschirm *Starteinstellungen*, auf dem Sie mit den Zifferntasten oder den Funktionstasten den gewünschten Modus auswählen. Welchen abgesicherten Modus Sie brauchen, hängt davon ab, welche Probleme zu lösen sind. Zur Verfügung stehen folgende Modi:
 - **Computer reparieren** Erscheint nur im herkömmlichen Startmenü und lädt wieder das Tool Systemstartreparatur, wie im Abschnitt »Reparieren und Wiederherstellen eines Computers« weiter unten in diesem Kapitel beschrieben.
 - **Abgesicherten Modus aktivieren** Lädt in der Initialisierungssequenz nur die wichtigsten Dateien, Dienste und Treiber. Dazu gehören die Treiber für Maus, Monitor, Tastatur, Massenspeicher und Basisvideo. Es werden weder Netzwerktreiber geladen noch Netzwerkdienste gestartet.
 - **Abgesicherten Modus mit Netzwerktreibern aktivieren** Lädt die wichtigsten Dateien, Dienste und Treiber sowie Dienste und Treiber für das Netzwerk.
 - **Abgesicherten Modus mit Eingabeaufforderung aktivieren** Lädt die wichtigsten Dateien, Dienste und Treiber und öffnet dann statt der grafischen Oberfläche von Windows 8 eine Eingabeaufforderung. Es werden weder Netzwerktreiber geladen noch Netzwerkdienste gestartet.

TIPP Im abgesicherten Modus mit Eingabeaufforderung können Sie die Explorershell von der Befehlszeile aus öffnen, indem Sie STRG+UMSCHALT+ESC drücken, um den Task-Manager zu öffnen. Wählen Sie dann den Menübefehl *Datei/Neuer Task ausführen*, um das Dialogfeld *Neuen Task erstellen* zu öffnen. Geben Sie **explorer.exe** ein und tippen oder klicken Sie auf OK.

- **Startprotokollierung aktivieren** Erlaubt die Protokollierung des Startvorgangs in einem Startprotokoll.
 - **Anzeige mit niedriger Auflösung aktivieren** Ermöglicht den Start des Systems mit einer niedrigen Auflösung von 640 × 480 Bildpunkten. Das ist nützlich, wenn ein Grafikmodus eingestellt wurde, der sich nicht für den aktuell verwendeten Monitor eignet.
 - **Automatischen Neustart bei Systemfehler deaktivieren** Verhindert, dass Windows nach einem Absturz neu startet. Andernfalls startet Windows standardmäßig neu, wenn ein Absturz auftritt. Wenn Windows wiederholt neu startet, handelt es sich möglicherweise um ein Problem mit der Firmwarekonfiguration, wie in Kapitel 4, »Verwalten von Firmware, Startkonfiguration und Systemstart«, beschrieben.
 - **Erzwingen der Treibersignatur deaktivieren** Startet den Computer im abgesicherten Modus, ohne die Richtlinieneinstellungen für die digitale Signatur von Treibern durchzusetzen. Ist ein Treiber mit einer ungültigen oder fehlenden digitalen Signatur die Ursache des Fehlstarts, können sie damit das Problem vorerst beheben, sodass Sie den Computer starten und das Problem lösen können, indem Sie einen neuen Treiber installieren oder die Richtlinieneinstellungen für Treibersignaturen ändern.
 - **Schutz des Antischadsoftware-Frühstarts deaktivieren** Startet den Computer im abgesicherten Modus, allerdings ohne die Starttreiber für die Antischadsoftware-Software des Computers. Falls dieser Starttreiber den Start des Computers verhindert, suchen Sie auf der Website des Herstellers nach einem Update, mit dem sich das Startproblem lösen lässt, oder sie konfigurieren die Software ohne Schutz beim Systemstart.
 - **Drücken Sie die EINGABETASTE, um zum Betriebssystem zurückzukehren** Starten den Computer mit den normalen Einstellungen.
5. Tritt das Startproblem beim Start im abgesicherten Modus nicht erneut auf, können Sie die Standardeinstellungen und die Basisgerätetreiber als Ursachen ausschließen. Ist ein neu installiertes Gerät oder ein aktualisierter Gerätetreiber die Ursache des Problems, können Sie das Gerät im abgesicherten Modus entfernen, die Aktualisierung rückgängig machen oder eine andere Version der Treibersoftware installieren.
 6. Gibt es beim normalen Systemstart immer noch Probleme und vermuten Sie, dass die Ursache bei der Hardware, der Software oder bei den Einstellungen liegt, bleiben Sie im abgesicherten Modus und versuchen, vorherige Änderungen mit der Systemwiederherstellung rückgängig zu machen, wie im Abschnitt »Sichern und Wiederherstellen des Systemzustands mit der Systemwiederherstellung« gleich im Anschluss beschrieben.
 7. Löst auch die Systemwiederherstellung das Problem nicht, versuchen Sie, die Startoptionen zu ändern, wie im Abschnitt »Verwalten der Systemkonfiguration und der Systemstartoptionen« von Kapitel 2 beschrieben.

Sichern und Wiederherstellen des Systemzustands mit der Systemwiederherstellung

Im Abschnitt »Die Registerkarte Computerschutz« von Kapitel 2 wurde die Systemwiederherstellung vorgestellt und ihre Konfiguration beschrieben. Wiederherstellungspunkte lassen sich zur Wiederherstellung von Systemen verwenden, auf denen sich nach der Durchführung einer Aktualisierung, nach der Installation von Software oder von Hardware oder nach anderen Änderungen Probleme ergeben. Die folgenden Abschnitte beschreiben, wie sich Wiederherstellungspunkte manuell erstellen lassen und wie

das System mit Wiederherstellungspunkten wiederhergestellt werden kann. Diese Wiederherstellungsvorgänge lassen sich in den meisten Fällen rückgängig machen.

Grundlagen der Wiederherstellungspunkte

Die Systemwiederherstellung überwacht das Betriebssystem auf Änderungen und erstellt in regelmäßigen Abständen Wiederherstellungspunkte, bevor Änderungen durchgeführt werden. Dazu wird ein Abbild der Systemkonfiguration erstellt und auf den Datenträger geschrieben, damit sich dieses Abbild bei Bedarf zur Wiederherstellung des Systems in dem Zustand verwenden lässt, in dem es sich zum Zeitpunkt der Erstellung des Wiederherstellungspunkts befand. Wichtig ist, dass die Systemwiederherstellung keine persönlichen Daten betrifft. Sie können ein System mit einem Wiederherstellungspunkt wiederherstellen, ohne die Anwendungsdaten, zwischengespeicherten Dateien oder Dokumente der Benutzer zu verändern. Die Systemwiederherstellung schreibt auch keine Informationen in den Dokumentordner.

Die Systemwiederherstellung überwacht und speichert Konfigurationsdaten für jedes Laufwerk eines Computers separat. Das bedeutet, dass auf jedem Laufwerk Speicherplatz für die Systemwiederherstellung reserviert wird. Außerdem können Sie die Überwachung von bestimmten Laufwerken bei Bedarf deaktivieren. Ist ein Laufwerk für die Systemwiederherstellung konfiguriert, können Sie es nach Änderungen wiederherstellen, falls sich Probleme ergeben sollten. Ist ein Laufwerk nicht für die Systemwiederherstellung konfiguriert, werden Änderungen nicht erfasst und das Laufwerk lässt sich auch nicht wiederherstellen, falls sich nach Änderungen Probleme ergeben. Auf den meisten Computern sollten Sie eine Systemwiederherstellung für das Systemlaufwerk einrichten, auf dem die Betriebssystemdateien liegen, und für alle Laufwerke, auf denen wichtige Anwendungen liegen.

Wiederherstellungspunkte lassen sich auf drei verschiedene Arten erstellen: als Prüfpunkte, nach Datum oder bei bestimmten Ereignissen. Einzelne Abbilder, die vom Betriebssystem erstellt werden, heißen Systemwiederherstellungspunkte. Normale Systemwiederherstellungspunkte werden in Abständen von ungefähr 24 Stunden erstellt. Wird ein Computer ausgeschaltet, wenn der tägliche Prüfpunkt auf dem Plan steht, erstellt die Systemwiederherstellung den Prüfpunkt nach dem nächsten Start des Computers.

HINWEIS

Ältere Windows-Versionen erstellen bereits bei der Installation des Betriebssystems einen ersten Wiederherstellungspunkt, bei der Installation von Windows 8 ist dies aber nicht der Fall. Mit *PC auffrischen* und *Originaleinstellung wiederherstellen* stehen Optionen zur Verfügung, mit denen sich der Computer in seinen Anfangszustand zurückversetzen lässt. Weitere Informationen über diese beiden Optionen finden Sie weiter vorne in diesem Kapitel im Abschnitt »Wiederherstellen nach einem fehlgeschlagenen Start«.

Wenn die Systemwiederherstellung aktiviert ist, werden manche Abbilder automatisch erstellt, wenn bestimmte Ereignisse eintreten, zum Beispiel bei Änderungen oder der Installation von Anwendungen. Der Einfachheit halber nenne ich diese Abbilder »Installationswiederherstellungspunkte«. Tatsächlich gibt es mehrere dieser Wiederherstellungspunkte und jeder hat eine andere Aufgabe. Auf Ereignisbasis werden folgende Wiederherstellungspunkte erstellt:

- **Installationswiederherstellungspunkte** Werden vor der Installation von Programmen erstellt, die mit kompatiblen Installationsprogrammen installiert werden. Sie können Installationswiederherstellungspunkte zur Kontrolle der Anwendungsinstallation verwenden und um einen Computer in den Zustand zurückzusetzen, in dem er sich vor der Installation einer Anwendung befand. Die Wiederherstellung des Computerzustands bedeutet, dass alle Datei- und Registrierungseinstellungen für das installierte Programm verschwunden sind. Sie bedeutet auch, dass Programme und Systemdateien, die durch die Installation geändert wurden, wieder in ihre vorigen Zustände zurückversetzt

werden. Anschließend funktioniert das Programm aber nicht mehr und Sie müssen es neu installieren, falls der Benutzer es wieder verwenden möchte.

ACHTUNG Diese Wiederherstellungspunkte werden aus einem guten Grund *Installationswiederherstellungspunkte* genannt, und nicht *Programmeinstallationswiederherstellungspunkte*. Durch die Wiederherstellung werden nicht alle Anwendungsdateien entfernt, sondern nur die Datei- und Registrierungseinträge, die sich auf die Arbeit des Computers auswirken können. Um ein Programm vollständig zu entfernen, müssen Sie die Konsole *Programme und Features* aus der Systemsteuerung verwenden.

- **Wiederherstellungspunkte für automatische Updates** Werden vor der Installation eines automatischen Updates erstellt. Weist ein Computer nach der Installation eines automatischen Updates Probleme auf, können Sie den Wiederherstellungspunkt verwenden, um den Computer in seinen vorigen Zustand zurückzusetzen. (Sie können die Konsole *Programme und Features* verwenden, um automatische Updates zu entfernen.)
- **Wiederherstellungspunkte zum Rückgängigmachen der Wiederherstellung** Werden vor der Wiederherstellung eines Computers erstellt. Wenn Sie feststellen, dass Sie zum falschen Punkt zurückgegangen sind oder dass der Wiederherstellungspunkt nicht richtig funktioniert hat, können Sie diesen Wiederherstellungspunkt verwenden, um die Wiederherstellung rückgängig zu machen und den Computer in den Zustand zurückzusetzen, in dem er sich vor der Wiederherstellung befand.
- **Wiederherstellungspunkte für nichtsignierte Gerätetreiber** Werden vor der Installation eines nichtsignierten oder nichtzertifizierten Treibers auf einem Computer erstellt. Ergeben sich nach der Installation eines nichtsignierten oder nichtzertifizierten Treibers Probleme, können Sie diese Wiederherstellungspunkte zur Wiederherstellung des Computers in den Zustand verwenden, in dem er sich vor der Installation des Treibers befand. Was signierte und zertifizierte Treiber betrifft, sollte das normale Verfahren für die Wiederherstellung der Vorgängerversion des Treibers ausreichen.
- **Sicherungswiederherstellungspunkte** Werden vor der Wiederherstellung von Dateien oder Systemdaten mit dem Sicherungsprogramm erstellt. Schlägt die Wiederherstellung fehl oder arbeitet der Computer nach der Wiederherstellung nicht richtig, können Sie die Änderungen rückgängig machen und den Computer in den vorigen Zustand zurückversetzen.

Benutzer können Wiederherstellungspunkte auch manuell herstellen. Diese Wiederherstellungspunkte werden *manuelle Wiederherstellungspunkte* genannt. Sie sollten Benutzern empfehlen, vor irgendwelchen Arbeiten, die ein Problem für das System mit sich bringen könnten, Wiederherstellungspunkte zu erstellen.

Sie können einen Computer wiederherstellen, wenn er sich im Normalmodus oder im abgesicherten Modus befindet. Im Normalmodus wird vor der Wiederherstellung des Computers ein neuer Wiederherstellungspunkt erstellt. Im abgesicherten Modus wird aber kein Wiederherstellungspunkt erstellt, mit dem der Vorgang rückgängig gemacht werden könnte. Änderungen, die Sie im abgesicherten Modus durchführen, werden nicht erfasst und lassen sich auch nicht mit Wiederherstellungspunkten rückgängig machen. Allerdings können Sie im abgesicherten Modus mit zuvor erstellten Wiederherstellungspunkten eine Wiederherstellung durchführen.

Erstellen manueller Wiederherstellungspunkte

Mit folgenden Schritten können Sie einen manuellen Wiederherstellungspunkt erstellen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie im linken Fensterabschnitt auf *Computerschutz*.

3. Wählen Sie das Laufwerk aus, für das Sie einen Wiederherstellungspunkt erstellen möchten, und tippen oder klicken Sie dann auf *Erstellen*.
4. Geben Sie eine Beschreibung des Wiederherstellungspunkts ein, zum Beispiel »Vor der Installation des Monitortreiberupdates«. Tippen oder klicken Sie auf *Erstellen*.
5. Warten Sie, bis der Wiederherstellungspunkt erstellt ist, und tippen oder klicken Sie dann auf *OK*.

Wiederherstellen mit Wiederherstellungspunkten

Um einen Computer auf einen bestimmten Wiederherstellungspunkt zurückzuführen, während das Betriebssystem läuft, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System*.
2. Tippen oder klicken Sie im linken Fensterabschnitt auf *Computerschutz* und dann auf die Schaltfläche *Systemwiederherstellung*. Die Systemwiederherstellung untersucht die verfügbaren Wiederherstellungspunkte auf dem Computer. Dieser Prozess kann mehrere Minuten dauern. Wenn er abgeschlossen ist, empfiehlt die Systemwiederherstellung einen Wiederherstellungspunkt. Wenn Sie überprüfen möchten, welche Programme von der Wiederherstellung betroffen sind, tippen oder klicken Sie auf *Nach betroffenen Programmen suchen*.
3. Wenn Sie überprüfen möchten, welche Wiederherstellungspunkte noch verfügbar sind, wählen Sie *Anderen Wiederherstellungspunkt auswählen* und tippen oder klicken auf *Weiter*. Die jüngsten Wiederherstellungspunkte werden unter Angabe von Datum, Uhrzeit, Beschreibung und Typ aufgelistet. Sie können feststellen, auf welche Programme die Wiederherstellungsoperation Auswirkungen hat, indem Sie einen Wiederherstellungspunkt auswählen und auf *Nach betroffenen Programmen suchen* klicken. Um noch mehr Wiederherstellungspunkte zu sehen, tippen oder klicken Sie auf *Weitere Wiederherstellungspunkte anzeigen*. Um zu überprüfen, welche Programme von der Wiederherstellung mit einem bestimmten Wiederherstellungspunkt betroffen sind, tippen oder klicken Sie auf einen Wiederherstellungspunkt und tippen oder klicken dann auf *Nach betroffenen Programmen suchen*.
4. Wenn Sie einen Wiederherstellungspunkt ausgewählt haben oder den empfohlenen akzeptieren, tippen oder klicken Sie auf *Weiter*.
5. Tippen oder klicken Sie auf *Fertig stellen*. Tippen oder klicken Sie auf *Ja*, wenn Sie bestätigen sollen, ob Sie die Systemdateien und Einstellungen des Computers mit dem ausgewählten Wiederherstellungspunkt wiederherstellen wollen.

So führen Sie einen Computer auf einen bestimmten Wiederherstellungspunkt zurück, wenn das Betriebssystem nicht mehr läuft:

1. Wenn sich der Computer nicht normal starten lässt, wird beim Start der Wiederherstellungsbildschirm angezeigt. Tippen oder klicken Sie auf dem Wiederherstellungsbildschirm auf *Erweiterte Reparaturoptionen anzeigen* und dann auf *Problembehandlung*.
2. Tippen oder klicken Sie auf dem Problembehandlungsbildschirm auf *Erweiterte Optionen* und dann auf *System wiederherstellen*.
3. Die Systemwiederherstellung überprüft die auf dem Computer verfügbaren Wiederherstellungspunkte. Anschließend können Sie auf ähnliche Weise wie in den Schritten 3 bis 5 der vorigen Prozedur einen Wiederherstellungspunkt auswählen und anwenden.

Während der Wiederherstellung fährt die Systemwiederherstellung Windows 8 herunter. Durch den Abschluss der Wiederherstellung wird Windows 8 mit den Werten wiederhergestellt, die bei der Erstellung des gewählten Wiederherstellungspunkts galten. Nach dem Neustart des Systems wird ein Dialogfeld *Systemwiederherstellung* angezeigt. Lesen Sie die angezeigte Meldung und tippen oder klicken Sie

dann auf *Schließen*. Sollte Windows 8 immer noch nicht richtig arbeiten, können Sie einen anderen Wiederherstellungspunkt wählen oder den Wiederherstellungsvorgang rückgängig machen, indem Sie diese Prozedur wiederholen und diesmal die Option *Systemwiederherstellung rückgängig machen* wählen.

Problembehandlung der Systemwiederherstellung

Der Systemwiederherstellung gelingt es nicht immer, die Wiederherstellung fehlerfrei auszuführen. Wenn die Systemwiederherstellung es nicht schafft, den Computer auf den Zustand zurückzuführen, den er zur gewünschten Zeit hatte, können Sie den Wiederherstellungsvorgang erneut ausführen und versuchen, den Computer auf diese Weise wiederherzustellen. Wählen Sie diesmal aber einen anderen Wiederherstellungspunkt.

Erstellen und Verwenden des Dateiversionsverlaufs

Sie können den Dateiversionsverlauf verwenden, um Datensicherungen für persönliche Dateien aus Bibliotheken, den Desktop und für Kontakt- und Favoritenlisten durchzuführen. Sie müssen über die entsprechenden Berechtigungen verfügen, um Dateien auf einem Computer sichern und wiederherstellen zu können.

Konfigurieren von Dateiversionsverlaufsicherungen

Windows 8 kann automatisch persönliche Datensicherungen erstellen. Persönliche Datensicherungen dienen dazu, Bilder, Musik, Videos, E-Mails, Dokumente und andere wichtige Dateien in regelmäßigen Abständen zu sichern, damit sie sich bei Bedarf auf einem anderen Computer wiederherstellen lassen. Dabei werden die Ordner *Dokumente*, *Bilder*, *Musik* und *Videos* aus *Benutzer\Öffentlich* ebenso im Rahmen der Datensicherung gesichert wie die Unterordner *Kontakte*, *Desktop*, *Dokumente*, *Favoriten*, *Bilder*, *Musik* und *Videos* aus dem Profil des Benutzers.

Wie Abbildung 10.6 zeigt, wird der Dateiversionsverlauf in der Systemsteuerung konfiguriert.

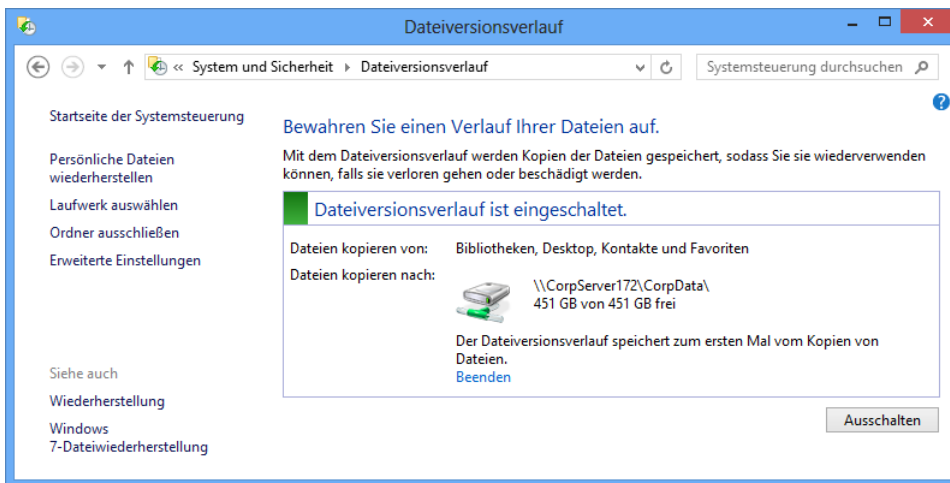


Abbildung 10.6 Die Seite *Dateiversionsverlauf* zeigt eine Übersicht über die aktuelle Konfiguration und den verfügbaren Speicherplatz am ausgewählten Speicherort an

Berücksichtigen Sie bei der Arbeit mit dem Dateiversionsverlauf Folgendes:

- Eine Datensicherung persönlicher Daten kann nur auf Wechselmedien oder Dateifreigaben erfolgen. Sie kann nicht auf den internen Laufwerken eines Computers erstellt werden.
- Die Sicherung persönlicher Daten erfolgt automatisch, wenn Sie den Dateiversionsverlauf aktiviert haben. Standardmäßig speichert der Dateiversionsverlauf die Dateikopien stündlich.
- Standardmäßig werden gespeicherte Versionen persönlicher Daten ohne Zeitbeschränkung aufbewahrt und dürfen nicht mehr als 5 Prozent des Speicherplatzes vom Speicherort beanspruchen.

Bei Speicherorten im Netzwerk wird die persönliche Datensicherung in einem Unterordner angelegt, der nach folgender Syntax benannt wird: *BenutzerName@DomäneOderComputer*, zum Beispiel *WilliamS@Cpandl.com* oder *WilliamS@CorpPC12*. In diesem Ordner gibt es einen Unterordner mit dem Namen des Computers des Benutzers, beispielsweise *CORPC12*, der wiederum die Unterordner *Configuration* und *Data* enthält. Bei Wechselmedien wird zuerst ein Stammordner namens *FileHistory* erstellt.

Aktivieren von Dateiversionsverlaufsicherungen und Konfigurieren der Geräte

Für USB-Laufwerke oder andere Wechselmedien können Sie auf folgende Weise automatische Datensicherungen aktivieren und Ihre erste Datensicherung manuell erstellen:

1. Schließen Sie ein USB-Laufwerk oder ein anderes Wechselmedium an den Computer an.
2. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *System und Sicherheit* auf *Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern*.
3. Tippen oder klicken Sie auf *Einschalten*. Windows 8 schaltet den Dateiversionsverlauf ein und erstellt eine erste Datensicherung.

Bei einem Speicherort im Netzwerk können Sie auf folgende Weise automatische Datensicherung aktivieren und Ihre erste Datensicherung erstellen.

1. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *System und Sicherheit* auf *Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern*.
2. Tippen oder klicken Sie auf *Laufwerk auswählen* und dann auf *Netzwerkadresse hinzufügen*. Falls die Netzwerkerkennung und Dateifreigabe deaktiviert ist und Sie eine entsprechende Meldung erhalten, tippen oder klicken Sie auf den Benachrichtigungsbereich und dann auf *Netzwerkerkennung und Dateifreigabe aktivieren*.
3. Geben Sie im Textfeld *Ordner* den UNC-Pfad des Ordners an, in dem die persönlichen Daten gespeichert werden sollen, beispielsweise *\\CorpServer172\CorpData*, und tippen oder klicken Sie dann auf *OK*.
4. Wenn Sie auf *Einschalten* tippen oder klicken, schaltet Windows 8 den Dateiversionsverlauf ein und erstellt die erste Datensicherung.

Mit den Optionen auf der Seite *Dateiversionsverlauf* können Sie die Einstellung der Datensicherung auf verschiedene Arten ändern. Für jeden Benutzer kann es immer nur ein Dateiversionsverlauf-Laufwerk geben. Sie können das Dateiversionsverlauf-Laufwerk an einen anderen Speicherort im Netzwerk verlegen. So ermöglicht Windows die automatische Verschiebung der Daten an den neuen Speicherort:

1. Tippen oder klicken Sie auf der Seite *Dateiversionsverlauf* auf *Laufwerk auswählen* und dann auf *Netzwerkadresse hinzufügen*.
2. Geben Sie im Textfeld *Ordner* den UNC-Pfad des Ordners an, in dem die persönlichen Daten gespeichert werden sollen, beispielsweise *\\CorpServer96\UserData*. An diesem Ort darf es noch keine Dateiversionsverlaufsdaten für den Benutzer geben.

3. Tippen oder klicken Sie auf *Ordner auswählen* und dann auf *OK*. Wenn Sie zur Bestätigung aufgefordert werden, dass Sie die vorhandenen persönlichen Daten des Benutzers verschieben möchten, tippen oder klicken Sie auf *Ja*. Wenn am betreffenden Speicherort bereits persönliche Daten für den Benutzer liegen, werden die Dateien nicht verschoben und Sie werden gegebenenfalls auf *OK* tippen oder klicken müssen, um zu bestätigen, dass Sie dies verstanden haben.

Sie können das Dateiversionsverlauf-Laufwerk auch von einem Speicherort im Netzwerk auf ein Wechselmedium umstellen oder von einem Wechselmedium auf ein anderes:

1. Schließen Sie ein USB-Laufwerk oder ein anderes Wechselmedium an den Computer an.
2. Tippen oder klicken Sie auf der Seite *Dateiversionsverlauf* auf *Laufwerk auswählen*.
3. Tippen oder klicken Sie auf das Wechselmedium, das verwendet werden soll, und dann auf *OK*.
4. Wenn Sie zur Bestätigung aufgefordert werden, dass Sie die vorhandenen persönlichen Daten des Benutzers verschieben möchten, tippen oder klicken Sie auf *Ja*. Wenn am betreffenden Speicherort bereits persönliche Daten für den Benutzer liegen, werden die Dateien nicht verschoben und Sie werden gegebenenfalls auf *OK* tippen oder klicken müssen, um zu bestätigen, dass Sie dies verstanden haben.

Ausschließen von Ordnern aus Dateiversionsverlaufsicherungen

Standardmäßig enthalten Datensicherungen persönlicher Daten, die mit dem Dateiversionsverlauf erstellt werden, die Unterordner *Dokumente*, *Bilder*, *Musik* und *Videos* von *Benutzer\Öffentlich* und die Unterordner *Kontakte*, *Desktop*, *Dokumente*, *Favoriten*, *Bilder*, *Musik* und *Videos* aus dem Profil des Benutzers. So schließen Sie Ordner aus der Datensicherung aus:

1. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *System und Sicherheit* auf *Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern*.
2. Tippen oder klicken Sie auf *Ordner ausschließen*. Alle derzeit ausgeschlossenen Ordner werden auf der Seite *Ordner ausschließen* angezeigt.
3. Wenn Sie einen Ordner ausschließen möchten, tippen oder klicken Sie auf *Hinzufügen*. Wählen Sie im Dialogfeld *Ordner auswählen* den Ordner aus, der ausgeschlossen werden soll, und tippen oder klicken Sie dann auf *Ordner auswählen*. Wenn Sie beispielsweise *Öffentliche Dokumente* ausschließen möchten, erweitern Sie *Bibliotheken* und *Dokumente*, tippen oder klicken auf *Öffentliche Dokumente* und tippen oder klicken dann auf *Ordner auswählen*.
4. Sollen die Daten aus einem ausgeschlossenen Ordner wieder in die Sicherung aufgenommen werden, wählen Sie den Ordner in der Liste *Ausgeschlossene Ordner und Bibliotheken* aus und tippen oder klicken auf *Entfernen*.

Ändern der Standardsicherungseinstellungen

Der Dateiversionsverlauf speichert standardmäßig stündlich Kopien der Dateien. Diese gespeicherten Versionen werden ohne Zeitbeschränkung aufbewahrt, solange sie nicht 5 Prozent der Speicherkapazität des verwendeten Speicherorts überschreiten. Auf folgende Weise können Sie die Standardeinstellungen ändern:

1. Tippen oder klicken Sie in der Systemsteuerung unter der Überschrift *System und Sicherheit* auf *Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern*.
2. Tippen oder klicken Sie auf *Erweiterte Einstellungen*. Die aktuellen Einstellungen werden auf der Seite *Erweiterte Einstellungen* angezeigt (Abbildung 10.7).

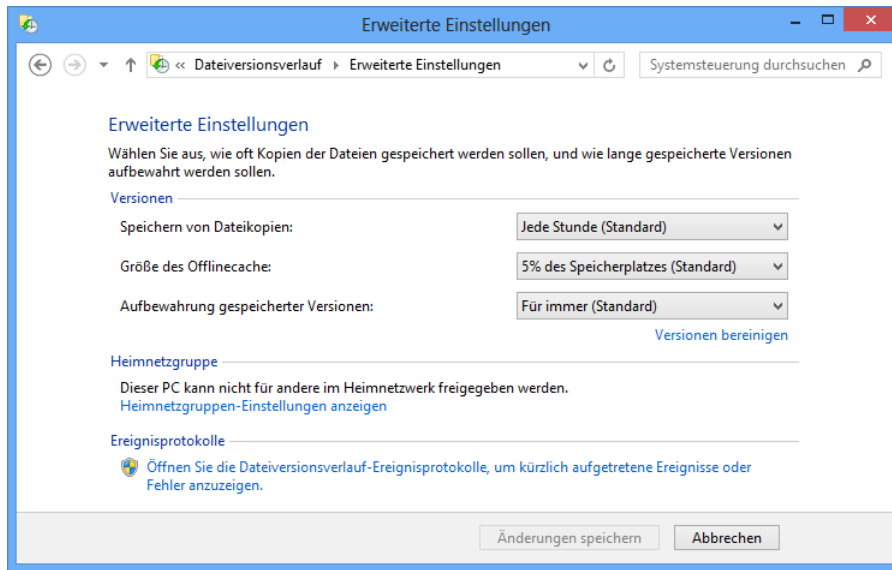


Abbildung 10.7 Anzeigen und Verwalten der Standardeinstellungen für den Dateiversionsverlauf

3. Verwenden Sie bei Bedarf die Liste *Speichern von Dateikopien*, um andere Sicherungsperioden einzustellen. Durch die Sicherungen entstehen gespeicherte Versionen, auf die ein Benutzer zurückgehen kann und die er zur Wiederherstellung verwenden kann. Die Systembelastung, die durch die Datensicherung hervorgerufen wird, können Sie durch längere Intervalle verringern, beispielsweise durch die Einstellungen *Alle 3 Stunden* oder *Alle 6 Stunden*. Die längste Periode ist *Täglich*.
4. Verwenden Sie bei Bedarf die Liste *Größe des Offlinecache*, um die maximale Größe des für Sicherungen verfügbaren Speicherplatzes einzustellen. Überprüfen Sie die Speicherkapazität des verwendeten Laufwerks und passen Sie den verwendeten Speicherplatz gegebenenfalls an. Verfügt das Laufwerk zum Beispiel über eine Speicherkapazität von 2 TByte, ist es vielleicht angebracht, 2 Prozent dieser Kapazität für den Offlinecache zu verwenden, während bei einem Laufwerk mit einer Speicherkapazität von 100 GByte eher 10 Prozent der Kapazität erforderlich sind.
5. Geben Sie in der Liste *Aufbewahrung gespeicherter Versionen* bei Bedarf an, wie lange die gespeicherten Versionen aufbewahrt werden sollen. Wählen Sie eine Einstellung, die für die Arbeitsweise des Benutzers sinnvoll ist. Wenn Sie *Für immer* wählen, werden die gespeicherten Versionen ohne Zeitbeschränkung aufbewahrt und auch dann nicht überschrieben, wenn der Offlinecache voll ist. Wenn Sie *Bis Platz benötigt wird* wählen, werden die gespeicherten Versionen aufbewahrt, bis der Offlinecache voll ist. Anschließend werden die ältesten Versionen nach Bedarf überschrieben, wenn neue Versionen aufgenommen werden. Alle anderen Einstellungen liegen zwischen diesen beiden Extremen und sorgen dafür, dass gespeicherte Versionen nach einer gewissen Zeit gelöscht werden. Allerdings können keine neuen Versionen aufgenommen werden, wenn der Offlinecache voll ist, bis neuer Speicherplatz verfügbar ist (indem alte Versionen ihre Verfallszeit erreichen).

PRAXISTIPP

Auf der Seite *Erweiterte Einstellungen* können Sie jederzeit manuell alte Dateiversionen löschen. Tippen oder klicken Sie auf *Versionen bereinigen*. Wählen Sie im Dialogfeld *Bereinigung des Dateiversionsverlaufs* die Zeitgrenzen für die Versionen aus, die gelöscht werden sollen, und tippen oder klicken Sie dann auf *Bereinigen*. Sie können zum Beispiel festlegen, dass alle Dateien gelöscht werden sollen, die älter als 6 Monate sind, oder dass alle Versionen bis auf die neuesten Versionen gelöscht werden sollen.

Wiederherstellen persönlicher Daten

Gehen Sie folgendermaßen vor, um persönliche Datendateien wiederherzustellen, die Sie vorher im Dateiversionsverlauf gesichert haben:

1. Tippen oder klicken Sie in der Systemsteuerung unter *System und Sicherheit* auf *Sicherungskopien von Dateien mit dem Dateiversionsverlauf speichern*.
2. Tippen oder klicken Sie auf *Persönliche Dateien wiederherstellen*. Suchen Sie auf der Startseite des Dateiversionsverlaufs mit den Schaltflächen *Vorherige Version* und *Nächste Version* die Version heraus, die Sie verwenden möchten. Sie können in den Ordnerstrukturen der Snapshots so navigieren, wie Sie es von den Ordnern eines Festplattenlaufwerks gewohnt sind.
3. Die Snapshots werden mit Datum, Uhrzeit und einer Versionsnummer aufgelistet (zum Beispiel *Donnerstag, 12. Oktober 2012 13:52 | 2 von 15*). Wenn Sie den Ordner oder die Datei gefunden haben, die Sie wiederherstellen möchten, klicken Sie sie mit der rechten Maustaste an oder halten sie gedrückt, und tippen oder klicken dann auf *Wiederherstellen*. Sie können auch mehrere Elemente auswählen, die wiederhergestellt werden sollen.

TIPP Sie können Dateien und Ordner auch an anderen Orten wiederherstellen. Nachdem Sie die Elemente ausgewählt haben, die Sie wiederherstellen möchten, klicken Sie eines der ausgewählten Elemente mit der rechten Maustaste an oder halten es gedrückt, und wählen *Wiederherstellen in*. Dann können Sie den gewünschten Speicherort für die Wiederherstellung auswählen.

Problembehandlung für Systemstart und Herunterfahren

Als Administrator haben Sie häufig mit Problemen zu tun, die sich beim Start oder beim Herunterfahren von Computern zeigen. Der folgende Abschnitt beschreibt, wie man solche Probleme angehen kann.

Behebung von Problemen beim Neustart und dem Herunterfahren des Systems

Normalerweise können Sie Windows 8 mit dem Schalter *Ein/Aus* herunterfahren oder neu starten. Wenn Sie mit dem Startbildschirm oder dem Desktop arbeiten, gehen Sie also folgendermaßen vor, um einen Computer herunterzufahren oder zu starten:

1. Zeigen Sie die Optionen durch eine Streifbewegung vom rechten Bildrand oder dadurch an, dass Sie den Mauszeiger in die untere rechte Ecke des Bildschirms bewegen.
2. Tippen oder klicken Sie auf *Einstellungen* und dann auf *Ein/Aus*.
3. Tippen oder klicken Sie je nach Bedarf auf *Herunterfahren* oder *Neu starten*.

In einer Standardkonfiguration können Sie auch den Ein/Aus-Schalter des Computers betätigen, um den Computer in der vorgesehenen Weise herunterzufahren. Manchmal lässt sich Windows 8 aber nicht wie gewohnt herunterfahren oder neu starten und Sie müssen andere Maßnahmen ergreifen. Gehen Sie in solchen Fällen folgendermaßen vor:

1. Drücken Sie STRG+ALT+ENTF. Der Windows-Bildschirm wird angezeigt. Tippen oder klicken Sie auf *Task-Manager*. Wird im Task-Manager nichts angezeigt, tippen oder klicken Sie auf *Mehr Details*.
2. Suchen Sie auf der Registerkarte *Prozesse* nach einer Anwendung oder einem Prozess, der nicht mehr reagiert. Werden alle Anwendungen normal ausgeführt, fahren Sie mit Schritt 5 fort.

3. Wählen Sie die Anwendung aus, die nicht mehr reagiert, und tippen oder klicken Sie dann auf *Task beenden*.
4. Wenn die Anwendung nicht darauf reagiert, erscheint eine Meldung, in der Sie entweder die Aufforderung zur Beendigung der Ausführung abbrechen oder die Anwendung sofort beenden können. Tippen oder klicken Sie auf *Jetzt beenden*.
5. Versuchen Sie gegebenenfalls, den Computer herunterzufahren oder neu zu starten. Drücken Sie STRG+ALT+ENTF, tippen oder klicken Sie auf das Netzschaltersymbol in der unteren rechten Ecke und klicken Sie dann nach Bedarf auf *Neu starten* oder *Herunterfahren*.

Windows 8 meldet auch den aktuellen Benutzer ab und fährt das System herunter, wenn Sie den Netzschalter des Computers drücken. Falls irgendwelche Programme nicht reagieren, können Sie wählen, ob Sie die Abmeldung erzwingen oder noch einige Sekunden warten wollen, bis Windows selbst die Abmeldung erzwingt.

PRAXISTIPP

Als letzten Ausweg müssen Sie das System vielleicht hart herunterfahren, indem Sie den Netzschalter des Computers länger gedrückt halten oder den Netzstecker ziehen. Wenn Sie das tun, wird beim nächsten Neustart wahrscheinlich die Datenträgerprüfung aktiv. Damit prüft der Computer, ob sich durch das harte Ausschalten vielleicht Probleme mit dem Dateisystem ergeben haben. Wird die Datenträgerprüfung nicht automatisch gestartet, empfiehlt es sich in solchen Fällen, sie manuell zu starten.

STOP-Fehler und ihre Bedeutung

Der Abschnitt »Einstellen der Wiederherstellungsoptionen« in Kapitel 2 beschreibt, wie Sie Windows 8 konfigurieren, um Debuginformationen zu erhalten. Wenn beim Start von Windows 8, bei der Installation einer Anwendung oder einer anderen Operation ein größerer Fehler auftritt, sehen Sie eine STOP-Fehlermeldung, die den ganzen Bildschirm füllt. Lesen Sie die Angaben sorgfältig und schreiben Sie sich folgende Informationen auf:

- **Fehlerbezeichnung** Die Bezeichnung des Fehlers sollte in der dritten Zeile des Fehlerbildschirms in Großbuchstaben angezeigt werden, wie zum Beispiel `KERNEL_STACK_INPAGE_ERROR`.
- **Empfehlungen zur Problembehebung** An die Fehlerbezeichnung schließen sich Empfehlungen zur Fehlerbehebung an. Um welche Empfehlungen es sich handelt, hängt von der Art des aufgetretenen Fehlers ab. Die Empfehlungen geben allgemeine Hinweise zur Behebung des Problems.
- **Fehlernummer** An die Empfehlungen zur Fehlerbehebung schließen sich technische Informationen an. In der Zeile unter der Überschrift des Abschnitts mit den technischen Informationen sehen Sie das Wort STOP, eine Fehlernummer und eine Parameterliste. Die Fehlernummer hinter dem Wort STOP, wie zum Beispiel in `STOP: 0X00000050`, sollten Sie sich aufschreiben.
- **Treiberinformationen** Direkt hinter der Zeile mit der STOP-Fehlernummer folgt eine Zeile mit dem Namen des Treibers, der den Fehler verursacht hat. Allerdings wird diese Angabe nur gemacht, wenn der Fehler auf einen bestimmten Treiber zurückverfolgt werden kann. Notieren Sie sich den Namen des Treibers.

Wenn das System so eingestellt ist, dass es STOP-Fehler ins Ereignisprotokoll einträgt, und dieser Eintrag vor dem völligen Absturz des Systems noch erfolgen kann, werden die Fehlernummer und die Fehlerparameter ins Systemprotokoll eingetragen, wobei *Save Dump* die Ereignisquelle ist. Der Ereigniseintrag gibt auch an, ob eine Absturzspeicherabbilddatei erstellt und wo sie gespeichert wurde.

PRAXISTIPP Windows 8 enthält eine Online-Absturzanalysefunktion, die es ermöglicht, die Absturzspeicherabbilddatei an den Microsoft-Produktsupport zu senden. Wenn die Fehlerberichterstattung aktiviert ist, können Sie diese Debuginformationen nach dem nächsten erfolgreichen Start des Systems an Microsoft übermitteln. Sie haben die Wahl, die Debuginformationen anonym zu übertragen oder Ihr Microsoft Connect-Konto anzugeben. Wenn Sie die Debuginformationen mit Ihrem Namen und Kontaktinformationen über Microsoft Connect übermitteln, versucht vielleicht ein Techniker, weitere Informationen von Ihnen zu erhalten. Vielleicht kann er Ihnen auch entsprechende Vorschläge zur Behebung des Problems machen.

Nachdem Sie die STOP-Fehlerinformationen aufgeschrieben haben, müssen Sie das System vielleicht im abgesicherten Modus neu starten, wie im Abschnitt »Reparieren eines Computers, um den Systemstart zu ermöglichen« weiter oben in diesem Kapitel beschrieben. Dann können Sie auf folgende Weise versuchen, das Problem zu lösen:

- **Suchen Sie in der Microsoft Knowledge Base eine Beschreibung des STOP-Fehlers** Besuchen Sie *support.microsoft.com* und suchen Sie in der Microsoft Knowledge Base nach der Fehlernummer als Schlüsselwort. Wenn mit der Fehlernummer ein bestimmtes Problem bezeichnet ist, sollten Sie einen entsprechenden Knowledge Base-Artikel finden. Orientieren Sie sich an der Beschreibung, um das Problem zu lösen.
- **Überprüfen Sie den Treiber (sofern Angaben über den Treiber gemacht wurden)** Wenn Sie das System neu starten, überprüfen Sie, ob der Treiber digital signiert ist. Wurde der Treiber vor Kurzem aktualisiert, könnten Sie in Erwägung ziehen, die Vorgängerversion wiederherzustellen. Dass der Treiber als Fehlerquelle genannt wird, bedeutet aber nicht, dass der Treiber tatsächlich fehlerhaft ist und ersetzt werden muss. Der STOP-Fehler kann auch durch andere Faktoren verursacht worden sein.
- **Überprüfen Sie, was sich in der letzten Zeit geändert hat** STOP-Fehler können durch Hardware und durch Software verursacht werden. Sehen Sie sich alle Programme und die Hardware genau an, die in der letzten Zeit im Computer installiert wurden. Wenn Sie neue Hardware installieren, dann achten Sie darauf, dass die Hardware richtig installiert ist, die neusten Treiber installiert sind und alles korrekt konfiguriert ist. Wenn Sie neue Software installieren, dann achten Sie darauf, dass die Installation erfolgreich abgeschlossen wird. Überprüfen Sie auch, ob es Updates oder Patches für die Software gibt.
- **Überprüfen Sie die Systemressourcen** STOP-Fehler können auftreten, wenn das System unter Speichermangel leidet, sei es im Arbeitsspeicher oder auf der Festplatte. Überprüfen Sie nach dem Start des Computers, ob auf den Laufwerken genügend Platz frei ist. Schaffen Sie bei Bedarf mit der Datenträgerbereinigung oder anderen Programmen Platz auf dem Datenträger. Öffnen Sie auch den Task-Manager, indem Sie STRG+ALT+ENTF drücken und dann auf *Task-Manager* tippen oder klicken. Überprüfen Sie auf der Registerkarte *Leistung*, wie viel Speicher frei ist. Wenn nur wenig Speicher verfügbar ist, überprüfen Sie, welche Programme so viel Speicher belegen. Überprüfen Sie auch, ob problematische Programme laufen, beispielsweise Adware oder Spyware.
- **Reparieren Sie die Systemdateien** STOP-Fehler können ihre Ursache auch in beschädigten Systemdateien oder darin haben, dass die falschen Versionen der Systemdateien verwendet werden. Wenn Sie eine Systemdatei als Ursache vermuten und sich das System nicht richtig starten lässt, müssen Sie das Betriebssystem vielleicht wiederherstellen, wie im Abschnitt »Reparieren eines Computers, um den Systemstart zu ermöglichen« weiter oben in diesem Kapitel beschrieben.

- **Überprüfen Sie Hardware und Firmware** STOP-Fehler können durch defekte Hardware verursacht werden. Stürzt ein Computer häufig ab, sollten Sie die Hardware genauer untersuchen. Überprüfen Sie zuerst die Hardwaredreiber, denn ein Treiber könnte Ursache der STOP-Fehler sein. Überprüfen Sie die Geräte. Sehen Sie sich insbesondere die Festplatten, das RAM, den Prozessor und die Grafikkarte genauer an. Eine Festplatte kann ausfallen, RAM kann Defekte haben, der Prozessor kann durch Überhitzung beschädigt werden und die Grafikkarte ist vielleicht zu Windows 8 inkompatibel. Überprüfen Sie auch die Firmware und ihre Einstellungen. Überprüfen Sie außerdem, ob vom Hersteller des Mainboards ein Update erhältlich ist.

Kapitel 11

Arbeiten mit TPM und BitLocker-Laufwerkverschlüsselung

In diesem Kapitel:

Einrichten von TPM	390
BitLocker-Laufwerkverschlüsselung: Grundlagen	402
Verwalten der BitLocker-Laufwerkverschlüsselung	412

Viele Sicherheitsfunktionen, die in das Betriebssystem Windows 8 eingebaut sind, dienen dazu, den Computer vor Angriffen von Personen zu schützen, die über ein Netzwerk oder aus dem Internet auf den Computer zugreifen wollen. Aber was ist, wenn jemand direkten Zugriff auf einen Computer oder Ihre Daten hat? In solchen Fällen greifen die Sicherheitsmechanismen von Windows nicht. Gelingt es jemandem, einen Computer zu starten (das kann auch unter einem anderen Betriebssystem sein, das er selbst installiert hat), kann er sich Zugriff auf alle Daten verschaffen, die auf dem Computer gespeichert sind. Im schlimmsten Fall sind dies streng vertrauliche Daten Ihrer Organisation. Weil außerdem USB-Flashlaufwerke weit verbreitet sind, tragen Benutzer ihre Daten oft mit sich herum. Wenn sie ein solches USB-Flashlaufwerk dann verlieren, sind die Daten meist völlig ungeschützt und jeder, der den USB-Stick findet, kann sie problemlos lesen und auswerten.

Um Computer und Daten in solchen Fällen zu schützen, bietet Windows 8 die BitLocker-Laufwerkverschlüsselung, BitLocker To Go und die Trusted Platform Module-Dienste. Durch die Kombination dieser Funktionen werden nicht nur der Computer, sondern auch Daten geschützt, die auf USB-Flashlaufwerken gespeichert sind. Die BitLocker-Laufwerkverschlüsselung ist eine Technik, die das ganze Volume verschlüsselt. BitLocker To Go ist eine Verschlüsselungstechnik für USB-Flashlaufwerke. Sie können TPM (Trusted Platform Module) mit der BitLocker-Laufwerkverschlüsselung kombinieren, um die Sicherheit zu erhöhen.

Einrichten von TPM

Nur wenn ein Windows 8-Computer mit einem kompatiblen TPM (Trusted Platform Module) und kompatibler Firmware ausgestattet ist, kann er die TPM-Dienste nutzen. Windows 8 unterstützt TPM Version 1.2 oder neuer und benötigt eine TCG-kompatible (Trusted Computing Group) Firmware. TCG-kompatible Firmware unterstützt die von der TCG definierte »Static Root of Trust Measurement« (SRTM), womit Eingriffe beim Startvorgang erkannt werden können. Bei manchen Konfigurationen von TPM und BitLocker-Laufwerkverschlüsselung müssen Sie außerdem sicherstellen, dass die Firmware das Lesen von USB-Flashlaufwerken beim Systemstart ermöglicht.

TPM: Die Grundlagen

Windows 8 bringt das verschlüsselnde Dateisystem (Encrypting File System, EFS) zum Verschlüsseln von Dateien und Ordnern mit. Damit können die Benutzer vertrauliche Daten schützen und der Zugriff darauf ist dann nur mit dem Schlüssel aus dem Zertifikat des jeweiligen Benutzers möglich. Verschlüsselungszertifikate sind als Daten im Profil eines Benutzers gespeichert. Solange Benutzer Zugriff auf ihr Profil und den darin gespeicherten Verschlüsselungsschlüssel haben, können sie auf ihre verschlüsselten Dateien zugreifen.

EFS sorgt zwar für sehr sicheren Schutz der Daten, lässt sich aber aushebeln, wenn ein Angreifer direkten Zugang zum Computer hat. Wenn ein Benutzer seinen Computer irgendwo vergisst, der Computer gestohlen wird oder ein Angreifer es schafft, sich heimlich am Computer anzumelden, schützt EFS die Daten unter Umständen nicht, weil der Angreifer versuchen kann, Zugriff auf den Computer zu erhalten, bevor das Betriebssystem startet. Dann kann er von einem anderen Betriebssystem aus auf die Festplatte zugreifen und die Konfiguration des Computers ändern. Möglicherweise gelingt es ihm dann, sich in ein Anmeldekonto auf dem ursprünglichen Betriebssystem einzuhacken und sich als der echte Benutzer anzumelden oder den Computer so zu konfigurieren, dass er sich als lokaler Administrator anmelden kann. Auf jeden Fall ist es dem Angreifer wahrscheinlich möglich, sich irgendwann vollständigen Zugriff auf einen Computer und seine Daten zu verschaffen.

Um einen Computer gegen direkte Angriffe abzusichern und eine zusätzliche Schutzschicht bereitzustellen, bietet Windows 8 die Trusted Platform Module-Dienste (TPM). Die TPM-Dienste schützen einen Computer mit einer speziellen Hardwarekomponente, dem *Trusted Platform Module*. Ein solches TPM ist ein Mikrochip, der normalerweise auf dem Mainboard eines Computers integriert ist, wo er über einen Hardwarebus mit dem übrigen System kommuniziert. Windows 8-Computer können mit einem TPM erweiterten Schutz für Daten bieten, sicherstellen, dass die Integrität der Startdateien gewährleistet ist, und überprüfen, ob die Festplatte manipuliert wurde, während das Betriebssystem ausgeschaltet war.

Ein TPM ist in der Lage, kryptografische Schlüssel zu generieren und sie so zu verschlüsseln, dass sie nur vom TPM selbst wieder entschlüsselt werden können. Dieser Prozess, der als *Wrapping* (»Kapselung«) oder *Bindung* bezeichnet wird, schützt vor einem Ausspähen des Schlüssels. Ein TPM hat einen Masterschlüssel, der als SRK (Storage Root Key) bezeichnet wird. Der SRK wird innerhalb des TPM gespeichert, um sicherzustellen, dass der geheime Teil des Schlüssels geheim bleibt.

Computer, in denen ein TPM eingebaut ist, können einen Schlüssel generieren, der nicht nur gekapselt, sondern auch versiegelt ist. Der Versiegelungsprozess sorgt dafür, dass der Schlüssel mit ganz bestimmten Plattformparametern verknüpft ist und nur entkapselt werden kann, wenn diese Plattformparameter dieselben Werte haben wie zu dem Zeitpunkt, als der Schlüssel erstellt wurde. Dies ist der Grund, warum Computer, die über ein TPM verfügen, besser gegen Angriffe geschützt sind.

Weil das TPM die geheimen Teile der Schlüsselpaare getrennt von dem Speicher verwaltet, der vom Betriebssystem kontrolliert wird, können die Schlüssel für das TPM versiegelt werden. Auf diese Weise lässt sich praktisch absolute Sicherheit bezüglich des Status eines Systems und seiner Vertrauenswürdigkeit erreichen. TPM-Schlüssel werden nur dann entsiegelt, wenn die Integrität des Systems intakt ist. Weil das TPM seine eigene interne Firmware und Schaltkreise zum Verarbeiten von Anweisungen benutzt, greift es nicht auf das Betriebssystem zurück. Es ist daher keiner Gefährdung durch Sicherheitslücken in externer Software ausgesetzt.

Das TPM kann auch benutzt werden, um Daten zu versiegeln und zu entsiegeln, die außerhalb des TPM generiert werden. Hier offenbart sich die ganze Leistungsfähigkeit des TPM. In Windows 8 trägt die Funktion, die auf ein TPM zugreift und mit seiner Hilfe einen Computer versiegelt, den Namen BitLocker-Laufwerkverschlüsselung. Die BitLocker-Laufwerkverschlüsselung kann nicht nur in TPM-Konfigurationen eingesetzt werden, sondern auch in Computern, die nicht über ein TPM verfügen. Die sicherste Methode besteht aber darin, ein TPM zu benutzen.

Wenn Sie die BitLocker-Laufwerkverschlüsselung und ein TPM nutzen, um den Startmanager und die Startdateien eines Computers zu versiegeln, können diese Komponenten nur dann entsiegelt werden, wenn sie sich nicht verändert haben, seit sie zuletzt versiegelt wurden. Das bedeutet, dass Sie mit dem TPM die Startdateien des Computers in einer Umgebung überprüfen können, die noch vor dem Start des Betriebssystems ausgeführt wird. Wenn Sie eine Festplatte mit dem TPM versiegeln, kann sie nur entsiegelt werden, wenn sich die Daten auf der Festplatte nicht verändert haben, seit die Festplatte zuletzt versiegelt wurde. So ist garantiert, dass eine Festplatte nicht manipuliert wurde, während das Betriebssystem ausgeschaltet war.

Wenn Sie die BitLocker-Laufwerkverschlüsselung einsetzen, aber Startmanager und Startdateien des Computers nicht mit einem TPM versiegeln, kann das TPM nicht benutzt werden, um die Startdateien des Computers vor dem Start des Betriebssystems zu überprüfen. In diesem Fall kann die Integrität des Startmanagers und der Startdateien eines Computers also nicht garantiert werden.

TPM: Verwaltung und Richtlinien

Windows 8 stellt mehrere Tools für die Arbeit mit einem TPM zur Verfügung. Die wichtigsten sind:

- **TPM-Verwaltung** Eine Konsole zum Konfigurieren und Verwalten eines TPM. Sie öffnen dieses Tool, indem Sie im *Apps*-Suchfeld **tpm.msc** eingeben und die EINGABETASTE drücken.
- **TPM-Sicherheitshardware verwalten** Ein Assistent zum Erstellen des benötigten TPM-Besitzerkennworts. Sie öffnen dieses Tool, indem Sie im *Apps*-Suchfeld **tpminit** eingeben und die EINGABETASTE drücken.

PRAXISTIPP Der Zugriff auf die TPM-Verwaltungskonsole kann in den Gruppenrichtlinien eingeschränkt werden. Falls Sie die Konsole nicht öffnen können, sollten Sie prüfen, ob ein Gruppenrichtlinienobjekt angewendet wird, das unter *Benutzerkonfiguration\Windows-Komponenten\Microsoft Management Console* Einschränkungen für die Verwaltungskonsole definiert.

Um auf dem lokalen Computer TPM-Verwaltungsarbeiten durchführen zu können, müssen Sie Mitglied der lokalen Gruppe *Administratoren* oder als lokaler Computeradministrator angemeldet sein. In der TPM-Verwaltung können Sie den detaillierten Status des TPM ermitteln. Wenn Sie die TPM-Verwaltung öffnen, ohne vorher das TPM zu aktivieren, erhalten Sie eine entsprechende Fehlermeldung. Sie bekommen auch einen Fehler angezeigt, wenn Sie versuchen, den Assistenten *TPM-Sicherheitshardware verwalten* auszuführen, ohne vorher das TPM einzuschalten.

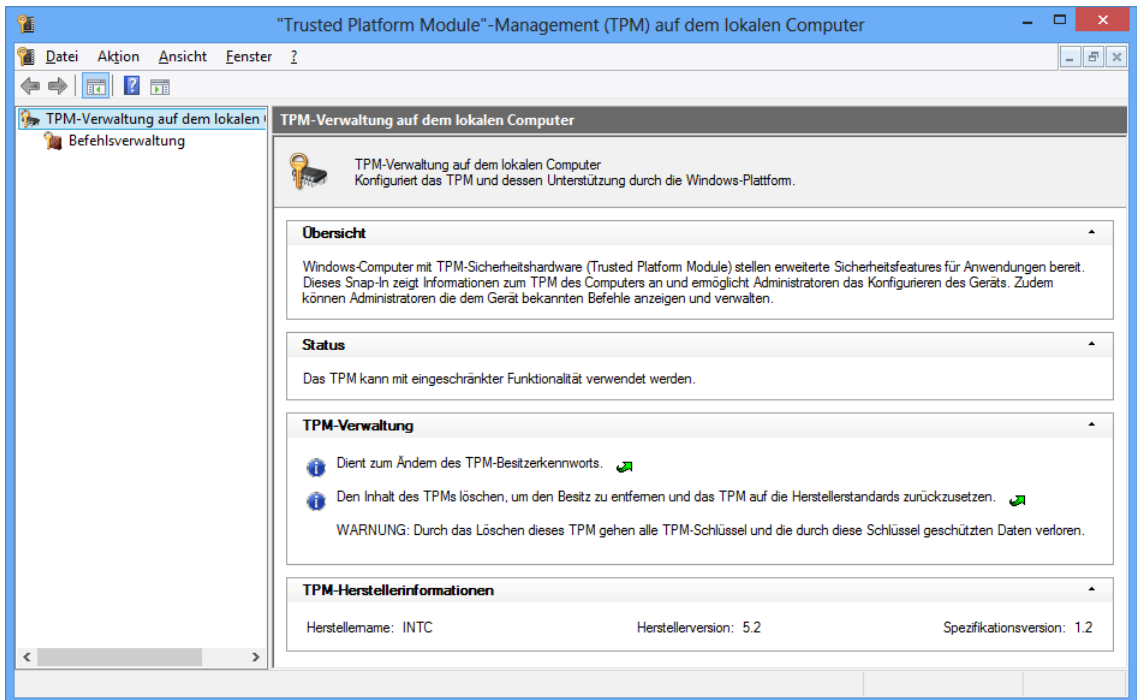


Abbildung 11.1 In der TPM-Verwaltungskonsole initialisieren und verwalten Sie das TPM

Tabelle 11.1 TPM-Statusanzeigen und ihre Bedeutung

Statusanzeige	Bedeutung
Das TPM ist aktiviert, und der Besitz des TPM wurde nicht übernommen	Das TPM ist in der Firmware aktiviert, es wurde aber noch nicht initialisiert.
Das TPM ist aktiviert, und der Besitz des TPM wurde übernommen	Das TPM ist in der Firmware aktiviert und es wurde initialisiert.
Das TPM ist deaktiviert, und der Besitz des TPM wurde nicht übernommen	Das TPM ist in der Software ausgeschaltet, wurde aber noch nicht initialisiert.
Das TPM ist deaktiviert, und der Besitz des TPM wurde übernommen	Das TPM wurde initialisiert, ist aber in der Software ausgeschaltet.

Nur wenn Sie das TPM in der Firmware aktiviert haben, können Sie mit den TPM-Tools arbeiten. Wenn Sie die TPM-Verwaltungskonsole öffnen (Abbildung 11.1), bekommen Sie den TPM-Status und Informationen zum Hersteller des TPM angezeigt. Der TPM-Status gibt den Zustand des TPM an (siehe Tabelle 11.1). In den Informationen zum TPM-Hersteller erfahren Sie, ob das TPM die Version 1.2 oder 2.0 der Spezifikation unterstützt. In Windows 8 brauchen Sie Unterstützung für TPM Version 1.2 oder neuer.

HINWEIS In älteren Windows-Versionen wurde der TPM-Zustand noch genau beschrieben, aber Windows 8 gibt als Zustand gewöhnlich nur *Das TPM ist einsatzbereit* oder *Das TPM ist nicht einsatzbereit* an. Wenn das TPM einsatzbereit ist, wurde es aktiviert und der Besitz des TPM wurde übernommen.

Standardmäßig speichern Windows 8 und Windows Server 2012 die vollständigen Autorisierungsangaben für den TPM-Besitz in der Registrierung des lokalen Computers ab. Diese wichtige Änderung ermöglicht es den Administratoren des lokalen Computers, TPM-Verwaltungsarbeiten durchzuführen, ohne das TPM-Kennwort eingeben zu müssen.

Die Richtlinie *Ebene der TPM-Besitzerautorisierungsinformationen für das Betriebssystem konfigurieren* steuert, in welchem Umfang Autorisierungsinformationen in der Registrierung gespeichert werden. Diese Richtlinien ist in den administrativen Vorlagen der Computerkonfiguration unter *System\Trusted Platform Module-Dienste* zu finden. Diese Richtlinie verfügt über drei Einstellungen:

- **Vollständig** Die vollständige TPM-Besitzerautorisierung, der TPM-Verwaltungsdelegierungs-BLOB und der TPM-Benutzerdelegierungs-BLOB werden in der Registrierung gespeichert. Diese Einstellung ermöglicht die Verwendung des TPM ohne externe oder Remotespeicherung der TPM-Besitzerautorisierung. Beachten Sie, dass Anwendungen auf TPM-Basis, die für ältere Windows-Versionen entwickelt wurden oder auf die TPM-Anti-Hammering-Logik angewiesen sind, vielleicht nicht die vollständige TPM-Besitzerautorisierung in der Registrierung unterstützen.
- **Delegiert** Nur der TPM-Verwaltungsdelegierungs-BLOB und der TPM-Benutzerdelegierungs-BLOB werden in der Registrierung gespeichert. Diese Stufe eignet sich für TPM-Anwendungen, die auf die TPM-Anti-Hammering-Logik angewiesen sind. Wenn Sie diese Einstellung verwenden, empfiehlt Microsoft, dass Sie die TPM-Besitzerautorisierung extern oder remote speichern.
- **Keine** In der Registrierung werden keine TPM-Besitzerautorisierungsdaten gespeichert. Verwenden Sie diese Einstellung, wenn die Kompatibilität zu älteren Windows-Versionen dies erfordert, und für Anwendungen, die auf eine externe oder Remotespeicherung der TPM-Besitzerautorisierung angewiesen sind. Wenn Sie diese Einstellung verwenden, ist eine externe oder Remotespeicherung der TPM-Besitzerautorisierung erforderlich, wie in älteren Windows-Versionen.

ACHTUNG Wenn Sie die Richtlinieneinstellung von *Vollständig* auf *Delegiert* ändern, oder umgekehrt, wird die vollständige TPM-Besitzerautorisierung neu erstellt und alle Kopien der alten TPM-Werte werden ungültig.

Wenn Sie diese Richtlinie auf *Delegiert* oder *Keine* einstellen, werden Sie vor den meisten TPM-Verwaltungsarbeiten zur Eingabe des TPM-Besitzerkennworts aufgefordert (Abbildung 11.2).

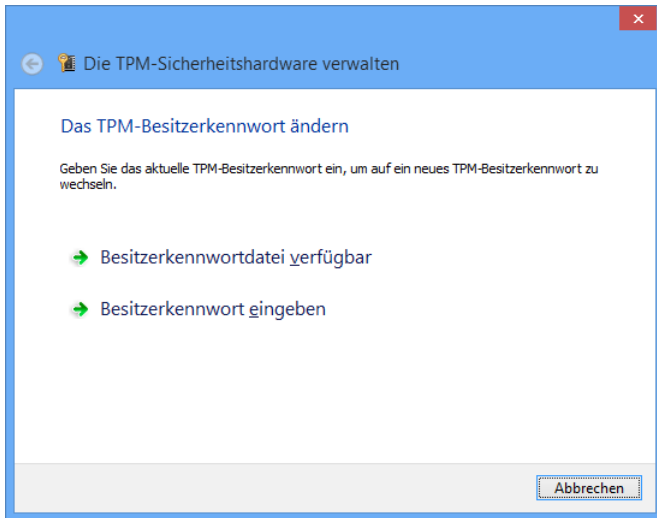


Abbildung 11.2 Geben Sie Ihr TPM-Besitzerkennwort ein, wenn Sie dazu aufgefordert werden

In älteren Windows-Versionen empfahl Microsoft, die TPM-Besitzerautorisierung für Domänencomputer in Active Directory zu speichern. Das ließ sich durch die Aktivierung der Richtlinie *TPM-Sicherung in den Active Directory-Domänendiensten aktivieren*, eine Erweiterung des Verzeichnisschemas und die Einstellung der entsprechenden Zugangskontrolle einrichten.

Die Aktivierung der Sicherung in Active Directory ändert die Art, wie TPM-Besitzinformationen gespeichert werden. Wenn *TPM-Sicherung in den Active Directory-Domänendiensten aktivieren* aktiviert und *Ebene der TPM-Besitzerautorisierungsinformationen für das Betriebssystem konfigurieren* deaktiviert oder nicht konfiguriert ist, werden nur der TPM-Verwaltungsdelegierungs-BLOB und der TPM-Benutzerdelegierungs-BLOB in der Registrierung gespeichert. Um die vollständigen TPM-Besitzinformationen zu speichern, müssen Sie die Einstellung *Vollständig* vornehmen (oder die Sicherung der TPM-Besitzerautorisierung in Active Directory deaktivieren).

Unter *System\Trusted Platform Module-Dienste* sind noch weitere Richtlinien verfügbar:

- *Standardliste der blockierten TPM-Befehle ignorieren*
- *Lokale Liste der blockierten TPM-Befehle ignorieren*
- *Standardbenutzer-Sperrdauer*
- *Standardbenutzer-Sperrschwelle (einzeln)*
- *Standardbenutzer-Sperrschwelle (gesamt)*

Diese Richtlinien steuern die Verwendung der Befehlssperrlisten und die Umstände, unter denen die Hardware nach fehlgeschlagenen Autorisierungen in den Sperrmodus wechselt. Ein Administrator kann alle Parameter, die mit der Sperrung zusammenhängen, in der TPM-Verwaltungskonsolle zurücksetzen.

Tippen oder klicken Sie im Menü *Aktion* auf *TPM-Sperre zurücksetzen*. Wenn die vollständige TPM-Besitzerautorisierung in der Registrierung gespeichert ist, brauchen Sie nicht das TPM-Besitzerkennwort einzugeben. Andernfalls folgen Sie der Anleitung, um das Besitzerkennwort anzugeben oder die Datei auszuwählen, in der das TPM-Besitzerkennwort gespeichert ist.

Aktivieren von TPM

Die Architektur der TPM-Dienste in Windows 8 stellt die grundlegenden Funktionen zur Verfügung, die gebraucht werden, um Computer, die ein TPM eingebaut haben, zu konfigurieren und bereitzustellen. Diese Architektur kann durch ein Feature namens BitLocker-Laufwerkverschlüsselung erweitert werden, das im Abschnitt »BitLocker-Laufwerkverschlüsselung: Grundlagen« weiter unten in diesem Kapitel beschrieben wird.

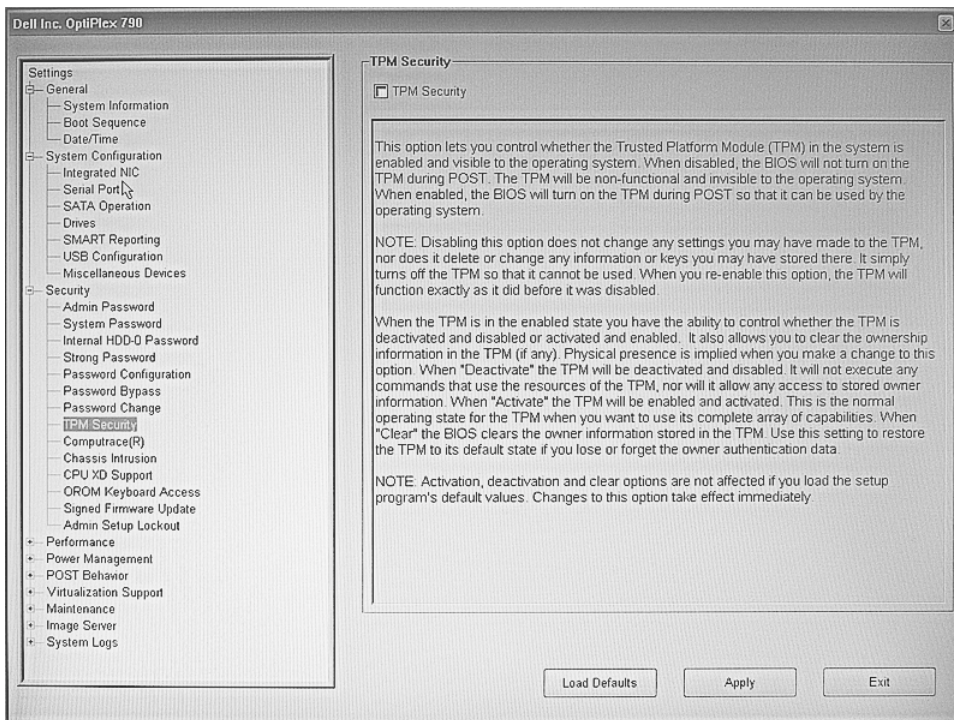


Abbildung 11.3 Aktivieren Sie das TPM in der Firmware

Bevor Sie das TPM benutzen können, müssen Sie es in der Firmware aktivieren. In manchen Fällen ist das TPM bei Computern, die ein TPM eingebaut haben, bereits im Auslieferungszustand aktiviert. Meist ist es aber in der Standardeinstellung deaktiviert. Bei einem meiner Computer musste ich folgende Schritte durchführen:

1. Den Computer starten und dann während des Startvorgangs F2 drücken, um auf die Firmware zuzugreifen. In der Firmware öffnete ich den Bildschirm *Advanced* und dann *Peripheral Configuration*.
2. Auf dem Bildschirm *Peripheral Configuration* war *Trusted Platform Module* als Option aufgeführt. Ich blätterte nach unten, um diese Option zu wählen, und drückte die EINGABETASTE, um ein Optionsmenü anzuzeigen. In diesem Menü wählte ich *Enable*. Zuletzt drückte ich wieder die EINGABETASTE.

3. Ich drückte F10, um die Änderungen an der Einstellung zu speichern und die Firmware zu verlassen. Ich drückte Y, um zu bestätigen, dass ich die Firmwareeinstellungen verlassen wollte. Der Computer startete daraufhin neu.

Auf einem anderen Computer musste ich Folgendes tun:

1. Den Computer starten und dann während des Startvorgangs F2 drücken, um auf die Firmware zuzugreifen. In der Firmware öffnete ich das Menü *Security* und dann den Bildschirm *TPM Security* (Abbildung 11.3).
2. Auf dem Bildschirm *TPM Security* musste ich das Kontrollkästchen *TPM Security* aktivieren und auf *Apply* tippen oder klicken.
3. Ich erhielt eine Meldung, die besagte, dass ich den Computer ausschalten und neu starten müsse, damit sich TPM vollständig aktivieren lässt.
4. Beim Verlassen der Firmware startete der Computer neu.

Anschließend müssen Sie das TPM initialisieren und auf die erste Verwendung vorbereiten. Im Rahmen dieses Vorgangs legen Sie das Besitzerkennwort für das TPM fest. Sobald das TPM aktiviert ist, können Sie die TPM-Konfiguration verwalten.

Initialisieren und Vorbereiten eines TPM für den ersten Einsatz

Indem Sie das TPM initialisieren, konfigurieren Sie es für den ersten Einsatz auf einem Computer, damit Sie die Volumes auf den Festplatten des Computers mit TPM sichern können. Bei diesem Initialisierungsprozess schalten Sie das TPM ein und legen dann den Besitzer des TPM fest. Wenn Sie den Besitz über das TPM übernehmen, weisen Sie ein Kennwort zu. Dadurch wird sichergestellt, dass nur der autorisierte TPM-Besitzer auf das TPM zugreifen und es verwalten kann. Das TPM-Kennwort wird gebraucht, um das TPM auszuschalten, wenn Sie es nicht mehr benutzen wollen, und um das TPM zu löschen, bevor der Computer ausgemustert wird. In einer Active Directory-Domäne können Sie Gruppenrichtlinien konfigurieren, um TPM-Kennwörter zu speichern.

Mit einem Administratorkonto können Sie auf folgende Weise das TPM initialisieren und das Besitzerkennwort festlegen:

1. Starten Sie die TPM-Verwaltungskonsole. Wählen Sie im Menü *Aktion* den Befehl *TPM vorbereiten*, um den Assistenten *TPM-Sicherheitshardware verwalten* (tpmunit) zu starten.

HINWEIS

Falls der Assistent *TPM-Sicherheitshardware verwalten* feststellt, dass die Firmware die Windows-Anforderungen für ein TPM nicht erfüllt, oder gar kein TPM findet, können Sie nicht fortfahren. Überprüfen Sie in diesem Fall, ob das TPM in der Firmware aktiviert ist.

PRAXISTIPP

Wurde das TPM schon vorher initialisiert und dann gelöscht, werden Sie aufgefordert, den Computer neu zu starten. Folgen Sie während des Startvorgangs den angezeigten Anweisungen, um das TPM in der Firmware zurückzusetzen. Der Assistent musste erneut starten, sobald Sie sich das nächste Mal anmelden. Auf meinen Systemen funktionierte das allerdings nicht. Nachdem ich auf *Neu starten* geklickt hatte, musste ich beim nächsten Start F2 drücken, um die Firmware zu öffnen. Dann musste ich das TPM deaktivieren, die Änderungen speichern und die Firmware verlassen. Dadurch wurde ein automatischer Reset ausgelöst. Anschließend musste ich wieder mit F2 die Firmware aufrufen, wo ich nun das TPM aktivieren, die Änderungen speichern und dann die Firmware verlassen konnte. Das löste einen weiteren automatischen Reset aus. Als das Betriebssystem geladen war, meldete ich mich an, woraufhin ich den Assistenten *TPM-Sicherheitshardware verwalten* erneut starten musste.

2. Wenn der Assistent seine ersten Arbeiten abgeschlossen hat, erscheint eine Meldung wie in Abbildung 11.4. Tippen oder klicken auf *Neu starten*, um den Computer neu zu starten.

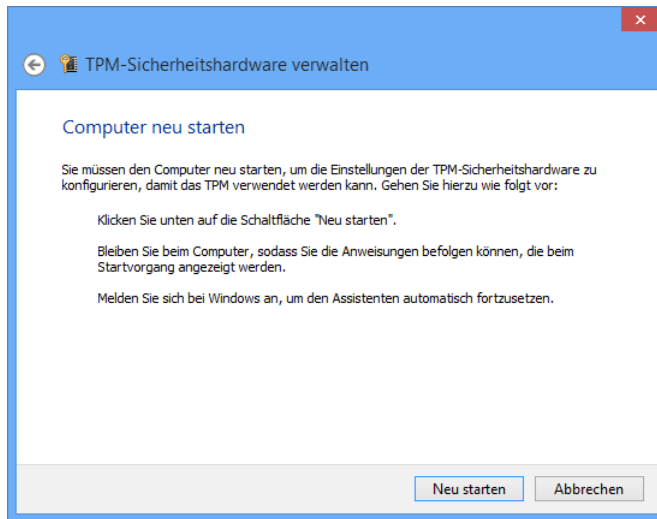


Abbildung 11.4 Nachdem der Assistent Windows auf die Verwendung des TPM vorbereitet hat, müssen Sie den Computer neu starten, damit die TPM-Hardware in der Firmware initialisiert werden kann

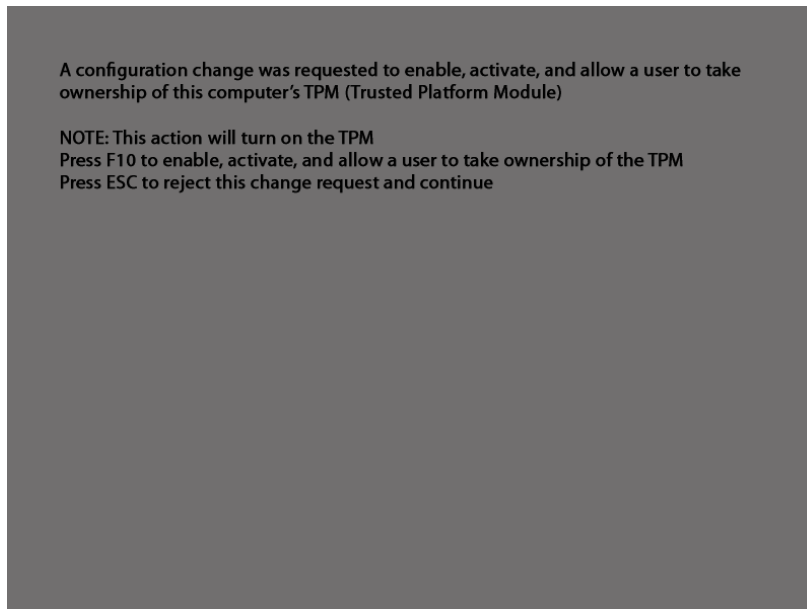


Abbildung 11.5 Bestätigen Sie bei Bedarf die Konfigurationsänderung in der Firmware

3. Hardware, die für Windows 8 und Windows Server 2012 entwickelt wurde, kann die Initialisierung gewöhnlich automatisch abschließen. Bei anderer Hardware brauchen Sie direkten Zugang zum Computer, um auf die Bestätigungsaufforderung der Firmware reagieren zu können. Abbildung 11.5 zeigt

ein Beispiel. In diesem Fall musste ich F10 drücken, um das TPM einzuschalten und zu aktivieren, damit ein Benutzer das TPM in Besitz nehmen kann.

4. Wenn Sie sich nach dem Neustart von Windows wieder angemeldet haben, läuft der Assistent *TPM-Sicherheitshardware verwalten* weiter. Windows übernimmt den Besitz am TPM. Dadurch wird TPM für die Verwendung im Betriebssystem vorbereitet.
5. Nachdem Windows das TPM in Besitz genommen hat, ist TPM einsatzbereit und Sie erhalten eine Bestätigungsmeldung wie in Abbildung 11.6.



Abbildung 11.6 Windows hat das TPM in Besitz genommen und das TPM ist einsatzbereit

6. Bevor Sie auf *Schließen* tippen oder klicken, möchten Sie vielleicht das TPM-Besitzerkennwort speichern. Tippen oder klicken Sie auf *TPM-Besitzerkennwort speichern*. Wählen Sie im Dialogfeld *Speichern* unter einen Speicherort für die Kennwortsicherungsdatei aus und tippen oder klicken Sie auf *Speichern*.
7. Der Status sollte in der TPM-Verwaltungskonsole nun als »*Das TPM ist einsatzbereit*« angegeben werden.

HINWEIS

In der Standardeinstellung wird die Kennwortsicherungsdatei unter dem Namen *<Computernamen>.tpm* gespeichert. Es ist am besten, wenn Sie das TPM-Besitzerkennwort auf einem Wechseldatenträger wie etwa einem USB-Flashlaufwerk speichern und den Wechseldatenträger an einem sicheren Ort aufbewahren. In einer Domäne, in der die Richtlinie *TPM-Sicherung in den Active Directory-Domänendiensten aktivieren* aktiviert ist, wird die Option zur Speicherung des TPM-Kennworts nicht angezeigt. In diesem Fall wird das Kennwort automatisch in Active Directory gespeichert.

WEITERE INFORMATIONEN

Bei der Kennwortsicherungsdatei handelt es sich um eine unverschlüsselte XML-Datei, die in jedem Texteditor geöffnet werden kann, um den Namen des Computers zu überprüfen, zu dem das Kennwort gehört. Im folgenden Beispiel wurde das Kennwort für ENGPC85 erstellt:

```
<?xml version="1.0" encoding="UTF-8"?>
<tpmOwnerData version="1.0" softwareAuthor="Microsoft Windows[Version 6.2.8250]"
  creationDate="2014-04-24T17:19:43-08:00"
  creationUser="ENGPC85\Administrator" machineName="ENGPC85">
  <tpmInfo manufacturerId="1398033696"/>
  <ownerAuth>cBHECAgNV8Z2EBJbERTSD87HJKL=</ownerAuth>
</tpmOwnerData>
```

Ein- und Ausschalten eines initialisierten TPM

Computer, in die ein TPM eingebaut ist, werden gelegentlich mit eingeschaltetem TPM geliefert. Wenn Sie das TPM nicht benutzen möchten, sollten Sie es in Besitz nehmen und dann ausschalten. Dadurch ist sichergestellt, dass sich das Betriebssystem im Besitz des TPM befindet und das TPM inaktiv ist. Auch wenn Sie einen Computer umkonfigurieren oder ausmustern wollen, sollten Sie das TPM löschen und ausschalten. Durch das Löschen werden alle gespeicherten Schlüssel gelöscht. Auf Daten, die mit diesen Schlüsseln verschlüsselt wurden, ist anschließend kein Zugriff mehr möglich.

Mit einem Administratorkonto können Sie das TPM folgendermaßen ausschalten:

1. Starten Sie die TPM-Verwaltungskonsole.
2. Wählen Sie im Menü *Aktion* den Befehl *TPM ausschalten*.
3. Wenn die vollständige TPM-Besitzerautorisierung in der Registrierung gespeichert ist, brauchen Sie kein TPM-Besitzerkennwort anzugeben. Andernfalls folgen Sie den Anweisungen, um das Besitzerkennwort anzugeben oder die Datei auszuwählen, in der es gespeichert ist.

Wenn Sie diese Schritte abgeschlossen haben, um das TPM in der Software auszuschalten, können Sie es jederzeit mit den Schritten wieder einschalten, die im Abschnitt »Initialisieren und Vorbereiten eines TPM für den ersten Einsatz« beschrieben sind.

Löschen des TPM

Wenn Sie das TPM löschen, werden die auf dem TPM gespeicherten Informationen gelöscht und der Besitz des TPMs abgegeben. Sie sollten das TPM löschen, wenn ein mit TPM ausgestatteter Computer ausgemustert werden soll. Durch das Löschen des TPM werden alle gespeicherten Schlüssel ungültig. Auf Daten, die mit diesen Schlüsseln verschlüsselt wurden, ist anschließend kein Zugriff mehr möglich.

Nach dem Löschen des TPM sollten Sie den Besitz am TPM übernehmen. Dadurch werden neue Informationen auf das TPM geschrieben. Anschließend können Sie das TPM ausschalten, damit es nicht mehr verfügbar ist.

Mit einem Administratorkonto können Sie das TPM auf folgende Weise löschen, in Besitz nehmen und ausschalten:

1. Starten Sie die TPM-Verwaltungskonsole. Wählen Sie im Menü *Aktion* den Befehl *TPM löschen*. Daraufhin wird der Assistent *Die TPM-Sicherheitshardware verwalten* gestartet.

ACHTUNG Wenn Sie das TPM löschen, wird es auf den Grundzustand zurückgesetzt. Dabei gehen alle Schlüssel verloren und somit auch alle Daten, die mit diesen Schlüsseln geschützt werden. Das TPM-Besitzerkennwort ist nicht erforderlich, um das TPM zu löschen.

2. Lesen Sie die Warnung auf der Seite *Die TPM-Sicherheitshardware löschen* und tippen oder klicken

Sie auf *Neu starten*, oder tippen oder klicken Sie auf *Abbrechen*, um den Vorgang abubrechen, ohne das TPM zu löschen.

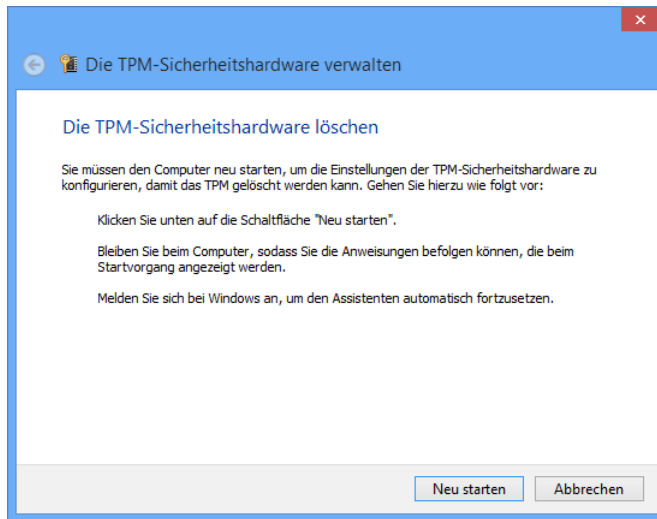


Abbildung 11.7 Tippen oder klicken Sie auf *Neu starten*, um zu bestätigen, dass Sie das TPM löschen möchten

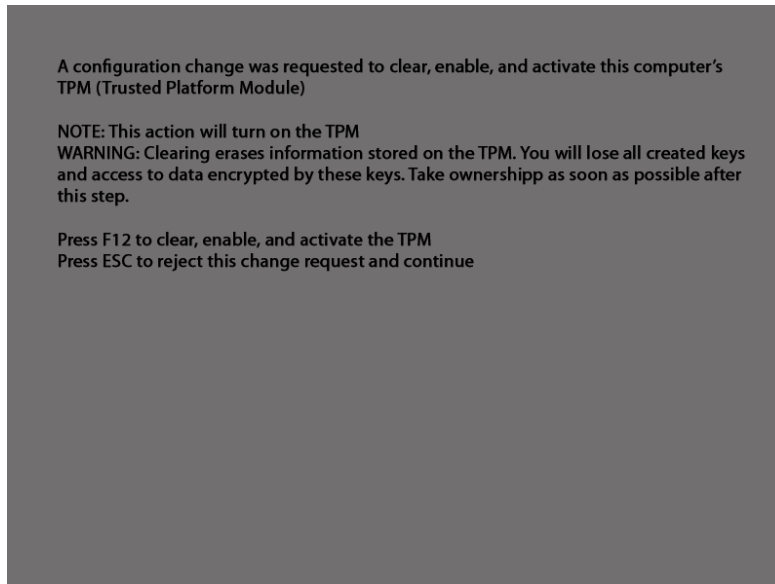


Abbildung 11.8 Bestätigen Sie die Konfigurationsänderung, wenn Sie dazu aufgefordert werden

3. Hardware, die für Windows 8 und Windows Server 2012 entwickelt wurde, kann die erneute Initialisierung gewöhnlich automatisch abschließen. Bei anderer Hardware brauchen Sie direkten Zugang zum Computer, um auf die Bestätigungsaufforderung der Firmware reagieren zu können. Abbildung 11.8 zeigt ein Beispiel. In diesem Fall musste ich F12 drücken, um das TPM zu löschen und zu aktivieren. Mit der ESCAPE-Taste hätte ich den Vorgang auch abbrechen können.

4. Folgen Sie nun den Schritten 4 bis 7 aus dem Abschnitt »Initialisieren und Vorbereiten eines TPM für den ersten Einsatz«.

Ändern des TPM-Besitzerkennworts

Sie können das TPM-Kennwort jederzeit ändern. Der wichtigste Grund, es zu tun, dürfte wohl der Verdacht sein, das TPM-Besitzerkennwort sei bekannt geworden. Vielleicht schreiben auch die Sicherheitsrichtlinien Ihres Arbeitgebers vor, das TPM-Besitzerkennwort in bestimmten Situationen zu ändern.

So ändern Sie das TPM-Besitzerkennwort:

1. Starten Sie die TPM-Verwaltungskonsole. Wählen Sie im Menü *Aktion* den Befehl *Besitzerkennwort ändern*. Daraufhin wird der Assistent *Die TPM-Sicherheitshardware verwalten* gestartet.
2. Wenn die vollständige TPM-Besitzerautorisierung in der Registrierung gespeichert ist, brauchen Sie das TPM-Besitzerkennwort nicht anzugeben. Andernfalls folgen Sie der Anleitung, um das Benutzerkennwort anzugeben oder die Datei auszuwählen, die das Benutzerkennwort enthält.
3. Auf der Seite *Das TPM-Besitzerkennwort erstellen* haben Sie die Wahl, das Kennwort manuell einzugeben oder automatisch erstellen zu lassen (Abbildung 11.9).

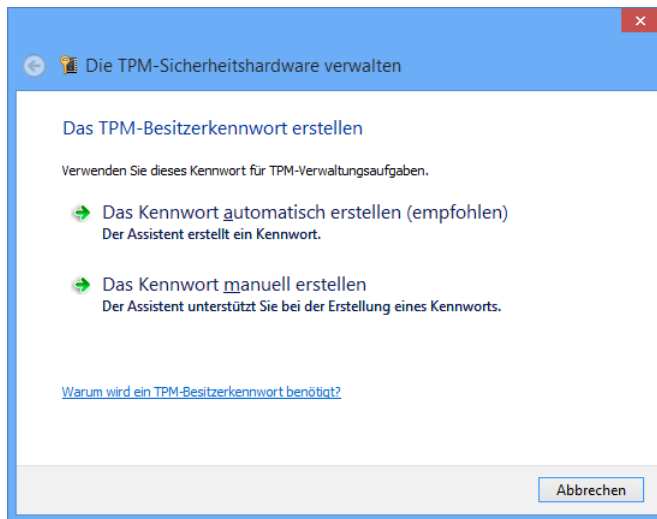


Abbildung 11.9 Erstellen eines neuen Kennworts

4. Wenn Sie möchten, dass der Assistent ein Kennwort für Sie erstellt, klicken Sie auf *Das Kennwort automatisch erstellen (empfohlen)*. Das neue TPM-Besitzerkennwort wird angezeigt. Tippen oder klicken auf *Kennwort ändern*.
5. Wenn Sie das neue Kennwort selbst festlegen möchten, wählen Sie *Das Kennwort manuell erstellen*. Geben Sie ein Kennwort ein, das mindestens acht Zeichen lang ist, und bestätigen Sie es. Tippen oder klicken Sie dann auf *Kennwort ändern*.
6. Bevor Sie auf *Schließen* tippen oder klicken, möchten Sie vielleicht das TPM-Besitzerkennwort speichern. Tippen oder klicken Sie auf *TPM-Besitzerkennwort speichern*. Wählen Sie im Dialogfeld *Speichern unter* einen Speicherort für die Kennwortsicherungsdatei aus und tippen oder klicken Sie auf *Speichern*.

BitLocker-Laufwerkverschlüsselung: Grundlagen

BitLocker ist in allen Editionen von Windows 8 verfügbar und wird in allen Editionen von Windows Server als Feature hinzugefügt. Die BitLocker-Laufwerkverschlüsselung und BitLocker To Go werden zwar oft unter dem gemeinsamen Begriff BitLocker zusammengefasst, sind aber separate, wenn auch ähnliche Funktionen. Die BitLocker-Laufwerkverschlüsselung dient dazu, Daten auf verlorenen, gestohlenen oder schlampig ausgemusterten Computern zu schützen. Es ist eine Verschlüsselungsmethode, die das ganze Volume verschlüsselt. BitLocker To Go wurde dafür entworfen, Daten auf externen Festplatten und USB-Flashlaufwerken zu schützen. Es verschlüsselt virtuelle Volumes. Standard-BitLocker verschlüsselt, indem es das gesamte Volume oder nur den verwendeten Teil des Volumes verschlüsselt. BitLocker To Go erstellt dagegen ein virtuelles Volume auf einem USB-Flashlaufwerk. Dieses virtuelle Volume wird dann mit einem Verschlüsselungsschlüssel verschlüsselt, der auf dem USB-Flashlaufwerk gespeichert ist.

Funktionsweise der BitLocker-Laufwerkverschlüsselung

Hat ein Benutzer direkten Zugriff auf einen Computer ohne BitLocker-Laufwerkverschlüsselung, stehen ihm viele Wege offen, um die vollständige Kontrolle über den Computer zu übernehmen und auf seine Daten zuzugreifen. Dabei ist es egal, ob die Daten mit EFS verschlüsselt sind oder nicht. Ein Benutzer kann den Computer etwa von einer Systemstartdiskette starten und das Administratorkennwort zurücksetzen. Oder der Benutzer installiert und startet ein anderes Betriebssystem und entsperrt dann über dieses Betriebssystem die andere Installation.

Die BitLocker-Laufwerkverschlüsselung verhindert jeglichen Zugriff auf die Laufwerke eines Computers, wenn nichtautorisierte Personen mit dem Computer arbeiten. Dazu kapselt es entweder ganze Laufwerke oder nur die benutzten Bereiche der Laufwerke in einer unangreifbaren Verschlüsselung. Versucht ein nichtautorisierter Benutzer, auf ein mit BitLocker verschlüsseltes Laufwerk zuzugreifen, verhindert die Verschlüsselung, dass dieser Benutzer auf irgendeine Weise die Daten ansehen oder manipulieren kann. Damit wird die Gefahr, dass sich nichtautorisierte Personen im Rahmen eines Offlineangriffs Zugriff auf vertrauliche Daten verschaffen, deutlich verringert.

ACHTUNG

Die BitLocker-Laufwerkverschlüsselung verschlechtert den Datenträgerdurchsatz. Sie ist für Computer gedacht, die sich nicht an einem sicheren Ort befinden und zusätzlichen Schutz erfordern.

Die BitLocker-Laufwerkverschlüsselung kann ein TPM nutzen, um die Integrität der Startmanager- und Startdateien beim Systemstart zu überprüfen und zu garantieren, dass die Festplatte des Computers nicht manipuliert wurde, während das Betriebssystem ausgeschaltet war. Die BitLocker-Laufwerkverschlüsselung speichert auch Parameter der Kernbetriebssystemdateien im TPM.

Jedes Mal, wenn der Computer gestartet wird, überprüft Windows die Startdateien, die Betriebssystemdateien und alle verschlüsselten Volumes, um sicherzustellen, dass sie nicht verändert wurden, während das Betriebssystem ausgeschaltet war. Hat sich etwas an den Dateien geändert, warnt Windows den Benutzer und verweigert die Freigabe des Schlüssels, der für den Zugriff auf Windows nötig ist. Der Computer wechselt daraufhin in den Wiederherstellungsmodus und fordert den Benutzer auf, einen Wiederherstellungsschlüssel bereitzustellen, bevor er den Zugriff auf das Startvolume erlaubt. Der Wiederherstellungsmodus wird auch verwendet, wenn ein mit BitLocker verschlüsseltes Festplattenlaufwerk in ein anderes System eingebaut wird.

Die BitLocker-Laufwerkverschlüsselung kann in Computern mit oder ohne TPM benutzt werden. Hat ein Computer ein TPM eingebaut, greift die BitLocker-Laufwerkverschlüsselung auf das TPM zurück, um den Schutz der Daten zu verbessern und die Integrität der Startdateien sicherzustellen. Die Kombination dieser Komponenten hilft, nichtautorisiertes Auslesen und Zugriff auf Daten zu verhindern. Dazu wird einerseits das ganze Windows-Volumen verschlüsselt, und andererseits werden die Startdateien gegen Manipulation geschützt. Wenn in einem Computer kein TPM eingebaut oder das TPM nicht zu Windows kompatibel ist, kann die BitLocker-Laufwerkverschlüsselung eingesetzt werden, um ganze Volumes zu verschlüsseln und sie auf diese Weise gegen Manipulation zu schützen. Bei dieser Konfiguration geht allerdings der zusätzliche Sicherheitsgewinn durch die Integritätsprüfung der Startdateien verloren.

Auf Computern mit einem kompatiblen und initialisierten TPM benutzt die BitLocker-Laufwerkverschlüsselung gewöhnlich einen der folgenden TPM-Modi:

- **Nur TPM** In diesem Modus wird TPM nur für die Überprüfung eingesetzt. Beim Start des Computers werden unter Einsatz des TPM die Startdateien, die Betriebssystemdateien und alle verschlüsselten Volumes überprüft. Weil der Benutzer keinen zusätzlichen Systemstartschlüssel benötigt, arbeitet dieser Modus für den Benutzer transparent, die Anmeldung verläuft wie gewohnt. Falls das TPM aber fehlt oder der Inhalt von Dateien oder Volumes geändert wurde, schaltet BitLocker in den Wiederherstellungsmodus, wo der Benutzer einen Wiederherstellungsschlüssel oder ein Kennwort braucht, um Zugriff auf das Startvolumen zu erhalten.
- **TPM und PIN** In diesem Modus werden sowohl das TPM als auch ein vom Benutzer eingegebener Zahlenschlüssel für die Überprüfung eingesetzt. Beim Start des Computers werden unter Einsatz des TPM die Startdateien, die Betriebssystemdateien und alle verschlüsselten Volumes überprüft. Der Benutzer muss auf Aufforderung eine PIN eingeben, damit der Systemstart fortgesetzt wird. Weiß der Benutzer die PIN nicht oder gibt er sie falsch ein, schaltet BitLocker in den Wiederherstellungsmodus, statt das Betriebssystem zu starten. Wie im vorherigen Fall schaltet BitLocker auch dann in den Wiederherstellungsmodus, wenn das TPM fehlt oder der Inhalt von Startdateien oder verschlüsselten Volumes geändert wurde.
- **TPM und Systemstartschlüssel** In diesem Modus werden sowohl das TPM als auch ein Systemstartschlüssel für die Überprüfung eingesetzt. Beim Start des Computers werden unter Einsatz des TPM die Startdateien, die Betriebssystemdateien und alle verschlüsselten Volumes überprüft. Der Benutzer braucht ein USB-Flashlaufwerk mit einem Systemstartschlüssel, um sich am Computer anzumelden. Verfügt der Benutzer nicht über den Systemstartschlüssel oder kann er ihn nicht richtig eingeben, schaltet BitLocker in den Wiederherstellungsmodus. Wie im vorherigen Fall schaltet BitLocker auch dann in den Wiederherstellungsmodus, wenn das TPM fehlt oder der Inhalt von Startdateien oder verschlüsselten Volumes geändert wurde.
- **TPM und Smartcard-Zertifikat** In diesem Modus werden das TPM und ein Smartcard-Zertifikat für die Überprüfung eingesetzt. Beim Start des Computers werden unter Einsatz des TPM die Startdateien, die Betriebssystemdateien und alle verschlüsselten Volumes überprüft. Der Benutzer braucht eine Smartcard mit einem gültigen Zertifikat, um sich am Computer anzumelden. Verfügt der Benutzer nicht über eine Smartcard mit gültigem Zertifikat, schaltet BitLocker in den Wiederherstellungsmodus. Wie im vorherigen Fall schaltet BitLocker auch dann in den Wiederherstellungsmodus, wenn das TPM fehlt oder der Inhalt von Startdateien oder verschlüsselten Volumes geändert wurde.

Mit Windows 8 und Windows Server 2012 ermöglicht die Netzwerkentsperrung das automatische Entsperren des Systemvolumens auf Computern, die über ein TPM verfügen, sofern die Computer zur Domäne gehören und mit ihr verbunden sind. Ist dies nicht der Fall, können andere Überprüfungsmethoden verwendet werden, beispielsweise eine Systemstart-PIN.

Auf Computern, die kein TPM haben oder bei denen das TPM inkompatibel ist, lassen sich Windows 8 und Windows Server 2012 so konfigurieren, dass sie für das Betriebssystemlaufwerk ein Entsperrungskennwort verwenden. Dazu müssen Sie in den administrativen Vorlagen der Computerkonfiguration die Richtlinie *Verwendung von Kennwörtern für Betriebssystemlaufwerke konfigurieren* unter *Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Betriebssystemlaufwerke* aktivieren. Für das Entsperrungskennwort können eine maximale Länge und die Kennwortkomplexität festgelegt werden. Die Standardlänge beträgt acht Zeichen. Das bedeutet, dass das Kennwort mindestens acht Zeichen lang sein muss.

Die Komplexitätsanforderungen werden auf folgende Weise überprüft:

- Immer überprüfen, mit der Einstellung *Kennwortkomplexität anfordern*
- Überprüfen, sofern möglich, mit der Einstellung *Kennwortkomplexität zulassen*
- Nicht überprüfen, mit der Einstellung *Kennwortkomplexität nicht zulassen*

Das Entsperrungskennwort wird überprüft, wenn Sie die BitLocker-Laufwerkverschlüsselung aktivieren und das Kennwort festlegen, und wenn ein Benutzer das Kennwort ändert. Wenn die Kennwortkomplexität erforderlich ist, können Sie ein Kennwort nur dann festlegen (und damit auch die Verschlüsselung nur aktivieren), wenn der Computer eine Verbindung zu einem Domänencontroller herstellen und die Komplexität des Kennworts überprüfen kann. Ist die Kennwortkomplexität zugelassen, versucht der Computer, die Komplexität des Kennworts bei seiner Festlegung zu überprüfen, aber er lässt es auch zu, dass Sie fortfahren und die Verschlüsselung aktivieren, wenn keine Domänencontroller verfügbar sind.

Auf Computern ohne ein TPM oder auf Computern, die nicht über kompatible TPMs verfügen, kann die BitLocker-Laufwerkverschlüsselung auch in einem Modus arbeiten, in dem nur ein Systemstartschlüssel verwendet wird, oder in einem Modus, der ein Smartcard-Zertifikat erfordert. Wird nur ein Systemstartschlüssel verwendet, braucht der Benutzer ein USB-Flashlaufwerk, auf dem der Systemstartschlüssel gespeichert ist. Der Benutzer steckt dieses USB-Flashlaufwerk an den Computer an, bevor er ihn einschaltet. Der auf dem Flashlaufwerk gespeicherte Schlüssel entsperrt den Computer.

Wird nur ein Smartcard-Zertifikat verwendet, braucht der Benutzer eine Smartcard mit einem gültigen Zertifikat. Der Benutzer legt die Smartcard ein, wenn er den Computer einschaltet, woraufhin das auf der Smartcard gespeicherte Zertifikat den Computer entsperrt.

Beachten Sie, dass Standardbenutzer die BitLocker-PIN- und das BitLocker-Kennwort für Betriebssystemlaufwerke, fest installierte Datenlaufwerke und Wechseldatenträger ändern können. Das ist eine wichtige Änderung gegenüber Windows 7, wo für diese Aufgaben noch Administratorberechtigungen erforderlich waren. Wenn Sie nicht möchten, dass Standardbenutzer diese Änderungen durchführen können, aktivieren Sie die Richtlinie *PIN- oder Kennwortänderungen durch Standardbenutzer nicht zulassen*. Diese Computerkonfigurationsrichtlinie ist unter *Windows-Komponenten\BitLocker-Laufwerkverschlüsselung\Betriebssystemlaufwerke* zu finden.

An der BitLocker-Laufwerkverschlüsselung wurden etliche wichtige Veränderungen vorgenommen, seit sie erstmals in Windows Vista implementiert wurde. In Windows 7 und höher haben Sie folgende Möglichkeiten:

- **Verschlüsseln von FAT- und NTFS-Volumes** Bisher konnten Sie nur NTFS-Volumes verschlüsseln. Wenn Sie FAT-Volumes verschlüsseln, können Sie auswählen, ob verschlüsselte Volumes auf Computern entsperrt und gelesen werden können, die unter Windows Vista und höher laufen. Diese Option wird über Gruppenrichtlinien konfiguriert. Sie ist aktiviert, wenn Sie BitLocker einschalten. Unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerkverschlüsselung* finden Sie mehrere separate Richtlinien für ältere Windows-Versionen, die es erlauben, FAT-formatierte fest eingebaute Laufwerke und FAT-formatierte Wechseldatenträger zu entsperren und zu lesen.

- **Erlauben, dass ein Daten-Wiederherstellungsagent für die BitLocker-Laufwerkverschlüsselung benutzt wird** Diese Option wird über Gruppenrichtlinien konfiguriert. Der Daten-Wiederherstellungsagent ist in der Lage, ein verschlüsseltes Volume zu entsperren und wiederherzustellen, wenn das persönliche Zertifikat des Wiederherstellungsagenten bereitgestellt oder ein 48-stelliges Wiederherstellungskennwort eingegeben wird. Sie können die Wiederherstellungsinformationen optional auch in Active Directory speichern. Unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen* gibt es getrennte Richtlinien für Betriebssystemvolumes, andere fest eingebaute Laufwerke und Wechseldatenträger.
- **Schreibzugriff auf Wechseldatenträger verhindern, die nicht mit BitLocker geschützt werden** Diese Option wird über Gruppenrichtlinien konfiguriert. Wenn Sie diese Option aktivieren, haben die Benutzer nur schreibgeschützten Zugriff auf unverschlüsselte Wechseldatenträger, aber Lese-/Schreib-Zugriff auf verschlüsselte Wechseldatenträger.

In einer Domäne sind standardmäßig die Domänenadministratoren Daten-Wiederherstellungsagenten. In einer Heimnetzgruppe oder Arbeitsgruppe gibt es standardmäßig keinen Daten-Wiederherstellungsagenten, aber Sie können einen festlegen. Ein Benutzer, den Sie zum Daten-Wiederherstellungsagenten machen wollen, braucht ein persönliches Verschlüsselungszertifikat. Sie können ein solches Zertifikat mit dem Dienstprogramm Cipher generieren und das Zertifikat dann verwenden, um den Daten-Wiederherstellungsagenten in der lokalen Sicherheitsrichtlinie unter *Richtlinien für öffentliche Schlüssel\BitLocker-Laufwerksverschlüsselung* einzutragen.

Windows Vista und Windows 7 unterstützen eine AES-Verschlüsselung mit einem Diffuser. Windows 8 unterstützt diese Verschlüsselung nicht mehr und bietet standardmäßig AES mit einer 128-Bit-Verschlüsselung oder mit 256-Bit-Verschlüsselung, sofern Sie die Richtlinie *Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen* aktivieren und auf *AES-256-Bit* einstellen. Die Verschlüsselungsstärke muss vor dem Einschalten von BitLocker festgelegt werden. Eine nachträgliche Änderung der Verschlüsselungsstärke bleibt ohne Wirkung, wenn das Laufwerk bereits verschlüsselt ist oder die Verschlüsselung bereits erfolgt.

Hardwareverschlüsselung, sicherer Start und Netzwerkentsperrung

Windows 8 und Windows Server 2012 führen eine Reihe von Erweiterungen für BitLocker ein. Die meisten dieser Erweiterungen lassen sich mit den administrativen Vorlagen der Computerkonfiguration unter *Windows-Komponenten\BitLocker-Laufwerkverschlüsselung* steuern und werden in diesem Abschnitt beschrieben.

Windows 8 unterstützt Festplattenlaufwerke mit Hardwareverschlüsselung. Die Verschlüsselung durch spezielle Hardware auf dem Festplattenlaufwerk ist schneller und entlastet den Prozessor des Computers. Verfügt ein Computer über Laufwerke mit Hardwareverschlüsselung, verwendet Windows 8 diese Verschlüsselung für BitLocker.

In den Gruppenrichtlinien können Sie genau festlegen, ob eine Verschlüsselung auf Softwarebasis erfolgen soll, wenn keine Hardwareverschlüsselung verfügbar ist, und ob die Verschlüsselung auf solche Algorithmen und Verschlüsselungsstärken beschränkt wird, die von der Hardware unterstützt werden. Dazu aktivieren Sie die Richtlinie *Verwendung der hardwarebasierten Verschlüsselung für Festplattenlaufwerke konfigurieren* und nehmen die entsprechenden Einstellungen vor. Wenn die Richtlinie aktiviert ist, müssen Sie insbesondere eine softwarebasierte Verschlüsselung zulassen, wenn keine Hardwareverschlüsselung verfügbar ist.

WEITERE INFORMATIONEN

Die Richtlinie *Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen* gilt nicht für eine hardwarebasierte Verschlüsselung. Die Richtlinie *Verwendung der hardwarebasierten Verschlüsselung für Festplattenlaufwerke konfigurieren* unter *Festplattenlaufwerke* legt die gewünschten hardwarebasierten Verschlüsselungsmethoden fest. Mit hardwarebasierter Verschlüsselung wird der Verschlüsselungsalgorithmus bei der Partitionierung des Laufwerks festgelegt.

Vielleicht möchten Sie auch noch die zulässigen Verschlüsselungsarten festlegen. Windows 8 ermöglicht Benutzern die Verschlüsselung ganzer Volumes oder die Verschlüsselung des verwendeten Bereichs. Die Verschlüsselung ganzer Volumes dauert zwar länger, ist aber sicherer, weil das gesamte Volume geschützt wird. Die Verschlüsselung des verwendeten Bereichs schützt nur den Teil des Laufwerks, auf dem Daten gespeichert sind. Standardmäßig lassen sich beide Varianten verwenden. Wenn Sie nur eine dieser beiden Verschlüsselungsarten zulassen möchten, aktivieren Sie die betreffende Laufwerksverschlüsselungstyp-richtlinie. Es gibt separate Richtlinien dieser Art für das Betriebssystem, für fest eingebaute Laufwerke und für Wechseldatenträger.

PRAXISTIPP

In Hochsicherheitsumgebungen empfiehlt es sich, das gesamte Volume zu verschlüsseln. In der Zeit, als dieses Buch entstand, und wenn es nicht bereits geändert wurde oder durch zukünftige Updates oder Service Packs geändert wird, erschienen gelöschte Dateien im freien Speicherbereich, wenn Sie nur den verwendeten Platz verschlüsseln. Folglich lassen sich die Informationen aus den Dateien mit bestimmten Tools wiederherstellen, bis die Dateien überschrieben werden.

Betriebssystemlaufwerke werden als Sonderfall behandelt. Windows 8 ermöglicht es, BitLocker vorab bereitzustellen, damit Sie die Verschlüsselung noch vor der Installation aktivieren können. Außerdem lässt sich Windows 8 so konfigurieren, dass es Folgendes tut:

- **Zusätzliche Authentifizierung beim Start anfordern.** Wenn Sie die entsprechende Richtlinie *Zusätzliche Authentifizierung beim Start anfordern* aktivieren und konfigurieren, ist eine Benutzereingabe erforderlich, selbst wenn der Plattform die Fähigkeit fehlt, Eingaben für die Vorabbereitstellung entgegenzunehmen. Damit auf solch einer Plattform eine USB-Tastatur in der Vor-Startumgebung verwendet werden kann, sollten Sie die Richtlinie *Verwendung der BitLocker-Authentifizierung mit erforderlicher Tastatureingabe vor dem Starten auf Slates aktivieren* auf *Aktiviert* einstellen.
- **Sicheren Start für Integritätsprüfung zulassen.** Der sichere Start wird standardmäßig verwendet, um die Startkonfigurationsdaten (Boot Configuration Data, BCD) entsprechend den TPM-Validierungsprofileinstellungen zu überprüfen. Wenn Sie den sicheren Start verwenden, werden die Einstellungen der Richtlinie *Erweitertes Validierungsprofil für Startkonfigurationsdaten verwenden* ignoriert (sofern Sie nicht den sicheren Start deaktivieren, indem Sie die Richtlinie *Sicheren Start für Integritätsprüfung zulassen* auf *Deaktiviert* stellen).

Die TPM-Validierungsprofileinstellungen sind plattformabhängig. Für Firmware auf BIOS-Basis verwenden Sie die Richtlinie *TPM-Plattformvalidierungsprofil für BIOS-basierte Firmwarekonfigurationen konfigurieren*. Für UEFI-Firmware (Unified Extensible Firmware Interface) verwenden Sie die Richtlinie *TPM-Plattformvalidierungsprofil für systemeigene UEFI-Firmwarekonfigurationen konfigurieren*. Bei der Aktivierung dieser Richtlinie geben Sie genau an, welche Plattformkonfigurationsregister (Platform Configuration Register, PCR) beim Start zur Überprüfung verwendet werden sollen (Abbildung 11.10).

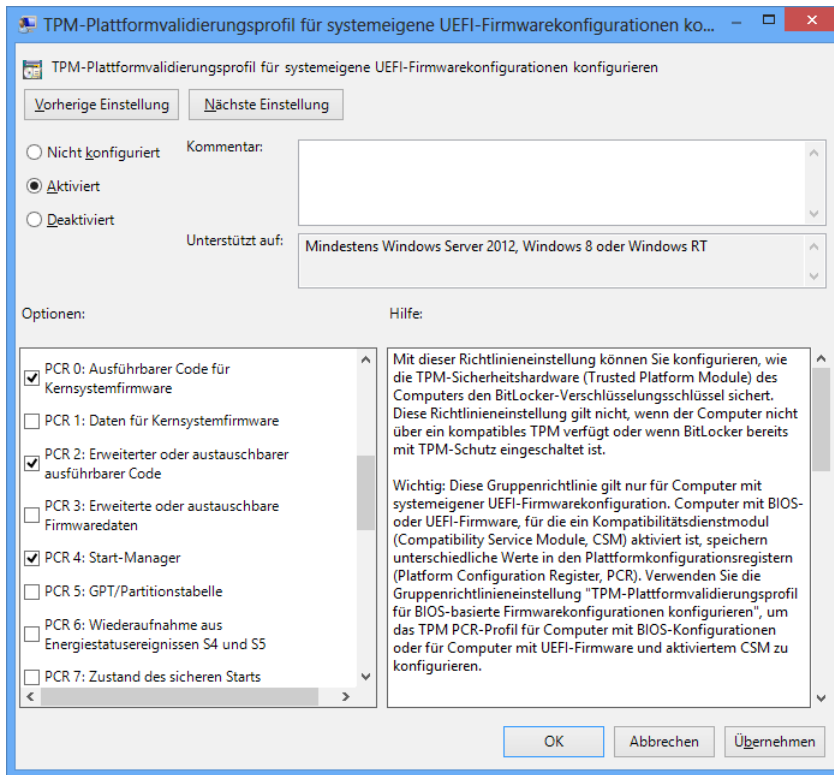


Abbildung 11.10 Auswählen der PCRs für die Überprüfung beim Start

Für BIOS-Firmware empfiehlt Microsoft die Verwendung der PCRs 0, 2, 4, 8, 9, 10, und 11. Für UEFI-Firmware empfiehlt Microsoft die Verwendung der PCRs 0, 2, 4, 7, und 11. In beiden Fällen ist die Einbeziehung von PCR 11 erforderlich, damit der BitLocker-Schutz durchgesetzt werden kann. Die Verwendung von PCR 7 ist erforderlich, um mit UEFI einen sicheren Start verwenden zu können (das müssen Sie durch die Wahl der entsprechenden Option aktivieren).

Wenn Sie einen Computer mit BitLocker schützen, können Sie eine zusätzliche Authentifizierung beim Start anfordern. Normalerweise bedeutet dies, dass der Benutzer einen Systemstartschlüssel auf einem USB-Flashlaufwerk zur Verfügung haben muss, oder eine Systemstart-PIN, oder beides. Die Netzwerkentsperrung bietet diesen zusätzlichen Schutz, ohne vom Benutzer einen Systemstartschlüssel, eine Systemstart-PIN oder beides anzufordern, indem sie das Betriebssystem beim Start des Computers automatisch entsperrt, wenn folgende Voraussetzungen erfüllt sind:

- Der BitLocker-geschützte Computer muss über ein aktiviertes TPM verfügen.
- Der Computer muss sich in einem vertrauenswürdigen Kabelnetzwerk befinden.
- Der Computer muss einer Domäne angehören und mit der Domäne verbunden sein.
- Ein Netzwerkentsperrungsserver mit einem gültigen Netzwerkentsperrungszertifikat ist verfügbar.

Da der Computer einer Domäne angehören und mit ihr verbunden sein muss, damit die Netzwerkentsperrung funktioniert, ist immer noch eine Benutzerauthentifizierung erforderlich, wenn ein Computer nicht mit einer Domäne verbunden ist. Ist er mit einer Domäne verbunden, stellt der Clientcomputer eine Verbindung zu einem Netzwerkentsperrungsserver her, um das Systemlaufwerk zu entsperren. Ge-

wöhnlich handelt es sich bei dem Netzwerkentsperrungsserver um einen Domänencontroller, der so konfiguriert wurde, dass er Netzwerkentsperrungszertifikate verwendet und an Clients sendet. Die Netzwerkentsperrungszertifikate wiederum werden zur Erstellung der Netzwerkentsperrungsschlüssel verwendet.

Sie können einen Domänencontroller so konfigurieren, dass er diese Zertifikate an Clients sendet. Dazu erstellen Sie ein X.509-Zertifikat für den Server, beispielsweise mit Certmsg.mc, und fügen dieses Zertifikat dann mit der Richtlinie *Zertifikat zur Netzwerkentsperrung für BitLocker-Laufwerkverschlüsselung* zu einem Gruppenrichtlinienobjekt hinzu, das für den Domänencontroller gilt. Sie finden diese Richtlinie zur Computerkonfiguration unter *Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel*.

Schließlich ermöglicht es Windows 8 auch, BitLocker während der Bereitstellung des Betriebssystems ebenfalls bereitzustellen. Das können Sie in der Windows-Vorinstallationsumgebung (Windows Pre-installation Environment, Windows PE) tun. Beachten Sie, dass Windows PowerShell ein DISM-Modul enthält, das Sie importieren können. Da dieses Modul bei der Suche nach den Namen von Features keine Platzhalter unterstützt, können Sie sich mit dem Cmdlet *Get-WindowsOptionalFeature* eine Liste der Featurenamen anzeigen lassen, wie im folgenden Beispiel:

```
get-windowsoptionalfeature -online | ft
```

Um BitLocker und die dazugehörigen Verwaltungsprogramme zu installieren, verwenden Sie folgenden Befehl:

```
enable-windowsoptionalfeature -online -featurename bitlocker,bitlocker-utilities,  
bitlocker-networkunlock -all
```

Bereitstellen der BitLocker-Laufwerkverschlüsselung

Wenn Sie in einem Unternehmen die BitLocker-Laufwerkverschlüsselung bereitstellen, ändert sich einiges an der Art und Weise, wie Administratoren und Benutzer mit Computern arbeiten. Bei einem Computer mit BitLocker-Laufwerkverschlüsselung muss der Benutzer gewöhnlich eingreifen, um das Betriebssystem zu starten. Er muss eine PIN eintippen, ein USB-Flashlaufwerk mit dem Systemstartschlüssel anschließen oder eine Smartcard mit einem gültigen Zertifikat einschieben. Wenn Sie die BitLocker-Laufwerkverschlüsselung bereitgestellt haben, können Sie aufgrund dieser Anforderungen nicht mehr sicher sein, dass eine Remoteverwaltung möglich ist, bei der ein Computer neu gestartet werden muss. Sofern Sie keinen direkten Zugriff auf den Computer haben, muss jemand vor Ort verfügbar sein, der die erforderliche PIN eintippt, das USB-Flashlaufwerk mit dem Systemstartschlüssel einsteckt oder die Smartcard mit dem gültigen Zertifikat einschiebt.

Um dieses Problem zu beheben, können Sie in Ihrem vertrauenswürdigen Kabelnetzwerk eine Netzwerkentsperrung einrichten. Bevor Sie die BitLocker-Laufwerkverschlüsselung einsetzen, sollten Sie die Computer Ihrer Organisation sorgfältig analysieren. Sie müssen Pläne und Abläufe für folgende Elemente entwickeln:

- Auswerten der verschiedenen BitLocker-Authentifizierungsmethoden und Anwenden der jeweils geeigneten Methoden
- Feststellen, ob Computer TPM unterstützen und ob somit TPM- oder Nicht-TPM-Konfigurationen für BitLocker verwendet werden müssen
- Speichern, Benutzen und regelmäßiges Ändern von Verschlüsselungsschlüsseln, Wiederherstellungskennwörtern und anderen Überprüfungsmechanismen, die von BitLocker benötigt werden

Sie müssen neue Verfahren für Elemente wie diese entwickeln:

- Ausführen alltäglicher Operationen mit BitLocker-verschlüsselten Laufwerken
- Anbieten von Administrationsupport für BitLocker-verschlüsselte Laufwerke
- Wiederherstellen von Computern mit BitLocker-verschlüsselten Laufwerken

In die Planung dieser Verfahren muss eingehen, auf welche Weise die BitLocker-Verschlüsselung funktioniert und welche Anforderungen bezüglich der Verfügbarkeit von PINs, Systemstartschlüsseln, Smartcards und Wiederherstellungsschlüsseln bestehen, wenn Sie mit BitLocker-verschlüsselten Computern arbeiten. Wenn Sie die Computer Ihrer Organisation analysiert und die grundlegenden Pläne und Verfahren entwickelt haben, müssen Sie einen Konfigurationsplan ausarbeiten, mit dem Sie die BitLocker-Laufwerkverschlüsselung implementieren.

Es stehen mehrere unterschiedliche Implementierungen der BitLocker-Laufwerkverschlüsselung zur Verfügung: die BitLocker-Laufwerkverschlüsselung, die ursprünglich in Windows Vista enthalten war, eine aktualisierte Version aus Windows Server 2008 und Windows 7 und die wiederum aktualisierte Version aus Windows Server 2012 und Windows 8. Computer, die unter Windows 8 und Windows Server 2012 laufen, können mit allen verfügbaren Versionen umgehen. Dagegen können ältere Windows-Versionen unter Umständen nicht die neueste BitLocker-Version nutzen. Es kann beispielsweise erforderlich werden, Gruppenrichtlinien zu konfigurieren, um den Zugriff aus älteren Windows-Versionen heraus zu ermöglichen.

Wenn Sie die BitLocker-Laufwerkverschlüsselung auf dem Laufwerk aktivieren wollen, auf dem das Betriebssystem Windows liegt, muss dieses Laufwerk mindestens zwei Partitionen haben:

- Die erste Partition ist für die BitLocker-Laufwerkverschlüsselung. Diese Partition, die als aktive Partition markiert ist, enthält alle Dateien, die gebraucht werden, um das Betriebssystem zu starten. Sie ist nicht verschlüsselt.
- Die zweite Partition ist die primäre Partition für das Betriebssystem und Ihre Daten. Diese Partition wird verschlüsselt, wenn Sie BitLocker aktivieren.

Bei BitLocker-Implementierungen, die älter als Windows 7 sind, müssen Sie die Partitionen auf ganz bestimmte Weise anlegen, um die Kompatibilität sicherzustellen. Das ist in Windows 7 und höher nicht mehr nötig. Wenn Sie Windows 7 und höher installieren, wird während des Setups automatisch eine zusätzliche Partition erstellt. In der Standardeinstellung wird diese zusätzliche Partition von der Windows-Wiederherstellungsumgebung (Windows RE) benutzt. Wenn Sie allerdings BitLocker auf dem Systemvolume aktivieren, verschiebt Windows die Dateien von Windows RE auf das Systemvolume und nutzt die zusätzliche Partition für BitLocker.

Es ist ganz einfach, BitLocker für eine Festplatte zu benutzen. Auf einem Computer mit kompatibelem TPM müssen Sie erst das TPM initialisieren, wie im Abschnitt »Initialisieren und Vorbereiten eines TPM für den ersten Einsatz« weiter oben in diesem Kapitel beschrieben. Anschließend aktivieren Sie BitLocker. Hat der Computer kein kompatibles TPM, brauchen Sie lediglich BitLocker auf Ihrer Festplatte zu aktivieren.

Lokale Gruppenrichtlinien und Active Directory-Gruppenrichtlinien helfen Ihnen dabei, die Konfiguration von TPM und BitLocker zu verwalten und zu pflegen. Die Gruppenrichtlinieneinstellungen für TPM-Dienste befinden sich im Zweig *Computerkonfiguration/Richtlinien/Administrative Vorlagen/System/Trusted Platform Module-Dienste*, und die Gruppenrichtlinieneinstellungen für BitLocker liegen unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerkverschlüsselung*. Es gibt separate Unterordner für fest eingebaute Datenlaufwerke, Betriebssystemlaufwerke und Wechseldatenträger.

Folgende Richtlinien stehen für Konfigurationsaufgaben zur Verfügung:

- Richtlinien in *Trusted Platform Module*-Dienste
 - Ebene der TPM-Besitzerautorisierungsinformationen für das Betriebssystem konfigurieren
 - Liste der blockierten TPM-Befehle konfigurieren
 - Standardliste der blockierten TPM-Befehle ignorieren
 - Lokale Liste der blockierten TPM-Befehle ignorieren
 - Standardbenutzer-Sperrschwelle (einzeln)
 - Standardbenutzer-Sperrdauer
 - Standardbenutzer-Sperrschwelle (gesamt)
 - TPM-Sicherung in den Active Directory-Domänendiensten aktivieren
- Richtlinien in *BitLocker-Laufwerkverschlüsselung*
 - Standardordner für Wiederherstellungskennwort auswählen
 - Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen
 - Überschreiben des Arbeitsspeichers beim Neustart verhindern
 - Eindeutige IDs für Ihre Organisation angeben
 - Einhaltung der Regel zur Smartcard-Zertifikatverwendung überprüfen
- Richtlinien in *Festplattenlaufwerke*
 - Zugriff auf BitLocker-geschützte Festplattenlaufwerke von früheren Windows-Versionen zulassen
 - Festlegen, wie BitLocker-geschützte Festplattenlaufwerke wiederhergestellt werden können
 - Verwendung der hardwarebasierten Verschlüsselung für Festplattenlaufwerke konfigurieren
 - Kennwortverwendung für Festplattenlaufwerke konfigurieren
 - Smartcard-Verwendung für Festplattenlaufwerke konfigurieren
 - Schreibzugriff auf Festplattenlaufwerke verweigern, die nicht durch BitLocker geschützt sind
 - Laufwerksverschlüsselungstyp auf Festplattenlaufwerken erzwingen
- Richtlinien in *Betriebssystemlaufwerke*
 - Erweiterte PINs für Systemstart zulassen
 - Netzwerkentsperrung beim Start zulassen
 - Sicheren Start für Integritätsprüfung zulassen
 - Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können
 - Minimale PIN-Länge für Systemstart konfigurieren
 - TPM-Plattformvalidierungsprofil für BIOS-basierte Firmwarekonfigurationen konfigurieren
 - TPM-Plattformvalidierungsprofil für systemeigene UEFI-Firmwarekonfigurationen konfigurieren
 - TPM-Plattformvalidierungsprofil konfigurieren (Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2)
 - Verwendung von Kennwörtern für Betriebssystemlaufwerke konfigurieren
 - PIN- oder Kennwortänderungen durch Standardbenutzer nicht zulassen
 - Laufwerksverschlüsselungstyp auf Betriebssystemlaufwerken erzwingen

- *Verwendung der BitLocker-Authentifizierung mit erforderlicher Tastatureingabe vor dem Starten auf Slates aktivieren*
- *Zusätzliche Authentifizierung beim Start anfordern*
- *Plattformvalidierungsdaten nach BitLocker-Wiederherstellung zurücksetzen*
- **Richtlinien in Wechseldatenträger**
 - *Zugriff auf BitLocker-geschützte Wechseldatenträger von früheren Windows-Versionen zulassen*
 - *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können*
 - *Verwendung der hardwarebasierten Verschlüsselung für Wechseldatenträger konfigurieren*
 - *Kennwortverwendung für Wechseldatenträger konfigurieren*
 - *Smartcard-Verwendung für Wechseldatenträger konfigurieren*
 - *Verwendung von BitLocker auf Wechseldatenträgern steuern*
 - *Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind*
 - *Laufwerkverschlüsselungstyp auf Wechseldatenträger erzwingen*

Active Directory enthält TPM- und BitLocker-Wiederherstellungserweiterungen für Computerobjekte. Bei TPM definieren diese Erweiterungen eine einzige Eigenschaft des Computerobjekts, die *ms-TPM-OwnerInformation* heißt. Wenn TPM initialisiert oder das Besitzerkennwort geändert wird, kann der Hash des TPM-Besitzerkennworts als Wert des Attributs *ms-TPM-OwnerInformation* im zugehörigen Computerobjekt gespeichert werden. Bei BitLocker definieren die Erweiterungen Wiederherstellungsobjekte als untergeordnete Objekte von Computerobjekten. Darin werden Wiederherstellungskennwörter gespeichert, die dann mit den jeweiligen BitLocker-verschlüsselten Volumes verknüpft werden.

Standardmäßig speichert Windows 8 die vollständige TPM-Besitzerautorisierung, den TPM-Verwaltungsdelegierungs-BLOB und den TPM-Benutzerdelegierungs-BLOB in der Registrierung. Wegen dieser Änderung brauchen Sie diese Informationen nicht mehr separat von Active Directory einzugeben, wenn Sie Datensicherungen und Wiederherstellungen durchführen. Weitere Informationen finden Sie im Abschnitt »TPM: Verwaltung und Richtlinien« weiter vorne in diesem Kapitel.

Um sicherzustellen, dass TPM- und BitLocker-Wiederherstellungsdaten immer verfügbar sind, sollten Sie die Gruppenrichtlinien so konfigurieren, dass die Wiederherstellungsdaten in Active Directory gespeichert werden.

- Aktivieren Sie die Richtlinie *Festlegen, wie BitLocker-geschützte Festplattenlaufwerke wiederhergestellt werden können* und übernehmen Sie die Standardoptionen, damit Datenwiederherstellungs-Agenten erlaubt sind und die Wiederherstellungsinformationen in Active Directory gespeichert werden.
- Aktivieren Sie die Richtlinie *Festlegen, wie BitLocker-geschützte Betriebssystemlaufwerke wiederhergestellt werden können* und übernehmen Sie die Standardoptionen, damit Datenwiederherstellungs-Agenten erlaubt sind und die Wiederherstellungsdaten in Active Directory gespeichert werden.
- Aktivieren Sie die Richtlinie *Festlegen, wie BitLocker-geschützte Wechseldatenträger wiederhergestellt werden können* und übernehmen Sie die Standardoptionen, damit Datenwiederherstellungs-Agenten erlaubt sind und die Wiederherstellungsdaten in Active Directory gespeichert werden.

PRAXISTIPP Wenn Ihr Unternehmen die FIPS-Anforderungen (Federal Information Processing Standard) erfüllen soll, dürfen Sie keine BitLocker-Wiederherstellungskennwörter generieren oder speichern. Stattdessen müssen Sie Windows so konfigurieren, dass es Wiederherstellungsschlüssel erstellt. Die FIPS-Einstellung finden Sie im Sicherheitsrichtlinieneditor unter *Lokale Richtlinien\Sicherheitsoptionen\Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden*.

Sie konfigurieren BitLocker so, dass es mit Wiederherstellungsschlüsseln arbeitet, indem Sie in lokalen Gruppenrichtlinien oder Active Directory-Gruppenrichtlinien die Richtlinie *Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden* aktivieren. Wenn diese Richtlinie aktiviert ist, können die Benutzer nur Wiederherstellungsschlüssel generieren.

Verwalten der BitLocker-Laufwerkverschlüsselung

Sie können die BitLocker-Laufwerkverschlüsselung sowohl auf Systemvolumes als auch auf Datenvolumes konfigurieren und aktivieren. Wenn Sie Systemvolumes verschlüsseln, müssen Sie den Computer beim Systemstart entsperren. Dazu verwenden Sie gewöhnlich ein TPM und die Netzwerkentsperrung, wenn Sie mit einer Domäne verbunden sind, oder ein TPM, einen Systemstartschlüssel, eine Systemstart-PIN oder eine Kombination dieser drei Elemente. Wenn Sie die strengsten Sicherheitsmechanismen implementieren wollen, sollten Sie alle drei Authentifizierungsmethoden einsetzen.

In der aktuellen Implementierung von BitLocker brauchen Sie das Systemvolume des Computers nicht zu verschlüsseln, bevor Sie eines seiner Datenvolumes verschlüsseln. Wenn Sie verschlüsselte Datenvolumes verwenden, stellt das Betriebssystem BitLocker-Datenvolumes genauso wie jedes andere Volume im Dateisystem bereit, es wird aber ein Kennwort oder eine Smartcard mit gültigem Zertifikat benötigt, um dieses Laufwerk zu entsperren.

Der Verschlüsselungsschlüssel für ein geschütztes Datenvolume wird unabhängig von dem für das Systemvolume und alle anderen geschützten Datenvolumes erstellt und gespeichert. Damit das Betriebssystem verschlüsselte Volumes im Dateisystem bereitstellen kann, wird die Schlüsselkette, die das Datenvolume schützt, in verschlüsseltem Format auf dem Betriebssystemvolume gespeichert. Schaltet das Betriebssystem in den Wiederherstellungsmodus, werden die Datenvolumes erst entsperrt, wenn das Betriebssystem den Wiederherstellungsmodus wieder verlassen hat.

Folgende Schritte sind nötig, um die BitLocker-Laufwerkverschlüsselung einzurichten:

1. Partitionieren der Festplatten des Computers und Installieren des Betriebssystems (sofern Sie einen neuen Computer konfigurieren). Windows-Setup partitioniert die Laufwerke automatisch für Sie. Das Volume, in dem die BitLocker-Daten gespeichert sind, muss aber immer das aktive Systemvolume sein.
2. Initialisieren und Konfigurieren des TPM im Computer (sofern vorhanden)
3. Einschalten des Features *BitLocker-Laufwerkverschlüsselung* (sofern nötig)
4. Überprüfen der Firmware, um sicherzustellen, dass der Computer vom Laufwerk mit der aktiven Systempartition und der Startpartition startet, nicht von einem USB- oder CD/DVD-Laufwerk (nur nötig, wenn Sie Systemvolumes verschlüsseln)
5. Einschalten und Konfigurieren der BitLocker-Laufwerkverschlüsselung

HINWEIS Wenn Sie auf einem Computer, der keiner Domäne angehört, ein Microsoft-Konto verwenden, haben Sie eine zusätzliche Speicheroption. Sie können den Wiederherstellungsschlüssel auf Windows Live SkyDrive speichern. Das SkyDrive-Konto des Benutzers enthält dann einen *BitLocker*-Ordner mit einer separaten Datei für jeden gespeicherten Wiederherstellungsschlüssel.

Sobald Sie die BitLocker-Verschlüsselung eingeschaltet und konfiguriert haben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung, um die Umgebung zu verwalten und eine Wiederherstellung durchzuführen.

Vorbereiten der BitLocker-Laufwerkverschlüsselung

Wie weiter oben beschrieben, kann die BitLocker-Laufwerkverschlüsselung in einem Computer mit oder ohne TPM eingesetzt werden. Bei beiden Konfigurationen sind einige Vorarbeiten nötig, bevor Sie die BitLocker-Laufwerkverschlüsselung einschalten und konfigurieren können.

Bei Windows 8 Pro und Enterprise sollte BitLocker standardmäßig installiert werden. Ist das nicht der Fall, können Sie das Feature *BitLocker-Laufwerkverschlüsselung* mit dem Assistenten *"Features hinzufügen"* installieren. Sie müssen den Computer anschließend neu starten, um den Installationsvorgang abzuschließen.

Ob ein Computer für BitLocker vorbereitet ist, erfahren Sie in der Konsole *BitLocker-Laufwerkverschlüsselung*. Tippen oder klicken in der Systemsteuerung auf *System und Sicherheit* und dann auf *BitLocker-Laufwerkverschlüsselung*. Falls das System nicht richtig konfiguriert ist, bekommen Sie eine Fehlermeldung angezeigt. In einem solchen Fall ist folgende Abhilfe möglich:

- Wenn Sie eine Fehlermeldung bezüglich TPM bekommen, obwohl der Computer mit einem kompatiblen TPM ausgestattet ist, sollten Sie im Abschnitt »Aktivieren von TPM« weiter oben in diesem Kapitel nachlesen, welche Zustände das TPM annehmen kann und wie Sie das TPM in der Firmware aktivieren.
- Wenn Sie eine Fehlermeldung bezüglich TPM auf einem Computer bekommen, der ein inkompatibles TPM oder gar kein TPM hat, müssen Sie die Gruppenrichtlinieneinstellungen des Computers ändern, damit Sie die BitLocker-Laufwerkverschlüsselung auch ohne vorhandenes TPM aktivieren können.

Sie konfigurieren die Richtlinieneinstellungen für die BitLocker-Verschlüsselung in den lokalen Gruppenrichtlinien oder Active Directory-Gruppenrichtlinien. In der Richtlinie für den lokalen Computer wenden Sie die Einstellungen auf das lokale Gruppenrichtlinienobjekt des Computers an. Bei Domänenrichtlinien wenden Sie die Einstellungen dagegen auf ein Gruppenrichtlinienobjekt an, das vom Computer verarbeitet wird. Wenn Sie mit Domänenrichtlinien arbeiten, können Sie auch Anforderungen für Computer mit einem TPM festlegen.

Gehen Sie folgendermaßen vor, um festzulegen, wie BitLocker auf Computern mit oder ohne TPM eingesetzt werden darf:

1. Öffnen Sie das gewünschte Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor.
2. Tippen oder klicken Sie unter *Computerkonfiguration/Richtlinien/Administrative Vorlagen/Windows-Komponenten/BitLocker-Laufwerkverschlüsselung/Betriebssystemlaufwerke* doppelt auf die Einstellung *Zusätzliche Authentifizierung beim Start anfordern*.

WICHTIG

Es gibt mehrere Versionen dieser Richtlinie und sie sind betriebssystemspezifisch. Konfigurieren Sie die Version oder Versionen dieser Richtlinie, die zu Ihrer Arbeitsumgebung und zu den Computern, auf denen die Richtlinien angewendet werden, passt. Die Optionen der Richtlinien unterscheiden sich etwas, weil die TPM-Funktionen auf den Betriebssystemen unterschiedlich unterstützt werden.

3. Definieren Sie die Richtlinieneinstellung im Dialogfeld *Zusätzliche Authentifizierung beim Start anfordern*, indem Sie die Option *Aktiviert* auswählen.

4. Sie haben jetzt folgende Möglichkeiten:
 - Wenn Sie wollen, dass BitLocker benutzt werden kann, auch wenn kein kompatibles TPM vorhanden ist, müssen Sie das Kontrollkästchen *BitLocker ohne kompatibles TPM zulassen* aktivieren. Das ändert die Richtlinieneinstellung so, dass Sie BitLocker-Verschlüsselung mit einem Systemstartschlüssel auf einem Computer einsetzen können, der kein TPM hat.
 - Wenn Sie wollen, dass BitLocker nur eingesetzt werden kann, wenn ein TPM vorhanden ist, müssen Sie das Kontrollkästchen *BitLocker ohne kompatibles TPM zulassen* deaktivieren. Daraufhin wird die Richtlinieneinstellung so geändert, dass Sie die BitLocker-Verschlüsselung nur auf einem Computer mit TPM einsetzen können, wobei Sie eine Systemstart-PIN, einen Systemstartschlüssel oder beides eingeben.
5. Auf einem Computer mit kompatibelem TPM stehen mehrere Authentifizierungsmethoden für den Systemstart zur Auswahl, um zusätzlichen Schutz für die verschlüsselten Daten zur Verfügung zu stellen. Diese Authentifizierungsmethoden können optional oder obligatorisch sein. Anhand von Tabelle 11.2 können Sie einstellen, wie ein TPM mit den verfügbaren Authentifizierungsmethoden kombiniert werden kann. Welche Methoden verfügbar sind, hängt von der verwendeten betriebssystemspezifischen Version der Richtlinie ab.
6. Tippen oder klicken Sie auf OK, um Ihre Einstellungen zu speichern. Diese Richtlinie wird erzwungen, wenn die Gruppenrichtlinien das nächste Mal angewendet werden.
7. Schließen Sie den Gruppenrichtlinienverwaltungs-Editor. Sie können die Gruppenrichtlinien sofort auf den Computer anwenden, an dem Sie angemeldet sind, indem Sie im *Apps*-Suchfeld **gpupdate.exe /force** eingeben und die EINGABETASTE drücken.

Computer, die einen Systemstartschlüssel oder eine Systemstart-PIN haben, verfügen auch über ein Wiederherstellungskennwort oder -zertifikat. Sie brauchen dieses Wiederherstellungskennwort oder -zertifikat in diesen Fällen:

- Es werden Änderungen an den Systemstartdaten vorgenommen.
- Das verschlüsselte Laufwerk muss in einen anderen Computer eingebaut werden.
- Der Benutzer kann den richtigen Systemstartschlüssel oder die richtige PIN nicht eingeben.

Das Wiederherstellungskennwort oder -zertifikat sollte getrennt vom Systemstartschlüssel und der Systemstart-PIN verwaltet und aufbewahrt werden. Benutzer bekommen zwar Systemstartschlüssel oder Systemstart-PIN ausgehändigt, aber nur Administratoren sollten Zugriff auf Wiederherstellungskennwort oder -zertifikat haben. Als Administrator brauchen Sie das Wiederherstellungskennwort oder -zertifikat, um die verschlüsselten Daten auf dem Volume zu entsperren, wenn BitLocker einen Sperrstatus aktiviert. Sofern Sie keinen normalen Daten-Wiederherstellungsagenten benutzen, gilt das Wiederherstellungskennwort oder -zertifikat nur für die eine konkrete BitLocker-Verschlüsselung. Sie können damit also keine verschlüsselten Daten auf irgendeinem anderen BitLocker-verschlüsselten Volume wiederherstellen. Das funktioniert nicht einmal für andere BitLocker-verschlüsselte Volumes auf demselben Computer. Um die Sicherheit zu verbessern, sollten Sie Systemstartschlüssel und Wiederherstellungsdaten getrennt vom Computer lagern.

Wenn BitLocker installiert ist, steht die Konsole *BitLocker-Laufwerkverschlüsselung* in der Systemsteuerung zur Verfügung. Welche Konfigurationsoptionen für BitLocker angeboten werden, hängt davon ab, ob der Computer ein TPM hat und wie Sie die Gruppenrichtlinien konfiguriert haben.

Tabelle 11.2 Wichtige Optionen für den Einsatz eines TPM mit BitLocker

Beim Start des Computers	Einstellung für			
	TPM-Start konfigurieren	TPM-Systemstart-PIN konfigurieren	TPM-Systemstartschlüssel konfigurieren	TPM-Systemstartschlüssel und -PIN konfigurieren
Erlauben, dass TPM beim Systemstart benutzt wird	TPM zulassen	Nicht zulassen	Nicht zulassen	Nicht zulassen
Erzwingen, dass TPM beim Systemstart benutzt wird	TPM erforderlich	Nicht zulassen	Nicht zulassen	Nicht zulassen
Nur TPM mit einem Systemstartschlüssel benutzen	TPM zulassen oder erforderlich	Systemstart-PIN bei TPM zulassen oder erforderlich	Nicht zulassen	Nicht zulassen
Nur TPM mit einer Systemstart-PIN benutzen	TPM zulassen oder erforderlich	Nicht zulassen	Systemstartschlüssel bei TPM zulassen oder erforderlich	Nicht zulassen
Nur TPM mit einem Systemstartschlüssel und einer -PIN benutzen	TPM zulassen oder erforderlich	Nicht zulassen	Nicht zulassen	Systemstartschlüssel und -PIN mit TPM zulassen oder erforderlich
Erlauben, dass TPM mit einer anderen Authentifizierungsmethode kombiniert wird	TPM zulassen oder erforderlich	Systemstart-PIN bei TPM zulassen	Systemstartschlüssel bei TPM zulassen	Systemstartschlüssel und -PIN mit TPM zulassen

Aktivieren von BitLocker auf anderen Volumes als dem Systemvolume

Werden die Daten auf einem Volume verschlüsselt, das nicht das Systemvolume ist, werden alle darauf gespeicherten Daten geschützt. Sie können mit BitLocker jedes Volume verschlüsseln, das mit FAT, FAT32, exFAT oder NTFS formatiert ist. Wie lange es dauert, ein Laufwerk zu verschlüsseln, hängt von der zu verschlüsselnden Datenmenge, der Rechenleistung des Computers und der Auslastung des Computers ab.

Bevor Sie BitLocker aktivieren, sollten Sie in den Gruppenrichtlinien die Richtlinien und Einstellungen unter *Festplattenlaufwerke* konfigurieren und dann warten, bis die Gruppenrichtlinien aktualisiert sind. Wenn Sie das versäumen und BitLocker sofort aktivieren, müssen Sie es unter Umständen aus- und dann wieder einschalten, weil bestimmte Status- und Verwaltungsflags initialisiert werden, wenn Sie es einschalten.

Wenn Sie einen Computer mit mehreren Betriebssystemen haben oder Festplatten zwischen Computern austauschen, kann die Richtlinie *Zugriff auf BitLocker-geschützte Festplattenlaufwerke von früheren Windows-Versionen zulassen* in den Gruppenrichtlinien sicherstellen, dass Sie auch unter anderen Betriebssystemen und auf anderen Computern Zugriff auf das Volume haben. Entsperrte Laufwerke sind schreibgeschützt. Damit Sie ein verschlüsseltes Volume wiederherstellen können, sollten Sie Daten-Wiederherstellungsagenten erlauben und Wiederherstellungsdaten in Active Directory speichern.

Gehen Sie folgendermaßen vor, um die BitLocker-Verschlüsselung auf einem Volume zu aktivieren, das nicht das Systemvolume ist:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf das Datenvolume oder halten Sie es gedrückt, und wählen Sie dann *BitLocker aktivieren*. Bitlocker überprüft, ob Ihr Computer die Voraussetzungen erfüllt, und initialisiert das Laufwerk.

HINWEIS Falls BitLocker bereits aktiviert ist, wird statt des Befehls *BitLocker aktivieren* der Befehl *BitLocker verwalten* angezeigt.

2. Wählen Sie auf der Seite *Methode zum Entsperren des Laufwerks auswählen* (Abbildung 11.11) eine oder mehrere der folgenden Optionen aus und tippen oder klicken Sie auf *Weiter*:
- ***Kennwort zum Entsperren des Laufwerks verwenden*** Aktivieren Sie dieses Kontrollkästchen, wenn der Benutzer aufgefordert werden soll, ein Kennwort einzugeben, um das Laufwerk zu entsperren. Bei der Verwendung von Kennwörtern kann ein Laufwerk überall entsperrt und an andere Leute weitergegeben werden.
 - ***Smartcard zum Entsperren des Laufwerks verwenden*** Aktivieren Sie diese Option, wenn der Benutzer eine Smartcard verwenden und die Smartcard-PIN eintippen muss, um das Laufwerk zu entsperren. Weil dieses Feature ein Smartcardlesegerät voraussetzt, wird es normalerweise eingesetzt, um Laufwerke am Arbeitsplatz zu entsperren, und nicht für Laufwerke, die auch unterwegs benutzt werden.

HINWEIS Wenn Sie auf *Weiter* tippen oder klicken, erstellt der Assistent einen Wiederherstellungsschlüssel. Sie können den Schlüssel verwenden, um das Laufwerk zu entsperren, falls BitLocker eine Bedingung erkennt, die das Entsperren des Laufwerks beim Systemstart verhindert. Diesen Schlüssel sollten Sie auf einem Wechseldatenträger oder einer Netzwerkfreigabe speichern. Sie können den Schlüssel nicht auf dem verschlüsselten Volume oder im Stammverzeichnis eines fest eingebauten Laufwerks speichern.

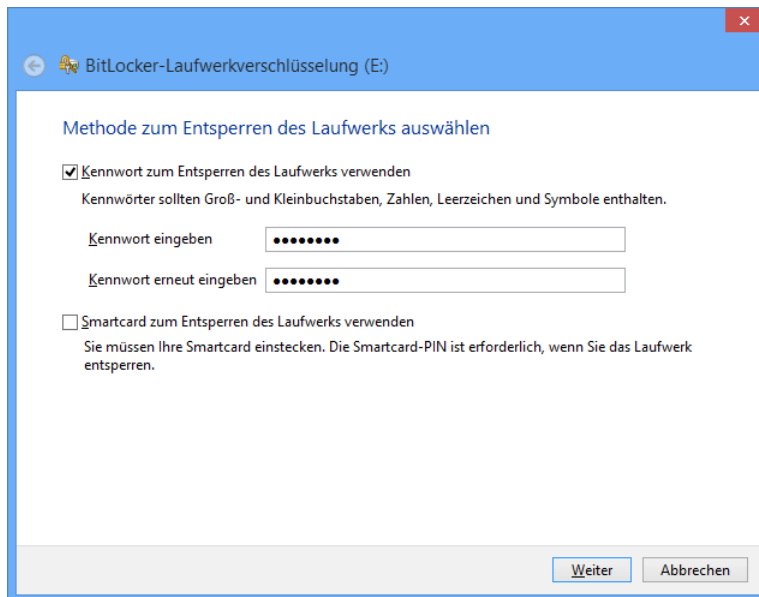
The screenshot shows a Windows dialog box titled "BitLocker-Laufwerkverschlüsselung (E:)" with a blue header bar. Below the title bar, the text "Methode zum Entsperren des Laufwerks auswählen" is displayed. There are two main options, each with a checkbox. The first option, "Kennwort zum Entsperren des Laufwerks verwenden", is checked. Below it, a note says "Kennwörter sollten Groß- und Kleinbuchstaben, Zahlen, Leerzeichen und Symbole enthalten." There are two input fields for the password, both showing seven dots. The second option, "Smartcard zum Entsperren des Laufwerks verwenden", is unchecked. Below it, a note says "Sie müssen Ihre Smartcard einstecken. Die Smartcard-PIN ist erforderlich, wenn Sie das Laufwerk entsperren." At the bottom right of the dialog, there are two buttons: "Weiter" and "Abbrechen".

Abbildung 11.11 Auswählen der Methode zum Entsperren eines Laufwerks

3. Wählen Sie auf der Seite *Wie soll der Wiederherstellungsschlüssel gesichert werden* einen sicheren Speicherort für den Wiederherstellungsschlüssel, vorzugsweise ein USB-Flashlaufwerk oder einen anderen Wechseldatenträger.

4. Sie können nun optional den Wiederherstellungsschlüssel in einem anderen Ordner speichern oder ihn ausdrucken. Tippen oder klicken Sie dazu die jeweilige Option an und folgen Sie den Anweisungen des Assistenten, um den Speicherort für den Wiederherstellungsschlüssel auszuwählen oder den Wiederherstellungsschlüssel auszudrucken. Tippen oder klicken Sie auf *Weiter*, wenn Sie fertig sind.
5. Wenn die Gruppenrichtlinien es zulassen, können Sie nun wählen, ob nur der verwendete Speicherplatz oder das gesamte Laufwerk verschlüsselt wird. Die Verschlüsselung auf den verwendeten Speicherplatz zu beschränken ist schneller als eine Verschlüsselung des gesamten Laufwerks. Außerdem ist dies die empfohlene Option für neue Computer und Laufwerke (außer in Hochsicherheitsumgebungen). Tippen oder klicken auf *Weiter*.
6. Tippen oder klicken Sie auf der Seite *Möchten Sie das Laufwerk jetzt verschlüsseln* auf *Verschlüsselung starten*. Wie lange der Verschlüsselungsvorgang dauert, hängt von der zu verschlüsselnden Datenmenge und anderen Faktoren ab.

Da sich der Verschlüsselungsvorgang anhalten und später fortsetzen lässt, können Sie den Computer herunterfahren, bevor das Laufwerk vollständig verschlüsselt ist. Die Verschlüsselung wird fortgesetzt, wenn Sie den Computer neu starten. Der Verschlüsselungszustand bleibt auch bei einem Stromausfall erhalten.

Aktivieren von BitLocker auf USB-Flashlaufwerken

Wenn Sie USB-Flashlaufwerke verschlüsseln, werden die Daten geschützt, die auf diesem Volume gespeichert sind. Sie können mit BitLocker alle USB-Flashlaufwerke verschlüsseln, die mit FAT, FAT32, exFAT oder NTFS formatiert sind. Wie lange es dauert, ein Laufwerk zu verschlüsseln, hängt von der Größe des Laufwerks, der Rechenleistung des Computers und der Auslastung des Computers ab.

Bevor Sie BitLocker aktivieren, sollten Sie in den Gruppenrichtlinien die Richtlinien und Einstellungen unter *Wechseldatenträger* konfigurieren und dann warten, bis die Gruppenrichtlinien aktualisiert sind. Wenn Sie das versäumen und BitLocker sofort aktivieren, müssen Sie es unter Umständen aus- und dann wieder einschalten, weil bestimmte Status- und Verwaltungsflags initialisiert werden, wenn Sie es einschalten.

Damit Sie ein verschlüsseltes Volume wiederherstellen können, sollten Sie Daten-Wiederherstellungsagenten erlauben und Wiederherstellungsdaten in Active Directory speichern. Wenn Sie ein verschlüsseltes Flashlaufwerk in älteren Windows-Versionen benutzen, stellt die Richtlinie *Zugriff auf BitLocker-geschützte Wechseldatenträger von früheren Windows-Versionen zulassen* sicher, dass Sie auch unter anderen Betriebssystemen und auf anderen Computern Zugriff auf das USB-Flashlaufwerk haben. Laufwerke sind schreibgeschützt, nachdem sie entsperrt wurden. Gehen Sie folgendermaßen vor, um die BitLocker-Verschlüsselung auf einem USB-Flashlaufwerk zu aktivieren:

1. Stecken Sie das USB-Flashlaufwerk ein. Klicken Sie das USB-Flashlaufwerk im Datei-Explorer mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie *Bitlocker aktivieren*. BitLocker überprüft dann, ob Ihr Computer die Voraussetzungen erfüllt, und initialisiert das Laufwerk.
2. Wählen Sie auf der Seite *Methode zum Entsperren des Laufwerks auswählen* eine oder mehrere der folgenden Optionen aus und tippen oder klicken Sie auf *Weiter*:
 - ***Kennwort zum Entsperren des Laufwerks verwenden*** Aktivieren Sie dieses Kontrollkästchen, wenn der Benutzer aufgefordert werden soll, ein Kennwort einzugeben, um das Laufwerk zu entsperren. Bei der Verwendung von Kennwörtern kann ein Laufwerk überall entsperrt und an andere Leute weitergegeben werden.

- **Smartcard zum Entsperren des Laufwerks verwenden** Aktivieren Sie diese Option, wenn der Benutzer eine Smartcard verwenden und die Smartcard-PIN eintippen muss, um das Laufwerk zu entsperren. Weil dieses Feature ein Smartcardlesegerät voraussetzt, wird es normalerweise eingesetzt, um Laufwerke am Arbeitsplatz zu entsperren, und nicht für Laufwerke, die auch unterwegs benutzt werden.
3. Tippen oder klicken Sie auf der Seite *Wie soll der Wiederherstellungsschlüssel gesichert werden auf In Datei speichern*.
 4. Wählen Sie im Dialogfeld *BitLocker-Wiederherstellungsschlüssel speichern* unter den Speicherort aus und tippen oder klicken Sie auf *Speichern*.
 5. Sie haben nun die Gelegenheit, den Wiederherstellungsschlüssel auszudrucken, wenn Sie möchten. Tippen oder klicken Sie auf *Weiter*, wenn Sie fertig sind.
 6. Wenn die Gruppenrichtlinien es zulassen, können Sie nun wählen, ob nur der verwendete Speicherplatz oder das gesamte Laufwerk verschlüsselt wird. Die Verschlüsselung auf den verwendeten Speicherplatz zu beschränken ist schneller als eine Verschlüsselung des gesamten Laufwerks. Außerdem ist dies die empfohlene Option für neue Computer und Laufwerke (außer in Hochsicherheitsumgebungen). Tippen oder klicken auf *Weiter*.
 7. Tippen oder klicken Sie auf der Seite *Möchten Sie das Laufwerk jetzt verschlüsseln* auf *Verschlüsselung starten*. Ziehen Sie das USB-Flashlaufwerk nicht ab, bevor der Verschlüsselungsvorgang abgeschlossen ist. Falls Sie es doch tun möchten, müssen Sie die Verschlüsselung vorher anhalten und später fortsetzen, um die Verschlüsselung abzuschließen. Wie lange der Verschlüsselungsvorgang dauert, hängt von der Größe des Laufwerks und anderen Faktoren ab.

Beim Verschlüsselungsvorgang passiert Folgendes:

1. Die Datei *Autorun.inf*, das BitLocker To Go-Lesetool und eine Datei namens *Liesmich.txt* werden auf das USB-Flashlaufwerk geschrieben.
2. Es wird ein virtuelles Volume mit dem verschlüsselten Inhalt des Laufwerks angelegt.
3. Das virtuelle Volume wird verschlüsselt, um seinen Inhalt zu schützen. Die Verschlüsselung eines USB-Flashlaufwerks dauert etwa 6 bis 10 Minuten pro Gigabyte. Sie können den Verschlüsselungsprozess unterbrechen und fortsetzen, solange Sie das Laufwerk in der Zwischenzeit nicht entfernen.

Wenn die automatische Wiedergabe aktiviert ist und Sie das verschlüsselte Laufwerk auf einem Windows 8-Computer in einen USB-Anschluss einstecken, zeigt Windows 8 auf dem sicheren Desktop eine Benachrichtigung an (Abbildung 11.12). Falls die Benachrichtigung wieder verschwindet, bevor Sie sie antippen oder anklicken können, entfernen Sie das verschlüsselte Laufwerk einfach und stecken es wieder ein.

Laufwerk "F:" entsperren
Dieses Laufwerk ist BitLocker-geschützt.

Abbildung 11.12 Tippen oder klicken Sie auf die Benachrichtigung

Tippen oder klicken Sie auf die Benachrichtigung, um das Dialogfeld *BitLocker* zu öffnen (Abbildung 11.13). Dieses Dialogfeld wird ebenfalls auf dem sicheren Desktop angezeigt.

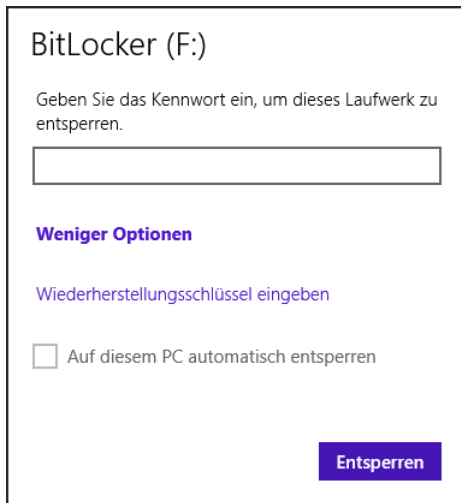


Abbildung 11.13 Entsperren des verschlüsselten Laufwerks

Geben Sie im Dialogfeld *BitLocker* das Kennwort ein, um das Laufwerk zu entsperren. Optional können Sie auf *Weitere Optionen* tippen oder klicken, damit Sie das Kontrollkästchen *Auf diesem PC automatisch entsperren* aktivieren können, um das Kennwort auf dem Systemvolume des Computers in einer verschlüsselten Datei zu speichern. Tippen oder klicken Sie schließlich auf *Entsperren*, um das Laufwerk zu entsperren, damit Sie damit arbeiten können.

Falls Sie das Kennwort für das Laufwerk vergessen oder verlieren, aber noch über den Wiederherstellungsschlüssel verfügen, tippen oder klicken Sie auf *Weitere Optionen* und dann auf *Wiederherstellungsschlüssel eingeben*. Geben Sie den 48-stelligen Wiederherstellungsschlüssel ein und tippen oder klicken Sie dann auf *Entsperren*. Der Schlüssel ist in der XML-formatierten Wiederherstellungsschlüsseldatei als Klartext gespeichert.

Aktivieren von BitLocker auf Systemvolumes

Bevor Sie ein Systemvolume verschlüsseln können, müssen Sie alle startfähigen Medien aus den CD/DVD-Laufwerken des Computers entfernen und alle USB-Flashlaufwerke abziehen. Nun können Sie die BitLocker-Verschlüsselung auf dem Systemvolume folgendermaßen aktivieren:

1. Klicken Sie das Systemvolume im Datei-Explorer mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie *BitLocker aktivieren*. Windows prüft nun den Computer und das Laufwerk, um sicherzustellen, dass es möglich ist, BitLocker zu aktivieren. Tippen oder klicken Sie auf *Weiter*.

HINWEIS Falls BitLocker bereits aktiviert ist, wird statt des Befehls *BitLocker aktivieren* der Befehl *BitLocker verwalten* angezeigt. Im Rahmen des Setups bereitet Windows auch die erforderliche BitLocker-Partition vor. Liegt Windows RE in dieser Partition, verschiebt Windows die Dateien von Windows RE in das Systemvolume und benutzt die frei gewordene Partition für BitLocker.

HINWEIS Falls der Computer nicht über ein TPM verfügt, muss in der Richtlinie *Zusätzliche Authentifizierung beim Start anfordern* für Betriebssystemlaufwerke die Option *BitLocker ohne kompatibles TPM zulassen* aktiviert werden.

2. Wie in Abbildung 11.14 zu sehen, können Sie nun die Systemstarteinstellungen für den BitLocker konfigurieren. Fahren Sie danach fort, wie in den folgenden Anleitungen beschrieben. Wenn der Computer nicht über ein TPM verfügt, sind andere Optionen verfügbar. Sie können ein Kennwort zum Entsperren des Laufwerks erstellen, oder Sie können ein USB-Flashlaufwerk verwenden, um den Systemstartschlüssel zu speichern.

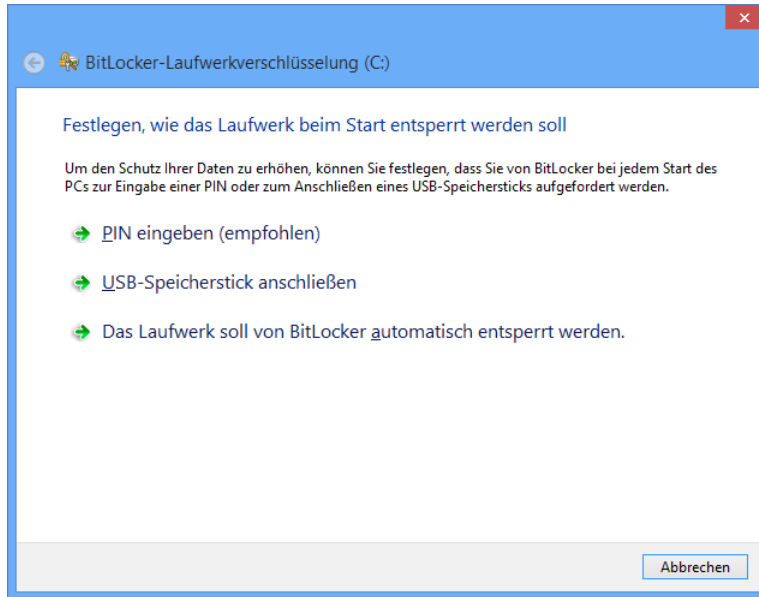


Abbildung 11.14 Konfigurieren der BitLocker-Systemstarteinstellungen

Wenn der Computer über ein TPM verfügt, können Sie BitLocker nutzen, um grundlegende Integritätsprüfungen des Volumes durchzuführen, ohne dass irgendwelche zusätzlichen Schlüssel benötigt werden. In dieser Konfiguration schützt BitLocker das Systemvolume durch Verschlüsselung. Diese Konfiguration hat folgende Merkmale:

- Sie gewährt den Zugriff auf das Volume allen Benutzern, die sich am Betriebssystem anmelden können.
- Sie verhindert, dass Personen, die direkten Zugriff auf den Computer haben, ein anderes Betriebssystem starten, um sich Zugriff auf die Daten des Volumes zu verschaffen.
- Sie ermöglicht es, den Computer mit oder ohne TPM für zusätzliche Systemstartsicherheit zu nutzen.
- Sie erfordert kein Kennwort und keine Smartcard mit einer PIN.

Gehen Sie folgendermaßen vor, um BitLocker ohne zusätzliche Schlüssel zu benutzen:

1. Tippen oder klicken Sie auf der Seite *Festlegen, wie das Laufwerk beim Start entsperrt werden soll* auf *Das Laufwerk soll von BitLocker automatisch entsperrt werden*.
2. Tippen oder klicken Sie auf der Seite *Wie soll der Wiederherstellungsschlüssel gesichert werden* auf *In Datei speichern*.
3. Wählen Sie im Dialogfeld *BitLocker-Wiederherstellungsschlüssel speichern* unter den Speicherort Ihres USB-Flashlaufwerks oder eine geeignete Netzwerkfreigabe aus und tippen oder klicken Sie auf *Speichern*.

4. Sie können nun optional den Wiederherstellungsschlüssel an einem anderen Ort speichern oder ihn ausdrucken. Tippen oder klicken Sie dazu die jeweilige Option an und folgen Sie den Anweisungen des Assistenten, um den Speicherort für den Wiederherstellungsschlüssel auszuwählen oder den Wiederherstellungsschlüssel auszudrucken. Tippen oder klicken Sie auf *Weiter*, wenn Sie fertig sind.
5. Wenn die Gruppenrichtlinien es zulassen, können Sie nun wählen, ob nur der verwendete Speicherplatz oder das gesamte Laufwerk verschlüsselt wird. Die Verschlüsselung auf den verwendeten Speicherplatz zu beschränken ist schneller als eine Verschlüsselung des gesamten Laufwerks. Außerdem ist dies die empfohlene Option für neue Computer und Laufwerke (außer in Hochsicherheitsumgebungen). Tippen oder klicken auf *Weiter*.
6. Tippen oder klicken Sie auf der Seite *Möchten Sie das Laufwerk jetzt verschlüsseln* auf *Verschlüsselung starten*. Wie lange der Verschlüsselungsvorgang dauert, hängt von der zu verschlüsselnden Datenmenge und anderen Faktoren ab.

Um die Sicherheit zu erhöhen, können Sie beim Start zusätzliche Authentifizierung anfordern. Diese Konfiguration weist folgende Merkmale auf:

- Sie gewährt den Zugriff auf das Volume allen Benutzern, die einen gültigen Schlüssel eingeben.
- Sie verhindert, dass Personen, die direkten Zugriff auf den Computer haben, ein anderes Betriebssystem starten, um sich Zugriff auf die Daten des Volumes zu verschaffen.
- Sie ermöglicht es, den Computer mit oder ohne TPM für zusätzliche Systemstartssicherheit zu nutzen.
- Sie erfordert ein Kennwort oder eine Smartcard mit einer PIN.
- Sie verwendet optional die Netzwerkentsperrung, um das Volume zu entsperren, wenn der Computer Mitglied einer Domäne ist und mit der Domäne verbunden ist.

Gehen Sie folgendermaßen vor, um die BitLocker-Verschlüsselung mit einem Systemstartsschlüssel zu kombinieren:

1. Schließen Sie ein USB-Flashlaufwerk an den Computer an (sofern noch nicht vorhanden). Verwenden Sie dabei kein USB-Flashlaufwerk, das BitLocker-verschlüsselt ist.
2. Tippen oder klicken Sie auf der Seite *Festlegen, wie das Laufwerk beim Start entsperrt werden soll* auf die Option *USB-Speicherstick anschließen*.
3. Wählen Sie auf der Seite *Systemstartsschlüssel speichern* Ihr USB-Flashlaufwerk aus und tippen oder klicken Sie auf *Speichern*.
4. Nun müssen Sie den Wiederherstellungsschlüssel speichern. Sie sollten Wiederherstellungsschlüssel und Systemstartsschlüssel nicht auf demselben Datenträger speichern. Entfernen Sie daher das USB-Flashlaufwerk und stecken Sie ein zweites USB-Flashlaufwerk ein.

HINWEIS

Der Systemstartsschlüssel ist etwas anderes als der Wiederherstellungsschlüssel. Wenn Sie einen Systemstartsschlüssel generieren, wird dieser Schlüssel benötigt, um den Computer zu starten. Der Wiederherstellungsschlüssel wird gebraucht, um den Computer zu entsperren, falls BitLocker in den Wiederherstellungsmodus schaltet; das kann passieren, wenn BitLocker erkennt, dass der Computer manipuliert wurde, während das Betriebssystem ausgeschaltet war.

5. Tippen oder klicken Sie auf der Seite *Wie soll der Wiederherstellungsschlüssel gesichert werden* auf *In Datei speichern*.
6. Wählen Sie im Dialogfeld *BitLocker-Wiederherstellungsschlüssel speichern* unter Ihr USB-Flashlaufwerk aus und tippen oder klicken Sie auf *Speichern*. Entfernen Sie das USB-Laufwerk mit dem Wiederherstellungsschlüssel noch nicht.

7. Sie können nun optional den Wiederherstellungsschlüssel in einem freigegebenen Ordner speichern oder ihn ausdrucken. Tippen oder klicken Sie dazu die jeweilige Option an und folgen Sie den Anweisungen des Assistenten, um den Speicherort für den Wiederherstellungsschlüssel auszuwählen oder den Wiederherstellungsschlüssel auszudrucken. Tippen oder klicken Sie auf *Weiter*, wenn Sie fertig sind.
8. Wenn die Gruppenrichtlinien es zulassen, können Sie nun wählen, ob nur der verwendete Speicherplatz oder das gesamte Laufwerk verschlüsselt wird. Die Verschlüsselung auf den verwendeten Speicherplatz zu beschränken ist schneller als eine Verschlüsselung des gesamten Laufwerks. Außerdem ist dies die empfohlene Option für neue Computer und Laufwerke (außer in Hochsicherheitsumgebungen). Tippen oder klicken auf *Weiter*.
9. Stellen Sie auf der Seite *Möchten Sie das Laufwerk jetzt verschlüsseln* sicher, dass das Kontrollkästchen *BitLocker-Systemüberprüfung ausführen* aktiviert ist, und tippen oder klicken Sie auf *Weiter*.
10. Bestätigen Sie, dass Sie den Computer neu starten wollen, indem Sie auf *Jetzt neu starten* tippen oder klicken. Der Computer wird nun neu gestartet und BitLocker stellt sicher, dass der Computer BitLocker-kompatibel und alles für die Verschlüsselung vorbereitet ist. Ist der Computer nicht für die Verschlüsselung bereit, erhalten Sie eine Fehlermeldung. In diesem Fall müssen Sie den Fehler beseitigen, bevor Sie den Vorgang fortsetzen können. Ist der Computer dagegen für die Verschlüsselung bereit, wird die Statuszeile *Verschlüsselung wird durchgeführt* angezeigt. Sie können den Status der Volumeverschlüsselung verfolgen, indem Sie den Mauszeiger im Infobereich der Taskleiste über das Symbol der BitLocker-Laufwerkverschlüsselung stellen. Wenn Sie doppelt auf dieses Symbol tippen oder klicken, können Sie das Dialogfeld *Verschlüsselung* öffnen und den Verschlüsselungsprozess genauer beobachten. Sie haben außerdem die Möglichkeit, den Verschlüsselungsprozess zu unterbrechen. Die Volumeverschlüsselung dauert etwa 1 Minute pro Gigabyte.

Sobald dieser Vorgang abgeschlossen ist, haben Sie das Betriebssystemvolume verschlüsselt und einen Wiederherstellungsschlüssel erstellt, der nur für dieses spezielle Volume gilt. Wenn Sie den Computer das nächste Mal einschalten, muss das USB-Flashlaufwerk mit dem Systemstartschlüssel in einen USB-Anschluss des Computers gesteckt sein oder der Computer muss mit dem Domänennetzwerk verbunden sein und die Netzwerkentsperrung verwenden. Wenn ein USB-Flashlaufwerk für den Start erforderlich ist und Sie haben das USB-Flashlaufwerk mit Ihrem Systemstartschlüssel nicht mehr, müssen Sie den Wiederherstellungsmodus starten und den Wiederherstellungsschlüssel bereitstellen, um Zugriff auf die Daten zu erhalten.

Gehen Sie folgendermaßen vor, um die BitLocker-Verschlüsselung in Kombination mit einer Systemstart-PIN zu aktivieren:

1. Tippen oder klicken Sie auf der Seite *Festlegen, wie das Laufwerk beim Start entsperrt werden soll* auf *PIN eingeben*.
2. Tippen Sie auf der Seite *PIN eingeben* die PIN ein und bestätigen Sie die Nummer durch erneute Eingabe. Als PIN können Sie eine beliebige Zahl wählen, solange sie 4 bis 20 Ziffern enthält. Die PIN wird auf dem Computer gespeichert.
3. Stecken Sie ein USB-Flashlaufwerk ein, auf dem Sie den Wiederherstellungsschlüssel speichern wollen, und tippen oder klicken Sie auf *PIN festlegen*. Verwenden Sie dabei kein USB-Flashlaufwerk, das BitLocker-verschlüsselt ist.

Fahren Sie mit den Schritten 5 bis 10 in der vorherigen Anleitung fort.

Sobald dieser Vorgang abgeschlossen ist, haben Sie das ganze Volume verschlüsselt und einen Wiederherstellungsschlüssel erstellt, der nur für dieses spezielle Volume gilt. Wenn Sie eine PIN oder einen Systemstartschlüssel erstellt haben, müssen Sie die PIN oder den Systemstartschlüssel beim nächsten

Start des Computers verwenden (oder der Computer ist mit einem Domänennetzwerk verbunden und kann die Netzwerkentsperrung verwenden). Davon abgesehen verändert sich die normale Bedienung des Computers nicht. Nur wenn Änderungen am TPM auftreten, der Zugriff auf das TPM nicht möglich ist oder jemand versucht hat, die Festplatte zu verändern, während das Betriebssystem ausgeschaltet war, schaltet der Computer in den Wiederherstellungsmodus, wo Sie den Wiederherstellungsschlüssel brauchen, um den Computer zu entsperren.

Verwalten von BitLocker und Beseitigen von Problemen

Ob ein Systemvolume, ein Datenvolume oder ein angestecktes USB-Flashlaufwerk BitLocker benutzt, stellen Sie fest, indem Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *BitLocker-Laufwerkverschlüsselung* tippen oder klicken. Nun wird der Status von BitLocker für jedes Volume angezeigt (Abbildung 11.15).

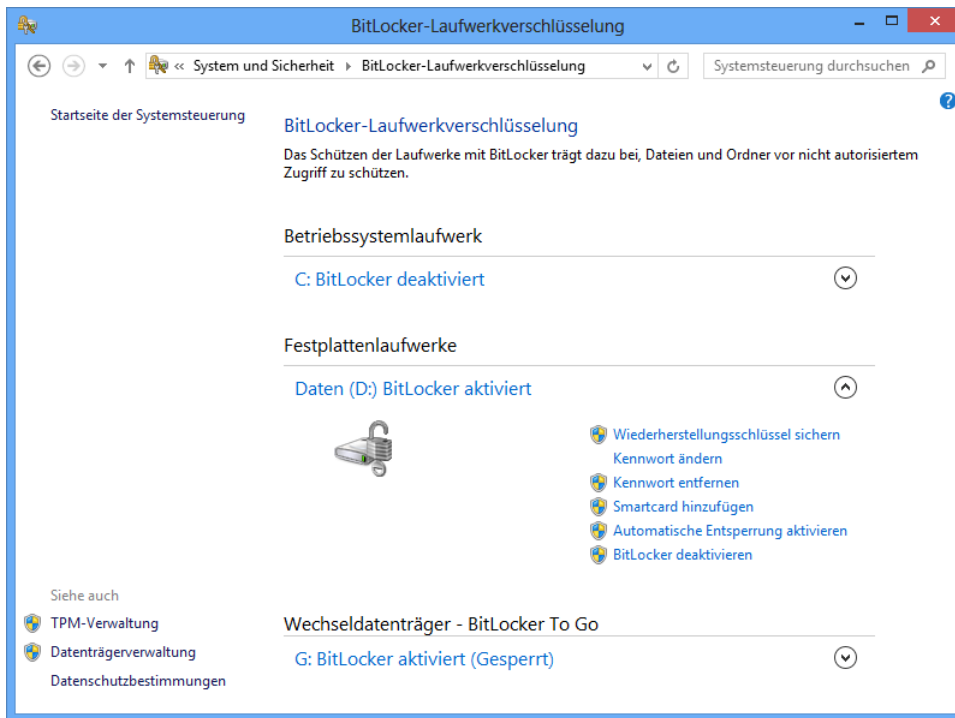


Abbildung 11.15 Überprüfen des aktuellen Status von BitLocker auf jedem Volume

Der Dienst *BitLocker-Laufwerkverschlüsselungsdienst* muss laufen, damit BitLocker einwandfrei funktioniert. Normalerweise ist dieser Dienst mit dem Starttyp *Manuell* konfiguriert und läuft unter dem Konto *SYSTEM*.

Wenn Sie BitLocker zusammen mit Smartcards einsetzen, muss der Dienst *Smartcard* laufen. Dieser Dienst ist normalerweise mit dem Starttyp *Manuell* konfiguriert und läuft unter dem Konto *LOKALER DIENST*.

Wenn Sie einen Systemstartschlüssel oder eine PIN sowie einen Wiederherstellungsschlüssel für einen Computer erstellt haben, können Sie mit den Optionen auf der Seite *BitLocker-Laufwerkverschlüsselung* in der Systemsteuerung bei Bedarf Duplikate von Systemstartschlüssel, Systemstart-PIN oder Wiederherstellungsschlüssel anfertigen, die Sie für die Datensicherung oder als Ersatz brauchen.

HINWEIS

Für fest eingebaute Daten- und Betriebssystemlaufwerke erreichen Sie diese Seite auch, indem Sie das Volume im Datei-Explorer mit der rechten Maustaste anklicken oder gedrückt halten und dann *Bitlocker verwalten* auswählen. Falls BitLocker ausgeschaltet ist, wird stattdessen die Option *Bitlocker aktivieren* angezeigt.

Welche Verwaltungsoptionen zur Verfügung stehen, hängt davon ab, welche Art von Volume Sie bearbeiten und welche Verschlüsselungseinstellungen Sie gewählt haben. Es gibt folgende Optionen:

- **Wiederherstellungsschlüssel sichern** Ermöglicht Ihnen, den Wiederherstellungsschlüssel zu sichern oder auszudrucken. Tippen oder klicken Sie auf diese Option und folgen Sie der Anleitung.
- **Kennwort ändern** Ermöglicht Ihnen die Änderung des Verschlüsselungskennworts. Tippen oder klicken Sie auf diese Option, geben Sie das alte Kennwort ein, geben Sie das neue Kennwort ein und bestätigen Sie es. Tippen oder klicken Sie auf *Kennwort ändern*.
- **Kennwort entfernen** Tippen oder klicken Sie auf diese Option, wenn es nicht mehr nötig sein soll, zum Entsperren des Laufwerks das Verschlüsselungskennwort einzugeben. Das geht allerdings nur, wenn Sie zuvor eine andere Entsperrungsmethode konfiguriert haben.
- **Smartcard hinzufügen** Fügt eine Smartcard zum Entsperren des Laufwerks hinzu. Tippen oder klicken Sie auf diese Option und folgen Sie dann den Anweisungen.
- **Smartcard entfernen** Tippen oder klicken Sie auf diese Option, wenn es nicht mehr nötig sein soll, zum Entsperren des Laufwerks die Smartcard zu verwenden.
- **Smartcard ändern** Ändert die Smartcard, die zum Entsperren des Laufwerks benutzt wird. Tippen oder klicken Sie auf diese Option und folgen Sie dann den Anweisungen.
- **Automatische Entsperrung aktivieren** Tippen oder klicken Sie auf diese Option, damit das Laufwerk künftig automatisch entsperrt wird.
- **Automatische Entsperrung deaktivieren** Tippen oder klicken Sie auf diese Option, um die automatische Entsperrung des Laufwerks auszuschalten.
- **Bitlocker deaktivieren** Tippen oder klicken Sie auf diese Option, um BitLocker zu deaktivieren und das Laufwerk zu entschlüsseln.

Wiederherstellen von Daten, die durch BitLocker-Laufwerkverschlüsselung geschützt werden

Wenn Sie die BitLocker-Laufwerkverschlüsselung eingerichtet haben und der Computer in den Wiederherstellungsmodus schaltet, müssen Sie ihn entsperren. Gehen Sie folgendermaßen vor, um ihn mit einem Wiederherstellungsschlüssel zu entsperren, der auf einem USB-Flashlaufwerk gespeichert ist:

1. Schalten Sie den Computer ein. Wenn der Computer gesperrt ist, wird die Wiederherstellungskonsole für die BitLocker-Laufwerkverschlüsselung geöffnet.
2. Stecken Sie auf Anforderung das USB-Flashlaufwerk ein, auf dem der Wiederherstellungsschlüssel gespeichert ist, und drücken Sie die EINGABETASTE.
3. Der Computer wird nun entsperrt und automatisch neu gestartet. Sie brauchen den Wiederherstellungsschlüssel nicht von Hand einzugeben.

Wenn Sie die Wiederherstellungsschlüsseldatei in einem Ordner auf einem anderen Computer oder auf einem Wechseldatenträger gespeichert haben, können Sie den anderen Computer benutzen, um die Wiederherstellungsschlüsseldatei zu öffnen und auszulesen. Sie finden die richtige Datei, indem Sie in der Wiederherstellungskonsole, die auf dem gesperrten Computer angezeigt wird, die Kennwort-ID suchen und sich diese Nummer notieren. Die Datei mit dem Wiederherstellungsschlüssel verwendet diese Kennwort-ID als Dateinamen. Öffnen Sie die Datei und suchen Sie den Wiederherstellungsschlüssel.

Gehen Sie folgendermaßen vor, um den Computer durch Eintippen des Wiederherstellungsschlüssels zu entsperren:

1. Schalten Sie den Computer ein. Wenn der Computer gesperrt ist, wird die Wiederherstellungskonsole für die BitLocker-Laufwerkverschlüsselung geöffnet.
2. Tippen Sie den Wiederherstellungsschlüssel ein und drücken Sie die EINGABETASTE. Der Computer wird entsperrt und automatisch neu gestartet.

Ein Computer wird beispielsweise gesperrt, wenn ein Benutzer versucht, den Wiederherstellungsschlüssel einzugeben, dabei aber einen Fehler macht. In der Wiederherstellungskonsole können Sie zweimal ESC drücken, um die Wiederherstellungs-Eingabeaufforderung zu verlassen und den Computer auszuschalten. Ein Computer wird auch gesperrt, wenn ein Fehler im Zusammenhang mit dem TPM auftritt oder die Systemstartdateien geändert werden. In diesem Fall bricht der Computer sehr früh im Startprozess ab, noch bevor das Betriebssystem startet. An diesem Punkt ist es unter Umständen noch nicht möglich, die normalen Zahlentasten auf der Tastatur des gesperrten Computers zu verwenden. In so einem Fall müssen Sie die Funktionstasten verwenden, um das Wiederherstellungskennwort einzugeben. Dabei stehen die Funktionstasten F1 bis F9 für die Ziffern 1 bis 9 und die Taste F10 für 0.

Deaktivieren oder Ausschalten der BitLocker-Laufwerkverschlüsselung

Wenn Sie Änderungen am TPM oder dem System vornehmen, müssen Sie unter Umständen die BitLocker-Verschlüsselung auf dem Systemvolume zeitweise ausschalten. Auf Datenvolumes ist es nicht möglich, die BitLocker-Verschlüsselung zeitweise auszuschalten, Datenvolumes können Sie nur entschlüsseln.

Gehen Sie folgendermaßen vor, um die BitLocker-Verschlüsselung auf dem Systemvolume zeitweise auszuschalten:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *BitLocker-Laufwerkverschlüsselung*.
2. Tippen oder klicken Sie neben dem Systemvolume auf *BitLocker deaktivieren*.
3. Tippen oder klicken Sie im Dialogfeld *BitLocker-Laufwerkverschlüsselung* auf *Bitlocker deaktivieren*.

Wenn dieser Vorgang abgeschlossen ist, haben Sie BitLocker auf dem Betriebssystemvolume zeitweise deaktiviert.

Gehen Sie folgendermaßen vor, um die BitLocker-Laufwerkverschlüsselung für ein Datenvolume auszuschalten und das Volume zu entschlüsseln:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *BitLocker-Laufwerkverschlüsselung*.
2. Tippen oder klicken Sie neben dem gewünschten Volume auf *BitLocker deaktivieren*.
3. Tippen oder klicken Sie im Dialogfeld *BitLocker-Laufwerkverschlüsselung* auf *Bitlocker deaktivieren*.

Gehen Sie folgendermaßen vor, um die BitLocker-Laufwerkverschlüsselung für ein USB-Flashlaufwerk auszuschalten und das Laufwerk zu entschlüsseln:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *BitLocker-Laufwerkverschlüsselung*.
2. Tippen oder klicken Sie neben dem gewünschten Volume auf *BitLocker deaktivieren*.
3. Tippen oder klicken Sie im Dialogfeld *BitLocker-Laufwerkverschlüsselung* auf *Bitlocker deaktivieren*.

Kapitel 12

Verwalten von Festplattenlaufwerken und Dateisystemen

In diesem Kapitel:

Grundlagen der Datenträgerverwaltung	428
Optimieren der Laufwerksleistung	436
Basisdatenträger und dynamische Datenträger	441
Verwenden von Basisdatenträgern und dynamischen Datenträgern	444
Verwenden von Datenträgern, Partitionen und Volumes	450
Partitionieren und Vorbereiten von Festplattenlaufwerken	452
Verwenden der Datenträgerspiegelung	465
Einbauen eines dynamischen Datenträgers in einen anderen Computer	467
Beseitigung auftretender Datenträgerprobleme	468
Arbeiten mit Wechselmediengeräten	479
Arbeiten mit Daten-CDs und -DVDs	481
Verwalten von Datenträgerkomprimierung und Dateiverschlüsselung	485

Die meisten Computer sind mit verschiedenen Arten von Laufwerken ausgestattet, darunter interne Festplattenlaufwerke und Laufwerke für Wechselmedien. Wichtigster Datenspeicher ist ein Festplattenlaufwerk. Gewöhnlich wird das erste Festplattenlaufwerk als *Datenträger 0* bezeichnet. Werden zusätzliche Festplatten installiert, erhalten Sie die Bezeichnungen *Datenträger 1*, *Datenträger 2* und so weiter. Dieses Kapitel beschreibt Programme und Techniken für die Verwaltung von Festplattenlaufwerken und Dateisystemen. Sie erfahren, wie man Laufwerke partitioniert, formatiert und von einem Laufwerkstyp in einen anderen konvertiert. Außerdem erfahren Sie etwas über Neuentwicklungen unter Windows 8, die sich auf die Verwendung der Treiber auswirken, wie Windows-ReadyBoost, Windows-ReadyDrive und Windows-SuperFetch.

Grundlagen der Datenträgerverwaltung

Unter Windows 8 können Sie ein Festplattenlaufwerk als Basisdatenträger oder als dynamischen Datenträger einsetzen.

- **Basisdatenträger** Dieser Laufwerkstyp wurde früher am meisten benutzt. Unter Windows 8 kann er in eine oder mehrere Partitionen aufgeteilt werden. *Partitionen* sind logische Abschnitte eines Laufwerks, die wie separate Laufwerke funktionieren. Damit eine Partition verwendet werden kann, muss sie mit einem bestimmten *Dateisystem* formatiert werden und einen Laufwerksbezeichner erhalten. Die formatierte Partition wird dann *Basisvolume* genannt und lässt sich im Computer wie ein eigenständiges Laufwerk verwenden. Windows 8 unterstützt auf Basisdatenträgern sowohl primäre Partitionen als auch erweiterte Partitionen. Eine primäre Partition wird zum Starten des Betriebssystems verwendet. Der Zugriff auf eine primäre Partition kann direkt mit dem *Laufwerksbezeichner* erfolgen. Eine primäre Partition lässt sich nicht weiter aufteilen. Der Zugriff auf eine erweiterte Partition ist etwas komplizierter. Wenn Sie eine erweiterte Partition erstellt haben, müssen Sie sie in ein oder mehrere logische Laufwerke aufteilen. Anschließend können Sie die logischen Laufwerke unabhängig voneinander verwenden. Auch sie sind über ihre Laufwerksbezeichner zugänglich.
- **Dynamische Datenträger** Dynamische Datenträger ermöglichen die Durchführung der gebräuchlichsten Verwaltungsarbeiten an Laufwerken, ohne dass ein Neustart des Computers erforderlich wird. Wie ein Basisdatenträger lässt sich auch ein *dynamischer Datenträger* aufteilen. Allerdings werden dynamische Datenträger in *Volumes* aufgeteilt und nicht mehr in Partitionen. Ein Volume ähnelt einer Partition. Der gebräuchlichste Volumetyp ist das einfache Volume. Ein einfaches Volume ist ein Volume, das sich auf ein Festplattenlaufwerk beschränkt. Es kann zum Start des Betriebssystems oder zur allgemeinen Datenspeicherung verwendet werden. Außerdem sind noch weitere Volumearten verfügbar, darunter auch solche, die sich über mehrere Festplattenlaufwerke erstrecken (ein *übergreifendes Volume*). Wie Partitionen oder logische Laufwerke müssen Sie auch ein Volume auf einem dynamischen Datenträger formatieren und ihm einen Laufwerksbezeichner zuweisen, bevor Sie es verwenden können. Das formatierte Volume wird *dynamisches Volume* genannt und lässt sich als lokales Laufwerk des Computers verwenden. Wenn sich ein dynamisches Volume über mehrere Festplattenlaufwerke erstreckt, erscheint es trotzdem nur als einzelnes lokales Laufwerk, für dessen Verwendung auch nur ein Laufwerksbezeichner erforderlich ist.

Sie können den Datenträgertyp von Basisdatenträger auf dynamischer Datenträger ändern, und umgekehrt. Wenn Sie einen Basisdatenträger in einen dynamischen Datenträger konvertieren, werden die Partitionen automatisch in Volumes des passenden Typs überführt, sodass keine Daten verloren gehen. Einen dynamischen Datenträger in einen Basisdatenträger zu konvertieren ist allerdings nicht so einfach. Sie müssen die Volumes auf dem dynamischen Datenträger löschen, bevor Sie den Datenträgertyp in einen Basisdatenträger ändern können. Beim Löschen der Volumes gehen alle Daten verloren, die darin

gespeichert sind. Sie erhalten diese Daten nur zurück, wenn Sie den Inhalt des Datenträgers aus einer Datensicherung wiederherstellen.

Neben dem Datenträgertyp haben alle Datenträger auch eine bestimmte Partitionsart (oder einen bestimmten *Partitionsstil*): entweder MBR (Master Boot Record) oder GPT (GUID Partition Table). Sowohl die 32-Bit- als auch die 64-Bit-Editionen von Windows 8 unterstützen sowohl MBR- als auch GPT-Partitionen, aber GPT wird in älteren Windows-Versionen nicht erkannt.

Der MBR enthält eine Partitionstabelle, die angibt, wo sich die Partitionen auf der Festplatte befinden. Bei dieser Partitionsart enthält der erste Sektor auf einer Festplatte den Master Boot Record und eine Binärcodedatei, die Master Boot Code heißt und zum Starten des Systems verwendet wird. Dieser Sektor ist nicht partitioniert und zum Schutz des Systems für den Benutzer nicht sichtbar.

Bei der Partitionierungsart MBR unterstützen Laufwerke Volumes bis zu 4 Terabyte (TByte) und verwenden einen von zwei Partitionstypen – primär oder erweitert. Ein MBR-Laufwerk kann bis zu vier primäre Partitionen besitzen, oder drei primäre Partitionen und eine erweiterte Partition. Primäre Partitionen sind Laufwerksabschnitte, auf die Sie zur Dateispeicherung direkt zugreifen können. Sie können eine primäre Partition für den Benutzerzugriff zugänglich machen, indem Sie darin ein Dateisystem erstellen. Im Gegensatz zu primären Partitionen können Sie auf erweiterte Partitionen nicht direkt zugreifen. Stattdessen können Sie erweiterte Partitionen mit einem oder mehreren logischen Laufwerken konfigurieren, die dem Speichern von Dateien dienen. Durch das Unterteilen erweiterter Partitionen in logische Laufwerke können Sie ein physisches Laufwerk in mehr als vier Bereiche unterteilen.

GPT wurde ursprünglich für Hochleistungscomputer mit Itanium-Architektur entwickelt. GPT wird für Laufwerke auf x86- und x64-Systemen empfohlen, die größer als 2 TByte sind. Der Hauptunterschied zwischen den Partitionsarten GPT und MBR besteht darin, wie Partitionsdaten gespeichert werden. Bei GPT werden die wichtigen Partitionsdaten in den einzelnen Partitionen gespeichert. Außerdem gibt es redundante primäre und Sicherungspartitionstabellen zur Verbesserung der strukturellen Integrität.

Wenngleich es wesentliche Unterschiede zwischen den Partitionsarten GPT und MBR gibt, werden die meisten festplattenbezogenen Aufgaben in derselben Weise durchgeführt. Wenn Sie Ihre Laufwerke daher erst einmal eingerichtet und konfiguriert haben, ist es normalerweise egal, ob der Datenträger mit MBR oder GPT partitioniert ist. Beachten Sie aber trotzdem folgende Punkte:

- MBR-Basisdatenträger können bis zu vier primäre Partitionen haben, oder drei primäre Partitionen und eine erweiterte Partition, wobei die erweiterte Partition wiederum mehrere logische Laufwerke enthalten kann. Ein dynamischer MBR-Datenträger kann beliebig viele Volumes enthalten.
- GPT-Datenträger unterstützen Partitionen mit bis zu 18 Exabyte (EByte) Größe und bis zu 128 Partitionen. Computer, die GPT-Datenträger verwenden, haben zwei erforderliche Partitionen und mindestens eine optionale OEM- oder Datenpartition. Die erforderlichen Partitionen sind die EFI-Systempartition (EFI System Partition, ESP) und die MSR-Partition (Microsoft Reserved). Welche optionalen Partitionen vorhanden sind, hängt zwar von der Systemkonfiguration ab, aber meist handelt es sich bei einer optionalen Partition um eine primäre Partition. Primäre Partitionen werden auf GPT-Datenträgern benutzt, um Benutzerdaten zu speichern.
- Auf einem x86- oder x64-Computer mit BIOS können Sie MBR für Systemstart- oder Datenlaufwerke verwenden, aber GPT nur für Datenlaufwerke. In x64-Computern mit EFI können Sie sowohl GPT- als auch MBR-Datenträger verwenden, aber Sie brauchen mindestens einen GPT-Datenträger, der die ESP und entweder eine primäre Partition oder ein einfaches Volume enthält, von dem das Betriebssystem gestartet wird.

Windows unterstützt FAT, FAT32, exFAT und NTFS. In FAT bestimmt die Zahl der Bits, die in der Dateizuordnungstabelle benutzt werden, mit welcher Variante Sie arbeiten und wie groß ein Volume höchstens sein kann. FAT16, auch einfach als FAT bezeichnet, definiert seine Dateizuordnungstabellen mit 16 Bits. Volumes, die 4 GByte oder kleiner sind, werden mit FAT16 formatiert. Es gibt auch eine 32-Bit-Version von FAT, die als FAT32 bezeichnet wird. FAT32 definiert seine Dateizuordnungstabellen mit 32 Bits. Mit den Windows-Formatierungstools können Sie FAT32-Volumes erstellen, die bis zu 32 GByte groß sind. Windows kann zwar größere FAT32-Volumes einbinden, die mit Fremdherstellertools erstellt wurden, aber für Volumes, die größer sind als 32 GByte, sollten Sie NTFS benutzen.

Die bevorzugten Formate für große interne und externe Festplatten sind NTFS und exFAT. Gegenüber den ersten Windows-Versionen stellt dies eine beträchtliche Entwicklung dar. Extended FAT, oder exFAT, ist eine erweiterte Version von FAT. Aus technischer Sicht hätte man es FAT64 nennen können (manche nennen es auch so). exFAT verwendet für die Dateizuordnungstabellen 64 Bits. Das ermöglicht es exFAT, die im FAT32-Dateisystem geltende Dateigrößenbeschränkung auf 4 GByte und die Volumengrößenbeschränkung auf 32 GByte zu überwinden. Das exFAT-Format unterstützt Zuordnungseinheiten bis zu 128 KByte auf Volumes bis zu 256 TByte. Das exFAT-Format wurde so entworfen, dass es in allen kompatiblen Betriebssystemen oder Geräten verwendet und gegebenenfalls zwischen diesen Geräten ausgetauscht werden kann. Dadurch hat exFAT gegenüber FAT einen Vorteil.

Unter exFAT können mehr als 1024 Dateien im selben Verzeichnis liegen. exFAT unterstützt Zugangssteuerungslisten und Transaktionen. Außerdem verwendet exFAT eine Cluster-Zuordnungstabelle für schnelle Speicherplatzzuweisungen und kontinuierliche Bitfolgen pro Datei für den schnellen Dateizugriff. Insgesamt ergibt sich daraus eine höhere Leistung. Eine verbesserte lückenlose Speicherung auf der Festplatte verbessert die Leistung bei der Arbeit mit Medien, beispielsweise bei der Aufzeichnung und Wiedergabe von digitalen Medien.

HINWEIS

Windows Server 2012 bietet ReFS (Resilient File System). Vielleicht ändert sich dies durch zukünftige Updates oder Service Packs, aber Windows 8 bietet in seiner Originalform keine ReFS-Unterstützung.

Windows 8 stellt mehrere Tools zum Verwalten der Datenträger im Computer bereit. Das erste wird oft übersehen: die Computerkonsole. Andere Tools sind die Datenträgerverwaltung, FSUtil und DiskPart. Partitionen und Volumes auf MBR- und GPT-Datenträgern können mit exFAT und NTFS formatiert werden. Wenn Sie Partitionen oder Volumes in der Datenträgerverwaltung erstellen, haben Sie die Gelegenheit, den Datenträger direkt beim Erstellen des Volumes zu formatieren und ihm einen Laufwerkbuchstaben oder einen Bereitstellungspunkt zuzuweisen. Sie können in der Datenträgerverwaltung die Partitionen und Volumes auf einem MBR-Datenträger mit exFAT und NTFS formatieren, aber für Partitionen und Volumes auf einem GPT-Datenträger steht nur NTFS zur Verfügung. Wenn Sie GPT-Datenträger mit FAT oder FAT32 formatieren wollen, müssen Sie die Programme Format oder DiskPart in der Eingabeaufforderung verwenden.

Sie können die Partitionsart von MBR in GPT ändern und umgekehrt von GPT in MBR. Das ist nützlich, wenn Sie Datenträger zwischen BIOS-Computern und EFI-Computern austauschen wollen oder neue Datenträger erhalten, die mit der falschen Partitionstabellenart eingerichtet sind. Sie können die Partitionstabellenart allerdings nur bei einem leeren Datenträger konvertieren. Das bedeutet, dass der Datenträger entweder neu oder frisch formatiert sein muss. Sie können einen Datenträger natürlich auch löschen, indem Sie seine Partitionen oder Volumes entfernen.

Wie im Abschnitt »Hardwareverschlüsselung, sicherer Start und Netzwerkentsperrung« von Kapitel 11, »Arbeiten mit TPM und BitLocker-Laufwerkverschlüsselung«, beschrieben, unterstützt Windows 8 die Verwendung von Festplattenlaufwerken mit Hardwareverschlüsselung. Solche Laufwerke verfügen über

spezielle Verschlüsselungsprozessoren, die das Betriebssystem entlasten und die Beanspruchung der Systemressourcen verringern. Windows 8 verwendet die Hardwareverschlüsselung für BitLocker, sofern verfügbar.

Windows 8 unterstützt Festplatten im Standardformat und im erweiterten Format. Standardformatlaufwerke verwenden 512 Bytes pro physischen Sektor und werden daher auch 512b-Laufwerke genannt. Laufwerke mit dem erweiterten Format verwenden 4096 Bytes pro physischen Sektor und werden auch 512e-Laufwerke genannt. 512e bedeutet eine beträchtliche Entwicklung für die Festplattenindustrie und ermöglicht riesige Laufwerke im Multiterabitebereich.

PRAXISTIPP Die kleinste Dateneinheit, die ein Festplattenlaufwerk schreiben kann, ist nicht das Byte, sondern der Sektor. 512b-Laufwerke schreiben jeweils 512 Bytes, 512e-Laufwerke 4096. In einer Eingabeaufforderung mit erhöhten Rechten können Sie mit folgender Eingabe überprüfen, wie groß ein physischer Sektor ist:

```
Fsutil fsinfo ntfsinfo LaufwerksBuchstabe
```

Darin ist *LaufwerksBuchstabe* der Buchstabe des zu überprüfenden Laufwerks, wie in

```
Fsutil fsinfo ntfsinfo c:
```

Größere physische Sektoren ermöglichen es, die Laufwerkskapazität gegenüber herkömmlichen Laufwerken beträchtlich zu steigern. Stehen nur 512-Byte-Sektoren zur Verfügung, müssen die Festplatten zusätzliche Verwaltungsarbeit leisten, um die Daten zu schreiben. Zur Leistungsoptimierung sollten Anwendungen so aktualisiert werden, dass sie mit der neuen Sektorgröße (4096 Byte) optimal arbeiten.

Verwenden der Computerkonsole

Wenn Sie die Computerkonsole öffnen möchten, tippen oder klicken Sie auf dem Desktop auf den Datei-Explorer. Tippen oder klicken Sie auf die Ortsauswahlschaltfläche und wählen Sie *Computer*, oder tippen oder klicken Sie im linken Bereich des Datei-Explorers auf den Knoten *Computer*.

HINWEIS Im Datei-Explorer zeigt die Adressleiste den absoluten oder relativen Pfad, den Sie gerade verwenden, und bietet Optionen für die Arbeit mit diesem Pfad. Von links nach rechts sind vier Benutzerschnittstellenelemente zu sehen: ein Ortssymbol, eine Ortsauswahlschaltfläche, Ortspfadeinträge und eine Schaltfläche *Vorherige Orte*.

In der Computerkonsole sehen Sie schnell, wie viel Speicher auf den Laufwerken eines Computers noch frei ist (Abbildung 12.1). Wenn Sie mit der Seite *Computer* arbeiten, gibt es im Menüband *Computer* folgende Optionen für Ort, Netzwerk und System:

- **Eigenschaften** Zeigt das Eigenschaftendialogfeld für das ausgewählte Element.
- **Öffnen** Öffnet das ausgewählte Element im selben Datei-Explorer-Fenster.
- **Umbenennen** Ermöglicht das Umbenennen des ausgewählten Elements.
- **Auf Medien zugreifen** Ermöglicht die Verbindung mit einem Medienserver oder die Trennung dieser Verbindung.
- **Netzlaufwerk verbinden** Ermöglicht die Zuordnung eines Netzlaufwerks oder die Trennung von diesem Laufwerk.
- **Netzwerkadresse hinzufügen** Ermöglicht die Erstellung einer Verknüpfung mit einer Website, einer FTP-Site, einem Speicherplatz oder einem anderen Ort im Netzwerk.
- **Systemsteuerung öffnen** Öffnet die Systemsteuerung im aktuellen Fenster.

- **Programm deinstallieren oder ändern** Öffnet die Seite *Programme und Features* in der Systemsteuerung.
- **Systemeigenschaften** Öffnet die Seite *System* aus der Systemsteuerung.
- **Verwalten** Öffnet die Computerverwaltung in einem neuen Fenster.

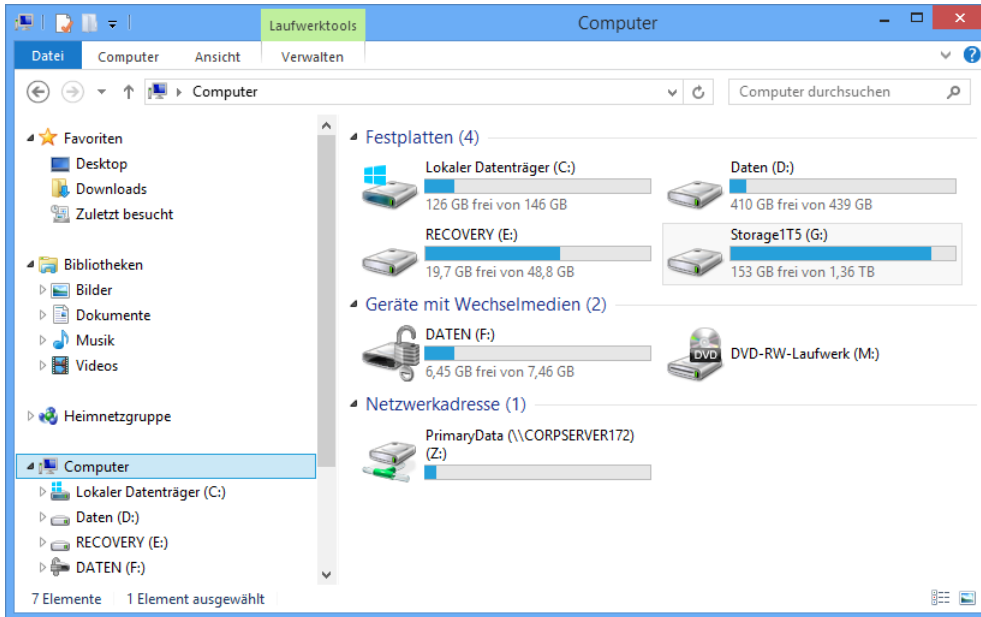


Abbildung 12.1 Die Konsole *Computer* bietet einen einfachen Zugang zu den Speichermedien eines Computers

Die Computerkonsole zeigt unter anderem folgende Informationen:

- **Festplatten** Listet die lokalen Laufwerke auf, die auf dem Computer verfügbar sind. Klicken Sie mit der rechten Maustaste auf ein Laufwerk oder halten Sie es gedrückt, um die verfügbaren Verwaltungsoptionen anzuzeigen. Dazu gehört auch der Befehl *Öffnen*, der das Laufwerk im Datei-Explorer öffnet. Sie erreichen wichtige Laufwerkstools, wenn Sie ein Laufwerk antippen oder anklicken und dann in der Menüleiste auf *Verwalten* tippen oder klicken.
- **Geräte mit Wechselmedien** Listet die Geräte mit Wechselmedien auf, einschließlich CD-, DVD- und Diskettenlaufwerke sowie USB-Flashlaufwerke. Klicken Sie mit der rechten Maustaste auf ein Gerät oder halten Sie es gedrückt, um die verfügbaren Verwaltungsoptionen anzuzeigen. Dazu gehört auch die Option *Auswerfen*, die beim Wechsel des Mediums sehr praktisch ist.

TIPP

USB-Flashlaufwerke und über FireWire, eSATA oder USB angeschlossene externe Festplattenlaufwerke verdrängen mehr und mehr die Diskettenlaufwerke und andere Gerätearten mit Wechselmedien. Verfügt ein Computer über einen USB-, eSATA- oder FireWire-Anschluss, können Sie auf einfache Weise ein Laufwerk anschließen oder entfernen. Bevor Sie aber ein USB-, eSATA oder FireWire-Laufwerk entfernen, sollten Sie dafür sorgen, dass es sich in einem definierten Zustand befindet. Eine Möglichkeit, dies zu erreichen, ist die Option *Auswerfen*. Tippen oder klicken Sie im Datei-Explorer oder einer vergleichbaren Darstellung, beispielsweise in der Liste der Geräte mit Wechselmedien, auf das Laufwerk, damit in der Menüleiste das Menü *Verwalten* erscheint. Tippen oder klicken Sie auf *Verwalten* und dann auf *Auswerfen*. Sofern keine Dateien auf dem Laufwerk geöffnet sind, sollte es dann möglich sein, das Laufwerk sicher zu entfernen.

- **Netzwerkadresse** Listet alle zugeordneten Netzlaufwerke auf. Ein Netzlaufwerk bietet Zugriff auf einen freigegebenen Ordner oder ein freigegebenes Laufwerk eines anderen Computers. Sie können Netzwerklaufwerke zuordnen, indem Sie auf der Seite *Computer* in der Menüleiste auf *Computer* tippen oder klicken und dann *Netzlaufwerk verbinden* wählen. Dadurch wird der Assistent für die Zuordnung von Netzlaufwerken gestartet. Um die Zuordnung aufzuheben, klicken Sie das Symbol der Netzwerkadresse mit der rechten Maustaste an oder halten es gedrückt, und wählen *Trennen*.

Verwenden der Datenträgerverwaltung

Das bevorzugte Werkzeug zur Konfiguration von Laufwerken ist die Datenträgerverwaltung. Sie bietet die Funktionen, die Sie zur Verwaltung von Festplattenlaufwerken, Partitionen, Volumes, von logischen Laufwerken und ihren Dateisystemen brauchen. Die Datenträgerverwaltung ist ein Snap-In der Microsoft Management Console (MMC), das als vorkonfigurierte Konsole in Windows enthalten ist und sich auch in Konsolen einfügen lässt, die Sie selbst zusammenstellen.

Mit der Datenträgerverwaltung können Sie folgende Arbeiten durchführen:

- Bestimmen der Kapazität, des freien Speicherplatzes, des Status und anderer Eigenschaften von Laufwerken
- Erstellen von Partitionen und logischen Laufwerken auf Basisdatenträgern
- Erstellen von Volumes auf dynamischen Datenträgern
- Erweitern von Volumes auf demselben Festplattenlaufwerk oder über mehrere Festplattenlaufwerke hinweg
- Formatieren von Volumes mit einem ausgewählten Dateisystem
- Zuweisen von Laufwerksbuchstaben und Pfaden zu Volumes
- Konvertieren von Basisdatenträgern in dynamische Datenträger, und umgekehrt

Die Datenträgerverwaltung ist auch in der Konsole *Computerverwaltung* enthalten. Sie können die Computerverwaltung in einer Eingabeaufforderung mit erhöhten Rechten starten, indem Sie **compmgmt.msc** eingeben. Oder geben Sie im Suchfeld *Apps* **compmgmt.msc** ein.

Wenn Sie die Computerverwaltung starten, werden Sie automatisch mit dem lokalen Computer verbunden. Um die Laufwerke von anderen Computern zu untersuchen, klicken Sie in der Strukturdarstellung mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten ihn gedrückt, und wählen im Kontextmenü *Verbindung mit anderem Computer herstellen*. Nun können Sie den Computer wählen, dessen Laufwerke Sie untersuchen möchten. Auf der Befehlszeile können Sie eine Verbindung mit einem anderen Computer herstellen, indem Sie mit dem Befehl **compmgmt.msc /computer=<ComputerName>** die Computerverwaltung starten, wobei *<ComputerName>* der Name des Remotecomputers ist, mit dem Sie eine Verbindung herstellen möchten.

In der Standardkonfiguration, wie sie in Abbildung 12.2 zu sehen ist, zeigt die Datenträgerverwaltung in ihrem oberen Bereich eine Volumeliste und in ihrem unteren Bereich eine grafische Ansicht. Es sind zwar immer nur zwei Ansichten zu sehen, aber es stehen drei zur Auswahl.

- **Volumeliste** Bietet eine Übersicht über die Laufwerke eines Computers unter Angabe einiger wichtiger Eigenschaften. Durch Tippen oder Klicken auf eine der Spalten wie *Layout* oder *Status* wird die Liste nach der angeklickten Spalte sortiert.

- **Grafische Ansicht** Stellt die verfügbaren physischen und logischen Laufwerke grafisch dar. Zu den Angaben über die physischen Laufwerke gehören die Laufwerksnummer und der Gerätetyp, wie Basis, Wechselmedium oder DVD, die Laufwerkskapazität und der Status des Geräts, also online oder offline. Für jedes logische Laufwerk auf dem physischen Laufwerk werden weitere Einzelheiten genannt, wie der Laufwerkbuchstabe und die Bezeichnung der Partition oder des Volumes, der Dateisystemtyp, wie exFAT oder NTFS, die Größe des Laufwerks und der Status des Laufwerks, wie *Fehlerfrei* oder *Fehler*.
- **Datenträgerliste** Bietet einen Überblick über die physischen Laufwerke. Zu den Angaben gehören die Laufwerksnummer und der Gerätetyp, wie Basis, Wechselmedium oder DVD, die Laufwerkskapazität, die Menge des noch nicht belegten Speichers, sofern vorhanden, der Status des Geräts, wie *Online* oder *Offline*, und die Art der Geräteschnittstelle, wie IDE (Integrated Device Electronics) oder ATA (Advanced Technology Attachment).

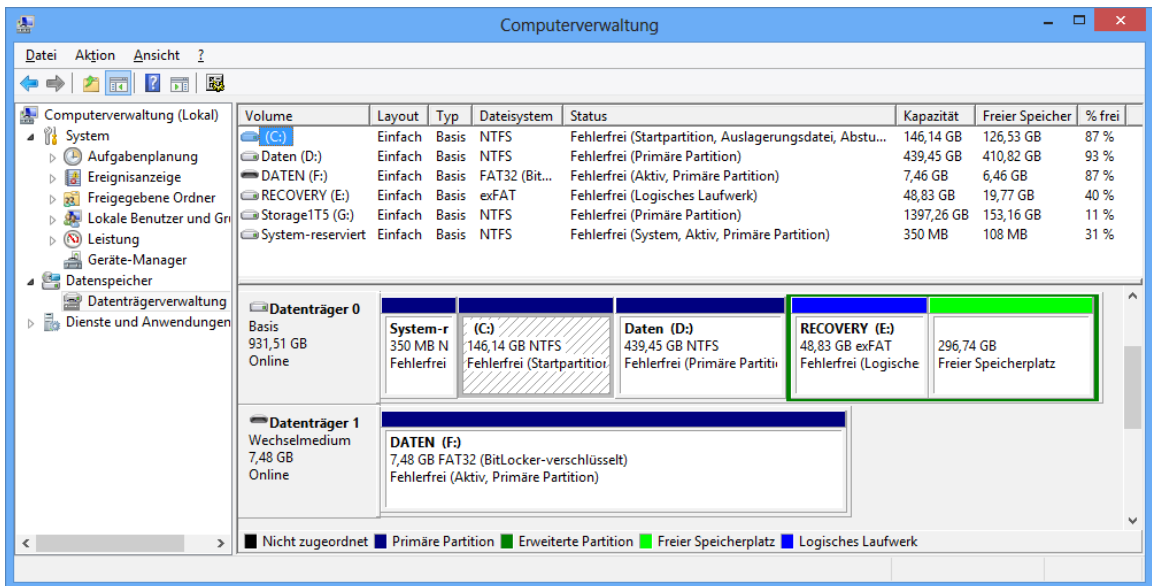


Abbildung 12.2 In der Datenträgerverwaltung verwalten Sie Laufwerke

Im Menü *Ansicht* können Sie die gewünschte Ansicht für den oberen und den unteren Bereich einstellen. Zur Änderung der Darstellung im oberen Bereich wählen Sie *Ansicht, Anzeige oben* und dann die gewünschte Ansicht. Zur Änderung der Darstellung im unteren Bereich wählen Sie *Ansicht, Anzeige unten* und dann die gewünschte Darstellungsart.

Wie Sie sehen, erhalten Sie in mehreren Ansichten Informationen über die verfügbaren Laufwerke. Wenn Sie mehr über ein Laufwerk erfahren möchten, klicken Sie es in der Volumelistenansicht mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen *Eigenschaften*. Dann öffnet sich ein Dialogfeld, das so ähnlich aussieht wie in Abbildung 12.3. Dasselbe Dialogfeld können Sie im Datei-Explorer öffnen, indem Sie das Hauptsymbol eines Laufwerks mit der rechten Maustaste anklicken oder es gedrückt halten, und dann *Eigenschaften* wählen. Wählen Sie auf der Registerkarte *Anpassen* eine Ansichtsvorlage aus, um festzulegen, wie Ordner im Inhaltsfensterabschnitt des Datei-Explorers angezeigt werden.

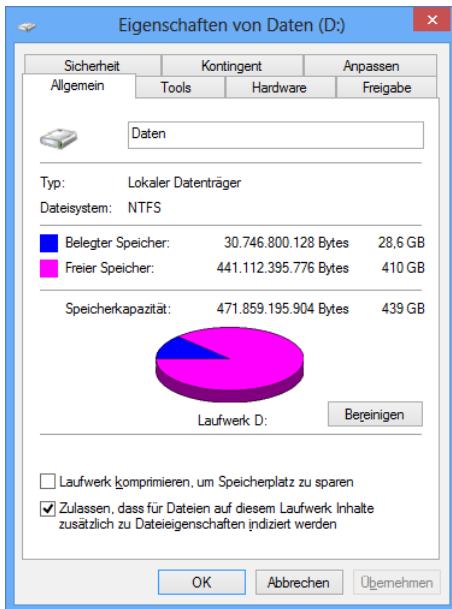


Abbildung 12.3 Das Dialogfeld *Eigenschaften* liefert ausführliche Informationen über ein Laufwerk

Verwenden von FSUtil und DiskPart

Windows 8 bietet auch Befehlszeilenprogramme zur Laufwerksverwaltung:

- **FSUtil** Dieses Programm ist für erfahrene Techniker gedacht, die sehr ins Detail gehen müssen. Mit FSUtil können Sie Metainformationen und andere Daten über Laufwerke abrufen, wie zum Beispiel USN-Journale (Update Sequence Number), Analysepunkte und Hardlinks. Außerdem erhalten Sie ausführliche Informationen über Sektoren und Zuordnungseinheiten, beispielsweise die Zahl der freien oder reservierten Zuordnungseinheiten eines Laufwerks. Eine Liste der in FSUtil verfügbaren Befehle erhalten Sie, wenn Sie in einer Eingabeaufforderung mit erhöhten Rechten **fsutil** eingeben. Informationen über einen bestimmten Befehl erhalten Sie mit *fsutil Befehlsname help*.
- **DiskPart** Ein textorientierter Befehlsinterpret, mit dem Sie Laufwerke, Partitionen und Volumes auf der Befehlszeile verwalten können. DiskPart kann nicht nur viele der Arbeiten durchführen, die Sie sonst in der Datenträgerverwaltung erledigen, sondern lässt sich auch mit Skripten zur Automatisierung der Datenträgerverwaltung verwenden. Sie starten DiskPart, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten **diskpart** eingeben. Dadurch gelangen Sie zur Eingabeaufforderung **DISKPART>**. Wenn Sie dann **help** eingeben und die EINGABETASTE drücken, erscheint eine Liste der verfügbaren Befehle mit einer kurzen Beschreibung ihrer Verwendung.

HINWEIS

Im Gegensatz zur Datenträgerverwaltung, die eine übersichtliche Benutzeroberfläche bietet und ziemlich leicht zu verwenden ist, handelt es sich bei FSUtil und DiskPart um komplexe Programme, die für erfahrene Administratoren gedacht sind. Ihre Verwendung wird in *Windows Command-Line Administrator's Pocket Consultant, Second Edition* (Microsoft Press, 2008) ausführlich besprochen. Ein Beispiel für die Verwendung von DiskPart finden Sie im Abschnitt »Kennzeichnen einer Partition als aktiv« weiter unten in diesem Kapitel.

Optimieren der Laufwerksleistung

Windows 8 verfügt über einige Optimierungsfunktionen, die sich auf die Verwendung von Laufwerken auswirken, diese in den folgenden Abschnitten ausführlicher beschrieben werden. Dazu gehören:

- **Windows-ReadyBoost** Steigert die Systemleistung, indem USB-Flashlaufwerke als zusätzliche Zwischenspeicher verwendet werden.
- **Windows-ReadyDrive** Steigert die Systemleistung auf Mobilcomputern, die mit Hybridlaufwerken ausgerüstet sind.
- **Windows-SuperFetch** Steigert die Systemleistung durch einen modifizierten Speicherverwaltungsalgorithmus.

Funktionsweise und Verwendung von Windows-ReadyBoost

Die Bedeutung der Laufwerke eines Computers beschränkt sich nicht auf das Lesen und Schreiben von Anwendungsdaten und Dokumenten. Das Betriebssystem verwendet die Laufwerke auch intensiv für Auslagerungsdateien und als Zwischenspeicher. Da Schreib- und Lesezugriffe auf Laufwerke wesentlich langsamer sind als Schreib- und Lesezugriffe auf den Arbeitsspeicher (RAM), können sich solche Vorgänge als Bremsklötze erweisen, unter denen die Gesamtleistung des Systems leidet. Windows 8 enthält Windows-ReadyBoost als Möglichkeit, Leistungseinbrüche durch Schreib- und Lesezugriffe auf Zwischenspeicher abzumildern.

Mit Windows-ReadyBoost lassen sich USB-Flashlaufwerke mit hinreichend schnellem Speicher als Zwischenspeicher für ausgelagerte Speicherseiten des Arbeitsspeichers verwenden. Durch die Verwendung von USB-Flashlaufwerken für die Zwischenspeicherung können Lesezugriffe unter Windows 8 schneller erfolgen, als wenn die Zwischenspeicherung auf Festplatten erfolgt. Da diese Zwischenspeicherung für alle Inhalte verwendet wird und sich nicht nur auf die Auslagerungsdatei oder System-DLLs (Dynamic-Link Libraries) beschränkt, steigt die Gesamtleistung des Computers, denn Flashlaufwerke können Daten bis zu zehnmal schneller lesen als herkömmliche Laufwerke.

Zu den USB-Flashlaufwerken, die sich mit Windows-ReadyBoost verwenden lassen, gehören USB-2.0-Flashlaufwerke (oder höher), SD-Karten (Secure Digital) und CompactFlash-Karten. Die Geräte müssen eine gewisse Geschwindigkeit aufweisen und über mindestens 256 MByte Speicher verfügen. Um die Leistung zu verbessern, empfehle ich, USB-Speichersticks mit möglichst schnellem Speicher zu kaufen. Enthält das Flashlaufwerk eine Mischung aus langsamem und schnellem Speicher, wird nur der schnelle Speicher zur Leistungssteigerung verwendet. Auf einem USB-Speicherstick können zwischen 230 und 15.196 MByte Flashspeicher für ReadyBoost reserviert werden. Eine empfehlenswerte Größe ist die 1- bis 3-fache Menge des verfügbaren Systemspeichers. Denken Sie aber daran, dass Sie momentan höchstens 15.196 MByte reservieren können.

Der Speicherplatz auf den USB-Flashlaufwerken wird hauptsächlich für wahlfreie Ein-/Ausgabeoperationen verwendet, denn bei sequenzieller Ein- und Ausgabe sind herkömmliche Laufwerke meistens schneller als Flashlaufwerke. Windows-ReadyBoost versucht, die Leistung zu optimieren und umfangreichere sequenzielle Lesezugriffe an die Festplattenlaufwerke des Computers zu übergeben. Damit USB-Flashlaufwerke jederzeit entfernt werden können, werden alle Daten auf die Festplatte geschrieben, bevor sie auf das Flashlaufwerk kopiert werden. Das bedeutet, dass alle Daten, die auf dem Flashlaufwerk gespeichert sind, auch auf der Festplatte vorhanden sind und durch die Entfernung des Flashgeräts kein Datenverlust entstehen sollte. Da auf dem Flashspeicher vielleicht sensible Daten liegen, verschlüsselt Windows-ReadyBoost außerdem die Daten, damit sie sich nur auf dem Computer verwenden lassen, auf dem sie ursprünglich geschrieben wurden.

Aktivieren und Konfigurieren von ReadyBoost

Mit Windows-ReadyBoost lassen sich USB-Flashlaufwerke mit hinreichend schnellem Flashspeicher als zusätzlicher Zwischenspeicher einsetzen. Wenn Sie ein USB-Flashlaufwerk an einem USB-2.0-Anschluss (oder höher) anschließen, überprüft Windows 8 die Geschwindigkeit des Flashspeichers des Geräts. Ist der Speicher schnell genug, lässt sich der Arbeitsspeicher des Computers auf das USB-Flashlaufwerk ausdehnen. Gewöhnlich sollte der Flashspeicher mindestens so schnell sein wie die Busgeschwindigkeit des Computers.

TIPP Windows markiert ein Gerät manchmal als nicht schnell genug, weil es die Leistungsanforderungen angeblich nicht erfüllt. Schlägt der erste Leistungstest bei einem Gerät fehl, können Sie das Gerät über die Registerkarte *ReadyBoost* erneut testen. Klicken Sie dazu im Datei-Explorer mit der rechten Maustaste auf das Gerät oder halten Sie es gedrückt, und wählen Sie den Befehl *Eigenschaften*. Tippen oder klicken Sie im Eigenschaftendialogfeld auf die Registerkarte *ReadyBoost* und dann auf *Erneut testen*.

Die folgende Anleitung beschreibt, wie Sie Windows ReadyBoost aktivieren und konfigurieren, sobald Sie einen USB-Speicherstick zum ersten Mal an Ihrem Computer verwenden:

1. Stecken Sie den USB-Speicherstick in einen Anschluss mit USB 2.0 oder schneller ein. Es erscheint eine Meldung mit der Aufforderung, sie anzuklicken, um eine Aktion für den Wechseldatenträger auszuwählen. Tippen oder klicken Sie diese Meldung an.
2. Wenn Sie auf *System beschleunigen* klicken, wird das Eigenschaftendialogfeld des Geräts geöffnet, wo bereits die Registerkarte *ReadyBoost* ausgewählt ist (Abbildung 12.4). Wählen Sie hier eine der folgenden Einstellungen und tippen oder klicken Sie auf *OK*:
 - Wählen Sie die Option *Dieses Gerät für ReadyBoost reservieren*, wenn Sie auf dem Gerät automatisch die Höchstmenge an Platz für ReadyBoost reservieren wollen. Wenn Sie diese Option wählen, wird nicht verhindert, dass ein Benutzer Dateien auf das Gerät schreibt. ReadyBoost wird lediglich so konfiguriert, dass es bei Bedarf so viel Platz nutzt, wie reserviert werden kann.
 - Wählen Sie die Option *Dieses Gerät verwenden* aus und stellen Sie mit dem Schieberegler *Für Systembeschleunigung zu reservierender Speicher* oder dem Kombinationsfeld ein, wie viel Platz für ReadyBoost verwendet werden soll, wenn Sie auf dem Gerät weniger Platz als die Höchstmenge zur Verfügung stellen wollen. In diesem Fall können Sie den freien Platz für Dateien und Daten nutzen.

Windows 8 dehnt den physischen Arbeitsspeicher des Computers auf das Gerät aus. In der Standardkonfiguration reserviert Windows-ReadyBoost den gesamten freien Platz auf dem Gerät, um die Systemgeschwindigkeit zu erhöhen.

PRAXISTIPP Sie können einen USB-Speicherstick nur dann für ReadyBoost einsetzen, wenn das Gerät mindestens 2,5 Megabit pro Sekunde (MBit/s) Durchsatz für zufällig verteilte Lesevorgänge mit 4-KByte-Blöcken und 1,75 MBit/s Durchsatz für zufällig verteilte Schreibvorgänge mit 512-KByte-Blöcken bietet. Sie können ReadyBoost zwar auf einem Gerät aktivieren, das Sie mit BitLocker To Go verschlüsselt haben, bedenken Sie aber, dass die Verschlüsselungs- und Entschlüsselungsprozesse möglicherweise die Lese-/Schreib-Leistung verschlechtern. Wollen Sie BitLocker To Go und ReadyBoost kombinieren, empfehle ich, das Gerät automatisch zu entsperren, sobald es angesteckt wird. Andernfalls muss der Benutzer das Gerät von Hand entsperren, um die Leistungsvorteile von ReadyBoost ausnutzen zu können.

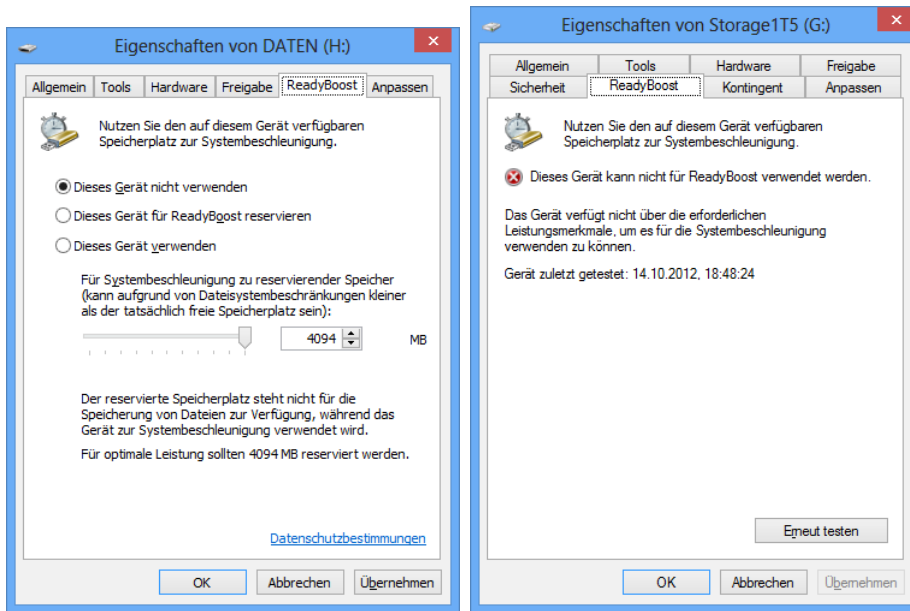


Abbildung 12.4 Konfigurieren der Windows-ReadyBoost-Einstellungen

Um ein USB-Flashlaufwerk für Windows-ReadyBoost zu verwenden, das Sie bereits angeschlossen oder zuvor ausdrücklich nicht für Windows-ReadyBoost verwendet haben, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Datei-Explorer oder eine andere Explorer-Ansicht, beispielsweise *Computer*.
2. Klicken Sie in der Liste *Geräte mit Wechselmedien* mit der rechten Maustaste auf das USB-Flashlaufwerk oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*.
3. Konfigurieren Sie auf der Registerkarte *ReadyBoost* die Optionen, wie in Schritt 2 der vorherigen Anleitung beschrieben. Tippen oder klicken Sie auf *OK*.

Wenn ein USB-Flashlaufwerk ReadyBoost nicht unterstützt, können Sie das Gerät auch nicht für ReadyBoost aktivieren. Sie können ein USB-Flashlaufwerk, das vollständig für ReadyBoost verwendet wird, jederzeit sicher entfernen, ohne Daten zu verlieren oder das System negativ zu beeinträchtigen. Allerdings geht die Systemleistung durch die Entfernung des Geräts auf die normale Stufe zurück, die es ohne USB-Flashlaufwerk erbringt. Gehen Sie folgendermaßen vor, um ein Gerät zu entfernen, das einen ReadyBoost-Speicherbereich und Datendateien enthält:

1. Öffnen Sie den Datei-Explorer oder eine andere Explorer-Ansicht, wie zum Beispiel *Computer*.
2. Klicken Sie mit der rechten Maustaste auf das Gerät oder halten Sie es gedrückt, und wählen Sie den Befehl *Auswerfen*. Wenn Sie Dateien auf dem Gerät geöffnet haben oder das Gerät im Datei-Explorer angezeigt wird, müssen Sie unter Umständen die Dateien und Explorer-Fenster schließen, bevor Sie das Gerät abziehen können.

Funktionsweise und Verwendung von Windows-ReadyDrive

Windows-ReadyDrive verbessert die Leistung von Mobilcomputern, die mit Hybridlaufwerken ausgerüstet sind. Ein Hybridlaufwerk ist eine Kombination von Flash-RAM und herkömmlichem Festplattenlaufwerk. Da Flash-RAM wesentlich schneller ist als das herkömmliche Laufwerk, schreiben Mobilcomputer, auf denen Windows 8 ausgeführt wird, Daten und Änderungen zuerst in den Flashspeicher. In bestimm-

ten Abständen werden diese Schreibzugriffe und Änderungen mit dem Festplattenlaufwerk synchronisiert. Dieser Lösungsansatz bewirkt, dass das Festplattenlaufwerk nicht so oft eingeschaltet werden muss, und das spart Strom.

Das Flash-RAM von Hybridlaufwerken kann für schnellere Wechsel zwischen Normalmodus und einem Energiesparmodus oder Ruhezustand verwendet werden. In diesem Fall wird die Information für die Reaktivierung des Systems ins Flash-RAM geschrieben, bevor das System in einen Energiesparmodus oder in den Ruhezustand übergeht oder heruntergefahren wird. Wenn Sie den Computer dann einschalten oder reaktivieren, werden die Daten aus dem Flash-RAM ausgelesen.

Sie brauchen ReadyDrive nicht zu aktivieren, es wird auf Mobilcomputern mit Hybridlaufwerken automatisch aktiviert.

Funktionsweise und Verwendung von Windows-SuperFetch

Windows 8 erreicht durch eine andere Kontrolle über Benutzer- und Hintergrundprozessen eine verbesserte Reaktionsfähigkeit des Systems und eine höhere Leistung. In Windows XP haben Benutzerprozesse und Hintergrundprozesse dieselbe Priorität bei der Speicherbenutzung. Benutzerprozesse und Hintergrundprozesse werden in den Speicher geladen, wenn sie ausgeführt werden. Da eine Prioritätsregel fehlt, ergibt sich oft eine Art Verdrängungswettbewerb um den Speicher. Außerdem bleiben Hintergrundprozesse nach ihrer Ausführung zu lange im Speicher, was zu Leistungseinbußen führt. Die Daten für Benutzerprozesse müssen dann auf Anforderung neu in den Speicher geladen werden. Windows 8 löst dieses Problem, indem es dafür sorgt, dass Hintergrundprozesse nach ihrer Ausführung aus dem Speicher verschwinden und dass die von ihnen verdrängten Daten für Benutzerprozesse wieder geladen werden.

Unter Windows XP haben Benutzerprozesse und Hintergrundprozesse dieselbe E/A-Priorität. Das führt oft zu Konflikten und einer schlechten Leistung bei Schreib- und Lesezugriffen. Windows 8 löst dieses Problem durch die Einführung von E/A-Warteschlangen mit hoher und mit niedriger Priorität. Priorisierte Ein-/Ausgabevorgänge werden von Benutzerprozessen für die Lese- und Schreibzugriffe auf Laufwerke verwendet. Für die Schreib- und Lesezugriffe der Hintergrundprozesse auf Laufwerke gilt eine niedrige Priorität.

HINWEIS

Unter Windows 8 werden viele Dienste und Verwaltungsarbeiten als Hintergrundprozesse ausgeführt. Beispielsweise wird unter Windows 8 eine automatische Defragmentierung eingeplant, die regelmäßig Laufwerke defragmentiert. Diese Defragmentierung wird als Hintergrundprozess ausgeführt und verwendet Ein-/Ausgabevorgänge niedriger Priorität.

Die Schlüsselfunktion für die Priorisierung von Speicher- und Ein-/Ausgabevorgängen ist Windows-SuperFetch. Windows-SuperFetch verbessert die Systemleistung durch einen modifizierten Speicherverwaltungsalgorithmus. Im Gegensatz zum Speicherverwaltungsalgorithmus von Windows XP und früheren Windows-Versionen optimiert SuperFetch die Speicherverwendung danach, wie der Benutzer den Computer verwendet. SuperFetch erreicht dies durch folgende Verhaltensweisen:

- **Unterscheiden zwischen Benutzeranwendungen und Hintergrunddiensten, die auf dem Computer ausgeführt werden** SuperFetch erreicht eine höhere Reaktionsfähigkeit des Computers auf Benutzereingaben, indem es den Prozessen des aktuellen Benutzers gegenüber Hintergrundprozessen eine höhere Priorität gibt. Da Benutzerprozesse eine höhere Priorität haben als Hintergrundprozesse, können Hintergrundprozesse nicht mehr so viel Prozessorzeit beanspruchen und das System reagiert schneller auf die Eingaben des Benutzers.

- **Optimieren des Speichers für Benutzeranwendungen nach der Ausführung von Hintergrundprozessen** Die Verwaltungsprozesse von Windows 8 nutzen Leerlaufzeiten besser aus, als es frühere Windows-Versionen getan haben. Ein größerer Anteil der Verwaltungsprozesse wird jetzt in die Leerlaufphasen verlegt, wie zum Beispiel die Defragmentierung und die Datensicherung. Befindet sich der Computer im Leerlauf, werden Hintergrundprozesse wie gewöhnlich ausgeführt. Wird aber ein Hintergrundprozess beendet, versetzt SuperFetch den Speicher wieder in den Zustand, in dem er sich vor der Ausführung des Hintergrundprozesses befand. Auf diese Weise wird der Speicher für Benutzerprozesse optimiert und der Computer reagiert schneller auf Eingaben des Benutzers.
- **Erfassen der am häufigsten verwendeten Anwendungen und Abschätzen der Anforderungen des Benutzers** SuperFetch führt Buch darüber, welche Anwendungen am häufigsten ausgeführt werden, und merkt sich auch, wann diese Anwendungen gewöhnlich verwendet werden. Dann verwendet SuperFetch diese Informationen, um die Anwendungen vorab zu laden und für den Gebrauch vorzubereiten, bevor der Benutzer die Anwendung voraussichtlich benutzen wird. Im Lauf der Zeit werden Benutzerwechsel und Anwendungsstarts dadurch schneller.
- **Berücksichtigen der Prioritätsunterschiede bei Ein-/Ausgabevorgängen** SuperFetch nutzt die Vorteile der E/A-Warteschlangen hoher Priorität aus, um Schreib- und Lesevorgänge für Benutzerprozesse zu optimieren und die Reaktionsfähigkeit des Systems unter Windows 8 insgesamt zu verbessern. Wenn mehrere Prozesse um E/A-Ressourcen konkurrieren, erhalten Prozesse hoher Priorität mehr E/A-Zeit als Prozesse geringerer Priorität. Daher zeigen Benutzerprozesse und Anwendungen eine bessere Leistung und es gibt weniger Konkurrenz um E/A-Zeit, wenn Benutzerprozesse und Hintergrundprozesse gleichzeitig ausgeführt werden.

Alle Windows 8-Versionen unterstützen SuperFetch. Als Administrator sollten Sie nicht nur verstehen, wie SuperFetch funktioniert, sondern auch, wie es konfiguriert ist. Wesentliche Merkmale von SuperFetch sind:

- Es wird als Dienst namens *Superfetch* ausgeführt. Dieser Dienst wird beim Hochfahren des Systems automatisch gestartet und meldet sich mit dem Konto *SYSTEM* an.
- Es verwendet die ausführbare Datei *SvcHost.exe* und wird unter Netzwerkausschluss ausgeführt. Das bedeutet, dass SuperFetch nur auf den lokalen Computer zugreifen kann und keinen Zugriff auf die Netzwerke hat, mit denen der Computer verbunden ist.
- Es hängt von der Filter-Manager-Komponente ab. Der Filter-Manager liefert die Datei- und Dateisysteminformationen, die SuperFetch braucht; er wird automatisch mit dem Betriebssystem installiert.
- Es schreibt Vorabrufdaten in den Ordner *%SystemRoot%\Prefetch*. Die Vorabrufdaten sollen den Start von Anwendungen beschleunigen. Im *Prefetch*-Ordner finden Sie auch eine ganze Reihe von Datenbankdateien, in denen bestimmte Daten über die bisherige Verwendung der Anwendungen erfasst werden. Sie sollen die Leistung der Anwendungen verbessern. Auch Anwendungsfehler werden in einer Datenbank erfasst.

HINWEIS

Der Ordner *Prefetch* wird automatisch gewartet, Sie brauchen ihn oder seinen Inhalt nicht zu löschen.

Wenn Sie größere Änderungen am Betriebssystem vornehmen, Service Packs oder Updates einspielen oder Anwendungen installieren und umkonfigurieren, müssen die Benutzer möglicherweise etwas länger warten, bis das Betriebssystem hochgefahren ist. Wie stark diese Verzögerung ist, hängt davon ab, wie umfassend die Änderungen sind und wie viel Daten zur Speichernutzung SuperFetch neu aufbauen muss. Manchmal, etwa nach der Installation eines Service Packs, pendelt sich die Systemstartgeschwindigkeit erst nach einigen Neustarts wieder auf das vorherige Niveau ein.

Basisdatenträger und dynamische Datenträger

Es ist noch gar nicht so lange her, dass die Festplatten der ausgelieferten Windows-Computer als Basisdatenträger konfiguriert wurden. Aber weil die Verbraucher immer größere und robustere Laufwerke verlangen, gehen die Hersteller zunehmend dazu über, ihre Festplatten als dynamische Datenträger zu konfigurieren. Statt mit einem einzigen 500-GB-Byte-Laufwerk ausgerüstet zu sein, hat ein neuer Computer vielleicht ein übergreifendes 1000-GB-Byte-Volume, wobei zwei 500-GB-Byte-Laufwerke wie ein einziges logisches Laufwerk verwendet werden. In diesem Szenario dienen übergreifende Volumes dazu, mehrere Festplatten so aussehen zu lassen, als handle es sich um eine einzige große Festplatte. Der beste Weg, dies unter Windows 8 zu erreichen, führt über dynamische Datenträger.

Da mehr und mehr Computer mit dynamischen Datenträgern ausgeliefert werden, stellt sich für Sie vielleicht die Frage, ob Sie die noch in Ihren Computern vorhandenen Basisdatenträger in dynamische Datenträger umwandeln sollen. In manchen Fällen wird die Frage vielleicht durch einen Zwang zur Standardisierung entschieden. Vielleicht wollen Sie alle Desktops einer bestimmten Abteilung gleich konfigurieren, damit sie leichter zu verwalten sind. In anderen Fällen schreibt das IT-Management vielleicht die Umstellung vor, weil eine Konvertierung von Basisdatenträgern in dynamische Datenträger als Upgrade angesehen wird. (Man stellt also Computer mit einem alten Laufwerkstyp auf einen aktuelleren Laufwerkstyp um.) Bevor Sie sich aber dazu entschließen, eine Umstellung von einem Laufwerkstyp auf einen anderen vorzunehmen, stehen die Fragen im Vordergrund, worum es eigentlich geht, welche Funktionen geboten und welche nicht geboten werden.

Ein Basisdatenträger ist ein Laufwerk, auf dem es ein oder mehrere Basisvolumes gibt, die in primären Partitionen liegen, und zusätzlich eine optionale erweiterte Partition, die logische Laufwerke enthält. Eine primäre Partition ist ein Abschnitt des Laufwerks, den Sie direkt formatieren und zur Datenspeicherung verwenden können. Jedes Festplattenlaufwerk kann bis zu vier primäre Partitionen haben. Sie machen eine primäre Partition verwendungsfähig, indem Sie ein Dateisystem in ihr erstellen. Eine der primären Partitionen können Sie auch durch eine erweiterte Partition ersetzen (eine Festplatte kann also über bis zu drei primäre Partitionen und eine erweiterte Partition verfügen). Im Gegensatz zu primären Partitionen können Sie aber erweiterte Partitionen nicht direkt formatieren. Vorher müssen Sie in der erweiterten Partition ein oder mehrere logische Laufwerke einrichten, die sich dann formatieren und zur Datenspeicherung verwenden lassen. Da sich eine erweiterte Partition in mehrere logische Laufwerke aufteilen lässt, können Sie ein Festplattenlaufwerk also in mehr als vier Abschnitte aufteilen. In einer einzigen erweiterten Partition können Sie zum Beispiel die logischen Laufwerke F, G und H anlegen.

Ein dynamischer Datenträger ist ein Laufwerk, auf dem es ein oder mehrere dynamische Volumes gibt. Im Gegensatz zu Basisdatenträgern ist die Zahl der Volumes, die es auf einem dynamischen Datenträger geben kann, nicht durch eine feste Vorgabe begrenzt. Sie können so viele Volumes anlegen, wie auf das Laufwerk passen, und jedes dieser Volumes lässt sich erweitern oder als Systemvolume verwenden. Basisdatenträger lassen sich zwar in jedem Windows-Betriebssystem verwenden, aber dynamische Datenträger können erst ab Windows 2000 oder höher eingesetzt werden.

Ein großer Vorteil der dynamischen Datenträger lag bisher darin, dass mehrere physische Laufwerke mit den Spanning-, Stripeset- oder Spiegelungsfunktionen von Windows zu einem logischen Laufwerk zusammengefasst werden können. In Windows 8 ist es nun allerdings auch möglich, Basisdatenträger mit diesen Techniken zusammenzufassen. Wenn Sie ein übergreifendes Volume oder ein Stripesetvolume erstellen, dann erstellen Sie ein Volume, das sich nicht auf ein einziges physisches Laufwerk beschränkt, sondern sich über zwei oder mehr Laufwerke erstreckt, wobei von jedem dieser Laufwerke nur ein Teil oder auch alles verwendet wird. Der Unterschied zwischen übergreifenden Volumes und Stripesetvolumes liegt in der Art und Weise, wie Daten gespeichert und verwaltet werden. Übergreifende Volumes

behandelt Windows 8 so, wie es eine einzige große Partition behandeln würde. Es nutzt also nicht die Tatsache aus, dass eigentlich mehrere Geräte zur Verfügung stehen, die gleichzeitig Lese- oder Schreibzugriffe durchführen könnten. Bei Stripesetvolumes schreibt Windows 8 auf jedes am Volume beteiligte Laufwerk einen Teil der Daten. Gewöhnlich ergibt sich daraus ein schnellerer Schreib- und Lesezugriff auf die Daten, weil sie auf mehrere Laufwerke verteilt und von mehreren Laufwerken gelesen werden. Bei der Spiegelung werden zwei Laufwerke zu einem einzigen fehlertoleranten Volume zusammengefasst. Fällt ein Laufwerk aus, bleibt das andere verfügbar und das Volume kann wiederhergestellt werden.

ACHTUNG Aus technischer Sicht handelt es sich bei Stripesetvolumes um RAID-0 (Redundant Array of Independent Disks, level 0) und bei der Spiegelung um RAID-1. Die Laufwerksspiegelung ist fehlertolerant, aber weder übergreifende Volumes noch Stripesetvolumes bieten Fehlertoleranz. Fällt eine der beteiligten Festplatten aus, so fällt das ganze Volume aus.

Weil Sie in Windows 8 nun auch Basisdatenträger zu übergreifenden, Stripeset- und gespiegelten Volumes zusammenfassen können, bleiben als wesentliche Vorteile der dynamischen Datenträger gegenüber den Basisdatenträgern die verbesserte Fehlerkorrektur und -erkennung sowie die Fähigkeit, den Datenträger zu ändern, ohne den Computer neu starten zu müssen. Andere verfügbare Features hängen von der Datenträgerformatierung ab, ob Sie also exFAT oder NTFS benutzen.

Wenn Sie einen Datenträger mit einem Dateisystem formatieren, untergliedert das Dateisystem den Datenträger in Cluster (in der Benutzeroberfläche auch als Zuordnungseinheiten bezeichnet). Diese Cluster sind logische Gruppen von Sektoren. Auf 512b-Laufwerken verwenden FAT, FAT32, exFAT und NTFS eine feste Sektorgröße von 512 Byte, die Clustergröße kann aber verändert werden. Beträgt die Clustergröße beispielsweise 4.096 Byte, besteht jeder Cluster aus acht Sektoren, da ein Sektor 512 Byte enthält.

Tabelle 12.1 fasst die Standardclustergrößen für FAT16, FAT32, exFAT und NTFS zusammen. Sie haben die Möglichkeit, die Clustergröße festzulegen, wenn Sie das Dateisystem auf einem Datenträger anlegen. Sie können natürlich auch die Standardclustergröße übernehmen. Die möglichen Werte für die Clustergröße hängen dabei immer vom Dateisystem ab.

PRAXISTIPP Windows-Plattformen arbeiten mit vier FAT-Dateisystemen: FAT12, FAT16, FAT32 und exFAT. Der Unterschied zwischen FAT12, FAT16 und FAT32 liegt darin, wie viele Bits für Einträge in den Dateizuordnungstabellen benutzt werden; dies sind 12, 16 beziehungsweise 32 Bits. Aus Sicht des Benutzers liegt der wesentliche Unterschied zwischen diesen Dateisystemen in der theoretischen Maximalgröße für ein Volume. Dies sind 16 MByte für ein FAT12-Volume, 4 GByte für FAT16 und 2 TByte für FAT32. Wird der Begriff FAT ohne Zahlzusatz verwendet, ist im Allgemeinen sowohl FAT16 als auch FAT32 gemeint. exFAT (Extended FAT) ist eine erweiterte Version von FAT32. exFAT bietet dieselbe einfache Bedienung wie FAT32, beseitigt aber die Dateigrößenbeschränkung auf 4 GByte und die Volumengrößenbeschränkung auf 32 GByte, die in FAT32-Dateisystemen gelegentlich zu Problemen führen. Das exFAT-Format unterstützt auch Zuordnungseinheiten mit bis zu 32.768 KByte Größe. exFAT ist so entworfen, dass es problemlos in allen kompatiblen Betriebssystemen oder Geräten benutzt und zwischen solchen Systemen ausgetauscht werden kann. Damit hat exFAT einen wichtigen Vorteil gegenüber FAT.

Das wichtigste Merkmal von Clustern ist, dass sie die kleinste Einheit bilden, mit der Festplattenplatz zugewiesen wird. Jeder Cluster kann höchstens eine Datei enthalten. Wenn Sie also eine 1 KByte große Datei erstellen, die Clustergröße aber 4 KByte beträgt, bleiben 3 KByte Platz im Cluster leer, der nicht für andere Dateien genutzt werden kann. Das ist unvermeidlich. Ist ein einzelner Cluster nicht groß genug für eine ganze Datei, werden die übrigen Dateidaten im nächsten freien Cluster gespeichert und dann wieder im nächsten, bis die Datei vollständig gespeichert ist. Bei FAT enthält der erste Cluster, der von

einer Datei benutzt wird, einen Zeiger auf den zweiten Cluster, der zweite Cluster einen Zeiger auf den nächsten und so weiter, bis Sie zum letzten Cluster einer Datei kommen, in dem statt eines Zeigers die Dateiendemarkierung EOF (End Of File) steht.

Tabelle 12.1 Standardclustergrößen für FAT16, FAT32, exFAT und NTFS

Volumegröße	Clustergröße			
	FAT16	FAT32	exFAT	NTFS
7 bis 16 MByte	512 Byte (als FAT12)	Nicht unterstützt	4 KByte	512 Byte
17 bis 32 MByte	512 Byte	Nicht unterstützt	4 KByte	512 Byte
33 bis 64 MByte	1 KByte	512 Byte	4 KByte	512 Byte
65 bis 128 MByte	2 KByte	1 KByte	4 KByte	512 Byte
129 bis 256 MByte	4 KByte	2 KByte	4 KByte	512 Byte
257 bis 512 MByte	8 KByte	4 KByte	32 KByte	512 Byte
513 bis 1.024 MByte	16 KByte	4 KByte	32 KByte	1 KByte
1.025 MByte bis 2 GByte	32 KByte	4 KByte	32 KByte	2 KByte
2 bis 4 GByte	64 KByte	4 KByte	32 KByte	4 KByte
4 bis 8 GByte	Nicht unterstützt	4 KByte	32 KByte	4 KByte
8 bis 16 GByte	Nicht unterstützt	8 KByte	32 KByte	4 KByte
16 bis 32 GByte	Nicht unterstützt	16 KByte	32 KByte	4 KByte
32 GByte bis 2 TByte	Nicht unterstützt	*	128 KByte	4 KByte
2 bis 16 TByte	Nicht unterstützt	*	128 KByte	4 KByte
16 bis 32 TByte	Nicht unterstützt	*	128 KByte	8 KByte
32 bis 64 TByte	Nicht unterstützt	*	128 KByte	16 KByte
64 bis 128 TByte	Nicht unterstützt	*	128 KByte	32 KByte
128 bis 256 TByte	Nicht unterstützt	*	128 KByte	64 KByte

* Mit den Windows-Formatierungstools sind Sie auf 32 GByte beschränkt. Mit Tools anderer Anbieter können auch größere Volumes erstellt werden.

Das Datenträger-E/A-Subsystem verwaltet die Struktur der Datenträger. Windows verwaltet dagegen die logische Datenträgerstruktur auf der Dateisystemebene. Die logische Struktur eines Datenträgers bezieht sich auf die Basis- oder dynamischen Volumes, die Sie auf einem Datenträger erstellen, und auf die Dateisysteme, mit denen diese Volumes formatiert sind. Sie können sowohl Basisvolumes als auch dynamische Volumes mit FAT oder NTFS formatieren. Jeder Dateisystemtyp hat eine andere Struktur, und jedes Dateisystem bietet Vor- und Nachteile.

Sie können zwar im selben Computer Basisdatenträger und dynamische Datenträger einsetzen, aber die Laufwerke, die an einem Volume beteiligt sind, müssen vom selben Typ sein. Die Umwandlung von Basisdatenträgern in dynamische Datenträger, und umgekehrt, wird im Abschnitt »Konvertieren eines Basisdatenträgers in einen dynamischen Datenträger, und umgekehrt« weiter unten in diesem Kapitel beschrieben. Beachten Sie bitte, dass Sie zwar einen Basisdatenträger in einen dynamischen Datenträger konvertieren können, wobei die Daten normalerweise erhalten bleiben, aber bevor Sie einen dynamischen Datenträger in einen Basisdatenträger umwandeln können, müssen Sie alle vorhandenen Partitionen des dynamischen Datenträgers löschen. Durch das Löschen der Partitionen gehen auch die Daten

auf den betreffenden Laufwerken verloren. Schließlich sei noch erwähnt, dass dynamische Datenträger nicht auf Wechselmedien oder den Laufwerken eines portablen Computers erstellt werden können. Das bedeutet, dass Laptops, Tablet-PCs und andere Arten von tragbaren Computern nur über Basisdatenträger verfügen.

ACHTUNG Seien Sie vorsichtig, wenn Sie auf Laptops arbeiten. Manche Laptopkonfigurationen bringen die Datenträgerverwaltung zu der Annahme, dass sie einen Basisdatenträger in einen dynamischen Datenträger konvertieren könnte. Das kann auf Computern geschehen, die nicht APM (Advanced Power Management) oder ACPI (Advanced Configuration and Power Interface) unterstützen. Es scheint zwar so, als würden dynamische Datenträger unterstützt, aber das ist ein Irrtum. Der Versuch, auf einem solchen Laptop einen Basisdatenträger in einen dynamischen Datenträger zu konvertieren, kann die ganze Festplatte zerstören.

HINWEIS Externe Festplattenlaufwerke, die über FireWire, USB oder eSATA angeschlossen werden, lassen sich in manchen Fällen in dynamische Datenträger konvertieren. Der Microsoft Knowledge Base-Artikel 299598, »So wird's gemacht: Konvertieren eines IEEE 1394-Festplattenlaufwerks in ein dynamisches Festplattenlaufwerk in Windows XP«, beschreibt die Einzelheiten. Allerdings warnt der Artikel nicht eindringlich genug vor den Einschränkungen und Folgen. Die externe Festplatte darf nur an *einem* Computer verwendet werden. Wenn Sie planen, dieses Laufwerk in Zukunft an einen anderen Computer anzuschließen, sollten Sie es nicht in einen dynamischen Datenträger umwandeln. Außerdem sollten Sie unbedingt die Daten sichern, bevor Sie versuchen, ein externes Laufwerk zu konvertieren, das über FireWire oder USB angeschlossen ist. Probieren Sie die Konvertierung vorher an einem identischen Laufwerk, das keine wichtigen Daten enthält, in einer Entwicklungs- oder Testumgebung aus und überprüfen Sie dann, ob das Laufwerk ordnungsgemäß funktioniert.

Verwenden von Basisdatenträgern und dynamischen Datenträgern

Was die Verwendung von Basisdatenträgern und dynamischen Datenträgern betrifft, ähneln sich viele Vorgänge, wie zum Beispiel die Initialisierung neuer Laufwerke, die Kennzeichnung des aktiven Laufwerks oder die Änderung des Laufwerkstyps. Bevor Sie diese Arbeiten durchführen, sollten Sie natürlich verstehen, was mit Laufwerksbezeichnungen wie *Aktiv*, *Startpartition*, *Systempartition* und anderen Bezeichnungen gemeint ist.

Bedeutung der Laufwerksbezeichnungen

Basisdatenträger können primäre und erweiterte Partitionen haben. Eine primäre Partition kann zum Start des Betriebssystems verwendet werden. Eine primäre Partition lässt sich zwar nicht weiter unterteilen, aber erweiterte Partitionen lassen sich in ein oder mehrere logische Laufwerke aufteilen, die unabhängig voneinander verwendet werden können.

Dynamische Datenträger werden in Volumes aufgeteilt, wobei das einfache Volume der gebräuchlichste Volumetyp ist. Ein einfaches Volume ist ein Volume auf einem Festplattenlaufwerk und kann zum Start des Betriebssystems verwendet werden. Dynamische Volumes können sich dagegen über mehrere Festplattenlaufwerke erstrecken.

Ganz gleich, ob Sie mit Basisdatenträgern oder dynamischen Datenträgern arbeiten, Sie sollten bei MBR-Datenträgern besonders auf fünf spezielle Arten von Laufwerksabschnitten achten.

- **Aktiv** Die aktive Partition oder das aktive Volume ist der Laufwerksabschnitt, von dem ein Computer gestartet wird. Sind mehrere Betriebssysteme installiert, muss die aktive Partition die Startdateien des Betriebssystems enthalten, das Sie starten möchten, und es muss sich um eine primäre Partition eines Basisdatenträgers oder um ein einfaches Volume eines dynamischen Datenträgers handeln. Normalerweise wird die aktive Partition in der Datenträgerverwaltung nicht speziell als solche gekennzeichnet. Gewöhnlich ist es die primäre Partition oder das erste einfache Volume auf Datenträger 0. Allerdings sehen Sie wahrscheinlich die Kennzeichnung *Aktiv*, wenn Sie die Standardkonfiguration ändern.

ACHTUNG Bei Wechselmedien kann der Status *Aktiv* angezeigt werden, nicht zu verwechseln mit der Kennzeichnung einer aktiven Partition. Genauer gesagt, USB- und FireWire-Kartenleser für CompactFlash-Karten und andere Kartentypen werden vielleicht mit dem Status *Aktiv* angezeigt, wenn eine Karte eingesteckt und das Gerät online ist. Wichtig ist auch, dass ein Wechselmedium in manchen Fällen als Datenträger 0 gelistet werden kann. In diesem Fall müssen Sie die aktive Partition auf dem ersten physischen Festplattenlaufwerk suchen. Gibt es im Computer beispielsweise Datenträger 0, Datenträger 1 und Datenträger 2, und das erste Festplattenlaufwerk in dieser Sequenz ist Datenträger 1, dann ist die aktive Partition höchstwahrscheinlich die erste primäre Partition auf Datenträger 1.

- **System** Die Systempartition oder das Systemvolume enthält die hardwarespezifischen Dateien, die erforderlich sind, um das Betriebssystem zu laden. Die Systempartition oder das Systemvolume kann ein gespiegeltes, aber kein übergreifendes Volume oder Stripesetvolume sein. Die Systempartition wird in der Spalte *Status* der Volumeliste und der grafischen Ansicht der Datenträgerverwaltung entsprechend bezeichnet.
- **Start** Die Startpartition oder das Startvolume enthält das Betriebssystem und seine Dateien. Die Startpartition oder das Startvolume kann ein gespiegeltes, aber kein übergreifendes Volume oder Stripesetvolume sein. Auf den meisten Systemen dient dieselbe Partition oder dasselbe Volume als Start- und Systempartition oder -volume. Es hat zwar den Anschein, als seien die Bezeichnungen Start- und Systempartition vertauscht worden, aber diese Konvention wird seit der Einführung von Windows NT unverändert verwendet. Wie die aktive Partition wird auch die Startpartition in der Datenträgerverwaltung nicht besonders gekennzeichnet. In den meisten Fällen handelt es sich um die primäre Partition oder das erste einfache Volume auf Datenträger 0. Wird das Betriebssystem aber in einer anderen Partition oder auf einem anderen Volume installiert, sehen Sie vielleicht die Beschriftung *Startpartition*.
- **Auslagerungsdatei** Eine Auslagerungsdateipartition oder ein Auslagerungsdateivolume enthält eine Auslagerungsdatei, die vom Betriebssystem verwendet wird. Da ein Computer je nach Konfiguration des virtuellen Speichers auf mehreren Laufwerken Speicherseiten auslagern kann, kann es auch mehrere Auslagerungsdateipartitionen oder Auslagerungsdateivolumes geben. Je nach den konfigurierten Service Packs weist er aber vielleicht nur das primäre Volume als Träger einer Auslagerungsdatei aus. Einzelheiten über die Verwendung und Einstellung der Auslagerungsdateien finden Sie im Abschnitt »Konfigurieren des virtuellen Arbeitsspeichers« von Kapitel 2, »Konfigurieren von Windows 8-Computern«.
- **Absturzabbild** Die Absturzabbildpartition oder das Absturzabbildvolume nimmt die Speicherabbilddatei auf, die das Betriebssystem im Falle eines Absturzes zu speichern versucht. Wie in Kapitel 2 im Abschnitt »Einstellen der Wiederherstellungsoptionen« besprochen, dienen Speicherabbilddateien zur Diagnose der Absturzursache. Standardmäßig werden Speicherabbilddateien im Ordner *%SystemRoot%* gespeichert, sie können aber auf jedem beliebigen Volume oder jeder beliebigen Partition gespeichert werden.

Jeder Computer hat eine aktive, eine System-, eine Start- und eine Absturzabbildpartition oder ein entsprechendes Volume, wobei diese Partitionen oder Volumes kombiniert werden können. Die Kennzeichnung *Absturzabbild* ist die einzige, die auf mehreren Partitionen oder Volumes erscheinen kann.

Installieren und Initialisieren neuer Festplattenlaufwerke

Unter Windows 8 ist es recht einfach geworden, einen Computer mit neuen Festplatten auszurüsten. Nachdem Sie die Festplattenlaufwerke nach den Anweisungen des Herstellers eingebaut haben, starten Sie das System, melden sich an und starten die Datenträgerverwaltung. Falls die neuen Festplattenlaufwerke bereits initialisiert wurden, sollten sie automatisch online gebracht werden, wenn Sie im Menü *Aktion* die Option *Datenträger neu einlesen* wählen. Mit der Initialisierung ist gemeint, dass die Laufwerke bereits über eine Laufwerkssignatur verfügen, damit Schreib- und Lesezugriffe möglich sind. Wenn Sie neue Laufwerke verwenden, die noch nicht initialisiert wurden, also noch nicht über eine Signatur verfügen, startet die Datenträgerverwaltung den Assistenten zum Initialisieren und Konvertieren von Datenträgern, sobald sie gestartet wird und die neuen Laufwerke erkennt.

Sie können den Assistenten zum Initialisieren und Konvertieren von Datenträgern folgendermaßen zum Initialisieren der Laufwerke verwenden:

1. Klicken Sie auf der Willkommenseite auf *Weiter*. Auf der Seite *Wählen Sie die Datenträger aus, die initialisiert werden sollen* sind die neuen Laufwerke automatisch für die Initialisierung vorgewählt, aber wenn Sie nicht wollen, dass ein bestimmtes Laufwerk initialisiert wird, können Sie die entsprechende Option löschen.
2. Tippen oder klicken Sie auf *Weiter*, um zur Seite *Wählen Sie den zu konvertierenden Datenträger* zu gelangen. Auf dieser Seite werden die neuen Festplattenlaufwerke und alle systemfremden oder Startlaufwerke angezeigt, die in dynamische Datenträger konvertiert werden können. Die neuen Datenträger sind nicht standardmäßig vorgewählt. Wenn Sie die Datenträger konvertieren möchten, wählen Sie sie aus und tippen oder klicken dann auf *Weiter*.
3. Die letzte Seite zeigt die Optionen, die Sie ausgewählt haben, und die Arbeiten, die an jedem Laufwerk durchgeführt werden. Wenn alle Optionen richtig sind, tippen oder klicken Sie auf *Fertig stellen*, dann führt der Assistent die angegebenen Aktionen durch. Wenn Sie ein Laufwerk zur Initialisierung ausgewählt haben, schreibt der Assistent eine Laufwerkssignatur auf das Festplattenlaufwerk. Wenn Sie die Konvertierung eines Datenträgers gewählt haben, wandelt der Assistent den Datenträger in einen dynamischen Datenträger um, nachdem er die Laufwerkssignatur geschrieben hat.

Wenn Sie den Assistenten nicht verwenden möchten, können Sie ihn einfach schließen und stattdessen die Datenträgerverwaltung zur Verwaltung des Laufwerks verwenden. Das Laufwerk wird in der Datenträgerliste mit dem Status *Nicht initialisiert* aufgeführt und durch ein rotes Symbol gekennzeichnet, das wie ein kleiner, nach unten gerichteter Pfeil aussieht. Dann können Sie das Laufwerkssymbol mit der rechten Maustaste anklicken oder es gedrückt halten und *Datenträgerinitialisierung* wählen. Bestätigen Sie die Auswahl (oder ergänzen Sie die Auswahl, wenn mehrere Laufwerke initialisiert werden sollen) und starten Sie die Initialisierung durch Tippen oder Klicken auf *OK*. Die Umwandlung in einen dynamischen Datenträger wird dann durchgeführt, wie im Abschnitt »Konvertieren eines Basisdatenträgers in einen dynamischen Datenträger, und umgekehrt« weiter unten in diesem Kapitel beschrieben.

Ändern der Partitionstabellenart bei einem Datenträger

Sie können die Partitionstabellenart von MBR in GPT oder von GPT in MBR konvertieren. Diese Umstellung ist nützlich, wenn Sie Datenträger zwischen Computern austauschen wollen, die unterschiedliche Prozessorarchitekturen haben, oder wenn Sie neue Datenträger erhalten, die mit der falschen Partitionstabellenart formatiert sind. Sie können die Partitionstabellenart allerdings nur bei einem leeren Datenträger konvertieren. Der Datenträger muss also entweder neu oder frisch formatiert sein. Sie können einen Datenträger natürlich auch löschen, indem Sie seine Partitionen oder Volumes entfernen.

Sie können die Datenträgerverwaltung oder DiskPart verwenden, um die Partitionstabellenart zu ändern. Wenn Sie die Partitionsart eines leeren Datenträgers in der Datenträgerverwaltung ändern wollen, starten Sie die Computerverwaltung in der Systemsteuerung unter *Verwaltung* oder geben im *Apps*-Suchfeld **compmgmt.msc** ein und drücken die EINGABETASTE. Erweitern Sie in der Computerverwaltung den Knoten *Datenspeicher* und wählen Sie *Datenträgerverwaltung* aus. Es werden nun alle verfügbaren Datenträger angezeigt. Klicken Sie in der Grafiksicht in der linken Spalte mit der rechten Maustaste auf den Datenträger, den Sie konvertieren wollen, oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Zu GPT-Datenträger konvertieren* oder *Zu MBR-Datenträger konvertieren*.

Mit DiskPart ändern Sie die Partitionsart eines leeren Datenträgers, indem Sie DiskPart in einer Eingabeaufforderung mit erhöhten Rechten durch Eingabe von **diskpart** starten und dann den Datenträger auswählen, den Sie konvertieren wollen. Möchten Sie beispielsweise Datenträger 2 konvertieren, müssen Sie den Befehl **select disk 2** eingeben. Wenn Sie auf diese Weise den Datenträger ausgewählt haben, können Sie ihn von MBR in GPT konvertieren, indem Sie **convert gpt** verwenden. Entsprechend konvertiert der Befehl **convert mbr** den Datenträger von GPT in MBR.

Kennzeichnen einer Partition als aktiv

Normalerweise brauchen Sie keine Partitionskennzeichnungen zu ändern. Wenn Sie nur mit Windows 8 arbeiten oder außer Windows 8 nur andere Windows-Versionen auf Ihrem Computer installiert haben, brauchen Sie die aktive Partition nicht zu ändern. Auf einem Computer mit MBR-Laufwerken ist die aktive Partition gewöhnlich die primäre Partition oder das erste einfache Volume auf Datenträger 0. Wenn Sie Windows 8 auf Laufwerk C: installieren und Windows 2000 oder höher auf einer anderen Partition, beispielsweise Laufwerk D, brauchen Sie die aktive Partition nicht zu ändern, um Windows 8 oder das andere Betriebssystem starten zu können. Wenn Sie aber ein anderes Betriebssystem starten möchten, das nicht zu den Windows-Betriebssystemen gehört, müssen Sie dessen Betriebssystempartition gewöhnlich als aktiv kennzeichnen und das System dann neu starten, um das andere Betriebssystem verwenden zu können.

HINWEIS

Nur primäre Partitionen können als aktiv gekennzeichnet werden. Sie können keine logischen Laufwerke als aktiv kennzeichnen und Sie können keine Volumes als aktiv kennzeichnen. Wenn Sie einen Basisdatenträger, auf dem eine aktive Partition liegt, in einen dynamischen Datenträger konvertieren, wird aus dieser Partition ein einfaches Volume, das automatisch aktiv ist.

Um eine Partition als aktiv zu kennzeichnen, gehen Sie folgendermaßen vor:

1. Starten Sie die Datenträgerverwaltung, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten oder im *Apps*-Suchfeld **diskmgmt.msc** eingeben.
2. Klicken Sie mit der rechten Maustaste auf die primäre Partition, die Sie als aktiv kennzeichnen möchten, oder halten Sie sie gedrückt, und wählen Sie dann *Partition als aktiv markieren*.

ACHTUNG Wenn Sie eine Partition oder ein Volume als aktiv kennzeichnen, lässt die Datenträgerverwaltung die Änderung der Partitionskennzeichnung vielleicht nicht zu, mit der Folge, dass sich das Betriebssystem vielleicht nicht mehr hochfahren lässt, wenn Sie den Computer neu starten. Die einzige Abhilfe, die ich gefunden habe, ist, mit DiskPart alle erforderlichen Änderungen durchzuführen, bevor das System neu gestartet wird oder bevor nach einem fehlgeschlagenen Startversuch die Systemstartreparatur verwendet wird.

Listing 12.1 zeigt ein Beispiel für eine DiskPart-Sitzung, bei der die aktive Partition festgelegt wird. Wie Sie sehen, zeigt DiskPart nach dem Start den eigenen Namen und die Version an, die Sie verwenden, sowie den Namen des Computers. Dann wählen Sie den Datenträger aus, mit dem Sie arbeiten möchten, und listen seine Partitionen auf. In diesem Beispiel habe ich Datenträger 0 ausgewählt, die Partitionen aufgelistet und dann Partition 1 gewählt. Nachdem Sie einen Datenträger und eine Partition ausgewählt haben, können Sie mit der Partition arbeiten. Durch die Eingabe von **active** und einen Druck auf die EINGABETASTE wird die Partition dann als aktiv gekennzeichnet. Wenn Sie fertig sind, verlassen Sie DiskPart mit dem Befehl **exit**.

HINWEIS In diesem Beispiel wird Datenträger 0 verwendet. Vielleicht ist Datenträger 0 aber nicht das Festplattenlaufwerk, das Sie bearbeiten möchten. Mit dem Befehl *List Disk* können Sie die verfügbaren Datenträger auflisten und anhand der angezeigten Informationen einen Datenträger auswählen.

Listing 12.1 Festlegen der aktiven Partition mit DiskPart

```
C:>diskpart

Microsoft DiskPart version 6.2.8250
Copyright (C) 1999-2012 Microsoft Corporation.
Auf Computer: ENGPC85
DISKPART> select disk 0
Datenträger 0 ist jetzt der gewählte Datenträger.
DISKPART> list partition
  Partition ###  Typ                Größe      Offset
  -----
  Partition 1    Primär              932 GByte  1024 KByte
DISKPART> select partition 1
Partition 1 ist jetzt die gewählte Partition.
DISKPART> active
Die aktuelle Partition wurde als aktiv markiert.
DISKPART> exit
```

Konvertieren eines Basisdatenträgers in einen dynamischen Datenträger, und umgekehrt

Am einfachsten lässt sich ein Basisdatenträger in der Datenträgerverwaltung in einen dynamischen Datenträger konvertieren, und umgekehrt. Wenn Sie den Datenträger in einen dynamischen Datenträger umwandeln, werden Partitionen automatisch in Volumes des entsprechenden Typs konvertiert. Aus primären Partitionen werden einfache Volumes. Aus logischen Laufwerken in erweiterten Partitionen werden einfache Volumes. Der unbelegte (freie) Platz in einer erweiterten Partition wird als *Freier Speicherplatz* gekennzeichnet. Diese Volumes lassen sich nicht mehr in Partitionen zurückverwandeln. Stattdessen müssen Sie die Volumes des dynamischen Datenträgers löschen und das Festplattenlaufwerk dann in

einen Basisdatenträger umwandeln. Durch das Löschen der Volumes gehen auch alle Informationen verloren, die auf dem Datenträger gespeichert sind.

Bevor Sie einen Basisdatenträger in einen dynamischen Datenträger konvertieren, sollten Sie sicherstellen, dass Sie auf dem Computer keine frühere Windows-Version starten müssen. Außerdem sollten Sie dafür sorgen, dass am Ende des Festplattenlaufwerks 1 MByte Platz frei ist. Die Datenträgerverwaltung reserviert zwar diesen Platz, wenn sie Partitionen und Volumes erstellt, aber die Datenträgerverwaltungsprogramme von anderen Betriebssystemen tun dies vielleicht nicht. Die Folge wäre, dass die Konvertierung fehlschlägt. Außerdem dürfen Sie folgende Einschränkungen nicht außer Acht lassen:

- Sie können keine Wechselmedien in dynamische Datenträger konvertieren. Wechselmedienlaufwerke lassen sich nur als Basisdatenträger mit primären Partitionen konfigurieren.
- Partitionen eines Datenträgers, die Teil eines übergreifenden oder Stripesetvolumes sind, aber nicht die System- oder die Startpartition sind, können konvertiert werden. Sie müssen dann aber alle Laufwerke im Satz zusammen konvertieren.

Zur Umwandlung eines Basisdatenträgers in einen dynamischen Datenträger gehen Sie folgendermaßen vor:

1. In der Datenträgerverwaltung klicken Sie den betreffenden Basisdatenträger entweder in der Datenträgerliste oder im linken Bereich der grafischen Ansicht mit der rechten Maustaste an oder halten ihn gedrückt, und wählen *In dynamischen Datenträger konvertieren*.
2. Im Dialogfeld *In dynamischen Datenträger konvertieren* wählen Sie die Kontrollkästchen der Datenträger, die Sie konvertieren möchten (Abbildung 12.5).

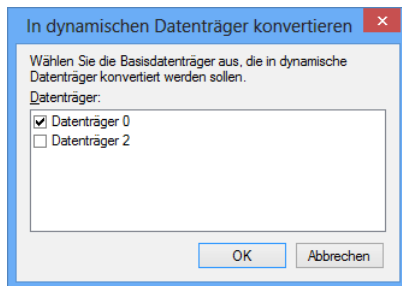


Abbildung 12.5 Wählen Sie den Basisdatenträger aus, der konvertiert werden soll

3. Wenn es auf dem zu konvertierenden Datenträger keine formatierten Volumes gibt, führt Antippen oder Anklicken von OK zur Umwandlung des Datenträgers und Sie brauchen die folgenden Schritte nicht durchzuführen. Gibt es bereits formatierte Volumes auf dem zu konvertierenden Datenträger, öffnet sich nach dem Anklicken oder Antippen von OK das Dialogfeld *Zu konvertierende Datenträger* und Sie müssen die folgenden Schritte durchführen, um die Konvertierung abzuschließen.
4. Das Dialogfeld *Zu konvertierende Datenträger* zeigt die Datenträger an, die konvertiert werden sollen, damit Sie die Umwandlung bestätigen können. Beachten Sie bitte den Wert in der Spalte *Wird konvertiert*. Dort sollte *Ja* stehen, wenn der Datenträger die Konvertierungskriterien erfüllt. Tippen oder klicken Sie auf *Details*, wenn Sie sich ansehen möchten, welche Volumes der ausgewählte Datenträger enthält. Wenn Sie die Konvertierung fortsetzen möchten, tippen oder klicken Sie auf OK, um das Dialogfeld *Konvertierungsdetails* zu schließen.

5. Um die Konvertierung einzuleiten, tippen oder klicken Sie auf *Konvertieren*. Die Datenträgerverwaltung weist Sie darauf hin, dass Sie ältere Versionen von Windows nach der Konvertierung nicht mehr von den Volumes der ausgewählten Datenträger starten können. Tippen oder klicken Sie auf *Ja*, wenn Sie fortfahren möchten.
6. Dann werden Sie eventuell darauf hingewiesen, dass die Bereitstellung der Dateisysteme auf den zu konvertierenden Datenträgern aufgehoben werden muss. Das bedeutet, dass der Datenträger offline genommen wird und zeitweilig nicht mehr verwendet werden kann. Tippen oder klicken Sie auf *Ja*, um fortzufahren. Enthält der gewählte Datenträger die Startpartition, die Systempartition oder eine in Verwendung befindliche Partition, muss die Datenträgerverwaltung den Computer neu starten und Sie erhalten eine weitere Meldung.

Zur Umwandlung eines dynamischen Datenträgers in einen Basisdatenträger gehen Sie so vor:

1. Bevor Sie einen dynamischen Datenträger in einen Basisdatenträger konvertieren können, müssen Sie alle dynamischen Volumes auf dem Datenträger löschen. Weil die enthaltenen Daten dadurch verloren gehen, sollten Sie die Volumes sichern und überprüfen, ob die Datensicherungen in Ordnung sind, bevor Sie die Umwandlung durchführen.
2. Wenn Sie die Konvertierung vorbereitet haben, starten Sie die Datenträgerverwaltung. Klicken Sie den Datenträger, den Sie konvertieren möchten, mit der rechten Maustaste an in der Datenträgerverwaltung oder halten Sie ihn gedrückt, und wählen Sie *In einen Basisdatenträger konvertieren*. Dadurch wird der dynamische Datenträger in einen Basisdatenträger konvertiert und Sie können dann neue Partitionen und logische Laufwerke auf dem Datenträger erstellen.

Verwenden von Datenträgern, Partitionen und Volumes

Bevor Sie auf einem Festplattenlaufwerk Daten speichern können, müssen Sie das Laufwerk vorbereiten, indem Sie einen Datenträgertyp festlegen, die Festplatte partitionieren, passende Laufwerksbezeichner vergeben und die Partitionen oder Volumes formatieren.

Nach der Formatierung müssen Sie jeder Partition oder jedem Volume einen Laufwerksbezeichner zuweisen. Dabei kann es sich um einen Buchstaben oder um einen Pfad handeln. Mit den Laufwerksbuchstaben können Sie die Dateisysteme in den verschiedenen Partitionen der Festplattenlaufwerke ansprechen. Zur Verfügung stehen im Prinzip die Laufwerksbuchstaben A bis Z. Allerdings ist A gewöhnlich bereits an das Diskettenlaufwerk vergeben. Ist der Computer mit einem zweiten Diskettenlaufwerk oder einem anderen Wechsellaufwerk ausgerüstet, erhält dies gewöhnlich den Buchstaben B (oder B bleibt unbenutzt). Die erste Partition oder das erste Volume auf Datenträger 0 erhält gewöhnlich den Buchstaben C. Der Laufwerksbuchstabe D wird gewöhnlich an das erste CD-ROM- oder DVD-ROM-Laufwerk vergeben. In der Praxis sind auf den meisten Systemen daher nur noch die Laufwerksbuchstaben E bis Z verfügbar. Wenn Sie zusätzliche Volumes brauchen, können Sie sie mit Laufwerkspfaden anlegen.

Ein Laufwerkspfad gibt einen bestimmten Ordner auf einem bereits vorhandenen Laufwerk an. Sie könnten zum Beispiel zusätzliche Laufwerke als *C:\Dokumente1*, *C:\Dokumente2* und *C:\Dokumente3* einrichten. Laufwerkspfade können für Basisdatenträger und für dynamische Datenträger verwendet werden. Die einzige Beschränkung ist, dass ein Laufwerkspfad auf einen leeren Ordner verweisen muss, der auf einem lokalen, mit NTFS formatierten Datenträger liegt.

Durch die Formatierung erhält eine Partition oder ein Volume ein Dateisystem mit den erforderlichen Grundstrukturen zur Verwaltung von Dateien. Unter Windows können Sie eine Partition oder ein Volume gewöhnlich mit FAT, FAT32 oder NTFS formatieren. Jedes dieser Dateisysteme stellt bestimmte Anforderungen und hat bestimmte Grenzen.

FAT (auch FAT16 genannt) ist ein 16-Bit-Dateisystem, das für Volumegrößen bis zu 4 GByte entwickelt wurde. FAT verwendet einen Startsektor, in dem Informationen über die Art des Datenträgers, Anfangs- und Endsektoren und die aktive Partition gespeichert sind. FAT hat seinen Namen von der Dateizuordnungstabelle (engl. File Allocation Table) erhalten, die es für die Zuordnung der Zuordnungseinheiten zu Dateien und Ordnern verwendet. Es gibt eine Haupttabelle und ein Duplikat. Das Duplikat kann zur Wiederherstellung der Haupttabelle dienen, falls diese beschädigt wird. Außerdem ist FAT in der Lage, Zuordnungseinheiten (das sind kleine Abschnitte des Datenträgers, in denen Daten liegen) als unbenutzt, belegt, unbrauchbar oder reserviert zu kennzeichnen. Das macht FAT zu einem ziemlich robusten Dateisystem. Am besten ist FAT für Volumes geeignet, die 2 GByte oder kleiner sind. Die maximale Dateigröße beträgt 2 GByte. FAT kann auf Disketten und Wechselmedien verwendet werden.

FAT32 ist eine 32-Bit-Version von FAT16 und verfügt über einige zusätzliche Features und Fähigkeiten. Wie FAT16 verwendet FAT32 eine primäre Dateizuordnungstabelle und ein Duplikat. Auch FAT32 kann Zuordnungseinheiten als unbenutzt, belegt, unbrauchbar oder reserviert kennzeichnen und lässt sich ebenfalls auf Wechselmedien verwenden. Im Gegensatz zu FAT16 beträgt die Mindestgröße eines FAT32-Volumes 33 MByte, die Maximalgröße 32 GByte und die maximale Dateigröße 4 GByte. exFAT ist eine erweiterte 64-Bit-Version von FAT.

Um die Geschwindigkeit und andere Vorteile von FAT zu nutzen, können Sie auf Volumes, die größer als 32 GByte sind, exFAT verwenden. Windows 8 unterstützt exFAT auf internen und externen Volumes.

HINWEIS Die Begrenzung der Dateigröße auf 4 GByte unter FAT32 ist seit Windows 2000 in Kraft. Mit FAT32 können einige frühere Windows-Versionen und auch andere Betriebssysteme größere Volumes anlegen.

NTFS unterscheidet sich sehr stark von FAT. Statt in einer Dateizuordnungstabelle verwaltet NTFS die Informationen über Dateien und Ordner in einer relationalen Datenbank. Diese Datenbank wird MFT (Master File Table) genannt und enthält einen Datensatz über jede Datei und jeden Ordner des Volumes sowie zusätzliche Informationen für die Verwaltung des Volumes. Insgesamt ist NTFS durch die MFT wesentlich zuverlässiger und im Falle eines Fehlers besser wiederherstellbar als FAT16 oder FAT32. Das bedeutet, dass sich NTFS leichter von Laufwerksfehlern erholt als FAT16 und FAT32 und dass sich unter NTFS ganz allgemein weniger Probleme mit den Datenträgern ergeben.

Einen Teil dieser Robustheit hat auch exFAT zu bieten, das Transaktionen verwendet, um die Zuverlässigkeit und Wiederherstellbarkeit zu verbessern. NTFS und exFAT weisen bei Standardlaufwerken eine maximale Volumegröße von 256 TByte auf und eine maximale Dateigröße, die nur durch die Volumegröße beschränkt wird.

Auf Disketten können Sie NTFS oder exFAT zwar nicht einsetzen, aber auf bestimmten anderen Wechselmedien. Außerdem bietet exFAT im Gegensatz zu FAT16 und FAT32, die als Sicherheitsvorkehrung Dateien lediglich als schreibgeschützt, als verborgen oder als Systemdatei kennzeichnen können, eine einfache Zugriffskontrolle. Allerdings verfügt nur NTFS über ein erweitertes Sicherheitssystem, in dem Sie die Zugriffsberechtigungen auf Dateien und Ordner sehr genau festlegen können. Und nur NTFS unterstützt noch andere wichtige Funktionen wie Komprimierung, Verschlüsselung und Kontingente.

HINWEIS Es gibt verschiedene NTFS-Versionen. Mit Windows 2000 wurde NTFS 5 eingeführt. Unter Windows XP wurde NTFS 5.1 verfügbar. Da die meisten aktuellen Computer NTFS 5 oder höher verwenden, möchte ich mich in diesem Buch auf NTFS 5 und höher konzentrieren. Wenn Sie ein System mit einer älteren Windows-Version aktualisieren, erhalten Sie bei der Installation normalerweise die Gelegenheit, die vorhandenen NTFS-Volumes in die neusten Versionen zu konvertieren. In den meisten Fällen ist dies auch sinnvoll, da Sie dann die neusten NTFS-Funktionen verwenden können. Wenn Sie

die NTFS-Version eines Volumes ermitteln möchten, geben Sie in einer Eingabeaufforderung mit erhöhten Rechten folgenden Befehl ein:

```
fsutil fsinfo ntfsinfo c:
```

Darin ist C: der Bezeichner des Laufwerks, das Sie überprüfen möchten. Wenn die interne NTFS-Version als 3.1 aufgelistet wird, arbeiten Sie tatsächlich mit NTFS 5.1.

Partitionieren und Vorbereiten von Festplattenlaufwerken

Die Datenträgerverwaltung ist das wichtigste Werkzeug für die Partitionierung und Vorbereitung von Festplattenlaufwerken. Mit der Datenträgerverwaltung können Sie Festplatten partitionieren, Laufwerksbezeichner zuweisen und Partitionen oder Volumes formatieren. Die Gegenstücke zur Datenträgerverwaltung auf der Befehlszeile sind DiskPart für die Partitionierung und Zuweisung der Laufwerksbezeichner sowie Format für die Formatierung.

Erstellen von Partitionen, logischen Laufwerken und einfachen Volumes

Windows 8 vereinfacht die Benutzeroberfläche der Datenträgerverwaltung durch die Verwendung derselben Dialogfelder und Assistenten für Partitionen und Volumes. Die ersten drei Volumes eines Basisdatenträgers werden automatisch als primäre Partitionen erstellt. Wenn Sie versuchen, auf einem Basisdatenträger ein viertes Volume zu erstellen, wird der übrige freie Platz des Datenträgers automatisch in eine erweiterte Partition umgewandelt, die einen logischen Datenträger in der von Ihnen angegebenen Größe enthält. Alle weiteren Volumes, die Sie anlegen, werden automatisch in der erweiterten Partition erstellt.

HINWEIS

Wie bereits erwähnt, kann ein MBR-Datenträger vier primäre Partitionen haben. Wenn Sie allerdings eine vierte primäre Partition erstellt haben, können Sie den Datenträger nicht mehr weiter unterteilen. Aus diesem Grund erstellt Windows 8 automatisch eine erweiterte Partition. Innerhalb dieser erweiterten Partition können Sie mehrere logische Laufwerke anlegen.

In der Datenträgerverwaltung erstellen Sie mit folgenden Schritten Partitionen, logische Laufwerke und einfache Volumes:

1. Klicken Sie in der grafischen Ansicht der Datenträgerverwaltung mit der rechten Maustaste auf einen nicht zugeordneten oder freien Bereich, oder halten Sie ihn gedrückt, und wählen Sie dann *Neues einfaches Volume*. Dadurch wird der Assistent zum Erstellen neuer einfacher Volumes gestartet. Lesen Sie die Willkommenseite und tippen oder klicken Sie auf *Weiter*.
2. Auf der Seite *Volumegröße festlegen* (Abbildung 12.6) können Sie die minimale und maximale Größe des Volumes in MByte ablesen und die Größe des neuen Volumes innerhalb dieser Grenzen angeben. Legen Sie die gewünschte Größe im Feld *Größe des einfachen Volumes in MB* fest und tippen oder klicken Sie auf *Weiter*.

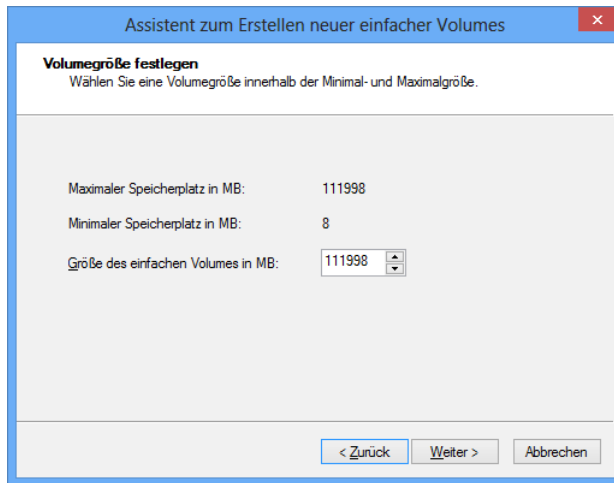


Abbildung 12.6 Geben Sie die Größe des neuen Volumes an

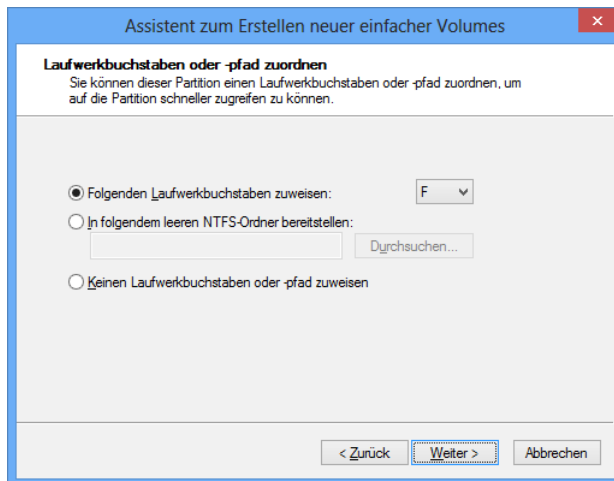


Abbildung 12.7 Weisen Sie einen Laufwerksbezeichner zu oder verschieben Sie die Zuweisung auf später

3. Auf der Seite *Laufwerksbuchstaben oder -pfad zuordnen* (Abbildung 12.7) geben Sie den gewünschten Laufwerksbuchstaben oder Pfad an und tippen oder klicken dann auf *Weiter*. Es sind folgende Optionen verfügbar:
 - **Folgenden Laufwerksbuchstaben zuweisen** Wählen Sie einen Buchstaben aus der Liste aus. Standardmäßig wählt Windows 8 den ersten verfügbaren Buchstaben aus, wobei es reservierte Laufwerksbuchstaben ebenso ausschließt wie Buchstaben, die bereits lokalen Laufwerken und Netzlaufwerken zugewiesen wurden.
 - **In folgendem leeren NTFS-Ordner bereitstellen** Wählen Sie diese Option, wenn Sie die Partition in einem leeren NTFS-Ordner bereitstellen möchten. Dann geben Sie den Pfad eines vorhandenen Ordners ein oder tippen oder klicken auf *Durchsuchen*, um einen Ordner herauszusuchen oder neu anzulegen.

- **Keinen Laufwerksbuchstaben oder -pfad zuweisen** Wählen Sie diese Option, wenn Sie eine Partition erstellen möchten, ohne ihr einen Laufwerksbuchstaben oder Pfad zuzuweisen. Wenn Sie die Partition später für die Datenspeicherung verfügbar machen möchten, können Sie ihr dann einen Laufwerksbuchstaben oder Pfad zuweisen.

HINWEIS Volumes müssen keine Laufwerksbuchstaben oder Pfade zugewiesen bekommen. Ein Volume ohne Bezeichner wird als nicht bereitgestellt eingestuft und ist für praktische Zwecke nicht zu gebrauchen. Ein nicht bereitgestelltes Volume kann später durch die Zuweisung eines Laufwerksbuchstabens oder Pfads bereitgestellt werden. Weitere Einzelheiten finden Sie im Abschnitt »Zuweisen, Ändern oder Entfernen von Laufwerksbuchstaben und Laufwerkspfaden« dieses Kapitels.

4. Verwenden Sie die Seite *Partition formatieren* (Abbildung 12.8), um festzulegen, ob und wie das Volume formatiert werden soll. Wenn das Volume formatiert werden soll, wählen Sie *Dieses Volume mit folgenden Einstellungen formatieren* und konfigurieren folgende Optionen:
 - **Zu verwendendes Dateisystem** Legt als Dateisystem FAT, FAT32 oder NTFS fest. NTFS ist in den meisten Fällen vorgewählt. Wenn Sie das Dateisystem FAT oder FAT32 wählen, können Sie es später mit dem Programm Convert in NTFS konvertieren. NTFS-Partitionen lassen sich aber nicht in FAT oder FAT32 konvertieren.

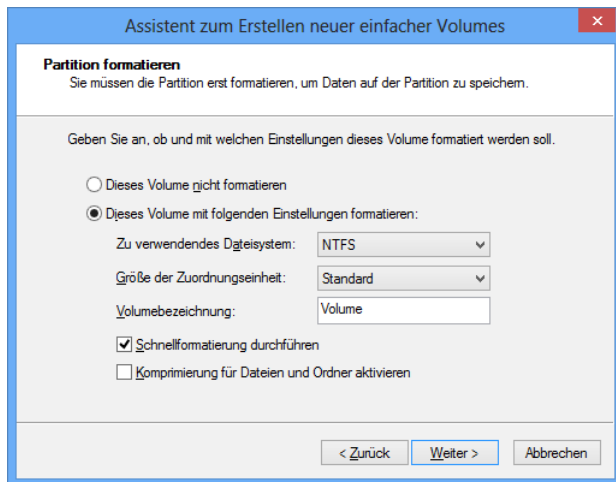


Abbildung 12.8 Stellen Sie die Formatierungsoptionen für die Partition ein

- **Größe der Zuordnungseinheit** Legt die Größe einer Zuordnungseinheit im Dateisystem fest. Das ist die Basiseinheit für die Verwaltung des Speicherplatzes auf dem Datenträger. Die Standardgröße einer Zuordnungseinheit hängt vom gewählten Dateisystem und von der Größe des Volumes ab und wird vor der Formatierung ermittelt. Wenn Sie eine bestimmte Größe einstellen möchten, können Sie das tun. Wenn Sie viele kleine Dateien verwenden, möchten Sie vielleicht einen kleineren Wert einstellen, beispielsweise 512 oder 1024 Byte. Mit kleineren Zuordnungseinheiten belegen kleine Dateien weniger Platz.

- **Volumebezeichnung** Legt eine Bezeichnung oder Beschriftung für die Partition fest. Diese Bezeichnung ist der Name des Volumes, wobei *Volume* als Standardname vorgegeben wird. Sie können den Namen jederzeit ändern, indem Sie das Volume im Datei-Explorer mit der rechten Maustaste anklicken oder es gedrückt halten, *Eigenschaften* wählen und im Namensfeld der Registerkarte *Allgemein* einen neuen Namen eingeben.
 - **Schnellformatierung durchführen** Weist Windows 8 an, eine schnelle Formatierung durchzuführen, ohne die Partition auf Fehler zu überprüfen. Bei großen Partitionen kann diese Option einige Minuten Zeit einsparen. Allerdings ist es besser, eine Überprüfung auf Fehler vorzunehmen. Dadurch kann die Datenträgerverwaltung beschädigte Zuordnungseinheiten erkennen und von der Verwendung ausschließen.
 - **Komprimierung für Dateien und Ordner aktivieren** Schaltet die Komprimierung des Volumes ein. Die integrierte Komprimierung ist nur für NTFS verfügbar. Unter NTFS erfolgt die Komprimierung ohne Zutun des Benutzers und komprimierte Dateien werden wie gewöhnliche Dateien verwendet. Wenn Sie diese Option wählen, werden Dateien und Verzeichnisse des Laufwerks automatisch komprimiert. Weitere Informationen über das Komprimieren von Laufwerken, Dateien und Verzeichnissen finden Sie im Abschnitt »Komprimieren von Datenträgern und Daten« weiter unten in diesem Kapitel.
5. Tippen oder klicken Sie auf *Weiter*, überprüfen Sie Ihre Einstellungen und tippen oder klicken Sie dann auf *Fertig stellen*.

Erstellen von übergreifenden und Stripesetvolumes

Mit übergreifenden Volumes und Stripesetvolumes können Sie Volumes erstellen, die sich über mehrere Festplattenlaufwerke erstrecken. Wenn Sie solche Volumes erstellen, berücksichtigen Sie bitte Folgendes:

- Ein übergreifendes Volume verwendet freien Speicherplatz von mehreren Datenträgern desselben Typs. Wenn auf zwei oder mehr Datenträgern desselben Typs noch Platz frei ist, können Sie diesen Platz zu einem übergreifenden Volume zusammenfassen. Ein übergreifendes Volume ist nicht fehlertolerant und weist eine durchschnittliche Schreib-/Leseleistung auf. Dateien werden so auf dem verfügbaren Platz angeordnet, als handle es sich um ein einziges großes Volume. Wenn eines der beteiligten Festplattenlaufwerke ausfällt, fällt auch das ganze Volume aus und die Daten sind alle verloren.
- Ein Stripesetvolume verwendet freien Speicherplatz von mehreren Festplattenlaufwerken und teilt die Daten beim Schreiben nach einem bestimmten Schema auf die Laufwerke auf. Dadurch ergeben sich schnellere Schreib- und Lesezugriffe, weil mehrere Laufwerke gleichzeitig Daten schreiben und lesen. Auf einem Stripeset, der sich über drei Datenträger erstreckt, werden die Daten aus einer Datei zum Beispiel erst auf Datenträger 1 geschrieben, dann auf Datenträger 2 und schließlich auf Datenträger 3, jeweils in 64-KByte-Blöcken. Wie ein übergreifendes Volume ist auch ein Stripesetvolume nicht fehlertolerant. Wenn also eines der beteiligten Festplattenlaufwerke ausfällt, fällt das ganze Volume aus und die Daten sind alle verloren. Dieser Lösungsansatz wird ebenfalls RAID 0 genannt.
- Ein Stripesetvolume mit Parität verwendet drei oder mehr Volumes, die auf verschiedenen Festplatten liegen, um einen Stripeset mit Parität zu erstellen. Fällt ein Festplattenlaufwerk aus, lassen sich die Daten trotzdem noch wiederherstellen. Dieser Lösungsansatz, der auch RAID 5 genannt wird, bietet mit einem geringeren Speicherplatzaufwand als eine Volumespiegelung nicht nur Fehlertoleranz, sondern auch eine bessere Leseleistung als eine Spiegelung.

HINWEIS

Wenn Sie nur einen Datenträger zur Verfügung haben, können Sie keine übergreifenden Volumes oder Stripesetvolumes erstellen. Beachten Sie bitte auch, dass sich einfache Volumes und übergreifende Volumes erweitern lassen und dadurch größer werden. RAID 0-Volumes und RAID 5-Volumes lassen sich dagegen nicht erweitern. Wenn Sie also ein RAID 0-Volume oder ein RAID 5-Volume anlegen, sollten Sie die Größe wählen, die Sie auch verwenden möchten. Sonst müssen Sie das Stripesetvolume später löschen und neu erstellen. Außerdem sollten Start- und Systemvolumes nicht auf einem RAID 0- oder RAID 5-Laufwerk liegen. Verwenden Sie für diese Volumes nicht RAID 0 oder RAID 5.

WEITERE INFORMATIONEN

Um die gewünschte Fehlertoleranz zu erreichen, berechnet und speichert RAID 5 Paritätsinformationen mit den Datenblöcken. Fällt eines der am Stripeset beteiligten Laufwerke aus, lassen Sie die Daten mit diesen Paritätsinformationen wiederherstellen. Fallen zwei Laufwerke aus, reichen die Paritätsinformationen allerdings nicht mehr aus und Sie müssen das Volume aus einer Datensicherung wiederherstellen.

Übergreifende Volumes und Stripesetvolumes erstellen Sie folgendermaßen in der Datenträgerverwaltung:

1. Klicken Sie in der grafischen Ansicht der Datenträgerverwaltung mit der rechten Maustaste einen freien Bereich an oder halten Sie ihn gedrückt, und wählen Sie dann nach Bedarf *Neues übergreifendes Volume*, *Neues Stripesetvolume* oder *Neues RAID-5-Volume*. Lesen Sie die Willkommenseite und tippen oder klicken Sie dann auf *Weiter*. Denken Sie daran, dass Windows 8 zwar übergreifende und Stripesetvolumes auf Basisdatenträgern unterstützt, manche Basisdatenträger aber nicht als Mitglieder von übergreifenden oder Stripesetvolumes eingesetzt werden können.
2. Wählen Sie auf der Seite *Datenträger auswählen* die Datenträger aus, die Teil des Volumes werden sollen, und legen Sie die Größen der Segmente auf den Datenträgern fest. Die Datenträger müssen denselben Datenträgertyp haben, also entweder alle Basisdatenträger oder alle dynamische Datenträger sein. Tippen oder klicken Sie auf *Weiter*.

Im Listenfeld *Verfügbar* werden die verfügbaren dynamischen Datenträger angezeigt. Wählen Sie einen Datenträger aus und tippen oder klicken Sie dann auf *Hinzufügen*, um den Datenträger zur Liste *Ausgewählt* hinzuzufügen. Wenn Sie den falschen Datenträger ausgewählt haben, können Sie ihn in der Liste *Ausgewählt* auswählen und durch Tippen oder Klicken auf *Entfernen* wieder entfernen.

Legen Sie fest, wie viel Platz Sie von jedem Datenträger verwenden möchten. Dazu wählen Sie die Datenträger der Reihe nach in der Liste *Ausgewählt* aus und geben dann im Feld *Speicherplatz in MB* an, wie viel Platz verwendet werden soll. Berücksichtigen Sie dabei, dass das Textfeld *Maximal verfügbarer Speicherplatz in MB* die Größe des freien Bereichs auf dem ausgewählten Datenträger und das Textfeld *Gesamtgröße des Volumes in MB* die derzeit eingestellte Gesamtgröße des neuen Volumes angibt.

TIPP

Es gibt eine einfache Methode, um auf allen ausgewählten Datenträgern dieselbe Speichermenge zu verwenden. Markieren Sie alle beteiligten Datenträger, indem Sie die UMSCHALT-Taste drücken und dann in der Liste *Ausgewählt* den ersten und den letzten Datenträger anklicken. Wenn Sie nun den zu verwendenden Speicherplatz angeben, gilt diese Einstellung für alle ausgewählten Datenträger.

3. Folgen Sie den Schritten 3 bis 5 des vorigen Abschnitts »Erstellen von Partitionen, logischen Laufwerken und einfachen Volumes«.

Erweitern und Verkleinern von Volumes

Windows 8 verwendet für den Start des Betriebssystems nicht *Ntldr* und *Boot.ini*. Stattdessen verfügt Windows 8 über eine Pre-Boot-Umgebung, in welcher der Windows-Start-Manager zur Kontrolle des Systemstarts und zum Laden der von Ihnen gewählten Startanwendung verwendet wird. Außerdem erlöst der Windows-Start-Manager das Betriebssystem Windows von seiner Abhängigkeit von MS-DOS und ermöglicht es, die Laufwerke auf neue Weise zu verwenden. Unter Windows 8 ist es möglich, Basisdatenträger und dynamische Datenträger zu erweitern und zu verkleinern. Um Volumes zu erweitern oder zu verkleinern, können Sie die Datenträgerverwaltung oder DiskPart verwenden. Stripesetvolumes lassen sich aber weder erweitern noch verkleinern.

Zur Vergrößerung eines Volumes konvertieren Sie unbelegten Platz und fügen ihn zum vorhandenen Volume hinzu. Der Speicherplatz für ein übergreifendes Volume auf dynamischen Datenträgern kann von jedem verfügbaren dynamischen Datenträger stammen, nicht nur von denen, auf denen das Volume ursprünglich erstellt wurde. Sie können also den freien Platz von mehreren dynamischen Datenträgern dazu verwenden, um ein vorhandenes Volume zu erweitern.

ACHTUNG

Bevor Sie versuchen, ein Volume zu erweitern, müssen Sie die Beschränkungen kennen. Zum einen lassen sich einfache und übergreifende Volumes nur erweitern, wenn sie formatiert sind und es sich bei dem verwendeten Dateisystem um NTFS handelt. Stripesetvolumes können Sie nicht erweitern. Sie können auch keine Volumes erweitern, die mit FAT, FAT32 oder exFAT formatiert sind. Außerdem können Sie keine Systempartition und keine Startpartition erweitern (das ist nicht von der Konfiguration dieser Volumes abhängig).

Sie können ein Basisvolume, ein einfaches Volume oder ein übergreifendes Volume mit folgenden Schritten verkleinern:

1. Klicken Sie in der Datenträgerverwaltung mit der rechten Maustaste auf das Volume, das Sie verkleinern möchten, oder halten Sie es gedrückt, und wählen Sie dann *Volume verkleinern*. Diese Option ist nur verfügbar, wenn das Volume die bereits beschriebenen Kriterien erfüllt.

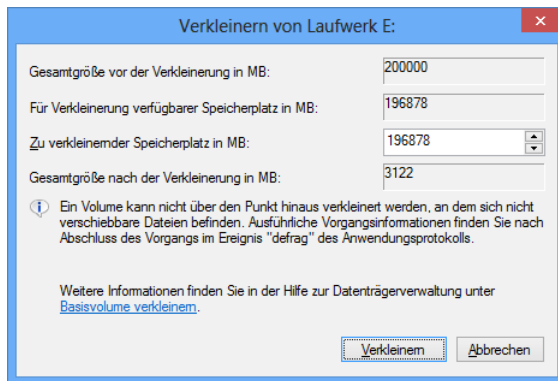


Abbildung 12.09 Legen Sie fest, um wie viel Speicherplatz das Volume verkleinert werden soll

2. Geben Sie im Dialogfeld *Verkleinern von Laufwerk* (Abbildung 12.9) an, um welchen Wert das Volume verkleinert werden soll. Das Dialogfeld *Verkleinern von Laufwerk* zeigt folgende Informationen:
 - **Gesamtgröße vor der Verkleinerung in MB** Zeigt die Gesamtkapazität des Volumes in MByte. Das ist die formatierte Größe des Volumes.
 - **Für Verkleinerung verfügbarer Speicherplatz in MB** Zeigt den höchsten Wert, um den das Volume verkleinert werden kann. Dieser Wert stellt nicht die Menge an freiem Speicherplatz dar, sondern die Menge an Speicherplatz, die weggenommen werden kann. Darin ist nicht der Platz enthalten, der für die Hauptdateitabelle (Master File Table, MFT), Volumeschattenkopien, Auslagerungsdateien und temporäre Dateien reserviert ist.
 - **Zu verkleinernder Speicherplatz in MB** Die Platzmenge, die vom Volume entfernt werden kann. Der Anfangswert entspricht der Gesamtmenge an Speicherplatz, die vom Volume entfernt werden kann. Damit das Volume eine gute Leistung liefern kann, sollten Sie dafür sorgen, dass nach der Verkleinerung noch mindestens 10 Prozent der resultierenden Kapazität an Speicherplatz frei ist.
 - **Gesamtgröße nach der Verkleinerung in MB** Zeigt die Gesamtgröße des Volumes in MByte nach der Verkleinerung. Das ist die neue formatierte Größe des Volumes.
3. Tippen oder klicken Sie auf *Verkleinern*.

Sie können ein Basisvolume, ein einfaches Volume oder ein übergreifendes Volume mit folgenden Schritten erweitern:

1. Klicken Sie in der Datenträgerverwaltung mit der rechten Maustaste auf das Volume, das Sie erweitern möchten, oder halten Sie es gedrückt, und wählen Sie dann *Volume erweitern*. Diese Option ist nur verfügbar, wenn das Volume die bereits beschriebenen Kriterien erfüllt und auf einem oder mehreren Datenträgern des Systems Speicherplatz unbelegt ist.
2. Lesen Sie die Einführungsmeldung des Assistenten zum Erweitern von Volumes und tippen oder klicken Sie dann auf *Weiter*.
3. Wählen Sie auf der Seite *Datenträger auswählen* den oder die Datenträger aus, auf die das Volume erweitert werden soll. Alle Datenträger, die bereits für das Volume verwendet werden, sind automatisch vorgewählt. Standardmäßig wird der gesamte noch unbelegte Platz auf diesen Datenträgern verwendet.
4. Sie können auch den freien Platz auf anderen Datenträgern mit einbeziehen, und zwar folgendermaßen:
 - Tippen oder klicken Sie im Listenfeld *Verfügbar* auf den Datenträger und dann auf *Hinzufügen*, um den Datenträger in die Liste *Ausgewählt* aufzunehmen.
 - Wählen Sie der Reihe nach jeden Datenträger in der Liste *Ausgewählt* und geben Sie im Textfeld *Speicherplatz in MB* die Speichermenge an, die auf dem ausgewählten Laufwerk verwendet werden soll.
5. Tippen oder klicken Sie auf *Weiter*, überprüfen Sie Ihre Einstellungen und tippen oder klicken Sie dann auf *Fertig stellen*.

Formatieren von Partitionen und Volumes

Wenn Sie eine Partition oder ein Volume formatieren, erstellen Sie dadurch ein Dateisystem, das zur Speicherung von Daten verwendet werden kann. Durch die Formatierung werden alle Daten endgültig gelöscht, die sich im betreffenden Abschnitt des Festplattenlaufwerks befinden. Dabei handelt es sich um

eine High-Level-Formatierung, die eine Dateisystemstruktur erstellt, und nicht um eine Grundformatierung, durch die ein Festplattenlaufwerk verwendungsfähig wird. (Neue Laufwerke werden initialisiert, wenn sie angeschlossen werden, sofern sie noch nicht vom Hersteller entsprechend vorbereitet wurden). Um eine Partition oder ein Volume zu formatieren, klicken Sie es in der Datenträgerverwaltung mit der rechten Maustaste an oder halten es gedrückt, und wählen *Formatieren*. Dadurch öffnet sich das Dialogfeld *Formatieren* (Abbildung 12.10). Wenn Sie Abbildung 12.8 mit 12.10 vergleichen, werden Sie feststellen, dass es sich im Wesentlichen um dieselben Optionen handelt.

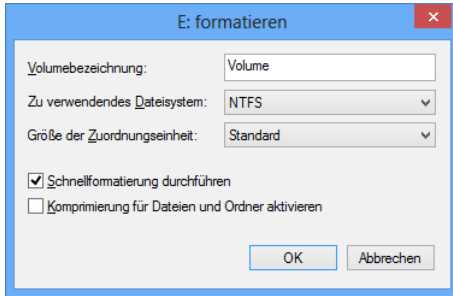


Abbildung 12.10 Verwenden Sie das Dialogfeld *Formatieren* zur Formatierung von Partitionen und Volumes. Sie können das gewünschte Dateisystem auswählen und einen Namen für das Volume festlegen

Nach der Wahl der gewünschten Werte tippen oder klicken Sie auf *OK*. Da alle in der Partition vorhandenen Daten durch die Formatierung zerstört werden, gibt Ihnen die Datenträgerverwaltung eine letzte Gelegenheit, den Vorgang abzubrechen. Tippen oder klicken Sie auf *OK*, wenn Sie die Formatierung durchführen möchten. Dann ändert die Datenträgerverwaltung den Status des Datenträgers, um den Formatierungsvorgang erkennbar zu machen, und gibt auch prozentual an, wie weit die Formatierung vorangeschritten ist, sofern Sie nicht die Option *Schnellformatierung durchführen* gewählt haben. Wenn die Formatierung abgeschlossen ist, wird der Status wieder entsprechend geändert.

Zuweisen, Ändern oder Entfernen von Laufwerksbuchstaben und Laufwerkspfad

Jeder primären Partition, jedem logischen Laufwerk und jedem Volume können ein Laufwerksbuchstabe und ein oder mehrere Laufwerkspfade zugewiesen werden, sofern die Laufwerkspfade auf leere NTFS-Ordner verweisen. Einmal zugewiesen, bleibt der Laufwerksbuchstabe oder der Laufwerkspfad bei jedem Start des Computers derselbe. Mit Ausnahme von Partitionen oder Volumes, die als System- oder Startpartition gekennzeichnet sind, können Sie den Laufwerksbuchstaben oder die Pfadzuweisung jederzeit ändern. Sie können den Laufwerksbuchstaben oder Laufwerkspfad auch entfernen, mit Ausnahme der Partitionen und Volumes, die als System- oder Startpartition gekennzeichnet sind.

Sie verwalten den Laufwerksbuchstaben oder Pfad einer Partition oder eines Volumes in der Datenträgerverwaltung. Klicken Sie in der Volumelisten- oder der grafischen Ansicht mit der rechten Maustaste auf die Partition oder das Volume, das Sie konfigurieren wollen, oder halten Sie die Partition oder das Volume gedrückt, und wählen Sie den Befehl *Laufwerksbuchstaben und -pfade ändern*. Dadurch wird ein Dialogfeld geöffnet (Abbildung 12.11). Nun können Sie folgende Arbeiten durchführen:

- **Hinzufügen eines Laufwerkspfads** Tippen oder klicken Sie auf *Hinzufügen*, wählen Sie *In folgendem leeren NTFS-Ordner bereitstellen* und geben Sie dann den Pfad eines vorhandenen Ordners an, oder tippen oder klicken Sie auf *Durchsuchen*, um einen Ordner herauszusuchen oder zu erstellen.
- **Entfernen eines Laufwerkspfads** Wählen Sie den zu entfernenden Laufwerkspfad aus, tippen oder klicken Sie erst auf *Entfernen* und dann auf *Ja*.
- **Zuweisen eines Laufwerksbuchstabens** Tippen oder klicken Sie auf *Hinzufügen*, wählen Sie *Folgenden Laufwerksbuchstaben zuweisen* und wählen Sie dann einen freien Laufwerksbuchstaben aus, den Sie dem Laufwerk zuweisen möchten.
- **Ändern des Laufwerksbuchstabens** Wählen Sie den aktuellen Laufwerksbuchstaben und tippen oder klicken Sie dann auf *Ändern*. Wählen Sie *Folgenden Laufwerksbuchstaben zuweisen* und suchen Sie dann einen anderen Laufwerksbuchstaben für den Datenträger aus.
- **Entfernen eines Laufwerksbuchstabens** Wählen Sie den aktuellen Laufwerksbuchstaben und tippen oder klicken Sie auf *Entfernen* und dann auf *Ja*.

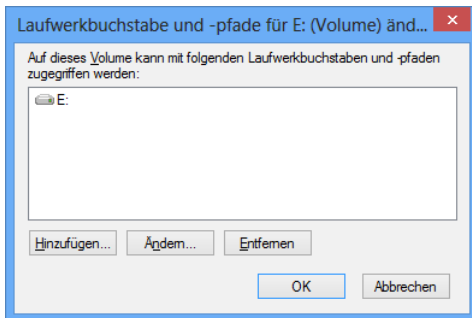


Abbildung 12.11 Hinzufügen, Ändern oder Entfernen von Laufwerksbuchstaben und -pfaden

HINWEIS Wenn Sie versuchen, den Buchstaben eines Laufwerks zu ändern, das verwendet wird, zeigt Windows 8 eine entsprechende Warnung an. Sie müssen die Programme beenden, die das betreffende Laufwerk verwenden, und den Versuch dann wiederholen. Oder Sie erlauben der Datenträgerverwaltung, die Änderung einfach durchzuführen, indem Sie in der Warnung auf *Ja* tippen oder klicken.

PRAXISTIPP Wenn der Laufwerksbuchstabe, den Sie verwenden wollen, nicht verfügbar ist, bedeutet dies, dass er bereits anderweitig verwendet wird. Manchmal lässt sich dieses Problem durch einen Tausch der Buchstaben lösen. Wird der Buchstabe D beispielsweise für das DVD-RW-Laufwerk verwendet und Laufwerk E: ist ein Volume auf einer lokalen Festplatte, können Sie die Buchstaben tauschen. Dann ist D das Volume auf der lokalen Festplatte und E das DVD-RW-Laufwerk. Dazu entfernen Sie zuerst den Laufwerksbuchstaben, der dem DVD-RW-Laufwerk zugewiesen wurde. Dann weisen Sie den freien Buchstaben D dem lokalen Volume zu. Dadurch wird das E frei, das Sie nun dem DVD-RW-Laufwerk zuweisen können. Vergessen Sie aber nicht, dass der Tausch von Laufwerksbuchstaben unerwartete Folgen haben kann. So könnte beispielsweise der Pfad einer Anwendung mit dem Laufwerksbuchstaben in die Registrierung eingetragen worden sein. Wenn Sie die Laufwerksbuchstaben vertauschen, gilt der Pfad natürlich nicht mehr. Verknüpfungen mit Dateien oder Programmen, die auf dem Laufwerk liegen, können ebenfalls von der Vertauschung der Laufwerksbuchstaben betroffen sein und müssen angepasst oder neu erstellt werden.

Zuweisen, Ändern oder Löschen einer Volumebezeichnung

Eine Volumebezeichnung ist ein Name für eine Partition oder ein Volume. Die Volumebezeichnung wird in verschiedenen Programmen von Windows 8 angezeigt, zum Beispiel im Datei-Explorer und in der Computerkonsole, und soll einen Hinweis auf den Inhalt des Datenträgers geben.

HINWEIS Bei FAT- und FAT32-Volumes darf die Volumebezeichnung bis zu 11 Zeichen lang sein und kann Leerzeichen enthalten, bei NTFS-Volumes darf sie bis zu 32 Zeichen lang sein. Volumebezeichnungen von NTFS-Volumes dürfen Sonderzeichen wie * / \ [] ; | = , . + " ? < > enthalten, bei FAT- und FAT32-Volumes ist das nicht erlaubt.

Volumebezeichnungen können Sie in der Computerverwaltung oder in der Computerkonsole zuweisen, ändern oder löschen. In der Computerverwaltung gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie die Computerverwaltung. Erweitern Sie den Knoten *Datenspeicher* und wählen Sie dann den Knoten *Datenträgerverwaltung*.
2. Klicken Sie in der Volumeliste mit der rechten Maustaste das Laufwerkssymbol an, mit dem Sie arbeiten möchten, oder halten Sie es gedrückt, und wählen Sie *Eigenschaften*.
3. Auf der Registerkarte *Allgemein* des *Eigenschaften*-Dialogfelds können Sie im Namensfeld einen neuen Namen für das Volume eingeben oder die vorhandene Bezeichnung löschen. Tippen oder klicken Sie dann auf *OK*.

In der Computerkonsole können Sie eine Volumebezeichnung folgendermaßen zuweisen, ändern oder löschen:

1. Um die Konsole *Computer* zu öffnen, tippen oder klicken Sie auf dem Desktop auf das *Explorer*-Symbol. Tippen oder klicken Sie im Datei-Explorer auf die Ortsauswahlschaltfläche und dann auf *Computer*.
2. Klicken Sie mit der rechten Maustaste auf das Laufwerkssymbol oder halten Sie es gedrückt, und wählen Sie *Eigenschaften*.
3. Auf der Registerkarte *Allgemein* des *Eigenschaften*-Dialogfelds können Sie im Namensfeld einen neuen Namen eingeben oder die vorhandene Bezeichnung löschen. Tippen oder klicken Sie dann auf *OK*.

Löschen von Partitionen, Volumes und logischen Laufwerken

Wenn Sie die Konfiguration eines Datenträgers ändern möchten, der bereits vollständig belegt ist, müssen Sie vorhandene Partitionen, logische Laufwerke oder Volumes löschen. Da diese Löschung nicht rückgängig gemacht werden kann, sollten Sie vorher immer eine Sicherung durchführen und eine Partition, ein logisches Laufwerk oder ein Volume vor dem Löschen auf wichtige Dateien und Ordner durchsehen. Wenn es auf dem Computer übergreifende Volumes oder Stripesetvolumes gibt, müssen Sie beim Löschen der Volumes sehr vorsichtig sein. Durch das Löschen eines Volumes aus einem Set wird das ganze Set gelöscht. Anders gesagt, das ganze Volume und alle darin enthaltenen Daten sind dann verloren.

ACHTUNG Das Löschen einer Partition, eines Laufwerks oder eines Volumes ist ein drastischer Schritt, der sich nicht rückgängig machen lässt. Dadurch wird das dazugehörige Dateisystem entfernt und die darin enthaltenen Daten gehen verloren.

HINWEIS

Damit das System nicht gefährdet wird, können Sie die System- und die Startpartition nicht löschen. Allerdings lässt Windows 8 es zu, dass Sie die aktive Partition oder das aktive Volume löschen, wenn es nicht als Startpartition oder Systempartition gekennzeichnet ist. Überprüfen Sie vorher immer, ob die Partition oder das Volume, das Sie löschen wollen, wichtige Daten oder Dateien enthält.

Mit folgenden Schritten können Sie eine primäre Partition, ein Volume oder ein logisches Laufwerk löschen:

1. Klicken Sie in der Datenträgerverwaltung mit der rechten Maustaste auf die Partition, das Volume oder Laufwerk, das Sie löschen möchten, oder halten Sie es gedrückt. Wählen Sie dann *Durchsuchen*. Kopieren Sie im Datei-Explorer alle Daten auf ein anderes Volume oder überprüfen Sie die Sicherungskopie, um sicherzustellen, dass die Daten ordnungsgemäß gespeichert wurden.
2. Klicken Sie in der Datenträgerverwaltung wieder mit der rechten Maustaste auf die Partition, das Volume oder das Laufwerk oder halten Sie es gedrückt, und wählen Sie *Volume löschen*.
3. Bestätigen Sie die geplante Löschung, indem Sie auf *Ja* tippen oder klicken.

Die Löschung einer erweiterten Partition unterscheidet sich etwas von der Löschung einer primären Partition oder eines logischen Laufwerks. Um eine erweiterte Partition zu löschen, müssen Sie zuerst alle darin enthaltenen logischen Laufwerke löschen, wie gerade beschrieben. Anschließend können Sie die erweiterte Partition auswählen und löschen.

Konvertieren eines Volumes nach NTFS

Zu Windows 8 gehört ein Befehlszeilenprogramm für die Konvertierung von FAT- und FAT32-Volumes in NTFS-Volumes. Dieses Programm namens *Convert* (*Convert.exe*) liegt im Ordner `%SystemRoot%\System32`. Wenn Sie ein Volume mit diesem Programm konvertieren, bleibt die Datei- und Verzeichnisstruktur erhalten und es gehen normalerweise keine Daten verloren.

ACHTUNG

Windows 8 bietet kein Programm für die Umwandlung von NTFS in FAT oder FAT32. Die einzige Möglichkeit, von NTFS zu FAT oder FAT32 zu gelangen, ist die Löschung der Partition, wie im vorigen Abschnitt beschrieben, und die anschließende Neuerstellung der Partition als FAT- oder FAT32-Volume. *Convert* kann auch keine exFAT-Volumes nach NTFS konvertieren.

Wenn Sie ein Laufwerk konvertieren möchten, geben Sie in einer Eingabeaufforderung mit erhöhten Rechten folgenden Befehl ein:

```
convert Volume /FS:NTFS
```

Darin ist *Volume* der Laufwerksbuchstabe, gefolgt von einem Doppelpunkt, oder ein Laufwerkspfad oder ein Volumenname. Wollen Sie zum Beispiel Laufwerk D: nach NTFS konvertieren, geben Sie folgenden Befehl ein:

```
convert D: /FS:NTFS
```

Die vollständige Syntax des Befehls *Convert* lautet:

```
convert Volume /FS:NTFS [/V] [/X] [/CvtArea:Dateiname] [/NoSecurity]
```

Die Optionen und Parameter bedeuten:

- **Volume** Gibt das zu konvertierende Volume an und muss als vollständiger Laufwerksbezeichner angegeben werden (Laufwerksbuchstabe, gefolgt von einem Doppelpunkt). Sie können auch einen Bereitstellungspunkt oder einen Volumenamen angeben.

- **/FS:NTFS** Gibt an, dass das Volume nach NTFS konvertiert wird. Das ist die einzige Dateisystemoption.
- **/V** Die Konvertierung erfolgt mit ausführlicheren Kommentaren.
- **/X** Hebt die Bereitstellung des Volumes auf, sofern erforderlich.
- **/CvtArea:Dateiname** Gibt eine möglichst zusammenhängende Datei aus dem Stammverzeichnis als Platzhalter für die Dateien des NTFS-Dateisystems an, insbesondere für die MFT. Wenn Sie keine Datei angeben, verwendet Convert die Standardkonfiguration und reserviert 12,5 Prozent der Partition oder des Volumes. Dadurch soll die Fragmentierung der MFT verhindert werden.
- **/NoSecurity** Nimmt die NTFS-Sicherheitseinstellungen an den Dateien und Ordnern so vor, dass die Gruppe *Jeder* darauf zugreifen kann. Dadurch wird das ganze Dateisystem für jeden zugänglich, der sich lokal oder remote am Computer anmelden kann.

Vor der Konvertierung überprüft der Befehl Convert, ob auf dem Volume ausreichend freier Platz zur Verfügung steht. Im Allgemeinen braucht Convert einen freien Speicherblock, der ungefähr 25 Prozent des belegten Speicherplatzes entspricht. Wenn ein Laufwerk beispielsweise 10 GByte Daten speichert, braucht Convert ungefähr 2,5 GByte freien Platz. Ist nicht genug Platz frei, bricht Convert den Vorgang mit der Aufforderung ab, mehr Platz zu schaffen. Steht genügend Platz zur Verfügung, führt Convert die Umwandlung durch. Sie müssen etwas Geduld haben, denn die Konvertierung kann einige Minuten dauern (auf großen Laufwerken entsprechend länger). Verwenden Sie keine Dateien oder Anwendungen auf dem Laufwerk, während die Konvertierung läuft.

HINWEIS

Bevor Sie das Programm Convert verwenden, sollten Sie noch einmal überprüfen, ob die Partition als aktive Systempartition oder als Startpartition dient, die das Betriebssystem enthält. Auf MBR-Laufwerken können Sie die aktive Systempartition nach NTFS konvertieren. Dazu braucht das System aber exklusiven Zugriff auf diese Partition, den es nur beim Start erhält. Wenn Sie also versuchen, die aktive Systempartition nach NTFS zu konvertieren, zeigt Convert eine Meldung an, in der Sie gefragt werden, ob Sie das Laufwerk beim nächsten Start des Systems konvertieren möchten. Wenn Sie mit *Ja* antworten, wird die Systempartition beim nächsten Neustart konvertiert. Meistens sind mehrere Neustarts erforderlich, damit ein System die aktive Systempartition vollständig konvertieren kann. Kein Grund zur Panik, lassen Sie das System einfach machen.

PRAXISTIPP

Sie können die Leistung eines Volumes verbessern, indem Sie mit der Option **/CvtArea** Platz für die MFT reservieren. Dadurch soll die Fragmentierung der MFT verhindert werden. Worum geht es? Im Lauf der Zeit wird die MFT vielleicht mehr Platz beanspruchen, als für sie reserviert wurde. Dann muss das Betriebssystem die MFT in andere Bereiche des Datenträgers erweitern. Das Defragmentierungsprogramm von Windows 8 kann zwar auch die MFT defragmentieren, aber es kann den ersten Abschnitt der MFT nicht verschieben, und es ist sehr unwahrscheinlich, dass direkt im Anschluss an die MFT Platz frei ist. Vermutlich stehen dort irgendwelche Dateien.

Um der Fragmentierung der MFT vorzubeugen, möchten Sie vielleicht mehr Platz als die üblichen 12,5 Prozent der Partitions- oder Volumekapazität reservieren. Sie könnten zum Beispiel mehr Platz für die MFT reservieren, wenn viele kleine Dateien auf dem Volume gespeichert werden sollen statt der üblichen Mischung aus kleinen und großen Dateien. Um den zu reservierenden Platz festzulegen, können Sie mit FSUtil eine Platzhalterdatei in der gewünschten Größe anlegen. Anschließend können Sie das Volume nach NTFS konvertieren und mit der Option **/CvtArea** den Namen der Platzhalterdatei angeben.

In diesem Beispiel verwende ich FSUtil, um eine Platzhalterdatei namens *Temp.txt* mit einer Größe von 1.5 GByte (das sind 1.500.000.000 Byte) anzulegen:

```
fsutil file createnew c:\temp.txt 1500000000
```

Um diese Platzhalterdatei bei der Konvertierung von Laufwerk C: nach NTFS für die MFT zu verwenden, würden Sie folgenden Befehl eingeben:

```
convert c: /fs:ntfs /cvtarea:temp.txt
```

Beachten Sie bitte, dass die Platzhalterdatei in der Partition oder in dem Volume angelegt werden muss, das konvertiert werden soll. Während der Konvertierung wird die Datei mit NTFS-Metadaten überschrieben, und der restliche Platz, der in der Datei noch frei bleibt, wird für die zukünftige Verwendung durch die MFT reserviert.

Wiederherstellen eines einfachen, übergreifenden oder Stripesetvolumes

Probleme mit Basispartitionen und einfachen Volumes sind recht einfach zu beheben, weil nur ein Laufwerk beteiligt ist. Übergreifende Volumes oder Stripesetvolumes können sich dagegen über mehrere Festplattenlaufwerke erstrecken, und der Ausfall einer Festplatte macht das ganze Volume unbrauchbar, wenn keine Paritätsdaten zur Verfügung stehen. Der Laufwerkstatus kann als *Fehlend*, *Fehler*, *Online (Fehler)*, *Offline* oder *Nicht lesbar* ausgewiesen werden.

Sie sehen den Status *Fehlend* (und gelegentlich *Offline*), wenn die Verbindung zu Laufwerken getrennt oder die Laufwerke abgeschaltet wurden. Handelt es sich um ein externes Speichergerät, sollten Sie die Kabelverbindungen und die Stromversorgung überprüfen. Eine erneute Verbindung sollte die Laufwerke wieder zugänglich machen – manchmal soll auch schon das simple Einschalten geholfen haben. Dann müssen Sie die Datenträgerverwaltung starten und das fehlende Laufwerk neu einlesen. Klicken Sie mit der rechten Maustaste auf das fehlende Laufwerk oder halten Sie es gedrückt, und wählen Sie *Datenträger neu einlesen*. Wenn die Datenträgerverwaltung fertig ist, klicken Sie wieder mit der rechten Maustaste auf das Laufwerk oder halten es gedrückt, und wählen *Datenträger reaktivieren*. Die Statusangaben *Fehler*, *Online (Fehler)* oder *Nicht lesbar* können auftreten, wenn ein Laufwerk E/A-Probleme hat. Versuchen Sie auch in solchen Fällen, das Laufwerk neu einzulesen und zu reaktivieren. Wird das Laufwerk nicht in den Zustand *Fehlerfrei* zurückversetzt, ist es vielleicht an der Zeit, es durch ein neues zu ersetzen.

TIPP

Gelegentlich ist es erforderlich, den Computer neu zu starten, damit ein Laufwerk wieder online ist. Wenn auch das nicht das Problem löst, überprüfen Sie das Laufwerk, seinen Controller und die Kabel. Sorgen Sie auch dafür, dass die Stromversorgung angeschlossen und eingeschaltet ist.

Wiederherstellen eines Stripesets mit Parität

Ein RAID-5-Stripeset lässt sich wiederherstellen, falls ein Festplattenlaufwerk ausfällt. Ob ein Laufwerk aus dem Stripeset mit Parität ausgefallen ist, erkennen Sie daran, dass sich die Statusangabe auf *Fehlerhafte Redundanz* ändert und der Status des betreffenden Volumes auf *Fehlend*, *Offline* oder *Online (Fehler)* wechselt.

Sie können RAID-5-Volumes wiederherstellen. Allerdings müssen Sie Festplatten mit derselben Partitionstabellenart verwenden, entweder MBR oder GPT. Dazu müssen alle Laufwerke des RAID-5-Festplattensatzes online sein. Der Status des Sets sollte *Fehlerhafte Redundanz* sein. Was Sie nun zur Wiederherstellung tun können, hängt vom Status des ausgefallenen Volumes ab.

- Lautet der Status *Fehlend* oder *Offline*, sorgen Sie dafür, dass das Laufwerk richtig angeschlossen ist und Strom erhält. Dann öffnen Sie die Datenträgerverwaltung, klicken das ausgefallene Volume mit der rechten Maustaste an oder halten es gedrückt, und wählen *Volume erneut aktivieren*. Der Status des Laufwerks sollte sich auf *Wird neu erzeugt* und dann auf *Fehlerfrei* ändern.

- Ist der Status *Online (Fehler)*, klicken Sie das ausgefallene Laufwerk mit der rechten Maustaste an oder halten es gedrückt, und wählen *Volume erneut aktivieren*. Der Status des Laufwerks sollte sich auf *Wird neu erzeugt* und dann auf *Fehlerfrei* ändern. Falls sich der Status nicht in *Fehlerfrei* ändert, klicken Sie das Volume mit der rechten Maustaste an oder halten es gedrückt, und wählen *Parität erneut erzeugen*.
- Wird eines der Laufwerke als *Nicht lesbar* ausgewiesen, müssen Sie die Laufwerke vielleicht neu einlesen. Wählen Sie dazu im Menü *Aktion* der Datenträgerverwaltung *Datenträger neu einlesen*. Wenn sich der Laufwerksstatus nicht ändert, müssen Sie den Computer vielleicht neu starten.
- Lässt sich eines der Laufwerke nicht in den Zustand *Online* versetzen, müssen Sie den ausgefallenen Bereich des RAID-5-Sets ersetzen. Klicken Sie den ausgefallenen Datenträger mit der rechten Maustaste an oder halten Sie ihn gedrückt, und wählen Sie dann *Datenträger entfernen*. Nun müssen Sie für den RAID-5-Set auf einer weiteren dynamischen Festplatte einen nicht belegten Speicherbereich auswählen. Der Bereich muss so groß sein wie der zu ersetzende Bereich und kann nicht auf einem der Laufwerke liegen, die bereits im RAID-5-Set verwendet werden. Steht nicht genügend Platz zur Verfügung, ist der Befehl *Volume reparieren* nicht verfügbar und Sie müssen für weiteren freien Speicherplatz sorgen, indem Sie andere Volumes löschen oder das ausgefallene Laufwerk ersetzen.

PRAXISTIPP Sofern möglich, sollten Sie die Daten vor diesen Wiederherstellungsmaßnahmen sichern. Dann können Sie Ihre Daten auch wiederherstellen, falls sich weitere Probleme ergeben.

Verwenden der Datenträgerspiegelung

Bei der Datenträgerspiegelung verwenden Sie gleich große Volumes auf zwei unterschiedlichen Laufwerken, um einen Datensatz doppelt zu erstellen. Auf die beiden Datenträger werden dieselben Daten geschrieben. Sollte eine Festplatte ausfallen, können Sie die Daten immer noch von der anderen lesen.

Die Datenträgerspiegelung bietet zwar Fehlertoleranz, ihr Hauptnachteil besteht aber darin, dass sie die Größe des Speicherplatzes halbiert. Um eine 500 GByte große Festplatte zu spiegeln, benötigen Sie weitere 500 GByte. Sie verwenden also 1000 GByte Speicherplatz, um 500 GByte Daten zu speichern.

Erstellen von gespiegelten Volumes

Gehen Sie folgendermaßen vor, um einen Spiegelsatz zu erstellen:

1. Klicken Sie in der grafischen Ansicht der Datenträgerverwaltung mit der rechten Maustaste auf einen als *Nicht zugeordnet* markierten Bereich eines dynamischen Datenträgers oder halten Sie ihn gedrückt, und wählen Sie danach *Neues gespiegeltes Volume*. Der *Assistent zum Erstellen neuer gespiegelter Volumes* wird gestartet. Lesen Sie den Begrüßungsdialog und tippen oder klicken Sie auf *Weiter*.
2. Erstellen Sie das Volume, wie im Abschnitt »Erstellen von übergreifenden und Stripesetvolumes« weiter vorne in diesem Kapitel beschrieben. Der Hauptunterschied besteht darin, dass Sie zwei gleich große Volumes erstellen müssen, die sich auf unterschiedlichen Datenträgern befinden. Sie können auf der Seite *Datenträger auswählen* erst fortfahren, wenn Sie die beiden Festplatten ausgewählt haben, mit denen Sie arbeiten möchten.
3. Wie die anderen RAID-Techniken erfolgt die Spiegelung für den Benutzer unbemerkt. Benutzer verwenden den Spiegelsatz wie ein einzelnes Laufwerk, auf das sie wie auf alle anderen Laufwerke zugreifen können.

HINWEIS

Eine normale Spiegelung hat den Status »Fehlerfrei«. Während der Erstellung der Spiegelung kann der Status »Die Synchronisation wird wiederholt« angezeigt werden. Damit wird Ihnen mitgeteilt, dass die Datenträgerverwaltung die Spiegelung einrichtet.

Sie müssen einen Spiegelsatz nicht von Grund auf neu erstellen, sondern können dazu auch ein bereits vorhandenes Volume verwenden. Dabei muss es sich um eine Basispartition oder ein einfaches Volume handeln, und ein zweiter Datenträger muss einen Bereich mit nicht zugeordnetem Speicherplatz besitzen, der größer oder gleich dem Speicherplatz auf dem vorhandenen Volume ist.

Gehen Sie folgendermaßen vor, um ein vorhandenes Volume in der Datenträgerverwaltung zu spiegeln:

1. Klicken Sie mit der rechten Maustaste auf die Basispartition oder das Volume, das Sie spiegeln wollen, oder halten Sie sie gedrückt, und wählen Sie *Spiegelung hinzufügen* aus. Das Dialogfeld *Spiegelung hinzufügen* wird geöffnet.
2. Wählen Sie im Listenfeld *Datenträger* einen Speicherort für die Spiegelung und tippen oder klicken Sie auf *Spiegelung hinzufügen*. Windows 8 startet die Einrichtung der Spiegelung. In der Datenträgerverwaltung wird für beide Volumes der Status *Die Synchronisation wird wiederholt* angezeigt. Der Datenträger, auf dem das gespiegelte Volume erstellt wird, ist mit einem Warnsymbol markiert.

Aufheben der Spiegelung

Es gibt manchmal Gründe, einen Spiegelsatz wieder aufzutrennen. Wenn Sie Ihre Laufwerke nicht mehr spiegeln wollen, können Sie die Spiegelung aufheben, damit der Festplattenplatz für andere Zwecke frei wird. Fällt eine der Festplatten aus einem Spiegelsatz aus, laufen die Datenträgeroperationen weiter, aber früher oder später müssen Sie den Spiegelsatz reparieren, und dazu müssen Sie die Spiegelung aufheben und dann neu einrichten. Obwohl beim Aufheben einer Spiegelung keine Daten im Satz gelöscht werden, sollten Sie zuvor Sicherungskopien erstellen. Damit wird sichergestellt, dass Sie die Daten im Fall eines Problems wiederherstellen können.

Gehen Sie folgendermaßen vor, um einen Spiegelsatz in der Datenträgerverwaltung aufzutrennen:

1. Klicken Sie mit der rechten Maustaste auf eines der Volumes im Spiegelsatz oder halten Sie es gedrückt, und wählen Sie den Befehl *Gespiegeltes Volume aufteilen*.
2. Bestätigen Sie die Aufhebung der Spiegelung, indem Sie auf *Ja* tippen oder klicken. Sollte das Volume gerade verwendet werden, wird ein weiteres Warndialogfeld angezeigt. Bestätigen Sie durch Klicken auf *Ja*, dass Sie fortfahren möchten.

Windows 8 hebt die Spiegelung auf und erstellt zwei unabhängige Volumes. (Sie brauchen eine Spiegelung nicht aufzuteilen, bevor Sie die Spiegelung entfernen. Bei der Entfernung bricht Windows die Spiegelung automatisch auf.)

Entfernen eines Spiegelsatzes

In der Datenträgerverwaltung können Sie eines der Volumes aus einem Spiegelsatz entfernen. Dabei werden alle Daten auf der entfernten Spiegelung gelöscht und der von ihnen belegte Speicherplatz als *Nicht zugeordnet* markiert.

Zum Entfernen einer Spiegelung gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf eines der Volumes im Spiegelsatz oder halten Sie es gedrückt, und wählen Sie den Befehl *Spiegelung entfernen*. Daraufhin öffnet sich das Dialogfeld *Spiegelung entfernen*.

2. Wählen Sie im Dialogfeld *Spiegelung entfernen* den Datenträger, von dem die Spiegelung entfernt werden soll, und tippen oder klicken Sie auf *Spiegelung entfernen*.
3. Bestätigen Sie nach Aufforderung die Aktion. Alle Daten auf der entfernten Spiegelung werden gelöscht.

Einbauen eines dynamischen Datenträgers in einen anderen Computer

Ein wichtiger Vorteil von dynamischen Datenträgern gegenüber Basisdatenträgern ist, dass sie sich leicht in andere Computer einbauen lassen. Wenn Sie zum Beispiel einen Computer eingerichtet haben und dann zu dem Schluss kommen, dass Sie das zusätzliche Festplattenlaufwerk nicht wirklich brauchen, können Sie es ziemlich leicht in einen anderen Computer einbauen, in dem es besser genutzt wird. Vor dem Ausbau eines Festplattenlaufwerks und dem Einbau im neuen Computer sollten Sie Folgendes tun:

1. Öffnen Sie auf dem Computer, auf dem der dynamische Datenträger installiert ist, die Datenträgerverwaltung und überprüfen Sie die Statusangaben der Datenträger. Der Status sollte *Fehlerfrei* sein. Ist er es nicht, beheben Sie etwaige Probleme, bevor Sie eine Festplatte herausnehmen.

ACHTUNG Datenträger mit BitLocker-Laufwerkverschlüsselung lassen sich nicht auf diese Weise in andere Computer einbauen. Windows 8 Pro und Enterprise bieten die BitLocker-Laufwerkverschlüsselung, die das Laufwerk in gewisser Weise versiegelt, damit Offline-Manipulationen erkannt werden und dazu führen, dass das Laufwerk nicht verwendbar ist, bis ein Administrator es entriegelt. Weitere Informationen zur BitLocker-Laufwerkverschlüsselung finden Sie in Kapitel 11, »Arbeiten mit TPM und BitLocker-Laufwerkverschlüsselung«.

2. Überprüfen Sie die Festplattensubsysteme des Originalcomputers und des Computers, in den Sie das Laufwerk einbauen möchten. Beide Computer müssen identische Festplattensubsysteme aufweisen. Tun sie es nicht, passt die Plug & Play-Kennung des Systemlaufwerks vom Originalcomputer nicht zu dem, was der Zielcomputer erwartet. Folglich ist der Zielcomputer nicht in der Lage, die richtigen Treiber zu laden, und der Startvorgang könnte fehlschlagen.
3. Prüfen Sie, ob einer der Datenträger, den Sie ausbauen, Teil eines übergreifenden oder erweiterten Volumes oder eines Stripesetvolumes ist. Ist dies der Fall, schreiben Sie sich am besten auf, welcher Datenträger Teil welches Sets ist, und planen Sie den Umbau aller beteiligten Festplattenlaufwerke ein. Wenn Sie nur einen Teil eines Sets umbauen, sollten Sie sich über die Konsequenzen im Klaren sein. Wenn Sie einen Teil eines übergreifenden oder erweiterten Volumes oder eines Stripesetvolumes entfernen, wird das betreffende Volume auf dem Originalcomputer unbrauchbar, aus dem Sie ein Laufwerk ausbauen, und ist auch nicht auf dem Zielcomputer zu gebrauchen.

Wenn Sie die Vorbereitungen abgeschlossen haben, tun Sie Folgendes:

1. Starten Sie auf dem Originalcomputer die Computerverwaltung. Wählen Sie in der Strukturdarstellung den *Geräte-Manager*. Erweitern Sie in der Geräteliste *Laufwerke*. Dadurch wird eine Liste aller Festplattenlaufwerke sichtbar, die im Computer installiert sind. Klicken Sie mit der rechten Maustaste auf jedes Laufwerk, das Sie ausbauen möchten, oder halten Sie es gedrückt, und wählen Sie dann *Deinstallieren*. Wenn Sie sich nicht sicher sind, um welche Laufwerke es sich handelt, klicken Sie jedes Laufwerk mit der rechten Maustaste an oder halten es gedrückt, und wählen *Eigenschaften*. Wählen Sie im *Eigenschaften*-Dialogfeld die Registerkarte *Volumes* und tippen oder klicken Sie dann auf *Aktualisieren*. Dann sehen Sie, welche Volumes auf dem ausgewählten Laufwerk liegen.

2. Öffnen Sie in der Computerverwaltung des Originalcomputers nun die Datenträgerverwaltung. Klicken Sie mit der rechten Maustaste auf jedes Laufwerk, das Sie ausbauen möchten, oder halten Sie es gedrückt, und wählen Sie dann *Datenträger entfernen*.
3. Wenn Sie damit fertig sind, können Sie die Festplattenlaufwerke ausbauen. Sind die Laufwerke bei laufendem Computer austauschbar und wird diese Funktion auf beiden Computern unterstützt, entfernen Sie die Laufwerke aus dem Originalcomputer und bauen sie in den Zielcomputer ein. Andernfalls fahren Sie beide Computer herunter, schalten sie aus, bauen die Laufwerke aus dem Originalcomputer aus und in den Zielcomputer ein. Wenn Sie fertig sind, fahren Sie die Computer wieder hoch.
4. Öffnen Sie auf dem Zielcomputer die Datenträgerverwaltung und wählen Sie im Menü *Aktion* den Befehl *Datenträger neu einlesen*. Wenn die Datenträgerverwaltung mit der Untersuchung der Laufwerke fertig ist, klicken Sie jedes Laufwerk, das als *Fremd* gekennzeichnet ist, mit der rechten Maustaste an oder halten es gedrückt, und wählen *Fremde Datenträger importieren*. Nun sollten Sie auf dem Zielcomputer auf die Laufwerke und ihre Volumes zugreifen können.

HINWEIS

Die Volumes auf dem dynamischen Datenträger sollten die Laufwerksbuchstaben behalten, die sie auf dem Originalcomputer hatten. Wird einer der Laufwerksbuchstaben bereits auf dem Zielcomputer verwendet, erhält das betreffende Volume den nächsten freien Laufwerksbuchstaben. Wurde einem dynamischen Volume noch kein Laufwerksbuchstabe zugewiesen, erhält es durch den Einbau in einen anderen Computer nicht automatisch einen. Außerdem werden die Volumes nicht automatisch bereitgestellt, wenn die automatische Bereitstellung deaktiviert ist. Dann müssen Sie selbst für die Bereitstellung der Volumes sorgen und ihnen Laufwerksbuchstaben zuweisen.

Beseitigung auftretender Datenträgerprobleme

Windows 8 macht während des Starts und im Normalbetrieb intensiven Gebrauch von Festplattenlaufwerken. Durch eine Optimierung der Festplattenlaufwerke eines Computers lässt sich die Leistung des Betriebssystems und der Anwendung manchmal erstaunlich verbessern. Konzentrieren Sie sich auf die Verwendung des Speicherplatzes, auf Laufwerksfehler und auf die Dateifragmentierung. Vielleicht sollten Sie auch eine Komprimierung der Dateien in Erwägung ziehen, um den Platzbedarf der Datendateien zu verringern und Platz für zusätzliche Dateien zu schaffen.

HINWEIS

Laufwerksverwaltungsprogramme wie die Datenträgerbereinigung, die Datenträgerprüfung und die Defragmentierung nutzen die neue Ressourcenpriorisierung von Windows 8, wie im Abschnitt »Funktionsweise und Verwendung von Windows-SuperFetch« weiter oben in diesem Kapitel beschrieben. Dadurch können diese Programme im Hintergrund laufen und die Leerlaufzeiten des Systems ausnutzen, mit dem Ergebnis, dass der Benutzer eine ziemlich konstante Systemleistung zur Verfügung hat, obwohl im Hintergrund Wartungsprogramme laufen.

Überwachen Sie auf allen Systemlaufwerken die Speicherplatzbelegung. Werden die Laufwerke zu voll, können ihre Leistung und die Leistung des Systems insgesamt zurückgehen, besonders dann, wenn der Platz für die Speicherung von Auslagerungsdateien oder temporären Dateien knapp wird. Die Speicherplatzbelegung lässt sich zum Beispiel mit der Datenträgerbereinigung verringern, indem überflüssige Dateien gelöscht und alte Dateien komprimiert werden. Einzelheiten über dieses Programm erfahren Sie im Abschnitt »Arbeiten mit der Datenträgerbereinigung« von Kapitel 2. Damit Sie die Benutzer nicht ständig an die Verwendung der Datenträgerbereinigung erinnern müssen, können Sie eine automatische Ausführung vorsehen, wie im Abschnitt »Planen von Wartungsarbeiten« in Kapitel 10 beschrieben.

Mit der Datenträgerverwaltung können Sie die Zustände der Laufwerke und ihrer Volumes überprüfen. Der Laufwerkszustand wird in der grafischen Ansicht unter der Bezeichnung des Datenträgers und in der Datenträgerliste in der Spalte *Status* angezeigt. Der Volumestatus wird in der grafischen Ansicht im Rahmen der allgemeinen Angaben über das Volume und in der Volumeliste in der Spalte *Status* angezeigt.

Tabelle 12.2 Bedeutung von Laufwerkstatusmeldungen und Problembhebung

Status	Beschreibung	Lösung
Online	Der normale Datenträgerstatus. Er bedeutet, dass das Laufwerk verfügbar ist und keine Probleme hat.	Das Laufwerk weist keine bekannten Probleme auf. Sie brauchen nichts zu reparieren.
Online (Fehler)	Auf einem Datenträger wurden E/A-Fehler festgestellt.	Sie können versuchen, temporäre Fehler zu beheben, indem Sie das Laufwerk mit der rechten Maustaste anklicken oder gedrückt halten und <i>Datenträger reaktivieren</i> wählen. Funktioniert das nicht, ist das Laufwerk vielleicht beschädigt. Führen Sie einen gründlichen Test des Laufwerks durch.
Offline	Das Laufwerk ist nicht verfügbar. Vielleicht ist es zerstört oder zeitweilig nicht verfügbar. Wenn sich der Laufwerkstatus in <i>Fehlend</i> ändert, ist das Laufwerk im System nicht mehr zu erkennen.	Überprüfen Sie das Laufwerk, den Controller und die Kabel. Sorgen Sie dafür, dass das Laufwerk richtig angeschlossen ist und über Strom verfügt. Versuchen Sie, das Laufwerk mit dem Befehl <i>Datenträger reaktivieren</i> wieder online zu bringen (sofern möglich).
Fremd	Das Laufwerk wurde zwar an Ihren Computer angeschlossen, aber noch nicht importiert. Ein ausgefallenes Laufwerk, das wieder online ist, wird manchmal als <i>Fremd</i> aufgeführt.	Klicken Sie das Laufwerk mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie <i>Fremde Datenträger importieren</i> , um das Laufwerk zum System hinzuzufügen.
Nicht lesbar	Das Laufwerk ist derzeit nicht verfügbar. Das kann geschehen, wenn Laufwerke erneut eingelesen werden.	Bei FireWire-/USB-Kartenlesern wird dieser Status vielleicht angezeigt, wenn die Karte nicht oder falsch formatiert ist oder aus dem Leser entfernt wurde. Wenn sich das Laufwerk nicht einlesen lässt, ist es vielleicht defekt oder weist E/A-Fehler auf. Klicken Sie das Laufwerk mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie <i>Datenträger neu einlesen</i> (auch im Menü <i>Aktion</i> verfügbar), um das Problem zu beheben. Vielleicht müssen Sie das System auch neu starten.
Nicht erkannt	Das Laufwerk ist von einem unbekannten Typ und kann nicht im System verwendet werden. Ein Laufwerk von einem Nicht-Windows-System kann so angezeigt werden.	Wenn das Laufwerk von einem anderen Betriebssystem stammt, unternehmen Sie gar nichts. Sie können das Laufwerk nicht im Computer verwenden. Nehmen Sie ein anderes.
Nicht initialisiert	Das Laufwerk hat keine gültige Signatur. Ein Laufwerk von einem Nicht-Windows-System kann so angezeigt werden.	Wenn das Laufwerk von einem anderen Betriebssystem stammt, unternehmen Sie gar nichts. Sie können das Laufwerk nicht im Computer verwenden. Nehmen Sie ein anderes. Um das Laufwerk für die Verwendung unter Windows 8 vorzubereiten, klicken Sie das Laufwerk mit der rechten Maustaste an oder halten es gedrückt, und wählen <i>Datenträger initialisieren</i> .
Kein Medium	Es wurde kein Datenträger in das DVD-ROM-Laufwerk oder das Wechseldatenträgerlaufwerk eingelegt, oder das Medium wurde entfernt. Dieser Status wird nur für DVD-ROM-Laufwerke und Wechseldatenträgerlaufwerke angezeigt.	Legen Sie eine DVD oder das passende Wechselmedium ein, um das Laufwerk online zu bringen. Bei FireWire-/USB-Kartenlesern wird dieser Status gewöhnlich, aber nicht immer angezeigt, wenn die Karte entfernt wird.

Tabelle 12.2 beschreibt Statusmeldungen für Laufwerke und schlägt Maßnahmen zur Behebung des Problems vor.

Tabelle 12.3 beschreibt Statusmeldungen für Volumes und schlägt Maßnahmen zur Behebung des Problems vor.

Tabelle 12.3 Bedeutung von Volumestatusmeldungen und Problembehebung

Status	Beschreibung	Lösung
Daten nicht redundant	Fehlertolerante Volumes auf einem Fremd-datenträger sind unvollständig. Sie müssen vergessen haben, die anderen Datenträger aus einem Spiegelsatz hinzuzufügen.	Fügen Sie die restlichen Datenträger hinzu und importieren Sie alle Datenträger gleichzeitig.
Die Daten sind nicht vollständig	Übergreifende Volumes auf einem Fremd-datenträger sind unvollständig. Sie müssen vergessen haben, einen anderen Datenträger aus dem übergreifenden Volumesatz hinzuzufügen.	Fügen Sie den Datenträger hinzu, der den Rest des übergreifenden Volumes enthält, und importieren Sie alle Datenträger gleichzeitig.
Die Synchronisation wird wiederholt	Ein vorübergehender Zustand, der angibt, dass ein Spiegelsatz neu synchronisiert wird.	Der Fortschritt wird als Prozentsatz angezeigt. Danach sollte das Volume wieder den Status »Fehlerfrei« aufweisen.
Fehler	Ein Fehlerstatus. Das Laufwerk ist nicht verfügbar oder beschädigt.	Sorgen Sie dafür, dass das Laufwerk online ist, klicken Sie das Laufwerk bei Bedarf mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie <i>Datenträger reaktivieren</i> . Klicken Sie das Volume mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie <i>Volume erneut aktivieren</i> . Überprüfen Sie, ob das Laufwerk richtig angeschlossen ist.
Fehlerfrei	Der normale Status eines Volumes.	Das Laufwerk weist keine bekannten Probleme auf. Sie brauchen nichts zu reparieren.
Fehlerfrei (Risiko)	Windows hat Probleme bei Lese- oder Schreibzugriffen auf das Laufwerk gehabt, auf dem das Volume liegt. Dieser Status wird angezeigt, wenn Fehler aufgetreten sind.	Klicken Sie das Laufwerk mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie <i>Datenträger reaktivieren</i> . Wird das Laufwerk weiterhin mit diesem Status angezeigt oder erscheint diese Statusanzeige gelegentlich, könnte das Laufwerk vollständig ausfallen. Sie sollten alle auf dem Laufwerk gespeicherten Daten sichern.
Fehlerfrei (Unbekannte Partition)	Windows erkennt die Partition nicht. Das kann geschehen, wenn die Partition von einem anderen Betriebssystem angelegt wurde. Oder die Partition wurde vom Hersteller angelegt und dient zur Speicherung von Systemdateien.	Es sind keine Reparaturen erforderlich.
Fehlerhafte Redundanz	Fehlertolerante Laufwerke sind nicht mehr synchron.	Sie können versuchen, die Laufwerke wieder zu synchronisieren, indem Sie das fehlerhafte Volume mit der rechten Maustaste anklicken oder gedrückt halten, und <i>Volume erneut aktivieren</i> wählen.
Formatierung	Ein temporärer Status. Er bedeutet, dass das Volume gerade formatiert wird.	Der Fortschritt der Formatierung wird in Prozent angezeigt, sofern Sie nicht die Option <i>Schnellformatierung durchführen</i> gewählt haben.
Initialisierung	Ein temporärer Status. Er bedeutet, dass das Laufwerk initialisiert wird.	Der Laufwerkstatus sollte sich nach wenigen Sekunden ändern. ►

Status	Beschreibung	Lösung
Unbekannt	Das Volume ist nicht verfügbar. Vielleicht ist der Startsektor beschädigt.	Vielleicht ist das Volume von einem Startsektorvirus befallen. Überprüfen Sie es mit einem aktuellen Virens Scanner. Ist kein Virus zu finden, starten Sie das System von der Windows 8-DVD und verwenden den Befehl <i>fixmbr</i> der Wiederherstellungskonsole zur Wiederherstellung des MBR (Master Boot Record).
Veraltete Daten	Fehlertolerante Daten auf Fremddatenträgern sind nicht synchronisiert.	Lesen Sie die Datenträger neu ein, oder starten Sie den Computer neu und überprüfen Sie anschließend den Status. Ein neuer Status sollte angezeigt werden, wie zum Beispiel »Fehlerhafte Redundanz«.

Reparieren von Fehlern und Inkonsistenzen auf Datenträgern

Windows 8 bietet verbesserte Funktionen, die den manuellen Wartungsaufwand für Festplattenlaufwerke verringern. Die folgenden Verbesserungen haben die deutlichsten Auswirkungen auf Ihre Arbeit mit Datenträgern:

- Transaktionales NTFS
- Selbstheilendes NTFS

Transaktionales NTFS erlaubt es, Dateioperationen auf einem NTFS-Volume transaktional durchzuführen. Das bedeutet, dass Programme eine Transaktion einsetzen können, um ganze Sätze von Datei- und Registrierungsoperationen so zusammenzufassen, dass sie entweder alle erfolgreich abgeschlossen oder alle rückgängig gemacht werden. Während eine Transaktion aktiv ist, werden die Änderungen außerhalb der Transaktion noch nicht sichtbar. Die Änderungen werden erst bestätigt und vollständig auf den Datenträger geschrieben, wenn die Transaktion erfolgreich abgeschlossen wurde. Falls eine Transaktion fehlschlägt oder unvollständig war, macht das Programm die transaktionalen Operationen rückgängig, um das Dateisystem in den Zustand zurückzusetzen, den es vor der Transaktion hatte.

Transaktionen, die mehrere Volumes betreffen, werden vom Kernel Transaction Manager (KTM) gesteuert. Der KTM unterstützt die unabhängige Wiederherstellung von Volumes für den Fall, dass eine Transaktion fehlschlägt. Der lokale Ressourcenmanager für ein Volume verwaltet ein separates Transaktionsprotokoll und hat die Aufgabe, Threads für Transaktionen von den Threads getrennt zu halten, die die Dateioperationen ausführen.

Früher mussten Sie das Tool Datenträgerprüfung verwenden, um Fehler und Inkonsistenzen in NTFS-Volumes eines Datenträgers zu reparieren. Weil dieser Vorgang die Verfügbarkeit von Windows-Systemen beeinträchtigen kann, setzt Windows 8 ein selbstheilendes NTFS (engl. Self-Healing NTFS) ein, um Probleme im Dateisystem zu reparieren, ohne dass dafür separate Wartungstools eingesetzt werden müssen. Weil der Großteil des Selbstheilungsprozesses automatisch aktiviert und durchgeführt wird, brauchen Sie nur noch bei der Volumewartung tätig zu werden, wenn Sie vom Betriebssystem benachrichtigt werden, dass sich ein Problem nicht automatisch beheben lässt. Falls ein solcher Fehler auftritt, informiert Windows 8 Sie über das Problem und bietet mögliche Lösungen an.

Selbstheilendes NTFS bietet viele Vorteile gegenüber der Datenträgerprüfung, zum Beispiel:

- Die Datenträgerprüfung braucht exklusiven Zugriff auf Volumes. Das bedeutet, dass System- und Startvolumes nur geprüft werden können, bevor das Betriebssystem startet. Beim selbstheilenden NTFS steht das Dateisystem dagegen immer zur Verfügung und muss in den meisten Fällen nicht offline repariert werden.

- Selbstheilendes NTFS versucht, so viele Daten wie möglich zu retten, falls ein Fehler aufgetreten ist. Es reduziert fehlerhafte Dateisystembereitstellungen, die vorher auftreten konnten, wenn ein Volume bekannte Fehler oder Inkonsistenzen aufwies. Beim Neustart repariert das selbstheilende NTFS das Volume sofort, damit es bereitgestellt werden kann.
- Selbstheilendes NTFS meldet, welche Reparaturen es am Volume vorgenommen hat. Das geschieht über vorhandene *Chkdsk.exe*-Mechanismen, Verzeichnisbenachrichtigungen und USN-Journaleinträge (Update Sequence Number). Das ermöglicht es autorisierten Benutzern und Administratoren, die Reparaturoperationen zu überwachen. Sie erhalten dabei Meldungen, die angeben, dass überprüft oder auf den Abschluss von Reparaturen gewartet wird und wie weit der jeweilige Vorgang fortgeschritten ist.
- Selbstheilendes NTFS kann ein Volume nicht wiederherstellen, falls ein NTFS-Volume vorliegt, aber der Startsektor nicht lesbar ist. In diesem Fall müssen Sie ein Offlinetool ausführen, das den Startsektor repariert. Anschließend kann das selbstheilende NTFS die Wiederherstellung einleiten.

Selbstheilendes NTFS ist eine großartige Verbesserung, aber manchmal kann es sinnvoll (oder unvermeidbar) sein, die Integrität eines Datenträgers von Hand zu überprüfen. In diesen Fällen können Sie die Datenträgerprüfung (*Chkdsk.exe*) verwenden, um Probleme auf FAT-, FAT32- und NTFS-Volumes aufzuspüren und bei Bedarf zu beseitigen. Die Datenträgerprüfung sucht und korrigiert zwar viele Arten von Fehlern, doch wird hauptsächlich nach Inkonsistenzen im Dateisystem und in den zugehörigen Metadaten gesucht. Darüber hinaus ist der Nutzen des Dienstprogramms jedoch eher beschränkt.

Prüfen auf Laufwerksfehler

Im Rahmen der automatischen Wartung führt Windows 8 eine vorsorgliche Untersuchung der NTFS-Volumes Ihres Computers durch. Wie andere Teile der automatischen Wartung überprüft Windows Festplatten mit der Datenträgerprüfung um 3 Uhr nachts, wenn der Computer am Stromnetz angeschlossen ist und das Betriebssystem nichts zu tun hat. Ist dies nicht möglich, überprüft Windows die Laufwerke bei der nächsten Gelegenheit, wenn der Computer am Stromnetz angeschlossen ist und das Betriebssystem sich im Leerlauf befindet. Wenn Sie diesen Zeitplan ändern möchten, müssen Sie die Laufzeit für die automatische Wartung anders einstellen, wie im Abschnitt »Anpassen von *Hilfe und Support*« von Kapitel 9, »Verwalten von Hardwaregeräten und Treibern«, beschrieben. Die automatische Wartung löst zwar die Überprüfung der Laufwerke aus, aber die Datenträgerprüfung wird von einer separaten Aufgabe aufgerufen und verwaltet. In der Aufgabenplanung finden Sie die Aufgabe *ProactiveScan* in der Aufgabenplanungsbibliothek unter *Microsoft\Windows\Chkdsk*. Ausführliche Angaben über die bisherigen Läufe finden Sie auf der Registerkarte *Verlauf*.

Sie sollten die Integrität der Volumes regelmäßig mit der Datenträgerprüfung (*Chkdsk.exe*) überprüfen. Die Datenträgerprüfung überprüft Volumes und kann viele Fehlerarten beheben, die auf FAT16-, FAT32-, exFAT- und NTFS-Volumes gelegentlich auftreten. Die Datenträgerprüfung vergleicht zum Beispiel die Volumebitmap mit den Zuordnungseinheiten, die den Dateien aus dem Dateisystem zugeordnet sind, und erkennt auf diese Weise Abweichungen. Allerdings kann die Datenträgerprüfung keine zerstörten Daten in Dateien reparieren, deren äußerliche Struktur intakt ist. Sie können die Datenträgerprüfung auf einer Befehlszeile oder in einer grafischen Schnittstelle starten.

Unter Windows 8 führt die Datenträgerprüfung anders als auf älteren Windows-Versionen eine erweiterte Überprüfung und gegebenenfalls eine automatische Reparatur durch. Wenn Sie also NTFS-Volumes überprüfen, führt die Datenträgerprüfung eine Online-Überprüfung und Analyse durch, um Laufwerksfehler zu erkennen. Sie schreibt Informationen über erkannte Schäden in die Systemdatei *\$corrupt*. Wird das Volume benutzt, lassen sich erkannte Schäden vielleicht reparieren, wenn das Volume offline ge-

schaltet wird. Allerdings werden die offenen Dateihandles dadurch ungültig. Was die Start- und Systemvolumes betrifft, werden Reparaturen beim nächsten Start des Computers durchgeführt.

Die Speicherung der Schadensmeldungen und eine Reparatur, während das Volume nicht an das Betriebssystem angeschlossen ist, ermöglicht Windows eine schnelle Reparatur des Volumes. Außerdem ermöglicht dieses Verfahren Ihnen, das Laufwerk weiter zu verwenden, während es überprüft wird. Gewöhnlich dauert die Offline-Reparatur nur wenige Sekunden. Die alten Untersuchungs- und Reparaturmethoden würden im Vergleich dazu bei großen Volumes Stunden beanspruchen.

FAT, FAT32 und exFAT (FAT-Volumes) unterstützen diese erweiterten Funktionen nicht. Wenn Sie die Datenträgerprüfung auf FAT-Volumes anwenden, verwendet Windows 8 die alten Überprüfungs- und Reparaturmethoden. Das bedeutet, dass das Volume gewöhnlich offline geschaltet werden muss und vorerst nicht benutzt werden darf.

Ausführen der Datenträgerprüfung in der Befehlszeile

Sie können die Datenträgerprüfung in einer Eingabeaufforderung mit erhöhten Rechten starten oder sie in anderen Programmen ausführen. Wenn Sie in einer Eingabeaufforderung mit erhöhten Rechten beispielsweise Laufwerk C: überprüfen möchten, geben Sie folgenden Befehl ein:

```
chkdsk /scan C:
```

Dann analysiert die Datenträgerprüfung das Laufwerk und meldet alle Probleme, auf die sie stößt. Wenn Sie keine zusätzlichen Optionen angeben, repariert die Datenträgerprüfung aber keine Defekte. Um Fehler auf Laufwerk C: zu reparieren, geben Sie folgenden Befehl ein:

```
chkdsk /spotfix C:
```

Eine Reparatur des Volumes erfordert den exklusiven Zugriff auf das Volume. Wie das im Detail funktioniert, hängt von der Art des Volumes ab:

- Handelt es sich bei dem Volume nicht um ein Systemvolume, erscheint eine Meldung, in der Sie gefragt werden, ob die Bereitstellung des Volumes für die Reparatur aufgehoben werden soll. In diesem Fall können Sie **J** eingeben, um fortzufahren, oder **N**, um die Aufhebung der Bereitstellung abzubrechen. Wenn Sie die Aufhebung der Bereitstellung abbrechen, werden Sie gefragt, ob das Volume beim nächsten Start des Computers überprüft werden soll. Mit **J** können Sie die Reparatur auf den Plan setzen, mit **N** den ganzen Vorgang abbrechen.
- Handelt es sich um ein Systemvolume, werden Sie gefragt, ob die Reparatur beim nächsten Start des Computers durchgeführt werden soll. Geben Sie **J** ein, wenn die Reparatur durchgeführt werden soll, oder **N**, um die Reparatur abzubrechen.

Die Optionen `/scan` und `/spotfix` dürfen beim Aufruf der Datenträgerprüfung nicht kombiniert werden, weil die Überprüfung und die Reparatur nun zwei voneinander unabhängige Vorgänge sind.

Die Syntax des Befehls `Chkdsk` lautet:

```
CHKDSK [Volume[[Pfad]Dateiname]] [/F] [/V] [/R] [/X] [/I] [/C] [/B]  
[ /L[:Größe]] [/scan] [/forceofflinefix] [/perf] [/spotfix] [/sdcleanup] [/offlinescanandfix]
```

Die Optionen und Argumente von `Chkdsk` haben folgende Bedeutungen:

- **Volume** Gibt das zu prüfende Volume an.
- **Pfad/Dateiname** Gibt Dateien an, die auf Fragmentierung überprüft werden sollen (nur bei FAT-Volumes).
- **/B** Sucht erneut nach defekten Clustern auf dem Volume (nur NTFS; bedingt `/R`).
- **/C** Überspringt den Test auf zyklische Teilstrukturen in der Ordnerstruktur (nur NTFS).

- **/F** Behebt Fehler auf dem Laufwerk, wobei die Überprüfung und Reparatur offline erfolgt (die alte Methode).
- **/I** Führt nur eine minimale Überprüfung der Indexeinträge durch (nur NTFS).
- **/L:Größe** Legt die Größe der Protokolldatei fest (nur NTFS).
- **/R** Erkennt fehlerhafte Sektoren und stellt lesbare Daten wieder her (bedingt **/F**).
- **/V** Zeigt den vollständigen Pfad und Namen jeder Datei auf dem Laufwerk an (FAT-Volumes). Zeigt Bereinigungsmeldungen an, sofern vorhanden (NTFS).
- **/X** Erzwingt die Aufhebung der Bereitstellung des Volumes, sofern erforderlich (bedingt **/F**).

Auf NTFS-Volumes lassen sich unter Windows 8 mit folgenden Optionen die erweiterten Funktionen der Datenträgerprüfung verwenden.

- **/forceofflinefix** Muss zusammen mit **/scan** verwendet werden. Überspringt die Online-Reparatur aller gefundenen Fehler.
- **/scan** Führt eine Online-Überprüfung des Volumes aus, die Standardeinstellung. Bei dieser Überprüfung erkannte Fehler werden in die Systemdatei *\$corrupt* eingetragen.
- **/perf** Führt die Überprüfung so schnell wie möglich durch und verwendet dabei mehr Systemressourcen.
- **/spotfix** Ermöglicht die Online-Reparatur bestimmter Fehler (die Standardeinstellung).
- **/sdcleanup** Löscht unnötige Sicherheitsbeschreibungsdaten. Bedingt **/F** (mit der alten Überprüfungs- und Reparaturmethode).
- **/offlinescanandfix** Führt eine Offlineüberprüfung und Offlinereparatur des Volumes aus.

Interaktive Ausführung der Datenträgerprüfung

Sie können die Datenträgerprüfung mit der Computerverwaltung auch interaktiv ausführen. So überprüfen Sie die Laufwerke des lokalen Computers:

1. Wählen Sie in der Computerverwaltung den Knoten *Datenspeicher* und dann den Knoten *Datenträgerverwaltung*. Klicken Sie ein Laufwerk in der Datenträgerliste oder in der grafischen Ansicht mit der rechten Maustaste an oder halten Sie es gedrückt, und wählen Sie *Eigenschaften*.

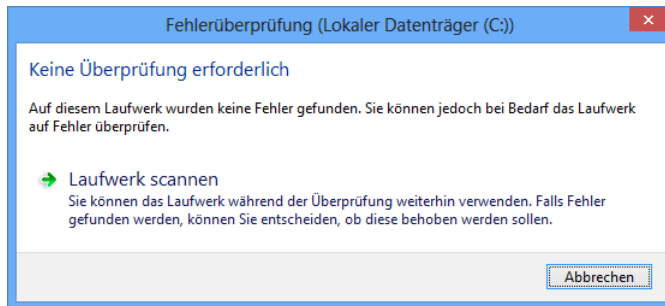


Abbildung 12.12 Die Datenträgerprüfung ist durch Tippen oder Klicken auf die Schaltfläche *Prüfen* im Eigenschaftendialogfeld des Datenträgers zugänglich. Verwenden Sie die Datenträgerprüfung zur Überprüfung eines Datenträgers auf Fehler und zur Fehlerreparatur

2. Tippen oder klicken Sie auf der Registerkarte *Tools* auf *Prüfen*. Dadurch öffnet sich das Dialogfeld *Fehlerüberprüfung* (Abbildung 12.12). Bei NTFS-Volumes haben Sie die Option *Laufwerk scannen* zur Verfügung, bei FAT-Volumes die Option *Laufwerk scannen und reparieren*.
3. Klicken Sie auf *Laufwerk scannen* oder *Laufwerk scannen und reparieren*, um die Überprüfung zu starten. Ist das Volume fehlerfrei, bestätigt Windows dies. Werden Fehler erkannt, stehen Ihnen weitere Optionen zur Verfügung. Wie bei der Überprüfung von Laufwerken in einer Eingabeaufforderung hängt die weitere Vorgehensweise davon ab, ob es sich um ein Systemvolume handelt oder nicht, und ob es mit NTFS oder FAT formatiert ist.

Defragmentieren von Datenträgern

Bei jedem Hinzufügen oder Entfernen von Dateien auf einem Laufwerk können die Daten fragmentiert werden. Wenn ein Laufwerk fragmentiert ist, lassen sich Dateien nicht in einem zusammenhängenden Bereich der Festplatte speichern. Als Folge davon muss das Betriebssystem die Datei in mehreren kleineren Bereichen auf der Festplatte speichern und benötigt daher beim Auslesen der Datei von der Festplatte mehr Zeit. Um die Fragmentierung zu verringern, defragmentiert Windows 8 die Volumes im Rahmen der automatischen Wartung. Wie die Datenträgerüberprüfung wird auch der Aufruf und die Verwaltung der Datenträgeroptimierung von einer separaten Aufgabe gesteuert. In der Aufgabenplanung finden Sie unter *Microsoft\Windows\Defrag* die Aufgabe *Scheduled Defrag* in der Aufgabenplanungsbibliothek. Ausführliche Angaben über die bisherigen Läufe finden Sie auf der Registerkarte *Verlauf* der Aufgabe.

Solange der Computer aus dem Stromnetz betrieben wird, kann die automatische Überprüfung und Optimierung von Laufwerken in den Leerlaufzeiten des Betriebssystems erfolgen, während die Laufwerke online sind. Standardmäßig wird die Laufwerksoptimierung aber nicht täglich, sondern wöchentlich durchgeführt. Dafür gibt es einen guten Grund. Normalerweise müssen die Laufwerke eines Computers nur gelegentlich optimiert werden. In den meisten Fällen reicht eine wöchentliche Optimierung aus. Beachten Sie aber, dass es im Gegensatz zu den Datenvolumes, die sich schnell analysieren und optimieren lassen, wesentlich länger dauern kann, Systemvolumes online zu optimieren. Große Systemvolumes werden daher vielleicht nicht vollständig überprüft und optimiert, besonders dann, wenn der Computer für Wartungsarbeiten ausgeschaltet und dann aktiv benutzt wird, während er mit Strom aus dem Stromnetz versorgt wird.

Gehen Sie folgendermaßen vor, um einen Datenträger von Hand zu defragmentieren:

1. Wählen Sie in der Computerverwaltung den Knoten *Datenspeicher* und dann den Knoten *Datenträgerverwaltung*. Klicken Sie mit der rechten Maustaste auf ein Laufwerk oder halten Sie es gedrückt, und wählen Sie *Eigenschaften*.
2. Tippen oder klicken Sie auf der Registerkarte *Tools* auf *Optimieren*. Tippen oder klicken Sie im Dialogfeld *Laufwerke optimieren* auf das Laufwerk, das Sie überprüfen möchten, und dann auf *Analysieren*. Die Datenträgerdefragmentierung analysiert nun das Laufwerk und stellt fest, ob es defragmentiert werden muss. Ist das der Fall, empfiehlt das Tool Ihnen, die Optimierung durchzuführen.
3. Die Spalte *Aktueller Status* zeigt den Zustand jedes Laufwerks und die prozentuale Fragmentierung bei der letzten Prüfung. Um ein Laufwerk zu defragmentieren, tippen oder klicken Sie auf das Laufwerk und dann auf *Optimieren*.

HINWEIS

Abhängig von der Größe des Datenträgers kann die Defragmentierung bis zu einigen Stunden dauern. Sie können jederzeit auf *Anhalten* klicken, um die Defragmentierung zu beenden.

In älteren Windows-Versionen war es möglich, den Tag und die Uhrzeit der Ausführung separat festzulegen, nun führt Windows die Defragmentierung im Rahmen der automatischen Wartung aus. Standardmäßig erfolgen die Überprüfung und gegebenenfalls die Defragmentierung ungefähr einmal in der Woche. Sie können die ungefähre Startzeit über die Einstellung der Startzeit der automatischen Wartung festlegen. Windows informiert Sie zudem, wenn Sie drei aufeinanderfolgende Ausführungstermine verpasst haben. Alle internen und bestimmte externe Laufwerke werden im Rahmen der üblichen Wartung automatisch optimiert, ebenso die neuen Laufwerke, die Sie an Ihren Computer anschließen.

1. Wählen Sie in der Computerverwaltung den Knoten *Datenspeicher* und dann den Knoten *Datenträgerverwaltung*. Klicken Sie mit der rechten Maustaste auf einen Datenträger oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Eigenschaften*.
2. Tippen oder klicken Sie auf der Registerkarte *Tools* auf *Optimieren*. Daraufhin öffnet sich das Dialogfeld *Laufwerke optimieren* (Abbildung 12.13).

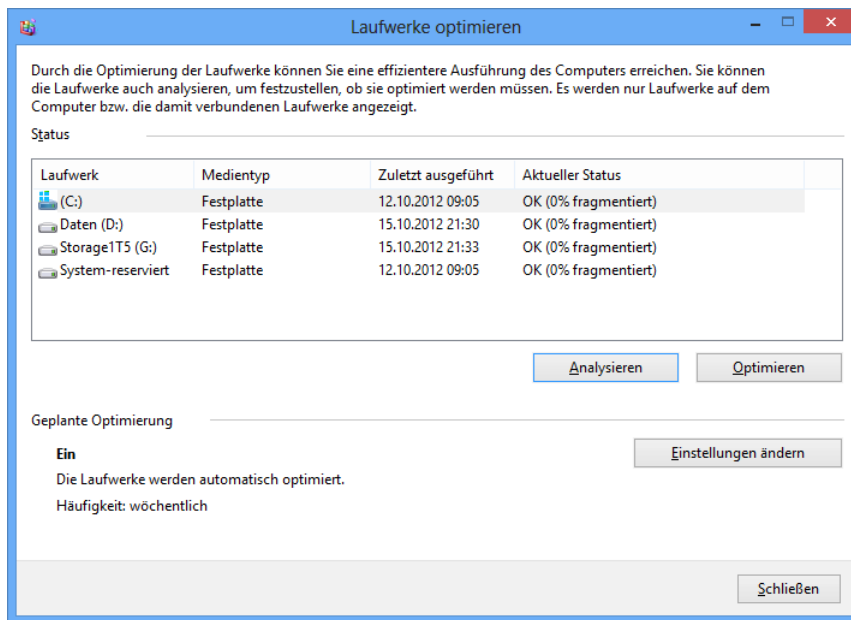


Abbildung 12.13 Windows optimiert die Laufwerke, um eine möglichst hohe Leistung zu gewährleisten

3. Wenn Sie die Optimierung konfigurieren möchten, tippen oder klicken Sie auf *Einstellungen ändern*. Abbildung 12.14 zeigt das Dialogfeld, das dann erscheint. Um die automatische Defragmentierung abzuschalten, löschen Sie das Kontrollkästchen *Ausführung nach Zeitplan*. Um sie zu aktivieren, wählen Sie *Ausführung nach Zeitplan*.
4. Die Abbildung zeigt die Standardeinstellung. In der Dropdownliste *Häufigkeit* können Sie *Täglich*, *Wöchentlich* oder *Monatlich* auswählen. Wenn Sie nicht über versäumte Optimierungsläufe informiert werden möchten, löschen Sie das Kontrollkästchen *Benachrichtigen, wenn drei aufeinanderfolgende geplante Ausführungen fehlen*.
5. Wenn Sie einstellen wollen, welche Datenträger defragmentiert werden, tippen oder klicken Sie auf *Auswählen* und wählen dann die Volumes aus, die defragmentiert werden sollen. In der Standardeinstellung werden alle Datenträger defragmentiert, die im Computer installiert oder an den Computer angeschlossen sind. Auch alle neuen Datenträger werden automatisch defragmentiert. Aktivieren Sie

die Kontrollkästchen der Datenträger, die automatisch defragmentiert werden sollen, und deaktivieren Sie die Kontrollkästchen der Datenträger, die nicht automatisch defragmentiert werden sollen. Tippen oder klicken Sie auf *OK*, um Ihre Einstellungen zu speichern.

6. Tippen oder klicken Sie auf *OK* und dann auf *Schließen*.

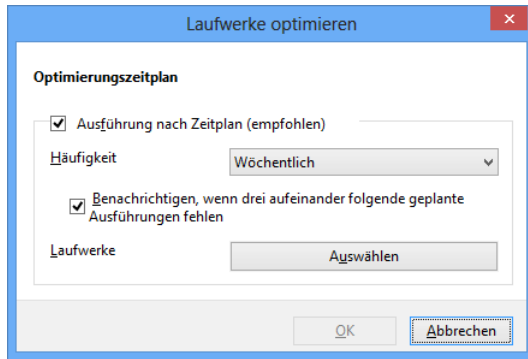


Abbildung 12.14 Einstellen des gewünschten Zeitplans für die automatisierte Defragmentierung

HINWEIS Windows holt versäumte Defragmentierungen automatisch in einem zyklischen Verfahren nach. Das bedeutet: Wenn ein geplanter Defragmentierungslauf angehalten und neu gestartet wird, setzt der Computer die Defragmentierung automatisch beim nächsten Volume fort, dessen Defragmentierung noch nicht abgeschlossen ist.

Neusynchronisieren und Reparieren eines Spiegelsatzes

Windows 8 synchronisiert gespiegelte Volumes automatisch. Die Synchronisierung von Daten auf gespiegelten Datenträgern kann jedoch verloren gehen. Wenn beispielsweise ein Laufwerk zeitweilig oder ganz ausfällt, werden die Daten nur auf das Laufwerk geschrieben, das noch in Betrieb ist.

Sie können Spiegelsätze neu synchronisieren und reparieren, müssen aber den Satz aus Festplatten erneut aufbauen, die denselben Partitionsverwaltungstyp (MBR oder GPT) haben. Beide Laufwerke des Spiegelsatzes müssen in Betrieb sein. Weil ein Datenträger des Spiegelsatzes ausgefallen ist, müsste der Status des Spiegelsatzes »Fehlerhafte Redundanz« lauten. Die Korrekturmaßnahme hängt vom Status des fehlerhaften Volumes ab:

- Falls der Status »Fehlt« oder »Offline« lautet, stellen Sie sicher, dass das Laufwerk mit Strom versorgt wird und ordnungsgemäß angeschlossen ist. Starten Sie danach die Datenträgerverwaltung, klicken Sie mit der rechten Maustaste auf das fehlerhafte Volume oder halten Sie es gedrückt, und wählen Sie *Volume erneut aktivieren* aus. Der Laufwerkstatus sollte sich in »Erneut erzeugen« und anschließend in »Fehlerfrei« ändern. Falls das Volume nicht in den Zustand »Fehlerfrei« zurückkehrt, klicken Sie mit der rechten Maustaste darauf oder halten Sie es gedrückt, und wählen Sie dann *Spiegelung erneut synchronisieren*.
- Wenn der Status »Online (Fehler)« lautet, klicken Sie mit der rechten Maustaste auf das fehlerhafte Volume oder halten Sie es gedrückt und wählen *Volume erneut aktivieren* aus. Der Laufwerkstatus sollte sich in »Erneut erzeugen« und anschließend in »Fehlerfrei« ändern. Falls das Volume nicht in den Zustand »Fehlerfrei« zurückkehrt, klicken Sie mit der rechten Maustaste darauf oder halten es gedrückt, und wählen *Spiegelung erneut synchronisieren*.

- Wenn ein Laufwerk als »Nicht lesbar« angezeigt wird, lesen Sie die Laufwerke im System neu ein, indem Sie im Menü *Aktion* der Datenträgerverwaltung auf *Datenträger neu einlesen* klicken. Falls sich der Laufwerkstatus nicht ändert, müssen Sie den Computer neu starten.
- Wenn ein Laufwerk dann noch immer nicht läuft, klicken Sie mit der rechten Maustaste auf das fehlerhafte Volume oder halten es gedrückt, und wählen danach *Spiegelung entfernen* aus. Tippen oder klicken Sie anschließend mit der rechten Maustaste auf das verbleibende Volume im ursprünglichen Spiegelsatz und wählen Sie *Spiegelung hinzufügen* aus. Nun müssen Sie das Volume auf einen nicht zugeordneten Bereich auf einem anderen Laufwerk spiegeln. Ist nicht genug Platz auf einem anderen Laufwerk frei, müssen Sie gegebenenfalls Platz freimachen, indem Sie andere Volumes löschen oder das fehlerhafte Laufwerk austauschen.

Reparieren eines gespiegelten Systemvolumes, um den Systemstart zu ermöglichen

Der Ausfall eines gespiegelten Laufwerks kann den Start des Systems verhindern. Normalerweise geschieht dies, wenn Sie das Systemvolume, das Startvolume oder beide spiegeln und das primäre gespiegelte Laufwerk ausfällt.

Wenn Sie ein Systemvolume spiegeln, sollte das Betriebssystem einen Eintrag zum Start-Manager des Systems hinzufügen, der Ihnen erlaubt, die sekundäre Spiegelung zu starten. Mit diesem Eintrag in der Start-Manager-Datei ist das Beheben des Ausfalls eines primären gespiegelten Laufwerks wesentlich einfacher als zuvor, weil Sie nur den Eintrag für den Start der Spiegelung zu wählen brauchen. Wenn Sie das Startvolume spiegeln und kein zweiter Eintrag für die Spiegelung erstellt wird, können Sie die Starteinträge im Start-Manager selbst anpassen, indem Sie einen Eintrag mit dem BCD-Editor (*bcdedit.exe*) hinzufügen. Ob der zweite Eintrag erstellt wurde, können Sie überprüfen, indem Sie in einer Eingabeaufforderung mit erhöhten Rechten *bcdedit* eingeben.

Falls das Betriebssystem vom primären Systemvolume nicht gestartet werden kann, starten Sie das System neu und wählen für das zu startende Betriebssystem die Option *Startspiegelung – Sekundäres Plex*. Das System sollte normal starten. Nachdem Sie das System erfolgreich vom sekundären Laufwerk gestartet haben, können Sie nach Wunsch die Wartung zeitlich planen, die zum Neuerstellen der Spiegelung erforderlich ist. Sie müssen die folgenden Schritte ausführen:

1. Fahren Sie das System herunter und tauschen Sie das ausgefallene Volume aus, oder fügen Sie ein Festplattenlaufwerk hinzu. Starten Sie danach das System neu.
2. Heben Sie die Spiegelung auf und erstellen Sie die Spiegelung auf dem ausgetauschten Laufwerk neu. Dies ist in der Regel Datenträger 0. Klicken Sie mit der rechten Maustaste auf das andere Volume, das zur ursprünglichen Spiegelung gehörte, oder halten Sie es gedrückt, und wählen Sie *Spiegelung hinzufügen* aus. Das Dialogfeld *Spiegelung hinzufügen* wird geöffnet.
3. Wählen Sie im Listenfeld *Datenträger* einen Speicherort für die Spiegelung und tippen oder klicken Sie auf *Spiegelung hinzufügen*. Windows 8 startet die Einrichtung der Spiegelung. In der Datenträgerverwaltung wird für beide Volumes der Status »Die Synchronisation wird wiederholt« angezeigt. Der Datenträger, auf dem das gespiegelte Volume erstellt wird, ist mit einem Warnsymbol markiert.
4. Wenn sich die primäre Spiegelung (das Original-Systemvolume) auf dem hinzugefügten oder als Ersatz eingebauten Laufwerk befinden soll, heben Sie in der Datenträgerverwaltung die Spiegelung wieder auf. Prüfen Sie, ob das primäre Laufwerk im ursprünglichen Spiegelsatz den Laufwerkbuchstaben hat, der zuvor der gesamten Spiegelung zugewiesen war. Ist dies nicht der Fall, weisen Sie den entsprechenden Laufwerkbuchstaben zu.

5. Klicken Sie mit der rechten Maustaste auf das Laufwerk, das Sie hinzugefügt oder als Ersatz eingebaut haben, oder halten Sie es gedrückt, und wählen Sie *Spiegelung hinzufügen* aus. Erstellen Sie nun die Spiegelung neu.
6. Prüfen Sie die Systemstartkonfiguration und stellen Sie sicher, dass das Laufwerk, das Sie hinzugefügt oder als Ersatz eingebaut haben, während des Starts verwendet wird. Unter Umständen müssen Sie die Systemstartkonfiguration überarbeiten, um dies sicherzustellen.

Arbeiten mit Wechselmediengeräten

Wechselmediengeräte können mit NTFS, FAT, FAT32 und exFAT formatiert sein. Externe Speichergeräte werden einfach nur mit einem Computer verbunden. Die Geräte müssen nicht in den Computer eingebaut werden. Das macht externe Speichergeräte einfacher und schneller installierbar als die meisten Festplattenlaufwerke. Die meisten externen Speichergeräte haben eine USB-, eine FireWire- oder eine eSATA-Schnittstelle. Wenn Sie mit USB und FireWire arbeiten, hängen die Übertragungsgeschwindigkeit und die Gesamtleistung des Geräts aus Sicht des Benutzers vor allem davon ab, welche Schnittstellenversion unterstützt wird.

Momentan sind mehrere Versionen von USB und FireWire in Gebrauch. USB 2.0 ist der Industriestandard, wobei sich USB 3.0 immer stärker durchsetzt. USB 2.0-Geräte lassen sich in die Kategorien »full speed« (bis zu 12 MBit/s) und »high speed« (bis zu 480 MBit/s) einordnen. High-Speed-USB 2.0 unterstützt zwar Datenübertragungen mit einer maximalen Geschwindigkeit von 480 MBit/s, die Durchschnittsübertragungsraten liegen aber gewöhnlich bei 10 bis 30 MByte/s. Die tatsächlich erreichbare Dauertransferrate hängt von vielen Faktoren ab, zum Beispiel vom Typ des Geräts, den übertragenen Daten und der Geschwindigkeit des Computers. Jeder USB-Controller auf einem Computer hat eine bestimmte Bandbreite zur Verfügung, die sich alle Geräte teilen müssen, die an diesen Controller angeschlossen sind. Die Übertragungsraten sind deutlich geringer, wenn der Computer einen USB-Anschluss mit einer älteren Version als das angeschlossene Gerät aufweist. Wenn Sie zum Beispiel ein USB 2.0-Gerät an einen USB 1.0-Anschluss anstecken (oder umgekehrt), läuft das Gerät mit der deutlich langsameren Übertragungsgeschwindigkeit von USB 1.0.

Die Anschlüsse für USB 1.0, 1.1 und 2.0 sehen alle gleich aus. Die meisten USB 3.0-Anschlüsse, die ich gesehen habe, waren allerdings farblich gekennzeichnet, damit sie leichter zu erkennen sind. Trotzdem ist der Blick ins Handbuch des Computers die einfachste Methode, um festzustellen, welche Art von USB-Anschlüssen ein Computer hat. Neuere LCD-Monitore haben oft USB 2.0-Anschlüsse, an die Sie ebenfalls Geräte anstecken können. Wenn Sie USB-Geräte mit einem Monitor verbinden, dient der Monitor als USB-Hub. Wie bei allen USB-Hubs teilen sich alle Geräte, die an denselben Hub angeschlossen sind, die Bandbreite. Die Gesamtbandbreite wird durch die Geschwindigkeit des USB-Anschlusses am Computer begrenzt, an den der Hub angesteckt ist.

FireWire (IEEE 1394) ist ein Hochleistungs-Verbindungsstandard, der eine Peer-to-Peer-Architektur nutzt. Dabei handeln Peripheriegeräte Buskonflikte untereinander aus, um festzulegen, welches Gerät einen Datentransfer am besten steuern kann. Auch bei FireWire sind momentan mehrere Versionen in Gebrauch. FireWire 400 (IEEE 1394a) hat eine maximale Dauertransferrate von bis zu 400 MBit/s. IEEE 1394b ermöglicht 400 MBit/s (S400), 800 MBit/s (S800) und 1600 MBit/s (S1600). Wie bei USB gilt: Wenn Sie ein IEEE 1394b-Gerät an einen IEEE 1394a-Anschluss anschließen, oder umgekehrt, läuft das Gerät mit der deutlich geringeren Übertragungsgeschwindigkeit von FireWire 400.

Wie bei USB liegen die Geschwindigkeiten bei Dauerübertragungen auch bei IEEE 1394a und IEEE 1394b deutlich unter den maximalen Übertragungsraten. Die Anschlüsse und Kabel von IEEE 1394a und IEEE 1394b sehen anders aus, was ihre Unterscheidung erleichtert – wenn man weiß, worauf man achten muss.

FireWire 400-Anschlüsse und -Kabel sehen genauso aus wie alte FireWire-Versionen, die vor Verabschiedung der Spezifikationen IEEE 1394a und IEEE 1394b verwendet wurden. FireWire-Kabel und -Anschlüsse mit 4 Polen (4 Adern) übertragen keinen Strom über den Bus. FireWire 400-Kabel und -Anschlüsse haben 6 Pole, und FireWire 800- und FireWire 1600-Kabel und -Anschlüsse 9 Pole.

Netzwerkfähige Geräte können Sie wahrscheinlich mit herkömmlichen Ethernet-Kabeln an Ihr Netzwerk anschließen. Viele dieser Geräte übertragen die Daten inzwischen mit 1 Gigabit pro Sekunde (GBit/s). Das entspricht 1000 MBit/s. Auch Geräte mit 10 GBit/s verbreiten sich zunehmend.

Bevor Sie ein externes Gerät für einen Computer kaufen, sollten Sie prüfen, welche Schnittstellen Ihr Computer hat und welche Schnittstellen das Gerät benutzt. In manchen Fällen finden Sie ein Gerät mit zwei Schnittstellen, das USB 2.0 und FireWire 400 unterstützt, oder sogar mit drei Schnittstellen, das USB 2.0, FireWire 400 und FireWire 800 unterstützt. Ein Gerät mit zwei oder drei Schnittstellen ist natürlich flexibler einsetzbar.

In der Konsole *Computer* oder der Datenträgerverwaltung arbeiten Sie mit Wechseldatenträgern, indem Sie mit der rechten Maustaste auf den Datenträger klicken oder ihn gedrückt halten, und dann einen der folgenden Befehle wählen:

- Wählen Sie den Befehl *Öffnen*, um den Inhalt des Datenträgers im Datei-Explorer anzuzeigen.
- Wählen Sie den Befehl *Formatieren*, um den Wechseldatenträger zu formatieren, wie im Abschnitt »Formatieren von Partitionen und Volumes« weiter oben in diesem Kapitel beschrieben. Wechseldatenträger haben im Allgemeinen nur eine einzige Partition.
- Wählen Sie den Befehl *Eigenschaften*, um seine Eigenschaften anzuzeigen oder zu ändern. Auf der Registerkarte *Allgemein* im Eigenschaftendialogfeld können Sie die Volumebezeichnung ändern, wie im Abschnitt »Zuweisen, Ändern oder Löschen einer Volumebezeichnung« weiter oben in diesem Kapitel beschrieben.

Wenn Sie mit Wechseldatenträgern arbeiten, können Sie die Datenträger- und Ordneransichten anpassen. Klicken Sie dazu mit der rechten Maustaste auf den Datenträger oder Ordner oder halten Sie ihn gedrückt, wählen Sie den Befehl *Eigenschaften* und tippen oder klicken Sie auf die Registerkarte *Anpassen*. Sie können nun den Standardordnertyp auswählen und dadurch festlegen, welche Details in der Standardeinstellung angezeigt werden. Zum Beispiel können Sie als Standardordnertyp den Eintrag *Dokumente*, *Bilder* oder *Videos* wählen. Sie können außerdem Ordnerbilder und -symbole auswählen.

Wechseldatenträger unterstützen die Netzwerkfreigabe von Dateien und Ordnern. Sie konfigurieren die Freigabe bei einem Wechseldatenträger genauso wie bei einer normalen Dateifreigabe. Sie können Freigabeberechtigungen zuweisen, Zwischenspeicherungsoptionen für Offlinedateien konfigurieren und die Zahl der gleichzeitigen Benutzer begrenzen. Sie können einen Wechseldatenträger vollständig freigeben oder einzelne Ordner auswählen, die auf dem Wechseldatenträger gespeichert sind. Sie können auch mehrere Freigabeinstanzen erstellen.

Wechseldatenträger unterscheiden sich von Standard-NTFS-Freigaben dadurch, dass es unter Umständen keine zugrunde liegende Sicherheitsarchitektur gibt. Bei exFAT, FAT oder FAT32 haben die gespeicherten Ordner und Dateien keinerlei Sicherheitsberechtigungen oder andere Sicherheitsmechanismen, abgesehen von den grundlegenden Attributen *Schreibgeschützt* und *Versteckt*, die Sie einstellen können.

Arbeiten mit Daten-CDs und -DVDs

CD- und DVD-Abbilder werden oft in Form von ISO-Dateien gespeichert, ebenso Blu-ray-Datenträger. Windows 8 ist in der Lage, mit ISO-Abbildern umzugehen und sie auf CD oder DVD zu brennen. Windows 8 stellt auch integrierte Brennfunktionen zur Verfügung, mit denen Sie Daten-CDs und -DVDs erstellen können. Allerdings sollten Sie sich vorher mit den Datenträgertypen und Dateisystemoptionen vertraut machen, die für diese Medien zur Verfügung stehen.

Brennen von Medien: Die Grundlagen

Windows 8 zeigt im Datei-Explorer standardmäßig den Befehl *Auf Datenträger brennen* im Kontextmenü des DVD-Laufwerks an. Wenn Sie diesen Befehl verwenden, wird der Assistent *Auf Datenträger brennen* gestartet, in dem Sie eine Daten-Disk erstellen können. Denken Sie daran, dass sich Computer-CD/DVD-Player von CD- und DVD-Playern für das Wohnzimmer oder Autos unterscheiden. Der CD/DVD-Player in Ihrem Computer dient normalerweise dazu, industriell hergestellte CD-ROMs und DVD-ROMs sowie am Computer gebrannte CDs und DVDs in bestimmten Formaten zu lesen. Dagegen kann es durchaus sein, dass CD- oder DVD-Player für Wohnzimmer oder Auto nicht in der Lage sind, eine CD oder DVD zu erkennen, die von Ihnen auf einem Computer erstellt wurde.

Die meisten CD/DVD-Brenner unterstützen mehrere Disktypen. Windows 8 bietet integrierte Unterstützung zum Brennen von Daten-CDs auf CD-R, CD+R und CD-RW sowie zum Brennen von Daten-DVDs auf DVD-R, DVD-RW, DVD+R, DVD+RW und DVD-RAM. DVDs können einseitig (single-sided) und einschichtig (single-layered) oder einseitig und doppelschichtig (dual-layered) sein. Windows 8 bietet auch integrierte Unterstützung für Blu-ray. Ist in einem Computer ein geeigneter Blu-ray-Brenner eingebaut, können Sie möglicherweise auch Blu-ray-Disks brennen.

Windows 8 unterstützt zwei Ansätze, um Disks zu brennen:

- Mastering
- Livedateisystem

Die meisten Windows-Programme erstellen Datendisks im Masteringverfahren. Das Dateisystemformat für solche Disks wird automatisch ausgewählt. Beim Masteringverfahren wählen Sie die Dateien aus, die Sie auf eine Disk schreiben wollen, und brennen dann alle diese Dateien auf einmal. Wenn Sie große Dateisammlungen auf Disk brennen, ist das ein bequemes Verfahren. Dazu kommt der Vorteil, dass die Kompatibilität zu allen Computern oder Geräten gewahrt bleibt, die Unterstützung für den Typ Datendisk bieten, die Sie erstellen.

Wenn Sie Dateien im Masteringverfahren auf Datendisks schreiben, brennen Sie die Dateien in einer Sitzung. In vielen CD/DVD-Brennprogrammen haben Sie die Möglichkeit, Sitzungen (engl. session) offen zu lassen, damit Sie später weitere Dateien hinzufügen können. Erst wenn Sie alle Dateien hinzugefügt haben, die Sie brauchen, schließen Sie die Sitzung. Indem Sie die Sitzung schließen, stellen Sie die Disk fertig, damit sie von anderen Computern und Geräten gelesen werden kann. Während eine Sitzung noch offen ist, kann die Disk nur auf einem kompatiblen Computer gelesen werden.

Eine Datendisk mit einem Livedateisystem funktioniert dagegen wie jeder andere Wechselmedientyp, etwa USB-Speichersticks oder externe Festplattenlaufwerke. Sie können Dateien zur Disk hinzufügen, ohne sie brennen zu müssen. Dazu kopieren Sie die Dateien einfach über die Zwischenablage oder ziehen sie mit der Maus auf das gewünschte Ziel. Ist die Disk löschbar, können Sie Dateien entfernen, indem Sie sie auswählen und löschen. Wenn Sie die Disk auswerfen, können Sie sie später erneut in Ihr CD/DVD-Laufwerk einlegen und weiterhin wie mit einem Wechseldatenträger damit arbeiten.

Datendisks mit einem Livedateisystem sind mit UDF (Universal Disk Format) formatiert statt mit CDFS (CD File System). Im Allgemeinen sind nur Computer in der Lage, UDF-Datendisks zu lesen. Windows 8 unterstützt das Brennen von Datendisks mit verschiedenen UDF-Versionen:

- **UDF 1.5** Ein Format, das zu Windows 2000 und neueren Windows-Versionen kompatibel ist. Windows 98- oder Apple-Computer können es unter Umständen nicht lesen.
- **UDF 2.0** Ein Format, das zu Windows XP und neueren Windows-Versionen kompatibel ist. Windows 98-, Windows 2000- oder Apple-Computer können es unter Umständen nicht lesen.
- **UDF 2.01** Das Standardformat. Es enthält wesentliche Neuerungen, die sich in den meisten Fällen als nützlich erweisen. Dieses Format ist zu Windows XP und neueren Windows-Versionen kompatibel. Windows 98-, Windows 2000- oder Apple-Computer können es unter Umständen nicht lesen.
- **UDF 2.5** Ein Format, das für Windows Vista und neuer optimiert ist. Ältere Windows-Versionen oder Apple-Computer können es unter Umständen nicht lesen.

Bereitstellen von ISO-Abbildern

Wenn Sie ein ISO-Abbild bereitstellen, erstellen Sie dadurch ein virtuelles Laufwerk, das Sie wie ein physisches Laufwerk verwenden können. Wenn Sie zum Beispiel eine ISO-Datei bereitstellen, in der die Installationsdateien einer Anwendung liegen, können Sie diese ISO-Datei zur Installation der Anwendung verwenden.

Nach einer der beiden folgenden Methoden können Sie ein ISO-Abbild als virtuelles Laufwerk bereitstellen:

1. Klicken Sie die ISO-Datei im Datei-Explorer mit der rechten Maustaste an oder halten Sie sie gedrückt, und wählen Sie dann *Bereitstellen*.
2. Tippen oder klicken Sie im Datei-Explorer auf die ISO-Datei, die Sie zur Erstellung einer Datendisk verwenden möchten. Klicken Sie die ISO-Datei, die Sie bereitstellen möchten, mit der rechten Maustaste an oder halten Sie sie gedrückt, und wählen Sie *Bereitstellen*.

ISO-Abbilder auf Disk brennen

Um aus einem ISO-Abbild eine verwendbare CD/DVD zu machen, müssen Sie das Abbild auf einen geeigneten Rohling brennen. Anschließend können Sie den Datenträger in den Laufwerken von Computern verwenden. So brennen Sie ein ISO-Abbild:

1. Legen Sie einen leeren Rohling in Ihren CD/DVD-Brenner ein. Ignorieren Sie die Aufforderung, eine Aktion auszuwählen. Falls Sie die Meldung doch antippen oder anklicken, schließen Sie die Aktionsliste wieder mit *Keine Aktion durchführen*.
2. Klicken Sie die ISO-Datei, aus der Sie eine Daten-CD/DVD machen möchten, im Datei-Explorer mit der rechten Maustaste an oder halten Sie sie gedrückt, und wählen Sie *Datenträgerabbild brennen*.
3. Stellen Sie im Dialogfeld *Windows-Brenner für Datenträgerabbilder* (Abbildung 12.15) in der Dropdownliste *CD/DVD-Brenner* ein, welcher Brenner verwendet wird, und tippen oder klicken Sie auf *Brennen*.

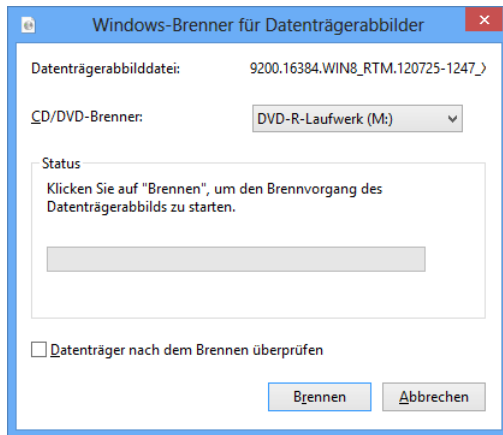


Abbildung 12.15 ISO-Abbilder auf Disk brennen

Gemasterte Disks brennen

Gehen Sie folgendermaßen vor, um eine gemasterte Disk zu brennen:

1. Legen Sie einen leeren Rohling in Ihren CD/DVD-Brenner ein. Sie haben nun folgende Möglichkeiten:
 - Wenn die Meldung erscheint, dass eine Aktion ausgewählt werden soll, tippen oder klicken Sie diese Meldung an. Wählen Sie in der Aktionsliste *Dateien auf Datenträger brennen*.
 - Erscheint diese Meldung nicht, öffnen Sie den Datei-Explorer und tippen oder klicken in der Strukturdarstellung links auf *Computer*. Klicken Sie mit der rechten Maustaste auf den CD/DVD-Brenner oder halten Sie ihn gedrückt, und wählen Sie *Automatische Wiedergabe öffnen*. Tippen oder klicken Sie nun in der Aktionsliste auf *Dateien auf Datenträger brennen*.
2. Geben Sie im Assistenten *Auf Datenträger brennen* (Abbildung 12.16) einen Datenträgertitel ein. Wählen Sie die Option *Mit einem CD/DVD-Player* aus, um eine gemasterte Disk zu erstellen. Sobald Sie auf *Weiter* tippen oder klicken, wird die Datendisk im Datei-Explorer geöffnet. Der Hauptbereich des Fensters zeigt eine leere Liste an. Schließen Sie dieses Fenster nicht.
3. Wählen Sie im Datei-Explorer die gewünschten Dateien aus und ziehen oder kopieren Sie sie in die Liste der zu brennenden Dateien. Die Dateien in dieser Liste werden von ihrem ursprünglichen Speicherort gelesen und als temporäre Dateien in einen temporären Ordner geschrieben. Dieser temporäre Ordner wird im Profil des Benutzers erstellt. Es werden Kopien der Dateien angelegt, um sicherzustellen, dass sich alle Dateien am selben Platz befinden und Sie ausreichende Berechtigungen für den Zugriff auf die Dateien haben, bevor Sie versuchen, die Daten auf den Rohling zu brennen.
4. Wenn Sie fertig sind, klicken Sie mit der Maustaste auf einen freien Bereich unter *Dateien, die auf den Datenträger geschrieben werden sollen* oder halten diese Stelle gedrückt, und wählen *Auf Datenträger brennen*. Im Assistenten *Auf Datenträger brennen* ist der Datenträgertitel eingestellt, den Sie vorher eingegeben haben. Die Brenngeschwindigkeit ist auf die höchste Geschwindigkeit gestellt, die vom CD/DVD-Laufwerk unterstützt wird.
5. Sobald Sie auf *Weiter* tippen oder klicken, fügt Windows 8 die Dateien, die Sie ausgewählt haben, zu einem Datenträgerabbild hinzu und schreibt die Dateien dann auf Ihre Datendisk. Wenn der Brennvorgang beendet ist, wirft Windows 8 die Disk in der Standardeinstellung automatisch aus. Außerdem werden standardmäßig alle temporäre Dateien gelöscht. Sie können nun auf *Fertig stellen* tippen

oder klicken, um den Assistenten *Auf Datenträger brennen* zu beenden. Wenn Sie dieselben Dateien auf eine weitere Disk brennen wollen, aktivieren Sie das Kontrollkästchen *Ja, diese Dateien auf einen anderen Datenträger brennen*, bevor Sie auf *Fertig stellen* tippen oder klicken.



Abbildung 12.16 Vorbereitungen zum Brennen von Daten auf eine Disk

Sollte beim Brennvorgang ein Fehler auftreten, erhalten Sie eine Fehlermeldung. Sie haben nun die Möglichkeit, den Vorgang mit einer anderen Disk zu wiederholen, die noch nicht gebrannten temporären Dateien zu löschen oder alle temporären Dateien zu speichern, damit Sie später einen neuen Brennversuch unternehmen können. Wenn Sie es noch einmal probieren, sollten Sie diesmal eine niedrigere Brenngeschwindigkeit einstellen. Selbst wenn Ihr CD/DVD-Laufwerk mit hoher Geschwindigkeit brennen kann, ist der Rohling unter Umständen nicht für die ausgewählte Geschwindigkeit zertifiziert.

Wenn ein Fehler beim Brennen auftritt, wurde wahrscheinlich nur ein Teil Ihrer Dateien auf die Disk geschrieben. Wenn die Sitzung noch offen ist, können Sie erneut versuchen, die Disk zu brennen. Manchmal müssen Sie allerdings einen neuen Rohling einlegen.

Disks mit Livedateisystemen brennen

Gehen Sie folgendermaßen vor, um eine Datendisk mit einem Livedateisystem zu brennen:

1. Legen Sie eine leere Disk in Ihren CD/DVD-Brenner ein. Wenn der Assistent *Auf Datenträger brennen* nicht automatisch erscheint, öffnen Sie das *Computer*-Fenster. Tippen oder klicken Sie im *Computer*-Fenster doppelt auf den Brenner. Wird stattdessen das Dialogfeld *Automatische Wiedergabe* angezeigt, wählen Sie in der Aktionsliste *Dateien auf Datenträger brennen*.
2. Geben Sie im Assistenten *Auf Datenträger brennen* einen Datenträgertitel ein. Wählen Sie die Option *Wie ein USB-Speicherstick* aus, um eine UDF-Disk mit Livedateisystem zu erstellen. Sobald Sie auf *Weiter* klicken, legt Windows ein Livedateisystem auf der Disk an und öffnet sie im Datei-Explorer.
3. Der Detailbereich im Datei-Explorer ist noch leer. Schließen Sie den Datei-Explorer nicht.
4. Weil Sie mit einer Livedisk arbeiten, gibt es keine Liste der zu brennenden Dateien. Sie können nun in der Disk Dateien hinzufügen und entfernen, genau wie bei jedem anderen Datenträger. Handelt es sich um eine löschbare Disk, werden die Dateien gelöscht und der Platz wird für andere Dateien freigegeben. Bei normalen Rohlingen, die nur einmal beschrieben werden können, werden die Da-

teien als gelöscht markiert, bleiben aber auf der Disk. Daher bleibt der Platz der gelöschten Dateien belegt, er kann nicht für andere Dateien genutzt werden.

5. Während die Disk eingelegt ist, hält Windows 8 eine Brennsitzung für die Disk offen. Sobald Sie die Livedatendisk auswerfen, schließt Windows 8 die Brennsitzung, damit Sie die Disk in anderen Computern verwenden können. Später können Sie die Disk jederzeit wieder einlegen und im Datei-Explorer Dateien hinzufügen und entfernen. Windows öffnet nur eine neue Brennsitzung, wenn Sie den Inhalt der Disk ändern. Wie zuvor können Sie die Sitzung schließen, indem Sie die Disk auswerfen. Sie können eine Brennsitzung auch schließen, indem Sie im Fenster *Computer* mit der rechten Maustaste auf das CD/DVD-Laufwerk klicken oder es gedrückt halten, und den Befehl *Sitzung schließen* wählen.

Ändern der Standardbrennoptionen

Gehen Sie folgendermaßen vor, um die Standardbrennoptionen eines Computers zu ändern:

1. Öffnen Sie das *Computer*-Fenster. Klicken Sie im Fenster *Computer* mit der rechten Maustaste auf das CD/DVD-Laufwerk oder halten Sie es gedrückt, und wählen Sie den Befehl *Eigenschaften*.
2. Wählen Sie auf der Registerkarte *Aufnahme* in der Dropdownliste *Datenträger brennen* den Standardbrenner aus, sofern der Computer mehrere Brenner eingebaut hat.
3. Legen Sie mit den angebotenen Optionen fest, wo die temporären Dateien gespeichert werden.
4. Deaktivieren Sie das Kontrollkästchen *Datenträger automatisch nach einem Brennvorgang (Mastered) auswerfen*, wenn Sie nicht wollen, dass gemasterte Disks automatisch ausgeworfen werden.
5. In der Standardeinstellung schließt Windows Disks mit Livedateisystemen, sobald Sie sie auswerfen. Tippen oder klicken Sie auf *Globale Einstellungen*, um dieses Verhalten zu überprüfen oder zu ändern. Wählen Sie mit den Kontrollkästchen im Dialogfeld *Globale Einstellungen* aus, ob und wann Sitzungen geschlossen werden, und tippen oder klicken Sie auf *OK*.
6. Tippen oder klicken Sie auf *OK*, um Ihre Einstellungen zu speichern.

Verwalten von Datenträgerkomprimierung und Dateiverschlüsselung

Wenn Sie ein Laufwerk mit NTFS formatieren, können Sie in Windows 8 die Datenträgerkomprimierung oder die Dateiverschlüsselung aktivieren. Komprimierung bewirkt, dass Dateien weniger Platz auf der Festplatte benötigen, und Verschlüsselung bietet einen zusätzlichen Schutz für Ihre Daten. Datenträgerkomprimierung und Dateiverschlüsselung schließen sich gegenseitig aus, Sie können also nicht beides gleichzeitig verwenden. Durch die BitLocker-Laufwerkverschlüsselung wird allerdings keine der beiden Funktionen beeinflusst. Die BitLocker-Laufwerkverschlüsselung erstellt verschlüsselte Datenträger auf der Volumeebene und schützt einen Computer gegen externe Manipulationen, die vor dem Start des Betriebssystems erfolgen.

Komprimieren von Datenträgern und Daten

Mit der integrierten Komprimierung werden alle auf einem Laufwerk gespeicherten Dateien und Verzeichnisse bei ihrer Erstellung automatisch komprimiert. Da die Komprimierung für Benutzer unbemerkt erfolgt, kann auf komprimierte Daten wie auf normale Daten zugegriffen werden. Der Unterschied besteht darin, dass Sie auf einem komprimierten Laufwerk mehr Informationen speichern können als auf

einem nichtkomprimierten Laufwerk. Der Datei-Explorer zeigt die Namen von komprimierten Ressourcen blau an.

PRAXISTIPP

Die Komprimierung ist sicherlich eine nützliche Funktion zum Einsparen von Festplattenspeicher. Komprimierte Daten können jedoch nicht verschlüsselt werden. Komprimierung und Verschlüsselung schließen sich bei NTFS-Volumes gegenseitig aus. Sie können nicht beide Methoden gleichzeitig verwenden. Weitere Informationen zur Verschlüsselung finden Sie im Abschnitt »Verschlüsseln von Laufwerken und Daten« weiter unten in diesem Kapitel. Wenn Sie versuchen, verschlüsselte Daten zu komprimieren, werden die Daten von Windows 8 automatisch entschlüsselt und anschließend komprimiert. Wenn Sie versuchen, komprimierte Daten zu verschlüsseln, werden die Daten von Windows 8 automatisch dekomprimiert und anschließend verschlüsselt.

Komprimieren von Laufwerken

Um ein Laufwerk und seinen ganzen Inhalt zu komprimieren, gehen Sie so vor:

1. Drücken oder klicken Sie mit der rechten Maustaste im Datei-Explorer oder der Datenträgerverwaltung auf das zu komprimierende Laufwerk und tippen oder klicken Sie anschließend auf *Eigenschaften*.
2. Wählen Sie *Laufwerk komprimieren, um Speicherplatz zu sparen* und tippen oder klicken Sie auf OK.

Komprimieren von Verzeichnissen und Dateien

Wenn Sie ein Laufwerk nicht vollständig komprimieren möchten, können Sie in Windows 8 Verzeichnisse und Dateien selektiv komprimieren. Um eine Datei oder ein Verzeichnis zu komprimieren, gehen Sie wie folgt vor:

1. Tippen oder klicken Sie im Datei-Explorer mit der rechten Maustaste auf die zu komprimierende Datei oder das zu komprimierende Verzeichnis und klicken Sie anschließend auf *Eigenschaften*.
2. Tippen oder klicken Sie im entsprechenden Eigenschaftendialogfeld auf der Registerkarte *Allgemein* auf *Erweitert*. Aktivieren Sie im Dialogfeld *Erweiterte Attribute* das Kontrollkästchen *Inhalt komprimieren, um Speicherplatz zu sparen*, wie in Abbildung 12.17 dargestellt. Tippen oder klicken Sie zweimal auf OK.

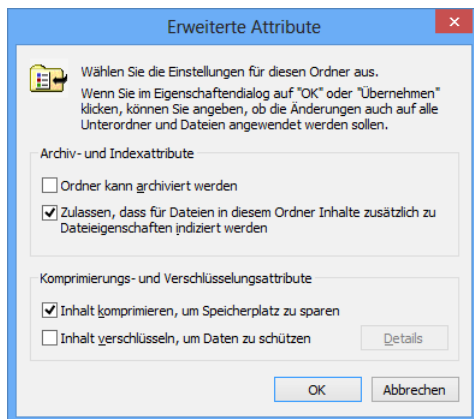


Abbildung 12.17 Komprimieren von ausgewählten Dateien oder Verzeichnissen

Einzelne Dateien markiert Windows 8 als komprimiert und komprimiert sie anschließend. Bei einem Verzeichnis markiert Windows 8 das Verzeichnis als komprimiert und komprimiert anschließend alle Dateien, die sich darin befinden. Falls das Verzeichnis Unterordner enthält, zeigt Windows 8 ein Dialogfeld an, mit dem Sie alle zu dem Verzeichnis gehörenden Unterordner komprimieren können. Wählen Sie *Änderungen für diesen Ordner, Unterordner und Dateien übernehmen* aus und tippen oder klicken Sie auf OK. Wenn Sie ein Verzeichnis komprimiert haben, werden alle neuen Dateien, die in das Verzeichnis kopiert oder darin erstellt werden, automatisch komprimiert.

HINWEIS

Wenn Sie eine nichtkomprimierte Datei von einem anderen Laufwerk in einen komprimierten Ordner verschieben, wird sie komprimiert. Wenn Sie jedoch eine nichtkomprimierte Datei in einen komprimierten Ordner auf demselben NTFS-Laufwerk verschieben, wird sie nicht komprimiert. Beachten Sie außerdem, dass komprimierte Dateien nicht verschlüsselt werden können.

Dekomprimieren komprimierter Laufwerke

Der Datei-Explorer zeigt die Namen von komprimierten Dateien und Ordnern blau an. Sie können die Komprimierung eines Laufwerks wie folgt entfernen:

1. Klicken Sie im Datei-Explorer oder der Datenträgerverwaltung mit der rechten Maustaste auf das zu erweiternde Laufwerk oder halten Sie es gedrückt, und tippen oder klicken Sie anschließend auf *Eigenschaften*.
2. Deaktivieren Sie das Kontrollkästchen *Laufwerk komprimieren, um Speicherplatz zu sparen* und tippen oder klicken Sie auf OK.

TIPP

Windows prüft immer erst den verfügbaren Speicherplatz, bevor komprimierte Daten erweitert werden. Das sollten Sie auch tun. Wenn es weniger freien als belegten Speicherplatz gibt, können Sie die Dekomprimierung unter Umständen nicht durchführen. Beispiel: Wenn ein komprimiertes Laufwerk 150 GByte Speicherplatz benutzt und 70 GByte freien Speicherplatz hat, ist nicht genug freier Speicherplatz für das Dekomprimieren des Laufwerks vorhanden. Gewöhnlich brauchen Sie ungefähr 1,5 bis 2 Mal mehr freien Speicherplatz, als komprimierte Daten vorliegen.

Dekomprimieren komprimierter Verzeichnisse und Dateien

Wenn Sie später eine komprimierte Datei oder ein komprimiertes Verzeichnis dekomprimieren möchten, kehren Sie den Vorgang wie folgt um:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf die Datei oder das Verzeichnis oder halten Sie sie gedrückt, und wählen Sie den Befehl *Eigenschaften*.
2. Tippen oder klicken Sie im entsprechenden Eigenschaftendialogfeld auf der Registerkarte *Allgemein* auf *Erweitert*. Deaktivieren Sie das Kontrollkästchen *Inhalt komprimieren, um Speicherplatz zu sparen*. Tippen oder klicken Sie zweimal auf OK.

Bei Dateien hebt Windows 8 die Komprimierung auf und erweitert die Datei. Bei Verzeichnissen dekomprimiert das Betriebssystem alle Dateien im Verzeichnis. Falls das Verzeichnis Unterordner enthält, können Sie auch bei diesen die Komprimierung entfernen. Wählen Sie dazu nach Aufforderung *Änderungen für diesen Ordner, Unterordner und Dateien übernehmen* aus und tippen oder klicken Sie auf OK.

TIPP

Windows 8 enthält auch befehlszeilenorientierte Dienstprogramme für die Komprimierung und Dekomprimierung von Daten. Das Komprimierungsprogramm heißt *Compact.exe*, das Dekomprimierungsprogramm *Expand.exe*.

Verschlüsseln von Laufwerken und Daten

NTFS bietet im Vergleich zu anderen Dateisystemen, die Sie mit Windows 8 verwenden können, viele Vorteile. Einer der Hauptvorteile ist die Möglichkeit der automatischen Ver- und Entschlüsselung durch das verschlüsselnde Dateisystem (Encrypting File System, EFS). Durch die Datenverschlüsselung versehen Sie vertrauliche Daten mit einem zusätzlichen Schutz, der verhindert, dass andere Benutzer den Inhalt der verschlüsselten Daten lesen können. Einer der besonderen Vorteile der Verschlüsselung ist also, dass nur der vorgesehene Benutzer auf die Daten zugreifen kann. Allerdings ist dieser Vorteil auch in der Hinsicht ein Nachteil, dass der Benutzer die Verschlüsselung entfernen muss, damit autorisierte Benutzer auf die Daten zugreifen können.

HINWEIS

Wie zuvor erwähnt, können Sie verschlüsselte Dateien nicht komprimieren, da sich die Verschlüsselungs- und Komprimierungsfunktionen von Windows 8 gegenseitig ausschließen. Sie können nur eine der Funktionen, jedoch nicht beide gleichzeitig verwenden.

Grundlagen der Verschlüsselung und des verschlüsselnden Dateisystems

Die Dateiverschlüsselung wird auf Ordner- oder Dateibasis unterstützt. Eine Datei, die in einem für die Verschlüsselung markierten Ordner abgelegt wird, wird automatisch verschlüsselt. Dateien im verschlüsselten Format können nur von dem Benutzer gelesen werden, der die Datei verschlüsselt hat. Bevor andere Benutzer eine verschlüsselte Datei lesen können, muss der Benutzer die Datei entschlüsseln.

Eine verschlüsselte Datei hat einen eindeutigen Verschlüsselungsschlüssel. Dies bedeutet, dass eine verschlüsselte Datei wie jede andere Datei kopiert, verschoben und umbenannt werden kann, wobei diese Aktionen in den meisten Fällen keinen Einfluss auf die Verschlüsselung der Daten haben (Einzelheiten finden Sie im Abschnitt »Arbeiten mit verschlüsselten Dateien und Ordnern« weiter unten in diesem Kapitel). Der Benutzer, der die Datei verschlüsselt hat, kann immer auf die Datei zugreifen. Voraussetzung ist, dass das Verschlüsselungszertifikat des Benutzers auf dem Computer verfügbar ist, den er benutzt. Für diesen Benutzer erfolgt der Ver- und Entschlüsselungsprozess automatisch und unbemerkt.

EFS ist der Prozess, der die Ver- und Entschlüsselung vornimmt. In der Standardeinrichtung des EFS können Benutzer Dateien verschlüsseln, ohne dazu eine Sonderberechtigung zu benötigen. Dateien werden mit einem öffentlichen/privaten Schlüssel verschlüsselt, der vom EFS für jeden einzelnen Benutzer automatisch erzeugt wird.

Verschlüsselungszertifikate werden als Teil der Daten in Benutzerprofilen gespeichert. Wenn ein Benutzer mit mehreren Computern arbeitet und die Verschlüsselung nutzen möchte, muss ein Administrator für diesen Benutzer ein servergespeichertes Profil konfigurieren. Ein servergespeichertes Profil stellt sicher, dass von anderen Computern auf die Profildaten und Verschlüsselungszertifikate des Benutzers zugegriffen werden kann. Ohne diese Konfiguration können Benutzer nicht von anderen Computern auf ihre verschlüsselten Dateien zugreifen.

Obwohl sie separate Funktionen sind, enthalten sowohl die BitLocker-Laufwerkverschlüsselung als auch EFS ein integriertes Datenwiederherstellungssystem zum Schutz gegen Datenverlust. Dieses Wiederherstellungssystem sorgt dafür, dass verschlüsselte Daten wiederhergestellt werden können, falls das auf öffentlichen Schlüsseln basierende Zertifikat eines Benutzers verloren geht oder gelöscht wird. Dies ist häufig der Fall, wenn ein Benutzer das Unternehmen verlässt und das dazugehörige Benutzerkonto gelöscht wird. Auch wenn sich ein Vorgesetzter an dem Benutzerkonto anmelden, Dateien überprüfen und wichtige Dateien in anderen Ordnern speichern konnte, ist nach einem Löschen des Benutzerkontos der Zugriff auf verschlüsselte Dateien und Volumes nur möglich, wenn die Verschlüsselung entfernt wird.

oder die Dateien auf ein FAT- oder FAT32-Volume verschoben werden (auf denen EFS-Verschlüsselung nicht unterstützt wird und die BitLocker-Verschlüsselung nicht aktiviert ist).

Um nach dem Löschen des Benutzerkontos auf verschlüsselte Dateien zuzugreifen, brauchen Sie einen Wiederherstellungs-Agenten. Wiederherstellungs-Agenten haben Zugriff auf den Dateiverschlüsselungsschlüssel, der zum Entsperren von Daten in verschlüsselten Dateien benötigt wird. Um vertrauliche Daten zu schützen, können Wiederherstellungs-Agenten allerdings nicht auf den privaten Schlüssel eines Benutzers oder auf Informationen zu privaten Schlüsseln zugreifen.

Windows 8 verschlüsselt Volumes, auch wenn keine BitLocker-Wiederherstellungs-Agenten definiert sind, aber Windows 8 verschlüsselt Dateien nur, wenn EFS-Wiederherstellungs-Agenten eingerichtet worden sind. Aus diesem Grund werden EFS-Wiederherstellungs-Agenten automatisch zugewiesen. Auch die erforderlichen Wiederherstellungszertifikate werden automatisch erzeugt. Dies stellt sicher, dass verschlüsselte Dateien auf jeden Fall wiederhergestellt werden können.

Wiederherstellungs-Agenten werden auf zwei Ebenen konfiguriert:

- **Domäne** Der Wiederherstellungs-Agent für eine Domäne wird automatisch konfiguriert, wenn der erste Windows 8-Domänencontroller installiert wird. Der standardmäßige Wiederherstellungs-Agent ist der Domänenadministrator. In den Gruppenrichtlinien können Domänenadministratoren weitere Wiederherstellungs-Agenten zuweisen. Domänenadministratoren können für Wiederherstellungs-Agenten geltende Rechte auch an vorgesehene Sicherheitsadministratoren delegieren.
- **Lokaler Computer** Wenn ein Computer zu einer Arbeitsgruppe oder einer eigenständigen Konfiguration gehört, ist der Administrator des lokalen Computers standardmäßig der Wiederherstellungs-Agent. Weitere Wiederherstellungs-Agenten können bestimmt werden. Wenn Sie darüber hinaus in einer Domänenumgebung lokale Wiederherstellungs-Agenten anstelle von Wiederherstellungs-Agenten auf Domänenebene wünschen, müssen Sie die Wiederherstellungsrichtlinie aus der Gruppenrichtlinie für die Domäne löschen.

Sie können Wiederherstellungs-Agenten löschen, wenn sie nicht eingesetzt werden sollen. Wenn Sie jedoch alle Wiederherstellungs-Agenten für EFS löschen, verschlüsselt EFS keine Dateien mehr. Damit EFS ordnungsgemäß arbeiten kann, muss mindestens ein Agent konfiguriert werden.

Verschlüsseln von Verzeichnissen und Dateien

Bei NTFS-Volumes lässt Sie Windows 8 die Dateien und Ordner zur Verschlüsselung auswählen. Wenn Sie eine Datei verschlüsseln, werden die darin enthaltenen Daten in ein verschlüsseltes Format umgewandelt, das nur von der Person gelesen werden kann, die die Datei verschlüsselt hat. Benutzer können Dateien nur dann verschlüsseln, wenn Sie die entsprechenden Zugriffsberechtigungen besitzen. Wenn Sie Ordner verschlüsseln, wird der Ordner zwar als verschlüsselt markiert, in Wirklichkeit werden jedoch nur die darin enthaltenen Dateien verschlüsselt. Alle Dateien, die in einem als verschlüsselt markierten Ordner erstellt oder zu ihm hinzugefügt werden, werden automatisch verschlüsselt. Der Datei-Explorer zeigt die Namen von verschlüsselten Ressourcen grün an.

Um eine Datei oder ein Verzeichnis zu verschlüsseln, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die zu verschlüsselnde Datei oder auf das zu verschlüsselnde Verzeichnis oder halten Sie sie gedrückt und wählen Sie anschließend *Eigenschaften*.
2. Tippen oder klicken Sie im Eigenschaftendialogfeld auf der Registerkarte *Allgemein* auf *Erweitert*. Aktivieren Sie anschließend das Kontrollkästchen *Inhalt verschlüsseln, um Daten zu schützen*. Tippen oder klicken Sie zweimal auf OK.

HINWEIS

Komprimierte Dateien, Systemdateien und schreibgeschützte Dateien lassen sich nicht verschlüsseln. Wenn Sie versuchen, komprimierte Dateien zu verschlüsseln, werden sie automatisch dekomprimiert und anschließend verschlüsselt. Der Versuch, Systemdateien zu verschlüsseln, führt zu einem Fehler.

Windows 8 markiert eine einzelne Datei als verschlüsselt und verschlüsselt sie anschließend. Bei einem Verzeichnis markiert Windows 8 das Verzeichnis als verschlüsselt und verschlüsselt anschließend alle Dateien, die sich darin befinden. Falls das Verzeichnis Unterordner enthält, zeigt Windows 8 ein Dialogfeld an, in dem Sie alle zu dem Verzeichnis gehörenden Unterordner verschlüsseln können. Wählen Sie *Änderungen für diesen Ordner, Unterordner und Dateien übernehmen* aus und tippen oder klicken Sie zweimal auf OK.

HINWEIS

Auf NTFS-Volumes bleiben Dateien auch dann verschlüsselt, wenn sie verschoben, kopiert oder umbenannt werden. Wenn Sie eine verschlüsselte Datei auf ein FAT-, FAT32- oder exFAT-Laufwerk kopieren oder verschieben, wird sie vor dem Vorgang automatisch entschlüsselt. Deshalb müssen Sie zum Kopieren oder Verschieben der Datei die entsprechenden Berechtigungen besitzen.

Arbeiten mit verschlüsselten Dateien und Ordnern

Ich habe bereits erwähnt, dass Sie verschlüsselte Dateien und Ordner wie andere Dateien kopieren, verschieben und umbenennen können. Das stimmt zwar, aber nur »in den meisten Fällen«. Beim Arbeiten mit verschlüsselten Dateien treten kaum Probleme auf, solange Sie mit NTFS-Volumes auf demselben Computer arbeiten. Wenn Sie mit anderen Dateisystemen oder anderen Computern arbeiten, können dagegen gewisse Probleme auftreten. Zwei der gängigsten Szenarien sind die folgenden:

- **Kopieren zwischen Volumes auf demselben Computer** Wenn Sie verschlüsselte Dateien oder Ordner auf demselben Computer von einem NTFS-Volume in ein anderes kopieren oder verschieben, bleiben die Dateien verschlüsselt. Wenn Sie jedoch verschlüsselte Dateien auf ein FAT-, FAT32- oder exFAT-Volume kopieren oder verschieben, werden die Dateien vor der Übertragung entschlüsselt und anschließend als Standarddateien übertragen und am Zielort unverschlüsselt gespeichert. FAT, FAT32 und exFAT unterstützen die Verschlüsselung nicht.
- **Kopieren zwischen Volumes auf verschiedenen Computer** Wenn Sie verschlüsselte Dateien oder Ordner von einem NTFS-Volume auf ein anderes kopieren oder verschieben, das auf einem anderen Computer liegt, bleiben die Dateien verschlüsselt, solange der Zielcomputer die Verschlüsselung von Dateien zulässt und dem Remotecomputer für Delegierungszwecke vertraut wird. Andernfalls werden die Dateien entschlüsselt und als Standarddateien übertragen. Gleiches gilt, wenn Sie verschlüsselte Dateien auf ein FAT-, FAT32- oder exFAT-Volume auf einem anderen Computer kopieren oder verschieben. FAT, FAT32 und exFAT unterstützen die Verschlüsselung nicht.

Nachdem Sie eine vertrauliche Datei übertragen haben, die verschlüsselt wurde, möchten Sie bestimmt prüfen, ob sie noch verschlüsselt ist. Klicken Sie mit der rechten Maustaste auf die Datei oder halten Sie sie gedrückt, und wählen Sie *Eigenschaften*. Tippen oder klicken Sie im Eigenschaftendialogfeld auf der Registerkarte *Allgemein* auf *Erweitert*. Das Kontrollkästchen *Inhalt verschlüsseln, um Daten zu schützen* sollte aktiviert sein.

Konfigurieren von Wiederherstellungsrichtlinien

In Domänen werden EFS- und BitLocker-Wiederherstellungsrichtlinien für Domänencontroller und Mitgliedscomputer automatisch konfiguriert. Domänenadministratoren sind standardmäßig auch die EFS- und BitLocker-Wiederherstellungs-Agenten für alle Computer in der Domäne. In Arbeitsgruppen

oder Heimnetzgruppen ist der lokale Administrator der EFS-Wiederherstellungs-Agent für eine eigenständige Arbeitsstation. BitLocker hat keinen Standardwiederherstellungs-Agenten für Heimnetzgruppen oder Arbeitsgruppen.

Im Gruppenrichtlinienverwaltungs-Editor können Sie Wiederherstellungs-Agenten anzeigen, zuweisen und löschen. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten.
2. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor den Knoten mit den Dateiwiederherstellungs-Agenten. Erweitern Sie dazu *Computerkonfiguration*, *Windows-Einstellungen*, *Sicherheitseinstellungen* und *Richtlinien für öffentliche Schlüssel* und wählen Sie entweder *Verschlüsselndes Dateisystem* oder *BitLocker-Laufwerkverschlüsselung*, je nachdem, welchen Wiederherstellungs-Agenten Sie bearbeiten wollen.
3. Im rechten Bereich des Fensters werden die gegenwärtig zugewiesenen Wiederherstellungszertifikate aufgeführt. Wiederherstellungszertifikate werden unter anderem nach dem Zertifikatsempfänger, dem Aussteller, dem Ablaufdatum und dem Zweck aufgeführt.
4. Um einen weiteren Wiederherstellungs-Agenten zuzuweisen, klicken Sie mit der rechten Maustaste auf *Verschlüsselndes Dateisystem* oder *BitLocker-Laufwerkverschlüsselung* oder halten den Knoten gedrückt, und wählen *Datenwiederherstellungs-Agenten hinzufügen*. Der *Assistent für das Hinzufügen eines Wiederherstellungs-Agenten* wird gestartet. Hier können Sie ein zuvor erzeugtes Zertifikat auswählen, das einem Benutzer zugewiesen wurde, und es als vorgesehenes Wiederherstellungszertifikat markieren. Tippen oder klicken Sie auf *Weiter*.
5. Tippen oder klicken Sie im Dialogfeld *Wiederherstellungs-Agenten auswählen* auf *Verzeichnis durchsuchen* und wählen Sie anschließend im Dialogfeld *Benutzer, Kontakte, Gruppen suchen* den Benutzer, mit dem Sie arbeiten möchten.

HINWEIS

Bevor Sie weitere Wiederherstellungs-Agenten zuweisen können, müssen Sie in der Domäne eine Stammzertifizierungsstelle einrichten. Danach müssen Sie mit dem Snap-In *Zertifikate* ein persönliches Zertifikat anfordern, das die Vorlage *EFS-Wiederherstellungs-Agent* verwendet. Die Stammzertifizierungsstelle muss anschließend die Zertifikatsanforderung gegebenenfalls genehmigen, damit das Zertifikat erstellt wird und verwendet werden kann.

6. Um einen Wiederherstellungs-Agenten zu löschen, wählen Sie im rechten Fenster das Zertifikat des Wiederherstellungs-Agenten aus und drücken die ENTF-Taste. Wenn Sie zum Bestätigen der Aktion aufgefordert werden, tippen oder klicken Sie auf *Ja*, um das Zertifikat unwiderruflich zu löschen. Falls die Wiederherstellungsrichtlinie für EFS leer ist (was bedeutet, dass es keine weiteren zugewiesenen Wiederherstellungs-Agenten gibt), wird das verschlüsselnde Dateisystem ausgeschaltet und es werden keine Dateien mehr verschlüsselt. Für die vorhandenen EFS-verschlüsselten Ressourcen gibt es dann keinen Wiederherstellungs-Agenten mehr.

Freigeben verschlüsselter Dateien

Standardmäßig können verschlüsselte Dateien nur von ihren Besitzern eingesehen werden. Wenn auch andere Benutzer Zugriff auf den Inhalt einer verschlüsselten Datei erhalten sollen, müssen Sie die Datei entschlüsseln oder den Benutzern auf folgende Weise ein spezielles Zugriffsrecht auf die Datei gewähren:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf die Datei oder den Ordner oder halten Sie sie gedrückt und wählen Sie den Befehl *Eigenschaften*.

2. Tippen oder klicken Sie auf der Registerkarte *Allgemein* des Eigenschaftendialogfelds auf *Erweitert* und dann im Dialogfeld *Erweiterte Attribute* auf *Details*.
Das Dialogfeld *Benutzerzugriff auf* erscheint und listet namentlich die Benutzer auf, die Zugriff auf die verschlüsselte Datei haben.
3. Um anderen Benutzern Zugriff auf die Datei zu gewähren, tippen oder klicken Sie auf *Hinzufügen*.
4. Sofern für den Benutzer, dem Sie Zugriff gewähren, ein Benutzerzertifikat verfügbar ist, wählen Sie den Namen des Benutzers in der Liste aus und tippen oder klicken dann auf *OK*.

Entschlüsseln von Verzeichnissen und Dateien

Der Datei-Explorer zeigt die Namen verschlüsselter Ressourcen grün an. Wenn Sie später eine Datei oder ein Verzeichnis entschlüsseln möchten, kehren Sie den Vorgang wie folgt um:

1. Tippen oder klicken Sie im Datei-Explorer mit der rechten Maustaste auf die Datei oder das Verzeichnis oder halten Sie sie gedrückt und wählen Sie *Eigenschaften*.
2. Tippen oder klicken Sie im Eigenschaftendialogfeld auf der Registerkarte *Allgemein* auf *Erweitert*. Deaktivieren Sie das Kontrollkästchen *Inhalt verschlüsseln, um Daten zu schützen*. Tippen oder klicken Sie zweimal auf *OK*.

Dateien werden von Windows 8 entschlüsselt und in ihrem ursprünglichen Format wiederhergestellt. Bei Verzeichnissen werden alle darin enthaltenen Dateien entschlüsselt. Falls das Verzeichnis Unterordner enthält, können Sie auch bei diesen die Verschlüsselung entfernen. Wählen Sie dazu nach Aufforderung *Änderungen für diesen Ordner, Unterordner und Dateien übernehmen* aus und tippen oder klicken Sie auf *OK*.

TIPP Windows 8 enthält auch ein befehlszeilenorientiertes Dienstprogramm für die Ver- und Entschlüsselung von Daten. Es hat den Namen *Cipher.exe*. Wenn Sie in der Befehlszeile nur **cipher** eingeben, wird der Verschlüsselungsstatus aller Ordner im aktuellen Verzeichnis angezeigt.

Kapitel 13

Verwalten der Dateisicherheit und Ressourcenfreigabe

In diesem Kapitel:

Optionen für die Dateisicherheit und Dateifreigabe	494
Kontrollieren des Zugriffs auf Dateien und Ordner mit NTFS-Berechtigungen	499
Freigeben von Dateien und Ordnern im Netzwerk	516
Verwenden und Konfigurieren der Freigabe öffentlicher Ordner	530
Überwachen von Datei- und Ordnerzugriff	532

Ob Sie Windows 8 nun in einer Domäne, einer Arbeitsgruppe oder einer Heimnetzgruppe verwenden, nur wenige Aspekte des Betriebssystems sind wichtiger als die Sicherheit und die Freigabe von Dateien. Dateisicherheit und Dateifreigabe sind so eng miteinander verflochten, dass es kaum möglich ist, von dem einen Punkt zu reden, ohne den anderen zu erwähnen. *Dateisicherheit* bedeutet, dass wichtige Daten auf Ihren Systemen geschützt werden, indem der Zugriff auf Daten beschränkt wird. *Dateifreigabe* bedeutet, dass auch andere Benutzer auf Daten zugreifen und mehrere Benutzer die freigegebenen Dateien gemeinsam verwenden dürfen.

Optionen für die Dateisicherheit und Dateifreigabe

Auf Windows 8-Computern hängt die Sicherheit und Freigabe von Dateien von zwei Faktoren ab, nämlich vom Datenträgerformat und von den Computereinstellungen. Vom Format des Datenträgers hängt es ab, welche Sicherheitsoptionen verfügbar sind. Datenträger können mit dem FAT-Dateisystem (FAT16, FAT32 oder exFAT) oder dem Dateisystem NTFS formatiert werden. Die Sicherheitsoptionen von FAT- und NTFS-Volumes unterscheiden sich sehr stark.

- FAT bietet Ihnen nur eine sehr begrenzte Kontrolle über den Dateizugriff. Dateien können nur als *Schreibgeschützt*, *Verborgen* oder *System* gekennzeichnet werden. Diese Flags können zwar für Dateien und Ordner festgelegt werden, aber wer Zugriff auf das FAT-Volume hat, kann diese Einstellungen außer Kraft setzen oder ändern. Das bedeutet, dass es letztlich keinen zuverlässigen Schutz vor Dateizugriffen oder Löschungen gibt. Jeder Benutzer kann praktisch ohne Einschränkung auf jede Datei zugreifen oder sie löschen.
- NTFS bietet Ihnen die Kontrolle des Zugriffs auf Dateien und Ordner, indem Sie Berechtigungen vergeben, die den Zugriff explizit erlauben oder verbieten. Solche Berechtigungen lassen sich für einzelne Benutzer oder für Gruppen vergeben. Das gibt Ihnen eine sehr genaue Kontrolle über Datei- und Ordnerzugriffe. Sie können beispielsweise festlegen, dass Benutzer aus der Gruppe der Manager den Vollzugriff auf einen Ordner und seine Dateien haben, aber die Benutzer aus der Gruppe der Vertreter keinen irgendwie gearteten Zugriff auf diesen Ordner erhalten.

Die Einstellung des Computers bestimmt, wie Dateien freigegeben werden können. Für SMB (Server Message Block) unterstützt Windows 8 zwei Dateifreigabemodelle:

- **Standardordnerfreigabe** Ermöglicht Ihnen die Freigabe von Dateien aus jedem Ordner Ihres Computers, auf FAT- und auf NTFS-Volumes. Wer Zugriff auf freigegebene Ordner erhält, ergibt sich aus zwei Berechtigungssätzen, nämlich aus den Zugriffsberechtigungen (sie werden im Abschnitt »Kontrollieren des Zugriffs auf Dateien und Ordner mit NTFS-Berechtigungen« weiter unten in diesem Kapitel besprochen) und den Freigabeberechtigungen (sie werden im Abschnitt »Freigeben von Dateien und Ordnern im Netzwerk« weiter unten in diesem Kapitel besprochen). Zusammengenommen ermöglichen Ihnen Freigabe- und Zugriffsberechtigungen die Kontrolle darüber, wer Zugriff auf freigegebene Ordner erhält und wie weit dieser Zugriff reicht. Sie brauchen die Dateien, die Sie freigeben, nicht extra an spezielle Orte zu kopieren.
- **Freigabe in öffentlichen Ordnern** Ermöglicht die Freigabe von Dateien aus dem Ordner *%SystemDrive%\Users\Public* eines Computers (in der Benutzeroberfläche heißt dieser Ordner *Öffentlich*). Aus den Zugriffsberechtigungen für den Ordner *Public* geht hervor, welche Benutzer und Gruppen Zugriff auf öffentlich freigegebene Dateien erhalten und wie weit dieser Zugriff reicht. Wenn Sie Dateien in den Ordner *Public* verschieben oder kopieren, werden die Zugriffsberechtigungen so geändert, dass sie zum Ordner *Public* passen. Außerdem werden noch einige zusätzliche Berechtigungen festgelegt. Weitere Informationen finden Sie im Abschnitt »Verwenden und Konfigurieren der Freigabe öffentlicher Ordner« weiter unten in diesem Kapitel.

HINWEIS

Bei der Standardordnerfreigabe erhalten lokale Benutzer nicht automatisch Zugriff auf Daten, die auf einem Computer gespeichert sind. Der lokale Zugang zu Dateien und Ordnern wird durch die Sicherheitseinstellungen auf dem lokalen Datenträger kontrolliert. Wenn ein lokaler Datenträger mit FAT formatiert ist, können Sie zwar versuchen, Dateien und Ordner mit den Flags *Schreibgeschützt*, *Verborgen* oder *System* zu schützen, aber Sie können den Zugang nicht beschränken. Wenn der lokale Datenträger mit NTFS formatiert ist, können Sie den Zugang sehr genau kontrollieren, indem Sie einzelnen Benutzern oder Gruppen den Zugang gestatten oder verwehren.

Bei der Freigabe durch öffentliche Ordner werden Dateien, die in den Ordner *Public* kopiert werden, für jeden zugänglich, der sich lokal anmelden kann, und zwar unabhängig davon, ob er auf dem Computer über ein Administratorkonto oder nur über ein Standardbenutzerkonto verfügt. Auch der Zugriff über das Netzwerk kann für den Ordner *Public* zugelassen werden. Dadurch wird der Ordner *Public* und sein Inhalt für jeden zugänglich, der via Netzwerk Zugriff auf den Computer hat.

Windows Server 2012 ergänzt das Sicherheitssystem durch zusätzliche Schichten mit Verbundidentitäten, forderungs- oder anspruchsbasierter Zugangssteuerung und zentralen Zugangsrichtlinien. Unter Windows 8 und Windows Server 2012 können Sie eine forderungsbasierte Zugangssteuerung für Dateien und Ordner auf NTFS-Volumes einrichten. Unter Windows Server 2012 wird der Zugang von Benutzern zu Dateien und Ordnern entweder direkt über Zugriffs- und Freigabeberechtigungen oder indirekt mit einer forderungsbasierten Zugangssteuerung und zentralen Zugangsrichtlinien gesteuert.

Im Gegensatz zu älteren Windows-Versionen, bei denen sich immer nur ein Freigabemodell einsetzen ließ, können Windows 8-Computer beide Freigabemodelle zusammen verwenden. Der Hauptvorteil der Standardfreigabe ist, dass die Benutzer jeden beliebigen Ordner auf einem Computer freigeben können. Sie brauchen dazu keine Dateien oder Ordner an einen anderen Ort zu kopieren oder zu verschieben. Öffentliche Ordner sind dagegen festgelegte Orte für den Austausch von Dateien. Wenn Benutzer Dateien und Ordner in öffentliche Ordner kopieren (und die Freigabe in öffentlichen Ordnern aktiviert ist), stehen diese Dateien und Ordner anderen Benutzern auf dem Computer und im Netzwerk zur Verfügung.

Der Datei-Explorer bietet mehrere Optionen, wenn Sie Ordner auswählen:

- **In Bibliothek aufnehmen** Erstellt zwischen dem Ordner und seinem Inhalt eine Verknüpfung mit einem der Ordner *Dokumente*, *Musik*, *Bilder*, *Videos* oder einem anderen Bibliotheksordner des Benutzers. Der Benutzer kann dann den Inhalt des Ordners durchsuchen und bearbeiten, als wäre er Teil der angegebenen Bibliothek. Aber immer, wenn der Benutzer in einem Bibliotheksordner mit einer dieser Dateien arbeitet, greift er in Wirklichkeit auf die Datei an ihrem ursprünglichen Speicherort zu.
- **Freigeben für** Gibt den Ordner über die Standardordnerfreigabe frei. In einer Heimnetzgruppe haben Benutzer die Möglichkeit, den Ordner für alle anderen in der Heimnetzgruppe freizugeben, und zwar entweder schreibgeschützt oder mit Lese-/Schreibzugriff. In einer Arbeitsgruppe oder Domäne können die Benutzer auswählen, für welche Personen sie den Ordner freigeben wollen. In beiden Fällen können die Benutzer außerdem *Freigabe beenden* wählen und die Freigabe damit beenden.

Die Standardfreigabekonfiguration für Computer hängt davon ab, ob sie Mitglieder von Heimnetzgruppen, Arbeitsgruppen oder Domänen sind. Wenn Sie eine Heimnetzgruppe einrichten, legen Sie fest, welche Dateitypen freigegeben werden und ob Drucker freigegeben werden. Computer, die Mitglieder derselben Heimnetzgruppe sind, können dann automatisch Dateien wie Bilder, Musik, Videos und Dokumente sowie Drucker freigeben.

Es ist recht simpel, Ordner innerhalb einer Heimnetzgruppe schreibgeschützt oder mit Lese-/Schreibzugriff freizugeben. Gehen Sie folgendermaßen vor, um die Freigabe in einer Heimnetzgruppe zu aktivieren:

1. Klicken Sie den gewünschten Ordner im Datei-Explorer mit der rechten Maustaste an oder halten Sie ihn gedrückt.
2. Wählen Sie *Freigeben für* und dann *Heimnetzgruppe (anzeigen)* oder *Heimnetzgruppe (anzeigen und bearbeiten)*.

Dieses simple Verfahren zum Freigeben von Ordnern mag für Benutzer, die in Büros arbeiten, recht verlockend aussehen. Dabei wird aber auch ein sehr weitgehender Zugriff auf die Daten des Benutzers gewährt. Am Arbeitsplatz ist davon im Allgemeinen abzuraten. Aus diesem Grund sollten Sie die Benutzer in einer Heimnetzgruppe auffordern, Daten lieber für bestimmte Personen freizugeben statt für alle. Die Freigabe für bestimmte Personen ist die einzige Technik, die Sie in Arbeitsgruppen und Domänen nutzen können.

Gehen Sie folgendermaßen vor, um die Freigabe für bestimmte Personen zu aktivieren:

1. Klicken Sie den gewünschten Ordner im Datei-Explorer mit der rechten Maustaste an oder halten Sie ihn gedrückt.
2. Wählen Sie *Freigeben für* und dann *Bestimmte Personen*. Daraufhin öffnet sich der Dateifreigabe-Assistent. In der Standardeinstellung ist die lokale Gruppe *Administratoren* als Besitzer der Freigabe eingetragen, und der momentan angemeldete Benutzer bekommt Lese-/Schreibzugriff gewährt.
3. Wählen Sie im Dateifreigabe-Assistenten mit den verfügbaren Optionen aus, für welche Personen die Freigabe gelten soll. Wollen Sie beispielsweise alle Benutzer auswählen, die lokale Konten auf dem Computer haben, können Sie den Gruppennamen *Benutzer* eingeben und auf *Hinzufügen* tippen oder klicken. Das ist etwas anderes als die Freigabe für alle, weil die Gruppe *Jeder* alle Konten umfasst, die Zugriffsberechtigung auf den Computer haben, und nicht nur die Konten, die Domänen- oder lokale Benutzer sind.
4. Die Standardfreigabeberechtigung ist schreibgeschützt (*Lesen*). Sie stellen eine Berechtigungsstufe für einen Benutzer oder eine Gruppe ein, indem Sie auf den Benutzer- oder Gruppennamen tippen oder klicken und dann *Lesen* oder *Lesen/Schreiben* auswählen.
5. Tippen oder klicken Sie auf *Freigabe*, um den Ordner freizugeben, und dann auf *Fertig*.

Gehen Sie folgendermaßen vor, um Freigaben zu entfernen:

1. Klicken Sie den gewünschten Ordner im Datei-Explorer mit der rechten Maustaste an oder halten Sie ihn gedrückt.
2. Wählen Sie *Freigeben für* und dann *Freigabe beenden*.
3. Wählen Sie im Dateifreigabe-Assistenten *Freigabe beenden*.

Wenn Sie die erste Standardordnerfreigabe auf einem Computer anlegen, erstellt Windows standardmäßig die Ausnahme für Datei- und Druckerfreigabe in der Windows-Firewall. Diese eingehende Ausnahme erlaubt anderen Computern im Netzwerk, SMB-Verkehr (Server Message Block) durch die Windows-Firewall zu senden, um auf die Freigabe zuzugreifen. Um das zuzulassen, öffnet Windows die folgenden Ports:

- UDP-Port 137, der für die NetBIOS-Namensauflösung benutzt wird
- UDP-Port 138, der für NetBIOS-Datagrammübertragung und -empfang benutzt wird
- TCP-Port 139, der für den NetBIOS-Sitzungsdienst benutzt wird
- Dynamische Ports für ICMPv4 und ICMPv6 (die bei Bedarf für Echoanforderungen benutzt werden)

Damit ist im Grunde auch schon erklärt, wie die Standardordnerfreigabe funktioniert. Weiter unten in diesem Kapitel beschreibe ich genauer, wie die Freigabe für bestimmte Personen arbeitet. Aber bevor irgendjemand etwas freigeben kann, muss die Netzwerkfreigabe aktiviert sein.

Die Netzwerkfreigabeeinstellungen dienen dazu, ausreichende Sicherheit für jede der verschiedenen Netzwerkategorien zu gewährleisten, mit denen sich ein Computer verbindet. Aus diesem Grund pflegt Windows für jeden Netzwerktyp, den ein Computer nutzt, ein separates Netzwerkprofil. Im Allgemeinen sind die meisten Netzwerkerkennungs- und Freigabeeinstellungen standardmäßig deaktiviert. Gehen Sie folgendermaßen vor, um Netzwerkerkennungs- und Freigabeeinstellungen zu konfigurieren:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Heimnetzgruppen- und Freigabeoptionen auswählen* und dann auf die Verknüpfung *Erweiterte Freigabeeinstellungen ändern*.
2. Jedes verfügbare Netzwerkprofil hat einen eigenen Verwaltungsabschnitt mit den jeweiligen Konfigurationseinstellungen. Tippen oder klicken Sie auf die Pfeilschaltfläche, um das Profil anzuzeigen, das Sie bearbeiten wollen.
3. Die Netzwerkerkennung, eine Option für private, öffentliche und Domänennetzwerke, wirkt sich darauf aus, ob ein Computer andere Computer und Geräte im Netzwerk findet und ob andere Computer im Netzwerk diesen Computer finden. Schalten Sie die Netzwerkerkennung an oder aus, indem Sie die entsprechende Option auswählen.
4. Die Datei- und Druckerfreigabe, ebenfalls eine Option für private, öffentliche und Domänennetzwerke, steuert, ob ein Computer Dateien und Drucker freigeben kann. Schalten Sie die Datei- und Druckerfreigabe an oder aus, indem Sie die entsprechende Option auswählen.
5. Die Freigabe des öffentlichen Ordners unter *Alle Netzwerke* steuert, ob ein Computer Dateien in den öffentlichen Ordnern freigeben kann. Schalten Sie die Freigabe des öffentlichen Ordners an oder aus, indem Sie die entsprechende Option auswählen.
6. Medienstreaming unter *Alle Netzwerke* erlaubt den Benutzern, Musik, Videos und Bilder freizugeben und auf Musik, Videos und Bilder auf anderen Computern zuzugreifen. Schalten Sie das Medienstreaming ein, indem Sie auf die entsprechende Verknüpfung und dann auf die Schaltfläche *Medienstreaming aktivieren* klicken, und konfigurieren Sie dann die gewünschten Optionen für das Medienstreaming. Wenn Sie anderen Benutzern erlauben, von Ihren Computern aus Musik zu hören, Videos abzuspielen und Bilder anzuzeigen, kann sich das auf die Leistung auswirken, daher sollten Sie sich genau überlegen, ob Sie dieses Feature aktivieren.
7. Windows setzt Verschlüsselung ein, um Ihre freigegebenen Daten sicher zu übertragen. In der Standardeinstellung ist die Verschlüsselungsstufe auf 128-Bit-Verschlüsselung eingestellt (in den meisten Konfigurationen). Sie sollten aber sicherstellen, dass die Computer und Geräte, für die Sie Daten freigeben, diese Verschlüsselungsstufe auch unterstützen. Wählen Sie andernfalls eine niedrigere Verschlüsselungsstufe aus oder aktualisieren Sie die Verschlüsselungsunterstützung auf den anderen Geräten und Computern.
8. In Arbeitsgruppen und Heimnetzgruppen sorgt das kennwortgeschützte Freigeben dafür, dass nur Benutzer, die über ein Konto und ein Kennwort auf dem lokalen Computer verfügen, auf freigegebene Ressourcen zugreifen dürfen. Schalten Sie das kennwortgeschützte Freigeben an oder aus, indem Sie die entsprechende Option auswählen.
9. Tippen oder klicken Sie auf *Änderungen speichern*, um Ihre Einstellungen zu speichern.

In den Gruppenrichtlinien können Sie verhindern, dass Computer einer Heimnetzgruppe beitreten, indem Sie die Richtlinie *Beitritt des Computers zu einer Heimnetzgruppe verhindern* aktivieren. Diese Richtlinie befindet sich im Zweig *Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Heimnetzgruppe*.

Außerdem können Sie in den Gruppenrichtlinien einschränken, auf welche Weise die Freigabe arbeitet. Die wesentlichen Einschränkungen für die Freigabefunktionen werden in der Richtlinie *Verhindert, dass Benutzer Dateien innerhalb ihres Profils freigeben* konfiguriert. Sie finden diese Richtlinie unter *Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Netzwerkfreigabe*. Diese Einstellung kontrolliert, ob die Freigabe in Ordnern erlaubt ist, die einem Benutzerprofil zugeordnet sind, insbesondere im Ordner %SystemDrive%\Users. Beachten Sie bitte folgende Punkte, wenn Sie mit der Einstellung *Verhindert, dass Benutzer Dateien innerhalb ihres Profils freigeben* arbeiten:

- Ist diese Einstellung *Nicht konfiguriert* (die Standardeinstellung), dürfen Benutzer Dateien für andere Benutzer aus dem Netzwerk freigeben, sofern sich ein Benutzer mit Administratorrechten auf dem Computer für die Dateifreigabe entscheidet. Um sich für die Dateifreigabe zu entscheiden, braucht der Administrator nichts weiter zu tun, als eine Datei aus seinem Profil freizugeben.
- Ist die Einstellung *Aktiviert*, können Benutzer keine Dateien aus ihren Profilen mit dem Dateifreigabe-Assistenten freigeben und der Dateifreigabe-Assistent erstellt keine Freigaben im Ordner %SystemDrive%\Users.
- Ist diese Einstellung *Deaktiviert*, was erforderlich sein kann, um eine geerbte *Aktiviert*-Einstellung außer Kraft zu setzen, können Benutzer Dateien aus ihrem Profil für andere Benutzer aus dem Netzwerk freigeben, sofern sich ein Benutzer mit Administratorrechten auf dem Computer für die Dateifreigabe entscheidet.
- Um die Gruppenrichtlinie *Verhindert, dass Benutzer Dateien innerhalb ihres Profils freigeben* zu konfigurieren, gehen Sie folgendermaßen vor:
 1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Erweitern Sie den Zweig *Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Netzwerkfreigabe*.
 2. Tippen oder klicken Sie doppelt auf *Verhindert, dass Benutzer Dateien innerhalb ihres Profils freigeben*.
 3. Wählen Sie *Nicht konfiguriert*, *Aktiviert* oder *Deaktiviert* aus und tippen oder klicken Sie auf *OK*.

Die Versuchung ist zwar groß, eine Freigabe des öffentlichen Ordners zu verwenden, aber die meisten Organisationen, auch kleine Firmen, sind wohl besser beraten, für alle Firmendateien und -daten die Standardordnerfreigabe zu verwenden. Sie ist einfach sicherer und bietet besseren Schutz. Statt die Datenschleusen zu öffnen, schließt sie die Türen und blockiert unerwünschte Zugriffe. Ein möglichst guter Schutz für einen der wichtigsten Werte einer Organisation, ihre Daten, ist entscheidend.

Freigabeberechtigungen werden nur verwendet, wenn ein Benutzer versucht, von einem anderen Computer des Netzwerks aus auf eine Datei oder einen Ordner zuzugreifen. Zugriffsberechtigungen wirken dagegen immer, ob der Benutzer nun lokal angemeldet ist oder über das Netzwerk einen Remotezugriff auf die Datei oder den Ordner durchführt. Beim Remotezugriff werden zuerst die Freigabeberechtigungen angewendet und dann die Zugriffsberechtigungen.

In gewisser Weise bedeutet dies, dass Dateizugriffsberechtigungen und Standardordnerfreigabeberechtigungen wie Schutzhüllen für Daten funktionieren. Dateizugriffsberechtigungen, die erste Hülle, schützen Ihre Daten bei lokalen Zugriffen. Wenn sich ein Benutzer lokal an einem Computer anmeldet, können ihm Dateizugriffsberechtigungen den Zugang zu Dateien und Ordnern erlauben oder verwehren. Dateifreigabeberechtigungen, die zweite Hülle, werden für Remotezugriffe verwendet. Versucht ein Benutzer einen Remotezugriff auf Daten, erlauben oder verwehren ihm Dateifreigabeberechtigungen den Zugriff. Da Ihre Daten aber zusätzlich noch von der ersten Schutzhülle geschützt werden, muss der Benutzer auch über die entsprechenden Dateizugriffsberechtigungen verfügen, um mit den Dateien und Ordnern arbeiten zu können.

Kontrollieren des Zugriffs auf Dateien und Ordner mit NTFS-Berechtigungen

NTFS-Berechtigungen werden bei jedem Dateizugriff berücksichtigt. Sie sind recht komplex. Um sie als Administrator richtig einstellen zu können, müssen Sie folgende Grundbegriffe verstehen:

- **Standardberechtigungen** Was sind Standardberechtigungen und wie werden sie verwendet?
- **Forderungsbasierte Berechtigungen** Was sind Forderungen (oder Ansprüche) von Benutzern und Geräten und wie werden sie verwendet?
- **Spezielle Berechtigungen** Was sind spezielle Berechtigungen und wie werden sie verwendet?
- **Besitz einer Datei** Was bedeutet Dateibesitz und wie wird er eingesetzt?
- **Vererbung** Was ist Vererbung und wie wirkt sie?
- **Effektive Berechtigungen** Wie werden die effektiven Berechtigungen von Dateien ermittelt?

Bedeutung und Verwendung der Standardberechtigungen

In Windows 8 hat der Besitzer einer Datei oder eines Ordners das Recht, anderen den Zugriff auf diese Ressource zu gewähren oder zu verweigern, wie es auch Mitglieder der Gruppe *Administratoren* und andere autorisierte Benutzer tun. Mit der Einstellung *Zulassen* gewähren Sie einem Benutzer oder einer Gruppe diese Berechtigung. Mit der Einstellung *Verweigern* entziehen Sie einem Benutzer oder einer Gruppe die Berechtigung. Denken Sie daran, dass Einträge, die Berechtigungen verweigern, Vorrang vor Einträgen haben, die Berechtigungen zulassen. Ist ein Benutzer also Mitglied von zwei Gruppen, wobei der einen Gruppe eine Berechtigung gewährt und der anderen dieselbe Berechtigung verweigert wird, wird dem Benutzer diese Berechtigung verweigert.

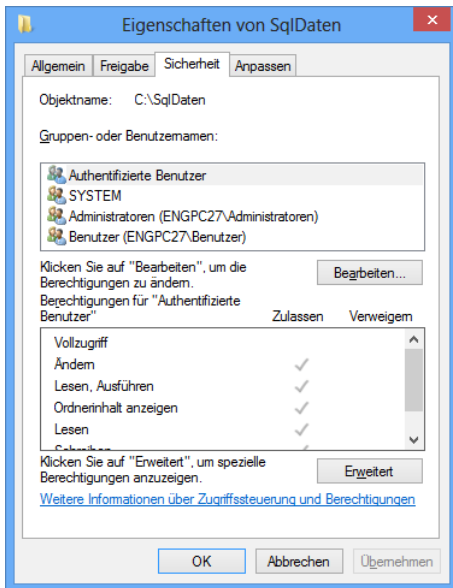


Abbildung 13.1 Die Registerkarte *Sicherheit* zeigt die zugewiesenen Standardberechtigungen

Tabelle 13.1 Standardberechtigungen für Dateien und Ordner

Berechtigung	Beschreibung
<i>Vollzugriff</i>	Gewährt dem Benutzer oder der Gruppe die volle Kontrolle über die gewählte Datei oder den Ordner und erlaubt das Lesen, Schreiben, Ändern und Löschen von Dateien und untergeordneten Ordnern. Ein Benutzer mit <i>Vollzugriff</i> -Berechtigung auf eine Datei oder einen Ordner kann Berechtigungen ändern, Dateien unabhängig von den für die Dateien vergebenen Berechtigungen aus dem Ordner löschen und eine Datei oder einen untergeordneten Ordner auch in Besitz nehmen. Durch die Vergabe dieser Berechtigung sind auch alle anderen Berechtigungen eingeschlossen.
<i>Ändern</i>	Erlaubt dem Benutzer oder der Gruppe, Dateien zu lesen, zu schreiben, zu ändern und zu löschen. Ein Benutzer mit der Berechtigung <i>Ändern</i> kann auch Dateien und untergeordnete Ordner erstellen, aber keine Dateien in Besitz nehmen. Die Vergabe dieser Berechtigungen schließt alle darin enthaltenen Berechtigungen ein.
<i>Lesen und Ausführen</i>	Erlaubt die Anzeige und Auflistung von Dateien und untergeordneten Ordnern sowie die Ausführung von Dateien. Wird diese Berechtigung für einen Ordner vergeben, erben alle darin enthaltenen Dateien und untergeordneten Ordner diese Einstellung. Die Vergabe dieser Berechtigung schließt auch die Berechtigungen <i>Ordnerinhalt anzeigen</i> und <i>Lesen</i> ein.
<i>Ordnerinhalt anzeigen</i> (nur für Ordner)	Ähnelt der Berechtigung <i>Lesen und Ausführen</i> , kann aber nur für Ordner vergeben werden. Ermöglicht die Anzeige und Auflistung von Dateien und untergeordneten Ordnern sowie die Ausführung von Dateien. Im Gegensatz zu <i>Lesen und Ausführen</i> wird diese Einstellung aber nur von untergeordneten Ordnern geerbt, also nicht von Dateien, die im betreffenden Ordner oder untergeordneten Ordner liegen.
<i>Lesen</i>	Erlaubt dem Benutzer oder der Gruppe die Anzeige und Auflistung des Inhalts eines Ordners. Ein Benutzer mit dieser Berechtigung kann Dateiattribute anzeigen, Berechtigungen lesen und Dateien synchronisieren. <i>Lesen</i> ist die einzige Berechtigung, die zur Ausführung von Skripts erforderlich ist. Lesezugriff ist für den Zugriff auf eine Verknüpfung und die von ihr bezeichnete Datei erforderlich.
<i>Schreiben</i>	Erlaubt einem Benutzer oder einer Gruppe die Erstellung neuer Dateien und das Schreiben von Daten in vorhandene Dateien. Ein Benutzer mit dieser Berechtigung kann auch Dateiattribute anzeigen, Berechtigungen lesen und Dateien synchronisieren. Gibt man einem Benutzer die Berechtigung <i>Schreiben</i> , aber nicht das Recht, eine Datei oder einen Ordner zu löschen, wird er dadurch nicht daran gehindert, den Inhalt des Ordners oder der Datei zu löschen.

Im Datei-Explorer können Sie sich die aktuell vergebenen Standardberechtigungen ansehen, indem Sie eine Datei oder einen Ordner mit der rechten Maustaste anklicken oder die Datei oder den Ordner gedrückt halten, im Kontextmenü *Eigenschaften* wählen und dann im *Eigenschaften*-Dialogfeld die Registerkarte *Sicherheit* anklicken.

Wie aus Abbildung 13.1 hervorgeht, zeigt die Liste *Gruppen- oder Benutzernamen* alle Benutzer und Gruppen, die über Zugriffsberechtigungen für die ausgewählte Ressource verfügen. Wenn Sie einen Benutzer oder eine Gruppe auswählen, zeigt die Liste *Berechtigungen für* die zugewiesenen Berechtigungen. Wird das Häkchen hinter einer Berechtigung abgeblendet dargestellt, bedeutet dies, dass die Berechtigung von einem übergeordneten Ordner geerbt wurde. Vererbung wird ausführlicher im Abschnitt »Vererben von Berechtigungen« weiter unten in diesem Kapitel besprochen.

Verwenden und Vergeben von Standardberechtigungen

Alle Berechtigungen werden im Dateisystem in der Zugriffssteuerungsliste (Access Control List, ACL) eines Ordners oder einer Datei gespeichert. Tabelle 13.1 beschreibt sechs Standardberechtigungen für Ordner, von denen fünf auch für Dateien verwendet werden. Manche Berechtigungen werden zwar von übergeordneten Ordnern geerbt, aber alle Berechtigungen werden auf einer bestimmten Stufe der Dateisystemhierarchie explizit definiert. Die Berechtigungen werden in dieser Liste in etwa in der Reihenfolge ihres Wirkungsbereichs aufgeführt, von *Vollzugriff* mit den meisten Berechtigungen bis hin zu *Lesen* und *Schreiben*, die spezielle Berechtigungen festlegen.

Genauso wichtig wie die Standardberechtigungen sind die Benutzer und Gruppen, denen Sie diese Berechtigungen zuweisen. Wenn ein Benutzer oder eine Gruppe, denen Sie Berechtigungen zuweisen möchten, bereits in der Liste *Gruppen- oder Benutzernamen* der Registerkarte *Sicherheit* verzeichnet ist, können Sie die zugewiesenen Berechtigungen ändern, indem Sie auf *Bearbeiten* tippen oder klicken und dann die gewünschten Einstellungen in den Spalten *Zulassen* und *Verweigern* der Liste *Berechtigungen für* vornehmen. Wählen Sie die Kontrollkästchen in der Spalte *Zulassen*, um Berechtigungen zu vergeben, oder löschen Sie die Kontrollkästchen, um Berechtigungen aufzuheben. Tippen oder klicken Sie zuletzt auf *OK*.

Um einem Benutzer oder einer Gruppe eine bestimmte Berechtigung ausdrücklich zu entziehen, wählen Sie das entsprechende Kontrollkästchen in der Spalte *Verweigern*. Da verweigernde Berechtigungen Vorrang vor anderen Berechtigungen haben, ist *Verweigern* in zwei bestimmten Szenarios sehr nützlich:

- Wenn ein Benutzer Mitglied einer Gruppe ist, die bestimmte Berechtigungen erhalten hat, aber dieser spezielle Benutzer nicht über die Berechtigung verfügen soll und Sie den Benutzer nicht aus der entsprechenden Gruppe entfernen können oder wollen, können Sie die ererbten Berechtigungen außer Kraft setzen, indem Sie dem speziellen Benutzer die Berechtigung verweigern.
- Wenn von einem übergeordneten Ordner eine bestimmte Berechtigung geerbt wird und ein Benutzer oder eine Gruppe nicht über diese Berechtigung verfügen soll, können Sie die vergebenen Berechtigungen (in den meisten Fällen) außer Kraft setzen, indem Sie dem Benutzer oder der Gruppe explizit die betreffende Berechtigung verweigern.

Wenn Benutzer oder Gruppen, denen Sie Berechtigungen zuweisen möchten, noch nicht auf der Registerkarte *Sicherheit* in der Liste *Gruppen- oder Benutzernamen* stehen, können Sie sie sehr einfach hinzufügen. Um Benutzern oder Gruppen, die noch nicht auf der Registerkarte *Sicherheit* einer Datei oder eines Ordners erfasst sind, Standardberechtigungen zuzuweisen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie auf der Registerkarte *Sicherheit* auf *Bearbeiten*. Dadurch öffnet sich das Dialogfeld *Berechtigungen für*.
2. Tippen oder klicken Sie im Dialogfeld *Berechtigungen für* auf *Hinzufügen*, um das Dialogfeld *Benutzer, Computer, Dienstkonto oder Gruppe auswählen* zu öffnen (Abbildung 13.2).

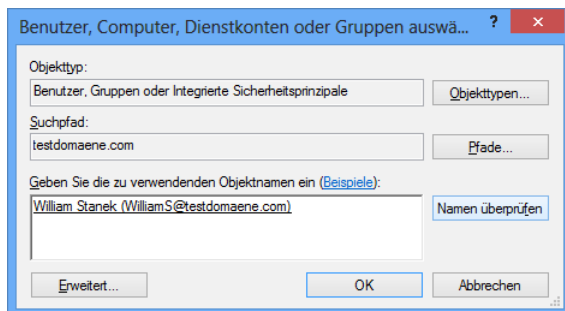


Abbildung 13.2 Verwenden Sie das Dialogfeld *Benutzer, Computer, Dienstkonto oder Gruppe auswählen* für die Auswahl der Benutzer oder Gruppen, denen Sie Berechtigungen zuweisen möchten

HINWEIS In einer Arbeitsgruppe heißt dieses Dialogfeld *Benutzer oder Gruppen auswählen*. Beide Dialogfelder haben denselben Zweck.

TIPP Überprüfen Sie auf jeden Fall den Wert im Feld *Suchpfad*. In Arbeitsgruppen zeigen Computer nur lokale Konten und Gruppen an. In Domänen lassen sich andere Werte für dieses Feld einstellen. Der Anfangswert ist die Standarddomäne (die Anmeldedomäne) des aktuell angemeldeten Benutzers. Wenn Sie nicht dort nach Benutzer- und Gruppenkonten suchen möchten, tippen oder klicken Sie auf *Pfade*, um eine Liste der Orte anzuzeigen, die Sie durchsuchen können. Darin sind die aktuelle Domäne, vertrauenswürdige Domänen und andere Orte verzeichnet, auf die Sie Zugriff haben.

3. Geben Sie den Namen eines Benutzer- oder Gruppenkontos ein. Achten Sie darauf, dass Sie den Kontonamen eingeben und nicht den Anzeigenamen des Benutzers. Sie können mehrere Namen angeben, wobei die Namen jeweils durch ein Semikolon voneinander getrennt sind.
4. Tippen oder klicken Sie auf *Namen überprüfen*. Wird für jeden Eintrag nur eine Übereinstimmung gefunden, dann wird das Dialogfeld automatisch entsprechend aktualisiert und jeder Eintrag ist unterstrichen. Andernfalls sehen Sie ein weiteres Dialogfeld. Wird keine Übereinstimmung gefunden, haben Sie den Namen falsch eingegeben oder Sie suchen am falschen Ort. Ändern Sie den Namen im Dialogfeld *Name nicht gefunden* und versuchen Sie es noch einmal. Oder Sie tippen oder klicken *Pfade* an und stellen einen anderen Suchpfad ein. Wurden mehrere Übereinstimmungen gefunden, wählen Sie im Dialogfeld *Mehrere Namen gefunden* den oder die gewünschten Namen und tippen oder klicken auf *OK*. Die Benutzer und Gruppen werden in die Liste *Gruppen- oder Benutzernamen* aufgenommen.
5. Nun können Sie die Berechtigungen für jeden Benutzer und jede Gruppe einstellen, die Sie hinzugefügt haben, indem Sie den Kontonamen wählen und dann die Zugriffsberechtigungen nach Bedarf gewähren oder verweigern.

Tabelle 13.2 Bei der Zuweisung von Berechtigungen werden auch Spezialidentitäten eingesetzt

Spezialidentität	Beschreibung
<i>ANONYMOUS-ANMELDUNG</i>	Umfasst alle Netzwerkanmeldungen, bei denen keine Anmeldeinformationen angegeben werden. Diese Spezialidentität wird für anonyme Zugriffe auf Ressourcen verwendet, wie sie beispielsweise auf einem Webserver geboten werden.
<i>Authentifizierte Benutzer</i>	Umfasst Benutzer und Computer, die sich mit Benutzernamen und Kennwort angemeldet haben. Enthält keine Benutzer, die sich mit dem Gastkonto angemeldet haben. Das gilt auch dann, wenn dem Gastkonto ein Kennwort zugewiesen wurde.
<i>Benutzer</i>	Umfasst nur authentifizierte Benutzer und Domänenbenutzer. Die vordefinierte Gruppe <i>Benutzer</i> wird gegenüber <i>Jeder</i> bevorzugt.
<i>DIALUP</i>	Umfasst alle Benutzer, die über eine Wählverbindung auf den Computer zugreifen. Diese Identität dient dazu, per Wählverbindung verbundene Benutzer von allen anderen Benutzerarten zu unterscheiden.
<i>ERSTELLER-BESITZER</i>	Die Spezialidentität für das Konto, das eine Datei oder einen Ordner erstellt hat. Windows 8 verwendet diese Gruppe, um das Konto zu identifizieren, das die ultimative Autorität über die Datei oder einen Ordner hat.
<i>INTERAKTIV</i>	Umfasst alle Benutzer, die lokal oder über eine Remotedesktopverbindung angemeldet sind.
<i>Jeder</i>	Umfasst alle interaktiven Benutzer, Benutzer mit Wählverbindungen und authentifizierte Benutzer. Auch Gäste gehören zu dieser Gruppe, nicht aber anonyme Benutzer.
<i>NETZWERK</i>	Umfasst alle Benutzer, die via Netzwerk angemeldet sind. Diese Identität erlaubt Remotebenutzern den Zugriff auf eine Ressource, umfasst aber nicht interaktive Anmeldungen, die über Remotedesktopverbindungen erfolgen.

Spezialidentitäten und empfohlene Vorgehensweisen für die Zuweisung von Berechtigungen

Wenn Sie mit Standardberechtigungen arbeiten, ist es nicht nur wichtig zu wissen, wie Berechtigungen verwendet werden, sondern auch, wie man die Zuweisung von Berechtigungen durch Spezialidentitäten vereinfachen kann. Von diesen Spezialidentitäten werden *Ersteller-Besitzer* und *Benutzer* am häufigsten verwendet. Aber auch die anderen werden gelegentlich verwendet (Tabelle 13.2). Spezialidentitäten sind automatisch Mitglieder bestimmter Gruppen. Sie konfigurieren die Berechtigungen für eine Spezialidentität, indem Sie den Namen der Spezialidentität genauso eingeben wie den Namen eines beliebigen anderen Benutzers oder einer Gruppe.

Eine gründliche Beschäftigung mit diesen Spezialidentitäten kann Ihnen helfen, die Berechtigungen für NTFS-Volumes effizienter zu vergeben. Außerdem können Sie sich an folgenden Richtlinien orientieren, wenn Sie Berechtigungen einstellen:

- **Beachten Sie die Dateisystemhierarchie** Vererbung spielt bei der Vergabe von Berechtigungen eine große Rolle. Standardmäßig gelten die Berechtigungen, die Sie für einen Ordner vergeben, auch für alle Dateien und Unterordner, die in diesem Ordner enthalten sind. Vor diesem Hintergrund beginnen Sie die Einstellung der Berechtigungen am besten im Stammordner eines lokalen Datenträgers oder des Benutzerprofils (beide dienen als Stammordner, bilden also die oberste Ebene in der Ordnerhierarchie).
- **Arbeiten Sie nach Plan** Stellen Sie keine Berechtigungen ein, ohne zuvor einen klaren Plan ausgearbeitet zu haben. Wenn die Berechtigungen in den verschiedenen Ordnersebenen aus dem Tritt geraten und Sie eine Möglichkeit suchen, alles wieder ins Lot zu bringen, damit es eine gewisse Kontinuität gibt, dann können Sie die Berechtigungen im übergeordneten Ordner so einstellen, wie sie sein sollen, und dann die Berechtigungen aller in diesem Ordner enthaltenen Dateien und Unterordner mit den Verfahren zurücksetzen, die im Abschnitt »Wiederherstellen geerbter Berechtigungen« weiter unten in diesem Kapitel beschrieben werden.
- **Gewähren Sie nur die wirklich benötigten Berechtigungen** Ein wichtiger Aspekt der Dateizugriffssteuerung in NTFS ist, dass Berechtigungen explizit zugewiesen werden müssen. Wenn Sie einem Benutzer eine bestimmte Berechtigung nicht geben und der Benutzer kein Mitglied einer Gruppe ist, die über diese Berechtigung verfügt, dann hat der Benutzer diese Berechtigung nicht. So einfach ist das. Bei der Vergabe von Berechtigungen ist diese Regel besonders wichtig, weil die Versuchung groß ist, Benutzern einfach den Vollzugriff zu geben, statt genau die benötigten Berechtigungen festzulegen. Das *Prinzip der geringstmöglichen Rechte* bedeutet, Benutzern genau die Berechtigungen zu geben, die sie zur Erledigung ihrer Arbeit brauchen.
- **Verwenden Sie Gruppen zur Vereinfachung der Verwaltung** Wann immer möglich, sollten Sie Benutzer zu Mitgliedern der passenden Gruppen machen und dann die Berechtigungen dieser Gruppen festlegen, statt Berechtigungen an einzelne Benutzer zu vergeben. Dann können Sie neuen Benutzern nämlich einen maßgeschneiderten Berechtigungssatz zuweisen, indem Sie die neuen Benutzer zu Mitgliedern der entsprechenden Gruppen machen. Wird ein Benutzer versetzt und gehört dann zu einer anderen Gruppe, ändern Sie einfach die Gruppenmitgliedschaft entsprechend. Tritt Sarah beispielsweise ins Verkaufsteam ein, können Sie sie in die Gruppen *SalesUS* und *SalesCan* aufnehmen, damit sie Zugang zu den entsprechenden Daten erhält. Sollte sie das Verkaufsteam später verlassen und ins Marketingteam wechseln, können Sie ihre Mitgliedschaft in den Gruppen *SalesUS* und *SalesCan* löschen und sie in die Gruppen *MarketingUS* und *MarketingCan* aufnehmen. Das ist wesentlich einfacher, als die Berechtigungen für jeden Ordner zu überarbeiten, auf den Sarah Zugriff erhalten soll.

- **Verwenden Sie zentrale Zugangsrichtlinien** Verwenden Sie auf Ihren Domänencontrollern zentrale Zugriffsrichtlinien, um die Berechtigungen, die Benutzer oder Geräte für den Zugriff auf Ressourcen brauchen, genau festzulegen.

Zuweisen von speziellen Berechtigungen

Windows 8 verwendet spezielle Berechtigungen, um die Berechtigungen von Benutzern und Gruppen genau einzustellen. Wenn Sie mit Standardberechtigungen arbeiten, übersetzt Windows 8 diese Angaben in spezielle Berechtigungen, mit denen die zugelassenen Aktionen genau festgelegt werden. Die Standardberechtigungen setzen sich aus folgenden speziellen Berechtigungen zusammen:

- *Lesen*
 - ☐ *Ordner auflisten / Daten lesen*
 - ☐ *Attribute lesen*
 - ☐ *Erweiterte Attribute lesen*
 - ☐ *Berechtigungen lesen*
- *Lesen und Ausführen oder Ordnerinhalt anzeigen*
 - ☐ Alle speziellen Berechtigungen, die bereits für *Lesen* genannt wurden
 - ☐ *Ordner durchsuchen / Datei ausführen*
- *Schreiben*
 - ☐ *Dateien erstellen / Daten schreiben*
 - ☐ *Ordner erstellen / Daten anhängen*
 - ☐ *Attribute schreiben*
 - ☐ *Erweiterte Attribute schreiben*
- *Ändern*
 - ☐ Alle speziellen Berechtigungen, die bereits für *Lesen* genannt wurden
 - ☐ Alle speziellen Berechtigungen, die bereits für *Schreiben* genannt wurden
 - ☐ *Löschen*
- *Vollzugriff*
 - ☐ Alle bisher aufgeführten speziellen Berechtigungen
 - ☐ *Unterordner und Dateien löschen*
 - ☐ *Berechtigungen ändern*
 - ☐ *Besitz übernehmen*

Tabelle 13.3 beschreibt, was die speziellen Berechtigungen in Windows 8 bedeuten.

Im Datei-Explorer können Sie sich die speziellen Berechtigungen ansehen, die für eine Datei oder einen Ordner vergeben wurden, indem Sie die Datei oder den Ordner mit der rechten Maustaste anklicken oder gedrückt halten, und dann *Eigenschaften* wählen. Im *Eigenschaften*-Dialogfeld wählen Sie die Registerkarte *Sicherheit* und tippen oder klicken dann auf *Erweitert*, um das Dialogfeld *Erweiterte Sicherheitseinstellungen* zu öffnen (Abbildung 13.3). In diesem Dialogfeld werden die Berechtigungen fast so wie auf der Registerkarte *Sicherheit* angezeigt. Der entscheidende Unterschied ist, dass die einzelnen gewährten oder verweigerten Berechtigungen angezeigt werden, und auch, ob und woher die Berechtigungen geerbt wurden und für welche Ressourcen sie gelten.

Tabelle 13.3 Spezielle Berechtigungen für Dateien und Ordner

Spezielle Berechtigung	Beschreibung
<i>Ordner durchsuchen / Datei ausführen</i>	<i>Ordner durchsuchen</i> ermöglicht den direkten Zugang zu einem Ordner, um Unterordner zu erreichen, selbst wenn keine explizite Berechtigung zum Lesen der Daten vorliegt, die er enthält. <i>Datei ausführen</i> erlaubt die Ausführung einer ausführbaren Datei.
<i>Ordner auflisten / Daten lesen</i>	<i>Ordner auflisten</i> ermöglicht die Anzeige von Datei- und Ordnernamen. <i>Daten lesen</i> ermöglicht die Anzeige von Dateiinhalten.
<i>Attribute lesen</i>	Erlaubt das Lesen der Standardattribute einer Datei oder eines Ordners. Zu diesen Attributen gehören <i>Schreibgeschützt</i> , <i>Verborgен</i> , <i>System</i> und <i>Archiv</i> .
<i>Erweiterte Attribute lesen</i>	Ermöglicht die Anzeige von erweiterten Attributen (benannte Datenströme), die zu einer Datei gehören.
<i>Dateien erstellen / Daten schreiben</i>	<i>Dateien erstellen</i> erlaubt es, neue Dateien in einem Ordner abzulegen. <i>Daten schreiben</i> erlaubt es, in einer Datei vorhandene Daten zu überschreiben (aber nicht, neue Daten an eine Datei anzuhängen, dafür ist <i>Daten anhängen</i> erforderlich).
<i>Ordner erstellen / Daten anhängen</i>	<i>Ordner erstellen</i> erlaubt das Erstellen von Unterordnern in Ordnern. <i>Daten anhängen</i> erlaubt das Anhängen von Daten ans Ende einer vorhandenen Datei (aber nicht das Überschreiben von vorhandenen Daten, dafür ist <i>Daten schreiben</i> erforderlich).
<i>Attribute schreiben</i>	Erlaubt Ihnen die Änderung der Standardattribute einer Datei oder eines Ordners. Zu diesen Attributen gehören <i>Schreibgeschützt</i> , <i>Verborgен</i> , <i>System</i> und <i>Archiv</i> .
<i>Erweiterte Attribute schreiben</i>	Erlaubt Ihnen die Änderung von erweiterten Attributen (benannte Datenströme), die zu einer Datei gehören.
<i>Unterordner und Dateien löschen</i>	Erlaubt Ihnen, den Inhalt eines Ordners zu löschen. Wenn Sie über diese Berechtigung verfügen, können Sie Unterordner und die Dateien in einem Ordner selbst dann löschen, wenn Sie für den Unterordner oder die Datei nicht über die Berechtigung <i>Löschen</i> verfügen.
<i>Löschen</i>	Erlaubt Ihnen, eine Datei oder einen Ordner zu löschen. Ist der Ordner nicht leer und verfügen Sie für eine seiner Dateien oder Unterordner nicht über die Berechtigung <i>Löschen</i> , können Sie den Ordner nur löschen, wenn Sie über die Berechtigung <i>Unterordner und Dateien löschen</i> verfügen.
<i>Berechtigungen lesen</i>	Erlaubt Ihnen das Lesen der Standardberechtigungen und der speziellen Berechtigungen, die mit einer Datei oder einem Ordner verknüpft sind.
<i>Berechtigungen ändern</i>	Erlaubt Ihnen die Änderung der Standardberechtigungen und der speziellen Berechtigungen, die mit einer Datei oder einem Ordner verknüpft sind.
<i>Besitz übernehmen</i>	Erlaubt Ihnen, eine Datei oder einen Ordner in Besitz zu nehmen. Standardmäßig können Administratoren immer Besitz von einer Datei oder einem Ordner ergreifen und dieses Recht auch anderen gewähren.

WEITERE INFORMATIONEN

Abbildung 13.3 zeigt statt eines Benutzernamens die GUID des Besitzers an. Unter Windows 8 deutet dies gewöhnlich darauf hin, dass der Ordner oder die Datei von jemandem erstellt wurde, der auf dem Computer ein anderes Betriebssystem verwendet hat, beispielsweise in einer Dual-Boot-Konfiguration.

Im Dialogfeld *Erweiterte Sicherheitseinstellungen* können Sie auf folgende Weise spezielle Berechtigungen für einen Sicherheitsprinzipal festlegen:

1. Wenn der Benutzer bereits über Berechtigungen für die Datei oder den Ordner verfügt, können Sie die speziellen Berechtigungen anzeigen oder ändern, indem Sie *Anzeigen* oder *Berechtigungen ändern* antippen oder anklicken. Überspringen Sie die Schritte 2 bis 5.

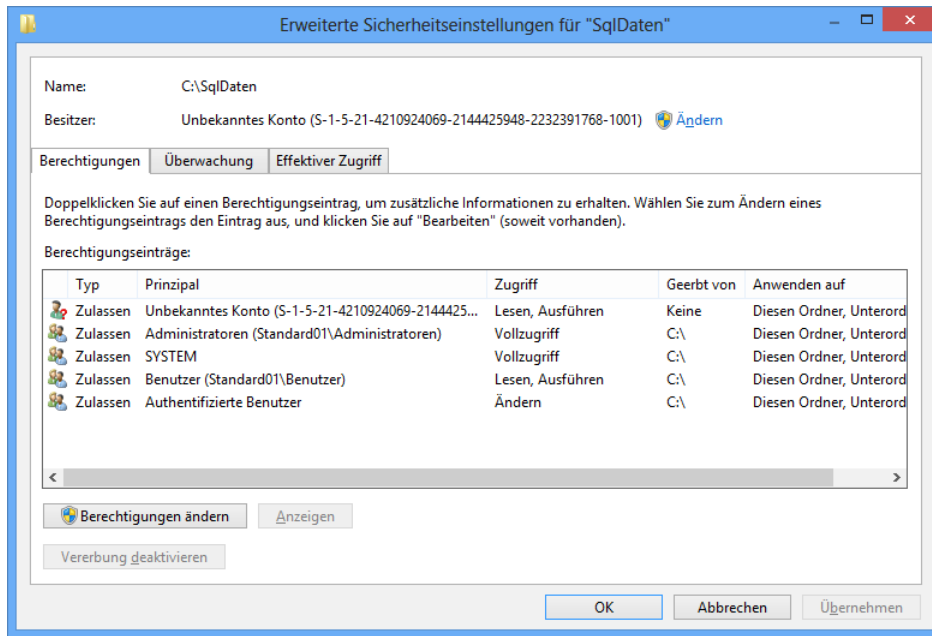


Abbildung 13.3 Verwenden Sie das Dialogfeld *Erweiterte Sicherheitseinstellungen* zur Einstellung spezieller Berechtigungen

- Tippen oder klicken Sie auf *Hinzufügen*, um das Dialogfeld *Berechtigungseintrag für* anzuzeigen. Tippen oder klicken auf *Prinzipal auswählen*, um das Dialogfeld *Benutzer, Computer, Dienstkonto oder Gruppe auswählen* zu öffnen.
- Geben Sie den Namen eines Benutzer- oder Gruppenkontos ein. Achten Sie darauf, dass Sie den Kontonamen angeben und nicht den Anzeigenamen. An dieser Stelle darf immer nur ein einzelner Name eingegeben werden.
- Tippen oder klicken Sie auf *Namen überprüfen*. Liegt für den Eintrag nur eine einzige Übereinstimmung vor, wird das Dialogfeld automatisch aktualisiert und der Eintrag wird unterstrichen. Andernfalls erscheint ein weiteres Dialogfeld. Sind keine Übereinstimmungen vorhanden, haben Sie vermutlich den Namen falsch eingegeben oder Sie suchen an der falschen Stelle. Ändern Sie den Namen und versuchen Sie es noch einmal. Oder tippen oder klicken Sie auf *Pfade*, um einen anderen Ort auszuwählen. Werden mehrere Übereinstimmungen gefunden, wählen Sie im Dialogfeld *Mehrere Namen gefunden* den gewünschten Namen aus und tippen oder klicken auf *OK*.
- Tippen oder klicken Sie auf *OK*. Der Benutzer oder die Gruppe wird als Prinzipal hinzugefügt und das Dialogfeld *Berechtigungseintrag für* wird aktualisiert.
- Standardmäßig werden nur die Grundberechtigungen angezeigt. Tippen oder klicken Sie auf *Erweiterte Berechtigungen anzeigen*, um die speziellen Berechtigungen anzuzeigen (Abbildung 13.4).
- Stellen Sie in der Liste *Typ* ein, ob Sie gewährte oder verweigerte spezielle Berechtigungen festlegen. Wählen Sie dann die Berechtigungen aus, die gewährt oder verweigert werden sollen. Wenn Berechtigungen abgeblendet dargestellt und unzugänglich sind, wurden sie vom übergeordneten Ordner geerbt.

HINWEIS Spezielle Berechtigungen werden separat gewährt oder verweigert. Wenn Sie also bestimmte Berechtigungen gewähren und andere verweigern möchten, konfigurieren Sie erst die gewährten Berechtigungen und in einem zweiten Durchgang, der wieder bei Schritt 1 beginnt, die verweigerten.

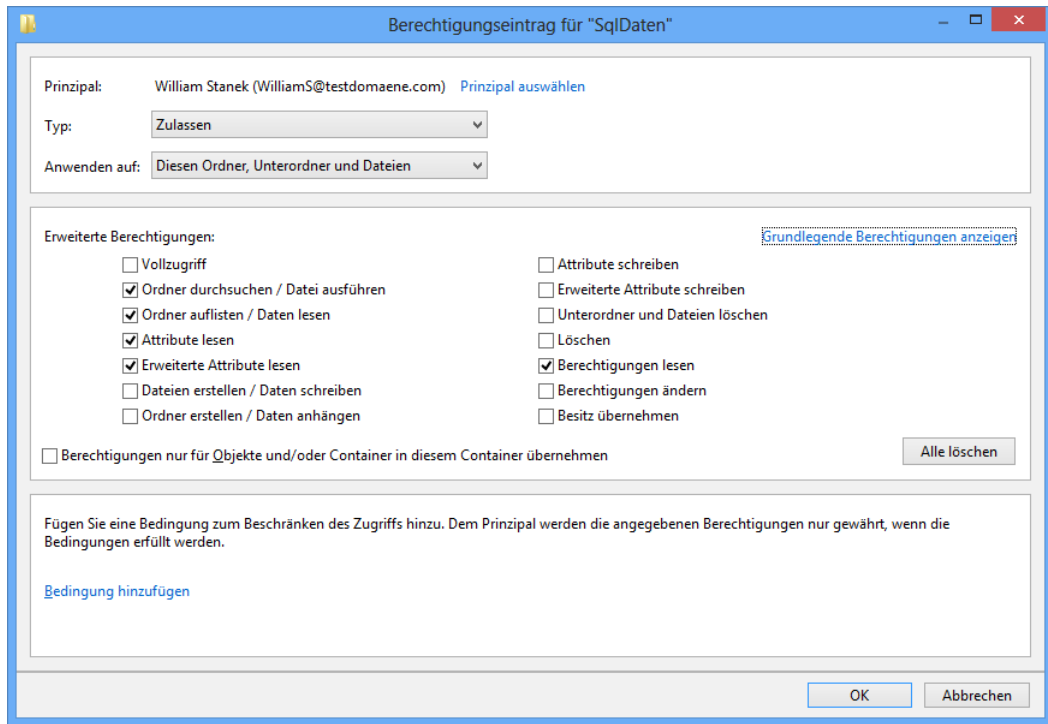


Abbildung 13.4 Stellen Sie die speziellen Berechtigungen ein, die gewährt oder verweigert werden sollen

8. Wenn die Optionen der Liste *Anwenden auf* zugänglich sind, stellen Sie die Vererbung der Berechtigungen nach Bedarf ein. Es sind folgende Optionen verfügbar:
 - **Nur diesen Ordner** Die Berechtigungen gelten nur für den aktuell ausgewählten Ordner.
 - **Diesen Ordner, Unterordner und Dateien** Die Berechtigungen gelten für den ausgewählten Ordner, seine Unterordner und alle Dateien in diesen Ordnern.
 - **Diesen Ordner, Unterordner** Die Berechtigungen gelten nur für den ausgewählten Ordner und seine Unterordner. Sie gelten nicht für Dateien in diesen Ordnern.
 - **Diesen Ordner, Dateien** Die Berechtigungen gelten für den gewählten Ordner und die Dateien, die in ihm liegen. Sie gelten nicht für Unterordner dieses Ordners.
 - **Nur Unterordner und Dateien** Die Berechtigungen gelten für die Unterordner des gewählten Ordners und für die Dateien, die in ihnen liegen. Sie gelten nicht für den gewählten Ordner.
 - **Nur Unterordner** Die Berechtigungen gelten für die Unterordner des gewählten Ordners, aber nicht für den gewählten Ordner oder für die Dateien in diesen Ordnern.
 - **Nur Dateien** Die Berechtigungen gelten für alle Dateien im gewählten Ordner und in seinen Unterordnern. Sie gelten nicht für den gewählten Ordner selbst oder für seine Unterordner.
9. Wenn Sie die Berechtigungen eingestellt haben, tippen oder klicken Sie auf **OK**.

Zuweisen von anspruchsbasierten Berechtigungen

Bei der forderungs- oder anspruchsbasierten Zugangssteuerung wird der Zugang zu Ressourcen mit Verbundidentitäten gesteuert. Die anspruchsbasierte Zugangssteuerung für den Remotezugriff auf Ressourcen und die zentralen Zugriffsrichtlinien setzen für die Authentifizierung von Ansprüchen den Kerberos-Schutz voraus. Der Kerberos-Schutz verbessert die Domänensicherheit, weil er eine Kommunikation der zur Domäne gehörenden Clients und Domänencontroller über sichere, verschlüsselte Kanäle ermöglicht.

Die einfachste Methode, einen Anspruch oder eine Forderung zu erstellen, besteht darin, die Bedingungen festzulegen, durch die der Zugriff beschränkt wird. Dabei ist es wichtig, zu welchen Gruppen ein Benutzer oder Gerät gehört und in welchen der Benutzer oder das Gerät kein Mitglied sein darf. Weiter entwickelte Lösungsansätze verwenden Zugangsregeln, Anspruchstypen und Ressourceneigenschaften, um bestimmte Kriterien, die erfüllt sein müssen, bevor der Zugang gewährt wird, genau festzulegen.

Anders gesagt, Ansprüche (oder Forderungen) legen genau fest, welche Eigenschaften Benutzer und Geräte für den Zugriff auf eine Datei oder einen Ordner haben müssen. Bei einem Anspruch auf der Basis der Gruppenmitgliedschaft können Sie zum Beispiel Folgendes festlegen:

- Ein Benutzer oder Gerät *kann* Mitglied einer beliebigen Gruppe sein, die in einem Anspruch aufgeführt wird. Das Gerät kann zum Beispiel Mitglied der Gruppe *Engineering Computers* sein.
- Ein Benutzer oder Gerät *muss* Mitglied jeder Gruppe sein, die in einem Anspruch aufgeführt wird. Das Gerät muss zum Beispiel Mitglied der Gruppen *Engineering Computers* und *Restricted Access* sein.
- Ein Benutzer oder Gerät *darf nicht* Mitglied einer der Gruppe sein, die in einem Anspruch aufgeführt werden. Das Gerät darf zum Beispiel nicht Mitglied der Gruppe *Temp Computers* sein.
- Ein Benutzer oder Gerät *darf nicht* Mitglied aller der Gruppen sein, die in einem Anspruch aufgeführt werden. Das Gerät darf zum Beispiel nicht Mitglied der Gruppen *Temp Computers* oder *Contract Computers* sein.

WEITERE INFORMATIONEN

Die zentralen Richtlinien für die Zugangssteuerung legen Sie in Active Directory fest. Diese Richtlinien werden dynamisch auf das gesamte Unternehmen angewandt. Die zentralen Zugriffsregeln verwenden bedingte Ausdrücke, für die Sie die Ressourceneigenschaften, Anspruchstypen und/oder Gruppenzugehörigkeit festlegen, ebenso die Server, auf denen die Richtlinie gelten soll.

Bevor Sie Bedingungen für den anspruchsbasierten Zugang zu den Dateien und Ordnern eines Computers definieren und anwenden können, muss die entsprechende Richtlinie aktiviert werden. Für Computer, die keiner Domäne angehören, aktivieren und konfigurieren Sie die Richtlinie *Unterstützung des Kerberos-Domänencontrollers für Ansprüche, Verbundauthentifizierung und Kerberos-Schutz* unter *System\KDC* in den administrativen Vorlagen der Computerkonfiguration. Die Richtlinie muss auf einen bestimmten Modus eingestellt werden. Folgende Modi sind verfügbar:

- **Unterstützt** Domänencontroller unterstützen Ansprüche, Verbundidentitäten und den Kerberos-Schutz. Clientcomputer, die keinen Kerberos-Schutz unterstützen, können authentifiziert werden.
- **Immer Ansprüche liefern** Wie *Unterstützt*, aber Domänencontroller geben immer Ansprüche für Konten zurück.
- **Ungeschützte Authentifizierungsanfragen ablehnen** Der Kerberos-Schutz ist erforderlich. Clientcomputer, die keinen Kerberos-Schutz unterstützen, können nicht authentifiziert werden.

Zur Anwendung in einer Domäne sollte die Richtlinie für die anspruchsbasierte Authentifizierung auf allen Domänencontrollern der Domäne aktiviert sein, um ein einheitliches Verhalten sicherzustellen. Deswegen aktiviert und konfiguriert man diese Richtlinie gewöhnlich im Gruppenrichtlinienobjekt des Standarddomänencontrollers (Default Domain Controller) oder im höchsten Gruppenrichtlinienobjekt, das mit der Organisationseinheit der Domänencontroller verknüpft ist.

Die Richtlinie *Unterstützung des Kerberos-Clients für Ansprüche, Verbundauthentifizierung und Kerberos-Schutz* kontrolliert, ob der Kerberos-Client unter Windows 8 oder Windows Server 2012 Ansprüche und Verbundauthentifizierung anfordert. Die Richtlinie muss für kompatible Kerberos-Clients aktiviert werden, damit Ansprüche und Verbundauthentifizierung für die dynamische Zugangssteuerung mit Kerberos-Schutz angefordert werden. Sie finden diese Richtlinie in den administrativen Vorlagen der Computerkonfiguration unter *System\Kerberos*.

Nachdem Sie diese Richtlinien aktiviert und konfiguriert haben, können Sie folgendermaßen die Bedingungen für Ansprüche festlegen:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf die gewünschte Datei oder den Ordner oder halten Sie das Objekt gedrückt, und wählen Sie *Eigenschaften*. Wählen Sie im Dialogfeld *Eigenschaften* die Registerkarte *Sicherheit* und tippen oder klicken Sie auf *Erweitert*, um das Dialogfeld *Erweiterte Sicherheitseinstellungen* zu öffnen (Abbildung 13.3).
2. Wenn der Benutzer oder die Gruppe bereits über Berechtigungen für die Datei oder den Ordner verfügt, können Sie die vorhandenen Berechtigungen bearbeiten. Wählen Sie den Benutzer aus, dessen Berechtigungen Sie bearbeiten möchten, tippen oder klicken Sie auf *Bearbeiten* und überspringen Sie die Schritte 3 bis 6.
3. Tippen oder klicken Sie auf *Hinzufügen*, um das Dialogfeld *Berechtigungseintrag für* zu öffnen. Tippen oder klicken Sie auf *Prinzipal auswählen*, um das Dialogfeld *Benutzer, Computer, Dienstkonto oder Gruppe auswählen* zu öffnen.
4. Geben Sie den Namen eines Benutzer- oder eines Gruppenkontos ein. Achten Sie darauf, dass Sie den Kontonamen eines Benutzers eingeben und nicht den Anzeigenamen des Benutzers. Es darf immer nur ein einziger Name eingegeben werden.
5. Tippen oder klicken Sie auf *Namen überprüfen*. Liegt für den Eintrag nur eine einzige Übereinstimmung vor, wird das Dialogfeld automatisch aktualisiert und der Eintrag wird unterstrichen. Andernfalls erscheint ein weiteres Dialogfeld. Sind keine Übereinstimmungen vorhanden, haben Sie vermutlich den Namen falsch eingegeben oder Sie suchen an der falschen Stelle. Ändern Sie den Namen und versuchen Sie es noch einmal. Oder tippen oder klicken Sie auf *Pfade*, um einen anderen Ort auszuwählen. Werden mehrere Übereinstimmungen gefunden, wählen Sie im Dialogfeld *Mehrere Namen gefunden* den gewünschten Namen aus und tippen oder klicken auf *OK*.
6. Tippen oder klicken Sie auf *OK*. Der Benutzer oder die Gruppe wird als Prinzipal hinzugefügt. Tippen oder klicken Sie auf *Bedingung hinzufügen*.
7. Verwenden Sie die verfügbaren Optionen, um die Bedingung oder die Bedingungen festzulegen, die erfüllt sein müssen, damit der Zugang gewährt wird. Für Benutzer und Gruppen legen Sie die Grundforderungen auf der Basis von Gruppenmitgliedschaften, zuvor definierten Anspruchstypen oder beidem fest. Bei Ressourceneigenschaften definieren Sie Bedingungen für Eigenschaftswerte.
8. Wenn Sie mit den Bedingungen fertig sind, tippen oder klicken Sie auf *OK*.

Dateibesitz und Berechtigungszuweisung

Der Besitzer einer Datei oder eines Ordners hat das Recht, den Zugriff auf diese Ressource zu gewähren oder zu verweigern. Mitglieder der Gruppe *Administratoren* und andere autorisierte Benutzer haben zwar ebenfalls das Recht, Zugriff zu gewähren oder zu verweigern, aber der Besitzer hat die Autorität, nicht mit Administrationsrechten ausgestattete Benutzer auszusperren. Der einzige Weg, wieder Zugang zu dieser Ressource zu erhalten, besteht darin, dass ein Administrator oder ein Sicherungsoperator die Ressource in Besitz nimmt. Daher ist es für die Berechtigungsvergabe bei einer Datei oder einem Ordner wichtig, wer der Besitzer ist.

Besitzer einer Datei oder eines Ordners ist die Person, die diese Ressource angelegt hat. Der Besitz kann auf mehreren verschiedenen Wegen ergriffen oder übertragen werden. Der aktuelle Besitzer einer Datei oder eines Ordners kann jederzeit den Besitz an einen anderen Benutzer oder eine andere Gruppe übertragen. Ein Mitglied der Administratorgruppe kann jederzeit Besitz von einer Datei oder einem Ordner ergreifen oder den Besitz an einen anderen Benutzer oder eine andere Gruppe übertragen, selbst wenn diese nach den aktuellen Berechtigungen keinen Zugriff auf die Ressource haben. Jeder Benutzer mit der Berechtigung *Besitz übernehmen* für die Datei oder den Ordner kann den Besitz übernehmen, wie auch jedes Mitglied der Gruppe der *Sicherungs-Operatoren* (oder jeder andere, der über das Benutzerrecht *Wiederherstellen von Dateien und Verzeichnissen* verfügt).

So weisen Sie den Besitz an einer Datei oder einem Ordner zu:

1. Öffnen Sie im Datei-Explorer das *Eigenschaften*-Dialogfeld der Datei oder des Ordners, indem Sie die Datei oder den Ordner mit der rechten Maustaste anklicken oder gedrückt halten, und *Eigenschaften* wählen.
2. Tippen oder klicken Sie auf der Registerkarte *Sicherheit* auf *Erweitert*, um das Dialogfeld *Erweiterte Sicherheitseinstellungen* zu öffnen. Es zeigt im oberen Bereich den Besitzer an.

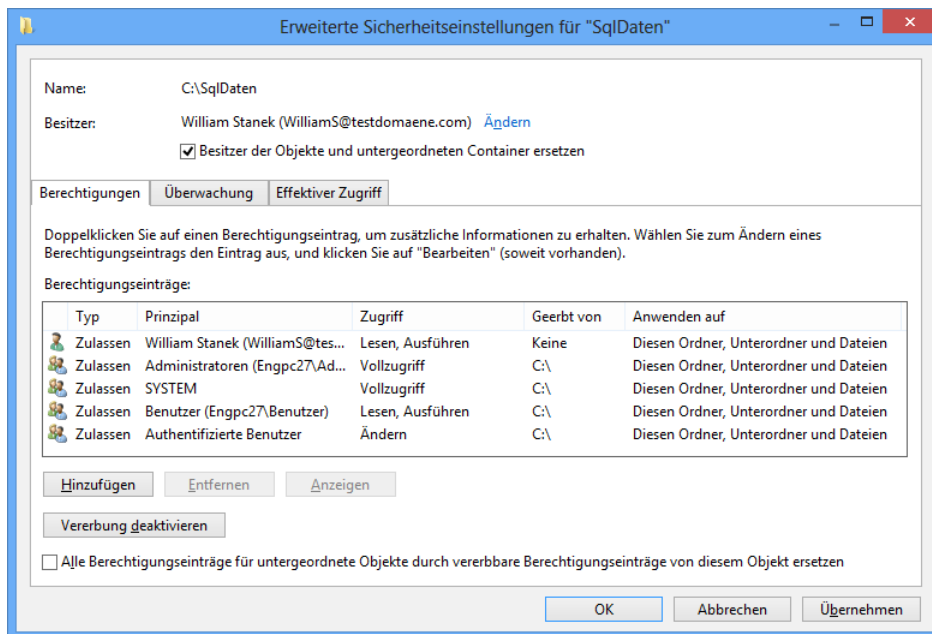


Abbildung 13.5 Im Dialogfeld *Erweiterte Sicherheitseinstellungen* können Sie eine Datei oder einen Ordner in Besitz nehmen

3. Tippen oder klicken Sie neben dem Namen des Besitzers auf *Ändern* und wählen Sie im Dialogfeld *Benutzer, Computer, Dienstkonto oder Gruppe auswählen* den neuen Besitzer aus. Wenn Sie einen Ordner in Besitz nehmen, können Sie auch alle seine Unterordner und die darin enthaltenen Dateien in Besitz nehmen, indem Sie die Option *Besitzer der Objekte und untergeordneten Container ersetzen* wählen (Abbildung 13.5).
4. Tippen oder klicken Sie auf die OK-Schaltflächen der beiden geöffneten Dialogfelder, wenn Sie fertig sind.

Vererben von Berechtigungen

In der Datei- und Ordnerhierarchie von Windows 8 sind der Stammordner eines lokalen Volumes und der Ordner *%UserProfile%* die Stammordner für alle Dateien und Ordner, die sie standardmäßig enthalten. Wenn Sie eine Ressource hinzufügen, erbt diese die Berechtigungen des Stammordners des lokalen Volumes oder des Benutzerprofilordners. Das können Sie ändern, indem Sie die Vererbungseinstellungen eines Ordners so anpassen, dass er nicht länger die Berechtigungen von seinem übergeordneten Ordner erbt. Dadurch entsteht in gewisser Weise ein neuer Stammordner, dessen Berechtigungen von allen Ordnern und Dateien geerbt werden, die Sie zu diesem Ordner hinzufügen.

Grundlagen der Vererbung

Die Vererbung erfolgt automatisch, und vererbte Berechtigungen werden bei der Erstellung einer Datei oder eines Ordners zugewiesen. Wenn Sie nicht wollen, dass eine Datei oder ein Ordner über dieselben Berechtigungen wie ihr übergeordneter Ordner verfügt, haben Sie mehrere Alternativen:

- Beenden Sie die Vererbung der Berechtigungen vom übergeordneten Ordner und wandeln Sie alle geerbten Berechtigungen in explizite Berechtigungen um oder löschen Sie alle geerbten Berechtigungen.
- Stellen Sie im neuen übergeordneten Ordner alle Berechtigungen ein, die seine Dateien und Unterordner haben sollen.
- Versuchen Sie nach Bedarf, ererbte Berechtigungen außer Kraft zu setzen, indem Sie das Gegenteil der Berechtigung festlegen. In den meisten Fällen hat *Verweigern* Vorrang vor *Zulassen*.

Geerbte Berechtigungen werden auf der Registerkarte *Sicherheit* des *Eigenschaften*-Dialogfelds einer Datei oder eines Ordners abgeblendet (unzugänglich) dargestellt. Wenn Sie einem Ordner neue Berechtigungen zuweisen, gelten diese Berechtigungen auch für die Dateien und Unterordner des Ordners und ergänzen oder ersetzen die vorhandenen Berechtigungen. Daher können Sie unabhängig vom übergeordneten Ordner zusätzlichen Benutzern oder Gruppen Zugriff auf die Ressourcen eines Ordners geben oder diesen Zugriff einschränken.

Zum besseren Verständnis der Vererbung folgende Beispiele:

- Auf Laufwerk C: erstellen Sie einen Ordner namens *Daten* und dann einen Unterordner namens *AktuelleProjekte*. Standardmäßig erbt *Daten* die Berechtigungen des Ordners C:\, und diese Berechtigungen werden wiederum vom Ordner *AktuelleProjekte* geerbt. Alle Dateien, die Sie zu den Ordnern C:\, C:\Daten und C:\Daten\AktuelleProjekte hinzufügen, haben dieselben Berechtigungen, nämlich die, die sie vom Ordner C:\ erben oder die für sie eingestellt wurden.
- Auf Laufwerk C: erstellen Sie einen Ordner namens *Dokumente* und dann einen Unterordner namens *Arbeit*. Sie deaktivieren die Vererbung für den Ordner *Arbeit* und entfernen dann die vom übergeordneten Ordner C:\ geerbten Berechtigungen. Alle Dateien, die Sie in den Ordner C:\Dokumente\Arbeit einfügen, erben die Berechtigungen des Ordners C:\Dokumente, sonst nichts.

- Auf Laufwerk C: erstellen Sie einen Ordner namens *Sicherung* und dann einen Unterordner namens *Verkauf*. Sie legen für den Ordner *Verkauf* Berechtigungen fest, die den Mitgliedern der Gruppe *Verkauf* Zugriff gewähren. Alle Dateien, die zum Ordner *C:\Sicherung\Verkauf* hinzugefügt werden, erben die Berechtigungen des Ordners *C:* und verfügen zusätzlich über die Zugriffsberechtigungen für Mitglieder der Gruppe *Verkauf*.

PRAXISTIPP

Viele neue Administratoren fragen sich, was der Vorteil der Vererbung sein soll und warum sie verwendet wird. Vererbung erweckt zwar gelegentlich den Anschein, mehr Probleme zu bereiten, als die Sache wert ist, aber das täuscht. Mit Vererbung können Sie sehr effizient Berechtigungen verwalten. Ohne Vererbung müssten Sie die Berechtigungen für jeden Ordner und jede Datei festlegen, die Sie erstellen. Wenn Sie die Berechtigungen später ändern wollen, müssen Sie wieder alle Ihre Ordner und Dateien bearbeiten. Mit Vererbung erben alle neuen Dateien und Ordner automatisch einen Berechtigungssatz. Wenn Sie die Berechtigungen ändern möchten, brauchen Sie die Änderung nur an einem Stammordner oder übergeordneten Ordner durchzuführen. Die Änderungen können dann automatisch für alle Unterordner und Dateien dieses Ordners gelten. Auf diese Weise lässt sich ein einziger Berechtigungssatz auf viele Dateien und Ordner anwenden, ohne die Sicherheitseinstellungen für alle Dateien und Ordner einzeln vornehmen zu müssen.

Anzeigen der geerbten Berechtigungen

Um die geerbten Berechtigungen einer Datei oder eines Ordners anzuzeigen, klicken Sie im Datei-Explorer mit der rechten Maustaste auf die Datei oder den Ordner oder halten sie gedrückt und wählen *Eigenschaften*. Auf der Registerkarte *Sicherheit* des *Eigenschaften*-Dialogfelds tippen oder klicken Sie auf *Erweitert*, um das Dialogfeld *Erweiterte Sicherheitseinstellungen* zu öffnen, wie bereits weiter oben in Abbildung 13.3 gezeigt. Die Spalte *Berechtigung* zeigt die aktuellen Berechtigungen an, die für die Ressource eingestellt wurden. Für ererbte Berechtigungen zeigt die Spalte *Geerbt von* den übergeordneten Ordner an. Wird die Berechtigung wiederum an andere Ressourcen weitervererbt, zeigt die Spalte *Anwenden auf* an, welche Ressourcenarten die Berechtigung erben.

Beenden der Vererbung

Wenn Sie in den Sicherheitseinstellungen einer Datei oder eines Ordners die Vererbung deaktivieren, erben die Datei oder der Ordner keine Berechtigungseinstellungen mehr von den übergeordneten Ordnern. Sie haben dann die Wahl, die ererbten Berechtigungen für die Datei oder den Ordner in explizite Berechtigungen umzuwandeln, wodurch die Berechtigungen bearbeitbar werden, oder sämtliche ererbten Berechtigungen von der Datei oder dem Ordner zu entfernen.

Wenn Sie nicht möchten, dass ein Ordner Berechtigungen von einem übergeordneten Ordner erbt, gehen Sie folgendermaßen vor:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf die Datei oder den Ordner oder halten Sie Datei oder Ordner gedrückt, und wählen dann *Eigenschaften*. Auf der Registerkarte *Sicherheit* tippen oder klicken Sie auf *Erweitert*. Dadurch öffnet sich das Dialogfeld *Erweiterte Sicherheitseinstellungen* mit vorgewählter Registerkarte *Berechtigungen*.
2. Auf der Registerkarte *Berechtigungen* sehen Sie eine Schaltfläche mit der Beschriftung *Vererbung deaktivieren*, wenn die Vererbung aktiviert ist. Tippen oder klicken Sie auf *Vererbung deaktivieren*.
3. Wie Abbildung 13.6 zeigt, können Sie nun die ererbten Berechtigungen in explizite Berechtigungen umwandeln oder sie entfernen, damit nur die Berechtigungen gelten, die Sie explizit für die Datei oder den Ordner festlegen.

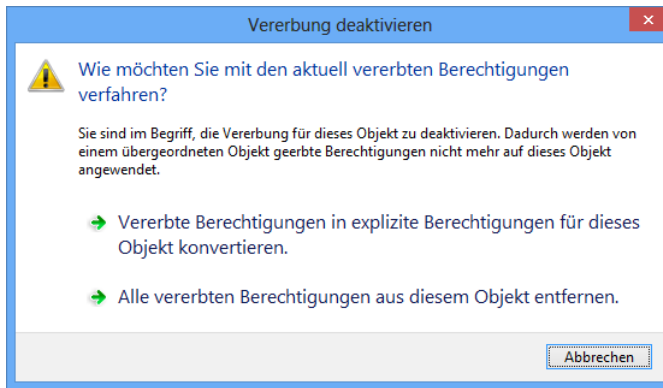


Abbildung 13.6 Umwandeln oder Entfernen von geerbten Berechtigungen

TIPP Wenn Sie die geerbten Berechtigungen entfernt haben und noch keine anderen Berechtigungen zugewiesen wurden, kann niemand auf die Ressourcen zugreifen, mit Ausnahme des Besitzers. Dadurch wird jeder von einer Datei oder einem Ordner ausgesperrt, bis auf den Besitzer. Allerdings haben Administratoren immer noch das Recht, die Ressource in Besitz zu nehmen, ohne die eingestellten Berechtigungen berücksichtigen zu müssen. Wenn also ein Administrator von einer Datei oder einem Ordner ausgesperrt wurde, aber unbedingt Zugang zu der Ressource braucht, kann er die Ressource einfach in Besitz nehmen, um unbeschränkten Zugang zu erhalten.

Wiederherstellen geerbter Berechtigungen

Nach einer gewissen Zeit können die Berechtigungen von Dateien und Unterordnern so stark von denen des übergeordneten Ordners abweichen, dass es kaum noch möglich ist, den Zugriff effizient zu verwalten. Um die Verwaltung des Datei- und Ordnerzugriffs zu vereinfachen, können Sie zu einer drastischen Maßnahme greifen und von allen Ressourcen, die in einem übergeordneten Ordner enthalten sind, die Berechtigungen entfernen. Dann ersetzen Sie die Berechtigungen durch Berechtigungen, die vom übergeordneten Ordner geerbt werden. Auf diese Weise ersetzen die Berechtigungen, die Sie im übergeordneten Ordner festlegen, die Berechtigungen der darin enthaltenen Dateien und Unterordner.

Um die Vererbung der Berechtigungen von einem übergeordneten Ordner wiederherzustellen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf den Ordner oder halten Sie ihn gedrückt, und wählen dann *Eigenschaften*. Auf der Registerkarte *Sicherheit* tippen oder klicken Sie auf *Erweitert*.
2. Wählen Sie auf der Registerkarte *Berechtigungen* die Option *Alle Berechtigungen für untergeordnete Objekte durch vererbte Berechtigungen von diesem Objekt ersetzen* und tippen oder klicken Sie auf *OK*.
3. Sie erhalten eine Meldung wie in Abbildung 13.7 mit der Erklärung, dass durch diesen Vorgang alle explizit definierten Berechtigungen durch vererbte Berechtigungen ersetzt werden. Tippen oder klicken Sie auf *Ja*.

Allerdings brauchen Sie die vorhandenen Berechtigungen nicht vollständig zu ersetzen, um die Vererbung der Berechtigungen von einem übergeordneten Ordner einzurichten. Wurde eine Datei oder ein Ordner so konfiguriert, dass er keine Berechtigungen von einem übergeordneten Ordner erbt, können Sie die Vererbung reaktivieren, damit die Datei oder der Ordner wieder Berechtigungen vom übergeordneten Ordner erbt. Und so geht es:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf die Datei oder den Ordner, der die geerbten Berechtigungen übernehmen soll, oder halten Sie Datei oder Ordner gedrückt, und wählen Sie den Befehl *Eigenschaften*. Tippen oder klicken Sie auf der Registerkarte *Sicherheit* auf *Erweitert*.
2. Tippen oder klicken Sie auf der Registerkarte *Berechtigungen* auf *Vererbung aktivieren* und dann auf OK. Beachten Sie, dass die Schaltfläche *Vererbung aktivieren* nur verfügbar ist, wenn die Berechtigungsvererbung derzeit deaktiviert ist.

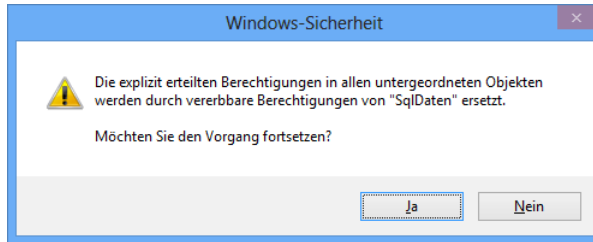


Abbildung 13.7 Tippen oder klicken Sie auf *Ja*, wenn Sie die vorhandenen Berechtigungen ersetzen möchten

Ermitteln der effektiven Berechtigungen und Problembehebung

NTFS-Berechtigungen sind komplex und können schwer zu verwalten sein. Manchmal kann eine Änderung, selbst eine sehr kleine, unerwartete Auswirkungen haben. Benutzer stellen plötzlich fest, dass sie keinen Zugriff mehr auf Dateien haben, mit denen sie vorher problemlos arbeiten konnten. Oder sie stellen fest, dass sie Zugang zu Dateien haben, zu denen sie eigentlich keinen Zugang haben sollten. In beiden Szenarios stimmt etwas nicht mit den Berechtigungen. Sie haben ein Problem und Sie müssen es lösen.

Die Fehlersuche sollte bei solchen und anderen Problemen, die mit falsch eingestellten Berechtigungen zusammenhängen, mit der Bestimmung der effektiven Berechtigungen für die fraglichen Dateien oder Ordner beginnen. Wie die Bezeichnung schon verrät, handelt es sich bei den effektiven Berechtigungen um die Berechtigungen, die tatsächlich für einen bestimmten Benutzer oder eine bestimmte Gruppe wirksam sind. Die effektiven Berechtigungen sind wichtig, weil es sich um die Berechtigungen handelt, die sich aus dem Zusammenwirken aller beteiligten Berechtigungssätze ergeben.

Für einen Benutzer ergeben sich die effektiven Berechtigungen aus den Berechtigungen, die einem Benutzer gewährt oder verweigert wurden, sei es explizit oder durch seine Mitgliedschaft in einer bestimmten Gruppe, deren Berechtigungen auch für ihn gelten. Ist *JimB* zum Beispiel Mitglied der Gruppen *Benutzer*, *Verkauf*, *Marketing*, *Spezifikationen* und *Manager*, ergibt sich die effektive Berechtigung, die für eine Datei oder einen Ordner gilt, aus der kumulativen Wirkung der Berechtigungen, die *JimB* explizit zugewiesen wurden, und der Berechtigungen, die den Gruppen *Benutzer*, *Verkauf*, *Marketing*, *Spezifikationen* und *Manager* zugewiesen wurden. Ist *JimB* Mitglied einer Gruppe, der eine Berechtigung explizit verweigert wird, wird diese Berechtigung auch *JimB* verweigert, selbst wenn einer anderen Gruppe die Berechtigung gewährt wird. *Verweigern*-Einträge haben Vorrang vor *Zulassen*-Einträgen.

Dasselbe gilt für Benutzer- und Geräteansprüche. Wenn Sie eine anspruchsbasierte Authentifizierung eingerichtet und einen Benutzeranspruch hinzugefügt haben, kann dieser Anspruch den Zugang verhindern. In vergleichbarer Weise kann auch ein Geräteanspruch den Zugang verhindern.

Um die effektiven Berechtigungen eines Benutzers oder einer Gruppe an einer Datei oder einem Ordner zu bestimmen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf die Datei oder den Ordner, mit dem Sie arbeiten möchten, oder halten Sie Datei oder Ordner gedrückt, und wählen Sie dann *Eigenschaften*. Wählen Sie im *Eigenschaften*-Dialogfeld die Registerkarte *Sicherheit* und tippen oder klicken Sie auf *Erweitert*.
2. Tippen oder klicken Sie im Dialogfeld *Erweiterte Sicherheitseinstellungen* auf die Registerkarte *Effektiver Zugriff*. Bestimmen Sie mit den verfügbaren Optionen die effektiven Berechtigungen für Benutzer, Gruppen und Geräte. Berücksichtigen Sie dabei Folgendes:
 - Wenn Sie nur überprüfen möchten, über welche Berechtigungen ein bestimmter Benutzer oder eine Benutzergruppe verfügt, tippen oder klicken Sie auf *Einen Benutzer auswählen*, geben den Namen des Benutzers oder der Gruppe ein und tippen oder klicken auf *OK*.
 - Wenn Sie nur überprüfen möchten, über welche Berechtigungen ein bestimmtes Gerät oder eine Gerätegruppe verfügt, tippen oder klicken auf *Gerät auswählen*, geben den Namen des Geräts oder der Gerätegruppe ein und tippen oder klicken auf *OK*.
 - Wenn Sie herausfinden möchten, über welche Berechtigungen ein bestimmter Benutzer oder eine Benutzergruppe auf einem bestimmten Gerät oder in einer Gerätegruppe verfügt, geben Sie beides an, Benutzer oder Benutzergruppe sowie Gerät oder Gerätegruppe.
3. Tippen oder klicken Sie auf *Effektiven Zugriff anzeigen*. Die effektiven Berechtigungen des angegebenen Benutzers oder der Gruppe werden mit dem vollständigen Satz der speziellen Berechtigungen angezeigt. Hat ein Benutzer Vollzugriff auf die gewählte Ressource, verfügt er über die Berechtigungen, die in Abbildung 13.8 zu sehen sind. Andernfalls ist nur eine Teilmenge der Berechtigungen gekennzeichnet und Sie müssen sorgfältig prüfen, ob der Benutzer oder die Gruppe über die erforderlichen Berechtigungen verfügt. Vielleicht hilft Ihnen Tabelle 13.3 weiter oben in diesem Kapitel bei der Bewertung der Berechtigungen.

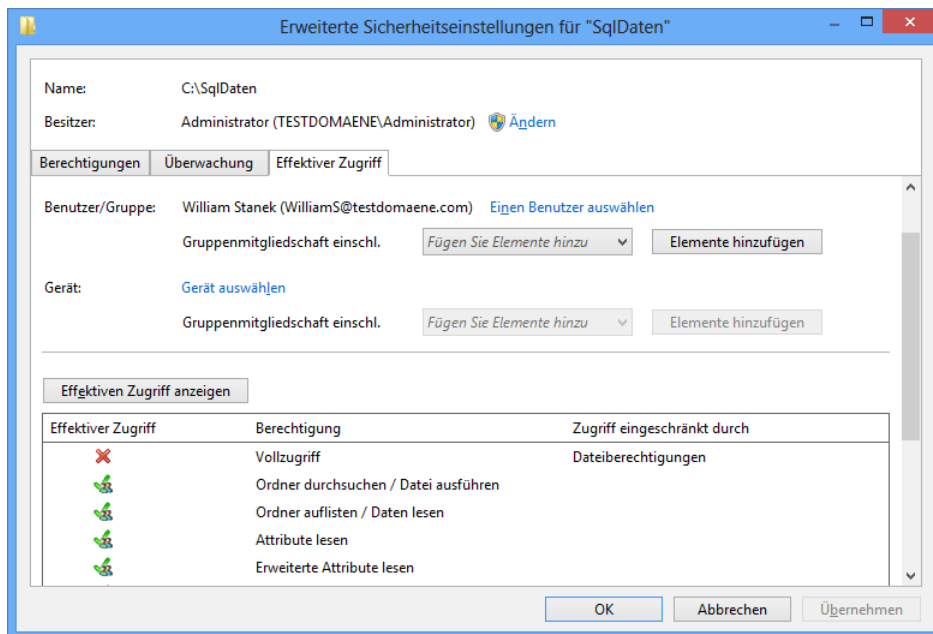


Abbildung 13.8 Jede markierte Berechtigung wurde dem angegebenen Benutzer oder der Gruppe gewährt

HINWEIS

Sie müssen über die entsprechenden Berechtigungen verfügen, um die effektiven Berechtigungen eines Benutzers oder einer Gruppe anzeigen zu können. Beachten Sie bitte, dass Sie nicht die effektiven Berechtigungen von impliziten Gruppen oder Spezialidentitäten bestimmen können, wie zum Beispiel *Authentifizierte Benutzer* oder *Jeder*. Außerdem werden bei der Bestimmung der effektiven Berechtigungen nicht die Berechtigungen berücksichtigt, die ein Benutzer hat, wenn er *Ersteller-Besitzer* ist.

Freigeben von Dateien und Ordnern im Netzwerk

Windows 8 unterstützt zwei Dateifreigabemodelle: die Freigabe von öffentlichen Ordnern und die Standardordnerfreigabe. Beide Verfahren lassen sich zwar in Arbeitsgruppen und Domänen anwenden, aber die Standardordnerfreigabe wird bevorzugt, weil sie sicherer ist als die Freigabe von öffentlichen Ordnern. Bei der Standardordnerfreigabe können Sie mit Standardberechtigungen festlegen, wer über das Netzwerk Zugriff auf die Dateien und Ordner erhält. Die Einstellungen für die Standardordnerfreigabe werden auf Computerbasis aktiviert oder deaktiviert. Gehen Sie folgendermaßen vor, um die Dateifreigabe ein- oder auszuschalten:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Heimnetzgruppen- und Freigabeoptionen auswählen* und dann auf *Erweiterte Freigabeeinstellungen ändern*.
2. Jedes verfügbare Netzwerkprofil hat einen eigenen Verwaltungsabschnitt mit den jeweiligen Konfigurationseinstellungen. Tippen oder klicken Sie auf die entsprechende Pfeilschaltfläche, um das Profil anzuzeigen, das Sie bearbeiten wollen.
3. Wählen Sie die Option *Datei- und Druckerfreigabe aktivieren*, wenn Sie die Datei- und Druckerfreigabe einschalten wollen. Mit der Option *Datei- und Druckerfreigabe deaktivieren* schalten Sie die Datei- und Druckerfreigabe aus. Tippen oder klicken Sie auf *Änderungen speichern*.

Das SMB-Protokoll (Server Message Block) ist das wichtigste Dateifreigabeprotokoll für Windows-Computer. Wenn Ordner im Netzwerk freigegeben werden, liest und schreibt ein SMB-Client die Dateien und fordert Dienstleistungen von dem Computer an, auf dem der freigegebene Ordner liegt. Windows 8 und Windows Server 2012 unterstützen SMB Version 3.0 und enthalten einen SMB 3.0-kompatiblen Client.

SMB 3.0 bietet viele Leistungsverbesserungen, insbesondere bei der Verwendung von Dateiserverclustern. Eine der Erweiterungen, die nach der Installation verfügbar sind und keine spezielle Konfiguration erfordern, ist die Verschlüsselung der SMB-Daten von Endpunkt zu Endpunkt. Sie macht die Verwendung von IPSec, spezieller Hardware oder WAN-Beschleunigern (Wide Area Network) überflüssig, wenn es darum geht, die Daten bei der Übertragung vor unberechtigten Zugriffen zu schützen. Die SMB-Verschlüsselung kann für den ganzen Server oder für jede Freigabe einzeln aktiviert werden.

Kontrollieren des Zugriffs auf Netzwerkfreigaben

Wenn ein Benutzer über das Netzwerk auf eine Datei oder einen Ordner zugreift und die Standardordnerfreigabe aktiviert ist, werden zwei Ebenen von Berechtigungssätzen verwendet. Beide zusammen bestimmen, was ein Benutzer mit einer bestimmten freigegebenen Datei oder einem freigegebenen Verzeichnis tun kann. Die erste Ebene der Berechtigungen wird durch die Freigabeberechtigungen gebildet. Sie definieren den maximalen Zugriff. Ein Benutzer oder eine Gruppe kann nicht über mehr Berechtigungen verfügen, als durch die Freigabe festgelegt wird. Die zweite Ebene der Berechtigungen wird durch die Berechtigungen gebildet, die für die Dateien und Ordner festgelegt wurden. Diese Berechtigungen dienen dazu, die zulässigen Aktionen weiter einzuschränken.

Drei Freigabeberechtigungen sind verfügbar:

- **Besitzer** Benutzer mit dieser Berechtigung haben die Berechtigungen *Vollzugriff*, *Lesen* und *Ändern*. Außerdem dürfen sie Dateien- und Ordnerberechtigungen ändern und Dateien und Ordner in Besitz nehmen. Wenn Sie für eine freigegebene Ressource über die Berechtigung *Besitzer* verfügen, haben Sie vollen Zugriff auf die freigegebene Ressource.
- **Lesen/Schreiben** Benutzer mit dieser Berechtigung haben die Berechtigungen *Lesen* und *Ändern*, außerdem dürfen sie Dateien und Unterordner erstellen, Dateien ändern, Attribute von Dateien und Unterordnern ändern und Dateien und Unterordner löschen. Wenn Sie für eine freigegebene Ressource über die Berechtigung *Lesen/Schreiben* verfügen, können Sie ihre Daten lesen, ändern und löschen, aber nicht in Besitz nehmen.
- **Lesen** Benutzer mit dieser Berechtigung haben nur die Berechtigung *Lesen*. Sie können Datei- und Ordnernamen anzeigen, auf die Unterordner einer Freigabe zugreifen, Dateidaten und Attribute lesen und Programmdateien ausführen. Wenn Sie für eine freigegebene Ressource über die Berechtigung *Lesen* verfügen, können Sie nur Leseoperationen durchführen.

Berechtigungen, die Gruppen zugewiesen werden, wirken so: Wenn ein Benutzer Mitglied einer Gruppe ist, die über Freigabeberechtigungen verfügt, verfügt auch der Benutzer über diese Berechtigungen. Ist der Benutzer Mitglied mehrerer Gruppen, sind die Berechtigungen kumulativ. Ist der Benutzer zum Beispiel Mitglied einer Gruppe, die über die Berechtigung *Lesen/Schreiben* verfügt, erhält auch der Benutzer Zugriff mit der Berechtigung *Lesen/Schreiben*. Hat eine der Gruppen, in denen der Benutzer Mitglied ist, die Freigabeberechtigung *Lesen* und eine andere Gruppe hat die Berechtigung *Besitzer*, verfügt auch der Benutzer über die Freigabeberechtigung *Besitzer*.

Sie können das ändern, indem Sie eine Berechtigung explizit verweigern. Die Verweigerung einer Berechtigung hat Vorrang und setzt die Gewährung von Berechtigungen außer Kraft. Wenn Sie nicht wollen, dass ein Benutzer oder eine Gruppe über eine bestimmte Berechtigung verfügt, konfigurieren Sie die Freigabeberechtigungen so, dass dem Benutzer oder der Gruppe die Berechtigung verweigert wird. Ist ein Benutzer beispielsweise Mitglied einer Gruppe, die für eine Freigabe über die Berechtigung *Besitzer* verfügt, aber der Benutzer soll nur die Berechtigung *Lesen/Schreiben* erhalten, konfigurieren Sie die Berechtigungen für diesen Benutzer so, dass ihm die Berechtigung *Besitzer* verweigert wird.

Erstellen einer freigegebenen Ressource

Ordner können in Arbeitsgruppen und in Domänen freigegeben werden. Um auf einem Computer die erste Ressource freigegeben zu können, müssen Sie ein lokaler Administrator sein. Die Freigabe der ersten Ressource bereitet den Computer auf die Freigabe von anderen Ressourcen vor und ermöglicht anderen Benutzern die Freigabe von Ressourcen, die ihnen gehören oder für die sie über die entsprechenden Zugriffsberechtigungen verfügen.

Freigaben lassen sich mit mehreren Programmen erstellen:

- **Datei-Explorer** Verwenden Sie den Datei-Explorer, wenn Sie auf dem Computer, an dem Sie angemeldet sind, Ordner freigeben möchten.
- **Computerverwaltung** Verwenden Sie die Computerverwaltung, wenn Sie auf den Computern, mit denen Sie eine Verbindung herstellen können, Ordner freigeben möchten.
- **Net share** Verwenden Sie *net share* in einer Befehlszeile, wenn Sie zur Freigabe von Ordnern Skripts verwenden möchten. Wenn Sie in einer Eingabeaufforderung **net share /?** eingeben, zeigt Ihnen das Programm die Syntax des Befehls an.

- **SmbShare** Verwenden Sie das SmbShare-Modul zur Erstellung und Verwaltung von Freigaben. Wenn Sie in einer Windows PowerShell-Eingabeaufforderung `Get-Help smbshare` eingeben, erhalten Sie eine Liste der entsprechenden Cmdlets.

Das Erstellen einer freigegebenen Ressource erfordert mehrere Arbeitsgänge. Zuerst geben Sie den Ordner frei, damit er zugänglich wird. Dann legen Sie die Freigabeberechtigungen fest. Anschließend sollten Sie die Dateisystemberechtigungen überprüfen und nach Bedarf ändern. Dieser Abschnitt beschreibt die Freigabe einer Ressource und die Einstellung der Berechtigungen mit dem Datei-Explorer und der Computerverwaltung. Einzelheiten über die Einstellung der Dateisystemberechtigungen finden Sie im Abschnitt »Kontrollieren des Zugriffs auf Dateien und Ordner mit NTFS-Berechtigungen« weiter oben in diesem Kapitel.

Freigeben einer Ressource und Einstellen der Freigabeberechtigungen im Datei-Explorer

Der Datei-Explorer unterstützt Standard- und erweiterte Freigaben. Mit der Standardfreigabe können Sie beliebige Ordner außer dem Stammordner eines Laufwerks freigeben. Bei der erweiterten Freigabe können Sie den Stammordner eines Laufwerks sowie beliebige andere Ordner freigeben. Die Stammordner von Laufwerken werden automatisch als administrative Freigaben freigegeben.

So geben Sie einen Ordner mit der Standardfreigabe frei:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf den Ordner, den Sie freigeben möchten, oder halten Sie ihn gedrückt, und wählen Sie *Freigeben für* und dann *Bestimmte Personen*. Daraufhin öffnet sich der Dateifreigabe-Assistent (Abbildung 13.9).

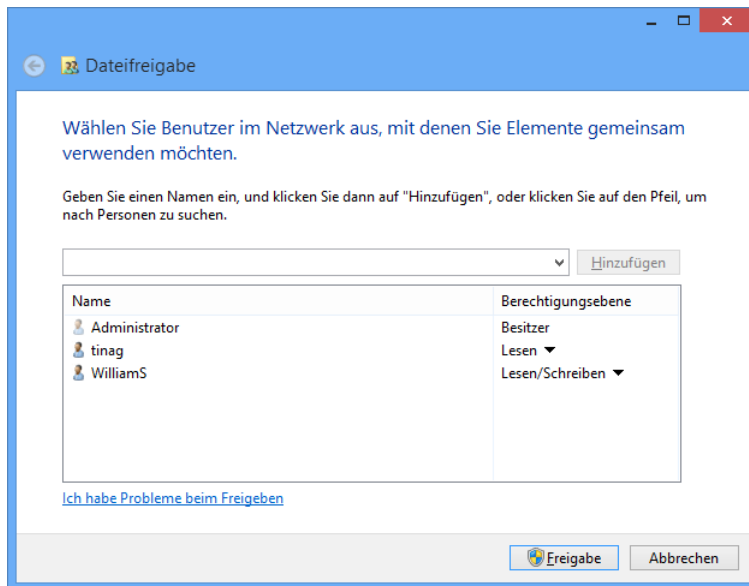


Abbildung 13.9 Im Dateifreigabe-Assistenten konfigurieren Sie die Freigabe der ausgewählten Dateien oder Ordner

2. Geben Sie einen Namen ein und tippen oder klicken Sie auf *Hinzufügen* oder das Pfeilsymbol, um den gewünschten Benutzer auszuwählen. In Arbeitsgruppen zeigt der Computer immer nur die lokalen Konten und Gruppen an. In Domänen werden lokale Benutzer und Gruppen, zusätzlich aber auch Domänenbenutzer aufgeführt.

3. Wenn Sie auf *Hinzufügen* tippen oder klicken, werden die gewählten Benutzer und Gruppen zur Namensliste hinzugefügt. Dann können Sie für jeden Benutzer und jede Gruppe die Berechtigungen einstellen, indem Sie ein Konto anklicken, um die verfügbaren Berechtigungsebenen anzuzeigen, und dann die passende Berechtigungsebene wählen. Zur Verfügung stehen die Berechtigungsebenen *Lesen*, *Lesen/Schreiben* und *Besitzer*.
4. Zum Schluss tippen oder klicken Sie auf *Freigabe*, um die Freigabe zu erstellen. Nachdem Windows 8 die Freigabe erstellt und auf die Verwendung vorbereitet hat, notieren Sie sich den Freigabenamen. Das ist der Name, unter dem die Ressource zugänglich ist. Wenn Sie jemandem per E-Mail einen Link auf die freigegebene Ressource senden möchten, tippen oder klicken Sie auf den Link *E-Mail*. Wenn Sie einen Link auf die freigegebene Ressource in die Zwischenablage kopieren möchten, tippen oder klicken Sie auf den Link *kopieren*. Tippen oder klicken Sie zuletzt auf *Fertig*.

HINWEIS Wenn Sie eine Freigabe erstellen, greifen die Benutzer gewöhnlich mit einem abgekürzten UNC-Pfad (Universal Naming Convention) auf die Freigabe zu. Geben Sie beispielsweise den Ordner *C:\Daten\Berichte\Aktuell* auf dem Computer *CorPC85* unter dem Namen *Berichte* frei, können andere Benutzer mit dem UNC-Pfad *\\CorPC85\Berichte* auf diesen Ordner zugreifen. Wenn Sie einen Ordner allerdings innerhalb eines Benutzerprofils freigeben, verwenden die Benutzer für den Zugriff auf den Ordner einen Pfad, der den Ordner relativ zum Ordner *Users* auf dem Computer angibt. Das ist so, weil Windows Freigaben relativ zum Speicherort des Ordners innerhalb des Ordners *Users* konfiguriert. Gibt beispielsweise *MollyH* ihren Ordner *Documents* auf *CustPC27* frei, lautet der UNC-Pfad für diese Freigabe *\\CustPC27\Users\MollyH\Documents*.

Gehen Sie folgendermaßen vor, um einen Ordner über die erweiterte Freigabe freizugeben:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf den Ordner, den Sie freigeben möchten, oder halten Sie ihn gedrückt, und wählen Sie den Befehl *Eigenschaften*. Daraufhin öffnet sich das Eigenschaftendialogfeld des Ordners.
2. Tippen oder klicken Sie auf der Registerkarte *Freigabe* auf *Erweiterte Freigabe*. Aktivieren Sie im Dialogfeld *Erweiterte Freigabe* das Kontrollkästchen *Diesen Ordner freigeben*.
3. Windows trägt als Freigabenamen standardmäßig den Ordernamen ein. Sie können entweder diesen Standardfreigabenamen übernehmen oder einen anderen Namen eintippen.
4. Tippen oder klicken Sie auf *Berechtigungen*. Konfigurieren Sie im Dialogfeld *Berechtigungen für die Zugriffsberechtigungen* für die Freigabe. Tippen oder klicken Sie auf *OK*.
5. Tippen oder klicken Sie auf *Zwischenspeichern*. Legen Sie im Dialogfeld *Offlineeinstellungen* fest, ob und wie Daten für die Offlineverwendung zwischengespeichert werden. Tippen oder klicken Sie auf *OK*.
6. Tippen oder klicken Sie auf *OK* und dann auf *Schließen*.

Ändern oder Beenden der Freigabe

Wenn Sie einen Ordner, der bereits freigegeben ist, mit der rechten Maustaste anklicken oder ihn gedrückt halten, und im Kontextmenü *Freigeben für* und dann *Freigabe beenden* wählen, entfernen Sie die Freigabeeinstellungen und beenden die Freigabe des Ordners. Die Freigabeberechtigungen ändern Sie, indem Sie mit der rechten Maustaste auf den freigegebenen Ordner klicken oder ihn gedrückt halten, und im Kontextmenü erst *Freigeben für* und dann *Bestimmte Personen* wählen. Nun können Sie weiteren Benutzern und Gruppen den Zugriff erlauben, wie weiter oben beschrieben. Sie entfernen den Zugriff für einen Benutzer oder eine Gruppe, indem Sie den Benutzer oder die Gruppe in der Namensliste auswählen und *Entfernen* wählen. Tippen oder klicken Sie auf *Freigabe*, wenn Sie die gewünschten Änderungen

vorgenommen haben. Die Optionen werden nun neu konfiguriert. Tippen oder klicken Sie zuletzt auf *Fertig*.

Wenn Sie die erweiterte Freigabe nutzen, konfigurieren Sie die Freigabeeinstellungen, indem Sie mit der rechten Maustaste auf den Ordner klicken oder ihn gedrückt halten, und den Befehl *Eigenschaften* wählen. Tippen oder klicken Sie auf der Registerkarte *Freigabe* auf *Erweiterte Freigabe*. Nun können Sie Freigaben aktivieren oder deaktivieren und Verbindungslimits für Benutzer festlegen. Außerdem können Sie hier die Berechtigungen und die Zwischenspeicherung konfigurieren.

Freigeben eines Ordners und Einstellen der Freigabeberechtigungen in der Computerverwaltung

In der Computerverwaltung können Sie einen Ordner auf jedem Computer freigeben, auf dem Sie über Administratorrechte verfügen. Durch den Remotezugriff auf den Computer sparen Sie normalerweise Zeit, weil Sie sich nicht lokal anmelden müssen und Ihren Schreibtisch nicht zu verlassen brauchen. Mit der Computerverwaltung können Sie einen Ordner folgendermaßen freigeben:

1. Starten Sie die Computerverwaltung in der Systemsteuerung unter *Verwaltung* oder geben Sie im Suchfeld *Apps compmgmt.msc* ein und drücken Sie die EINGABETASTE. Standardmäßig stellt die Computerverwaltung eine Verbindung mit dem lokalen Computer her und zeigt im Stammknoten der Strukturdarstellung die Beschriftung *Computerverwaltung (Lokal)*.

TIPP Wenn Sie mit dem Assistenten zum Erstellen von Ordnerfreigaben einen Ordner des lokalen Computers freigeben möchten, starten Sie den Assistenten direkt und überspringen die Punkte 1 bis 4. Geben Sie in einer Eingabeaufforderung mit erhöhten Rechten einfach **shrpwbw** ein und tippen oder klicken Sie dann auf *Weiter*, wenn der Assistent gestartet wird.

2. Klicken Sie in der Strukturdarstellung mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen Sie dann *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* ist die Option *Anderen Computer* vorgewählt. Geben Sie den vollqualifizierten Domänennamen des Computers ein, mit dem Sie arbeiten möchten, wie zum Beispiel **engpc08.microsoft.com**, wobei *engpc08* der Computername ist und *microsoft.com* der Domänenname. Wenn Sie den Computernamen nicht kennen, aber die Netzwerkerkennung aktiviert ist, können Sie auf *Durchsuchen* klicken und den Computer heraussuchen, mit dem Sie arbeiten möchten.
3. Erweitern Sie die Ordner *System* und *Freigegebene Ordner* und wählen Sie dann *Freigaben*, um die aktuell freigegebenen Ordner des Computers anzuzeigen, mit dem Sie arbeiten (Abbildung 13.10).
4. Um den Assistenten zum Erstellen von Ordnerfreigaben zu starten, klicken Sie den Knoten *Freigaben* mit der rechten Maustaste an oder halten ihn gedrückt, und wählen dann *Neue Freigabe*. Tippen oder klicken Sie auf *Weiter*, um die Seite *Ordnerpfad* anzuzeigen.
5. Geben Sie im Textfeld *Ordnerpfad* den vollständigen Pfad des Ordners an, den Sie freigeben möchten, beispielsweise **C:\Daten**. Wenn Sie den vollständigen Pfad nicht kennen, tippen oder klicken Sie auf *Durchsuchen* und suchen dann im Dialogfeld *Ordner suchen* den Ordner heraus, den Sie freigeben möchten. Im Dialogfeld *Ordner suchen* können Sie auch einen neuen Ordner anlegen, den Sie anschließend freigeben. Tippen oder klicken Sie auf *Weiter*, um zur Seite *Name, Beschreibung und Einstellungen* zu wechseln.
6. Geben Sie im Textfeld *Freigabename* einen Namen für die Freigabe ein. Freigabennamen müssen auf jedem Computer eindeutig sein. Sie können bis zu 80 Zeichen lang sein und Leerzeichen enthalten.

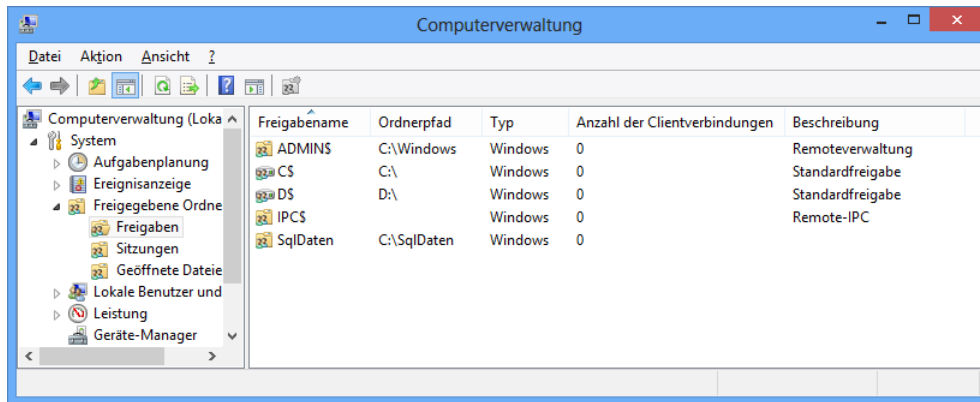


Abbildung 13.10 Im Knoten *Freigaben* sind alle freigegebenen Ordner aufgeführt

7. Geben Sie im Textfeld *Beschreibung* eine Beschreibung der Freigabe ein.

TIPP Standardmäßig sind nur Dateien und Programme, die Benutzer auswählen, offline verfügbar. Tippen oder klicken Sie auf *Ändern*, wenn Sie die Offlineeinstellungen ändern möchten. Durch die Wahl von *Alle Dateien und Programme, die Benutzer über den freigegebenen Ordner öffnen, automatisch offline verfügbar machen* können Sie dafür sorgen, dass alle Dateien und Ordner automatisch offline verfügbar sind, während die Wahl von *Keine Dateien oder Programme aus dem freigegebenen Ordner offline verfügbar machen* die Offlineverwendung der Programme und Dateien verhindert. Tippen oder klicken Sie auf *OK*.

8. Wenn Sie fortfahren möchten, wechseln Sie durch Tippen oder Klicken auf *Weiter* auf die Seite *Berechtigungen für freigegebene Ordner*. Folgende Optionen stehen zur Verfügung:
- ***Alle Benutzer haben schreibgeschützten Zugriff*** Die Standardoption. Benutzer erhalten das Recht, Dateien anzuzeigen und Daten zu lesen, können aber keine Dateien oder Ordner erstellen, ändern oder löschen.
 - ***Administratoren haben Voll-, andere Benutzer schreibgeschützten Zugriff*** Administratoren erhalten Vollzugriff auf die Freigabe, andere Benutzer nur Lesezugriff. Administratoren können Dateien und Ordner erstellen, ändern und löschen. Auf einem NTFS-Dateisystem erhalten Administratoren auch das Recht, Berechtigungen zu ändern und Dateien und Ordner in Besitz zu nehmen. Benutzer können nur Dateien anzeigen und Daten lesen. Sie können keine Dateien oder Ordner erstellen, ändern oder löschen.
 - ***Administratoren haben Vollzugriff, andere Benutzer haben keinen Zugriff*** Gibt Administratoren Vollzugriff auf die Freigabe.
 - ***Berechtigungen anpassen*** Ermöglicht Ihnen die Einstellung der Berechtigungen für bestimmte Benutzer oder Gruppen. Gewöhnlich ist dies die empfehlenswerte Methode. Um diese Option zu verwenden, wählen Sie *Berechtigungen anpassen*, tippen oder klicken auf *Benutzerdefiniert* und stellen die Berechtigungen für die Freigabe ein.
9. Nachdem Sie die Berechtigungen für die Freigabe eingestellt haben, tippen oder klicken Sie auf *Fertig stellen*, damit die Freigabe erstellt wird. Tippen oder klicken Sie noch einmal auf *Fertig stellen*, um den Assistenten zu beenden.

Wenn Sie später die Freigabe des Ordners beenden möchten, können Sie dies in der Computerverwaltung tun, indem Sie den freigegebenen Ordner mit der rechten Maustaste anklicken oder ihn gedrückt halten und *Freigabe aufheben* wählen. Wenn Sie dazu aufgefordert werden, bestätigen Sie den Vorgang durch Tippen oder Klicken auf *Ja*.

Erstellen und Verwalten von freigegebenen Ordnern mit Gruppenrichtlinien

Sie können Ordner auch durch Gruppenrichtlinieneinstellungen freigeben. Diesen Ansatz empfehle ich nur, wenn Sie die Zielcomputer detailliert auswählen können, damit nur Computer, die tatsächlich auch Daten freigeben sollen, mit freigegebenen Ordnern konfiguriert werden.

Gehen Sie folgendermaßen vor, um ein Einstellungselement anzulegen, mit dem Sie freigegebene Ordner erstellen, aktualisieren, ersetzen oder löschen:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Erweitern Sie den Zweig *Computerkonfiguration\Einstellungen\Windows-Einstellungen* und wählen Sie *Netzwerkfreigaben* aus.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Netzwerkfreigaben* oder halten Sie ihn gedrückt, und wählen Sie *Neu/Netzwerkfreigabe*. Daraufhin öffnet sich das Eigenschaftendialogfeld für die neue Netzwerkfreigabe.
3. Wählen Sie in der Liste *Aktion* des Eigenschaftendialogfelds den Eintrag *Erstellen*, *Aktualisieren*, *Ersetzen* oder *Löschen* aus.
4. Geben Sie im Textfeld *Freigabename* einen Namen für die Freigabe ein. Freigabennamen müssen auf jedem System eindeutig sein. Sie können bis zu 80 Zeichen lang sein und dürfen Leerzeichen enthalten.
5. Geben Sie im Textfeld *Ordnerpfad* den vollständigen Pfad des Ordners ein, den Sie freigeben wollen, zum Beispiel *C:\Daten*. Wenn Sie den vollständigen Pfad nicht wissen, können Sie auch auf die *Durchsuchen*-Schaltfläche tippen oder klicken und im Dialogfeld *Ordnerauswahl* einen geeigneten Ordner heraussuchen.

PRAXISTIPP

Wenn Sie im Ordnerpfad eine Umgebungsvariable verwenden wollen, können Sie F3 drücken, um eine Liste der definierten Systemvariablen anzuzeigen. Tippen oder klicken Sie auf die Variable, die Sie in den Pfad einbauen wollen, beispielsweise *LogonUser*. In der Standardeinstellung werden Variablen von den Gruppenrichtlinien aufgelöst, bevor sie auf dem Computer eines Benutzers angewendet werden. Soll die Variable stattdessen als Platzhalter benutzt werden, der erst auf dem Computer des Benutzers aufgelöst wird, müssen Sie das Kontrollkästchen *Variable auflösen* löschen, bevor Sie auf *Auswählen* tippen oder klicken. Daraufhin wird ein Platzhalter für die Variable eingefügt, der erst auf dem Computer des Benutzers aufgelöst wird.

In den Gruppenrichtlinieneinstellungen können Sie leicht erkennen, welche Variablen von den Gruppenrichtlinien und welche erst auf dem Computer des Benutzers aufgelöst werden. Variablen, die von den Gruppenrichtlinien aufgelöst werden, haben die Syntax *%Variablenname%*, zum Beispiel *%ProgramFilesDir%*. Dagegen haben Variablen, die erst auf dem Computer des Benutzers aufgelöst werden, die Syntax *%<Variablenname>%*, beispielsweise *%<ProgramFilesDir>%*.

6. Tippen Sie im Textfeld *Kommentar* eine Beschreibung für den Inhalt der Freigabe ein.
7. Wenn Sie Freigaben aktualisieren oder löschen, können Sie alle Freigaben eines bestimmten Typs ändern oder löschen. Sie sind also nicht auf eine einzige Freigabe beschränkt. Für diese Aufgabe stehen folgende Möglichkeiten zur Auswahl:

- Aktivieren Sie das Kontrollkästchen *Alle regulären Freigaben aktualisieren* oder *Alle regulären Freigaben löschen*, um alle Freigaben zu aktualisieren oder zu löschen, die keine ausgeblendeten, administrativen oder speziellen Freigaben sind.
- Aktivieren Sie das Kontrollkästchen *Alle ausgeblendeten Freigaben mit Ausnahme administrativer Freigaben aktualisieren* oder *Alle ausgeblendeten Freigaben mit Ausnahme administrativer Freigaben löschen*, um alle ausgeblendeten Freigaben zu aktualisieren oder zu löschen, die keine administrativen und speziellen Freigaben sind (dazu gehören Freigaben für Laufwerksbuchstaben, *ADMIN\$*, *FAX\$*, *IPC\$* und *Print\$*).
- Aktivieren Sie das Kontrollkästchen *Alle administrativen Freigaben mit Laufwerksbuchstabe aktualisieren* oder *Alle administrativen Freigaben mit Laufwerksbuchstabe löschen*, um alle administrativen Freigaben für Laufwerksbuchstaben zu aktualisieren oder zu löschen.

HINWEIS Wenn Sie spezielle Freigaben, etwa *ADMIN\$*, *FAX\$*, *IPC\$* und *Print\$*, oder andere Systemfreigaben wie *SYSVOL* und *NETLOGON* ändern möchten, können Sie ein Element für die jeweilige Freigabe erstellen und dann im Textfeld *Freigabename* den Namen der speziellen Freigabe eintragen.

8. Stellen Sie ein, wie viele Benutzer gleichzeitig auf die Freigabe zugreifen dürfen. Wählen Sie die Option *Höchstanzahl zulassen* aus, wenn Sie so viele Benutzer zulassen wollen, wie das Betriebssystem ermöglicht. Oder wählen Sie *Zugelassene Benutzeranzahl* aus, um selbst eine Höchstzahl festzulegen.
9. Legen Sie fest, ob die Zugriffssteuerung für die Entscheidung eingesetzt werden soll, ob Benutzer Ordner in der Freigabe ansehen dürfen. Wählen Sie unter *Zugriffsbasierte Aufzählung* die Option *Aktivieren*, wenn nur Benutzer, die über die Berechtigung *Lesen* verfügen, die Ordner in der Freigabe zu sehen bekommen sollen. Wählen Sie *Deaktivieren*, wenn allen Benutzern erlaubt sein soll, die Ordner innerhalb der Freigabe anzusehen.
10. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Weil Sie in diesem Fall eine Einstellung erzwingen, ist es sinnvoll, die Einstellung jedes Mal anzuwenden, wenn die Gruppenrichtlinien aktualisiert werden. Deaktivieren Sie daher das Kontrollkästchen *Nur einmal anwenden*.
11. Tippen oder klicken Sie auf *OK*. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Element angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Element definiert haben.

Verwenden von freigegebenen Ressourcen

Sobald Sie eine Datei oder einen Ordner freigegeben haben, können Benutzer die Freigaben als Netzwerkressourcen verwenden oder auf ihren Computern mit einem Laufwerksbuchstaben verknüpfen. Nach der Zuordnung eines Laufwerksbuchstabens können Benutzer mit den Ressourcen arbeiten, als handle es sich um ein lokales Laufwerk auf ihrem Computer.

Mit folgenden Schritten können Sie eine freigegebene Datei oder einen freigegebenen Ordner als Netzlaufwerk verbinden:

1. Öffnen Sie den Datei-Explorer, tippen oder klicken Sie auf die Optionsschaltfläche ganz links in der Adressleiste (das kleine Dreieck) und tippen oder klicken Sie dann auf *Computer*. Dadurch öffnet sich das *Computer*-Fenster.
2. Tippen oder klicken Sie in der Menüleiste auf *Computer* und dann auf die Schaltfläche *Netzlaufwerk verbinden*. Dadurch öffnet sich das Dialogfeld *Netzlaufwerk verbinden* (Abbildung 13.11).

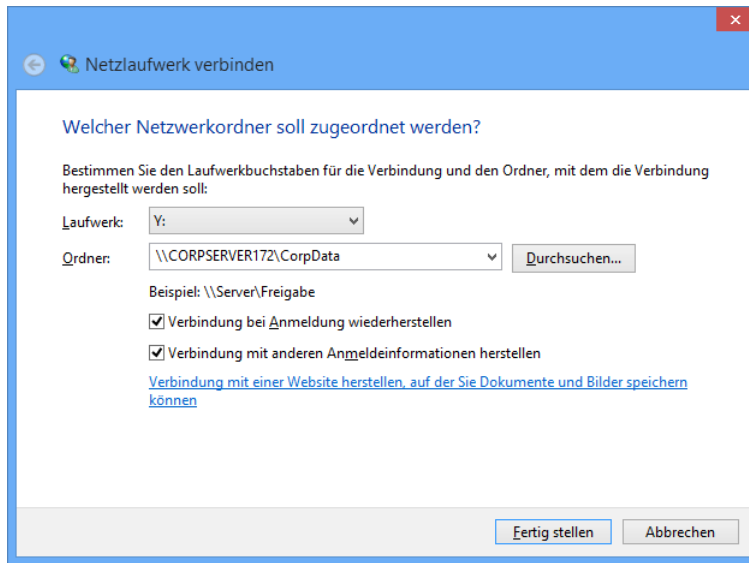


Abbildung 13.11 Ordnen Sie die Freigabe zu, die Sie als Netzlaufwerk verwenden möchten

3. Wählen Sie im Feld *Laufwerk* einen freien Laufwerksbuchstaben aus und klicken Sie dann auf die Schaltfläche *Durchsuchen* rechts neben dem Feld *Ordner*. Im Dialogfeld *Ordner suchen* erweitern Sie die Netzwerkordner, bis Sie den Namen der Arbeitsgruppe oder Domäne wählen können, mit der Sie arbeiten möchten.
4. Wenn Sie den Knoten eines Computers aus einer Arbeitsgruppe oder einer Domäne erweitern, sehen Sie eine Liste der freigegebenen Ordner. Wählen Sie den freigegebenen Ordner aus, mit dem Sie arbeiten möchten, und tippen oder klicken Sie dann auf *OK*.
5. Wählen Sie *Verbindung bei Anmeldung wiederherstellen*, wenn Windows 8 die Verbindung zum freigegebenen Ordner zu Beginn der nächsten Sitzung automatisch wiederherstellen soll.
6. Tippen oder klicken Sie auf *Fertig stellen*. Falls der momentan angemeldete Benutzer keine ausreichenden Zugriffsberechtigungen für die Freigabe hat, müssen Sie das Kontrollkästchen *Verbindung mit anderen Anmeldeinformationen herstellen* aktivieren, bevor Sie auf *Fertig stellen* klicken. Anschließend haben Sie die Gelegenheit, Benutzername und Kennwort des Kontos einzugeben, unter dem Sie die Verbindung zum freigegebenen Ordner herstellen wollen. Geben Sie den Benutzernamen im Format *Domäne\Benutzername* ein, zum Beispiel *Cpandl\Williams*. Wählen Sie *Anmeldedaten speichern*, bevor Sie auf *OK* tippen oder klicken, wenn Sie möchten, dass die Anmeldedaten gespeichert werden. Andernfalls müssen Sie die Anmeldeinformationen künftig wieder eingeben, um die Verbindung herzustellen.

Denken Sie bei der Zuordnung von Netzlaufwerken daran, dass ein Computer in folgenden Situationen in den Offlinemodus wechselt:

- Wenn der Server nicht erreichbar ist
- Wenn das Netzwerk zu langsam ist (wie in den Gruppenrichtlinien festgelegt)
- Wenn ein Benutzer im Datei-Explorer die Option *Offlinebetrieb* wählt
- Wenn das zugeordnete Laufwerk für die permanente Offlineverwendung konfiguriert ist

Um die permanente Offlineverwendung zu aktivieren, klicken Sie das zugeordnete Netzlaufwerk im Datei-Explorer mit der rechten Maustaste an oder halten es gedrückt, und wählen dann *Immer offline verfügbar*. Bei Bedarf konfiguriert und startet Windows 8 dann den Dienst *Offlinedateien*, damit die dafür vorgesehenen Dateien und Programme, die auf dem Server liegen, auf dem Computer zwischengespeichert werden können, auf dem Sie arbeiten. Falls sich der Computer in einem langsamen Netzwerk befindet, entscheiden auch die Gruppenrichtlinieneinstellungen für langsame Netzwerke darüber, ob Dateien kopiert werden. Wie langsame Verbindungen für Offlinedateien verwendet werden, können Sie mit der Richtlinie *Modus für langsame Richtlinien konfigurieren* festlegen, zu finden in den administrativen Vorlagen der Computerkonfiguration unter *Netzwerk\Offlinedateien*.

Die permanente Offlineverwendung ist in Windows 8 und Windows Server 2012 neu. Ist sie aktiviert, verwendet Windows 8 das zugeordnete Netzlaufwerk immer im Offlinemodus. Es hängt dann von den auf dem Server festgelegten Einstellungen für die Zwischenspeicherung ab, welche Dateien und Programme für die Offlineverwendung auf dem Computer gespeichert werden. Standardmäßig sind nur Dateien und Programme für die Offlineverwendung verfügbar, die von Benutzern dafür ausgewählt werden, und Sie müssen gegebenenfalls die Einstellungen für den freigegebenen Ordner auf dem Server (oder mit Gruppenrichtlinien) ändern, um die Zwischenspeicherung anzupassen.

Der Dienst *Offlinedateien* ist für die Verwaltung des Offlinedateizwischenspeichers und die Synchronisierung von Änderungen zuständig. Standardmäßig überträgt der Dienst Änderungen alle 2 Stunden auf den Server. Wie die Hintergrundsynchonisierung für Offlinedateien arbeitet, können Sie mit der Richtlinie *Hintergrundsynchronisierung konfigurieren* festlegen, zu finden in den administrativen Vorlagen der Computerkonfiguration unter *Netzwerk\Offlinedateien*.

HINWEIS

Die permanente Offlineverwendung ist eine Funktion von Windows 8 und Windows Server 2012. Nur Computer, die zu Domänen gehören und auf denen Windows 8 oder Windows Server 2012 ausgeführt wird, können die permanente Offlineverwendung nutzen.

Wenn Sie sich später dazu entschließen, das Netzlaufwerk nicht mehr zu verwenden, öffnen Sie den Datei-Explorer und wählen den Knoten *Computer*. Unter *Netzwerkadresse* klicken Sie mit der rechten Maustaste auf das Netzlaufwerksymbol oder halten es gedrückt, und wählen *Trennen*.

Gehen Sie folgendermaßen vor, um die Gruppenrichtlinien zu öffnen und mit einem Element auf mehreren Computern in einer ganzen Domäne die Netzlaufwerke zu konfigurieren:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Erweitern Sie *Benutzerkonfiguration\Einstellungen\Windows-Einstellungen* und wählen Sie *Laufwerkzuordnungen* aus.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Laufwerkzuordnungen* oder halten Sie ihn gedrückt, und wählen Sie *Neu/Zugeordnetes Laufwerk*. Daraufhin öffnet sich das Eigenschaftendialogfeld für das neue Laufwerk.
3. Wählen Sie in der Dropdownliste *Aktion* des Eigenschaftendialogfelds den Eintrag *Erstellen, Aktualisieren, Ersetzen* oder *Löschen* aus.
4. Geben Sie im Textfeld *Speicherort* den UNC-Pfad der Netzwerkfreigabe ein, zum Beispiel *\\CorpServer45\corpdatashare*, oder tippen oder klicken Sie auf die dazugehörige Schaltfläche, um eine Freigabe auszuwählen.

PRAXISTIPP

Wenn Sie im Freigabepfad eine Umgebungsvariable verwenden wollen, können Sie ins Textfeld *Speicherort* tippen oder klicken und F3 drücken, um eine Liste der definierten Systemvariablen anzuzeigen. Tippen oder klicken Sie auf die Variable, die Sie in den Pfad einbauen wollen, beispielsweise *LogonUser*. In der Standardeinstellung werden Variablen von den Gruppenrichtlinien aufgelöst, bevor sie auf dem Computer eines Benutzers angewendet werden. Soll die Variable stattdessen als Platzhalter benutzt werden, der erst auf dem Computer des Benutzers aufgelöst wird, müssen Sie das Kontrollkästchen *Variable auflösen* aktivieren, bevor Sie auf *Auswählen* klicken. Daraufhin wird ein Platzhalter für die Variable eingefügt, der erst auf dem Computer des Benutzers aufgelöst wird.

In den Gruppenrichtlinieneinstellungen können Sie leicht erkennen, welche Variablen von den Gruppenrichtlinien und welche erst auf dem Computer des Benutzers aufgelöst werden. Variablen, die von den Gruppenrichtlinien aufgelöst werden, haben die Syntax *%Variablenname%*, zum Beispiel *%ProgramFilesDir%*. Dagegen haben Variablen, die auf dem Computer des Benutzers aufgelöst werden, die Syntax *%<Variablenname>%*, beispielsweise *%<ProgramFilesDir>%*.

5. Aktivieren Sie das Kontrollkästchen *Verbindung wiederherstellen*, wenn Windows 8 die Verbindung zum freigegebenen Ordner automatisch beim Start jeder Sitzung neu aufbauen soll.
6. Geben Sie im Textfeld *Beschriften als* einen Namen für das Netzlaufwerk ein.
7. Wählen Sie im Bereich *Laufwerkbuchstabe* aus, wie der Laufwerkbuchstabe zugewiesen werden soll. Wählen Sie die Option *Ersten verfügbaren verwenden, beginnend bei* aus und geben Sie dann den ersten Laufwerkbuchstaben ein, um den ersten freien Laufwerkbuchstaben ab dem angegebenen Buchstaben zu verwenden. Wählen Sie die Option *Verwenden* und wählen Sie den Laufwerkbuchstaben aus, wenn immer genau dieser Laufwerkbuchstabe benutzt werden soll. Sofern Sie nicht sicher sind, dass ein Laufwerkbuchstabe immer frei ist, sollten Sie den ersten verfügbaren Laufwerkbuchstaben verwenden.
8. Optional können Sie eingeben, welche Anmeldeinformationen verwendet werden sollen, um die Verbindung zur Netzwerkfreigabe aufzubauen.
 - Geben Sie die Anmeldeinformationen ein, wenn Sie ein Netzlaufwerk unter Verwendung anderer Anmeldeinformationen zuordnen wollen als derjenigen des Benutzers. Das Kennwort wird verschlüsselt und auf Domänencontrollern im Gruppenrichtlinienobjekt in *Sysvol* gespeichert.
 - Geben Sie *%<LogonUser>%* in das Textfeld *Benutzername* ein und lassen Sie die Textfelder *Kennwort* und *Kennwort bestätigen* leer, wenn die Benutzer die erforderlichen Anmeldeinformationen selbst eingeben sollen.

HINWEIS

Anmeldeinformationen für ein Netzlaufwerk abzuspeichern, ist aus Sicherheitsgründen keine gute Lösung. Sie sollten diesen Ansatz nur in Ausnahmefällen verwenden. Wenn Sie diese Technik dennoch nutzen, sollten Sie das Kennwort des verwendeten Benutzerkontos zumindest regelmäßig ändern und dann die Kennwörter in allen Elementen anpassen, die dieses Konto benutzen.

9. Es stehen weitere Optionen zur Verfügung, mit denen Sie das Laufwerk, das Sie konfigurieren, oder alle Laufwerke ausblenden oder einblenden können. Wenn Sie alle Laufwerke ein- oder ausblenden, wirkt sich das sowohl auf Netzlaufwerke als auch physische Laufwerke aus.
10. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. Weil Sie in diesem Fall eine Einstellung erzwingen, ist es sinnvoll, die Einstellung jedes Mal anzuwenden, wenn die Gruppenrichtlinien aktualisiert werden. Deaktivieren Sie daher das Kontrollkästchen *Nur einmalig anwenden*.

11. Tippen oder klicken Sie auf **OK**. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Verwenden von freigegebenen Ordnern zur Administration

In Windows 8 gibt es einige spezielle Freigaben, die automatisch erstellt werden und für die Verwendung durch Administratoren oder das Betriebssystem vorgesehen sind. Die meisten dieser speziellen Freigaben haben ein Dollarzeichen (\$) an den Namen angehängt und bleiben dadurch den Benutzern verborgen. Als Administrator müssen Sie vielleicht selbst verborgene Freigaben erstellen oder mit den vordefinierten speziellen Freigaben arbeiten.

Es ist nicht schwer, eine verborgene Freigabe zu erstellen. Sie brauchen nur ein Dollarzeichen (\$) ans Ende des Freigabenamens anzuhängen. Vielleicht möchten Sie den Ordner *C:\Berichte* freigeben, wollen aber nicht, dass er in den normalen Freigabelisten aufgeführt wird. Sie brauchen dieser Freigabe dann nur den Namen *Berichte\$* statt *Berichte* zu geben. Damit wird aber nicht der Zugriff auf die Freigabe kontrolliert. Der Zugriff auf Freigaben wird durch Berechtigungen kontrolliert, unabhängig davon, ob die Freigabe sichtbar ist oder nicht.

Welche speziellen Freigaben auf einem System verfügbar sind, hängt von der Konfiguration des Systems ab. Das bedeutet, dass es auf einigen Computern vielleicht mehr Freigaben gibt als auf anderen. Tabelle 13.4 beschreibt die gebräuchlicheren speziellen und administrativen Freigaben.

Die besten Werkzeuge für die Arbeit mit speziellen oder aus anderen Gründen verborgenen Freigaben sind der Befehl *net share* und die Computerverwaltung. Wenn Sie eine Liste aller Freigaben brauchen, die es auf dem lokalen Computer gibt, einschließlich der speziellen Freigaben für Administratoren, geben Sie in einer Eingabeaufforderung einfach den Befehl **net share** ein. Zur Anzeige der Freigaben, die es auf anderen Computern aus dem Netzwerk gibt, gehen Sie folgendermaßen vor:

1. Starten Sie die Computerverwaltung in der Systemsteuerung unter *Verwaltung* oder geben Sie im *Apps*-Suchfeld **compmgmt.msc** ein und drücken Sie die **EINGABETASTE**. Standardmäßig stellt die Computerverwaltung eine Verbindung mit dem lokalen Computer her und zeigt im Stammknoten der Strukturdarstellung die Beschriftung *Computerverwaltung (Lokal)*.
2. Klicken Sie in der Strukturdarstellung mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen Sie dann *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* ist die Option *Anderen Computer* vorgewählt. Geben Sie den Hostnamen oder vollqualifizierten Domännennamen des Computers ein, mit dem Sie arbeiten möchten, wie zum Beispiel **engpc08** oder **engpc08.microsoft.com**, wobei *engpc08* der Computernamen ist und *microsoft.com* der Domänenname. Wenn Sie den Computernamen nicht kennen, aber die Netzwerkerkennung aktiviert ist, können Sie auf *Durchsuchen* tippen oder klicken und den Computer heraussuchen, mit dem Sie arbeiten möchten.
3. Erweitern Sie *System* und *Freigegebene Ordner* und wählen Sie dann *Freigaben*, um eine Liste der Freigaben anzuzeigen, die es auf dem ausgewählten Computer gibt.

Wenn Sie Ordner oder Dateien verwalten, können sich Situationen ergeben, in denen keine Benutzer mit einem freigegebenen Ordner verbunden sein sollten. Wenn Sie beispielsweise Dateien an einen anderen Ort verschieben, möchten Sie vermutlich sicherstellen, dass niemand diese Dateien während der Verschiebung verwendet. Eine Möglichkeit herauszufinden, ob jemand mit freigegebenen Ordnern und deren Dateien arbeitet, ist die Untersuchung der Benutzersitzungen und der geöffneten Dateien.

Tabelle 13.4 Spezielle und administrative Freigaben

Freigabename	Beschreibung
<i>C\$, D\$, E\$</i> und andere Freigaben von lokalen Volumes	Eine spezielle Freigabe des Stammverzeichnisses eines Volumes. Die Freigaben der lokalen Laufwerke werden <i>C\$, D\$, E\$</i> und so weiter genannt. Dieses Schema gilt auch für die Freigaben von CD/DVD-ROM-Laufwerken. Diese Freigaben ermöglichen es Mitgliedern der Gruppen <i>Administratoren</i> und <i>Sicherungs-Operatoren</i> , eine Verbindung zum Stammordner eines lokalen Datenträgers herzustellen und Verwaltungsarbeiten durchzuführen. Wenn Sie zum Beispiel eine Zuordnung mit <i>C\$</i> herstellen, haben Sie Vollzugriff auf diesen lokalen Datenträger.
<i>ADMIN\$</i>	Eine administrative Freigabe für den Zugriff auf den Ordner <i>%SystemRoot%</i> , in dem die Betriebssystemdateien liegen. Diese Freigabe ist für die Remoteadministration vorgesehen. Für Administratoren, die remote mit Computern arbeiten, ist <i>ADMIN\$</i> ein bequemer Weg für den Zugriff auf den Betriebssystemordner.
<i>IPC\$</i>	Eine administrative Freigabe für die Unterstützung von benannten Pipes, die Programme zur Interprozesskommunikation verwenden (also für die Kommunikation zwischen verschiedenen Prozessen). Da benannte Pipes über das Netzwerk geleitet werden können und lokale Systeme mit Remotesystemen verbinden können, lassen sie sich auch zur Remoteadministration verwenden.
<i>PRINT\$</i>	Unterstützt die Freigabe von Druckern, indem sie Zugriff auf Druckertreiber bietet. Wenn Sie einen Drucker freigeben, kopiert das System die Druckertreiber in diese Freigabe, damit auch andere Computer bei Bedarf darauf zugreifen können.

Jeder Benutzer, der eine Verbindung mit einem freigegebenen Ordner herstellt, erstellt damit eine Benutzersitzung. Wenn Sie herausfinden möchten, wer gerade verbunden ist, tippen oder klicken Sie in der Konsolenstruktur unter *Freigegebene Ordner* auf *Sitzungen*. Die aktuellen Benutzer werden im rechten Konsolenbereich aufgelistet. Um einen Benutzer von der Freigabe zu trennen und seine Sitzung zu beenden, klicken Sie im rechten Konsolenbereich mit der rechten Maustaste auf einen Sitzungseintrag oder halten ihn gedrückt, wählen *Sitzung schließen* und tippen oder klicken dann auf *Ja*, um den Vorgang zu bestätigen. Um alle Benutzersitzungen zu trennen, klicken Sie in der Konsolenstruktur *Sitzungen* mit der rechten Maustaste an oder halten den Knoten gedrückt, wählen *Alle Sitzungen trennen* und tippen oder klicken dann auf *Ja*, um den Vorgang zu bestätigen.

Jede freigegebene Datei, die gerade benutzt wird, erscheint in der Liste der geöffneten Dateien. Wenn Sie herausfinden möchten, um welche Dateien es sich handelt, tippen oder klicken Sie in der Konsolenstruktur unter *Freigegebene Ordner* auf *Geöffnete Dateien*. Im rechten Konsolenbereich werden die geöffneten Dateien aufgelistet. Um eine geöffnete Datei zu schließen, klicken Sie den betreffenden Eintrag im rechten Konsolenbereich mit der rechten Maustaste an oder halten ihn gedrückt, wählen *Geöffnete Datei schließen* und tippen oder klicken dann auf *Ja*, um den Vorgang zu bestätigen. Um alle geöffneten Dateien zu schließen, klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Knoten *Geöffnete Dateien* oder halten ihn gedrückt, wählen *Alle geöffneten Dateien trennen* und tippen oder klicken dann auf *Ja*, um den Vorgang zu bestätigen.

Problembehebung in der Dateifreigabe

Die meisten Probleme im Bereich der Dateifreigabe können Sie mit folgenden Maßnahmen diagnostizieren und beseitigen:

- **Prüfen Sie die Verbindung zwischen dem Computer, der die Ressourcen freigibt, und dem Computer, dessen Benutzer versucht, auf die freigegebenen Ressourcen zuzugreifen** Beide Computer müssen an das Netzwerk angeschlossen und mit den richtigen TCP/IP-Einstellungen konfiguriert sein. Bei beiden Computern muss die Firewall so eingerichtet sein, dass sie eingehende und ausgehende Verbindungen erlaubt. Auf dem Computer, der Ressourcen freigibt, muss in der Windows-

Firewall die Ausnahme für die Datei- und Druckerfreigabe aktiviert sein. Die Windows-Firewall unterstützt mehrere aktive Profile, und das aktive, angewendete Profil muss richtig konfiguriert sein. Falls Sie Firewallsoftware eines Fremdherstellers verwenden, müssen eingehende Verbindungen auf UDP-Port 137, UDP-Port 138, TCP-Port 139 und allen Ports für ICMPv4 und (sofern für Echo-Anforderungen nötig) ICMPv6 erlaubt sein.

- **Überprüfen Sie die Anmeldeinformationen der Verbindung** Wenn beide Computer Mitglieder einer Domäne sind, sollte der Benutzer die Verbindung zur Freigabe mit Domänenanmeldeinformationen herstellen. Hat sich der Benutzer als lokaler Benutzer statt als Domänenbenutzer an seinem Computer angemeldet, müssen Sie sicherstellen, dass dieser Benutzer für die Verbindung zur Freigabe alternative Anmeldeinformationen verwendet und dass diese alternativen Anmeldeinformationen zu einem geeigneten Benutzerkonto in der richtigen Domäne gehören.
- **Prüfen Sie die erweiterten Freigabeeinstellungen im Netzwerk- und Freigabecenter** Damit Dateien auf einem Windows 8-Desktopcomputer erfolgreich freigegeben werden können, muss die Datei- und Druckerfreigabe für das aktive (aktuelle) Netzwerkprofil eingeschaltet sein. Außerdem darf die Richtlinie *Verhindert, dass Benutzer Dateien innerhalb ihres Profils freigeben* nicht aktiviert sein. Computer können Verbindung zu mehreren Netzwerken gleichzeitig herstellen, und für alle aktiven Netzwerke muss der Netzwerktyp im Netzwerk- und Freigabecenter richtig konfiguriert sein.
- **Prüfen Sie den Netzwerktyp für das aktive Netzwerk** Im Netzwerk- und Freigabecenter muss der Netzwerktyp auf beiden Computern richtig eingestellt sein. Ist der Netzwerktyp als öffentliches Netzwerk konfiguriert, sind viele Freigabe- und Verbindungseinstellungen gesperrt und eingeschränkt.
- **Prüfen Sie die Freigabeberechtigungen, die zugrunde liegenden NTFS-Berechtigungen und die Zugriffsflags von Dateien** Die Freigabeberechtigungen müssen so konfiguriert sein, dass der Benutzer Zugriff erhält. Und die zugrunde liegenden NTFS-Berechtigungen müssen so konfiguriert sein, dass sie dem Benutzer Zugriff gewähren. Zugriffsflags für Dateien müssen gelöscht sein, damit die Dateien nicht als schreibgeschützt, ausgeblendet oder Systemdateien markiert sind.

Bei einer detaillierteren Problembehandlung müssen Sie sich die DNS-Konfiguration auf beiden Computern sowie ihre Domänenmitgliedschaft ansehen. Im Idealfall befinden sich beide Computer im selben Netzwerk oder in Netzwerken, die über schnelle Ethernetverbindungen miteinander verbunden sind. Außerdem sollten beide Computer Mitglieder derselben Domäne sein oder in vertrauenswürdigen Domänen liegen.

Der Serverdienst muss laufen, damit Dateien freigegeben werden können. Prüfen Sie auf dem Computer, der Dateien freigibt, ob der Serverdienst läuft und richtig konfiguriert ist. Normalerweise müsste der Serverdienst für den automatischen Start konfiguriert sein und unter dem Konto *SYSTEM* laufen. Der Serverdienst setzt voraus, dass ein Server-SMB-Treiber verfügbar ist. Ob diese Voraussetzung erfüllt ist, können Sie auf der Registerkarte *Abhängigkeiten* im Eigenschaftendialogfeld des Dienstes prüfen.

Stellen Sie in den Gruppenrichtlinien für den Computer, der Dateien freigibt, sicher, dass der Benutzer das Recht *Auf diesen Computer vom Netzwerk aus zugreifen* besitzt. Dieses Benutzerrecht wird über *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechten* verwaltet. Standardmäßig verfügen alle authentifizierten Benutzer über dieses Benutzerrecht.

In den Gruppenrichtlinien können Sie auch Richtlinien für die Unterstützung nach verweigerten Zugriffen konfigurieren, um Benutzern bei der Suche nach Ansprechpartnern zu helfen, wenn sie Schwierigkeiten mit dem Zugriff auf Dateien haben. Wenn Sie Richtlinien für die Unterstützung nach Zugriffsverweigerungen aktivieren und konfigurieren, können Sie die Fehlermeldungen durch zusätzliche Texte,

durch Verknüpfungen mit Hilfeseiten oder Dokumente und durch eine E-Mail-Adresse ergänzen, über die Hilfe angefordert werden kann.

Aktivieren Sie diese Unterstützung mit der Richtlinie *Unterstützung nach "Zugriff verweigert" auf Client für alle Dateitypen aktivieren*. Wie die Unterstützung funktionieren soll, legen Sie mit *Meldung für Fehler vom Typ "Zugriff verweigert" anpassen* fest. Diese Richtlinien sind in den administrativen Vorlagen der Computerkonfiguration unter *System\Unterstützung nach "Zugriff verweigert"* zu finden.

Verwenden und Konfigurieren der Freigabe öffentlicher Ordner

Sinn einer Freigabe von öffentlichen Ordnern ist es, Benutzern die Freigabe von Dateien und Ordnern an einem zentralen Ort zu ermöglichen. Dadurch sind Benutzer in der Lage, schnell zu überblicken, was sie für andere freigegeben haben. Außerdem können sie die freigegebenen Dateien leichter nach Typen zusammenfassen. Dieser Abschnitt beschreibt, wie die Freigabe in öffentlichen Ordnern funktioniert und wie sie konfiguriert wird.

Verwenden der Freigabe in öffentlichen Ordnern

Wenn Sie die Freigabe im öffentlichen Ordner verwenden, kopieren oder verschieben Sie die Dateien, die Sie freigeben möchten, in den Ordner *Benutzer/Öffentlich* (*%SystemDrive%\Users\Public*) des Computers. Der Ordner *Öffentlich* (*Public*) enthält einige Unterordner, die zur Organisation der freigegebenen Dateien verwendet werden können:

- **Öffentlicher Desktop** Wird für freigegebene Desktopobjekte verwendet.
- **Öffentliche Dokumente, Öffentliche Musik, Öffentliche Bilder, Öffentliche TV-Aufzeichnungen, Öffentliche Videos** Werden für freigegebene Dokument- und Mediendateien benutzt.
- **Öffentliche Downloads** Wird für freigegebene Downloads benutzt.

Alle Inhalte, die in diesen Unterordnern gespeichert werden, sind für alle Benutzer zugänglich, die sich am Computer anmelden (und für alle Remotebenutzer, sofern der Ordner *Öffentlich* für den Netzwerkzugriff freigegeben wurde).

Gewöhnlich greifen Benutzer über das Fenster *Bibliotheken* auf öffentliche Ordner zu. Tippen oder klicken Sie im Datei-Explorer auf die Optionsschaltfläche ganz links in der Adressleiste und tippen oder klicken Sie dann auf *Bibliotheken*. Erweitern Sie den Knoten *Dokumente*, um den Ordner *Öffentliche Dokumente* zu sehen. Nach der Erweiterung des Knotens *Musik* sehen Sie den Ordner *Öffentliche Musik*, unter *Bilder* finden Sie *Öffentliche Bilder* und unter *Videos* liegt der Ordner *Öffentliche Videos*.

Standardmäßig kann jeder, der auf einem Computer über ein Benutzerkonto und das passende Kennwort verfügt, auf den öffentlichen Ordner eines Computers zugreifen. Wenn Sie Dateien in den öffentlichen Ordner kopieren oder verschieben, werden die Zugriffsberechtigungen so angepasst, dass sie zum öffentlichen Ordner passen. Außerdem werden noch einige zusätzliche Berechtigungen vergeben.

Die Standardberechtigungen für den öffentlichen Ordner erlauben den lokalen Computerbenutzern, öffentliche Dateien zu lesen, in ihnen zu schreiben, sie zu ändern oder zu löschen. In den Ordnern *Öffentliche Musik*, *Öffentliche Bilder* und *Öffentliche Videos* erhält *%ComputerName%\Benutzer* die Berechtigungen *Lesen und Ausführen* sowie *Lesen*.

Die Freigabekonfiguration des Ordners *Public* lässt sich auf zweierlei Art und Weise ändern:

- Sie erlauben Benutzern, die über das Netzwerk zugreifen, die Anzeige und das Öffnen von Dateien, aber nicht die Änderung, Erstellung oder Löschung öffentlicher Dateien. Wenn Sie diese Option einstellen, erhält die implizite Gruppe *Jeder* die Berechtigungen *Lesen und Ausführen* und *Lesen* für öffentliche Dateien sowie *Lesen und Ausführen*, *Ordnerinhalt anzeigen* und *Lesen* für öffentliche Ordner.
- Sie erlauben Benutzern, die über das Netzwerk zugreifen, die Anzeige und Verwaltung öffentlicher Dateien. Dadurch können Remotebenutzer öffentliche Dateien öffnen, ändern, erstellen und löschen. Wenn Sie diese Option einstellen, erhält die implizite Gruppe *Jeder* die Berechtigung *Vollzugriff* für öffentliche Dateien und öffentliche Ordner.

Der nächste Abschnitt beschreibt, wie die Freigabe des öffentlichen Ordners konfiguriert wird.

Konfigurieren der Freigabe öffentlicher Ordner

Die Freigabe öffentlicher Ordner erfolgt auf Computerbasis. Für den Ordner *Öffentlich (Public)* und seine Unterordner werden dieselben Einstellungen verwendet. Sie können die öffentlichen Ordner mit folgenden Schritten freigeben:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Heimnetzgruppen- und Freigabeoptionen auswählen* und dann auf die Verknüpfung *Erweiterte Freigabeeinstellungen ändern*.
2. Erweitern Sie das Netzwerkprofil *Alle Netzwerke*. Wählen Sie unter *Freigabe des öffentlichen Ordners* die Freigabeoption, die Sie verwenden möchten. Verfügbar sind folgende Optionen:
 - ***Freigabe einschalten, sodass jeder Benutzer mit Netzwerkzugriff in Dateien in den Ordnern "Öffentlich" lesen und schreiben kann*** Wählen Sie diese Option, um jedem, der über das Netzwerk auf den Computer zugreifen kann, die Berechtigung *Besitzer* für den öffentlichen Ordner und alle öffentlichen Daten zu geben. (Allerdings kann die Windows-Firewall bei entsprechender Einstellung Zugriffe von außen verhindern.)
 - ***"Freigabe des öffentlichen Ordners" deaktivieren*** Wählen Sie diese Option, um Netzwerkzugriffe auf die öffentlichen Ordner zu deaktivieren und Zugriffe auf öffentliche Daten nur für Benutzer zuzulassen, die lokal am Computer angemeldet sind.
3. In privaten Netzwerken verwaltet gewöhnlich Windows die Verbindungen zu anderen Computern aus einer Heimnetzgruppe. Wenn es auf allen Computern dieselben Benutzerkonten mit denselben Kennwörtern gibt, können Sie Windows anweisen, stattdessen Ihr Konto für den Zugriff auf freigegebene Dateien, freigegebene Drucker und öffentliche Ordner zu verwenden. Erweitern Sie das Netzwerkprofil *Privat* und wählen Sie unter *Heimnetzgruppen-Verbindungen* die Option *Benutzerkonten und Kennwörter zum Herstellen von Verbindungen mit anderen Computern verwenden*.
4. Tippen oder klicken Sie auf *Änderungen speichern*, um die Änderungen zu speichern.

Überwachen von Datei- und Ordnerzugriff

Zugriffsberechtigungen helfen zwar dabei, Daten zu schützen, sie lassen aber nicht erkennen, wer unrechtmäßig versucht hat, auf Dateien und Ordner zuzugreifen, oder wer wichtige Dateien versehentlich oder absichtlich gelöscht hat. Um zu verfolgen, wer auf Dateien und Ordner zugreift und was diese Benutzer dabei gemacht haben, müssen Sie die Überwachung für Datei- und Ordnerzugriff konfigurieren. Sie verfolgen den Datei- und Ordnerzugriff, indem Sie die Überwachung aktivieren, festlegen, welche Dateien und Ordner überwacht werden, und dann die Sicherheitsprotokolle analysieren.

Aktivieren der Überwachung für Dateien und Ordner

Sie konfigurieren Überwachungsrichtlinien über Gruppenrichtlinien oder die lokale Sicherheitsrichtlinie. Verwenden Sie Gruppenrichtlinien, wenn Sie Überwachungsrichtlinien im gesamten Unternehmen konfigurieren wollen. Die lokale Sicherheitsrichtlinie eignet sich dagegen besser, wenn Sie Überwachungsrichtlinien auf einem bestimmten Computer einrichten wollen. Denken Sie aber daran, dass die lokale Richtlinie von den Gruppenrichtlinien außer Kraft gesetzt werden kann.

Sie haben mehrere Möglichkeiten, die Überwachung für Dateien und Ordner zu aktivieren:

- Zur Konfiguration der Richtlinien auf einem einzelnen Computer öffnen Sie die Konsole *Lokale Sicherheitsrichtlinie*. Wenn Sie die Anzeige der Verwaltungstools für den Startbildschirm aktiviert haben, finden Sie dort eine entsprechende Kachel. Sie können die Konsole auch öffnen, indem Sie die WINDOWS-Taste drücken, **secpol.msc** eingeben und dann die EINGABETASTE drücken. Erweitern Sie in der Konsole den Knoten *Lokale Richtlinien* und wählen Sie dann *Überwachungsrichtlinie*.
- Eine unternehmensweite Richtlinie konfigurieren Sie, indem Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor öffnen. Erweitern Sie anschließend den Zweig *Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien* und wählen Sie *Überwachungsrichtlinie* aus.

Tippen oder klicken Sie anschließend doppelt auf *Objektzugriffsversuche überwachen*. Daraufhin öffnet sich das Dialogfeld *Eigenschaften von Objektzugriffsversuche überwachen*. Aktivieren Sie unter *Diese Versuche überwachen* das Kontrollkästchen *Erfolgreich*, um erfolgreiche Zugriffsversuche zu protokollieren, das Kontrollkästchen *Fehler*, um fehlgeschlagene Zugriffsversuche zu protokollieren, oder beide Kontrollkästchen. Tippen oder klicken Sie schließlich auf OK. Damit wird die Überwachung aktiviert, aber es ist noch nicht festgelegt, welche Dateien und Ordner überwacht werden.

Konfigurieren und Analysieren der Überwachung

Sobald Sie die Richtlinie *Objektzugriffsversuche überwachen* aktiviert haben, können Sie einstellen, ob und wie der Zugriff auf Ordner und Dateien verfolgt wird. Dazu stellen Sie die Überwachungsstufe für einzelne Ordner und Dateien ein. Denken Sie daran, dass Überwachung nur auf NTFS-Volumes zur Verfügung steht und dass die Vererbungsregeln auch für die Überwachung von Dateien und Ordnern gelten. Sie können daher den Zugriff auf alle Dateien oder Ordner eines Volumes überwachen, indem Sie einfach festlegen, dass Sie den Stammordner des Volumes überwachen.

Gehen Sie folgendermaßen vor, um auszuwählen, welche Dateien und Ordner überwacht werden:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf die Datei oder den Ordner, der überwacht werden soll, oder halten Sie Datei oder Ordner gedrückt, und wählen Sie den Befehl *Eigenschaften*.

2. Tippen oder klicken Sie im Eigenschaftendialogfeld auf die Registerkarte *Sicherheit* und dann auf *Erweitert*.
3. Tippen oder klicken Sie im Dialogfeld *Erweiterte Sicherheitseinstellungen* auf der Registerkarte *Überwachung* auf *Weiter*. Daraufhin öffnet sich eine bearbeitbare Version der Registerkarte *Überwachung* (Abbildung 13.12).

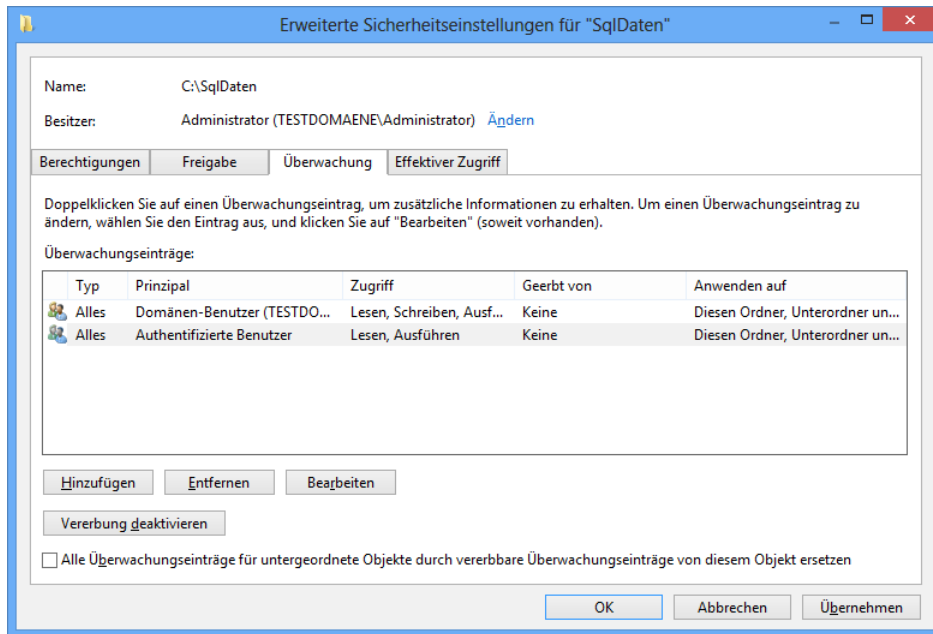


Abbildung 13.12 Konfigurieren der Überwachungseinstellungen

4. Tippen oder klicken Sie auf *Hinzufügen*, um das Dialogfeld *Überwachungseintrag für* zu öffnen. Tippen oder klicken Sie auf *Prinzipal auswählen*, um das Dialogfeld *Benutzer, Computer, Dienstkonto oder Gruppe auswählen* zu öffnen.
5. Geben Sie den Namen eines Benutzer- oder Gruppenkontos ein. Achten Sie darauf, dass Sie nicht den Anzeigenamen, sondern den Kontonamen verwenden. An dieser Stelle darf immer nur ein einzelner Name eingegeben werden.
6. Tippen oder klicken Sie auf *Namen überprüfen*. Liegt für den Eintrag nur eine einzige Übereinstimmung vor, wird das Dialogfeld automatisch aktualisiert und der Eintrag wird unterstrichen. Andernfalls erscheint ein weiteres Dialogfeld. Sind keine Übereinstimmungen vorhanden, haben Sie vermutlich den Namen falsch eingegeben oder Sie suchen an der falschen Stelle. Ändern Sie den Namen und versuchen Sie es noch einmal. Oder tippen oder klicken Sie auf *Pfade*, um einen anderen Ort auszuwählen. Werden mehrere Übereinstimmungen gefunden, wählen Sie im Dialogfeld *Mehrere Namen gefunden* den gewünschten Namen aus und tippen oder klicken auf *OK*.
7. Tippen oder klicken auf *OK*. Der Benutzer oder die Gruppe wird hinzugefügt und das Dialogfeld *Überwachungseintrag für* wird aktualisiert. Standardmäßig werden nur die Grundberechtigungen angezeigt. Tippen oder klicken Sie auf *Erweiterte Berechtigungen anzeigen*, um die speziellen Berechtigungen anzuzeigen (Abbildung 13.13).

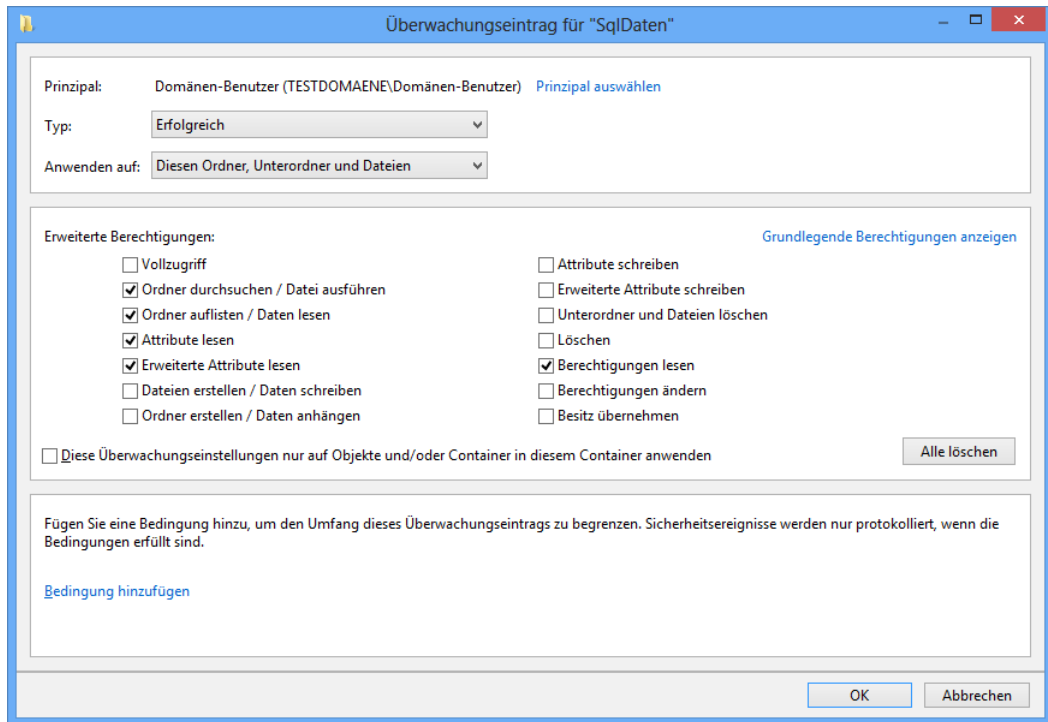


Abbildung 13.13 Festlegen, welche Aktionen für die ausgewählten Benutzer, Gruppen oder Computer überwacht werden

8. Stellen Sie in der Dropdownliste *Anwenden auf* ein, wie der Überwachungseintrag angewendet werden soll. Folgende Einstellungen stehen zur Verfügung:
 - **Nur diesen Ordner** Die Überwachungseinträge gelten nur für den aktuell ausgewählten Ordner.
 - **Diesen Ordner, Unterordner und Dateien** Die Überwachungseinträge gelten für den ausgewählten Ordner, seine Unterordner und alle Dateien in diesen Ordnern.
 - **Diesen Ordner, Unterordner** Die Überwachungseinträge gelten nur für den ausgewählten Ordner und seine Unterordner. Sie gelten nicht für Dateien in diesen Ordnern.
 - **Diesen Ordner, Dateien** Die Überwachungseinträge gelten für den gewählten Ordner und die Dateien, die in ihm liegen. Sie gelten nicht für Unterordner dieses Ordners.
 - **Nur Unterordner und Dateien** Die Überwachungseinträge gelten für die Unterordner des gewählten Ordners und für die Dateien, die in ihnen liegen. Sie gelten nicht für den gewählten Ordner.
 - **Nur Unterordner** Die Überwachungseinträge gelten für die Unterordner des gewählten Ordners, aber nicht für den gewählten Ordner oder für die Dateien in diesen Ordnern.
 - **Nur Dateien** Die Überwachungseinträge gelten für alle Dateien im gewählten Ordner und in seinen Unterordnern. Sie gelten nicht für den gewählten Ordner selbst oder für seine Unterordner.
9. Wählen Sie in der *Typ*-Liste aus, ob Sie die Überwachung von erfolgreichen oder fehlgeschlagenen Zugriffen konfigurieren, oder beides. Legen Sie dann fest, welche Ereignisse überwacht werden sollen. Die Ereignisse werden durch dieselben speziellen Berechtigungen angegeben, die in diesem Kapitel bereits in den Tabellen 13.1 und 13.3 beschrieben wurden.

10. Wenn Sie mit einem Ordner arbeiten und die Überwachungseinträge für alle untergeordneten Objekte dieses Ordners ersetzen möchten (aber nicht für den Ordner selbst), wählen Sie *Diese Überwachungseinträge nur auf Objekte und/oder Container in diesem Container anwenden*.

PRAXISTIPP

Mit der Option *Anwenden auf* legen Sie die Orte oder Objekte fest, die überwacht werden sollen. Die Einstellung *Diese Überwachungseinträge nur auf Objekte und/oder Container in diesem Container anwenden* steuert, wie die Überwachungseinstellungen angewendet werden. Wenn dieses Kontrollkästchen gewählt ist, ersetzen die Überwachungseinstellungen des übergeordneten Objekts die Einstellungen in den untergeordneten Objekten. Wenn diese Option gelöscht ist, werden die Überwachungseinstellungen des übergeordneten Objekts mit den vorhandenen Einstellungen der untergeordneten Objekte zusammengeführt.

11. Wenn Sie eine anspruchsbasierte Authentifizierung verwenden und den Bereich eines Überwachungseintrags beschränken möchten, können Sie entsprechende Bedingungen zum Überwachungseintrag hinzufügen. Sind beispielsweise alle Firmencomputer Mitglieder der Gruppe *Domänencomputer*, möchten Sie vielleicht die Zugriffe genauer überwachen, die durch Geräte erfolgen, die nicht zu dieser Gruppe gehören.
12. Wenn Sie mit den Einstellungen fertig sind, tippen oder klicken Sie auf *OK*. Wiederholen Sie diesen Vorgang nach Bedarf zur Überwachung von anderen Benutzern, Gruppen oder Computern.

Oft ist es nützlich, ausschließlich fehlgeschlagene Aktionen zu überwachen. Auf diese Weise erfahren Sie, wenn jemand versucht hat, eine Aktion auszuführen, die ihm aber nicht gelungen ist. Denken Sie daran, dass ein fehlgeschlagener Zugriff nicht zwangsläufig bedeutet, dass jemand versucht, in eine Datei oder einen Ordner einzubrechen. Möglicherweise hat ein Benutzer lediglich doppelt auf einen Ordner oder eine Datei geklickt oder getippt, auf die er keinen Zugriff hat. Außerdem werden bei einem Fehlschlag bestimmter Aktionen gleich mehrere Fehlversuche protokolliert, obwohl der Benutzer nur einmal versucht hat, die Aktion auszuführen. Unabhängig davon sollten Sie eine Serie mehrerer fehlgeschlagener Versuche immer genauer untersuchen, weil die Möglichkeit besteht, dass jemand probiert, in einen Computer einzubrechen.

Jedes Mal, wenn auf Dateien und Ordner zugegriffen wird, für die Sie die Überwachung konfiguriert haben, wird die Aktion in das Sicherheitsprotokoll des Systems geschrieben. Dieses Protokoll können Sie sich in der Ereignisanzeige ansehen. Bei erfolgreichen Aktionen, beispielsweise erfolgreichen Lesezugriffen auf eine Datei, werden Erfolgsereignisse aufgezeichnet. Schlägt eine Aktion dagegen fehl, etwa weil eine Datei nicht gelöscht werden kann, werden Fehlerereignisse aufgezeichnet. Um erweiterte Überwachungsrichtlinien zu konfigurieren, öffnen Sie ein Gruppenrichtlinienobjekt zur Bearbeitung im *Gruppenrichtlinienverwaltungs-Editor*. Erweitern Sie dann in der Computerkonfiguration *Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration*. Erweitern Sie außerdem den Knoten *Überwachungsrichtlinien*. Dann finden Sie mehrere Knoten für die Konfiguration von Richtlinien vor:

- *Kontoanmeldung*
- *Kontoverwaltung*
- *Detaillierte Überwachung*
- *DS-Zugriff*
- *Anmelden/Abmelden*
- *Objektzugriff*
- *Richtlinienänderung*

- *Berechtigungen*
- *System*
- *Globale Objektüberwachung*

Wählen Sie in der Strukturansicht die Kategorie aus, die Sie bearbeiten möchten, beispielsweise *Kontoanmeldung*. Dann erscheinen die verfügbaren Unterkategorien auf der rechten Seite des Fensters. Tippen oder klicken Sie die Unterkategorie, die Sie bearbeiten möchten, doppelt an, beispielsweise *Überprüfen der Anmeldeinformationen überwachen*. Wählen Sie im dazugehörigen Eigenschaftendialogfeld *Folgende Überwachungsereignisse konfigurieren*. Wählen Sie anschließend *Erfolg*, *Fehler* oder beides, um die Art der überwachten Ereignisse festzulegen, und tippen oder klicken Sie auf *OK*. Dadurch wird die Überwachung der betreffenden Unterkategorie aktiviert.

Kapitel 14

Verwalten von Datenzugriff und Verfügbarkeit

In diesem Kapitel:

Konfigurieren von Datei-Explorer-Optionen	538
Verwalten von Offlinedateien	544
Konfigurieren von Datenträgerkontingenten	555
Verwenden von BranchCache	563

Die Verwaltung von Datenzugriff und Verfügbarkeit ist eine zentrale Aufgabe bei der Benutzer- und Systemadministration. Neben der üblichen Datei- und Ordnerverwaltung gehören die Einstellung der Optionen des Microsoft Datei-Explorers, die Verwaltung der Offlinedateieinstellungen, die Vergabe von Datenträgerkontingenten und die Konfiguration von »Zwischenspeichern für Zweigstellen« (Branch-Caches) zu den Arbeiten, die häufiger anfallen. Von den Datei-Explorer-Optionen hängt es ab, welche Funktionen zur Datei- und Ordnerverwaltung und welche Dateitypen verfügbar sind. Die Offlinedateieinstellungen kontrollieren die Verfügbarkeit von Dateien und Ordnern, wenn Benutzer offline arbeiten. Datenträgerkontingente begrenzen den Speicherplatz, der Benutzern auf den Datenträgern zur Verfügung steht. Und BranchCache speichert heruntergeladene Dokumente und Dateien lokal, damit sie schneller abgerufen werden können.

Konfigurieren von Datei-Explorer-Optionen

Wenn Sie etwas darüber nachdenken, werden Sie wahrscheinlich feststellen, dass Sie bei Ihrer Arbeit am Computer einen großen Teil der Zeit damit verbringen, Dateien und Ordner zu verwalten. Sie erstellen Dateien und Ordner, in denen Informationen gespeichert und organisiert werden. Sie verschieben die Dateien und Ordner von einem Speicherort an einen anderen. Sie stellen die Datei- und Ordneigenschaften ein und so weiter. Von der vielen Zeit und dem Aufwand mit der Arbeit an Dateien und Ordnern ersparen Sie sich einen Teil, wenn Sie einige simple Techniken für die effektive Verwaltung beherzigen.

Anpassen des Datei-Explorers

Der Datei-Explorer ist das Werkzeug der Wahl, wenn es um die Arbeit mit Dateien und Ordnern geht. Leider sind seine Standardeinstellungen für den Durchschnittsnutzer konfiguriert und nicht für erfahrene Benutzer oder gar Administratoren. Beispielsweise wollen Sie als Administrator oft die Dateinamenserweiterungen und ausgeblendete Dateitypen sehen. In der Standardeinstellung zeigt der Datei-Explorer keine ausgeblendeten Dateitypen und keine Dateinamenserweiterungen.

In Windows 8 lassen sich die entsprechenden Optionen leicht im Menüband *Ansicht* aktivieren. Tippen oder klicken Sie im Datei-Explorer auf *Ansicht*, um das Menüband zu öffnen. Aktivieren Sie dann *Ausgeblendete Elemente*, damit auch ausgeblendete Dateien und Ordner angezeigt werden (aber keine geschützten Systemdateien). Aktivieren Sie dann *Dateinamenerweiterungen*, damit die Erweiterungen der Dateinamen angezeigt werden.

Und so ändern Sie die anderen Standardeinstellungen:

1. Tippen oder klicken Sie im Menüband *Ansicht* des Datei-Explorers auf *Optionen*. Dadurch öffnet sich das Dialogfeld *Ordneroptionen* mit vorgewählter Registerkarte *Allgemein*.
2. Wählen Sie die Registerkarte *Ansicht*, damit die erweiterten Einstellungen für den Datei-Explorer angezeigt werden (Abbildung 14.1).
3. Nun können Sie Einstellungen für den Datei-Explorer vornehmen. Es stehen folgende Optionen zur Wahl:
 - **Bei der Eingabe in der Listenansicht** Wenn Sie in der Listenansicht arbeiten und eine Buchstaben-taste drücken, wählt der Datei-Explorer standardmäßig die erste Datei oder den ersten Ordner aus, dessen Name mit diesem Buchstaben beginnt. Wählen Sie die Option *Automatisch in Suchfeld eingeben* aus, wenn Sie möchten, dass der eingetippte Text stattdessen in das Suchfeld eingetragen wird.

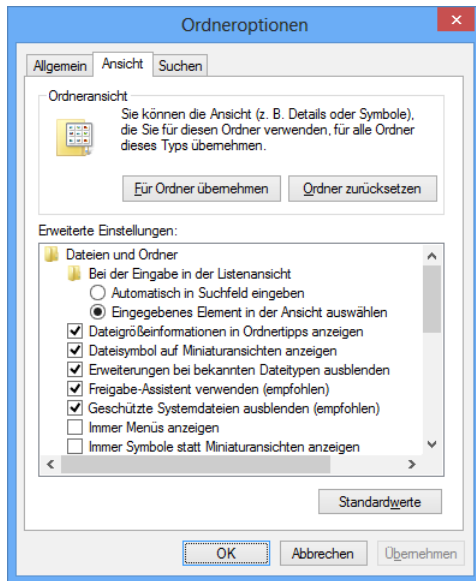


Abbildung 14.1 Einstellen der Optionen des Datei-Explorers im Dialogfeld *Ordneroptionen*

- ***Dateigrößinformationen in Ordnerinfos anzeigen*** Wenn Sie den Mauszeiger über einen Ordernamen oder ein Ordnersymbol bewegen, zeigt der Datei-Explorer standardmäßig ein Quick-Info an, in dem Datum und Uhrzeit der Erstellung, Größe des Ordners und eine abgekürzte Liste der Dateien aufgelistet sind. Deaktivieren Sie diese Option, wenn weniger Informationen angezeigt werden sollen (nur Datum und Uhrzeit der Erstellung).
- ***Dateisymbol auf Miniaturansichten anzeigen*** In der Standardeinstellung fügt der Datei-Explorer Dateisymbole zu den angezeigten Vorschaubildern hinzu. Deaktivieren Sie diese Option, wenn Sie Vorschaubilder ohne Dateisymbole sehen wollen.
- ***Erweiterungen bei bekannten Dateitypen ausblenden*** In der Standardeinstellung zeigt der Datei-Explorer für bekannte Dateitypen keine Dateierweiterungen an. Deaktivieren Sie diese Option, wenn Sie Dateierweiterungen für alle Dateitypen anzeigen möchten. (Diese Option lässt sich auch mit dem Kontrollkästchen *Dateinamenerweiterungen* im Menüband *Ansicht* ändern).
- ***Freigabe-Assistent verwenden*** In der Standardeinstellung benutzt der Datei-Explorer den Dateifreigabe-Assistenten, um Dateifreigaben zu konfigurieren, wie in Kapitel 13, »Verwalten der Dateisicherheit und Ressourcenfreigabe«, beschrieben. Deaktivieren Sie diese Option, wenn Sie lieber die erweiterte Dateifreigabe verwenden. Wenn Sie Dateien freigeben, müssen Sie auf der Registerkarte *Freigabe* auf *Erweiterte Freigabe* tippen oder klicken, um Berechtigungen, Zwischenspeicherung und Verbindungseinstellungen separat zu konfigurieren.
- ***Geschützte Systemdateien ausblenden*** Der Datei-Explorer zeigt standardmäßig keine Betriebssystemdateien an. Deaktivieren Sie diese Option, um auch Betriebssystemdateien aufzulisten.
- ***Immer Symbole statt Miniaturansichten anzeigen*** In der Standardeinstellung zeigt der Datei-Explorer für Bilder und andere Dateitypen große Vorschaubilder des tatsächlichen Inhalts. In Ordnern, die viele Bilder enthalten, kann dies sehr lästig werden, weil der Datei-Explorer für jedes einzelne Bild eine Vorschau berechnen muss. Wählen Sie diese Option, damit die Vorschaubilder deaktiviert sind, solange Sie nicht explizit die Darstellung von Vorschaubildern auswählen.

- **Konflikte bei der Ordnerzusammenführung ausblenden** Standardmäßig zeigt der Datei-Explorer keine Informationen über Konflikte an, die sich bei der Zusammenführung von Ordnern ergeben. Deaktivieren Sie diese Option, damit Informationen über Konflikte bei der Ordnerzusammenführung angezeigt werden.
- **Kontrollkästchen zur Auswahl von Elementen verwenden** Sie können im Datei-Explorer Dateien, Ordner und andere Elemente standardmäßig nur mit den üblichen Techniken auswählen, etwa durch Anklicken, Anklicken bei gedrückter UMSCHALT-Taste und Anklicken bei gedrückter STRG-Taste. Aktivieren Sie diese Option, wenn der Datei-Explorer Kontrollkästchen anzeigen soll, mit denen Sie mehrere Dateien und Ordner auswählen können.
- **Laufwerkbuchstaben anzeigen** In der Standardeinstellung zeigt der Datei-Explorer in den Informationen der Adressleiste den Laufwerkbuchstaben an. Deaktivieren Sie diese Option, wenn Sie keine Laufwerkbuchstaben angezeigt bekommen möchten.
- **Leere Laufwerke im Ordner "Computer" ausblenden** Standardmäßig zeigt der Datei-Explorer im Fenster *Computer* keine Informationen über leere Laufwerke an. Deaktivieren Sie diese Option, wenn Sie auch Informationen über leere Laufwerke auflisten wollen.
- **Ordnerfenster in einem eigenen Prozess starten** In der Standardeinstellung führt Windows alle Instanzen des Datei-Explorers im selben Prozess aus. Das spart Arbeitsspeicher, und im Allgemeinen werden neue Fenster dann schneller geöffnet, aber es bedeutet auch, dass alle Instanzen des Datei-Explorers voneinander abhängen. Stürzt eine Instanz ab, stürzen sie alle ab. Und wenn eine Instanz im Wartezustand festhängt, werden unter Umständen alle Instanzen blockiert. Aktivieren Sie diese Option, wenn Sie dieses Verhalten ändern möchten, damit Windows für jede Instanz des Datei-Explorers einen eigenen Prozess startet.
- **Popupinformation für Elemente in Ordnern und auf dem Desktop anzeigen** In der Standardeinstellung zeigt der Datei-Explorer QuickInfos mit zusätzlichen Informationen über eine Datei oder einen Ordner an, wenn Sie die Maus über die Datei oder den Ordner ziehen. Deaktivieren Sie diese Option, wenn keine QuickInfos erscheinen sollen.
- **Statusleiste anzeigen** Der Datei-Explorer zeigt standardmäßig eine Statusleiste an. Wenn er diese Statusleiste nicht zeigen soll, deaktivieren Sie diese Option.
- **Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen** Der Datei-Explorer listet verschlüsselte und komprimierte Dateien standardmäßig in anderer Farbe auf als normale Dateien. Verschlüsselte Dateien werden mit grüner Schrift angezeigt, komprimierte Dateien mit blauer Schrift. Deaktivieren Sie diese Option, wenn Sie keine unterschiedlichen Farben verwenden wollen.
- **Versteckte Dateien und Ordner** In der Standardeinstellung zeigt der Datei-Explorer keine ausgeblendeten Dateien, Ordner oder Laufwerke an. Wählen Sie die Option *Ausgeblendete Dateien, Ordner und Laufwerke anzeigen*, wenn Sie diese Elemente anzeigen möchten. (Diese Option lässt sich auch mit dem Kontrollkästchen *Ausgeblendete Elemente* im Menüband *Ansicht* ändern.)
- **Vollständigen Pfad in der Titelleiste anzeigen** Wenn Sie ALT+TABULATOR-TASTE drücken und die ALT-Taste gedrückt halten, zeigt Windows standardmäßig eine Vorschau aller offenen Fenster an, in der man mit der TABULATOR-TASTE oder mit der Maus das gewünschte Fenster auswählen kann. Standardmäßig zeigt Windows dabei für das Fenster des Datei-Explorers den Namen des aktuellen Ordners an. Wählen Sie diese Option, wenn stattdessen der vollständige Pfad angezeigt werden soll.

- **Vorherige Ordnerfenster bei der Anmeldung wiederherstellen** Wenn sich der Benutzer abmeldet, kann der Datei-Explorer speichern, welche Ordner geöffnet sind, und diese Ordner bei der nächsten Anmeldung des Benutzers automatisch wieder öffnen. Diese Funktion ist standardmäßig deaktiviert. Wählen Sie diese Option, um sie zu aktivieren.
- **Vorschauhandler im Vorschaufenster anzeigen** Wenn der Fensterabschnitt mit der Vorschauansicht sichtbar ist, zeigt der Datei-Explorer standardmäßig Vorschaubilder der ausgewählten Dateien und Ordner an. Deaktivieren Sie diese Option, wenn Sie keine Vorschaubilder sehen wollen.

Konfigurieren erweiterter Datei-Explorer-Optionen

Benutzer und Administratoren arbeiten häufig mit dem Datei-Explorer oder einer ähnlichen Darstellung, beispielsweise in der Computerkonsole. Als Administrator werden Sie sich gelegentlich wünschen, mehr mit dem Datei-Explorer tun zu können. Vielleicht haben Sie Folgendes vor:

- Computer bereitstellen, bei denen bestimmte Datei-Explorer-Funktionen gesperrt sind. Vielleicht möchten Sie verhindern, dass Benutzer die Registerkarte *Hardware* verwenden können, damit sie nicht die Hardware des Computers untersuchen und Einstellungen verändern können.
- Zugriff auf lokale Datenträger einschränken oder sperren. Vielleicht möchten Sie verhindern, dass Benutzer auf den Computern, die Sie bereitstellen, die CD/DVD-Brennfunktionen verwenden.

Solche und andere erweiterte Konfigurationsoptionen werden in diesem Abschnitt besprochen.

Einstellen von Gruppenrichtlinien für den Datei-Explorer und Ordneransichten

Wie so viele Windows 8-Funktionen lassen sich auch die Optionen, die im Datei-Explorer verfügbar sind, mit Gruppenrichtlinien kontrollieren. Da viele dieser Optionen Ordneransichten und Einstellungen erweitern, lohnt es sich, sie näher zu untersuchen. Tabelle 14.1 gibt Ihnen einen Überblick über Richtlinien, die Sie vielleicht verwenden möchten, und beschreibt ihre Anwendung. Zu finden sind die Richtlinien unter *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\Windows-Komponenten\Datei-Explorer*.

Wie aus Tabelle 14.1 hervorgeht, steuern viele Datei-Explorer-Richtlinien die Verfügbarkeit von bestimmten Optionen, beispielsweise von Menüelementen oder Registerkarten in Dialogfeldern. Um diese Optionen für alle Benutzer eines Computers zu konfigurieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie im Gruppenrichtlinienverwaltungs-Editor ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten. Die Richtlinien befinden sich im Zweig *Benutzerkonfiguration\Richtlinien\Administrative Vorlagen\Windows-Komponenten\Datei-Explorer*.

Tabelle 14.1 Richtlinien für den Datei-Explorer

Richtlinienname	Beschreibung
<i>Anzeige von Miniaturansichten deaktivieren und nur Symbole anzeigen</i>	Deaktiviert die Erstellung und Anzeige von Vorschaubildern, wenn Benutzer auf Ordner des lokalen Computers zugreifen. Das kann die Wartezeit verringern und den ersten Zugriff auf einen Ordner für den Benutzer beschleunigen. Allerdings muss der Benutzer sich Mediendateien dann unter Umständen ansehen, um sie unterscheiden zu können.
<i>Anzeige von Miniaturansichten deaktivieren und nur Symbole für Netzwerkordner anzeigen</i>	Deaktiviert die Erstellung und Anzeige von Vorschaubildern, wenn Benutzer auf Netzwerkordner zugreifen. Das kann die Wartezeit verringern und den ersten Zugriff auf einen Ordner für den Benutzer beschleunigen. Allerdings muss der Benutzer sich Mediendateien dann unter Umständen ansehen, um sie unterscheiden zu können. ►

Richtlinienname	Beschreibung
<i>Bestätigungsdialog beim Löschen von Dateien anzeigen</i>	Zeigt ein Bestätigungsdialogfeld an, wenn Sie Dateien löschen oder in den Papierkorb werfen.
<i>CD-Brennfunktionen entfernen</i>	Entfernt die Funktionen zur Änderung und Erstellung von CDs aus dem Datei-Explorer. Benutzer werden aber nicht daran gehindert, andere CD-Brennprogramme zu verwenden.
<i>Datei-Explorer mit minimiertem Menüband starten</i>	Steuert, ob der Datei-Explorer das Menüband vollständig anzeigt oder minimiert. Sie können festlegen, ob die Einstellung für das erste Öffnen oder für alle neuen Datei-Explorer-Fenster gilt.
<i>Den Menüeintrag "Verwalten" im Datei-Explorer-Kontextmenü ausblenden</i>	Entfernt den Menüeintrag <i>Verwalten</i> aus dem Startbildschirm und aus den Kontextmenüs der Datei-Explorer-Ansichten. Dieser Menüpunkt dient zum Öffnen der Computerverwaltung.
<i>Diese angegebenen Datenträger im Fenster "Arbeitsplatz" ausblenden</i>	Entfernt die Symbole für ausgewählte Laufwerke aus den Datei-Explorer-Ansichten. Benutzer können aber mit anderen Methoden noch auf Laufwerke zugreifen.
<i>Menü "Datei" aus Datei-Explorer entfernen</i>	Entfernt das <i>Datei</i> -Menü aus den Datei-Explorer-Ansichten, hindert Benutzer aber nicht daran, auf andere Weise die Arbeiten durchzuführen, die mit dem <i>Datei</i> -Menü möglich sind.
<i>Nur benutzerbezogene oder zugelassene Shellerweiterungen zulassen</i>	Shellerweiterungen erweitern die Funktionen, die im Datei-Explorer verfügbar sind. Diese Einstellung erlaubt einem Computer nur die Verwendung von Shellerweiterungen, die zuvor von einem Administrator genehmigt wurden oder die keinen Einfluss auf andere Benutzer des Computers haben. Genehmigte Shellerweiterungen müssen unter <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved</code> in der Registrierung eingetragen werden.
<i>Optionen "Netzlaufwerk verbinden" und "Netzlaufwerk trennen" entfernen</i>	Verhindert, dass Benutzer den Datei-Explorer dazu verwenden, um Netzlaufwerke zu verbinden oder zu trennen. Das hindert sie nicht daran, es auf anderen Wegen zu tun, beispielsweise in einer Eingabeaufforderung.
<i>Registerkarte "DFS" entfernen</i>	Entfernt die Registerkarte <i>DFS</i> aus dem Datei-Explorer und den Datei-Explorer-Ansichten. Benutzer können diese Registerkarte nicht mehr verwenden, um DSF-Einstellungen (Distributed File System) anzuzeigen oder zu ändern. Beachten Sie bitte, dass die <i>DFS</i> -Registerkarte nur verfügbar ist, wenn in der Arbeitsgruppe oder Domäne DFS konfiguriert ist.
<i>Registerkarte "Hardware" entfernen</i>	Entfernt die Registerkarte <i>Hardware</i> aus allen Dialogfeldern und verhindert, dass Benutzer diese Registerkarte zur Anzeige oder Änderung von Hardwareeinstellungen oder zur Fehlersuche in Hardwaregeräten verwenden.
<i>Registerkarte "Sicherheit" entfernen</i>	Entfernt die Registerkarte <i>Sicherheit</i> aus den <i>Eigenschaften</i> -Dialogfeldern von Dateien, Ordnern, Verknüpfungen und Laufwerken. Dadurch werden Benutzer daran gehindert, die entsprechenden Datei- und Ordnerberechtigungen anzuzeigen oder zu ändern.
<i>Standardkontextmenü aus Datei-Explorer entfernen</i>	Entfernt die Kontextmenüs vom Desktop und Datei-Explorer, damit Benutzer sie nicht mehr mit einem Klick mit der rechten Maustaste oder durch Gedrückthalten anzeigen können.
<i>Windows-Bibliotheksfeatures deaktivieren, die indizierte Dateidaten verwenden</i>	Deaktiviert alle zusammenfassenden Ansichten außer <i>Nach Ordner</i> sowie alle Suchfiltervorschläge außer Änderungsdatum und Größe. Deaktiviert außerdem die Ansicht von Dateiinhaltsausschnitten im Inhaltsmodus und schließt Bibliotheken aus <i>Start</i> -Suchen aus.
<i>Zugriff auf Laufwerke vom Arbeitsplatz nicht zulassen</i>	Verhindert, dass Benutzer in Datei-Explorer-Ansichten auf ausgewählte Laufwerke zugreifen. Benutzer können auch nicht über die Dialogfelder <i>Ausführen</i> oder <i>Netzlaufwerk verbinden</i> auf Dateien zugreifen, die auf diesen Laufwerken liegen.
<i>Zwischenspeicherung von Bildern in Miniaturansicht deaktivieren</i>	Deaktiviert die Zwischenspeicherung von Vorschaubildern.

2. Tippen oder klicken Sie doppelt auf die Richtlinie, die Sie einstellen möchten. Dadurch öffnet sich ein *Eigenschaften*-Dialogfeld. Wählen Sie eine der folgenden Optionen:
 - **Nicht konfiguriert** Gibt an, dass für diese Richtlinie keine Änderungen an der Registrierung vorgenommen werden.
 - **Aktiviert** Aktiviert die Richtlinie und aktualisiert die Registrierung.
 - **Deaktiviert** Deaktiviert die Richtlinie und aktualisiert die Registrierung.
3. Tippen oder klicken Sie auf **OK**.

HINWEIS In den weiteren Abschnitten dieses Kapitels finden Sie eine ausführlichere Beschreibung einiger dieser Richtlinien. Lesen Sie insbesondere den nächsten Abschnitt, »Verwalten des Laufwerkszugriffs im Datei-Explorer«, der die gezielte Deaktivierung oder Sperrung des Laufwerkszugriffs im Datei-Explorer beschreibt.

Verwalten des Laufwerkszugriffs im Datei-Explorer

Vielleicht möchten Sie den Zugriff auf Dateien sperren, die auf bestimmten Laufwerken liegen, oder sogar bestimmte Laufwerke des Systems verbergen. Das erreichen Sie durch entsprechende Gruppenrichtlinien. Die Richtlinien, die Sie dafür brauchen, sind *Diese angegebenen Datenträger im Fenster "Arbeitsplatz" ausblenden* und *Zugriff auf Laufwerke vom Arbeitsplatz nicht zulassen*.

Das Verbergen oder Ausblenden von Laufwerken hindert Benutzer zwar daran, die Laufwerke im Datei-Explorer-Ansichten zu verwenden, aber es hält sie nicht davon ab, auf anderen Wegen auf die Laufwerke zuzugreifen. Im Gegensatz dazu hält das Sperren oder Blockieren von Laufwerken Benutzer vom Zugriff auf die Dateien ab, die auf den Laufwerken liegen, und sorgt auch dafür, dass diese Dateien nicht über Datei-Explorer, *Ausführen* oder *Netzlaufwerk verbinden* zugänglich sind. Allerdings werden dadurch nicht die Laufwerkssymbole oder Ordnerstrukturen im Datei-Explorer ausgeblendet.

Um ausgewählte Laufwerke zu verbergen oder den Dateizugriff auf ausgewählten Laufwerken zu verhindern, gehen Sie folgendermaßen vor:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Die Richtlinien befinden sich im Zweig *Benutzerkonfiguration\ Richtlinien\ Administrative Vorlagen\ Windows-Komponenten\ Datei-Explorer*.
2. Um Laufwerke zu verbergen, tippen oder klicken Sie *Diese angegebenen Datenträger im Fenster "Arbeitsplatz" ausblenden* doppelt an und wählen dann **Aktiviert**. Anschließend geben Sie die Laufwerke an, die Sie verbergen möchten, und tippen oder klicken dann auf **OK**. Die wichtigsten Optionen sind:
 - Wählen Sie *Alle Laufwerke einschränken*, um den Zugriff auf alle internen Festplattenlaufwerke und Diskettenlaufwerke einzuschränken.
 - Wählen Sie *Nur Laufwerke A und B beschränken*, um den Zugriff auf Diskettenlaufwerke zu beschränken.
 - Wählen Sie *Nur Laufwerke A, B und C beschränken*, um den Zugriff auf Diskettenlaufwerke und Laufwerk C: zu beschränken.
 - Wählen Sie *Nur Laufwerk C beschränken*, um den Zugriff auf Laufwerk C: zu beschränken.
 - Wählen Sie *Nur Laufwerk D beschränken*, um den Zugriff auf Laufwerk D: zu beschränken.
 - Wählen Sie *Laufwerke nicht einschränken*, um zusätzliche Beschränkungen aufzuheben, die sonst gelten würden.

3. Um auf bestimmten Laufwerken den Dateizugriff zu sperren, tippen oder klicken Sie *Zugriff auf Laufwerke vom Arbeitsplatz nicht zulassen* doppelt an und wählen *Aktiviert*. Dann wählen Sie die Laufwerke aus, auf denen Sie den Zugriff sperren möchten, und tippen oder klicken auf OK.

HINWEIS

Von der Berechtigung *Ordnerinhalt anzeigen* hängt es ab, ob ein Benutzer die Dateien sehen kann, die in einem Ordner liegen. Wenn Sie sicherstellen möchten, dass Benutzer nicht die Namen der Ordner anzeigen können, die auf einem Laufwerk liegen, sollten Sie diese Laufwerke zusätzlich verbergen. Das ist die einfachste Methode, die Anzeige der Ordner eines Laufwerks zu verhindern.

Verwalten von Offlinedateien

Die Konfiguration von Offlinedateien ist ein Vorgang, für den mehrere Schritte erforderlich sind. Er beginnt mit der Einstellung der entsprechenden Gruppenrichtlinien, setzt sich mit der Einstellung der betreffenden Offlineordner fort und endet mit der Einstellung der Benutzeroptionen für die Offlinearbeit. In erster Linie sind es zwar die Laptopbenutzer, weil sie ihre Laptops nach Hause oder anderswohin mitnehmen, aber von der Offlinedateieinstellung können alle Benutzer profitieren. Die Einstellung der Gruppenrichtlinien für Offlinedateien wurde in Kapitel 5, »Konfigurieren von Benutzer- und Computer-richtlinien«, besprochen. Dieser Abschnitt geht näher auf Offlinedateien und ihre Konfiguration ein.

Grundlagen der Offlinedateien

Offlinedateien sind Netzwerkdateien, die auf den Computern der Benutzer zwischengespeichert werden, damit sie auch dann verfügbar sind, wenn die Benutzer nicht mit dem Netzwerk verbunden sind oder das Netzwerk ausgefallen ist. Einmal konfiguriert, greift Windows 8 automatisch auf Offlinedateien zurück, wenn die Netzwerkdateien nicht verfügbar sind. Dadurch sind Benutzer in der Lage, ihre Arbeit mit den Netzwerkdateien ohne Unterbrechung fortzusetzen. Sobald die Verbindung mit dem Netzwerk wiederhergestellt ist, synchronisiert Windows 8 automatisch die Dateien vom Computer des Benutzers mit den Dateien im Netzwerkordner.

Welche Änderungen übernommen werden, hängt davon ab, wie die Änderungen erfolgt sind. Wenn mehrere Benutzer eine bestimmte Offlinedatei geändert haben, können sie die Konfliktauflösungsfunktionen verwenden, um die vorhandene Version mit ihrer Dateiversion zu überschreiben, die vorhandene Dateiversion zu bewahren oder beide Versionen im Netzwerk zu speichern. Wenn ein Benutzer eine Offlinedatei löscht, wird die Datei auch im Netzwerk gelöscht, es sei denn, jemand anders hat inzwischen die Netzwerkdatei geändert, sodass sie einen aktuelleren Zeitstempel trägt. In diesem seltenen Fall wird die Datei vom Computer des Benutzers gelöscht, und nicht vom Netzwerk. Ändert ein Benutzer eine Offlinedatei, die jemand anders im Netzwerk löscht, können die Benutzer entscheiden, ob sie ihre Version im Netzwerk speichern oder von ihren Computern löschen.

Windows 8 bietet einige wichtige Funktionen für Offlinedateien:

- **Beschränkung der Synchronisierung auf Änderungen** Windows 8 ermöglicht eine schnellere Synchronisierung, indem es nur die geänderten Blöcke einer Datei synchronisiert.
- **Ghosting von nicht verfügbaren Dateien und Ordnern** Wenn der Inhalt eines Ordners nur teilweise offline verfügbar ist, erstellt Windows 8 für die anderen Dateien und Ordner Platzhalter (»ghosted entries«), um den Onlinekontext zu bewahren. Wenn Sie keine Verbindung zum betreffenden Ordner haben, sehen Sie also nicht nur die normalen Einträge für Offlinedateien und Ordner, sondern auch die Platzhalter.

- **Abgeladene Datenübertragung** Werden Daten innerhalb von kompatiblen Speicherarrays oder zwischen solchen Massenspeichern kopiert oder verschoben, überträgt Windows Server 2012 diese Dateiübertragung transparent und automatisch auf die Speichergeräte. Die Hostcomputer sind an der Datenübertragung dann nicht mehr beteiligt. Kopiert oder verschiebt ein Benutzer zum Beispiel einen Ordner aus einem freigegebenen Ordner von einem Dateiserver auf einen anderen und die Server verwenden kompatible Speicherarrays (dasselbe Speicherarray), werden die Daten direkt übertragen. Die Übertragung erfolgt nicht über die Hostserver.
- **Synchronisierung in Netzwerken mit nutzungsbedingten Kosten** Standardmäßig werden Offlinedateien nicht im Hintergrund synchronisiert, wenn die Verbindung über Mobilfunk- oder andere Netzwerke erfolgt, bei denen zusätzliche Kosten entstehen, wenn die Verbindungen nicht ortsfest erfolgen oder die geplante Datenmenge fast erreicht oder überschritten ist. Die Schwellenwerte für den Modus für langsame Verbindungen können Sie mit der Richtlinie *Modus für langsame Verbindungen konfigurieren* festlegen und die Hintergrundsynchonisierung konfigurieren Sie mit *Dateisynchronisierung für kostenbezogene Netzwerke aktivieren*, zu finden in den administrativen Vorlagen der Computerkonfiguration unter *Netzwerk\Offlinedateien*.
- **Zwischenspeicherung von umgeleiteten Ordnern** Die üblichen vordefinierten Spezialordner sind automatisch offline verfügbar, wenn sie auf Netzwerkfreigaben umgeleitet werden. Wenn bestimmte umgeleitete Spezialordner nicht offline verfügbar sein sollen, können Sie bestimmte oder alle Ordner mit der Richtlinie *Bestimmte umgeleitete Ordner nicht automatisch offline verfügbar machen* von der Zwischenspeicherung für die Offlineverwendung ausschließen. Sie finden diese Richtlinie in den administrativen Vorlagen der Benutzerkonfiguration unter *System\Ordnerumleitung*.

Benutzer und Administratoren haben die Kontrolle darüber, wann Offlinedateien synchronisiert werden. Eine automatische Synchronisierung kann ausgelöst werden, wenn sich der Benutzer an- oder abmeldet oder wenn Computer in einen Energiesparmodus oder in den Ruhezustand wechseln. Wie die automatische Synchronisierung genau erfolgt, hängt von Gruppenrichtlinien und Benutzereinstellungen ab. Einzelheiten über die Konfiguration von Offlinedateien in den Gruppenrichtlinien finden Sie in Kapitel 5 im Abschnitt »Konfigurieren von Offlinedateirichtlinien«.

Benutzer können die Synchronisierung eines ganzen Netzwerkordners, eines bestimmten Ordners und seines Inhalts oder die Synchronisierung einer bestimmten Datei einleiten, indem sie Ordner oder Datei im Datei-Explorer gedrückt halten oder mit der rechten Maustaste anklicken, *Synchronisierung* wählen und auf *Ausgewählte Offlinedateien synchronisieren* tippen oder klicken.

Manuell lässt sich eine Synchronisierung im Synchronisierungscenter durchführen. Sie erreichen das Synchronisierungscenter auf mehreren Wegen:

- Tippen oder klicken Sie in der Systemsteuerung rechts oben auf den Eintrag neben *Anzeige* und wählen Sie *Große Symbole* oder *Kleine Symbole*. Tippen oder klicken Sie dann auf *Synchronisierungscenter*.
- Geben Sie in im Suchfeld *Systemsteuerung durchsuchen* der Systemsteuerung **Syn** ein und tippen oder klicken Sie auf *Synchronisierungscenter*.

Dateien und Ordner offline verfügbar machen

Freigegebene Netzwerkordner können für die Offlineverwendung verfügbar gemacht werden. Standardmäßig sind alle Unterordner und Dateien in den freigegebenen Ordnern ebenfalls offline verfügbar. Bei Bedarf können Sie die Verfügbarkeit einzelner Dateien und Unterordner ändern. Dazu müssen Sie die Verfügbarkeit der betreffenden Dateien und Unterordner einzeln einstellen. Vergessen Sie nicht, dass neue Dateien, die zu einem freigegebenen und offline verwendeten Ordner hinzugefügt werden, nicht automatisch an die offline arbeitenden Benutzer verteilt werden. Zum Austausch von Updates muss der Offlineordner synchronisiert werden.

Sie können Offlinedateien mit dem Datei-Explorer oder der Computerverwaltungskonsole konfigurieren. Da die Computerverwaltung Sie in die Lage versetzt, Offlinedateien auf jedem Ihrer Netzwerkcomputer zu verwalten, ist sie gewöhnlich das beste Werkzeug. Dateien und Ordner offline verfügbar zu machen ist ein Vorgang, der in drei Schritten erfolgt. Zuerst geben Sie Ordner frei. Dann machen Sie die Ordner für die Offlineverwendung verfügbar. Und schließlich wählen die Benutzer die Dateien und Ordner aus, die sie offline verwenden wollen.

Schritt 1: Freigeben der Ordner

In der Computerverwaltungskonsole geben Sie einen Ordner folgendermaßen für die gemeinsame Verwendung frei:

1. Klicken Sie in der Strukturdarstellung mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen Sie dann *Verbindung mit anderem Computer herstellen*. Wählen Sie im Dialogfeld *Computer auswählen* den Computer aus, mit dem Sie arbeiten möchten.
2. Erweitern Sie in der Konsolenstruktur die Knoten *System* und *Freigegebene Ordner* und wählen Sie dann *Freigaben*. In der Detailansicht werden die aktuellen Freigaben des Computers angezeigt.
3. Klicken Sie mit der rechten Maustaste auf den Knoten *Freigaben* oder halten Sie ihn gedrückt, und wählen Sie dann *Neue Freigabe*. Dadurch wird der Assistent zum Erstellen von Ordnerfreigaben gestartet, der zur Freigabe von Ordnern verwendet werden kann. Dieser Vorgang wurde bereits in Kapitel 13 im Abschnitt »Freigeben eines Ordners und Einstellen der Freigabeberechtigungen in der Computerverwaltung« beschrieben.

Schritt 2: Bereitstellen der Ordner für die Offlineverwendung

In der Computerverwaltungskonsole machen Sie einen freigegebenen Ordner folgendermaßen für die Offlineverwendung verfügbar:

1. Klicken Sie in der Strukturdarstellung mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen Sie dann *Verbindung mit anderem Computer herstellen*. Wählen Sie im Dialogfeld *Computer auswählen* den Computer aus, mit dem Sie arbeiten möchten.
2. Erweitern Sie in der Konsolenstruktur die Knoten *System* und *Freigegebene Ordner* und wählen Sie dann *Freigaben*.
3. Tippen oder klicken Sie doppelt auf die Freigabe, die Sie offline verfügbar machen möchten. Tippen oder klicken Sie auf der Registerkarte *Allgemein* auf *Offlineeinstellungen*.

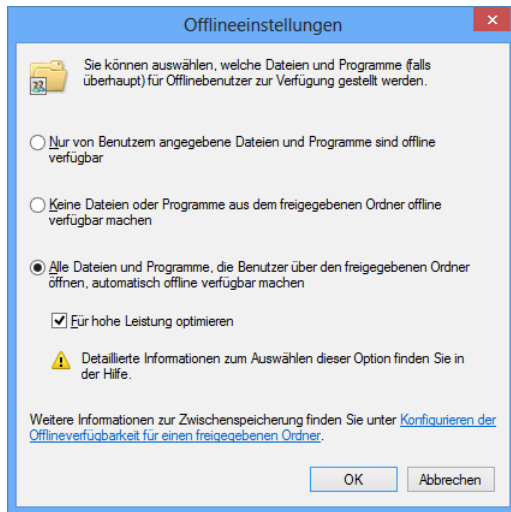


Abbildung 14.2 Optionen für die Zwischenspeicherung von Offlinedateien legen Sie im Dialogfeld *Offlineeinstellungen* fest

4. Im Dialogfeld *Offlineeinstellungen*, das in Abbildung 14.2 zu sehen ist, wählen Sie eine der folgenden Optionen:

- **Nur von Benutzern angegebene Dateien und Programme sind offline verfügbar** Verwenden Sie diese Einstellung, wenn Sie möchten, dass die Benutzer selbst die Dateien auswählen können, die sie offline zur Verfügung haben möchten. Das ist die Standardoption. Sie ist am besten geeignet, wenn es mehrere Benutzer gibt, die dieselben Dateien aus einem Ordner ändern möchten. Sobald sie für die manuelle Auswahl konfiguriert sind, werden Dateien automatisch heruntergeladen und für die Offlineverwendung verfügbar gemacht. Wurde zuvor eine ältere Version eines Dokuments zwischengespeichert, wird diese ältere Version gelöscht. Wenn eine Datei online verwendet wird, geht aus der Serverversion immer hervor, dass die Datei gerade verwendet wird. Bei der Wahl dieser Option können Sie auch BranchCache aktivieren. Dadurch können Computer in kleineren Filialen oder Außenstellen Dateien zwischenspeichern, die von einem freigegebenen Ordner heruntergeladen werden, und diese Dateien dann für die anderen Computer der Zweigstelle verfügbar machen.
- **Alle Dateien und Programme, die Benutzer über den freigegebenen Ordner öffnen, automatisch offline verfügbar machen** Verwenden Sie diese Einstellung für Ordner, in denen Benutzerdaten und Programme liegen. Geöffnete Dateien und ausführbare Programmdateien werden automatisch heruntergeladen und für die Offlineverwendung verfügbar gemacht. Wurde zuvor eine ältere Version eines Dokuments zwischengespeichert, so wird die ältere Version aus dem lokalen Zwischenspeicher gelöscht. Wird eine Datei online verwendet, geht aus der Serverversion immer hervor, dass die Datei gerade verwendet wird. Treten Versionskonflikte auf, werden entsprechende Meldungen angezeigt.

Bei dieser Option können Sie außerdem *Für hohe Leistung optimieren* wählen, um eine erweiterte Zwischenspeicherung der Dateien zu ermöglichen. Durch diese erweiterte Zwischenspeicherung können Programme zwischengespeichert werden, die im Netzwerk freigegeben sind, damit sie auch lokal ausgeführt werden können. Auch das kann die Leistung verbessern.

5. Tippen oder klicken Sie zweimal auf OK.

Schritt 3: Auswählen der Dateien und Ordner für die Offlineverwendung

Nachdem Sie die Freigaben erstellt und für die Offlineverwendung konfiguriert haben, können Sie mit folgenden Schritten die Dateien und Ordner auswählen, die offline verwendet werden sollen:

1. Ordnen Sie einem freigegebenen Ordner oder einer freigegebenen Datei ein Netzlaufwerk zu, wie in Kapitel 13 im Abschnitt »Verwenden von freigegebenen Ressourcen« besprochen.
2. Tippen oder klicken Sie im Datei-Explorer auf die Ortsauswahlschaltfläche und tippen oder klicken Sie dann auf *Computer*. Dadurch öffnet sich das *Computer*-Fenster.
3. Erstellen Sie mit einer der folgenden Methoden einen Offlinecache:
 - Um den ganzen Inhalt eines freigegebenen Ordners auf den Computer des Benutzers zu kopieren und für die Offlineverwendung verfügbar zu machen, klicken Sie unter *Netzwerkadresse* mit der rechten Maustaste auf die gewünschte Freigabe oder halten Sie gedrückt, und wählen dann *Immer offline verfügbar*.
 - Um nur einen ausgewählten Ordner (und seinen Inhalt) oder eine ausgewählte Datei auf den Computer des Benutzers zu kopieren und für die Offlineverwendung verfügbar zu machen, suchen Sie die Netzwerkdatei oder den Ordner in der Computerkonsole heraus und tippen oder klicken dann mit der rechten Maustaste auf die Datei oder den Ordner oder halten sie gedrückt, und wählen *Immer offline verfügbar*.

Durch die Auswahl von Dateien und Ordnern für die Offlineverwendung wird auf dem Computer des Benutzers ein lokaler Cache eingerichtet, in dem die Dateien und Ordner zwischengespeichert werden. Außerdem entsteht dadurch eine Synchronisierungspartnerschaft zwischen dem lokalen Computer und dem Computer, auf dem die freigegebenen Ressourcen liegen, oder eine bereits vorhandene Synchronisierungspartnerschaft wird auf die zusätzlichen Dateien und Ordner erweitert. Synchronisierungspartnerschaften können im Synchronisierungscenter verwaltet werden, wie es im Abschnitt »Verwalten der Offlinedateisynchronisierung« weiter unten in diesem Kapitel noch beschrieben wird.

Offline arbeiten Sie, wenn Ihr Computer nicht mit dem lokalen Netzwerk verbunden ist. Dass Sie offline arbeiten, erkennen Sie im Fenster *Computer* an einem roten X über den Netzlaufwerken oder im Infobereich der Taskleiste. Wenn Sie offline arbeiten, können Sie fast genauso auf Netzwerkdateien zugreifen, als wären Sie mit dem Netzwerk verbunden. Sie verfügen über dieselben Berechtigungen, als würden Sie online arbeiten. Wenn Sie also über Lesezugriff auf eine bestimmte Datei verfügen, solange Sie mit dem Netzwerk verbunden sind, und dann offline arbeiten, können Sie die Datei zwar lesen, aber nicht ändern.

Verwalten der Offlinedateisynchronisierung

Die Synchronisierung des Offlinedateizwischenspeichers hält die Dateien auf dem Clientcomputer auf dem Laufenden und sorgt für die Übertragung von Änderungen, die der Benutzer durchgeführt hat, auf den freigegebenen Ordner. Wie Windows die Synchronisierung durchführt, hängt davon ab, ob eine schnelle, eine langsame oder eine teure Netzwerkverbindung zur Verfügung steht.

Das Synchronisierungscenter, zu sehen in Abbildung 14.3, vereinfacht die Verwaltung zwischengespeicherter Offlinedateien und -ordner. Im Synchronisierungscenter wird für jeden freigegebenen Ordner, der lokal zwischengespeichert wird, eine Synchronisierungspartnerschaft eingerichtet. Jede eingerichtete Synchronisierungspartnerschaft hat einige Eigenschaften, mit denen Sie den Zeitpunkt und die Art der Synchronisation steuern können.

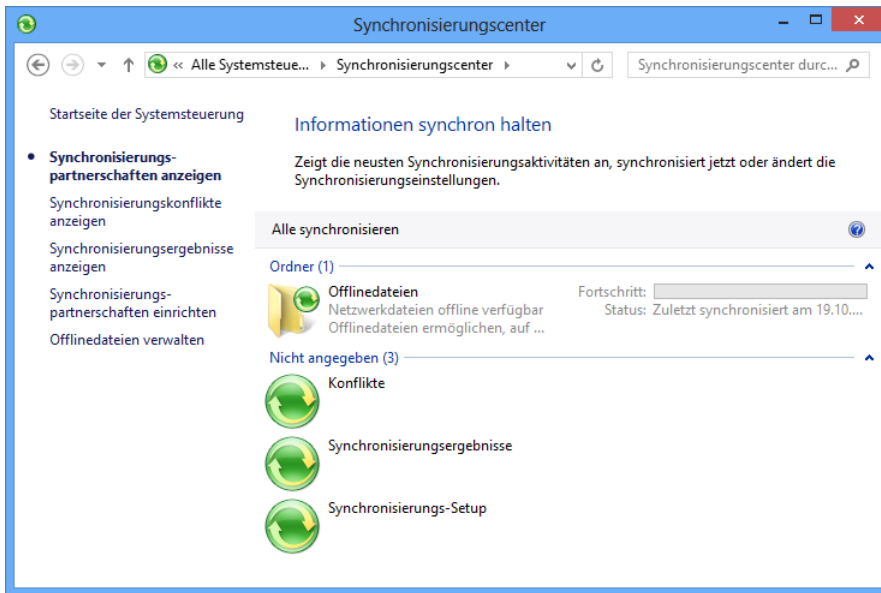


Abbildung 14.3 Verwenden Sie das *Synchronisierungszentrum* zur Durchführung der Synchronisation und zur Anzeige der Ergebnisse

Sie können das Synchronisierungszentrum in der Systemsteuerung öffnen. Tippen oder klicken Sie in der Systemsteuerung rechts oben auf den Eintrag neben *Anzeige* und wählen Sie *Große Symbole* oder *Kleine Symbole*. Tippen oder klicken Sie dann auf *Synchronisierungszentrum*. Wenn Sie das Synchronisierungszentrum geöffnet haben, können Sie leicht überprüfen, ob es Synchronisationsprobleme gibt, und die Synchronisierung konfigurieren, einleiten oder abbrechen.

Im Synchronisierungszentrum ist standardmäßig die Seite *Synchronisierungspartnerschaften anzeigen* vorgewählt. Auf dieser Seite können Sie manuell eine Synchronisierung der Offlinedateien einleiten, indem Sie den Eintrag *Offlinedateien* mit der rechten Maustaste anklicken oder gedrückt halten, und dann *Offlinedateien synchronisieren* wählen.

Mit Gruppenrichtlinien lässt sich genau festlegen, wie die Dateisynchronisierung erfolgen soll. Im Allgemeinen werden Offlinedateien automatisch synchronisiert, wenn ein Benutzer wieder eine Verbindung zum Netzwerk herstellt, nachdem er zuvor vom Netzwerk getrennt war oder es vorgezogen hat, offline zu arbeiten. Sie können die Synchronisierung so einstellen, dass sie zu einem der folgenden Zeitpunkte erfolgt:

- Zu einer festgelegten Zeit
- Wenn sich der Benutzer anmeldet
- Wenn sich der Computer im Leerlauf befindet
- Wenn der Benutzer Windows sperrt oder die Sperrung aufhebt

Planen der Synchronisierung

Zeitpläne für die Synchronisierung können Sie mit folgenden Schritten erstellen und verwalten:

1. Tippen oder klicken Sie die Synchronisierungspartnerschaft, für die eine Synchronisierung durchgeführt werden soll, im Synchronisierungscenter mit der rechten Maustaste an oder halten Sie sie gedrückt, und wählen Sie *Zeitplan für Offlinedateien*.
2. Falls Sie bereits einen Synchronisierungszeitplan für diese Ressource erstellt haben, können Sie nun:
 - **Einen neuen Zeitplan erstellen** Tippen oder klicken Sie auf *Einen neuen Synchronisierungszeitplan erstellen* und fahren Sie mit den Schritten 3 bis 7 fort.
 - **Einen vorhandenen Zeitplan anzeigen oder bearbeiten** Tippen oder klicken Sie auf *Einen vorhandenen Synchronisierungszeitplan anzeigen oder bearbeiten*, dann auf den zu bearbeitenden Zeitplan, auf *Weiter* und fahren Sie mit den Schritten 3 bis 7 fort.
 - **Einen vorhandenen Zeitplan löschen** Tippen oder klicken Sie auf *Einen vorhandenen Synchronisierungszeitplan löschen*, tippen oder klicken Sie auf den zu löschenden Zeitplan und dann auf *Löschen*. Tippen oder klicken Sie auf *OK* und überspringen Sie die restlichen Schritte.
3. Überprüfen Sie die Elemente, die Sie konfigurieren möchten, und löschen Sie die Kontrollkästchen von allen Elementen, die Sie nicht konfigurieren möchten. Tippen oder klicken Sie dann auf *Weiter* und auf *Nach Zeitplan*.
4. Die Optionen *Starten am* und *um* sind so voreingestellt, dass die Synchronisierung sofort beginnen kann (Abbildung 14.4). Wenn Sie möchten, dass die geplante Synchronisierung zu einem anderen Zeitpunkt stattfindet, stellen Sie das Datum und die Uhrzeit entsprechend ein.

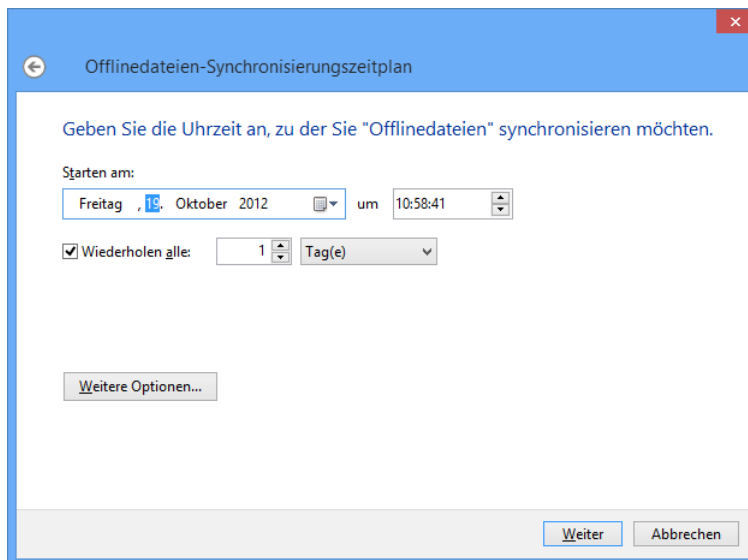


Abbildung 14.4 Erstellen eines Synchronisierungszeitplans

5. Die Option *Wiederholen alle* bestimmt das Synchronisierungsintervall. Vorgegeben wird eine tägliche Synchronisierung. Sie können das Intervall auch auf einen Wert im Bereich Minuten, Stunden, Tage, Wochen oder Monate einstellen. Da nur Änderungen synchronisiert werden, könnten Sie eine etwas häufigere Synchronisierung einstellen, als Sie es unter Windows XP tun würden. Bei wichtigen Dateien könnten Sie beispielsweise eine Synchronisierung in Erwägung ziehen, die alle 3 bis 4 Stunden erfolgt.

6. Wenn Sie die Bedingungen genauer festlegen möchten, unter denen eine Synchronisierung erfolgt, tippen oder klicken Sie auf *Weitere Optionen*. Standardmäßig wird eine Synchronisierung nur eingeleitet, wenn sich der Computer im normalen Betriebszustand befindet, also nicht im Standbymodus oder im Ruhezustand. Sie können die Synchronisierung so einstellen, dass sie:
 - Nur erfolgt, wenn sich der Computer seit N Minuten im Leerlauf befindet, wobei N ein Wert ist, den Sie festlegen.
 - Nur erfolgt, wenn der Computer mit Strom aus dem Stromnetz betrieben wird (also nicht mit dem Akku).
 - Beendet wird, wenn der Computer wieder etwas zu tun hat (er befindet sich nicht mehr im Leerlauf).
 - Beendet wird, wenn der Computer nicht mehr mit Strom aus dem Stromnetz betrieben wird.
7. Tippen oder klicken Sie auf *Weiter*, wenn Sie fertig sind. Geben Sie dem Synchronisierungszeitplan einen eindeutigen und verständlichen Namen und tippen oder klicken Sie dann auf *Zeitplan sichern*.

Ereignisgesteuertes Synchronisieren

Eine Synchronisierung, die durch bestimmte Ereignisse oder Aktionen eingeleitet wird, können Sie mit folgenden Schritten erstellen und verwalten:

1. Tippen oder klicken Sie die Synchronisierungspartnerschaft, für die eine Synchronisierung durchgeführt werden soll, im Synchronisierungcenter an und tippen oder klicken Sie dann auf *Zeitplan*.
2. Falls Sie bereits einen Synchronisierungszeitplan für diese Ressource erstellt haben, können Sie nun:
 - **Einen neuen Zeitplan erstellen** Tippen oder klicken Sie auf *Einen neuen Synchronisierungszeitplan erstellen* und fahren Sie mit den Schritten 3 bis 6 fort.
 - **Einen vorhandenen Zeitplan anzeigen oder bearbeiten** Tippen oder klicken Sie auf *Einen vorhandenen Synchronisierungszeitplan anzeigen oder bearbeiten*, tippen oder klicken Sie auf den zu bearbeitenden Zeitplan, dann auf *Weiter* und fahren Sie mit den Schritten 3 bis 6 fort.
 - **Einen vorhandenen Zeitplan löschen** Tippen oder klicken Sie auf *Einen vorhandenen Synchronisierungszeitplan löschen*, tippen oder klicken Sie auf den zu löschenden Zeitplan und dann auf *Löschen*. Tippen oder klicken Sie auf *OK* und überspringen Sie die restlichen Schritte.
3. Überprüfen Sie die Elemente, die Sie konfigurieren möchten, und löschen Sie die Kontrollkästchen aller Elemente, die Sie nicht konfigurieren möchten. Tippen oder klicken Sie dann auf *Weiter*. Tippen oder klicken Sie auf *Bei Eintreten eines Ereignisses*.
4. Legen Sie mit den verfügbaren Kontrollkästchen die Ereignisse und Aktionen fest, die eine automatische Synchronisierung einleiten (Abbildung 14.5).
 - Wenn sich ein Benutzer am Computer anmeldet
 - Wenn sich der Computer seit N Minuten im Leerlauf befindet, wobei N ein Wert ist, den Sie festlegen
 - Wenn ein Benutzer den Computer sperrt
 - Wenn ein Benutzer den Computer entsperrt
5. Wenn Sie fertig sind, tippen oder klicken Sie auf *Weiter*. Geben Sie dem Synchronisierungszeitplan einen eindeutigen und verständlichen Namen und klicken Sie dann auf *Zeitplan sichern*.

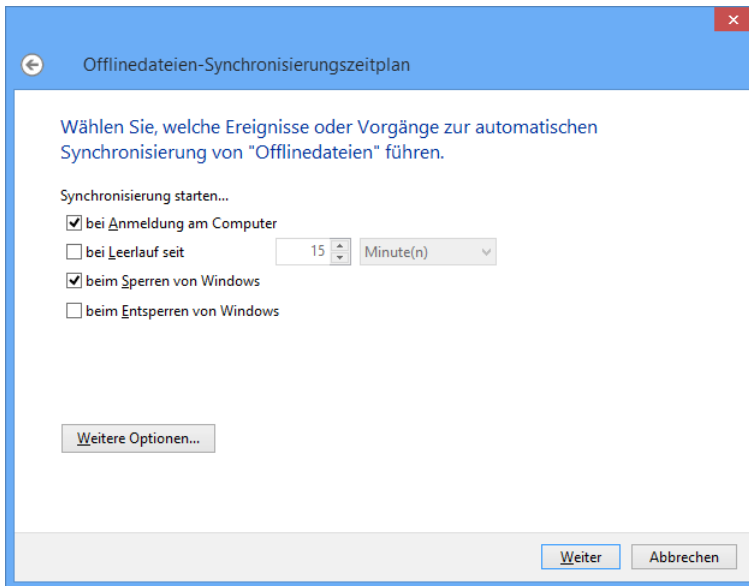


Abbildung 14.5 Synchronisierung auf der Basis von Ereignissen und Vorgängen

Lösen von Synchronisierungskonflikten

In den Synchronisierungsergebnissen finden Sie nähere Einzelheiten, Fehlermeldungen und Warnungen. Zur Anzeige der aktuellen Synchronisierungsergebnisse öffnen Sie das Synchronisierungscenter und tippen oder klicken auf *Synchronisierungsergebnisse anzeigen*. Anhand der Details können Sie überprüfen, wann die Synchronisierung begonnen, abgebrochen oder abgeschlossen wurde. An der Anzeige von Fehlern und Warnungen können Sie erkennen, ob es Probleme mit der Konfiguration der Synchronisierung gibt.

Synchronisierungskonflikte treten auf, wenn ein Benutzer eine Datei offline ändert, die online von einem anderen Benutzer aktualisiert worden ist. Sie können Synchronisierungskonflikte mit folgenden Schritten anzeigen und lösen:

1. Tippen oder klicken Sie im Synchronisierungscenter auf *Synchronisierungskonflikte anzeigen*.
2. Der Hauptfensterabschnitt zeigt an, ob irgendwelche Konflikte aufgetreten sind (Abbildung 14.6).
3. Zum Öffnen des Dialogfelds *Konflikt auflösen* klicken Sie doppelt auf die Zeile der Konfliktmeldung.
4. Nun können Sie Folgendes tun:
 - Tippen oder klicken Sie auf die Version, die Sie behalten möchten. Wenn Sie die lokale Version behalten und die Netzwerkversion überschreiben möchten, tippen oder klicken Sie auf die Version, die mit *Auf diesem Computer* gekennzeichnet ist. Wenn Sie die Netzwerkversion behalten und die lokale Version überschreiben möchten, tippen oder klicken Sie auf die Version, für die der Netzwerkpfad angezeigt wird.
 - Tippen oder klicken Sie auf *Beide Versionen behalten*, wenn Sie die lokale Version unter einem anderen Namen im Netzwerkpfad speichern möchten. Der neue Name ist gewöhnlich der alte Name mit einer numerischen Ergänzung, die als Versionsnummer dienen kann. Wenn Sie nicht sicher sind, welche Version Sie behalten sollen, speichern Sie beide Versionen und vergleichen sie sorgfältig. Entscheiden Sie bei allen unterschiedlichen Stellen, welche Änderung Sie übernehmen und welche Sie verwerfen.

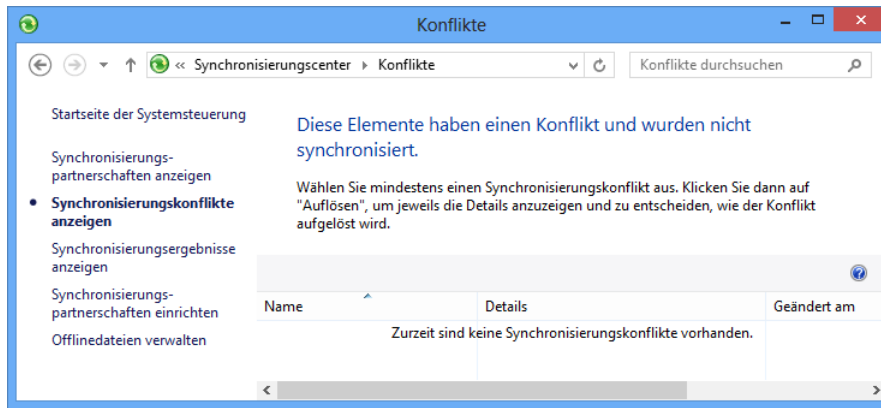


Abbildung 14.6 Konflikte werden mit dem Namen des Dokuments, dem Dateityp, dem Änderungsdatum, der Synchronisierungspartnerschaft und der Konfliktart aufgelistet

Konfigurieren von Datenträgernutzungslimits für Offlinedateien

Sie können im Synchronisierungscenter steuern, wie viel Platz für Offlinedateien benutzt wird und zur Verfügung gestellt wird. In der Standardeinstellung wird die Obergrenze für den Speicherplatz, der höchstens für Offlinedateien belegt werden darf, als Prozentwert festgelegt, der sich auf die Größe des Datenträgers bezieht, auf dem die Benutzerprofile des Computers gespeichert sind. Gehen Sie folgendermaßen vor, um die Datenträgernutzungslimits für Offlinedateien zu konfigurieren:

1. Tippen oder klicken Sie im Synchronisierungscenter auf *Offlinedateien verwalten*. Daraufhin öffnet sich das Dialogfeld *Offlinedateien*.
2. Auf der Registerkarte *Datenträgerverwendung* wird angezeigt, wie viel Platz von allen Offlinedateien und den zugehörigen temporären Dateien belegt wird (Abbildung 14.7). Temporäre Dateien werden erstellt, wenn Benutzer auf ihrem Computer mit Offlinedateien arbeiten.
3. Überprüfen Sie das Limit für alle Offlinedateien und die zugehörigen temporären Dateien. Es ist einmal als Größe in der Einheit Megabyte (MB) oder Gigabyte (GB) angegeben und zusätzlich als Prozentwert, der sich auf die Größe des Datenträgers bezieht, auf dem die Benutzerprofile des Computers gespeichert sind.
4. Tippen oder klicken Sie auf *Limits ändern*. Stellen Sie im Dialogfeld *Datenträgernutzungslimits für Offlinedateien* mit den Schiebereglern die Limits für alle Offlinedateien und die zugehörigen temporären Dateien ein und tippen oder klicken Sie auf *OK*.
5. Tippen oder klicken Sie auf *Temporäre Dateien löschen*, um alle temporären Dateien zu löschen, die nicht mehr benutzt werden. Das Löschen der temporären Dateien hat keine Auswirkung auf die lokal gespeicherten Kopien der Netzwerkdateien.
6. Tippen oder klicken Sie auf *OK*.

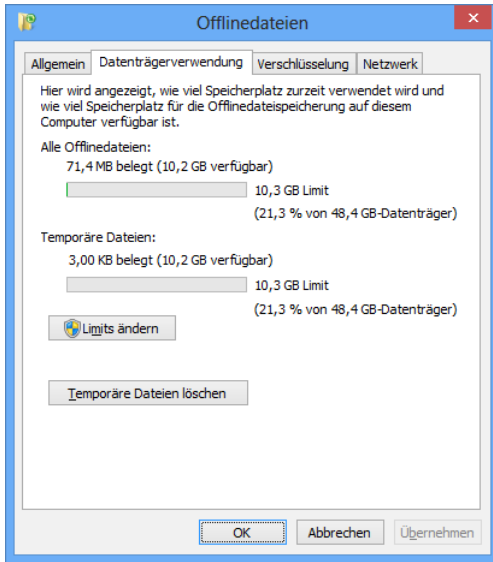


Abbildung 14.7 Konfigurieren der Datenträgerlimits für Offlinedateien

Verwalten der Verschlüsselung für Offlinedateien

Um die Sicherheit zu verbessern, können Sie festlegen, dass Offlinedateien verschlüsselt werden. Wenn Sie Offlinedateien verschlüsseln, werden nur die Dateien verschlüsselt, die auf Ihrem Computer gespeichert sind, aber nicht die Dateien im Netzwerk. Benutzer brauchen die verschlüsselten Dateien nicht zu entschlüsseln, um damit zu arbeiten. Die Entschlüsselung wird automatisch vom Betriebssystem erledigt. Gehen Sie folgendermaßen vor, um Offlinedateien zu verschlüsseln:

1. Tippen oder klicken Sie im Synchronisierungscenter auf *Offlinedateien verwalten*. Daraufhin öffnet sich das Dialogfeld *Offlinedateien*.
2. Überprüfen Sie auf der Seite *Verschlüsselung*, ob die Offlinedateien verschlüsselt sind oder nicht. Wenn sie nicht verschlüsselt sind, tippen oder klicken Sie auf der Registerkarte *Verschlüsselung* auf *Verschlüsseln*, um alle Offlinedateien zu verschlüsseln. Tippen oder klicken Sie anschließend auf *OK*.

Wollen Sie die Verschlüsselung später wieder deaktivieren, müssen Sie diesen Vorgang wiederholen, wobei Sie diesmal auf die Schaltfläche *Entschlüsseln* klicken.

Sperren der Offlineverwendung von Dateien

Als Administrator können Sie festlegen, welche Dateien nicht für die Offlineverwendung zur Verfügung stehen. Dies kann zum Beispiel notwendig sein, wenn ein freigegebener Ordner bestimmte Dateien enthalten muss, die von den Benutzern nicht verändert werden dürfen. Damit diese Dateien nicht offline zur Verfügung stehen, sollten Sie eine bestimmte Ausschlussrichtlinie festlegen, wie in Kapitel 5 im Abschnitt »Konfigurieren von Offlinedateirichtlinien« beschrieben.

In der Computerverwaltungskonsolle können Sie freigegebene Ordner mit folgenden Schritten für die Offlineverwendung sperren:

1. Klicken Sie in der Strukturdarstellung mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt, und wählen Sie dann *Verbindung mit anderem Computer herstellen*. Wählen Sie im Dialogfeld *Computer auswählen* den Computer aus, mit dem Sie arbeiten möchten.
2. Erweitern Sie in der Konsolenstruktur die Knoten *System* und *Freigegebene Ordner* und wählen Sie dann *Freigaben*.
3. Tippen oder klicken Sie die Freigabe, die Sie für die Offlineverwendung sperren möchten, doppelt an. Tippen oder klicken Sie auf der Registerkarte *Allgemein* auf *Offlineeinstellungen*.
4. Im Dialogfeld *Offlineeinstellungen* wählen Sie *Keine Dateien oder Programme aus dem freigegebenen Ordner offline verfügbar machen*.
5. Tippen oder klicken Sie auf *OK*.

Gehen Sie folgendermaßen vor, wenn Sie die Verwendung von Offlinedateien auf einem Clientcomputer vollständig deaktivieren wollen:

1. Tippen oder klicken Sie im Synchronisierungscenter auf *Offlinedateien verwalten*. Daraufhin öffnet sich das Dialogfeld *Offlinedateien*.
2. Tippen oder klicken Sie auf der Registerkarte *Allgemein* auf *Offlinedateien deaktivieren* und dann auf *OK*.

Sollten Sie die Offlinedateien später wieder aktivieren wollen, müssen Sie diesen Vorgang wiederholen, wobei Sie diesmal auf *Offlinedateien aktivieren* klicken.

Konfigurieren von Datenträgerkontingenten

Die folgenden Abschnitte beschreiben die Verwendung und Verwaltung von Datenträgerkontingenten. Datenträgerkontingente unterstützen Sie bei der Verwaltung des Speicherplatzes, der auf Datenträgern zur Verfügung steht, und werden auf Basis der Volumes konfiguriert. Nur Volumes, die mit dem Dateisystem NTFS formatiert sind, können Kontingente verwalten. Der erste Schritt zur Einrichtung von Datenträgerkontingenten ist die Aktivierung der entsprechenden Datenträgerkontingentrichtlinien, wie in Kapitel 5 im Abschnitt »Konfigurieren von Datenträgerkontingentrichtlinien« beschrieben. Nachdem Sie die erforderlichen Richtlinien konfiguriert haben, können Sie für die Volumes eines Computers Kontingente festlegen.

Verwenden von Datenträgerkontingenten

Administratoren verwenden Datenträgerkontingente zur Verwaltung des Speicherplatzes auf wichtigen Volumes, zum Beispiel auf den Volumes, auf denen die Freigaben für Benutzer- oder Firmendaten liegen. Wenn Sie Datenträgerkontingente aktivieren, legen Sie eine Kontingentgrenze und eine Warnstufe fest. Die Kontingentgrenze beschränkt entweder den maximalen Speicherplatz, der einem Benutzer zur Verfügung steht (dadurch wird ein Benutzer daran gehindert, noch mehr Informationen auf dem Volume zu speichern), oder ihre Überschreitung führt zur Erstellung eines entsprechenden Protokolleintrags, oder beides. Die Warnstufe können Sie dazu verwenden, den Benutzer zu informieren und die nahezu vollständige Belegung des Kontingents zu protokollieren.

PRAXISTIPP

Die meisten Administratoren richten Kontingente zwar so ein, dass die Beschränkung durchgesetzt wird, aber Sie müssen die Beschränkung nicht zwangsläufig als harte Grenze interpretieren. Vielleicht fragen Sie sich, welchen Sinn ein Kontingent mit einer offenen Grenze haben soll. Manchmal reicht es aus, den Platzverbrauch auf Benutzerbasis zu erfassen und informiert zu werden, wenn einige Benutzer eine bestimmte Grenze erreichen oder überschreiten. Statt den Benutzern den zusätzlichen Platz zu verweigern, können Sie sich darauf beschränken, eine entsprechende Meldung im Anwendungsprotokoll zu erfassen.

Datenträgerkontingente gelten nur für normale Benutzer, nicht für Administratoren. Man kann Administratoren selbst dann keinen Speicherplatz verweigern, wenn sie Datenträgerkontingente überschreiten, die eigentlich durchgesetzt werden sollen. Kontingentgrenzen und Warnstufen lassen sich in KByte, MByte, GByte, TByte (Terabyte), PByte (Petabyte) und EByte (Exabyte) festlegen. In einer typischen Umgebung legen Sie Grenzen in der Größenordnung von MByte oder GByte fest. Auf einer Freigabe für Firmendaten, die von mehreren Mitarbeitern einer Abteilung benutzt wird, würden Sie den verfügbaren Speicherplatz beispielsweise auf 20 bis 100 GByte beschränken. Für eine Benutzerfreigabe würden Sie vermutlich eine wesentlich kleinere Datenmenge vorsehen, beispielsweise 5 bis 20 GByte, damit kein Benutzer mit großen Mengen persönlicher Daten zu viel Platz verbraucht. Gewöhnlich legen Sie die Warnstufe bei einem bestimmten Prozentsatz der Kontingentgrenze fest. Sie können als Warnstufe zum Beispiel 90 bis 95 Prozent des Kontingents einstellen.

Da Datenträgerkontingente auf Volumebasis und auf Benutzerbasis erfasst werden, wirkt sich die Speicherbelegung durch einen Benutzer nicht auf die Kontingente von anderen Benutzern aus. Überschreitet also ein Benutzer sein Kontingent, gelten Beschränkungen, sofern vorgesehen, nur für diesen Benutzer und nicht für die anderen. Überschreitet ein Benutzer beispielsweise ein 5-GByte-Kontingent und ist das Volume so konfiguriert, dass das Kontingent durchgesetzt wird, kann der Benutzer keine Daten mehr auf dem Volume speichern. Allerdings kann er Dateien und Ordner vom Volume löschen, um Platz zu schaffen. Der Benutzer könnte auch Dateien und Ordner in einen komprimierten Bereich des Volumes verschieben, wodurch auch wieder Platz frei werden könnte. Die Verschiebung von Dateien in einen anderen Bereich des Volumes wirkt sich nicht auf die Kontingentgrenze aus. Der verfügbare Platz ist derselbe, sofern der Benutzer nicht unkomprimierte Dateien und Ordner in einen komprimierten Ordner verschiebt. Jedenfalls können andere Benutzer weiterhin Daten auf dem Volume speichern, solange noch Platz frei ist, auch wenn ein Benutzer sein Kontingent ausgeschöpft hat.

Datenträgerkontingente können Sie auf lokalen Volumes und auf Remotevolumes aktivieren. Bei der Kontingentverwaltung auf lokalen Volumes arbeiten Sie direkt mit dem lokalen Datenträger. Zur Verwaltung von Kontingenten für Remotevolumes müssen Sie das Stammverzeichnis des Volumes freigeben und dann die Kontingente auf dem Volume festlegen. Beachten Sie bitte, dass Betriebssystem- und Anwendungsprogrammdateien nicht in die lokale Kontingentberechnung des Benutzers einfließen, der diese Dateien installiert hat. Systemdateien gehören dem Konto *TrustedInstaller* und Programmdateien dem Konto *SYSTEM*.

Nur Mitglieder der Domänenadministratorgruppe oder der lokalen Administratorgruppe können Datenträgerkontingente festlegen. Mit lokalen Gruppenrichtlinien können Sie Datenträgerkontingente auf einzelnen Computern festlegen. Mit Gruppenrichtlinien, die im ganzen Standort, in der Domäne oder Organisationseinheit gelten, können Sie Datenträgerkontingente für größere Benutzer- oder Computergruppen festlegen. Die Kontingentverwaltung ist eine gewisse zusätzliche Belastung für die Computer. Wie hoch der Aufwand ist, hängt ab von der Zahl der durchzusetzenden Datenträgerkontingente, von der Größe der Volumes, von der gespeicherten Datenmenge und von der Zahl der Benutzer, für die Kontingente verwaltet werden müssen.

Auch wenn es den Anschein hat, als würden Datenträgerkontingente auf Benutzerbasis erfasst, verwaltet Windows 8 die Kontingente nach Sicherheitskennungen (SIDs). Daher können Sie die Namen der Benutzer ändern, ohne die Konfiguration der Kontingente zu beeinträchtigen. Die Verwaltung nach SIDs verursacht wieder einen gewissen zusätzlichen Aufwand, wenn die aktuellen Werte für die Benutzer angezeigt werden, weil Windows 8 die SIDs mit den Kontennamen abgleichen muss, damit die Benutzernamen in den Dialogfeldern angezeigt werden können. Das wiederum bedeutet Zugriffe auf die lokale Benutzerverwaltung oder auf einen Active Directory-Domänencontroller. Sobald die Namen bekannt sind, werden sie in einer lokalen Datei zwischengespeichert, damit sie beim nächsten Mal sofort verfügbar sind. Der Abfragecache wird nur gelegentlich aktualisiert. Wenn Sie also eine Diskrepanz zwischen der Konfiguration und der Anzeige feststellen, müssen Sie die Informationen aktualisieren. Gewöhnlich reicht es aus, im aktuellen Fenster *Aktualisieren* zu wählen oder die Funktionstaste F5 zu drücken.

Aktivieren von Datenträgerkontingenten auf NTFS-Volumes

Datenträgerkontingente werden auf Volumebasis festgelegt und sind nur auf NTFS-Volumes konfigurierbar. Am besten konfigurieren Sie Datenträgerkontingente über Gruppenrichtlinien, wie in Kapitel 5 beschrieben. Sobald die gewünschten Richtlinien konfiguriert sind, können Sie Datenträgerkontingenteinträge erstellen, um Kontingente für bestimmte Benutzer und Gruppen zu verwalten.

Wollen Sie Kontingente lieber auf jedem Computer einzeln konfigurieren, können Sie die Datenträgerkontingente auf einem NTFS-Volume folgendermaßen aktivieren:

1. Starten Sie die Computerverwaltung. Standardmäßig werden Sie mit dem lokalen Computer verbunden. Wenn Sie auf einem anderen Computer Datenträgerkontingente einrichten möchten, klicken Sie in der Konsolenstruktur mit der rechten Maustaste den Knoten *Computerverwaltung* an oder halten ihn gedrückt, und wählen dann *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* wählen Sie den Computer aus, mit dem Sie arbeiten möchten.
2. Erweitern Sie in der Konsolenstruktur *Datenspeicher* und wählen Sie dann *Datenträgerverwaltung*. In der Detailansicht werden die Volumes des ausgewählten Computers angezeigt.
3. Klicken Sie in der Volumeliste oder in der grafischen Ansicht mit der rechten Maustaste auf das Volume, mit dem Sie arbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*.
4. Tippen oder klicken Sie auf die Registerkarte *Kontingent* und wählen Sie dann das Kontrollkästchen *Kontingentverwaltung aktivieren* (Abbildung 14.8).
5. Um für alle Benutzer ein Standardkontingent festzulegen, wählen Sie *Speicherplatz beschränken auf* und legen dann mit den entsprechenden Feldern ein Limit fest. Stellen Sie dann mit den Feldern unter *Warnstufe festlegen auf* eine Standardwarnstufe ein. Üblich sind Werte von 90 bis 95 Prozent des Datenträgerkontingents.

TIPP Das Standarddatenträgerkontingent und die Warnstufe gelten zwar für alle Benutzer, aber Sie können mit dem Dialogfeld *Kontingenteinträge* die Standardwerte überschreiben und für die einzelnen Benutzer unterschiedliche Werte festlegen. Wenn Sie viele verschiedene Einstellungen vornehmen und die Einstellungen nicht auf jedem Volume mit ähnlichen Werten und Verwendungszweck wiederholen möchten, können Sie sie exportieren und auf einem anderen Volume importieren.

6. Um die Kontingentgrenze verbindlich vorzuschreiben und Benutzer an ihrer Überschreitung zu hindern, wählen Sie das Kontrollkästchen *Speicherplatz bei Kontingentüberschreitung verweigern*. Vergessen Sie bitte nicht, dass diese Grenze für Benutzer gilt, aber nicht für Administratoren.

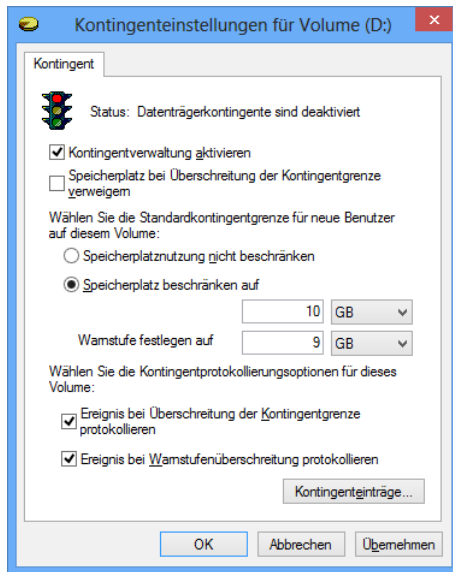


Abbildung 14.8 Nachdem Sie die Kontingentverwaltung aktiviert haben, können Sie für alle Benutzer Kontingente und Warnstufen festlegen

7. Wenn bei Überschreitung der Warnstufe oder der Kontingentgrenze eine Ereignismeldung protokolliert werden soll, verwenden Sie die entsprechenden *Ereignis protokollieren*-Kontrollkästchen.
8. Falls das Kontingentsystem noch nicht aktiviert ist, sehen Sie nach einem Klick auf OK eine entsprechende Meldung, mit der Sie gefragt werden, ob das Kontingentsystem aktiviert werden soll. Tippen oder klicken Sie auf OK, damit Windows 8 das Volume untersuchen und die aktuelle Verwendung erfassen kann. Sofern Benutzer die aktuelle Grenze oder Warnstufe überschreiten, können entsprechende Reaktionen erfolgen. Dazu kann gehören, weitere Datenspeicherungen auf dem Volume zu sperren, den Benutzer beim nächsten Zugriff auf das Volume zu informieren und entsprechende Ereignismeldungen zu protokollieren.

Anzeigen von Datenträgerkontingenteinträgen

Die Verwendung des Festplattenplatzes wird auf Benutzerbasis erfasst. Sind Datenträgerkontingente aktiviert, gibt es für jeden Benutzer, der Daten auf einem Volume speichert, einen Eintrag in der Datenträgerkontingentdatei. Dieser Eintrag wird regelmäßig aktualisiert und gibt den aktuell belegten Platz, das verfügbare Kontingent, die Warnstufe und den Prozentsatz der Belegung an. Als Administrator können Sie Datenträgerkontingenteinträge ändern und für bestimmte Benutzer andere Grenzen und Warnstufen einstellen. Außerdem können Sie Datenträgerkontingenteinträge für Benutzer erstellen, die noch keine Daten auf dem Volume gespeichert haben. Durch die Erstellung solcher Einträge sorgen Sie dafür, dass bei seinem ersten Zugriff auf das Volume bereits ein gültiger Grenzwert samt Warnstufe für einen Benutzer vorliegt.

Die aktuellen Datenträgerkontingenteinträge für ein Volume können Sie folgendermaßen anzeigen:

1. Starten Sie die Computerverwaltung. Standardmäßig werden Sie mit dem lokalen Computer verbunden. Wenn Sie sich die Datenträgerkontingenteinträge auf einem Remotecomputer ansehen möchten, klicken Sie in der Konsolenstruktur mit der rechten Maustaste den Knoten *Computerverwaltung* an

oder halten ihn gedrückt, und wählen dann *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* wählen Sie den Computer aus, mit dem Sie arbeiten möchten.

2. Erweitern Sie in der Konsolenstruktur *Datenspeicher* und wählen Sie dann *Datenträgerverwaltung*. In der Detailansicht werden die Volumes des ausgewählten Computers angezeigt.
3. Klicken Sie in der Volumeliste oder in der grafischen Ansicht mit der rechten Maustaste auf das Volume, mit dem Sie arbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*.
4. Tippen oder klicken Sie auf der Registerkarte *Kontingent* auf *Kontingenteinträge*. Dadurch öffnet sich das Dialogfeld *Kontingenteinträge für*.

Kontingenteinträge zeigen die aktuelle Belegung eines Volumes sowie Kontingentgrenzen und Warnstufen an. Die Statusanzeige soll einen schnellen Hinweis darauf liefern, ob ein Benutzer sein Kontingent überschritten hat. Der Status OK bedeutet, dass der Benutzer innerhalb seines Kontingents liegt. Jeder andere Status bedeutet normalerweise, dass der Benutzer eine Warnstufe oder die Kontingentgrenze erreicht hat.

Erstellen von Datenträgerkontingenteinträgen

Sie können nicht nur Datenträgerkontingenteinträge für Benutzer erstellen, die noch keine Daten auf dem Volume gespeichert haben, sondern auch für Benutzer, die bereits Daten auf einem Volume gespeichert haben. Daher können Sie bei Bedarf für jeden Benutzer Grenzen und Warnstufen festlegen. Darauf werden Sie zurückgreifen müssen, wenn ein Benutzer häufig mehr Daten als andere speichern muss. Beispielsweise könnte ein Grafikdesigner einen wesentlich höheren Bedarf an Speicherplatz entwickeln als ein Kundenberater. Die gute Nachricht lautet, dass Sie Datenträgerkontingenteinträge auf andere Volumes exportieren können. Dadurch können Sie sehr schnell für mehrere Volumes dieselben Regeln festlegen.

Um auf einem Volume einen Datenträgerkontingenteintrag zu erstellen, gehen Sie folgendermaßen vor:

1. Erweitern Sie in der Computerverwaltung den Knoten *Datenspeicher* und wählen Sie dann *Datenträgerverwaltung*. Klicken Sie in der Volumeliste oder in der grafischen Ansicht mit der rechten Maustaste auf das Volume, mit dem Sie arbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*.
2. Tippen oder klicken Sie auf der Registerkarte *Kontingent* auf *Kontingenteinträge*. Die aktuellen Kontingenteinträge für alle Benutzer werden aufgelistet. Drücken Sie die Funktionstaste F5 oder wählen Sie im *Ansicht*-Menü *Aktualisieren*, um die Liste zu aktualisieren.
3. Wenn es für den Benutzer noch keinen Eintrag auf dem Volume gibt, können Sie einen Eintrag erstellen. Wählen Sie im *Kontingent*-Menü *Neuer Kontingenteintrag*. Dadurch öffnet sich das Dialogfeld *Benutzer auswählen*.
4. Im Dialogfeld *Benutzer auswählen* geben Sie im Feld *Geben Sie die zu verwendenden Objektnamen ein* den Namen eines Benutzers ein und tippen oder klicken dann auf *Namen überprüfen*. Werden mehrere Übereinstimmungen gefunden, wählen Sie das gewünschte Konto und tippen oder klicken dann auf OK. Werden keine Übereinstimmungen gefunden, korrigieren Sie Ihre Eingabe und versuchen es noch einmal. Wiederholen Sie diesen Vorgang so oft wie nötig und tippen oder klicken Sie auf OK, wenn Sie fertig sind.
5. Sobald Sie einen Namen gewählt haben, wird das Dialogfeld *Neuen Kontingenteintrag hinzufügen* angezeigt. Sie haben zwei Optionen. Sie können die Kontingentbeschränkung für diesen Benutzer aufheben, indem Sie *Speicherplatznutzung nicht beschränken* wählen. Oder Sie legen eine bestimmte

Grenze und Warnstufe fest, indem Sie *Speicherplatz beschränken auf* wählen und in den dazugehörigen Feldern die entsprechenden Werte eingeben.

6. Tippen oder klicken Sie auf OK. Schließen Sie das Dialogfeld *Kontingenteinträge*. Tippen oder klicken Sie auch im *Eigenschaften*-Dialogfeld auf OK.

Aktualisieren und Anpassen von Datenträgerkontingenteinträgen

Sie können jederzeit die Datenträgerkontingenteinträge für einzelne Benutzer ändern und anpassen. Gehen Sie folgendermaßen vor:

1. Erweitern Sie in der Computerverwaltung den Knoten *Datenspeicher* und wählen Sie dann *Datenträgerverwaltung*. Klicken Sie in der Volumeliste oder in der grafischen Ansicht mit der rechten Maustaste auf das Volume, mit dem Sie arbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*.
2. Tippen oder klicken Sie auf der Registerkarte *Kontingent* auf *Kontingenteinträge*. Die aktuellen Kontingenteinträge für alle Benutzer werden aufgelistet. Drücken Sie die Funktionstaste F5 oder wählen Sie im *Ansicht*-Menü *Aktualisieren*, um die Liste zu aktualisieren.
3. Tippen oder klicken Sie den Benutzereintrag doppelt an. Dadurch öffnet sich das Dialogfeld *Kontingenteinstellungen*, das dem Dialogfeld aus der bereits gezeigten Abbildung 14.8 ähnelt.
4. Wenn Sie die Kontingentbeschränkung für den Benutzer aufheben möchten, wählen Sie *Speicherplatznutzung nicht beschränken*.
5. Wenn Sie das aktuelle Kontingent und die Warnstufe ändern möchten, wählen Sie *Speicherplatz beschränken auf* und geben dann die entsprechenden Werte ein.
6. Tippen oder klicken Sie auf OK.

Löschen von Datenträgerkontingenteinträgen

Wenn Sie auf einem Volume Datenträgerkontingenteinträge erstellt haben und ein Benutzer das Volume nicht länger verwendet, können Sie den entsprechenden Datenträgerkontingenteintrag löschen. Wenn Sie den Datenträgerkontingenteintrag eines Benutzers löschen, werden alle Dateien auf dem Volume, die diesem Benutzer gehören, in einem Dialogfeld angezeigt. Sie können diese Dateien dauerhaft löschen, in Besitz nehmen oder in einen anderen Ordner auf einem anderen Volume kopieren.

Um den Datenträgerkontingenteintrag eines Benutzers zu löschen und die verbleibenden Dateien auf dem Volume zu verwalten, gehen Sie folgendermaßen vor:

1. Erweitern Sie in der Computerverwaltung den Knoten *Datenspeicher* und wählen Sie dann *Datenträgerverwaltung*. Klicken Sie in der Volumeliste oder in der grafischen Ansicht mit der rechten Maustaste auf das Volume, mit dem Sie arbeiten möchten, oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*.
2. Tippen oder klicken Sie auf der Registerkarte *Kontingent* auf *Kontingenteinträge*. Die aktuellen Kontingenteinträge für alle Benutzer werden aufgelistet. Drücken Sie die Funktionstaste F5 oder wählen Sie im *Ansicht*-Menü *Aktualisieren*, um die Liste zu aktualisieren.
3. Wählen Sie den Datenträgerkontingenteintrag aus, den Sie löschen möchten, und drücken Sie dann ENTF oder wählen Sie im *Kontingent*-Menü *Kontingenteintrag löschen*. Mit der UMSCHALT-Taste oder der STRG-Taste können Sie mehrere Einträge auswählen.

4. Wenn Sie dazu aufgefordert werden, bestätigen Sie den Vorgang durch Tippen oder Klicken auf *Ja*. Dadurch öffnet sich das Dialogfeld *Datenträgerkontingent* mit einer Liste der aktuellen Dateien, die dem ausgewählten Benutzer oder den ausgewählten Benutzern gehören.
5. In der Liste *Dateien auflisten von* können Sie einen der Benutzer auswählen, dessen Datenträgerkontingenteintrag Sie löschen wollen, und sich dessen Dateien ansehen. Dann müssen Sie angeben, was mit den Dateien geschehen soll. Sie können die Dateien individuell behandeln, indem Sie einzelne Dateien auswählen und dann die entsprechende Option wählen. Mit der UMSCHALT- oder STRG-Taste können Sie mehrere Einträge auswählen. Folgende Optionen stehen zur Wahl:
 - **Nur Ordner anzeigen** Ändert die Darstellung, damit nur Ordner angezeigt werden, in denen Dateien des Benutzers liegen. Auf diese Weise können Sie alle Dateien des Benutzers in einem bestimmten Ordner löschen, verschieben oder in Besitz nehmen.
 - **Nur Dateien anzeigen** Zeigt alle Dateien, die dem Benutzer gehören, nach den Ordnern an, in denen sie erstellt wurden.
 - **Dateien unwiderruflich löschen** Wählen Sie die zu löschenden Dateien aus und tippen oder klicken Sie auf *Löschen*. Wenn Sie dazu aufgefordert werden, bestätigen Sie den Vorgang durch Tippen oder Klicken auf *Ja*.
 - **Besitz von Dateien übernehmen** Wählen Sie die Dateien aus, die Sie in Besitz nehmen möchten, und tippen oder klicken Sie dann auf *Besitz übernehmen*.
 - **Dateien verschieben nach** Wählen Sie die Dateien aus, die Sie verschieben möchten, und geben Sie dann im Eingabefeld den Pfad eines Ordners auf einem anderen Volume ein. Wenn Sie den Pfad nicht genau kennen, den Sie verwenden möchten, tippen oder klicken Sie auf *Durchsuchen*, um das Dialogfeld *Ordner suchen* zu öffnen und den Ordner herauszusuchen. Wenn Sie ihn gefunden haben, tippen oder klicken Sie auf *Verschieben*.
6. Tippen oder klicken Sie auf *Schließen*, wenn Sie die Arbeit mit den Dateien abgeschlossen haben. Sofern Sie alle Benutzerdateien entsprechend behandelt haben, werden die Datenträgerkontingenteinträge gelöscht.

Exportieren und Importieren von Datenträgerkontingenteinträgen

Statt die Datenträgerkontingenteinträge auf jedem einzelnen Volume erneut vorzunehmen, können Sie sie von einem Quellvolume exportieren und auf einem anderen Volume importieren. Beide Volumes müssen mit NTFS formatiert sein. Um Datenträgerkontingenteinträge zu exportieren und dann zu importieren, gehen Sie folgendermaßen vor:

1. Starten Sie die Computerverwaltung. Standardmäßig werden Sie mit dem lokalen Computer verbunden. Wenn Sie mit den Kontingenteinträgen eines anderen Computers arbeiten möchten, klicken Sie in der Konsolenstruktur mit der rechten Maustaste den Knoten *Computerverwaltung* an oder halten ihn gedrückt, und wählen dann *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* wählen Sie den Computer aus, mit dem Sie arbeiten möchten.
2. Erweitern Sie in der Konsolenstruktur *Datenspeicher* und wählen Sie dann *Datenträgerverwaltung*. In der Detailansicht werden die Volumes des ausgewählten Computers angezeigt.
3. Tippen oder klicken Sie in der Volumeliste oder in der grafischen Ansicht mit der rechten Maustaste auf das Quellvolume und wählen Sie dann *Eigenschaften*.
4. Tippen oder klicken Sie auf der Registerkarte *Kontingent* auf *Kontingenteinträge*. Dadurch öffnet sich das Dialogfeld *Kontingenteinträge*.

5. Wählen Sie im *Kontingent*-Menü *Exportieren*. Dadurch öffnet sich das Dialogfeld *Exportiert Kontingenteinstellungen*. Wählen Sie den Ort aus, an dem Sie die Datei mit den Kontingenteinstellungen speichern möchten, und geben Sie im Textfeld *Dateiname* einen Namen für die Datei ein. Tippen oder klicken Sie dann auf *Speichern*.

TIPP Wenn Sie die Einstellungsdatei auf einem zugeordneten Laufwerk auf dem Zielvolume speichern, ist der Import einfacher. Kontingentdateien sind ziemlich klein, Sie brauchen sich also keine Gedanken über den Speicherplatz zu machen.

6. Wählen Sie im *Kontingent*-Menü *Schließen*, um das Dialogfeld *Kontingenteinträge* zu schließen. Tippen oder klicken Sie auf *OK*, um das *Eigenschaften*-Dialogfeld zu schließen.
7. Klicken Sie in der Strukturdarstellung mit der rechten Maustaste auf den Knoten *Computerverwaltung* oder halten Sie ihn gedrückt. Wählen Sie im Kontextmenü *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* wählen Sie den Computer aus, auf dem das Zielvolume liegt, auf das Sie die exportierten Einstellungen importieren möchten.
8. Erweitern Sie *Datenspeicher* und wählen Sie dann *Datenträgerverwaltung*. Tippen oder klicken Sie mit der rechten Maustaste in der Volumeliste oder in der grafischen Ansicht auf das Zielvolume und wählen Sie *Eigenschaften*.
9. Tippen oder klicken Sie auf die Registerkarte *Kontingent*. Sorgen Sie dafür, dass *Kontingentverwaltung aktivieren* gewählt ist, und tippen oder klicken Sie dann auf *Kontingenteinträge*. Dadurch öffnet sich das Dialogfeld *Kontingenteinträge* für das Zielvolume.
10. Wählen Sie im *Kontingent*-Menü *Importieren*. Wählen Sie im Dialogfeld *Importiert Kontingenteinstellungen* die Kontingenteinstellungsdatei aus, die Sie zuvor gespeichert haben. Tippen oder klicken Sie auf *Öffnen*.
11. Sofern es auf dem Volume bereits Kontingenteinträge gibt, haben Sie nun die Gelegenheit, diese Einträge zu erhalten oder zu ersetzen. Werden Sie auf einen Konflikt hingewiesen, können Sie den vorhandenen Eintrag durch Tippen oder Klicken auf *Ja* ersetzen oder durch Tippen oder Klicken auf *Nein* erhalten. Wenn Sie vor dem Tippen oder Klicken auf *Ja* oder *Nein* das Kontrollkästchen *Auf alle Kontingenteinträge anwenden* wählen, gilt Ihre Entscheidung, die vorhandenen Einträge zu erhalten oder zu ersetzen, für alle Einträge.

Deaktivieren von Datenträgerkontingenten

Sie können Datenträgerkontingente für einzelne Benutzer oder für alle Benutzer eines Volumes deaktivieren. Wenn Sie das Kontingent für einen bestimmten Benutzer deaktivieren, muss dieser Benutzer zwar kein festgelegtes Kontingent mehr einhalten, aber für die anderen Benutzer ändert sich nichts. Wenn Sie die Kontingentverwaltung eines ganzen Volumes deaktivieren, wird für dieses Volume keine Kontingentverwaltung mehr durchgeführt. Um das Kontingent eines bestimmten Benutzers zu deaktivieren, wenden Sie die Methode an, die im Abschnitt »Aktualisieren und Anpassen von Datenträgerkontingenteinträgen« weiter oben in diesem Kapitel beschrieben wurde. Um die Kontingentverwaltung für ein ganzes Volume zu deaktivieren, gehen Sie folgendermaßen vor:

1. Starten Sie die Computerverwaltung. Standardmäßig werden Sie mit dem lokalen Computer verbunden. Wenn Sie die Kontingentverwaltung auf einem Remotecomputer deaktivieren möchten, klicken Sie in der Konsolenstruktur mit der rechten Maustaste den Knoten *Computerverwaltung* an oder halten ihn gedrückt, und wählen dann *Verbindung mit anderem Computer herstellen*. Im Dialogfeld *Computer auswählen* wählen Sie den Computer aus, mit dem Sie arbeiten möchten.

2. Erweitern Sie in der Konsolenstruktur *Datenspeicher* und wählen Sie dann *Datenträgerverwaltung*. In der Detailansicht werden die Volumes des ausgewählten Computers angezeigt.
3. Klicken Sie in der Volumeliste oder in der grafischen Ansicht mit der rechten Maustaste auf das gewünschte Volume oder halten Sie es gedrückt, und wählen Sie dann *Eigenschaften*.
4. Löschen Sie auf der Registerkarte *Kontingent* das Kontrollkästchen *Kontingentverwaltung aktivieren*. Tippen oder klicken Sie auf *OK*. Wenn Sie zur Bestätigung des Vorgangs aufgefordert werden, tippen oder klicken Sie auf *OK*.

Verwenden von BranchCache

Windows BranchCache dient zur Zwischenspeicherung von Dateien. Es arbeitet mit dem intelligenten Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS) zusammen. Administratoren können BranchCache in den Gruppenrichtlinien aktivieren, damit Computer Dokumente und andere Dateitypen aus einem lokalen Zwischenspeicher (engl. cache) holen, statt die Dateien über das Netzwerk von Servern abzurufen.

BranchCache funktioniert mit Dateien, die über HTTP (Hypertext Transfer Protocol) und SMB (Server Message Block) übertragen werden. Daher werden Dateien zwischengespeichert, die von Intranetwebservern und internen Dateiservern stammen. Die Zwischenspeicherung kann die Reaktionszeiten erheblich verbessern und die Übertragung von Dokumenten, Webseiten und Multimediainhalt deutlich beschleunigen.

BranchCache verwendet eine Client/Server-Architektur und ist in die Windows-Dateidienste und die Speicherdienste integriert. Zwei Versionen von BranchCache sind verfügbar:

- BranchCache Version 1 wurde mit Windows 7 und Windows Server 2008 Release 2 veröffentlicht (und für Windows Vista mit BITS 4.0 verfügbar gemacht).
- BranchCache Version 2 wurde mit Windows 8 und Windows Server 2012 veröffentlicht.

Die beiden Versionen sind sehr verschieden und verwenden Lösungsansätze, die nicht miteinander vereinbar sind. Version 1 hält sich an den herkömmlichen Lösungsansatz für Zwischenspeicher. In Version 2 verwendet BranchCache Datendeduplizierungstechniken, mit denen die Datenübertragung über WANs (Wide Area Networks) zu den Zweigstellen optimiert wird. BranchCache 2 verwendet Datenblöcke variabler Größe und komprimiert die Daten, um bei der Dateiübertragung eine höhere Effizienz zu erreichen. Zwischengespeicherte Dateien werden nicht als Datenströme gespeichert, sondern durch Platzhalter (stubs) ersetzt, die auf Datenblöcke in einem gemeinsamen Zwischenspeicher verweisen. Die Aufteilung von Dateien in Datenblöcke unterstützt kompatible Clientcomputer bei dem Versuch, nur eine Instanz von doppelten Inhalten herunterzuladen, und sie unterstützt BranchCache bei dem Bestreben, von doppelten Inhalten nur eine Instanz zu speichern. Durch die Aufteilung von Dateien in Datenblöcke ist es auch möglich, nur den Teil einer Datei zu übertragen, der sich geändert hat, statt die gesamte Datei übertragen zu müssen. Beachten Sie auch, dass BranchCache die bereits in Datenblöcke aufgeteilte Datei verwenden kann und es nicht erforderlich ist, die Datei für die Übertragung zu bearbeiten, wenn es auf einem Volume einen freigegebenen Ordner gibt, der bereits dupliziert wurde.

Im Allgemeinen legen LAN-Grenzen (Local Area Network) fest, wie BranchCache arbeitet, nachdem es implementiert wurde. Ist ein LAN mit der Hauptniederlassung über ein Netzwerk verbunden, bei dem die Netzwerklatenz für einen Roundtrip mehr als 80 Millisekunden beträgt, verwenden Clients in diesem LAN nach Möglichkeit den lokalen Cache. Wenn mehrere LANs untereinander mit einem schnellen Netzwerk verbunden sind, können sie auch einen gemeinsamen lokalen Cache benutzen.

Wenn Sie BranchCache aktivieren und dann zum ersten Mal über das Netzwerk auf eine Datei zugegriffen wird, die in einer Intranetwebsite oder auf einem Dateiserver liegt, überträgt Windows 8 die Datei vom Quellserver und speichert sie lokal in der Zweigstelle. Wenn später derselbe oder ein anderer Benutzer in der Zweigstelle erneut auf diese Datei zugreift, sucht Windows die Datei im lokalen Cache. Findet es die Datei dort, fragt Windows den Quellserver ab, um zu prüfen, ob sich die Datei geändert hat, seit sie zwischengespeichert wurde. Hat sich die Datei nicht verändert, ruft Windows sie aus dem lokalen Cache ab, damit die Datei nicht erneut über das WAN (Wide Area Network) gesendet werden muss. Hat sich die Datei geändert, ruft Windows sie vom Quellserver ab und aktualisiert die Kopie im Cache.

In Version 2 werden die zwischengespeicherten Daten standardmäßig verschlüsselt, um die Sicherheit zu verbessern, und der gehostete Cache auf Windows Servern wird mit einer ESE-Datenbank (Extensible Storage Engine) verwaltet. Die ESE-Datenbank ermöglicht es einem gehosteten Cacheserver, Terabytes von Daten zu speichern und viele Clients effizient zu bedienen. Außerdem können Administratoren Inhalte vorab auf gehosteten Cacheservern speichern, bevor der Inhalt angefordert wird. Diese Vorabversorgung mit Daten sorgt dafür, dass die Daten schnell im lokalen Zwischenspeicher verfügbar sind. Wenn Sie Inhalte von Medien vorab speichern, beispielsweise von externen Laufwerken oder von DVDs, müssen die Inhalte nicht über das Netzwerk übertragen werden.

Sie können BranchCache so konfigurieren, dass es in einem der beiden folgenden Modi arbeitet:

- **Verteilter Cache** In diesem Modus hosten die Desktopcomputer der Benutzer, auf denen eine kompatible Windows-Version verwendet wird, verteilte Dateizwischenspeicher. In der Zweigstelle muss kein Server installiert werden, weil jeder lokale Computer Dateien zwischenspeichert und versendet.
- **Gehosteter Cache** In diesem Modus hosten kompatible Dateiserver in der Zweigstelle den lokalen Dateicache. Die Server speichern Dateien und versenden sie an die Clients in der Zweigstelle.

HINWEIS BranchCache Version 2 ermöglicht zwar die Ausweitung der Zwischenspeicherung auf mehrere Server, aber BranchCache Version 1 lässt in einer Zweigstelle nur einen einzigen Server für den gehosteten Zwischenspeicher zu.

Offensichtlich haben beide Zwischenspeicherungsmodi ihre Vor- und Nachteile. Beim verteilten Cache brauchen Sie keinen Server zu installieren, bevor Sie den BranchCache aktivieren können, aber die Desktopcomputer der Benutzer müssen den Cache verwalten und die Dateien verteilen. Das verbraucht Rechenleistung, wodurch die Leistung der Desktopcomputer unter Umständen leidet. Beim gehosteten Cachemodus müssen Sie einen oder mehrere Server installieren, bevor Sie BranchCache aktivieren. Aber sobald die Server einmal eingerichtet sind und laufen, erledigen sie die gesamte Verarbeitung und die Cacheverwaltung. Das ist ein erheblicher Vorteil gegenüber dem verteilten Cache.

Beim BranchCache sind folgende Punkte zu beachten:

- BranchCache verhindert nicht, dass Benutzer Dateien lokal speichern. Es kümmert sich nur um Leseanforderungen, etwa wenn ein Benutzer eine Datei von einem Dateiserver anfordert.
- BranchCache arbeitet nahtlos mit Verschlüsselung und Technologien für sichere Datenübertragung wie SMB-Signing und IPsec zusammen.
- In der Standardeinstellung werden Netzwerkdateien nur dann in der Zweigstelle zwischengespeichert, wenn die Netzwerklatenz für einen Roundtrip mehr als 80 Millisekunden beträgt.

Installiert und konfiguriert wird BranchCache mit folgenden Schritten:

- Bereiten Sie einen BranchCache-fähigen Dateiserver vor, indem Sie zu einem Dateiserver den Rollendienst *BranchCache für Netzwerkdateien* hinzufügen.

- Bereiten Sie einen BranchCache-fähigen Inhaltsserver vor (beispielsweise einen Webserver oder einen Anwendungsserver auf BITS-Basis), indem Sie das Feature *BranchCache* zum Server hinzufügen.
- Installieren Sie einen Server für den gehosteten Cache, indem Sie in der Zweigstelle das Feature *BranchCache* zu einem Server hinzufügen.
- Bereiten Sie die Clients auf BranchCache vor, indem Sie BranchCache und den BranchCache-Modus (verteilt oder gehostet) auf den Clients aktivieren.

Gehen Sie folgendermaßen vor, um BranchCache zu aktivieren und zu konfigurieren:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienverwaltungs-Editor. Sie finden die benötigten Richtlinien im Zweig *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\BranchCache*.
2. Tippen oder doppelklicken Sie auf *BranchCache aktivieren*. Wählen Sie im Eigenschaftendialogfeld die Option *Aktiviert* aus und tippen oder klicken Sie auf *OK*.
3. Sie haben jetzt folgende Möglichkeiten:
 - Klicken Sie doppelt auf *BranchCache-Modus "Verteilter Cache" festlegen*, um den verteilten BranchCache zu aktivieren. Wählen Sie im Eigenschaftendialogfeld *Aktiviert* aus und tippen oder klicken Sie auf *OK*.
 - Klicken Sie doppelt auf *BranchCache-Modus "Gehosteter Cache" festlegen*, um den gehosteten BranchCache zu aktivieren. Wählen Sie im Eigenschaftendialogfeld die Option *Aktiviert* aus, geben Sie den Hostnamen des Cacheservers ein und tippen oder klicken Sie auf *OK*.
 - Um die Zwischenspeicherung im gehosteten Cache für BranchCache Version 2-Clients zu aktivieren, tippen oder klicken Sie doppelt auf *Gehostete Cacheserver konfigurieren*. Wählen Sie im Eigenschaftendialogfeld *Aktiviert* und wählen Sie dann *Anzeigen*. Geben Sie im Dialogfeld *Inhalt anzeigen* den vollqualifizierten Hostnamen oder die IP-Adresse jedes Cacheservers der Version 2 aus der Zweigstelle an, für den das GPO gilt. Tippen oder klicken Sie zweimal auf *OK*.

HINWEIS Wenn Sie die Richtlinie *Gehostete Cacheserver konfigurieren*, ignorieren Windows 8-Clients die Einstellungen der Richtlinie *BranchCache-Modus "Gehosteter Cache" festlegen*.

PRAXISTIPP In einer gemischten Umgebung können die unterschiedlichen Lösungsansätze von Version 1 und Version 2 von BranchCache für die Zwischenspeicherung zu Effizienz- und Kompatibilitätsproblemen führen. Wenn Sie möchten, dass Windows 8-Clients Version 1 statt Version 2 verwenden, erreichen Sie dies, indem Sie die Richtlinie *Versionsunterstützung für BranchCache für Clients konfigurieren* aktivieren und die Versionsoption auf *Windows Vista mit installiertem BITS 4.0, Windows 7 oder Windows Server 2008 R2* einstellen.

4. Sie können einstellen, welche Netzwerklatenz nötig ist, um die Zwischenspeicherung auszulösen, indem Sie doppelt auf *BranchCache für Netzwerkdateien konfigurieren* klicken. Wählen Sie im Eigenschaftendialogfeld die Option *Aktiviert*. Geben Sie die Netzwerklatenz für den Roundtrip ein, ab der Netzwerkdateien zwischengespeichert werden sollen. Dieser Wert wird in der Einheit Millisekunden angegeben. Wenn Sie den Wert 0 einstellen, werden Dateien immer zwischengespeichert.
5. Wenn Sie gehostetes BranchCache aktiviert haben, können Sie doppelt auf *Prozentuale Speicherplatzbelegung durch Clientcomputercache festlegen* klicken. Wählen Sie im Eigenschaftendialogfeld die Option *Aktiviert* aus. Geben Sie ein, welchen Prozentsatz der gesamten Festplattenkapazität der Client-

computer für BranchCache verwenden soll, und tippen oder klicken Sie auf OK. In der Standardeinstellung beträgt die Maximalgröße für den Cache 5 Prozent des gesamten Festplattenplatzes.

Mit BranchCache Version 2 ist es auch möglich, dass kompatible Clients Active Directory nach gehosteten Cacheservern durchsuchen, die zu ihrem aktuellen Active Directory-Standort gehören, und sich selbst automatisch für den Modus »Gehosteter Cache« konfigurieren, sofern dies möglich ist. Verwenden Sie die Richtlinie *Automatische Erkennung von gehostetem Cache pro Dienstverbindungspunkt aktivieren*, um dies zu ermöglichen.

Kapitel 15

Konfigurieren und Problembehandlung von TCP/IP-Netzwerken

In diesem Kapitel:

Überblick über die Netzwerkfunktionen von Windows 8	568
Installieren der Netzwerkkomponenten	572
Konfigurieren von Netzwerkverbindungen	576
Verwalten von Netzwerkverbindungen	585
Problembehandlung und Testen von Netzwerkeinstellungen	588

Dieses Kapitel legt den Schwerpunkt auf die Verwaltung von Netzwerk- und Drahtlosverbindungen, die zur Kommunikation in einem Computernetz verwendet werden. Damit das Netzwerk einwandfrei funktioniert, müssen Sie die erforderlichen Netzwerkkomponenten installieren und die Netzwerkkommunikation mit Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) und Windows Internet Naming Service (WINS) konfigurieren. DHCP dient zur dynamischen Konfiguration des Netzwerks und der IP-Adressen. DNS und WINS bieten Namenszuordnungsdienste, wobei DNS der bevorzugte Dienst ist und WINS nur noch aus Gründen der Abwärtskompatibilität zu früheren Windows-Versionen verfügbar ist.

Überblick über die Netzwerkfunktionen von Windows 8

Die Netzwerkfunktionen von Windows 8 umfassen folgende Komponenten:

- **Netzwerk-Explorer** Bietet eine zentrale Konsole für die Anzeige von Computern und Geräten im Netzwerk.
- **Netzwerk- und Freigabecenter** Bietet eine zentrale Konsole für die Anzeige und Verwaltung der Netzwerk- und Freigabekonfiguration eines Computers.
- **Netzwerkd Diagnose** Bietet eine automatische Diagnose zur Behebung von Netzwerkproblemen.

Bevor wir uns näher mit der Nutzung dieser Netzwerktools befassen, müssen Sie wissen, auf welchen Windows 8-Funktionen diese Tools basieren. Es sind dies die Netzwerkerkennung, die es ermöglicht, andere Computer und Geräte im Netzwerk zu erkennen, und die Netzwerkzustandsüberwachung, die Änderungen in der Netzwerkkonfiguration und den Verbindungen erkennt.

Netzwerkerkennung und Netzwerkkategorien

Von den Einstellungen Ihres Computers zur Netzwerkerkennung hängt es ab, welche Computer und Geräte Sie in den Netzwerkprogrammen von Windows 8 sehen und anzeigen können. Zusammen mit der Windows-Firewall eines Computers erlauben oder sperren die Einstellungen zur Netzwerkerkennung:

- Die Erkennung von Computern und Geräten im Netzwerk
- Die Erkennung Ihres Computers durch andere Computer

Die Einstellungen zur Netzwerkerkennung sollen bei jedem Netzwerktyp, mit dem ein Computer Verbindungen herstellen kann, für angemessene Sicherheitsvorkehrungen sorgen. Es sind drei Kategorien von Netzwerken definiert:

- **Domänennetzwerk** Ein Netzwerk, in dem die Computer mit einer Domäne verbunden sind, in der sie Mitglieder sind
- **Privates Netzwerk** Ein Netzwerk, in dem die Computer zu einer Arbeitsgruppe oder Heimnetzgruppe zusammengefasst sind. Die einzelnen Computer sind dabei nicht direkt mit dem öffentlichen Internet verbunden.
- **Öffentliches Netzwerk** Ein Netzwerk an einem öffentlichen Ort, etwa in einem Café oder auf einem Flughafen

HINWEIS

In der Standardeinstellung sind Netzwerkerkennung und Dateifreigabe nicht aktiviert, sie können aber für Domänen- und private Netzwerke aktiviert werden. Im Fenster *Netzwerk* oder in den erweiterten Freigabeeinstellungen im Netzwerk- und Freigabecenter können Sie Netzwerkerkennung und Dateifreigabe aktivieren. Dadurch bauen Sie Einschränkungen ab, sodass die Computer im Netzwerk andere Computer und Geräte in diesem Netzwerk erkennen und Dateien

freigeben können. Netzwerkerkennung und Dateifreigabe sind in einem öffentlichen Netzwerk standardmäßig gesperrt. Daraus ergibt sich eine höhere Sicherheit, denn Computer im öffentlichen Netzwerk können andere Computer und Geräte nicht ohne Weiteres erkennen. Sind Netzwerkerkennung und Dateifreigabe allerdings deaktiviert, so sind Dateien und Drucker, die Sie auf Ihrem Computer freigegeben haben, im Netzwerk nicht zugänglich. Außerdem sind manche Anwendungen vielleicht nicht in der Lage, auf das Netzwerk zuzugreifen.

Da ein Computer die Einstellungen für jede Netzwerkkategorie separat speichert, können Sie in jeder Kategorie andere Einstellungen konfigurieren, die festlegen, welche Arten von Netzwerkverkehr erlaubt sind oder blockiert werden. Wenn Sie Ihren Computer das erste Mal mit einem Netzwerk verbinden, versucht Windows 8 festzustellen, ob Sie sich zu Hause, am Arbeitsplatz oder an einem öffentlichen Ort befinden. Diese Auswahl legt die Netzwerkkategorie fest. Wenn Sie Ihre Netzwerkverbindung anschließend ändern oder eine Verbindung mit einem neuen Netzwerk herstellen, versucht Windows 8, die Netzwerkkategorie automatisch zu ermitteln. Ist Windows 8 dazu nicht in der Lage, verwendet es die Kategorie öffentliches Netzwerk. Wenn Sie den Computer zum Mitglied einer Domäne machen, ändert sich das Netzwerk, mit dem der Computer verbunden ist, in ein Domänennetzwerk.

Anhand der Netzwerkkategorie schaltet Windows 8 die Netzwerkerkennung ein oder aus. Der Zustand *An (Aktiviert)* bedeutet, dass der Computer andere Computer und Geräte im Netzwerk erkennen kann und dass umgekehrt andere Computer im Netzwerk diesen Computer erkennen können. Der Zustand *Aus (Deaktiviert)* bedeutet, dass der Computer andere Computer und Geräte im Netzwerk nicht erkennen kann und dass auch andere Computer im Netzwerk diesen Computer nicht erkennen können.

Manchmal weist Windows 8 die Kategorie öffentliches Netzwerk zu, obwohl sich der Computer in Wirklichkeit in einem privaten Netzwerk befindet und Mitglied einer Arbeitsgruppe ist (oder zu einer Heimnetzgruppe hinzugefügt werden soll). Dieses Problem tritt meist auf, weil die TCP/IP-Einstellungen falsch konfiguriert sind. Aber selbst wenn die TCP/IP-Einstellungen und der Computer richtig konfiguriert sind, taucht dieses Problem gelegentlich auf.

Damit das Netzwerk einwandfrei funktioniert, müssen Sie die Netzwerkkategorie ändern. Andernfalls kann der Computer möglicherweise nicht auf andere Ressourcen im Netzwerk zugreifen. Warum? Die Windows-Firewall und die Windows-Firewall mit erweiterter Sicherheit legen anhand der Netzwerkkategorie fest, wie sie den Computer schützen. Computer haben für jede Netzwerkkategorie ein eigenes Windows-Firewallprofil, wobei das Firewallprofil für öffentliche Netzwerke die stärksten Einschränkungen durchsetzt.

Sie können dieses Problem beispielsweise dadurch lösen, dass Sie mit dem Heimnetzgruppen-Problembehandlungsmodul die Netzwerkkategorie von öffentlich auf privat ändern. Gehen Sie dazu folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Heimnetzgruppen- und Freigabeoptionen auswählen*. Tippen oder klicken Sie auf *Heimnetzgruppen-Problembehandlung starten*.
2. Tippen oder klicken Sie auf der ersten Seite des Problembehandlungsmoduls auf *Weiter*.
3. Auf der Seite *Netzwerkprobleme behandeln* müssten Sie eine Meldung sehen, dass manche Netzwerkprobleme mit Heimnetzgruppen zu tun haben. Tippen oder klicken Sie auf *Schritt überspringen*.
4. Das Problembehandlungsmodul sollte nun feststellen, dass der Netzwerkstandort falsch eingestellt ist. Wählen Sie *Diese Korrektur anwenden*, wenn Sie gefragt werden, ob der Netzwerkstandort auf privat geändert werden soll.

5. Folgen Sie den Anweisungen, wenn Sie eine Heimnetzgruppe erstellen oder einer vorhandenen beitreten wollen. Tippen oder klicken Sie andernfalls auf *Abbrechen*, um das Problembehandlungsmodul zu beenden.

PRAXISTIPP

Manchmal hat ein Computer, dessen Netzwerkkategorie auf öffentlich eingestellt ist, Probleme mit dem Beitritt zu einer Domäne. Die TCP/IP-Einstellungen des Computers können zwar die Ursache für dieses Problem sein, aber auch das angewendete Firewallprofil kann schuld sein. Weil das öffentliche Firewallprofil standardmäßig die stärksten Einschränkungen erzwingt, blockieren die Einstellungen unter Umständen Verbindungen, die für den Beitritt zur Domäne gebraucht werden. Sie können dieses Problem umgehen, indem Sie die Windows-Firewall kurz ausschalten oder dem eben beschriebenen Verfahren folgen, um Windows zu zwingen, die Netzwerkkategorie von öffentlich auf privat zu ändern.

Verwenden des Netzwerk-Explorers

Der Netzwerk-Explorer zeigt eine Liste der Computer und Geräte an, die im Netzwerk erkannt wurden. Sie haben mehrere Möglichkeiten, den Netzwerk-Explorer zu öffnen:

- Tippen oder klicken Sie auf dem Startbildschirm auf *Explorer*. Tippen oder klicken Sie im Datei-Explorer auf die Schaltfläche zum Auswählen des Speicherorts und dann auf *Netzwerk*.
- Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet*. Tippen oder klicken Sie unter *Netzwerk- und Freigabecenter* auf *Netzwerkcomputer und -geräte anzeigen*.

HINWEIS

Im Datei-Explorer enthält die Adressleiste vier Elemente: ein Speicherortsymbol, eine Schaltfläche zum Auswählen des Speicherorts, Einträge für den Speicherort und die Schaltfläche *Vorherige Orte*. Tippen oder klicken Sie auf die Schaltfläche zum Auswählen des Speicherorts, nicht auf das Speicherortsymbol.

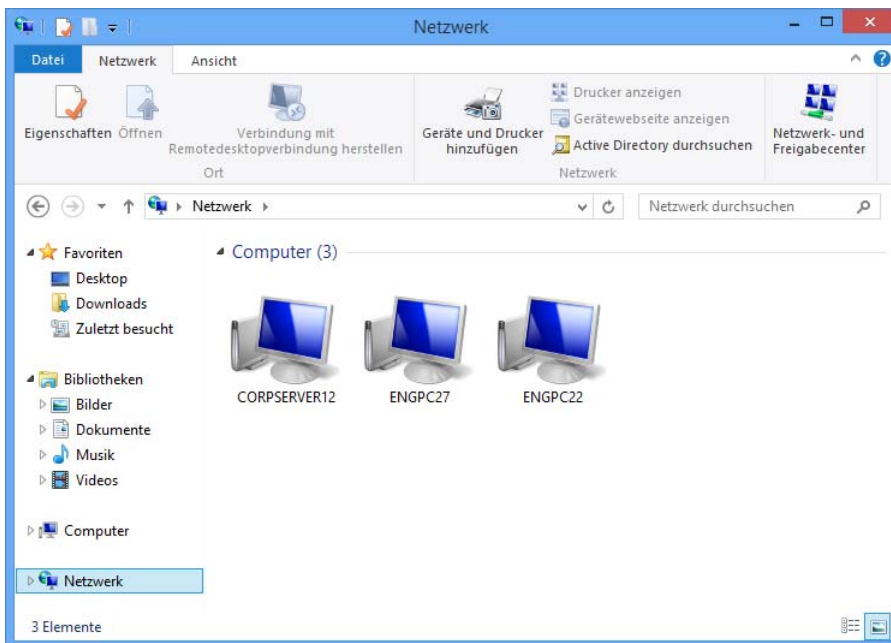


Abbildung 15.1 Im Netzwerk-Explorer können Sie die Netzwerkerkennung aktivieren und Netzwerkressourcen sehen, soweit es die aktuelle Konfiguration zulässt

Die Netzwerkerkennungseinstellungen für den Computer legen fest, welche Computer und Geräte im Netzwerk-Explorer aufgelistet werden. Ist die Netzwerkerkennung aktiviert, bekommen Sie die anderen Computer im Netzwerk angezeigt (Abbildung 15.1). Ist die Netzwerkerkennung gesperrt, sehen Sie in der Infoleiste des Netzwerk-Explorers einen entsprechenden Hinweis. Wenn Sie diese Warnmeldung antippen oder anklicken und dann *Netzwerkerkennung und Dateifreigabe aktivieren* wählen, wird die Netzwerkerkennung aktiviert und in der Windows-Firewall werden die entsprechenden Ports geöffnet, damit die Netzwerkerkennung funktioniert. Sofern noch keine Änderungen vorgenommen wurden, die sich auf die Netzwerkerkennung auswirken, befindet sich der Computer in einem Zustand, in dem er andere Computer und Geräte erkennt. Die Freigabe von Druckern, Dateien und Medien muss zusätzlich konfiguriert werden, wie in Kapitel 13, »Verwalten der Dateisicherheit und Ressourcenfreigabe«, besprochen.

Sofern Sie über die erforderlichen Berechtigungen verfügen, können Sie jeden Computer und jedes Gerät, das im Netzwerk-Explorer zu sehen ist, näher untersuchen. Tippen oder klicken Sie doppelt auf das Symbol eines Computers, wenn Sie auf seine freigegebenen Ressourcen zugreifen möchten. Tippen oder klicken Sie doppelt auf das Symbol eines Geräts, wenn Sie auf seine Verwaltungsschnittstelle zugreifen oder seine Ressourcen untersuchen möchten.

Auf der Symbolleiste des Netzwerk-Explorers finden Sie mehrere Optionen:

- **Netzwerk- und Freigabecenter** Wenn Sie den Netzwerkstatus anzeigen oder Netzwerkeinstellungen verwalten möchten, öffnet das Anklicken oder Antippen von *Netzwerk- und Freigabecenter* das Netzwerk- und Freigabecenter. Mehr dazu im nächsten Abschnitt, »Verwenden des Netzwerk- und Freigabecenters«.
- **Geräte und Drucker hinzufügen** Startet den Assistenten *Gerät hinzufügen*, mit dem Sie lokale oder Netzwerkdrucker, drahtlos vernetzte Drucker oder Bluetooth-Drucker installieren oder Drahtlosgeräte anschließen können, die zwar erkannt, aber noch nicht konfiguriert wurden.
- **Active Directory durchsuchen** Öffnet ein *Suchen*-Dialogfeld, in dem Sie Active Directory nach Benutzern, Kontakten, Gruppen, Computern, Druckern, freigegebenen Ordnern und anderen Elementen durchsuchen können (nur in Domänen).

Verwenden des Netzwerk- und Freigabecenters

Das Netzwerk- und Freigabecenter (Abbildung 15.2) zeigt einen Überblick über die aktuelle Netzwerkkonfiguration und den Netzwerkstatus an. In der Systemsteuerung können Sie das Netzwerk- und Freigabecenter öffnen, indem Sie unter *Netzwerk und Internet* auf *Netzwerkstatus und -aufgaben anzeigen* tippen oder klicken.

Das Netzwerk- und Freigabecenter listet die momentan aktiven Netzwerke mit ihrem Namen auf und bietet einen Überblick über die Netzwerke. Die Netzwerknamen werden fett angezeigt. Der Wert unter einem Netzwerknamen verrät die Kategorie des Netzwerks: Es gibt Domänennetzwerke, private Netzwerke und öffentliche Netzwerke. Der Zugriffstyp gibt an, ob und wie der Computer mit dem Netzwerk verbunden ist. Mögliche Werte für den Zugriffstyp sind *Kein Netzwerkzugriff*, *Kein Internetzugriff* oder *Internet*. Wenn Sie auf den Namen einer Netzwerkverbindung tippen oder klicken, wird das entsprechende *Status*-Dialogfeld geöffnet.

Wenn Sie auf *Adaptereinstellungen ändern* tippen oder klicken, öffnet sich die Seite *Netzwerkverbindungen*, auf der Sie Netzwerkverbindungen verwalten. Um die Freigabe zu konfigurieren, tippen oder klicken Sie auf *Erweiterte Freigabeeinstellungen ändern*. Daraufhin werden Optionen zum Konfigurieren der Freigabe- und Netzwerkerkennungseinstellungen für jedes Netzwerkprofil angezeigt. Sie verwalten ein Profil, indem Sie den entsprechenden Abschnitt durch Antippen oder Anklicken der Pfeilschaltfläche öffnen, die gewünschten Einstellungen wählen und schließlich auf *Änderungen speichern* tippen oder

klicken. Sie schalten die Netzwerkerkennung ein oder aus, indem Sie die Option *Netzwerkerkennung einschalten* oder *Netzwerkerkennung ausschalten* wählen und dann auf *Änderungen speichern* tippen oder klicken.

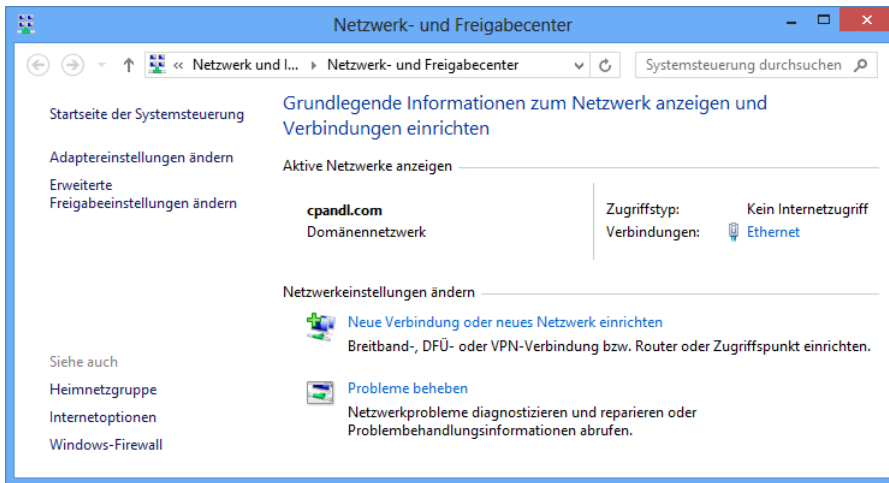


Abbildung 15.2 Verwenden Sie das *Netzwerk- und Freigabecenter* zur Anzeige des Netzwerkstatus und von Netzwerkdetails

Im Netzwerk- und Freigabecenter haben Sie auch die Möglichkeit, ein Netzwerkproblem zu untersuchen. Tippen oder klicken Sie dazu auf *Probleme beheben* und dann auf das Problembehandlungsmodul, das Sie ausführen wollen, zum Beispiel *Eingehende Verbindungen* oder *Netzwerkadapter*. Folgen Sie anschließend den Anweisungen, während die Windows-Netzwerkd Diagnose versucht, das Netzwerkproblem zu identifizieren und eine mögliche Lösung vorzuschlagen.

Installieren der Netzwerkkomponenten

Wenn Sie einen Computer vernetzen möchten, müssen Sie die TCP/IP-Komponenten und einen Netzwerkadapter installieren. Windows 8 verwendet TCP/IP als Standardprotokoll für WAN-Verbindungen (Wide Area Network). Die Netzwerkkomponenten werden normalerweise bereits bei der Installation von Windows 8 installiert. Sie können die TCP/IP-Komponenten aber auch über Eigenschaften von Netzwerkverbindungen installieren.

Verwenden von TCP/IP und des dualen IP-Stacks

Die Protokolle TCP und IP ermöglichen Computern die Kommunikation über verschiedene Netzwerke und über das Internet. Dafür sind allerdings Netzwerkadapter erforderlich, sei es eine herkömmliche, fest eingebaute Netzwerkadapterkarte, ein USB-Netzwerkadapter, ein PC-Card-Adapter oder ein Adapter, der bereits auf dem Mainboard integriert ist. Windows 8 verfügt über eine duale IP-Schichtenarchitektur, in der die beiden Protokolle Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6) implementiert sind, die die Transport- und Frame-Schichten gemeinsam nutzen.

IPv4 und IPv6 werden auf sehr unterschiedliche Weise verwendet. IPv4 arbeitet mit 32-Bit-Adressen und ist in den meisten Netzwerken die Hauptversion, die von IP verwendet wird, auch im Internet. IPv6 arbeitet mit 128-Bit-Adressen und stellt die nächste Generation von IP dar.

Die 32-Bit-Adressen von IPv4 werden gewöhnlich in Form von vier Dezimalzahlen ausgedrückt, wie zum Beispiel 127.0.0.1 oder 192.168.1.20. Die vier Dezimalzahlen werden auch Oktette genannt, weil sie jeweils 8 Bits der 32-Bit-Zahl darstellen. Bei IPv4-Standardunicastadressen stellt ein variabler Teil der IP-Adresse die Netzwerkkennung dar, und ein zweiter, ebenfalls variabler Teil der IP-Adresse ist die Hostkennung. Es gibt keinen festen Zusammenhang zwischen der IPv4-Adresse eines Hosts und der internen Maschinenadresse (MAC), die vom Netzwerkadapter des Hosts verwendet wird.

Die 128-Bit-Adressen von IPv6 werden in acht 16-Bit-Blöcke aufgeteilt, die jeweils durch einen Doppelpunkt voneinander getrennt sind. Jeder 16-Bit-Block wird hexadezimal dargestellt. Bei IPv6-Standardunicastadressen stellen die ersten 64 Bits die Netzwerkkennung dar und die zweiten 64 Bits die Netzwerkschnittstelle. Eine IPv6-Adresse könnte beispielsweise so aussehen:

FEC0:0:0:02BC:FF:BECB:FE4F:961D

Da viele Blöcke einer IPv6-Adresse 0 sind, werden aufeinanderfolgende Nullblöcke auch in der Form »::« angegeben. (Die Amerikaner nennen diese Schreibweise »double-colon«-Notation.) Die beiden Nullblöcke aus der obigen Adresse werden bei dieser Schreibweise folgendermaßen komprimiert:

FEC0::02BC:FF:BECB:FE4F:961D

Gibt es drei oder mehr Nullblöcke, werden sie in derselben Weise komprimiert. Aus FFE8:0:0:0:0:0:1 wird dann zum Beispiel FFE8::1.

Wird bei der Installation des Betriebssystems Netzwerkhardware erkannt, werden IPv4 und IPv6 standardmäßig aktiviert. Sie brauchen keine Komponente nachträglich zu installieren, um IPv6 zur Verfügung zu haben. Die IP-Architektur von Windows 8 wird *Dual-TCP/IP-Stack* genannt. Tabelle 15.1 beschreibt die wichtigsten TCP/IP-Funktionen, die im Dual-TCP/IP-Stack implementiert sind. Tabelle 15.2 beschreibt die wichtigsten TCP/IP-Funktionen für IPv6.

Tabelle 15.1 Wichtige TCP/IP-Funktionen im Dual-TCP/IP-Stack

Unterstützte Funktion	Beschreibung
Automatische Anpassung des Empfängerfensters	Optimiert TCP-Übertragungen für den Host, der die Daten empfängt, abhängig von den aktuellen Netzwerkbedingungen durch eine automatische Größenanpassung der Speicherpuffer (die »Empfängerfenster«), die für die eintreffenden Daten verwendet werden.
Automatische Erkennung von Black-Hole-Routern	Verhindert, dass TCP-Verbindungen beendet werden, weil zwischengeschaltete Router einfach große TCP-Segmente, erneute Übertragungen oder Fehlermeldungen verwerfen.
Automatische erneute Versuche, wenn das Gateway nicht reagiert	Sorgt dafür, dass ein nicht erreichbares Gateway regelmäßig daraufhin überprüft wird, ob es wieder verfügbar ist.
Erholung/Wiederherstellung nach Verlusten mit SACK-Informationen	Ermöglicht die Verwendung von SACK-Informationen zur Erholung nach Datenverlusten, wenn doppelte Bestätigungen empfangen wurden, und zur schnelleren Erholung, wenn mehrere Segmente nicht beim Empfänger eingetroffen sind.
Erkennung nicht erreichbarer Nachbarknoten für IPv4	Erkennt, wenn benachbarte Knoten und Router nicht mehr erreichbar sind, und informiert darüber.
Erweiterte selektive Bestätigungen	Erweitert die Art, wie selektive Bestätigungen (SACKs) verwendet werden. Ermöglicht einem Empfänger die Bestätigung des Empfangs von bis zu vier nicht aufeinanderfolgenden Datenblöcken und die Bestätigung von doppelten Paketen. Das erleichtert dem Sender die Überprüfung, ob er ein Segment unnötig erneut übertragen hat, und die Anpassung seines Verhaltens, um unnötige erneute Übertragungen zu vermeiden. ►

Unterstützte Funktion	Beschreibung
Erweiterte TCP-Daten	Unterstützt die Diagnose, ob der Flaschenhals bei einer Verbindung die sendende Anwendung ist, die Empfängeranwendung oder das Netzwerk.
Modifizierter schneller Wiederherstellungsalgorithmus	Bietet einen höheren Durchsatz, weil der Sender die Übertragungsrate auf andere Weise erhöhen kann, wenn in einem Datenfenster mehrere Segmente verloren gehen und der Sender eine Bestätigung erhält, aus der hervorgeht, dass nur ein Teil der Daten empfangen wurde.
Netzwerkd Diagnose-Framework	Bietet ein erweiterbares Framework, das Benutzer bei der Behebung von Problemen mit Netzwerkverbindungen unterstützt.
Routingfächer	Verhindert die unerwünschte Weiterleitung von Daten zwischen Schnittstellen durch die Zuordnung einer Schnittstelle oder mehrerer Schnittstellen zu einer Anmeldesitzung, die über eigene Routingtabellen verfügt.
Übertragungswiederholungs-Timeout-Erkennung	Nimmt bei plötzlichen, temporären Erhöhungen der Übertragungswiederholungs-Timeouts Korrekturen vor und verhindert eine unnötige erneute Übertragung von Segmenten.
Verbund-TCP	Optimiert TCP-Übertragungen für den sendenden Host durch eine Vergrößerung der Datenmenge, die über eine Verbindung übertragen wird, wobei dafür gesorgt wird, dass andere TCP-Verbindungen nicht beeinträchtigt werden.
Windows-Filterplattform	Bietet APIs für die Erweiterung der TCP/IP-Filterarchitektur, die somit neue Funktionen unterstützen kann.

Tabelle 15.2 Wichtige Funktionen des Dual-TCP/IP-Stacks für IPv6

Unterstützte Funktion	Beschreibung
DHCPv6-fähiger DHCP-Client	Erweitert den DHCP-Client, damit er IPv6 unterstützt und eine zustandsbehaftete automatische Adressenkonfiguration mit einem DHCPv6-Server ermöglicht.
IP Security	Erlaubt die Verwendung von Internet Key Exchange (IKE) und Datenverschlüsselung für IPv6.
IPv6 über Point-to-Point-Protokoll (PPPv6)	Erlaubt IPv6-Übermittlungen über Verbindungen auf PPP-Basis. Das wiederum ermöglicht Remoteclients die Verbindung mit einem Internet Service Provider (ISP) auf IPv6-Basis über Wählverbindungen oder PPPoE-Verbindungen (PPP over Ethernet).
Multicast Listener Discovery Version 2 (MLDv2)	Bietet Unterstützung für quellspezifische Multicastübertragungen und entspricht dem Internet Group Management Protocol Version 3 (IGMPv3) für IPv4.
Symmetrische Netzwerkadressen-übersetzung	Ordnet die interne (private) Adresse und Portnummer verschiedenen externen (öffentlichen) Adressen und Ports zu, je nach der externen Zieladresse.
Verbindungslokale Multicast-Namensauflösung (Link-Local Multicast Name Resolution, LLMNR)	Erlaubt IPv6-Hosts im selben Subnetz die gegenseitige Namensauflösung ohne DNS-Server.
Zufällige Schnittstellenkennungen	Verhindert das Scannen von IPv6-Adressen auf der Basis der bekannten Firmenkennungen der Netzwerkadapterhersteller. Standardmäßig generiert Windows 8 für nichttemporäre automatisch konfigurierte IPv6-Adressen zufällige Schnittstellenkennungen, auch für öffentliche und verbindungslokale Adressen.

Installieren von Netzwerkadaptern

Netzwerkadapter sind Hardwaregeräte, die zur Kommunikation in Netzwerken verwendet werden. Sie können Netzwerkadapter folgendermaßen installieren und einstellen:

1. Folgen Sie den Anweisungen des Herstellers. Vielleicht müssen Sie mit der mitgelieferten Software die Interrupt- oder Porteinstellung des Adapters ändern.
2. Wenn Sie eine interne Netzwerkkarte installieren, fahren Sie den Computer herunter, schalten ihn aus, trennen ihn vom Strom und installieren die Adapterkarte in einem passenden Steckplatz des Computers. Wenn Sie fertig sind, bauen Sie alles wieder zusammen, verbinden den Computer mit der Stromversorgung und schalten ihn ein.
3. Windows 8 sollte den neuen Adapter beim Start erkennen. Wenn Sie über eine separate Treiber-CD für den Adapter verfügen, sollten Sie die CD nun einlegen. Andernfalls werden Sie vielleicht dazu aufgefordert, eine CD mit passenden Treibern einzulegen.
4. Falls Windows 8 den Adapter nicht automatisch erkennt, folgen Sie den Installationsbeschreibungen im Abschnitt »Arbeiten mit Gerätetreibern« in Kapitel 9, »Verwalten von Hardwaregeräten und Treibern«.
5. Wenn keine Netzwerkdienste auf dem Computer installiert sind, installieren Sie die Dienste, wie im nächsten Abschnitt beschrieben.

Installieren der Netzwerkdienste (TCP/IP)

Falls Sie TCP/IP nach der Installation von Windows 8 nachträglich installieren, melden Sie sich mit einem Administratorkonto auf dem Computer an und gehen folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im Netzwerk- und Freigabecenter unter *Aktive Netzwerke anzeigen* auf den Link für die Netzwerkverbindung.

TIPP

Ist die Netzwerkverbindung, die Sie bearbeiten wollen, nicht aktiv, können Sie auf *Adaptereinstellungen ändern* tippen oder klicken. Klicken Sie dann im Fenster *Netzwerkverbindungen* mit der rechten Maustaste auf die Verbindung, die Sie bearbeiten wollen, oder halten Sie sie gedrückt, und wählen Sie den Befehl *Eigenschaften*.

3. Tippen oder klicken Sie im Dialogfeld *Status* auf *Eigenschaften*. Daraufhin öffnet sich das Eigenschaftendialogfeld für die Verbindung, in dem die Registerkarte *Netzwerk* ausgewählt ist (Abbildung 15.3).
4. Sofern *Internetprotokoll Version 6 (TCP/IPv6)*, *Internetprotokoll Version 4 (TCP/IPv4)* oder beide nicht in der Liste der installierten Komponenten aufgeführt sind, müssen Sie diese Komponenten installieren. Tippen oder klicken Sie dazu auf *Installieren*, dann auf *Protokoll* und auf *Hinzufügen*. Wählen Sie im Dialogfeld *Netzwerkprotokoll auswählen* das Protokoll aus, das Sie installieren wollen, und tippen oder klicken Sie auf *OK*. Wiederholen Sie diesen Schritt, wenn Sie sowohl TCP/IPv6 als auch TCP/IPv4 installieren müssen.
5. Stellen Sie im Eigenschaftendialogfeld der Netzwerkverbindung sicher, dass folgende Elemente aktiviert sind: *Internetprotokoll Version 6 (TCP/IPv6)*, *Internetprotokoll Version 4 (TCP/IPv4)* oder beide. Tippen oder klicken Sie auf *OK*.
6. Folgen Sie bei Bedarf der Anleitung im nächsten Abschnitt, um die Netzwerkverbindungen für den Computer zu konfigurieren.

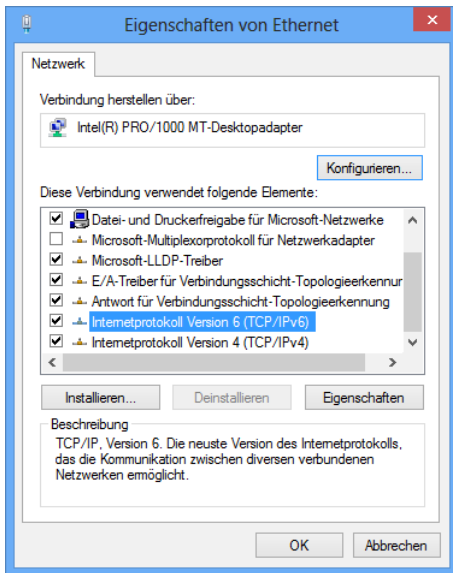


Abbildung 15.3 TCP/IP installieren und konfigurieren
Sie im Eigenschaftendialogfeld einer Netzwerkverbindung

Konfigurieren von Netzwerkverbindungen

Eine Netzwerkverbindung wird automatisch erstellt, wenn ein Computer über einen Netzwerkadapter verfügt und mit einem Netzwerk verbunden ist. Sind mehrere Netzwerkadapter im Computer installiert und ist der Computer mit einem Netzwerk verbunden, so wird für jeden Adapter eine Netzwerkverbindung angelegt. Ist keine Netzwerkverbindung verfügbar, sollten Sie den Computer mit einem Netzwerk verbinden oder eine andere Verbindungsart erstellen, wie im Abschnitt »Verwalten von Netzwerkverbindungen« weiter unten in diesem Kapitel beschrieben.

Computer verwenden IP-Adressen für die Kommunikation über TCP/IP. Unter Windows 8 lassen sich IP-Adressen auf folgende Weise einstellen:

- **Manuell** IP-Adressen, die manuell zugewiesen werden, nennt man *statische IP-Adressen*. Statische IP-Adressen sind fest und ändern sich nicht, solange Sie es nicht tun. Gewöhnlich weisen Sie Windows-Servern statische IP-Adressen zu. Wenn Sie das tun, müssen Sie noch weitere Angaben machen, damit der Server im Netzwerk kommunizieren kann.
- **Dynamische** Dynamische IP-Adressen werden beim Start eines Computers von einem DHCP-Server zugewiesen, sofern es im Netzwerk einen DHCP-Server gibt. Diese Adressen können sich im Lauf der Zeit ändern. Dynamische IP-Adressierung ist die Standardkonfiguration.
- **Alternativ (nur IPv4)** Wenn ein Computer auf die Verwendung von DHCPv4 eingestellt ist und kein DHCPv4-Server verfügbar ist, weist Windows 8 automatisch eine alternative private IP-Adresse zu. Standardmäßig liegt diese alternative IPv4-Adresse im Bereich von 169.254.0.1 bis 169.254.255.254, wobei die Subnetzmaske 255.255.0.0 ist. Sie können auch eine benutzerdefinierte alternative IPv4-Adresse angeben, was für Notebookbenutzer besonders nützlich ist.

Konfigurieren statischer IP-Adressen

Wenn Sie eine statische IP-Adresse zuweisen möchten, müssen Sie dem Computer die IP-Adresse mitteilen, die er verwenden soll, sowie die Subnetzmaske für diese IP-Adresse und bei Bedarf auch das Standardgateway, das für die Internetkommunikation verwendet werden soll. Eine IP-Adresse ist eine numerische Kennung für einen Computer. Das IP-Adressierungsschema hängt von der Konfiguration eines Netzwerks ab. Gewöhnlich werden IP-Adressen so vergeben, dass sich bestimmte Netzwerksegmente ergeben.

IPv6-Adressen und IPv4-Adressen unterscheiden sich sehr voneinander, wie im Abschnitt »Verwenden von TCP/IP und des dualen IP-Stacks« weiter oben in diesem Kapitel beschrieben. In IPv6 stellen die ersten 64 Bits die Netzwerkennung dar und die übrigen 64 Bits die Netzwerkschnittstelle. In IPv4 stellt eine variable Anzahl von Anfangsbits die Netzwerkennung dar und die verbleibenden Bits die Hostkennung. Wenn Sie zum Beispiel mit IPv4 auf einem Computer im Netzwerksegment 10.0.10.0 mit der Subnetzmaske 255.255.255.0 arbeiten, bilden die ersten drei Bytes die Netzwerkennung. Diese eindeutige Netzwerkennung lautet 10.0.10.0. Der für Computerhosts verfügbare Adressenbereich reicht von 10.0.10.1 bis 10.0.10.254. Die Adresse 10.0.10.255 ist für Netzwerk-Broadcasts reserviert.

Wenn Sie in einem privaten Netzwerk arbeiten, das direkt mit dem Internet verbunden ist, sollten Sie private IPv4-Adressen verwenden. Tabelle 15.3 listet die privaten IPv4-Netzwerkadressen auf.

Tabelle 15.3 Private IPv4-Netzwerkadressen

Private Netzwerk- kennung	Subnetz- maske	Verfügbarer IP-Adressbereich	Broadcast- adresse
10.0.0.0	255.0.0.0	10.0.0.0–10.255.255.254	10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0–172.31.255.254	172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0–192.168.255.254	192.168.255.255

Alle anderen IPv4-Netzwerkadressen sind öffentlich und müssen gemietet oder gekauft werden. Wenn das Netzwerk direkt mit dem Internet verbunden ist und Sie von Ihrem Internetprovider einen IPv4-Adressenbereich erhalten haben, können Sie diese IPv4-Adressen verwenden.

Überprüfen einer Adresse mit dem Ping-Befehl

Bevor Sie eine statische IP-Adresse vergeben, sollten Sie überprüfen, ob die Adresse bereits verwendet wird oder für DHCP reserviert ist. Mit dem Befehl Ping finden Sie heraus, ob eine Adresse verwendet wird. Öffnen Sie eine Eingabeaufforderung und geben Sie **ping** ein, gefolgt von der IP-Adresse, die Sie überprüfen möchten.

Um die IPv4-Adresse 10.0.10.12 zu testen, würden Sie folgenden Befehl verwenden:

```
ping 10.0.10.12
```

Um die IPv6-Adresse FEC0::02BC:FF:BECB:FE4F:961D zu testen, würden Sie folgenden Befehl verwenden:

```
ping FEC0::02BC:FF:BECB:FE4F:961D
```

Wenn Sie von Ping eine Erfolgsmeldung erhalten, ist die IP-Adresse in Gebrauch und Sie sollten eine andere wählen. Ergibt sich bei allen vier Versuchen, die Ping durchführt, eine Zeitüberschreitung, ist die IP-Adresse gerade nicht im Netzwerk aktiv und wird vermutlich nicht verwendet. Allerdings kann eine Firewall Ihre Ping-Anfragen blocken. Außerdem sollte der zuständige Netzwerkadministrator Ihnen sagen können, ob eine IP-Adresse verwendet wird.

Konfigurieren statischer IPv4- oder IPv6-Adressen

Für jeden installierten Netzwerkadapter ist eine Netzwerkverbindung verfügbar. Diese Verbindungen werden automatisch erstellt. Um für eine bestimmte Verbindung eine statische IP-Adresse einzustellen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im Netzwerk- und Freigabecenter unter *Aktive Netzwerke anzeigen* auf den Link für die Netzwerkverbindung.
3. Tippen oder klicken Sie im *Status*-Dialogfeld der Netzwerkverbindung auf *Eigenschaften*. Dadurch öffnet sich das Eigenschaftendialogfeld der Netzwerkverbindung.
4. Tippen oder klicken Sie doppelt auf *Internetprotokoll Version 6 (TCP/IPv6)* oder *Internetprotokoll Version 4 (TCP/IPv4)*, je nachdem, welche Art von IP-Adresse Sie konfigurieren wollen.
5. Bei einer IPv6-Adresse tun Sie Folgendes:
 - Tippen oder klicken Sie auf *Folgende IPv6-Adresse verwenden* und geben Sie dann im Textfeld *IPv6-Adresse* die IPv6-Adresse ein. Die IPv6-Adresse, die Sie dem Computer geben, darf im Netzwerk noch nicht verwendet werden.
 - Das Feld *Subnetzpräfixlänge* ist erforderlich, damit der Computer im Netzwerk kommunizieren kann. Windows 8 sollte im Textfeld *Subnetzpräfixlänge* einen Standardwert vorgeben. Wenn das Netzwerk keine variablen Längen für Subnetzpräfixe verwendet, sollte der Standardwert ausreichen. Aber wenn die Subnetzpräfixlänge variabel ist, sollten Sie den Wert so einstellen, wie es für Ihr Subnetz erforderlich ist.
6. Bei einer IPv4-Adresse tun Sie Folgendes:
 - Tippen oder klicken Sie auf *Folgende IP-Adresse verwenden* und geben Sie im Feld *IP-Adresse* die IPv4-Adresse ein. Die IPv4-Adresse, die Sie dem Computer zuweisen, darf im Netzwerk noch nicht verwendet werden.
 - Das Feld *Subnetzmaske* ist erforderlich, damit der Computer im Netzwerk kommunizieren kann. Windows 8 sollte im Textfeld *Subnetzmaske* einen Standardwert vorgeben. Wenn das Netzwerk keine Subnetze variabler Länge verwendet, sollte der Standardwert ausreichen. Andernfalls sollten Sie den Wert so einstellen, wie es für Ihr Subnetz erforderlich ist.
7. Wenn der Computer Zugriff auf andere TCP/IP-Netzwerke, das Internet oder andere Subnetze braucht, legen Sie ein Standardgateway fest. Geben Sie im Textfeld *Standardgateway* die IP-Adresse des Standardrouters des Netzwerks ein.
8. DNS wird für die Namenszuordnung verwendet. Geben Sie in den entsprechenden Textfeldern die Adressen des bevorzugten DNS-Servers und eines zweiten DNS-Servers ein, sofern vorhanden.
9. Wenn Sie fertig sind, tippen oder klicken Sie zweimal auf *OK* und einmal auf *Schließen*. Wiederholen Sie diesen Vorgang für alle anderen Netzwerkadapter und IP-Protokolle, die Sie konfigurieren möchten.
10. Für IPv4-Adressen konfigurieren Sie bei Bedarf WINS, wie im Abschnitt »Konfigurieren der WINS-Namenszuordnung« weiter unten in diesem Kapitel beschrieben.

Konfigurieren dynamischer und alternativer IP-Adressen

Auf Arbeitsstationen lassen sich zwar auch statische IP-Adressen einsetzen, aber die meisten Arbeitsstationen verwenden dynamische oder alternative Adressen oder beides. Sie konfigurieren dynamische und alternative Adressen auf folgende Weise:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im Netzwerk- und Freigabecenter unter *Aktive Netzwerke anzeigen* auf den Link für die Netzwerkverbindung.
3. Tippen oder klicken Sie im *Status*-Dialogfeld der Netzwerkverbindung auf *Eigenschaften*. Dadurch öffnet sich das Eigenschaftendialogfeld der Netzwerkverbindung.

HINWEIS

Im *Status*-Dialogfeld der Netzwerkverbindung wird für jeden installierten Netzwerkadapter eine Netzwerkverbindung angezeigt. Diese Verbindungen werden automatisch erstellt. Wenn Sie für einen bestimmten Adapter keine Netzwerkverbindung sehen, überprüfen Sie den Treiber für diesen Adapter. Vielleicht wurde er nicht korrekt installiert.

4. Tippen oder klicken Sie doppelt auf *Internetprotokoll Version 6 (TCP/IPv6)* oder *Internetprotokoll Version 4 (TCP/IPv4)*, je nachdem, welchen Typ IP-Adresse Sie konfigurieren.
5. Wählen Sie *IPv6-Adresse automatisch beziehen* beziehungsweise *IP-Adresse automatisch beziehen*, je nachdem, welchen Typ IP-Adresse Sie konfigurieren. Wählen Sie bei Bedarf *DNS-Serveradresse automatisch beziehen*. Oder wählen Sie *Folgende DNS-Serveradressen verwenden* und geben Sie dann in den entsprechenden Textfeldern die Adressen des bevorzugten DNS-Servers und eines zweiten DNS-Servers ein, sofern vorhanden.
6. Wenn Sie auf Desktopcomputern dynamische IPv4-Adressen verwenden, sollten Sie auch noch eine automatische alternative Adresse konfigurieren. Dazu wählen Sie auf der Registerkarte *Alternative Konfiguration* die Option *Automatisch zugewiesene, private IP-Adresse*. Tippen oder klicken Sie auf die OK-Schaltflächen der beiden geöffneten Dialogfelder, tippen oder klicken Sie auf *Schließen* und überspringen Sie die restlichen Schritte.
7. Wenn Sie auf mobilen Computern dynamische IPv4-Adressen verwenden, werden Sie die alternative Adresse gewöhnlich manuell einstellen. Wählen Sie dazu auf der Registerkarte *Alternative Konfiguration* die Option *Benutzerdefiniert*. Geben Sie dann im Textfeld *IP-Adresse* die IP-Adresse ein, die Sie verwenden möchten. Bei der IP-Adresse, die Sie dem Computer zuweisen, sollte es sich um eine private IP-Adresse handeln, wie in Tabelle 15.3 beschrieben. Die Adresse darf im Netzwerk noch nicht in Gebrauch sein, wenn Sie die neuen Einstellungen übernehmen.
8. Vervollständigen Sie die Einstellung der alternativen Konfiguration für dynamische IPv4-Adressen durch die Eingaben für Subnetzmaske, Standardgateway, DNS und WINS. Wenn Sie fertig sind, tippen oder klicken Sie zweimal auf OK und dann auf *Schließen*.

HINWEIS

Ausführlichere Informationen über die Konfiguration von Notebooks finden Sie im Abschnitt »Konfigurieren des Netzwerks auf mobilen Geräten« in Kapitel 16, »Verwalten von mobilen Netzwerken und Remotezugriff«.

Konfigurieren mehrerer Gateways

Um für eine gewisse Fehlertoleranz beim Ausfall eines Routers zu sorgen, können Sie Windows 8-Computer so konfigurieren, dass sie mehrere Standardgateways verwenden. Werden mehrere Gateways eingesetzt, entscheidet Windows 8 anhand der Gatewaymetrik, welches Gateway verwendet wird. Die Gatewaymetrik ist ein Maß für die Routingkosten, die bei der Verwendung eines Gateways entstehen. Das Gateway mit den geringsten Kosten (der kleinsten Gatewaymetrik) wird zuerst verwendet. Ist keine Kommunikation mit diesem Gateway möglich, versucht Windows 8 es mit dem Gateway, das die zweitniedrigsten Kosten verursacht.

Wie mehrere Gateways am besten konfiguriert werden, hängt vom Aufbau Ihres Netzwerks ab. Wenn die Computer DHCP verwenden, werden Sie die zusätzlichen Gateways wahrscheinlich im DHCP-Server einstellen. Verwenden die Computer statische IP-Adressen oder wollen Sie die Gateways in bestimmter Weise festlegen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im Netzwerk- und Freigabecenter unter *Aktive Netzwerke anzeigen* auf den Link für die Netzwerkverbindung.
3. Tippen oder klicken Sie im *Status*-Dialogfeld der Netzwerkverbindung auf *Eigenschaften*. Dadurch öffnet sich das Eigenschaftendialogfeld der Netzwerkverbindung.
4. Tippen oder klicken Sie doppelt auf *Internetprotokoll Version 6 (TCP/IPv6)* oder *Internetprotokoll Version 4 (TCP/IPv4)*, je nachdem, welchen Typ IP-Adresse Sie konfigurieren.
5. Tippen oder klicken Sie auf *Erweitert*, um das Dialogfeld *Erweiterte TCP/IP-Einstellungen* zu öffnen (Abbildung 15.4).

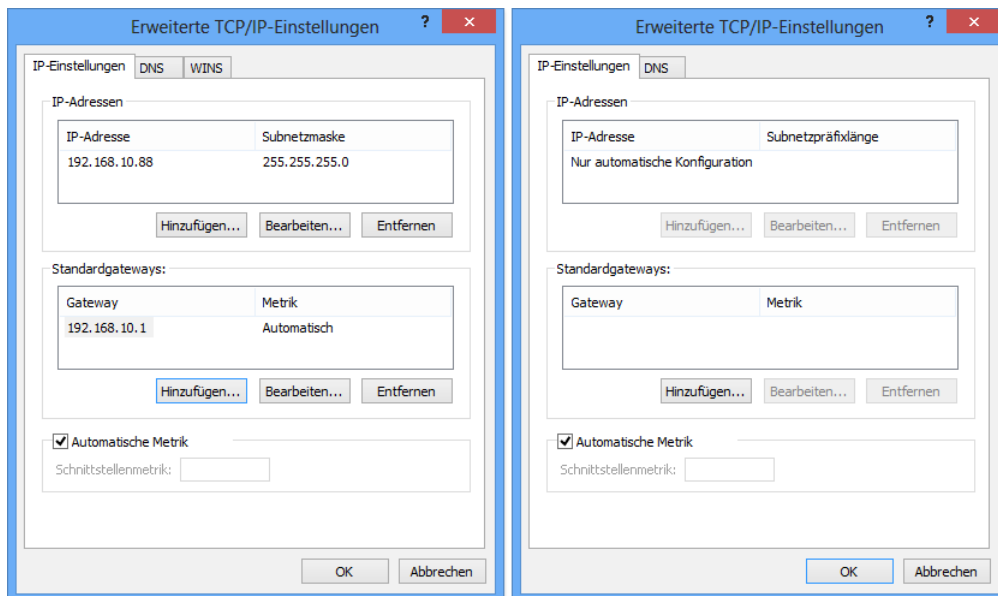


Abbildung 15.4 Verwenden Sie das Dialogfeld *Erweiterte TCP/IP-Einstellungen*, wenn Sie mehrere IP-Adressen und Gateways konfigurieren möchten (links die Version für IPv4, rechts die für IPv6)

6. Sofern bereits Gateways manuell konfiguriert wurden, werden sie unter *Standardgateways* angezeigt. Bei Bedarf können Sie zusätzliche Gateways eintragen. Tippen oder klicken Sie auf *Hinzufügen* und geben Sie im Textfeld *Gateway* die Gatewayadresse ein.
7. Standardmäßig weist Windows 8 dem Gateway automatisch eine Metrik zu. Sie können die Metrik auch manuell festlegen. Dazu löschen Sie das Kontrollkästchen *Automatische Metrik* und geben im Textfeld *Metrik* den gewünschten Wert ein.
8. Tippen oder klicken Sie auf *Hinzufügen* und wiederholen Sie die Schritte 6 und 7 für jedes Gateway, das Sie hinzufügen möchten.
9. Tippen oder klicken Sie dreimal auf *OK* und dann auf *Schließen*.

Konfigurieren der DNS-Auflösung

DNS ist ein Namensauflösungsdienst, der dazu dient, die IP-Adresse eines Computers zu ermitteln, von dem der Hostname bekannt ist. Dadurch sind Benutzer in der Lage, mit Hostnamen wie in *http://www.msn.com* oder *http://www.microsoft.com* zu arbeiten, statt IP-Adressen wie 192.168.5.102 oder 192.168.12.68 verwenden zu müssen. DNS ist der bevorzugte Namensdienst für Windows 8 und das Internet.

Wie bei Gateways hängt auch die beste Konfiguration von DNS davon ab, wie Ihr Netzwerk aufgebaut ist. Wenn die Computer DHCP verwenden, werden Sie DNS wahrscheinlich im DHCP-Server einstellen. Verwenden die Computer statische IP-Adressen oder wollen Sie DNS für einen einzelnen Benutzer oder ein einzelnes System festlegen, müssen Sie DNS manuell konfigurieren.

DNS-Grundeinstellungen

Die DNS-Grundeinstellungen können Sie folgendermaßen vornehmen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im Netzwerk- und Freigabecenter unter *Aktive Netzwerke anzeigen* auf den Link für die Netzwerkverbindung.
3. Tippen oder klicken Sie im *Status*-Dialogfeld der Netzwerkverbindung auf *Eigenschaften*. Dadurch öffnet sich das Eigenschaftendialogfeld der Netzwerkverbindung.
4. Tippen oder klicken Sie doppelt auf *Internetprotokoll Version 6 (TCP/IPv6)* oder *Internetprotokoll Version 4 (TCP/IPv4)*, je nachdem, welchen Typ IP-Adresse Sie konfigurieren.
5. Wenn der Computer DHCP verwendet und Sie die DNS-Serveradressen per DHCP zuweisen möchten, wählen Sie *DNS-Serveradresse automatisch beziehen*. Andernfalls wählen Sie *Folgende DNS-Serveradressen verwenden* und geben in den Textfeldern die Adressen des bevorzugten und des zweiten DNS-Servers ein, sofern vorhanden.
6. Tippen oder klicken Sie auf die *OK*-Schaltflächen der beiden geöffneten Dialogfelder und dann auf *Schließen*.

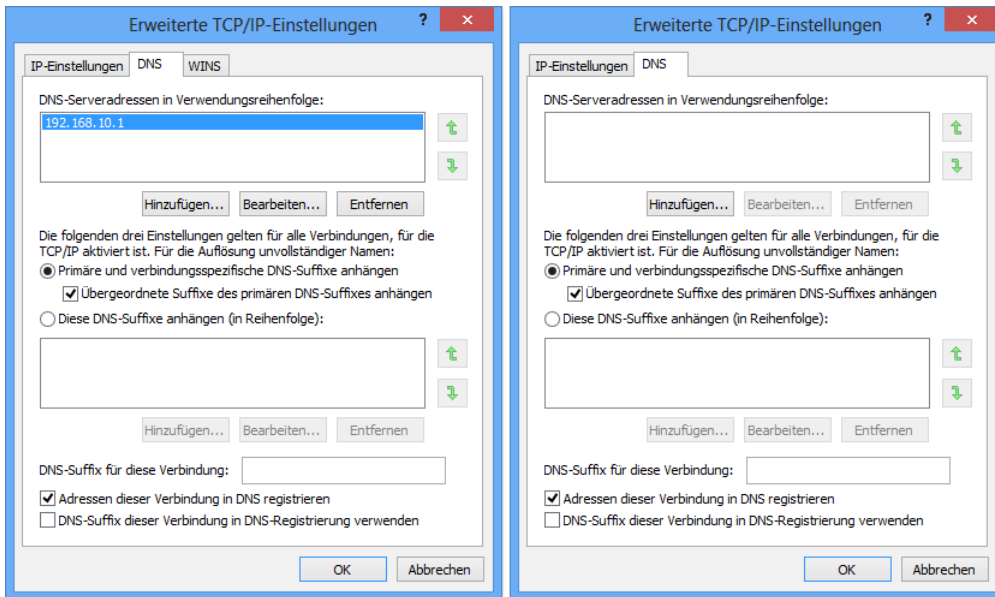


Abbildung 15.5 Verwenden Sie die Registerkarte *DNS* des Dialogfelds *Erweiterte TCP/IP-Einstellungen* für erweiterte DNS-Einstellungen (links die Version für IPv4, rechts die für IPv6)

Erweiterte DNS-Einstellungen

Erweiterte DNS-Einstellungen nehmen Sie auf der Registerkarte *DNS* des Dialogfelds *Erweiterte TCP/IP-Einstellungen* vor (Abbildung 15.5). Verwenden Sie die Felder der Registerkarte *DNS* folgendermaßen:

- **DNS-Serveradressen in Verwendungsreihenfolge** Geben Sie in diesem Bereich die IP-Adressen der DNS-Server an, die zur Domänennamensauflösung verwendet werden sollen. Tippen oder klicken Sie auf *Hinzufügen*, wenn Sie eine Server-IP-Adresse in die Liste eintragen möchten. Tippen oder klicken Sie auf *Entfernen*, um die ausgewählte Serveradresse aus der Liste zu entfernen. Tippen oder klicken Sie auf *Bearbeiten*, um den ausgewählten Eintrag zu bearbeiten. Sie können mehrere DNS-Server für die DNS-Auflösung angeben. Ihre Priorität ergibt sich aus der Reihenfolge in der Liste. Wenn der erste Server nicht auf eine Aufforderung zur Namensauflösung reagiert, wird der nächste Server aus der Liste verwendet, und so weiter. Wenn Sie die Position eines Servers in der Liste ändern möchten, wählen Sie ihn aus und verwenden dann eine der beiden Pfeilschaltflächen.
- **Primäre und verbindungspezifische DNS-Suffixe anhängen** Diese Option ist normalerweise vorgewählt. Verwenden Sie diese Option, um unvollständig angegebene Computernamen in der übergeordneten Domäne aufzulösen. Wird beispielsweise der Computername *Gandolf* angegeben und ist *microsoft.com* die übergeordnete Domäne, ergibt sich der vollständige Computername *gandolf.microsoft.com*. Ist der Computername in der übergeordneten Domäne nicht bekannt, schlägt die Abfrage fehl. Die übergeordnete Domäne ist die Domäne, die im Dialogfeld *Systemeigenschaften* auf der Registerkarte *Computernamen* angegeben ist. (Prüfen Sie diese Einstellungen, indem Sie in der Systemsteuerung auf *System und Sicherheit* und dann auf *System* tippen oder klicken.)
- **Übergeordnete Suffixe des primären DNS-Suffixes anhängen** Diese Option ist standardmäßig vorgewählt. Wählen Sie diese Option, um unvollständig angegebene Computernamen in der Domänenhierarchie aufzulösen. Schlägt eine Abfrage in der direkt übergeordneten Domäne fehl, wird das Suffix von deren übergeordneter Domäne für die Abfrage verwendet. Dieser Vorgang wiederholt sich so lange, bis die Spitze der DNS-Domänenhierarchie erreicht ist. Wird beispielsweise in der Domäne *dev*.

microsoft.com ein Computer namens *Gandolf* verwendet, würde DNS als Computernamen *gandolf.dev.microsoft.com* verwenden. Wenn das nicht funktioniert, würde DNS als Computernamen *gandolf.microsoft.com* verwenden.

- **Diese DNS-Suffixe anhängen (in Reihenfolge)** Wählen Sie diese Option, wenn Sie bestimmte DNS-Suffixe für die Namensauflösung vorgeben möchten, statt die Namen über die übergeordneten Domänen aufzulösen. Um ein Domänensuffix in die Liste einzutragen, tippen oder klicken Sie auf *Hinzufügen*. Wenn Sie einen Eintrag aus der Liste löschen möchten, wählen Sie ihn aus und tippen oder klicken auf *Entfernen*. Zur Bearbeitung eines ausgewählten Eintrags tippen oder klicken Sie auf *Bearbeiten*. Sie können mehrere Domänensuffixe angeben, die in der angegebenen Reihenfolge verwendet werden. Führt das erste Suffix zu keinem Ergebnis, verwendet DNS das nächste Suffix aus der Liste. Schlägt auch das fehl, wird das nächste Suffix verwendet, und so weiter. Wenn Sie die Reihenfolge der Domänensuffixe ändern möchten, wählen Sie ein Suffix aus und verwenden dann eine der beiden Pfeilschaltflächen, um die Position des Suffixes in der Liste zu ändern.
- **DNS-Suffix für diese Verbindung** Mit dieser Option legen Sie ein bestimmtes DNS-Suffix für die Verbindung fest, das Vorrang vor den DNS-Namen hat, die bereits für diese Verbindung konfiguriert wurden. Meist werden Sie den DNS-Domännennamen allerdings festlegen, indem Sie in der Systemsteuerung auf *System und Sicherheit* tippen oder klicken, dann auf *System* und schließlich auf *Einstellungen ändern*. Tippen oder klicken Sie im Dialogfeld *Systemeigenschaften* auf der Registerkarte *Computernamen* auf *Ändern* und dann auf *Weitere*. Nun können Sie das primäre DNS-Suffix für den Computer im entsprechenden Textfeld eingeben. Tippen oder klicken Sie dreimal auf *OK*, um Ihre Änderungen abzuspeichern.
- **Adressen dieser Verbindung in DNS registrieren** Wählen Sie diese Option, wenn alle IP-Adressen für diese Verbindung unter dem vollständig angegebenen Domännennamen des Computers in DNS registriert werden sollen. Standardmäßig ist die Option vorgewählt.

Dynamische DNS-Aktualisierungen werden im Zusammenhang mit DHCP verwendet, damit ein Client seinen A-Datensatz (Hostadresse) aktualisieren kann, falls sich seine IP-Adresse ändert, und damit der DHCP-Server den PTR-Datensatz (Pointer) für den Client auf dem DNS-Server aktualisieren kann. Der DHCP-Server kann auch so eingestellt werden, dass er die beiden A- und PTR-Datensätze für den Client aktualisiert. Dynamische DNS-Aktualisierungen werden erst auf DNS-Servern mit BIND 5.1 oder höher geboten sowie unter Microsoft Windows 2000 Server und neueren Windows-Versionen.
- **DNS-Suffix dieser Verbindung in DNS-Registrierung verwenden** Wählen Sie dies, wenn alle IP-Adressen für diese Verbindung unter der übergeordneten Domäne in DNS eingetragen werden sollen.

Konfigurieren der WINS-Namenszuordnung

Mit WINS setzen Sie NetBIOS-Computernamen in IPv4-Adressen um. Sie können WINS einsetzen, damit die Computer eines Netzwerks die Adressen anderer Computer aus dem Netzwerk bestimmen können. Wenn im Netzwerk ein WINS-Server installiert ist, übernimmt dieser die Zuordnung der Computernamen. WINS wird zwar auf allen Windows-Versionen unterstützt, aber unter Windows 8 gibt es WINS hauptsächlich aus Gründen der Abwärtskompatibilität zu früheren Windows-Versionen.

Sie können Windows 8-Computer auch so einstellen, dass sie NetBIOS-Computernamen mit der lokalen Datei *LMHOSTS* auflösen. Allerdings wird *LMHOSTS* nur berücksichtigt, wenn die normalen Methoden zur Namensauflösung fehlschlagen. In einem sauber konfigurierten Netzwerk wird diese Datei kaum verwendet. Die bevorzugte Methode zur Auflösung von NetBIOS-Computernamen ist WINS mit einem WINS-Server.

Wie bei Gateways und DNS hängt die beste Methode zur Konfiguration von WINS davon ab, wie Ihr Netzwerk aufgebaut ist. Wenn die Computer DHCP verwenden, werden Sie WINS wahrscheinlich im DHCP-Server einstellen. Verwenden die Computer statische IPv4-Adressen oder wollen Sie WINS für einen einzelnen Benutzer oder ein System festlegen, müssen Sie WINS manuell konfigurieren.

Sie können WINS folgendermaßen manuell einstellen:

1. Öffnen Sie das Dialogfeld *Erweiterte TCP/IP-Einstellungen* und tippen oder klicken Sie auf die Registerkarte *WINS*. Hier finden Sie das Feld *WINS-Adressen in Verwendungsreihenfolge* (Abbildung 15.6).

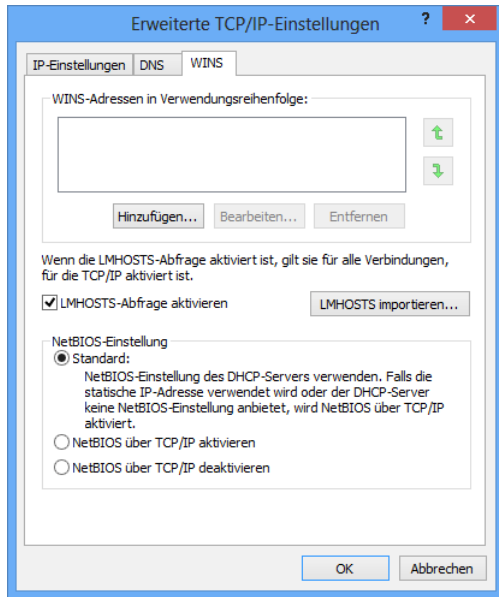


Abbildung 15.6 Verwenden Sie für IPv4 die Registerkarte *WINS* des Dialogfelds *Erweiterte TCP/IP-Einstellungen* zur Einstellung der WINS-Auflösung von NetBIOS-Computernamen

2. In der Liste *WINS-Adressen in Verwendungsreihenfolge* können Sie die IPv4-Adressen der WINS-Server angeben, die für die NetBIOS-Namensauflösung verwendet werden. Tippen oder klicken Sie auf *Hinzufügen*, wenn Sie die IPv4-Adresse eines Servers in die Liste eintragen möchten. Tippen oder klicken Sie auf *Entfernen*, um den ausgewählten Server aus der Liste zu löschen. Und wenn Sie einen Eintrag bearbeiten möchten, wählen Sie ihn aus und tippen oder klicken auf *Bearbeiten*.
3. Sie können zur WINS-Namensauflösung mehrere Server angeben, die in der Reihenfolge kontaktiert werden, in der sie in der Liste stehen. Beantwortet der erste Server die Anforderung einer NetBIOS-Namensauflösung nicht, wird der nächste Server aus der Liste kontaktiert, und so weiter. Zur Änderung der Position eines Servers in der Liste wählen Sie den Server aus und verwenden dann eine der beiden Pfeilschaltflächen.
4. Um *LMHOSTS*-Abfragen zu erlauben, wählen Sie das Kontrollkästchen *LMHOSTS-Abfrage aktivieren*. Wenn der Computer eine bereits vorhandene *LMHOSTS*-Datei verwenden soll, die irgendwo im Netzwerk liegt, rufen Sie diese Datei ab, indem Sie auf *LMHOSTS importieren* tippen oder klicken und die Datei herausuchen. Gewöhnlich greifen Sie nur dann auf *LMHOSTS* zurück, wenn andere Methoden der Namensauflösung versagen.

5. Die WINS-Namensauflösung greift auf NetBIOS über TCP/IP zurück. Wählen Sie zur WINS-Namensauflösung mit NetBIOS eine der folgenden Optionen:
 - Wenn Sie DHCP und dynamische Adressierung verwenden, können Sie die NetBIOS-Einstellung vom DHCP-Server abrufen. Wählen Sie *Standard: NetBIOS-Einstellung des DHCP-Servers verwenden*.
 - Wenn Sie mit statischen IP-Adressen arbeiten oder der DHCP-Server keine NetBIOS-Einstellung liefert, wählen Sie *NetBIOS über TCP/IP aktivieren*.
 - Wird im Netzwerk weder WINS noch NetBIOS verwendet, wählen Sie *NetBIOS über TCP/IP deaktivieren*. Das schaltet die NetBIOS-Broadcasts aus, die der Computer sonst im Netzwerk versenden würde.
6. Tippen oder klicken Sie dreimal auf *OK* und dann auf *Schließen*. Wiederholen Sie diese Prozedur bei Bedarf für andere Netzwerkadapter.

TIPP *LMHOSTS*-Dateien werden lokal auf Computerbasis verwaltet, daher sind sie nicht besonders zuverlässig. Statt sich auf *LMHOSTS* zu verlassen, sorgen Sie besser dafür, dass Ihre DNS- und WINS-Server sauber konfiguriert und im Netzwerk verfügbar sind, damit die Namensauflösung zentral verwaltet und durchgeführt werden kann.

Verwalten von Netzwerkverbindungen

Netzwerkverbindungen ermöglichen es Computern, auf Ressourcen im Netzwerk und im Internet zuzugreifen. Für jeden Netzwerkadapter, der im Computer installiert ist, wird automatisch eine Netzwerkverbindung erstellt. Dieser Abschnitt beschreibt die Verwaltung dieser Verbindungen.

Aktivieren und Deaktivieren von Netzwerkverbindungen

Netzwerkverbindungen werden automatisch erstellt und konfiguriert. Wenn Sie eine Verbindung deaktivieren möchten, damit sie nicht mehr benutzt werden kann, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im linken Fensterabschnitt des Netzwerk- und Freigabecenters auf *Adaptereinstellungen ändern*.
3. Klicken Sie im Fenster *Netzwerkverbindungen* mit der rechten Maustaste auf die Verbindung oder halten Sie sie gedrückt, und wählen Sie den Befehl *Deaktivieren*.
4. Wenn Sie die Verbindung später wieder aktivieren möchten, klicken Sie die Verbindung wieder mit der rechten Maustaste an oder halten sie gedrückt, und wählen *Aktivieren*.

Wenn Sie die Netzwerkverbindung trennen oder eine andere Verbindung herstellen möchten, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im linken Fensterabschnitt des Netzwerk- und Freigabecenters auf *Adaptereinstellungen ändern*.

3. Klicken Sie im Fenster *Netzwerkverbindungen* mit der rechten Maustaste auf die Verbindung oder halten Sie sie gedrückt, und wählen Sie den Befehl *Verbindung herstellen/trennen*. Tippen oder klicken Sie im Bildschirmabschnitt *Netzwerke* auf die gewünschte Verbindung und dann auf *Trennen*. Gewöhnlich bieten nur Drahtlos- und Remotezugriffsverbindungen diese Möglichkeit.
4. Wenn Sie die Verbindung später wieder herstellen möchten, klicken Sie in *Netzwerkverbindungen* mit der rechten Maustaste auf die Verbindung oder halten sie gedrückt, und wählen *Verbindung herstellen/trennen*. Tippen oder klicken Sie dann im Bildschirmabschnitt *Netzwerke* auf die gewünschte Verbindung und dann auf *Verbinden*.

Überprüfen von Status, Geschwindigkeit und Aktivität von Netzwerkverbindungen

Um den Status einer Netzwerkverbindung zu überprüfen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im Netzwerk- und Freigabecenter unter *Aktive Netzwerke anzeigen* auf den Link für die Netzwerkverbindung.
3. Dadurch öffnet sich das *Status*-Dialogfeld der Netzwerkverbindung. Wenn die Verbindung deaktiviert ist oder sich das Netzkabel gelöst hat, können Sie nicht auf dieses Dialogfeld zugreifen. Aktivieren Sie die Verbindung wieder oder stecken Sie das Netzkabel wieder ein, um das Problem zu lösen. Versuchen Sie dann erneut, das Statusdialogfeld anzuzeigen.

Die Registerkarte *Allgemein* des *Status*-Dialogfelds der Netzwerkverbindung (Abbildung 15.7) zeigt nützliche Informationen über die Verbindung an:

- **IPv4-Konnektivität** Der aktuelle IPv4-Verbindungsstatus und die Verbindungsart. Gewöhnlich wird der Status als *Kein Internetzugriff* angezeigt, wenn eine Verbindung mit einem internen Netzwerk besteht, als *Internet*, wenn der Computer auf das Internet zugreifen kann, oder als *Kein Netzwerkzugriff*, wenn keine Verbindung mit einem Netzwerk besteht.
- **IPv6-Konnektivität** Der aktuelle IPv6-Verbindungsstatus und die Verbindungsart. Gewöhnlich wird der Status als *Kein Internetzugriff* angezeigt, wenn eine Verbindung mit einem internen Netzwerk besteht, als *Internet*, wenn der Computer auf das Internet zugreifen kann, oder als *Kein Netzwerkzugriff*, wenn keine Verbindung mit einem Netzwerk besteht.
- **Medienstatus** Der Zustand des Mediums. Weil das Statusdialogfeld nur verfügbar ist, wenn die Verbindung aktiviert ist, sehen Sie den Status gewöhnlich als *Aktiviert*.
- **Dauer** Gibt an, wie lange die Verbindung besteht. Wenn die Verbindung erst kurze Zeit besteht, hat der Benutzer erst vor Kurzem eine Verbindung hergestellt oder die Verbindung wurde kürzlich zurückgesetzt.
- **Übertragungsrate** Die Verbindungsgeschwindigkeit. Hier wird abhängig von der Verbindung 10,0 MBit/s, 100,0 MBit/s oder 1,0 GBit/s angezeigt. Eine falsche Einstellung kann die Leistung des Computers beeinträchtigen.
- **Bytes** Die Anzahl der Bytes, die über die Verbindung gesendet oder empfangen wurden. Während der Computer Datenpakete sendet oder empfängt, blinkt das Computersymbol, um den Datenverkehr anzuzeigen.

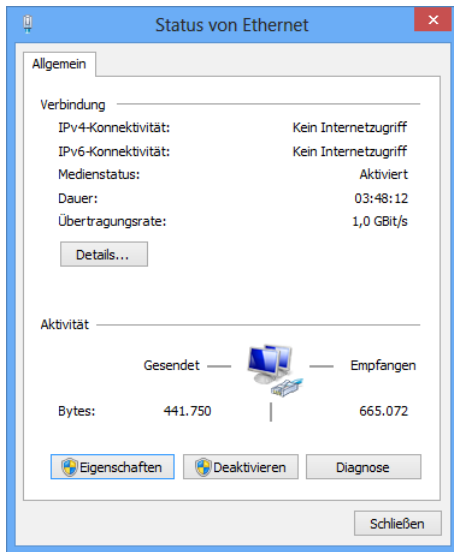


Abbildung 15.7 Die Registerkarte *Allgemein* des *Status*-Dialogfelds der Netzwerkverbindung bietet eine Zusammenstellung von wichtigen Informationen über die Verbindung

Anzeigen der Netzwerkkonfiguration

In Windows 8 können Sie die aktuelle Konfiguration von Netzwerkadaptern auf verschiedene Weise anzeigen. Um die Konfiguration mithilfe des *Status*-Dialogfelds anzuzeigen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann auf *Netzwerk- und Freigabecenter*.
2. Tippen oder klicken Sie im linken Fensterabschnitt des Netzwerk- und Freigabecenters auf *Adapter-einstellungen ändern*.
3. Tippen oder klicken Sie in *Netzwerkverbindungen* doppelt auf die Verbindung, die Sie überprüfen möchten. Dadurch öffnet sich das *Status*-Dialogfeld der Netzwerkverbindung. Wenn die Verbindung deaktiviert ist oder sich das Netzkabel gelöst hat, können Sie nicht auf dieses Dialogfeld zugreifen. Aktivieren Sie die Verbindung wieder oder stecken Sie das Netzkabel wieder ein, um das Problem zu lösen. Versuchen Sie dann erneut, das Statusdialogfeld anzuzeigen.
4. Tippen oder klicken Sie auf *Details*, um ausführlichere Informationen über die IP-Adresskonfiguration anzuzeigen, unter anderem folgende:
 - **Physische Adresse** Die Computer- oder MAC-Adresse (Media Access Control) des Netzwerkadapters. Diese Adresse ist für jeden Netzwerkadapter eindeutig.
 - **IPv4-Adresse** Die IPv4-Adresse für die IPv4-Kommunikation
 - **IPv4-Subnetzmaske** Die Subnetzmaske für die IPv4-Kommunikation
 - **IPv4-Standardgateway** Die IPv4-Adresse des Standardgateways für die IPv4-Kommunikation
 - **IPv4-DNS-Server** IP-Adressen für DNS-Server, die für die IPv4-Kommunikation verwendet werden

- **IPv4-WINS-Server** IP-Adressen für WINS-Server, die für die IPv4-Kommunikation verwendet werden
- **IPv4-DHCP-Server** Die IP-Adresse des DHCPv4-Servers, von dem die aktuelle Lease bezogen wurde (nur DHCPv4)
- **Lease erhalten** Der Zeitpunkt (mit Datum und Uhrzeit), an dem die DHCPv4-Lease bezogen wurde (nur DHCPv4)
- **Lease läuft ab** Der Zeitpunkt (mit Datum und Uhrzeit), an dem die DHCPv4-Lease abläuft (nur DHCPv4)

Sie können sich die erweiterten Einstellungen auch mit dem Befehl `Ipconfig` ansehen. Dazu gehen Sie folgendermaßen vor:

1. Öffnen Sie eine Eingabeaufforderung. Dazu können Sie `cmd` in das *Apps*-Suchfeld eingeben und dann die EINGABETASTE drücken.
2. Geben Sie in der Befehlszeile `ipconfig /all` ein. Es werden ausführliche Informationen über alle Netzwerkadapter angezeigt, die auf dem Computer konfiguriert wurden.

HINWEIS Die Eingabeaufforderung wird im Standardbenutzermodus geöffnet, sie ist keine Eingabeaufforderung mit erhöhten Rechten.

Umbenennen von Netzwerkverbindungen

Windows 8 weist Netzwerkverbindungen anfänglich Standardnamen zu. Auf der Seite *Netzwerkverbindungen* können Sie eine Verbindung umbenennen, indem Sie die Verbindung mit der rechten Maustaste anklicken oder gedrückt halten, *Umbenennen* wählen und dann einen neuen Namen für die Verbindung eingeben. Verfügt der Computer über mehrere Netzwerkverbindungen, hilft eine passende Benennung der Verbindungen Ihnen und anderen, den Überblick über die Bedeutungen der Verbindungen zu behalten. Sie öffnen das Fenster *Netzwerkverbindungen*, indem Sie im Netzwerk- und Freigabecenter auf *Adaptereinstellungen ändern* tippen oder klicken.

Problembehandlung und Testen von Netzwerkeinstellungen

Zu Windows 8 gehören viele Programme, mit denen sich TCP/IP-Verbindungen testen und Verbindungsprobleme beheben lassen. Die folgenden Abschnitte beschreiben neben der automatischen Diagnose Standardtests, die Sie bei der Einrichtung oder Änderung der Netzwerkeinstellungen eines Computers durchführen sollten, und Verfahren zur Behebung von schwierigen Netzwerkproblemen, die sich im Zusammenhang mit DHCP und DNS ergeben können. Der letzte Abschnitt beschreibt eine recht ausführliche Netzwerkdiagnose.

Diagnostizieren und Beheben von Netzwerkverbindungsproblemen

Gelegentlich werden Netzkabelstecker versehentlich aus den Buchsen herausgezogen oder der Netzwerkadapter kann aus irgendwelchen Gründen zeitweilig nicht arbeiten. Nachdem Sie das Kabel wieder eingesteckt oder das Adapterproblem gelöst haben, sollte die Verbindung automatisch wiederhergestellt werden. Verbindungsprobleme im LAN können Sie diagnostizieren, indem Sie mit der rechten Maustaste

auf das Netzwerkbenachrichtigungssymbol in der Taskleiste tippen oder klicken und dann *Problembehandlung* wählen.

Die Windows-Netzwerkdiagnose versucht dann, das Problem zu erkennen. Stattdessen können Sie die Windows-Netzwerkdiagnose auch starten, indem Sie die Verbindung in *Netzwerkverbindungen* mit der rechten Maustaste anklicken oder gedrückt halten, und dann *Diagnose* wählen.

Wie aus Abbildung 15.8 hervorgeht, werden einige mögliche Lösungen vorgeschlagen, sofern es erkennbare Konfigurationsprobleme gibt. Einige Probleme lassen sich automatisch beheben, indem man die vorgeschlagene Lösung anklickt. Bei anderen Lösungsvorschlägen sind zusätzliche Arbeitsgänge erforderlich, beispielsweise wenn Sie einen Netzwerkrouter oder ein Breitbandmodem zurücksetzen müssen. Wenn Ihre Aktion das Problem nicht löst, hilft Ihnen vielleicht ein anderer Lösungsvorschlag aus diesem Abschnitt zur Problembehebung weiter.

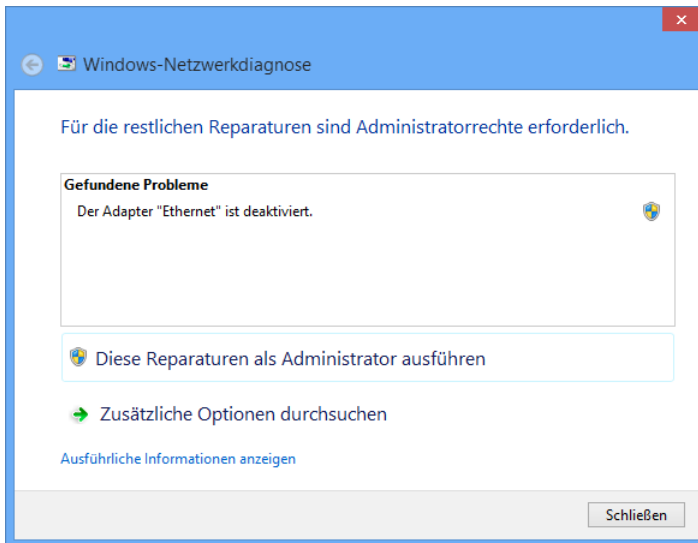


Abbildung 15.8 Versuchen Sie, das Problem durch eine passende Auswahl oder die vorgeschlagenen Aktionen zu lösen

Diagnostizieren und Beheben von Internetverbindungsproblemen

Da es so viele Abhängigkeiten zwischen Diensten, Protokollen und Konfigurationseinstellungen gibt, kann die Behebung von Netzwerkproblemen schwierig sein. Aber Windows 8 bietet ein leistungsfähiges Netzwerkdiagnoseprogramm zur leichteren Identifizierung von Problemen in folgenden Bereichen:

- Allgemeine Verbindungsprobleme im Netzwerk
- Internetdiensteinstellungen für E-Mail, Newsgroups und Proxys
- Einstellungen für Modems, Netzwerkclients und Netzwerkadapter
- DNS-, DHCP- und WINS-Konfiguration
- Standardgateways und IP-Adressen

Im Netzwerk- und Freigabecenter diagnostizieren Sie Probleme, indem Sie auf *Probleme beheben* tippen oder klicken und dann ein Problembehandlungsmodul auswählen, zum Beispiel *Netzwerkadapter*, *Eingehende Verbindungen* oder *Internetverbindungen*.

Dann versucht die Windows-Netzwerkdiagnose, das Problem zu identifizieren. Liegt ein erkennbares Konfigurationsproblem vor, wird eine Liste mit Lösungsvorschlägen angezeigt. Einige Probleme lassen sich automatisch beheben, indem Sie die vorgeschlagene Lösung anklicken. Bei anderen Lösungsvorschlägen sind zusätzliche Arbeitsgänge erforderlich, beispielsweise wenn Sie einen Netzwerkrouter oder ein Breitbandmodem zurücksetzen müssen. Wenn Ihre Aktion das Problem nicht löst, hilft Ihnen vielleicht ein anderer Lösungsvorschlag aus diesem Abschnitt zur Problembehebung weiter.

Durchführen von einfachen Standardtests

Wenn Sie einen neuen Computer installieren oder die Netzwerkeinstellungen eines Computers verändern, sollten Sie anschließend die Konfiguration überprüfen. Der einfachste TCP/IP-Test ist, mit dem Befehl Ping zu überprüfen, ob der Computer eine Verbindung mit dem Netzwerk herstellen kann. Um Ping zu verwenden, geben Sie in einer Eingabeaufforderung **ping <Host>** ein, wobei **<Host>** entweder der Name oder die IP-Adresse des Computers ist, den Sie erreichen möchten.

Unter Windows 8 können Sie die Konfiguration auf folgende Weise mit Ping testen:

- **Versuchen Sie, IP-Adressen mit Ping zu erreichen** Wenn der Computer richtig konfiguriert ist und der Computer, den Sie erreichen wollen, im Netzwerk verfügbar ist, sollte Ping eine Antwort erhalten, sofern die Firewall des Computers die Verwendung von Ping zulässt. Kann Ping den Zielcomputer nicht erreichen oder wird Ping von der Firewall blockiert, meldet es eine Zeitüberschreitung.
- **Überprüfen Sie in Domänen, die WINS verwenden, NetBIOS-Computernamen mit Ping** Wenn NetBIOS-Computernamen von Ping korrekt aufgelöst werden, sind NetBIOS-Funktionen wie WINS richtig für den Computer konfiguriert.
- **Überprüfen Sie in Domänen, die DNS verwenden, DNS-Hostnamen mit Ping** Wenn vollständig angegebene DNS-Hostnamen von Ping korrekt aufgelöst werden, ist die DNS-Namensauflösung richtig konfiguriert.

Sie können auch die Navigation im Netzwerk auf dem Computer testen. Wenn der Computer Mitglied einer Windows 8-Domäne ist und das Suchen nach Computern in der Domäne zugelassen ist, melden Sie sich auf dem Computer bei der Domäne an und suchen dann mit dem Datei-Explorer oder dem Netzwerk-Explorer in der Domäne nach anderen Computern. Anschließend melden Sie sich auf einem anderen Computer bei der Domäne an und versuchen, den Computer zu finden, den Sie gerade konfiguriert haben. Diese Tests geben Ihnen einen guten Hinweis darauf, ob die DNS-Auflösung in der lokalen Umgebung richtig durchgeführt wird. Wenn Sie die gesuchten Computer nicht finden können, überprüfen Sie die Einstellung des DNS-Dienstes und der Protokolle.

PRAXISTIPP

Der Zugriff auf Netzwerkressourcen im Netzwerk-Explorer hängt vom Dienst *Computerbrowser* und den Einstellungen zur Netzwerkerkennung ab. Der Dienst *Computerbrowser* ist für die Auflistung der Computer zuständig, die im Netzwerk vorhanden sind. Wurde der Dienst angehalten oder arbeitet er nicht richtig, kann ein Computer nicht die Ressourcen sehen, die im Netzwerk verfügbar sind. Den Zustand dieses Dienstes können Sie in der Computerverwaltung überprüfen. Erweitern Sie *Dienste und Anwendungen* und wählen Sie dann in der Strukturdarstellung *Dienste*. Der Status des Dienstes *Computerbrowser* sollte *Wird ausgeführt* sein. Ist das Feld mit der Statusanzeige leer, läuft der Dienst nicht und sollte gestartet werden.

Es kann vorkommen, dass der Dienst *Computerbrowser* zwar normal läuft, aber im Netzwerk-Explorer trotzdem keine aktualisierte Liste der Ressourcen verfügbar ist. Das kann sich so ergeben, weil der Dienst die Ressourcenliste nur in gewissen Abständen aktualisiert und das Netzwerk nicht ständig auf Änderungen überprüft. Wenn eine Ressource nicht aufgeführt wird, die Sie verwenden möchten, können Sie ent-

weder warten, bis sie verfügbar ist (das sollte in den meisten Fällen weniger als 15 Minuten dauern), oder Sie stellen direkt eine Verbindung mit der Ressource her. Dazu verwenden Sie den UNC-Namen (Universal Naming Convention) oder die IP-Adresse der Ressource, wie im Abschnitt »Verwenden von freigegebenen Ressourcen« in Kapitel 13 beschrieben.

Gelegentlich ist die Netzwerkerkennung und Freigabe auch so eingestellt, dass keine Netzwerkerkennung erfolgen kann. Um dieses Problem zu lösen, müssen Sie die Netzwerkerkennung zulassen. Tun Sie Folgendes:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Netzwerkstatus und -aufgaben anzeigen*.
2. Tippen oder klicken Sie im linken Fensterabschnitt des Netzwerk- und Freigabecenters auf *Erweiterte Freigabeeinstellungen ändern*.
3. Es werden Optionen angezeigt, mit denen Sie die Freigabe- und Netzwerkerkennungseinstellungen für jedes Netzwerkprofil des Computers konfigurieren können. Wählen Sie die gewünschten Einstellungen für jedes Profil. Wenn beispielsweise die Netzwerkerkennung in einem Profil deaktiviert ist, obwohl sie aktiviert sein sollte, müssen Sie auf die Option *Netzwerkerkennung einschalten* tippen oder klicken.
4. Tippen oder klicken Sie auf *Änderungen speichern*.

Beheben von IP-Adressierungsproblemen

Wie sich die aktuelle IP-Adresseneinstellung eines Computers ermitteln lässt, wird im Abschnitt »Anzeigen der Netzwerkkonfiguration« weiter oben in diesem Kapitel beschrieben. Wenn ein Computer mit dem Zugriff auf Netzwerkressourcen oder mit der Kommunikation mit anderen Computern Probleme hat, liegt das vielleicht an einer falschen Einstellung der IP-Adressen. Sehen Sie sich die eingestellte IP-Adresse genau an und überprüfen Sie auch die anderen IP-Adresseneinstellungen. Orientieren Sie sich an folgenden Hinweisen:

- Wenn die IPv4-Adresse, die dem Computer zugewiesen wurde, im Bereich von 169.254.0.1 bis 169.254.255.254 liegt, verwendet der Computer automatisch zugewiesene private IP-Adressen (Automatic Private IP Addressing, APIPA). Eine private IP-Adresse wird dem Computer automatisch zugewiesen, wenn er für die Verwendung von DHCP konfiguriert ist und der DHCP-Client keinen DHCP-Server erreichen kann. Wenn Windows 8 APIPA benutzt, überprüft es regelmäßig, ob ein DHCP-Server verfügbar geworden ist. Sofern der Computer nicht irgendwann eine dynamische IP-Adresse anfordern kann, weist das gewöhnlich auf ein Problem mit der Netzwerkverbindung hin. Überprüfen Sie das Netzkabel vom Computer bis zu dem Switch oder Hub, mit dem es verbunden sein soll.
- Stehen die IPv4-Adresse und die Subnetzmaske des Computers auf 0.0.0.0, ist kein Netzwerk geschlossen oder jemand versucht, eine statische IP-Adresse zu verwenden, die im Netzwerk bereits in Gebrauch ist. In diesem Fall sollten Sie das Fenster *Netzwerkverbindungen* öffnen und den Zustand der Verbindung überprüfen. Wurde die Verbindung deaktiviert oder getrennt, sollte dieser Zustand angezeigt werden. Klicken Sie mit der rechten Maustaste auf die Verbindung oder halten Sie sie gedrückt, und wählen Sie nach Bedarf *Aktivieren* oder *Reparieren*. Ist die Verbindung bereits aktiviert, müssen Sie vermutlich die IP-Adresse der Verbindung ändern.
- Wurde die IP-Adresse dynamisch zugewiesen, überprüfen Sie, ob ein anderer Computer im Netzwerk dieselbe Adresse verwendet. Das können Sie tun, indem Sie von dem Computer, den Sie untersuchen, das Netzkabel abziehen und die fragliche Adresse auf einem anderen Computer mit Ping überprüfen. Wenn ein Computer auf Ping antwortet, wissen Sie, dass ein anderer Computer dieselbe

Adresse verwendet. Dieser Computer hat vermutlich eine falsche statische IP-Adresse erhalten oder die Adressenreservierung wurde nicht richtig eingestellt.

- Wenn die IP-Adresse anscheinend in Ordnung ist, überprüfen Sie die Einstellungen für Netzwerkmaske, Gateway, DNS und WINS. Vergleichen Sie die Einstellungen des Computers, an dem Sie arbeiten, mit den Einstellungen eines anderen Computers, von dem Sie wissen, dass er im Netzwerk einwandfrei arbeitet. Einer der größten Problembereiche ist die Netzwerkmaske. Wenn Subnetze verwendet werden, kann die Netzwerkmaske, die in einem Bereich des Netzwerks verwendet wird, der Netzwerkmaske aus einem anderen Bereich zum Verwechseln ähnlich sehen. So könnte die Netzwerkmaske in einem IPv4-Bereich beispielsweise 255.255.255.240 lauten und in einem anderen IPv4-Bereich 255.255.255.248.

Freigeben und Erneuern der DHCP-Zuweisung

DHCP-Server können viele Netzwerkeinstellungen automatisch zuweisen. Dazu gehören IP-Adressen, Standardgateways, bevorzugter und alternativer DNS-Server, bevorzugter und alternativer WINS-Server und mehr. Wenn Computer die dynamische Adressierung verwenden, dann mieten sie sozusagen für eine gewisse Zeit eine bestimmte IP-Adresse. Man sagt, sie erhalten eine Lease. Diese Lease gilt nur für eine bestimmte Zeit und muss regelmäßig erneuert werden. Wenn es soweit ist, kontaktiert der Computer den DHCP-Server, von dem er die Lease erhalten hat. Ist der Server verfügbar, wird die Lease erneuert und eine neue Leaseperiode gewährt. Sie können Leases bei Bedarf auch manuell erneuern, sei es auf den einzelnen Computern oder unter Verwendung des DHCP-Servers.

Bei der Leasezuweisung und -erneuerung können Probleme auftreten, die eine Netzwerkkommunikation verhindern. Wenn der Server nicht verfügbar ist und vor Ablauf der Lease nicht erreicht werden kann, kann die IP-Adresse ungültig werden. Wenn das geschieht, kann der Computer die alternative Adressenkonfiguration verwenden, wobei diese Einstellungen in den meisten Fällen aber nicht passen und keine einwandfreie Kommunikation ermöglichen. Um das Problem zu lösen, müssen Sie die aktuelle Lease löschen und die DHCP-Lease erneuern.

Ein weiteres Problem kann sich ergeben, wenn Benutzer zwischen verschiedenen Büros und Subnetzen der Organisation pendeln. Wenn sie den Ort wechseln, könnten ihre Computer die DHCP-Einstellungen vom falschen Server erhalten. Kehren sie dann ins Büro zurück, verhalten sich ihre Computer seltsam und arbeiten nicht mehr richtig, weil sie ihre Einstellungen am anderen Ort vom falschen DHCP-Server erhalten haben. Wenn das geschieht, müssen Sie die aktuelle Lease löschen und die DHCP-Lease erneuern.

Sie können DHCP-Leases folgendermaßen freigeben und erneuern:

1. Tippen oder klicken Sie im linken Fensterabschnitt des Netzwerk- und Freigabecenters auf *Adapter-einstellungen ändern*.
2. Klicken Sie im Fenster *Netzwerkverbindungen* mit der rechten Maustaste auf die Verbindung, die Sie bearbeiten wollen, oder halten Sie sie gedrückt, und wählen Sie den Befehl *Diagnose*.
3. Wenn der Computer über eine oder mehrere dynamisch zugewiesene IP-Adressen verfügt, sollte einer der Lösungsvorschläge *Rufen Sie neue TCP/IP-Einstellungen für den Adapter "(Name)" automatisch ab* sein. Tippen oder klicken Sie auf diese Option.

Sie können die Einstellungen auch mit dem Befehl `Ipconfig` löschen und erneuern, und zwar folgendermaßen:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten. Dazu können Sie **cmd** in das *Apps*-Suchfeld eingeben, auf der Seite *Apps* mit der rechten Maustaste auf *Eingabeaufforderung* klicken oder es gedrückt halten, und dann auf *Als Admin ausführen* tippen oder klicken.
2. Geben Sie in der Befehlszeile **ipconfig /release** ein, um die aktuellen Einstellungen von allen Netzwerkadaptern zu löschen. Erneuern Sie dann die Lease mit dem Befehl **ipconfig /renew**.
3. Wenn Sie einfach nur die DHCP-Lease für alle Netzwerkadapter erneuern möchten, geben Sie in der Befehlszeile **ipconfig /renew** ein.
4. Sie können die aktualisierten Einstellungen überprüfen, indem Sie in der Befehlszeile **ipconfig /all** eingeben.

PRAXISTIPP

Wenn Sie vergessen, die alten DHCP-Einstellungen freizugeben, bevor Sie die Anweisung geben, die DHCP-Einstellungen zu erneuern, versucht der Computer, die Einstellungen in dem Netzwerk zu erneuern, mit dem er zuletzt verbunden war. Ist der Computer an ein neues Netzwerk angeschlossen, gelingt es ihm unter Umständen nicht, eine Verbindung zu dem Server oder dem Gerät herzustellen, das ihm vorher seine DHCP-Einstellungen zugewiesen hat.

Wenn der Computer über mehrere Netzwerkadapter verfügt und Sie nur mit einem oder einem Teil der vorhandenen Adapter arbeiten möchten, können Sie das tun, indem Sie hinter dem Befehl `ipconfig /renew` oder `ipconfig /release` den Namen der Verbindung angeben, je nach Bedarf vollständig oder teilweise. Verwenden Sie das Sternchen (*) als Platzhalter für beliebige Zeichen im Verbindungsnamen. Wenn Sie zum Beispiel die Lease für alle Verbindungen erneuern möchten, deren Namen mit *Loc* beginnt, können Sie den Befehl **ipconfig /renew Loc*** eingeben. Wenn Sie die Einstellungen für alle Verbindungen löschen wollen, in denen das Wort *Network* vorkommt, können Sie den Befehl **ipconfig /release *Network*** verwenden.

Registrieren von DNS-Einträgen und Leeren des DNS-Auflösungscaches

Der DNS-Auflösungscache führt Buch über die DNS-Anfragen, die durchgeführt werden, wenn ein Benutzer mit TCP/IP auf Netzwerkressourcen zugreift. Dieser Cache enthält Einträge für die Umsetzung vom Hostnamen auf IP-Adressen (forward lookup) und Einträge für die Umsetzung von IP-Adressen auf Hostnamen (reverse lookup). Sobald ein Eintrag für einen bestimmten DNS-Host im Auflösungscache eingetragen ist, braucht der lokale Computer nicht mehr externe Server abzufragen, um die DNS-Informationen für diesen Host zu erhalten. Er kann die DNS-Anfragen bereits mit seinen lokalen Informationen beantworten und somit schneller reagieren.

Wie lange Einträge im Auflösungscache zwischengespeichert werden, hängt von der verbleibenden Gültigkeitsdauer (Time To Live, TTL) ab, die dem Datensatz vom Quellserver zugewilligt wurde. Wenn Sie sich die aktuellen Einträge ansehen und die verbleibende Gültigkeitsdauer der Datensätze überprüfen möchten, können Sie in einer Eingabeaufforderung mit erhöhten Rechten **ipconfig /displaydns** eingeben. Als verbleibende Gültigkeitsdauer wird die Zahl der Sekunden angegeben, die ein bestimmter Datensatz im Cache bleiben kann, bevor er ungültig wird. Die Gültigkeitsdauer wird vom lokalen Computer kontinuierlich herabgezählt. Sobald der Wert auf 0 fällt, ist der Datensatz ungültig und wird aus dem Auflösungscache gelöscht.

Es kann sich die Situation ergeben, dass ein Auflösungscache gelöscht werden muss, um alte Einträge zu entfernen und die Computer in die Lage zu versetzen, aktualisierte DNS-Einträge abzurufen, bevor die alten Einträge abgelaufen sind und sowieso aus dem Cache gelöscht werden. Gewöhnlich ist dies der Fall, wenn sich IP-Adressen von Servern ändern und die aktuellen Einträge aus dem Auflösungscache noch

die alten Adressen angeben und nicht die neuen. Gelegentlich stimmen die Einträge im Auflösungs-cache auch aus anderen Gründen nicht, zum Beispiel dann, wenn DHCP falsch konfiguriert wurde.

PRAXISTIPP Erfahrene Administratoren wissen, dass sie einige Wochen vor einer geplanten Änderung beginnen sollten, die Gültigkeitsdauer der DNS-Datensätze, die sich ändern werden, herabzusetzen. Gewöhnlich bedeutet das, die Gültigkeitsdauer von einigen Tagen (oder Wochen) auf einige Stunden herabzusetzen, damit sich die Änderungen schneller auf die Computer verbreiten, die die entsprechenden DNS-Datensätze zwischengespeichert haben. Sobald die Änderung durchgeführt ist, sollten die Administratoren wieder die ursprüngliche Gültigkeitsdauer einstellen, um die Zahl der Erneuerungsanforderungen zu verringern.

In den meisten Fällen können Sie Probleme mit dem DNS-Auflösungs-cache beheben, indem Sie den Cache leeren oder die DNS-Datensätze erneut registrieren. Wenn Sie den Auflösungs-cache leeren, werden alle DNS-Datensätze aus dem Cache gelöscht und erst dann neue Einträge erstellt, wenn der Computer wieder für einen bestimmten Host oder eine bestimmte IP-Adresse eine DNS-Abfrage durchführt. Wenn Sie die DNS-Einträge erneut registrieren, versucht Windows 8, die aktuellen DHCP-Leases zu erneuern, und führt dann für alle DNS-Einträge im Auflösungs-cache erneut DNS-Abfragen durch. Durch den erneuten Abruf der Hosts und der IP-Adressen werden die Einträge im Auflösungs-cache aktualisiert und registriert. Im Normalfall werden Sie den Auflösungs-cache einfach leeren und den Computer dann nach Bedarf die erforderlichen DNS-Anfragen durchführen lassen. Registrieren Sie die DNS-Einträge nur dann erneut, wenn Sie vermuten, dass es Probleme mit DHCP und dem DNS-Auflösungs-cache gibt.

Sie können mit dem Befehl `Ipconfig` auf folgende Weise den DNS-Auflösungs-cache leeren oder die DNS-Datensätze erneut registrieren:

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten. Dazu können Sie **cmd** in das *Apps*-Suchfeld eingeben, auf der Seite *Apps* mit der rechten Maustaste auf *Eingabeaufforderung* klicken oder es gedrückt halten, und dann auf *Als Admin ausführen* tippen oder klicken.
2. Um den Auflösungs-cache zu löschen, geben Sie in der Befehlszeile **ipconfig /flushdns** ein.
3. Um die DHCP-Leases zu erneuern und die DNS-Einträge erneut zu registrieren, geben Sie in der Befehlszeile **ipconfig /registerdns** ein.
4. Wenn die Arbeiten abgeschlossen sind, können Sie das Ergebnis überprüfen, indem Sie in der Befehlszeile **ipconfig /displaydns** eingeben.

Kapitel 16

Verwalten von mobilen Netzwerken und Remotezugriff

In diesem Kapitel:

Konfigurieren des Netzwerks auf mobilen Geräten	596
Mobile Netzwerke und Remotezugriff	602
Erstellen von Verbindungen für den Remotezugriff	604
Einstellen der Verbindungseigenschaften	613
Herstellen von Verbindungen	624
Drahtlosnetzwerke	628

Oft möchten Benutzer eine Verbindung zum Netzwerk ihrer Organisation mit einem Computer herstellen, der sich gar nicht am Standort der Organisation befindet. Dazu brauchen sie eine Wähl-, eine Breitband-, eine VPN- (Virtuelles Privates Netzwerk) oder eine DirectAccess-Verbindung. Wählverbindungen ermöglichen den Benutzern, mit einem Modem über eine gewöhnliche Telefonleitung die Verbindung zum Netzwerk ihrer Organisation herzustellen. Breitbandverbindungen ermöglichen den Benutzern, mit ihren Computern über DSL-Router (Digital Subscriber Line) oder Kabelmodems eine Verbindung zum Netzwerk ihrer Organisation herzustellen. VPN und DirectAccess nutzen Verschlüsselung, um über bestehende Verbindungen eine sichere Verbindung herzustellen, wobei es sich um eine LAN-, Wähl- oder Breitbandverbindung handeln kann. Zunehmend werden auch Drahtlosverbindungen verwendet. Bei einer Drahtlosverbindung stellen Computer die Verbindung mit speziellen Netzwerkadaptern her, die über integrierte Sende- und Empfangsvorrichtungen und Antennen verfügen und mit anderen Drahtlosgeräten dieser Art kommunizieren können.

Konfigurieren des Netzwerks auf mobilen Geräten

Die meisten mobilen Geräte brauchen mehrere Netzwerkkonfigurationen: eine für das Büro, eine für zu Hause und vielleicht noch eine für unterwegs. Im Büro verwendet das mobile Gerät gewöhnlich Netzwerkeinstellungen, die ihm von einem DHCP-Server (Dynamic Host Configuration Protocol) zugewiesen werden. Zu Hause verwendet das mobile Gerät eine andere Netzwerkeinstellung, um in einem kleinen Netzwerk beispielsweise auf einen freigegebenen Drucker und auf einen Breitband-Internetanschluss zuzugreifen. Manche mobilen Geräte müssen für eine WiFi-Verbindung konfiguriert werden, während der Benutzer nicht an seinem Schreibtisch sitzt, und für DHCP, während das mobile Gerät durch ein Kabel mit dem Netzwerk verbunden ist, oder umgekehrt. Wenn das System seine Hauptnetzwerkeinstellung mit DHCP erhält, können Sie eine zweite Netzwerkeinstellung für die Gelegenheiten vornehmen, bei denen kein DHCP-Server verfügbar ist, beispielsweise auf Reisen oder zu Hause. Systeme können Zweitkonfigurationen entweder automatisch oder aufgrund einer Benutzereingabe verwenden. In Konferenzräumen oder unterwegs müssen Nutzer ihre mobilen Geräte manchmal mit vernetzten Projektoren verbinden – für diese Aufgabe gibt es den Assistenten zum Herstellen einer Verbindung mit dem Netzwerkprojektor.



Abbildung 16.1 Verwalten wichtiger Einstellungen für mobile Geräte

Verwenden des Windows-Mobilitätscenters

Das Windows-Mobilitätscenter (Abbildung 16.1) ist ein zentraler Ort für die Verwaltung wichtiger Funktionen, die für mobile Geräte typisch sind. Es umfasst eine Reihe von Steuerelementgruppen in Form kleiner Kacheln, die einen schnellen Zugriff auf die gebräuchlichsten Einstellungen für mobile Geräte bieten. Auf einem mobilen Gerät erreichen Sie das Windows-Mobilitätscenter, indem Sie das Energieversorgungssymbol im Infobereich der Taskleiste mit der rechten Maustaste anklicken oder gedrückt halten, und dann *Windows-Mobilitätscenter* wählen, oder indem Sie in der Systemsteuerung unter *Hardware und Sound* auf *Häufig verwendete Mobilitätseinstellungen ändern* tippen oder klicken.

Die Steuerelementkacheln des Windows-Mobilitätscenters ermöglichen Ihnen eine Änderung der ausgewählten Werte. Sie können beispielsweise die Bildschirmhelligkeit mit einem Schieberegler einstellen, den gewünschten Energiesparplan aus einer Liste auswählen und die Präsentationseinstellungen mit einer Schaltfläche ein- und ausschalten. Welche Steuerelementkacheln verfügbar sind, hängt von der Art des mobilen Geräts und vom Hersteller ab. Die gebräuchlichsten Steuerelementkacheln sind:

- **Akkustatus** Zeigt den Ladezustand des Akkus. In der angebotenen Auswahlliste können Sie bei Bedarf einen anderen Energiesparplan auswählen. Wenn Sie selbst Energiepläne definiert haben, sind auch diese verfügbar. Tippen oder klicken Sie auf das Symbol, um die Seite *Energieoptionen* der Systemsteuerung zu öffnen.
- **Helligkeit** Ermöglicht Ihnen die Einstellung der Helligkeit des Monitors. Sofern die Helligkeit auf Ihrem Computer einstellbar ist, können Sie sie mit dem Schieberegler ändern. Tippen oder klicken Sie auf das Symbol, um die Seite *Energieoptionen* der Systemsteuerung zu öffnen. Das Energieversorgungssymbol im Infobereich der Taskleiste bietet ähnliche Optionen. Auch im Fensterabschnitt *Einstellungen* finden Sie eine Helligkeitseinstellung.
- **Externer Monitor** Ermöglicht Ihnen die Verbindung mit einem externen Monitor, der über ein Kabel angeschlossen wird, sofern die Hardware dies zulässt und es beispielsweise für eine Präsentation erforderlich ist. Tippen oder klicken Sie auf *Monitor anschließen*, um den externen Monitor mit Bilddaten zu versorgen. Tippen oder klicken Sie auf das Symbol, um die Seite *Bildschirmauflösung* der Systemsteuerung zu öffnen.
- **Präsentationseinstellungen** Ermöglicht es Ihnen, den Präsentationsmodus ein- und auszuschalten. Im Präsentationsmodus gehen das Grafiksystem und die Festplatte nicht in einen Ruhezustand über, wenn niemand am Computer arbeitet. Tippen oder klicken Sie auf *Einschalten*, um in den Präsentationsmodus zu wechseln. Tippen oder klicken Sie auf das Symbol, um das Dialogfeld *Präsentationseinstellungen* zu öffnen.
- **Synchronisierungszentrum** Ermöglicht Ihnen die Anzeige des Zustands der Dateisynchronisation und die Durchführung einer Synchronisation. Tippen oder klicken Sie auf *Synchronisierung*, um eine neue Synchronisierung im Synchronisierungszentrum einzuleiten. Tippen oder klicken Sie auf das Symbol, um die Seite *Synchronisierungszentrum* der Systemsteuerung zu öffnen.
- **Lautstärke** Ermöglicht Ihnen die Einstellung der aktuellen Lautstärke. Sofern die Lautstärke auf Ihrem Computer einstellbar ist, können Sie sie mit dem Schieberegler ändern. Aktivieren Sie das Kontrollkästchen *Ton aus*, um die Lautsprecher stummzuschalten. Tippen oder klicken Sie auf das Symbol, um das Dialogfeld *Sound* zu öffnen. Das Lautsprechersymbol im Infobereich der Taskleiste bietet ähnliche Optionen.

Manche Hersteller von mobilen Geräten passen das Windows-Mobilitätscenter an, indem sie ihre eigenen Steuerelementkacheln hinzufügen und so die Standardoptionen ergänzen. Zum Beispiel enthalten einige HP-Notebooks eine Steuerelementkachel für den »HP Wireless Assistant«, in dem Sie Drahtlosnetzwerkeinstellungen für das integrierte Drahtlosgerät konfigurieren können.

Mobile Benutzer müssen in der Lage sein, das Netzwerk schnell abzuschalten. Dazu stehen mehrere Möglichkeiten zur Verfügung, aber am schnellsten geht es, wenn Sie in den Flugzeugmodus schalten. Während der Flugzeugmodus aktiv ist, sind alle Netzwerkfunktionen deaktiviert. Wenn Sie den Flugzeugmodus später wieder ausschalten, werden alle Netzwerke wieder eingeschaltet. Sie schalten in den Flugzeugmodus, indem Sie im Infobereich der Taskleiste auf das Netzwerksymbol tippen oder klicken, um den Bildschirmabschnitt *Netzwerke* zu öffnen. Aktivieren Sie nun den Flugzeugmodus, indem Sie auf den entsprechenden Schalter tippen oder klicken. Der Flugzeugmodus müsste nun eingeschaltet sein.

Stattdessen können Sie den Flugzeugmodus auch folgendermaßen einschalten:

1. Streifen Sie vom rechten Bildschirmrand oder drücken Sie die Tastenkombination **WINDOWS+I**.
2. Tippen oder klicken Sie auf das Symbol des aktuellen Netzwerks.
3. Tippen oder klicken Sie auf den Schalter *Flugzeugmodus*, um ihn in die Stellung *Ein* zu bringen.

Wenn Sie einen dieser Abläufe wiederholen, wird der Flugzeugmodus beim nächsten Antippen oder Anklicken des Schalters wieder deaktiviert.

Konfigurieren von dynamischen IP-Adressen

DHCP ermöglicht es, eine zentrale, automatische Vergabe von IP-Adressen und TCP/IP-Grundeinstellungen einzurichten. Wenn es in Ihrem Netzwerk einen DHCP-Server gibt, können Sie die Netzwerkadapterkarten der Computer so einstellen, dass sie automatisch eine IP-Adresse erhalten. Anschließend überlassen Sie es dem DHCP-Server, die erforderlichen Informationen zu liefern. Wenn Sie dynamische IP-Adressen sowohl für IPv4 als auch IPv6 zuweisen wollen, müssen Sie separate DHCP-Dienste für IPv4 und IPv6 einrichten.

Gehen Sie folgendermaßen vor, um dynamische IP-Adressen zu konfigurieren:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Netzwerkstatus und -aufgaben anzeigen*.
2. Tippen oder klicken Sie im linken Fensterabschnitt des Netzwerk- und Freigabecenters auf *Adapter-einstellungen ändern*.
3. Das Fenster *Netzwerkverbindungen* zeigt eine Liste der verfügbaren Netzwerkverbindungen an, die auf dem Computer eingerichtet wurden. Klicken Sie mit der rechten Maustaste auf die Verbindung, die Sie einstellen möchten, oder halten Sie sie gedrückt, und wählen Sie dann *Eigenschaften*.
4. Tippen oder klicken Sie doppelt auf *Internetprotokoll Version 4 (TCP/IPv4)* oder wählen Sie *Internetprotokoll Version 4 (TCP/IPv4)* aus und tippen oder klicken Sie dann auf die Schaltfläche *Eigenschaften*. Dadurch öffnet sich das Dialogfeld *Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)*, zu sehen in Abbildung 16.2.
5. Wählen Sie *IP-Adresse automatisch beziehen*. Bei Bedarf wählen Sie auch *DNS-Serveradresse automatisch beziehen*. Oder Sie wählen *Folgende DNS-Serveradressen verwenden* und geben in den Eingabefeldern dann die Adressen des bevorzugten und des alternativen DNS-Servers ein.
6. Tippen oder klicken Sie auf *OK*.
7. Falls Ihre Organisation oder das Netzwerk IPv6 verwendet, können Sie doppelt auf *Internetprotokoll Version 6 (TCP/IPv6)* tippen oder klicken. Wählen Sie *IPv6-Adresse automatisch beziehen* aus. Bei Bedarf können Sie auch *DNS-Serveradresse automatisch beziehen* oder die Option *Folgende DNS-Serveradressen verwenden* wählen und in den entsprechenden Eingabefeldern die Adressen des bevorzugten und des alternativen DNS-Servers eingeben. Tippen oder klicken Sie auf *OK*.
8. Konfigurieren Sie bei Bedarf die alternativen privaten IP-Adressen (siehe nächsten Abschnitt).

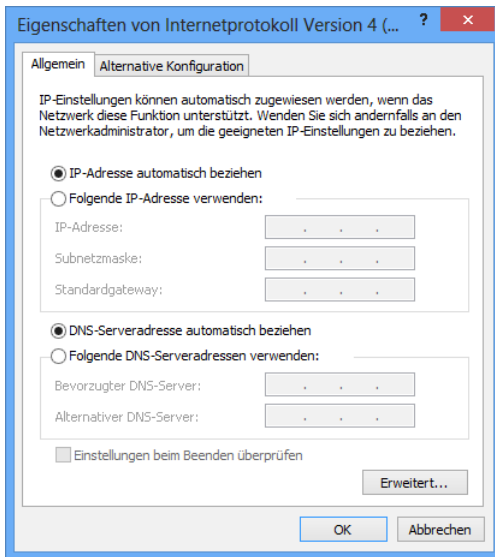


Abbildung 16.2 Für die Verwendung von DHCP stellen Sie den Computer so ein, dass er seine IP-Adresse automatisch anfordert

Konfigurieren von alternativen privaten IP-Adressen

Nur IPv4-Verbindungen verfügen über alternative Einstellungen. Wenn Sie für eine IPv4-Verbindung DHCP verwenden, wird eine automatische private IP-Adresse (APIPA) zugewiesen, falls der DHCP-Server beim Start des Systems oder bei Ablauf der Gültigkeit der alten Adresse nicht erreichbar ist. Die automatische private IP-Adresse liegt im Bereich von 169.254.0.1 bis 169.254.255.254, die Subnetzmaske lautet 255.255.0.0. Da eine automatische private IP-Adresse keine Standardgateway-, DNS- oder WINS-Einstellungen umfasst, ist ein Computer, der eine alternative IP-Adresse verwendet, in einem separaten Netzwerksegment im APIPA-Bereich isoliert.

Wenn Sie sicherstellen möchten, dass ein Computer eine bestimmte IP-Adresse und eine definierte Netzwerkkonfiguration verwendet, wenn kein DHCP-Server verfügbar ist, müssen Sie die alternative Konfiguration manuell vornehmen. Einer der wichtigsten Gründe, sich mit alternativen Konfigurationen zu beschäftigen, sind Benutzer mobiler Geräte, die ihre Computer von der Arbeit mit nach Hause nehmen. Das mobile Gerät eines Benutzers lässt sich so konfigurieren, dass es am Arbeitsplatz eine dynamisch zugewiesene IP-Adresse verwendet und zu Hause eine alternative IP-Adressenkonfiguration. Bevor Sie anfangen, sollten Sie den Benutzer nach der Netzwerkkonfiguration fragen, die er zu Hause verwendet, einschließlich IP-Adresse, Gateway- und DNS-Serveradressen, die vielleicht vom Internetprovider vorgegeben wird.

Zur Konfiguration alternativer privater IP-Adressen gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Netzwerkstatus und -aufgaben anzeigen*.
2. Tippen oder klicken Sie im linken Fensterabschnitt des Netzwerk- und Freigabecenters auf *Adapter-einstellungen ändern*.

3. Das Fenster *Netzwerkverbindungen* zeigt eine Liste der verfügbaren Netzwerkverbindungen an, die auf dem Computer eingerichtet wurden. Klicken Sie mit der rechten Maustaste auf die Verbindung, die Sie einstellen möchten, oder halten Sie sie gedrückt und wählen Sie dann *Eigenschaften*.
4. Tippen oder klicken Sie doppelt auf *Internetprotokoll Version 4 (TCP/IPv4)* oder wählen Sie *Internetprotokoll Version 4 (TCP/IPv4)* aus und tippen oder klicken Sie dann auf die Schaltfläche *Eigenschaften*. Dadurch öffnet sich das Dialogfeld *Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)*.
5. Sofern Sie den Adapter bereits so konfiguriert haben, dass er seine IP-Adresse automatisch bezieht, müsste die Registerkarte *Alternative Konfiguration* verfügbar sein (Abbildung 16.3).

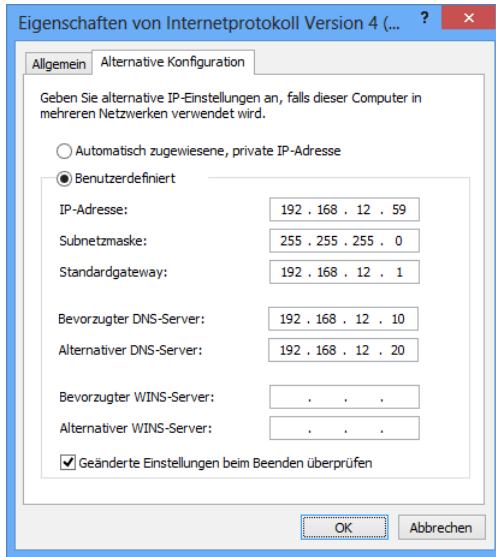


Abbildung 16.3 Auf der Registerkarte *Alternative Konfiguration* stellen Sie die privaten IP-Adressen für den Computer ein

6. Wählen Sie auf der Registerkarte *Alternative Konfiguration* die Option *Benutzerdefiniert*. Geben Sie dann im Feld *IP-Adresse* die IP-Adresse ein, die Sie verwenden möchten. Bei der IP-Adresse, die Sie dem Computer zuweisen, sollte es sich um eine private IP-Adresse handeln, die zu dem Zeitpunkt, an dem die Zuweisung erfolgt, nicht bereits anderweitig benutzt wird. Private IP-Adressen, die normalerweise benutzt werden, liegen in den Bereichen 10.0.0.1 bis 10.255.255.254, 172.16.0.1 bis 172.31.255.254 und 192.168.0.1 bis 192.168.255.254 (ausgenommen sind IP-Adressen, die für Netzwerk-IDs und Broadcasts reserviert sind).
7. Das Feld *Subnetzmaske* sorgt dafür, dass die Kommunikation der Computer im Netzwerk ordnungsgemäß erfolgen kann. Windows 8 sollte in diesem Feld einen Standardwert für die Subnetzmaske vorgeben. Wenn es im Netzwerk keine Subnetze gibt, sollte der Standardwert ausreichen. Werden aber Subnetze eingesetzt, müssen Sie die Subnetzmaske so anpassen, dass sie zum Zielnetzwerk passt.
8. Sofern der Computer auf andere TCP/IP-Netzwerke, das Internet oder andere Subnetze zugreifen soll, müssen Sie ein Standardgateway festlegen. Geben Sie im Feld *Standardgateway* die IP-Adresse des Standardrouters des Netzwerks an.
9. DNS-Server werden für die Namensauflösung in Domänen gebraucht. Geben Sie in den verfügbaren Feldern einen bevorzugten und einen alternativen DNS-Server an.

10. Wird im Netzwerk aus Gründen der Abwärtskompatibilität mit früheren Windows-Versionen WINS verwendet, legen Sie mit den verfügbaren Feldern einen bevorzugten und einen alternativen WINS-Server fest.
11. Wenn Sie fertig sind, tippen oder klicken Sie zweimal auf OK, um die geöffneten Dialogfelder zu schließen.

Verbinden mit Netzwerkprojektoren

In vielen Versammlungs- und Konferenzräumen sind Netzwerkprojektoren verfügbar, die für Präsentationen eingesetzt werden können. Um diese Projektorart benutzen zu können, müssen Sie Ihren Computer mit dem lokalen Netzwerk verbinden und dann den Assistenten zum Herstellen einer Verbindung mit dem Netzwerkprojektor verwenden. Der Assistent unterstützt Sie bei der Suche nach den Projektoren im Netzwerk und bei der Herstellung einer Verbindung.

Bevor ein mobiles Gerät den Assistenten nutzen kann, müssen Sie das Feature *Netzwerkprojektor* hinzufügen. Gehen Sie dazu folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Programme* und dann unter *Programme und Features* auf *Windows-Features aktivieren oder deaktivieren*.
2. Aktivieren Sie im Dialogfeld *Windows-Funktionen* das Kontrollkästchen *Netzwerkprojektor* und tippen oder klicken Sie auf OK.

Sobald Sie das Feature *Netzwerkprojektor* installieren, wird das Tool *Verbindung mit Netzwerkprojektor* im Abschnitt *Windows-Zubehör* zur Apps-Seite hinzugefügt. Außerdem steht dieses Tool auf der Startseite zur Verfügung. Bevor ein Benutzer einen Vortrag hält, kann er die Standardeinstellungen für Präsentationen konfigurieren:

- Bildschirmschoner ausschalten
- Lautstärke festlegen
- Einen bestimmten Hintergrund oder ein Hintergrundbild anzeigen

Diese Einstellungen konfigurieren Sie im Dialogfeld *Präsentationseinstellungen*. Wenn Sie mit dem Mobilitätscenter arbeiten, können Sie dieses Dialogfeld öffnen, indem Sie in der Kachel *Präsentationseinstellungen* auf das Netzwerkprojektorsymbol tippen oder klicken.

Sie können den Assistenten zum Herstellen einer Verbindung mit dem Netzwerkprojektor folgendermaßen starten und verwenden:

1. Tippen oder klicken Sie auf der Startseite oder der Apps-Seite auf *Verbindung mit Netzwerkprojektor*.
2. Falls Sie noch nie eine Verbindung mit einem Netzwerkprojektor hergestellt haben und die Windows-Firewall aktiv ist, tippen oder klicken Sie auf *Kommunikation des Netzwerkprojektors mit dem Computer zulassen*, damit der Netzwerkprojektor durch die Windows-Firewall hindurch mit dem Computer kommunizieren kann.
3. Wenn Sie unter den Projektoren, die im lokalen Netzwerk verfügbar sind, einen Projektor auswählen möchten, tippen oder klicken Sie auf *Nach einem Projektor suchen*. Der Assistent sucht im Netzwerk nach Projektoren und zeigt seine Ergebnisse zusammen mit einer Liste der Projektoren an, die Sie zuletzt benutzt haben. Tippen oder klicken Sie auf den Projektor, den Sie benutzen möchten, geben Sie bei Bedarf ein Kennwort für den Projektor ein und tippen oder klicken Sie dann auf *Verbinden*.
4. Wenn Sie die Netzwerkadresse des Projektors kennen, tippen oder klicken Sie auf *Die Projektornetzwerkadresse eingeben*. Geben Sie auf der Seite *Geben Sie die Netzwerkadresse eines Netzwerkprojektors ein* die Netzwerkadresse des Projektors ein, beispielsweise <http://intranet.cpandl.local/projectors/>

confb-proj1. Geben Sie bei Bedarf ein Kennwort für den Projektor ein und tippen oder klicken Sie dann auf *Verbinden*.

5. Sobald eine Verbindung mit dem Projektor hergestellt ist, tippen oder klicken Sie auf *Fertig stellen*, um den Assistenten zu beenden und mit dem Projektor zu arbeiten.

Mobile Netzwerke und Remotezugriff

Die Methoden unterscheiden sich zwar grundlegend, aber Direktwahl-, Breitband-, VPN- und Direct-Access-Verbindungen ermöglichen Benutzern den Remotezugang zum Netzwerk ihrer Organisation. Bei einer typischen Direktwahlkonfiguration verwenden Remotebenutzer das Modem ihres Computers und eine normale Telefonleitung, um eine Verbindung mit einem Modempool im Büro herzustellen. Ein Windows-Server verwaltet den Modempool, authentifiziert die Anmeldekennung und das Kennwort mit dem *Routing- und RAS*-Dienst und autorisiert den Benutzer zum Zugriff auf das interne Netzwerk. Dann kann der Benutzer die Netzwerkressourcen verwenden, als wäre er vor Ort.

Abbildung 16.4 stellt Direktwahlverbindungen mit Modempools dar. Analogmodems verwenden Telefonleitungen, um Benutzer mit Übertragungsgeschwindigkeiten bis 56 KBit/s (Kilobit pro Sekunde) pro Kanal mit dem internen Netzwerk zu verbinden. Digitalmodems verwenden die Kanäle einer ISDN- oder T1-Leitung, um Benutzer mit Übertragungsgeschwindigkeiten bis zu 64 KBit/s mit dem internen Netzwerk zu verbinden. In einer Standardkonfiguration sind im Pool vielleicht 8, 12 oder 16 Modems vorhanden, von denen jedes über seine eigene Leitung oder seinen eigenen Übertragungskanal verfügt. Gewöhnlich gibt es eine spezielle Nummer für den Modempool, die von Benutzern angerufen werden kann. Unter dieser Nummer erhalten Benutzer eine Verbindung mit dem ersten Modem aus dem Pool. Wenn diese Nummer belegt ist, wird der Benutzer zur nächsten Nummer weitergeschaltet, die zu einer Verbindung mit dem nächsten Modem aus dem Pool führt, und so weiter. Auf diese Weise können Benutzer alle Modems des Pools unter derselben Nummer erreichen.

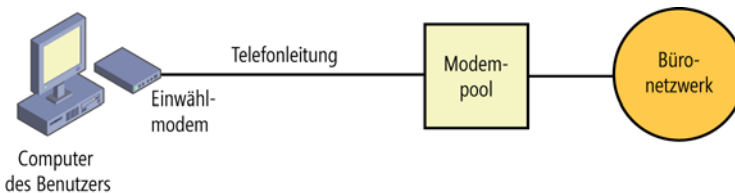


Abbildung 16.4 Die Verbindung mit dem Büronetzwerk kann mit einer Wahlverbindung über einen Modempool erfolgen

Im Gegensatz zur Direktwahlverbindung, die im Prinzip direkt zum Büronetzwerk erfolgt, werden Breitbandverbindungen über das Netzwerk eines ISPs (Internet Service Provider) hergestellt. Der DSL-Router, das Kabelmodem oder das Mobiltelefonmodem des Benutzers stellt eine Verbindung zum ISP her, der wiederum den Benutzer mit dem öffentlichen Internet verbindet. Um eine Verbindung mit dem Büronetzwerk herzustellen, müssen Breitbandbenutzer eine VPN- oder DirectAccess-Verbindung zwischen ihrem Computer und dem Büronetzwerk herstellen. Abbildung 16.5 skizziert, wie VPN und DirectAccess funktionieren, wenn der Benutzer entweder eine Telefonleitung mit DSL-Router oder ein Kabel mit Kabelmodem zur Verfügung hat.

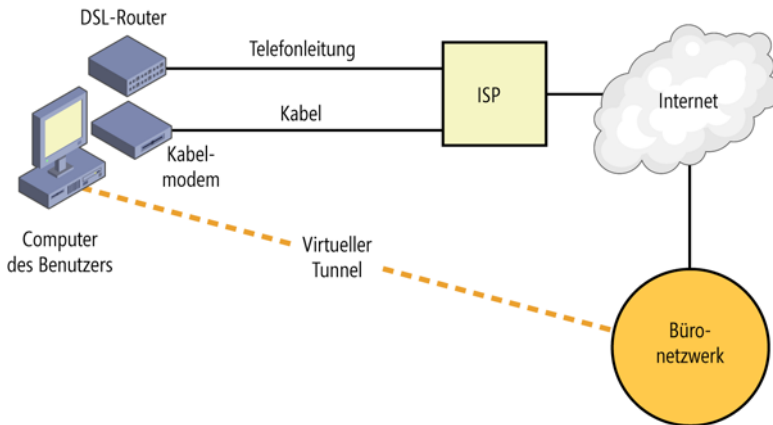


Abbildung 16.5 Die Verbindung zum Büronetzwerk kann auch durch einen virtuellen Tunnel erfolgen

Ein VPN ist im Prinzip eine Erweiterung des privaten Netzwerks, die über das öffentliche Internet erfolgt. Sobald ein Benutzer die Verbindung hergestellt hat, erscheint es ihm so, als wäre er direkt mit dem Büronetzwerk verbunden. Er kann die Netzwerkressourcen so verwenden, wie er es auch im Büro tun würde. Diese nahtlose Verbindung ist möglich, weil so etwas wie ein virtueller Tunnel zwischen dem Computer des Benutzers und dem Büronetzwerk eingerichtet wird. Dabei kümmert sich die VPN-Technologie um die Übertragung der Informationen über das öffentliche Internet. Gewöhnlich wird eine von zwei VPN-Technologien verwendet: PPTP (Point-to-Point Tunneling Protocol) oder L2TP (Layer 2 Tunneling Protocol).

L2TP und PPTP bieten Verschlüsselung und Schutz vor Angriffen, aber nur L2TP verwendet IPSec zur sicheren Verschlüsselung. Dadurch bietet es die höhere Sicherheit dieser beiden Varianten. Leider ist L2TP aber schwerer zu konfigurieren. Wenn Sie L2TP verwenden, müssen Sie die Microsoft-Zertifikatsdienste oder Zertifikatserver von anderen Anbietern verwenden, um für jedes System, das sich über L2TP mit dem Netzwerk verbinden will, Zertifikate auszustellen.

VPN können Sie aber nicht nur bei Breitbandverbindungen verwenden, sondern auch bei Wählverbindungen. Bei dieser Konfiguration stellen Benutzer erst eine Verbindung mit dem öffentlichen Internet her und dann eine private Verbindung mit dem Büronetzwerk. Wenn das die Standardprozedur für alle Wählverbindungen wird, braucht Ihre Organisation keine privaten Leitungen für den Modempool mehr zu reservieren.

DirectAccess ist ein anderer Ansatz für virtuelle Tunnel. Es unterscheidet sich zwar ganz erheblich von VPN, das Grundprinzip ist aber dasselbe: Eine DirectAccess-Verbindung ist eine Erweiterung eines privaten Netzwerks über das öffentliche Internet. Sobald ein Benutzer eine Verbindung aufgebaut hat (was automatisch passiert, wenn dieses Feature aktiviert ist), sieht es für ihn aus, als wäre er direkt mit dem Büronetzwerk verbunden. Er kann daher sofort auf Netzwerkressourcen zugreifen, so als würde er direkt im Büro arbeiten. Diese nahtlosen Verbindungen sind möglich, weil ein virtueller Tunnel zwischen dem Computer des Benutzers und dem Büronetzwerk aufgebaut wird, wobei die DirectAccess-Technologie selbstständig die Daten durch das öffentliche Internet leitet.

In Windows Server 2012 wurden DirectAccess und der Routing- und RAS-Dienst in der Rolle *Remotezugriff* zusammengefasst, doch die neue Implementierung unterscheidet sich von der Vorgängerversion aus Windows Server 2008 Release 2. Auch in der neuen Implementierung bleibt DirectAccess eine Client-/Server-Technologie, die auf IPv6 und IPSec aufbaut, es benötigt aber keine PKI (Public Key Infrastructure) mehr. Während DirectAccess in Windows Server 2008 R2 zwei IPSec-Tunnel verwendet, um die Verbin-

dung zum Unternehmensnetzwerk aufzubauen, beschränkt sich Windows Server 2012 standardmäßig auf einen einzigen IPSec-Tunnel (weil die Standardimplementierung keine Zertifikate für die Authentifizierung nutzt). Wenn Sie allerdings eine Zwei-Faktoren-Authentifizierung, etwa mit Smartcards und Netzwerkzugriffsschutzintegration, implementieren wollen, müssen Sie DirectAccess mit zwei IPSec-Tunneln bereitstellen.

Windows Server 2012-DirectAccess unterstützt mehrere Domänen und hat die Unterstützung für Netzwerklastenausgleich integriert. DirectAccess-Clients kommunizieren über IPv6, während sie ihre Remoteverbindung nutzen, aber der Remotezugriffsserver enthält eine integrierte Protokollumsetzung (NAT64) sowie ein Namensauflösungsgateway (DNS64), das die IPv6-Kommunikation von DirectAccess-Clients in IPv4 für die internen Server konvertiert. Auf diese Weise können DirectAccess-Clients auf reine IPv4-Intranetcomputer zugreifen, aber die reinen IPv4-Intranetcomputer können ihrerseits keine Verbindung zu DirectAccess-Clients aufbauen. Das hat den Grund, dass die Netzwerkadressübersetzung nur in einer Richtung funktioniert und für Kommunikation gedacht ist, die von DirectAccess-Clients eingeleitet wird.

Clientcomputer müssen unter der Enterprise Edition von Windows 7 oder neuer laufen. Servercomputer müssen unter Windows Server 2008 Release 2 oder neuer laufen. Damit Sie DirectAccess nutzen können, müssen Sie IPv6 inklusive DNSv6 und DHCPv6 sowohl auf den Client- als auch den Servercomputern einrichten und konfigurieren, und zwar im gesamten Unternehmen.

Im Gruppenrichtlinienzweig *Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Netzwerkverbindungen* können Sie mit der Richtlinie *Gesamten Datenverkehr über das interne Netzwerk weiterleiten* steuern, wie DirectAccess arbeitet. Wenn ein Benutzer eine Verbindung zum Arbeitsplatznetzwerk herstellt, greift der Computer des Benutzers in der Standardeinstellung auf Internetressourcen direkt zu, nicht über das Unternehmensnetzwerk. Wenn Sie diese Richtlinie aktivieren, verwendet der Computer des Benutzers das Unternehmensnetzwerk, um auf das Internet zuzugreifen.

Offensichtlich haben beide Ansätze ihre Vor- und Nachteile. Wenn Sie Internetverkehr nicht durch das interne Netzwerk weiterleiten, verringern Sie die Belastung und die Datenmenge in der Internetanbindung des Unternehmens. Dabei opfern Sie aber die zusätzlichen Sicherheitsmechanismen, die möglicherweise eingerichtet wurden, um das interne Netzwerk zu schützen. Leiten Sie den Internetverkehr dagegen durch das interne Netzwerk, erhöhen Sie die Belastung und die Datenmenge in der Internetanbindung des Unternehmens, und unter Umständen steigen Latenz und Reaktionszeiten gewaltig an, wenn der Benutzer mit Internetressourcen arbeitet. Andererseits stellen Sie sicher, dass alle zusätzlichen Sicherheitsmaßnahmen durchgesetzt werden, die das interne Netzwerk schützen.

Erstellen von Verbindungen für den Remotezugriff

Wie bereits beschrieben, können Sie Wahl- und Breitbandverbindungen für den Remotezugriff verwenden. Wenn Sie höhere Sicherheit wünschen, können Sie für diese Verbindungen VPN konfigurieren. Sobald Sie DirectAccess aktiviert haben, arbeitet es für den Benutzer völlig unbemerkt. Der Benutzer braucht lediglich eine Verbindung zum Internet aufzubauen, anschließend kann er sofort auf das Unternehmensnetzwerk zugreifen.

Microsoft Windows 8 bietet einen Assistenten für die Erstellung dieser Verbindungen. In den meisten Fällen werden Sie diesen Assistenten über das Netzwerk- und Freigabecenter starten. Tippen oder klicken Sie dazu im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten*. Dann können Sie Wahl-, Breitband- und VPN-Verbindungen herstellen.

PRAXISTIPP

Überlegen Sie, ob Sie Ihre Arbeit nicht durch Gruppenrichtlinien erleichtern können. Wenn Sie auf mehreren Computern dieselben Verbindungseinstellungen verwenden möchten, können Sie die Wähl- und VPN-Verbindungen mithilfe von Gruppenrichtlinieneinstellungen erstellen. Außerdem ist es möglich, die Einstellungen in Gruppenrichtlinien zu importieren. Die Einstellungen sind dann für alle Computer verfügbar, auf die dieses Gruppenrichtlinienobjekt angewendet wird. Diese Methode können Sie verwenden zur Einrichtung von neuen Verbindungskonfigurationen, für die Aktualisierung von vorhandenen Verbindungen, sofern Änderungen erforderlich sind, und auch um vorhandene Verbindungen zu löschen und durch neue zu ersetzen.

Erstellen einer Wählverbindung

Windows 8 bietet zwei Optionen für Wählverbindungen. Sie können eine Wählverbindung zu einem ISP herstellen oder eine Wählverbindung zum Arbeitsplatz. Die Verbindungen werden zwar auf etwas unterschiedliche Weise eingerichtet, aber die Einstellungen sind weitgehend dieselben, mit folgenden Ausnahmen:

- Eine Wählverbindung zu einem ISP verwendet *nicht* die Komponente *Client für Microsoft-Netzwerke* und versucht standardmäßig eine Neuwahl, falls die Verbindung unterbrochen wird.
- Eine Wählverbindung zum Arbeitsplatz verwendet die Komponente *Client für Microsoft-Netzwerke* und versucht standardmäßig *keine* Neuwahl, falls die Verbindung unterbrochen wird.

Die Netzwerkkomponente *Client für Microsoft-Netzwerke* ermöglicht Windows 8-Systemen die Kommunikation in einer Windows-Domäne oder -Arbeitsgruppe. Da an den meisten Arbeitsplätzen Windows-Domänen oder -Arbeitsgruppen verwendet werden, bei einigen ISPs aber nicht, wird die Komponente für Umgebungen am Arbeitsplatz konfiguriert, und nicht für ISPs.

Die Erstellung von Wählverbindungen erfolgt in zwei Schritten. Bevor Sie eine Wählverbindung einrichten, sollten Sie die aktuellen Telefon- und Modemoptionen überprüfen, mit denen die Wählregeln festgelegt werden. Sobald die Wählregeln konfiguriert sind, können Sie eine Wählverbindung erstellen.

Arbeiten mit Wählregeln und Standorten

Wählregeln legen fest, welche Nummern Modems wählen sollen und welche zusätzlichen Dinge bei der Verbindung zu beachten sind. Die fertigen Wählregeln werden im Systemsteuerungstool *Telefon und Modem* als Standorte gespeichert.

Anzeigen und Einstellen des eigenen Standorts

Um den eigenen Standort (den Standardstandort) anzuzeigen und einzustellen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie im Fenster *Systemsteuerung* in der Dropdownliste *Anzeige* auf *Große Symbole* oder *Kleine Symbole*.
2. Tippen oder klicken Sie auf *Telefon und Modem*. Wenn Sie dieses Programm zum ersten Mal starten, erscheint das Dialogfeld *Standortinformationen* (Abbildung 16.6).
3. Geben Sie die folgenden Daten ein, um den Standardstandort (eigenen Standort) zu konfigurieren:
 - **Land/Region** Legt das Land (oder die Region) fest, in dem Sie sich befinden, beispielsweise Deutschland.
 - **Ortskennzahl** Die Vorwahl Ihres Standorts, zum Beispiel 89.

- **Netzkennzahl (falls erforderlich)** Hier können Sie ein Telefonnetz angeben, das für die Wahl und Herstellung der Verbindungen benutzt werden soll. Diese Angabe kann erforderlich sein, wenn Sie Ferngespräche oder internationale Verbindungen verwenden.
- **Amtskennziffer (falls erforderlich)** Geben Sie die Nummer ein, die Sie brauchen, um ein Amt zu erreichen, sofern erforderlich. Dieser Code kann bei bestimmten Telefonanlagen oder in Hotels erforderlich sein.

Standortinformationen

Damit Sie Telefon- oder Modemverbindungen herstellen können, müssen Sie folgende Informationen zu Ihrem Standort angeben.

Land/Region
Deutschland

Ortskennzahl
89

Netzkennzahl (falls erforderlich)

Amtskennziffer (falls erforderlich)
9

Wählverfahren für den Standort:
☒ MFV (Ton) ☐ IWW (Impuls)

OK Abbrechen

Abbildung 16.6 Wenn Sie das erste Mal *Telefon und Modem* verwenden, müssen Sie den Standort angeben

Telefon und Modem

Wählregeln Modems Erweitert

In der folgenden Liste sind alle angegebenen Standorte aufgelistet. Wählen Sie den Standort aus, von dem aus gewählt werden soll.

Standorte:

Standort	Ortskennzahl
☒ Eigener Standort	89

Neu... Bearbeiten... Löschen

OK Abbrechen Übernehmen

Abbildung 16.7 Überprüfen Sie, ob die Wählregeln richtig konfiguriert sind

4. Wählen Sie unter *Wählverfahren für den Standort* nach Bedarf *MFV (Ton)* oder *IWV (Impuls)*. In den meisten Gebieten dürfte die Tonwahl verwendbar sein.
5. Sobald Sie einen Standort definiert und auf *OK* geklickt haben, können Sie das Dialogfeld *Telefon und Modem* sehen (Abbildung 16.7).

Von diesem Zeitpunkt an brauchen Sie keinen Standardstandort mehr einzurichten.

Die für einen Computer konfigurierten Standorte werden in der Liste *Standorte* mit Namen und Ortskennzahl aufgeführt. Der Ort, von dem aus Sie anrufen, ist ausgewählt und wird durch Fettschrift hervorgehoben.

6. Anfangs wird der Standardstandort als eigener Standort festgelegt. Wenn Sie einen anderen Standort wählen, können Sie ihn zum aktuellen oder Standardstandort machen. Ich empfehle, den Standardstandort (eigener Standort) zu überarbeiten und ihm einen Namen zu geben, der auch die Stadt oder den Standort des Büros enthält. Wenn Sie die Einstellungen für einen ausgewählten Standort überprüfen möchten, tippen oder klicken Sie auf *Bearbeiten*. Um dem Standort einen anderen Namen zu geben, geben Sie im Feld *Standortname* auf der Registerkarte *Allgemein* den neuen Namen ein und tippen oder klicken dann auf *OK*.

HINWEIS

Von allen Wählregeln werden Sie vermutlich am häufigsten mit der Ortskennzahl zu tun haben. Bei der Installation des Betriebssystems ist vielleicht die falsche oder gar keine Ortskennzahl festgelegt worden. Und die festgelegte Ortskennzahl ist meistens nicht die Vorwahl, die der Benutzer braucht, wenn er von zu Hause aus eine Verbindung herstellen möchte.

Definieren von Wählstandorten

Sie können unterschiedliche Wählstandorte definieren, indem Sie für jede Ortskennzahl, die der Benutzer für seine Verbindungen benutzt, einen passenden Satz an Regeln festlegen. Einen Wählstandort definieren Sie so:

1. Tippen oder klicken Sie im Fenster *Systemsteuerung* in der Dropdownliste *Anzeige* auf *Große Symbole* oder *Kleine Symbole*.
2. Tippen oder klicken Sie auf *Telefon und Modem*. Tippen oder klicken Sie im Dialogfeld *Telefon und Modem* auf der Registerkarte *Wählregeln* auf *Neu*. Daraufhin öffnet sich das Dialogfeld *Neuer Standort*.
3. Das Dialogfeld *Neuer Standort* hat drei Registerkarten:
 - **Allgemein** Legt den Standortnamen fest, das Land (die Region) und die Ortskennzahl. Auf dieser Registerkarte können Sie auch die Amtskennziffern für Orts- und Ferngespräche angeben, die Wartefunktion beim Wählen deaktivieren und zwischen Ton- und Impulswahl wählen. Achten Sie darauf, dass Sie einen gut verständlichen Standortnamen vergeben. Gewöhnlich ist dies der Name der Stadt oder des Gebiets, in dem der Benutzer die Verbindung herstellt.
 - **Ortskennzahlregeln** Legt die Regeln für Verbindungen von einem Standort zu einem anderen und innerhalb des Standorts fest. Diese Regeln sind auch von Nutzen, wenn Verbindungen innerhalb des Kennzahlgebiets (oder Bereichscodes) je nach Präfix Orts- oder Ferngespräche sind.
 - **Callingcard** Legt die Callingcard für Anrufe von diesem Standort fest. Die Callingcardinformationen der größeren Telefongesellschaften werden angeboten. Sie können auch neue Callingcarddatensätze erstellen.
4. Wenn Sie einen Standort definiert haben, überprüfen Sie, ob der Standardstandort im Dialogfeld *Telefon und Modem* noch stimmt. Vielleicht müssen Sie einen anderen Eintrag wählen. Tippen oder klicken Sie auf *OK*.

Löschen von Wahlstandorten

Einen Wahlstandort löschen Sie folgendermaßen:

1. Tippen oder klicken Sie im Fenster *Systemsteuerung* in der Dropdownliste *Anzeige* auf *Große Symbole* oder *Kleine Symbole*. Tippen oder klicken Sie auf *Telefon und Modem*.
2. Wählen Sie im Dialogfeld *Telefon und Modem* den Standort, den Sie löschen wollen, und tippen oder klicken Sie dann auf *Löschen*. Wenn Sie zur Bestätigung des Vorgangs aufgefordert werden, tippen oder klicken Sie auf *Ja*.
3. Wählen Sie den Wahlstandort aus, den Sie als Standardstandort einstellen möchten, und tippen oder klicken Sie dann auf *OK*.

Erstellen einer Internet-Wahlverbindung zu einem ISP

Sie können folgendermaßen Wahlverbindungen erstellen:

- Wenn Benutzer eine Verbindung über einen ISP herstellen, der seine eigenen Standorte (Point of Presence, POP) über das ganze Land (oder die ganze Welt) verteilt anbietet, konfigurieren Sie gewöhnlich Wahlregeln und Verbindungen für bestimmte Standorte. Sie können beispielsweise einen Wahlstandort namens *Seattle* erstellen und eine Wahlverbindung namens *Verbindung mit ISP in Seattle aufnehmen*. In dieser Konfiguration geben Sie die Ortskennzahl für Seattle ein und legen die erforderlichen speziellen Wahlregeln fest. Natürlich legen Sie auch alle weiteren Nummern und Zahlen fest, die in Seattle für die Verbindung mit dem ISP erforderlich sind. Außerdem müssen Sie den Benutzern noch zeigen, wie man den aktuellen Standort einstellt, wenn man durch das Land reist.
- Wenn Benutzer spezielle Nummern wählen, um beispielsweise per Ferngespräch Verbindung zum Modempool im Büro aufzunehmen oder einen speziellen Anschluss eines ISPs zu wählen, konfigurieren Sie normalerweise separate Verbindungen statt separater Standorte. In diesem Fall erstellen Sie eine Verbindung, die per Ferngespräch die gewünschte Verbindung herstellt, sowie eine Verbindung, die verwendet wird, wenn sich der Benutzer im lokalen Umfeld aufhält. Dann brauchen Sie nur einen Wahlstandort.

Um eine Wahlverbindung zum Internet herzustellen, gehen Sie folgendermaßen vor:

1. Bevor Sie die Wahlverbindung erstellen, überprüfen Sie die aktuellen Telefon- und Modemoptionen, wie im Abschnitt »Arbeiten mit Wahlregeln und Standorten« weiter oben in diesem Kapitel beschrieben.

HINWEIS

Wenn Sie für eine Verbindung Wahlregeln und dann Ortskennzahl und Land festlegen, lässt sich die Verbindung eventuell auch für Ferngespräche benutzen, die unter Umständen sehr teuer werden. Wenn Sie das verhindern möchten, sollten Sie diese Angaben noch einmal genau überprüfen.

2. Tippen oder klicken Sie im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten*. Daraufhin wird der Assistent *Eine Verbindung oder ein Netzwerk einrichten* gestartet.
3. Wählen Sie *Verbindung mit dem Internet herstellen* und tippen oder klicken Sie auf *Weiter*. Ist der Computer bereits mit dem Internet verbunden, müssen Sie auf *Trotzdem eine neue Verbindung einrichten* tippen oder klicken. Wenn bereits eine Wahlverbindung vorhanden ist, können Sie diese Verbindung umkonfigurieren oder eine neue Verbindung erstellen. Üblicherweise erstellen Sie eine neue Verbindung, wählen Sie also *Nein, eine neue Verbindung erstellen* aus und tippen oder klicken Sie auf *Weiter*.

4. Geben Sie im Textfeld *Einwählrufnummer* die Telefonnummer ein, die für diese Verbindung angerufen werden soll.
5. Machen Sie nun die Angaben für das Konto. Geben Sie im Feld *Benutzername* den Namen des Benutzers ein und im Feld *Kennwort* das Kennwort. Durch die Wahl von *Dieses Kennwort speichern* können Sie zwar dafür sorgen, dass das Kennwort gespeichert wird, aber empfehlenswert ist das nicht, weil es jedem, der Zugriff auf den Computer hat, die Verwendung dieser Verbindung erlaubt.
6. Im Feld *Verbindungsname* geben Sie der Verbindung einen Namen, beispielsweise *Dienstanbieter*. Denken Sie daran, dass der Name zwar kurz sein sollte (50 Zeichen oder weniger), aber auch gut verständlich.
7. Wenn die Verbindung für alle Benutzer des Computers verfügbar sein soll, wählen Sie *Anderen Benutzern erlauben, diese Verbindung zu verwenden*. Diese Option ist nützlich, wenn Sie die Verbindung über Gruppenrichtlinien verfügbar machen möchten und keine Benutzeranmeldeinformationen angegeben haben.
8. Tippen oder klicken Sie auf *Verbinden*, um die Wählverbindung zu erstellen und eine Verbindung herzustellen. Sofern Sie jetzt keine Verbindung aufbauen wollen, können Sie auf *Überspringen* tippen oder klicken. Tippen oder klicken Sie dann auf *Schließen*. Um die Verbindung zu testen, folgen Sie der Beschreibung im Abschnitt »Herstellen von Verbindungen« weiter unten in diesem Kapitel.

PRAXISTIPP

Die meisten Organisationen verwenden digitale Telefonsysteme, die keine externen Analogverbindungen zulassen. Wenn dies auch in Ihrem Büro der Fall ist, brauchen Sie Zugang zu einer Analogleitung, um die Verbindung zu testen. Manche Digitaltelefone können mit Digital-zu-analog-Wandlern ausgerüstet werden, die Sie für den Test von Wählverbindungen verwenden können. Häufig findet man solche Konverter bei Konferenztelefonen oder Faxgeräten. Manchmal sind Konferenztelefone oder Faxgeräte auch direkt an analogen Telefonleitungen angeschlossen.

Erstellen einer Wählverbindung zum Arbeitsplatz

Eine Wählverbindung zum Arbeitsplatznetzwerk bauen Sie ähnlich auf wie eine Wählverbindung zum Internet. Gehen Sie folgendermaßen vor, um eine Wählverbindung zum Arbeitsplatz zu erstellen:

1. Tippen oder klicken Sie im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten*. Daraufhin wird der Assistent *Eine Verbindung oder ein Netzwerk einrichten* gestartet.
2. Wählen Sie *Verbindung mit dem Arbeitsplatz herstellen* aus und tippen oder klicken Sie auf *Weiter*. Sofern Sie schon eine Verbindung haben, können Sie die Konfiguration dieser Verbindung ändern oder eine neue Verbindung erstellen. Üblicherweise erstellen Sie eine neue Verbindung, tippen oder klicken Sie also auf *Nein, eine neue Verbindung erstellen*.
3. Tippen oder klicken Sie auf der Seite *Wie möchten Sie eine Verbindung herstellen* auf *Direkt wählen*.
4. Geben Sie im Textfeld *Rufnummer* die Telefonnummer ein, die für diese Verbindung gewählt werden soll. Tragen Sie im Feld *Zielname* den Namen für die Verbindung ein, beispielsweise »Hauptniederlassung« oder »Büro Seattle«. Denken Sie daran, dass der Name kurz (höchstens 50 Zeichen), aber aussagekräftig sein sollte.
5. Aktivieren Sie *Eine Smartcard verwenden*, wenn Sie eine Smartcard für die Verbindung benutzen wollen.
6. Wenn die Verbindung allen Benutzern des Computers zur Verfügung stehen soll, können Sie das Kontrollkästchen *Anderen Benutzern erlauben, diese Verbindung zu verwenden* aktivieren. Das ist besonders nützlich, wenn Sie die Verbindung über Gruppenrichtlinien zuweisen wollen und keine Benutzeranmeldungsdaten eingeben.

7. Sofern Sie die Verbindung nicht gleich testen wollen, können Sie das Kontrollkästchen *Jetzt nicht verbinden* aktivieren. Meist nutzen Sie diese Möglichkeit, um den Verbindungsaufbau zu überspringen. Andernfalls schlägt der Verbindungsaufbau möglicherweise fehl, wenn Sie eine Verbindung für einen anderen Standort einrichten, etwa die Internetverbindung zu Hause bei einem Benutzer, und diese Einstellungen im Netzwerk des Unternehmens nicht funktionieren.
8. Tippen oder klicken Sie auf *Weiter*. Geben Sie die Kontoinformationen für die Verbindung ein. Tragen Sie den Benutzernamen und das Kennwort in die entsprechenden Felder ein.

SICHERHEIT

Sie können zwar mit dem Kontrollkästchen *Dieses Kennwort speichern* festlegen, dass das Kennwort gespeichert wird, das ist aber aus Sicherheitsgründen abzulehnen, weil auf diese Weise jeder, der Zugriff auf den Computer hat, die Verbindung nutzen kann.

9. Wenn Sie eine Verbindung zu einer Domäne herstellen, können Sie die Domäne, bei der Sie sich anmelden, im Feld *Domäne* eintragen.
10. Wenn Sie vorher angegeben haben, dass Sie die Verbindung jetzt nicht herstellen wollen, müssen Sie auf *Erstellen* tippen oder klicken, um die Verbindung zu erstellen. Tippen oder klicken Sie andernfalls auf *Verbinden*, um die Verbindung zu erstellen und sich einzuwählen. Tippen oder klicken Sie auf *Schließen*.

In den Gruppenrichtlinien können Sie Wählverbindungen mithilfe von Richtlinieneinstellungen im Zweig *Netzwerkoptionen* erstellen, bearbeiten und löschen. Gehen Sie folgendermaßen vor, um Richtlinien für Netzwerkoptionen zu konfigurieren:

1. Öffnen Sie ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) zum Bearbeiten im Gruppenrichtlinienobjekt-Editor. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Netzwerkoptionen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Netzwerkoptionen* auswählen.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Netzwerkoptionen* oder halten Sie ihn gedrückt, und wählen Sie *Neu/DFÜ-Verbindung*. Daraufhin öffnet sich das Eigenschaftendialogfeld für die Wählverbindung.
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Erstellen*, *Aktualisieren* oder *Ersetzen* aus.
4. Wählen Sie *Verbindung für alle Benutzer* aus, wenn die Verbindung allen Benutzern des Computers zur Verfügung stehen soll, oder *Benutzerverbindung*, wenn die Verbindung nur dem Benutzer zur Verfügung stehen soll, für den die Richtlinie verarbeitet wird.
5. Geben Sie einen Verbindungsnamen und die Rufnummer ein.
6. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. In vielen Fällen ist es sinnvoll, die Richtlinie nur einmal anzuwenden. Aktivieren Sie in diesem Fall *Nur einmal anwenden*.
7. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Erstellen einer Breitbandverbindung zum Internet

In mancher Hinsicht sind Breitbandverbindungen viel leichter zu konfigurieren als Wählverbindungen. Wenn Sie mit Breitbandverbindungen arbeiten, brauchen Sie keine Wählregeln festzulegen oder Standorte zu definieren. Sie brauchen sich auch keine Gedanken über Callingcards, ISP-Zugriffsnummern oder Wiederholungsprioritäten zu machen. Das macht die Verwendung von Breitbandverbindungen sehr viel einfacher.

Manche Breitbandanbieter geben ihren Kunden einen Router oder ein Modem, das sie für die Verbindung zum Dienstanbieter brauchen. Außerdem braucht jeder Benutzer einen Netzwerkadapter in seinem Computer, über den die Verbindung zum DSL-Router oder Kabelmodem hergestellt wird. In dieser Konfiguration ist es erforderlich, dass die Verbindung über das LAN erfolgt statt über eine bestimmte Breitbandverbindung. Daher ist es die LAN-Verbindung, die korrekt eingerichtet werden muss, damit eine Internetverbindung möglich wird. Eine spezielle Breitbandverbindung brauchen Sie nicht zu erstellen.

Bei Bedarf können Sie allerdings eine Breitbandverbindung einrichten. In manchen Fällen müssen Sie das tun, um bestimmte Anforderungen an die Konfiguration zu erfüllen, die der ISP stellt, beispielsweise sichere Authentifizierung, oder damit Sie den Benutzernamen und das Kennwort eingeben können, die der Breitbandanbieter verlangt.

Eine Breitbandverbindung mit dem Internet erstellen Sie folgendermaßen:

1. Tippen oder klicken Sie im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten*. Daraufhin wird der Assistent *Eine Verbindung oder ein Netzwerk einrichten* gestartet.
2. Wählen Sie *Verbindung mit dem Internet herstellen* aus und tippen oder klicken Sie auf *Weiter*. Ist der Computer bereits mit dem Internet verbunden, müssen Sie auf *Trotzdem eine neue Verbindung einrichten* tippen oder klicken. Sofern Sie schon eine Verbindung eingerichtet haben, können Sie die Konfiguration dieser Verbindung ändern oder eine neue Verbindung erstellen. Üblicherweise erstellen Sie eine neue Verbindung, wählen Sie also *Nein, eine neue Verbindung erstellen* aus und tippen oder klicken Sie auf *Weiter*.
3. Tippen oder klicken Sie auf der Seite *Wie möchten Sie eine Verbindung herstellen* auf *Breitband (PPPoE)*, um eine Breitbandverbindung zum Internet zu erstellen.
4. Nehmen Sie nun folgende Einstellungen vor und tippen oder klicken Sie auf *Weiter*:
 - Tragen Sie die Kontoinformationen für die Verbindung ein. Tragen Sie den Benutzernamen und das Kennwort in die entsprechenden Felder ein.

SICHERHEIT

Sie können zwar mit dem Kontrollkästchen *Dieses Kennwort speichern* festlegen, dass das Kennwort gespeichert wird, das ist aber aus Sicherheitsgründen abzulehnen, weil auf diese Weise jeder, der Zugriff auf den Computer hat, die Verbindung nutzen kann.

- Tragen Sie im Feld *Verbindungsname* den Namen für die Verbindung ein, beispielsweise »Sichere Breitbandverbindung zum Büro Seattle«. Denken Sie daran, dass der Name kurz (höchstens 50 Zeichen), aber aussagekräftig sein sollte.
- Wenn die Verbindung allen Benutzern des Computers zur Verfügung stehen soll, können Sie das Kontrollkästchen *Anderen Benutzern erlauben, diese Verbindung zu verwenden* aktivieren. Das ist besonders nützlich, wenn Sie die Verbindung über Gruppenrichtlinien zuweisen wollen und keine Benutzeranmeldungsdaten eingegeben haben.

5. Tippen oder klicken Sie auf *Verbinden*, um die Verbindung zu erstellen und sie aufzubauen. Gewöhnlich schlägt der erste Test fehl, weil Sie eine Breitbandverbindung für einen anderen Ort einrichten, beispielsweise für die Internetverbindung, die der Benutzer zu Hause verwenden soll, und diese Einstellungen funktionieren nicht im Firmennetzwerk. Deswegen haben Sie die Möglichkeit, auf *Überspringen* zu tippen oder zu klicken, um den Verbindungstest zu überspringen. Tippen oder klicken Sie auf *Schließen*.

TIPP

Um eine Breitbandverbindung zu testen, brauchen Sie einen DSL-Router oder ein Kabelmodem. Achten Sie darauf, dass Sie alle speziellen Konfigurationen vornehmen, die der ISP vielleicht verlangt, wie im Abschnitt »Einstellen der Verbindungseigenschaften« weiter unten in diesem Kapitel beschrieben.

Erstellen einer VPN-Verbindung

VPNs dienen zur Einrichtung von sicheren Kommunikationskanälen über eine vorhandene Wähl- oder Breitbandverbindung. Sie müssen die IP-Adresse oder den vollqualifizierten Domännennamen des Remotezugriffsservers kennen, mit dem Sie eine Verbindung herstellen möchten. Wenn die erforderliche Verbindung verfügbar ist und Sie die erforderlichen Angaben über den Host kennen, können Sie die Verbindung folgendermaßen einrichten:

1. Tippen oder klicken Sie im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten*. Daraufhin wird der Assistent *Eine Verbindung oder ein Netzwerk einrichten* gestartet.
2. Um eine VPN-Verbindung zu erstellen, wählen Sie *Verbindung mit dem Arbeitsplatz herstellen* und tippen oder klicken auf *Weiter*.
3. Wenn Sie bereits eine Wählverbindung eingerichtet haben, müssen Sie *Nein, eine neue Verbindung erstellen* auswählen und dann auf *Weiter* tippen oder klicken.
4. Tippen oder klicken Sie auf *Die Internetverbindung (VPN) verwenden*.
5. Der Benutzer muss eine Verbindung zum Internet herstellen, sei es als Einwahl- oder als Breitbandverbindung, bevor er das VPN verwenden kann. Wählen Sie eine vorhandene Verbindung aus und tippen oder klicken Sie auf *Weiter*.
6. Geben Sie die IPv4- oder IPv6-Adresse oder den vollqualifizierten Domännennamen des Computers an, mit dem eine Verbindung hergestellt werden soll, wie zum Beispiel 157.54.0.1 oder *external.microsoft.com*. In den meisten Fällen dürfte es sich um einen Remotezugriffsserver handeln, den Sie für das Büronetzwerk konfiguriert haben.
7. Geben Sie der Verbindung im Feld *Zielname* einen Namen. Wenn der Computer so konfiguriert ist, dass die Authentifizierung mit Smartcard erfolgt, wählen Sie *Eine Smartcard verwenden*.
8. Wenn die Verbindung für alle Benutzer des Computers verfügbar sein soll, wählen Sie *Anderen Benutzern erlauben, diese Verbindung zu verwenden*. Diese Option ist am besten geeignet, wenn Sie die Verbindung über Gruppenrichtlinien verfügbar machen möchten und keine Benutzeranmeldeinformationen angegeben haben.

SICHERHEIT

Sie können zwar mit dem Kontrollkästchen *Anmeldedaten speichern* festlegen, dass die Anmeldeinformationen gespeichert werden, das ist aber aus Sicherheitsgründen abzulehnen, weil auf diese Weise jeder, der Zugriff auf den Computer hat, die Verbindung nutzen kann. Wenn Sie *Anmeldedaten speichern* deaktiviert lassen, wird der Benutzer aufgefordert, sein Kennwort einzugeben.

9. Tippen oder klicken Sie auf *Erstellen*.

In den Gruppenrichtlinien können Sie VPN-Verbindungen mithilfe von Richtlinieneinstellungen im Zweig *Netzwerkoptionen* erstellen, bearbeiten und löschen. Gehen Sie folgendermaßen vor, um Richtlinien für Netzwerkoptionen zu konfigurieren:

1. Öffnen Sie ein Gruppenrichtlinienobjekt zum Bearbeiten im Gruppenrichtlinienobjekt-Editor. Wenn Sie Einstellungen für Computer konfigurieren wollen, müssen Sie den Knoten *Computerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Netzwerkoptionen* auswählen. Wollen Sie dagegen Einstellungen für Benutzer konfigurieren, müssen Sie *Benutzerkonfiguration\Einstellungen\Systemsteuerungseinstellungen* erweitern und dann *Netzwerkoptionen* auswählen.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Netzwerkoptionen* oder halten Sie ihn gedrückt, und wählen Sie *Neu/VPN-Verbindung*. Daraufhin öffnet sich das Eigenschaftendialogfeld für die Verbindung.
3. Wählen Sie in der Dropdownliste *Aktion* den Eintrag *Erstellen*, *Aktualisieren* oder *Ersetzen* aus.
4. Wählen Sie *Verbindung für alle Benutzer* aus, wenn die Verbindung allen Benutzern des Computers zur Verfügung stehen soll, oder *Benutzerverbindung*, wenn die Verbindung nur dem Benutzer zur Verfügung stehen soll, für den die Richtlinie verarbeitet wird.
5. Geben Sie einen Verbindungsnamen und die IP-Adresse ein. Stattdessen können Sie auch das Kontrollkästchen *DNS-Name verwenden* aktivieren und dann den vollqualifizierten Domänennamen eingeben.
6. Wählen Sie auf der Registerkarte *Sicherheit* die Option *Erweitert* aus. Legen Sie in der Dropdownliste *Datenverschlüsselung* fest, ob und wie Verschlüsselung eingesetzt werden soll. Gewöhnlich ist es sinnvoll, die Verschlüsselung erforderlich zu machen. Stellen Sie unter *Anmeldesicherheit* ein, welche Sicherheitsoptionen verwendet werden sollen.
7. Legen Sie mit den Optionen auf der Registerkarte *Gemeinsam* fest, wie die Einstellungen angewendet werden. In vielen Fällen ist es sinnvoll, die Richtlinie nur einmal anzuwenden. Aktivieren Sie in diesem Fall *Nur einmal anwenden*.
8. Tippen oder klicken Sie auf OK. Wenn die Gruppenrichtlinien das nächste Mal aktualisiert werden, wird das Einstellungselement angewendet, wie es im Gruppenrichtlinienobjekt festgelegt ist, in dem Sie das Einstellungselement definiert haben.

Einstellen der Verbindungseigenschaften

Wenn Sie mit einer Wähl-, Breitband- oder VPN-Verbindung arbeiten, müssen Sie nach der Erstellung der Verbindung oft noch zusätzliche Eigenschaften festlegen. In diesem Abschnitt werden die wichtigsten Eigenschaften beschrieben, mit denen Sie es zu tun haben werden.

HINWEIS

Vergessen Sie bei der Einstellung der Verbindungseigenschaften nicht, dass eine VPN-Verbindung auf eine vorhandene Wähl- oder Breitbandverbindung angewiesen ist und dass die Konfiguration der beiden Verbindungen unabhängig voneinander erfolgt. Was VPN betrifft, wird zuerst die Trägerverbindung mit den Einstellungen eingerichtet, die für sie erforderlich sind. Dann erfolgt der Versuch, darauf mit den VPN-Einstellungen eine VPN-Verbindung aufzubauen. Im Hinblick auf dieses Zusammenspiel sollten Sie zuerst die Trägerverbindung einrichten und dann erst die VPN-Einstellungen vornehmen. Weichen Sie nur davon ab, wenn Sie versuchen, VPN-Probleme zu beheben. In diesem Fall sollten Sie mit der VPN-Konfiguration beginnen und sich dann bis zurück zu den Einstellungen für die Trägerverbindung durcharbeiten.

Einstellen der automatischen oder manuellen Verbindungen

Windows 8 kann so eingestellt werden, dass es Wähl-, Breitband- oder VPN-Verbindungen automatisch herstellt, wenn ein Benutzer Programme verwendet, die eine Internetverbindung brauchen, wie beispielsweise einen Webbrowser. Wie automatische Verbindungen funktionieren, hängt von den Einstellungen im Dialogfeld *Eigenschaften von Internet* ab. Folgende Optionen stehen zur Wahl:

- **Keine Verbindung wählen** Benutzer müssen Verbindungen manuell herstellen.
- **Nur wählen, wenn keine Netzwerkverbindung besteht** Die Verbindung wird bei Bedarf automatisch hergestellt, aber nur dann, wenn keine Netzwerkverbindung besteht.
- **Immer Standardverbindung wählen** Die Standardverbindung wird immer hergestellt, wenn eine Internetverbindung gebraucht wird (selbst wenn bereits andere Verbindungen bestehen).

TIPP Die beste Einstellung für automatische Verbindungen hängt davon ab, wie Ihre Organisation arbeitet. Im Gegensatz zu dem, was viele Administratoren vermuten, sind Benutzer mobiler Geräte gewöhnlich weniger frustriert, wenn ihre Computer auf *Keine Verbindung wählen* eingestellt sind. Das liegt einfach daran, dass die Benutzer oft keine Wählverbindungen einrichten können, wenn sie nicht im Büro sind. Und es ist einfach lästig, wenn der Computer beim Kundenbesuch oder bei einer Präsentation ständig versucht, irgendwelche Telefonnummern zu wählen. Andererseits werden Benutzer mit Desktopcomputern in einem externen Büro oder zu Hause vermutlich automatische Verbindungen bevorzugen.

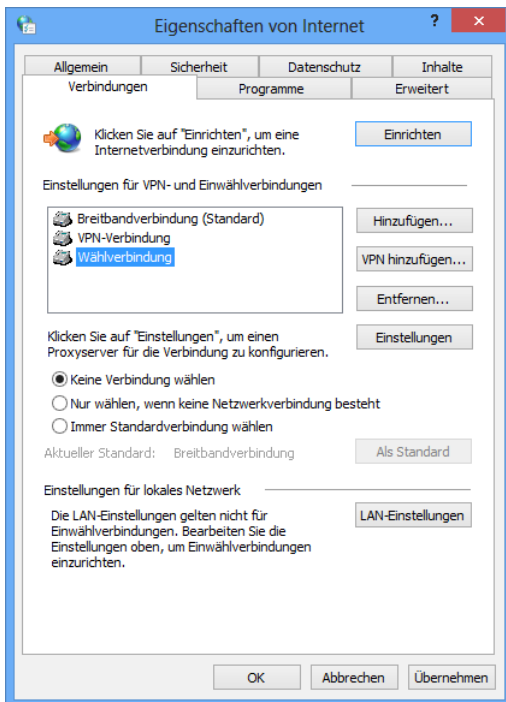


Abbildung 16.8 Auf der Registerkarte *Verbindungen* stellen Sie ein, ob Verbindungen automatisch oder manuell hergestellt werden

Um Computer auf eine manuelle Verbindung einzustellen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet*. Tippen oder klicken Sie in *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen* (Abbildung 16.8).
2. Wählen Sie *Keine Verbindung wählen* und tippen oder klicken Sie dann auf *OK*.

Mit folgenden Schritten können Sie automatische Verbindungen einstellen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet*. Tippen oder klicken Sie in *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie *Nur wählen, wenn keine Netzwerkverbindung besteht*, wenn die Verbindungen automatisch hergestellt werden sollen, wenn keine LAN-Verbindung verfügbar ist. Wählen Sie *Immer Standardverbindung wählen*, wenn die Verbindungen immer automatisch hergestellt werden sollen.
3. Die Liste *Einstellungen für VPN- und Einwählverbindungen* zeigt die konfigurierten Wähl-, Breitband- und VPN-Verbindungen. Wählen Sie die Verbindung, die Sie bei der Herstellung von Verbindungen als Standardverbindung verwenden möchten, und tippen oder klicken Sie dann auf *Als Standard*.
4. Tippen oder klicken Sie auf *OK*.

Einstellen des Proxys für mobile Verbindungen

Wie die Einstellungen der Verbindungen lassen sich auch die Einstellungen für Proxyserver manuell oder automatisch durchführen. Bei der manuellen Konfiguration müssen Sie jede Eigenschaft selbst festlegen, Schritt für Schritt. Bei der automatischen Konfiguration kann der Computer versuchen, die Proxyservereinstellungen zu ermitteln und dann die Optionen festzulegen, oder er liest die Werte aus einem Konfigurationsskript.

HINWEIS

Proxysteinstellungen für mehrere Systeme lassen sich in den Gruppenrichtlinien durchführen. Wenn Sie die Proxysteinstellungen nicht mit Gruppenrichtlinien vornehmen wollen, können Sie die Einstellungen für die Verbindungen einzeln durchführen, wie in diesem Abschnitt besprochen.

Konfigurationsskripts lassen sich auf dem lokalen Computer in einer Datei oder unter einer Internetadresse speichern. Die Verwendung von Konfigurationsskripten kann viel Zeit ersparen, da sonst jede Verbindung, die eingerichtet wird, separat konfiguriert werden muss. Außerdem können sich die VPN-Einstellungen von denen ihrer Trägerverbindung unterscheiden, da VPN-Verbindungen auf vorhandenen Verbindungen aufsetzen.

Zur automatischen Konfiguration der Proxys für eine Verbindung gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet*. Tippen oder klicken Sie in *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie im Listenfeld *Einstellungen für VPN- und Einwählverbindungen* die Verbindung aus, die Sie einstellen möchten, und tippen oder klicken Sie dann auf *Einstellungen*. Es erscheint ein Dialogfeld wie das *Einstellungen*-Dialogfeld aus Abbildung 16.9.
3. Wenn Sie eine automatische Ermittlung der Proxyeinstellung bei der Herstellung einer Verbindung wünschen, wählen Sie *Einstellungen automatisch erkennen*.

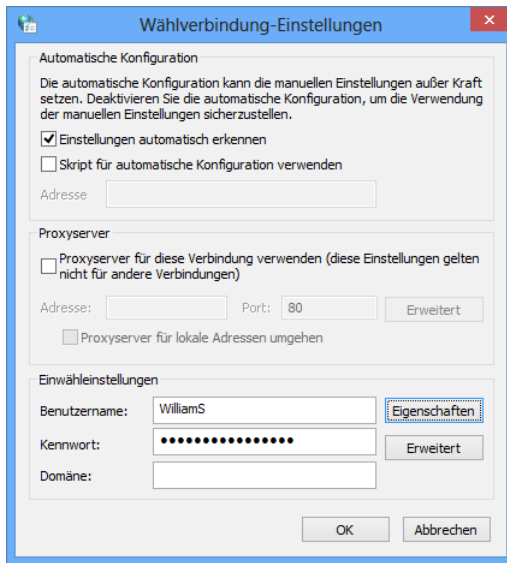


Abbildung 16.9 Proxyeinstellungen können automatisch gesucht oder aus Skripts gelesen werden

4. Soll ein Konfigurationsskript verwendet werden, wählen Sie *Skript für automatische Konfiguration verwenden* und geben dann den Dateipfad oder die URL des Skripts ein. In Dateipfaden können Sie auch Umgebungsvariablen verwenden, wie zum Beispiel in `%UserProfile%\PROXY.VBS`. Wenn Sie eine URL angeben, achten Sie darauf, dass es die Computer-URL ist, wie in `http://proxy.microsoft.com/proxy.vbs`.
5. Um sicherzustellen, dass nur automatische Einstellungen verwendet werden, löschen Sie das Kontrollkästchen *Proxyserver für diese Verbindung verwenden*.
6. Tippen oder klicken Sie zweimal auf OK.

Für eine manuelle Konfiguration der Proxys gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet*. Tippen oder klicken Sie in *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie im Listenfeld *Einstellungen für VPN- und Einwählverbindungen* die Wählverbindung aus, die Sie einstellen möchten, und tippen oder klicken Sie dann auf *Einstellungen*.
3. Löschen Sie die Kontrollkästchen *Einstellungen automatisch erkennen* und *Skript für automatische Konfiguration verwenden*, falls sie gewählt sind.
4. Wählen Sie *Proxyserver für diese Verbindung verwenden*. Das Kontrollkästchen *Proxyserver für lokale Adressen umgehen* wird nicht standardmäßig vorgewählt. In den meisten Fällen werden Sie aber für Abfragen bei Servern aus demselben Netzwerksegment keinen Proxy verwenden. Wählen Sie also auch noch *Proxyserver für lokale Adressen umgehen*. Wenn *Proxyserver für lokale Adressen umgehen* nicht gewählt ist, kann es vorkommen, dass Benutzer für Zugriffe auf Intranetserver, die über Ihre Proxyserver erfolgen, zusätzliche Berechtigungen brauchen.
5. Tippen oder klicken Sie auf *Erweitert*, um das Dialogfeld *Proxyeinstellungen* zu öffnen (Abbildung 16.10).

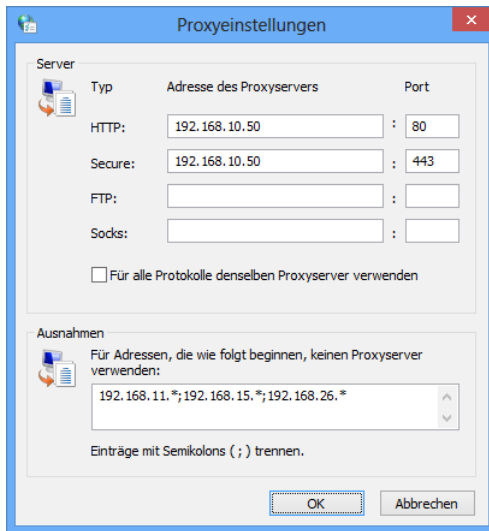


Abbildung 16.10 Sie können für alle Dienste denselben Proxy verwenden oder mehrere Proxys einstellen

6. Geben Sie die IP-Adressen der Proxys in den Textfeldern des Bereichs *Server* ein. Dort gibt es zwei Spalten mit Textfeldern:
 - **Adresse des Proxyservers** Legt die IP-Adresse des Proxyservers oder der Proxyserver fest. Geben Sie für jeden Dienst eine IP-Adresse an. Wenn für einen bestimmten Dienst mehrere Proxys vorgesehen sind, geben Sie die IP-Adressen der einzelnen Proxyserver in der Reihenfolge ein, in der sie vom Webclient kontaktiert werden sollen, wobei die Adressen jeweils durch ein Semikolon voneinander getrennt werden. Soll für einen Dienst kein Proxy vorgesehen sein, geben Sie im entsprechenden Textfeld auch nichts ein.
 - **Port** Legt die Portnummer fest, auf welcher der Proxyserver auf Anfragen antwortet. Die meisten Proxyserver verwenden für alle Anfragen Port 80. Die Standardports sind Port 80 für Hypertext Transfer Protocol (HTTP), Port 443 für Secure Sockets Layer (SSL, aufgelistet als *Secure*), Port 21 für File Transfer Protocol (FTP) und Port 1081 für Socks. Fragen Sie den Webadministrator Ihrer Organisation nach den genauen Einstellungen.
7. Mit dem Kontrollkästchen *Für alle Protokolle denselben Proxyserver verwenden* können Sie für die Dienste HTTP, SSL, FTP und Socks dieselbe IP-Adressen- und Porteinstellung verwenden. Sie haben folgende Optionen:
 - Wenn Ihre Organisation Proxyserver verwendet, die sich um alle Anfragen kümmern, aktivieren Sie das Kontrollkästchen *Für alle Protokolle denselben Proxyserver verwenden* und geben die IP-Adresse ein, die Sie verwenden möchten, sowie die Nummer des Ports, auf dem der Server antwortet.
 - Wenn Sie für jeden Dienst einen oder mehrere separate Proxyserver verwenden möchten, löschen Sie das Kontrollkästchen *Für alle Protokolle denselben Proxyserver verwenden* und geben in den Textfeldern die erforderlichen IP-Adressen und Portnummern ein.
8. Wenn Ihr Netzwerk aus mehreren Segmenten besteht oder wenn es bestimmte Server gibt, für die keine Proxys verwendet werden sollen, geben Sie in der Liste *Ausnahmen* die entsprechenden IP-Adressen ein. Die Einträge werden jeweils durch ein Semikolon voneinander abgetrennt. Das Stern-

chen (*) kann als Platzhalter für einen Adressenbereich von 0 bis 255 dienen, wie zum Beispiel in 192.*.*, 192.168.*.* oder 192.168.10.*.

9. Tippen oder klicken Sie dreimal auf OK.

Einstellen der Verbindungsanmeldungsinformationen

Für jede Verbindung, die Sie erstellen, lassen sich die Anmeldeinformationen separat einstellen. Mit folgenden Schritten können Sie einen Benutzernamen, ein Kennwort und eine Domäne festlegen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann im Fenster *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie in der Liste *Einstellungen für VPN- und Einwählverbindungen* die Verbindung aus, die Sie konfigurieren wollen, und tippen oder klicken Sie auf *Einstellungen*.
3. Geben Sie Benutzername und Kennwort für die Verbindung in die entsprechenden Textfelder ein.
4. Ist ein Domänenname erforderlich, geben Sie ihn im Textfeld *Domäne* ein.
5. Tippen oder klicken Sie zweimal auf OK.

Die Einstellung der Anmeldeinformationen für eine Verbindung ist nicht der letzte Konfigurationsschritt. Sie sollten auch noch festlegen, ob Benutzer zur Eingabe der Anmeldeinformationen oder einer Telefonnummer aufgefordert werden. Ist zur Verbindungsherstellung eine Anmeldedomäne erforderlich, sollten Sie dafür sorgen, dass die Anmeldedomäne zusammen mit den anderen Anmeldeinformationen übermittelt wird. Standardmäßig ist der Domänenname nicht eingeschlossen.

Stellen Sie die zusätzlichen Optionen folgendermaßen ein:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann im Fenster *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie in der Liste *Einstellungen für VPN- und Einwählverbindungen* die Verbindung aus, die Sie konfigurieren wollen, und tippen oder klicken Sie auf *Einstellungen*.
3. Tippen oder klicken Sie im *Einstellungen*-Dialogfeld auf *Eigenschaften*.
4. Tippen oder klicken Sie im Eigenschaftendialogfeld auf die Registerkarte *Optionen*. Nun können Sie die folgenden Optionen einstellen:
 - Sollen während des Verbindungsaufbaus Statusanzeigen erfolgen, wählen Sie *Status während des Wählens anzeigen*.
 - Damit bei Bedarf die Anmeldeinformationen vom Benutzer angefordert werden, wählen Sie *Name, Kennwort, Zertifikat usw. abfragen*.
 - Damit bei Bedarf der Name der Anmeldedomäne zur Verfügung steht, wählen Sie *Windows-Anmeldedomäne einbeziehen*.
 - Soll der Benutzer bei Bedarf eine Telefonnummer eingeben, wählen Sie *Rufnummer abfragen*.
5. Tippen oder klicken Sie dreimal auf OK.

Einstellen der automatischen Verbindungstrennung

Für Wahlverbindungen können Sie einstellen, ob Windows 8 die Leitung trennt, nachdem die Verbindung während des eingestellten Zeitraums nicht benutzt wurde und möglicherweise nicht mehr gebraucht wird. Zur Einstellung der Wahlwiederholungsoptionen gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann im Fenster *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie in der Liste *Einstellungen für VPN- und Einwählverbindungen* die Wahlverbindung aus, die Sie konfigurieren wollen, und tippen oder klicken Sie auf *Einstellungen*.
3. Tippen oder klicken Sie im *Einstellungen*-Dialogfeld auf *Eigenschaften*. Tippen oder klicken Sie auf die Registerkarte *Optionen*. Stellen Sie in der Dropdownliste *Leerlaufzeit, nach der aufgelegt wird* ein, ob Windows 8 eine Verbindung automatisch trennen soll, wenn sie für den angegebenen Zeitraum nicht verwendet wurde. Verfügbare Einstellungen sind *Niemals*, *1 Minute*, *5 Minuten*, *10 Minuten*, *20 Minuten* (die Standardeinstellung), *30 Minuten*, *1 Stunde*, *2 Stunden*, *4 Stunden*, *8 Stunden* und *24 Stunden*.
4. Tippen oder klicken Sie auf *OK*, um zum *Einstellungen*-Dialogfeld zurückzukehren. Tippen oder klicken Sie im Abschnitt *Einwähleinstellungen* auf *Erweitert*. Aktivieren oder deaktivieren Sie das Kontrollkästchen *Verbindung trennen, wenn diese nicht mehr benötigt wird*, um festzulegen, ob Windows 8 die Verbindung trennt, wenn ein Benutzer alle Internetprogramme beendet hat, die andernfalls diese Verbindung benutzen.
5. Tippen oder klicken Sie dreimal auf *OK*.

TIPP

Wenn sich Benutzer darüber beschweren, dass die Verbindungen während der Einwählsitzung getrennt werden, könnte das Problem bei den Trennungseinstellungen liegen. Sprechen Sie mit den Benutzern darüber, wie sie das Internet verwenden. Überlegen Sie dann, ob Sie die Einstellungen so ändern können, dass die Ansprüche der Benutzer besser berücksichtigt werden. Ein weiterer Grund für Trennungen kann darin liegen, wie die Option *Leerlaufzeit, nach der aufgelegt wird* eingestellt ist. Normalerweise ist es allerdings sinnvoll, eine ungenutzte Verbindung nach einiger Zeit zu trennen.

Einstellen der Wählregeln für eine Verbindung

Wahlverbindungen lassen sich mit oder ohne Wählregeln konfigurieren. Wenn Sie keine Wählregeln verwenden, wird immer die Telefonnummer angewählt, die Sie der Verbindung zuweisen. Wenn Sie Wählregeln festlegen, bestimmt der aktuelle Wahlstandort, ob die Verbindung als Orts- oder als Ferngespräch hergestellt wird.

Zur Anzeige und Einstellung der Wählregeln für eine Verbindung gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann im Fenster *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie in der Liste *Einstellungen für VPN- und Einwählverbindungen* die Wahlverbindung aus, die Sie konfigurieren wollen, und tippen oder klicken Sie auf *Einstellungen*.
3. Tippen oder klicken Sie im *Einstellungen*-Dialogfeld auf *Eigenschaften*. Daraufhin öffnet sich ein Eigenschaftendialogfeld.

4. Damit die Verbindung mit den vorgesehenen Regeln erstellt wird, wählen Sie auf der Registerkarte *Allgemein* das Kontrollkästchen *Wählregeln verwenden*, geben dann eine Ortskennzahl ein und wählen ein Land oder eine Region aus.
5. Sollen keine Wählregeln verwendet werden, löschen Sie das Kontrollkästchen *Wählregeln verwenden*.
6. Tippen oder klicken Sie dreimal auf OK.

Einstellen der bevorzugten und der alternativen Rufnummern

Bei Wählverbindungen können Sie zwei Arten von Rufnummern konfigurieren: die Hauptnummer, die für einen Verbindungsversuch angerufen wird, und eine alternative Nummer für den Fall, dass die Verbindungsversuche mit der Hauptnummer fehlschlagen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann im Fenster *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie in der Liste *Einstellungen für VPN- und Einwählverbindungen* die Wählverbindung aus, die Sie konfigurieren wollen, und tippen oder klicken Sie auf *Einstellungen*.
3. Tippen oder klicken Sie im *Einstellungen*-Dialogfeld auf *Eigenschaften*. Daraufhin öffnet sich ein Eigenschaftendialogfeld.
4. Die bevorzugte Telefonnummer wird im Textfeld *Rufnummer* angezeigt. Geben Sie bei Bedarf eine neue Nummer ein.
5. Tippen oder klicken Sie auf *Andere*. Dadurch öffnet sich das Dialogfeld *Alternative Rufnummern*. Nun können Sie die bevorzugte und die alternative Rufnummer folgendermaßen bearbeiten:
 - Wenn Sie eine neue Rufnummer hinzufügen möchten, tippen oder klicken Sie auf *Hinzufügen*. Dadurch wird das Dialogfeld *Alternative Rufnummern hinzufügen* geöffnet. Geben Sie dann im Textfeld *Rufnummer* die alternative Rufnummer so ein, wie man sie lokal wählen würde. Bei Bedarf können Sie einen Bindestrich verwenden, wie beispielsweise in 555-1234. Wenn Sie Wählregeln festlegen möchten, wählen Sie *Wählregeln verwenden*, geben dann eine Ortskennzahl ein und wählen ein Land oder eine Region. Tippen oder klicken Sie auf OK.
 - Wenn Sie die Reihenfolge ändern möchten, in der die Telefonnummern gewählt werden, wählen Sie eine Nummer in der Rufnummernliste und ändern ihre Position in der Liste mit den Pfeilschaltflächen. Die erste Nummer in der Liste wird die bevorzugte Rufnummer.
 - Zur Bearbeitung einer Rufnummer wählen Sie eine Nummer aus der Rufnummernliste aus und tippen oder klicken dann auf *Bearbeiten*. Ändern Sie dann die Einstellung der Nummer im Dialogfeld *Alternative Rufnummer bearbeiten*.
 - Um eine Rufnummer zu löschen, wählen Sie sie in der Rufnummernliste aus und tippen oder klicken dann auf *Löschen*.
6. Wenn die alternativen Rufnummern automatisch verwendet werden sollen, wählen Sie *Nächste Rufnummer versuchen, falls Wählvorgang fehlschlägt*. Sie können auch dafür sorgen, dass Windows 8 eine erfolgreich verwendete Nummer an die Spitze der Liste stellt und zur bevorzugten Nummer macht. Wählen Sie dazu *Rufnummer bei Verbindung in der Liste nach oben verschieben*.
7. Tippen oder klicken Sie viermal auf OK.

Einstellen der Identitätsprüfung

Eine zuverlässige Identitätsprüfung ist wichtig, um ein Netzwerk zu schützen. Wenn sich Benutzer ins Büronetzwerk einwählen, sollte sichergestellt werden, dass sie wirklich die Personen sind, die sie zu sein vorgeben, sofern das überhaupt möglich ist. Die Standardeinstellung für Wählverbindungen sieht allerdings anders aus. Bei den meisten Verbindungen können die Anmeldeinformationen der Benutzer im Klartext übermittelt werden. Wenn Sie verbieten, dass unverschlüsselte Kennwörter übertragen werden, versucht Windows 8, die Anmeldeinformationen mit einem sicheren Verfahren wie MSCHAP Version 2 oder Challenge Handshake Authentication Protocol (CHAP) zu übermitteln, und nicht in Klartext. Sie können Verbindungen auch so einstellen, dass sie das Extensible Authentication Protocol (EAP) verwenden.

Bei Wähl- und Breitbandverbindungen können Sie eine dieser Optionen wählen. VPN ist dagegen nur mit sicheren Methoden möglich. Wenn Sie ein gesichertes Kennwort verlangen, können Sie auch den Windows-Anmeldenamen, das Kennwort und die Domäne automatisch übermitteln, die in der Konfiguration angegeben wurden. Die automatische Übermittlung der Windows-Anmeldeinformationen ist sinnvoll, wenn Benutzer eine Verbindung zum Büro herstellen und in der Windows-Domäne authentifiziert werden müssen. Bei beiden sicheren Validierungsmethoden können Sie die Datenverschlüsselung verlangen und Windows 8 dazu veranlassen, die Verbindung zu trennen, wenn keine Verschlüsselung möglich ist. Die Verschlüsselung erfolgt bei der Windows-Authentifizierung mit gesicherten Kennwörtern oder Smartcards automatisch.

Sie können die Identitätsprüfung folgendermaßen einstellen:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann im Fenster *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.
2. Wählen Sie in der Liste *Einstellungen für VPN- und Einwählverbindungen* die Verbindung aus, die Sie konfigurieren wollen, und tippen oder klicken Sie auf *Einstellungen*.
3. Tippen oder klicken Sie im *Einstellungen*-Dialogfeld auf *Eigenschaften*.
4. Tippen oder klicken Sie im Eigenschaftendialogfeld auf die Registerkarte *Sicherheit*. Bei VPNs können Sie einstellen, welches Verbindungsprotokoll benutzt wird, oder die automatische Erkennung verwenden. Wenn Sie gesicherte Kennwörter verlangen, können Sie auch eine automatische Anmeldung einstellen und eine Datenverschlüsselung verlangen. Beide Optionen sind nützlich, wenn die Anmeldung an einer Windows-Domäne erfolgt. Allerdings müssen die Einstellungen unterstützt werden, sonst können sich Benutzer nicht anmelden und es kommt keine Verbindung zustande.

Wenn Sie Smartcards verwenden, sollten Sie ebenfalls eine Datenverschlüsselung verlangen. Die Datenverschlüsselung ist unverzichtbar, um die Unversehrtheit und Sicherheit der Daten sicherzustellen, die zwischen Sender und Empfänger ausgetauscht werden. Wenn Sie unter *Datenverschlüsselung* den Eintrag *Erforderlich* wählen, die Verbindung aber nicht durch Verschlüsselung gesichert wird, bricht der Clientcomputer die Verbindung ab.

5. Wählen Sie die erlaubten Authentifizierungsprotokolle aus und tippen oder klicken Sie auf *OK*.

Einstellen der Netzwerkprotokolle und -komponenten

Wie Netzwerkprotokolle und -komponenten konfiguriert werden, hängt von der Art der Verbindung ab. Wie aus Tabelle 16.1 hervorgeht, können Wählverbindungen das Point-to-Point Protocol (PPP) oder das Serial Line Internet Protocol (SLIP) als Verbindungsprotokoll verwenden. Breitbandverbindungen verwenden Point-to-Point Protocol over Ethernet (PPPoE). Die meisten VPN-Verbindungen verwenden

PPTP oder L2TP. Neuere VPN-Verbindungen verwenden manchmal Secure Sockets Tunneling Protocol (SSTP) oder IKEv2. Bei IKEv2 können die Verbindungen während der Authentifizierung Computertzertifikate nutzen.

Tabelle 16.1 Verfügbare Verbindungsprotokolle bei unterschiedlichen Verbindungstypen

Verbindungstyp	Verbindungsprotokoll	Beschreibung
Wählverbindung	PPP	Dient zur Herstellung von Verbindungen mit Windows-Servern über Wählverbindungen.
Wählverbindung	SLIP	Dient zur Herstellung von Verbindungen mit UNIX-Servern über Wählverbindungen. Nur verfügbar, wenn Sie entsprechende Software von anderen Herstellern installieren.
Breitbandverbindung	PPPoE	Dient zur Herstellung einer Point-to-Point-Breitbandverbindung über Ethernet.
VPN	Automatisch	Erkennt automatisch, welches VPN-Protokoll verfügbar ist, und richtet mit diesem Protokoll einen virtuellen Tunnel ein.
VPN	PPTP-VPN	Richtet PPTP für ein VPN ein. PPTP ist eine Erweiterung von PPP.
VPN	L2TP-IPSec-VPN	Richtet L2TP für ein VPN ein. L2TP verwendet IPSec zur Verbesserung der Sicherheit.
VPN	IKEv2	Richtet IKE Version 2 für ein VPN ein. IKEv2 nutzt den IPSec-Tunnelmodus, um die Sicherheit zu erhöhen.
VPN	SSTP	Richtet SSTP für ein VPN ein. SSTP überträgt PPP- oder L2TP-Verkehr durch einen SSL-Kanal.
DirectAccess	IPv6 over IPSec	Richtet über eine vorhandene Verbindung einen sicheren Tunnel zu einem Arbeitsplatz ein.

Für mobile Netzwerke werden drei Netzwerkkomponenten verwendet: Transmission Control Protocol/Internet Protocol (TCP/IP), Datei- und Druckerfreigabe für Microsoft-Netzwerke und Client für Microsoft-Netzwerke. Wie aus Tabelle 16.2 hervorgeht, hängt die Konfiguration dieser Komponenten von der Art der Verbindung ab, die ursprünglich erstellt wurde. Sie können diese Einstellungen nach Bedarf ändern. Bei Bedarf können Sie auch weitere Netzwerkkomponenten installieren.

Tabelle 16.2 Standardkomponentenkonfiguration bei unterschiedlichen Verbindungstypen

Wählverbindungs-komponente	Beschreibung	Breit-band	Standard-wählver-bindung	Wählver-bindung ins Büro	VPN
Transmission Control Protocol/Internet Protocol (TCP/IP)	TCP/IPv4 und TCP/IPv6 sind für Netzwerkkommunikation erforderlich. Standardmäßig wird DHCP für Verbindungen verwendet, sofern dies nicht durch entsprechende Einstellungen geändert wird.	Ja	Ja	Ja	Ja
Datei- und Druckerfreigabe für Microsoft-Netzwerke	Ermöglicht die Freigabe von Druckern und Dateien über die Netzwerkverbindung. Ermöglicht die Zuordnung von Druckern und Laufwerken.	Nein	Nein	Nein	Ja
Client für Microsoft-Netzwerke	Ermöglicht Windows-Authentifizierung in Windows-Domänen. Ermöglicht es dem Computer, als Domänenclient zu arbeiten.	Nein	Nein	Ja	Ja

Zur Anzeige und Änderung der Netzwerkoptionen einer Verbindung gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *Netzwerk und Internet* und dann im Fenster *Netzwerk und Internet* auf *Internetoptionen*. Tippen oder klicken Sie im Dialogfeld *Eigenschaften von Internet* auf die Registerkarte *Verbindungen*.

2. Wählen Sie in der Liste *Einstellungen für VPN- und Einwählverbindungen* die Verbindung aus, die Sie konfigurieren wollen, und tippen oder klicken Sie auf *Einstellungen*.
3. Tippen oder klicken Sie im *Einstellungen*-Dialogfeld auf *Eigenschaften*.
4. Tippen oder klicken Sie im Eigenschaftendialogfeld auf die Registerkarte *Netzwerk*. Hier können Sie folgende Einstellungen vornehmen:
 - Aktivieren Sie Netzwerkkomponenten, indem Sie in der Liste *Diese Verbindung verwendet folgende Elemente* die entsprechenden Kontrollkästchen wählen.
 - Deaktivieren Sie Netzwerkkomponenten, indem Sie in der Liste *Diese Verbindung verwendet folgende Elemente* die entsprechenden Kontrollkästchen löschen.

TIPP Falls eine der in Tabelle 16.2 aufgeführten Netzwerkkomponenten nicht verfügbar, aber für eine Verbindung erforderlich ist, können Sie sie installieren. Tippen oder klicken Sie auf der Registerkarte *Netzwerk* auf *Installieren*. Wählen Sie dann den Komponententyp, tippen oder klicken Sie auf *Hinzufügen* und wählen Sie anschließend in der Auswahlliste die gewünschte Komponente aus.

5. Standardmäßig verwenden Verbindungen DHCP zur Konfiguration der Netzwerkeinstellungen, einschließlich der zu verwendenden IP-Adresse, der Subnetzmaske, des Standardgateways, der DNS-Server und der WINS-Server. Wenn Sie eine statische IP-Adresse zuweisen oder andere Einstellungen ändern möchten, wählen Sie *Internetprotokoll Version 4 (TCP/IPv4)* oder *Internetprotokoll Version 6 (TCP/IPv6)* aus und tippen oder klicken dann auf *Eigenschaften*. Dadurch öffnet sich das jeweilige Eigenschaftendialogfeld, das Sie konfigurieren können, wie weiter oben in diesem Kapitel beschrieben.
6. Tippen oder klicken Sie dreimal auf *OK*.

Aktivieren und Deaktivieren der Windows-Firewall für Netzwerkverbindungen

Bei Wahl-, Breitband- und VPN-Verbindungen möchten Sie dem Computer vielleicht einen zusätzlichen Schutz vor Angriffen geben, indem Sie die Windows-Firewall verwenden. Diese integrierte Firewall schützt Windows 8-Computer, indem sie die Informationsarten beschränkt, die ausgetauscht werden können. Durch die Einstellung entsprechender Beschränkungen können Sie die Gefahr verringern, dass jemand in Ihr System einbricht. Und die Beschränkung von Sicherheitsrisiken ist sehr wichtig, wenn Benutzer von außen durch die Firewall und durch Proxyserver hindurch auf das Netzwerk Ihrer Organisation zugreifen.

Standardmäßig ist die Windows-Firewall für alle Verbindungen aktiviert. Sie kann für jeden Netzwerktyp, zu dem der Benutzer eine Verbindung herstellt, einzeln aktiviert oder deaktiviert werden. Um die Windows-Firewall für einzelne Verbindungen zu aktivieren oder zu deaktivieren, gehen Sie so vor:

1. Tippen oder klicken Sie in der Systemsteuerung auf *System und Sicherheit*.
2. Tippen oder klicken Sie auf *Windows-Firewall*. Tippen oder klicken Sie im linken Fensterabschnitt der Seite *Windows-Firewall* auf *Windows-Firewall ein- oder ausschalten*.
3. Auf der Seite *Einstellungen anpassen* sind die Windows-Firewalleinstellungen für jeden Netzwerktyp aufgelistet, zu dem der Benutzer eine Verbindung herstellen kann. Wählen Sie bei jedem Netzwerktyp entweder *Windows-Firewall aktivieren* oder *Windows-Firewall deaktivieren*.
4. Tippen oder klicken Sie auf *OK*, wenn Sie fertig sind.

Herstellen von Verbindungen

Wie im Abschnitt »Einstellen der automatischen oder manuellen Verbindungen« weiter oben in diesem Kapitel beschrieben, können Wahl-, Breitband- und VPN-Verbindungen manuell oder automatisch hergestellt werden. Die manuelle Verbindung lässt den Benutzern die Wahl, wann eine Verbindung hergestellt werden soll. Bei der automatischen Methode wird die Verbindung hergestellt, wenn der Benutzer ein Programm startet, das auf den Netzwerkzugriff angewiesen ist, etwa einen Webbrowser.

Verbinden mit Wahlverbindungen

Wahlverbindungen werden zwischen zwei Modems über eine gewöhnliche Telefonverbindung hergestellt. Zur Herstellung der Verbindung gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Taskleiste auf das Benachrichtigungssymbol des Netzwerks oder streifen Sie vom rechten Bildschirmrand, tippen Sie auf *Einstellungen* und dann auf das Netzwerksymbol.
2. Tippen oder klicken Sie im Bildschirmabschnitt *Netzwerke* auf die Wahlverbindung, die Sie benutzen wollen, und tippen oder klicken Sie dann auf die Schaltfläche *Verbinden*.
3. Überprüfen Sie, ob der angezeigte Benutzername richtig ist. Sofern das Kennwort für dieses Konto vorher eingegeben und gespeichert wurde, können Sie das zwischengespeicherte Kennwort verwenden, ohne es erneut eintippen zu müssen. Geben Sie andernfalls das Kennwort für das Konto ein, wenn es noch nicht zwischengespeichert ist oder Sie es ändern müssen.
4. Falls Sie immer diesen Benutzernamen und das Kennwort verwenden möchten, wenn Sie diese Verbindung benutzen, wählen Sie *Benutzernamen und Kennwort speichern für* und *Nur für eigene Verwendung*.

TIPP

Wenn dieser Benutzername und das Kennwort von jedem Benutzer verwendet werden soll, der die Verbindung herstellen möchte, wählen Sie *Benutzernamen und Kennwort speichern für* und dann *Alle Benutzer dieses Computers*. Verwenden Sie diese Option nicht, wenn Sie planen, die Verbindung durch Gruppenrichtlinien verfügbar zu machen, damit Ihr Kennwort nicht allgemein bekannt wird.

5. Die Dropdownliste *Wählen* zeigt die Nummer an, die gewählt wird. Standardmäßig wird die bevorzugte Nummer verwendet. Wenn Sie eine andere Nummer verwenden möchten, tippen oder klicken Sie auf die Schaltfläche der Dropdownliste und wählen dann die gewünschte Nummer aus.
6. Tippen oder klicken Sie auf *Wählen*. Wenn das Modem eine Verbindung mit dem ISP oder dem Büronetzwerk herstellen kann, wird eine Übertragungsgeschwindigkeit angezeigt. Diese Geschwindigkeit wird bei jedem Anruf neu ausgehandelt und hängt von der Leistungsfähigkeit der beteiligten Modems, vom verfügbaren Komprimierungsalgorithmus und von der Qualität der Verbindung ab.

Sie können sich die Verbindungseigenschaften ansehen, indem Sie im Bildschirmabschnitt *Netzwerke* die Wahlverbindung gedrückt halten oder mit der rechten Maustaste anklicken und *Verbindungseigenschaften anzeigen* wählen. Wenn Sie Probleme haben, Wahlverbindungen herzustellen, helfen Ihnen vielleicht folgende Hinweise weiter:

- **Problem:** Das Modem wählt und erreicht das andere Modem, kann aber keine Verbindung herstellen. Es macht Geräusche, bis Sie den Vorgang abbrechen.

Lösung: Gewöhnlich sind schlechte Leitungen die Ursache des Problems. Störgeräusche auf der Leitung können eine Verbindung verhindern. Überprüfen Sie die Verbindungen zwischen dem Modem

und der Telefonsteckdose. Fragen Sie bei der Telefongesellschaft nach, ob die Leitung getestet und das Problem behoben werden kann.

- **Problem:** Das Modem wählt und scheint eine Verbindung herzustellen, aber dann wird die Verbindung zum ISP oder zum Büronetzwerk unerwartet unterbrochen. Es hat den Anschein, als sei die Verbindung gar nicht erst vollständig zustande gekommen.

Lösung: Überprüfen Sie Ihre Netzwerkprotokolle und Komponenten, wie im Abschnitt »Einstellen der Netzwerkprotokolle und -komponenten« weiter oben in diesem Kapitel beschrieben. Wenn dort alles in Ordnung ist, überprüfen Sie, ob sie Windows-Anmeldeinformationen und die Domäne übermitteln, denn das könnte erforderlich sein, wie im Abschnitt »Einstellen der Verbindungsanmeldungsinformationen« weiter oben in diesem Kapitel beschrieben.

- **Problem:** Der Benutzer erhält keinen Zugang zu den Ressourcen der Windows-Domäne.

Lösung: Vielleicht ist der Client für Microsoft-Netzwerke für den Zugriff auf das Büronetzwerk erforderlich. Aktivieren Sie diese Komponente und sorgen Sie dafür, dass bei Bedarf die Domäne angegeben wird.

- **Problem:** Der Benutzer kommt nicht durch. Das Modem scheint die Nummer falsch zu wählen. Sie können hören, dass es zu viel oder zu wenig Ziffern wählt.

Lösung: Überprüfen Sie die Wählregeln für die Verbindung und den aktuell gewählten Wählstandort. Sorgen Sie dafür, dass die Einstellungen für den aktuellen Standort des Benutzers stimmen.

- **Problem:** Das Modem zeigt an, dass es kein Freizeichen erhält, aber es scheint korrekt installiert und in Ordnung zu sein.

Lösung: Überprüfen Sie das Verbindungskabel zwischen Modem und Telefonsteckdose und sorgen Sie dafür, dass die Stecker richtig sitzen. Manche Modems haben zwei Anschlüsse, einen mit der Beschriftung Phone/In und einen mit der Beschriftung Line/Out. Das Modemkabel von der Telefonsteckdose sollte mit dem Anschluss Line/Out verbunden werden. Manche Modemanschlüsse sind nur für Daten oder spezielle Leitungsarten vorgesehen, nicht für gewöhnliche Telefon- oder Modemverbindungen. Probieren Sie einen anderen Anschluss.

- **Problem:** Der Computer hängt, sobald der Benutzer das Modem verwendet.

Lösung: Das liegt höchstwahrscheinlich an einem Gerätekonflikt. Orientieren Sie sich bei der Konfigurierung und Fehlerbehebung an den Beschreibungen aus Kapitel 9, »Verwalten von Hardwaregeräten und Treibern«.

- **Problem:** Manche Dienste hängen oder arbeiten nicht richtig.

Lösung: Überprüfen Sie die Proxy- und Firewallinstellungen. Diese Einstellungen können die verfügbaren Dienste einschränken.

Verbinden mit Breitbandverbindungen

Breitbandverbindungen werden mit einem Kabelmodem und einer speziellen Leitung eingerichtet oder mit einem DSL-Router und einer Telefonleitung. Um eine Breitbandverbindung herzustellen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Taskleiste auf das Benachrichtigungssymbol des Netzwerks oder streifen Sie vom rechten Bildschirmrand, tippen Sie auf *Einstellungen* und dann auf das Netzwerksymbol.
2. Tippen oder klicken Sie im Bildschirmabschnitt *Netzwerke* auf die Breitbandverbindung, die Sie benutzen wollen, und tippen oder klicken Sie dann auf die Schaltfläche *Verbinden*.

3. Sofern Benutzername und Kennwort für die Verbindung vorher noch nicht eingegeben wurden, müssen Sie den Benutzernamen und das Kennwort eintippen, wenn Sie dazu aufgefordert werden. Tippen oder klicken Sie anschließend auf *OK*.

Sie können sich die Verbindungseigenschaften ansehen, indem Sie im Bildschirmabschnitt *Netzwerke* die Breitbandverbindung gedrückt halten oder mit der rechten Maustaste anklicken und *Verbindungseigenschaften anzeigen* wählen.

Windows 8 speichert die Anmeldeinformationen für Breitbandverbindungen und verwendet sie künftig jedes Mal, wenn Sie eine Verbindung aufbauen. Sie können die zwischengespeicherten Anmeldeinformationen löschen, um neue Anmeldeinformationen einzugeben. Klicken Sie dazu im Bildschirmabschnitt *Netzwerke* mit der rechten Maustaste auf die Breitbandverbindung oder halten Sie sie gedrückt, und wählen Sie *Zwischengespeicherte Anmeldeinformationen löschen*.

Wenn Sie Probleme haben, Breitbandverbindungen herzustellen, helfen Ihnen vielleicht folgende Hinweise weiter:

- **Problem:** Es lässt sich keine Verbindung herstellen. Die Verbindung scheint gar nicht zu funktionieren.
Lösung: Überprüfen Sie die Netzwerkverbindungen. Sorgen Sie dafür, dass die Verbindungskabel zwischen dem Computer und dem DSL-Router oder Kabelmodem korrekt eingesteckt sind.
- **Problem:** Die Verbindung wird unerwartet unterbrochen. Es hat den Anschein, als sei die Verbindung gar nicht erst vollständig zustande gekommen.
Lösung: Überprüfen Sie Ihre Netzwerkprotokolle und Komponenten, wie im Abschnitt »Einstellen der Netzwerkprotokolle und -komponenten« weiter oben in diesem Kapitel beschrieben. Wenn dort alles in Ordnung ist, überprüfen Sie, ob sie Windows-Anmeldeinformationen und die Domäne übermitteln, denn das könnte erforderlich sein, wie im Abschnitt »Einstellen der Verbindungsanmeldungsinformationen« weiter oben in diesem Kapitel beschrieben.
- **Problem:** Manche Dienste hängen oder arbeiten nicht richtig.
Lösung: Überprüfen Sie die Proxy- und Firewall-Einstellungen. Diese Einstellungen können die verfügbaren Dienste einschränken.
- **Problem:** Sie erhalten keinen Zugang zu den Ressourcen der Windows-Domäne.
Lösung: Vielleicht ist der Client für Microsoft-Netzwerke für den Zugriff auf das Büronetzwerk erforderlich. Aktivieren Sie diese Komponente und sorgen Sie dafür, dass bei Bedarf die Domäne angegeben wird.

Verbinden mit VPN

Eine VPN-Verbindung wird über eine bestehende Netzwerk-, Wähl- oder Breitbandverbindung hergestellt. VPN-Verbindungen werden als eigenständige Verbindungen neben Wähl-, Breitband- oder LAN-Verbindungen angezeigt. Um eine VPN-Verbindung herzustellen, gehen Sie folgendermaßen vor:

1. Tippen oder klicken Sie in der Taskleiste auf das Benachrichtigungssymbol des Netzwerks oder streifen Sie vom rechten Bildschirmrand, tippen Sie auf *Einstellungen* und dann auf das Netzwerksymbol.
2. Tippen oder klicken Sie im Bildschirmabschnitt *Netzwerke* auf die VPN-Verbindung, die Sie benutzen wollen, und tippen oder klicken Sie dann auf die Schaltfläche *Verbinden*.
3. Wenn die Verbindung so konfiguriert ist, dass zuerst die Trägerverbindung hergestellt wird, versucht Windows 8, diese Verbindung herzustellen, bevor es die VPN-Verbindung herstellt. Wenn Sie dazu aufgefordert werden, die Herstellung dieser Verbindung zu bestätigen, tippen oder klicken Sie auf *Ja*.

Stellen Sie dann die Trägerverbindung her, wie im Abschnitt »Verbinden mit Wählverbindungen« weiter oben in diesem Kapitel beschrieben.

4. Sobald die Trägerverbindung besteht, sehen Sie ein *Verbindung*-Dialogfeld. Nachdem Sie den angezeigten Benutzernamen überprüft und das Kennwort für das Netzwerkkonto eingegeben haben, sofern es noch nicht angezeigt wird, tippen oder klicken Sie auf *Verbinden*.

Sie können sich die Verbindungseigenschaften ansehen, indem Sie im Bildschirmabschnitt *Netzwerke* die VPN-Verbindung gedrückt halten oder mit der rechten Maustaste anklicken und *Verbindungseigenschaften anzeigen* wählen. Wenn Sie Probleme haben, Verbindungen herzustellen, helfen Ihnen vielleicht folgende Hinweise weiter:

- **Problem:** Es lässt sich keine Verbindung herstellen. Es scheint gar nichts zu funktionieren.

Lösung: Überprüfen Sie die Netzwerkverbindungen. Sorgen Sie dafür, dass die Verbindungskabel zwischen dem Computer und dem DSL-Router oder Kabelmodem richtig eingesteckt sind. Stellen Sie bei einer Wählverbindung sicher, dass das Telefonkabel an das Modem angeschlossen ist.

- **Problem:** Es wird eine Fehlermeldung angezeigt, die den Hostnamen betrifft.

Lösung: Der Hostname wurde vielleicht falsch angegeben. Überprüfen Sie, ob der Hostname in den Einstellungen vollständig angegeben wurde, zum Beispiel als *external01.microsoft.com* und nicht einfach nur als *external01*. Vielleicht funktioniert auch die DNS-Namensauflösung nicht richtig. Wenn das der Fall ist, geben Sie die IP-Adresse des Hosts statt seines Namens ein.

- **Problem:** Es wird eine Fehlermeldung angezeigt, in der von einer ungültigen IP-Adresse die Rede ist.

Lösung: Überprüfen Sie die IP-Adresse oder geben Sie die Adresse neu ein. War die IP-Adresse korrekt, ist das TCP/IP-Netzwerk vielleicht falsch konfiguriert. Überprüfen Sie Ihre Netzwerkprotokolle und -komponenten, wie im Abschnitt »Einstellen der Netzwerkprotokolle und -komponenten« weiter oben in diesem Kapitel beschrieben. Vielleicht müssen Sie ein Standardgateway und eine statische IP-Adresse für die Verbindung festlegen.

- **Problem:** Es wird eine Meldung angezeigt, in der es heißt, das Protokoll werde nicht unterstützt, und die Verbindung kommt nicht zustande.

Lösung: Stellen Sie das Protokoll auf automatisch, statt es explizit auf PPTP, L2TP, SSTP oder IKEv2 einzustellen. Prüfen Sie die Einstellungen für die sichere Anmeldung. Vielleicht ist die Einstellung so erfolgt, dass ein Kennwort statt einer Smartcard erforderlich ist, oder umgekehrt. Wenn die Einstellungen in Ordnung sind, überprüfen Sie, ob sie Windows-Anmeldeinformationen und die Domäne übermitteln, denn das könnte erforderlich sein, wie im Abschnitt »Einstellen der Verbindungsanmeldungsinformationen« weiter oben in diesem Kapitel beschrieben.

- **Problem:** Es lassen sich keine Netzlaufwerke zuordnen und keine Drucker verwenden.

Lösung: Für die Zuordnung von Netzlaufwerken und die Verwendung von freigegebenen Druckern ist die Datei- und Druckerfreigabe für Microsoft-Netzwerke erforderlich. Aktivieren Sie diese Komponente, wie im Abschnitt »Einstellen der Netzwerkprotokolle und -komponenten« dieses Kapitels beschrieben.

- **Problem:** Manche Dienste hängen oder arbeiten nicht richtig.

Lösung: Überprüfen Sie die Proxy- und Firewall-Einstellungen. Diese Einstellungen können die verfügbaren Dienste einschränken.

Drahtlosnetzwerke

Damit Benutzer ihre mobilen Geräte leichter zu Meetings und in andere Räumlichkeiten des Bürogebäudes mitnehmen und ans Netzwerk anschließen können, installieren viele Organisationen Drahtlosnetzwerke. Drahtlosnetzwerke (oder Funknetzwerke) können in verschiedenen Konfigurationen aufgebaut und verwendet werden. Dieser Abschnitt beschreibt die gebräuchlichsten Konfigurationen.

Drahtlosgeräte und Drahtlostechnologien

Wenn Sie mit Drahtlosnetzwerken arbeiten, sind *Drahtlosnetzwerkadapter* und *Drahtloszugriffspunkt* die häufigsten Begriffe, mit denen Sie es zu tun haben. Drahtlosnetzwerkadapter gibt es beispielsweise als PCI-Karten (Peripheral Component Interconnect) für Desktopgeräte und als USB-Geräte für mobile Computer oder Desktops. Die meisten modernen Mobilgeräte haben aber bereits einen Drahtlosadapter eingebaut. Ein Drahtlosadapter kommuniziert mithilfe einer integrierten Sende- und Empfangsvorrichtung und einer kleinen Antenne mit einem Zugriffspunkt (access point). Im Normalfall ist ein Zugriffspunkt direkt mit dem herkömmlichen Netzwerk der Organisation verbunden und kann auch selbst als Netzwerkhub oder -switch dienen. Das bedeutet, dass er über Buchsen verfügt, die Kabelverbindungen ermöglichen, und dass er natürlich Drahtlosverbindungen herstellen kann. Für Zugriffspunkte gibt es auch noch andere Bezeichnungen, beispielsweise *Basisstationen* oder *drahtlose Gateways*.

Die gebräuchlichsten Drahtlosadapter und Zugriffspunkte basieren auf der IEEE-Spezifikation 802.11. Drahtlosgeräte, die auf dieser Spezifikation basieren, können WiFi-zertifiziert sein, um zu beweisen, dass ihre Leistung und Kompatibilität sorgfältig überprüft wurde. Tabelle 16.3 bietet einen Funktionsvergleich der gebräuchlichsten Drahtlostechnologien, die auf IEEE 802.11 basieren. Die Tabelle beschreibt vier Standards. Jeder hat seine Vor- und Nachteile. An dieser Stelle sei darauf hingewiesen, dass Drahtlosgeräte nach 802.11a zwar nicht mit Geräten nach 802.11b oder 802.11g kommunizieren können, aber derzeit verwenden nur wenige Geräte den 5-Gigahertz-Bereich. Daher ist die Wahrscheinlichkeit für Störungen durch andere Drahtlosgeräte, die hauptsächlich im 2,4-GHz-Bereich arbeiten, geringer.

Tabelle 16.3 Technologien für Drahtlosnetzwerke

Drahtlosstandard	802.11a	802.11b	802.11g	802.11n
Geschwindigkeit	Bis zu 54 MBit/s	Bis zu 11 MBit/s	Bis zu 54 MBit/s	Bis zu 540 MBit/s
Sendefrequenz	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz, 5 GHz oder beide
Effektive Reichweite in Gebäuden	Ungefähr 7 bis 22 Meter	Ungefähr 30 bis 45 Meter	Ungefähr 30 bis 45 Meter	Ungefähr 60 bis 90 Meter
Kompatibilität	Nicht kompatibel zu 802.11b und 802.11g	Drahtlosgeräte nach 802.11b können mit 11 MBit/s mit Drahtlosgeräten nach 802.11g kommunizieren. Drahtlosgeräte nach 802.11g können mit 11 MBit/s mit Zugriffspunkten nach 802.11b kommunizieren.	Drahtlosgeräte nach 802.11g können mit 11 MBit/s mit Drahtlosgeräten nach 802.11b kommunizieren.	Drahtlosgeräte nach 802.11n können mit 11 MBit/s mit Drahtlosgeräten nach 802.11b und mit 54 MBit/s mit Drahtlosgeräten nach 802.11g kommunizieren.

Zu den neueren Übertragungsspezifikationen in 802.11 gehört 802.11n. 802.11n bietet eine Geschwindigkeit von bis zu 540 MBit/s und kann mit 802.11b- und 802.11g-Geräten kommunizieren. Um eine hohe Übertragungsgeschwindigkeit zu erreichen, kann 802.11n mehrere Empfänger und mehrere Sender nutzen. Jeder Sender kann wiederum einen oder mehrere Datenstreams übertragen. Je mehr solcher

Streams ein Gerät auf alle Sender und Empfänger verteilt, desto höher wird der Durchsatz. Viele Geräte nach dem Standard 802.11n, die mehrere Sender und Empfänger eingebaut haben, fassen allerdings schwache und reflektierte Signale in einem Datenstream zusammen, um die Reichweite zu erhöhen.

Zur Verbesserung der Sicherheit hat das IEEE den Standard 802.11i definiert. Im Gegensatz zu den Standards 802.11a, 802.11b, 802.11g und 802.11n beschäftigt sich der Standard 802.11i aber nicht mit Übertragungsgeschwindigkeiten und Sendefrequenzen. 802.11i ist ein Sicherheitsstandard, durch den die vorhandenen Standards ergänzt werden. Genauer gesagt, er beschreibt zusätzliche Sicherheitsfunktionen für die Funkspezifikationen von 802.11a, 802.11b, 802.11g und 802.11n. Das bedeutet, dass Netzwerkadapter und Zugriffspunkte nach 802.11a die Sicherheitsfunktionen von 802.11i übernehmen können, wie auch die Drahtlosprodukte nach 802.11b, 802.11g und 802.11n.

HINWEIS

Beachten Sie bitte, dass manche Computer, insbesondere mobile Geräte, bereits integrierte Chipsätze enthalten, die mehrere Drahtlostechnologien unterstützen. Wi-Fi Protected Access Version 2 (WPA2) ist die von der Wi-Fi Alliance zertifizierte Implementierung von 802.11i. WPA2 bietet alle Elemente, die der Standard 802.11i verlangt.

PRAXISTIPP

Beschäftigen Sie sich mit den Kompatibilitätsproblemen, die sich ergeben können, bevor Sie Geräte einsetzen, die nicht auf IEEE 802.11 basieren. Es gibt immer mehr Geräte im Handel, die sehr hohe Übertragungsgeschwindigkeiten erreichen. Einige dieser Geräte erreichen die höhere Geschwindigkeit durch Komprimierung und ähnliche Methoden, wobei sie sich im Rahmen der IEEE 802.11-Spezifikation bewegen. Andere verwenden vielleicht Spezialentwicklungen des Herstellers. Das kann bedeuten, dass Sie die Drahtlosadapter und Zugriffspunkte dieses Herstellers verwenden müssen, um die höhere Übertragungsleistung zu erreichen. Weitere Informationen über Drahtlosstandards und zertifizierte Geräte finden Sie unter <http://www.wi-fi.org>.

Sicherheit im Drahtlosnetzwerk

Die Absicherung eines Drahtlosnetzwerks unterscheidet sich wesentlich von der Absicherung eines herkömmlichen Netzwerks. Bei einem herkömmlichen Netzwerk erfolgt die Verbindung des Computers mit dem Netzwerk über ein spezielles Netzkabel. Ein Benutzer muss ein Kabel verwenden, um seinen Computer elektrisch mit dem Netzwerk zu verbinden, und er braucht dafür Zugang zu einem der internen Switches oder Hubs. Schließt ein Unbefugter seinen Computer ans Netzwerk an, ist das ziemlich leicht zu erkennen. Folgt man dem Kabel, gelangt man irgendwann zum Computer des Eindringlings.

Wenn Sie dagegen ein Drahtlosnetzwerk installieren, hat im Prinzip jeder, der sich in Reichweite eines Ihrer Zugriffspunkte aufhält, Zugriff auf Ihr Netzwerk. Dann kann er nicht nur die ausgesendeten Signale empfangen, sondern auch versuchen, ins Netzwerk einzubrechen. Die schlechte Nachricht lautet, dass es schwierig ist, den Eindringling zu lokalisieren, weil es keinen Draht gibt, dem man nur zu folgen braucht. Und die richtig schlechte Nachricht lautet, dass ein Benutzer gewöhnlich bereits hinter der Firewall Ihrer Organisation ist, wenn es ihm gelingt, über einen Drahtloszugriffspunkt Zugang zum Netzwerk zu erhalten. Um das Netzwerk zu schützen, sollten Sie seine Firewall konfigurieren, sofern eine verfügbar ist, und die Drahtlosgeräte so einrichten, dass alle Übertragungen verschlüsselt werden.

Die simpelste Verschlüsselungsmethode für Drahtlosgeräte ist Wireless Equivalency Protection (WEP). Wenn Sie WEP verwenden, werden die Daten mit einem geheimen Schlüssel verschlüsselt, der 40, 128 oder 152 Bit lang oder länger sein kann. Alle Daten werden vor der Übertragung mit einem symmetrischen Schlüssel verschlüsselt, der vom WEP-Schlüssel oder Kennwort abgeleitet wird. Jeder Computer, der die Daten lesen will, muss in der Lage sein, sie mit diesem Schlüssel zu entschlüsseln. In einem typischen herkömmlichen Netzwerk ist die Verschlüsselung mit einem gemeinsamen geheimen Schlüssel schon ausreichend, um die Daten zu schützen. In einem Drahtlosnetzwerk mit hohem Übertragungsauf-

kommen ist es möglich, dass jemand den gemeinsamen Schlüssel knackt. Und weil sich der Schlüssel gewöhnlich über längere Zeit nicht ändert, kann sich der Eindringling dann Zugriff auf das interne Netzwerk Ihrer Organisation verschaffen.

Da WEP nur eine sehr simple Absicherung bieten kann, wird dringend von seiner Verwendung abgeraten, es sei denn, es gibt keine Alternative. Die bevorzugten Alternativen zu WEP sind Wi-Fi Protected Access (WPA) und WPA2. WPA wurde von der Wi-Fi Alliance als Interimsstandard übernommen, bevor der Standard 802.11i in Kraft trat. WPA2 beruht auf dem offiziellen 802.11i-Standard und ist vollständig abwärtskompatibel zu WPA.

WPA und WPA2 sind in der Lage, Schlüssel zu wechseln, um die Sicherheit zu erhöhen, und die Art zu ändern, wie Schlüssel abgeleitet werden. Durch den Wechsel der Verschlüsselungsschlüssel nach einer gewissen Zeit und dadurch, dass sie nicht immer in derselben Weise abgeleitet werden, bieten WPA und WPA2 gegenüber WEP eine wesentlich höhere Sicherheit. WPA- und WPA2-kompatible Geräte können in einem Enterprise-Modus oder in einem Personal-Modus (für kleine Firmen und Privatanwender) betrieben werden:

- **Der Enterprise-Modus bietet die Authentifizierung mit IEEE 802.1X und EAP** Im Enterprise-Modus verwenden die Drahtlosgeräte zwei Schlüsselsätze: Sitzungsschlüssel und Gruppenschlüssel. Sitzungsschlüssel sind für jede Zuordnung zwischen einem Zugriffspunkt und einem Drahtlosclient eindeutig. Sie dienen dazu, eine virtuelle private Verbindung zwischen Zugriffspunkt und Client herzustellen. Gruppenschlüssel werden von allen Clients benutzt, die mit demselben Zugriffspunkt verbunden sind. Beide Schlüsselsätze werden dynamisch erzeugt und rotieren, um die Integrität der Schlüssel auch über längere Zeiträume hinweg zu schützen.
- **Der Personal-Modus bietet die Authentifizierung mit einem vordefinierten Schlüssel oder Kennwort** In einer Konfiguration für kleine Büros oder Privatanwender arbeitet WPA mit einem vordefinierten Verschlüsselungsschlüssel, statt den Verschlüsselungsschlüssel zu übertragen. Bei dieser Konfiguration gibt der Benutzer beim Zugriffspunkt einen Hauptschlüssel ein (den Gruppenschlüssel) und richtet dann alle anderen Drahtlosgeräte so ein, dass sie diesen Hauptschlüssel verwenden. Ein Drahtlosgerät verwendet den Hauptschlüssel als Ausgangspunkt, um nach mathematischen Verfahren einen Sitzungsschlüssel zu berechnen. Diesen Sitzungsschlüssel ändert es in gewissen Abständen, sodass derselbe Sitzungsschlüssel nie zweimal verwendet wird. Die Schlüsselrotation erfolgt automatisch und wird im Hintergrund durchgeführt.

WPA und WPA2 sind vollständig kompatibel zu 802.11a, 802.11b, 802.11g und 802.11n. Viele Drahtlosgeräte, die verkauft wurden, bevor es WPA und WPA2 gab, können durch ein Softwareupgrade kompatibel zu WPA und WPA2 gemacht werden. Was WPA betrifft, sind gewöhnlich keine weiteren Modifikationen erforderlich. Für WPA2 gilt das nicht, denn manches Drahtlosgerät braucht vielleicht einen anderen Prozessor oder ein anderes Hardwareupgrade, um die rechenintensive AES-Verschlüsselung (Advanced Encryption Standard) durchführen zu können.

Beachten Sie bei der Arbeit mit WPA und WPA2 bitte Folgendes:

- Alle Produkte mit Wi-Fi-Zertifikat für WPA2 können mit Produkten zusammenarbeiten, die über ein Wi-Fi-Zertifikat für WPA verfügen.
- In WPA und WPA2 gibt es die Betriebsmodi Enterprise und Personal.
- WPA und WPA2 verwenden zur Authentifizierung 802.1X und EAP.
- WPA bietet eine starke Datenverschlüsselung nach dem Temporal Key Integrity Protocol (TKIP).
- WPA2 bietet eine erweiterte Datenverschlüsselung mit AES. Dadurch kann WPA2 den Federal Information Processing Standard (FIPS) 140-2 einiger Behörden erfüllen.

HINWEIS

WPA und WPA2 bieten beide eine hohe Sicherheit, um dafür zu sorgen, dass private Daten privat bleiben und nur autorisierte Benutzer Zugang zu einem Drahtlosnetzwerk erhalten. Nur WPA2 bietet eine starke Verschlüsselung durch AES, wie es von einigen Firmen und Behörden verlangt wird.

Robust Security Network (RSN) ist eine weitere Sicherheitstechnologie, die von 802.11i-kompatiblen Geräten unterstützt wird. RSN ermöglicht es den Drahtlosgeräten, ihre Authentifizierungs- und Verschlüsselungsalgorithmen dynamisch zu vereinbaren. Das bedeutet, dass sich die Authentifizierungs- und Verschlüsselungsalgorithmen, die von RSN-kompatiblen Geräten verwendet werden, ändern können. Neue Authentifizierungsmethoden und -algorithmen können hinzugefügt werden, um Sicherheitsproblemen zu begegnen. RSN basiert auf EAP und AES.

Installieren und Konfigurieren eines Drahtlosadapters

Neben mobilen Geräten mit eingebauten Drahtlosadaptern sind die beiden wichtigsten Arten von Drahtlosadaptern, die Sie verwenden werden, PC Card-Geräte für Notebooks und PCI-Karten für Desktops. Diese Adapter sind am einfachsten zu konfigurieren und nach meiner Erfahrung auch am zuverlässigsten. Außerdem sind Geräte üblich, die über USB mit einem Notebook oder Desktopcomputer verbunden werden. Wenn Sie USB-Drahtlosgeräte verwenden, denken Sie bitte daran, dass es mehrere USB-Spezifikationen gibt, darunter USB 2.0 und den Nachfolger, das schnellere USB 3.0. Ein Drahtlosgerät, das USB 3.0-konform ist, muss an einen USB 3.0-Anschluss angeschlossen werden, um richtig zu funktionieren und die Geschwindigkeit zu bieten, die Sie erwarten.

Im Rahmen der Installation bietet der größte Teil der Installationssoftware seine Unterstützung bei der Einstellung des Drahtlosgeräts an. Dabei müssen Sie gewöhnlich den Namen des Drahtlosnetzwerks angeben, mit dem Sie eine Verbindung herstellen möchten, und den Modus, in dem das Gerät betrieben werden soll. Drahtlosadapter haben zwei Betriebsarten:

- **Ad-Hoc** Im Ad-Hoc-Modus stellen Sie den Drahtlosadapter so ein, dass er eine direkte Verbindung zu anderen Computern aufnehmen kann, die mit kompatiblen Drahtlosadaptern ausgerüstet sind.
- **Infrastruktur** Im Infrastrukturmodus konfigurieren Sie den Drahtlosadapter für den Einsatz in einem Drahtlosnetzwerk. Bei dieser Konfiguration ist der Adapter darauf vorbereitet, eine Verbindung mit einem Zugriffspunkt herzustellen, also keine Direktverbindung mit anderen Computern.

Nach der Einstellung des Betriebsmodus müssen Sie vielleicht den Verschlüsselungsschlüssel eingeben, der verwendet werden soll. Wenn Ihre Organisation WEP verwendet, müssen Sie gewöhnlich den erforderlichen Verschlüsselungsschlüssel eingeben. Meistens wird dieser Schlüssel als Netzwerkschlüssel bezeichnet. Bei WPA/WPA2 werden Sie den erforderlichen Verschlüsselungsschlüssel höchstwahrscheinlich in Form eines Zertifikats oder einer Smartcard angeben.

Verwenden von Drahtlosnetzwerken und Drahtlosverbindungen

Sobald die Installation des Geräts abgeschlossen ist, müssten Sie eine Verbindung über das Drahtlosnetzwerk herstellen können. Wie bei herkömmlichen Netzwerkkarten mit ihren Ethernetverbindungen gibt es für Drahtlosnetzwerkadapter eine WiFi-Verbindung, die für die Verbindung mit einem bestimmten Netzwerk zuständig ist, das als öffentliches, privates oder Domänennetzwerk ausgewiesen ist. Wenn ein Computer mit einer herkömmlichen und einer Drahtlosverbindung ausgerüstet ist, kann er zwei aktive Verbindungen haben: eine mit einem herkömmlichen Netzwerk und eine mit einem Drahtlosnetzwerk.

Bei WiFi-Verbindungen werden folgende zusätzliche Details über das Netzwerk und die Verbindung angezeigt:

- Der Name des Drahtlosnetzwerks (in Klammern nach der Verbindungstypangabe)
- Die aktuelle Signalstärke. Wird die Signalstärke mit nur einem Strich dargestellt, ist sie schlecht. Erfolgt die Darstellung mit fünf Strichen, ist die Signalstärke ausgezeichnet.
- Ein Link zum Trennen der Drahtlosverbindung

So zeigen Sie die Einstellungen für eine Drahtlosverbindung an:

1. Tippen oder klicken Sie in der Systemsteuerung unter *Netzwerk und Internet* auf *Netzwerkstatus und -aufgaben anzeigen*.
2. Tippen oder klicken Sie im linken Fensterabschnitt des Netzwerk- und Freigabecenters auf *Adapter-einstellungen ändern*.
3. Das Fenster *Netzwerkverbindungen* zeigt eine Liste aller Netzwerkverbindungen an, die auf dem Computer konfiguriert sind. Klicken Sie mit der rechten Maustaste auf die Drahtlosverbindung, die Sie verwenden wollen, oder halten Sie sie gedrückt, und wählen Sie den Befehl *Status*.
4. Es erscheint ein Dialogfeld wie in Abbildung 16.11. Sie können im Dialogfeld *Status von WiFi* den Status der Verbindung überprüfen und die Verbindung in ähnlicher Weise einstellen wie bei anderen Verbindungstypen. Außerdem wird angezeigt, welche Übertragungsrate die Verbindung bietet und wie lange sie bereits besteht.

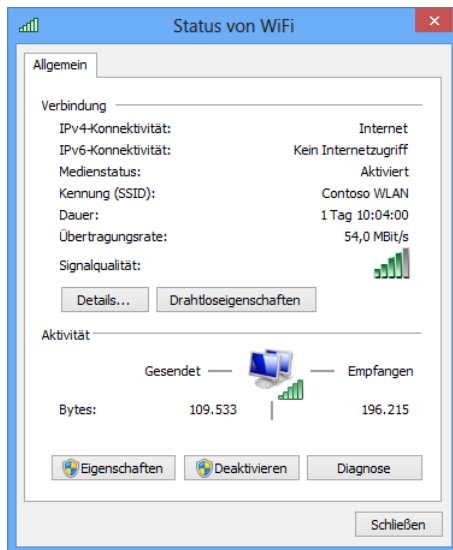


Abbildung 16.11 Überprüfen Sie in diesem Dialogfeld den Status und die Signalstärke einer Drahtlosnetzwerkverbindung

Wie Ethernetverbindungen verfügen auch WiFi-Verbindungen über einstellbare Eigenschaften. Die Beschreibung der Konfiguration von Netzwerkverbindungen gilt weitgehend auch für WiFi-Verbindungen. Sie können Folgendes tun:

- Netzwerkfunktionen für Clients, Dienste und Protokolle installieren oder entfernen. Tippen oder klicken Sie im Dialogfeld *Status von WiFi* auf *Eigenschaften* und dann nach Bedarf auf *Installieren* oder *Deinstallieren*.
- TCP/IPv6- und TCP/IPv4-Einstellungen für DHCP, statische IP-Adressen und dynamische IP-Adressierung durchführen. Tippen oder klicken Sie im Dialogfeld *Status von WiFi* auf *Eigenschaften* und dann doppelt auf *Internetprotokoll Version 6 (TCP/IPv6)* oder *Internetprotokoll Version 4 (TCP/IPv4)*.
- Drahtlosverbindungen deaktivieren oder überprüfen. Tippen oder klicken Sie im Dialogfeld *Status von WiFi* nach Bedarf auf *Deaktivieren* oder *Diagnose*.

Wenn sich bei der Erstellung von Drahtlosverbindungen Probleme ergeben und die automatische Diagnose die Probleme nicht lösen kann, helfen Ihnen vielleicht folgende Hinweise weiter:

- **Problem:** Eingeschränkte oder gar keine Verbindung mit dem Drahtlosnetzwerk.
Lösung: Überprüfen Sie die Signalstärke. Wenn das Signal zu schwach ist, müssen Sie entweder näher an den Zugriffspunkt herangehen oder Ihre Antenne neu ausrichten. Bei einer eingebauten Antenne müssen Sie vielleicht die Ausrichtung des mobilen Geräts zum Zugriffspunkt ändern. Das Problem könnte auch darin bestehen, dass das Netzwerk keine Verbindung herstellt und die Netzwerkadressen nicht richtig eingestellt sind. Prüfen Sie den Verbindungsstatus, indem Sie im Netzwerk- und Freigabecenter auf den Link der Verbindung tippen oder klicken und sich den Verbindungsstatus im Dialogfeld *Status von WiFi* ansehen. Wird der Medienstatus nicht als *Aktiviert* angezeigt, können Sie auf *Diagnose* tippen oder klicken und versuchen, das Problem mithilfe der automatischen Netzwerkdiagnose zu beseitigen.
- **Problem:** Sie können keine Verbindung mit einem Drahtlosnetzwerk herstellen.
Lösung: Wenn Sie sich außerhalb des Empfangsbereichs befinden, kann Ihr Computer keine Verbindung mit dem Drahtlosnetzwerk herstellen. Tippen oder klicken Sie auf das Netzwerksymbol in der Taskleiste. Der Computer öffnet den Bildschirmabschnitt *Netzwerke*, in dem Sie sehen, ob Netzwerke verfügbar und in Reichweite sind. Sie können hier auch prüfen, ob der Flugzeugmodus ausgeschaltet ist. Während der Flugzeugmodus eingeschaltet ist, können Sie keine Verbindungen herstellen. Sie stellen eine Verbindung zu einem WiFi-Netzwerk her, indem Sie auf eine Verbindung tippen oder klicken und dann auf *Verbinden* tippen oder klicken. Wenn Sie keine Verbindung zum Netzwerk aufbauen können oder das Netzwerk nicht in der Liste auftaucht, sollten Sie näher an den Zugriffspunkt herangehen oder die Position Ihrer Antenne oder des Computers in Bezug auf den Zugriffspunkt ändern. Vielleicht ist der Computer auch nicht so konfiguriert, dass er eine Verbindung mit diesem Netzwerk herstellen kann.

TIPP Sie erreichen bessere Übertragungsgeschwindigkeiten bis hin zu dem Wert, der mit der verfügbaren Technik maximal erreichbar ist, wenn das Signal stark ist. Wenn das Signal zu schwach ist, wird die Übertragungsgeschwindigkeit vielleicht sehr stark nach unten angepasst. Versuchen Sie, die Signalstärke zu erhöhen, indem Sie die Antenne des Adapters besser ausrichten oder die Position des Computers relativ zum Zugriffspunkt verändern.

Verbinden mit Drahtlosnetzwerken

Jeder Drahtloszugriffspunkt, in dessen Sendebereich sich ein Computer befindet, sollte für einen Computer mit einem Drahtlosadapter erreichbar sein. Standardmäßig ist Windows 8 so eingestellt, dass es die geeigneten Einstellungen automatisch ermittelt. Benötigt eine Verbindung ein Kennwort oder andere Anmeldeinformationen, werden Sie aufgefordert, die Anmeldeinformationen einzugeben, sobald Sie versuchen, eine Verbindung zum Drahtlosnetzwerk herzustellen. Sie haben auch die Möglichkeit, Drahtlosverbindungen für Benutzer vorzukonfigurieren. Daher können Sie bei Bedarf eine andere Authentifizierung, eine andere Verschlüsselung und andere Kommunikationsoptionen konfigurieren.

Gehen Sie folgendermaßen vor, um eine Verbindung für ein Drahtlosnetzwerk vorzukonfigurieren:

1. Tippen oder klicken Sie im Netzwerk- und Freigabecenter auf *Neue Verbindung oder neues Netzwerk einrichten*. Daraufhin wird der Assistent *Eine Verbindung oder ein Netzwerk einrichten* gestartet.
2. Wählen Sie *Manuell mit einem Funknetzwerk verbinden* und tippen oder klicken Sie dann auf *Weiter*.
Sie müssen nun Informationen über das Drahtlosnetzwerk eingeben, mit dem Sie eine Verbindung herstellen möchten. Um welche Angaben es sich handelt, sollte Ihr Netzwerkadministrator Ihnen sagen können.
3. Geben Sie im Feld *Netzwerkname* den Namen des Netzwerks ein (auch als Netzwerkennung oder SSID bezeichnet).
4. Wählen Sie in der Liste *Sicherheitstyp* die Art der Absicherung aus, die verwendet wird. Der *Verschlüsselungstyp* wird dann automatisch für Sie eingetragen.
5. Bei *WEP* und *WPA-Personal* müssen Sie im Feld *Sicherheitsschlüssel* den geforderten Schlüssel oder das Kennwort eingeben. Für einen WEP-Schlüssel gibt es zum Beispiel folgende Varianten:
 - 5 Zeichen mit Beachtung der Groß-/Kleinschreibung
 - 13 Zeichen mit Beachtung der Groß-/Kleinschreibung
 - 10 Hexadezimalzeichen ohne Beachtung der Groß-/Kleinschreibung
 - 26 Hexadezimalzeichen ohne Beachtung der Groß-/Kleinschreibung
6. Standardmäßig wird die Verbindung automatisch hergestellt, sobald sich der Benutzer anmeldet. Soll der Computer auch dann versuchen, eine Verbindung mit dem Netzwerk herzustellen, wenn das Netzwerk nicht erreichbar ist, weil es vielleicht zu weit entfernt ist, wählen Sie *Verbinden, selbst wenn das Netzwerk keine Kennung aussendet*. Wenn Sie dieses Kontrollkästchen nicht auswählen, wird die Verbindung nur dann im Bildschirmabschnitt *Netzwerke* aufgelistet, während sich das Netzwerk in Reichweite befindet und seine SSID aussendet.
7. Tippen oder klicken Sie auf *Weiter* und dann auf *Schließen*.

Sofern Sie sich in Reichweite eines Drahtlosnetzwerks befinden, ist es nicht nötig, eine Verbindung vorzukonfigurieren. Stattdessen können Sie die Verbindung direkt herstellen, wobei Windows die richtigen Einstellungen selbst ermittelt. Gehen Sie folgendermaßen vor, um eine Verbindung zu einem Drahtlosnetzwerk herzustellen:

1. Tippen oder klicken Sie in der Taskleiste auf das Benachrichtigungssymbol des Netzwerks oder streifen Sie vom rechten Bildschirmrand, tippen Sie auf *Einstellungen* und dann auf das Netzwerksymbol.
2. Im Bildschirmabschnitt *Netzwerke* werden alle verfügbaren Netzwerke mit Namen, Status und Signalstärke aufgelistet.

3. Nun können Sie die Verbindung zu einem Drahtlosnetzwerk herstellen oder trennen:
- Stellen Sie die Verbindung zu einem Drahtlosnetzwerk her, indem Sie das gewünschte Netzwerk auswählen und auf *Verbinden* tippen oder klicken.
 - Trennen Sie die Verbindung zu einem Drahtlosnetzwerk, indem Sie das gewünschte Netzwerk auswählen und auf *Trennen* tippen oder klicken.

Verwalten und Problembehandlung von Drahtlosnetzwerken

Sie verwalten Drahtlosnetzwerke im Bildschirmabschnitt *Netzwerke*. Wenn Sie eine Drahtlosverbindung mit der rechten Maustaste anklicken oder gedrückt halten, stehen die folgenden Verwaltungsbefehle zur Verfügung:

- ***Geschätzte Datennutzung anzeigen*** Zeigt die geschätzte Datenmenge an, die durch die Verbindung übertragen wurde. Tippen oder klicken Sie auf *Zurücksetzen*, um den Nutzungszähler zurückzusetzen.
- ***Als getaktete Verbindung festlegen*** Stellt ein, dass die Verbindung getaktet ist, damit Windows 8 Regeln und Richtlinien für getaktete Verbindungen anwendet.
- ***Als Verbindung ohne Taktung festlegen*** Stellt ein, dass die Verbindung nicht getaktet ist, damit Windows 8 Regeln und Richtlinien für getaktete Verbindungen nicht mehr anwendet.
- ***Dieses Netzwerk nicht mehr nutzen*** Löscht eine gespeicherte Verbindung aus der Liste der verfügbaren Verbindungen. Das ist nützlich, wenn Sie eine manuell erstellte Verbindung nicht mehr brauchen.
- ***Freigabe aktivieren bzw. deaktivieren*** Mit diesem Befehl stellen Sie ein, ob Sie die Freigabe zwischen Computern aktivieren und eine Verbindung zu Geräten in diesem Netzwerk herstellen wollen.
- ***Verbindungseigenschaften anzeigen*** Öffnet das Eigenschaftendialogfeld für die Verbindung, wobei die Registerkarte *Sicherheit* ausgewählt ist. Auf diese Weise können Sie schnell die Sicherheitseinstellungen anzeigen und ändern.

Windows 8 enthält zahlreiche Tools für Problembehandlung und Test der Netzwerkkonnektivität. Der Abschnitt »Problembehandlung und Testen von Netzwerkeinstellungen« in Kapitel 15, »Konfigurieren und Problembehandlung von TCP/IP-Netzwerken«, beschreibt Techniken für die Diagnose und Beseitigung von Netzwerkproblemen. Bei Drahtlosnetzwerken werden Sie mit ähnlichen Problemen zu tun haben. Neben den dort schon beschriebenen Problembehandlungstechniken können Sie Folgendes probieren:

- Prüfen Sie die Sicherheitskonfiguration für das Drahtlosnetzwerk und überzeugen Sie sich, dass die Einstellungen richtig sind. Geben Sie den Sicherheitsschlüssel erneut ein.
- Stellen Sie sicher, dass das Drahtlosgerät richtig aufgestellt ist und sich in Reichweite des Drahtloszugriffspunkts befindet. Sie können auch versuchen, den Computer näher zum Zugriffspunkt zu bringen.
- Stellen Sie sicher, dass keine Störungen von anderen Geräten ausgehen, die denselben Frequenzbereich verwenden, oder von Geräten, die magnetische Felder generieren. Versuchen Sie, Geräte wegzustellen oder auszuschalten, wenn sie Störungen verursachen.

Stichwortverzeichnis

- \$ (Dollarzeichen) 527
 - * (Stern) 593, 617
 - 128-Bit-Adressen 572
 - 1394-Debuggen 179f.
 - 16-Bit-Anwendungen 286
 - 16-Bit-Architektur 151
 - 16-Bit-Treiber 286
 - 32-Bit-Adressen 572
 - 32-Bit-Architektur 39, 152
 - 32-Bit- und 64-Bit-Treiberspeicher 337
 - 386-Modus 286
 - 512b/e-Laufwerke 431
 - 64-Bit-Architektur
 - EFI 152
 - Entwurf und Auswirkungen 26ff.
 - MBR- und GPT-Partitionsarten 429
 - UEFI 152
 - Windows 8 39
- A**
- Abbilddateien, Sicherheitseinstellungen ändern 34
 - Abbilddienste 153
 - Abbruchfehler 93, 167, 386ff.
 - Abgesicherter Modus, Option 151, 169, 181, 376
 - Abgesicherter Start, Option 79
 - Abhängige Dienste während Systemstart 167
 - Abmelden
 - Deinstallieren von Software 293
 - Dienste 318
 - Remotedesktopsitzungen 265
 - Skriptrichtlinien 206f.
 - Synchronisieren von Offlinedateien 551
 - Absturzabbilddateien 93, 387
 - Absturzabbildpartitionen/-volumes 445
 - Abstürze 305, 387, *siehe auch* Problembehandlung
 - Abziehen von Komponenten 53
 - ACL (Zugriffssteuerungsliste) 500
 - ACPI 152f., 159, 444
 - ACT (Application Compatibility Toolkit) 277
 - Active Directory-Benutzer und -Computer-Konsole 50, 226, 231
 - Active Directory-Domänen 37, 83, 226, 410f.
 - Active Directory-Gruppenrichtlinien 186
 - Anmeldebildschirme 245
 - Bearbeitungszustände 217
 - Erstellen und Bearbeiten von Einstellungselementen 220
 - Active Directory-Gruppenrichtlinien (*Fortsetzung*)
 - Gemeinsame Optionen-Registerkarte, Optionen 222
 - Geräte, Tasks und Dienste 219
 - Konfigurieren von Einstellungen 216–219
 - Nicht angewendete Einstellungen 223
 - Sicherheitskonfiguration 237
 - Standort-, Domänen- und Organisationseinheitenrichtlinien 190ff.
 - Typen unverwalteter Richtlinieneinstellungen 214ff.
 - Verarbeitungsreihenfolge 221
 - Verwaltungsaktionen 216
 - Zielelemente 223
 - Adapter 323, *siehe auch* Grafik-, Netzwerkkarten, Drahtlosadapter
 - Address Resolution Protocol Service Binding Protocol 154
 - Ad-hoc-Modus (Drahtlos) 631
 - ADM-Dateien 192
 - ADMIN\$-Freigabe 523, 528
 - Administrative Benutzer, Anwendungen 276
 - Administrative Freigaben 527
 - Administrative Vorlagen *Siehe* ADMX-Dateien
 - Administratorbenutzeranwendungen 274
 - Administratorbenutzerkonten 47f., 232ff.
 - Administratorengruppe 228, 230, 499–507, 510–516, 556
 - Administratorgenehmigungsmodus 234–238
 - Administratorkonten 228, 234–238
 - Administratormodus 233
 - Administrator-Zugriffstoken 274, 277
 - ADMX-Dateien (administrative Vorlagen) 192f., 195, *siehe auch* Richtlinieneinstellungen
 - Adressleiste 122, 125
 - Advanced Configuration and Power Interface *Siehe* ACPI
 - Advanced Encryption Standard (AES) 630
 - 128-Bit Cyclical Bit Check (AES-128-CBC) 488
 - Advanced Power Management (APM) 444
 - Advanced Programmable Interrupt Controller (APIC) 181f.
 - AES (Advanced Encryption Standard) 630
 - AES-128-CBC 488
 - Akkus
 - Energiesparplanoptionen 101
 - Energiewarnungen 110
 - Firmwarekonfigurationsdetails 156
 - Gesamtbetriebsdauer 111
 - Hybride Laufwerke 438
 - Ruhezustand 52
 - Status 597
 - Aktionen (Aufgaben) 369, 372

- Aktive Netzwerke 571
- Aktive Partitionen 38, 166, 412, 445, 447, 462f.
- Aktive Volumes 445, 462
- Aktivieren von Windows 45, 64
- Aktiviert, Gruppenrichtlinienzustand 193f.
- Aktiv-Status (Wechseldatenträger) 445
- Aktualisieren
 - Datenträgerkontingente 560
 - Dynamische DNS-Updates 583
 - Offlinedateien 548–553
- Alarmer (Energiebenachrichtigungen) 110
- Alle Apps 270
- Alternative IP-Adressen 576, 579, 599
- Alternative Shells 182
- AMD Opteron-Prozessor (AMD64) 26, 87, 160
- AMX (Manifestdateien) 337
- Analogmodems 602, 609
- Andocken 271, 123
- Anfordern der Remoteunterstützung 204
- "Angeforderte Remoteunterstützung" konfigurieren, Richtlinie 263
- Anhalten von Diensten 320
- Anhängen von Daten 505
- Anhebung 234
 - Administratoranwendungen 274
 - Administratorgenehmigungsmodus 236
 - Administratorkonten 48
 - Anwendungsprivilegien 275
 - Böswillige Software 232
 - Fälschen von Eingabeaufforderungen 276
 - Richtlinieneinstellungen 203
 - Sicherheit und Benachrichtigung 236, 276
- Anmeldeinformationen
 - Anwendungsinstallation 280
 - Bearbeiten 250
 - Datensicherung und Wiederherstellung 250
 - Dienste 318
 - Drahtlosnetzwerke 634
 - Eingabeaufforderung 236
 - Heimnetzgruppen oder Arbeitsgruppen 247
 - Hinzufügen 247
 - Kennwörter 249
 - Löschen 251
 - Netzwerkfreigaben 524, 526, 529
 - Typen 246
 - Zertifikatbasierte 249
- Anmeldeinformationsverwaltung 247, 249ff.
- Anmelden
 - Anmeldebildschirme 244
 - Aufgabenplanung 369, 372
 - Benutzerkonten 48
 - Dienstanmeldung 320
 - Dienste 318
 - Domänenkonten 231, 240
 - Lokale Anmeldung 231
 - Remotedesktop 263
 - Remotezugriff 618
 - Anmelden (*Fortsetzung*)
 - Richtlinien 209ff.
 - Skriptrichtlinien 206f.
 - Synchronisieren von Offlinedateien 549, 551
- Anonymous-Anmeldung, Identität 502
- Anpassen-Seite 114, 116
- Anspruchsbasierte Zugangssteuerung 508
 - Bedingungen festlegen 509
 - effektive Ansprüche 514
 - Richtlinien 508
 - Überwachung 535
- Antivirenprogramme 307
- Antwortdateien 31, 38
- Anwendungen
 - 32-Bit und 64-Bit 27
 - Administratorbenutzer und Standardbenutzer 274
 - Administratorkonten 232
 - Aktuell ausgeführte 291
 - Anhebung 234
 - Anzeige Probleme 146
 - Arbeitsverzeichnisse 121
 - Aufräumen von Programmdateien 74
 - Ausführen bei Anmeldung 209f.
 - Ausführungsebene 277ff.
 - Ausführungslisten 210
 - Ausführungsmodi 233
 - AutoPlay, Feature 281, 299
 - Autostartanwendungen 80, 118f., 121f.
 - Befehlspfade 295f.
 - Berechtigungen 505
 - Dateierweiterungen und Zuordnungen 297ff.
 - Deinstallieren 292
 - DEP 87
 - Ereignisprotokolle 366
 - Ereignissounds 128
 - Fehler 316
 - Fensteranordnung 129
 - Fixieren auf Taskleiste 123
 - Geräteprobleme 349
 - Gruppenrichtlinieneinstellungen 192
 - Installieren 280–284
 - Integritätsebene 276
 - Kompatibilität 286–290, 315
 - Legacy 146, 275
 - Leistungseinstellungen 85
 - Neuinstallation 37
 - Offlineverwendung 547
 - Priorität und Vorladen 440
 - Privilegien 274f.
 - Problembehandlung 315
 - Problemberichterstattung 311
 - Reagiert nicht 306, 386
 - Remotedesktopverbindungen 267
 - Reparieren 292
 - Richtlinien 215, 217
 - Setupprogramme 281
 - Signierte 75, 237

Anwendungen (Fortsetzung)

- Standard 293
- Standard- und Administratormodus 233
- UAC-konform 274
- Umgebungsinformationen 69
- Unverwaltete Richtlinienereinstellungen 215
- Validierte 237
- Veröffentlichen 285
- Virtualisierung 275, 279
- Vor Kurzem geändert oder hinzugefügt 387
- Wiederherstellungspunkte 378
- Zugriffstoken 233, 274
- Zuweisen 285

Anwendungsbildschirm 25

Anwendungseinträge (BCD) 177

Anwendungskompatibilitäts-Toolkit 28

Anwendungssteuerungsrichtlinien 280

Anwendungsverwaltungsdienst 318

Anzeige

- Auflösung 138, 144, 377
- Benutzerprivilegien 233
- Bildschirmdarstellung erweitern 143
- Bildschirm-Farbkalibrierung 146
- Bildwiederholrate 139, 145
- Energieeinstellungen 135
- Entmagnetisieren 147
- Externe 597
- Farbe und Darstellung 136ff.
- Farbprofile 145
- Farbtiefe 144
- Fehler während Systemstart 164
- Firmware 155f.
- Flackern 147
- Herunterfahren 101
- Legacy-Anwendungen, Probleme 289
- Lesbarkeit anpassen 138
- Mehrere Monitore, Unterstützung 143
- mit hohem Kontrast 137
- Monitor wechseln 142
- Problembehandlung 146, 377
- Prüfen der Treiber 139
- Remotedesktopeninstellungen 265
- skalieren 138
- Treiber ändern 140ff.
- Typen 142

Anzeigen

- Ausgeblendete Aufgaben 370
- Ausgeblendete Dateien 538
- Benutzersitzungen mit Freigaberessourcen 527
- Berechtigungen 500, 504
- Dateien mit Tastenkombination 538
- Dateierweiterungen 539
- Datenträgerkontingenteinträge 558
- Ereignisprotokolle 367
- Geerbte Berechtigungen 512
- Geplante Aufgaben 370
- Geplante Synchronisierungseinstellungen 550

Anzeigen (Fortsetzung)

- Infobereichsymbole 124
- Netzwerkkonfiguration 587
- Symbolleisten 125
- Systemdateien 538
- Update- und Installationsverlauf 359
- Wählverbindungen, Speicherorte 605

APIC (Advanced Programmable Interrupt Controller) 181f.

APIPA (Automatic Private IP Addressing) 591, 599

APM (Advanced Power Management) 444

Application Compatibility Toolkit (ACT) 277

Apps *Siehe auch* Desktop-Apps

- Elemente an Taskleiste anheften 25
- Sperrbildschirm 115
- wechseln zu 25

Arbeitsgruppen

- Anmelden 48
- Dateifreigabeoptionen 495
- Erstellen von Freigaben 517–522
- Gespeicherte Anmeldeinformationen 247
- Heimnetzgruppen 46
- Informationen 64
- Kennwörter 242
- Konten 231
- Lokale Benutzerkonten 238
- UAC 47
- Wiederherstellung, Richtlinien 490

Arbeitsplatznetzwerke 605, 609f.

Arbeitsspeicher

- Abbruchfehler 387
- Angeben 170
- Arbeitsspeicher aus unteren Adressbereichen 181
- BCD-Speichereinträge 179f.
- Bildschirmeschoner 134
- DEP 87, 182
- Diagnose 57, 176
- Einstufungen 66
- Fehlermeldungen 347
- Firmwarekonfigurationsdetails 156
- Grafik 136
- Hinzufügen 324
- Informationen 64
- Legacy-Anwendungen 286
- Nicht ausführbare Abschnitte 87, 182
- Optimieren 440
- Physische Arbeitsspeicheradressen 180
- Priorität 439f.
- Problembehandlung 163, 304
- Puffer 573
- Startoptionen 79
- Startvorgang 154, 162
- Überschreiben 410
- Verringern 181
- Windows 8, Voraussetzungen 39
- Windows-ReadyBoost 436ff.
- Arbeitsspeichernutzungspriorität 439f.
- Arbeitsspeicherzuweisungsdienste 153

Arbeitsstationen *Siehe* Computer
 Arbeitsverzeichnisse 121
 ARP (Address Resolution Protocol) 154
 ARPSBP (Address Resolution Protocol Service Binding Protocol) 154
 Assistent zum Aktivieren von Windows 45
 Assistent zum Erstellen freizugebender Ordner 520, 546
 Assistent zum Initialisieren und Konvertieren von Datenträgern 446
 Assistent zum Suchen neuer Hardware 339
 Assoc-Tool 297
 Audio aufzeichnen, Problembehandlungsmodule 314
 Audiocontroller 154
 Auf Datenträger brennen, Assistent 481, 483f.
 Aufbrechen von Spiegelsätzen 466
 Aufgaben, Richtlinien 215
 Aufgabenplanung 62, 368, 370
 Aufgabenplanung und Schtasks 368
 automatische Wartung 313
 Ereignisprotokolle 366
 Funktionen und Anpassen 368–373
 Problembehandlung 372
 Typen von Aufgaben 369
 Unverwaltete Richtlinienereinstellungen 215, 219
 Verwalten von Aufgaben 370
 Auflösen
 Synchronisierungskonflikte 552
 Variablen 522
 Auflösung
 Ändern 144
 Drucken 138
 Grafikanzeige 180
 Lesbarkeit 138
 Problembehandlung 139
 Treiberdetails 139
 Aufwacheinstellungen 102, 108, 159ff.
 Aufwachen aus dem Ruhezustand, Eintrag 178
 Aufwacheignisse 160, 358
 Aufwecken, Windows Resume Loader 375
 Aufzeichnen von Problemen 260
 Ausbalanciert, Energiesparplan 52, 100
 Ausführbare Dateien *Siehe* Anwendungen
 Ausführen
 Anwendungen 291
 Anwendungsprivilegien 275
 DISM 30
 Ausführliche Ausgaben 79, 173
 Ausführungsebene für Anwendungen 277ff.
 Ausführungsliste, Anwendungen 210
 Ausführungsschutz 87
 Ausgeblendete Aufgaben 369f.
 Ausgeblendete Dateien 538
 Ausgeblendete Geräte 337
 Ausgeblendete Skripts 207
 Ausgeschaltet, Zustand 160
 Auslagerungsdateien (Pagefile.sys) 85, 162, 436, 445
 Auslagerungsdateipartitionen oder -volumes 445

Auswerfen von Geräten 349, 432, 438
 Authenticode 276
 Authentifizierte Benutzer, Identität 502
 Authentifizierung
 Anmeldeinformationen 246
 BitLocker, Richtlinien 410
 Remotedesktopsitzungen 265
 Remotezugriff 621
 Startvorgang 162
 TPM-Methoden 414
 Automatic Private IP Addressing (APIPA) 591, 599
 Automatisch ausblenden, Feature 123
 Automatisch optimierte Monitore 147
 Automatische Anpassung des Empfängerfensters, Feature 573
 Automatische Erkennung von Black-Hole-Routern 573
 Automatische Installation 31, 38
 Automatische Netzwerkverbindungen 614
 Automatische Neuverbindung 265
 Automatische Reparatur 375
 Automatische Speicherabbilder 93
 Automatische Synchronisierung 545, 549ff.
 Automatische Updates 355, 357ff., 379
 Automatische Wartung
 Anpassen 312
 Ausführungszeit 356
 geplante Durchführung 313
 Statusangaben 313
 Automatischer Neustart 181, 377
 Automatisches Neusenden bei ausgefallenem Gateway 573
 AutoPlay, Feature 280f., 299, 418
 Autostartanwendungen
 Aktivieren 80
 BCD-Speichereinträge 177
 Deaktivieren 80, 171
 Festlegen für Benutzer 119
 Hinzufügen und Deinstallieren 121f.
 Ordnerspeicherort 119
 Verknüpfungen 118–121
 Autostart-Ordner 119, 121f.

B

Bandbreite 364
 Basisdatenträger 441
 Datenträgerverwaltung-Tool 433
 Funktionen 428–435
 Konvertieren in dynamische 428, 433, 448ff.
 Merkmale 441–450
 Notebooks 444
 Partitionen 38, 428–435
 Übergreifende oder Stripeset 456
 Vergrößern/Verkleinern 457
 Volumes 444ff.
 Basisvideo, Option 79
 Baudraten 179f.
 BCDBoot-Tool 29

- BCD-Editor und BCD-Speicher
 - Anzeigen gespeicherter Einträge 173–176
 - DEP 182
 - Eintragseigenschaften 174f.
 - Eintragswerte 178–182
 - Erstellen von Speichern 176
 - Exportieren des Inhalts 173
 - Funktionen und Befehle 171ff.
 - GUIDs 174, 176
 - Importieren und Exportieren von Speichern 177
 - Kopieren oder Erstellen von Einträgen 173, 177
 - Legacy-Betriebssystemeinträge 175
 - PAE-Konfiguration 182
 - Problembehandlung 163
 - Sichern von Daten 172
 - Standardbetriebssystem, Eintrag 183
 - Standardtimeouts 184
 - Startablauf temporär ändern 184
 - Starteinträge für gespiegelte Datenträger 478
 - System und Nicht-System 173, 176
 - Systemstart 151, 155
 - Wiederherstellen 173
 - Zusätzliche Betriebssystemeinträge 175
- BCD-Registrierungsdatei 151
- Beantworten von Einladungen 365
- Bearbeitungszustände 217, 223
- Bedingungen (Aufgaben) 369, 372
- Beenden
 - Aufgaben 370
 - Dateifreigabe 519
 - Dienste 320
 - Geerbte Berechtigungen 512
 - Hängende Anwendungen 386
- Befehlspfad 295f.
- Befehlshell-Batchskripts 206, 368
- Befehlszeile 29, 40, 287
- Begrüßungsbildschirm, Konfiguration 244
- Benachrichtigungen
 - Administratorgenehmigungsmodus 235
 - Akkuwarnungen 110
 - Anpassen 124, 310–316
 - Datenträgerkontingente 195, 197, 555
 - Dienste 318
 - durch Apps, Verlauf 272
 - Energiewarnungen 110
 - Ereignisse 366
 - Geräte-Manager 336
 - Hardwarefehlermeldungen 346–349
 - Infobereich 124
 - Synchronisierungscenter 552
 - Updates 358
 - Wartungscenter 45f., 306
- Benachrichtigungen-Seite 116
- Benutzer *Siehe auch* Benutzerkonten
 - Administrative, Richtlinien 194
 - Anmeldeinformationen 246–251
 - Anmeldungs- und Systemstartrichtlinien 209ff.
- Benutzer (*Fortsetzung*)
 - Benutzer hinzufügen, Assistent 240
 - Berechtigungen, Liste 501
 - Dateifreigabe 496
 - Datenträgerkontingente 556, 558
 - Ereignisprotokolleinträge 367
 - Gruppenrichtlinieneinstellungen 191, 193
 - Hilfe- und Supportfeatures anpassen 310
 - Hinzufügen zu Gruppen 256
 - Installieren von Anwendungen 283
 - Lokale Benutzerkonten 47
 - Netzwerkrichtlinien 202f.
 - Neue Konten 252
 - Offlinedateirichtlinien 198–202
 - Persönliche Bibliotheken 44
 - Persönliche Ordner 44
 - Profile 89, 488
 - Remotedesktopliste 264
 - Remotezugriff 260–267
 - Richtlinieneinstellungen 186
 - Skriptrichtlinien 205–209
 - Skriptzuweisungen 208
 - Spezielle Berechtigungen 505f.
 - Standardberechtigungen 499–507, 510–516
 - Unverwaltete Richtlinieneinstellungen 214ff., 220
 - wechseln 244
- Benutzer hinzufügen, Assistent 240
- Benutzer, Identität 502
- Benutzerdatenquellen, Richtlinien 215
- Benutzerdefinierte Standbyoptionen 103
- Benutzerdefinierter Systemstart 77, 169
- Benutzer-Gruppe 230f., 496
- Benutzerkonten
 - Aktivieren oder Deaktivieren 257
 - Anmelden 48
 - Anmeldenames 227
 - Deinstallieren und Zugriff verweigern 246
 - Gastkonten 258
 - Geplante Aufgaben 372
 - Gruppenkonten 229ff.
 - Hinzufügen 238
 - Kennwörter 50ff., 228, 242
 - Kennworthinweise 242
 - Lokale Benutzerkonten 227ff.
 - Löschen 259
 - Microsoft-Konto 239
 - Neue Konten 252
 - Remotezugriff 260–267
 - Schnelle Benutzerumschaltung 49
 - Standardgruppen/-konten 228
 - synchronisiert 239
 - Typ ändern 241
 - UAC 232ff.
 - Umbenennen 259
 - und Family Safety 248
- Benutzerkonten-Dienstprogramm 242
- Benutzerkontensteuerung *Siehe* UAC

- Benutzermodusausnahmen 180
- Benutzernamen 618, 624, 626
 - verbergen 245
- Benutzeroberfläche anpassen 114, 147
- Benutzer-Ordner 122
- Benutzerprofile 89, 488
- Benutzerprozesse 439f.
- Benutzer-Seite 116
- Benutzerspezifische lokale Gruppenrichtlinienobjekte 187
- Benutzerumgebungsvariablen 88, 91, 167
- Benutzervariable, Richtlinien 216
- Benutzerzertifikate 492
- Benutzte Dateien 353
- Berechtigungen
 - Anpassung 265
 - Anzeigen 504
 - Aufgabenplanung 369
 - Dateibesitz 510
 - Dateifreigabe 496
 - effektiv, ermitteln 514
 - Effektive 514
 - Empfehlungen 503
 - Erweiterte Freigaben 519
 - Gruppen 503
 - Gruppenrichtlinieneinstellungen 186
 - Installieren und Ausführen von Anwendungen 275
 - Legacy-Anwendungen, Probleme 289
 - Lesen oder Bearbeiten 505
 - Netzwerkfreigaben 516, 521
 - NTFS-Dateisystem 494, 499–507, 510–516
 - Öffentlich-Ordner 530
 - Offlinedateien 548
 - Prinzip der geringstmöglichen Rechte 503
 - Problembehandlung 280, 289, 514, 529
 - Sicherheit-Registerkarte 542
 - Spezialidentitäten 516
 - Spezielle Berechtigungen 504–507
 - Standardfreigaben 519
 - Vererbung 501, 511–514
 - Verschlüsselung 489
 - Verweigern und Vorrang 499, 501
 - Wechseldatenträgergeräte 480
 - Weitergeben 511
 - Zugriffs- und Freigabeberechtigungen 494
- Bereitstellung
 - Anpassen von Windows-Abbildern 35
 - Anwendungen 285
 - Automatisieren 32
 - BitLocker 408–412
 - DISM 30f.
 - Erstellen von Windows-Abbildern 31f.
 - ISO-Abbilder 482
 - nach Genehmigung durch einen Administrator 34
 - Skripts 32
 - Vorabberichten von Computern 33
 - WIM-Dateien 31
 - Windows PE 29
 - Bereitstellungstools 28
- Berichte
 - Berichtswarteschlange konfigurieren 317
 - Datenträgerbereinigung-Tool 74
 - Energieeffizienzdiagnose-Bericht 99
 - Energieprobleme 98
 - Signaturprüfung-Dienstprogramm 76
 - Systemintegritätsberichte 68
 - Wartungscenterlinks 307
 - Zuverlässigkeitsberichte 308
- Berichte, Probleme *Siehe* Problemberichterstattung
- Besitz 393, 396, 399, 500, 505, 510, 560
- Betriebsprotokolle, Gruppenrichtlinien 187
- Betriebssysteme
 - 64-Bit-Unterstützung 27
 - Anzeigen beim Systemstart 92
 - BitLocker, Richtlinien 410
 - Standard 183
 - Startreihenfolge 183
 - Startvorgang 154
- Betriebssystemkonfiguration *Siehe* Konfiguration, Betriebssysteme
- Betriebssystemlaufwerke 406
 - Richtlinien 410
- Betriebssystemordner 528
- Betriebssystem-Startinformationen, Option 79
- Bezeichnungen für Volumes und Partitionen 455, 461
- Bibliotheken 44, 495
- Bildcode, Anmeldung, Richtlinie 210
- Bilddateien 130
- Bildschirmanzeige *Siehe* Anzeige
- Bildschirm-Farbkalibrierung 146
- Bildschirmschoner 128, 133f.
- Bildwiederholrate 139, 145
- BIND, dynamische DNS-Updates 583
- Bindung (TPM) 391
- BIOS (Basic Input/Output System) 27, 38, 150f., 166
- BIS (Boot Integrity Services) 153
- BitLocker To Go 51, 402, 418, 437
- BitLocker-Laufwerkverschlüsselung
 - Bereitstellen 408–412
 - Bereitstellung vorbereiten 413f.
 - Deaktivieren oder Ausschalten 425
 - Entsperrern des Computers 424
 - Funktionen 402–405
 - Installieren von Software 413
 - Kennwörter ändern 404
 - Kennwortkomplexität 404
 - Konfigurieren 412
 - Konsole 413
 - Nicht-System-Volumes 415
 - PIN 422
 - Problembehandlung 423–426
 - Richtlinien 410
 - Richtlinieneinstellungen 409
 - Speichern von Datensicherungsinformationen 411
 - Status 423

BitLocker-Laufwerkverschlüsselung (*Fortsetzung*)
 Systemvolumes 419–422
 TPM 391
 USB-Flashlaufwerk, Installation 417
 Verschieben von Datenträgern 467
 Verschlüsselungsstärke 405
 Versionen 409
 Wechseldatenträger, Systemstarteinstellungen 161
 Wiederherstellen von Daten 424
 Wiederherstellung, Richtlinien 490
 Wiederherstellungskennwörter 414
 Wiederherstellungskonsole 424
 BITS (Intelligenter Hintergrundübertragungsdienst) 353, 563
 Black-Hole-Router-Erkennung 573
 Blockierte Anwendungen 276
 Blockierte Datenträger-E/A-Operationen 305
 Blockierte Herausgeber 276
 Blockierte Laufwerkszugriffe 543
 Blockierte Netzwerkerkennung 571
 Blockierte TPM-Befehle 410
 Bluetooth-Geräte 329ff., 333ff.
 Blu-ray, Unterstützung 481
 Boolesche Werte, BCD-Speichereinträge 178
 Boot Integrity Services (BIS) 153
 Boot.ini-Datei 60, 155, 172
 Bootmgr-Datei *Siehe* Start-Manager
 Bootsector (Windows-Startsektoranwendung) 172, 177
 Bootsect-Tool 29
 Böswillige Software 182, 232, 274, 307
 BranchCache 563ff.
 Breitbandverbindungen 602
 Anmeldung konfigurieren 618
 Aufbauen 625
 Automatische oder manuelle Verbindungen 614
 Erstellen 611
 Identitätsüberprüfung 621
 Netzwerkprotokolle und Komponenten 621ff.
 Problembehandlung 626
 Proxyeinstellungen 615–618
 Windows-Firewall 623
 Brennen, Disks 481–484

C

CDs und CD-Laufwerke
 AutoPlay, Feature 299
 Dateien öffnen 293
 Daten-CDs 481–485
 Deinstallieren der Brennfähigkeit 542
 Freigabenamen 528
 Kein Medium, Laufwerksstatus 469
 CHAP (Challenge Handshake Authentication Protocol) 621
 Charmleiste öffnen 24
 Charms 24
 Chat-Fenster (Remoteunterstützung) 364f.
 Chkdsk.exe *Siehe* Datenträgerprüfung-Tool

Cipher-Dienstprogramm 405, 492
 Client für Microsoft-Netzwerke, Komponente 605, 622
 Cluster 442f., 454
 CMOS-Firmwareschnittstelle 155
 COM (Component Object Model) 27, 316
 Compact-Dienstprogramm 487
 CompactFlash-Karten 436, 445
 Component Object Model (COM) 27, 316
 Computer
 64-Bit-Unterstützung 27
 Administrative, Richtlinien 194
 Anmeldungs- und Systemstartrichtlinien 209ff.
 Automatische Problemerkennung 307
 Automatische Updates 355
 Datei- und Datenverwaltungsrichtlinien 195–202
 Einstellungen für die Problemberichterstattung 311
 Ereignisprotokolleinträge 367
 Gruppenrichtlinieneinstellungen 191
 Herunterfahren 385
 Namen 64
 Netzwerkrichtlinien 202f.
 Netzwerkzugriffstypen 571
 Neu starten 385
 Offlinedateirichtlinien 198–202
 Registrierungsänderungen für Gruppenrichtlinien 193
 Remotezugriff 260–267
 Richtlinieneinstellungen 186
 Skriptrichtlinien 205–209
 Spezielle Berechtigungen 505f.
 Unverwaltete Richtlinieneinstellungen 214ff., 220
 Windows-Leistungindex 65
 Zuverlässigkeits- und Stabilitätsberichte 308
 Zuweisen von Skripts 208
 Computer-Konsole 431
 Computernamen-Registerkarte (Systemeigenschaften) 83
 Computerreparaturmodus 376
 Computerschutz-Registerkarte (Systemeigenschaften) 94–97, 379
 Computersymbol 131
 Computerverwaltung öffnen 368
 Computerverwaltung-Konsole
 Administrative Freigaben 527
 Aktivieren von Offlinedateien 546
 Aufbau 306
 Beenden, Starten oder Anhalten von Diensten 320
 Dateifreigabeeinstellungen 520ff.
 Dienste konfigurieren 317
 Ereignisprotokolle anzeigen 367
 Funktionen 61
 Netzwerkfreigaben 517, 527
 öffnen 61
 Remotecomputerverwaltung 63
 Convert-Dienstprogramm 462
 Cotype-Tool 29
 CRC (Cyclic Redundancy Checking) 153
 Current-Registrierungswert 167
 Cursordesigns 128
 Cyclic Redundancy Checking (CRC) 153

- D**
- Darstellung 84, 136ff.
 - Datagrammübertragung 496
 - Datei- und Druckerfreigabe für MS-Netzwerke, Komponente 622
 - Datei- und Druckerfreigabe, Ausnahme 496, 528
 - Dateien
 - Attribute 505
 - Ausgeblendete 538
 - Benutzte Dateien und Updates 305, 353
 - Beschreibungen 540
 - Besitz 510
 - Brennen auf CDs oder DVDs 481, 484
 - Cluster 442
 - Datei-Explorer, Konfiguration 538–544
 - Datenträgerbereinigung 73
 - Deinstallierte Programme, Überreste 293
 - Desktopspeicherort 129
 - Einladungen zur Remoteunterstützung 362f.
 - Erweitern komprimierter 487
 - Erweiterungen *Siehe* Dateierweiterungen
 - Freigeben *Siehe* Dateifreigabe
 - Gerätetreiber 337f.
 - Größe 539
 - Hintergrundübertragung 318
 - Komprimieren 486
 - Netzwerkberechtigungen 516
 - NTFS-Berechtigungen 499–507, 510–516
 - Öffentlich-Ordner 530
 - Offlinedateien *Siehe* Offlinedateien und Ordner
 - Richtlinien 215, 217
 - Signaturprüfung 75
 - Spezielle Berechtigungen 507
 - Standardprogramme 293
 - Unverwaltete Richtlinieneinstellungen 215
 - Verknüpfungen 119
 - Verschlüsselung 488–492
 - Versionen 95, 544
 - Vorschau 541
 - Wiederherstellen von Vorgängerversionen 373
 - Zuordnungen 297ff.
 - Dateien für virtuelle Festplatten (VHD) 30, 60
 - Dateien öffnen 297ff.
 - Dateierweiterungen
 - Aktivierung 285
 - Anzeigen 539
 - Dateiverknüpfungen 297ff.
 - Offlineverwendung 199
 - Standardprogramme 293
 - Datei-Explorer 163, 517, 538f., 541ff., 590
 - Adressleiste 431
 - Dateifreigabe
 - Administrative Freigaben 527
 - Aktivieren der Netzwerkfreigabe 496, 516, 539
 - Ändern oder Deaktivieren 496, 519
 - Computerverwaltung 520ff.
 - Entschlüsselte Dateien 491
 - Dateifreigabe (*Fortsetzung*)
 - Freigabe beenden 495
 - Gruppenrichtlinien 522
 - Netzwerkfreigaben 516
 - NTFS-Berechtigungen 499–507, 510–516
 - Öffentlich-Ordner 530f.
 - Offlineverwendung von Dateien 521, 546ff.
 - Problembehandlung 528f.
 - Sicherheit 494–498
 - Typen 494, 516
 - Überwachen und Verfolgen 532–535
 - Verhindern 498
 - Wechseldatenträger 480
 - Zugriff auf Ressourcen 523–527
 - Dateifreigabe-Assistent 496, 518, 539
 - Datei-Menü entfernen 542
 - Dateinamen 286, 505
 - Dateipfade 295f.
 - Dateisignaturverifizierung 72
 - Dateisysteme *Siehe auch* einzelne Dateisysteme, z.B. FAT, NTFS
 - Auswählen 454
 - Basisdatenträger 428
 - BitLocker 404
 - Cluster 442f.
 - exFAT 430
 - FAT, FAT16 und FAT32 430
 - Formatieren von Festplatten 450, 458
 - Konvertieren in NTFS 462
 - Logische Laufwerke 443
 - ReFS 430
 - Sicherheits- und Freigabeoptionen 494
 - Verschlüsselung 490
 - Wechseldatenträger 479
 - Dateisystemobjekt-Verknüpfungen 120
 - Dateisystemtest *Siehe* Datenträgerprüfung-Tool
 - Dateityp, Richtlinien 215
 - Dateitypen *Siehe* Dateierweiterungen
 - Dateiverknüpfungen 297ff.
 - Dateiversionsverlauf 381–384
 - Dateiverwaltungsrichtlinien 195–202
 - Dateizuordnungstabellen 430
 - Daten nicht redundant/vollständig, Volumestatus 470
 - Datenausführungsverhinderung (DEP) 87, 182
 - Datenpartitionen 39
 - Datenquellen, Richtlinien 215, 217
 - Datensicherung *Siehe auch* Sichern und Wiederherstellen
 - Anmeldeinformationen 250
 - BCD-Speicherdaten 172
 - BitLocker-Wiederherstellungsinformationen 411
 - Erstellen von Datensicherungen 381ff.
 - Konfigurieren von Datensicherungen 381
 - Persönliche Daten 381
 - Systemabbilder 381
 - Systemwiederherstellungstool 377–381
 - TPM 398, 411
 - Wiederherstellen persönlicher Daten 385
 - WMI-Repository 71

- Datensicherungstool 72
- Datenträger defragmentieren 72, 475ff.
- Datenträgerbereinigung 72f., 468
- Datenträgerfehler reparieren 471–475
- Datenträgerformate *Siehe* Dateisysteme
- Datenträgerkontingente 555–562
- Datenträgerprüfung-Tool 386, 468, 471–475
- Datenträgersignaturen 446
- Datenträgerverwaltung-Konsole
 - Aktive Partitionen 38
 - Basis- und dynamische Datenträger 448ff.
 - Datenträger defragmentieren 475ff.
 - Datenträgerkontingente 557–562
 - Formatieren von Partitionen und Volumes 458
 - Funktionen und Anzeige 433
 - Gespiegelte Datenträger 465ff.
 - Initialisieren von Datenträgern 446
 - Komprimieren von Laufwerken 486
 - Laufwerkbuchstaben und -pfade 459
 - Löschen von Partitionen oder Volumes 461
 - MBR- und GPT-Datenträger 447
 - Partitionen, Logische Laufwerke und einfache Volumes 452–455
 - Statusmeldungen 469f.
 - Übergreifende und Stripesetvolumes 455
 - Verkleinern oder Vergrößern von Volumes 457f.
 - Verschieben von Datenträgern 467
 - Virtuelle Festplattenlaufwerke 60
 - Volumebezeichnungen 461
 - Volumezustandsmeldungen 470f.
 - Wiederherstellen von Volumes 464
 - Zugriff 63
- Datenverwaltungsrichtlinien 195–202
- Datenvolumes 412, 425
- Datenwiederherstellungs-Agenten 405, 411
- Datum 550
- Dauer von Verbindungen 586
- DCOM (Remoteunterstützungsanforderungen) 361
- Deaktiviert, Gruppenrichtlinienzustand 193f.
- Debuggen
 - Abbruchfehler 386ff.
 - Aktivieren 170, 173
 - BCD-Speichereinträge 179
 - Debuginformationen schreiben 93
 - Globale Debugparameter 176
 - Kernel 181
 - Onlinecrashanalyse, Feature 387
 - Privater Debuggertransport 181
 - Startoptionen 79
- Default-Registrierungswert 167
- Defragmentierung 72, 468, 475ff.
- Deinstallieren *Siehe auch* Löschen, Auswerfen von Geräten
 - Anwendungen 292
 - Geräte 336
 - Gerätetreiber 345
 - Systemwiederherstellung 379
 - Unvollständige Deinstallation 281
- Dekomprimieren von Daten 487
- DEP (Datenausführungsverhinderung) 87, 182
- Designs 45, 127ff.
 - mit hohem Kontrast 137
- Designs-Ordner 129
- Desktop
 - Anpassen 114, 129–132, 147
 - Anzeigen 23
 - Dateien und Ordner 129
 - Erweitern auf mehrere Monitore 143
 - Freigeben 530
 - Hintergrundbilder 128f.
 - Öffnen 23
 - Sicherer und Standard 234
 - Symbole 131
 - Symbolleiste 126
 - Taskleiste 122–125
 - Verknüpfungen 118–121
- Desktop-Apps 270, *siehe auch* Anwendungen
 - alle Apps 270
 - andocken 271
 - Nachverfolgung 272
 - Richtlinien für Benachrichtigungen 272
 - verwalten 270
- Desktopbilder (Energiesparplan) 101
- Desktop-Ordner 119
- Desktop-Programme 270
 - automatisches Öffnen verhindern 272
- DFS (verteiltes Dateisystem) 542
- DHCP (Dynamic Host Configuration Protocol)
 - Alternative Einstellungen 596
 - DHCPv4, DHCPv6 und Dienstbindung 154
 - DNS-Serveradressen 581
 - Drahtlosnetzwerke 633
 - Dynamische IP-Adressen 576
 - Freigeben und Erneuern 592
 - Konfiguration anzeigen 588
 - Konfigurieren von WINS 584
 - Mobile Computer, Einstellungen 598
 - Standardnetzwerkeinstellungen 623
- DHCPv6-fähiger DHCP-Client, Feature 574
- Diagnosesystemstart 77, 169
- Diagnosetools *Siehe auch* Problembehandlung, Problembehandlungsmodule
 - Hardwarefehlermeldungsliste 346–349
 - Integrierte 55
 - Remoteunterstützung und Remotedesktop 260
 - Systemstartkonfiguration 169
- Dialup, Identität 502
- Diashow 101, *siehe auch* Projektoren
- Dienste
 - Aktivieren 81
 - Anhalten von Geräten 349
 - Anmeldung 320
 - Beenden, Starten oder Anhalten 320
 - Deaktivieren 81, 170, 322
 - Ereignisprotokolle 366

Dienste (Fortsetzung)

- Gerätefehlermeldungen 348
- Konfigurieren 317
- Laden 77
- Neustart und Wiederherstellung 321
- Problembehandlung 163, 376
- Reaktionsgeschwindigkeit 85
- Startvorgang 162
- Supportdienste 317ff.
- SYSTEM-Konto 228
- Systemstartfehler 166
- Systemstartkonfiguration 320
- Unverwaltete Richtlinieneinstellungen 215, 219, 322
- Wiederherstellung, Richtlinien 305

Dienste für System Management BIOS (SMBIOS) 152

Dienste, Richtlinien 215

Dienste-Tool 63

Dienstkonten 505f.

Dienststeuerungs-Manager 162, 167

Digital Video Interface (DVI) 142

Digital-Analog-Konverter 609

Digitale Signaturen 75, 337, 377

Digitalmodems 602

Direct Memory Access (DMA) 68

DirectAccess, Feature 56, 203, 314, 603, 622

DirectX 9-Grafikprozessoren 39, 136

DirectX-Diagnosetool 72

Direktwählverbindungen *Siehe* Wählverbindungen

Discmastering 481

Diskette 51, 244

Diskettenlaufwerke 543

DiskPart-Tool 29, 43, 435, 452

- Aktive Partitionen 448
- MBR- und GPT-Datenträger 447
- Virtuelle Festplattenlaufwerke 60

DISM (Tool zur Abbildverwaltung für die Bereitstellung)

- Anpassen von Windows-Abbildern 35
- ausführen 30
- Unterbefehle 30f.
- verwenden 30
- wichtige Befehle 35
- wichtige Unterbefehle 35
- Windows PE 29
- Windows-Editionen 30

DisplayPort-Adapter 143

Distributed Transaction Coordinator 229

DLLs (Dynamic-Link Library) 27, 316, 337

DMA (Direct Memory Access) 68

DNS (Domain Name System)

- Adresse automatisch abrufen 579
- Cache leeren 593
- DHCP-Adresse freigeben und erneuern 592
- Drucker 334
- Dynamische Updates 583
- Hinzufügen von IP-Adressen 582
- Konfiguration anzeigen 587
- Konfigurieren 581ff.

DNS (Domain Name System) (Fortsetzung)

- Netzwerkfreigaben 529
- Ping 590
- PowerShell 26
- Primäres DNS-Suffix 83
- Private IPv4-Adressen 600
- Prüfen von Einstellungen 83
- Registrieren von Adressen 583, 593
- Statische IP-Adressen 578
- Suffixe 582

Dollarzeichen (\$) 527

Domain Name System *Siehe* DNS

Domänen

- Anmeldebildschirme 245
- Anmelden 49
- Anmeldennamen 227
- Anmeldung mit lokalem oder Domänenkonto 231
- Begrüßungsbildschirm 245
- Computer, Mitgliedschaft 83
- Datei- und Datenrichtlinien 195–202
- Dateifreigabeoptionen 495
- Deinstallieren von Konten und Zugriff verweigern 246
- Domänenbenutzerkonten 226
- Freigaben 517–522
- Informationen 64
- Kennwörter 50, 244
- Lokale Anmeldung 240
- Netzwerkverbindungsrichtlinien 203
- Remotезugriff 618
- Richtlinieneinstellungen 186
- Sicherheitskonfiguration 237
- UAC 48
- Updateserver 358
- Verschlüsselung, Wiederherstellungsrichtlinien 490
- VPN-Verbindungen 612
- Wählverbindungen 610
- Wiederherstellungsagenten 489

Domänenadministratorgruppe 556

Domänengruppenrichtlinienobjekte 188, 190–193

Doppelpunkte in IP-Adressen 573

Doppelte Geräte 349

DOS-Anwendungen 286

Double-Colon-Notation 573

Download

- Benutzerprivilegien 233
- Designs 127
- Öffentliche Downloads-Ordner 530
- Updates 40, 42, 352ff.
- Vertrauenswürdige Partner 353

DPI (Dots Per Inch) 138

Drahtlosadapter 631

Drahtlosgateways 628

Drahtlosgeräte 329ff., 333ff.

Drahtlosnetzwerke 628–635

- Energiespareinstellungen 101
- Notebookeinstellungen 596

Drivers-Ordner 337

DriverStore-Ordner 337
 Drucken
 Auflösung 138
 Wiederherstellungsschlüssel 417f.
 Drucker 215, 233, 267, 331–335
 Drucker, Problembehandlungsmodule 314
 Druckerfreigabe 497, 516, 528
 Druckerinstallations-Assistent 331, 333
 Druckertreiberupdates 355
 Drvload-Tool 29
 DSL-Router 602
 Dual-Boot 415
 Dual-IP-Schicht-Architektur 572
 Dual-Link-DVI 142
 Dual-TCP/IP-Stack 573f.
 Durchsatz 402, 437, 574
 DVDs und DVD-Laufwerke
 AutoPlay, Feature 299
 Dateien öffnen 293
 Daten-DVDs 481–485
 Freigabenamen 528
 DVI, DVI-I, DVI-A, DVI-D (Digital Video Interface) 142
 Dynamic Host Configuration Protocol *Siehe* DHCP
 Dynamic-Link Library 27, 316, 337
 Dynamische Datenträger und Volumes 441
 Datenträgerverwaltung-Tool 433
 Externe Festplattenlaufwerke 444
 Fehlerkorrektur 442
 Funktionen 428–435
 Gespiegelte Datenträger 441
 Konvertieren in Basisdatenträger 428, 433, 448ff.
 Merkmale 441–450
 Notebooks 444
 Partitionen 38, 428–435
 Stripeset-Datenträger 441, 456
 Übergreifende Datenträger 441, 456
 Vergrößern 457
 Verkleinern 457
 Verschieben in neue Systeme 467
 Volumes 428, 444ff.
 Wechseldatenträger 443
 Dynamische IP-Adressen 576, 579, 591f., 596, 598, 633

E

E\$-Freigabe 528
 E/A-Priorität 439
 E/A-Probleme 68, 305, 464, 469
 EAP (Extensible Authentication Protocol) 621, 630
 Easy Connect-Einladungen 362f.
 Echoanforderungen 496
 EEPROM 163
 Effektive Berechtigungen 514
 Effektiver Zugriff 514
 EFI (Extensible Firmware Interface) 27, 39, 150, 166, 173
 EFI-Bytecode, virtuelle Computer 153
 EFI-Systempartition (ESP) 27, 39, 429

EFS (Verschlüsselndes Dateisystem) 390, 488ff.
 Eigene Zertifikate, Speicher 249
 Eigenschaften von BCD-Einträgen 174f.
 Eigenschaftendialogfeld (Anwendungen) 287, 290
 Eigenschaftendialogfeld (Unverwaltete Richtlinieneinstellungen) 221
 Eine Verbindung oder ein Netzwerk einrichten, Assistent 608f., 611f.
 Einfache Volumes 428, 448, 452–455, 457f., 464
 Eingabe/Ausgabe (E/A) *Siehe* E/A-Probleme
 Eingabeaufforderung nach Updates 358
 Eingehende Verbindungen, Problembehandlungsmodule 314
 Einladungen 204f., 261f., 361, 363ff.
 Einmal ausführen, Anwendungsausführungsebene 277
 Einstellungen *Siehe* (Unverwaltete) Richtlinieneinstellungen
 Einstellungen synchronisieren-Seite 117
 Einstellungen, Charm 24
 Einstellungserweiterungen 223
 Einstellungsleiste 24f.
 Einstufungen 65
 Einwählverbindungen *Siehe* Wählverbindungen
 EIST (Enhanced Intel SpeedStep Technology) 160
 Elektromagnetische Störung 147, 330, 635
 E-Mail-Einladungen zur Remoteunterstützung 205, 362f.
 Emergency Management Services *Siehe* EMS
 Empfänger (Drahtlos oder Bluetooth) 329
 Empfangsfenster 573
 Empfohlene Updates 355
 EMS (Emergency Management Services) 173, 176, 179ff.
 Energieeffizienzdiagnose-Bericht 99
 Energieoptionen, Richtlinien 215
 Energiesparen, Problembehandlungsmodule 314
 Energiesparpläne
 Aktive Pläne 98
 Auflisten 98
 Auswählen und optimieren 104ff.
 Einstellungen 67
 Erstellen 106
 Konfigurieren 100–104
 Löschen 98
 Richtlinien 215, 217
 Typen 100
 Windows 8-Optionen 52f.
 Energieverwaltung
 ACPI-Energiezustände 159ff.
 Alarme und Benachrichtigungen 110
 Anzeige 135
 Befehlszeilenoptionen 98ff.
 Benutzerprivilegien 233
 Bildschirmschoner 134
 Energiesparpläne 100–104, 106
 Energiezustände 159ff.
 Gruppenrichtlinieneinstellungen 109
 Kennwortschutz 108
 Notebooks 97
 Problembehandlungsmodule 314
 Updates 358

- Energiezustände 159ff.
 - Energy-Report.html-Datei 99
 - Enhanced Intel SpeedStep Technology (EIST) 160
 - Enterprise-Mode-WPA 630
 - Entfernen
 - Leerlaufzeit und Wählverbindungen 619
 - Netzwerkfreigaben 525
 - Remotezugriffsoptionen 619
 - USB- oder FireWire-Laufwerke 432
 - Verhindern 542
 - Entmagnetisieren, Monitor 147
 - Entschlüsseln, Dateien 425, 489, 491f.
 - Entsiegeln von Schlüsseln 391
 - Entsperren des Computers 424, 549
 - Entspernte Laufwerke 415
 - EPIC (Explicitly Parallel Instruction Computing) 27
 - Erben von Einträgen (BCD-Speicher) 177
 - Ereignisanzeige 62, 368
 - Ereignisdienste (UEFI) 153
 - Ereignisprotokolle 366f., 386
 - Ereignisprotokollese-Gruppe 230
 - Ereignisse 366, 369, 378, 551
 - Erholung/Wiederherstellung nach Verlusten mit SACK-Informationen, Feature 573
 - Erkennen
 - Geräte 324ff.
 - Hardwareänderungen 336, 348
 - IPv6-Adressen 574
 - Erkennung des Übertragungswiederholungs-Timeouts 574
 - Erkennung nicht erreichbarer Nachbarknoten für IPv4 573
 - Ermittlung privater Netzwerkhosts 273
 - Erneuern, DHCP-Einstellungen 592
 - Ersteller-Besitzer, Identität 502
 - Erstes Megabyte, Richtlinie 180
 - Erweitern komprimierter Laufwerke 487
 - Erweitern von Volumes, Assistent 458
 - Erweiterte Attribute 505
 - Erweiterte Bildschirmdarstellung 143
 - Erweiterte Freigabe 518f.
 - Erweiterte Optionen für Windows-Betriebssystemlader 181
 - Erweiterte Ordneroptionen, Richtlinien 215
 - Erweiterte Partitionen oder Volumes 428
 - Basisdatenträger 441, 448
 - Datenträgerverwaltung-Tool 433
 - Dynamische Datenträger 441, 448
 - Einfache und übergreifende Volumes 456
 - Einschränkungen 457
 - Erstellen 452, 457f.
 - Löschen 462
 - MBR-Laufwerke 429
 - Verschieben von Datenträgern in neue Systeme 467
 - Erweiterte selektive Bestätigungen, Feature 573
 - Erweiterte Startoptionen, Menü 168, 376
 - Erweiterte TCP-Statistiken, Feature 574
 - Erweiterte Zwischenspeicherung 547
 - Erweiterter Arbeitsspeicher 437
 - Erweitert-Registerkarte (Systemeigenschaften-Dialogfeld) 84
 - Erweiterung, Aktivierung 285
 - Erweiterungskarten 154
 - Erzwingen
 - Datenträgerkontingente 556f.
 - Einstellungen 214
 - Erzwingen der Treibersignatur deaktivieren 151, 377
 - eSATA-Geräte und -Anschlüsse 53, 444
 - Geräte installieren 326
 - ESP (EFI-Systempartition) 27, 39, 429
 - Ethernet-Protokolle 622
 - Ethernetverbindungen 576–586, 588–594
 - exFAT 430, 442f., 479, 490
 - Explicitly Parallel Instruction Computing (EPIC) 27
 - Explorer-Favoriten-Ordner 119
 - Explorer-Links-Ordner 119
 - Explorershell 120, 376
 - Exportieren
 - BCD-Speichereinträge 173
 - Datenträgerkontingenteinstellungen 561
 - Zeitplan, Aufgaben 370
 - Extended-FAT-Dateisystem (exFAT) 442f., 479, 490
 - Extensible Authentication Protocol (EAP) 621
 - Extensible Firmware Interface *Siehe* EFI
 - Externe Geräte 324, 444, 480, 597
 - Externe IP-Adressen 574
- ## F
- Failed-Registrierungswert 167
 - Fälschen von Anhebungsaufforderungen 276
 - Farben
 - Bildschirm-Farbkalibrierung 146
 - Designs 129
 - Farbtiefe 139, 144
 - Fensterschnittstelle 136ff.
 - Flecken auf Anzeige 146
 - Remotedesktopeinstellungen 265
 - Stärke und Transparenz 137
 - Verschlüsselte oder komprimierte Dateien 540
 - Farbprofile 145
 - FAT, FAT16 und FAT32, Dateisysteme 430, 451
 - BitLocker 404, 415
 - Bits 430
 - Clustergröße 442f.
 - Dateisicherheit und -freigabe 494
 - EFI-Shell 39
 - Konvertieren in NTFS 462
 - Vergleiche 442
 - Verschlüsselung 490
 - Volumebezeichnungen 461
 - Wechseldatenträger 479
 - Favoriten-Menü 119
 - FAX\$-Freigabe 523
 - Federal Information Processing Standard (FIPS) 411, 630
 - Fehler 57, 366
 - Fehler, Laufwerksstatus 464
 - Fehler, Volumestatus 470

- Fehlerberichterstattung 305, 317f.
- Fehlerfrei (Risiko), Volumestatus 470
- Fehlerfrei (Unbekannte Partition), Volumestatus 470
- Fehlermeldungen 386ff., 392, 552
- Fehlerredundanzstatus 477
- Fehlertoleranz (Datenträger und Volumes) 455, 465, 470
- Fehlgeschlagene Dateizugriffe 534
- Fenster (Schnittstelle) 120, 129, 136ff., 540
- Fernsehen 530
- Fest eingebautes Laufwerk, Richtlinien 410
- Festplatten 40, 428, 450, 468
 - Auslagerungsdateien 86
 - Basis und dynamisch 38, 441–450
 - Computer-Konsole 431
 - Datenträgerverwaltung-Tool 433
 - Defragmentieren 475ff.
 - DiskPart-Tool 435
 - Einstufungen 66
 - Fehler während Systemstart 164
 - Fehlererkennung 57
 - Firmwareschnittstelle 155
 - Fremde 469
 - FSUtil-Tool 435
 - Gespiegelte 465ff.
 - GPT-Partitionen 152, 447
 - Gültige Signaturen 469
 - Hardwareverschlüsselung 405, 430
 - Herunterfahren 102
 - Hybride 438
 - Installieren und Initialisieren 446
 - Interne und externe 324
 - Komprimierung 485ff.
 - Konfigurationstools 430–435
 - Kontingente 555–563
 - Konvertieren in NTFS 462
 - Laufwerkbuchstaben und -pfade 459
 - Leere 540
 - Leistung 436–440
 - Logische 452–455
 - Löschen von Volumes oder Partitionen 461
 - MBR und GPT 447
 - Partitionen 428–435, 452–455
 - Partitionstypen oder Volumes 444ff.
 - Problembehandlung 468–479
 - Probleme bei Installation 43
 - Remotedesktopverbindungen 267
 - Reparieren 471–475
 - Startvorgang 154
 - Statusmeldungen 469f.
 - Stripesetvolumes 455
 - Systemstart 161
 - Systemwiederherstellung 95
 - Tools für Formatierung und Partitionierung 452
 - Übergreifende Volumes 455
 - Verbergen 542f.
 - Vergrößern von Volumes 457f.
 - Verhindern des Zugriffs 542
- Festplatten (*Fortsetzung*)
 - Verkleinern von Volumes 457f.
 - Verschieben in neue Systeme 467
 - Verschlüsselung 409f., 488–492
 - Volumestatusmeldungen 470f.
 - Wechseldatenträger *Siehe* Wechseldatenträger
 - Wiederherstellen 378, 464
 - x86- und Itanium-Computer 27
- Festplattenlaufwerke *Siehe* Festplatten, Wechseldatenträger
- Festplattenplatz
 - Abbruchfehler 387
 - Datenträgerkontingentrichtlinien 195ff.
 - Freier Platz und Leistung 67
 - Speichergeräte 433
 - Systemwiederherstellung 95, 197
 - Windows 8, Voraussetzungen 40
- File Transfer Protocol (FTP) 617
- Filtermanager 440
- FIPS (Federal Information Processing Standard) 411, 630
- Firewalls
 - Drahtlosnetzwerke 629
 - Freigaben 528
 - Geräte 330
 - Konfigurieren von Verbindungen 623
 - Mehrere Netzwerke 55
 - Netzwerkerkennung 568
 - Profile 569
 - Remotedesktop, Feature 266
 - Remoteunterstützung 362
 - Richtlinien 202
 - Status 307
- FireWire-Geräte
 - Abziehen 53
 - Aktiv-Status 445
 - Dateisysteme und -formate 479
 - Dynamische Datenträger 444
 - Entfernen 432
 - Installieren 326–329
 - Kein Medium, Laufwerksstatus 469
 - Nicht lesbar, Status 469
 - Versionen 479
- Firmware und Firmwareschnittstellen
 - 64-Bit-Architektur 27
 - Beispiele für Schnittstellen 156–159
 - Energiezustände und Verwaltung 159
 - Fehler während Systemstart 164
 - Firmwareschnittstellenabstraktion 55
 - Kennungen 176
 - Kennwörter 156
 - Konfigurationsdetails 156
 - Konfigurieren von Startoptionen 164
 - Laufzeitdienste 151
 - Manuelle Konfiguration 348
 - Motherboardchipsätze 150
 - Problembehandlung 163
 - Schnittstellentypen 150
 - Startvorgang 155, 162

Firmware und Firmwareschnittstellen *(Fortsetzung)*

- Systemstartdienste 151
- Systemstarteinstellungen 161
- Systemstartprozess 154
- Tastenkombinationen 158
- TCG-kompatibel 390
- TPM-kompatibel 390
- UEFI, Überblick 152ff.
- Update 150, 156
- Versionen 156
- Firmware-Start-Manager 172
- Fixierte Elemente 123
- Fixit-portable-Dienstprogramm 293
- FixMbr 471
- Flashgeräte *Siehe* USB-Speicherstick
- Flashspeicher 163, 438
- Flimmernde Anzeige 147
- Flugzeugmodus 598, 633
- Formatieren
 - Partitionen und Volumes 454, 458
 - Schnellformatierung, Feature 455
 - Speichergeräte 433, 450
 - Statusmeldungen 470
 - Wechseldatenträger 479
- Format-Tool 452
- Fortsetzen, Dienste 320
- Forward-Lookups 593
- Fragmentierung 463
- Freier Festplattenplatz 448, 457
 - Abbruchfehler 387
 - Anzeigen 433
 - Basis- und dynamische Datenträger 448
 - Empfohlene Menge 40
 - Leistungseinstufungen 67
 - Offlinedateien 553
 - Problembehandlung 468
- Freigabeberechtigungen 494, 498, 517
- Freigaben 517–529, 532–535, 542
 - Ausgeblendete 527, 543
 - Überwachen und Verfolgen 532–535
 - Verhindern der Pfadzuordnung 542
- Freigeben, DHCP-Einstellungen 592
- Freigegebene Drucker 215, 332
- Freigegebene Ordner, Problembehandlungsmodule 315
- Freigegebene Ordner-Tool 62
- Fremde Datenträger 469ff.
- FSUtil-Tool 435
- FTP (File Transfer Protocol) 617
- Ftype-Tool 297
- Funktionstasten 425

G

- Gäste-Gruppe 228, 230
- Gastkonten 228, 258
- Gatewaydienst auf Anwendungsebene 229
- Gatewaymetriken 580

Gateways

- Anzeigen 587
- Ausgefallene Gateways 573
- DHCP-Adresse freigeben und erneuern 592
- Drahtlos *Siehe* Drahtlosnetzwerke
- Konfigurieren 580
- Statische IP-Adressen 578
- Geerbte Berechtigungen 500f., 503f., 511–514, 535
- Gehostete Caches 564
- Gemeinsame Nutzung der Internetverbindung, Feature 202
- Gemeinsame Optionen-Registerkarte (Hardware) 222
- Gemeinsame Schlüssel 629
- Generische Anmeldeinformationen 247
- Geplante Aufgabe, Richtlinien 215
- Geplante Aufgaben *Siehe* Aufgabenplanung
- Geplante Offlinedateisynchronisation 549
- Geplante Updates 358
- Geräte *Siehe auch* einzelne Gerätetypen
 - Aktivieren und Deaktivieren 342, 346
 - Ausgeblendete 337
 - Automatisches Hilfesystem 304–323
 - Charm 24
 - Doppelte 349
 - Drahtlos, Netzwerk und Bluetooth 329ff.
 - effektive Berechtigungen bestimmen 515
 - Einschränken der Installation 343
 - Energieinformationen 98
 - Fehlererkennung 57
 - Fehlermeldungsliste 346–349
 - Firmwareschnittstelle 155
 - Gerätetreiber 337–349
 - Interne, USB oder FireWire 326–329
 - Kontoprivilegien 233
 - Legacy 347
 - Löschen von Treibern 345
 - Sicher entfernen 349
 - Systemstamm 181
 - Typen 323
 - Unverwaltete Richtlinieneinstellungen 215, 219
 - Vorhandene installieren 324ff.
- Geräte, Richtlinien 215
- Gerätekategorie-GUIDs 343
- Geräte-Manager 63, 335, 346–349
- Gerätetreiber
 - 32- und 64-Bit-Treiberspeicher 337
 - Abbruchfehler 386
 - Aktivieren oder Deaktivieren 342, 345
 - Automatisches Hilfesystem 304–323
 - Dateiinformationen 338
 - Deinstallieren 345
 - Deinstallieren von Treibern 345
 - Drahtlos, Netzwerk und Bluetooth 329ff.
 - Drucker 331
 - Einschränken der Installation 343
 - Energiesparanforderungen 98
 - Fehlermeldungsliste 346–349
 - Grafikkarte und Monitor 139–142, 146

- Gerätetreiber (*Fortsetzung*)
 - Installieren 324–329, 339–342
 - Interne, USB oder FireWire 326–329
 - Ladefehler, Richtlinien 181
 - Neuinstallation 345
 - Problembehandlung 146, 163, 376
 - Signierte und unsignierte 338
 - Startvorgang 162, 376
 - Suchen 339
 - Systemstartfehler 166
 - Testumgebungen 340
 - Update 328, 339–342
 - Vorhandene Hardware 324ff.
 - Vorversion wiederherstellen 344
 - Wiederherstellungspunkte 379
 - vor Update 328
 - Gesamtstrukturen 191
 - Geschwindigkeit
 - Drahtlosgeräte 628, 633
 - Ethernetverbindungen 586
 - ReadyBoost-Geräte 437
 - Systemstart 168
 - Gesperrte Dateien 513
 - Gesperrte Konten 257
 - Gesperrte Taskleiste 123
 - Gesperrter Computer 549
 - Gespiegelte Datenträger 441, 465f., 470, 477f.
 - Ghosting nicht verfügbarer Dateien 544
 - Globale Debugparameter 173, 176
 - GPOs (Gruppenrichtlinienobjekte) 188
 - Administrative Vorlagen 194
 - Bearbeiten 189, 220
 - Deinstallieren von Elementen 223
 - Fehlerverarbeitung 222
 - Gruppenrichtlinienobjektverknüpfungen und GPOs 191
 - Lokale Gruppenrichtlinien 187–190
 - Standort-, Domänen- und Organisationseinheitengruppenrichtlinien 190ff.
 - Verknüpfungen und Objekte 191
 - GPT (GUID Partition Table) 429
 - EFI 152
 - Itanium-Computer 27
 - UEFI 152
 - Wechseln zu MBR 430, 447
 - GPUs (Graphics Processing Units) 136
 - Grafik (Spiele) 66, 100
 - Grafikchipsätze 156
 - Grafikkarten
 - Bildwiederholrate 145
 - Einstufungen 66
 - Energiesparpläne 100
 - Farbfähigkeiten 144
 - Problembehandlung 146
 - Prüfen der Treiber 139
 - Startvorgang 154
 - Treiber ändern 140ff.
 - Windows 8, Voraussetzungen 39
 - Grafikmodus 167, 180
 - Grafische Verbesserungen 84, 136
 - Graphics Processing Units (GPUs) 136
 - Größe ändern
 - Taskleiste 123
 - Volumes und Partitionen 458
 - Gruppen *Siehe auch* Heimnetzgruppen, Arbeitsgruppen, Domänen
 - Berechtigungszuweisungen 503
 - Computer, Mitgliedschaft 83
 - Features 229ff.
 - Lokale Gruppen 254ff.
 - Löschen 259
 - Mitglieder hinzufügen 256
 - Netzwerkberechtigungen 517
 - Planen von Updates 358
 - SIDs 230
 - Spezielle Berechtigungen 505f.
 - Standardberechtigungen 499–507, 510–516
 - Standardkonten 228
 - Typen 46, 229ff.
 - Umbenennen 259
 - Unverwaltete Richtlinieneinstellungen 215
 - Gruppenkonten *Siehe* Gruppen
 - Gruppenrichtlinien *Siehe auch* Richtlinien, (Unverwaltete) Richtlinieneinstellungen
 - Active Directory-Gruppenrichtlinien 186
 - Bereitstellen von Anwendungen 285
 - Computer- und Benutzerskripts 205–209
 - Gemeinsame Optionen-Registerkarte, Elemente 222
 - Konfigurieren 192–195
 - Konflikte 186
 - Lokale Gruppenrichtlinien 186–190
 - Reihenfolge der Anwendung 186
 - Verarbeitungseinstellungen 221
 - Gruppenrichtlinienergebnis-Assistent 191
 - Gruppenrichtlinienmodellierungs-Assistent 191
 - Gruppenrichtlinienobjekte 283
 - Gruppenrichtlinienobjekt-Editor 188
 - Gruppenrichtlinienverwaltung-Konsole 190f., 193
 - Gruppenrichtlinienverwaltungs-Editor 188f., 191, 193f., 220
 - Gruppenschlüssel 630
 - GUID Partition Table *Siehe* GPT
 - GUIDs (BCD-Speicherkennungen) 174ff.
 - GUIDs (Geräteklassen) 343
 - Gültige Signaturen 469
- ## H
- Hacking, Vorbeugung 390, 402
 - HAL (Hardware Abstraction Layer) 162f., 166, 181, 337
 - Hardware
 - Aktivieren und Deaktivieren 346
 - Drahtlos, Netzwerk und Bluetooth 329ff.
 - Drucker 331–335
 - Einstufungen 66
 - Ereignisprotokolle 366

Hardware (Fortsetzung)

Fehler während Systemstart 164
 Fehlererkennung 57
 Fehlermeldungsliste 346–349
 Geräte-Manager 335
 Gerätetreiber 337–349
 Hilfesystem 304–323
 Konfiguration 83
 Problembehandlung 377
 Systeminformationen 68
 Systemintegritätsberichte 68
 Vor Kurzem geändert oder hinzugefügt 387
 Windows 8, Voraussetzungen 39
 Hardware Abstraction Layer *Siehe* HAL
 Hardware und Geräte, Problembehandlungsmodule 314
 Hardware-Assistent 339
 Hardware-Registerkarte (Systemeigenschaften) 83, 542
 Hardwareupdate-Assistent 336
 Hardwareverschlüsselung 405, 430
 Hart herunterfahren 386
 Hauptbenutzer-Gruppe 230, 275
 Hauptschlüssel 242
 HDMI (High-Definition Multimedia Interface) 142
 Heimnetzgruppen
 Anmelden 48
 Arbeitsgruppen 46
 Dateifreigabe 495
 Gespeicherte Anmeldeinformationen 247
 Informationen 64
 Kennwörter 242
 Lokale Benutzerkonten 238
 UAC 47
 Wiederherstellung, Richtlinien 490
 Heimnetzgruppennetzwerk, Problembehandlungsmodule 314
 Heimnetzwerke 596
 Helpdesks 261ff.
 Herunterfahren 49, 385
 ACPI-Energiezustände 159ff.
 Auslagerungsdateien löschen 87
 Fehler durch Geräte 349
 Hart herunterfahren 386
 Problembehandlung 385
 Skriptrichtlinien 206f.
 Windows 8-Optionen 52f.
 High-Definition Multimedia Interface (HDMI) 142
 Hilfe und Support
 Anpassen 310–317
 Dienste konfigurieren 317
 Neustart-Manager 305
 Problembehandlungsmodule 314ff.
 Probleme erkennen 304
 Supportdienste 317ff.
 Wartungscenterbenachrichtigungen 306–310
 Zuverlässigkeitsberichte 308
 Hintergrund, Anmeldung 210
 Hintergrundbilder, Desktop 101, 127ff.
 Hintergrundprozesse 439f.

Hintergrundsynchronisierung 199f.
 Hinweise, Kennwort 242f.
 Hochleistung Energiesparplan 100
 Hohe Priorität, E/A 439
 HTTP (Hypertext Transfer Protocol) 617
 Hubs (USB) 479
 Human Interface Infrastructure, Unterstützung 153
 Hybrider Ruhezustand 98, 101
 Hypervisor-Debug Einstellungen 179
 Hypervisorparameter 173, 176
 Hypervisorstarttyp 181

I

IA64-Prozessoren (Itanium) 27, 38f., 155, 429
 ICMP (Ping) 187, 496
 Identitätsüberprüfung 621
 IEEE 1394-Geräte *Siehe* FireWire-Geräte
 IEEE 802.11a/b/g/n 628
 IEEE 802.11i 629f.
 IGMPv3 (Internet Group Management Protocol Version 3) 574
 IKE (Internet Key Exchange) 574
 ImageX-Tool 29, 32
 Immer als Admin ausführen, Anwendungen 277
 Importieren von Datenträgerkontingenteinstellungen 561
 Indizierte Dateidaten 541
 Indizierungseinstellungen 67
 INF-Dateien (Setupinformationen) 281, 337
 Infobereich, Benachrichtigungen 124
 Informationsereignisse 366
 Infrastrukturmodus (Drahtlos) 631
 INI-Dateien, Richtlinien 215
 Initialisierung
 Physische Datenträger 446
 Problembehandlung 163
 Protokollierung 181
 Startvorgang 162
 Systemstartfehler 164
 TPM 395f.
 Volumes 470
 Initialisierungsdateien 54
 Installationswiederstellungspunkte 95, 378
 Installieren von Hardware
 Drahtlos, Netzwerk und Bluetooth 329ff.
 Drucker 331–335
 Einschränken mit Gruppenrichtlinien 343
 Gerätetreiber 339–342
 Interne, USB oder FireWire 326–329
 Netzwerkkarten 575, 631
 Netzwerkkomponenten 572–576
 Vorhandene Geräte 324ff.
 Wiederherstellungspunkte 378
 Installieren von Software
 Administratorgenehmigungsmodus, Einstellungen 235
 Alle Benutzer und ausgewählte Benutzer 283
 Anwendungsinstallation 280–284
 AutoPlay 280f.

Installieren von Software (*Fortsetzung*)

- BitLocker 409, 413, 418
- Fehlerbenachrichtigungen 306
- Grafikkartentreiber 141
- Gruppenrichtlinienbereitstellungen 285
- Installieren beim ersten Aufruf 285
- Kompatibilitätsprüfung 282
- Netzwerkkomponenten 572–576
- Privilegien 275
- Probleme 280
- Setupprogramme 281
- TCP/IP 575
- Updates 352ff., 359
- Wiederherstellungspunkte 378

Installieren von Windows 8 28, *siehe auch* Bereitstellung

- Aktivieren 45
- Automatische Installation 31
- Befehlszeile 40
- Installieren 39–43
- Interaktiv und automatisiert 38
- Neuinstallationen und Upgrades 37
- Problembehandlung 43
- Vorbereitungen 38f.
- Vorherige Versionen 74
- Windows PE 29

Installierte Programme (Systemsteuerung) 292

InstallShield 281, 293

Integriertes Diagnosetool 72

Integritätsebene 276

Intel Quick Resume Technology Driver (QRTD) 160

Intel Xeon-Prozessoren 26

Intelligenter Hintergrundübertragungsdienst 228, 318, 563

Intel-Prozessoren, Energieeinstellungen 160

Interaktiv, Identität 502

Interaktive Installation 38, 40–43

Interne IP-Adressen 574

Interne Laufwerke 324, 326–329, 543

Internet

- Installieren von Software 281
- Routing, Richtlinien 604
- Sicherheit 307
- Verbindung, Richtlinien 217
- Verknüpfungen mit Ressourcen 119

Internet Explorer

- Leistungs-Problembehandlungsmodul 314
- Richtlinieneinstellungen 215

Internet Group Management Protocol Version 3 (IGMPv3) 574

Internet Key Exchange (IKE) 574

Internetprovider 605, 608

Internetverbindungen, Problembehandlungsmodul 314

Internetverbindungsfirewall, Feature 202

Interruptanforderungen (IRQs) 68

IP-Adressen

- Alternative 579
- DHCP-Adresse freigeben und erneuern 592
- Drucker 334
- Dynamische IP-Adressen 579

IP-Adressen (*Fortsetzung*)

- Hinzufügen 582
- Interne und externe zuordnen 574
- IPv4- und IPv6-Adressierung 572
- Konfiguration anzeigen 587
- Mobile Computer, Einstellungen 598
- Netzwerkgeräte 330
- Ping 590
- PowerShell-Remoteverwaltung 26
- Private und öffentliche Adressen 574
- Probleme beseitigen 591
- Proxyserver 617
- Prüfen 83
- Statische 576
- VPN-Verbindungen 612

IPC\$-Freigabe 523, 528

Ipconfig-Befehl 588, 593f.

IPSec (IP Security) 564, 574, 603, 622

IPv4 und IPv6 572

- Alternative Adressen 576, 599
- DirectAccess 604
- Drahtlosnetzwerke 633
- Dual-DHCP 574
- Dynamische oder alternative IP-Adressen 579
- Erkennen für Adressen 574
- Installieren 575
- Konfiguration anzeigen 587
- Mobile Computer, Einstellungen 598
- Private IPv4-Adressen 577
- Probleme beseitigen 591
- Statische IP-Adressen 577f.
- Verbindungsstatus prüfen 586
- VPN-Verbindungen 612

IPv6 over IPSec-Protokoll 622

IPv6 over Point-to-Point Protocol (PPPoE), Feature 574

IRQs (Interruptanforderungen) 68

ISA-Interrupts 348

iSCSI, Unterstützung 153

ISO-Dateien 481f.

ISPs (Internetprovider) 605, 608

Itanium-basierte Systeme *Siehe* IA64-Prozessoren (Itanium)

J

Jeder, Identität 502

Jeder-Gruppe 496

JScript 206

K

Kabel 147, 330

Kabelmodems 602

Kacheln 270

Kaltstart 162

Kapseln (TPM) 391

Karten 323, *siehe auch* Grafikkarten, Netzwerkkarten, PCI, Smartcards

- Kein GUI-Start, Option 79, 169
- Kein Medium, Laufwerksstatus 469
- Kennungen (BCD-Speicher) 174, 176f.
- Kennwörter
 - Ändern 50
 - Anmeldeinformationen 249
 - Benutzerkonten 50ff., 228
 - Bildschirmschoner 133
 - BitLocker 410, 416f., 424
 - Breitbandverbindungen 626
 - Dateifreigabe 497
 - Domänen 50
 - Drahtlosnetzwerke 630, 634
 - Firmwareschnittstellen 156
 - Hinweise 242f.
 - Lokale Konten 237, 242
 - Öffentlich-Ordner 531
 - Planen der Administration 409
 - Remoteunterstützung 363
 - Remotezugriff 618
 - Rücksetzdiskette 50, 244
 - Ruhezustand 103, 108
 - TPM 395f., 399, 401
 - Verschlüsselung 621
 - Wählverbindungen 609, 624
 - Wiederherstellen 243
 - Zurücksetzen 51
- Kennwort-ID-Wiederherstellungsschlüssel 425
- Kennwortrücksetz-Assistent 51
- Kennwortrücksetzdiskette 50, 242, 244, 265
- Kerberos-Authentifizierung 246
- Kerberos-Schutz 508
- Kernel 93, 162f., 166, 173, 181
- Kernel Transaction Manager (KTM) 471
- Klassischer Anmeldebildschirm 210, 244
- Kleine Speicherabbilder 93
- Kompatibilität
 - 16-Bit- und MS-DOS-Programme 286
 - Anzeige Probleme 146
 - Application Compatibility Toolkit 277
 - Aufgabenplanung 369
 - Erzwingen 287
 - Fehlermeldungen 348f.
 - Kompatibilitätsdatenbank ausschalten 317
 - Legacy-Anwendungen 275
 - Manuelle Einstellungen 290
 - Programmkompatibilität 317
 - Programmkompatibilitäts-Assistent 282, 287ff.
 - Treiberprobleme 316
 - Virtualisierung 275
 - Webkompatibilitätslisten 355
- Kompatibilitätseinstellungen 282
- Kompatibilitätsprobleme, Richtlinie 317
- Komponenten 69, *siehe auch* einzelne Komponententypen
- Komprimierung
 - Aktivieren 455
 - Dateien und Verzeichnisse 485ff.
 - Komprimierung (*Fortsetzung*)
 - Datei-Explorer, Anzeigeeoptionen 540
 - Erweitern komprimierter Laufwerke 487
 - Remotedesktopsitzungen 267
 - UEFI, Unterstützung 153
 - Verschlüsselung 490
- Konfiguration
 - Aktuelles Betriebssystem, Kennung 176
 - Anwendungsleistung 85
 - Automatisches Hilfesystem 304–323
 - Betriebssysteminformationen 64
 - Computerverwaltung-Konsole 61
 - DEP (Datenausführungsverhinderung) 87
 - Energieverwaltung 97–112
 - Erweiterte Systeminformationen 68
 - Firmware 156–159
 - Geräte-Manager 335
 - Hardware 83
 - Leistungsoptionen 84
 - Letzte als funktionierend bekannte Konfiguration 167
 - Manuelle Jumper- oder Firmwareeinstellungen 348
 - Namen und Adressen von Computern 83
 - Richtlinieneinstellungen 192–195
 - Starten und Wiederherstellen-Dialogfeld, Optionen 168
 - Startoptionen 92
 - System- und Leistungsdaten 64–68
 - System und Umgebungsvariablen 88–91
 - Systemeigenschaften-Dialogfeld 82–97
 - Systemfehler und Debuggen 93
 - Systemkonfigurationsprogramm 76–82
 - Systemsupporttools 60, 72–81
 - Systemwiederherstellungseinstellungen 94–97
 - Virtueller Arbeitsspeicher 85ff.
 - Wiederherstellungsoptionen 93, 378
 - WMI-Steuerung 70ff.
- Konfigurationsflags 181
- Konfigurationsskripts 615
- Konflikte
 - Fehlermeldungen 348
 - Richtlinieneinstellungen 186, 188
- Konfliktlösung (Offlinedateien) 544, 552
- Konnektivitätseinstellungen 202–205
- Konsolenunterstützung (UEFI) 153
- Konten *Siehe auch* einzelne Kontentypen
 - Anmeldeinformationen 246–251
 - Anmeldenamen 227
 - Deinstallieren und Zugriff verweigern 246
 - Gesperrte 257
 - Kennwörter 50ff.
 - Lokale Benutzerkonten 47
 - Pseudokonten 228
 - Serverspeicherte Benutzerprofile 247
 - SIDs (Sicherheits-IDs) 228
 - Willkommenseite 245
- Kontextmenüs 542
- Kontingentgrenzen 195ff., 555–563
- Kontrollkästchen in Datei-Explorer 540f.

- Konvertieren
 - Basis- oder dynamische Datenträger 433, 448ff.
 - FAT-Laufwerke in NTFS 462
 - Kopieren
 - BCD-Speichereinträge 177
 - Befehlspfad 295
 - BitLocker-PINs oder -Schlüssel 424
 - Dateien auf CDs oder DVDs 481
 - Öffentlich-Ordner 495
 - Verschlüsselte Dateien 490
 - Kritisch, Akkualarm 110f.
 - Kritische Updates 352
 - Kritischer Systemfehler 93
 - Kryptografie-Operatoren-Gruppe 230
 - KTM (Kernel Transaction Manager) 471
 - Kurze Dateinamen 286
- L**
- L2TP (Layer 2 Tunneling Protocol) 603, 621
 - LAN 563
 - Lange Dateinamen 286
 - Langsame Verbindungen 199f.
 - Laptops *Siehe* Notebooks und Tablet PCs
 - LastKnownGood-Registrierungswert 167
 - Latenz 602
 - Laufwerkbezeichnungen 450
 - Laufwerkbuchstaben
 - Benutzte oder reservierte 460
 - Datei-Explorer 540
 - Verschobene Datenträger 468
 - Zuordnen zu Freigaben 523, 526
 - Zuweisen 433, 450, 459
 - Laufwerke, virtuelle 482
 - Laufwerkoptimierung 72
 - Laufwerks-E/A-Subsystem 443
 - Laufwerkspfade 433, 450, 459
 - Laufwerkzuordnungen, Richtlinien 215, 217
 - Laufzeitdienste 151, 153
 - Lautstärke 597
 - Layer 2 Tunneling Protocol (L2TP) 603, 621
 - Leases (DHCP) 588
 - Leere Laufwerke 540
 - Leeren von DNS-Caches 593
 - Leerlaufzeit 440, 549, 619
 - Legacy-Anwendungen 274, 286
 - Ausführungsliste 210
 - Legacy-Anwendungen, Ausführungsliste 210
 - Legacy-Betriebssystem, BCD-Speichereinträge 172, 175
 - Legacy-Geräte 347f.
 - Legacy-Skripts 206
 - Leistung
 - Anwendungseinstellungen 85
 - BranchCache 563
 - Darstellung 84
 - Datenprotokollierung 181
 - Einstufungen 64
 - Leistung (*Fortsetzung*)
 - Energiesparpläne 101
 - Fragmentierung 463
 - Leistungsoptionen-Dialogfeld 84
 - Optionen einstellen 84
 - Probleme erkennen 304
 - Problemerkennung 57
 - Speichergeräte 436–440
 - TCP-Statistiken 574
 - Leistungsinformationen und -tools 66ff., 136
 - Leistungsmonitor-Konsole 57
 - Leistungsoptionen-Dialogfeld öffnen 84
 - Leistungsprotokollbenutzer-Gruppe 230
 - Leistung-Tool 63
 - Lesbarkeit anpassen 138
 - Lesen-Berechtigung 500
 - Letzte als funktionierend bekannte Konfiguration 181
 - Linkfavoriten 119
 - Links-Symbolleiste 125
 - Linkverknüpfungen 119f.
 - Livedatesystem, CDs und DVDs 481, 484
 - Lizenz 45
 - LLMNR (Verbindungslokale Multicast-Namensauflösung) 574
 - LMHOSTS-Dateien 583ff.
 - Logische Laufwerke
 - Aktive Partitionen 447
 - Basisdatenträger 441
 - Dateisystemverwaltung 443
 - Datenträgerverwaltung-Tool 433
 - Erstellen 452–455
 - Laufwerkbuchstaben und -pfade 459
 - Liste anzeigen 434
 - Löschen 461
 - Wechseln zwischen Basis- und dynamischen Datenträgern 448
 - Lokale Administratorkonten 234–238
 - Lokale Benutzer und Gruppen, Richtlinien 215
 - Lokale Benutzer und Gruppen-Dienstprogramm
 - Erstellen von lokalen Gruppen 254
 - Hinzufügen und Deinstallieren von Gruppenmitgliedern 256
 - Konten aktivieren oder deaktivieren 257
 - Konten löschen 260
 - Konten umbenennen 259
 - Kontotyp ändern 241
 - Verwalten von Benutzerkonten 226, 251
 - Zugriff 63
 - Lokale Benutzerkonten
 - Administratorgenehmigungsmodus 234–238
 - Aktivieren oder Deaktivieren 257
 - Anmeldenamen 227
 - Deinstallieren und Zugriff verweigern 246
 - Domänenkonten 231
 - Erstellen 238f., 252ff.
 - Features 227ff.
 - Gastkonten 258
 - Kennwörter 242
 - Lokale Anmeldung 237–246
 - Löschen 259

Lokale Benutzerkonten (*Fortsetzung*)

- Optimieren der UAC 234–238
- Remotezugriff 260–267
- Typen 47, 241
- UAC und Anhebung 232–238
- Umbenennen 259
- Lokale Computer 186
- Lokale Drucker 215, 331ff.
- Lokale Gruppen 229, 254ff.
- Lokale Gruppenrichtlinien 186–190, 193
- Lokale Konten *Siehe auch* Lokale Benutzerkonten
 - Anmeldeinformationen 246–251
 - Anmeldung und Begrüßungsbildschirm 244
 - Deinstallieren und Zugriff verweigern 246
 - Domänenanmeldung 231
 - erstellen 238f.
 - Gruppenkonten 251–260
 - Kennwörter 237
 - Lokale Administratorkonten 234–238
 - Lokale Anmeldung 237–246
 - Lokale Benutzerkonten 251–260
 - Löschen 259
 - Remotezugriff 260–267
 - Umbenennen 259
 - Wiederherstellungsagenten 489
- Lokale Sicherheitsautorität 162, 167
- Lokale Sicherheitsrichtlinie-Konsole 237, 258, 405
- LOKALER DIENST-Konto 228, 318
- Lösungen (Wartungscenter) 45, 307, 316
- Lpkset-up-Tool 29

M

- MAC (Computeradresse) 573, 587, 603
- Makewinpmedia-Tool 29
- Managed Network Protocol (MNP) 154
- Managed Network Service Binding Protocol (MNSBP) 154
- Manifestdateien 337
- Manipulationen *Siehe* Hacking, Vorbeugung
- Manuelle Netzwerkverbindungen 614
- Manuelle Synchronisierung 549
- Manuelle Wiederherstellungspunkte 95, 379
- Master Boot Record *Siehe* MBR
- Masterdateitabelle (MFT) 451
- Masterstartcode 429
- Mausgeräte 128, 164
- Mauszeigerdesigns 128
- MBit/s, Übertragungsrate 479
- MBR (Master Boot Record)
 - Absturzabbildpartitionen oder -volumes 445
 - Aktive Partitionen oder Volumes 445
 - Auslagerungsdateipartitionen oder -volumes 445
 - BIOS 152
 - Fehler während Systemstart 166
 - Festplattenfähigkeiten 429
 - Kapazität von Volumes 429
 - Laufwerke in GPT konvertieren 430, 447

MBR (Master Boot Record) (*Fortsetzung*)

- Partitionstypen 429
- Start-, Systempartitionen oder -volumes 445
- x86-Architektur 27
- Zahl der Partitionen 429
- Medien, Unterstützung 153
- Medienstatus von Verbindungen 586
- Medienstreaming 497
- Mehrere Monitore, Unterstützung 143
- Mehrere Prozessoren 79, 348
- Menüs, Löschen 542
- Message Signaled Interrupt (MSI) 181
- MFT (Masterdateitabelle) 451, 463
- Microsoft
 - Absturzabbilddateien senden 387
 - Produktupdates 355
- Microsoft JScript 206
- Microsoft Knowledge Base 368, 387
- Microsoft Office-Temporärdateien 74
- Microsoft Remote Control Incident-Dateien 362
- Microsoft Update 355
- Microsoft Visual Basic Scripting Edition 206
- Microsoft Windows 8 *Siehe* Windows 8
- Microsoft Windows Installer 281, 293
- Microsoft Windows Installer-Dateien (MSI) 285
- Microsoft-Datensicherungstool 379
- Microsoft-Konto 226f., 239, 227
- Microsoft-reservierte Partition (MSR) 39, 429
- Microsoft-Zertifikatdienste 603
- Mikrochips (TPM) 391
- Mklink-Dienstprogramm 44
- MLDv2 (Multicast Listener Discovery Version 2) 574
- MNP (Managed Network Protocol) 154
- MNSBP (Managed Network Service Binding Protocol) 154
- Mobile Computer *Siehe* Notebooks und Tablet PCs
- Mobile Geräte 619, 628
 - Alternative IP-Adressen 599
 - Anmeldung konfigurieren 618
 - Automatische oder manuelle Verbindungen 614
 - Breitbandverbindungen 611
 - Dynamische IP-Adressen 598
 - Flugzeugmodus 598, 633
 - Identitätsüberprüfung 621
 - Netzwerkprojektoren 601
 - Netzwerkprotokolle und Komponenten 621ff.
 - Netzwerkverbindungen 596–602, 614, 624–627
 - Proxysteinstellungen 615–618
 - Remotezugriffsverbindungen 604–613
 - VPN-Verbindungen 612
 - Wahlverbindungen 605–610, 614, 619
 - Windows-Firewall 623
 - Windows-Mobilitätscenter 597
- Mobile Netzwerke *Siehe auch* Notebooks und Tablet PCs
 - Anmeldung konfigurieren 618
 - Automatische oder manuelle Verbindungen 614
 - Breitbandverbindungen 611, 625
 - Drahtlosnetzwerke 634f.

Mobile Netzwerke (*Fortsetzung*)

- Flugzeugmodus 598, 633
- Identitätsüberprüfung 621
- Netzwerkprotokolle und Komponenten 621ff.
- Notebookkonfiguration 596–602
- Proxyeinstellungen 615–618
- Remotedesktop 266
- Remoteunterstützung 362
- Remotezugriffsverbindungen 604–613
- Telefonnummern 620
- Trennung 619
- Typen von Verbindungen 602
- VPN-Verbindungen 612, 626
- Wahlregeln 619
- Wahlverbindungen 602, 605–610, 624f.
- Windows-Firewall 623
- Mobiltelefonmodems 602
- Modempools 602
- Modems 602, 605–608, 611
- Modifizierter schneller Wiederherstellungsalgorithmus 574
- Modularisierung 55
- Monitore *Siehe* Anzeige
- Motherboardchipsätze 150, 154
- MS-CHAP Version 2 621
- MS-DOS 286
- MSI (Message Signaled Interrupt) 181
- MSI-Dateien (Windows Installer) 285
- MSR (Microsoft-reservierte Partition) 39, 429
- MsRcIncident-Dateien 362
- Multicast Listener Discovery Version 2 (MLDv2), Feature 574
- Multimedia-Energieeinstellungen 102

N

- Nachholen von Updates 359
- Named Pipes 528
- Namen
 - Anmeldung 227
 - Computer 83
 - SIDs 228
 - Verknüpfungen 120
- Namensauflösung 496, 581–585, *siehe auch* DHCP, DNS, WINS
- Namespaces 71
- NAT (Network Address Translation) 260, 363
- Net Share-Befehl 517, 527
- NetBIOS-Namen 26, 496, 583ff., 590
- Netcfg-Tool 29
- NETLOGON-Freigabe 523
- Net-Tool 29
- Network Address Translation (NAT) 260, 363
- Netzlaufwerke 433
- Netzschalter 53, 102, 108, 162
- Netzwerk- und Freigabecenter
 - Erstellen von Verbindungen 604
 - Funktionen 568, 571
 - Problembehandlung für Freigaben 529
 - Verbindungsstatus 55
- Netzwerk, Identität 502
- Netzwerkadressprotokolle, Unterstützung 154
- Netzwerkauswertung 55
- Netzwerk-Bridge 202
- Netzwerkd Diagnose 568
- Netzwerkd Diagnose-Framework, Feature 574
- NETZWERKDIENT-Konto 229
- Netzwerkdrucker 331, 333ff.
- Netzwerke
 - Aktive 571
 - Aktivieren der Freigabe 496
 - Analysieren 56
 - Auswertung und Erkennung 55, 568
 - BranchCache 563
 - Dateifreigabe 480, 516
 - Dateiverknüpfungen 119
 - Diagnosetools 56
 - DirectAccess, Feature 56
 - Domänennetzwerke 568
 - Drahtlos *Siehe* Drahtlosnetzwerke
 - Ermittlung privater Netzwerkhosts 273
 - Ethernetverbindungen 576–588
 - Firewallprofile 569
 - Firewalls 307
 - Geschwindigkeit 585–588
 - Heimnetzgruppen 46
 - Komponenten installieren 572–576
 - Latenz 200, 565
 - Mobiler Zugriff *Siehe* Mobile Netzwerke
 - Netzwerk- und Freigabecenter 571
 - Netzwerk-Explorer 570
 - Netzwerkisolation 273
 - Öffentliche Netzwerke 568
 - Offlinedateien 544–555
 - Private Netzwerke 568
 - Problembehandlung 588–594
 - Proxyerkennung 273
 - Remotezugriff 604–613
 - Richtlinien 202–205, 215
 - Sicherheit 273
 - Standorttyp 46
 - Systemstart 161
 - UEFI, Unterstützung 153
 - Verbindungstypen 621ff.
 - VPN-Verbindungen 56, 215
 - Warten bei Systemstart/Anmeldung 210
 - Wechseldatenträgergeräte 480
 - Windows 8-Features und -Tools 568
- Netzwerkerkennung 55, 331, 497, 568, 571, 590
- Netzwerk-Explorer 568, 570, 590
- Netzwerkfreigaben *Siehe* Freigaben
- Netzwerkfreigaben, Richtlinien 215, 217
- Netzwerkkarten 314, 329ff., 572, 575, 587, 628, 631
- Netzwerkkonfigurations-Operatoren-Gruppe 230
- Netzwerkkonsole, Infobereich 124
- Netzwerkprojektoren 596, 601
- Netzwerkprotokolle 153, 621ff.

- Netzwerkschlüssel 631
- Netzwerksymbol 131
- Netzwerkverbindungen
 - Aufbauen 624–627
 - Breitband 611, 625
 - Drahtlos 634f.
 - Flugzeugmodus 598, 633
 - Geschwindigkeit 624
 - Konfiguration 587
 - LAN 576–588
 - Notebooks 596–602
 - Problembehandlung 588–594
 - Remotedesktop 266
 - Remoteunterstützung 362
 - Remotezugriff 604–613
 - Typen 602
 - Umbenennen 588
 - VPN 612, 626
 - Wählverbindungen 605–610, 624f.
 - Zugriffstypen 571
- Netzwerkzugriffsschutzclient 307
- Neu starten 49, 385
- Neue Aufgabe erstellen, Assistent 372
- Neues einfaches Volume, Assistent 452
- Neues gespiegeltes Volume, Assistent 465
- Neuinstallation 37
 - Gerätetreiber 345
- Neustart
 - Abgesicherter Modus und andere Optionen 376
 - Automatische deaktivieren 377
 - Automatischer Neustart 181
 - BitLocker 408
 - Dienste 320f.
 - Nach Updates beschränken 353
 - Verzögern nach Updates 358
- Neustartkonfiguration 93
- Neustart-Manager 305
- Neusynchronisierung, gespiegelte Datenträger 470, 477
- Neuverbinden mit Freigaben 524, 526
- Nicht angewendete Einstellungen 223
- Nicht ausführbarer Arbeitsspeicher 182
- Nicht erkannt, Laufwerksstatus 469
- Nicht erzwungene Datenträgerkontingente 556
- Nicht initialisiert, Laufwerksstatus 469
- Nicht konfiguriert, Gruppenrichtlinienzustand 193f.
- Nicht lesbar, Laufwerksstatus 464, 469, 478
- Nicht synchronisierte Daten 471
- Nicht verfügbare Dateien, Ghosting 544
- Nicht vom Herausgeber verifizierte (unsigned) Anwendungen 276
- Nichtflüchtiger Speicher 163
- Nicht-System-BCD-Speicher 173, 176
- Nicht-System-Volumes 415
- Nicht-Windows-Betriebssysteme 447, 469
- Niedrige Priorität, E/A 439
- NLA (Network Location Awareness) 187
- No-Execute-Schutz (NX), Prozessorfeature 87, 175, 181f., 349

- Normaler Systemstart 77, 169
- Notebooks und Tablet PCs
 - Akkuinformationen 99
 - Deckel, Energieoptionen 102
 - Drahtlosverbindungen *Siehe* Drahtlosnetzwerke
 - Dynamische Datenträger 443
 - Energieversorgungssymbol 100
 - Energieverwaltung 97, 135
 - Firmwarekonfiguration 156
 - Netzwerkzugriffsrichtlinien 203
 - Offlinedateien 544
 - Ruhezustand 52
 - Windows-ReadyDrive 438
- NTFS-Dateisystem 430, 451
 - Berechtigungen 504–507, 514
 - BitLocker 404, 415
 - Clustergröße 442f.
 - Dateibesitz 510
 - Dateisicherheit und -freigabe 494
 - Datenträgerkontingente 195, 555–563
 - Konvertieren von FAT-Laufwerken 462
 - Selbstheilendes NTFS 471
 - Standardberechtigungen 499–502
 - Transaktionales NTFS 471
 - Verschlüsselung 490
 - Versionen von NTFS 451
 - Volumebezeichnungen 461
 - Wechseldatenträger 479
- Ntldr (Windows-Legacybetriebssystem-Ladeprogramm)
 - Ältere Windows-Versionen starten 172
 - BCD-Speichereinträge 175, 179
 - Kennungen 176
 - Startvorgang 155
 - Windows 8 60
- NTLM-Authentifizierung 246
- NX (No-Execute-Schutz), Prozessorfeature 87, 175, 181f., 349

O

- OEM-Partitionen 429
- Öffentliche Netzwerke 529, 568
- Öffentliche Schlüssel 228, 488
- Öffentlich-Ordner 494, 497f., 516, 530f.
- Offline, Laufwerksstatus 464, 469
- Offlinedateien und -ordner
 - Aufräumen 74
 - Benutzen 548
 - Dateifreigabe 521
 - Funktionen und Prozesse 544–555
 - Offlinedateirichtlinien 198–202
 - permanente Offlineverwendung 525
 - Synchronisierung 200, 544, 548–553
- Oktette 573
- Online, Laufwerksstatus 469
- Online (Fehler), Laufwerksstatus 464, 469, 477
- Onlinecrashanalyse, Feature 387
- Optionale Updates 352

Ordner

- Anordnen auf Bildschirm 129
 - Anzeigen des Inhalts verhindern 544
 - Attribute 505
 - Bei Installation erstellte 44
 - Besitz 510
 - Datei-Explorer, Konfiguration 538–544
 - Deinstallierte Programme, Überreste 293
 - Desktopspeicherort 129
 - Erweitern komprimierter 487
 - Freigabe in öffentlichen Ordnern 494
 - Ghosting 544
 - Komprimieren 486
 - Netzwerkberechtigungen 516
 - NTFS-Berechtigungen 499–507, 510–516
 - Offline *Siehe* Offlinedateien und Ordner
 - Spezielle Berechtigungen 507
 - Standardordnerfreigabe 494
 - Symbolische Links 44
 - Symbolleisten 126
 - Unverwaltete Richtlinieneinstellungen 215, 217
 - Verknüpfungen 119
 - Verschlüsselung 488–492
 - Wiederherstellen von Vorgängerversionen 373
- Ordner, Richtlinien 215, 217
- Ordneroptionen, Dialogfeld 538
- Ordneroptionen, Richtlinien 215
- Organisationseinheiten (OUs) 186, 190–193, 195–202
- Originaleinstellung wiederherstellen 374
- Oscdimg-Tool 29
- Osloader-Eintrag 172, 177
- OUs *Siehe* Organisationseinheiten (OUs)

P

- PAE-Modus (Physical Address Extension) 87, 178, 181f.
- Papierkorb 74, 131, 542
- Parallelanschluss 331
- Partitionen
- Absturzabbilder 445
 - Aktive oder Startpartition 166, 445, 447
 - Auslagerungsdateipartitionen 445
 - Basis- und dynamische Datenträger 448
 - Bezeichnungen 455, 461
 - BitLocker 409, 412
 - Datenträgerverwaltung-Tool 433
 - Erstellen 452–455
 - Formatieren 454, 458
 - Funktionen 428–435
 - IA64-Computer 39
 - Laufwerkbuchstaben und -pfade 459
 - Löschen 443, 461
 - MBR und GPT 429, 447
 - Nicht erkannt 470
 - Partitionsarten 429
 - Partitionsstil 429
 - Probleme während Installation 43

Partitionen (*Fortsetzung*)

- Standardstartpartitionen 79
 - System 445
 - Typen 38, 428–435
 - Wiederherstellen 464
- Partitionsstil 429
- PATH-Variable 295f.
- Payloads 354
- PC auffrischen 374
- PC Card-Netzwerkarten 572, 628, 631
- PCA (Programmkompatibilitäts-Assistent) 146, 282, 287ff., 317
- PC-Einstellungen
- Anpassen-Seite 114
 - Benachrichtigungen-Seite 116
 - Benutzer-Seite 116
 - Datenschutz-Seite 116
 - Einstellungen synchronisieren-Seite 117
 - Öffnen 24, 114
 - optimieren 114
 - Sperrbildschirm 114
 - Suche-Seite 116
 - Teilen-Seite 116
- PCI (Peripheral Component Interconnect) 79, 153, 160, 170, 182, 348, 628, 631
- PCI Express 103
- PCI-Energieverwaltung, Aufwacherereignisse 160
- Peer Name Resolution-Protokoll (PNRP) 362
- Peripheral Component Interconnect *Siehe* PCI, PCI Express
- Permanente Offlineverwendung 525
- Personalisierung 66, 128, 130, 136
- Personal-Mode-WPA 630
- Persönliche Bibliotheken 44
- Persönliche Daten 381, 385
- Persönliche Ordner 44
- Pfade
- BCD-Eigenschaften 175
 - Datei-Explorer 540
 - Laufwerkspfade 433, 450, 459
 - Umgebungsvariablen 522
- Phoenix SecureCore 156–159
- Physical Address Extension *Siehe* PAE-Modus
- Physische Angriffe 390–402, 407
- Physische Arbeitsspeicheradressen 180
- Physische Datenträger 434, 441, 443, 446
- PIN 403, 409ff., 415, 421f., 424
- Ping (ICMP) 187, 577, 590
- Pixel 144
- Planen
- BitLocker-Bereitstellungen 408
 - Dateiberechtigungen 503
 - Sicherheitsadministration 409
- Platzhalter bei Namensauflösung 593
- Plug & Play-Geräte 68
- PnP-Geräte 68
- PNRP (Peer Name Resolution-Protokoll) 362
- Point Of Presence (POP) 608
- Point-and-Print-Treiberupdates 355

- Point-to-Point Protocol (PPP) 622
- Point-to-Point Tunneling Protocol (PPTP) 603, 621
- POP (Point Of Presence) 608
- Ports
 - Dateifreigabe und offene Ports 496
 - Debugports 179
 - Druckerkonfiguration 331
 - EMS-Ports 179
 - Geräte 324
 - HTTP, SSL, FTP oder Socks 617
 - Netzwerkfreigaben 528
 - Proxyserver 617
 - Remoteunterstützung 361
 - Zuordnen 574
- POST (Power-On Self Test) 162f.
- PPP (Point-to-Point Protocol) 622
- PPPoE (PPP over Ethernet) 574, 611, 622
- PPPoE (IPv6 over Point-to-Point Protocol) 574
- PPTP (Point-to-Point Tunneling Protocol) 603, 621
- Präsentationseinstellungen 597, 601
- Preboot Execution Environment (PXE) 153
- Primäre Computer 232
- Primäre Partitionen 428f., 441, 445, 447f., 452
- Primäres DNS-Suffix 83
- PRINT\$-Freigabe 523, 528
- Prinzip der geringstmöglichen Rechte 503
- Priorität von Anwendungen 440
- Private IPv4-Adressen 577, 599
- Private Kernel 181
- Private Netzwerke 568, *siehe auch* VPN-Verbindungen
- Private Schlüssel 228
- Privater Debuggertransport 181
- Privilegien 186, 233, *siehe auch* Berechtigungen
- ProactiveScan 472
- Problematische Geräte 69
- Problemaufzeichnung 260
- Problembehandlung
 - Abbruchfehler 386ff.
 - Anzeige und Grafikkarten 146
 - Anzeigeauflösung 139
 - Aufgabenplanung 372
 - Automatische Reparatur 375
 - bei der Programmkompatibilität 287
 - Benutzerspezifische Einstellungen 313
 - Berechtigungen 514
 - BitLocker 423–426
 - Bluetooth 329
 - Breitbandverbindungen 626
 - Brennen von Dateien 484
 - Dateifreigabe 528f.
 - Dateiversionsverlauf 381–384
 - Datenträgerfehler 471–475
 - Dienste 81
 - Drahtlosgeräte 329
 - Drahtlosverbindungen 633, 635
 - Druckerverbindungen 334
 - Energieproblemberichte 98
 - Problembehandlung (*Fortsetzung*)
 - Ereignisprotokolle 366
 - fehlgeschlagener Start 374
 - Festplattenlaufwerke 468–479
 - Gerätetreiber 344
 - Gespiegelte Datenträger 466, 478
 - Gruppenrichtlinien 316f.
 - Herunterfahren 385
 - Installation 43
 - Integrierte Tools 55, 314ff.
 - Kompatibilitätsprobleme 287ff.
 - Laufwerkbuchstaben oder -pfade 460
 - Microsoft Knowledge Base 368
 - Netzwerkverbindungen 56, 330, 574, 588–594
 - Originaleinstellung wiederherstellen 374
 - Partitionen 448
 - PC aufrischen 374
 - Problemaufzeichnung 260
 - ReadyBoost 437
 - Remoteunterstützung 261ff., 361–365
 - Ruhezustand 52, 99, 375
 - Sichern und Wiederherstellen 373, 381ff., 464
 - Starteinstellungen 375
 - Startprobleme 385
 - Startprozess 79, 169, 478
 - SuperFetch 440
 - System wiederherstellen 374
 - Systemimage-Wiederherstellung 374
 - Systemintegritätsberichte 68
 - Systemstart 163–168, 375ff., 385
 - Systemwiederherstellung 377–381
 - TPM 392
 - Updates 360
 - Volumestatusmeldungen 470f.
 - VPN-Verbindungen 627
 - Wahlverbindungen 624
 - Wartungscenter 45f., 307
 - Windows 8-Fehler 366ff.
 - Windows PE 29
 - Windows-Tools 315
 - Problembehandlungsmodule 314ff.
 - Problemberichte und -lösungen, Feature 318, 346, 366
 - Problemberichterstattung 311
 - Profilbild 116
 - Programm zur Verbesserung der Benutzerfreundlichkeit 316
 - Programme-Menü 119
 - Programme-Ordner 119, 284, 293
 - Programmkompatibilität, Problembehandlungsmodule 314
 - Programmkompatibilitäts-Assistent 305, *siehe auch* PCA
 - Projektoren 596, 601
- Protokolle
 - Dateifreigabeaktivitäten 532–535
 - Datenträgerkontingenteinträge 558
 - Dienste 318
 - Kontingentgrenzen 195, 197
 - Leistungsdaten 181
 - Problembehandlung 366

Protokolle (*Fortsetzung*)

- Remoteunterstützungssitzungen 263
- Startprotokolle 79
- Systemfehler 93
- Überprüfte Dateisignaturen 76
- Warnstufen 366
- WMI-Fehler 71
- Proxyerkennung 273
- Proxyservereinstellungen 615–618
- Prozesse
 - Ereignisprotokolle 366
 - Neue Fenster 540
 - SuperFetch-Dienstprogramm 439f.

Prozessoren

- APIC-Cluster 181
- Bildschirmschoner 134
- Einstufungen 66
- Energieoptionen 103
- Firmwarekonfiguration 156
- Firmwareschnittstelle 155
- Informationen 64
- Mehrere 181
- Startoptionen 79
- Startvorgang 154
- Windows 8, Voraussetzungen 39
- Zahl 170, 181

Prozessorzeitplanung 85

Pseudokonten 228

PXE (Preboot Execution Environment) 153

Q

- QRTD (Intel Quick Resume Technology Driver) 160
- Quelldateien (SYS) 337
- Quellen in Ereignisprotokollen 366
- Quick-Resume-Modus 161
- Quick-Sleep-Modus 161

R

RAID-Controller 442

RAM

- Abbruchfehler 387
- Fehler 176
- Hinzufügen 324
- Hybride Laufwerke 438
- Optionen 176
- Virtueller Arbeitsspeicher 85
- Windows 8, Voraussetzungen 39

RDP-Dateien 265

ReadyBoost 436ff.

Reaktionsgeschwindigkeit 68, 85, 602

Reaktivieren, gespiegelte Datenträger 477

Recent-Ordner 119

Rechte Maustaste, Menüs 542

ReFS (Resilient File System) 430

Regionale Einstellungen, Richtlinien 215, 217

Regionseinstellungen (Telefon) 605, 607

Registrieren von DNS-Adressen 583, 593

Registrierung 193, 210, 215f., 275, 279, 298, 347f.
aufräumen mit Fixit 293

Registrierungs-Editor 344

Registrierungsrichtlinien 215ff.

Registrierungsstrukturen 162, 166

Reichweite von Drahtlosgeräten 628

Remotecomputer

- Aufgabenplanung 368
- BitLocker 408
- Computerverwaltung-Konsole 63
- Datenträgerkontingente 556
- Energieplankonfiguration 100
- Geräte konfigurieren 335
- PowerShell-Verwaltung 26
- Systeminformationen 69
- Window-Firewall-Ausnahmen 64

Remotedesktop, Feature 64, 260, 263–266

Remotedesktopbenutzer-Gruppe 230

Remotedesktopdienste 229

Remotedienstverwaltung 64

Remote-Ereignisprotokollverwaltung 64

Remoteprozeduraufruf (RPC) 229

Remoteserver-Verwaltungstools (RSAT) 190

Remoteunterstützung anbieten-Tool 72, 365

Remoteunterstützung, Feature 72, 260

Chat-Fenster 364f.

Deaktivieren 205

Einladungen 204, 361, 363ff.

Funktionen und Features 361ff.

Hilfe anbieten 365

Konfigurieren 261ff.

Problemaufzeichnung 260

Richtlinieneinstellungen 204

Remoteunterstützungsanbieter-Gruppe 361

Remoteverwaltung geplanter Aufgaben 64

Remoteverwaltungsbenutzer-Gruppe 230

Remotevolumeverwaltung 64

Remotenzugriff

- Anmeldung konfigurieren 618
- Aufbauen von Verbindungen 624–627
- Automatische oder manuelle Verbindungen 614
- Berechtigungen 498
- Breitbandverbindungen 611
- Dateifreigabeeinstellungen 520ff.
- Drahtlos *Siehe* Drahtlosnetzwerke
- Identitätsüberprüfung 621
- Protokolle und Komponenten 621ff.
- Proxysteinstellungen 615–618
- Remoteunterstützungsrichtlinien 204
- Richtlinieneinstellungen 203
- Telefonnummern 620
- Verbindungstypen 602
- VPN-Verbindungen 612
- Wählverbindungen 605–610, 619
- Windows-Firewall 623

- Reparieren
 - Anwendungen 292
 - Computer 376
 - Datenträgerfehler 471–475
 - Gespiegelte Datenträger 477f.
 - Replikations-Operator-Gruppe 231
 - Repositories (WMI-Statistiken) 71
 - Reservestromalarm 110, 112
 - Reservierte Laufwerkbuchstaben 460
 - Ressourcenmonitor 68
 - Ressourcenverbrauch 347
 - Ressourcenzuweisung 337, 347
 - Resume (Windows Resume Loader) 172, 177
 - Reverse-Lookups 593
 - Richtlinien *Siehe auch* Gruppenrichtlinien, (Unverwaltete) Richtlinieneneinstellungen
 - Anmeldung 209ff.
 - Anwendungssteuerung 280
 - Autostartanwendungen 122
 - Befehlspfade 296
 - Benutzerkonten 252f.
 - BitLocker 404, 409, 411, 413
 - BranchCache 565
 - Datei- und Datenverwaltung 195–202
 - Datei-Explorer 541ff.
 - Dateifreigabe 497, 522, 532
 - Dateityp und Zuordnungen 298
 - Datenträgerkontingente 556
 - Dienste 219, 322
 - DirectAccess 604
 - Domänen 190ff.
 - Drucker 334
 - Energiesparplan 106f.
 - Energieverwaltung 109
 - Funktionstasten 219
 - Gemeinsame Optionen-Registerkarte, Anzeige 222
 - Geräte 219, 342f.
 - Gerätetreiber 339
 - Gruppen 255f.
 - Konnektivität 202–205
 - Konten 258ff.
 - Lokale Drucker 332
 - Netzwerkübersicht 525
 - Nicht signierte Treiber 338
 - Offlinedateien 549
 - Ordneransichten 541ff.
 - Organisationseinheiten 190ff.
 - Problembehandlung und Diagnose 316f.
 - Remotedesktop 265
 - Remoteunterstützung 263
 - Sites 190ff.
 - Skripts 205–209
 - Softwareeinschränkungen 280
 - Systemstart 209ff.
 - Tasks 219
 - TPM 411
 - UAC-Anwendung 279
 - Richtlinien (*Fortsetzung*)
 - Umgebungsvariablen 90
 - Updates 353, 357ff.
 - Verschlüsselung 488
 - VPN-Verbindungen 613
 - Wählverbindungen 610
 - Zugriff 202–205
 - Richtlinien für Softwareeinschränkung *Siehe* Anwendungssteuerungsrichtlinien
 - Richtlinieneinstellungen
 - Aktivierte 193f.
 - Anwendungsreihenfolge 186
 - Deaktivierte Einstellungen 193f.
 - Konfiguration 192–195
 - Konflikte 186, 188
 - Lokale Einstellungen 187–190
 - Nicht konfiguriert 193f.
 - Robust Security Network (RSN) 631
 - Rotierender Verschlüsselungsschlüssel 630
 - Router 573, 580, 611
 - Routing, Richtlinien 604
 - Routingfächer, Feature 574
 - Routingkosten 580
 - Routingtabellen 574
 - RPC (Remote Procedure Call) 229
 - RSAT (Remoteserver-Verwaltungstools) 190
 - RSA-Verschlüsselung mit öffentlichem Schlüssel 488
 - RSN (Robust Security Network) 631
 - Ruhezustand 98, 101, 159ff., 178, 358, 375
 - ACPI-Energiezustände 159ff.
 - Einstellungen 102
 - Hybrider Ruhezustand 98, 101
 - Kennwörter 103
 - Planung 101
 - Problembehandlung 375
 - Typen 98
 - Windows 8-Optionen 52f.
- ## S
- S0–S5, Energiezustände 159ff.
 - SACKs (selektive Bestätigungen) 573
 - SAL (System Abstraction Layer) 153
 - Scheduled Defrag 475
 - Schnelle Benutzerumschaltung 49
 - Schnellformatierung, Feature 455
 - Schnellstartleiste 123
 - Schnittstellen, Firmware *Siehe* Firmware und Firmwareschnittstellen
 - Schreibgeschützte Dateien 490
 - Schreibzugriff 410f., 500
 - Schriftarten 138, 233
 - Schtasks-Tool 368
 - Schutz des Antischadsoftware-Frühstarts deaktivieren 377
 - SCSI, Unterstützung 153
 - SD-Karten (Secure Digital) 436
 - Secure Digital-Karten (SD) 436

- Secure Sockets Layer (SSL) 488
- Sehnschwäche 137
- Seitenrahmennummern (Arbeitsspeicher) 180
- Selbstheilendes NTFS 471
- Selektive Bestätigungen *Siehe* SACKs
- Sendefrequenz (Drahtlos) 628
- Senden an-Menü 119
- Senden von Informationen an Microsoft 308, 317
- SendTo-Ordner 119
- Serial Line Internet Protocol (SLIP) 622
- SERIAL-Debug Einstellungen 179f.
- Serielle Schnittstellen 180, 267, 331
- Server 563, 592, 602
- Server Message Block (SMB) 496, 516
- Servergespeicherte Benutzerprofile 247, 488
- Service Packs 282, 337, 352
- Setupinformationsdateien (INF) 337
- Setuppakete 281, 292
- SHA1-Hashing 488
- SHA1-Thumbprints 265
- Shellerweiterungen 542
- Shellobjekt-Verknüpfungen 120
- Sicherer Desktop 234f.
- Sicherer Start 406
- Sicheres Entfernen, Anwendung 349
- Sicherheit 232–238
 - Administratorgenehmigungsmodus 236
 - Anwendungszugriffstoken 274
 - Benutzer- und Gruppenkonten 226–229, 251–260
 - BitLocker 402–405, 408–412
 - Dateibesitz 510
 - Dateifreigabe 494–507, 510–529, 532–535
 - Deaktivieren von Diensten 322
 - Domäneneinstellungen 237
 - Drahtlosnetzwerke 629ff.
 - Gastkonten 258
 - Geplante Aufgaben 372
 - Gespeicherte Anmeldeinformationen 246–251
 - IEEE 802.11i 629
 - Internet Explorer, Problembehandlungsmodule 314
 - Internetrouting, Richtlinien 604
 - Kerberos-Schutz 508
 - Lokale Anmeldung 237–246
 - Netzwerke 273
 - Öffentlich-Ordner 530f.
 - Prinzip der geringstmöglichen Rechte 503
 - Remotedesktop 263–266
 - Remoteunterstützung 261
 - Remotenzugriff 260–267, 621
 - Signierte und unsignierte Anwendungen 276
 - TPM-Funktionen 390–401, 407
 - Unverwaltete Richtlinienereinstellungen 223
 - Wartungcenter 45f., 307
 - Windows Update 352
 - Windows-Protokolle 366
 - WMI-Steuerung 71
 - Zugang zu Windows Store steuern 271f.
- Sicherheit-Registerkarte (Eigenschaftendialogfeld) 542
- Sicherheitsgruppen 229
- Sicherheitsschlüssel 634
- Sicherheitsupdates 352
- Sichern und Wiederherstellen 373, 381, 385
- Sicherungs-Operatoren-Gruppe 231, 510
- Sichtbare Skripts 207
- SIDs (Sicherheits-IDs) 228, 230, 259, 557
- Signalstärke 632
- Signaturprüfung 75
- Signierte Anwendungen 237, 276
- Signierte Gerätetreiber 338, 379
- Simple Network Protocol (SNP) 153
- Sitzungs-Manager 162f., 167
- Sitzungsschlüssel 630
- Skripts
 - Bereitstellungsskripts 32
 - Computer- und Benutzerrichtlinien 205–209
 - DiskPart-Tool 435
 - Lesen-Berechtigung 500
 - Löschen 208
 - Proxyservereinstellungen 615
 - Richtlinientypen 205
 - Typen 206
 - Zuweisen 208
- SLIP (Serial Line Internet Protocol) 622
- Smartcards
 - Administration 409
 - Benutzerkonten 228
 - Drahtlosverbindungen 631
 - Verschlüsselung 410, 416, 418, 424, 621
 - Wahlverbindungen 609
 - Zertifikate 403
- SmartScreen anpassen 312
- SMB (Server Message Block) 496, 516, 564
 - Verschlüsselung 516
- SMBIOS (Dienste für System Management BIOS) 152
- SNP (Simple Network Protocol) 153
- SoC (System on Chip) 150
- Socks-Protokoll 617
- Sofortige Updateinstallation 358
- Software *Siehe* Anwendungen, Installieren von Software
- Softwareaktualisierung, Assistent 142, 339f.
- Software-Dienstprogramm 300
- Sortieren, Dateien mit Tastenkombination 538
- Sound 111, 127f., 597
- Sound abspielen, Problembehandlungsmodule 314
- Spanning *Siehe* Übergreifende Volumes
- SpeedStep 160
- Speichergeräte *Siehe auch* Festplatten, Wechseldatenträger
 - Basis und dynamisch 448ff.
 - CD- und DVD-Geräte 481–485
 - Computer-Konsole 431
 - Dateisysteme 450
 - Datenträgerverwaltung-Tool 433
 - Defragmentieren 475ff.
 - DiskPart-Tool 435

- Speichergeräte (*Fortsetzung*)
 - Firmwarekonfiguration 156
 - Formatieren 450, 452
 - FSUtil-Tool 435
 - Gespiegelte Datenträger 465ff.
 - Hybride Laufwerke 438
 - Installieren und Initialisieren 446
 - Komprimierung 485ff.
 - Kontingente 555–563
 - Laufwerkbuchstaben und -pfade 459
 - Leistung 436–440
 - MBR und GPT 447
 - Partitionen oder Volumes 444ff., 452–455
 - Problembehandlung 468–479
 - Statusmeldungen 469f.
 - Stripesetvolumes 455
 - Übergreifende Volumes 455
 - Vergrößern oder Verkleinern von Volumes 457f.
 - Verschlüsselung 488–492
- Speichern
 - BranchCache 564
 - Designs 128
- Speicherorte
 - Benutzer 502
 - Verknüpfungen 120
- Sperrbildschirm 244
 - Anpassen 114
 - Einstellen 244
 - Statusinformationen 115
- Sperrbildschirm-Apps 115
- Spezialidentitäten 502ff., 516
- Spezielle Berechtigungen 505
- Spezielle Freigaben 527
- Spiegelung, BCD-Einträge 173
- SRK (Storage Root Key) 391
- SSIDs (Netzwerkennungen) 634
- SSL (Secure Sockets Layer) 488, 617
- Staging-Dateien 71
- Stammordner 511
- Standardanwendungen 293
- Standardanwendungsmodus 233
- Standardaufgaben 369
- Standardbenutzeranwendungen 274
- Standardbenutzerkonten 47, 232ff., 236
- Standardbenutzermodus 233
- Standardbenutzer-Zugriffstoken 274
- Standardberechtigungen 499–504
- Standardbetriebssystem, Eintrag 183
- Standarddesktop 234
- Standardfreigabe 518
- Standardgateways 578, 580, 587, 592, 600
- Standardordnerfreigabe 494, 498, 516
- Standardstartpartition 79
- Standardstarttimeouts 184
- Standbymodus 160
- Standorte, Wählverbindungen 605, 607
- Standortrichtlinien 186, 190–193, 195–202
- Start, Charm 24
- Startablauf temporär ändern 184
- Startanwendungen 180
- Start-Bildschirm 23, *siehe auch* Startseite
 - Kacheln 270
 - Verwaltungsprogramme hinzufügen 61
- Starteinstellungen 375
- Starten, Dienste 320
- Starten und Wiederherstellen-Dialogfeld 91ff., 168
- Start-Kacheln 270
- Startkonfigurationsdatenspeicher *Siehe* BCD-Editor/-Speicher
- Startladeprogramm 162f., 166
- Start-Manager
 - BCD-Editor-Befehle 172f.
 - BCD-Speichereinstellungen 151
 - Fehler während Systemstart 166
 - Problembehandlung 163
 - Reihenfolge 183
 - Startvorgang 162
 - TPM-Versiegelung 391
- Startmenü, Verknüpfungen 119
- Start-Menü 23
- StartMenu-Ordner 119
- Startpartitionen 38, 166, 412, 445
- Startprotokollierung 167, 169, 181, 377
- Startreihenfolge 155, 161, 164, 172f.
- Startschlüssel 403, 409, 415, 421, 424
- Startseite anpassen 116, *siehe auch* Start-Bildschirm
- Startsektoren 471
- Startumgebung 54, 151
- Startvolumes 445, 478
- Statische IP-Adressen 576ff., 584, 591, 596, 623, 633
- Statusmeldungen 618
- Stern (*) 593, 617
- Storage Root Key (SRK) 391
- Störungen bei Drahtlosnetzwerken 635
- Streaming, Medien 497
- Stripesetvolumes 63, 441, 449, 455, 461, 464, 467
- Subnetze 330, 578, 592
- Subnetzmasken 577, 587, 600
- Suche und Indizierung, Problembehandlungsmodule 315
- Suchen
 - Befehlspfadreihenfolge 295
 - Dateiverknüpfung, Reihenfolge 297
 - Gerätetreiber 339
 - Indizierte Dateidaten 541
- Suchen, Charm 24
- Suche-Seite 116
- Suchfeld 24
- Suchleiste 24
- Suchserver festlegen, Windows Update 352
- SuperFetch-Dienstprogramm 439f.
- Supervisor 156
- Support *Siehe* Hilfe und Support
- Supportdienste, Liste 317ff.
- Switchback 283

Symbole

- Anpassen 131
- Anzeige konfigurieren 541
- Datei-Explorer, Auswahl 539
- Dateiverknüpfungen 297
- Designs 127
- Hinzufügen 132
- Infobereich 124
- Löschen 132
- Verbergen 132
- Verknüpfungen 120
- Symbolische Links 44
- Symbolleisten 125f.
- Symmetrische Netzwerkadressenübersetzung, Feature 574
- Synchronisierte Konten *Siehe* Microsoft-Konto
- Synchronisierungszentrum und Synchronisierung
 - Auflösen von Konflikten 552
 - Automatische Synchronisierung 549ff.
 - Berechtigungen 500
 - Details, Fehler und Benachrichtigungen 552
 - Festplattenplatzeinstellungen 553
 - Hintergrund 200
 - Konfigurieren von Richtlinien 199
 - Manuelle Synchronisierung 549
 - Notebookeinstellungen 597
 - Offlinedateien 544
 - Synchronisierungspartnerschaften 548
 - Verschlüsseln von Dateien 554
 - Verwalten der Synchronisierung 545
- Synchronisierungszeitplan 550
- SYS-Dateien (Quelldateien) 337
- System Abstraction Layer (SAL) 153
- System on Chip (SoC) 150
- System wiederherstellen 374
- Systemanwendungen 277
- System-BCD-Speicher 173
- Systemcache 436
- Systemdateien
 - Abbruchfehler 387
 - Anzeigen 538
 - Problembehandlung Systemstart 375ff.
 - Signaturprüfung 75
 - Verschlüsselung 490
- Systemdatenquellen, Richtlinien 215
- Systemdienste 162
- SystemDrive-Umgebungsvariable 44
- Systemeigenschaften-Dialogfeld 65, 83f., 94–97, 379
- Systemfreigaben 523
- Systemimage-Wiederherstellung 374
- Systeminformationen 68
- Systemkomponenten 366
- Systemkonfiguration 73, 77–81, 169ff.
- Systemkonsole 64ff.
- SYSTEM-Konto 228, 318, 320, 368
- Systemmonitorbenutzer-Gruppe 230
- Systempartitionen 38, 445, 463

Systemprüfungspunkte 95, 378

Systemstamm 181f.

Systemstart

- Ablauf 162
- Anwendungen *Siehe* Autostartanwendungen
- Automatischer Neustart 93
- Autostartanwendungen 80
- Beschleunigen 168
- Dienste 81, 320
- Dual-Boot 415
- Elemente laden 78
- Energiezustände und Verwaltung 159
- Firmwareschnittstellen 155
- Firmwarestarteinstellungen 161
- Gespiegelte Laufwerksprobleme 478
- Konfigurieren 92, 169ff.
- Medien 43
- Modi 77, 151, 168
- Problembehandlung 77, 163–168, 180, 375ff., 385
- Richtlinien 209ff.
- Skriptrichtlinien 206f.
- Startvorgang 154, 162
- Systemstartprozess 154
- Tastenkombinationen 151
- Typen 169
- Unverwaltete Richtlinieneinstellungen 122
- Systemstartablauf *Siehe* Startreihenfolge
- Systemstartdebugger 180
- Systemstartdienste 151, 153
- Systemstartkonfiguration
 - Angaben beim Systemstart 78
 - BCD-Editor 171ff.
 - BCD-Speicherverwaltung 173–176
 - Mehrere Betriebssysteme 92
 - Optionen 164
 - Starten und Wiederherstellen-Dialogfeld 168
 - Startoptionen 78ff.
 - Verwalten 169ff.
- Systemstartreparaturtool (StR) 375ff., 448
- Systemstartstatus, Richtlinie 181
- Systemsteuerung 24f.
- Systemsteuerungseinstellungen, Richtlinien 214
- Systemstruktur 349
- Systemsupporttools
 - Computerverwaltung 61
 - Dateisignaturverifizierung 75
 - Datenträgerbereinigung 73
 - Leistungsinformationen und -tools 66ff.
 - Liste 72
 - Systeminformationen 68
 - Systemkonfiguration 76–82
 - Systemkonsole 64ff.
 - WMI-Steuerung 70ff.
- Systemumgebungsvariablen 88, 91
- Systemvariablen 88–91
- Systemvolumes 412, 419–422, 425, 441, 445, 478

Systemwiederherstellungstool 73
 Aktivieren oder Deaktivieren 197
 Installationswiederherstellungspunkte 281
 Konfiguration 94–97
 Normaler oder abgesicherter Modus 379
 Problembehandlung 380
 Richtlinienereinstellungen 197
 Wiederherstellen von Systemen 380
 Wiederherstellungspunkte 377–381
 SYSVOL-Freigabe 523

T

Tablet PCs *Siehe* Notebooks und Tablet PCs
 Taskleiste 122–125
 Elemente aus Apps anheften 25
 Task-Manager 68, 291, 385
 Starten 80
 Taskprioritätsdienste 153
 Tastaturfehler 164
 Tastenkürzel 120
 TCG (Trusted Computing Group) 390
 TCP/IP-Drucker, Richtlinien 215
 TCP/IP-Konfiguration
 Drahtlosnetzwerke 633
 Dual-TCP/IP 573f.
 Ethernetverbindungen 576–585
 Filterungsarchitektur 574
 Komponenten installieren 572–576
 Mobile Computer, Einstellungen 598
 Netzwerk- und Freigabecenter 571
 Netzwerkerkennung 568
 Netzwerk-Explorer 570
 Netzwerkfreigaben 528
 Problembehandlung 588–594
 Standardkonfiguration 622
 Windows 8-Features und -Tools 568
 TCP/IP-NetBIOS-Helper 229
 TCP-Ports 496
 Technischer Support *Siehe* Hilfe und Support
 Teilen, Charm 24
 Teilen-Seite 117
 Telefon und Modem-Tool 605–608
 Telefonnummern 618, 620
 Telefonverbindungen, Richtlinien 215
 Temporal Key Integrity Protocol (TKIP) 630
 Temporärdateien 73, 483, 553
 Teredo 362
 Terminaldienste 266
 Testcode, Signaturzertifikate 180
 Testen von Ethernetverbindungen 588–594
 Testumgebungen 297, 340
 Textanzeige 111
 Textlesbarkeit anpassen 138
 Time To Live (TTL) 593
 Timeouts 79, 168, 173, 184
 Timer, Aufwacheinstellungen 102

TKIP (Temporal Key Integrity Protocol) 630
 TLS (Transport Layer Security), Verschlüsselung 488
 Tonwahl 607
 Tool zur Abbildverwaltung für die Bereitstellung *Siehe* DISM
 TPM (Trusted Platform Module) 390
 Aktivieren und Benutzen von TPM 395
 Authentifizierungsmethoden 414
 Besitzerkennwort ändern 401
 BitLocker 402, 412
 Einrichten 390
 Funktionen und Implementierung 390–401, 407
 Löschen 399
 Richtlinien 410
 Speichern von Datensicherungsinformationen 411
 Sperre zurücksetzen 394
 Tools (tpm.msc) 392
 TPM ausschalten 399
 TPM einschalten 396
 TPM-Verwaltung öffnen 392
 Validierungsprofileinstellungen 406
 Verwaltung und Richtlinien 392
 TPM-Plattform, Validierungsprofile 410
 TPM-Sicherheitshardware verwalten, Assistent 392, 396, 399
 Tragbare Computer *Siehe* Notebooks und Tablet PCs
 Tragbare Wechsellaufwerke *Siehe* Wechseldatenträger
 Transaktionales NTFS 471
 Transparenz 129
 Transport Layer Security (TLS), Verschlüsselung 488
 Treiber *Siehe* Gerätetreiber
 Treibermodell, Systemstartdienste 153
 Trigger 369, 372
 Triple-DES-Verschlüsselung 488
 Trusted Computing Group (TCG) 390
 Trusted Platform Module (TPM) 390
 TTL (Time To Live) 593

U

UAC (Benutzerkontensteuerung)
 Administratorgenehmigungsmodus 234–238
 Anheben der Privilegien 275
 Heimnetzgruppen, Arbeitsgruppen und Domänen 47f.
 Installation erkennen 279
 Kennwörter 242
 Legacy-Anwendungen 275
 Optimieren 234–238
 Sicherheitseinstellungen 236
 Status 307
 UAC-konforme Anwendungen 274
 Verwalten von Benutzerkonten 226
 Virtualisierung von Schreibzugriffen 279
 Zugriffstoken 274
 Übergeordnete Domänen 582
 Übergeordnete Ordner 511–514
 Übergreifende Volumes 63, 428
 Daten nicht vollständig, Status 470
 Dynamische Datenträger 441

Übergreifende Volumes (*Fortsetzung*)

- Erstellen 455
- Löschen 461
- Verkleinern oder Vergrößern 457f.
- Verschieben von Datenträgern in neue Systeme 467
- Wechseln zwischen Basis- und dynamischen Datenträgern 449
- Wiederherstellen 464
- Übertragungsraten (Wechseldatenträger) 479
- Übertragungswiederholungs-Timeout 574
- Überwachung der Dateifreigabe 532–535
- Überwachungsereignisse 366
- UDF (Universal Disc Format) 482, 484
- UDP-Ports 496, 528
- UEFI (Unified Extensible Firmware Interface)
 - 64-Bit-Architektur 27
 - Funktionen und Dienste 152ff.
 - Startprozesse 150
 - Startvorgang 155
- Uhr 124, 233
- UIAccess-Programme 237
- Umbenennen
 - Netzwerkverbindungen 588
 - Verschlüsselte Dateien 490
- Umgebung, Richtlinien 216f.
- Umgebungsvariablen
 - Auflösen 522
 - Befehlspfad 296
 - Fehlermeldungen 349
 - Konfigurieren 88–91
 - Ordnerpfade 522
 - Startvorgang 162, 167
 - Syntax 44
- Umgehen von Proxyservern 616
- Umschaltung, schnelle Benutzerumschaltung 49
- Unattend.xml-Datei 31
- Unbeaufsichtigte Installation, Antwortdateien 31, 38
- Unbekannt, Volumestatus 471
- UNC-Pfade (Universal Naming Convention) 199, 519
- Unified Extensible Firmware Interface *Siehe* UEFI
- Universal Disc Format (UDF) *Siehe* UDF
- Universal Naming Convention (UNC) 199, 519
- UNIX-Server 622
- Unsignierte Anwendungen 276
- Unsignierte Gerätetreiber 338, 379
- Untere Adressbereiche, Arbeitsspeicher 181
- Untergeordnete Organisationseinheit, Richtlinien 186
- Unterordner 487, 500, 505, 507
- Unterstützung *Siehe* Systemsupporttools
- Unterstützungseinladungen 261
- Unverifizierte Anwendungen 276
- Unverwaltete Richtlinieneinstellungen 216–223
 - Verknüpfungen 118
- Update
 - Abgelehnte Updates 360
 - Ausblenden von Updates 360
 - Automatische Updates 352–360
 - Benutzerkontoprivilegien 233

Update (*Fortsetzung*)

- Benutzte Dateien markieren 305
- Deaktivieren von Updates 359
- Deinstallieren von Updates nach Installation 360
- Dienste 318
- Firmware 150, 156
- Freigaben 523
- Geräte-Manager 336
- Gerätetreiber 324, 328, 339–342
- Grafikkartentreiber 141
- Installationsmöglichkeiten 353
- Module 31
- Offlinedateien 546
- Richtlinieneinstellungen 357ff.
- Rollups 352
- Suchen nach Updates 358f.
- Updates während Installation herunterladen 40, 42
- Updateserver 358
- Updatetypen 352, 355
- Vertrauenswürdige Partner 353
- Wartungscenter 45f.
- Webkompatibilitätslisten 355
- Wichtige Updates 353
- Wiederherstellungspunkte 328, 379
- Windows Update 352ff.
- Update Sequence Number (USN) 472
- Upgrade von Windows 37
- UPnP (Remoteunterstützungsanforderungen) 362
- URL-Verknüpfungen 119ff.
- USB-Debug Einstellungen 179f.
- USB-Geräte
 - Abziehen 53
 - Auswerfen 432
 - Benutzerdefinierte Standbyoptionen 103
 - BitLocker 402, 404, 417, 426
 - Dateisysteme und Formatieren 479
 - Drahtlosadapter 628, 631
 - Drucker 331
 - Dynamische Datenträger 444
 - Entschlüsseln 426
 - Hubs 479
 - Installieren 326–329
 - Kennworrücksetzdiskette 51, 244
 - Netzwerkkarten 572
 - ReadyBoost 436ff.
 - Systemstart 161, 164
 - UEFI, Unterstützung 153
 - Versionen 479
- USB-Hubs 479
- USB-Kartenleser 445, 469
- USB-Stick
 - Auswerfen 432
 - BitLocker 402, 404
 - Kennworrücksetzdiskette 51, 244
 - ReadyBoost 436ff.
 - Startreihenfolge 164
- User State Migration Tool (USMT) 28

UserName-Umgebungsvariable 44
 USN-Journal 472

V

- Validierte ausführbare Dateien 237
- VAMT (Volume Activation Management Tool) 28
- Variable Länge, Subnetzunterteilung 578
- Variablen 88–91, 522
- VBScript 206
- Ventilatorgeschwindigkeit 103
- Veraltete COM-Objekte 316
- Veraltete Daten, Volumestatus 471
- Veraltete DLLs 316
- Verbergen 542–544
 - Benachrichtigungssymbole 124
 - Symbole 132
 - Symbolleisten 126
 - Taskleiste 123
 - Updates 360
- Verbindung mit einem Netzwerkprojektor herstellen 596, 601
- Verbindungen 337, *siehe auch* Netzwerkverbindungen
- Verbindungslokale Multicast-Namensauflösung (LLMNR) 574
- Verbundidentitäten 508
- Verbund-TCP, Feature 574
- Verfizierte Anwendungen 276
- Verfolgen der Dateifreigabe 532–535
- Vergessene Kennwörter 50f.
- Verknüpfungen (Schnittstelle) 118–121, 216
- Verknüpfungen (Techniken)
 - Anzeigen von Dateien mit Tastenkombination 538
 - Firmwareverknüpfungen 158
 - Tastenkürzel 120
 - Unverwaltete Richtlinieneinstellungen 219
 - Zugriff auf Startoptionen 151
- Verknüpfungen, Richtlinien 118, 216f.
- Verlauf, Feature 122, 308, 359
- Veröffentlichen von Anwendungen 285
- Verschieben
 - Dateien nach Datenträgerkontingentlöschung 560
 - Dynamische Datenträger in neue Systeme 467
 - Taskleiste 123
 - Verschlüsselte Dateien 490
- Verschlüsselndes Dateisystem *Siehe* EFS
- Verschlüsselung *Siehe auch* EFS (Verschlüsselndes Dateisystem)
 - BitLocker 402–405, 408–412, 418
 - BranchCache 564
 - Cipher-Dienstprogramm 492
 - Datei-Explorer, Anzeige 540
 - Dateifreigabe 497
 - Dateisysteme 404
 - Drahtlosnetzwerke 629
 - Dual-TCP/IP 574
 - Einladungen zur Remoteunterstützung 204
 - Entschlüsseln von Daten 492
 - Entschlüsselte Dateien 491
 - Gruppenrichtlinien 488
 - Verschlüsselung (*Fortsetzung*)
 - Kennwörter und Daten wiederherstellen 243
 - Kennwörter und verschlüsselte Dateien 242
 - L2TP und PPTP 603
 - Offlinedateien 199ff., 554
 - Remotedesktopsitzungen 265
 - TPM-Prozess 391
 - Überprüfungstechniken 621
 - VPN-Verbindungen 613
- Verschlüsselungsschlüssel 488
- Verschlüsselungsstärke 410
- Versiegeln von Schlüsseln 391
- Versionen von Dateien 373, 544, 552
- Versteckte Freigaben 527
- Verteilergruppen 229
- Verteilte Caches 564
- Verteiltes Dateisystem (DFS) 542
- Vertrauenswürdige Anwendungen 276
- Vertrauenswürdige Partner 353
- Verwalten von Elementen (Datei-Explorer) 542
- Verwaltete Einstellungen *Siehe* Richtlinieneinstellungen
- Verwaltungsaktion, Richtlinien 216
- Verwaltungstools
 - häufig benutzte Anwendungen 25
 - zum Start-Bildschirm hinzufügen 61
- Verweigern-Berechtigungen 501, 514
- VESA (Video Electronics Standards Association) 180
- VGA-Anzeige 143, 182
- VGA-Einstellungen 79, 182
- VHD-Dateien 30, 60, *siehe auch* Virtuelle Computer
- Video Electronics Standards Association (VESA) 180
- Video Graphics Array *Siehe* VGA-Anzeige, VGA-Einstellungen
- Videoeinstellungen *Siehe* Anzeige
- Videos 102, 497, 530
- Viiv-basierte Computer 161
- Viren 471
- Virtualisierung 275, 279, 286
- Virtuelle Computer 30
- Virtuelle Festplattenlaufwerke 60
- Virtuelle Laufwerke 482
- Virtuelle private Netzwerke *Siehe* VPN-Verbindungen
- Virtuelle Tunnel 603, 622
- Virtuelle Volumes 418
- Virtueller Adressraum 181
- Virtueller Arbeitsspeicher 85ff.
- Visual Basic-Skripts 206
- Visuelle Effekte 67, 84f.
- Vollbildmodus 271
- Vollständige Speicherabbilder 93
- Volumenaktivierungsverwaltungstool (VAMT) 28
- Volumenlizenz, Keys 45
- Volumes *Siehe auch* Partitionen
 - Absturzabbildvolumes 445
 - Aktive Volumes 445, 447
 - Auslagerungsdateivolumes 445
 - Basisdatenträger 441
 - Bezeichnungen 455, 461

Volumes (*Fortsetzung*)

- BitLocker 402
- Datenträgerkontingente 556
- Datenträgertypen 443
- Datenträgerverwaltung 433
- Dynamische Datenträger 428
- Einfache Volumes 452–455
- Formatieren 454, 458
- Gespiegelte Datenträger 466
- Größe 452
- Laufwerkbuchstaben und -pfade 459
- Liste anzeigen 433
- Löschen 448, 461
- Startvolumes 445
- Statusmeldungen 470f.
- Stripesetvolumes 455
- Systemvolumes 445
- Übergreifende Volumes 455
- Vergrößern/Verkleinern 433, 457f.
- Wechseln zwischen Basis- und dynamischen Datenträgern 448
- Wiederherstellen 464
- Vom Administrator zugewiesene Ordner und Dateien 198f.
- Vom Herausgeber verifizierte (signierte) Anwendungen 276
- Vor Kurzem geänderte Hardware 387
- Vorgängerversionen 94
 - auf Dateiservern 373
- Vorgängerversionen von Daten 373
- Vorinstallierte Schlüssel 630
- Vorladen von Anwendungen 440
- Vorlagen *Siehe* ADMX-Dateien (administrative Vorlagen)
- Vorschau von Dateien 541
- Vorschaubilder 74, 539, 541f.
- Vorwahl 605, 607
- VPN-Verbindungen 603
 - Anmeldung konfigurieren 618
 - Aufbauen 626
 - Automatische oder manuelle Verbindungen 614
 - Benutzerkontoprivilegien 233
 - DirectAccess 56
 - Erstellen 612
 - Identitätsüberprüfung 621
 - Netzwerkprotokolle und Komponenten 621ff.
 - Problembehandlung 627
 - Proxeinstellungen 615–618
 - Richtlinien 215
 - Unverwaltete Richtlinieneinstellungen 215
 - Windows-Firewall 623

W

Wählregeln 605–608

Wählverbindungen

- Anmeldung konfigurieren 618
- Arbeitsplatznetzwerkverbindungen 609f.
- Aufbauen 624f.
- Automatische oder manuelle 614
- Erstellen 605

Wählverbindungen (*Fortsetzung*)

- Identitätsüberprüfung 621
- Internetproviderverbindungen 608
- Netzwerkprotokolle und Komponenten 621ff.
- PPPoE, Unterstützung 574
- Primäre und alternative Telefonnummern 620
- Problembehandlung 624
- Probleme mit automatischer Einwahl 614
- Proxeinstellungen 615–618
- Prozesse 602
- Trennung 619
- Unverwaltete Richtlinieneinstellungen 215
- Wählregeln 605–608
- Windows-Firewall 623
- Wake-On-Lan-Einstellungen 160
- Wallpaper-Ordner 129
- WAN (Wide Area Network) 572
- Warnungen 45f., 235, 310–316, 346–349
 - im Wartungszentrum 307
- Warteschlange, Aufgaben 372
- Wartung
 - Aufgabenplanung 368–373
 - Automatische Updates 352–360
 - Datensicherung 381ff.
 - Richtlinien für den Zeitplan 357
 - Wartung, Problembehandlungsmodule 315
 - Wartungszentrum 45f., 307
- Wartungszentrum
 - automatische Wartung 312
 - Benachrichtigungen 306–316
 - Hardwarefehlerrmeldungen 346–349
 - Infobereich 124
 - Lösungen archivieren 308
 - Probleme beseitigen 308
 - Problemerkennung 307
 - SmartScreen 312
 - Starten 45f.
 - Symbol ausblenden 316
 - Zuverlässigkeitsberichte 308
- Watchdog-Timer 153
- WDDM-Treiber 39, 136
- Webanmeldeinformationen 246
- Webseiten als Offlinedateien 74
- Wechseldatenträger
 - Aktiv-Status 445
 - AutoPlay, Feature 299
 - BitLocker, Richtlinien 411
 - CD- und DVD-Geräte 481–485
 - Computer-Konsole 431
 - Dateien öffnen 293
 - Dateisysteme und Formate 479
 - Datenträgerkontingentrictlinien 195
 - Dynamische Datenträger 443, 449
 - Kein Medium, Laufwerksstatus 469
 - Leistung 436–440
 - Schreibzugriff verweigern 405
 - Systemstart 161

- Wechseldatenträger, Richtlinien 411
- Weitere Tools (Leistung) 68
- WEP (Wired Equivalent Privacy) 233, 629, 631
- Werte (BCD-Speicher) 178–182
- Wide Area Network (WAN) 572
- Wiederbeschreibbare Discs 481
- Wiederherstellen
 - Anmeldeinformationen 250
 - BCD-Speicher 173
 - Computer 377–381
 - Desktopdesigns 128
 - Dienste neu starten 321
 - Geerbte Berechtigungen 513
 - gelöschte Windows-Binärdateien 354
 - Kennwörter 243
 - Komponenten 354
 - Persönliche Daten 385
 - Systemwiederherstellungstool 377–381
 - Volumes 464
 - Vorgängerversionen von Dateien 95
 - Wiederherstellungspunkte 380
 - WMI-Repository 71
- Wiederherstellung, Ablauf 180
- Wiederherstellungsagent 489, 491
- Wiederstellungsagent hinzufügen, Assistent 491
- Wiederstellungserweiterungen 411
- Wiederstellungskennwörter 410, 414
- Wiederherstellungsmodus 402, 424
- Wiederherstellungsobjekte 411
- Wiederherstellungsoperationen 379
- Wiederherstellungspunkte 281, 377–380
 - Grundlagen 378
 - manuell erstellen 379
 - wiederherstellen 380
- Wiederherstellungsschlüssel 402, 409, 411, 416, 418, 421, 424
- Wiederherstellungstools 29, 39
- Wiederherstellungszertifikate 414, 491
- Wiederholen der Synchronisierung 550
- Wi-Fi Protected Access (WPA) 629ff.
- Wi-Fi Protected Access Version 2 (WPA2) 629ff.
- Wi-Fi-Verbindungen *Siehe* Drahtlosnetzwerke
- WIM (Windows Imaging Format)
 - Bereitstellung 30f.
 - Verteilen von Windows 55
- WIM (Windows Imaging) 23
- Win32-Subsystem 162
- Windows 2000 280
- Windows 7 37
- Windows 8 28
 - Architektur 54–58
 - BCD-Speicher 151
 - Designs 45
 - Diagnose- und Problembehandlungstools 55, 304
 - Editionen 22, 64
 - Elemente der Oberfläche 23
 - Energiesparpläne 52f.
 - Gruppenrichtlinieneinstellungen 192
 - Windows 8 (*Fortsetzung*)
 - Hardwareunabhängigkeit 55
 - Hardwarevoraussetzungen 39
 - Hinzufügen oder Deinstallieren von Funktionen 300
 - Installieren 39–43
 - Konfiguration *Siehe* Konfiguration
 - Modularisierung 55
 - Netzwerktools 568
 - Neuinstallationen und Upgrades 37
 - Problembehandlung für Fehler 366ff.
 - Remotedesktopsitzungen 263
 - Überblick 22
 - Versionsinformationen 64
 - Vorbereiten der Installation 38f.
 - Vorinstallationsumgebung 23
- Windows 8 Enterprise 22, 402, 604
- Windows 8 Pro 22
- Windows 8 RT 22f.
- Windows 8 Ultimate 402
- Windows Automated Installation Kit 32
- Windows BranchCache 563ff.
- Windows Hardware Quality Lab (WHQL) 338
- Windows Imaging-Format (WIM) 23
- Windows Internet Naming Service *Siehe* WINS
- Windows Management Instrumentation (WMI) 63, 70ff., 318
- Windows On Arm (WOA) 150
- Windows PE (Windows Preinstallation Environment) 28
 - Befehlszeilentools 29
 - Funktionen 29
 - Systemstart deaktivieren 182
- Windows PE 4.0 23
- Windows Performance Toolkit (WPT) 28
- Windows PowerShell 25f., 206, 314, 318, *siehe auch* PowerShell 2.0
- Windows Preinstallation Environment *Siehe* Windows PE
- Windows RE (Windows-Wiederherstellungsumgebung)
 - Partitionen 409
 - Tools 39
- Windows Resume Loader 172, 177, 180, 375
- Windows Script Host (WSH) 206, 368
- Windows Server 2008 151, 280, 564
- Windows Server 2008 R2 604
- Windows Server 2012 603
- Windows Server Update Services (WSUS) 352
- Windows Store, Zugang steuern 271f.
- Windows Update
 - Ausblenden von Updates 360
 - Ausführungszeit 356
 - Benachrichtigungen 307
 - Deinstallieren von automatischen Updates 360
 - Konfigurieren von Updates 352ff.
 - Problembehandlungsmodule 315
 - Suchen nach Updates 359
 - Suchserver festlegen 352
 - Verlauf und Installationsstatus 359
 - Wichtige Updates 353
 - Wiederherstellen abgelehnter Updates 360
- Windows Vista 37, 151, 175, 263, 280

- Windows Vista-Anwendungen 276
 - Windows XP 37, 232, 277, 280
 - Windows.old-Ordner 40f.
 - Windows-64-x86-Emulationsschicht (WOW) 27
 - Windows-Abbilder-Dateien *Siehe* WIM
 - Windows-Anmeldeinformationen 246f.
 - Windows-Anmelde-Manager 162, 167
 - Windows-Authentifizierung 621f.
 - Windows-Bereitstellungsdienste 38
 - Windows-Betriebssystemlader 180ff.
 - Windows-Bewertungsdienste 28
 - Windows-Bewertungstoolkit 28
 - Windows-Datensicherung 307
 - Windows-Defender 369
 - Windows-EasyTransfer 37
 - Windows-Eingabeaufforderung, Systemstart 79
 - Windows-Einstellungen, Richtlinien 214
 - Windows-Filterplattform, Feature 574
 - Windows-Firewall *Siehe auch* Firewalls
 - Ausnahmen für Remoteverwaltung 64
 - Datei- und Druckerfreigabe, Ausnahme 496
 - Mehrere Netzwerke 55
 - Netzwerkerkennung 331, 568
 - Netzwerkkategorie 569
 - Netzwerkverbindungen 623
 - Profile 569
 - Remotedesktop, Feature 265f.
 - Remoteunterstützung, Feature 361f.
 - Richtlinien 202
 - Windows-Legacybetriebssystem-Ladeprogramm *Siehe* Ntldr
 - Windows-Leistungindex 65
 - Windows-Netzwerkdiagnose 56, 572, 589
 - Windows-Netzwerkisolation 273
 - Windows-Pushbenachrichtigungsdienst (WNS), Richtlinien 272
 - Windows-ReadyBoost 436ff.
 - Windows-ReadyDrive 438
 - Windows-Remoteunterstützung, Assistent 361, 365
 - Windows-Setup 38, 281, 366
 - Windows-Skripts 206
 - Windows-Speicherdiagnosetool 57, 175, 179f.
 - Windows-Speichertestprogramm, Eintrag 179
 - Windows-Startladeprogramm
 - BCD-Speichereinträge 171, 173ff.
 - Einstellungen 176
 - Fehler während Systemstart 166
 - Funktionen 151
 - Startvorgang 155
 - Windows-Start-Manager
 - Abgesicherter Modus und andere Optionen 376
 - BCD-Speichereinträge 171, 173ff., 180
 - Einstellungen 176
 - Funktionen 151
 - Startoptionen 78ff.
 - Startvorgang 155
 - Systemstart konfigurieren 92
 - Systemstartfehler 166
 - Windows 8-Systemstart 54
 - Windows-Startsektoranwendung 172
 - Windows-SuperFetch 439f.
 - Windows-Systemabbild-Manager 32, 38
 - Windows-Upgrade 74
 - Windows-Vorinstallationsumgebung 28
 - Windows-Wiederherstellungsumgebung *Siehe* Windows RE
 - WINS (Windows Internet Naming Service) 583ff., 588, 590, 592, 601
 - Wird initialisiert, Volumestatus 470
 - Wird wiederhergestellt, Laufwerksstatus 477
 - Wired Equivalent Privacy *Siehe* WEP
 - Wired for Management Baseline (WMB) 152
 - Wireless Protected Setup (WPS) 329
 - Wise Install 281, 293
 - WMB (Wired for Management Baseline) 152
 - WMI (Windows Management Instrumentation) 70ff., 318
 - WMI-Steuerung, Zugriff 63
 - WNS (Windows Push Notification Service) 272
 - WOA (Windows On Arm) 150
 - Startvorgang 155
 - Systemstart 163
 - WOW (Windows-64-x86-Emulationsschicht) 27
 - WPA (Wi-Fi Protected Access) 629ff.
 - WPA2 (Wi-Fi Protected Access Version 2) 629ff.
 - Wpeinit-Tool 29
 - WPS (Wireless Protected Setup) 329
 - WSH (Windows Script Host) 206, 368
 - WSUS (Windows Server Update Services) 352
 - WS-Verwaltung-Protokoll 318
- X**
- x64-Architektur 26f., 152, 429
 - x86-Architektur 27, 38, 151, 429
- Z**
- Zeichen in Volumebezeichnungen 461
 - Zeigegeräte 164
 - Zeigerdesigns 128
 - Zeit (Synchronisierung) 550
 - Zeitlimits
 - Einladungen 205, 261, 364
 - Skripts 206
 - Zeitsynchronisierung 318
 - Zeitzone 233
 - Zertifikate
 - Benutzerkonten 228
 - Daten-Wiederherstellungsagenten 405
 - Drahtlosverbindungen 631
 - Kennwörter 242
 - Remoteanmeldung konfigurieren 618
 - Remotedesktop 265
 - Testcode, Signaturzertifikate 180
 - Verschlüsselungszertifikate 488
 - Wiederherstellungszertifikate 491
 - Zertifikatbasierte Anmeldeinformationen 247, 249

Zertifikate (*Fortsetzung*)

Zertifikatserver 603

Zertifizierte Treiber 337, 379

Zertifizierungsstelle 491

Zielgruppen, Editor 223

Zielgruppenadressierung auf Elementebene 223

Zielpfade 120

Zufällige Schnittstellen-IDs, Feature 574

Zugriff *Siehe auch* Berechtigungen

Benutzer- und Gruppenkonten 226–229, 251–260

Bereitstellung von Berechtigungen 498

BitLocker 402–405, 408–412

Dateibesitz 510

Datei-Explorer 538–544

Dateifreigabe, Überwachung 532–535

Dateifreigabeberechtigungen 499–507, 510–516

Dateifreigabeoptionen 494–498, 523–527

Drahtlos *Siehe* Drahtlosnetzwerke

effektiver, bestimmen 514

Entschlüsselte Dateien 491

Gespeicherte Anmeldeinformationen 246–251

Lokale Anmeldung 237–246

Netzwerkfreigaben 516

Netzwerkverbindung, Zugriffstypen 571

Öffentlich-Ordner freigeben 530f.

Offlinedateien 544–555

Prinzip der geringstmöglichen Rechte 503

Remotedesktop 263–266

Remotezugriff *Siehe* Remotezugriff

Richtlinieneinstellungen 180, 202–205

TPM-Funktionen 390–401, 407

Zugriff (*Fortsetzung*)

UAC 232–238

Verweigern auf Arbeitsstationen 246

Zugriffsberechtigungen 494

Zugriffspunkte (Drahtlos) 628, *siehe auch* Drahtlosnetzwerke

Zugriffsrichtlinien 180, 202–205

Zugriffssteuerungsliste (ACL) 500

Zugriffssteuerungs-Unterstützungsoperatoren-Gruppe 231

Zugriffstoken 233, 274

Zuletzt verwendete Dokumente 119

Zuordnen

Freigaben 523

Ports 574

Verhindern der Laufwerkszuordnung 542

Zurücksetzen

Computer 153

Kennwörter 51

TPM 396

Zusatztaste 120

Zuverlässigkeitsberichte 308

Zwischenspeicherung

Datenträgerkontingent, Abfragecache 557

Leeren von DNS-Caches 593

Netzwerkfreigabe von Dateien 519

Offlinedateieinstellungen 547f.

Remotedesktopsitzungen 267

Startvorgang 154

Vorschaubilder 542

Wechseldatenträgergeräte 480

Windows BranchCache 563ff.

Windows-ReadyBoost 436

Der Autor

William R. Stanek (<http://www.williamstanek.com>) verfügt über mehr als 20 Jahre praktischer Erfahrung mit Computerprogrammierung und Softwareentwicklung. Er ist ein führender Technologieexperte, ein ausgezeichnete Autor (das können Sie wörtlich nehmen) und ein verdammt guter Kursleiter. Im Lauf der Jahre half er mit seinem praktischen Rat schon Millionen von Programmierern, Entwicklern und Netzwerkingenieuren auf der ganzen Welt. Unter seinen neusten Büchern sind *Windows 8 – Ratgeber für Administratoren* und *Windows Server 2012 Inside Out* (nur in englischer Sprache erhältlich).



William R. Stanek ist seit 1991 in der kommerziellen Internetgemeinschaft tätig. Die Grundlagen seiner geschäftlichen und technologischen Erfahrung stammen aus über 11 Jahren Militärdienst. Er verfügt über beträchtliche Erfahrung in der Entwicklung von Servertechnologie, Verschlüsselung und Internetlösungen. Er hat viele technische Whitepapers und Trainingskurse über verschiedene Themen geschrieben. Als Experte und Consultant ist er sehr gefragt.

William R. Stanek besitzt einen B.S. (magna cum laude) in Informatik und einen M.S. (mit Auszeichnung) in Informationssystemen. Er lebt mit seiner Frau und seinen Kindern im pazifischen Nordwesten der USA.

William R. Stanek hat vor Kurzem seine Liebe zur Natur wiederentdeckt. Wenn er nicht schreibt, vertreibt er sich die Zeit mit Wandern, Radfahren oder Reisen, immer zusammen mit seiner Familie auf der Suche nach neuen Abenteuern.

Auf Twitter finden Sie William R. Stanek unter twitter.com/WilliamStanek, auf Facebook unter www.facebook.com/William.Stanek.Author.