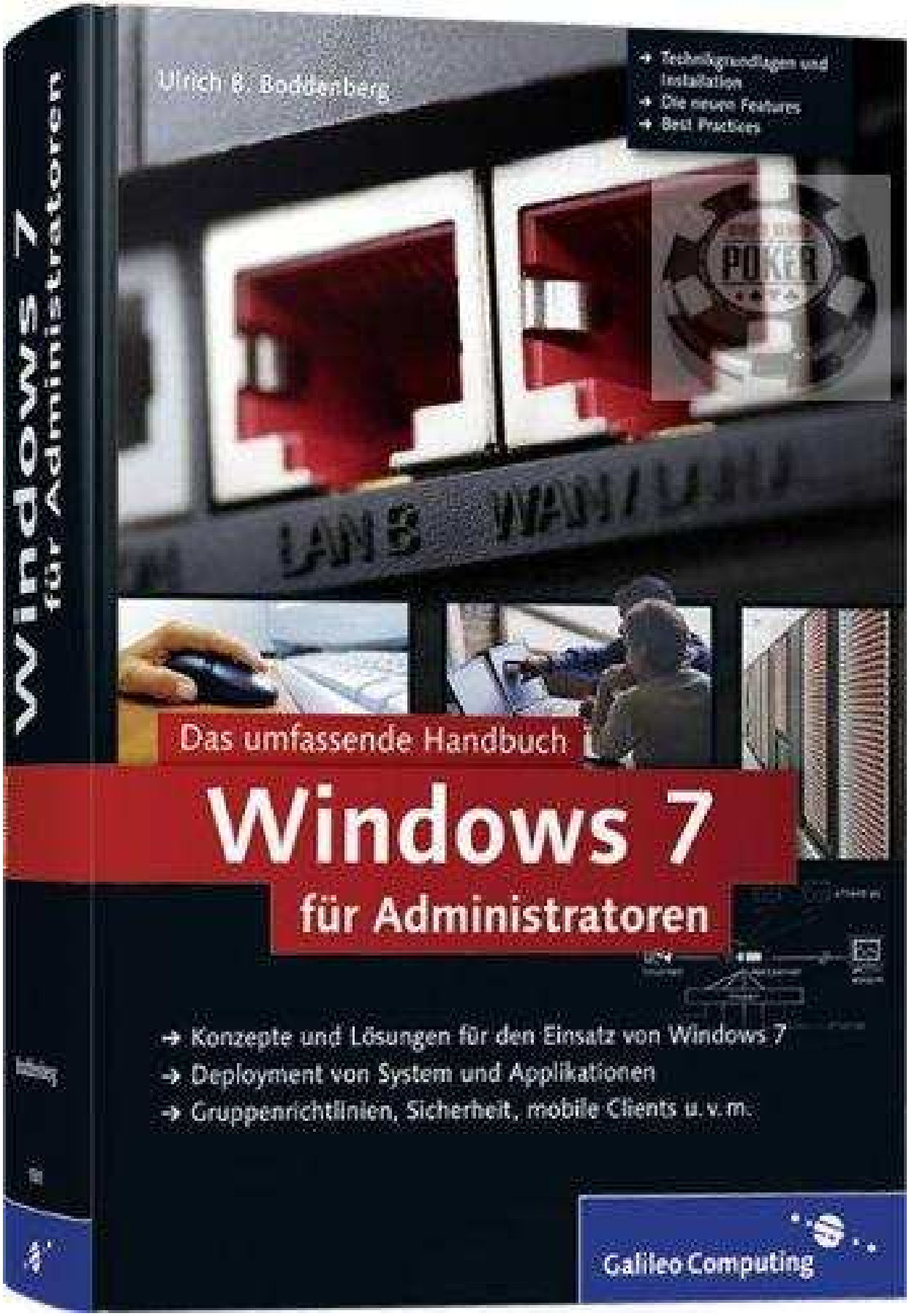

Windows 7
für Administratoren
Ulrich B. Boddenberg
→ Technikgrundlagen und Installation
→ Die neuen Features
→ Best Practices
POKER
Das umfassende Handbuch
Windows 7
für Administratoren
→ Konzepte und Lösungen für den Einsatz von Windows 7
→ Deployment von System und Applikationen
→ Gruppenrichtlinien, Sicherheit, mobile Clients u. v. m.
Galileo Computing

Ulrich B. Boddenberg

Windows 7 für Administratoren

Das umfassende Handbuch

Galileo Press

Liebe Leserin, lieber Leser,

Windows 7 ist da. Viele Anwender haben mit Spannung und vielleicht sogar etwas ungeduldig auf Windows 7 gewartet. Systemadministratoren, Entscheider und IT-Verantwortliche denken da vielleicht eher anders, denn mit der Einführung eines neuen Systems kommt Arbeit auf sie zu. Die Einführung eines neuen Client-Systems will gut geplant und technisch professionell durchgeführt werden. Vielleicht sehen einige unter Ihnen neben den zahlreichen Vorteilen und Verbesserungen gegenüber Vorversionen auch diesen Aspekt. Um Ihnen Sorgen und Arbeit abzunehmen, hat unser Autor Ulrich B. Boddenberg dieses Buch geschrieben.

Vielleicht kennen Sie ihn ja bereits, denn er hat sich unter Administratoren und Entscheidern, die in einem technischen Umfeld arbeiten, das von Microsoft-Server-Produkten dominiert wird, einen Namen gemacht. Seine Bücher »Konzepte und Lösungen für Microsoft-Netzwerke«, »Exchange Server« oder sein Buch zum SharePoint Server zeichnet eines besonders aus: Sie vermitteln lösungsorientiertes Praxiswissen jenseits von reinen Funktionsbeschreibungen.

So lauten etwa typische Pressestimmen zu seinen Werken:

»Wichtig für den Leser ist, dass mehrere Lösungen eines Problems dargestellt und deren Auswirkungen aufgezeigt werden, damit wird es dem Nachahmer bei der Problemlösung erheblich leichter gemacht.«
Daten und Analysen

»Boddenberg gelingt es, einen umfassenden Überblick über die Technologie mit einem hohen Praxisnutzen zu verbinden.«
InfoWeek

Auch das vorliegende Buch hält dieses Versprechen. Umfassend und konsequent am Arbeitsalltag eines Administrators orientiert, beschreibt es alles, was Sie als Administrator über Windows 7 wissen sollten. Eine unverzichtbare Hilfe und ein Berater auf Papier, immer an Ihrer Seite.

Herr Boddenberg und ich freuen uns auf Ihre Rückmeldungen!

Viel Freude beim Lesen wünscht

Ihr Jan Watermann
Lektorat Galileo Computing

jan.watermann@galileo-press.de
www.galileocomputing.de
Galileo Press · Rheinwerkallee 4 · 53227 Bonn

Auf einen Blick

1 Gedanken zum Buch 17

2 Aufbau des Buchs 21

3 Business Value 25

4 Einstieg 57

5 Einige Technologiegrundlagen 71

6 Deployment 185

7 Aktivierung 309

8 Windows RE 339

9 Applikationen und Windows 7 351

10 Microsoft Desktop Optimization Pack 387

11 Gruppenrichtlinien 409

12 Sicherheit 481

13 Mobile Clients 631

14 Suchen und Finden 701

15 Mehrsprachige Umgebungen 717

16 Client-Management mit System Center Configuration Manager 2007 R2 (SCCM) 727

Der Name Galileo Press geht auf den italienischen Mathematiker und Philosophen Galileo Galilei (1564–1642) zurück. Er gilt als Gründungsfigur der neuzeitlichen Wissenschaft und wurde berühmt als Verfechter des modernen, heliozentrischen Weltbilds. Legendär ist sein Ausspruch *Eppur se muove* (Und sie bewegt sich doch). Das Emblem von Galileo Press ist der Jupiter, umkreist von den vier Galileischen Monden. Galilei entdeckte die nach ihm benannten Monde 1610.

Gerne stehen wir Ihnen mit Rat und Tat zur Seite:
jan.watermann@galileo-press.de bei Fragen und Anmerkungen zum Inhalt des Buches
service@galileo-press.de für versandkostenfreie Bestellungen und Reklamationen
julia.bruch@galileo-press.de für Rezensions- und Schulungsexemplare

Lektorat Jan Watermann
Korrektorat Friederike Daenecke, Zülpich
Cover Barbara Thoben, Köln
Titelbild Barbara Thoben, Köln
Typografie und Layout Vera Brauner
Herstellung Vera Brauner
Satz Typographie & Computer, Krefeld
Druck und Bindung Bercker Graphischer Betrieb, Kevelaer

Dieses Buch wurde gesetzt aus der Linotype Syntax Serif (9,25/13,25 pt) in FrameMaker.
Gedruckt wurde es auf chlorfrei gebleichtem Offsetpapier.

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

ISBN 978-3-8362-1501-5

© Galileo Press, Bonn 2010
1. Auflage 2010

Das vorliegende Werk ist in all seinen Teilen urheberrechtlich geschützt. Alle Rechte vorbehalten, insbesondere das Recht der Übersetzung, des Vortrags, der Reproduktion, der Vervielfältigung auf fotomechanischem oder anderen Wegen und der Speicherung in elektronischen Medien. Ungeachtet der Sorgfalt, die auf die Erstellung von Text, Abbildungen und Programmen verwendet wurde, können weder Verlag noch Autor, Herausgeber oder Übersetzer für mögliche Fehler und deren Folgen eine juristische Verantwortung oder irgendeine Haftung übernehmen. Die in diesem Werk wiedergegebenen Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. können auch ohne besondere Kennzeichnung Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.

Inhalt

1 Gedanken zum Buch 17

2 Aufbau des Buchs 21

3 Business Value 25

3.1 Ein kurzer Blick zurück 26
3.1.1 Windows 1, 2 und 3 26
3.1.2 Windows NT kommt (3.1 bis 3.51) 29
3.1.3 Windows NT 4 – Der Durchbruch 30
3.1.4 Windows 2000 Professional 32
3.1.5 Windows XP 33
3.1.6 Windows Vista 34
3.2 Gründe für ein neues Betriebssystem 35
3.2.1 Bedarf an einer modernen Plattform 35
Softwarearchitektur 37
NAP, BitLocker, AppLocker, DirectAccess & Co. 39
3.2.2 Optimiertes Deployment und Management 40
3.2.3 Verbesserte Sicherheit 42
3.2.4 Einfachere Bedienung 43
3.2.5 Mobile Szenarien 44
3.2.6 Support-Situation 45
3.3 »Better Together« 47
3.4 Hardware 48
3.5 Infrastrukturoptimierung 50

4 Einstieg 57

4.1 Was ist neu? 59
4.1.1 Sicherheit 60
4.1.2 Mobilität 61
4.1.3 Deployment 62
4.1.4 Management 63
4.1.5 Suche 64
4.1.6 Zusammenarbeit mit Windows Server 2008 R2 65
4.2 Editionen und Lizenzen 65
4.2.1 Editionen 66

4.2.2 Zugriffslizenzen (CALs) 68
4.2.3 Lizenzverträge 69

5 Einige Technologiegrundlagen 71

5.1 Netzwerk 71
5.1.1 IPv4 vs. IPv6 73
Unterschiede 74
IPv6 – die Adressierung 75
Vergabe von IPv6-Adressen 82
Abschalten von IPv6 83
5.2 Profile 84
5.2.1 Vorteile und Nachteile 86
5.2.2 Servergespeicherte Profile in mehrsprachigen Umgebungen 86
5.2.3 Zwischenspeichern der Profile 87
5.3 Die Registry 89
5.4 Windows-Funktionen 92
5.5 Das .NET Framework 93
5.5.1 Der Grundgedanke 95
5.5.2 .NET bei der Arbeit 97
5.5.3 .NET Framework und .NET Compact Framework 98
5.5.4 Code Access Security 102
5.5.5 Von Codegruppen und Berechtigungssätzen 103
Berechtigungssatz 104
Codegruppe 104
5.6 WPF, WCF, WWF und CardSpace 106
5.7 Geräte 107
5.8 Die Active Directory-Zertifikatdienste 109
5.8.1 Einige Anwendungsszenarien 109
Internet-Authentifizierung und Verschlüsselung 109
Sichere E-Mail 112
Codesignatur 115
IP-Verschlüsselung 116
Anmeldung mit Smartcard 117
EFS 117
Wireless Authentification (802.1X) 118
Fazit 118
5.8.2 Installation der Zertifikatdienste und Migration (einstufige Architektur) 119
Wiederherstellen der Zertifikatdatenbank 127

5.8.3 Zertifikate aus Sicht des Clients 129
5.8.4 Zertifizierungspfad 134
5.8.5 Zertifikatsvorlagen 135
5.8.6 Weboberfläche 143
5.8.7 Mehrstufige Architekturen 146
Rollen 147
Architekturen 149
5.9 VPNs mit Windows 7 und Windows Server 2008 R2 151
5.9.1 Gateway-Architektur 153
5.9.2 Grundkonfiguration des VPN-Servers 154
5.9.3 VPN einrichten – allgemein 159
5.9.4 Einwahlberechtigung 165
5.9.5 PPTP-VPN 165
5.9.6 L2TP-VPN 168
5.9.7 SSTP 171
5.9.8 Automatischer Modus 177
5.9.9 Connection Manager Administration Kit (CMAK, Verbindungs-Manager-Verwaltungskit) 179

6 Deployment 185

6.1 Einführende Überlegungen 185
6.1.1 Standardisierung 185
6.1.2 Lokale Daten und Profile 187
6.1.3 Vorinstallierte Versionen und Re-Imaging-Recht 187
6.1.4 Der Deployment-Prozess 189
6.2 WAIK installieren und Testumgebung 190
6.3 Installationsimage vorbereiten – erster Durchlauf 191
6.3.1 Antwortdatei vorbereiten 192
6.3.2 Installation durchführen 200
6.3.3 Installation anpassen und verallgemeinern 202
6.3.4 WinPE-Startimage erzeugen 204
6.3.5 WIM erzeugen 207
6.3.6 Kurzer Test 209
6.4 Windows-Bereitstellungsdienste (WDS) installieren und einsetzen 211
6.4.1 Voraussetzungen 212
6.4.2 WDS installieren 213
6.4.3 WDS-Erstkonfiguration 215
6.4.4 Start- und Installationsabbilder hinzufügen 219
6.4.5 Ein erster »kleiner« Test mit WDS 223

6.5 PXE und TFTP – genauer hingeschaut 228
6.6 WDS-Startvorgang automatisieren 232
6.6.1 Automatisierung der Installation des Windows-Bereitstellungsdiensteclients 233
Antwortdatei erstellen 233
Bereitstellungsdienste anpassen 239
Probleme? 240
6.6.2 Automatisierte Anpassung des Betriebssystems (Windows Setup) 242
Antwortdatei erstellen 242
Bereitstellungsdienste anpassen 245
6.6.3 Das Verfahren testen und prüfen 246
Der Domänenbeitritt gelingt nicht 247
Dialoge des Mini-Setups erscheinen 248
Wie bekommt der PC seinen Namen? 249
Wie bekommt der PC die Antwortdatei? 250
6.7 Computer vorab bereitstellen 251
6.7.1 PC bereitstellen 252
6.7.2 Weitere Möglichkeiten 255
6.7.3 Computer mit Active Directory-Werkzeug anlegen 256
6.8 PXE-Antwortrichtlinie und ausstehende Geräte 259
6.9 Ein eigenes WIM-Image installieren 267
6.10 Image-Pflege 267
6.10.1 WIM-Image mounten 269
6.10.2 Treiber verwalten 272
Vorhandene Treiber anzeigen 272
Treiber hinzufügen 273
Treiber löschen 275
6.10.3 Packages verwalten 275
6.10.4 Features aktivieren und deaktivieren 277
6.10.5 Image unmounten und Änderungen speichern 279
6.10.6 Das Ergebnis der Bemühungen 279
6.10.7 Treiber und Boot-Images 281
6.11 Treiber und Windows-Bereitstellungsdienste 282
6.11.1 Treibergruppe einrichten 283
6.11.2 Treiberpaket hinzufügen 287
6.11.3 Ein Blick in setupact.log 291
6.12 Multicastübertragungen 292
6.12.1 Multicastübertragung einrichten und konfigurieren 292
6.12.2 … und die Übertragung läuft 296

6.13 User State Migration Tool 299
6.13.1 USMT – simpel 299
6.13.2 USMT detailliert steuern 302
Wie werden die USMT-Werkzeuge gesteuert? 302
Was kann migriert werden? 303
6.14 Was ist mit »einfach drüberinstallieren«? 306
6.15 Weitere Anmerkungen zum Deployment 306

7 Aktivierung 309

7.1 Lizenztypen und Produkt-Keys 309
7.2 Volume Activation 2.0 311
7.2.1 Produktgruppen 311
7.2.2 Zeitfenster und Toleranzperioden 312
Aktivierung mit MAK-Key 313
Aktivierung mit KMS 314
7.2.3 RFM – Reduced Functionality Mode 315
7.3 VAMT 318
7.3.1 Clients konfigurieren 319
7.3.2 MAK-Keys verwalten 321
7.4 MAK – Multiple Activation Key 323
7.4.1 Aktivieren am PC 323
7.4.2 VAMT – MAK Independent Activate 325
7.4.3 VAMT – MAK Proxy Activate 326
7.5 KMS – Key Management Service 329
7.5.1 Funktionsweise 329
Der Activation Count 330
Produktgruppen 333
7.5.2 Installation 334
Windows Server 2008 und Windows 7/Vista als KMS-Host 334
Windows Server 2003 als KMS-Host 335
7.5.3 Achtung! 336
7.6 Fazit: MAK vs. KMS 337

8 Windows RE 339

8.1 (Standard-)Funktionalität 341
8.2 Win RE-Image erstellen und in WDS integrieren 343
8.2.1 Image erstellen 343

8.2.2 Integration in die Windows-Bereitstellungsdienste vornehmen ... 344
8.2.3 Test ... 345
8.3 Windows RE-Umgebung anpassen ... 347

9 Applikationen und Windows 7 ... 351

9.1 Application Compatibility Toolkit (ACT) ... 351
9.1.1 Installation ... 352
9.1.2 Daten sammeln ... 355
9.1.3 Analysieren – Community-Informationen ... 360
9.1.4 Analysieren – automatisch ermittelte Probleme ... 364
9.1.5 Analysieren – strukturiert selbst machen ... 365
9.1.6 Fazit ... 371
9.2 Windows 7 XP Mode und Windows Virtual PC ... 371
9.2.1 Voraussetzungen ... 372
9.2.2 Installation und Einrichtungen ... 373
9.2.3 Applikation installieren ... 377
9.2.4 XP Mode – Ein paar Nachteile ... 380
9.3 Windows Virtual PC im Allgemeinen ... 381
9.3.1 Die Neuerungen ... 381
9.3.2 Anlegen einer neuen VM und Konfiguration ... 382

10 Microsoft Desktop Optimization Pack ... 387

10.1 Enterprise Desktop Virtualization ... 388
10.2 Application Virtualization ... 389
10.3 Diagnostic and Recovery Toolset (DaRT) ... 391
10.4 Asset Inventory Service ... 393
10.5 Advanced Group Policy Management (AGPM) ... 393
10.5.1 Installation ... 394
Server ... 394
Client ... 396
10.5.2 Verwendung ... 398
10.5.3 Benutzer mit reduzierten Berechtigungen ... 403
10.6 System Center Desktop Error Monitoring ... 406

11 Gruppenrichtlinien ... 409

11.1 Anwendungsbeispiel ... 410
11.2 Richtlinien für Computer und Benutzer ... 413

11.3 Verteilung über Domänencontroller 415
11.4 Vererbung 420
11.5 Sicherheit und Vorrang 424
11.6 Filter 426
11.7 Abarbeitungsreihenfolge 427
11.8 Lokale GPOs 429
11.8.1 Das lokale Richtlinienobjekt bearbeiten 429
11.8.2 GPO für Administratoren und Nicht-Administratoren bearbeiten 430
11.8.3 Benutzerspezifische GPOs 430
11.9 Starter-Gruppenrichtlinienobjekte/Starter-GPOs 432
11.9.1 Anlegen 433
11.9.2 Anwenden 435
11.9.3 Sichern & Co. 436
11.10 ADM vs. ADMX 438
11.10.1 Kurze ADMX-Inspektion 439
11.10.2 Ablageorte und einen zentralen Speicherort einrichten 441
11.10.3 Windows 7-ADMX-Dateien in ältere Systeme kopieren 444
11.10.4 ADM-Dateien migrieren 445
11.10.5 Eigene ADMX-Dateien erstellen 449
11.11 Zuweisen und Bearbeiten von Gruppenrichtlinien 450
11.11.1 Gruppenrichtlinienobjekte anlegen und bearbeiten 452
11.11.2 Verknüpfungen hinzufügen und bearbeiten 456
11.11.3 Gruppenrichtlinienmodellierung 459
11.11.4 Gruppenrichtlinienergebnisse 464
11.12 WMI-Filter 466
11.13 Softwareverteilung mit Gruppenrichtlinien 470
11.14 Loopback-Verarbeitung 473
11.15 Gruppenrichtlinien-Voreinstellungen (Preferences) 474
11.16 AGPM – Advanced Group Policy Management 479

12 Sicherheit 481

12.1 Mein Lieblingsbeispiel in Sachen Sicherheit 486
12.2 Windows Server Update Services (WSUS) 489
12.2.1 Die Funktionsweise 490
12.2.2 Installation 491
Voraussetzungen installieren 491
WSUS installieren 492

12.2.3 Erstkonfiguration mit dem Assistenten 494
12.2.4 Konfiguration und Betrieb 501
Gruppen anlegen, Computer zuordnen 502
Computer überwachen 504
Synchronisierungen überwachen 504
12.2.5 Updates genehmigen 505
Automatische Genehmigung konfigurieren 505
Updates manuell genehmigen 507
12.2.6 Gruppenrichtlinie konfigurieren 509
12.2.7 Ein kurzer Blick auf den WSUS-Client 511
12.2.8 Mit Berichten arbeiten 513
12.3 Netzwerkrichtlinien- und Zugriffsdienste 515
12.3.1 Wie funktioniert NAP? 516
12.3.2 Netzwerkrichtlinienserver 520
12.3.3 Client vorbereiten 522
12.3.4 Ein mehrstufiges NAP-Konzept vorbereiten 524
Konfiguration auf dem zentralen Netzwerkrichtlinienserver 525
Konfiguration auf den RADIUS-Proxyservern 527
12.3.5 NAP für DHCP-Zugriff 529
Erster Installationsschritt und Netzwerkrichtlinienserver-Design 530
Einrichtung mit dem Assistenten 530
Was der Assistent alles getan hat 535
Verbindungsanforderungsrichtlinien 535
Netzwerkrichtlinien 536
Integritätsrichtlinien 539
Systemintegritätsprüfungen 539
Vorbereitung des DHCP-Servers 542
Aus Sicht des Clients 544
Betrachtung mit dem Netzwerkmonitor 549
12.3.6 Und die anderen Netzwerkverbindungsmethoden? 551
12.4 Windows-Firewall 551
12.4.1 Erster Kontakt 553
12.4.2 Grundkonfiguration 555
12.4.3 Regeln verwalten und definieren 557
Überblick 557
Eine Regel im Detail 559
12.4.4 Regel aktivieren (durch eine Applikation) 563
12.4.5 Eine Regel selbst erstellen 565
12.4.6 Mit Gruppenrichtlinien arbeiten 570

12.4.7 Gruppenrichtlinien vs. »individuelle Anpassungen« 575
12.4.8 Verbindungssicherheitsregeln 575
12.5 AppLocker 579
12.5.1 Funktion, Konfiguration und Anwendung – ein Beispiel 581
Voraussetzungen 581
Konfigurationswerkzeug 581
Standardregeln erzeugen 583
Erzwingung konfigurieren 586
Testen 587
12.5.2 Regeln erstellen 588
Regeln automatisch generieren 588
Regeln manuell erstellen 591
12.5.3 Konfiguration über Gruppenrichtlinien 593
12.6 Benutzerkontensteuerung (User Account Control) 595
12.7 BitLocker 597
12.7.1 Voraussetzungen 598
12.7.2 BitLocker auf einem einzelnen PC einrichten 600
12.7.3 BitLocker To Go auf einem einzelnen PC einrichten 605
Einrichten 605
Auf ursprünglichem PC öffnen 608
Auf einem Nicht-Windows 7-PC öffnen 609
12.7.4 AD-Integration 611
AD vorbereiten (Schema-Erweiterung durchführen) 612
Gruppenrichtlinien konfigurieren 612
TPM initialisieren 616
BitLocker aktivieren 620
12.7.5 Wiederherstellen 622
BitLocker-Kennwortwiederherstellungs-Viewer 623
BitLocker To Go-Kennwort vergessen 626
Verwendung eines Datenwiederherstellungs-Agenten (Data Recovery Agent) 629
12.8 Virenschutz 629

13 Mobile Clients 631

13.1 Gedanken zum Thema 632
13.1.1 Arbeitswelt – gestern heute und morgen 636
Gestern 637
Heute 637
Morgen 640

13.1.2 Kosten 642
13.2 DirectAccess 643
13.2.1 Funktionsweise 644
13.2.2 Einige Technologiegrundlagen 646
IPv6 und Tunnelmechanismen 646
IPSec 649
Namensauflösung und NRPT 649
Network Location Server 651
Zertifikate 651
13.2.3 Vorbereitende Maßnahmen 652
Domänencontroller und DNS-Server 652
PKI einrichten 652
Verteilungspunkt für Zertifikatssperrliste anlegen 654
Zertifikate anfordern und Auto Enrollment für Zertfikate 655
Sicherheitsgruppe anlegen 658
IP-Konfiguration der Server aktualisieren 658
IPv6- und IPv4-ICMP-Anforderungen zulassen 660
Network Locator Server vorbereiten 661
DirectAccess-Server vorbereiten 662
13.2.4 DirectAccess installieren und einrichten 663
DirectAccess-Verwaltungskonsole installieren 663
Ersteinrichtung mit der DirectAccess-Verwaltungskonsole 664
Monitoring 671
13.2.5 Ein wenig genauer hingeschaut … 672
13.2.6 Aus der Clientperspektive 676
IP-Konfiguration 676
NRPT 677
Registrierung im DNS 678
Zugriff auf das Unternehmens-LAN 679
Zugriff auf den DirectAccess-Client 680
13.2.7 Noch mehr DirectAccess 681
13.2.8 Die Sicherheit 681
13.3 BranchCache 681
13.3.1 Voraussetzungen 682
13.3.2 Funktionsweise 683
Verteilter Cache 683
Gehosteter Cache 685
13.3.3 Server konfigurieren 688

13.3.4 Clients konfigurieren ... 691
13.3.5 Hosted Cache ... 694
Konfiguration des Servers ... 694
Clientkonfiguration ... 696
13.3.6 Fazit ... 697
13.4 VPN Reconnect ... 697
13.5 Mobile Broadband ... 698

14 Suchen und Finden ... 701

14.1 Die Desktop-Suche ... 702
14.1.1 Funktion für den Anwender ... 703
14.1.2 Konfiguration über Gruppenrichtlinien ... 704
14.2 Search Federations ... 705
14.3 Bibliotheken ... 709
14.3.1 Dateifreigabe indizieren und zu Bibliothek hinzufügen ... 711
14.3.2 Anwenden ... 714

15 Mehrsprachige Umgebungen ... 717

15.1 Sprache manuell auf einem bestehenden Betriebssystem installieren ... 719
15.2 Multilingual von Anfang an ... 725
15.3 Profile ... 725

16 Client-Management mit System Center Configuration Manager 2007 R2 (SCCM) ... 727

16.1 Grundprinzipien ... 729
16.1.1 Standorte und (Server-)Rollen ... 729
16.1.2 Sammlungen ... 732
16.1.3 Pakete und Ankündigungen ... 733
16.2 Agenten ausrollen ... 734
16.2.1 Ermittlungsmethoden ... 734
16.2.2 Clientinstallationsmethoden ... 736
16.2.3 Clientagenten ... 737
16.3 Inventar und Berichte ... 738
16.3.1 Abfragen ... 739
Standardabfragen ... 739
Eigene Abfragen erstellen ... 739

16.3.2 Ressourcen-Explorer 742
16.3.3 Berichte 744
16.4 Softwareverteilung 748
16.4.1 Paketerstellung 748
Paket erstellen 749
Programm hinzufügen 753
Verteilungspunkte verwalten 755
16.4.2 Ankündigung erstellen 759
16.5 Betriebssystem verteilen 763
16.5.1 Referenz-PC vorbereiten 764
16.5.2 Ein Image mit PXE-Boot erfassen 765
Computer importieren 766
Tasksequenz erstellen 769
Tasksequenz ankündigen 772
PXE-Boot durchführen und Image erfassen 773
16.5.3 Einen neuen PC ausrollen 777
Betriebssystemabbild hinzufügen 778
Tasksequenz erstellen 779
Computer importieren und Ankündigung erstellen 785
Netzwerkboot durchführen und Image ausrollen 786
16.6 Anwendersupport 787
16.6.1 Fernsteuerung 788
16.6.2 Sonstige Hilfsmittel 790
16.7 Sonstige Funktionen des Configuration Managers 790

Index 793

Dareios und Parysatis hatten zwei Söhne, von welchen der ältere Artaxerxes, der jüngere Kyros hieß. Als nun Dareios krank danieder lag und vermutete, dass sein Leben zu Ende gehe, wünschte er, seine beiden Söhne um sich zu haben.
(Xenophon, Anabasis, Übersetzung von F.K. Hertlein)

1 Gedanken zum Buch

Mit dem oben genannten Satz beginnt die *Anabasis* von Xenophon (* um 426, † um 355 vor Christus). In einem Satz zusammengefasst, geht es in dem Werk darum, dass Xenophon die geschlagene griechische Expeditionsarmee von Kunaxa nach Byzanz führt. Es ist auch unter dem Titel »Der Zug der Zehntausend« bekannt, denn es wird beschrieben, wie ein für damalige Verhältnisse großer Heeresverband unter enormen physischen und psychischen Entbehrungen durch das kleinasiatische Hochland geführt wird.

Bei genauerem Nachdenken (und ein wenig Fantasie) gibt es durchaus Parallelen zum Thema dieses Buchs, nämlich dem Windows-Client im Unternehmen:

- Zu Fuß von Kunaxa nach Byzanz zu marschieren, ist an sich schon eine enorme Herausforderung.
- Wenn Sie 10 000 Personen über diese Strecke führen müssen, bekommt die Angelegenheit noch zusätzliche Schwierigkeitsgrade. Man bedenke etwa, dass eine einzelne Person immer irgendwo einen Schlafplatz und ein wenig Nahrung finden wird. Bei einer Gruppe von 10 000 ist das schon deutlich komplizierter. Ganz zu schweigen von der Eigendynamik, die in einer Gruppe herrscht, angefangen von Verzweiflung, Frustration bis hin zu Neid und Missgunst.

Die Parallele zu unserem Thema:

- Einen PC »gut« aufzusetzen, sodass alle Features eines modernen Betriebssystems wie Windows 7 optimal genutzt werden, ist nicht ganz trivial.
- Bei Dutzenden, Hunderten, Tausenden oder gar Zehntausenden PCs bekommt die Aufgabe eine ganz neue Dimension: Es ist nicht damit getan, dass Sie eine Installation vielfach duplizieren, sondern es wird viel komplexer: Allein schon die Frage, wie man Hunderte oder Tausende von Windows 7-Installationen

effizient aktiviert, bedarf schon einiger Überlegungen. Nachdem das griechische Herr sich in Marsch gesetzt hatte, musste Xenophon auch Diverses zur »Betreuung« seiner Soldaten unternehmen. Verpflegung, gesundheitliche Versorgung und Motivation sind nur drei der Aufgaben. Ebenso verhält es sich mit den PCs: Sind diese beim Anwender eingerichtet, geht es erst richtig los: Patches/Upgrades anwenden, Probleme beheben, Anwenderfragen beantworten – eine lange Liste wichtiger Aufgaben.

Moderne Clientbetriebssysteme sind darauf ausgerichtet, umfangreiche Unterstützung für das Deployment und Management zu bieten. Natürlich sind auch Aspekte wie eine einfach zu bedienende und komfortable Benutzeroberfläche wichtig, für Administratoren und Systemarchitekten sind aber eher die Hintergründe interessant, die für einen reibungslosen Betrieb sorgen.

Genau hier setzt dieses Buch an: Es zeigt »die Technik«, behält aber stets im Auge, dass Sie alles unter Umständen hundertfach oder tausendfach in Ihrer Clientumgebung durchführen müssen.

Bei vielen IT-Professionals schwingt, zumindest unbewusst und im Hinterkopf, das Gefühl mit, dass Server-Technologie komplizierte und spannende High-Tech ist, während die Beschäftigung mit den Clients eher ein fast etwas lahmes Thema ist, das ja auch »die Anfänger machen können«. Diese Gedanken sind aber Relikte aus den 90er-Jahren, als einem komplexen Netzwerkbetriebssystem ziemlich dumme DOS-Clients gegenüberstanden. Heute stehen die Clientbetriebssysteme dem Server in puncto Komplexität kaum nach – schließlich liegt eine umfangreiche gemeinsame Codebasis zugrunde. Die Herausforderung im Clientumfeld ist dann zunächst, dass Sie nicht nur wenige Server, sondern Dutzende, Hunderte oder Tausende Clients im Griff haben müssen. Und dann sitzen die Anwender nicht mehr artig in der Firma, sondern jetten mit den Clients um die ganze Welt. Die Anforderungen nach Mobilität und Sicherheit sind also ebenfalls zwingend zu erfüllen.

Der Betrieb der Clientlandschaft ist dann aber nicht »nur« eine Technikfrage, sondern stellt auch hohe Anforderungen an die Qualität der Prozesse, beispielsweise:

- Wie organisiert man die Auslieferung von neuen PCs?
- Wie kann man den Benutzern bei Störungen oder Fragen optimal helfen? Insbesondere geht es darum, das Problem schnell (!) dem richtigen Ansprechpartner zuzuleiten und die Bearbeitung zu kontrollieren.
- Wie kann man möglichst störungsfrei umfangreiche Software-Rollouts organisieren oder Hardware tauschen?

Dieses Buch ist in erster Linie ein »Technikbuch« und kein Buch über die Optimierung von IT-Prozessen. Trotzdem empfehle ich jedem Clientverantwortlichen, sich intensiv um Dokumentation und Optimierung der Prozesse zu kümmern – Stichwörter wie *ITIL* sollten zu Ihrem täglichen Denken gehören.

Ich erhalte von Ihnen, liebe Leser, häufig E-Mails mit der Nachfrage, ob ich Ihnen in einem Projekt helfen, ein Konzept überprüfen, einen Vortrag bei einer Veranstaltung halten oder dergleichen für Sie tun kann. Ja, grundsätzlich kann ich das natürlich machen – sehr gern! Wenn Sie mit mir in Kontakt treten möchten, freue ich mich über Ihre E-Mail an *ulrich@boddenberg.de*.

Sie sind auch herzlich eingeladen, meine Website *http://www.boddenberg.de* zu besuchen.

Vielen lieben Dank an meine Frau Ilona und unsere Amy für die mentale Unterstützung bei diesem Projekt.

Weiterhin bedanke ich mich bei meinen Kunden, die ihre Probleme mit mir teilen und somit wertvolle Hilfe dazu leisten, dass dieses Buch den »richtigen« Praxisbezug hat.

Dortmund,
Ulrich B. Boddenberg

Der ältere war nun eben bei ihm; den Kyros aber rief er zu sich aus der Provinz, über die er ihn zum Statthalter eingesetzt hatte, wie er ihn denn auch zum Befehlshaber aller Truppen ernannt hatte, deren Sammelplatz die Ebene von Kastalos ist.

2 Aufbau des Buchs

Dieses Buch über Windows 7 richtet sich in erster Linie an Administratoren, Systemarchitekten, IT-Verantwortliche und Entscheider.

Diese Personengruppe braucht kein Anwenderbuch, in dem erklärt wird, wie man die Bildschirmauflösung umstellt oder wie man mit Windows 7 eine DVD besser abspielen kann. Vielmehr möchte ich zeigen, welche Möglichkeiten das neue Clientbetriebssystem im Unternehmenseinsatz bietet und wie man diese implementiert.

Diese Zielsetzung bedingt, dass ein weit größerer Bereich betrachtet wird, als nur das Betriebssystem selbst. Ich habe diesen Leitgedanken des Buchs auf Abbildung 2.1 visualisiert:

- Im Zentrum steht natürlich das Windows 7-Betriebssystem mit seinen Möglichkeiten und Fähigkeiten – das wird durch den inneren Kreis symbolisiert.
- Um das Betriebssystem herum gibt es im professionellen Einsatz viele Aufgabenstellungen, die eine breitere Betrachtung erfordern:
  - Da sind beispielsweise die Aufgaben *Management, Deployment* und *Sicherheit* zu nennen.
  - Ein wichtiges Thema ist die mobile Nutzung, die auch eine eingehende Betrachtung der Themen *Internet-Gateway* und *Netzwerk* erforderlich macht.
  - Ein Betriebssystem ohne *Applikationen* wäre wie ein Auto ohne Gaspedal. Daher spielen Applikationen und insbesondere deren Kompatibilität zu Windows 7 natürlich auch eine wichtige Rolle.
  - Das Management des Betriebssystems ist natürlich eine ganz wesentliche Aufgabe, die zu einem nicht geringen Teil mittels *Gruppenrichtlinien* erledigt wird. Das Thema dieses Buchs ist aber auch der *System Center Configu-*

ration Manager (SCCM) – als exemplarisches Beispiel für ein modernes Client-Management-System.

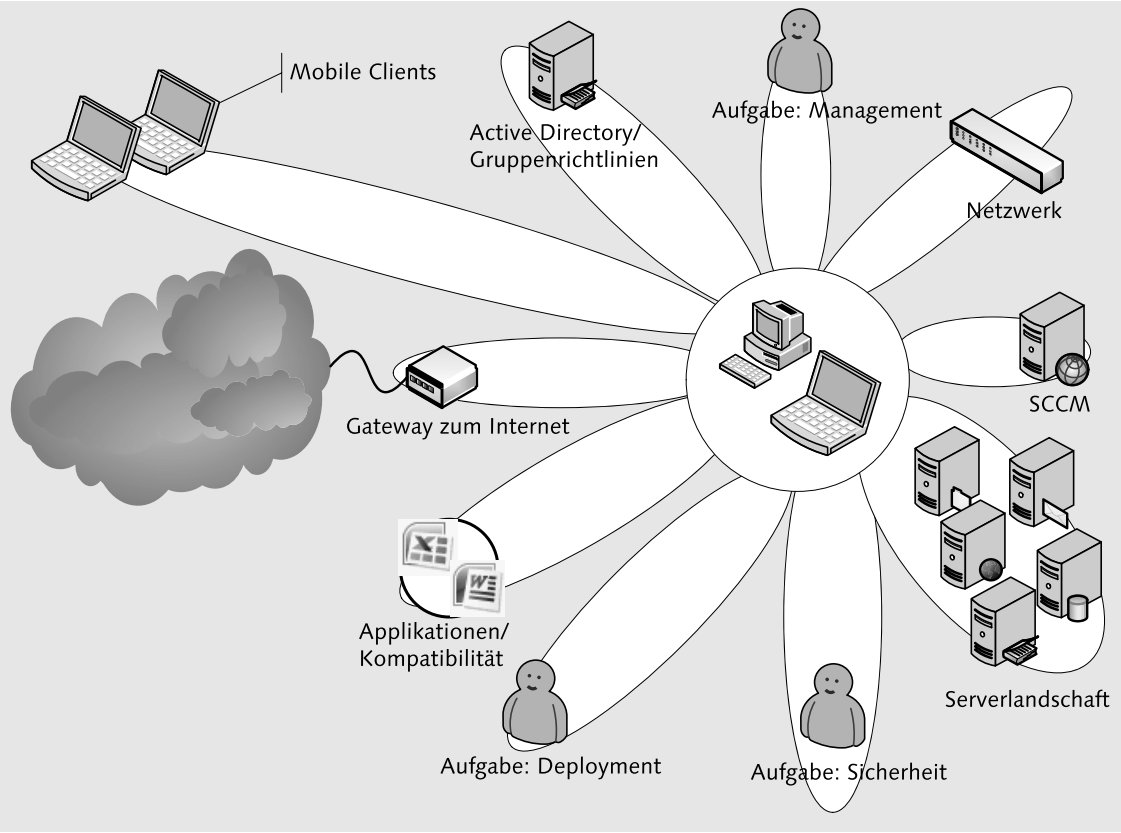


Abbildung 2.1 Die Themen dieses Buchs in grafischer Darstellung

Mein Buch betrachtet Windows 7 in einer umfassenden Darstellung, denn ohne das »Drumherum« kommen die wahren Fähigkeiten des neuen Betriebssystems aus Redmond im betrieblichen Einsatz nur sehr begrenzt zur Geltung.

Erst im Zusammenspiel mit dem Rest der Umgebung spielt Windows 7 seine Stärken aus. Ich bin sicher, dass Sie feststellen werden, dass es viele Aspekte mitbringt, die das Unternehmen wirklich nach vorn bringen, und dass das neue Windows so echte Mehrwerte für das Unternehmen bietet – und vom *Business Value* handelt dann auch das erste Kapitel: Gemeinsam mit Ihnen werde ich da die Frage erörtern, warum wir überhaupt über ein neues Betriebssystem nachdenken und wie es zum Unternehmenserfolg beitragen kann.

Hier noch ein wenig Statistik, mit der die Schwerpunkte des Buchs anhand von harten Zahlen beschrieben werden:

- Den seitenmäßig umfangreichsten Teil machen die Themen Deployment und Aktivierung aus, nämlich ein bisschen mehr als 19 %.
- Es folgt das Thema Sicherheit mit ein bisschen weniger als 19 % des Umfangs.

- Im Kapitel zum Technologieüberblick bespreche ich diverse Grundlagen, die Sie kennen sollten. Dass dieses Kapitel knapp 15 % des Umfangs ausmacht, zeigt, wie vielfältig die Welt des Clientbetriebssystems ist.
- Bei den heutigen Business-Anforderungen ist die mobile Nutzung zunehmend wichtig. Das schlägt sich in einem Textanteil von ca. 10,4 % des Umfangs dieses Buchs nieder.
- Ein wesentliche Rolle beim Management spielen die Gruppenrichtlininen: Sie sorgen für 9,7 % des Umfangs.

Die Aufstellung soll natürlich nicht suggerieren, dass die anderen Themen weniger wichtig seien – sie sind nur nicht ganz so umfangreich. Allein schon am Umfang lassen sich also die wesentlichen Themen ablesen:

- Deployment
- Management
- Sicherheit
- Mobilität

Ich denke, dass genau diese vier Themen auch für Ihr Business die wesentlichen Fragestellungen sind, oder?

Es reiste also Kyros zu ihm und nahm den Tissaphernes als seinen Freund, wie er meinte, mit sich. Auch begleiteten ihn auf dieser Reise dreihundert Hopliten von seinen griechischen Truppen, samt deren Anführer, dem Parrhasier Xenias.

3 Business Value

Da Sie sich dieses Buch gekauft oder ausgeliehen haben oder es vielleicht einfach nur durchblättern, haben Sie ein mehr oder weniger starkes Interesse an Windows 7. Nun ist es aber vermutlich so, dass auch Ihr Unternehmen bzw. Ihre Organisation kein Geld übrig hat, um »nicht notwendige« IT-Projekte (um es mal vorsichtig auszudrücken) durchzuführen. Irgendwann werden Sie also eine Entscheidungsvorlage ausarbeiten müssen, in der klipp und klar begründet ist, warum Geld für die Einführung von Windows 7 ausgegeben werden muss.

Für einen IT-Menschen ist es zwar irgendwie ganz einleuchtend, dass man nach einigen Jahren das Clientbetriebssystem aktualisiert. Rein statistisch gesehen wird in Ihrem Unternehmen vermutlich *Windows XP* oder *Windows 2000* im Einsatz sein – im letztgenannten Fall feiert das Clientbetriebssystem also bald seinen 10. Geburtstag. Das allein ist aber nun kein Grund fürs Geldausgeben. Warum verwendet man eigentlich nicht einfach Windows NT4 auf den Desktops weiter? Oder wenn nun schon *Windows 2000 Workstation* oder gar *XP professional* in Betrieb sind, könnten die doch problemlos noch die nächsten zehn Jahre ihren Dienst tun! Verdient das Unternehmen etwa dadurch mehr Geld, dass für viel Geld das Betriebssystem erneuert wird? Nein, dann lassen wir es doch besser bleiben. Full Stop!

Nun, es gibt natürlich jede Menge gute Gründe, warum es sinnvoll ist, über ein neues Clientbetriebssystem nachzudenken. Ich würde hier aber dringend empfehlen, die Beschäftigung mit dem Thema direkt ein wenig ganzheitlicher und nachhaltiger zu gestalten und nicht »nur« ein wenig auf die Betriebssystem-Technik zu schauen, sondern auch Serviceprozesse, Servicequalität, das Management der Umgebung und weitere Business-Anforderungen wie Mobilität und Sicherheit in die Betrachtung einzubeziehen. Um es an dieser Stelle ruhig etwas provokant zu sagen: Wenn Sie zwar Ihre Windows-2000-Workstation-Systeme mit mehr oder weniger großem Aufwand durch Windows 7-Systeme ersetzen, an-

sonsten aber alles beim Alten bleibt, haben Sie nur wenig gewonnen. Sie haben natürlich ein paar Probleme gelöst, beispielsweise:

- Sie setzen nicht mehr ein Betriebssystem ein, für das Microsoft keinen Support mehr anbietet.
- Sie brauchen sich keine Sorgen mehr zu machen, dass es zu dem in Ihrem Unternehmen großflächig eingesetzten Betriebssystem keine Hardwareunterstützung gibt, sprich, dass keine neuen PCs mehr angeschafft werden können oder zumindest die Auswahl schwierig ist.

Wenn das aber Ihre einzigen Argumente für das neue Betriebssystem sind, dann verschenken Sie einerseits recht viel Potenzial und tragen andererseits auch zum »IT-Frust« von eher kaufmännisch-orientierten Entscheidern: »Die IT tut dauernd irgendetwas, verbraucht viel Geld, aber wirkliche Verbesserungen gibt's nicht!«

Wir werden uns in diesem Kapitel mit einigen Argumentationslinien befassen. Vorher gibt es aber noch einen kurzen rückwärtsgerichteten Blick. Ich finde, dass ein Blick in die Vergangenheit hilft, die Sinne für zukünftige Anforderungen zu schärfen …

3.1 Ein kurzer Blick zurück

Ich möchte Sie zunächst auf eine kleine Zeitreise mitnehmen und Ihnen einige frühere Versionen des Windows-Betriebssystems nebst einer kurzen »historischen Einordnung« zeigen.

3.1.1 Windows 1, 2 und 3

Das erste Windows-Betriebssystem war, wie sollte es auch anders sein, Microsoft Windows Version 1.01 und erschien im Jahre 1985. Auf Abbildung 3.1 sehen Sie den Startbildschirm.

Die Windows-Version 1.01 habe ich selbst nie zu sehen bekommen, was an zwei Dingen lag:

- Ich machte damals (übrigens im Alter von 14 Jahren) meine ersten Gehversuche in der Computerwelt mit einem C64, später dann mit einem Atari ST.
- Es gab wenig »Killeranwendungen«, die die Installation von Windows 1.01 vorausgesetzt hätten. Ich nehme daher an, dass die wenigsten Leser dieses Buchs diese erste Windows-Version wirklich produktiv genutzt haben. Textverarbeitung und Tabellenkalkulation ging damals auch noch ganz gut unter DOS.

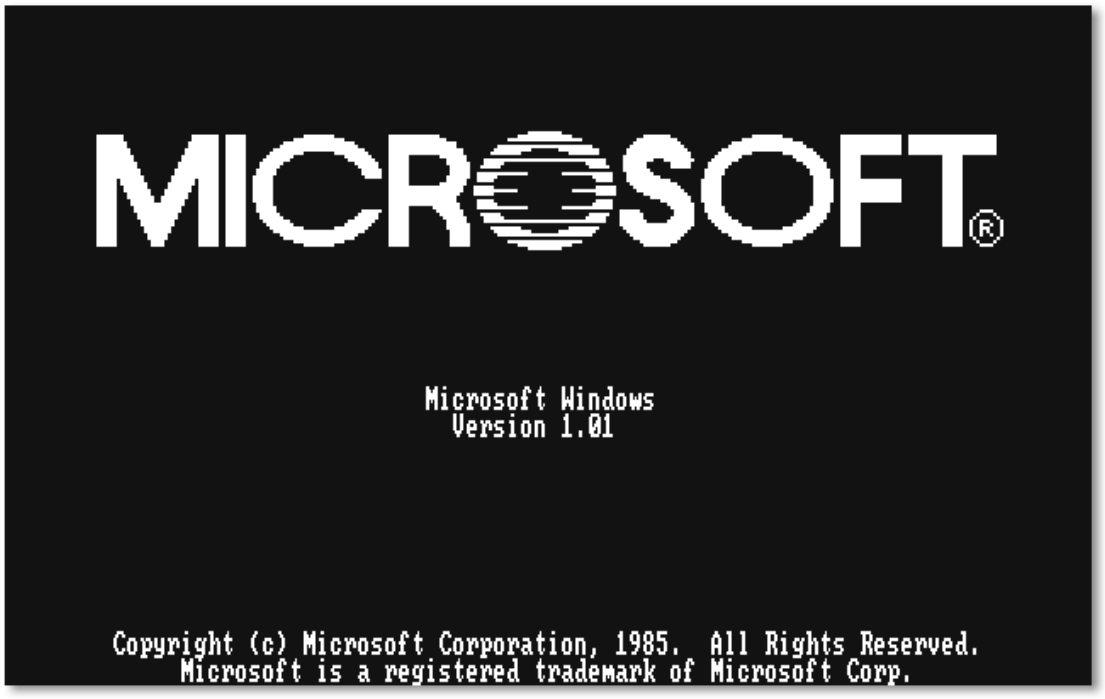


Abbildung 3.1 Der Startbildschirm von Windows 1.01 (Quelle: www.winhistory.de)

Apropos DOS: Dieses lag damals in der Version 3.1 vor und bildete die Grundlage für Windows 1.01. Auf Abbildung 3.2 sehen Sie einen Dateimanager, der auch treffend mit MS-DOS Executive überschrieben ist. Dieser »Dateimanager« ist übrigens die Hauptoberfläche von Windows 1.01 gewesen – der Programm-Manager kam erst mit Version 3.

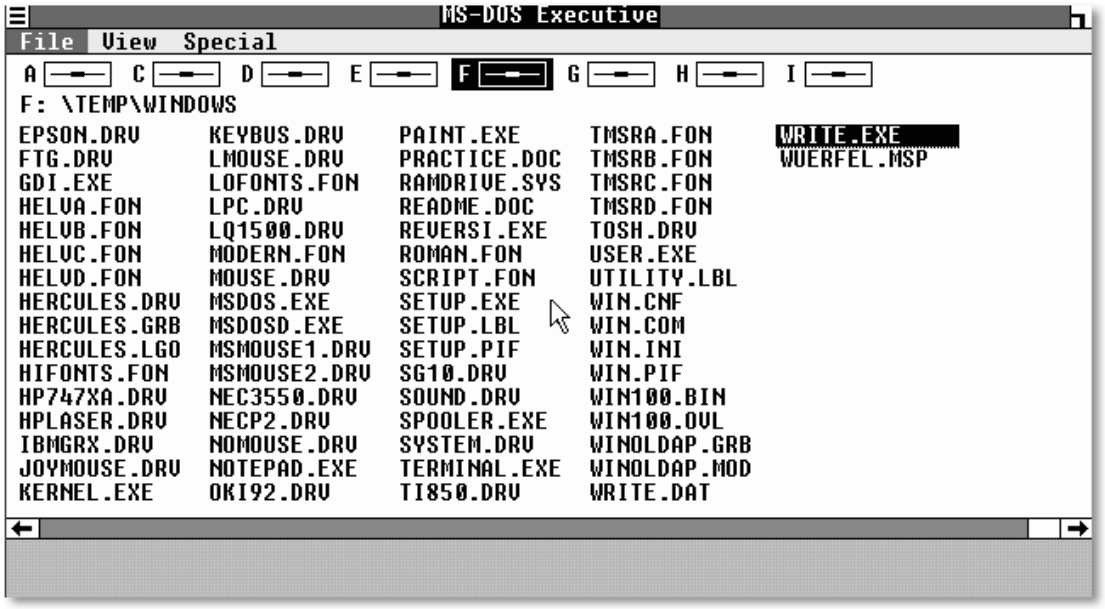


Abbildung 3.2 Die Hauptoberfläche von Windows 1.01 (Quelle: www.winhistory.de)

Unabhängig davon, ob die Benutzer mit Windows arbeiteten oder nicht, war das Aufgabengebiet recht eng umrissen:

- Der Personal Computer war eine bessere elektrische Schreibmaschine.
- Der PC wurde für die ersten Ansätze der Tabellenkalkulation verwendet.
- Eventuell diente er als Terminal für Host-Anwendungen.

Ein LAN mit zentralen Servern war damals etwas, was größeren Firmen vorbehalten war, im Allgemeinen war der nicht vernetzte Einzelplatz-PC der Stand der Technik. Wenn zwei Kollegen Dokumente austauschen mussten, ging das eben auch auf Diskette.

Die erste Windows-Version, mit der ich gearbeitet habe, war die Version 2.03, die im Jahre 1987 erschien. Die Anwendung war damals *Aldus Pagemaker*, eine Desktop-Publishing-Software. Diese Software, die aufgrund ihrer Aufgabe nicht im Textmodus laufen konnte, nutzte Windows vermutlich vor allem deshalb, weil Windows eine Abstraktion der Grafikkarte mitbrachte. Wer grafische Anwendungen unter DOS programmiert hat, der weiß, dass unterschiedliche Grafikkarten mit unterschiedlichen Fähigkeiten zu berücksichtigen waren. Simpel ausgedrückt: Wer viele Grafikkarten unterstützen wollte, hatte viel Arbeit. Mit Windows konnte man die eingebauten Grafikfunktionen verwenden ohne von direkt mit der Grafikkarte zu tun zu haben – ein gigantischer Vorteil.

Gleiches gilt natürlich auch für alle anderen angeschlossenen Geräte wie Maus, Tastatur, Drucker, Schnittstellen etc.

Der wirkliche »Durchbruch« kam dann mit Windows 3.0, das im Jahr 1990 erschien. 1992 folgte *Windows 3.1*, und 1993 erschien *Windows for Workgroups 3.11*. Mit Windows 3 wurde die Oberfläche deutlich verändert, es tauchte erstmalig der Programm-Manager auf. Entscheidend war aber, dass es mittlerweile jede Menge nützliche Anwendungen für Windows gab. Man konnte die komplette Büroarbeit mit Windows-Applikationen erledigen. Zugegebenermaßen waren branchenspezifische Applikationen häufig DOS-Anwendungen, aber die Anwender forderten Windows-Applikationen, woran die Hersteller auch mit mehr oder weniger starkem Engagement arbeiteten.

Zu Zeiten von Windows 3 waren auch lokale Netzwerke nichts Außergewöhnliches mehr, und auch kleinere Firmen vernetzten ihre PCs. Der Sinn und Zweck der Vernetzung war aber primär die Ablage von Dateien auf einem zentralen Server und die gemeinsame Verwendung von teuren Ressourcen wie Laserdruckern. Mit anderen Worten: Der PC war in erster Linie eine bessere Schreibmaschine – jetzt mit Netzwerkanschluss.

Mit Windows for Workgroups (WfW) gab es eine Peer-to-Peer-Lösung, die ohne einen dedizierten Server auskam. Rückwirkend betrachtet, hat WfW dem Thema »Computervernetzung in kleinen Umgebungen« ungeheuren Vorschub geleistet – auch wenn sich einem heute noch die Zehennägel bei dem Gedanken aufrollen, dass ein einfacher Selbstbau-PC den lebensnotwendigen Datenbestand eines kleinen Mittelständlers trug – ohne RAID, ohne vernünftige Sicherung und ohne Desasterkonzept.

3.1.2 Windows NT kommt (3.1 bis 3.51)

Im Sommer 1993 erschien *Windows NT 3.1 Workstation*. Auch wenn die praktischen Auswirkungen für die IT-Welt zunächst eher gering waren, war es zumindest ein technologischer Paukenschlag: Unter der grafischen Oberfläche werkelte kein DOS, es war also wirklich ein eigenständiges Betriebssystem entstanden. Mit der DOS/Windows-3.11-Kombination hat Windows NT 3.1 Workstation lediglich die grafische Oberfläche gemeinsam; Abbildung 3.3 zeigt den wohlbekannten PROGRAM MANAGER.

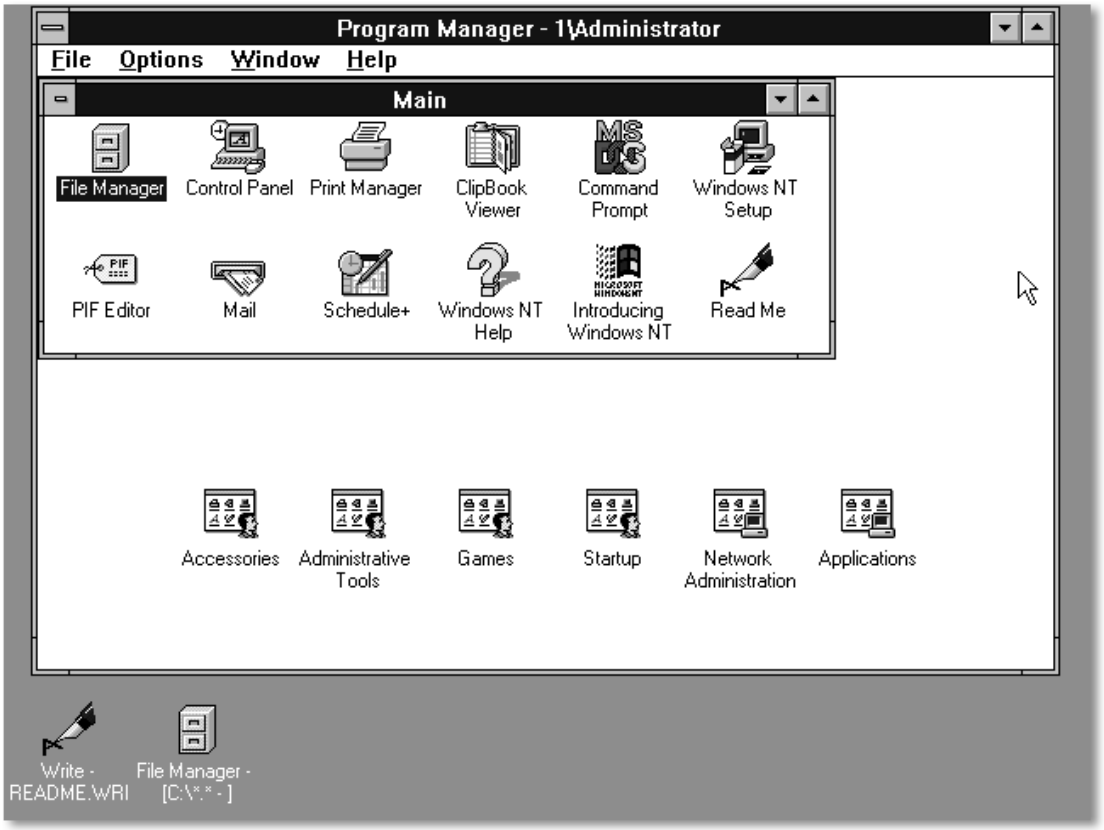


Abbildung 3.3 Die Oberfläche von Windows NT 3.5 Workstation (Quelle: www.winhistory.de)

Im Herbst 1994 (NT 3.5) und Sommer 1995 (NT 3.51) kamen dann die Folgeversionen, die allmählich auch eine gewisse Bedeutung im Markt erlangten. NT 3.1 war zwar verfügbar und grundsätzlich auch ein gutes Produkt, aber bekanntlich brauchen neue Konzepte ja eine Weile, bis sie wirklich Massenware werden. Wer einmal NT 3.1 installiert hat, weiß, dass das auch nicht so ganz trivial war: Abgesehen von einer sehr ansehnlichen Menge von Disketten, von denen dann garantiert eine nicht gelesen werden konnte, war das neue Betriebssystem nicht unbedingt mit reicher Treiberunterstützung gesegnet. NT 3.5 und NT 3.51 waren dann zumindest schon so etabliert, dass zumindest jeder Marken-PC mit diesem Betriebssystem betrieben werden konnte.

3.1.3 Windows NT 4 – Der Durchbruch

Ohne jetzt pathetisch werden zu wollen: *Windows NT 4 Workstation* kann man wohl getrost als den Durchbruch der NT-Technologie bezeichnen. Im Spätsommer 1996 kam diese Version auf den Markt, die wohl eine der langlebigsten Betriebssystemversionen überhaupt ist. Auch heute (im Herbst 2009) habe ich noch viele Kunden, die Windows NT 4 sowohl im Client- als auch im Serverbereich einsetzen – 13 Jahre ist eine phänomenale Einsatzdauer für ein Betriebssystem.

Auf den ersten Blick fällt Windows NT4 natürlich durch die an Windows 95 angelehnte Oberfläche auf (Abbildung 3.4). Es gibt keinen Program Manager mehr, sondern Ausklappmenüs und einen Start-Button, hübschere Symbole und dergleichen mehr.

Wenn auch aus Sicht der Anwender die Oberfläche der Hauptunterschied gewesen sein mag, ist der wesentliche Punkt bei NT4 eher die strategische Bedeutung: Mit dieser Version war die NT-Technologie wirklich nachhaltig im Markt angekommen. Um die Jahrtausendwende gab es kaum ein mittleres oder größeres Unternehmen, das nicht auf den Anwender-PCs Windows NT4 eingesetzt hätte. Windows 95, 98, 98SE (Second Edition) und ME haben nie eine nennenswerte Verbreitung in den Unternehmen gefunden. Letztendlich war das von Microsoft ja auch so gewollt:

- Die Non-NT-Betriebssysteme, also Windows 95, 98, 98SE und ME wurden für den Privatbereich positioniert.
- Für Business-Anwendungen wurden die NT-Betriebssysteme empfohlen.

Windows NT war (und ist) ein gutes Betriebssystem – sonst gäbe es nicht noch immer produktiv laufende Installationen. Es hat aber auch diverse Nachteile, die in der Praxis mehr oder weniger unangenehm waren:

- Der Treibersupport war immer recht kritisch.
- NT4 war recht umständlich zu installieren und zu warten.
- NT4 auf Notebooks ist ziemlich katastrophal gewesen.

Abbildung 3.4 Die Windows-NT 4-Linie verwendete die Windows 95-Optik. (Quelle: www.winhistory.de)

Wer heute noch NT4 einsetzt, hat unter anderem mit diesen Problemen zu kämpfen:

- NT4 läuft nicht mehr auf moderner Hardware, insbesondere wegen fehlender Treiber.
- Moderne Softwareprodukte laufen nicht mehr auf NT4, beispielsweise *Office 2007*, *Internet Explorer 7* oder *8*.
- Etliche Technologien stehen nicht für die NT4-Plattform zur Verfügung, beispielsweise die aktuellen Versionen des *.NET Frameworks* nebst Erweiterungen wie die *Windows Communications Foundation* (WCF) oder die *Windows Presentation Foundation* (WPF). Allein hierdurch können viele moderne Anwendungen nicht mit NT4 verwendet werden.
- NT4 kennt das *Active Directory* nicht, sodass beispielsweise Gruppenrichtlinien nicht verwendet werden können.
- Nicht zuletzt ist der Support seit Jahren ausgelaufen. Hierdurch sind einerseits keine Support-Anfragen bei Microsoft möglich, andererseits gibt es keine Updates/Patches mehr. Letzteres bedeutet unter anderem, dass Sicherheitslücken nicht mehr geschlossen werden.

3.1.4 Windows 2000 Professional

Im Februar 2000 kam die nächste NT-Generation auf den Markt, und zwar gleichzeitig mit einer Desktop- und einer Server-Variante. Das Betriebssystem meldet sich zwar intern als *Version 5*, hieß auch in der Betaphase *Windows NT5*, erreichte den Markt dann aber schließlich als *Windows 2000*. Der Hinweis auf die zugrunde liegende NT-Technologie im Startbildschirm (Abbildung 3.5) war wohl als Qualitätsmerkmal gedacht und sollte Sicherheit vermitteln und Kompatibilität signalisieren. In der Tat konnten Applikationen, die auf Windows NT problemlos liefen, auch unter Windows 2000 ausgeführt werden.

Windows 2000 beseitigte einige üble NT-Eigenschaften, wie beispielsweise die miserable Hardwareerkennung, führte eine vernünftige Unterstützung von mobilen Geräten ein und war insgesamt stabiler als Windows NT.

Vergessen wir ebenfalls nicht, dass Microsoft mit der *Windows 2000*-Generation deutlich im Bereich der Verwaltbarkeit nachgelegt hat: Hier wäre insbesondere das Active Directory zu nennen, in dessen Schlepptau auch Funktionen wie die Gruppenrichtlinien eingeführt worden sind.

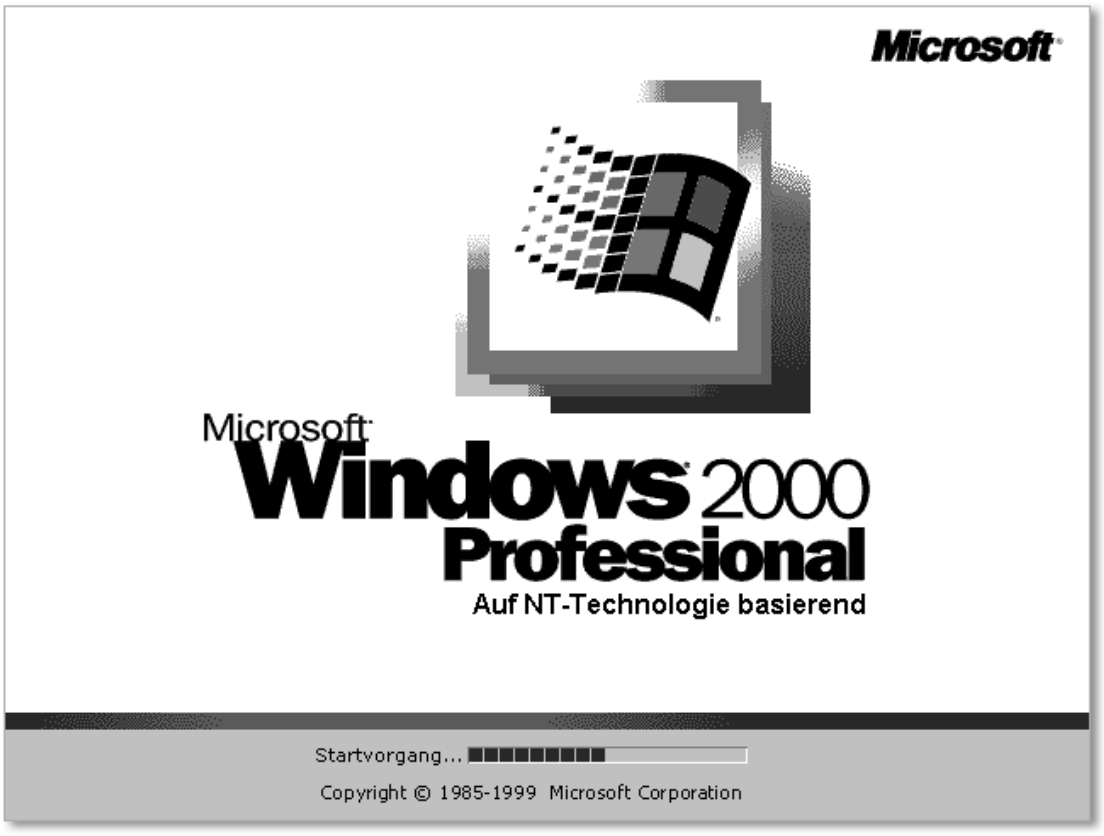


Abbildung 3.5 Der Startbildschirm von Windows 2000 – »Auf NT-Technologie basierend« (Quelle: www.winhistory.com)

3.1.5 Windows XP

Im Herbst 2001 beglückte Microsoft den Markt mit Windows XP. Dieses Betriebssystem ist im Grunde genommen ein optimiertes *Windows 2000 Professional*, was man auch an der Versionsnummer erkennt: Sie lautet 5.1.

Gegenüber Windows 2000 gab es zwar diverse Erweiterungen, die Versionsnummer deutete aber an, dass es sich nicht um eine vollkommen umgekrempelte Betriebssystemversion handelte. Allerdings gab es noch eine weitere »strategische« Bedeutung: Mit Windows XP wurden erstmalig die NT-Linie und die *Windows 9x*-Linie zusammengeführt. Windows XP hat so gesehen also zwei »Ahnen«; das zeigt sich auch in den beiden Editionen:

- *Windows XP Home*: Dies war die Version für zu Hause, die etwas eingeschränkt war und beispielsweise kein Domänenmitglied werden kann.
- *Windows XP Professional*: Dies war die Version für den Business-Einsatz in Windows-Netzen.

Windows XP war einerseits optisch verbessert (Abbildung 3.6), andererseits gab es auch eher technische Erweiterungen.

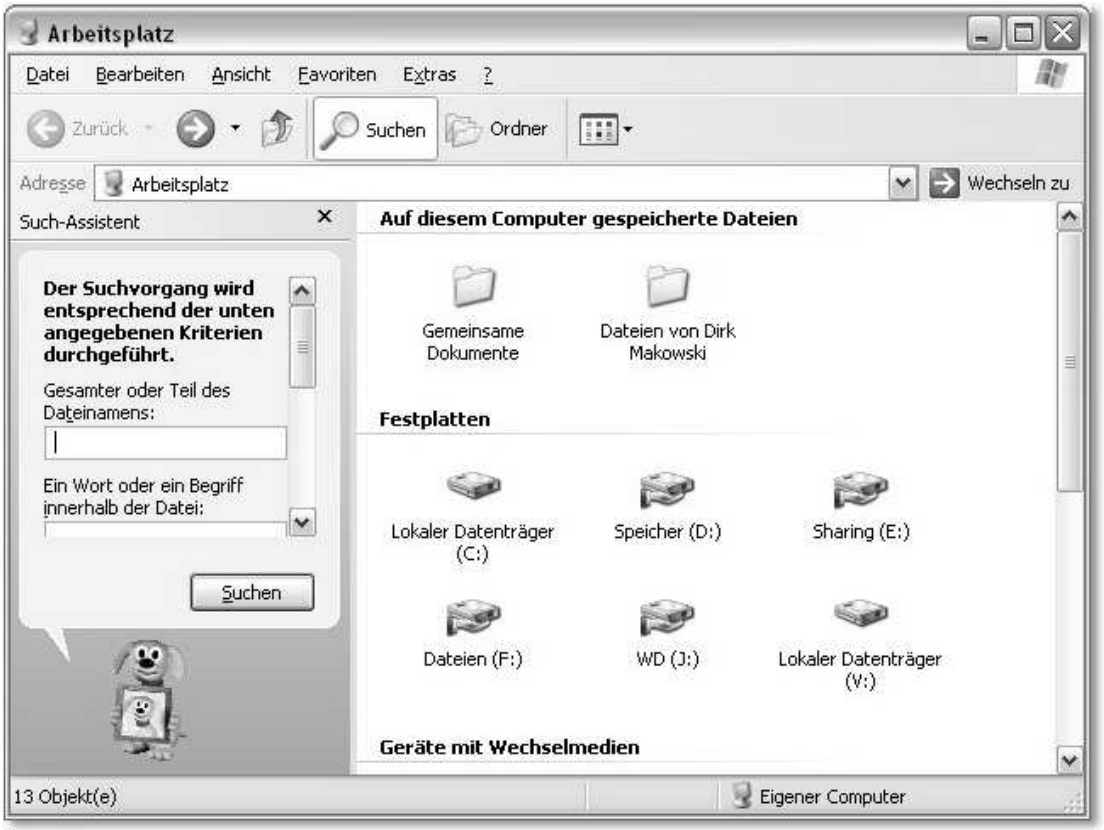


Abbildung 3.6 Windows XP war optisch noch ein wenig bunter als Windows 2000. (Quelle: www.winhistory.de)

- Das Treibermodell war optimiert worden.
- Es gab zwecks Optimierung der Verwaltung mehr Gruppenrichtlinien.
- Stabilität und Performance waren optimiert worden.

Windows XP war übrigens das erste Microsoft-Desktop-Betriebssystem, das auch in einer x64-Version verfügbar war.

3.1.6 Windows Vista

Windows Vista, das sich als *Version 6* meldet, erschien in Deutschland Ende 2006. Vista ist nun nicht so erfolgreich gewesen, wie Microsoft es geplant hatte: Von Anfang an war in der Presse zu lesen, dass viele Unternehmen Windows Vista auslassen und direkt auf den Nachfolger warten wollten. Hierfür gab es diverse Gründe: Sie begannen bei hohen Hardwareanforderungen, reichten über Kritik an der Oberfläche und endeten bei Problemen mit der Kompatibilität von Applikationen.

Anzumerken wäre, dass diejenigen meiner Kunden, die Vista eingeführt haben, insgesamt eher positive Erfahrungen gemacht haben. Trotzdem beobachte ich auch bei meinen Kunden den klaren Trend, Vista auszulassen und sich direkt auf Windows 7 zu stürzen.

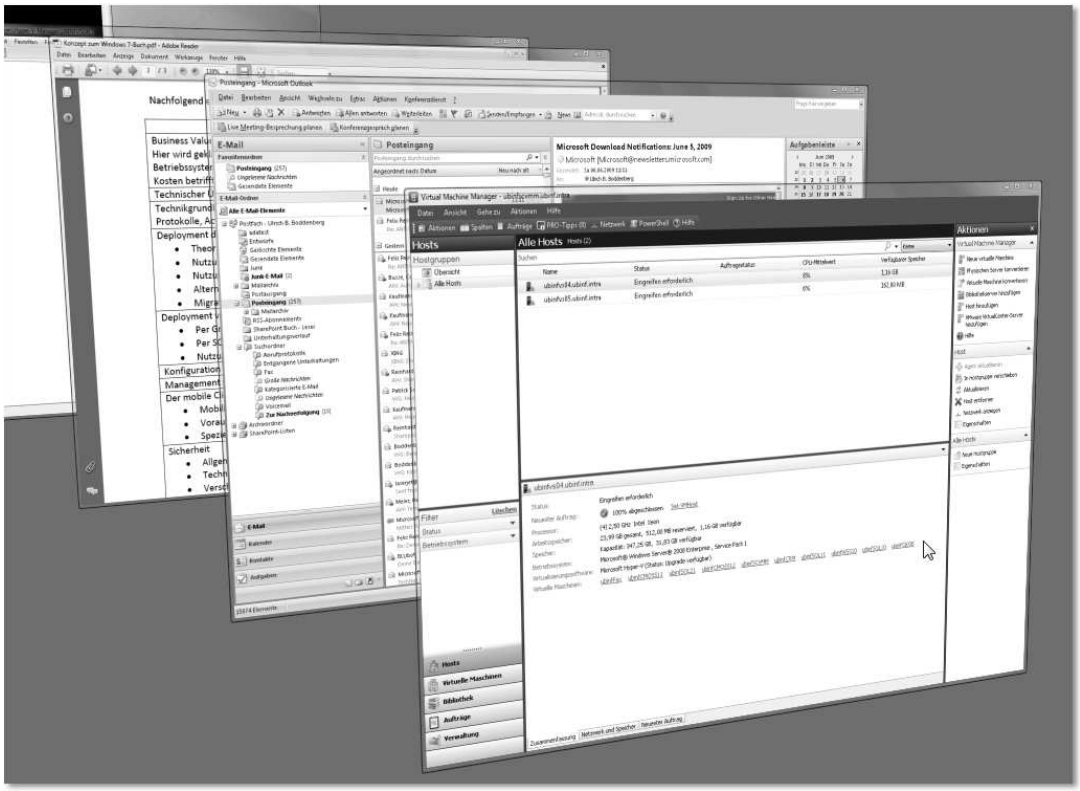


Abbildung 3.7 Das »Flippen« ist nur einer von vielen optischen Effekten von Windows Vista. Unter der Haube steckt diverse neue Technologie.

Dabei gibt es durchaus vielfältige Anforderungen, die Vista bedienen konnte, angefangen von einer modernen Oberfläche (Abbildung 3.7), über zusätzliche Sicherheitsfunktionen und bessere Möglichkeiten von Deployment und Verwaltung bis hin zu einer modernen Gesamtarchitektur.

Falls Sie in Ihrem Unternehmen bzw. Ihrer Organisation bereits Vista implementiert haben, gibt es wenig Grund zum Verdruss: Viele wesentliche Probleme, die Sie vermutlich im Bereich der Applikationskompatibilität lösen mussten, wären Ihnen auch begegnet, wenn Sie direkt auf Windows 7 gegangen wären. Insofern dürfte auch ein »schleichender« Tausch von Windows Vista gegen Windows 7 vergleichsweise einfach zu machen sein.

3.2 Gründe für ein neues Betriebssystem

Untersuchen wir nun die Gründe für den Einsatz eines neuen Betriebssystems. Anders gesagt lautet die Frage: Warum sollte man eines der zuvor genannten Betriebssysteme gegen Windows 7 tauschen?

Wie ich bereits zu Beginn des Kapitels erläutert habe, werden Sie sich irgendwann dieser Frage stellen und Ihrem Boss gute Gründe präsentieren müssen, warum es das Unternehmen nach vorn bringt, wenn mehr oder weniger viel Geld in die Desktop-Infrastruktur investiert wird. Die Reihenfolge, in der die Aspekte genannt sind, stellen keine Wertung dar, die Gewichtung dürfte für jedes Szenario individuell sein.

3.2.1 Bedarf an einer modernen Plattform

Dies ist in erster Linie ein Technikbuch, insofern möchte ich mit diesem Aspekt beginnen. Bestimmt können Sie sich noch mehr oder weniger gut an DOS erinnern? Das war ein Betriebssystem, das wirklich nur eine Aufgabe hatte, nämlich eine simple »Ablauf-Umgebung« für Programme bereitzustellen. Selbstverständlich stellte DOS einige Funktionen bereit, mit deren Hilfe ein solches Programm beispielsweise eine Datei von der Festplatte lesen, ein Zeichen auf den Bildschirm bringen oder eine Tastatureingabe erhalten konnte – viele andere Möglichkeiten gab es dann nun aber auch nicht. Wenn Sie einen Blick auf Abbildung 3.8 werfen, sehen Sie, was ich meine: Windows 7 bringt eine große Zahl von unterschiedlichen Features mit, die von Benutzern und Applikationen genutzt werden können. Ich spreche nicht davon, dass das mitgelieferte *MS Paint* nun eine modernere *Ribbon*-Oberfläche hat (das Vista-Paint hatte das übrigens noch nicht) oder dass nun standardmäßig ein Schachprogramm (*Chess Titans*) vorhanden ist.

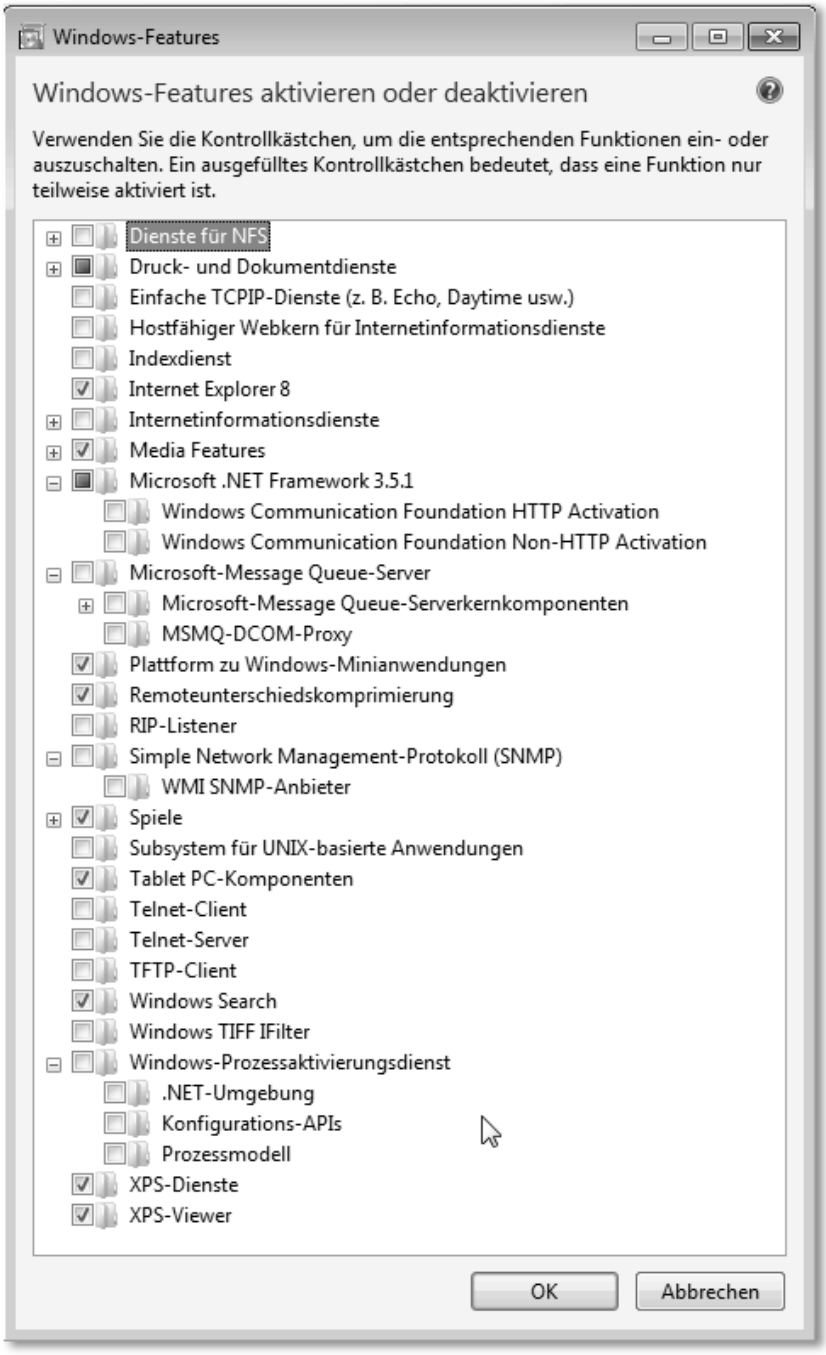


Abbildung 3.8 Windows 7 bringt eine große Zahl von Features aus ganz unterschiedlichen Anwendungsbereichen mit.

Es geht vielmehr um Komponenten wie das .NET Framework, den Windows-Prozessaktivierungsdienst oder viele andere im Betriebssystem eingebaute Funktionen, die moderne Anwendungen nutzen können. Denken Sie beispielsweise auch an den modernen IP-Stack, die Unterstützung für alternative Eingabemöglichkeiten (*Windows Touch*), neue Grafikfunktionen, verbesserten Multi-Core-Support und vieles andere mehr.

Softwarearchitektur

Abbildung 3.9 verdeutlicht nochmals die Unterschiede in den Architekturen:

- Auf der linken Seite (»Alte Architektur …«) bietet das Betriebssystem nur Grundfunktionen. Somit müssen die Anwendungen viele Funktionen selbst implementieren (jeweils dargestellt durch eine schwarze Form). Die Applikationen müssen sich beispielsweise selbst um Authentifizierung, den sicheren Aufbau von Netzwerkverbindungen, das Zeichnen von komplexen Oberflächenelementen und -effekten und dergleichen mehr kümmern.

  Da es Funktionen gibt, die (fast) jede Applikation benötigt (z. B. Authentifizierung des Benutzers), hat sich jeder Programmierer von Neuem mit deren Umsetzung aufhalten müssen.

  Das Szenario entspricht beispielsweise der DOS-Welt, in der das Betriebssystem über hinreichend wenig eigene Intelligenz verfügte.
- Auf der rechten Seite (»Moderne Architektur …«) sind die Funktionen von den Anwendungen in das Betriebssystem verlagert worden. Selbstverständlich benötigen auch moderne Programme vielerlei Grundfunktionen, wie die bereits mehrfach genannte Benutzer-Authentifizierung. Der Unterschied ist, dass die Programmierer einfach Betriebssystemfunktionen verwenden können und nicht jede benötigte Funktionalität »zu Fuß« programmieren müssen.

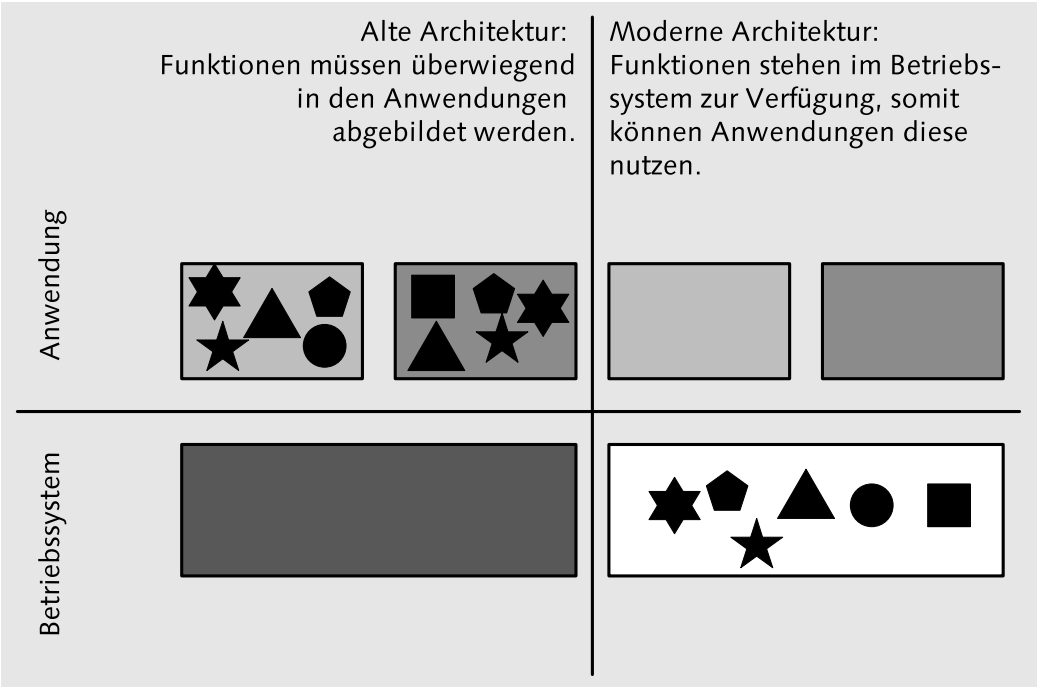


Abbildung 3.9 Je mehr Funktionen das Betriebssystem enthält, desto weniger muss die einzelne Applikation beherrschen.

Es ist völlig einleuchtend, dass die moderne Architektur zu deutlich verringerten Entwicklungskosten führt – immerhin muss der Programmierer weniger Funktionen implementieren.

Ein kritischer Zeitgenosse könnte nun mit folgenden Einwänden kommen:

- Viele Programme, die in den Unternehmen bzw. Organisationen eingesetzt werden, sind so alt (bzw. altertümlich programmiert), dass diese von den Funktionen moderner Betriebssysteme nur recht wenige nutzen.
- Warum baut man nicht einfach Bibliotheken zum Nachinstallieren, die auch alte Betriebssysteme um diese benötigten Funktionen ergänzen?

Ja, diese Gedanken sind sicherlich nicht von der Hand zu weisen, sind aber, mit Verlaub gesagt, wenig nachhaltig gedacht.

Natürlich gibt es jede Menge Software, die entweder hinreichend alt ist oder zwar neu ist, aber von Programmierern entwickelt wurde, die sich selbst nicht weiterentwickelt haben und noch so programmieren wie zur Jahrtausendwende. Solche Software profitiert natürlich nicht von einem modernen Betriebssystem – eher im Gegenteil.

Es wäre aber nun fatal, die IT-Strategie daran auszurichten, dass technisch schlechte und/oder veraltete Software eingesetzt wird.

Zu bedenken ist auch, dass auch der umgekehrte Fall gilt: Bleibt die Betriebssysteminfrastruktur auf einem alten Stand stehen, werden Sie keine moderne Software ausführen können: Neue Software läuft irgendwann nicht mehr auf alten Betriebssystemen. Ein kleines Beispiel sehen Sie in Abbildung 3.10, in der die Anforderungen für das *.NET Framework 3.5 SP1* zu sehen sind: Windows XP wird noch unterstützt, aber Windows 2000 nicht mehr. Wenn Sie eine Software einsetzen möchten, die das .NET Framework 3.5 voraussetzt und Sie nur Windows 2000 auf den Arbeitsplätzen einsetzen, dann haben Sie leider verloren.

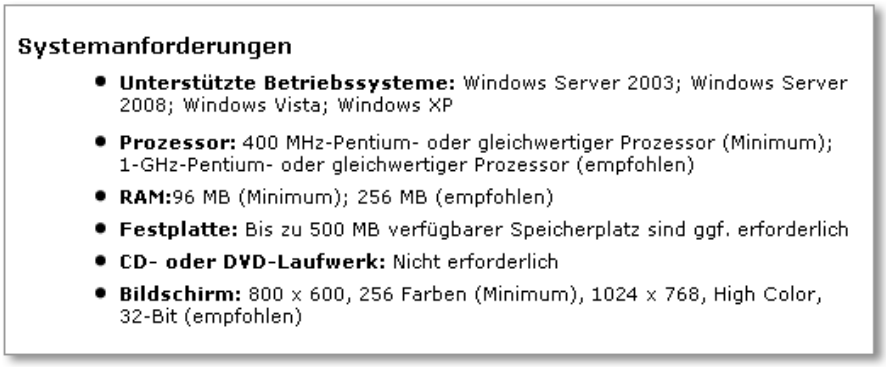


Abbildung 3.10 Die Anforderungen von .NET Framework 3.5 SP1. Es läuft zwar noch mit Windows XP; mit Windows 2000 klappt's nicht mehr.

Somit kommen wir zum zweiten Einwand: Warum werden nicht sämtliche Softwareprodukte so entwickelt, dass sie mehr oder wenig beliebig lange rückwärtskompatibel sind? Tja, würde man immer so denken, gäbe es auch kein bleifreies Benzin, weil vor dreißig Jahren die Mehrheit der Fahrzeuge verbleites Benzin benötigte. Man kann nicht bis in alle Ewigkeit rückwärtskompatibel bleiben. Auch Betriebssysteme entwickeln sich weiter. Als Windows 2000 herauskam, gab es noch keine x64-Prozessoren, 64 MB war noch ein einigermaßen gesunder Wert für den Hauptspeicherausbau, und 1024*748 Pixel war die normale Bildschirmauflösung – ach ja, ganz zu schweigen von Prozessoren mit vier oder acht Kernen. Ein Betriebssystem muss bezüglich Architektur und Funktionalität an diese Gegebenheiten angepasst werden. Demnach macht es wenig Sinn, auf Rückwärtskompatibilität für immer zu setzen.

NAP, BitLocker, AppLocker, DirectAccess & Co.

Wie bereits erwähnt, gibt es jede Menge Anforderungen, die vom Betriebssystem abgedeckt werden können oder zumindest abgedeckt werden könnten. Schauen Sie auf die »Landkarte« in Abbildung 3.11 auf Seite 40: Sie werden mir sicherlich zustimmen, dass die Grundlage, nämlich das Ausführen von Applikationen, zwar der zentrale Dreh- und Angelpunkt, bei Weitem aber nicht alles ist. Ein modernes Betriebssystem, auf das Sie Ihre Desktop-Strategie für morgen abstimmen, muss auch alle zusätzlichen Aspekte abdecken können:

- Es muss optimal die *Netzwerkkommunikation* unterstützen, beispielsweise auch IPv6 unterstützen, den Umgang mit der digitalen Identität gemäß heutigen Anforderungen unterstützen, performant kommunizieren und vieles andere mehr.
- Das Betriebssystem muss *benutzerfreundlich* sein – allein grafische Unterstützung und Bedienung mit der Maus reicht nicht.
- Es muss umfassend und einfach zu *managen* sein.
- Es muss die *Mobilitätsanforderungen* des modernen Business unterstützen.
- Und das Ganze muss unter maximalen *Sicherheitsvorkehrungen* ablaufen.

Wenn Sie im Detail über diese Anforderungen nachdenken, werden Sie mit mir übereinstimmen, dass diese nur mit Technologie zu realisieren sind, die von vornherein darauf ausgerichtet ist. Es genügt also nicht, Windows 2000 zu nehmen und mit ein paar Ergänzungen auszustatten.

Aller Voraussicht nach werden Sie die auf Abbildung 3.11 genannten Anforderungen in Ihrem Unternehmen bzw. Ihrer Organisation wiederfinden. Ich würde sagen, dass ein modernes Betriebssystem benötigt wird.

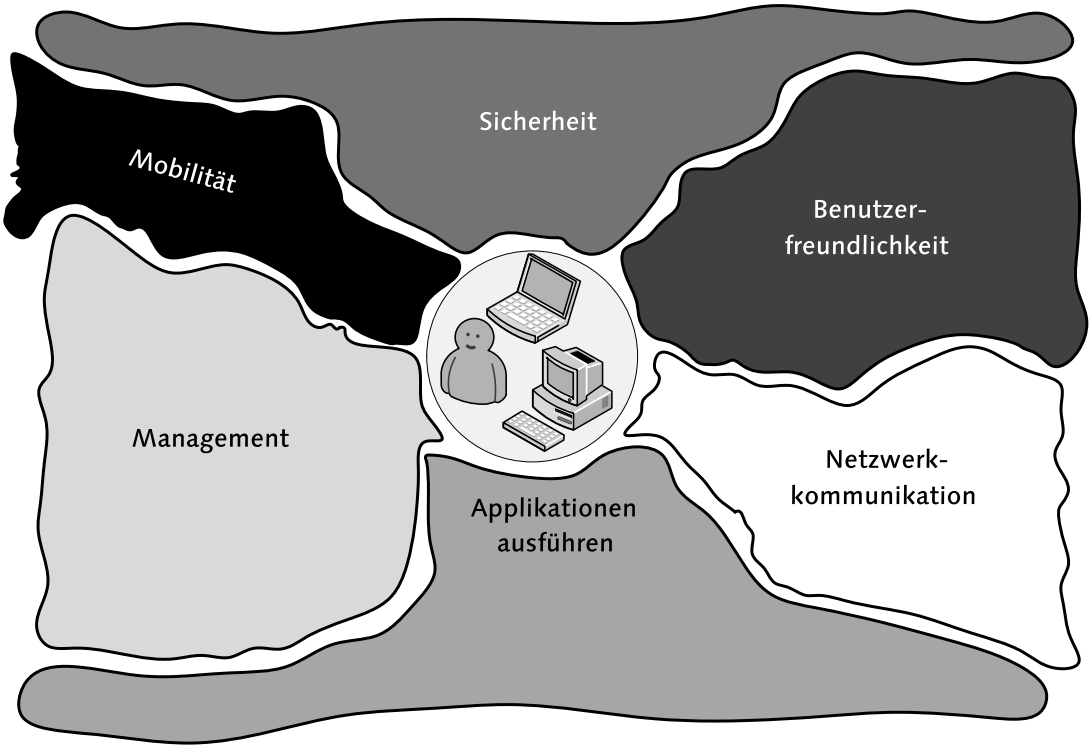


Abbildung 3.11 Viele Aspekte, die ein modernes Betriebssystem abdecken muss

3.2.2 Optimiertes Deployment und Management

Die diversen Analysten haben uns seit Jahren immer gepredigt, dass die wahren Kosten des PC-Einsatzes im Unternehmen nicht in der Anschaffung liegen, sondern in den Betriebskosten. Wenn ein PC angeliefert wird, werden Sie vermutlich folgende Schritte unternehmen:

- Der PC wird neu aufgesetzt. Sie installieren also das Betriebssystem und die benötigten Applikationen.
- Wenn der PC beim Benutzer im Betrieb ist, wird es verschiedene Servicefälle geben, beispielsweise:
  - Der PC funktioniert aus irgendwelchen Gründen nicht. Dies kann beispielsweise an Softwarefehlern oder Hardwarefehlern liegen, vielleicht auch daran, dass der Anwender »herumgebastelt« hat.
  - Updates müssen installiert werden.
  - Neue Programme müssen installiert werden.
  - Der Benutzer hat Probleme mit dem System, die vielleicht nicht unbedingt technischer Natur sind, sondern er »scheitert« an mangelnden Kenntnissen in der Bedienung des Systems.
- Am Ende seines Lebens wird der PC verschrottet, wobei insbesondere eventuell vorhandene Daten gelöscht werden müssen.

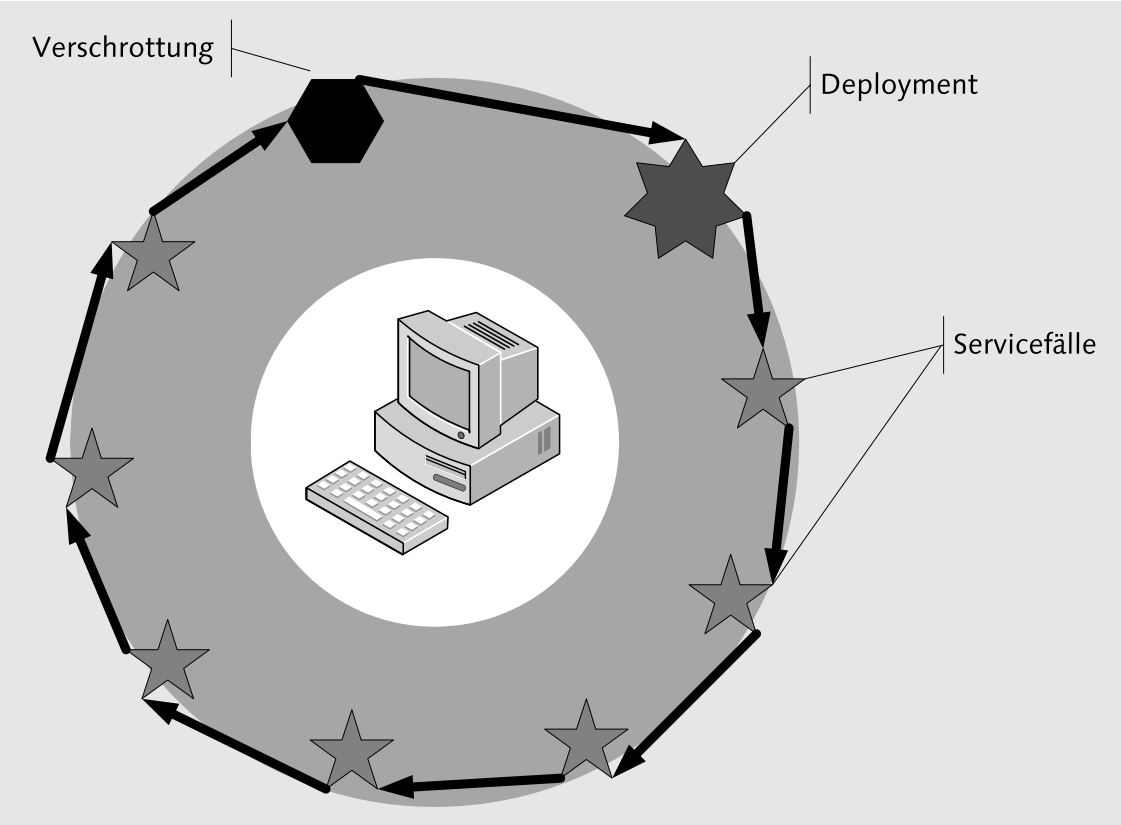


Abbildung 3.12 Ein ewiger Kreislauf: Deployment – Service – Verschrottung

Die Themenfelder Deplyoment und Management einer PC-Umgebung zielen ganz klar auf die Kosten. Die Optimierung ist hier insbesondere deshalb lohnend, weil es eben direkt um Dutzende, Hunderte oder vielleicht sogar Tausende von Systemen geht. Das Optimierungsergebnis lässt sich sogar in Zahlen ausdrücken: Ein um 10 Minuten verringerter Aufwand beim Deployment wirkt sich bei jährlich 500 Vorgängen mit 5.000 gesparten Minuten aus – immerhin.

Wenn man ein wenig genauer hinschaut, stellt sich natürlich die Frage, wie man nun genau ansetzen muss, um positive Effekte zu erreichen:

- Der Deployment-Prozess muss optimiert werden. Dies ist insbesondere dadurch zu erreichen, dass das zu installierende Betriebssystem die notwendigen Fähigkeiten mitbringt – und diese auch genutzt werden.
- Die Kosten für die Servicefälle lassen sich am besten dadurch optimieren, dass deren Anzahl reduziert wird.

Der letztgenannte Punkt ist allerdings noch ein wenig genauer zu betrachten: Servicefälle, die durch Störungen ausgelöst werden, lassen sich durch zuverlässige Hardware und ein stabiles Betriebssystem nebst fachgerechter Installation reduzieren. Es gibt natürlich auch nicht vermeidbare Fälle, nämlich bei der Installa-

tion von Updates und Patches. Die Optimierung besteht zunächst darin, dass das Betriebssystem für diese Anwendungsfälle optimiert ist. Allerdings ist für das Anwenden von Updates und Patches eine gewisse Infrastruktur erforderlich – beispielsweise der *Windows Server Update Service* (WSUS) für die Installation von Patches und der *System Center Configuration Manager* (SCCM) für alle übrigen Client-Management-Aufgaben, wie etwa die Verteilung von Software oder die Inventarisierung.

Eine Voraussetzung für einen messbaren Erfolg ist einerseits ein modernes Betriebssystem, andererseits aber auch, dass schlaue Leute sich Gedanken über die Prozesse machen.

3.2.3 Verbesserte Sicherheit

Sicherheit ist eine Anforderung, die letztendlich alle Komponenten des Betriebssystems betrifft. Wenn man zurückschaut, hat sich die Situation in den letzten Jahren schon allein dadurch verändert, dass die Benutzer anders mit den Systemen arbeiten: Das Notebook ist immer dabei, ständiger Kontakt mit allen möglichen Systemen innerhalb und außerhalb des Unternehmensnetzes ist notwendig. Weiterhin haben sich in den letzten Jahren auch die Bedrohungsszenarien geändert: Wer hat beispielsweise im Jahr 2001, also als XP erschien, über Phishing und Bot-Netze nachgedacht?

Natürlich ist es eine nach wie vor gültige Erkenntnis, dass ein gepflegtes System, das gut konfiguriert ist und regelmäßig Patches erhält, als wesentlich sicherer angesehen werden kann als ein solches, das vor vier Jahren irgendwie aufgesetzt worden ist, seitdem nie ein Update gesehen hat und an dem der Anwender nach Herzenslust selbst heruminstallieren kann.

Neben der »Pflegequalität« finden sich noch einige andere Ansatzpunkte:

- Für Notebooks ist es im Grunde genommen notwendig, eine Festplattenverschlüsselung durchzuführen. Ansonsten besteht die Gefahr, dass bei einem Verlust des Systems Daten in falsche Hände gelangen. Sollte das Notebook sich ohne Kennwortschutz in Betrieb nehmen lassen, könnte sogar Zugang zum Unternehmensnetz damit erlangt werden. Seit Windows Vista ist für diese Zwecke die *BitLocker*-Technologie vorhanden (nicht in allen Editionen!). Mit *BitLocker To Go* gibt es mittlerweile auch Unterstützung für Wechselmedien wie USB-Sticks.
- Wenn Sie verhindern können, dass Applikationen starten können, die nicht von der Unternehmens-IT autorisiert sind, wären Sie schon einen sehr deutlichen Schritt weiter. Windows 7 bringt hierzu die *AppLocker*-Technologie mit.

- Nicht zu unterschätzen ist auch der Nutzen einer Desktop-Firewall, beispielsweise der *Windows-Firewall*. Man kann nicht mehr unbedingt davon ausgehen, dass das interne Netz eines Unternehmens frei von Schadcode ist – beispielsweise hat *SQL Slammer* viele IT-Organisationen auf den harten Boden der Tatsachen geholt. Ein erhöhtes Gefährdungspotenzial ist weiterhin auch für Notebooks zu erkennen, die unterwegs an öffentlichen WLAN-Hotspots oder zu Hause am DSL-Anschluss des Mitarbeiters betrieben werden. Ohne eine Desktop-Firewall dürfte es annähernd sicher sein, dass das Notebook »befallen« wird.

Die vorherigen Beispiele gingen davon aus, dass der PC bzw. das Notebook geschützt wird. Ein durchaus wichtiger Ansatz darüber hinaus ist der Schutz des Netzes vor einem System, das eventuell nicht »gesund« ist. Der Grundgedanke bei Technologien wie NAP (*Network Access Protection*) ist, dass ein Computer nur dann eine Verbindung zum Netz aufbauen oder auf bestimmte Ressourcen zugreifen darf, wenn gewisse Mindeststandards erreicht sind. Man könnte beispielsweise festlegen, dass ein PC nur dann Zugriff erhält, wenn ein Virenscanner mit aktuellen Signaturen installiert ist und aktuelle Patches aufgespielt worden sind. Mit *Windows Vista* und *Windows Server 2008* wurde die schon erwähnte NAP-Technologie (Network Access Protection) verfügbar, die Sie natürlich mit *Windows 7* ebenfalls nutzen können.

Sie sehen also, dass ein modernes Betriebssystem vielfältige Möglichkeiten bietet, um in puncto Sicherheit aufzurüsten. Es sei aber deutlich darauf hingewiesen, dass sich die Sicherheitslage nicht unbedingt allein dadurch verbessert, dass Windows 7 eingeführt wird. Die korrekte Sichtweise ist, dass Sicherheit ein immerwährender Prozess ist, der durch die Fähigkeiten von Windows 7 entscheidend unterstützt werden kann.

3.2.4 Einfachere Bedienung

Ich kenne Administratoren, die bei der Arbeit mit einem Windows XP-System als ersten Schritt die Windows 2000-Optik des Startmenüs einstellen. Für die Oberflächen von Windows Vista oder Windows 7 haben sie nur mitleidige Blicke übrig und suchen als Erstes nach einer Möglichkeit, die Optik auf Windows 2000 zurückzusetzen. Da ich diese Kollegen ansonsten fachlich sehr schätze, möchte ich mich auch weiter nicht beschweren. Ich möchte aber an dieser Stelle darauf hinweisen, dass wir IT-Professionals eventuell eine andere Vorstellung von Bedienbarkeit und Benutzeroberflächen haben als unsere Benutzer.

Generell gilt, dass die Microsoft-Oberflächen nicht die intuitivsten und benutzerfreundlichsten der Branche sind. Ich selbst bin da sicherlich nicht ganz objektiv –

ich kenne aber mehrere Personen, die jahrelang mit Windows-Systemen gearbeitet haben und mir voneinander unabhängig vorschwärmen, wie einfach und intuitiv der Mac zu bedienen ist, der für zu Hause angeschafft worden ist. Nun denn, für solche eher weichen Faktoren wie intuitive Bedienbarkeit der Oberfläche gibt es sicherlich durchaus unterschiedliche Sichtweisen. Fakt ist aber, dass es gut ist, dass Microsoft an der Oberfläche des Betriebssystems arbeitet. Eine Änderung der Optik der Oberfläche führt zunächst zu einem gewissen »Umgewöhnungsaufwand«. Den hatten wir übrigens auch, als Windows NT4 die Windows 95-Oberfläche verpasst bekam und der Programm-Manager verschwand. Stellen Sie sich vor, es gäbe noch immer dieses Ungetüm – fatal! Ich nehme an, dass sowohl die IT-Professionals als auch die Benutzer die Windows 7-Oberfläche schätzen lernen.

Das Thema »Einfache Bedienbarkeit« ist aber nicht nur eine Frage der Oberfläche und der Anordnung der Menüs. Auch solche Aspekte wie ein einfacher Aufbau einer Verbindung zum Unternehmensnetz oder das Finden von Informationen tragen zur Effizienzsteigerung der Anwender bei.

Aspekte wie die einfache Bedienbarkeit nebst den daraus resultierenden Effizienzsteigerungen sind schlecht messbar und in Zahlen auszudrücken. Trotzdem leuchtet es sicher jedem ein, dass eine leichte und intuitivere Bedienung zu verbesserten Arbeitsergebnissen führen kann.

3.2.5 Mobile Szenarien

Die Anwender von heute und erst recht die Nutzer von morgen sind mobil – und zwar mit steigender Tendenz. Wenn die Notebooks aber nicht mehr nur im relativ gehegten und gepflegten Unternehmens-LAN stehen, sondern in der Flughafen-Lounge, im WLAN von Starbucks, per UMTS-Karte oder im Homeoffice in Betrieb genommen werden sollen, gibt es zwei Kernfragen:

- Welche Technologien sind notwendig, damit die mobilen Mitarbeiter Zugriff auf die benötigten Daten haben? Ein Notebook zu haben und es überall auf der Welt anschalten zu können, schafft an sich noch keine mobile Arbeitsumgebung.
- Ein extrem wichtiger Punkt ist die Gewährleistung der Sicherheit, sowohl für das Notebook selbst, als auch für die darauf gespeicherten Daten und das Unternehmensnetz; einige Beispiele:
  - Die Wahrscheinlichkeit, dass das Notebook von Malware, Viren, Trojanern und dergleichen infiziert wird, steigt, wenn es sich nicht in dem relativ abgeschotteten Unternehmensnetz befindet.

- Wird das Notebook verloren oder gar gezielt gestohlen, sind die darauf gespeicherten Daten hochgradig gefährdet und könnten Unbefugten in die Hände fallen.
- Ist das Notebook beim »Außeneinsatz« infiziert worden und kehrt es in das Unternehmensnetz zurück oder baut per VPN eine Verbindung dorthin auf, könnte das Notebook Schadcode in das Unternehmensnetz bringen. Ein weiteres Risiko könnte auch darin bestehen, dass ein Unbefugter Zugriff auf das Notebook erhält und mit diesem eine Verbindung in das Unternehmensnetz aufbaut und aufgrund von gespeicherten Anmeldeinformationen auf vertrauliche Daten, E-Mails etc. zugreifen kann oder – was noch schlimmer ist – die Daten unbemerkt modifizieren kann.

Weiterhin ist es natürlich in mobilen Szenarien wünschenswert, dass das Betriebssystem in der Lage ist, die Hardware dem mobilen Einsatz entsprechend zu steuern. Ich denke hier beispielsweise an Funktionen zur Optimierung der Akkulaufzeit.

Kurz gesagt gibt es in mobilen Szenarien durchaus Anforderungen, die ein älteres Betriebssystem nicht oder nur sehr begrenzt erfüllen kann. Man braucht hier gar nicht bis zu NT4 zurückzugehen: Auch Windows XP, das »nur« der Vor-Vorgänger von Windows 7 ist, bekleckert sich in mobilen Szenarien nicht unbedingt mit Ruhm. So gibt es beispielsweise keine Funktion zur Verschlüsselung von Festplatten, nur sehr rudimentäre Werkzeuge zum Aufbau einer Verbindung zu einem WLAN etc.

3.2.6 Support-Situation

Ein beliebtes Argument für die Einführung eines neuen Betriebssystems (oder einer Applikation oder eines Applikationsservers) ist auslaufender Support. Das ist grundsätzlich auch keine ganz falsche Argumentation, daher sehen Sie in Tabelle 3.1 eine Aufstellung der Support-Saten der auf NT-basierenden Clientbetriebssysteme (Quelle: *http://support.microsoft.com/gp/lifeselectwin*).

Produkt	Allg. Verfügbarkeitsdatum	Mainstream Support bis	Extended Support bis
NT Workstation 3.1	23.10.1993	31.12.2000	Nicht zutreffend
NT Workstation 3.51	30.05.1995	21.12.2000	21.12.2001
NT Workstation 4.0	29.07.1996	30.06.2002	20.06.2004
Windows 2000 Professional	31.03.2000	30.06.2005	13.07.2010

Tabelle 3.1 Support-Situation bei den NT-basierten Clientbetriebssystemen

Produkt	Allg. Verfügbarkeitsdatum	Mainstream Support bis	Extended Support bis
Windows XP Professional	31.12.2001	14.04.2009	30.04.2014
Windows Vista Business	25.01.2007	10.04.2012	11.04.2017

Tabelle 3.1 Support-Situation bei den NT-basierten Clientbetriebssystemen (Forts.)

Mainstream vs. Extended Support

Es stellt sich natürlich noch die Frage, was genau man sich unter Mainstream bzw. Extended Support vorzustellen hat.

Ich zitiere hierzu Microsoft (*http://support.microsoft.com/lifecycle/*):

»**Der Mainstream Support** stellt die erste Phase des Produktlebenszyklus dar. Innerhalb des Supportzeitraums für das gegenwärtig unterstützte Service Pack beinhaltet der Mainstream Support folgende Leistungen:

- Bearbeitung technischer Anfragen (kostenfreier Support, kostenpflichtiger Support von Anfragen oder Abrechnung auf Stundenbasis, Garantieanfragen)
- Security Update Support
- Beantragung von nicht-sicherheitsrelevanten Hotfixes

Die **Extended Supportphase** folgt der Mainstream Supportphase für Business- und Entwicklerprodukte. Innerhalb des Supportzeitraums für das gegenwärtig unterstützte Service Pack beinhaltet der Extended Support folgende Leistungen:

- Kostenpflichtiger Support
- Security Update Support ohne zusätzliche Kosten
- Beantragung von Hotfixes, die nicht im Zusammenhang mit sicherheits-relevanten Themen stehen, nur im Rahmen einer getrennten Vereinbarung. Einzelne Fixes werden getrennt berechnet.«

Auffällig in Tabelle 3.1 ist die vergleichsweise lange Mainstream-Support-Phase für Windows XP, was wohl Kundenforderungen geschuldet ist, da XP in den Unternehmen das am weitesten verbreitete Betriebssystem ist und die Einführung von Windows Vista eher zögerlich erfolgte. Wie dem auch immer sei: Windows XP ist mittlerweile im Extended Support, was zunächst einmal nicht unbedingt ein zwingender Grund für ein Betriebssystem-Upgrade ist. Die zuvor aufgeführten Gründe wiegen meines Erachtens deutlich schwerer.

Wenn Sie eines oder mehrere meiner Serverbücher gelesen haben, wissen Sie, dass ich generell sehr darauf bedacht bin, dass eine Konfiguration von Microsoft tatsächlich auch supportet ist. Bei »mysteriösen« Problemen ist es in jedem Fall billiger, eine kostenpflichtige Support-Anfrage bei Microsoft zu stellen, als selbst stundenlang oder vielleicht auch tagelang und gegebenenfalls mit externer Unter-

stützung herumzubasteln. Auch im Clientumfeld ist die Möglichkeit, Support-Anfragen stellen zu können, wertvoll. Da man im Business-Umfeld aber ohnehin stets mit kostenpflichtigen Anfragen arbeitet, halte ich es nicht für allzu problematisch, wenn ein Betriebssystem vom Mainstream in den Extended Support gewechselt ist. So allmählich wird es jetzt aber schon Zeit, Windows 2000 loszuwerden (Tabelle 3.1). Falls der ein oder andere Leser aber tatsächlich noch Windows 2000 Professional einsetzt, wiegen die weiter vorn genannten Gründe aber vermutlich viel schwerer, als der so allmählich auslaufende Extended Support.

Ich mache häufig Strategie-Workshops mit Kunden, wobei es darum geht, den Ist-Zustand zu untersuchen, die Anforderungen des Business zu betrachten und herauszufinden, was man schlauerweise für die Zukunft plant. Ich habe bisher noch nie (!) den Fall erlebt, dass als Ergebnis herauskam, dass eigentlich alles wunderbar sei, man aber trotzdem upgraden müsse, weil der Support ausläuft: Bevor wir bei dem Punkt »Support-Situation« angekommen sind, hat es normalerweise schon hinreichend viele andere Argumente gegeben, warum ein Upgrade der Clientbetriebssysteme sinnvoll und zielführend ist. Allerdings gibt es hin und wieder auch die andere Situation: Ich habe durchaus Kunden, die derzeit, aus welchen Gründen auch immer, keine relevanten Anforderungen aus dem Business bekommen oder aber diese nicht umsetzen sollen. Mir fällt es in solchen Fällen schwer, ein teures Upgrade der Clientbetriebssysteme durchzuführen, »nur« weil es in den Extended Support gewechselt ist.

3.3 »Better Together«

Etliche Funktionen des Clientbetriebssystems Windows 7 stehen nur zur Verfügung, wenn im Hintergrund die entsprechenden Windows-Server arbeiten. Dies reicht von offensichtlichen Aspekten, dass eben eine Active-Directory-Integration und somit beispielsweise die Verwendung von Gruppenrichtlinien nicht ohne Domäne möglich ist (da reicht aber beispielsweise auch ein AD, das auf Windows-Server-2003-Maschinen basiert). Es gibt aber auch Windows 7-Features, die die Verwendung von Windows Server 2008 oder gar Windows Server 2008 R2 voraussetzen. Zu nennen wären hier beispielsweise NAP (*Network Access Protection*), *BitLocker* (Server werden für die zentrale Verwaltung benötigt) oder *DirectAccess* (das geht übrigens nur mit einen Windows Server 2008 R2).

Es ist übrigens nicht erforderlich, dass für die Nutzung solcher Features sämtliche Server auf *Windows Server 2008* umgestellt werden müssen. Im Allgemeinen handelt es sich nur um einzelne Dienstserver, die ein aktuelles Betriebssystem verwenden müssen. Das hört sich zwar zunächst nicht dramatisch an, es steckt aber eine gewisse Kostendynamik dahinter, denn wenn potenziell alle Clients auf den

einzigen Windows Server 2008 zugreifen, müssen flächendeckend CALs (*Client Access Licenses*, Client-Zugriffslizenzen) beschafft werden. Wenn Sie hinreichend viele Clients haben, kann das durchaus ein beachtlicher Kostenblock werden.

Neben speziellen Features, die auf Serverunterstützung angewiesen sind, profitiert die Gesamtumgebung auch aus technischer Sicht davon, dass Clients und Server sich auf einem gleichen oder ähnlichen technischen Niveau befinden. Ohne jetzt bis in die Tiefen der Protokollimplementation und dergleichen hinabsteigen zu wollen, möchte ich die altbekannte Weisheit zitieren, dass das Gesamtsystem eben letztendlich doch nur so gut ist wie das schwächste Glied. Oder noch anders gesagt: Die Qualität des neuen Blu-ray-Players nebst entsprechenden Medien kommt eben nicht zur Geltung, wenn der angeschlossene Röhrenfernseher das Erbstück von Opa ist.

Microsoft hat das marketingmäßig aufbereitet und wirbt mit dem Schlagwort »Better Together«, daher auch die Überschrift dieses Absatzes. Man kann es aber durchaus auch deutlicher formulieren: Den vollen Leistungsumfang von Windows 7 werden Sie erst erhalten, wenn die Serverlandschaft, zumindest partiell, ein zum Clientbetriebssystem passendes Niveau hat. Um bei dem zuvor erwähnten Vergleich zu bleiben: Kein visueller Hochgenuss, wenn Opas Fernseher nicht ausrangiert wird.

3.4 Hardware

Ich habe die ganze Zeit die Vorteile eines »modernen Betriebssystems« angepriesen – aber auch dieses muss auf einer dazu passenden Hardware laufen. Es ist davon auszugehen, dass Ihre Anwender nicht sonderlich glücklich damit werden, wenn Windows 7 auf einem alten Pentium-II-System mit 256 MB Speicher installiert wird. Das ist natürlich keine wirklich überraschende Erkenntnis, allerdings ist das für den Entscheidungsprozess, ob und wann Sie mit Windows 7 beginnen, keine ganz unwesentliche Frage. Die Mindest-Hardwareanforderungen sind:

- Prozessortakt > 1 GHz
- Hauptspeicher (RAM) > 1 GB
- Festplattenplatz > 40 GB
- Grafikkarte mit DirectX 9-Unterstützung mit mindestens 128 MB Speicher

Sie können einigermaßen getrost davon ausgehen, dass vor fünf Jahren beschaffte PCs diese Anforderungen nicht erfüllen. Bevor Sie ein Windows 7-Rollout auf wirklich alte Hardware durchführen, sollten Sie generell lieber noch den nächsten Hardwaretausch-Zyklus abwarten.

Kunden, die bereits auf Windows Vista migriert haben, dürften bereits geeignete Hardware einsetzen – Windows 7 hat letztendlich dieselben Anforderungen wie der direkte Vorgänger.

Meiner – allerdings nicht repräsentativen Beobachtung nach wird in den meisten Unternehmen eine geplante Windows 7-Migration ohnehin mit einem Hardwaretausch einhergehen. Dieser Weg dürfte aus verschiedenen Gründen der simpelste sein, beispielsweise:

- Es gibt keine Probleme mit Treibern, die für bestimmte ältere Komponenten nicht brauchbar sind.
- Die »Downtime« für die Anwender ist minimal.
- Die Chance zur Vereinheitlichung einer gewachsenen Umgebung ist gegeben.

Migration und Hardware

Damit es keine Missverständnisse gibt:

Meine Argumentationslinie ist nicht: »Kaufen Sie neue Hardware für Windows 7.«

Vielmehr soll es heißen: »Stimmen Sie Ihre Windows 7-Einführung mit dem Erwerb neuer Hardware ab.«

Im Grunde genommen gibt es für ein mittelständisches Unternehmen drei Fälle:

1. Ich habe etliche Kunden, die in Erwartung von Windows 7 die eigentlich fällige Hardwareerneuerung seit geraumer Zeit vor sich herschieben. Dies ist natürlich eine nahezu ideale Situation: Kaufen Sie also »alles neu«.
2. Vergleichsweise einfach zu entscheiden sind auch Szenarien, in denen die Hardware zwar noch nicht wirklich alt ist, aber die Ablösung noch nicht sofort geplant ist, sondern beispielsweise in ein bis zwei Jahren. Sofern nicht zwingende Gründe dafür sprechen, könnte man gegebenenfalls mit der Windows 7-Einführung noch warten und diese dann mit dem Hardwareaustausch durchführen. Das macht aus zwei Gründen Sinn:
   - Eine Migration auf bestehenden Maschinen ist regelmäßig nicht ganz trivial zu planen, unter anderem auch wegen der Treibersituation.
   - Wenn die Hardware in beispielsweise zwei Jahren zur Ablösung ansteht, wäre es natürlich ziemlich unwirtschaftlich, jetzt eine Migration durchzuführen und in zwei Jahren das Thema wieder auf dem Tisch zu haben.
3. Wenn beispielsweise vor einem halben Jahr eine Vista-Migration auf neue Hardware abgeschlossen worden ist, dürfte nur ein Windows 7-Update auf derselben Hardware in Frage kommen. Vermutlich wird es aber kaum einen Entscheider geben, der direkt eine weitere Migration genehmigt, sodass in

diesen Unternehmen Windows 7 vermutlich zunächst unberücksichtigt bleibt. Fairerweise muss man aber auch feststellen, dass der Technologieunterschied zwischen Windows 7 und Vista bei Weiterem nicht so groß ist, wie er zwischen Vista und XP oder gar Windows 7 und XP ist.

In vielen Unternehmen hat es sich übrigens eingebürgert, dass Notebooks und Desktops nicht um jeden Preis auf demselben Niveau gehalten werden. So kenne ich etliche Unternehmen, die auf den Desktops zwar XP einsetzen, auf den Notebooks aber bereits auf Vista umgestiegen sind. Insofern könnte auch Windows 7 in bestimmten Unternehmen als Notebook-Betriebssystem beginnen, allein schon wegen BitLocker und DirectAccess.

Wie auch immer: Sie sehen, dass die Hardwarestrategie und die Betriebssystemstrategie Hand in Hand gehen müssen – ansonsten gibt es nur Stückwerk oder höhere Kosten als eigentlich notwendig, wenn eigentlich vermeidbare Migrationsvorgänge durchgeführt werden.

Bitte beachten Sie

Bei der Hardwareauswahl ist Sorgfalt angesagt: Wenn Sie beispielsweise darauf spekuliert haben, BitLocker zur Festplattenverschlüsselung bei Notebooks zu nutzen, müssen Sie unbedingt darauf achten, dass die anzuschaffenden Geräte über einen TPM-Chip (*Trusted Platform Module*) verfügen. »Richtige« Business-Notebooks haben diesen Chip mittlerweile, Billig-Produkte und so gut wie alle Consumer-Notebooks verfügen nicht über den TPM-Chip.

3.5 Infrastrukturoptimierung

Wenn die Arbeit der IT im Wesentlichen aus »Brandbekämpfung« besteht, macht es Sinn, zu überlegen, ob das auf Dauer so weitergehen kann. Es ist durchaus nicht schlecht, zunächst theoretisch zu überlegen, was man erreichen möchte. Bei Ihren Überlegungen müssen Sie nicht ganz von vorn anfangen, denn viele Verfahren und Prozesse sind ja bereits »durchdacht« worden.

Ein interessanter Ansatz ist das Microsoft-Modell zur Infrastrukturoptimierung, das die verschiedenen Reifegrade der IT-Infrastruktur beschreibt. Abbildung 3.13 zeigt die vier definierten Phasen:

- *Basis:* In dieser Phase erfolgt der IT-Betrieb sozusagen »auf Zuruf«. Charakteristisch für die IT-Infrastruktur im Basiszustand sind manuelle, lokal ablaufende Prozesse, eine minimale zentrale Steuerung, nicht vorhandene bzw. nicht durchgesetzte IT-Richtlinien und -Standards im Hinblick auf Sicherheit, Datensicherung, Imageverwaltung und -bereitstellung, Einhaltung von Vor-

schriften und andere allgemeine IT-Standards. In diesem Zustand fehlen Kenntnisse der derzeitigen Infrastruktur bzw. der Strategien, mit denen eine Verbesserung erreicht werden könnte. Aufgrund fehlender Tools und Ressourcen ist die Fehlerfreiheit von Anwendungen und Diensten nicht sichergestellt. Es fehlt ein Medium für den Austausch von erworbenem Fachwissen im IT-Bereich. Kunden mit einer Basisinfrastruktur haben Probleme damit, ihre Umgebungen zu steuern, müssen hohe Kosten für die Verwaltung von Desktops und Servern einplanen, sind im Allgemeinen anfällig für Sicherheitsbedrohungen und können nur geringfügig positive Impulse seitens der IT nutzen. Patches, Softwarebereitstellungen und Dienste werden mit großem Aufwand und hohen Kosten bereitgestellt.

- *Standardisiert*: In einer standardisierten Infrastruktur werden durch den Einsatz von Standards und Richtlinien zur Verwaltung von Desktops und Servern Kontrollmechanismen eingeführt. Diese regeln auch die Verwendung von Computern im Netzwerk sowie die Verwaltung von Ressourcen, Sicherheitsrichtlinien und der Zugriffssteuerung mithilfe von Active Directory. Unternehmen mit standardisierten Infrastrukturen haben den Wert von grundlegenden Standards und Richtlinien erkannt, verhalten sich aber trotzdem noch eher reaktiv. Im Allgemeinen stellen sie Patches, neue Software und Desktopdienste mit mittlerem Aufwand zu mittleren bis hohen Kosten zur Verfügung. Sie haben einen angemessenen Bestand an Hardware- und Softwareprodukten und fangen langsam damit an, Lizenzen zu verwalten. Zwar wurde die Sicherheit durch ein schützendes Umkreisnetzwerk verbessert, die interne Sicherheit könnte aber immer noch gefährdet sein.
- *Rationalisiert*: In einer rationalisierten Infrastruktur sind die bei der Verwaltung von Desktops und Servern anfallenden Kosten am niedrigsten. Prozesse und Richtlinien sind so ausgereift, dass sie maßgeblich zum Unternehmenswachstum beitragen. Die Sicherheit wird proaktiv gewahrt, und die Reaktion auf Bedrohungen und Herausforderungen erfolgt schnell und kontrolliert.

  Durch die Zero-Touch-Bereitstellung werden Kosten gesenkt, die zur Bereitstellung erforderliche Zeit wird minimiert, und technische Anforderungen werden schneller bewältigt. Die Anzahl erforderlicher Images ist minimal, und die Verwaltung von Desktops erfordert nur einen äußerst geringen Aufwand. Der Bestand an Hardware- und Softwareprodukten bleibt übersichtlich. Es werden nur die tatsächlich benötigten Lizenzen und Computer erworben. Mit den strengen Richtlinien und Kontrollfunktionen vom Desktop und Server über die Firewall bis hin zum Extranet wird die Sicherheit außerordentlich proaktiv gewahrt.

- *Dynamisch*: Eine dynamische Infrastruktur wird IT-Strukturen anderer Reifegrade um Längen voraus sein. Die Kosten sind vollständig unter Kontrolle, die Integration von Benutzern und Daten, Desktops und Servern verläuft nahtlos, die Zusammenarbeit zwischen Benutzern und Abteilungen ist umfassend, Dienste und Möglichkeiten von mobilen Benutzern entsprechen faktisch dem innerbetrieblichen Niveau.

  Prozesse sind vollständig automatisiert und häufig in die Technologie selbst integriert, wodurch die IT-Abteilung an die Bedürfnisse des Unternehmens angepasst und entsprechend verwaltet werden kann. Zusätzliche Investitionen in die Technologie verschaffen dem Unternehmen spezifische, schnelle und messbare Vorteile.

  Systeme mit automatischer Bereitstellung und Quarantänefähigkeiten stellen die Patchverwaltung und die Einhaltung bewährter Sicherheitsrichtlinien sicher. Auf diese Weise kann eine dynamische Organisation Prozesse automatisieren und dadurch die Stabilität verbessern, Kosten senken und Serviceleistungen optimieren.

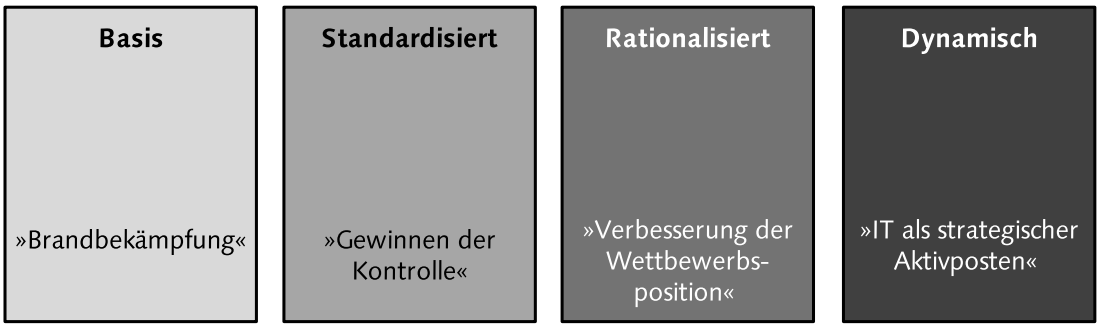


Abbildung 3.13 Infrastrukturoptimierung: Die vier »Zustände« der Unternehmens-IT

Etwas provokant und stark vereinfacht gesagt, beschreibt das Infrastrukturoptimierungsmodell die Chance, von einer chaotischen IT, die eher ein notwendiges, aber lästiges Übel ist, zu einem System zu kommen, das den Mitarbeitern hilft, erfolgreicher im Business zu sein. Sprich: Das Unternehmen verdient mehr Geld, weil es perfekt mit Informationen umgehen kann.

Das Infrastrukturoptimierungsmodell hört sich einleuchtend an, gleichwohl geht es natürlich auch darum, konkrete Schritte zu erkennen und einzuleiten. Das Modell definiert drei Bereiche, die wir nachfolgend ein wenig genauer unter die Lupe nehmen werden:

- Core Infrastructure Optimization (Core IO)
- Business Productivity Infrastructure Optimization
- Application Platform Optimization

Abbildung 3.14 zeigt die drei Reifegrade des Infrastrukturoptimierungsmodells zusammen mit den Themen des Aufgabenbereichs *Core Infrastructure Optimization* (Core IO). Wie die Berzeichnung schon vermuten lässt, geht es um die Grundlagenthemen:

- Wie sorgt man dafür, dass die Identität der Benutzer eindeutig und sicher festgestellt werden kann, ohne dass die Benutzer zigfach seine Anmeldeinformationen eingebenmüssen? Wie sorgt man dafür, dass die Benutzer jederzeit sicheren Zugriff auf das Netz erhalten?
- Wie kann man Desktop-PCs, Notebooks, Mobilgeräte (Smartphone & Co). und Server effizient managen? Hier geht es einseits um das initiale Deployment der Systeme, aber auch um Pflege und – insbesondere im Serverbereich – um die Erkennung von vorhandenen oder sich ankündigenden Engpässen.
- Das Thema *Security und Networking* ist natürlich ein ganz wesentliches Grundlagenthema. In der modernen »verbundenen Welt« ist sowohl der Schutz der Informationen als auch der Schutz der Infrastruktur eine vordringliche Aufgabe. Schwierig ist sie unter anderem deshalb, weil eine vollständige Abschottung nicht möglich ist, da die Anwender ja von jedem beliebigen Punkt der Welt auf die gespeicherten Informationen zugreifen können müssen. Weiterhin spielt die Kommunikation mit Partnern, also beispielsweise Kunden und Lieferanten, ebenfalls eine immer größere Rolle.

  Auch am Netzwerk gibt es häufig diverse »Baustellen« – sowohl in puncto Sicherheit als auch in puncto Zuverlässigkeit, Stabilität und Managebarkeit.
- Es versteht sich von selbst, dass leistungsfähige Werkzeuge zur Sicherung und zur Wiederherstellung vorhanden sein müssen. Es genügt aber nicht, »nur« eine Sicherung anzufertigen. Hierzu gehören ausgefeilte Prozesse und Konzepte, die definieren, welche Informationen wann und wie gesichert werden, welches die maximal vertretbare Datenverlustzeit ist und wie eine Wiederherstellung einzelner Datensätze, eines Servers oder des Gesamtsystems ablaufen muss.

Abbildung 3.15 zeigt die Themen des Bereichs der *Business Productivity Infrastructure Optimization*. Wie der Name bereits sagt, geht es darum, zu überlegen, wie es zu schaffen ist, dass die Anwender mit den Systemen effizienter arbeiten – also die Produktivität zu steigern. Fakt ist, dass in vielen Unternehmen noch so gearbeitet wird, wie 1995:

- Anmelden
- Word/Excel öffnen
- Datei auf der Netzwerkfreigabe suchen
- …

… enorme Produktivitätsverluste inklusive. Zu berücksichtigen ist, dass nicht »nur« die Produktivität der Benutzer mit den Systemen genauso hoch (oder niedrig) ist wie vor zehn Jahren. Hinzu kommt, dass es streng genommen Verschwendung ist, nur einen Bruchteil der Fähigkeiten der teuer gekauften Systeme zu nutzen.

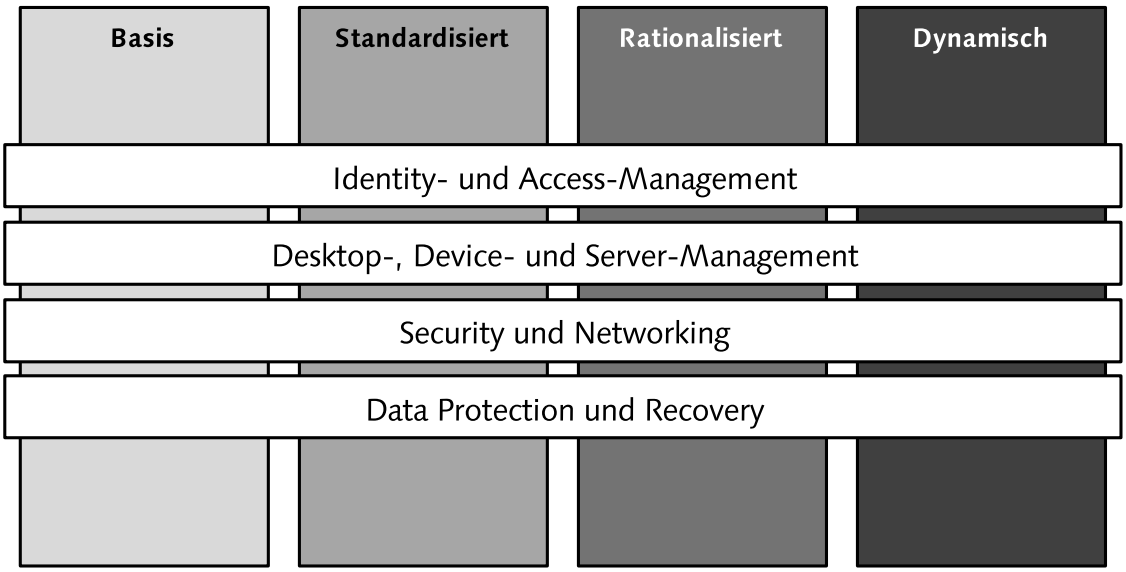


Abbildung 3.14 Die Themen der Core Infrastructure Optimization

Die Themen der Business-Productivity-Optimierung sind:

- Hinter *Unified Communications* steckt der Gedanke, alle Kommunikationsformen (beispielsweise E-Mail, Presence, Telefonie, Videoconferencing) unter einem einheitlichen Technologie- und Bedienkonzept zusammenzufassen und so für die Benutzer die täglichen Kommunikationsvorgänge zu vereinfachen und neue innovative Möglichkeiten zu schaffen.
- *Collaboration* befasst sich damit, wie Teams optimal zusammenarbeiten und Informationen austauschen. Eine »Collaboration-per-E-Mail« ist niemals optimal, und das klassische Dateisystem hat ebenfalls im Laufe der letzten Jahre mehr oder weniger eindrucksvoll bewiesen, dass es für aktuelle Collaboration-Anforderungen mehr als ungeeignet ist.
- *Enterprise Content Management* umfasst den unternehmensweiten Umgang mit dem Unternehmenswissen. Neben dem eigentlichen Bereitstellen der Informationen geht es hier auch um die rechtssichere Verarbeitung, um Workflows zur Genehmigung und Verteilung der Inhalte und vieles andere mehr.

- Ein wesentliches Problem in so gut wie jeder Umgebung ist, dass zwar viel Wissen gespeichert ist, die Anwender es aber trotzdem nicht finden. Es ist also eine Suchmöglichkeit (*Enterprise Search*) notwendig, die gemäß der Berechtigungen des jeweils suchenden Benutzers alle gesuchten Informationen findet, egal in welchem System diese liegen.
- *Business Intelligence* beschreibt Verfahren und Prozesse zur systematischen Analyse von Daten in elektronischer Form. Business Intelligence hat sich als wesentliche Technologie erwiesen, um Benutzern Businessdaten in »aufbereiteter« Form zur Verfügung zu stellen.

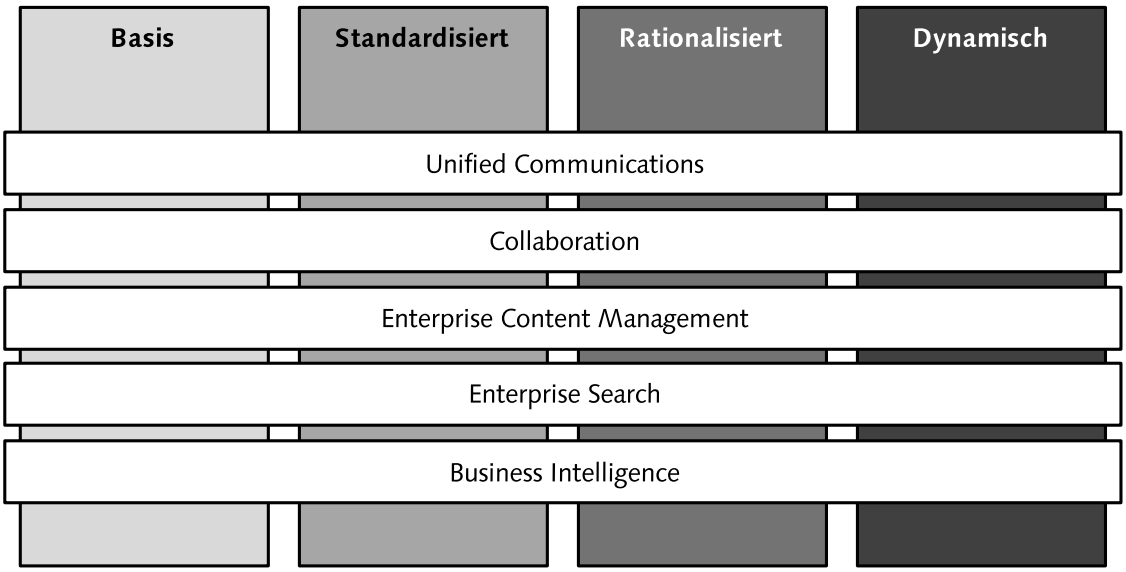


Abbildung 3.15 Die Themen der Business Productivity Infrastructure Optimization

Abbildung 3.16 zeigt die Themen des dritten Bereichs, nämlich der *Application Platform Optimization*. Die hier angesprochenen Themen sind recht »entwicklungsnah«. Es geht um die Einführung einer SOA (Service Oriented Architecture), die Abbildung von Geschäftsprozessen, die Verbesserung der Bedienbarkeit und vieles andere mehr.

Wenn Sie den Reifegrad Ihres Unternehmens festgestellt haben, geht es nun darum, zu planen, wie Sie zur »nächsten Ebene« gelangen. Sie werden nicht alle Schritte auf einmal erledigen können, insofern ist eine sinnvolle Sequenzierung der Teilschritte erforderlich.

In diesem Buch werden Sie diverse Technologien kennenlernen, die im Rahmen der Infrastrukturoptimierung eingesetzt werden können.

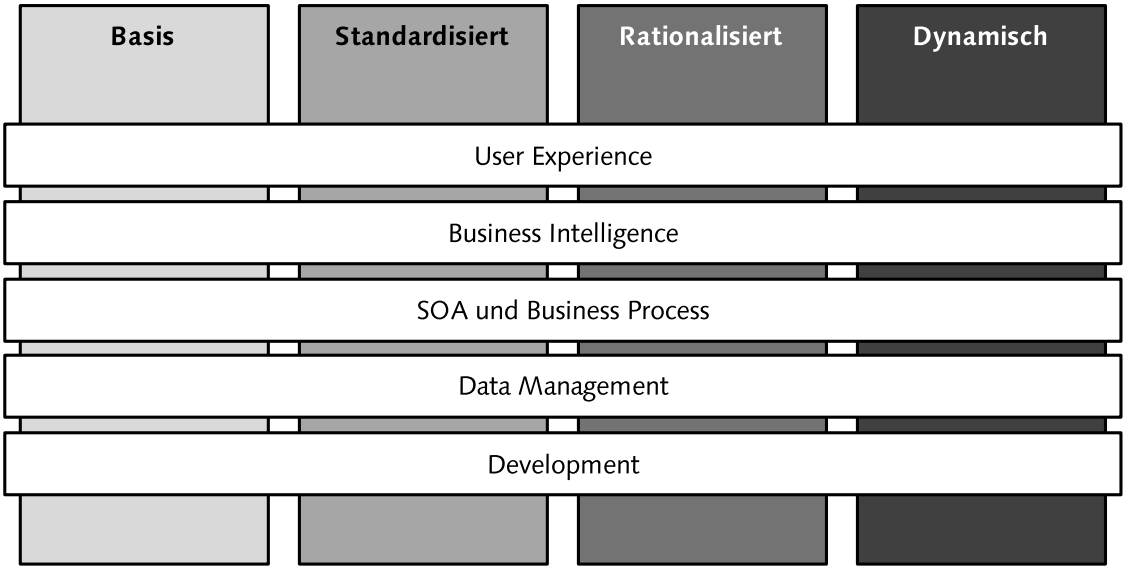


Abbildung 3.16 Die Themen der Application Platform Optimization

Infrastrukturoptimierungsmodell

Mehr Informationen zu dem Infrastrukturoptimierungsmodell finden Sie unter der URL *http://www.microsoft.com/germany/io/default.mspx.*

Nachdem aber Dareios gestorben und Artaxerxes auf den Thron gelangt war, verdächtigte Tissaphernes den Kyros bei seinem Bruder, als ob er Schlimmes gegen ihn im Schilde führe.

4 Einstieg

Wenn Sie Windows 7 das erste Mal sehen, wird Ihnen natürlich zunächst die modernisierte Oberfläche auffallen, insbesondere natürlich die höhere Taskleiste (Abbildung 4.1). Wenn Sie sich ein wenig mit der neuen Windows 7-Oberfläche beschäftigt haben, werden Sie feststellen, dass diese wieder ein bisschen intuitiver geworden ist. Es wird sicherlich Zeitgenossen geben, die anmerken, dass die absolut geradlinige, einprägsame und selbsterklärende Bedienbarkeit der Oberflächen des Herstellers mit dem angebissenen Apfel nicht erreicht worden ist – aber über Geschmack lässt sich ja bekanntlich streiten.

Ich habe mit etlichen Anwendern gesprochen, die in Unternehmen als Pilotbenutzer in früheren Kompatibilitätstests mit dem *Release Candidate* gearbeitet haben. Diese haben durchweg ein sehr positives Feedback gegeben. Die Anwender kamen sowohl von der Windows XP- als auch von der Windows Vista-Plattform.

Generell wird für alle, die bereits Erfahrungen mit der Vista-Oberfläche gemacht haben, die Umgewöhnung relativ schnell gehen. Die Änderungen zwischen Vista und Windows 7 sind jedenfalls deutlich geringer ausgefallen, als zwischen XP und Vista.

Es ist übrigens immer interessant, die Microsoft-Versionsnummern zu beobachten:

- Windows NT 3.x
- Windows NT 4
- Die Windows 2000-Familie meldete sich als NT 5.0.
- Windows XP gab sich als NT 5.1 zu erkennen.
- Der Windows Server 2003 hört(e) auf die Versionsnummer 5.2.
- Windows Vista und Windows Server 2008 kamen mit der Versionsnummer 6 zu uns.

Abbildung 4.1 Neue Oberfläche – und darunter viel neue Technik

- Wer erwartet hat, dass Windows 7 nun dem Namen entsprechend die Versionsnummer 7 hat, sieht sich allerdings getäuscht: Wie Sie auf Abbildung 4.2 sehen können, meldet sich ein Windows 7 als *Microsoft Windows Version 6.1.7600* (Windows Server 2008 R2 meldet sich übrigens mit derselben Versionsnummer).

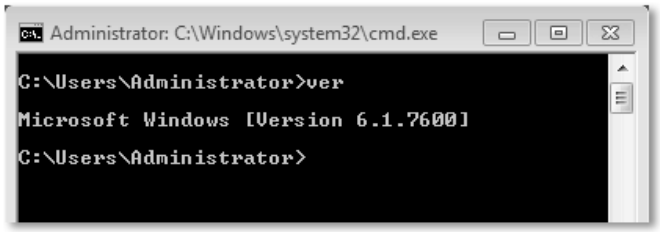


Abbildung 4.2 Windows 7 ist eigentlich Windows 6.1.

Es wäre jedoch deutlich untertrieben, Windows 7 als eine Art großes Vista-Service-Pack zu bezeichnen, wie der recht kleine Sprung in der Versionsnummer vermuten lassen könnte. Einerseits ist Windows 7 eine eher evolutionäre Weiterentwicklung von Vista. Andererseits sind recht viele insbesondere im Unternehmensumfeld sehr interessante neue Funktionen dazugekommen. Der Mehrwert von Windows 7 fällt dadurch deutlich größer aus als der von Vista.

4.1 Was ist neu?

Wenn Sie Windows 7 installieren und sich ein wenig »durchklicken«, werden Sie selbst viele kleinere und größere Änderungen bemerken. Immerhin hat Microsoft ja auch knapp drei Jahre seit dem Erscheinen von Vista daran gearbeitet (Volumenlizenzen von Vista gab es in Deutschland in etwa ab November 2006). Die Tatsache, dass WordPad nun auch die aus der Office-2007-Suite bekannte Ribbon-Oberfläche verwendet, gehört zu diesen vielen Änderungen im Detail.

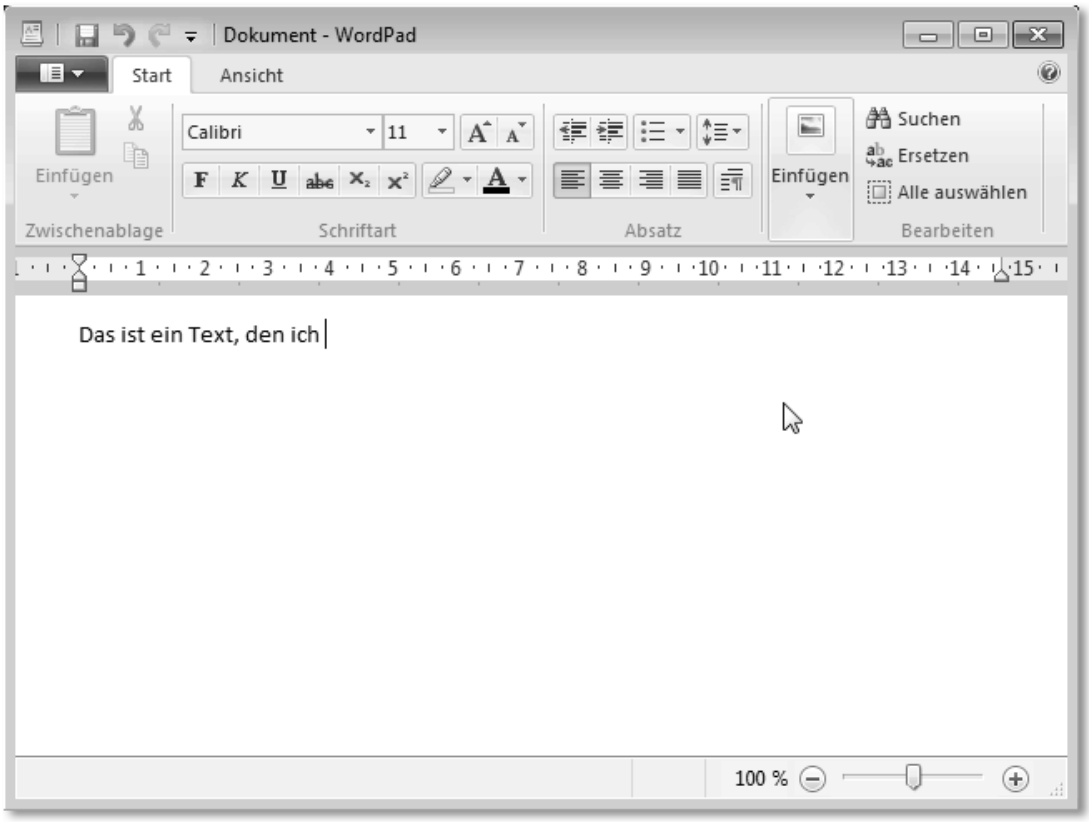


Abbildung 4.3 Auch eine Neuerung: WordPad ist mit der aus Office 2007 bekannten Ribbon-Oberfläche ausgestattet.

Ich möchte mich in diesem Buch aber nicht mit diesen eher simplen Neuerungen beschäftigen – welchen IT-Professional interessiert schon, ob WordPad eine Ribbon-Oberfläche hat? Vielmehr möchte ich tabellarisch die Änderungen zusammenfassen, die im Unternehmenseinsatz relevant sind und dabei teilweise nicht so deutlich ins Auge springen.

Die wesentlichen Neuerungen lassen sich in fünf Kategorien zusammenfassen:

- Sicherheit
- Mobilität
- Management

- Deployment
- Suche

4.1.1 Sicherheit

Das Thema Sicherheit ist bei Microsoft bekanntlich sehr hoch aufgehängt. Schließlich sind die Microsoft-Produkte aufgrund der immensen Verbreitung einem weit härteren Praxistest ausgesetzt als jedes andere Software- oder Hardwareprodukt. Letztendlich führt jede Behebung eines Fehlers zu einer Verbesserung der Sicherheit, denn jeder Fehler im Code könnte (!) zu einem Sicherheitsproblem führen.

Tabelle 4.1 zeigt diverse Neuerungen im Sicherheitsumfeld. Bereits bei den ersten drei Positionen dürfte den meisten IT-Professionals in den Unternehmen ein lautes »Endlich« über die Lippen kommen: Die Verschlüsselung von Notebooks nebst mobilen Datenträgern wie USB-Sticks ist heute absolutes Pflichtprogramm. Ebenso steht eine bessere Kontrolle darüber, was auf den PCs wirklich ausgeführt wird, weit oben auf der Wunschliste.

Auf den ersten Blick nicht ganz so spektakulär ist die Möglichkeit der Windows-Firewall, gleichzeitig mit mehreren aktiven Profilen zu arbeiten – auf den ersten Blick fragen Sie sich bestimmt, wozu das nützen soll. Die Antwort ist, dass dies aufgrund von DirectAccess notwendig geworden ist, bei dem der PC in der Tat unterschiedliche aktive Verbindungen hat, nämlich eine ins Unternehmensnetz und eine ins öffentliche Internet.

Funktion	XP SP3	Vista SP1	Windows 7
BitLocker (Festplattenverschlüsselung) nur in den Editionen *Enterprise* und *Ultimate*		X	X (verbessert)
BitLocker To Go (Verschlüsselung für mobile Datenträger) nur in den Editionen *Enterprise* und *Ultimate*			X (neu)
AppLocker (Kontrolle über die ausführbaren Programme) nur in den Editionen *Enterprise* und *Ultimate*			X (neu)
Mehrere gleichzeitige Firewall-Profile			X (neu)
Garnulare Überwachung		X	X (verbessert)
User Account Control (UAC)		X	X (verbessert)

Tabelle 4.1 Neuerungen im Bereich Sicherheit

Funktion	XP SP3	Vista SP1	Windows 7
Unterstützung von Smart-Cards	X	X	X (verbessert)
Unterstützung für biometrische Authentifizierung	Drittanbieter	Drittanbieter	X (neu)

Tabelle 4.1 Neuerungen im Bereich Sicherheit (Forts.)

4.1.2 Mobilität

Seit Jahren geben IT-Manager bei der Frage nach den wichtigsten Aufgabenstellungen für die IT an, dass Mobilität ein Schlüsselthema ist. Kein Wunder, für immer mehr Mitarbeiter in den Unternehmen gibt es keinen festen Schreibtisch im Büro mehr, sondern sie arbeiten dort, wo sie sich gerade aufhalten. Im Homeoffice, in der Flughafen-Lounge, in der Eisenbahn, auf dem Autobahn-Rastplatz und vielleicht auch mal an einem Schreibtisch in einer Niederlassung des Unternehmens.

Es ist also zunehmend wichtig, dass die Mitarbeiter erstens jederzeit, komfortabel und sicher auf die Unternehmensdaten zugreifen können. Zweitens muss aber auch dafür Sorge getragen werden, dass die mobilen Arbeitsplätze trotzdem vernünftig verwaltet werden können und beispielsweise mit aktuellen Gruppenrichtlinien, Virenscanner-Updates, Patches und neuen Softwareversionen versorgt werden. *DirectAccess* ist die neue Antwort auf diese Herausforderungen, und in der Tat halte ich die Umschreibung »VPN der nächsten Generation« nicht für untertrieben. DirectAccess ist sozusagen eine »Always-connected«-Lösung für mobile Mitarbeiter.

Mit *BranchCache* gibt es eine weitere interessante Technologie, die nicht auf den einzelnen mobilen Mitarbeiter, sondern auf Niederlassungen zielt. Da heute die meisten Mittelständler Vertriebsniederlassungen, Fertigungsstandorte und Servicestützpunkte bundesweit, europaweit und auf der ganzen Welt unterhalten, ist die Frage nach der Performance beim Zugriff über WAN-Strecken stets aktuell. BranchCache ist, wie der Name ja bereits vermuten lässt, eine intelligente Caching-Lösung, die einmal übertragene Inhalte zwischenspeichert und dann lokal zur Verfügung stellt.

Funktion	XP SP3	Vista SP1	Windows 7
DirectAccess (ständige Anbindung von mobilen Benutzern, »VPN der nächsten Generation«) nur in den Editionen *Enterprise* und *Ultimate*. Benötigt weiterhin einen Windows Server 2008 R2.			X (neu)

Tabelle 4.2 Neuerungen im Bereich Mobilität

Funktion	XP SP3	Vista SP1	Windows 7
VPN Reconnect (sorgt dafür, dass VPN-Tunnel bei Verbindungsunterbrechungen nicht geschlossen werden)			X (neu)
BranchCache (Zwischenspeicherung von Inhalten, um Zugriffe über WAN-Verbindungen zu minimieren) nur in den Editionen *Enterprise* und *Ultimate*. Benötigt weiterhin einen Windows Server 2008 R2.			X (neu)
Mobile Broadband (direkte Unterstützung für UMTS-Karten)			X (neu)

Tabelle 4.2 Neuerungen im Bereich Mobilität (Forts.)

Neben den in Tabelle 4.2 genannten Themen ist für die Unterstützung des mobilen Arbeitens natürlich auch die Optimierung des Power-Managements zu erwähnen. Hier kann ich zwar nicht von größeren Revolutionen berichten, trotzdem ist auch an diesen eher unauffälligen Verbesserungen gearbeitet worden.

Sicherheit und Mobilität lassen sich regelmäßig schlecht voneinander abgrenzen. Daher könnte man die Festplattenverschlüsselung im Grunde genommen auch zu den Mobilitäts-Features zählen: Kein Notebook sollte heute mehr ohne verschlüsselte Festplatten herumgetragen werden!

4.1.3 Deployment

Bekanntlich fängt für Administratoren die Arbeit schon an, lange bevor der Benutzer seinen Windows 7-PC zum ersten Mal zu Gesicht bekommt. Wenn Sie nicht nur einige wenige PCs in einem Kleinunternehmen administrieren, sondern für mehrere Dutzend, Hundert oder gar Tausend Systeme verantwortlich sind, ist es absolut notwendig, dass das Betriebssystem einfach zu installieren ist.

Die meisten Unternehmen haben Windows NT, 2000 und XP nach der altbewährten Methode ausgerollt:

- Master-PC-Images erstellen (für jeden Hardware-Typ und Aufgabenbereich ein Image)
- Ghost-Image erstellen
- Ghost-Image auf PCs aufbringen und *Newsid* ausführen bzw. das Image mit *Sysprep* vorbereiten und den Mini-Setup-Wizard durchlaufen lassen

Diese Methode würde zwar nach wie vor funktionieren, ist aber aus verschiedenen Gründen nicht mehr zeitgemäß: Dies fängt bei der Pflege des Images an, geht

über das Management der Treiber und endet bei der Aktivierung. Seit Windows Vista ist es eben nicht mehr so, dass Volumenlizenzen nicht aktiviert werden müssen, wie es bei XP noch der Fall war.

Funktion	XP SP3	Vista SP1	Windows 7
Deployment Image Servicing & Management (mounten und bearbeiten eines WIM-Images)		X	X (verbessert)
Dynamic Driver Provisioning (während der Installation dynamisch Treiber hinzufügen)			X (neu)
Volumen-Aktivierung (Aktivierung der Betriebssysteme mit MAK und KMS)		X	X (verbessert)
Multicast Multiple Stream Transfer (unterstützt die gleichzeitige Installation von vielen Systemen)			X (neu)
User State Migration Tool (hilft beim »Umziehen« eines Benutzers auf einen neuen PC)	X	X	X (verbessert)
VHD Image Management & Deployment (Installationsunterstützung für VHD-Medien, als Ergänzung zu WIM)			X (neu)
Booten von VHD-Medien			X (neu)

Tabelle 4.3 Neuerungen im Bereich Deployment

Microsoft stellt das WAIK (*Windows Automated Installation Kit*) im Download Center zur Verfügung. In diesem finden sich neben ausführlichem Dokumentationsmaterial diverse Werkzeuge, um das Deployment des Betriebssystems zu vereinfachen und zu beschleunigen.

Eine wichtige Deployment-Komponente bringt der Windows Server 2008 mit, nämlich die *Windows Deployment Services* (WDS, Windows-Bereitstellungsdienste). WDS ermöglicht unter anderem das Booten aus dem Netzwerk und ist in das Deployment-Konzept bestens integriert.

4.1.4 Management

Für Administratoren stellt sich natürlich die Frage, wie eine Umgebung optimal zu verwalten ist. *Das* wesentliche Hilfsmittel sind natürlich nach wie vor die Gruppenrichtlinien, die um diverse weitere Konfigurationsmöglichkeiten erweitert worden sind. Für die Automatisierung von Aufgaben ist nun die *Windows PowerShell* standardmäßig vorhanden, und wenn ein PC nicht mehr bootet, hilft das *Windows Recovery Environment* (Windows RE). Windows RE stellt eine wei-

tere startbare Umgebung bereit, von der aus Reparaturmaßnahmen durchgeführt werden können.

In Unternehmen, die in mehreren Ländern tätig sind, stellt sich regelmäßig die Frage, ob Benutzer Installationen in ihren jeweiligen Landessprachen erhalten können. Dies ist zwar generell immer möglich gewesen, war aber eher umständlich – und zwar sowohl beim Deployment als auch bei der Administration und Pflege. Mit Windows 7 ist es nun sehr simpel, dem Installations-Image weitere Sprachpakete hinzuzufügen. Sofern gewünscht, können verschiedene Benutzer auf einem PC in unterschiedlichen Sprachen arbeiten.

Funktion	XP SP3	Vista SP1	Windows 7
Windows PowerShell 2.0	Download	Download	X
Gruppenrichtlinien-Einstellungen (Preferences)	Download	X	X
Windows Recovery Environment (booten einer weiteren Instanz, um Probleme zu beheben)		X	X (verbessert)
Windows Troubleshooting Platform			X (neu)
Unified Tracing	X	X	X (verbessert)
Problem Steps Recorder			X (neu)
Mehrsprachigkeit nur in den Editionen *Enterprise* und *Ultimate*	X	X	X (verbessert)

Tabelle 4.4 Neuerungen im Bereich Management

4.1.5 Suche

Es ist eine traurige Erkenntnis, dass die meisten Unternehmen und Organisationen terabyteweise Daten horten und jedes Jahr neue Festplatten dazukaufen, die Benutzer aber effektiv auf nicht viel mehr Informationen zugreifen können. Das Problem ergibt sich primär aus zwei Gründen:

- Das klassische Dateisystem ist als Informationsablage eindeutig nicht geeignet. Es gibt intelligentere Möglichkeiten, allen voran *Microsoft SharePoint*.
- Die Benutzer können nicht oder nur sehr rudimentär suchen.

Windows 7 verfügt über einige neue Suchmöglichkeiten, wobei die bekannte Desktop-Suche nun auch »in einem Guss« Informationen einbeziehen kann, die

außerhalb des lokalen PCs liegen. Das ist im Unternehmensumfeld natürlich sehr wertvoll, da die Daten ja schließlich nicht auf lokalen Festplatten liegen (bzw. liegen sollten), sondern auf unterschiedlichen Servern zu finden sind.

Funktion	XP SP3	Vista SP1	Windows 7
Desktop Suche	Download	X	X (verbessert)
Bibliotheken (bessere Organisation von lokalen Dateien)			X (neu)
Search Federation			X (neu)
Enterprise Search Scopes nur in den Editionen *Enterprise* und *Ultimate*			X (neu)

Tabelle 4.5 Neuerungen im Bereich Suche

4.1.6 Zusammenarbeit mit Windows Server 2008 R2

Sie werden in der Liste der Neuerungen Windows 7-Komponenten gefunden haben, die nur in Zusammenarbeit mit einem Windows Server 2008 R2 funktionieren – dies sind speziell DirectAccess und BranchCache. Andere Features, wie das Speichern von BitLocker-Schlüsseln im Active Directory, funktionieren auch mit älteren Serverversionen.

Wenn Sie diese Features nutzen möchten, sind Sie keinesfalls gezwungen, sämtliche Server in Ihrer Umgebung auf Windows Server 2008 R2 umzustellen, es betrifft jeweils nur einen bzw. wenige Server.

Um der Frage zuvorzukommen: Wenn Sie keinen einzigen Server einsetzen, auf dem Windows Server 2008 läuft, können Sie selbstverständlich erfolgreich Windows 7 einsetzen – es gibt dann eben kein DirectAccess und kein BranchCache.

4.2 Editionen und Lizenzen

Windows 7 ist, wie auch seine Vorgängerversionen, kostenpflichtig – das ist keine Überraschung.

Wenn Sie zum ersten Mal auf eine Windows 7-Preisliste schauen, werden Sie eine Vielzahl von Editionen zu unterschiedlichen Preisen finden – da ist es notwendig, einmal genauer hinzusehen.

Weiterhin möchte ich in einem der folgenden Unterabschnitte daran erinnern, dass neben der Windows 7-Lizenz auch Client-Zugriffslizenzen (CAL, Client Access License) notwendig werden.

4.2.1 Editionen

Von den meisten Microsoft-Produkten gibt es verschiedene Editionen, die sich im Leistungs- bzw. Feature-Umfang unterscheiden. Erwartungsgemäß ist ein weiteres wesentliches Unterscheidungsmerkmal der Preis, sodass es sich lohnt, sorgfältig zu prüfen, welcher Bedarf tatsächlich besteht.

Zu XP-Zeiten war es noch verhältnismäßig einfach, da gab es eine Edition für Unternehmen (*XP Professional*) und die für den engagierten Heimanwender (*XP Home*). Windows 7 gibt es in hingegen in sechs Editionen:

- *Starter*: Diese Edition ist deutlich eingeschränkt und insbesondere für die Verwendung auf leistungsschwacher Hardware, wie beispielsweise Netbooks gedacht. Diese Version wird nur über OEMs (Gerätehersteller) erhältlich sein. Es kann nur eine Anwendung gleichzeitig laufen, was aber auf Netbooks im Allgemeinen kein Problem sein sollte.
- *Home Basic*: Diese Edition ist für preis-sensible Märkte gedacht, sie bietet beispielsweise keine Aero-Oberfläche und kein Media Center.
- *Home Premium*: Dies ist die Edition, die sich auf den meisten Consumer-PCs finden wird. Sie beinhaltet sämtliche Multimedia-Features, ist allerdings im Unternehmensbereich nicht einsetzbar, unter anderem schon deshalb, weil kein Beitritt zu einer Domäne möglich ist.
- *Professional*: Die Professional-Edition ist für die Szenarien gedacht, in denen zuvor *Windows Vista Business* eingesetzt wurde. Sie kann in Unternehmensnetzen genutzt werden, bietet aber keine Premium-Funktionen wie beispielsweise BitLocker, DirectAccess und BranchCache.
- *Enterprise*: Die Enterprise-Edition verfügt über sämtliche *Premium*-Features. Diese Edition ist nur im Rahmen eines Volumenlizenzvertrags erhätlich. Sie enthält kein *Windows Media Center*, was ja auch im Normalfall nicht im Business-Einsatz benötigt wird.
- *Ultimate*: Dies ist die größte Edition, alles ist drin: *Premium*-Features und *Media Center*.

In Tabelle 4.6 finden Sie einen detaillierten Vergleich der Möglichkeiten der Editionen.

Funktion	Starter	Home Basic	Home Premium	Professio-nal	Ultimate	Enterprise
HomeGroup-Unterstützung	X	X	X	X	X	X
Unbegrenzt viele Anwen-dungen	nur 3	X	X	X	X	X
Mobilitäts-center		X	X	X	X	X
Erweiterte Netzwerk-funktionen		X	X	X	X	X
Aero Glass-Oberfläche			X	X	X	X
Windows Media Center			X	X	X	
Multi-Touch			X	X	X	X
Verschlüsseltes Dateisystem (EFS)				X	X	X
Domänen-anbindung				X	X	X
Remote Desktop				X	X	X
XP Mode					X	X
BitLocker					X	X
BitLocker To Go					X	X
AppLocker					X	X
DirectAccess					X	X
BranchCache					X	X
Unterstützung mehrerer Sprachen					X	X
Booten von virtuellem Laufwerk					X	X

Tabelle 4.6 Die Editionen im Vergleich

Versionen für den Unternehmenseinsatz

Da Sie als Leser dieses Buchs Windows 7 für den Unternehmenseinsatz benötigen, lichtet sich der Editionsdschungel sehr schnell. Es kommen nur zwei Varianten in Frage:

- *Professional*: Wenn jetzt und zukünftig kein Bedarf für die Premium-Features (BitLocker, AppLocker, DirectAccess, BranchCache und Multilanguage-Support) besteht, wählen Sie die Professional Edition.
- *Enterprise/Ultimate*: Wenn Sie ein oder mehrere der Premium-Features nutzen möchten, wählen Sie die Ultimate- oder Enterprise-Edition.
  Wenn Sie kein Volumenlizenzkunde sind, müssen Sie sich für Ultimate entscheiden. Wenn Sie Volumenlizenzkunde sind, dürfte die Enterprise-Edition die günstigere Wahl sein. Die Enterprise-Edition enthält nicht das Media Center, was aber zu verschmerzen sein dürfte.

Es zwingt Sie niemand, auf allen PCs die gleiche Edition einzusetzen. Sie können nach Bedarf die Professional- und die Enterprise/Ultimate-Edition mischen. Ob die Ersparnis dann aber die Mehraufwände beim Management aufwiegt, darf zumindest bezweifelt werden.

4.2.2 Zugriffslizenzen (CALs)

Wenn Sie Windows 7-Lizenzen für Ihre PCs und Notebooks erworben haben, ist das gut, aber erst ein Teil der notwendigen Lizenzen. Zugriffe auf Microsoft-Server müssen in der Regel lizenziert werden. Es handelt sich dabei um Client-Zugriffslizenzen (CAL, Client Access License).

Auf Abbildung 4.4 sehen Sie ein kleines Netz, in dem ein Domänencontroller, ein Dateiserver, ein SQL-Server und ein Exchange-Server vorhanden sind. Sie benötigen für den Windows 7-PC noch folgende CALs:

- 1 Windows-CAL: Diese berechtigt Sie generell zum Zugriff auf die im Serverbetriebssystem enthaltenen Dienste. In diesem Fall werden die Domänencontroller- und die Dateiserver-Funktionalität in Anspruch genommen, weiterhin erfolgen authentifizierte Zugriffe auf das Betriebssystem des SQL- und des Exchange-Servers.

1. 1 SQL-Server-CAL
2. 1 Exchange-CAL

CALs

Sie benötigen nur eine Windows-CAL und nicht vier Windows-CALs, weil Microsoft bei diesen CALs eine Lizenzierung pro Arbeitsplatz anbietet, d. h., Sie kaufen CALs für jeden PC und dieser kann auf beliebig viele Server im Netz zugreifen.

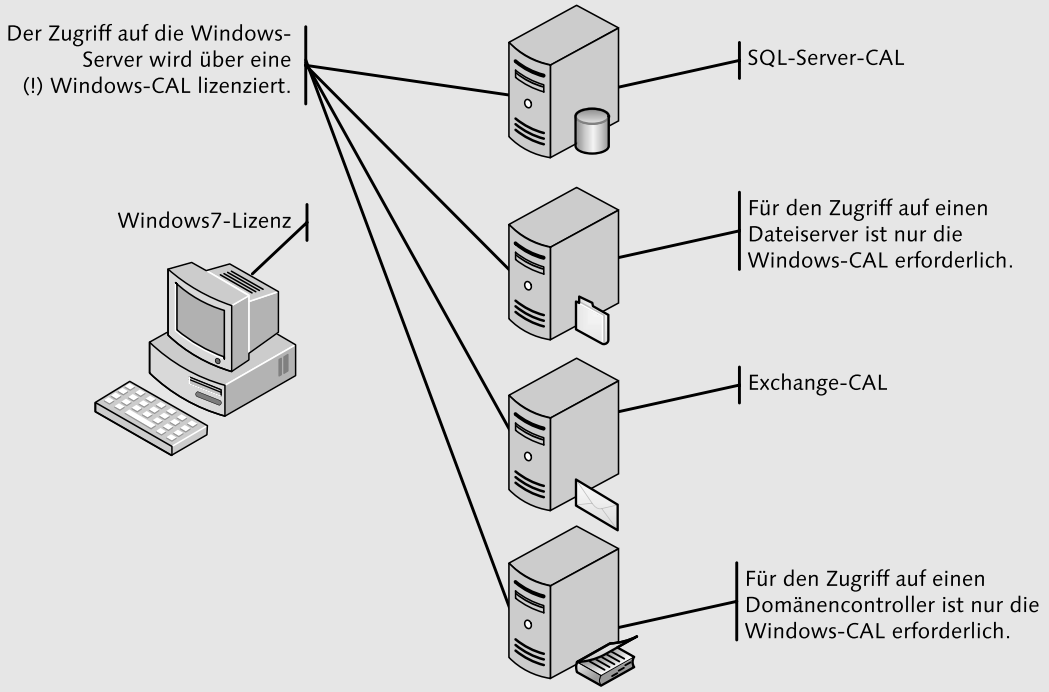


Abbildung 4.4 Neben der Windows 7-Lizenz benötigen Sie für den Zugriff auf Server entsprechende Client-Zugriffslizenzen (CALs).

Eventuell verfügt Ihr Unternehmen über umfassendere Lizenzverträge, bei denen mittels einer »universalen CAL« (die dann *Core CAL* heißt) der Zugriff auf Betriebssysteme und Applikationsserver lizenziert wird.

Ich möchte in diesem Technik-Buch nicht weiter auf die Tücken und Optimierungsmöglichkeiten der Lizenzbeschaffung eingehen – mir ist aber wichtig, dass Sie im Hinterkopf haben, dass die Zugriffe auf Server aller Art grundsätzlich nicht durch den Erwerb des Windows 7-Betriebssystems abgedeckt sind.

4.2.3 Lizenzverträge

Wenn Sie den Lizenzbedarf, also die benötigte Anzahl an Lizenzen, ermittelt haben, geht es darum, die günstige Beschaffungsvariante zu finden. Verschiedene Arten von Volumen-Lizenzverträgen, beispielsweise Open, *Enterprise Agreement* oder *Select* stehen zur Auswahl. Somit gibt es bei der Lizenzierung zwei Fragestellungen:

- Welche Lizenzen werden in welcher Stückzahl benötigt?
- Wie beschafft man diese am besten?

Ich möchte Ihnen an dieser Stelle dringend empfehlen, das Thema sehr ernst zu nehmen. Einerseits geht es natürlich um die rechtliche Sicherheit, bei der Lizenzierung »alles richtig« zu machen.

Andererseits sind durchaus Einsparpotenziale zu finden: Etliche Kunden sind überlizenziert und/oder sind durch eine eher willkürliche Lizenzbeschaffung in einer insgesamt sehr ungünstigen Kostensituation. Ein fundiertes Software-Management nebst einer Auswahl der optimalen Vertragsformen können hier durchaus finanzielle positive Ergebnisse bringen.

Da dies in erster Linie ein Technik-Buch ist, möchte ich hier nicht weiter in die Tiefen und Untiefen der Microsoft-Lizenzmodelle einsteigen. Empfohlen sei allerdings die SAM-(Software Asset Management-)Webseite, die Microsofts Ansatz für die Lizenzverwaltung vorstellt. Dort gibt es auch Kontaktdaten von Partnern, die sich genau auf dieses Thema spezialisiert haben: *http://www.microsoft.com/germany/sam/default.mspx*.

Dieser schenkte ihm Glauben und ließ den Kyros festnehmen, um ihn hinzurichten; seine Mutter aber bat ihn los und bewirkte seine Rücksendung in seine Statthalterschaft.

5 Einige Technologiegrundlagen

In diesem Kapitel möchte ich Ihnen einige Technologiegrundlagen vorstellen. Wenn Sie Windows 7 einsetzen, werden Sie es mit vielerlei Technologiebereichen zu tun bekommen. Dies beginnt mit Fragestellungen rund um das TCP/IP-Protokoll, geht über die Zertifikatsdienste und endet bei den Möglichkeiten der VPN-Anbindung.

Da dies ein Buch für IT-Professionals ist, werde ich Ihnen nicht erklären, was eine Domäne und was ein Domänencontroller ist. Ich werde stattdessen einige Bereiche aus dem erweiterten Umfeld des Clientbetriebssystems herauspicken, die meiner Erfahrung nach häufig zu Verständnisschwierigkeiten führen.

5.1 Netzwerk

Vermutlich werden Sie Windows 7 im Netzwerk einsetzen, also geht der erste Blick dieses Kapitels auf diesen Bereich. Denjenigen Lesern, die bereits mit Windows Vista gearbeitet haben, ist es nicht neu, dass Sie neben der IPv4-Adresse standardmäßig auch eine IPv6-Adresse erhalten (Abbildung 5.1). Keine Frage, IPv6 gehört die Zukunft, aber diese ist in den meisten Unternehmen noch nicht angekommen, zumal es im europäischen Internet auch noch überhaupt keinen größeren (!) Provider gibt, der seine Kunden standardmäßig mit IPv6-Adressen versorgt. Ich sehe heute (Spätsommer 2009) noch keine zwingende Notwendigkeit, im Unternehmensnetz eine nachhaltige und ganzheitliche IPv6-Einführung voranzutreiben. Allerdings kommt IPv6 näher: Wenn Sie DirectAccess einsetzen, müssen Server und Clients zumindest teilweise IPv6 »sprechen« und eine der Tunneltechnologien (*6to4, Teredo, ISATAP*) nutzen.

Ebenfalls bereits aus Vista bekannt ist das *Netzwerk- und Freigabecenter* (Abbildung 5.2). Unter anderen wird hier eine Netzwerkverbindung einem Netzwerkstandort zugeordnet (Domäne, Heimnetzwerk, öffentliches Netz).

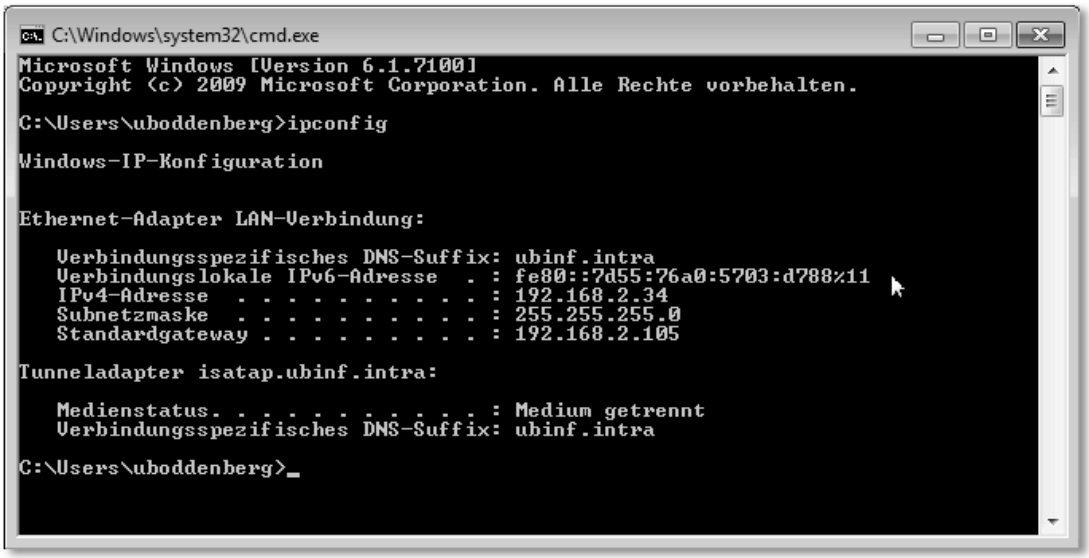


Abbildung 5.1 Windows 7 »spricht« standardmäßig IPv6.

Anhand des zugeordneten Netzwerkstandorts wird unter anderem das Regelwerk der Windows-Firewall gewählt. Im Normalfall gibt es an dieser Stelle zwar keine »Unfälle«; dennoch macht es Sinn, diese Mechanismen zu kennen.

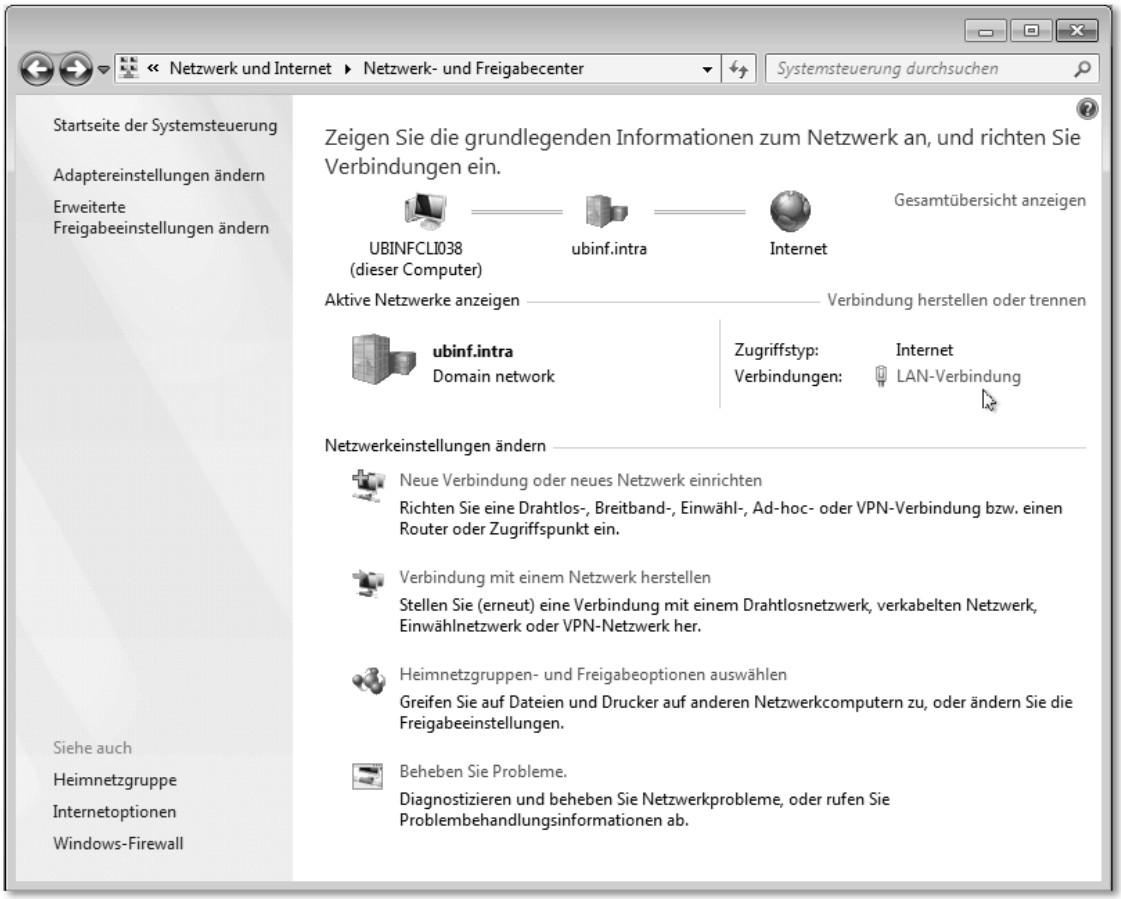


Abbildung 5.2 Das Netzwerk- und Freigabecenter von Windows 7

5.1.1 IPv4 vs. IPv6

Spricht man ganz allgemein über Netzwerkprotokolle, denken die meisten Personen vermutlich zuerst an TCP/IP. Ich möchte in diesem Buch nicht die Grundlagen des IP-Protokolls durchkauen, da diese jemandem, der sich professionell mit IT-Systemen beschäftigt, geläufig sein dürften.

Bei Upgrades auf moderne Client- oder Serverbetriebssysteme oder den vorgeschalteten Strategie-Workshops stellen mir viele Kunden die Frage, »Uli, sollten wir nicht gleich auch IPv6 einführen?«. Ist ein Unternehmen hinreichend modern ausgestattet, also mit Windows Server 2003/2008 und XP und Windows 7/Vista im Clientumfeld, liegt der Gedanke nahe, dass eine nachhaltige Einführung von IPv6 gar nicht so kompliziert sein kann, zumal IPv6 ja bereits durch Autokonfiguration, Neighbour Discovery und diverse andere Möglichkeiten einigermaßen »handhabbar« erscheint.

Um es gleich vorweg zu nehmen: Derzeit gibt es meines Erachtens für die IT-Abteilungen in mittelständischen Unternehmen deutlich wichtigere Dinge zu tun, als sich ausgerechnet mit der Einführung von IPv6 zu beschäftigen. Es ist keine Frage, dass IPv6 irgendwann auf der Tagesordnung stehen wird, aber es gibt derzeit noch etliche Aspekte, die dagegen sprechen, sofort darauf zu setzen:

- *Netzwerkinfrastruktur*: Windows Server 2008 (und auch WS 2003 auf entsprechendem Patch-Level) und auch die aktuellen Clientbetriebssysteme (Windows 7/Vista und XP auf entsprechendem Patch-Level) unterstützen IPv6. Gut! Vermutlich wird aber nur ein kleiner Teil der sonstigen Netzwerkkomponenten tatsächlich IPv6 unterstützen, geschweige dafür konfiguriert sein. Ich denke hier an Router, Firewalls, Switches, WLAN-Access-Points, Netzwerkdrucker und sonstiges Equipment. Sind im Netz noch reine IPv4-Komponenten vorhanden, müssen Sie entweder die IPv4- und IPv6-Infrastruktur parallel betreiben oder aber Umsetzungstechnologien wie ISATAP, 6to4 oder Teredo einsetzen. Man kann das alles machen, es ist aber nicht unbedingt simpel.

  Es ist keine Frage, dass Sie bei Neuanschaffungen im Netzwerkbereich unbedingt auf IPv6-Fähigkeit achten sollten – solange aber der überwiegende Teil der Komponenten nur IPv4 beherrscht, wird eine IPv6-Einführung unnötig kompliziert.

- *Das europäische Internet*: Man spricht zwar davon, dass die IPv4-Adressen knapp werden, die Situation ist im asiatischen Raum allerdings deutlich kritischer als im europäischen – ich vermute die Mehrheit der Leser in Europa, obwohl ich bereits auch eine Leserzuschrift aus China bekommen habe. In Europa sind viele Provider demzufolge gar nicht so sehr bemüht, möglichst

schnell auf den IPv6-Zug aufzuspringen und ihre Kunden dafür zu begeistern. Nun ist festzuhalten, dass man ein UnternehmensNetz mit einigen Hundert, einigen Tausend oder auch einigen Zehntausend PCs ganz prima mit der »alten« IP-Technologie aufbauen kann. Interessant wird es dann schon eher, das IPv6-Internet zu integrieren und die Vorteile zu nutzen. Solange aber viele Provider noch nicht so ohne Weiteres in der Lage sind, ganz selbstverständlich IPv6-Adressbereiche an ihre Kunden zu vergeben, sehe ich keine zwingende Notwendigkeit, das lokale Netz mit großen Anstrengungen komplett auf IPv6 zu migrieren.

Es sollte nicht unerwähnt bleiben, dass IPv6 keine triviale Technologie ist. Insbesondere in Unternehmen, die über mehrere Standorte verteilt sind, muss man sich schon einigermaßen intensiv Gedanken über Routing-Strukturen, Adressvergabe, Namensauflösung und dergleichen mehr machen. Auch der Übergang vom lokalen IPv6-Netz in das IPv6-Internet muss sorgfältig konzipiert und umgesetzt werden. Der Gedanke, dass man im Zuge des ersten *Windows Server 2008*-Systems oder bei der Einführung der ersten Windows 7-Clients »mal eben schnell« auch IPv6 implementiert, ist also maximal unrealistisch.

Ein weiterer Aspekt wäre an dieser Stelle noch zu nennen: Wenn Sie zu Ihrem Geschäftsführer gehen und ihm die Idee IPv6-Einführung vorstellen, werden Sie ihm erklären müssen, wo der konkrete Business Value liegt – also wie und warum das Unternehmen mehr Geld verdient, wenn es IPv6 einführt. Schließlich ist die IPv6-Einführung ein teures Vergnügen, weil Sie vermutlich jede Menge Equipment (z. B. neue Router und Switches) einkaufen müssen und sich intensiv mit der Thematik befassen oder externe Consulting-Leistung einkaufen müssen.

Es ist völlig klar, dass Ihr Unternehmen irgendwann den IPv6-Schritt gehen muss – es dürfte aber ziemlich schwierig bis unmöglich sein, die Argumente zu finden, warum man das heute und nicht in drei Jahren tun muss.

Es gibt durchaus Situationen, in denen es auch heute zu empfehlen ist, sich sehr intensiv mit IPv6 zu beschäftigen. Wenn Sie aber nicht zufällig bei einem Provider arbeiten oder aber in einem sehr großen Unternehmen mit sehr komplexen Netzwerkanforderungen, werden Sie sich derzeit vermutlich dafür entscheiden, das Thema IPv6 zu einen späteren Zeitpunkt, vielleicht in zwei oder drei Jahren, gezielt anzugehen. Achten Sie bis dahin aber darauf, dass alle Neuanschaffungen IPv6-fähig sind.

Unterschiede

Tabelle 5.1 zeigt Ihnen einige technische Aspekte und Begriffe im Vergleich zwischen IPv4 und IPv6.

IPv4-Adressen	IPv6-Adressen
Internet address classes	Nicht verfügbar in IPv6
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IP addresses	Global unicast addresses
Private IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/10)
Autoconfigured addresses (169.254.0.0/16)	Link-Local Addresses (FE80::/64)
Textdarstellung: dezimale Darstellung, getrennt durch Punkte	Textdarstellung: hexadezimale Darstellung, getrennt durch Punkte
Darstellung der Netzwerk-Bits: Subnetzmaske in dezimale Darstellung, getrennt durch Punkte oder Präfix-Länge	Darstellung der Netzwerk-Bits: nur Präfix-Länge
DNS-Namensauflösung: IPv4 host address (A) resource record	DNS-Namensauflösung: IPv6 host address (AAAA) resource record
DNS-reverse-Namensauflösung: IN-ADDR.ARPA domain	DNS-reverse-Namensauflösung: IP6.ARPA domain

Tabelle 5.1 Tabellarischer Vergleich zwischen IPv4 und IPv6

IPv6 – die Adressierung

Die klassischen IP-Adressen, die aus vier Bytes bestehen (ww.xx.yy.zz) bezeichnet man als IPv4-(Version 4-)Adressen. Schon seit geraumer Zeit wird darüber gesprochen, dass diese Adressen relativ schnell knapp werden. Zumindest in Europa ist zwar dem Vernehmen nach noch keine dramatische Adressknappheit eingetreten, was aber nur eine Frage der Zeit ist.

IPv4 unterstützt 2^{32} Adressen. In leichter vorstellbarer Notation ergibt das 4.294.967.296 Adressen, also etwas über 4 Milliarden. Wenn man überlegt, dass in Zukunft jede Uhr, jeder Kühlschrank und jeder Heizkörper eine IP-Adresse haben wird, wird klar, dass in absehbarer Zeit etwas geschehen muss. Als IPv4 in den 1970er-Jahren entwickelt wurde, war es absolut undenkbar, dass dieser Adressraum einmal knapp werden könnte.

Die – übrigens gar nicht mal so neue – Antwort auf das Adressproblem heißt IPv6. Der neue Adressstandard arbeitet mit 128-Bit-Adressen, sodass die Anzahl der Adressen 2^{128} beträgt. Weil ich diese lange Zahl unglaublich faszinierend finde, möchte ich Sie Ihnen einmal ausgedruckt zeigen:

```
2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456
```

Für diese Zahl kenne ich übrigens keinen Namen. Warten wir einmal ab, ob auch dieser Adressraum in 30 Jahren knapp wird.

Adresssyntax

Die 32-Bit-IPv4-Adressen werden in Gruppen zu je 8 Bit unterteilt. Weil sich

```
11000000 10101000 1100100 11001001
```

für einen Menschen ziemlich schlecht liest, gibt man die vier 8-Bit-Werte in dezimaler Notation an, sodass die zuvor genannte Adresse als

```
192.168.100.201
```

geschrieben wird.

Bei den 128-Bit-IPv6-Adressen wird ähnlich vorgegangen. Zunächst sehen Sie eine IPv6-Adresse in binärer Notation:

```
00100000000000010000110110111000000000000000000000010111100111011
00000010101010100000000011111111111111100010100010011100010110 10
```

Die Begeisterung eines menschlichen Betrachters dürfte sich bei diesem Anblick einigermaßen in Grenzen halten.

Man hat sich darauf verständigt, diese Adressen in Gruppen zu jeweils 16 Bit zu unterteilen, sodass sich diese Notation ergibt:

```
0010000000000001  0000110110111000  0000000000000000  0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010
```

Und damit Administratoren keine Krise beim Eingeben von Adressen bekommen, hat man sich auf eine hexadezimale Darstellung der Gruppen geeinigt, sodass die Adresse schließlich wie folgt aussieht:

```
2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A
```

Da IPv6-Adressen des Öfteren größere Mengen von Blöcken enthalten, die nur aus Nullen bestehen, gibt es die Möglichkeit, diese Nullen-Blöcke nicht zu schreiben. Hierzu direkt ein Beispiel:

Die Adresse

```
FE80:0:0:0:2AA:FF:FE9A:4CA2
```

kann verkürzt notiert werden, und zwar als:

```
FE80::2AA:FF:FE9A:4CA2
```

Das bedeutet, dass eine Anzahl von nebeneinander liegenden Nullen-Blöcken durch :: ersetzt werden kann. Wie viele Blöcke tatsächlich weggelassen wurden, kann leicht ermittelt werden, weil eine IPv6-Adresse insgesamt immer 8 Blöcke (128 Bit) umfasst.

Hier noch ein umgekehrtes Beispiel: Die verkürzt geschriebene Adresse `FF02:30::5` (drei Blöcke) ergibt in der Langform `FF02:30:0:0:0:0:0:5`.

Zu erwähnen wäre an dieser Stelle, dass es ebenso wie bei IPv4 auch eine Subnetzmaske gibt, mit der definiert wird, wo der »Netz-Teil« der Adresse beginnt.

Adresstypen

Für IPv6 sind die folgenden drei Adresstypen definiert:

- *Unicast*: Eine Unicast-Adresse ist einem Netzwerkinterface eines Hosts zugewiesen. Dies ist letztendlich »die normale IPv6-Adresse«.
- *Multicast*: Über eine Multicast-Adresse werden null bis beliebig viele Netzwerkinterfaces eines oder beliebig vieler Hosts angesprochen.
- *Anycast*: Eine Anycast-Adresse steht sozusagen stellvertretend für beliebig viele Unicast-Adressen. Die Routing-Topologie sorgt dafür, dass die an die Anycast-Adresse gesendeten Pakete stets zu der nächsten Unicast-Adresse (bezogen auf die Routing-Distanz) gesendet werden.

Beim flüchtigen Lesen wird vielleicht der Unterschied zwischen Multicast und Anycast nicht ganz klar, daher möchte ich das noch etwas deutlicher formulieren:

- *Multicast* wird verwendet, wenn ein Host an viele andere Hosts sendet. Ein typisches Beispiel ist das Broadcasting von Multimedia-Inhalten an viele Clients.
- In einem *Anycast*-Szenario kommuniziert ein Host mit einem Zielhost. Im Gegensatz zu einem Unicast-Szenario wird der Kommunikationspartner aber durch die Routing-Topologie ermittelt.

Die *Unicast*-Adressen unterteilen sich wiederum in sechs unterschiedliche Typen:

- *Link-Local Addresses*: Diese IPv6-Adressen werden automatisch allen physikalischen und virtuellen Netzwerkschnittstellen hinzugefügt. Diese Adressen sind nur im lokalen Netzwerksegment erreichbar, können also nicht geroutet werden. Diese Adressen sind mit den 169.254.0.0/16-Adressen aus der IPv4-Welt vergleichbar.
- *Site-Local Addresses*: Diese Adressen sind eigentlich als Äquivalent zu den privaten IPv4-Adressen gedacht gewesen, wurden aber in RFC 3879 wieder »abgeschafft«. Für den Aufbau eines privaten gerouteten Netzes werden die *Unique Local Addresses* verwendet.

- *Unique Local Addresses*: Diese Adressen können im gesamten internen Netz geroutet werden, sind aber nicht über das Internet erreichbar. Aufgrund der Abschaffung der Site-Local Addresses fungieren die Unique Local Addresses als Äquivalent zu den privaten IPv4-Addressräumen.
- *Global Unicast Addresses*: Diese Adressen können im IPv6-Internet geroutet werden. Man kann diese mit den öffentlichen IPv4-Adressen vergleichen.
- *Special Addresses*: Hier sind verschiedene »spezielle« Adressen zusammengefasst. Ein Beispiel wäre die Loopback-Adresse.
- *Transition Addresses*: Zur Gewährleistung der Koexistenz von IPv4 und IPv6 sind spezielle Addressräume und -typen definiert.

Einige Adresstypen werde ich in den folgenden Abschnitten etwas genauer beschreiben:

Link-Local Addresses

Die *Link-Local Addresses* werden von einem IPv6-Host automatisch erzeugt. Auch wenn Sie bislang in Richtung IPv6 noch nichts unternommen haben, sind diese Adressen vorhanden. Ein Aufruf von `ipconfig` auf einem Windows-Server-2008-System (oder auf einem Vista-System oder einem XP/WS2003 mit installiertem IPv6) wird unter anderem die Verbindungslokale IPv6-Adresse, also die *Link-local Address* zutage fördern. Auf Abbildung 5.1 ist ein Windows 7-System gezeigt, bei dem bislang keinerlei IPv6-Konfigurationsschritte unternommen worden sind, trotzdem ist die Verbindungslokale IPv6-Adresse vorhanden.

Auch in einem weiter nicht auf die Verwendung von IPv6 vorbereiteten Netz funktioniert die Kommunikation über die Link-Local Addresses. Abbildung 5.3 zeigt, wie ein Windows-Client einen Windows Server 2008 anpingt – es klappt!

Bei aller Euphorie über die IPv6-Kommunikation zwischen den beiden Systemen sei aber darauf hingewiesen, dass das noch sehr weit von einer funktionierenden nachhaltigen IPv6-Implementation entfernt ist:

- Zunächst funktionieren die Link-Local Addresses wie zuvor erwähnt nur im lokalen Netzwerksegment.
- Da für IPv6 kein DNS-Server verfügbar ist, wird der Host sich mit dieser Adresse nicht im DNS registrieren. Somit werden andere Systeme nur dessen IPv4-Adresse finden.

Einige weitere Punkte wären dieser Aufzählung noch hinzuzufügen. Trotzdem lässt sich festhalten, dass die IPv6-Kommunikation über die Link-Local Addresses grundsätzlich funktioniert.

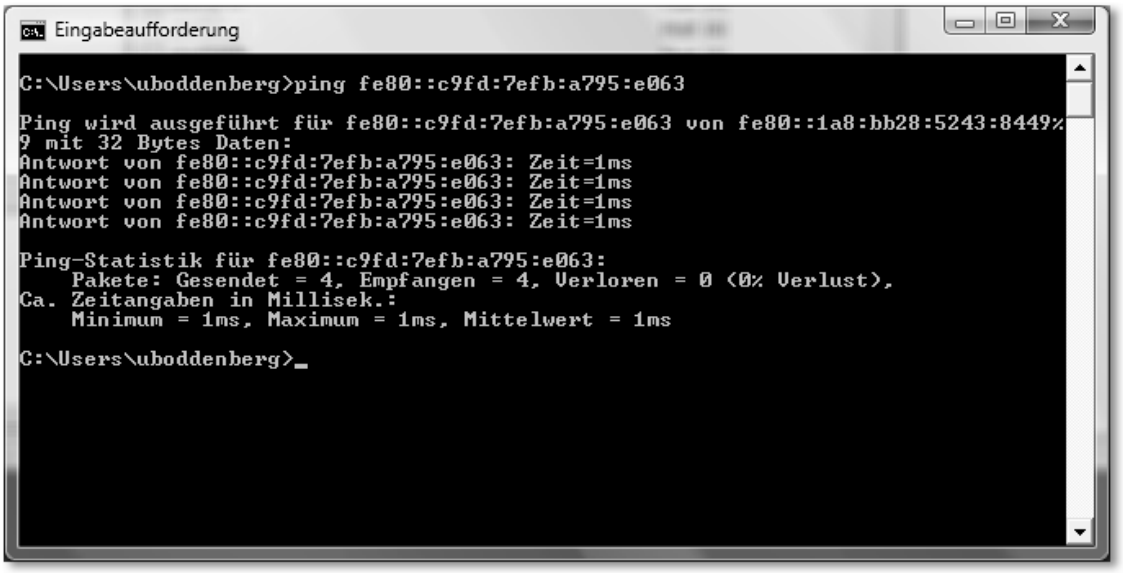


Abbildung 5.3 Netzwerkverkehr über die Link-local Addresses funktioniert auf Anhieb.

Die Link-Local Addresses werden aus einem genau festgelegten Adressbereich vergeben. Auf Abbildung 5.4 habe ich das ein wenig visualisiert:

- Die nicht routbare Netzwerkadresse ist 64 Bits lang, und für die Identifizierung des Hosts im LAN stehen ebenfalls 64 Bits zur Verfügung.
- Die ersten 10 Bits einer Link-Local Address lauten immer `1111 1110 10`. Wenn man einmal nachrechnet, entspricht die Binärzahl `1111 1110` der hexadezimalen `FE`.

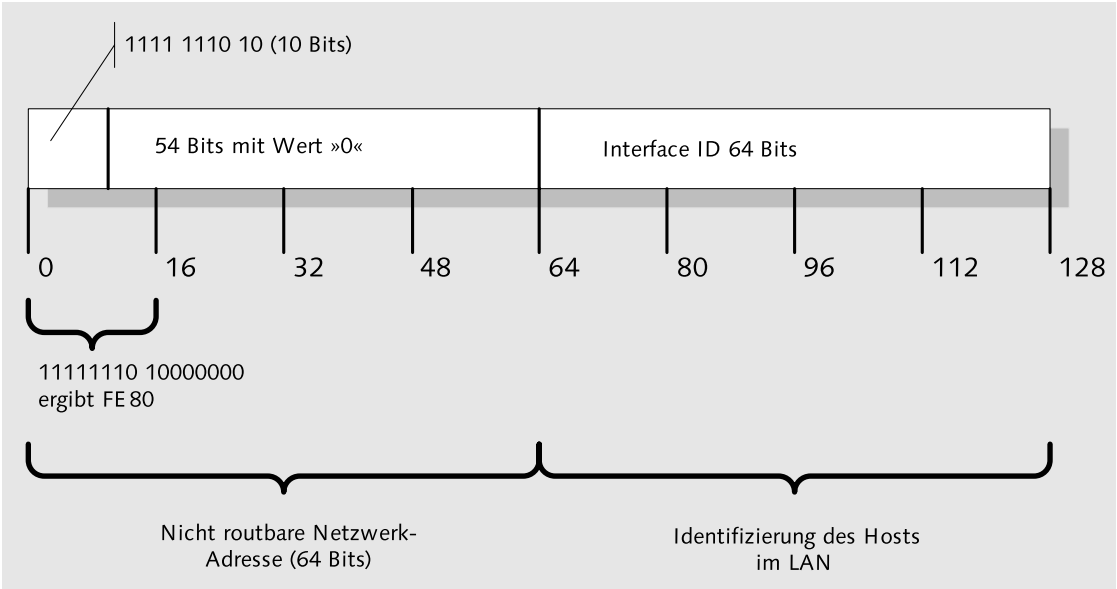


Abbildung 5.4 Link-Local Addresses

- Die weiteren 54 Bits der Netzwerkadresse werden mit Nullen aufgefüllt. Demzufolge hat der erste 16-Bit-Block den Wert `1111 1110 1000 0000`. Konvertiert man diese Zahl ins hexadezimale System, kommt `FE80` heraus. Wenn Sie zu **XXXXXXXXX** zurückblättern, werden Sie sehen, dass `FE80` der Block der Link-Local Address des Systems ist.

Unique Local Addresses

In der IPv4-Welt kennt man die für private Netze reservierten Adressbereiche, also `10.0.0.0/8`, `172.16.0.0/12` und `192.168.0.0/16`. Auch in der IPv6-Welt gibt es solche Adressbereiche. Diese nennt man *Unique Local Addresses*.

Mithilfe von Unique Local Addresses können Unternehmen und Organisationen eigene komplexe IPv6-Netze aufbauen. Der Aufbau dieses Adresstyps ist auf Abbildung 5.5 gezeigt:

- Die ersten 7 Bits einer Unique Local Address sind stets 111 101. Das achte Bit ist das Local-Flag, das anzeigt, dass es sich um eine lokale Adresse handelt (also eine Adresse, die nicht im Internet geroutet wird). Dieses Bit ist immer 1, schließlich geht es hier ja um Unique **Local** Addresses. Der Wert 0 ist übrigens nicht definiert.

  Folglich beginnt eine Unique Local Address stets mit `1111 1101`, woraus sich für den ersten Block `FD00` ergibt.
- In den nächsten 40 Bits kann das jeweilige Unternehmen bzw. die Organisation für jeden Standort (in der englischen Literatur: *Site*) eine *Global ID* bestimmen. Diese kann frei gewählt werden, allerdings wird empfohlen, diese zufällig zu wählen. Die Begründung ist, dass bei einer möglichen Unternehmensfusion, bei der zusätzliche Standorte zum Gesamtnetz hinzukommen, keine Überlappung der Adressbereiche zu erwarten ist.

  Bei 2^40 (1.099.511.627.776) Möglichkeiten müsste man schon sehr viel Pech haben, wenn für zwei Standorte zufällig dieselbe Global ID gewählt wurde.
- Die folgenden 16 Bits definieren das Subnetz innerhalb des Standorts.
- Es folgt die 64 Bit lange *Interface ID*, die die Netzwerkschnittstellen der Hosts im lokalen Netzwerksegment definiert.

Im Gegensatz zu den Link-Local Addresses werden Unique Local Addresses nicht »von selbst« vergeben, sondern müssen konfiguriert werden – besser gesagt muss die Vergabe der Adressen konfiguriert werden.

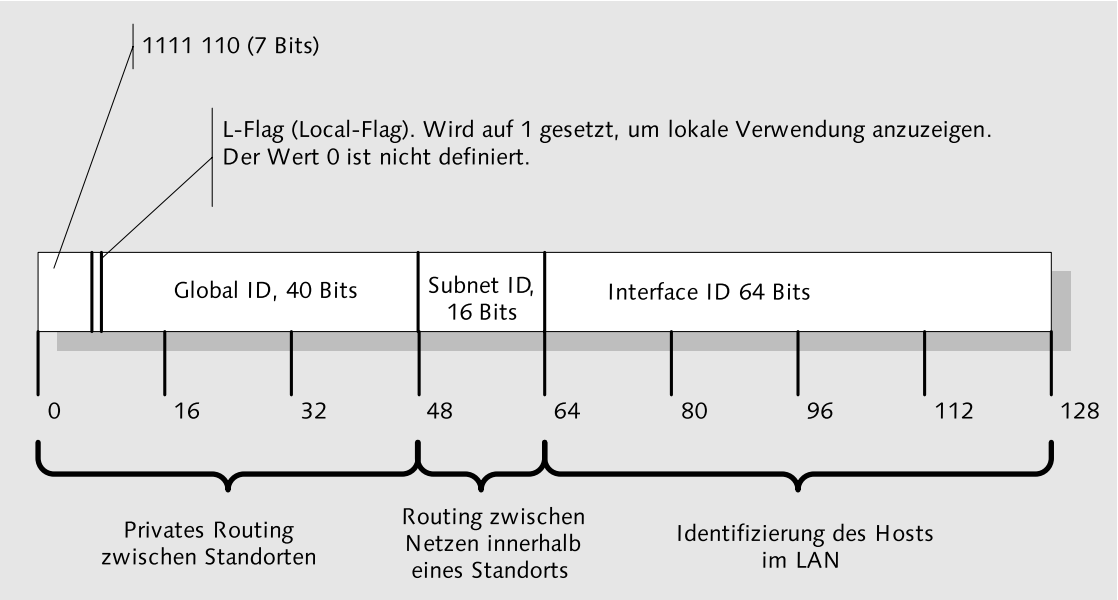


Abbildung 5.5 Aufbau einer Unique Local Address

Global Unicast Addresses

Global Unicast Addresses sind sozusagen die öffentlichen Internet-Adressen. Diese werden benötigt, um Daten durch das Internet zu transportieren. Auf Abbildung 5.6 ist der Aufbau dieser Adressen gezeigt:

- Bei einer Global Unicast Address sind die ersten drei Bits stets auf `001` gesetzt. Da für die Definition des *Global Routing Prefix* dann noch 45 Bits verbleiben, können 35.184.372.088.832 (35 Billionen!) Bereiche für die Standorte von Unternehmen bzw. Organisationen vergeben werden.
- Mit den nächsten 16 Bits werden die unterschiedlichen Netze des jeweiligen Unternehmensstandorts beschrieben.
- Es folgt die 64 Bit lange Interface ID, die die Netzwerkschnittstellen der Hosts im lokalen Netzwerksegment definiert.

Bei dem Design von IPv4 warwohl niemand auch nur im Entferntesten auf den Gedanken gekommen, dass der Adressraum irgendwann knapp werden könnte, was dann aber doch passiert ist. Um in der heutigen IPv4-Welt ein eigenes C-Netz aus dem offiziellen Internet-Adressbereich zu erhalten, muss man schon eine einigermaßen plausible Begründung vorlegen können.

Diese »Engpässe« dürften mit IPv6 endgültig der Vergangenheit angehören, denn selbst wenn jeder Erdenbürger ein eigenes Global Routing Prefix haben wollte, wäre der prozentuale Anteil der vergebenen Bereiche immer noch beinahe bei 0 %.

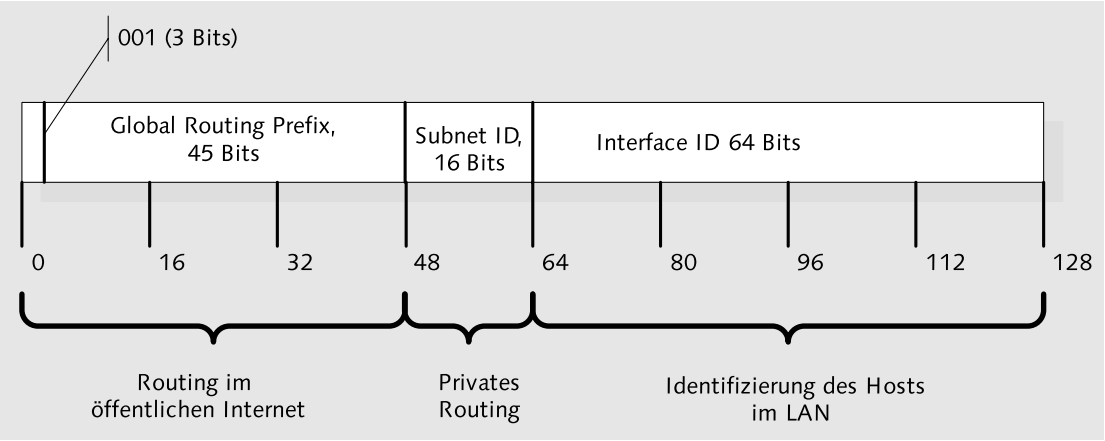


Abbildung 5.6 Aufbau einer Global Unicast Address

Vergabe von IPv6-Adressen

Es steht Ihnen selbstverständlich frei, IPv6-Adressen (genauer: Global Unicast Addresses oder Unique Local Addresses) per Hand zu vergeben. Da dies aber eher mühselig ist, haben die Entwickler von IPv6 natürlich Möglichkeiten für die automatische Adressvergabe vorgesehen, wobei es drei Varianten gibt:

- *Stateless*: In diesem Konfigurationsmodus erhält das IPv6-System die Adressinformationen, insbesondere über das Netz, in dem es sich befindet, über einen Router. Die eigentliche Host-Adresse ermittelt der Client dann selbst. Ein DHCPv6-Server ist hierbei nicht notwendig, kann aber verwendet werden, um zusätzliche Konfigurationsinformationen wie beispielsweise die Adressen von DNS-Servern und dergleichen bereitzustellen (siehe Variante *Both*).
- *Stateful*: Man spricht von einer Stateful-Configuration, wenn die Adressvergabe durch einen DHCP-Server erfolgt. Dies ist dann der Fall, wenn die Antwort des Routers dies erzwingt oder aber wenn in dem Netz kein Router vorhanden ist (oder zumindest keiner, der IPv6-*Router Advertising Messages* versendet).
- *Both*: Ein Mischbetrieb ist, wie bereits zuvor angedeutet, möglich. Die eigentliche Adressvergabe kann *stateless* erfolgen, wobei der Router per Flag (*Managed Address Configuration* oder *Other Stateful Configuration*) vorgeben kann, dass das IPv6-System weitere Konfigurationsoptionen mittels DHCPv6 beziehen soll. Diese zusätzlichen Konfigurationsoptionen können beispielsweise das Standardgateway, die Adressen der DNS-Server und dergleichen mehr sein.

Aus Sicht des IPv6-Clients ist die automatische Adresskonfiguration nicht allzu spannend, dafür muss man sich umso mehr mit den Routern auseinandersetzen.

Dieser Themenbereich geht weit über die Zielsetzung dieser kurzen Einführung in IPv6 hinaus. Ich möchte aber erwähnen, dass ein Windows Server 2008 als nativer IPv6-Router konfiguriert werden kann und somit die für die *Stateless Autoconfiguration* benötigte Rolle übernehmen kann. Falls Sie ein paar Stichworte zum Weitersuchen benötigen, zeige ich Ihnen hier den Befehl, mit dem das Routing für ein Netzwerkinterface aktiviert wird:

```
netsh interface ipv6 set interface "Local Area Connection" forwarding=enabled advertise=enabled
```

Keine Stateful Adress Configuration

An dieser Stelle sei darauf hingewiesen, dass die IPv6-Implementationen für Windows XP und Windows Server 2003 keine Stateful Address Configuration unterstützen. Windows 7/Vista und Windows Server 2008 unterstützen alle Modi.

Ich möchte an dieser Stelle nicht zu sehr ins Detail gehen, empfehle aber allen Interessierten, nach dem Stichwort *Neighbor Discovery* zu suchen und weiterzulesen. Über diesen Mechanismus werden folgende Aufgaben abgewickelt:

- Identifizieren von Routern im Netzwerk
- Identifizieren der eigenen IP-Adressen, Prefixes und sonstiger Konfigurationsaspekte
- Auflösen der Layer-2-Adressen, vergleichbar dem ARP-Protokoll bei IPv4

Abschalten von IPv6

Auch wenn Sie sich (zunächst) dafür entscheiden, keine ganzheitliche IPv6-Struktur zu planen, können Sie IPv6 auf Windows7/Vista- und Windows-Server-2008-Systemen im Allgemeinen problemlos mitlaufen lassen.

Es gibt allerdings durchaus Situationen, in denen ein aktives IPv6 »lästig« ist oder sogar zu Problemen führt. Ein Beispiel für den ersten Fall ist die Installation des DHCP-Servers: Ist IPv6 aktiv, besteht der Konfigurationsassistent ziemlich penetrant auf einer festen IPv6-Adresse.

IPv6 kann bei Windows Server 2008 und Windows Windows7/Vista nicht deinstalliert, sondern nur deaktiviert werden – ebendies gilt übrigens auch für IPv4. Sie können IPv6 entweder für jedes Netzwerkinterface einzeln deaktivieren (Abbildung 5.7) oder mittels eines Registry-Keys die IPv6-Funktionalität für das gesamte System abschalten. Der Name des Registry-Keys lautet:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisabledComponents

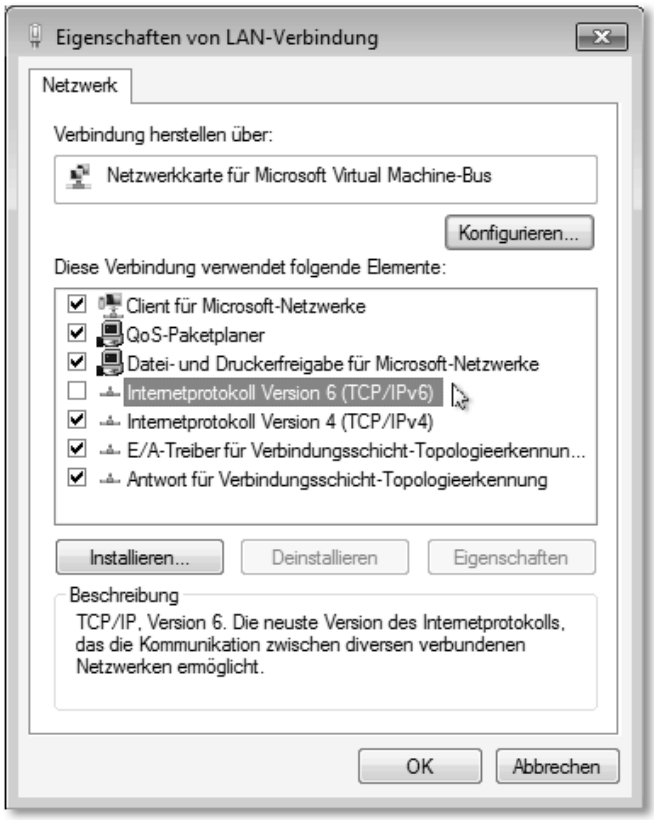


Abbildung 5.7 IPv6 kann deaktiviert, aber nicht deinstalliert werden.

Er ist vom Typ DWORD. Um die IPv6-Funktionalität komplett abzuschalten, muss als Wert `0xFF` gesetzt werden. Anzumerken wäre, dass die unterschiedlichen IPv6-Komponenten mittels dieses Werts (Bitmaske!) selektiv deaktiviert werden können. `0xFF` ist sozusagen der »Hauptschalter«.

Vorsicht bei Deaktivierung

Sie sollten sich allerdings genau überlegen, ob Sie wirklich IPv6 flächendeckend deaktivieren möchten. Es gibt Technologien, die die neue IP-Version verwenden und ohne sie nicht funktionsfähig sind. Das Paradebeispiel ist DirectAccess, das Sie in Abschnitt 13.2 kennenlernen werden.

5.2 Profile

Ein beliebtes Thema sind die Benutzerprofile. Beim Anlegen der Profile haben Sie zwei Möglichkeiten:

- lokale Profile
- servergespeicherte Profile (Roaming Profiles)

Hinter den servergespeicherten Profilen steckt im Grunde genommen ein simples Prinzip:

- In einem Active-Directory-Attribut wird ein Pfad zu dem Benutzerprofil gespeichert. Dieser Eintrag muss auf eine Dateifreigabe verweisen. Es hat sich zwar eingebürgert, eine versteckte Freigabe (sie endet mit einem $-Zeichen) zu wählen, dies ist aber keine Voraussetzung (Abbildung 5.8).
- Wenn der Benutzer sich anmeldet, wird das Profil vom Server geladen und lokal gespeichert.
- Meldet sich der Benutzer ab, wird das geänderte Profil wieder auf den Server kopiert.

Das Profil wird also niemals direkt vom Server verwendet, sondern hin und her kopiert.

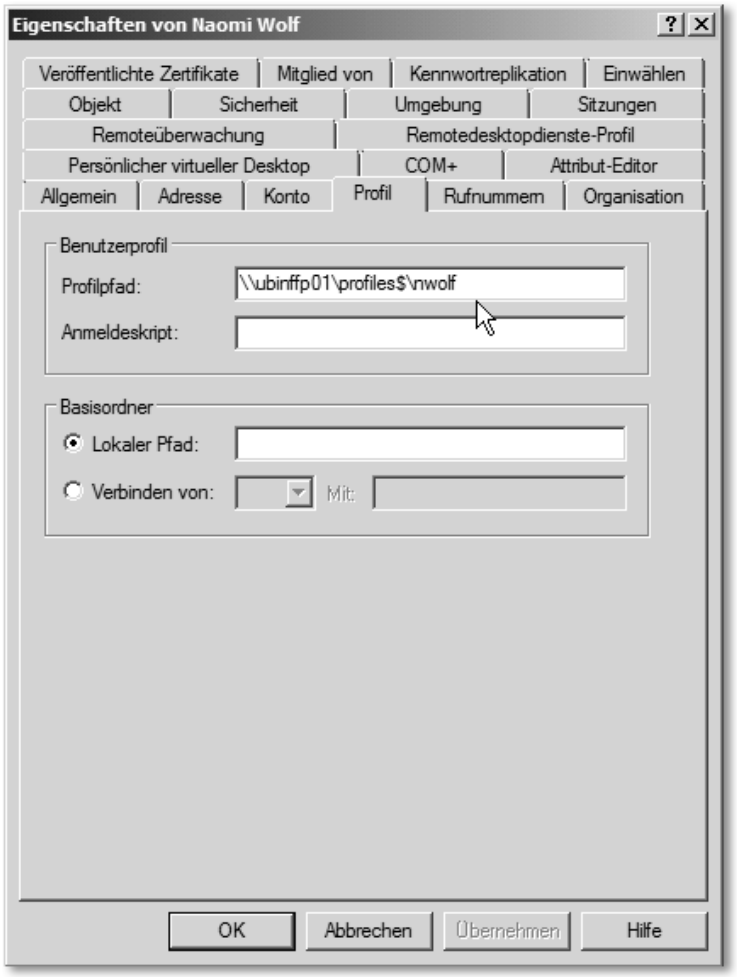


Abbildung 5.8 Ist im Active Directory ein Profilpfad angegeben, verfügt der Benutzer über ein servergespeichertes Profil.

5.2.1 Vorteile und Nachteile

Servergespeicherte Profile wurden in den frühen Anfangszeiten von Windows NT vor allem mit dem Vorteil angepriesen, dass sich ein Benutzer an jedem beliebigen PC im Netzwerk anmelden kann und stets sein individuelles Profil, also seine Einstellungen, erhält.

Dabei stellt sich natürlich zunächst die Frage, in wie vielen Umgebungen die Benutzer wirklich zwischen PCs hin- und herwandern? Hinzu kommt, dass es in einigen Unternehmen Besprechungsräume mit Präsentations-Notebooks gibt, auf denen es sogar sehr ungünstig ist, wenn alle Profileinstellungen mitgenommen werden.

Die Hauptvorteile von servergespeicherten Profilen sind:

- Das Profil des Benutzers mit allen Einstellungen und darin gespeicherten Dateien liegt auf einem Server und kann dort gesichert werden.
- Wenn ein PC ausgetauscht wird, sei es geplant oder ungeplant, brauchen Sie sich um das Benutzerprofil keine Sorgen zu machen: Alle Einstellungen werden auf dem neuen PC verfügbar sein.

Die servergespeicherten Profile haben natürlich auch Nachteile:

- Wenn Benutzer sich auf unterschiedlichen PCs anmelden, laufen Verknüpfungen wahrscheinlich ins Leere. Wenn der Benutzer normalerweise auf einem PC mit installiertem Office arbeitet, sind beispielsweise Startmenü-Verknüpfungen vorhanden. Meldet er sich nun auf einem PC ohne das Office-Paket an, werden diese Verknüpfungen nicht funkionieren.
- Wenn der Benutzer sich an einem anderen Standort des Unternehmens anmeldet, wird sein Profil über die WAN-Verbindung geholt. Eventuell ist es mehrere Gigabytes groß, was zu lästigen Wartezeiten führen kann.

Ich tendiere zwar im Allgemeinen zu servergespeicherten Profilen, insbesondere wegen stark vereinfachter PC-Austausch-Szenarien, es könnte aber auch konkret in Ihrer Umgebung gewichtige Gründe dagegen geben. Genaues Überlegen und Hinschauen macht also absolut Sinn.

5.2.2 Servergespeicherte Profile in mehrsprachigen Umgebungen

Ein mittelständisches Unternehmen wird heute vermutlich Auslandsniederlassungen in nicht deutschsprachigen Regionen haben. Es ist ein kleiner Komfortfaktor für fremdsprachige Benutzer, diese auf einem in deren Muttersprache lokalisierten Windows 7 arbeiten zu lassen. Wie Sie in Kapitel 15 sehen werden,

bieten die Windows 7-Editionen *Enterprise* und *Ultimate* eine umfassende Unterstützung für mehrsprachige Umgebungen.

Ist in einem Profil einmal eine Anpassung an eine Sprache vorgenommen worden, wird diese Sprache verwendet, sofern auf dem PC das entsprechende Sprachpaket installiert ist.

Abbildung 5.9 bringt den Beweis:

- Der Anwender meldet sich auf einem Windows 7-PC an. Die Systemsprache ist Russisch, folglich wird die Willkommensseite in dieser Sprache angezeigt.
- Hat sich der Anwender angemeldet, geht es auf Deutsch, der von ihm ausgewählten und im Profil gespeicherten Sprache, weiter.

Keine Sprachfestlegung

Sofern der Benutzer keine Sprache festgelegt hat, erscheint das Betriebssystem in der Systemsprache.

Abbildung 5.9 Systemsprache: Russisch – Anwendersprache: Deutsch. Hat der Anwender die Anmeldung in der Fremdsprache bewältigt, kann er gemäß seiner Profileinstellungen auf Deutsch weiterarbeiten.

5.2.3 Zwischenspeichern der Profile

Interessant ist die Frage, was bei einer Anmeldung passiert, wenn der Server, auf dem der Benutzer sich anmeldet, nicht vorhanden ist. Das Thema ist vor allem für

Notebook-Anwender interessant, die sich ja häufig auf dem Notebook anmelden und eben nicht mit dem Unternehmens-LAN verbunden sind. Wie bereits erwähnt, werden die Profile, die letztendlich »nur« ein Verzeichnis nebst Unterverzeichnissen sind, bei der An- und Abmeldung kopiert.

Wenn Sie nicht per Gruppenrichtlinie ein anderes Verhalten erzwingen, wird die lokale Kopie der Gruppenrichtlinie nicht gelöscht. Abbildung 5.10 zeigt einen Dialog, der über SYSTEMEIGENSCHAFTEN • ERWEITERT • BENUTZERPROFILE-EINSTELLUNGEN erreichbar ist:

- Es sind einige lokale Profile vorhanden. Es haben sich also Benutzer angemeldet, bei denen im Active Directory kein Profilpfad angegeben war.
- Für den Benutzer *ubinf\rmeier* ist ein servergespeichertes Profil vermerkt. Das Profil des Benutzers wurde bei der letzten Anmeldung vom angegebenen Serverspeicherort auf die lokale Festplatte kopiert und auch bei der Abmeldung nicht gelöscht.
  Wenn der Benutzer sich in einem Offline-Szenario anmeldet, wird das zwischengespeicherte Profil verwendet werden.

Abbildung 5.10 Die Profile werden zwischengespeichert.

5.3 Die Registry

Einem IT-Professional brauche ich wohl kaum zu erzählen, was die Registry ist. Gut. Es kann trotzdem nicht schaden, ein paar Dinge im Zusammenhang mit der Registry zu verinnerlichen. Wie Sie auf Abbildung 5.11 sehen können, gibt es fünf Hauptschlüssel:

- HKEY_LOCAL_MACHINE enthält Konfigurationsdaten für den Computer.
- HKEY_CURRENT_USER enthält die Konfiguration für den aktuell angemeldeten Benutzer.
- HKEY_USERS enthält Einstellungen für die Benutzer, die sich bereits einmal auf dem Computer angemeldet haben.
- HKEY_CLASSES_ROOT ist ein Verweis auf HKEY_LOCAL_MACHINE\Software\Classes.
- HKEY_CURRENT_CONFIG verweist auf die aktuelle Konfiguration und dient zur Beschleunigung des Zugriffs.

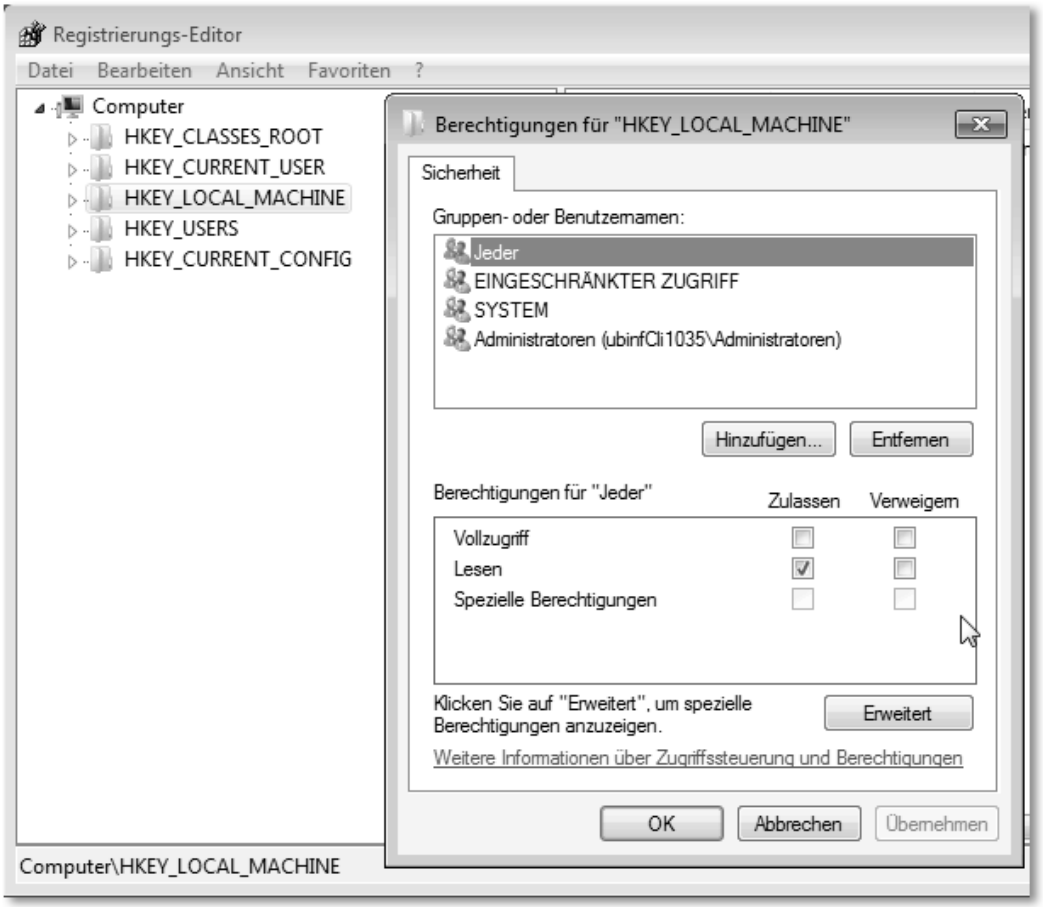


Abbildung 5.11 Auf HKEY_LOCAL_MACHINE haben normale Benutzer nur lesenden Zugriff.

Ich möchte nun eigentlich zwar nicht von wichtigen und unwichtigen Hauptschlüsseln sprechen, trotzdem gilt, dass man meistens mit HKEY_CURRENT_USER und HKEY_LOCAL_MACHINE zu tun hat. Dies sind auch die beiden Zweige, in denen Einstellungen von den Gruppenrichtlinien angepasst werden:

- HKEY_LOCAL_MACHINE-Einträge werden von den Computerrichtlinien angepasst.
- HKEY_CURRENT_USER-Einträge werden von den Benutzerrichtlinien angepasst.

Interessant ist nun, einmal die Berechtigungen dieser beiden Registry-Zweige anzuschauen:

- Auf HKEY_LOCAL_MACHINE hat zwar *Jeder* lesenden Zugriff, Änderungen vornehmen kann aber nur ein Administrator (und natürlich das SYSTEM, Abbildung 5.11).
- Auf HKEY_CURRENT_USER hat der aktuell angemeldete Benutzer Vollzugriff (Abbildung 5.12).

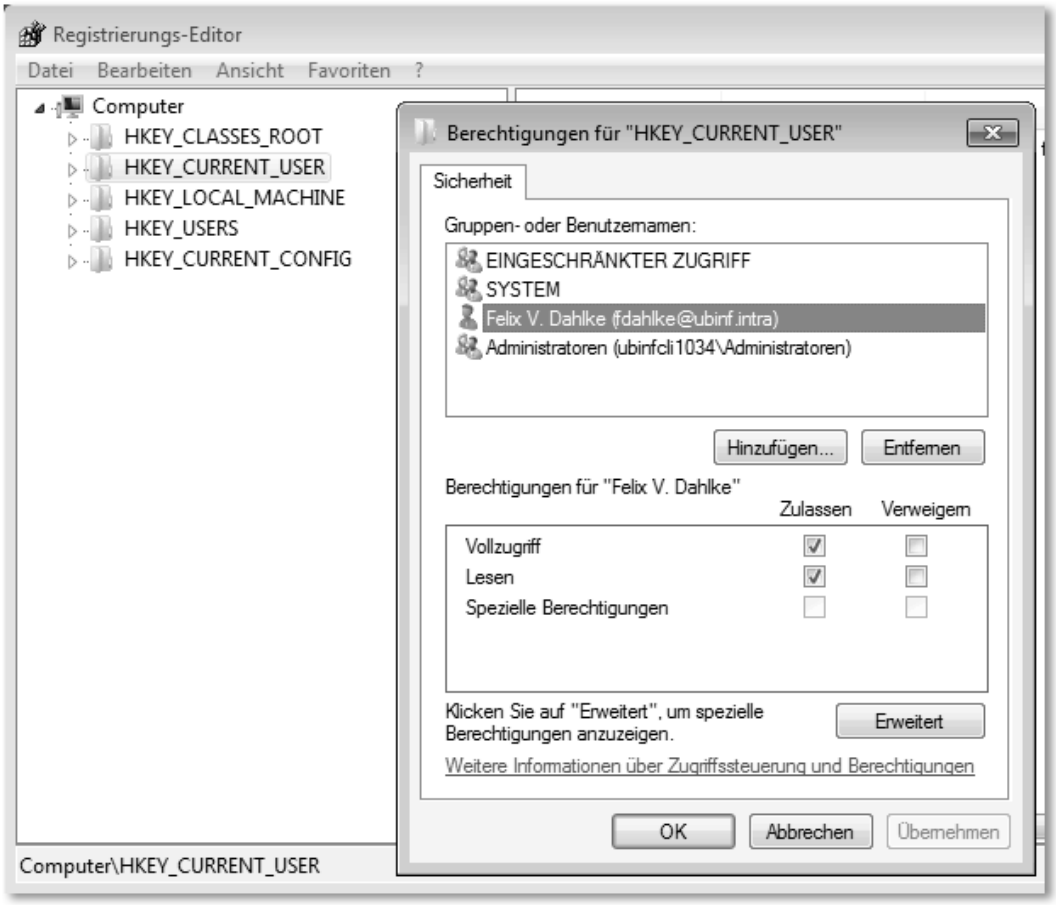


Abbildung 5.12 Auf HKEY_CURRENT_USER hat der angemeldete Benutzer (in diesem Fall fdahlke@ubinf.intra) Vollzugriff.

Mit diesem minimalen Wissen über die Berechtigungen für diese beiden Abschnitte der Registry lassen sich bereits diverse Kompatibilitätsprobleme erklären.

Es gab und gibt noch immer Programme, die darauf bestehen, in HKEY_LOCAL_MACHINE zu schreiben und dort beispielsweise das Datum des letzten Start des Programms oder die zuletzt vom Benutzer eingestellte Größe des Fensters zu speichern. Wie Sie auf Abbildung 5.11 gesehen haben, kann nun aber nur ein Administrator in diesen Bereich der Registrierung schreiben. Peng! Die Applikation verursacht einen Fehler oder stürzt gleich ganz ab, wenn der aktuelle Benutzer keine Adminberechtigungen hat.

Nun ist es natürlich für die Gesamtsicherheit der Umgebung absolut tödlich, auf das Problem mit Adminberechtigungen für jeden einzelnen Benutzer zu reagieren, zumal das User Account Control da ohnehin noch einen weiteren Riegel vorschiebt.

XP Mode als Retter

Software, die sich so verhält, ist grundsätzlich nicht bzw. nur sehr eingeschränkt Windows 7-fähig. Die einzige Rettung ist der XP Mode, der in Abschnitt 9.2, »Windows 7 XP Mode und Windows Virtual PC«, besprochen wird.

Das »Innenleben« der Registry dürfte jeder Leser bereits zu Genüge kennen. Die vorhandenen Attribute verfügen über unterschiedliche Datentypen (Text, Zahl, Binärwert) – auch in Windows 7 verhält sich das nicht anders (Abbildung 5.13).

Seit Vista/Windows Server 2008 gibt es übrigens einen weiteren Datentyp, nämlich QWORD, mit dem eine 64-Bit-Zahl repräsentiert wird. Ich habe letztens erlebt, dass beim Hinzufügen eines Registry-Werts versehentlich ein QWORD statt eines DWORDs angegeben worden ist. Der Wert (»1«) wurde dann eingetragen, was auch problemlos möglich war und somit nicht weiter auffiel. Das Ergebnis war allerdings, dass das Betriebssystem die gewünschte Änderung nicht akzeptierte: Eine QWORD-Eins ist nicht gleich einer DWORD-Eins. Die Kollegen haben den Fehler stundenlang gesucht (Abbildung 5.14).

Die Moral von der Geschicht': Man kann bei Anpassungen an der Registry nicht aufmerksam genug sein. Das ist an sich zwar hinlänglich bekannt, es gibt aber noch immer neue Fallen.

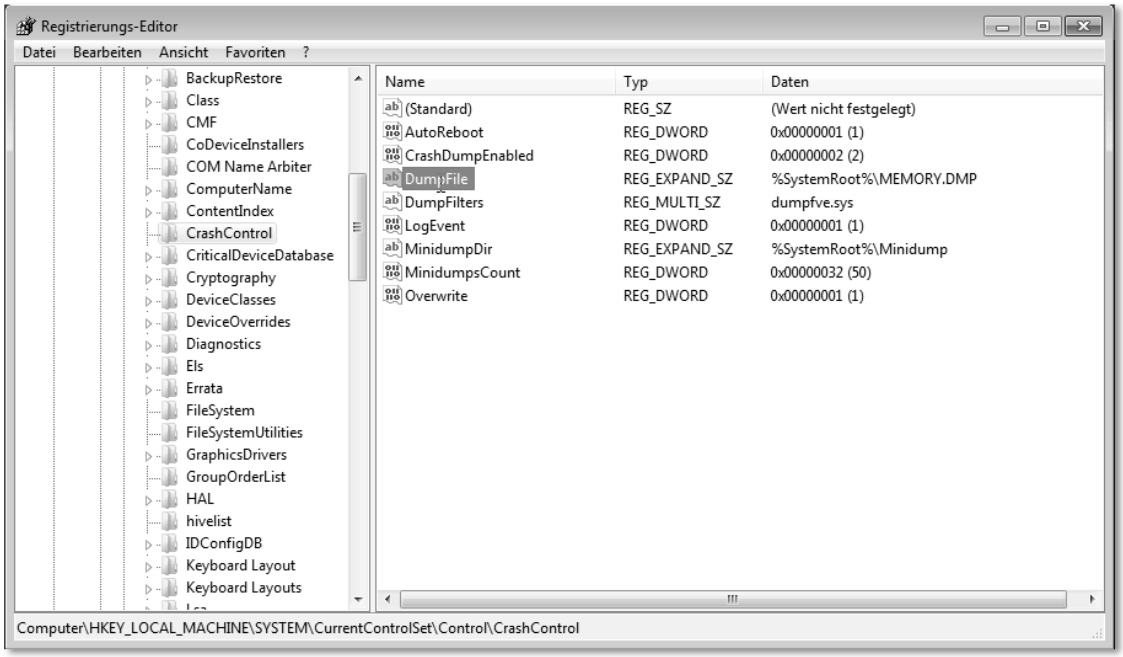


Abbildung 5.13 Das hat sicher jeder schon einmal gesehen: Das »Innenleben« der Registry, angezeigt vom Registrierungs-Editor.

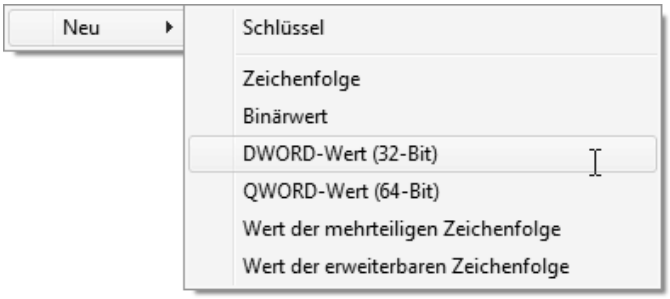


Abbildung 5.14 Beim Hinzufügen neuer Attribute ist es extrem wichtig, den Datentyp korrekt zu wählen.

5.4 Windows-Funktionen

Wenn Sie eine standardmäßige Windows 7-Installation durchführen, ist lediglich ein Teil der Funktionen des Betriebssystems installiert. Auf Abbildung 5.15 sehen Sie die Liste der aktivierbaren Windows-Funktionen. Es gibt dabei durchaus Funktionen, die man einem Client nicht unbedingt zuordnen würde, wie beispielsweise die INTERNETINFORMATIONSDIENSTE – in denen ein sowohl kompletter als auch komplexer Webserver enthalten ist.

Einer der Grundgedanken des modularen Aufbaus ist, dass Komponenten, die nicht benötigt werden und daher nicht installiert sind, auch nicht gewartet werden müssen und kein Sicherheitsproblem darstellen. Vielleicht erinnern Sie sich

noch an die Sicherheitsprobleme bei Windows 2000: Eine wesentliche Ursache war, dass immer schön sämtliche Komponenten installiert worden sind. Diese gerieten dann schnell in Vergessenheit – zumindest bei den Leuten, die sie hätten pflegen und warten sollen. Saboteure und Datendiebe haben sich beispielsweise über jede Menge »offene« und nicht gewartete Webserver gefreut. So etwas darf sich einfach nicht wiederholen, daher sollten Sie sowohl bei Clients als auch bei Servern darauf achten, nicht mehr zu aktivieren als unbedingt notwendig.

Für Administratoren zunächst etwas gewöhnungsbedürftig ist, dass der Telnet-Client standardmäßig nicht aktiviert ist – dieser eignet sich ja recht gut, um die Erreichbarkeit von Serverports zu prüfen. Wie auch immer: Er ist es standardmäßig nicht.

Funktionen aktivieren/deaktivieren

Was ist nun zu tun, wenn Sie in einem Windows 7-Installationsimage bestimmte Funktionen aktivieren und andere deaktivieren möchten? Die Antwort finden Sie in Abschnitt 6.10.4, »Features aktivieren und deaktivieren«. Sie können im Installations-Image beliebig Features aktivieren und deaktivieren – und zwar ohne, dass Sie dieses Image auf einem PC booten müssten!

5.5 Das .NET Framework

Wenn Sie die Liste der Windows-Funktionen auf Abbildung 5.15 durchsehen, wird Ihnen vielleicht das Microsoft .NET Framework 3.5.1 aufgefallen sein. Als IT-Professional werden Sie das .NET Framework mit Sicherheit zumindest dem Namen nach kennen. Bei Workshops gibt es aber immer hinreichend viele Fragen im dem Stil: »Uli, kannst Du bitte nochmal genau erklären, wozu das .NET Framework da ist?« Kein Problem, das werde ich gern tun.

Als der *Windows Server 2003* sich noch im Beta-Stadium befand, hieß das Produkt *.NET-Server*. Erst relativ kurz vor dem Erscheinen wurde der Name in das nun bekannte Windows Server 2003 geändert – bekanntlich ist auch mit dem Betriebssystem Windows Server 2008 und mit Windows 7 der Begriff ».NET« nicht in den Produktnamen eingezogen.

Wenn man oberflächlich schaut, wo denn nun ».NET« drinsteckt, findet man auf den ersten Blick nur das Framework und das etwas »unhandliche« .NET-Konfigurationswerkzeug, dessen Sinn vielen Administratoren nicht so recht klar werden will (Abbildung 5.16).

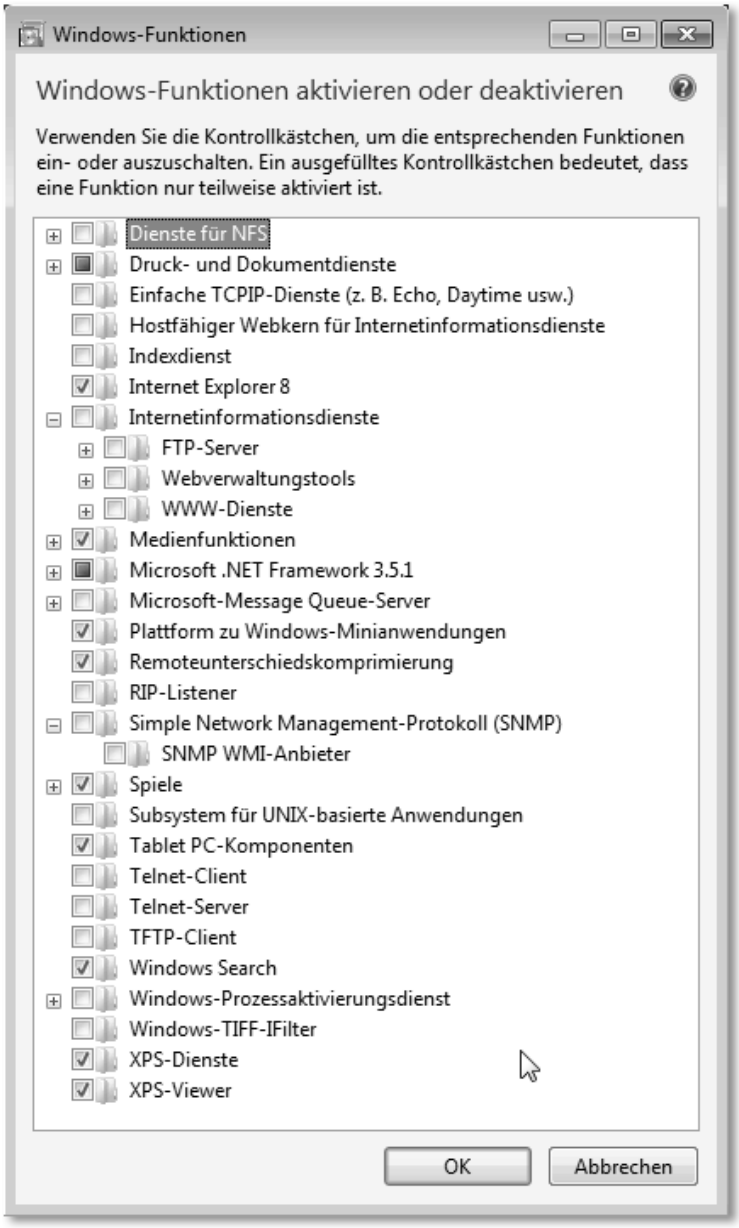


Abbildung 5.15 Die Windows-Funktionen können hier hinzugefügt und entfernt werden.

Grafisches Werkzeug nur bei installiertem SDK

Das grafische Konfigurationswerkzeug ist leider nur vorhanden, wenn das *.NET Framework SDK* auf dem PC bzw. Server installiert ist. Ist das SDK nicht installiert, steht lediglich das Kommandozeilenwerkzeug *CasPol.exe* zur Verfügung, das sich im Pfad *C:\Windows\Microsoft.NET\Framework\v2.0.50727* findet. Anhand des grafischen Werkzeugs lassen sich die Zusammenhänge allerdings einfacher erklären als mit dem Kommandozeilenwerkzeug.

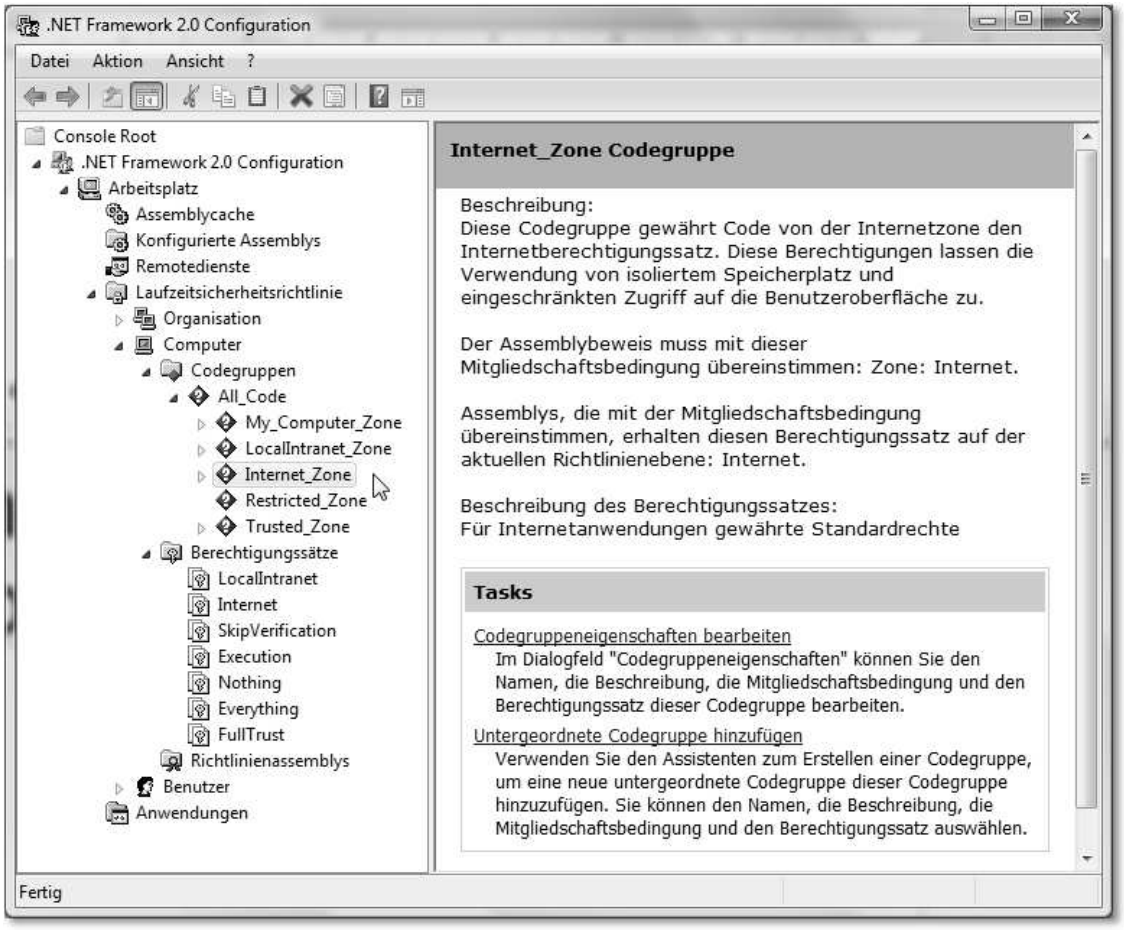


Abbildung 5.16 Das .NET-Framework-Konfigurationswerkzeug (Bestandteil des .NET Framework SDKs)

5.5.1 Der Grundgedanke

Der Grundgedanke hinter .NET ist eigentlich gar nicht kompliziert. Auf Abbildung 5.17 erkennen Sie, worum es in der heutigen IT geht: Es gibt die unterschiedlichsten Clientsysteme und verschiedenste Server bzw. Applikations-Server. Damit die Anwender effizient mit den Systemen arbeiten können, ist Software notwendig, die Funktionen bereitstellt, mit denen die Geschäftsprozesse des Unternehmens oder der Organisation abgebildet werden können. In der Skizze bezeichne ich diese als »Anwendungssysteme«.

Heute reicht es beispielsweise häufig nicht mehr aus, einen Exchange-Server zu installieren, mit dem die Benutzer sich Nachrichten senden können oder gegenseitig auf die Terminkalender zugreifen können. Stattdessen wird das Messaging-System auch in die betrieblichen Abläufe integriert, um es beispielsweise als Transportmedium für den Workflow der CRM-Abläufe zu verwenden.

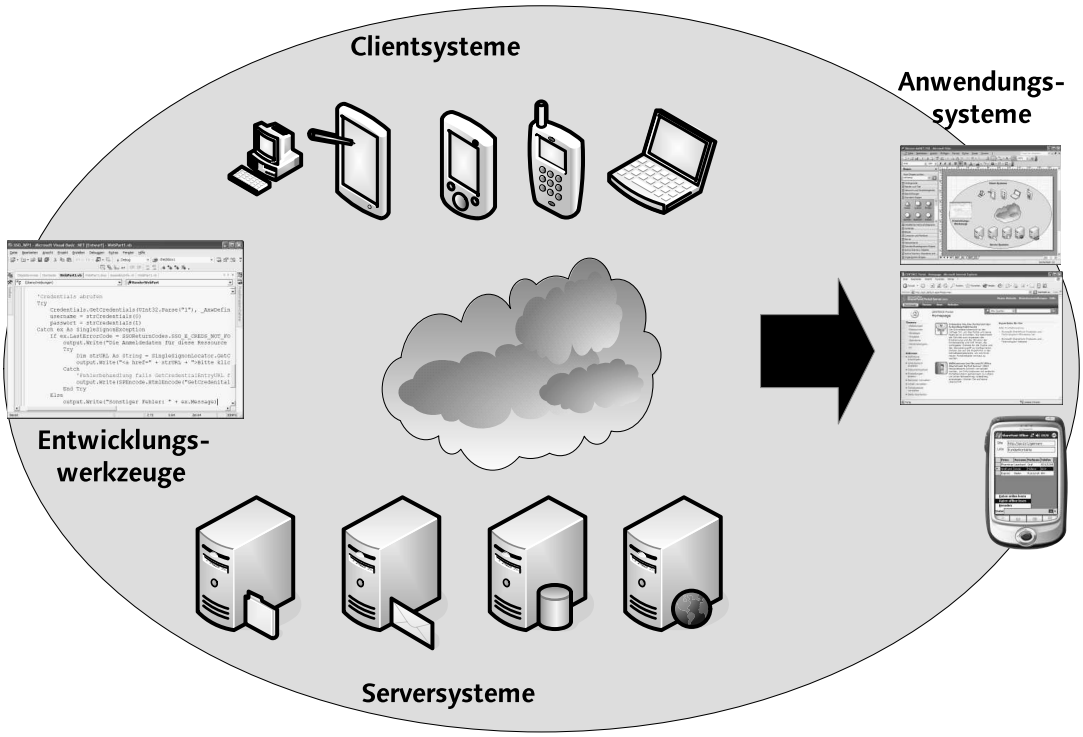


Abbildung 5.17 Ein Blick in die heutige IT-Landschaft

Der Zugriff auf dieses Gesamtsystem soll natürlich nicht nur in der Firma vom lokalen PC aus, sondern an jedem Ort der Welt erfolgen können. Und weil man nicht ständig PC und Notebook mit sich herumschleppen möchte, müssen auch mobile Clients wie PocketPC/PDA oder Handy den Zugriff ermöglichen.

Ein weiteres Beispiel: Eine Firma, die einen großen technischen Außendienst unterhält, wird stark daran interessiert sein, die Techniker enger in die Ablaufsteuerung einzubinden. Ihr Ziel ist es, die Fertigmeldung des Technikers, zeitliche Aufwände und verbrauchtes Material möglichst schnell in die zentralen Systeme zu übermitteln. Der Techniker soll sich nun weder schwerpunktmäßig mit einem Computer (Notebook auspacken, hochfahren, Eingaben vornehmen, herunterfahren, einpacken) beschäftigen, noch möchte man größere Investitionen (wie die Anschaffung von 300 Notebooks) tätigen. Da jeder Techniker ein Handy hat, wäre es natürlich naheliegend, dieses Kommunikationswerkzeug in die Prozesse einzubinden.

Die beiden Beispiele zeigen den Trend:

Es geht letztendlich darum, alle vorhandenen Clients (PCs, Notebooks, PocketPC, Handy/Smartphone) einzubinden und dabei alle Server zu nutzen, die ebenfalls Daten miteinander austauschen.

»Gut«, werden Sie sagen, »man muss also Software entwickeln, die auf allen Clients läuft, die auf alle Applikationsserver zugreifen kann und die in der Lage ist, auch über den Transportweg Internet kommunizieren zu können. Zudem soll die Software einen sicheren Betrieb gewährleisten und performant laufen.«

Jedem wird klar sein, dass diese Anforderungen nicht ganz einfach zu erfüllen sind. Natürlich ist dies alles auch ohne .NET zu realisieren, aber dies ist alles schon nicht mehr ganz trivial: Unterschiedliche Clients, Zugriff auf Applikationsserver, die diversen Protokolle beherrschen – das sind alles recht anspruchsvolle Aufgaben.

Halten Sie sich insbesondere vor Augen, dass wir nicht nur über Software sprechen, die zehntausendmal verkauft wird, sondern dass die Geschäftsprozesse vieler Firmen so individuell sind, dass man zwar nicht komplette Systeme, aber die Bindeglieder zwischen und zu vorhandenen Applikationsservern entwickeln muss.

Kurz gesagt: Sehen Sie .NET als die integrative Komponente, sozusagen als den »Leim« an, mit dem Sie Clients und Applikationsserver »zusammenkleben« können. Ob eine neues Standard-Anwendungssystem entsteht oder ob Sie zur Optimierung Ihrer individuellen Geschäftsprozesse Exchange und SharePoint mit Ihrem SAP-System »verheiraten« möchten, .NET wird Ihnen eine große Hilfe sein. Einen kurzen Überblick, wie dies geschieht, erhalten Sie im nächsten Abschnitt.

5.5.2 .NET bei der Arbeit

Abbildung 5.18 zeigt einen groben schematischen Überblick über unterschiedliche Anwendungsarchitekturen:

- In jedem Fall befindet sich in der Mitte das Betriebssystem nebst darunter liegender Hardware.
- »Klassische« Applikationen, hier als *Unmanaged Applications* bezeichnet, setzen direkt auf dem Betriebssystem auf.
- Die linke Hälfte der Abbildung zeigt *Managed Applications*. Gemanagt werden diese von der *Common Language Runtime* des .NET Frameworks, die in jedem Fall zwischen der Managed Application und dem Betriebssystem liegt. Was nun tatsächlich »gemanagt« wird, erfahren Sie im nächsten Abschnitt.
- Die Managed Applications können die *Klassenbibliothek* des .NET Frameworks verwenden (linker oberer Quadrant). Dies wird in den meisten Fällen auch geschehen, da die Klassenbibliothek für Entwickler eine signifikante Arbeitserleichterung darstellt. Außer auf die Klassenbibliothek können Managed

Applications auf weitere Bibliotheken zugreifen, die bespielsweise API-Funktionen zum Zugriff auf Applikationen wie Exchange oder SharePoint beinhalten.

- Die letzte Variante sind *Managed Web Applications*: Direkt über dem Betriebssystem liegen hier die *Internet Information Services* und darüber die *ASP.NET Runtime*, auf der dann schließlich die Webapplikation ausgeführt wird.

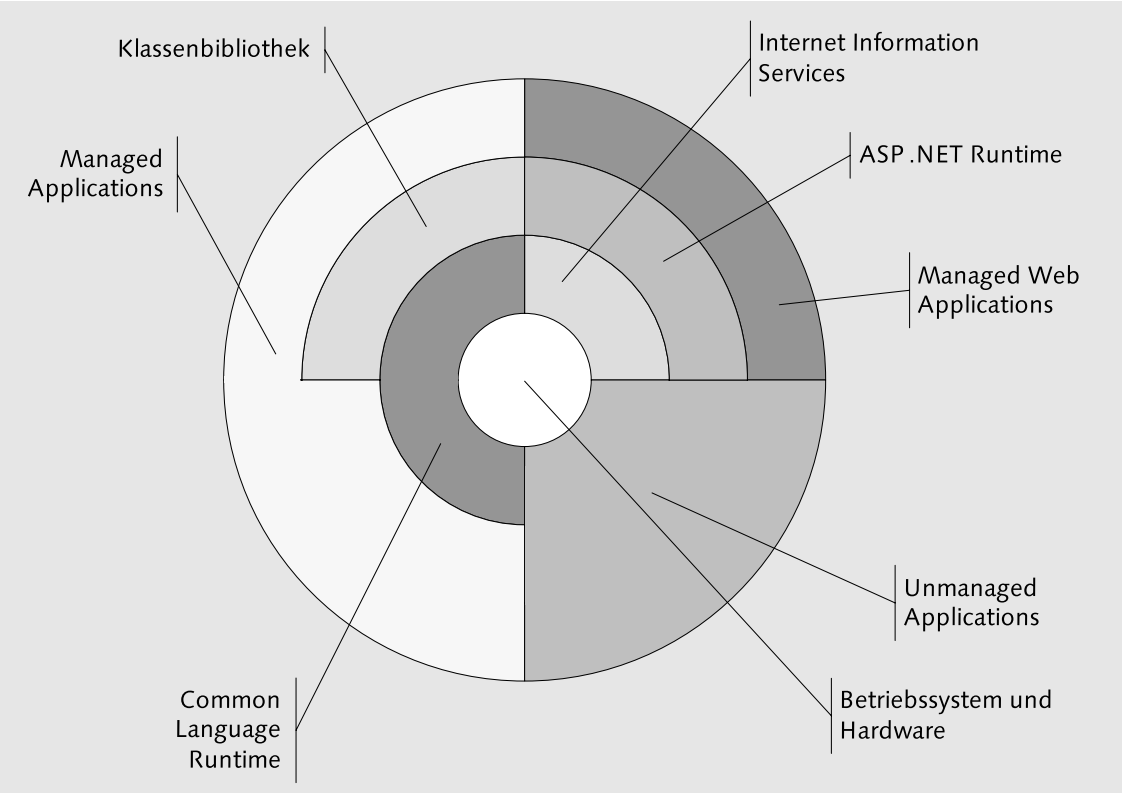


Abbildung 5.18 Die .NET-Anwendungsarchitektur

5.5.3 .NET Framework und .NET Compact Framework

Am Anfang habe ich erläutert, dass .NET eher ein Konzept oder eine Philosophie ist und nicht ein einzelnes fertiges Produkt. Trotzdem gibt es *den* .NET-Download, nämlich das .NET Framework. Dieses benötigen Sie, wenn Sie .NET-Applikationen ausführen möchten. Bei Windows 7 und auch beim Windows Server 2008 R2 ist es standardmäßig in der aktuellsten Version integriert, bei den anderen Betriebssystemen müssen Sie es nachinstallieren. Verfügbar ist das .NET Framework für die folgenden Microsoft-Betriebssysteme (in chronologischer Reihenfolge des Erscheinungsdatums):

- Windows XP
- Windows 2003

- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2

Mono

Interessanterweise gibt es ein Open-Source-Projekt, das sich mit dem »Nachbau« des .NET Frameworks für Linux/Unix beschäftigt. Es heißt *Mono*. Nähere Informationen darüber finden Sie unter *http://www.mono-project.com.*

Inwieweit dieses Projekt in der näheren Zukunft tatsächliche Bedeutung im Alltag der Unternehmens-IT erlangt, kann man sicherlich kontrovers diskutieren. Interessant ist aber in jedem Fall, dass sich etliche hochkompetente und teilweise renommierte Entwickler daranbegeben, einen .NET-Klon zu entwickeln.

Schauen wir uns das .NET Framework kurz an. Auf Abbildung 5.19 ist das übliche Schichtenmodell zu erkennen.

- Die Grundlage ist die Windows-Plattform, momentan Win32.
- In der nächsthöheren Schicht finden sich bekannte Technologien wie COM+, MSMQ (Message Queuing), die Internet Information Services (IIS) und ADO als Technologie für den Datenzugriff.
- Dann geht es richtig los mit .NET in Form der *Common Language Runtime*, der Klassenbibliothek und etlichen weiteren Komponenten.
- Die oberste Schicht bilden die Programmiersprachen, mit denen .NET-Code erzeugt werden kann. Es sind dies mittlerweile nicht nur die von Microsoft in Visual Studio bereitgestellten Programmiersprachen VB.net, C#, J# und C++, mittlerweile unterstützen auch andere Hersteller wie beispielsweise Borland mit dem Delphi-Produkt die .NET-Entwicklung.

Die Ausführung von .NET-Code unterscheidet sich grundlegend von der Ausführung »normaler« Programme. Bei Letzteren erzeugt der Compiler nativen Code, der direkt ausgeführt werden kann. In einer .NET-Umgebung verhält es sich anders, wie Sie in dem Flussdiagramm aus Abbildung 5.20 erkennen können:

- Der Compiler erzeugt zwar eine EXE- oder DLL-Datei, allerdings besteht diese aus einer Art Zwischencode, der *Intermediate Language* (IL). Diese Dateien sind ohne das .NET Framework nicht ausführbar, obwohl sie die Extension EXE haben. Sie können das einfach verifizieren, in dem Sie eine .NET-EXE auf eine Maschine ohne installiertes Framework kopieren und versuchen, diese Datei zu starten – es wird eine Meldung erscheinen, dass ein .NET Framework erforderlich ist.

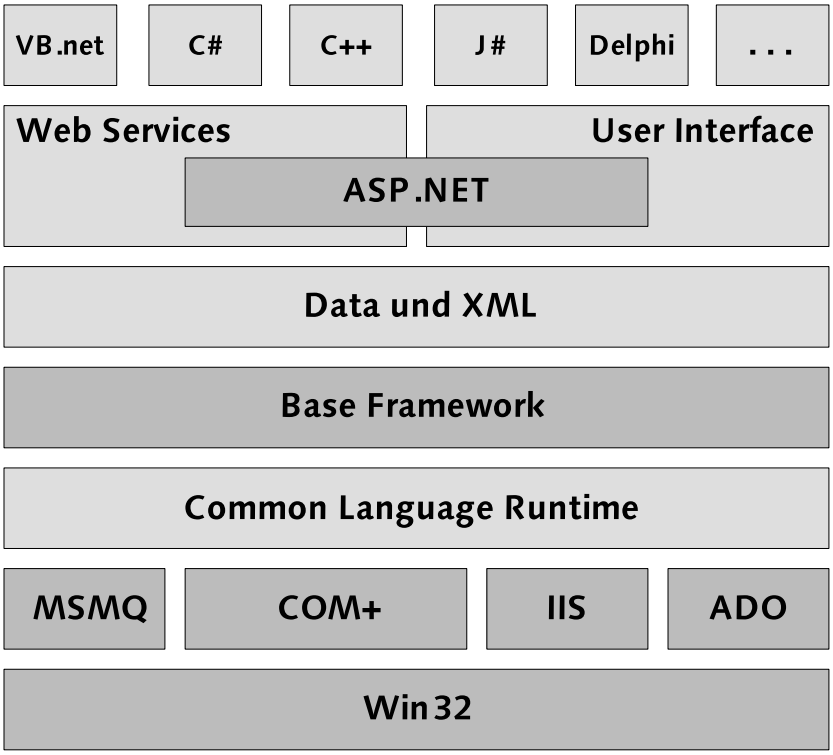


Abbildung 5.19 Das .NET Framework im Schichtenmodell

- Startet man eine .NET-EXE, wird die *Common Language Runtime* aktiv. Zunächst ermittelt der *Class Loader*, welche Assemblys zur Ausführung zusätzlich benötigt werden. Diese finden sich zumeist in DLL-Dateien.
- Als Nächstes erstellt der JIT-Compiler aus der Intermediate Language »echten« ausführbaren Code. Der JIT-Compiler benötigt für diese Kompilierung nur wenige Augenblicke; dieser Vorgang ist vom Zeitbedarf nicht vergleichbar mit der Kompilierung in Visual Studio. Das Kompilieren zur Laufzeit bietet übrigens den Vorteil, dass eine auf die Maschine optimierte Übersetzung erfolgen kann. Herkömmlicher Code ist für den kleinsten gemeinsamen Nenner (letztendlich also für den ältesten noch unterstützten x86-Prozessor) übersetzt. Bei Messungen hat sich herausgestellt, dass geJITteter Code in der Tat häufig schneller ist, obwohl am Anfang der Kompilierungsvorgang durchgeführt werden muss.
- Während der Ausführung des Codes achtet die Laufzeitumgebung darauf, dass die Sicherheitsrichtlinien eineghalten werden, die in der *Code Access Security* definiert sind (hierzu mehr im nächsten Abschnitt).

Neben dem .NET Framework existiert mit dem *.NET Compact Framework* eine spezielle Variante des .NET Frameworks für mobile Geräte mit WinCE-basierten Betriebssystemen, unter anderem solche mit dem *Windows Mobile*-Betriebssystem. Für noch kleinere Geräte ist das *.NET Micro Framework* gedacht.

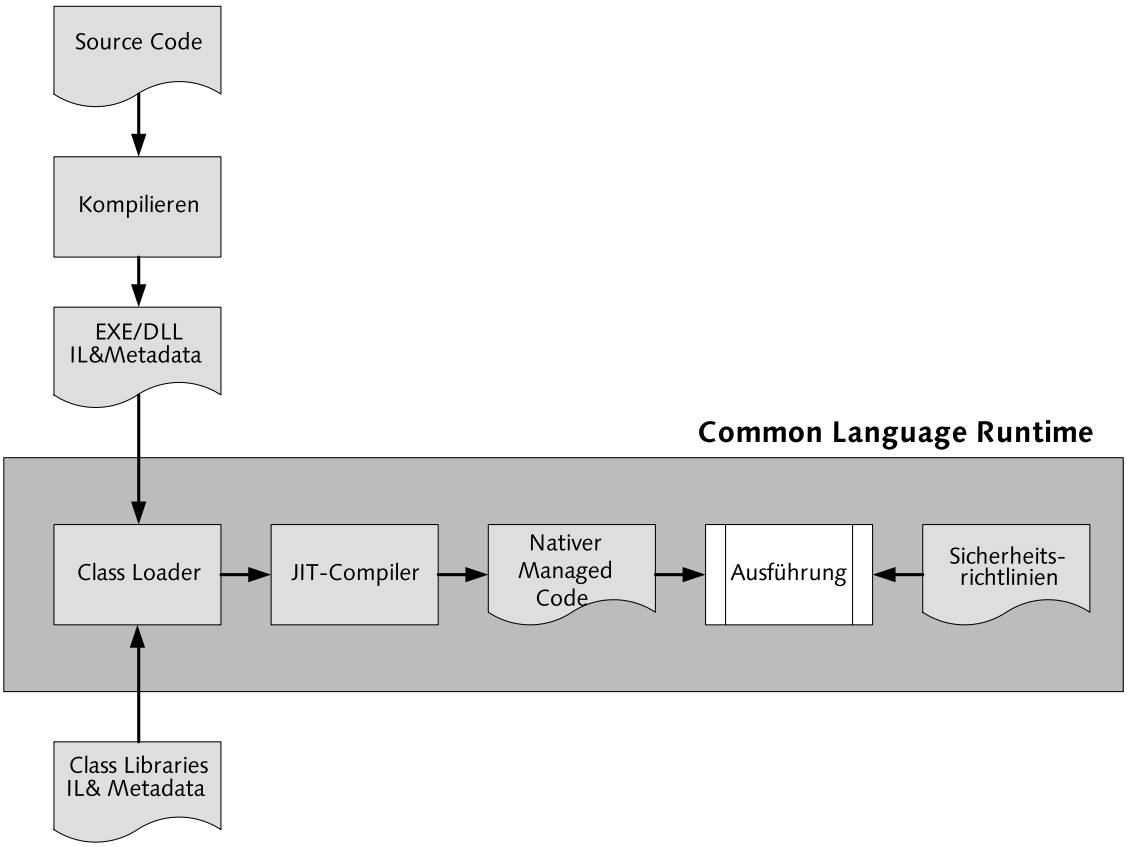


Abbildung 5.20 Die Ausführung von .NET-Code

Die Klassenbibliothek des *.NET Compact Frameworks* ist eine Untermenge derjenigen des »großen« Frameworks, enthält allerdings deutlich weniger Funktionen. Das hängt zum einen damit zusammen, dass ein installiertes .NET Framework mit deutschem Sprachpaket deutlich über 100 MB Speicher beansprucht, was für viele mobile Geräte deutlich zu viel ist. Darüber hinaus sind etliche Funktionen zu ressourcenintensiv, als das man diese sinnvoll auf einem Mobilgerät einsetzen könnte.

Dem .NET Compact Framework (.NET CF) fehlen einige grundlegende Eigenschaften des großen .NET Frameworks. .NET CF verfügt beispielsweise *nicht* über Code Access Security.

Das .NET Compact Framework ist ein innovativer, wichtiger Schritt in die richtige Richtung, denn damit kann ein Entwickler, der Erfahrungen im .NET-Umfeld gesammelt hat, mit relativ geringem Einarbeitungsaufwand anspruchsvolle Applikationen für Mobilgeräte entwickeln. Die Klassenbibliothek, die von .NET CF zur Verfügung gestellt wird, dürfte im Umfeld der Entwicklung für Mobilgeräte in dieser Funktionsvielfalt einzigartig sein.

5.5.4 Code Access Security

Ein wichtiges Merkmal des .NET Frameworks (aber *nicht* des .NET Compact Frameworks) ist die *Code Access Security*.

Normalerweise kann eine Applikation auf alle Ressourcen zugreifen, auf die der Benutzer, der die Applikation startet, Zugriff hat. Der Schwachpunkt liegt auf der Hand: Häufig starten Benutzer recht unbedacht eine Applikation, die beispielsweise per E-Mail auf die Maschine gekommen ist, haben aber überhaupt keine Kontrolle darüber, was diese Applikation anschließend tut: Vielleicht installiert sie eine Backdoor, durchsucht das Filesystem, greift auf das Internet zu oder klaut E-Mail-Adressen.

Mit anderen Worten sind einer Applikation, die gestartet ist, nur noch Riegel in Form der Benutzerberechtigungen vorgeschoben. Das bedeutet, dass die gestartete Applikation, je nach Benutzerumgebung, relativ frei »schalten und walten« kann.

Das Prinzip der Code-Access-Security-Richtlinien (*CASpol*) bringt hier sehr deutliche Verbesserungen – allerdings nur für *Managed Applications*!

Für jede einzelne Assembly (das kann eine .EXE- oder .DLL-Datei sein) kann individuell definiert werden, auf welche Ressourcen sie zugreifen kann.

Abbildung 5.21 zeigt die Konfiguration eines Berechtigungssatzes: Eine Assembly darf den SQL-Client verwenden und im Verzeichnis *c:\temp* lesend und schreibend auf Dateien zugreifen. Sonst nichts! Kein Zugriff auf andere Netzwerkressourcen, keine Manipulation der Registrierung etc.

Im Klartext bedeutet das, dass *Sie* festlegen, was eine ausführbare Datei darf, und dass sich die ausführbare Datei eben nicht das holen kann, was sie gern hätte.

Obwohl diese Vorgehensweise eindeutig in die richtige Richtung weist, muss man die Euphorie zunächst bremsen: Die Code Access Security funktioniert ausschließlich mit *Managed Code*, der von der Laufzeitumgebung des .NET Frameworks ausgeführt wird.

Solange Sie nicht *Unmanaged Code* auf den Systemen komplett ausschließen können, gibt es durch das Verfahren natürlich keine verbesserte Gesamtsicherheit. Um bösartigen Unmanaged Code auszuschließen, können Sie beispielsweise auf die *Richtlinien für Softwareeinschränkungen* (Gruppenrichtlinien) oder noch besser auf die Nachfolgetechnologie *AppLocker* (siehe Abschnitt 12.5) zurückgreifen.

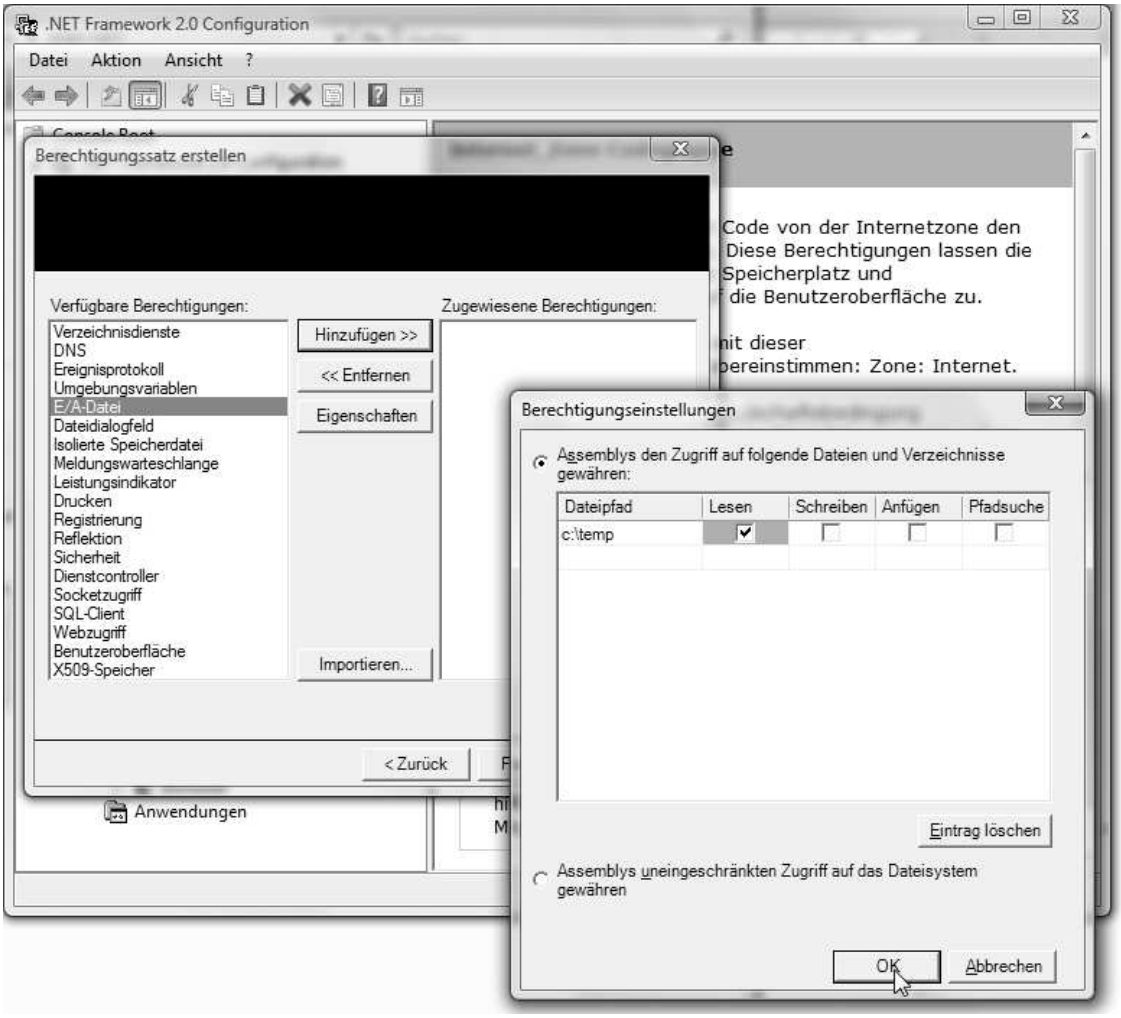


Abbildung 5.21 Erstellen eines Berechtigungssatzes mit dem Konfigurationswerkzeug des .NET Frameworks

Code Access Security kann natürlich nur funktionieren, wenn Sie das Konzept nicht aushebeln und alle Assemblys mit *Full Trust*, also ohne Einschränkungen, laufen lassen.

Damit Sie einen »visuellen Eindruck« bekommen, wie es aussieht, wenn die Code Access Security den Ressourcenzugriff verhindert, habe ich ein kleines Programm geschrieben, das versucht, auf einen SQL-Server zuzugreifen. Da die Assembly (d. h. die EXE-Datei) keine Berechtigung dazu hat, wird der Zugriff verhindert (Abbildung 5.22).

5.5.5 Von Codegruppen und Berechtigungssätzen

Bei der Arbeit mit der Code Access Security haben Sie in erster Linie mit Codegruppen und Berechtigungssätzen zu tun.

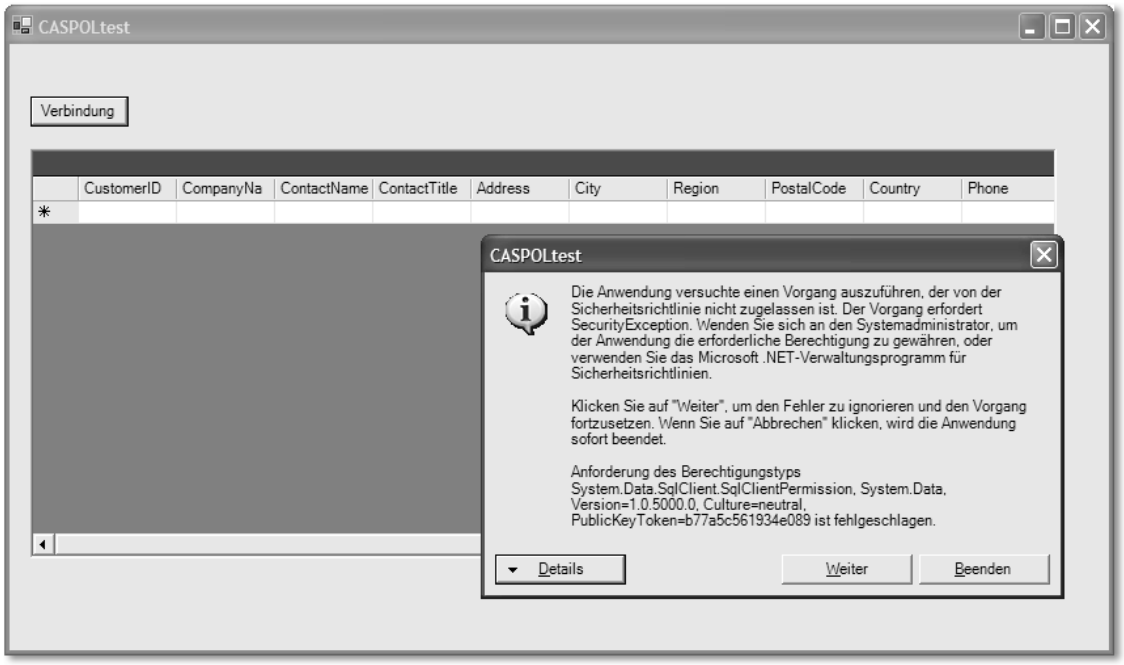


Abbildung 5.22 Ein Programm versucht auf den SQL-Server zuzugreifen. Die Code Access Security verhindert den Zugriff.

Berechtigungssatz

Das Erstellen eines Berechtigungssatzes haben Sie bereits auf Abbildung 5.21 gesehen. In einem Berechtigungssatz wird festgehalten, welche Rechte eine Assembly hat, also auf welche Ressourcen sie zugreifen kann.

Codegruppe

Nun müssen Sie dem System noch mitteilen, auf welche Applikationen der zuvor erstellte Berechtigungssatz angewendet werden soll. Hierzu werden Codegruppen verwendet. Die Assembly kann beispielsweise anhand des Hashwerts, des Publishers, des starken Namens, der Herkunfts-URL und einiger anderer mehr identifiziert werden (Abbildung 5.23).

Zum Schluss wird der Codegruppe ein zuvor ersteller Berechtigungssatz zugewiesen. Ab sofort gelten die neuen Einstellungen für die entsprechende Assembly (Abbildung 5.24).

Die vorangegangenen Screenshots stammten aus der .NET-Framework-Konfigurationsapplikation. Die Konfigurationsdateien werden als XML-Dateien gespeichert und können demzufolge auch einfach mit einem Texteditor bearbeitet werden – von fortgeschrittenen Benutzern.

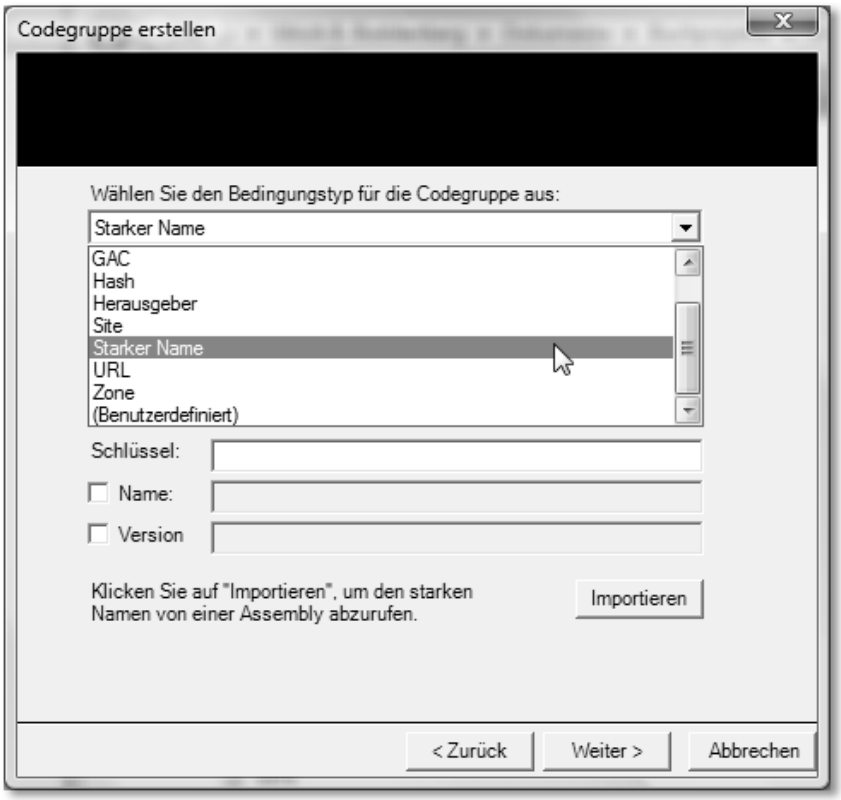


Abbildung 5.23 Ein Bedingungstyp für die Codegruppe wird ausgewählt. Dies dient zur Identifikation einer Assembly bzw. von deren Herkunft.

Abbildung 5.24 Den Assemblys dieser Codegruppe wird ein Berechtigungssatz zugewiesen.

Nicht in allen Fällen können Sie sich vom grafischen Werkzeug helfen lassen: Beispielsweise werden Sie bei der Konfiguration der Code Access Security in SharePoint in jedem Fall XML-Dateien bearbeiten müssen, da standardmäßig kein entsprechendes grafisches Konfigurationswerkzeug vorhanden ist.

5.6 WPF, WCF, WWF und CardSpace

Seit dem .NET Framework 3.0 gibt es vier weitere Komponenten, die sich hinter den kryptischen Abkürzungen der Überschrift verbergen:

- *WPF*: Die *Windows Presentation Foundation* stellt neuartige Fähigkeiten für die Bildschirmausgabe bereit. Das GDI, das *Graphics Device Interface*, das im Grunde genommen schon seit Windows 1 mit an Bord ist, ist mit seinen Fähigkeiten mittlerweile an diverse Grenzen gestoßen. Die Möglichkeiten der WPF kommen aber nur zum Tragen, wenn sie von Programmen tatsächlich auch genutzt werden. In der Betaphase war diese Technologie unter dem Codenamen *Avalon* bekannt.
- *WCF*: Die *Windows Communication Foundation* stellt für Applikationen diverse Methoden für die dienstorientierte Kommunikation zur Verfügung. Diese sind wichtig, um die Anforderungen moderner verteilter Anwendungen abzudecken. Unter einer einheitlichen API finden sich somit Kommunikationstechnologien wie Webservices, DCOM oder Enterprise Services. In der Betaphase war diese Technologie unter dem Codenamen *Indigo* bekannt.
- *WWF*: Die *Windows Workflow Foundation* ermöglicht Applikationen, Workflows zu initiieren und abarbeiten zu lassen. Die WWF ist nicht im klassischen Sinn ein »Workflow Server«, denn sie bietet selbst beispielsweise keine Interaktionsmöglichkeiten mit Benutzern und muss stets von einer Applikation gehostet werden. Die WWF wird beispielsweise von SharePoint für die Bereitstellung von Workflows verwendet: In diesem Fall hostet SharePoint also die WWF und bringt diverse Workflow-Aktivitäten (z. B. Eingabe entgegennehmen, Wert eines Felds ändern, Workflow-Aufgabe erzeugen) mit, die dann die Workflows mit Leben füllen.
- CardSpace: Bei CardSpace handelt es sich um eine Technologie, mit der Anwender ihre digitalen Identitäten verwalten können. Es handelt sich hierbei aber nicht um einen simplen »Identitäts-Tresor«, sondern CardSpace interagiert mit dafür vorbereiteten Applikationen.

Diese vier Technologien sind für Administratoren nicht so sehr spannend, weil es so direkt keine zu erledigenden Aufgaben gibt. Insbesondere die drei Technolo-

gien mit »Foundation« im Namen erleichtern es aber Entwicklern kolossal, leistungsfähige moderne Anwendungen zu erstellen.

Wenn eine Applikation eine der Foundations benötigt, müssen Sie lediglich die Windows-Funktion .NET Framework 3.5.1 aktivieren; es ist durchaus möglich, dass noch weitere Komponenten installiert werden müssen. Das gilt insbesondere für die WCF-Aktivierung (Abbildung 5.25).

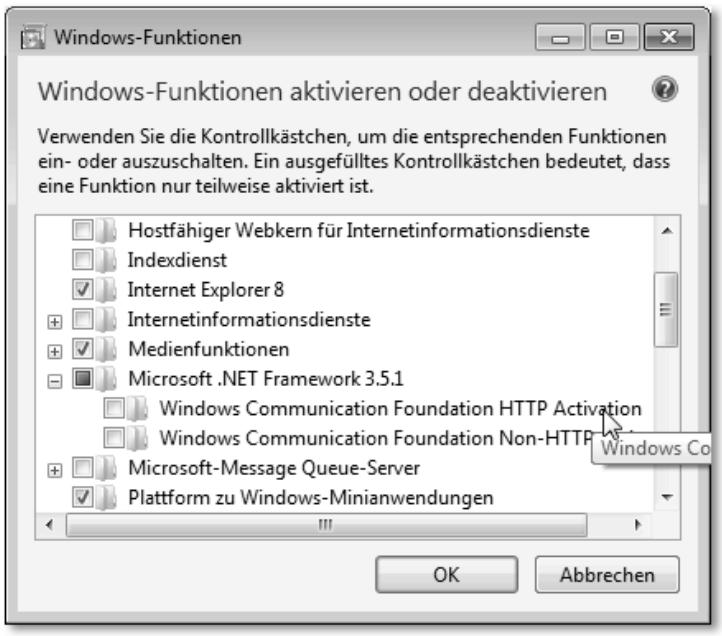


Abbildung 5.25 Aktivieren des .NET Frameworks

5.7 Geräte

Den Dialog aus Abbildung 5.26 dürfte jeder Administrator kennen: Er zeigt den Geräte-Manager. Bei der Neuinstallation eines PCs sollte die Kontrolle des Geräte-Managers zum dringendsten Pflichtprogramm gehören – sollte für das eine oder andere Gerät kein Treiber vorhanden sein oder aber der Treiber nicht funktionieren, wird ein gelbes Fragezeichen bei dem Gerät angezeigt werden.

Wenn Sie das Deployment vorbereiten, wird der Geräte-Manager eine wertvolle Hilfe sein – um Treiber auszuprobieren, nachzuinstallieren etc.

Neben den Hardwaregeräten gibt es diverse Einträge, die sich auf Systemgeräte beziehen. Diese können Sie anzeigen, wenn Sie den Menüpunkt Ansicht • Ausgeblendete Geräte wählen. Im Allgemeinen gibt es mit diesen Komponenten keine Probleme (Abbildung 5.27).

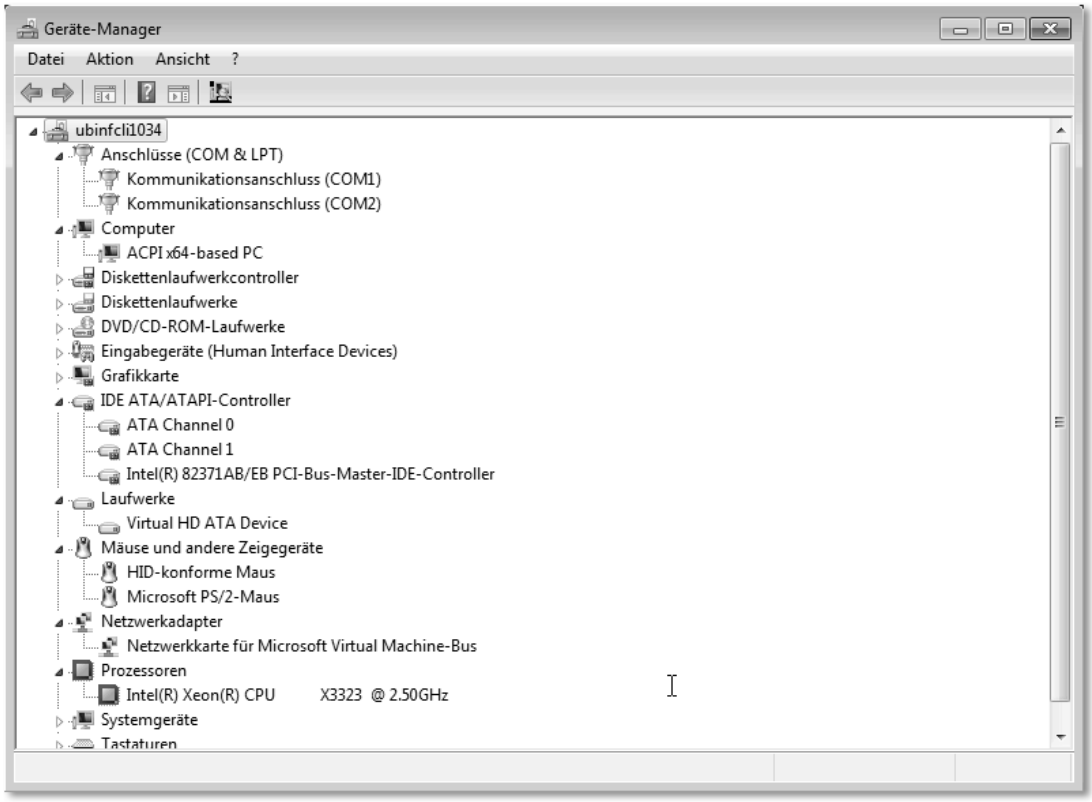


Abbildung 5.26 Der Geräte-Manager zeigt die installierten Geräte an.

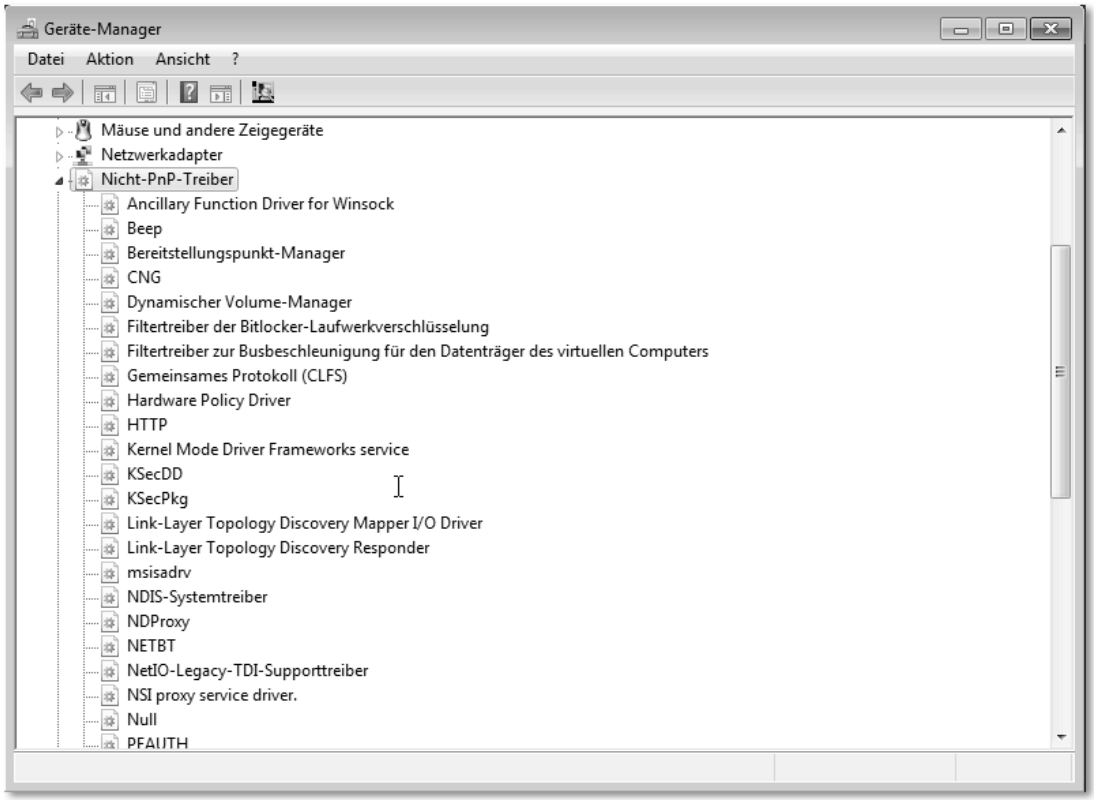


Abbildung 5.27 Hier werden ausgeblendete Geräte angezeigt.

Häufig installieren Dritthersteller zusätzliche Geräte, die dann ebenfalls in der Rubrik NICHT-PNP-TREIBER auftauchen, beispielsweise Virenscanner. Falls diese Komponenten Probleme bereiten, können Sie diese über den Geräte-Manager kontrollieren, deinstallieren und anpassen.

5.8 Die Active Directory-Zertifikatdienste

Diverse Windows 7-Funktionen benötigen Zertifikate. Erfahrungsgemäß gibt es in den meisten Umgebungen keine eigene PKI (Public Key Infrastructure). Ohne eine solche werden Sie aber beispielsweise DirectAccess nicht umsetzen können.

Aus diesem Grunde erhalten Sie anbei eine »Schnelleinführung« in das Thema Active Directory-Zertifikatdienste.

Die zu Zeiten von Windows Server 2003 *Zertifikatsdienste* genannte Funktionalität ist jetzt in die Active Directory-Familie aufgenommen worden und heißt *Active Directory-Zertifkatdienste*, in englischen Versionen *Active Directory Certificate Server* (AD CS).

Diese namensmäßige Anpassung erscheint mir durchaus sinnvoll zu sein, da nun alles, was im weitesten Sinne mit Authentifizierung zu tun hat, beim Active Directory angesiedelt ist.

AD CS

Aus Gründen der besseren Lesbarkeit verwende ich im weiteren Verlauf häufig die englische Abkürzung AD CS, anstatt jedes Mal lang und breit »Active Directory-Zertifikatdienste« zu schreiben.

5.8.1 Einige Anwendungsszenarien

Wenn Sie sich nicht ganz sicher sind, ob Sie in Ihrem Unternehmen bzw. in Ihrer Organisation ein Zertifikatswesen einführen sollen, möchte ich Ihnen zunächst einige Anwendungsszenarien nennen. Sie werden höchstwahrscheinlich feststellen, dass Sie um AD CS nicht herumkommen werden, zumindest mittelfristig.

Internet-Authentifizierung und Verschlüsselung

Der bekannteste Anwendungsfall ist die Authentifizierung eines Servers im Internet. Wenn ein Benutzer einen Server im Internet anwählt, d. h., den Namen im Browser angibt, möchte er sicher sein, dass der erreichte Server auch tatsächlich der ist, als der er sich ausgibt. Etwas »praktischer« formuliert: Wenn der Benutzer *www.dasIstMeineBank.de* anwählt, möchte er sicher sein, dass nicht irgendein

»Hacker« (bzw. Phisher) den DNS-Eintrag gekapert und auf seinen Server umgeleitet hat und sich nun eine gefälschte Website der Kombination aus Kontonummer, PIN und TAN bemächtigt.

Greift ein Benutzer auf *https://www.dasIstMeineBank.de* zu und stimmt irgendetwas nicht mit dem Zertifikat, gibt es eine entsprechende Warnung im Browser. Eine Warnung kann es aus drei Gründen geben:

- Das Zertifikat ist zeitlich nicht gültig.
- Das Zertifikat passt nicht zum angewählten Namen. Wenn der Benutzer *https://www.dasIstMeineBank.de* angewählt hat, das Zertifikat aber für *https://www.nichtMeineBank.com* ausgestellt ist, gibt es eine Warnung.
- Das Zertifikat ist von einer Zertifizierungsstelle ausgestellt worden, der nicht vertraut wird – bzw. technischer gesprochen: deren Stammzertifikat nicht im Zertifikatsspeicher des PCs vorhanden ist.

Wenn ein Benutzer über einen sicheren Kanal (https://) eine Verbindung zu einer Website aufbaut, deren Zertifikat nicht in Ordnung ist, wird er vom Internet Explorer gewarnt. Abbildung 5.28 zeigt die Warnung des Internet Explorer 8. Auch die Vorgängerversionen haben bei Zertifikatsfehlern gewarnt, wenn auch nicht so deutlich. Solche Meldungen machen natürlich nur Sinn, wenn die Anwender daraus auch die richtigen Schlüsse ziehen und sie nicht einfach nur wegklicken.

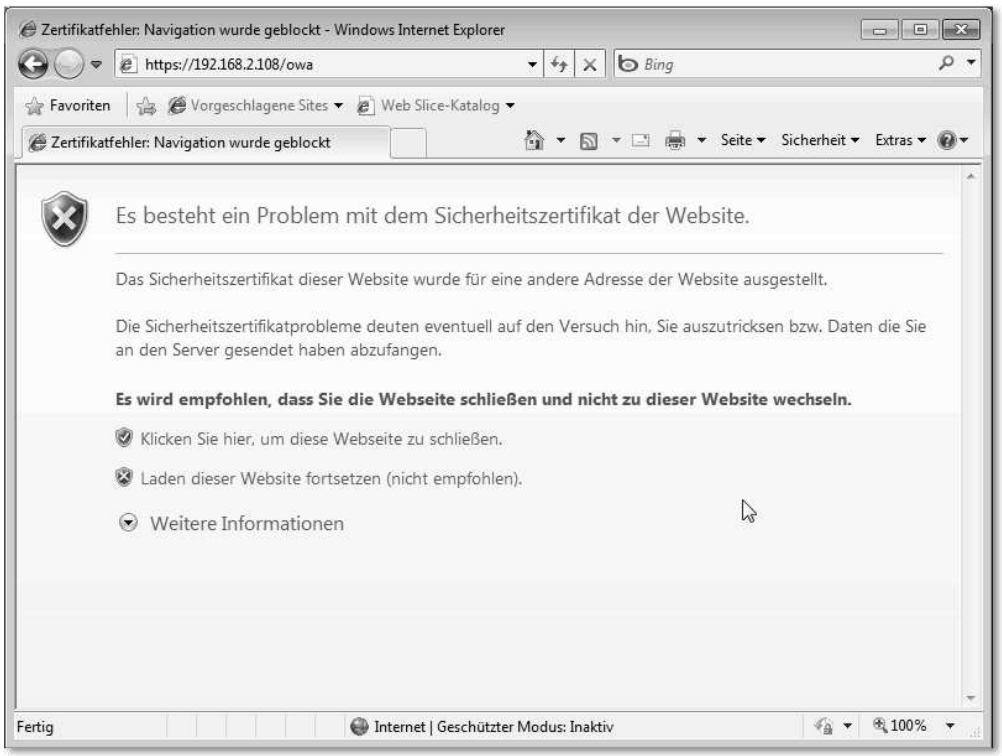


Abbildung 5.28 Internet Explorer warnt, wenn das Zertifikat einer Website nicht in Ordnung ist. Die Benutzer müssen lernen, dass eine solche Meldung ernst genommen werden muss.

Beim Zugriff auf Webserver dienen die Zertifikate weiterhin zur Verschlüsselung des Datenstroms. Abbildung 5.29 zeigt, wie HTTP mit SSL-Verschlüsselung funktioniert:

- Zunächst baut der Client eine Verbindung zum Webserver auf. Da er eine sichere Verbindung aufbauen möchte, greift er auf den Port für HTTP über SSL zu. Dies ist im Allgemeinen Port 443.
- Der Server »antwortet« mit einer Kopie seines öffentlichen Zertifikatsschlüssels.
- Im nächsten Schritt überprüft der Client, ob dieser Zertifikatsschlüssel von einem Herausgeber (d. h. einer Stammzertifizierungsstelle) stammt, dem er vertraut. Diese Prüfung endet nur dann positiv, wenn das Zertifikat der Stammzertifizierungsstelle im Zertifikatsspeicher für »vertauenswürdige Stammzertifizierungsstellen« des Clients hinterlegt ist.

  Die Logik dahinter ist also wie folgt: »Ich vertraue der Stammzertifizierungsstelle, also traue ich auch allen Zertifikaten, die diese nachweisbar herausgegeben hat.« Der Nachweis, dass ein Zertifikat wirklich von einer Stammzertifizierungsstelle kommt, funktioniert über kryptografische Methoden.
- Nun handeln Client und Server einen Sitzungsschlüssel aus. Da der Client über den öffentlichen Schlüssel des Servers verfügt, kann er den Sitzungsschlüssel so verschlüsseln, dass dieser nur vom Server mit dessen privatem Schlüssel decodiert werden kann.
- Mit dem (übrigens symmetrischen) Sitzungsschlüssel können nun die Daten verschlüsselt werden, die ausgetauscht werden sollen.

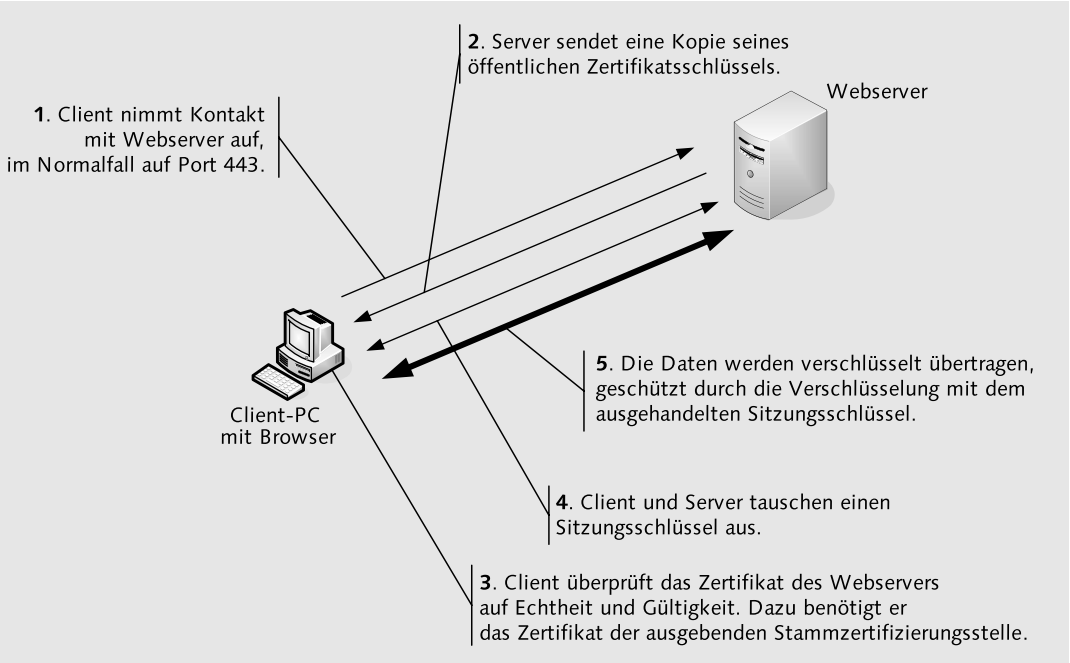


Abbildung 5.29 Die Funktionsweise von HTTP über SSL (HTTPS)

Sichere E-Mail

Es ist kein Geheimnis mehr, dass Mails unverschlüsselt durch das Internet reisen, was insbesondere diese beiden Probleme nach sich zieht: Jemand, der sich an irgendeiner Stelle des Transportwegs Zugriff auf die Mails verschaffen kann, ist in der Lage,

- die Mails zu lesen und/oder
- die Mails zu manipulieren.

Das »Sich-Zugriff-Verschaffen« ist zwar nicht ganz trivial, wo ein Interesse ist, ist aber auch ein Weg. Abhilfe schafft das Signieren und Verschlüsseln von E-Mails. Das Signieren schützt eine Nachricht vor Manipulation, und das Verschlüsseln verhindert einen unautorisierten Zugriff.

Wenn zwei Personen geheime Mails austauschen möchten, könnten sie einen Geheimcode vereinbaren, mit dem die Inhalte codiert werden. Beide Personen kennen den Schlüssel, und dieser wird sowohl zum Verschlüsseln als auch zum Entschlüsseln verwendet. So weit ist alles gut.

Das Verfahren wird dann ausgesprochen »unhandlich«, wenn potenziell jeder Mitarbeiter einer Firma mit jedem anderen kommunizieren möchte. Jeder müsste einen geheimen Schlüssel mit jedem anderen Mitarbeiter vereinbaren, um Nachrichten auszutauschen. Bei 1 000 Mitarbeitern ergibt das die bescheidene Anzahl von $1\,000^2$ = 1 000 000 Schlüsseln. Wenn in Zukunft alle 8 000 000 000 Einwohner der Welt miteinander in E-Mail-Kontakt treten können, müssten in der Endausbaustufe insgesamt 64 000 000 000 000 000 000 Schlüssel vorhanden sein. Die symmetrische Verschlüsselung (beim Verschlüsseln und Entschlüsseln wird derselbe Schlüssel verwendet) führt also in eine Sackgasse. Aus diesem Grund wird für die E-Mail-Verschlüsselung und -Signatur ein asymmetrisches Verfahren verwendet, das – Sie ahnen es bereits – auf Zertifikaten basiert.

Nachfolgend stelle ich das Verschlüsseln und das Signieren von E-Mails kurz vor. Wenn Sie die Abläufe verstanden haben, hilft Ihnen das, auch alle anderen asymmetrischen Vorgänge zu begreifen.

Verschlüsseln

Für die Verschlüsselung von Mails wird ein PKI-basiertes Verfahren verwendet. PKI ist die Abkürzung für *Public Key Infrastructure*, d. h., es wird ein Verfahren verwendet, bei dem jeder Benutzer über ein Schlüsselpaar verfügt, das aus einem privaten und einem öffentlichen Schlüssel besteht. In einer Exchange-Umgebung werden die Schlüssel im Active Directory gespeichert.

Das Verfahren ist stark vereinfacht in Abbildung 5.30 dargestellt:

- Der Sender fordert den öffentlichen Schlüssel des Empfängers an. Diesen erhält er beispielsweise aus dem Active Directory. Im Active Directory wird der Schlüssel übrigens in den globalen Katalog repliziert, sodass auch in sehr großen Organisationen ein schneller Zugriff gewährleistet ist.
- Der Sender verschlüsselt die Mail mit dem öffentlichen Schlüssel des Empfängers.
- Die verschlüsselte Mail wird übertragen.
- Der Empfänger kann mit seinem privaten Schlüssel die mit dem zugehörigen öffentlichen Schlüssel verschlüsselte Mail entschlüsseln.

Abbildung 5.30 Asymmetrische Verschlüsselung von E-Mails

Abgewandeltes Verfahren

Leider ist die asymmetrische Verschlüsselung kein besonders performantes Verfahren. Aus diesem Grund wird das oben beschriebene Verfahren in der Praxis leicht abgewandelt: Der Sender erzeugt einen Schlüssel für eine symmetrische Verschlüsselung, mit dem dann der Mailinhalt und gegebenenfalls Anhänge codiert werden. Dieser symmetrische Schlüssel wird mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt und ebenfalls in der Mail mitgesendet. Der Empfänger decodiert nun zunächst den vom Sender erzeugten symmetrischen Schlüssel mit seinem privaten Schlüssel. Daraufhin entschlüsselt er mit dem symmetrischen Schlüssel den Mailinhalt und die Anhänge. (Eigentlich ist es ganz einfach, man muss es aber vermutlich zweimal lesen.)

Signieren

Das im vorherigen Abschnitt besprochene Verfahren bezog sich auf die Verschlüsselung der auszutauschenden Informationen. In vielen Fällen ist es ebenfalls wichtig, dass die Echtheit einer Mail überprüft werden kann. Auch diese Aufgabenstellung kann mit einer Public Key Infrastructure realisiert werden.

Die Vorgehensweise ist in Abbildung 5.31 (Seite 114) vereinfacht dargestellt:

- Der Sender ermittelt einen Hash-Wert über die Mailinhalte nebst eventuellen Anlagen. Das resultierende »Datenpaket« wird übrigens als *Digest* bezeichnet. Dieser Digest wird mit der Mail übermittelt.
- Wenn der Empfänger die Echtheit der E-Mail überprüfen will, um sicherzustellen, dass diese nicht unautorisiert verändert worden ist, fordert er den öffentlichen Schlüssel des Senders an. Diesen erhält er beispielsweise aus dem Active Directory.
- Mit dem öffentlichen Schlüssel kann er testen, ob der übermittelte Digest zu dem Mailinhalt (gegebenenfalls nebst Anlagen) passt. Passt der Inhalt nicht, ist entweder an der Mail oder am Digest manipuliert worden.

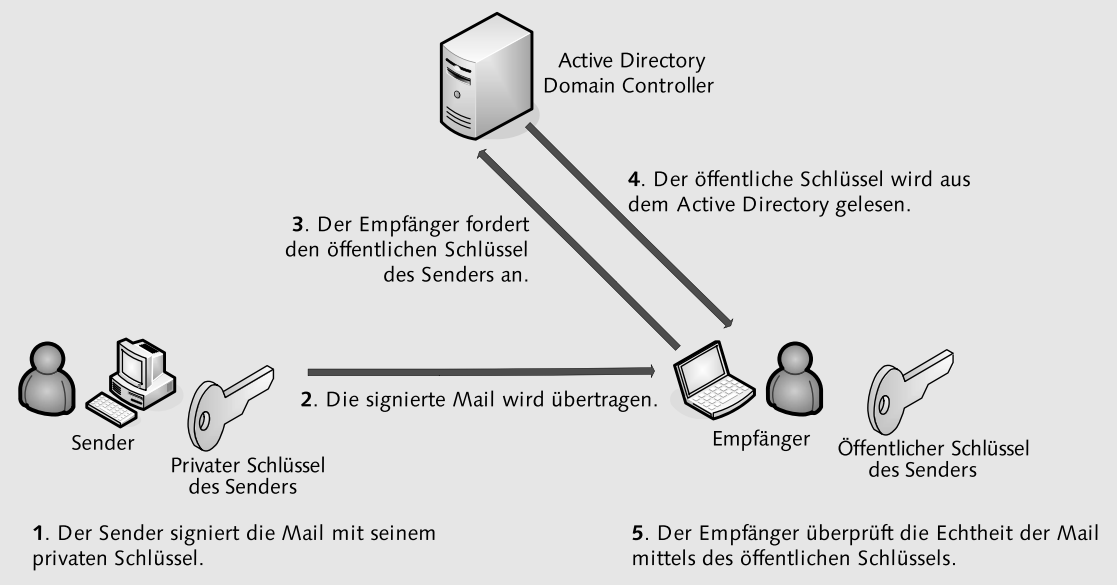


Abbildung 5.31 Signieren von E-Mails

Einfache Überprüfung

Die Überprüfung der Signatur wird in der Praxis etwas anders vorgenommen, als zuvor beschrieben. Zur Überprüfung von Mailsignaturen benötigen Sie nicht den öffentlichen Schlüssel des Absenders, sondern es genügt, wenn Sie der ausgebenden Zertifizierungsstelle vertrauen – und dementsprechend deren Zertifikat installiert haben.

Codesignatur

Die Codesignatur ist in etwa mit dem Signieren von E-Mails zu vergleichen. Hierbei geht es darum, einwandfrei festzustellen, wer ein Stück Code entwickelt und in Umlauf gebracht hat. Ohne Codesignatur kann jeder »Dunkelmann« (oder natürlich auch eine »Dunkelfrau«) ein Stück Code entwickeln, in Umlauf bringen und behaupten, dass es von Microsoft sei – in Wahrheit ist es aber ein Trojaner, der E-Mail-Adressen oder Bankdaten ausspäht.

Bei der Codesignatur wird, genauso wie bei der E-Mail-Signatur, eine Prüfsumme gebildet, die mit dem privaten Schlüssel des Herausgebers signiert wird. Mit dem öffentlichen Schlüssel des Herausgebers (bzw. dem öffentlichen Schlüssel der Stammzertifizierungsstelle, die den Schlüssel des Herausgebers erzeugt hat) kann geprüft werden, ob die Prüfsumme nicht manipuliert worden ist. Dann kann noch kontrolliert werden, ob die zu installierende Datei zu der Prüfsumme passt. Ist irgendwo manipuliert worden, schlägt die Überprüfung fehl, und Sie wissen auf jeden Fall, dass etwas nicht in Ordnung ist.

Auch wenn Ihr Unternehmen nicht selbst Software entwickelt, könnten Sie mit der Codesignatur in Berührung kommen: Bei Office-Makros, die in fast jedem Unternehmen existieren, könnte die Signatur ebenfalls interessant sein. Makros werden definitiv für viele Aufgaben benötigt und sind ja auch durchaus sinnvoll und hilfreich. Bösartige Makros können aber genauso viel Schaden anrichten wie »normaler Code«.

Ein guter Kompromiss zwischen »niemals Makros ausführen« und »alle Makros ausführen« ist, nur von einem vertrauenswürdigen Herausgeber signierte Makros zuzulassen. Dies ist in den Office-Applikationen konfigurierbar: Abbildung 5.32 zeigt den Konfigurationsdialog aus Word 2003. Das eigene Stammzertifikat ist in die Liste der vertrauenswürdigen Herausgeber aufgenommen worden.

Abbildung 5.33 zeigt, wie ein Makro im VBA-Editor von Word 2003 signiert wird. Der Menüpunkt Digitale Signatur führt zu einem Dialog, der die Zertifikate zeigt, die auf dem lokalen System zur Codesignierung zugelassen sind. Das gewünschte Zertifikat kann ausgewählt werden – und das Makro ist signiert.

In der heutigen Zeit, in der schädlicher bzw. bösartiger Code zu einem wirklich ernsten Problem geworden ist, spielt die Codesignatur bereits eine wichtige Rolle – und zwar mit steigender Tendenz. Wenn Sie eigenen Code, der eben auch aus Makros, Skripts oder dergleichen bestehen kann, signieren möchten, benötigen Sie entsprechende Zertifikate.

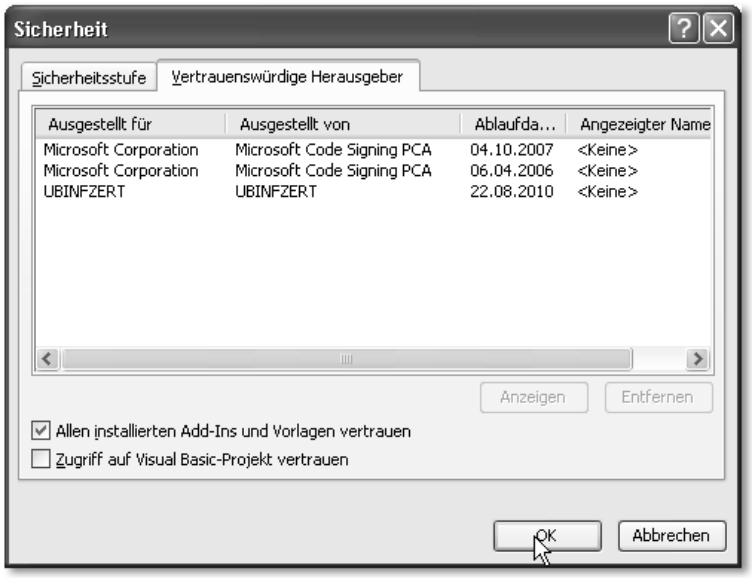


Abbildung 5.32 Die Ausführung von Makros kann auf solche Makros beschränkt werden, die von vertrauenswürdigen Herausgebern signiert worden sind.

Momentan sind wir als IT-Gesellschaft leider noch weit davon entfernt, dass jeder Code, der zum Einsatz kommen soll, signiert ist. Daher ist es nicht möglich, die Ausführung von nicht signiertem (bzw. nicht mit einem Zertifikat einer vertrauenswürdigen Stammzertifizierungsstelle signiertem) Code zu verbieten. In absehbarer Zeit dürfte diese Vision aber Realität werden, was ein großer Schritt in Richtung »sicherer Systeme« wäre.

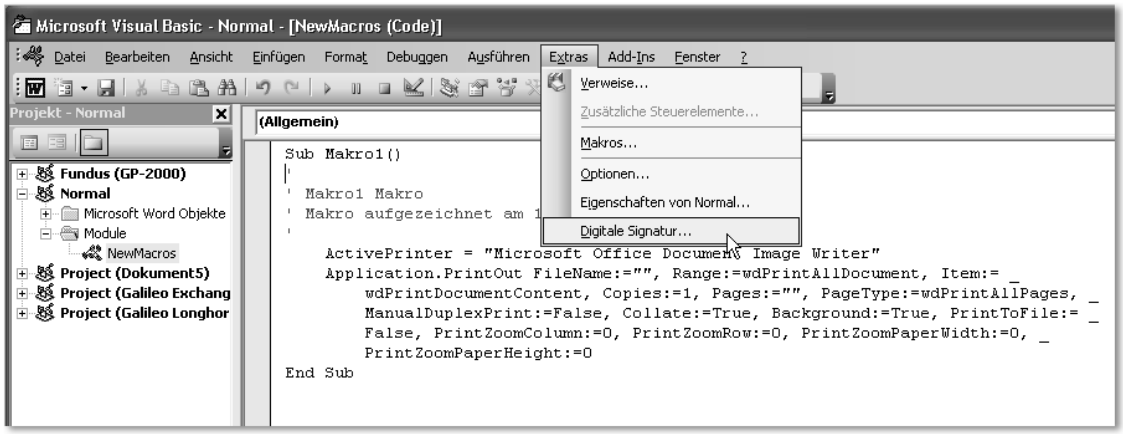


Abbildung 5.33 Konfigurieren der Signatur im VBA-Editor von Word 2003

IP-Verschlüsselung

Auch bei der IP-Kommunikation spielen Verschlüsselung und Signatur eine wichtige Rolle. Auch hier geht es darum, dass die Vertraulichkeit und die Integrität des Datenverkehrs geschützt werden müssen, sprich: Niemand soll die Kommunikation unbefugt mitlesen können, und niemand soll sie verfälschen können. Die

IPSec-Technologie hilft bei der Umsetzung dieser Anforderungen, benötigt aber hierbei Zertifikate.

Anmeldung mit Smartcard

Es ist bekannt, dass die klassische Anmeldung mit Benutzernamen und Passwort nicht höchsten Sicherheitsanforderungen genügt. Die Anmeldung mit Smartcards ist eine häufig verwendete Alternative. Hierbei handelt es sich um eine Zwei-Faktor-Authentifizierung, was bedeutet, dass für die Anmeldung zwei Voraussetzungen erfüllt sein müssen:

- *Haben*: Man muss im Besitz der Smartcard bzw. des darauf gespeicherten Zertifikats sein.
- *Wissen*: Man muss wissen, wie das zugehörige Kennwort heißt.

Ein bekanntes Beispiel für eine Zwei-Faktor-Authentifizierung ist das Abheben von Bargeld mittels EC-Karte: Sie müssen im Besitz der EC-Karte sein und diese in den Automaten schieben, und Sie müssen die PIN kennen. Wenn nicht beide Anforderungen erfüllt werden, bekommen Sie nur Geld, indem Sie den Automaten aufbrechen oder Ähnliches anstellen.

Auf den Smartcards ist ein Benutzerzertifikat gespeichert, das prinzipiell neben der Anmeldung auch für andere Zwecke verwendet werden könnte.

EFS

Encrypting File System (EFS) bezeichnet die Fähigkeit des NTFS-Dateisystems, Dateien zu verschlüsseln.

Wenn Sie in den Eigenschaften einer Datei oder eines Ordners die Verschlüsselung aktivieren, wird zunächst geprüft, ob ein passendes Zertifikat im Zertifikatsspeicher des Benutzers vorhanden ist. Ist dies nicht der Fall, wird eines generiert, wobei es zwei Varianten gibt:

- Wenn im Active Directory eine Unternehmenszertifizierungsstelle vorhanden ist, wird dort automatisch (ohne dass der Benutzer es merkt) ein Zertifikat angefordert und installiert. (Das funktioniert, wenn die Zertifizierungsstelle Zertifikatsanforderungen automatisch verarbeitet.)
- Ist keine Unternehmenszertifizierungsstelle vorhanden, wird auf der lokalen Maschine ein Zertifikat erzeugt.

Zertifikate werden also für EFS auf jeden Fall benötigt. Nun ist es einleuchtend, dass es unbedingt zu bevorzugen ist, dass die EFS-Zertifikate von einer zentralen Zertifizierungsstelle erzeugt werden, als dass jeder Server für jeden Benutzer separate Zertifikate erzeugt; denken Sie vor allem an den Wiederherstellungs-Agenten.

Abbildung 5.34 zeigt ein für die Verwendung mit dem »verschlüsselnden Dateisystem« vorgesehenes Zertifikat im Zertifikatsspeicher des Benutzers.

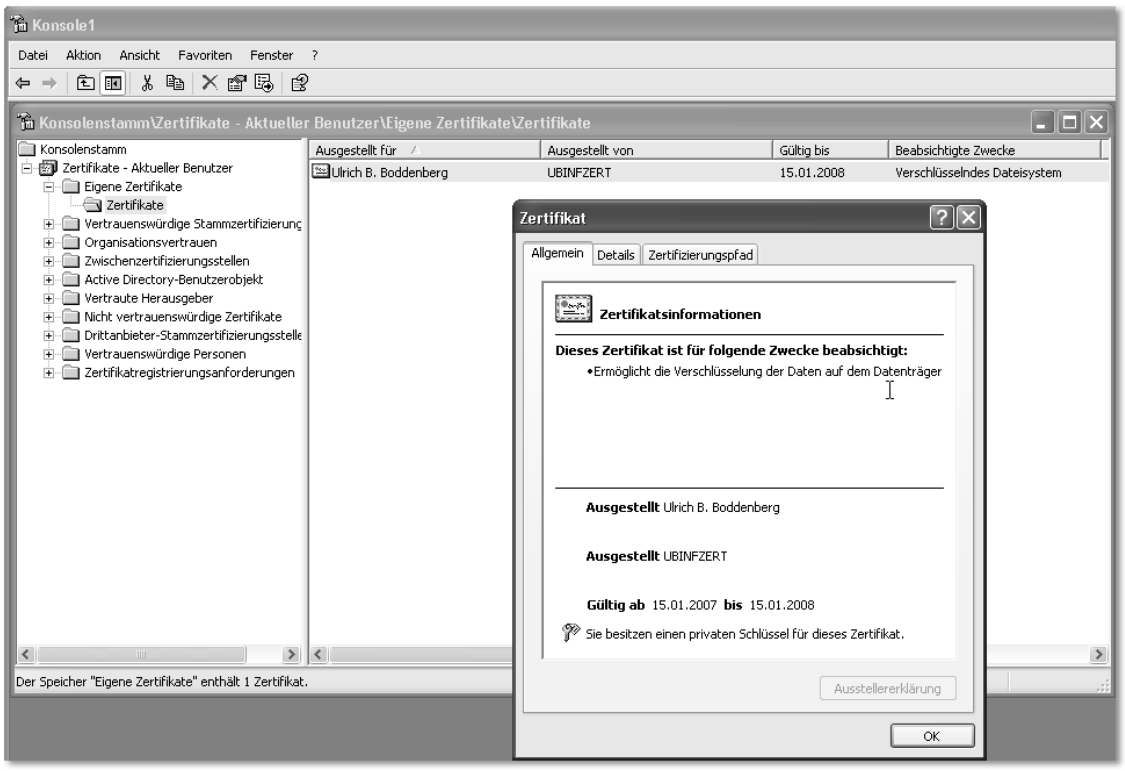


Abbildung 5.34 Das Zertifikat für die Verschlüsselung von Dateien im Zertifikatsspeicher des Benutzers

Wireless Authentification (802.1X)

Soll WLAN, also drahtloses Ethernet, genutzt werden, wird man – wenn man nicht gerade grob fahrlässig handeln möchte – eine Authentifizierung der Benutzer fordern. Erst korrekt authentifizierte Benutzer dürfen Zugriff auf das LAN bekommen.

Um eine optimale Authentifizierung zu gewährleisten, greift man auch bei diesem Anwendungsfall auf Zertifikate zurück, wobei ein entsprechendes Benutzerzertifikat im Zertifikatsspeicher des Anwenders auf dem drahtlos verbundenen Computer vorhanden sein muss.

Fazit

Das Verschlüsseln und Signieren von Informationen oder Kommunikation ist ein wesentlicher Bestandteil von modernen Informationssystemen. Die Anwendungsfälle sind außerordentlich vielfältig und basieren zumeist auf Zertifikaten, die nur sinnvoll zu nutzen sind, wenn sozusagen im Hintergrund eine PKI, eine Public Key Infrastructure, arbeitet.

5.8.2 Installation der Zertifikatdienste und Migration (einstufige Architektur)

Eine *Public Key Infrastructure* (PKI) besteht im einfachsten Fall aus einem Server, der *Active Directory-Zertifikatdienste* (AD CS) ausführt. Dieser Server verfügt über das Stammzertifikat und stellt für Benutzer, Computer, Netzwerkgeräte etc. Zertifikate aus. Dies ist dann eine einstufige Architektur.

In einer größeren und auf Sicherheit bedachten Umgebung wird man eine zweistufige Architektur einführen, bei der das Stammzertifikat der PKI nicht von dem Server ausgestellt worden ist, der die Zertifikate herausgibt. In einer komplexen (weltweit) verteilten Umgebung kann das Zertifikatswesen durchaus auch dreistufig organisiert sein.

Mit den Architekturfragen werden wir uns an späterer Stelle auseinandersetzen, zunächst erläutere ich Ihnen, wie ein einstufiges Zertifikatswesen auf Windows Server 2008 implementiert wird.

Hinweis

Ich zeige hier direkt auch die Migration von einer bestehenden Zertifizierungsstelle.

Um die Active Directory-Zertifikatdienste zu installieren, fügen Sie im Server-Manager eine neue Rolle hinzu. Abbildung 5.35 zeigt den Dialog zur Auswahl der Rolle – der Start ist also einfach. Der Rest der Installation geschieht wie gewohnt über einen Assistenten.

Der erste Dialog des Assistenten beschäftigt sich mit der Frage, welche Komponenten der Active Directory-Zertifikatdienste nun installiert werden sollen (Abbildung 5.36):

- Zertifizierungsstelle: Das ist die »eigentliche« Kernkomponente. Sie ist in der Lage, Zertifikate auszustellen und zu verwalten.
- Zertifizierungsstellen-Webregistrierung: Bei dieser Komponente handelt es sich um ein Webfrontend, mit dessen Hilfe die Benutzer Zertifikate anfordern und einige andere Tätigkeiten im Zusammenhang mit Zertifikaten durchführen können. Dieses Werkzeug werden Sie im weiteren Verlauf kennenlernen.
- Online-Responder: Dies ist eine Komponente, um mittels des *Online Certificate Status Protocol* (OCSP) Informationen über Zertifikatsrückrufe (Revocations) über das Internet bereitzustellen.
- Registrierungsdienst für Netzwerkgeräte: Über diese Komponente können Netzwerkkomponenten wie beispielsweise Router Zertifikate anfordern.

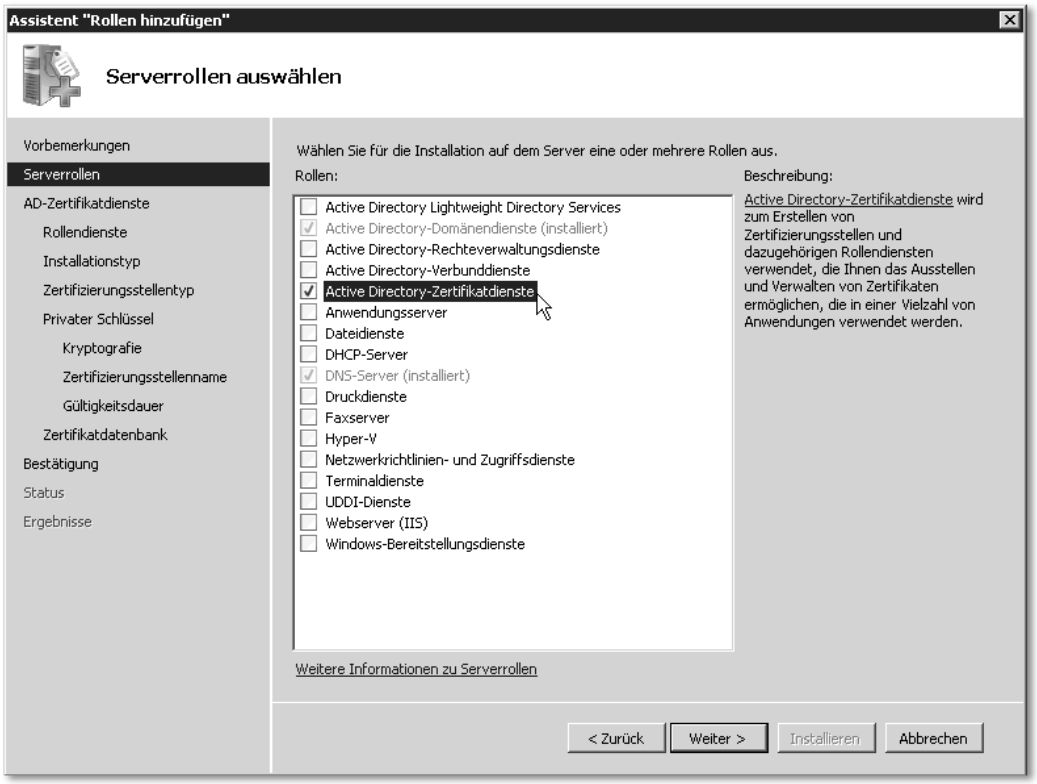


Abbildung 5.35 Für die Installation der Active Directory-Zertifikatdienste wird eine neue Rolle hinzugefügt.

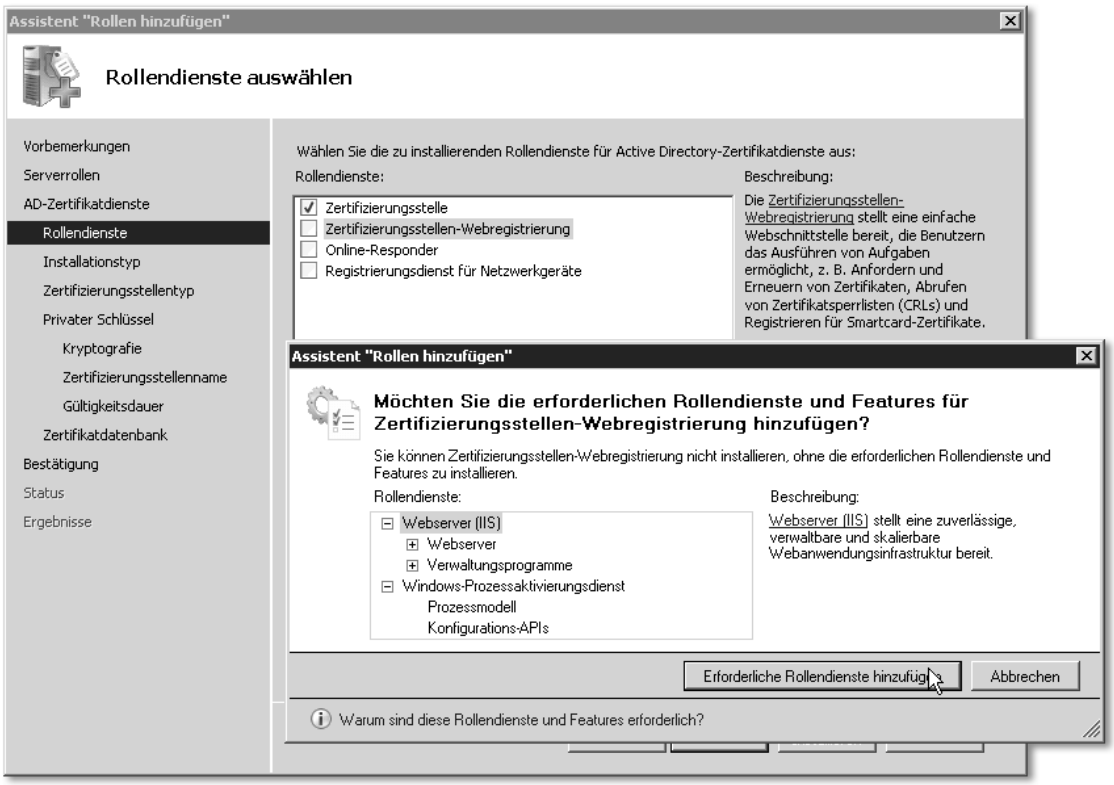


Abbildung 5.36 Die Active Directory-Zertifikatdienste bestehen aus vier Komponenten.

Für dieses Beispiel wird auch die Webregistrierung installiert. Demnach muss auch der Webserver als abhängige Komponente hinzugefügt werden.

Als Nächstes müssen Sie nun festlegen, ob Sie eine Enterprise- oder eine Standalone-Zertifizierungsstelle einrichten möchten (Abbildung 5.37).

- Eine Enterprise-Zertifizierungsstelle ist in das Active Directory integriert (Option UNTERNEHMEN).
- Eine Standalone-Zertifizierungsstelle (Option EIGENSTÄNDIG) kann zwar auf einem Server, der sich im AD befindet, installiert werden, ist aber nicht weiter integriert.

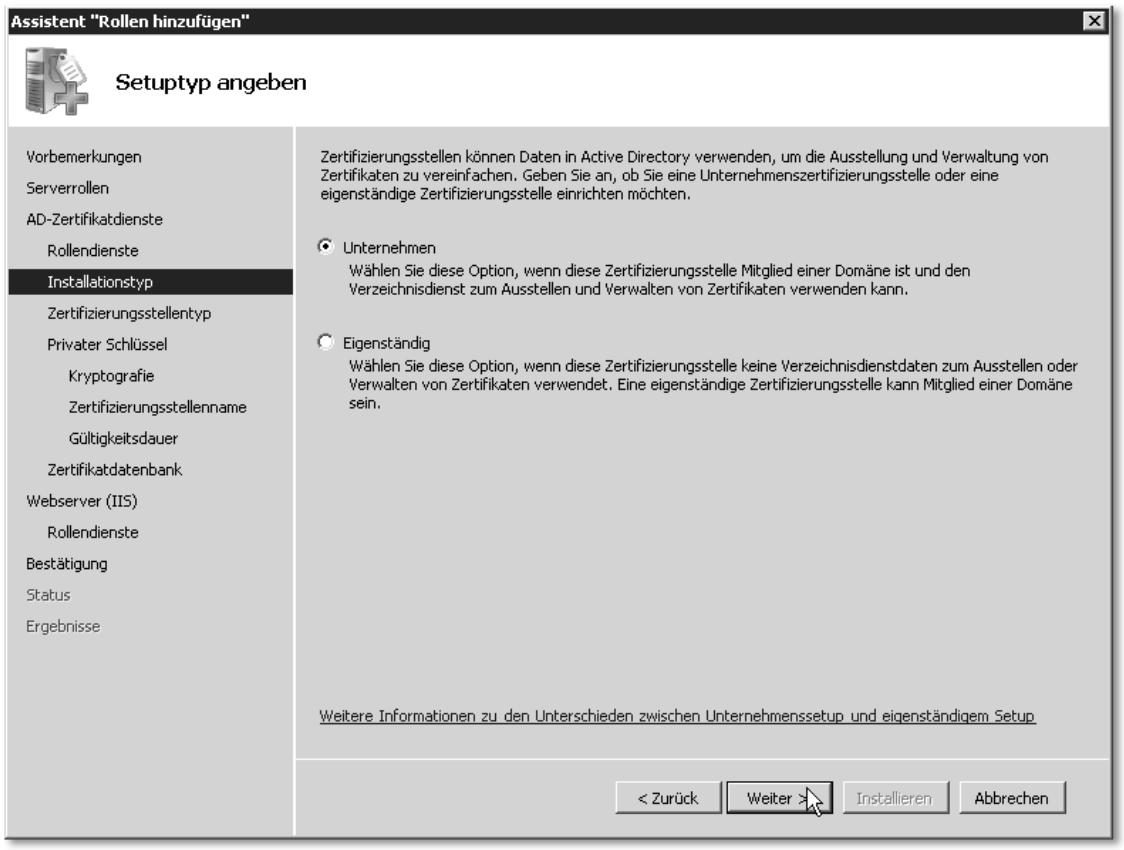


Abbildung 5.37 Im Active Directory wird man im Allgemeinen eine Enterprise-Zertifizierungsstelle installieren.

Unterschiede bei der Standard- und der Enterprise-Edition

Eine Enterprise-Zertifizierungsstelle kann auf einer Standard-Edition des Windows-Server-Betriebssystems installiert werden.

Es gibt aber im Bereich der Zertifizierungsstellen Unterschiede zwischen der Enterprise- und der Standard-Edition des Betriebssystems: Bei einer Zertifizierungsstelle, die auf der Standard-Edition läuft, können keine Vorlagen angepasst werden.

»Integriert« bedeutet in diesem Zusammenhang beispielsweise, dass die Zertifizierungsstelle im Active Directory eingetragen wird. Clients, die ein Zertifikat anfordern, finden dieses durch eine Suche im Active Directory.

In Abbildung 5.38 sehen Sie die Suche nach einem ENROLLMENT SERVICE, also einer Zertifizierungsstelle, die Zertifikate herausgibt, in ADSI-Editor. Der Konfigurationsnamenskontext enthält unterhalb des Knotens SERVICES einen Eintrag PUBLIC KEY SERVICES. Dort finden Sie im Unterpunkt ENROLLMENT SERVICES eine Liste aller Server, die Zertifikate ausstellen. In den Eigenschaften eines solchen Eintrags findet sich neben einigen anderen Informationen auch der DNS-Name des Servers. Hierhin kann ein Active Directory-Client seine Zertifikatsanforderung senden.

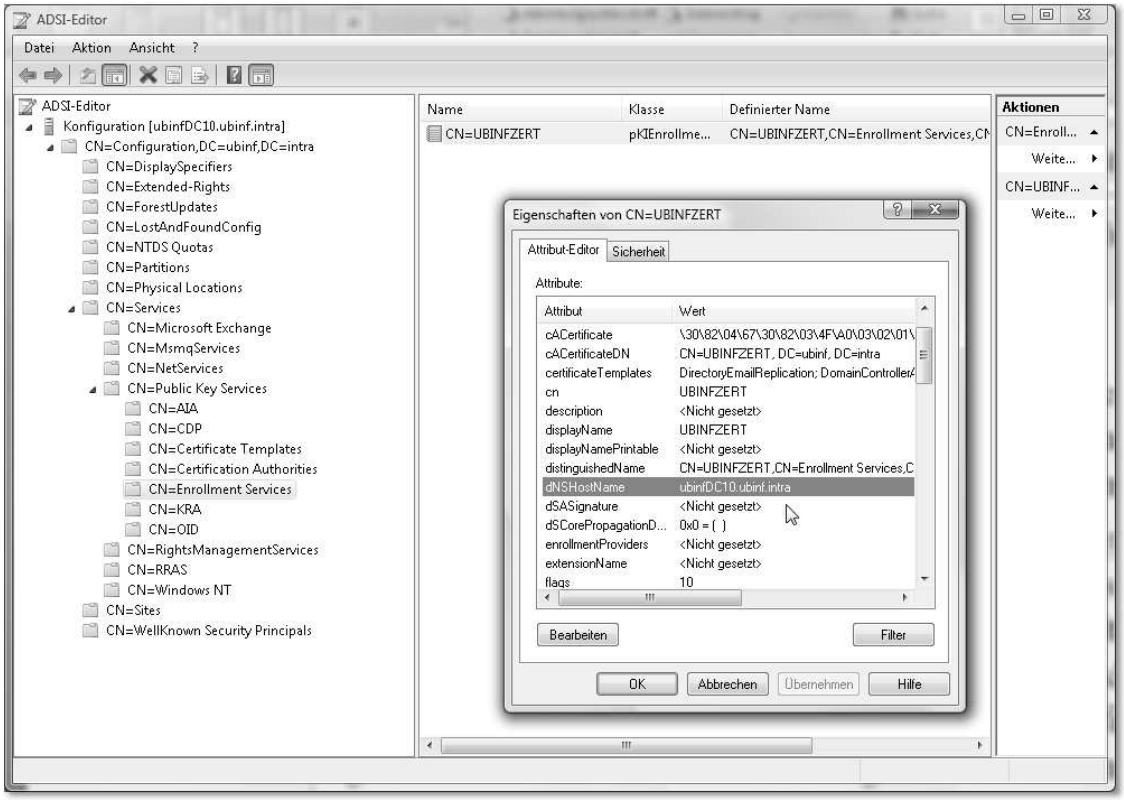


Abbildung 5.38 Eine Enterprise-Zertifizierungsstelle ist im Konfigurationsnamenskontext des Active Directory verzeichnet.

Im nächsten Schritt muss der Typ der Zertifizierungsstelle festgelegt werden (Abbildung 5.39):

- Wenn Sie die erste Zertifizierungsstelle installieren, wird diese eine STAMMZERTIFIZIERUNGSSTELLE (Root CA) werden. Dies ist die höchste Zertifizierungsstelle in der PKI.

- Falls die installierte Zertifizierungsstelle eine untergeordnete Rolle in einer umfangreicheren PKI einnehmen soll, entscheiden Sie sich für den zweiten Punkt, eine Untergeordnete Zertifizierungsstelle (Subordinate CA).

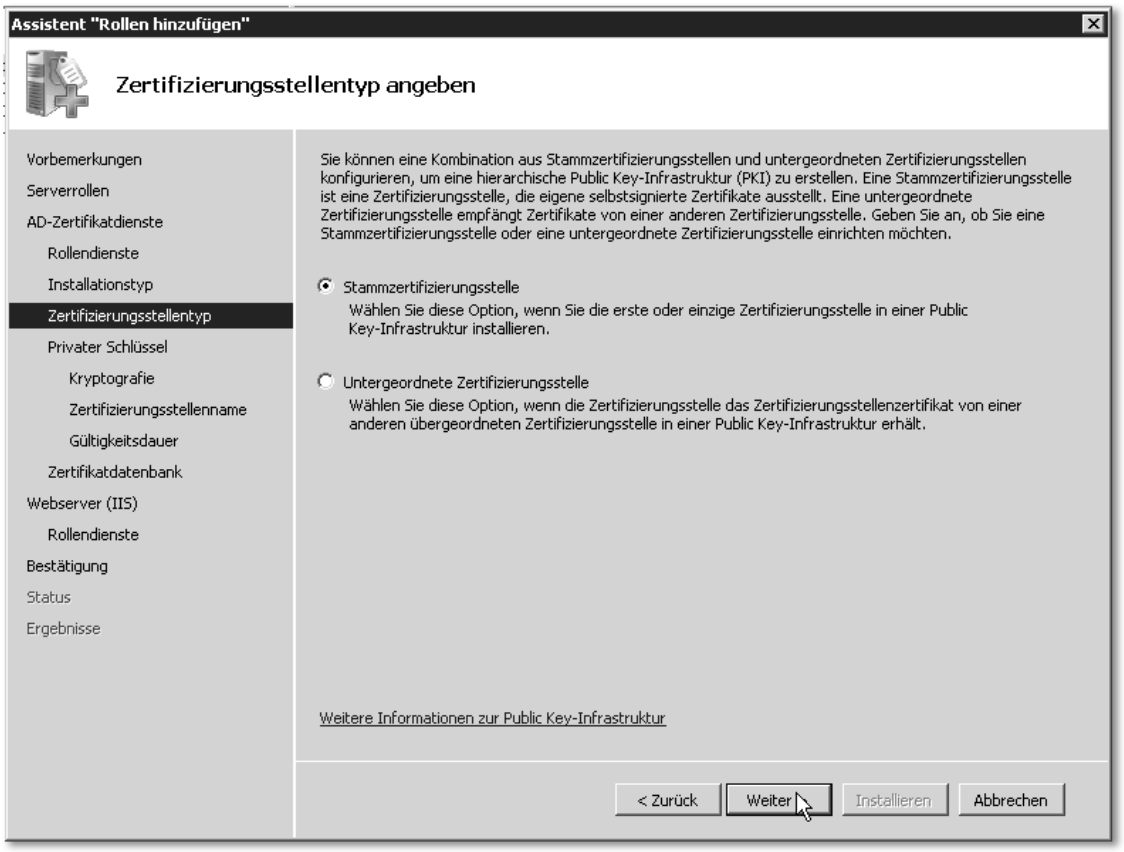


Abbildung 5.39 Die erste Zertifizierungsstelle wird eine Stammzertifizierungsstelle (Root CA).

Weitere Informationen zum Aufbau einer komplexeren PKI-Hierarchie finden Sie im weiteren Verlauf des Kapitels.

Beachten Sie, dass der Name des Servers, auf dem die Zertifizierungsstelle installiert wird, nicht mehr geändert werden kann. Das heißt, Sie könnten ihn schon ändern, aber der Zertifizierungsstelle wird das gar nicht gut bekommen.

Eine Zertifizierungsstelle braucht einen privaten Schlüssel. Falls ein solcher vorhanden ist (z. B. weil es sich bei der Installation um eine Neuinstallation/Migration eines zuvor bereits vorhandenen Systems handelt), kann er an dieser Stelle eingelesen werden. Bei einer Erstinstallation werden Sie einen neuen Schlüssel erzeugen lassen. Die benötigte Option können Sie in dem Dialog aus Abbildung 5.40 auswählen.

Falls Sie bereits über ein Zertifikat für die Zertifizierungsstelle verfügen (weil es die Zertifizierungsstelle bereits gab), können Sie es in dem Dialog aus Abbildung 5.41 auswählen.

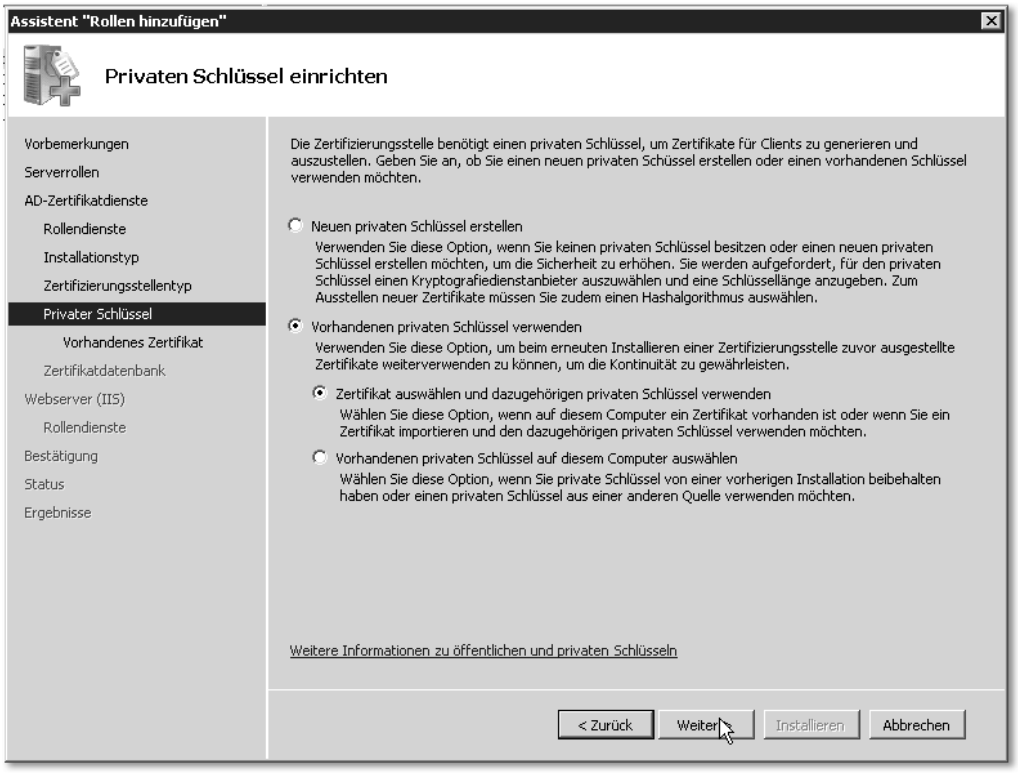


Abbildung 5.40 Bei einer Migration/Installation greifen Sie auf einen vorhandenen privaten Schlüssel zu; bei einer Erstinstallation lassen Sie einen neuen privaten Schlüssel erstellen.

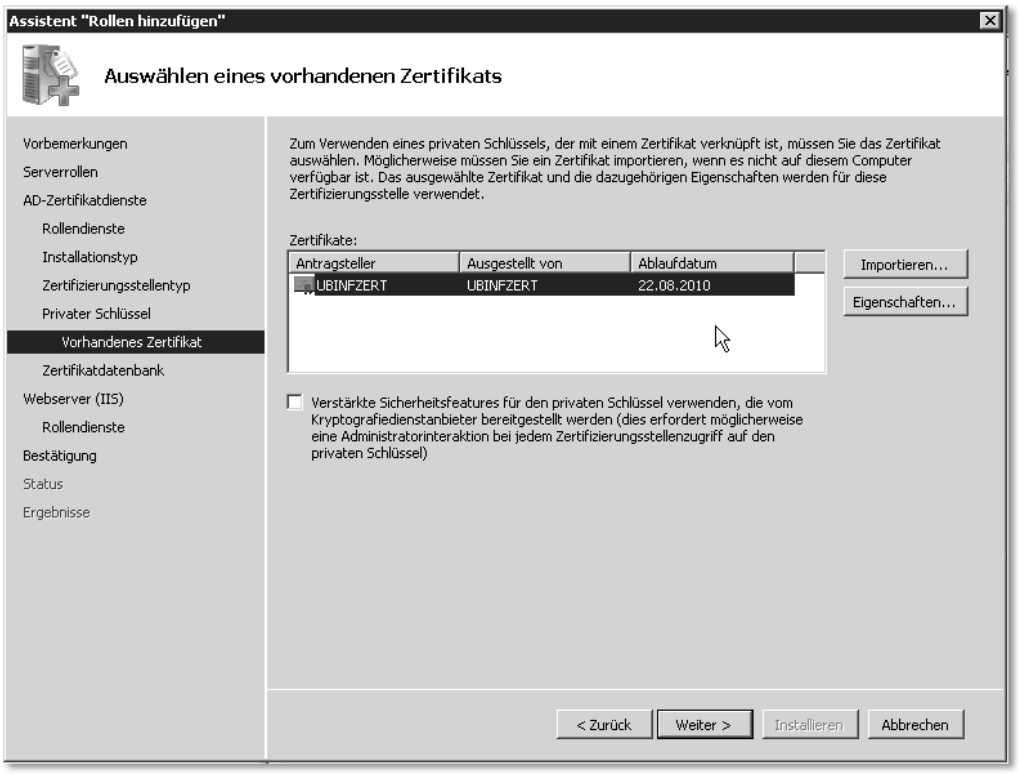


Abbildung 5.41 Ist bereits ein Zertifikat für die Stammzertifizierungsstelle vorhanden, wählen Sie es hier aus.

Sicherung und Sicherheit

Das Erzeugen des privaten Schlüssels der Stammzertifizierungsstelle ist mit einem Mausklick geschehen. Für das »weitere Leben« dieses Schlüssels gelten allerdings ein paar elementar wichtige Regeln – und zwar die Sicherung und Sicherheit betreffend:

- *Sicherung*: Der erzeugte Schlüssel muss unbedingt gesichert und sorgfältig aufbewahrt werden. Es ist absolut essenziell, dass er nicht durch irgendwelche unglücklichen Umstände verloren geht. Wenn dies doch passiert, bedeutet das, dass Sie Ihr komplettes Zertifikatswesen neu aufsetzen müssen.
- *Sicherheit*: Der erzeugte Schlüssel darf keinesfalls unberechtigten Personen in die Hände fallen. Diese könnten beispielsweise beliebige Zertifikate erzeugen und durch gefälschte Identitäten Schaden anrichten – im ungünstigsten Fall wird das jahrelang nicht bemerkt.

Der erzeugte private Schlüssel ist das Herzstück Ihres Zertifikatswesens und muss dementsprechend sorgfältig behandelt werden.

Falls Sie zum ersten Mal eine Stammzertifizierungsstelle installieren und folglich im Dialog aus Abbildung 5.40 das Erstellen eines neuen privaten Schlüssels gewählt haben, müssen Sie Folgendes tun:

- Auf der dann folgenden Dialogseite können der *Cryptographic Service Provider*, der Hash-Algorithmus und die Schlüssellänge eingestellt werden. Im Normalfall können die vorbelegten Werte übernommen werden. Ein höherer Wert für die Schlüssellänge bringt vordergründig zwar »mehr Sicherheit«; ich gehe aber davon aus, dass die meisten Unternehmen und Organisationen wesentlich dringlichere (und bislang häufig noch unbemerkte) Sicherheitsprobleme haben als nun ausgerechnet die Schlüssellänge des Schlüssels der Stammzertifizierungsstelle.
- Weiter geht es mit dem Namen der Stammzertifizierungsstelle. Wie ich Ihnen bereits weiter vorn gezeigt habe, werden die Zertifizierungsstellen im Active Directory eingetragen, um Anwendungen ein leichtes Auffinden zu ermöglichen. Demzufolge braucht der Name nicht unbedingt besonders »menschenfreundlich« zu sein. Der Assistent setzt den Namen aus der Domäne und dem Server zusammen, sodass sich ein »Bandwurmeffekt« einstellt. Das macht aber nichts. Mein Tipp lautet also, die vorgeschlagenen Werte zu bestätigen.
- Im nächsten Dialog fragt der Assistent nach der Gültigkeit des zu erzeugenden Schlüssels. Der voreingestellte Wert von fünf Jahren ist für eine einstufige Stammzertifizierungsstelle durchaus üblich.

  Kürzere Gültigkeitszeiträume finden sich bei Zertifikaten für Benutzer oder Computer. Das Problem bei kurzen Laufzeiten ist, dass die Zertifikate häufig erneuert werden müssen, was bei Benutzer- und Computerzertifikaten auch

kein Problem darstellt. Bei einer Stammzertifizierungsstelle ist das alles nicht mehr so ganz unproblematisch, weil die Gültigkeit der von ihr ausgestellten Zertifikate auch dementsprechend angepasst werden muss. In mehrstufigen PKI-Architekturen ist es nicht unüblich, dass das Stammzertifikat eine Gültigkeitsdauer von 20 Jahren oder länger hat. Wenn Sie sich die Gültigkeitsdauer der mit den Betriebssystemen mitgelieferten Zertifikate kommerzieller Stammzertifizierungsstellen anschauen (Verisign, Thawte & Co.) werden Sie feststellen, dass diese teilweise sogar für 30 Jahre gültig sind.

Grundsätzlich würde ich für die Stammzertifizierungsstelle eher zu einer längeren als zu einer kürzeren Gültigkeitsdauer tendieren.

Die letzte Auswahl in diesem Assistenten bezieht sich auf den Speicherort für die Zertifikatsdatenbank. In dieser Zertifikatsdatenbank werden alle Informationen beispielsweise zu den ausgestellten und widerrufenen Zertifikaten gespeichert. Es versteht sich von selbst, dass dieser Speicherort gut gesichert sein muss und dass die Zertifikatsdatenbank regelmäßig gesichert werden muss (Abbildung 5.42).

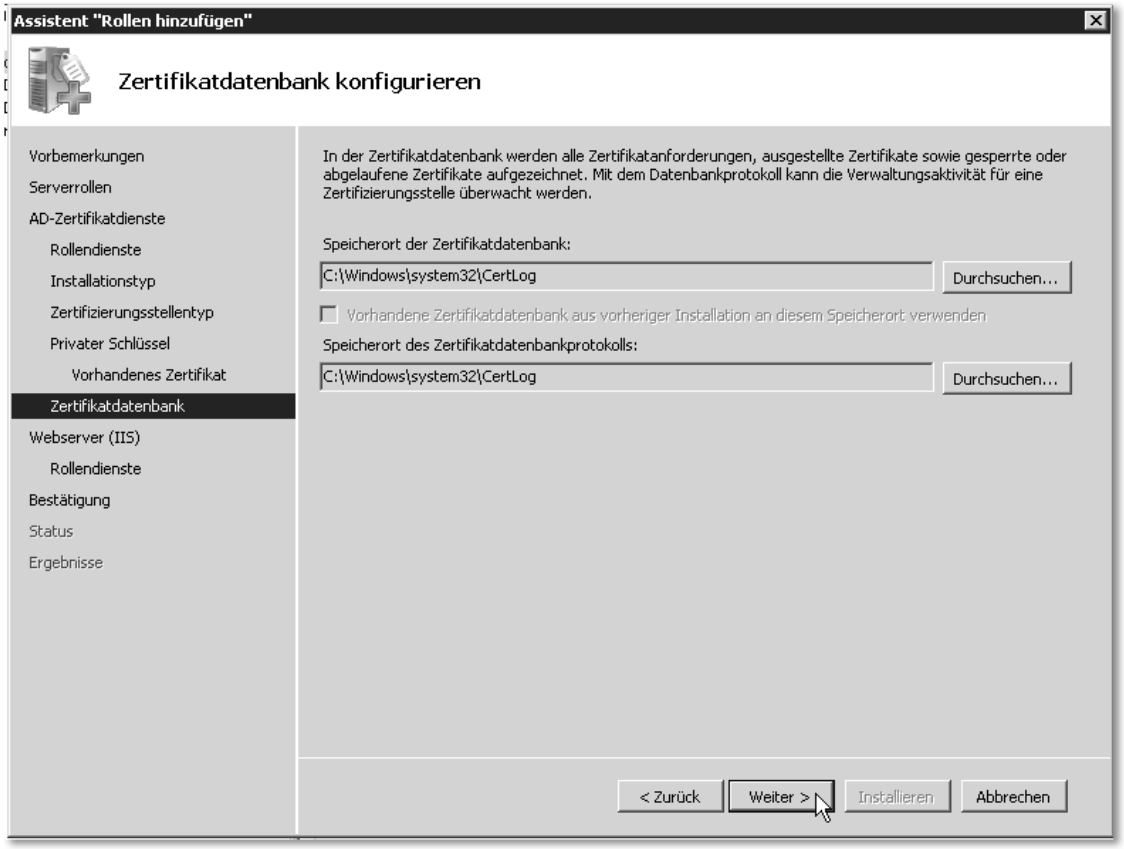


Abbildung 5.42 Der Speicherort für die Zertifikatsdatenbank wird in diesem Dialogschritt ausgewählt.

PKI-Installation ist unumgänglich, aber nicht schwierig

Das Thema Zertifikate wird von vielen Administratoren nur sehr zurückhaltend und mit wenig Begeisterung angegangen. Das liegt vermutlich daran, dass den Zertifikaten die Aura eines schwierigen und komplizierten Themas anhaftet.

Wie schon zu Beginn des Abschnitts erwähnt wurde, werden Sie spätestens mittelfristig nicht um eine Public Key Infrastructure herumkommen, die eigene Zertifikate ausgibt. Außerdem haben Sie gesehen, dass die Installation gar nicht schwierig ist.

Wiederherstellen der Zertifikatdatenbank

Falls Sie eine bestehende Zertifizierungsstelle ersetzen, muss nun noch die Zertifikatdatenbank wiederhergestellt werden. Hierzu starten Sie die Konfiguration der Zertifizierungsstelle und rufen den Menüpunkt ZERTIFIZIERUNGSSTELLE WIEDERHERSTELLEN auf (Abbildung 5.43).

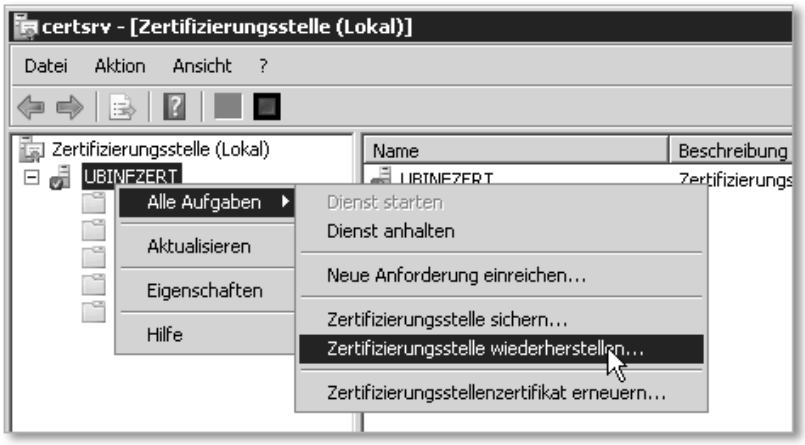


Abbildung 5.43 In der neu installierten Zertifizierungsstelle rufen Sie das Einspielen der Sicherung auf.

Der daraufhin gezeigte Dialog fragt ab, was wiederhergestellt werden soll. Zur Auswahl stehen das ZERTIFIZIERUNGSSTELLENZERTIFIKAT und die ZERTIFIKATDATENBANK. Weiterhin muss der Pfad, in dem sich die Sicherung der Zertifizierungsstelle befindet, angegeben werden (Abbildung 5.44).

Falls Sie das Zertifizierungsstellenzertifikat wiederherstellen, wird ein Zugriff auf den privaten Schlüssel erfolgen. Dieser Vorgang ist durch ein Kennwort gesichert, das bei der Sicherung festgelegt worden ist (Abbildung 5.45).

Abbildung 5.44 Mit diesem Dialog starten Sie die Wiederherstellung.

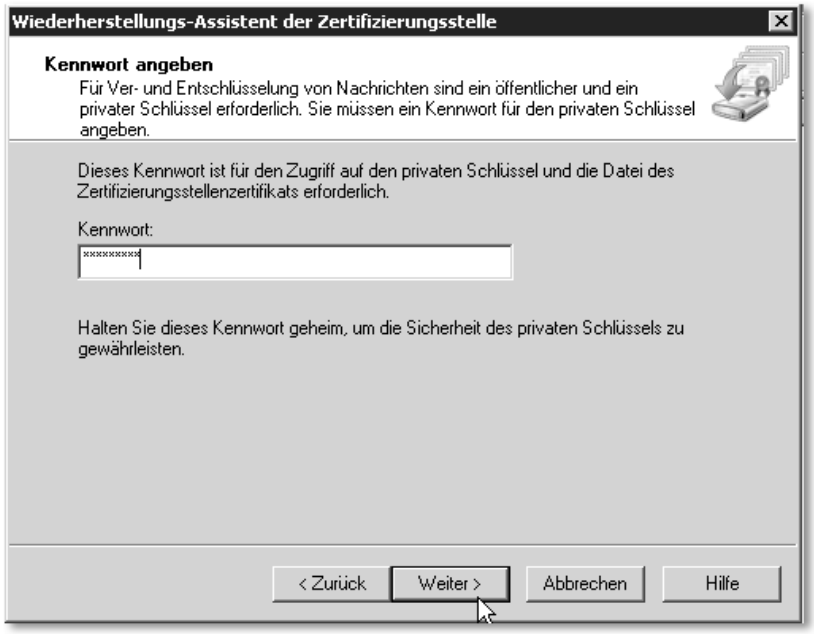


Abbildung 5.45 Beim Zugriff auf den privaten Schlüssel wird ein Kennwort abgefragt.

Nach der erfolgreichen Wiederherstellung wird der Assistent anbieten, die Zertifikatdienste zu starten – und fertig (Abbildung 5.46)!

Sie können leicht überprüfen, ob die Wiederherstellung der Zertifikatdatenbank einwandfrei funktioniert hat, indem Sie die Liste der bereits ausgestellten Zertifikate abrufen (Abbildung 5.47). Das Verschieben der Zertifizierungsstelle ist also ohne Verlust der »Historie« durch simple Sicherung und Rücksicherung möglich.

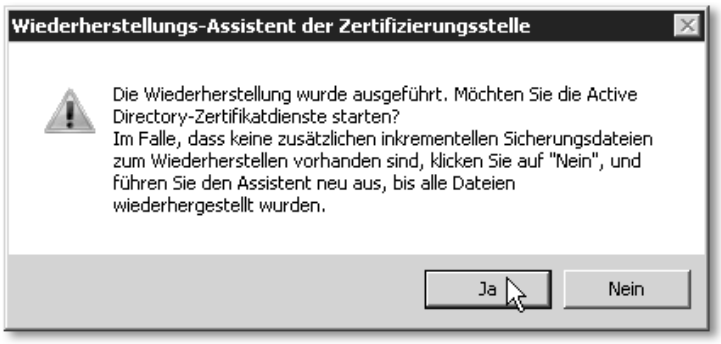


Abbildung 5.46 Nach der erfolgten Wiederherstellung wird der Assistent die Zertifizierungsstelle starten.

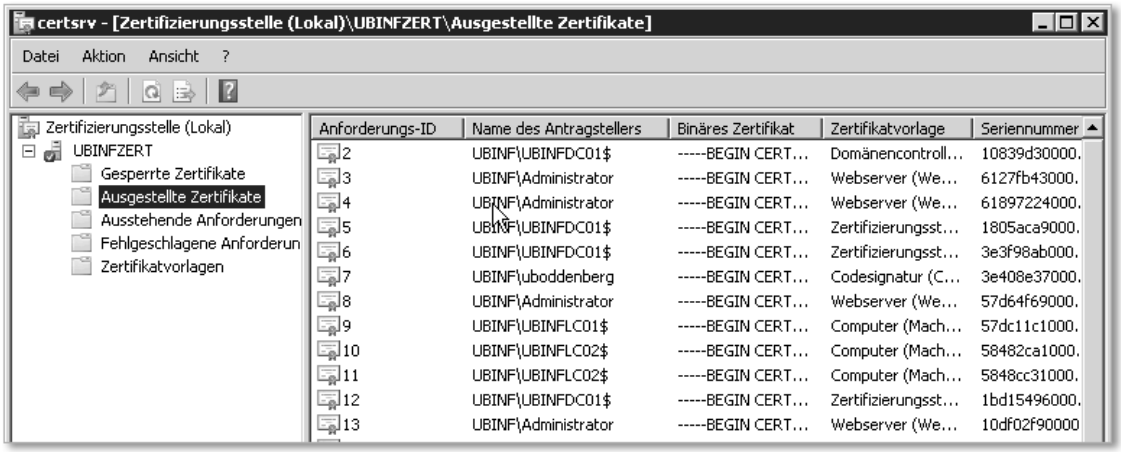


Abbildung 5.47 Nach der Wiederherstellung sind auch die bereits ausgestellten Zertifikate sichtbar.

5.8.3 Zertifikate aus Sicht des Clients

Eine Stammzertifizierungsstelle zu haben ist zwar sehr schön, bringt aber nur sehr wenig, wenn Sie keine Zertifikate damit ausstellen. Es gibt viele verschiedene Wege, ein Zertifikat auf einen Client zu bringen. Ich werde Ihnen in diesem Abschnitt einige vorstellen.

Zunächst beginnen wir aber mit einem Zertifikat, das Sie auf Ihren Clients nicht mehr installieren müssen – weil es schon da ist. Das Zertifikat der im Active Directory als Stammzertifizierungsstelle installierten Zertifizierungsstelle (Enterprise CA) wird, ohne dass Sie etwas daran tun müssen, auf alle Domänenmitglieder (Domänencontroller, Mitgliedsserver, Clients) verteilt. Haben Sie Zweifel? Dann schauen Sie doch im MMC Snap-In ZERTIFIKATE nach. In Abbildung 5.48 können Sie erkennen, dass das eigene Zertifikat tatsächlich neben den Stammzertifikaten solch illustrer Unternehmen wie Microsoft und Verisign einsortiert worden ist.

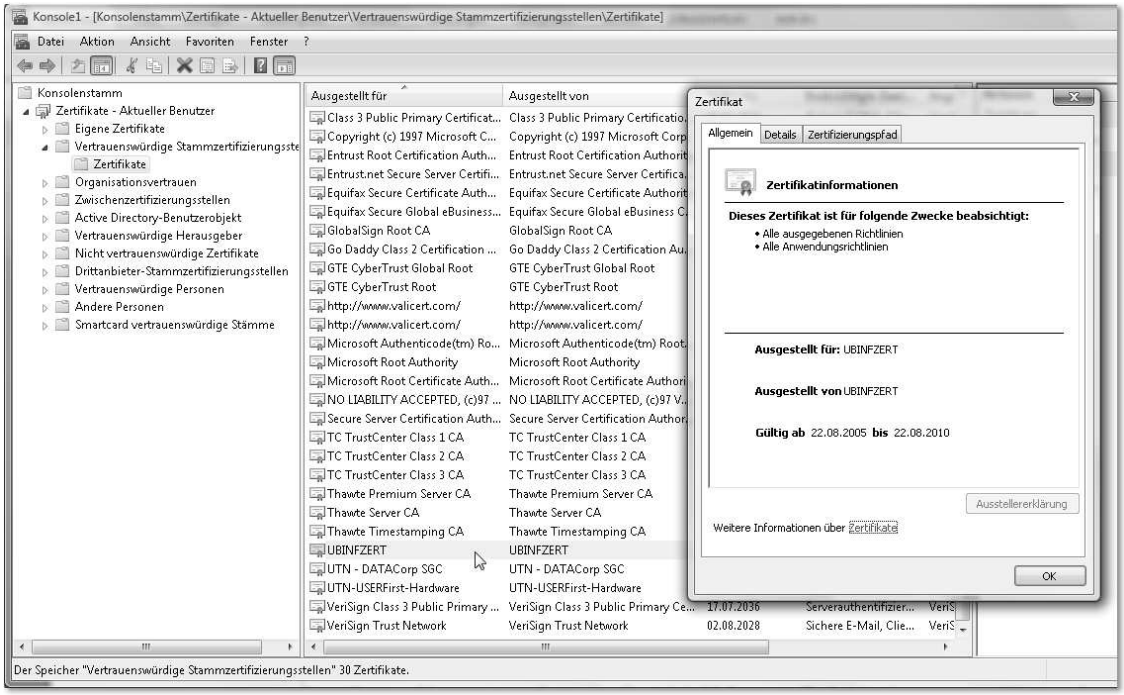


Abbildung 5.48 Das Zertifikat der eigenen Stammzertifizierungsstelle wird automatisch auf allen Computern der Domäne installiert.

Nun wird der Benutzer für einige Anwendungsfälle (z. B. Verschlüsseln und Signieren von E-Mails, EFS-Dateisystemverschlüsselung etc.) ein Benutzerzertifikat benötigen. Auch dies lässt sich auf verschiedene Weisen realisieren. Beispielsweise kann jeder Benutzer über das MMC-Snap-In ZERTIFIKATE ein Benutzerzertifikat anfordern, das dann im selben Arbeitsgang auch gleich installiert wird. Wie es gemacht wird, können Sie in Abbildung 5.49 sehen.

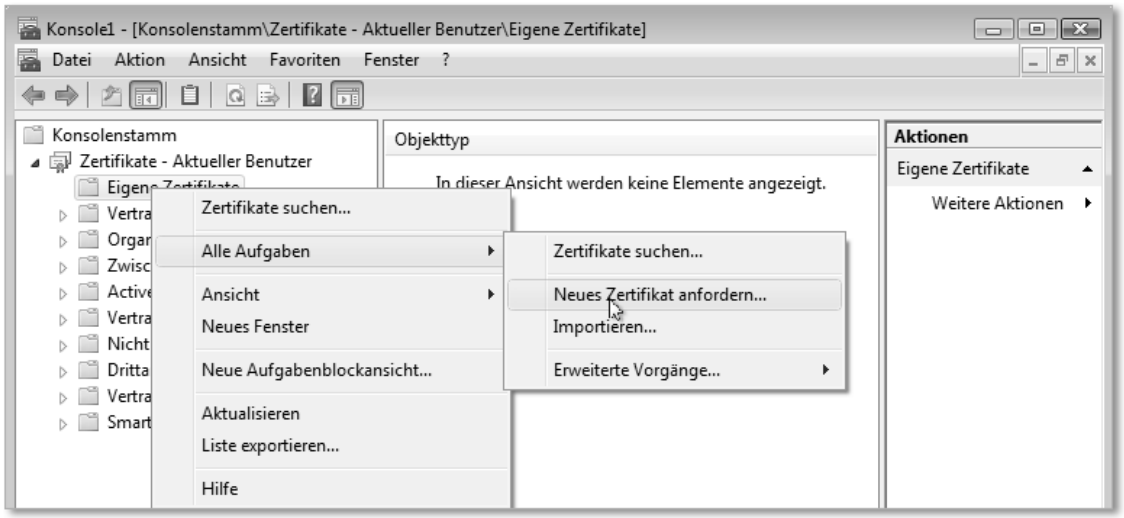


Abbildung 5.49 Ein Benutzer kann mit dem Snap-In ein neues Zertifikat anfordern.

Wie üblich startet ein Assistent, mit dem zunächst der Typ des Zertifikats gewählt werden kann (Abbildung 5.50). Angezeigt werden hier nur die Zertifikate, zu denen der Benutzer berechtigt ist – mehr dazu folgt ein wenig später in Abschnitt 5.8.5, »Zertifikatsvorlagen«.

Auf diese Weise lassen sich übrigens nicht nur Benutzerzertifikate, sondern auch solche für Computer anfordern.

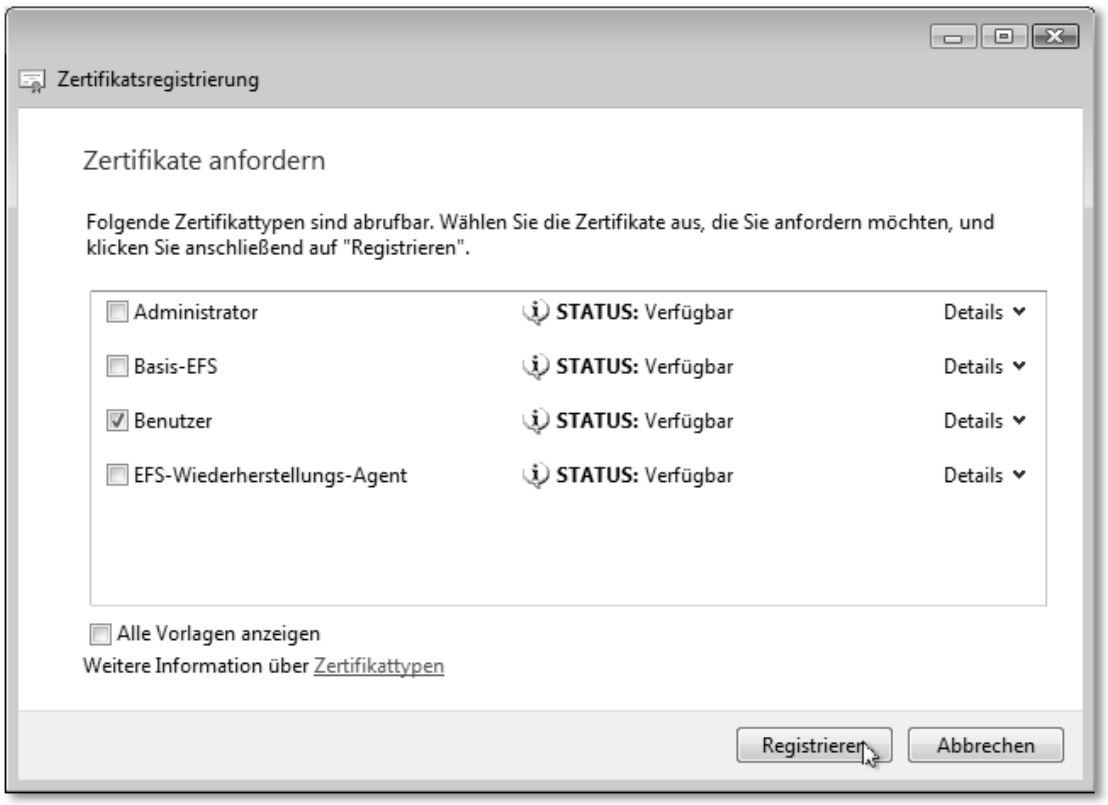


Abbildung 5.50 Zunächst muss der Typ der Zertifikats ausgewählt werden.

Das Snap-In ermittelt zunächst im Active Directory, wo sich eine Zertifizierungsstelle befindet. Anschließend wird das Zertifikat angefordert. Wenn die Zertifizierungsstelle so konfiguriert ist, dass Zertifikatsanforderungen automatisch verarbeitet werden, ist das Zertifikat wenige Sekunden später ausgestellt und installiert. Es sollte so aussehen wie in Abbildung 5.51 gezeigt.

Das neu ausgestellte Zertifikat wird sich im ZERTIFIKATE-Snap-In unter EIGENE ZERTIFIKATE • ZERTIFIKATE finden. Sie können Details zu dem ausgestellten Zertifikat in dessen Eigenschaftendialog einsehen, beispielsweise (Abbildung 5.52):

- Das Zertifikat ist für die Verschlüsselung von Dateien, für das Signieren und Verschlüsseln von E-Mails und für die Authentifizierung geeignet.
- Das Zertifikat ist ein Jahr lang gültig.

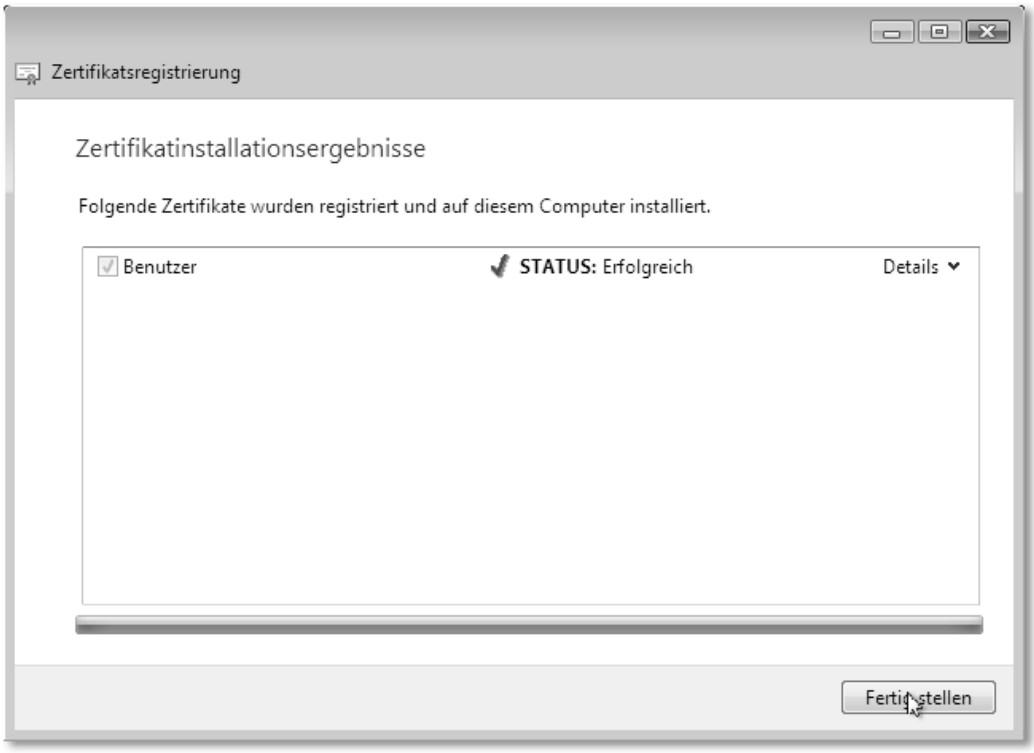


Abbildung 5.51 Das Anfordern und Installieren des Zertifikats war erfolgreich, wenn diese Meldung angezeigt wird.

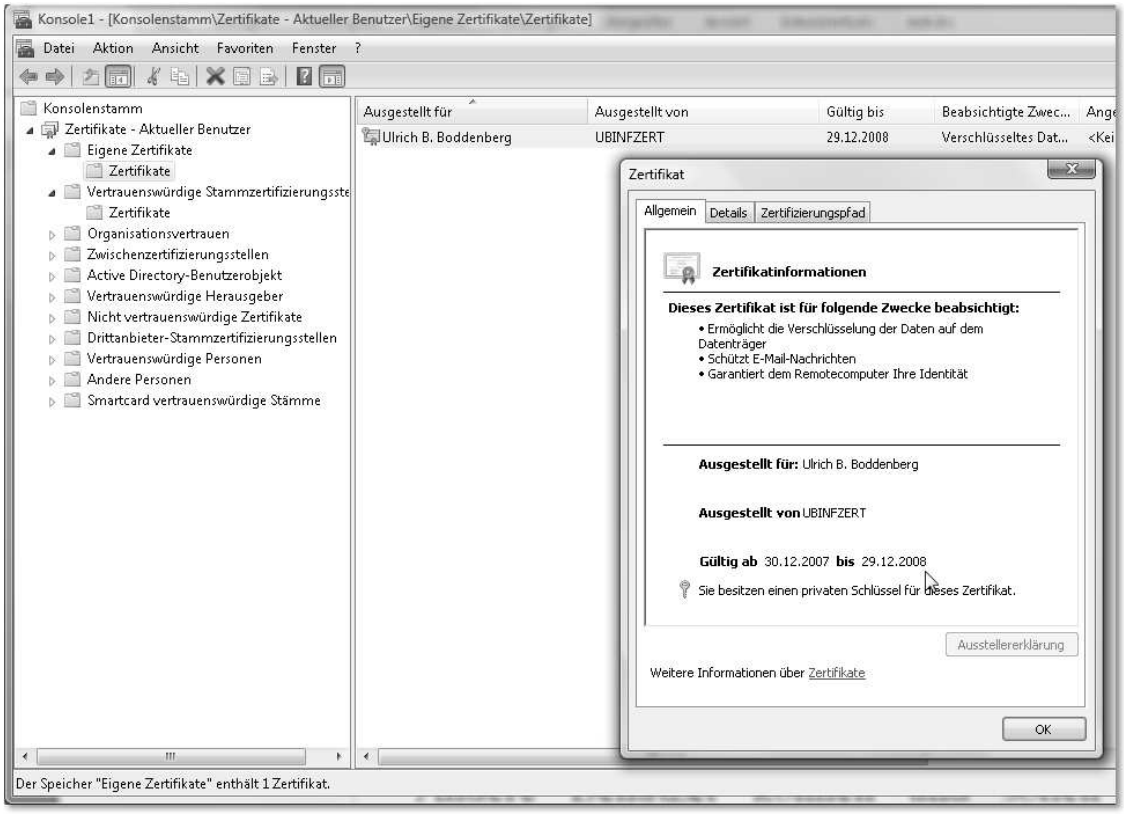


Abbildung 5.52 Das neu erstellte Zertifikat kann im »Zertifikate«-Snap-In eingesehen werden.

- Der Benutzer besitzt den privaten Schlüssel für das Zertifikat. Andere Benutzer können und sollen über den öffentlichen Schlüssel verfügen (z. B., um Mails für dessen Besitzer zu verschlüsseln), der private Schlüssel ist aber nur einem Benutzer vorbehalten.

Benutzerzertifikate werden nicht nur auf dem Computer, mit dem das Zertifikat angefordert wurde, sondern auch im Active Directory gespeichert. Dies dient zwei Zwecken:

- Das Benutzerzertifikat steht auch bereit, wenn der Benutzer sich an einem anderen PC anmeldet. Der lokale Zertifikatsspeicher erhält dann das im Active Directory gespeicherte Zertifikat (bzw. die dort gespeicherten Zertifikate).
- Benötigt ein anderer Benutzer den öffentlichen Schlüssel des Zertifikats, kann dies mittels des Active Directory realisiert werden. Dies wird beispielsweise genutzt, wenn ein Outlook-Client eine E-Mail für einen anderen Benutzer verschlüsseln möchte.

In Abbildung 5.53 sehen Sie in ADSI-Editor, dass das Zertifikat im Benutzerobjekt abgelegt ist – und zwar wird das Attribut USERCERTIFICATE verwendet. Wenn, wie in der Abbildung, mehrere Zertifikate für diesen Benutzer vorhanden sind, werden sie alle in ADSI-Editor angezeigt.

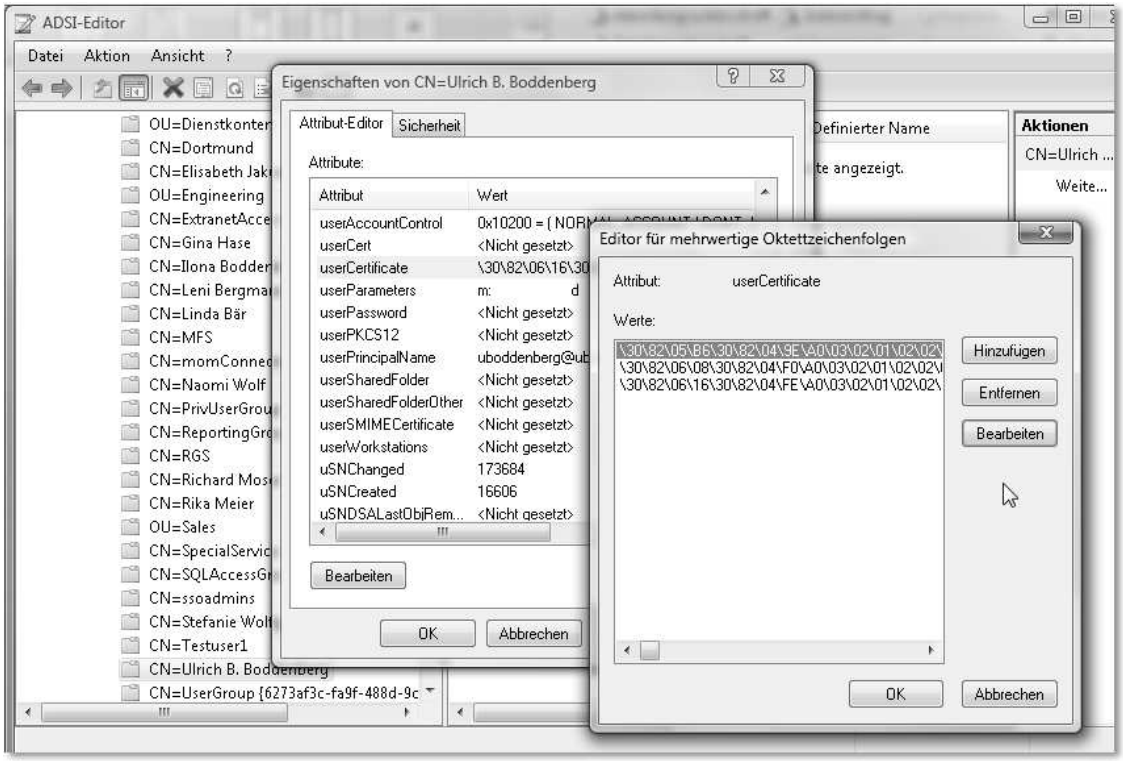


Abbildung 5.53 Benutzerzertifikate werden im Active Directory gespeichert – hier gezeigt mit ADSI-Editor.

Sie können das ausgestellte Zertifikat übrigens auch über das Konfigurationswerkzeug der Zertifizierungsstelle sehen. Unterhalb des Knotens Ausgestellte Zertifikate wird es verzeichnet sein (Abbildung 5.54).

Im Kontextmenü kann das Zertifikat beispielsweise exportiert und auch gesperrt werden. Das Sperren eines Zertifikats ist beispielsweise dann notwendig, wenn ein Mitarbeiter das Unternehmen verlässt oder das Zertifikat gestohlen worden ist (z. B. gemeinsam mit einem Notebook).

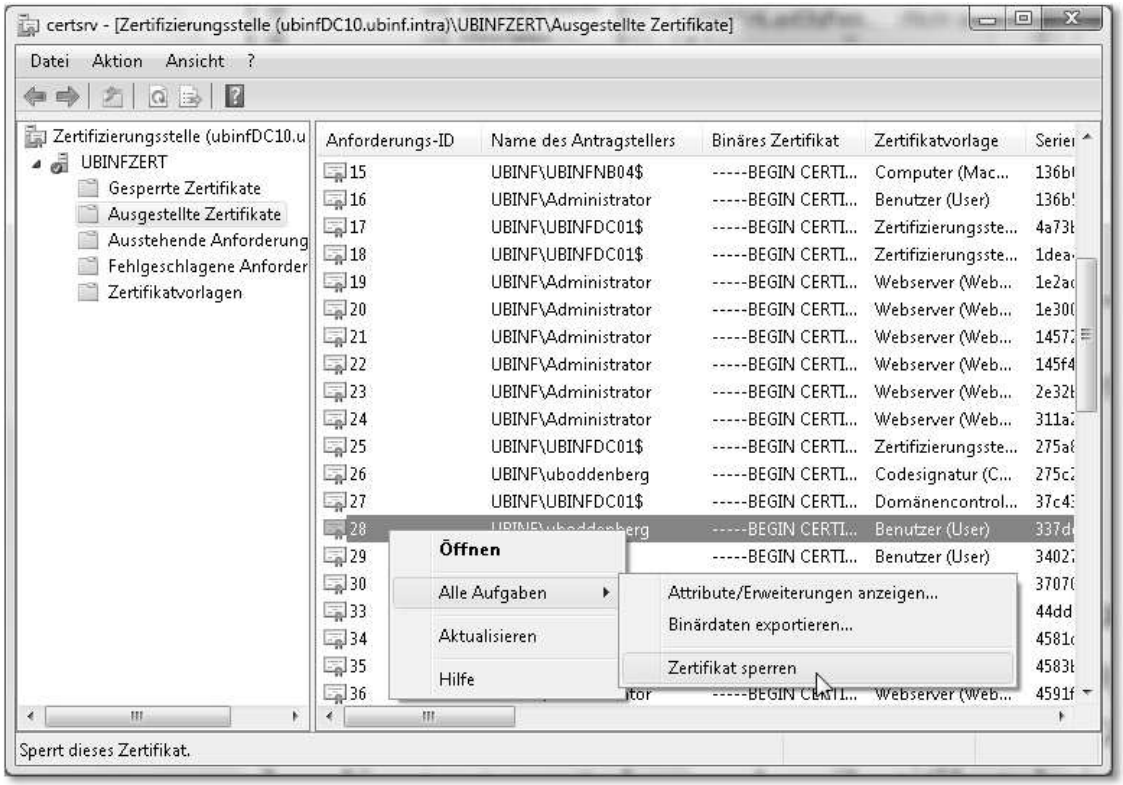


Abbildung 5.54 Ausgestellte Zertifikate werden im Konfigurationswerkzeug für die Zertifizierungsstelle angezeigt.

5.8.4 Zertifizierungspfad

In den Eigenschaften des Zertifikats findet sich die Karteikarte Zertifizierungspfad. Einen einfachen Zertifizierungspfad zeigt Abbildung 5.55. Sie sehen ein Personenzertifikat, das von einer Stammzertifizierungsstelle ausgestellt worden ist. Bei mehrstufigen PKI-Architekturen sind in diesem Dialog auch alle Zwischenzertifizierungsstellen zu sehen, die zwischen Stammzertifizierungsstelle und Zertifikat liegen.

Abbildung 5.55 Im Eigenschaftendialog wird der Zertifizierungspfad angezeigt.

5.8.5 Zertifikatsvorlagen

Sie haben bereits erfahren, dass es viele unterschiedliche Zertifikatstypen gibt, beispielsweise solche für Computer, für Benutzer und vieles andere mehr. Das »wirkliche« Unterscheidungsmerkmal der Zertifikate sind die Verwendungszwecke des Zertifikats, beispielsweise:

- Clientauthentifizierung
- Serverauthentifizierung
- E-Mail-Verschlüsselung und -Signierung
- Verschlüsselndes Dateisystem
- Codesignatur

Wie Sie in Abbildung 5.56 erkennen können, sind in der Zertifikatsverwaltung verschiedene Zertifikatsvorlagen vorhanden. Die genauen Verwendungszwecke sind aus dem Eigenschaftendialog der jeweiligen Zertifikatsvorlage ersichtlich.

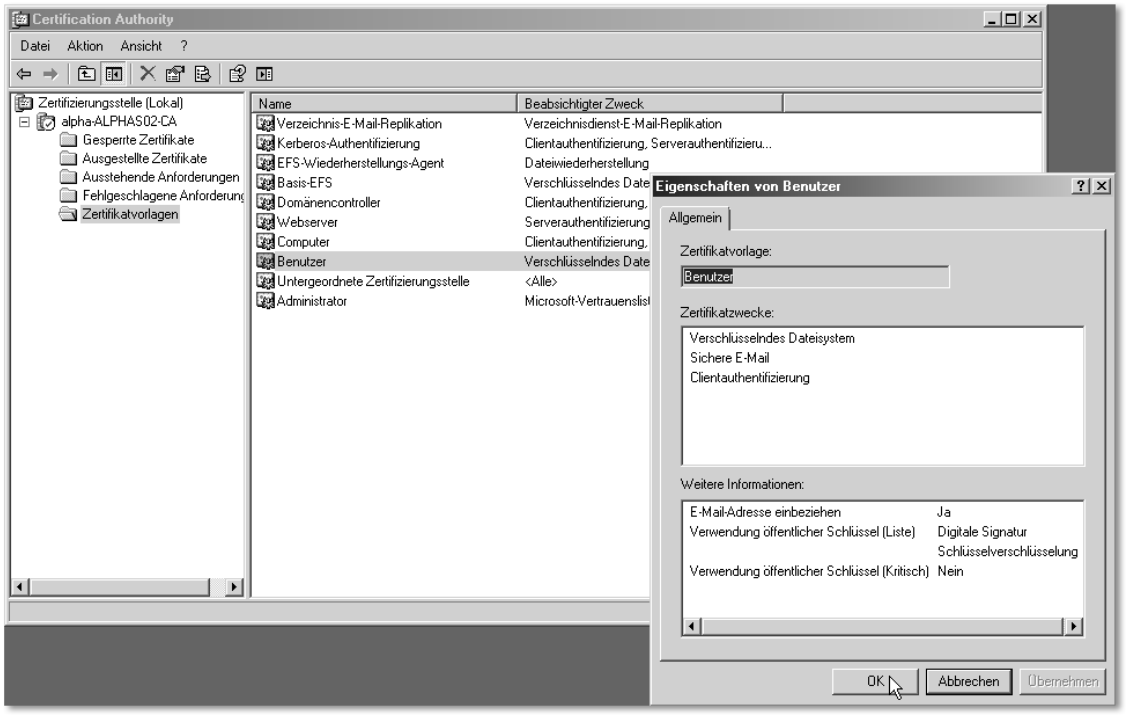


Abbildung 5.56 Zertifikate, die auf einer dieser Zertifikatsvorlagen basieren, können Sie bei dieser Zertifizierungsstelle erhalten.

Festzustellen ist, dass jedes Zertifikat, das von einer Zertifizierungsstelle ausgestellt wird, auf einer Zertifikatsvorlage basieren muss. Um also Zertifikate zu erzeugen, die für eine bestimmte Kombination von Verwendungszwecken vorgesehen sind, müssen Sie eine entsprechende Zertifikatsvorlage erstellen. In diesem Abschnitt führe ich Ihnen vor, wie eine Zertifikatsvorlage für Benutzer erstellt wird, deren Zertifikate nur für CLIENTAUTHENTIFIZIERUNG und SICHERE E-MAIL, nicht aber für das verschlüsselnde Dateisystem verwendet werden können.

Der erste Schritt ist das Aufrufen des Verwaltungswerkzeugs für die Zertifikatsvorlagen. Hierzu gibt es zwei Möglichkeiten:

- In der Verwaltung der Zertifizierungsstelle können Sie im Kontextmenü des Eintrags ZERTIFIKATVORLAGEN die Verwaltung derselben aufrufen (Abbildung 5.57).
- Alternativ können Sie das Snap-In ZERTIFIKATVORLAGEN direkt der MMC hinzufügen.

In dem Snap-In zur Verwaltung der Zertifikatsvorlagen sind deutlich mehr Vorlagen zu sehen als in dem entsprechenden Knoten der Verwaltung der Zertifizierungsstelle. Mit anderen Worten: Nicht alle vorhandenen Zertifikatsvorlagen sind auch direkt für die Zertifizierungsstelle aktiv.

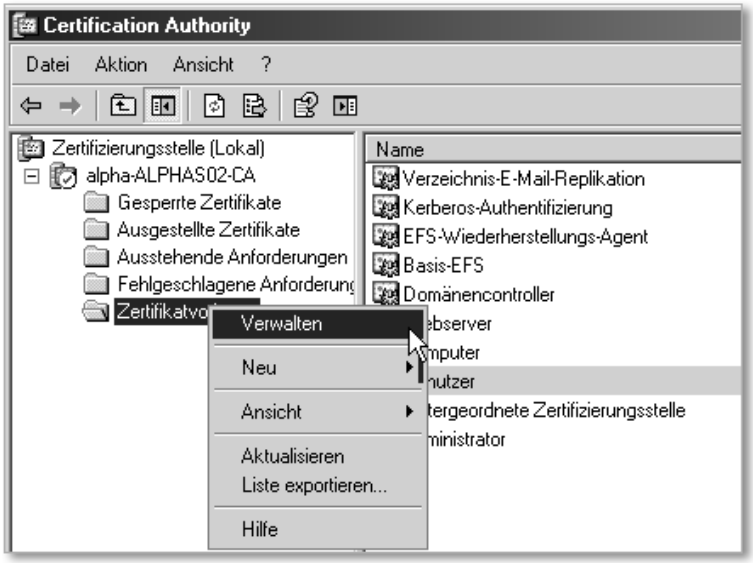


Abbildung 5.57 Um alle Zertifikatsvorlagen zu verwalten, wählen Sie einfach die entsprechende Funktion im Kontextmenü.

Man kann einerseits die vorhandenen und noch nicht von der Zertifizierungsstelle verwendeten Vorlagen aktivieren. Darüber hinaus können auch eigene Zertifikatsvorlagen mit einer individuellen Kombination von Verwendungszwecken eingerichtet werden.

In diesem Beispiel soll eine neue Benutzer-Zertifikatsvorlage erstellt werden, die im Gegensatz zur Standardvorlage nicht für die Verwendung des verschlüsselnden Dateisystems vorgesehen ist. Der erste Schritt hierzu ist in Abbildung 5.58 gezeigt: Sie wählen die »ähnlichste« Vorlage aus (in diesem Fall BENUTZER) und rufen in deren Kontextmenü die Funktion DOPPELTE VORLAGE auf. Was dieser Befehl macht, ist leicht zu erraten – es wird eine Kopie der Zertifikatsvorlage angelegt. Aus dieser Kopie wird dann die neue Zertifikatsvorlage erstellt.

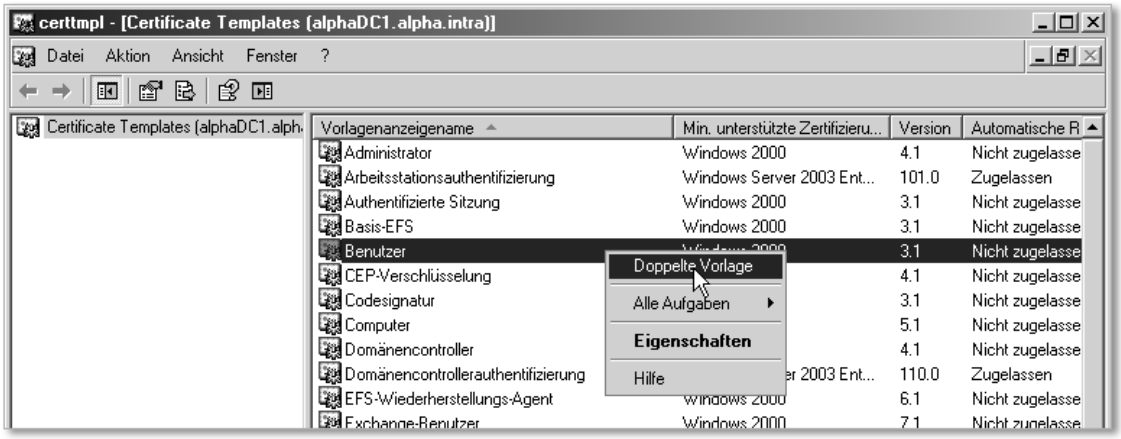


Abbildung 5.58 Am einfachsten erstellen Sie eine neue Vorlage, indem Sie eine bestehende duplizieren.

Beim Erstellen der Kopie der Zertifikatsvorlage werden Sie gefragt werden, auf welcher Version der Stammzertifizierungsstelle die neue Zertifikatsvorlage basieren soll. Zur Auswahl stehen die Optionen Windows Server 2003 Enterprise Edition und Windows Server 2008, Enterprise Edition (Abbildung 5.59).

Abbildung 5.59 Hier legen Sie fest, auf welchem Betriebssystem die Zertifizierungsstelle mindestens laufen muss.

Nur Enterprise Edition

Der Dialog aus Abbildung 5.59 lässt es schon erkennen, trotzdem sei nochmals ganz deutlich darauf hingewiesen, dass eine Zertifizierungsstelle, die »eigene« Vorlagen unterstützt, auf der Enterprise Edition des Betriebssystems Windows Server 2008 ausgeführt werden muss.

Sofern Sie eine Vorlage konfigurieren, die eine Windows-Server-2008-Zertifizierungsstelle voraussetzt, gibt es einige zusätzliche Einstellmöglichkeiten, beispielsweise zur Kryptografie (welcher Cryptography Service Provider soll verwendet werden etc.).

Als Nächstes rufen Sie den Eigenschaftendialog der neuen Zertifikatsvorlage auf und nehmen die notwendigen Konfigurationsänderungen vor (Abbildung 5.60). Ich werde nicht jede einzelne Option beschreiben; die meisten Einstellungen sind selbsterklärend.

Zunächst zur Registerkarte Allgemein: Hier können Sie den Vorlagennamen und den Vorlagenanzeigenamen wählen, was kaum spektakulär ist. Im Normalfall werden Sie die Zertifikatsvorlage im Active Directory veröffentlichen, was zur Folge hat, dass AD-Clients die Vorlage beim Anfordern eines neuen Zertifikats in der Auswahlliste sehen.

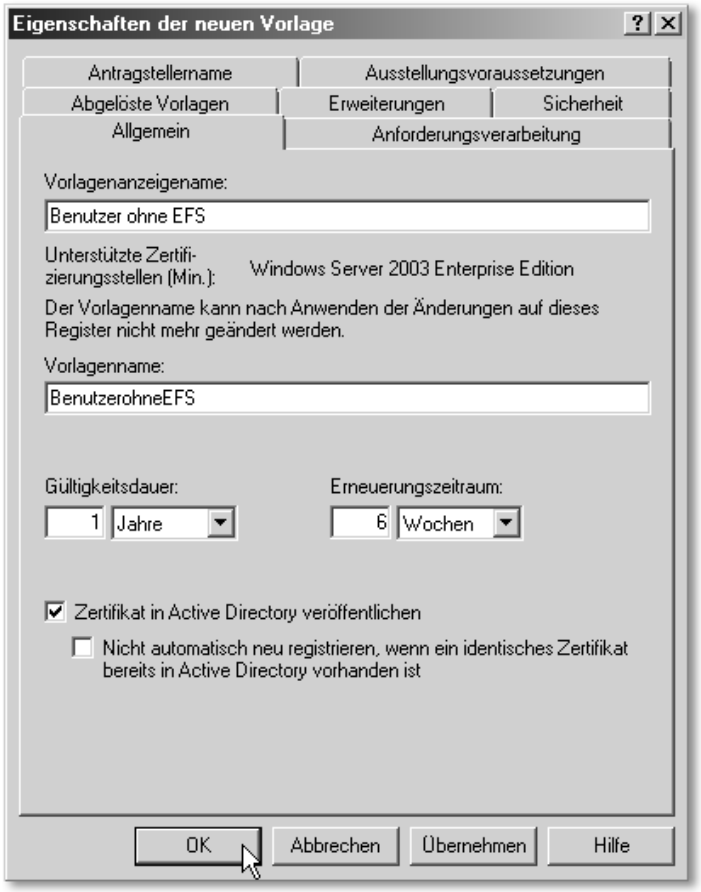


Abbildung 5.60 Konfiguration der neuen Zertifikatsvorlage

Wichtig ist natürlich auch der Gültigkeitszeitraum, der je nach Verwendungszweck konfiguriert werden kann und soll. Bei einem Benutzerzertifikat ist ein Jahr ein durchaus sinnvoller Wert. Aus Gründen der Sicherheit sollte er nicht zu lang sein – aber auch nicht zu kurz, damit Sie nicht ständig das Zertifikat erneuern müssen.

Besonders hinweisen möchte ich Sie auf den Eintrag UNTERSTÜTZTE ZERTIFIZIERUNGSSTELLEN (MIN.), den Sie nicht verändern können. Ein dupliziertes Zertifikat erfordert immer, dass die ausstellende Zertifizierungsstelle auf einem Enterprise-Edition-Server läuft. Das hat nicht unbedingt einen technischen Grund, sondern ist eine zu beachtende Lizenzbestimmung, die Sie bei der Planung unbedingt berücksichtigen müssen.

Sofern die Zertifizierungsstelle in das Active Directory integriert ist (Enterprise CA) und die Zertifikatsvorlage im AD veröffentlicht wird, sieht es im Active Directory so aus, wie auf Abbildung 5.61 gezeigt:

- Die Zertifizierungsstelle ist im Konfigurationsnamenskontext verzeichnet.
- In den Eigenschaften der Zertifizierungsstelle, genauer gesagt im Attribut CERTIFICATETEMPLATES, sind die verwendeten Zertifikatsvorlagen aufgeführt.

- Details zu den einzelnen Zertifikatsvorlagen können, sofern sie im AD veröffentlicht werden, ebenfalls im Konfigurationsnamenskontext ermittelt werden. Unter CONFIGURATION • SERVICES • PUBLIC KEY SERVICES • CERTIFICATE TEMPLATES sind Informationen zu dieser Zertifikatsvorlage gespeichert.

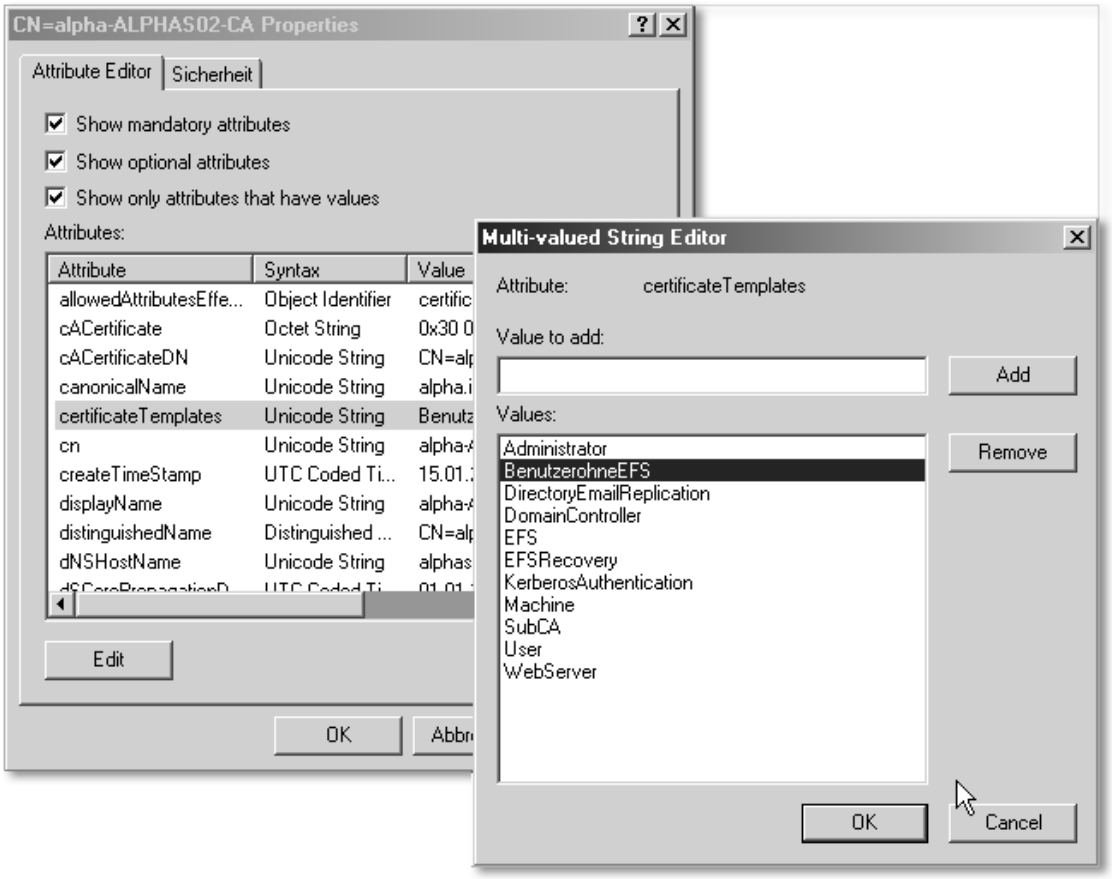


Abbildung 5.61 Ein Blick ins Active Directory mit ADSI-Editor. Die neue Zertifikatsvorlage ist in der Eigenschaft »certificateTemplates« der Zertifizierungsstelle verzeichnet.

Ich zeige Ihnen die Beispiele mit ADSI-Editor übrigens nicht etwa deshalb, weil ich Sie animieren möchte, mit diesem Werkzeug im AD »herzumzuadministrieren«, sondern um Ihnen zu helfen, die Hintergründe zu verstehen. Um im Problemfall schnell die richtigen Schlüsse zu ziehen, ist es einfach wichtig, ein wenig die Hintergründe zu kennen.

Nun müssen Sie noch konfigurieren, für welche Zwecke dieses Zertifikat verwendet werden soll. Dies erledigen Sie auf der Karteikarte ERWEITERUNGEN, indem Sie die ANWENDUNGSRICHTLINIEN bearbeiten (Abbildung 5.62).

In dem hier vorgeführten Beispiel sollen die mittels dieser Vorlage ausgestellten Zertifikate nicht für das verschlüsselnde Dateisystem verwendet werden; demzufolge wird der entsprechende Eintrag gelöscht. Genauso können weitere Verwendungszwecke hinzugefügt werden.

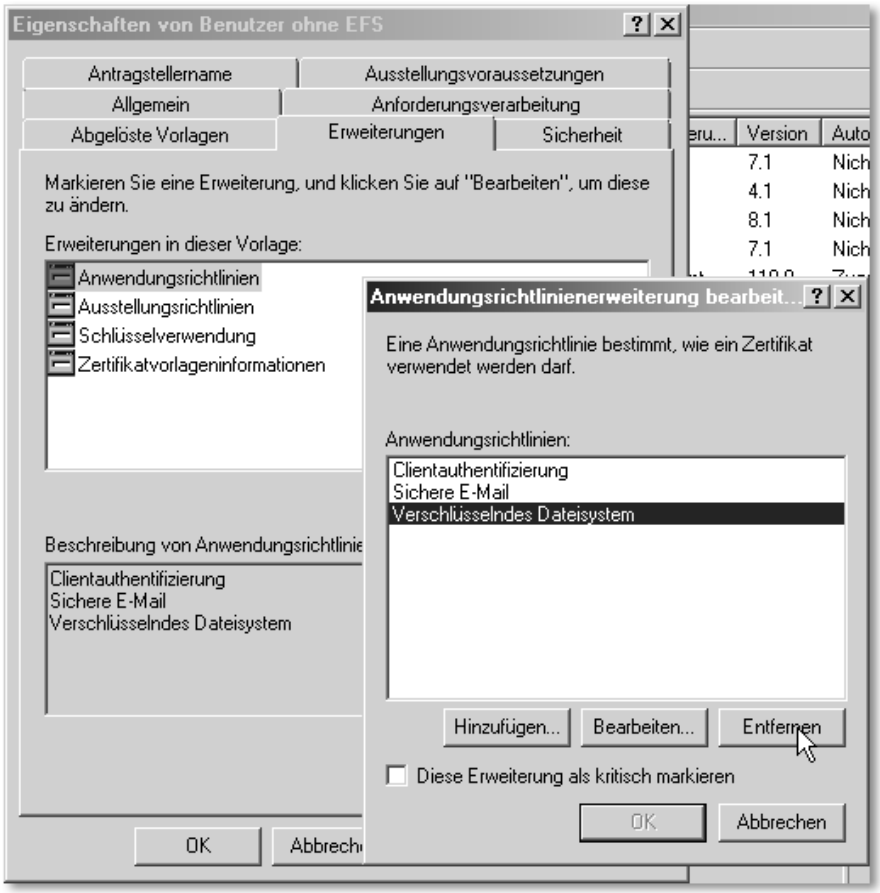


Abbildung 5.62 So wird die Anwendungsrichtlinie der neuen Vorlage konfiguriert.

Etliche weitere Konfigurationsmöglichkeiten stehen zur Verfügung, werden an dieser Stelle aber nicht weiter besprochen. Ist die Konfiguration der neuen Zertifikatsvorlage abgeschlossen, wird diese in der Liste der Vorlagen aufgeführt werden (Abbildung 5.63). Wie erwartet wird als notwendige Zertifizierungsstelle ein Enterprise-Edition-Server angegeben.

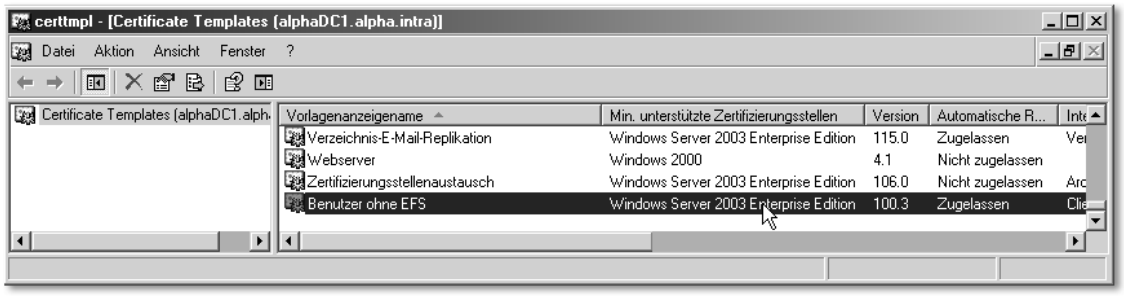


Abbildung 5.63 Die neue Zertifikatsvorlage benötigt einen Enterprise-Edition-Server.

Da nun die Zertifikatsvorlage konfiguriert ist, kommen wir zum letzten Schritt, nämlich zum Hinzufügen der neuen Zertifikatsvorlage als auszustellende Zertifikatsvorlage. Hierzu wählen Sie im Kontextmenü des Knotens ZERTIFIKATVORLAGE

in dem Snap-In Zertifizierungsstelle die Funktion Neu • Auszustellende Zertifikatvorlage. Es wird ein Dialog erscheinen, der die installierten Zertifikatsvorlagen anzeigt; durch Auswahl von OK können Sie die selektierte Vorlage hinzufügen (Abbildung 5.64).

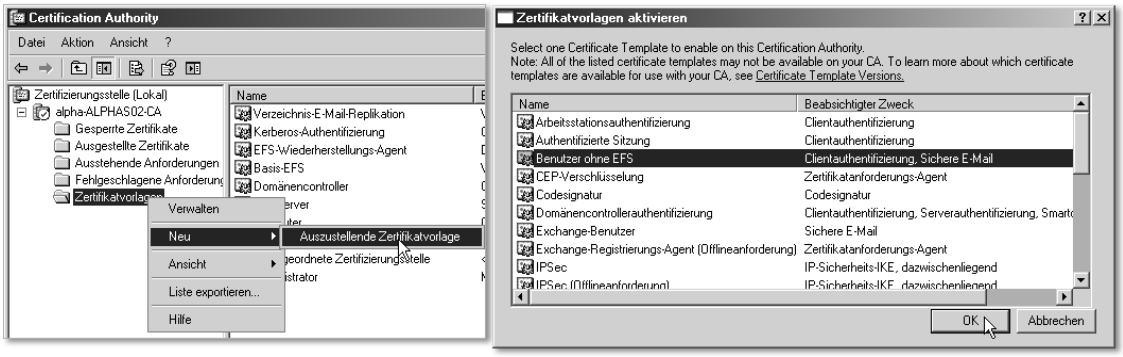


Abbildung 5.64 Die neue Zertifikatsvorlage wird zu den auszustellenden Zertifikatsvorlagen hinzugefügt.

Wenn ein Benutzer mittels des Snap-Ins Zertifikate auf seinem PC/Notebook ein Zertifikat anfordern will, wird ihm die neue Vorlage ebenfalls in der Auswahlliste angezeigt werden (Abbildung 5.65).

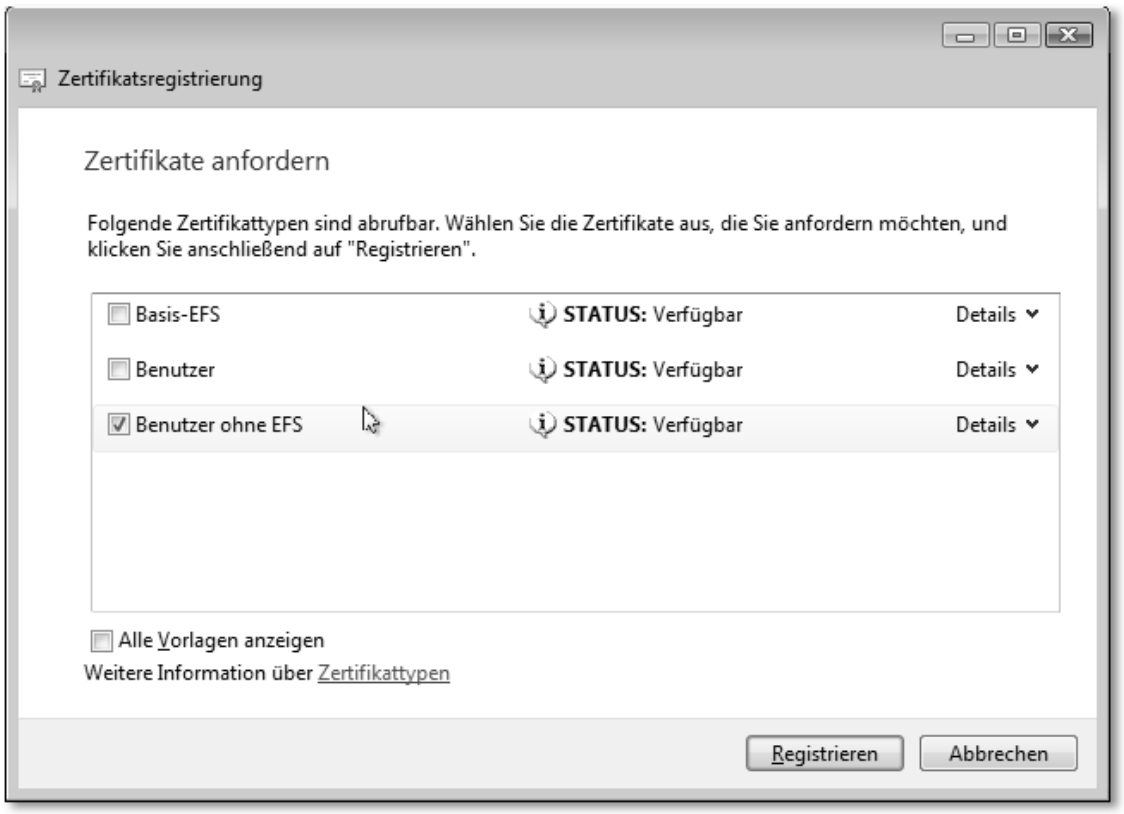


Abbildung 5.65 Ein auf der neuen Zertifikatsvorlage basierendes Zertifikat kann nun vom Benutzer angefordert werden.

Welche Zertifikatsvorlagen einem Benutzer tatsächlich angezeigt werden, hängt davon ab, welche Berechtigungen in der Zertifikatsvorlage gesetzt worden sind. Angezeigt werden nur diejenigen Vorlagen, bei denen der Benutzer das Recht »Registrieren« hat. Die Berechtigungen können im Eigenschaftendialog der Zertifikatsvorlage auf der Karteikarte SICHERHEIT eingestellt werden.

Zum Schluss möchte ich Ihnen zeigen, dass das Zertifikat tatsächlich gemäß den Einstellungen in der Zertifikatsvorlage erstellt worden ist (Abbildung 5.66):

- Als Verwendungszwecke sind nur *Clientauthentifizierung* (GARANTIERT DEM REMOTECOMPUTER…) und *Sichere E-Mail* (SCHÜTZT E-MAIL-NACHRICHTEN) vorhanden. Der Verwendungszweck *Verschlüsselndes Dateisystem*, der bei der Originalvorlage vorhanden ist, fehlt.
- Das Gültigkeitsdatum ist auf ein Jahr beschränkt.

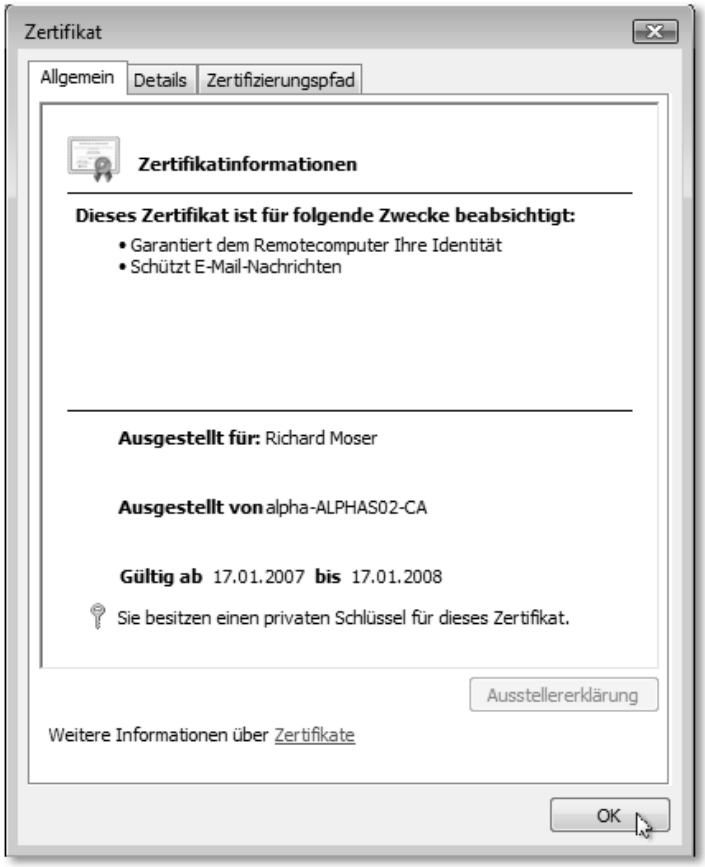


Abbildung 5.66 Ein auf der neuen Vorlage basierendes Zertifikat

5.8.6 Weboberfläche

Zertifikate können alternativ auch über eine Weboberfläche angefordert werden. Diese muss allerdings zunächst installiert werden. Falls Sie dies nicht ohnehin bereits bei der Installation der eigentlichen Zertifizierungsstelle erledigt haben,

müssen Sie die Weboberfläche nachinstallieren. Der genaue Name dieser Komponente lautet ZERTIFIZIERUNGSSTELLEN-WEBREGISTRIERUNG. Sind die benötigten Komponenten installiert, müsste sich im Server-Manager ein Bild wie in Abbildung 5.67 ergeben.

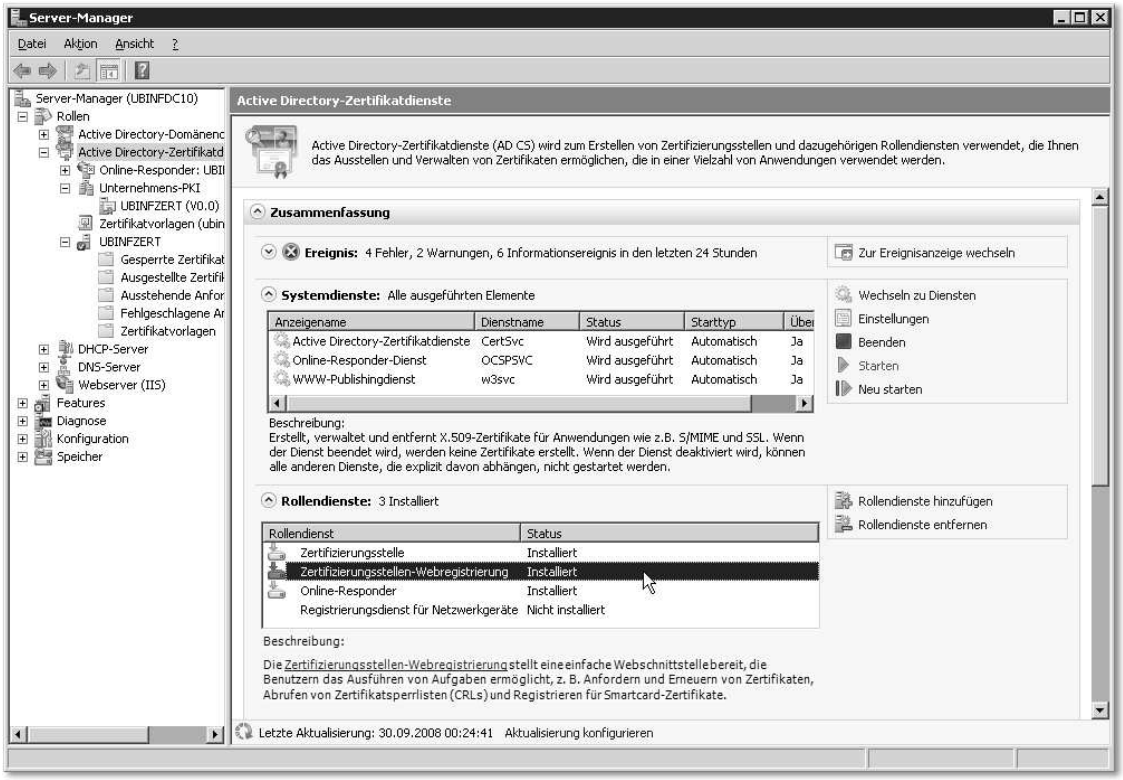


Abbildung 5.67 Um weitere Komponenten der Active Directory-Zertifikatsdienste zu installieren, können Sie den Server-Manager verwenden – hier ist aber bereits alles vorhanden.

Ist das Webfrontend installiert, können Benutzer durch Eingabe der URL *servername.domain.ext/certsrv* die Webapplikation zur Anforderung von Zertifikaten aufrufen (Abbildung 5.68). Neben dem Anfordern eines neuen Zertifikats können weitere Funktionen aufgerufen werden: So können Benutzer den Status ausstehender Zertifikate anzeigen. Das ist interessant, wenn die Zertifizierungsstelle die Zertifikatsanforderungen nicht direkt bearbeitet, sondern ein Administrator von Hand die Ausstellung von Zertifikaten genehmigt oder ablehnt. Weiterhin können das Zertifikat der Zertifizierungsstelle, die Sperrliste und einiges andere mehr in unterschiedlichen Formaten heruntergeladen werden.

Die Weboberfläche dürfte beispielsweise in Szenarien interessant sein, in denen nicht nur Windows-PCs, die Domänenmitglied sind, in einer Umgebung vorhanden sind, sondern auch Unix-Systeme, auf denen ebenfalls Zertifikate installiert werden müssen. Für diese können Sie mittels der Weboberfläche recht einfach die benötigten Zertifikate beziehen.

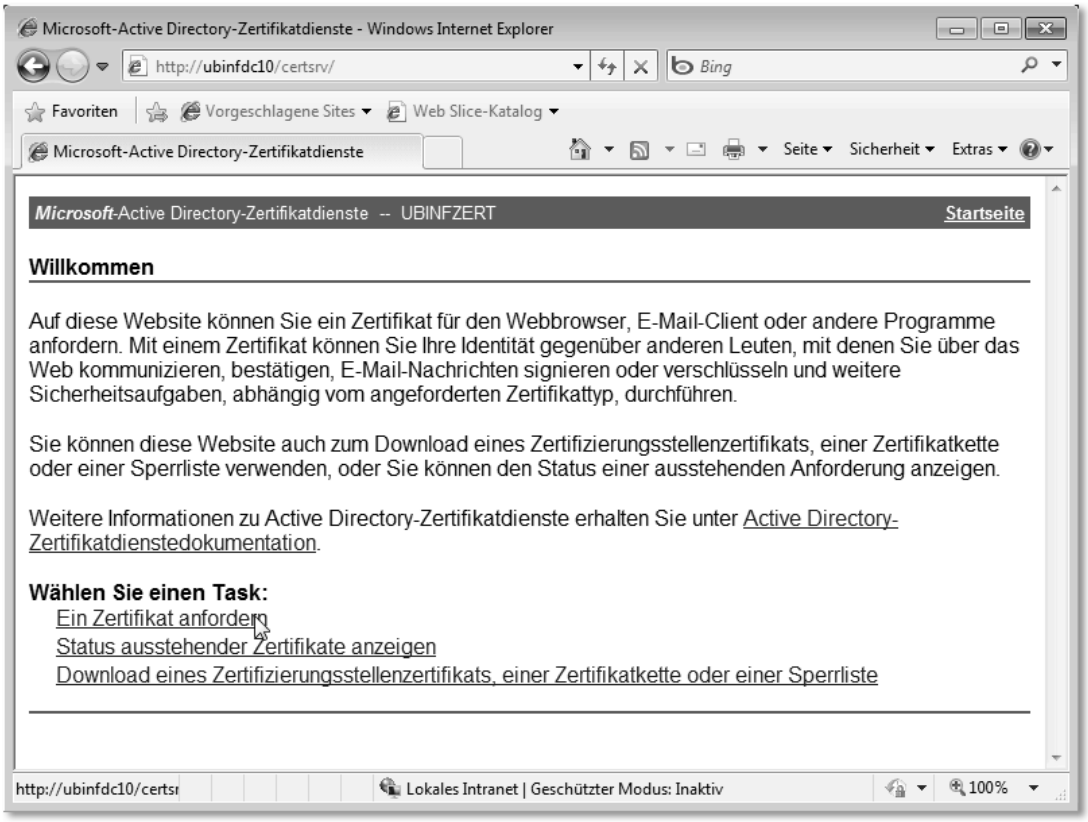


Abbildung 5.68 Die Startseite des Webinterfaces

Entscheidet man sich für das Anfordern eines neuen Zertifikats, möchte die Webanwendung wissen, ob ein BENUTZERZERTIFIKAT angefordert werden soll oder eine ERWEITERTE ZERTIFIKATSANFORDERUNG eingereicht wird (Abbildung 5.69). Der erste Fall ist aus Sicht eines Administrators eher unspektakulär – es wird eben ein Benutzerzertifikat angefordert und erstellt.

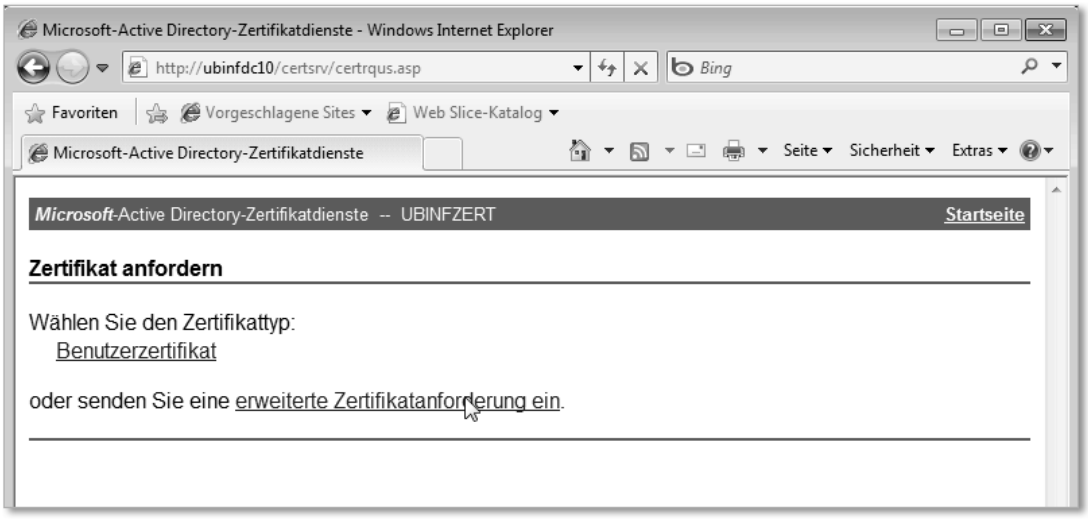


Abbildung 5.69 An dieser Stelle kann ein »Benutzerzertifikat« angefordert oder eine »erweiterte Zertifikatsanforderung« eingereicht werden.

Der Dialog für die Erweiterte Zertifikatanforderung ist in Abbildung 5.70 zu sehen. Hier können Sie die zu verwendende Zertifikatvorlage nebst einigen weiteren Parametern definieren. Der Benutzer, der auf der Abbildung beim Anfordern des Zertifikats eingeloggt war, war Mitglied der Domänenadministratoren-Gruppe. Ein »normaler« Benutzer kann natürlich keine Zertifikate für solche Zwecke wie Untergeordnete Zertifizierungsstelle anfordern.

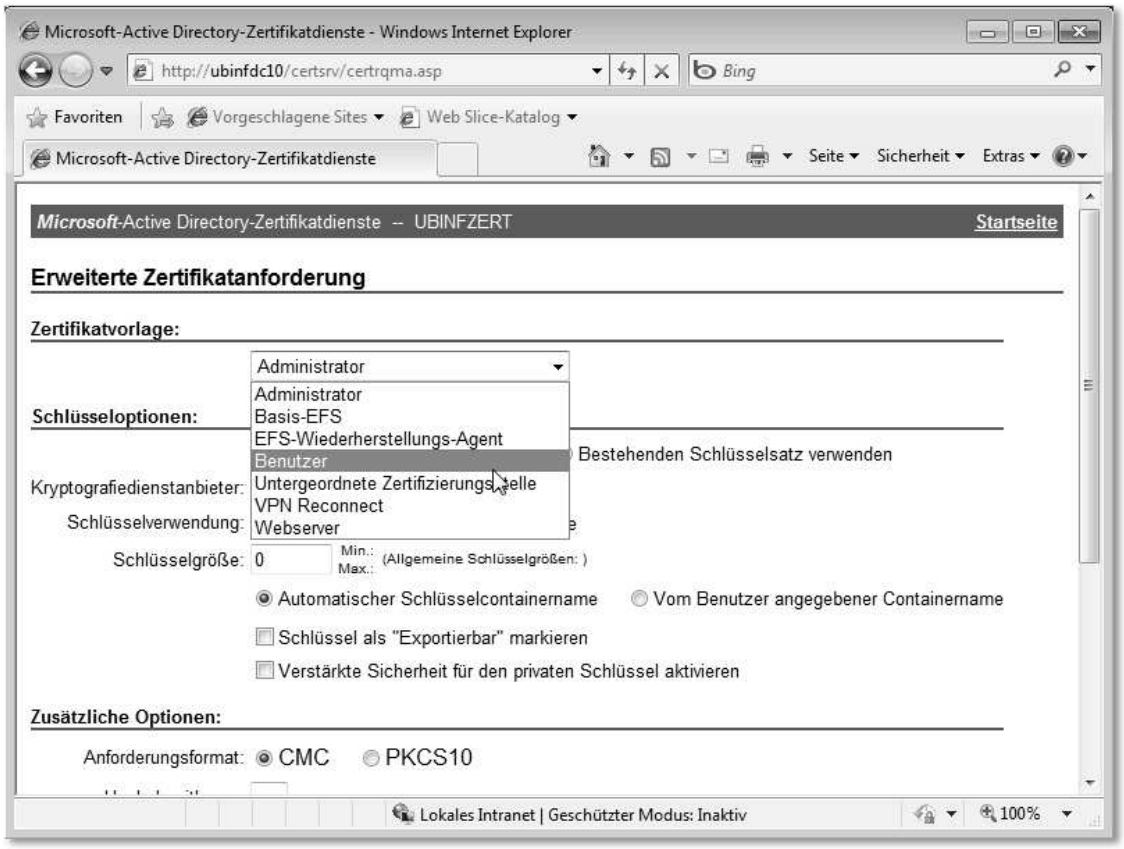


Abbildung 5.70 Im Dialog »Erweiterte Zertifikatanforderung« des Webinterface können Sie den Zertifikatstyp nebst einiger Parameter wählen.

5.8.7 Mehrstufige Architekturen

In dem bisher gezeigten Szenario kommt nur eine einzige Zertifizierungsstelle zum Einsatz, die gleichzeitig die Funktion der Stammzertifizierungsstelle (*Root CA*) und der ausstellenden Zertifizierungsstelle (*Issuing CA*) übernimmt. Das funktioniert zwar, ist aber, zumindest für eine größere Organisation, nicht die empfohlene Konfiguration. Der Grund ist vor allem die extreme Schutzbedürftigkeit des privaten Schlüssels der Stammzertifizierungsstelle.

Aus diesem Grund wird man, zumindest in einer größeren Umgebung, ein mehrstufiges Zertifikatswesen aufbauen. Man kennt ein-, zwei-, drei- und vierstufige Architekturen.

- In kleinen Umgebungen wird man, insbesondere aus Kostengründen, eine einstufige PKI-Infrastruktur aufbauen.
- In mittleren Umgebungen bietet sich eine zweistufige PKI-Infrastruktur an. In einer solchen Infrastruktur existieren eine Stammzertifizierungsstelle und eine oder mehrere untergeordnete Zertifizierungsstellen. Das Ausstellen der Zertifikate wird ausschließlich von den untergeordeneten Zertifizierungsstellen übernommen. Die Stammzertifizierungsstelle ist im Optimalfall gar nicht mit dem Netzwerk verbunden.
- In großen Umgebungen kann noch eine zusätzliche Schicht eingezogen werden. Die zusätzlichen Zertifizierungsstellen werden *Intermediate CA* genannt. Eine solche Vorgehensweise bietet sich beispielsweise an, um für die Europa- und die Asien-Organisation separat administrierbare große PKI-Infrastrukturen aufzubauen, die aber sozusagen ein gemeinsames »Erbe«, also eine gemeinsame Stammzertifizierungsstelle haben.
- Wenn auch eine dreistufige Architektur nicht reicht, kann eine weitere Schicht unterhalb der obersten Zertifizierungsstelle eingezogen werden. Diese Zertifizierungsstellen werden *Subordinate CA* genannt. Da nur die wenigsten Leser eine vierstufige PKI-Architektur implementieren werden, wird diese hier nicht weiter besprochen.

Die unterschiedlichen Rollen, die eine Zertifizierungsstelle einnehmen kann, unterscheiden sich in der technischen Umsetzung.

Rollen

Im Folgenden werden stichwortartig die unterschiedlichen Rollen beschrieben, die eine Zertifizierungsstelle einnehmen kann.

Stammzertifizierungsstelle (Root CA)

Die oberste Stammzertifizierungsstelle hat das Stammzertifikat der ganzen PKI-Struktur ausgestellt. Dieses ist, wie bereits erwähnt, extrem schutzbedürftig. Würde es einer fremden und/oder bösartigen Person in die Hände fallen, ist Ihre komplette PKI wertlos, da die Person beliebige Zertifikate ausstellen kann, die bei einer kryptografischen Prüfung als gültig erkannt werden.

Aus diesem Grund wird diese Stammzertifizierungsstelle in einer zweistufigen (und höher) Architektur im günstigsten Fall als Offline-CA angelegt. Das bedeutet:

- Dieser Server ist kein Domänenmitglied.
- Demzufolge wird die Zertifizierungsstelle nicht als Enterprise-, sondern als Standalone-CA installiert. (Eine Enterprise-CA ist in das Active Directory integriert.)

- Dieser Server verfügt über keinen Netzwerkanschluss.
- Dieser Server muss physikalisch geschützt sein. (Denken Sie an die Folgen eines Diebstahls des ganzen Servers oder des Zertifikats.)
- Diese Zertifizierungsstelle stellt nur Zertifikate für die untergeordneten Zertifizierungsstellen aus. Diese Zertifikate werden dann auf einer Diskette oder einem USB-Stick transportiert.
- Die Gültigkeitsdauer des Zertifikats dieser Zertifizierungsstelle ist sehr lang, beispielsweise 10 oder 20 Jahre. Als Schlüssellänge kann man 4096 Bit wählen.

Intermediate CA

Die Intermediate CAs werden in einer dreistufigen Architektur verwendet. Es handelt sich um Zertifizierungsstellen mit erhöhtem Schutzbedarf, die nicht dazu gedacht sind, Zertifikate für andere Objekte als die untergeordneten Zertifizierungsstellen auszustellen. Die Intermediate CAs kommen insbesondere dann zum Einsatz, wenn in einer sehr großen Organisation in verschiedenen Bereichen Zertifikate mit unterschiedlichen Policys erstellt und separat administriert werden sollen. Ebenso können separate Zertifikatssperrlisten (CRL, Certificate Revocation List) erzeugt werden.

Für den Aufbau einer Intermediate CA gelten folgende Regeln:

- Dieser Server ist kein Domänenmitglied.
- Demzufolge wird die Zertifizierungsstelle nicht als Enterprise-, sondern als Standalone-CA installiert. (Eine Enterprise-CA ist in das Active Directory integriert.)
- Dieser Server verfügt im Optimalfall über keinen Netzwerkanschluss.
- Dieser Server muss physikalisch geschützt sein. (Denken Sie an die Folgen eines Diebstahls des ganzen Servers oder des Zertifikats.)
- Diese Zertifizierungsstelle stellt nur Zertifikate für die untergeordneten Zertifizierungsstellen aus. Diese Zertifikate werden dann auf einer Diskette oder einem USB-Stick transportiert.
- Die Gültigkeitsdauer des Zertifikats dieser Zertifizierungsstelle ist sehr lang, beispielsweise 10 oder 20 Jahre. Als Schlüssellänge kann man 2048 oder 4096 Bit wählen.

Sie sehen, dass der Anforderungskatalog von Stammzertifizierungsstellen (Root CA) und Intermediate CAs so gut wie identisch ist.

Issuing CA

Die Issuing CAs erstellen nun tatsächlich Zertifikate für Benutzer, Computer, Webserver, Codesignaturen und vieles andere mehr. Diese Zertifizierungsstellen haben einen Netzwerkanschluss, sind als Enterprise-CA in die Domäne integriert und kommunizieren mit anderen Systemen.

Hier einige Stichpunkte zum Aufbau einer Issuing CA:

- Dieser Server ist ein Domänenmitglied.
- Die Zertifizierungsstelle wird als Enterprise-CA (Unternehmenszertifizierungsstelle) installiert.
- Dieser Server verfügt über einen Netzwerkanschluss und kommuniziert mit anderen Systemen.
- Die Installation muss mit besonderer Sorgfalt erfolgen, um keine »Hintertüren« zum unbefugten Zugriff auf diesen Server zu ermöglichen.
- Dieser Server muss physikalisch geschützt sein. (Denken Sie an die Folgen eines Diebstahls des ganzen Servers oder des Zertifikats.)
- Diese Zertifizierungsstelle stellt Zertifikate für Benutzer, Computer, Codesignaturen und vieles andere aus.
- Die Gültigkeitsdauer des Zertifikats dieser Zertifizierungsstelle ist weniger lang als bei einer Root- oder Intermediate CA. Ein guter Wert sind fünf Jahre. Als Schlüssellänge kann man 2048 Bit wählen.
- Diese Zertifizierungsstellen sollten auf einem Betriebssystem der Enterprise-Edition installiert werden, um alle Zertifikatsvorlagen verwenden zu können.

Architekturen

In Abbildung 5.71, Abbildung 5.72 und Abbildung 5.73 sehen Sie zwei- und dreistufige PKI-Infrastrukturen in unterschiedlichen Ausprägungen.

Abbildung 5.71 zeigt den einfachsten Fall einer zweistufigen PKI-Infrastruktur. Sie besteht aus einer Stammzertifizierungsstelle (Root CA) und einer Zertifizierungsstelle, die Zertifikate für Benutzer und Computer erstellt (Issuing CA). Wie ich zuvor beschrieben habe, wird die Root CA möglichst als Offline-System ohne Netzwerkanschluss realisiert. Diese Architektur dürfte für die meisten mittelständischen Unternehmen geeignet sein.

Die zweistufige Architektur bietet die Möglichkeit, eine beliebige Anzahl von Issuing CAs einzurichten (Abbildung 5.72). Dies könnte beispielsweise interessant sein, wenn die Organisation sehr groß und verteilt und nur durch sehr schmalbandige Weitverkehrsverbindungen verbunden ist. Eine Issuing CA könnte beispielsweise in Europa, eine andere in Asien stehen.

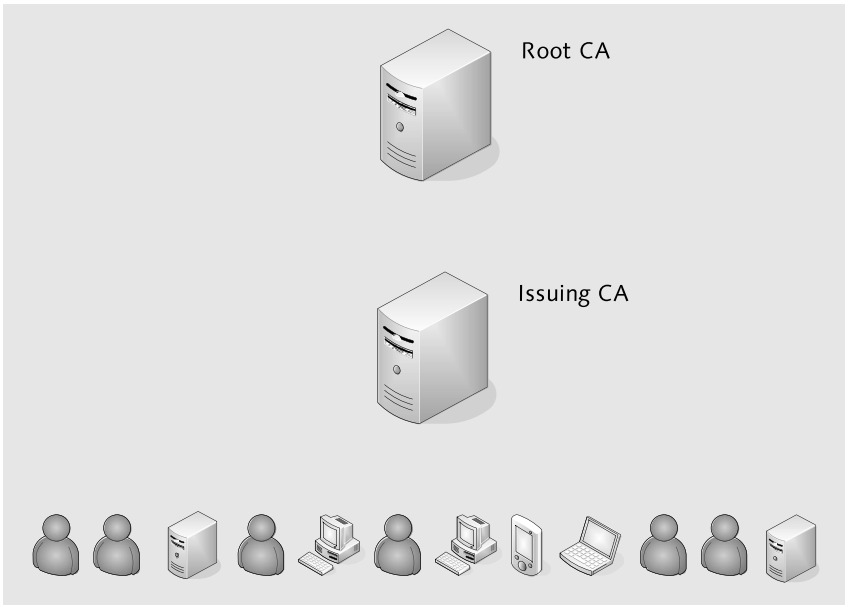


Abbildung 5.71 Die einfachste Möglichkeit einer zweistufigen PKI-Infrastruktur

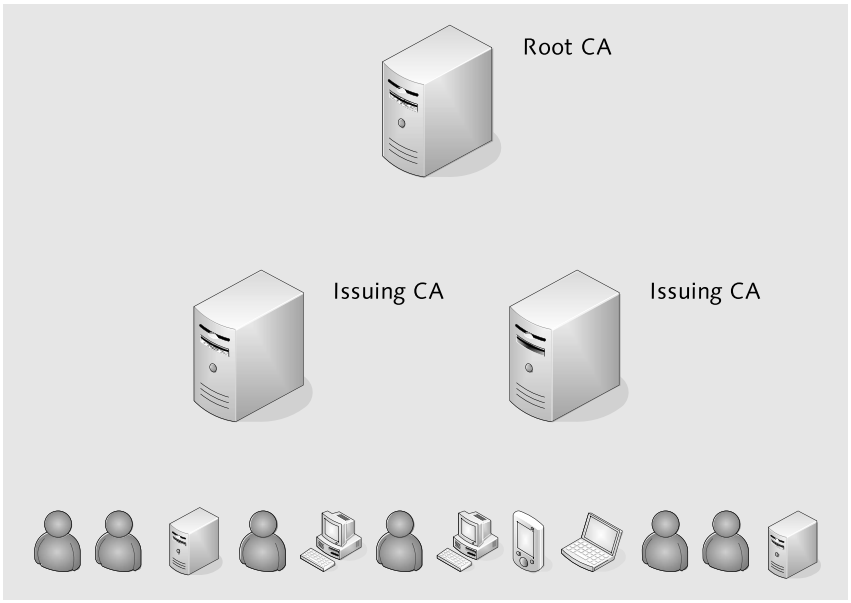


Abbildung 5.72 Eine zweistufige PKI-Infrastruktur

Die nächste Ausbaustufe ist die Verwendung von Intermediate CAs, die ihrerseits Zertifikate für die Issuing CAs erstellen (Abbildung 5.73). Diese PKI-Architektur bietet die Möglichkeit, mit separaten Policys und separaten Zertifikatssperrlisten zu arbeiten. Unter einer Intermediate CA können jeweils beliebig viele Issuing CAs betrieben werden; oder technisch korrekter: Eine Intermediate CA kann für beliebig viele Issuing CAs Zertifikate erzeugen.

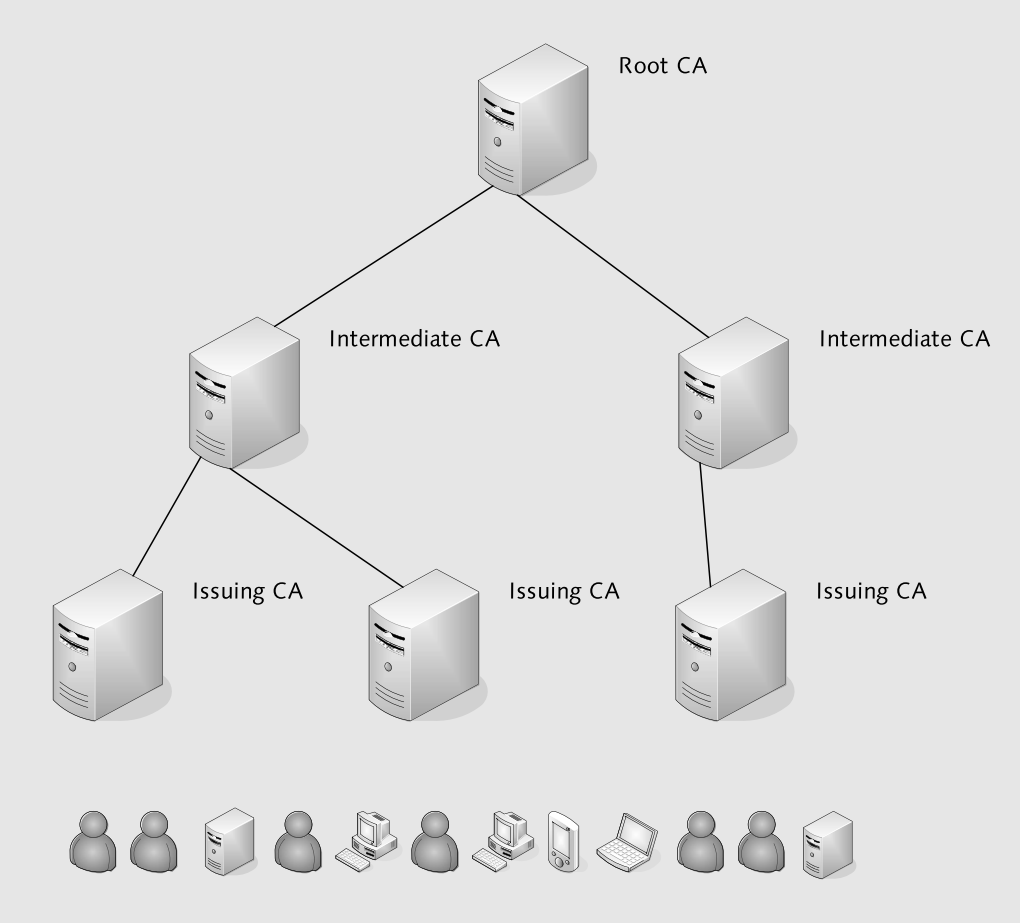


Abbildung 5.73 Eine dreistufige PKI-Infrastruktur

Obgleich die PKI-Architektur nun bereits recht komplex und weitverzweigt ist, lässt sich alles auf ein Zertifikat zurückführen, nämlich auf das Zertifikat der Stammzertifizierungsstelle.

5.9 VPNs mit Windows 7 und Windows Server 2008 R2

Wie bereits mehrfach erwähnt, gehört die Anbindung von Niederlassungen und mobilen Mitarbeitern zu den wichtigsten Funktionen, die eine moderne Unternehmens-IT gewährleisten muss.

Nun gibt es mit DirectAccess eine äußerst elegante Möglichkeit, mobile Computer einzubinden (siehe Abschnitt 13.2). Da DirectAccess aber verschiedene Voraussetzungen hat, die nicht immer erfüllbar sein werden, spielt das »normale« VPN weiterhin eine wichtige Rolle.

Windows 7 ist ein recht universeller VPN-Client. Es unterstützt folgende Tunneling-Protokolle:

- PPTP
- L2TP
- SSTP
- IKEv2

Die Tunneling-Protokolle sind als WAN-Miniport-Treiber installiert. Sie können das erkennen, wenn Sie im Geräte-Manager auch die ausgeblendeten Geräte anzeigen lassen (Abbildung 5.74).

Des Weiteren können natürlich VPN-Clients von Drittherstellern implementiert werden.

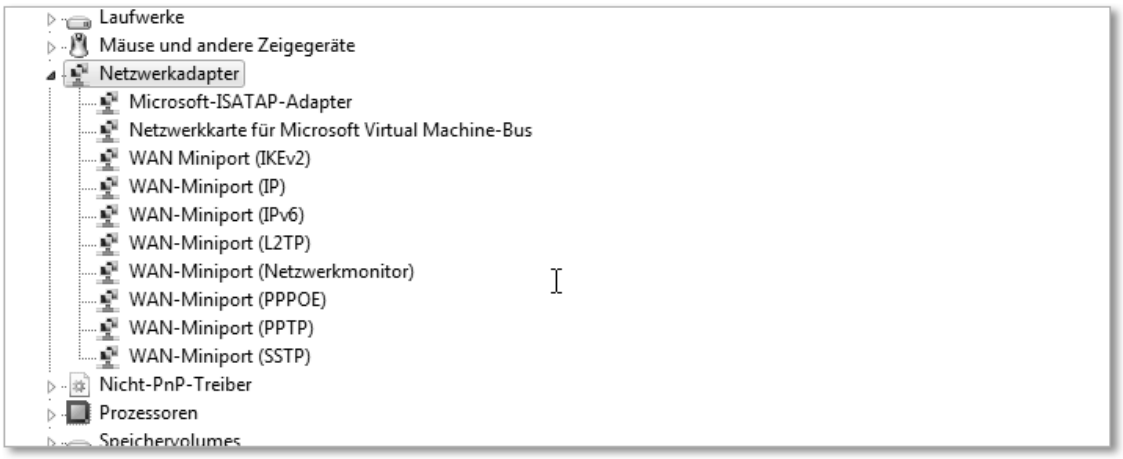


Abbildung 5.74 Es sind vier WAN-Miniport-Treiber für den Aufbau von VPN-Verbindungen vorhanden.

Ich möchte Ihnen nun zeigen, wie man mit Windows 7 Verbindungen mit den vier VPN-Typen aufbaut, und dabei ein wenig Hintergrundwissen vermitteln.

Bei dieser Gelegenheit möchte ich Ihnen auch die Fähigkeiten des Windows Server 2008 R2 als VPN-Server vorstellen. Microsofts Server ist ein recht flexibler und einfach zu handhabender VPN-Server. Er kann nahtlos durch recht anspruchsvolle Technologien wie *Network Access Protection* (siehe Abschnitt 12.3, »Netzwerkrichtlinien- und Zugriffsdienste«) ergänzt werden. Windows-Administratoren werden sich ohnehin freuen, dass sie sich in einer letztendlich bekannten und vollintegrierten Umgebung befinden.

Darüber hinaus ist diese Variante recht günstig in der Anschaffung, da Sie die Client-Zugriffslizenzen (CALs) ja vermutlich ohnehin beschafft haben werden.

5.9.1 Gateway-Architektur

Zunächst stellt sich die Frage, wie Sie den VPN-Server in Ihre Gateway-Architektur einpassen. Hier gibt es verschiedene Möglichkeiten. Insbesondere ist die Frage zu beantworten, ob die VPN-Benutzer direkt im Innenbereich des LANs landen sollen oder noch durch eine Firewall müssen:

- Wenn Sie sich dafür entscheiden, dass die VPN-Benutzer direkten Zugriff auf das LAN erhalten sollen, kommt ein Aufbau wie in Abbildung 5.75 gezeigt in Frage.
- Sofern der Innenbereich des Netzes mit einer Firewall von den VPN-Benutzern abgetrennt werden soll, könnte man wie auf Abbildung 5.76 gezeigt vorgehen. Dort werden das externe und interne LAN des VPN-Servers in zwei unterschiedlichen DMZs einer Firewall angeschlossen. Alternativ könnte man natürlich auch mit zwei Firewalls arbeiten.

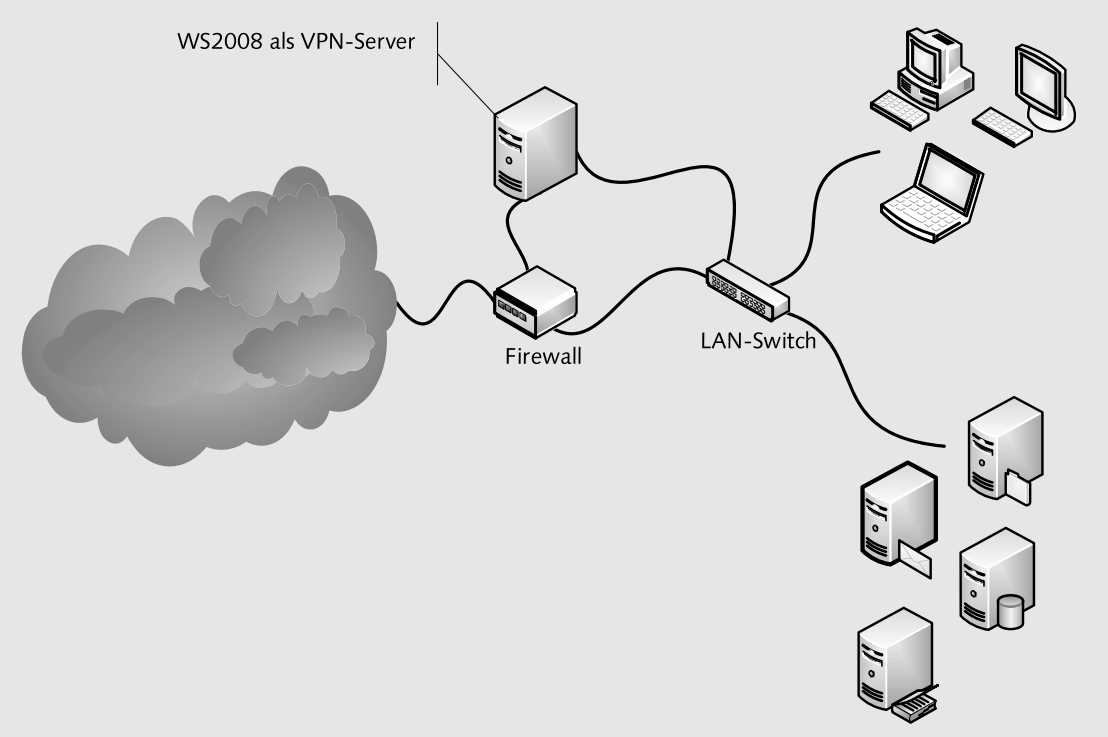


Abbildung 5.75 Möglicher Aufbau einer VPN-Umgebung

Die zweite Variante vermittelt eine irgendwie gefühlte höhere Sicherheit – das ist auch nicht von der Hand zu weisen. Ich möchte allerdings zu bedenken geben, dass ich etliche Unternehmen und Organisationen kenne, die zwar die in Abbildung 5.76 gezeigte Variante implementiert haben, die Firewall zwischen VPN-Server und dem Innenbereich dann aber vollständig geöffnet haben; Kommentar: »Ja, wieso? Uli, Du weißt doch, dass unsere VPN-Benutzer auf alles Zugriff haben sollen!« Das ist okay, dann kann man aber auch gleich das Szenario aus Abbildung 5.75 wählen.

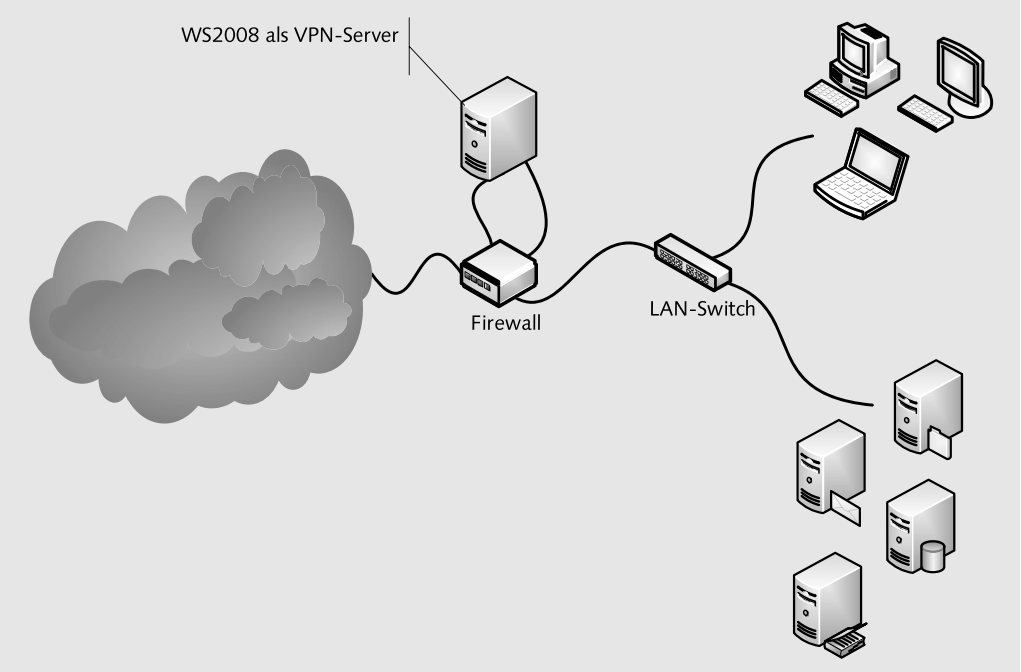


Abbildung 5.76 Alternativer Aufbau der VPN-Umgebung

Natting

Generell gilt, dass es am einfachsten wäre, wenn die externe, also internetseitige Netzwerkkarte des VPN-Servers, eine geroutete öffentliche IP-Adresse hätte. Sofern Sie ihm »nur« eine genattete IP-Adresse zur Verfügung stellen können, hängt es von dem nattenden Router bzw. der nattenden Firewall ab, ob ein Verbindungsaufbau möglich ist. Router/Firewall müssen ein Natting für ein Tunneling-Protokoll explizit unterstützen.

5.9.2 Grundkonfiguration des VPN-Servers

Wenn Sie mit der Einrichtung des VPN-Servers beginnen, sollte dieser über zwei Netzwerkanschlüsse verfügen. Der eine Anschluss nimmt den Verkehr aus dem Internet entgegen, der andere kommuniziert mit dem internen LAN.

Die VPN-Server-Funktionalität ist ein Bestandteil der Netzwerkrichtlinien- und Zugriffsdienste, folglich muss dem Server diese Rolle hinzugefügt werden (Abbildung 5.77).

Der Installationsassistent wird Sie auf der nächsten Seite fragen, welche Rollendienste installiert werden sollen (Abbildung 5.78). Für die Erstellung eines VPN-Servers benötigen Sie prinzipiell nur die Routing- und RAS-Dienste. Sofern Sie die zugreifenden Clients auf Einhaltung bestimmter Richtlinien (z. B. »Sind alle Patches installiert?«, »Ist ein aktueller Virenscanner vorhanden?« etc.) prüfen möchten, benötigen Sie zusätzlich den Netzwerkrichtlinienserver (siehe Abschnitt 12.3, »Netzwerkrichtlinien- und Zugriffsdienste«).

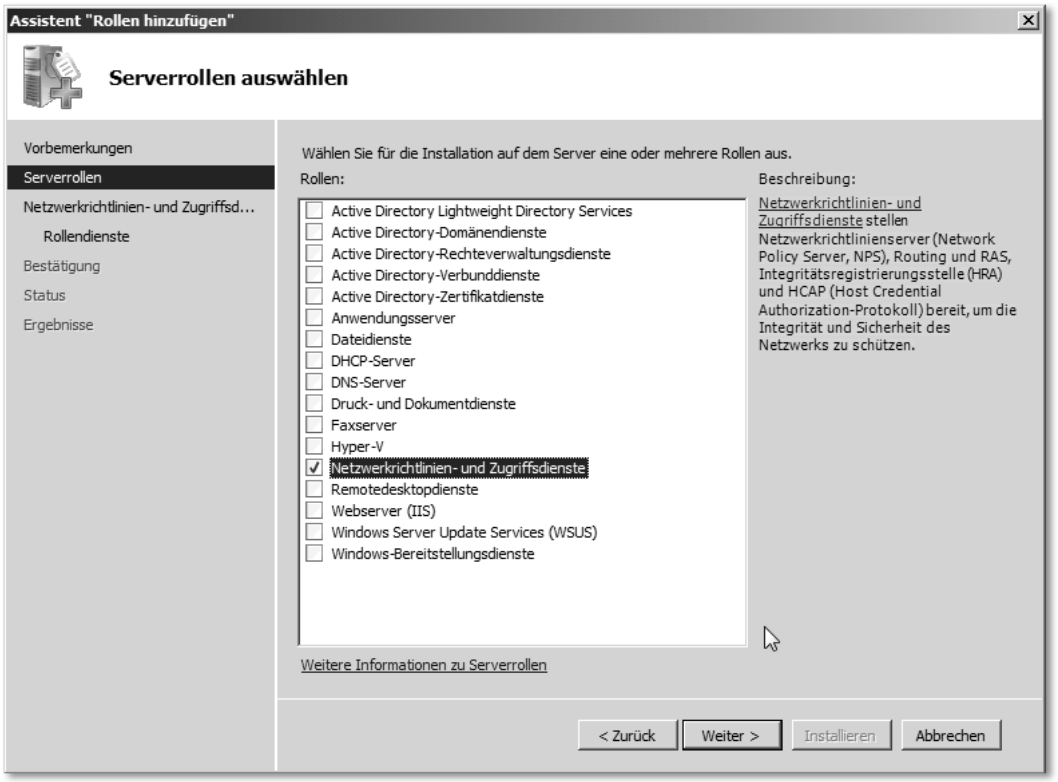


Abbildung 5.77 Wenn Sie aus einem Windows Server 2008 einen VPN-Server machen möchten, müssen Sie die Rolle »Netzwerkrichtlinien- und Zugriffsdienste« installieren.

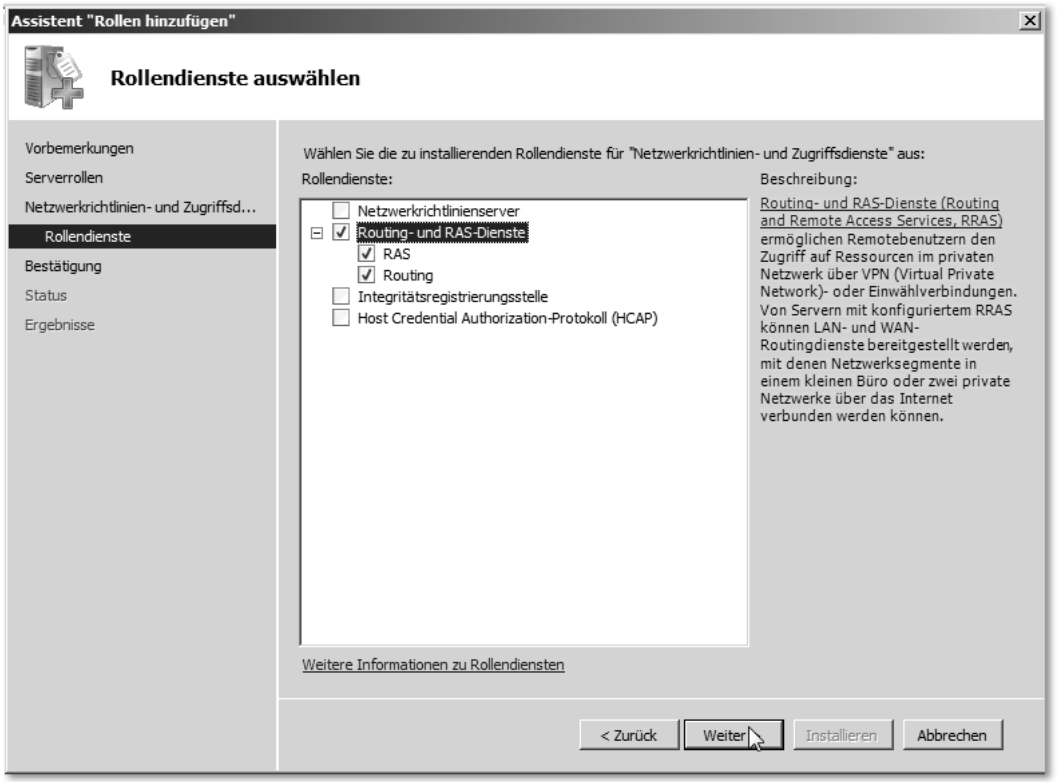


Abbildung 5.78 Sie benötigen mindestens den Rollendienst »Routing- und RAS-Dienste«.

Die Installation der Rolle erfordert ansonsten keine weiteren Eingaben.

Nach Abschluss der Installation können Sie in der Verwaltung das Werkzeug ROUTING UND RAS starten. Ein Assistent hilft bei der Ersteinrichtung. Wie Sie auf Abbildung 5.79 sehen können, stehen diverse Konfigurationsmodelle zur Verfügung. Sie können sich allerdings auch für die Option BENUTZERDEFINIERTE KONFIGURATION entscheiden und komplett manuell konfigurieren.

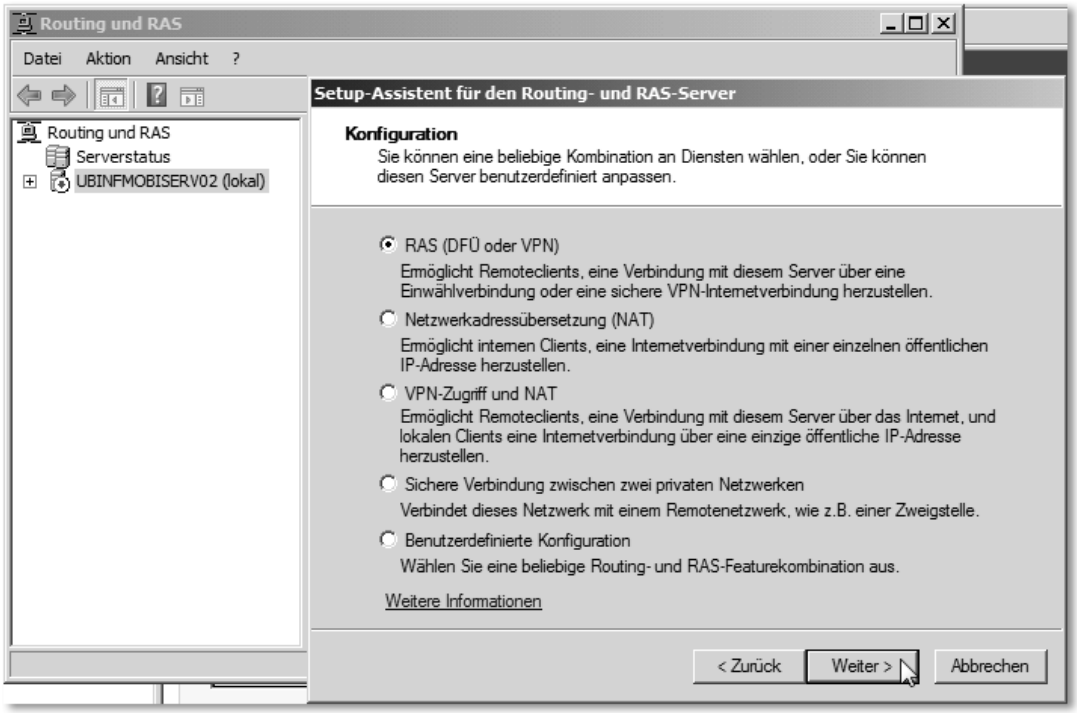


Abbildung 5.79 Der Installationsassistent kann bereits eine Konfiguration vorbereiten, Sie können diese Arbeiten aber auch komplett »zu Fuß« ausführen.

In diesem Beispiel habe ich mir vom Assistenten helfen lassen. Dieser führt durch folgende Entscheidungen:

- Zunächst können Sie festlegen, ob Sie den Server für VPN und/oder RAS verwenden möchten. Ja, die Remoteeinwahl per Modem wird auch noch immer unterstützt (Abbildung 5.80).
- Im nächsten Schritt müssen Sie die internetseitige Netzwerkkarte auswählen, was auch unproblematisch ist (Abbildung 5.81).
- Im nun folgenden Dialog wird definiert, wie die IP-Adressen für die sich verbindenden Remoteclients ermittelt werden. Im Allgemeinen die beste Möglichkeit ist die Verwendung von DHCP, alternativ kann der VPN-Server auch die Zuweisung von Adressen vornehmen (Abbildung 5.82).
- Im letzten Dialog des Assistenten können Sie entscheiden, ob die Authentifizierung durch den VPN-Server erfolgen soll oder ob ein nachgelagerter

RADIUS-Server zur Authentifizierung verwendet werden soll. Soll der VPN-Server die Authentifizierung durchführen, muss er Domänenmitglied sein, oder es können sich nur lokal angelegte Benutzer anmelden (Abbildung 5.83).

Abbildung 5.80 Entscheiden Sie sich zunächst für die Unterstützung von VPN-Verbindungen.

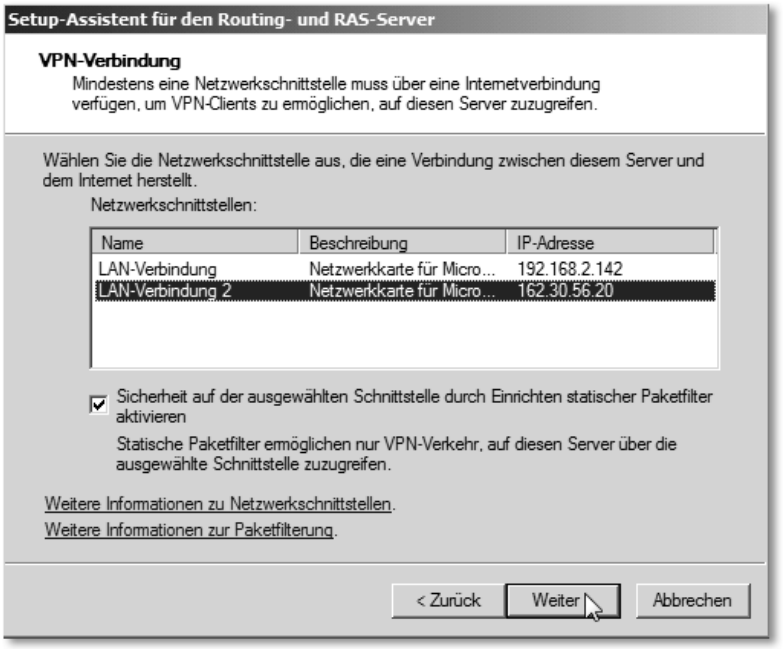


Abbildung 5.81 Anschließend müssen Sie die internetseitige Netzwerkschnittstelle auswählen.

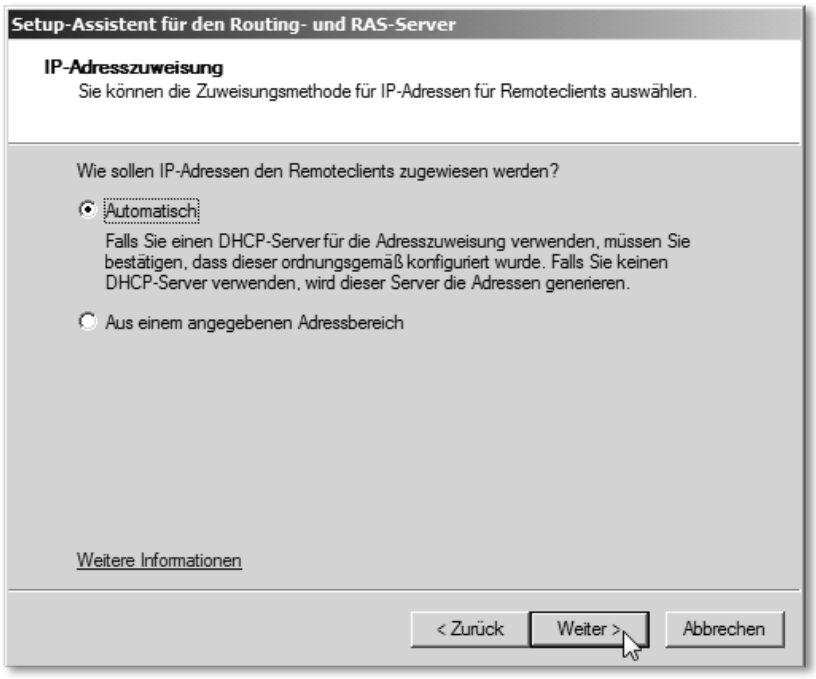


Abbildung 5.82 In diesem Dialog wird konfiguriert, wie die Adresszuweisung erfolgen soll.

Abbildung 5.83 Hier wird korrigiert, wo die Authentifizierung stattfinden soll.

Spätere Änderungen möglich

Sämtliche Einstellungen, die dieser Assistent für die Ersteinrichtung vornimmt, können Sie natürlich später beliebig ändern.

5.9.3 VPN einrichten – allgemein

Die Einrichtung einer VPN-Verbindung in Windows 7 ist nicht kompliziert. Sie beginnt im Netzwerk- und Freigabecenter, genauer gesagt mit dem Menüpunkt NEUE VERBINDUNG ODER NEUES NETZWERK EINRICHTEN (Abbildung 5.82).

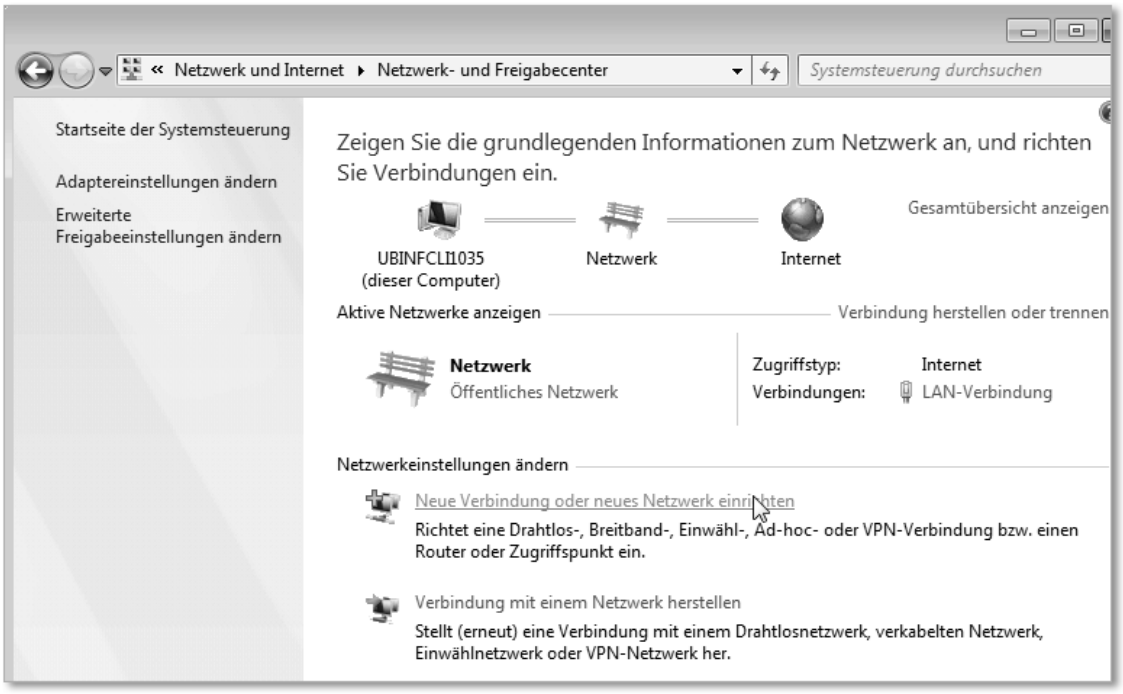


Abbildung 5.84 Die Einrichtung einer neuen VPN-Verbindung beginnt im Netzwerk- und Freigabecenter.

Es startet ein Assistent, der neben einer VPN-Verbindung auch diverse andere Netzwerkverbindungen aufbauen kann. Wenn Sie noch einmal Abbildung 5.74 ansehen, ist das auch einleuchtend, denn die Treiber für die diversen Tunnelingprotokolle sind nur einige unter vielen (Abbildung 5.85). Der nächste Dialog des Assistenten ist ebenfalls leicht zu bearbeiten – es geht um die Frage, ob Sie ein VPN oder eine Einwahlverbindung einrichten möchten (Abbildung 5.86).

In den nächsten beiden Dialogen werden nun die technischen Daten für die neue VPN-Verbindung erfasst:

- Zunächst geht es um die Internetadresse des VPN-Servers. Hier kann eine IP-Adresse oder ein Name eingetragen werden.

  Es könnte unter Umständen empfehlenswert sein, die Checkbox JETZT NICHT VERBINDEN… zu aktivieren. Dies empfiehlt sich immer dann, wenn Sie nach dem Durchlauf des Assistenten noch ein wenig »Feintuning« vornehmen möchten (Abbildung 5.87).

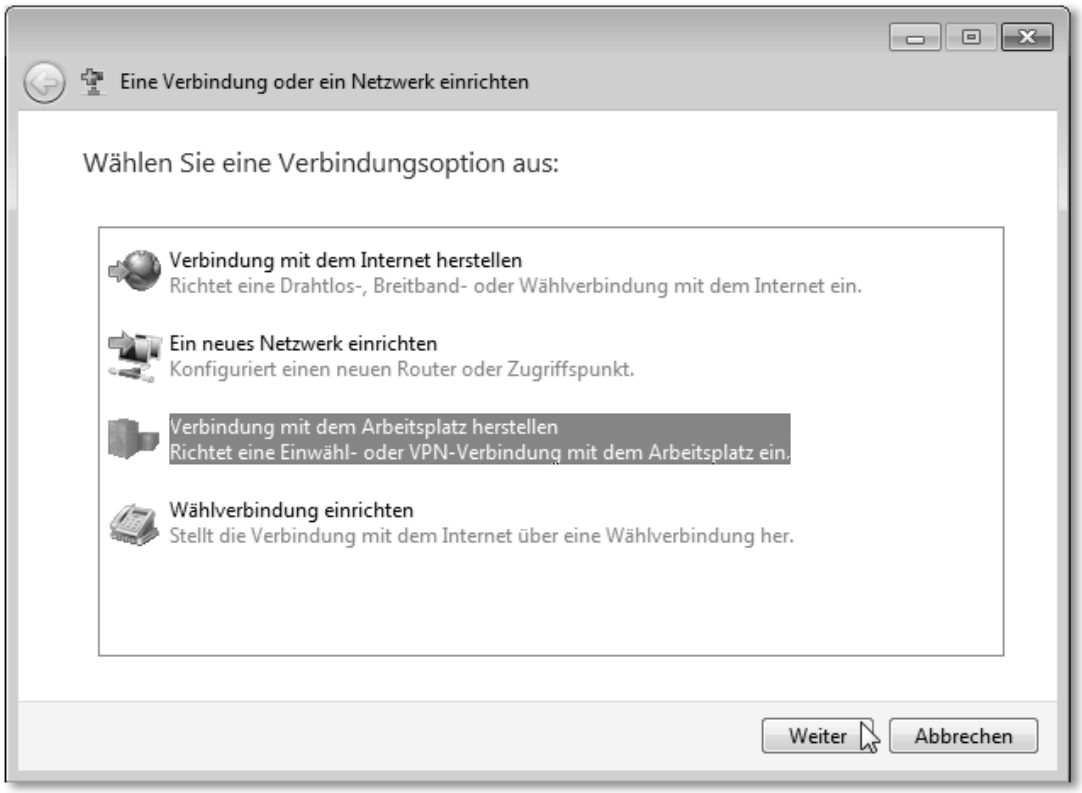


Abbildung 5.85 Ein VPN wird mit dieser Option eingerichtet.

Abbildung 5.86 Sie können ein VPN erstellen oder eine Direktwahlverbindung einrichten.

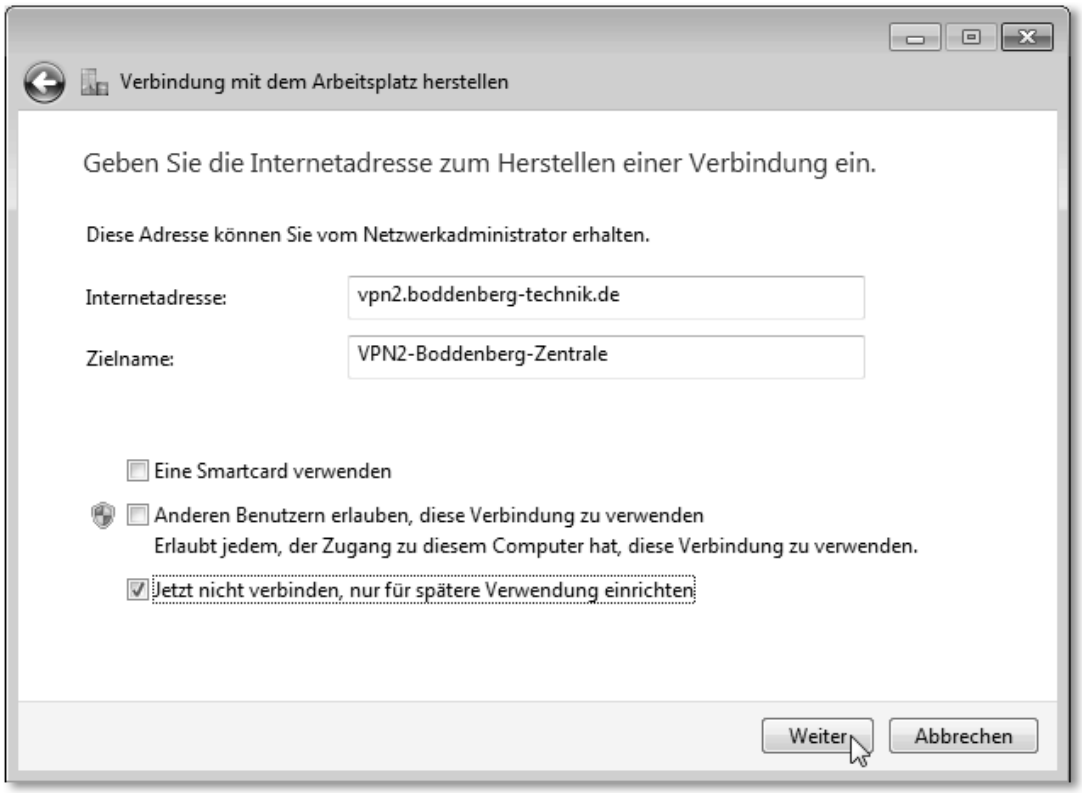


Abbildung 5.87 Zunächst werden die Verbindungsdaten erfasst.

- Im nächsten Dialog werden Benutzername, Kennwort und optional die Domäne erfasst. Beim Verbindungsaufbau zum Windows-Netz ist das zumindest empfehlenswert (Abbildung 5.88).

Das Verwalten der VPN-Einträge und das Verbinden funktionieren anders als bei Windows Vista – als ich das erste Mal mit Windows 7 gearbeitet hatte, musste ich schon ein wenig suchen.

Wenn Sie auf das Netzwerksymbol in der Taskleiste (den kleinen grauen Monitor mit dem dicken Netzwerkkabel und dem überdimensionalen Stecker) klicken oder alternativ im Netzwerk- und Freigabecenter den Link VERBINDUNG MIT EINEM NETZWERK HERSTELLEN wählen, erscheint die auf Abbildung 5.89 gezeigte Fläche. Dort wird einerseits gezeigt, mit welchen Netzwerken derzeit eine Verbindung besteht (hier »nur« mit einem öffentlichen NETZWERK mit Internetzugriff), andererseits werden die eingerichteten Verbindungen gezeigt – nebst Kontextmenüpunkten für das VERBINDEN und Bearbeiten der EIGENSCHAFTEN.

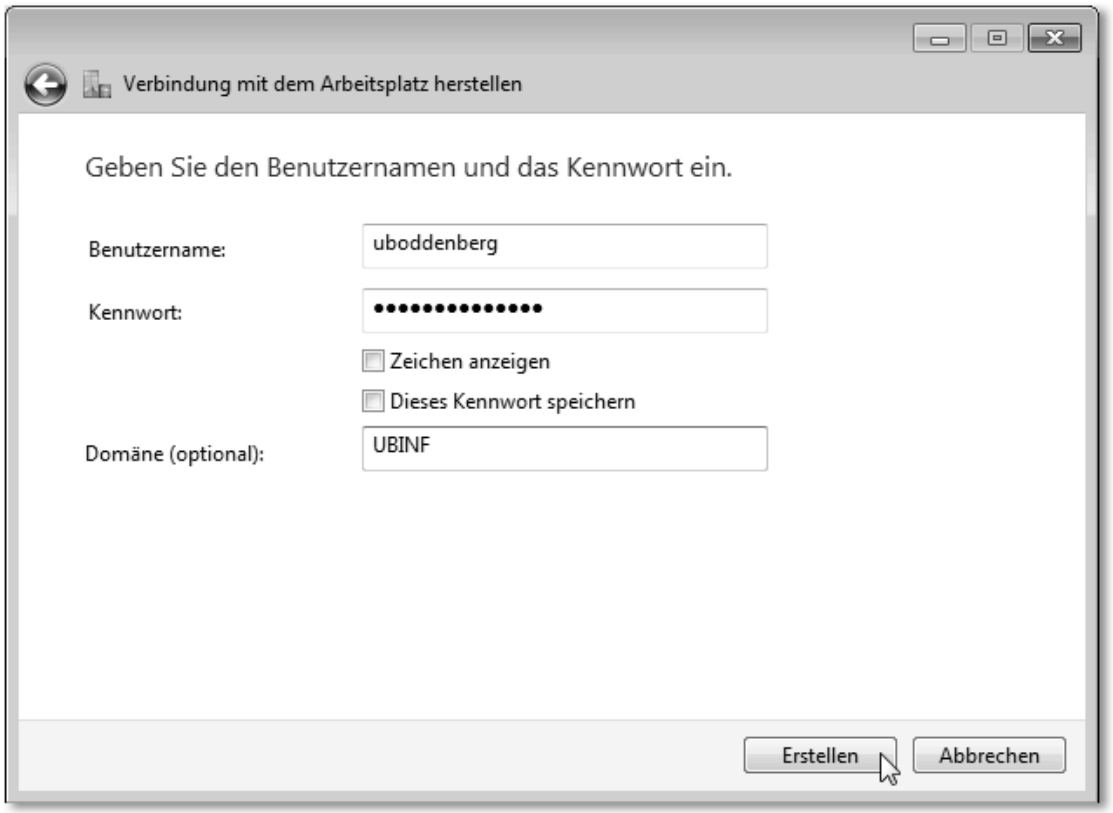


Abbildung 5.88 Hier geben Sie die Benutzerdaten ein.

Abbildung 5.89 Wenn Sie auf das Netzwerksymbol klicken, erscheint die Liste der konfigurierten VPN-Netzwerke.

Wenn eine VPN-Verbindung existiert, ändert sich die Anzeige dahingehend, dass nun zwei aktiv verbundene Netze angezeigt werden (Abbildung 5.90). Beim angezeigten Domänennetzwerk UBINF.INTRA ist übrigens zu beachten, dass das nicht der Name der VPN-Verbindung ist, sondern dass Windows 7 korrekt den Namen der Domäne identifiziert hat.

Windows 7 hat übrigens nicht »nur« den Namen richtig identifiziert, sondern hat auch den Typ des Netzwerkstandorts richtig erkannt: ein Domänennetzwerk – das ist an dem Symbol zu erkennen.

Abbildung 5.90 Hier ist eine bestehende VPN-Verbindung vorhanden.

Wenn eine VPN-Verbindung besteht, ist es auch interessant, einen Blick auf die Windows-Firewall zu werfen (Abbildung 5.91). Auch diese erkennt korrekt, dass eine Verbindung zu einem Domänennetzwerk und eine Verbindung zu einem öffentlichen Netzwerk existiert.

Eine Neuerung der Windows-Firewall in Windows 7 ist, dass mehrere Profile gleichzeitig aktiv sein können – das ist hier der Fall.

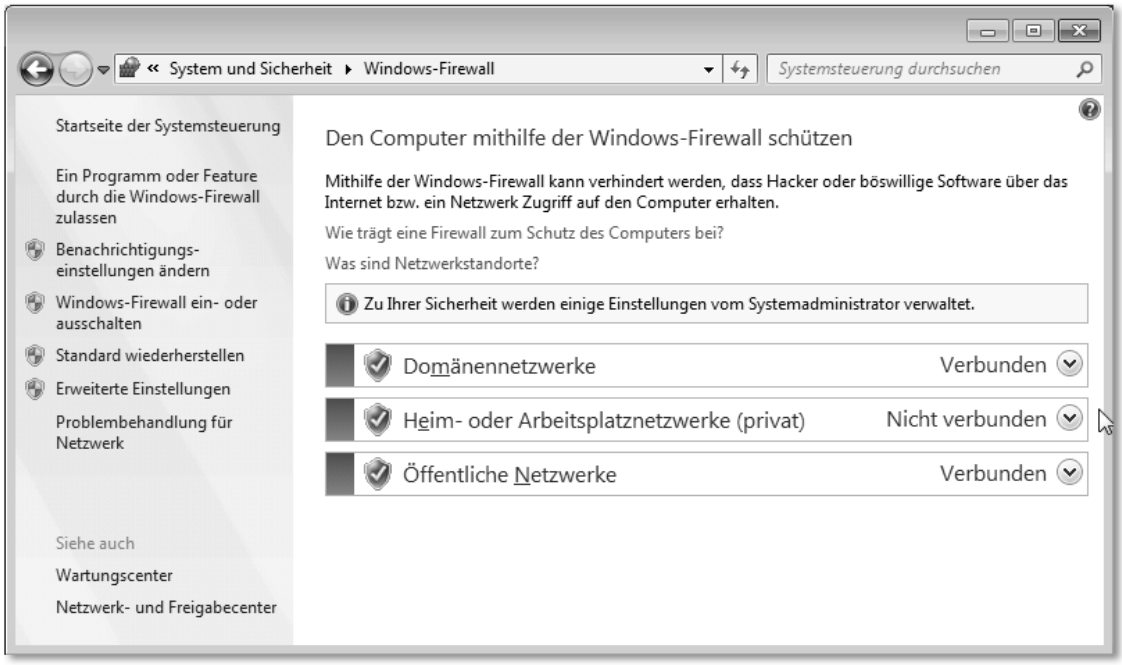


Abbildung 5.91 Wenn Sie den Status der Firewall abrufen, werden auch dort zwei verbundene Netzwerkstandorte angezeigt.

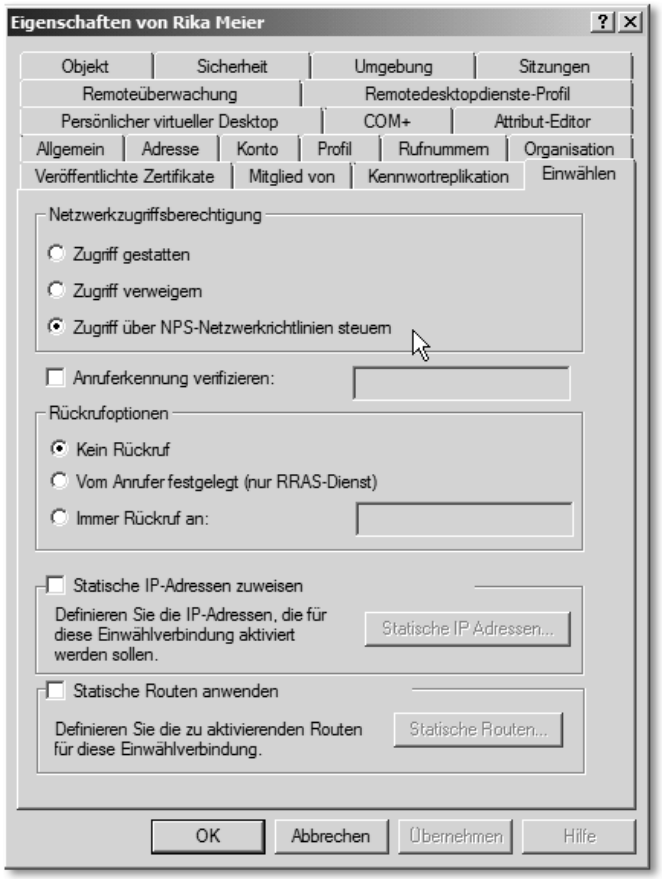


Abbildung 5.92 In den Eigenschaften des Kontos werden die Einwahlberechtigungen konfiguriert.

5.9.4 Einwahlberechtigung

Nicht jeder Benutzer muss notwendigerweise Einwahlberechtigungen haben. Die Steuerung der Berechtigung erfolgt über ein Active Directory-Attribut. Sie konfigurieren es in den Eigenschaften des Benutzers, auf der Registerkarte EINWÄHLEN (Abbildung 5.92). Sie haben drei Möglichkeiten:

- ZUGRIFF GESTATTEN
- ZUGRIFF VERWEIGERN
- ZUGRIFF ÜBER NPS-NETZWERKRICHTLINIEN STEUERN. NPS ist der *Network Policy Server*. Sie lernen ihn ansatzweise in Abschnitt 12.3, »Netzwerkrichtlinien- und Zugriffsdienste«, kennen.

Wenn ein Benutzer versucht, sich einzuwählen, und keine Berechtigungen hat, erscheint die Fehlermeldung aus Abbildung 5.93.

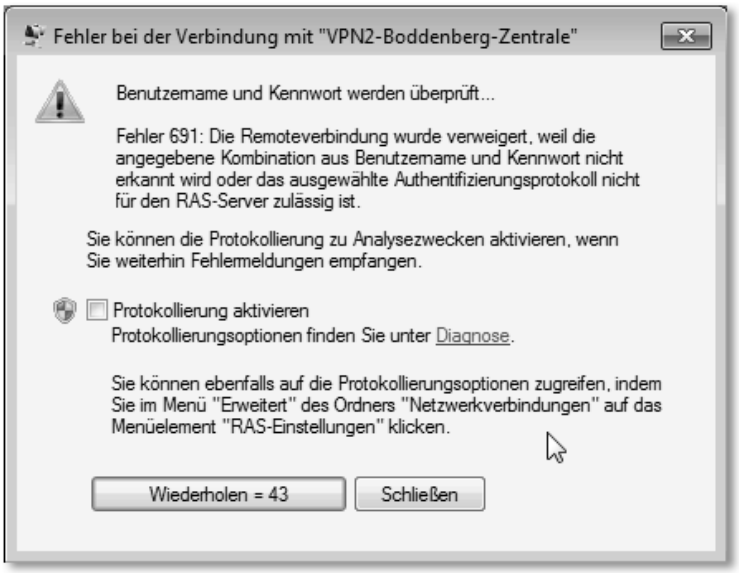


Abbildung 5.93 Diese Meldung erscheint, wenn eine Verbindung nicht möglich ist, weil der Benutzer keine Einwahlberechtigung hat.

5.9.5 PPTP-VPN

In den Eigenschaften der VPN-Verbindung können Sie festlegen, welcher VPN-TYP verwendet werden soll. Etwas genauer ausgedrückt, wählen Sie das zu verwendende Tunneling-Protokoll.

Das vermutlich in der Anwendung simpelste Tunneling-Protokoll ist PPTP, das Point-to-Point-Tunneling-Protokoll. Es kann unterschiedliche Protokolle (TCP/IP, NetBEUI, IPX) tunneln und benötigt keine weitere Voraussetzungen wie beispielsweise Zertifikate zur Authentifizierung und Verschlüsselung.

PPTP ist unter Sicherheitsaspekten nicht optimal, da die Verschlüsselungsstärke von der Länge des verwendeten Kennworts abhängig ist. Etwas salopp gesagt, würde ich es so ausdrücken: Für den »normalen« Gebrauch dürfte die Verwendung von PPTP akzeptabel sein. Sofern Sie mit einer realistischen (!) Bedrohung durch Industriespionage rechnen müssen, sollten Sie ein anderes Tunneling-Protokoll als Basis für Ihre VPN-Verbindungen wählen.

Die Konfiguration von PPTP ist schnell abgehandelt. Auf Abbildung 5.94 sehen Sie die Registerkarte SICHERHEIT des EIGENSCHAFTEN-Dialogs der VPN-Verbindung.

Hier bestimmen Sie den VPN-Typ und nehmen gegebenenfalls weitere Einstellungen vor. Bei der Auswahl von PPTP ist die Schaltfläche ERWEITERE EINSTELLUNGEN allerdings deaktiviert – es gibt zum PPTP-Protokoll nichts einzustellen.

Sie sollten darauf achten, dass Datenverschlüsselung als ERFORDERLICH konfiguriert ist. Das PPTP-Protokoll selbst beinhaltet keine Verschlüsselungsverfahren, aber auf höheren Protokollschichten kann selbstverständlich eine Verschlüsselung durchgeführt werden

Die zu verwendende Authentifizierungsmethode hängt von dem VPN-Server ab, mit dem der Client eine Verbindung aufbaut. Sie haben zwei generelle Möglichkeiten:

- Sie verwenden eine *EAP-basierte Authentifizierung*. EAP steht für *Extensible Authentication Protocol*. Es handelt sich dabei um ein erweiterbares Protokoll, das mit unterschiedlichen Verfahren arbeiten kann. Sofern Sie sich also in einen Microsoft VPN-Server einwählen, ist eines der EAP-Protokolle die beste Wahl.

  Zur Verfügung stehen drei Microsoft-Authentifizierungsverfahren, die jeweils mehr oder weniger umfangreich konfigurierbare Eigenschaften besitzen. Auf Abbildung 5.93 sehen Sie die Konfiguration von EAP-MSCHAP v2, bei dem konfiguriert werden kann, dass die aktuellen Anmeldeinformationen des Benutzers verwendet werden. Ist dies so konfiguriert, braucht der Anwender keine zusätzlichen Anmeldeinformationen einzugeben.

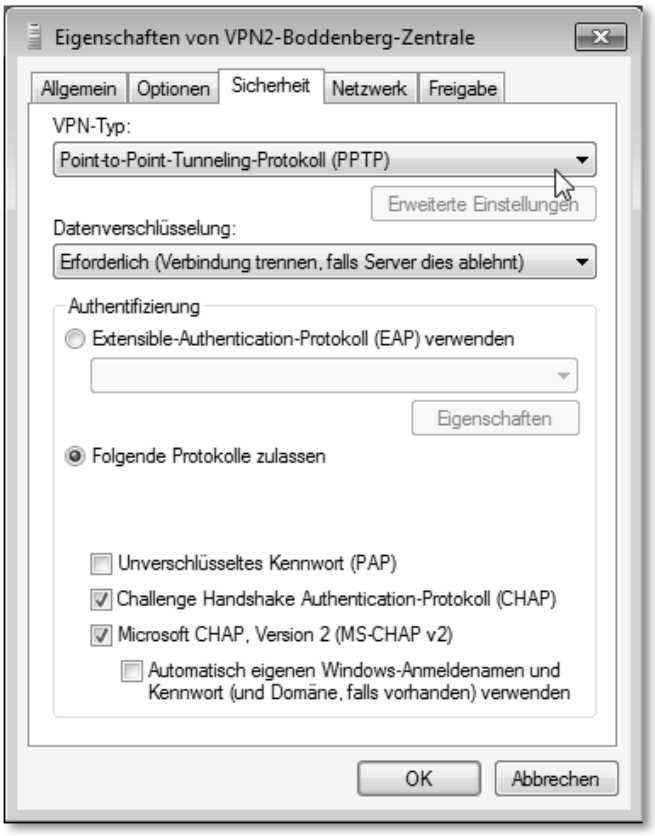


Abbildung 5.94 Beim Point-to-Point-Tunneling-Protokoll gibt es nicht viel einzustellen.

- Wenn Sie nicht EAP verwenden möchten oder können, lässt sich unter der Option FOLGENDE PROTOKOLLE ZULASSEN bestimmen, welche Authentifizierungsprotokolle verwendet werden können. PAP, bei dem das unverschlüsselte Kennwort übertragen wird, ist sicherlich keine gute Wahl. Bei der Verwendung von MSCHAP kann die Verwendung der aktuellen Windows-Anmeldeinformationen konfiguriert werden – eine zusätzliche Passworteingabe ist dann beim Verbindungsaufbau nicht erforderlich.

PPTP-Kommunikation

Die PPTP-Kommunikation läuft über den Serverport 1723 (TCP). Weiterhin wird das GRE-Protokoll (*Generic Routing Encapsulation Protocol*) zum Einkapseln der Daten verwendet.

PPTP-Kommunikation kann grundsätzlich genattet werden, allerdings müssen die NAT-Geräte (also Router und Firewall) dies explizit unterstützen.

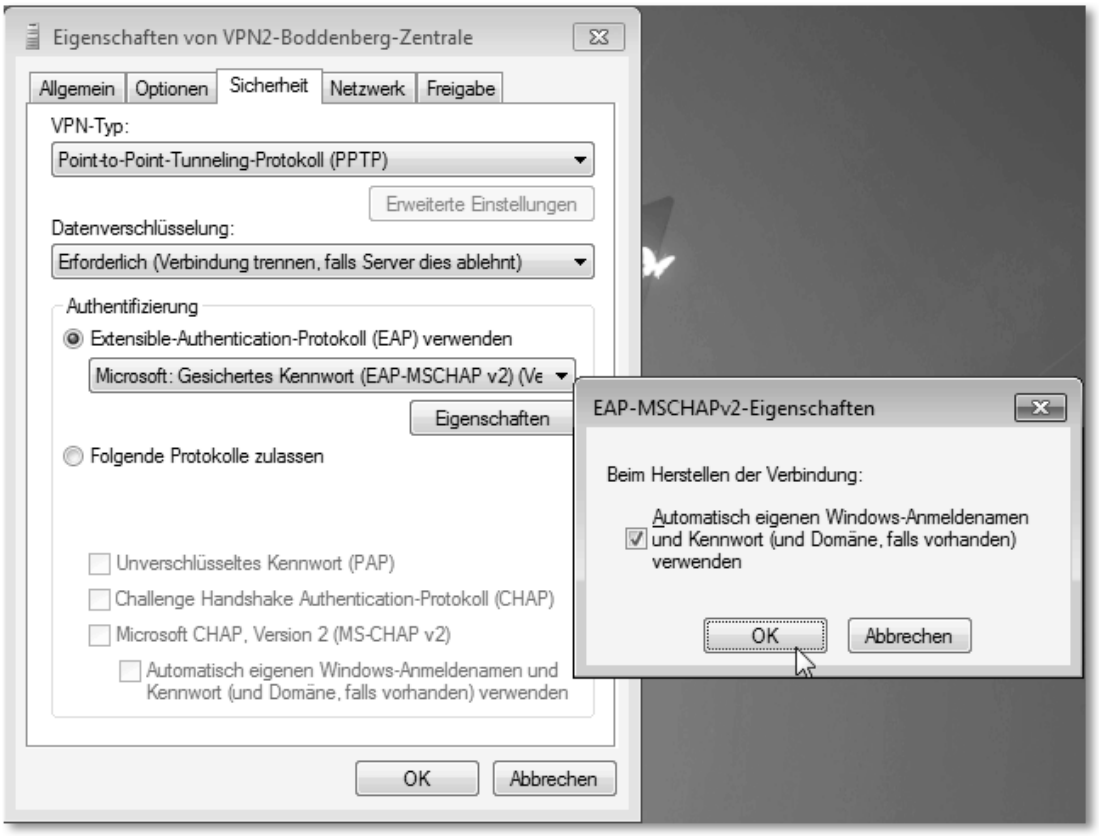


Abbildung 5.95 Sie können festlegen, welches Authentifizierungsprotokoll verwendet werden soll. Hilfreich ist auch die automatische Übermittlung der Windows-Anmeldeinformationen.

5.9.6 L2TP-VPN

Die komplette Bezeichnung dieser VPN-Variante ist L2TP/IPSec. Das beschreibt eigentlich schon ziemlich genau, wie das Verfahren funktioniert:

- Der VPN-Tunnel wird mittels des L2TP-Protokolls aufgebaut. Wie bei PPTP ist im L2TP keine Verschlüsselung der übertragenen Daten enthalten.
- Die verschlüsselte Datenübertragung erfolgt über IPSec.

Bei der Verwendung von L2TP/IPSec fallen vielen Administratoren zunächst Stichwörter wie *Zertifikate* und *Vorinstallierter Schlüssel* (PSK, Pre-Shared Key) ein. Beides gehört zu dem Verfahren, allerdings nicht zu L2TP, sondern zu IPSec. Die Authentifizierung bei L2TP erfolgt über ein zu bestimmendes Authentifizierungsprotokoll, beispielsweise EAP (nebst Erweiterung) oder CHAP. IPSec hingegen basiert prinzipiell auf einer zertifikatsbasierten Authentifizierung, d. h., sowohl der Client als auch der Server müssen über ein entsprechendes Zertifikat verfügen. Das ist so weit auch alles bestens, nur was passiert, wenn ein Unternehmen bzw. eine Organisation (noch) keine eigene PKI implementiert hat und folglich nicht über Zertifikate verfügt?

In diesem Fall kann ein vorinstallierter Schlüssel, vermutlich besser bekannt unter dem englischen Begriff *Pre-Shared Key* (PSK), verwendet werden.

In den Erweiterten Einstellungen für L2TP/IPSec ist nun auch genau das auswählbar: Sie können festlegen, ob mit einem vorinstallierten Schlüssel oder Zertifikaten gearbeitet werden soll (Abbildung 5.96). Der Konfigurationsdialog Erweiterte Egenschaften ist übrigens etwas missverständlich, denn es geht hier eigentlich nicht um die L2TP-Authentifizierung, sondern um die IPSec-Authentifizierung!

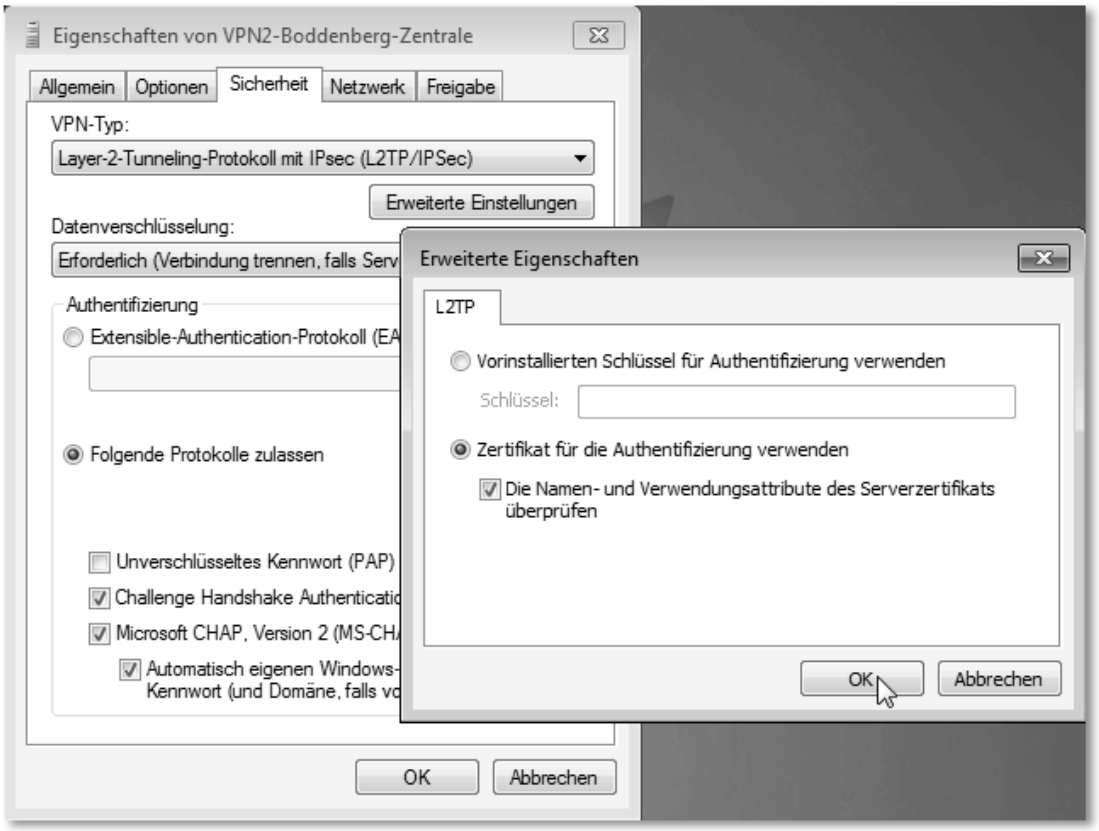


Abbildung 5.96 L2TP kann entweder mit einem vorinstallierten Schlüssel (PSK, Pre-Shared Key) oder mit Zertifikaten arbeiten.

Keine vorinstallierten Schlüssel

Auch wenn die Nutzung von vorinstallierten Schlüsseln weit verbreitet ist, wird sie nicht empfohlen! Ursprünglich sind vorinstallierte Schlüssel nur für Testzwecke gedacht gewesen.

Die empfohlene Methode ist die Arbeit mit Zertifikaten.

Falls Sie mit vorinstallierten Schlüsseln arbeiten, muss dieser Schlüssel auch auf dem VPN-Server eingetragen werden. Sie können den Schlüssel im Verwaltungswerkzeug Routing und RAS in den Servereigenschaften konfigurieren (Abbil-

dung 5.97). Der vorinstallierte Schlüssel ist übrigens eine beliebige Zeichenkette, die Sie sich frei ausdenken können.

Abbildung 5.97 Möglich, aber nicht empfohlen: die Verwendung eines vorinstallierten Schlüssels

Abbildung 5.98 zeigt den Auszug einer L2TP/IPSec-Kommunikation im Netzwerkmonitor:

- Zunächst wird die IPSec-Authentifizierung ausgehandelt (zu sehen in den Paketen 12 bis 23).

  Zur Sicherung des Tunnels wird IPSec verwendet, folglich muss zunächst die IPSec-Authentifizierung nebst Schlüsselaustausch stattfinden. Hierzu wird das Protokoll IKE (*Internet Key Exchange*) verwendet.
- Nach Abschluss der Authentifizierungsphase erfolgt die gesicherte Kommunikation über IPSec. Das sehen Sie an den ESP-Paketen (*Encapsulating Security Payload*).

Bei Betrachtung der Netzwerkpakete wird dann auch klar, warum es *L2TP over IPSec* heißt: Zunächst wird die IPSec-Verbindung aufgebaut, und darüber wird der L2TP-Tunnel geführt.

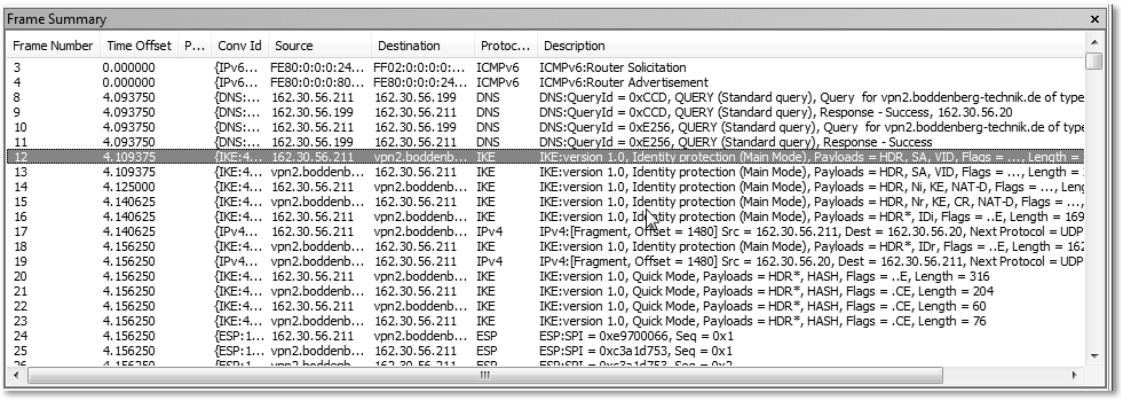


Abbildung 5.98 L2TP/IPSec im Netzwerkmonitor. Zunächst erfolgt die Authentifizierung (IKE-Pakete), dann erfolgt die Kommunikation über IPSec (ESP-Pakete).

NAT-Fähigkeit

L2TP/IPSec ist prinzipiell NAT-fähig, allerdings müssen sowohl die L2TP/IPSec-Implementationen auf VPN-Client und -Server als auch alle zwischengeschalteten Netzwerkkomponenten (Router/Firewall) dies unterstützen.

5.9.7 SSTP

Die beiden zuvor gezeigten Tunneling-Protokolle, also PPTP und L2TP, gibt es für IT-Zeitbegriffe schon ewig. SSTP, das *Secure Socket Tunneling Protocol* ist vergleichsweise neu und tauchte zuerst im Windows Vista SP1 und in Windows Server 2008 auf.

Wenn Anwender sich mit ihrem Notebooks in fremden Netzen, beispielsweise beim Kunden, befinden, scheitert der Aufbau der VPN-Verbindung häufig daran, dass die Firewall des Netzes keinen PPTP oder L2TP/IPSec-Verkehr zulässt. Auch von WLAN-Hotspots in Flughafen-Lounges und dergleichen ist schon berichtet worden, dass »nur« HTTP- bzw. HTTPS-Zugriffe über die Firewall gestattet sind.

Der naheliegende Gedanke ist also, die so gut wie überall zulässigen SSL-Pakete zum Aufbau des VPN-Tunnels zu verwenden – und genau das passiert bei einer SSTP-Verbindung.

Auf dem Client muss lediglich der VPN-Typ ausgewählt werden, Erweiterte Einstellungen sind für SSTP nicht vorhanden (Abbildung 5.99).

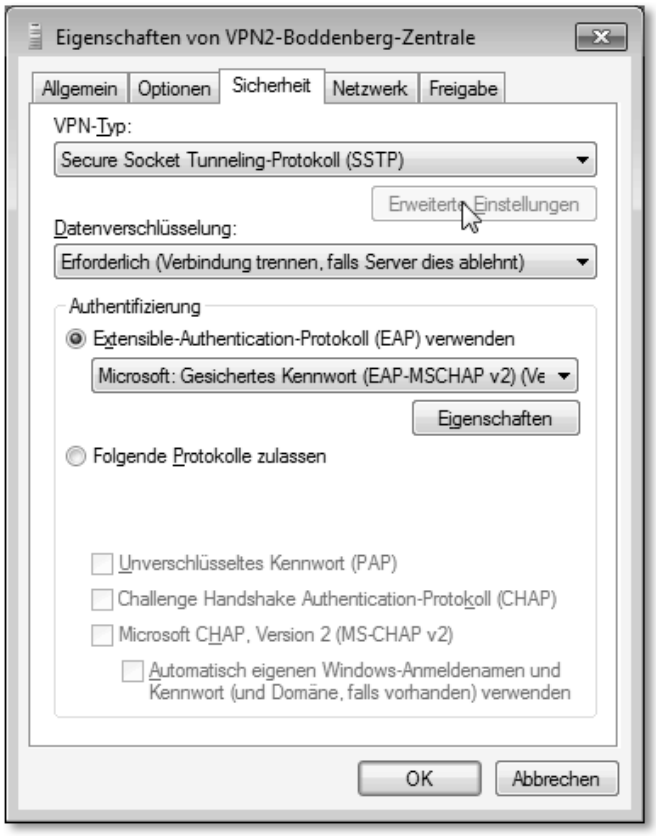


Abbildung 5.99 Beim SSTP-Protokoll gibt es nichts in den »Erweiterten Einstellungen« zu konfigurieren.

Auf dem Server ist, wie bei allen SSL-Verbindungen, ein Zertifikat erforderlich, das die drei bekannten Bedingungen erfüllen muss:

- Das Zertifikat muss zeitlich gültig sein.
- Der Client muss dem Zertifikat vertrauen. Das geschieht dadurch, dass er der zertifikatausgebenden Stelle vertraut, was wiederum dadurch gewährleistet wird, dass der öffentliche Teil des Zertifikats der Stammzertifizierungsstelle an der entsprechenden Stelle des Zertifikatsspeichers des Clients vorhanden ist.
- Das Zertifikat muss dem Namen entsprechen, den der Client aufgerufen hat. Wenn der Client sich mit *vpn2.boddenberg-technik.de* verbinden möchte, darf nicht ein auf den internen Namen des Servers ausgestelltes Zertifikat (z. B. *ubinfmobiserv02.ubinf.intra*) präsentiert werden.

Die zeitliche Gültigkeit des Zertifikats sollte einfach zu erfüllen sein. Wenn das Zertifikat von einer eigenen Active-Directory-integrierten Zertifizierungsstelle herausgegeben worden ist, befindet sich deren Stammzertifikat im Speicher für vertrauenswürdige Stammzertifizierungsstellen – also auch kein Problem.

Der dritte Aspekt ist meistens der fehleranfälligste – obwohl das Folgende eigentlich wirklich kein Problem ist:

- Erzeugen Sie ein Zertifikat für den Namen, den der im Internet befindliche Client zum Verbinden mit dem VPN-Server aufrufen wird (z. B. *vpn2.boddenberg-technik.de*).
- Importieren Sie das Zertifikat in den lokalen Zertifikatsspeicher des Computers.
- In den Eigenschaften des VPN-Servers im Werkzeug ROUTING UND RAS können Sie im Abschnitt SSL-ZERTIFIKATBINDUNG das Zertifikat auswählen (Abbildung 5.100).

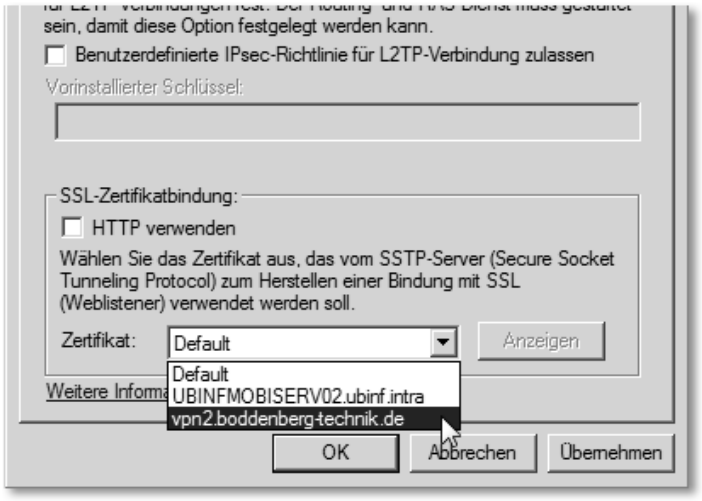


Abbildung 5.100 Bei der serverseitigen Vorbereitung von SSTP ist es extrem wichtig, dass Sie das »passende« Zertifikat auswählen.

Es könnte jetzt sein, dass Ihnen die Fehlermeldung aus Abbildung 5.101 präsentiert wird, die Sie – so leid es mir tut – nicht mit einem grafischen Konfigurationswerkzeug aus dem Weg räumen können.

Diese Fehlermeldung tritt beispielsweise dann auf, wenn bereits ein anderes Zertifikat mit dem Verwendungszweck Serverauthentifizierung auf dem Computer installiert worden ist. In meiner Beispielkonfiguration werden Computerzertifikate per *Auto Enrollment* automatisch auf allen Systemen installiert. Das auf Abbildung 5.100 in der Dropdown-Liste gezeigte Zertifikat *UBINFMOBISERV02.ubinf.intra* ist auf diesem Weg auf die Maschine gekommen. Dieses Zertifikat ist an *HTTP.sys* gebunden worden, was dazu führt, dass Sie nicht das benötigte Zertifikat für SSTP auswählen können.

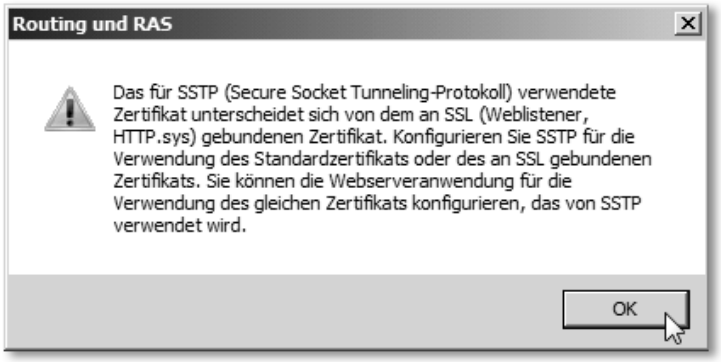


Abbildung 5.101 Diese Fehlermeldung erscheint, wenn »HTTP.sys« bereits an ein anderen Zertifikat gebunden ist.

Die Lösung für das Problem besteht darin, die Bindung des Zertifikats an *HTTP.sys* aufzuheben. Auf Abbildung 5.100 ist zu sehen, wie das gemacht wird:

- Mit dem Befehl `netsh http show sslcert` können Sie die aktuellen Bindungen anschauen. Sie sehen, dass an 0.0.0.0:443 (alle IP-Adressen des Computers, Port 443) ein Zertifikat mit dem Hashwert `e235b`... gebunden ist. Für IPv6 ergibt sich dasselbe Bild.
- Mit `netsh http delete sslcert ipport=0.0.0.0:443` können Sie diese Bindung aufheben. Der entsprechende Befehl für IPv6 lautet `netsh http delete sslcert ipport=[::]:443`.

Nun wird das Zertifikat für den externen Namen auswählbar sein (Abbildung 5.100).

Sperrliste

Eine weitere wichtige Voraussetzung ist, dass die Sperrliste für das verwendete Zertifikat aus dem öffentlichen Internet abrufbar ist!

Die Kontrolle, ob das Zertifikat nicht auf der Sperrliste steht, findet statt, bevor wie VPN-Verbindung benutzbar ist. Daher hilft es nicht, wenn die Sperrliste im internen Netz abrufbar ist.

Nun wird der Verbindungsaufbau per SSTP möglich sein. Die Kontrolle im Netzwerkmonitor zeigt, dass die Verbindung in der Tat über das SSL-Protokoll erfolgt. Somit sollte eine Verwendung über Router und Firewalls hinweg möglich sein (Abbildung 5.103).

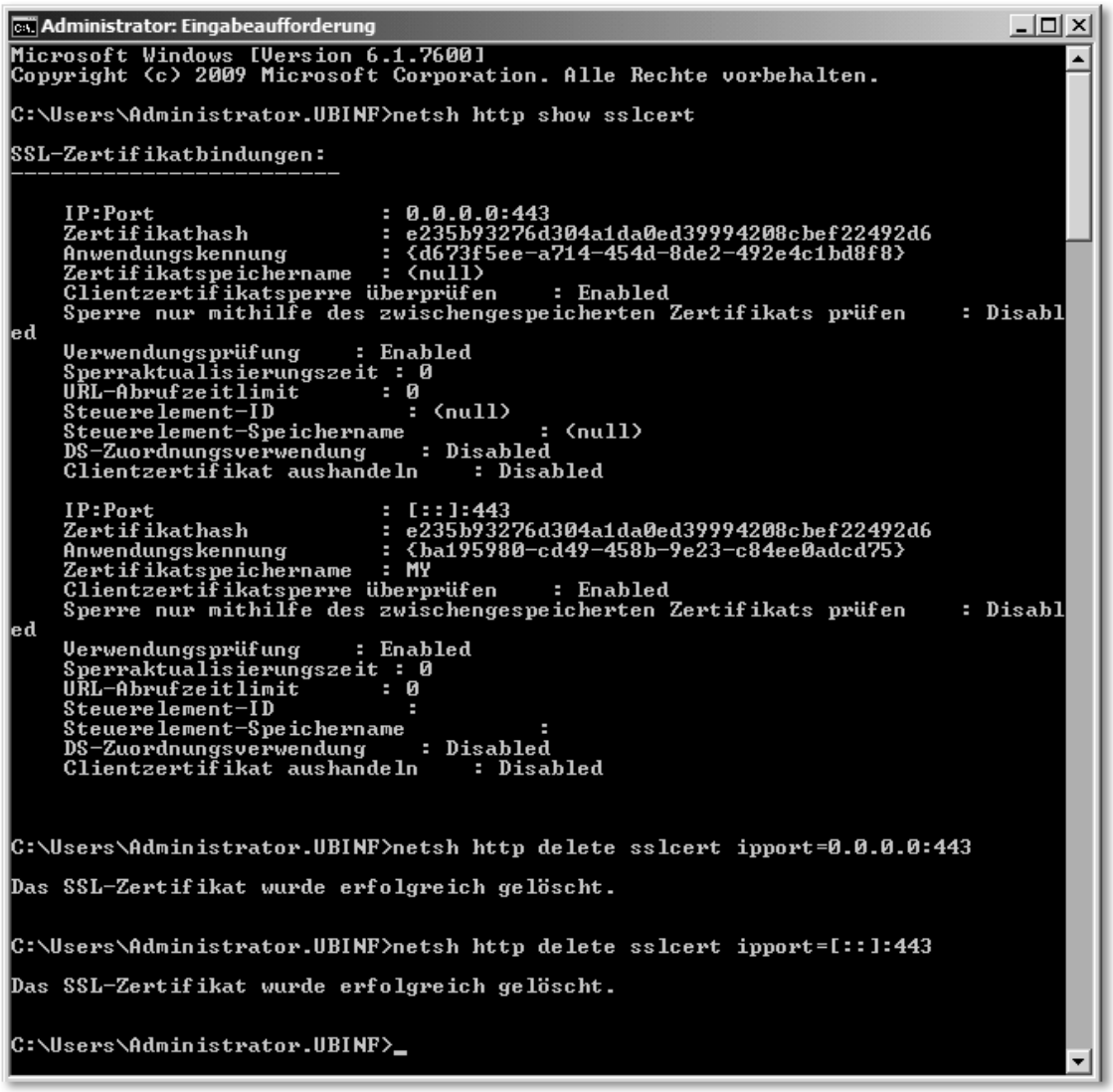


Abbildung 5.102 Die Bindung eines Zertifikats an »HTTP.sys« wird aufgehoben.

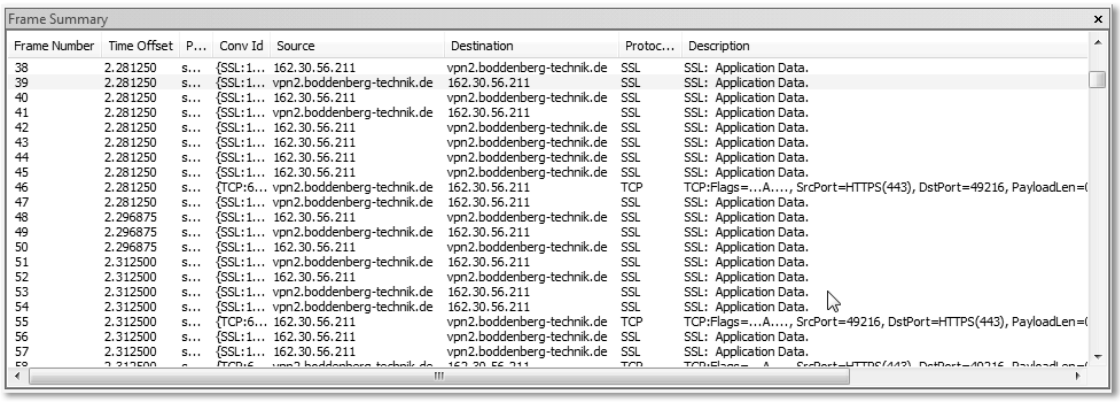


Abbildung 5.103 Wie erwartet läuft der Verkehr komplett über den SSL-Port 443.

Troubleshooting – typische Probleme

SSTP ist zwar grundsätzlich unproblematisch in Konfiguration und Anwendung, trotzdem treten hin und wieder Probleme auf – wie immer. Die meiner Erfahrung nach zwei häufigsten Probleme bespreche ich in diesem Abschnitt.

Ein häufiges Problem ist, dass der Name des für SSTP ausgewählten Zertifikats (Abbildung 5.100) nicht zu dem vom Client aufgerufenen Namen passt. Es erscheint dann die Fehlermeldung aus Abbildung 5.104. Dazu zwei Hinweise:

- Wenn die Clients *vpn1.boddenberg-technik.de* aufrufen, muss das Zertifikat genau auf diesen Namen ausgestellt sein.
- Wenn die Clients den VPN-Server über dessen IP-Adresse erreichen, muss das Zertifikat auf die IP-Adresse ausgestellt sein.

Abbildung 5.104 Einer der häufigsten Fehler ist ein Zertifikat, das für den falschen Namen ausgestellt ist.

Ein zweites wirklich häufiges Problem ist in Abbildung 5.105 zu sehen. Hinter dieser wenig prägnanten Beschreibung steckt die Ursache, dass die Zertifikatssperrliste nicht erreichbar ist, der SSTP-Client also nicht überprüfen kann, ob das Zertifikat, mit dem der VPN-Sicher abgesichert ist, gesperrt wurde.

Das Problem lässt sich wie folgt lösen:

- Definieren Sie in den Eigenschaften der Zertifizierungsstelle eine zusätzliche externe URL für die Sperrliste.
- Kopieren Sie Sperrliste in diese URL.

Bei DirectAccess wird ebenfalls eine Sperrliste benötigt. Das Verfahren ist in Abschnitt 13.2.3, »Vorbereitende Maßnahmen« genauer beschrieben.

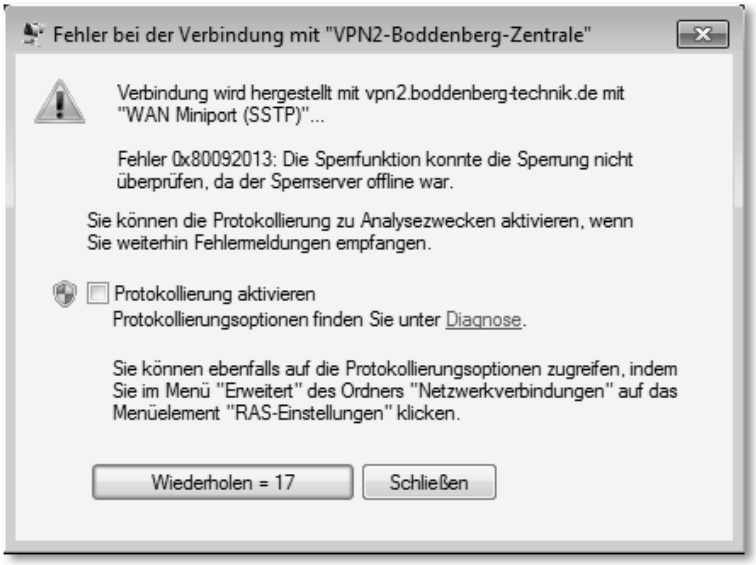


Abbildung 5.105 Ein weiteres häufiges Problem ist eine nicht vorhandene Zertifikatssperrliste.

Falls Sie keinen externen Verteilungspunkt für die Zertifikatssperrlisten einrichten können, lässt sich die Überprüfung der Sperrliste ausschalten:

- Navigieren Sie im Registry-Editor zu diesem Abschnitt: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Sstpsvc\parameters*
- Legen Sie ein neues DWORD namens `NoCertRevocationCheck` an, und setzen Sie den Wert auf 1.

Ein Neustart ist nicht erforderlich, die Einstellung ist sofort aktiv.

Deaktivierung ist nicht sinnvoll

Beachten Sie, dass das Deaktivieren der Überprüfung der Zertifikatssperrliste zwar ein funktionierender Workaround ist – unter Sicherheitsaspekten ist das aber nicht im Sinne des Erfinders. Dass neuerdings einige Technologien (neben SSTP gilt das beispielsweise auch für DirectAccess) die Zertifikatssperrliste überprüfen, ist grundsätzlich sinnvoll und sollte nicht ohne Not unterbunden werden. Insbesondere dann, wenn in Ihrem Unternehmen hoher Wert auf IT-Sicherheit gelegt wird, ist es unbedingt notwendig, gegebenenfalls ein korrumpiertes Zertifikat sperren zu können.

5.9.8 Automatischer Modus

Neben den bisher besprochenen VPN-Typen existiert die Option Automatisch. Bei dieser versucht der Client selbstständig, eine VPN-Verbindung aufzubauen. In den Erweiterten Einstellungen finden sich daher die Konfigurationsoptionen

für L2TP und IKEv2 (PPTP und SSTP haben keine Erweiterten Einstellungen, vgl. Abbildung 5.106). Die Reihenfolge, in der der Verbindungsaufbau probiert wird, ist:

1. IKEv2
2. SSTP
3. PPTP
4. L2PT/IPSec

LMAK

Diese Reihenfolge gilt, wenn die Verbindung mit dem »eingebauten« VPN-Client konfiguriert wurde.

Bei Verbindungen, die mit dem CMAK (*Connection Manager Administration Kit*) erstellt wurden, kann eine andere Reihenfolge definiert sein.

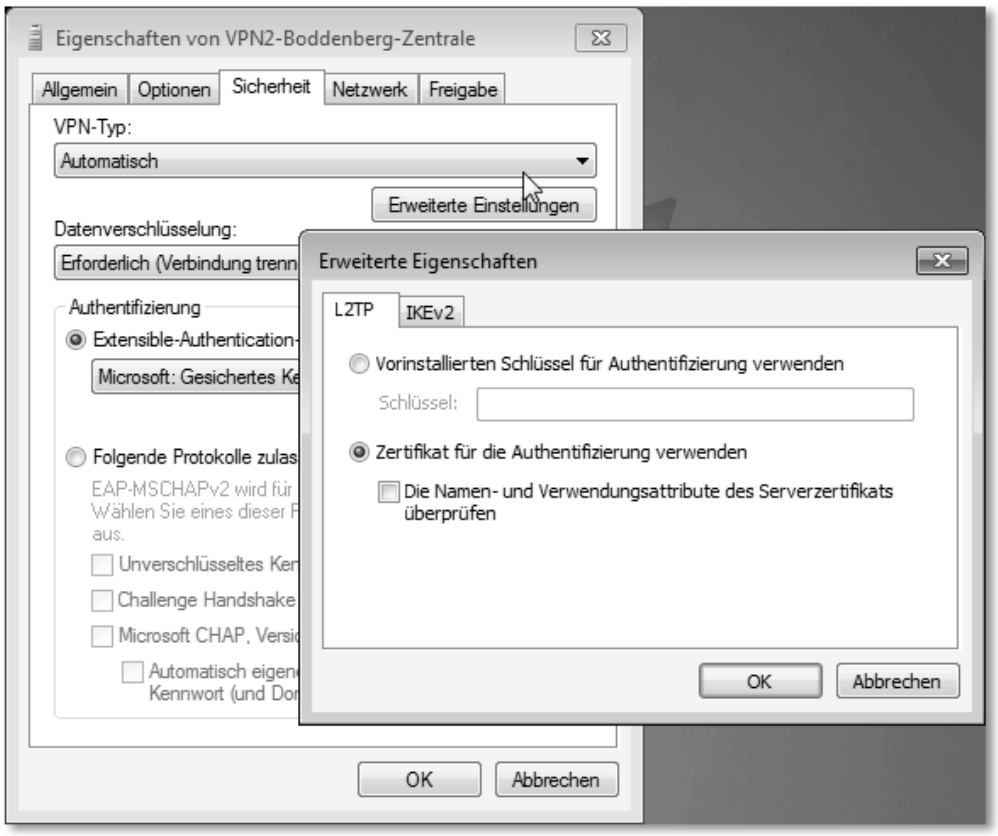


Abbildung 5.106 Beim VPN-Typ »Automatisch« wird erst PPTP, dann L2TP und zum Schluss SSTP probiert.

5.9.9 Connection Manager Administration Kit (CMAK, Verbindungs-Manager-Verwaltungskit)

Nun stehen wir wieder vor dem beliebten Problem: »Was tun wir, wenn nicht nur drei PCs, sondern dreihundert mit der VPN-Verbindung konfiguriert werden sollen?« In diesem Fall ist die Lösung das *Connection Manager Administration Kit* (CMAK).

CMAK

Zur besseren Lesbarkeit bleibe ich bei der Bezeichnung CMAK.

In Windows Server 2008 und Windows Server 2008 R2 gibt es ein Feature, das in den deutschen Versionen *Verbindungs-Manager-Verwaltungskit* heißt und ohne weitere Konfigurationsarbeiten installiert werden kann (Abbildung 5.107).

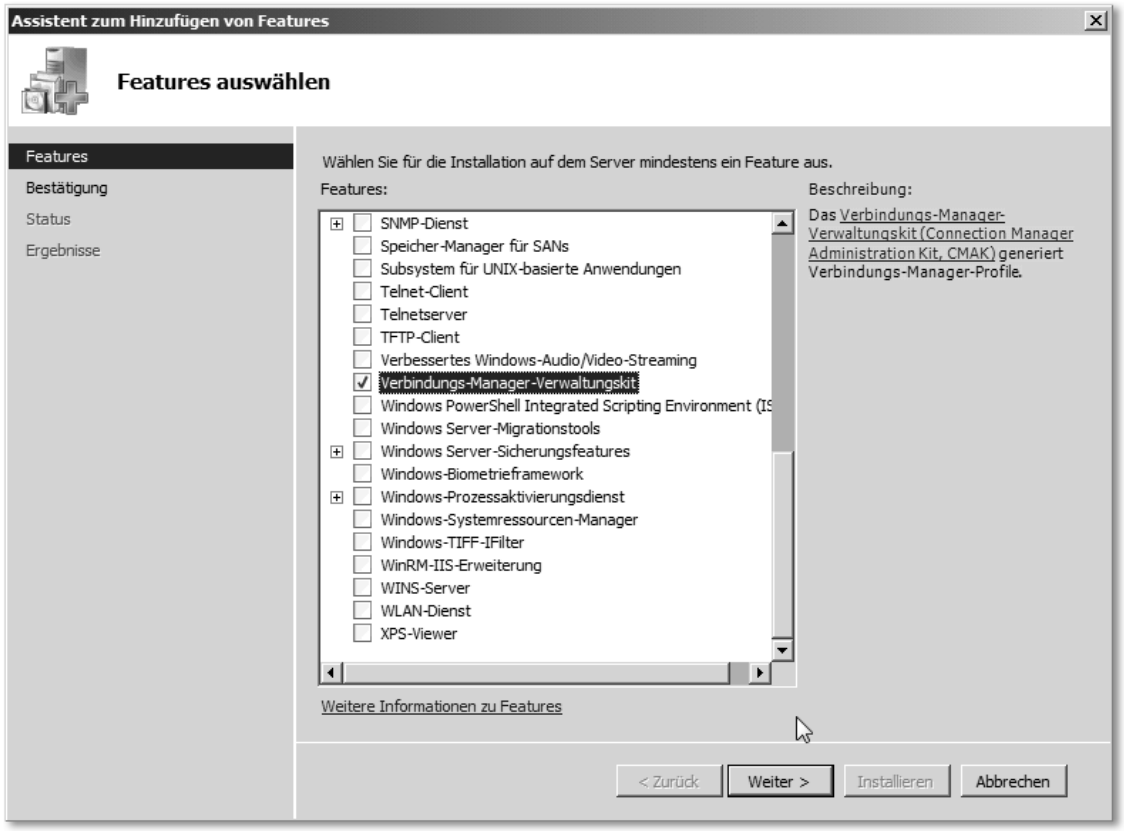


Abbildung 5.107 Das »Connection Manager Administration Kit« (CMAK) bzw. »Verbindungs-Manager-Verwaltungskit« ist ein Feature von Windows Server 2008.

Die erste sichtbare Komponente vom CMAK ist ein Assistent (Abbildung 5.108). Dieser Assistent ist ziemlich umfangreich, deshalb werde ich die notwendigen Eingaben nicht Schritt für Schritt durchgehen. Die Dialoge des Assistenten sind

zwar in ihrer Konsequenz nicht immer sofort völlig selbsterklärend, aber die Aufgabe ist für jeden Administrator lösbar.

Abbildung 5.108 Dieser Assistent erstellt ein Verbindungs-Manager-Profil.

Im Verlauf des Assistenten wird natürlich ein VPN-Eintrag erstellt – das ist ja auch der Zweck der Übung. In den Eigenschaften dieses Eintrags müssen Sie unter anderem eine VPN-Strategie konfigurieren (Abbildung 5.109).

Wie ich im vorherigen Abschnitt über den VPN-Typ beschrieben habe, ist beim Anlegen einer Verbindung mit dem VPN-Client von Windows 7 die Verbindungsreihenfolge beim VPN-Typ auf Automatisch festgelegt und kann nicht verändert werden. CMAK bietet mehr Konfigurationsmöglichkeiten, übrigens auch was Verbindungsthemen jenseits von VPN betrifft.

Nach dem Durcharbeiten des Assistenten wird eine EXE-Datei erstellt, die auf den Clients installiert werden kann und Verbindungen gemäß den im Assistenten getroffenen Einstellungen einrichtet (Abbildung 5.110). Die EXE-Datei kann mit einer Softwareverteilungslösung verteilt werden, und mit der Option `/Q` kann ein Quiet-Modus gewählt werden – wenn die Datei ohne den Parameter für den Quiet-Modus aufgerufen wird, erscheint zunächst die Abfrage aus Abbildung 5.110.

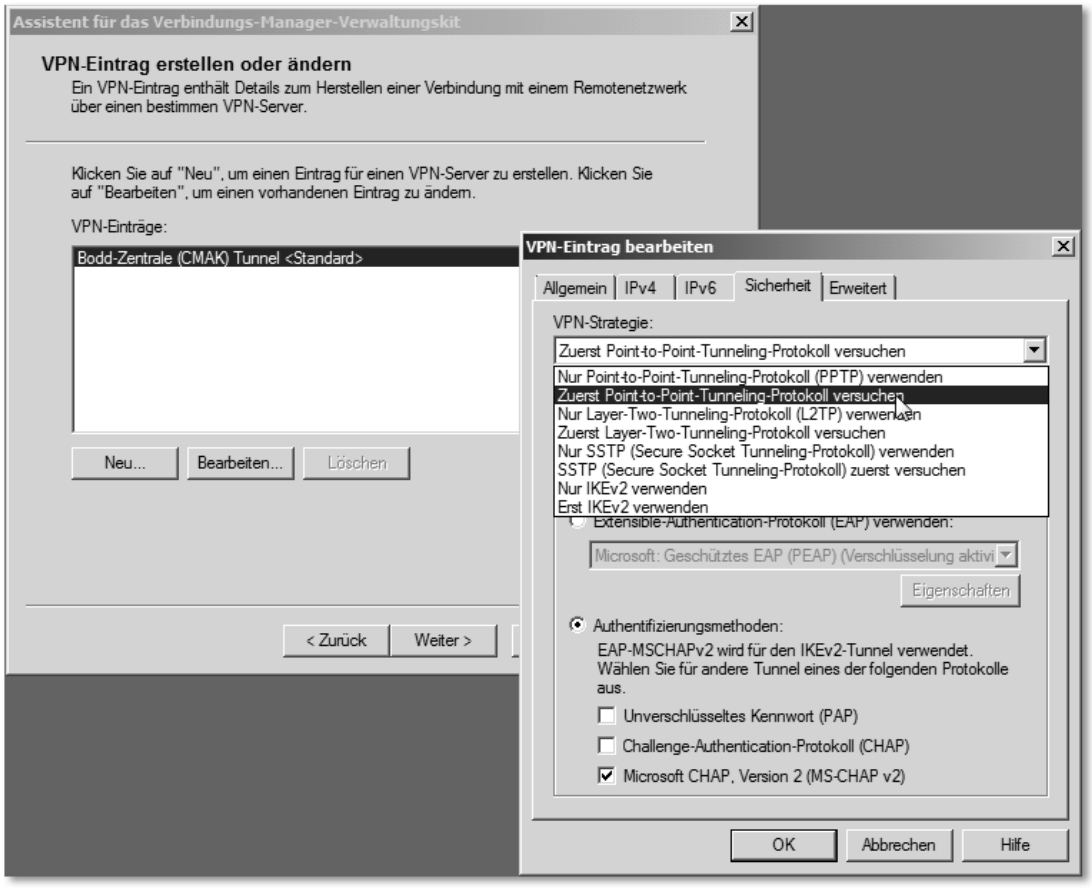


Abbildung 5.109 Sie können verschiedene VPN-Strategien konfigurieren.

Abbildung 5.110 Nach dem Durcharbeiten des Assistenten wird eine Installationsdatei erzeugt.

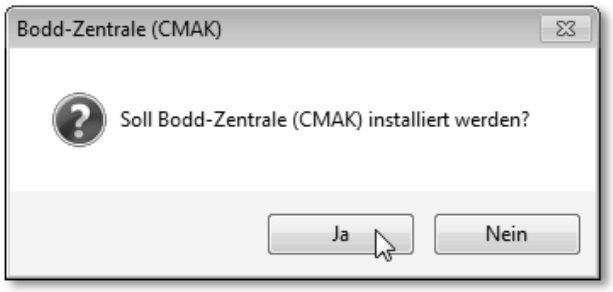


Abbildung 5.111 Wenn die EXE-Datei nicht im Quiet-Modus (»/Q«) aufgerufen wird, gibt es noch diesen Hinweis, bevor die Verbindung eingerichtet wird.

Im Verlauf des Assistenten können Sie übrigens diverse Einstellungen vornehmen, die so weit gehen, dass der Anmeldedialog mit veränderten Texten und auch Bildern versehen werden kann. Einen so gut wie nicht veränderten CMAK-Anmeldedialog sehen Sie in Abbildung 5.112 – er wurde optisch leicht modifiziert, aber ansonsten ist alles vorhanden.

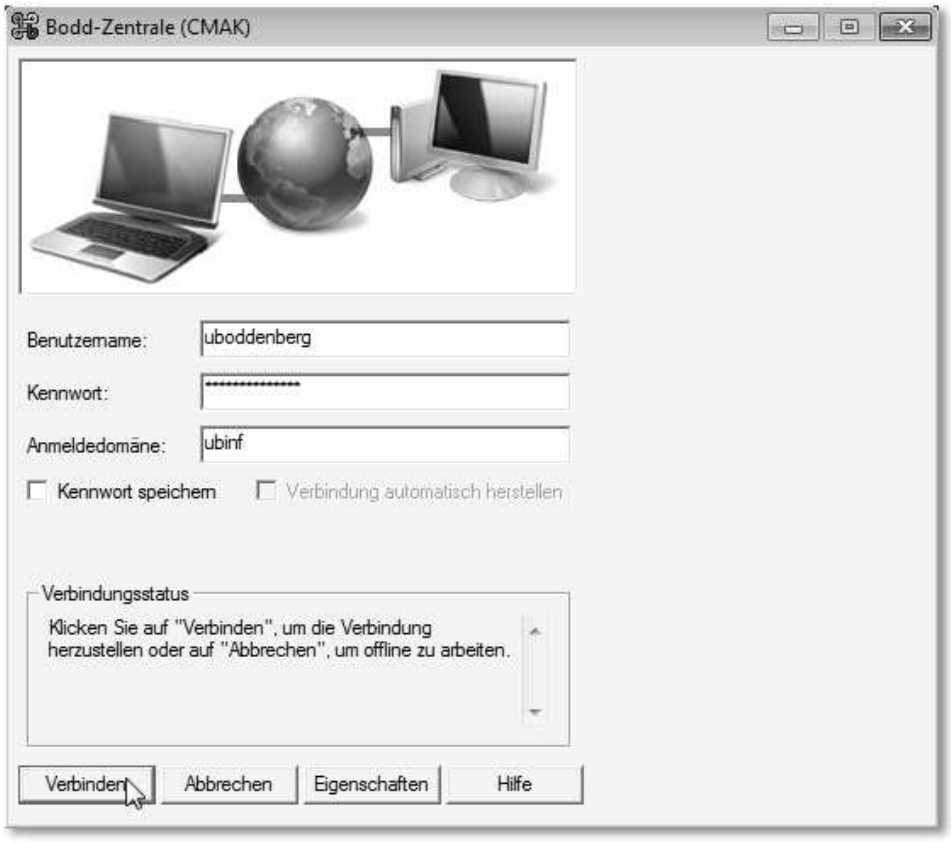


Abbildung 5.112 Dies ist der Dialog zum Verbindungsaufbau.

Dass eine mit CMAK eingerichtete Verbindung letztendlich ganz »normal« gehandhabt wird, sehen Sie in dem auf Abbildung 5.113 gezeigten Dialog zur Verwaltung und Auswahl der Verbindungen. Hinter dem Namen der Verbindung er-

scheint zwar ein anderes Symbol, die Funktionalität und Integration entspricht aber den Verbindungen, die in Windows 7 angelegt worden sind. (Das eingeklammerte Wort »CMAK« wird übrigens nicht automatisch vergeben, so habe ich vielmehr die einzurichtende Verbindung genannt.)

Abbildung 5.113 Die CMAK-Verbindung ist mit einem anderen Symbol gekennzeichnet.

Hinweisen möchte ich noch darauf, dass in den Eigenschaften einer mit CMAK angelegten Verbindung etwas andere Konfigurationsoptionen zur Verfügung stehen – genauer gesagt: weniger Konfigurationsoptionen. Der Benutzer hat beispielsweise nicht die Möglichkeit, die Verbindung umzukonfigurieren und beispielsweise den VPN-Typ oder die Authentifizierung zu ändern.

Nach seiner Rückkehr sinnt dieser durch die Gefahr, die ihn bedroht, und den erlittenen Schimpf bewogen auf Mittel, wie er sich für die Zukunft der Gewalt seines Bruders entziehen und, wo möglich, an seiner Statt König werden könne.

6 Deployment

Bevor der Benutzer mit dem Betriebssystem arbeiten kann, muss es installiert werden – das ist so weit einleuchtend. Wenn Sie Dutzende oder Hunderte von Installationen von Windows 7 durchführen müssen, spielt die Automatisierung und Vereinheitlichung des Installationsprozesses eine große Rolle. Einerseits soll die eigentliche Installation schnell und möglichst kostengünstig ablaufen, andererseits sollen die PCs auch in der Betriebsphase einfach zu warten und zu managen sein. Letzteres ist nur dann erreichbar, wenn alle Systeme identisch aufgesetzt sind, also nicht individuell über jeden PC nachgedacht werden muss.

Der Pflicht-Download für alle, die sich mit der automatisierten Installation von Windows 7 auseinandersetzen, ist das *Windows Automated Installation Kit* (WAIK), das auch in einer Version für Windows 7 vorliegt (Abbildung 6.1).

6.1 Einführende Überlegungen

Es gibt nun natürlich mehrere Wege, wie ein Betriebssystem auf den PC kommen kann. Sie müssen sich dabei aber stets die Frage stellen, wie gut die durchgeführte Installation dann letztendlich zu betreiben ist.

6.1.1 Standardisierung

Bevor wir in die Technik einsteigen, möchte ich ein wirklich wesentliches Thema erwähnen: die Standardisierung.

Dreh- und Angelpunkt sowohl eines effizienten Deployment-Prozesses als auch einer kostengünstigen Betriebsphase ist eine möglichst hohe Standardisierung der PCs – das betrifft sowohl die Hardware als auch die Art und Weise, wie das Betriebssystem installiert wird.

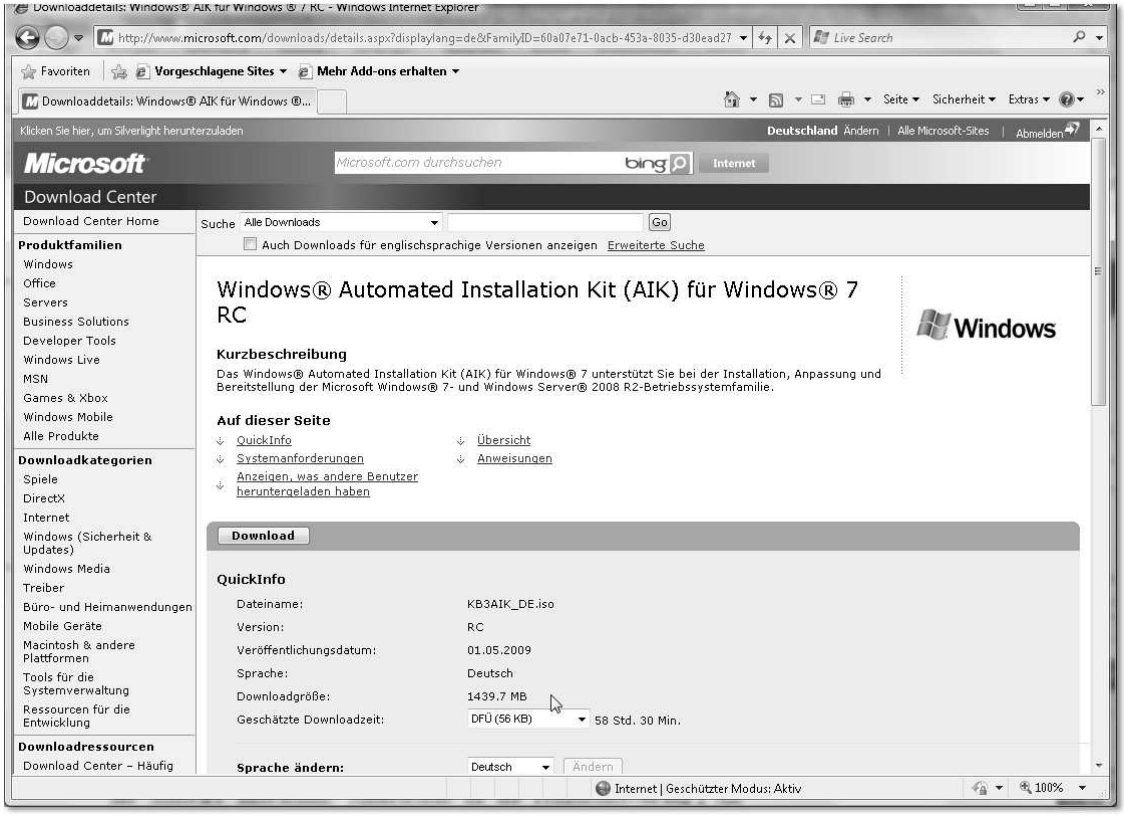


Abbildung 6.1 Pflicht-Download: WAIK for Windows 7

Im günstigsten Fall sieht jeder PC softwaremäßig gleich aus, sodass Sie einfach an einer Konsole auf einen Knopf drücken und zehn Minuten später ist ein PC aufgesetzt – einfach durch Installation des Standard-Images. So weitgehend wird eine Vereinheitlichung im Allgemeinen nicht möglich sein, da die Abteilungen unterschiedliche Anforderungen an die Applikationen haben. Somit gibt es für das optimale Szenario in der Praxis zwei Wege:

- Sie installieren immer dasselbe Image, das einen »Grundstandard« für das Unternehmen darstellt. Individuell benötigte Applikationen werden entsprechend nachinstalliert – im Optimalfall geschieht das automatisch.
- Sie arbeiten mit mehreren Images, verwenden also für jede Abteilung ein anderes Image.

Der erstgenannte Fall ist eigentlich der bessere, denn Sie müssen nicht mehrere Images pflegen und hätten vermutlich auch im zweiten Fall die Situation, dass bei dem einen oder anderen Anwender etwas nachinstalliert werden muss.

6.1.2 Lokale Daten und Profile

Beim Austausch von PCs oder auch bei einer Neuinstallation eines bestehenden PCs im Fehler- oder Upgrade-Fall stellen lokal auf dem PC vorhandene Daten eine wesentliche »Bremse« dar. Diese müssen gesichert und auf den neuen PC übertragen werden, wobei erschwerend hinzukommt, dass dies mit Profilen nicht so ganz simpel ist. Optimalerweise sollte es also keine Benutzerdateien auf PCs geben, was in der Praxis bedeutet:

- Sorgen Sie dafür, dass die Benutzer gar nicht erst in Versuchung geführt werden, Dateien lokal abzuspeichern. Dies lässt sich einerseits durch eine entsprechend restriktive Vergabe von Dateisystemberechtigungen erzwingen, andererseits sollte auch jeder Benutzer darauf hingewiesen werden, dass es streng verboten (!) ist, Dateien lokal zu speichern.
- Verwenden Sie servergespeicherte Profile (*Roaming Profiles*).

Bei den servergespeicherten Profilen schwingt immer ein wenig der Gedanke mit, dass diese in erster Linie dazu dienen, dass Benutzer sich an beliebigen PCs im Unternehmen anmelden können und trotzdem stets ihre Einstellungen zur Hand haben. Ja, das ist ein Aspekt – dieser spielt meiner Erfahrung nach aber nur selten wirklich eine Rolle. Wichtig im Zusammenhang mit servergespeicherten Profilen sind aber die »implizite Sicherung« des Profils und die deutliche Vereinfachung im Fall eines Austauschs oder einer Neuinstallation des PCs.

Weitere Informationen

Mehr zum Thema Profile finden Sie auch in Abschnitt 5.2.

6.1.3 Vorinstallierte Versionen und Re-Imaging-Recht

Wenn Sie nicht als Großabnehmer PCs ohne vorinstalliertes Betriebssystem kaufen, wird es auf Ihren Geräten bereits ein Windows 7 geben. Warum also nicht einfach den PC einschalten, 15 Minuten warten, bis das vorinstallierte Betriebssystem eingerichtet ist und den Benutzer losarbeiten lassen?

Ein wesentliches Problem ist, dass die vorinstallierten Images mit Sicherheit nicht gemäß Ihrer Vorgaben bzw. Vorstellungen eingerichtet sein werden. Vermutlich installieren Sie standardmäßig keine Spiele und Testversionen von Virenscannern und Bildbearbeitungswerkzeugen mit. Dafür möchten Sie vielleicht andere Software einfügen, wie beispielsweise den Adobe Reader.

Zu bedenken ist auch, dass bei der Beschaffung von PCs zu unterschiedlichen Zeitpunkten vermutlich auch leicht unterschiedliche Vorinstallationen geliefert werden.

Eventuell entspricht auch die Partitionierung nicht Ihren Vorstellungen oder Sie möchten den Beitritt zur Domäne optimieren – kurzum: Es gibt viele Gründe dafür, nicht einfach die vorinstallierte Version zu verwenden.

Wenn Sie sich dafür entscheiden, das Betriebssystem neu zu installieren und dabei eine Volumenlizenzversion aufspielen, stellt sich die Frage nach den lizenzrechtlichen Aspekten.

Grundsätzlich gewährt Microsoft Volumenlizenzkunden (!) das Recht auf *Re-Imaging*. Vereinfacht gesagt bedeutet dies, dass beispielsweise auf einem PC, der vom Hersteller mit einer Windows 7-Business-Lizenz verkauft worden ist, ein Image aufgebracht werden darf, das von einem Windows 7-Business-Volumenlizenzdatenträger installiert wurde. Die Bedingungen für die legale, also lizenzbestimmungskonforme Nutzung des Re-Imaging-Rechts sind relativ eng:

- Re-Imaging ist nur erlaubt, wenn das zu installierende Image mit einem legal erworbenen Volumenlizenzdatenträger erstellt worden ist, also im Rahmen des Volumenlizenzvertrags.
  Ein Re-Imaging auf ein mit einem OEM/SB/FPP-Datenträger erstelltes Image ist in jedem Fall verboten. (Zu den Abkürzungen siehe den grauen Kasten weiter unten.)
- Die für den PC lizenzierte Betriebssystemversion und das via Image installierte Betriebssystem müssen dieselben Editionen sein. Ein Re-Imaging vom *Windows 7 Home* auf *Windows 7 Business* ist beispielsweise nicht zulässig.
- Selbstverständlich müssen auch die Produktversionen übereinstimmen. Eine für einen PC vorhandene Windows-Vista-Lizenz kann nicht mit Windows 7 re-imagt werden. Das ist aber wohl einleuchtend.
- Beim Re-Imaging müssen die Sprachen übereinstimmen. Ein Re-Imaging einer deutschen *Windows 7-Business*-Lizenz auf ein englisches *Windows 7 Business* ist nicht erlaubt.

Lizenzierung

Dieses Buch kann eine fundierte Lizenzberatung nicht ersetzen. Die Aussagen, die ich hier zur Lizenzierung mache, könnten von Microsoft kurzfristig geändert werden, außerdem könnten Ihr Volumenlizenzvertrag oder Ihre Einzellizenzen speziellen Bedingungen unterliegen.

Eine recht lesenswerte Einführung in das Thema Re-Imaging finden Sie hier: *http://download.microsoft.com/download/3/D/4/3D42BDC2-6725-4B29-B75A-A5B04179958B/Reimaging.docx*

Weiter vorn sind einige Typen von Einzellizenzen erwähnt; hier eine kurze Zusammenfassung:

- *FPP* (*Full Packaged Product*): Hierbei handelt es sich um die klassischen Einzellizenzen. Wenn Sie in die Computerabteilung eines Kaufhauses gehen und ein Windows 7-Paket (mit buntem Karton) erwerben, wird es sich um ein Full Packed Product handeln.
- *OEM* (*Original Equipment Manufacturer*): Diese Produkttypen finden sich vorinstalliert auf Marken-PCs.
- *SB* (*System Builder*). Diese Produktversionen wird von Fachhändlern mit »selbstgebauten« PCs vertrieben und ist somit auch für die Vorinstallation vorgesehen.

6.1.4 Der Deployment-Prozess

Wenn Sie ein zu verteilendes Image erstellt haben, müssen Sie entscheiden, wie Sie es auf die PCs aufbringen möchten. Es gibt dazu zwei Methoden:

- Sie starten den PC, auf dem Sie Windows 7 installieren wollen, von einem startfähigen, eventuell temporär angeschlossenen Medium, beispielsweise einer USB-Platte oder auch einer DVD.
- Sie booten aus dem Netz.

Eine dritte Variante wäre freilich die Installation direkt von der Original-Windows 7-DVD, aber diese Variante dürfte in der Unternehmenspraxis wirklich nur eine sehr untergeordnete Rolle spielen.

Die meisten Kunden erstellen heute ein Image, das zum Rollout neuer PCs oder zum Neuinstallieren von vorhandenen PCs verwendet wird. Nun ist noch zu entscheiden, wie das Image auf einen PC gebracht werden soll:

- Sie können über das Netzwerk booten (PXE-Boot) und direkt vom Server installieren.
- Sie booten über ein Medium und führen die Installation auch von diesem aus. Das besagte Medium könnte eine bootfähige DVD, eine USB-Wechselplatte oder dergleichen sein.

Eine weitere wichtige Entscheidung ist, ob Sie die PCs zunächst in der IT auspacken und installieren möchten und dann den fertig installierten PC zum Anwender bringen oder ob die Installation des PCs beim Anwender stattfinden soll. Der »klassische« Fall ist die Vorbereitung der PCs im IT-Labor, allerdings erscheint mir das heute gar nicht der zeitsparendste Weg zu sein. Eine Netzwerkinstallation von einem Image geht so schnell, dass durchaus folgende Vorgehensweise denkbar ist:

- Der Techniker geht mit dem neuen PC zum Arbeitsplatz des Anwenders.
- Der alte PC wird abgebaut und der neue angeschlossen.
- Der neue PC wird gestartet, bootet aus dem Netz und führt die Installation durch.

- In dieser Zeit verpackt der Techniker den alten PC, kümmert sich um das saubere Verlegen von Kabeln, regelt Formalitäten mit dem Anwender und tut dergleichen mehr.

Während der Techniker mit dem letztgenannten Schritt beschäftigt ist, dürfte auch die Installation durchgelaufen sein. Nun werden unter Umständen die Nachinstallation von Anwendungen und Patches die Installationszeit verlängern, trotzdem dürfte in vielen Fällen der Gesamtprozess nicht allzu lange dauern.

Wenn der Techniker an jedem einzelnen PC noch zwei Stunden herumbasteln muss, dann wird die Installation beim Anwender nicht funktionieren. Es stellt sich dann allerdings die Frage, ob es nicht erforderlich ist, das Thema Standardisierung nochmals genau aufzugreifen.

6.2 WAIK installieren und Testumgebung

Der erste Schritt ist die Installation des *Windows Automated Installation Kit* (WAIK). Dieses enthält einerseits verschiedene Dokumentationen, andererseits einige Werkzeuge, unter anderem den Windows-Systemabbild-Manager, mit dem sich Definitionsdateien für die unbeaufsichtigte Installation erzeugen lassen. Das WAIK ist als Download erhältlich (siehe auch Abbildung 6.1), die Installation startet mit dem Dialog aus Abbildung 6.2. Für eine initiale Installation wählen Sie den Menüpunkt WINDOWS AIK-SETUP.

Abbildung 6.2 Installation des Windows Automated Installation Kit (WAIK)

Da die WAIK-Installation problemlos durchläuft, lautet die Frage eigentlich nicht, *wie* man es installiert, sondern vielmehr *wohin*. Das hört sich zunächst irgendwie trivial an, aber die Frage ist durchaus begründet.

Das WAIK gehört auf den PC, mit dem der jeweilige Administrator das Deployment verwaltet. Auf diesen PC werden Sie gegebenenfalls noch einige andere Dinge installieren, beispielsweise eine Software zum Erstellen und Modifizieren von ISO-Images und ähnliche Werkzeuge. Dieser PC kann durchaus Ihr »normaler« Admin-Arbeitsplatz sein, es hat sich in der Praxis aber durchaus bewährt, eine separate Maschine dafür vorzusehen. Der Grund ist simpel: In etwas größeren Unternehmen arbeiten häufig mehrere Leute an einem Thema, wobei es dann hilfreich ist, wenn hierfür ein gemeinsamer PC genutzt werden kann, auf dem »alles drauf« ist. Dieser PC kann übrigens auch eine virtuelle Maschine sein.

Wenn Sie Installationen testen oder eine Master-Installation erzeugen möchten, können Sie als Ziel ebenfalls mit virtuellen Maschinen arbeiten. Dies ist durchaus sinnvoll, denn man kann schnell Zwischenstände wegsichern, Snapshots anfertigen und zurückholen und dergleichen mehr. Der große Nachteil ist, dass Sie im Normalfall irgendwann die Hardware ins Spiel bringen müssen, was insbesondere die Installation von Treiberpaketen bedeutet. Grundsätzlich ist es aber kein schlechter Weg, zunächst mit einer virtuellen »Zielumgebung« zu arbeiten und dann erst in der Endphase mit PC-Hardware zu validieren und gegebenenfalls Ergänzungen vorzunehmen. Die erwähnten Möglichkeiten wie das Erstellen von Snapshots führen schon zu einem deutlichen Produktivitätsgewinn – ansonsten sind Sie ständig damit beschäftigt, mit einem Imaging-Tool (z. B. *Ghost, TrueImage*) Zwischenstände zu sichern.

Noch ein Hinweis

Das WAIK muss auf einem Admin/Techniker-PC installiert werden, es kommt keinesfalls auf die Zielmaschine!

6.3 Installationsimage vorbereiten – erster Durchlauf

Sie können Windows 7 natürlich ganz klassisch mit einer unbeaufsichtigten Installation von DVD auf die Maschine bringen. Der schnellere Weg ist aber definitiv die Nutzung des mit Windows 7 eingeführten WIM-Imageformats. WIM steht für *Windows Imaging Format* – den Umgang mit WIM und etliche Möglichkeiten dieses Formats nebst den dazu passenden Werkzeugen führe ich Ihnen im Verlauf des Kapitels vor.

Um zu einem WIM-Installation-Image zu kommen, beschreibt Microsoft im WAIK einen Weg, der zunächst mit einer unbeaufsichtigten Installation beginnt. Ich zeige Ihnen hier mehr oder weniger den im WAIK dokumentierten Weg. Wenn das erste Image dann erstellt ist, wird es um weitere Anpassungen, das Hinzufügen von Treibern und einiges andere mehr gehen.

In diesem ersten Durchlauf werden Sie auch einige im WAIK enthaltenen Werkzeuge kennenlernen, wie beispielsweise den *Windows System Image Manager* (WSIM) oder ein Kommandozeilenwerkzeug zum Erzeugen eines WinPE-Start-WIMs.

6.3.1 Antwortdatei vorbereiten

Der erste Schritt ist das Erzeugen einer Antwortdatei, um eine automatische Installation des Betriebssystems durchzuführen. Wer bereits Antwortdateien für automatische Installationen erstellt hat, erinnert sich an Textdateien und die Arbeit mit *Notepad.exe*. Seit Windows Vista (und damit erst recht mit Windows 7) geht das deutlich komfortabler:

- Als Antwortdatei wird ein XML-Dokument verwendet.
- Zur Erstellung des Antwort-XML-Dokuments enthält das WAIK den *Windows System Image Manager* (WSIM).

Bevor Sie nun WSIM starten, sollten Sie das Installations-Image von der Windows 7-DVD in das lokale Dateisystem Ihres Arbeits-PCs (also des PCs mit dem installierten WAIK) kopieren. Die Datei heißt *install.wim* und befindet sich im Verzeichnis */sources* der DVD. Sie ist ungefähr drei Gigabyte groß.

Dann starten Sie den WSIM und wählen zunächst den Menüpunkt Windows-Abbild auswählen (Abbildung 6.3).

In einer WIM-Datei können mehrere Abbilder vorhanden sein, was bei der *install.wim* übrigens auch der Fall ist. Somit wird WSIM zunächst erfragen, welches in der WIM-Datei vorhandene Abbild verwendet werden soll (Abbildung 6.4).

Hinweis

Der Screenshot wurde mit einem Retail-Datenträger des *Release Candidate* aufgenommen. Ein Volumenlizenz-Datenträger der finalen Version wird dann selbstverständlich auch die übrigen Versionen, insbesondere *Business* und *Enterprise* enthalten.

WSIM wird sich zunächst beschweren, dass keine Katalogdatei vorhanden ist (Abbildung 6.5). Entscheiden Sie sich einfach für das Erstellen einer solchen. Je nach Schnelligkeit der Festplatte kann das Erstellen durchaus eine Weile dauern – Sie haben also Zeit für eine Kaffeepause.

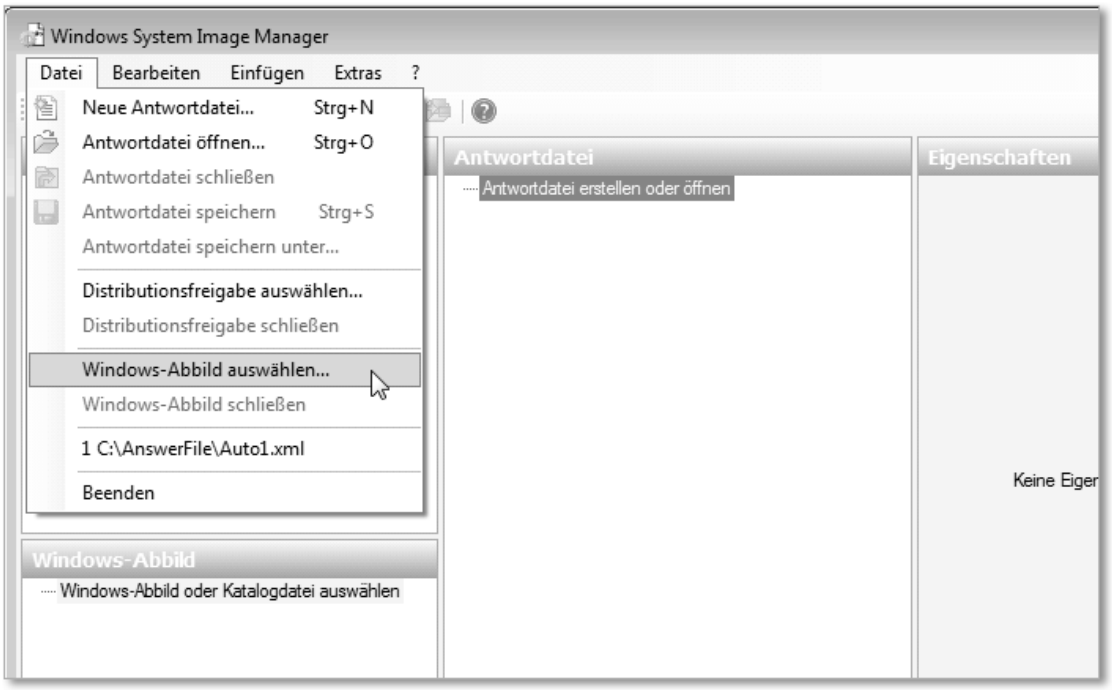


Abbildung 6.3 Der erste Schritt im WSIM ist das Auswählen eines Windows-Abbilds.

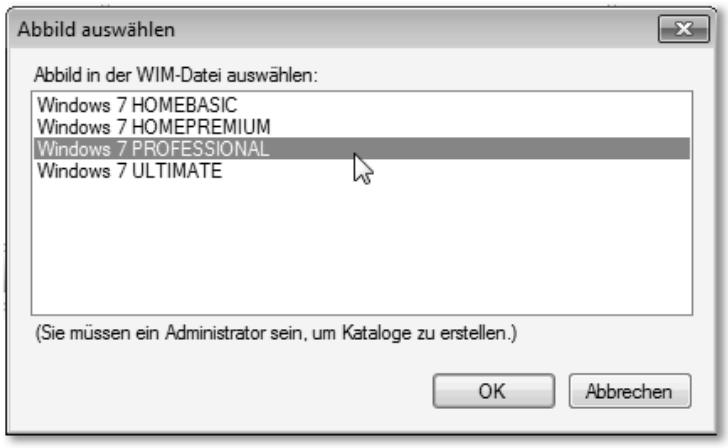


Abbildung 6.4 In der WIM-Datei sind mehrere Abbilder vorhanden – wählen Sie eines davon aus.

Ist die Katalogdatei erstellt, werden im Fenster Windows-Abbild diverse Konfigurationskomponenten angezeigt werden. Dies sind die Einstellungen, die Sie später der Antwortdatei übergeben können. Blättern Sie ruhig einmal in den möglichen Einstellungen. Sie werden sehen, dass dort so ziemlich alles auswählbar ist, was man sich in puncto Betriebssysteminstallation vorstellen kann (Abbildung 6.6).

Der nächste Schritt ist das Anlegen einer neuen Antwortdatei. Rufen Sie dazu den gleichnamigen Menüpunkt auf. Das Ergebnis ist, dass im WSIM eine leere Antwortdatei angezeigt wird, in der sieben Konfigurationsphasen zu sehen sind (Abbildung 6.7).

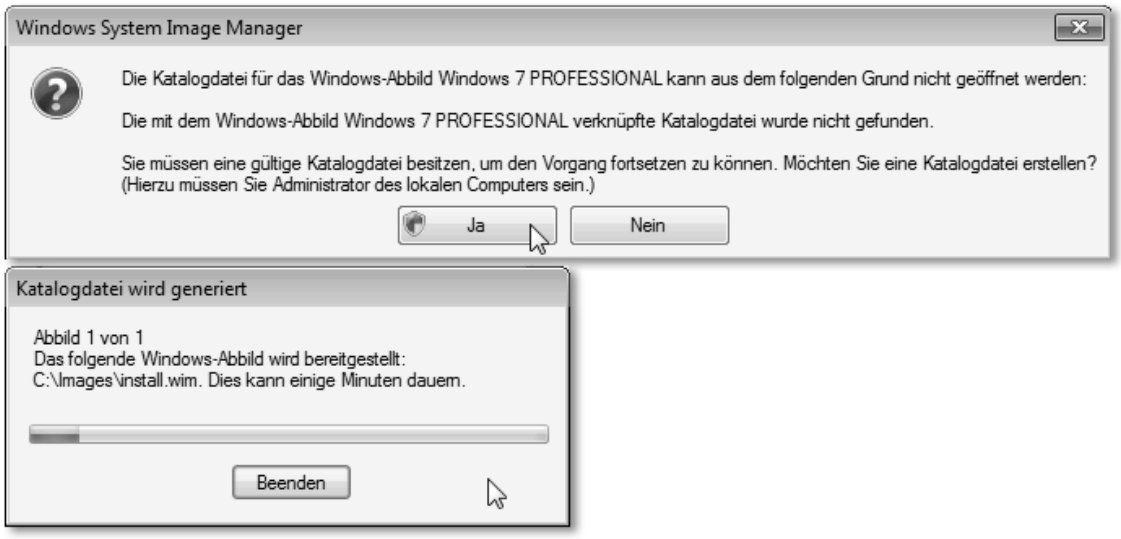


Abbildung 6.5 Zunächst muss der Katalog erstellt werden.
Kurz gesagt: Das kann lange dauern.

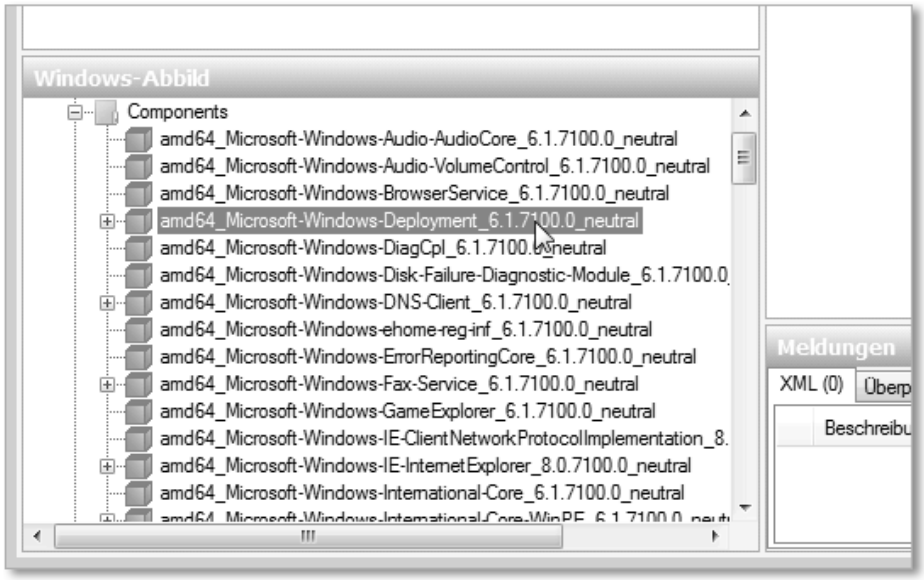


Abbildung 6.6 Ist der Katalog erstellt, werden die konfigurierbaren Komponenten angezeigt.

In diesen Konfigurationsphasen werden im nächsten Schritt die Einstellungen konfiguriert, die Sie in der Antwortdatei vornehmen wollen.

Um der Antwortdatei eine Einstellung hinzuzufügen, selektieren Sie die Einstellung zunächst im Fenster Windows-Abbild und fügen sie dann mittels des entsprechenden Punkts im Kontextmenü zur Antwortdatei hinzu. Abbildung 6.8 zeigt, wie es gemacht wird. Beachten Sie, dass es Einstellungen gibt, die in mehreren Konfigurationsphasen der Antwortdatei möglich sind.

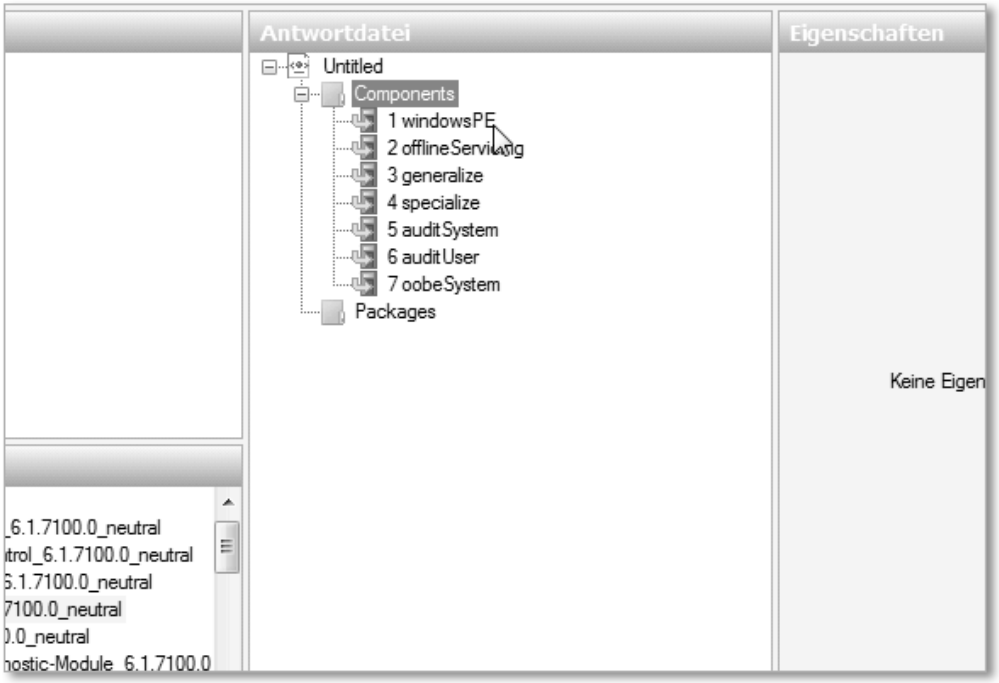


Abbildung 6.7 Eine leere Antwortdatei wartet auf »Befüllung«. Sie ist in sieben Konfigurationsphasen gegliedert.

Beim Hinzufügen müssen Sie also darauf achten, den richtigen Menüpunkt zu selektieren. Ansonsten gibt es unter Umständen merkwürdige Verhaltensweisen, nach denen man genauso lange wie verzweifelt suchen kann.

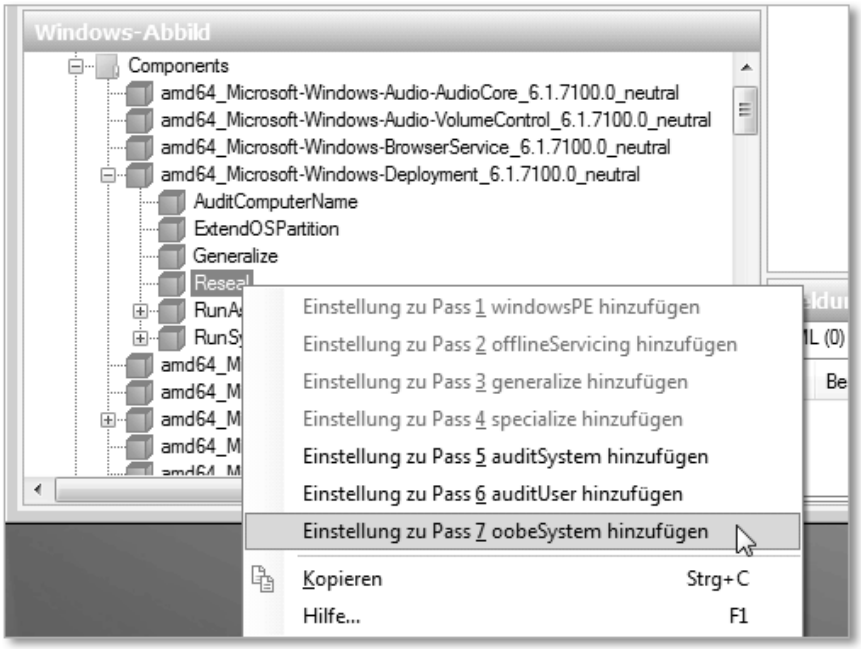


Abbildung 6.8 Hinzufügen von Einstellungen zur Antwortdatei

Um eine funktionierende Antwortdatei für diesen initialen Durchlauf zu verwenden, fügen Sie die in Tabelle 6.1 genannten Komponenten den entsprechenden Konfigurationsphasen der Antwortdatei hinzu.

Festplattenlayout

Wie ich bereits zu Beginn erwähnt habe, orientiert sich die hier gezeigte Vorgehensweise am Beispiel des WAIKs. In diesem wird die Festplatte in zwei Partitionen unterteilt: in eine kleine 200 MB große Partition und eine, die den Rest der Platte einnimmt. Dieses Festplattenlayout macht dann Sinn, wenn Sie die BitLocker-Verschlüsselung verwenden möchten.

Komponente	Konfigurationsphase
Microsoft-Windows-Deployment\Reseal	oobeSystem
Microsoft-Windows-International-Core-WinPE\SetupUILanguage	windowsPE
Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions\CreatePartition	windowsPE
Microsoft-Windows-Setup\DiskConfiguration\Disk\ModifyPartitions\ModifyPartition	windowsPE
Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions\CreatePartition	windowsPE
Microsoft-Windows-Setup\DiskConfiguration\Disk\ModifyPartitions\ModifyPartition	windowsPE
Microsoft-Windows-Setup\ImageInstall\OSImage\InstallTo	windowsPE
Microsoft-Windows-Setup\UserData	windowsPE
Microsoft-Windows-Shell-Setup\OOBE	oobeSystem
Optional: Microsoft-Windows-IE-InternetExplorer	specialize

Tabelle 6.1 Diese Komponenten werden zu der Antwortdatei hinzugefügt.

Wenn Sie die Komponenten hinzugefügt haben, sollte die Antwortdatei in etwa so aussehen wie in Abbildung 6.9. Die in der Antwortdatei definierte Vorgehensweise lässt sich nun anhand der Konfigurationsphasen recht gut erkennen:

- In der ersten Phase (WINDOWSPE) wird die Festplatte eingerichtet und das Image installiert.
- In einer späteren Phase (SPECIALIZE) werden einige Einstellungen vorgenommen, hier wird beispielsweise der Internet Explorer vorkonfiguriert.

- In der letzten Phase (oobeSystem, Out of Box Experience) wird hier konfiguriert, dass der Computer nicht nach der Installation heruntergefahren und dabei auf »Grundeinstellungen« zurückgesetzt werden soll.

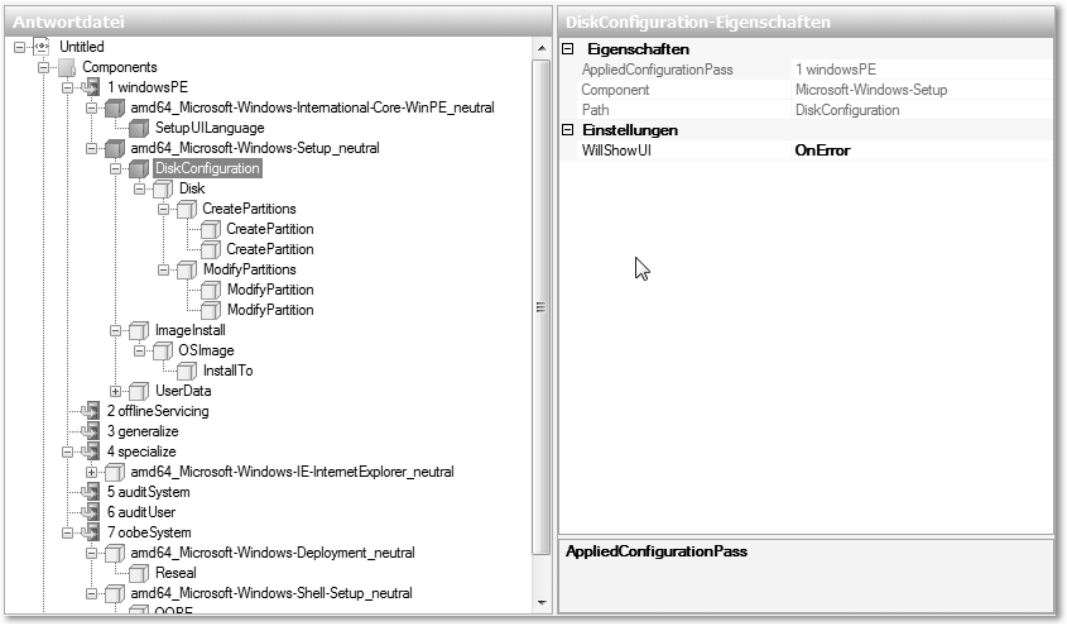


Abbildung 6.9 So sollte die Antwortdatei angezeigt werden, wenn alle Komponenten hinzugefügt worden sind.

Abbildung 6.10 zeigt, wie man den Eigenschaften der Komponenten Werte zuweist. Teilweise finden sich Comboboxen mit vordefinierten Werten; die meisten Eingabemöglichkeiten sind jedoch einfache Textfelder, die Zahlen- oder Stringwerte aufnehmen. Es ist übrigens nicht erforderlich, alle Werte zu setzen. Ist ein Wert nicht vorhanden, erscheint er nicht in der Antwortdatei, und es wird ein Standardwert herangezogen – oder eine Option bleibt unkonfiguriert.

Für dieses Szenario sollen die in Tabelle 6.2 aufgeführten Werte gesetzt werden. Insbesondere geht es hier um die Lokalisierung und das Anlegen der Partitionen auf der Festplatte.

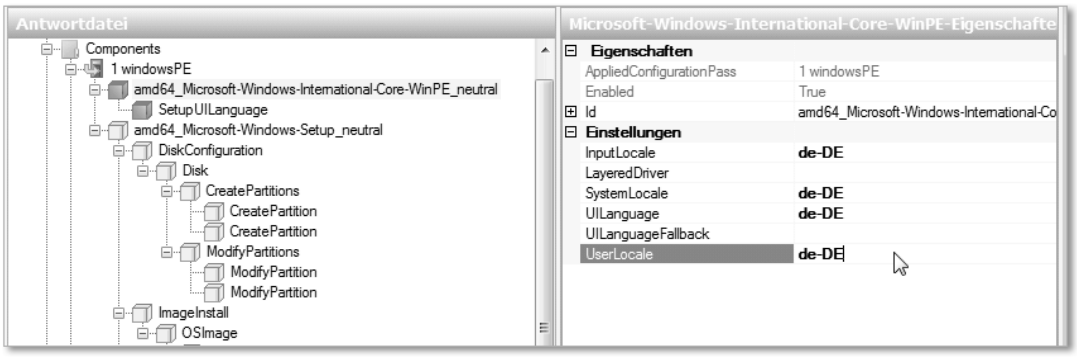


Abbildung 6.10 Den Eigenschaften Werte zuweisen

Konfigurationsphase	Komponente	Wert
1 WindowsPE	Microsoft-Windows-International-Core-WinPE	InputLocale = *<Eingabegebietsschema>* Beispiel: de-DE SystemLocale = *<Systemgebietsschema>* Beispiel: de-DE UILanguage = *<Benutzeroberflächensprache>* Beispiel: de-DE UserLocale = *<Benutzergebietsschema>* Beispiel: de-DE
1 WindowsPE	Microsoft-Windows-International-Core-WinPE\SetupUILanguage	UILanguage = *<Benutzeroberflächensprache>* Beispiel: de-DE
1 WindowsPE	Microsoft-Windows-Setup\DiskConfiguration	WillShowUI = OnError
1 WindowsPE	Microsoft-Windows-Setup\DiskConfiguration\Disk	DiskID = 0 WillWipeDisk = true
1 WindowsPE	Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions\CreatePartition	Order = 1 Size = 200 Type = Primary
1 WindowsPE	Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions\CreatePartition	Extend = true Order = 2 Type = Primary
1 WindowsPE	Microsoft Windows Setup\DiskConfiguration\Disk\ModifyPartitions\ModifyPartition	Active = true Format = NTFS Label = System Order = 1 PartitionID = 1
1 WindowsPE	Microsoft Windows Setup\DiskConfiguration\Disk\ModifyPartitions\ModifyPartition	Format = NTFS Label = Windows Order = 2 PartitionID = 2
1 WindowsPE	Microsoft Windows-Setup\ImageInstall\OSImage	InstallToAvailablePartition = false WillShowUI = OnError
1 WindowsPE	Microsoft-Windows-Setup\ImageInstall\OSImage\InstallTo	DiskID = 0 PartitionID = 2

Tabelle 6.2 Diese Werte sollen für die Eigenschaften der Komponenten gesetzt werden.

Konfigurations-phase	Komponente	Wert
1 WindowsPE	Microsoft-Windows-Setup\UserData	`AcceptEula = true`
1 WindowsPE	Microsoft-Windows-Setup\UserData\ProductKey	`Key = <Product Key>` `WillShowUI = OnError`
4 Specialize	*Optional:* Microsoft-Windows-IE-InternetExplorer	`Home_Page = <Startseite des Unternehmens>`
7 oobeSystem	Microsoft-Windows-Deployment\Reseal	`ForceShutdownNow = false` `Mode = Audit`
7 oobeSystem	Microsoft-Windows-Shell-Setup\OOBE	`HideEULAPage = true` `ProtectYourPC = 3`

Tabelle 6.2 Diese Werte sollen für die Eigenschaften der Komponenten gesetzt werden.

Eine durchaus hilfreiche Funktion ist die Überprüfung der Antwortdatei, die Sie über den Menüpunkt EXTRAS • ANTWORTDATEI ÜBERPRÜFEN starten. Abbildung 6.11 zeigt das Ergebnis des Vorgangs in meinem Fall. Es gibt zwar diverse Warnungen, diese beziehen sich allerdings sämtlich darauf, dass eine Einstellung nicht geändert wurde – das ist durchaus eine Warnung wert, muss aber nicht zwingend korrigiert werden. Durch einen Mausklick auf die Meldung wechseln Sie übrigens zu der entsprechenden Position im Bearbeitungsfenster der Antwortdatei.

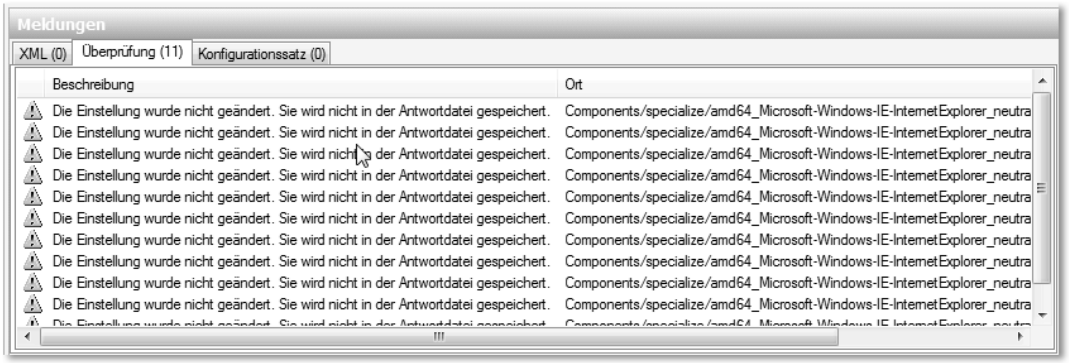


Abbildung 6.11 Das Überprüfen der Antwortdatei fördert eventuell Warnungen und Fehler zutage.

Anzumerken wäre, dass die Überprüfung zwar »technische« Fehler herausfindet, allerdings nicht dafür garantieren kann, dass die Datei letztendlich das bewirkt, was Sie vorhaben.

Der nächste Schritt ist das Speichern der mühevoll erstellten Antwortdatei – und zwar unter dem Namen *autounattend.xml*. Speichern Sie die Datei zunächst einfach im lokalen Dateisystem, an die richtige Stelle verschieben wir sie gleich im

Anschluss. Wenn Sie die Datei öffnen, beispielsweise mit dem Internet Explorer, sehen Sie ein lupenreines XML-Dokument (Abbildung 6.12). Für diejenigen unter Ihnen, die noch mit Windows XP-Antwortdateien gearbeitet haben, beginnt also die Zeit des Umlernens. Da die strukturierten XML-Dokumente eigentlich nur Vorteile haben, sollte das aber kein sonderlich schmerzhafter Prozess sein.

Abbildung 6.12 So sieht die erzeugte Antwortdatei aus – ein XML-Dokument.

6.3.2 Installation durchführen

Nun wird mithilfe der frisch erzeugten Antwortdatei eine Installation von Windows 7 durchgeführt. Zunächst stellt sich aber die Frage: Wohin mit der *autounattend.xml*? Windows 7 sucht, wie auch übrigens Windows Vista, die *autounattend.xml* im Root-Verzeichnis der am PC angeschlossenen Wechseldatenträger. In der WAIK-Dokumentation wird stets vorgeschlagen, die Datei auf einen USB-Stick zu kopieren. Grundsätzlich ist das auch eine gute Idee, es klappt aber nicht, wenn Sie die Vorbereitung der Image-Installationen in virtuellen Maschinen durchführen. Die meisten Virtualisierungsprodukte können USB-Sticks nicht – oder zumindest nicht ohne Zusatzsoft- und -hardware – den virtuellen Maschinen zur Verfügung stellen.

Als Alterantive bleibt »der Klassiker« unter den Wechseldatenträgern, nämlich die gute alte Diskette, die von allen wesentlichen Virtualisierungsprodukten unterstützt wird. Kopieren Sie also die *autoattend.xml*-Datei auf die virtuelle Diskette, und legen Sie diese in die virtuelle Maschine für die Testinstallation des Betriebssystems ein. Auf Abbildung 6.14 sehen Sie, wie das mit Hyper-V gemacht wird.

Einmal abgesehen von der Antwortdatei wird nur die Windows 7-DVD benötigt, von der gebootet wird. Eine Eingabe wird erforderlich sein, wenn es um die Auswahl der zu installierenden Betriebssytem-Edition geht (Abbildung 6.15).

Abbildung 6.13 Die Antwortdatei muss auf einem Wechseldatenträger gespeichert werden, zum Beispiel auf einer Diskette.

Abbildung 6.14 Einlegen einer Diskette in eine Hyper-V-VM

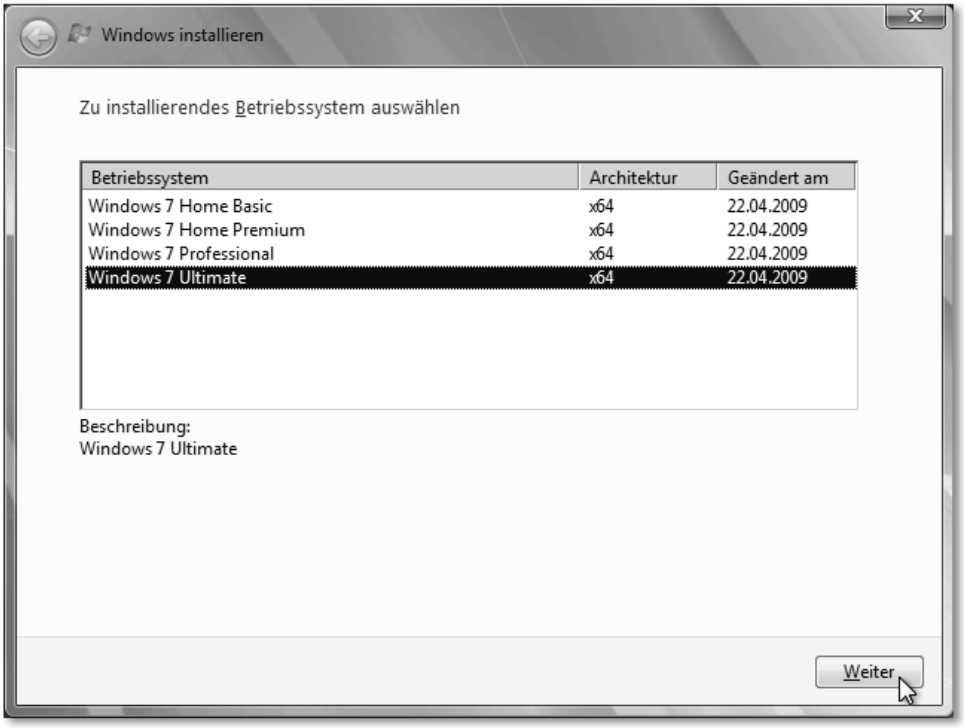


Abbildung 6.15 Mit der »autoattended.xml« muss nur die Betriebssystem-Version gewählt werden.

Ansonsten läuft die Installation vollkommen automatisch und ohne jede weitere Benutzerinteraktion ab.

6.3.3 Installation anpassen und verallgemeinern

Wenn die Installation abgeschlossen ist, werden Sie in etwa die in Abbildung 6.16 gezeigte Situation vorfinden: Auf dem PC ist der lokale Administrator eingeloggt, außerdem ist das Systemvorbereitungsprogramm *Sysprep* gestartet worden.

Abbildung 6.16 Wenn der Installationsvorgang beendet ist, ist auf dem PC der Administrator eingeloggt und Sysprep gestartet.

Vielleicht verspüren Sie den Drang zu prüfen, ob die *autoattend.xml*-Datei wirklich verwendet worden ist. Es gibt natürlich Hunderte von Aspekten, die man überprüfen könnte – zwei davon möchte ich Ihnen kurz vorstellen:

- Sie können sich die Partitionierung der Festplatte anschauen. Wenn alles geklappt hat, dann werden auf der ersten Festplatte zwei Partitionen vorhanden sein, von denen die erste 200 MB groß ist. Abbildung 6.17 zeigt, dass alles funktioniert hat.
- Die noch etwas »wissenschaftlichere« Methode ist es natürlich, in das Protokoll zu schauen. Die Setup-Protokolle finden Sie im Verzeichnis *c:\windows\panther*. In der Datei *setupact.log* werden alle Schritte dokumentiert, unter anderem auch, dass die Datei *A:\autounattend.xml* für die Installation herangezogen worden ist (Abbildung 6.18).

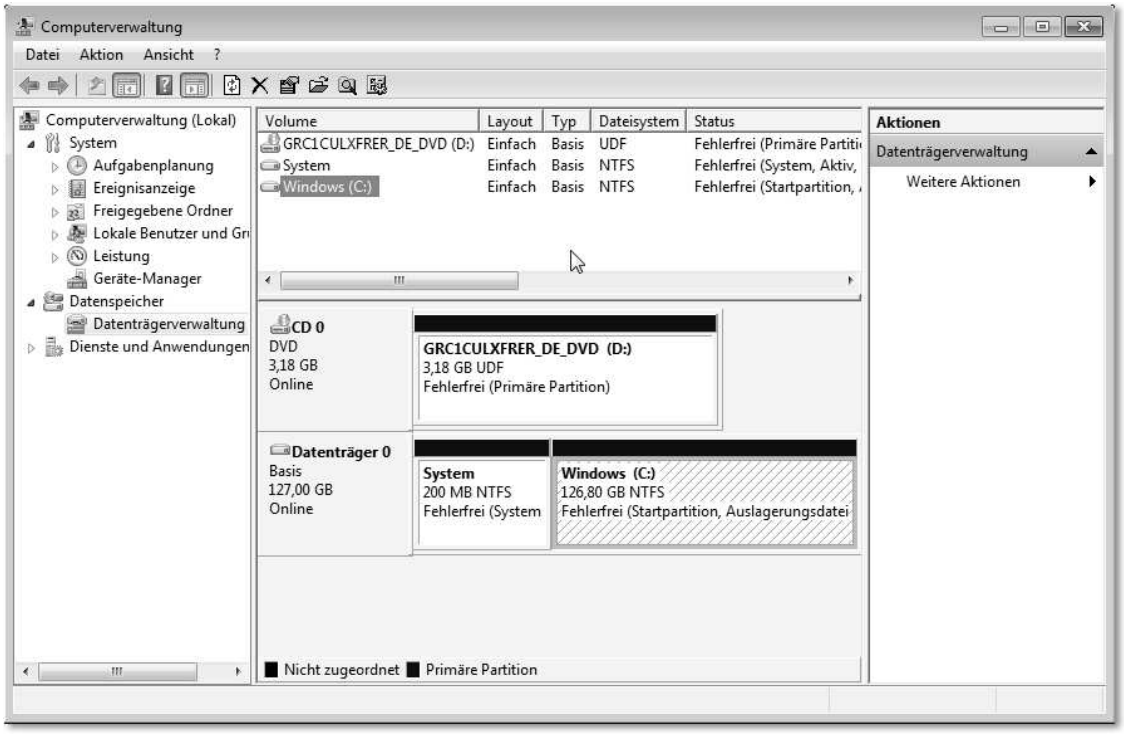


Abbildung 6.17 Kleine Kontrolle: Die Festplatte ist so partitioniert worden, wie es konfiguriert wurde.

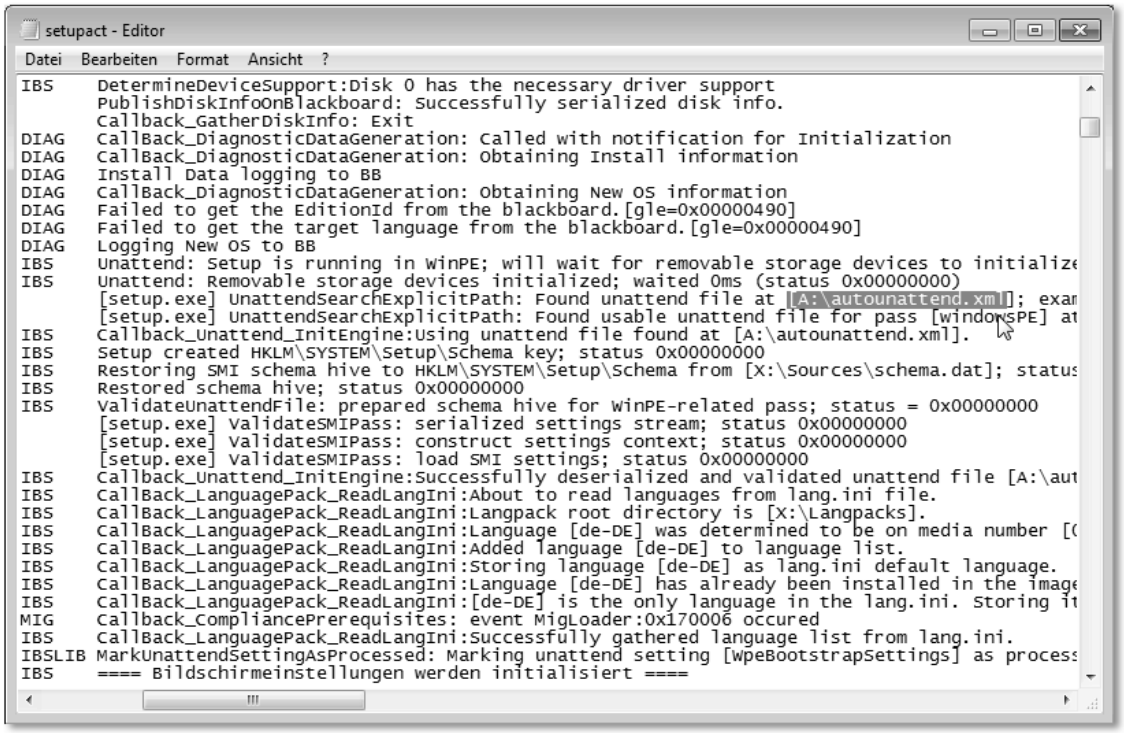


Abbildung 6.18 In der Datei »setupact.log« wird jeder Schritt ausführlich protokolliert – zum Beispiel auch die Antwortdatei.

Nun können Sie weitere Anpassungen am Image vornehmen, beispielsweise weitere Software, wie etwa den Acrobat Reader, installieren. Wenn alle Anpassungen vorgenommen worden sind, starten Sie wieder Sysprep – sofern es nicht ohnehin noch geöffnet ist – und nehmen die in Abbildung 6.19 gezeigten Einstellungen vor. *Sysprep.exe* finden Sie übrigens im Verzeichnis *c:\windows\system32\sysprep*.

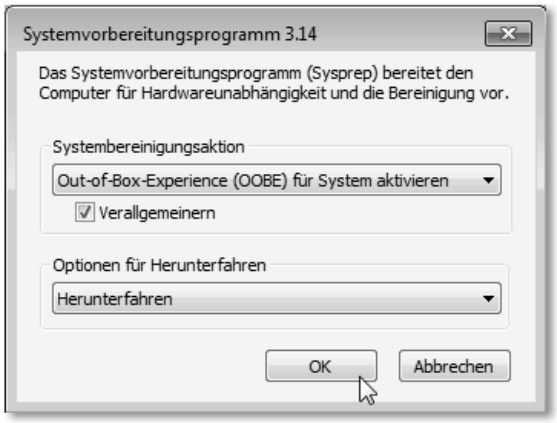


Abbildung 6.19 Wenn alle Anpassungsarbeiten erledigt worden sind, können Sie das Systemvorbereitungsprogramm ausführen.

Bei der Systemvorbereitung wird das System auf einen Status gesetzt, den ein PC hat, der zum ersten Mal gestartet wird. Unter anderem wird die Aktivierung zurückgesetzt, der PC hat keinen Namen, und es wird ein volles Plug&Play zur Treibererkennung und einiges andere mehr durchgeführt. Der Systemvorbereitungsvorgang wird ein kleines Weilchen dauern (Abbildung 6.20), und am Ende wird das System heruntergefahren.

Abbildung 6.20 Die Systemvorbereitung nimmt einige Zeit in Anspruch.

6.3.4 WinPE-Startimage erzeugen

Nun ist es zwar schon ganz gut, dass der PC zur Referenzinstallation geworden ist; das bringt aber natürlich nur etwas, wenn dieses Image auch irgendwie vom PC herunterkommt und zur WIM-Datei wird.

Die Vorgehensweise ist eigentlich ganz einfach:

- Sie starten den PC mit einer speziellen Boot-CD.

- Auf dieser CD muss sich ein Werkzeug befinden, mit dem das Image erfasst wird – dieses Werkzeug ist *IMAGEX.exe*, das im WAIK enthalten ist.

Nun ist im WAIK allerdings kein fertiges ISO-Image vorhanden, sondern Sie müssen eines erstellen. Die gute Nachricht ist, dass im WAIK die notwendigen Hilfsmittel vorhanden sind.

In meinem Beispiel erzeuge ich ein Boot-Image für einen x64-PC. Die Vorgehensweise im Telegrammstil:

- Öffnen Sie die WAIK-Eingabeaufforderung als Administrator. Der entsprechende Menüpunkt findet sich in der WAIK-Gruppe des Startmenüs.
- Rufen Sie die *copype.cmd* auf. Als Parameter geben Sie die Architektur und das Zielverzeichnis an, also beispielsweise `copype.cmd amd64 c:\winpe_amd64` (Abbildung 6.21).

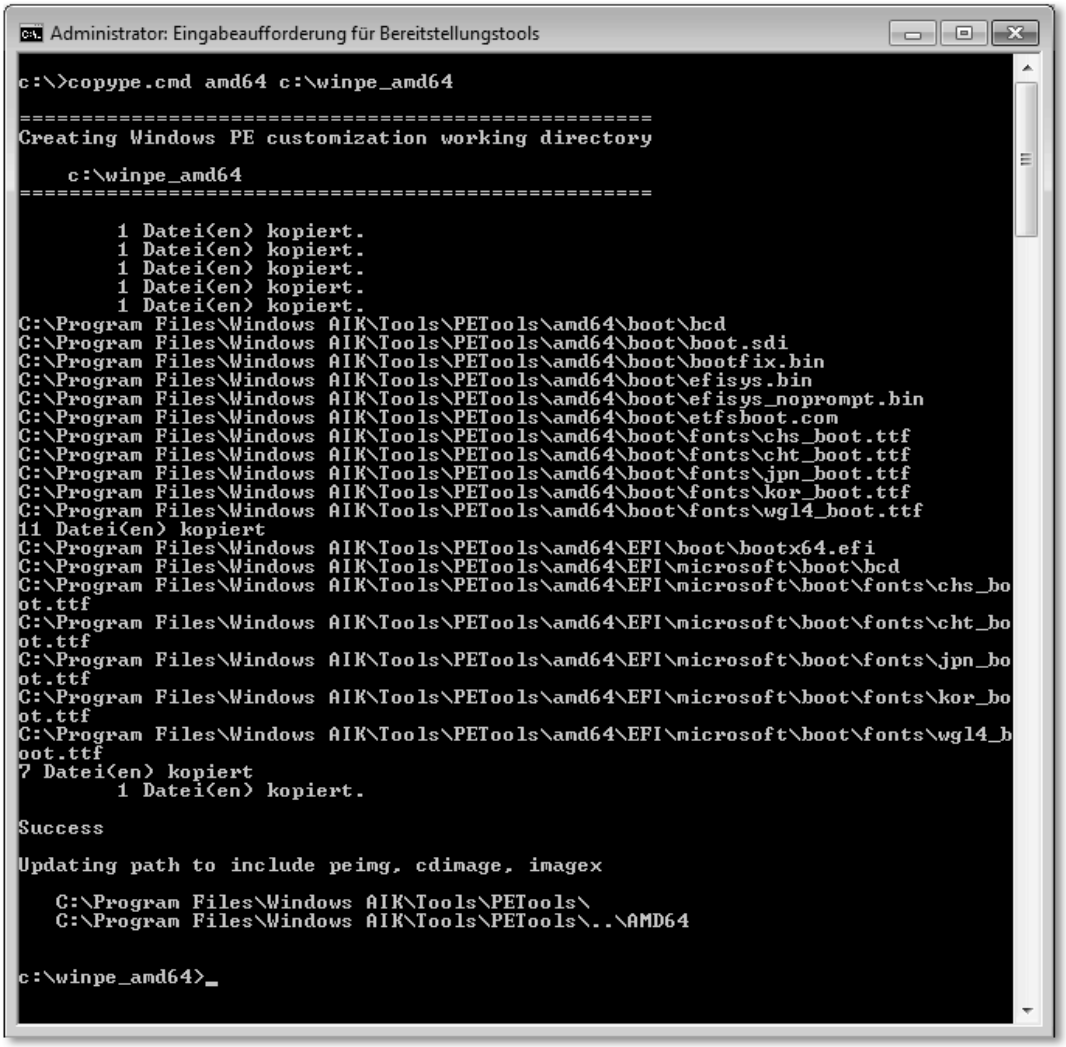


Abbildung 6.21 Ein Boot-Image für ein x64-System wird erzeugt.

- Im nächsten Schritt fügen Sie die im WAIK vorhandene Datei *imagex.exe* in das soeben angelegte ISO-Unterverzeichnis ein. Dies ist durch einfaches Kopieren zu bewerkstelligen. Abbildung 6.22 illustriert diesen Vorgang.

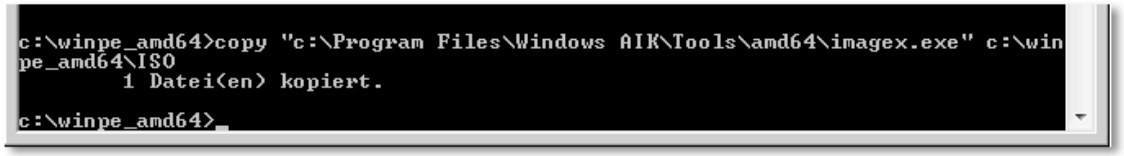


Abbildung 6.22 In das ISO-Image müssen Sie »imagex.exe« einfügen – dies lässt sich durch einfaches Kopieren bewerkstelligen.

- Ein wesentlicher Schritt, der leider in einigen offiziellen Dokumentationen fehlt, ist das Kopieren der Datei *boot.wim* in das Verzeichnis *sources* des neu entstandenen ISO-Verzeichnisses (Abbildung 6.23). Die Datei *boot.wim* finden Sie auf der Windows 7-DVD im Verzeichnis *sources*.

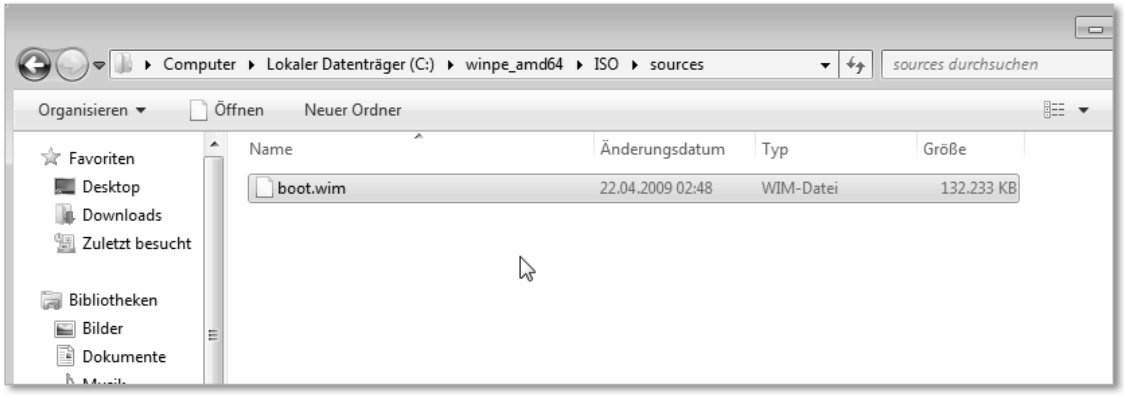


Abbildung 6.23 Die Datei »boot.wim« müssen Sie in das Verzeichnis »\ISO\sources« kopieren.

- Nun müssen Sie noch aus den Dateien im *\ISO*-Verzeichnis eine bootfähige CD machen. Auch das ist vergleichsweise einfach, denn das WAIK liefert das Werkzeug *oscdimg* mit. Dieses rufen Sie auf, wie in Abbildung 6.24 gezeigt.
- Wenig später halten Sie ein ISO-Image in den Händen (bzw. auf der Festplatte), das Sie nun auf CD brennen können. Das WAIK enthält zwar viele hilfreiche Werkzeuge, aber kein CD-Brenn-Programm.

  Wenn Sie in einer virtuellen Umgebung arbeiten, können Sie das Image booten natürlich direkt.

Mit Utilitys wie etwa dem *Magic ISO Maker* können Sie die entstandene ISO-Datei inspizieren. Zum einen ist die Dateistruktur des *\ISO*-Verzeichnisses zu sehen. Weiterhin ist das Image als BOOTABLE markiert – das ist ja auch nicht verwunderlich, schließlich soll davon ja gestartet werden (Abbildung 6.25).

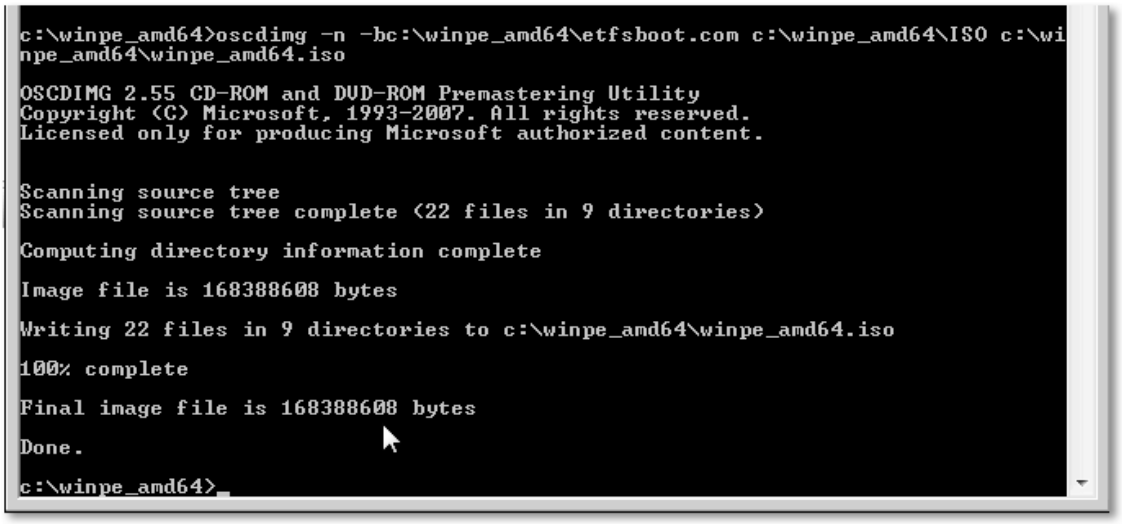


Abbildung 6.24 Mit dem Werkzeug »oscdimg« erzeugen Sie aus dem ISO-Verzeichnis eine ISO-Boot-Image. Achten Sie auf die Größe: Ist alles korrekt, muss die resultierende ISO-Datei ca. 170 MB groß sein.

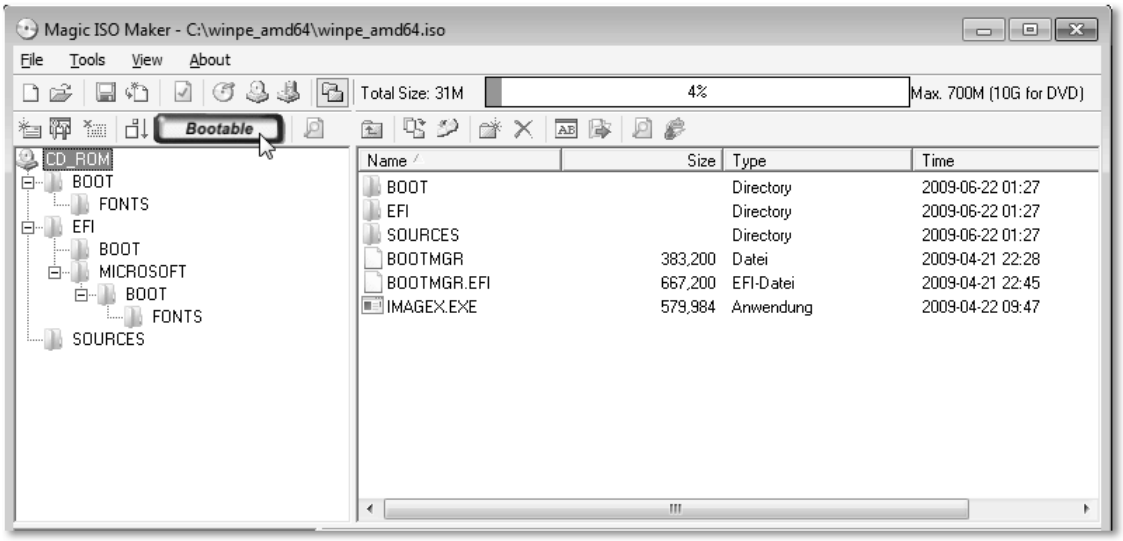


Abbildung 6.25 Mit dem Magic ISO Maker können Sie die neu erzeugte ISO-Datei inspizieren. Das ISO-Image ist bootfähig.

6.3.5 WIM erzeugen

Legen Sie nun die gebrannte Boot-CD in den Ziel-PC, oder mounten Sie das ISO-Image in einer virtuellen Maschine. Eigentlich sollte ohne weitere Probleme in Windows PE gestartet werden. Wenn das nicht funktioniert und stattdessen der in Abbildung 6.26 gezeigte Fehler erscheint, liegt das vermutlich daran, dass Sie die Datei *boot.wim* nicht vor dem Erzeugen der ISO-Datei in das *\sources*-Verzeichnis kopiert haben. Diese »Panne« geschieht auch deshalb relativ leicht, weil einige offizielle Dokumente diesen Schritt nicht nennen.

Abbildung 6.26 Wenn diese Meldung beim Start des neu erstellten BOOT-ISOs erscheint, haben Sie vermutlich die »boot.wim«-Datei nicht kopiert.

Sofern beim Startvorgang keine Probleme aufgetreten sind, sollte eine Eingabeaufforderung vor einem hübschen, dezent grauen Streifenmuster zu sehen sein (Abbildung 6.27).

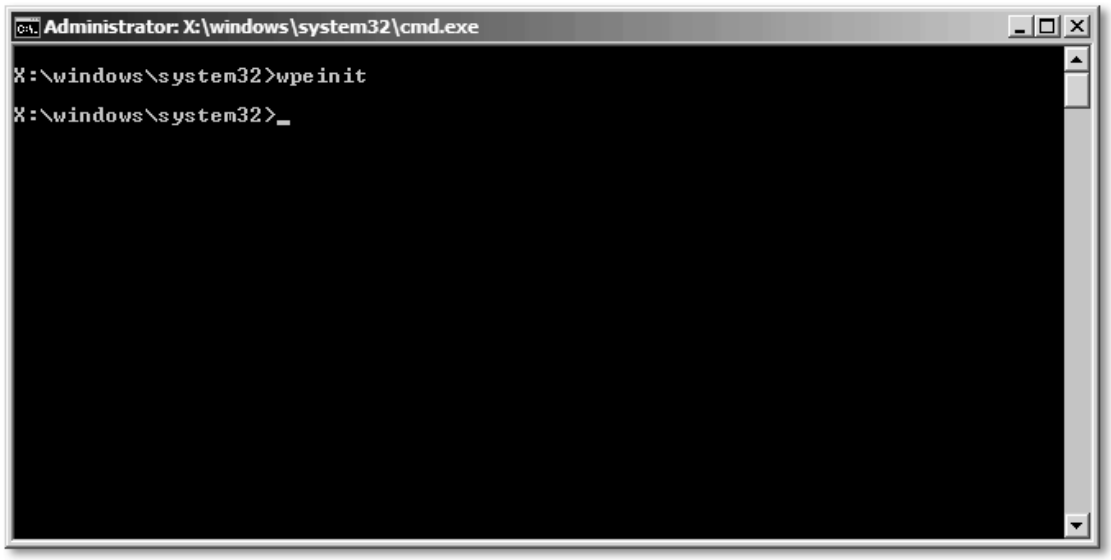


Abbildung 6.27 Wenn der Start des Boot-ISOs ordnungsgemäß funktioniert hat, wird sich dieses Bild zeigen.

Hier können Sie nun zwei Dinge unternehmen (Abbildung 6.28):

- Verbinden Sie sich mit dem Netzwerklaufwerk, auf das die Datei kopiert werden soll.
- Führen Sie durch einen entsprechend parametrisierten Aufruf des Programms *imagex* den Capture-Vorgang durch. Die wesentlichen Kommandozeilenparameter können Sie der Abbildung entnehmen.

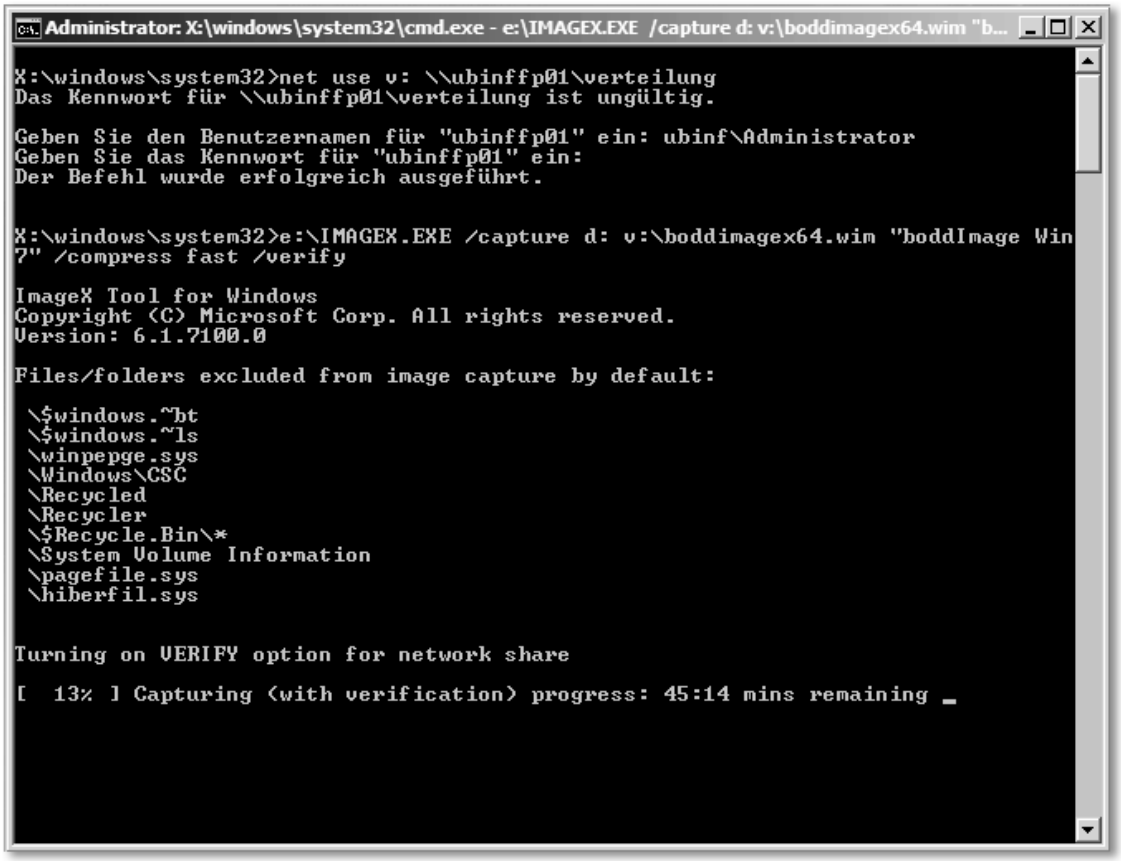


Abbildung 6.28 Verbinden Sie sich zunächst zu einem Netzwerklaufwerk, und erstellen Sie dann mit IMAGEX.EXE das WIM-Image.

Sofern Sie nicht umfangreiche Softwarepakete auf das Ziel-System installiert haben, wird das Image um die 3 Gigabytes groß sein.

6.3.6 Kurzer Test

Für diejenigen, die bislang noch nicht mit dem Systemvorbereitungsprogramm (*Sysprep*) gearbeitet haben, hier ein kurzer Überblick: Sysprep modifiziert einen PC so, dass er sich beim nächsten Start so verhält, als sei er noch nie gestartet worden. Unter anderem fragt das System beim Hochfahren, welche Sprache denn verwendet werden soll (Abbildung 6.29), und auch der Name des PCs ist dem

System plötzlich entfallen und wird abgefragt (Abbildung 6.30). Auch im nicht direkt sichtbaren Bereich tut sich einiges:

- Zum Beispiel erhält der PC eine neue SID, sodass er ein im Netz eindeutiges System wird. In früheren Zeiten hat man dazu gern *NewSID* von *sysinternals.com* verwendet – nicht schlecht, aber zumindest nicht von Microsoft supportet.
- Die Aktivierung des PCs wurde rückgängig gemacht und muss neu durchgeführt werden.

Abbildung 6.29 Wenn das Systemvorbereitungsprogramm (Sysprep) den PC behandelt hat, wird beim ersten Startvorgang zunächst nach der Sprache gefragt.

Die abgefragten Parameter können in einer Antwortdatei hinterlegt werden. Somit kann auch dieser Teil des Deploymentprozesses automatisiert werden. Das Systemvorbereitungsprogramm (Sysprep) hat also beim Deployment eine ziemlich hohe Bedeutung –vergessen Sie es also nicht.

Auf einem Windows 7-PC ist Sysprep bereits vorhanden, und zwar im Pfad *c:\windows\system32\sysprep*. Nutzen Sie unbedingt das »eingebaute« Windows 7-Sysprep und nicht eine aus dem Internet heruntergeladene Version – das gibt Probleme.

Abbildung 6.30 Auch der Name des PCs ist plötzlich nicht mehr bekannt.

6.4 Windows-Bereitstellungsdienste (WDS) installieren und einsetzen

Sie haben im vorherigen Abschnitt gesehen, wie man eine Referenzinstallation erstellt. Weiterhin haben Sie gesehen, wie man ein individuelles Start-ISO-Image erstellt, mit dessen Hilfe ein WIM-Image von der Referenzinstallation erstellt worden ist – und zwar mithilfe des Programms *imagex.exe*. Sie könnten nun natürlich den umgekehrten Weg gehen, um ein Image auf einen PC aufzubringen: zunächst mit einer Start-DVD booten, dann partitionieren und schließlich mit *imagex.exe* die WIM-Datei (bzw. deren Inhalt) auf die Festplatte bringen.

Diese Vorgehensweise funktioniert, ist aber eigentlich nicht mehr ganz zeitgemäß. Jeder einigermaßen moderne PC bzw. Notebook erlaubt einen Bootvorgang aus dem Netzwerk – dazu muss das Gerät übrigens nicht brandneu sein, auch vor fünf Jahren war das Booten aus dem Netz absolut Standard. Für das Verfahren wird – mal abgesehen von der Fähigkeit des Clients – ein wenig Serverunterstützung benötigt. In Windows Server 2003 war RIS (*Remote Installation Services*) ent-

halten, und Windows Server 2008 bringt hierfür die WDS (*Windows Deployment Services*, in den deutschen Versionen *Windows-Bereitstellungsdienste*) mit.

PXE

Beim Thema »Booten aus dem Netz« fällt stets das Stichwort *PXE*, ausgesprochen bedeutet das *Pre-Boot Execution Environment*. PXE ist ein Verfahren, das einem Client die Durchführung eines Bootvorgangs über das Netz ermöglicht. Bei einem solchen Vorgang bezieht der Client zunächst eine DHCP-Adresse über das Netz, anschließend wird über TFTP (*Trivial FTP*) von einem Boot-Server das Boot-Image geladen.

Um Windows 7 (übrigens auch Vista) automatisch zu installieren, benötigen Sie Windows Server 2008 mit WDS – das im 2003er-Server enthaltene RIS ist für die Windows 7-Installation nicht geeignet.

Die *Windows-Bereitstellungsdienste* (WDS) bestehen aus drei Komponentengruppen:

- *Serverkomponenten*: Wenn Sie auf einem Server die WDS installieren, werden technisch gesehen ein PXE-Server und ein TFTP-Server installiert. Neben diesen Hauptkomponenten gibt es noch zusätzliche Funktionen, um beispielsweise Multicast-Übertragungen zu ermöglichen.
- *Clientkomponenten*: Hier wäre insbesondere die Windows-Vorinstallationsumgebung (WinPE, *Windows Pre-Installation Environment*) zu nennen, die beim Bootvorgang gestartet wird.
- Natürlich gehören auch *Verwaltungskomponenten* dazu, nämlich sowohl eine grafische Oberfläche (ein Snap-In für die *Microsoft Management Console*, MMC) als auch ein Kommandozeilenwerkzeug (`WDSUTIL`).

6.4.1 Voraussetzungen

Die ersten drei Voraussetzungen für die Windows-Bereitstellungsdienste dürften eigentlich überall erfüllt sein:

- Im Netz muss ein funktionierender DNS-Server vorhanden sein.
- Im Netz muss ein funktionierender DHCP-Server vorhanden sein.
- Der WDS-Server muss Mitglied einer Active Directory-Domäne sein.

Die vierte Voraussetzung ist zwar nicht schwer zu erfüllen, aber auch nicht so ganz selbstverständlich wie die zuvor genannten: Es wird dringend empfohlen, die Images nicht auf die Systempartition, sondern auf eine separate Partition zu legen. Es muss nicht ein separates physikalisches RAID-Set sein, eine Partition auf

einer großen Festplatte genügt. Ein mögliches Layout mit zwei RAID-Sets sehen Sie auf Abbildung 6.31.

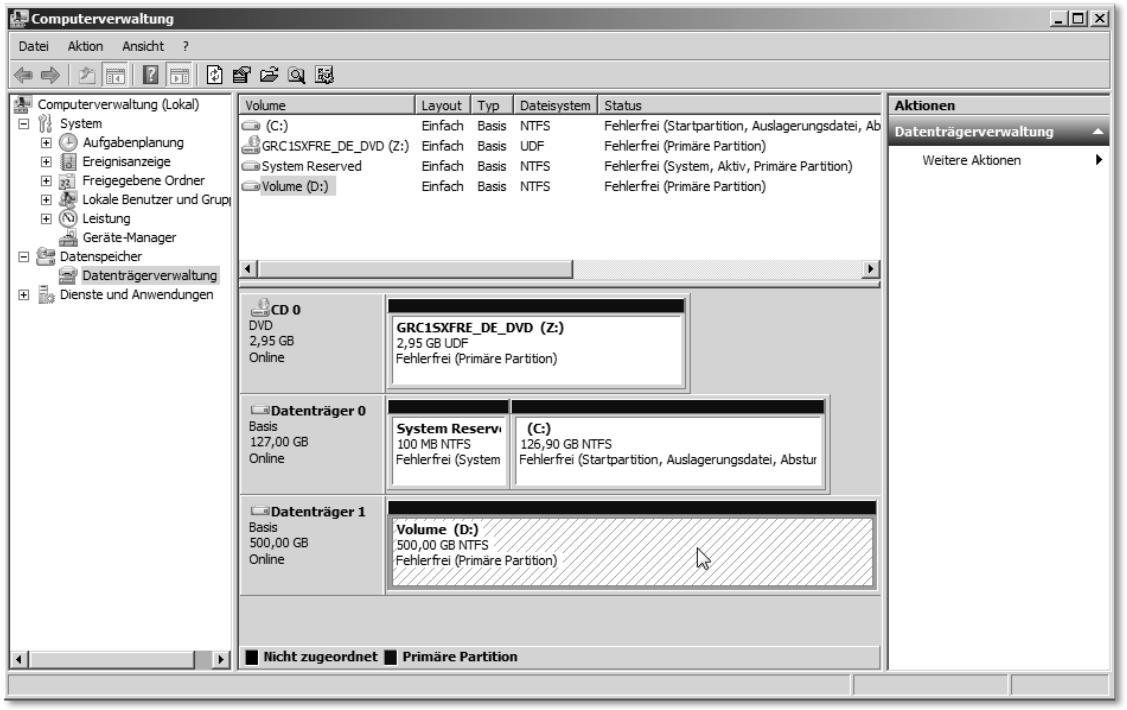


Abbildung 6.31 Die zu verteilenden Images sollen auf einer separaten Partition liegen – eine Festplattenkonfiguration könnte also beispielsweise so aussehen, wie hier gezeigt ist.

WDS nicht auf DHCP-Server

Der Server, auf dem Sie die WDS installieren, sollte nach Möglichkeit kein DHCP-Server sein. Eine solche Konfiguration ist zwar möglich (und es gibt sogar einen grafischen Dialog, um Anpassungen vorzunehmen), trotzdem schafft das meines Erachtens höchstens zusätzliche Verwirrung und Probleme.

Ein Unternehmen bzw. eine Organisation, die sich für den Einsatz von WDS entscheidet, dürfte im Allgemeinen mehr als einen Server haben, sodass es nicht unbedingt notwendig sein dürfte, diesen Dienst ausgerechnet gemeinsam mit dem DHCP-Dienst laufen zu lassen.

6.4.2 WDS installieren

Die Installation der WDS ist simpel. Sie müssen eigentlich nur wissen, dass diese eine installierbare Rolle des Windows Server 2008 sind. Die hier gezeigten Screenshots zeigen zwar einen Windows Server 2008 R2, ein »alter« Windows Server 2008 (ohne R2) kann aber genauso verwendet werden, und die Installation sieht identisch aus.

Wählen Sie also das Hinzufügen einer Rolle, und entscheiden Sie sich für die Windows-Bereitstellungsdienste (Abbildung 6.32).

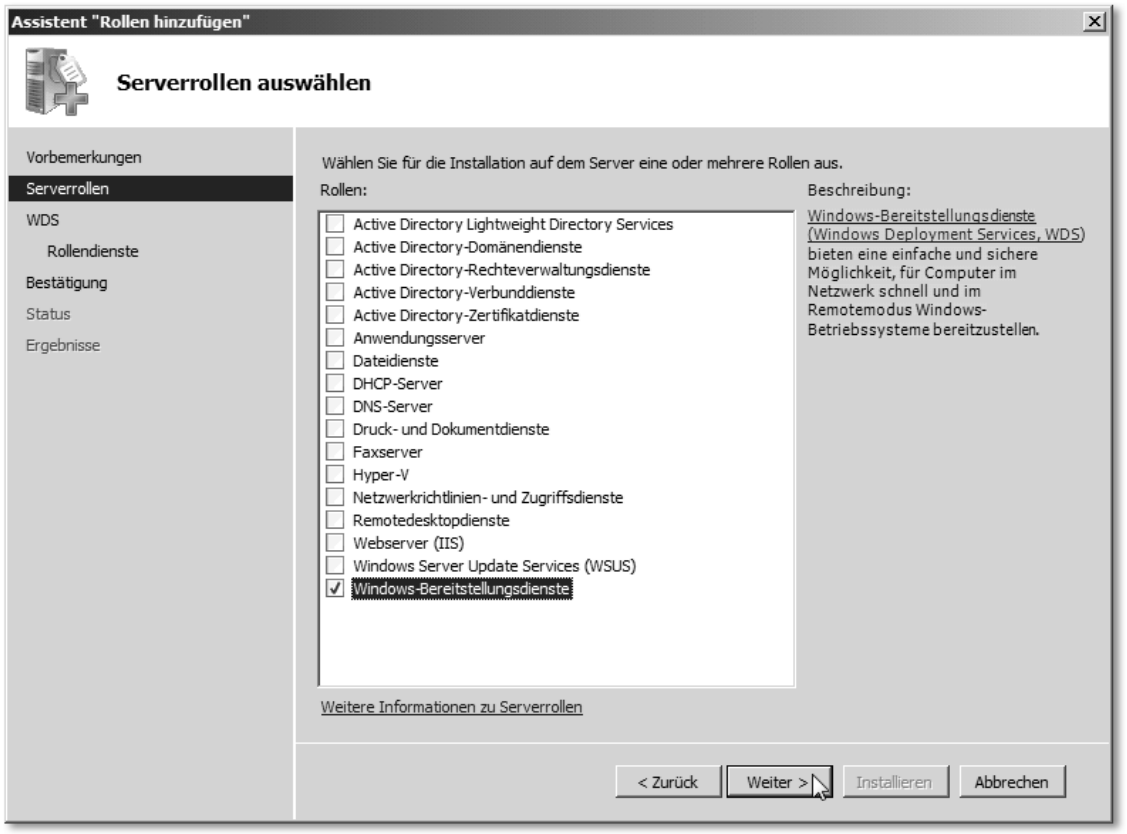


Abbildung 6.32 WDS ist eine zu installierende Rolle.

Wie häufig bei der Installation einer weiteren Rolle wird der Assistent nach den zu installierenden Rollendiensten fragen, wobei standardmäßig beide Optionen vorbelegt sind (Abbildung 6.33).

Sofern Sie einen »vollen« WDS-Server installieren möchten, müssen beide Komponenten aktiviert bleiben:

- Der Bereitstellungsserver ist sozusagen die Kernkomponente.
- Ein oder mehrere Transportserver können zusätzlich installiert werden, um beispielsweise die WDS-Funktionalität in ein durch Router getrenntes Netzwerksegment zu bringen.

Die Installation läuft ohne weitere Fragen (und hoffentlich ohne irgendwelche Zwischenfälle) durch.

Danach führen Sie die Erstkonfiguration durch.

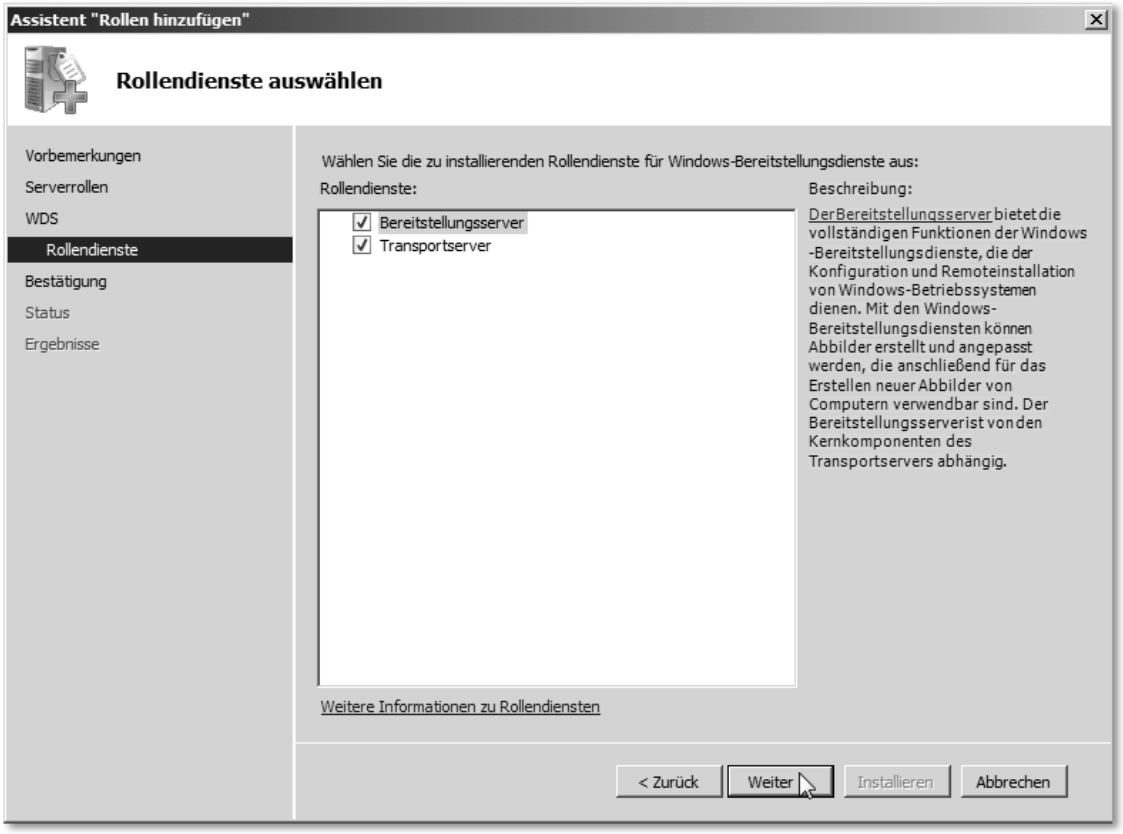


Abbildung 6.33 In einer kleinen Installation mit einem einzelnen Server werden dort beide Rollendienste installiert.

6.4.3 WDS-Erstkonfiguration

Die Erstkonfiguration der Windows-Bereitstellungsdienste geschieht wie erwartet mit einem Assistenten. Starten Sie das Konfigurationswerkzeug WINDOWS-BEREITSTELLUNGSDIENSTE, und wählen Sie dort den Menüpunkt SERVER KONFIGURIEREN (Abbildung 6.34).

Abbildung 6.34 Die Bereitstellungsdienste sind zwar vorhanden – müssen aber erst konfiguriert werden.

Der Assistent wird Sie zunächst darauf hinweisen, dass einige Voraussetzungen zu erfüllen sind. Der Server muss also ein Domänenmitglied sein, es muss ein DNS- und ein DHCP-Server vorhanden sein, und es muss eine separate NTFS-Partition für die Abbilder geben (Abbildung 6.35).

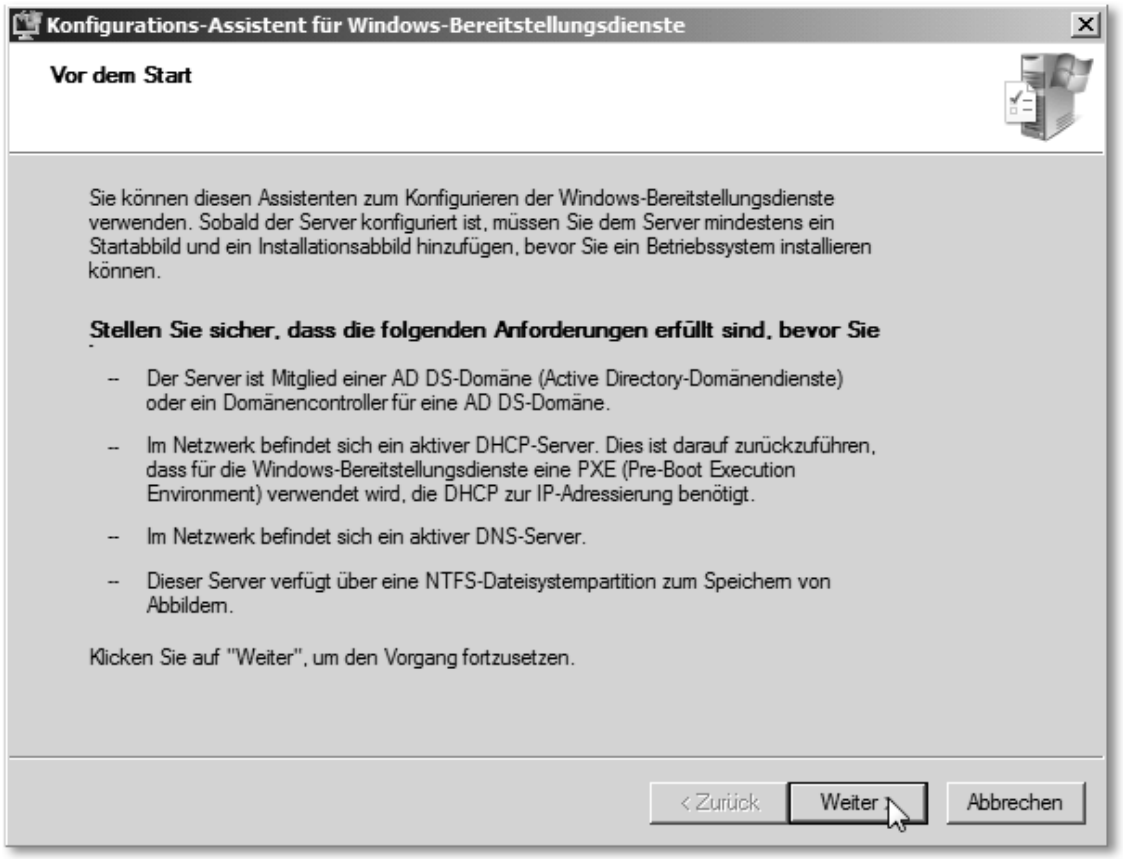


Abbildung 6.35 Der Konfigurationsassistent weist nochmals auf die Anforderungen hin.

Der erste Dialog, in dem Sie eine Eingabe vornehmen müssen, bezieht sich auf den Speicherort für den *Remoteinstallationsordner*, in dem die Abbilder etc. gespeichert werden. Wie ich bereits mehrfach bei der Besprechung der Voraussetzungen erwähnthabe, muss es sich hierbei um eine NTFS-Partition handeln und es sollte keine Systempartition sein (Abbildung 6.36).

Im nächsten Schritt wählen Sie aus, wie der WDS-Server auf Clientanfragen reagieren soll, was im Grunde genommen nicht wirklich spektakulär ist (Abbildung 6.37):

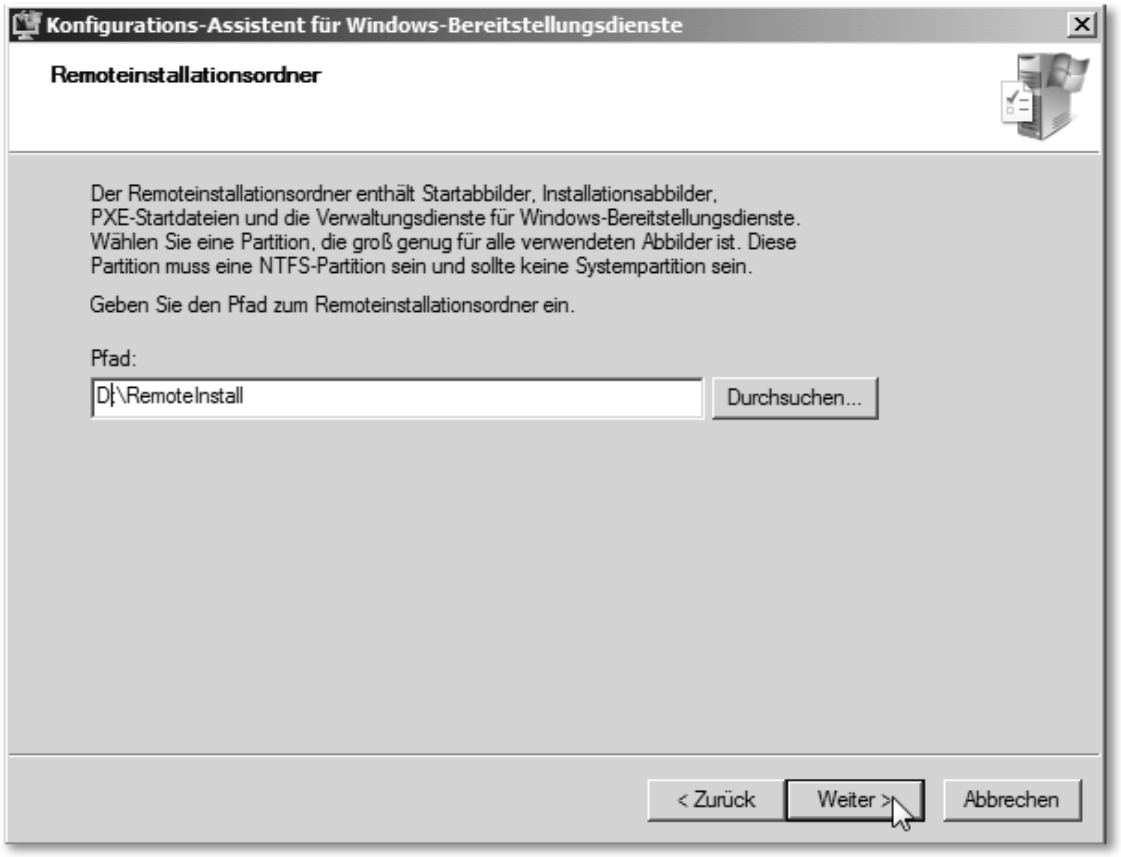


Abbildung 6.36 Die Auswahl des Verzeichnisses für den Remoteinstallationsordner. Denken Sie daran, dass er nicht auf der Systempartition liegen soll!

- Die erste Option (KEINEM CLIENTCOMPUTER ANTWORTEN) schaltet den WDS-Server sozusagen ab. Ein Client kann noch so verzweifelt versuchen, einen Server für den Netzwerkbootvorgang zu finden: Dieses System wird nicht antworten.
- Die mittlere Einstellung besagt, dass nur solchen Clients geantwortet wird, die bekannt sind. Bekannt wird ein Client dadurch, dass das zugehörige Computerkonto im Active Directory vorhanden ist.

  Im entsprechenden AD-Objekt wird im Attribut *netbootGUID* die MAC-Adresse des PCs eingetragen. Dies wird später noch genauer gezeigt. Falls Sie im grafischen WDS-Konfigurationswerkzeug eine Möglichkeit suchen, um diese Einträge vorzunehmen, muss ich Sie direkt enttäuschen, denn diese gibt es nicht. Sie müssen stattdessen mit dem Kommandozeilenwerkzeug WDSUTIL arbeiten.

Diese Einstellung ist durchaus sinnvoll, denn Sie können verhindern, dass unautorisierte Hardware im Unternehmensnetz mit einer »offiziellen« Betriebssysteminstallation versehen wird. Alle unbekannten Geräte werden nicht aus dem Netzwerk booten können.

- Ist die dritte Option gewählt, antwortet der WDS auf jede Anfrage. Sie können aber dadurch ein wenig mehr Kontrolle in den Vorgang bringen, dass unbekannte Computer zunächst genehmigt werden müssen – das führe ich Ihnen später am Beispiel vor.

Abbildung 6.37 Legen Sie fest, auf welche Clients die Bereitstellungsdienste reagieren sollen. Diese Einstellung sorgt dafür, dass immer reagiert wird.

Damit ist die (Grund-)Konfiguration der Bereitstellungsdienste eigentlich auch schon abgeschlossen. Im nächsten Schritt müssen Start- und Installationsabbilder hinzugefügt werden.

Der Assistent bietet direkt an, diese Arbeit sofort zu erledigen, was im Normalfall eine gute Idee ist (Abbildung 6.38). Sie können diesen Arbeitsschritt zwar jederzeit später durchführen, allerdings können Sie ohne Abbilder nicht viel mit dem neu installierten WDS anfangen.

Abbildung 6.38 Fertig – aber jetzt geht es erst richtig los, nämlich mit dem Hinzufügen von Abbildern.

6.4.4 Start- und Installationsabbilder hinzufügen

Im WDS gibt es zwei Typen von Abbildern:

- *Startabbilder* enthalten die Betriebssystemdateien, die der Client per TFTP über das Netz holt, um überhaupt booten zu können. Startabbilder sind auf den Microsoft-Betriebssystem-DVDs (Windows Server 2008 und Windows 7) vorhanden. Alternativ können Sie auch selbst erstellte Startabbilder verwenden.
- *Installationsabbilder* enthalten sozusagen das zu installierende Betriebssystem. Es können standardmäßige Installationsabbilder (auf den Microsoft-Datenträgern vorhanden) oder selbst erstellte verwendet werden. In den selbst erstellten Installationsabbildern können zusätzliche Softwarekomponenten wie beispielsweise der Adobe Reader vorhanden sein.

Die Abbilder liegen im WIM-Format vor (*Windows Imaging Format*).

Wenn Sie die WDS-Erstkonfiguration mit dem Assistenten abgeschlossen haben, wird er Sie im Anschluss zu dem Dialog aus Abbildung 6.39 führen. Sie können als Quelle das Verzeichnis *\sources* der Windows-Server-2008-DVD angeben, die sich vermutlich im Laufwerk des Servers befindet. In diesem Verzeichnis sind Abbilder vorhanden. Das gilt übrigens auch für die Windows 7-DVD.

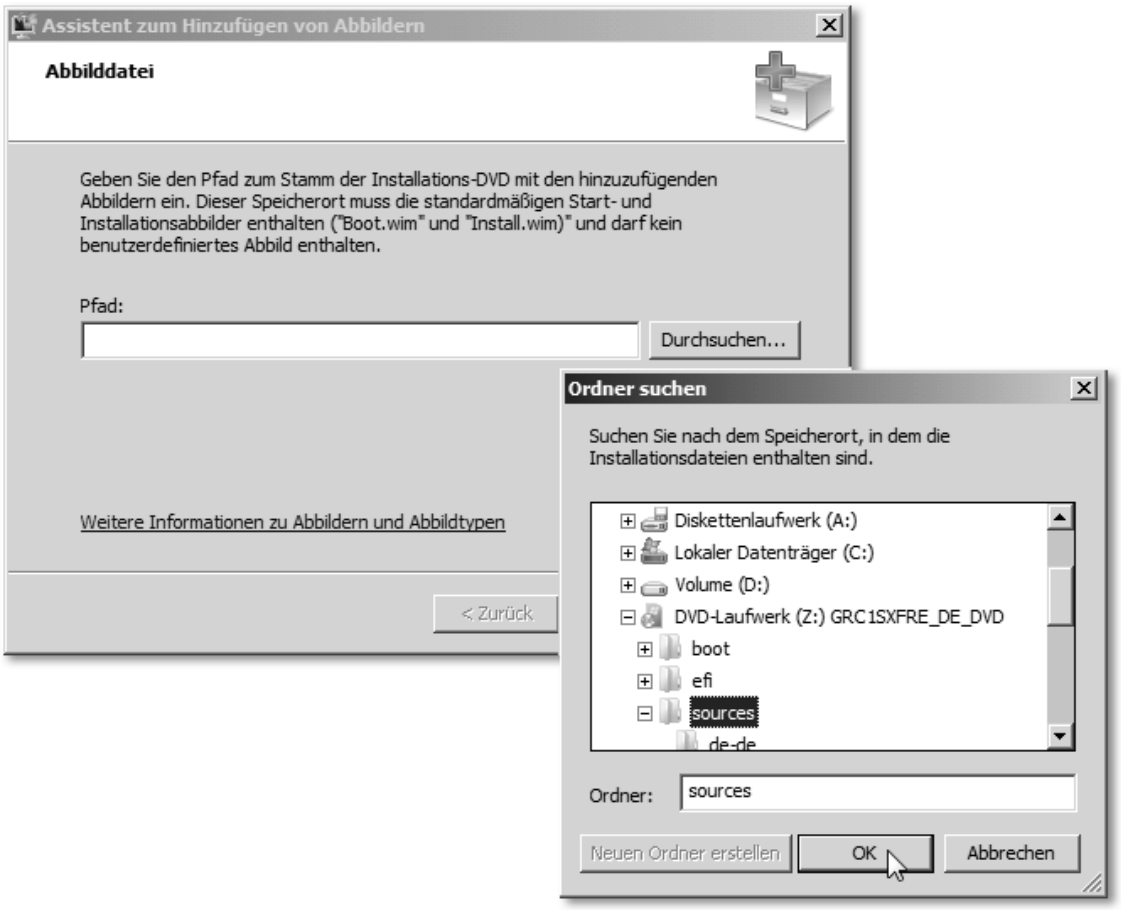


Abbildung 6.39 Fügen Sie Abbilddateien hinzu. Diese finden Sie beispielsweise auf der Windows Server 2008-DVD und natürlich auf der Windows 7-DVD.

Wenn Sie den Pfad angegeben haben, wird ein Dialog erscheinen, der erfragt, welcher Abbildgruppe die neuen Images angehören sollen (Abbildung 6.40). Dies ist »nur ein Name«, es macht aber durchaus Sinn, die Abbilder ein wenig zu organisieren, insbesondere wenn Sie im Laufe der Arbeit mit WDS viele eigene Abbilder erstellen. Wählen Sie hier beispielsweise die Bezeichnung Windows Server 2008 R2. Da die Namen der Abbildgruppen jederzeit geändert werden können, ist es auch kein Drama, wenn Sie zunächst die voreingestellte Bezeichnung bestätigen (oder aus lauter Übermut HUGO in das Feld schreiben).

Im Falle der Windows Server 2008 R2-DVD wird der Assistent Sie darauf hinweisen, dass Sie ein Startabbild und acht Installationsabbilder installieren (Abbildung 6.41).

Wie Sie wissen, gibt es die modernen Microsoft-Betriebssysteme in zwei oder drei Varianten für unterschiedliche Hardwarearchitekturen: Serverbetriebssysteme sind als x86-, x64- und IA64-Version erhältlich, die Clientbetriebssysteme gibt es als x86- und x64-Version.

Abbildung 6.40 In den Windows-Bereitstellungsdiensten werden die Abbilder in Abbildgruppen organisiert.

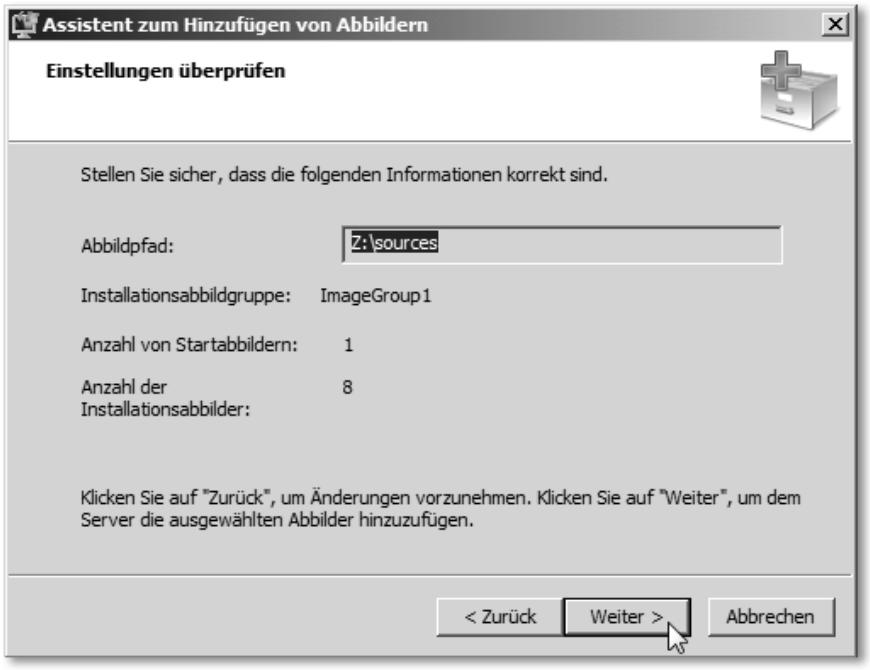


Abbildung 6.41 Auf der Windows Server 2008 R2-DVD werden ein Startabbild und acht Installationsabbilder gefunden.

Dementsprechend gibt es sowohl die Startabbilder als auch die Installationsabbilder für die unterschiedlichen Hardwarearchitekturen. Auf einer x64-DVD sind »nur« die x64-Abbilder enthalten. Wenn Sie also planen, auch andere Hardware-

architekturen zu unterstützen, müssen die entsprechenden Abbilder hinzugefügt werden. Diese finden Sie auf den DVDs für die jeweilige Architektur.

Apropos »hinzufügen«: Die Abbilder werden von der zuvor angegebenen Installationsquelle (Abbildung 6.39) in den Remoteinstallationsordner (Abbildung 6.36) kopiert. Dieser Vorgang wird ein Weilchen dauern, denn die Windows Server 2008- und Windows 7-Installationsimages sind immerhin um die 3 GB groß.

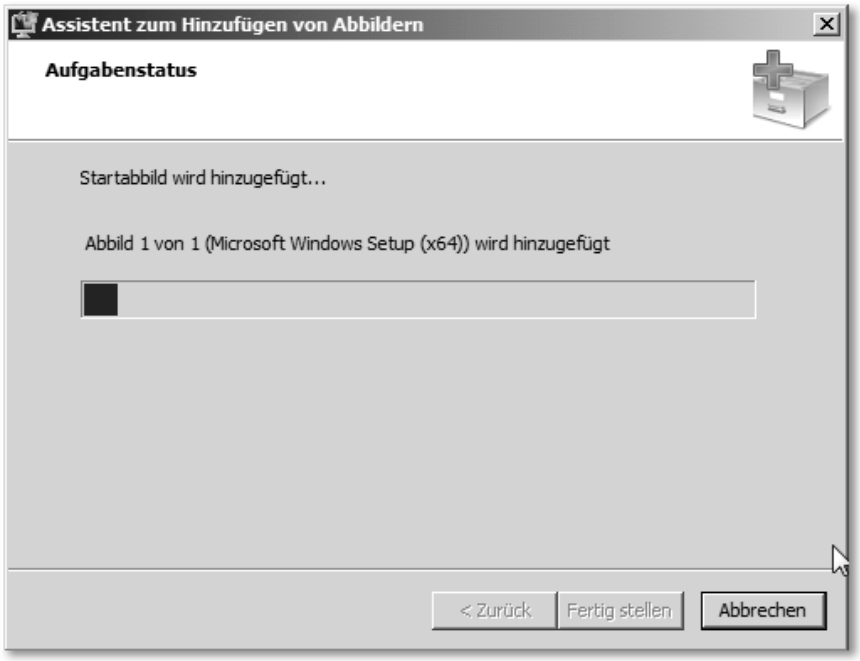


Abbildung 6.42 Das Hinzufügen von Installationsabbildern läuft zwar ohne Administratoreingriff – dauert aber.

Wenn Sie meinem Beispiel gefolgt sind, sind jetzt zwar Windows-Server-2008-R2-Installationabbilder verfügbar – das ist hier aber ein Windows 7-Buch, folglich müssen noch entsprechende Abbilder hinzugefügt werden:

- Legen Sie die Windows 7-DVD ein.
- Fügen Sie eine Abbildgruppe WINDOWS 7 hinzu – das ist optional, aber empfehlenswert.
- Wählen Sie im Kontextmenü den Menüpunkt INSTALLATIONSABBILD HINZUFÜGEN (Abbildung 6.43).
- Das Windows 7-Installationsabbild heißt *install.wim* und findet sich im Ordner *\sources* der Windows 7-DVD.
- Der Assistent wird nun noch von Ihnen wissen wollen, welche der vorhandenen Abbilder hinzugefügt werden sollen. Auf einer Volumenlizenz-DVD werden noch weitere Versionen vorhanden sein (insbesondere *Business* und *Enterprise*).

Nun wird der Assistent die gewählten Abbilder in den Remoteinstallationsordner kopieren – schon fertig!

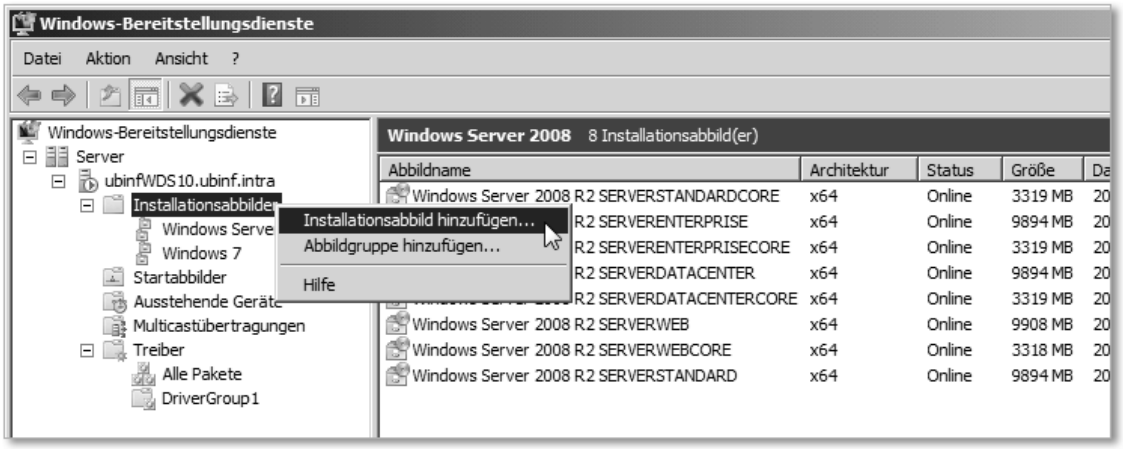


Abbildung 6.43 Um weitere Installationsabbilder (beispielsweise von der Windows 7-DVD) hinzuzufügen, wählen Sie diesen Menüpunkt.

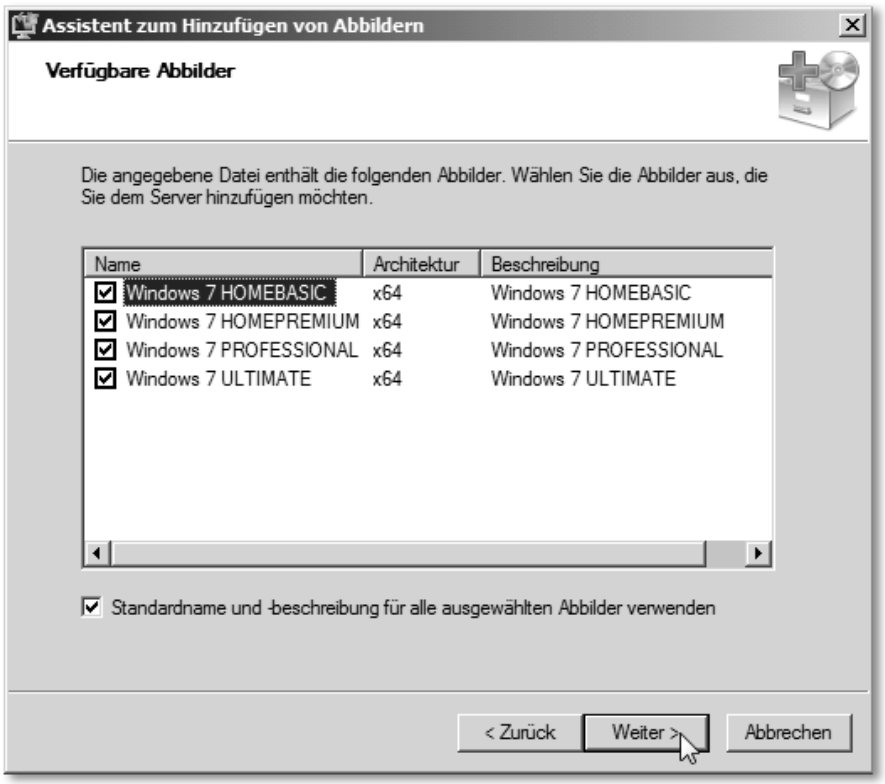


Abbildung 6.44 Wählen Sie die Abbilder aus der Datei aus.

6.4.5 Ein erster »kleiner« Test mit WDS

Nachdem nun die Grundkonfiguration der Bereitstellungsdienste abgeschlossen ist, liegt es nahe, einen kleinen Test durchzuführen. Ich zeige Ihnen hier das komplette Szenario, möchte allerdings darauf hinweisen, dass natürlich noch etliche

Anpassungen notwendig sind, bis die Lösung vollständig konfiguriert ist. Es kann aber auch in Ihrer Umgebung keinesfalls schaden, bereits jetzt einen kleinen Test durchzuführen, um zu kontrollieren, ob die Bereitstellungsdienste grundsätzlich betriebsbereit sind. Ein solcher Test würde übrigens auch zutage fördern, ob es gegebenenfalls noch Probleme in Ihrem Netzwerk gibt, die ein erfolgreiches Deployment mit WDS verhindern.

Initiieren Sie also einen Netzwerkbootvorgang auf einem Client. Eventuell müssen Sie auf dem Client die Startreihenfolge anpassen. Die meisten Clients ermöglichen eine temporäre Anpassung der Startreihenfolge mit der F12-Taste.

Es sollte sich in etwa ein Szenario wie auf Abbildung 6.45 ergeben:

- Der Client erhält eine Adresse vom DHCP-Server.
- Sie werden aufgefordert, F12 für den Startvorgang zu drücken.

Hinweis

Die Beispiele dieses Buchs sind teilweise mit virtuellen Maschinen realisiert worden. Hier ist zu beachten, dass nur die Ältere Netzwerkkarte in der Lage ist, einen Netzwerkbootvorgang auszuführen, die Netzwerkkarte kann dies nicht (Stand Hyper-V aus Windows Server 2008 SP1).

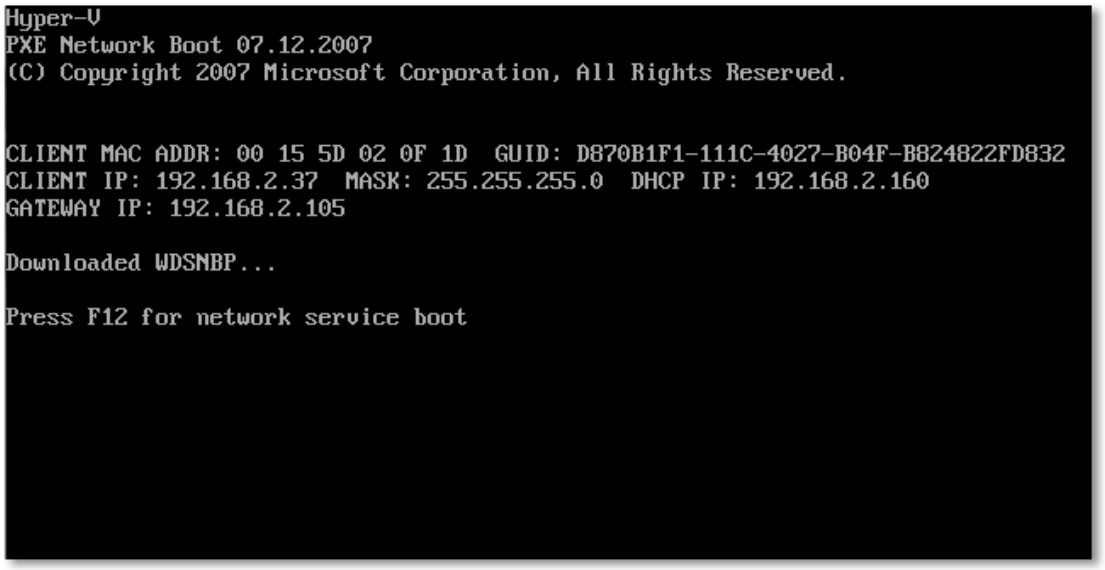


Abbildung 6.45 Der PXE-Bootvorgang des Clients. Das »F12« stammt bereits von den WDS.

Sofern mehrere Startabbilder vorhanden sind, erscheint eine Auswahlliste. Diese Auswahlliste kann übrigens maximal 13 Startabbilder enthalten – das sollte aber genügen.

Wenn der Startvorgang läuft, wird sich in etwa die auf Abbildung 6.46 gezeigte Installation einstellen. Angenehmerweise wird angezeigt, von welcher IP-Adresse das Boot-Image geladen wurde, außerdem ist der Pfad zu sehen, den Sie auch im Remoteinstallationsordner wiederfinden werden. Wenn Sie so weit gekommen sind, können Sie sich übrigens ein wenig selbst auf die Schulter klopfen, denn ab jetzt funktionieren die Windows-Bereitstellungsdienste sind in Ihrer Umgebung. Der Rest ist dann Feintuning, wobei das jedoch der weitaus umfangreichere Teil wird.

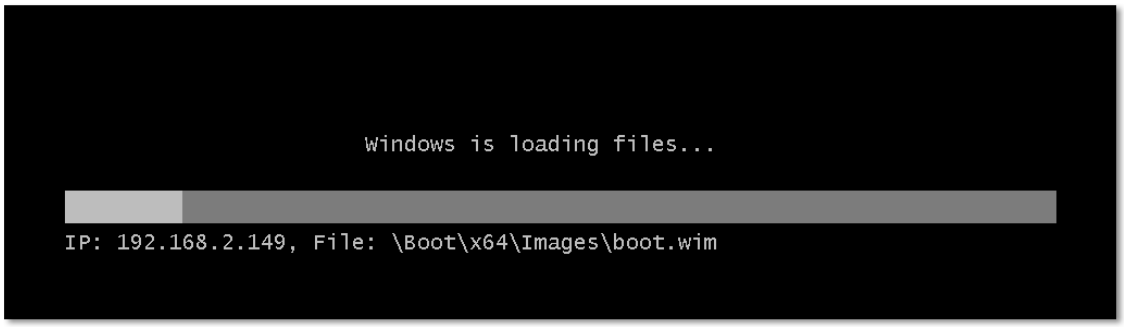


Abbildung 6.46 Hier wird, wie unschwer zu erkennen ist, das Startabbild (»boot.wim«) geladen.

Nach kurzer Zeit wird der Dialog aus Abbildung 6.47 erscheinen, in dem die Windows-Bereitstellungsdienste (siehe auch die Überschrift im Dialog) die Lokalisierung abfragen. Vielleicht fragen Sie sich nun, warum Sie mit derlei Fragen behelligt werden, wo doch eigentlich das Thema »automatische Installation« auf dem Plan steht.

Die Antwort ist im Grunde genommen aber ganz einfach: Um den hier gezeigten Installationsvorgang zu automatisieren, müssen Sie noch Konfigurationsdateien erstellen und diese zuordnen. Dann ist es selbstverständlich möglich, den Installationsvorgang so weit zu automatisieren, dass keinerlei Eingaben notwendig sind.

Da bislang keine Dateien für die unbeaufsichtigte Installation hinterlegt worden sind, werden Sie nach einer Authentifizierung für die Anmeldung am Bereitstellungsserver (Abbildung 6.48) und nach dem zu verwendenden Image (Abbildung 6.49) gefragt. Wie ich schon gesagt habe, können diese Abfragen in einer Datei für die unbeaufsichtigte Installation hinterlegt werden.

Abbildung 6.50 wird jedem, der bereits Windows 7 oder auch Windows Server 2008 installiert hat, bekannt vorkommen. Die Installation läuft zwar komplett über das Netz ab, verwendet aber dieselbe Installationsroutine. Hier gibt es also keine Überraschungen mehr.

Abbildung 6.47 Wenn der initiale Startvorgang erfolgreich gewesen ist, werden Sie von diesem Auswahldialog begrüßt.

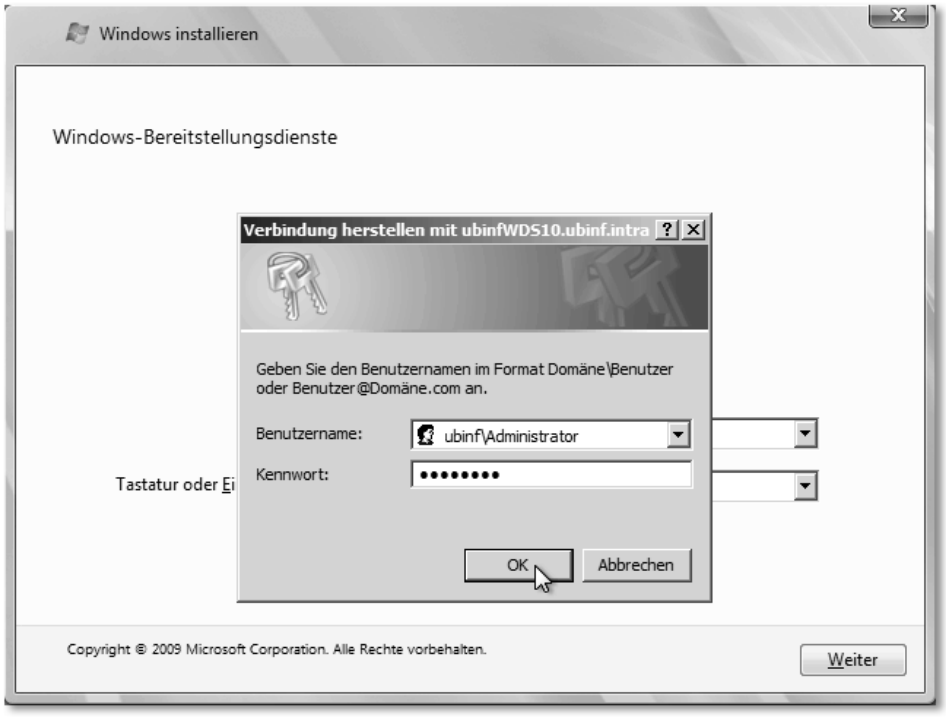


Abbildung 6.48 Die Bereitstellungsdienste erfordern eine Authentifizierung.

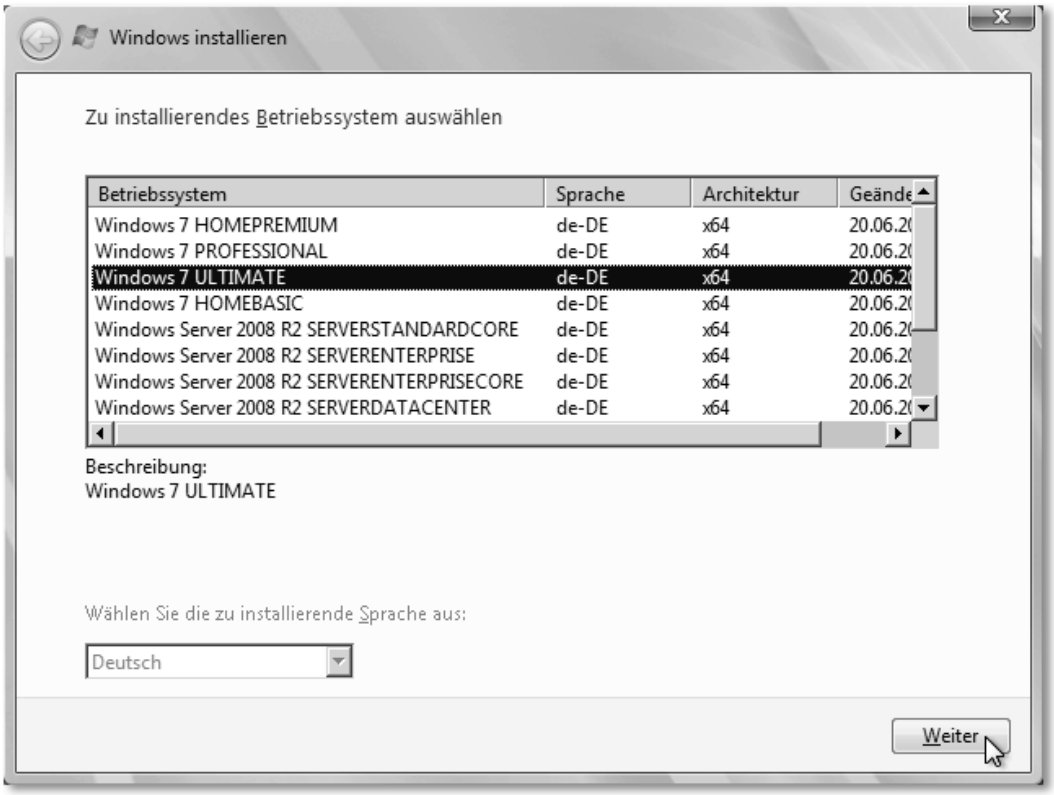


Abbildung 6.49 Das zu verwendende Installationsabbild wählen Sie hier aus.

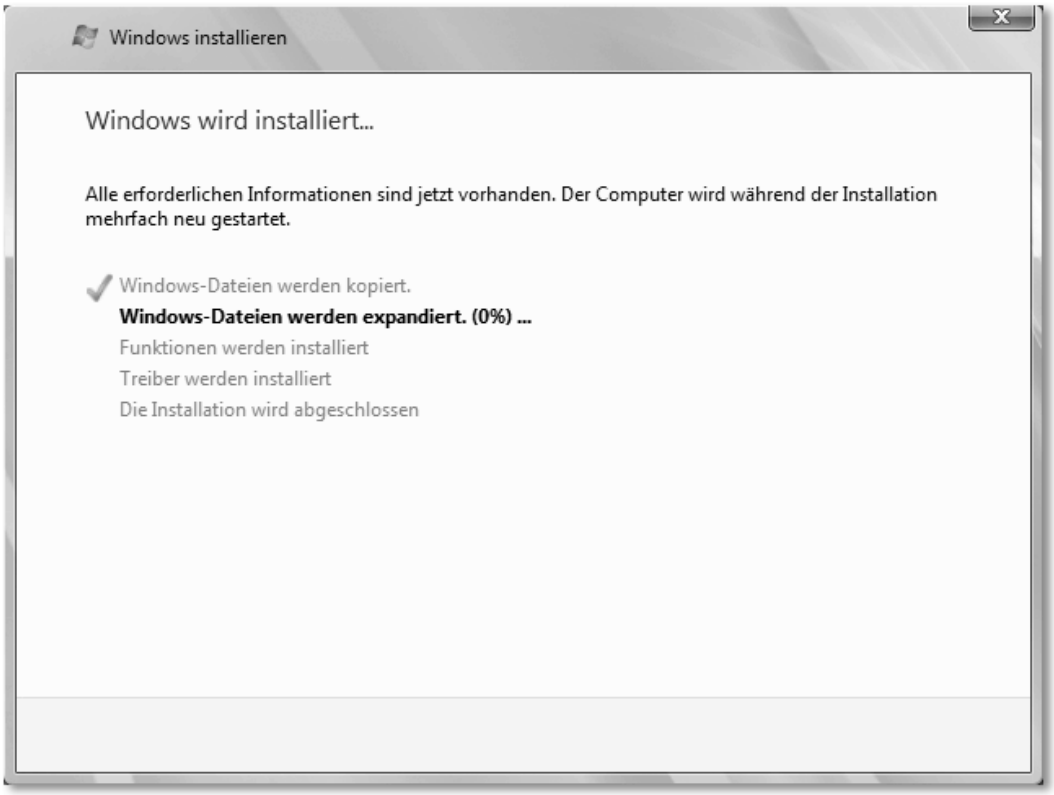


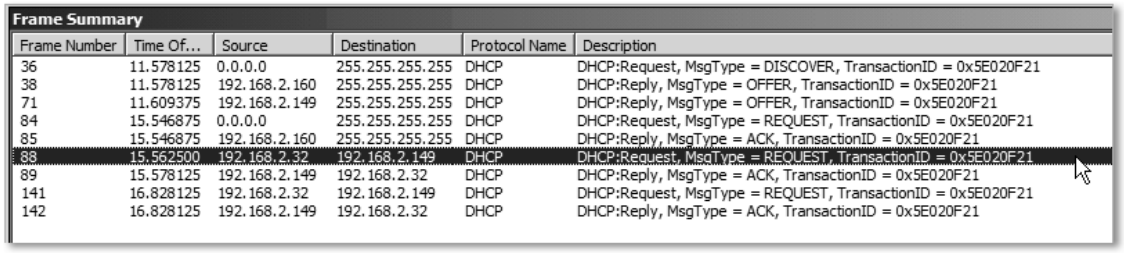
Abbildung 6.50 Die Installation läuft wie gewohnt ab.

6.5 PXE und TFTP – genauer hingeschaut

Um den Bootvorgang zu verstehen, kann es nicht schaden, ein wenig hinter die Kulissen zu schauen – in diesem Fall bedeutet das, den Netzwerkmonitor einzuschalten und ein wenig die Pakete zu betrachten. Die Messung, die hier gezeigt wird, habe ich mit dem *Microsoft Netzwerkmonitor 3.3* auf dem WDS-Server erstellt.

Zunächst sehen Sie auf Abbildung 6.51 den DHCP-Datenverkehr:

- Paket 36 ist der DHCP-Request des Clients.
- Paket 38 ist die Antwort des DHCP-Servers, in der eine IP-Adresse angeboten wird. Paket 71 ist die Antwort des WDS-Servers.
- Die Antwort des DHCP-Servers (#38) wird in der Tat verwendet, um eine IP-Adresse zu erhalten. In den Paketen 84 und 85 erfolgt die Anforderung der Lease der IP-Adresse (REQUEST) und die Bestätigung des Servers (ACK).
- Aus der Antwort des WDS-Servers (Paket 71) erfährt der Client, wo sich im Netz ein PXE-Server findet.



Frame Summary

Frame Number	Time Of...	Source	Destination	Protocol Name	Description
36	11.578125	0.0.0.0	255.255.255.255	DHCP	DHCP:Request, MsgType = DISCOVER, TransactionID = 0x5E020F21
38	11.578125	192.168.2.160	255.255.255.255	DHCP	DHCP:Reply, MsgType = OFFER, TransactionID = 0x5E020F21
71	11.609375	192.168.2.149	255.255.255.255	DHCP	DHCP:Reply, MsgType = OFFER, TransactionID = 0x5E020F21
84	15.546875	0.0.0.0	255.255.255.255	DHCP	DHCP:Request, MsgType = REQUEST, TransactionID = 0x5E020F21
85	15.546875	192.168.2.160	255.255.255.255	DHCP	DHCP:Reply, MsgType = ACK, TransactionID = 0x5E020F21
88	15.562500	192.168.2.32	192.168.2.149	DHCP	DHCP:Request, MsgType = REQUEST, TransactionID = 0x5E020F21
89	15.578125	192.168.2.149	192.168.2.32	DHCP	DHCP:Reply, MsgType = ACK, TransactionID = 0x5E020F21
141	16.828125	192.168.2.32	192.168.2.149	DHCP	DHCP:Request, MsgType = REQUEST, TransactionID = 0x5E020F21
142	16.828125	192.168.2.149	192.168.2.32	DHCP	DHCP:Reply, MsgType = ACK, TransactionID = 0x5E020F21

Abbildung 6.51 Der DHCP-Datenverkehr

Interessant ist nun Paket 88: Dort meldet sich der Client mit einer festen IP-Adresse beim WDS-Server und führt ein REQUEST durch. Da er durch die Antwort auf den ursprünglichen PXE-Request ja bereits erfahren hat, wo im Netz sich ein PXE-Server befindet (Paket 71), wendet er sich gezielt an diesen. Er fordert dabei allerdings keine IP-Adresse an (die hat er ja schon), sondern fragt nach einer Bootdatei – in dem DHCP-Request sind entsprechende Flags gesetzt.

Abbildung 6.52 zeigt die Detailansicht von Paket 89, also der Antwort des WDS-Servers auf die Anfrage nach der Bootdatei. Wie Sie sehen, wird ein BootFileName übermittelt (siehe Markierung). Die angegebene Datei finden Sie übrigens auch im Dateisystem des WDS-Servers – natürlich unterhalb des als Remoteinstallationsordners angegebenen Pfads (Abbildung 6.53).

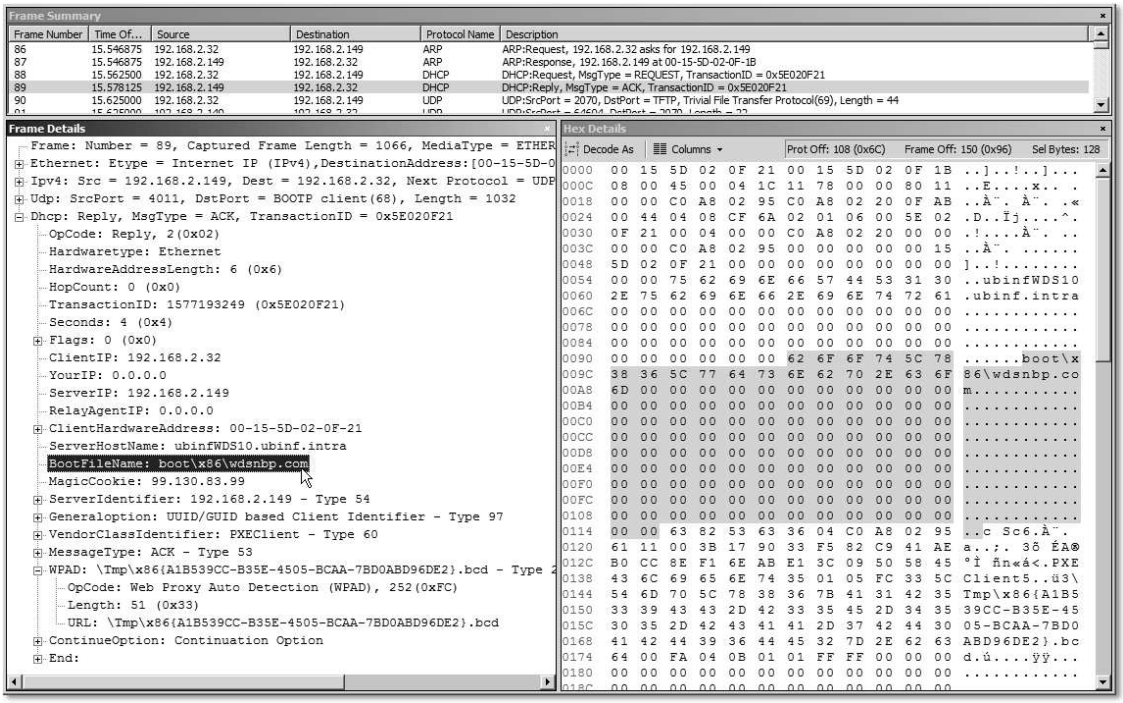


Abbildung 6.52 Die Detailansicht von Paket 89

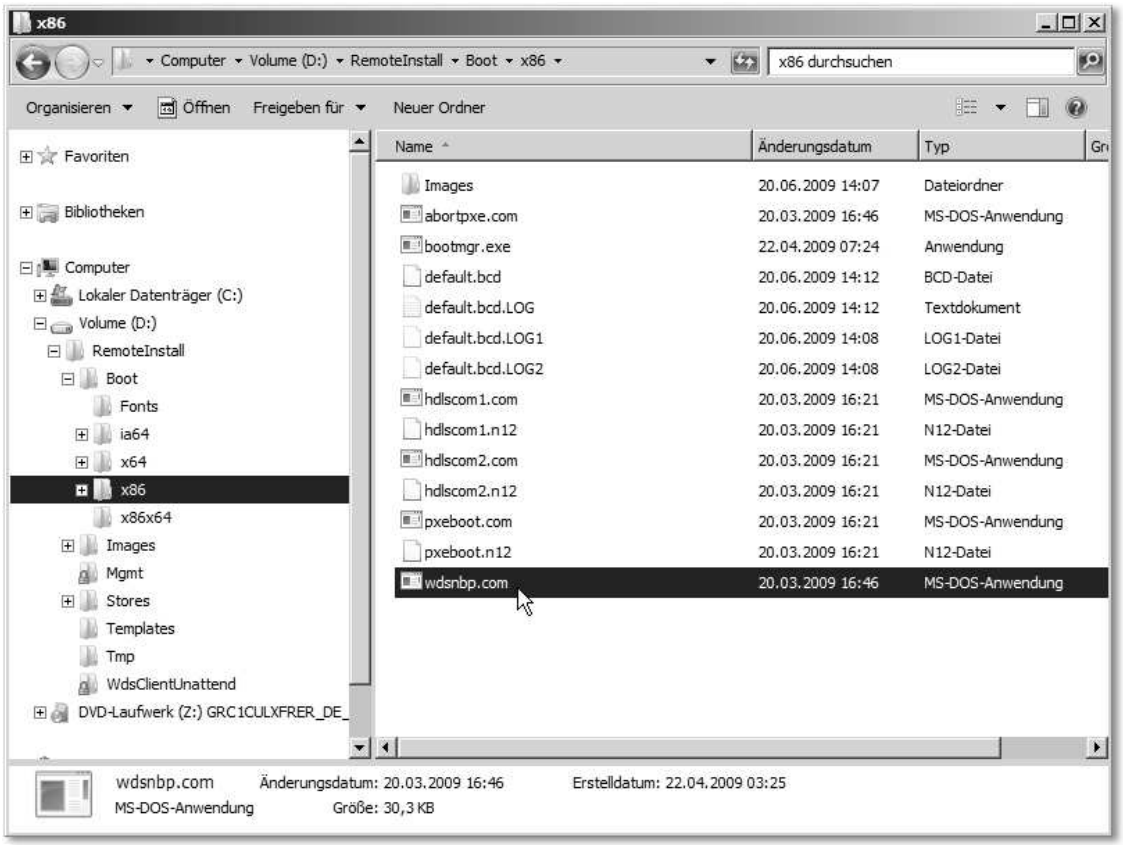
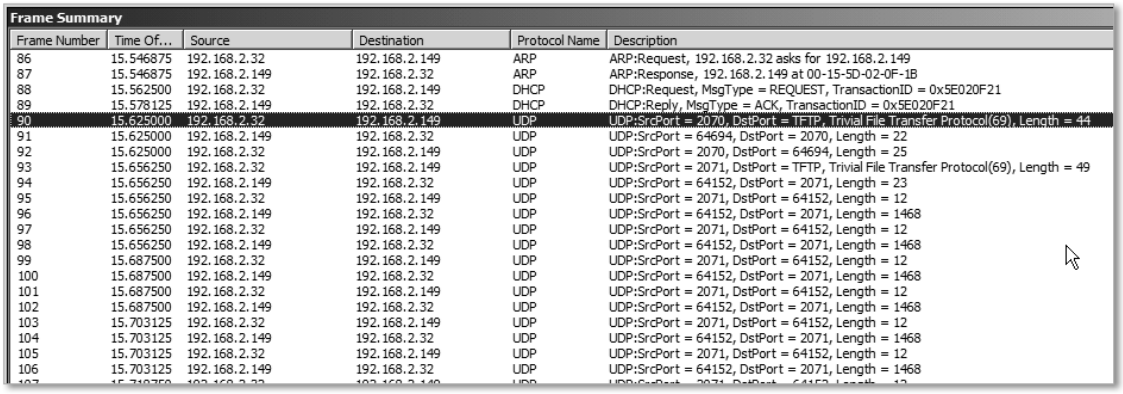


Abbildung 6.53 Das angegebene Boot-File findet sich auch im Dateisystem des Bereitstellungsdienst-Servers wieder.

Auf Abbildung 6.54 ist zu sehen, was nach der Übermittlung des Boot-File-Namens geschieht (Paket 90 ff.): Die Datei wird mittels FTFP (Trivial File Transfer Protocol) heruntergeladen und ausgeführt. TFTP ist wie der Name schon sagt (»Trivial…«) ein außerordentlich simpel gehaltenes Protokoll zur Dateiübertragung, das viele Möglichkeiten des großen Bruders FTP nicht unterstützt – die braucht es zum einfachen Herunterladen einer Datei im Übrigen ja auch nicht. Wie Sie im Netzwerkmonitor sehen, verwendet es für die Übertragung das UDP-Protokoll und nicht TCP wie das »große FTP«.



Frame Summary

Frame Number	Time Of...	Source	Destination	Protocol Name	Description
86	15.546875	192.168.2.32	192.168.2.149	ARP	ARP:Request, 192.168.2.32 asks for 192.168.2.149
87	15.546875	192.168.2.149	192.168.2.32	ARP	ARP:Response, 192.168.2.149 at 00-15-5D-02-0F-1B
88	15.562500	192.168.2.32	192.168.2.149	DHCP	DHCP:Request, MsgType = REQUEST, TransactionID = 0x5E020F21
89	15.578125	192.168.2.149	192.168.2.32	DHCP	DHCP:Reply, MsgType = ACK, TransactionID = 0x5E020F21
90	15.625000	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2070, DstPort = TFTP, Trivial File Transfer Protocol(69), Length = 44
91	15.625000	192.168.2.149	192.168.2.32	UDP	UDP:SrcPort = 64694, DstPort = 2070, Length = 22
92	15.625000	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2070, DstPort = 64694, Length = 25
93	15.656250	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2071, DstPort = TFTP, Trivial File Transfer Protocol(69), Length = 49
94	15.656250	192.168.2.149	192.168.2.32	UDP	UDP:SrcPort = 64152, DstPort = 2071, Length = 23
95	15.656250	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2071, DstPort = 64152, Length = 12
96	15.656250	192.168.2.149	192.168.2.32	UDP	UDP:SrcPort = 64152, DstPort = 2071, Length = 1468
97	15.656250	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2071, DstPort = 64152, Length = 12
98	15.656250	192.168.2.149	192.168.2.32	UDP	UDP:SrcPort = 64152, DstPort = 2071, Length = 1468
99	15.687500	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2071, DstPort = 64152, Length = 12
100	15.687500	192.168.2.149	192.168.2.32	UDP	UDP:SrcPort = 64152, DstPort = 2071, Length = 1468
101	15.687500	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2071, DstPort = 64152, Length = 12
102	15.687500	192.168.2.149	192.168.2.32	UDP	UDP:SrcPort = 64152, DstPort = 2071, Length = 1468
103	15.703125	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2071, DstPort = 64152, Length = 12
104	15.703125	192.168.2.149	192.168.2.32	UDP	UDP:SrcPort = 64152, DstPort = 2071, Length = 1468
105	15.703125	192.168.2.32	192.168.2.149	UDP	UDP:SrcPort = 2071, DstPort = 64152, Length = 12
106	15.703125	192.168.2.149	192.168.2.32	UDP	UDP:SrcPort = 64152, DstPort = 2071, Length = 1468

Abbildung 6.54 Nachdem die DHCP-Modalitäten ausgehandelt sind, beginnt die Übertragung mit TFTP.

Wenn Sie zu Abbildung 6.51 zurückblättern, sehen Sie, dass in den Pakten 141 und 142 noch einmal ein DHCP-Kommunikationsvorgang zwischen dem Client und dem WDS-Server durchgeführt wird. Dieser Effekt ist ganz einfach zu erklären:

- Der Benutzer erhält vom Code des zuerst geladenen Boot-Files die Aufforderung, F12 zu drücken (das kann man übrigens in den Eigenschaften des WDS-Servers auch anders konfigurieren). Weiterhin würde, sofern mehrere infrage kommende Bootimages vorhanden sind, ein Dialog zur Auswahl des Bootimages erscheinen.
- Hat der Benutzer F12 gedrückt, wird die eigentliche Windows-Vorinstallationsumgebung gestartet. In Paket 141 wird über das DHCP-Protokoll der entsprechende BootFileName übermittelt. Dies ist auf Abbildung 6.55 zu sehen. Bei genauem Hinsehen werden Sie feststellen, dass die Datei aus dem *x64*-Verzeichnis geladen wird. Offensichtlich wird also von dem zuerst ausgeführten Boot-File die Architektur des Computers bestimmt und dann per DHCP das passende Boot-File ermittelt.
- Ab Paket 143 beginnt dann wieder ein TFTP-Vorgang, der wieder das ermittelte Boot-File lädt, das dann zur Ausführung gebracht wird und die Windows-Vorinstallationsumgebung startet.

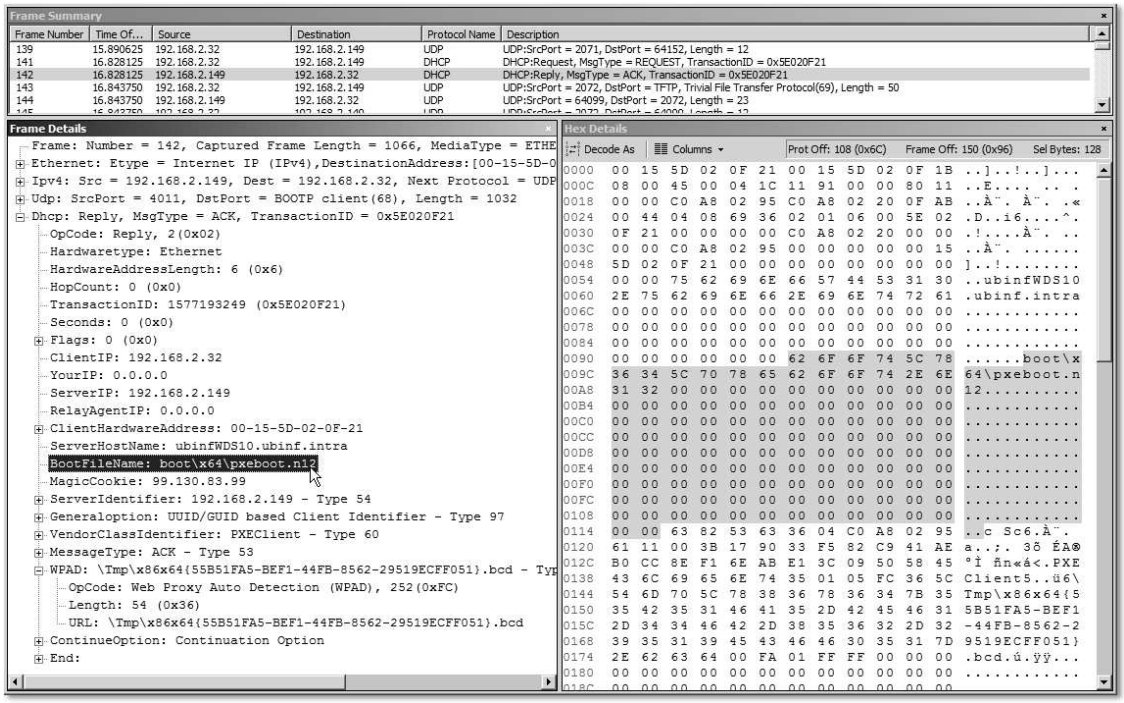


Abbildung 6.55 Die Detailansicht von Paket 141

Wenn der WDS-Server, genauer gesagt dessen PXE-Server-Komponente, dem Client nicht antwortet, wird sich die auf Abbildung 6.56 gezeigte Situation ergeben. Der Client wird zunächst anzeigen, dass er einen DHCP-Vorgang durchführt, nach ca. einer Minute wird der Client aber mit der Meldung abbrechen, dass er keinen Boot-File-Namen erhalten hat. Als PXE-Experte wissen Sie nun, dass ein DHCP-OFFER-Paket des PXE-Servers erwartet wurde und nicht kam (vgl. Abbildung 6.51, Paket 71).

Abbildung 6.56 So sieht es aus, wenn kein PXE-Server antwortet.

Im Grunde genommen ist der PXE-Vorgang also wirklich weder Hexenwerk noch Raketentechnik: Er ergänzt auf recht simple Art und Weise das vorhandene DHCP-Verfahren.

Bei der Installation der Windows-Bereitstellungsdienste werden übrigens einige Ausnahmen in der Windows-Firewall konfiguriert. Wenn der Bootvorgang partout nicht funktionieren will, wäre an dieser Stelle beispielsweise ein Ansatzpunkt.

Weiterhin dürfen Sie natürlich nicht vergessen, ein Startabbild hinzuzufügen (siehe auch Abbildung 6.41). Als letzte Nothilfe können Sie natürlich auch mit dem Netzwerkmonitor arbeiten und prüfen, ob die PXE-Komponente des WDS-Servers überhaupt antwortet.

6.6 WDS-Startvorgang automatisieren

In Abschnitt 6.3, »Installationsimage vorbereiten – erster Durchlauf«, habe ich Ihnen gezeigt, wie Sie eine automatisierte Installation durchführen können. Eine vollkommen automatisch ablaufende Installation wäre natürlich auch in Verbindung mit den Windows-Bereitstellungsdiensten fein.

Es gibt beim Deployment grundsätzlich zwei Teilbereiche, die Sie betrachten müssen:

- die Automatisierung der Installation des Windows-Bereitstellungsdienste-clients, beispielsweise die Auswahl der Sprache, des zu verwendenden Images, die Partitionierung der Festplatte etc.
- die automatisierte Anpassung des Betriebssystems, um zum Beispiel den Rechnernamen festzulegen, einen Produkt-Key einzutragen, der Domäne beizutreten oder um die Standardseite des Internet Explorers festzulegen

Für beide Aufgaben müssen XML-Dokumente erstellt werden, die die notwendigen Einstellungen und Antworten enthalten. Freundlicherweise hilft Ihnen bei der Erstellung der *Windows System Image Manager* (WSIM), den Sie bereits bei der ersten in diesem Kapitel durchgeführten unbeaufsichtigten Installation verwendet haben (siehe Abschnitt 6.3).

Anzumerken wäre allerdings, dass Sie nicht einfach die zuvor erstellte Datei für die unbeaufsichtigte Installation (*autounattend.xml*) verwenden können – die Verwendung der WDS erfordert eine leicht veränderte Konfiguration.

Ein wesentlicher Aspekt der unbeaufsichtigten Installation bei der Nutzung der Windows-Bereitstellungsdienste ist, dass Sie für die beiden Teilbereiche des Deployment-Vorgangs jeweils eine eigene Datei für die unbeaufsichtigte Abarbeitung erstellen müssen.

Um dieses Zwei-Phasen-Modell zu verdeutlichen, habe ich eine kleine Skizze erstellt (Abbildung 6.57):

- Zunächst erfolgt ein PXE-Bootvorgang.
- Ist dieser erfolgreich, läuft der Windows-Bereitstellungsdiensteclient. Dieser partitioniert beispielsweise die Festplatte und bringt das WIM-Image auf diese

auf. Dies ist der erste zu automatisierende Vorgang – vermutlich möchten Sie das ja nicht per Hand erledigen.

- Nachdem das WIM-Image aufgespielt worden ist, wird der PC neu gestartet. Er bootet nun von der Festplatte.
- In 99,9 % der Fälle kann ein Image nicht ohne weitere Anpassung verwendet werden – sonst hätten ja beispielsweise sämtliche PCs den gleichen Namen und die gleiche SID. Das WIM-Image wird also mit *SYSPREP.exe* »verallgemeinert«. Es wird somit beim Startvorgang etliches abfragen, wie beispielsweise den Rechnernamen, den zu verwendenden Lizenz-Key und einiges andere mehr. Dies ist der zweite zu automatisierende Vorgang.

Anmerkung

Zum letzten Punkt wäre anzumerken, dass bei der Installation eines Standard-WIM-Images von den Installations-DVDs ebenso eine Abfrage grundlegender Parameter erfolgt – das kennt jeder, der jemals ein Betriebssystem installiert hat. Die Standard-WIMs sind ebenso »verallgemeinert«, wie Sie es mit *SYSPREP.exe* für eigene WIMs vornehmen müssen.

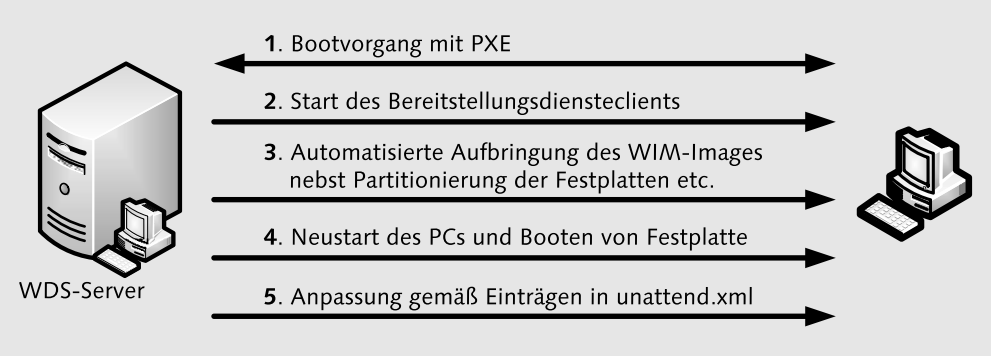


Abbildung 6.57 Der Ablauf der Installation bei der Nutzung der Windows-Bereitstellungsdienste

6.6.1 Automatisierung der Installation des Windows-Bereitstellungsdienstclients

Zunächst kümmern wir uns um die Automatisierung des Windows-Bereitstellungsdienstclients. Das hört sich ein wenig sperrig an, beschreibt aber lediglich, was zu tun ist, damit das zu installierende WIM-Image ohne weitere Benutzereingaben auf die Festplatte kommt.

Antwortdatei erstellen

Im *Windows System Image Manager* (WSIM) laden Sie zunächst ein Image und rufen anschließend das Erstellen einer neuen Antwortdatei auf.

Den Umgang mit dem WSIM habe ich bereits in Abschnitt 6.3.1, »Antwortdatei vorbereiten«, vorgeführt, blättern Sie gegebenenfalls nochmals dorthin zurück. Um eine Antwortdatei für den Bereitstellungsdiensteclient zu erzeugen, fügen Sie wie gewohnt die benötigten Einstellungen hinzu. Relevant sind allerdings nur diejenigen, die zum ersten Abschnitt der Antwortdatei hinzugefügt werden können; im Kontextmenü der Einstellung muss der Menüpunkt Einstellung zu Pass 1 windowsPW hinzufügen auswählbar sein (Abbildung 6.58).

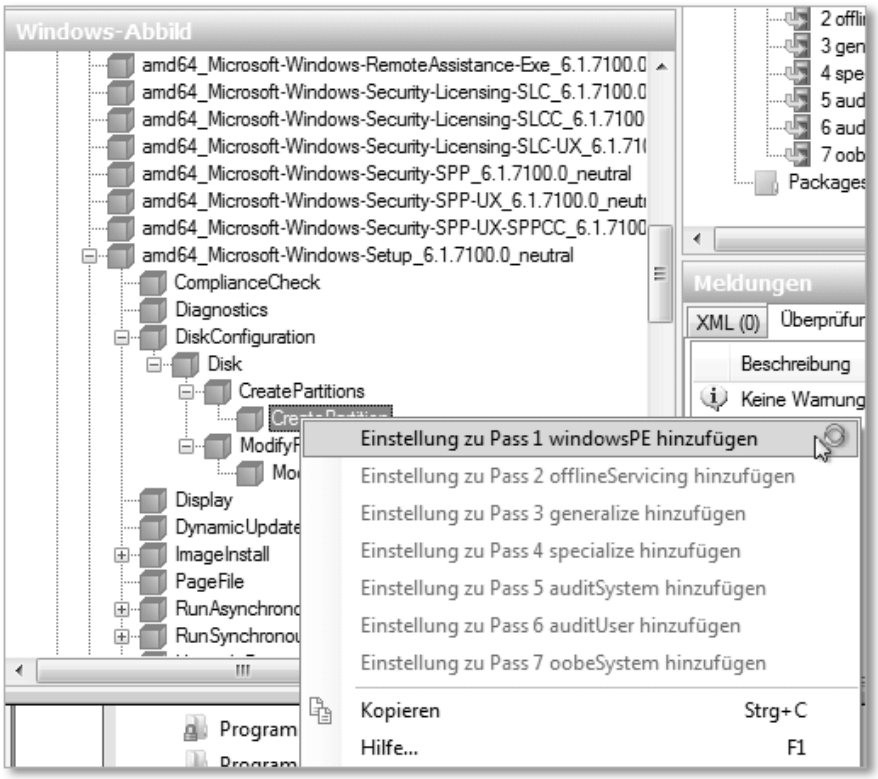


Abbildung 6.58 Einstellungen werden der Antwortdatei hinzugefügt.

Abbildung 6.59 zeigt, wie in etwa eine Antwortdatei aussehen muss, die die grundlegenden Anforderungen erfüllt:

- Es wird angegeben, welche Sprache (bzw. Lokalisierung) verwendet werden soll. In Deutschland wäre das de-DE.
- Weiterhin muss die Plattenkonfiguration vorgenommen werden. Falls Sie planen, BitLocker zu verwenden, müssen zwei Partitionen erstellt werden: eine kleine Systempartition (200 MB) und eine große Hauptpartition.
- Der dritte notwendige Abschnitt ist passend mit Windows DeploymentServices überschrieben. Hier wird festgelegt, welches Image auf welche Partition installiert werden soll. Außerdem werden ein Benutzername und ein Kennwort benötigt, um die Verbindung zum WDS-Server aufzubauen.

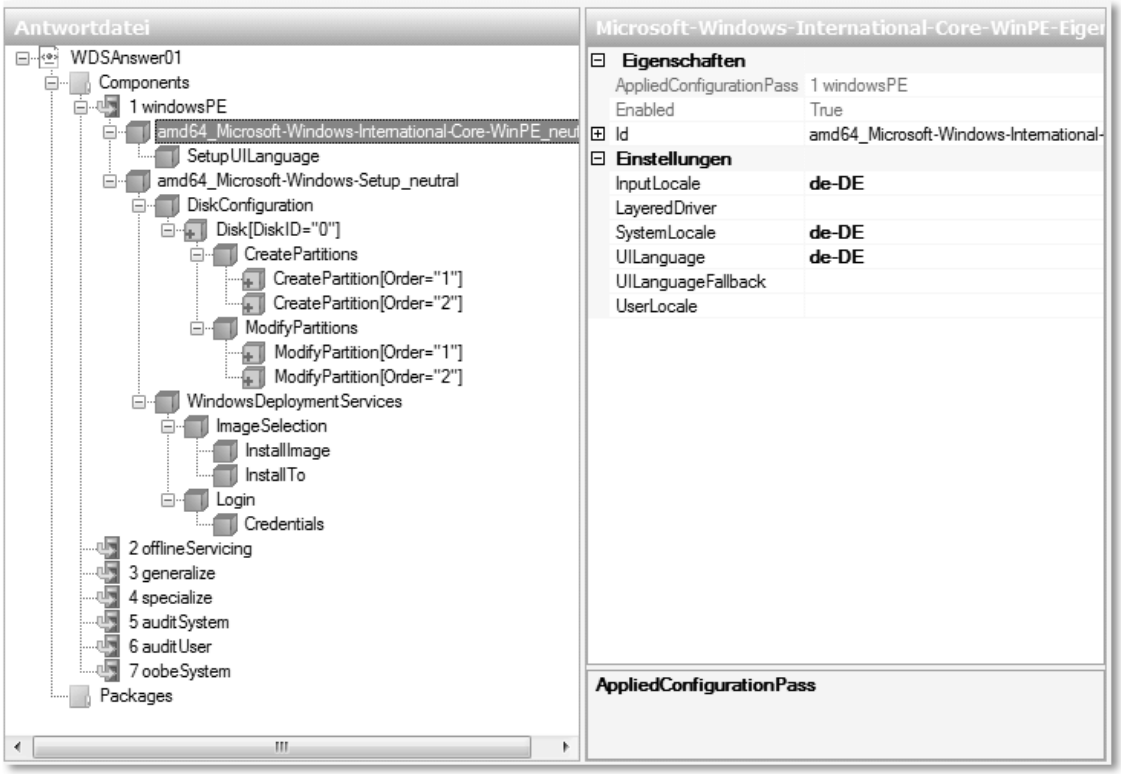


Abbildung 6.59 Erstellen einer Antwortdatei mit WSIM

Damit Sie die Einstellungen direkt nachvollziehen können, enthält Tabelle 6.3 die notwendigen Einstellungen, um eine automatische Verarbeitung der vom Windows-Bereitstellungsdienstclient durchgeführten Schritte zu realisieren. Die gezeigten Einstellungen gehen von folgender Annahme aus:

- Es ist eine Festplatte im PC vorhanden, auf die auch installiert wird. Diese Festplatte wird komplett gelöscht (`WillWipeDisk`).
- Es werden zwei Partitionen angelegt; eine erste 200 MB große Partition wird aktiv gesetzt. Als »eigentliche« Windows-Partition wird eine zweite eingerichtet, die dann den kompletten restlichen Bereich der Platte einnimmt (`Extend=true`).
  Die Bezeichnungen (Labels) der Partitionen sind übrigens beliebig.

Diese Plattenkonfiguration eignet sich übrigens für eine Benutzung von BitLocker.

Einstellung	Werte
Microsoft-Windows-International-Core-WinPE	InputLocale=de-DE SystemLocale=de-DE UILanguage=de-DE
Microsoft-Windows-International-Core-WinPE N SetupUILanguage	UILanguage=de-DE
Microsoft-Windows-Setup N DiskConfiguration N Disk[DiskID="0"]	DiskID=0 WillWipeDisk=true
Microsoft-Windows-Setup N DiskConfiguration N Disk[DiskID="0"] N CreatePartitions N CreatePartition[Order="1"]	Extend=false Order=1 Size=200 Type=Primary
Microsoft-Windows-Setup N DiskConfiguration N Disk[DiskID="0"] N CreatePartitions N CreatePartition[Order="2"]	Extend=true Order=2 Type=Primary
Microsoft-Windows-Setup N DiskConfiguration N Disk[DiskID="0"] N ModifyPartitions N ModifyPartition[Order="1"]	Active=true Format=NTFS Label=System Order=1 PartitionID=1
Microsoft-Windows-Setup N DiskConfiguration N Disk[DiskID="0"] N ModifyPartitions N ModifyPartition[Order="2"]	Format=NTFS Label=Windows Order=2 PartitionID=2
Microsoft-Windows-Setup N WindowsDeploymentServices N ImageSelection N InstallImage	Filename= ImageGroup= ImageName= (siehe Erläuterungen)
Microsoft-Windows-Setup N WindowsDeploymentServices N ImageSelection N InstallTo	DiskID=0 PartitionID=2
Microsoft-Windows-Setup N WindowsDeploymentServices N Login N Credentials	Domain= Password= Username= (siehe Erläuterungen)

Tabelle 6.3 Mit diesen Einstellungen lässt sich eine Automatisierung des Bereitstellungsdiensteclients realisieren.

Zu den Einstellungen in Microsoft-Windows-Setup • WindowsDeployment-Services • ImageSelection • InstallImage hätte ich noch einen kleinen Hinweis: Konfiguriert wird hier, welches auf dem WDS-Server gespeicherte Image auf die Platte kopiert werden soll.

Abbildung 6.60 zeigt ein Beispiel für die Konfiguration der entsprechenden Einstellungen – so weit, so gut. Die Frage ist allerdings, wie man nun die richtigen Einstellungen im konkreten Fall ermittelt – beispielsweise ist der Dateiname ja nicht unbedingt »sprechend«. Die Aufgabe ist aber ganz simpel zu lösen (Abbildung 6.61 sagt mehr als tausend Worte):

- Suchen Sie im Verwaltungswerkzeug für die Windows-Bereitstellungsdienste das gewünschte Image heraus.
- Rufen Sie dessen Eigenschaften auf. Dort finden Sie alle benötigten Einstellungen.

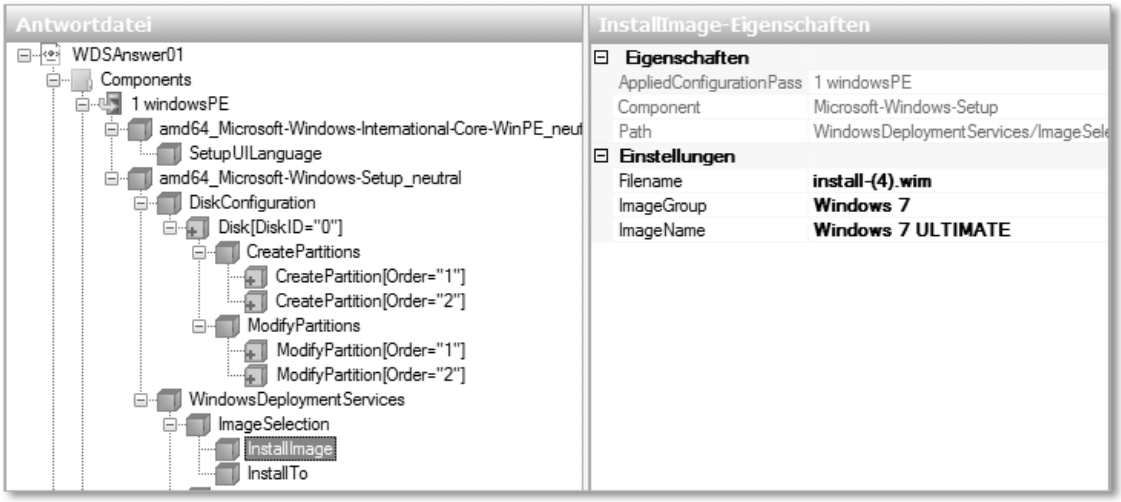


Abbildung 6.60 Ein Beispiel für die Auswahl des WIM-Images, das Sie per WDS installieren

Der zweite erwähnenswerte Aspekt sind die benötigten Anmeldeinformationen. Damit der Bereitstellungsdienstclient überhaupt auf das Image zugreifen kann, muss er sich gegenüber dem WDS-Server authentifizieren – das könnte man zwar auch abstellen, aber eigentlich ist es ja nicht schlecht, wenn keine beliebigen anonymen Zugriffe notwendig sind. Das Konto für die Authentifizierung wird in der entstehenden XML-Datei im Klartext gespeichert, es ist also keine gute Idee, ausgerechnet den Domänenadmin zu verwenden (Abbildung 6.62 zeigt die Konfiguration im WSIM).

Ein Blick auf die Registerkarte Benutzerberechtigungen eines Images zeigt, dass Authentifizierte Benutzer standardmäßig lesenden Zugriff haben – das genügt (Abbildung 6.63).

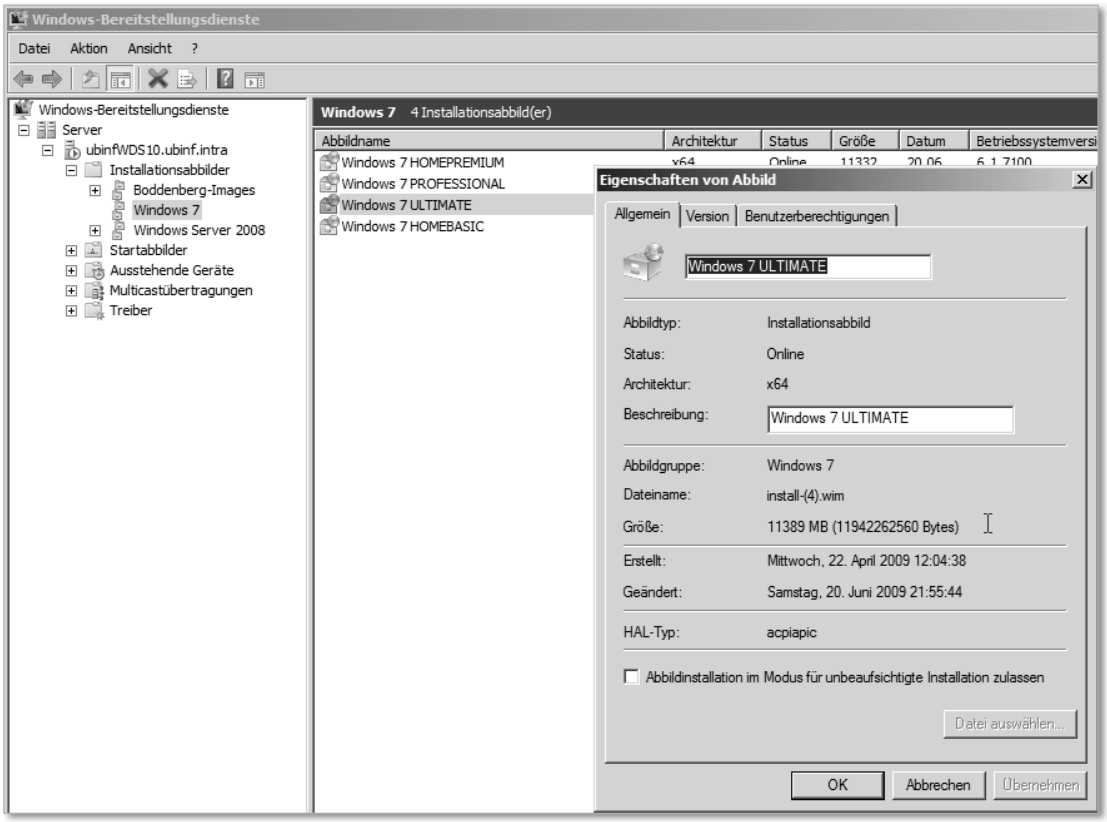


Abbildung 6.61 Hier können Sie die benötigten Informationen über das Image ermitteln.

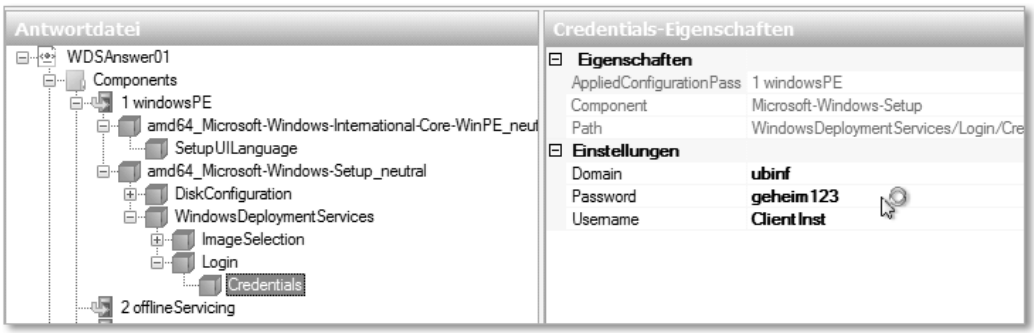


Abbildung 6.62 In der Konfigurationsdatei müssen Sie Credentials für den Zugriff auf den WDS-Server angeben.

Legen Sie also ein Benutzerkonto für diesen Zweck im Active Directory an. Dieses Konto sollte keine administrativen Rechte haben, sondern einfach ein Konto für einen simplen Benutzer sein.

Die fertige Antwortdatei muss in das Verzeichnis *WdsClientUnattend* im Remoteinstallationsordner gespeichert werden, also beispielsweise nach *d:\RemoteInstall\WdsClientUnattend*. Der Dateiname ist beliebig. Wählen Sie einen sprechenden Namen, der Ihnen auch in drei Jahren noch verrät, was Sie mit dieser Datei bezwecken wollten.

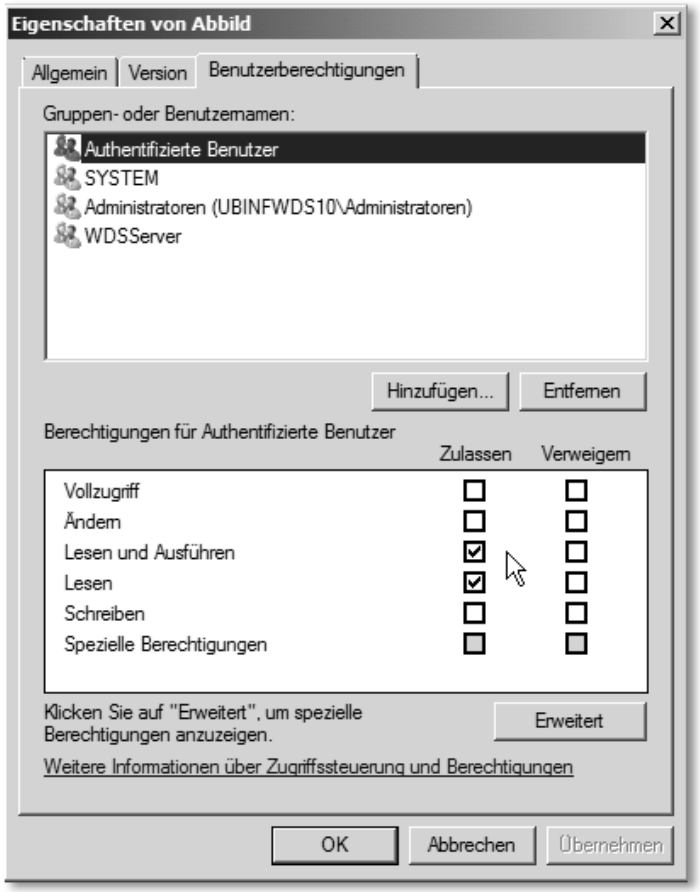


Abbildung 6.63 Standardmäßig kann jeder authentifizierte Benutzer auf das WIM-Image zugreifen.

Vor dem Speichern der Antwortdatei sollten Sie den Menüpunkt EXTRAS • ANTWORTDATEI ÜBERPRÜFEN ausführen. Eine erfolgreiche Überprüfung sagt zwar nichts darüber aus, ob die Antwortdatei dann tatsächlich zu dem gewünschten Ergebnis führen wird – immerhin sind aber keine groben Syntaxfehler in der Datei.

Bereitstellungsdienste anpassen

Damit tatsächlich eine unbeaufsichtigte Installation durchgeführt wird, rufen Sie im Eigenschaften-Dialog des Servers im WDS-Verwaltungswerkzeug die Registerkarte CLIENT auf (Abbildung 6.64). Dort können Sie einerseits die unbeaufsichtigte Installation grundsätzlich aktivieren und andererseits für jede Hardwarearchitektur eine Antwortdatei auswählen.

Es ist nun durchaus möglich, dass Sie für bestimmte PCs oder PC-Gruppen eine individuelle Antwortdatei wählen möchten. Da in der Antwortdatei auch das Installationsimage angegeben wird (Abbildung 6.60), ermöglicht die Verwendung von verschiedenen Antwortdateien implizit auch individuelle WIM-Zuweisungen.

Das Zuweisen einer individuellen Antwortdatei an einen Client ist allerdings nicht mit der grafischen Oberfläche möglich, dies muss mit WDSUTIL auf der Kommandozeile erfolgen – ich zeige Ihnen das ein wenig später in Abschnitt 6.7, »Computer vorab bereitstellen«.

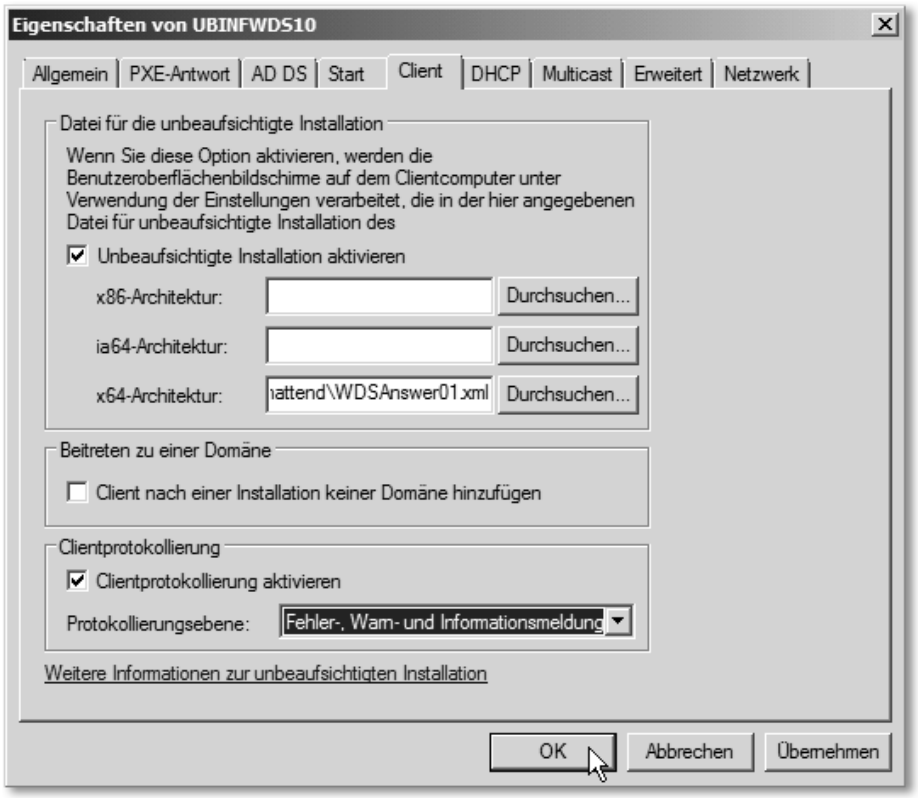


Abbildung 6.64 Aktivieren Sie die unbeaufsichtigte Installation, und wählen Sie eine Antwortdatei für die Plattform aus.

Probleme?

Wie immer gilt: »Nobody is perfect.« Auch wenn Sie die Antwortdatei in WSIM überprüft haben, ist es denkbar, dass die Antwortdatei nicht »läuft« bzw. zu falschen Ergebnissen führt.

Der deutlichste Fall ist, dass der Installationsprozess abgebrochen werden muss. Ein Beispiel sehen Sie auf Abbildung 6.65. Hier konnte dem Datenträger 0 übrigens deshalb keine Volumenbezeichnung zugewiesen werden, weil das zu verwendende Dateisystem bei der Einstellung ModifyPartition vergessen wurde.

Wenn die Installation grundsätzlich zwar funktioniert, aber Verlauf und/oder Ergebnis des Installationsvorgangs nicht den Vorstellungen entsprechen, gibt es ein ausführliches Logfile, in dem Sie nachschauen können. Im Verzeichnis *c:\windows\panther* des frisch installierten Betriebssystems finden sich einige hilfreiche Dateien, unter anderem auch die *setupact.log*. Abbildung 6.66 zeigt den Abschnitt

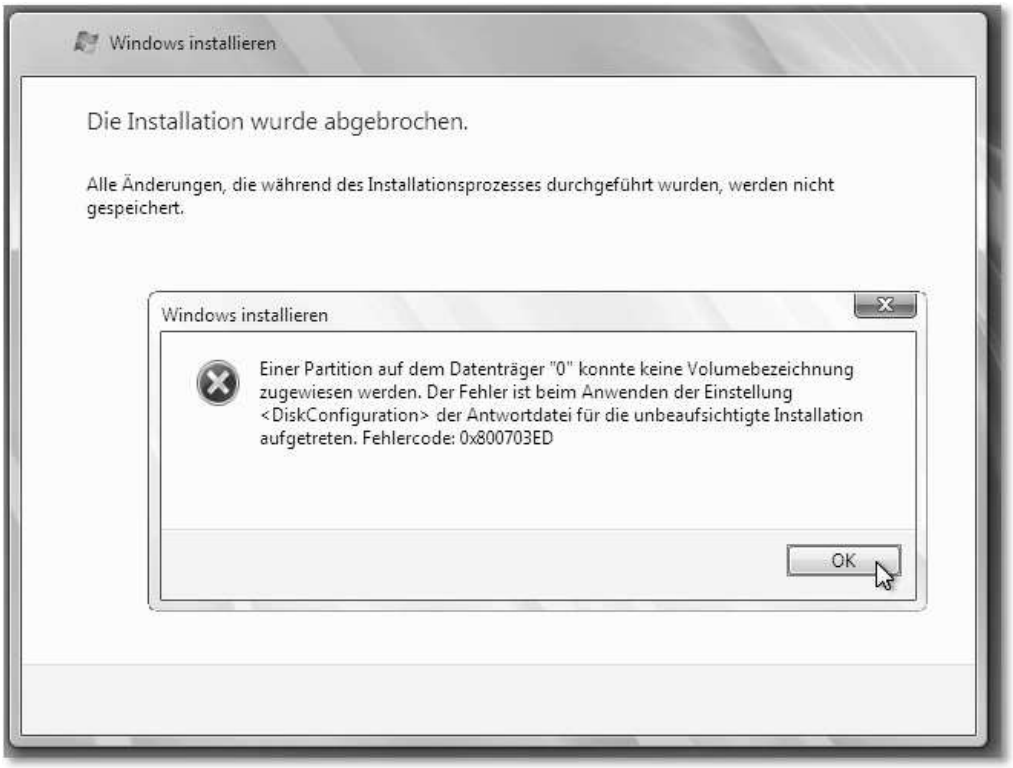


Abbildung 6.65 Ist die Antwortdatei fehlerhaft, erscheinen Meldungen wie diese.

der *setupact.log*, in dem das zu installierende Image selektiert wird. Sie sehen zunächst die Auflistung der vorhandenen Images, dann folgt die Zeile USER SELECTED A IMAGE... Es hat zwar kein Benutzer vor dem System gesessen, allerdings wurde die Auswahl per Antwortdatei getroffen – das funktioniert also!

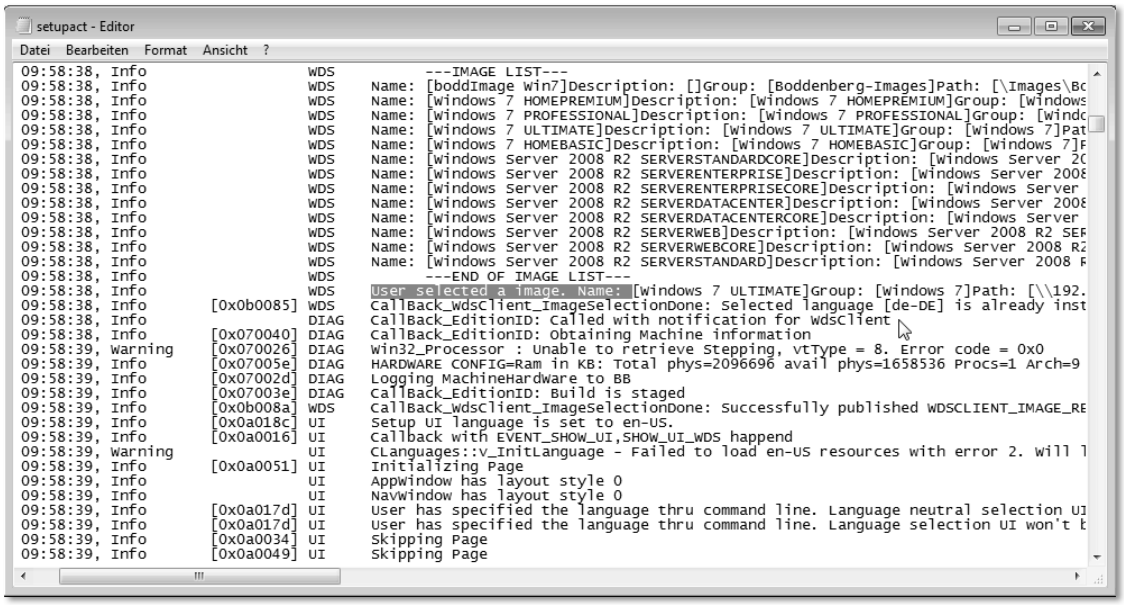


Abbildung 6.66 Hier ist der Abschnitt der »setupact.log«-Datei zu sehen, in dem das zu installierende Image ausgewählt wird.

Die *setupact.log*-Datei zu lesen ist zugegebenermaßen nicht in 10 Sekunden erledigt, da sie wirklich umfangreich ist. Sie müssen sich also zu dem gesuchten Abschnitt mehr oder weniger lange durchkämpfen. Haben Sie erst einmal den richtigen Abschnitt gefunden, steht in erschöpfender Ausführlichkeit drin, was benötigt wird.

6.6.2 Automatisierte Anpassung des Betriebssystems (Windows Setup)

Wenn das WIM-Image auf der Festplatte installiert ist, wird das frisch installierte Betriebssystem zum ersten Mal gestartet, und der »Rest« von Windows Setup läuft – zumindest dann, wenn das WIM-Image mit SYSPREP behandelt worden ist.

Das Mini-Setup, das bei einer mit SYSPREP behandelten Installation startet, fragt unter anderem die Eingabesprache, den Rechnernamen, lokal anzulegende Benutzer und dergleichen mehr ab. Ein gewollter »Nebeneffekt« von SYSPREP ist übrigens, dass die Betriebssysteminstanz eine neue SID (*Security Identifier*, diese sollen bzw. müssen in einer Domäne einzigartig sein) erhält und die Aktivierung erneut vorgenommen werden muss. Wenn Sie über den letzten Punkt erschrocken sind und erheblichen Aufwand durch die Aktivierung befürchten, möchte ich Ihnen direkt Kapitel 7, »Aktivierung«, empfehlen.

Neben den beschriebenen Konfigurationen und Anpassungen ist es beispielsweise erforderlich, den PC in die Domäne aufzunehmen. Für diesen Schritt soll natürlich auch kein Administrator losziehen müssen – das braucht er auch nicht, denn auch dies lässt sich natürlich automatisieren.

Antwortdatei erstellen

Das Erstellen der Antwortdatei geschieht wie gewohnt mit dem *Windows System Image Manager* (WSIM). Die Vorgehensweise funktioniert grundsätzlich so, wie auch schon in Abschnitt 6.3.1, »Antwortdatei vorbereiten« beschrieben wurde:

- Laden Sie zunächst ein WIM-Image.
- Erzeugen Sie eine neue Antwortdatei.
- Nehmen Sie die benötigten Änderungen vor.

Tabelle 6.4 zeigt die notwendigen Einstellungen für eine Antwortdatei, mit der Sie einen Installationsvorgang ohne Benutzereingriffe durchführen können. Bei Bedarf können Sie natürlich beliebige zusätzliche Einstellungen hinzufügen; dies ist die Minimalmenge an Einträgen. Abbildung 6.69 zeigt die Struktur der Antwortdatei im WSIM.

Unattended Windows Setup Reference

Teilweise sind die einzutragenden Werte im WSIM nicht so beschrieben, dass sich sofort die konkrete Bedeutung erschlösse. Das WAIK enthält eine Dokumentation namens *Unattended Windows Setup Reference*. Dort lassen sich beispielsweise auch Eigenschaften wie *ProtectYourPC* nachschlagen, unter denen man sich wirklich nichts vorstellen kann (dabei geht es übrigens um das automatische Einspielen von Updates).

Einstellung	Werte

Specialize N Microsoft-Windows-Shell-Setup	`ComputerName=%MACHINENAME%`
	`ProductKey=[Wert]`
	(siehe Erläuterungen)

Specialize N Microsoft-Widnows-Unattened-Join N Identification	`UnsecureJoin=true` (siehe Erläuterungen)

oobeSystem N Microsoft-Windows-International-Core	`InputLocale=de-DE`
	`SystemLocale=de-DE`
	`UILanguage=de-DE`
	`UserLocale=de-DE`

oobeSystem N Microsoft-Windows-Shell-Setup	`TimeZone=W.Europe Standard Time`

oobeSystem N Microsoft-Windows-Shell-Setup N OOBE	`HideEULAPage=true`
	`NetworkLocation=Work`
	`ProtectYourPC=1`

oobeSystem N Microsoft-Windows-Shell-Setup N UserAccounts N DomainAccounts	(siehe Erläuterungen)

Tabelle 6.4 Automatisierung des Windows Setup

Einige Aspekte der Antwortdatei sind durchaus erläuterungsbedürftig:

ProductKey: Sofern Sie mit einem MAK-Key (*Multiple Activation Key*) arbeiten, tragen Sie diesen hier ein. Falls Sie den *Key Management Service* (KMS) verwenden, tragen Sie hier den allgemeinen Schlüssel ein.

Wenn Sie keine Volumenlizenzierung verwenden, wird alles deutlich komplizierter, denn dann brauchen Sie für jede Betriebssysteminstanz einen anderen Key – sehr unpraktisch.

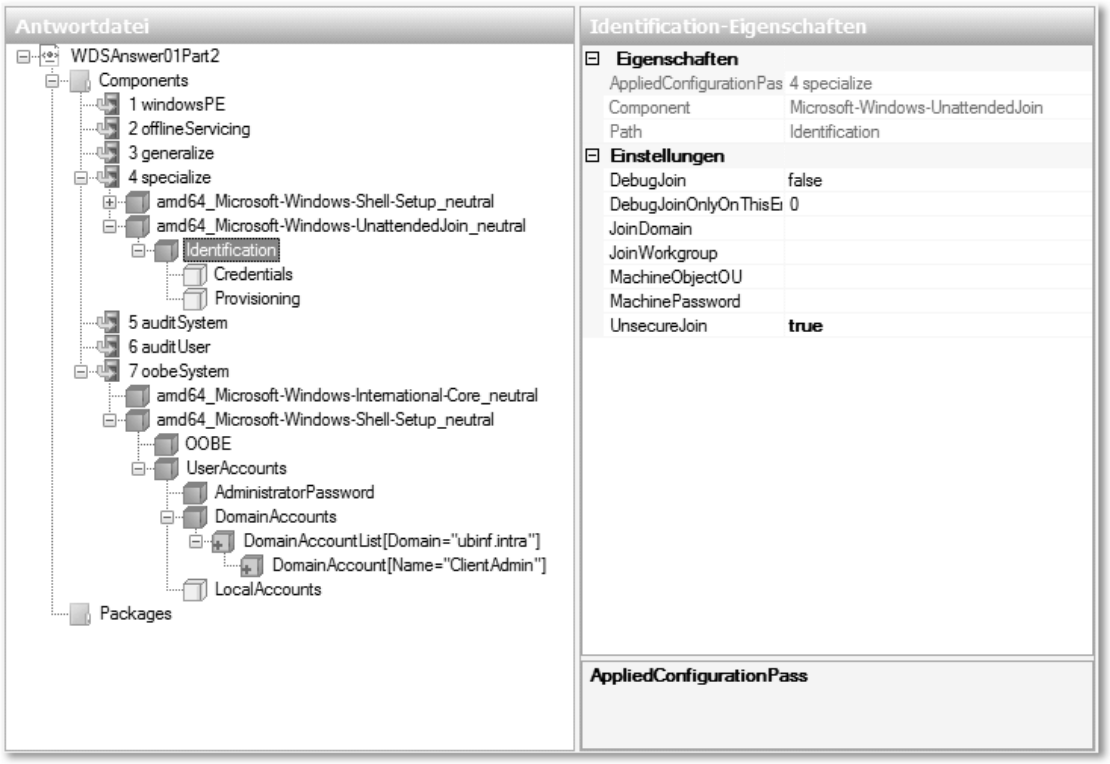


Abbildung 6.67 Die Antwortdatei im WSIM

Vermutlich soll der neu installierte PC Mitglied einer Domäne werden. Es gibt hier grundsätzlich zwei Verfahren:

- *SecureJoin*: Dies ist der »normale« Domänenbeitritt, bei dem ein entsprechend berechtigtes Benutzerkonto (z. B. Administrator) angegeben werden muss. Der Nachteil hierbei ist, dass das Kennwort des Kontos im Klartext in der Antwort gespeichert werden muss.
- *UnsecureJoin*: Bei diesem Verfahren werden keine Credentials in der Antwortdatei gespeichert. Stattdessen wird ein dynamisch generiertes Kennwort verwendet. Es wird in der ersten Phase des Installationsvorgangs erzeugt (Booten vom Netz und Aufbringen des Images) und dann in der zweiten Phase (Windows Setup) verwendet.

Der *UnsecureJoin* ist, trotz der Bezeichnung, nicht grundsätzlich unsicher. Es basiert seit Windows Vista auf einem dynamisch generierten Kennwort, sodass ein Angriff nicht sehr wahrscheinlich ist – oder anders gesagt: Man könnte einfacher angreifen, um Daten zu stehlen.

Wenn Sie Windows 7 installieren, wird standardmäßig nach einem lokalen Benutzerkonto gefragt. Auch wenn Sie kein lokales Konto anlegen möchten, ist dies kein optionaler Schritt – der Grund ist, dass das Administrator-Konto bei Windows 7 standardmäßig deaktiviert ist und ja schließlich ein Konto vorhanden sein

muss, mit dem eine Erstanmeldung erfolgen kann (das war übrigens auch bei Windows Vista so).

Wenn Sie nun in der Antwortdatei kein neues Benutzerkonto anlegen lassen, wird beim ersten Hochfahren des Betriebssystems ein Dialog erscheinen, der dieses lokale Konto erfragt – sehr lästig. Das Problem ist allerdings lösbar: Vermutlich haben Sie ohnehin ein Domänenkonto, das der lokalen Administratorengruppe hinzugefügt werden soll, ohne aber Domänenadministrator zu sein. Das ist das »typische« Helpdesk-Konto.

Wenn Sie in der Antwortdatei dieses Domänenkonto der lokalen Administratorengruppe hinzufügen, funktioniert alles so wie gedacht: Es kommt zu keiner Nachfrage nach einem lokalen Konto beim Windows Setup-Vorgang, und es wird kein lokales Konto angelegt.

Die Konfiguration des entsprechenden Abschnitts ist auf Abbildung 6.68 zu sehen. Im Knoten DomainAccountList wird noch die Domäne eingetragen.

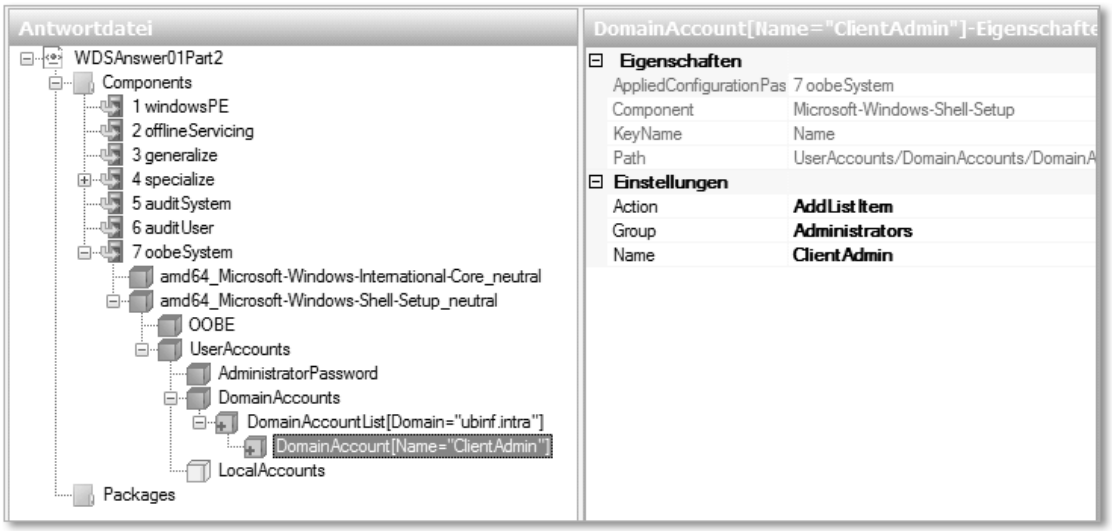


Abbildung 6.68 Hinzufügen eines Domänenkontos zu der lokalen Administratorgruppe

Bereitstellungsdienste anpassen

Um den Bereitstellungsdiensten beizubringen, dass im Anschluss an das Aufbringen des Images die neu erstellte Antwortdatei angewendet werden soll, gehen Sie so vor:

- Rufen Sie die Eigenschaften des Images auf (Abbildung 6.69).
- Aktivieren Sie die Checkbox Abbildinstallation im Modus für unbeaufsichtigte Installation zulassen.
- Wählen Sie die soeben erstellte Antwortdatei aus.

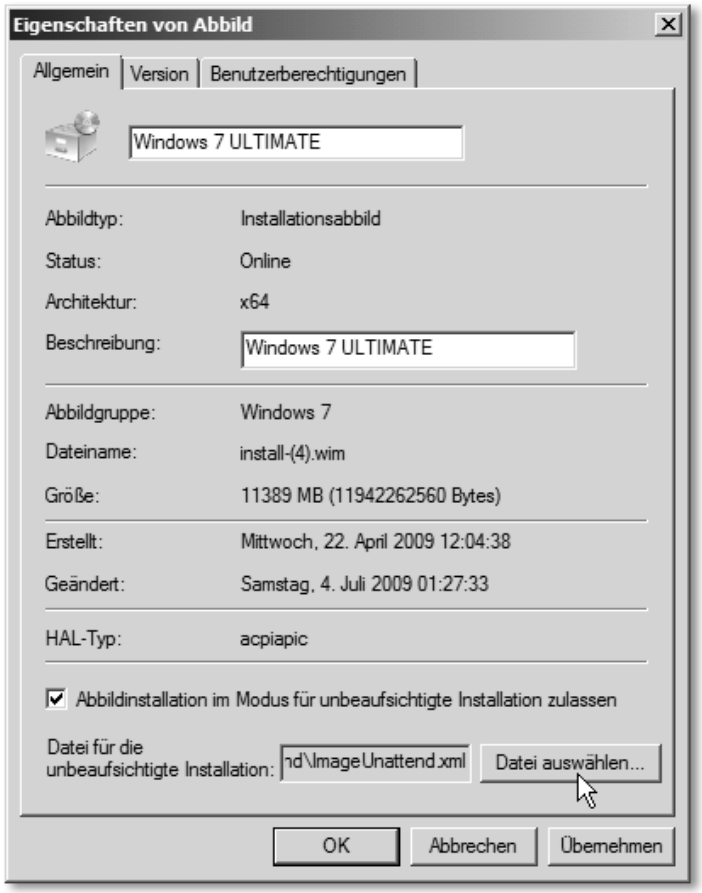


Abbildung 6.69 In den Eigenschaften des Images können Sie die »Abbildinstallation im Modus für unbeaufsichtigte Installation zulassen«.

Wenn Sie die Antwortdatei in dem Dialog auswählen, wird diese in ein Verzeichnis unterhalb des Remoteinstallationsorders auf dem WDS-Server kopiert und in *ImageUnattend.xml* umbenannt. In meinem Beispiel lautet der komplette Dateiname *D:\RemoteInstall\Images\Windows 7\install-(4)\Unattend\ImageUnattend.xml*.

6.6.3 Das Verfahren testen und prüfen

Nach Abschluss der Vorbereitungen können Sie den kompletten Installationsvorgang durchführen und testen:

- Nach dem NetzwerkBootvorgang wird die Festplatte eingerichtet und das WIM-Image auf die Festplatte kopiert. Die Automatisierung erfolgt durch die erste Antwortdatei (siehe Abschnitt 6.6.1, »Automatisierung der Installation des Windows-Bereitstellungsdienstclients«).
- Dann wird das neu installierte Windows gestartet und das Mini-Setup ausgeführt. Dieser Teil wird durch die zweite Antwortdatei automatisiert (siehe Abschnitt 6.6.2, »Automatisierte Anpassung des Betriebssystems«).

Auch wenn in der Theorie alles klar und eigentlich ganz logisch ist, können in der Praxis beim Windows Setup (zweiter Teil) Fehler auftreten. Dazu finden Sie nachfolgend einige Hinweise, Ergebnisse und Hintergründe.

Der Domänenbeitritt gelingt nicht

Es kann durchaus sein, dass der Beitritt zur Domäne nicht funktioniert. Wenn Sie in der Antwortdatei wie vorgeschlagen kein lokales Konto erstellen, sondern der lokalen Administratorgruppe ein Domänenkonto hinzugefügt haben, können Sie sich nicht anmelden:

- Das lokale Administrator-Konto ist deaktiviert, kann also für eine Anmeldung nicht verwendet werden.
- Wenn der PC nicht in die Domäne aufgenommen werden konnte, können Sie sich nicht mit einem Domänenkonto anmelden.

Abbildung 6.70 zeigt den Anmeldedialog eines PCs, bei dem der Domänenbeitritt nicht funktioniert hat: Unter den Eingabefeldern für Benutzername und Kennwort finden sich keinerlei Hinweise auf die Domäne.

Abbildung 6.70 Wenn sich der Anmeldebildschirm so darstellt, hat der Beitritt zur Domäne nicht funktioniert.

In diesem Fall können Sie die Installation direkt von vorn beginnen – allerdings sollten Sie das nicht tun, ohne den Fehler aufgespürt zu haben.

Warum kann der Beitritt zur Domäne fehlschlagen? Wenn man Schreibfehler ausschließen kann, handelt es sich vermutlich um ein Berechtigungsproblem:

- Bei einem SecureJoin hat das angegebene Konto nicht die Berechtigungen, um in der Organisationseinheit, in der das Computerkonto angelegt wird, Objekte zu erstellen.
- Wenn das Computerkonto bei einem UnsecureJoin bereits vorhanden ist, sollte es eigentlich kein Problem geben. Sofern das Computerkonto noch nicht vorhanden ist, muss das Konto, mit dem die erste Installationsphase durchgeführt wird (siehe Abschnitt 6.6.1, »Automatisierung der Installation des Windows-Bereitstellungsdienstclients«) in der OU Objekte erstellen und ändern dürfen.

Dialoge des Mini-Setups erscheinen

Wenn nach dem Neustart des installierten Betriebssystems Dialoge des Mini-Setups erscheinen (z. B. Sprache auswählen, Benutzer eingeben, Rechnernamen auswählen, Zeitzone bestimmen), sind nicht alle notwendigen Aspekte in der Antwortdatei konfiguriert worden. Wie auch in Tabelle 6.4 beschrieben, finden sich diese Einstellungen in der Phase oobeSystem der Antwortdatei (Abbildung 6.71):

- In den Eigenschaften des Knotens Microsoft-Windows-International-Core werden einige Einstellungen für die zu verwendende Sprache vorgenommen.
- Im Knoten Microsoft-Windows-Shell-Setup • OOBE werden weitere Automatisierungseinstellungen hinterlegt, beispielsweise das Überspringen der Anzeige der Lizenzbedingungen.

Abbildung 6.71 Die Einstellungen für das Mini-Setup finden sich in der Phase »oobeSystem«.

In Foren findet man regelmäßig Beispiele, in denen die Eigenschaften SkipMachineOOBE und/oder SkipUserOOBE auf `true` gesetzt werden (die Eigenschaften sind auf Abbildung 6.71 zu sehen). Bei einer solchen Konfiguration werden in der Tat keine Dialoge angezeigt, allerdings ist dies in der Dokumentation als »deprecated« (missbilligt) gekennzeichnet – Sie sollten also im Klartext diese Einstellung nicht benutzen.

Natürlich führt die Verwendung von SkipMachineOOBE dazu, dass kein Dialog des Mini-Setups angezeigt wird. Sie riskieren dadurch allerdings, dass unter Umständen benötigte Parameter nicht konfiguriert werden. Dies geschieht insbesondere dann, wenn in der Antwortdatei nicht alles vorhanden ist. Der »richtige Weg« ist also, so lange die Antwortdatei anzupassen, bis diese alle Fragen beantwortet und somit das Mini-Setup wirklich »stumm« durchläuft.

Wie bekommt der PC seinen Namen?

Jeder PC in einer Domäne benötigt einen individuellen Namen. Für die Vergabe des Namens gibt es drei Mechanismen:

- Die Bereitstellungsdienste können einen Namen für den PC erzeugen. Der auf Abbildung 6.72 gezeigte Dialog (Sie erreichen ihn über die Eigenschaften des WDS-Servers) zeigt die entsprechende Eingabemöglichkeit: Der PC kann beispielsweise mit dem Namen des Installationsbenutzers und einer laufenden Nummer versehen werden. Folgende Platzhalter stehen zur Verfügung:
  - `%First`: der Vorname des installierenden Benutzers
  - `%Last`: der Nachname des installierenden Benutzers
  - `%Username`: der Benutzername des installierenden Benutzers
  - `%MAC`: die Hardwareadresse der Netzwerkkarte des PCs
  - `%[0][n]#`: eine fortlaufende Nummer mit *n* Stellen.
- Der elegantere und in der Praxis meist verwendete Weg ist, die PCs vorab bereitzustellen. Dann erhalten diese genau den gewünschten Namen und nicht eine mehr oder weniger zufällig generierte Bezeichnung. Mehr zum Thema Bereitstellung finden Sie in Abschnitt 6.7, »Computer vorab bereitstellen«.
- Falls der PC bereits in der Domäne vorhanden war und neu installiert wird, erhält er denselben Namen wie vor der Neuinstallation.

Damit die Namenszuweisung tatsächlich reibungslos funktioniert, muss im WSIM und somit in der Antwortdatei die Variable `%MACHINENAME%` verwendet werden – ein Bild, nämlich Abbildung 6.73, sagt wie immer mehr als viele Worte.

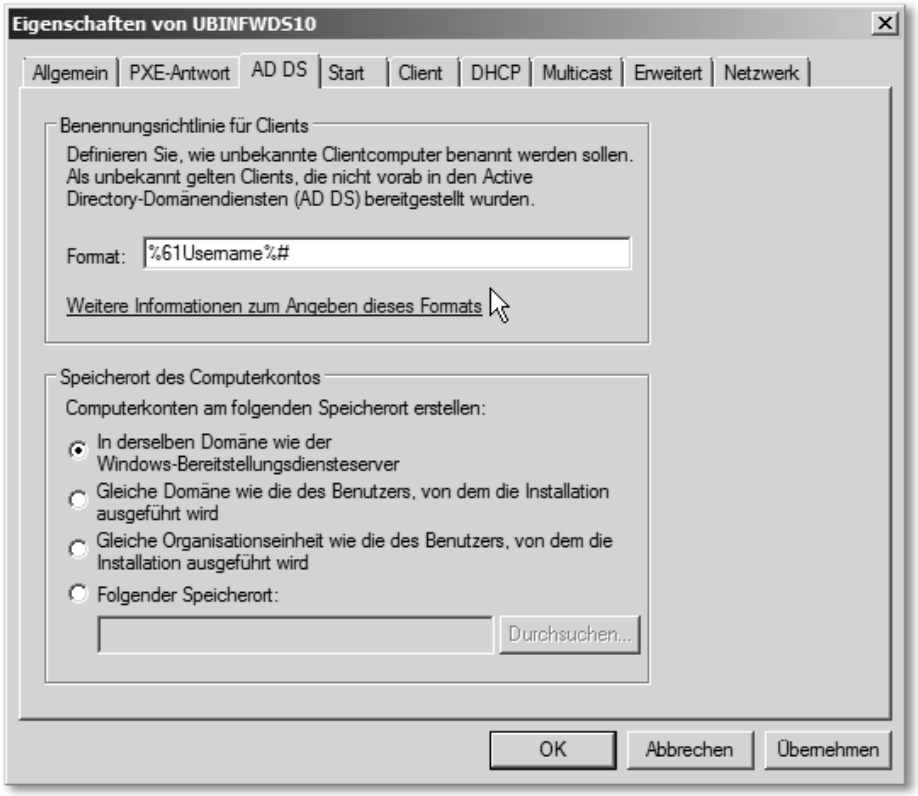


Abbildung 6.72 In diesem Dialog legen Sie fest, wie unbekannte Clients benannt werden sollen.

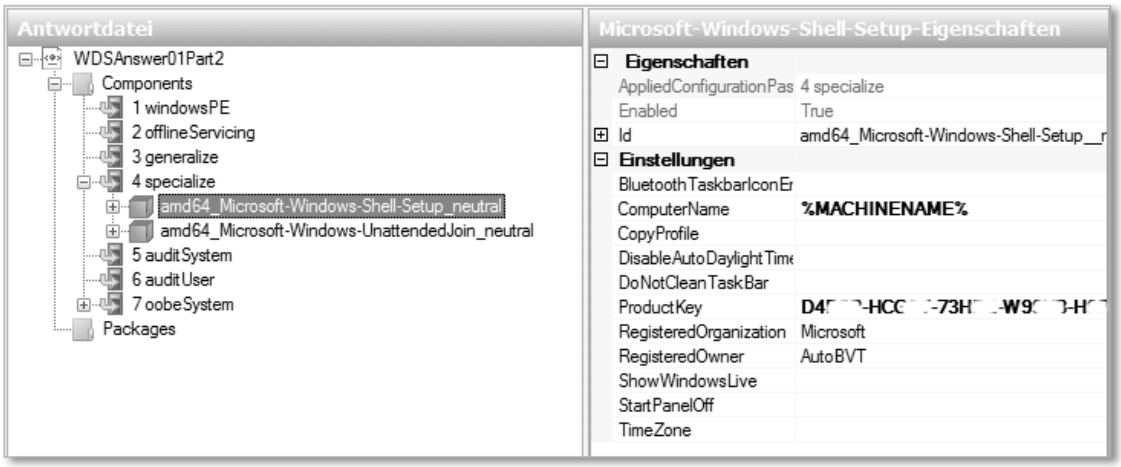


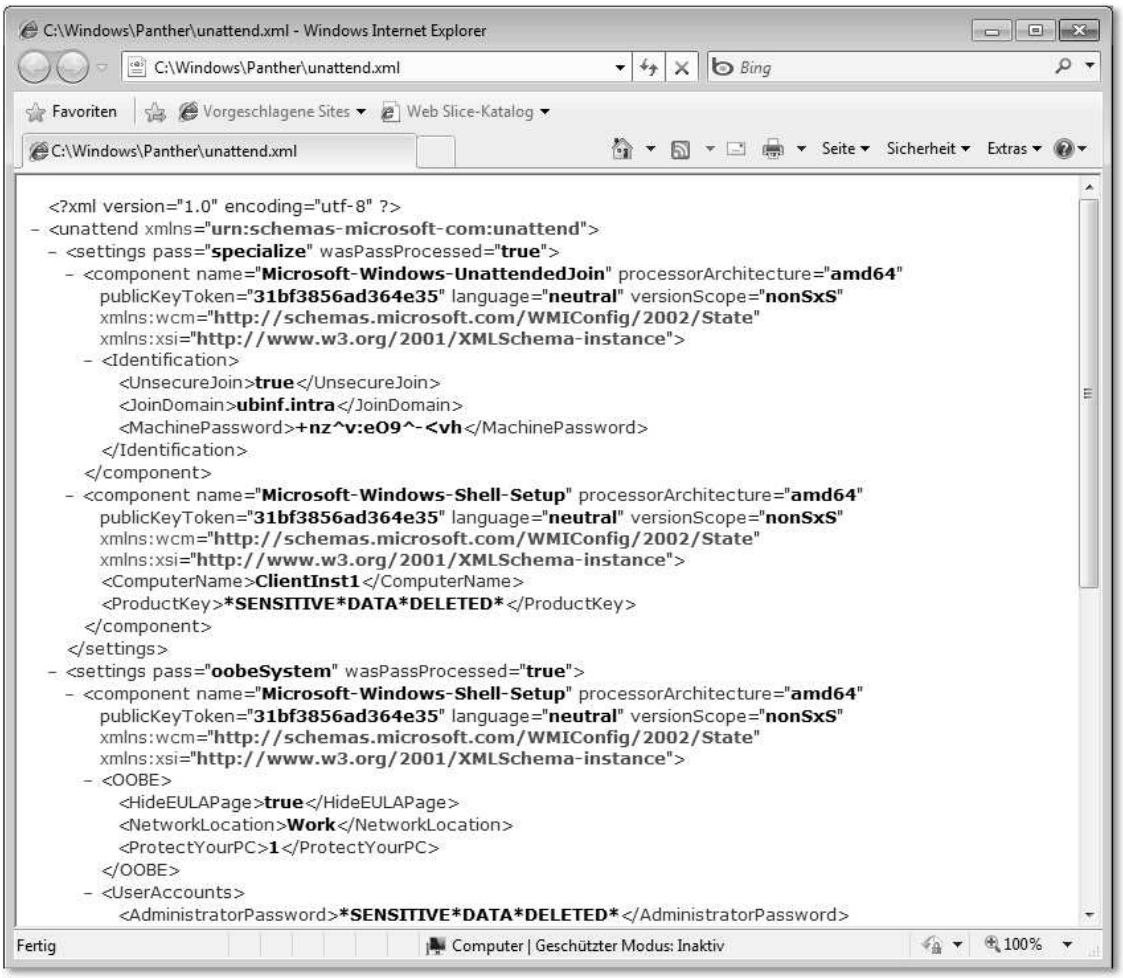
Abbildung 6.73 Als Computername muss die Variable »%MACHINENAME%« eingetragen werden.

Wie bekommt der PC die Antwortdatei?

Wir haben zwar nun die Antwortdatei erstellt und auf dem WDS-Server hinterlegt, interessant ist allerdings, wie diese modifiziert wird und dem Client bereitgestellt wird. Die im zweiten Installationsabschnitt (Windows Setup) verwendete

Antwortdatei findet sich im Pfad *C:\Windows\Panther\unattend.xml*. Abbildung 6.74 zeigt eine solche Datei. Sie sehen unter anderem, dass die Variable `%MACHINENAME%` durch einen konkreten Computernamen ersetzt worden ist.

Die individuelle Antwortdatei wird vor dem Start in die zweite Installationsphase, also nach dem Kopieren des Images auf die Festplatte, individualisiert, auf die Platte kopiert und dann vom Mini-Setup verwendet.




```
<?xml version="1.0" encoding="utf-8" ?>
- <unattend xmlns="urn:schemas-microsoft-com:unattend">
  - <settings pass="specialize" wasPassProcessed="true">
    - <component name="Microsoft-Windows-UnattendedJoin" processorArchitecture="amd64"
        publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
        xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      - <Identification>
          <UnsecureJoin>true</UnsecureJoin>
          <JoinDomain>ubinf.intra</JoinDomain>
          <MachinePassword>+nz^v:eO9^-<vh</MachinePassword>
        </Identification>
      </component>
    - <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
        publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
        xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <ComputerName>ClientInst1</ComputerName>
        <ProductKey>*SENSITIVE*DATA*DELETED*</ProductKey>
      </component>
    </settings>
  - <settings pass="oobeSystem" wasPassProcessed="true">
    - <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
        publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
        xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      - <OOBE>
          <HideEULAPage>true</HideEULAPage>
          <NetworkLocation>Work</NetworkLocation>
          <ProtectYourPC>1</ProtectYourPC>
        </OOBE>
      - <UserAccounts>
          <AdministratorPassword>*SENSITIVE*DATA*DELETED*</AdministratorPassword>
```

Abbildung 6.74 Dies ist die Datei »unattend.xml«, die in die Installation kopiert wurde. Beachten Sie, dass beispielsweise der »ComputerName« eingesetzt worden ist.

6.7 Computer vorab bereitstellen

Einen Test-PC per unbeaufsichtigtem Netzwerkbootvorgang installieren zu können, ist ja grundsätzlich schon »ganz nett«, im professionellen Umfeld genügt das aber bei Weiterem nicht. Hier muss jedem PC eine individuelle Bezeichnung zugewiesen werden, gegebenenfalls müssen auch separate WIM-Images ausgewählt werden. So wäre es denkbar, dass in der Installation für den Vertrieb bereits der

CRM-Client enthalten ist, während die Mitarbeiter in der Fertigung eine Software für die Fertigungssteuerung bekommen. Kurz gesagt ist es erforderlich, einem PC bereits Einstellungen (wie Name, Installations-Image) zuzuweisen, bevor dieser zum ersten Mal gebootet wird.

Vielleicht haben Sie auf der Suche nach einer solchen Einstellmöglichkeit bereits ein wenig das grafische WDS-Administrationswerkzeug durchforstet, dies allerdings wahrscheinlich erfolglos. Der Grund ist dabei nicht, dass solcherlei Einstellungen nicht getroffen werden könnten, sondern vielmehr, dass dies mit dem Kommandozeilenwerkzeug WDSUTIL vorgenommen werden muss. Keine Frage: Wäre dies im grafischen Werkzeug zu verwalten, wäre das sehr angenehm, es ist nun aber eben nicht möglich.

Active Directory-Werkzeug

Wenn es auf einem Server mit installierten Bereitstellungsdiensten installiert ist, bietet das Werkzeug *Active Directory-Benutzer und -Computer* eine Möglichkeit zum Anlegen eines neuen Computerkontos nebst Eintrag für MAC-Adresse bzw. GUID. Mehr dazu finden Sie in Abschnitt 6.7.3, »Computer mit Active Directory-Werkzeug anlegen«.

6.7.1 PC bereitstellen

Damit die Bereitstellungsdienste einen PC identifizieren können, den es im Unternehmen noch nie gegeben hat,der aber nun mit einem bestimmten Namen und einer bestimmten Konfiguration installiert werden soll, muss es ein Kriterium geben. Dieses Kriterium ist entweder die Hardwareadresse der Netzwerkkarte (MAC-Adresse) oder bei neueren Systemen eine GUID.

An diese Identität gelangen Sie beispielsweise dadurch, dass Sie den PC einschalten, beim Beginn des Netzwerkbootvorgangs anhalten (Pause-Taste) und dann ganz simpel abschreiben (Abbildung 6.75).

Abbildung 6.75 Bei den meisten PCs wird die MAC-Adresse des Clients beim Booten angezeigt.

Wenn Sie größere Chargen von PCs ins Feld bringen müssen und diese direkt am Arbeitsplatz des Benutzers installieren wollen, wäre es natürlich recht lästig,

wenn Sie erst den PC anschalten müssten, um die MAC-Adresse zu erhalten. Die Hersteller von für Unternehmen gedachten PCs sind mittlerweile darauf eingestellt, PCs mit Aufklebern mit mehr oder weniger umfangreichen Daten zu versehen. Hierzu zählen beispielsweise Kundenname, Bestellnummer und natürlich auch die MAC-Adresse der eingebauten Netzwerkkarte. Abbildung 6.76 zeigt einen Screenshot der Dell-Bestell-Website. Hier können Sie festlegen, welche Daten auf dem PC vermerkt werden sollen.

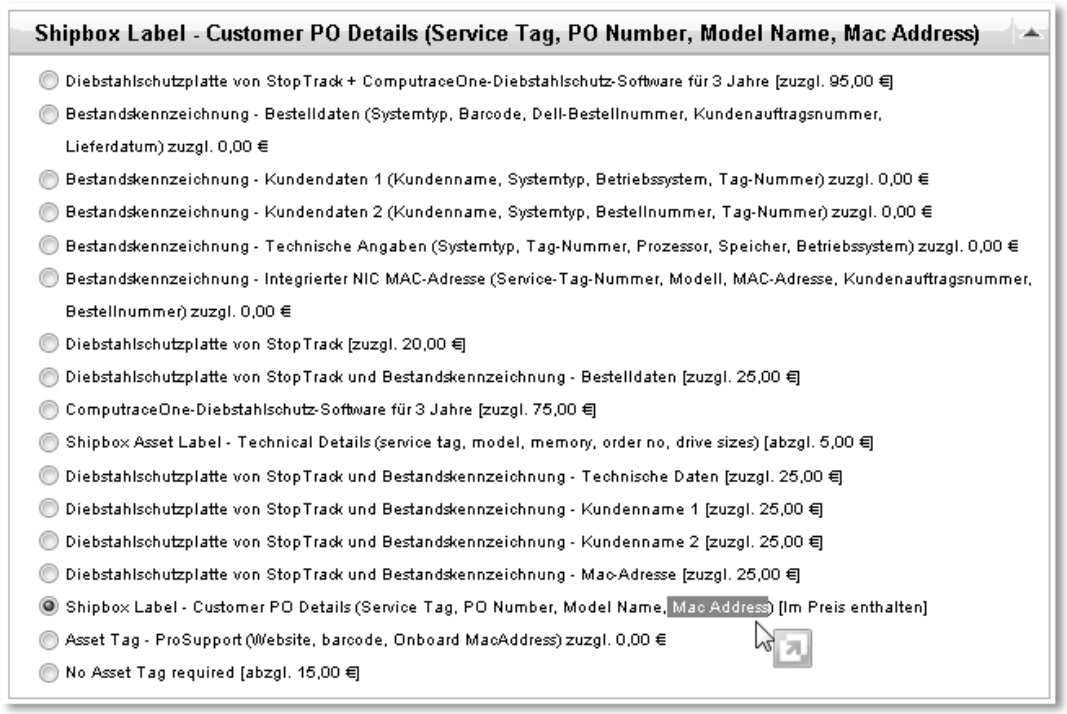


Abbildung 6.76 Bei Systemen für den Unternehmenseinsatz können Labels mit umfangreichen Daten, unter anderem auch mit der MAC-Adresse, geordert werden. (Quelle: Dell-Website)

Im günstigsten Fall übergeben Hersteller bzw. Lieferanten diese Daten auch elektronisch, sodass Sie MAC-Adressen und zu vergebende Namen leicht einlesen können.

Sie müssen nun für den neuen PC ein Computerkonto in der Domäne anlegen und die MAC-Adresse dort vermerken. WDSUTIL bietet hierfür eine Option, sodass die auf Abbildung 6.77 gezeigte Befehlszeile eingegeben werden kann. Das Ergebnis ist wie erwartet ein neues Computerkonto im Active Directory, wobei sich die MAC-Adresse im Attribut NETBOOTGUID wiederfindet (Abbildung 6.78).

Wenn ein bereits vorhandener PC neu installiert wird, beispielsweise aufgrund eines nicht behehbbaren Fehlers oder weil ein Betriebssystem-Update durchgeführt wird, erhält er denselben Namen wie bisher – der PC ist ja bereits im Active Directory bereitgestellt.

```
Microsoft Windows [Version 6.1.7100]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Administrator.UBINF>wdsutil  /Add-Device /Device:ubinfCli273 /ID:00-15-
5D-02-0F-23

Verwaltungsdienstprogramm für die Windows-Bereitstellungsdienste [Version 6.1.71
00.0]
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Der Befehl wurde erfolgreich ausgeführt.

C:\Users\Administrator.UBINF>
```

Abbildung 6.77 Mit WDSUTIL fügen Sie den Computer hinzu.

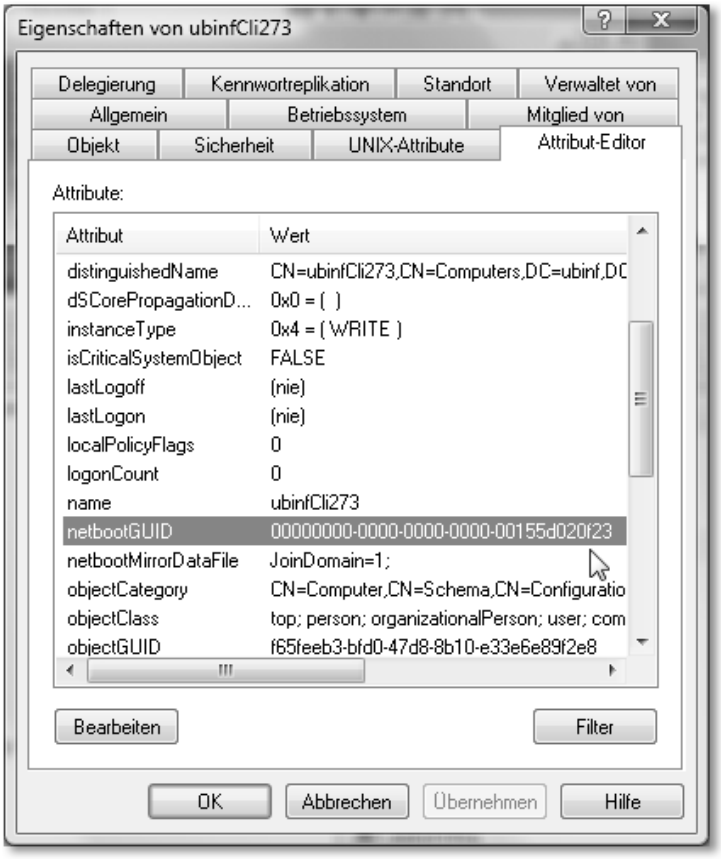


Abbildung 6.78 Das Computerkonto im AD-Adminwerkzeug nach dem Hinzufügen

Werte und Optionen

Wichtig ist, dass Sie bei der Erstellung der Antwortdatei als Wert für das Attribut ComputerName die Variable %MACHINENAME% einsetzen (siehe Tabelle 6.4).

Bei der Erstellung des Computerkontos benötigen Sie gegebenenfalls zusätzlich die Optionen /Domain und /OU, mit denen Sie steuern können, in welcher Domäne und Organisationseinheit das Computerkonto erstellt werden soll. Wenn Sie diese Optionen nicht eingeben, wird das Konto im Container Computers der aktuellen Domäne erstellt.

6.7.2 Weitere Möglichkeiten

Mit WDSUTIL lässt sich deutlich mehr realisieren, als »nur« ein Computerkonto anzulegen und das `netbootGUID`-Attribut zu setzen. Generell gilt, dass WDSUTIL über eine recht detaillierte Hilfefunktion verfügt. So führt beispielsweise die Eingabe des Befehls `WDSUTIL /add-device /?` zu einer recht ausführlichen Erläuterung der möglichen Eingabeoptionen (Abbildung 6.79).

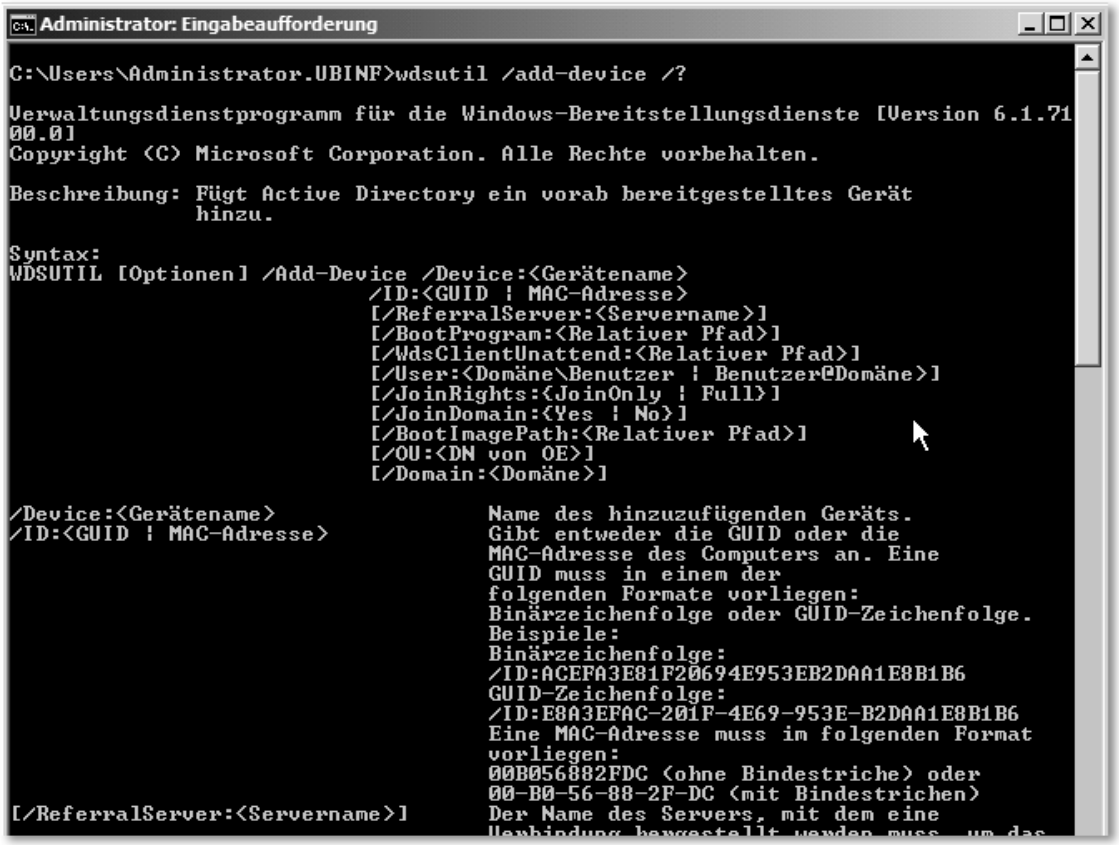


Abbildung 6.79 WDSUTIL verfügt über recht umfangreiche und auch größtenteils wirklich hilfreiche Hilfetexte.

Ohne jetzt jede einzelne Option ausführlich mit Beispielen erörtern zu wollen, sind die wichtigsten Optionen:

- Auswahl des zu verwendenden BootImages (/BootImagePath): Bei dieser Option wird der relative Pfad zum Boot-Image angegeben, das unterhalb des Remoteinstallationsordners liegt.
- Zur Konfiguration des Domänenbeitritts des PCs während des Setups gibt es zwei Optionen, nämlich /User und /JoinRights. Mit diesen beiden Optionen können Sie ein Benutzerkonto dazu berechtigen, den Domänenbeitritt für diesen PC durchzuführen. Das hier angegebene Konto muss in einer der Antwortdateien konfiguriert werden: Wenn in der Konfiguration der Antwortdatei für

den Windows-Bereitstellungsdiensteclient beispielsweise das Konto *ClientInst* angegeben ist, müssen diesem auch die Rechte zum Durchführen des Domänenbeitritts gewährt werden.

Es gibt übrigens noch eine weitere Option, nämlich /JoinDomain. Da der Standardwert aber das Beitreten zur Domäne ist, gibt es hier eigentlich keinen Handlungsbedarf.

- Ein wesentlicher Punkt ist die Option /WdsClientUnattend. Hier müssen Sie auswählen, welche Antwortdatei für den Windows-Bereitstellungsdiensteclient für den jeweiligen Client verwendet werden soll. Wie Sie aus Abschnitt 6.6.1 wissen, wird in dieser Datei unter anderem das zu installierende WIM-Image ausgewählt. Letztendlich ordnen Sie also über diese Option einem PC das zu installierende WIM-Image zu.

6.7.3 Computer mit Active Directory-Werkzeug anlegen

Das grafische WDS-Administrationswerkzeug verfügt zwar nicht über eine grafische Möglichkeit, um Computer vorab bereitzustellen (sprich, um ein Konto im AD anzulegen und das Attribut netbootGUID zu setzen), dafür wird das Werkzeug *Active Directory-Benutzer und -Computer* über ein Add-In erweitert. Dies gilt zumindest dann, wenn das AD-Benutzerverwaltungsprogramm auf dem WDS-Server läuft.

Hinweis

Mit dem Werkzeug *Active Directory-Benutzer und -Computer* einen Server zu installieren, ohne ihn zum Domänencontroller zu machen, ist eigentlich simpel. Sie fügen den Rollendienst *Active Directory-Domänendienste* hinzu. Das installiert zwar die entsprechenden Dateien, um aus dem Server aber tatsächlich einen Domänencontroller zu machen, ist die Ausführung von *dcpromo* erforderlich – und das machen Sie einfach nicht.

Hier nun ein kurzer Überblick über die Vorgehensweise beim Anlegen eines Computers:

- Wählen Sie im Werkzeug *Active Directory-Benutzer und -Computer* das Erstellen eines neuen Computerobjekts aus (im Kontextmenü des Containers, in dem es erstellt werden soll).
- Auf der ersten Seite des Assistenten können Sie den Computernamen erfassen. Außerdem kann ein Benutzer oder eine Gruppe angegeben werden, die den Benutzer an die Domäne anbinden kann. Hier wählen Sie das Benutzerkonto, mit dem der Windows-Bereitstellungsdiensteclient am WDS-Server authentifiziert wird (siehe Abschnitt 6.6.1, »Automatisierung der Installation

des Windows-Bereitstellungsdienstclients«). Den Dialog aus Abbildung 6.80 sehen Sie übrigens auch, wenn die Bereitstellungsdienste nicht installiert sind.

Abbildung 6.80 So legen Sie einen neuen Computer im »Active Directory-Benutzer und -Computer«-Werkzeug an.

- Auf der zweiten Seite des Assistenten tragen Sie die GUID bzw. die MAC-Adresse des Computers ein (Abbildung 6.81). Etwas technischer gesprochen, handelt es sich hier um den Wert, der später in das Attribut `netbootGUID` eingesetzt wird.

Abbildung 6.81 Auf der zweiten Seite des Assistenten können Sie eine Computer-ID eintragen.

Sie müssen hier übrigens eine GUID eintragen, ansonsten steht die Schaltfläche Weiter nicht zur Verfügung. Falls Sie nur die MAC-Adresse und nicht die GUID zur Verfügung haben, tragen Sie in die ersten vier Abschnitte der GUID Nullen (»0«) ein und in den letzten Abschnitt die MAC-Adresse. Eine MAC-Adresse 00-15-5D-02-0F-23 wird dann zu `{00000000-0000-0000-0000-00155D020F23}` (diese Umsetzung kann man übrigens erkennen, wenn man mit WDSUTIL eine Mac-Adresse hinzufügt).

- Die dritte Dialogseite ermöglicht das Eintragen des zu verwendenden Remoteinstallationsservers (WDS-Servers) – auch eine Einstellung, die man mit WDSUTIL vornehmen könnte, die hier aber ein wenig komfortabler möglich ist (Abbildung 6.82).

Abbildung 6.82 Bei Bedarf können Sie einen bestimmten Remoteinstallationsserver auswählen.

Dieser Assistent ist zwar schon recht hilfreich, leider fehlt die Möglichkeit, zu bestimmen, welche Antwortdatei der Bereitstellungsdiensteclient verwenden soll (WDSUTIL-Option: /WdsClientUnattend). Die Antwortdatei bestimmt letztendlich, welches WIM-Image auf die Maschine kopiert wird.

Das erweiterte Konfigurationswerkzeug *Active Directory-Benutzer und -Computer* bietet noch eine zusätzliche Unterstützung bei der Arbeit mit den Bereitstellungsdiensten. In den Eigenschaften eines Computerkontos findet sich nun die Registerkarte Remoteinstallation (Abbildung 6.83). Sofern ein bestimmter Remoteinstallationsserver für den Client konfiguriert ist, steht die Schaltfläche Servereinstellungen zur Verfügung. Ein Klick hierauf öffnet das Computer-

konto des WDS-Servers, in dessen Eigenschaften einige grundlegende Einstellungen für die Bereitstellungsdienste getroffen werden können.

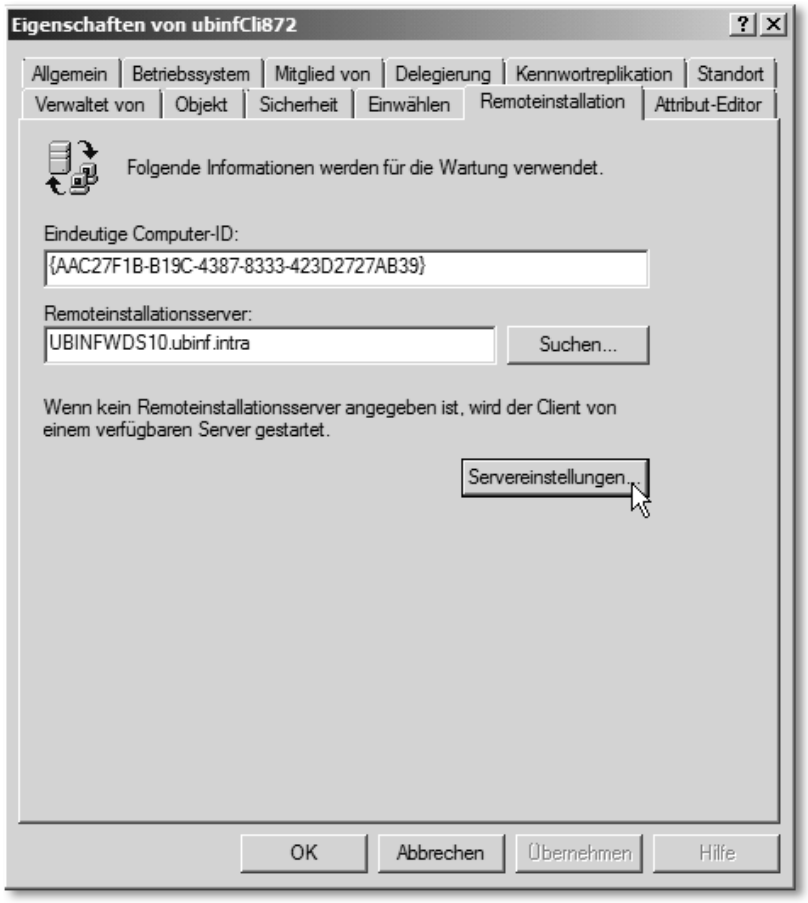


Abbildung 6.83 In den Eigenschaften des Computerkontos existiert eine Registerkarte »Remoteinstallation« (ebenfalls nur ab Windows Server 2008 R2).

6.8 PXE-Antwortrichtlinie und ausstehende Geräte

Bei der Ersteinrichtung von WDS muss unter anderem konfiguriert werden, ob der WDS-Server auch unbekannten Clients antworten soll – diesen Aspekt möchte ich gern vertiefen. Falls Sie »Querleser« sind: Ein »unbekannter Client« aus WDS-Sicht ist einer, der nicht bereits über ein Computerkonto im Active Directory verfügt. Wie Sie im vorherigen Abschnitt erfahren haben, können Sie neue Computer vorab bereitstellen, sodass unter anderem der »richtige« Computername gesetzt wird oder das für den zukünftigen Aufgabenbereich des Geräts am besten geeignete WIM-Image.

In den Eigenschaften des WDS-Servers und dort auf der Registerkarte PXE-Antwort (Abbildung 6.84) lässt sich beispielsweise festlegen, dass der WDS-Server nur bekannten (d. h. im AD vorhandenen) Computern antwortet.

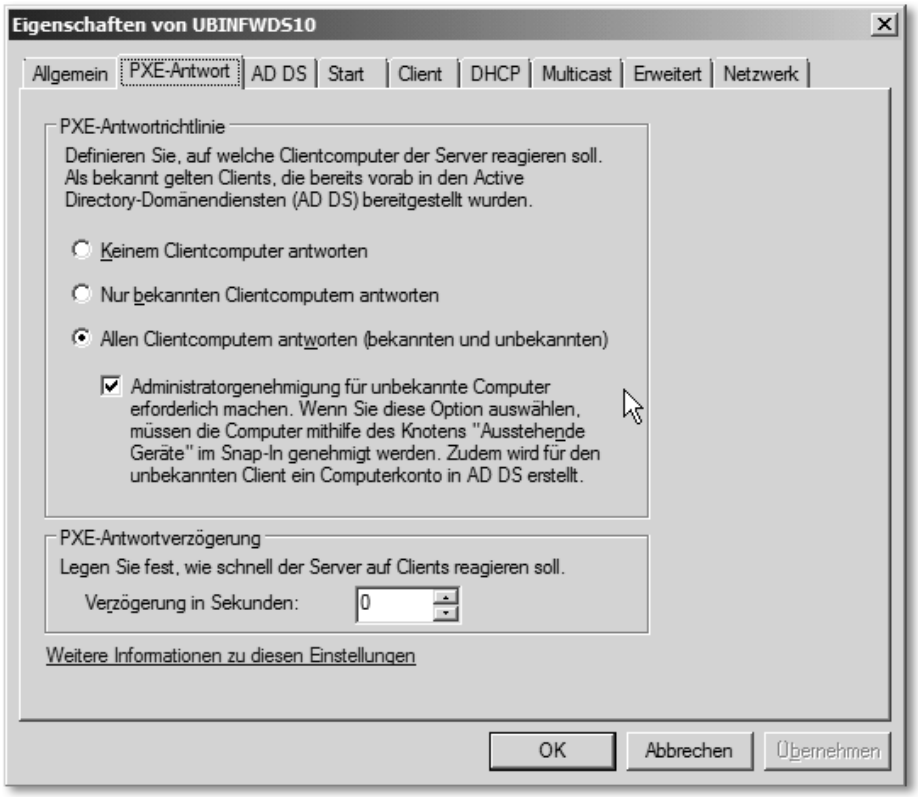


Abbildung 6.84 Die Einstellung, dass unbekannte Clients zunächst genehmigt werden müssen, ist in der Praxis durchaus sinnvoll.

Sie können aber auch anders vorgehen:

- Sie wählen aus, dass der WDS allen Clientcomputern antwortet, verlangen durch das Aktivieren der entsprechenden Checkbox allerdings, dass ein unbekannter Computer genehmigt werden muss (Abbildung 6.84).
- Wenn ein nicht bereitgestellter, also unbekannter Computer einen PXE-Bootvorgang durchführt, beginnt zunächst ein normaler Startvorgang, der dann allerdings »hängen bleibt« (Abbildung 6.85). Der Client wird in dieser Wartestellung bleiben und regelmäßig seinen Status beim WDS-Server abfragen. Das Intervall kann übrigens mit WDSUTIL angepasst werden.
- Im Verwaltungswerkzeug für die Bereitstellungsdienste werden Sie den in Wartestellung befindlichen PC unterhalb des Knotens Ausstehende Geräte sehen können (Abbildung 6.86).
- Im Kontextmenü des jeweiligen ausstehenden PCs können Sie die Installation genehmigen oder ablehnen.
- Im Kontextmenü des Knotens Ausstehende Geräte gibt es Menüpunkte, um alle wartenden Geräte mit einem Klick zu genehmigen oder abzulehnen.

Abbildung 6.85 Ein unbekannter Client in »Wartestellung«

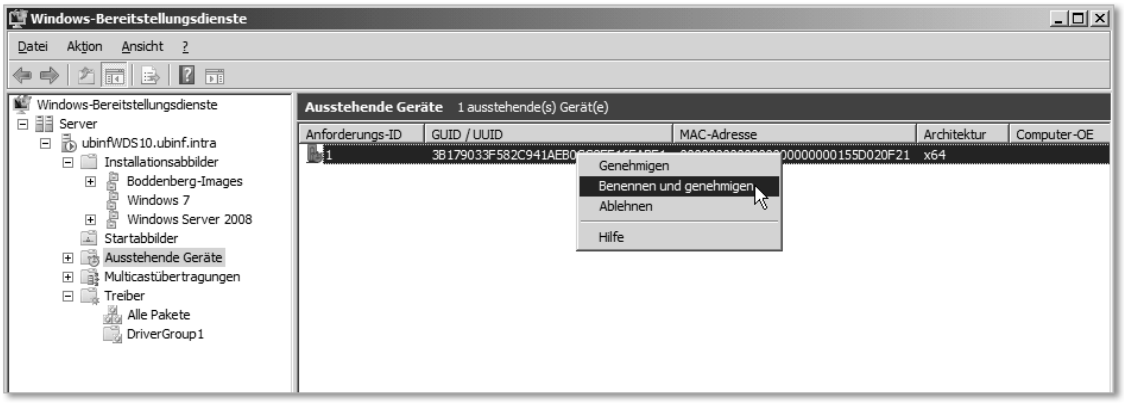


Abbildung 6.86 Im Verwaltungswerkzeug für die Windows-Bereitstellungsdienste kann der Computer genehmigt werden. Außerdem kann der Name vorgegeben werden.

Wie Sie auf Abbildung 6.86 sehen, gibt es zwei Optionen beim Genehmigen:

- GENEHMIGEN: Hierbei wird die Installation des Computers genehmigt, und es wird ein automatisch von WDS ermittelter Name vergeben. Die Syntax für die Namensvergabe wird in den Eigenschaften des WDS-Servers auf der Registerkarte AD DS konfiguriert.
- BENENNEN UND GENEHMIGEN: Bei der Verwendung dieser Option wird zunächst der zu verwendende Computername abgefragt. Den recht unspektakulären Dialog sehen Sie auf Abbildung 6.87.

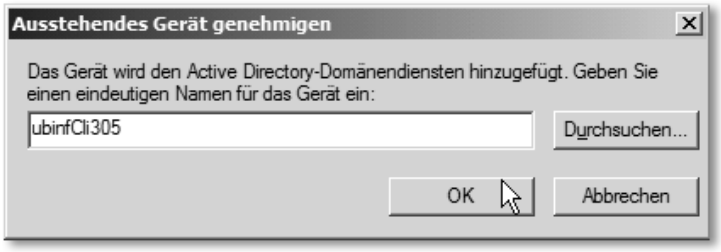


Abbildung 6.87 Beim Genehmigen eines PCs können Sie einen Namen vorgeben.

Die Möglichkeit, den zukünftigen Namen anzugeben, ist zwar schon hilfreich, in der Praxis werden Sie aber vermutlich noch weitergehende Anforderungen haben, wie etwa das Festlegen der zu verwendenden Antwortdatei (und damit des zu installierenden WIM-Images) oder des Benutzernamens, der zum Beitreten zur Domäne berechtigt werden soll.

Diese erweiterten Möglichkeiten können mit WDSUTIL genutzt werden. Hier sehen Sie drei Beispiele für die Genehmigung mit WDSUTIL:

- *Beispiel 1*: Genehmigen des Computers mit der Anforderungs-ID 1 (vergleiche Abbildung 6.86) mit dem Namen *ubinfCli305*:

  ```
  WDSUTIL /Approve-AutoAddDevices /RequestID:1 /Machine-Name:ubinfCli305
  ```

- *Beispiel 2*: Wie Beispiel 1, aber zusätzlich geben Sie eine Antwortdatei an und passen die Berechtigungen für das Hinzufügen zum AD an:

  ```
  WDSUTIL /Approve-AutoAddDevices /RequestID:1 /Machine-Name:ubinfCli305 /User:ubinf\ClientInst /JoinRights:Full /WdsClient-Unattend:WdsClientUnattend\Unattend.xml
  ```

- *Beispiel 3*: Genehmigen aller wartenden Computer mit Standardeinstellungen:

  ```
  WDSUTIL /Approve-AutoAddDevices /RequestID:All
  ```

Das hört sich so weit alles nicht weiter kompliziert an, umso größer wird aber Ihre Enttäuschung sein, wenn beim Ausführen des Genehmigungsvorgangs die Meldung aus Abbildung 6.88 erscheint: ZUGRIFF VERWEIGERT.

Der Grund für diese Meldung ist, dass die Genehmigung mit dem Computerkonto des WDS-Servers durchgeführt wird. Dieses hat standardmäßig nicht die Genehmigung, um im Active Directory neue Objekte anzulegen. Was zur Anpassung zu tun ist, zeige ich Ihnen im nächsten Abschnitt.

Abbildung 6.88 Wenn beim Genehmigen eines PCs diese Meldung erscheint, gibt es Handlungsbedarf bezüglich der AD-Berechtigungen.

Berechtigungen anpassen

Damit das Genehmigen funktioniert (und nicht mit ZUGRIFF VERWEIGERT endet), muss das Computerkonto des WDS-Servers Berechtigungen zum Erstellen von Objekten erhalten:

- Öffnen Sie das Konfigurationswerkzeug *Active Directory-Benutzer und -Computer*.
- Wählen Sie dort im Kontextmenü der Organisationseinheit bzw. des Containers, in dem sich die Computerobjekte befinden bzw. befinden sollen, den Menüpunkt OBJEKTVERWALTUNG ZUWEISEN.

  In den englischsprachigen Versionen heißt dieser Menüpunkt übrigens DELEGATE CONTROL.
- Im ersten Dialog des Assistenten müssen Sie das Konto angeben, dem Sie Rechte zuweisen möchten (Abbildung 6.89, links).

  In diesem Fall ist das ein Computerkonto, was zwar grundsätzlich kein Problem ist, aber erfordert, dass Sie im HINZUFÜGEN-Dialog den auszuwählenden Objekttyp anpassen.
- Der nächste Dialog ermöglicht die Auswahl von Aufgaben, die Sie dem Benutzer oder der Gruppe bzw. in diesem Fall dem Computerkonto zuweisen möchten (Abbildung 6.89, rechts).

  Wählen Sie in diesem Dialog die Option BENUTZERDEFINIERTE TASKS…
- In den nächsten Dialogen legen Sie fest, dass Sie in dem gewählten Ordner neue Computer-Objekte erstellen lassen möchten. Die auszuwählenden Einstellungen entnehmen Sie bitte Abbildung 6.90.

Abbildung 6.89 Wählen Sie das Computerkonto des WDS-Servers aus.

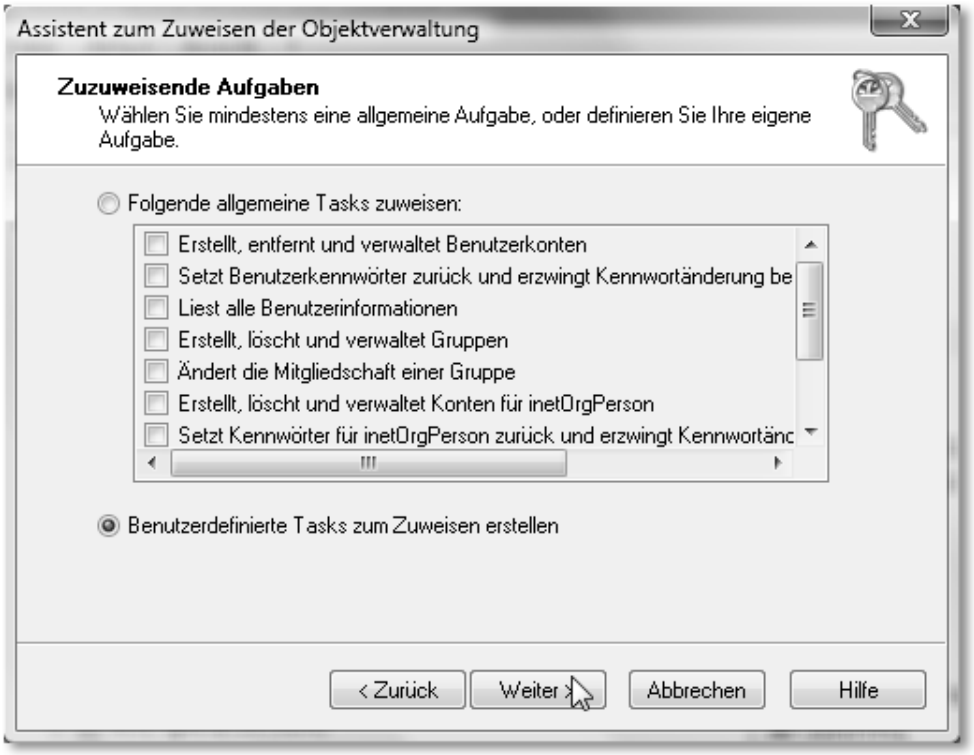


Abbildung 6.90 Entscheiden Sie sich für die »Benutzerdefinierten Tasks«.

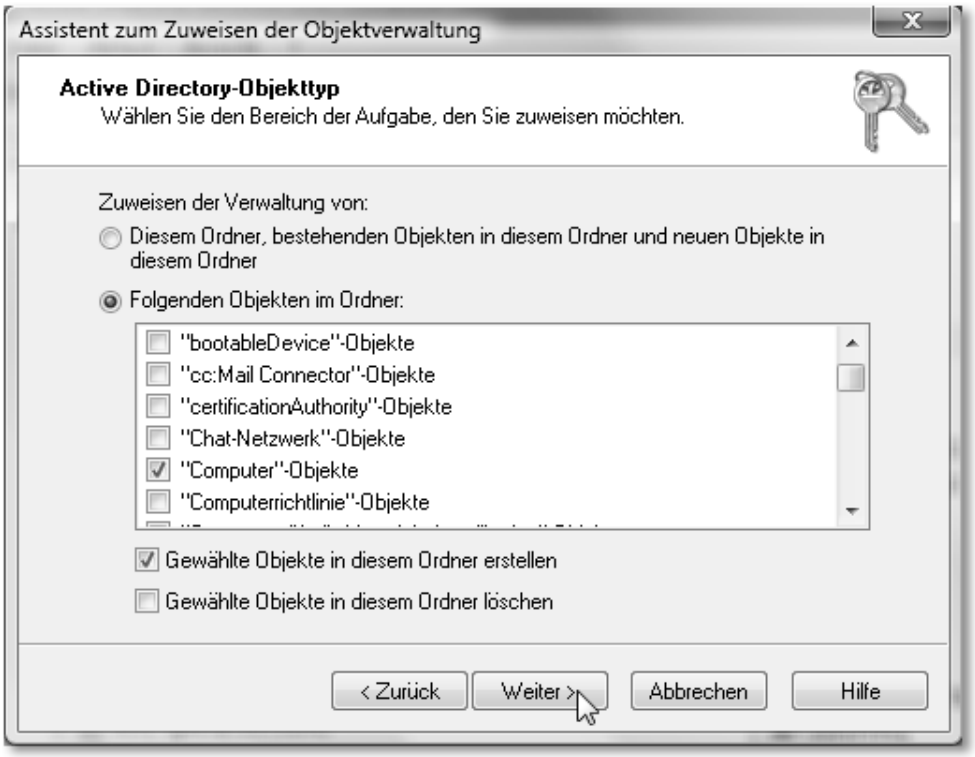


Abbildung 6.91 Legen Sie diese Einstellungen fest.

Abbildung 6.92 Wählen Sie diese Berechtigungen.

Es kann nicht schaden, die vom Assistenten durchgeführten Änderungen kurz zu kontrollieren. Rufen Sie dazu den Eigenschaftendialog der Organisationseinheit auf, und wechseln Sie auf die Registerkarte SICHERHEIT. Dort wird nun das Computerkonto des WDS-Servers zu sehen sein. Zugewiesen sind SPEZIELLE BERECHTIGUNGEN (Abbildung 6.93).

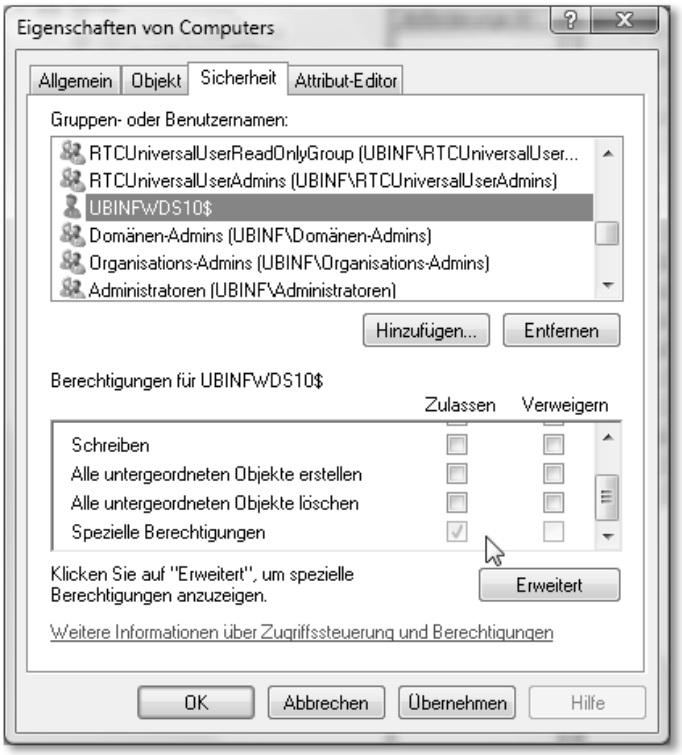


Abbildung 6.93 Das Ergebnis ist, dass »spezielle Berechtigungen« für das Computerkonto des WDS-Servers gesetzt sind.

Erfreulicherweise ist es nun möglich, ausstehende Geräte zu genehmigen. Sobald Sie nun einen Computer genehmigen, passieren zwei Dinge:

- Sie werden freundlich darüber informiert, dass das Gerät genehmigt wurde (Abbildung 6.94).
- Der bislang angehaltene Vorgang (Abbildung 6.85) wird nach einer kurzen Wartezeit (Abfrageintervall) fortgesetzt, und die Installation beginnt.

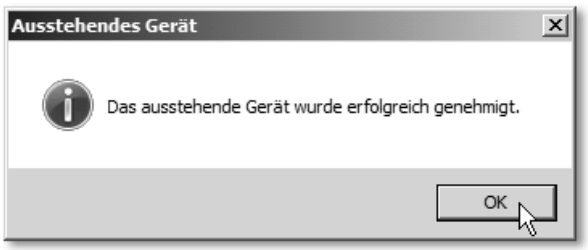


Abbildung 6.94 Prima, jetzt klappt's!

6.9 Ein eigenes WIM-Image installieren

Den Beispielen im Abschnitt 6.6, »WDS-Startvorgang automatisieren« lag stets ein Standard-Image zugrunde, das direkt von der Produkt-DVD kam. Einer der großen Vorteile der Installation mit WIM-Images ist die Möglichkeit, stattdessen eigene Images zu verwenden, die beispielsweise allgemeine (wie Acrobat Reader) oder spezielle Software (wie einen CRM-Client, ein Konstruktionsprogramm) oder auch zusätzliche Treiber enthalten. In Abschnitt 6.3 habe ich eine eigene Referenzinstallation erstellt und aus dieser ein WIM-Image erzeugt. Wenn Sie eigene Images erzeugt haben und auf PCs mit WDS installieren möchten, müssen Sie letztendlich »nur« dieselbe Vorgehensweise wie bei einer Installation der Standard-Images einhalten:

- Sie installieren und importieren ein WIM-Image auf den WDS-Server.
- Sie erstellen eine Antwortdatei für den Windows-Bereitstellungsdiensteclient und integrieren sie auf den WDS-Server (siehe Abschnitt 6.6.1).
- Sie erstellen eine Antwortdatei für das Windows-Setup und ordnen sie dem Image auf dem WDS-Server zu (siehe Abschnitt 6.6.2).
- Sofern die Antwortdatei für den Windows-Bereitstellungsclient nicht die in den Eigenschaften des WDS-Servers hinterlegte Standarddatei für die Betriebssystemarchitektur ist (Abbildung 6.64), stellen Sie einen PC mit WDSUTIL bereit und spezifizieren die Antwortdatei mit dem Parameter `/WdsClientUnattend`. Zur Erinnerung: Die Antwortdatei enthält unter anderem die Information, welches WIM-Image installiert werden soll.

Wenn alle Vorbereitungen getroffen sind, brauchen Sie nur noch den neuen PC zu starten, und ein Weilchen später ist Ihr eigenes Image installiert, der PC in die Domäne aufgenommen – und der Benutzer kann damit losarbeiten.

PC »verallgemeinern«

An dieser Stelle sei nochmals daran erinnert, dass Sie den Referenz-PC vor der Erfassung des Images »verallgemeinern« müssen (siehe Abschnitt 6.3.3). Dies ist unbedingt notwendig, da ein aus diesem Image erzeugter PC unter anderem keine individuelle SID hätte und das Mini-Setup nicht beim ersten Start aufgerufen würde.

6.10 Image-Pflege

Wenn Sie die »heile Labor-Welt« verlassen haben und mit echter Hardware umgehen, werden Sie es nicht vermeiden können, hin und wieder Anpassungen vorzunehmen, insbesondere natürlich Treiber hinzuzufügen und zu aktualisieren.

Für das Hinzufügen von Treibern gibt es nun zwar verschiedene Strategien. Eine auf den ersten Blick recht simple Möglichkeit wäre, die Treiber direkt in das Image zu integrieren. Das hört sich absolut sinnvoll an, auf den zweiten Blick stellt sich aber die Frage, wie man die Treiber ohne größeren Aufwand in das Image hinein- und gegebenenfalls wieder herausbekommt (bestimmte Treiberpakete könnten auch irgendwann veraltet sein). Anzumerken wäre, dass es ein relativ großer Aufwand ist, ständig den Referenz-PC komplett neu in ein Image konvertieren zu müssen. Das Starten des Referenz-PCs ist übrigens auch mit hohem Aufwand verbunden, da dieser mit SYSPREP »verallgemeinert« wird und beim ersten Start das Mini-Setup (u. a. Festlegen des Namens etc.) durchläuft.

Es wäre also sehr hilfreich, wenn man Treiber direkt im WIM-Image pflegen könnte – und genau das ist mit einem Werkzeug namens *DISM.exe* möglich. Auf Englisch bedeutet die Abkürzung DISM *Deployment Image Servicing and Management Tool*. In der deutschen Version meldet es sich mit *Tool zur Abbildverwaltung für die Bereitstellung*.

DISM kann noch mehr, als »nur« Treiber zu integrieren: Mit DISM können Sie auch Packages (Installationsdateien) und Features verwalten. Ich werde Ihnen in den folgenden Abschnitten einige Möglichkeiten zur Pflege eines WIM-Images vorführen. Sie werden sehen, dass es fast erschreckend einfach ist, beispielsweise für eine neue PC-Baureihe benötigte Treiber hinzuzufügen.

Beispiel WIN-Image

Ich führe Ihnen in den folgenden Abschnitten die Möglichkeiten von DISM anhand eines WIM-Images vor. Dieselben Möglichkeiten stehen auch für VHD-Images (Virtual Hard Disk) zur Verfügung.

DISM ist Bestandteil des WAIK.

Die Bearbeitung des Images muss nicht auf dem WDS-Server vorgenommen werden, sondern kann auf jedem beliebigen PC erfolgen; Sie müssen dann lediglich die WIM-Datei kopieren.

DISM ist übrigens eine Kommandozeilenanwendung. Um sie zu starten, sollten Sie die in der WAIK-Startmenügruppe vorhandene Eingabeaufforderung mit Administrator-Privilegien öffnen. Die Eingabe von `dism` fördert dann die auf Abbildung 6.95 gezeigte Ansicht zutage. Ich persönlich erschrecke mich immer, wenn sich allein die Befehlsauflistung einer Kommandozeilenanwendung über mehr als eine Bildschirmseite erstreckt – Sie werden aber sehen, dass die Arbeit mit DISM vergleichsweise einfach ist.

```
C:\Program Files\Windows AIK\Tools\PETools>dism

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0


DISM.exe [DISM-Optionen] {WIM-Befehl} [<WIM-Argumente>]
DISM.exe {/Image:<Pfad zum Offlineabbild> | /Online} [DISM-Optionen]
         {Wartungsbefehl} [<Wartungsargumente>]

BESCHREIBUNG:

  DISM dient zum Aufzählen, Installieren, Deinstallieren, Konfigurieren
  und Aktualisieren von Funktionen und Paketen in Windows-Abbildern.
  Welche Befehle verfügbar sind, hängt davon ab, welches Abbild gewartet
  wird und ob es sich bei dem Abbild um ein Offlineabbild oder um ein
  Onlineabbild handelt.

WIM-BEFEHLE:

  /Get-MountedWimInfo     - Zeigt Informationen zu bereitgestellten WIM-Abbilder
n an.
  /Get-WimInfo            - Zeigt Informationen zu Abbildern in einer WIM-Datei
an.
  /Commit-Wim             - Speichert Änderungen auf einem bereitgestellten WIM-
Abbild.
  /Unmount-Wim            - Hebt die Bereitstellung eines bereitgestellten WIM-A
bbilds auf.
  /Mount-Wim              - Stellt ein Abbild aus einer WIM-Datei bereit.
  /Remount-Wim            - Stellt ein verwaistes WIM-Bereitstellungsverzeichnis
 wieder her.
  /Cleanup-Wim            - Löscht Ressourcen, die mit beschädigten bereitgestel
lten
                            WIM-Abbildern verknüpft sind.

ABBILDSPEZIFIKATIONEN:

  /Online                 - Verwendet das ausgeführte Betriebssystem als Ziel.
  /Image                  - Gibt den Pfad zum Stammverzeichnis eines
                            Windows-Offlineabbilds an.

DISM-OPTIONEN:

  /English                - Zeigt die Befehlszeile in englischer Sprache an.
  /Format                 - Gibt das Berichtsausgabeformat an.
  /WinDir                 - Gibt den Pfad zum Windows-Verzeichnis an.
  /SysDriveDir            - Gibt den Pfad zur Systemladedatei namens
                            "BootMgr" an.
  /LogPath                - Gibt den Pfad zur Protokolldatei an.
  /LogLevel               - Gibt die Ausgabeebene für das Protokoll an (1 - 4).
  /NoRestart              - Unterdrückt automatische Neustarts und Aufforderunge
n zum Neustart.
  /Quiet                  - Unterdrückt alle Ausgaben mit Ausnahme von Fehlermel
dungen.
  /ScratchDir             - Gibt den Pfad zu einem Entwurfsverzeichnis an.

Weitere Informationen zu diesen DISM-Optionen und den zugehörigen
Argumenten erhalten Sie, indem Sie direkt vor "/?" eine Option angeben.

  Beispiele:
    DISM.exe /Mount-Wim /?
    DISM.exe /ScratchDir /?
    DISM.exe /Image:C:\test\offline /?
    DISM.exe /Online /?


C:\Program Files\Windows AIK\Tools\PETools>_
```

Abbildung 6.95 Ein erster Blick auf DISM – es sieht komplizierter aus, als es letztendlich ist.

6.10.1 WIM-Image mounten

Der erste Schritt bei der Arbeit mit DISM ist das Mounten eines WIM-Images. Es wird dabei in ein Verzeichnis des lokalen Dateisystems gemountet. Die Vorgehensweise ist simpel:

- Legen Sie ein leeres Verzeichnis an, beispielsweise *c:\mount*.
- Für Sie den Befehl `dism /mount-wim` aus. Als Parameter geben Sie die WIM-Datei, das Mount-Verzeichnis und einen Indexwert an. Optional können Sie

den Parameter `/readonly` angeben, um das WIM-Image schreibgeschützt zu mounten (Abbildung 6.96).

- Nach kurzer Zeit wird das WIM-Image in dem Ordner bereitgestellt sein, und Sie werden es als »normale« Dateistruktur in dem angegebenen Ordner sehen (Abbildung 6.97).

```
C:\Program Files\Windows AIK\Tools\PETools>dism /mount-wim /WimFile:c:\Images\bo
ddimagex64.wim /index:1  /MountDir:c:\mount

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbild wird bereitgestellt
[==========================100.0%==========================]
Der Vorgang wurde erfolgreich beendet.

C:\Program Files\Windows AIK\Tools\PETools>_
```

Abbildung 6.96 Mounten eines WIM-Images

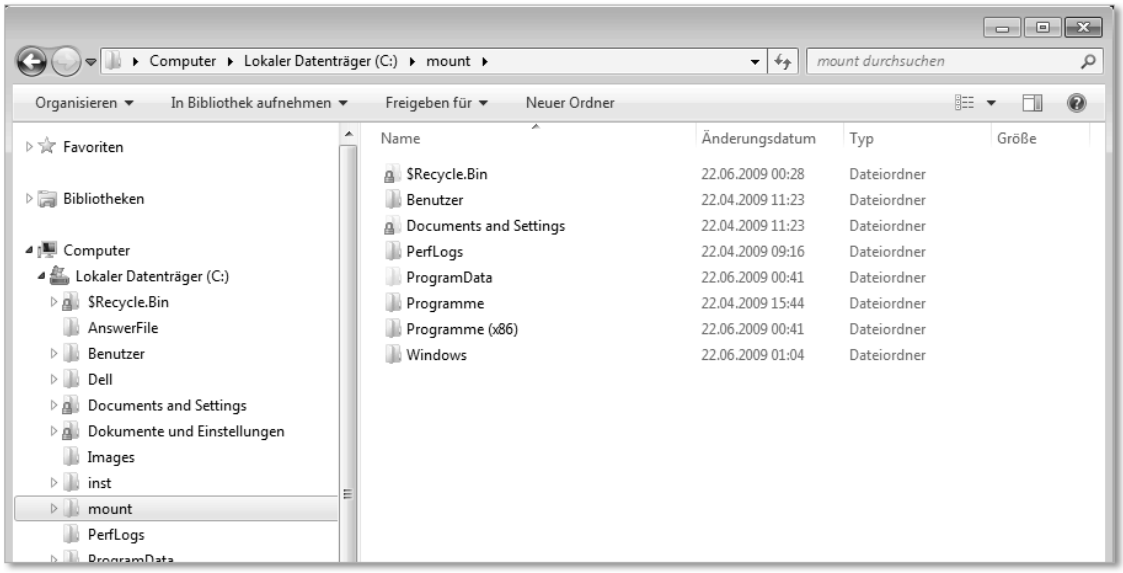


Abbildung 6.97 Das gemountete Image erscheint in dem angegebenen Ordner in »normaler« Dateistruktur.

Sie können jetzt in das gemountete Image Dateien hineinkopieren und diese verändern. Weitaus spannender ist aber das Bearbeiten von Treibern, Packages und Features, wofür DISM eigene Funktionen mitbringt.

Änderungen annehmen oder verwerfen

Nach dem Bearbeiten wird die Bereitstellung des Images mit der Option `/Unmount-Wim` wieder beendet. Dabei können Sie entscheiden, ob die vorgenommenen Änderung übernommen oder verworfen werden sollen.

Ist ein Image gemountet, können Sie mit dem Befehl `dism /image:[Pfad] /?` die Liste der nun zur Verfügung stehenden Befehle erfragen. Abbildung 6.98 ist zeigt den Anfang (!) der Ausgabe.

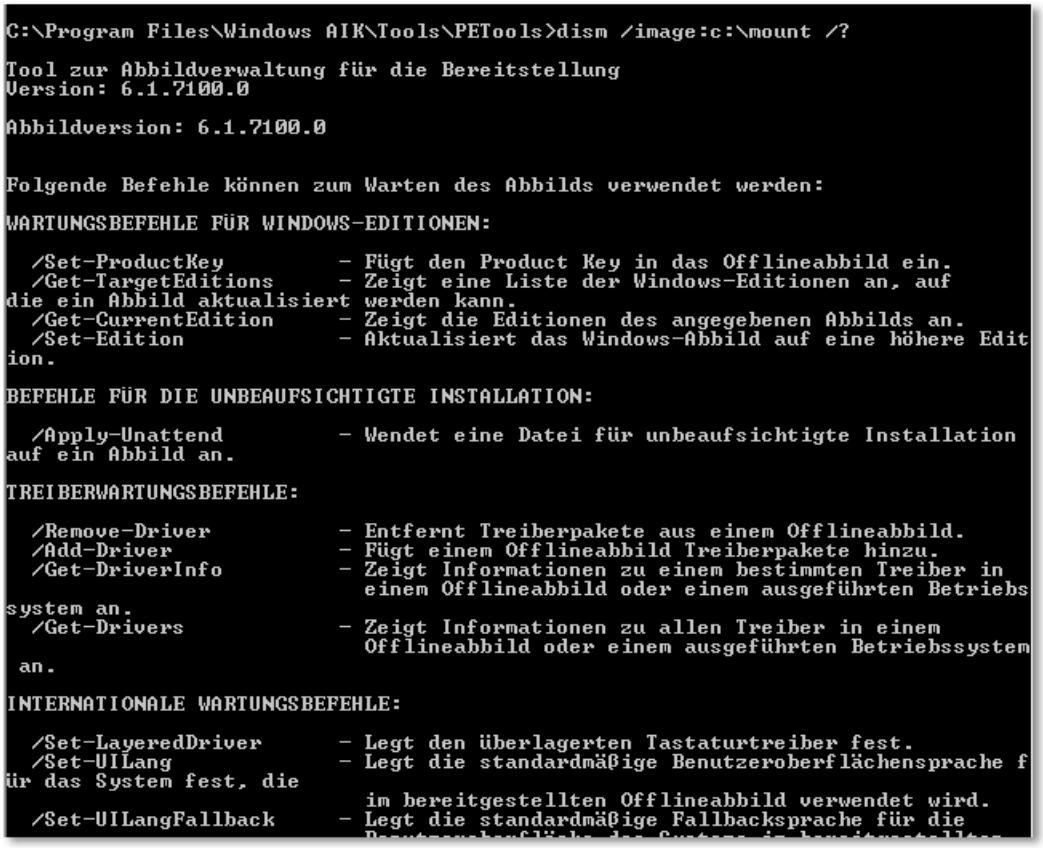


Abbildung 6.98 Für ein gemountetes Image stehen viele Optionen zur Verfügung.

Es gibt für die Modifikation eines Images folgende Bereiche:

- Wartungsbefehle für Windows-Editionen: Hier können Sie beispielsweise einen *ProductKey* einsetzen und in gewissen Grenzen die Windows-Edition (*Business, Enterprise, Ultimate* etc.) anpassen.
- Befehle für die unbeaufsichtigte Installation: In dieser Gruppe findet sich ein Befehl, um eine Datei für die unbeaufsichtigte Installation auf das Abbild anzuwenden.
- Treiberwartungsbefehle: Hier finden sich Befehle, um Treiber hinzuzufügen und zu entfernen.
- Internationale Wartungsbefehle: Dieser Bereich umfasst Befehle, mit denen Spracheinstellungen vorgenommen werden können, beispielsweise die Eingabesprache, die Sprache der Benutzeroberfläche und dergleichen mehr.
- Wartungsbefehle für Anwendungen: In dieser Kategorie gibt es Befehle, um die installierten Anwendungen anzuzeigen.

- PAKETWARTUNGSBEFEHLE: Diese letzte Gruppe enthält diverse Befehle, mit denen Packages hinzugefügt und entfernt werden können. Außerdem lassen sich Features aktivieren und deaktivieren.

6.10.2 Treiber verwalten

Eines der wichtigsten Themen bei der Arbeit mit Images ist der Umgang mit Treibern. Vermutlich werden während der Lebensdauer eines mit viel Mühe erstellten Images neue PC-Baureihen in Ihr Unternehmen kommen. Selbst wenn Sie immer dieselben PC-Typen einsetzen, kommen Sie an der Pflege von Treibern nicht vorbei, weil die Hersteller ihre Treiber im Allgemeinen mehr oder weniger regelmäßig aktualisieren. Es wäre wenig optimal, zwei Jahre alte Treiber zu installieren, nur weil diese im Image vorhanden sind. Mit DISM ist die Pflege von Treibern in einem Image in der Tat simpel.

Vorhandene Treiber anzeigen

Sie rufen ie Liste der in dem Image vorhandenen Treiber mit dem Befehl `dism /image:[Pfad] /get-drivers` ab. Dieser Aufruf führt zu dem auf Abbildung 6.99 gezeigten Resultat.

```
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mount /get-drivers

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbildversion: 6.1.7100.0

Liste der Treiber von Drittanbietern wird aus dem Treiberspeicher abgerufen...

Treiberpaketauflistung:

Veröffentlichter Name : oem0.inf
Originaldateiname : prnms001.inf
Posteingang : Nein
Klassenname : Printer
Anbietername : Microsoft
Datum : 21.06.2006
Version : 6.1.7100.0

Der Vorgang wurde erfolgreich beendet.

C:\Program Files\Windows AIK\Tools\PETools>_
```

Abbildung 6.99 Die Liste der im Treiberspeicher vorhandenen Treiber von Drittanbietern

Der Befehl `/get-drivers` kann noch um den optionalen Parameter `/all` ergänzt werden. Ohne `/all` werden die Treiber von Drittanbietern angezeigt. Wird der Parameter `/all` angegeben, werden seitenweise Standardtreiber angezeigt, was im Allgemeinen aber herzlich uninteressant sein dürfte.

Treiber hinzufügen

Das Hinzufügen von Treibern geschieht mit dem Befehl `/add-driver`. Es gibt hier zwei Aufrufmöglichkeiten:

- Entweder fügen Sie gezielt einen Treiber hinzu, indem Sie dessen **.inf*-Datei angeben.
- Mit dem Parameter `/recurse` können Sie alle Treiber hinzufügen, die im angegebenen Unterverzeichnis vorhanden sind. Sie können also Treibersammlungen für bestimmte Geräte in einem Unterverzeichnis pflegen und diese in einem Rutsch hinzufügen.

Auf Abbildung 6.100 habe ich einen Treiber (einen Druckertreiber von Dell) hinzugefügt und anschließend die Liste der Treiber von Drittanbietern im Treiberspeicher aufgerufen.

```
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mount /add-driver /dri
ver:c:\Dell\Drivers\R202860\Win_x64\PCL\German\dlxzizi.inf

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbildversion: 6.1.7100.0

Anzahl der zu installierenden Treiberpakete: 1.
1 von 1 - c:\Dell\Drivers\R202860\Win_x64\PCL\German\dlxzizi.inf wird installier
t: Das Treiberpaket wurde erfolgreich installiert.
Der Vorgang wurde erfolgreich beendet.

C:\Program Files\Windows AIK\Tools\PETools>
C:\Program Files\Windows AIK\Tools\PETools>
C:\Program Files\Windows AIK\Tools\PETools>
C:\Program Files\Windows AIK\Tools\PETools>
C:\Program Files\Windows AIK\Tools\PETools>
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mount /get-drivers

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbildversion: 6.1.7100.0

Liste der Treiber von Drittanbietern wird aus dem Treiberspeicher abgerufen...

Treiberpaketauflistung:

Veröffentlichter Name : oem0.inf
Originaldateiname : prnms001.inf
Posteingang : Nein
Klassenname : Printer
Anbietername : Microsoft
Datum : 21.06.2006
Version : 6.1.7100.0

Veröffentlichter Name : oem1.inf
Originaldateiname : dlxzizi.inf
Posteingang : Nein
Klassenname : Printer
Anbietername : Dell Inc.
Datum : 30.07.2008
Version : 1.0.18.0

Der Vorgang wurde erfolgreich beendet.

C:\Program Files\Windows AIK\Tools\PETools>
```

Abbildung 6.100 Hinzufügen eines Treibers und neuerliche Abfrage der installierten Treiber von Drittanbietern

Sie sehen, dass automatisch ein Veröffentlichter Name erzeugt wird (hier *oem1.inf*), den Sie auch verwenden, um diesen Treiber anzusprechen, beispielsweise beim Löschen desselben.

Die Dateien des Treibers werden übrigens in das Verzeichnis *\Windows\System32\DriverStore\FileRepository* kopiert, wie Sie mit dem Datei-Explorer leicht nachprüfen können (Abbildung 6.101).

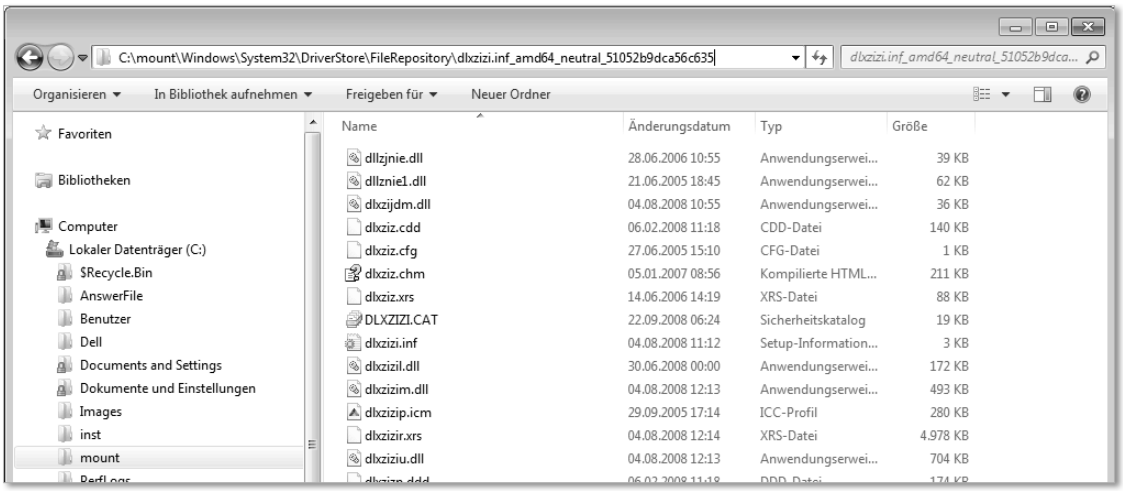


Abbildung 6.101 Die Dateien des neu installierten Treibers landen im Ordner »...\DriverStore\FileRepository\...«.

Sie können mit dem Befehl `/get-driverinfo` Details zu einem bestimmten Treiber aufrufen. Geben Sie als Parameter den veröffentlichten Namen, also beispielsweise `oem1.inf` an. Diese Namen erhalten Sie aus der Treiberliste (Abbildung 6.100). Die Details für den soeben installierten Dell-Druckertreiber sehen Sie auf Abbildung 6.102 (stark verkürzte Darstellung).

```
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mount /get-driverinfo
/driver:oem1.inf

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbildversion: 6.1.7100.0

Treiberpaketinformationen:

Veröffentlichter Name : oem1.inf
Treiberspeicherpfad : c:\mount\Windows\System32\DriverStore\FileRepository\dlxzi
zi.inf_amd64_neutral_51052b9dca56c635\dlxzizi.inf
Klassenname : Printer
Klassenbeschreibung : Drucker
Klassen-GUID : {4D36E979-E325-11CE-BFC1-08002BE10318}
Datum : 30.07.2008
Version : 1.0.18.0
Für den Start erforderlich : Nein

Treiber für Architektur : x86

    Hersteller : Dell Inc.
    Beschreibung : Dell Color Laser 5110cn PCL6
    Architektur : x86
    Hardware-ID : LPTENUM\DellColor_Laser_51107328
    Dienstname :
    Kompatible IDs :
    IDs ausschließen :

    Hersteller : Dell Inc.
```

Abbildung 6.102 Detailinformationen zu einem Treiber lassen sich mit »/get-driverinfo« anzeigen (stark verkürzte Darstellung).

Unsignierte Treiber

Grundsätzlich sollten Treiber durch Microsoft geprüft und signiert sein. Um signiert zu werden, müssen Treiber einige qualitätssichernde Kriterien erfüllen. Die Treibersignatur ist für den jeweiligen Hersteller letztendlich mit Kosten verbunden, was wohl ein Grund ist, weshalb es aus der Community durchaus Kritik gegeben hat.

Wenn man allerdings bedenkt, dass schlechte Treiber zu teilweise heftigen Stabilitätsproblemen führen, ist diese Qualitätssicherung sicherlich ein Schritt in die richtige Richtung.

Um unsignierte Treiber für die x64-Version des Betriebssystems hinzuzufügen, muss der Parameter `/ForceUnsigned` angegeben werden.

Treiber löschen

Treiber können natürlich auch wieder gelöscht werden. Dies ist beispielsweise dann empfehlenswert, wenn Sie eine neue Treiberversion installieren möchten oder wenn eine bestimmte PC-Baureihe in Ihrem Unternehmen außer Dienst gestellt wird. Die Syntax lautet:

```
Dism /Image:[Pfad] /remove-driver /Driver:[veröffentlichter Name]
```

Den veröffentlichten Namen erhalten Sie aus der Treiberliste (`/get-drivers`). Ein veröffentlichter Name ist beispielsweise *oem1.inf*.

6.10.3 Packages verwalten

Neben der Verwaltung von Treibern bieten Packages einen interessanten Anwendungsfall. In die Kategorie *Packages* gehören beispielsweise:

- Erweiterungen und Updates, die im MSU-Format zur Verfügung gestellt werden
- Sprachpakete

… kurz gesagt lässt sich alles, was als *.MSU oder *.CAB verteilt wird, als Package einbinden. Wenn Sie mit DISM abfragen, welche Packages derzeit installiert sind, erhalten Sie bei einer »frischen« Installation das Ergebnis, das Sie auf Abbildung 6.103 sehen. Der Befehl zur Abfrage führt zu keinen großen Überraschungen: `/get-packages`.

Die übrigen Befehle im Zusammenhang mit Packages sind denjenigen der Treiberverwaltung sehr ähnlich:

- `/Get-Packages` zeigt alle installierten Packages an.
- `/Get-PackageInfo` zeigt Detailinfos zu einem bestimmten Package an.
- `/Add-Package` fügt ein neues Package hinzu.
- `/Remove-Package` löscht das angegebene Package.

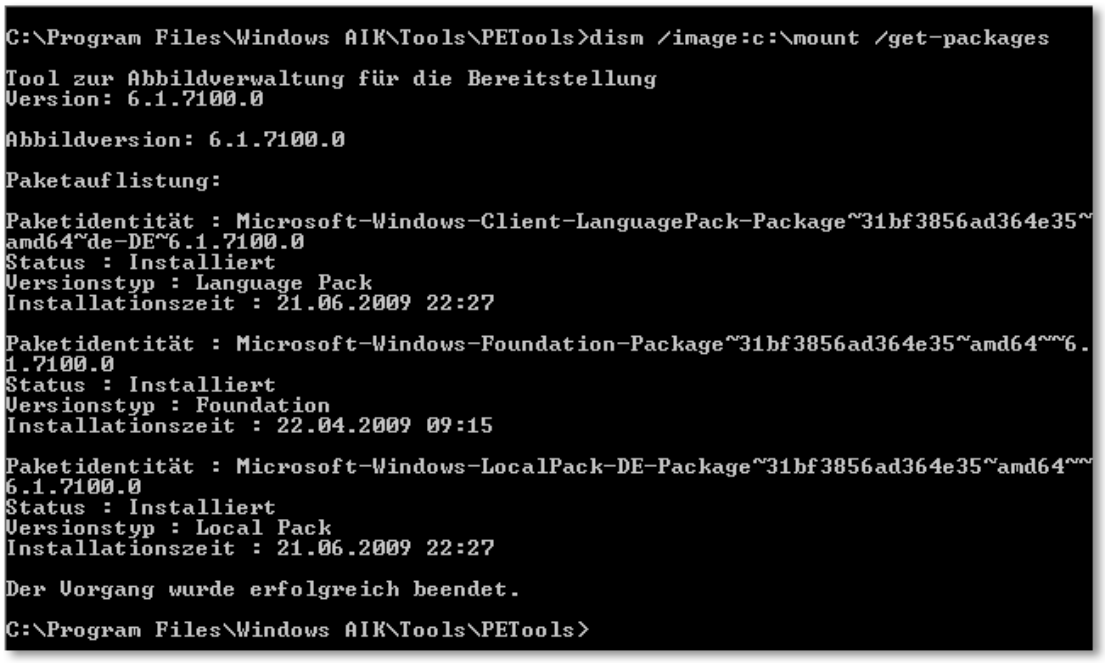


Abbildung 6.103 Die derzeit installierten Packages

Für dieses Installationsbeispiel habe ich dem Image eine MSU-Datei hinzugefügt. Diese enthält die *Remote Server Administration Tools for Windows 7*. Das wäre also ein Anwendungsfall für ein Image, das für Administrator- und Helpdesk-Arbeitsplätze verwendet wird.

Abbildung 6.104 zeigt die Vorgehensweise – sie ist wenig überraschend. Ein interessantes Detail findet sich allerdings in der Auflistung der aktuell installierten Pakete: Das neue Paket wird als noch nicht installiertes Update (INSTALLATION STEHT AUS) angezeigt.

Wie Sie es von Updates kennen, erfolgt die endgültige Installation erst bei einem Neustart des Systems. Das ist zwar grundsätzlich kein Problem, zu bedenken ist aber, dass bei einer größeren Menge von Updates bzw. Erweiterungen, die auf diese Weise hinzugefügt werden, die Installationszeit zunimmt. Das ist ein Aspekt, den Sie zumindest im Auge behalten sollten.

```
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mount /add-package /pa
ckagepath:c:\inst\Windows6.1-KB958830-x64.msu

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbildversion: 6.1.7100.0

1 von 1 werden verarbeitet - Paket "c:\inst\Windows6.1-KB958830-x64.msu" wird hi
nzugefügt
[==========================100.0%==========================]
Der Vorgang wurde erfolgreich beendet.

C:\Program Files\Windows AIK\Tools\PETools>
C:\Program Files\Windows AIK\Tools\PETools>
C:\Program Files\Windows AIK\Tools\PETools>
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mount /get-packages

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbildversion: 6.1.7100.0

Paketauflistung:

Paketidentität : Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~
amd64~de-DE~6.1.7100.0
Status : Installiert
Versionstyp : Language Pack
Installationszeit : 21.06.2009 22:27

Paketidentität : Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~6.
1.7100.0
Status : Installiert
Versionstyp : Foundation
Installationszeit : 22.04.2009 09:15

Paketidentität : Microsoft-Windows-LocalPack-DE-Package~31bf3856ad364e35~amd64~~
6.1.7100.0
Status : Installiert
Versionstyp : Local Pack
Installationszeit : 21.06.2009 22:27

Paketidentität : Microsoft-Windows-RemoteServerAdministrationTools-Package-TopLe
vel~31bf3856ad364e35~amd64~~6.1.7100.0
Status : Installation steht aus
Versionstyp : Update
Installationszeit : 12.07.2009 17:43

Der Vorgang wurde erfolgreich beendet.

C:\Program Files\Windows AIK\Tools\PETools>
```

Abbildung 6.104 Hinzufügen eines Packages. Beachten Sie den »Status« in der Auflistung.

6.10.4 Features aktivieren und deaktivieren

Features sind in diesem Zusammenhang die Komponenten, die über die Systemsteuerung aktiviert oder deaktiviert werden können – ein Bild sagt mehr als tausend Worte: Abbildung 6.105.

Vielleicht werden Sie jetzt fragen, warum man das im Image erledigen soll, wo es doch auch zig andere Möglichkeiten gibt. Antwort: Natürlich gibt es auch andere Möglichkeiten, mit DISM ist es aber sehr einfach.

Die momentan aktiven oder deaktivierten Features können Sie sich mit dem Befehl `/get-features` anzeigen lassen; auf Abbildung 6.106 sehen Sie das Ergebnis. Sie aktivieren und deaktivieren Features mit `/EnableFeatures` und `/Disable-Feature`. Um Details zu einem Feature anzuzeigen, steht der Befehl `/Get-FeatureInfo` zur Verfügung.

Abbildung 6.105 Diese Features können über DISM aktiviert und deaktiviert werden.

```
C:\Program Files\Windows AIK\Tools\PETools>dism /image:c:\mount /get-features!mo
re

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbildversion: 6.1.7100.0

Featureauflistung für das Paket : Microsoft-Windows-Foundation-Package~31bf3856a
d364e35~amd64~~6.1.7100.0

Featurename : OEMHelpCustomization
Status : Deaktiviert

Featurename : CorporationHelpCustomization
Status : Deaktiviert

Featurename : SimpleTCP
Status : Deaktiviert

Featurename : SNMP
Status : Deaktiviert

Featurename : WMISnmpProvider
Status : Deaktiviert

Featurename : TelnetServer
Status : Deaktiviert

Featurename : TelnetClient
Status : Deaktiviert

Featurename : WindowsGadgetPlatform
Status : Aktiviert

Featurename : InboxGames
Status : Aktiviert

Featurename : More Games
Status : Aktiviert

Featurename : Solitaire
Status : Aktiviert

Featurename : SpiderSolitaire
Status : Aktiviert

Featurename : Hearts
```

Abbildung 6.106 Die aktivierten und deaktivierten Features können Sie mit diesem DISM-Aufruf anschauen.

6.10.5 Image unmounten und Änderungen speichern

Nach Abschluss der Arbeiten müssen Sie das Image unmounten. Dabei müssen Sie eine dieser beiden Optionen wählen:

- `/Commit` pflegt die Änderungen in das Image ein.
- `/Discard` verwirft die Änderungen.

Die Syntax zum Unmount nebst »Soll-Ergebnis« sehen Sie auf Abbildung 6.107.

```
C:\Program Files\Windows AIK\Tools\PETools>dism /unmount-wim /mountdir:c:\mount
/commit

Tool zur Abbildverwaltung für die Bereitstellung
Version: 6.1.7100.0

Abbilddatei: c:\Images\boddimagex64.wim
Abbildindex: 1
Abbild wird gespeichert
[==========================100.0%==========================]
Bereitstellung des Abbilds wird aufgehoben
[==========================100.0%==========================]
Der Vorgang wurde erfolgreich beendet.

C:\Program Files\Windows AIK\Tools\PETools>
```

Abbildung 6.107 Nach Abschluss der Änderungen muss das Image unmounted werden.

Noch ein Hinweis

Achten Sie darauf, dass beim Unmounten keine Dateien in dem Image geöffnet sind und auch nicht vom Explorer o. Ä. angezeigt werden. In einem solchen Fall bricht der Vorgang mit einem Fehler ab.

6.10.6 Das Ergebnis der Bemühungen

Interessant ist nun auszuprobieren, was die Änderungen in dem Image beim Installationsvorgang bewirken. Blättern Sie zu Abbildung 6.104 zurück: Dort hatte ich ein Package installiert, und bei der anschließenden Auflistung wurde dessen Status mit INSTALLATION STEHT AUS angegeben. Wenn Sie mit diesem Wissen noch einmal das während der Installation gezeigte Statusfenster anschauen, wird einiges klarer (Abbildung 6.108): Es gibt die Punkte FUNKTIONEN WERDEN INSTALLIERT und TREIBER WERDEN INSTALLIERT. Offensichtlich werden also diese im Image befindlichen Komponenten erst zur Installationszeit »richtig« in das Betriebssystem integriert.

Sie können den Erfolg aller drei Modifikationsmaßnahmen (Treiber hinzugefügt, Package hinzugefügt, einige Features, nämlich Spiele, deaktiviert) überprüfen:

- Ich habe einen Druckertreiber installiert. Folglich müsste dieser als installierbarer Drucker ausgewiesen werden – voilà, er ist da, wie auf Abbildung 6.109 zu sehen ist.

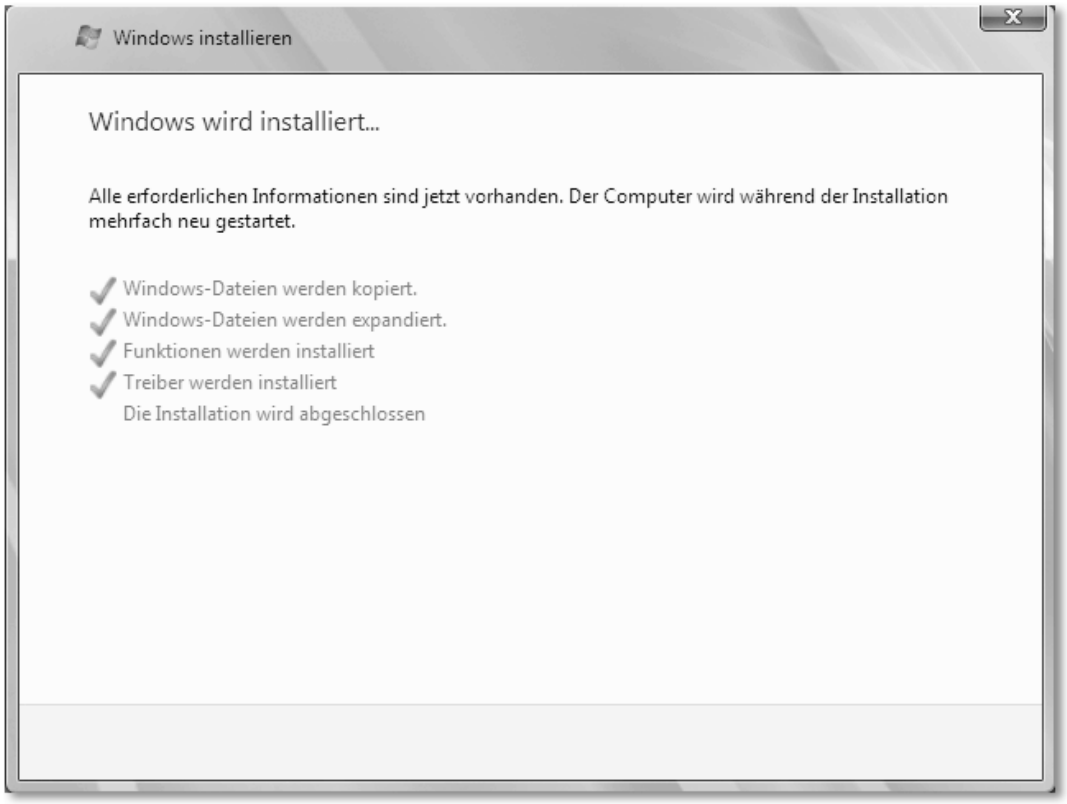


Abbildung 6.108 Während des Installationsprozesses werden Treiber und Funktionen installiert.

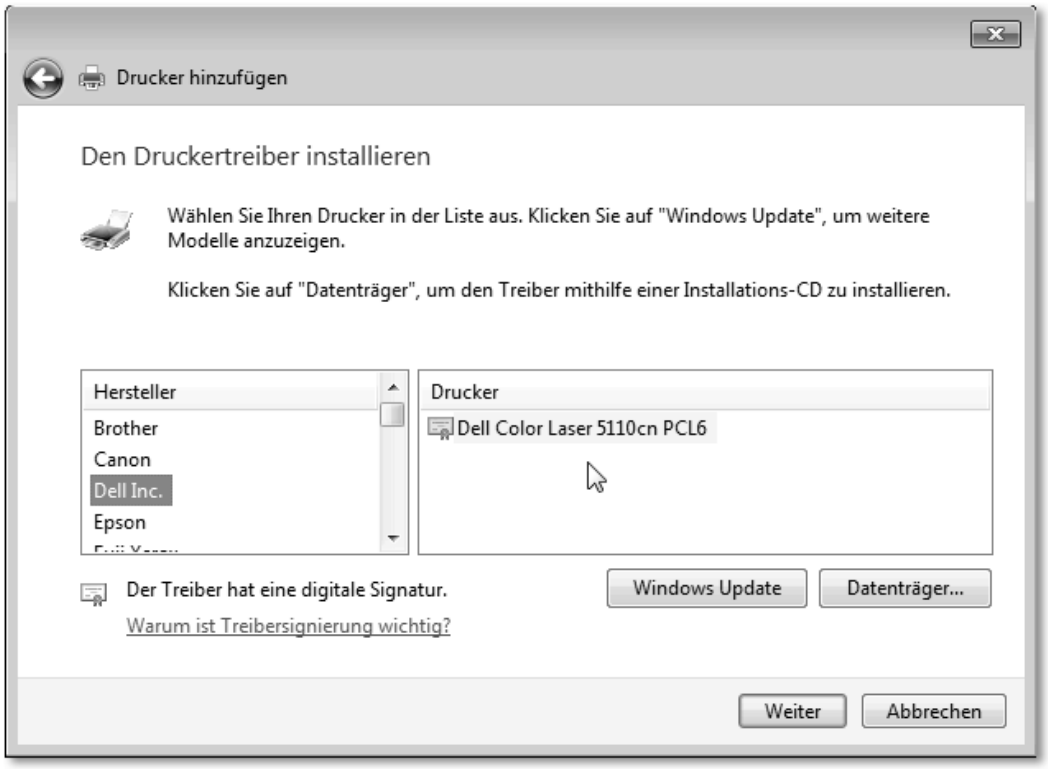


Abbildung 6.109 Der dem Image hinzugefügte Treiber steht zur Verfügung – hier der Beweis.

- Ich habe das Package mit den *Remote Server Administration Tools for Windows 7* installiert, diese liegen in Form einer MSU-Datei vor. Die gewünschten Werkzeuge werden als Feature hinzugefügt, müssen aber noch installiert werden. Wie Abbildung 6.110 (links) zeigt, sind diese in der Feature-Auflistung vorhanden.
- Abbildung 6.110 (rechts), zeigt schließlich, dass die deaktivierten Features auch tatsächlich deaktiviert sind. Da ein »normaler« Benutzer keine Windows-Features aktivieren kann, stehen ihm die auf diese Weise deaktivierten Spiele nicht zur Verfügung – und er muss nun *Purble Place* spielen.

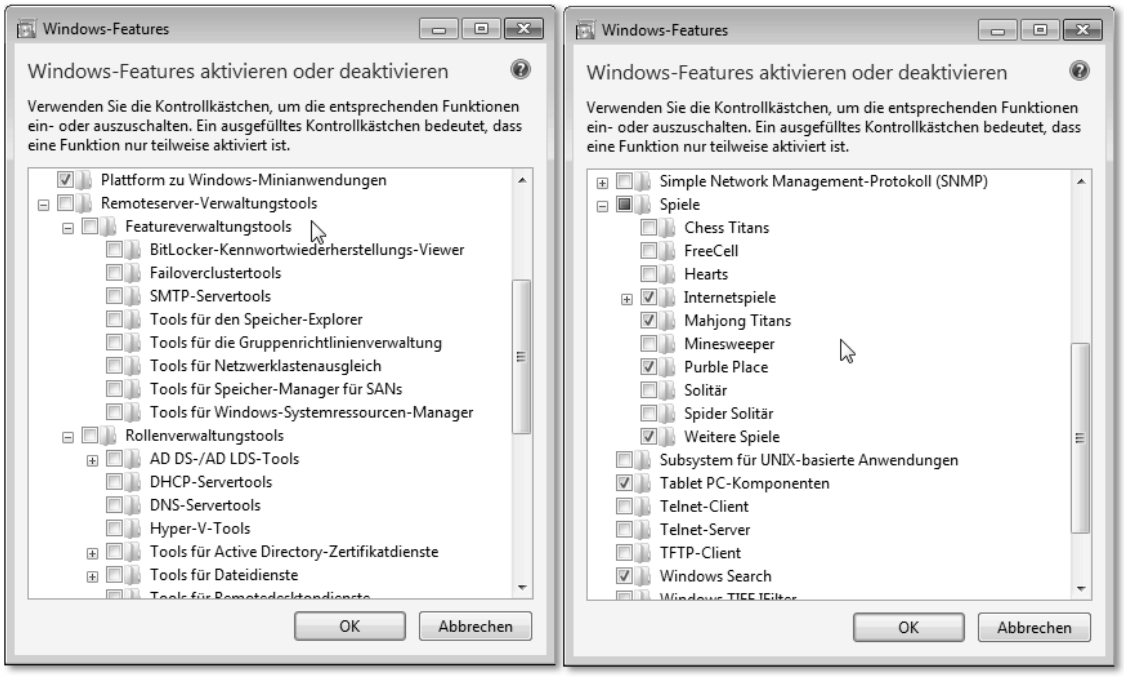


Abbildung 6.110 Die Remoteserver-Verwaltungstools wurden als Package in das WIM-Image eingefügt. Etliche Spiele wurden deaktiviert.

6.10.7 Treiber und Boot-Images

Bislang hatte ich das Aktualisieren von Treibern und sonstige Image-Pflege-Maßnahmen eher auf Installations-Images bezogen. Im Normalfall dürften in den aktuellen Boot-Images geeignete Treiber vorhanden sein, um starten zu können. Falls der PC einen exotischen Festplatten-Controller verwendet, könnte es sein, dass ein entsprechender Treiber in das Boot-Image integriert werden muss. Gehen Sie dazu so vor, wie beschrieben: Mounten Sie das WIM-Image, integrieren Sie den Treiber (`/add-driver`), und unmounten Sie ihn mit dem Parameter `/commit`.

6.11 Treiber und Windows-Bereitstellungsdienste

Vermutlich haben Sie bereits ein wenig in dem Verwaltungswerkzeug für die Windows-Bereitstellungsdienste gestöbert und dabei den Knoten TREIBER entdeckt (Abbildung 6.111). Hier stellt sich nun die Frage, wie diese Treiberfunktion sich von der zuvor gezeigten Integration von Treibern in das Image unterscheidet (siehe Abschnitt 6.10.2, »Treiber verwalten«).

Die WDS können bei der Installation eines WIM-Images einen Treiberspeicherort zur Verfügung stellen. Das funktioniert bei allen Betriebssystemen ab Vista SP1 (also auch Windows Server 2008, Windows Server 2008 R2 und natürlich Windows 7). Sie können sich das so vorstellen, dass beim Plug&Play-Vorgang, also der Hardwareerkennung und Treiberinstallation, die hier hinzugefügten Treiberpakete als zusätzliche Quelle zur Verfügung stehen.

Netzwerkkartentreiber bei Bedarf integrieren

Damit die Installation der über den WDS-Server zur Verfügung gestellten Treiber funktioniert, muss der WDS-Server über eine Netzwerkverbindung erreichbar sein. Sollte ein passender Netzwerkkartentreiber nicht im Standardumfang von Windows 7 enthalten sein, müssen Sie einen solchen in das Boot-Image integrieren (von der Vorgehensweise so, wie in Abschnitt 6.10.2, »Treiber verwalten«, beschrieben).

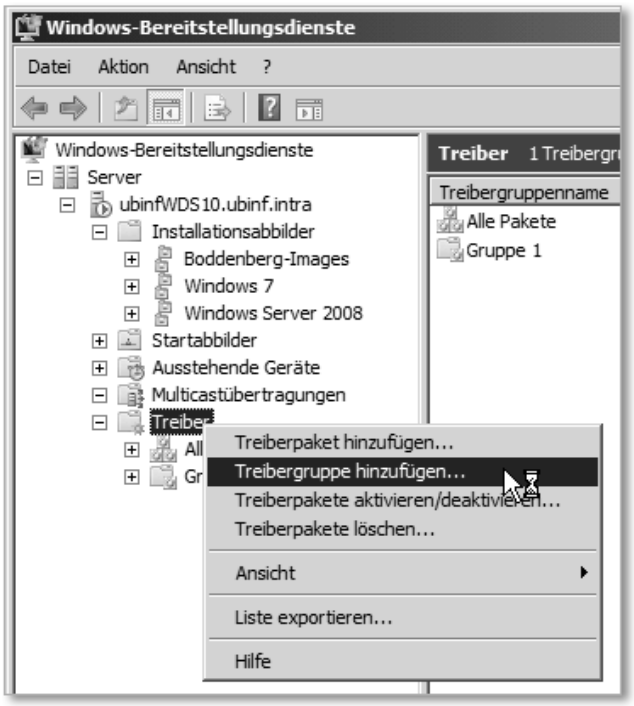


Abbildung 6.111 Im Kontextmenü des Knotens »Treiber« finden sich diverse Menüpunkte zum Verwalten.

Die Verwendung der Treiberfunktionalität macht es also noch einfacher, Treiber für neue Geräte bereitzustellen – wie das geht, zeige ich Ihnen in den nächsten Abschnitten.

6.11.1 Treibergruppe einrichten

Auf Abbildung 6.111 sehen Sie, dass es neben Treiberpaketen noch Treibergruppen gibt. Die Treibergruppen verfolgen zwei Ziele:

- In Treibergruppen können Treiberpakete strukturiert angeordnet werden. Wenn Sie viel unterschiedliche Hardware mit vielen unterschiedlichen Treibern haben, kann das schon vorteilhaft sein.
- Der in etlichen Fällen wichtigere Zweck ist allerdings, dass über die Gruppen gesteuert werden kann, für welche Hardware und welches Image die in einer Gruppe vorhandenen Treiber zur Verfügung stehen. Es kann durchaus notwendig sein, bestimmte Treiber von einem Hardwaretyp auszuschließen, weil der Treiber zuerst erkannt und anstelle eines viel besser geeigneten Treibers installiert wird.

Treiberpakete können übrigens Mitglied mehrerer Treibergruppen sein, insofern gibt es ein hohes Maß an Flexibilität. Diese hohe Flexibilität hat aber auch durchaus Schattenseiten: Falls Sie wirklich darauf angewiesen sind, Treiber von bestimmten PC-Typen fernzuhalten, gibt es schon einen gewissen Planungsaufwand.

Treibergruppen erstellen Sie, wie erwartet, mit einem Assistenten, den Sie über das Kontextmenü des Knotens TREIBER (vergleiche Abbildung 6.111) aufrufen können. Der Assistent fragt erst ganz harmlos nach einem Namen für die Treibergruppe (Abbildung 6.112) – das ist der richtige Moment, um nochmals auf einen organisatorischen Aspekt hinzuweisen. Ich habe als Namen DRUCKER eingetragen, was sich ja zunächst auch sinnvoll anhört: Alle Druckertreiber werden in einer Gruppe zusammengefasst und nach Bedarf installiert: Das ist so weit in Ordnung.

Es könnte aber darüber hinaus notwendig sein, separate Treibergruppen für bestimmte Gerätefamilien einzurichten (z. B. *Dell Optiplex, Lenovo ThinkPad*), die dann über Filter zugewiesen werden. Sie sollten also nicht ausschließlich in Treiberkategorien (Druckertreiber, Monitortreiber etc.) denken, sondern berücksichtigen, dass es notwendig sein könnte (!), Treiber mithilfe von gefilterten Treibergruppen zu separieren.

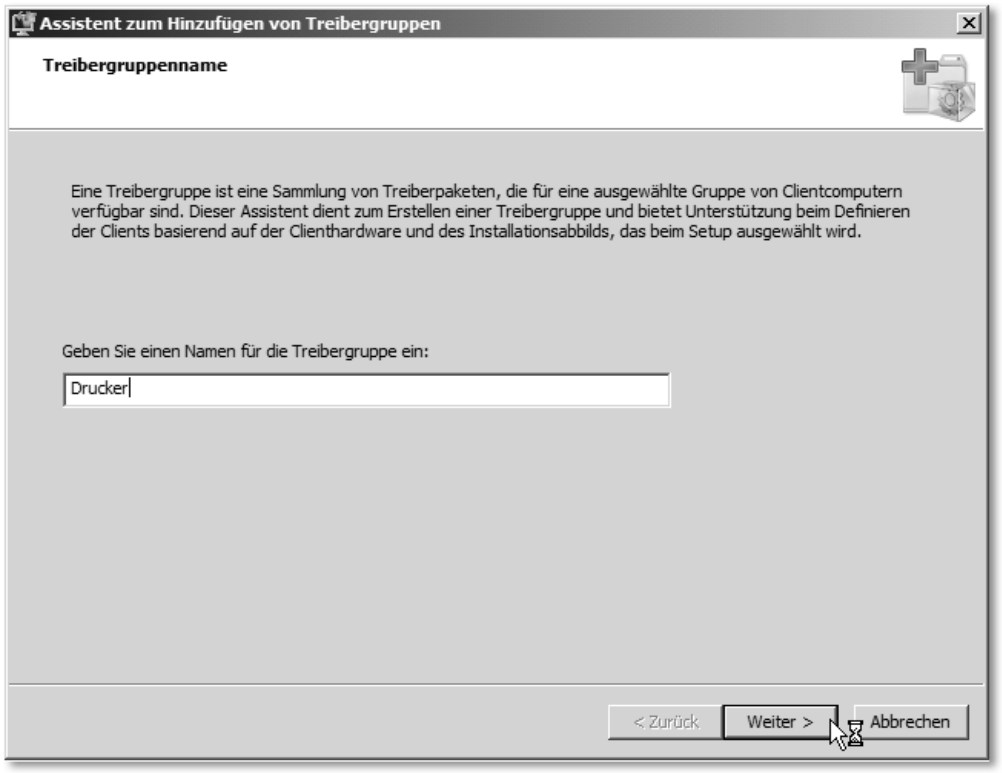


Abbildung 6.112 Es ist unter Umständen sinnvoll, die Treiberpakete auf mehrere Treibergruppen aufzuteilen.

Eine Treibergruppe verfügt über zwei unterschiedliche Filtermechanismen:

- *Clienthardwarefilter* (Abbildung 6.113):
  Wenn die einer bestimmten Treibergruppe zugeordneten Treiber nur für bestimmte Hardware verwendet werden sollen, kann das über diese Filter gesteuert werden. Wie Sie auf der Abbildung sehen, gibt es Filter wie beispielsweise Hersteller, BIOS oder UUID (ID des PCs). Die Filter können positiv (ist gleich) oder negativ (ist ungleich) wirken.
- *Installationsabbildfilter* (Abbildung 6.114):
  Sie können weiterhin die Verfügbarkeit von Treibern über das Installationsabbild filtern. Wenn Sie also ein deutsches Windows 7 installieren, können Sie dafür sorgen, dass auch nur deutschsprachige Treiber installiert werden. Oder Sie können verhindern, dass für Windows 7 versehentlich ein alter Windows-XP-Treiber erkannt und installiert wird, der dann im schlimmsten Fall den Start des Betriebssystems verhindert.

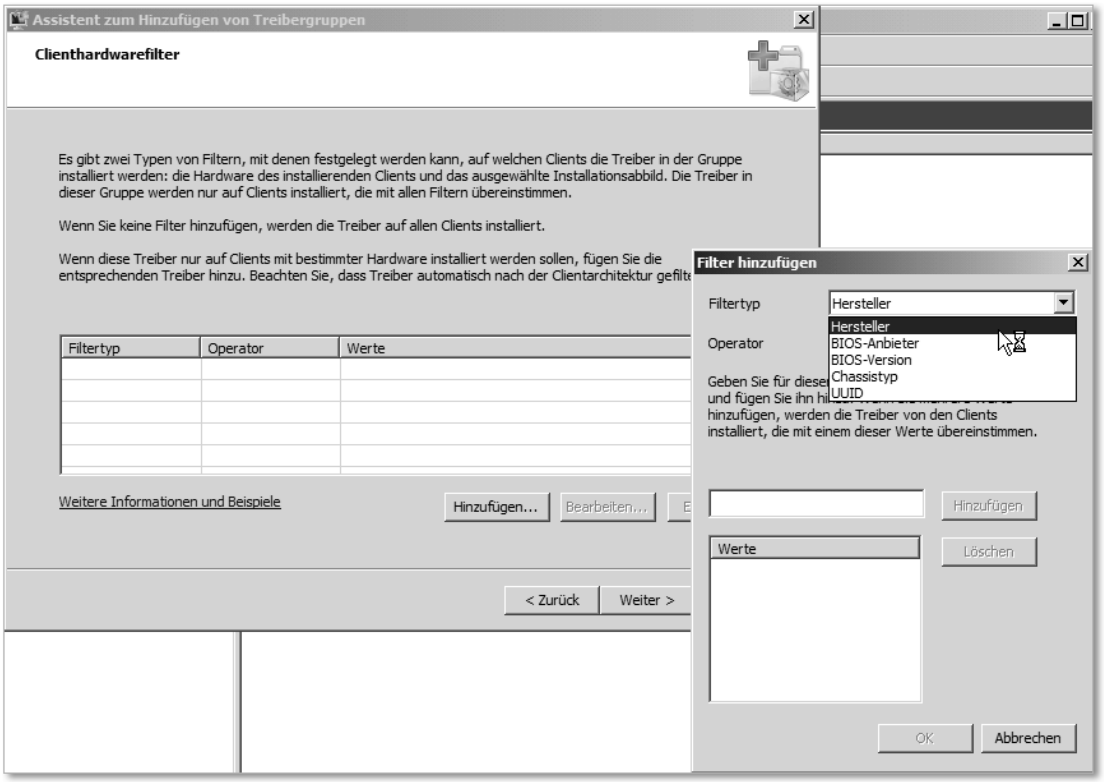


Abbildung 6.113 Optional können Sie Filter für die Clienthardware einrichten.

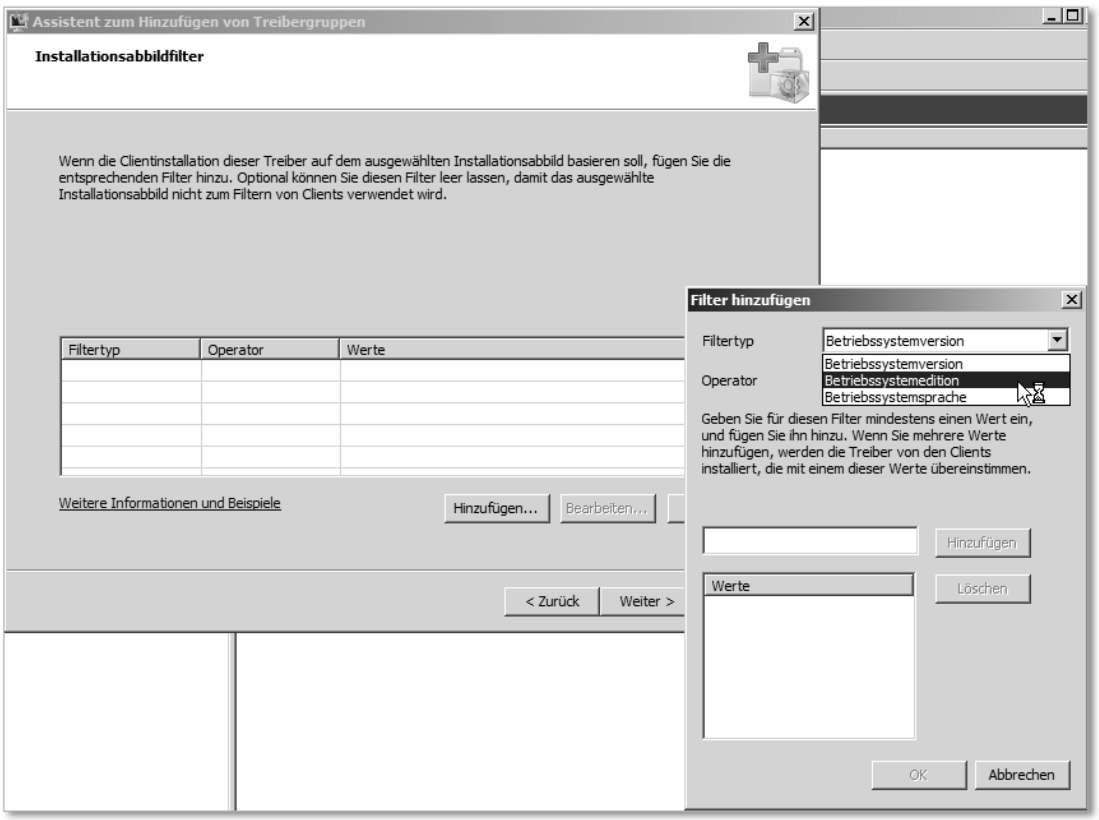


Abbildung 6.114 Über diese Filter ordnen Sie die Treibergruppen den Installationsabbildern zu.

Erst prüfen, ob es Probleme gibt

Bevor Sie nun schon hektisch ein Team-Meeting einberufen und mit gezückten Stiften zum Flipchart laufen, um ein Treibergruppenfilterkonzept zu entwerfen, möchte ich kurz bremsen: In den meisten Fällen funktioniert die Treibererkennung von Windows 7 (und übrigens auch von seinen Vorgängern) sehr ordentlich und installiert eben nicht unsinnige und Probleme verursachende Treiber. Die Empfehlung ist also, zunächst ohne komplizierte Filtermaßnahmen zu starten und zu beobachten, ob alles funktioniert. Sollte es Probleme geben, können Sie dann mit Filtern eingreifen.

Der nächste Dialog fragt, ob nur die wirklich benötigten Treiber installiert werden sollen oder ob Sie gern alle Treiber der Gruppe auf den PCs wiederfinden möchten (Abbildung 6.115):

- Im Allgemeinen macht es Sinn, nur die laut Hardwareerkennung wirklich benötigten Treiber zu installieren.
- Es sind allerdings Szenarien denkbar, in denen bestimmte Treiber auf jeden Fall installiert werden sollen. So wäre es beispielsweise denkbar, dass auf allen Notebooks Druckertreiber für einige Modelle installiert werden, mit denen die Außendienstmitarbeiter im Heimbüro arbeiten. Diese Treiber müssten natürlich unabhängig von den zum Installationszeitpunkt angeschlossenen Geräten auf die Installation kopiert werden.

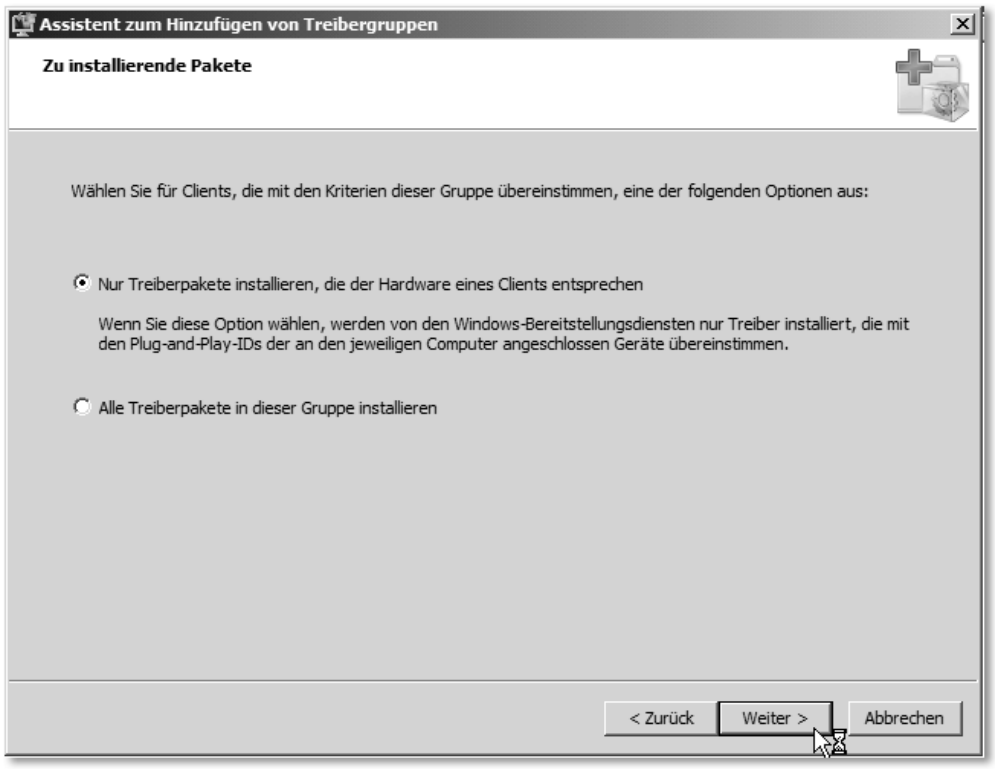


Abbildung 6.115 Sinnvolle Einstellung: Es werden nur Treiberpakete installiert, die auch zur Hardware passen.

Zum Vergleich ein Beispiel: Wenn Sie einen Druckertreiber zur Treibergruppe hinzufügen und der Drucker ist zum Installationszeitpunkt *nicht* angeschlossen, werden Sie folgendes Verhalten beobachten:

- Ist die erste Option gewählt (NUR TREIBERPAKETE INSTALLIEREN...), wird der Druckertreiber beim späteren manuellen Hinzufügen nicht zur Auswahl stehen.
- Ist die Option ALLE TREIBERPAKETE... gewählt, wird der Treiber auf der Betriebssysteminstallation vorhanden sein. Es ergibt sich also ein Szenario, wie es auf Abbildung 6.109 gezeigt ist.

6.11.2 Treiberpaket hinzufügen

Das Hinzufügen eines Treiberpakets ist ähnlich simpel. Sie wählen den entsprechenden Menüpunkt des Kontextmenüs (vergleiche Abbildung 6.111), worauf-hin ein Assistent startet:

- Entscheiden Sie zunächst, ob Sie gezielt eine .INF-Datei angeben möchten oder ob alle Treiber installiert werden sollen, die sich in einem Verzeichnis und seinen Unterverzeichnissen befinden (Abbildung 6.116).

Abbildung 6.116 Hinzufügen eines Treiberpakets

An dieser Stelle möchte ich Sie auf den auf der Dialogseite angebrachten Hinweis aufmerksam machen, der besagt, dass die zu installierenden Treiber ausgepackt sein müssen. Treiber in einem ZIP-, EXE- oder MSI-Archiv werden nicht gefunden.

- Im zweiten Schritt erhalten Sie eine genaue Auflistung der gefundenen Treiber, wobei auch eine einzelne INF-Datei mehrere Treiber – beispielsweise für verschiedene Hardwarearchitekturen – enthalten kann. Sie können individuell auswählen, was dem WDS-Treiberarchiv hinzugefügt werden soll.

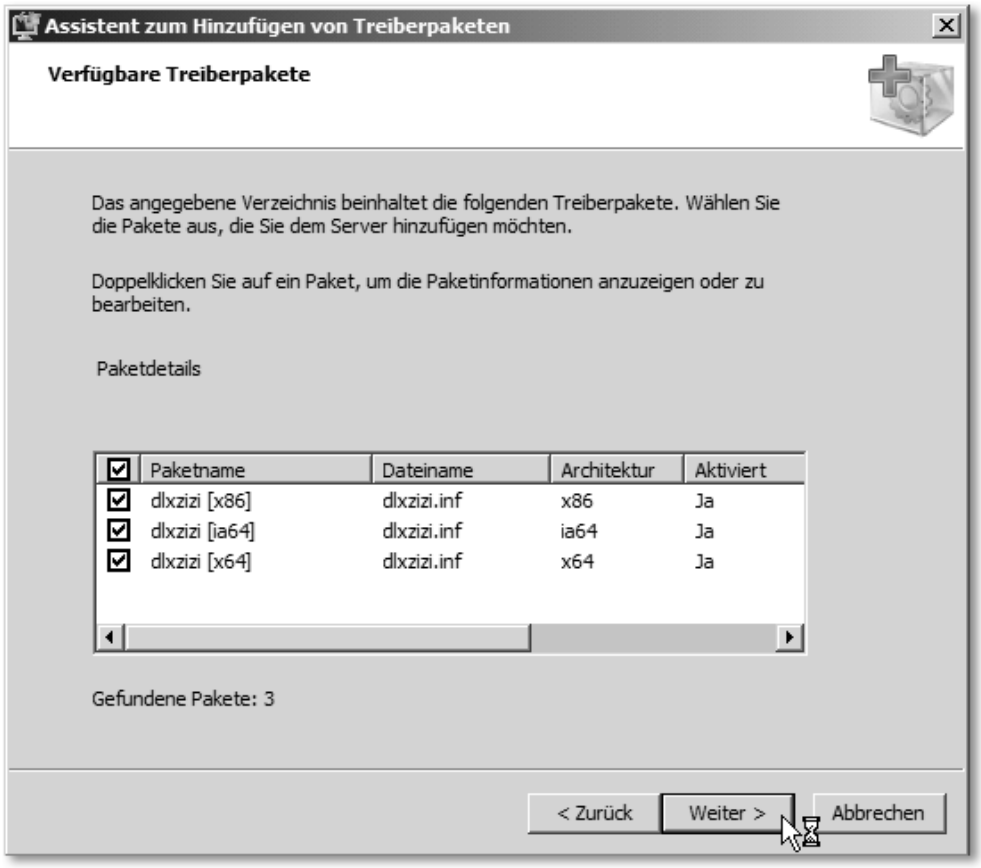


Abbildung 6.117 Die im Treiberpaket enthaltenen Pakete können separat ausgewählt werden.

- Der dritte Schritt besteht darin, auszuwählen, in welche Treibergruppe das neue Treiberpaket einsortiert werden soll. Sie können eine bestehende Gruppe wählen, eine neue erstellen, oder das Treiberpaket wird zu keiner Gruppe hinzugefügt (Abbildung 6.118).

Anzumerken wäre, dass Sie die Zugehörigkeit eines Treiberpakets zu einer oder mehreren Gruppen jederzeit und absolut problemlos modifizieren können.

Abbildung 6.118 Der Treiber kann einer bestehenden Treibergruppe hinzugefügt werden.

Hierzu gibt es zwei Möglichkeiten:

- Im Kontextmenü einer Gruppe findet sich ein Menüpunkt namens TREIBERPAKET ZU DIESER GRUPPE HINZUFÜGEN. Es erscheint ein Dialogfenster, in dem Sie recht einfach nach Treibern suchen können, die für eine Gruppe relevant sind. Auf Abbildung 6.119 suche ich beispielsweise nach Druckertreibern von Dell für ein x64-Betriebssystem. Aus den Suchergebnissen können Sie dann die Treiber auswählen, die Sie tatsächlich der Gruppe hinzugefügen wollen.
- Die zweite Möglichkeit führt über den Eigenschaften-Dialog des Treiberpakets. Auf der ersten Registerkarte sind einige allgemeine Details zum Treiber gezeigt (Abbildung 6.120). Die Registerkarte GRUPPENMITGLIEDSCHAFT enthält einen einfach zu bedienenden Dialog, mit dem das Treiberpaket einer oder mehreren Gruppen hinzugefügt werden kann.

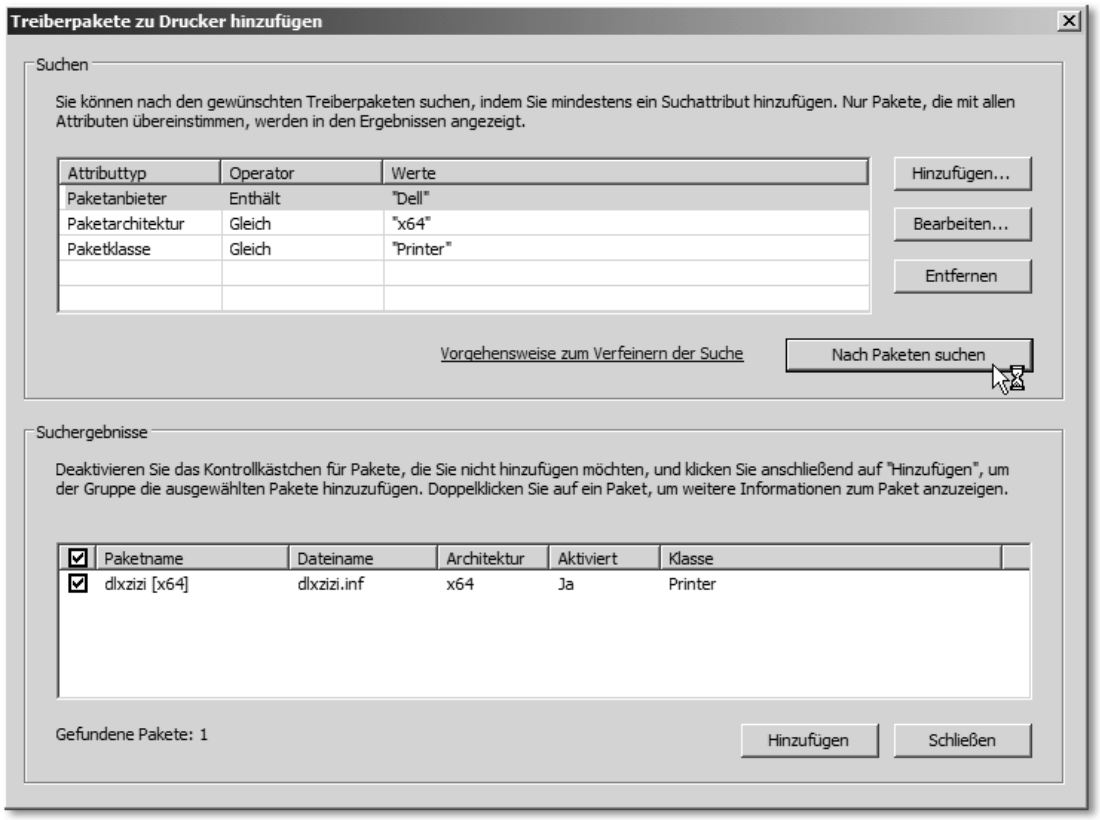


Abbildung 6.119 Mit diesem Suchdialog können Sie recht einfach Treiber finden und einer Treibergruppe hinzufügen.

Abbildung 6.120 Die Eigenschaften eines Treibers. Auf der Registerkarte »Gruppenmitgliedschaft« können Sie sich schnell orientieren, in welchen Gruppen der Treiber enthalten ist.

6.11.3 Ein Blick in setupact.log

Wie Sie wissen, kann man den Installationsvorgang sehr detailliert mit den Logs verfolgen, die im Verzeichnis *c:\windows\panther* liegen. Abbildung 6.121 zeigt die relevante Stelle in der Datei *setupact.log*:

- In der Konfiguration der Treibergruppe war eingestellt, dass die dort enthaltenen Treiber auch installiert werden sollen, wenn sie nicht aktuell gebraucht werden.
- Da der entsprechende Dell-Drucker zum Installationszeitpunkt nicht am PC angeschlossen war, traf genau dies zu.
- In der Abbildung ist der Pfad markiert, von wo die Treiber gelesen werden. Die IP-Adresse verweist auf den WDS-Server.
- Das Treiberpaket enthält Versionen für alle drei Architekturen (siehe auch Abbildung 6.117). Diese werden auch korrekt aufgelistet.

  Schaut man später an den Treiberspeicherort (*c:\Windows\System32\DriverStore\FileRepository*), wird man übrigens feststellen, dass nur die Treiber für die passende Hardwarearchitektur installiert worden sind. Vernünftig, denn was sollen auch IA64-Treiber auf einer x64-Plattform (wo sie ja nicht laufen)?

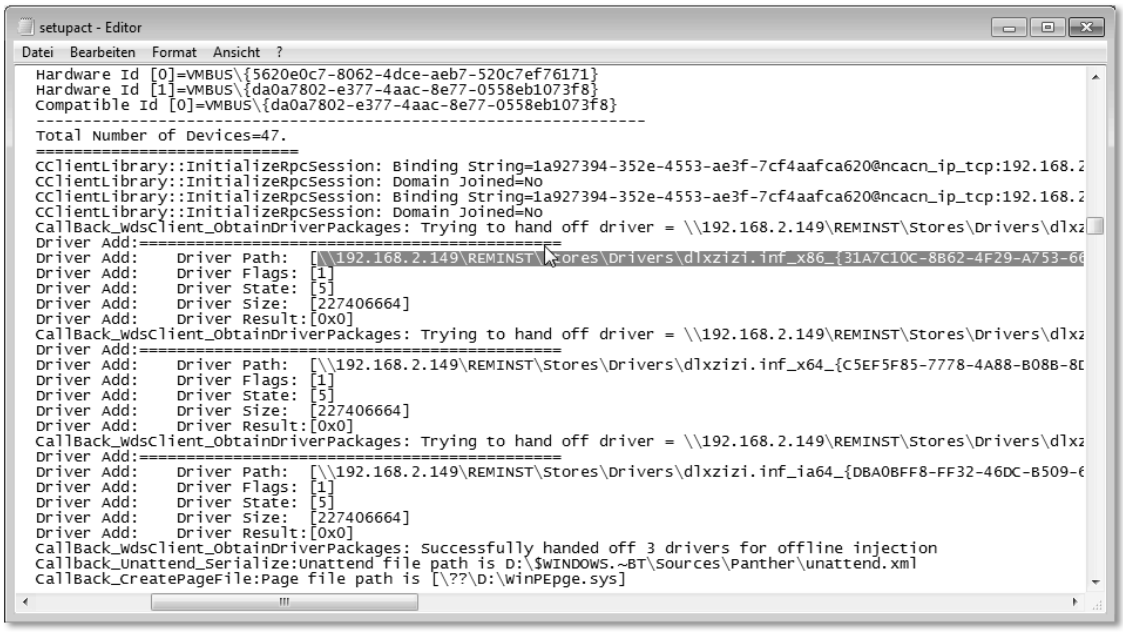


Abbildung 6.121 Das Einsetzen der Treiber in der Datei »setupact.log«

6.12 Multicastübertragungen

Wenn Sie einzelne Clients installieren, brauchen Sie sich um Themen wie Netzwerkbandbreite und Serverbelastung nicht groß zu kümmern. Wenn Sie aber in relativ kurzer Zeit Hunderte Clients installieren, sind die Datenmengen, die bewegt werden müssen, eventuell zu groß. Die eigentliche Netzwerkbandbreite ist vermutlich nicht das eigentliche Problem, sondern viel mehr der WDS-Server, der große Downloads von Dutzenden Clients nicht verkraften wird. Der Engpass sind hier sowohl die Netzwerkbandbreite des WDS-Servers zum Core-Switch als auch die Leistung der Platten.

Ein weiteres Problem sind Installationen an Remote-Standorten. Auch auf gut ausgebauten Strecken ist es ein signifikanter Unterschied, ob Sie einmal 3,5 GB oder dreißigmal 3,5 GB übertragen.

Der Lösungsansatz ist die Übertragung mittels Multicasting. Die Grundidee ist eigentlich recht simpel: Die Daten werden einmal gesendet und dabei von mehreren Clients empfangen. Letztendlich ist es aber nicht ganz so simpel, unter anderem deshalb, weil nicht unbedingt davon ausgegangen werden kann, dass alle Clients exakt zur selben Zeit starten. Demzufolge muss die Übertragung mehrmals durchgeführt werden. Das insgesamt übertragene Volumen sollte aber trotzdem deutlich geringer sein als bei konventioneller Vorgehensweise.

In den Eigenschaften des WDS-Servers findet sich eine Registerkarte, auf der einige Konfigurationen für das Multicasting vorgenommen werden können (Abbildung 6.122). Die Optionen sind meines Erachtens selbsterklärend.

Die Verwendung von Multicastübertragungen ist einfacher, als es sich vielleicht anhört – das werden Sie gleich sehen.

Die Probleme (oder besser: Herausforderungen) bestehen eher in der Konfiguration der beteiligten Netzwerkkomponenten, zumindest dann, wenn Sie nicht nur ein lokales Netz betreiben, sondern in einer mehr oder weniger großen gerouteten Infrastruktur leben. Das wird also ein Projekt, bei dem Server- und Netzwerkadministratoren beweisen können, dass gute Zusammenarbeit möglich ist.

6.12.1 Multicastübertragung einrichten und konfigurieren

Wenn Sie eine Multicastübertragung verwenden möchten, müssen Sie eine solche erstellen – ein gleichnamiger Menüpunkt findet sich im Kontextmenü des Knotens Multicastübertragungen (Abbildung 6.123).

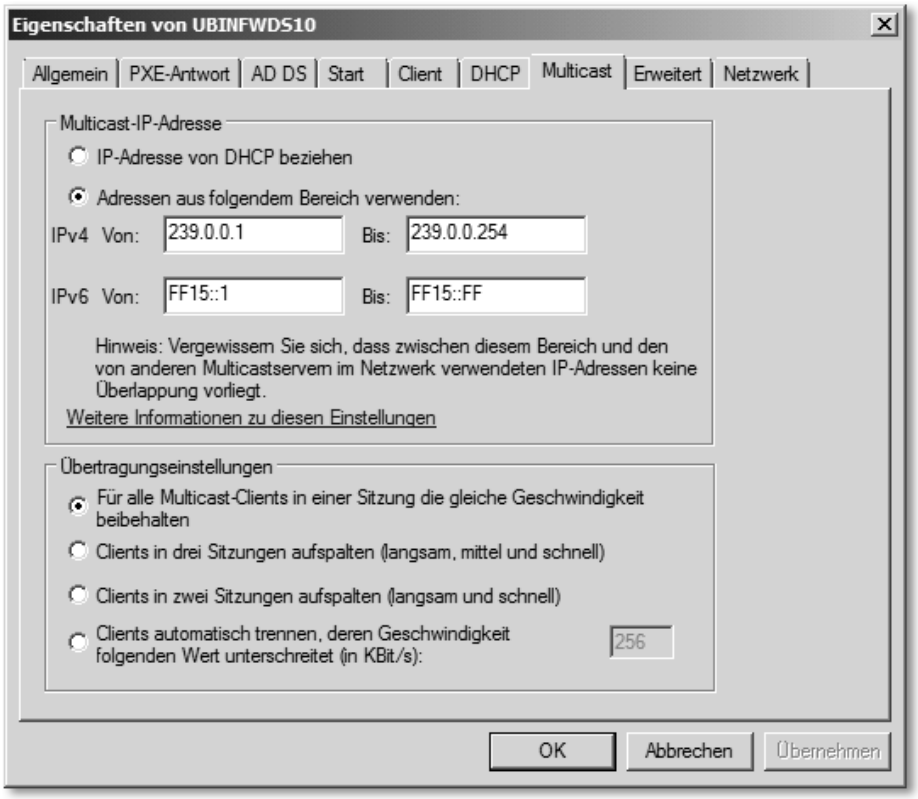


Abbildung 6.122 Konfiguration von Multicastübertragungen in den Eigenschaften des WDS-Servers

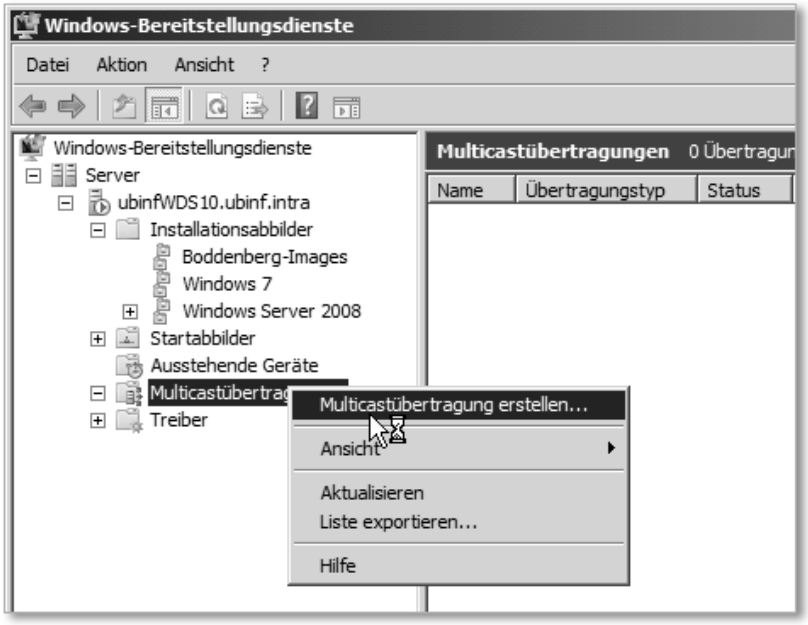


Abbildung 6.123 Hier initiieren Sie das Erstellen einer Multicastübertragung.

Der Assistent startet mit der obligatorischen Abfrage eines Namens für die Multicastübertragung (Abbildung 6.124).

Abbildung 6.124 Die erste Dialogseite zum Erstellen der Multicastübertragung

Eigentlich ist das nicht weiter spektakulär, aber um einen geeigneten Namen zu wählen, ist es erforderlich, das Konzept zu kennen, das ich hier im Telegrammstil erläutere:

- Eine Multicastübertragung wird für ein WIM-Image konfiguriert. Aus diesem Grund ist der nächste Dialog auch die Auswahl des Images, für das die Übertragung erstellt wird (Abbildung 6.125).
- Wenn ein Client dieses Image installieren möchte, entweder weil es das Standard-Image ist oder weil eine entsprechende Konfiguration vorgenommen worden ist, wird eine Multicast-Übertragung initiiert. Anders gesagt: Das Image kann nicht mehr ohne Multicasting heruntergeladen werden.

Ist das WIM-Image der Multicastübertragung zugeordnet, müssen Sie noch den Multicasttyp auswählen. Hier geht es nicht um so etwas Komplexes wie etwa unterschiedliche Protokolle, sondern ganz profan darum, wann und wie die Übertragung gestartet wird (Abbildung 6.126):

- Die erste Option, nämlich CAST (AUTOMATISCH), sorgt dafür, dass die Übertragung sofort startet, wenn ein Client das Image anfordert. Der Unterschied zu einer »normalen« Übertragung (also ohne Multicasting) ist, dass später hinzukommende Clients in die Übertragung einbezogen werden. Damit diese das Image komplett erhalten, beginnt die Übertragung später von vorn.

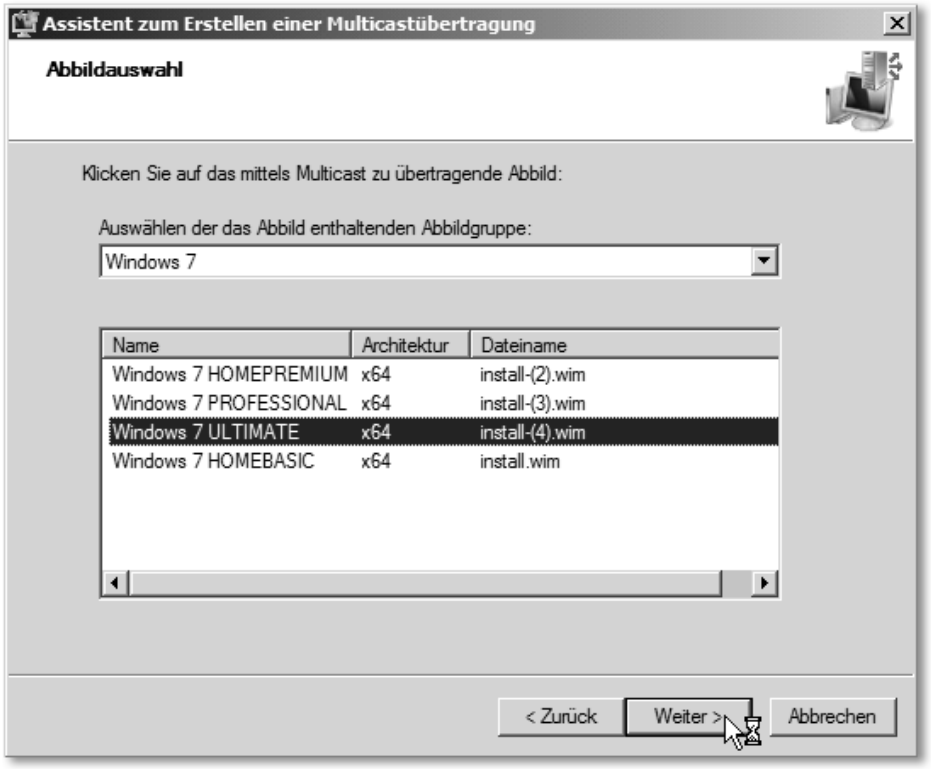


Abbildung 6.125 Auswahl des Abbilds, das mittels Multicast übertragen werden soll.

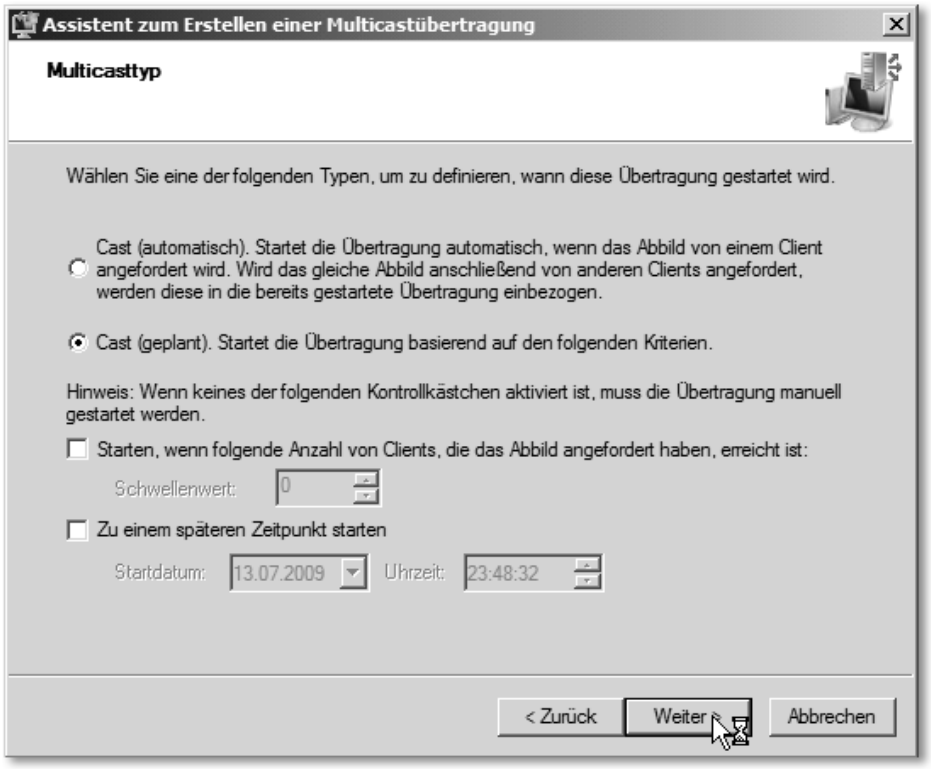


Abbildung 6.126 In diesem Dialog bestimmen Sie den Multicasttyp.

- Ist die Option CAST (GEPLANT) gewählt, startet die Übertragung an die Clients entweder bei einer bestimmten Anzahl von Clients, die auf die Übertragung warten, oder zu einem bestimmten Zeitpunkt.
  Sofern keine Startbedingungen gewählt sind, muss die Übertragung manuell gestartet werden.

Welchen Multicasttyp Sie wählen, hängt von Ihren individuellen Rahmenbedingungen ab:

- Wenn mehrere Teams neue PCs vorbereiten, macht es sicherlich Sinn, die erste Option (AUTOMATISCH) zu wählen: Die Übertragung beginnt sofort, und das Image ist in absehbarer Zeit auf dem PC.
- Sofern eine größere Menge von PCs vorbereitet und dann in einem Rutsch installiert werden soll, eignet sich die zweite Option.

6.12.2 … und die Übertragung läuft

Wenn für ein Image eine Multicastübertragung konfiguriert ist, erhalten es die Clients über dieses Verfahren – das ist so weit einleuchtend und wurde bereits zuvor erläutert. Welche Clients an einer Multicastübertragung »teilnehmen« bzw. auf den Start einer Übertragung warten, können Sie im WDS-Konfigurationswerkzeug unterhalb des jeweiligen Knotens sehen: Auf Abbildung 6.127 warten derzeit zwei Clients auf den Beginn einer Übertragung, die für einen manuellen Start konfiguriert ist.

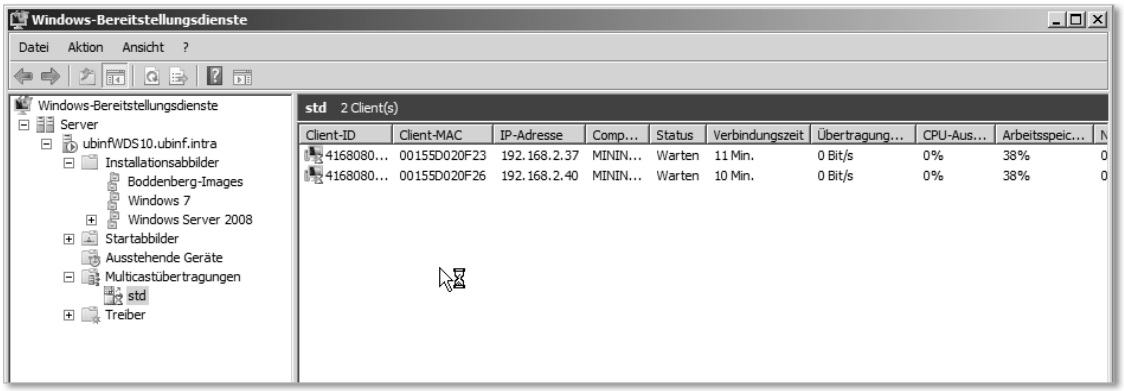


Abbildung 6.127 Momentan warten zwei Clients auf den Beginn der Multicastübertragung.

Auf den Clients bietet sich derweil die in Abbildung 6.126 gezeigte Ansicht: Der Client fragt in regelmäßigen Abständen den WDS-Server ab und wartet auf den Start der Übertragung. Diesen Bildschirm sehen Sie übrigens auch bei einer »normalen« Installation für einige Sekunden. Daher ist das eventuell ein wenig verwirrend, und man könnte auf die Idee kommen, dass etwas nicht stimmt. Keine

Sorge, es passt alles – es wäre allerdings schön, wenn der Client anzeigen würde, dass er auf den Beginn einer Multicastübertragung wartet.

Abbildung 6.128 Dieser Client wartet darauf, dass die Multicastübertragung beginnt – für die Wunschliste: Es wäre schön, wenn das angezeigt würde.

In dem auf den Screenshots gezeigten Beispiel wurden für die Multicastübertragungen keine Startbedingungen angegeben, sodass die Übertragung manuell gestartet werden muss (Abbildung 6.129).

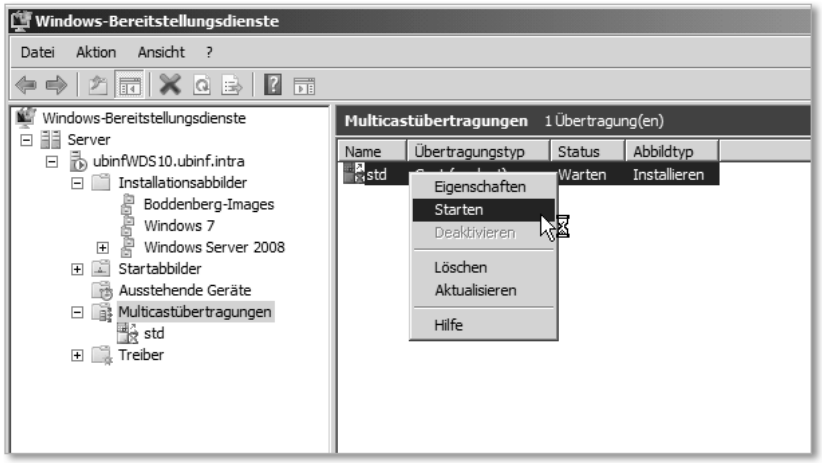


Abbildung 6.129 Wenn die Multicastübertragung nicht für einen automatischen Start konfiguriert ist, müssen Sie sie manuell starten.

Ist die Übertragung gestartet, ist wenige Sekunden später auf den Clients zu sehen, dass die Übertragung läuft. Auch in der WDS-Administrationskonsole ist zu sehen, dass die Übertragung läuft: Es werden unter anderem der prozentuale Fortschritt und die Übertragungsgeschwindigkeit angezeigt (Abbildung 6.130).

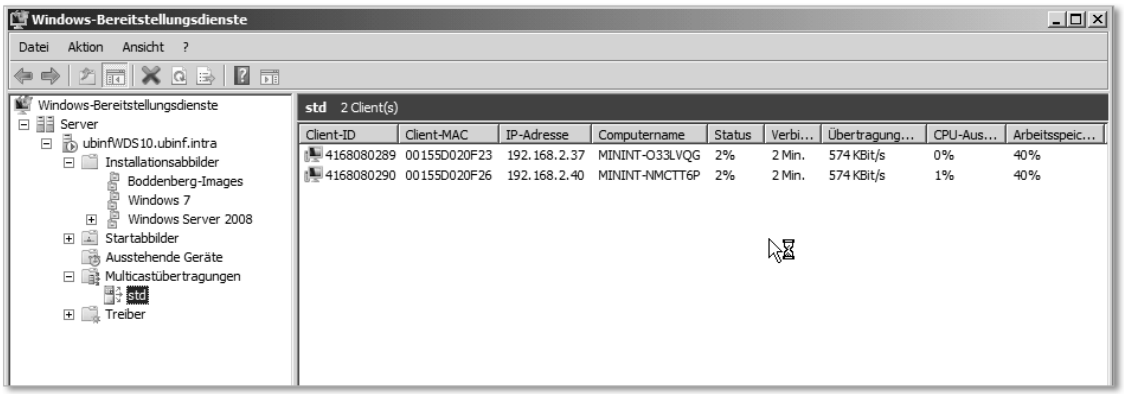


Abbildung 6.130 Hier läuft die Übertragung.

Auf Abbildung 6.131 habe ich eine Multicastübertragung mit dem Netzwerkmonitor mitgeschnitten. Sie sehen, dass von dem WDS-Server (192.168.2.149) Pakete per UDP an die Multicastadresse 239.0.0.104 gesendet werden.

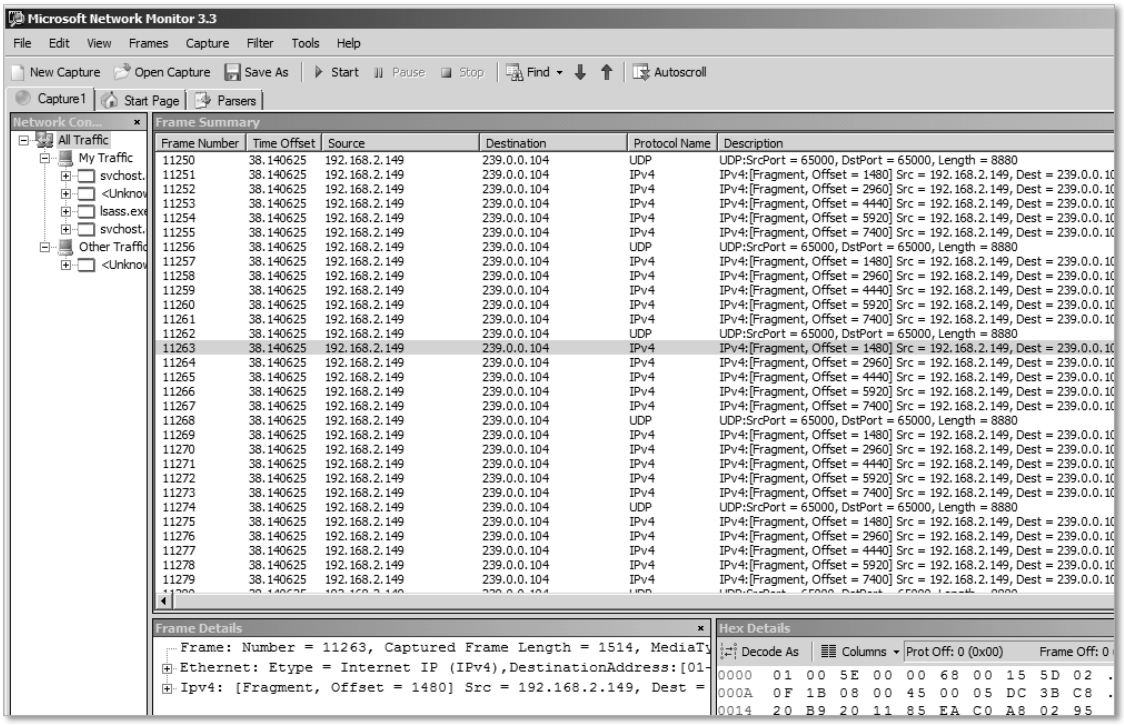


Abbildung 6.131 Die Übertragung im Netzwerkmonitor. Der WDS-Server sendet an die Multicastadresse.

Der Bereich für die Multicastadressen ist in meinem Beispiel in den Einstellungen des WDS-Servers vorgegeben (Abbildung 6.122). Wie Sie unter anderem auf Abbildung 6.128 sehen können, haben die Clients eine normale IP-Adresse. Über diese IP-Adresse liefern die Clients regelmäßig Rückmeldungen an den WDS-Server. Dies ist notwendig, weil die eigentliche Multicastübertragung über UDP-Pakete erfolgt und somit keine Rückmeldung des Clients an den Server stattfindet.

6.13 User State Migration Tool

Wenn in Ihrem Unternehmen keine servergespeicherten Profile (*Roaming Profiles*) eingesetzt werden, ist das Übernehmen der Profile der Benutzer kein ganz triviales Problem. Selbst wenn die Anwender keine Daten im Profil, sondern alles brav auf Netzwerklaufwerken speichern, sollten Sie sich um die Profile kümmern. Alternativ müssten Sie sämtliche Einstellungen des Benutzers nochmals vornehmen, angefangen vom Outlook-Profil bis hin zum Hintergrundbild.

6.13.1 USMT – simpel

Seit geraumer Zeit bietet Microsoft das *User State Migration Tool* (USMT) an, um Profile (und einiges mehr, siehe nächster Abschnitt) von einem PC auf einen anderen zu übertragen. Die aktuelle Version ist im WAIK enthalten (*C:\Programme\Windows AIK\Tools\USMT*. Unter diesem Pfad findet sich ein Verzeichnis für x86- und eines für x64-Maschinen). Das Werkzeug besteht im Wesentlichen aus zwei ausführbaren Dateien, nämlich:

- *ScanState.exe*: Liest Benutzerprofilinformationen (und mehr) von einem PC.
- *LoadState.exe*: Schreibt die von ScanState gesammelten Informationen zurück.

Auch wenn Sie sich mit den Details, insbesondere der Erstellung von Steuerdateien, nicht beschäftigen möchten, können Sie mit USMT recht schnell und einfach zum Erfolg kommen.

Ich führe Ihnen nachfolgend ein kleines Beispiel vor:

- Auf einem PC mit der 32-Bit-Version von Windows XP arbeitet der Benutzer *ubinf\fdahlke*.
- Der Hardware des PCs soll ausgetauscht werden, als neues Betriebssystem soll Windows 7 in der 64-Bit-Version zum Einsatz kommen.
- Im Unternehmensnetz werden keine servergespeicherten Profile eingesetzt, sodass das Profil des Benutzers migriert werden muss.
- Sinnvollerweise sollen auch Anwendungseinstellungen migriert werden.

Die Aufgabe kann einigermaßen simpel mit USMT durchgeführt werden, wobei folgende Schritte auszuführen sind:

- Kopieren Sie die für die Hardwarearchitektur des Clients benötigte Version von USMT (x86 oder x64) auf den PC, von dem Benutzerprofil und Einstellungen gelesen werden sollen. Die benötigten Dateien finden Sie in der WAIK-Installation (*C:\Programme\Windows AIK\Tools\USMT*). Die USMT-Anwendungen können übrigens auch von einem USB-Stick gestartet werden.
- Melden Sie sich als Administrator (bzw. mit lokalen administrativen Rechten) an.
- Starten Sie *ScanState.exe,* und lassen Sie sie die benötigten Daten auf ein Netzwerklaufwerk speichern. Abbildung 6.132 zeigt den entsprechenden Vorgang. Hier die Erläuterung der Kommandozeilenoptionen:
  - `/ue:*\*` sorgt dafür, dass keinerlei Benutzerprofile erfasst werden (`ue` steht für *user exclude*).
  - `/ui:ubinf\fdahlke` weist ScanState an, die Informationen zu dem angegebenen Benutzer zu erfassen (`ui` steht für *user include*). Die Kombination aus dem `/ue`- und dem `/ui`-Schalter sorgt dafür, dass nur Daten des dediziert angegebenen Benutzers erfasst werden.
  - Mit `/i`-Optionen werden die Definitionsdateien integriert. Diese Dateien enthalten die Steuerungsinformationen für USMT, beispielsweise welche Dateien und Registry-Einträge gespeichert werden sollen. *Miguser.xml* und *Migapp.xml* sind standardmäßig im USMT-Verzeichnis vorhanden. Sie können beliebige eigene Dateien erstellen, um spezielle Migrationsanforderungen zu erfüllen.
  - Die Option `/o` sorgt

Auf dem neuen PC führen Sie *LoadState.exe* aus, das sich ebenfalls im USMT-Verzeichnis befindet. Sie müssen mit administrativen Berechtigungen angemeldet sein und das Kommandozeilenfenster mit der Option Als Administrator ausführen gestartet haben. Als Parameter für den LoadState-Aufruf geben Sie den Speicherpfad auf dem Dateiserver und die XML-Definitionsdateien an. Letztere müssen die gleichen wie beim ScanState-Aufruf sein, in diesem Fall *MigUser.xml* und *MigApp.xml* (Abbildung 6.133).

Wenn der *LoadState*-Vorgang erfolgreich abgeschlossen wurde, wird der Benutzer bei der Anmeldung an dem neuen PC seine gewohnte Arbeitsumgebung vorfinden. Auf Abbildung 6.134 sehen Sie, dass der in der vorherigen XP-Umgebung eingestellte Bildschirmhintergrund und ein auf dem Desktop abgelegtes Dokument vorhanden sind.

```
M:\USMT\x86>scanstate.exe \\ubinffp01\verteilung\Migration\ubinfXP612 /ue:*\* /u
i:ubinf\fdahlke /i:miguser.xml /i:migapp.xml /o

Log messages are being sent to 'M:\USMT\x86\scanstate.log'

Starting the migration process
Processing the settings store

Examining the system to discover the migration units
 UBINF\fdahlke (1 of 2): 100% done
 This Computer (2 of 2): 100% done

Selecting migration units

Gathering data
 UBINF\fdahlke (1 of 2): 100% done
 This Computer (2 of 2): 100% done
 Commit

Success.

ScanState return code: 0

M:\USMT\x86>_
```

Abbildung 6.132 Mit ScanState werden die Profile auf einem PC eingelesen – in diesem Fall allerdings nur das Profil des Benutzers »ubinf\fdahlke«.

Anwendung wird nicht migriert

Ich möchte noch darauf hinweisen, dass USMT zwar Anwendungseinstellungen migriert, nicht aber die Anwendung selbst. Sie müssen auf dem Ziel-PC also beispielsweise die Microsoft-Office-Suite installieren, bevor der LoadState-Vorgang ausgeführt wird.

```
M:\USMT\amd64>loadstate.exe \\ubinffp01\verteilung\Migration\ubinfXP612 /I:migus
er.xml /i:migapp.xml

Log messages are being sent to 'M:\USMT\amd64\loadstate.log'

Starting the migration process
Processing the settings store

Selecting migration units

Examining the system to discover the migration units
 UBINF\fdahlke (1 of 2): 100% done
 This Computer (2 of 2): 100% done

Applying data
 UBINF\fdahlke (1 of 2): 100% done
 This Computer (2 of 2): 100% done

Success.

LoadState return code: 0

M:\USMT\amd64>_
```

Abbildung 6.133 Mit »LoadState« werden Profile zurückgeschrieben.

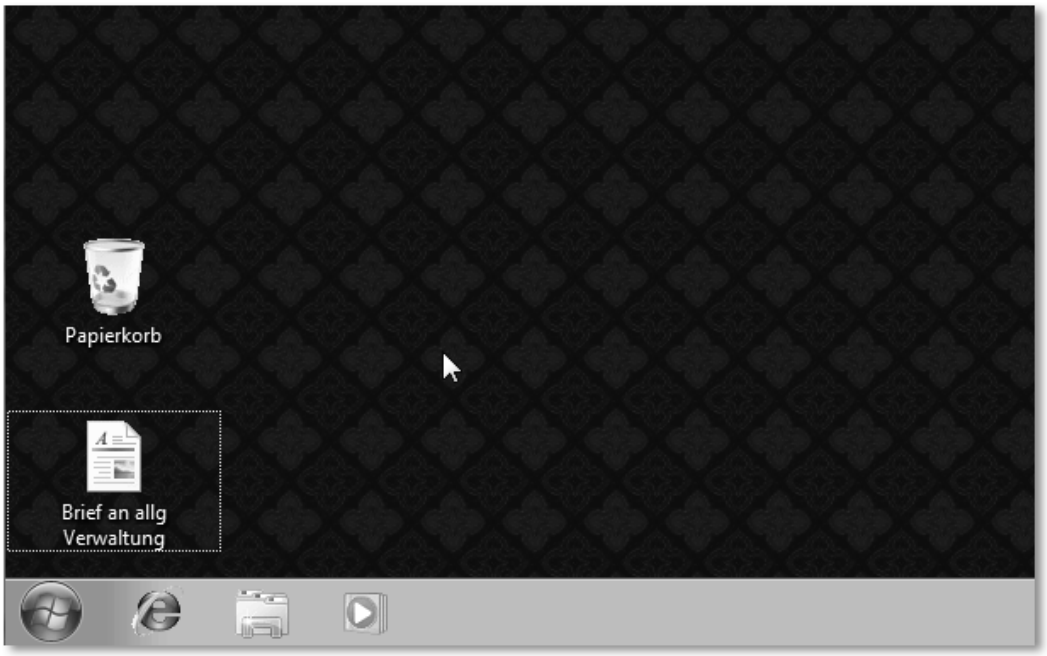


Abbildung 6.134 Die »Tapete« und die auf dem Desktop abgespeicherten Dateien sind da – funktioniert also.

6.13.2 USMT detailliert steuern

Im vorherigen Abschnitt haben Sie gesehen, dass die Migration von Profilen und Einstellungen mit USMT vergleichsweise simpel durchzuführen ist. Sofern Sie allerdings die Einstellungen spezieller Applikationen migrieren möchten oder aus bestimmten Nicht-Standard-Verzeichnissen (z. B. *c:\spezialapp\daten\user*) Daten »retten« möchten, kann USMT das für Sie zwar übernehmen, Sie müssen sich dann allerdings mit dem Werkzeug einigermaßen intensiv beschäftigen.

Ich möchte an dieser Stelle nicht seitenlang über die Erstellung der USMT-XML-Steuerdateien schreiben, da dies erfahrungsgemäß nur für einen kleinen Teil der Leser interessant sein dürfte. Wenn Sie die nachfolgend vermittelten Grundlagen kennen, dürfte es aber kein Problem sein, mithilfe der im WAIK enthaltenen Hilfedatei (*USMT.chm*) die gewünschten Einstellungen vorzunehmen.

Wie werden die USMT-Werkzeuge gesteuert?

Die USMT-Werkzeuge *ScanState* und *LoadState* werden durch XML-Dateien gesteuert. Drei Dateien sind standardmäßig vorhanden, nämlich:

- *MigApp.XML*: Sie enthält Einstellungen für die Migration von Anwendungen.
- *MigDocs.XML*: Sie enthält Einstellungen für die Migration von Dokumenten.
- *MigUser.XML*: Sie enthält Einstellungen für die Migration von Benutzerprofilen.

Abbildung 6.135 zeigt einen Ausschnitt aus der *MigUser.xml*. Diese XML-Dateien sind recht umfangreich. Wenn Sie sich mit ihrer Struktur und ihrem Inhalt beschäftigen, sind sie allerdings durchaus verständlich. Im Grunde genommen wird in diesen Dateien »nur« definiert, was und wo USMT suchen soll, beispielweise Dateien, Registry-Einträge und dergleichen.

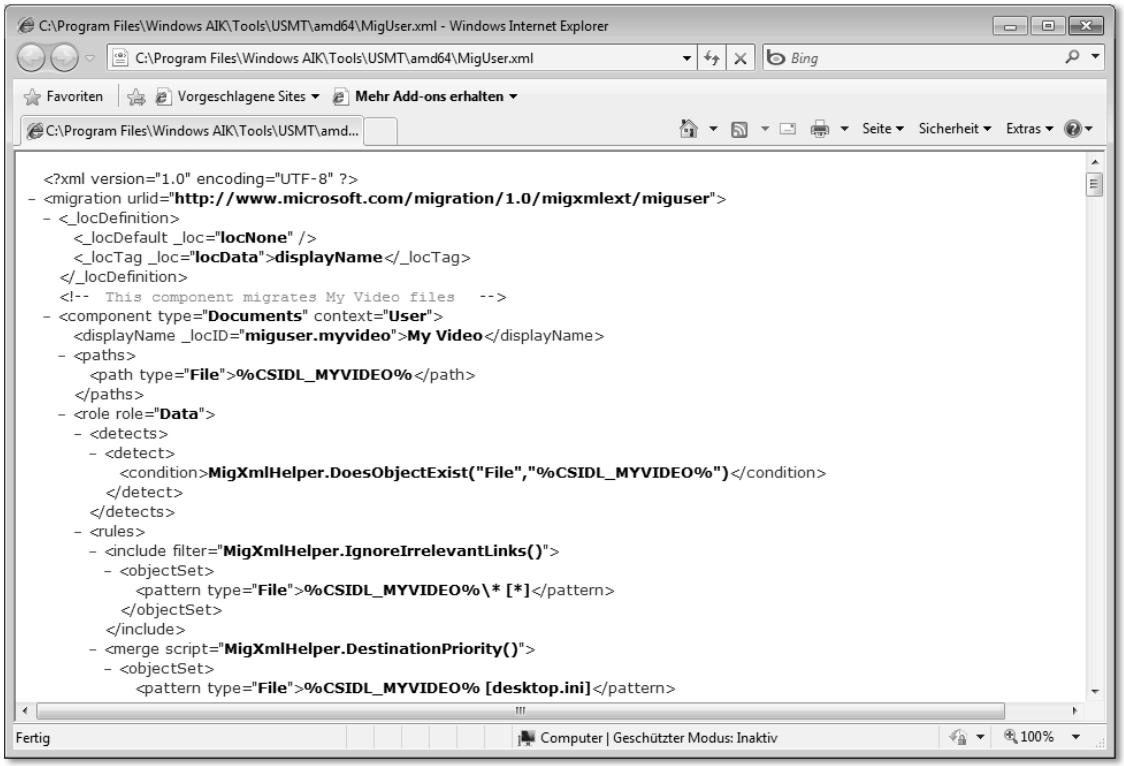


Abbildung 6.135 Ein Ausschnitt aus der Datei »MigUser.xml«

Wenn Sie den Steuerdateien eigene Anweisungen hinzufügen möchten, sollten Sie übrigens nicht die Standarddateien modifizieren, sondern separate Dateien anlegen. Diese werden dann über den Parameter `/i` in den Programmaufruf integriert.

Was kann migriert werden?

Grundsätzlich kann USMT Dateien aller Art und Registry-Einträge migrieren – egal welche. Auf diesem Wege lässt sich grundsätzlich alles migrieren.

Die folgenden Auflistungen zeigen, welche Dateien und Registry-Einträge mit den Standardeinstellungen migriert werden (Quelle: USMT-Dokumentation).

Folgende Benutzerdaten werden, gesteuert durch *MigUser.xml*, migriert:

- Ordner aus den Benutzerprofilen. Darin enthalten sind die Benutzerordner *Dokumente, Videos, Bilder*, die Desktop-Dateien, das Start-Menü, die Schnellstart-Einträge und die Favoriten.

- Ordner von *Alle Benutzer* (*All Users*) und öffentliche Profile
- Folgende Dateitypen werden migriert: *.qdf*, *.qsd*, *.qel*, *.qph*, *.doc*, *.dot*, *.rtf*, *.mcw*, *.wps*, *.scd*, *.wri*, *.wpd*, *.xl**, *.csv*, *.iqy*, *.dqy*, *.oqy*, *.rqy*, *.wk**, *.wq1*, *.slk*, *.dif*, *.ppt**, *.pps**, *.pot**, *.sh3*, *.ch3*, *.pre*, *.ppa*, *.txt*, *.pst*, *.one**, *.mpp*, *.vsd*, *.vl**, *.or6*, *.accdb*, *.mdb*, *.pub*, *.xla*, *.xlb*, *.xls*

Diese Betriebssystemkomponenten werden migriert:

- Einstellungen für erleichterte Bedienung
- Desktop-Oberfläche
- Einstellungen für die Kommandozeile
- Wählverbindungen
- Favoriten
- Ordneroptionen
- Schriften
- Mitgliedschaften in den lokalen Gruppen
- Einstellungen des Internet Explorers (ab Version 6.0)
- ODBC-Einstellungen (*Microsoft Open Database Connectivity*)
- Microsoft Outlook Express-Dateien (**.dbx*)
- Einstellungen für Maus und Tastatur
- Multimedia-Einstellungen
- Telefon- und Modem-Einstellungen
- RAS-Telefonbücher (*.pbk*)
- Regionseinstellungen
- Fernzugriff
- Bildschrimschoner-Einstellungen
- Einstellungen für die Aufgabenleiste
- Hintergrundbilder

Tabelle 6.5 zeigt, welche Anwendungen und Versionen standardmäßig unterstützt werden.

Produkt	Version
Adobe Acrobat Reader	4.0, 6.0, 7.x
Adobe PhotoShop	CS, CS2, CS3

Tabelle 6.5 Einstellungen dieser Anwendungen werden standardmäßig migriert.

Produkt	Version
AOL Instant Messenger	5.9
Apple iTunes	6.0
Apple QuickTime Player	7
Corel Paint Shop Professional	9.0
CuteFTP Professional	6.0, 7.0
Eudora	5, 6, 7
ICQ Pro	2003b
IBM Lotus Notes	6.x, 7.0
IBM Lotus SmartSuite Lotus 1-2-3 Organizer WordPro	9, 9.8
MusicMatch JukeBox Basic	7.x, 8.x, 10.x
Microsoft Windows Media Player	7–9, 11
Microsoft Office Microsoft Access Microsoft Excel Microsoft FrontPage Microsoft Outlook Microsoft PowerPoint Microsoft Publisher Microsoft Word	2000, XP, 2003, 2007*
MSN Messenger	6.1, 7.0, 7.5
Microsoft OneNote	2003, 2007
Microsoft Project	2003, 2007
Microsoft Visio	2003, 2007
Windows Live Messenger	8.0
Microsoft Works	7.0, 8.0
Mozilla Firefox	1.8
Odigo Messenger	4.0
Quicken	2001–2006 *Home* und *Business*
RealPlayer Basic	6.x, 10

Tabelle 6.5 Einstellungen dieser Anwendungen werden standardmäßig migriert. (Forts.)

Produkt	Version
SpyBot – Search & Destroy	1.4
WinAmp	5
WinZip	8.0, 9.0, 10.0
WordPerfect Office	11, 12, X3
WS_FTP Pro	8, 9, 10
Yahoo Messenger	5.x, 6.x, 7.x

Tabelle 6.5 Einstellungen dieser Anwendungen werden standardmäßig migriert. (Forts.)

6.14 Was ist mit »einfach drüberinstallieren«?

Die Betrachtungen des Kapitels gingen immer von einer Neuinstallation von Windows 7 aus. Nun wird es etliche Fälle geben, in denen zwar Windows 7 eingesetzt werden soll, dies aber nicht mit der Beschaffung neuer Hardware einhergeht.

Ich bin, aus reichlicher Erfahrung, kein Anhänger von »einfach drüberinstallieren« oder – etwas technischer gesprochen – von In-Place-Migration. Diese Vorgehensweise lässt zwar vermuten, dass man recht schnell und einfach zu einem Ergebnis kommt, da eine Neuinstallation von Anwendungen nicht notwendig ist und außerdem auch die Profildaten erhalten bleiben. Problematisch ist aber, dass die entstandene Installation eventuell nicht so »sauber« ist wie eine frische Installation. Ich empfehle also generell eine Neuinstallation, auch wenn Sie die Hardware nicht erneuern. Mit Unterstützung durch WDS, WIM-Images und andere Windows 7-Möglichkeiten ist eine Neuinstallation zügig zu erledigen. Wenn die PCs in Ihrem Unternehmen nicht kompliziert einzurichtende Einzelstücke sind, gibt es eigentlich keinen Grund für das »Drüberinstallieren«.

6.15 Weitere Anmerkungen zum Deployment

Über das Deployment von Windows 7 könnte man noch viele weitere Seiten füllen, da es noch fast unbegrenzt viele weitere Facetten gibt. Ich habe in diesem Kapitel stark auf die Nutzung der WDS abgezielt. Windows 7 lässt sich natürlich auch ohne WDS installieren, so könnten Sie auch Windows PE von CD booten und mit *imagex.exe* ein individuelles WIM-Image installieren. Ich denke aber, dass die WDS die Technologie der Wahl sind: Wenn die Administratoren in einem Unternehmen schon so weit sind, eigene WIM-Images anzufertigen, ist die WDS-Nutzung einfach sinnvoll und naheliegend. Gleiches gilt für Unattended-

Dateien: Wenn Sie in der Lage sein wollen, unbeaufsichtigt Installationen durchzuführen, macht es recht wenig Sinn, mit DVDs herumzulaufen. Es gibt natürlich hinreichend Fälle, in denen die WDS-Nutzung nicht sinnvoll möglich ist: Mir fällt spontan ein kleiner Außenstandort ein, in dem man bei einer Installation nicht ein 3 GB großes Installations-Image über die WAN-Verbindung laden kann. Hier macht eine DVD-basierte unbeaufsichtigte Installation natürlich Sinn.

Ich möchte noch darauf hinweisen, dass es theoretisch PCs geben könnte, bei denen ein Booten vom Netzwerk nicht möglich ist. In diesem Fall könnte man eine Windows PE-Boot-CD anfertigen, die dann Kontakt zum WDS-Server aufnimmt. Wie das gemacht wird, ist in der Microsoft-Dokumentation beschrieben. Ich persönlich halte das aber für kein zentrales Thema:

- Wenn der PC so alt ist, dass er nicht aus dem Netz booten kann, ist er vermutlich für Windows 7 ohnehin nicht geeignet.
- Falls der Netzwerkbootvorgang misslingt, weil aufgrund einer Segmentierung des Netzes die DHCP-Kommunikation misslingt, sollten Sie lieber an der Ursache des Problems (der Konfiguration der Netzwerkkomponenten) arbeiten, anstatt auf den Netzwerkbootvorgang zu verzichten.

Von seiner Mutter Parysatis nun wurde Kyros begünstigt, da sie ihn mehr liebte als Artaxerxes, den regierenden König.

7 Aktivierung

Seit Windows XP ist es erforderlich, das Betriebssystem zu aktivieren. Somit ist es wenig überraschend, dass dies auch für Windows 7 zutrifft (Abbildung 7.1). Es ist sicherlich legitim, dass Microsoft etwas gegen nicht lizenzierte Kopien der Software unternimmt. Andererseits ist die Produktaktivierung ein weiteres Thema, mit dem Administratoren und Systemarchitekten sich beschäftigen müssen.

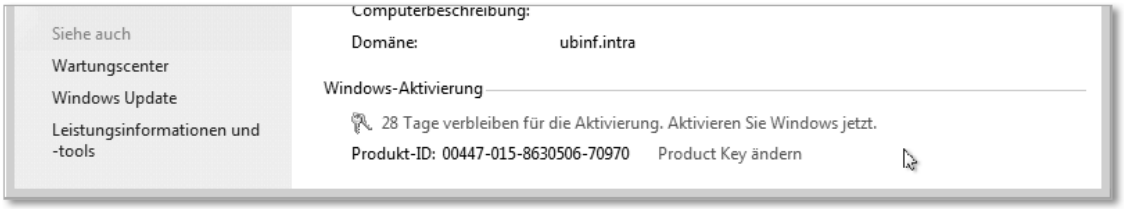


Abbildung 7.1 Auch bei Windows 7 ist die Aktivierung ein wichtiges Thema.

Zu Zeiten von Windows XP war das Leben im Unternehmen noch recht einfach: Sofern Volumenlizenzen eingesetzt worden sind, war keine Aktivierung notwendig. Wenn Unternehmen keine Volumenlizenzen, sondern beispielsweise OEM-Versionen gekauft hatten, mussten sie jeden PC »zu Fuß« aktivieren, aber na ja – sie haben ja vorher gewusst, worauf sie sich mit diesem Lizenztyp eingelassen haben.

Seit Windows Vista müssen auch Volumenlizenzen aktiviert werden, mit anderen Worten: Mit dem Thema müssen Sie sich beschäftigen.

7.1 Lizenztypen und Produkt-Keys

Wer sich mit der Lizenzierung beschäftigt hat, dürfte diese als sehr komplexes Thema kennengelernt haben. Da wir uns in diesem Kapitel aber »nur« mit der Produktaktivierung beschäftigen, wird es nicht ganz so wild. Im Grunde genommen müssen Sie eigentlich nur zwischen zwei simplen Fällen unterscheiden:

- Ihr Unternehmen verwendet Software aus einem der zahlreichen Volumenlizenz-Programme (z. B. Open, Select, EA).
- Ihr Unternehmen nutzt keine Volumenlizenzen, sondern verwendet Retail- oder OEM-Versionen.

Windows 7 vorinstalliert

Vermutlich wird es auch bei Windows 7 PCs mit vorinstalliertem Betriebssystem geben, das bereits aktiviert ist. Insbesondere die Systeme der großen Hersteller wie Dell oder HP dürften so ausgeliefert werden.

Wenn Sie sich für die Volumenlizenzierung entschieden haben, geht die Arbeit übrigens erst richtig los: Die Wahl der optimalen Lizenzierung ist komplex. Es gibt hochbezahlte Berater, die nichts anderes tun, als sich um die Auswahl der besten Lizenzierungsform zu kümmern. In diesem Buch werde ich mich nicht weiter mit den Theorien des Lizenzrechts befassen. Ich möchte Ihnen als erste Anlaufstelle den entsprechenden Bereich der Microsoft-Website empfehlen: *http://www.microsoft.com/licensing/default.aspx*.

Sie werden vermutlich feststellen, dass die Volumenlizenzen nicht unbedingt die preisgünstigsten sind. Selbst wenn Sie *Select* in der höchsten Stufe kaufen können, werden vermutlich OEM-Versionen (die auch unter dem Stichwort *System-Builder-Lizenzen* bekannt sind) rein vom Anschaffungspreis her günstiger sein. Allerdings: Die Volumenlizenzversionen bieten andere Vorteile, die durchaus die höheren Kosten rechtfertigen – und zwar insbesondere beim Lizenzmanagement.

Bei der Nutzung von Volumenlizenzen gibt es zwei Typen von Keys, die unterschiedliche Aktivierungen erfordern:

- *MAK* (*Multiple Activation Key*): Diese entsprechen in etwa den Volumenlizenz-Keys von Windows XP: Ist die Aktivierung einmal erfolgt, gilt diese sozusagen für ewig, zumindest solange es keine wesentlichen Änderungen bei der Hardware gibt.
  Die Aktivierung erfolgt in direkter Kommunikation mit Microsoft.
- *KMS* (*Key Management System*): Dieser Key-Typ wurde im Rahmen der *Volume Activation 2.0*, also mit *Vista* und *Windows Server 2008*, eingeführt. Vereinfacht gesagt besteht die Idee darin, dass ein eigener Aktivierungsserver in Ihrem Netz installiert wird und dieser die Aktivierungsvorgänge mit den Clients abwickelt. Dieser Server kommuniziert regelmäßig mit Microsoft. Im Gegensatz zur Aktivierung mit MAKs wird bei diesem Verfahren mindestens alle 180 Tage die Aktivierung wiederholt.

Nicht verwechseln

Es ist wichtig, dass Sie MAK- und KMS-Keys nicht verwechseln. Wenn es doch passiert, ist das zwar kein Drama, führt aber unter Umständen zu weniger erwünschten »Effekten«. Mehr dazu folgt im Verlauf des Kapitels (Abschnitt 7.5.3, »Achtung!«).

7.2 Volume Activation 2.0

Wenn Sie sich mit dem Aktivieren von Volumenlizenzen von Windows 7, Windows Vista und Windows Server 2008 beschäftigen, werden Sie eher früher als später auf das Stichwort *Volume Activation 2.0* stoßen.

Unter diesem Titel sind im Grunde genommen die Konzepte für die Aktivierung zusammengefasst. Hierzu gehören beispielsweise die Aktivierungskonzepte MAK und KMS, die Definitionen über Ablaufdaten oder auch Konzepte und Planungshinweise, wie man richtig mit der Aktivierung umgeht bzw. umgehen soll.

Es gibt natürlich auch eine Technet-Website zum Thema Volumenaktivierung, und zwar unter *http://technet.microsoft.com/en-us/windows/dd197314.aspx*.

7.2.1 Produktgruppen

Bei der Volumenaktivierung gibt es vier Produktgruppen, nämlich:

- Clients: Dort sind Windows 7 und Vista enthalten, und zwar in den Editionen *Business* und *Enterprise*.
- Produktgruppe A: Windows Web Server 2008
- Produktgruppe B: Windows Server 2008, *Standard*- und *Enterprise*-Edition
- Produktgruppe C: Windows Server 2008 Datacenter und Windows Server 2008 für Itanium-Prozessoren

Volumenlizenzkunden erhalten im Normalfall einen KMS-Key und einen MAK-Key pro Produktgruppe – vorausgesetzt, es sind überhaupt Lizenzen für die entsprechende Gruppe im Volumenlizenzvertrag enthalten.

Nur im Key

Es ist durchaus denkbar, dass beispielsweise im Volumenlizenz-Portal kein MAK-Key für eine bestimmte Produktgruppe enthalten ist. Dieser sollte sich dann aber über eine Funktion im Volumenlizenzportal anfordern lassen.

Auch wenn Sie 2.500 Server der Gruppe B und 45.000 Clients per Volumenlizenzprogramm erworben haben, erhalten Sie »nur« einen KMS- und einen MAK-Key. Diese unterstützen eine hinreichend häufige Aktivierung – Sie brauchen also für Ihre 45 000 Windows 7-Lizenzen nicht 45 000 Keys zu verwalten. Bei OEM- oder Retail-Lizenzen wäre genau das der Fall.

Abbildung 7.2 zeigt die Produktgruppen in einer hierarchischen Anordnung. Diese Darstellung sollten Sie sich ruhig merken, insbesondere wenn Sie mit KMS arbeiten möchten. Der Grund ist, dass ein KMS-Host auf Basis von Windows 7 nur Windows 7-Clients aktivieren kann. Basiert der KMS-Host aber beispielsweise auf einem Gruppe-B-Betriebssystem (Windows Server 2008 Standard oder Enterprise), kann er Betriebssysteme seiner und der darunter angesiedelten Produktgruppen aktivieren. Ich werde in Abschnitt 7.5 nochmals genauer darauf eingehen – aber eigentlich ist es nicht so kompliziert. Wenn Sie sich die Produktgruppen von vornherein in dieser Pyramidendarstellung merken, haben Sie schon das wichtigste Wissen im Kopf.

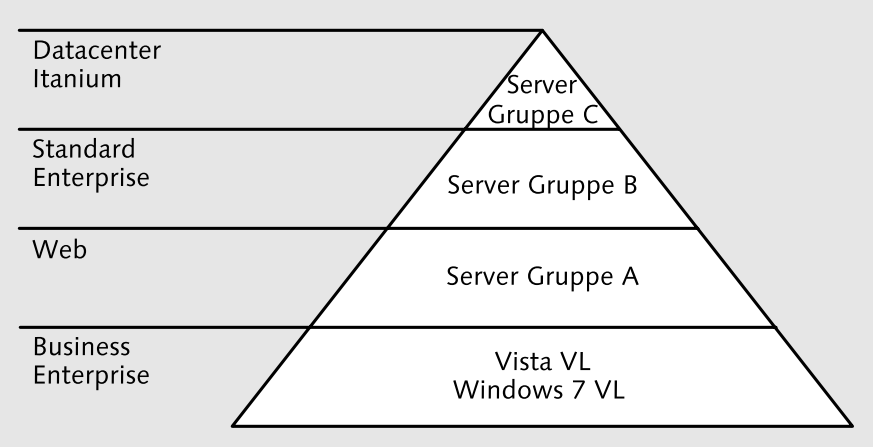


Abbildung 7.2 Die unterschiedlichen Gruppen in »Volume Activation 2.0«

7.2.2 Zeitfenster und Toleranzperioden

Eine wesentliche Frage bei der Aktivierung ist, wann diese erfolgen muss, damit der Benutzer nicht mit Meldungen über eine fehlende Aktivierung und dergleichen behelligt wird.

Zunächst müssen Sie einige Begriffe lernen:

- *Grace Period* (Toleranzperiode): Das ist die Zeitspanne, die das Betriebssystem ohne Einschränkung arbeitet, obwohl es nicht aktiviert ist.
- *OOB* (*Out of Box*): Dieser Begriff findet sich in den Microsoft-Unterlagen als Zustand, den das Betriebssystem direkt nach der Installation hat (also: »gerade aus der Verpackung genommen«, d. h. neu).

- *OOT* (*Out of Tolerance*): Die Situation, dass Windows OOT ist, ergibt sich, wenn es signifikante Hardwareänderungen gibt.

Wenn Sie ein Betriebssystem nicht aktivieren, ergibt sich die in Abbildung 7.3 dargestellte Verhaltensweise:

- Nach der Installation haben Sie zunächst 30 Tage Zeit, um eine Aktivierung durchzuführen. Die Zeitangabe 30 Tage gilt für Windows 7 und Vista. Beim Windows Server 2008 sind es 60 Tage.
- Ist nach 30 Tagen die Aktivierung nicht erfolgt, können Sie ein *Rearm* durchführen, das unter anderen dem Zähler für die Aktivierung zurücksetzt. Ein Rearm kann dreimal durchgeführt werden. Daraus ergibt sich, dass man die Aktivierung 120 Tage hinauszögern kann. Danach erscheinen verschiedene Benachrichtigungen.

Rearm

Das Rearm wird mittels des Kommandozeilenaufrufs `slmgr -rearm` durchgeführt.

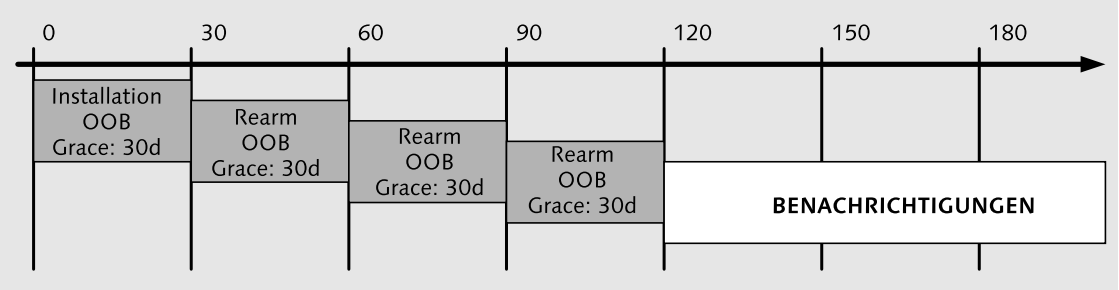


Abbildung 7.3 Wenn Sie Windows 7 (oder Vista) installiert haben, haben Sie 30 Tage für die Aktivierung Zeit. Danach kann dreimal ein Rearm durchgeführt werden.

Aktivierung mit MAK-Key

Die zeitlichen Einflüsse der Aktivierung mit einem MAK-Key sind vergleichsweise simpel (Abbildung 7.4):

- Nach der Installation befindet sich das System zunächst in der 30-tägigen *Grace Period*, während der die Aktivierung mit dem MAK-Key jederzeit erfolgen kann. Gegebenenfalls kann ein Rearm durchgeführt werden, um den Zeitpunkt hinauszuschieben, zu dem es Benachrichtigungen wegen nicht erfolgter Aktivierung gibt.
- Ist die Aktivierung erfolgt, läuft der Status niemals ab.

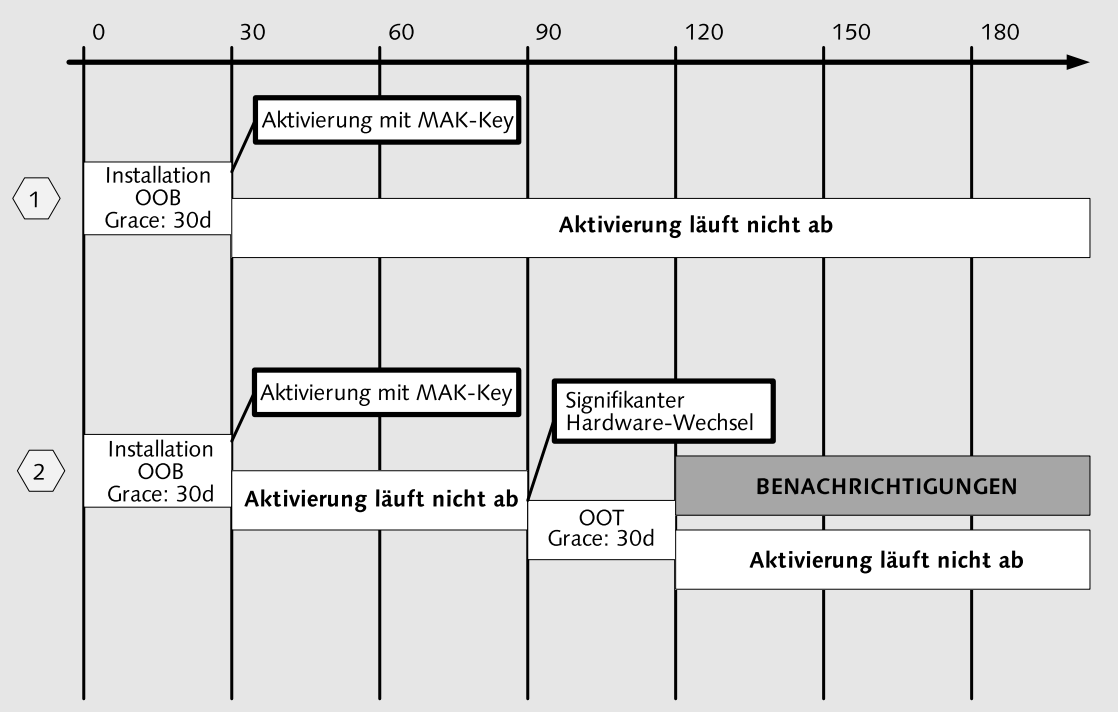


Abbildung 7.4 Die Aktivierung mit einem MAK-Key

Es gibt allerdings einen Fall, in dem die Aktivierung ungültig wird und wiederholt werden muss (Abbildung 7.4, Fall 2). Sofern es signifikante Hardwareänderungen gibt, ist eine nochmalige Aktivierung erforderlich; eine signifikante Änderung ist beispielsweise der Wechsel des Prozessortyps. In diesem Fall läuft das System in eine 30-tägige *Grace Period*, die nicht verlängert werden kann. Man spricht hier übrigens auch von *OOT-Grace* (OOT = Out of Tolerance). Erfolgt eine Aktivierung, gilt diese wiederum unbegrenzt mit der bereits bekannten Ausnahme der signifikanten Hardwareänderung.

Grace Period

Wie zuvor beschrieben, beträgt die OOB-*Grace Period* (also bei Neuinstallation) bei Windows 7 und Vista 30 Tage, beim Windows Server 2008 sind es 60 Tage.

Die Länge der OOT-*Grace Period* beträgt bei den Servern ebenfalls nur 30 Tage.

Aktivierung mit KMS

Das zeitliche Verhalten bei der Nutzung von KMS ist ein wenig komplizierter, wie auf Abbildung 7.5 zu erkennen ist:

- *Fall 1*: Zunächst wird mit dem KMS-Key der KMS-Host aktiviert. Dies funktioniert letztendlich genauso wie eine Aktivierung mittels MAK-Key. Insbesondere ist zu nennen, dass die Aktivierung nicht abläuft.

- *Fall 2*: Nach einer Neuinstallation läuft das System zunächst innerhalb der OOB-*Grace Period*. Sofern der KMS-Client keinen KMS-Host finden kann und somit keine Aktivierung durchgeführt werden kann, werden entsprechende Benachrichtigungen angezeigt. Ist die Aktivierung hingegen erfolgreich, ist diese für 180 Tage gültig. Standardmäßig wird alle sieben Tage versucht, die Aktivierung zu aktualisieren.
- *Fall 3*: Wenn die Aktivierung 180 Tage lang nicht erneuert werden kann, geht das System in die OOT-*Grace Period* (30 Tage) über. Ist eine Aktivierung nicht möglich, werden die Benachrichtigungen angezeigt.
- *Fall 4*: Wenn während des Gültigkeitszeitraums der Aktivierung signifikante Hardwareänderungen durchgeführt werden, geht das System in die OOT-*Grace Period* (30 Tage) über. Es wird direkt versuchen, Kontant zum KMS-Host aufzunehmen, um die Aktivierung zu erneuern. Ist dies innerhalb der *Grace Period* nicht möglich, werden die Benachrichtigungen angezeigt.

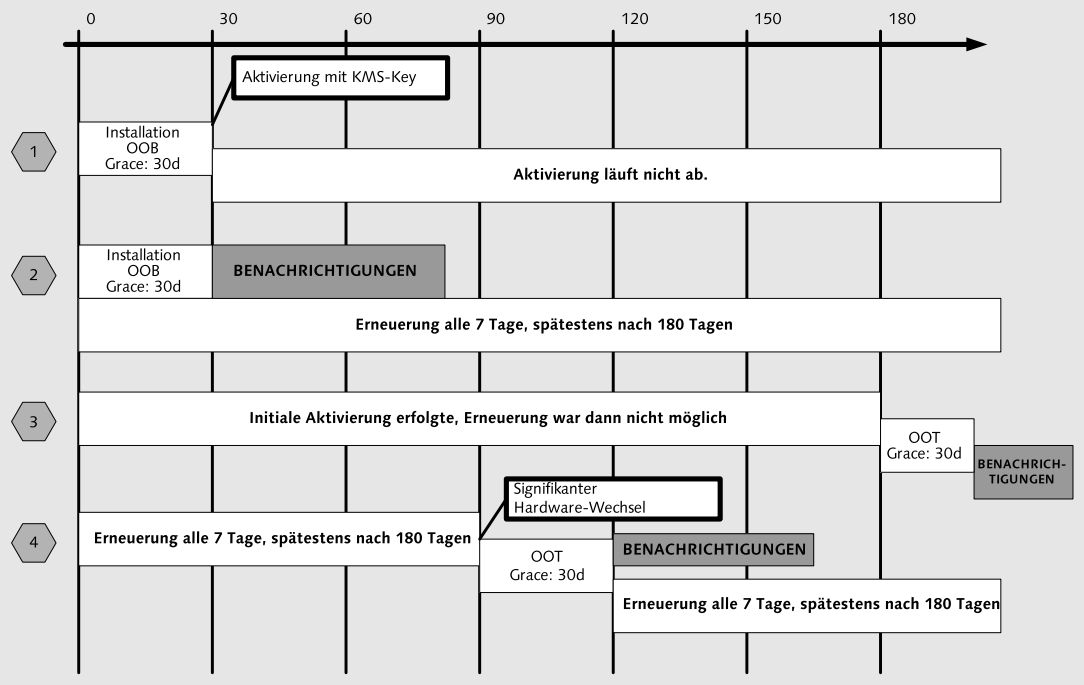


Abbildung 7.5 Die KMS-Aktivierung

7.2.3 RFM – Reduced Functionality Mode

Im vorigen Abschnitt war immer die Rede davon, dass es »Benachrichtigungen« geben wird, wenn das Betriebssystem nicht rechtzeitig aktiviert wird. Vielleicht haben Sie aus Windows XP/2003-Zeiten oder von Vista vor SP1 noch in Erinnerung, dass das Betriebssystem deutlich »massiver« wird, wenn keine Aktivierung erfolgt: Auf Abbildung 7.6 sehen Sie beispielsweise die Reaktion eines nicht aktivierten Windows Server 2003, der schlicht und ergreifend die Benutzeranmeldung verweigert.

In Umgebungen, die nur einen sehr reduzierten Zugang zum Internet haben, kann das unter Umständen schon recht unangenehm werden, weil dann nur noch die telefonische Aktivierung bleibt – machbar, aber mühsam. Da keine Anmeldung am System möglich ist, ist dann auch keine Anpassung der IP-Adressen möglich und dergleichen.

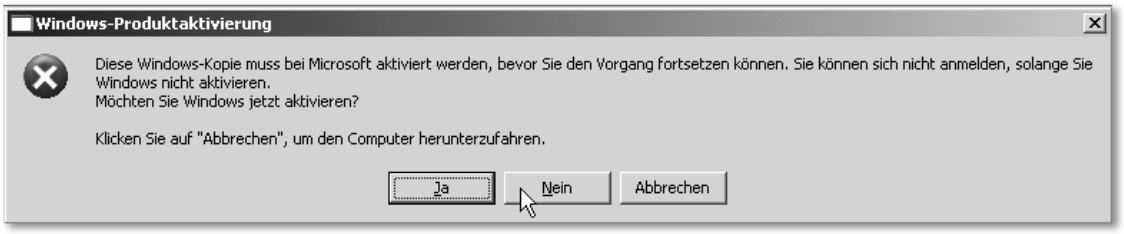


Abbildung 7.6 Windows war früher ziemlich aggressiv, wenn die Aktivierung überfällig war (hier: Windows Server 2003).

Seit Windows Server 2008 und Vista SP1 (und somit auch bei Windows 7) ist das Verhalten der Betriebssysteme deutlich »zahmer« geworden. Befindet sich das Betriebssystem außerhalb der *Grace Period*, gibt es folgende Verhaltensweisen:

- Bei der Anmeldung erfolgt die Aufforderung zur Aktivierung. Das System legt eine halbe Gedenkminute ein, durch Klick auf SPÄTER AKTIVIEREN kann man sich aber auch ohne Aktivierung anmelden (Abbildung 7.7).
- Der Desktophintergrund wird schwarz und auch der angemeldete Benutzer sieht hin und wieder Hinweise (Abbildung 7.8).
- *Windows Update* installiert keine Updates mehr, die mit der Bemerkung *Nur Originalsoftware* gekennzeichnet sind – kurz gesagt werden nur noch als kritisch eingestufte Updates installiert.

Dieser Benachrichtigungsmodus ist durchaus lästig für die Anwender, allerdings schlittert man bei Problemen bei der Aktivierung nicht direkt in die totale Katastrophe. Dies ist meines Erachtens auch eine wichtige Information für Administratoren, die KMS einführen wollen und sich eben fragen, was passiert, wenn der KMS-Host unbemerkt offline geht. Schließlich muss die Aktivierung jedes einzelnen Clients spätestens nach 180 Tagen erneuert werden.

Der erste Teil der Antwort ist, dass die Verwendung eines geeigneten Überwachungswerkzeugs (am besten des *System Center Operations Manager 2007*) beim Ausfall der KMS-Host-Komponente warnen kann. Der zweite Teil der Antwort ist, dass es zwar einigermaßen lästig und super-peinlich wäre, wenn Dutzende oder Hunderte Clients in den Benachrichtigungsmodus wechseln (u. a. auch wegen solcher Wörter wie *Softwarefälschung*, siehe Abbildung 7.8), immerhin führt das aber nicht zum kompletten Stillstand des Unternehmens.

Abbildung 7.7 Ist das System außerhalb des zeitlichen Toleranzbereichs nicht aktiviert, muss man zwar eine halbe Gedenkminute einlegen, kann die Anmeldung aber fortsetzen.

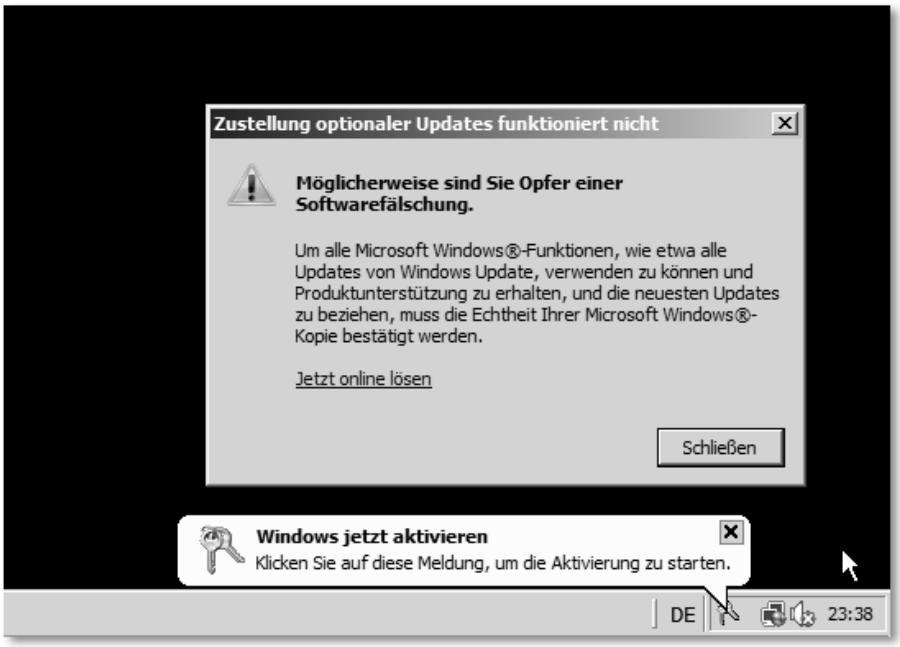


Abbildung 7.8 Der Bildschirmhintergrund wird schwarz, und Benachrichtigungen werden eingeblendet (hier im Bild ein Windows Server 2008).

7.3 VAMT

Da ein Administrator leicht den Überblick über die Aktivierungsstatus der Maschinen verlieren kann, gibt es von Microsoft ein wenig »Utility-Support« für die Erledigung dieser Aufgabe. Das Werkzeug trägt den etwas sperrigen Namen *Volume Activation Management Tool* und ist im Download Center kostenlos erhältlich (Suchbegriff: VAMT).

VAMT ermittelt zunächst eine Liste der Computer im Active Directory und prüft dann per direkter Kommunikation deren Aktivierungsstatus. Neben der AD-Ermittlung lassen sich auch gezielt IP-Adressen oder Namen angeben, auch die Ermittlung in einer Workgroup ist möglich.

Das Ergebnis der Bemühungen von VAMT in einem Teilbereich meiner Testumgebung ist auf Abbildung 7.9 zu sehen. Sie erkennen die verschiedenen Aktivierungsstatus:

- Es gibt MAK-Clients, die aktiviert sind.
- Es gibt KMS-Clients, die innerhalb der OOB GRACE (also installiert, noch nicht aktiviert, aber innerhalb der Toleranz) sind.
- Es finden sich sowohl MAK- als auch KMS-Clients, deren Status NOTIFICATION ist, d. h., sie sind außerhalb der Grace Period.

Vordergründig funktioniert die Testumgebung, bei genauerem Hinschauen mit VAMT zeigen sich aber diverse Probleme, die behoben werden müssen. Angenehmerweise gibt es verschiedene Ansichten, sodass Sie sich per Mausklick zum Beispiel alle Maschinen anzeigen lassen können, die in der INITIAL OUT-OF-BOX (OOB) GRACE sind. Auf diese Weise lassen sich auch größere Mengen von Systemen einigermaßen übersichtlich darstellen.

Daten abspeichern

Beachten Sie, dass der eigentliche Ermittlungsvorgang relativ lange dauert: Immerhin wird jeder Computer direkt angesprochen. Daher empfiehlt es sich, die ermittelten Daten abzuspeichern (FILE • SAVE) und beim neuen Start von VAMT zu öffnen.

Ein gezieltes Refresh einzelner Computer oder ganzer Gruppen ist möglich.

VAMT kann allerdings nicht »nur« anzeigen, sondern auch Aktionen ausführen, insbesondere sei die MAK-Aktivierung (INDEPENDENT und PROXY) zu nennen (Abbildung 7.10). Diese führe ich Ihnen ein wenig später in Abschnitt 7.4, »MAK – Multiple Activation Key«, vor.

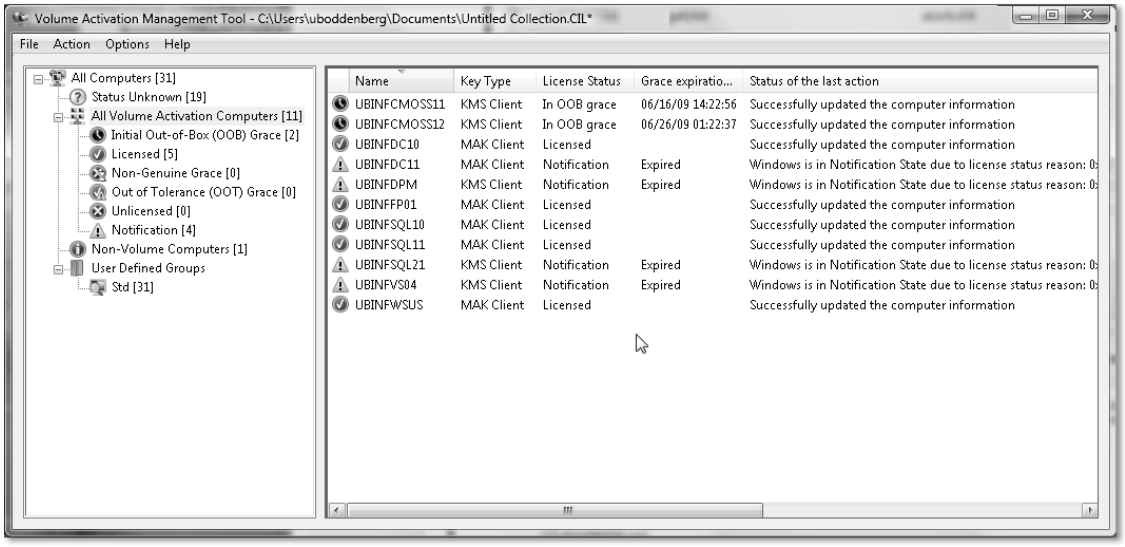


Abbildung 7.9 Mit VAMT lassen sich die Aktivierungsstatus der Systeme relativ leicht ermitteln.

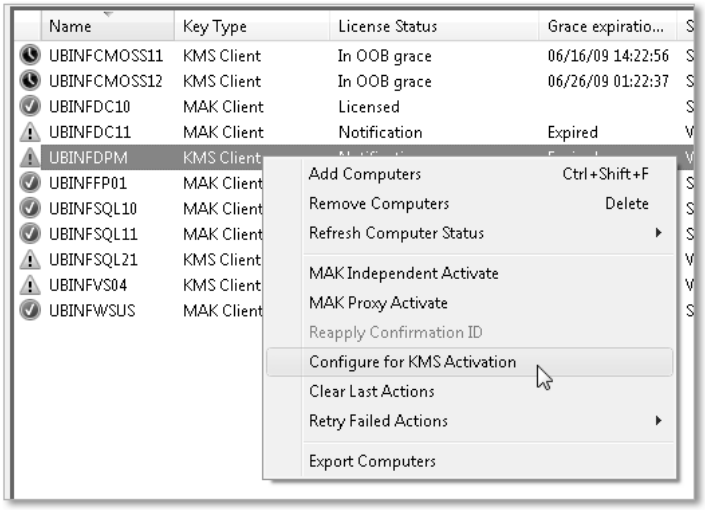


Abbildung 7.10 In den Eigenschaften der gefundenen Computer finden sich auch einige Aktivitäten.

7.3.1 Clients konfigurieren

Wie bereits erwähnt, kommuniziert VAMT direkt mit den Systemen, seien es Windows 7- bzw. Vista- oder Windows-Server-2008-Systeme. Ein Server ist im Allgemeinen auf die Kontaktaufnahme von Clients eingestellt, ein typisches Clientsystem ist dies aber nicht. Die Windows-Firewall verhindert derlei Zugriffe, was ja grundsätzlich auch zu begrüßen ist. Das Ergebnis ist aber, dass VAMT keinerlei Informationen über die Clients ermitteln kann, wobei es gerade da besonders wichtig wäre.

Es ist natürlich nicht notwendig, die Windows-Firewall zu deaktivieren, allerdings müssen Sie ein kleines Loch in die Firewalls bohren. So wird's gemacht:

- Rufen Sie die Systemsteuerung auf.
- Wechseln Sie zu System und Sicherheit.
- Dort findet sich der Abschnitt Windows-Firewall. Dort wählen Sie den Menüpunkt Programm über die Windows-Firewall kommunizieren lassen (Abbildung 7.11).

Abbildung 7.11 Damit VAMT mit einem System kommunizieren kann, muss eingehende WMI-Kommunikation auf der Windows-Firewall freigeschaltet werden.

- In dem dann erscheinenden Dialog selektieren Sie Windows-Verwaltungsinstrumentation (WMI). Im Normalfall sollte es genügen, wenn Sie das Profil Domäne zulassen (Abbildung 7.12).

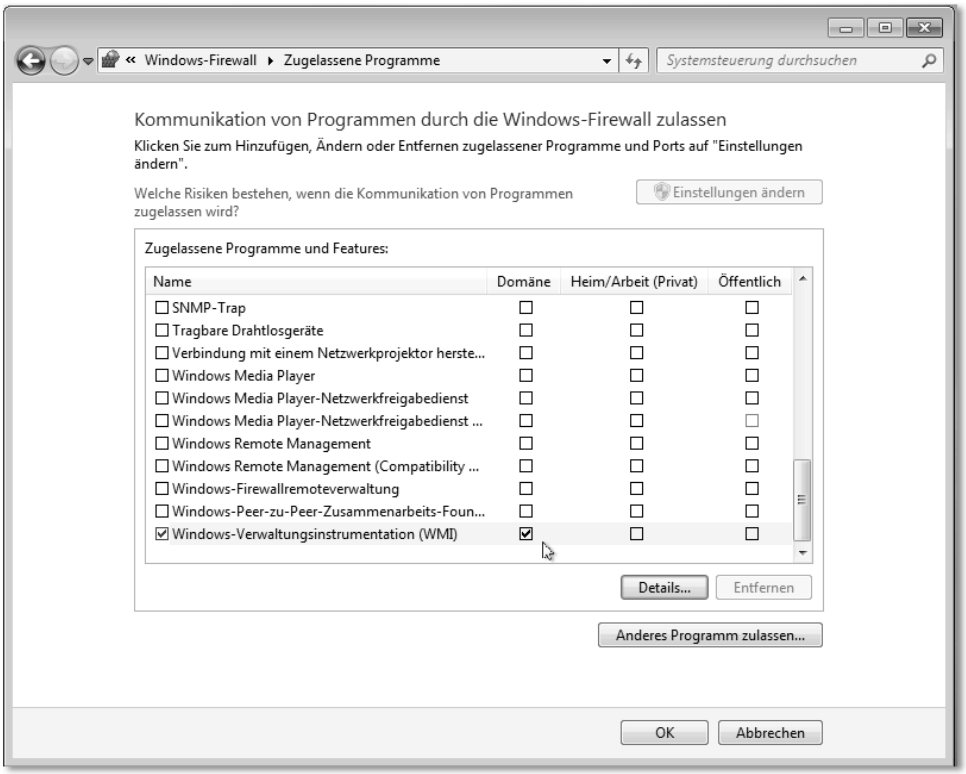


Abbildung 7.12 »Windows-Verwaltungsinstrumentation (WMI)« muss zugelassen werden.

Konfiguration über Gruppenrichtlinien

Nun brauchen Sie natürlich nicht zu fürchten, dass Sie zu jedem PC laufen müssen, um dort ein Loch in die Firewall zu bohren. Die Windows-Firewall ist über Gruppenrichtlinien konfigurierbar; Abbildung 7.13 hilft Ihnen beim Suchen.

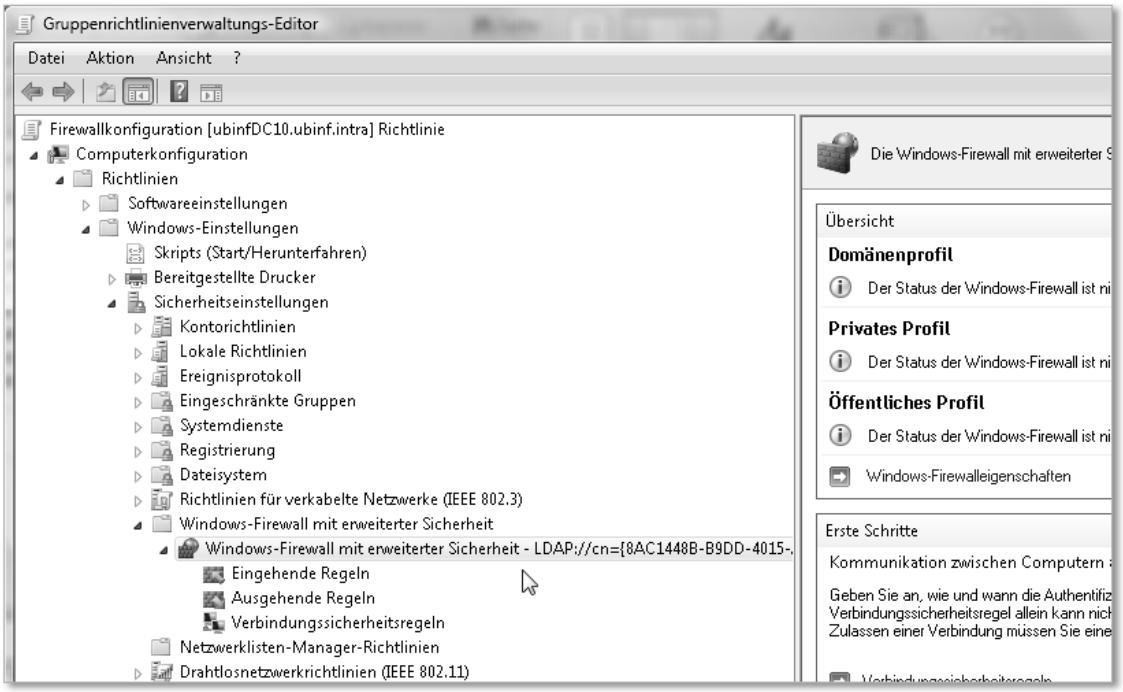


Abbildung 7.13 Die Windows-Firewall kann über Gruppenrichtlinien konfiguriert werden.

Mehr zur Konfiguration

Die Konfiguration mit Gruppenrichtlinien wird sehr ausführlich in Kapitel 11 behandelt.

7.3.2 MAK-Keys verwalten

Eine interessante Funktion von VAMT ist die Möglichkeit, MAK-Keys zu verwalten. So richtig Sinn macht das natürlich mit der später gezeigten Möglichkeit, mittels VAMT die Aktivierung vorzunehmen bzw. zu initiieren. Wählen Sie den Menüpunkt Action • Manage MAKs. Sie gelangen dann zu dem Dialog aus Abbildung 7.14. Ein recht angenehmes Feature ist übrigens, dass Sie VAMT ermitteln lassen können, wie viele Aktivierungsvorgänge mit dem jeweiligen MAK-Key noch ausgeführt werden können (Remaining Activations).

Bei ?????????? mit der Aktivierung

Falls Sie mit einem MAK-Key keine Aktivierungen mehr durchführen können, hilft ein Anruf bei Microsoft. Dort können weitere Aktivierungen für den MAK-Key freigeschaltet werden. Da die Anzahl der möglichen Aktivierungsvorgänge aber stets zu Ihrem Lizenzvertrag passt, sollte das normalerweise nicht notwendig sein.

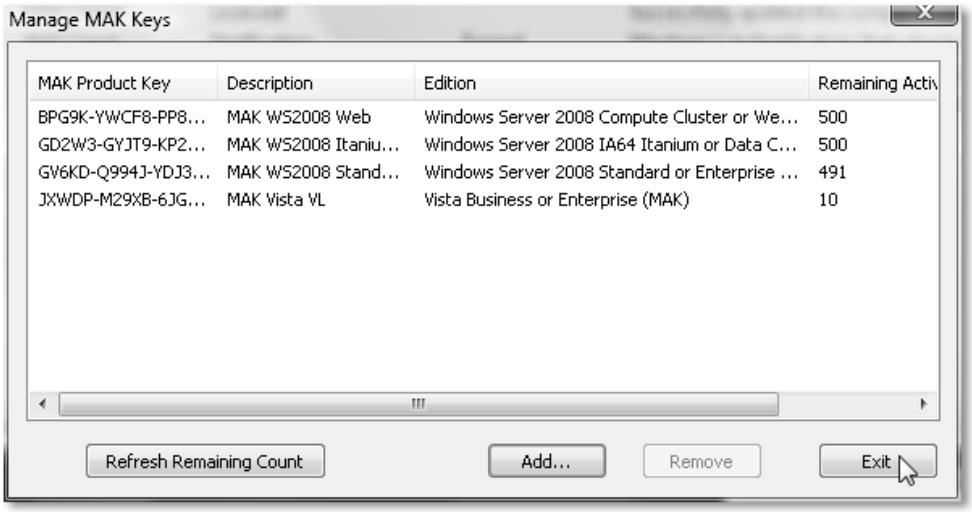


Abbildung 7.14 Bei der Verwaltung der MAK-Keys lässt sich auch die Anzahl der verbleibenden Aktivierungen ermitteln.

Das Hinzufügen eines MAK-Keys ist auf Abbildung 7.15 gezeigt. Wenn Sie auf die Schaltfläche VALIDATE klicken, wird eine Verbindung zu Microsoft aufgebaut. Beim Überprüfen der Gültigkeit wird auch der MAK EDITION TYPE ermittelt.

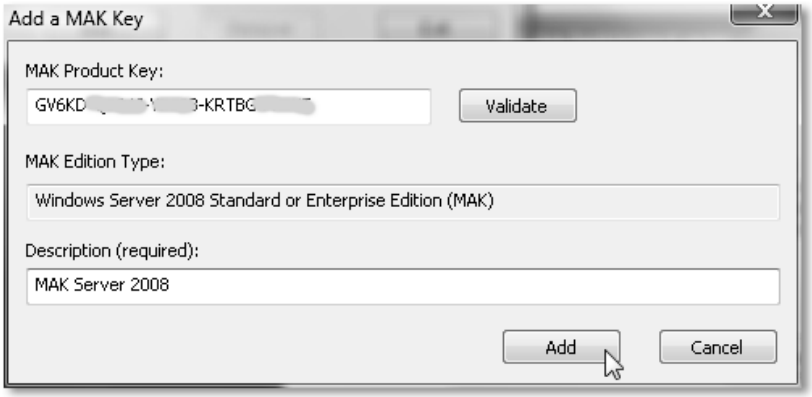


Abbildung 7.15 So geben Sie einen weiteren MAK-Key ein.

Daten abspeichern

Damit die hier eingegebenen MAK-Keys auch beim nächsten Starten von VAMT vorhanden sind, müssen Sie über den Menüpunkt FILE • SAVE die aktuellen Daten speichern und beim nächsten Start wieder laden.

7.4 MAK – Multiple Activation Key

Die simpelste Möglichkeit, Volumenlizenzen zu aktivieren, ist die Verwendung eines MAK-Keys. Der Name (*Multiple Activation Key*) beschreibt ziemlich eindeutig das Konzept: Mit einem MAK-Key können Sie sämtliche Betriebssysteme einer Produktgruppe, also beispielsweise alle Windows 7-Systeme oder alle Windows-Server-2008-Systeme aktivieren. Um die Aktivierung durchzuführen, gibt es diese Möglichkeiten:

- Sie melden sich an dem zu aktivierenden System an und initiieren dort die Aktivierung. Dies kann über die grafische Oberfläche oder per Kommandozeile geschehen. Hierbei gibt es wiederum zwei Möglichkeiten:
  - Die Aktivierung wird über das Internet durchgeführt.
  - Die Aktivierung wird telefonisch erledigt.
- Sie initiieren die Aktivierung mit VAMT, und der Computer wickelt den notwendigen Datenaustausch mit dem Microsoft Activation Service ab (*MAK Independent Activate*).
- Sie initiieren die Aktivierung mit VAMT, und der VAMT-Computer wickelt den notwendigen Datenaustausch mit dem Microsoft Activation Service ab (*MAK Proxy Activate*).

7.4.1 Aktivieren am PC

Der einfachste Fall, der in diesem Buch mehr oder weniger nur der Vollständigkeit halber erwähnt wird, ist die Aktivierung direkt am PC mittels der grafischen Oberfläche. Abbildung 7.16 zeigt, wie das gemacht wird.

DNS-Name nicht vorhanden

Obwohl alles ganz simpel aussieht, kann folgendes Problem auftreten: Eventuell erhalten Sie eine Fehlermeldung, in der Ihnen sinngemäß mitgeteilt wird, dass der DNS-Name nicht vorhanden sei.

Das Problem tritt im Allgemeinen dann auf, wenn Sie von einem Volumenlizenzdatenträger installieren, aber keinen KMS-Host installiert und im DNS registriert haben (siehe auch die Ausführungen in Abschnitt 7.5, »KMS – Key Management Service«).

Wenn Sie ein von einem Volumenlizenzdatenträger installiertes Betriebssystem aktivieren möchten, müssen Sie also zunächst Ihren MAK-Key eintragen.

Alternativ gibt es auch die Möglichkeit, mit der Kommandozeile zu arbeiten. Hierzu steht das Script *slmgr.vbs* zur Verfügung, das sich in *c:\windows\system32* befindet. Wenn Sie es ohne Parameter aufrufen, werden die möglichen Optionen angezeigt (Abbildung 7.17).

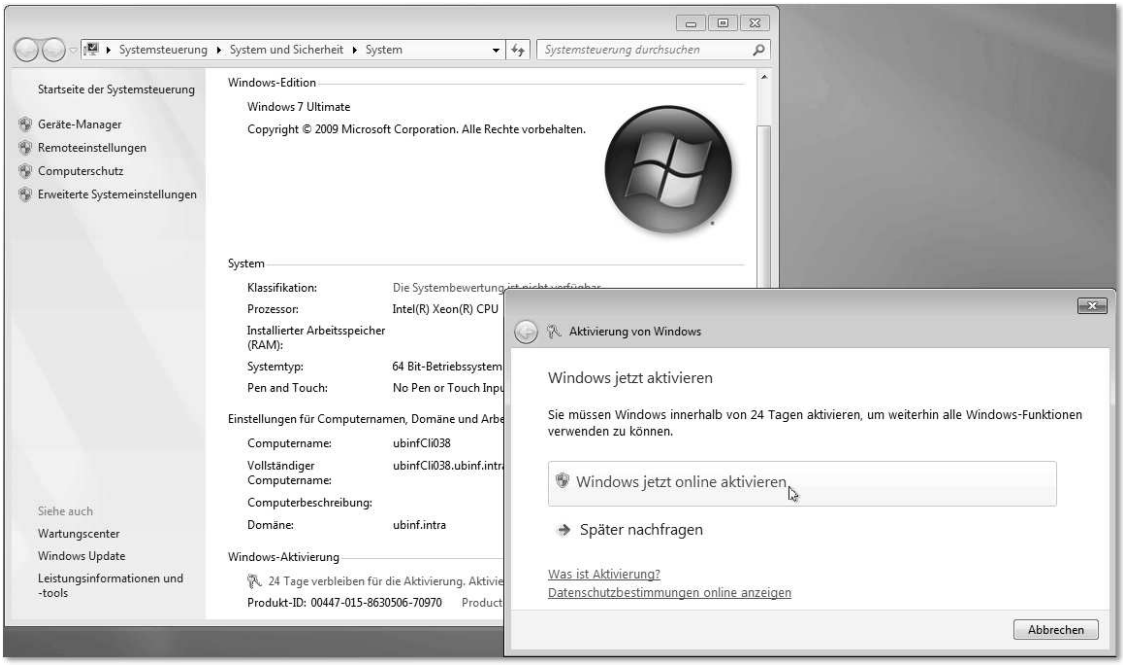


Abbildung 7.16 Sie können die Aktivierung natürlich über die grafische Benutzeroberfläche durchführen.

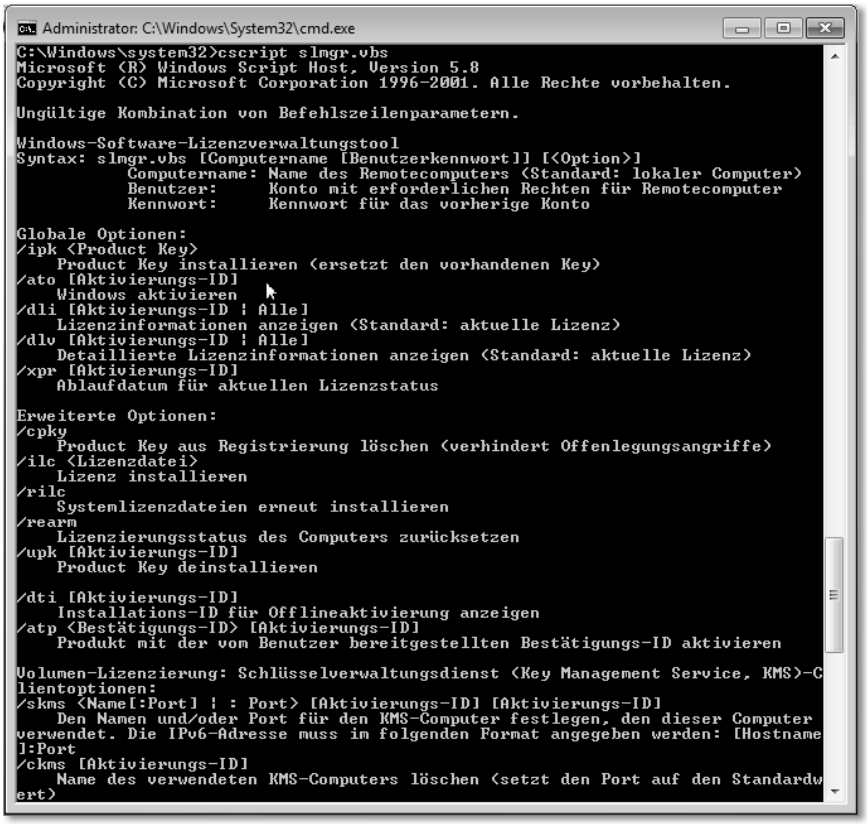


Abbildung 7.17 Alternativ können Sie die Aktivierung auch per Kommandozeile vornehmen.

Die wichtigsten sind:

- `/ipk`: Installiert einen neuen Key. Das wird benötigt, wenn Sie ein vom Volumenlizenzdatenträger installiertes Betriebssystem mit einem MAK-Key aktivieren wollen (siehe vorheriger Kasten).
- `/ato`: Aktiviert das Betriebssystem.

Sie könnten nun natürlich auf die Idee kommen, selbst ein Aktivierungsskript zu entwickeln, das beispielsweise als Teil des Login-Skripts abgearbeitet wird. Sie könnten mit `/dli` den Status abfragen und die Rückgabe auswerten. Sofern das Betriebssystem nicht aktiviert ist, würden Sie dann mittels `/ipk` den MAK-Key eintragen und die Aktivierung durch Aufruf der `/ato`-Option durchführen.

Ja, das ginge! Aber bevor Sie sich solche Mühe machen, wäre der wesentlich bessere Weg, über KMS nachzudenken (siehe Abschnitt 7.5, »KMS – Key Management Service«).

7.4.2 VAMT – MAK Independent Activate

MAK Independent Activate hört sich zwar hochwichtig und hochkompliziert an, ist aber im Grunde genommen eine recht simple Funktion:

- VAMT kann einen neuen MAK-Key auf das System bringen.
- VAMT kann die Aktivierung veranlassen.

Wenn Sie den entsprechenden Menüpunkt im Kontextmenü eines Computers oder einer Gruppe auswählen, erscheint zunächst der Dialog aus Abbildung 7.18:

- Wählen Sie aus, ob ein MAK-Key installiert werden soll. Wenn VAMT dies erledigen soll, muss ein passender (Produktgruppe) MAK-Key hinterlegt worden sein (siehe auch Abschnitt 7.3.2, »MAK-Keys verwalten«).
- Die zweite Einstellung legt fest, ob die Aktivierung vorgenommen werden soll, was mit der Option Activate Now gesteuert wird.

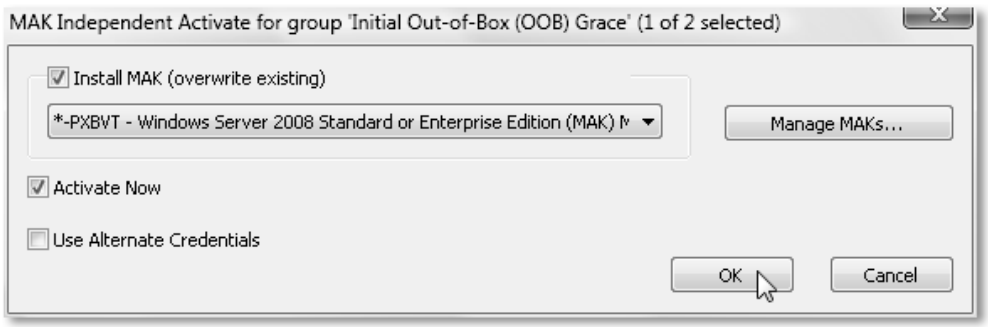


Abbildung 7.18 Sie können auswählen, ob ein MAK-Key installiert werden soll und/oder die Aktivierung durchgeführt werden soll.

Zum Verständnis der Aktivierungsfunktion sei gesagt, dass VAMT das zu aktivierende System anweist, den Vorgang auszuführen. Das Zielsystem beginnt also den Kommunikationsvorgang mit Microsoft, während VAMT »nur« steuert.

Sofern Sie die den Austausch des MAK-Keys gewählt haben, wird es noch die auf Abbildung 7.19 gezeigte Warnmeldung geben, die vor dem *Reduced Functionality Mode* (RFM) warnt. Wie im gleichnamigen Abschnitt 7.2.3 beschrieben wurde, brauchen Sie diesen Modus aber nicht so sehr zu fürchten, denn seit Vista SP1 gibt es »nur« Benachrichtigungen. Das ist zwar auch hinreichend lästig, wenn Sie aber direkt eine Aktivierung durchführen, ist es ohnehin kein Problem.

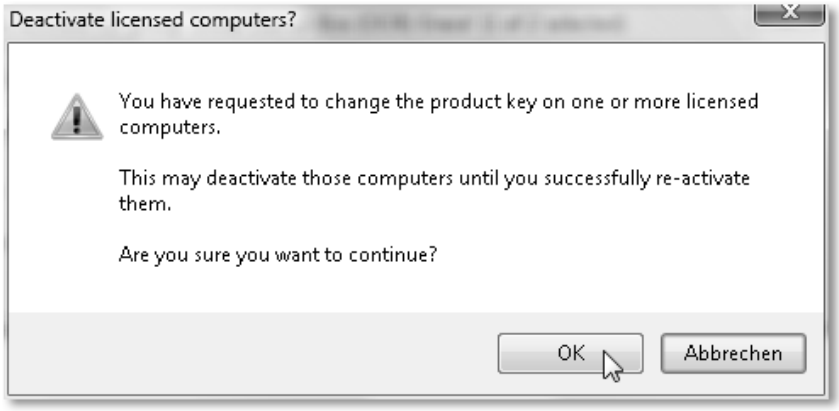


Abbildung 7.19 Eine gut gemeinte Warnung, aber seit Vista SP1 werden die Maschinen nicht mehr deaktiviert (RFM).

7.4.3 VAMT – MAK Proxy Activate

Eine wesentliche Voraussetzung bei der Arbeit mit MAK-Keys ist die Möglichkeit der Kommunikation mit den *Microsoft Activation Services*, die über das Internet per SSL-Verbindung erreichbar sind. Was geschieht nun, wenn Systeme aktiviert werden müssen, die keine oder nur sehr eingeschränkte Internet-Konnektivität haben? Auf diese Frage gibt es zwei Antworten:

- Sie arbeiten mit der telefonischen Aktivierung, was leider sehr (!) mühsam ist und allenfalls als Strafarbeit taugt. Wenn man diesen Vorgang für ein oder zwei Systeme ausführen muss, ist das noch machbar, wenn Sie auf diese Art Dutzende oder Hunderte Systeme aktivieren müssen, ist das unzumutbar!
- Sie nutzen die vom VAMT angebotene Proxy-Aktivierung.

Die letztgenannte Funktion wird im Kontextmenü eines Systems oder einer Gruppe aufgerufen und führt zu dem Dialog aus Abbildung 7.20, der diese Einstellungen zulässt:

- Es kann ein neuer MAK-Key installiert werden. Dieser muss vorher erfasst worden sein (siehe Abschnitt 7.3.2).
- Die Aktivierungsbestätigung (*Confirmation ID*) kann bei den Microsoft Activation Services angefordert werden.
- Die Aktivierungsbestätigung kann auf das System gebracht werden, wodurch das System aktiviert wird.

Weiterhin können alternative Anmeldeinformationen angegeben werden, falls der derzeit angemeldete Windows-Benutzer keine Admin-Rechte auf dem Zielsystem hat.

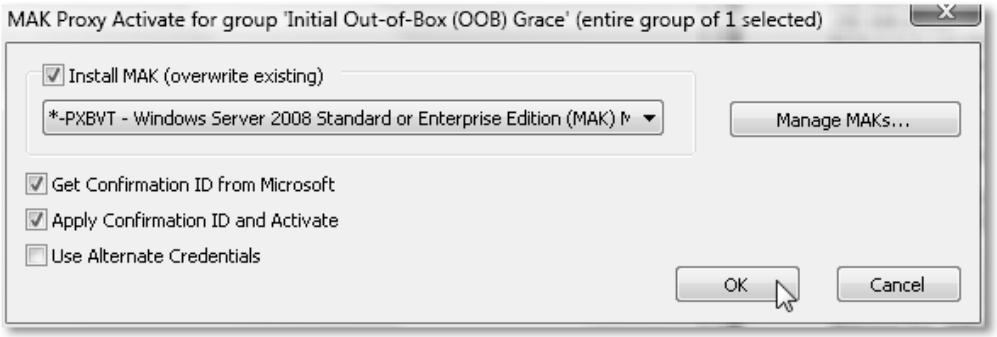


Abbildung 7.20 Beim »MAK Proxy Activate« gibt es gegenüber dem »Independent Activate« veränderte Einstellungen.

Beim eigentlichen Proxy-Activate-Vorgang geschieht Folgendes:

- VAMT installiert optional den MAK-Key und ermittelt auf dem zu aktivierenden Computer die Installation ID (IID).
- VAMT kommuniziert mit Microsoft, sendet also die IID und erhält die Confirmation ID (CID).
- Dann wird die CID auf dem Zielsystem installiert – und somit ist es aktiviert.

Während VAMT arbeitet, werden Sie einige Meldungen sehen, anhand derer man nachvollziehen kann, was passiert ist (Abbildung 7.21):

- Zuerst wurde der MAK-Key auf dem System installiert (links).
- Dann wurde die CID von Microsoft angefordert und auf dem System installiert (rechts).

Ich habe den Netzwerkverkehr bei der Proxy-Aktivierung mitgeschnitten, um den Vorgang zum einen im Detail zu betrachten und auch die Frage nach den zu öffnenden Ports zu klären.

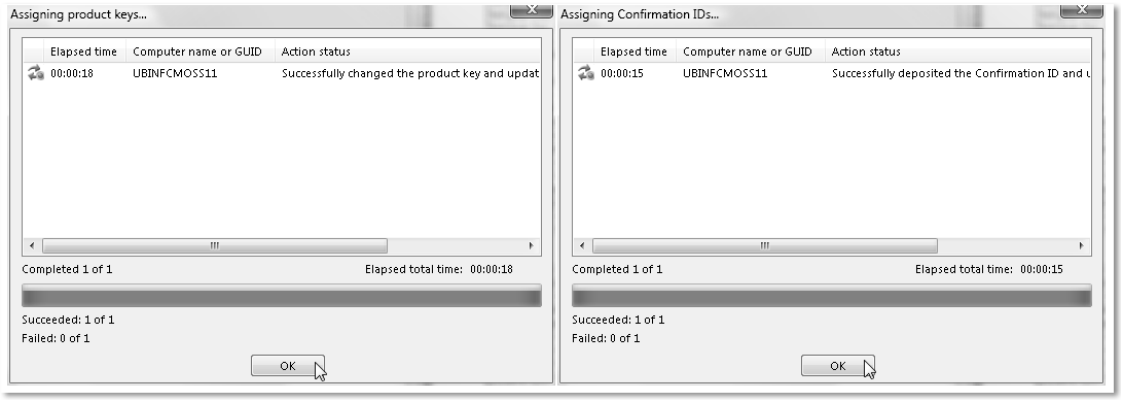


Abbildung 7.21 Zwei Schritte: Austausch des MAK-Keys (links) und Durchführung der Aktivierung

Abbildung 7.22 zeigt einen Auszug; nicht auf der Abbildung zu sehen sind die initialen Kommunikationsvorgänge zur Installation des MAK-Keys und der Anforderung der Installation ID (IID):

- Bei Paket 1281 beginnt die Kommunikation mit Microsoft, zunächst mit einer DNS-Abfrage nach dem Host *go.microsoft.com.*
- Dort wird der Client zum Host *activation.sls.microsoft.com* umgeleitet, in Paket 1294 gibt es die entsprechende DNS-Abfrage.
- Bis einschließlich Paket 1350 erfolgt der Datenaustausch mit Microsoft. Verwendet wird eine SSL-Verbindung auf Port 443 (also der Standard-SSL-Port).

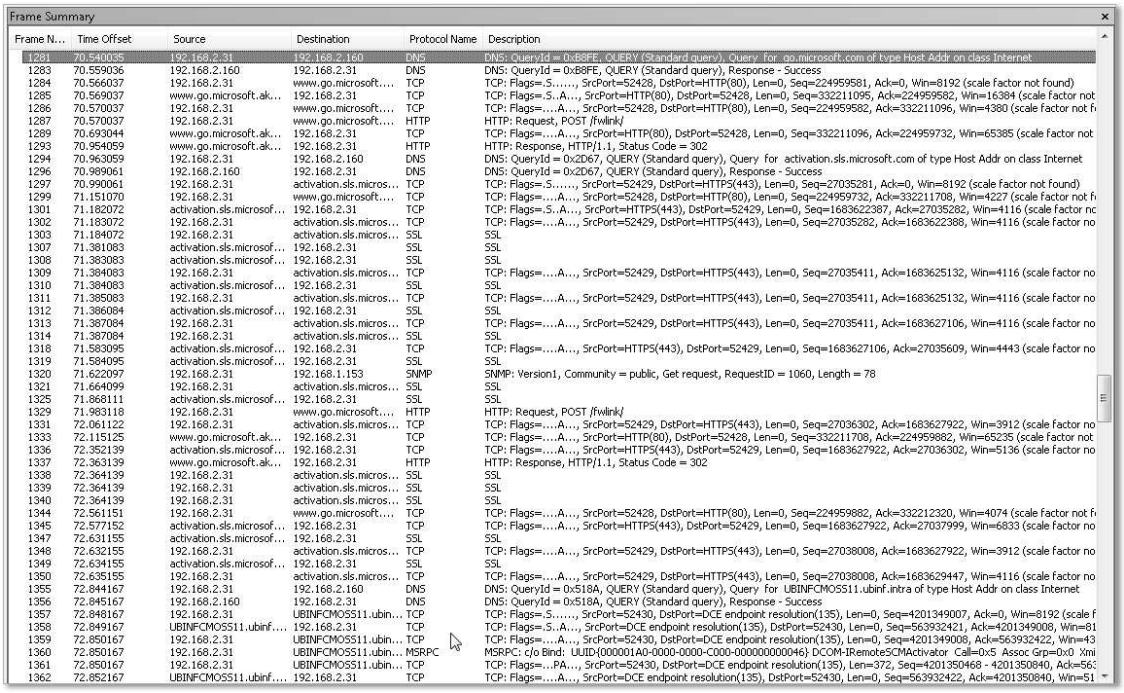


Abbildung 7.22 Ein Teil des Netzwerkverkehrs beim MAK-Proxy-Activate-Vorgang

- Paket 1355 ist eine DNS-Abfrage nach dem zu aktivierenden Host (*ubinfcmoss11.ubinf.intra*).
- Ab Paket 1357 erfolgt die Installation der von Microsoft erhaltenen *Confirmation ID* (CID) auf dem Zielserver. Hier wird das MSRPC-Protokoll auf Port 135 verwendet.

7.5 KMS – Key Management Service

Der elegantere Weg für die Aktivierung von Volumenlizenz-Betriebssystemen ist die Verwendung von KMS, dem Key Management Service. Der wesentliche Vorteil im Gegensatz zur Aktivierung mit MAK-Keys ist, dass die Clients keine direkte oder indirekte (*Proxy Activation*, siehe Abschnitt 7.4.3) Kommunikation mit Microsoft durchführen müssen. Vielmehr implementieren Sie in Ihrem Netz einen eigenen Aktivierungsserver, mit dem die Aktivierung durchgeführt wird. Dieser Server muss zwar regelmäßig mit Microsoft kommunizieren, ansonsten gibt es aber keine externe Kommunikation.

Dass KMS der für Unternehmen eigentlich vorgesehene Weg ist, lässt sich auch der Tatsache entnehmen, dass die von einem Volumenlizenz-Datenträger installierten Systeme als KMS-Client konfiguriert sind. In der Praxis bedeutet das, dass sie versuchen, den netzinternen KMS-Host zu finden, um sich dort zu aktivieren.

KMS-Clients

KMS-Clients können Windows Vista, Windows 7 und Windows Server 2008 sein.

7.5.1 Funktionsweise

Die Funktionsweise der Aktivierung mit KMS ist auf Abbildung 7.23 dargestellt:

- Der erste Schritt ist die Aktivierung des KMS-Hosts, was genauso wie beim MAK-Key funktioniert.
- Wenn ein KMS-Client sich aktivieren möchte, findet er den KMS-Host standardmäßig per DNS-Abfrage. Bei der Installation des KMS-Hosts wird ein entsprechender Eintrag vorgenommen.
- Der KMS-Client kommuniziert mit dem KMS-Host, wobei Folgendes geschieht:
  - Der KMS-Client erzeugt seine *Client Machine ID* (CMID) und sendet diese zum KMS-Host.
  - Der KMS-Host fügt diese CMID zu seiner internen Tabelle hinzu.

- Der KMS-Host sendet die Anzahl der bisher erfolgten Aktivierungen (*Activation Count*) an den Client.
- Der KMS-Client prüft den *Activation Count* und aktiviert sich, wenn dieser hoch genug ist (mehr dazu im Anschluss).

- Der Client wird standardmäßig alle sieben Tage Kontakt zum KMS-Host aufnehmen, um die Aktivierung zu erneuern. Die Aktivierung ist 180 Tage lang gültig.

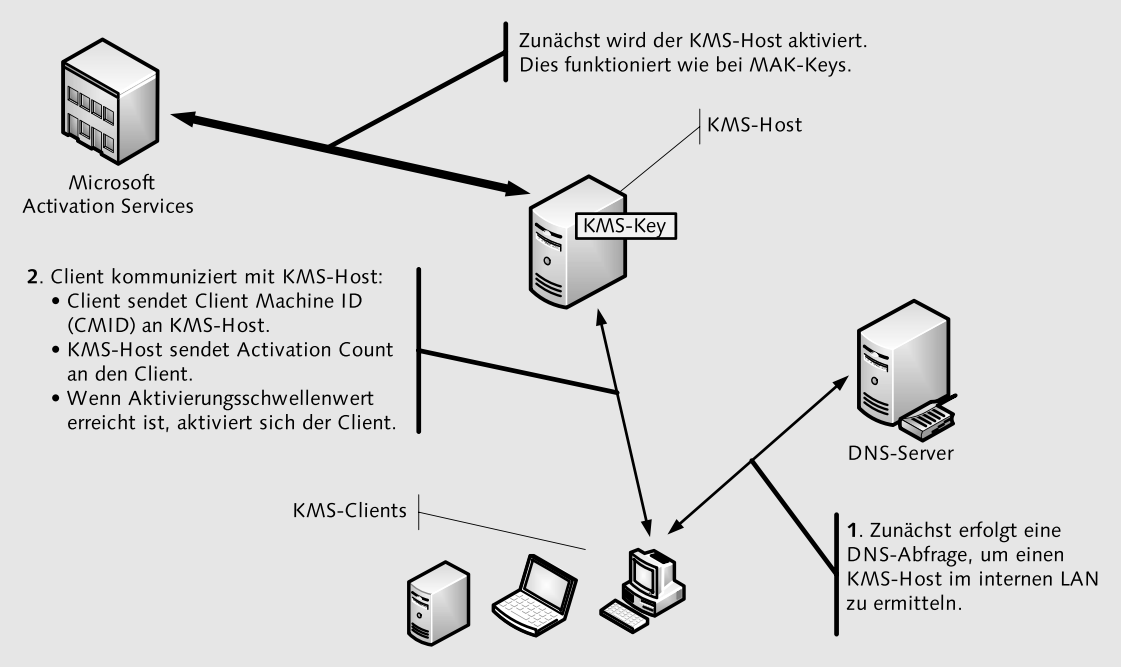


Abbildung 7.23 Die Funktionsweise der Aktivierung mit KMS

Kein separater Server nötig

Es ist durchaus nicht notwendig, dass der KMS-Dienst auf einem separaten Server ausgeführt wird. Im Grunde genommen ist das nur ein »kleiner« Dienst, der beispielsweise auf einem Domänencontroller ausgeführt werden kann.

Der Activation Count

Wenn Sie Volumenlizenz-Kunde sind, werden Sie von Microsoft einen oder mehrere KMS-Keys (für unterschiedliche Produktgruppen) erhalten haben. Das bedeutet aber noch lange nicht, dass Sie KMS tatsächlich nutzen können. Sie haben in der Beschreibung der Funktionsweise von einem *Activation Count* gelesen. Aus irgendwelchen politischen Gründen lässt Microsoft die Verwendung von KMS nicht zu, wenn weniger als 25 Client- oder 5 Serverbetriebssysteme aktiviert werden. Der KMS-Host kann installiert werden, und die KMS-Clients werden sich brav beim KMS-Host melden, allerdings funktioniert die Aktivierung erst, wenn die Schwellenwerte erreicht sind.

Solange sich nicht genügend KMS-Clients am KMS-Host gemeldet haben, wird die Aktivierung nicht vorgenommen. Erzwingt man die Aktivierung mit dem Assistenten, wird die Fehlermeldung aus Abbildung 7.24 zurückgegeben.

Die KMS-Clients werden alle zwei Stunden Kontakt zum KMS-Host aufbauen – sobald der *Activation Count* erreicht ist, wird die Aktivierung vorgenommen.

Umwandlung

Im Klartext bedeutet dass, dass Sie mit KMS nur beginnen können, wenn Sie innerhalb der *Grace Period* genügend KMS-Clients aktivieren können.

Falls Sie bereits diverse mit MAK-Keys aktivierte Systeme haben, können diese beispielsweise mit VAMT in KMS-Clients »umgewandelt« werden.

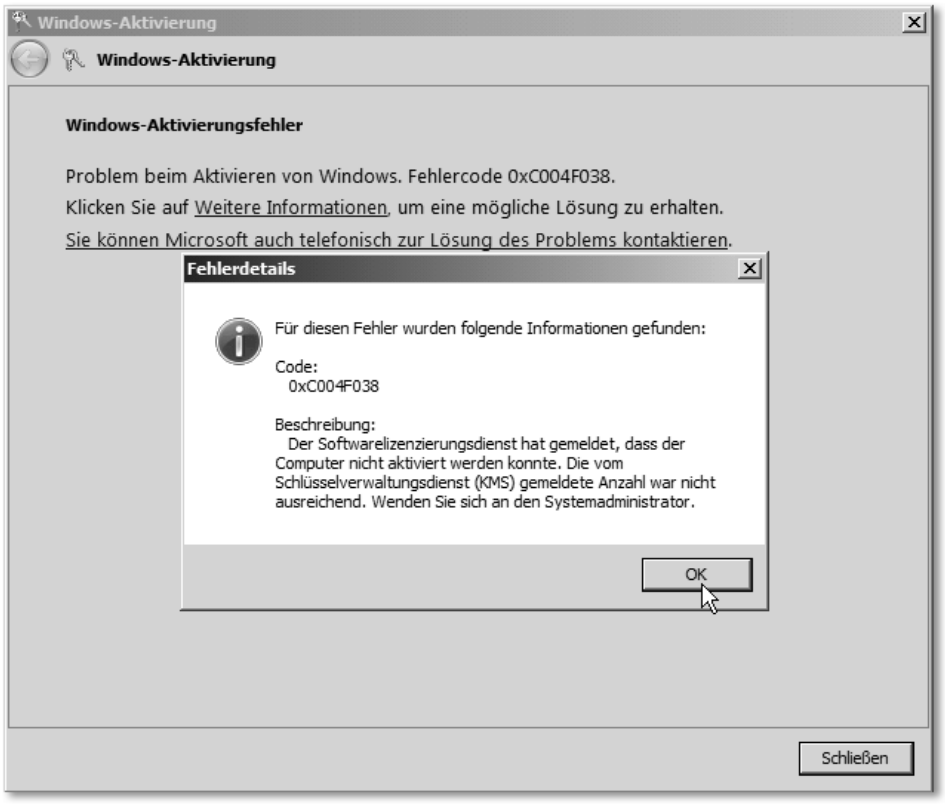


Abbildung 7.24 Sind bislang nicht ausreichend KMS-Clients am KMS-Host registriert, erhalten Sie am Client diese Fehlermeldung. (Der Screenshot stammt von einem Windows Server 2008.)

Tabelle 7.1 zeigt einige Beispiele, die zu verstehen helfen, unter welchen Voraussetzungen KMS wirklich aktiv arbeitet. Fazit ist:

- Windows Server 2008 kann aktiviert werden, wenn der *Activation Count* 5 oder größer ist.
- Windows 7 und Vista können aktiviert werden, wenn der *Activation Count* 25 oder größer ist.

Windows Server 2008	Windows 7, Vista	Activation Count	Aktiviert werden kann:
4	1	5	Windows Server 2008
1	4	5	Windows Server 2008
1	1	1	nichts
4	22	26	Windows 7/Vista

Tabelle 7.1 Diese Tabelle zeigt einige Beispiele, welche Betriebssysteme bei welcher KMS-Clientanzahl aktiviert werden können. (Quelle: Microsoft-Poster zu Volume Activation 2.0)

VMs zählen nicht

Ein weiterer extrem wichtiger Planungsaspekt ist, dass Betriebssysteme in virtuellen Maschinen zwar über KMS aktiviert werden können, aber virtuelle Maschinen nicht (!) für den *Activation Count* zählen.

Dies ist durchaus eine Falle für Kunden, die zunächst »nur« Windows Server 2008 und noch nicht Windows 7 einsetzen möchten und sehr nachhaltig auf Virtualisierung mit VMware setzen. Auch wenn zwanzig Windows-Server-2008-Server in VMs laufen, bleibt der *Activation Count* exakt bei Null.

Der *Activation Count* eines KMS-Hosts kann abgefragt werden, allerdings müssen Sie sich dazu in die Niederungen der Kommandozeile begeben. Das Skript *slmgr.vbs,* das Sie im Verzeichnis *c:\windows\system32* finden, kann mit dem Parameter `/dli` aufgerufen werden und zeigt dann unter anderem die AKTUELLE ANZAHL an (Abbildung 7.25).

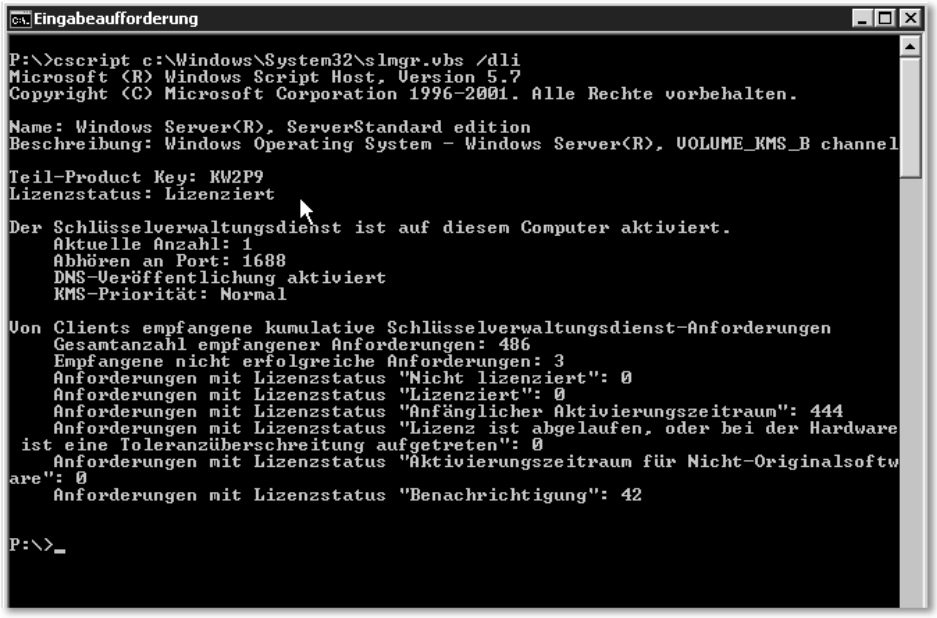


Abbildung 7.25 Mit »slmgr.vbs« können Sie den »Activation Count« abfragen. Achten Sie auf die Zeile »Aktuelle Anzahl«!

Jeder Host muss Activation Count überschreiten

Je nach Größe und Standortstruktur Ihres Unternehmens könnte es sinnvoll sein, mehrere KMS-Hosts zu implementieren. Beachten Sie, dass jeder dieser KMS-Hosts den *Activation Count* überschreiten muss – die KMS-Hosts »unterhalten« sich nicht untereinander.

Produktgruppen

Bereits zu Beginn des Kapitels habe ich Ihnen die vier vorhandenen Produktgruppen vorgestellt (Abbildung 7.2):

- Clientbetriebssysteme (*Business* und *Enterprise*)
- Server A: Web Server und HPC-Server
- Server B: *Standard*- und *Enterprise*-Edition
- Server C: *Data Center*-Edition und Itanium-Version

Je nach Lizenzvertrag haben Sie unter Umständen für jede Produktgruppe einen KMS-Key erhalten. Der KMS-Key ist dazu gedacht, um einen oder mehrere KMS-Hosts zu aktivieren, wobei der Key »nur« zur jeweiligen Produktgruppe passt.

Beim Aktivieren von KMS-Clients verhalten sich die KMS-Keys allerdings »hierarchisch«, was ja auch auf Abbildung 7.2 zu erkennen ist:

- Der Client-KMS-Key aktiviert nur Windows 7- und Vista-Betriebssysteme.
- Der Server-A-KMS-Key aktiviert die Serverbetriebssysteme seiner Produktgruppe (Web und HPC) und die Clientbetriebssysteme.

Etwas abstrakter gesagt gilt also, dass ein KMS-Client der eigenen Produktgruppe und darunter angeordnete aktivieren kann.

In den meisten Unternehmen wird somit folgende Vorgehensweise gewählt:

- Als KMS-Host wird ein Windows Server 2008 verwendet, beispielsweise ein Domänencontroller.
- Dieser kann dann Windows Server 2008 in der *Standard*- und der *Enterprise*-Version aktivieren (eigene Produktgruppe). Weiterhin können die *Web Server Edition* und die Clientbetriebssysteme aktiviert werden.

Daraus ergibt sich, dass der KMS-Key der Client-Produktgruppe nicht benötigt wird, denn die Aktivierung der Clientbetriebssysteme erfolgt mit einem Server. Alternativ könnten Sie übrigens auch einen Windows 7- oder Vista-Client zum Aktivieren der Clientbetriebssysteme verwenden und den KMS-Host darauf aktivieren – aber wozu?

7.5.2 Installation

Wenn Sie sich darüber im Klaren sind, welches System die Rolle des KMS-Hosts übernehmen soll, geht es um die Installation.

SSL

Ein KMS-Host muss regelmäßig mit den *Microsoft Activation Services* kommunizieren. Er muss demzufolge eine SSL-Verbindung in das Internet aufbauen können.

Windows Server 2008 und Windows 7/Vista als KMS-Host

Das Wort »Installation« ist in diesem Fall die Übertreibung der Woche, denn Sie brauchen die Maschine im Grunde genommen nur mit dem KMS-Key zu aktivieren – und schon ist das System ein KMS-Host. Irgendwelche Installationsarbeiten sind nicht erforderlich.

Bei der Aktivierung als KMS-Host sollte automatisch ein DNS-Eintrag erstellt werden. Dieser Eintrag ist extrem wichtig, weil die KMS-Clients den KMS-Host über diesen Eintrag finden.

Sie können zwei Aspekte kontrollieren:

- Prüfen Sie, ob auf dem KMS-Host keine Fehlermeldungen bezüglich der Erstellung des DNS-Eintrags vorhanden sind (teilweise kommt das vor).
- Sie können im DNS-Manager kontrollieren, ob der Eintrag vorhanden ist. Es muss, wie auf Abbildung 7.26 zu sehen, ein Eintrag namens _VLMCS vorhanden sein.

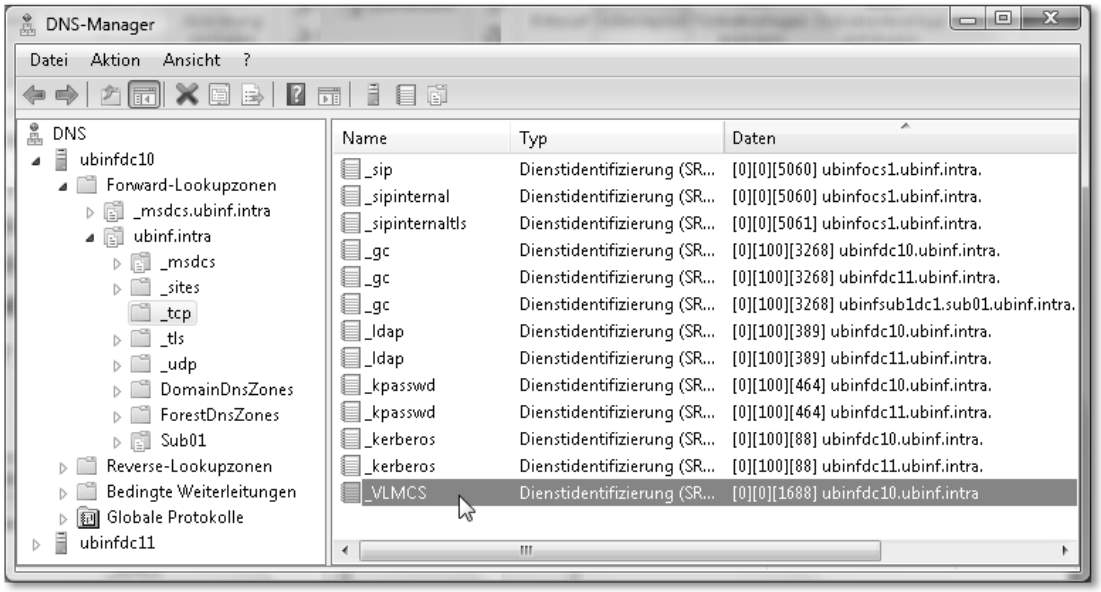


Abbildung 7.26 Der KMS-Host sollte einen Eintrag zur Dienstidentifizierung anlegen (_VLMCS).

Sollte es Probleme beim automatischen Anlegen des Eintrags geben, können Sie diesen auch manuell erzeugen:

- Starten Sie den DNS-Manager, und navigieren Sie in den Abschnitt Forward-Lookupzonen.
- Wählen Sie im Kontextmenü der Domäne den Menüpunkt Weitere neue Einträge.
- Wählen Sie in dem nun erscheinenden Dialog den Ressourceneintragstyp Dienstidentifizierung (SRV).
- Nehmen Sie den Eintrag wie auf Abbildung 7.27 gezeigt vor.

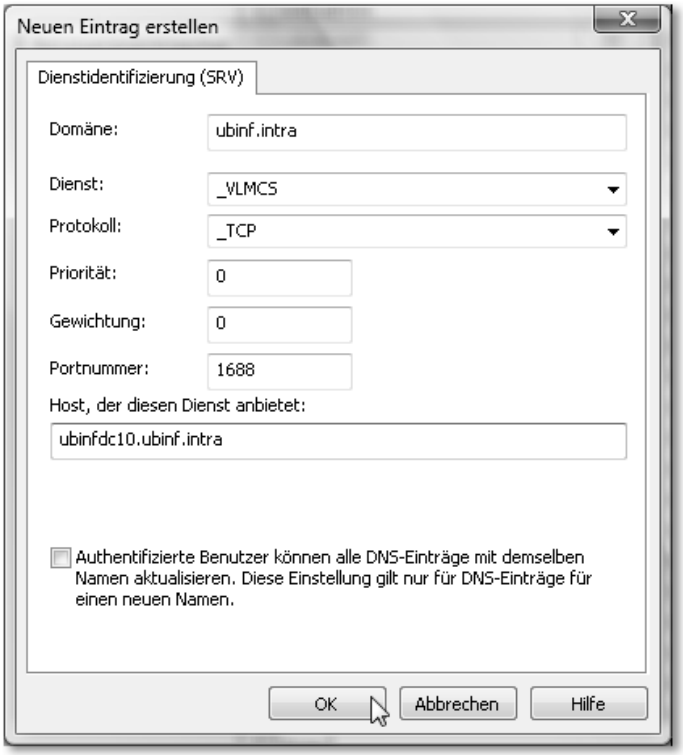


Abbildung 7.27 Falls der DNS-Eintrag, aus welchen Gründen auch immer, nicht automatisch erstellt werden kann, können Sie den Eintrag auch manuell vornehmen.

Windows Server 2003 als KMS-Host

Es ist nun natürlich denkbar, dass in Ihrem Unternehmen zwar Windows 7-Clients eingesetzt werden sollen, aber keine Windows-Server-2008-Maschinen vorhanden sind (z. B. wegen der Lizenzenkosten). Demnach könnte es wünschenswert sein, als KMS-Server eine Windows-Server-2003-Maschine zu wählen. Dies ist möglich, allerdings geht es nicht ganz so einfach wie bei den moderneren Betriebssystemen:

- Laden Sie aus dem Microsoft Download Center den KMS-Server für Windows Server 2003 herunter. Sie finden das Produkt mit den Suchbegriffen *KMS Windows Server 2003*. Achten Sie darauf, dass es eine x86- und eine x64-Version gibt.
- Extrahieren Sie das Paket, und führen Sie sowohl die eigentliche Installationsdatei als auch das Update aus.

Nun kann der KMS-Key installiert und aktiviert werden. Ab diesem Moment funktioniert der KMS-Host so wie ein KMS-HOST auf einem Windows Server 2008-System. Das Management erfolgt mit *slmgr.vbs*.

7.5.3 Achtung!

Ich habe es mehr als einmal erlebt, dass Kunden mehrere Systeme direkt mit dem KMS-Key aktiviert haben, diesen also wie einen MAK-Key verwendet haben. Die »Falle« ist, dass das zunächst auch gut geht; ein Blick mit VAMT offenbart aber das Problem (Abbildung 7.28; das ist übrigens ein Screenshot aus einer echten Kundenumgebung): Wenn die Aktivierung mit einem KMS-Key erfolgt, ist jede aktivierte Maschine ein KMS-Host. Das Betriebssystem läuft trotzdem, aber so bekommen Sie vermutlich die notwendigen Activation-Count-Summen nicht zusammen. Mal ganz abgesehen davon, dass das von einer sauberen Architektur meilenweit entfernt ist.

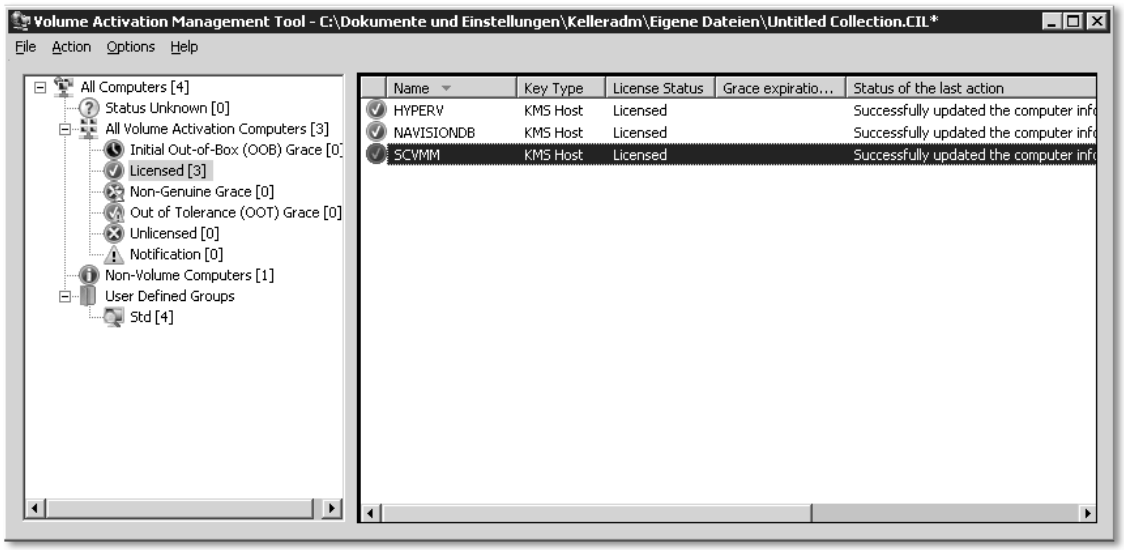


Abbildung 7.28 So sollte es eigentlich nicht sein: Plötzlich sind drei KMS-Hosts vorhanden, weil der KMS-Key mehrfach verwendet wurde.

7.6 Fazit: MAK vs. KMS

Grundsätzlich gilt, dass in einer größeren Umgebung eigentlich kein Weg an KMS vorbeiführt – es funktioniert dann alles mehr oder weniger automatisch, zumindest dann, wenn die zu aktivierenden Betriebssysteme von einem Volumenlizenzdatenträger installiert sind.

Ein gewisses Problem mit KMS ist, dass Sie eine Mindestanzahl von KMS-Clients benötigen. Wenn Sie diese Schwelle nicht überschreiten können, wird mittels KMS kein einziges System aktiviert (siehe den Abschnitt »Der Activation Count« in Abschnitt 7.5.1). Kleinere Unternehmen oder solche, die (noch) zu wenig Windows 7/Vista- und/oder Windows Server 2008-Systeme haben, müssen (!) zu MAK-Keys greifen.

Alle, die von den Leuten des Königs zu ihm kamen, entließ er in solcher Stimmung, dass sie ihm mehr als dem König zugetan waren.

8 Windows RE

Bekanntlich ist es ja nicht auszuschließen, dass ein PC nicht startet oder sonstwie »Ärger« macht – selbst mit Windows 7. Ein Hilfsmittel für solche Fälle ist *Windows RE*, wobei das Kürzel für *Recovery Environment*, also Wiederherstellungsumgebung, steht. Die Idee ist kurz gesagt, eine separate, auf einige wesentliche Komponenten reduzierte Betriebssysteminstanz zu starten, die einige Reparaturwerkzeuge bietet und darüber hinaus eine Eingabeaufforderung enthält, mit der ein Zugriff auf das Dateisystem des PCs möglich ist.

Windows RE basiert auf *Windows PE (Preinstallation Environment)*, das Sie bereits im Deployment-Kapitel kennengerlernt haben. Windows RE tritt standardmäßig dann in Erscheinung, wenn ein Windows 7-PC nicht starten kann; in diesem Fall wird angeboten, die Starthilfe zu starten (Abbildung 8.1). Die Starthilfe ist letztendlich eine Windows RE-Instanz, innerhalb derer einige Reparaturwerkzeuge ausgeführt werden.

Wiederherstellungsumgebung

Die Wiederherstellungsumgebung rufen Sie durch Drücken von F8 während des Startvorgangs auf.

Wesentliche Vorteile von Windows RE im Unternehmen sind:

- Es können nach Bedarf eigene Wiederherstellungswerkzeuge integriert werden.
- Sie können benötigte Treiber integrieren – sofern Hardware zum Einsatz kommt, die nicht standardmäßig von Windows 7 unterstützt wird.

Neben der Reparatur wäre beispielsweise auch ein Einspielen eines Images, somit also eine Neuinstallation möglich. Windows RE hat mehrere Zielgruppen:

- PC-Hersteller, die den Kunden eine einfache Möglichkeit geben wollen, einen »total verquasten« PC wieder in den funktionsfähigen Ursprungszustand zu versetzen

Abbildung 8.1 Kann ein PC nicht starten, wird die Starthilfe angeboten.

- Endbenutzer, die ein selbst erstelltes Sicherungs-Image wieder einspielen möchten
- Administratoren, die den PC-Service im Unternehmen optimieren möchten

Da dieses Buch sich im Wesentlichen an die letztgenannte Gruppe richtet, stelle ich Ihnen nachfolgend das Szenario vor, das mir im Unternehmensumfeld am sinnvollsten erscheint:

Wenn ein PC nicht startet, ist das prinzipiell kein Drama – zumindest dann nicht, wenn Sie eine einigermaßen weitgehende Standardisierung der PCs erreicht haben und Sie dem Benutzer durch eine simple Neuinstallation helfen können. Nichtsdestotrotz könnte ein Reparaturversuch, eventuell mit zusätzlichen Werkzeugen, sinnvoll sein. Im Unternehmensumfeld dürfte es sich anbieten, die (eventuell modifizierte) Windows-RE-Umgebung über die Windows-Bereitstellungsdienste (WDS) per Netzwerkbootvorgang zu starten. Andere Möglichkeiten sind:

- das Starten von CD
- die Integration einer zusätzlichen Windows RE-Umgebung auf die Festplatte (Wiederherstellungspartition)

Die letztgenannte Option macht auf einem stationären PC im Unternehmen nur wenig Sinn – hierbei halte ich das Starten von Windows RE per Netzwerkboot für wesentlich eleganter. Für PC-Hersteller ist es aber, insbesondere im Privatkundenbereich, ein eleganter Weg, um eine Neuinstallation zu ermöglichen.

Eine Sonderrolle nehmen Notebooks von Unternehmensmitarbeitern ein: Eventuell könnte es hier sinnvoll sein, ein Windows RE, mit dem das Standard-Unternehmens-Image aufgebracht werden kann, auf einer separaten Partition zu speichern. Wenn ein Kollege dienstlich in Malaysia ist und die Windows 7-Installation auf seinem Notebook aus irgendwelchen Gründen nicht mehr hochfährt, könnte die »Rettung« darin bestehen, ihn ein Image einspielen zu lassen, sprich: eine Neuinstallation durchzuführen. Ganz so einfach ist es zwar dann in der Praxis nicht, denn es müssen lokale Daten gesichert, das Gerät in die Domäne gehoben, individuelle Anpassungen vorgenommen werden und vieles andere mehr – wobei einiges ohne Zugriff auf das Unternehmensnetz gar nicht möglich ist. Eventuell ist die Möglichkeit, ein Standard-Abbild einzuspielen, aber zunächst besser als nichts.

Eine weitere Möglichkeit wäre, nach der Installation das Notebook zu imagen und dieses (individuelle) Image auf einer Wiederherstellungspartition zu hinterlegen. Den daraus resultierenden Vorteilen steht aber ein immenser Aufwand entgegen.

8.1 (Standard-)Funktionalität

Wenn Sie keine weiteren Anpassungen vorgenommen haben, können Sie die die Windows RE-Umgebung starten, in dem Sie folgende Schritte vornehmen:

- Starten Sie die Installation des originalen Windows 7-Installations-Images. Dies kann entweder per Netzwerkboot erfolgen (siehe u. a. Abschnitt 6.4.5 ff.), oder Sie booten von der Installations-DVD.
- Wenn der erste Installationsdialog erscheint, wählen Sie die Option Computerreparaturoptionen (Abbildung 8.2).

Eine der ersten Maßnahmen des Assistenten wird darin bestehen, herauszufinden, welche Windows-Installationen auf dem PC vorhanden sind. Das Ergebnis wird in etwa wie auf Abbildung 8.3 gezeigt aussehen: Sie können entweder eine bestehende Windows-Installation zur Reparatur auswählen oder sich für das Wiederherstellen eines Images entscheiden.

Abbildung 8.2 Wenn Sie das originale Windows 7-Installations-Image starten, gelangen Sie durch Auswahl der Computerreparaturoptionen in die Windows RE-Umgebung.

Wenn Sie sich für die Reparatur einer vorhandenen Installation entschieden haben, werden einige Wiederherstellungstools angezeigt (Abbildung 8.4). Neben einigen Werkzeugen, wie beispielsweise der SYSTEMSTARTREPARATUR, steht auch eine EINGABEAUFFORDERUNG zur Verfügung – um manuelle Anpassungen vorzunehmen.

Abbildung 8.3 Zunächst werden die vorhandenen Windows-Installationen gesucht. Eine davon können Sie für die Reparatur auswählen.

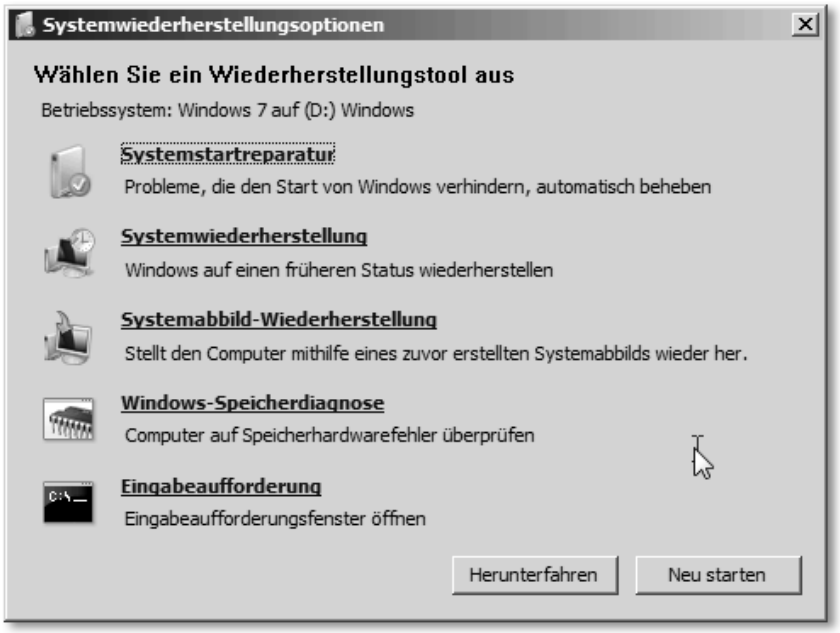


Abbildung 8.4 Diese Wiederherstellungstools sind standardmäßig vorhanden.

8.2 Win RE-Image erstellen und in WDS integrieren

In diesem Abschnitt werde ich Ihnen zeigen, wie Sie ein Windows RE-Image erstellen, dieses in die Windows-Bereitstellungsdienste integrieren und testen.

8.2.1 Image erstellen

Das Windows RE-Image wird mit den im WAIK enthaltenen Mitteln erstellt. Es gibt hierfür zwar keine grafische Unterstützung, es ist aber kein Problem:

- Starten Sie die *Eingabeaufforderung für Bereitstellungstools* mit administrativen Rechten (Als Administrator ausführen).
- Kopieren Sie alle benötigten Dateien in ein noch nicht existierendes Verzeichnis. Der Aufruf lautet: `copype.cmd <Architektur> <Ziel>`, also beispielsweise:

  ```
  copype.cmd amd64 c:\winREImage
  ```

- Integrieren Sie das das Boot-Image von der Windows 7-DVD. Die Aufrufe sind:
  - `imagex.exe /export /boot <DVD_Drive>\sources\boot.wim 2 c:\winREImage\winre.wim «Windows Recovery Environment"`
  - `imagex.exe /mountrw c:\winREImage\winre.wim 1 c:\winREImage\mount`

- Nun muss für das Image noch ein Windows RE-Skript erstellt werden:
  - Erstellen Sie mit dem Text-Editor eine Textdatei namens *Winpeshl.ini*. Sie muss Folgendes beinhalten:

    ```
    [LaunchApp]
    AppPath=X:\sources\recovery\recenv.exe
    ```

  - Die Datei wird in das Arbeitsverzeichnis kopiert, und zwar mit diesem Befehl:

```
copy winpeshl.ini C:\winREImage\mount\Windows\System32
```

- Nun haben Sie die Möglichkeit, weitere Treiber oder Tools hinzuzufügen.
- Im letzten Schritt werden die Änderungen in die Imagedatei kopiert. Der Befehl lautet:

```
imagex.exe /unmount /commit c:\winREImage\mount
```

Dieses Image können Sie nun mithilfe der Windows-Bereitstellungsdienste booten. Alternativ könnte es auch auf CD gebrannt oder in eine Windows-Installation integriert werden.

8.2.2 Integration in die Windows-Bereitstellungsdienste vornehmen

Der nächste Schritt ist die Integration des Windows RE-Boot-Images in die Windows-Bereitstellungsdienste. Öffnen Sie dazu das Verwaltungswerkzeug, und wählen Sie den entsprechenden Menüpunkt im Kontextmenü des Knotens Startabbilder (Abbildung 8.5).

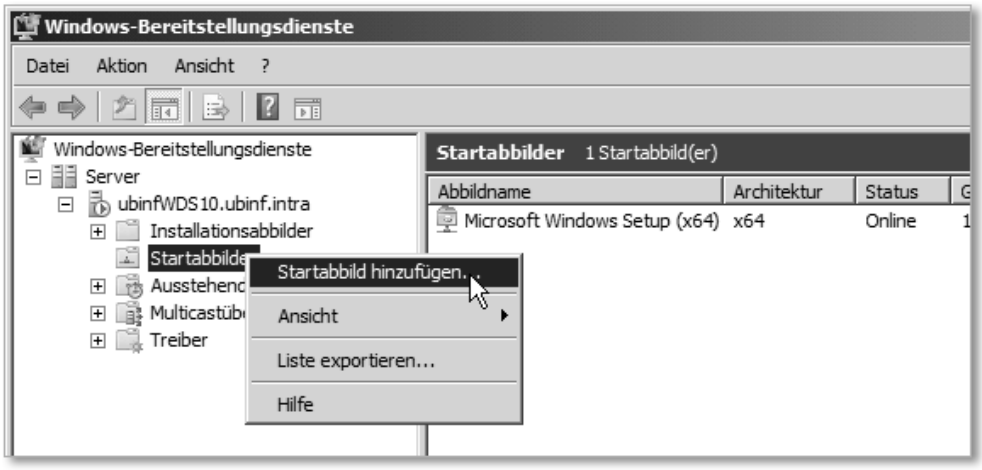


Abbildung 8.5 Das neue Windows RE-Image wird den Startabbildern hinzugefügt.

Der Assistent wird natürlich den Pfad des WIM-Images wissen wollten, außerdem können Sie einen Abbildnamen vergeben. Dieser ist beliebig wählbar. Sie

sollten allerdings bedenken, dass dieser Name in der Liste der startbaren Images erscheint – er sollte also möglichst selbsterklärend sein (Abbildung 8.6).

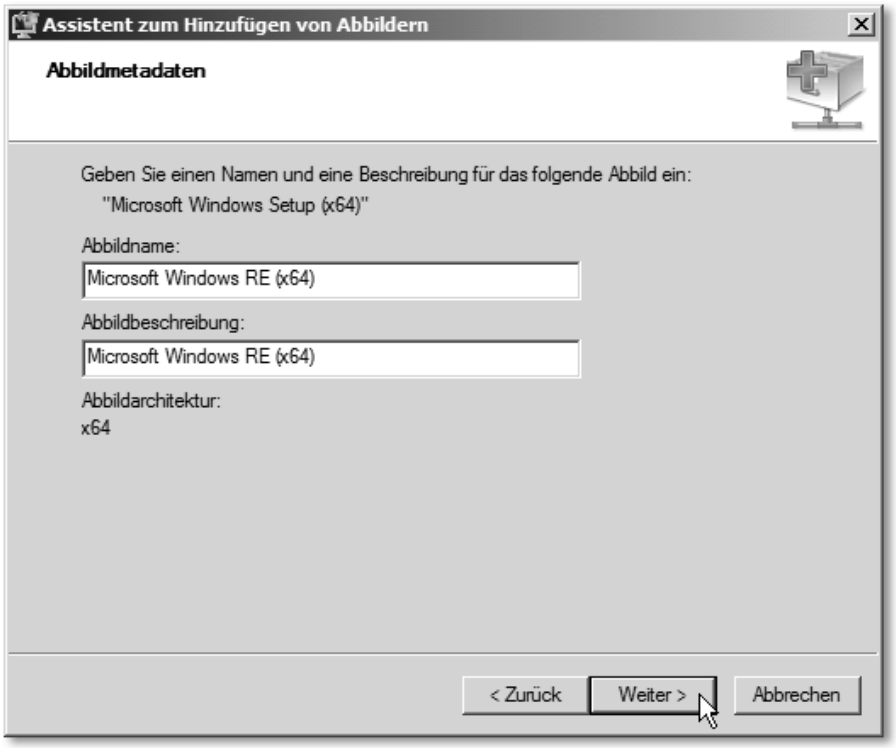


Abbildung 8.6 Vergeben Sie einen prägnanten Namen. Dieser wird später in der Auswahl der bootbaren Images erscheinen.

Damit ist die Integration des neuen Windows-RE-Start-Images in die Windows-Bereitstellungsdienste auch schon abgeschlossen.

8.2.3 Test

Kommen wir nun zum Test: Starten Sie auf einem PC den Netzwerkbootvorgang. Sofern mehr als ein Start-Image für die Hardwarearchitektur des PCs vorhanden ist, erscheint der Auswahldialog aus Abbildung 8.7 – das ist der Grund, weshalb ich Ihnen weiter vorn geraten habe, einen möglichst aussagekräftigen Namen für das neue Image zu wählen.

Wenn Sie das entsprechende Image ausgewählt haben, werden Sie sehen, dass der Programmstart vom »richtigen« Boot-Image erfolgt. Auf Abbildung 8.8 sehen Sie, dass aus dem Image *winre.wim* gestartet wird. (Es ist aber nicht erforderlich, dass der Name des Windows RE-Images auch tatsächlich *winre.wim* lautet. Der Name ist beliebig.)

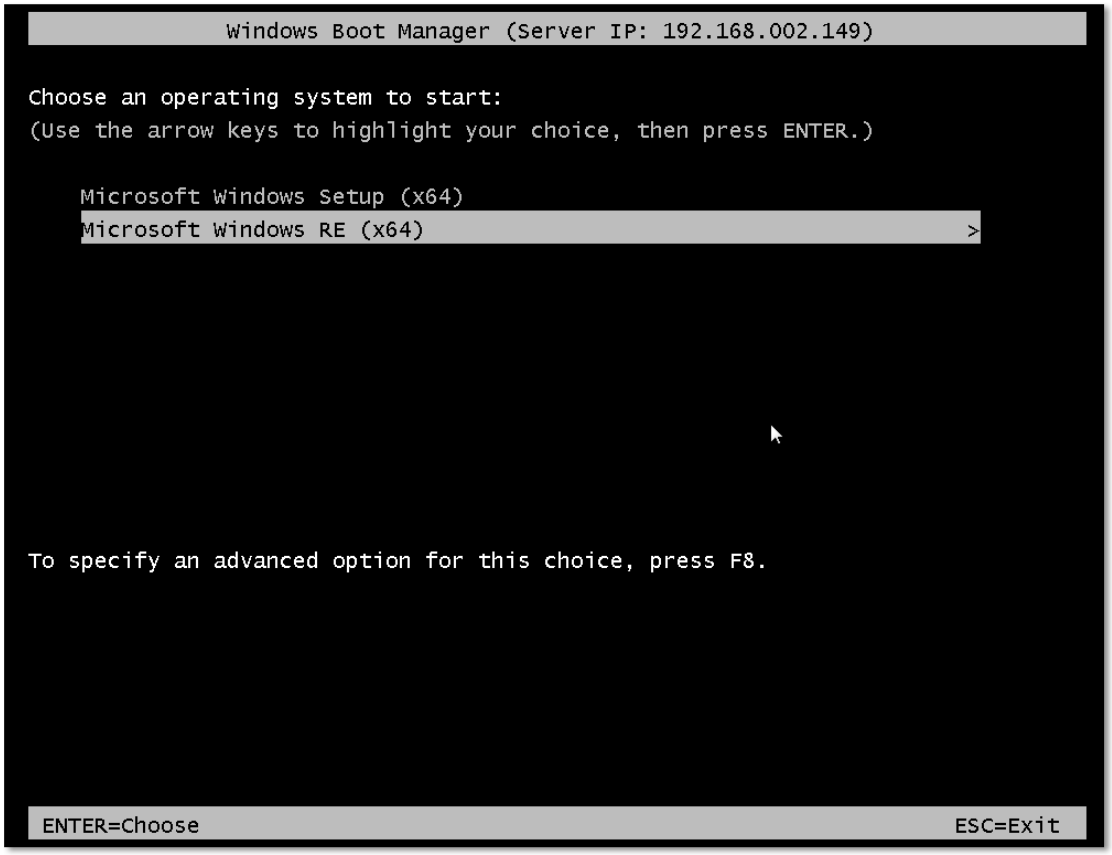


Abbildung 8.7 Wenn für die Hardwarearchitektur mehrere Boot-Images vorhanden sind, müssen Sie eines auswählen. Das neu hinzugefügte Windows RE-Image ist auch dabei.

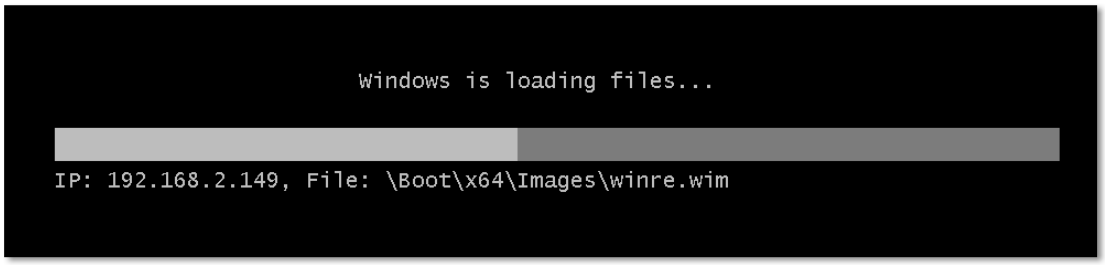


Abbildung 8.8 So soll es sein: Der Startvorgang erfolgt von dem Windows RE-Image (winre.wim).

Sie sehen übrigens, dass der Windows RE-Startvorgang exakt dem Startvorgang bei der Installation entspricht. Das ist im Grunde genommen ja auch nicht erstaunlich, denn Windows RE ist letztendlich »nur« ein Spezialfall von Windows PE.

Das erste »Lebenszeichen« von der Wiederherstellungsumgebung taucht auf, wenn Sie aufgefordert werden, die Tastatureingabemethode auszuwählen (Abbildung 8.9). In dem abgebildeten Fall kann übrigens keine andere Sprache als Deutsch gewählt werden, weil in dem Windows RE-Image keine zusätzlichen Sprachpakete installiert worden sind. Sofern Sie in der Wiederherstellungsumge-

bung mehrere Sprachen unterstützen möchten, können Sie Sprachpakete nachinstallieren – das funktioniert in etwa so, wie in Abschnitt 6.10 gezeigt.

Abbildung 8.9 Das erste Lebenszeichen der Systemwiederherstellungsoptionen ist die Auswahl der Sprache.

Wenn Sie die Tastatureingabemethode ausgewählt haben, setzt sich der Vorgang wie auf Abbildung 8.3 und Abbildung 8.4 gezeigt fort – es gibt keine weiteren Überraschungen.

8.3 Windows RE-Umgebung anpassen

Es ist durchaus denkbar, dass Sie für die Unterstützung des Wiederherstellungsvorgangs gern zusätzliche Programme in die Wiederherstellungsumgebung integrieren würden. Grundsätzlich ist es möglich, eigene Dateien (natürlich auch **.exe*) in das Boot-Image zu integrieren; in Abschnitt 6.10, »Image-Pflege«, ist die grundsätzliche Vorgehensweise erläutert. Sie können das auch noch ein wenig perfektionieren, indem Sie das gewünschte Werkzeug in die Auflistung der Systemwiederherstellungsoptionen integrieren. In diesem Artikel zeige ich Ihnen, wie dies gemacht wird.

Zunächst muss das in Abschnitt 8.2.1 erzeugte Boot-Image zur Bearbeitung gemountet werden. Dies geschieht mit folgendem Befehl (in meinem Fall ist *c:\winREImage* das zuvor angelegte Arbeitsverzeichnis für das Image):

```
Imagex /mountrw c:\winREImage\winre.wim 1 c:\winREImage\mount
```

Um ein eigenes Werkzeug in die Wiederherstellungsumgebung zu integrieren, sind folgende Schritte notwendig. (Die Datei »WinREConfig.xml« dient zur Ergänzung der Werkzeugauflistung in der Wiederherstellungsumgebung.)

- Legen Sie eine Datei namens *WinREConfig.xml* im Verzeichnis */sources/Recovery/Tools* in dem Verzeichnis des gemounteten Images an. (In meinem Fall lautet der komplette Pfad also *C:\windowsREImage\mount\sources\Recovery\Tools*.)
- Erstellen Sie das XML-Dokument. Im einfachsten Fall wird lediglich der relative Pfad (bezogen auf das Verzeichnis *...\Tools*) zu der ausführbaren Datei des zu integrierenden Werkzeugs angegeben (Abbildung 8.10).

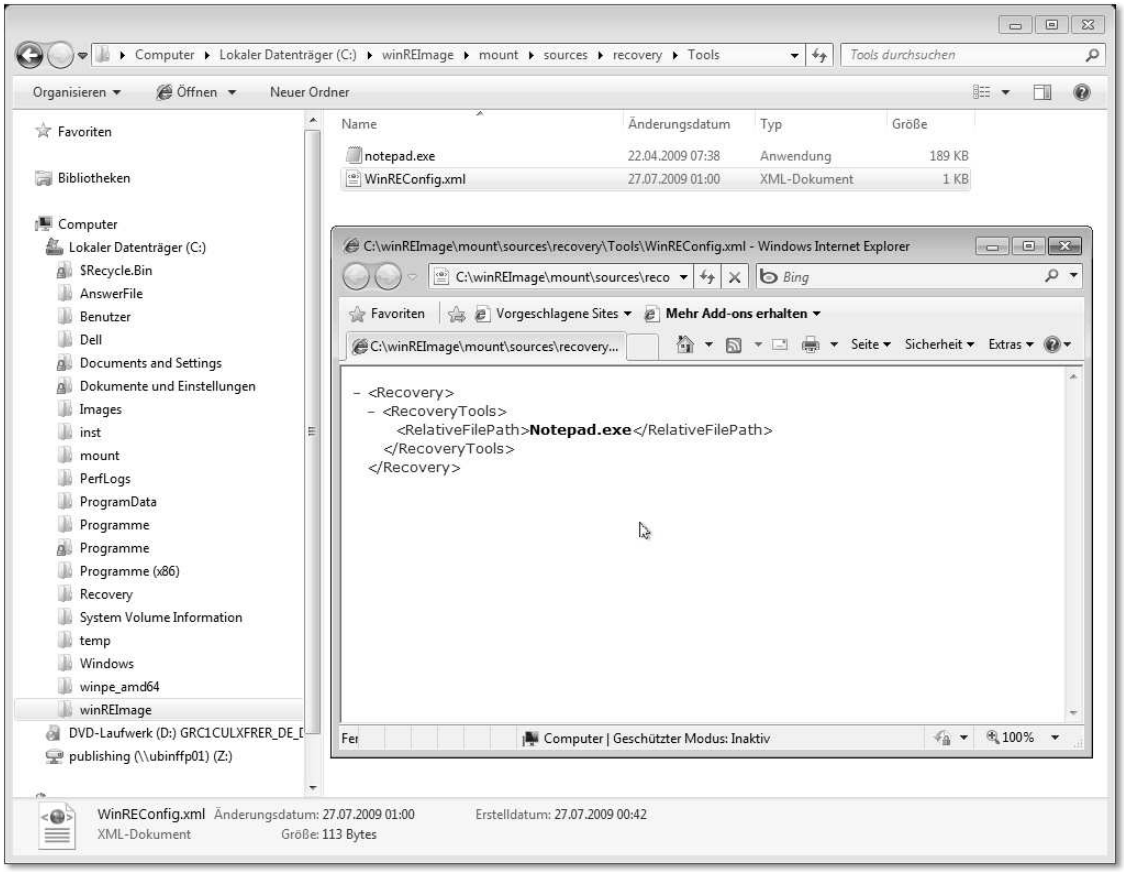


Abbildung 8.10 Die Datei »WinREConfig.xml« dient zur Ergänzung der Werkzeugauflistung in der Wiederherstellungsumgebung.

- Die ausführbare Datei des Werkzeugs kopieren Sie ebenfalls in das *...\Tools*-Verzeichnis.

In der WAIK-Dokumentation sind übrigens noch viel mehr mögliche Einstellungen für die XML-Datei vorhanden, als auf Abbildung 8.10 gezeigt werden. Suchen

Sie dort einfach nach dem Stichwort *WinREConfig.xml*: Es wird eine Fundstelle namens ANPASSUNG DES ERSCHEINUNGSBILDS... geben. Dort sind alle Optionen hinreichend verständlich erläutert.

Wenn Sie die Anpassungen vorgenommen haben, lassen Sie diese mit folgendem Befehl in das vorhandene Image »einbauen«:

```
Imagex.exe /unmount /commit c:\winREImage\mount
```

Nun muss das neu erzeugte Image noch auf den WDS-Server geladen werden. Dies können Sie im grafischen Konfigurationswerkzeug erledigen, indem Sie im Kontextmenü des vorhandenen Start-Images den Menüpunkt ABBILD ERSETZEN aufrufen.

Wenn Sie nun in die Wiederherstellungsumgebung booten, wird in der Liste der Wiederherstellungsoptionen der zusätzliche Menüpunkt zu sehen sein (Abbildung 8.11).

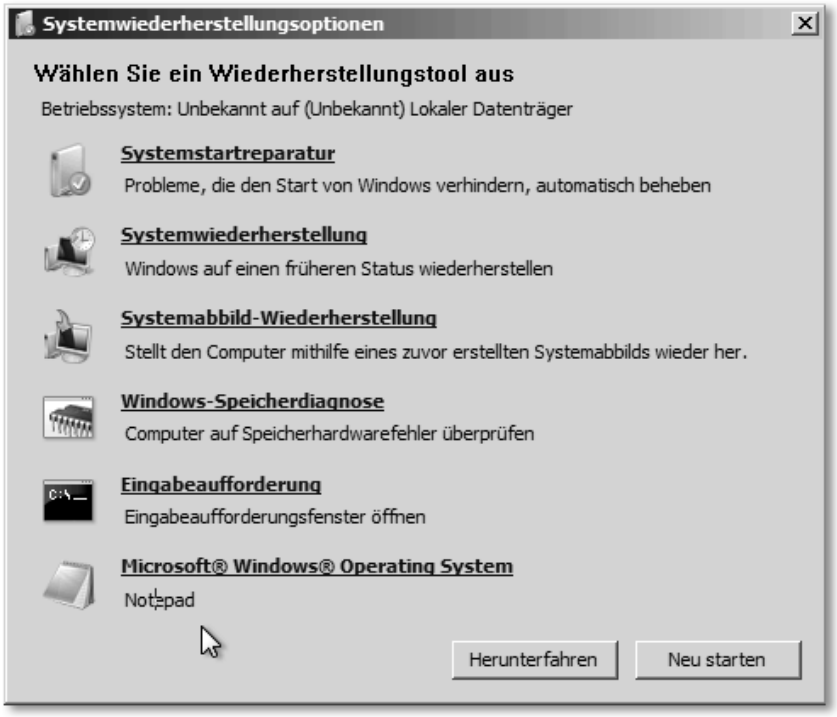


Abbildung 8.11 Der Auswahldialog für die Systemwiederherstellungsoptionen ist um den eigenen Eintrag ergänzt worden.

In den Internet-Foren findet man des Öfteren die Frage, wie man einen eigenen Namen für das hinzugefügte Werkzeug vergeben kann – diese Frage wird regelmäßig von den Kollegen gestellt, bei denen als Name UNKNOWN angezeigt wird. Die Antwort ist, dass der Name automatisch ermittelt wird und keine Möglichkeit besteht, diesen zu überschreiben (zumindest ist keine dokumentiert). Der Name

wird automatisch aus den Dateiversionsinformationen der ausführbaren Datei ermittelt, wobei es nun zwei Möglichkeiten für ein UNKNOWN gibt:

- In den Dateiversionsinformationen sind keine Informationen gespeichert.
- Das Programm, das die Systemwiederherstellungsoptionen auflistet, kann die angegebene ausführbare Datei nicht finden. Diesen Fall halte ich übrigens für wahrscheinlicher; überprüfen Sie also nochmals Ihre *WinREConfig.xml*.

Auch ließ er es sich angelegen sein, dass die ihm untergebenen Barbaren kriegstüchtig und ihm ergeben seien.

9 Applikationen und Windows 7

Ein schickes, schnelles und stabiles Betriebssystem zu haben, ist zwar schon gut, so richtig Sinn macht aber alles erst dann, wenn auch die benötigten Applikationen ausgeführt werden.

In diesem Abschnitt werde ich Ihnen zunächst zeigen, wie Sie mithilfe des *Application Compatibility Toolkits* die in Ihrer Umgebung vorhandenen Anwendungen analysieren können. Für die »schwierigen Fälle« gibt es den Windows XP-Mode – ein Windows XP in einer virtuellen Maschine mit »ein wenig Integration« in Windows 7 drumherum.

9.1 Application Compatibility Toolkit (ACT)

Bei Windows 7-Einführungen ist das Problem weniger die Installation des Betriebssystems, sondern die Applikationen, die funktionieren müssen. Dass ein Programm unter Windows 2000 oder XP läuft, heißt noch lange nicht, dass es unter Windows 7 läuft. Es gibt einige Dinge, die unter Windows 7 für eine Anwendung tabu sind, beispielsweise dürfen Sie nicht in bestimmte Registry-Bereiche schreiben. Nun können Sie bei vielen Applikationen davon ausgehen, dass sie funktionieren werden: Office 2007 wird beispielsweise kein Problem sein, aber für manch andere Anwendungen, die sich auf den PCs Ihres Unternehmens finden werden, dürfte es nicht so simpel sein.

Es gibt also mehrere Aufgaben:

- Sie müssen feststellen, welche Anwendungen auf den Systemen Ihres Unternehmens laufen.
- Sie müssen festlegen, welche Applikationen unbedingt funktionieren müssen.
- Optimalerweise können Sie auf Informationen zugreifen, die bereits andere Admins aufgezeichnet haben. Genauso wäre es fair, wenn Sie Ihre Erkenntnisse ebenfalls der Gemeinschaft zukommen ließen.

- Weiterhin benötigen Sie eine Anwendung, in der Sie strukturiert die Kompatibilitätsaufgaben abarbeiten können.

Das Application Compatibility Toolkit hilft Ihnen bei diesen Aufgaben. Es ist allerdings kein Zauberkasten, der Ihnen bei jedem gefundenen Programm sagt, ob es auf Windows 7 läuft und was Sie gegebenenfalls tun müssen, um es eben doch noch zum Laufen zu bringen. Das Application Compatibility Toolkist ist ein Werkzeug, das Ihnen hilft, substanzielle Arbeit strukturiert zu erledigen.

Ich werde Ihnen nachfolgend die Grundlagen des Produkts vorführen.

9.1.1 Installation

Das *Application Compatibility Toolkit* (ACT) steht im Microsoft DownloadCenter bereit – zur Unterstützung der Suche zeigt Abbildung 9.1 die Seite, die Sie finden müssen.

Bevor Sie sich in die Installation stürzen, müssen Sie eventuell ein wenig an den Voraussetzungen arbeiten: Das ACT benötigt für die Daten einen SQL Server 2005 oder 2008. Die kostenlose Version genügt. Falls sich in Ihrer Umgebung ein SQL Server findet, können Sie diesen natürlich verwenden.

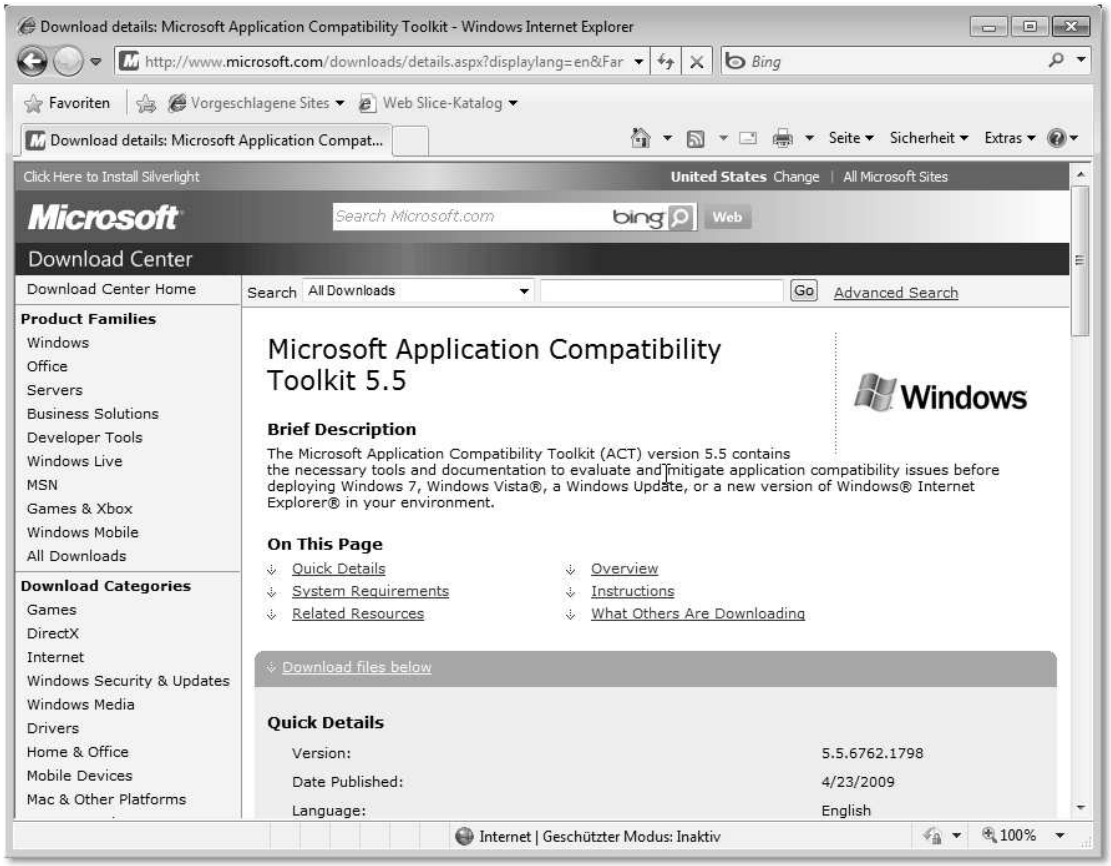


Abbildung 9.1 Das »Application Compatibility Toolkit« steht im Download Center bereit.

Die eigentliche Installation ist unproblematisch. Nach Abschluss der Installation sind diverse neue Menüpunkte im Startmenü vorhanden (Abbildung 9.2).

Starten Sie zunächst den Application Compatibility Manager. Sofern das der erste Start ist, wird ein Assistent Sie durch die Ersteinrichtung führen, zu der auch das Erzeugen der Datenbank gehört.

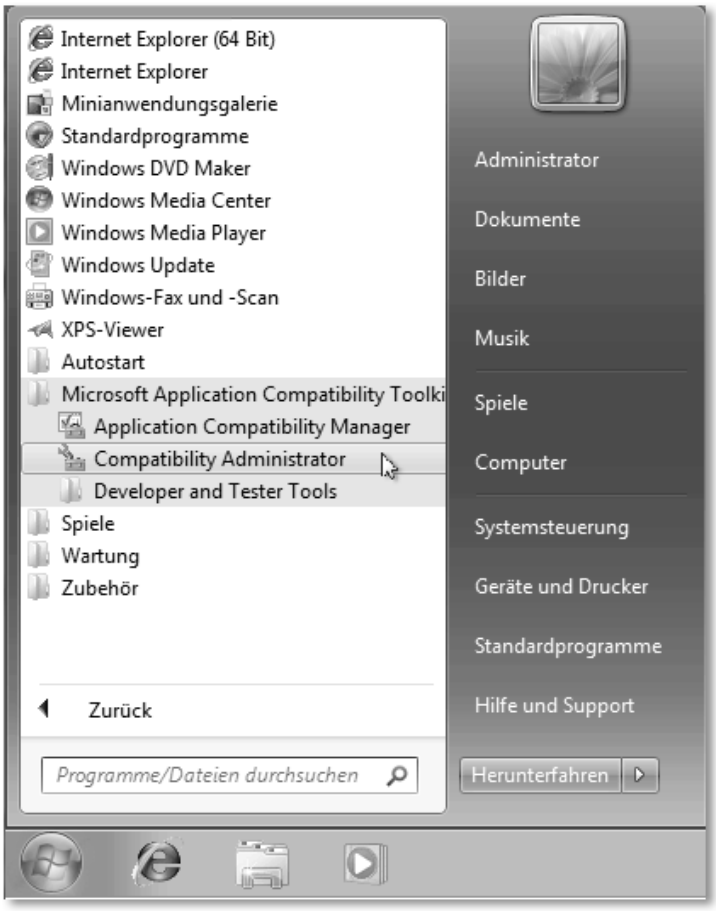


Abbildung 9.2 Nach der ACT-Installation stehen etliche Optionen zu Verfügung. Starten Sie zunächst den »Application Compatibility Manager«.

Hier ein kurzer Überblick über die im Verlauf des Assistenten notwendigen Eingaben:

- Im ersten Dialog müssen Sie entscheiden, ob Sie eine Enterprise configuration vornehmen möchten oder nur Reports anzeigen wollen.

  Wählen Sie die erste Option, um das erste bzw. einzige System aufzusetzen (Abbildung 9.3). Die zweite Option wird verwendet, wenn Sie ein zusätzliches System aufsetzen möchten, das nur für die Anzeige von Berichten verwendet wird.

- Auf der zweiten Dialogseite des Assistenten wählen Sie zunächst den zu verwendenden SQL Server aus. Dann können Sie einen Datenbanknamen bestimmen (frei auswählbar) und durch einen Klick auf CREATE eine Datenbank anlegen (Abbildung 9.4, links).
- Für die Sammlung der Daten von den zu überwachenden Clients wird eine Dateifreigabe benötigt. In dem auf Abbildung 9.4 rechts gezeigten Dialog können Sie einen lokalen Pfad auswählen. Die zugehörige Freigabe wird dann automatisch erzeugt.

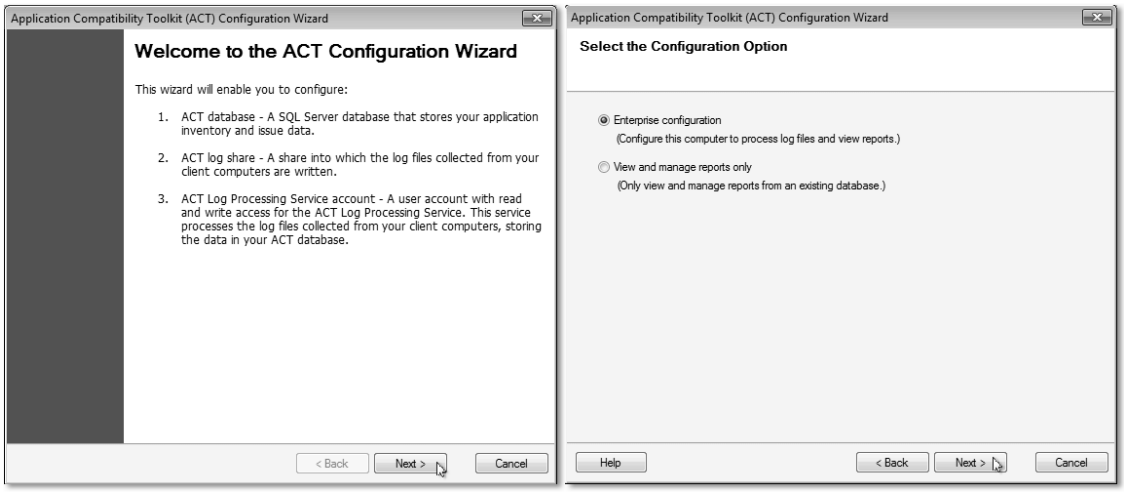


Abbildung 9.3 Entscheiden Sie sich für die »Enterprise configuration«.

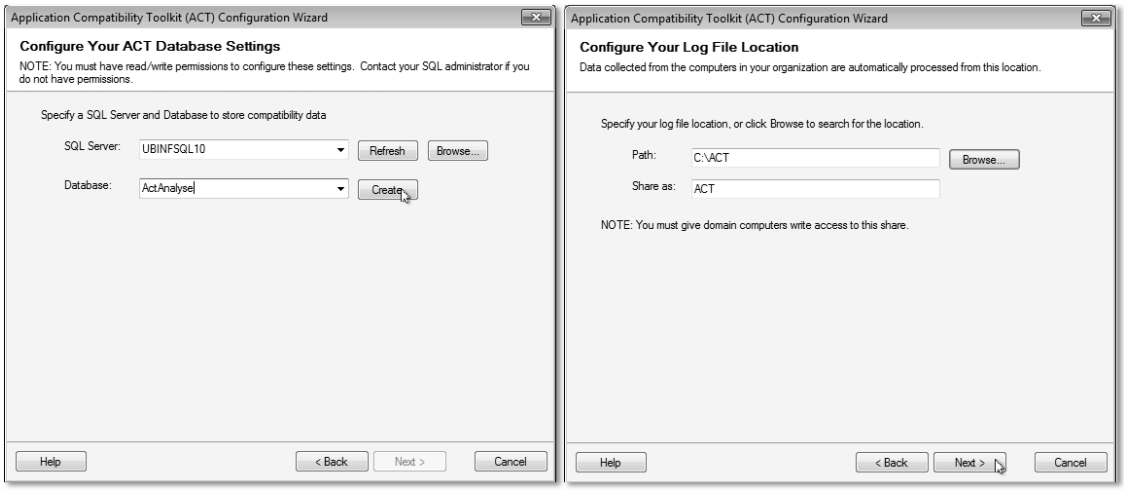


Abbildung 9.4 Legen Sie eine neue Datenbank an, und bestimmen Sie einen Freigabepfad für die Datensammlung.

- Der nächste Dialog legt fest, mit welchem Benutzerkonto die von den Clients übermittelten Informationen verarbeitet werden sollen. Da dieses Konto auch auf den SQL Server zugreifen muss, kommt LOCAL SYSTEM nur dann in Frage,

wenn der SQL Server auf derselben Betriebssysteminstanz wie die sonstigen ACT-Komponenten installiert ist.

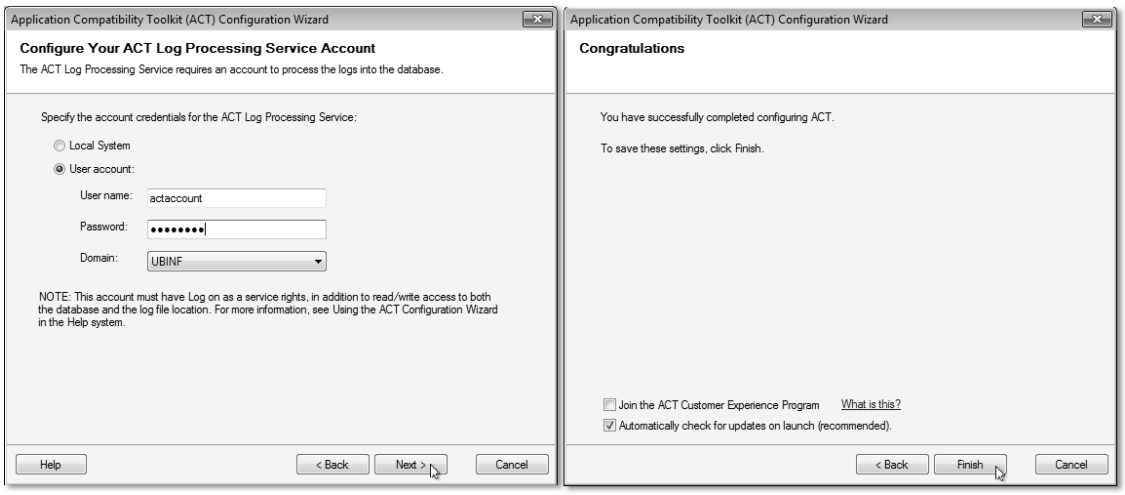


Abbildung 9.5 Bestimmen Sie das Konto, mit dem die von den Clients übermittelten Informationen verarbeitet werden.

9.1.2 Daten sammeln

Nach Abschluss des Assistenten sind Sie schon mittendrin in der Arbeit – die zu erledigenden Phasen sind (Abbildung 9.6):

- Collect – Sammeln Sie Informationen über die in Ihrer Umgebung vorhandenen Anwendungen.
- Analyze – Analysieren Sie die vorhandenen Anwendungen, legen Sie die Wichtigkeit der einzelnen Anwendungen für Ihr Unternehmen fest, und profitieren Sie von den Erkenntnissen anderer Benutzer.
- Test and Mitigate – Testen Sie Applikationen, und finden Sie Lösungen und Workarounds.

Der erste Schritt ist das Erstellen eines Pakets zur Datensammlung. Das Funktionsprinzip ist im Grunde genommen recht simpel:

- Aus den Konfigurationseinstellungen, die Sie im folgenden Dialog vornehmen, wird ein MSI-Paket erstellt.
- Dieses Paket wird auf die zu untersuchenden Computer verteilt. Das kann entweder per Hand erfolgen oder von einer Softwareverteilung durchgeführt werden.
- Die installierte Anwendung beginnt dann mit dem Sammeln von Daten.

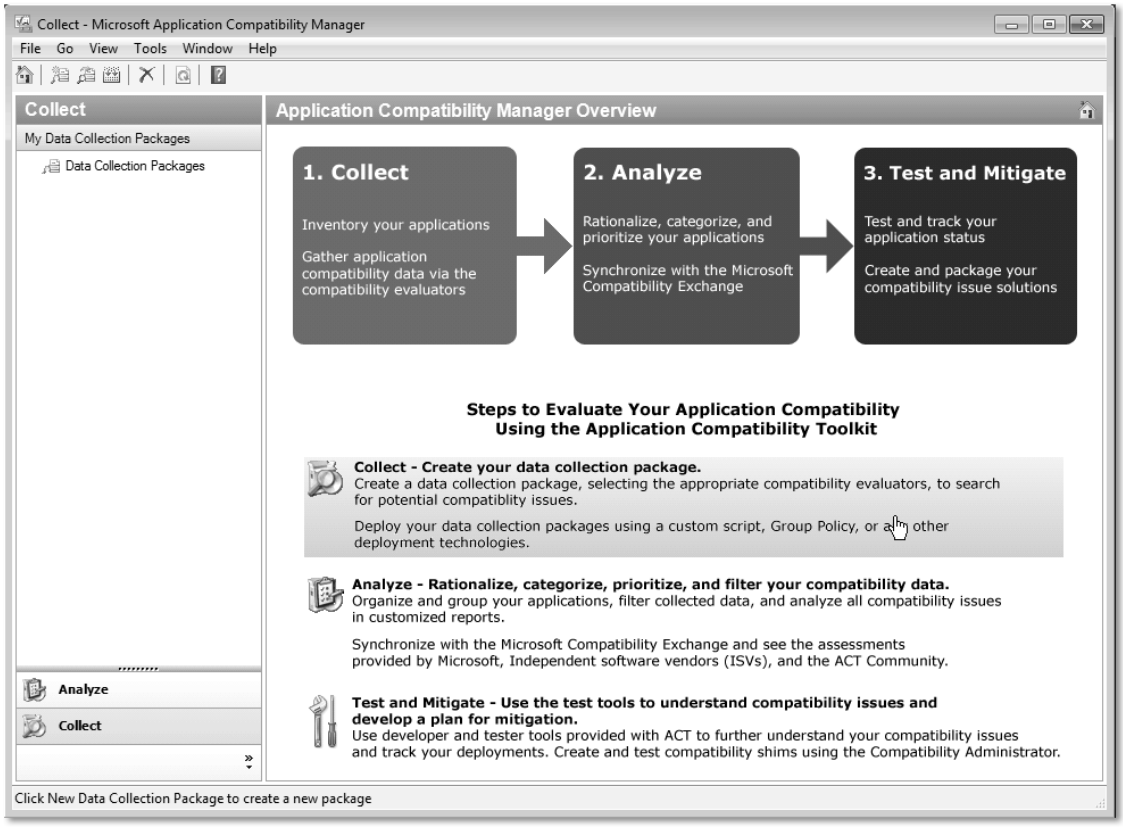


Abbildung 9.6 Nach Abschluss des Assistenten können Sie direkt mit der Arbeit beginnen: Sammeln – Analysieren – Testen.

Den Konfigurationsdialog für das Installationspaket für den »Datensammler« sehen Sie auf Abbildung 9.7:

- Sie können angeben, welchen Kompatibilitätsfall Sie untersuchen möchten. Sie können zwischen der Einführung eines neues Betriebssystems oder der Verteilung von Updates wählen.

  Ein Klick auf die Schaltfläche ADVANCED führt Sie zu dem auf Abbildung 9.8 gezeigten Dialog, mit dem Sie zusätzliche Testverfahren angeben können.
- Im nächsten Abschnitt können Sie festlegen, wann mit der Datensammlung begonnen werden soll. Dies kann direkt nach Abschluss der Installation oder zu einer bestimmten Uhrzeit sein.

  Interessant ist weiterhin die Frage, wie lange die Datensammlung durchgeführt werden soll. Dazu müssen Sie wissen, dass zunächst das Software-Inventar ermittelt wird. Danach werden die gestarteten Anwendungen »beobachtet«, um zu schauen, ob diese Aktionen durchführen, die unter Windows 7 problematisch sind – beispielsweise ob die Anwendungen in bestimmte Registry-Bereiche schreiben. Die Datensammlung sollte so lange durchgeführt werden, dass man davon ausgehen kann, dass jede einigermaßen relevante Appli-

kation einmal gestartet wurde. Der vorbelegte Wert von drei Tagen gilt zwar als ein akzeptabler Kompromiss; Applikationen, die nur einmal im Monat gestartet werden, beispielsweise zur Lohnabrechnung, erwischen Sie so aber vermutlich nicht unbedingt. Wählen Sie also lieber einen längeren Datenerfassungszeitraum. Da Sie mehrere Pakete zur Datensammlung anlegen können, ist durchaus ein »Feintuning« möglich.

Weiterhin können Sie definieren, wie oft Updates an das ACT-System gesendet werden sollen. Der kürzeste Zeitabstand ist zwei Stunden – durch die Wahl eines längeren Zeitraums wird das Ergebnis nicht genauer, Sie kommen nur schneller an Daten.

- Im nächsten Block können Sie die Freigabe angeben, in die der Client die gesammelten Daten kopieren soll.
- Im letzten Konfigurationsabschnitt können Sie ein LABEL vergeben. Sinn und Zweck: Wenn Sie mehrere unterschiedliche Datensammlungspakete erstellen, beispielsweise eines für PCs im Vertrieb, im Engineering, im Service etc., helfen Labels dabei, die Daten auseinanderzuhalten – Sie können später danach filtern.

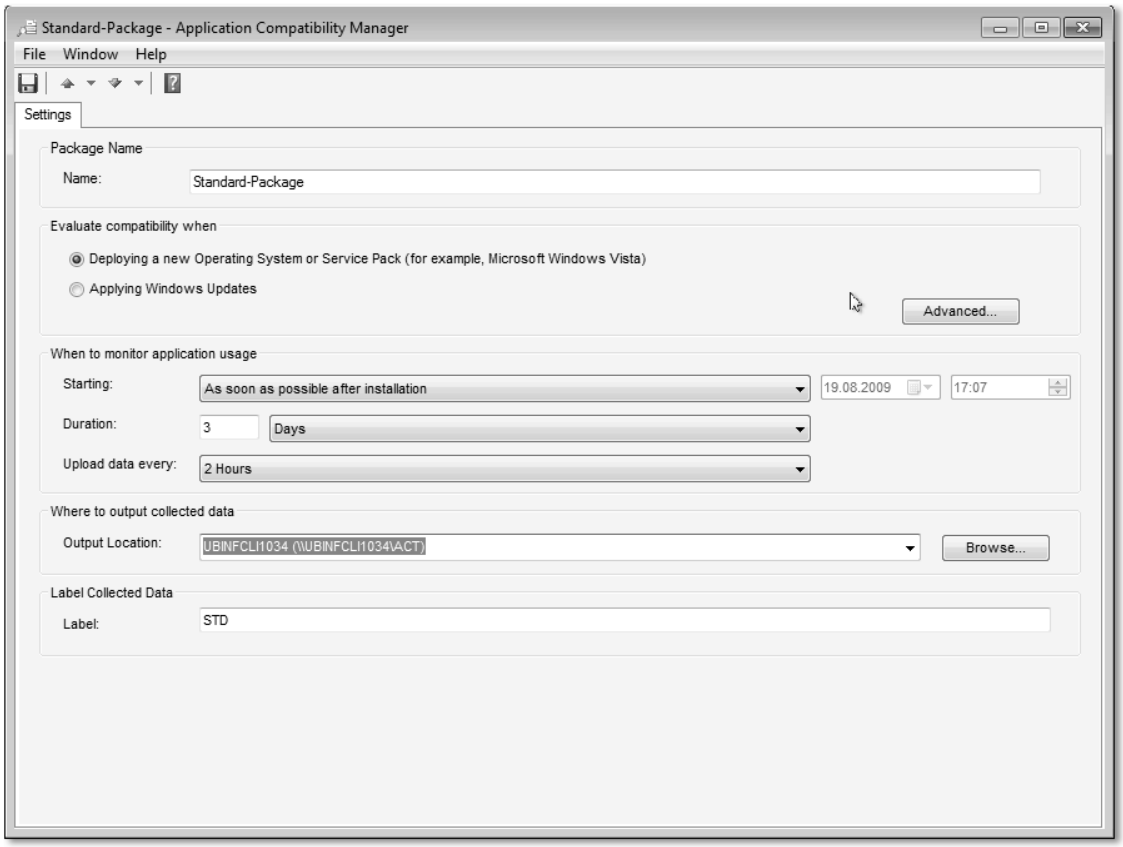


Abbildung 9.7 Definition eines Packages, das für die Sammlung der Anwendungsinformationen verwendet wird

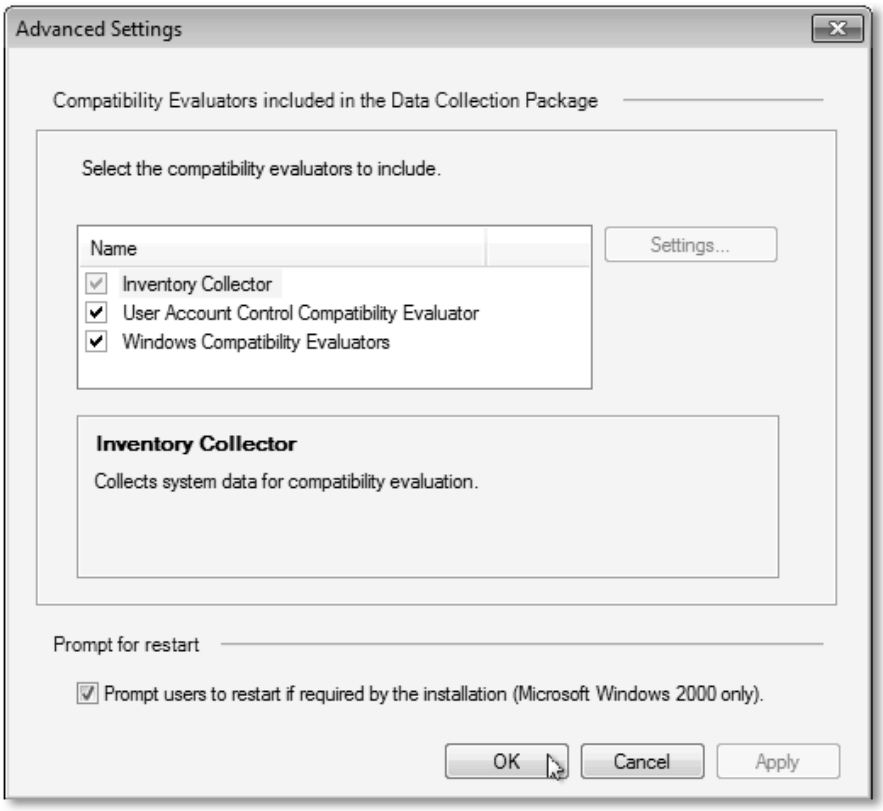


Abbildung 9.8 Die Feineinstellungen für die Überprüfung der Anwendungen

Wenn Sie alle Eingaben vorgenommen haben, können Sie zum Speichern auf das Speichern-Symbol (Diskette links oben) klicken. Es öffnet sich ein Dialog, in dem Sie das zu erzeugende MSI-Paket speichern können: Geben Sie dazu einen prägnanten Namen ein, wählen Sie ein Verzeichnis aus – und los! Das MSI-Paket wird zusammengestellt und steht dann zur Installation bereit (Abbildung 9.9).

Das MSI-Paket können Sie einerseits natürlich von Hand installieren, andererseits können Sie es per Gruppenrichtlinie oder mit einer Softwareverteilungslösung verteilen.

Wenn Sie als CURRENT VIEW die Einstellung BY STATUS wählen und auf das angezeigte Package klicken, erhalten Sie eine detaillierte Statusanzeige. Sie können erkennen, auf welchen PCs der Agent installiert worden ist und wann er sich mit neuen Daten gemeldet hat.

Wenn Sie den Aktualisierungszeitraum auf zwei Stunden gestellt haben, werden Sie erkennen, dass jeder PC alle zwei Stunden einen Eintrag erzeugt (Abbildung 9.10).

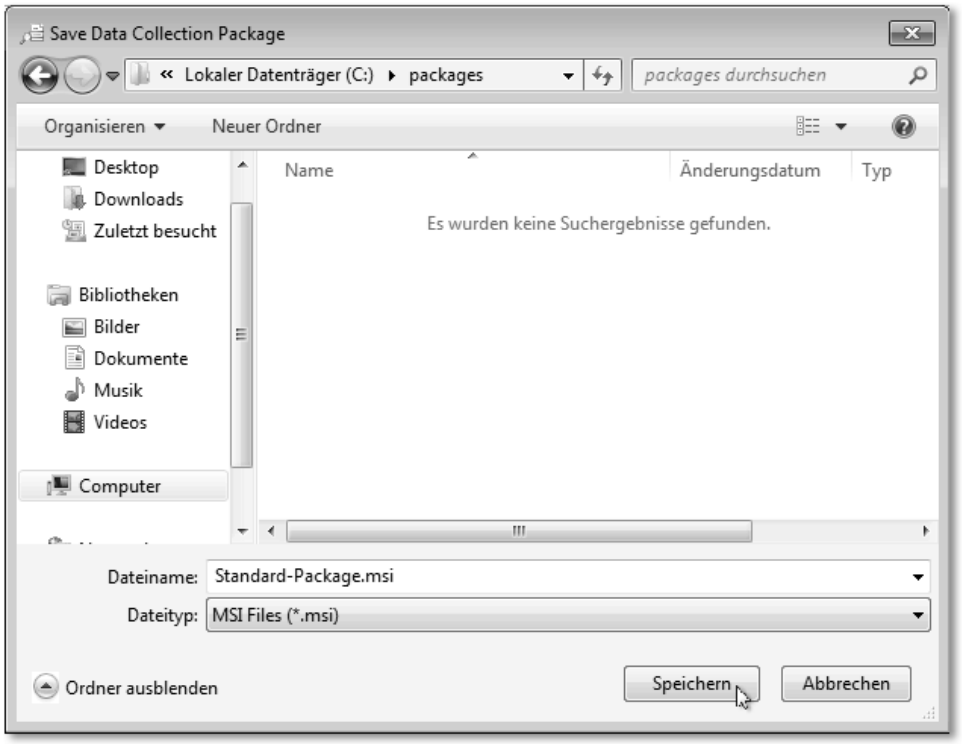


Abbildung 9.9 Ein MSI-Paket wird erzeugt. Dieses kann manuell installiert oder automatisch verteilt werden.

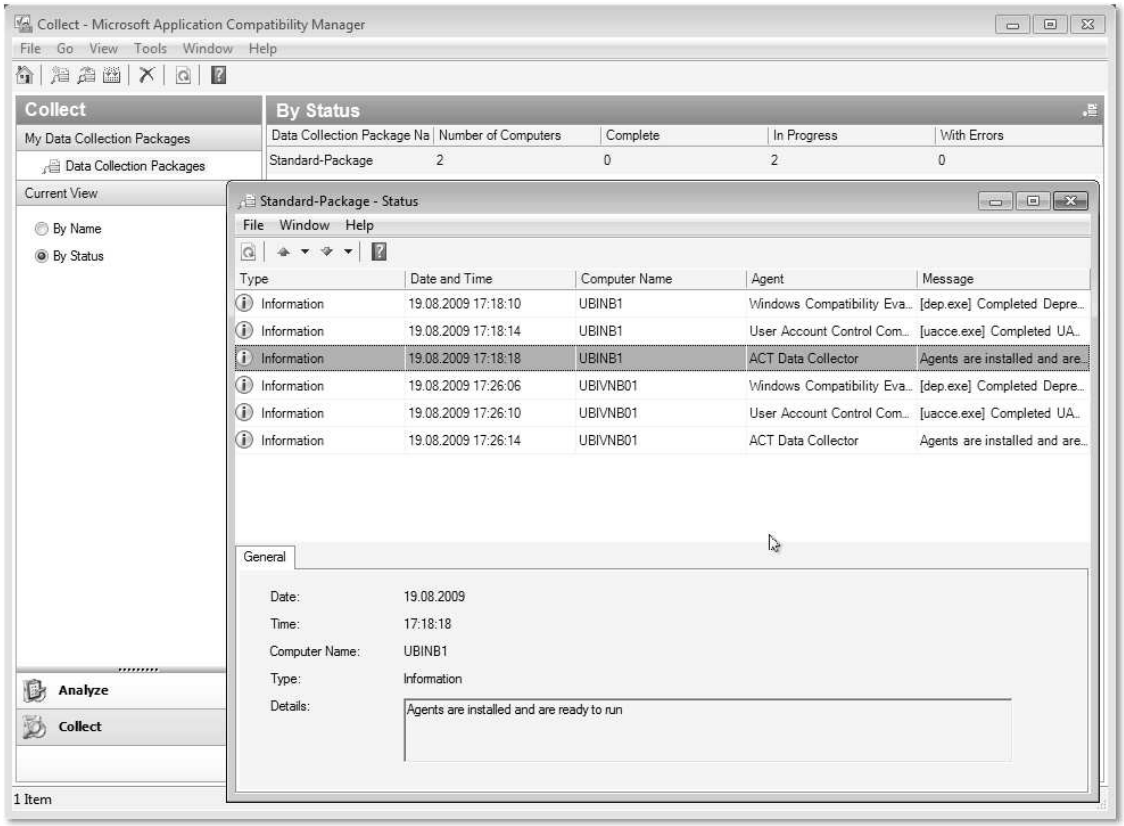


Abbildung 9.10 Sie können überwachen, ob der Agent installiert worden ist und sich meldet.

9.1.3 Analysieren – Community-Informationen

Kurz nachdem die Agenten installiert worden sind und den Betrieb aufgenommen haben, werden Sie im Programmbereich ANALYZE eine Liste der gefundenen Anwendungen sehen (Abbildung 9.11). Vermutlich werden Sie erstaunt sein, wie viele Programme auf den PCs vorhanden sind. Sie können die Liste natürlich beliebig sortieren und filtern.

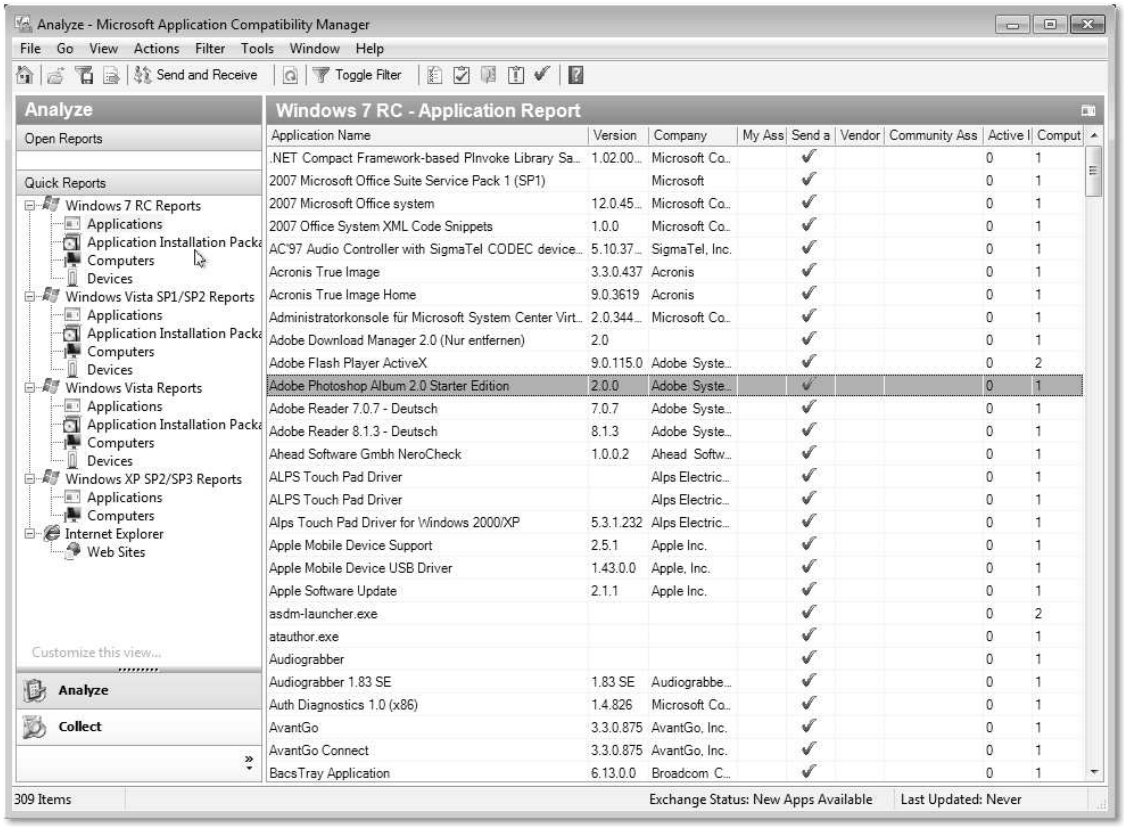


Abbildung 9.11 Kurz nach dem Start können Sie die Inventarinformationen einsehen.

Nun haben Sie zwar eine Liste der vorhandenen Programme, sind aber auch noch keinen deutlichen Schritt weitergekommen. Sie sind natürlich nicht der Erste, der vor diesem Berg von Anwendungen steht. Microsoft hat ein Community-Konzept implementiert:

- Sie stellen Ihre Ergebnisse der »Allgemeinheit« zur Verfügung.
- Sie bekommen die Ergebnisse der anderen zu Ihrer Verwendung.

Auch wenn Sie bisher noch keine Ergebnisse haben, können Sie den Datenaustausch durchführen lassen. Klicken Sie dazu auf SEND AND RECEIVE (siehe Abbildung 9.11 in der Menüleiste). Es werden dann Ihre Ergebnisse der Kompatibilitätsuntersuchung an Microsoft gesendet, und Sie bekommen die bereits von Microsoft zusammengetragenen Ergebnisse zurück.

Weitere Informationen

Wie Sie Ihre Untersuchungsergebnisse in ACT erfassen, sehen Sie ein wenig später.

Bevor die Daten gesendet werden, erscheint eine Information, welche Daten an Microsoft gesendet werden (Abbildung 9.12). Sie können sich auch eine detaillierte Liste der Programme anzeigen lassen, über die Informationen übermittelt werden (Abbildung 9.13). Selbstverständlich können Sie bestimmte Programme von der Übermittlung ausschließen. Sie bekommen dann aber auch keine Informationen, die andere Administratoren zu diesen Programmen ermittelt haben.

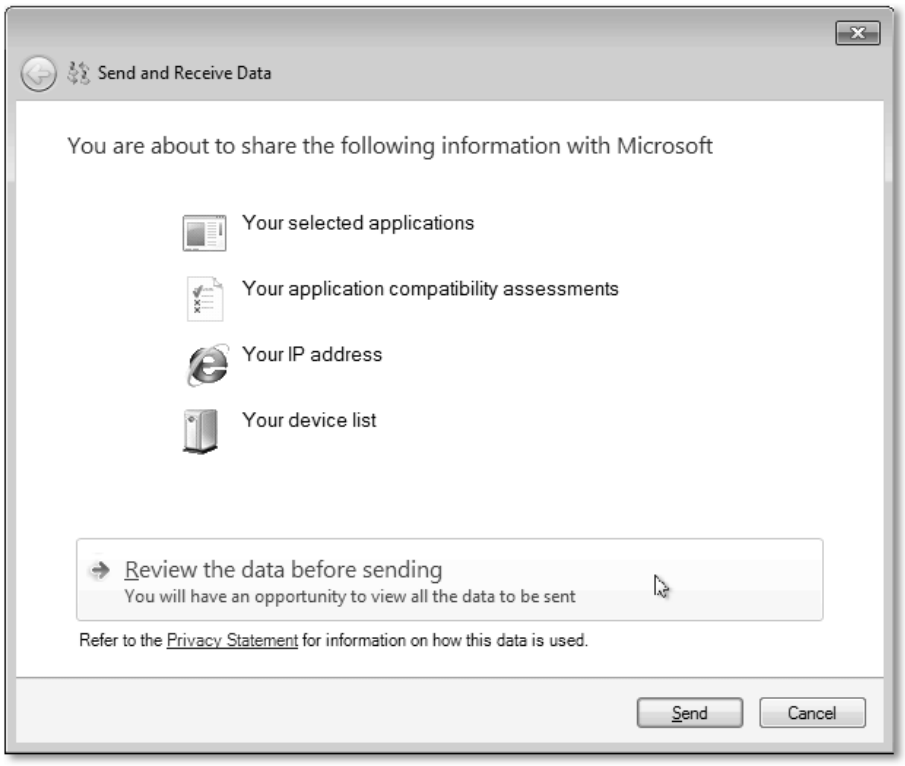


Abbildung 9.12 Wenn Sie den Datenaustausch aktivieren, werden Sie darüber informiert, welche Daten an Microsoft gesendet werden.

Die Datenübertragung wird einige Sekunden in Anspruch nehmen (Abbildung 9.14). Wenn Sie nach dem Abschluss nochmals die Anwendungsliste anschauen, werden Sie feststellen, dass etliche Programme eine Community-Wertung haben. Sie bekommen also frei Haus die Ergebnisse geliefert, die sich andere Administratoren erarbeitet haben. Auf Abbildung 9.15 können Sie sehen, dass der Apple Mobile Device USB Driver erfolgreich auf Kompatibilität mit Windows 7 getestet wurde. Das sind natürlich keine »offiziellen« Ergebnisse – es hat sich aber generell gezeigt, dass die Qualität der Community-Ergebnisse durchweg sehr gut ist. Teilweise finden sich auch Informationen, dass es mit dem Programm Probleme gibt. Nähere Informationen dazu finden Sie auf der Registerkarte Issues.

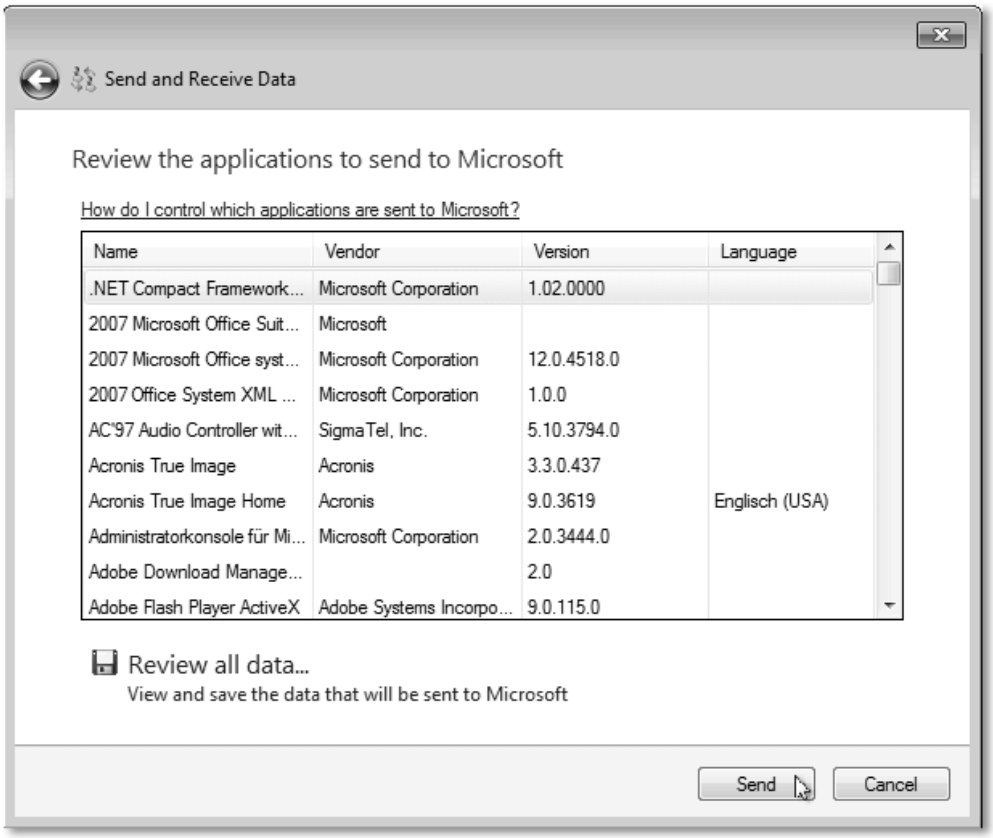


Abbildung 9.13 Sie können kontrollieren, zu welchen Anwendungen Informationen gesendet werden.

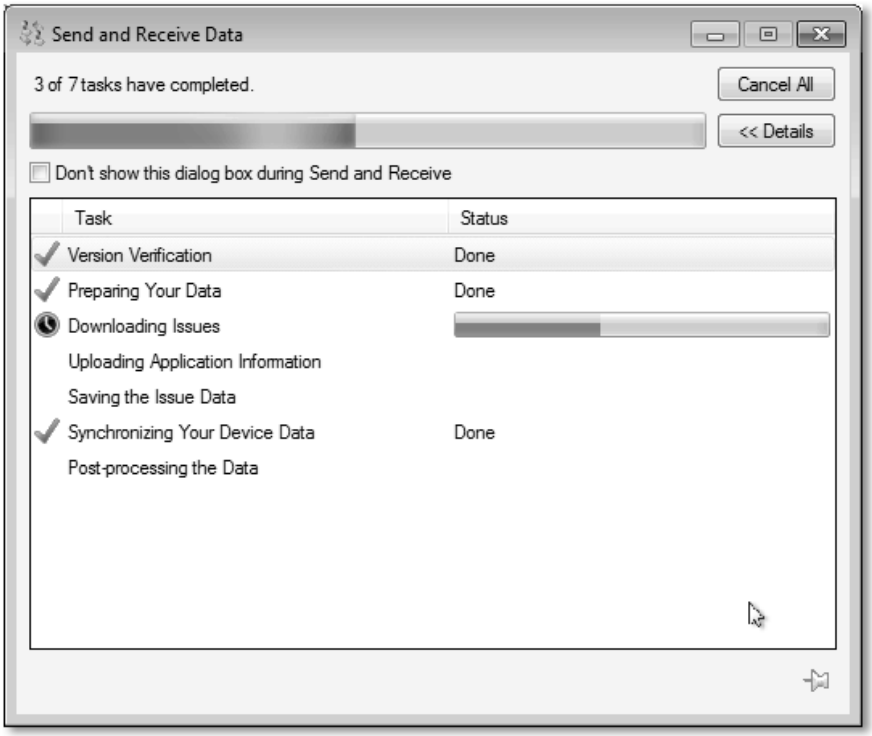


Abbildung 9.14 Die Datenübertragung läuft.

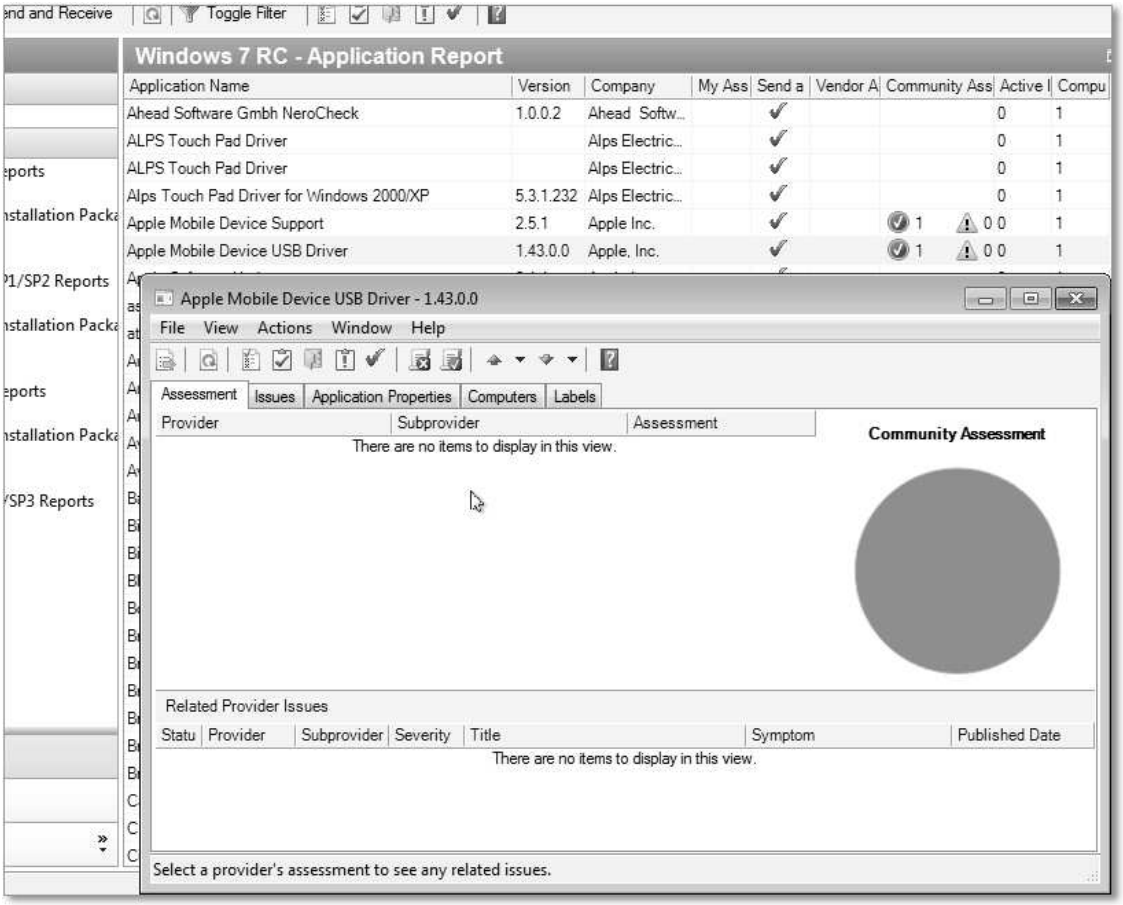


Abbildung 9.15 Es liegen zwar nicht zu allen Programmen Community-Informationen vor – hier wird eine positive Überprüfung angezeigt.

Bei einigen Applikationen findet sich übrigens auch die Information, dass die Applikation von ihrem Hersteller überprüft worden ist – das sind wertvolle Informationen, die momentan aber leider selten sind. Das sieht dann so aus wie auf Abbildung 9.16.

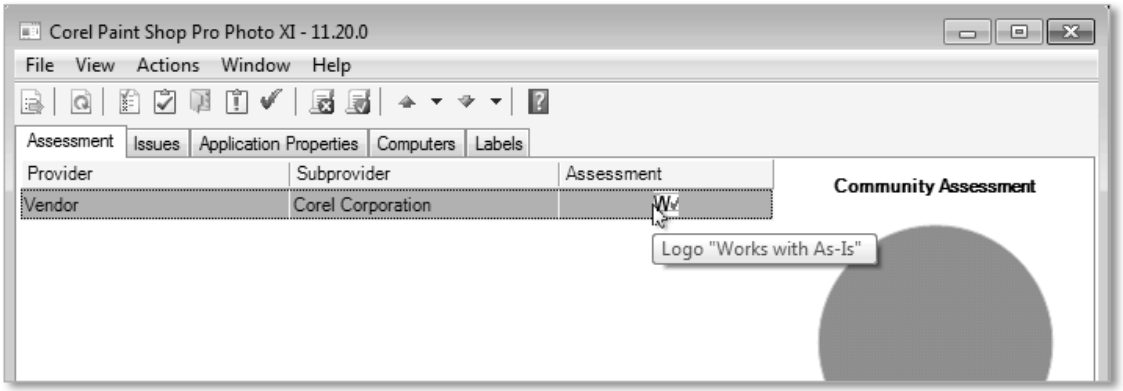


Abbildung 9.16 Zum Teil finden sich Informationen vom Hersteller der Software – in diesem Fall von Corel.

Die Hinweise der anderen Benutzer sind durchaus wertvoll, vermutlich können Sie einen Teil Ihrer Kompatibilitätsprobleme (oder vielleicht auch eben Nicht-Probleme) recht schnell abhaken.

Nicht vergessen!

Eine Community kann nur funktionieren, wenn jeder, der etwas weiß oder herausgefunden hat, seine Informationen mit dem Rest der Welt teilt. Im Klartext: Vergessen Sie nicht, auch noch einmal auf Send and Receive zu klicken, wenn Sie die Ergebnisse Ihrer eigenen Kompatibilitätstests im ACT eingetragen haben.

9.1.4 Analysieren – automatisch ermittelte Probleme

Es gibt etliche Kompatibilitätsprobleme, die automatisch ermittelt werden können, beispielsweise wenn eine Applikation in Bereiche schreibt, die in Windows 7 für eine im User-Mode laufende Applikation tabu sind.

Wenn auf einem PC, der von einem ACT-Agenten überwacht wird, eine Anwendung gestartet wird, werden einige Informationen aufgezeichnet. Auf Abbildung 9.17 sehen Sie einige Erkenntnisse zum Adobe Reader 7.07, der auf einem PC mit Windows XP gestartet wurde. Es gibt gleich drei Probleme mit der Registry, die nicht Windows 7-konform genutzt wird:

- Es wurde ein geschützter Registry-Key geöffnet.
- Es wurde in einen geschützten Registry-Key geschrieben.
- Es wurden Informationen im Zweig HKEY_LOCAL_MACHINE gespeichert.

Diese Aktionen sind in Windows XP kein Problem, wohl aber in Windows 7 und übrigens auch in Vista. Sie können also davon ausgehen, dass der Adobe Reader 7.0.7 unter Windows 7 nicht wirklich gut laufen wird.

Wie Sie auf Abbildung 9.17 sehen, gibt es einige Hinweise und Erläuterungen zu dem gefundenen Kompatibilitätsproblem.

Übrigens

UACCE bedeutet übrigens *User Account Control Compatibility Evaluator*.

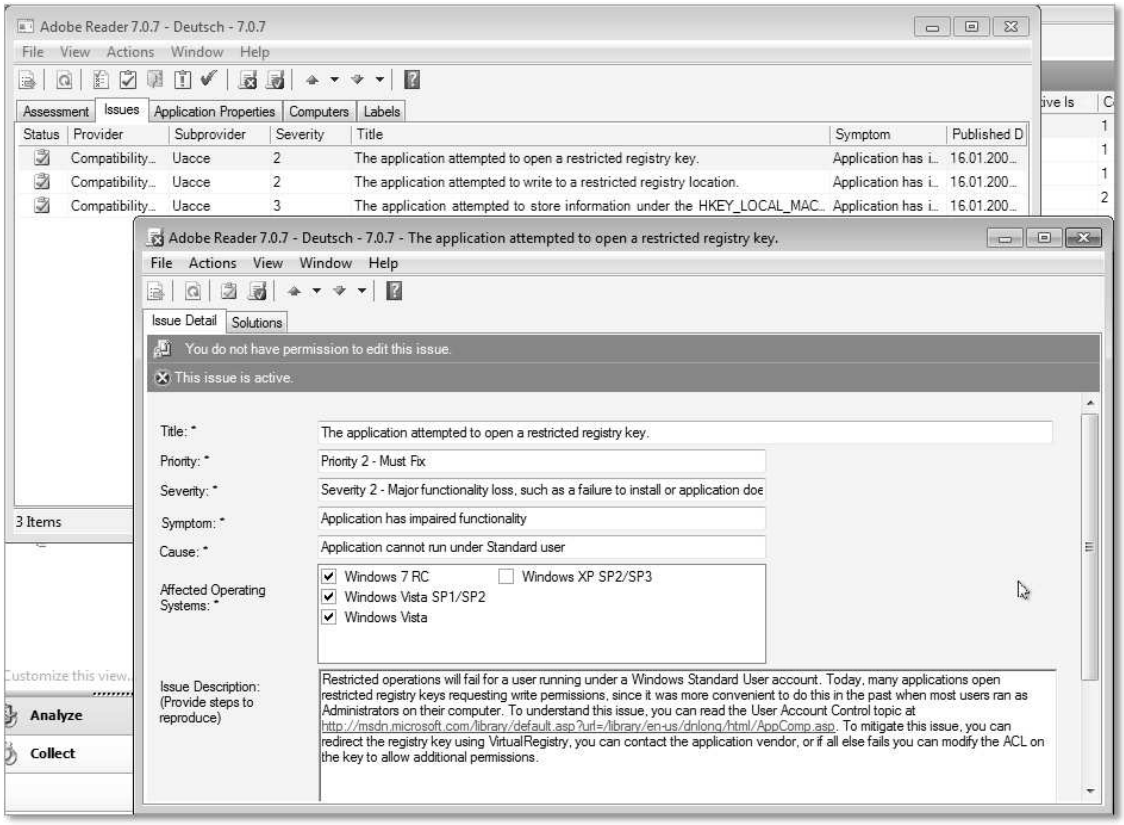


Abbildung 9.17 Diese Probleme wurden automatisch ermittelt. Der Adobe Reader 7 ist für Windows 7 nicht geeignet.

9.1.5 Analysieren – strukturiert selbst machen

Sie haben nun zwei Möglichkeiten gesehen, Kompatibilitätsinformationen zu erhalten: Informationen aus der Community und bei der technischen Prüfung ermittelte Probleme. Nun wird es hinreichend viele Applikationen geben, die nicht in der Community getestet und bewertet worden sind und bei der technischen Ermittlung keine Auffälligkeiten zeigen.

Das »Prinzip Hoffnung« (also dass die Applikation schon stabil unter Windows 7 laufen wird) ist sicherlich keine ideale Vorgehensweise für die Vorbereitung einer Windows 7-Einführung.

Wenn Sie also die eine oder andere Applikation einsetzen, die für das Funktionieren Ihres Unternehmens kritisch ist, sollten Sie diese sorgfältig testen. Das Application Compatibility Toolkit, genauer gesagt der *Application Compatibility Manager*, unterstützt Sie dabei, Ihre Anwendungen strukturiert zu bewerten und die Ergebnisse zu dokumentieren.

Testen ist Handarbeit

An dieser Stelle sei der Hinweis gegeben, dass das eigentliche Testen notwendigerweise solide Handarbeit ist: Sie müssen die Anwendung auf Windows 7 installieren und überprüfen, ob die Installation durchgeführt werden konnte, ob alle Komponenten installiert sind und ob alle Bereiche der Anwendung funktionieren. Das *Application Compatibility Toolkit* enthält ein Untermenü namens Developer and Tester Tools. Dort sind einige Werkzeuge vorhanden, beispielsweise zum Überprüfen, ob eine Anwendung Zugriffe versucht, die administrative Berechtigungen benötigen.

Vereinfacht betrachtet gibt es ja drei Fälle:

- Eine Anwendung läuft problemlos unter Windows 7.
- Eine Anwendung läuft nicht unter Windows 7, und die Anwendung ist nicht kritisch, d. h., man könnte auf sie im Notfall verzichten.
- Eine Anwendung läuft nicht unter Windows 7, sie ist aber unverzichtbar.

Die Grundlage für Ihre Tests ist in jedem Fall die Liste der gefundenen Anwendungen. Im Kontextmenü jeder Anwendung finden Sie einige Menüpunkte, mit denen Sie die einzelnen Anwendungen klassifizieren und Ihre Testergebnisse dokumentieren können (Abbildung 9.18).

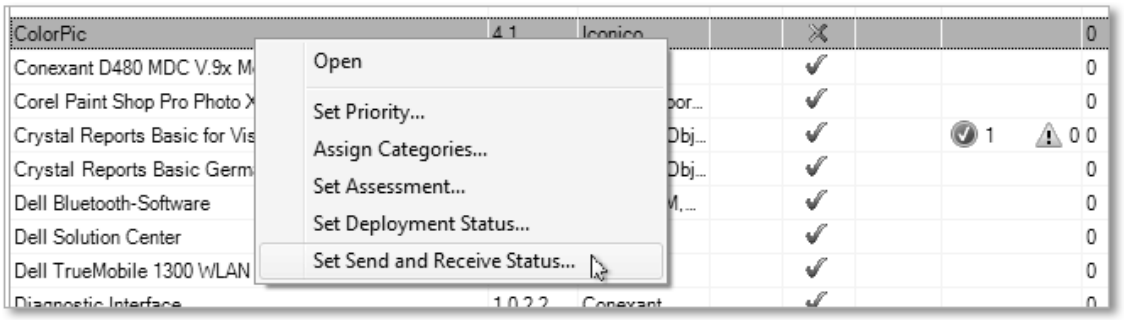


Abbildung 9.18 Im Kontextmenü der Anwendung können Sie einige Einstellungen vornehmen.

Zunächst eine Anmerkung zum Datenaustausch mit Microsoft: Wenn Sie beispielsweise eine selbst erstellte oder für Sie indiviuell entwickelte Anwendung testen und bewerten, möchten Sie die Daten darüber vielleicht nicht unbedingt an Microsoft senden – mit diesen Daten kann ja ohnehin niemand etwas anfangen.

In diesem Fall wählen Sie im Menüpunkt Set Send and Receive Status im Kontextmenü der Anwendung und entscheiden sich für Do not send to Microsoft (Abbildung 9.19). Es wird dann nicht in der Community-Datenbank verzeichnet werden, dass diese Anwendung bei Ihnen in Betrieb ist. Falls Sie auf diese Weise

beispielsweise Microsoft Word 2007 kennzeichnen, erhalten Sie aber auch keine Informationen, die andere Admins über diese Anwendung zusammengetragen haben. Das System »weiß« ja in diesem Fall nicht, dass die Anwendung in Ihrem Unternehmen eingesetzt wird.

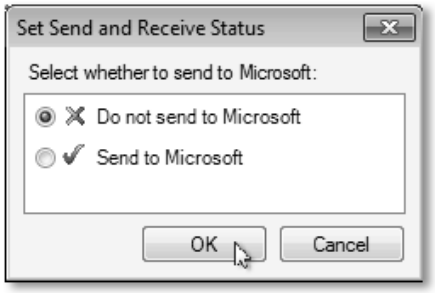


Abbildung 9.19 Sie können festlegen, dass über diese Anwendung keine Informationen an Microsoft gesendet werden sollen.

Die nächste Einstellung betrifft die Wichtigkeit dieser Anwendung (Menüpunkt: Set Priority, Abbildung 9.20). Sie können hiermit die Bedeutung für Ihr Unternehmen festlegen. Diese Einstellung hat zwar keine unmittelbaren Auswirkungen auf Funktionen des Application Compatibility Managers, ist aber beim Auswerten außerordentlich wertvoll: Sie können beispielsweise alle Anwendungen zeigen lassen, die als Business Critical eingestuft sind, aber noch nicht getestet sind oder als nicht-Windows 7-fähig eingestuft werden mussten. Oder Sie filtern die Anzeige so, dass die als Unimportant eingestuften Anwendungen gar nicht mehr in Ihren Arbeitslisten auftauchen.

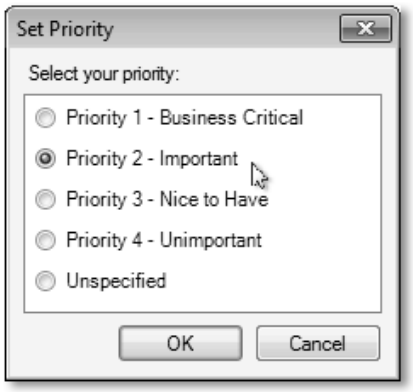


Abbildung 9.20 Bewerten Sie die Bedeutung bzw. Wichtigkeit des Programms für Ihr Unternehmen bzw. Ihre Organisation.

Ebenfalls wichtig für Berichte und Listen aller Art ist die Kategorisierung einer Anwendung. Den auf Abbildung 9.21 gezeigten Dialog erreichen Sie über den Menüpunkt Assign Categories. Wie Sie auf der Abbildung sehen können, lassen sich beliebig eigene Kategorien anlegen, die dann den Anwendungen zugeordnet

werden können. Mögliche Kategorien wären beispielsweise die Abteilung bzw. der Funktionsbereich, in der bzw. dem eine Anwendung eingesetzt wird, oder der IT-Mitarbeiter, der mit der Evaluation betraut ist.

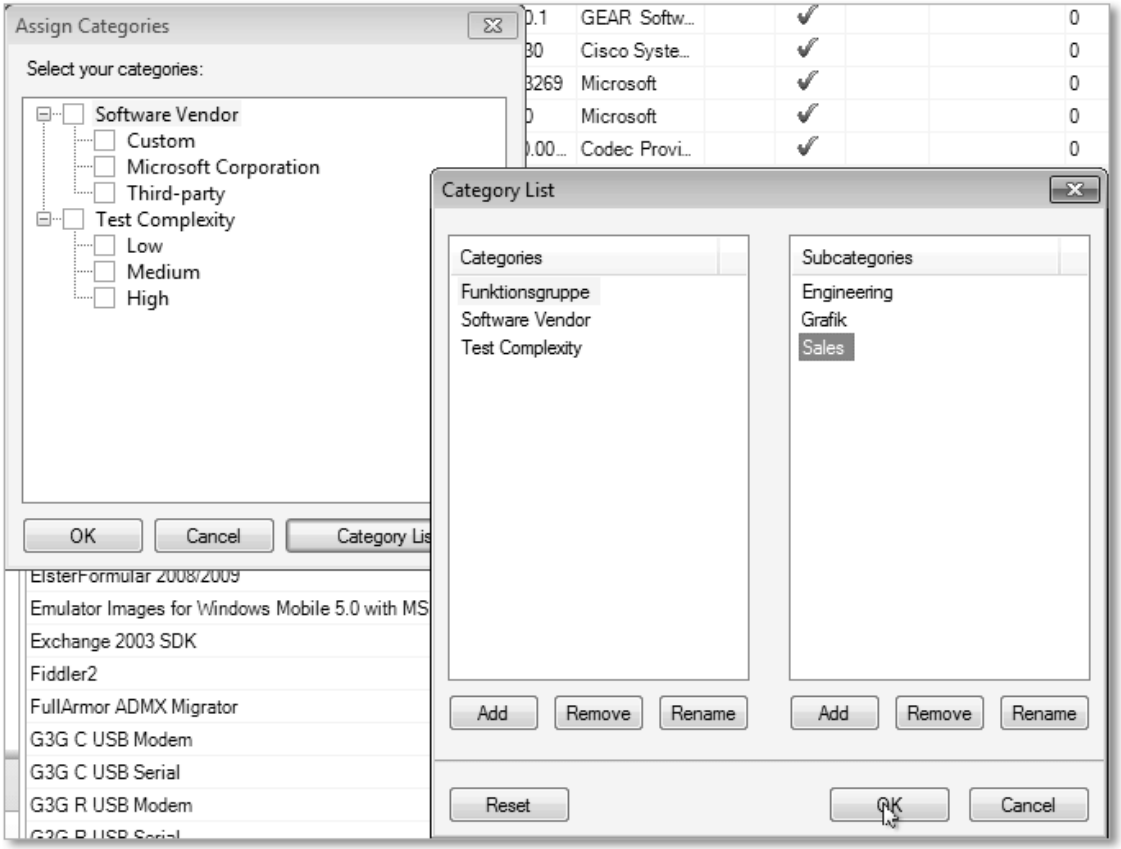


Abbildung 9.21 Die Anwendung kann keiner, einer oder mehreren Kategorien zugeordnet werden.

Den momentanen Status der Untersuchung können Sie in dem Dialog aus Abbildung 9.22 erfassen. In Berichten und Listen lässt sich dann sofort erkennen, welche Anwendung sich gerade im Test befindet.

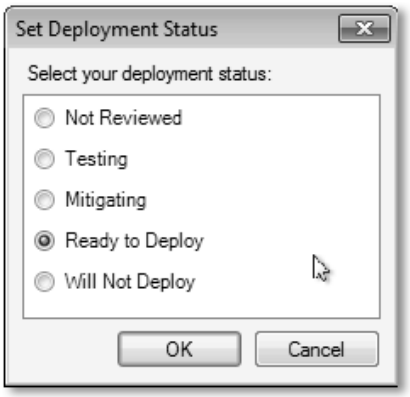


Abbildung 9.22 Hier dokumentieren Sie den derzeitigen Status.

Das endgültige Ergebnis der Untersuchungen können Sie in dem über den Menüpunkt Set Assessment erreichbaren Dialog dokumentieren (Abbildung 9.23).

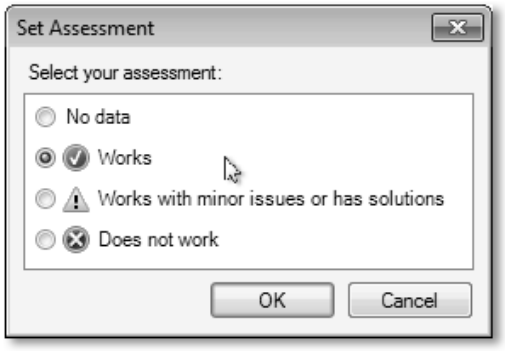


Abbildung 9.23 In diesem Dialog können Sie das Ergebnis Ihrer Überprüfung dokumentieren.

Wenn alle beteiligten Mitarbeiter die Status sorgfältig pflegen, kann der Projektleiter ganz problemlos den Stand der vorbereitenden Untersuchungen einsehen. Zwei mögliche Berichte sind:

- Welche geschäftskritischen Anwendungen befinden sich noch im Teststadium?
- Welche wichtigen oder geschäftskritischen Anwendungen können nicht unter Windows 7 eingesetzt werden?

Application Compatibility Manager

Wer schon einmal an einem größeren Migrationsprojekt mitgearbeitet hat, weiß, dass diese Fragen einerseits für den Projektleiter absolut elementar sind und dass er andererseits an diese Informationen häufig nur schwer kommt: Da werden Excel-Tabellen hin und her geschickt, und Informationen müssen mühsam aus E-Mails herausgesucht werden.

Der *Application Compatibility Manager* ist hier eine enorme Hilfe, da er sozusagen alles aus einer Hand bietet: Erfassung der eingesetzten Programme, einige grundlegende technische Tests, Community-Informationen und eine Oberfläche zur Dokumentation.

Er ist von daher ein Pflichtwerkzeug für jeden Projektleiter!

Häufig genügt es beim Testen nicht, einfach einen Status (»klappt«, »klappt nicht«) einzutragen. Vielmehr müssen Probleme und mögliche Lösungen im Detail dokumentiert werden. Wenn Sie die Eigenschaften einer Anwendung öffnen, existiert eine Registerkarte Issues, auf der im Detail alle Probleme erfasst, beschrieben und klassifiziert werden können. Abbildung 9.24 zeigt die Erfassung eines solchen beim Testen gefundenen Problems. Wie Sie sehen können, existiert auch eine Registerkarte Solutions, in der Lösungen für das Problem eingetragen werden können. Auf diese Weise entsteht eine eigene gut dokumentierte Wis-

sensbasis, die beschreibt, wie Ihre Anwendungen unter Windows 7 erfolgreich installiert und eingerichtet werden können.

Selbstverständlich können Sie nach ungelösten Problemen (Issues) filtern. Auf Abbildung 9.25 sehen Sie, dass es eine Filterbedingung Issues(+) gibt, die mit dem Operator Exists versehen werden kann. Sie können also ganz einfach alle Programme anzeigen lassen, deren Bewertung noch nicht abgeschlossen ist und mit denen es ungelöste Probleme gibt.

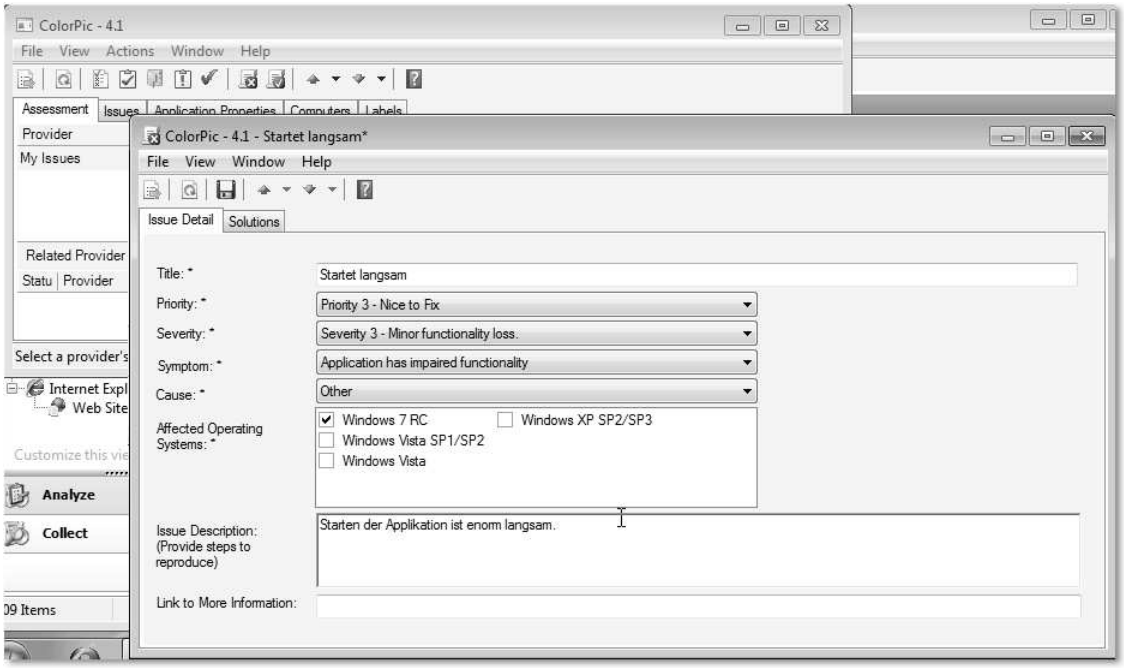


Abbildung 9.24 Gefundene Probleme (Issues) können hier dokumentiert und kategorisiert werden.

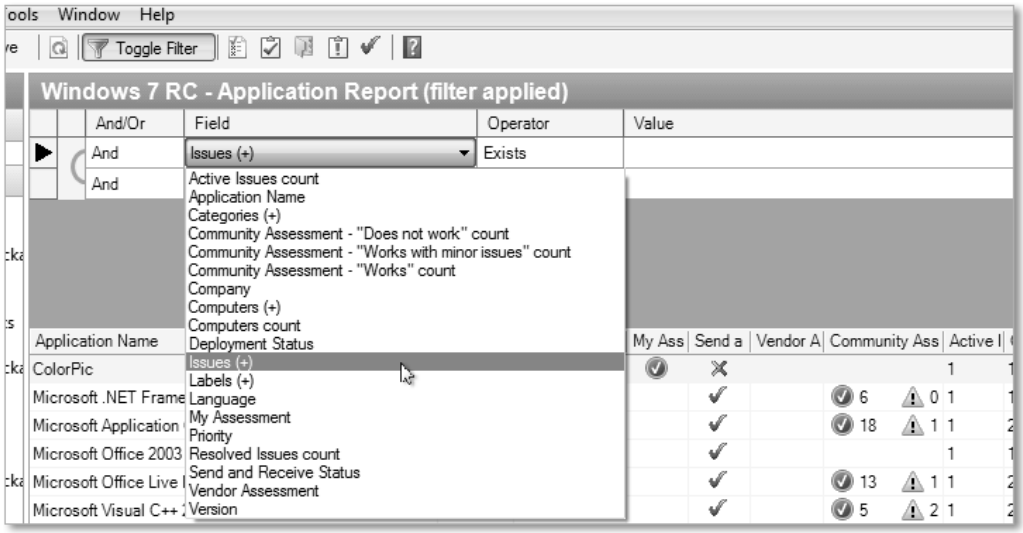


Abbildung 9.25 Sie können beim Filtern nach Applikationen suchen lassen, zu denen Issues vorhanden sind.

9.1.6 Fazit

Die Tatsache, dass es das *Application Compatibility Toolkit* (ACT) gibt, sollte nun nicht den Eindruck vermitteln, dass kaum eine Applikation auf Windows 7 laufen würde. Vermutlich werden die meisten Anwendungen sogar ganz problemlos ausführbar sein. Aber bekanntlich gibt es hinreichend viele technisch »sub-optimale« Anwendungen, die unter Windows 7 Probleme bereiten könnten (!). Bevor Sie mitten im Rollout-Prozess feststellen, dass eine geschäftskritische Anwendung überhaupt nicht läuft und zwei andere nur teilweise funktionieren, sollten Sie lieber eine sorgfältige Testphase vorschalten. Nur so haben Sie die Möglichkeit, Probleme strukturiert anzugehen, und sind nicht darauf angewiesen, hektisch mehr oder weniger schmutzige Workarounds zu »stricken«.

Falls sich die eine oder andere wichtige Anwendung wirklich unter Windows 7 nicht ausführen lässt, gibt es als »Rettung« den XP-Modus, über den ich im nächsten Abschnitt berichten werde.

9.2 Windows 7 XP Mode und Windows Virtual PC

Es ist durchaus denkbar, dass die eine oder andere Anwendung schlicht und ergreifend unter Windows 7 nicht läuft. Das ist übrigens nichts, was man Windows 7 als Nachteil ankreiden müsste. Es verhält sich so, dass zumeist Software betroffen ist, die ohnehin am Rande der Kompatibilitätsrichtlinien programmiert worden ist. Ein Programm darf nicht Benutzerinformationen im Registry-Zweig *HKEY_LocalMachine* speichern oder auf geschützte Bereiche der Registry zugreifen. Unter Windows XP gab es für Software noch deutlich mehr Freiheiten, insbesondere wenn die Benutzer lokale Administratorberechtigungen hatten. Unter Windows 7 (und übrigens auch unter Vista) gelten aber nun andere Regeln, und ein Programm kann eben nicht mehr nach Belieben schalten und walten. Die totale Freiheit für ausführbaren Code hat ja bekanntlich üble Viren- und Trojanerattacken nach sich gezogen – da ist also dringender Handlungsbedarf gewesen.

Sehr positiv ist zu bewerten, dass Microsoft nicht einen »Kompatibilitätsmodus« eingebaut hat, der das Sicherheitssystem aushebelt. Stattdessen wird eine virtuelle Maschine mit einem *Windows XP SP3* auf dem Windows 7-PC gestartet – in dieser Umgebung sollten dann auch die Problemfälle zum Laufen zu bringen sein.

Die aktuelle Version von *Virtual PC* heißt jetzt mit vollem Namen *Windows Virtual PC* und ist die Grundlage für den *XP Mode*. Microsoft hat einige Features eingebaut, die eine recht nahtlose Integration ermöglichen. Zu nennen wären hier insbesondere:

- Für eine in der XP-Umgebung installierte Anwendung werden die Startmenüeinträge in die Windows 7-Umgebung kopiert.
- Für die in der XP-Umgebung laufenden Applikationen gibt es eine Art »Seamless-Mode«, wie er von den Terminaldiensten bekannt ist. Es ist also auf den ersten Blick nicht mehr zu erkennen, dass die Anwendungen nicht nativ in der Windows 7-Umgebung laufen.

Der XP Mode ist für Business-Anwendungen gedacht und nicht etwa, um ältere Spiele zum Laufen zu bringen. Die grafischen Fähigkeiten der virtuellen Umgebung sind nach wie vor vergleichsweise beschränkt. Ebenso wäre zu erwähnen, dass auch grafisch intensive Business-Anwendungen (CAD, CAM, Bildbearbeitung etc.) im XP Mode eher zu enttäuschenden Resultaten führen dürften.

MED-V

In größeren Umgebungen, in denen eben nicht nur fünf bis zehn XP-Mode-Systeme eingeführt werden, stellen sich den Administratoren vermutlich bei dem Gedanken, auf jedem PC eine weitere Plattform managen zu müssen, die Nackenhaare auf. Aber keine Sorge, Microsoft hat auch an Sie gedacht und bietet mit MED-V (*Microsoft Enterprise Desktop Virtualization*) eine Lösung an, um Virtual-PC-Deployments in größeren Umgebungen durchzuführen.

Der XP Mode in der Version, wie sie in diesem Kapitel vorgeführt ist, ist also eher eine Lösung für kleinere Unternehmen oder zumindest für Szenarien, in denen nur wenige Benutzer zur XP-Mode-Umgebung greifen müssen.

9.2.1 Voraussetzungen

Für die Nutzung des XP Modes gibt es Software- und Hardwarevoraussetzungen:

- *Software*: XP Mode setzt ein Windows 7 der Editionen *Professional, Enterprise* oder *Ultimate* voraus.
- *Hardware*: *Windows Virtual PC* setzt voraus, dass der Prozessor Hardwarevirtualisierung unterstützt – das Stichwort ist hier *Intel VT*, wobei das Kürzel für *Virtualization Technology* steht. Die vergleichbare Technologie von AMD heißt *AMD-V* (V wie *Virtualization*).
  Auf Systemen mit Prozessoren, die diese Fähigkeit nicht mitbringen, kann Windows Virtual PC nicht eingesetzt werden.

Standardmäßig dürfte die Virtualisierungsfunktionalität des Prozessors abgeschaltet sein und muss im BIOS aktiviert werden. Die auf Abbildung 9.26 gezeigte Fehlermeldung erscheint in diesem Fall.

Abbildung 9.26 Wenn die Hardwarevirtualisierung nicht aktiviert oder vorhanden ist, kann Virtual PC nicht verwendet werden.

9.2.2 Installation und Einrichtungen

Bei den im August 2009 ausgelieferten Versionen von Windows 7 ist weder *Windows Virtual PC* noch der *XP Mode* vorhanden. Beides können Sie aber im Microsoft Download Center herunterladen.

Die Installation beider Lösungen ist ein Fall von WEITER • WEITER • FERTIG, also absolut unproblematisch (Abbildung 9.27).

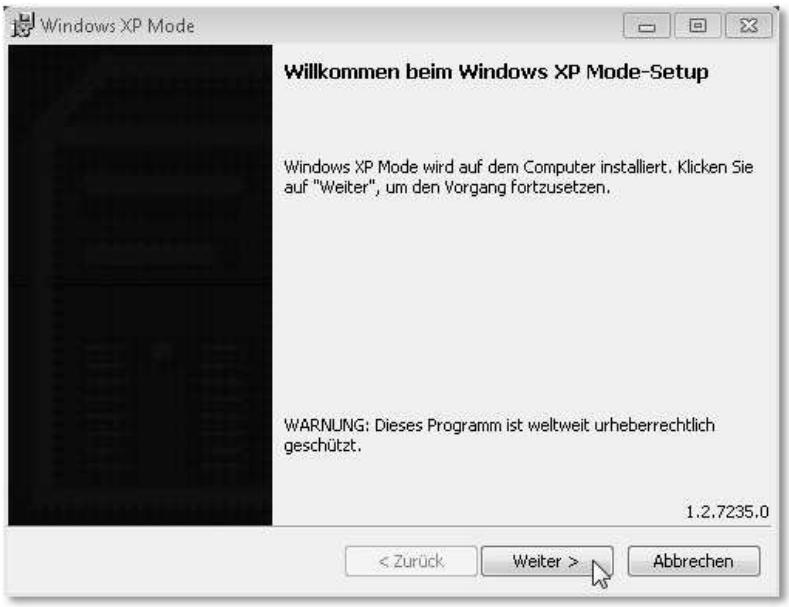


Abbildung 9.27 XP Mode muss separat installiert werden.

Nach Abschluss der Installation finden sich einige neue Einträge im Startmenü (Abbildung 9.28).

Abbildung 9.28 Nach der Installation findet sich der Eintrag für den »Windows XP Mode«. Der erste Start öffnet den Installationsassistenten.

Wenn Sie auf den Menüpunkt Windows XP Mode klicken, startet ein Assistent, der den XP Mode vorbereitet. Viel einzugeben haben Sie allerdings nicht: Es müssen nur der Installationsordner und Anmeldeinformationen eingegeben werden. Für die virtuelle Maschine des XP Mode wird ein Benutzer namens *XPMUser* angelegt. Sie müssen lediglich ein Passwort vergeben (Abbildung 9.29).

Die folgende XP-Mode-Installation dauert ein Weilchen und zeigt dem geneigten Benutzer eine hübsch animierte grafische Einführung in diese Funktion (Abbildung 9.30).

Nach Abschluss der Installation werden Sie ein Szenario wie aus Abbildung 9.31 sehen: Eine virtuelle Maschine mit Windows XP läuft auf dem Windows 7-Host. Sie können ein wenig die virtuelle XP-Maschine erkunden – aber ich möchte Ihnen nun nicht erzählen, was Windows XP so alles kann.

Interessant ist, dass in der virtuellen Maschine die Laufwerke des Windows 7-PCs verbunden sind (Abbildung 9.32). Weiterhin verfügt die virtuelle Maschine über eine Netzwerkverbindung und kann auf USB-Sticks zugreifen – die virtuelle Maschine ist also bereits ohne weitere Nacharbeiten gut integriert.

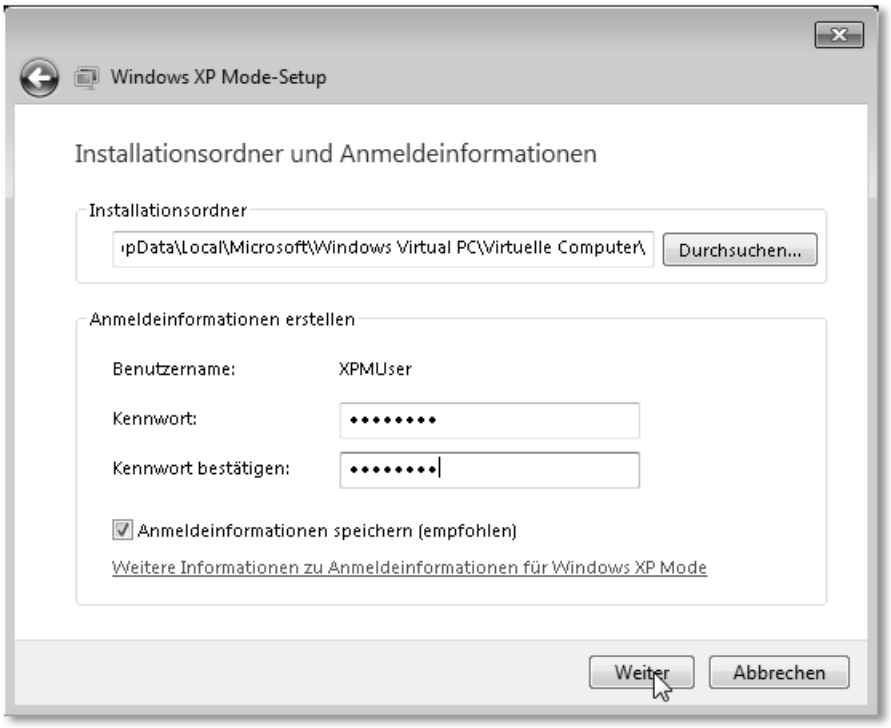


Abbildung 9.29 Der Installationsassistent für XP Mode

Abbildung 9.30 Während des Installationsvorgangs gibt es eine hübsche Animation – eine weitere Konfiguration ist nicht notwendig.

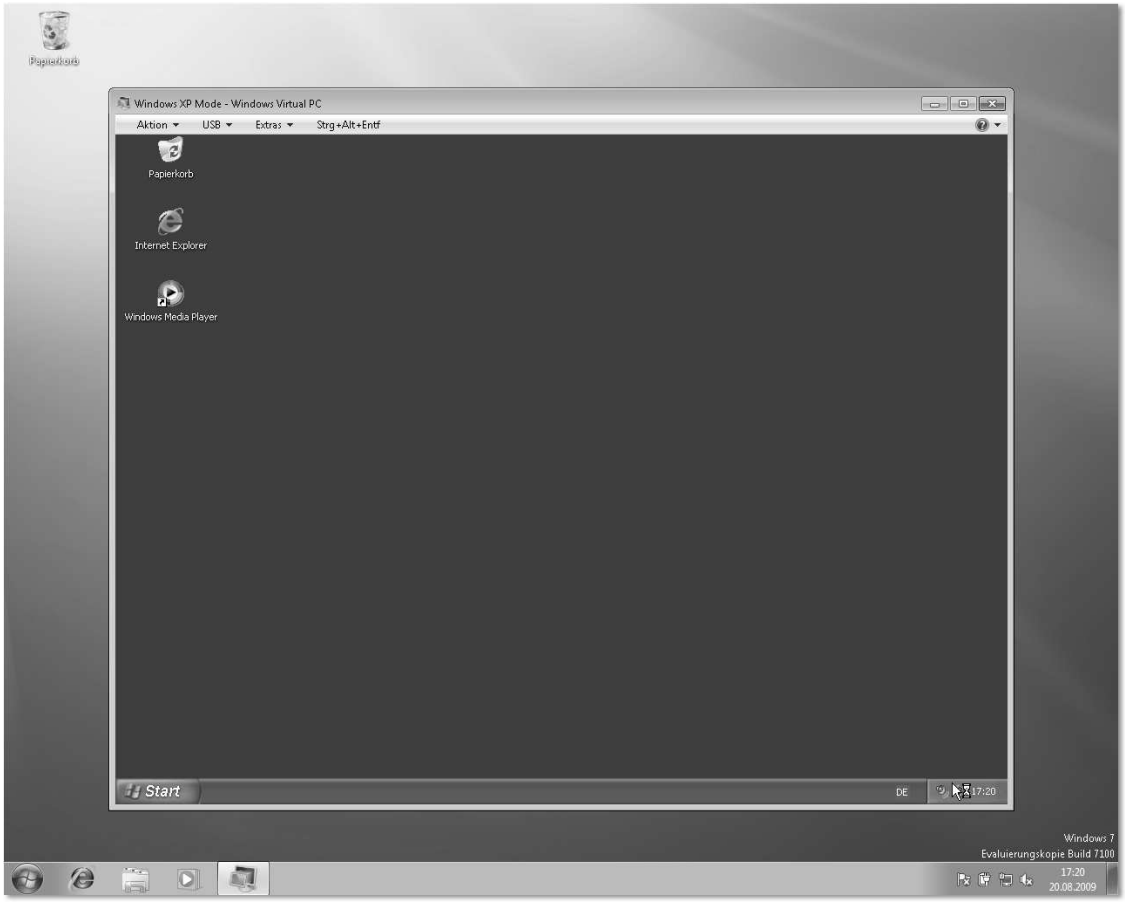


Abbildung 9.31 Nach dem Start wird die virtuelle Maschine mit einem XP SP3 gestartet.

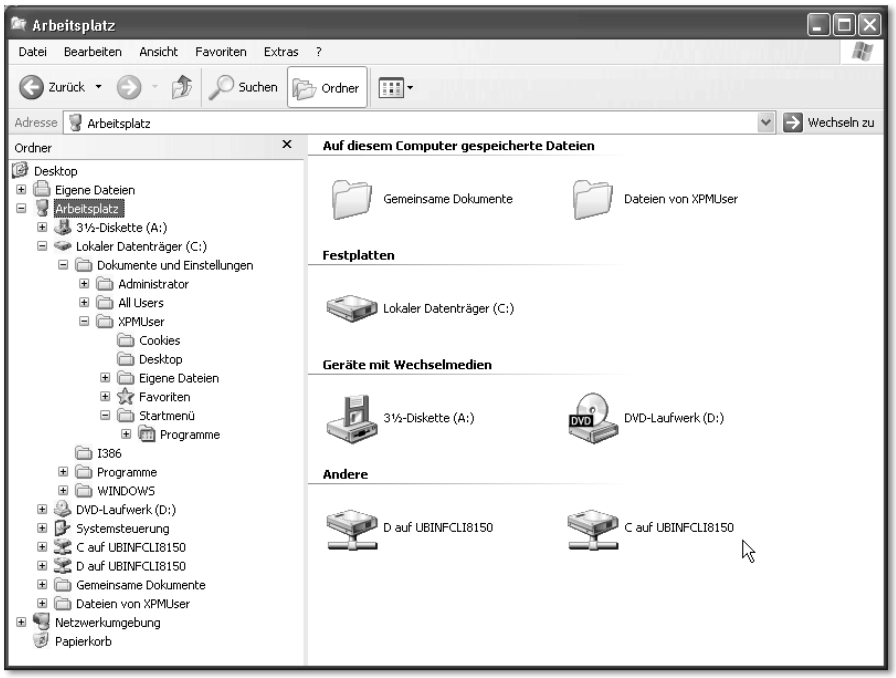


Abbildung 9.32 Der Explorer der virtuellen Windows XP-Maschine. Die lokalen Laufwerke des Host-PCs sind im Zugriff.

9.2.3 Applikation installieren

Da die virtuelle Maschine läuft, können Sie nun die Anwendungen installieren, die nicht nativ auf Windows 7 laufen können. Sie brauchen sich keine Gedanken zu machen – installieren Sie einfach.

Das Ergebnis ist, dass zunächst natürlich die Verknüpfungen der Applikation in der virtuellen Maschine angelegt sind (siehe Abbildung 9.33 links). Gleichzeitig findet sich im Windows 7-Startmenü die Verknüpfung auf die in der virtuellen Maschine installierten Programme. Wie Sie auf Abbildung 9.33 rechts sehen, ist dort die Verknüpfung auf den soeben installierten Acrobat Reader 6.0 hervorgehoben.

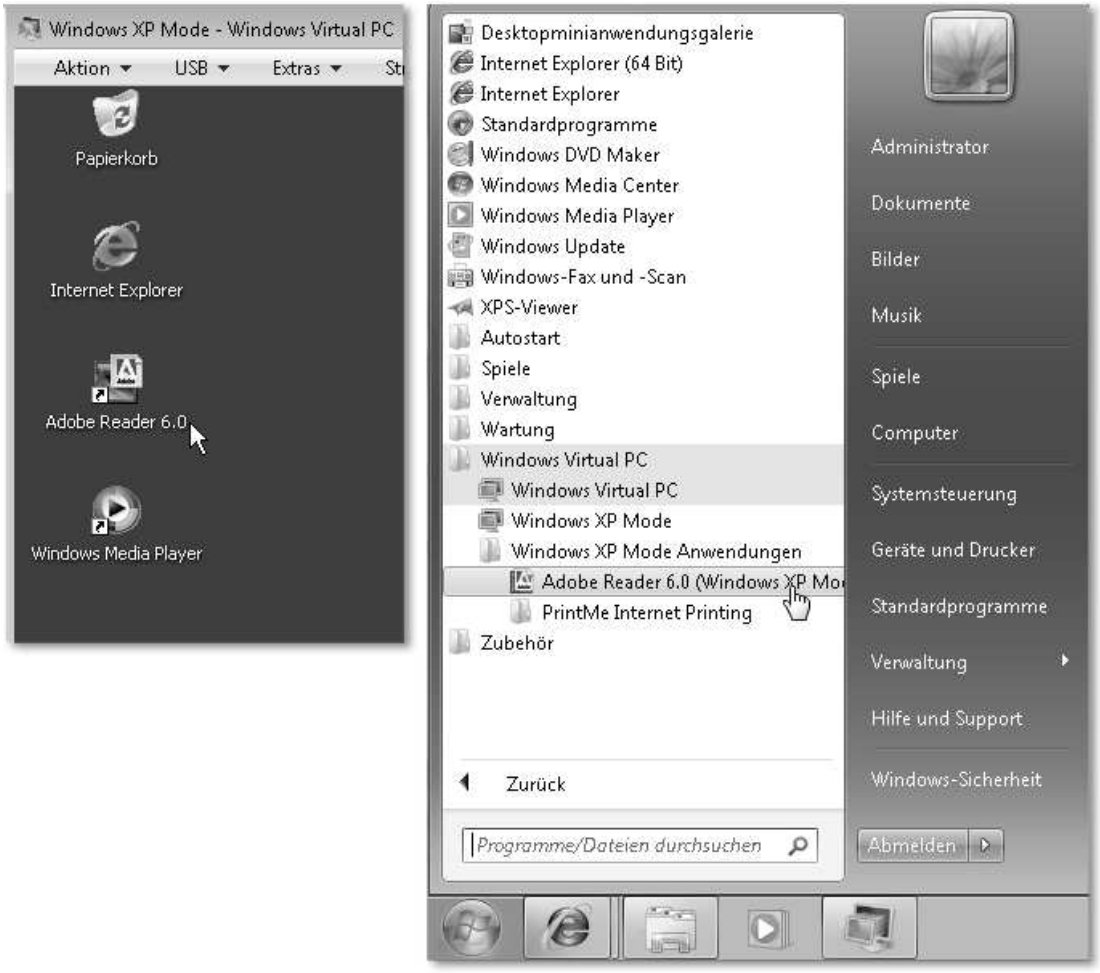


Abbildung 9.33 Nach der Installation einer Anwendung ist auch ein Link im Startmenü des Windows 7-PCs vorhanden.

Nun ist es durchaus interessant, einen kurzen Blick auf die im Windows 7-Startmenü angelegte Verknüpfung zu werfen. Es ist eine »ganz normale« Verknüpfung; interessant ist deren Ziel. Auf Abbildung 9.34 sehen Sie die Verknüpfung, und nachfolgend sehen Sie den vollständigen Eintrag:

%SystemRoot%\system32\rundll32.exe %SystemRoot%\system32\VMCPropertyHandler .dll,LaunchVMSal "Windows XP Mode" "||456be99" "Adobe Reader 6.0"

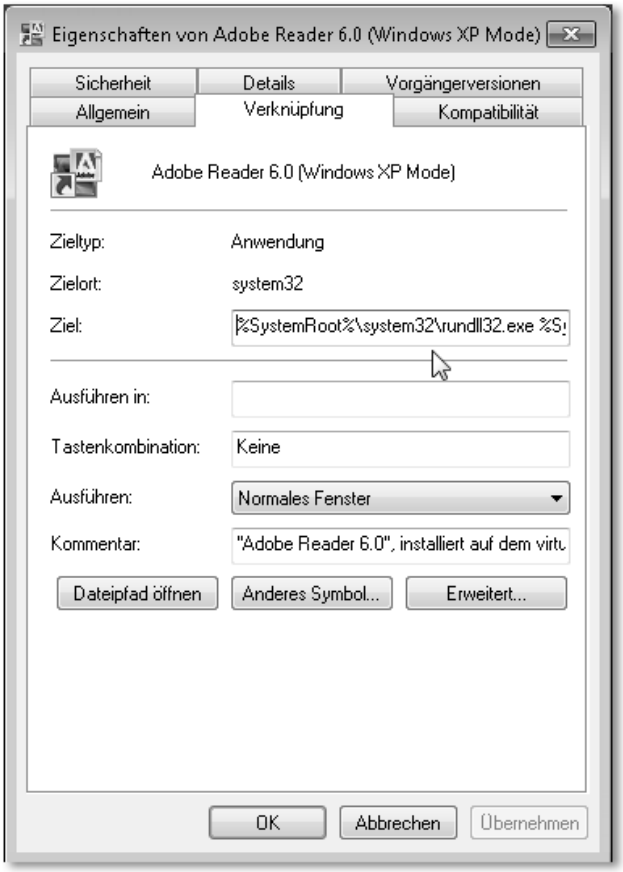


Abbildung 9.34 Die Verknüpfung auf die Anwendung in der virtuellen Maschine

Die Verknüpfung können Sie natürlich beliebig kopieren, auch auf den Desktop legen und alles das tun, was auch mit jeder anderen Verknüpfung möglich ist. Wenn Sie auf die Verknüpfung klicken, wird die Applikation *seamless*« (also ohne dass die virtuelle Maschine direkt sichtbar wird) gestartet.

Beachten Sie, dass die virtuelle Maschine nicht laufen darf, wenn eine Applikation gestartet wird. Wenn sie doch läuft, ist das kein Problem, allerdings wird die auf Abbildung 9.35 gezeigte Meldung erscheinen – Sie können die virtuelle Maschine einfach durch einen Mausklick schließen.

Eine gestartete Applikation ist auf den ersten Blick nicht von einer »wirklich« auf dem Windows 7-PC installierten Anwendung zu unterscheiden. Auf Abbildung 9.36 sehen Sie, wie ein Adobe Reader 6.0 auf einem Windows 7-PC ausgeführt wird – allerdings kommt die Applikation aus der virtuellen XP-Mode-Maschine. Auf den zweiten Blick werden Sie erkennen, dass die Rahmen des Fensters von XP gezeichnet worden sind – und eben nicht von Windows 7. Nichtsdestotrotz ist diese Darstellung eine wirklich gelungene Integration.

Abbildung 9.35 Wenn eine XP-Anwendung startet, darf der virtuelle Computer nicht laufen.

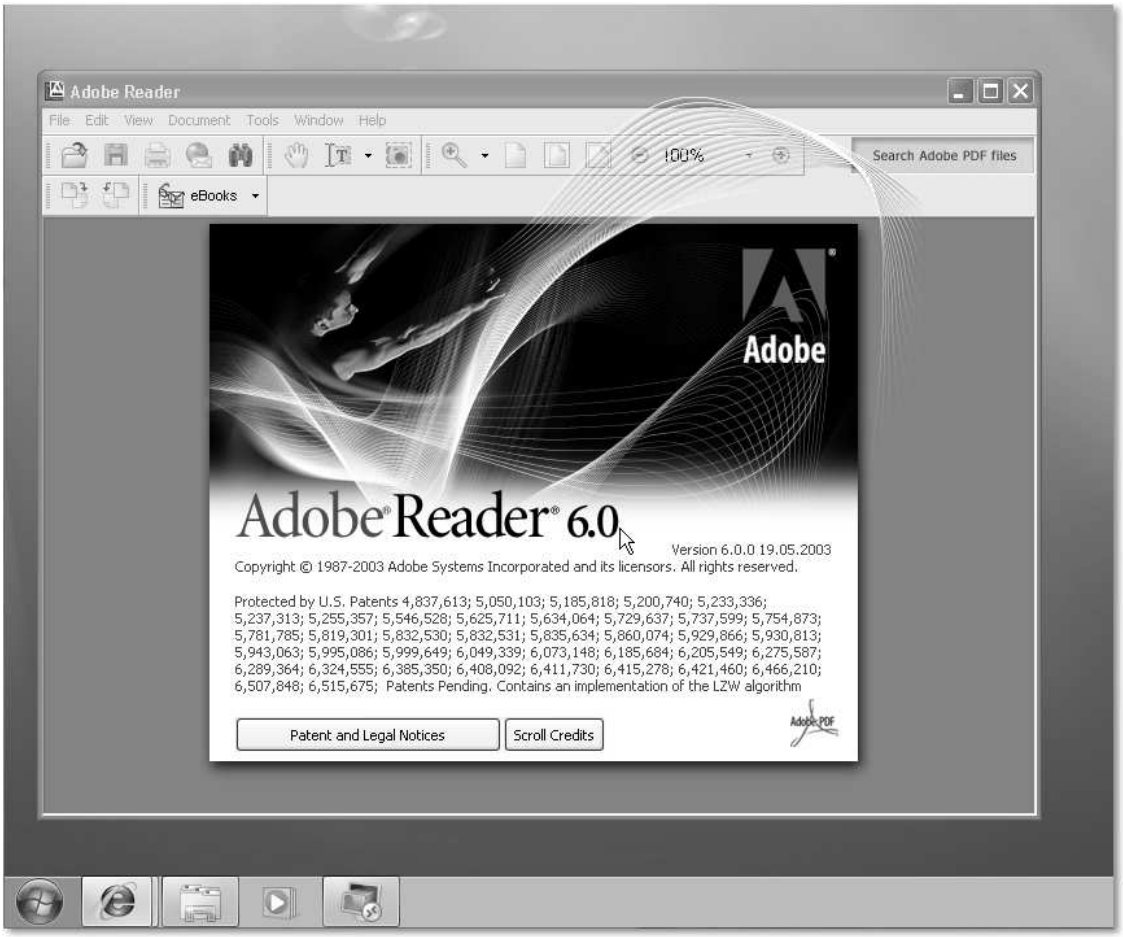


Abbildung 9.36 Adobe Reader 6.0 auf Windows 7

Ein weiteres interessantes Bild möchte ich Ihnen nicht vorenthalten: Auf Abbildung 9.37 sehen Sie, wie ein Internet Explorer 6.0 auf einem Windows 7-PC läuft. Natürlich steckt der XP Mode dahinter. Sie sehen, dass die seamless Ausführung auch mit dem IE funktioniert. Falls Sie also eine Webanwendung bereitstellen müssen, die nur mit einem älteren Internet Explorer läuft: Hier ist die Lösung!

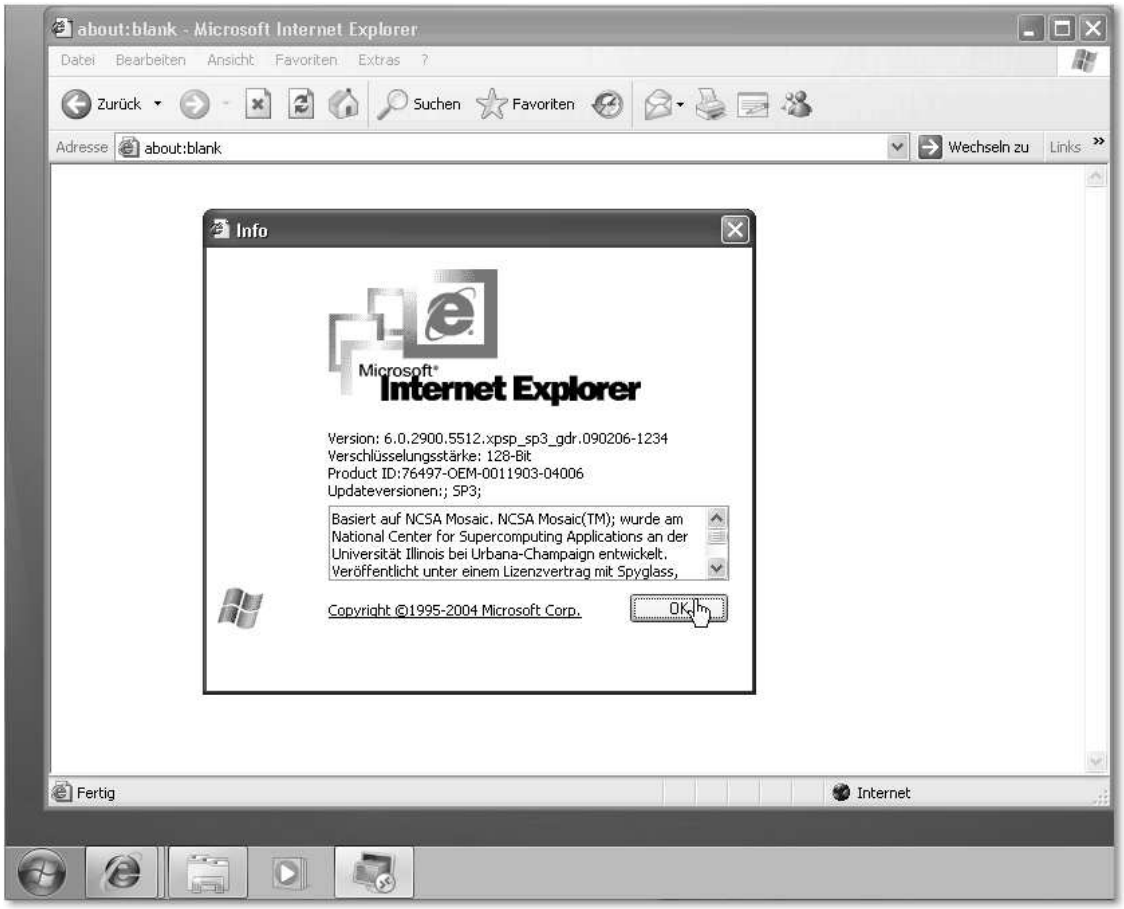


Abbildung 9.37 Auch nicht schlecht: Internet Explorer 6.0 auf Windows 7

9.2.4 XP Mode – Ein paar Nachteile

Der XP Mode hat viele Vorteile, es gibt aber auch einige Nachteile. Diese stellen zwar nicht das Konzept an sich in Frage, Sie sollten sie aber im Hinterkopf behalten.

Zunächst wäre zu erwähnen, dass trotz aller Integration eine weitere virtuelle Maschine vorhanden ist. Diese benötigt einen Virenscanner, muss mit Patches versorgt werden und vieles andere mehr – die üblichen Management-Aufgaben eben.

Weiterhin laufen die Applikationen im XP Mode nicht mit der Windows-Identität des Benutzers, sondern unter einem lokalen Account der virtuellen XP-Maschine.

Wenn eine Anwendung darauf angewiesen ist, unter der Windows-Identität des in Windows 7 angemeldeten Benutzers zu laufen, könnte das zu einem Problem werden: Im besten Fall werden die Anmeldeinformationen nochmals angefragt. Im ungünstigsten Fall läuft die Anwendung schlicht und ergreifend nicht.

9.3 Windows Virtual PC im Allgemeinen

Windows Virtual PC kann natürlich auch zu anderen Zwecken als für den XP Mode verwendet werden – es ist schließlich der Nachfolger von *Virtual PC 2007* und kann somit auch zum Aufbau von Testumgebungen und allem anderen, was in einer virtuellen Umgebung realisiert werden kann, verwendet werden.

Ich möchte nun nicht im Detail den Windows Virtual PC vorstellen – vermutlich dürfte er allen Admins mehr oder weniger gut bekannt sein.

9.3.1 Die Neuerungen

Der *Windows Virtual PC* hat gegenüber der Vorgängerversion *Virtual PC 2007* einige Neuerungen erfahren.

Hier sind die Neuerungen im Telegrammstil:

- Unterstützung des *Windows XP Mode*
- USB-Untertützung: Der Windows Virtual PC leitet den USB-Anschluss in die virtuelle Maschine um.
- Wenn Sie mehrere virtuelle Maschinen ausführen, werden diese in separaten Threads ausgeführt.
- Unterstützung der Zwischenablage zwischen Windows 7-Host und virtuellen Maschinen
- Umleitung von Druckern
- Umleitung von Smartcards in die virtuelle Maschine
- Gemeinsame Nutzung von Plattenbereichen zwischen Windows 7-Host und virtuellen Maschinen
- Unterstützung von höheren Bildschirmauflösungen

Unterschied zu den Virtual-PC-Vorgängerversionen

Ein wichtiger Unterschied zu den Virtual-PC-Vorgängerversionen ist die bereits zu Beginn des Abschnitts 9.2.1 erwähnte Notwendigkeit, dass der Windows 7-PC über einen Prozessor verfügen muss, der Virtualisierung unterstützt.

Auf älterer Hardware kann Windows Virtual PC demnach nicht verwendet werden.

9.3.2 Anlegen einer neuen VM und Konfiguration

Wenn Sie im Windows 7-Startmenü den Menüpunkt Windows Virtual PC auswählen, werden Sie auf den ersten Blick ein wenig überrascht sein – zumindest dann, wenn Sie *Virtual PC 2007*-Anwender gewesen sind. Es gibt nämlich keine eigene Verwaltungsapplikation mehr, vielmehr ist der Virtual PC nun in den Explorer integriert.

Sie sehen die bereits vorhandenen virtuellen Maschinen: in diesem Beispiel zunächst nur die Windows XP Mode-VM. Weiterhin finden Sie einen Menüpunkt zum Erstellen eines neuen virtuellen Computers (Abbildung 9.38).

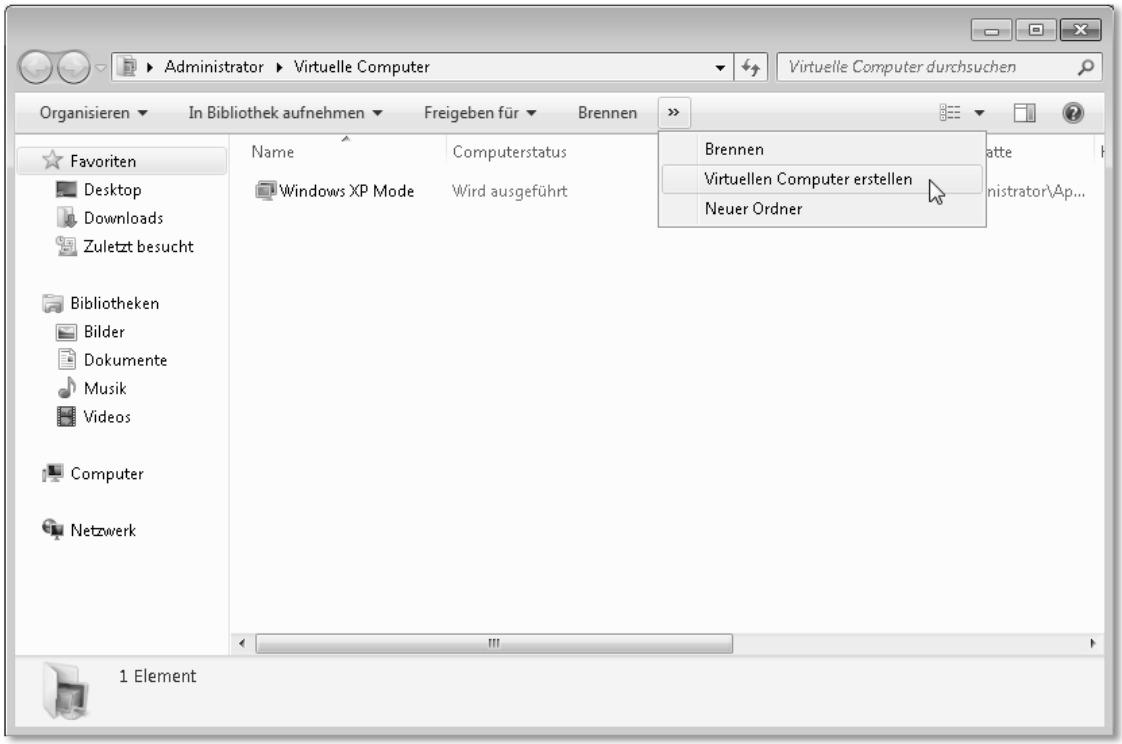


Abbildung 9.38 Eine neue virtuelle Maschine erstellen Sie hier.

Das Erstellen eines neuen virtuellen Computers wird von einem Assistenten übernommen – Sie kennen das vielleicht bereits aus dem Vorgängerprodukt:

- Der erste Schritt ist die Eingabe von Name und Speicherort der virtuellen Maschine (Abbildung 9.39).

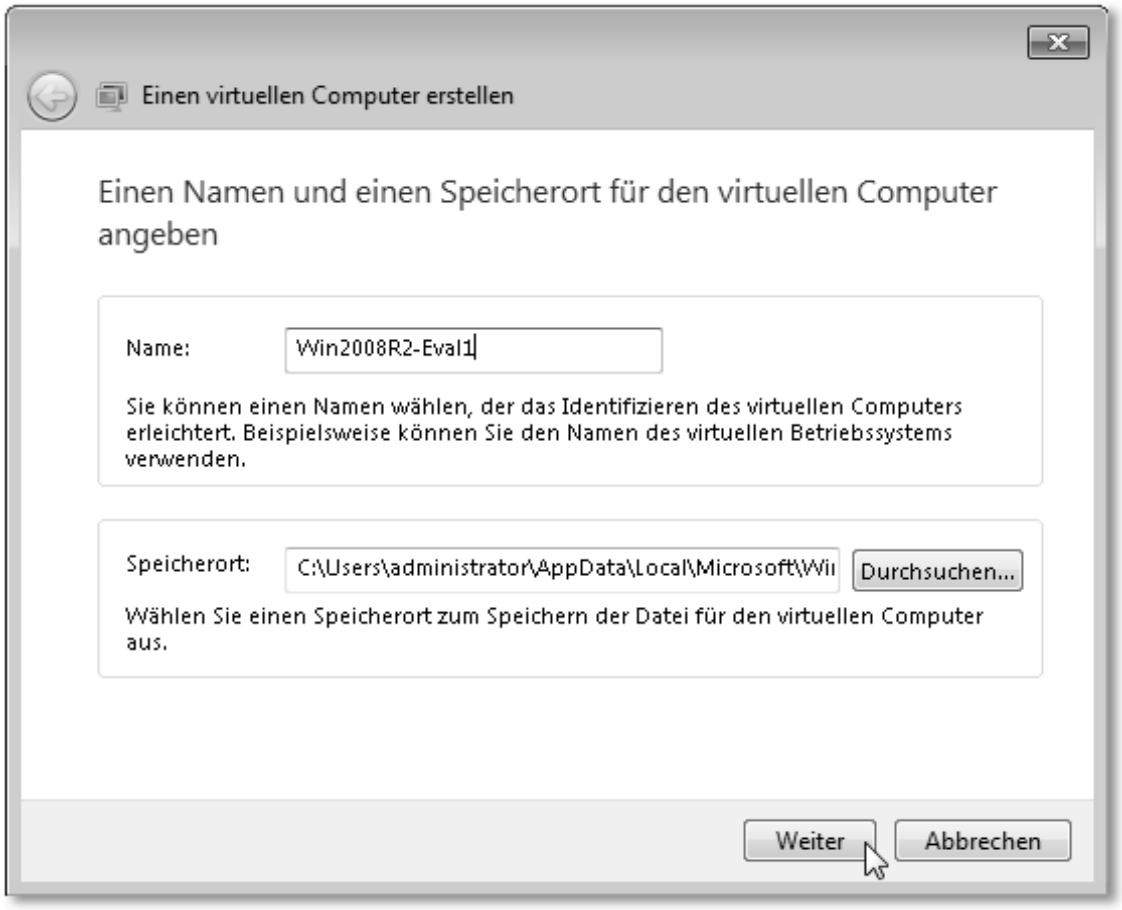


Abbildung 9.39 Zunächst braucht eine virtuelle Maschine einen Namen und einen Speicherort.

- Im nächsten Schritt wird der Arbeitsspeicher konfiguriert. Weiterhin können Sie festlegen, dass die virtuelle Maschine mit dem Netzwerk verbunden werden soll – das geschieht natürlich über die Netzwerkkarte des Windows 7-PCs (Abbildung 9.40).
- Im letzten Schritt wird die erste Festplatte der neuen virtuellen Maschine erstellt. Wenn Sie die Einstellungen vorgenommen haben, kann die virtuelle Maschine erstellt werden (Abbildung 9.41).

Wenn der PC erstellt ist, kann er jederzeit konfiguriert werden (Menüpunkt: EINSTELLUNGEN). Dabei stehen wesentlich mehr Optionen zur Verfügung als in dem Assistenten.

Wenn Sie bereits mit Virtual PC 2007 gearbeitet haben, wird Ihnen der Dialog auf Abbildung 9.42 in etwa bekannt vorkommen.

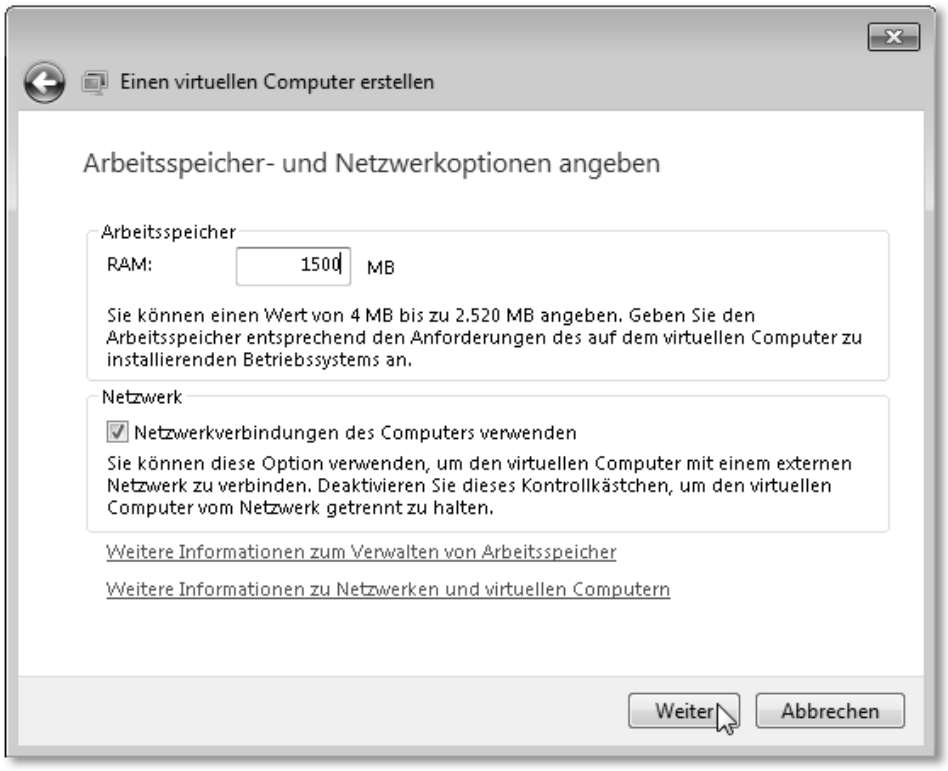


Abbildung 9.40 Legen Sie fest, wie viel Speicher die neue virtuelle Maschine erhalten soll.

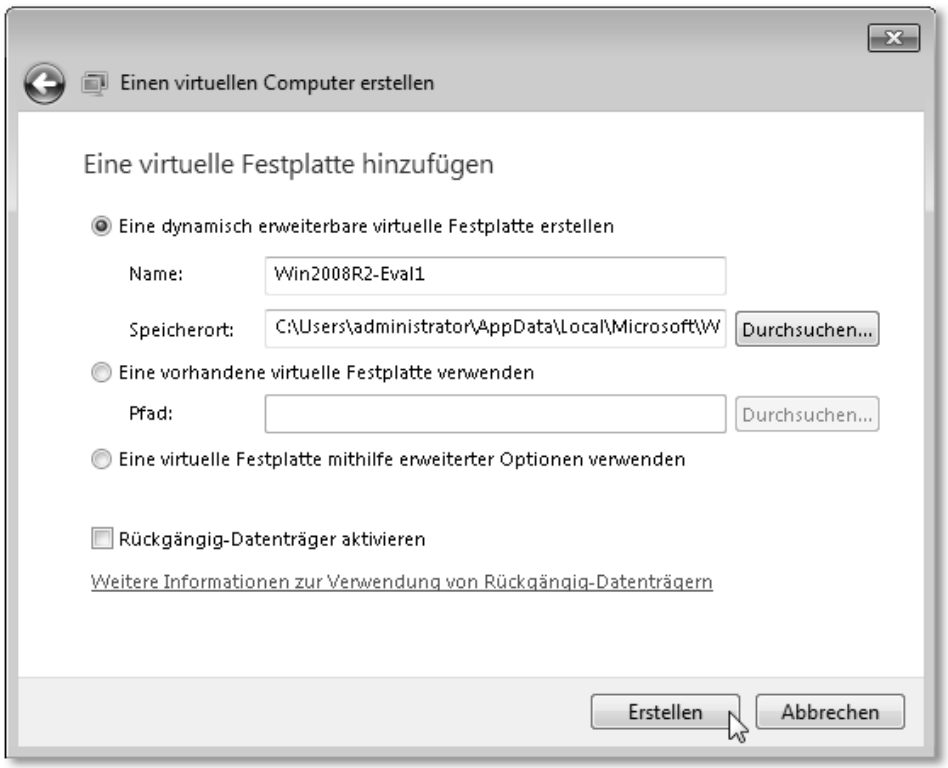


Abbildung 9.41 Wenn die erste virtuelle Festplatte konfiguriert ist, kann der virtuelle PC gestartet werden.

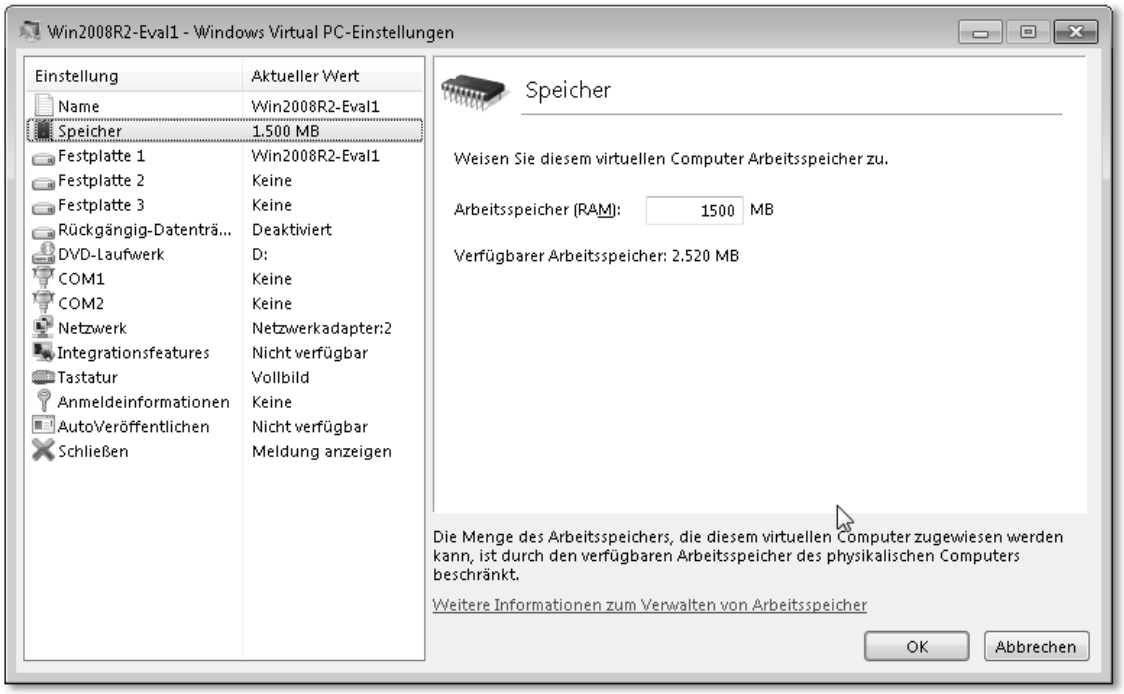


Abbildung 9.42 Die Einstellungen der virtuellen Maschine

Sein griechisches Heer aber sammelte er, soviel wie möglich, in der Stille, um den König ganz unvorbereitet zu überraschen.

10 Microsoft Desktop Optimization Pack

Für Software-Assurance-Kunden (*Software Assurance* ist eine Art Software-Pflegevertrag) stellt Microsoft das *Microsoft Desktop Optimization Pack* (MDOP) zur Verfügung. Das MDOP besteht aus sechs Werkzeugen, die in größeren Umgebungen recht wertvoll sein können (Abbildung 10.1).

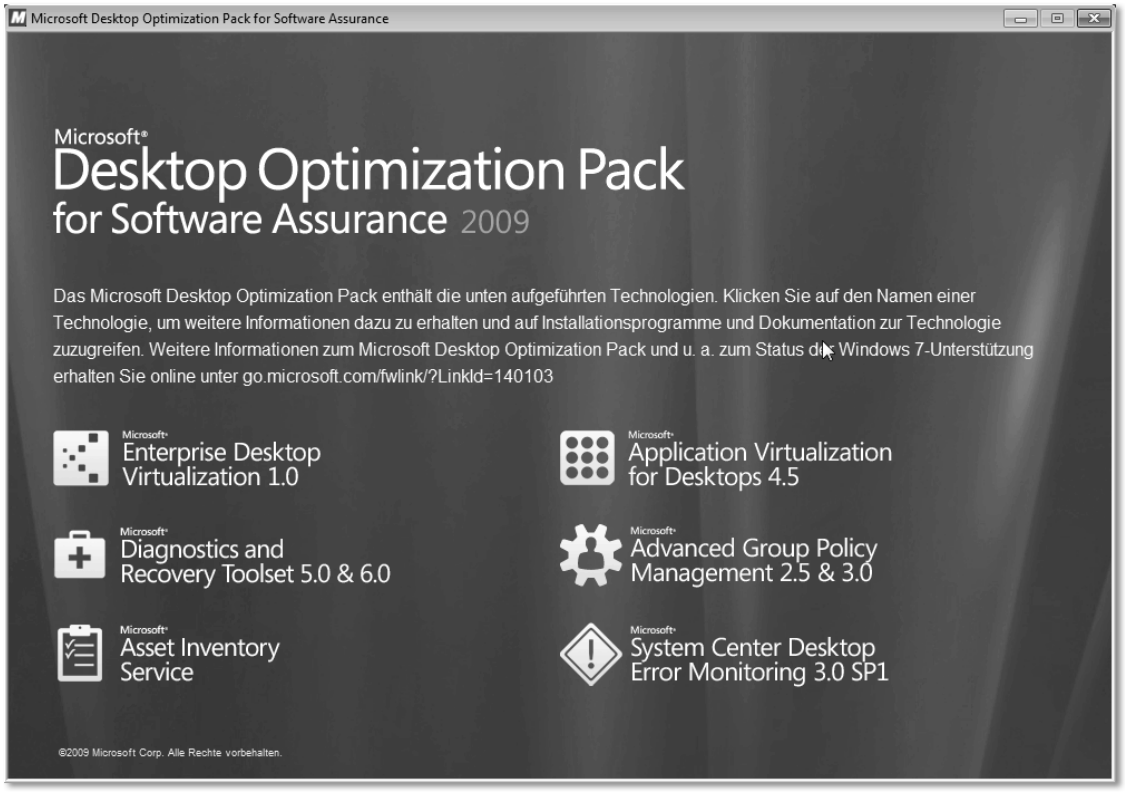


Abbildung 10.1 Die Startseite des Desktop Optimiziation Packs

Da zu dem Zeitpunkt, als dieses Buch geschrieben wurde, das MDOP »nur« bis zu *Windows Vista SP1* vorlag, werden die Möglichkeiten nur recht allgemein besprochen. Sie werden sich aber einen Eindruck von den Werkzeugen machen und bewerten können, ob diese in Ihre Umgebung passen.

10.1 Enterprise Desktop Virtualization

Sie haben in Kapitel 9.2 den *XP Mode* kennengerlernt, der dazu dient, mit Windows 7 inkompatible Applikationen in einer virtuellen Windows XP-Umgebung auszuführen. *XP Mode* ist in der vorgestellten Form allerdings eher für Umgebungen gedacht, in denen eher nur eine kleinere Anzahl von Installationen vorhanden ist. Der Grund ist, dass der XP Mode schlecht zu verwalten ist. Im Grunde genommen muss das Thema etwas weiter gefasst werden, denn die Komponente, die zentral verwaltet und gesteuert werden müsste, ist der *Virtual PC*.

Die zentrale Steuerung von Virtual-PC-Installationen ist nun auch genau die Aufgabe der *Enterprise Desktop Virtualization*. Es ist durchaus denkbar, dass ein Unternehmen recht intensiv mit virtuellen Maschinen auf den Desktops arbeitet. Gründe dafür gibt es genug, einige Beispiele:

- Als eErstes wären Kompatibilitätsprobleme von benötigten Programmen zu nennen, also der XP Mode.
- Grundsätzlich ist es natürlich denkbar, »kompliziert« zu installierende Programme generell in einem Virtual PC-Image auszurollen und gar nicht auf dem eigentlichen PC zu installieren.
- Entwickler könnten spezielle Virtual-PC-Installationen mit der Entwicklungsumgebung und solche mit verschiedenen Testumgebungen erhalten.
- Interessant wäre auch, für die privaten PCs der Anwender eine spezielle Unternehmensumgebung als Virtual-PC-Image bereitzustellen. Ein ähnlicher Fall wäre, wenn Sie Geschäftspartnern einen Teilzugriff auf Ihr Unternehmensnetz und bestimmte Anwendungen gewähren möchten. Auch hier könnte ein Virtual-PC-Image gute Dienste leisten.

Wenn Sie nicht nur fünf PCs, sondern mehrere Dutzend oder Hundert verwalten müssen, gibt es dringenden Bedarf an Automatisierung, und da kommt dann *Microsoft Enterprise Desktop Virtualization* (MED-V) ins Spiel.

Im *Desktop Optimization Pack 2009* ist *MED-V v1* enthalten, das den *Virtual PC 2007* unterstützt. *MED-V v2* wird auch den für *Windows 7* konzipierten *Windows Virtual PC* unterstützen – die v2-Version war zu dem Zeitpunkt, als ich dieses Buch geschrieben habe, aber noch nicht verfügbar.

MED-V v2 wird folgende Aufgabenbereiche haben:

- *Deployment*
  - Automatisieren der Ersteinrichtung von Virtual PC und XP-Mode mittels Skripts

  - Konfiguration der Einstellungen, insbesondere Speichernutzung, der virtuellen Maschinen, insbesondere der XP-Mode-VM.
- *Provisioning*
  - Zuordnen von Virtual-PC-Images zu bestimmten Benutzern und Gruppen
  - Definieren, welche Applikationen im XP-Mode im Startmenü erscheinen sollen
  - Definieren, welche Websites vom Browser im XP-Mode-Image angezeigt werden sollen
- *Control*
  - Einstellungen des Virtual PCs verwalten
  - Authentifizierung der Benutzer vor dem Zugriff auf Virtual PC
  - Festlegen eines Datums, nach dem der Benutzer keinen Zugriff mehr auf Virtual PC hat
- *Pflege und Support*
  - Vereinfachtes Ausliefern von geänderten Images bzw. Änderungen des Images
  - Zentrale Verwaltung von Fehlern, die in den virtuellen Umgebungen auf den Benutzer-PCs auftreten
  - Unterstützung bei der Fehlerdiagnose

System Center Virtual Machine Manager

Zu erwähnen wäre, dass Microsoft über ein weiteres Werkzeug für die Verwaltung von virtuellen Umgebungen verfügt, nämlich über den *System Center Virtual Machine Manager* (SCVMM).

SCVMM und MED-V sind aber für aber komplett unterschiedliche Anwendungsszenarien gedacht:

- SCVMM verwaltet virtuelle Maschinen, die auf speziellen virtuellen Servern laufen (Hyper-V und Microsoft Virtual Server).
- MED-V dient, wie soeben erläutert, zur Optimierung des Betriebs von virtuellen Maschinen auf Benutzer-PCs.

10.2 Application Virtualization

Jeder Administrator kennt das Problem, dass die Installation von Software unter Umständen nicht trivial ist. Es wird insbesondere dann schlimm, wenn zwei Programme eine DLL gleichen Namens, aber in unterschiedlichen Versionen benöti-

gen – die DLL-Hölle. Die Abhängigkeiten von Applikationen untereinander ist übrigens auch ein wesentliches Problem bei der Softwareverteilung. Dazu ein Beispiel:

- Applikation ist paketiert, und der Labortest gelingt.
- Applikation ist paketiert, und der Labortest gelingt ebenfalls.
- Auf PCs, auf denen Applikation A bereits installiert ist und B nachinstalliert wird, klappt alles.
- Auf PCs, auf denen Applikation B installiert ist und A nachinstalliert wird, funktionieren anschließend weder A noch B.

Solche und ähnliche Verhaltensweisen findet man in der Praxis gar nicht so sollten. Wenn in einem größeren Unternehmen ca. 100 verschiedene Applikation eingesetzt werden (das ist für einen größeren Mittelständler eher eine moderate Zahl), kann man davon ausgehen, dass es schlicht und ergreifend unmöglich ist, alle Kombinationen zu testen – von dem Beseitigen eventuell auftretender Störungen mal ganz zu schweigen.

Auch die beliebten Terminaldienste stoßen beim Thema Anwendungen an die Grenzen. Da das Installieren von Anwendungen auf Terminalservern noch komplizierter ist als auf »normalen« PCs, stellen die meisten IT-Abteilungen über Terminaldienste »nur« die »großen« Standardanwendungen, also insbesondere das Office-Paket und den Client der ERP-Software, zur Verfügung. Gäbe es keine »Interferenzen« zwischen Softwarepaketen, könnte man da sicher auch noch deutlich mehr machen.

Einen interessanten Ansatz bietet die *Application Virtualization*, deren Grundgedanke eigentlich ganz einfach ist (Abbildung 10.2):

- Applikationen werden nicht »direkt« in das Betriebssystem installiert, sondern in einem »speziellen Paket«.
- Diese Pakete werden in einer speziellen Laufzeitumgebung ausgeführt.
- Die Applikation »sieht« den Datenspeicher (Festplatte, Netzwerkfreigabe) des PCs und kann dessen Systemdienste (z. B. Windows-Dienste, Zwischenablage, COM, OLE etc.) nutzen.
- Spezifische Konfigurationsaspekte (wie spezielle DLLs, Anpassungen in der Registry und anderes) werden aber nicht auf dem PC vorgenommen, sondern nur in der abgeschotteten Laufzeitumgebung, in der sich die Anwendung befindet.

Auf diese Weise wird die Anwendung auf dem PC ausgeführt und kann dessen Ressourcen nutzen. Gleichwohl werden bei der Installation keine Veränderungen an dem PC (z. B. Änderungen in der Registry, Kopieren und Registrieren von DLL-Dateien) vorgenommen.

Dieser Ansatz ist natürlich nicht »nur« auf dem PC praktisch, sondern auch auf Terminalservern, wo eine Isolation der Applikationen vom Betriebssystem ja auch sehr sehr wünschenswert ist.

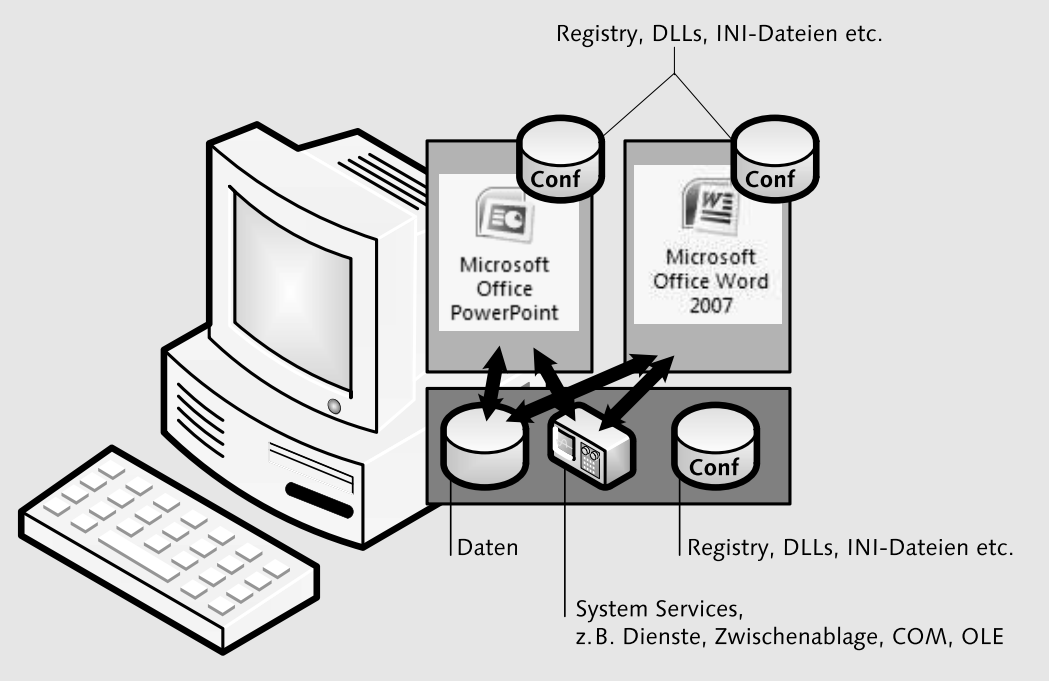


Abbildung 10.2 Vereinfachtes Schaubild zur Idee hinter der Application Virtualization

Das beschriebene Szenario kann heute schon umgesetzt werden, und zwar dank einer Technologie namens *App-V*. App-V stammt ursprünglich von der Firma *Softricity*, das Produkt hieß damals *SoftGrid*. Microsoft kaufte dieses Unternehmen im Jahre 2008 und vertrieb das Produkt zunächst unter dem Namen *Microsoft SoftGrid*. Im Rahmen der Vereinheitlichung der Benennung der Produktfamilien ist nun *App-V* daraus geworden.

10.3 Diagnostic and Recovery Toolset (DaRT)

Das *Diagnostic and Recovery Toolset* (DaRT) dient zur »Rettung« und Wiederherstellung von abgestürzten PCs.

Es ist derzeit (Spätsommer 2009) nur für Vista und Windows Server 2008 verfügbar und wird deshalb in diesem Windows 7-Buch nicht im Detail besprochen.

Das Herzstück von DaRT ist der *ERD-Commander*, der letztendlich eine bootbare Wiederherstellungsumgebung darstellt. Nach der Installation des DaRT gibt es ein Dienstprogramm, das dieses Startmedium erzeugt. Wie Sie auf Abbildung

10.3 sehen können, möchte das Dienstprogramm eine Vista-DVD verwenden – das ist natürlich für eine Windows 7-Umgebung nicht mehr wirklich gut.

Windows RE

Eine separate Wiederherstellungsumgebung ist unter Windows 7 grundsätzlich auch nicht mehr notwendig – schließlich gibt es *Windows RE* (*Recovery Environment*, siehe Kapitel 8).

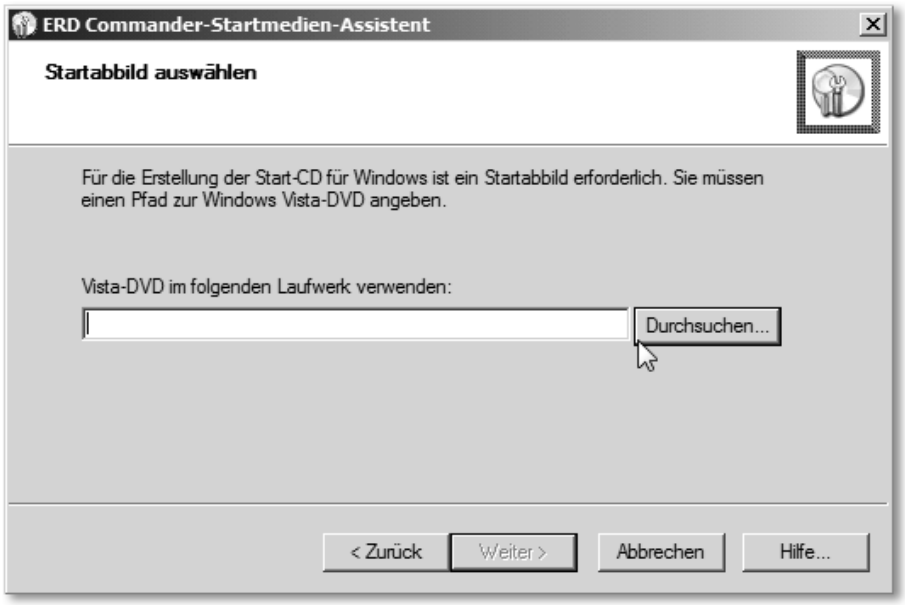


Abbildung 10.3 Für den ERD-Commander wird ein Startmedium auf Basis einer Vista-DVD erstellt.

Folgende Werkzeuge, mit denen abgestürzte oder nicht mehr startende Installationen analysiert und gegebenenfalls repariert werden können, sind im DaRT enthalten:

- *Service & Driver Manager*: Ermöglicht den Zugriff auf die Dienste und Treiber eines nicht mehr startenden Systems.
- *Event Log*: Ermöglicht den Zugriff auf das Ereignisprotokoll.
- *System Info*: Liefert Informationen über Treiber, Dateien und sonstiges über das System.
- *Disk Management*: Ermöglicht den Zugriff auf die Datenträgerverwaltung (und auch deren Modifikation).
- *Search*: Hierbei handelt es sich um ein Suchprogramm, um Dateien auf dem nicht mehr startenden System zu finden.
- *Computer Management*: Ermöglicht die Verwendung der Werkzeuge aus der Computerverwaltung für ein heruntergefahrenes System.

- *Disk Wipe*: Löscht Volumes oder ganze Festplatten.
- *Hotfix Uninstall*: Ermöglicht die gezielte Deinstallation von Hotfixes.
- *Locksmith*: Setzt die Kennwörter beliebiger lokaler Konten zurück – auch das Admin-Konto.
- *FileRestore*: Dient zur Wiederherstellung gelöschter Dateien.
- *Crash Analyzer*: Ermittelt den wahrscheinlichsten Grund für einen Absturz.
- *Disk Commander*: Dient zum Wiederherstellen gelöschter Partitionen, Verzeichnisse und Dateien.
- *Map Network Drive*: Verbindet ein Laufwerk mit einem anderen Netzwerk-PC.
- *File Sharing*: Erstellt Freigaben.
- Dient zum Deaktivieren von automatisch startenden Prozessen (Autorun/Startup).
- *Anti-Malware*: Werkzeug zum Entfernen von Malware

10.4 Asset Inventory Service

Asset Inventory Service (AIS) ist ermittelt die auf den PCs des Unternehmens installierte Software.

Eine zuverlässige Inventarisierung der vorhandenen Software ist einleuchtenderweise entscheidend, um eine korrekte Lizenzierung sicherzustellen.

10.5 Advanced Group Policy Management (AGPM)

Jedem ist klar, dass Gruppenrichtlinien ein sehr wichtiges, wenn nicht sogar das wichtigste Verwaltungswerkzeug in einer größeren Umgebung sind. In großen Organisationen wird regelmäßig kritisiert, dass die Standard-Verwaltungswerkzeuge (also insbesondere das Tool *Gruppenrichtlinienverwaltung*) kein vernünftiges Change-Management ermöglichen. Ein Administrator, der die notwendigen Berechtigungen hat, kann Änderungen vornehmen, ohne dass ein vorgeschalteter Genehmigungsprozess durchlaufen wird. Weiterhin gibt es keine Dokumentation über Änderungen, Versionen etc.

Da mit Gruppenrichtlinien sehr tiefgreifende Änderungen des Gesamtsystems möglich sind, ist zumindest für große Organisationen hier dringender Handlungsbedarf gegeben.

Advanced Group Policy Management (AGMP) besteht aus einer Server- und einer Clientkomponente. Derzeit (Spätsommer 2009) gibt es die Komponenten nur für *Windows Server 2008* und *Vista SP1* (Abbildung 10.4), was sich aber ändern wird.

Abbildung 10.4 Für AGPM gibt es sowohl Server- als auch Clientkomponenten.

10.5.1 Installation

Bevor Sie mit der Installation beginnen, müssen Sie die Frage beantworten, wie viele AGPM-Server benötigt werden. Generell gilt:

- Ein AGPM-Server kann mehrere Domänen einer Gesamtstruktur bedienen.
- Ein AGPM-Server kann nicht Domänen in unterschiedlichen Gesamtstrukturen bedienen.
- Innerhalb einer Gesamtstruktur kann es mehrere AGPM-Server geben.

Server

Der Server wird mithilfe eines Installationsassistenten installiert. Die Installation an sich ist vollkommen unproblematisch, Sie müssen nur einige Konten angeben.

Los geht es mit dem AGPM-Dienstkonto. Dieses ist das Konto, das die modifizierten Gruppenrichtlinien in das produktive Active Directory veröffentlicht. Es benötigt also Vollzugriff auf alle Gruppenrichtlinienobjekte. Es empfiehlt sich allerdings, nicht das Domänen-Administrator-Konto zu wählen – es ist keine gute Vorgehensweise, dieses Konto als Dienstkonto zu verwenden. Legen Sie stattdes-

sen ein separates Dienstkonto für AGPM an, und statten Sie es mit den benötigten Berechtigungen aus (Abbildung 10.5).

Im nächsten Dialog wird nach dem ersten AGPM-Administrator gefragt (Abbildung 10.6). Dieses Konto muss übrigens kein irgendwie gearteter Administrator sein. Mit ihm können weitere AGPM-Admins angelegt werden.

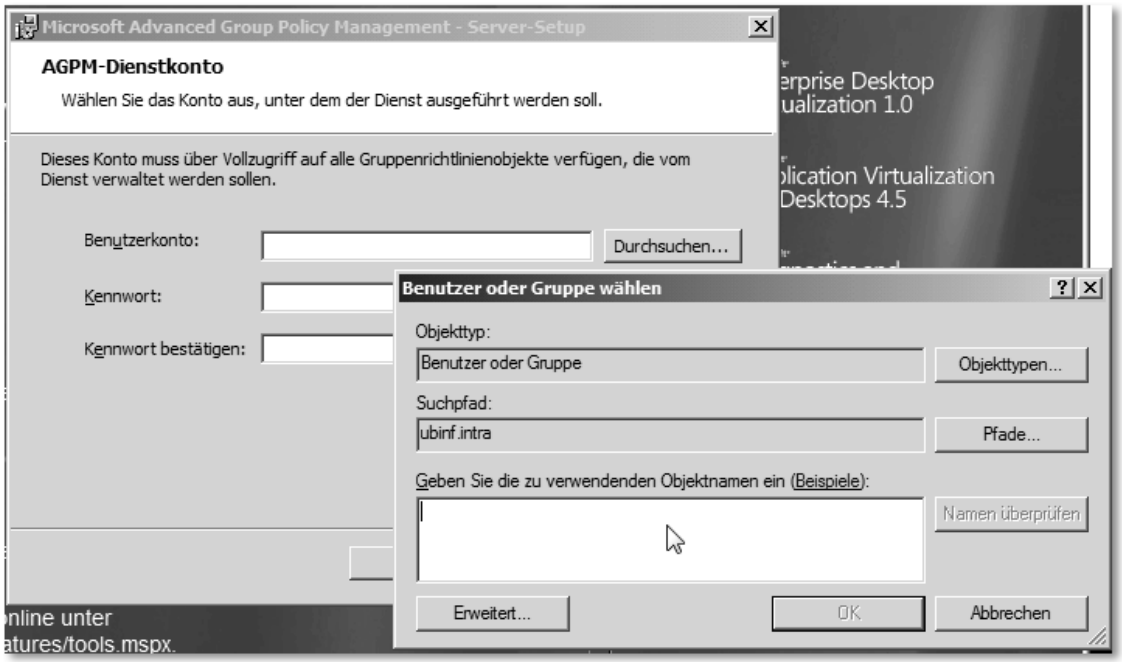


Abbildung 10.5 Das AGPM-Dienstkonto muss über Vollzugriff auf die verwalteten Richtlinien-Objekte verfügen.

Abbildung 10.6 Der erste AGPM-Administrator

AGPM ist eine Client-Server-Anwendung und benötigt demzufolge einen Port, auf dem die Clients den Server erreichen können. Diesen legen Sie in dem Dialog aus Abbildung 10.7 fest. Der Standardport ist 4600, und im Allgemeinen spricht nichts dagegen, diesen beizubehalten. Auf Wunsch bohrt der Installationsassistent auch das benötigte Loch in die Firewall.

Abbildung 10.7 Sie können den Port für die Zugriffe der Clients bestimmen. Das Installationsprogramm kann eine Portausnahme in der Firewall hinzufügen.

Als Nächstes präsentiert der Installationsassistent einen Dialog zur Sprachauswahl (Abbildung 10.8). Wählen Sie hier alle Clientsprachen aus, die in Ihrem Unternehmen vorhanden sind.

Die eigentliche Installation wird ein paar Augenblicke später abgeschlossen sein. An der installierten Serverkomponente gibt es zunächst keine weiteren Konfigurationsaufgaben, Sie können direkt zur Installation eines Clients schreiten.

Client

Der Client wird ebenfalls von einem Assistenten installiert. Die einzig wirklich spannende Eingabe sind der Name und die Portnummer, unter der der AGPM-Server zu erreichen ist (Abbildung 10.9).

Einen Eintrag im Startmenü werden Sie nach der Installation übrigens vergeblich suchen. Der Client ist eine Erweiterung der Gruppenrichtlinienverwaltung. Dort finden Sie nun den Knoten Änderungskontrolle. Wenn Sie diesen auswählen, werden etliche Registerkarten mit Einstellmöglichkeiten sichtbar (Abbildung 10.10).

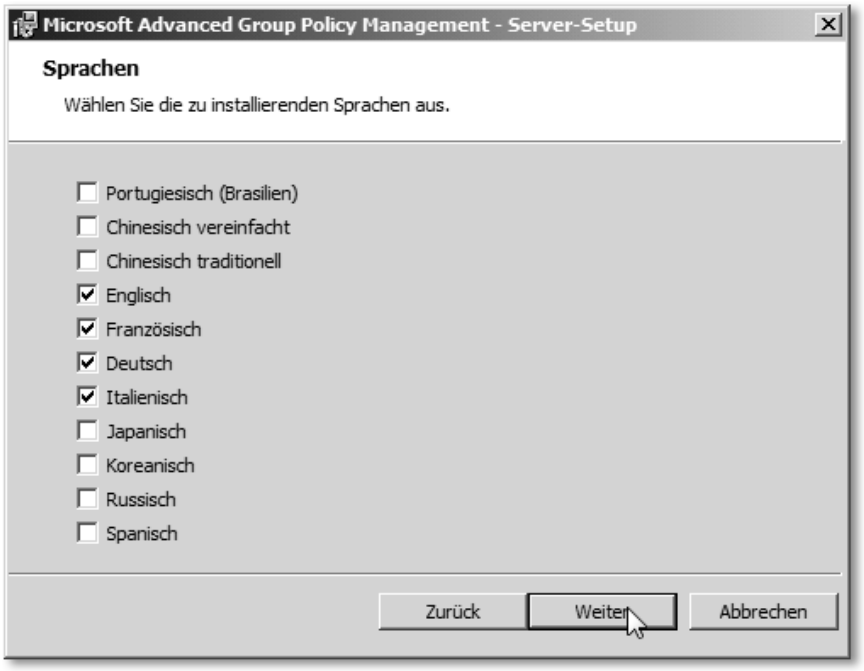


Abbildung 10.8 Wählen Sie die auf den Clients verwendeten Sprachen aus.

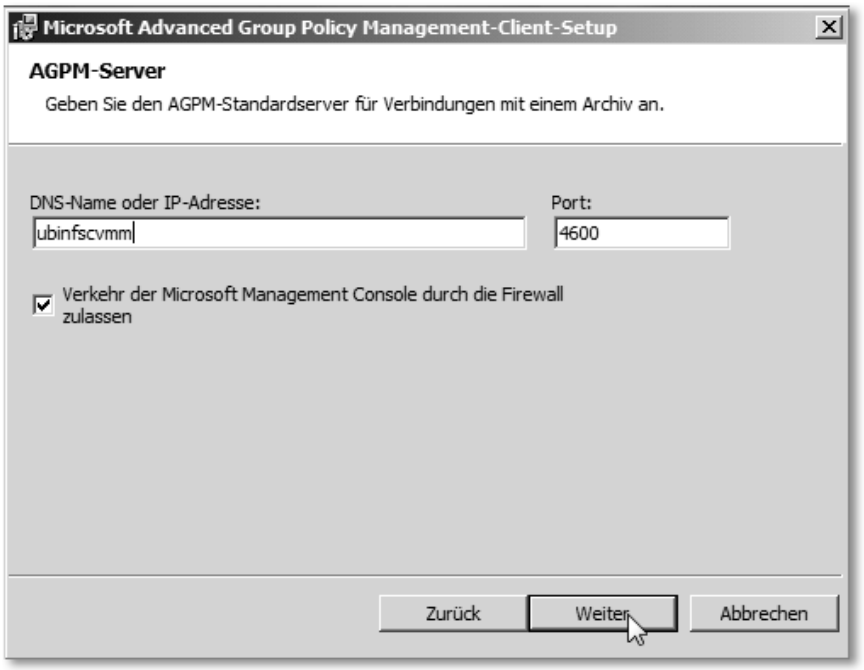


Abbildung 10.9 Bei der Clientinstallation werden Name und Portnummer des AGPM-Servers benötigt.

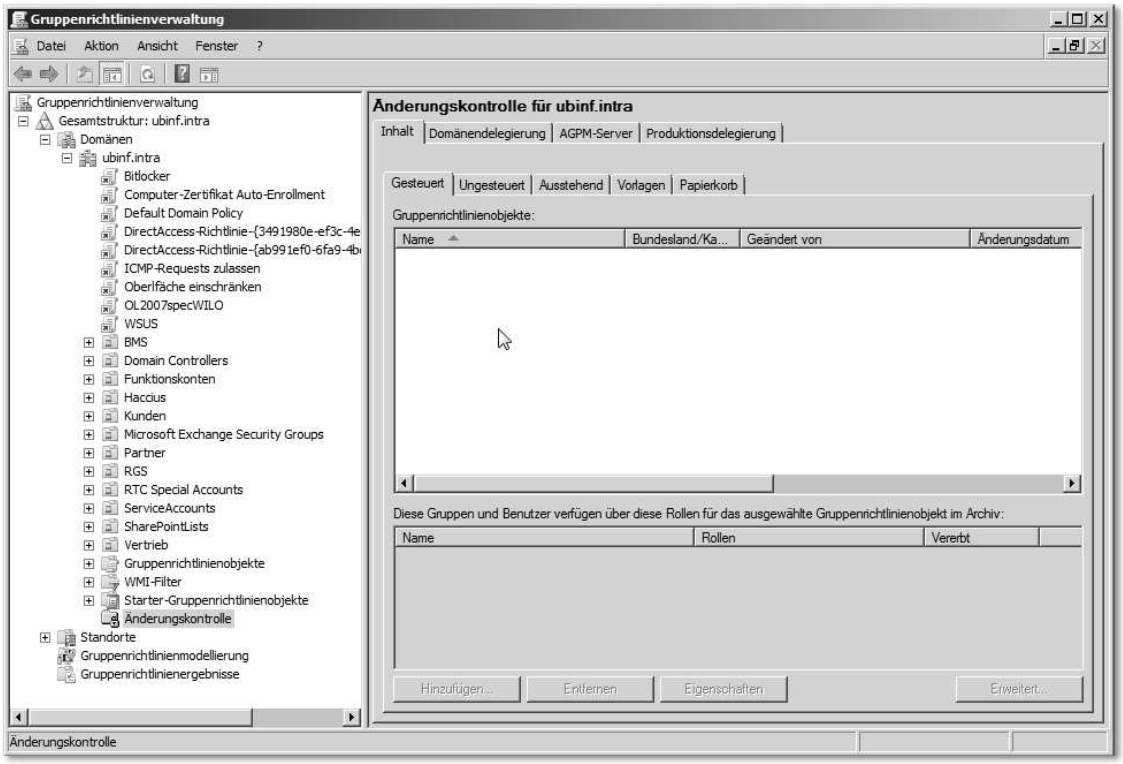


Abbildung 10.10 In der Gruppenrichtlinienverwaltung findet sich ein weiterer Menüpunkt: »Änderungskontrolle«.

10.5.2 Verwendung

Zunächst müssen Sie einen neuen Begriff lernen, nämlich die *gesteuertes Gruppenrichtlinienobjekt*. Es handelt sich hierbei letztendlich schon um eine »normale« Gruppenrichtlinie, allerdings ist um deren Erstellung und Modifikation ein Prozess implementiert worden, der Funktionen wie Auschecken, Einchecken, Genehmigung und Versionierung enthält.

Als Einstieg in die Materie zeige ich Ihnen auf Abbildung 10.11 den Prozess für das Neuanlegen einer Gruppenrichtlinie:

- Zunächst legt ein Mitglied der Rolle *Bearbeiter* ein neues gesteuertes Gruppenrichtlinienobjekt an.
- Das gesteuerte Gruppenrichtlinienobjekt muss erst von einem Mitglied der Rolle *Genehmiger* geprüft und genehmigt werden.
- Ist dies geschehen, kann der Bearbeiter die gesteuerte Gruppenrichtlinie auschecken, bearbeiten und wieder einchecken.
- Wenn der Bearbeiter alle Einstellungen konfiguriert hat, kann er eine Genehmigung anfordern.
- Der Genehmiger prüft die vorgenommenen Einstellungen, genehmigt sie und überführt die Gruppenrichtlinie damit in den Produktivbetrieb.

Der Prüfer

Neben *Bearbeiter* und *Genehmiger* gibt es noch eine dritte Rolle, nämlich *Prüfer*. Ein Prüfer kann gesteuerte Gruppenrichtlinienobjekte einsehen, allerdings nicht verändern oder genehmigen. Das ist sozusagen eine Read-Only-Rolle.

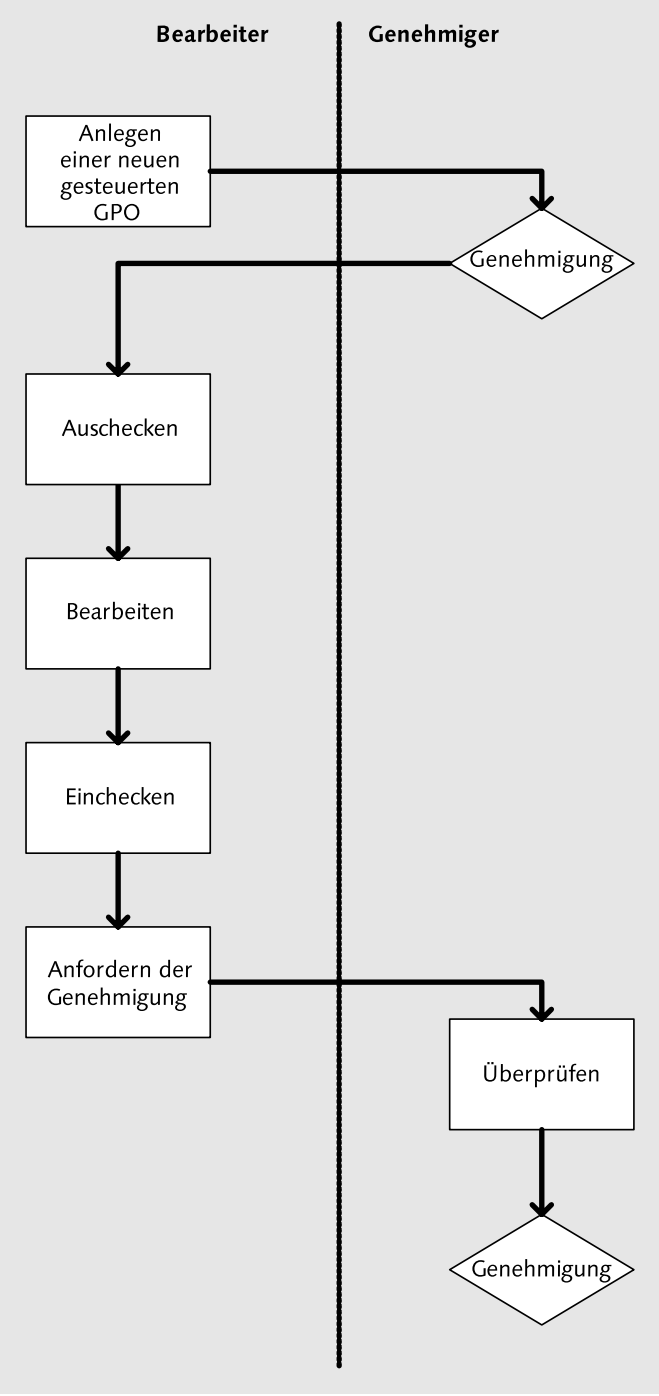


Abbildung 10.11 Ablauf der Erstellung einer neuen gesteuerten Gruppenrichtlinie

Ich möchte Ihnen nun die Erstellung eines gesteuerten Gruppenrichtlinienobjekts in der Praxis vorstellen. Zunächst bin ich als AGPM-Administrator mit Vollzugriff angemeldet – im nächsten Abschnitt sehen Sie den Vorgang mit einem Benutzerkonto mit geringeren Berechtigungen.

- Zunächst wird ein neues gespeichertes Gruppenrichtlinienobjekt angelegt. Dies geschieht beispielsweise über den entsprechenden Menüpunkt der Registerkarte GESTEUERT (Abbildung 10.12).

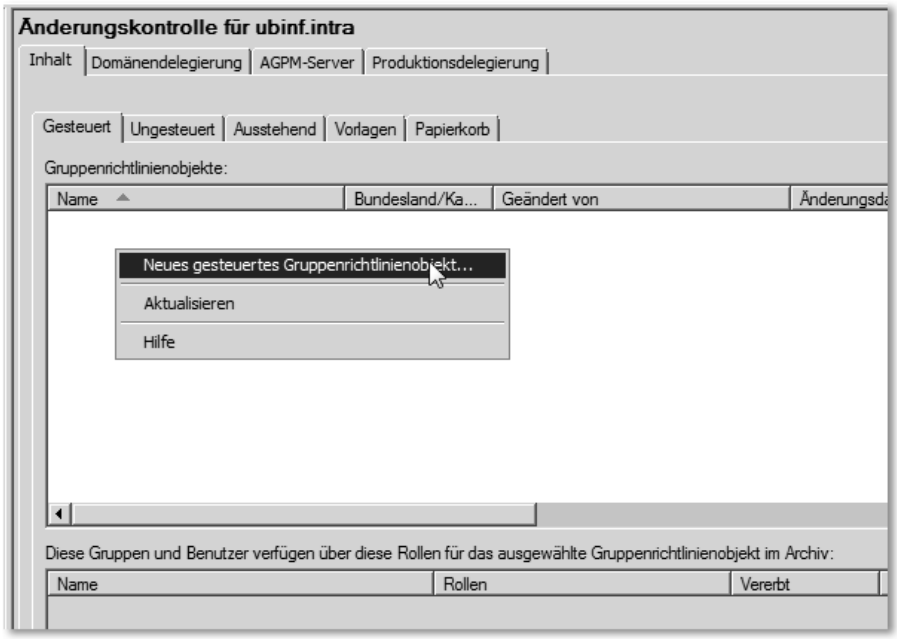


Abbildung 10.12 Zunächst wird ein neues gesteuertes Gruppenrichtlinienobjekt angelegt.

- Im folgenden Dialog werden einige grundlegende Parameter abgefragt wie der Name des neuen Gruppenrichtlinienobjekts oder die zu verwendende Vorlage (Abbildung 10.13).

  Sie können übrigens entscheiden, ob das neue Gruppenrichtlinienobjekt offline oder direkt in der Produktionsumgebung erstellt werden soll.
- Abbildung 10.14 zeigt das Kontextmenü des neu angelegten gesteuerten Gruppenrichtlinienobjekts. Zunächst soll das Objekt bearbeitet werden. Dazu muss es allerdings erst ausgecheckt werden.
- Auf Abbildung 10.15 sehen Sie das Bearbeiten des Gruppenrichtlinienobjekts. Dies wird mit dem »normalen« Gruppenrichtlinienverwaltungs-Editor erledigt. Interessant ist, dass das Gruppenrichtlinienobjekt dort als CHECKED OUT angezeigt wird.
- Nach dem Abschluss der Bearbeitung kann das Gruppenrichtlinienobjekt eingecheckt werden. Anschließend wählen Sie den Menüpunkt BEREITSTELLEN, um es in der Produktivumgebung zu aktivieren.

Abbildung 10.13 Das neue Gruppenrichtlinienobjekt bekommt einen Namen und kann auf einer Vorlage basieren.

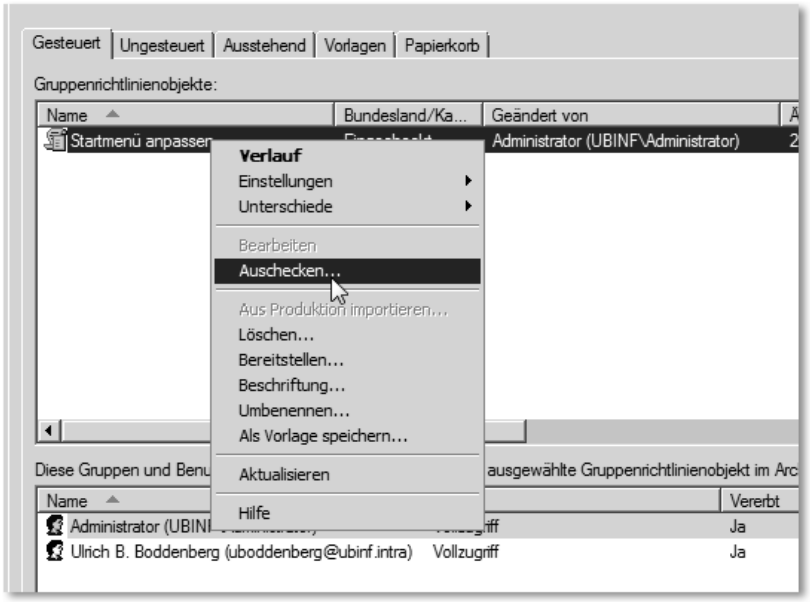


Abbildung 10.14 Vor dem Bearbeiten muss das Gruppenrichtlinienobjekt ausgecheckt werden.

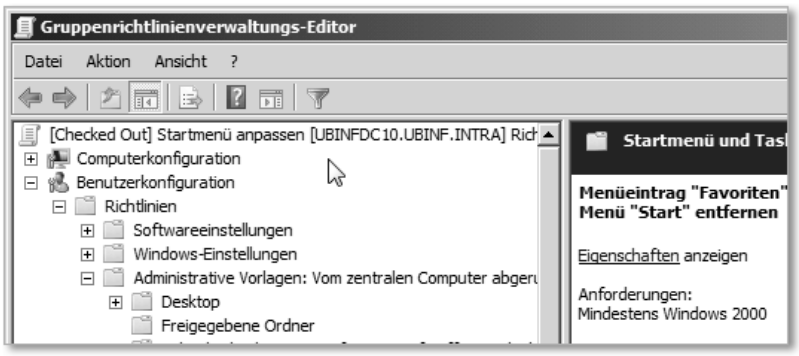


Abbildung 10.15 Die Bearbeitung erfolgt im Gruppenrichtlinienverwaltungs-Editor. Beachten Sie den »Checked Out«-Status.

Das Kontextmenü eines gesteuerten Gruppenrichtlinienobjekts hält einige interessante Funktionen bereit. Interessant ist beispielsweise die Versionshistorie, die über den Menüpunkt VERLAUF zu erreichen ist. Auf Abbildung 10.16 können Sie das bisherige Leben des Gruppenrichtlinienobjekts nachvollziehen, inklusive der Angabe, wer welchen Änderungsschritt vorgenommen hat.

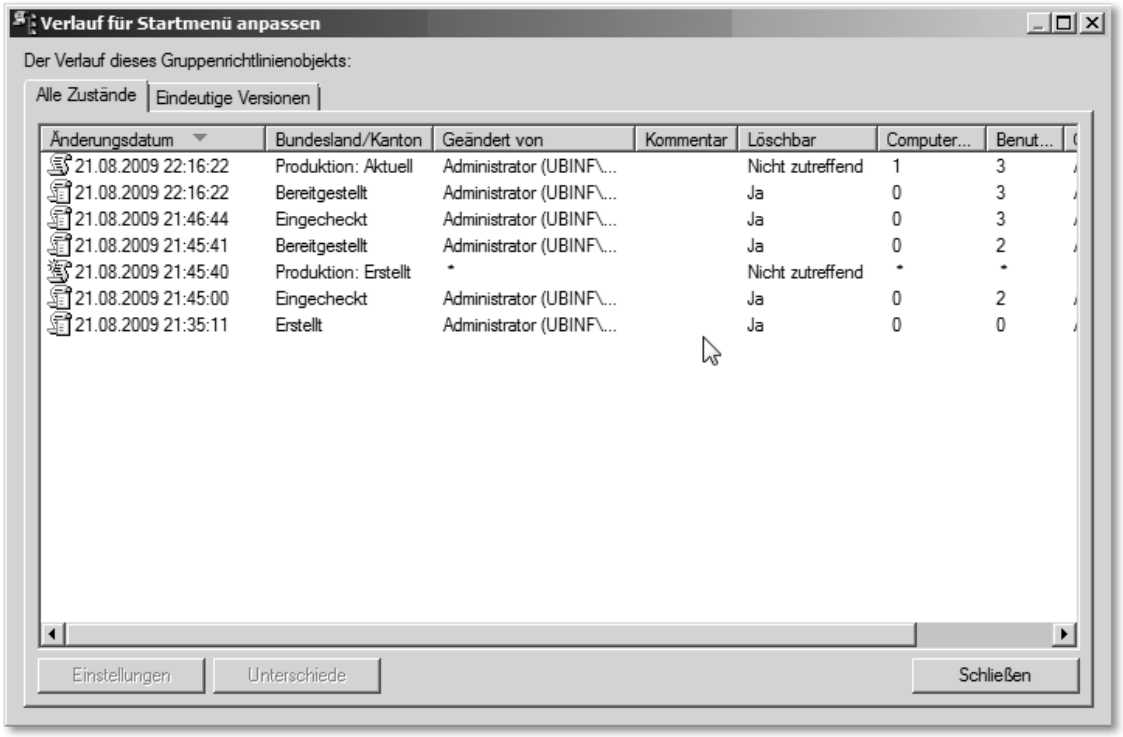


Abbildung 10.16 Im Dialog »Verlauf« können Sie kontrollieren, welche Versionen es bisher gegeben hat.

Ich möchte Sie noch auf zwei interessante Berichte hinweisen:

- Im Kontextmenü des Gruppenrichtlinienobjekts befindet sich der Menüpunkt EINSTELLUNGEN. Diese Funktion gibt eine Zusammenfassung der getroffenen Einstellungen aus, entweder als HTML oder XML-Dokument.
- Wenn es schon eine Versionshistorie (bzw. einen »Verlauf«) gibt, ist es natürlich auch wünschenswert, sich auf einfache Weise die Änderungen zwischen zwei Versionen anzeigen zu lassen. Der Menüpunkt UNTERSCHIEDE startet einen solchen Bericht. Ein Beispiel sehen Sie auf Abbildung 10.17.

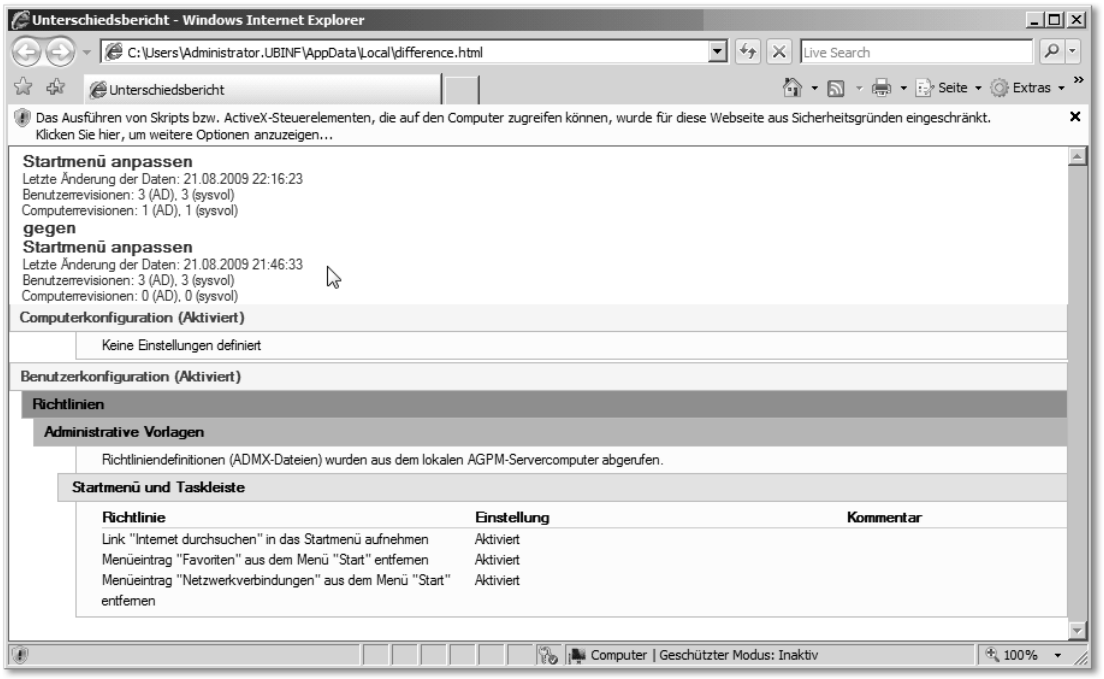


Abbildung 10.17 Dieser Bericht zeigt die Unterschiede zwischen zwei Versionen an.

10.5.3 Benutzer mit reduzierten Berechtigungen

Im Beispiel des vorherigen Abschnitts haben Sie zwar das Anlegen und Bearbeiten eines gesteuerten Gruppenrichtlinienobjekts gesehen – vermutlich haben Sie aber den Genehmigungsprozess vermisst. Der Grund ist, dass das verwendete Benutzerkonto genügend Berechtigungen hatte, um direkt ein Gruppenrichtlinienobjekt zu erstellen und zu bearbeiten. Hat der Benutzer genügend Berechtigungen, fordert auch AGPM keine Freigabe.

Das Beispiel dieses Abschnitts wurde mit einem Benutzerkonto durchgeführt, das standardmäßig keine Gruppenrichtlinienobjekte anlegen kann. Sie sehen auf Abbildung 10.18, dass die entsprechenden Menüpunkte nicht anwählbar sind.

Der erste Schritt ist die Vergabe von Berechtigungen für die Benutzung von AGPM. Auf Abbildung 10.19 ist zu sehen, wie dem Benutzer die Rolle BEARBEITER hinzugefügt wird. Dies ist eine typische Rolle für Administratoren/Operatoren in Niederlassungen oder solche Mitarbeiter, die sich um ein »Spezialthema« kümmern. Diese Personen können nun zwar ein neues Gruppenrichtlinienobjekt erstellen oder ein bestehendes anpassen – das muss aber jeweils von einem »höheren« Admin genehmigt werden.

Bei der Neuanlage eines verwalteten Gruppenrichtlinienobjekts erscheint ein gegenüber Abbildung 10.13 etwas erweiterter Dialog. Es wird dort darauf hingewiesen, dass ein im AGPM hinterlegter Administrator per E-Mail informiert wird. Weiterhin kann eine zusätzliche E-Mail-Adresse angegeben werden (Abbildung 10.20).

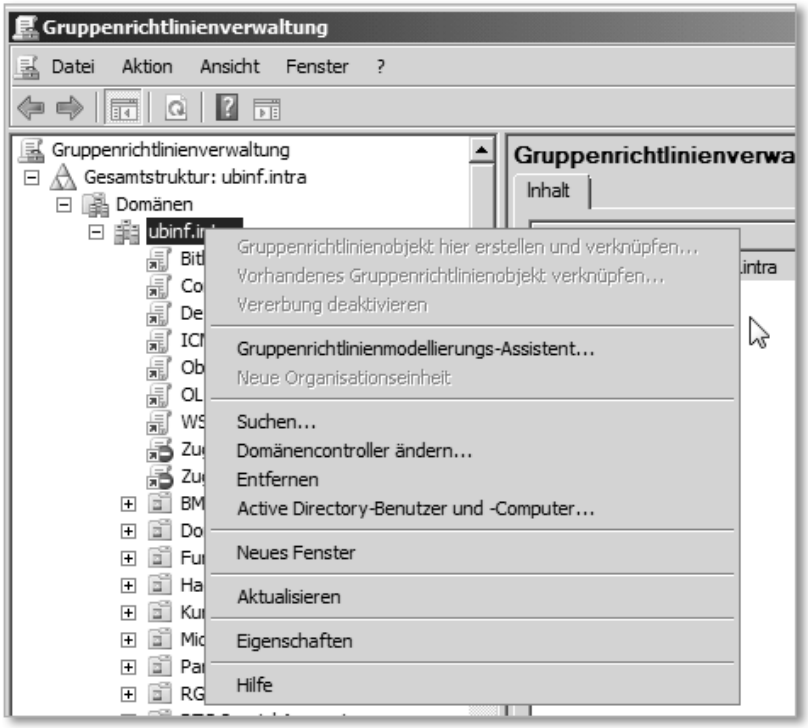


Abbildung 10.18 Der aktuelle Benutzer hat keine Berechtigungen, um ein neues Gruppenrichtlinienobjekt zu erstellen.

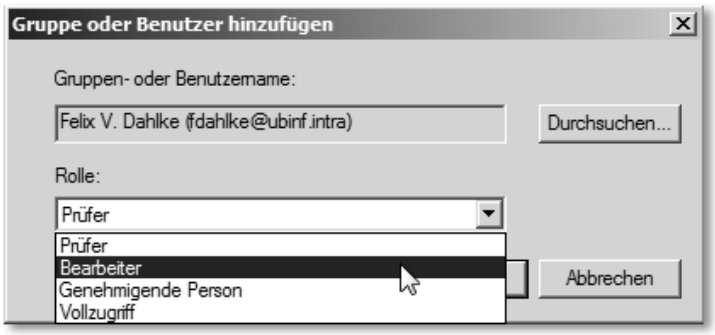


Abbildung 10.19 Ein Benutzer erhält Rechte als Bearbeiter in AGPM.

Die aus der Aktion resultierende E-Mail sehen Sie auf Abbildung 10.21 – dazu ist wohl nicht viel mehr zu sagen.

Nun kann sich ein Administrator mit Genehmigungsberechtigungen im AGPM-Client einloggen. Er wird im Kontextmenü des Gruppenrichtlinienobjekts die Menüpunkte GENEHMIGEN und ABLEHNEN sehen (Abbildung 10.22). Nach der Genehmigung kann dann die Übernahme in die Produktivumgebung erfolgen.

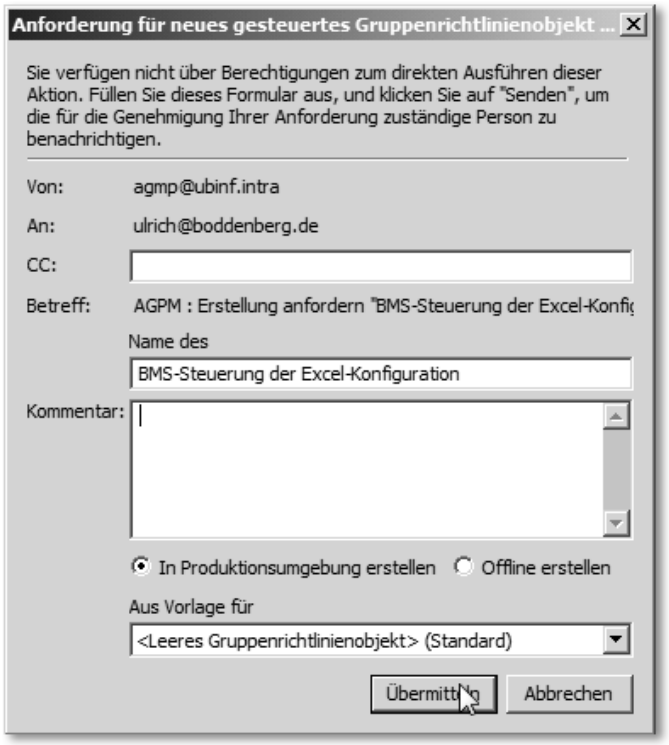


Abbildung 10.20 Ein Administrator mit Genehmigungsrechten wird darüber informiert, dass ein neues Gruppenrichtlinienobjekt angelegt werden soll.

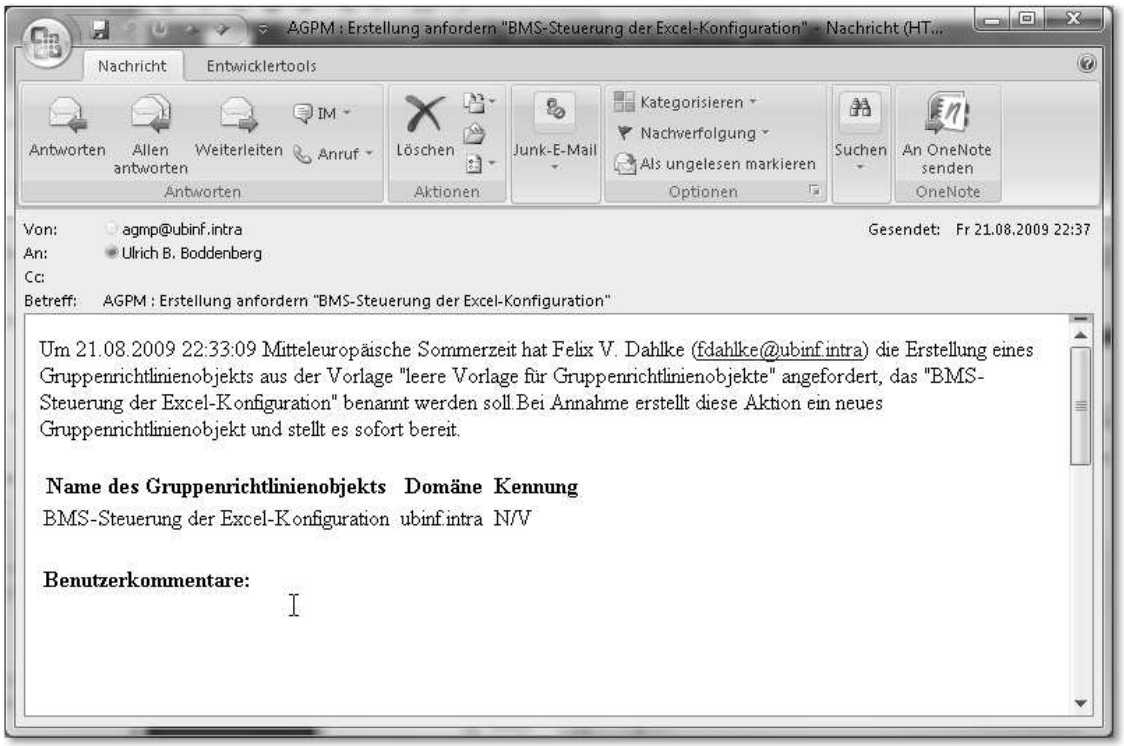


Abbildung 10.21 Der genehmigende Administrator erhält eine solche E-Mail.

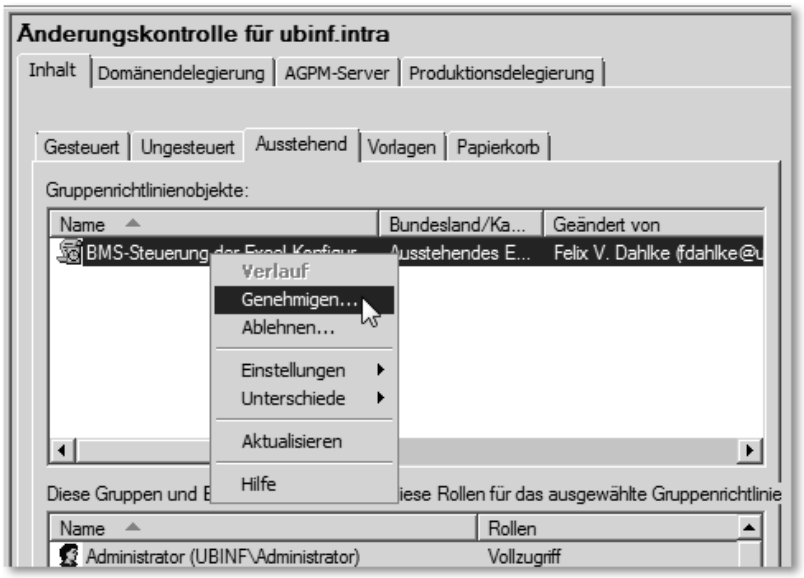


Abbildung 10.22 Hier ist zu sehen, wie ein Administrator das neue Gruppenrichtlinienobjekt genehmigt.

Bereitstellen der neuen oder geänderten Gruppenrichtlinien

Zur Vertiefung möchte ich erwähnen, dass das Bereitstellen der neuen oder geänderten Gruppenrichtlinien nicht mit dem Konto des angemeldeten Benutzers erfolgt. Eine Person, die Gruppenrichtlinien bearbeitet, muss also keine administrativen Rechte benötigen. AGPM verwendet dazu vielmehr das AGPM-Dienstkonto.

Aus diesem Grunde benötigt ein AGPM-Administrator außer der AGPM-Berechtigung (Abbildung 10.19) keine weiteren Berechtigungen – auch keine besonderen AD-Rechte.

10.6 System Center Desktop Error Monitoring

System Center Desktop Error Monitoring ist eine Komponente zur zentralen Erfassung von Fehlern und Störungen auf den Clientsystemen. Dieses System ist im Grunde genommen eine eingeschränkte Version des *System Center Operations Manager* (SCOM). Das sehen Sie bereits beim Start der Installation: Es erscheint eine Meldung, dass der *System Center Operations Manager* installiert wird (Abbildung 10.23).

SCOM

System Center Operations Manager ist ein System zur regelbasierten Überwachung von Servern, Applikationen, Clients und Netzwerkgeräten. Ich möchte an dieser Stelle nicht weiter auf dieses Serverprodukt eingehen, verweise Sie aber gern auf das Kapitel in meinem bei Galileo Press erschienen Buch *Konzepte und Lösungen für Microsoft-Netzwerke* (*http://www.galileocomputing.de/1304*).

Abbildung 10.23 »System Center Desktop Error Monitoring« ist im Grunde genommen eine eingeschränkte Version des »System Center Operations Manager«. Das ist auch bei der Installation zu erkennen.

Auf folgende Weise nun zog er dasselbe zusammen: Den Befehlshabern aller seiner Besatzungen in den Städten gab er den Befehl, recht viele tüchtige Peloponnesier anzuwerben, weil Tissaphernes etwas gegen die Städte beabsichtige.

11 Gruppenrichtlinien

Wer Windows-Clients administriert, egal ob sie unter Windows 7 oder früheren Versionen laufen, muss sich zwingend mit dem Thema Gruppenrichtlinien auseinandersetzen – Erfahrung in diesem Umfeld ist eine absolute Schlüsselqualifikation für Clientadmins.

Mit Gruppenrichtlinien (GPO, *Group Policy Object*) können diverse Konfigurationen für Benutzer oder Computer vorgenommen werden – und zwar in Abhängigkeit von Standort, Domäne und Organisationseinheit (OU), in der sich der Computer oder der Benutzer befindet. Gruppenrichtlinien sind *das* Administrationswerkzeug für die Windows-Umgebung.

Letztendlich werden bei der Anwendung von Gruppenrichtlinien Werte in der Registry modifiziert, und zwar genauer gesagt Werte in den Zweigen HKEY_CURRENT_USER und HKEY_LOCAL_MACHINE. Mit den Gruppenrichtlinien werden also Einschränkungen für Benutzer konfiguriert, aber auch Einstellungen für Computer vorgenommen, z. B. zur Sicherheitskonfiguration für drahtlose Netzwerke.

In den Gruppenrichtlinien werden übrigens auch die anzuwendenden Login-Skripts konfiguriert.

Gruppenrichtlinien wirken auf alle Betriebssysteme ab Windows 2000 aufwärts. Mit ihnen können Einstellungen sowohl auf den Client- als auch auf den Serverbetriebssystemen angepasst werden.

Neben der Möglichkeit, Einstellungen anzupassen, kann mittels Gruppenrichtlinien eine Verteilung von Software realisiert werden. Diese Art der Softwareverteilung erreicht nicht die Leistungsfähigkeit spezieller Systeme wie beispielsweise Microsoft SCCM (*System Center Configuration Manager*), ist aber in vielen Fällen durchaus ausreichend.

Die bereits in Windows Server 2008 enthaltenen Einstellmöglichkeiten für Gruppenrichtlinien decken bei Weitem nicht alles ab:

- Für die Administration von Anwendungen liefern viele Hersteller, so auch Microsoft selbst, Vorlagen für Gruppenrichtlinien mit. Auf diese Weise ist beispielsweise das Office-Paket sehr weitgehend anpassbar.
- Bei Bedarf können auch eigene Gruppenrichtlinien erstellt werden, sodass man als Administrator die völlige Freiheit hat, alles über Gruppenrichtlinien zu konfigurieren, was über die Registry eingestellt werden kann.

11.1 Anwendungsbeispiel

Falls Sie bisher nicht mit Gruppenrichtlinien in Berührung gekommen sind, zeige ich Ihnen zum Einstieg ein Anwendungsbeispiel.

Auf Abbildung 11.1 ist das Startmenü eines Windows 7-Clients zu sehen.

Abbildung 11.1 Das »normale« Startmenü eines Windows 7-Clients

Viele Unternehmen möchten die Möglichkeiten der Anwender mehr oder weniger stark einschränken. Da das Startmenü der primäre Weg ist, um Applikationen oder Konfigurationsdialoge aufzurufen, läge es also nahe, das Startmenü entsprechend »abzumagern«. Auf der Wunschliste stehen weiterhin folgende Punkte:

- Es sollen nicht an jedem PC einzeln Einstellungen vorgenommen werden müssen.
- Die Änderungen müssen auf bestimmte Teilmengen von Benutzern und Computern zu beschränken sein. Es wäre schlecht, wenn die Administratoren ebenfalls nur ein eingeschränktes Startmenü hätten.

Auf Abbildung 11.2 ist gezeigt, wie ein Gruppenrichtlinienobjekt mit der Organisationseinheit *Vertrieb* verknüpft wird. Es können beliebig viele Gruppenrichtlinienobjekte mit einer OU verknüpft werden. Ein Gruppenrichtlinienobjekt kann umgekehrt mit beliebig vielen OUs verknüpft werden.

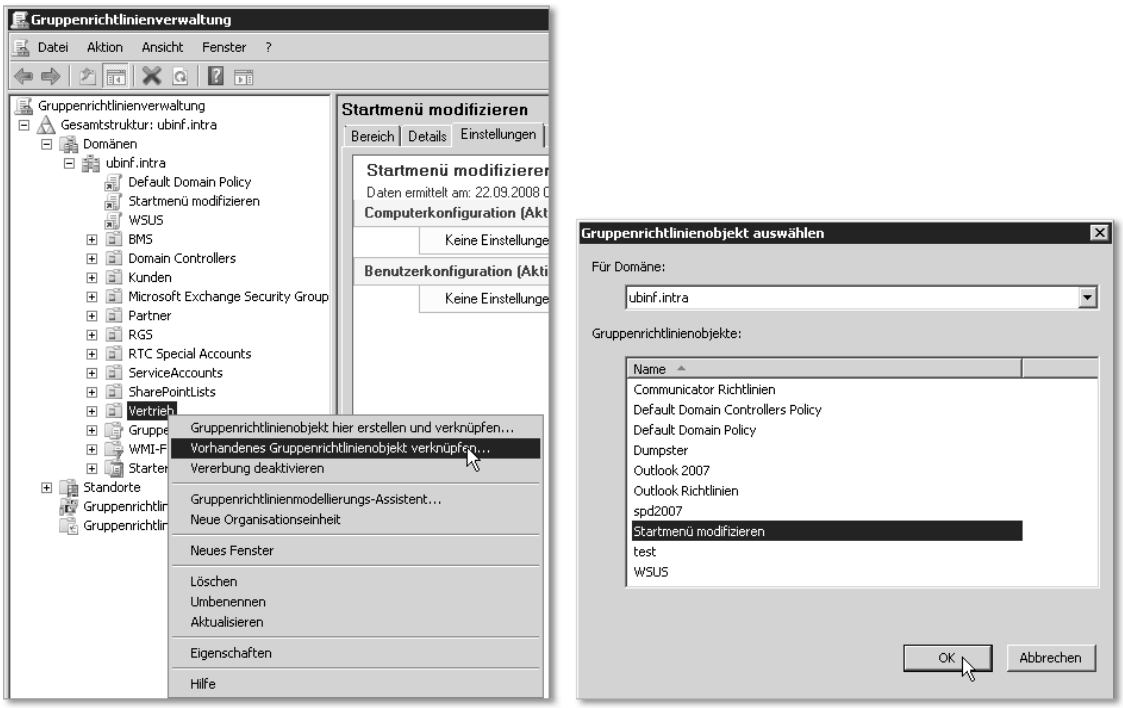


Abbildung 11.2 Ein Gruppenrichtlinienobjekt wird mit der OU »Vertrieb« verknüpft.

Ein Gruppenrichtlinienobjekt enthält jeweils beliebig viele Einstellungen. Man könnte prinzipiell alle anzuwendenden Einstellungen in einem Gruppenrichtlinienobjekt vornehmen. Erfahrungsgemäß ist die Administration dann übersichtlicher, wenn Sie die Einstellungen, die Sie vornehmen wollen, in Gruppen zusammenfassen und auf mehrere Gruppenrichtlinienobjekte verteilen.

Verknüpfungen auf Gruppenrichtlinienobjekte

Die Arbeit mit der Gruppenrichtlinienverwaltung wird ein wenig später vorgeführt.

Bereits hier wäre anzumerken, dass in den Dialogen eigentlich nur Verknüpfungen auf Gruppenrichtlinienobjekte angezeigt werden – doch dazu später mehr!

Das Bearbeiten des Gruppenrichtlinienobjekts, also das Vornehmen der gewünschten Einstellungen, ist eine Arbeit, die viel mit »Suchen« zu tun hat. Der Grund hierfür ist, dass es eine enorme Vielfalt an Einstellmöglichkeiten gibt – Windows ist ein komplexes System, und es ist sehr weitgehend über Gruppenrichtlinien zu steuern. Dementsprechend vielfältig geht es im Gruppenrichtlinienobjekt-Editor zu (Abbildung 11.3).

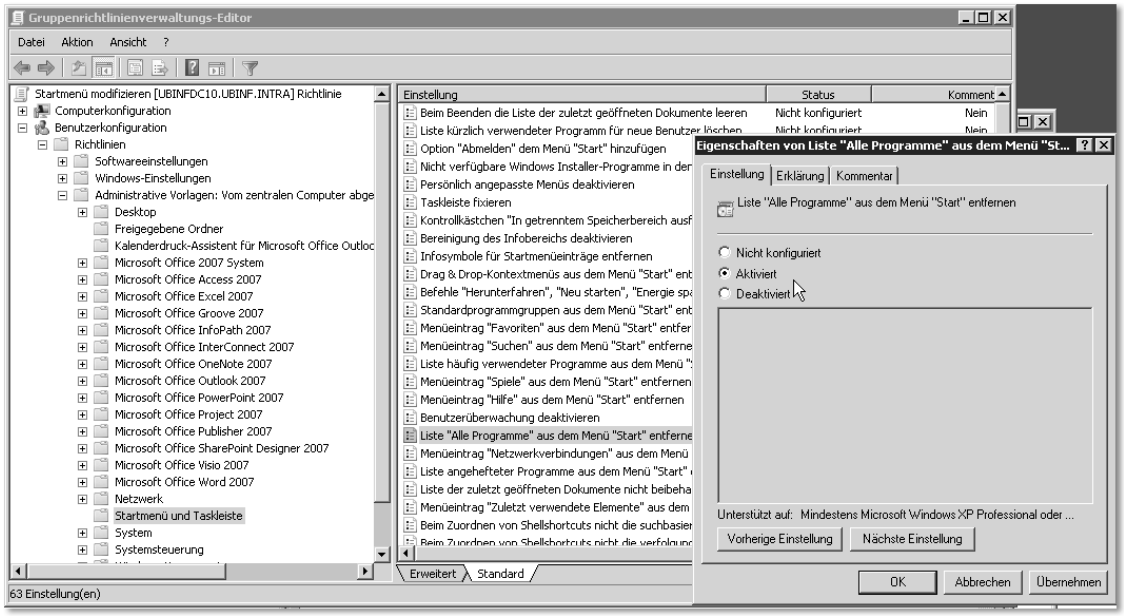


Abbildung 11.3 Bei der Erstellung der Gruppenrichtlinie kann aus Hunderten von Einstellungen ausgewählt werden.

Meldet sich der Benutzer das nächste Mal am System an, werden die vorgegebenen Einstellungen angewendet. Auf Abbildung 11.4 ist zu sehen, dass der Eintrag Alle Programme nicht mehr angezeigt wird.

Mit Gruppenrichtlinien kann nicht nur das optische Erscheinungsbild angepasst werden; im Grunde genommen können Sie all das, was in der Systemsteuerung einzustellen ist, mit Gruppenrichtlinien bequem von Ihrem Schreibtisch aus konfigurieren – und noch viel mehr, denn es gibt in Windows-Systemen viel mehr zu konfigurieren, als in den grafischen Werkzeugen angezeigt wird.

Abbildung 11.4 Die erstellte Richtlinie entfernt »Alle Programme« aus dem Startmenü.

11.2 Richtlinien für Computer und Benutzer

Ein Gruppenrichtlinienobjekt ist immer zweigeteilt. Es gibt einen Bereich COMPUTERKONFIGURATION und einen weiteren namens BENUTZERKONFIGURATION. Auf Abbildung 11.5 ist ein Blick in die COMPUTERKONFIGURATION gezeigt. Sie erkennen dort diverse Sicherheitseinstellungen, die Möglichkeit zur Konfiguration der Windows-Firewall, Zugriff auf die Einstellungen für die *Network Access Protection* und vieles andere mehr. Interessant ist auch der Knoten SOFTWAREINSTALLATION; mit dieser Funktion kann ein Windows-Installer-Paket an Computer verteilt werden. Mehr dazu erfahren Sie im weiteren Verlauf des Abschnitts.

Abbildung 11.6 zeigt einen kleinen Ausschnitt der BENUTZERKONFIGURATION. Wenn Sie diese mit der COMPUTERKONFIGURATION vergleichen, werden Sie erkennen, dass grundsätzlich beide dieselbe Struktur haben, denn sie bestehen aus folgenden drei Gruppen:

- SOFTWAREEINSTELLUNGEN: Hier wird die Verteilung von Softwarepaketen (nur Windows-Installer-Pakete, also *.MSI-Dateien) konfiguriert.

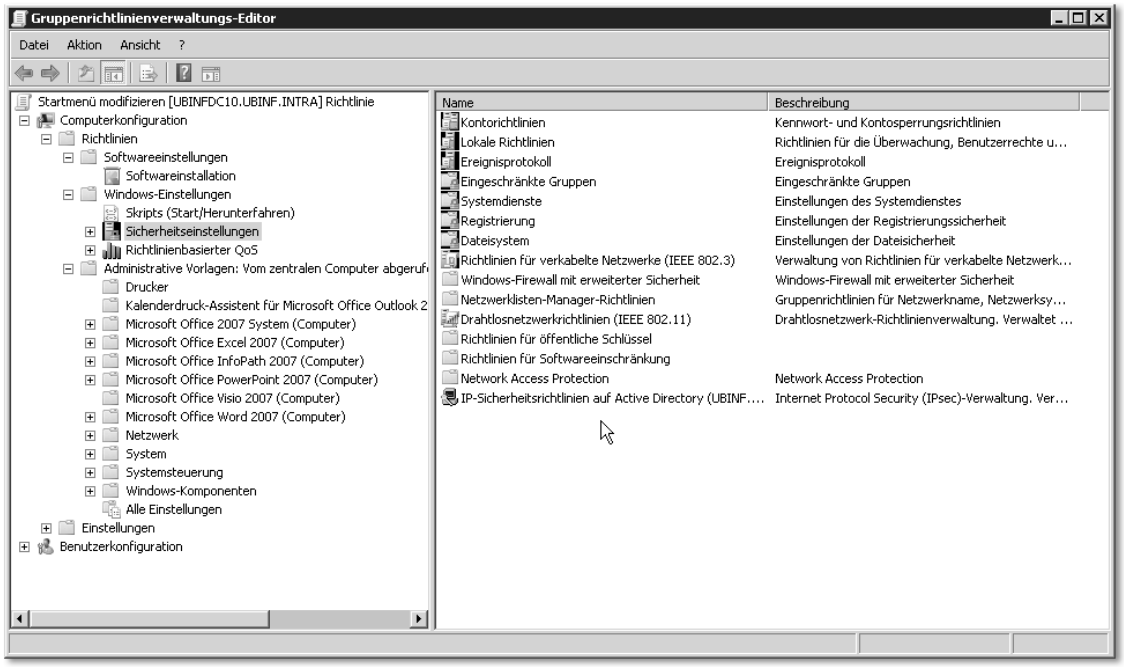


Abbildung 11.5 In Bereich »Computerkonfiguration« des Gruppenrichtlinienobjekts werden alle systemseitigen Einstellungen vorgenommen. Einige Beispiele sind auf der Abbildung zu sehen.

- WINDOWS-EINSTELLUNGEN: Hier finden sich die »Windows-nahen« Einstellmöglichkeiten, beispielsweise für die Ausführung von Skripts, die Sicherheitsrichtlinien und einiges andere mehr.
- ADMINISTRATIVE VORLAGEN: Alle anderen Einstellungen finden sich unter dem Knoten ADMINISTRATIVE VORLAGEN. Die Konfiguration von zusätzlichen Softwarekomponenten oder das Erscheinungsbild der Oberfläche wird mit den hier Einstellmöglichkeiten festgelegt, die Sie hier finden. Wenn Sie eigene Gruppenrichtlinien erstellen möchten, werden diese immer unterhalb des Knotens ADMINISTRATIVE VORLAGEN zu finden sein.

Sie sollten sich ruhig die Zeit nehmen, in diesem Wust von Konfigurationsmöglichkeiten zu stöbern. Man findet häufig Optionen mit dem »Könnte-ich-gut-einsetzen«-Effekt.

In dem Gruppenrichtlinienobjekt-Editor von Windows Server 2008 finden sich bereits die für Windows Vista (und alle Vorgängerversionen) benötigten Einstellmöglichkeiten. Windows 7 enthält einige zusätzliche Einstellmöglichkeiten, die zu Zeiten des Windows Server 2008 noch nicht bekannt waren. Da weitere Einstellmöglichkeiten über den Weg der *Administrativen Vorlagen* hinzugefügt werden können, können diese und auch zukünftige Features der Clients mit den heute aktuellen Serverversionen verwaltet werden.

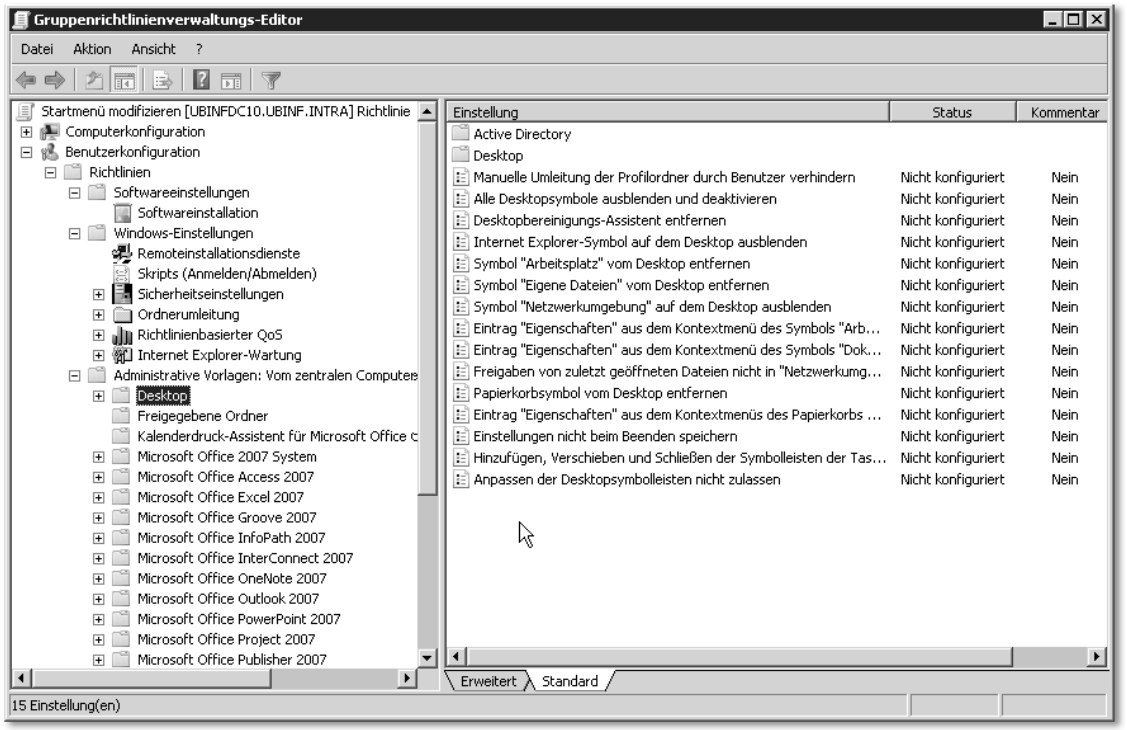


Abbildung 11.6 Der Bereich »Benutzerkonfiguration« des Gruppenrichtlinienobjekts beschäftigen sich primär mit der Fragestellung, auf welche Betriebssystemfunktionen der Benutzer Zugriff hat und wie das optische Erscheinungsbild sein soll.

Kleine Warnung

Sie haben durchaus die Möglichkeit, sich selbst auszusperren. Wenn Sie eine domänenweit gültige Gruppenrichtlinie definieren, die sämtlichen Benutzern alle Möglichkeiten auf dem Desktop wegnimmt, gilt das auch für Administratoren. Das ist dann, vorsichtig gesagt, schon sehr, sehr ungünstig.

11.3 Verteilung über Domänencontroller

Die Gruppenrichtlinien zu erstellen ist zwar schon gut, so richtig sinnvoll wird es aber erst, wenn diese auf den Clients auch zur Anwendung kommen.

Im Grunde genommen ist die Vorgehensweise nicht kompliziert. Auf Abbildung 11.7 ist ein Blick mit ADSI-Editor in das Active Directory gezeigt, genauer gesagt in den Abschnitt CN=System,CN=Policies des Domänennamenskontexts. Dort finden sich mehrere mit einer GUID benannte Einträge: Dies sind die Gruppenrichtlinienobjekte. Schaut man sich die Attribute eines solchen Objekts an, findet man beispielsweise den Anzeigenamen (*displayName*) der Gruppenrichtlinie und einen Pfad ins Dateisystem (*gPCFileSysPath*).

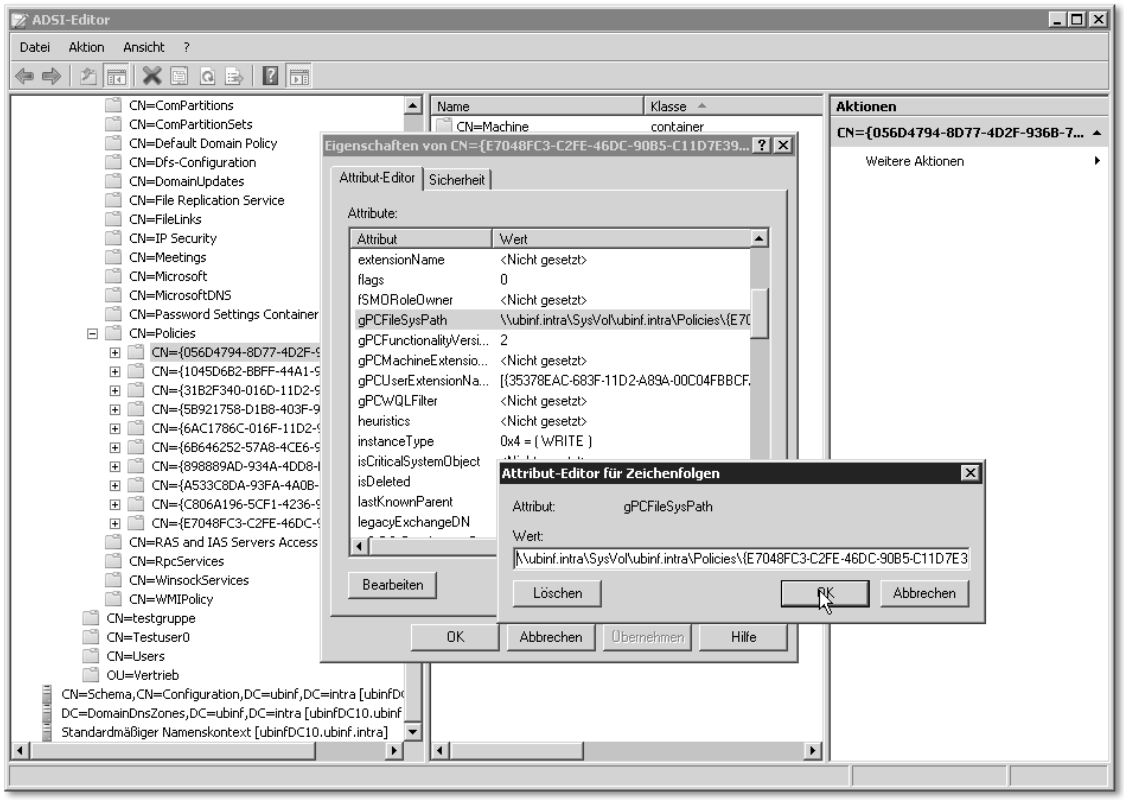


Abbildung 11.7 Die Informationen über die angelegten Gruppenrichtlinien können Sie im Domänennamenskontext finden, hier mit ADSI-Editor. Zu sehen sind beispielsweise der Displayname und ein Pfad ins Dateisystem.

Der Pfad ins Dateisystem lässt darauf schließen, dass das eigentliche Regelwerk, also die Information über die zu setzenden Registry-Einstellungen, im Dateisystem gespeichert wird. Genauso verhält es sich: Jeder Domänencontroller verfügt über ein freigegebenes Verzeichnis *SYSVOL*, das einen Unterordner *Policies* enthält, in dem wiederum Unterordner vorhanden sind, die mit den GUIDs benannt sind, die Sie bereits in ADSI-Editor gesehen haben. Abbildung 11.8 zeigt den Blick in das entsprechende Verzeichnis einer Gruppenrichtlinie.

In dem Verzeichnis der Gruppenrichtlinie findet sich ein Ordner *Machine* und ein Ordner *User*. In Letzterem liegt in diesem Fall eine Datei namens *Registry.pol*, die Informationen darüber enthält, was die Gruppenrichtlinie in der Registry einträgt. Je nach Inhalt des Gruppenrichtlinienobjekts können weitere Unterordner, Skriptdateien und dergleichen vorhanden sein. In dem gezeigten Gruppenrichtlinienobjekt-Verzeichnis ist neben *Machine* und *User* ein Ordner *Adm* vorhanden. Hier wird die Datei der verwendeten administrativen Vorlage gespeichert; mehr dazu erfahren Sie später in diesem Abschnitt.

Damit alle Domänencontroller einer Domäne die Gruppenrichtlinien bereitstellen können, ist es erforderlich, dass die *SYSVOL*-Verzeichnisse repliziert werden.

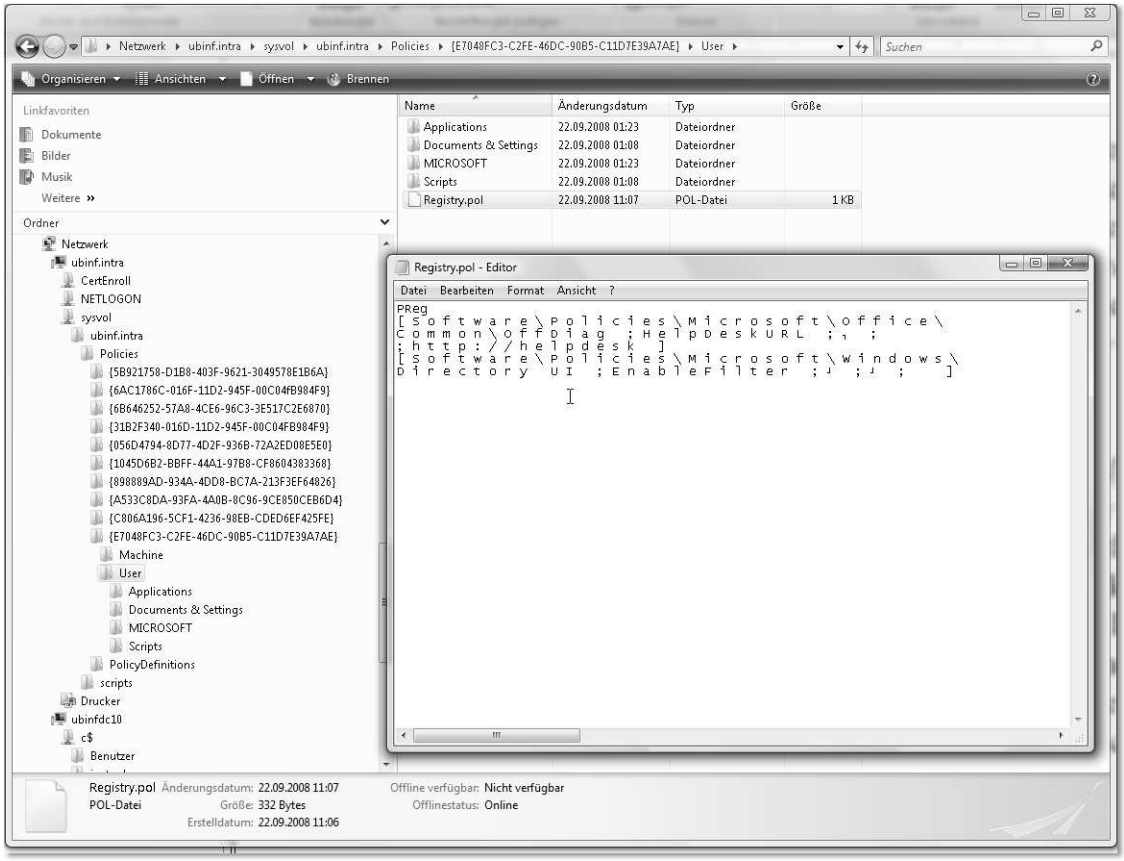


Abbildung 11.8 Die Dateien zu den Gruppenrichtlinienobjekten liegen in der Freigabe »SYSVOL«, die sich auf jedem Domänencontroller befindet.

Dies wird vom DFS-Replikationsdienst übernommen. Falls die Replikation der *SYSVOL*-Verzeichnisse nicht funktioniert, ist akuter Handlungsbedarf vorhanden. Diese Störung wird zwar nicht zum Stillstand der gesamten Produktionsumgebung führen, trotzdem wird es Beeinträchtigungen geben, weil entweder nicht alle Clients die notwendigen Einstellungen erhalten und/oder Benutzer plötzlich ein anderes optisches Erscheinungsbild als am Vortag erhalten – in Abhängigkeit von dem Domänencontroller, an dem die Anmeldung erfolgte.

Fehler des DFS-Replikationsdiensts werden im Ereignisprotokoll angezeigt. Unterhalb des Knotens Anwendungs- und Dienstprotokolle befindet sich das benötigte Protokoll (Abbildung 11.9). Da es in einer etwas größeren Umgebung unmöglich sein wird, jederzeit alle Protokolle im Blick zu haben, bietet sich die Einführung eines automatischen Systems an, das solche Meldungen konsolidiert und möglichst auch interpretiert. Ein bewährtes und preislich einigermaßen moderates System ist der *Microsoft System Center Operations Manager* (SCOM).

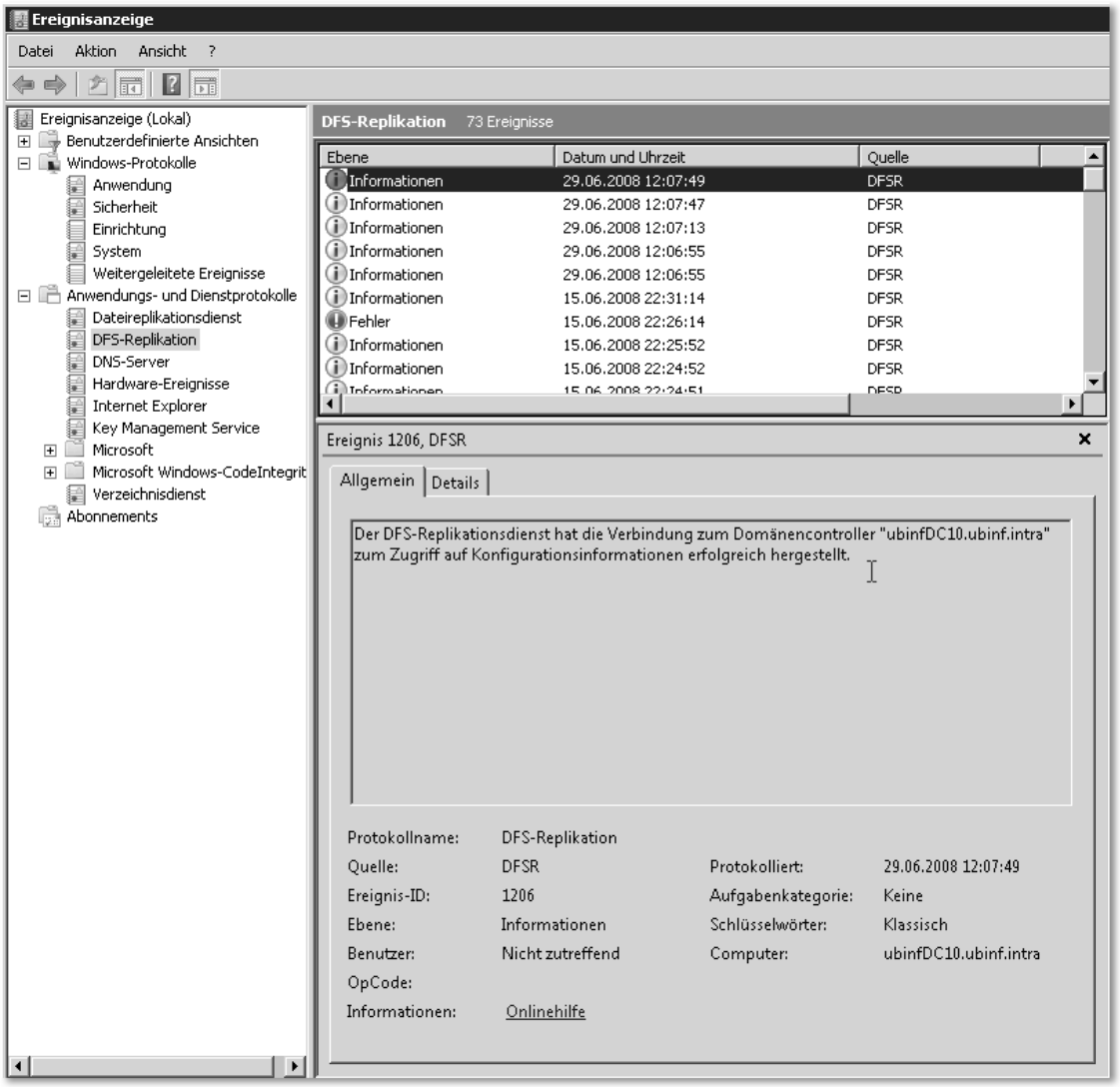


Abbildung 11.9 Meldungen und Fehler betreffs der Replikation werden im Ereignisprotokoll, Abschnitt »DFS-Replikation«, angezeigt.

Nachdem Sie nun wissen, wo die Gruppenrichtlinienobjekte angelegt werden, ergibt sich noch die Frage, wie die Zuordnung zu den Domänen, Organisationseinheiten und Standorten erfolgt.

Auf Abbildung 11.10 sind in ADSI-Editor die Attribute der Organisationseinheit *Vertrieb*« gezeigt. Unter anderem ist auch das Attribut `gPLink` vorhanden, das auf die Gruppenrichtlinienobjekte verweist, die von dieser OU verwendet werden sollen.

Nachfolgend ist der Inhalt des `gPLink`-Attributs aus Abbildung 11.10 aufgeführt: Es sind zwei Verweise auf Gruppenrichtlinienobjekte. Die GUIDs finden Sie auf Abbildung 11.7 und Abbildung 11.8 (in den Baumansichten zu sehen) wieder.

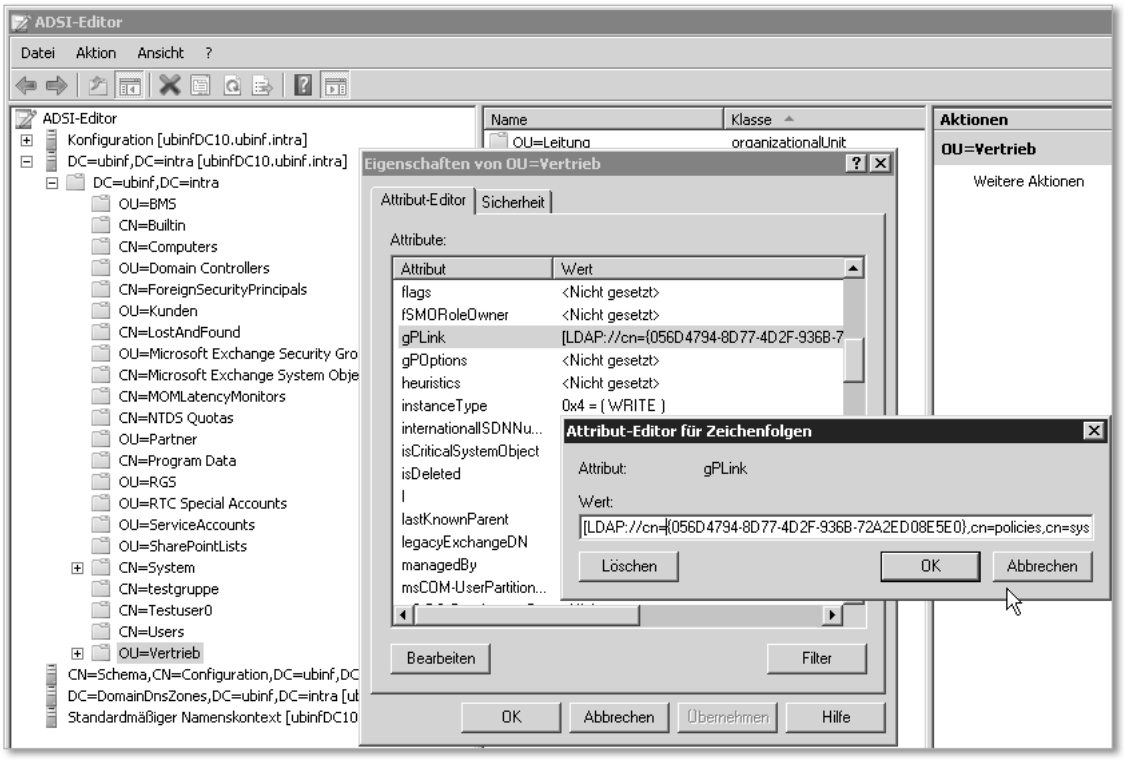


Abbildung 11.10 Die Organisationseinheit verfügt über das Attribut »gPLink«, das Verweise auf Gruppenrichtlinienobjekte enthält.

```
[LDAP://cn={056D4794-8D77-4D2F-936B-72A2ED08E5E0},cn=poli-
cies,cn=system,DC=ubinf,DC=intra;0]
```

```
[LDAP://cn={E7048FC3-C2FE-46DC-90B5-C11D7E39A7AE},cn=poli-
cies,cn=system,DC=ubinf,DC=intra;0]
```

Nun wird auch das Gesamtbild klar, das auf der stark vereinfachten Darstellung auf Abbildung 11.11 zu sehen ist:

- Organisationseinheiten, Domänen und Standorte speichern Verweise auf Gruppenrichtlinienobjekte.
- Eine Organisationseinheit, Domäne oder Standorte können auf ein, mehrere oder kein Gruppenrichtlinienobjekt verweisen.
- Auf ein Gruppenrichtlinienobjekt kann von keiner, einer oder mehreren Organisationseinheiten, Domänen oder Standorten verwiesen werden.

Es ist wichtig, diese Zusammenhänge zu verstehen – sonst wird man funktionsgleiche Gruppenrichtlinienobjekte doppelt anlegen und sich eventuell über die Formulierung in einigen Konfigurationsdialogen wundern.

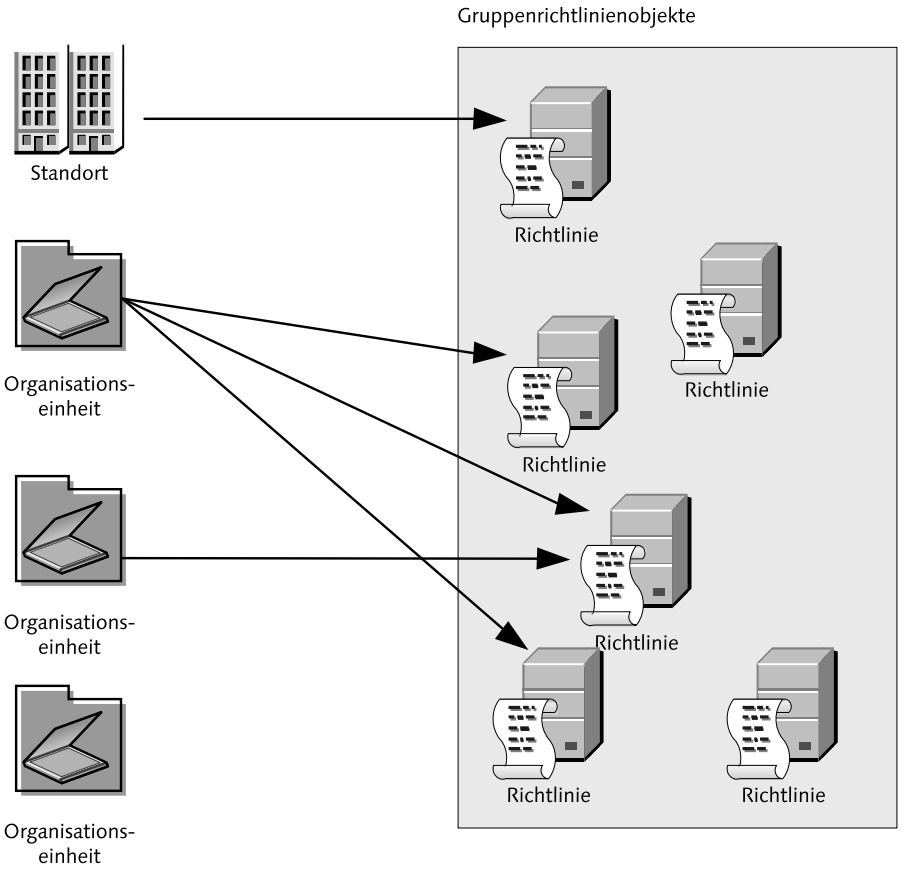


Abbildung 11.11 Standorte und Organisationseinheiten speichern Verweise auf Gruppenrichtlinienobjekte.

11.4 Vererbung

Wie bereits erwähnt, können Gruppenrichtlinien an drei »Orten« angelegt werden:

- Domäne
- Organisationseinheit
- Standort

Speicherorte für Gruppenrichtlinien

Wichtig zu erwähnen ist, dass Windows 7/Vista und Windows Server 2008 zusätzlich über *drei lokale Gruppenrichtlinienobjekte* verfügen. Insofern gibt es für diese Betriebssysteme vier »Orte«, an denen Gruppenrichtlinien gespeichert werden. Mehr dazu erfahren Sie ein wenig später.

Die Gültigkeitsbereiche der Gruppenrichtlinie sind einfach zu verstehen:

- Eine *lokale Gruppenrichtlinie* gilt einleuchtenderweise nur auf dem lokalen Computer. Windows 7/Vista und Windows Server 2008 verfügen über drei

lokale GPOs, die eine zusätzliche Einschränkung des Gültigkeitsbereichs ermöglichen. Mehr dazu folgt ein wenig später.

- Eine *Standortrichtlinie* gilt für alle Computer an einem Standort und alle Benutzer, die sich dort anmelden.
- Eine *Domänenrichtlinie* wird auf alle in der Domäne befindlichen Benutzer- und Computer angewendet.
- Eine *Gruppenrichtlinie*, die in einer Organisationseinheit definiert ist, gilt für alle dort angesiedelten Objekte, einschließlich denen, die in »Unter-OUs« angelegt sind (und auch für die OU in der OU in der OU…).

Es wirken also offensichtlich mehrere Gruppenrichtlinien auf ein Benutzer- oder Computer-Objekt. Daher ist die Reihenfolge nicht uninteressant. Abbildung 11.12 zeigt, in welcher Reihenfolge die Gruppenrichtlinien für den mit einem Pfeil gekennzeichneten Benutzer abgearbeitet werden:

1. Zunächst wird die Gruppenrichtlinie des Standorts abgearbeitet.
2. Dann wird die Gruppenrichtlinie der Domäne abgearbeitet
3. Als Nächstes wird die Gruppenrichtlinie der »äußeren« Organisationseinheit (OU) abgearbeitet.
4. Zuletzt wird die Gruppenrichtlinie der »inneren« OU verarbeitet.

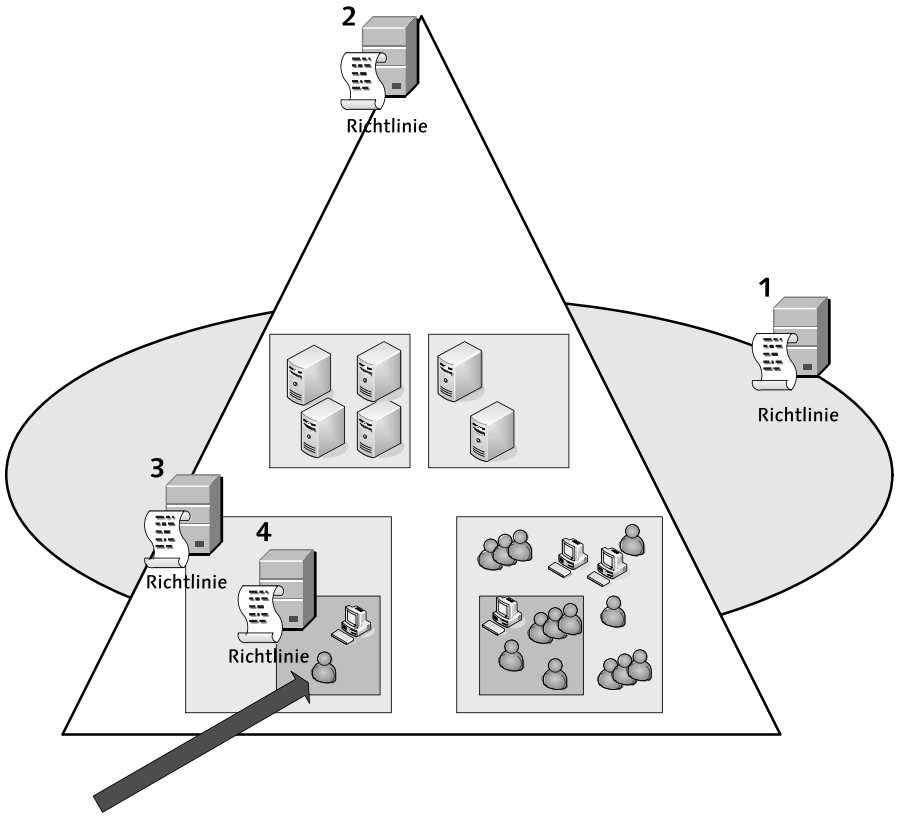


Abbildung 11.12 Die Reihenfolge, in der die Gruppenrichtlinien abgearbeitet werden

Schritt 0

In einem (nicht auf der Zeichnung abgebildeten) Schritt 0, werden bei Windows 7/Vista und Windows Server 2008 die lokalen GPOs verarbeitet.

Die Gruppenrichtlinien überschreiben sich in der Reihenfolge der Abarbeitung und wirken additiv; ein »praktisches Beispiel« sehen Sie in Tabelle 11.1, die auch die genaue Abarbeitungsreihenfolge zeigt:

Richtlinie	Konfiguration
Win7, Vista, WS2008: Lokale GPO	Nicht konfiguriert
Win7, Vista, WS2008: Lokale GPO für Admin-Konten oder Nicht-Admin-Konten	Nicht konfiguriert
Win7, Vista, WS2008: Lokale benutzerspezifische GPO	Nicht konfiguriert
Standort	Aktiviert
Domain	Deaktiviert
OU 1 (»äußere«)	Aktiviert
OU 2 (»innere«)	Nicht konfiguriert
Resultat	Aktiviert

Tabelle 11.1 Reihenfolge bei der Abarbeitung von Gruppenrichtlinien

So weit einleuchtend? Gut!

In dem Dialog auf Abbildung 11.13 ist eine Option zu erkennen, die die zuvor gezeigte Tabelle nichtig macht – sie heißt Vererbung deaktivieren. Ist diese Option gesetzt, werden übergeordnete Richtlinien eben nicht mehr vererbt. In einer so konfigurierten OU zählen nur deren eigene Richtlinien, die dann aber weiter »nach unten« vererbt werden. Das kleinere Bildschirmfoto im rechten Bereich von Abbildung 11.13 zeigt, dass ein kleines blaues Aufrufezeichen bei einer OU mit deaktivierter Vererbung angezeigt wird.

Gruppenrichtlinienverwaltung

Den Umgang mit dem Konfigurationswerkzeug *Gruppenrichtlinienverwaltung* zeige ich recht ausführlich in einem späteren Abschnitt. Dort sehen Sie auch, wie man mit dem Werkzeug anzeigt, welche Gruppenrichtlinienobjekte in einer OU tatsächlich angewendet werden.

Abbildung 11.14 zeigt, dass in der Gruppenrichtlinienverwaltung bei einem Standort der Menüpunkt Vererbung deaktivieren nicht vorhanden ist. Der Grund ist, dass es bei Standorten keine Vererbung geben kann:

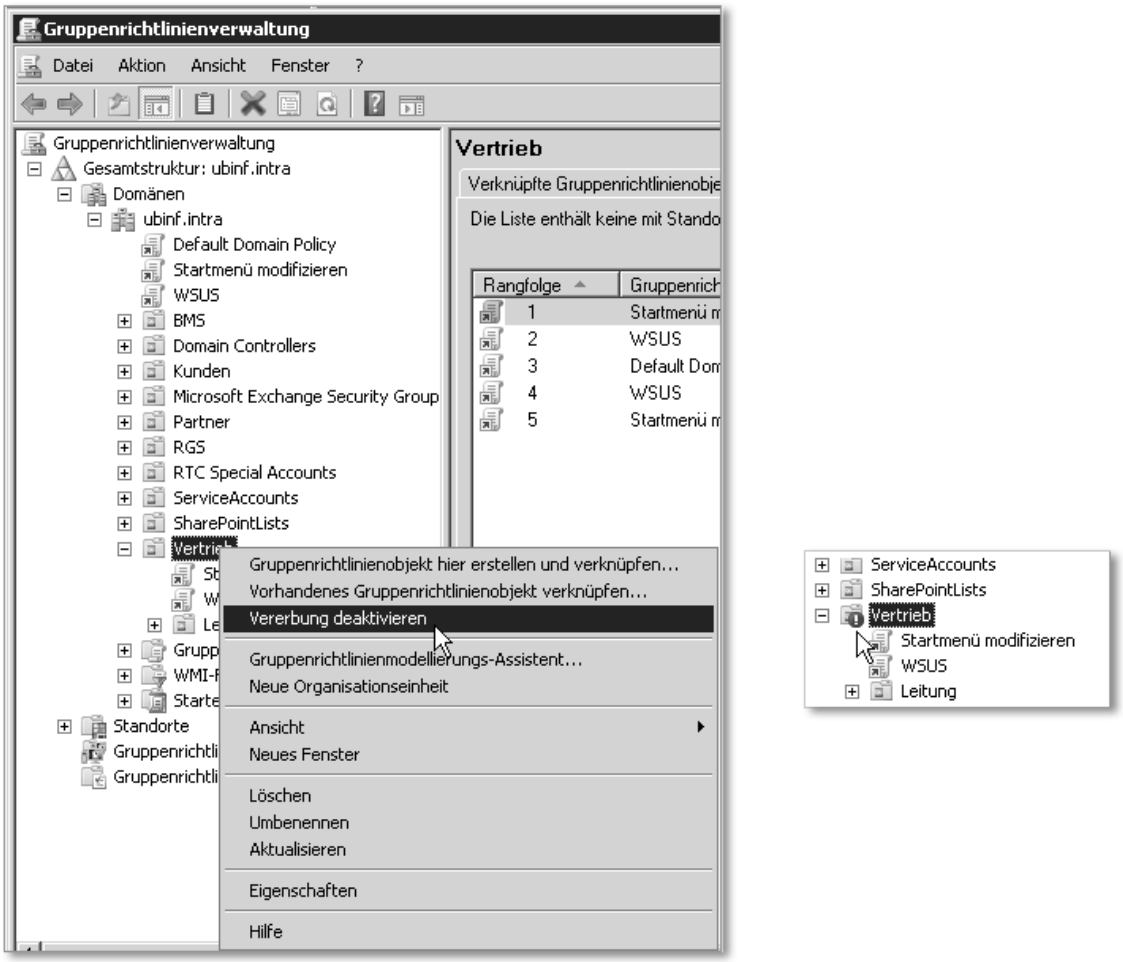


Abbildung 11.13 Die Vererbung der Gruppenrichtlinien kann deaktiviert werden. Ist für eine OU die Vererbung deaktiviert, wird diese mit einem kleinen blauen Ausrufezeichen dargestellt (rechts).

- Oberhalb einer OU könnte eine andere OU angesiedelt sein. In jedem Fall ist über einer OU eine Domäne.
- Im Falle der physikalischen Struktur des Active Directorys gibt es keinen übergeordneten Standort oder einen Unterstandort. Daher kann es auch keine Vererbung geben, was wiederum bedeutet, dass die Einstellung VERERBUNG DEAKTIVIEREN nicht relevant und darum nicht vorhanden ist.

Ansonsten gilt auch bei Gruppenrichtlinienobjekt-Verknüpfungen für Standorte, dass bei überlappenden Einstellungen die in der Liste höher angeordnete Einstellung »gewinnt«.

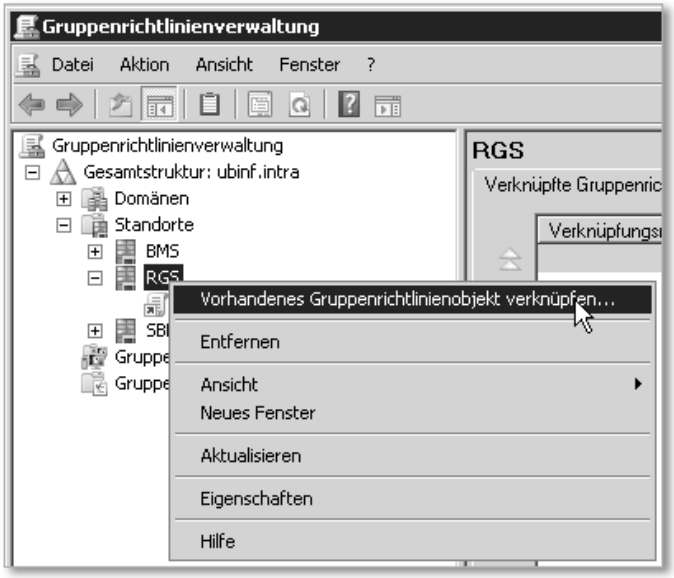


Abbildung 11.14 Bei Standorten gibt es kein »Vererbung deaktivieren«.

11.5 Sicherheit und Vorrang

Wie alle anderen Objekte im Active Directory hat auch ein Gruppenrichtlinienobjekt Sicherheitseinstellungen. Standardmäßig können *authentifizierte Benutzer* ein Gruppenrichtlinienobjekt lesen (Abbildung 11.15). Verweigert man einer bestimmten Person oder einer Gruppe die Leseberechtigung, kann bei diesen das Gruppenrichtlinienobjekt nicht angewendet werden, selbst wenn in der Organisationseinheit bzw. der Domäne oder dem Standort eine Verknüpfung vorhanden ist. Man könnte sich folgendes Szenario überlegen:

- Für die Organisationseinheit *Vertrieb* wird ein Gruppenrichtlinienobjekt angelegt; genauer: Es wird ein Gruppenrichtlinienobjekt angelegt und in der OU *Vertrieb* eine Verknüpfung auf dieses angelegt.
- Bei allen Vertriebsmitarbeitern bis auf *Naomi Wolf* sollen die dort definierten Einstellungen angewendet werden. Naomi Wolfs Benutzerobjekt ist aber in der OU gespeichert und soll dort auch bleiben.
- Wenn man Naomi gezielt den Zugriff auf dieses Gruppenrichtlinienobjekt verweigert (Verweigern ist stärker als vererbter Zugriff), wird es bei ihr nicht angewendet werden.

Ich persönlich bin kein Freund dieser Vorgehensweise, weil es irgendwann weitgehend unüberschaubar ist, bei wem welche Gruppenrichtlinie zur Anwendung kommt. Wenn es notwendig ist, bestimmte Benutzer vor einem Gruppenrichtlinienobjekt »zu schützen«, kann dieser Weg gegangen werden, diese Vorgehensweise sollte aber eine Ausnahme bleiben.

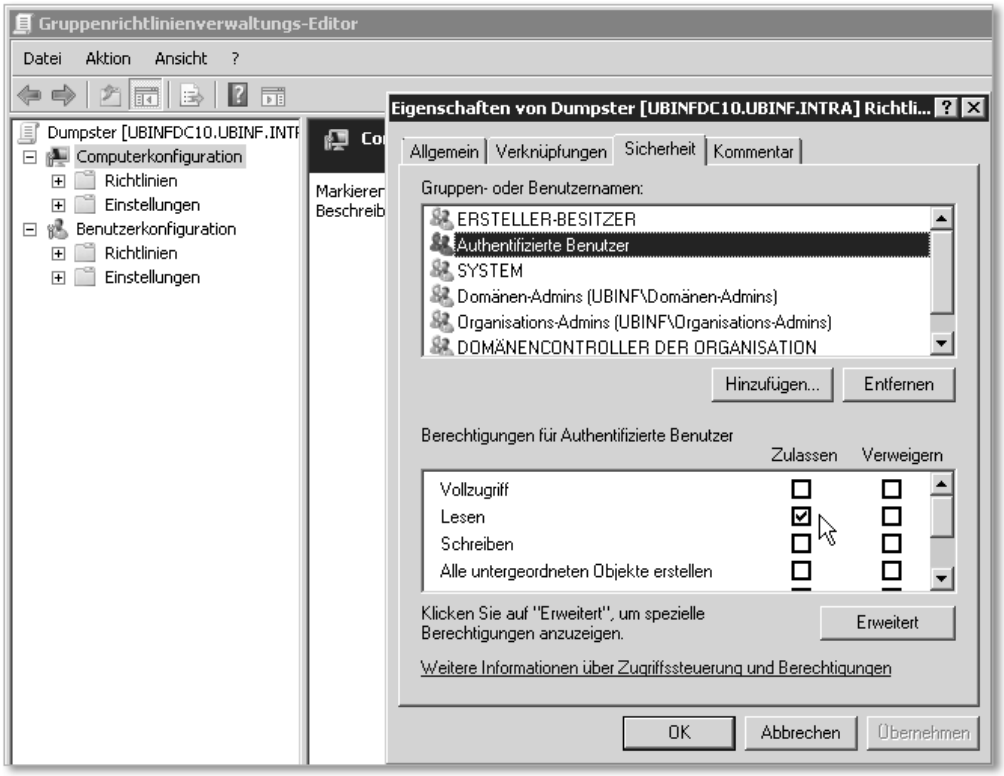


Abbildung 11.15 Auch die Gruppenrichtlinienobjekte sind mit Sicherheitseinstellungen versehen.

Denken Sie daran, dass sich das Ändern der Sicherheitseinstellung auf das Gruppenrichtlinienobjekt und nicht auf eine einzelne Verknüpfung bezieht.

Etwas weiter vorn haben Sie die Möglichkeit Vererbung deaktivieren kennengelernt. Es gibt auch das genaue Gegenteil, nämlich die Einstellung Erzwungen (Abbildung 11.16).

Der alte Name

Blitzinfo für »alte AD-Hasen«: Früher hieß diese Option Kein Vorrang.

Diese Option bewirkt, dass die in einer Gruppenrichtlinie festgelegten Einstellungen nicht von einer »späteren« Richtlinie überschrieben werden können. Ein kleines Beispiel:

- Auf der Ebene der Domäne wird mittels einer Verknüpfung auf ein Gruppenrichtlinienobjekt festgelegt, dass der Hintergrund des Bildschirms schweinchenrosa sein muss.
- Im Normalfall könnte auf der Ebene der Organisationseinheiten festgelegt werden, dass die Hintergrundfarbe babyblau sein soll. Die OU-Richtlinie überschreibt die Domänenrichtlinie.

- Wenn auf Domänenebene die *Verknüpfung*soption (!) KEIN VORRANG gesetzt wird, werden sämtliche Bildschirmhintergründe aller Systeme in der Domäne schweinchenrosa sein.

ERZWUNGEN ist übrigens auch »stärker«, als VERERBUNG DEAKTIVIEREN. Diese Option ist beispielsweise nicht unpraktisch, wenn in Ihrer Organisation die Verwaltung der OUs, inklusive Gruppenrichtlinien, an »Unteradministratoren« delegiert ist. Gruppenrichtlinien, die Ihnen wichtig erscheinen, können Sie dann trotzdem durchsetzen, egal ob der Kollege keine Bildschirmhintergründe in Schweinchenrosa mag.

Beachten Sie, dass ERZWUNGEN eine Verknüpfungsoption ist. Mit den vorherigen Erklärungen werden Sie leicht verstehen können, was das bedeutet.

Der Dialog aus Abbildung 11.16 bietet weiterhin die Möglichkeit, eine Verknüpfung zu deaktivieren.

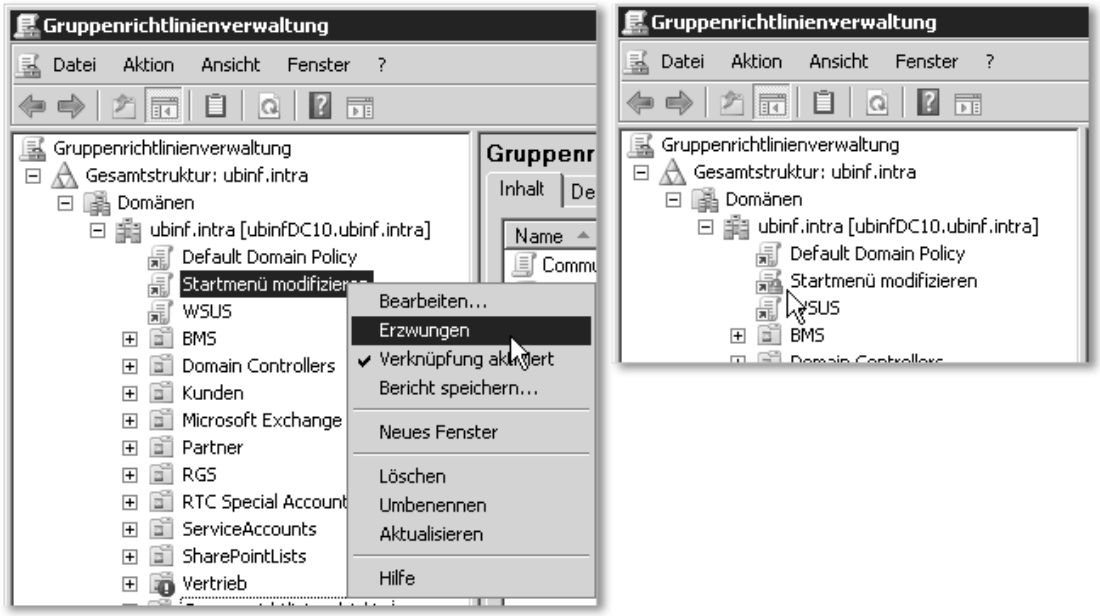


Abbildung 11.16 Mit der Option »Erzwungen« sind vererbte Gruppenrichtlinien-Einstellungen nicht mehr überschreibbar. Eine entsprechend konfigurierte Verknüpfung wird mit einem kleinen Schloss angezeigt.

11.6 Filter

Eine weitere Möglichkeit, um die Anwendung einer Gruppenrichtlinie zu bestimmen, ist die Verwendung von WMI-Filtern. Filterkriterien können über die *WMI Query Language* formuliert werden und beziehen sich zumeist auf Hardware- und/oder Betriebssystemgegebenheiten. Interessant ist das insbesondere bei

Richtlinien zur Verteilung von Software: Sie können beispielsweise festlegen, dass die Installation (d. h. die Anwendung der Richtlinie) nur dann erfolgt, wenn mindestens 2 GB freier Plattenspeicher vorhanden sind und das Betriebssystem Windows XP ist.

Die Verwendung von Filtern wird im weiteren Verlauf des Kapitels am Beispiel vorgeführt.

11.7 Abarbeitungsreihenfolge

Weiter vorn habe ich bereits zwei wichtige Sachverhalte genannt:

- Innerhalb einer Domäne findet eine Vererbung der Gruppenrichtlinien statt, d. h., eine Organisationseinheit (OU) erbt immer die Gruppenrichtlinien der höheren OU, wobei der Vorgang transitiv ist. Die Vererbung kann bei Bedarf deaktiviert werden. Durch die Einstellung ERZWUNGEN kann das aber wiederum außer Kraft gesetzt werden.
- Wenn Sie Einstellungen konfigurieren, ist es in den meisten Fällen günstiger, diese in verschiedene Gruppenrichtlinienobjekte (GPO) aufzuteilen. Hierdurch wird es einerseits übersichtlicher, andererseits verbessert sich auch die Wiederverwendbarkeit des einzelnen GPOs.

Wenn Sie also so, wie in Abbildung 11.17 gezeigt ist, mehrere Verknüpfungen erstellt haben, ist die Verknüpfungsreihenfolge konfigurierbar. Sie sehen die Zahlen in der ersten Spalte: Diese gibt die Abarbeitungsreihenfolge an. Beachten Sie, dass die Verknüpfung mit der niedrigsten Ordnungszahl zuletzt ausgeführt wird und im Zweifelsfall von den »Vorgängern« vorgenommene Änderungen überschreibt.

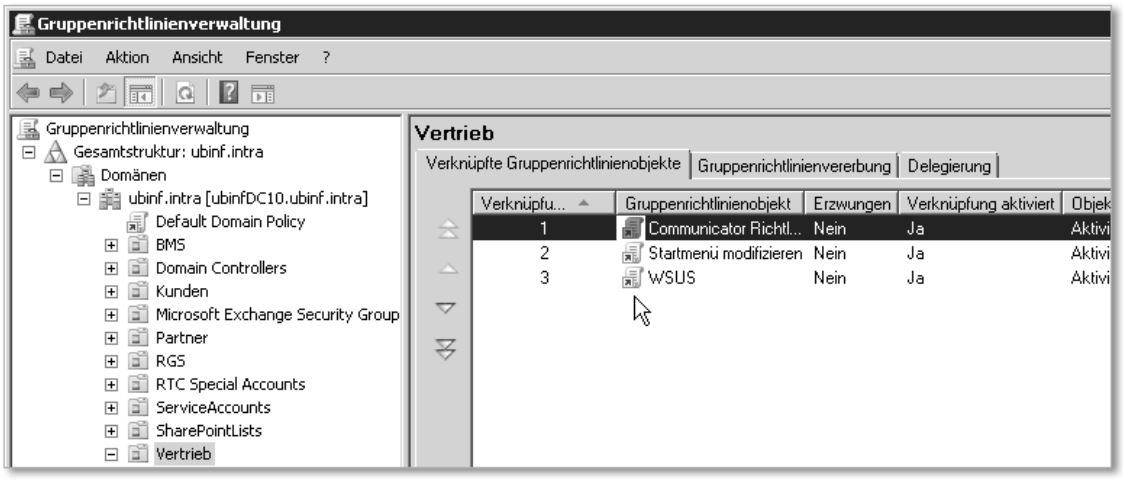


Abbildung 11.17 Wenn Sie mehrere Verknüpfungen zu Gruppenrichtlinienobjekten angelegt haben, ist deren Reihenfolge wichtig.

Nun dürfte der »Überschreiben-Fall« eigentlich nie auftreten – wenn doch, würde ich empfehlen, zunächst dieses organisatorische Problem zu lösen. Auf der Abbildung habe ich drei Verknüpfungen vorgenommen, nämlich eine zu einem GPO mit Richtlinien für *Office Communicator*, eine zur Modifikation des Startmenüs und eine für die Konfiguration des WSUS-Clients. Da jeweils gänzlich unterschiedliche Einstellungen vorgenommen worden sind, gibt es kein Überschreiben, sodass die Verarbeitungsreihenfolge letztendlich keine Rolle spielt – man sollte es aber trotzdem kennen.

Zum Stichwort »Abarbeitungsreihenfolge« gibt es in der Gruppenrichtlinienverwaltung noch ein wertvolles Mini-Werkzeug, auf das ich Sie an dieser Stelle hinweisen möchte (Abbildung 11.18): Auf der Registerkarte GRUPPENRICHTLINIENVERERBUNG findet sich eine Darstellung der angewendeten Richtlinien nebst Rangfolge. Es gilt, dass das Gruppenrichtlinienobjekt mit der kleinsten Ordnungszahl das zuletzt ausgeführte ist. Seine Einstellungen »gelten« also, sofern nicht zuvor für eine bestimmte Einstellung das Attribut ERZWUNGEN gesetzt worden ist.

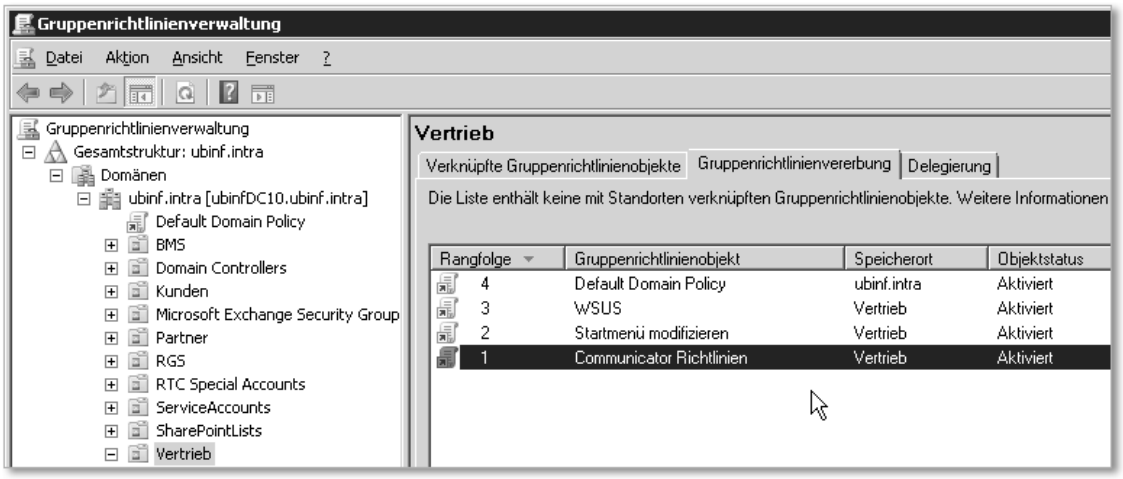


Abbildung 11.18 Auf der Registerkarte »Gruppenrichtlinienvererbung« gibt es einen Schnellüberblick über die Reihenfolge der Abarbeitung.

Gruppenrichtlinienmodellierung

Wenn Sie intensiver »forschen« möchten, bietet auch die Ansicht GRUPPENRICHTLINIENVERERBUNG zu wenige Details, sondern nur erste Anhaltspunkte. Mehr Informationen erhalten Sie mit der Funktion GRUPPENRICHTLINIENMODELLIERUNG, die später vorgestellt wird. Alte AD-Hasen kennen diese Funktion als RICHTLINIENERGEBNISSATZ.

11.8 Lokale GPOs

Windows 7/Vista und Windows Server 2008 kennen drei lokale Gruppenrichtlinienobjekte (GPOs), mit denen erstaunlicherweise Einstellungen des lokalen Computers konfiguriert werden können.

Es gibt drei GPOs, nämlich:

- das lokale Richtlinienobjekt (Local Policy Object)
- eine GPO für Administratoren und eine für Nicht-Administratoren
- eine benutzerspezifische lokale GPO

Diese GPOs, die übrigens bei der Verarbeitung die niedrigste Rangfolge haben (d. h., ihre Einstellungen werden von den Active-Directory-basierten GPOs überschrieben, falls es divergierende Einstellungen gibt), sind beispielsweise dann sinnvoll, wenn Sie in Ihrem Unternehmen »spezielle« Computer haben, für die zusätzliche Einstellungen getroffen werden müssen.

Das Konfigurieren der lokalen Gruppenrichtlinien funktioniert letztendlich nicht anders als bei den »normalen« Active-Directory-basierten Richtlinien.

Einleuchtenderweise gibt es keine Verknüpfungen, sondern es wird direkt das jeweilige Gruppenrichtlinienobjekt bearbeitet.

Ich zeige Ihnen nachfolgend im Schnelldurchlauf, wie man zur Konfiguration der jeweiligen Richtlinie gelangt. Die Screenshots sind übrigens auf einem Vista-PC entstanden – auf dem Windows Server 2008 sieht es genauso aus.

11.8.1 Das lokale Richtlinienobjekt bearbeiten

Um das lokale Richtlinienobjekt zu bearbeiten, starten Sie die *Management Console* (*mmc.exe*) und wählen das Hinzufügen eines Snap-Ins.

In dem Dialog, der sich dann öffnet, fügen Sie das Snap-In Gruppenrichtlinienobjekt-Editor hinzu und wählen in dem sich dann öffnenden Snap-In das vorgegebene Gruppenrichtlinienobjekt Lokaler Computer (Abbildung 11.19). Das war's schon.

Auf Abbildung 11.20 sehen Sie die geöffnete lokale Richtlinie. Sie ist bezüglich der Konfiguration in der Tat eine »ganz normale« GPO, in der sowohl Computer- als auch Benutzereinstellungen vorgenommen werden können.

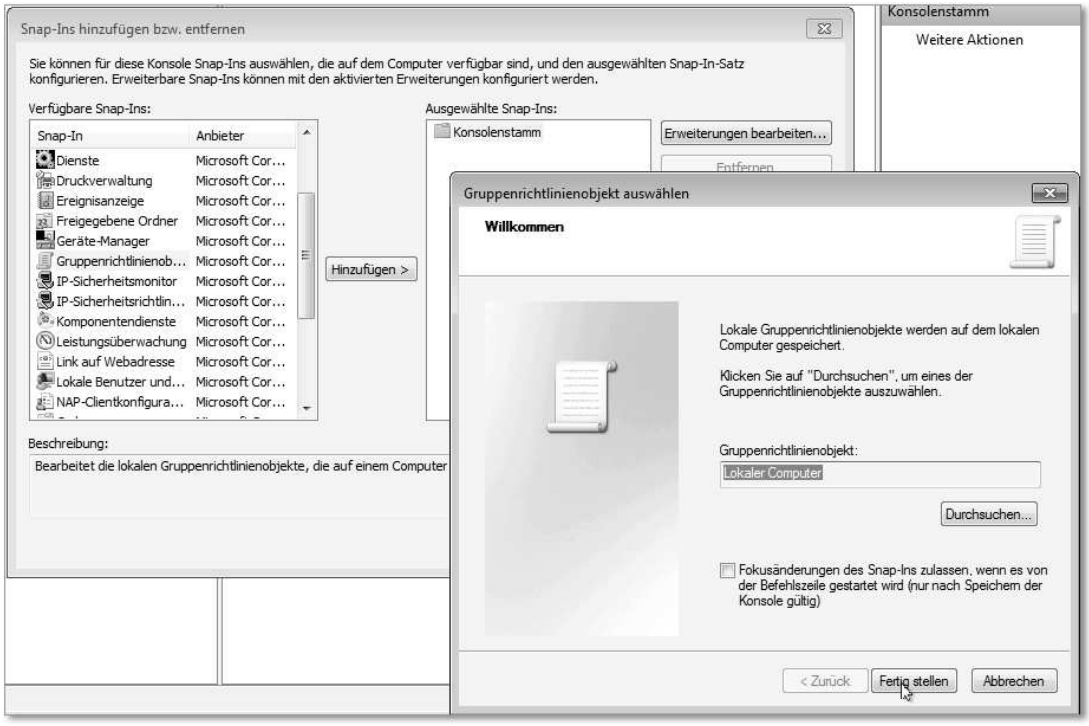


Abbildung 11.19 Um das lokale Richtlinienobjekt zu bearbeiten, wird die entsprechende Konsole geöffnet.

11.8.2 GPO für Administratoren und Nicht-Administratoren bearbeiten

Die GPO für Administratoren und Nicht-Administratoren ist insofern eine ganz »pfiffige« Angelegenheit, als dass Sie beispielsweise für lokale Admins weniger restriktive Einstellungen als für Nicht-Admins konfigurieren können.

Das Öffnen dieser Richtlinien funktioniert wie im zuvor beschriebenen Fall über das GRUPPENRICHTLINIENOBJEKT-EDITOR-Snap-In. Der einzige Unterschied ist, dass Sie in diesem Fall nicht das vorgegebene Objekt bestätigen, sondern DURCHSUCHEN anklicken und sich im folgenden Dialog entweder für die Gruppe ADMINISTRATOREN oder für die NICHT-ADMINISTRATOREN entscheiden (Abbildung 11.21).

Auf Abbildung 11.22 habe ich beide Richtlinien in einer Konsole geöffnet (fügen Sie dazu einfach zweimal das Snap-In mit unterschiedlichen Einstellungen hinzu). Zu erkennen ist, dass es »nur« Benutzereinstellungen gibt – schließlich handelt es sich hierbei um eine reine Benutzer-GPO.

11.8.3 Benutzerspezifische GPOs

Um eine lokale benutzerspezifische GPO zu erstellen, beginnen Sie wie in dem zuvor gezeigten Fall. In dem Dialog aus Abbildung 11.21 entscheiden Sie sich für den Benutzer, für den die Richtlinie erstellt werden soll.

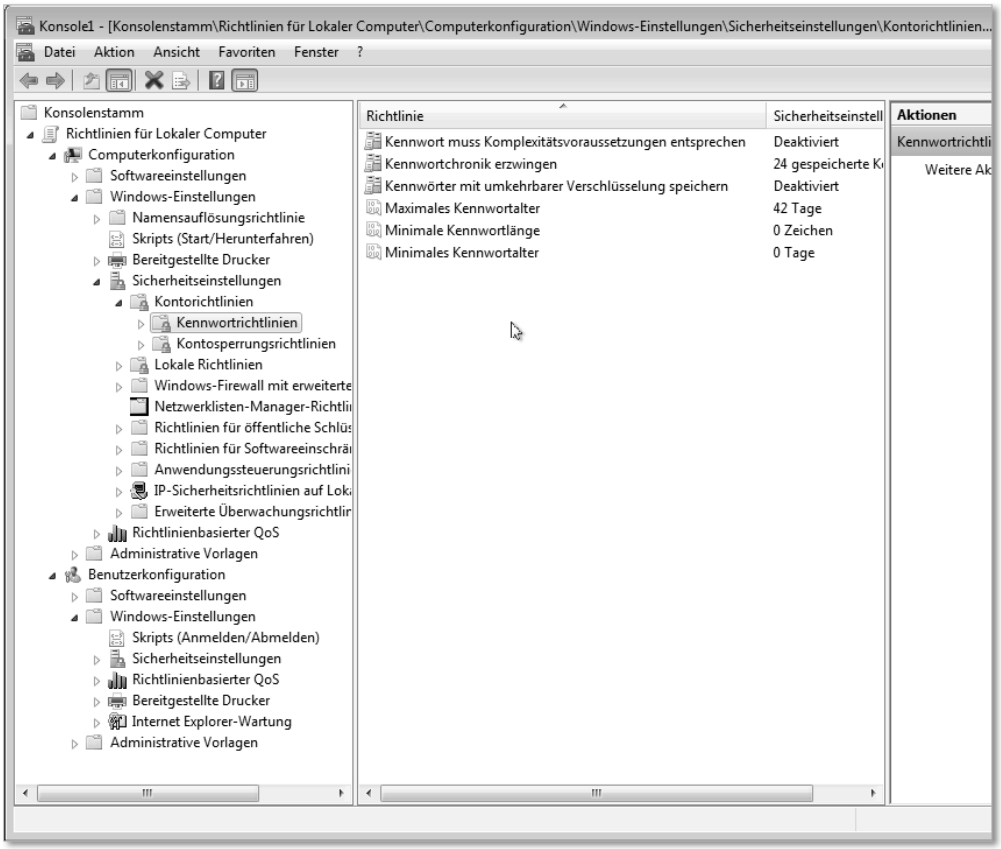


Abbildung 11.20 So bearbeiten Sie die »Richtlinien für Lokaler Computer«. Im Grunde genommen ist es eine ganz normale GPO.

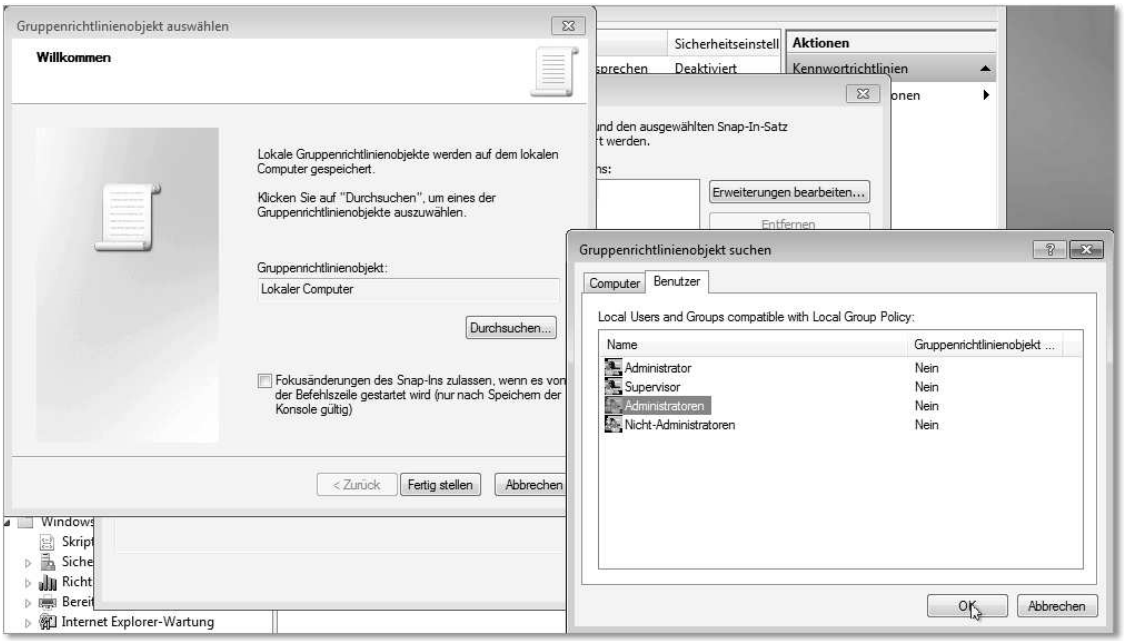


Abbildung 11.21 In diesem Dialog können Sie die Gruppen »Administratoren« und »Nicht-Administratoren« sowie einzelne Benutzer auswählen.

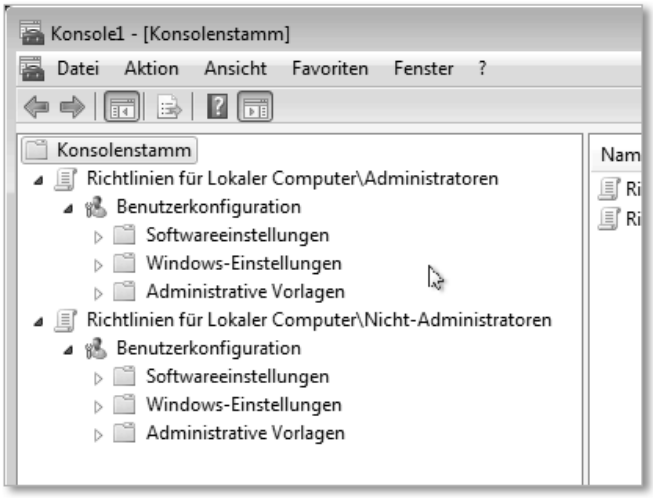


Abbildung 11.22 Hier werden die Einstellungen für lokale Administratoren und lokale Nicht-Administratoren zur Bearbeitung angezeigt.

Beachten Sie, dass Sie hier lediglich aus lokalen Benutzern auswählen können. Eine spezielle lokale Richtlinie für einen bestimmten Domänen-Benutzer können Sie leider nicht erstellen.

11.9 Starter-Gruppenrichtlinienobjekte/Starter-GPOs

Die Vererbung von Gruppenrichtlinien-Einstellungen ist ohne Zweifel eine sehr leistungsfähige Funktionalität, die aber nicht immer greift:

- Es könnte Szenarien geben, in denen ähnliche Abteilungen unternehmensweit so über die Domäne verteilt sind, dass die Einstellungen nicht über Vererbung vorgenommen werden können. Dies passiert beispielsweise, wenn das AD nach einem geografischen Modell aufgebaut ist und es an mehreren Standorten OUs mit Vertriebsmitarbeitern gibt.
- Über Domänengrenzen hinweg gibt es keine GPO-Vererbung. Wenn also alle Vertriebsmitarbeiter eines Konzerns mit mehreren Domänen die gleichen Einstellungen erhalten sollen, müssen Sie in jeder Domäne ein Gruppenrichtlinienobjekt anlegen.

Mit Windows Server 2008 gibt es hier eine Möglichkeit, um das »Immer-Wieder-Abtippen« von bestimmten Einstellungen zu vermeiden – die Lösung lautet *Starter-Gruppenrichtlinienobjekte* (*Starter-GPOs*). Diese können Sie sich als eine Art »Vorlage« vorstellen, die beim Erstellen von neuen Objekten herangezogen werden kann. Es gibt zwischen dem Starter-GPO und dem daraus erstellten Gruppenrichtlinienobjekt keine Vererbung, vielmehr handelt es sich um einen einmaligen Kopiervorgang.

Wenn Sie in der Gruppenrichtlinienverwaltung einen gezielten Blick in eine Domäne riskieren, werden Sie beim ersten Zugriff den Hinweis erhalten, dass noch kein Ordner für Starter-Gruppenrichtlinienobjekte in der Domäne vorhanden ist (Abbildung 11.23). Der per Mausklick auszulösende Erstellungsvorgang geschieht ohne weitere Eingaben oder sonstige vom Administrator auszuführende Aktionen.

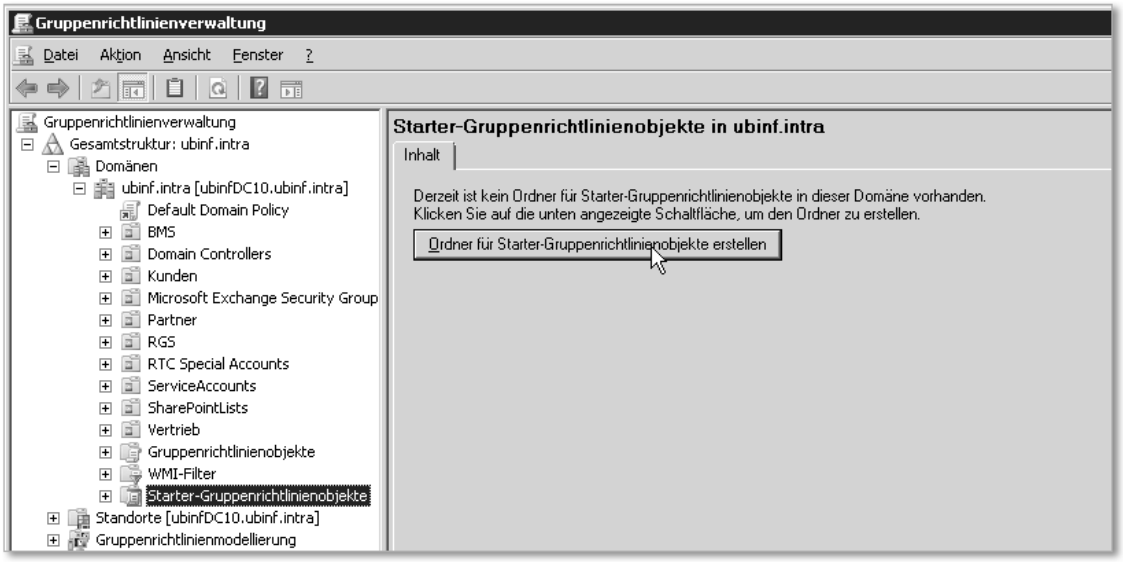


Abbildung 11.23 Beim ersten Anzeigen des Knotens »Starter-Gruppenrichtlinienobjekte« wird das Anlegen eines Ordners angeboten.

11.9.1 Anlegen

Um ein neues Starter-Gruppenrichtlinienobjekt zu erstellen, wählen Sie zunächst im Kontextmenü des Starter-Gruppenrichtlinienobjekt-Containers den Menüpunkt Neu (welch' Überraschung ...). Der sich daraufhin öffnende Dialog ist maximal unspektakulär, denn Sie können nur einen Namen und einen Kommentar eingeben (Abbildung 11.24).

Abbildung 11.24 Anlegen eines neuen Starter-GPOs – das ist nicht wirklich spektakulär.

Die eigentliche Arbeit beginnt, wenn das neue Objekt angelegt ist. Sie wählen dann in dessen Kontextmenü den Menüpunkt BEARBEITEN (Abbildung 11.25).

Abbildung 11.25 Das neu angelegte Starter-GPO-Objekt kann nun bearbeitet werden.

Das Bearbeiten der Einstellungen des Starter-Gruppenrichtlinienobjekts geschieht mit einer etwas modifizierten Version des Gruppenrichtlinien-Editors. Sie sehen auf Abbildung 11.26 grundsätzlich die bekannte Applikation, in der sowohl der Knoten COMPUTERKONFIGURATION als auch der Knoten BENUTZERKONFIGURATION vorhanden ist. Sie können aber »nur« ADMINISTRATIVE VORLAGEN bearbeiten.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, können Sie den Editor verlassen und das Starter-Gruppenrichtlinienobjekt verwenden.

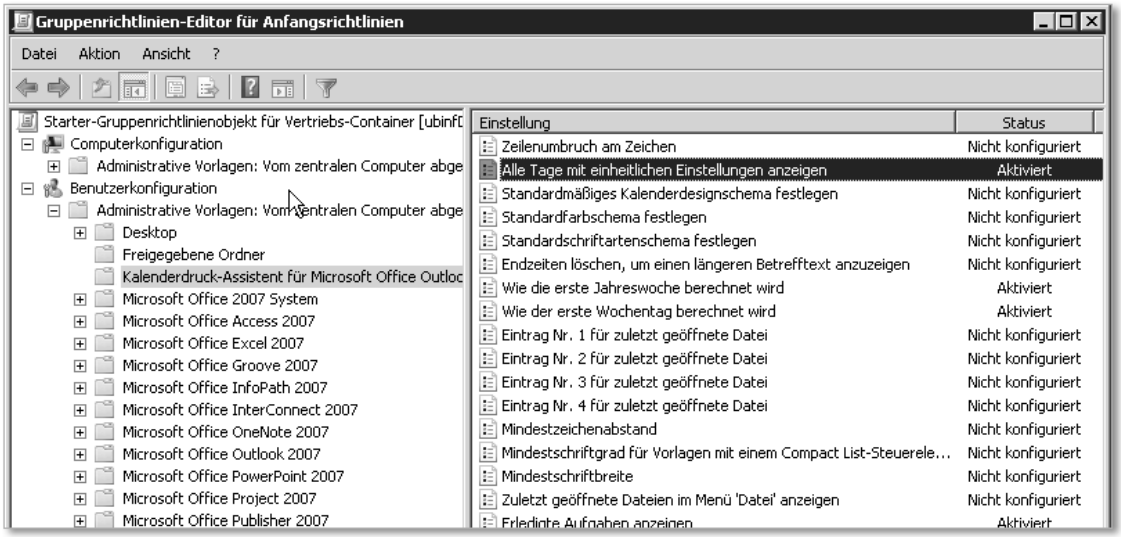


Abbildung 11.26 Das Bearbeiten der Starter-GPO erfolgt wie gewohnt im Gruppenrichtlinien-Editor. Es gibt allerdings »nur« den Knoten »Administrative Vorlagen«.

11.9.2 Anwenden

Um ein neues Gruppenrichtlinienobjekt aus einem Starter-Gruppenrichtlinienobjekt zu erstellen, wählen Sie im Kontextmenü des letztgenannten den entsprechenden Menüpunkt (Abbildung 11.27). Die einzige Eingabe, die nun von Ihnen verlangt wird, ist die Festlegung eines Namens für das neue GPO (Abbildung 11.28).

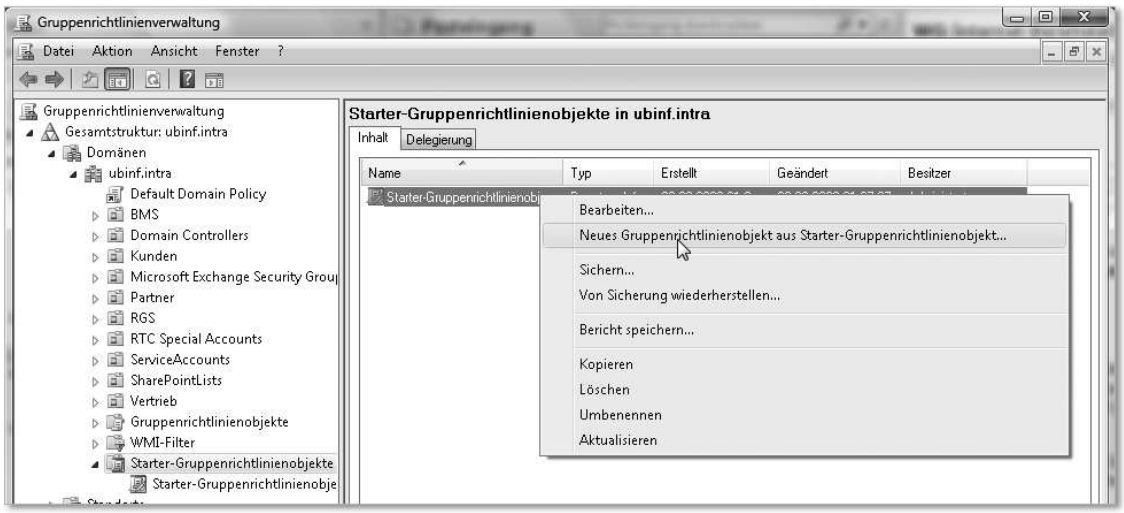


Abbildung 11.27 So erstellen Sie ein neues Gruppenrichtlinienobjekt aus dem Starter-GPO.

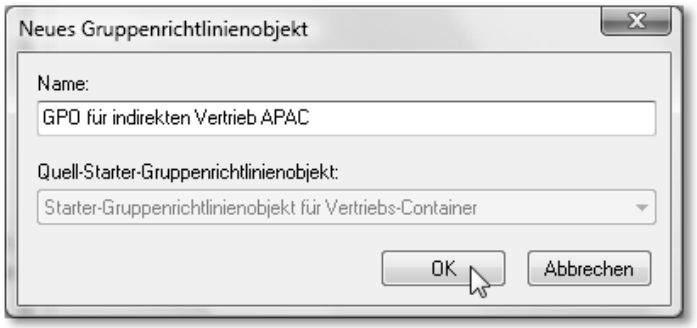


Abbildung 11.28 Beim Erstellen des neuen Gruppenrichtlinienobjekts müssen Sie lediglich den Namen angeben ...

Einen kurzen Augenblick später wird das neue GPO im Container GRUPPENRICHTLINIENOBJEKTE vorhanden sein. Eine erste kurze Inspektion zeigt, dass die Einstellungen des Starter-Objekts korrekt übertragen worden sind (Abbildung 11.29).

Nun können Sie bei Bedarf noch die eine oder andere Ergänzung oder Änderung vornehmen und dann die Verknüpfungen mit den OUs (oder der Domäne oder den Standorten) erstellen. Fertig.

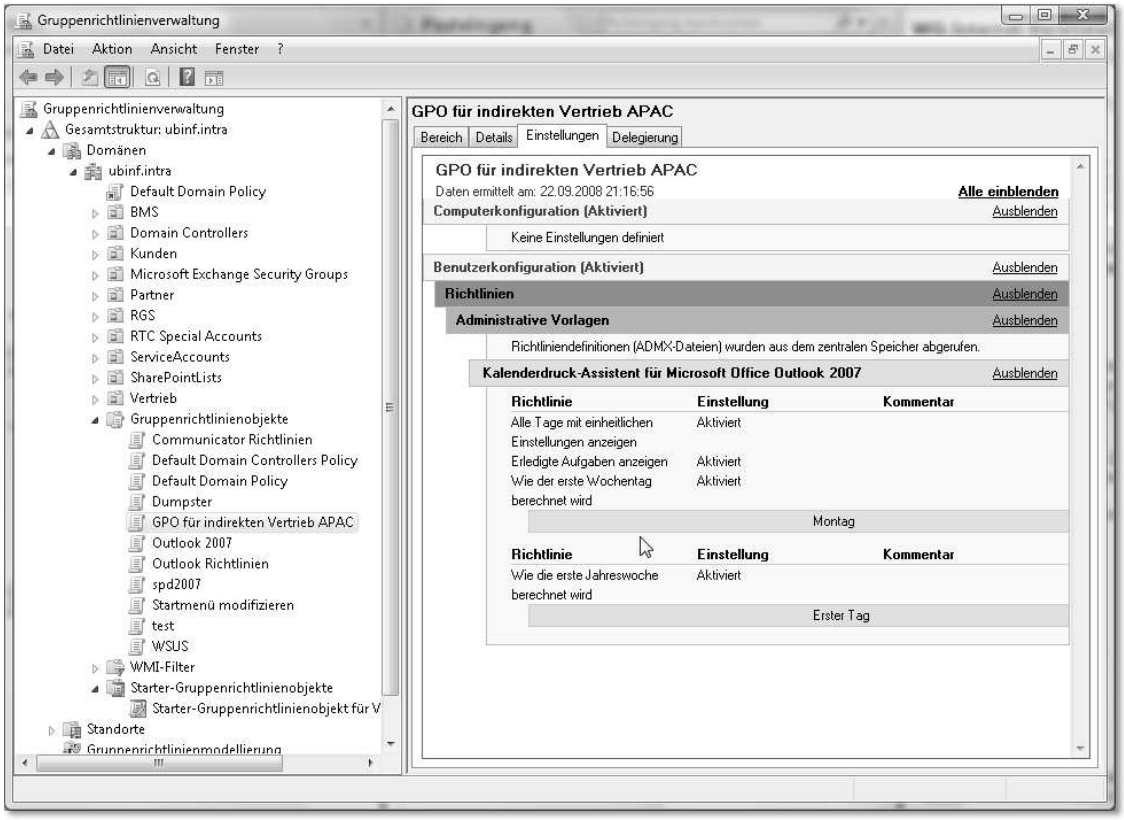


Abbildung 11.29 … et voilà: Alle Einstellungen sind in dem neuen Objekt vorhanden. Es kann nun noch modifiziert und dann einer OU zugewiesen werden.

11.9.3 Sichern & Co.

Etwas zu sichern ist in der IT immer eine gute Idee – um das zu erfahren, haben Sie aber bestimmt nicht dieses Buch gekauft. Gerade im Zusammenhang mit den Starter-Gruppenrichtlinienobjekten gibt es in der Tat noch einen anderen Anwendungsfall.

Wenn Sie ein Starter-Gruppenrichtlinienobjekt außerhalb »seiner« Domäne verwenden möchten, müssen Sie es sichern und in der zweiten Domäne zurücksichern. Das ist zum Glück simpel:

- Zunächst sichern Sie das Starter-Gruppenrichtlinienobjekt. Sie können dazu die Schaltfläche Als CAB-Datei speichern nutzen, die sich am Fuß des Starter-Gruppenrichtlinienobjekte-Dialogs befindet. Eingegeben wird ein simpler Dateiname; der Speicherort ist beliebig (Abbildung 11.30).
- Beim Laden des Starter-Gruppenrichtlinienobjekts wird die gesicherte CAB-Datei herangezogen. Der Dialog aus Abbildung 11.31 ermittelt einige grundlegende Angaben aus der CAB-Datei und kann über die Schaltfläche Einstellungen anzeigen sogar eine Art »Preview« des zu ladenden Objekts ausgeben.

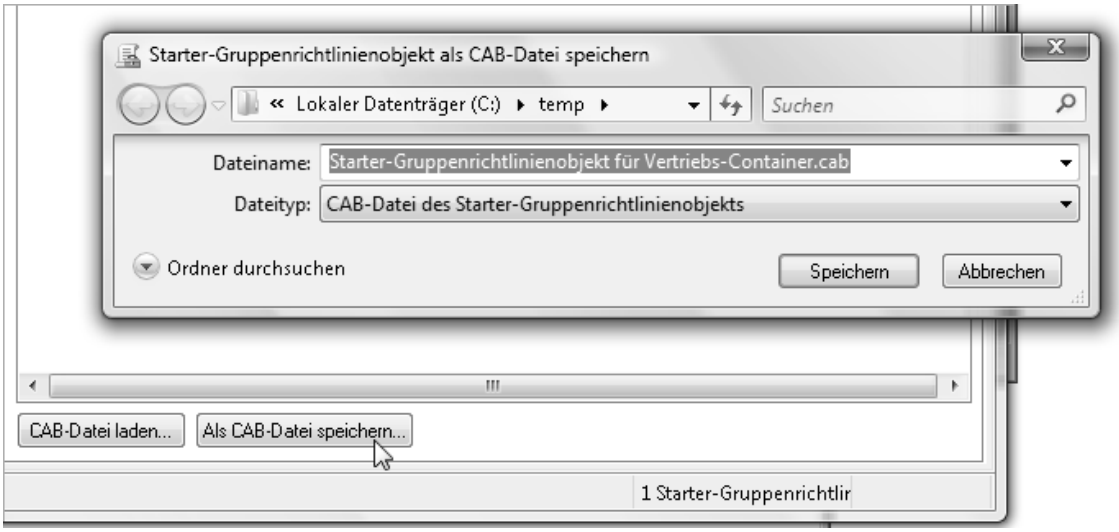


Abbildung 11.30 Das Starter-Gruppenrichtlinienobjekt kann als CAB-Datei gespeichert werden.

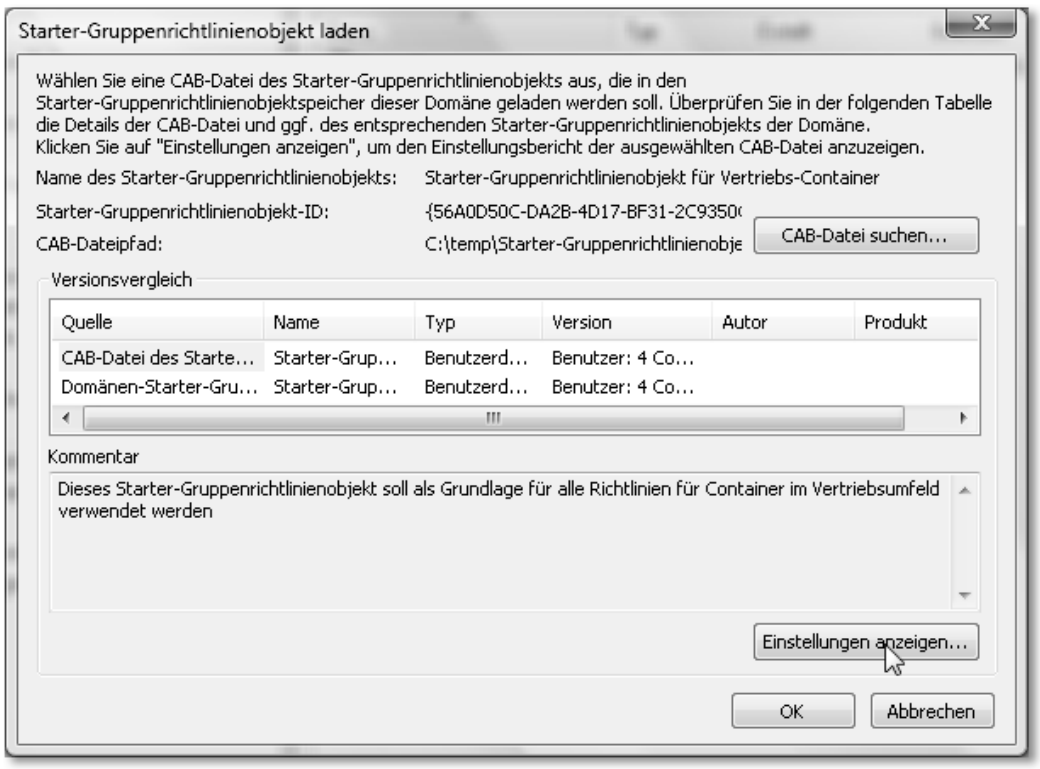


Abbildung 11.31 Eine Wiederherstellung des Starter-Gruppenrichtlinienobjekts ist ebenfalls einfach möglich. Vor der Wiederherstellung können Sie sich mittels »Einstellungen anzeigen« einen Überblick darüber verschaffen, was überhaupt »drinsteht«.

11.10 ADM vs. ADMX

Mit administrativen Vorlagen können beliebige Registry-Einstellungen in das »Gruppenrichtlinien-System« eingefügt werden. Der vermutlich häufigste Verwendungsfall sind die Gruppenrichtlinien-Vorlagen für Microsoft Office, die Tausende von Konfigurationsmöglichkeiten bieten, mit denen alle Office-Installationen von einer zentralen Stelle, nämlich dem Administrator-PC, aus konfiguriert werden können.

Seit nunmehr knapp 9 Jahren, genauer gesagt seit Februar 2000 mit der Einführung von Windows 2000, werden die administrativen Vorlagen in **.ADM*-Dateien gespeichert. Dieses Verfahren funktioniert zwar, hat aber einige entscheidende Nachteile, beispielsweise:

- Die **.ADM*-Dateien bieten keine Mehrsprachigkeit.
- Es gibt keine zentrale Ablage für die administrativen Vorlagen.
- In Zeiten, in denen im Wesentlichen alles in XML-Dokumenten gespeichert wird, wirkt das alte ADM-Format etwas »behäbig«.

Mit der Einführung von Windows Vista und Windows Server 2008 (und natürlich auch in der Folge mit Windows 7) hat Microsoft die administrativen Templates in ein neues XML-basiertes Format überführt: die *ADMX*-Dateien.

Bei Ihren ersten Schritten in der Applikation zur Gruppenrichtlinienverwaltungs haben Sie zunächst vermutlich noch nichts von ADMX-Dateien mitbekommen, trotzdem sollten und müssen Sie einige Hintergründe kennen. Unter anderem deshalb, weil Sie einen zentralen Speicherort einrichten müssen – das ist nichts Dramatisches, aber ein wenig Beschäftigung mit dem Thema ist unvermeidbar.

ADMX-Dateien sind Vorlagen

Falls Sie die Verwaltungswerkzeuge für das Active Directory auf einem Administrator-PC und nicht auf einem Server laufen lassen, müssen Sie diesen auf Windows Vista bringen und die dort installierbaren Verwaltungswerkzeuge einsetzen.

Die »alten« Verwaltungswerkzeuge können nicht mit den neuen ADMX-Dateien umgehen.

An dieser Stelle sei noch darauf hingewiesen, dass es sich bei den ADMX-Dateien (genauso wie bei den ADM-Dateien) um Richtlinien*vorlagen* handelt. Die resultierenden Richtlinien, die dann letztendlich auf PCs und Server angewendet werden, blieben unverändert und finden sich in den **.POL*-Dateien (vergleiche Abbildung 11.8).

Ich werde manchmal gefragt, ob die Verwendung von ADMX-Dateien dazu führt, dass Windows 2000- und XP-Clients keine Gruppenrichtlinien mehr empfangen können: Die Antwort ist ganz eindeutig Nein (denn es ändert sich »nur« etwas am Vorlagenformat und nicht an den vom Computer geladenen Richtlinien).

11.10.1 Kurze ADMX-Inspektion

Beim Blick in eine ADMX-Datei fällt zunächst auf, dass es sich um ein XML-Dokument handelt. Die meisten Administratoren sind zwar aus irgendwelchen mystischen Gründen von XML-Dokumenten recht wenig begeistert – aber es hilft ja nix … Unabhängig von eventuellen Ressentiments sind die XML-Dokumente nach meinem Geschmack wesentlich besser handhabbar als strukturlose Textdateien, was aber auch eine Frage des Werkzeugs ist, mit dem man sie bearbeitet.

Abbildung 11.32 Eine ADMX-Datei, in der eine Einstellung definiert ist …

Abbildung 11.32 zeigt eine ADMX-Datei, in der lediglich eine Einstellung vorgenommen wird. Der inhaltlich entscheidende Teil findet sich im Abschnitt `<policies>`, wobei in diesem Fall nur ein `<policy>`-Objekt vorhanden ist. Folgende Informationen sind in diesem enthalten:

- Es hat zunächst einen Namen, nämlich `DFSDiscoverDC`.
- Es handelt sich um eine Computerrichtlinie, was man an `class=«Machine«` erkennt. Alternative Werte sind `User` und `Both`.
- Der Anzeigename und die Beschreibung (`displayName`, `explainText`) sind in diesem XML-Dokument nicht vorhanden, es sind lediglich Verweise angegeben. Die anzuzeigenden Texte finden sich in einer separaten Datei (**.adml*), die in mehreren Sprachversionen vorliegen kann. Der Wert des Attributs `presentation` verweist ebenfalls auf einen Knoten in der *.ADML-Datei; dort werden die lokalisierten Namen der Eingabeelemente hinterlegt.
- Der Attribut-Wert `key` definiert den Pfad in der Registry.
- Unter `parentCategory` wird angegeben, wo in der Baumdarstellung diese Richtlinie angezeigt werden soll, nämlich unterhalb des Knotens NETZWERK (`windows:Network`).

- Weiterhin findet sich unterhalb von `supportedOn` die Angabe, ab welcher Betriebssystemversion diese Einstellung vorgenommen werden kann.
- Im Abschnitt `<elements>` können beliebig viele vom Benutzer anzugebende Werte definiert werden, also die Werte, die dann letztendlich in die Registry geschrieben werden. Auch hierzu werden in der *.ADML-Datei lokalisierte Beschreibungen vorgehalten.

Die ADML-Dateien liegen in einem Ordner unterhalb des eigentlichen Richtlinienverzeichnisses. Wie ich ein wenig später noch genauer zeigen werde, gibt es für jede Kultur ein separates Verzeichnis. Die Kultur besteht letztendlich aus zwei Angaben: der Sprache und der Region. Im deutschen Sprachraum gibt es folgende Kulturen:

de-AT	0x0C07	Deutsch (Österreich)
de-DE	0x0407	Deutsch (Deutschland)
de-LI	0x1407	Deutsch (Liechtenstein)
de-LU	0x1007	Deutsch (Luxemburg)
de-CH	0x0807	Deutsch (Schweiz)

Bei einem deutschsprachigen und für den Einsatz in Deutschland konfigurierten Windows Server 2008 oder Windows7/Vista existieren zwei Sprachverzeichnisse, nämlich de-DE und en-US. Abbildung 11.33 zeigt die **.adml*-Datei, die die zuvor gezeigte **.admx*-Datei um die deutschsprachigen Einträge ergänzt. Sie finden dort die Elemente, auf die in der **.admx*-Datei verwiesen wird.

DFS.adml* | DFS.admx* | Startseite

```
<?xml version="1.0" encoding="utf-8"?>
<!--  (c) 2006 Microsoft Corporation  -->
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                           revision="1.0" schemaVersion="1.0" xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefin
  <displayName>Anzeigenamen hier eingeben</displayName>
  <description>Beschreibung hier eingeben</description>
  <resources>
    <stringTable>
      <string id="DFSDiscoverDC">Festlegen, wie oft ein DFS-Client Domänencontroller sucht</string>
      <string id="DFSDiscoverDC_Help">Ermöglicht Ihnen festzulegen, wie oft ein DFS-Client (Distributed File System) versucht, Do

Standardmäßig versucht ein DFS-Client alle 15 Minuten, Domänencontroller zu finden.

Wenn Sie diese Einstellung aktivieren, können Sie festlegen, wie oft ein DFS-Client versucht, Domänencontroller zu finden. Der We

Wenn Sie diese Einstellung deaktivieren oder nicht konfigurieren, wird der Standardwert von 15 Minuten verwendet.

Hinweis: Der verfügbare Mindestwert ist 15 Minuten. Wenn Sie versuchen, einen niedrigeren Wert als 15 Minuten einzustellen, wird
    </stringTable>
    <presentationTable>
      <presentation id="DFSDiscoverDC">
        <decimalTextBox refId="DFSDiscoverDialog" defaultValue="15">Zeit in Minuten:</decimalTextBox>
      </presentation>
    </presentationTable>
  </resources>
</policyDefinitionResources>
```

Abbildung 11.33 … und die zugehörige deutsche Sprachdatei

Im Gruppenrichtlinienverwaltungs-Werkzeug sehen Sie den Konfigurationsdialog der Richtlinie; erwartungsgemäß finden sich alle Elemente, die in der **.admx*- und der **.adml*-Datei vorhanden sind, hier wieder (Abbildung 11.34).

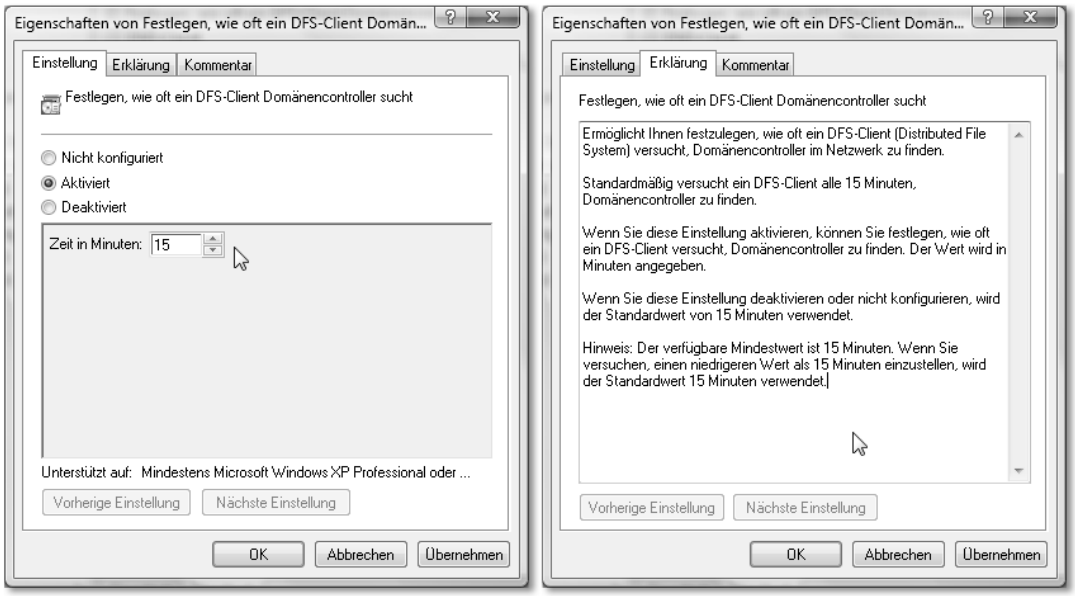


Abbildung 11.34 Das Ergebnis in der Gruppenrichtlinienverwaltungs-Applikation

11.10.2 Ablageorte und einen zentralen Speicherort einrichten

Nun stellt sich die unausweichliche Frage, wo die ADMX- und ADML-Dateien abgelegt werden. Da häufig eine weitere Forderung ist, dass die Gruppenrichtlinien nicht »nur« auf einem Domänencontroller bearbeitet werden können, sondern auch auf dem unter Vista laufenden Administrator-PC, wird diese Frage umso interessanter.

Auf einem Windows-Server-2008- oder Windows 7/Vista-Computer existiert ein Verzeichnis *c:\windows\PolicyDefinitions*, in dem die standardmäßigen ADMX- und ADML-Dateien liegen (Abbildung 11.35). Im Klartext bedeutet das, dass das Gruppenrichtlinienverwaltungs-Werkzeug jeweils auf die lokalen Vorlagen zurückgreift. Solange Sie »nur« mit den Standardvorlagen arbeiten, ist das kein Problem. Wenn Sie allerdings zusätzliche Vorlagen (z. B. solche für Microsoft Office oder »selbst gemachte«) verwenden, wäre es einigermaßen lästig, die Vorlagendateien kopieren zu müssen.

Nur die Vorlagen

Um auch an dieser Stelle Missverständnissen vorzubeugen: Es geht hier »nur« um die Vorlagen. Die eigentlichen Richtlinien (die *.pol-Datei etc. siehe Abbildung 11.8) werden unabhängig vom Vorhandensein der Richtliniendatei zwischen den Domänencontrollern repliziert und finden sich im SYSVOL-Verzeichnis.

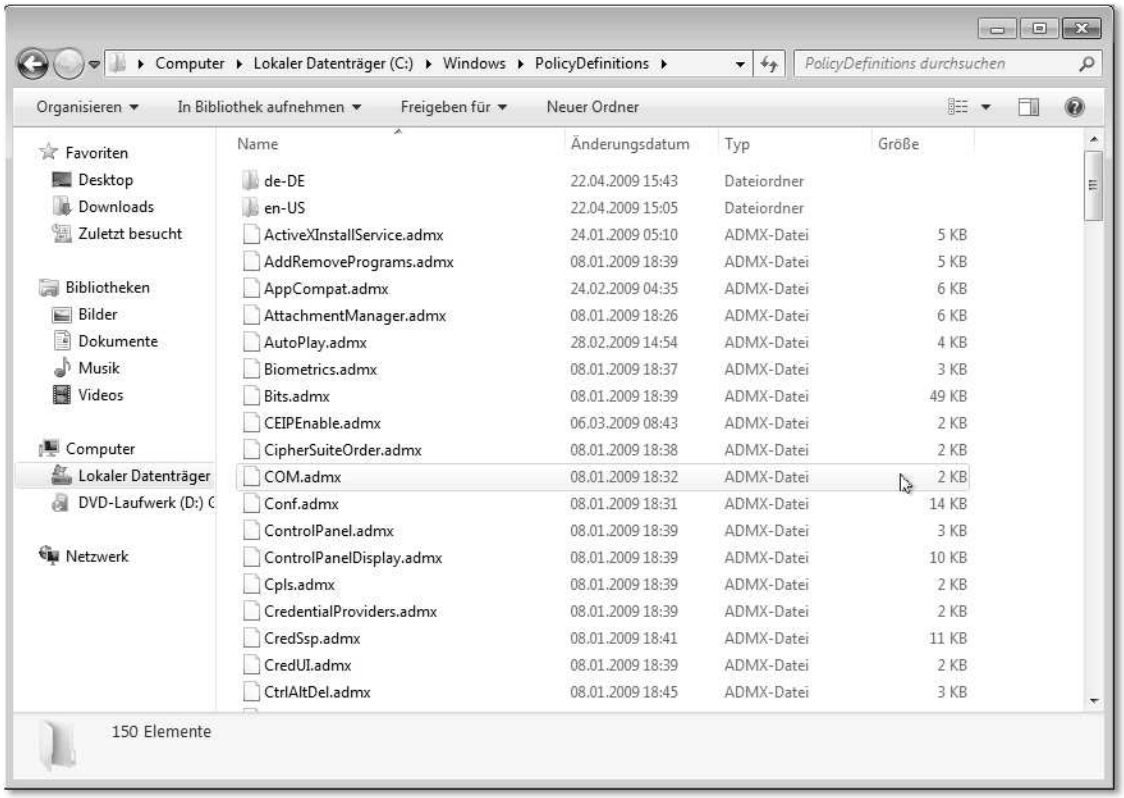


Abbildung 11.35 Standardmäßig liegen die ADMX- und ADML-Dateien auf einem Windows Vista- und einem Windows Server 2008-System genau hier.

Wesentlich schöner wäre es natürlich, wenn die Richtlinienvorlagen an einem zentralen Speicherort lägen, auf den dann das Gruppenrichtlinienverwaltungswerkzeug zugreift. Dies ist zwar vorgesehen, standardmäßig aber nicht implementiert (warum auch immer).

Das Einrichten des zentralen Speicherorts ist schnell erledigt. Kopieren Sie den kompletten *PolicyDefinitions*-Ordner in das Verzeichnis *c:\windows\SYSVOL\domain\Policies*. Das Ergebnis muss dann so wie auf Abbildung 11.36 gezeigt aussehen (der Screenshot stammt von einem Windows Server 2008).

Wenn Sie nun zusätzliche Vorlagen installieren möchten, kopieren Sie die zugehörigen Dateien ebenfalls an diesen zentralen Speicherort. Ich führe Ihnen das am Beispiel von Office 2007 vor:

- Im Microsoft Download Center erhalten Sie ein knapp 10 MB großes Paket namens *Administrative Vorlagendateien (ADM, ADMX, ADML) für 2007 Office System und Office-Anpassungstool Version 2.0.*
- Entpacken Sie das Paket in ein beliebiges (temporäres) Verzeichnis. Es enthält unter anderem den Ordner *ADMX*, in dem sich sowohl die eigentlichen Vorlagendateien als auch neun Ordner mit Sprachdateien finden (Abbildung 11.37).

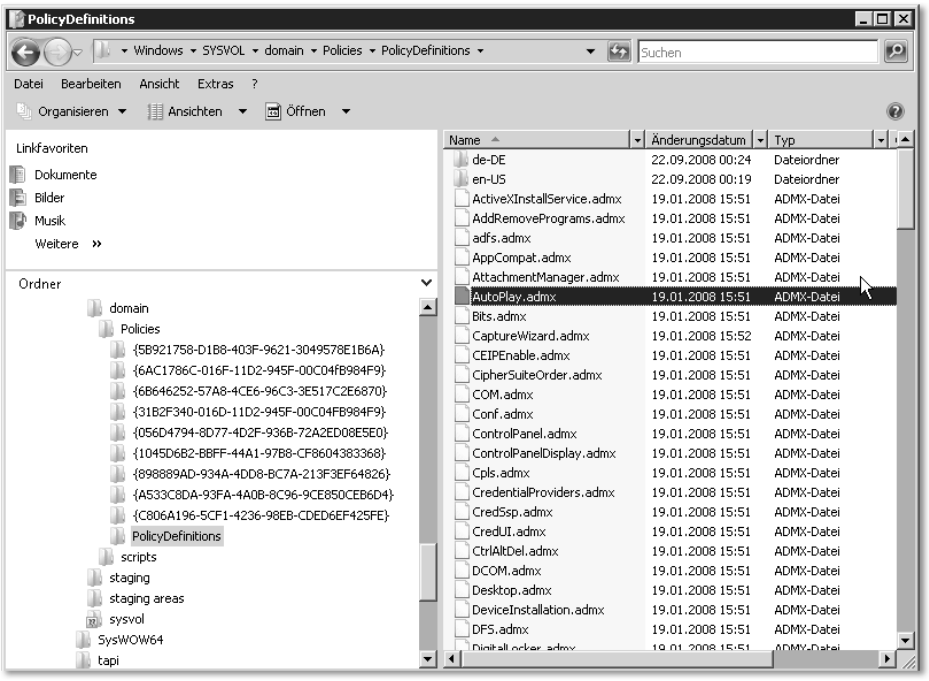


Abbildung 11.36 Um einen zentralen Speicherort für die Vorlagen (ADMX, ADML) einzurichten, legen Sie den »PolicyDefinitions«-Ordner unterhalb des Verzeichnisses »c:\windows\SYSVOL\domain\Policies« an. (Der Screenshot stammt vom Windows Server 2008.)

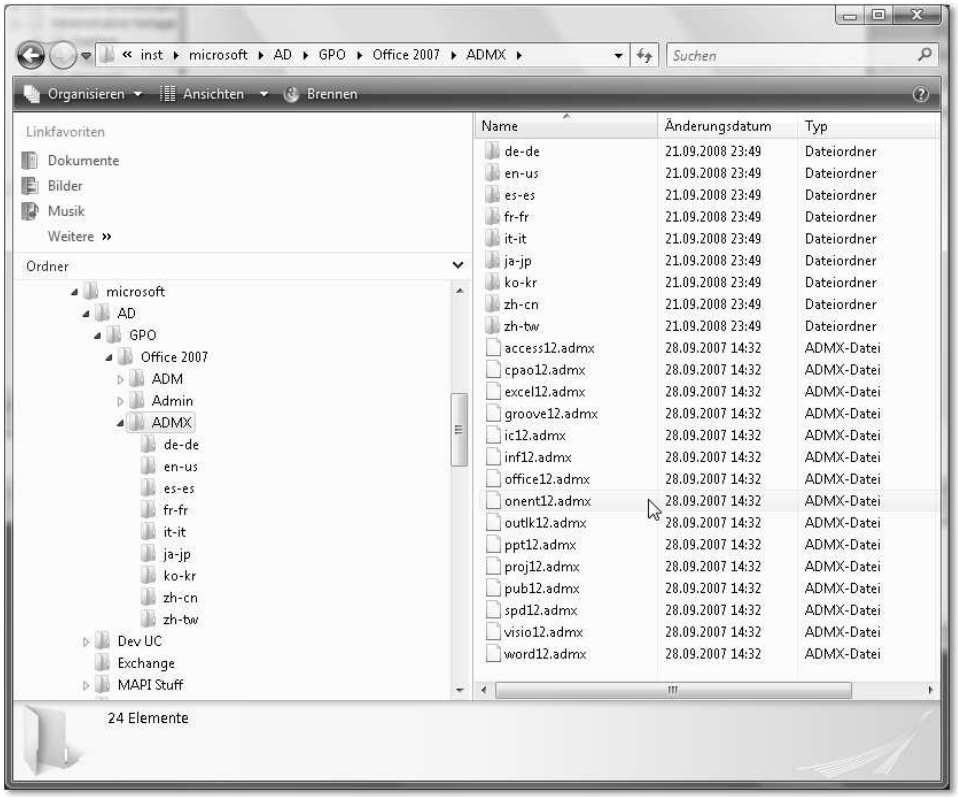


Abbildung 11.37 Das Vorlagenpaket für Office 2007 enthält ADMX-Dateien für die Applikationen nebst ADML-Dateien in neun Sprachen.

- Den Inhalt (!) des *ADMX*-Ordners kopieren Sie in den gemeinsamen Speicherort, wobei Sie natürlich nicht sämtliche Sprachen mitkopieren müssen.

  Um Missverständnisse zu vermeiden: Vereinfacht gesagt müssen die Office-ADMX-Dateien bei den »ursprünglichen« ADMX-Dateien liegen, und die ADML-Dateien kommen in die bereits vorhandenen Sprachverzeichnisse zu den bereits vorhandenen AMDL-Dateien.

Wenn Sie auf einer beliebigen Windows Server 2008-Maschine oder einem Vista-Client den Gruppenrichtlinienverwaltungs-Editor starten, werden Sie zwei Dinge feststellen (Abbildung 11.38):

- Alle in den zentrale Speicherort kopierten Vorlagen werden angezeigt.
- Beim Konto ADMINISTRATIVE VORLAGEN wird angezeigt, dass die Richtliniendefinitionen vom »zentralen Computer« abgerufen worden sind, also aus dem *SYSVOL*-Verzeichnis des Domänencontrollers, mit dem das Werkzeug arbeitet.

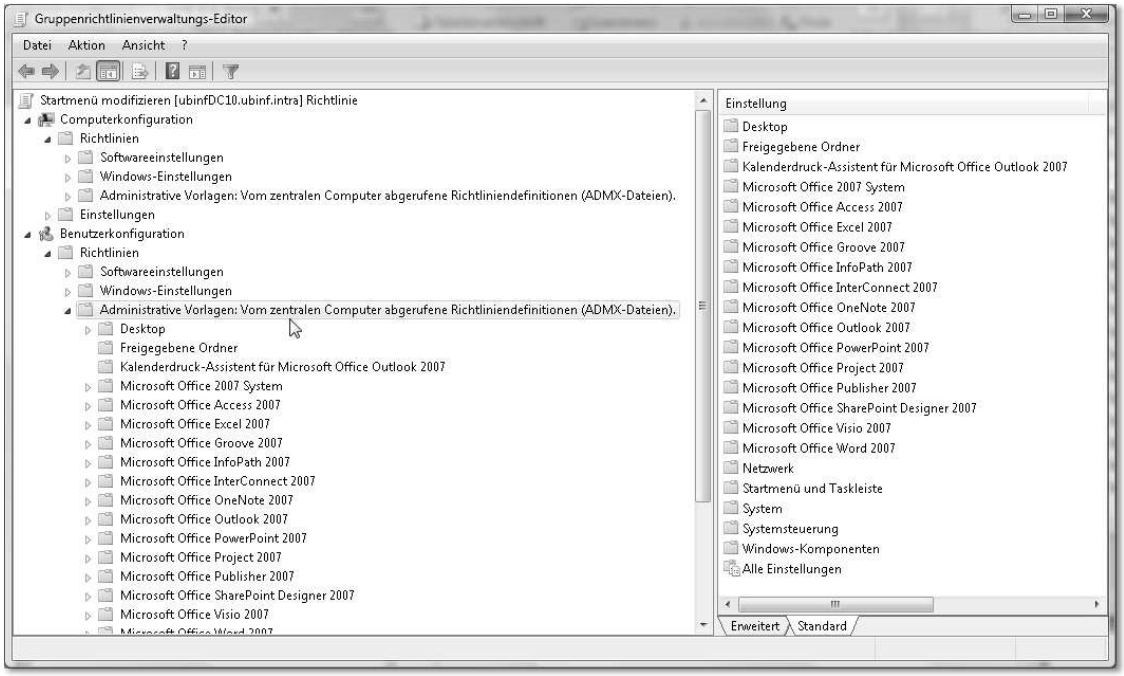


Abbildung 11.38 Der auf einem Vista-Client gestartete Gruppenrichtlinienverwaltungs-Editor zeigt automatisch alle im zentralen Speicherort installierten Vorlagen an.

11.10.3 Windows 7-ADMX-Dateien in ältere Systeme kopieren

Falls Sie nicht zufällig eine Domäne auf Basis von Windows Server 2008 R2 einsetzen, der bereits die aktuellen ADMX-Dateien mitbringt, müssen Sie die Windows 7-Dateien in das zentrale *PolicyDefinitions*-Verzeichnis kopieren. Damit nichts schiefgeht, folgt hier die genaue Anleitung:

- Auf einem Windows 7-PC navigieren Sie zum Ordner *c:\Windows\PolicyDefinitions*. In diesem liegen alle benötigten Dateien.
- Diese Dateien (**.asmx* inklusive der **.adml*-Dateien in den Unterverzeichnissen) kopieren Sie in das zentrale Verzeichnis *c:\windows\SYSVOL\domain\Policies\PolicyDefinitions* auf einem Domänencontroller (siehe auch Abbildung 11.36).

Wenn alles funktioniert hat, wird der Gruppenrichtlinienverwaltungs-Editor einige Richtlinien anzeigen, die als Anforderung Windows 7 haben (Abbildung 11.39).

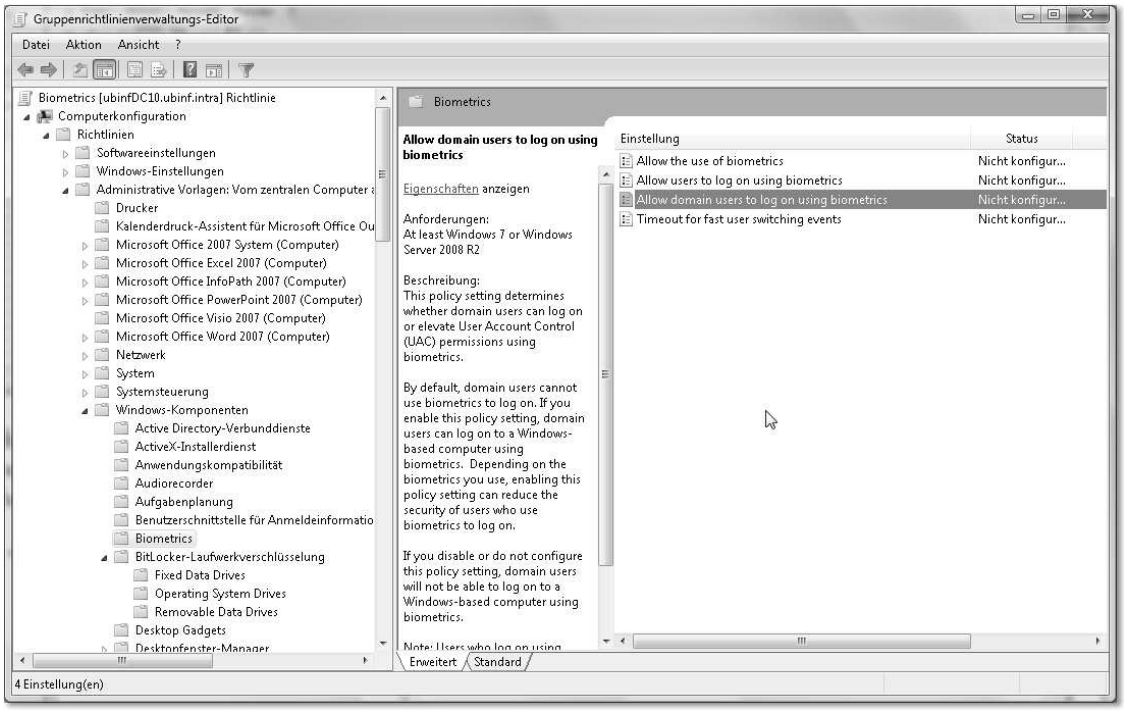


Abbildung 11.39 Nach dem Kopieren der Windows 7-Policy-Dateien in den zentralen Ordner sollten auch Richtlinien angezeigt werden, die als Mindestanforderung Windows 7 haben.

Nun steht dem Erstellen von speziellen Windows 7-Richtlinien nichts im Wege. An dieser Stelle möchte ich noch darauf hinweisen, dass die meisten »alten« Richtlinien (also solche, die auch schon mit Windows 2000 funktionsfähig waren) auch auf Windows 7 wirken.

11.10.4 ADM-Dateien migrieren

Wenn Sie eigene ADM-Dateien erstellt haben oder Produkte einsetzen, zu denen solche Vorlagen mitgeliefert worden sind, werden Sie sich fragen, wie nun die weitere Vorgehensweise ist. Sie haben zwei Möglichkeiten:

- Die »alten« ADM-Dateien werden von den Windows Server 2008-Gruppenrichtlinienverwaltungs-Werkzeuge unterstützt. Das Einfügen einer Gruppenrichtlinie, die auf einer ADM-Datei beruht, erfolgt wie unter Windows Server 2003.
- Der im Allgemeinen »bessere Weg« ist aber, die ADM-Datei in eine ADMX-Datei umzuwandeln.

Das Konvertieren der ADM- in eine ADMX-Datei muss nicht von Hand vorgenommen werden, da freundliche Menschen entsprechende Werkzeuge entwickelt haben. Zu diesen freundlichen Menschen gehören die Mitarbeiter der Firma *FullArmor*, die mit dem *ADMX Migrator* genau das passende Werkzeug entwickelt haben. Es ist im Microsoft Download Center erhältlich. Sie finden es, wenn Sie nach »ADMX Migrator« suchen.

Die Installation läuft assistentenbasiert ab, es gibt dazu keine weiteren Anmerkungen (Abbildung 11.40). Die Installation ist übrigens auch auf dem Administrator-PC möglich, Sie brauchen das Tool also nicht auf Ihrem schönen Domänencontroller zu installieren.

Abbildung 11.40 Den ADMX-Migrator bekommen Sie im Microsoft Download Center.

Um eine ADM-Datei zu konvertieren, starten Sie den ADMX Migrator und wählen im Kontextmenü den Menüpunkt GENERATE ADMX FROM ADM (Abbildung 11.41). Es wird sich ein Dialog zur Auswahl der ADM-Datei öffnen. Nach dem Selektieren der Datei beginnt die Konvertierung. Am Ende werden gegebenenfalls einige Warnungen angezeigt, beispielsweise zu nicht korrekt gesetzten Standard-

werten oder dergleichen. Zuletzt erscheint der Dialog aus Abbildung 11.42, in dem angegeben wird, wo genau die neu erzeugten Dateien zu finden sind – nämlich in einem zufällig benannten Verzeichnis im temporären Ordner des angemeldeten Benutzers.

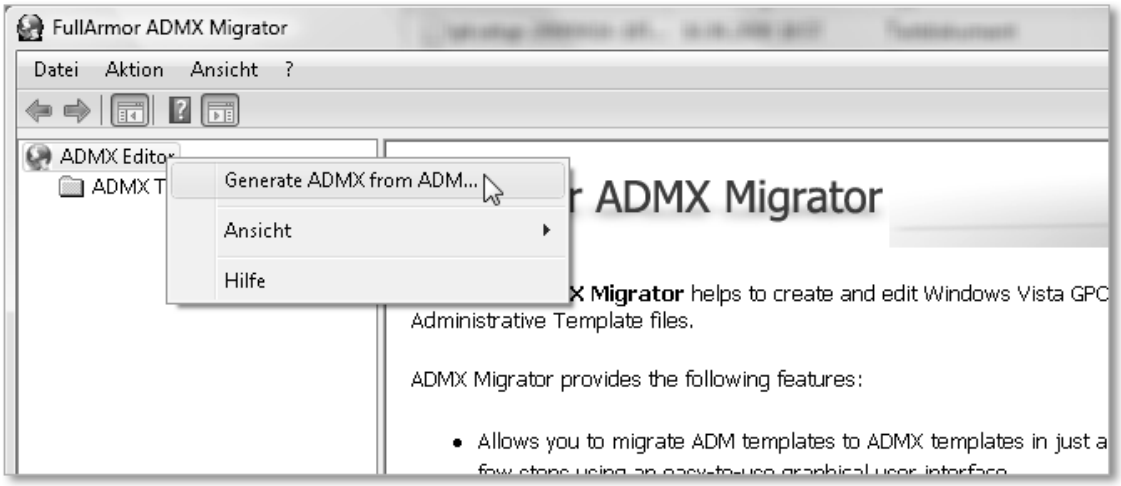


Abbildung 11.41 Der Konvertierungsvorgang beginnt im Kontextmenü.

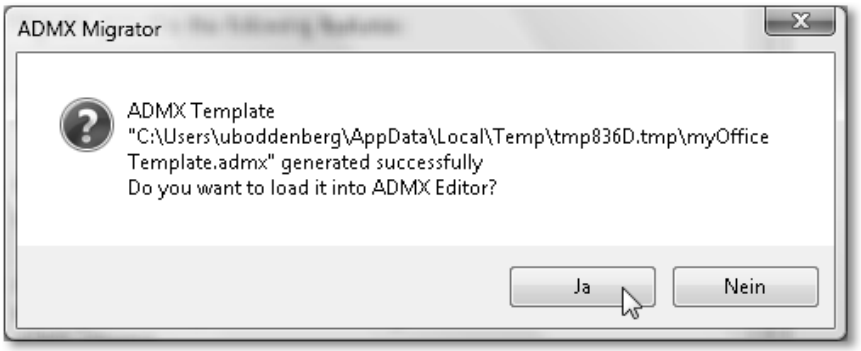


Abbildung 11.42 Die konvertierten Dateien werden in einem zufällig benannten Unterordner des Benutzer-Temp-Verzeichnisses angelegt.

Wenn Sie die erzeugte Vorlage in den ADMX-Editor laden lassen (siehe die Anzeige in Abbildung 11.42) erhalten Sie in etwa die Ansicht aus Abbildung 11.43. Sie können die Einstellungen anschauen und gegebenenfalls editieren.

Wenn Sie ein wenig »hinter die Kulissen« schauen, genauer gesagt in das Verzeichnis, in dem die neue Vorlage angelegt wurde, sehen Sie das bekannte Bild: Es ist eine ADMX-Datei vorhanden, außerdem befindet sich in einem gemäß der Sprache benannten Ordner die zugehörige ADML-Datei (Abbildung 11.44).

Im Kontextmenü der neu erzeugten Vorlage findet sich der Menüpunkt Save As, mit dem Sie die Dateien in einem etwas »benutzerfreundlicheren« Ordner (was das Finden betrifft) speichern können. Der Dialog ermöglicht die Auswahl der

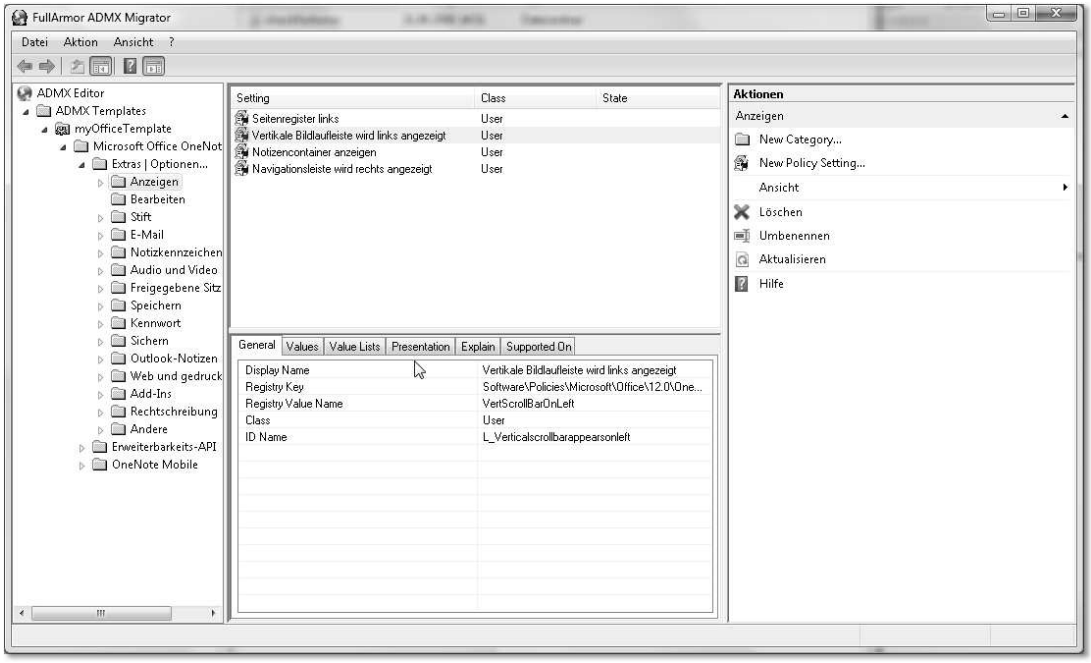


Abbildung 11.43 Ein Blick in die konvertierte Vorlage. Auf Wunsch können Sie sie auch bearbeiten.

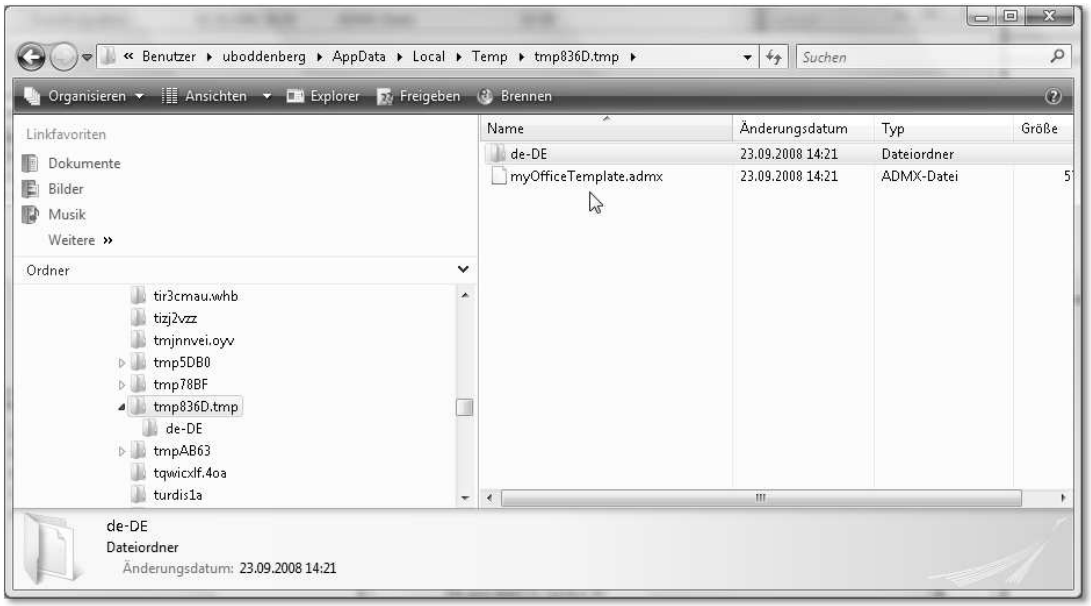


Abbildung 11.44 Es wurde übrigens eine ADMX-Datei nebst einer ADML-Datei im Kultur-Verzeichnis erzeugt.

Sprache, womit Sie letztendlich den Namen des Ordners der ADML-Datei beeinflussen (Abbildung 11.45).

Es stellt sich nun noch die Frage, wohin die erzeugten Dateien kopiert werden müssen. Die Antwort ist zweigeteilt:

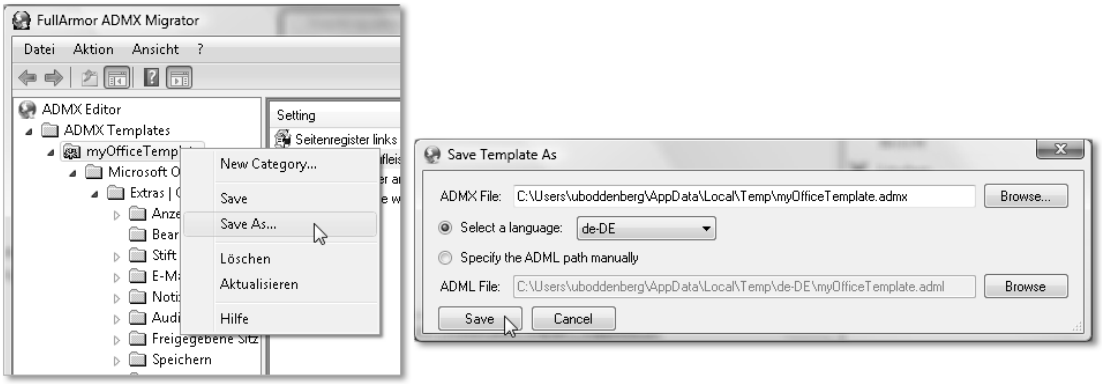


Abbildung 11.45 Beim Speichern können Sie die Sprache angeben.

- Wenn Sie einen zentralen Speicherort für die Vorlagen eingerichtet haben, werden die Dateien dort hineinkopiert (siehe Ausführungen im vorherigen Abschnitt).
- Falls Sie aus irgendwelchen Gründen keinen zentralen Speicherort eingerichtet haben, kommen die Dateien in das Verzeichnis *c:\windows\PolicyDefinitions.*

Das Gruppenrichtlinienverwaltungs-Werkzeug wird die neue Vorlage direkt anzeigen, und Sie können darauf basierende neue Gruppenrichtlinien anlegen.

11.10.5 Eigene ADMX-Dateien erstellen

Wenn Sie eigene ADMX-Dateien erstellen möchten, können Sie das entweder »zu Fuß« erledigen, oder aber Sie verwenden den ADMX Migrator. Bei der Arbeit mit dem ADMX Migrator beginnt das Erstellen einer eigenen Vorlage mit dem Befehl NEW TEMPLATE im Kontextmenü (Abbildung 11.46).

Nachdem Sie einen Namen für die neue Vorlage eingegeben haben, befindet sich der ADMX Migrator direkt im »Arbeitsmodus« (Abbildung 11.47): Hier können Sie nun zunächst einige grundlegende Einstellungen zur Vorlage vornehmen, beispielsweise auch, für welche Betriebssysteme sie gültig ist (SUPPORTED ON).

Als Nächstes erzeugen Sie Kategorien (NEW CATEGORY) und darin wieder weitere Kategorien und/oder Einstellungen (NEW POLICY SETTING).

Aus Gründen der vorgesehenen maximalen Seitenzahl für dieses Buch möchte ich jetzt nicht in epischer Breite vorführen, wie eine neue ADMX-Datei im ADMX Migrator erzeugt wird. Wenn Sie wissen, welche Registry-Einstellungen die Richtlinie modifizieren soll, und sich ein wenig mit ADMX Migrator beschäftigen, werden Sie recht schnell zum gewünschten Erfolg kommen.

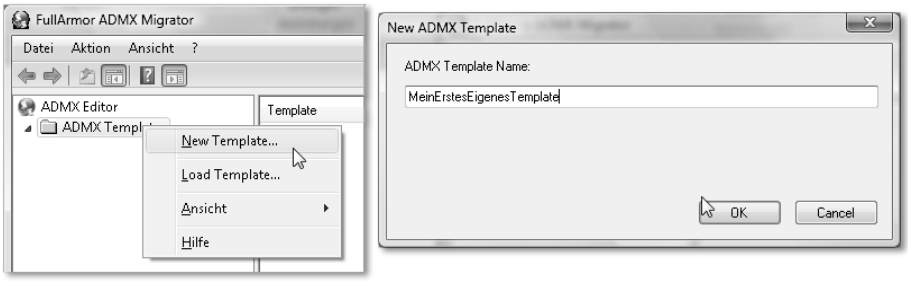


Abbildung 11.46 Auch eigene ADMX-Vorlagen können bequem mit dem ADMX Migrator erstellt werden.

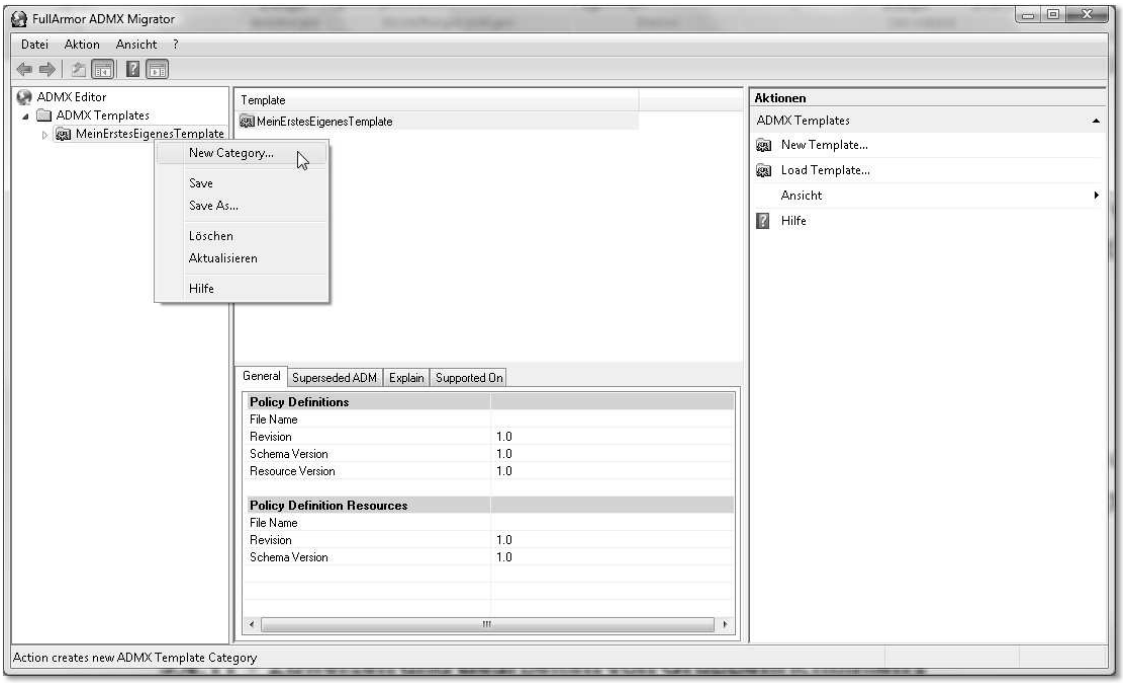


Abbildung 11.47 Und so füllt sich das eigene Template allmählich mit Leben.

11.11 Zuweisen und Bearbeiten von Gruppenrichtlinien

In Windows 2000 Server und Windows Server 2003 wurde die Konfiguration der Gruppenrichtlinien im EIGENSCHAFTEN-Dialog des Objekts (Domäne, OU, Standort) im *Active Directory-Benutzer und -Computer*-Snap-In (bzw. *Standorte und Dienste*-Snap-In für die Standortrichtlinie) vorgenommen. Man konnte zwar das gewünschte Ergebnis erreichen, es war aber nicht wirklich komfortabel. Microsoft hat dann die *Group Policy Management Console* (GPMC) zum Download bereitgestellt – und alle, die viel mit Gruppenrichtlinien gearbeitet haben, dürften dieses Werkzeug verwendet haben.

Mit Windows Server 2008 ist der »alte Weg«, also die Verwaltung der Gruppenrichtlinien im *Active Directory-Benutzer und -Computer*-Snap-In nicht mehr mög-

lich (in den Beta-Versionen ging das übrigens noch), stattdessen arbeitet man mit dem Nachfolger der *Group Policy Management Console* (GPMC) – und das Teil heißt jetzt *Gruppenrichtlinienverwaltung*. Es ist auf einem Windows-Server-2008-Domänencontroller standardmäßig vorhanden, auf einem Windows 7- oder Vista-PC steht es zur Verfügung, wenn Sie die Windows-Server-2008-Administrationswerkzeuge installieren (erhältlich im Microsoft Download Center; es gibt getrennte Downloads für Windows 7 und Vista).

Wenn Sie die vorangegangenen Seiten des Kapitels durchgearbeitet haben, wird Ihnen die Gruppenrichtlinienverwaltung bereits mehrfach auf Abbildungen begegnet sein; aber weil es so schön ist, zeige ich Sie Ihnen nochmals zum Einstieg in das Thema – also genießen Sie den wunderschönen Anblick auf Abbildung 11.48.

Keine Anmeldung am Server nötig

Die Abbildung ist übrigens auf einem Windows Vista-PC entstanden, den ich als Admin-PC für die Windows Server 2008-Umgebung verwende. Da ich Ihnen alle Schritte dieses Abschnitts auf dieser Maschine zeigen werde, erbringe ich auch gleich noch den Beweis, dass es absolut nicht notwendig ist, sich zu Administrationszwecken auf dem Server anzumelden. Mit den Admin-Werkzeugen für Windows 7 funktioniert es analog.

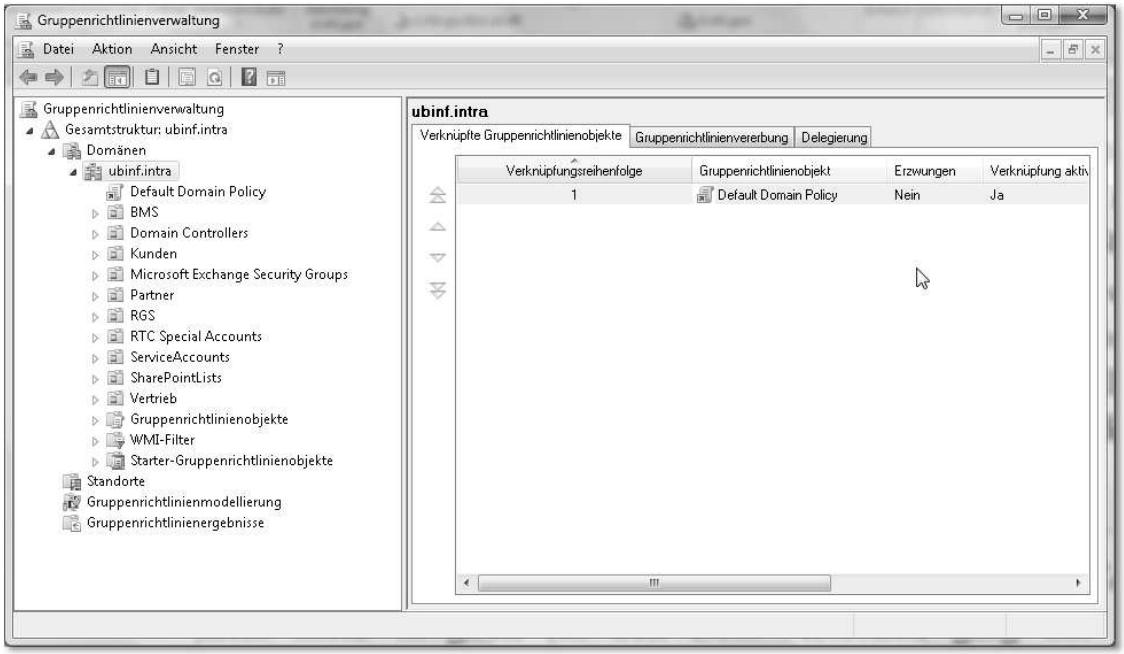


Abbildung 11.48 Die Gruppenrichtlinienverwaltung – hier auf einem Windows Vista-PC

Auch wenn Sie bislang nicht mit der GPMC gearbeitet haben, wird Ihnen die Arbeit mit der Gruppenrichtlinienverwaltung leicht von der Hand gehen – eventuell brauchen Sie eine kleine Eingewöhnungszeit, aber die wird nicht sehr schmerzhaft sein.

»Nur« Verknüpfungen

Bei der Arbeit mit der Gruppenrichtlinienverwaltung gibt es letztendlich einen Aspekt, den Sie sich vor Augen halten müssen. Ein Gruppenrichtlinienobjekt »klebt« niemals direkt an einer Domäne, einer OU oder einem Standort. Es gibt »nur« Verknüpfungen zu Gruppenrichtlinienobjekten, wobei ein Gruppenrichtlinienobjekt durchaus mit mehreren OUs verknüpft werden kann.

Viele Administratoren von kleineren Umgebungen, die bisher nicht mit der GPMC gearbeitet haben, tun sich mit diesem Zusammenhang schwer und finden die Gruppenrichtlinienverwaltung daher unhandlich. Es hilft Ihnen aber nichts, Sie müssen da durch! Ich wiederhole hier ausnahmsweise eine Abbildung (Abbildung 11.49), damit Sie sie ausschneiden und über den Schreibtisch oder – noch besser – über Ihr Bett hängen können, und zeige Ihnen die Zusammenhänge auf.

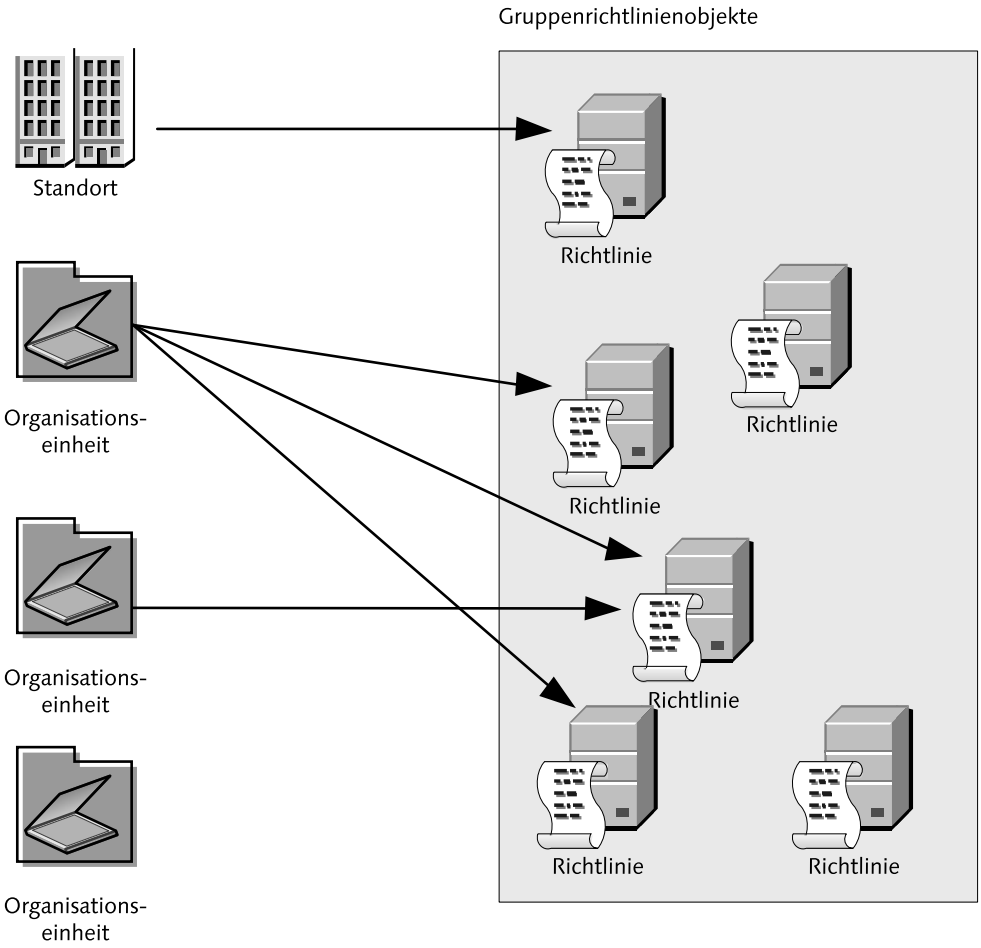


Abbildung 11.49 Eine Domäne, eine Organisationseinheit bzw. ein Standort ist mit den Gruppenrichtlinienobjekten »nur« verknüpft.

11.11.1 Gruppenrichtlinienobjekte anlegen und bearbeiten

Der erste Schritt ist das Anlegen eines Gruppenrichtlinienobjekts. Es gibt hierzu prinzipiell zwei Möglichkeiten:

- Sie navigieren zum Container GRUPPENRICHTLINIENOBJEKTE innerhalb der Domäne. In dessen Kontextmenü finden Sie den Menüpunkt NEU. Beim Neu-Anlegen des Gruppenrichtlinienobjekts können Sie zunächst den Namen auswählen, außerdem kann ein Starter-Gruppenrichtlinienobjekt (eine Art Vorlage, siehe Abschnitt 11.9) angegeben werden (Abbildung 11.50).
- Die zweite Möglichkeit ist, im Kontextmenü einer Organisationseinheit den Menüpunkt GRUPPENRICHTLINIENOBJEKT HIER ERSTELLEN UND VERKNÜPFEN zu wählen. Das Gruppenrichtlinienobjekt wird dabei ebenfalls im Container GRUPPENRICHTLINIENOBJEKTE erstellt, allerdings wird direkt eine Verknüpfung zur Organisationseinheit erstellt. Verknüpfungen zu weiteren OUs können natürlich später ebenfalls angelegt werden.

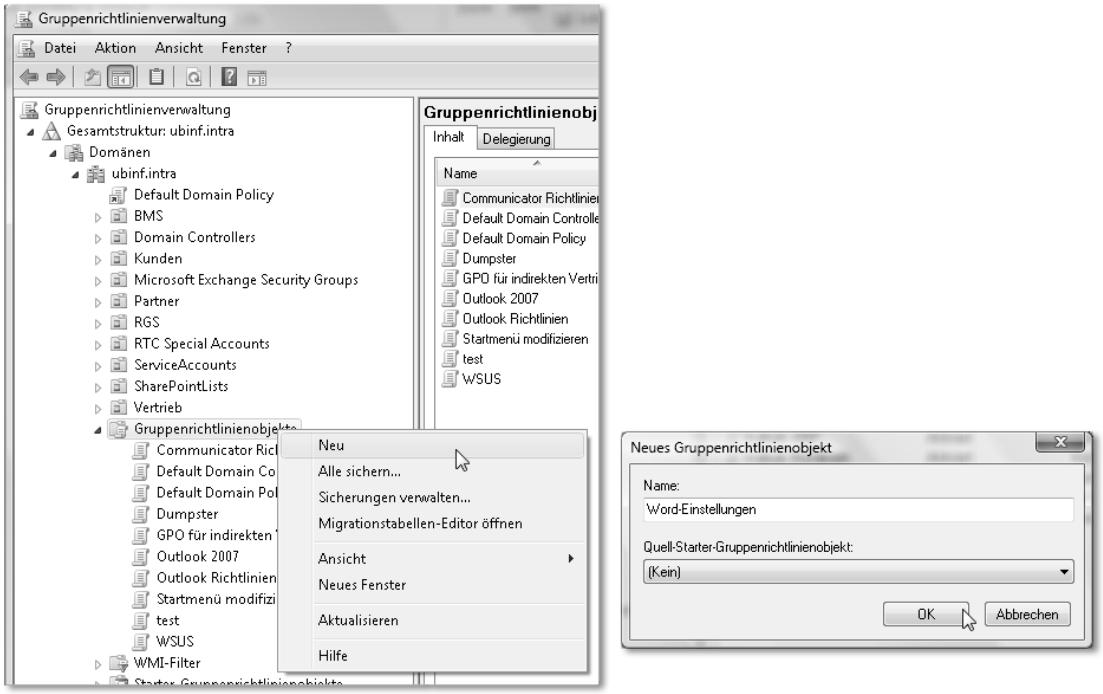


Abbildung 11.50 Erstellen eines neuen Gruppenrichtlinienobjekts

Das neu angelegte Gruppenrichtlinienobjekt ist bisher absolut wertlos. An diesem Zustand können Sie aber leicht etwas ändern, indem Sie Einstellungen darin vornehmen. Sie haben zwei Möglichkeiten, um das Gruppenrichtlinienobjekt zu bearbeiten:

- Sie können im Container GRUPPENRICHTLINIENOBJEKTE den Menüpunkt BEARBEITEN im Kontextmenü des jeweiligen Eintrags wählen (Abbildung 11.51).
- Wenn Sie eine Organisationseinheit ausgewählt haben und die Verknüpfungen zu den Gruppenrichtlinienobjekten vor sich sehen, führt der Menüpunkt BEARBEITEN der Verknüpfung ebenfalls zum Gruppenrichtlinienobjekt-Editor und somit zum Bearbeiten der Einstellungen.

Hinweis aus der Praxis

Sie können natürlich sämtliche Einstellungen in einem Gruppenrichtlinienobjekt vornehmen. Kein Problem, das funktioniert, es ist aber nicht sonderlich übersichtlich, und die Wiederverwendbarkeit des Gruppenrichtlinienobjekts ist gering. Ich empfehle meinen Kunden lieber mehrere Gruppenrichtlinien mit thematisch zusammenhängenden Einstellungen, also eine mit Desktop-Einstellungen, eine mit Word-Einstellungen etc. Auf diese Weise bleibt das einzelne Gruppenrichtlinienobjekt übersichtlich und kann mit verschiedenen Organisationseinheiten verknüpft werden – auch in verschiedenen Kombinationen: Beispielsweise kann das Word-Gruppenrichtlinienobjekt für eine bestimmte Organisationseinheit mit einem weniger restriktiven Desktop-Gruppenrichtlinienobjekt kombiniert werden.

Weiterhin ist es häufig ratsam, getrennte Gruppenrichtlinienobjekte für Computer- und Benutzereinstellungen anzulegen.

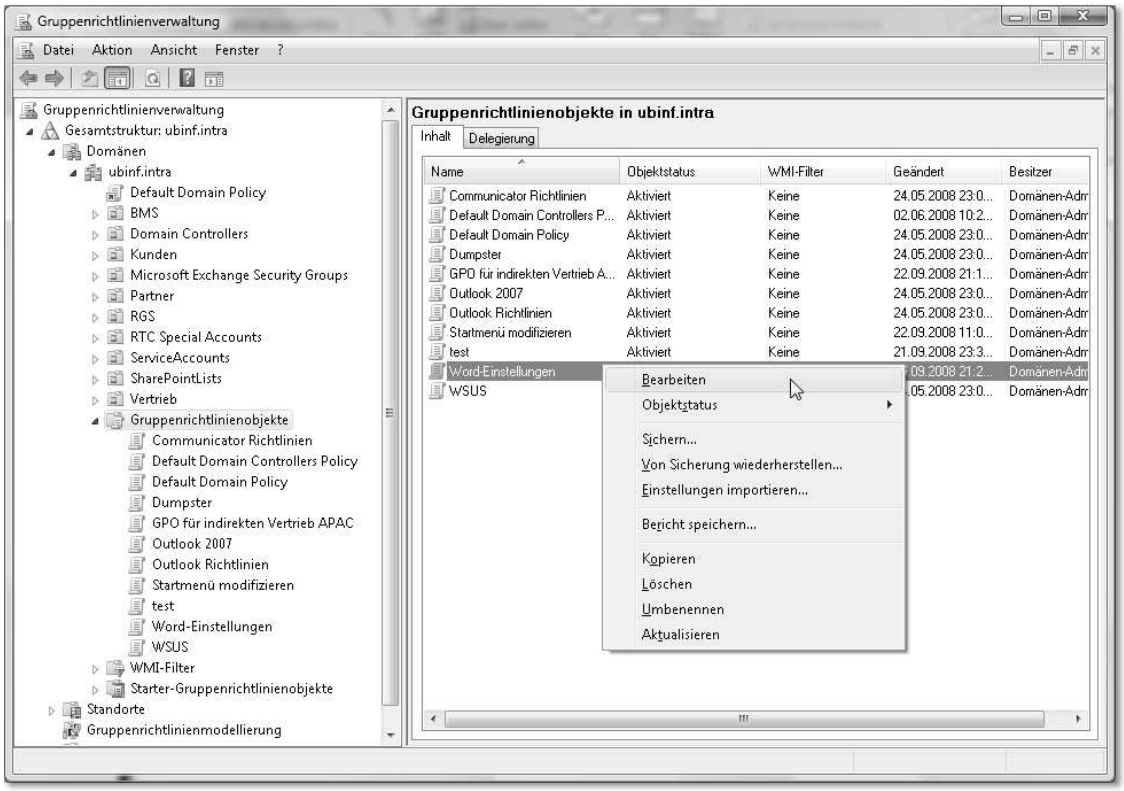


Abbildung 11.51 Die Bearbeitung des Gruppenrichtlinienobjekts wird im Kontextmenü aufgerufen.

Das eigentliche Bearbeiten des Gruppenrichtlinienobjekts erfolgt im Gruppenrichtlinienverwaltungs-Editor. Hier finden Sie die verschiedenen Einstellungen für Computer und Benutzer. Sie haben bereits standardmäßig die Auswahl aus Tausenden von Einstellungen, und durch administrative Vorlagen können Sie beliebige weitere hinzufügen – beispielsweise für das Office-Paket.

Das Bearbeiten von Einstellungen ist auf Abbildung 11.52 gezeigt – es dürfte selbsterklärend sein.

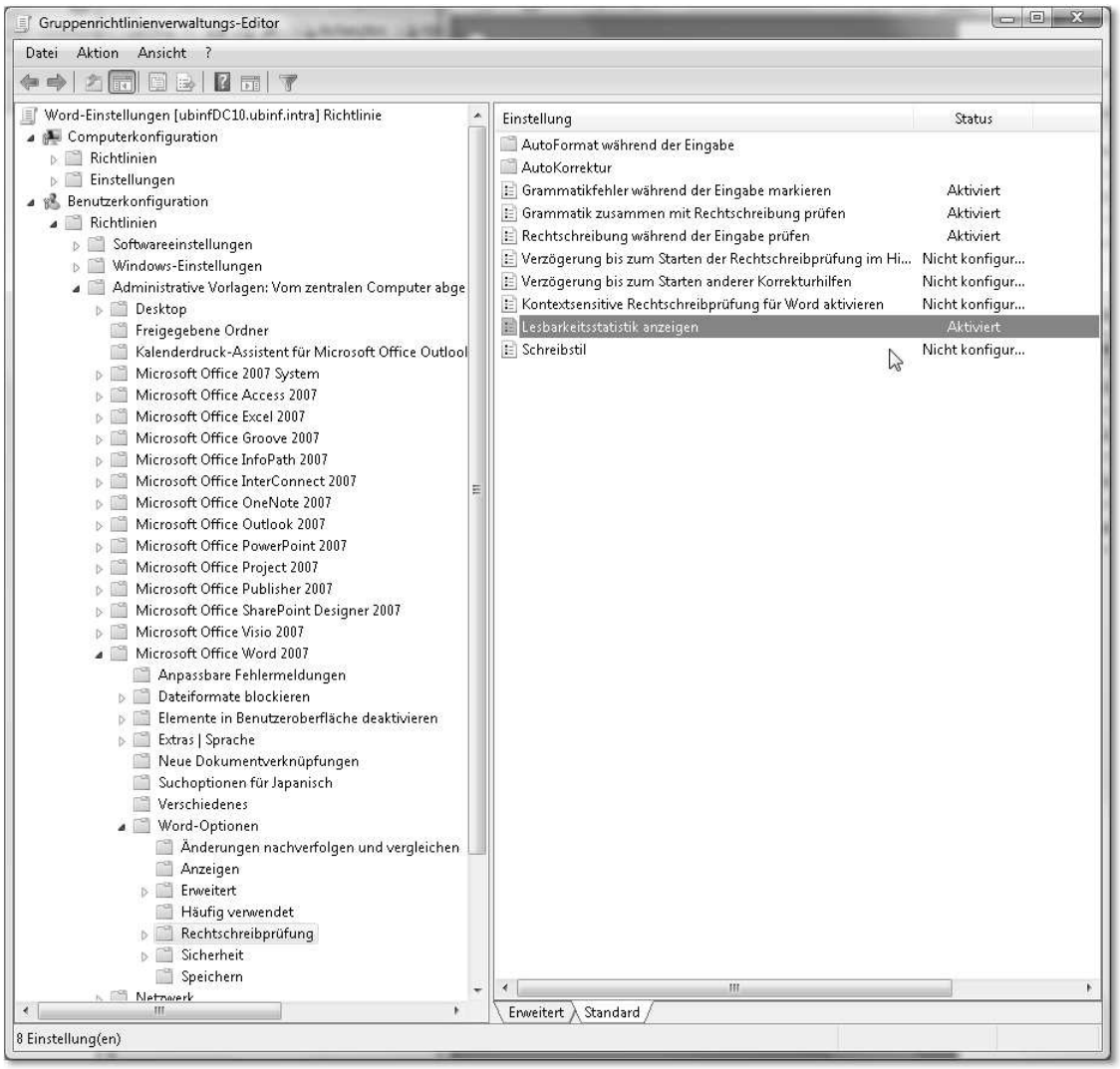


Abbildung 11.52 Die Konfiguration der Einstellungen im Gruppenrichtlinienverwaltungs-Editor

Wenn Sie den Gruppenrichtlinienobjekt-Editor wieder verlassen (ein explizites Speichern ist nicht notwendig), können Sie auf der Registerkarte EINSTELLUNGEN der Gruppenrichtlinienverwaltung die Zusammenfassung der konfigurierten Einstellungen einsehen (Abbildung 11.53).

Natürlich ist es auch interessant, wer ein Gruppenrichtlinienobjekt überhaupt konfigurieren kann – diese Einstellungen finden Sie auf der Registerkarte DELEGIERUNG, die auf Abbildung 11.54 zu sehen ist. Einträge hinzuzufügen ist kein Problem, es sei aber dringend darauf hingewiesen, dass Sie die Einträge SYSTEM und DOMÄNENCONTROLLER DER ORGANISATION keinesfalls entfernen dürfen.

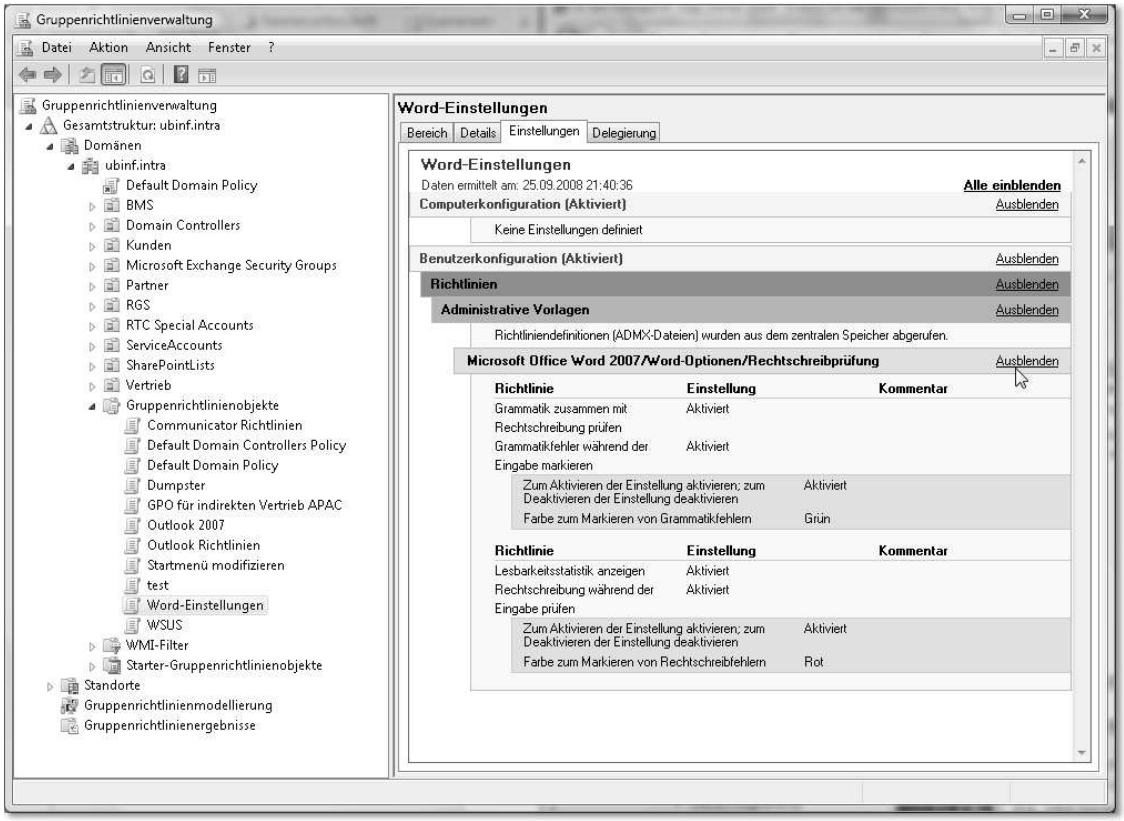


Abbildung 11.53 Eine Zusammenfassung der Einstellungen können Sie sich hier anzeigen lassen.

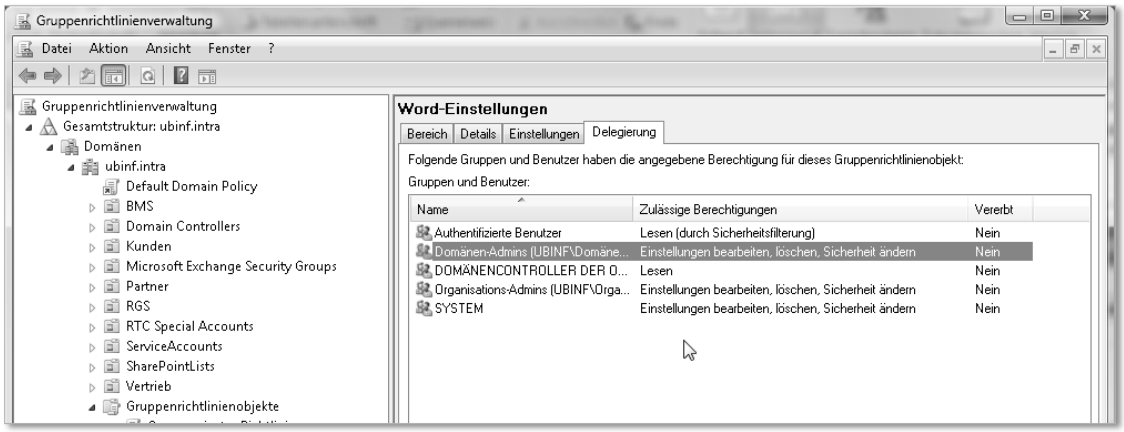


Abbildung 11.54 Auf der Karteikarte »Delegierung« wird festgelegt, welche Benutzer Berechtigungen haben.

11.11.2 Verknüpfungen hinzufügen und bearbeiten

Wenn das Gruppenrichtlinienobjekt erstellt ist und die Einstellungen konfiguriert sind, müssen Sie noch dafür sorgen, dass es auch tatsächlich angewendet wird. Dazu verknüpfen Sie es mit Organisationseinheiten, der Domäne und/oder mit Standorten. Um eine Organisationseinheit mit einem vorhandenen Gruppen-

richtlinienobjekt zu verknüpfen, wählen Sie im Kontextmenü der OU den Menüpunkt VORHANDENES GRUPPENRICHTLINIENOBJEKT VERKNÜPFEN (Abbildung 11.55).

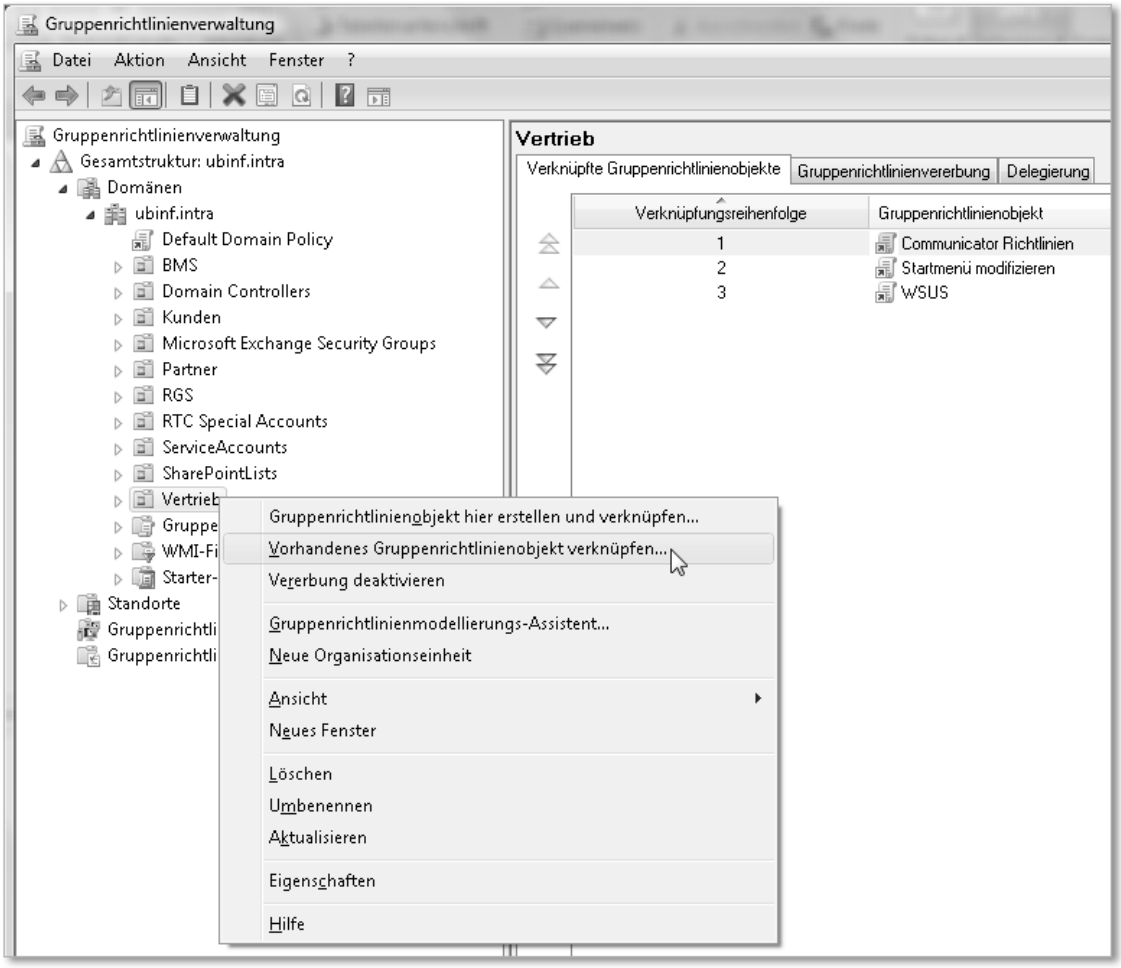


Abbildung 11.55 Im Kontextmenü der Organisationseinheit wird die Verknüpfung zu einem Gruppenrichtlinienobjekt erstellt.

Daraufhin erscheint eine Auflistung der vorhandenen Gruppenrichtlinienobjekte, und Sie können eines oder mehrere auswählen – und schon ist die Verknüpfung erstellt und aktiv (Abbildung 11.56).

Auf der Registerkarte VERKNÜPFTE GRUPPENRICHTLINIENOBJEKTE einer Organisationseinheit, Domäne oder eines Standorts sind alle Objekte aufgeführt, wobei die Reihenfolge entscheidend ist. Das Objekt mit der kleinsten Zahl wird zuletzt ausgeführt, hat also die höchste Priorität, falls unterschiedliche Werte für dieselbe Einstellung festgelegt worden sind – es sei denn, eine Verknüpfung wurde als ERZWUNGEN gekennzeichnet (Abbildung 11.57).

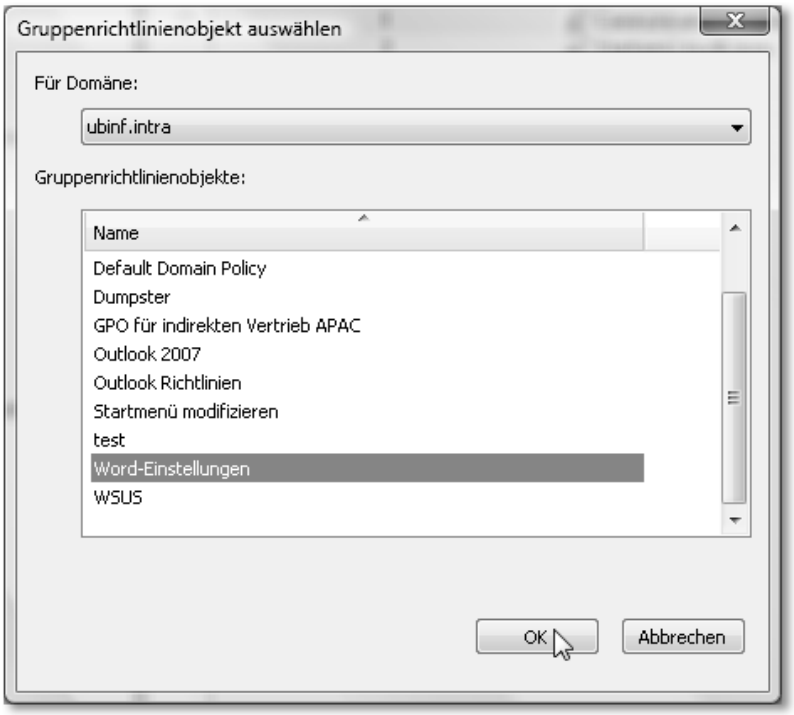


Abbildung 11.56 Auswahl des zu verknüpfenden Gruppenrichtlinienobjekts

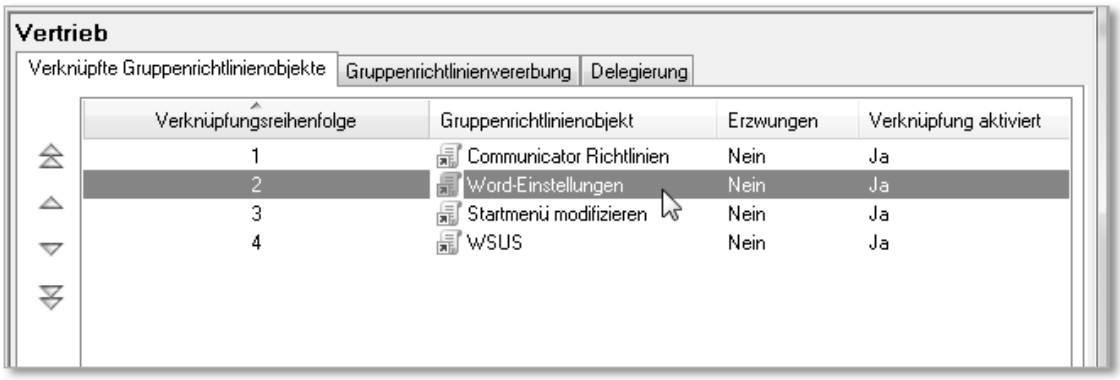


Abbildung 11.57 In der Liste der Verknüpfungen wird auch die Reihenfolge der Anwendung festgelegt.

Eine Verknüpfung verfügt über ein Kontextmenü, aus dem ich drei Menüpunkte speziell erwähnen möchte (Abbildung 11.58):

- BEARBEITEN öffnet das Gruppenrichtlinienobjekt zur Bearbeitung. Die Änderungen gelten dann für sämtliche Verknüpfungen, die auf das Gruppenrichtlinienobjekt verweisen.
- Wird eine Verknüpfung mit ERZWUNGEN markiert, bedeutet das, dass die von ihr vorgenommenen Einstellungen von später verarbeiteten Gruppenrichtlinienobjekten nicht überschrieben werden können. Dies wird weiter vorn im Abschnitt 11.4 erläutert.

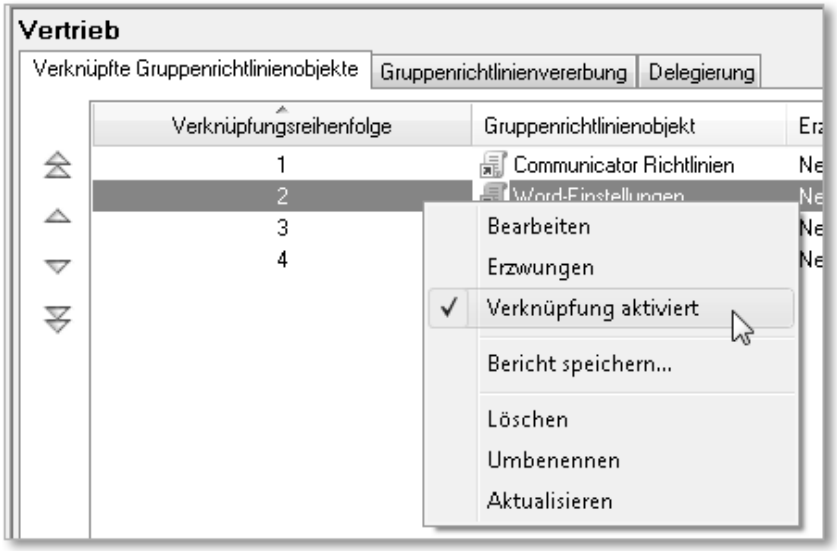


Abbildung 11.58 Im Kontextmenü der Verknüpfung kann diese unter anderem deaktiviert werden.

- Mit dem Menüpunkt VERKNÜPFUNG AKTIVIERT können Sie die Verarbeitung der Gruppenrichtlinie für die jeweilige OU, Domäne bzw. den jeweiligen Standort ein- und ausschalten.

11.11.3 Gruppenrichtlinienmodellierung

In komplexen Szenarien mit vielen Gruppenrichtlinien, die in einer umfangreichen OU-Struktur verarbeitet werden, kann die Übersicht leicht verloren gehen. Angenehmerweise bietet die Gruppenrichtlinienverwaltung Werkzeuge an, mit denen man recht bequem prüfen kann, welche Richtlinien zur Anwendung kommen – eines davon ist die *Gruppenrichtlinienmodellierung*.

Das grundsätzliche Konzept dahinter ist, dass mit einem Assistenten Szenarien erstellt werden, die bei Bedarf, also nach Änderungen, neu »errechnet« werden können. Der Ausgangspunkt ist also die Erstellung eines solchen Szenarios. Abbildung 11.59 zeigt, wie Sie damit beginnen.

Die erste Dialogseite ist auf Abbildung 11.60 gezeigt. Sie können hier bestimmen, ob die Simulation auf einem beliebigen DC ausgeführt werden soll oder ob Sie ein bestimmtes System festlegen möchten. Sofern Sie nicht von Replikationsproblemen (oder sehr langsamer Replikation) ausgehen, sollten Sie den DC ruhig automatisch ermitteln lassen, sonst wählen Sie eine Maschine aus der Auswahlliste aus.

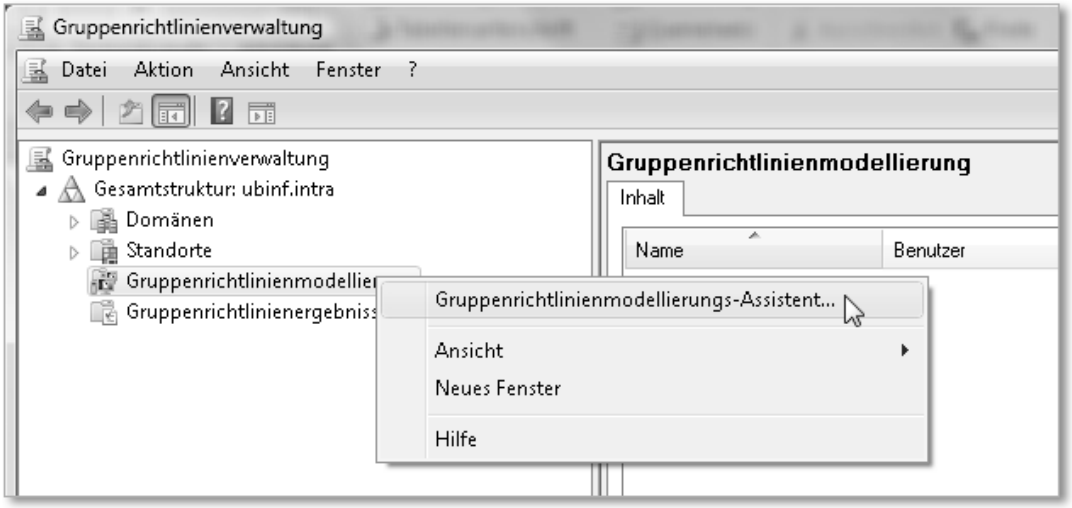


Abbildung 11.59 Aufruf des Gruppenrichtlinienmodellierungs-Assistenten

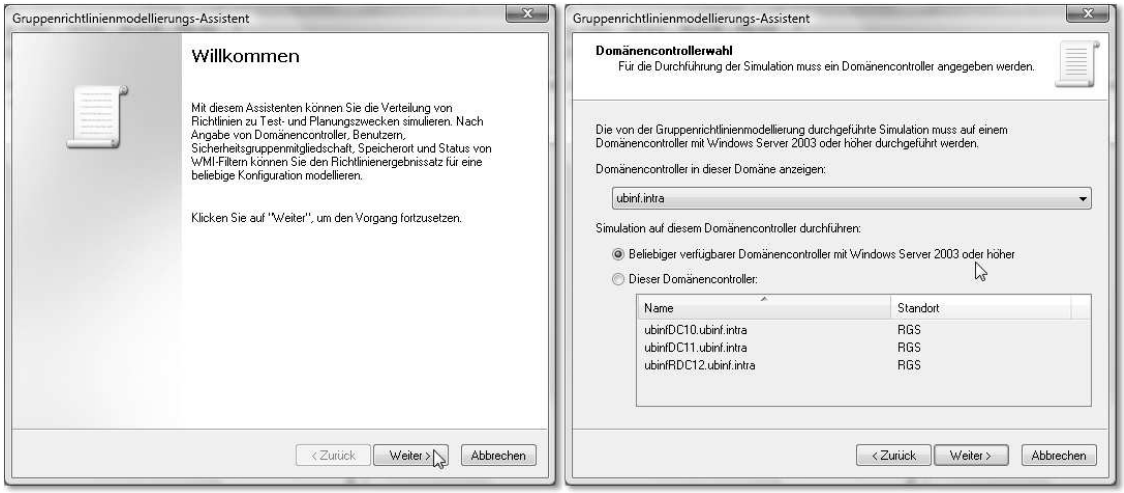


Abbildung 11.60 Der Gruppenrichtlinienmodellierungs-Assistent: Zunächst legen Sie fest, auf welchem Domänencontroller die Simulation durchgeführt werden soll.

Die nächste Dialogseite beschäftigt sich damit, Benutzerinformationen und Computerinformationen festzulegen (Abbildung 11.61, links). Sie können entweder einen bestimmten Benutzer/Container auswählen oder sich für Organisationseinheiten entscheiden.

Da auch an Standorten Richtlinien »kleben« können, wählen Sie auf der folgenden Dialogseite (Abbildung 11.61, rechts) einen Standort aus. Weiterhin können Sie eine Loopback-Verarbeitung (häufig in Terminal-Server-Umgebungen verwendet, siehe späterer Abschnitt und/oder eine langsame Verbindung konfigurieren.

Durchaus interessant bei der Gruppenrichtlinienmodellierung sind die WMI-Filter, die auch auf einer dedizierten Dialogseite ausgewählt werden können (Abbildung 11.62). Falls (noch) keine Filter vorhanden sind, brauchen Sie sich keine Ge-

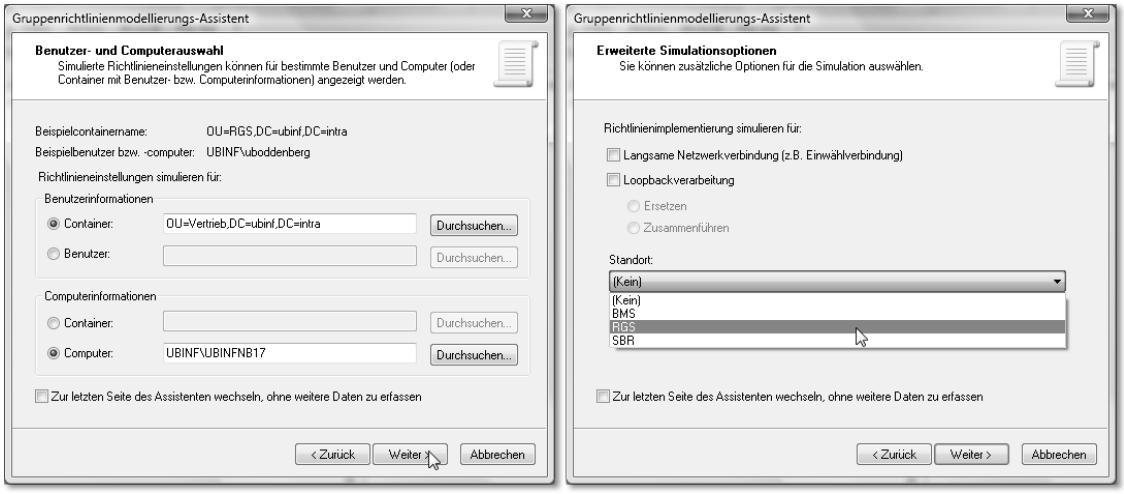


Abbildung 11.61 Im Assistenten wählen Sie den Benutzer, den Computer und den Standort aus.

danken zu machen, es klappt trotzdem. Überhaupt verfügen alle Dialogseiten des Assistenten mit Ausnahme der ersten über die Option Zur letzten Seite des Assistenten wechseln, ohne.... Es ist also keinesfalls erforderlich, dass Sie jede einzelne der Dialogseiten (und das sind einige!) durcharbeiten.

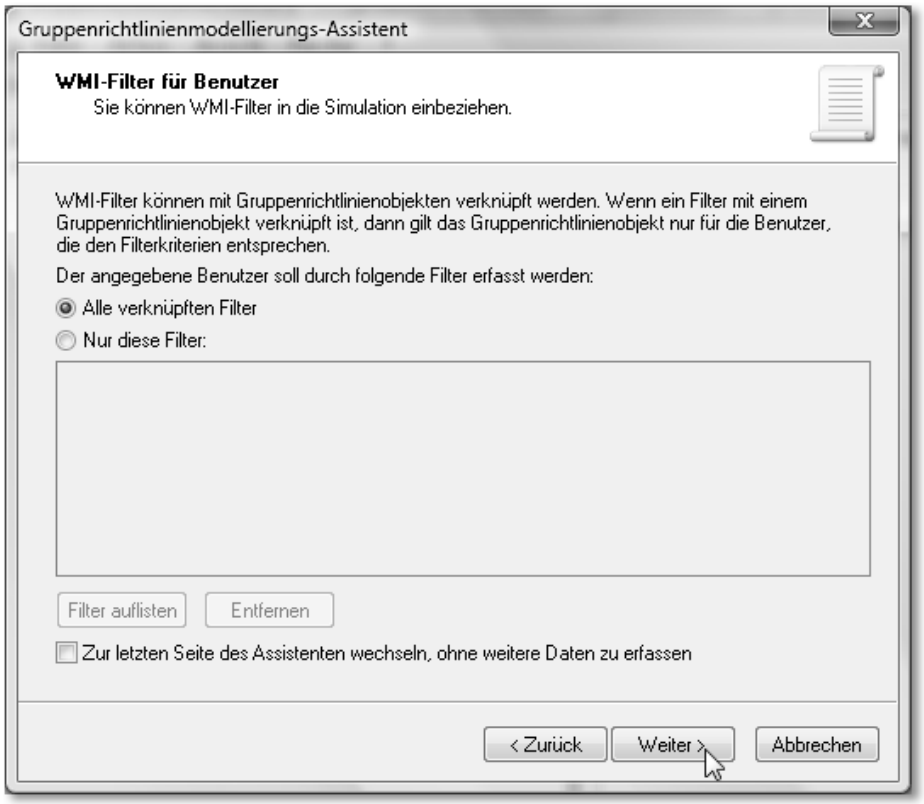


Abbildung 11.62 Die auszuführenden WMI-Filter können festgelegt werden.

Ein Ergebnis der Gruppenrichtlinienmodellierung ist auf der Registerkarte ZUSAMMENFASSUNG zu sehen (Abbildung 11.63).

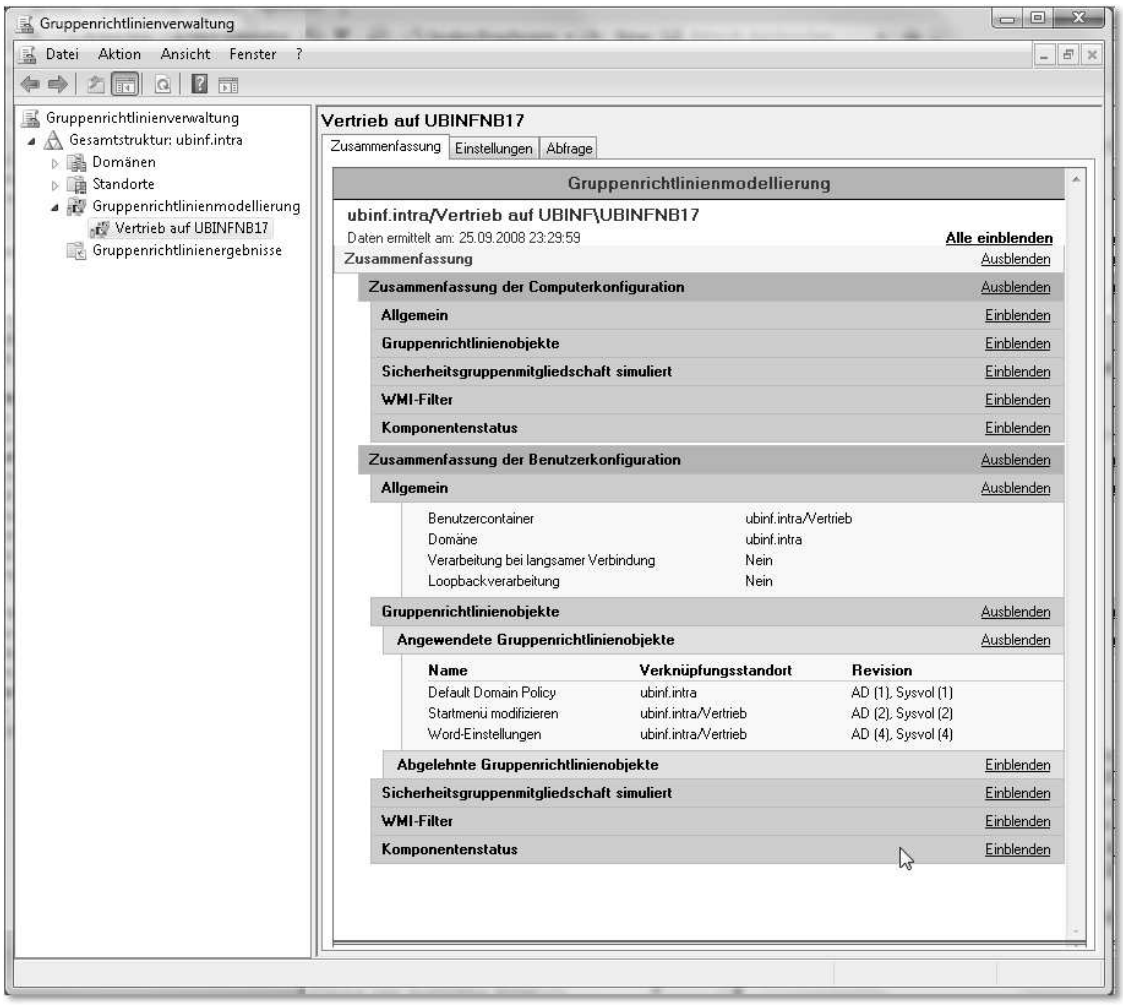


Abbildung 11.63 Ergebnis der Gruppenrichtlinienmodellierung

Unter anderem sehen Sie hier, welche Gruppenrichtlinienobjekte für die Computer- und die Benutzerkonfiguration herangezogen worden sind. Falls Sie die konkret angewendeten Einstellungen sehen möchten, wechseln Sie auf die Registerkarte EINSTELLUNGEN (Abbildung 11.64).

Das mit dem Assistenten erstellte Gruppenrichtlinienmodellierungs-Objekt enthält sozusagen eine Momentaufnahme, zeigt also das Verarbeitungsergebnis zum Zeitpunkt seines Erzeugens. Im Kontextmenü findet sich der Menüpunkt ABFRAGE ERNEUT AUSFÜHREN, womit die Ergebnisse dem aktuellen Zustand angepasst werden (Abbildung 11.65).

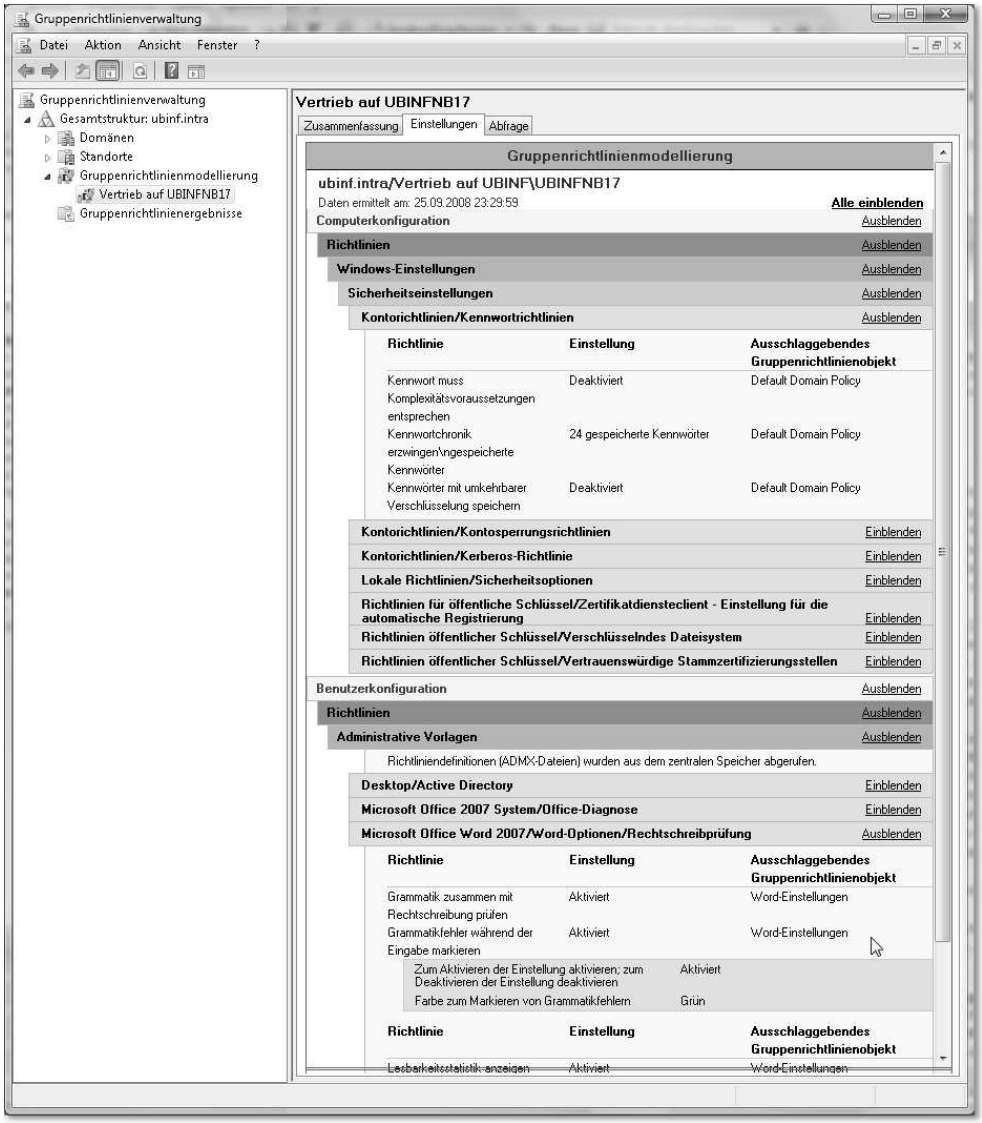


Abbildung 11.64 Die angewendeten Einstellungen können im Detail betrachtet werden.

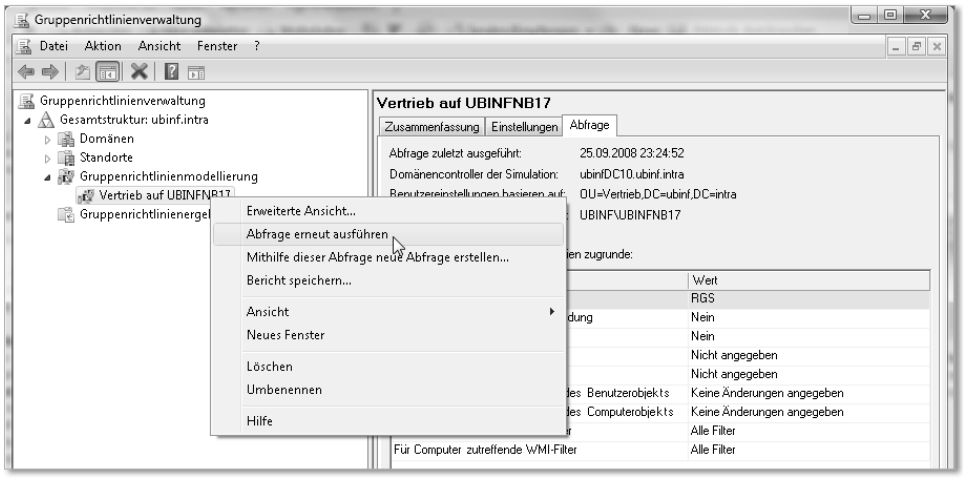


Abbildung 11.65 Sie können die Abfrage bei Bedarf erneut ausführen.

Sie können also verschiedene Objekte anlegen, mit denen Sie regelmäßig die Ergebnisse der Gruppenrichtlinienverarbeitung überprüfen können.

11.11.4 Gruppenrichtlinienergebnisse

Ähnlich, aber »etwas anders« als die Gruppenrichtlinienmodellierung verhält sich die Funktion *Gruppenrichtlinienergebnisse*. Auch können mit einem Assistenten (der Aufruf erfolgt, wie auf Abbildung 11.66 gezeigt) beliebig viele unterschiedliche Einträge erzeugt werden.

Die Computer- und Benutzerauswahl beschränkt sich allerdings auf einen bestimmten Computer und einen konkreten Benutzer. Abbildung 11.67 zeigt die beiden relevanten Screenshots aus dem Gruppenrichtlinienergebnis-Assistenten.

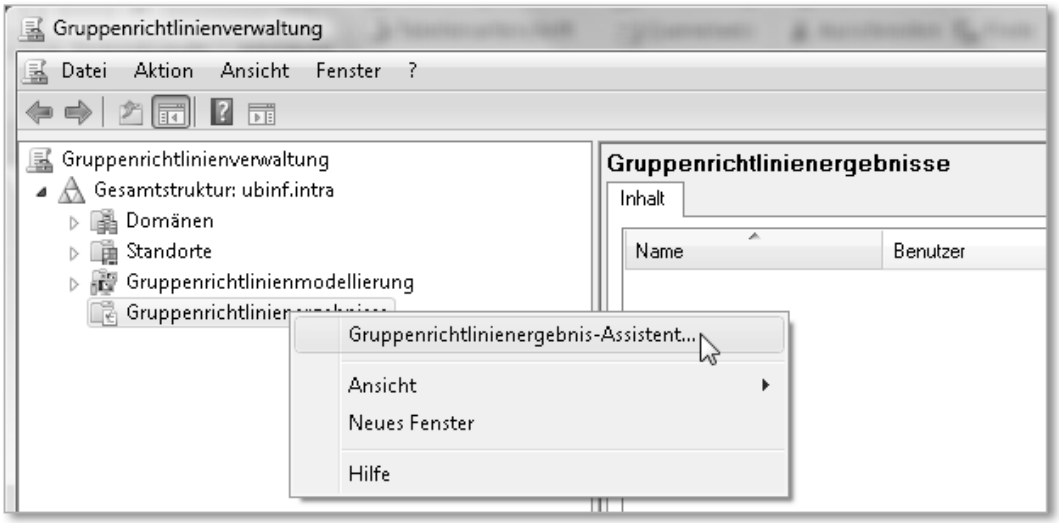


Abbildung 11.66 Hier wird der Gruppenrichtlinienergebnis-Assistent gestartet.

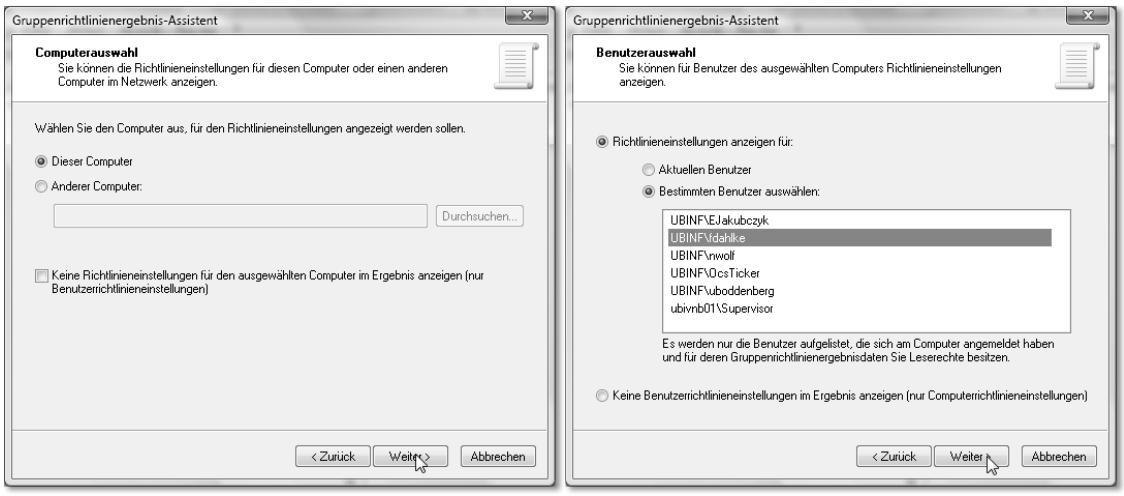


Abbildung 11.67 Computer und Benutzer für die Simulation können angezeigt werden.

Die Ergebnisse sehen Sie auf zwei Abbildungen:

- Abbildung 11.68 zeigt unter anderem die angewendeten und abgelehnten Gruppenrichtlinienobjekte – übrigens in der Reihenfolge der Verarbeitung.
- Abbildung 11.69 zeigt die konkreten Einstellungen, die aus der Verarbeitung der Gruppenrichtlinien resultieren.

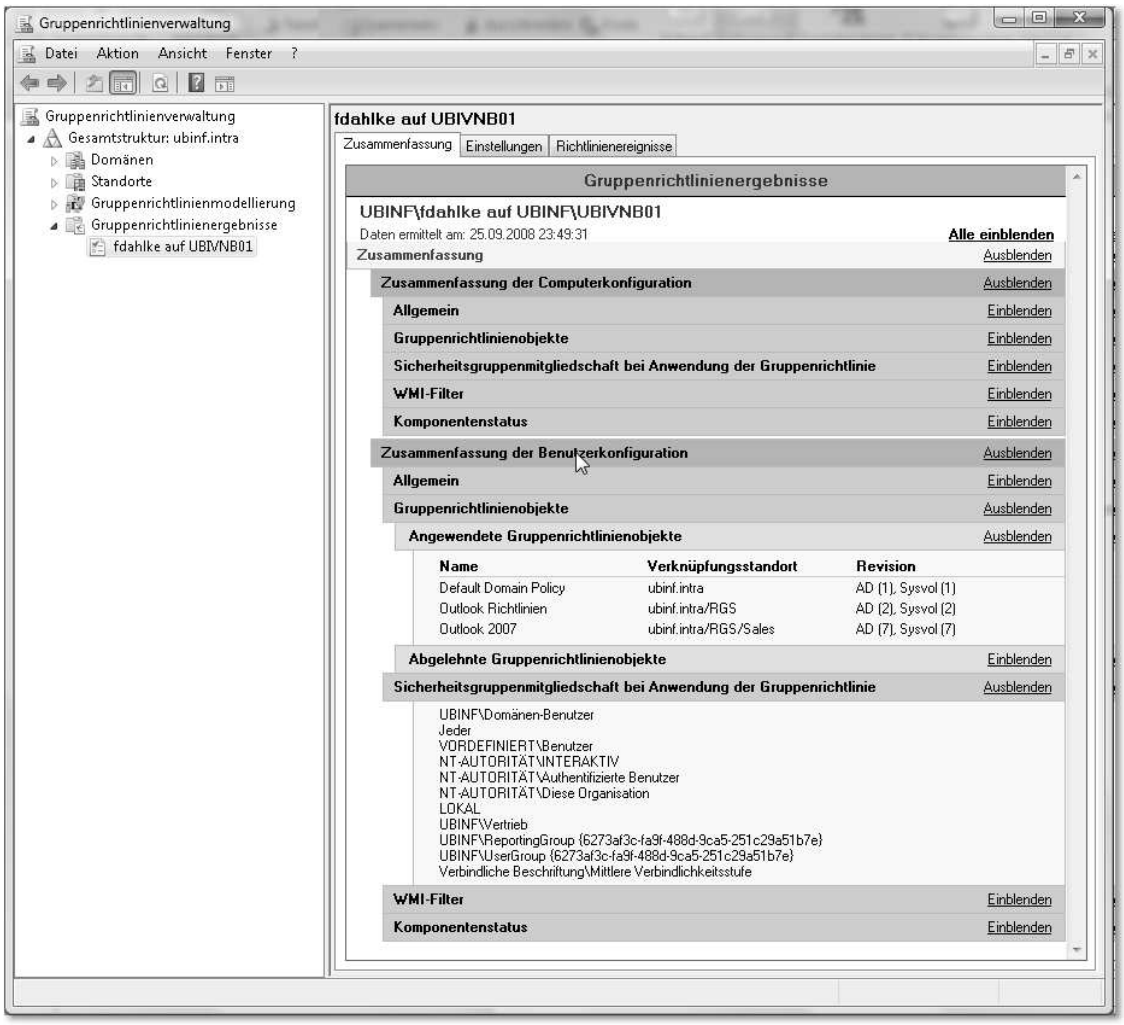


Abbildung 11.68 Dieser Dialog zeigt unter anderem die angewendeten Gruppenrichtlinienobjekte.

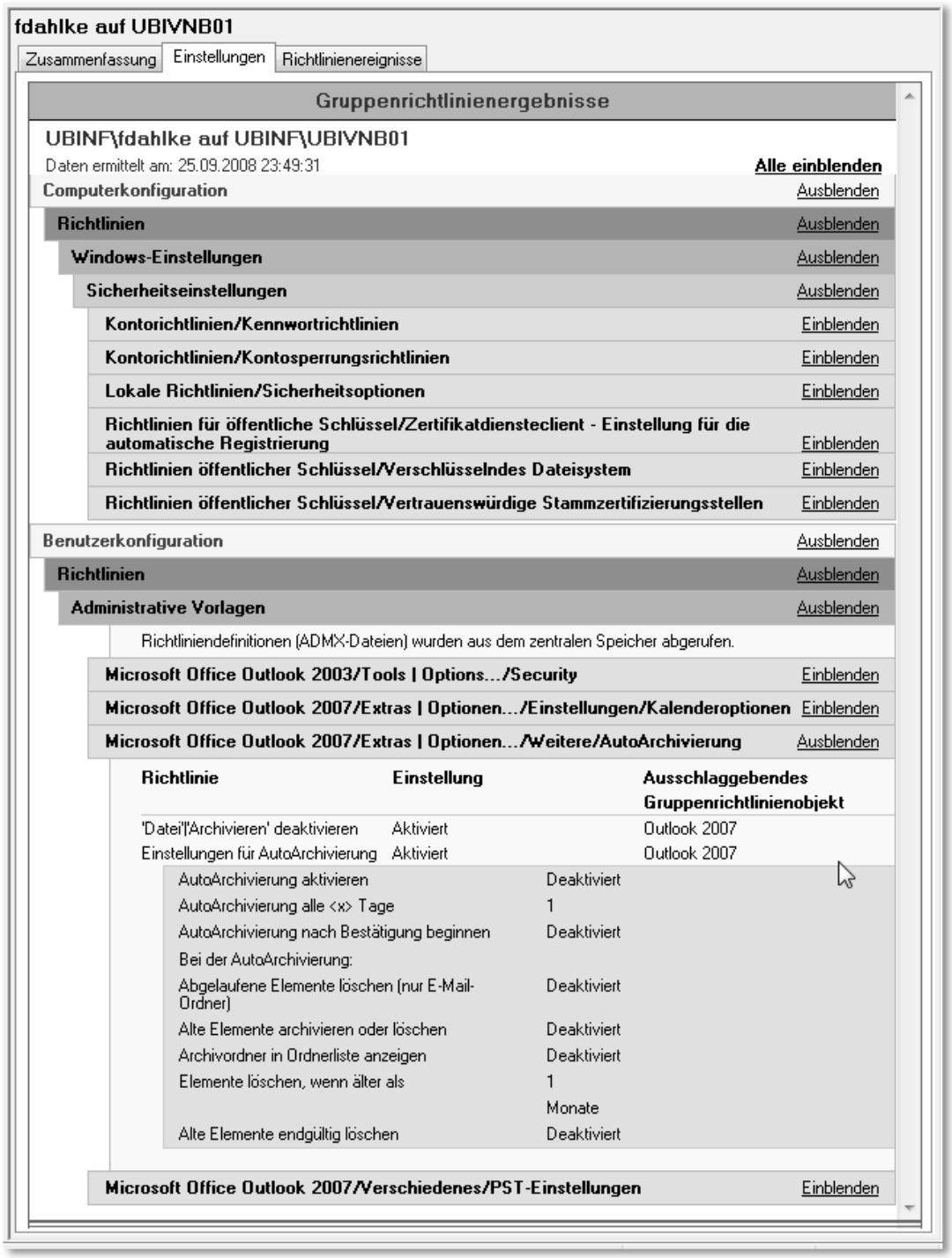


Abbildung 11.69 Auch die einzelnen Einstellungen werden gezeigt.

11.12 WMI-Filter

Ich habe weiter vorn erwähnt, dass man die Abarbeitung von Gruppenrichtlinien durch Berechtigungen steuern kann, habe aber darauf hingewiesen, dass das nur im Ausnahmefall geschehen sollte – es wird einfach zu unübersichtlich.

Eine sehr interessante andere Möglichkeit, um festzulegen, ob eine Gruppenrichtlinie tatsächlich angewendet werden soll, ist die Steuerung mittels WMI-Filtern. WMI steht für *Windows Management Instrumentation*, einen Ansatz, über den unter anderem auf Konfigurationsinformationen eines Computers zugegriffen werden kann. Mit WMI-Filtern lässt sich beispielsweise steuern, dass ein Gruppenrichtlinienobjekt nur auf Computern mit einem »Genuine Intel«-Prozessor ausgeführt werden soll.

WMI-Filter werden unterhalb der Domäne im Container WMI-Filter gespeichert. Das Anlegen eines neuen Filters geschieht wie erwartet im Kontextmenü (Abbildung 11.70).

Beim WMI-Filter gibt es prinzipiell nur wenig einzustellen: NAME und BESCHREIBUNG und die ABFRAGEN. Wie Sie auf Abbildung 11.71 sehen, verwendet die Abfragesprache eine SQL-ähnliche Syntax. Es handelt sich um die *WMI Query Language* (WQL).

Ich möchte an dieser Stelle nicht im Detail auf die WQL eingehen, da ich Ihnen ein wenig weiter hinten ein kleines Werkzeug vorstelle, mit dem Sie recht einfach Abfragen erzeugen können. Interessierten sei aber die Dokumentation in der MSDN empfohlen. Die entsprechende URL lautet *http://msdn.microsoft.com/en-us/library/aa394552.aspx.*

Abbildung 11.70 WMI-Filter werden in diesem Container gespeichert. Im Kontextmenü wird das Neu-Erstellen aufgerufen.

Wenn Sie in der Baumdarstellung der Gruppenrichtlinienverwaltung ein Gruppenrichtlinienobjekt auswählen, wird die Registerkarte BEREICH angezeigt werden. Im unteren Abschnitt können Sie einen WMI-Filter auswählen, der mit diesem Gruppenrichtlinienobjekt verknüpft werden soll (Abbildung 11.72). Ein WMI-Filter kann übrigens mit mehreren Gruppenrichtlinienobjekten verknüpft werden.

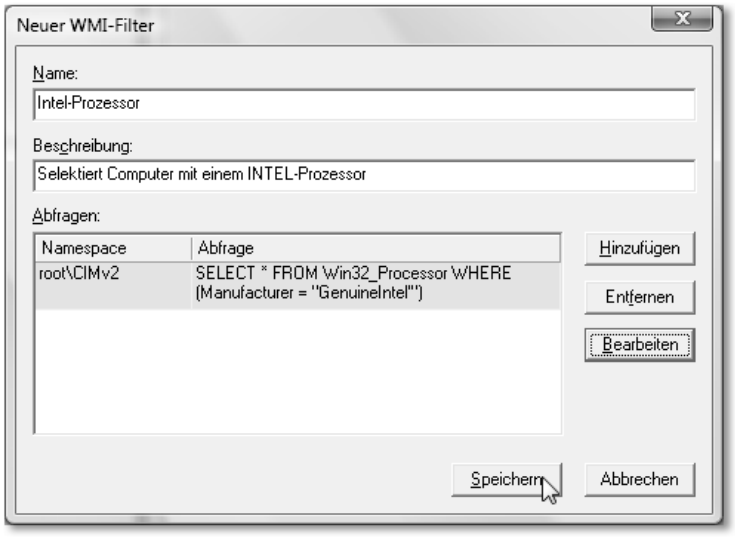


Abbildung 11.71 Ein WMI-Filter basiert primär auf einer Abfrage.

Wenn Sie die WMI-Filterung für ein Gruppenrichtlinienobjekt festgelegt haben, können Sie die Gruppenrichtlinienmodellierung starten und die Ergebnisse für eine OU (oder Domäne oder Standort) ermitteln, mit der dieses Gruppenrichtlinienobjekt verknüpft ist. Sie werden sehen, dass das Ergebnis des WMI-Filters berücksichtigt wird (Abbildung 11.73).

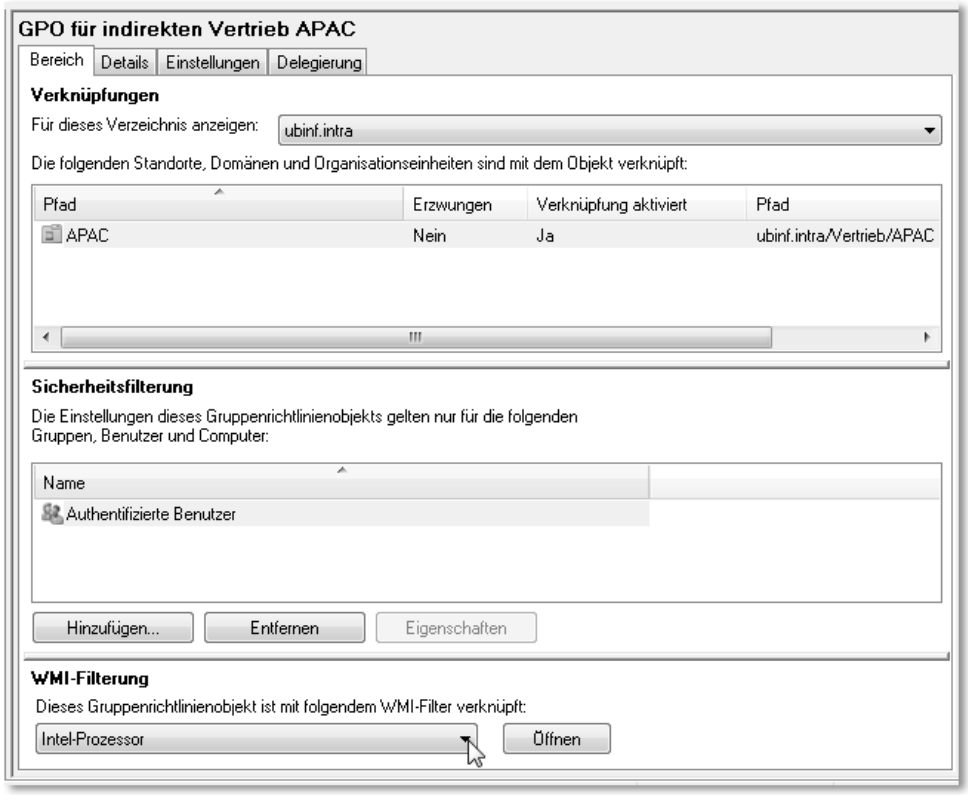


Abbildung 11.72 Im unteren Abschnitt des Dialogs weisen Sie den Filter einem Gruppenrichtlinienobjekt zu.

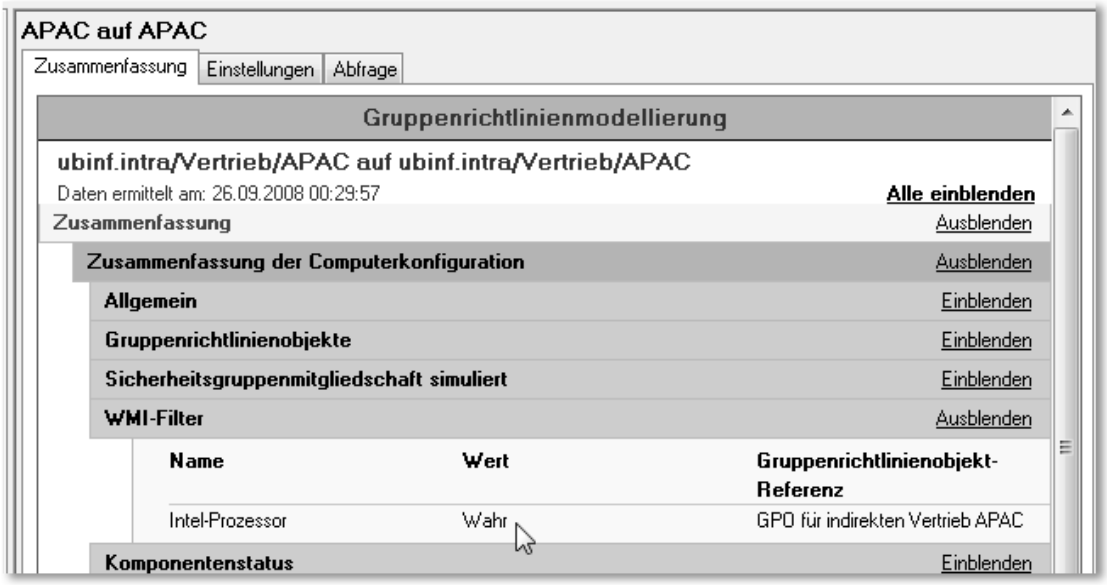


Abbildung 11.73 Der Ergebnis des WMI-Filters wird bei der Gruppenrichtlinienmodellierung berücksichtigt.

Ab Windows XP

Zu beachten ist, dass WMI-Filter nur auf Clients ab Windows XP ausgeführt werden können. Bei Windows 2000 stand diese Funktion noch nicht zur Verfügung – aber dies ist ja ohnehin ein Windows 7-Buch.

Obwohl das Werkzeug zur Gruppenrichtlinienverwaltung dem Administrator das Leben schon ziemlich weitgehend vereinfacht, lässt es Sie beim Erzeugen von WMI-Filtern allein. Es gibt nun zwei Möglichkeiten: Entweder Sie wühlen sich durch die Dokumentation und können nach einiger Zeit auch komplexe WMI-Abfragen formulieren – oder Sie lassen sich von einem kleinen Werkzeug helfen.

Ich verwende den *WMI Code Creator*, der unter diesem Suchbegriff im Microsoft Download Center erhältlich ist. Dieses Werkzeug zielt zwar darauf, komplette Codefragmente zu erzeugen und nicht nur eine »simple« Abfrage, letztgenannte fällt dabei aber natürlich auch ab.

Auf Abbildung 11.74 sehen Sie den WMI Code Creator in Aktion. Die Vorgehensweise dürfte weitgehend selbsterklärend sein. Auch wenn Sie noch nie eine Zeile C#-Code programmiert haben, finden Sie im Fenster GENERATED CODE ganz problemlos die eigentliche Abfrage. Durch einen Klick auf die Schaltfläche EXECUTE CODE wird die Abfrage (genauer gesagt: der erzeugte Code nebst Abfrage) ausgeführt und das Ergebnis in einem Textfenster angezeigt (Abbildung 11.75).

Die mit dem WMI Code Creator erzeugte Abfrage tragen Sie im WMI-Filter ein – und schon sind Sie fertig.

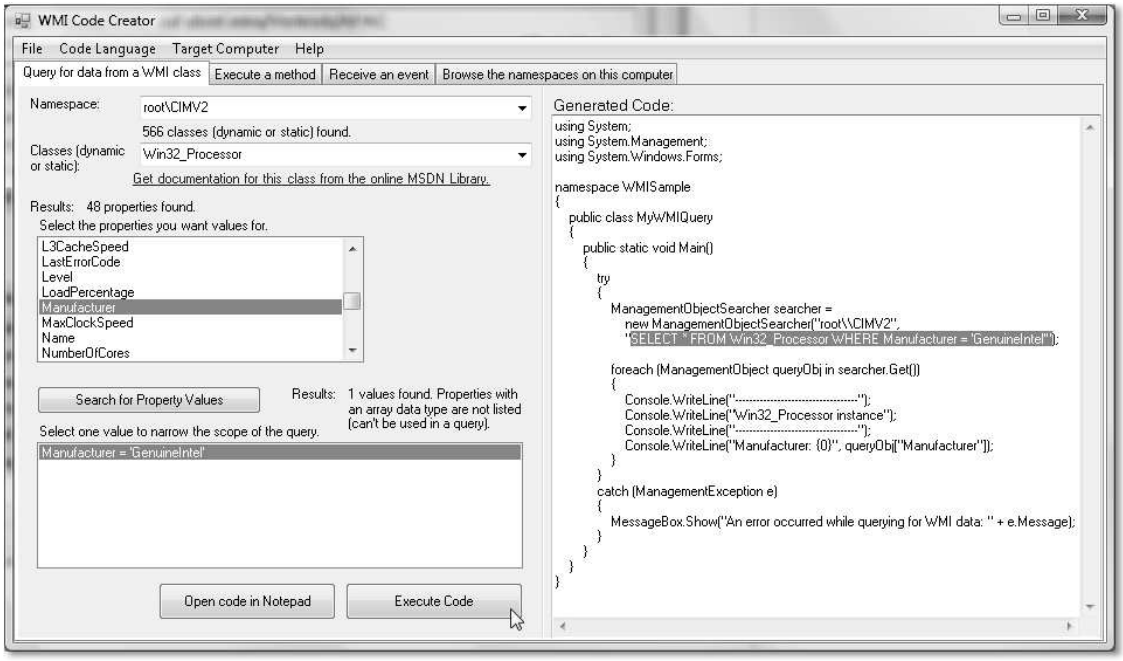


Abbildung 11.74 Abfragen können Sie bequem mit dem WMI Code Creator erstellen.

Abbildung 11.75 Die Schaltfläche »Execute Code« im WMI Code Creator führt zu diesem Ergebnis.

11.13 Softwareverteilung mit Gruppenrichtlinien

Mithilfe der Gruppenrichtlinien ist eine »begrenzte Softwareverteilung« möglich. Ich nenne sie deshalb »begrenzt«, weil die Möglichkeiten im Vergleich zu »großen« Lösungen, wie beispielsweise dem *System Center Configuration Manager 2007* (vormals *SMS*) eher bescheiden sind. Ich kenne aber etliche größere mittelständische Unternehmen, die ausschließlich auf Softwareverteilung per Gruppenrichtlinie setzen und damit durchaus erfolgreich sind. Eine wesentliche Einschränkung ist, dass »nur« MSI-Pakete verteilt werden können. In anderen Formaten vorliegende Software muss umgepackt werden.

Wie Sie wissen, gibt es in den Gruppenrichtlinien Einstellungen für Computer und solche für Benutzer. Ebendies gilt auch für die Softwareinstallation. Sie können also sowohl an Computer als auch an Benutzer verteilen. Klassischerweise ist die Denkweise zwar eher, dass man ein Stück Software an die Computer PC1998, PC8837 und PC0007 verteilt, die Verteilung an Benutzer hat aber durchaus auch Charme: Wenn die Vertriebsmitarbeiter beispielsweise *Microsoft Dynamics CRM* benötigen, verknüpft man die Vertriebs-OU mit der entsprechenden Gruppenrichtlinie. Dann wird auf einem Computer, auf dem ein Vertriebsmitarbeiter sich anmeldet, dieses Paket automatisch installiert. Ein unerwünschter Nebeneffekt könnte allerdings ein Lizenzproblem sein: Wenn Ihre Anwender fröhlich durchs Unternehmen wandern und sich hier und da anmelden, wird ständig das Softwarepaket installiert – und plötzlich haben Sie statt der lizenzierten 40 Installationen plötzlich 140.

Um eine gruppenrichtlinienbasierte Softwareverteilung durchzuführen, benötigen Sie zunächst ein Gruppenrichtlinienobjekt, in dem der Installationsvorgang definiert ist. Hierzu navigieren Sie zum Knoten Richtlinien • Softwareeinstellungen • Softwareinstallation und wählen in dessen Kontextmenü den Menüpunkt Neu • Paket. Abbildung 11.76 zeigt diesen Schritt für die Computerkonfiguration. In der Benutzerkonfiguration sieht es aber identisch aus.

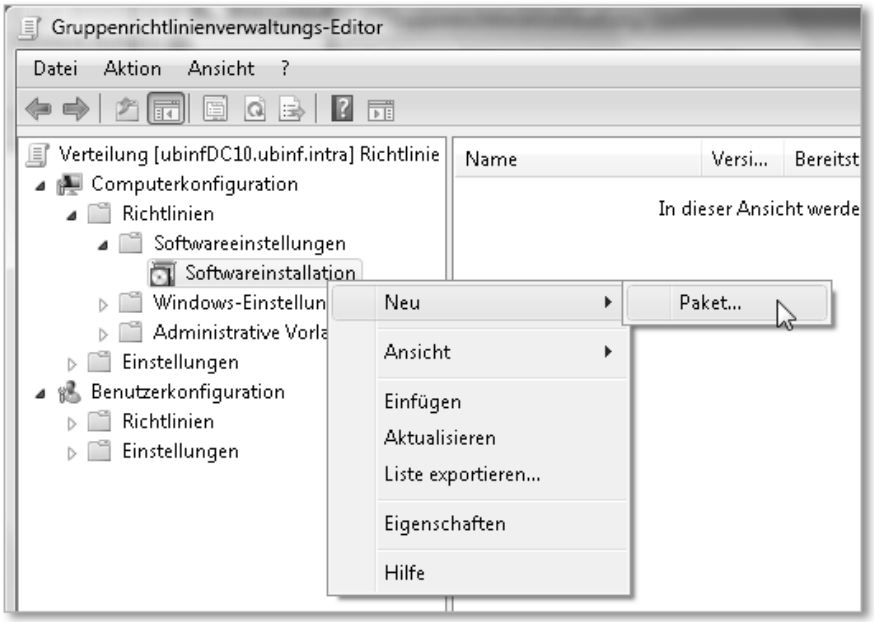


Abbildung 11.76 Die Softwareinstallation kann für Computer oder Benutzer konfiguriert werden.

Zunächst wird sich ein Dialog öffnen, in dem Sie das zu verteilende MSI-Paket auswählen können. Achten Sie darauf, dass es auf einer Dateifreigabe liegt und dass der Freigabepfad ausgewählt ist. Im Klartext: An *d:\fileshares\softdist* kom-

men die Computer im Netzwerk nicht heran, sondern nur an die entsprechende Freigabe *\\ubinfFile1\softdistshare*.

Als Nächstes müssen Sie die Bereitstellungsmethode auswählen. Dabei stehen zwei Optionen zur Auswahl (Abbildung 11.77):

- Veröffentlicht: Diese Option steht nur bei der Softwareinstallation in einer Benutzer-Gruppenrichtlinie zur Verfügung. Auf der Abbildung wird eine Computerrichtlinie erstellt, folglich ist sie dort ausgegraut.

  Diese Bereitstellungsmethode bewirkt, dass die Software unter Systemsteuerung • Programme (Windows 7/Vista) und Funktionen bzw. Systemsteuerung • Software (XP) angelegt und vom Benutzer installiert werden kann. Eine automatische Installation erfolgt also nicht.
- Bei der Methode Zugewiesen wird die Software direkt installiert, also ohne Zutun des Benutzers.

Abbildung 11.77 Auswahl der Bereitstellungsmethode (Die Option »Veröffentlicht« steht nur für eine Benutzerrichtlinie zur Verfügung.)

Wenn Sie die dritte Option, nämlich Erweitert, wählen, gelangen Sie zum Eigenschaften-Dialog der Einstellung. Letztendlich wählen Sie dort auch zwischen Veröffentlicht und Zugewiesen aus, haben aber direkt zusätzliche Konfigurationsmöglichkeiten (Abbildung 11.78).

Softwareverteilung

Wenn Sie eine Softwareverteilung über Gruppenrichtlinien durchführen, werden Sie sehr dankbar für die WMI-Filter sein. Mit diesen haben Sie die Möglichkeit, die Installation etwas feiner zu steuern. So können Sie beispielsweise verhindern, dass Software auf PCs mit weniger als 512 MB RAM installiert wird, oder dafür sorgen, dass die Installation nur durchgeführt wird, wenn auf dem C-Laufwerk mindestens 2 GB freier Speicherplatz vorhanden ist.

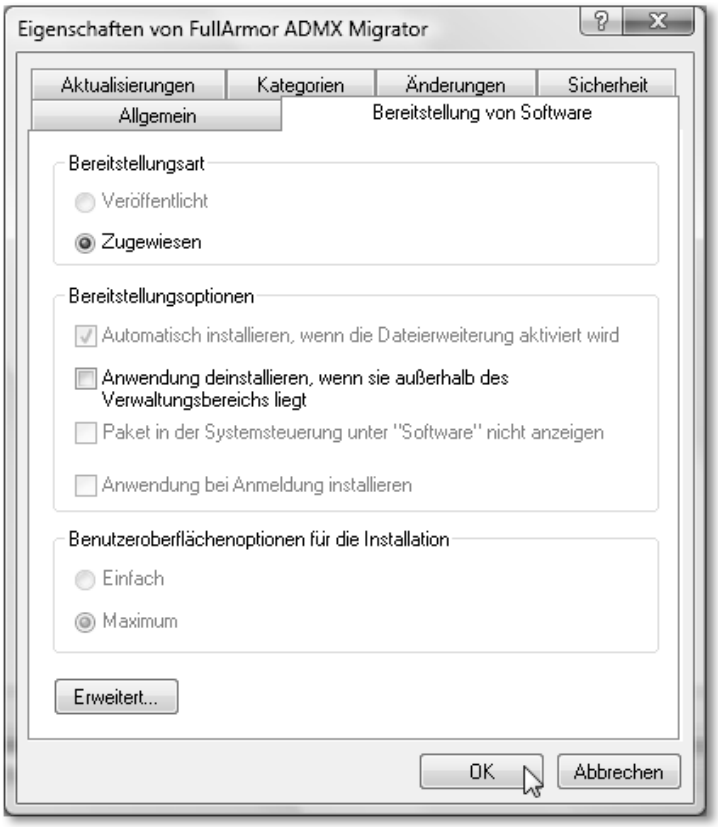


Abbildung 11.78 Der »Eigenschaften«-Dialog der Softwareinstallations-Einstellung

11.14 Loopback-Verarbeitung

Die Loopback-Verarbeitung ist beim Einsatz lokaler Clients vergleichsweise wenig relevant und wird hier eher der Vollständigkeit halber genannt. Im Terminalserver-Umfeld hingegen ist der Loopback-Verarbeitungsmodus ein sehr wichtiger Aspekt. Die Idee dahinter ist die folgende:

- Wenn sich ein Benutzer anmeldet, werden die Richtlinien angewendet, die in der OU gelten, in der das Benutzerobjekt angelegt ist. Dazu zählen auch die Vererbungen.
- Beim Loopback-Verarbeitungsmodus verhält sich das System so, als befände sich das Benutzerobjekt in der OU, in der das Computerobjekt (d. h. der Terminalserver) angelegt ist. Es werden also die in den dort gültigen Gruppenrichtlinien vorhandenen Benutzerrichtlinien angewendet.

Kurz gesagt ermöglicht es der Loopback-Verarbeitungsmodus, dass auf Terminalservern für dieselben Benutzerobjekte andere Gruppenrichtlinien zum Einsatz kommen, als wenn sich diese Benutzer auf einem Desktop-PC anmelden. In Umgebungen, in denen die Benutzer sowohl lokal installierte als auch über Terminal-

dienste bereitgestellte Anwendungen verwenden, kann dies außerordentlich praktisch sein.

Der Loopback-Verarbeitungsmodus wird mittels einer Gruppenrichtlinie für die entsprechenden Terminalserver aktiviert. Es macht vor diesem Hintergrund also Sinn, die Terminalserver in einer separaten OU anzusiedeln und eine entsprechende Gruppenrichtlinie zu erstellen (Abbildung 11.79).

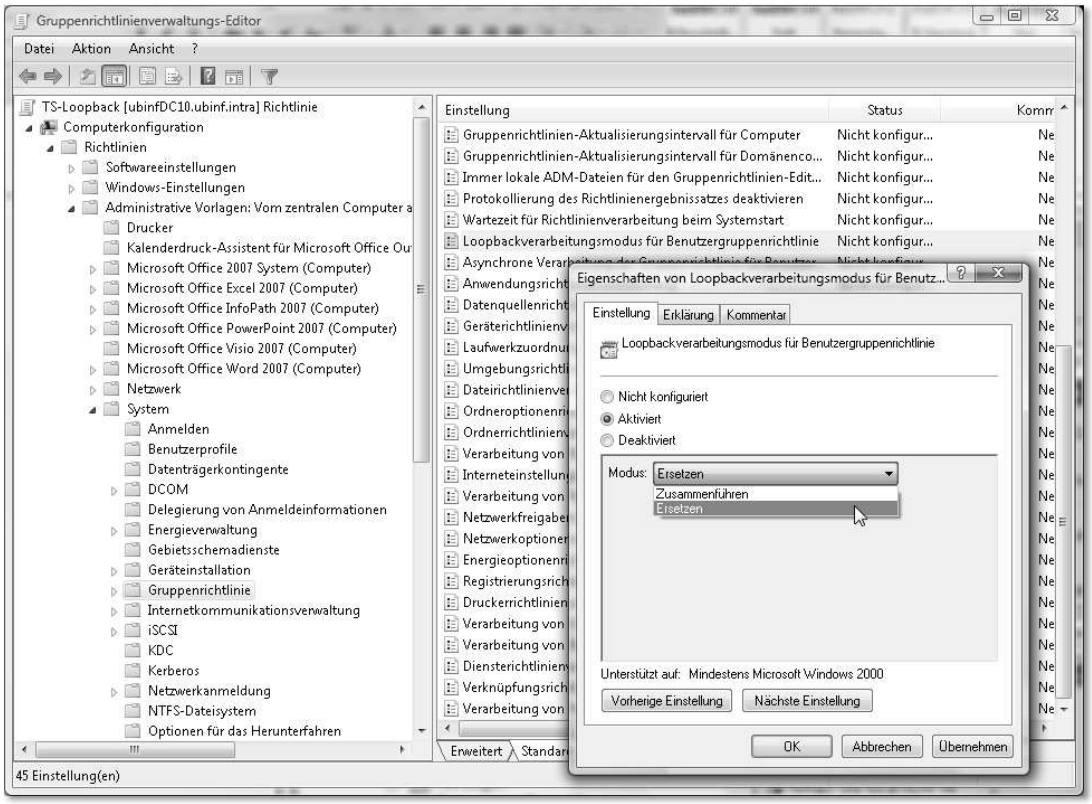


Abbildung 11.79 Der Loopbackverarbeitungsmodus wird durch eine Gruppenrichtlinie aktiviert.

11.15 Gruppenrichtlinien-Voreinstellungen (Preferences)

Wenn Sie sich bereits mit Gruppenrichtlinien unter Windows Server 2003 (oder früher) beschäftigt haben, wird Ihnen aufgefallen sein, dass in Wndows 7 im Gruppenrichtlinienverwaltungs-Editor außer RICHTLINIEN ein zusätzlicher Knoten namens EINSTELLUNGEN vorhanden ist. Dieser findet sich sowohl in der Benutzer- als auch in der Computerkonfiguration.

Es handelt sich hierbei um die *Voreinstellungen*, in der englischsprachigen Dokumentation heißen sie *Preferences*. Im Gegensatz zu den »normalen« Gruppenrichtlinien geht es hierbei weniger darum, bestimmte Einstellungen zu erzwingen, sondern um das Bereitstellen von diversen Voreinstellungen. Auf diese Weise

können und sollen die bislang für solche Zwecke verwendeten Login-Skripts eliminiert werden; weiterhin dürfte durch die Möglichkeit, diverse Voreinstellungen zu verteilen, die Notwendigkeit für verschiedene Images bei der PC-Installation entfallen.

Preferences

Dieses Feature ist neben dem ADMX-Format die wesentliche Neuerung bezüglich der Gruppenrichtlinien seit Windows Server 2008.

Die verwendete Technologie hat Microsoft übrigens durch die Akquisition der Firma *DesktopStandard* im Jahre 2006 erworben.

Als Clients können Windows XP SP2, Windows Server 2003 SP1 und alle späteren Versionen verwendet werden.

Tabelle 11.2 gibt einen Überblick über die Unterschiede zwischen den klassischen Gruppenrichtlinien und den Voreinstellungen:

Kategorie	Voreinstellung	Richtlinie
Erzwingung	Einstellungen werden nicht erzwungen. Die Konfigurationsmöglichkeit für den Benutzer bleibt erhalten. Einstellungen werden entweder einmal angewendet oder regelmäßig erneuert.	Einstellungen werden erzwungen. Die Konfigurationsmöglichkeit für die Benutzer ist nicht mehr vorhanden. Einstellungen werden regelmäßig erneuert.
Flexibilität	Es können Einstellungen für die Registry, Dateien etc. eingetragen werden. Registry-Einstellungen können importiert werden.	Richtlinien zur Verwaltung von Dateien, Ordnern etc. können nicht erstellt werden. Registry-Einstellungen müssen über administrative Vorlagen erzeugt werden.
Lokale Gruppenrichtlinie	Voreinstellungen sind in den drei lokalen Gruppenrichtlinien von Vista und Windows Server 2008 nicht vorhanden.	
Registry	Ursprüngliche Registry-Einstellungen werden überschrieben. Das Entfernen der Voreinstellungen stellt die ursprünglichen Registry-Einstellungen nicht wieder her.	Ursprüngliche Registry-Einstellungen bleiben erhalten. Wird eine Richtlinie entfernt, wird die ursprüngliche Registry-Einstellung wiederhergestellt.

Tabelle 11.2 Gruppenrichtlinien und ihre Voreinstellungen

Kategorie	Voreinstellung	Richtlinie
Zielgruppenadressierung und Filterung	Die Zielgruppenadressierung auf Ebene der einzelnen Voreinstellung ist vorhanden.	Eine Filterung auf Basis von WMIQuerys ist vorhanden. Filterung wird auf Ebene des Gruppenrichtlinienobjekts unterstützt.
Benutzerinterface	Das aus den »normalen« Einstellungen bekannte Benutzerinterface (d. h. die normalen Konfigurationsdialoge) wird in den meisten Fällen gezeigt.	Bei der Konfiguration der Richtlinien wird das etwas spartanische »Gruppenrichtlinien-Benutzerinface« verwendet.

Tabelle 11.2 Gruppenrichtlinien und ihre Voreinstellungen (Forts.)

Abbildung 11.80 zeigt die aufgeklappten Voreinstellungen für die Computer- und die Benutzerkonfiguration. Sie finden dort etliche interessante Aspekte wie das Setzen von Umgebungsvariablen, den Umgang mit INI-Dateien, den Zugriff auf lokale? Benutzer und Gruppen und vieles andere mehr.

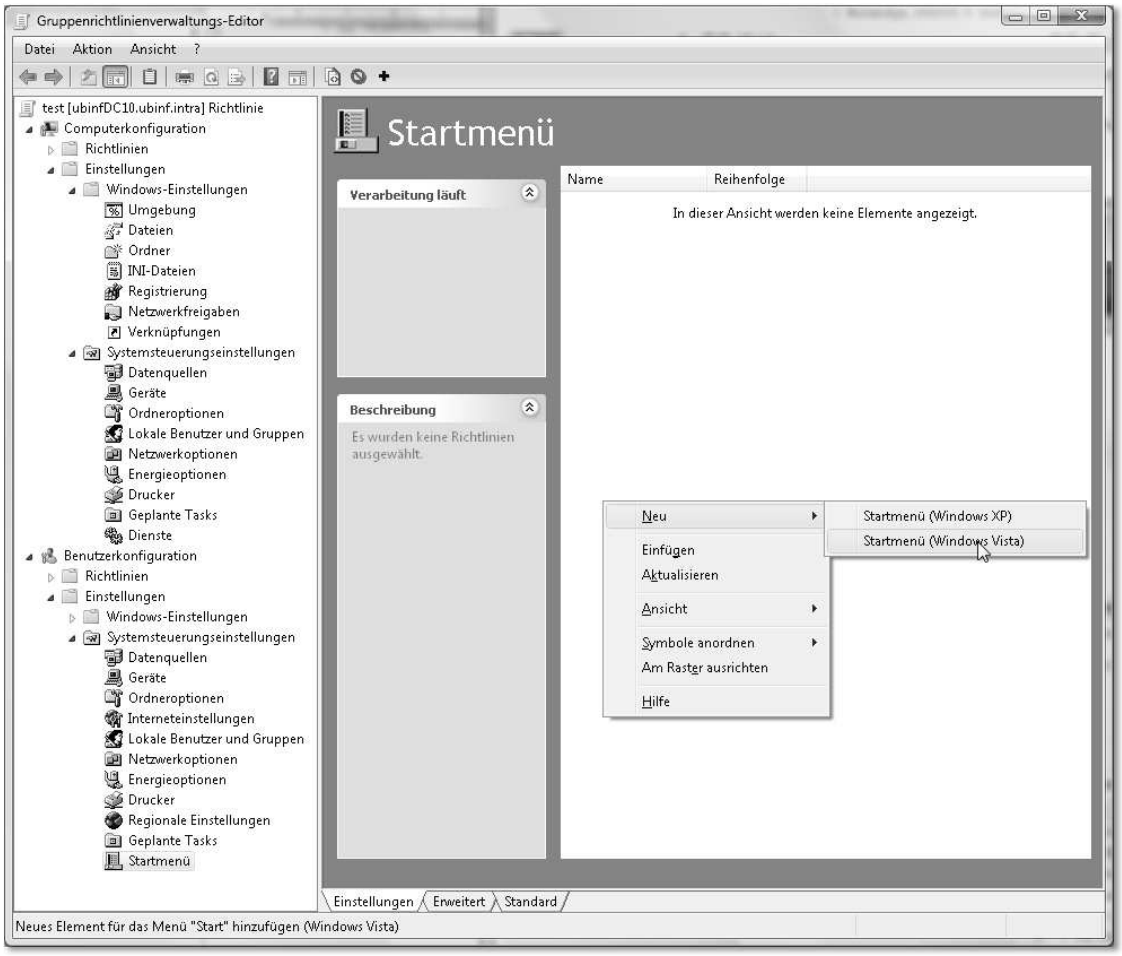


Abbildung 11.80 In einem Gruppenrichtlinienobjekt können Sie Voreinstellungen definieren.

Ein Merkmal der Voreinstellungen ist, dass die Konfiguration zumeist über Dialoge geschieht, die den »Original-Dialogen« nachempfunden sind, die bei der »normalen« Konfiguration verwendet werden. Abbildung 11.81 zeigt das Bearbeiten der Voreinstellungen für das Vista-Startmenü – die Dialoge kommen einem irgendwie bekannt vor.

Hinweis

In den folgenden Screenshots ist immer vom Windows Vista-Startmenü die Rede. Diese Einstellung wirkt aber auch für Windows 7.

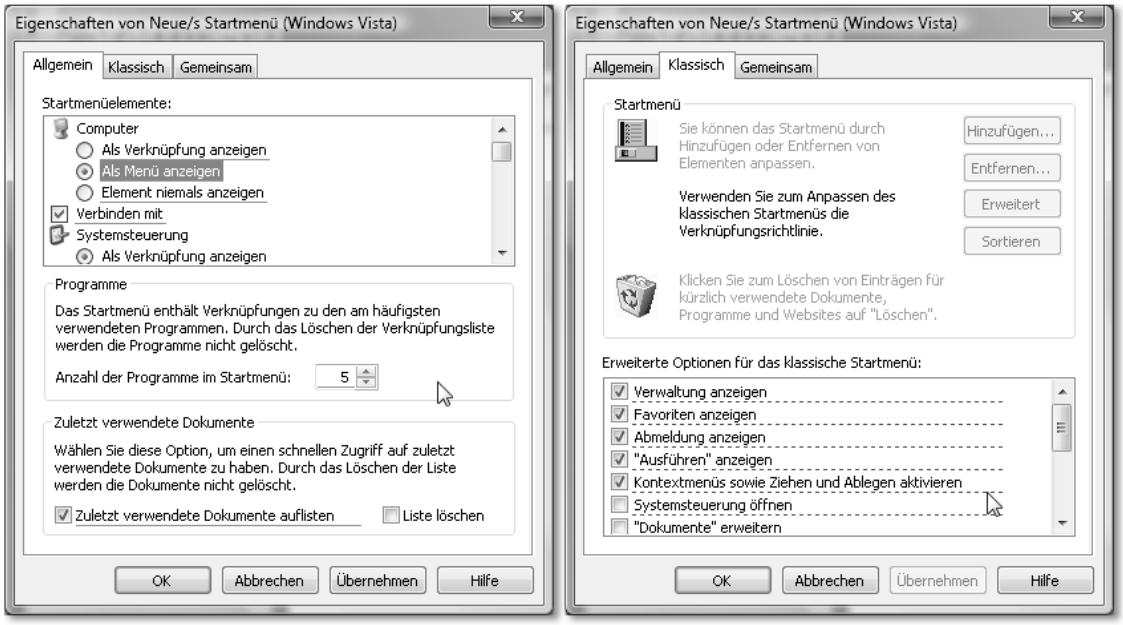


Abbildung 11.81 So bearbeiten Sie die Voreinstellung für das Startmenü.

Beachten Sie die Registerkarte GEMEINSAM im Konfigurationsdialog jeder Voreinstellung. Wie Sie auf Abbildung 11.82 sehen können, gibt es hier eine Möglichkeit, um festzulegen, ob die Voreinstellungen tatsächlich angewendet werden sollen: die *Zielgruppenadressierung*. Auf Abbildung 11.83 ist der *Zielgruppenadressierungseditor* zu sehen. Sie können in einer einfach zu handhabenden grafischen Benutzeroberfläche beispielsweise festlegen, dass die Voreinstellung nur für tragbare Computer angewendet werden soll. Diverse andere Möglichkeiten sind auf der Abbildung zu sehen.

Abbildung 11.84 zeigt, dass sich unter den Stichwörtern der Zielgruppenadressierungseinstellungen (z. B. TRAGBARER COMPUTER) durchaus noch weitere Einstellmöglichkeiten finden. So können Sie beispielsweise festlegen, dass eine Voreinstellung nur gelten soll, wenn das Notebook gedockt ist.

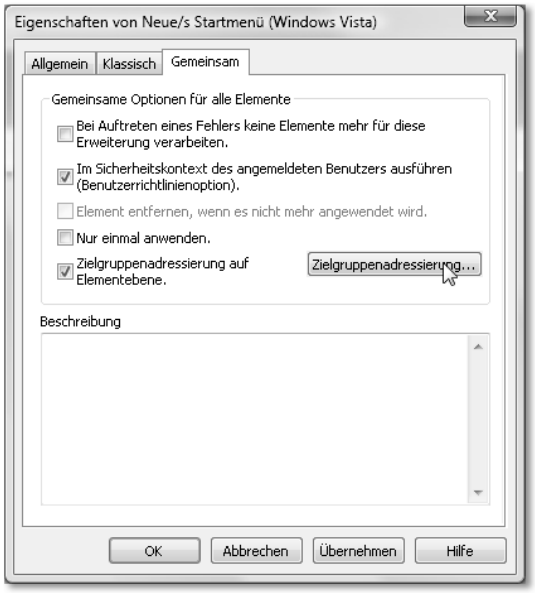


Abbildung 11.82 Auf der Registerkarte »Gemeinsam« rufen Sie den Dialog zur Konfiguration der Zielgruppenadressierung auf.

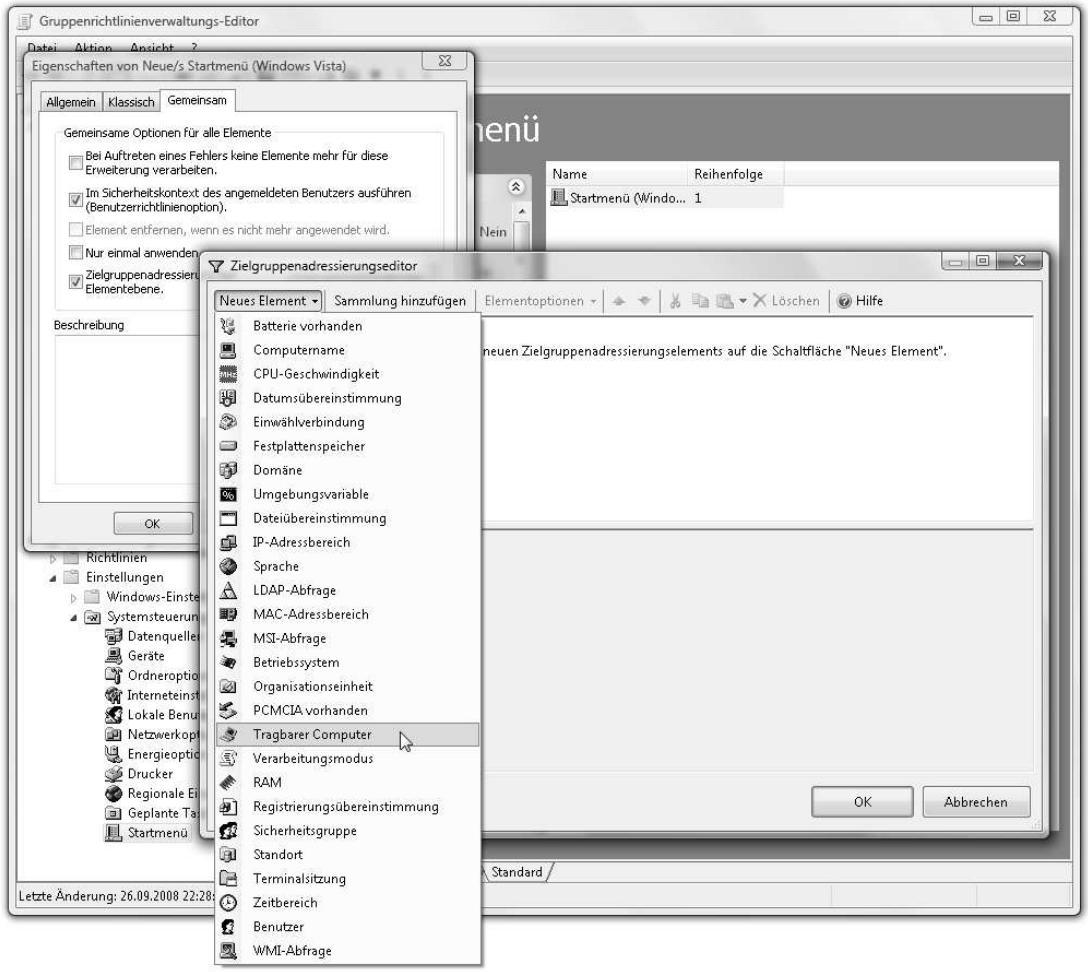


Abbildung 11.83 Der Zielgruppenadressierungseditor

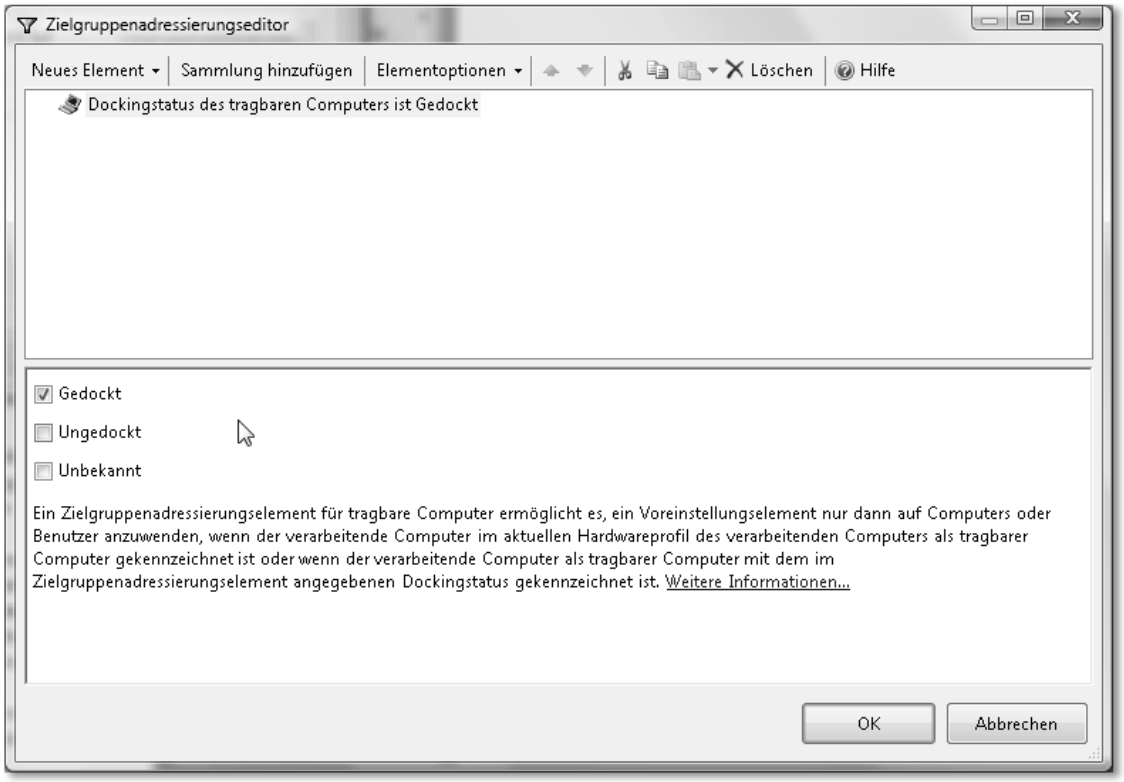


Abbildung 11.84 Hier wird die Einstellung für den Dockingstatus konfiguriert.

11.16 AGPM – Advanced Group Policy Management

Ich möchte darauf hinweisen, dass für Software-Assurance-Kunden im Rahmen des *Microsoft Desktop Optimization Packs* die Anwendung *Advanced Group Policy Management* (AGPM) zur Verfügung steht.

AGPM dürfte vor allem für mittlere und größere Unternehmen von Interesse sein – mehr dazu finden Sie in Abschnitt 10.5.

Es standen nämlich die ionischen Städte anfangs unter Tissaphernes, von dem König ihm verliehen, damals aber waren sie alle zu Kyros abgefallen, mit Ausnahme von Milet.

12 Sicherheit

Sicherheit ist ohne Zweifel eines der vordringlichsten Themen. In diesem Umfeld sehe ich fünf wichtige Aspekte, die ich kurz – und ohne ausschweifende mehr oder weniger philosophische Betrachtung – benennen möchte:

- *Die technischen Gegebenheiten des Betriebssystems*: Vielleicht erinnern Sie sich noch an die späten 90er-Jahre und den Anfang des neuen Jahrtausends: Damals jagte eine Pressemitteilung über neue spektakuläre Sicherheitslücken in den Microsoft-Produkten die nächste. Bewertet man diese Situation in ihrem »historischen Kontext«, ist das auch gar nicht so erstaunlich – alle anderen Betriebssysteme (inklusive das angeblich so sichere Linux) werden übrigens dieselben Probleme gehabt haben, was mangels Verbreitung und dem daraus resultierenden öffentlichen Interesse aber einfach nicht oder nicht so stark wahrgenommen wurde: In den 90er-Jahren liefen die Betriebssysteme in einer recht abgeschotteten Welt im lokalen Netz. Das Internet war vorhanden und wurde genutzt, war aber bei Weitem nicht so omnipräsent wie heute. In diesem lokalen Netz gab es folglich auch viel weniger Bedrohungen von außen. Das im Wesentlichen betrachtete Szenario waren Viren, die auf Datenträgern oder per E-Mail eingeschleppt wurden.

  Folglich hat wohl kaum ein Programmierer, egal ob bei Microsoft oder sonstwo, sich wirklich ernsthaft darüber Gedanken gemacht, dass sich ein Problem im Programmcode zu einem spektakulären Sicherheitsproblem entwickeln könnte. In einer verbundenen Welt, die dann insbesondere um die Jahrtausendwende Realität zu werden begann, wurden genau diese Programmfehler rigoros ausgenutzt – und traten als Sicherheitslücken in Erscheinung. Hätte die Welt weiterhin »nur« aus abgeschlossenen LANs bestanden, wären diese Fehler wohl nie zutage getreten – oder zumindest nicht so massiv.

  Ich möchte hier nun keine Programmierfehler schönreden, es ist aber schon wichtig, sich darüber klar zu werden, was damals geschehen ist und wie diese Erfahrungen eingeordnet werden müssen.

Man kann wohl mittlerweile schon davon ausgehen, dass Microsoft das Thema Codequalität sehr ernst nimmt und dass das diesbezügliche Niveau bei Windows 7 ein ganz anderes ist als beispielsweise bei NT4 oder auch bei dem ersten Windows 2000-Release.

Bekanntlich ist Software niemals komplett fehlerfrei und wird es auch niemals sein. Um diesem Punkt Rechnung zu tragen, gibt es regelmäßig Patches und Hotfixes.

- *Implementation des Betriebssystems*: Viele Angriffe auf NT4 und Windows 2000 machten sich die Tatsache zunutze, dass bei der Installation standardmäßig alle irgendwie verfügbaren Komponenten installiert wurden. Viele Angriffsszenarien nutzten beispielsweise die durch dieses Verhalten massig vorhandenen IIS-Dienste (Internet Information Server), die die Administratoren mangels Bewusstsein, dass diese überhaupt vorhanden waren, oder aufgrund fehlenden Know-hows nicht pflegten.

  Sowohl im Client- als auch im Serverumfeld geht Microsoft mittlerweile den Weg, dass nur die Komponenten vorhanden sind, die explizit vom Administrator installiert werden. Das ist sicher ein dringend notwendiger Schritt in die einzig sinnvolle Richtung.

  Die Verantwortung dafür, was der jeweilige Administrator nun aus dem Betriebssystem macht, kann Microsoft natürlich nicht übernehmen. Im Klartext sind also Administratoren und Systemarchitekten gefordert, eine qualitativ hochwertige Installation auf die PCs zu bringen. Hier bietet sich nun eine breite Palette von möglichen »Sünden«, die begangen werden könnten: Dies beginnt beim Ausrollen von veralteten Softwareständen, geht über das routinemäßige Abschalten der Windows-Firewall und endet bei der massenweisen Installation von nicht benötigten Betriebssystemkomponenten (oder sonstigen »Utilitys«).

  Es besteht also selbstverständlich die Möglichkeit, aus dem unter Sicherheitsaspekten eigentlich sehr ordentlichen Betriebssystem eine unternehmensgefährdende Daten- und Malware-Schleuder zu machen.

- *Die technischen Gegebenheiten der Gesamtumgebung*: Das Desktop-Betriebssystem ist niemals allein. Es ist umgeben von Servern, Netzwerkkomponenten, Protokollen, Software und dergleichen mehr. Es existiert in einer im Allgemeinen gewachsenen Unternehmensumgebung.

  Was ich sagen will: Es ist zweifelsfrei notwendig, dass Sie sich um eine unter Sicherheitsaspekten optimale Installation der Windows 7-Clients kümmern. Es ist aber genauso wichtig, dass Sie hin und wieder einen prüfenden Blick auf Ihr Gesamtszenario werfen. Zur Verdeutlichung empfehle ich die Lektüre des Beispiels im nächsten Abschnitt (Abschnitt 12.1, »Mein Lieblingsbeispiel«).

Letztendlich gilt hier, wie auch im richtigen Leben, dass die Kette nur so stark wie ihr schwächstes Glied ist. Wahrscheinlich werden die Windows 7-Clients nicht das schwächste Glied sein, allerdings ist Ihnen mit dieser Aussage auch nicht viel geholfen, wenn Sie ein Opfer von Datenklau und/oder Datenmanipulation geworden sind.

- *Die gelebten Vorgehensweisen bei Administration und Pflege des Systems*: Heute, im Jahr 2009, brauche ich wohl niemandem mehr zu erzählen, dass es notwendig ist, regelmäßig die von Microsoft zur Verfügung gestellten Patches einzuspielen – dachte ich. Ich verbringe meinen Tag damit, in der Gegend herumzugondeln und mir Installationen anzuschauen, und nur gefühlte 25 % der Unternehmen und Organisationen spielen diese Patches wirklich auch regelmäßig ein. Ja, mir ist klar, dass Patches auch zu Problemen führen können. Ja, mir ist auch klar, dass Updates und Patches sich nicht von selbst einspielen und WSUS auch nicht ganz adminfrei betrieben werden kann. Trotzdem ist eine Umgebung, in der PCs und Server ihr ganzes Leben lang auf dem Stand der Installation bleiben, unter Sicherheitsaspekten eine ziemliche Katastrophe – vorsichtig ausgedrückt. Da hilft es übrigens auch nur wenig, wenn es eine vom Geschäftsführer unterschriebene Unternehmensrichtlinie gibt, die das zur gewünschten und offiziell für gut befundenen Vorgehensweise erklärt.

  Es gibt aber diverse viel subtilere Beispiele, wie Sicherheitsprobleme in der Betriebsphase entstehen: Irgendetwas funktioniert nicht, und deswegen wird die Windows-Firewall »vorübergehend« abgeschaltet – blöd nur, dass soetwas leicht zur Dauerlösung wird. Beliebt sind auch mehr oder weniger hektisch durchgeführte Modifikationen von Sicherheitseinstellungen, Berechtigungen und Richtlinien: Häufig wird mehr zugelassen, als unbedingt notwendig ist, und dann gerät die Aufgabe, dies zu optimieren, in Vergessenheit – für immer. Ich möchte diese Anmerkungen nun keineswegs als Admin-Schelte verstanden wissen. Mir ist klar, dass die real existierenden Anwender schnell eine Lösung für ihr jeweiliges Problem fordern und es ihnen dabei herzlich egal ist, dass der Administrator dabei gegen besseres Wissen handelt. An dieser schleichenden Verschlechterung des Sicherheitsniveaus ist niemand wirklich »schuld«, wobei diese Erkenntnis allerdings nichts an dem Problem ändert. Es wird notwendig sein, genau zu definieren, wann welche Änderungen durchgeführt werden dürfen. Die Änderungen müssen bewertet und dokumentiert werden. Ein Ergebnis könnte übrigens auch sein, dass eine Anwendung nicht oder nur unter bestimmten eng eingrenzbaren Bedingungen eingesetzt werden darf, weil ihre Installation einen massiven Eingriff in das Sicherheitskonzept bedeuten würde (z. B. wenn eine Anwendung partout mit administrativen Berechtigungen ausgeführt werden will).

- *Der Umgang der Benutzer mit den Geräten und Programmen*: Der Klassiker für die Gefährdung der Sicherheit der Daten ist das Fehlverhalten der Benutzer. Ich möchte nun die Anwender nicht unter einen Generalverdacht stellen, es bleibt aber festzuhalten, dass es durchaus viele Situationen gibt, in denen Daten aufgrund schusseligen oder fahrlässigen Verhaltens gefährdet und/oder korrumpiert worden sind. Das beginnt mit dem im Taxi oder in der Flughafen-Lounge liegen gelassenen Notebook, und natürlich müssen auch gezielte Diebstähle in Betracht gezogen werden.

  Problematisch ist, dass viele Benutzer nach wie vor jeden Anhang öffnen und jedem noch so suspekten Link im Browser folgen, wenn er durch bestimmte Schlüsselbegriffe attraktiv gemacht wird. Etwas deutlicher: Viele (männliche) Zeitgenossen klicken garantiert auf einen Link oder einen Anhang, wenn sich dahinter leicht bekleidete Mitbürgerinnen vermuten lassen: »Sex sells malware«. Durch die üblichen Viren- und Malware-Abwehrmaßnahmen lässt sich auch hier technisch einiges bewirken, die Sensibilisierung der Anwender ist aber in jedem Fall wichtig.

  Das »Social Hacking«, dessen eine Facette das Erlangen von Zugängen durch Täuschen der Anwender ist (»Ich rufe vom IT-Service an und bräuchte einmal Ihr Kennwort, weil wir Ihnen eine neue Software installieren«), ist nach wie vor eine latente Gefahr. Ich fürchte, dass noch immer hinreichend viele Anwender auf derlei Tricks hereinfallen – zumindest wenn die Betrüger etwas geschickter sind, als einfach plump anzurufen und nachzufragen. Die Auswirkungen, wenn auf diese Weise Zugangsdaten verloren werden, sind übrigens größer geworden als noch vor ein paar Jahren: Die meisten Unternehmen ermöglichen den Mitarbeitern den Datenzugriff von Mobilgeräten oder aus dem Homeoffice. Mit anderen Worten: Man kann mit einem erbeuteten Zugang heute deutlich mehr anfangen als noch vor ein paar Jahren – und zwar ohne auch nur in der räumlichen Nähe des Unternehmens zu sein.

Welche Schlüsse können nun aus diesen Überlegungen gezogen werden?

- Es ist notwendig, die technischen Möglichkeiten auszuschöpfen. Dadurch lässt sich zwar nicht jedes Übel bekämpfen, man kann allerdings viele Bedrohungsszenarien minimieren.
- Die Administratoren und IT-Verantwortlichen müssen jede Änderungsmaßnahme hinterfragen, um nicht die Sicherheit des Gesamtsystems in der Betriebsphase immer weiter zu reduzieren. Dokumentierte Prozesse und Richtlinien helfen dabei.
- Jeder einzelne Benutzer muss sensibilisiert und zur aktiven Mitarbeit bei der Erreichung dieses Ziels angehalten werden. Dies geht erfahrungsgemäß bes-

ser, wenn dies nicht über »Drohungen« erreicht wird, sondern wenn die Anwender aus Einsicht und Überzeugung handeln. Dies ist natürlich einfacher gesagt als getan und hat auch viel damit zu tun, ob sich die Anwender grundsätzlich mit dem Unternehmen und dessen Zielen identifizieren oder ob sie nur dort arbeiten, weil sie keinen besseren Job bekommen konnten. Letzteres ist zwar nicht unbedingt ein Problem der IT, macht es aber schwerer, die Kollegen für das gemeinsame Ziel »Sicherheit« zu interessieren.

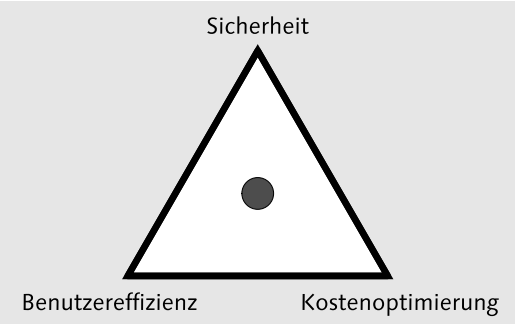


Abbildung 12.1 Das Spannungsfeld zwischen Sicherheit, Benutzereffizienz und Kostenoptimierung

Bei den Überlegungen, wie sich die Sicherheit eines Systems verbessern lässt, gibt es ein recht interessantes grafisches Modell (Abbildung 12.1): An die Ecken eines gleichseitigen Dreiecks werden die Aspekte *Sicherheit*, *Kostenoptimierung* und *Benutzereffizienz* aufgetragen. Sie können nun eine Kugel auf den Punkt der Fläche schieben, der für Ihr Unternehmen die optimale Kombination darstellt. Es gibt drei Extreme:

- Wenn Sie die Kugel komplett in die Ecke *Sicherheit* verschieben, bedeutet das, dass Sie beliebig Geld für alle möglichen Sicherheitstechnologien und -maßnahmen ausgeben und dabei die Benutzerumgebung konsequent auf maximale Sicherheit trimmen: Den Zugriff auf Daten von außen könnte man beispielsweise komplett unterbinden, und der Zugriff auf das Internet ist ebenfalls ein potenzielles Risiko, das es auszuschalten gilt. Weiterhin dürfen Unternehmensdaten nicht auf Notebooks mitgeführt werden. Weitere Aspekte sind denkbar.

  Die Umgebung wird zwar ein hohes Sicherheitsniveau aufweisen, aber besonders effizient werden die Benutzer nicht mehr arbeiten können.

- Ein weiteres Extrem wäre, alles auf maximale *Kostenoptimierung* zu trimmen. Dabei blieben notwendigerweise technische Sicherheitsmaßnahmen (die kosten im Allgemeinen Geld) auf der Strecke, und dasselbe gilt für die Benutzereffizienz.

- Das dritte Extrem wäre, alles an der *Benutzereffizienz* auszurichten oder, anders gesagt, den Benutzern das Leben so bequem wie möglich zu machen. Erlaubt man alles, was bequem ist und Spaß macht, wird dies fast notwendigerweise zulasten der Sicherheit gehen.

Wie immer im Leben wird es also auf einen Kompromiss hinauslaufen, da vermutlich auch in Ihrem Unternehmen bzw. Ihrer Organisation alle drei Aspekte gefragt sein werden. Sie müssen also erarbeiten, wo die Kugel hingeschoben werden soll. Vermutlich wird sie irgendwo mitten auf der Fläche liegen bleiben und eine leichte Tendenz in eine Richtung haben.

Sicherheit in der IT ist also letztendlich ein Kompromiss, wobei dies nicht bedeuten soll, dass die Umgebung dramatisch unsicher ist, nur weil den Benutzern die Kommunikation über das Internet gestattet wird und der Geschäftsführer kein unbegrenztes Budget bewilligt hat. Das Schutzbedürfnis wird ohnehin von Unternehmen und Unternehmen unterschiedlich sein. Hightechunternehmen, die in extrem sensiblen Bereichen tätig sind, werden sicherlich andere Anforderungen haben als beispielsweise ein kleiner mittelständischer Metallverarbeitungsbetrieb.

12.1 Mein Lieblingsbeispiel in Sachen Sicherheit

Ich finde es sehr positiv, wenn sich die IT-Verantwortlichen in Unternehmen und Organisationen mit dem Thema Sicherheit beschäftigen. Ich beobachte aber gar nicht so selten zwei Effekte:

- Es werden Maßnahmen geplant und teilweise auch umgesetzt, die das Unternehmen auch vor einem massiven gemeinsamen Angriff von russischem Geheimdienst, CIA, NSA und Mossad schützen könnten. Eine realistische Gefahrenabschätzung ist also unbedingt notwendig. Wenn Ihr Unternehmen weder ein attraktives Ziel für Industriespionage ist und auch nicht so bekannt und/oder verhasst ist, dass sich jeder Hacker der Welt daran beweisen möchte, kann man wohl eher von einem mittleren oder geringen Gefährdungspotenzial ausgehen.

  Die Sicherheit darf natürlich trotzdem nicht vernachlässigt werden, es macht dann aber wenig Sinn, so zu tun, als ob sie von Feinden und Spionen umzingelt seien, und massiv Geld in die Sicherheitsinfrastruktur zu pumpen. Bleiben Sie also realistisch, aber ohne dabei irgendwie leichtsinnig zu werden.
- Teilweise werden komplizierte Maßnahmen ergriffen, um bestimmte Gefährdungen auszuschließen. Auch wenn diese Maßnahmen hier und da vielleicht »überdimensioniert« sind, schadet es zunächst »nur« dem Budget. Kritisch ist

allerdings, wenn durch die Konzentration auf ein Bedrohungsszenario andere nicht berücksichtigt werden – eventuell sogar solche, die wesentlich »konkreter« sind.

Zu dem zweiten Punkt ein kleines Beispiel:

Technisch denkende Menschen tendieren meiner Erfahrung nach dazu, die ganz simplen Möglichkeiten für die »illegale Aneignung« von Daten zu vernachlässigen. Es ist schon nicht mehr ganz trivial, gezielt einen Trojaner einzuschleusen und diesen als »zuverlässige Backdoor« ins Unternehmensnetz zu positionieren. In vielen Fällen gibt es einen wesentlich einfacheren Weg, der auf Abbildung 12.2 skizziert ist:

- Ein WLAN-Access-Point ist in das Unternehmensnetz geschmuggelt worden.
- Wenn jeder Client, der eine IP-Adresse per DHCP anfordert, auch eine solche bekommt, kann sich der Dunkelmann bzw. die Dunkelfrau problemlos mit dem Notebook auf eine bequeme Bank in den Park hinter dem Firmengebäude setzen und ist im Innenbereich des Netzes.
- Ohne Zugangskennwort kommt man zwar zunächst nicht unbedingt weiter, aber befindet man sich IP-mäßig »innen«, kann man in aller Ruhe beginnen, die »üblichen Maßnahmen« ablaufen zu lassen, um irgendwo eine Schwachstelle zu finden (z. B. Portscanner einsetzen, Social-Hacking, Ausnutzung von bekannten Schwachstellen ungepatchter Systeme etc.).

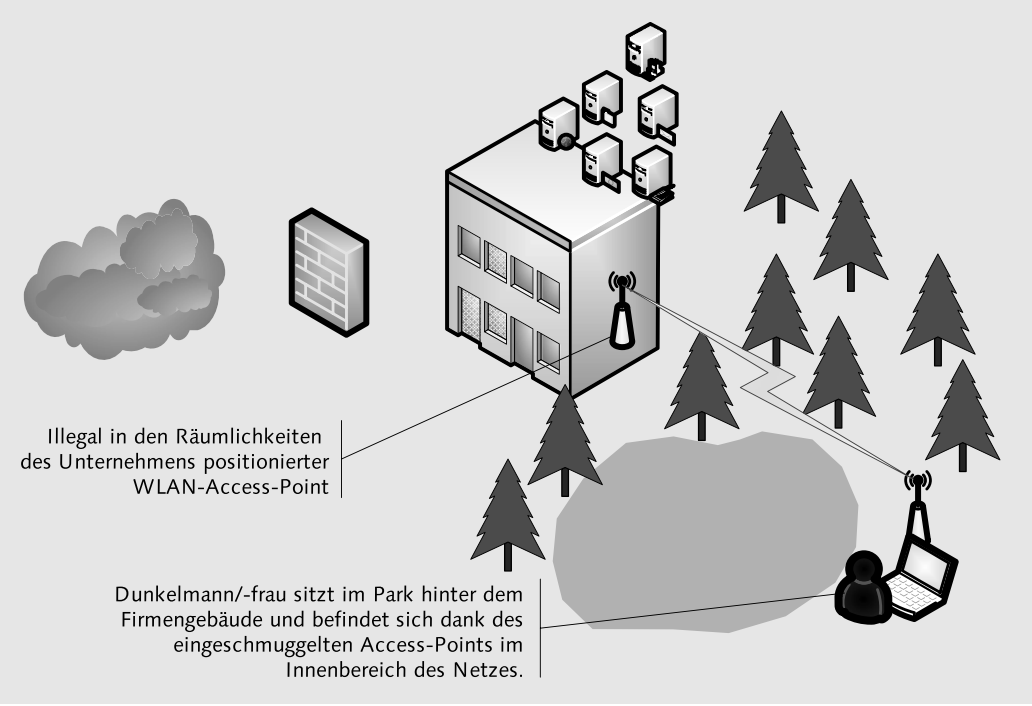


Abbildung 12.2 So einfach kommt man in ein Unternehmens-LAN, wenn ein WLAN-Access-Point »eingeschmuggelt« worden ist.

Einen WLAN-Access-Point irgendwo einzuschmuggeln, ist in vielen Unternehmen deutlich einfacher, als man auf den ersten Blick vielleicht vermutet. Ich besuche so gut wie jeden Tag Unternehmen, Organisationen und Behörden. Beim Warten auf den Ansprechpartner werde ich zumeist unbeaufsichtigt in Wartezonen, Besucherzimmern etc. zurückgelassen, in denen oft ungeschützte Netzwerkanschlüsse zu finden sind. Ich habe natürlich nie ausprobiert, ob es da wirklich eine Verbindung zum Netz gibt, vermutlich wäre man aber zumindest in 50 % der Fälle erfolgreich.

Viele Unternehmen und Organisationen haben Bereiche, die ganz offiziell für Kunden zugänglich sind, also Wartezonen, Show-Rooms, Verkaufsflächen, wo es auch durchaus möglich sein könnte, einen »trojanischen WLAN-AP« zu positionieren. Und wenn das alles nicht gelingt, hilft immer noch der gute alte Einbruch, bei dem seltsamerweise nichts gestohlen wird, aber irgendwo ein zusätzliches Teil zurückgelassen wird, das dann jahrelang unbemerkt bleibt: nämlich ein WLAN-AP, der irgendwo vor einem Drucker hängt. Denkbar ist auch, so etwas nicht in der gut bewachten Zentrale, sondern am Fertigungsstandort in Estland (oder wo auch immer) zu tun, wo die Sicherheitsmaßnahmen nicht so stark sind – da viele Unternehmen aber die VPN-Verbindungen vollkommen offen halten, ist so etwas für den Datendieb genauso gut.

Ich möchte mich nicht zu sehr auf den WLAN-Access-Point konzentrieren, Fakt ist aber, dass es viele Schwachstellen gibt, die zunächst gar nichts »mit Computern« zu tun haben, die aber ausgenutzt werden könnten. Daraus lassen sich drei Punkte ableiten:

- Schauen Sie ganzheitlich auf die Infrastruktur. Denken Sie wie ein Datendieb, und fragen Sie sich, wie Sie beim »Angriff« auf Ihr Unternehmen beginnen würden. Beseitigen Sie die offenkundigen Schwachstellen.
- Sie werden das Netzwerk niemals wirklich »dicht« bekommen. Dass jemand in eine Niederlassung einbricht und einen WLAN-AP montiert, können Sie nicht hundertprozentig verhindern. Denken Sie also über Maßnahmen nach, die es jemandem, der zwar eine physikalische Verbindung in Ihr Netz hat, schwer macht, tatsächlich zu kommunizieren. Die Port-Authentifizierung auf Basis der Switches, am besten in Verbindung mit der im Verlauf des Kapitels vorgestellten *Network Access Protection* (NAP) könnte so ein Ansatz sein.
- Da Sie auch nicht hundertprozentig ausschließen können, dass jemand Zugriff auf das Netz erhält (also nicht nur physikalisch »drin« ist, sondern auch kommunizieren kann), müssen die Systeme bestmöglich gesichert sein. Die Patches, die Microsoft monatlich veröffentlicht, dienen zu einem Großteil dazu, Sicherheitslücken der Systeme zu schließen. In vielen Fällen sind das genau die Sicherheitslücken, die ausgenutzt werden können, wenn man eine IP-Ver-

bindung zu den Computern hat. Weiterhin helfen die lokalen Firewalls (sprich die Windows-Firewall), eine weitere Verteidigungslinie aufzubauen.

In diese Überlegungen passt hinein, dass es Mitarbeiter geben könnte, die doch nicht so vertrauenswürdig und integer sind, wie sie eigentlich sein sollten. Unzufriedene Mitarbeiter mit Rachegelüsten sind immer ein Problem. Die Möglichkeiten, die ein solcher Mitarbeiter hat, sind häufig nicht mit Betriebssystemmitteln zu stoppen: Wer offiziell auf die Kundendatenbank zugreifen und die Datensätze exportieren kann, wird das auch mit »dunklen Absichten« können. Hier gilt es also, auch die Applikationen zu durchleuchten und Berechtigungen einzuschränken.

12.2 Windows Server Update Services (WSUS)

Es hat sich gezeigt, dass das Installieren von Patches, Service Packs oder sonstigen Updates einer der wichtigsten Beiträge sowohl zur »inneren Sicherheit« als auch für die Stabilität der Systeme ist.

So komplexe Produkte wie ein Windows-Betriebssystem, ein Exchange Server oder ein Office-Paket können notwendigerweise niemals fehlerfrei sein, trotz aller Qualitätssicherung in den Entwicklungsprozessen. Hierbei bezieht sich »fehlerfrei« sowohl auf die Resistenz gegen unautorisierte Zugriffsversuche (»Hacking«) als auch auf die stabile Funktion an sich.

Es ist extrem positiv zu bewerten, dass Microsoft mit Fehlern in den Produkten erstens sehr offen umgeht und zweitens recht zügig Patches zur Behebung derselben bereitstellt. Das ist in der IT-Branche vorbildlich. Obwohl es eigentlich selbstverständlich sein sollte, ist mir kein Hersteller bekannt, bei dem dieser Prozess so nachhaltig funktioniert.

Nun verhält es sich aber leider so, dass in den meisten Installationen zwar bei der Erstinstallation darauf geachtet wird, dass aktuelle Service Packs und Patches eingespielt sind, aber danach ist die Maschine sich selbst überlassen. Das war vor zehn Jahren so, vor fünf Jahren, letztes Jahr, ist auch heute so und wird vermutlich auch in der Zukunft noch immer so sein. Da es allerdings dringend notwendig ist, diesen Zustand bzw. Missstand zu beheben, scheint mir ein Abschnitt über WSUS in diesem Buch sehr angebracht zu sein.

Falls Sie glauben, dass Patch-Management mittlerweile eine Selbstverständlichkeit ist und es folglich doch eigentlich nicht notwendig ist, so die Trommel dafür zu rühren: Ich sehe häufig Umgebungen, deren Verantwortliche mich zwar ganz zerknirscht anschauen, aber in denen trotzdem Windows-2000-Server und -Clients ohne Service Pack und Patches eingesetzt werden.

Ich kann gut verstehen, dass man nicht monatlich 30 Server und 500 Clients besuchen kann, um dort Updates aufzuspielen. Da der *Windows Server Update Service* (WSUS) aber sowohl kostenlos als auch recht einfach einzuführen ist, gibt es ab jetzt keine Entschuldigungen mehr.

12.2.1 Die Funktionsweise

Die Funktionsweise von WSUS ist in Abbildung 12.3 gezeigt:

- Der WSUS-Server im Unternehmen bzw. in der Organisation lädt Update-Definitionen und Updates von der Microsoft-Update-Website herunter.
- Die Clients, auf denen der Microsoft-Update-Client standardmäßig vorhanden ist, werden über Gruppenrichtlinien konfiguriert. So erhalten sie auf diesem Weg die Information, welcher WSUS-Server verwendet werden soll, ob automatisch die Software-Updates installiert werden sollen und dergleichen mehr.
- Die Clients fragen nun regelmäßig den WSUS-Server ab und erhalten dabei gegebenenfalls die benötigten Updates.

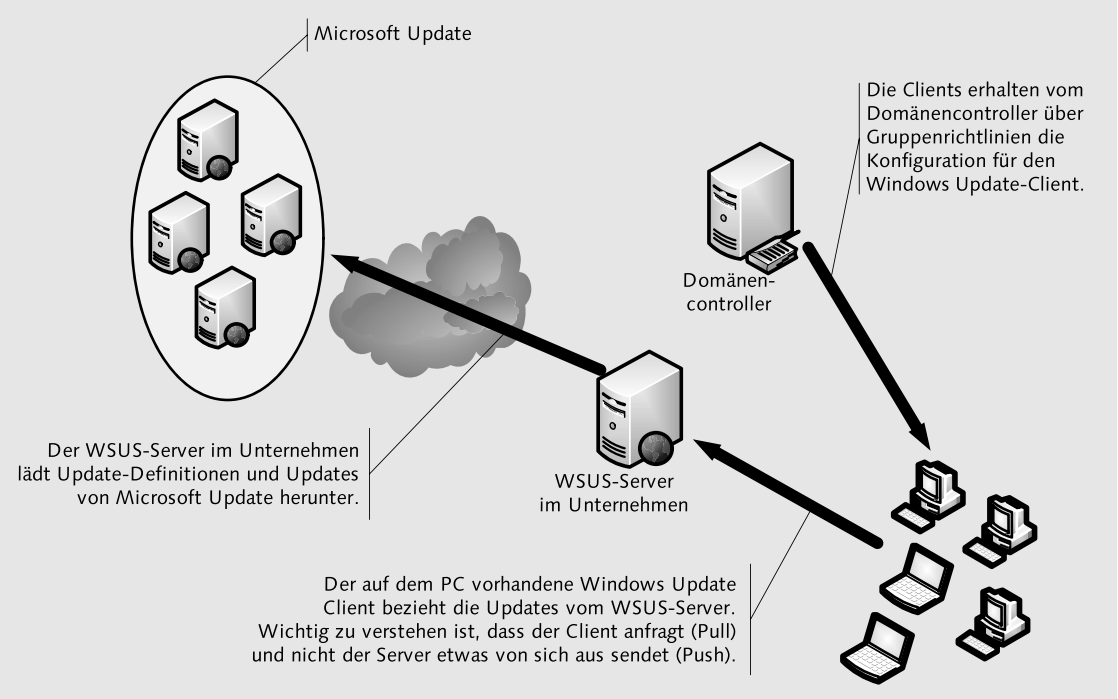


Abbildung 12.3 Stark vereinfacht: Die Funktionsweise von WSUS

Zwei Aspekte wären anzumerken:

- Welche Patches, Updates oder Service Packs letztendlich auf den WSUS-Clients installiert werden sollen, entscheidet weder Microsoft noch der WSUS-Server, sondern der Administrator. Sie können entweder jedes ein-

zelne Update individuell genehmigen, oder Sie erstellen eine oder mehrere Regeln, die dieses für Sie erledigen.

- Im Gegensatz zu vielen »großen« Softwareverteilungslösungen wird bei WSUS der Verteilungsvorgang nicht vom Server angestoßen. Vielmehr ist es die Aufgabe des Clients, sich in regelmäßigen Abständen beim Server zu melden und zu prüfen, ob es Updates für ihn gibt. WSUS basiert also auf einem Pull- und nicht auf einem Push-Verfahren.

Es gibt noch eine weitere gute Nachricht in Zusammenhang mit WSUS – jedenfalls für den Finanzvorstand des Unternehmens: Microsoft bietet WSUS kostenlos an. Das Produkt ist zwar nicht im Lieferumfang von Windows Server 2008 enthalten, kann aber problemlos im Microsoft Download Center heruntergeladen werden. Abbildung 12.4 dient als kleine Suchhilfe. Es ist übrigens notwendig, dass Sie auf das »SP1« achten, ansonsten ist die Version nicht für Windows Server 2008 geeignet; aber vielleicht gibt es, wenn Sie diese Zeilen lesen, ja auch bereits WSUS 4.0.

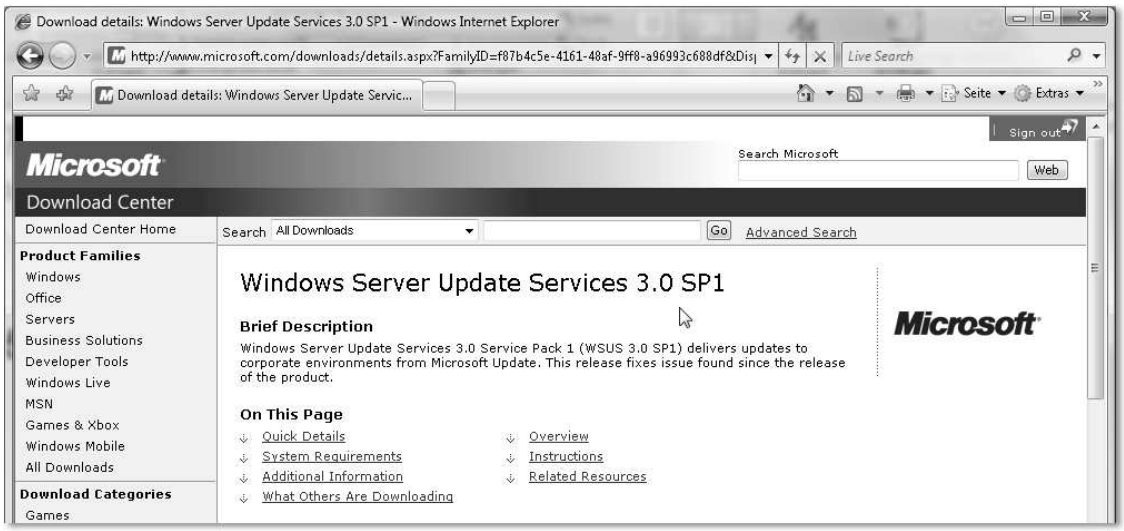


Abbildung 12.4 Kleine Suchhilfe: Das ist der momentan (Oktober 2009) aktuelle WSUS-Download. Zur Auswahl stehen ein 32- und ein 64-Bit-Download.

12.2.2 Installation

Die Installation ist – wie bei den meisten Microsoft-Produkten – unkompliziert, allerdings sind manuell einige Voraussetzungen zu installieren.

Voraussetzungen installieren

Die erste Voraussetzung ist, dass der Webserver (IIS) installiert ist. Das liegt übrigens nicht etwa daran, dass WSUS zur Verwaltung eine Weboberfläche hätte (hat es auch nicht), sondern dass die Clients über das HTTP-Protokoll zugreifen.

Das Hinzufügen der Rolle *Webserver (IIS)* wird wie üblich mit dem Server-Manager erledigt. Die Fragestellung dabei ist, welche Rollendienste installiert werden sollen. Hier die Antwort:

- Statischer Inhalt
- ASP.NET
- Windows-Authentifizierung
- IIS 6-Verwaltungskompatibilität
- IIS 6-Metabasiskompatibilität

Die zweite Komponente, die installiert sein muss, ist zwar optional, Sie sollten aber keinesfalls darauf verzichten. Die Rede ist vom *Report Viewer Redistributable*-Paket. Ist dieses nicht installiert, können Sie keine Reports anzeigen lassen, was für ein professionelles Management der WSUS-Installation natürlich eine Katastrophe ist. Abbildung 12.5 zeigt als Suchhilfe das aktuelle Paket im Download Center.

Abbildung 12.5 Suchhilfe für den »Report Viewer«

WSUS installieren

Die Installation erfolgt mithilfe eines Assistenten. Ich werde Sie auf ein paar Kleinigkeiten aufmerksam machen, aber viel Spannendes oder Problematisches gibt es nicht zu vermelden.

Zunächst ist interessant festzustellen, dass die WSUS-Verwaltungskonsole auch einzeln installiert werden kann (Abbildung 12.6, links). Das ist nicht uninteressant, denn so lässt sich vermeiden, dass der Administrator sich auf dem Server anmelden muss. Gut, das ist dank RDP kein Problem, ich bin aber immer dafür, unnötige Anmeldevorgänge auf dem Server zu vermeiden.

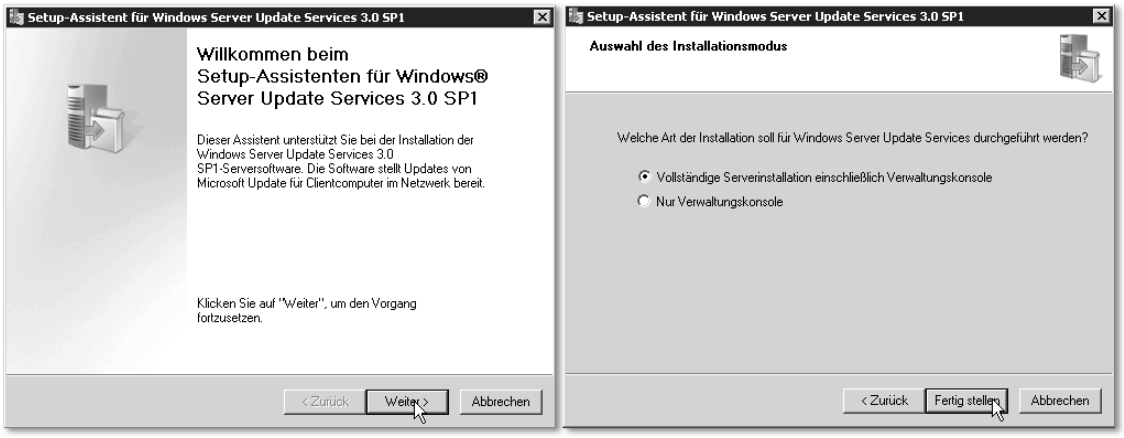


Abbildung 12.6 Wie Sie hier sehen, kann man die Verwaltungskonsole auch auf dem Adminarbeitsplatz installieren.

In den Dialogen aus Abbildung 12.7 müssen Sie zwei wichtige Entscheidungen treffen:

- Zunächst geht es darum, ob die Updates lokal auf Ihrem Server gespeichert werden sollen. Diese Checkbox werden Sie mit Sicherheit aktivieren, denn ansonsten würde jeder Client seine Updates über das Internet von Microsoft Update holen.

  Bei der Auswahl des Pfades müssen Sie aber beachten, dass die Datenmenge durchaus ganz ansehnlich ist. Auch wenn Sie »nur« deutschsprachige Versionen beziehen, kommen leicht einige Dutzend Gigabytes (!) zusammen.
- WSUS benötigt eine SQL Server-Datenbank. Falls Sie nicht über einen zentralen Datenbankserver verfügen, der noch ein wenig Last vertragen kann, können Sie den Assistenten die *Windows Internal Database* installieren lassen. Diese SQL-Server-Version ist ein Feature von Windows Server 2008; Sie brauchen es aber nicht per Hand hinzuzufügen.

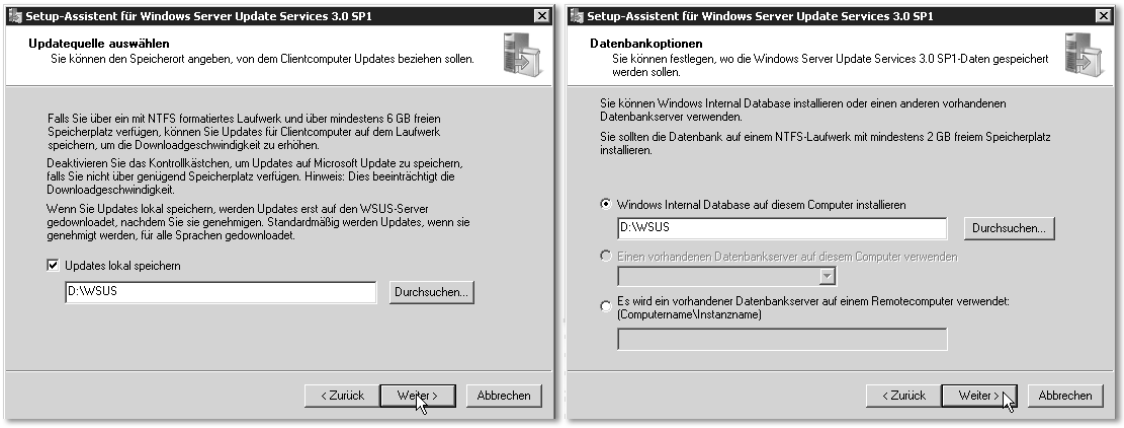


Abbildung 12.7 Die Frage nach den Ablageorten ist durchaus mit Vorsicht zu beantworten: Es kommen leicht einige Dutzend Gigabytes zusammen.

Die nächste (und letzte) Dialogseite des Assistenten bezieht sich auf die Website, in die die WSUS-Webkomponenten installiert werden sollen (Abbildung 12.8). Sofern keine andere Webanwendung auf dem Server installiert ist (oder werden soll), können Sie der Empfehlung des Assistenten folgen und die IIS-Standardwebsite verwenden. Alternativ kann der WSUS-Installationsassistent auch eine neue Website erstellen. Um diese Website eindeutig »identifizieren« zu können, gibt es drei Möglichkeiten:

- IP-Adresse
- Portnummer (also etwas anderes als 80; diese Möglichkeit würde ich nicht empfehlen)
- Host-Header

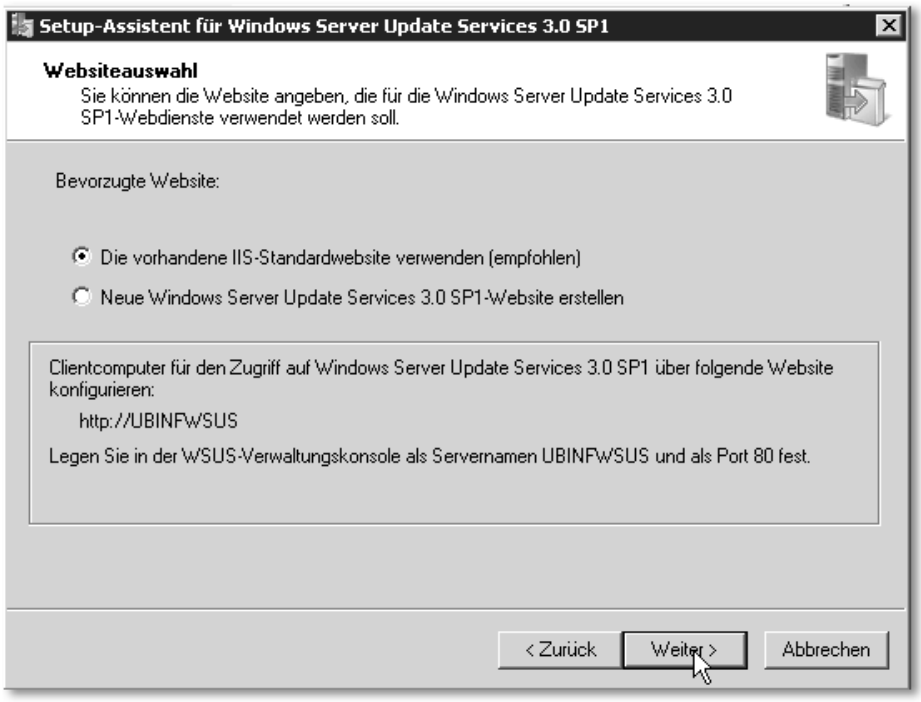


Abbildung 12.8 Ist auf der Standardwebsite nichts anderes installiert, können Sie WSUS dorthin installieren.

12.2.3 Erstkonfiguration mit dem Assistenten

Bei der Erstkonfiguration hilft ein freundlicher Assistent, der ein weitgehend betriebsbereites System hinterlässt.

Die erste Entscheidung ist, von welchem Server die Updates abgerufen werden sollen. In den meisten Umgebungen werden das die Microsoft-Systeme (Microsoft Update) sein. Für große verteilte Umgebungen, in denen mehrere WSUS-Server arbeiten, können Sie allerdings auch eine andere Quelle angeben, sodass die Dateien nicht zweimal aus dem Internet geholt werden müssen (Abbildung 12.9).

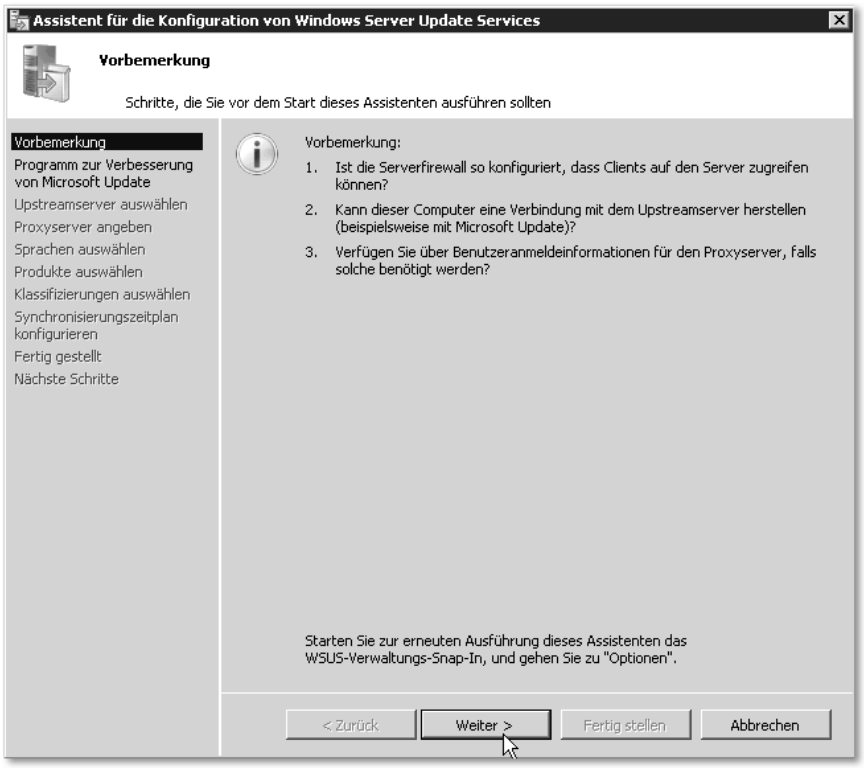


Abbildung 12.9 Vermutlich werden Sie die Updates vom Microsoft-Server beziehen. Für große Umgebungen mit mehreren WSUS-Servern gibt es auch die Möglichkeit, eine andere Quelle anzugeben.

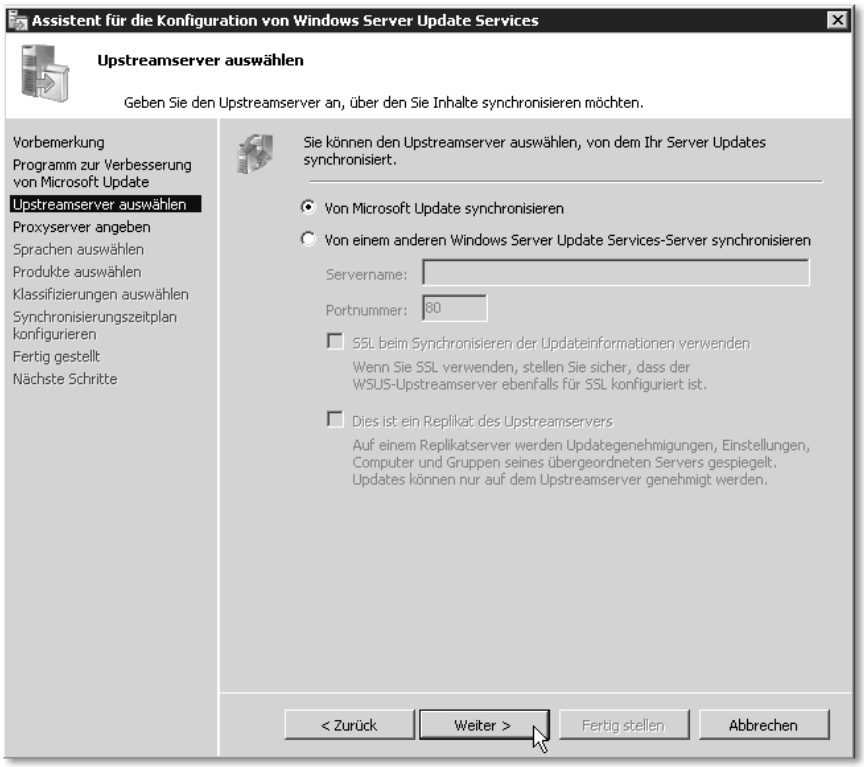


Abbildung 12.10 Der Assistent für die WSUS-Konfiguration

WSUS kann für die Verbindung natürlich einen Proxyserver verwenden; auch eine Authentifizierung an diesem ist möglich (Abbildung 12.11). Sind die Verbindungseinstellungen konfiguriert, können Sie mit einem Klick auf die Schaltfläche VERBINDUNG STARTEN die erste »Aktion« auslösen. Dies ist aber nicht nur ein simpler Verbindungstest, sondern es werden die Listen der auf der Update-Quelle zur Verfügung stehenden Sprachversionen, Produkte und Klassifizierungen geladen.

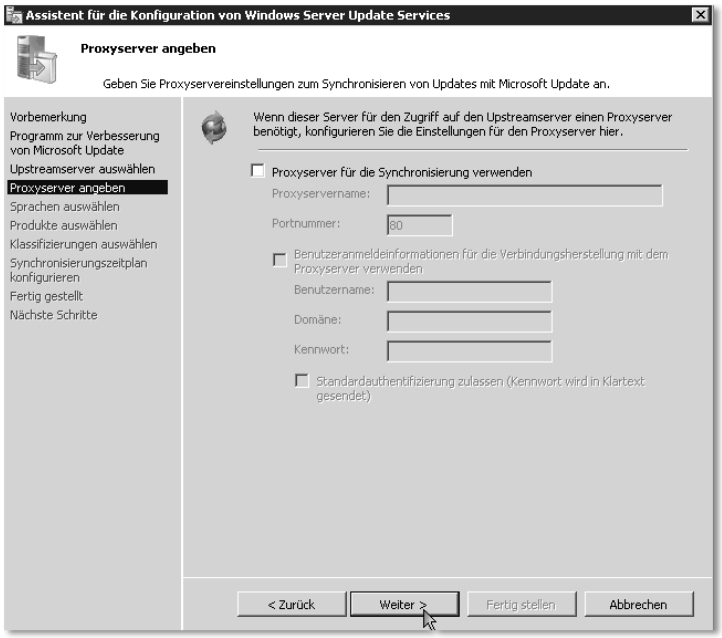


Abbildung 12.11 Nach der Konfiguration des Proxyservers (falls nötig), kann eine Verbindung aufgebaut werden. Dabei werden grundlegende Informationen über Sprachen, Produkte und Klassifizierungen abgerufen.

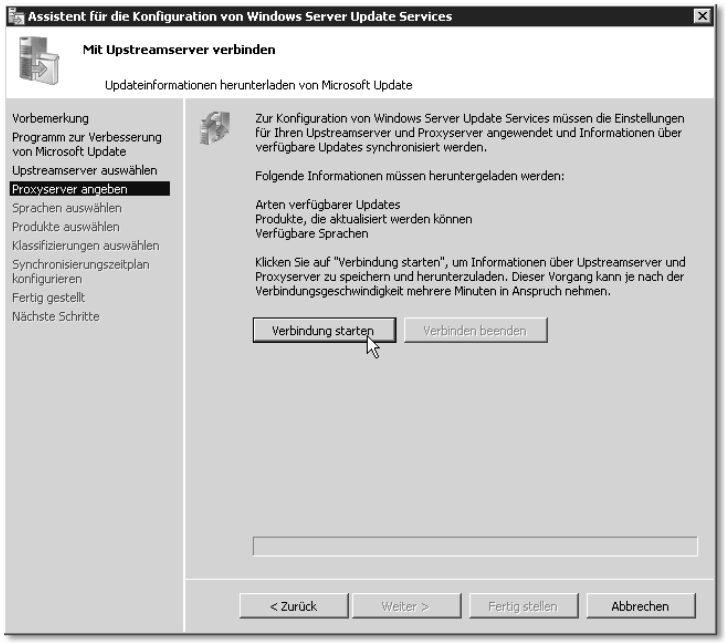


Abbildung 12.12 Hier starten Sie die Verbindung.

Auf den nächsten Dialogseiten geht es nun darum, festzulegen, welche Updates auf dem WSUS-Server zur Verfügung stehen sollen. Auch wenn es vielleicht sehr verlockend ist, »vorsichtshalber« alle Sprachversionen und Updates für alle Produkte zu beziehen, sollten Sie zumindest grob selektieren, was Sie benötigen. Wenn Sie zu großzügig auswählen, haben Sie schnell etliche 100 Gigabytes auf dem Server (Abbildung 12.13).

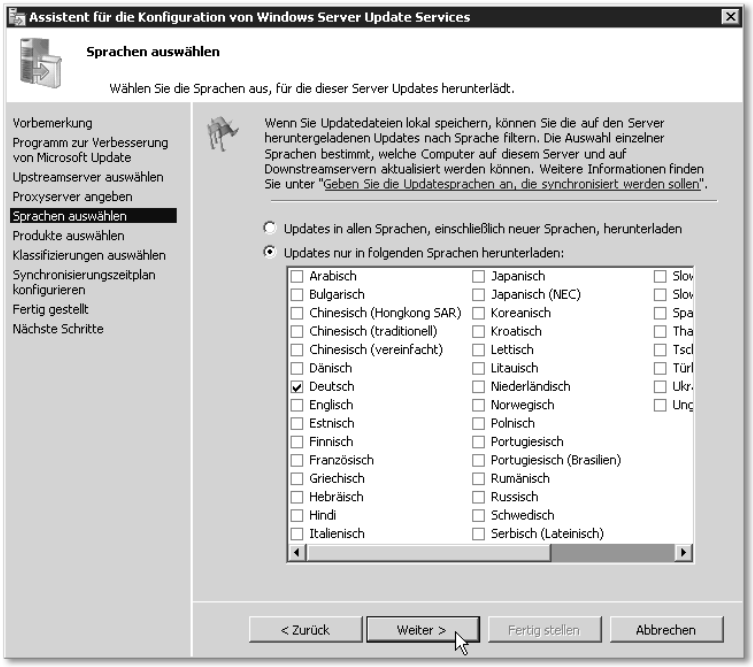


Abbildung 12.13 Geben Sie die in Ihrer Umgebung vorhandenen Sprachen an.

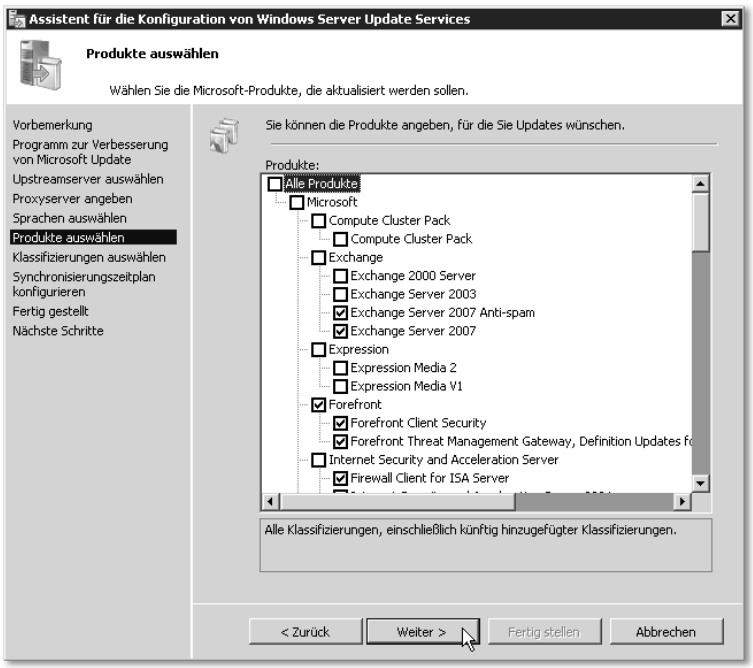


Abbildung 12.14 Wählen Sie auch die Produkte

Wenn Sie bereits WSUS einsetzen und sich fragen, wie Sie die Updates für Ihre neuen Windows 7-Clients bekommen, gibt es gute Nachrichten: Die Produktliste wird regelmäßig aktualisiert, somit taucht Windows 7 (und übrigens auch Windows Server 2008 R2) in dem Dialog aus Abbildung 12.15 auf. Diesen Dialog erreichen Sie übrigens über den Menüpunkt Optionen • Produkte und Klassifizierungen.

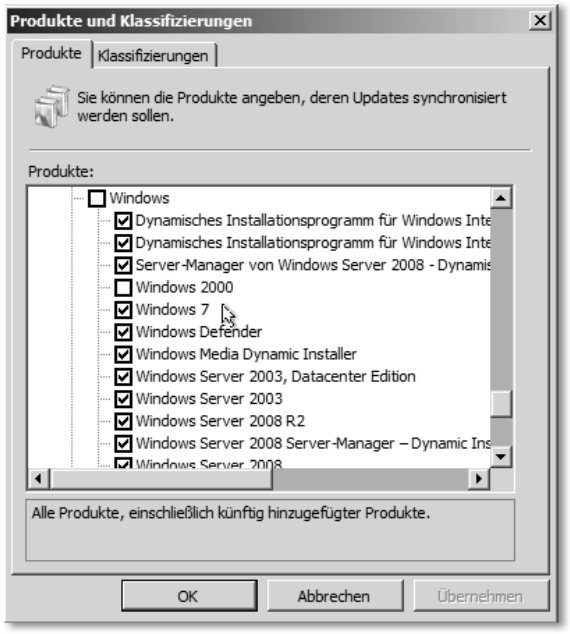


Abbildung 12.15 Windows 7 (und übrigens auch Windows Server 2008 R2) tauchen in der Produktliste auf und können ausgewählt werden.

Globalität

Übrigens: Auch wenn Sie Niederlassungen auf der ganzen Welt haben, müssen Sie entscheiden, ob Sie wirklich die Clients aus Fernost über den deutschen WSUS-Server versorgen möchten. Das kann man machen, aber wenn es sich um größere Niederlassungen handelt, dürften lokale WSUS-Server die deutlich bessere Idee sein. In diesem Fall brauchen Sie diese Sprachversionen gegebenenfalls auch nicht auf dem deutschen Server zu halten.

Bei der Auswahl der Klassifizierungen sollten Sie ebenfalls mit Augenmaß vorgehen. Wichtige Updates und Sicherheitsupdates sind natürlich »Pflichtprogramm«, allerdings sind Feature Packs und Tools im Allgemeinen Komponenten, die man meist eher nicht über WSUS installiert. Ich möchte nun zwar nicht um ein paar Gigabytes mehr oder weniger feilschen – wenn Sie viele Sprachversionen benötigen, summiert sich das. Ich mache mir übrigens weniger Sorgen um die Plattenkapazität, sondern um Ihre Internetanbindung. Wenn die ohnehin stark belastet ist, spielen »ein paar Gigabytes« eben doch eine Rolle (Abbildung 12.16).

Auf der nächsten Dialogseite geht es nun noch darum, die Synchronisierungshäufigkeit und die »Grundzeit« festzulegen (Abbildung 12.17).

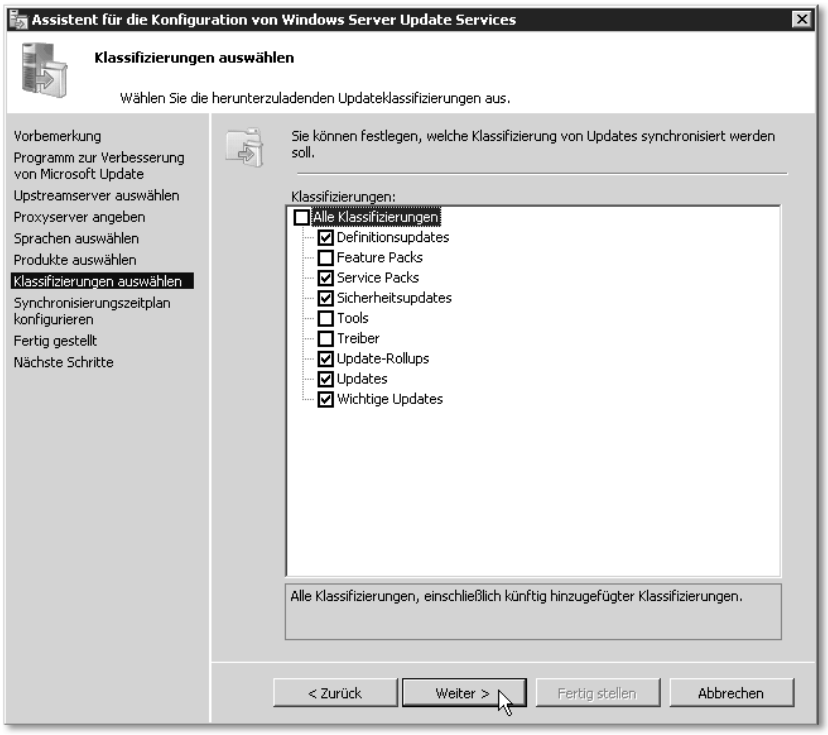


Abbildung 12.16 Wählen Sie, welche Arten von Updates heruntergeladen werden sollen.

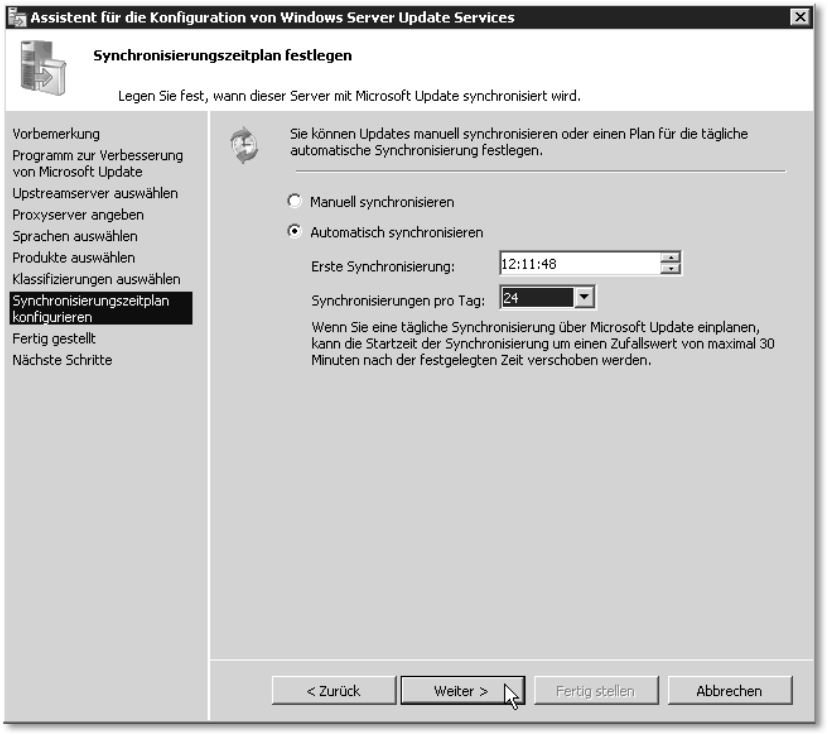


Abbildung 12.17 Legen Sie die Zeiten fest.

Tja, und dann haben Sie den Assistenten bereits durchgearbeitet. Auf der letzten Dialogseite bietet er Ihnen an, direkt die Erstsynchronisation zu beginnen. Das

macht Sinn, denn ohne Synchronisierung ist der Nutzwert der WSUS sehr begrenzt (Abbildung 12.18).

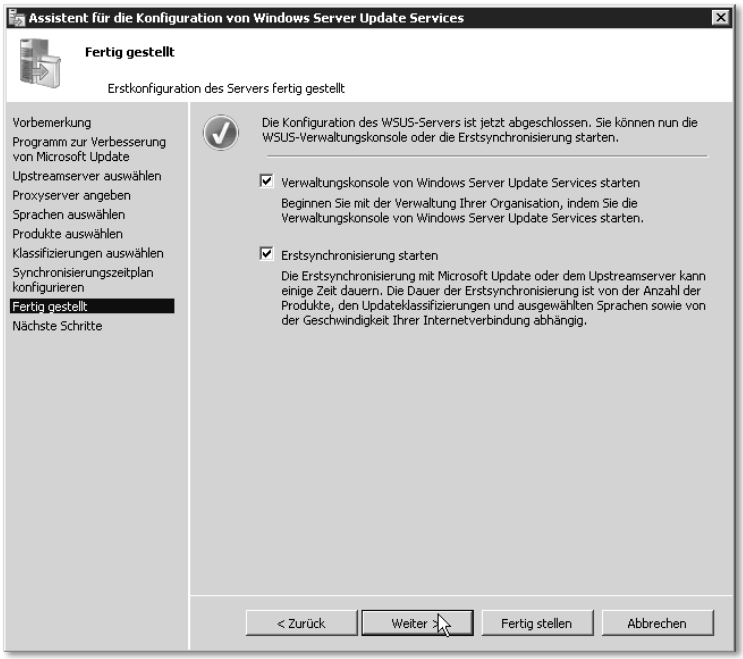


Abbildung 12.18 Auf Wunsch kann der Assistent direkt die Erstsynchronisation starten.

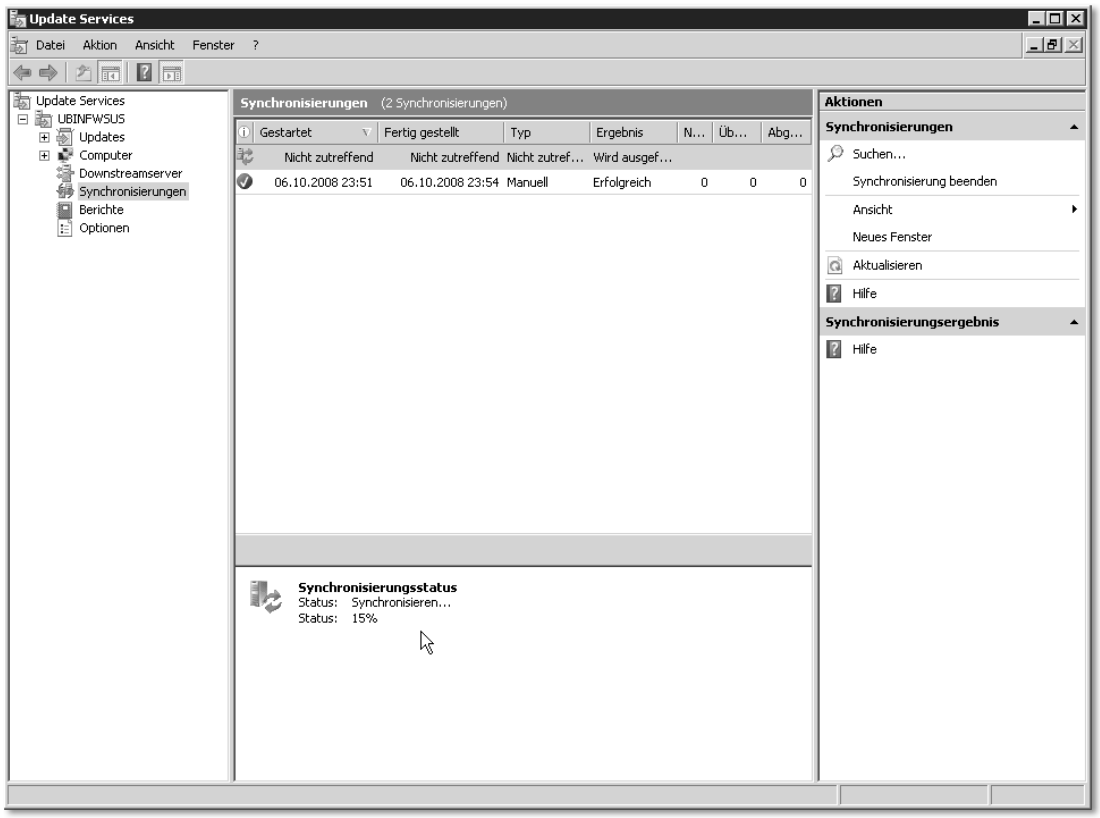


Abbildung 12.19 Hier ist in der Verwaltungskonsole von WSUS die laufende Erstsynchronisation zu sehen.

Ob die Synchronisierung läuft, können Sie übrigens in der Verwaltungskonsole erkennen: Wenn Sie den Knoten SYNCHRONISIERUNGEN wählen, sollten Sie einen laufenden Vorgang sehen (Abbildung 12.19).

12.2.4 Konfiguration und Betrieb

Auch wenn der soeben besprochene Assistent schon ein weitgehend lauffähiges System hinterlässt, gibt es in der WSUS-Verwaltungskonsole noch hinreichend viele weitere Optionen, die konfiguriert werden können. Abbildung 12.20 zeigt einen ersten Blick in die OPTIONEN der Verwaltungskonsole, wobei viele Bereiche bereits vom Assistenten abgearbeitet worden sind – aber vielleicht muss daran ja auch irgendwann etwas verändert werden.

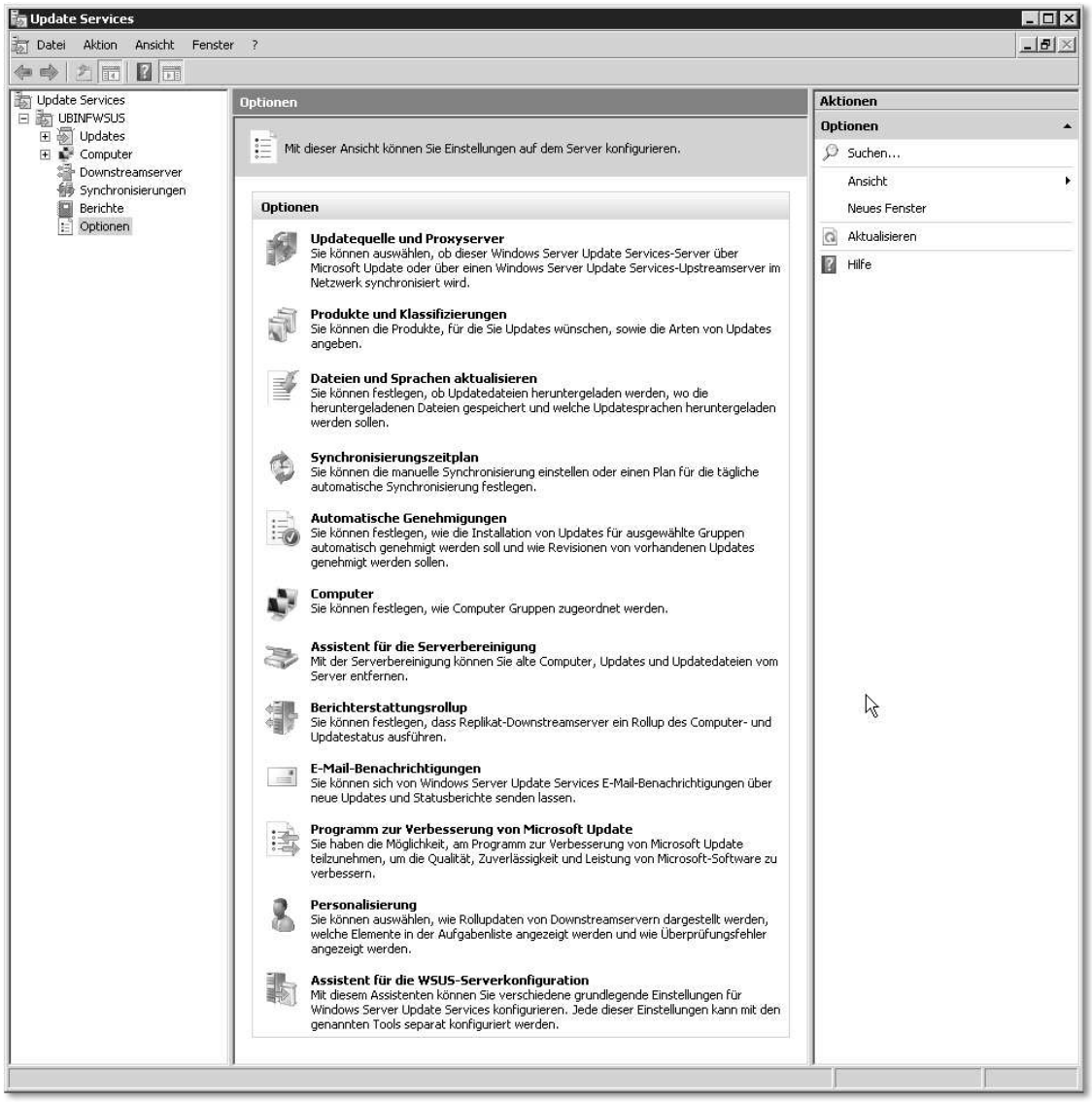


Abbildung 12.20 In der WSUS-Verwaltungskonsole gibt es immerhin ein Dutzend Optionen zu konfigurieren.

Wir werden nicht jeden Konfigurationsbereich ansehen, da diese Dialoge überwiegend selbsterklärend sind. Ich möchte Sie aber gern durch ein paar »wirklich wichtige Aspekte« führen.

Hinweis

Ein wesentlicher Konfigurationsaspekt sind die Automatischen Genehmigungen. Diese bespreche ich im weiteren Verlauf.

Die WSUS-Verwaltungskonsole finden Sie übrigens in der Gruppe Verwaltung des Startmenüs.

Gruppen anlegen, Computer zuordnen

Vermutlich werden Sie nicht alle Computer gleich behandeln wollen. Es gibt durchaus absolut unternehmenskritische Server, auf denen Sie vermutlich nicht automatisiert Updates einspielen möchten. Um dies zu steuern, gibt es zwei Ansatzpunkte:

- Mithilfe von Gruppenrichtlinien können Sie beispielsweise festlegen, ob die Computer Updates automatisch beziehen sollen und falls notwendig direkt einen Neustart durchführen.
- Über WSUS-Computergruppen steuern Sie vereinfacht gesagt, welche Computer welche Updates erhalten. Wenn Sie beispielsweise möchten, dass einige Clients das Service Pack 5 für Vista bekommen, andere aber nicht, können Sie das über die besagten WSUS-Computergruppen realisieren.

Ein Client, der sich zum ersten Mal beim WSUS-Server meldet, wird in die Gruppe Nicht zugewiesene Computer einsortiert. Wenn alle Systeme in Ihrem Netz dieselben Updates bekommen, könnten Sie sogar alle Computer dort belassen. Die meisten Administratoren möchten aber doch differenzieren können.

WSUS nicht zur Trennung

Sie benötigen diese Gruppen übrigens nicht, um Computer mit verschiedenen Betriebssystemen, Office-Versionen und dergleichen voneinander zu trennen. WSUS und der WSUS-Client sind so schlau, dass ein Windows XP-System keine Vista-Patches lädt und diese installiert (bzw. es versucht).

In einer kleinen und gleichzeitig einigermaßen simplen Umgebung könnte man beispielsweise drei Computergruppen einrichten:

- *Standardclients*: In diese Gruppe werden alle Clientsysteme einsortiert.
- *Server, Class A*: Das sind die wirklich kritischen und komplexen Systeme. Diese sollten natürlich auch aktuell gehalten werden, aber gegebenenfalls

möchten Sie die Updates für diese Systeme zuvor in einer Testumgebung ausprobieren.

- *Server, Class B*: Diese Server sind zwar ebenfalls wichtig, allerdings können zumindest kritische Patches für diese automatisch genehmigt werden.

Da ein WSUS-Client Mitglied in verschiedenen Gruppen sein kann, sind beliebig komplexe Gruppenkonzepte denkbar. Wenn mir die »WSUS-Beauftragten« von größeren Unternehmen ihre WSUS-Computergruppen-Strategie vorstellen, habe ich teilweise den Eindruck, dass es um die Realisierung der weichen Mondlandung und nicht »nur« um die Verteilung von Patches geht. Mit mehr oder weniger viel Mühe kann man das wirklich zur Perfektion treiben – Respekt!

Kommen wir zu den praktischen Dingen des Lebens (Abbildung 12.21):

- Das Anlegen von neuen WSUS-Computergruppen geschieht im Kontextmenü des Knotens ALLE COMPUTER. Sie benötigen hier nur einen gut klingenden Namen für die neue Gruppe.
- Um einen Computer einer oder mehrerer Gruppen zuzuordnen, wählen Sie den Menüpunkt MITGLIEDSCHAFT ÄNDERN des Kontextmenüs.

Hinweis

Die Gruppe oder Gruppen, in die ein Computer »einsortiert« werden soll, kann bzw. können alternativ auch in den Gruppenrichtlinien konfiguriert werden.

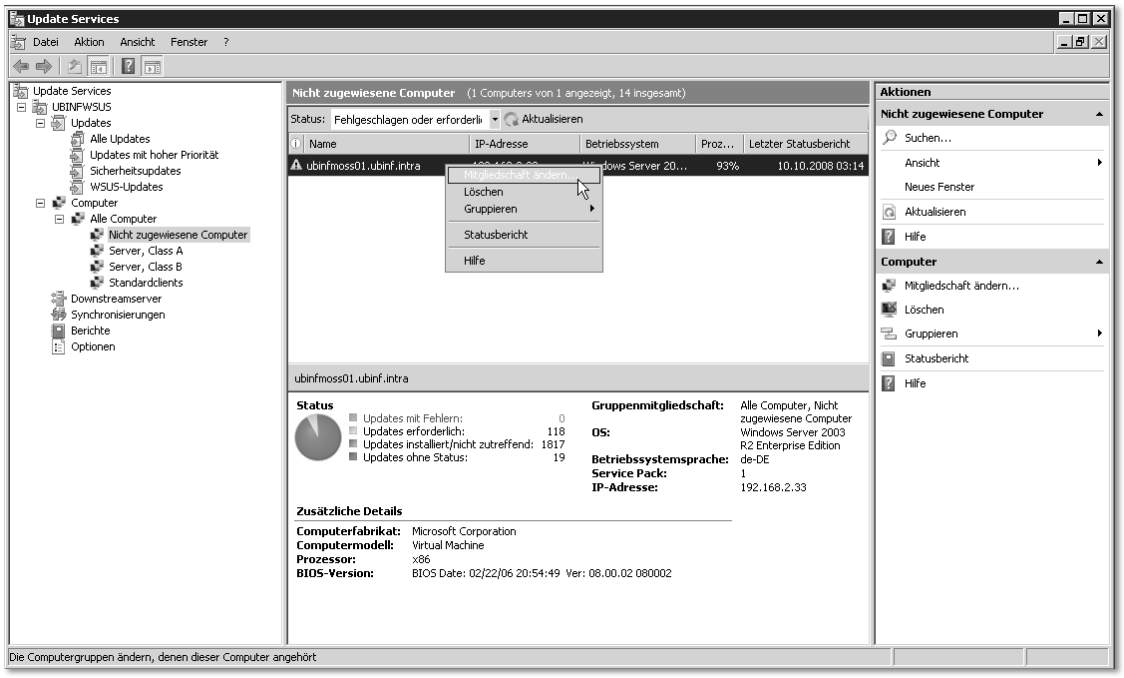


Abbildung 12.21 Ein neuer Computer wird standardmäßig in die Gruppe »Nicht zugewiesene Computer« einsortiert.

Computer überwachen

Wie ich weiter vorn erwähnt habe, basiert WSUS darauf, dass sich der Client regelmäßig beim Server »meldet«, um Updates zu beziehen. Falls der Client das längere Zeit nicht tut, kann es dafür zwei Gründe geben:

- Der Computer ist länger nicht eingeschaltet worden, beispielsweise weil der Besitzer im Urlaub oder dergleichen ist. Das kann natürlich für Server nicht zutreffen (schlecht wäre, wenn ein Server nicht mehr läuft, wenn der Admin im Urlaub ist, was aber oft genug vorkommt).
- Der WSUS-Client hat ein irgendwie geartetes Problem und kann nicht (mehr) mit dem Server kommunizieren.

In der Liste der Computer können Sie unter anderem erkennen, wann ein WSUS-Client sich das letzte Mal beim Server gemeldet hat (Abbildung 12.22). Die Liste kann beispielsweise nach dem Datum sortiert sein, sodass Sie sich relativ einfach einen Überblick verschaffen können.

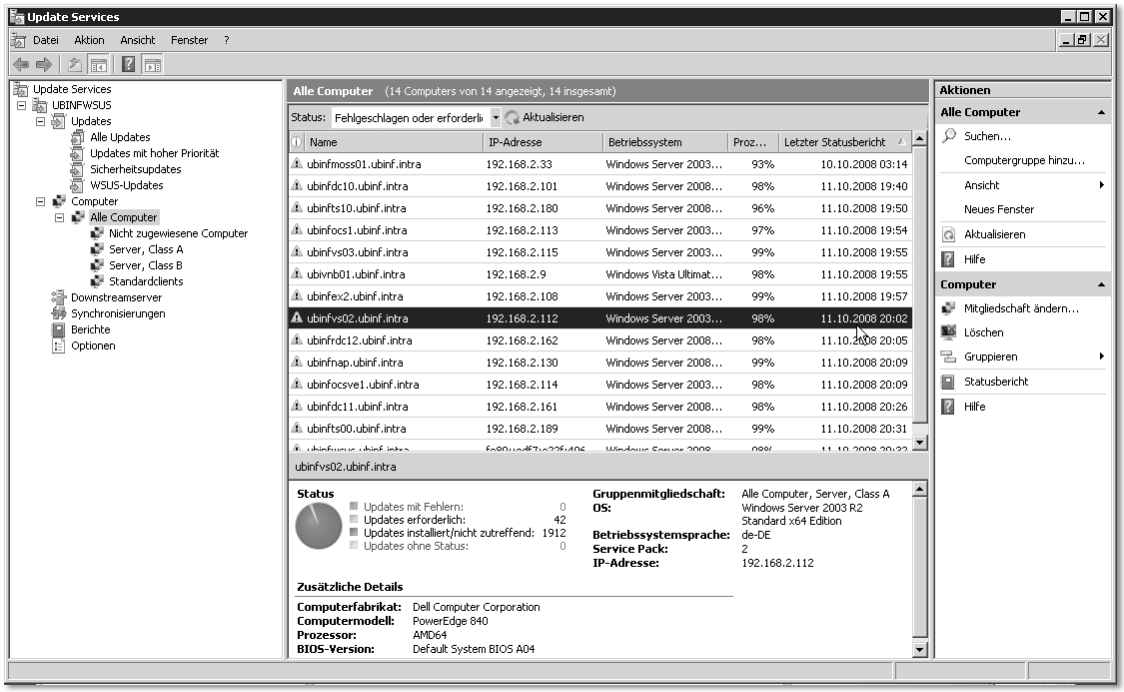


Abbildung 12.22 Hier bekommen Sie eine Übersicht über alle Computer. Wenn sich ein System lange nicht gemeldet oder Updates mit Fehlern hat, besteht Handlungsbedarf.

Synchronisierungen überwachen

Ein weiterer Aspekt, den Sie regelmäßig überprüfen sollten, ist die Durchführung bzw. der Erfolg der Synchronisierungen mit der Update-Quelle. Die in Abbildung 12.23 gezeigte Liste gibt einen Überblick über den Erfolg, den Zeitpunkt und die Anzahl der gefundenen Updates.

Im Kontextmenü jedes Eintrags findet sich der Menüpunkt STATUSBERICHT. Dort erhalten Sie Details zum Vorgang, beispielsweise welche neuen Updates gekommen sind und welche vorhandenen Updates dadurch ersetzt wurden.

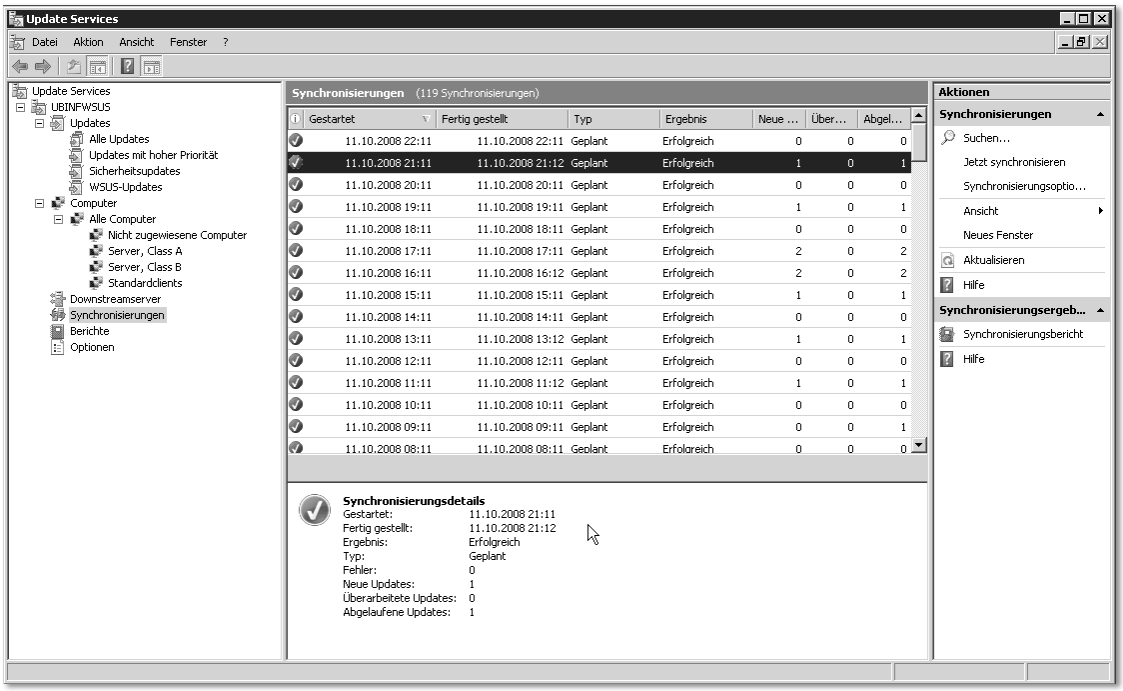


Abbildung 12.23 Es kann nicht schaden, gelegentlich die Synchronisierungsvorgänge zu überwachen.

12.2.5 Updates genehmigen

Auch wenn Sie bis hierhin alles perfekt konfiguriert haben, wird kein einziger Patch auf einen WSUS-Client gelangen. Der Grund ist, dass der WSUS-Server kein Update an einen WSUS-Client sendet, wenn es nicht genehmigt (d. h. freigegeben) ist. Genauer gesagt muss ein Update für jede einzelne Computergruppe genehmigt werden.

Da realistisch betrachtet kaum ein Administrator Zeit dafür haben wird, jedes einzelne Update zu kontrollieren und für die diversen angelegten Computergruppen zu genehmigen, können Sie sich von der AUTOMATISCHEN GENEHMIGUNG helfen lassen.

Automatische Genehmigung konfigurieren

In der Praxis arbeiten die meisten Administratoren mit automatischen Genehmigungen. Den Konfigurationsdialog rufen Sie in der Verwaltungskonsole über OPTIONEN • AUTOMATISCHE GENEHMIGUNGEN auf.

Standardmäßig vorhanden ist die Automatische Standardgenehmigungsregel, die besagt, dass Updates, die als Sicherheitsupdate oder Wichtiges Update klassifiziert sind, für Alle Computer genehmigt werden (Abbildung 12.24).

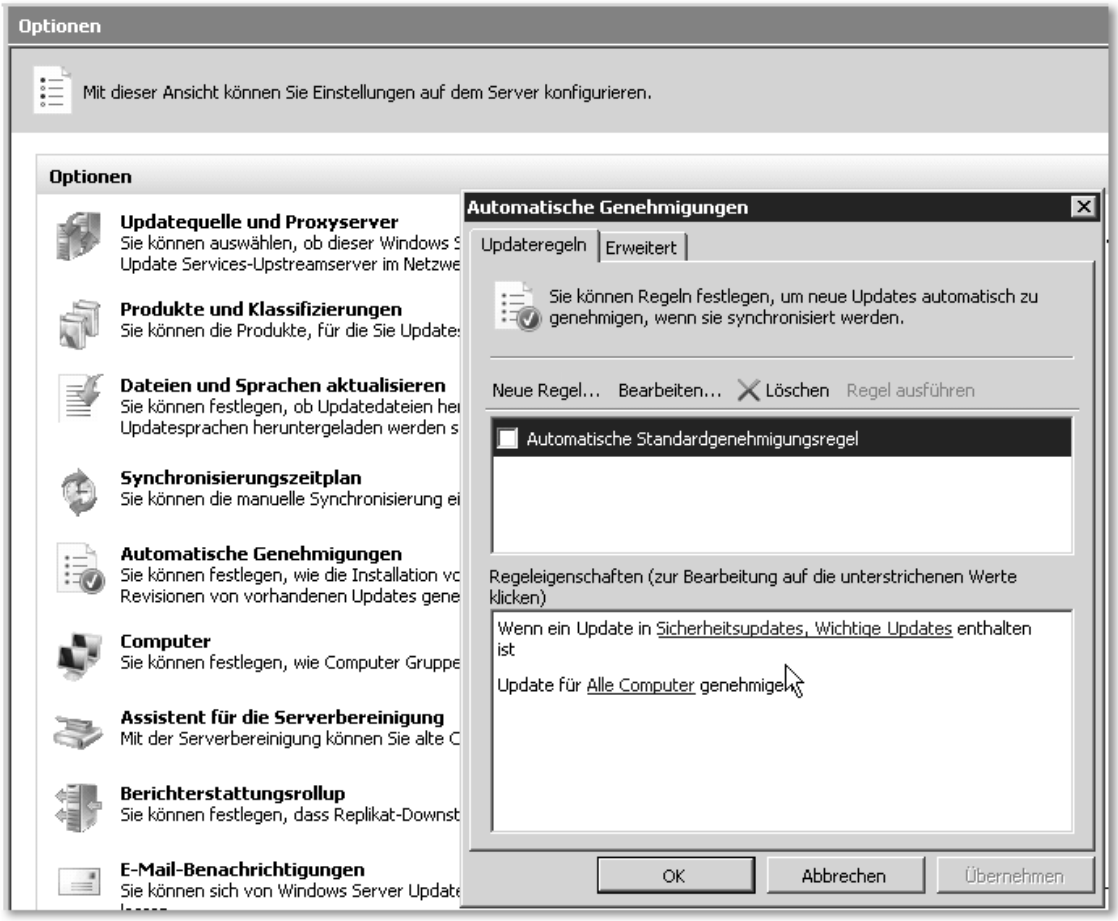


Abbildung 12.24 Sie können beliebig viele Regeln anlegen. Die »Automatische Standardgenehmigungsregel« ist bereits vorhanden, allerdings deaktiviert.

Sie können diese Regel bei Bedarf modifizieren. Bevor aber irgendetwas passiert, muss sie zunächst aktiviert werden.

Wenn Sie eine Regel erstellt und aktiviert haben, wirkt sie für neu eingehende Updates. Sie können die Regel sofort auf alle vorhandenen Updates anwenden, wenn Sie die Schaltfläche Regel ausführen anklicken (Abbildung 12.25).

Auf der Registerkarte Erweitert finden Sie einige zusätzliche Optionen:

- Es kann konfiguriert werden, dass Updates, die den WSUS-Server betreffen, automatisch genehmigt werden.
- Weiterhin gibt es zwei Einstellungen, die den Umgang mit Updateversionen betreffen.

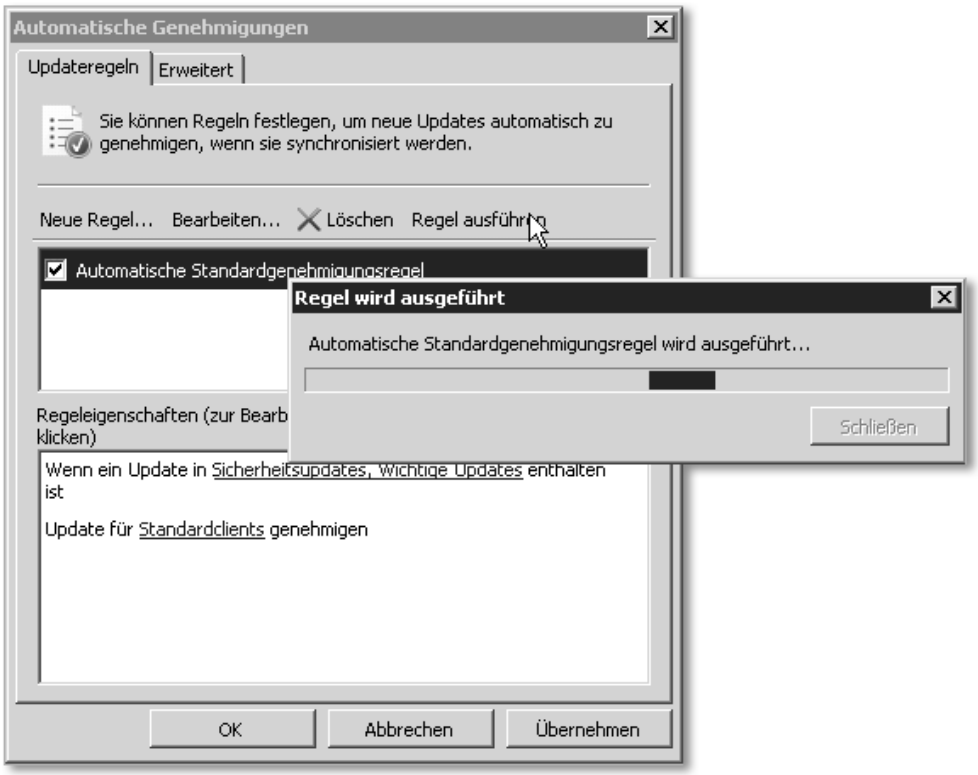


Abbildung 12.25 Eine Genehmigungsregel kann sofort ausgeführt werden.

Beim Umgang mit automatischen Genehmigungen gehen die meisten Unternehmen übrigens wie folgt vor:

- Updates, die als SICHERHEITSUPDATE oder WICHTIGES UPDATE klassifiziert sind, werden automatisch genehmigt – zumindest für Clients.
- Service Packs werden im Allgemeinen nicht automatisch genehmigt, sondern nach diversen Tests manuell genehmigt.
- Bei kritischen Servern empfiehlt es sich, gegebenenfalls zuvor in der Testumgebung die »Verträglichkeit« von Updates zu untersuchen.

  Also ist manuelles Genehmigen angesagt.

Updates manuell genehmigen

Unterhalb des Knotens UPDATES befinden sich vier verschiedene Kategorien. In der Kopfzeile der angezeigten Liste sind Filter vorhanden. Sie können nach dem Genehmigungsstatus (z. B. NICHT GENEHMIGT) und/oder dem Status (z. B. FEHLGESCHLAGEN oder ERFORDERLICH) filtern (Abbildung 12.26).

In dem Statusbereich (am unteren Rand des Fensters) wird ein Kurzüberblick zu dem selektierten Update gezeigt. Wenn Sie mehr Details sehen möchten, bei-

spielsweise die Server, für die das Update benötigt wird oder würde, wählen Sie den Menüpunkt STATUSBERICHT aus dem Kontextmenü des Eintrags (Abbildung 12.27).

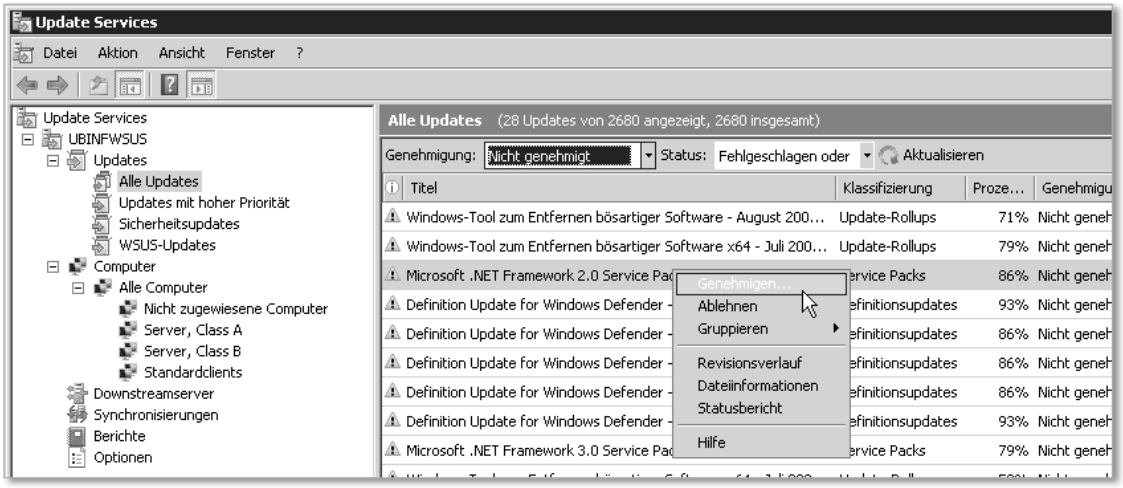


Abbildung 12.26 Die angezeigten Updates können gefiltert werden. Im Kontextmenü können Sie beispielsweise »Genehmigen« oder »Ablehnen« wählen.

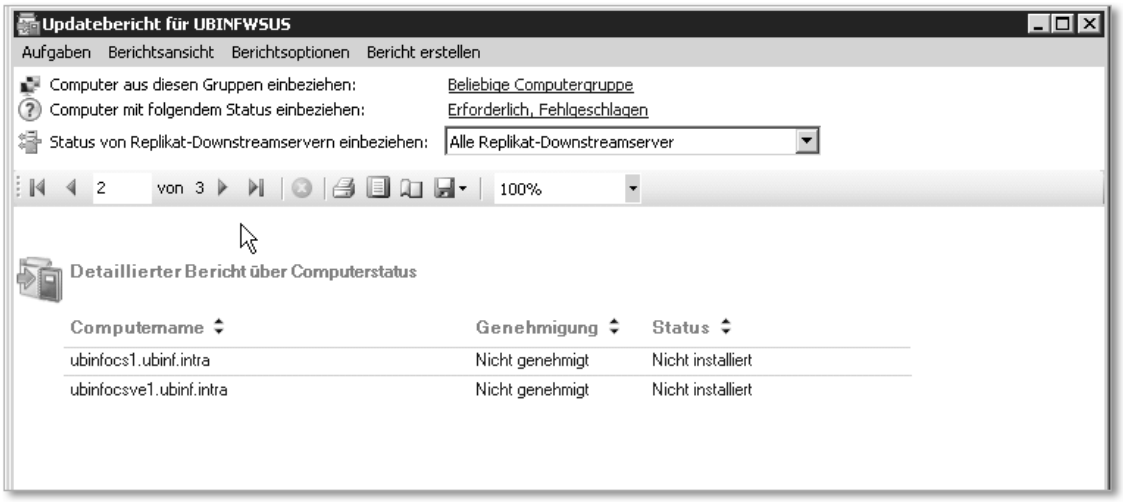


Abbildung 12.27 Im Statusbericht können Sie beispielsweise abfragen, welche Computer das Update benötigen.

Wenn Sie den Menüpunkt GENEHMIGEN aufrufen, erscheint der Dialog aus Abbildung 12.28, in dem Sie die Genehmigung für die einzelnen Gruppen steuern können. Wenn die WSUS-Clients einer solchen Gruppe das nächste Mal die Liste der einzuspielenden Updates abfragen, erhalten Sie dieses Update.

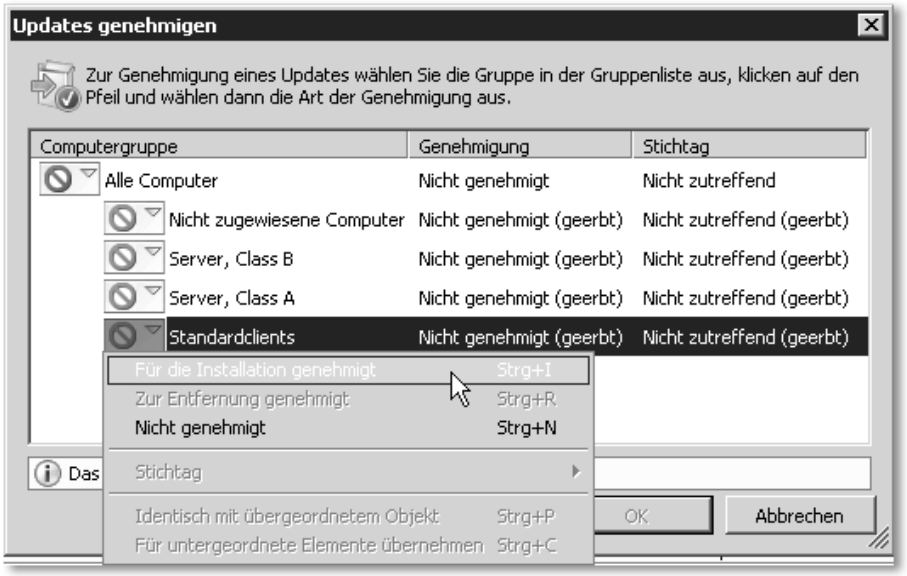


Abbildung 12.28 Das Update kann für »Alle Computer« oder ausgewählte Gruppen genehmigt werden.

12.2.6 Gruppenrichtlinie konfigurieren

Da die WSUS-Clients über Gruppenrichtlinien konfiguriert werden, ist es höchste Zeit, diesen Aspekt genauer zu betrachten.

Die Einstellungen finden Sie im Gruppenrichtlinienverwaltungs-Editor unter COMPUTERKONFIGURATION • RICHTLINIEN • ADMINISTRATIVE VORLAGEN • WINDOWS-KOMPONENTEN • WINDOWS UPDATE. Dort gibt es immerhin 15 Einstellungen, mit denen Sie das Verhalten recht granular steuern können. Abbildung 12.29 zeigt die Einstellung INTERNEN PFAD FÜR DEN MICROSOFT UPDATEDIENST ANGEBEN, also den Verweis auf Ihren WSUS-Server. Wenn Sie mehrere WSUS-Server an verschiedenen Standorten haben, ist das übrigens eine Einstellung, die sehr gut in einer Standortrichtlinie aufgehoben ist.

Sehr wichtig ist übrigens auch die in Abbildung 12.30 gezeigte Einstellung, die das automatische Einspielen von Updates regelt.

Die Einstellungen sind im Gruppenrichtlinienverwaltungs-Editor recht ausführlich beschrieben, sodass eine weitere Erläuterung an dieser Stelle nicht notwendig ist. Sie werden vermutlich ein wenig experimentieren müssen, bis Sie Ihre »individuellen Optimaleinstellungen« gefunden haben.

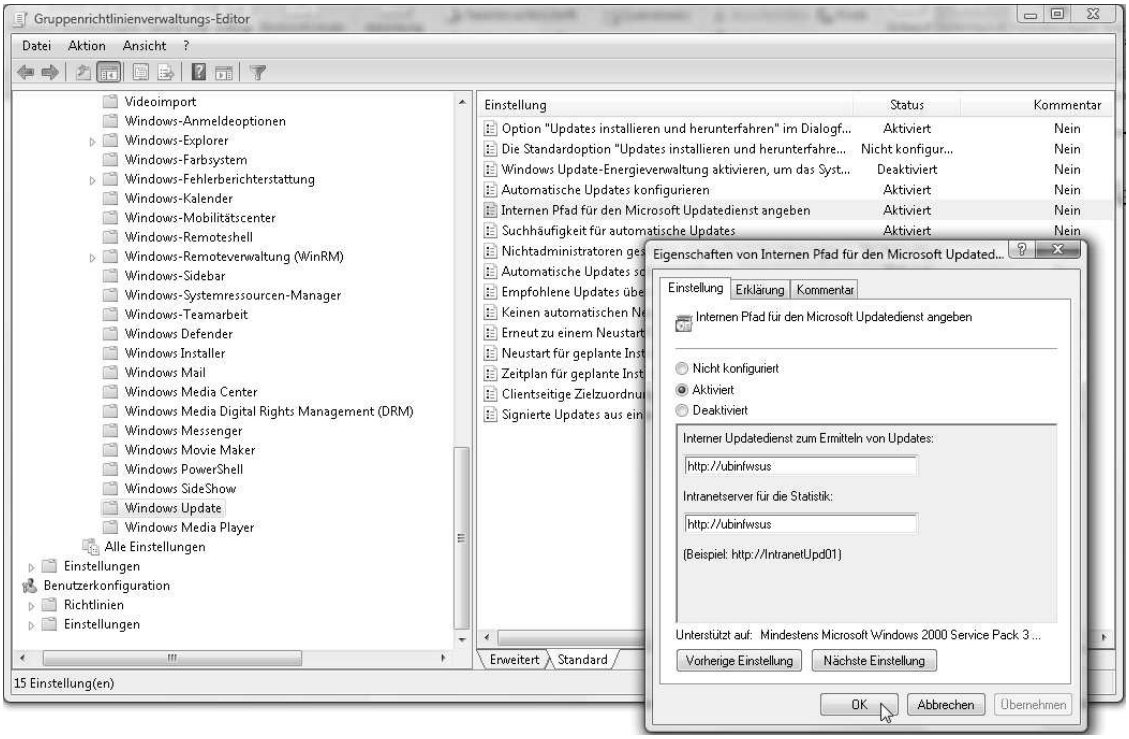


Abbildung 12.29 Für WSUS gibt es diverse Gruppenrichtlinien-Einstellungen. Hier wird der zu verwendende WSUS-Server angegeben.

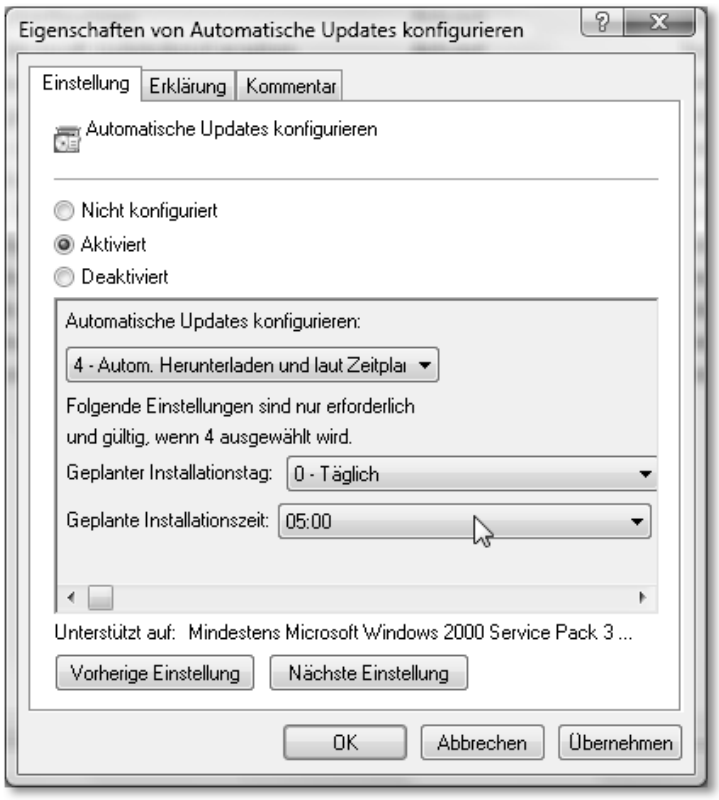


Abbildung 12.30 »Automatische Updates konfigurieren« ist eine besonders wichtige Einstellung: Hier legen Sie fest, ob und wann Updates automatisch eingespielt werden sollen.

12.2.7 Ein kurzer Blick auf den WSUS-Client

Die Betriebssysteme ab Windows 2000 SP3 verfügen standardmäßig über einen WSUS-Client. Abgesehen von dem kleinen Eintrag in der Menüleiste ist von ihm aber im Normalfall wenig zu sehen. In der Windows 7-Systemsteuerung findet sich ein Überblick über den aktuellen Status, was auf Abbildung 12.31 gezeigt ist; zu dem Zeitpunkt, als ich den Screenshot erstellt habe, hat es übrigens schlicht und ergreifend noch keine Updates für Windows 7 gegeben.

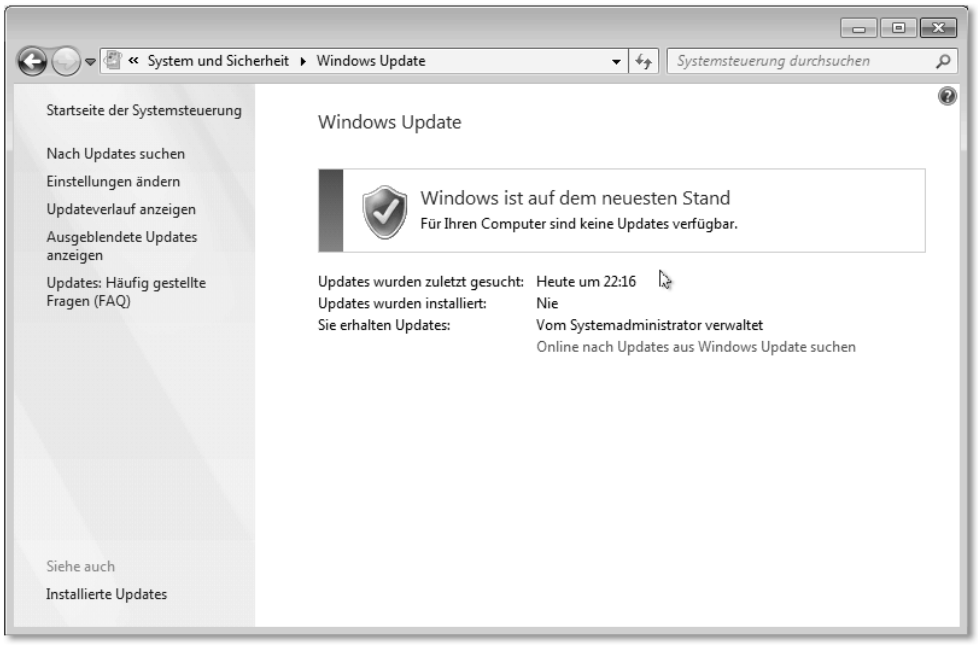


Abbildung 12.31 In der Windows 7-Systemsteuerung wird der Status von Windows Update angezeigt.

Auf Abbildung 12.32 sehen Sie die Konfiguration des Windows Update-Clients. Die über Gruppenrichtlinien konfigurierten Optionen sind allerdings für die lokale Konfiguration gesperrt – dies ist auch im Kopf des Dialogs an der Meldung Einige Einstellungen werden vom Systemadministrator verwaltet zu erkennen.

Hinweis

Außerdem besteht die Möglichkeit, einige Befehle mittels des Kommandozeilenprogramms `wuauclt` abzusetzen. Mit `wuauclt /detectnow` können Sie beispielsweise einen Überprüfungsvorgang einleiten, und `wuauclt /reportnow` sendet den aktuellen Status an den WSUS-Server.

Ich habe zuvor immer behauptet, dass die Kommunikation zwischen WSUS-Client und -Server über das HTTP-Protokoll abläuft. Den »Beweis« sehen Sie in einem Netzwerkmonitor-Mitschnitt (Abbildung 12.33). In der Abbildung sehen Sie übrigens den Beginn des »Nach Updates suchen«-Vorgangs.

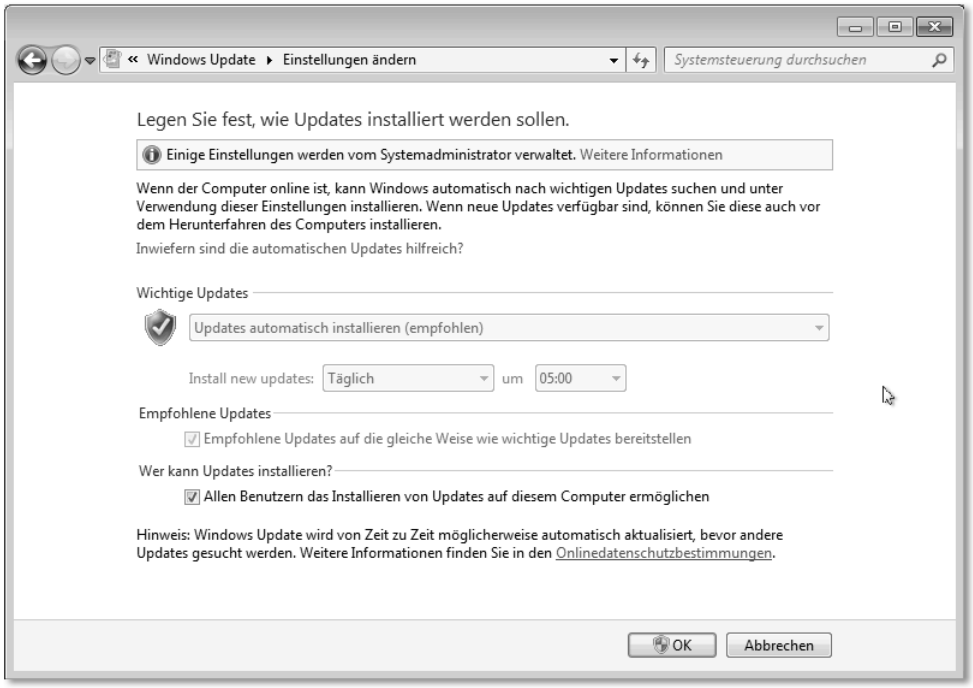


Abbildung 12.32 Konfigurationsänderungen sind nicht möglich, wenn die Einstellungen über Gruppenrichtlinien konfiguriert sind.

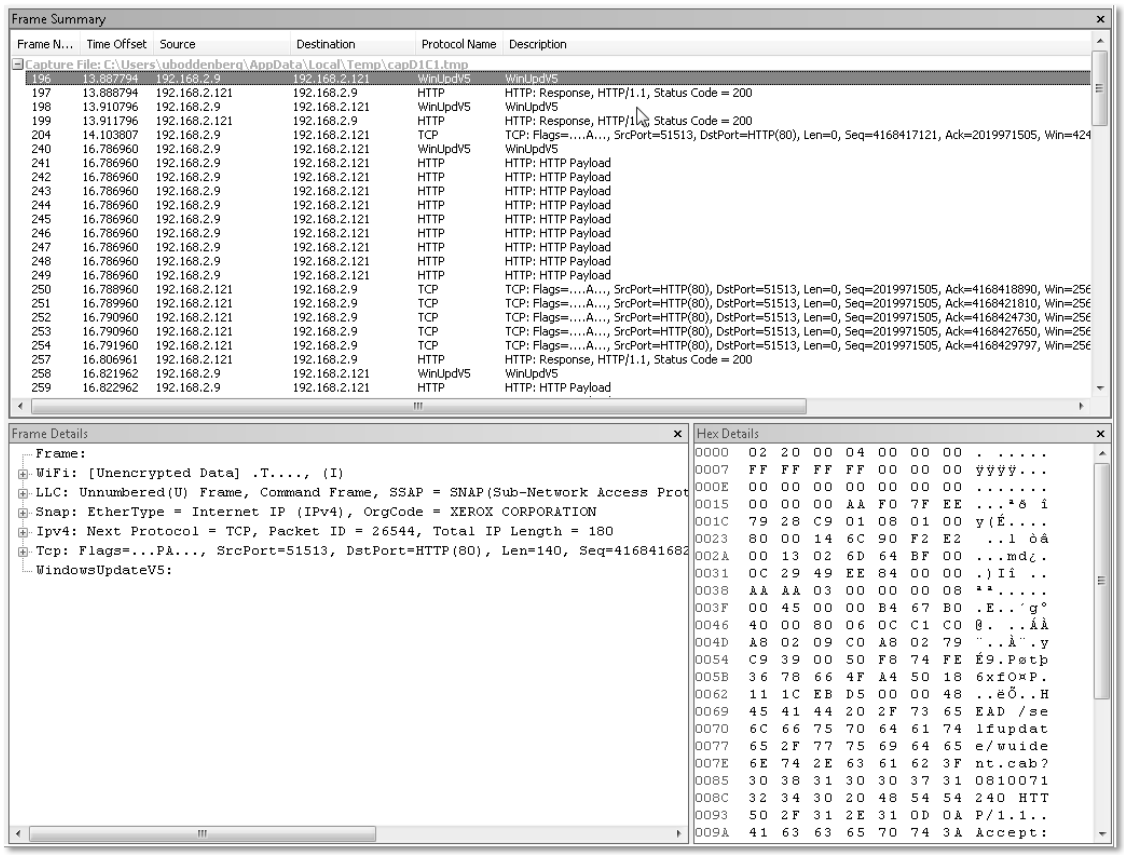


Abbildung 12.33 Im Netzwerkmonitor können Sie sich überzeugen, dass die Kommunikation zwischen WSUS-Server und -Client über HTTP abläuft.

12.2.8 Mit Berichten arbeiten

Wenn Sie das *Report Viewer Distributable*-Paket installiert haben (siehe Installationsvoraussetzungen in Abschnitt 12.2.2), können Sie diverse Berichte aufrufen. Unterhalb des Knotens BERICHTE finden Sie diverse allgemeine Reports. Die Beschreibung lässt bereits vermuten, worum es dort jeweils geht (Abbildung 12.30).

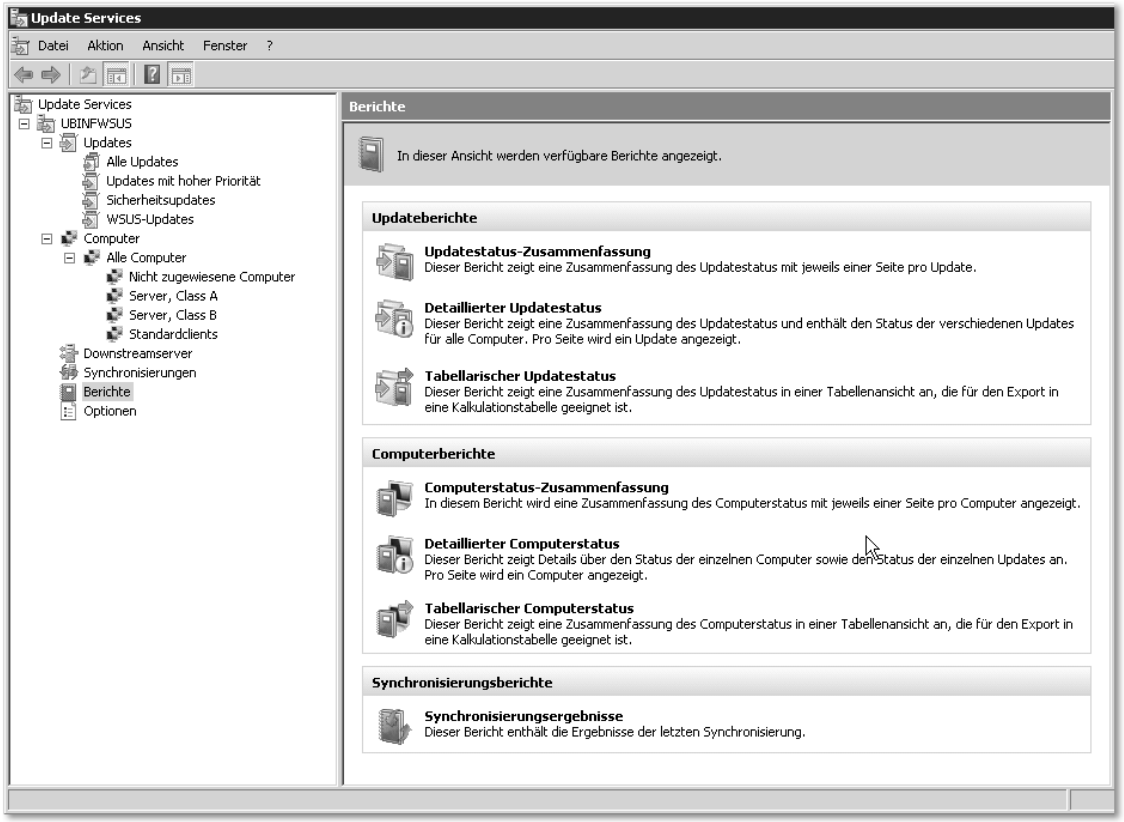


Abbildung 12.34 Mithilfe der Berichte können Sie diverse Aspekte ermitteln.

An verschiedenen Stellen der Verwaltungskonsole können Sie »spezielle« Berichte aufrufen, beispielsweise im Kontextmenü eines Updates (siehe auch Abbildung 12.36) oder eines Computers. Der Statusbericht des Computers ist in Abbildung 12.35 zu sehen. Neben einigen grundlegenden technischen Daten ist die STATUSZUSAMMENFASSUNG von besonderem Interesse. In diesem Fall ist zwar alles grün, allerdings wurden 7 Updates nicht installiert.

Wenn Sie mehr Details brauchen und wissen möchten, welche Updates nicht installiert werden können, wechseln Sie auf die zweite Seite des Berichts. Dort werden die Updates nebst Genehmigungs- und Installationsstatus gezeigt. In diesem Fall wurden die Updates also deswegen nicht installiert, weil sie schlicht und ergreifend nicht genehmigt sind – auch einleuchtend (Abbildung 12.36).

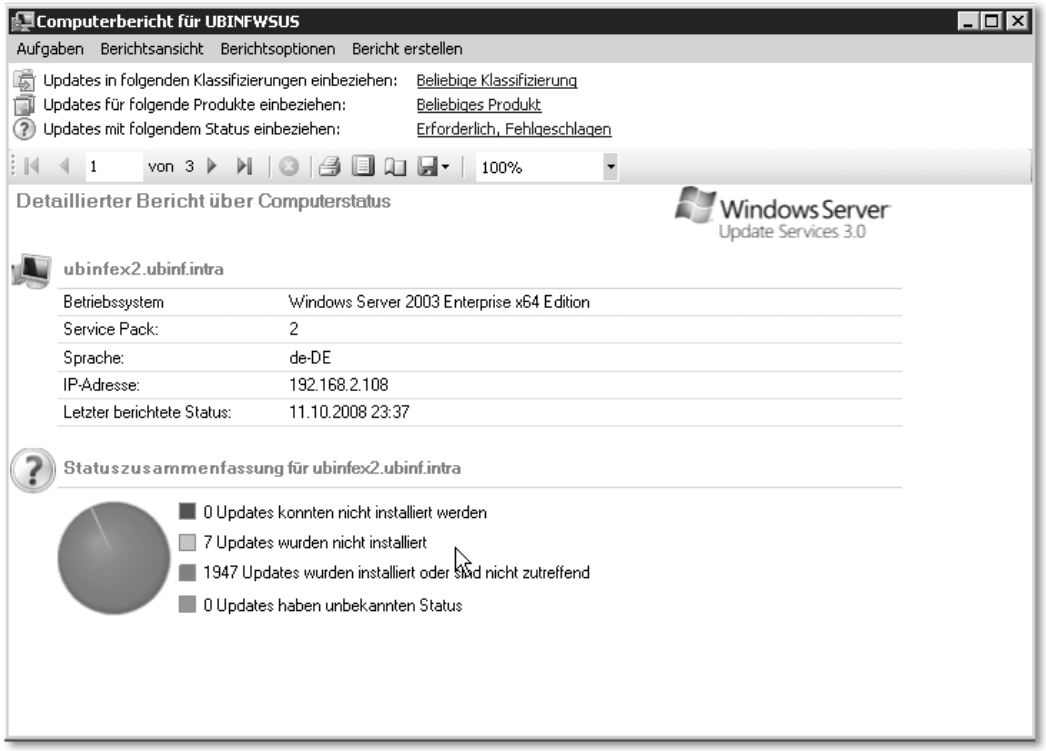


Abbildung 12.35 Diesen Detailbericht können Sie in der Verwaltungskonsole aus dem Kontextmenü des WSUS-Clients aufrufen.

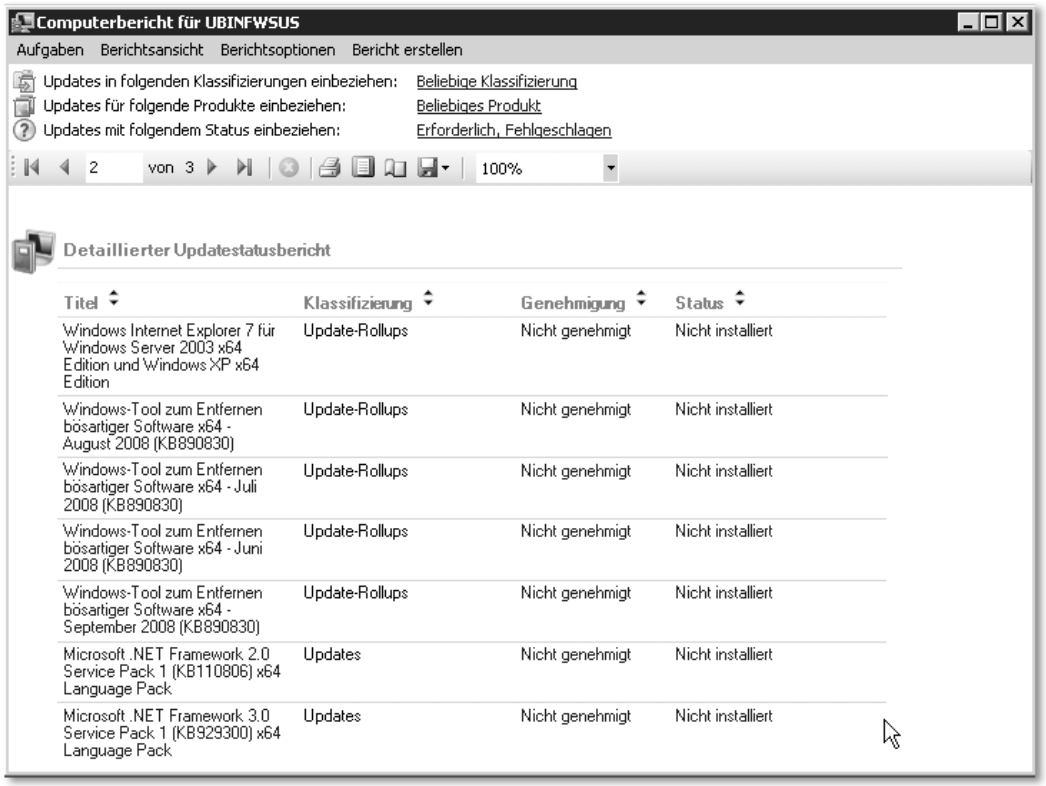


Abbildung 12.36 Nicht uninteressant ist auch der Updatestatusbericht. Sie können dort auch herausfinden, warum ein Update noch nicht installiert worden ist (»Nicht genehmigt«).

12.3 Netzwerkrichtlinien- und Zugriffsdienste

Unter dem Stichwort *Netzwerkrichtlinien- und Zugriffsdienste* sind diverse Technologien zu finden, die helfen, den Zugang zum Netz einerseits zu realisieren (z. B. *Remote Access Service*), aber auch abzusichern (z. B. *Network Policy Server*). Bei *Netzwerkrichtlinien- und Zugriffsdienste* handelt es sich um eine Rolle des Windows Server 2008, deren Komponenten über die entsprechende Funktion des Server-Managers installiert werden. Diese Dienste sind ein weiteres schönes Beispiel für die Zusammenarbeit von Windows 7 und Windows Server 2008.

Abbildung 12.37 zeigt die Komponenten, die Sie im Installationsdialog auswählen können.

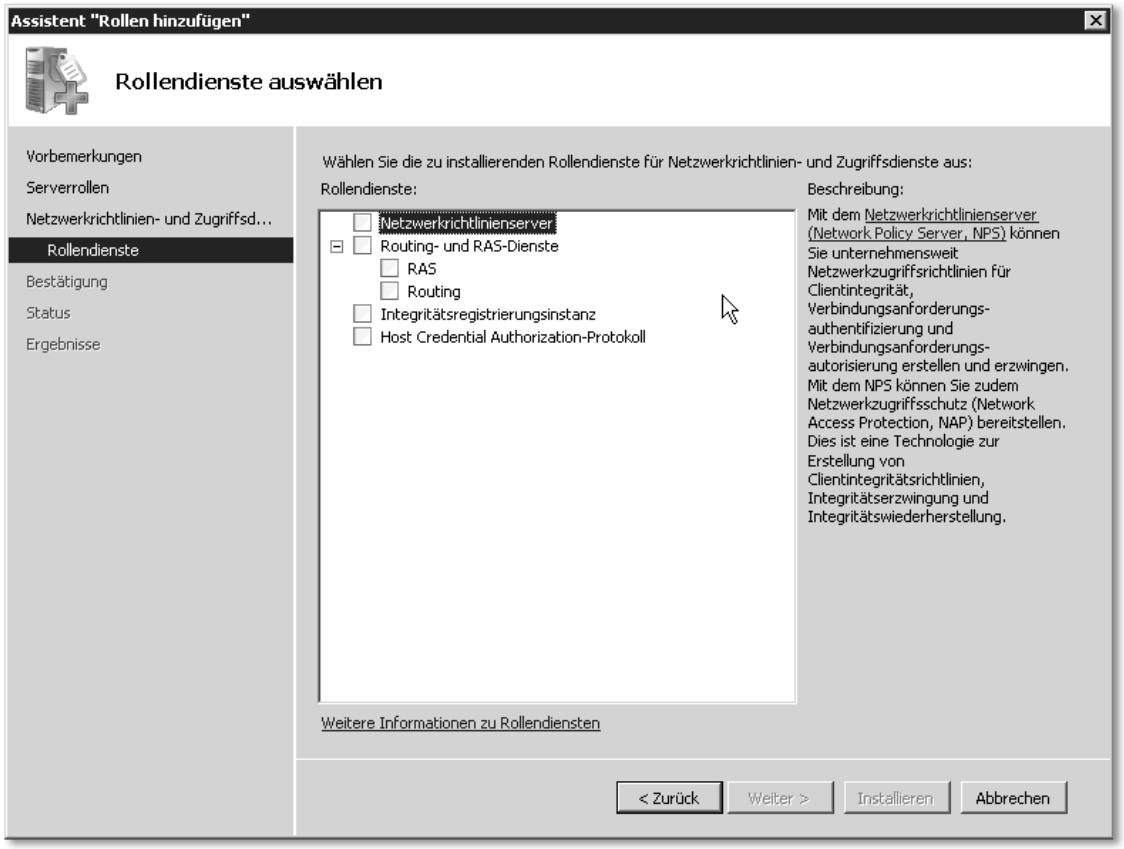


Abbildung 12.37 Diese Komponenten gehören zur Rolle »Netzwerkrichtlinien- und Zugriffsdienste«.

- NETZWERKRICHTLINIENSERVER: Mit dieser Komponente können Sie organisationsweise Regeln definieren und durchsetzen, mit denen der Zugriff auf das Netz gesichert werden kann.
- ROUTING- UND RAS-DIENSTE: Mit diesen Komponenten können VPN- und Einwahlverbindungen realisiert werden.

- Integritätsregistrierungsinstanz: Diese Komponente überprüft den Zustand des Clients und stellt ein Zertifikat aus, das auf der ermittelten Integrität des Clients beasiert. Diese wird benötigt, wenn NAP in Verbindung mit IPSec eingesetzt werden soll.
- Host Credential Authorization-Protokoll: Diese Komponente dient zur Interaktion mit dem *Cisco Access Control Server*.

Hinweis

In diesem Abschnitt werden wir uns mit den Netzwerkrichtlinien beschäftigen, die auch als *Network Access Protection* (NAP) bekannt sind.

Ich werde im weiteren Verlauf des Kapitels die Kurzbezeichnung NAP verwenden.

12.3.1 Wie funktioniert NAP?

Ich möchte an dieser Stelle NAP nicht bis ins letzte theoretische Detail diskutieren, sondern Ihnen eine grundsätzliche Idee von der Funktionsweise geben. Abbildung 12.38 zeigt eine stark vereinfachte Darstellung:

- Wenn ein Client auf das Netz zugreifen möchte, muss er sich zunächst mit einem der *NAP Enforcement Points* (NAP-Erzwingungspunkte) auseinandersetzen. NAP-Unterstützung gibt es für verschiedene Netzwerkverbindungsmethoden, beispielsweise DHCP, VPN, Terminaldienstegateway, IPSec und auch für drahtlose und drahtgebundene 802.1X-Geräte (z. B. Switches, WLAN-Access-Points).
- An dem Erzwingungspunkt wird der »Gesundheitszustand« des Clients überprüft. Beispielsweise wird abgefragt, ob aktuelle Virenpattern vorhanden sind, eine Firewall für alle Netzwerkverbindungen aktiv ist und die aktuellen Patches eingespielt worden sind.

  Technisch funktioniert das so, dass auf den Clients ein Stück Software, nämlich der NAP-Agent mit diversen Unterkomponenten, vorhanden sein muss, der diese Daten einsammelt und das Ergebnis an den jeweiligen Erzwingungspunkt (z. B. den DHCP-Server) übermittelt.
- Das Ergebnis der »Gesundheitsprüfung« sendet der Erzwingungspunkt an den Netzwerkrichtlinienserver, der anhand der dort konfigurierten Richtlinien entscheidet, ob dem Client Zugriff gewährt werden soll – oder eben nicht.
- Wird dem Client Zugriff gewährt, kann er auf die produktiven Server zugreifen.
- Wird dem Client kein Zugriff gewährt, weil er nicht alle Bedingungen für einen »gesunden Client« erfüllt, erhält er keinen Zugriff auf die produktiven

Server. Stattdessen erhält er Zugriff auf einen oder mehrere Wartungsserver. Die Idee ist, dass er sich von diesen Wartungsservern die fehlenden Dateien (also insbesondere Virenpattern, Patches etc.) holen kann. Nach dem Updatevorgang wird er dann nochmals einer Prüfung unterzogen, die er dann hoffentlich besteht.

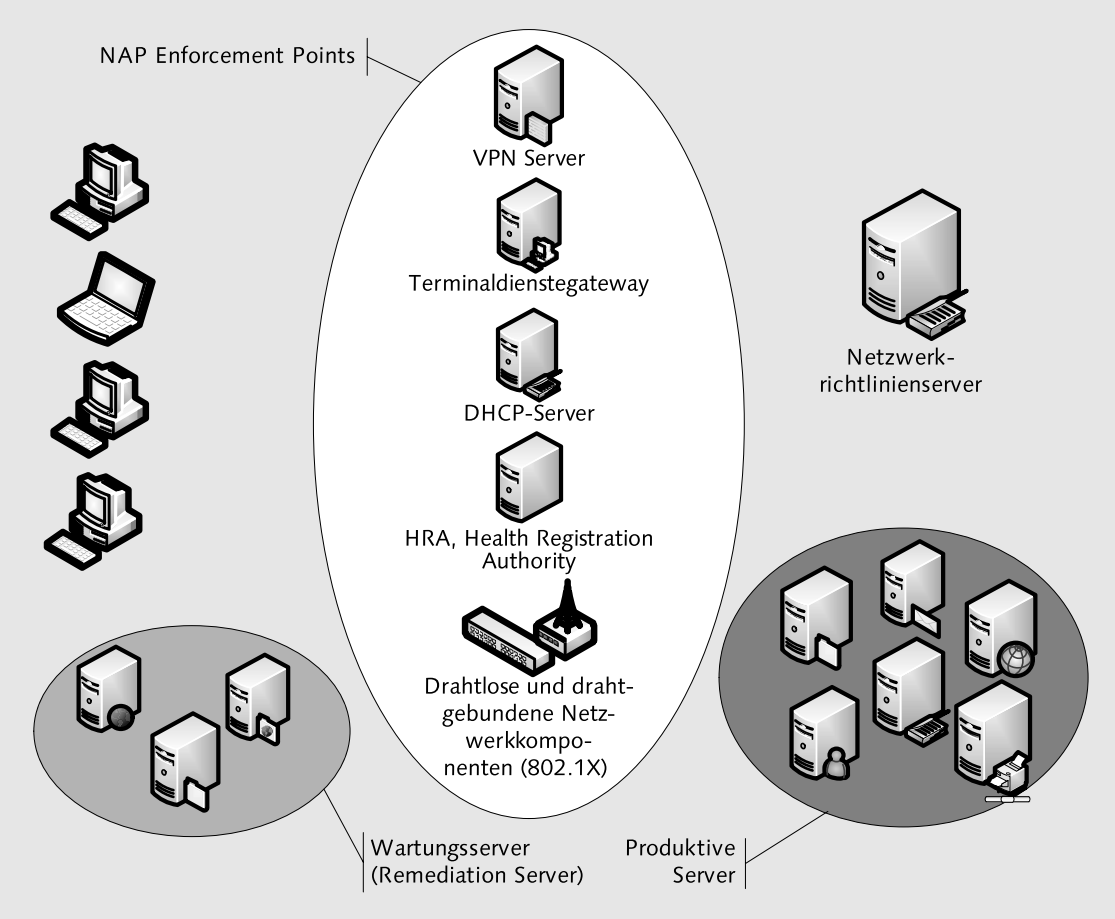


Abbildung 12.38 Die Idee hinter NAP in stark vereinfachter Darstellung

In Abbildung 12.39 lernen Sie einige wesentliche Komponenten von NAP in einer etwas technischeren Darstellung kennen:

Zunächst zum Client:

- Auf dem Client läuft ein *NAP-Agent*, der übrigens außer für Windows 7 für Windows Vista und Windows XP SP3 verfügbar ist.
- Dieser Agent verfügt über beliebig viele *System Health Agents* (SHA), die in der Lage sind, den »Gesundheitszustand« des Clients zu überprüfen. Hierzu gehört zum Beispiel, die Versionsnummer der aktuellsten Virensignatur zu ermitteln, den Zustand der Firewall (aktiviert/nicht aktiviert) zu überprüfen und Diverses mehr.

Dritthersteller können beliebige eigene SHAs programmieren, die beispielsweise die Versionsstände bestimmter Softwareprodukte prüfen oder schauen, ob der Monitor auch den aktuellen Ergonomiebestimmungen entspricht.

- Weiterhin sind an den NAP-Agenten beliebig viele *Enforcement Clients* angebunden. Es gibt beispielsweise einen Enforcement Client für DHCP, der die Kommunikationsvorgänge mit dem *DHCP-Enforcement Server* abwickelt.

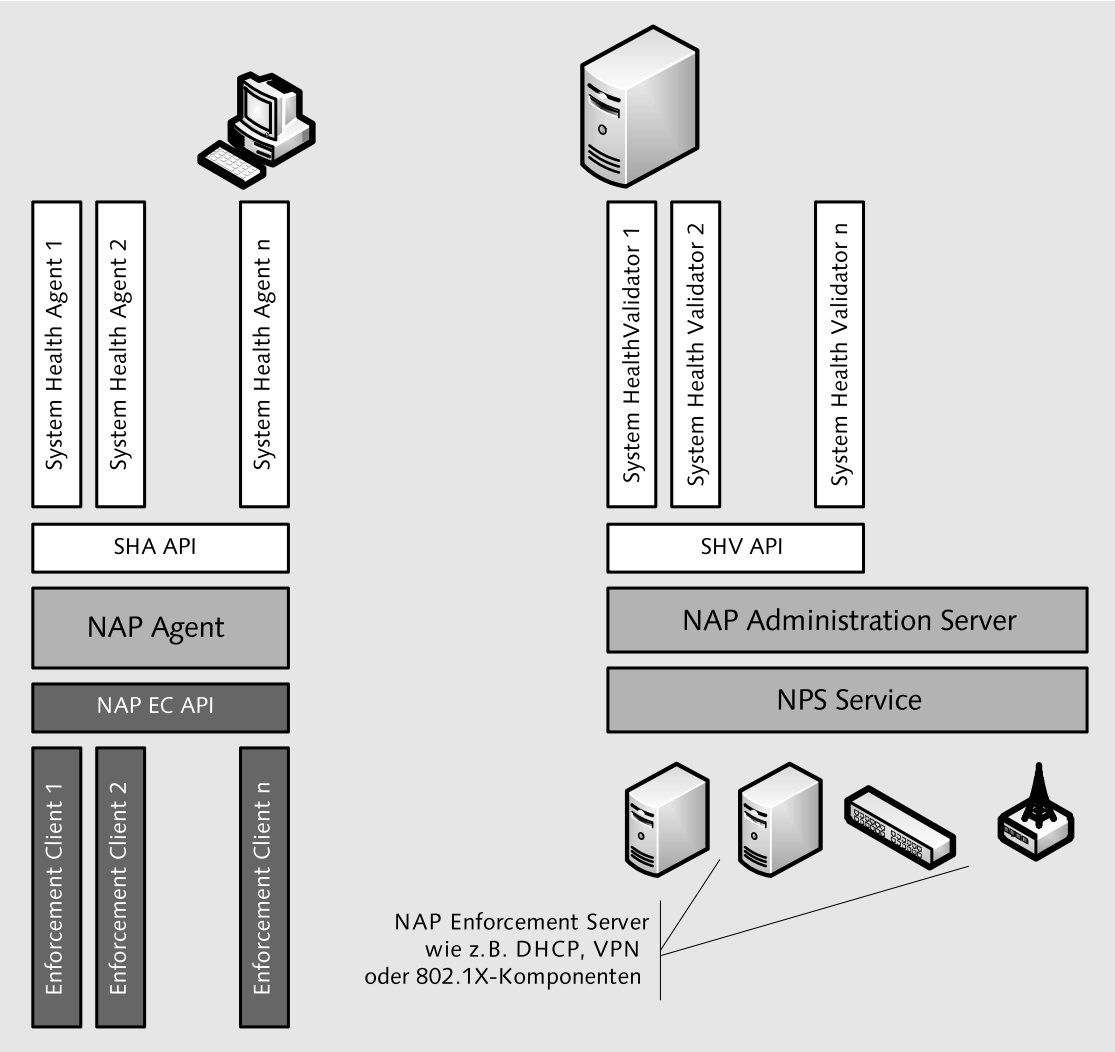


Abbildung 12.39 Die Komponenten vom NAP-Client und NAP-Server

Auf der Serverseite sieht es folgendermaßen aus (von unten nach oben):

- Zunächst gibt es verschiedene *Enforcement Server*. Dies können Windows-basierte Server (DHCP, Terminaldienstegateway, VPN-Server) sein, allerdings zählen auch 802.1X-Netzwerkgeräte (Switches, WLAN-APs) zu dieser Kategorie. Diese kommunizieren mit dem *Enforcement Client*.

- Der *NPS Service* ist letztendlich ein RADIUS-Server, der die Kommunikation mit den Enforcement Clients übernimmt. Der *NAP Administration Server* nimmt die Informationen über den Zugriff verlangenden Client vom NPS Service entgegen und leitet sie an die System Health Validators weiter.
- Die *System Health Validators* (SHV), von denen es ebenfalls beliebig viele geben kann, werten die empfangenen »Gesundheitszustandsinformationen« des Clients aus und prüfen, ob diese den aktuellen Anforderungen entsprechen. Ein SHV »weiß« zum Beispiel, ob es ausreicht, wenn das aktuelle Virenpattern vom 03.10.2009 stammt.

Diese Komponenten kommunizieren miteinander, und auch dabei gilt es einige Begriffe zu lernen (Abbildung 12.40):

- Die *System Health Agents* (SHA) ermitteln den Status in ihrem jeweiligen Gebiet (z. B. Virenpattern, Firewall-Status etc.) und leiten das Ergebnis in einem *Statement of Health* (SoH) an den NAP-Agent weiter.
- Die diversen SoHs werden in einem *System Statement of Health* (SSoH) zusammengefasst, das vom NAP-Agent an den jeweiligen Enforcement Client übergeben wird.
- Der *Enforcement Client* übergibt das SSoH an den Enforcement Server.
- Der *Enforcement Server* leitet das SSoH an den NAP Administration Server weiter.
- Der *NAP Administration Server* zerlegt das SSoH in die ursprünglichen SoHs, die an den jeweiligen System Health Validator (SHV) übergeben werden.

Aus Gründen der Übersichtlichkeit ist er nicht eingezeichnet, es gibt aber auch einen Rückweg:

- Die SHVs generieren jeweils eine SoHR, eine *Statement of Health Response*, in der einerseits angegeben ist, ob der Client kompatibel mit den Anforderungen ist; andererseits werden darin auch die Probleme (z. B. »Virenpattern zu alt«) benannt.
- Die diversen SoHRs werden zu einer SSoHR, einer *System Statement of Health Response*, zusammengefasst und zurück zum Client übertragen.

Weiterhin ermittelt der *NAP Administration Server* anhand der SoHRs, ob dem Client voller Zugriff gewährt werden soll oder ob er nur beschränkten Zugriff, nämlich auf die Wartungsserver, erhält.

Es kann individuell konfiguriert werden, ob alle SHVs »kompatibel« melden müssen oder ob es für vollen Zugriff auch noch ausreichend ist, wenn ein oder mehrere SHVs »nicht-kompatibel« melden.

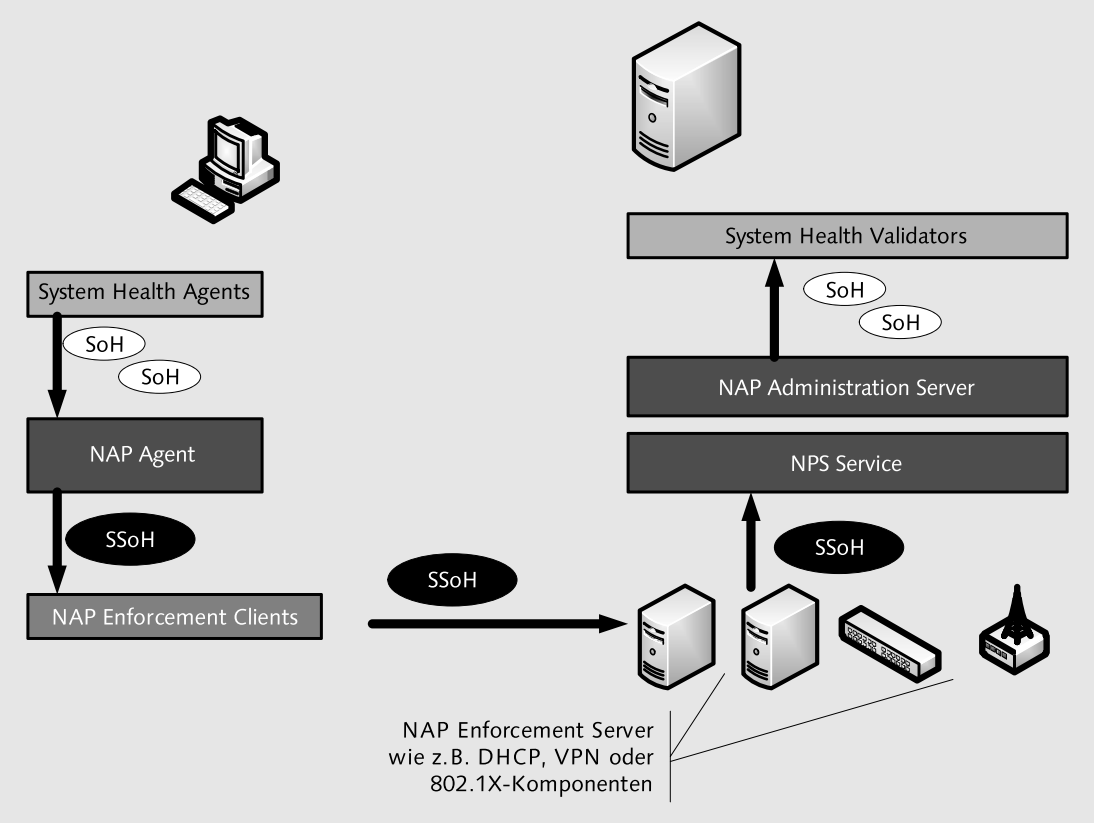


Abbildung 12.40 Die Kommunikationsvorgänge bei NAP

Ich möchte Ihnen dringend raten, sich diese Vorgänge zumindest ungefähr einzuprägen – Sie werden die Komponenten und Vorgänge später wiedererkennen.

Kommunikation

Die Kommunikation zwischen *Enforcement Server* und *NPS Service* läuft übrigens über das RADIUS-Protokoll ab. Aus diesem Grund können 802.1X-Komponenten recht problemlos eingebunden werden, indem diese als RADIUS-Client definiert werden. Sie müssen aber in der Lage sein, die SSoHs bzw. SSoHRs weiterzuleiten.

12.3.2 Netzwerkrichtlinienserver

Der Netzwerkrichtlinienserver (NPS, *Network Policy Server*) ermöglicht die Durchsetzung von organisationsweiten Regeln für die Kontrolle des Zugriffs von Clients. Die Hauptkomponenten sind der mit Windows Server 2008 erstmalig verfügbare *Netzwerkzugriffsschutz* (NAP, *Network Access Protection*) und der *RADIUS-Server*-Dienst.

Abbildung 12.41 gibt einen ersten Überblick über das Konfigurationswerkzeug. Sie sehen hier eine Vielzahl von Komponenten, deren Bedeutung Sie nun kennenlernen werden.

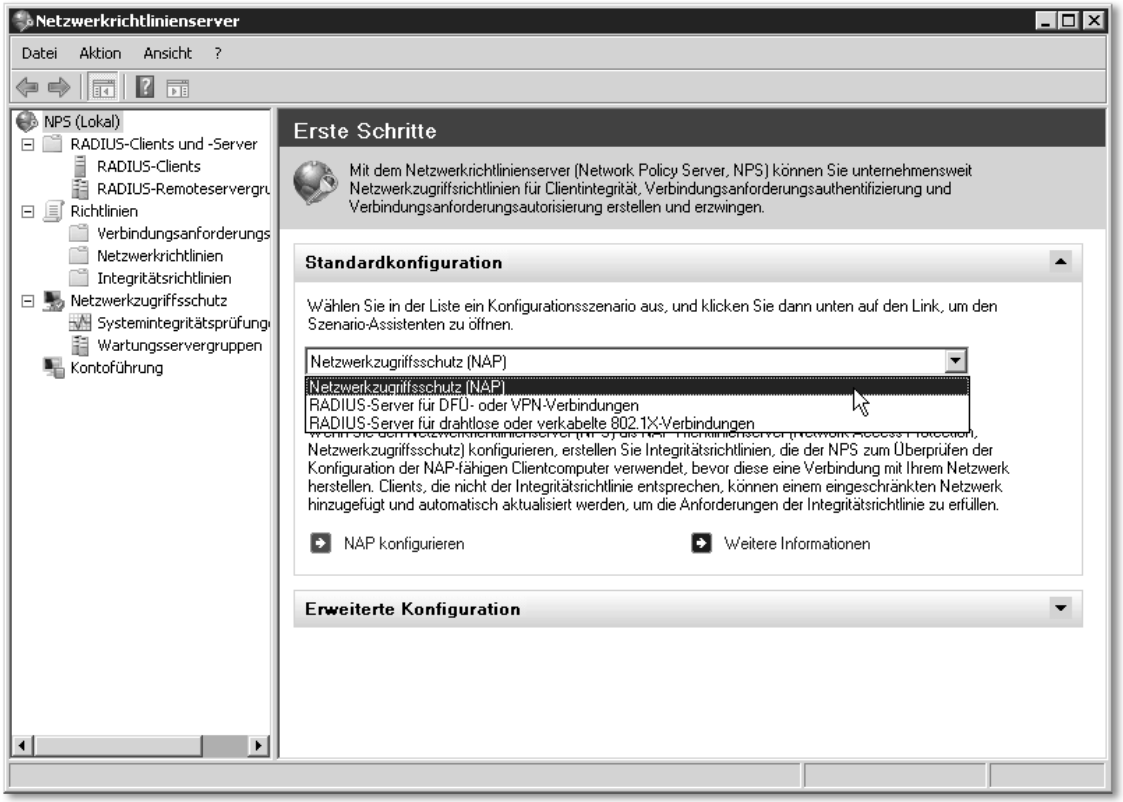


Abbildung 12.41 Das Konfigurationswerkzeug des Netzwerkrichtlinienservers

Ich möchte an dieser Stelle nun nicht jedes einzelne Element vorstellen, das im Netzwerkrichtlinienserver-Konfigurationswerkzeug zu sehen ist; ich möchte Ihnen aber jeweils ein Stichwort mitgeben. Sie werden die Elemente anhand eines Beispiels genauer kennenlernen:

- VERBINDUNGSANFORDERUNGSRICHTLINIEN: Diese Richtlinien legen fest, welche Verbindungen zum Netzwerkrichtlinienserver aufgebaut werden können. Mit diversen Bedingungen können Sie Einschränkungen definieren, beispielsweise bezüglich der Uhrzeit, des Herstellers der zugreifenden Komponente, des Benutzers und viele andere mehr. Mit einer solchen Richtlinie wird übrigens auch festgelegt, dass ein Zugriff an einen zentralen Netzwerkrichtliniensserver weitergeleitet werden soll.
- NETZWERKRICHTLINIEN: Mit den Netzwerkrichtlinien wird letztendlich festgelegt, welche Bedingungen zu einer Genehmigung oder einer Verweigerung des Zugriffs führen.
- INTEGRITÄTSRICHTLINIEN: Mit den Integritätsrichtlinien werden letztendlich die Bedingungen formuliert, die von einer Netzwerkrichtlinie ausgewertet werden. Hier wird insbesondere formuliert, welche Systemintegritätsprüfungen (SHV, *System Health Validator*) durchgeführt werden sollen.

- Systemintegritätsprüfungen: Hinter diesem Stichwort verbergen sich die SHVs, die *System Health Validators*. Standardmäßig wird eine Systemintegritätsprüfung mitgeliefert, die solche Aspekte wie Virenpattern, Firewallstatus und dergleichen mehr auswertet.
- Wartungsservergruppen: In Wartungsservergruppen werden diejenigen Server definiert, auf die ein Client Zugriff hat, wenn er als nicht zu den Richtlinien kompatibel erkannt wurde. Von diesen Servern kann der Client die benötigten Updates, Virenpattern etc. herunterladen.

Kontoführung

Hinter dem Stichwort Kontoführung verbirgt sich die Konfiguration der Protokollierung. Diese wird in diesem Buch zwar nicht weiter beschrieben, trotzdem sollten Sie diese Einstellmöglichkeit anschauen, um zu wissen, welche Protokollierungsoptionen einstellbar sind. Die Konfigurationsdialoge sind selbsterklärend.

12.3.3 Client vorbereiten

Wenn ein Client in einer NAP-aktivierten Umgebung arbeiten soll, müssen Sie zunächst einige Einstellungen vornehmen. Windows 7, Windows Vista und Windows XP (SP3) sind zwar grundsätzlich NAP-fähig, allerdings müssen Sie zwei Konfigurationsschritte durchführen:

- Der Dienst NAP-Agent muss auf den Starttyp Automatisch gestellt werden. Sinnvollerweise starten Sie ihn auch direkt (Abbildung 12.42).
- Die benötigten Erzwingungsclients müssen aktiviert werden.

Was ist ein Erzwingungsclient? Beim Netzwerkzugriffsschutz (NAP) wird der »Gesundheitszustand« des Clients überprüft und das Ergebnis an den Netzwerkrichtlinienserver übermittelt, der dann entscheidet, ob der Client zugriffsberechtigt ist – oder eben nicht.

Um die notwendigen Konfigurationsarbeiten »von Hand« zu erledigen, öffnen Sie in der MMC das Snap-In *NAP-Clientkonfiguration*, das in Abbildung 12.43 zu sehen ist.

Ist ein Erzwingungsclient erfolgreich aktiviert worden, finden Sie im Ereignisprotokoll einen entsprechenden Eintrag. Normalerweise gibt es zwar keine Probleme, einmal mehr kontrollieren kann aber im Zweifelsfall nicht schaden.

Ein Administrator, der NAP im Netz einführen möchte, muss nun natürlich nicht durchs Haus laufen und Dutzende, Hunderte oder Tausende PCs per Hand konfigurieren: Selbstverständlich können die NAP-Clienteinstellungen auch per Gruppenrichtlinie verteilt werden. Abbildung 12.44 zeigt die entsprechenden Einstellungen.

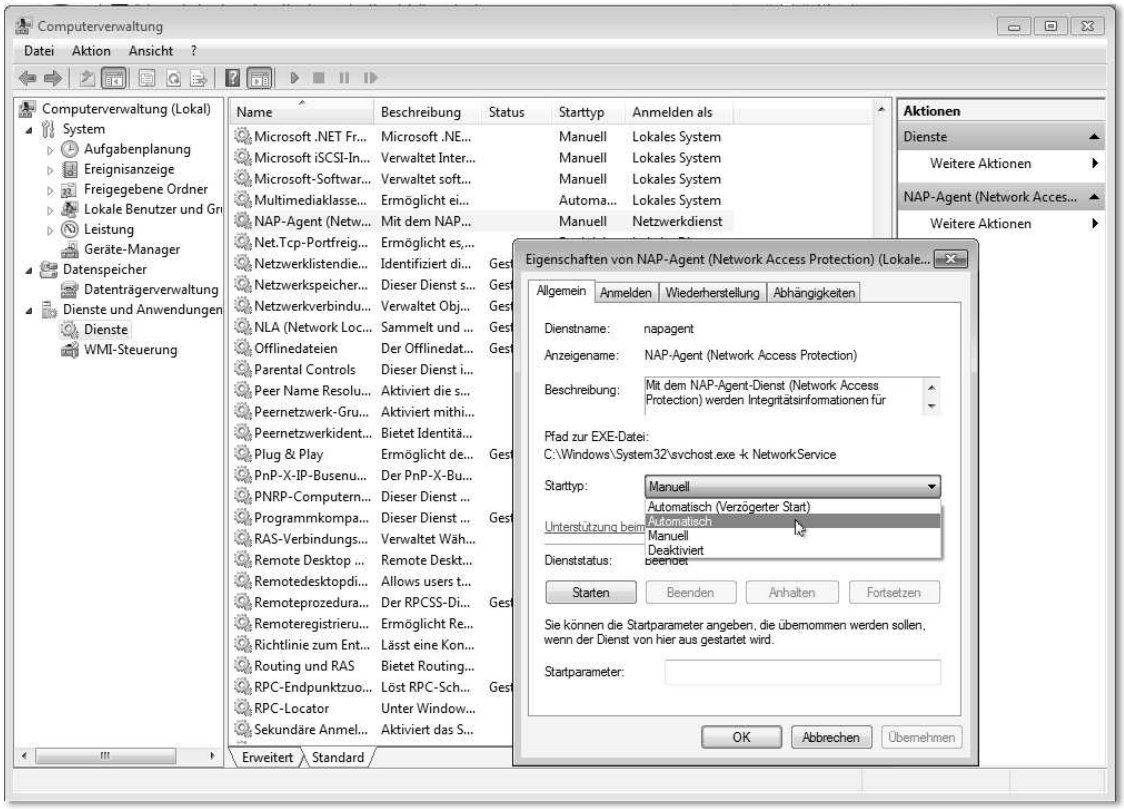


Abbildung 12.42 Auf dem Client muss der NAP-Agent-Dienst gestartet werden.

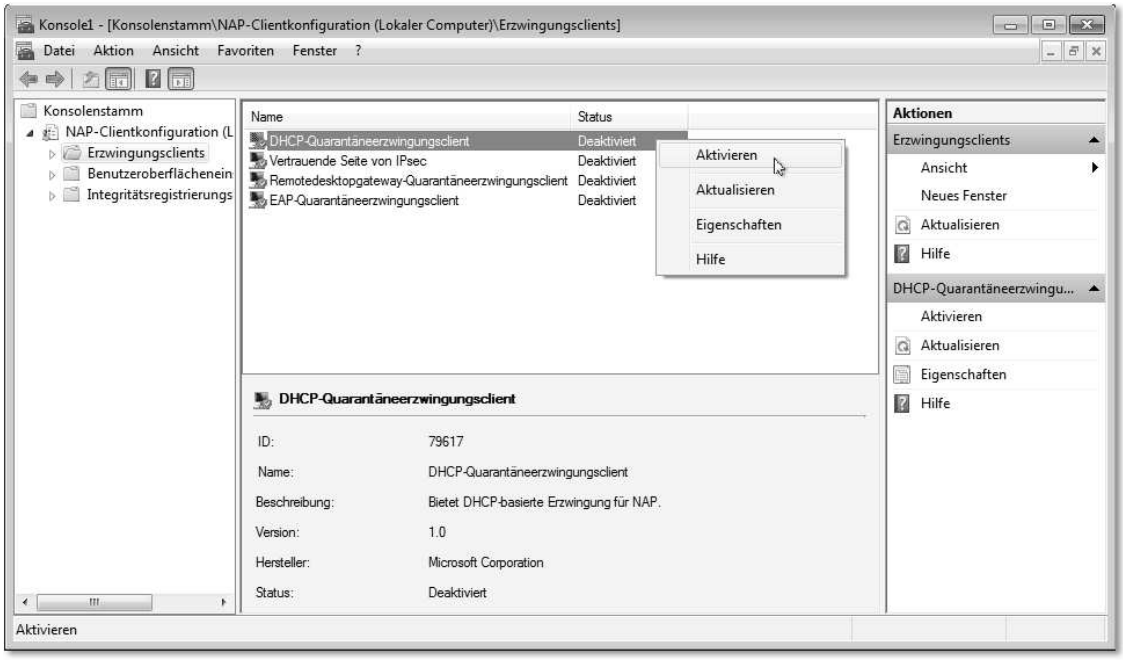


Abbildung 12.43 Aktiveren Sie in diesem Snap-In die benötigten Erzwingungsclients.

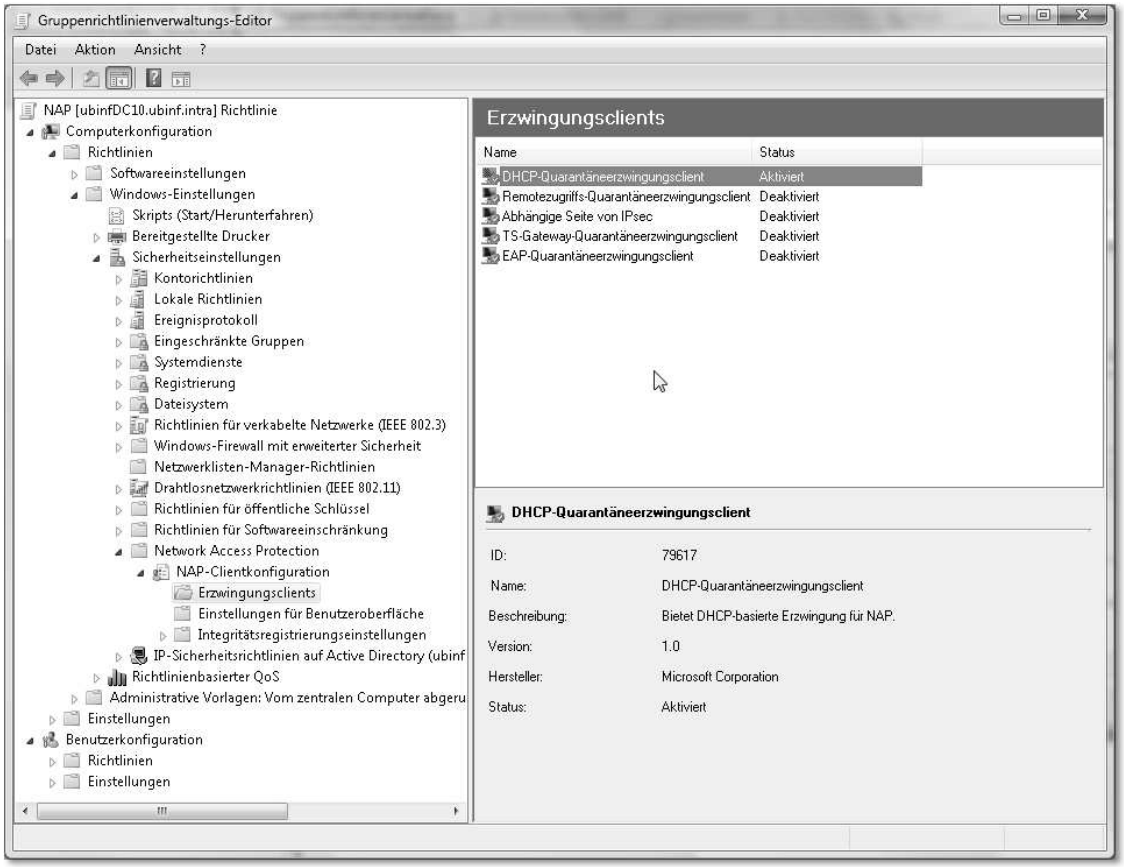


Abbildung 12.44 Die NAP-Clientkonfiguration ist natürlich auch per Gruppenrichtlinie möglich.

12.3.4 Ein mehrstufiges NAP-Konzept vorbereiten

Wenn Sie sich für die Einführung des Netzwerkzugriffsschutzes entscheiden, werden Sie vermutlich nicht »nur« eine, sondern mehrere Netzwerkverbindungsmethoden schützen wollen, also etwa DHCP und das Terminaldienstegateway. Nun ist es aber, um die beiden genannten Beispiele für Netzwerkverbindungsmethoden weiter zu betrachten, sowohl beim DHCP-Server als auch beim Terminaldienstegateway erforderlich, den *Netzwerkrichtlinienserver* (NPS) auf dem jeweiligen Dienste-Server zu installieren. Die meisten Administratoren dürften kaum erbaut sein, wenn die Verwaltung der Richtlinien jeweils lokal auf dem DHCP-Server, Terminaldienstegateway oder dergleichen stattfinden müsste – vielleicht gibt es ja auch mehrere davon.

In einer mittleren und größeren Umgebung wird also in etwa die Architektur aus Abbildung 12.45 gewünscht werden:

- Der Client wendet sich mit seinem Zugriffswunsch an einen Server, beispielsweise einen DHCP-Server oder ein Terminaldienstegateway.

- Auf den Servern ist zwar jeweils der Netzwerkrichtlinienserver installiert, diese sind aber so konfiguriert, dass sie die Anfragen an einen *zentralen* Netzwerkrichtlinienserver weiterleiten.
- Der zentrale Netzwerkrichtlinienserver prüft anhand der dort konfigurierten Richtlinien den Zugriff und übermittelt das Ergebnis.

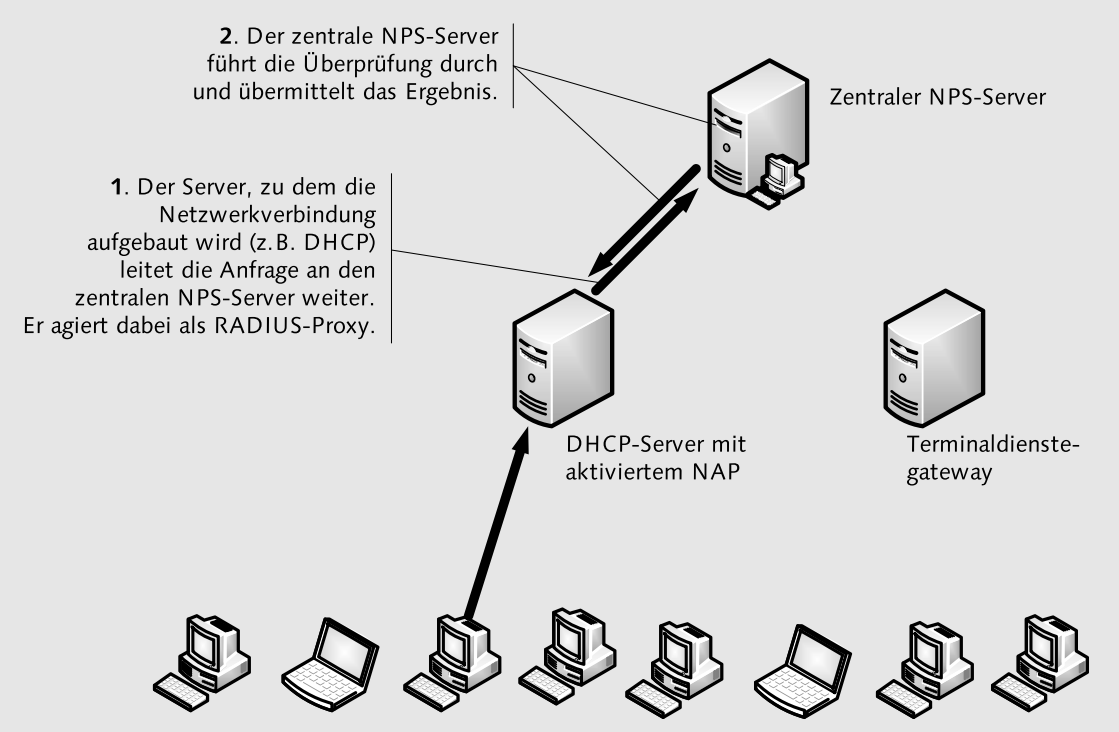


Abbildung 12.45 Wenn mehrere Netzwerkverbindungsmethoden durch NAP geschützt werden, kann trotzdem ein zentraler NPS-Server verwendet werden.

Da die Komponenten des Netzwerkzugriffsschutzes per RADIUS-Protokoll miteinander kommunizieren, agieren die Netzwerkrichtlinienserver auf den Servern (wie DHCP, Terminaldienstegateway etc.) technisch gesehen als RADIUS-Proxy.

Diese Architektur aufzubauen ist zwar nicht allzu schwierig, erschließt sich aber auch nicht unbedingt ganz intuitiv, sodass ich Ihnen die Vorgehensweise vorführe.

Konfiguration auf dem zentralen Netzwerkrichtlinienserver

Bei der Konfiguration von RADIUS-Client bzw. -Proxy auf der einen und dem RADIUS-Server auf der anderen Seite muss unter anderem ein gemeinsamer geheimer Schlüssel ausgetauscht werden. Da der Dialog zum Anlegen eines RADIUS-Clients diesen generieren kann, bietet es sich an, mit dem RADIUS-Client zu beginnen; prinzipiell ginge es aber auch »andersherum«.

Rufen Sie also auf dem zentralen Netzwerkrichtlinienserver den Menüpunkt Neuer RADIUS-Client auf; Abbildung 12.46 zeigt, wo dieser zu finden ist.

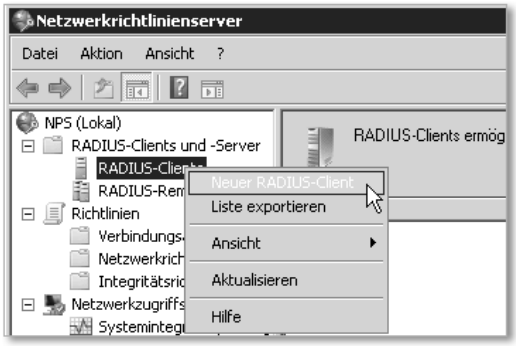


Abbildung 12.46 Dieser Menüpunkt startet das Anlegen eines RADIUS-Clients.

Abbildung 12.47 zeigt den Dialog, der sich nun öffnet. Die Einstellmöglichkeiten sind so weit selbsterklärend. Ich würde empfehlen, den gemeinsamen geheimen Schlüssel automatisch generieren zu lassen. Kopieren Sie den erzeugten Schlüssel (Zwischenablage), denn er muss ein wenig später im Client eingetragen werden.

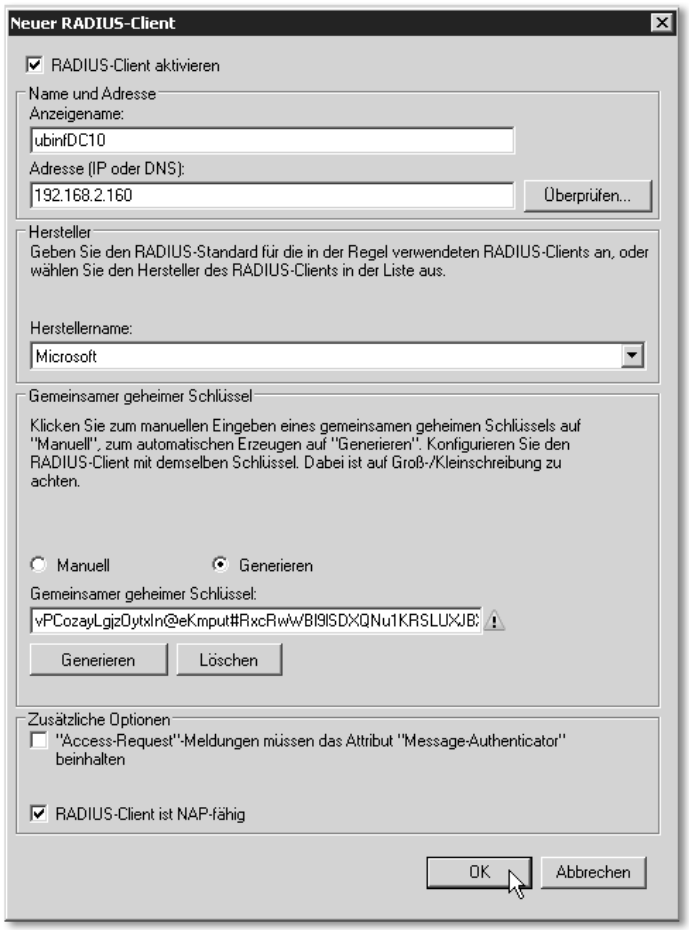


Abbildung 12.47 In diesem Dialog wird der RADIUS-Client angelegt. Kopieren Sie den »gemeinsamen geheimen Schlüssel«.

Konfiguration auf den RADIUS-Proxyservern

Auf den RADIUS-Proxyservern (z. B. DHCP-Server oder Terminaldienstegateway) muss der zentrale Netzwerkrichtlinienserver eingetragen werden. Hierzu wird eine neue RADIUS-Remoteservergruppe erzeugt, deren Mitglied der zentrale NPS ist.

Starten Sie die Konfiguration im Netzwerkrichtlinienserver-Snap-In mit dem Menüpunkt RADIUS-Remoteservergruppe • Neu (Abbildung 12.48).

Abbildung 12.48 Der Netzwerkrichtlinienserver, an den die Zugriffe weitergeleitet werden sollen, wird in einer neu zu erstellenden RADIUS-Remoteservergruppe angelegt.

In dem sich daraufhin öffnenden Dialog wird zunächst der Gruppenname der neuen RADIUS-Remoteservergruppe abgefragt. Weiterhin existiert eine Liste, in der beliebig viele RADIUS-Server eingetragen werden können. Wir erfassen hier nur einen, nämlich unseren zentralen NPS (Abbildung 12.49).

Die spannende Registerkarte beim Anlegen des RADIUS-Servers ist in Abbildung 12.46 gezeigt, denn hier wird der zuvor generierte gemeinsame geheime Schlüssel eingetragen. Die übrigen Einstellungen können Sie unverändert übernehmen.

Nun müssen Sie noch festlegen, dass alle Anforderungen an die zuvor angelegte RADIUS-Remoteservergruppe weitergeleitet werden sollen. Hierzu wechseln Sie in die Rubrik Verbindungsanforderungsrichtlinien und rufen der Einfachheit halber die Eigenschaften der vorhandenen Richtlinie auf. Auf der Registerkarte Einstellungen finden Sie im Abschnitt Authentifizierung die gesuchte Einstellung (Abbildung 12.51).

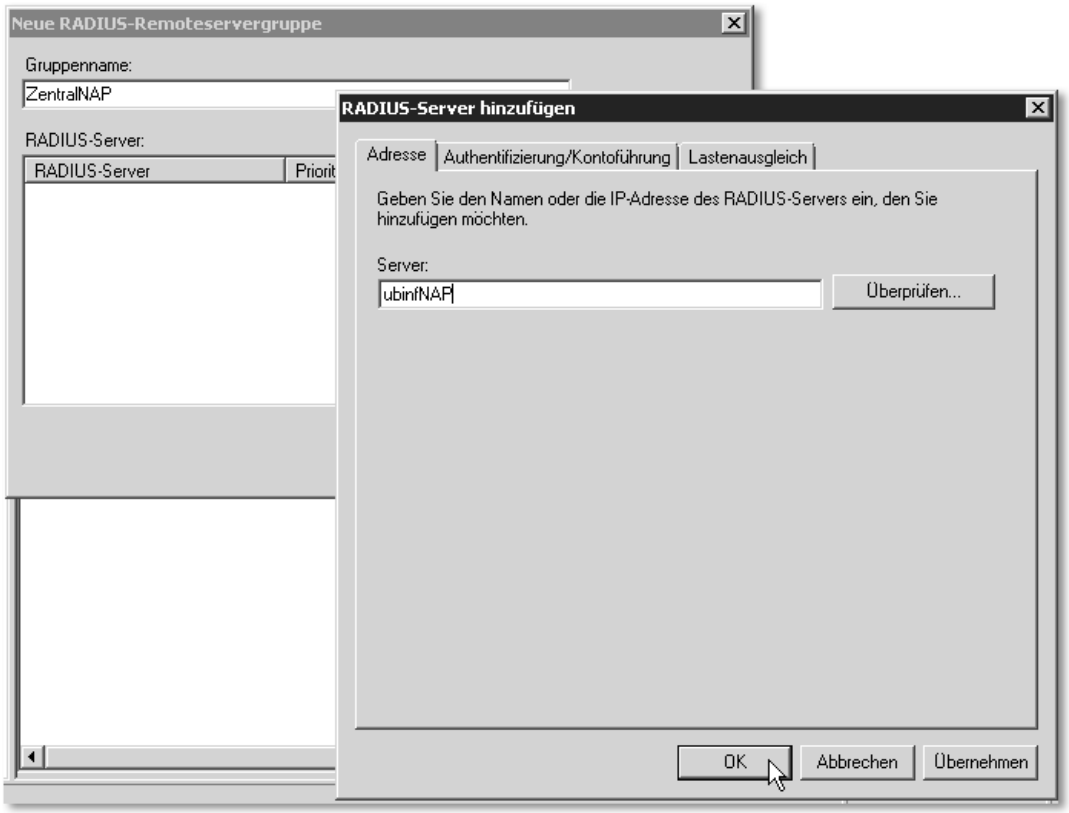


Abbildung 12.49 In der neuen RADIUS-Remoteservergruppe tragen Sie den zentralen Netzwerkrichtlinienserver ein.

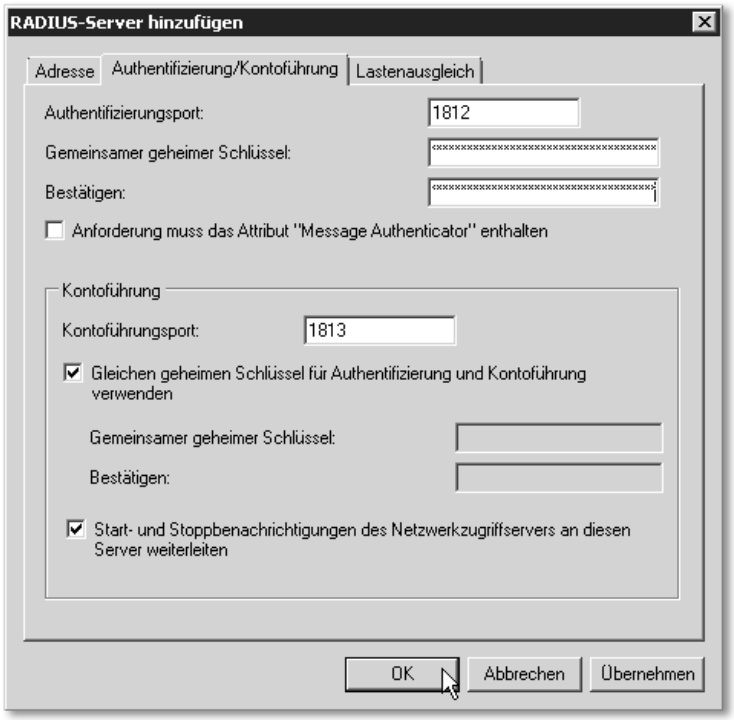


Abbildung 12.50 Auf dieser Registerkarte tragen Sie den zuvor erzeugten »gemeinsamen geheimen Schlüssel« ein.

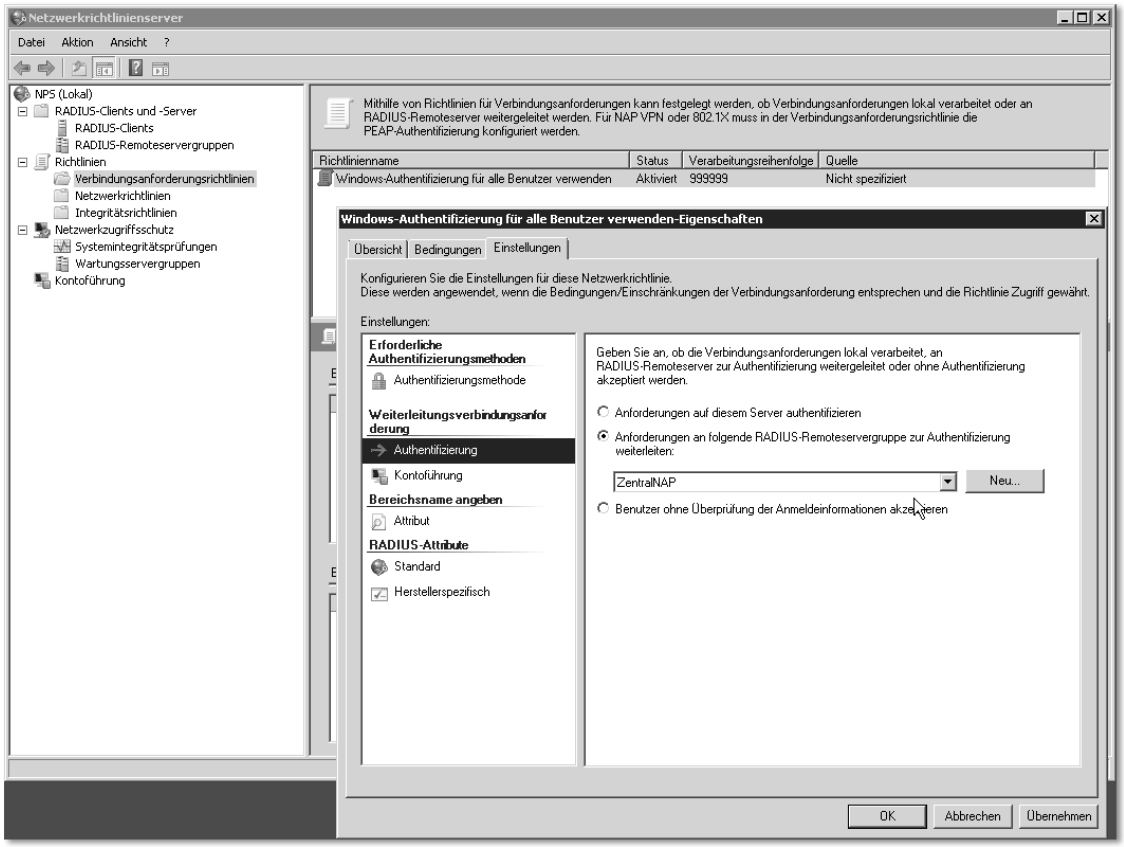


Abbildung 12.51 In einer Verbindungsanforderungsrichtlinie wird festgelegt, dass die Anforderungen an eine »RADIUS-Remoteservergruppe« weitergeleitet werden sollen.

12.3.5 NAP für DHCP-Zugriff

Die Absicherung des DHCP-Zugriffs hat einen Vorteil und einen Nachteil:

- Sie ist vergleichsweise einfach zu implementieren und umfasst dabei vermutlich fast alle Clients – vorausgesetzt, die Adressvergabe erfolgt über DHCP, wovon man aber zumeist ausgehen kann.
- Für einen »Dunkelmann« (oder natürlich auch eine »Dunkelfrau«), der bzw. die mutwillig einen »kranken« PC in das Netz schleusen möchte, ist DHCP-NAP sehr einfach zu umgehen, da es genügt, einfach eine statische IP-Adresse einzutragen.

Trotz dieses nicht ganz unwesentlichen Nachteils gilt: Wenn Sie sich darüber im Klaren sind, dass DHCP-NAP nicht gegen mutwillige Sabotage hilft, ist es durchaus eine sinnvolle Technologie, mit der sich ohne großen Aufwand verhindern lässt, dass PCs, die laut den Richtlinien gefährdet sind, ans Netz gelangen.

Kein IPv6

Wichtig zu erwähnen ist, dass DHCP NAP kein IPv6 unterstützt. Da meiner Erfahrung und Einschätzung nach die meisten Unternehmen und Organisationen auf absehbare Zeit weiterhin primär IPv4 fahren werden, sehe ich darin kein wesentliches Manko von DHCP NAP – momentan jedenfalls nicht.

Erster Installationsschritt und Netzwerkrichtlinienserver-Design

Bevor wir die eigentliche Einrichtung durchführen, ist eine Vorüberlegung notwendig: Auf jeden Fall muss auf dem DHCP-Server der Netzwerkrichtlinienserver installiert werden. Sie könnten die Richtlinien nun direkt auf diesem Server implementieren – und alles funktioniert.

Wenn Sie, wie weiter vorn im Abschnitt beschrieben wurde, einen zentralen Netzwerkrichtlinienserver verwenden möchten, müssen Sie zuerst den NPS-Server-Rollendienst auf dem DHCP-Server installieren und als RADIUS-Proxy konfigurieren. Dies habe ich Ihnen im Abschnitt »Konfiguration auf den RADIUS-Proxyservern« gezeigt.

Demnach sind die ersten Schritte:

- Wenn die Richtlinien direkt auf dem DHCP-Server konfiguriert werden sollen, müssen Sie dort nur den Rollendienst NETZWERKRICHTLINIENSERVER installieren.
- Falls die Richtlinienverarbeitung auf einem zentralen Netzwerkrichtlinienserver durchgeführt werden soll, installieren Sie zunächst die Rolle NETZWERKRICHTLINIENSERVER auf dem DHCP-Server und konfigurieren diesen dann als RADIUS-Proxy.

Einrichtung mit dem Assistenten

Sie können nun natürlich die benötigten Richtlinien (Verbindungsanforderungsrichtlinie, Netzwerkrichtlinie, Integritätsrichtlinie) per Hand erstellen – oder Sie machen sich das Leben ein bisschen einfacher und lassen den Assistenten für sich arbeiten. Den Einstieg zu dem Assistenten finden Sie, wenn Sie den obersten Knoten des Netzwerkrichtlinienserver-Verwaltungswerkzeugs selektieren und wie in Abbildung 12.52 gezeigt den Link NAP KONFIGURIEREN auswählen.

Hinweis

Wenn Sie mehrere Netzwerkrichtlinienserver einsetzen, also einen »zentralen« und einen auf dem DHCP-Server (als RADIUS-Proxy), werden die Richtlinien auf dem zentralen NPS angelegt.

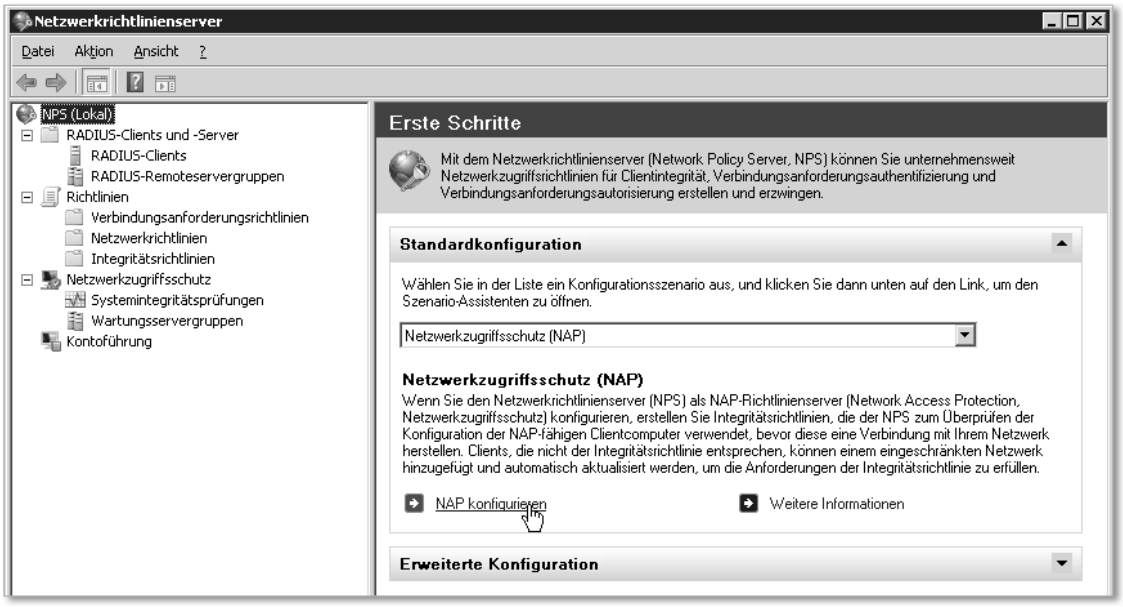


Abbildung 12.52 Hier starten Sie den Assistenten.

Der Assistent möchte zunächst von Ihnen wissen, für welche Netzwerkverbindungsmethode Sie nun Richtlinien erzeugen möchten. Gemäß der Zielsetzung dieses Abschnitts wählen Sie DHCP aus (Abbildung 12.53). In der Abbildung verdeckt die heruntergeklappte Combobox ein Textfeld, in das Sie den Namen der Richtlinie eingeben.

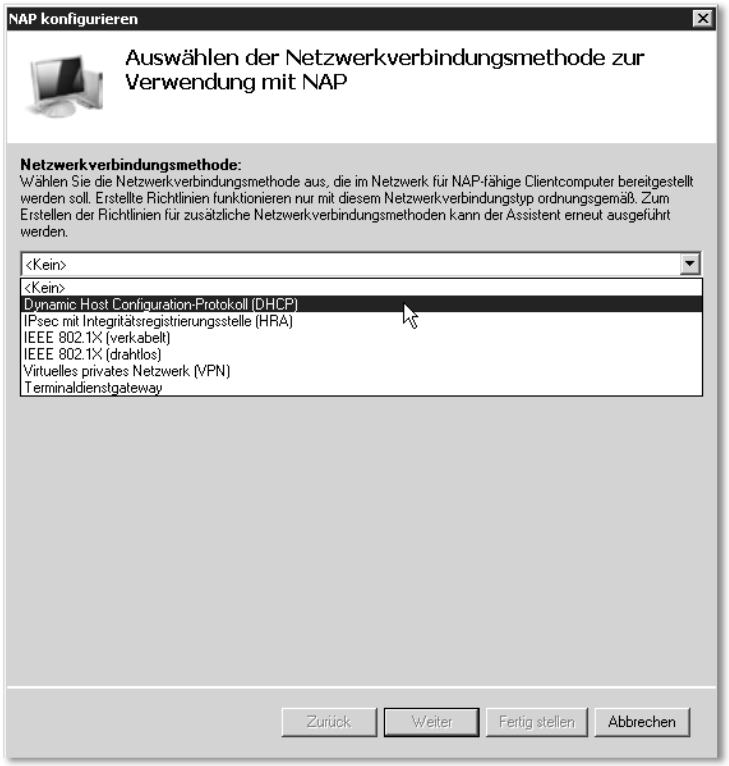


Abbildung 12.53 Zunächst wählen Sie die Netzwerkverbindungsmethode aus.

Abbildung 12.54 Optional können Sie die RADIUS-Clients auswählen.

Auf der nächsten Dialogseite können Sie die NAP-Erzwingungsserver angeben, auf denen DHCP-Server ausgeführt wird. Ob hier etwas eingetragen werden muss, hängt vom Gesamtszenario ab (Abbildung 12.54):

- Falls Sie die Richtlinien auf dem DHCP-Server abarbeiten lassen möchten, tragen Sie hier keinen RADIUS-Client ein.
- Ansonsten tragen Sie den DHCP-Server mit installiertem NPS als RADIUS-Client ein. Falls Sie die RADIUS-Client-zu-Server-Verbindung nicht bereits wie weiter vorn gezeigt eingerichtet haben, führt ein Klick auf Hinzufügen zu einem Dialog, in dem Sie den gemeinsamen geheimen Schlüssel festlegen können.

Die beiden nächsten Dialogseiten des Assistenten bleiben in dieser Testinstallation »leer« (Abbildung 12.55):

- Auf der links abgebildeten Dialogseite können Sie die Namen von DHCP-Bereichen eintragen, für die diese Richtlinie gültig sein soll. Wenn Sie keine Eingaben vornehmen, gilt die Regel für alle Bereiche der DHCP-Server.

  Anzumerken wäre, dass die eigentliche Konfiguration der DHCP-Server zusätzlich erfolgen muss – das zeige ich Ihnen ein wenig später.
- Wenn nur die Computer bestimmter Computergruppen DHCP-Adressen erhalten sollen, tragen Sie diese in der rechts abgebildeten Dialogseite ein.

Abbildung 12.55 Soll die Richtlinie für alle DHCP-Bereiche und für alle Benutzer/Computer gelten, bleibt die Dialogseite leer.

Abbildung 12.56 Auch diese Seite bleibt leer.

Die nächste Dialogseite ist wieder interessanter. Hier geht es um die Erfassung der Wartungsserver (Abbildung 12.57). Dies sind die Server, die auch erreichbar sein sollen, wenn der Computer keine gültige Konfiguration aufweist. Dies können beispielsweise die Server mit aktuellen Virenpattern oder der WSUS-Server sein.

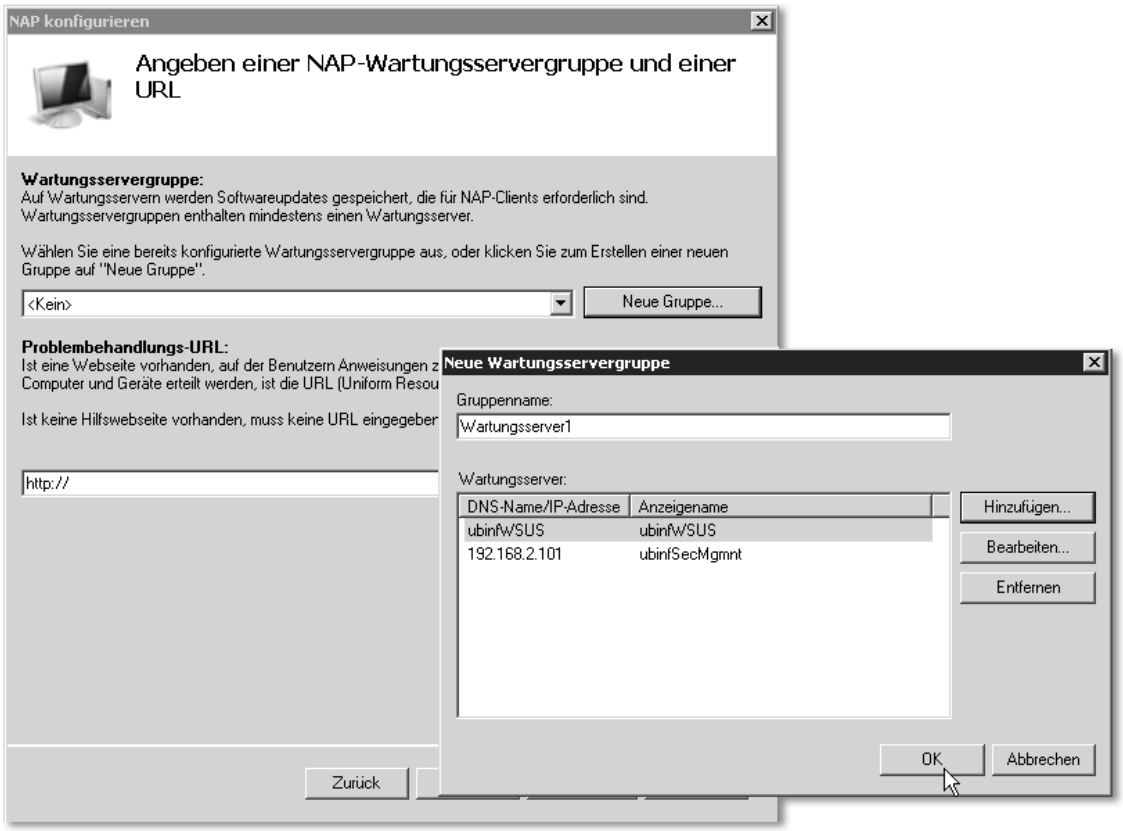


Abbildung 12.57 Eintragen von Wartungsservern

Auf der letzten Eingabeseite des Assistenten wählen Sie eine NAP-Integritätsrichtlinie aus. Diese beschreibt, welche Kriterien ein Computer erfüllen muss, um nicht als »potenziell krank und gefährdet« angesehen zu werden. Im Wesentlichen wählen Sie hier ein oder mehrere Systemintegritätsprüfungs-Objekte aus. In einer Standardinstallation, die nicht durch Drittherstellerkomponenten erweitert wurde, ist allerdings nur ein solches Objekt vorhanden, nämlich die Windows-Sicherheitsintegritätsverifizierung. In dieser sind solche Kriterien wie aktuelles Virenpattern, »Firewall aktiviert« oder »aktueller Patch-Level« definiert (Abbildung 12.58).

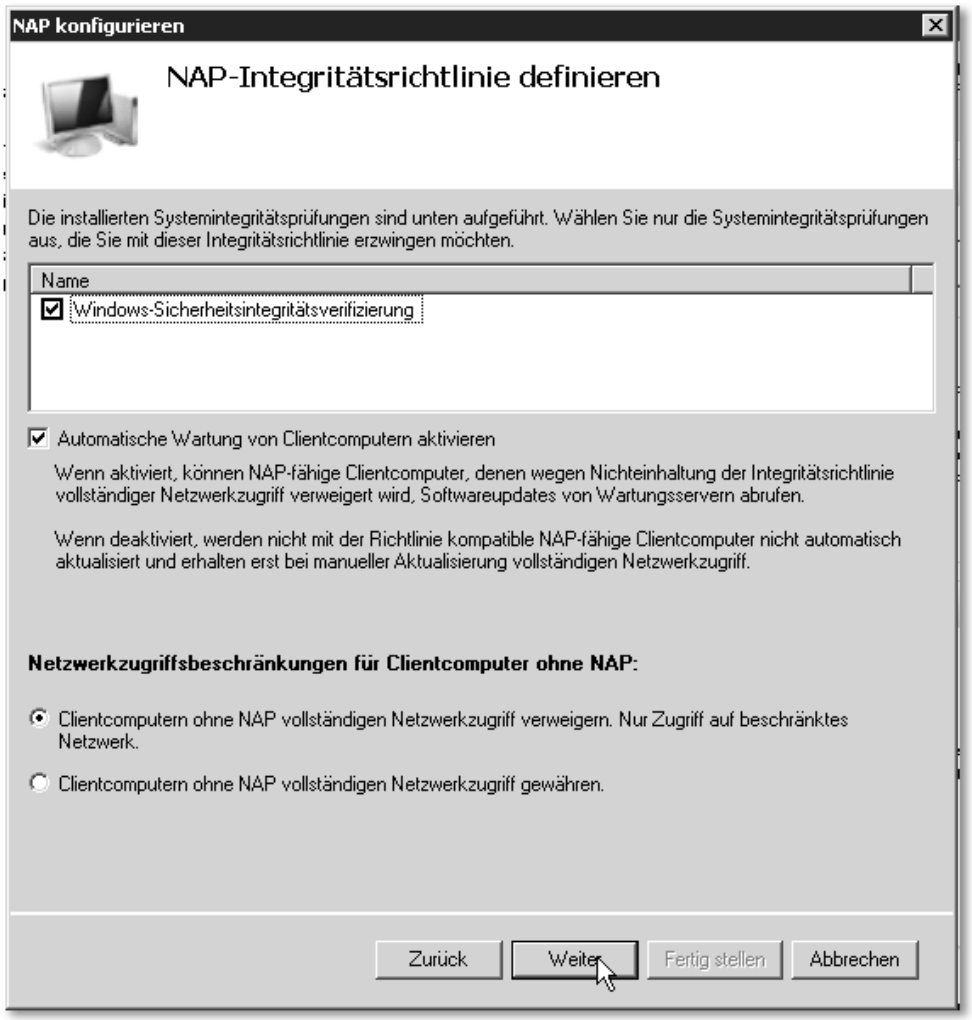


Abbildung 12.58 Standardmäßig ist nur eine Integritätsrichtlinie vorhanden. Wählen Sie sie aus.

Was der Assistent alles getan hat

Nach Abschluss des Assistenten sehen wir uns einmal an, was er alles eingerichtet hat.

Verbindungsanforderungsrichtlinien

Zunächst ist eine Verbindungsanforderungsrichtlinie angelegt worden, in der als Typ des Netzwerkzugriffsservers DHCP-Server angegeben ist (Abbildung 12.59).

In dieser Richtlinie sind keine weiteren Einstellungen vorgenommen worden, weshalb es hier auch nichts weiter zu besprechen gibt.

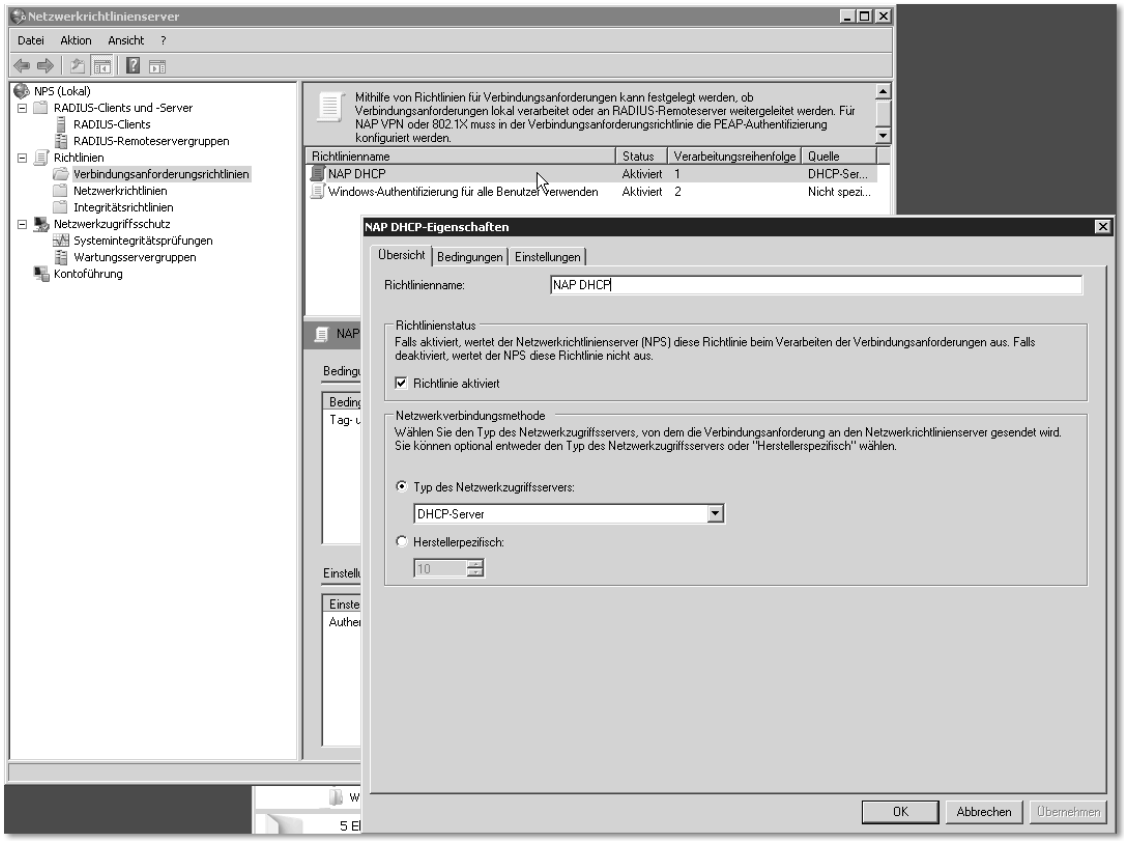


Abbildung 12.59 Eine neue Verbindungsanforderungsrichtlinie ist angelegt worden.

Netzwerkrichtlinien

Interessanter sind da schon die Änderungen an den Netzwerkrichtlinien. Hier gibt es drei neue Objekte (Abbildung 12.60):

- kompatible DHCP-Clients
- nicht kompatible DHCP-Clients
- nicht NAP-fähige DHCP-Clients

Die Einstellungen auf der Registerkarte Übersicht sind übrigens bei allen drei Richtlinien identisch. Dem Client wird Zugriff gewährt, d. h., eine IP-Adresse zugeteilt. Der Sinn dahinter ist, dass ja auch nicht kompatible Clients in irgendeiner Form Netzwerkkonnektivität benötigen, sonst könnten sie ja keine Patterns, Updates oder sonstige Objekte empfangen, die ihnen helfen können, wieder kompatibel zu werden.

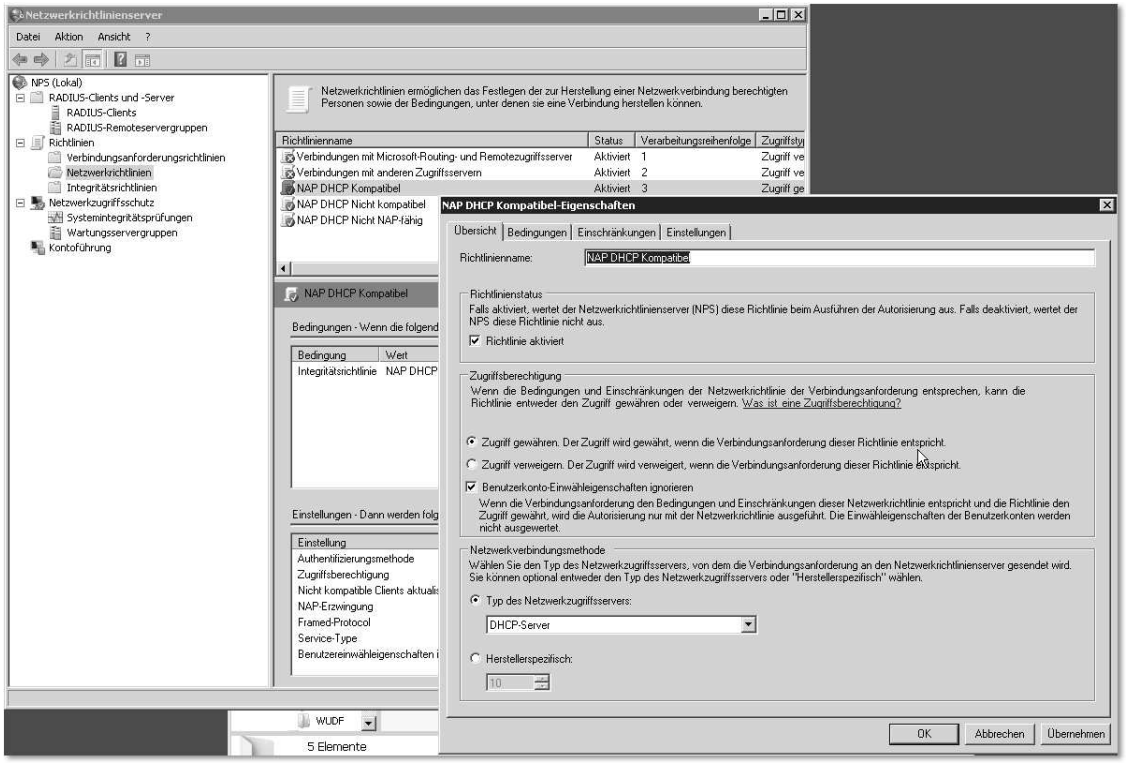


Abbildung 12.60 Drei neue Netzwerkrichtlinien sind angelegt worden.

Welche BEDINGUNGEN zu erfüllen sind, ist auf der gleichnamigen Registerkarte aufgeführt (Abbildung 12.61):

- Kompatible Clients müssen die Integritätsrichtlinie NAP DHCP KOMPATIBEL erfüllen, die ebenfalls vom Assistenten angelegt worden ist.
- Nicht kompatible Clients erfüllen die vom Assistenten angelegte Integritätsrichtlinie NAP DHCP NICHT KOMPATIBEL.
- Clients, die nicht NAP-fähig sind, erfüllen die Bedingung COMPUTER IST NICHT NAP-FÄHIG, was sozusagen eine »eingebaute Bedingung« ist.

Die drei Netzwerkrichtlinien unterscheiden sich in der eingetragenen Bedingung und in einem Punkt auf der Registerkarte EINSTELLUNGEN (Abbildung 12.62):

- Kompatiblen Clients wird VOLLSTÄNDIGER NETZWERKZUGRIFF gewährt.
- Nicht kompatiblen und nicht NAP-fähigen Clients wird EINGESCHRÄNKTER ZUGRIFF gewährt.

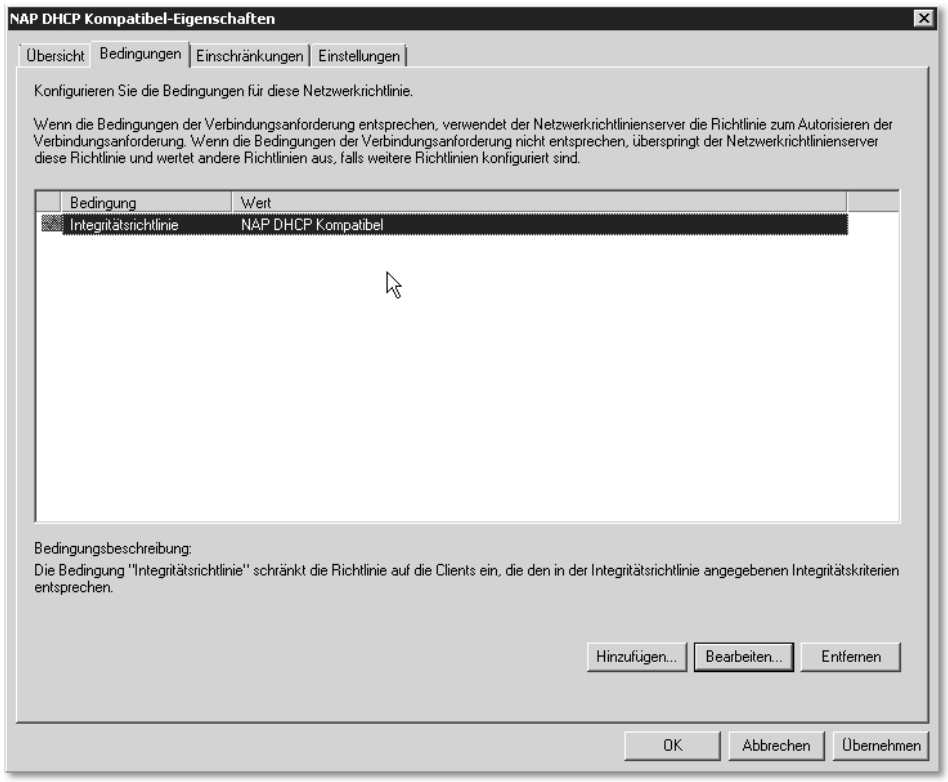


Abbildung 12.61 Als Bedingung ist eine Integritätsrichtlinie hinterlegt.

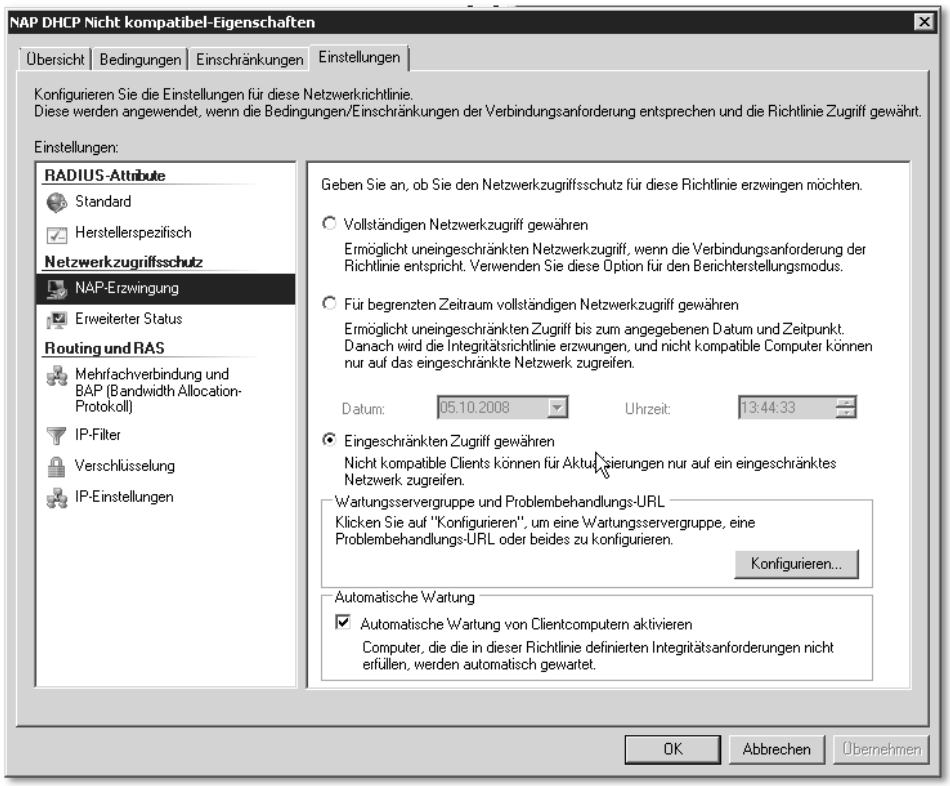


Abbildung 12.62 Ein nicht kompatibler Client erhält zwar eine IP-Adresse, ihm wird aber nur eingeschränkter Zugriff gewährt.

Integritätsrichtlinien

Weiterhin hat der Assistent zwei Integritätsrichtlinien erzeugt. Diese besagen:

- Ein Client ist NAP DHCP KOMPATIBEL, wenn er alle ausgewählten Systemintegritätsprüfungen besteht (Abbildung 12.63).
- Ein Client ist NAP DHCP NICHT KOMPATIBEL, wenn er mindestens eine der ausgewählten Prüfungen nicht besteht (Abbildung 12.64).

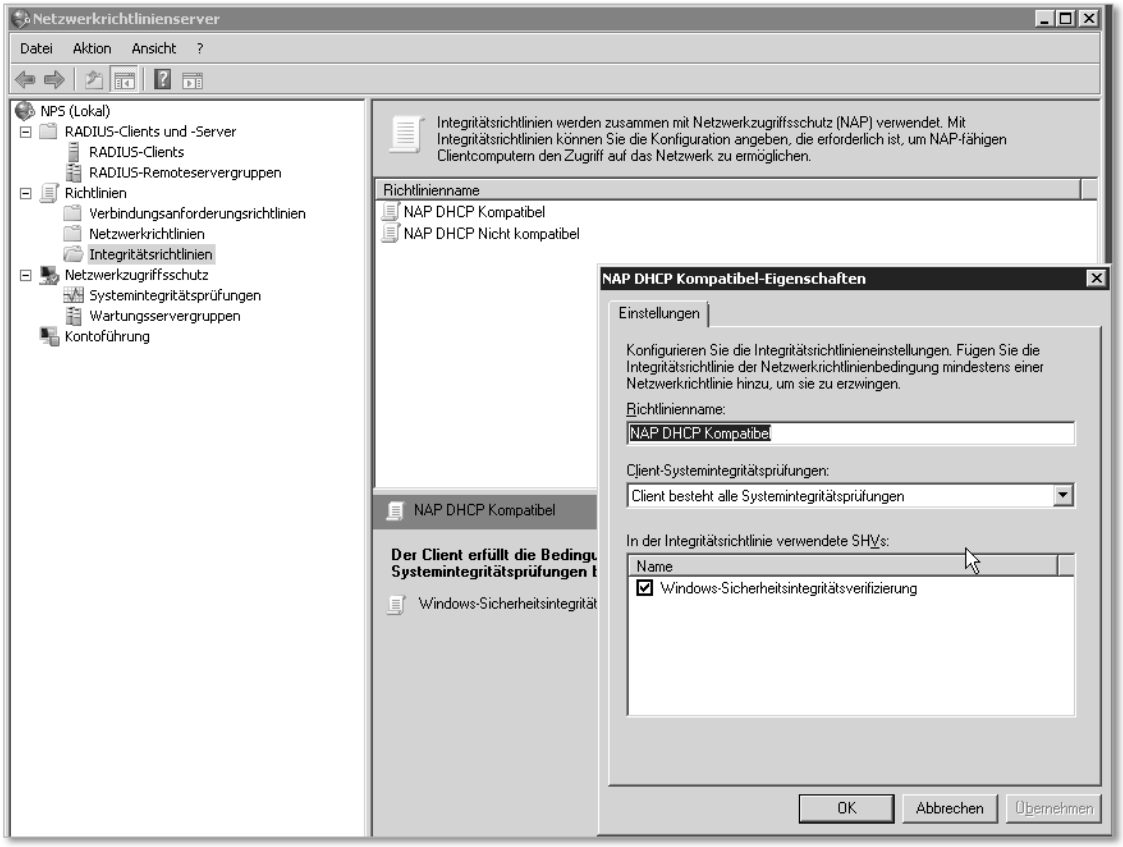


Abbildung 12.63 Ein Client ist »NAP DHCP Kompatibel«, wenn er alle ausgewählten Systemintegritätsprüfungen besteht.

Da es sich um eine nicht erweiterte Standardinstallation handelt, ist nur eine Systemintegritätsprüfung vorhanden. Es könnte aber auch durch Drittherstellerprodukte erweiterte Szenarien geben, in denen man mehrere oder eine andere Systemintegritätsprüfung auswählt.

Systemintegritätsprüfungen

Der Assistent nimmt zwar Modifizierungen im Abschnitt SYSTEMINTEGRITÄTSPRÜFUNGEN vor, trotzdem kann es nicht schaden, bei dieser Gelegenheit einen Blick dort hineinzuwerfen.

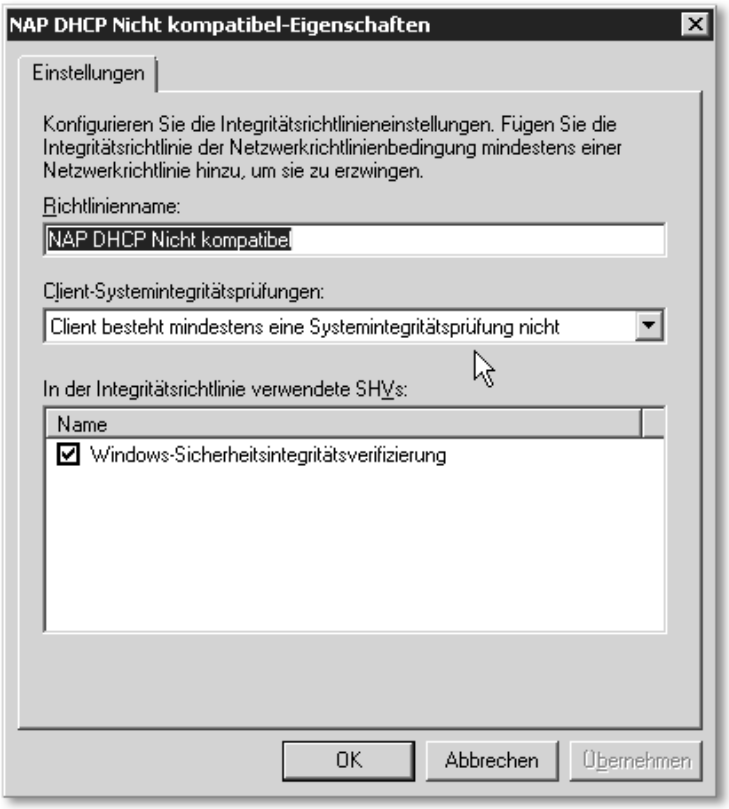


Abbildung 12.64 Ein Client ist »NAP DHCP Nicht kompatibel«, wenn er mindestens eine der ausgewählten Prüfungen nicht besteht.

In einer Standardinstallation ist nur eine Systemintegritätsprüfung vorhanden, nämlich die Windows-Sicherheitsintegritätsprüfung – Dritthersteller können hier übrigens eigene Erweiterungen integrieren.

In den Eigenschaften des Elements ist zunächst konfiguriert, wie sich das System verhalten soll, wenn eine der benötigten Komponenten (SHV, SHA) nicht reagiert oder nicht erreicht werden kann. Standardmäßig wird in einem solchen Fall NICHT KOMPATIBEL zurückgegeben, d. h., der Client erhält nur beschränkten Zugriff (Abbildung 12.65).

Über die Schaltfläche KONFIGURIEREN gelangen Sie zur »Detailkonfiguration« der gewählten Systemintegritätsprüfung (Abbildung 12.66):

- Auf der ersten Registerkarte können Sie einstellen, welche Bedingungen ein Windows 7- oder Windows-Vista-Client erfüllen muss, damit er die Systemintegritätsprüfung positiv besteht.
- Die zweite Registerkarte enthält Einstellungen für XP, wobei dort der SPYWARESCHUTZ nicht vorhanden ist.

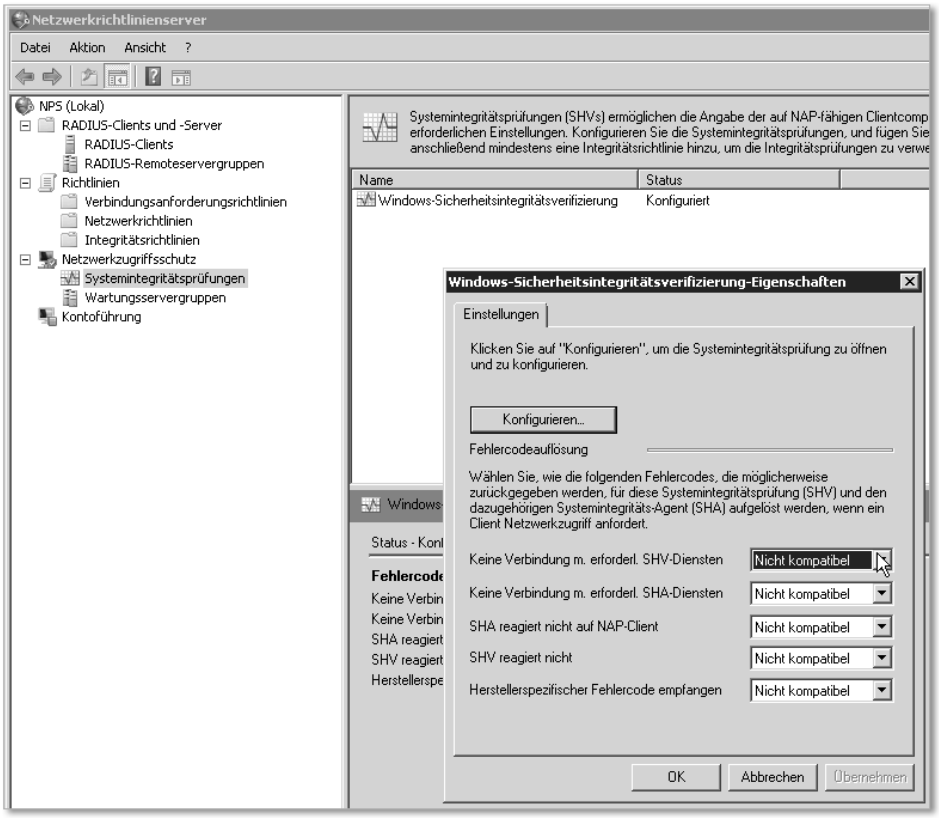


Abbildung 12.65 Standardmäßig wird »Nicht kompatibel« zurückgegeben, wenn bei der Überprüfung ein Fehler auftritt, beispielsweise eine Verbindung zu einem benötigten Dienst nicht aufgebaut werden kann.

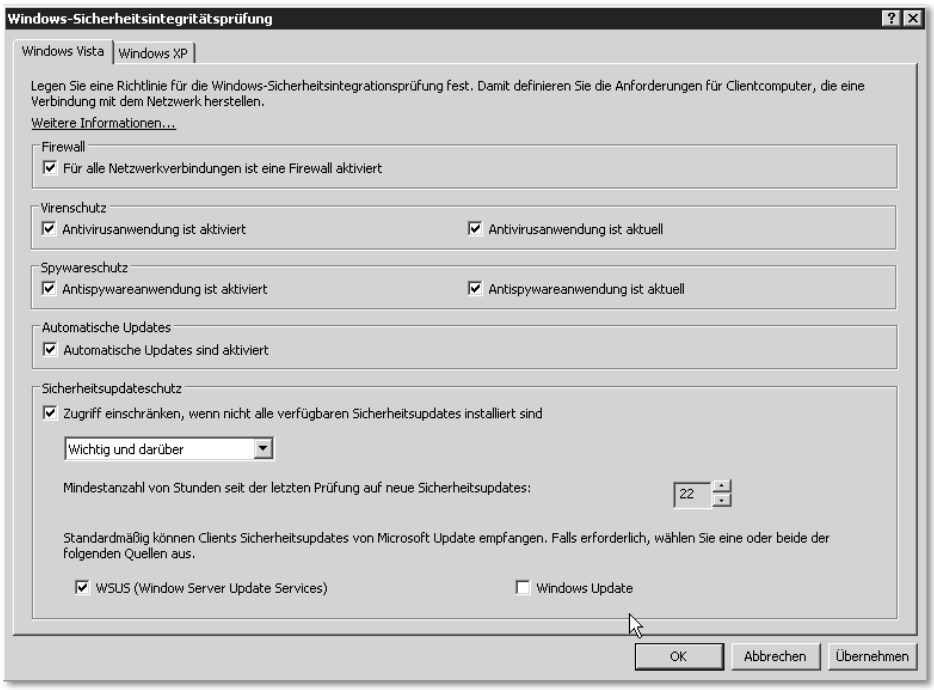


Abbildung 12.66 In der Konfiguration der »Windows-Sicherheitsintegritätsprüfung« können Sie festlegen, welche Bedingungen ein Client erfüllen muss.

Wartungsservergruppe

Unterhalb des Knotens Wartungsservergruppen ist die vom Assistenten erstellte Wartungsservergruppe zu finden. Zu ihr gibt es allerdings nichts weiter zu erklären, weshalb sie hier nicht weiter aufgeführt ist.

Vorbereitung des DHCP-Servers

Auf dem DHCP-Server sind ebenfalls noch einige Einstellungen vorzunehmen – keine Sorge, es handelt sich um nichts Kompliziertes.

Hinweis

Falls Sie dieses Kapitel nicht von vorn nach hinten durcharbeiten, sondern diese Seite mehr oder weniger zufällig aufgeschlagen haben, sei darauf hingewiesen, dass auf dem DHCP-Server der Netzwerkrichtlinienserver installiert und gegebenenfalls als RADIUS-Proxy konfiguriert werden muss.

In den Eigenschaften des Bereichs finden Sie die Registerkarte Netzwerkzugriffsschutz, auf der Sie festlegen, ob dieser Bereich dieser »Behandlung« unterliegt (Abbildung 12.67).

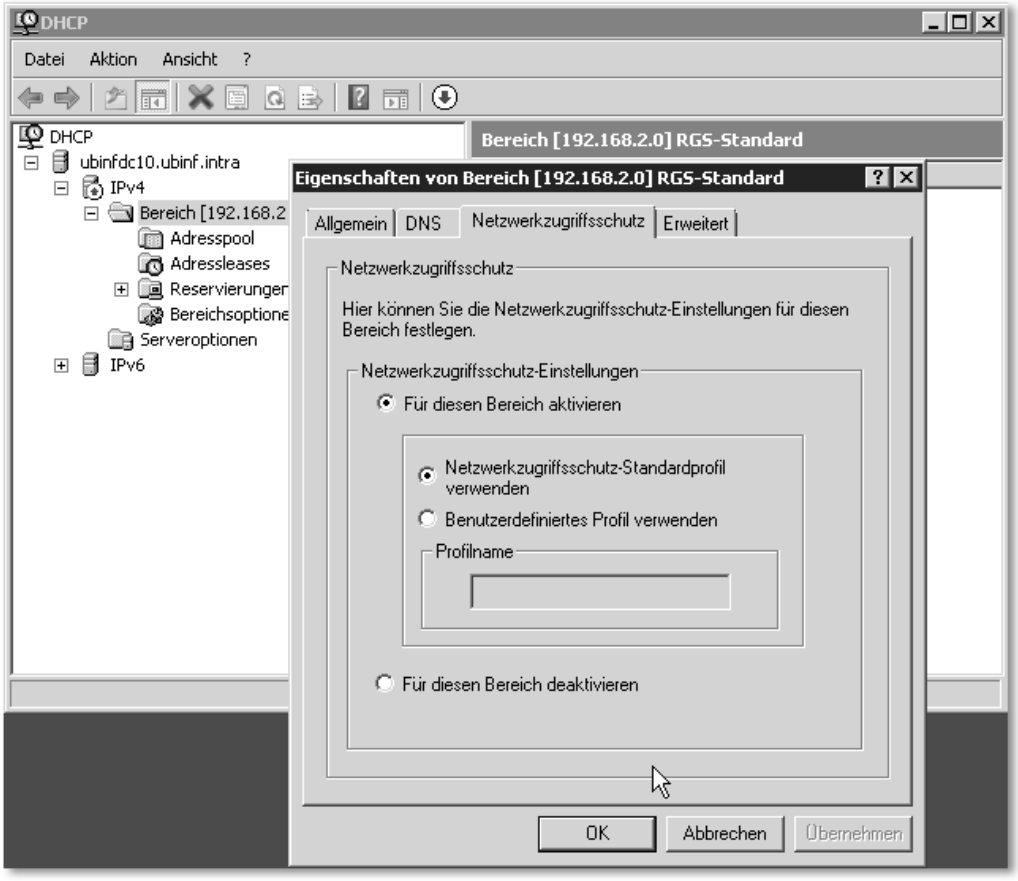


Abbildung 12.67 Der Netzwerkzugriffsschutz wird für den Bereich aktiviert.

Bei Nicht-Erreichbarkeit des Netzwerkrichtlinienservers

In den Eigenschaften des IPv4-Bereichs des Servers gibt es eine gleichnamige Registerkarte, auf der festgelegt werden kann, wie sich der DHCP-Server verhalten soll, wenn der Netzwerkrichtlinienserver nicht erreichbar ist.

Der zweite Schritt bei der Konfiguration des DHCP-Servers ist, dass Sie für die nicht kompatiblen Clients eigene Bereichsoptionen (z. B. DNS-Server) setzen können und müssen. Gehen Sie dazu so vor (Abbildung 12.68):

- Wählen Sie im Kontextmenü des Knotens BEREICHSOPTIONEN den Menüpunkt OPTIONEN KONFIGURIEREN. Wechseln Sie auf die Registerkarte ERWEITERT.
- Dort wählen Sie die Benutzerklasse STANDARDMÄSSIGE NETZWERKZUGRIFFSCHUTZ-KLASSE.
- Tragen Sie nun die gewünschten Bereichsoptionen ein.

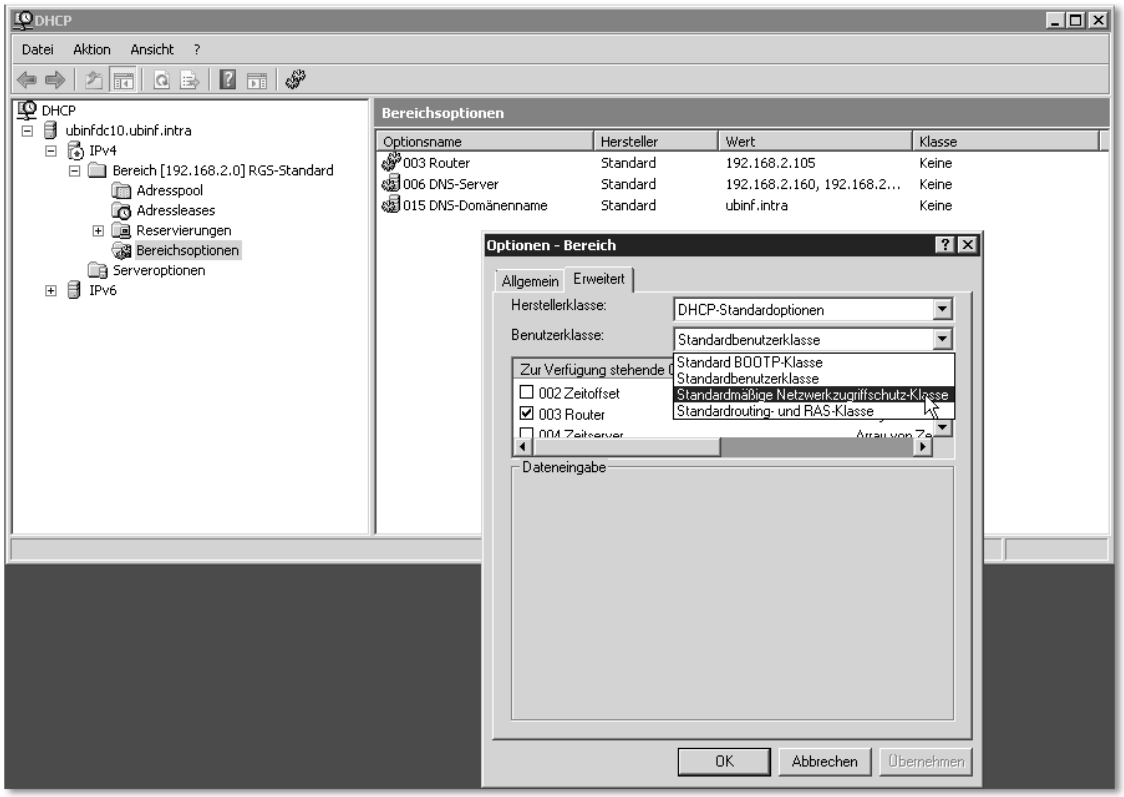


Abbildung 12.68 Bereichsoptionen, die bei nicht kompatiblen Clients vergeben werden sollen, tragen Sie in der »Standardmäßigen Netzwerkzugriffschutz-Klasse« ein.

Das Ergebnis wird dann beispielsweise so wie in Abbildung 12.69 gezeigt aussehen. In der Ansicht sehen Sie die Spalte KLASSE, die angibt, welche Option wohin gehört.

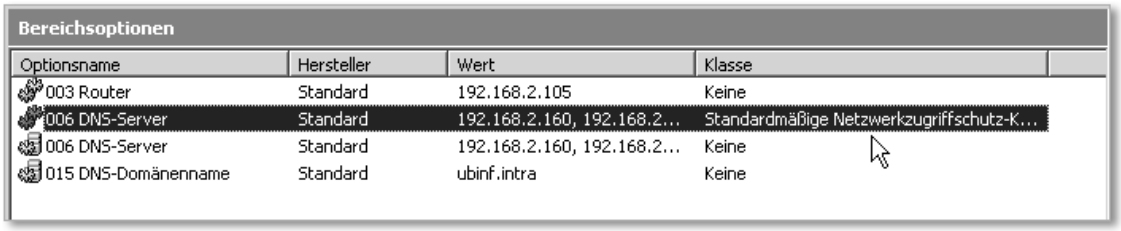


Abbildung 12.69 Bereichsoptionen aus verschiedenen Benutzerklassen

Aus Sicht des Clients

Wenn ein Client versucht, eine DHCP-Adresse zu erhalten, sein Zustand aber nicht den Anforderungen entspricht, wird die Benachrichtigung aus Abbildung 12.64 eingeblendet.

Meldung erzwingen

Sofern die Meldung nicht automatisch angezeigt wird, können Sie dies durch Eingabe von `napstat` auf der Kommandozeile erzwingen. Im Normalfall sollte das aber nicht notwendig sein.

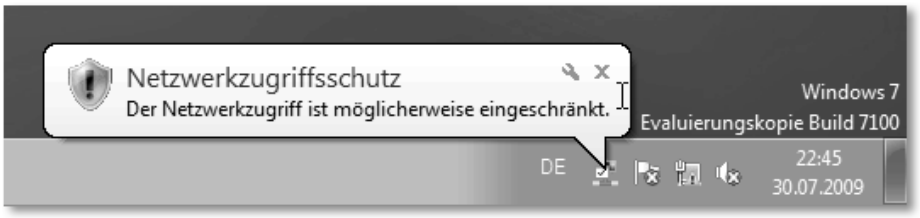


Abbildung 12.70 So sieht es aus, wenn der Client die Anforderungen nicht erfüllt.

Wenn Sie auf diese Meldung klicken, öffnet sich ein Dialog, der Sie darüber informiert, warum der Computer nur eingeschränkten Netzwerkzugriff erhält (Abbildung 12.71).

In Windows 7 werden Probleme, die den Netzwerkzugriffsschutz betreffen, im Wartungscenter angezeigt (Abbildung 12.72). Ein Klick auf LÖSUNG ANZEIGEN führt Sie übrigens zu dem Dialog aus Abbildung 12.71.

Das Wartungscenter erreichen Sie über die SYSTEMSTEUERUNG und deren Rubrik SYSTEM UND SICHERHEIT.

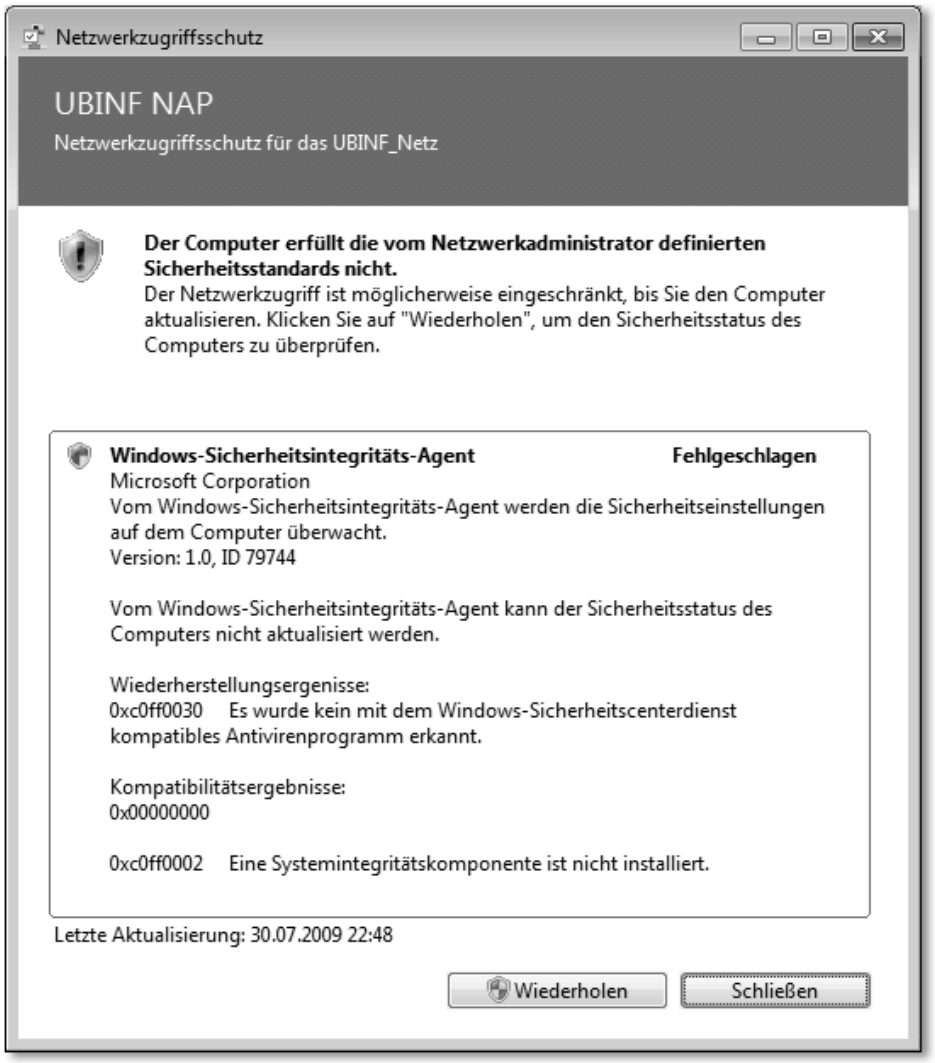


Abbildung 12.71 Diese Probleme führen dazu, dass der Computer nur eingeschränkten Netzwerkzugriff erhält.

Interessant ist, bei einem Computer mit eingeschränktem Netzwerkzugriff die IP-Konfiguration anzuschauen. Abbildung 12.73 zeigt ein `ipconfig /all`:

- Zunächst fällt natürlich der Eintrag `Systemquarantänestatus` ins Auge. Dieser steht auf `Eingeschränkt`.
- Außerdem ist die Subnetzmaske interessant. Bei dieser sind alle Bits gesetzt, also 255.255.255.255. Der Grund hierfür ist, dass der PC sich nicht »normal« im Netz befinden darf – er ist ja schließlich nicht »gesund«. Im DHCP-ACK-Netzwerkpaket werden einige Routinginformationen übermittelt. Das zeige ich Ihnen ein wenig später im Netzwerkmonitor.
- Die DNS-Einträge, die zuvor in der eingeschränkten DHCP-Klasse vorgenommen worden sind, sind vorhanden.

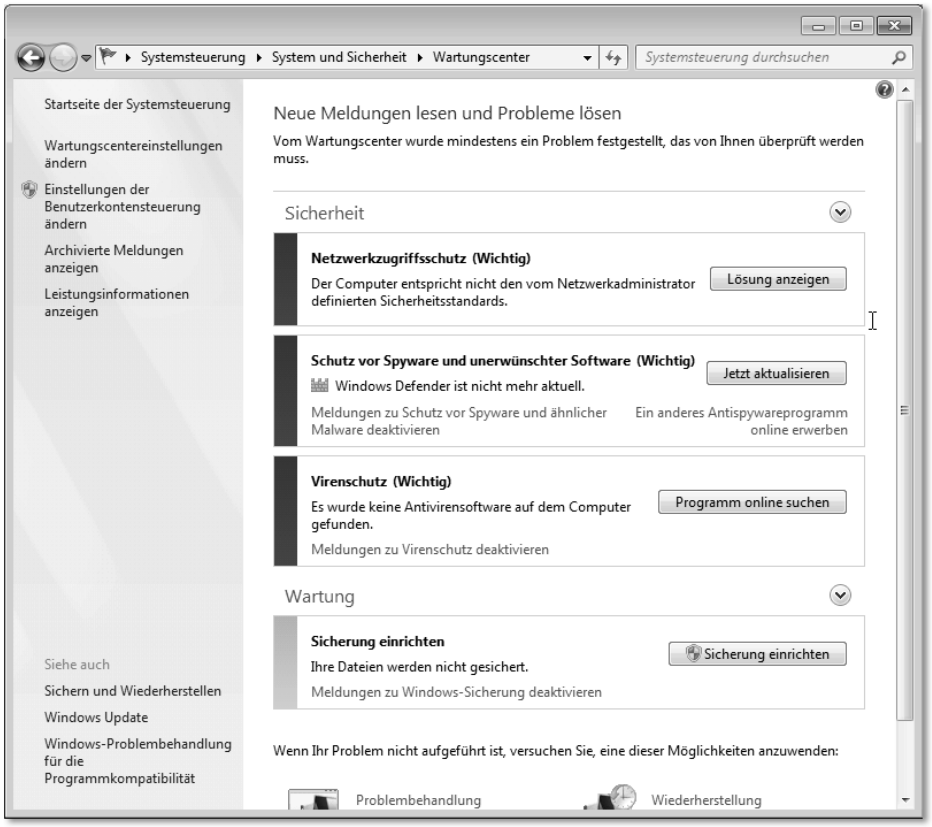


Abbildung 12.72 Im Wartungscenter werden Probleme beim Netzwerkzugriffsschutz angezeigt.

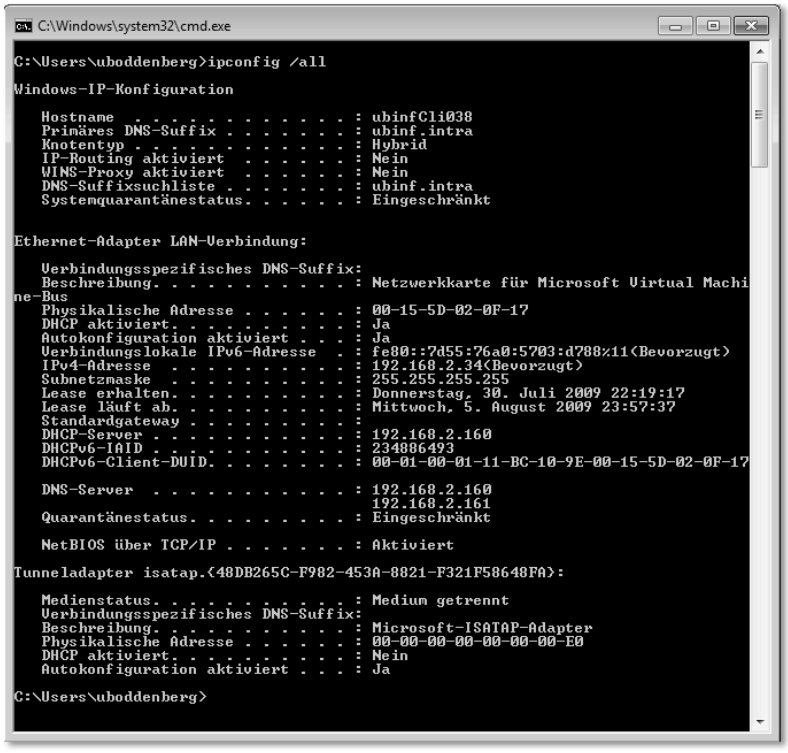


Abbildung 12.73 Die IP-Konfiguration eines Computers mit eingeschränktem Netzwerkstatus

In Abbildung 12.74 ist schließlich gezeigt, was passiert, wenn man unterschiedliche Systeme im Netz anpingt:

- Die als Wartungsserver angegebenen Systeme sind erreichbar,
- während es bei allen anderen Systemen zu Fehlermeldungen kommt.

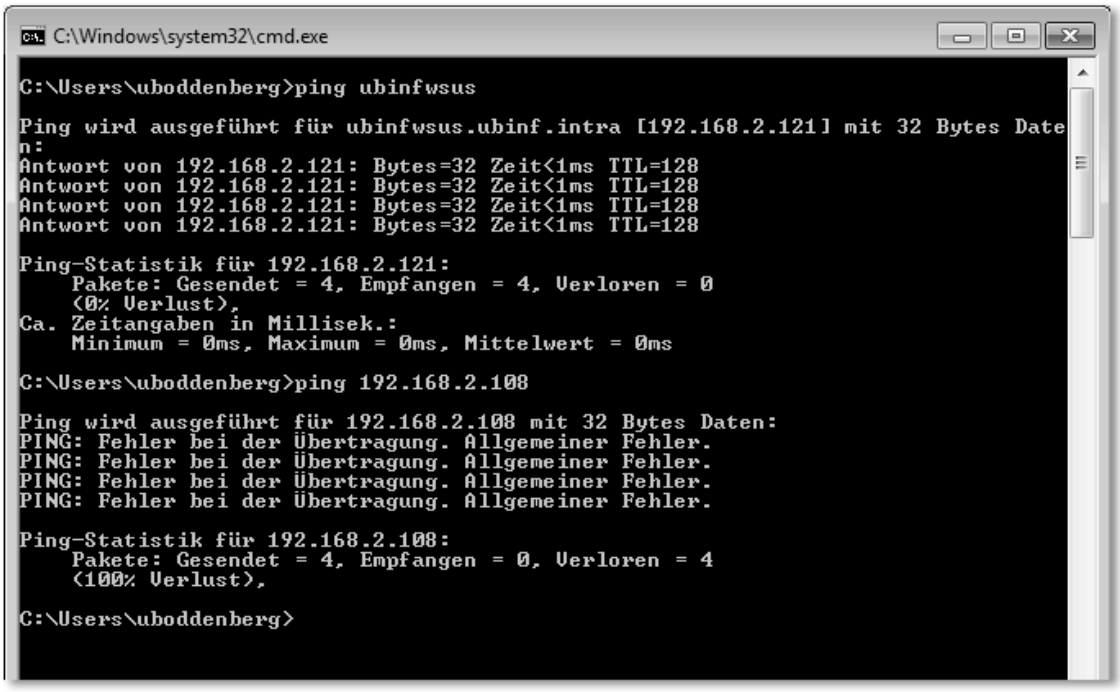


Abbildung 12.74 Die als Wartungsserver angegebenen Systeme können »angepingt« werden. Mit allen anderen ist keinerlei Kommunikation möglich.

Zum Abschluss möchte ich Ihnen noch vorführen, wie es aussieht, wenn der Computer die Netzwerkanforderungen erfüllt. In Abbildung 12.75 ist ein beruhigendes »Spruchband« zu sehen. Klickt man darauf, erscheint der bereits aus Abbildung 12.71 bekannte Dialog. Dieses Mal wurden vom Netzwerkrichtlinienserver aber keine Kritikpunkte übermittelt. Sie sehen stattdessen ein Häkchen, das »alles okay« signalisiert (Abbildung 12.76).

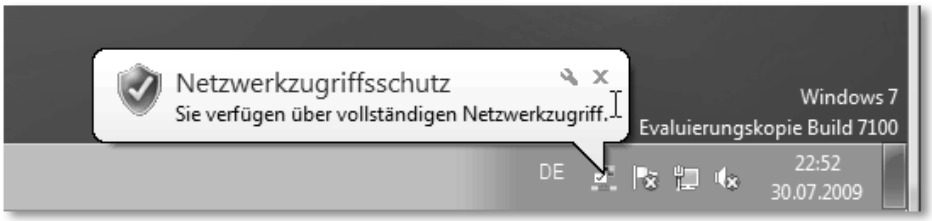


Abbildung 12.75 Wunderbar: Der Computer erfüllt die Netzwerkanforderungen.

Der Vollständigkeit halber sehen Sie auf Abbildung 12.77 noch einen kurzen Blick in die Netzwerkkonfiguration.

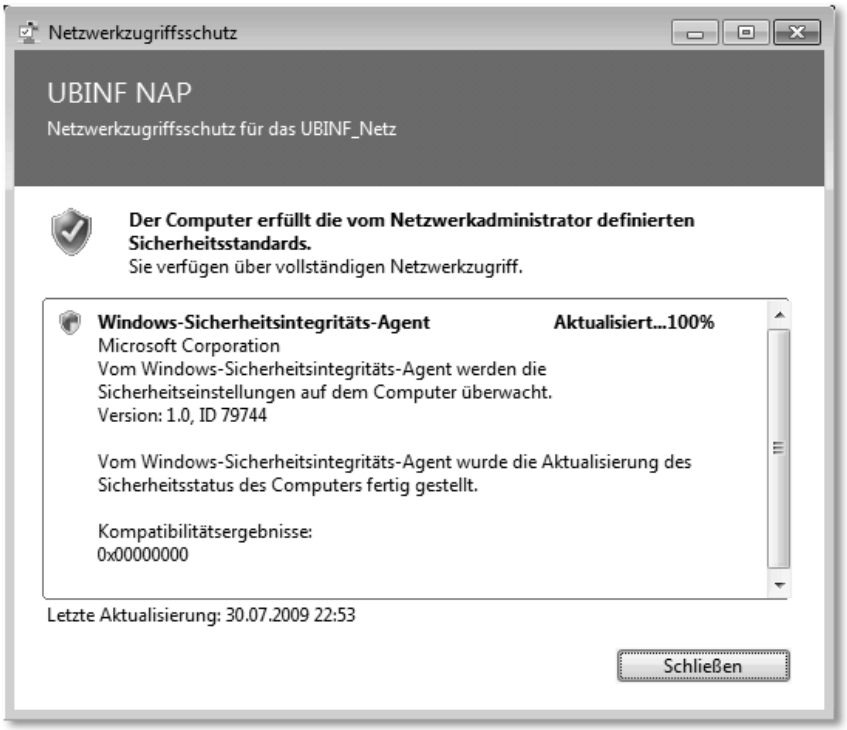


Abbildung 12.76 Im Gegensatz zu ist jetzt alles in Ordnung.

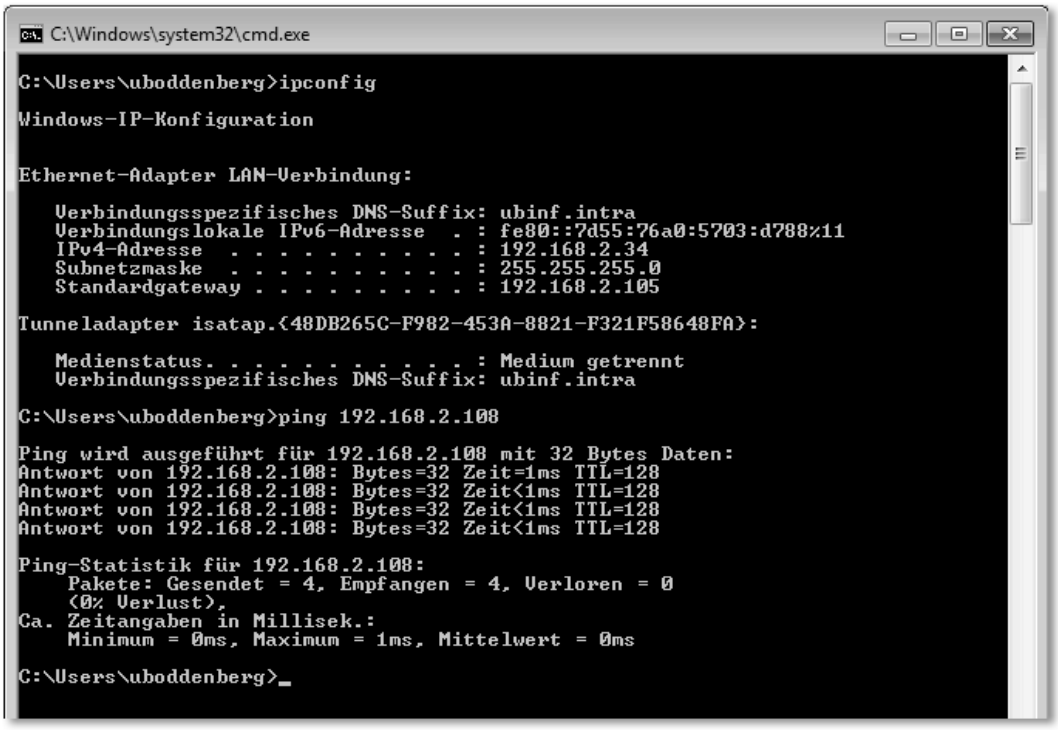


Abbildung 12.77 Die Subnetzmaske ist jetzt eine »normale« Class-C-Maske, und alle Hosts sind erreichbar.

Zunächst fällt auf, dass die Subnetzmaske eine »normale« Class-C-Maske ist. Außerdem ist das Standard-Gateway gesetzt, was für die eingeschränkte DHCP-Benutzerklasse nicht gesetzt war (vergleiche Abbildung 12.78). Außerdem kann wieder mit jedem Host kommuniziert werden, was in Abbildung 12.74 auch nicht möglich war: Es ist also alles wieder »normal«.

Hinweis zur Sicherheit

Wie ich bereits eingangs erwähnt habe, schützt DHCP-NAP nicht vor vorsätzlichem Missbrauch, denn ein PC könnte mit einer statischen IP-Adresse versehen werden und so den gesamten Mechanismus umgehen.

Da ein »normaler« Benutzer dazu aber keine Berechtigungen haben sollte (keine lokalen Admin-Rechte) und im günstigsten Fall die entsprechenden Konfigurationsdialoge ohnehin ausgeblendet sind, kann auch DHCP-NAP nicht so ohne Weiteres umgangen werden.

Festzuhalten bleibt, dass es recht einfach einzuführen und dabei durchaus wirksam ist.

Betrachtung mit dem Netzwerkmonitor

Falls Sie noch ein wenig hinter die Kulissen von DHCP-NAP schauen möchten, habe ich mit dem Netzwerkmonitor die DHCP-Kommunikation zwischen einem Client, der sich als nicht kompatibel herausstellt, und dem Server aufgezeichnet. Im Grunde genommen ist das ein »ganz normaler« DHCP-Vorgang, der aus den bekannten vier Phasen (DISCOVER, OFFER, REQUEST, ACK) besteht.

In Abbildung 12.78 sehen Sie das vom Client versendete DHCP-DISCOVER-Paket. Im Abschnitt VendorSpecificInformation, der vom Netzwerkmonitor leider nicht aussagekräftiger dargestellt werden kann, findet sich das SSoH (System State of Health), also die Informationen über den »Gesundheitszustand« des Clients. Im Klartext heißt das, dass ein NAP-aktivierter Client bereits zu Beginn des DHCP-Vorgangs seine Statusinformationen an den Server übermittelt. Da der Client zu diesem Zeitpunkt keine IP-Adresse hat, gibt es ja eigentlich auch keine andere Chance, als über diesen Weg die Informationen auszutauschen.

Interessant ist dann noch das DHCP-ACK-Paket, mit dem der Server dem Client die Bestätigung über die Vergabe der Adresse und diverse Konfigurationsdetails liefert. Abbildung 12.79 zeigt einen Blick in dieses Paket:

- In der zweiten Zeile der Frame Details ist die 255.255.255.255-Subnetzmaske zu erkennen, auf die ich Sie bereits in Abbildung 12.73 aufmerksam gemacht habe. Mit so einem Paket befindet sich der Client eigentlich auf einer einsamen Insel (zumindest IP-mäßig), weil er sich sozusagen in einem Ein-Host-Netz befindet, das keinerlei Verbindung zur Außenwelt hat.
- Dass der Client die Wartungsserver erreichen kann, wird dadurch ermöglicht, dass diese mit klassenlosen statischen Routen (ClasslessStaticRoute) angegeben sind.

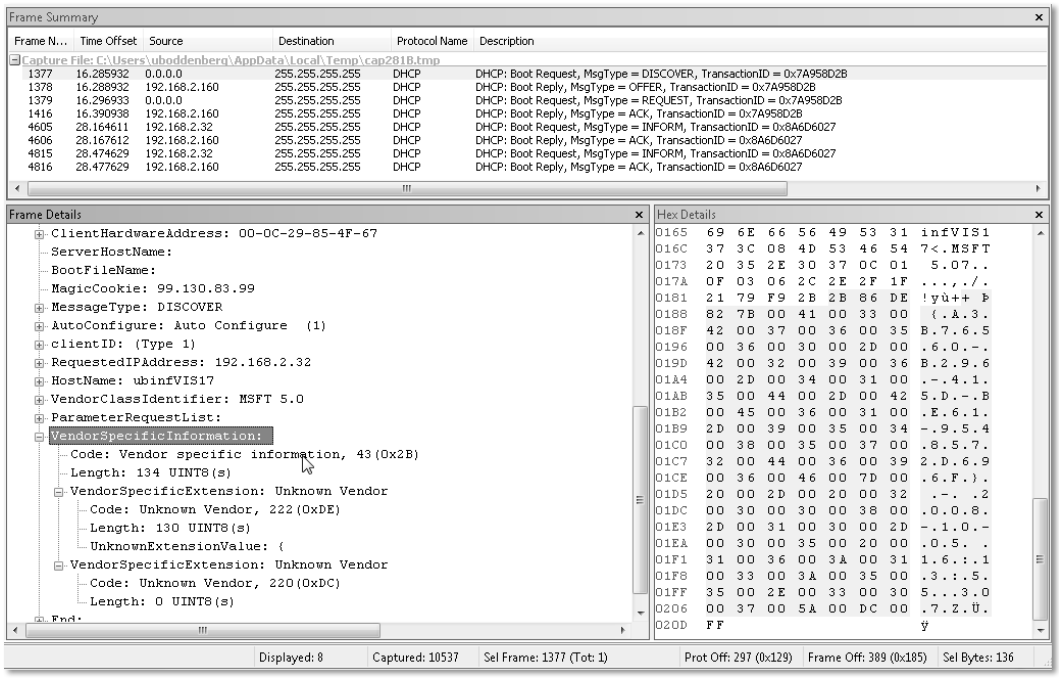


Abbildung 12.78 Das DHCP-DISCOVER-Paket enthält in den »VendorSpecificInformation« das SSoH (System State of Health).

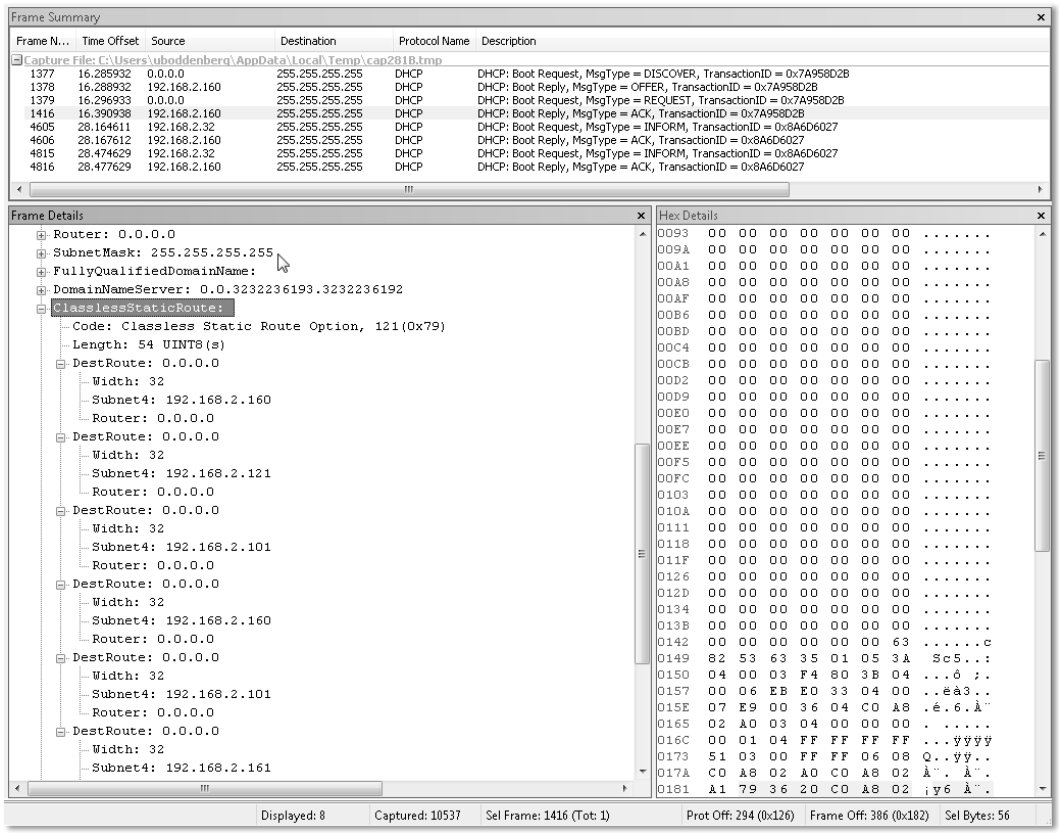


Abbildung 12.79 Im DHCP-ACK-Paket für einen nicht kompatiblen Client sind unter anderem die 255.255.255.255-Subnetzmaske und die klassenlosen statischen Routen zu den Wartungsservern zu erkennen.

12.3.6 Und die anderen Netzwerkverbindungsmethoden?

DHCP ist nun bekanntlich nicht die einzige Netzwerkverbindungsmethode, die mit NAP »ausgerüstet« werden kann (Abbildung 12.80).

Ich möchte nun aber einfach aus Gründen der zu erwartenden Seitenzahl dieses Buchs nicht jedes Szenario en detail vorführen, zumal die Konfiguration teilweise deutlich komplexer als beim DHCP-NAP ist.

Mein Ziel ist, dass Sie grundsätzlich verstehen, was man mit NAP umsetzen kann, und dass Sie ein erstes Gefühl dafür bekommen, wie die Umsetzung erfolgt. Sie werden nun in der Lage sein, mithilfe der Microsoft-Dokumentation die anderen Netzwerkverbindungsmethoden zur Verwendung mit NAP zu konfigurieren. Die Startseite für die Beschäftigung mit NAP ist *http://www.microsoft.com/technet/network/nap/default.mspx.*

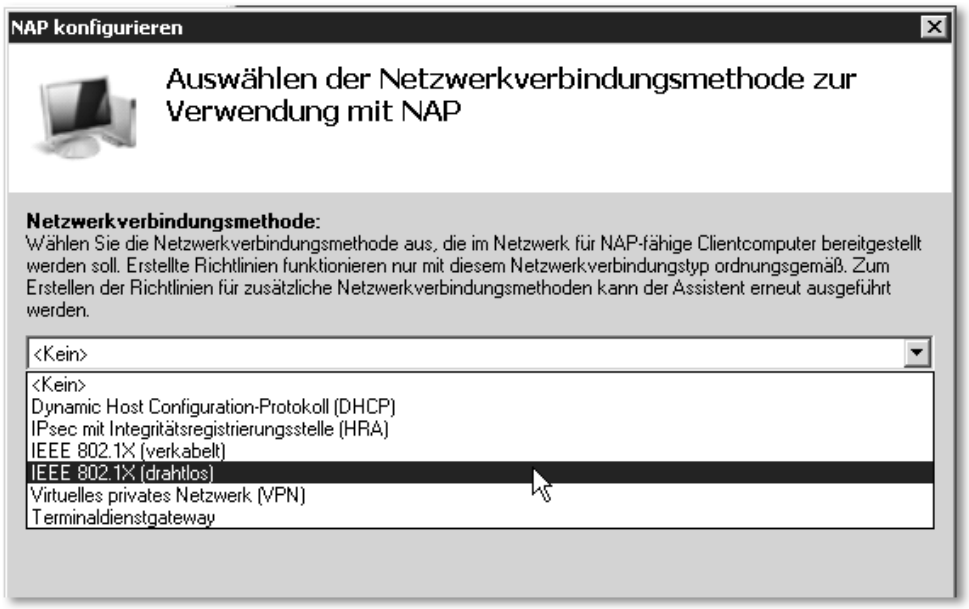


Abbildung 12.80 Der Assistent kann auch die Grundkonfiguration für diverse andere Netzwerkverbindungsmethoden erstellen.

12.4 Windows-Firewall

Eine im Betriebssystem integrierte Firewall ist ein naheliegender Gedanke. Da kaum jemand sich sicher sein kann, ob im Innenbereich des Netzes wirklich kein Schadcode (Viren, Trojaner etc.) ausgeführt wird, ist eine zusätzliche Schutzschicht sinnvoll, um das Risiko für die Server weitmöglichst zu minimieren und darüber hinaus die Verbreitung von elektronischem Ungeziefer im lokalen Netz einzudämmen.

Bereits Windows XP enthielt eine Version der Windows-Firewall, die allerdings nicht gerade durch »granulare Konfigurierbarkeit« beeindruckte. Die in Windows 7 enthaltene Version ist deutlich erweitert worden.

Ist die Windows-Firewall nicht aktiviert, erscheint eine unübersehbare Meldung (Abbildung 12.81). Einen schnellen Überblick über den Status der Windows-Firewall erhalten Sie auch beim Blick in das Wartungscenter (Abbildung 12.82).

Abbildung 12.81 Ist die Windows-Firewall deaktiviert, erhalten Sie eine unübersehbare Meldung.

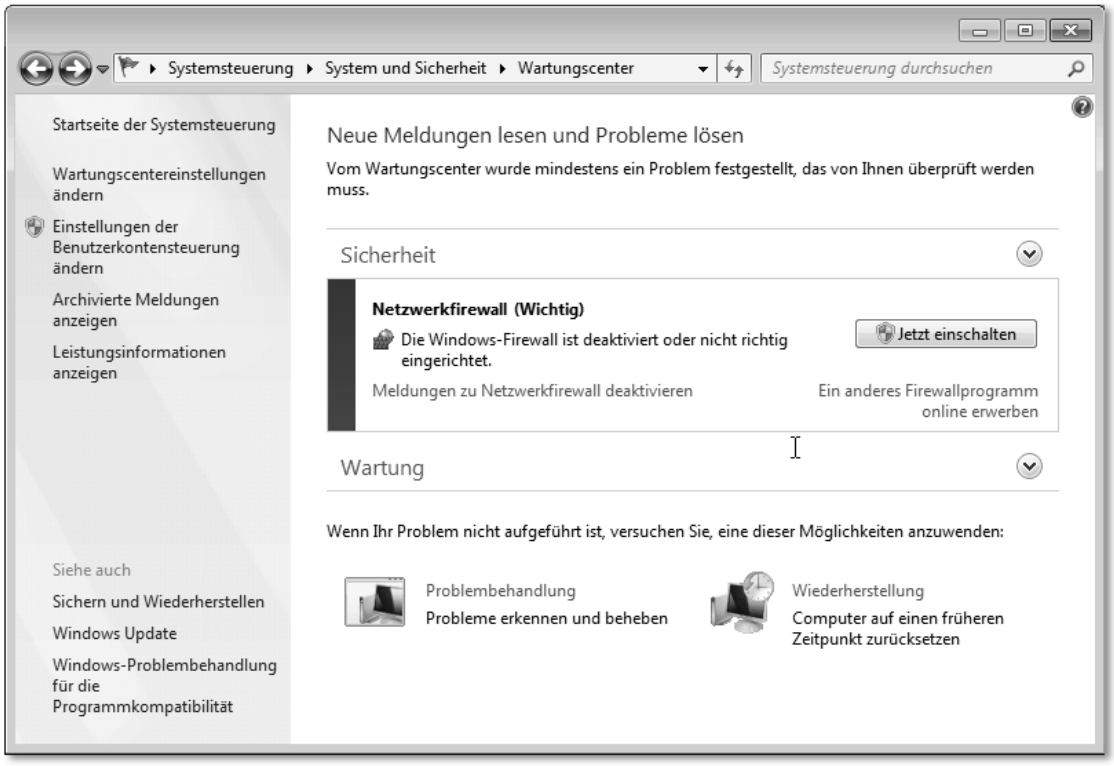


Abbildung 12.82 Wenn die Firewall-Konfiguration nicht in Ordnung ist, erscheint im Wartungscenter ein entsprechender Eintrag.

Die Windows-Firewall soll übrigens kein Ersatz für eine »richtige« Firewall sein, die am Internet-Gateway steht. Für solche Aufgaben kommen nach wie vor die »großen« Firewallsysteme wie *Cisco ASA* (vormals Pix) oder *CheckPoint FireWall-1* zum Einsatz, und auch der *Microsoft ISA Server 2006* eignet sich für dieses Aufgabengebiet. Die Windows-Firewall dient zur Absicherung des Servers gegen-

über dem LAN. Wie bereits erwähnt wurde, kann man auch in einem LAN, das durch Firewalls gegenüber dem Internet abgesichert ist, nicht von der »totalen Sicherheit« ausgehen. Mögliche Problempunkte sind:

- Es sind immer Angriffe aus dem LAN denkbar. Diese können entweder durch zu neugierige Benutzer (die irgendwelche aus dem Internet beschafften Werkzeuge ausprobieren) oder eingeschleuste Viren/Trojaner ausgelöst werden.
- Viele Firmen verfügen nach wie vor über Remote-Einwahlmöglichkeiten, um Wartungszugänge per Modem- oder ISDN-Verbindung bereitzustellen. Diese Einwahlpunkte sind teilweise grauenhaft schlecht abgesichert, weil sie häufig »mal eben schnell« umgesetzt worden sind. Erschwerend kommt hinzu, dass sie im VPN-Zeitalter häufig einfach vergessen werden. Jemand, der mit einem War-Dialer (einem Programm, das sequenziell alle Telefonnummern anruft und schaut, ob ein Modem/ISDN-Gerät reagiert) eine solche schlecht gesicherte Einwahlmöglichkeit findet, befindet sich mit etwas Glück im Innenbereich des Netzes.
- Die Möglichkeit, dass die Firewall am Internet-Gateway überwunden werden könnte, ist natürlich auch zu betrachten. Im Gegensatz zu den beiden zuvor genannten Varianten erscheint mir dies aber weniger wahrscheinlich. Die meisten Firmen haben das Internet-Gateway mittlerweile recht gut im Griff.

12.4.1 Erster Kontakt

Wenn Sie über die Systemsteuerung die Konfiguration der Windows-Firewall aufrufen, gelangen Sie zu dem auf Abbildung 12.83 gezeigten Dialog. Im Vergleich zur Windows-Firewall unter Vista fällt sofort ins Auge, dass separate Status für drei Netzwerkstandorte angezeigt werden. Wie man sieht, gibt es drei mögliche Standorte, nämlich:

- Der Computer ist mit der Domäne des Unternehmens verbunden.
- Der Computer befindet sich in einem privaten geschützten Netz, beispielsweise im Homeoffice neben einem DSL-Firewall-Router.
- Der Computer befindet sich an einem öffentlichen Ort, z. B. an einem WLAN-Hotspot.

Wenn Sie das erste Mal mit einem neuen Netz verbunden sind, wird Windows 7 fragen, welchem Netzwerkstandort es zugeordnet werden soll (die Festlegung kann übrigens im Netzwerk- und Freigabecenter geändert werden). Wie auch in Vista existiert für jeden Netzwerkstandort ein eigenes Profil – neu ist allerdings, dass mehrere Profile gleichzeitig aktiv sein können. Bei Vista wurde, wenn zwei Netzwerke aktiv waren, das Profil mit den höheren Restriktionen verwendet.

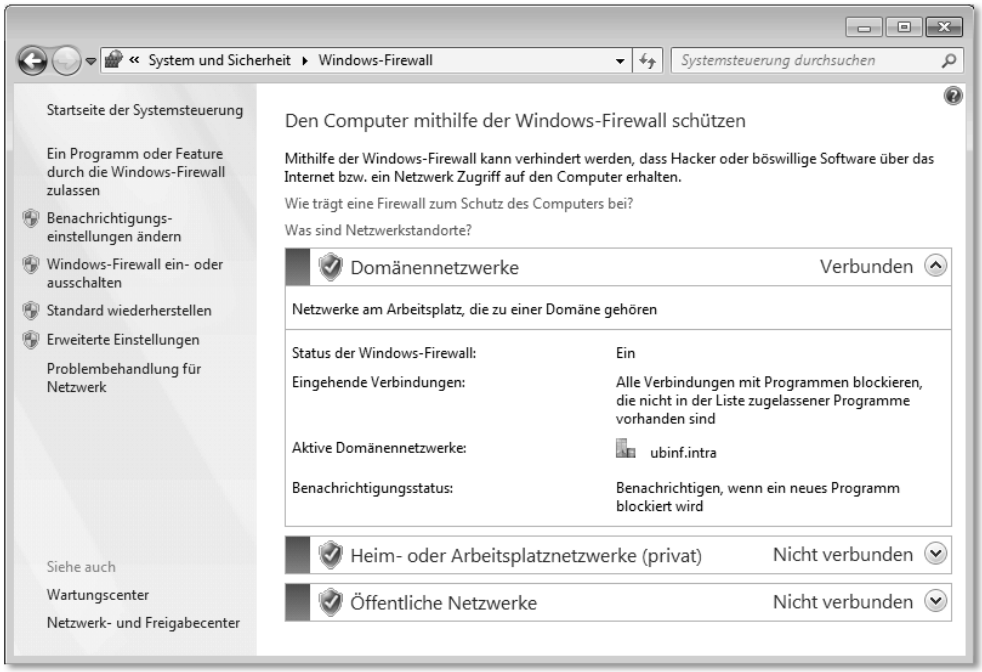


Abbildung 12.83 Der Einstiegsdialog für die Konfiguration der Windows-Firewall in Windows 7

Auf Abbildung 12.84 ist zu sehen, dass für jeden Standort separate Grundeinstellungen definiert werden können.

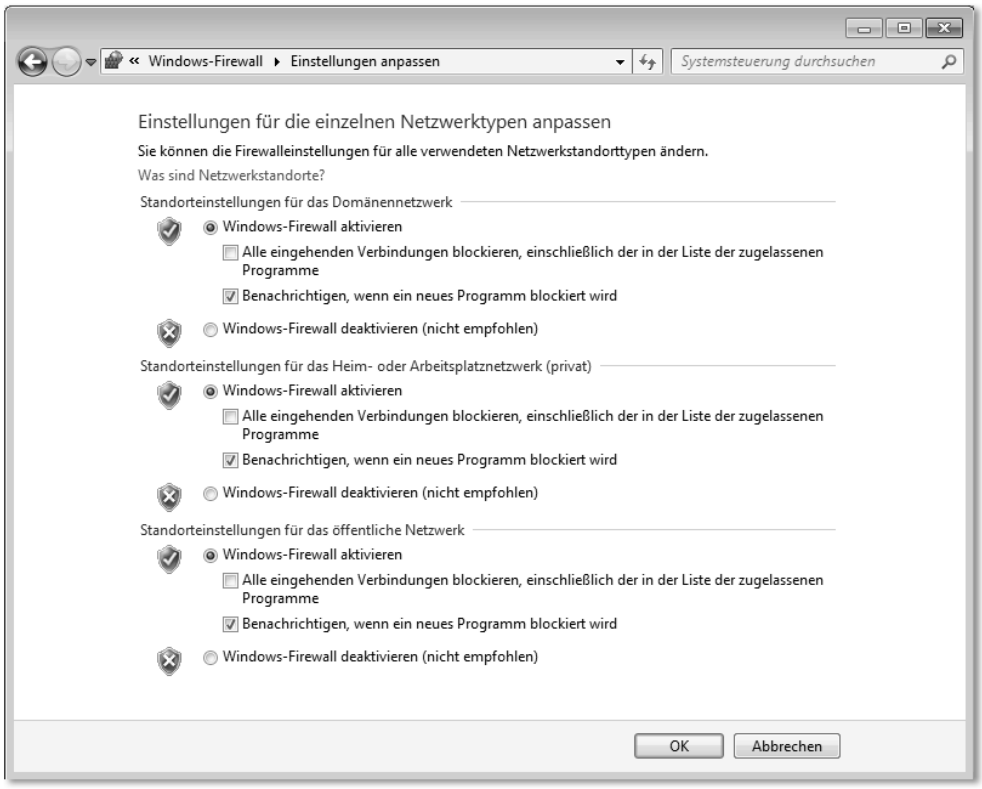


Abbildung 12.84 Die Windows-Firewall kann für die drei Netzwerkstandorte separat aktiviert/deaktiviert werden.

Weiterhin kann die Windows-Firewall für jeden Netzwerkstandort einzeln aktiviert/deaktiviert werden. Die Abbildung zeigt die Standardeinstellung: Die Windows-Firewall ist also für alle Netzwerkstandorte aktiv. Für jeden Standort können Sie übrigens ein eigenes Regelwerk erstellen, was Sie im Verlauf des Kapitels sehen werden.

12.4.2 Grundkonfiguration

Wenn Sie auf dem Startdialog der Windows-Firewall aus Abbildung 12.83 den Menüpunkt Erweiterte Einstellungen wählen, gelangen Sie zu dem Snap-In Windows-Firewall mit erweiterter Sicherheit. Der Wurzeleintrag des Baums verfügt im Kontextmenü über einen Menüpunkt Eigenschaften, der zu dem Dialog aus Abbildung 12.85 führt. Dieser Dialog enthält für jeden Netzwerkstandort eine separate Registerkarte, auf der die zugehörigen Grundeinstellungen vorgenommen sind. Kurz gesagt gilt standardmäßig immer:

- Eingehende Verbindungen werden blockiert, es sei denn, es sind anderslautende Einträge im Regelwerk vorhanden.
- Ausgehende Verbindungen werden zugelassen, es sei denn, es sind anderslautende Einträge im Regelwerk vorhanden.

Diese Einstellungen dürften für Clientsysteme (wir sind ja hier in einem Windows 7-Buch) sehr geeignet sein: Allzu viel Mühe werden Sie vermutlich mit der Windows-Firewall im Clientumfeld ohnehin nicht haben, da eingehende Verbindungen, die manuell konfiguriert werden müssen, ja eher die Ausnahme sein dürften.

Sie können einige weitere Einstellungen in einem Dialog vornehmen, den Sie über die Schaltflächen Anpassen aufrufen. Dort gibt es zwei interessante Einstellmöglichkeiten (Abbildung 12.86):

- Die Windows-Firewall kann Benutzer benachrichtigen, wenn eine Applikation versucht, auf eingehende Anforderungen zu lauschen, diese aber geblockt werden. Für einen »normalen« Benutzer sollte diese Option herzlich uninteressant sein, da die benötigten offenen Ports vom Administrator (über Gruppenrichtlinien) definiert werden. Für IT-Professionals oder Entwickler, die neue Software testen, ist eine solche Warnung hingegen von hohem Interesse.
- Unicastantwort: Falls ein Computer eine Broadcast-Message versendet, ist nicht genau vorhersehbar, welche anderen Computer antworten werden. Durch das Aktivieren der Option Unicastantwort zulassen wird die Windows-Firewall so konfiguriert, dass nach einer von diesem Computer versendeten Broadcast-Message drei Sekunden lang eingehende Antworten akzeptiert werden.

  Ob ein System generell darauf angewiesen ist, über Broadcasts zu kommunizieren, sei dahingestellt. Falls dies in einem Szenario der Fall sein sollte, hält die Windows-Firewall eine pragmatische Lösung bereit.

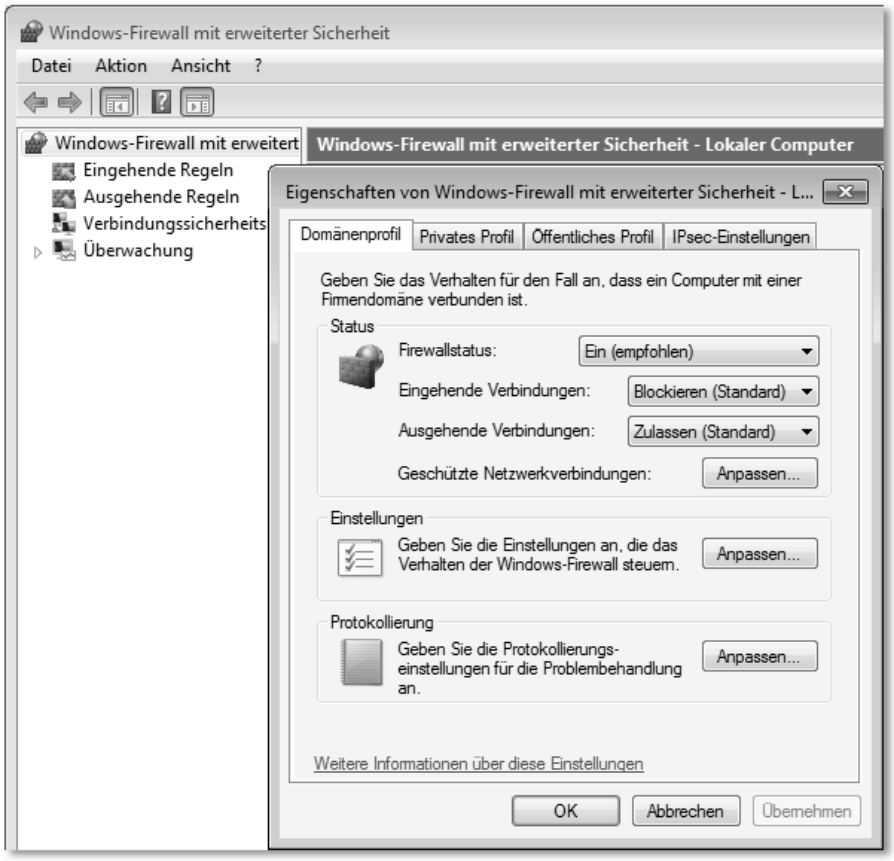


Abbildung 12.85 Die Grundkonfiguration nehmen Sie in diesem Dialog vor.

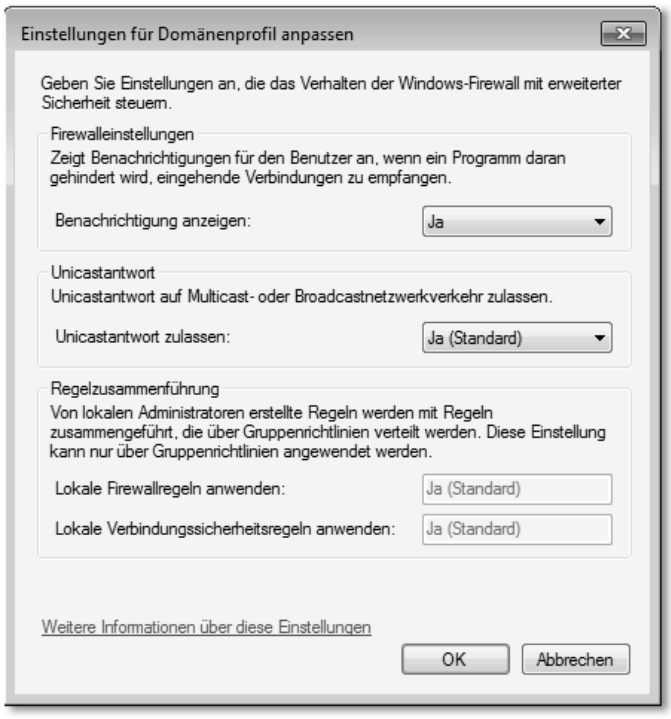


Abbildung 12.86 Einige spezielle Einstellungen der Windows-Firewall können Sie mit diesem Dialog vornehmen.

12.4.3 Regeln verwalten und definieren

Mit der Konfiguration von Windows-Firewall-Regeln haben im Allgemeinen eher die Serveradministratoren als die Clientadmins zu tun. Der Grund dafür ist, dass Server im Allgemeinen jede Menge eingehenden Datenverkehr haben, während dies auf Clients eher die Ausnahme ist. Aber auch auf Clients kann es durchaus eingehenden Datenverkehr geben, der über die Grundeinstellungen hinaus zugelassen werden muss. Der »Klassiker« sind Clients von Systemmanagement-Anwendungen, bei denen der Server Verbindung mit den Clients aufnehmen muss. Auch immer gern genutzt sind Fernsteuerungsprogramme, die zum Support bei Benutzerproblemen eingesetzt werden.

Da die Definition von eingehenden Regeln auf Clientsystemen eher eine »Nischenaufgabe« ist, werde ich hier nicht auf alle Details eingehen. Ebendies gilt übrigens auch für Aspekte wie das Annehmen von IPSec-Verbindungen und dergleichen mehr.

Überblick

Im Konfigurations-Snap-In der Windows-Firewall finden Sie einen Knoten für Eingehende Regeln und einen für Ausgehende Regeln. Ein erster Blick auf die Regeln bringt folgende Erkenntnisse (Abbildung 12.87):

- Es sind viele Regeln enthalten, allerdings sind nur wenige aktiv.
- Teilweise sind Regeln mehrfach vorhanden. In diesem Fall unterscheiden sie sich bezüglich des Profils (Netzwerkstandorts), für das sie Gültigkeit haben.

Die Liste mit den Regeln lässt sich einerseits mehr oder weniger beliebig sortieren, andererseits gibt es auch die Möglichkeit, Filter anzuwenden. Wenn Sie sich beispielsweise einen Überblick über alle Regeln machen möchten, die für das öffentliche Profil vorhanden sind, aktivieren Sie einfach den Filter aus Abbildung 12.88.

An dieser Stelle noch ein Hinweis: Diejenigen, die mit »normalen« Firewalls (sei es beispielsweise eine Cisco ASA/PIX, CheckPoint oder ISA Server) arbeiten, werden sich vielleicht wundern, dass es überhaupt die Möglichkeit gibt, die Regeln zu sortieren. Bei »normalen« Firewalls gibt es ja nur ein Sortierkriterium, nämlich die Abarbeitungsreihenfolge. Diese spielt bei der Windows-Firewall keine Rolle. Dies ist in diesem Anwendungsfall auch kein Problem (sonst hätte Microsoft das Thema ja vermutlich auch integriert) – für alte Firewall-Hasen, die erstmalig mit der Windows-Firewall zu tun haben, ist es vielleicht aber etwas ungewohnt.

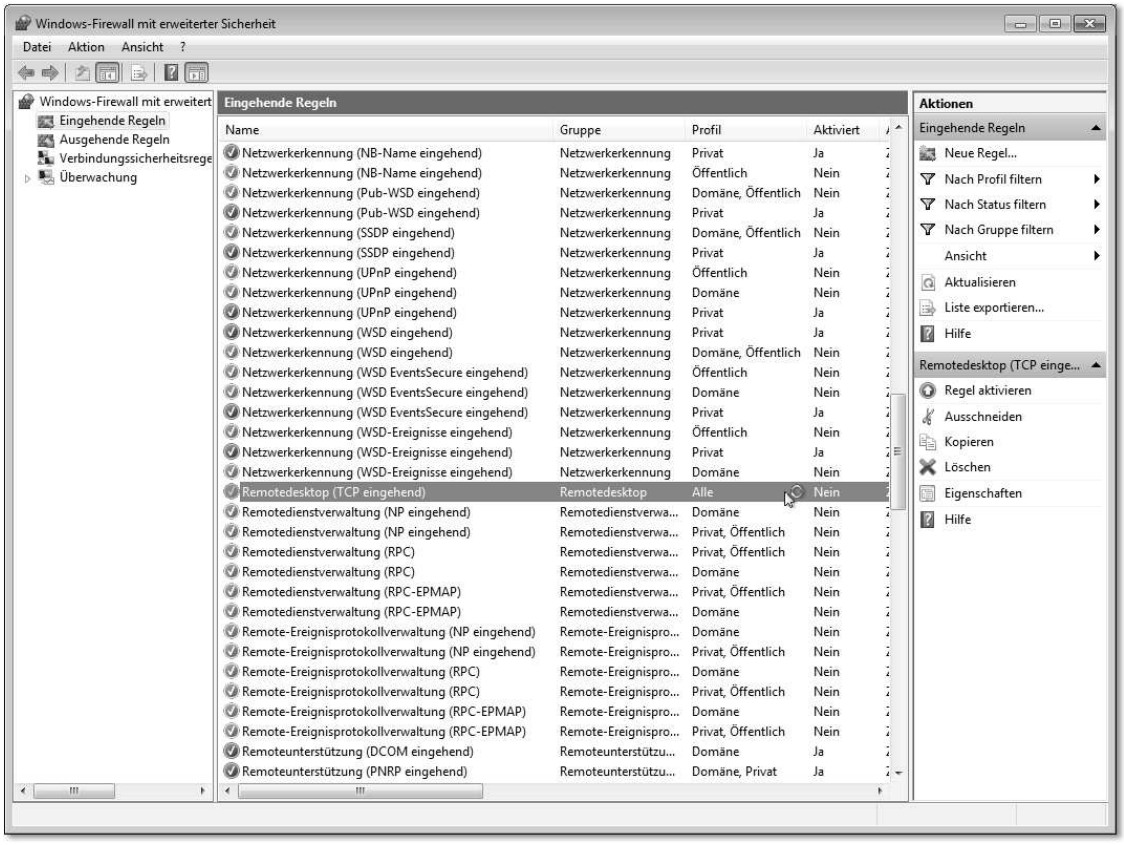


Abbildung 12.87 Die Liste der standardmäßig vorhandenen eingehenden Regeln

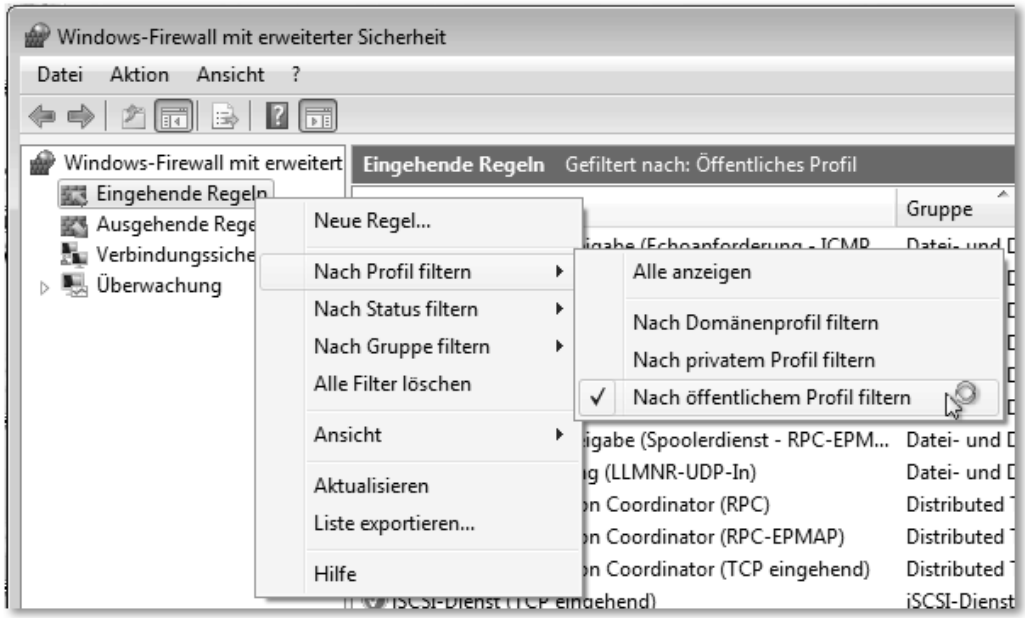


Abbildung 12.88 In der täglichen Arbeit sind die Filtermöglichkeiten recht wertvoll.

Eine Regel im Detail

Ein Gefühl für die Möglichkeiten der Windows-Firewall erhalten Sie am ehesten, wenn Sie eine Regel exemplarisch untersuchen. Ich werde das in diesem Buch am Beispiel der Regel für den Remotedesktop-Zugriff auf den Client vorführen. Dieser Zugriff geschieht standardmäßig über den TCP-Port 3389. Die Regel ist standardmäßig vorhanden, allerdings deaktiviert.

Abbildung 12.89 zeigt links die erste Registerkarte des EIGENSCHAFTEN-Dialogs einer Regel. Sie sieht irgendwie unscheinbar aus, allerdings findet sich unter der Überschrift AKTION die wichtigste Einstellmöglichkeit der Regel: Hier wird nämlich festgelegt, ob die Regel eine *Zulassungsregel* oder eine *Verweigerungsregel* (VERBINDUNG BLOCKIEREN) ist.

Es gibt noch eine dritte Möglichkeit, nämlich das *Zulassen einer sicheren Verbindung*. Was genau im Kontext dieser Regel eine sichere Verbindung ist, definieren Sie in dem Dialog aus Abbildung 12.90, den Sie über die Schaltfläche ANPASSEN erreichen:

- Standardmäßig wird eine authentifizierte und integritätsgeschützte (d. h. signierte) IPSec-Verbindung gefordert.
- Zusätzlich kann noch Verschlüsselung gefordert werden.
- Seit Windows 7 ist es möglich, eine authentifizierte, aber nicht integritätsgeschützte Verbindung vorzuschreiben.

Nur bei sicherer Verbindung

Ich möchte explizit darauf hinweisen, dass einige Optionen von Regeln nur angegeben werden können, wenn die Grundlage eine sichere Verbindung ist. Dies betrifft beispielsweise die Festlegung von Computern oder Anwendern, mit denen die Kommunikation explizit gestattet oder unterbunden wird.

Hintergrund ist, dass diese Aspekte nur ausgewertet werden können, wenn eine authentifizierte Verbindung vorhanden ist.

Auf Abbildung 12.89 können Sie rechts sehen, dass die Gültigkeit der Regel auf bestimmte Programme und/oder Dienste eingeschränkt werden kann.

Abbildung 12.91, rechts, zeigt die Einstellmöglichkeiten, die man von einer Firewall-Regel am ehesten erwartet, nämlich die Definition von Protokolltyp und Ports – viel mehr ist dazu zunächst auch nicht zu sagen.

Auf der Registerkarte, die Sie in Abbildung 12.91 links sehen, legen Sie fest, von welchen Computern die Verbindung aufgebaut werden kann und für welche die Regel keine Gültigkeit haben soll.

Um Missverständnisse zu vermeiden: Hier geht es nicht (!) um IP-Adressen, sondern wirklich um Computer (genau genommen um Computerkonten).

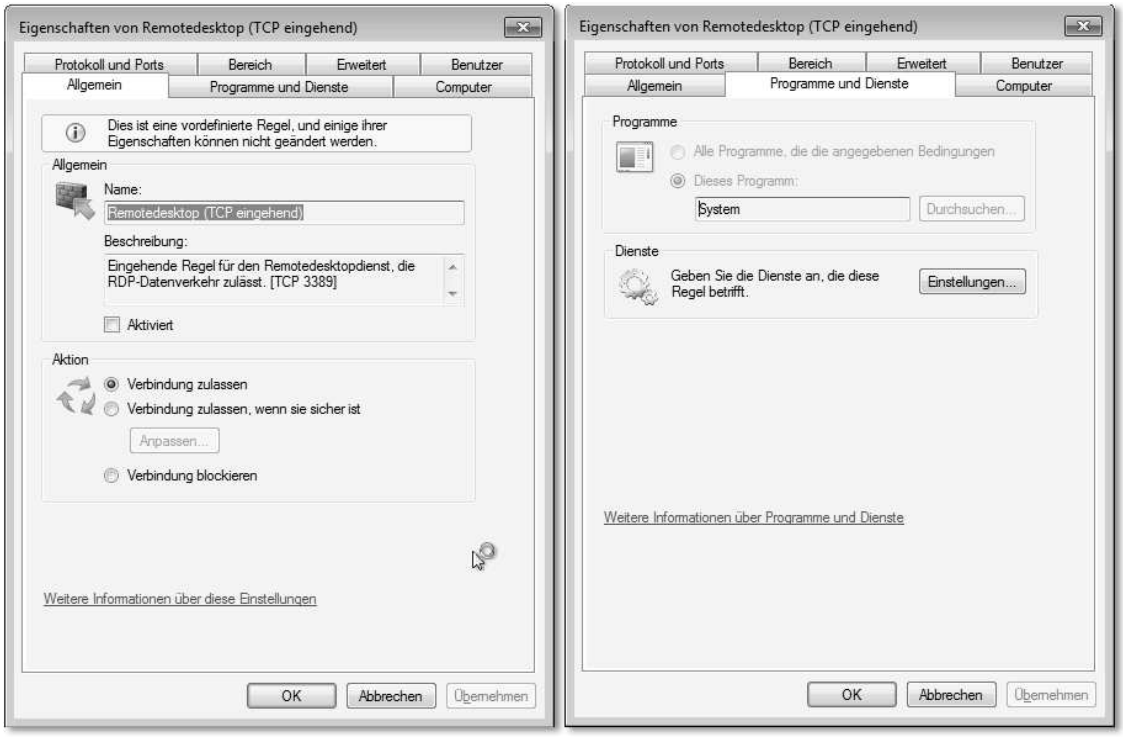


Abbildung 12.89 Die Regel für den Remotedesktop-Zugriff

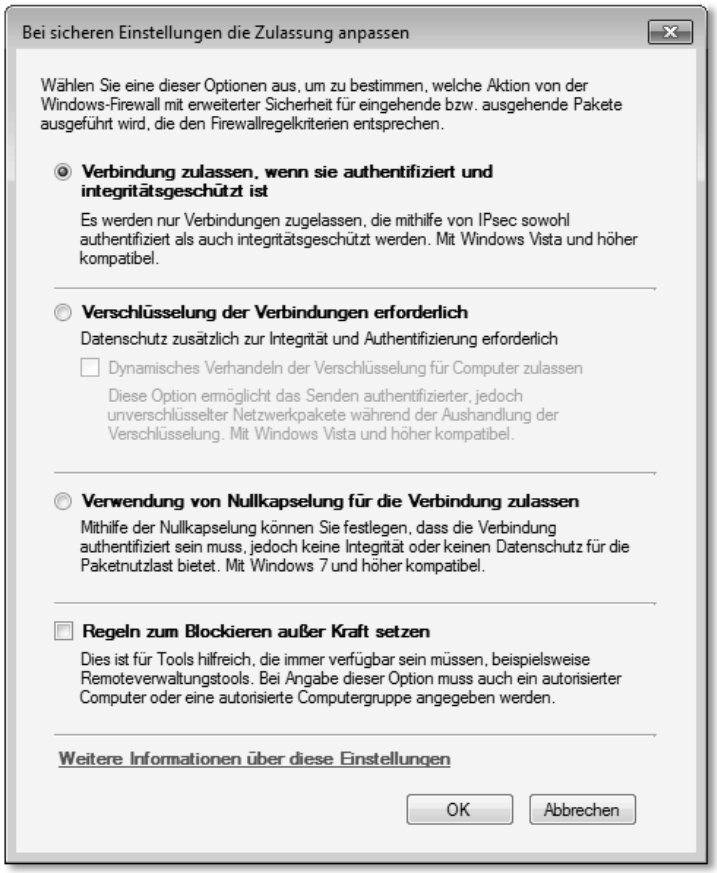


Abbildung 12.90 Die Einstellungen zur Definition einer sicheren Verbindung

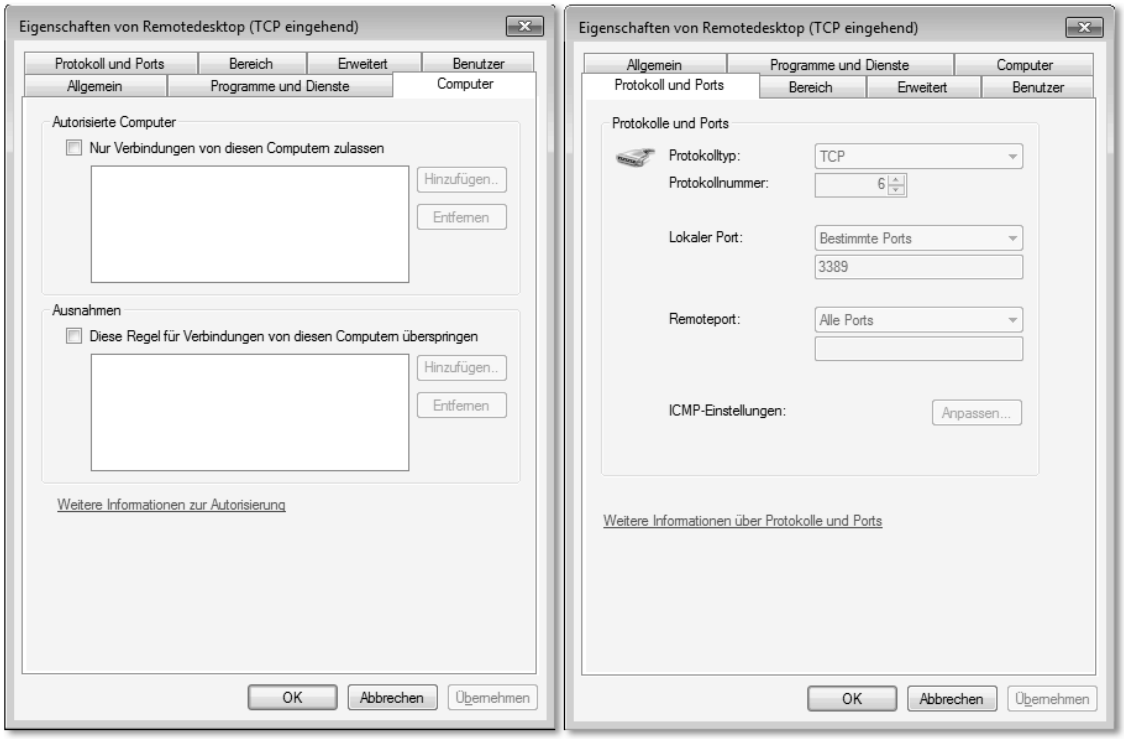


Abbildung 12.91 In einer Regel der Windows-Firewall lässt sich konfigurieren, dass die Regel nur für bestimmte Computer gilt.

Aus diesem Grund können die Einstellungen nur vorgenommen werden, wenn der Regel eine sichere Verbindung (siehe auch Abbildung 12.90) zugrunde liegt. Ist eine solche nicht konfiguriert, gibt es eine Warnmeldung, sobald die Checkbox selektiert wird.

Die Möglichkeit der Beschränkung auf bestimmte IP-Adressen finden Sie auf der Registerkarte BEREICH (Abbildung 12.92 links). Sie können hier sowohl die zu benutzenden lokalen IP-Adressen (des eigenen Computers) festlegen und natürlich auch diejenigen, die zugreifen dürfen. Neben einzelner Adressen sind auch Bereiche (von … bis) als Eingabewerte möglich.

Die Registerkarte ERWEITERT (Abbildung 12.92 rechts) enthält einige weitere Konfigurationsmöglichkeiten:

- Zunächst können Sie wählen, für welche Profile (also Netzwerkstandorte) die Regel Gültigkeit haben soll.
- Unter SCHNITTSTELLENTYPEN spezifizieren Sie, ob die Regel für LAN-, für Remote-Access- und/oder für WLAN-Verbindungen gelten soll.
- Mit der Checkbox mit der etwas drolligen Übersetzung RANDÜBERQUERUNG ZULASSEN legen Sie fest, ob der Datenverkehr, für den diese Regel gilt, »genattet« werden kann.

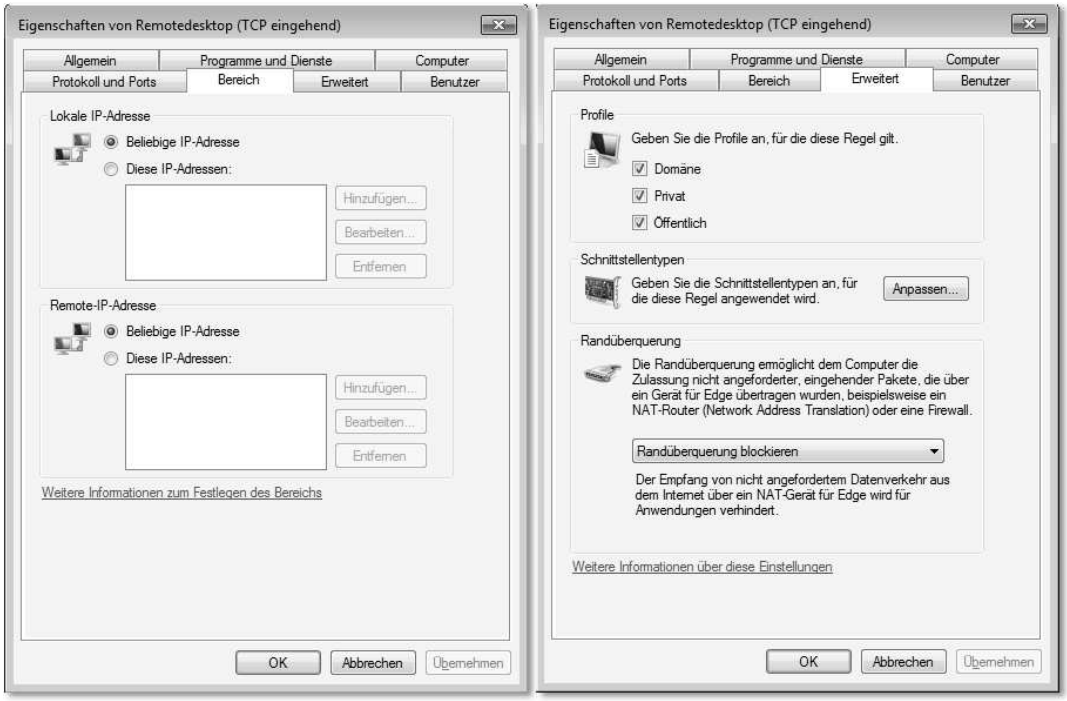


Abbildung 12.92 Auf diesen Registerkarten legen Sie unter anderem fest, mit welchen IP-Adressen kommuniziert wird (links) und für welche Profile diese Regel Gültigkeit haben soll.

Die letzte hier besprochene Registerkarte, nämlich Benutzer (Abbildung 12.93), dient zur Beschränkung des Zugriffs auf die hier angegebenen authentifizierten Benutzer.

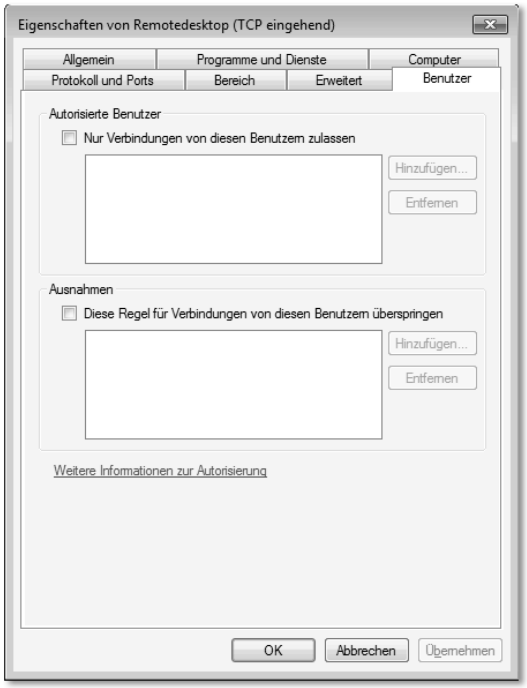


Abbildung 12.93 Es kann festgelegt werden, dass die Regel nur für die Zugriffe bestimmter Benutzer gilt.

Dies funktioniert, ähnlich wie die Einstellungen auf der Registerkarte Computer, nur dann, wenn eine sichere Verbindung (Abbildung 12.90) vorliegt.

Bei der Durchsicht der Optionen für eine Regel zeigt sich also, dass es erheblich mehr einzustellen gibt als nur IP-Adressen und Ports. Die Windows-Firewall ist recht eng mit dem Betriebssystem verwoben und nutzt entsprechend einige Möglichkeiten aus. Wie weit diese tatsächlich auf Clients relevant sind, dürfte von Fall zu Fall unterschiedlich sein.

12.4.4 Regel aktivieren (durch eine Applikation)

Grundsätzlich kann eine bereits vorhandene Regel mit den entsprechenden Menüpunkten des jeweiligen Kontextmenüs aktiviert und deaktiviert werden.

Häufig geht es aber auch komfortabler. Ich zeige Ihnen das am Beispiel der Aktivierung der Remotedesktop-Funktionalität. Beachten Sie, dass standardmäßig für eingehenden Remotedesktop-Zugriff eine deaktivierte Regel vorhanden ist (Abbildung 12.87 ff.)

Wenn Sie nun den Remotedesktop-Zugriff auf einen PC aktivieren möchten, müssen Sie die Funktionalität auf der Registerkarte Remote der Systemeigenschaften aktivieren (Abbildung 12.94).

Mit dem Aktivieren der Funktionalität allein ist es aber nicht getan, denn die Windows-Firewall gestattet standardmäßig keine TCP-Zugriffe auf den Port 3389 (den Standardport des RDP-Protokolls). Aus diesem Grund »bohrt« das Konfigurationsprogramm auch direkt ein passendes Loch in die Windows-Firewall und nimmt dabei eine kleinere Umbaumaßnahme vor. Wie Sie weiter vorn gesehen haben, ist für den Remotedesktop-Zugriff eine einzige Regel angelegt worden, die für alle drei Profile gilt und deaktiviert ist. Beim Aktivieren von Remotedesktop wird folgende Anpassung vorgenommen (Abbildung 12.95):

- Eine zweite Regel wird angelegt, die für die Profile Domäne und Privat gilt. Sie gestattet den Zugriff auf die aktivierte Remotedesktop-Funktionalität des PCs.
- Weiterhin vorhanden ist eine deaktivierte Zulassungsregel für das öffentliche Profil.

Anders gesagt verhindert die Windows-Firewall den Remotedesktop-Zugriff auf den PC, wenn sich dieser in einem öffentlichen Netz befindet – macht absolut Sinn, denke ich.

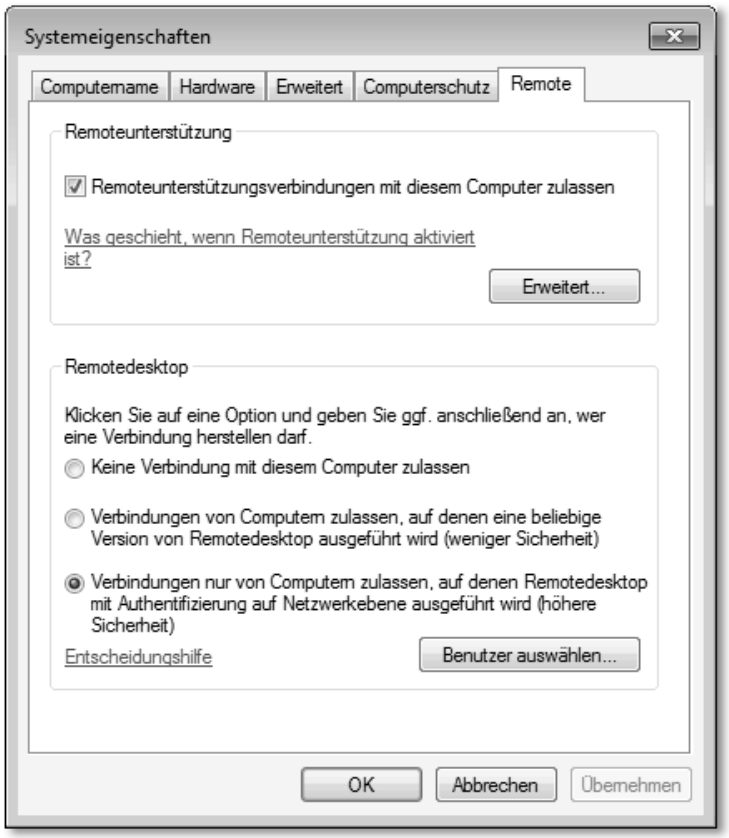


Abbildung 12.94 Aktivieren der Remotedesktop-Funktionalität

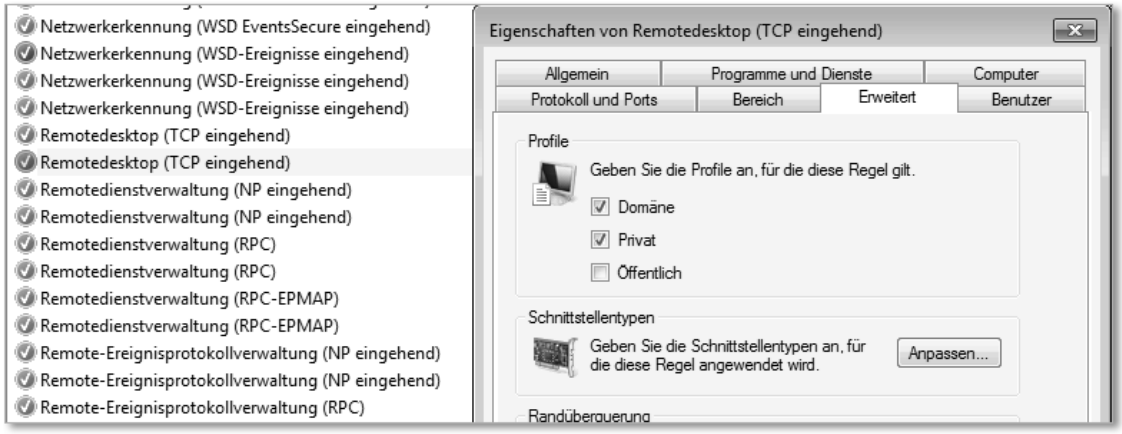


Abbildung 12.95 Bei der Aktivierung sind die Firewallregeln angepasst worden.

Hinweis

Generell gilt, dass eine moderne Applikation mit einem modernen Installationsprogramm heute davon ausgehen sollte, dass die Windows-Firewall auf einem PC aktiv ist und selbstständig die notwendigen Regeln hinzufügen und aktivieren.

Es kann aber nicht schaden, zu kontrollieren, wie die Modifikation aussieht. In dem Remotedesktop-Beispiel ist das durchaus sinnvoll umgesetzt – schließlich wird ein Remote-

desktop-Zugriff wohl kaum stattfinden, wenn der PC mit einem öffentlichen Netz verbunden ist. Er würde dann ein gefundenes Fressen für Portscanner.

Vermutlich wird eine solche Konfiguration auch bei den meisten Applikationen sinnvoll sein, die Ports für eingehende Verbindungen öffnen. Kontrollieren Sie aber besser, ob da nicht doch zu viel geöffnet worden ist, insbesondere im öffentlichen Profil.

12.4.5 Eine Regel selbst erstellen

Wenn Sie eine Regel benötigen, die nicht bereits vorhanden und lediglich deaktiviert ist, können Sie natürlich selbst eine solche erstellen. Eine beliebte Anforderung ist, dass Windows 7 zu Diagnosezwecken auf PINGs reagieren soll. Wie Sie auf Abbildung 12.96 sehen können, antwortet ein Windows 7-Client mit aktivierter Windows-Firewall standardmäßig nicht auf diese Anforderung.

Abbildung 12.96 Standardmäßig antwortet ein Windows 7-Client nicht auf PINGs.

Die Erstellung einer Regel geschieht wie gewohnt mit einem Assistenten, der über den Menüpunkt Neue Regel entweder im Knoten Eingehende Regeln oder Ausgehende Regeln – je nachdem, was erstellt werden soll – aufgerufen wird.

Auf der ersten Seite des Assistenten können Sie zwischen vier Regeltypen wählen (Abbildung 12.97). Die angebotenen Optionen sind weitgehend selbsterklärend:

- Sie können eine Regel erstellen, die die Kommunikation mit einem Programm erlaubt. Im nächsten Schritt wird der Assistent nach dem Pfad zu dem Programm fragen.
- Sie können eine Portregel erstellen und dabei einen bestimmten TCP- oder UDP-Port angeben.
- Die dritte Variante ist die Auswahl eines vordefinierten Regelwerks. Hier findet sich beispielsweise auch der Remotedesktop.
- Die Option Benutzerdefiniert ermöglicht eine absolut freie Auswahl, was die Definition der Regel betrifft.

Zum »Freischalten« der PING-Funktionalität müssen Sie die letzte Option (Benutzerdefiniert) wählen, da PING nicht auf dem TCP-Protokoll basiert – sondern eben ICMP-basiert ist.

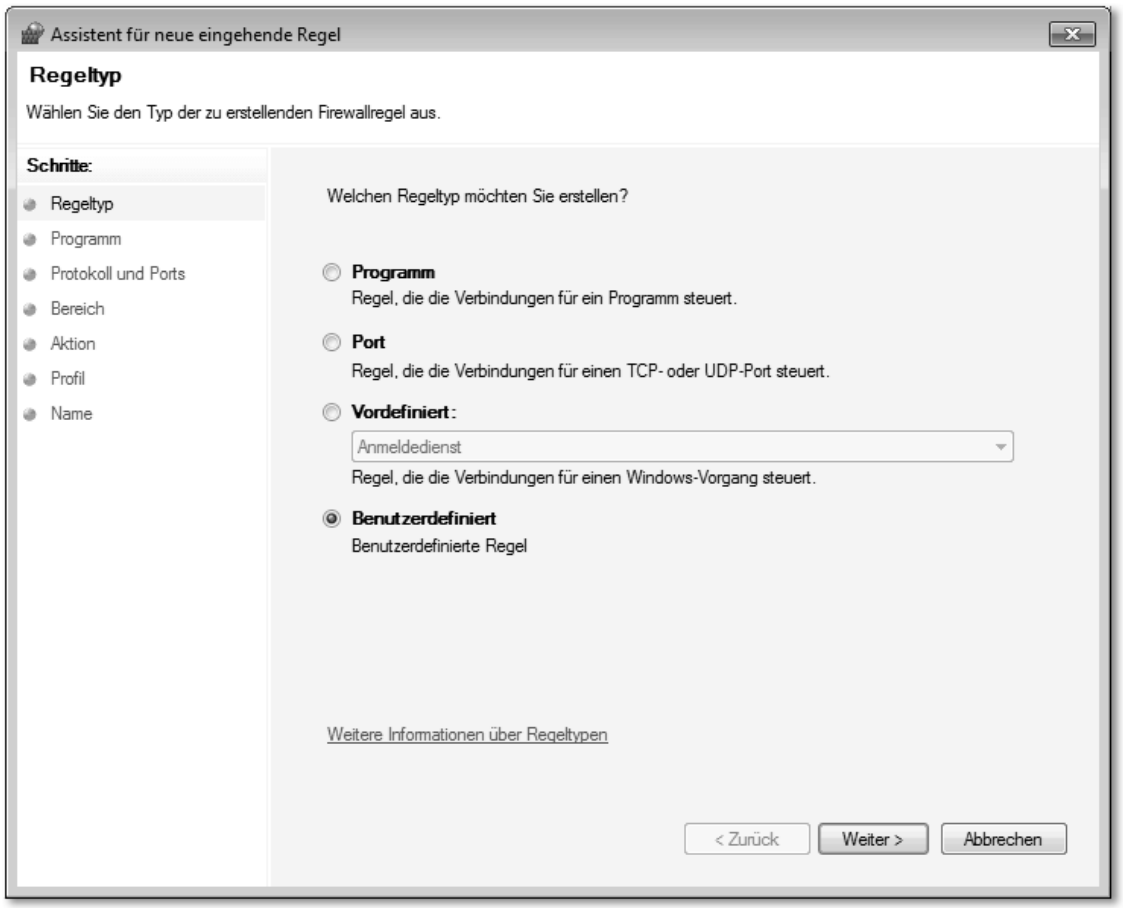


Abbildung 12.97 Der Typ der zu erstellenden Regel

Beim Erstellen einer benutzerdefinierten Regel wird zunächst abgefragt, für welches Programm diese Gültigkeit haben soll. Für dieses Beispiel ist eine genauere Spezifizierung an dieser Stelle nicht erforderlich, daher wird Alle Programme gewählt (Abbildung 12.98).

Der nächste Dialog ist deutlich spannender, denn hier wird ausgewählt, auf welches Protokoll nebst lokalen und Remoteports sich die Regel bezieht (Abbildung 12.99). ICMPv4 ist vergleichsweise einfach zu konfigurieren, da hier keine zusätzlichen Angaben zu Ports gemacht werden müssen (bzw. können). Auf der Abbildung nicht zu sehen, da er hinter der Dropdown-Liste versteckt ist, ist ein Schalter, der zu einem Dialog zum Anpassen der ICMP-Einstellungen führt. Sie können dort angeben, auf welche ICMP-Verbindungen die Regel angewendet werden soll – standardmäßig gilt sie für alle.

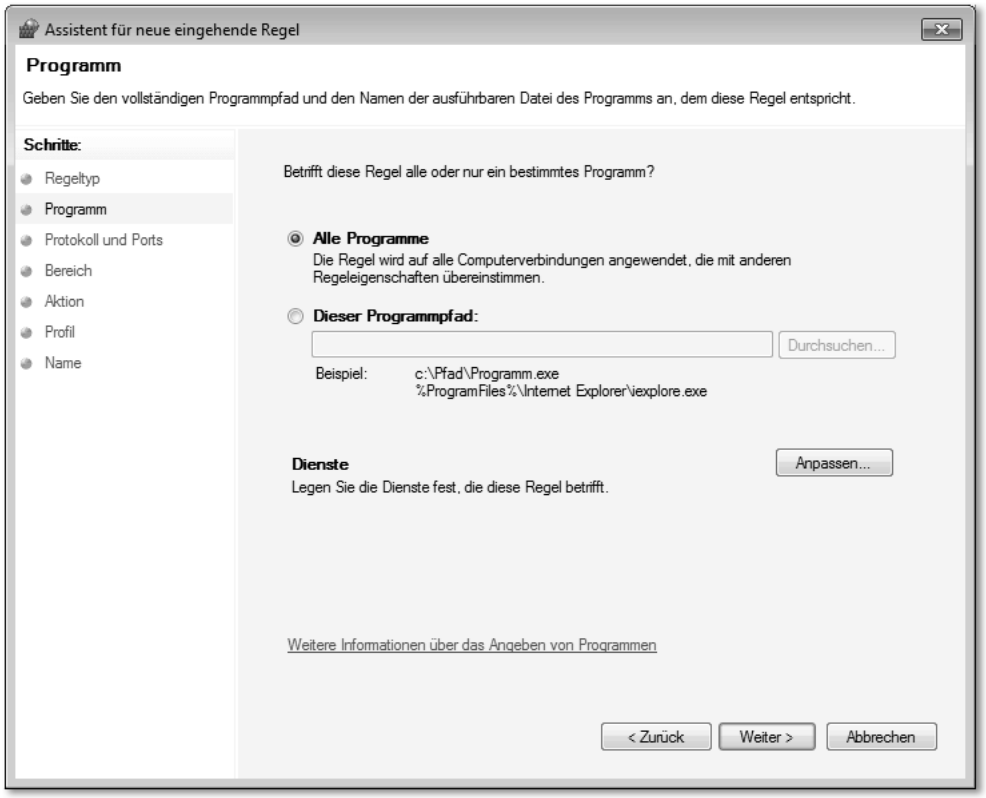


Abbildung 12.98 Bei einer benutzerdefinierten Regel wird ein Programmpfad abgefragt.

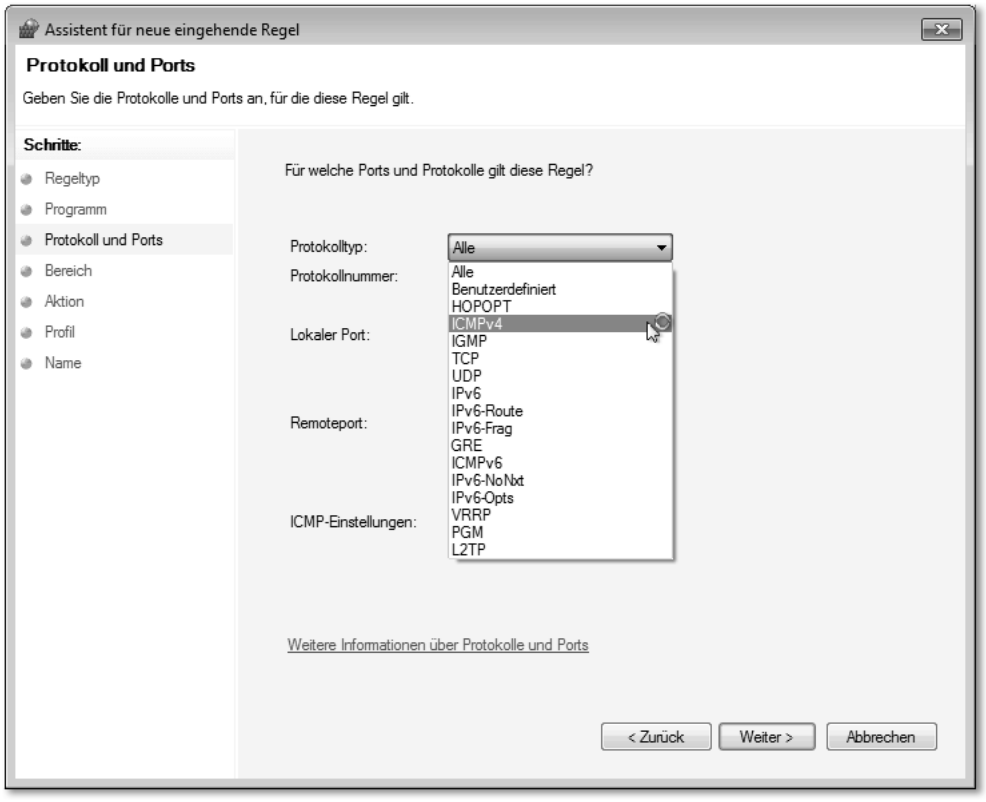


Abbildung 12.99 Auswahl des Protokolls und der Ports

Der Dialog auf Abbildung 12.100 fragt ab, für welche lokalen und entfernten IP-Adressen die Regel Gültigkeit haben soll – das dürfte so weit selbsterklärend sein. Jeder Computer soll den hier konfigurierten PC auf allen seinen IP-Adressen es ist aber zumeist ohnehin nur eine einzige) anpingen sollen. Es bleibt also bei den Standardeinstellungen.

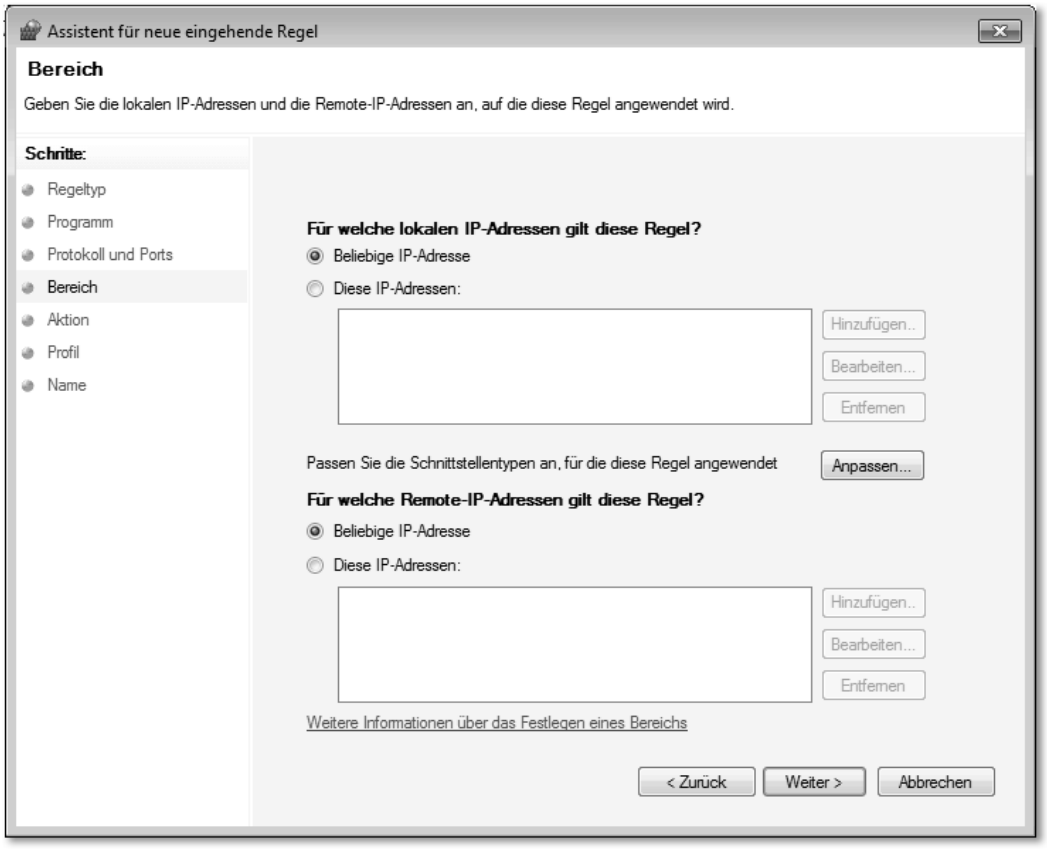


Abbildung 12.100 Definition der IP-Adressen, für die die Regel Gültigkeit hat

Ein wirklich zentraler Aspekt wird erst gegen Ende des Assistenten konfiguriert, nämlich ob es sich um eine Zulassungs- oder Verweigerungsregel handeln soll. Auch die dritte Variante, nämlich das Zulassen der Verbindung bei Bestehen einer sicheren Verbindung, kann angegeben werden. Die in diesem Beispiel erstellte PING-Regel ist eindeutig eine Zulassungsregel (Abbildung 12.101).

Im vorletzten Dialog legen Sie fest, für welche Profile die neu erstellte Regel gültig sein soll (Abbildung 12.102). Sie können selbstverständlich mehrere leicht voneinander abweichende Regeln konfigurieren, die unterschiedlichen Profilen zugeordnet sind. Sie können beispielsweise eine für das private und das Domänenprofil gültige PING-Regel bauen, die beinhaltet, dass jedem PC geantwortet wird. Eine separate PING-Regel für das öffentliche Profil könnte definieren, dass eine PING-Anforderung nur dann beantwortet wird, wenn die anfragenden Hosts aus dem eigenen IP-Adressbereich stammen.

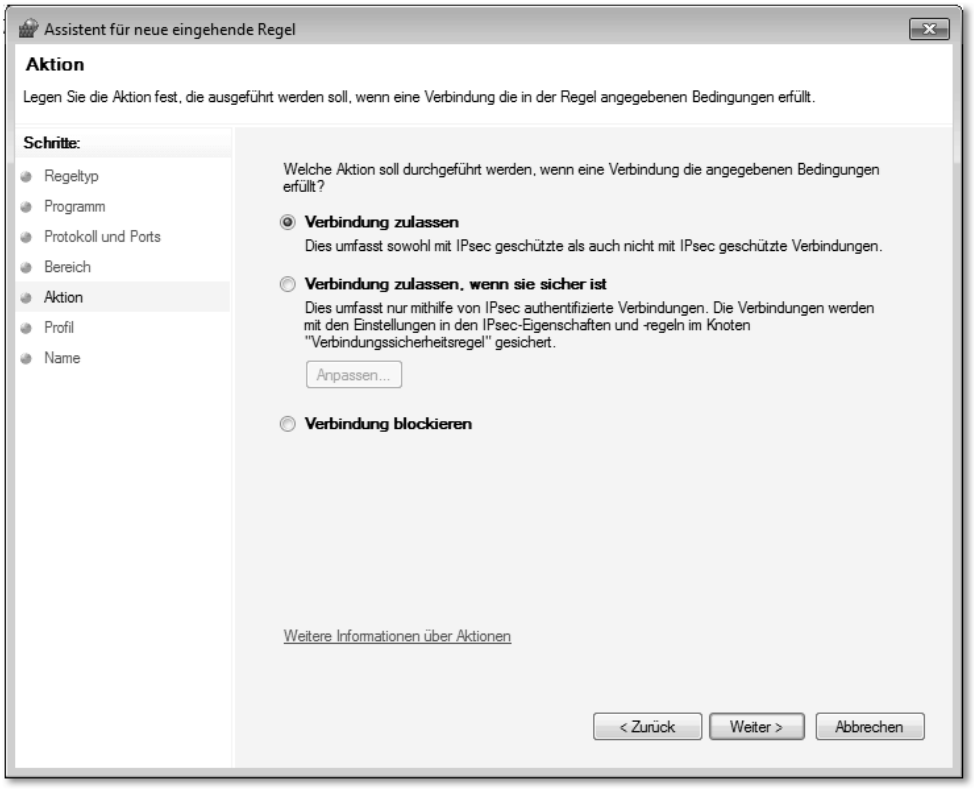


Abbildung 12.101 Dieser zentrale Aspekt wird erst recht weit zum Schluss konfiguriert, nämlich ob es sich um eine Zulassungs- oder Verweigerungsregel handeln soll.

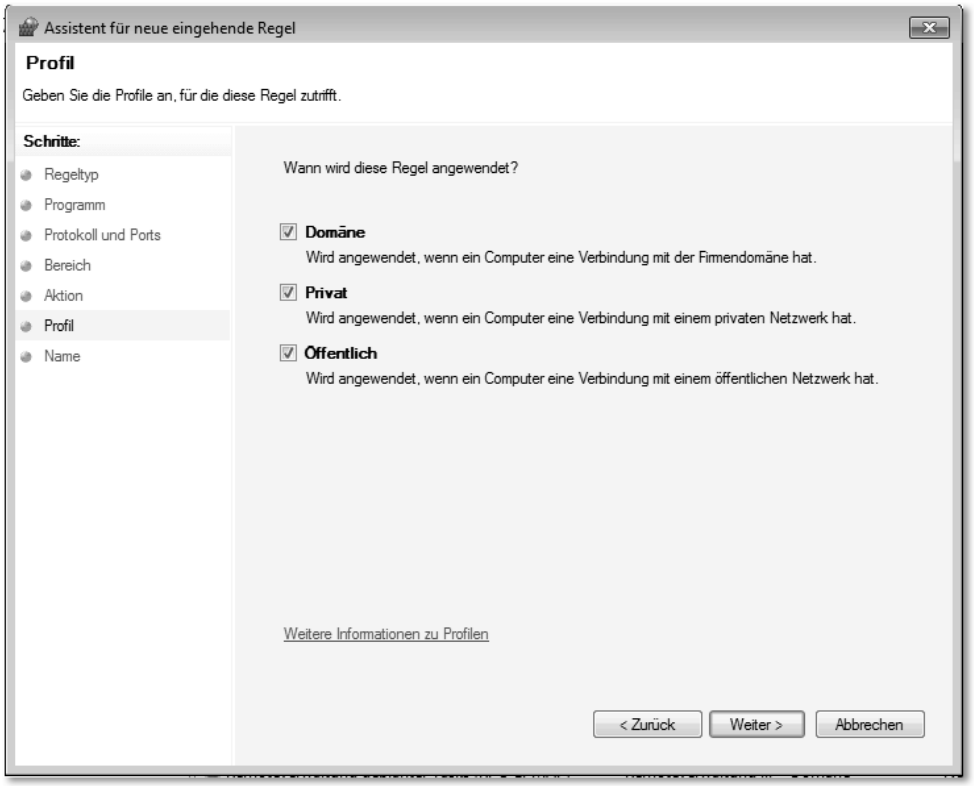


Abbildung 12.102 Im vorletzten Dialog wird die Gültigkeit der Regel für die Profile konfiguriert.

Der letzte Dialog des Assistenten fragt den Namen für die Regel ab (ohne Abbildung). Letztendlich ist der Name beliebig, es macht allerdings Sinn, sich an einem einheitlichen Schema zu orientieren – schließlich wollen Sie Ihre Regeln ja auch später ohne größere Probleme wiedererkennen.

Nach dem Abschluss des Assistenten ist die Regel sofort aktiv. Ein kleiner PING-Test, der jetzt erfolgreich ist, beweist es (Abbildung 12.103).

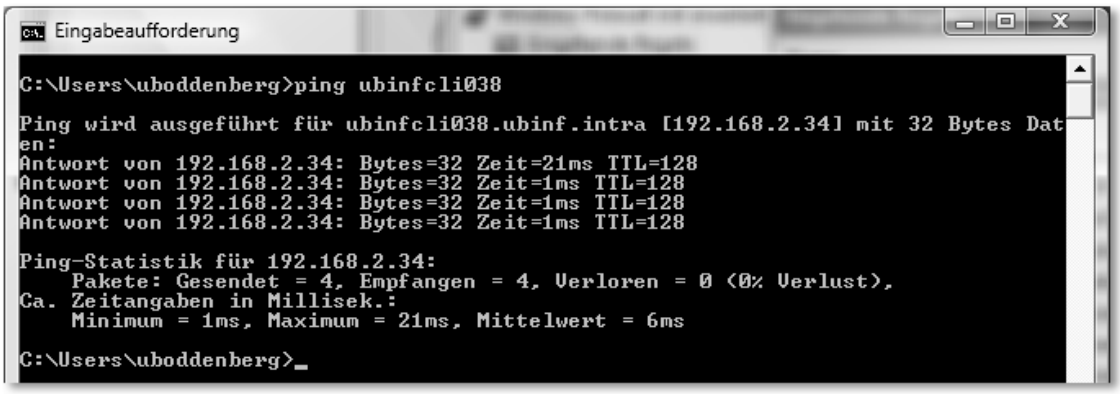


Abbildung 12.103 Die Regel ist sofort aktiv – es kann gepingt werden.

12.4.6 Mit Gruppenrichtlinien arbeiten

Dieses Buch wendet sich in erster Linie an Administratoren in Unternehmen, die im Allgemeinen nicht nur einen oder zwei PCs, sondern Dutzende, Hunderte oder Tausende von Systemen betreuen. Für einen Administrator dürfte also die vordringliche Frage sein, wie er Anpassungen der Windows-Firewall schnell und einfach auf allen PCs ausführen kann.

Richtig, die Lösung heißt *Gruppenrichtlinien*. Abbildung 12.104 zeigt die Bearbeitung eines Gruppenrichtlinienobjekts. Dort gibt es einen Abschnitt zur Konfiguration der Windows-Firewall – das Leben ist doch schön.

Die Vorgehensweise entspricht weitgehend derjenigen, die Sie vom lokalen Bearbeiten der Einstellungen der Windows-Firewall kennen. Es gibt also einstellbare Eigenschaften (Kontextmenü des obersten Knotens) sowie Regeln für eingehende und ausgehende Verbindungen und für die Verbindungssicherheit.

Um das Thema nicht allzu abstrakt zu behandeln, zeige ich Ihnen ein kleines Beispiel, das durchaus eine gewisse Relevanz hat: Bekanntlich wird ein Großteil von Spam-Nachrichten über Bot-Netze versendet. Diese funktionieren vereinfacht gesagt so, dass ein Stück Software ohne das Wissen des Benutzers auf seinem PC installiert wird. Solche PCs (und ein Botnetz umfasst Tausende davon) werden zentral vom Spammer gesteuert und versenden Spam-Mails. Der Mailversand geschieht über das SMTP-Protokoll (TCP, Port 25).

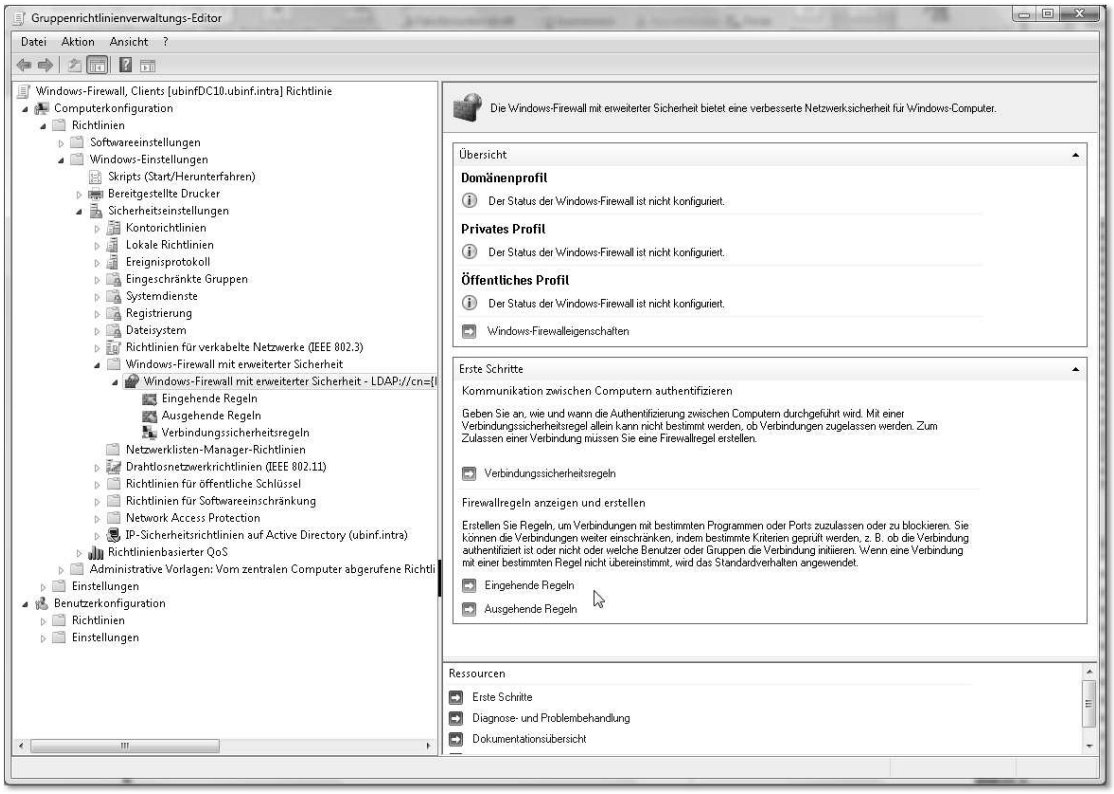


Abbildung 12.104 Die Windows-Firewall kann selbstverständlich über Gruppenrichtlinien gesteuert werden.

Falls trotz Virenscanner & Co. ein Bot auf einen Ihrer PCs gekommen ist, könnten Sie diesen weitgehend unschädlich machen, indem Sie eine ausgehende SMTP-Verbindung verhindern. (In Verbindung mit Exchange übermittelt Outlook E-Mails nicht per SMTP.) Der langen Rede kurzer Sinn ist, dass man sich durchaus überlegen könnte, eine Verweigerungsregel zu bauen, die ausgehenden SMTP-Datenverkehr verhindert. Diese Regel soll dann per Gruppenrichtlinie auf alle PCs des Unternehmens ausgerollt werden.

Wählen Sie also im Gruppenrichtlinienverwaltungs-Editor (Abbildung 12.104) das Erstellen einer neuen ausgehenden Regel. Im Assistenten geben Sie zunächst an, dass es sich um eine Portregel handelt (Abbildung 12.105), schließlich wollen Sie ja ausgehenden SMTP-Verkehr sperren (TCP, Port 25). Auf der zweiten Dialogseite des Assistenten besteht nun allerdings akute Verwechselungsgefahr (Abbildung 12.106): Man könnte versucht sein, in diesem Dialog den zu sperrenden Port, nämlich TCP-25, einzutragen. Bei genauerem Lesen werden Sie aber feststellen, dass in diesem Dialog lokale Ports abgefragt werden und eben nicht der Zielport auf dem Remote-System. Der Quellport, also der auf dem lokalen PC gewählte Port, ist in diesem Fall nicht relevant, also belassen Sie die Einstellung auf ALLE LOKALEN PORTS. Der Port des Zielsystems kann übrigens in diesem Assistenten nicht angegeben werden und muss später der fertigen Regel hinzugefügt werden.

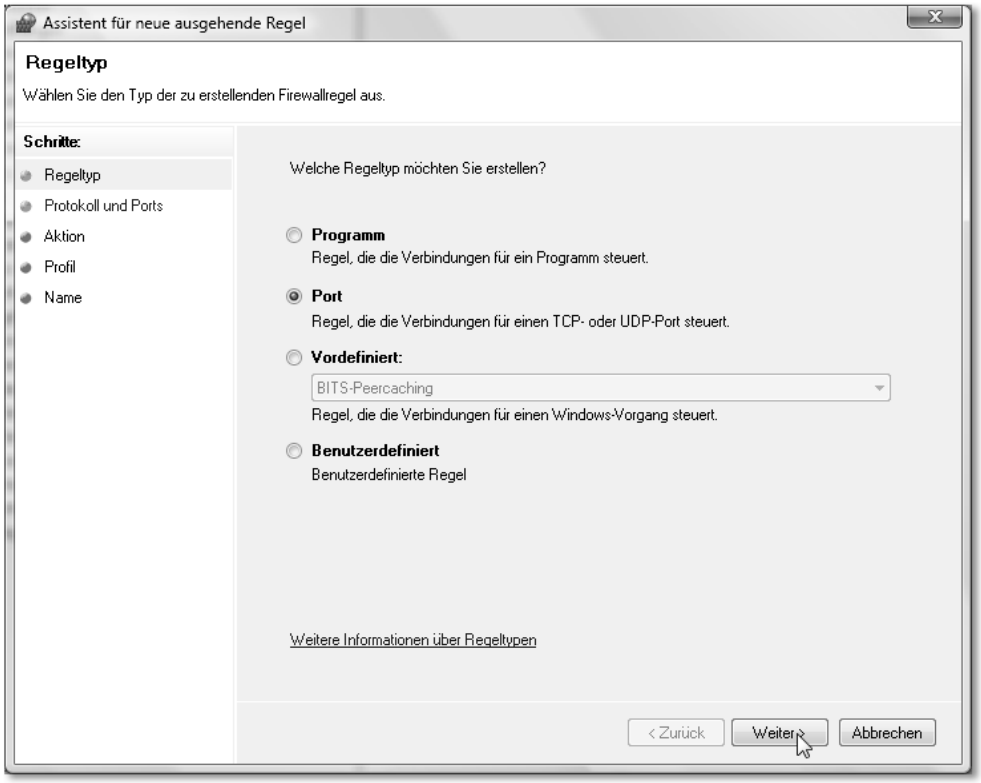


Abbildung 12.105 Für dieses Beispiel wird eine Port-Regel erzeugt.

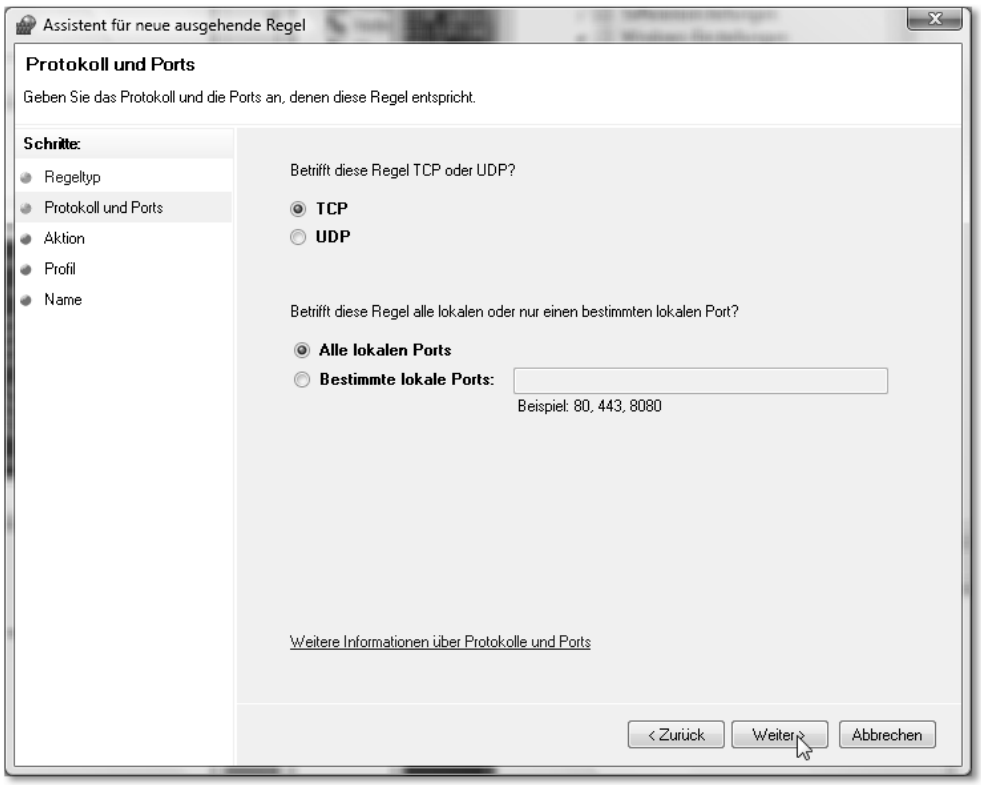


Abbildung 12.106 Lassen Sie sich nicht irritieren: Wir wollen zwar die Verbindung zu einem Remote-Port unterbinden, hier wird aber der lokale Port abgefragt.

Auf Abbildung 12.107 sehen Sie den Dialog, mit dem aus der Regel eine Verweigerungsregel gemacht wird. Die Eingabemöglichkeiten auf den übrigen Dialogseiten des Assistenten beziehen sich auf die Profile und den Namen der Regel.

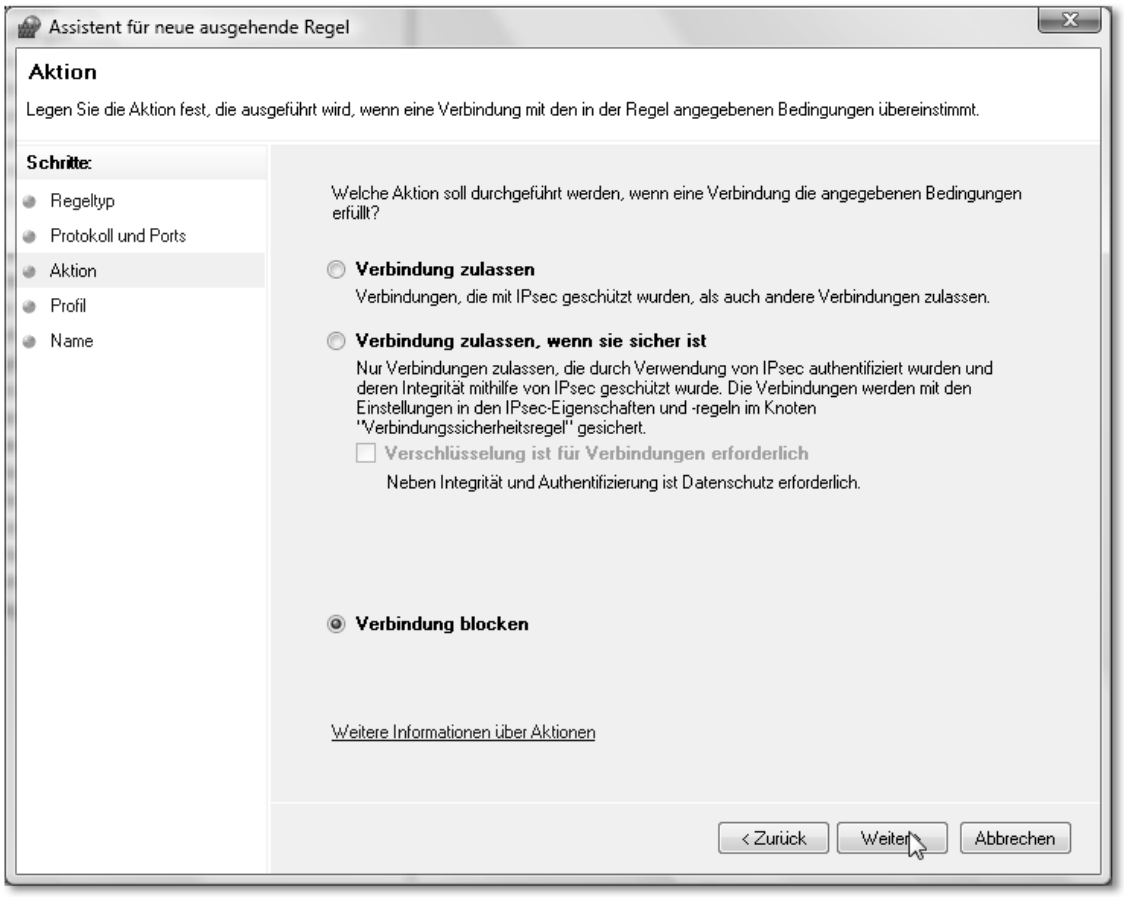


Abbildung 12.107 Diese Regel ist eine Verweigerungsregel.

Ist die Regel angelegt, rufen Sie deren Eigenschaften auf und wechseln auf die Registerkarte PROTOKOLL UND PORTS (Abbildung 12.108). Hier tragen Sie als REMOTEPORT die 25 (SMTP-Verkehr) ein. Und schon ist die Regel für die Gruppenrichtlinie erstellt.

Achten Sie darauf, dass dieses Gruppenrichtlinien-Objekt so verknüpft ist, dass es auf den PC angewendet wird, mit dem Sie testen.

Auf Abbildung 12.109 habe ich den Erfolg der Konfigurationsarbeit getestet:

- Zunächst kann eine SMTP-Verbindung zu einem E-Mail-Server aufgebaut werden. (Ich habe das mit dem Telnet-Client ausprobiert.)
- Mit dem `gpupdate`-Befehl wird die Anwendung der soeben geänderten Gruppenrichtlinie erzwungen.
- Anschließend ist der Aufbau der SMTP-Verbindung nicht mehr möglich.

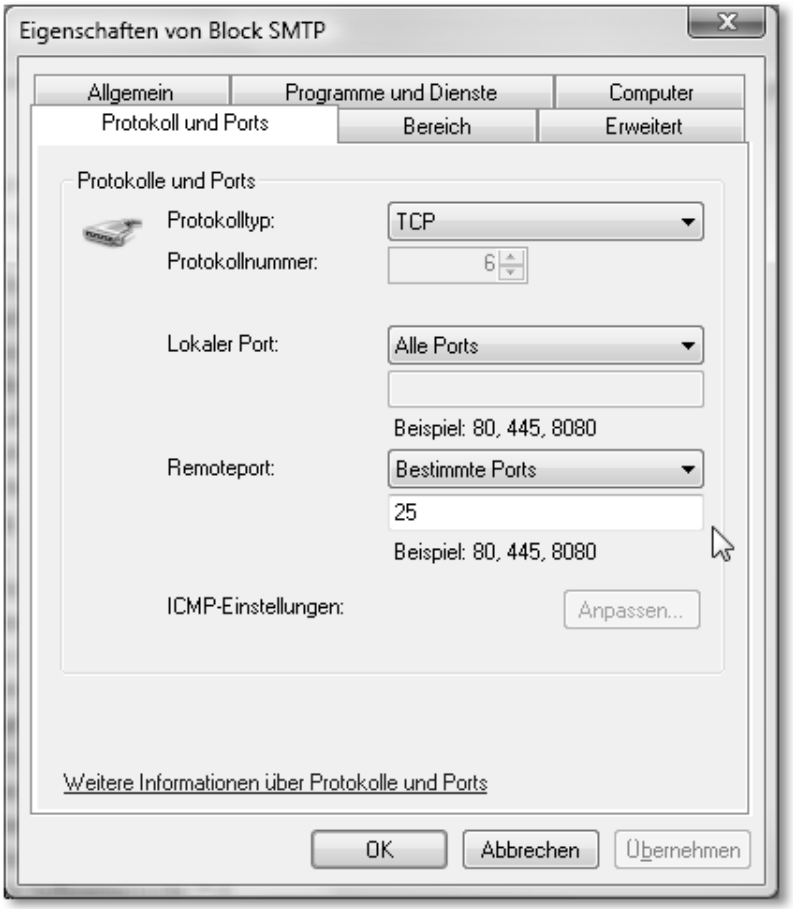


Abbildung 12.108 In den Eigenschaften der »fertigen« Regel wird nun der Remote-Port eingetragen.

Abbildung 12.109 Nach einem »gpupdate« kann der Client nicht mehr mit dem Mailserver kommunizieren.

12.4.7 Gruppenrichtlinien vs. »individuelle Anpassungen«

Wenn Sie ein Windows-Firewall-Regelwerk mit bestimmten Standardregeln per Gruppenrichtlinie verteilen, ist das grundsätzlich der richtige Weg. Was passiert nun aber, wenn ein bestimmter PC eben doch das SMTP-Protokoll nutzen oder sonstige eigentlich verbotene Aktionen durchführen muss?

Eine Möglichkeit ist, eine Grundkonfiguration per Gruppenrichtlinie auszurollen und lokal zu modifizieren. Um dies zu ermöglichen, rufen Sie im Gruppenrichtlinienverwaltungs-Editor die Eigenschaften des Knotens WINDOWS-FIREWALL MIT ERWEITERTER SICHERHEIT auf. Auf der Karteikarte DOMÄNENPROFIL rufen Sie das Anpassen der Einstellungen auf. In der Gruppenrichtlinie legen Sie dann unter dem Stichwort REGELZUSAMMENFÜHRUNG fest, dass von lokalen Administratoren erstellte Regeln verwendet werden. Diese werden dann mit den per Gruppenrichtlinie verteilten Regeln gemischt (Abbildung 12.110).

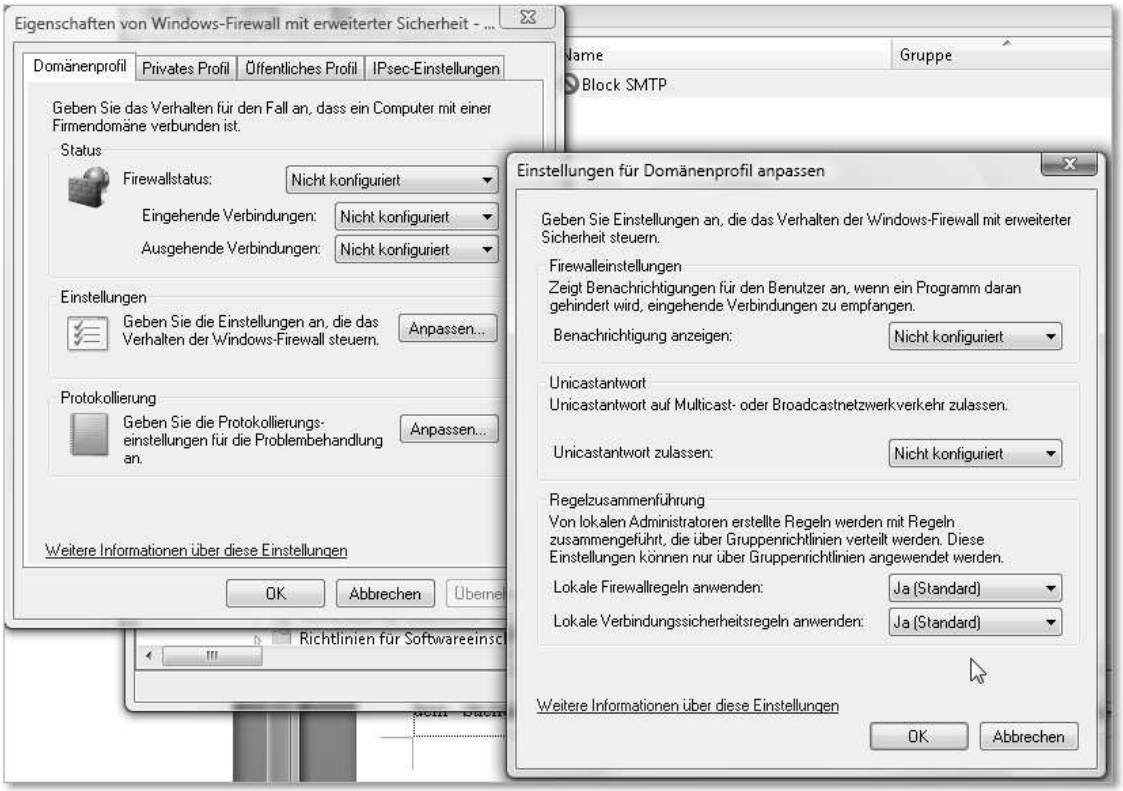


Abbildung 12.110 Die Regelzusammenführung sorgt dafür, dass von lokalen Administratoren erstellte Regeln ebenfalls angewendet werden.

12.4.8 Verbindungssicherheitsregeln

Mit den zuvor vorgestellten Regeln kann festgelegt werden, welche Kommunikationsvorgänge erlaubt oder verboten sind. Die Verbindungssicherheitsregeln er-

gänzen diese und ermöglichen die Definition verschiedener Szenarien, in denen die Verbindungen authentifiziert werden.

Wenn bei den »normalen« Regeln eingestellt wird, dass nur sichere Verbindungen zugelassen sind, muss die Verbindung einer der Regeln genügen, die in den Verbindungssicherheitsregeln definiert sind.

Ich werde Ihnen das Erstellen einer einfachen Regel vorführen, die dafür sorgt, dass nur authentifizierte Verbindungen zum Computer zugelassen sind. Im Kontextmenü des Knotens Verbindungssicherheitsregeln können Sie den Assistenten zur Erstellung einer neuen Regel aufrufen.

Im Assistenten wählen Sie zunächst den Typ der zu erstellenden Regel aus. Folgende Optionen stehen zur Verfügung (Abbildung 12.111):

- Isolierung: Die Verbindungen werden anhand von Authentifizierungskriterien eingeschränkt.
- Authentifizierungsausnahme: Verbindungen von den Computern, die in der Regel angegeben sind, werden nicht angenommen.
- Server-zu-Server: Die Verbindungen zwischen den in der Regel angegebenen Computern sollen authentifiziert werden.
- Tunnel: Die Verbindung zwischen Gatewaycomputern soll authentifiziert werden.

Für dieses Beispiel wählen Sie den Typ Isolierung. Der Computer wird sozusagen gegen nicht authentifizierte Computer isoliert.

Auf der nächsten Dialogseite konfigurieren Sie, welche Verbindungen authentifiziert werden müssen (Abbildung 12.112). Hierbei gibt es verschiedene Möglichkeiten:

- Sowohl für die eingehende als auch für die ausgehende Verbindung wird eine Authentifizierung angefordert. Falls diese nicht erfolgt, wird die Verbindung trotzdem zugelassen.
- Die zweite Option erzwingt eine Authentifizierung für eingehende Verbindungen – ohne Authentifizierung wird die Verbindung abgelehnt. Ausgehende Verbindungen werden auch ohne erfolgte Authentifizierung zugelassen.
- Die dritte Option erzwingt eine Authentifizierung sowohl für eingehende als auch für ausgehende Verbindungen.

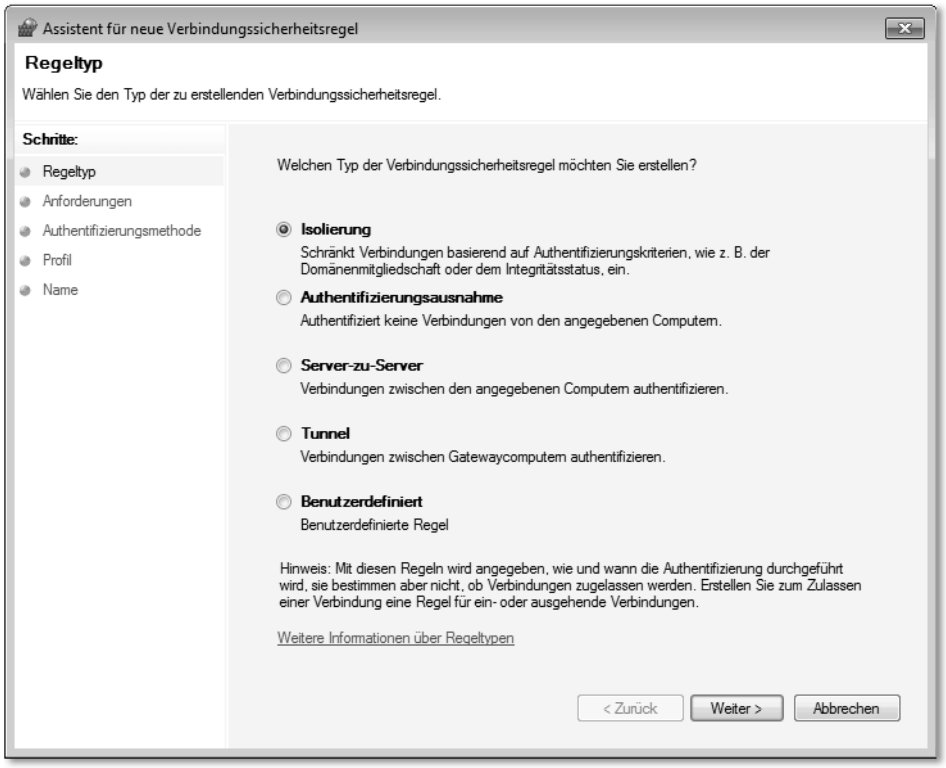


Abbildung 12.111 Zunächst wählen Sie im Assistenten den Typ der Verbindungssicherheitsregel aus.

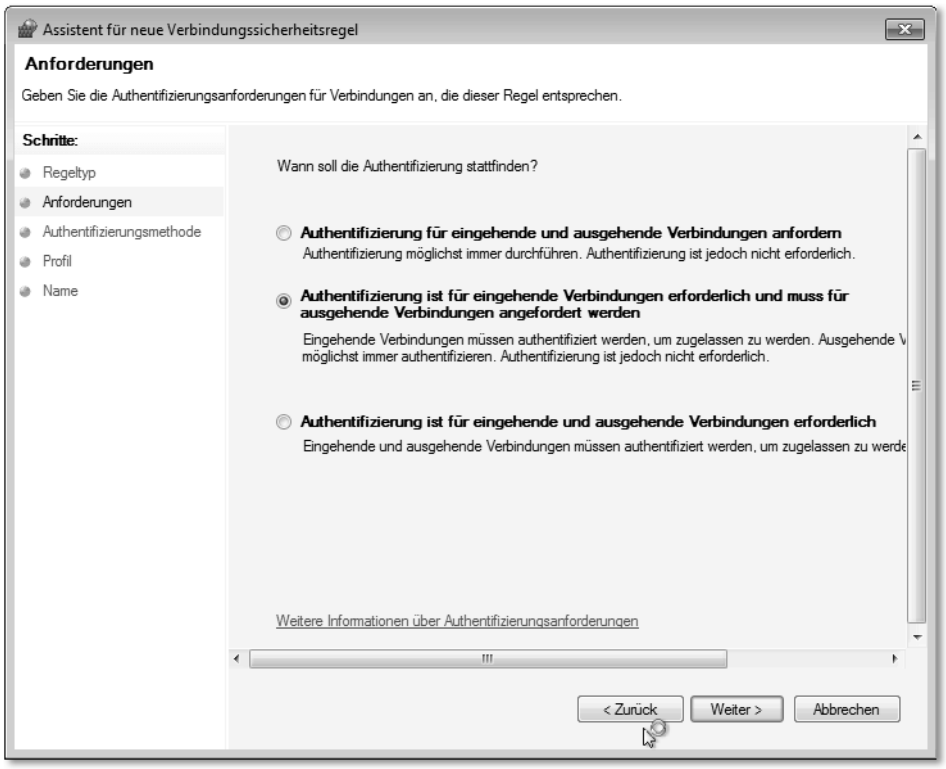


Abbildung 12.112 Hier legen Sie fest, ob eingehende und/oder ausgehende Verbindungen authentifiziert werden müssen.

Im nächsten Schritt legen Sie fest, wie authentifiziert werden soll (Abbildung 12.113):

- Authentifizierung von COMPUTER UND BENUTZER mittels Kerberos: Eine Verbindung kommt nur zustande, wenn sowohl der Computer als auch der Benutzer Mitglied der Domäne ist.
- Authentifizierung des COMPUTERS mittels Kerberos.
- Authentifizierung des Computers durch ein COMPUTERZERTIFIKAT. Hierbei wird überprüft, ob das vom Computer präsentierte Zertifikat von der angegebenen CA ausgestellt worden ist. Optional kann festgelegt werden, dass nur Zertifikate über den »Gesundheitszustand« des Computers akzeptiert werden. Solche Zertifikate werden von der Identitätsregistrierungsinstanz (*Health Certification Authority)* ausgestellt, einem Dienst, der Bestandteil der Rolle *Netzwerkrichtlinien- und Zugriffsdienste* (siehe vorheriger Abschnitt) ist.

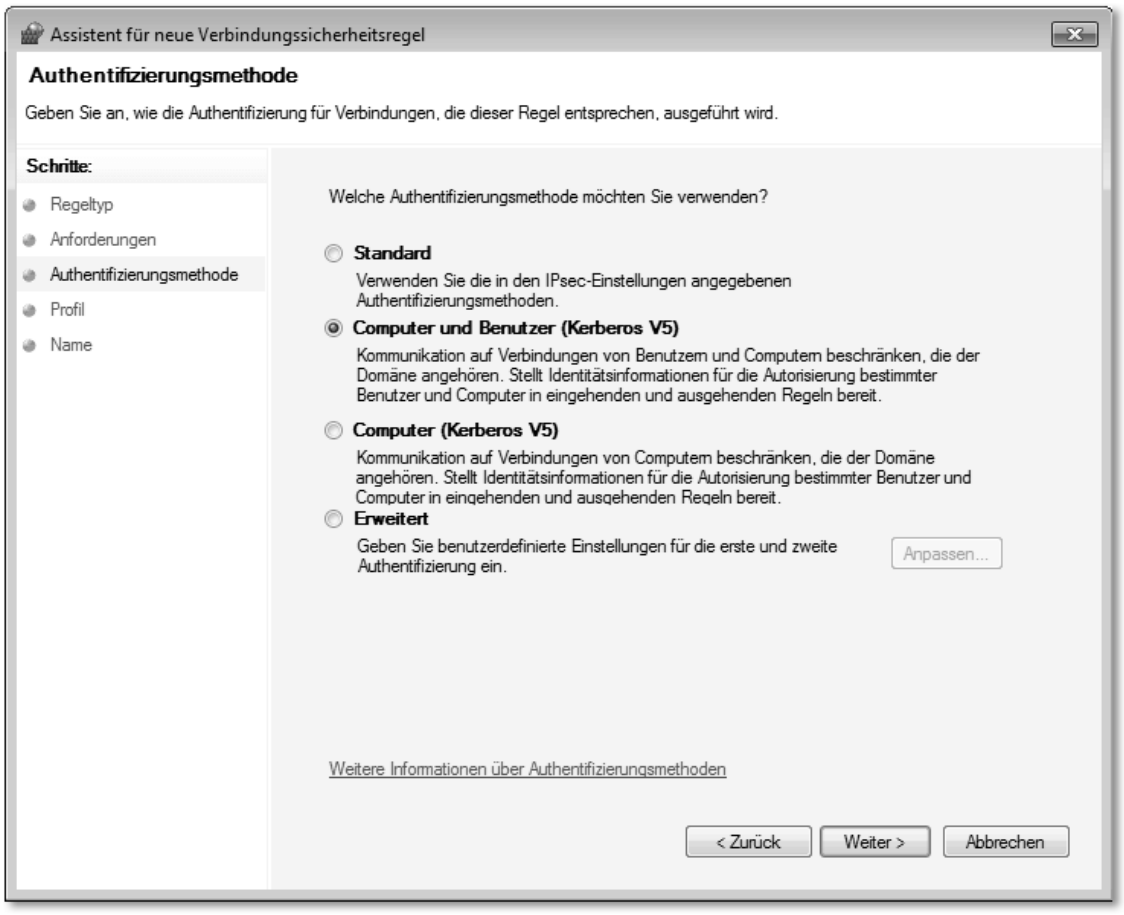


Abbildung 12.113 Sie können auswählen, ob Computer und Benutzer per Kerberos authentifiziert werden sollen. Alternativ können Computerzertifikate herangezogen werden.

Im vorletzten Schritt legen Sie fest, für welches Profil die neue Regel gelten soll. Die Profile werden automatisch gewählt, je nachdem, mit was für einem Netz-

werk der Computer verbunden ist. Der letzte Schritt ist übrigens die Vergabe des Namens für die neue Verbindungssicherheitsregel, was wohl nicht genauer diskutiert werden muss.

Der Assistent für eine Isolierungsregel bietet nicht die Möglichkeit, Einschränkungen bezüglich der Endpunkte zu definieren. Dies können Sie aber problemlos im EIGENSCHAFTEN-Dialog der angelegten Regel nachholen (Abbildung 12.114). Eine TCP/IP-Verbindung hat zwei Endpunkte – es »sprechen« ja auch zwei Geräte miteinander. Der eine Endpunkt ist eine IP-Adresse auf dem Computer, auf dem die Windows-Firewall installiert ist; der zweite Endpunkt ist dessen Kommunikationspartner, der im lokalen Netz oder in den Weiten des Internets stehen kann.

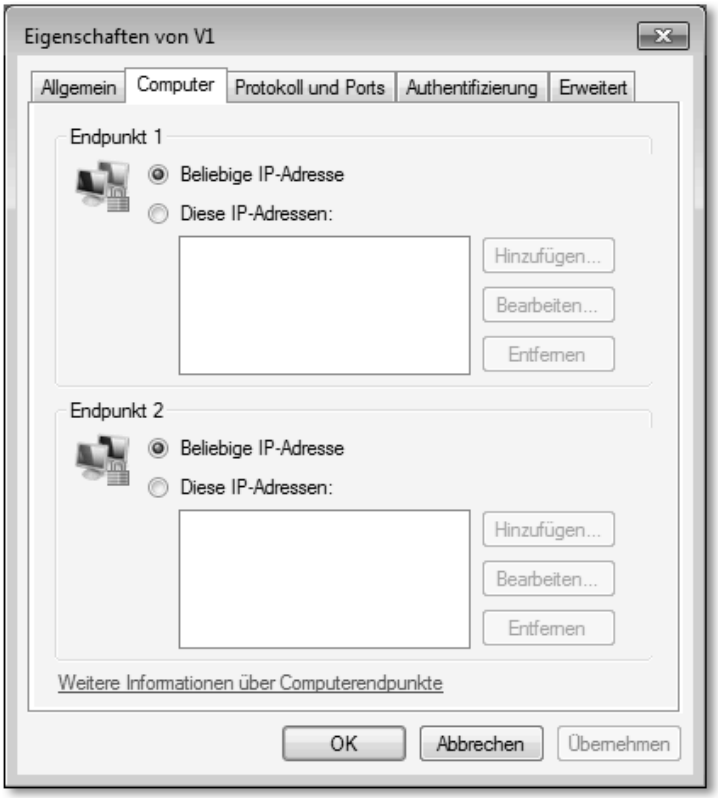


Abbildung 12.114 In dem »Eigenschaften«-Dialog der angelegten Regel können Sie die Endpunkte festlegen.

12.5 AppLocker

Sowohl ein Sicherheits- als auch ein Support-Problem ist die Tatsache, dass es nicht ganz einfach zu verhindern ist, dass Anwender Programme oder Skripts ausführen. Dieser Code kann beispielsweise per E-Mail, per Download aus dem Web, auf CDs oder USB-Sticks und auf diversen anderen Wegen auf den PC kommen. Mangels (administrativer) Berechtigungen können Benutzer zwar etliche In-

stallationen nicht ausführen, trotzdem können sie ein Programm starten. Das ausgeführte Programm könnte nun etwa ein Virus oder Trojaner sein, der Daten zerstört, modifiziert oder ausspäht. Vielleicht ist das Programm auch unsauber programmiert und blockiert den PC, ist mit anderen Anwendungen inkompatibel oder dergleichen mehr. Ein vom Benutzer eigenmächtig »eingeschlepptes« Programm könnte (!) also ein Sicherheitsproblem, ein Administrationsproblem oder beides sein.

Sie werden zunächst kaum verhindern können, dass der Benutzer eine ausführbare Datei starten kann. Die Erkenntnis, dass eine Funktion benötigt wird, mit der sich das Ausführen beliebiger Programme/Skripts verhindern lässt, ist nun nicht gerade neu: Seit Windows XP konnte man mit Gruppenrichtlinien Richtlinien für Softwareeinschränkung definieren (zur Erinnerung: Abbildung 12.115) – das ist sozusagen der Vorgänger von AppLocker.

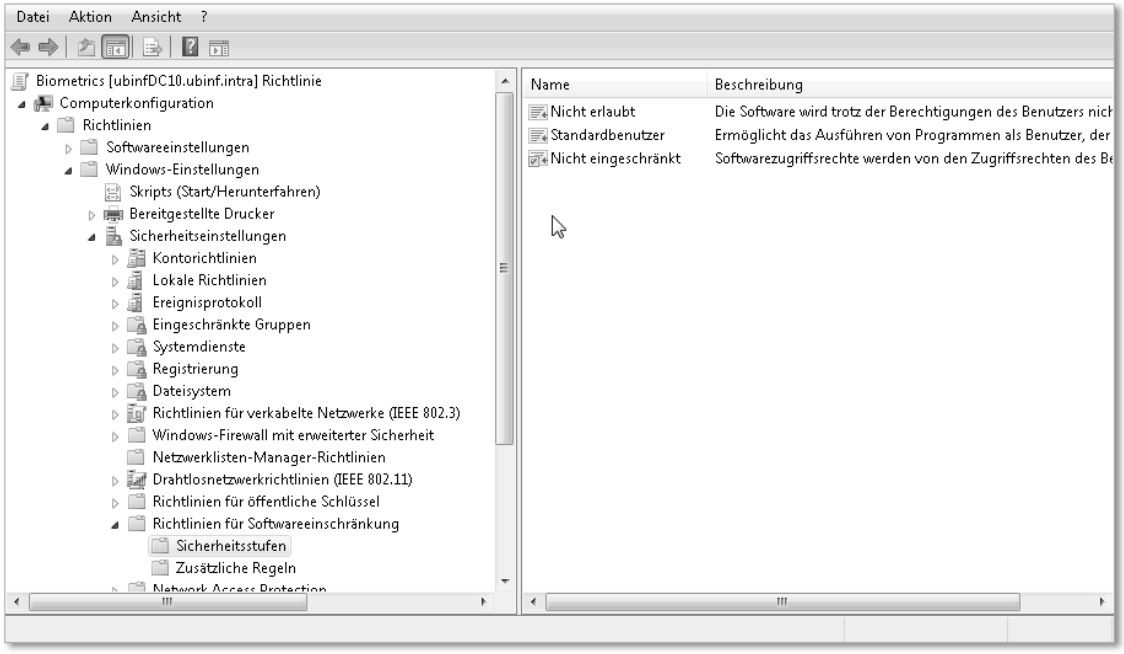


Abbildung 12.115 Quasi der Vorgänger von AppLocker: »Richtlinien für Softwareeinschränkung«

AppLocker kennt mehr Optionen und erlaubt feinere Abstufungen als die etwas grobkörnigen *Richtlinien für Softwareeinschränkung*. Die Idee ist aber die gleiche:

- Es wird definiert, welche Programme und/oder Skripts ausgeführt werden dürfen.
- Ist die Ausführung einer Anwendung nicht gestattet, erscheint beim Start derselben nicht das Programm, sondern nur eine Fehlermeldung.

Grundsätzlich gibt es zwei Vorgehensweisen:

- Sie erlauben grundsätzlich nichts und geben frei, was Ihren »offiziellen« Segen bekommen hat.
- Sie erlauben grundsätzlich alles und sperren, was Sie nicht im Unternehmen haben möchten.

Es liegt auf der Hand, dass die erste Variante erfolgversprechender sein wird. Sie können natürlich gezielt Anwendungen sperren (erinnern Sie sich eigentlich noch an »Moorhuhn«?), letztendlich werden Sie aber kaum hinter jeder einzelnen Anwendung herlaufen wollen und können.

Nur Enterprise oder Ultimate

An dieser Stelle sei noch darauf hingewiesen, dass AppLocker nicht mit jeder Windows 7-Edition funktioniert. PCs, auf denen AppLocker verwendet werden soll, müssen mit *Windows 7 Enterprise* oder *Ultimate* laufen.

12.5.1 Funktion, Konfiguration und Anwendung – ein Beispiel

Zum Einstieg zeige ich Ihnen ein simples AppLocker-Anwendungsbeispiel. Die Anforderung ist so simpel wie gewöhnlich – jeder Admin dürfte sich schon immer gewünscht haben, dass nur die Windows-Standardprogramme (z. B. der Taschenrechner oder Notepad) und die »offiziell« installierte Software gestartet werden können.

Voraussetzungen

Erste Voraussetzung ist, wie auch schon erwähnt, dass Windows 7 in der Enterprise- oder Ultimate-Edition vorhanden ist.

AppLocker benötigt Unterstützung durch einen im Hintergrund laufenden Dienst namens *Anwendungsidentität*. Der Name des Diensts verrät bereits, was sein Sinn und Zweck ist. Starten Sie also diesen Dienst, und legen Sie den Starttyp auf Automatisch fest (Abbildung 12.116).

Konfigurationswerkzeug

Die Konfiguration von AppLocker erfolgt über Richtlinien. Erste Tests können der Einfachheit halber mit lokalen Richtlinien erfolgen. Im Produktivbetrieb dürfte sich die Verwendung von AD-basierten Gruppenrichtlinien empfehlen.

Starten Sie also das Konfigurationswerkzeug Lokale Sicherheitsrichtlinie. Dazu rufen Sie `secpol.msc` auf. Unterhalb des Knotens Anwendungssteuerungsrichtlinien finden Sie die AppLocker-Einträge. Bereits beim ersten Darüberschauen erschließt sich, was zu tun ist (Abbildung 12.117).

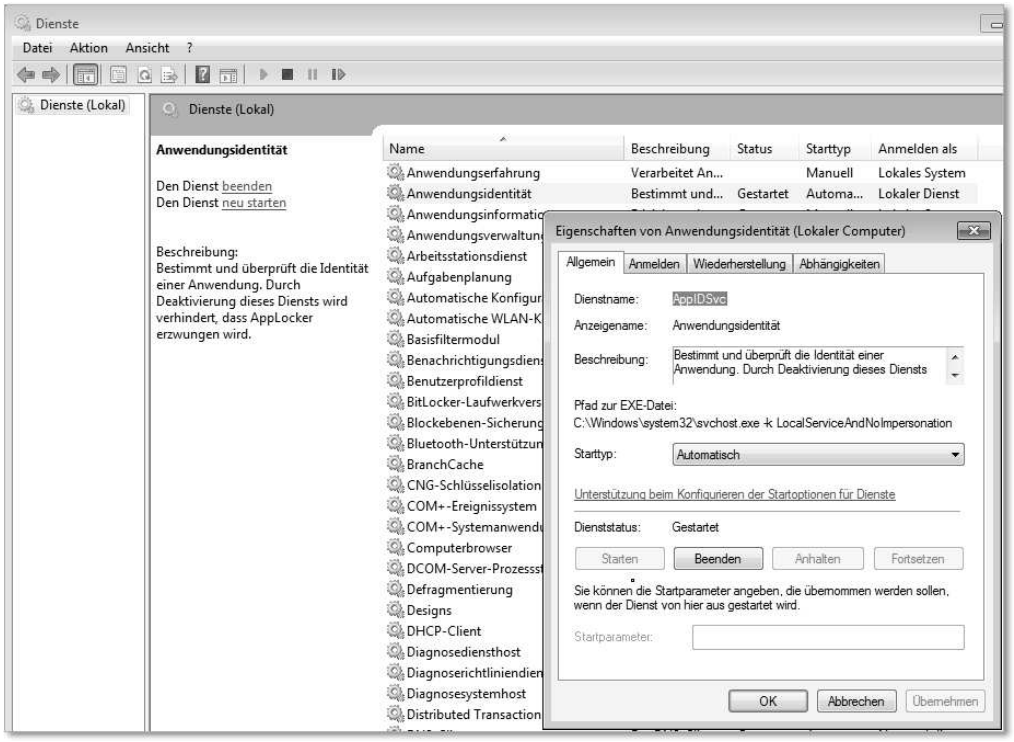


Abbildung 12.116 Der Dienst »Anwendungsidentität« muss gestartet werden.

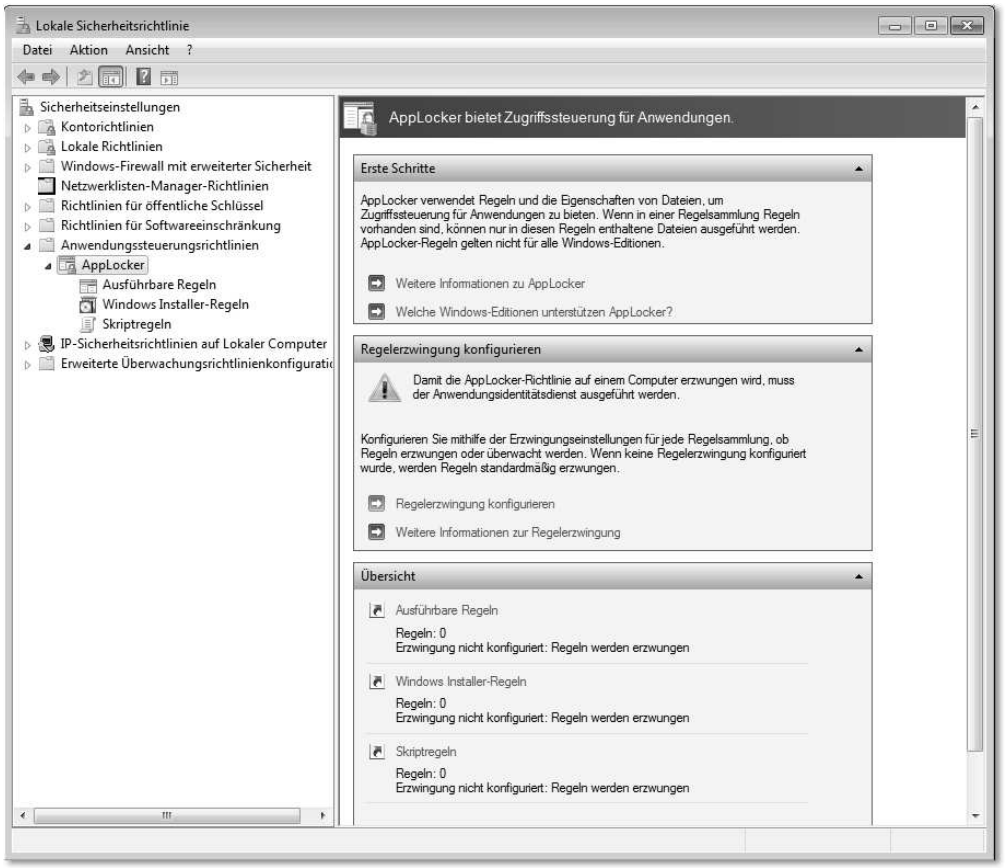


Abbildung 12.117 Die Konfiguration von AppLocker erfolgt über Richtlinien.

- Zunächst müssen Sie Regeln konfigurieren, und zwar gibt es Regeln für ausführbare Dateien, für den Windows Installer und für Skripts.
- Dann müssen Sie festlegen, dass die Regeln »erzwungen« werden.

Standardregeln erzeugen

Die meistgewählte Vorgehensweise bei der Anwendung von AppLocker dürfte sein, dass alles verboten wird und auf einer Positivliste (Whitelist) aufgeführt wird, was eben doch ausgeführt werden kann. Die Frage ist also, wie man ohne großen Aufwand diese Positivliste generiert. Vermutlich werden Sie alle Programme im Windows-Verzeichnis (dort ist ja z. B. der Taschenrechner, gegen den ja nichts einzuwenden ist) und alle Programme im *C:\Programme*-Verzeichnis zulassen wollen.

Zum *C:\Programme*-Verzeichnis wäre anzumerken, dass die Benutzer dort standardmäßig keinen schreibenden Zugriff haben. Programme, die sich dort befinden, müssen also vom Administrator installiert worden sein bzw. zum »Grundlieferumfang« des Betriebssystems oder Installations-Images gehören (Abbildung 12.118).

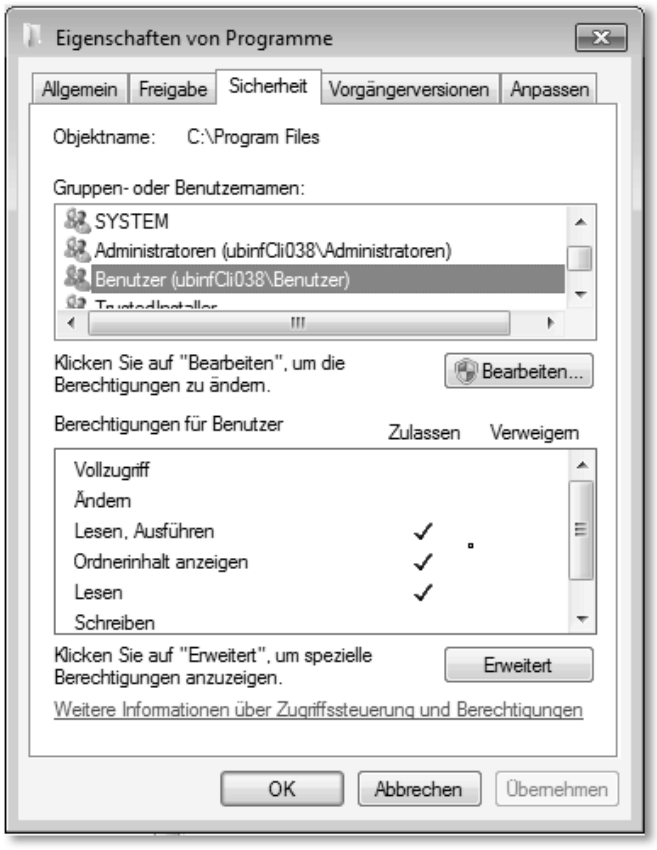


Abbildung 12.118 Im Verzeichnis »C:\Programme« haben Benutzer keinen schreibenden Zugriff.

Im Kontextmenü jedes der drei Regeltypen (Ausführbar, Windows Installer, Skripts) findet sich der Menüpunkt STANDARDREGELN ERSTELLEN. Dieser generiert drei grundlegende Regeln, auf denen Sie Ihre eigene AppLocker-Konfiguration aufbauen können (Abbildung 12.119).

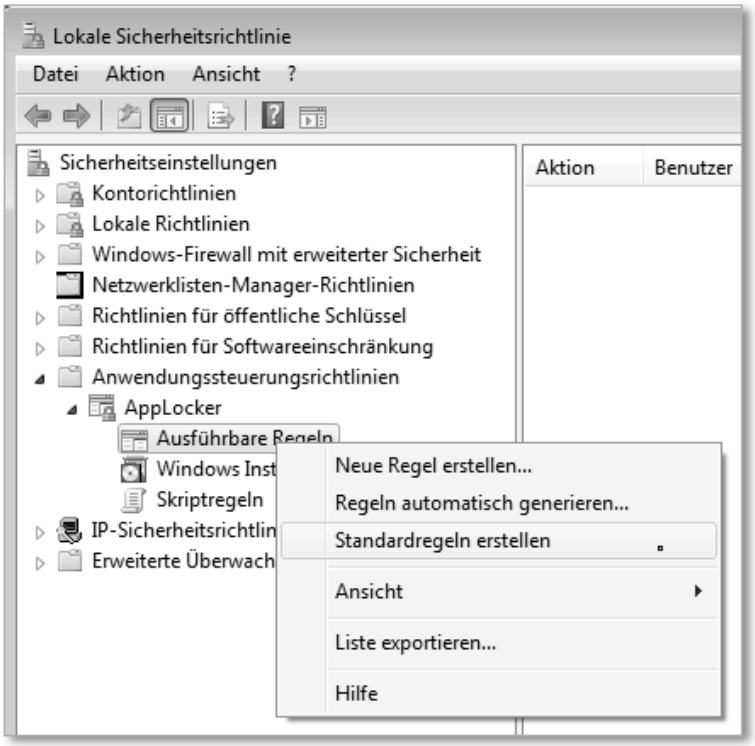


Abbildung 12.119 Mit dem Menüpunkt »Standardregeln erstellen« kommt man schnell zu drei grundlegenden AppLocker-Regeln.

Anzumerken wäre, dass Sie die Standardregeln nicht hinzufügen müssen – im Allgemeinen macht es Sinn, es ist aber kein Zwang.

Abbildung 12.120 zeigt die drei Standardregeln für ausführbare Programme:

- Alle Benutzer (JEDER) können Dateien im Ordner *Programme* (im Allgemeinen *C:\Programme*) ausführen.
- Alle Benutzer (JEDER) können Dateien im *Windows*-Ordner (im Allgemeinen *C:\Windows*) ausführen.
- Administratoren können alle Dateien ausführen.

Die Windows Installer-Standardregeln sind auf Abbildung 12.121 zu sehen:

- Alle Benutzer können digital signierte Windows Installer-Dateien ausführen.
- Alle Benutzer können Windows Installer-Dateien im Ordner *C:\Windows\Installer* ausführen.
- Administratoren können alle Windows Installier-Dateien ausführen.

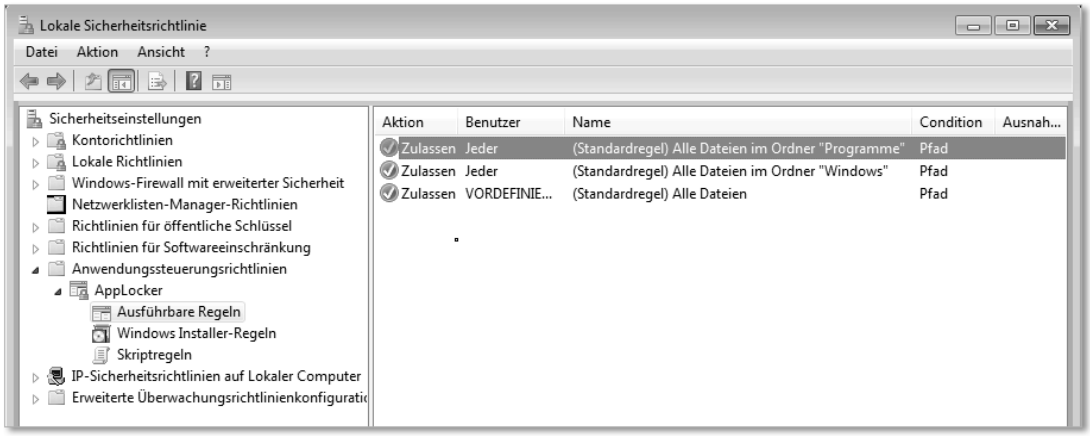


Abbildung 12.120 Die drei Standardregeln für ausführbare Dateien

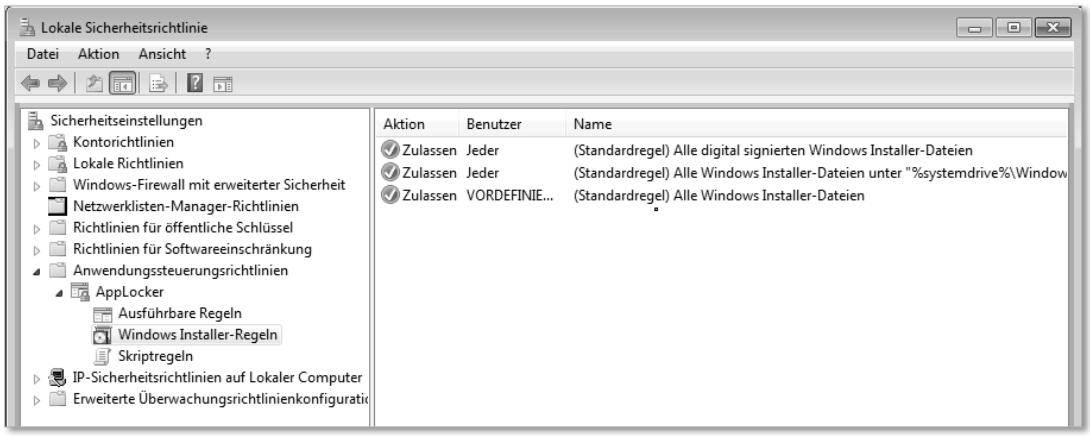


Abbildung 12.121 Die drei Standardregeln für Windows Installer-Dateien

Dass Benutzer bestimmte Windows Installer-Dateien ausführen können, ändert übrigens nichts daran, dass einfache Anwender keine Installationsvorgänge durchführen dürfen, die administrative Rechte erfordern.

Die Standardregeln für Skripts entsprechen übrigens denjenigen für ausführbare Dateien und sind daher nicht abgebildet.

Es bleibt noch zu klären, was genau unter ausführbare Regeln, Windows Installer-Regeln und Skriptregeln fällt. Tabelle 12.1 schafft Klarheit.

Regelsammlung	Zugeordnete Dateiformate
Ausführbare Regeln	*.exe* *.com*
Windows Installer-Regeln	*.msi* *.msp*

Tabelle 12.1 Den Regelsammlungen sind Dateiformate zugeordnet.

Regelsammlung	Zugeordnete Dateiformate
Skriptregeln	*.ps1* *.bat* *.cmd* *.vbs* *.js*
DLLs	*.dll* *.ocx*

Tabelle 12.1 Den Regelsammlungen sind Dateiformate zugeordnet. (Forts.)

Anpassung
Die Standardregeln können natürlich noch angepasst werden, insbesondere sei auf die Möglichkeit hingewiesen, Ausschlüsse für die Regel zu erstellen.

Erzwingung konfigurieren

Um AppLocker tatsächlich »scharf« zu schalten, müssen Sie nun nur noch die Erzwingung konfigurieren. Dies geschieht in einem EIGENSCHAFTEN-Dialog, den Sie über das Kontextmenü des APPLOCKER-Knotens erreichen. Viel Aufregendes gibt es nicht zu konfigurieren (Abbildung 12.122).

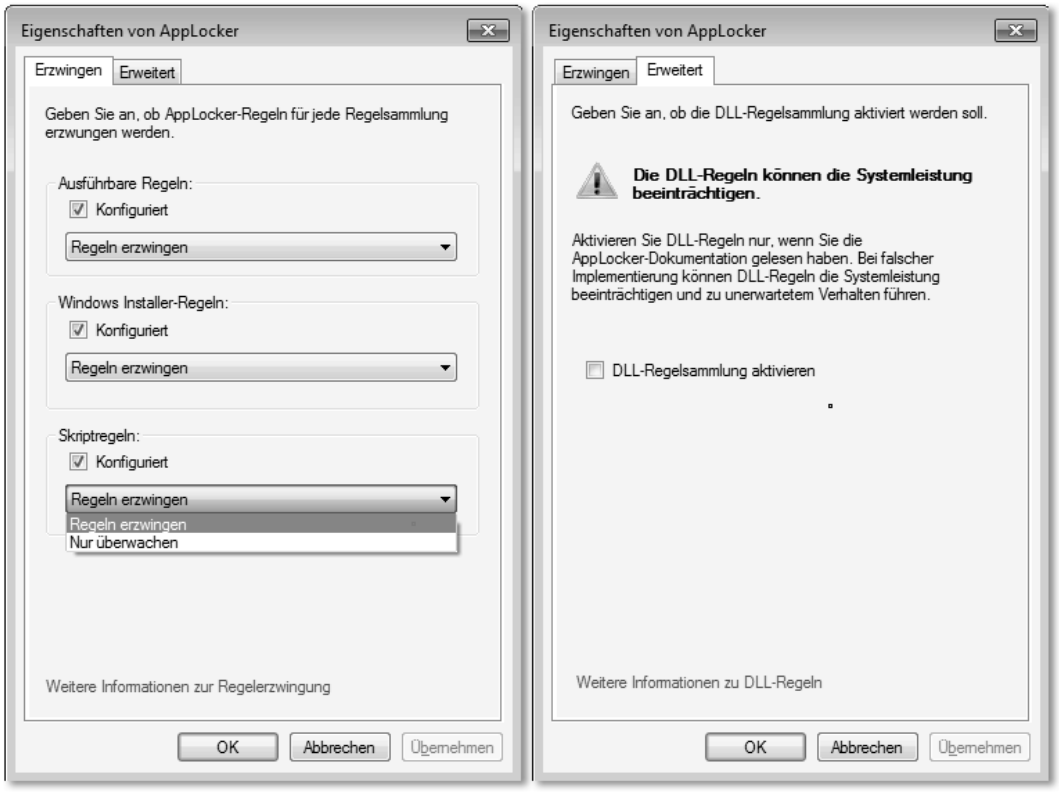


Abbildung 12.122 In den AppLocker-Eigenschaften konfigurieren Sie die Erzwingung.

- Sie können für jede der drei Regelsammlungen festlegen, ob diese konfiguriert ist (das ist sozusagen der Hauptschalter) und ob Sie die REGELN ERZWINGEN möchten oder NUR ÜBERWACHEN wollen.
- Auf der Registerkarte ERWEITERT können Sie AppLocker anweisen, alle DLLs, die von ausgeführten Programmen angesprochen werden, auf Zulässigkeit zu überprüfen. Wenn die Ausführung einer DLL nicht durch eine Regel abgedeckt ist, kann diese nicht verwendet werden. Falls die Anwendung derlei Fehler nicht sauber abfängt, kann es zu dem im Dialog genannten UNERWARTETEN VERHALTEN kommen.

Regelsammlung

Wenn Sie die DLL-REGELSAMMLUNG AKTIVIEREN, werden Sie in der Baumansicht eine weitere Regelsammlung vorfinden, in der Sie ebenfalls Standardregeln erstellen können.

Testen

Zum ersten Test habe ich eine Anwendung in den *C:\temp*-Ordner kopiert. Wenn die Standardregeln erzwungen werden, kann die Anwendung nicht starten – viel mehr ist dazu nicht zu sagen (Abbildung 12.123). Wenn sich die die ausführbare Datei unterhalb von *C:\Programme* befindet, kann sie erwartungsgemäß gestartet werden.

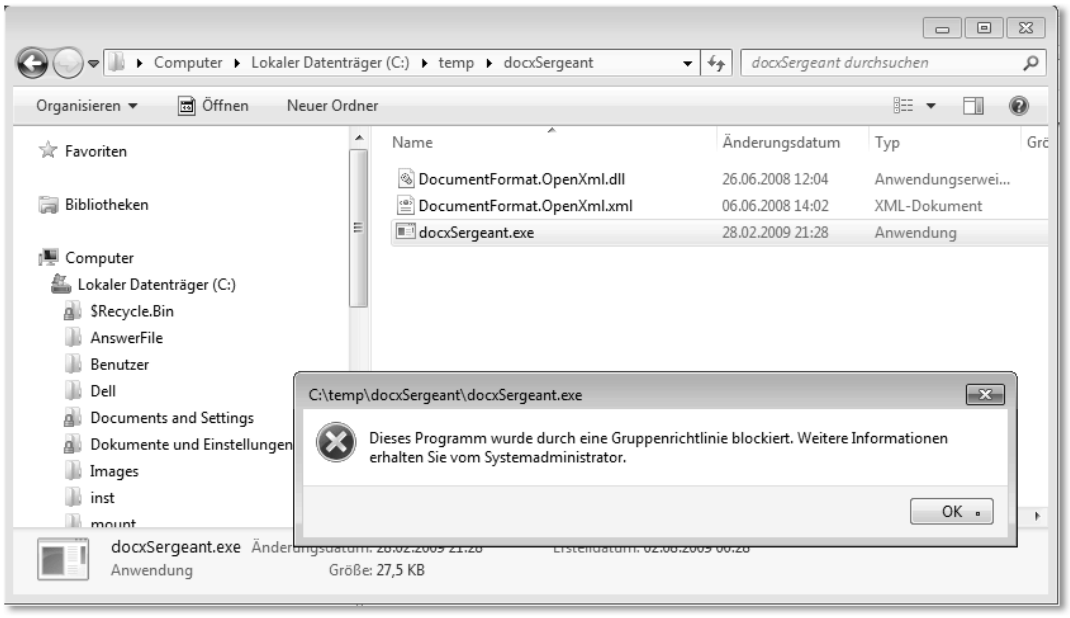


Abbildung 12.123 AppLocker verhindert den Start einer Anwendung.

Ist für die Regelsammlung der Audit-Modus (NUR ÜBERWACHEN) gewählt, startet die Anwendung, und im Ereignisprotokoll wird ein Eintrag erzeugt, der darauf hinweist, dass diese Datei eigentlich blockiert worden wäre (Abbildung 12.124).

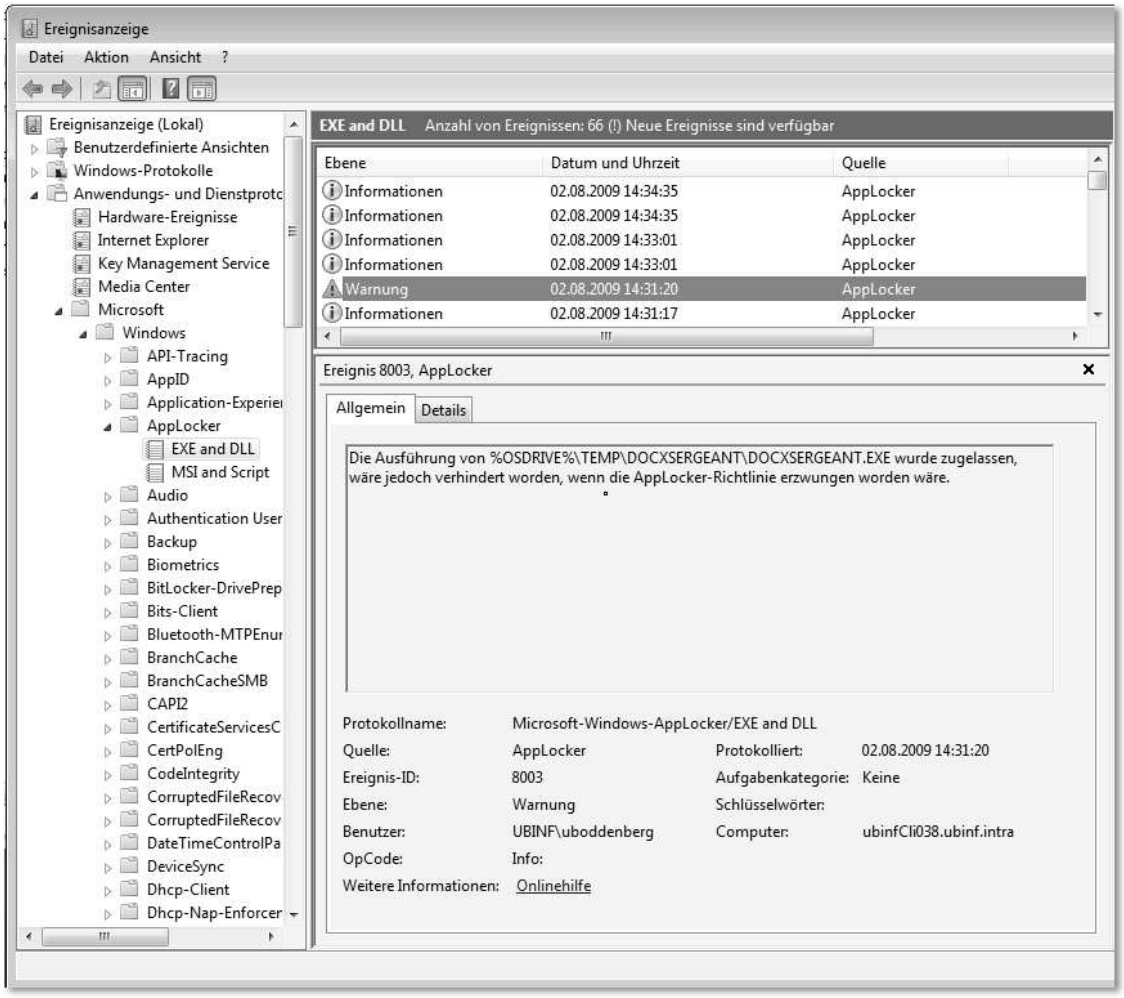


Abbildung 12.124 Im Audit-Modus protokolliert AppLocker die Zugriffe, die eigentlich geblockt werden würden,

12.5.2 Regeln erstellen

In vielen Fällen genügen vielleicht schon die Standardregeln, sprich: Wenn die Benutzer keine Programme außerhalb von *C:\Programme* oder *C:\Windows* ausführen müssen, brauchen Sie nichts weiter zu tun.

Wenn Sie allerdings mit Programmen arbeiten, die in anderen Pfaden liegen, müssen Sie zusätzliche Regeln erstellen. Das ist nicht schwer – in den nächsten Abschnitten zeige ich Ihnen die Möglichkeiten.

Regeln automatisch generieren

Recht hilfreich ist ein Assistent, der über den Menüpunkt Regeln automatisch generieren aufgerufen wird (Abbildung 12.125). »Automatisch generieren« bedeutet, dass anhand von Eingangsparametern (genauer gesagt einer Pfadangabe) eine oder mehrere Regeln erstellt werden.

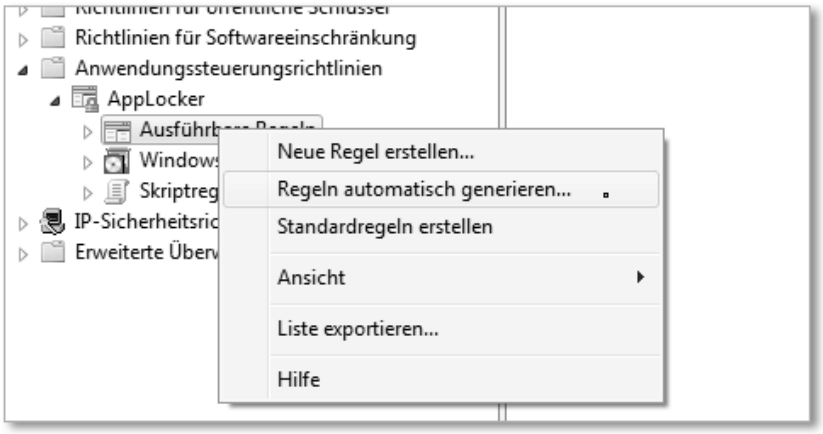


Abbildung 12.125 Hilfreich ist die Funktion zum automatischen Generieren von Regeln.

Der Assistent für das automatische Generieren einer Regel erfasst auf der ersten Seite folgende Angaben (Abbildung 12.126):

- In der ersten Zeile wird nach dem Ordner gefragt, der die zu analysierenden Dateien enthält. Anschließend werden die Dateien in diesem Ordner (und in darunter befindlichen Ordnern) analysiert und Regeln erstellt, die deren Ausführung zulassen.
- Die nächste Angabe bezieht sich auf die Benutzer, die die Applikation starten können sollen. Standardmäßig vorgegeben ist JEDER. Sie können aber beliebige andere Benutzer angeben.
- Die dritte Angabe ist ein Name, mit dem die erstellten Regeln benannt werden.

Auf der nächsten Dialogseite wird konfiguriert, welcher Regeltyp verwendet werden soll. Es wird empfohlen, eine Herausgeberregel zu erstellen, was bedeutet, dass die zulässigen Dateien anhand ihrer digitalen Signatur ermittelt werden. Sofern die Dateien nicht signiert sind, können *Dateihashs* oder der Dateipfad verwendet werden. Bei Dateihashs wird sozusagen eine Prüfsumme über jede einzelne Datei erstellt.

Sofern Sie keine Herausgeberregel verwenden möchten, kann die Verwendung von Dateihashs als primäre Variante konfiguriert werden (Abbildung 12.127).

Sofern Sie mit Dateihashs arbeiten, muss für jede zur Ausführung zugelassene Datei eine eigene Regel erstellt werden. Bei Verwendung der digitalen Signatur kann eine Regel ausreichend sein. Die Erstellung von Regeln, die auf digitalen Signaturen basieren, sehen Sie im nächsten Abschnitt ausführlicher.

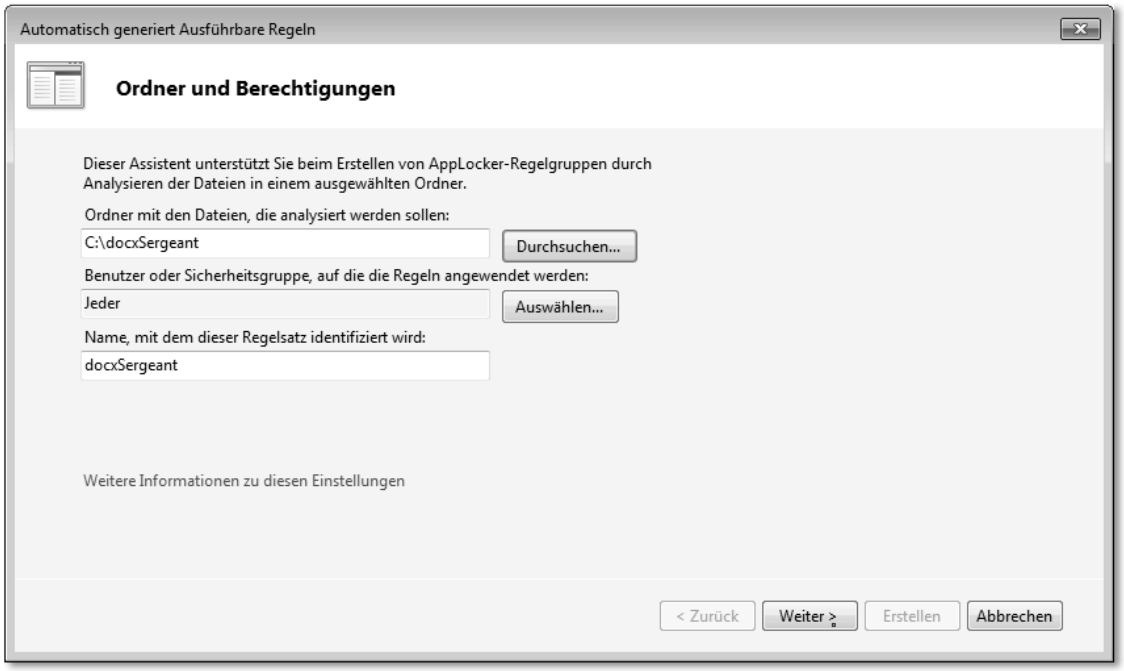


Abbildung 12.126 Dem Assistenten wird ein Pfad zur »Analyse« der Dateien vorgegeben.

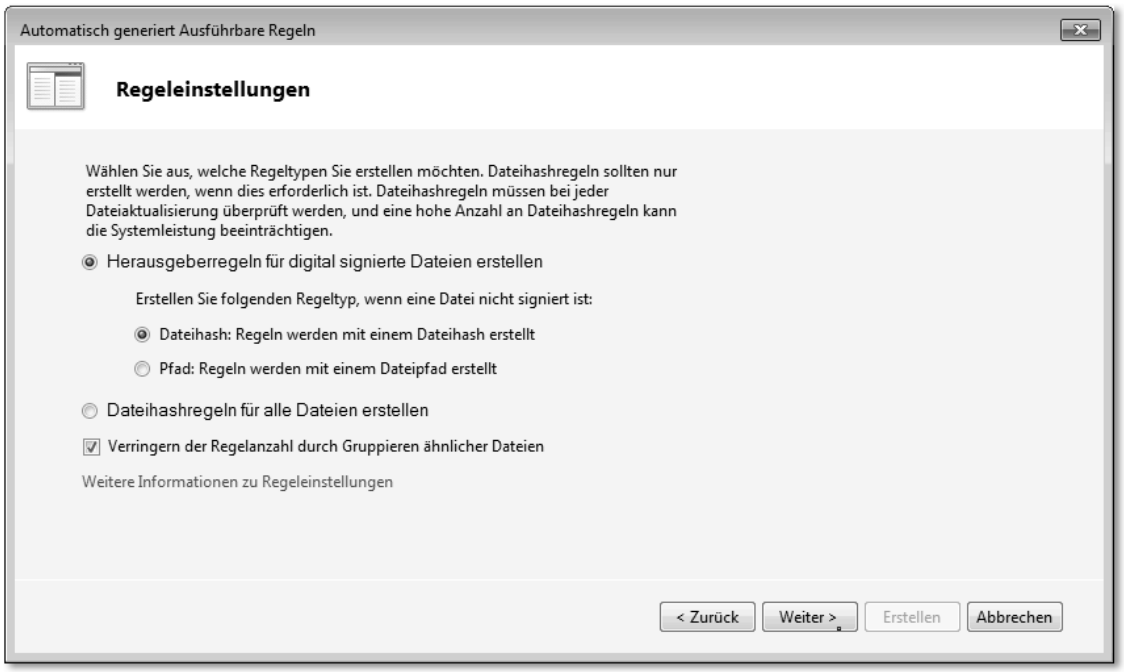


Abbildung 12.127 Entscheiden Sie, welcher Regeltyp erstellt werden soll.

Die letzte Seite des Assistenten zeigt Ihnen, wie viele Regeln erstellt würden, außerdem können Sie eine Vorschau aufrufen (Abbildung 12.128). Wenn Sie die Erstellung der Regeln bestätigen, finden sich diese wenige Augenblicke später in der AppLocker-Konfiguration.

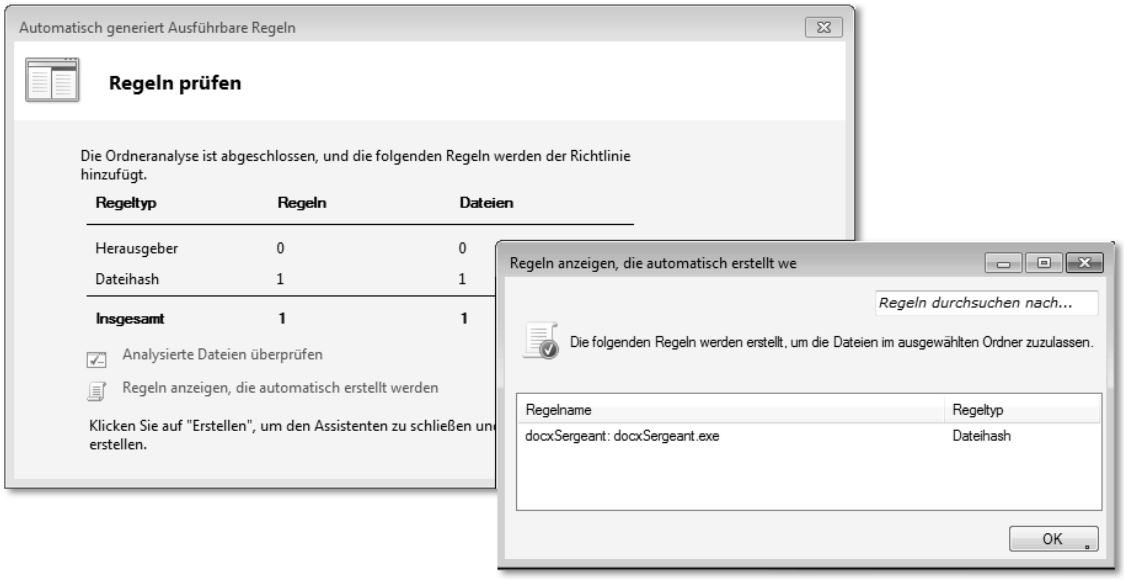


Abbildung 12.128 Vorschau auf die zu erstellenden Regeln

Regeln manuell erstellen

Es ist natürlich möglich, eine Regel ohne exzessive Automatisierungsunterstützung, also ganz manuell, zu erstellen. Wenn Sie den Menüpunkt NEUE REGEL ERSTELLEN wählen, gelangen Sie in einen Assistenten, der Sie durch diesen Vorgang führt.

Der erste Schritt beinhaltet die Entscheidung, ob Sie eine Zulassungs- oder eine Verweigerungsregel erstellen möchten. Außerdem können Sie Benutzer oder Gruppen angeben, für die diese Regel gelten soll. Auf Abbildung 12.129 wird eine Zulassungsregel erstellt, die für sämtliche Benutzer gültig sein soll.

Auf der zweiten Dialogseite wählen Sie, auf welchem Regeltyp die neue Regel basieren soll; es gibt drei Möglichkeiten (Abbildung 12.130):

- Eine Herausgeberregel basiert auf der digitalen Signatur der zuzulassenden Dateien – das bedingt natürlich, dass die Dateien tatsächlich signiert sind. Bei einem »vernünftigen« Softwarehersteller sollte das heute, im Jahre 2009, der Fall sein.
- Eine Pfadregel bezieht sich auf den Pfad, aus dem die Datei gestartet wird.
- Bei einem Dateihash wird über die Datei eine Prüfsumme gebildet.

In vielen Fällen ist die Herausgeberregel am elegantesten. Sie können damit verschiedene »Abstufungen« konfigurieren, indem Sie den Schieberegler auf die gewünschte Position schieben.

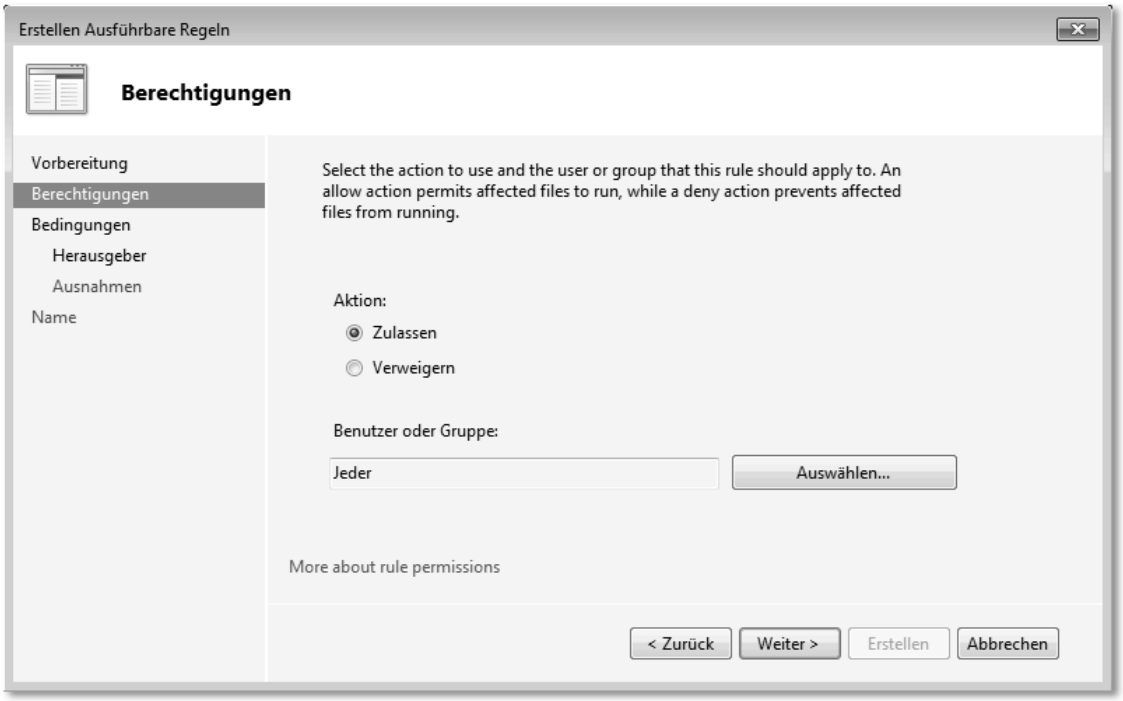


Abbildung 12.129 Legen Sie fest, ob es eine Zulassungs- oder Verweigerungsregel werden soll – und für welche Benutzer die Regel Gültigkeit haben soll.

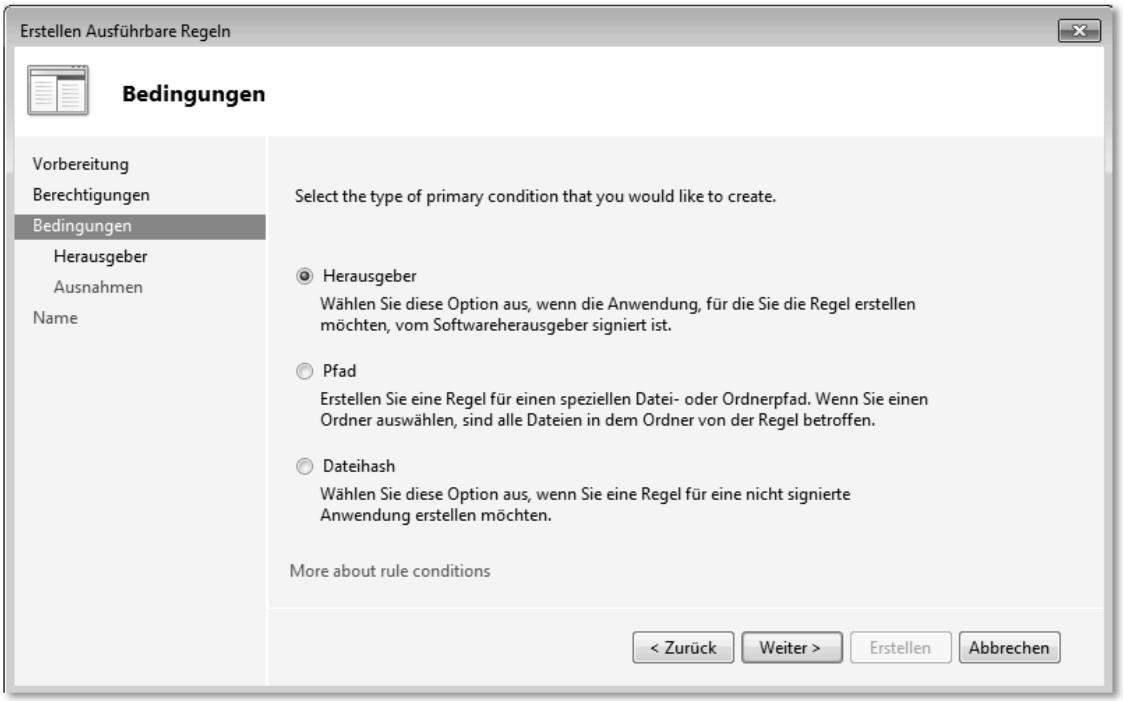


Abbildung 12.130 Wählen Sie die Bedingung. Dieses Beispiel arbeitet mit einer Herausgeberregel.

Die Festlegung erfolgt auf Basis einer auszuwählenden Referenzdatei (Abbildung 12.131, die Referenzdatei ist hier der *Acrobat Reader 9*):

- Sie können allen Dateien dieses Herausgebers, in diesem Fall *Adobe*, zulassen. Dabei ist es egal, wo sich diese im Dateisystem befinden und um welche Programme es sich handelt – Hauptsache sie sind von Adobe.
- Sie können etwas detaillierter werden und mit dieser Regel nur das Produkt *Adobe Reader* zulassen. Version, Dateiname und Speicherort spielen keine Rolle.
- Die nächste Detaillierungsstufe ist die Vorgabe eines Dateinamens.
- Weiterhin können Sie eine bestimmte Version fordern.

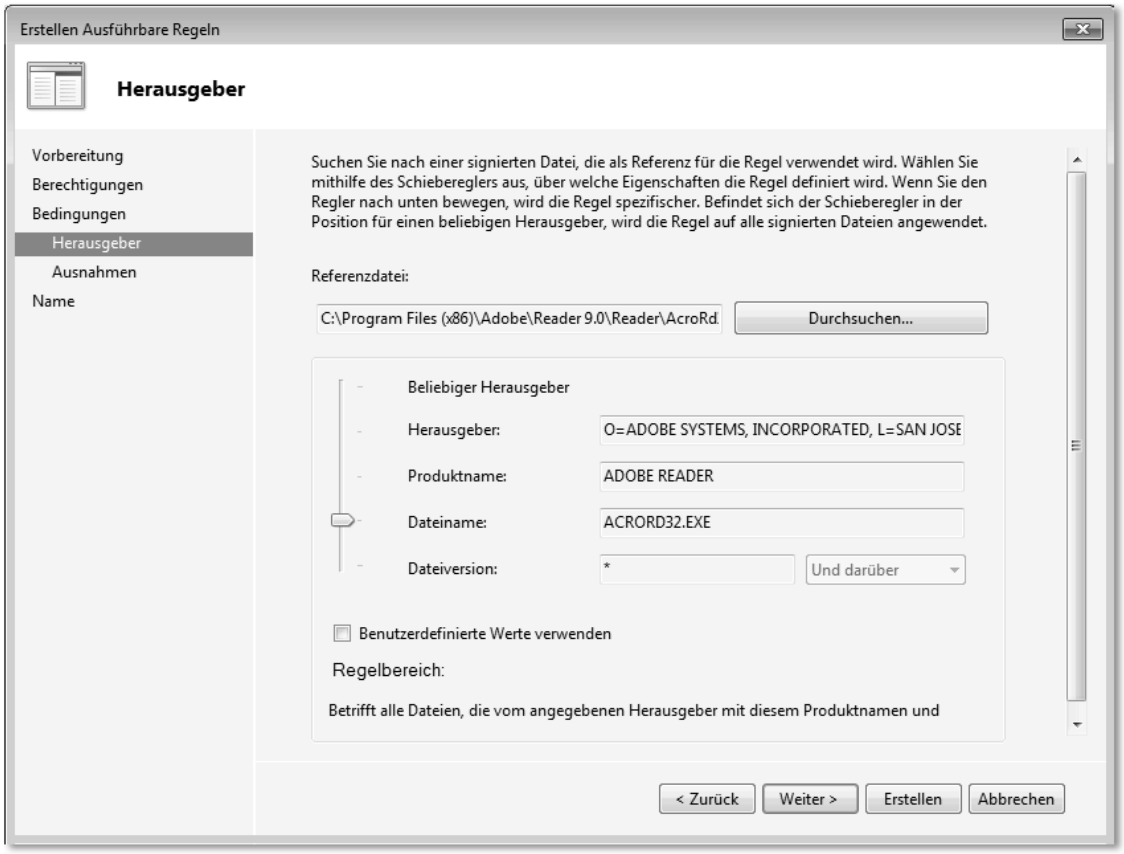


Abbildung 12.131 Auf Basis der Referenzdatei können Sie verschiedene Einstellungen vornehmen.

12.5.3 Konfiguration über Gruppenrichtlinien

Wenn Sie, wie alle Administratoren, nicht nur einen PC administrieren, sondern für viele Systeme verantwortlich sind, werden Sie von der Vorstellung, jeden PC einzeln konfigurieren zu müssen, wenig begeistert sein. Es besteht dazu aber keine Notwendigkeit, schließlich gibt es ja Gruppenrichtlinien. Wenn Sie das bis-

her über AppLocker Gesagte vor Ihrem inneren Auge Revue passieren lassen, werden Sie zwei Schritte sehen:

- Sie müssen festlegen, dass der Dienst *Anwendungsidentität* automatisch startet.
- Sie müssen AppLocker konfigurieren und Regeln erstellen.

Die erstgenannte Aufgabe lässt sich im Gruppenrichtlinienobjekt unter COMPUTERKONFIGURATION • RICHTLINIEN • WINDOWS-EINSTELLUNGEN • SICHERHEITSEINSTELLUNGEN • SYSTEMDIENSTE konfigurieren. Wie immer sagt ein Bild mehr als tausend Worte (Abbildung 12.132).

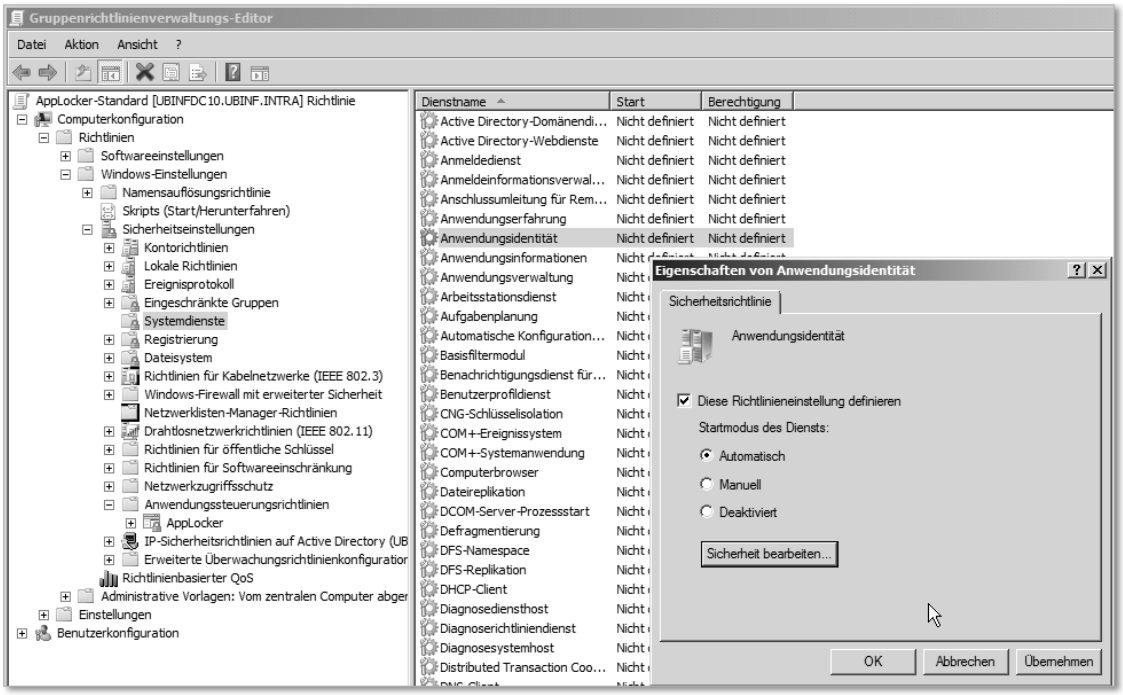


Abbildung 12.132 Sie können per Gruppenrichtlinie konfigurieren, dass der Dienst »Anwendungsidentität« automatisch gestartet wird.

Des Weiteren findet sich unterhalb von COMPUTERKONFIGURATION • RICHTLINIEN • WINDOWS-EINSTELLUNGEN • SICHERHEITSEINSTELLUNGEN • ANWENDUNGSSTEUERUNGSRICHTLINIEN der AppLocker-Knoten (Abbildung 12.133). Die Konfiguration erfolgt genauso wie bei der zuvor gezeigten Erstellung einer lokalen Sicherheitsrichtlinie.

Hinweis

Zu beachten ist, dass Sie die Einstellungen auf einem Windows Server 2008 R2-System vornehmen müssen oder einen Windows 7-PC verwenden müssen, auf dem die *Remote Server Administration Tools* installiert sind. Der Domänencontroller muss nicht auf dem Stand *Windows Server 2008 R2* sein.

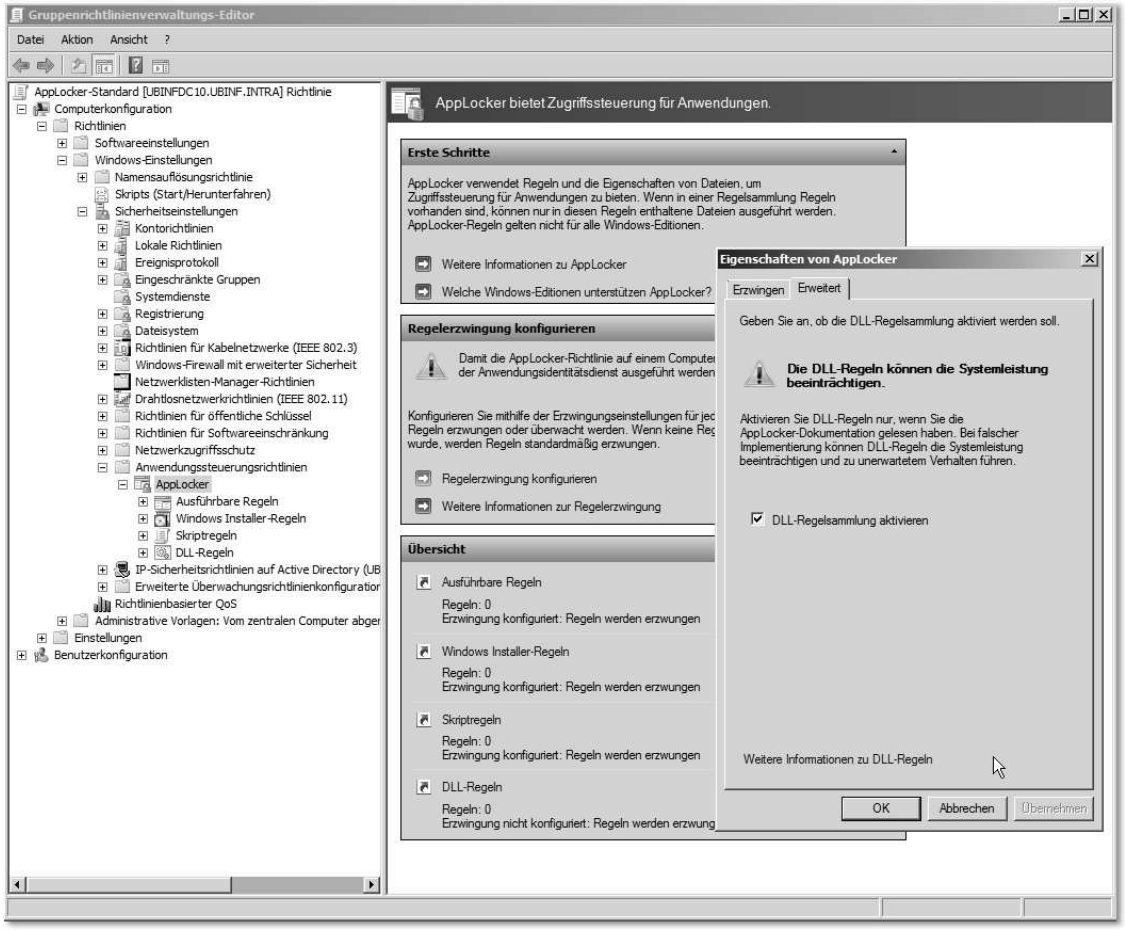


Abbildung 12.133 Sie können per Gruppenrichtlinien die Eigenschaften des AppLocker-Diensts und Regeln konfigurieren.

12.6 Benutzerkontensteuerung (User Account Control)

Mit Windows Vista wurde die Benutzerkontensteuerung (*User Account Control*) eingeführt. Negativ ausgedrückt, handelt es sich um die Funktion, die alle naselang (zumindest bei allen irgendwie systemrelevanten Aktionen) nachfragt, ob der Benutzer dies oder jenes wirklich will.

Ich meine, dass erstens jede zusätzliche Schutzschicht gut und richtig ist und dass es zweitens nicht schaden kann, die Anwender für ihr jeweiliges Tun stärker zu sensibilisieren. Die Benutzerkontensteuerung in Vista ist aus zwei Gründen in die Kritik geraten:

- Die Benutzer und Administratoren fühlten sich bevormundet, da das System immer wieder nachgefragt hat.

- Es gibt durchaus ältere und/oder schlecht programmierte Software, die mit der Benutzerkontensteuerung nicht zurechtkommt und folglich nicht oder nur teilweise funktioniert.

Mit Windows 7 hat Microsoft auf die Kritik reagiert und der Benutzerkontensteuerung ein grafisches Konfigurations-Frontend verpasst. Auf Abbildung 12.134 sehen Sie den Dialog der sich unter SYSTEMSTEUERUNG • SYSTEM UND SICHERHEIT • WARTUNGSCENTER findet: Mit dem Schieberegler wählen Sie eine der vier Stufen aus.

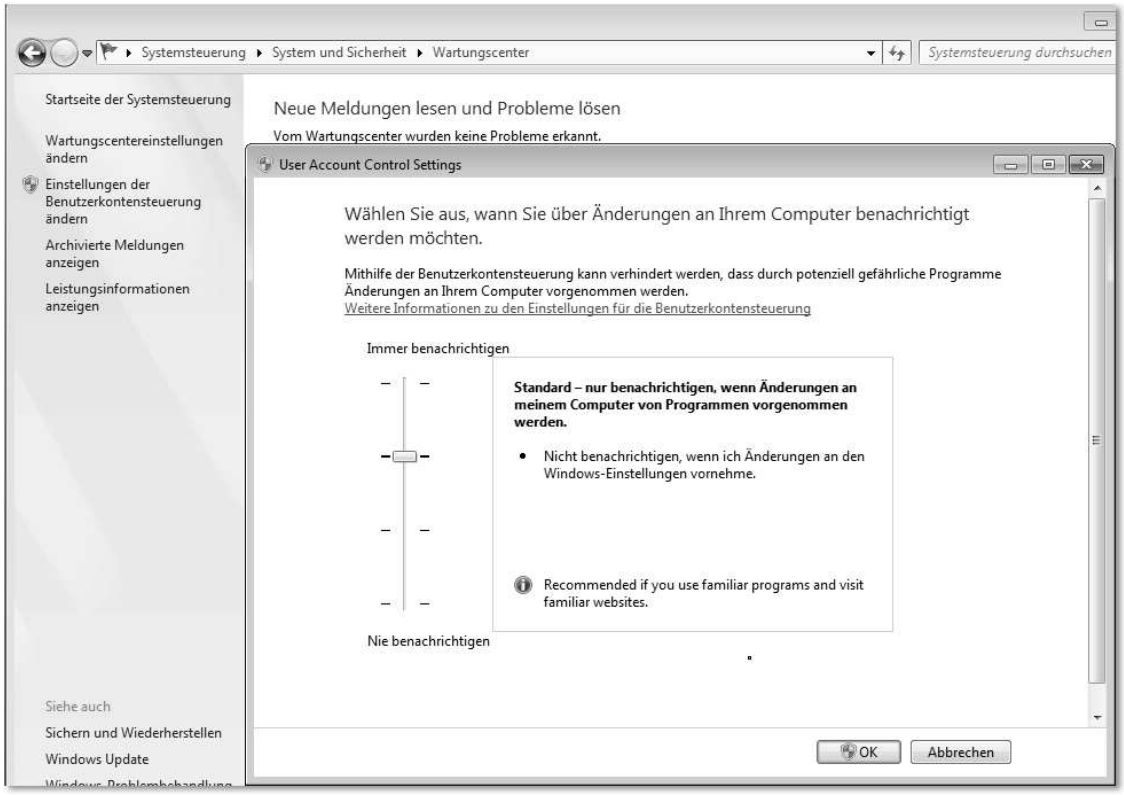


Abbildung 12.134 Die Einstellungen für die Benutzerkontensteuerung kann in Windows 7 konfiguriert werden.

Die Benutzerkontensteuerung kann natürlich über Gruppenrichtlinien konfiguriert werden, Abbildung 12.135 zeigt den entsprechenden Abschnitt im Gruppenrichtlinienverwaltungs-Editor. Anzumerken wäre, dass über Gruppenrichtlinien eine deutlich feinere Konfiguration als mit dem Systemsteuerungsdialog vorgenommen werden kann.

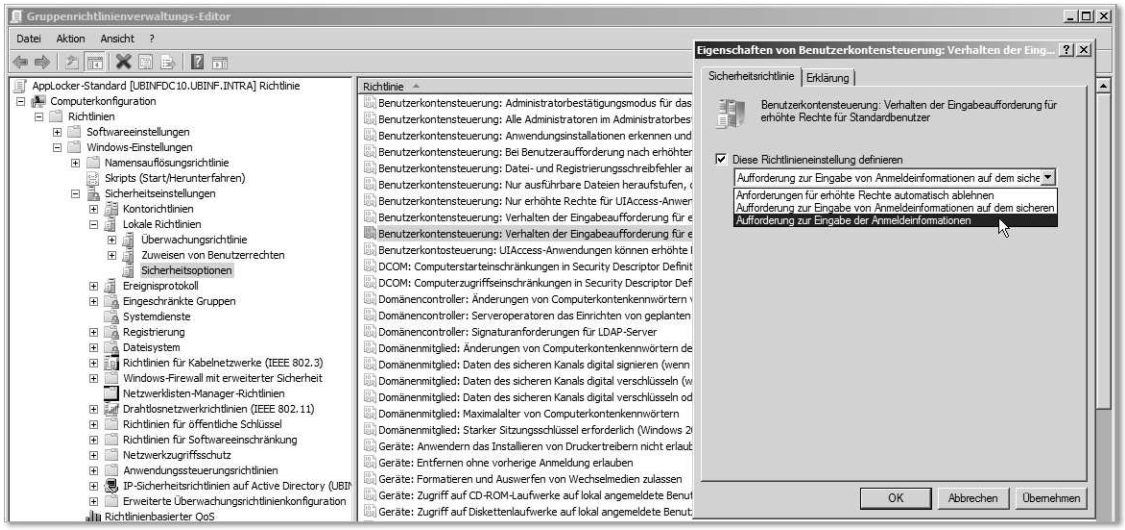


Abbildung 12.135 Detaillierte Einstellungen zur Benutzerkontensteuerung sind über die Gruppenrichtlinien möglich.

12.7 BitLocker

Was ist ein Hauptproblem bei der Benutzung von Notebooks?

Genau, das Gerät könnte verloren gehen oder gar mutwillig und gezielt gestohlen werden. In beiden Szenarien fällt das Notebook nebst Daten in falsche Hände. Nun fragt das Betriebssystem beim Start nach Anmeldeinformationen, aber das hält heute niemanden, der sich auskennt, wirklich auf: Er würde Festplatte aus dem Notebook ausbauen, in einen anderen PC einbauen, die NTFS-Berechtigungen auf der Platte verbiegen – und zugreifen.

Nun gibt es natürlich auch andere Möglichkeiten der Verschlüsselung von Daten, die entweder bereits seit mehreren Versionen erhältlich sind oder zusätzlich eingeführt werden können:

- NTFS ist in der Lage, Dateien zu verschlüsseln.
- Technologien wie die *Active Directory Rights Management Services* (AD RMS) verschlüsseln Daten und vermeiden dabei sogar, dass Passwörter manuell ausgetauscht werden müssen.

Trotzdem ist die Verschlüsselung der kompletten Festplatte für Notebooks eine sehr gefragte Funktion – aus gutem Grund:

- Der Benutzer braucht sich keine Gedanken zu machen, was er konkret tun muss, damit Dateien verschlüsselt werden. Selbst wenn die Anwender am Anfang noch motiviert sind, wird das spätestens nach zwei Tagen nachlassen und es bleiben doch Dokumente unverschlüsselt.

- Auch EFS (*Encrypting File System*, eine Funktion des NTFS-Dateisystems) kann nicht alles verschlüsseln, inbesondere nicht die Betriebssystemdateien.

Mit BitLocker stellte Microsoft erstmals mit Windows Vista einen eigenen Ansatz zur Festplattenverschlüsselung vor – davor musste man auf Drittanbieterprodukte zurückgreifen.

Die Windows 7-BitLocker-Implementation ist gegenüber der Vista-Version an einigen Punkten verbessert worden. Außerdem ist mit *BitLocker To Go* nun auch ein Verschlüsseln von Wechseldatenträgern wie USB-Festplatten und Memory-Sticks möglich.

Hinweis

BitLocker und *BitLocker To Go* erfordern *Windows 7 Enterprise* oder *Ultimate*.

12.7.1 Voraussetzungen

Die erste Voraussetzung habe ich bereits einige Zeilen zuvor genannt, nämlich die Windows 7-Edition: Nur in den Editionen *Enterprise* und *Ultimate* ist die BitLocker-Funktionalität enthalten.

Der zweite Punkt, den ich erwähnen möchte, ist nicht unbedingt eine zwingende Voraussetzung, aber dringend empfehlenswert. Die zu schützende Hardware sollte über ein TPM-Modul verfügen. Hierbei handelt es sich, stark vereinfacht gesagt, um einen Chip, der Verschlüsselungsinformationen speichert.

Sofern Geräte nicht über ein TPM-Modul verfügen, kann BitLocker verwendet werden, allerdings müssen die Benutzer dann den Schlüssel auf einem USB-Stick mit sich führen und diesen bei jedem Start an das Gerät stecken – das kann man machen, aber sonderlich elegant ist das nicht.

Ich würde im Business-Umfeld davon ausgehen, dass eine wirtschaftlich sinnvolle Lösung angestrebt wird. Es ist nun sicherlich nicht sinnvoll, in Uralt-Hardware noch viel Engagement für eine Windows 7-Installation nebst BitLocker-Implementierung zu stecken.

Wenn Sie neue Hardware beschaffen, sollten Sie also unbedingt darauf achten, dass ein TPM-Chip enthalten ist. Bei Business-Geräten ist das generell der Fall, sowohl bei Notebooks als auch bei Desktops. Teilweise muss bei Systemen, die speziell für »kleine Unternehmen« gedacht sind, das TPM-Modul extra hinzukonfiguriert werden: Abbildung 12.136 zeigt das im Beispiel des Dell-Konfigurators bei einem *Vostro*-Notebook (das ist die »Kleine-Unternehmen-Serie« von Dell).

Die Privatanwender-Serien haben im Allgemeinen keinen TPM-Chip. Ich gehe aber ohnehin nicht davon aus, dass im Unternehmensumfeld ernsthaft die Anschaffung von Consumer-Geräten erwogen wird.

Abbildung 12.136 Achten Sie darauf, dass neu zu beschaffende Hardware einen TPM-Chip enthält. (Quelle der Abbildung: Dell-Konfigurator, Vostro-Notebook)

Für den Einsatz von TPM ist eine geeignete Festplattenkonfiguration notwendig. Eine Standardkonfiguration mit nur einer Partition wird von BitLocker nicht unterstützt. Abbildung 12.137 zeigt eine typische Konfiguration:

- Als aktive Systempartition wird eine 200 MB große Partition angelegt.
- Die eigentliche Windows-Partition (korrekter Name: *Startpartition*) nimmt dann den Rest der Platte ein.

Die »große Partition« erhält weiterhin den Laufwerksbuchstaben »C:«, und die »kleine Partition« ist für einen Benutzer, der nicht zufällig in die Datenträgerverwaltung schaut, nicht sichtbar.

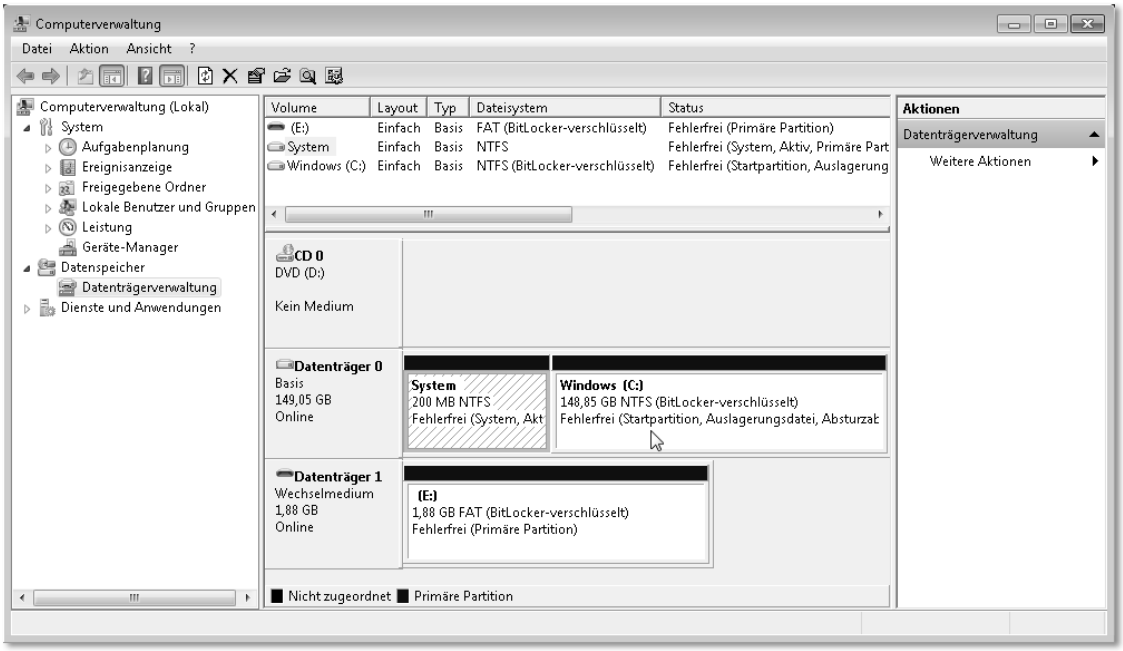


Abbildung 12.137 Die Plattenkonfiguration muss für die Verwendung von BitLocker vorbereitet sein.

Systempartition und Startpartition

Die Begriffe *Systempartition* und *Startpartition* sind durchaus erklärungsbedürftig und verwechselungsgefährdet, auch wenn man damit seit Jahren umgeht. Also:

- Als *Systempartition* bezeichnet man das Volume, das die hardwarespezifischen Dateien (z. B. *Ntldr* und *Ntdetect.com*) beinhaltet, die zum Starten von Windows erforderlich sind.
- Der Begriff *Startpartition* bezeichnet das Volume, auf dem die Windows-Betriebssystemdateien (standardmäßig im Ordner *WINDOWS*) und die Dateien gespeichert sind, die das Betriebssystem unterstützen (standardmäßig liegen sie im Ordner *WINDOWS\System32*).

Die Startpartition kann, muss jedoch nicht, mit der Systempartition identisch sein.

Die Beispiele im Deployment-Kapitel des Buchs (Kapitel 6) sind übrigens durchaus so ausgelegt, dass eine BitLocker-fähige Plattenkonfiguration entsteht.

12.7.2 BitLocker auf einem einzelnen PC einrichten

Wenn Sie einen einzelnen (oder zumindest nur ganz wenige) PCs mit BitLocker-Verschlüsselung konfigurieren möchten, können Sie im Grunde genommen ohne größere Planung loslegen. Schon an dieser Stelle sei darauf hingewiesen, dass diese Ad-hoc-Vorgehensweise nur in den wenigsten Unternehmen die richtige Methode sein wird, denn vermutlich sind mehr als ein oder zwei Notebooks im Einsatz – aber gut, ich werde Ihnen die »spontane« Variante im Schnelldurchlauf zeigen und dann in Abschnitt 12.7.4 auf die Details eingehen. Auf geht's:

Wenn der PC die Voraussetzungen erfüllt, können Sie in der Systemsteuerung, Gruppe SYSTEM UND SICHERHEIT, die Konfiguration der BITLOCKER-LAUFWERKSVERSCHLÜSSELUNG starten (Abbildung 12.138).

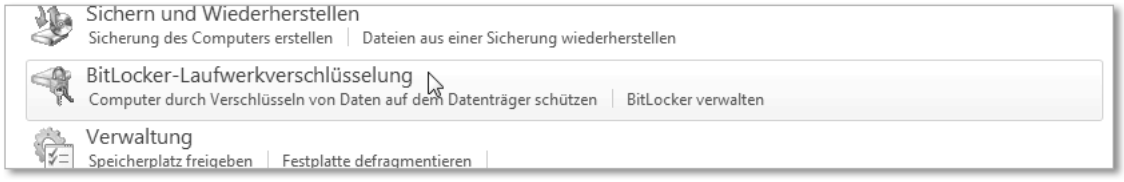


Abbildung 12.138 In der Systemsteuerung, Abschnitt »System und Sicherheit« findet sich der Einstieg in die BitLocker-Konfiguration.

In dem sich nun öffnenden Dialog werden Sie die im PC vorhandenen Festplatten und die extern angeschlossenen Massenspeicher (USB-Festplatte, USB-Stick) sehen. Bei den Geräten findet sich jeweils ein Link, um BitLocker zu aktivieren (Abbildung 12.139).

Der Assistent, der dann startet, stellt zunächst die wichtigste Frage überhaupt, nämlich, wie der Wiederherstellungsschlüssel gespeichert werden soll (Abbil-

dung 12.140). Diesen Schlüssel werden Sie brauchen, beispielsweise wenn Sie die Platte auf einem anderen System entschlüsseln möchten, wenn der TPM-Chip beschädigt ist oder dergleichen mehr. Dieser Schlüssel ist also absolut sensibel – Sie dürfen ihn erstens nicht verlieren und müssen ihn zweitens vor fremdem Zugriff schützen. Sie haben drei Möglichkeiten zur Auswahl:

- Speichern Sie ihn auf einem USB-Stick/Laufwerk.
- Speichern Sie ihn in einer Datei. Hier macht es natürlich keinen Sinn, den Schlüssel auf der Platte des Geräts zu speichern, die im Anschluss verschlüsselt wird. In dem Dialog zur Auswahl des Speicherorts kann auch ein Netzwerklaufwerk ausgewählt werden, was durchaus eine sinnvolle Möglichkeit wäre – vorausgesetzt, der gewählte Speicherort ist hinreichend geschützt.
- Die dritte angebotene Variante ist der Ausdruck des Wiederherstellungsschlüssels. Das hört sich zwar etwas »altertümlich« an, könnte aber durchaus auch Vorteile haben: Papierausdrucke lassen sich vergleichsweise einfach und über lange Zeiträume in feuerfesten Tresoren aufbewahren.

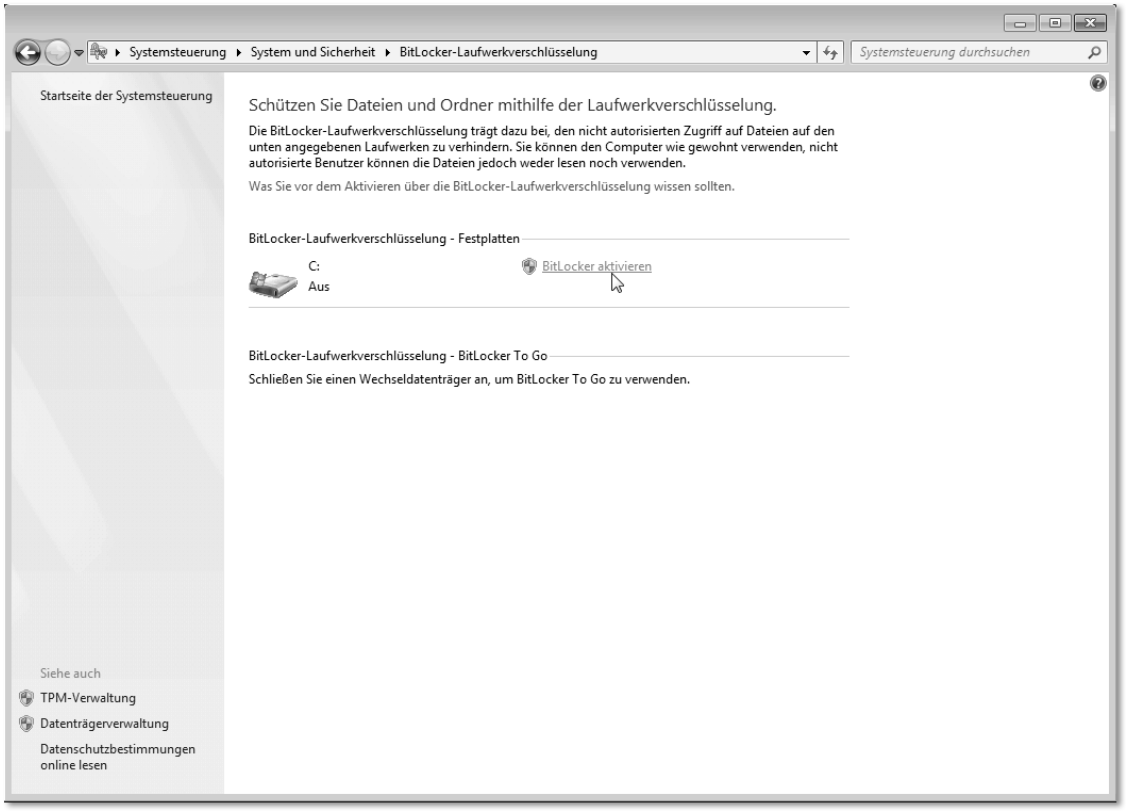


Abbildung 12.139 Hier starten Sie die BitLocker-Aktivierung für das C-Laufwerk.

Bevor die Verschlüsselung startet, bietet der Assistent noch an, eine Systemüberprüfung durchzuführen. Diese Option sollten Sie vorsichtshalber wählen – sicher ist besser.

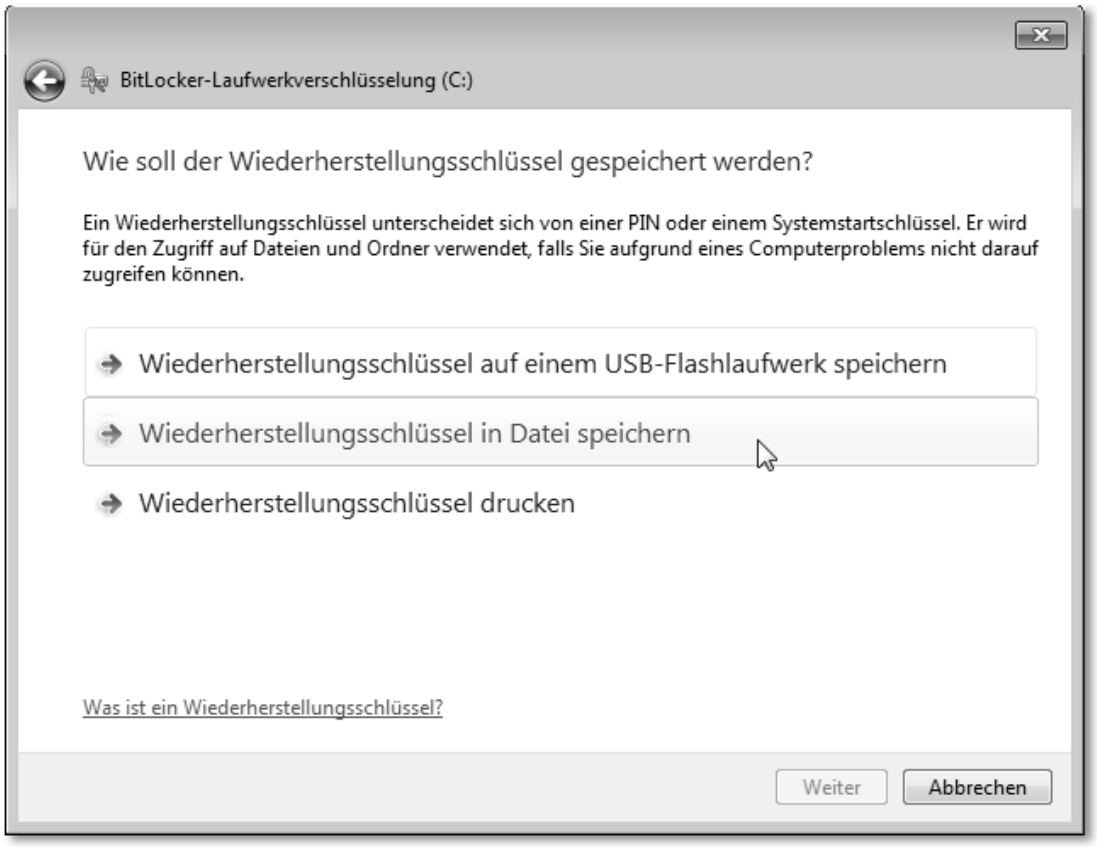


Abbildung 12.140 Der Wiederherstellungsschlüssel muss gespeichert oder gedruckt werden.

Diese Überprüfung soll unter anderem sicherstellen, dass es nicht durch einen »unglücklichen Systemfehler« (z. B. fehlerhafter Schreibzugriff) dazu kommt, dass mit einem anderen Schlüssel als dem verschlüsselt wird, der in der Datei mit dem Wiederherstellungsschlüssel hinterlegt ist. Das wäre fatal, denn eine Wiederherstellung wäre dann einleuchtenderweise nicht mehr möglich (Abbildung 12.141).

Die eigentliche Verschlüsselung wird, je nach Größe der zu verschlüsselnden Festplatte ein Weilchen dauern – zwischen zwanzig Minuten und einer Stunde. Bevor die Verschlüsselung startet, ist ein Neustart fällig, danach wird der Vorgang im Hintergrund ausgeführt. Im System-Tray liegt eine entsprechende Anzeige, die vergrößert werden kann und den aktuellen Fortschritt offenbart (Abbildung 12.142).

Während die Verschlüsselung läuft, zeigt der Explorer übrigens nur noch sehr wenig freien Speicherplatz. Abbildung 12.143 und Abbildung 12.144 zeigen diesen Effekt:

- Während die Verschlüsselung läuft, werden nur knapp 6 GB freier Speicherplatz auf dem Laufwerk angezeigt.
- Nachdem die Verschlüsselung beendet ist, werden die tatsächlichen freien 136 GB angezeigt.

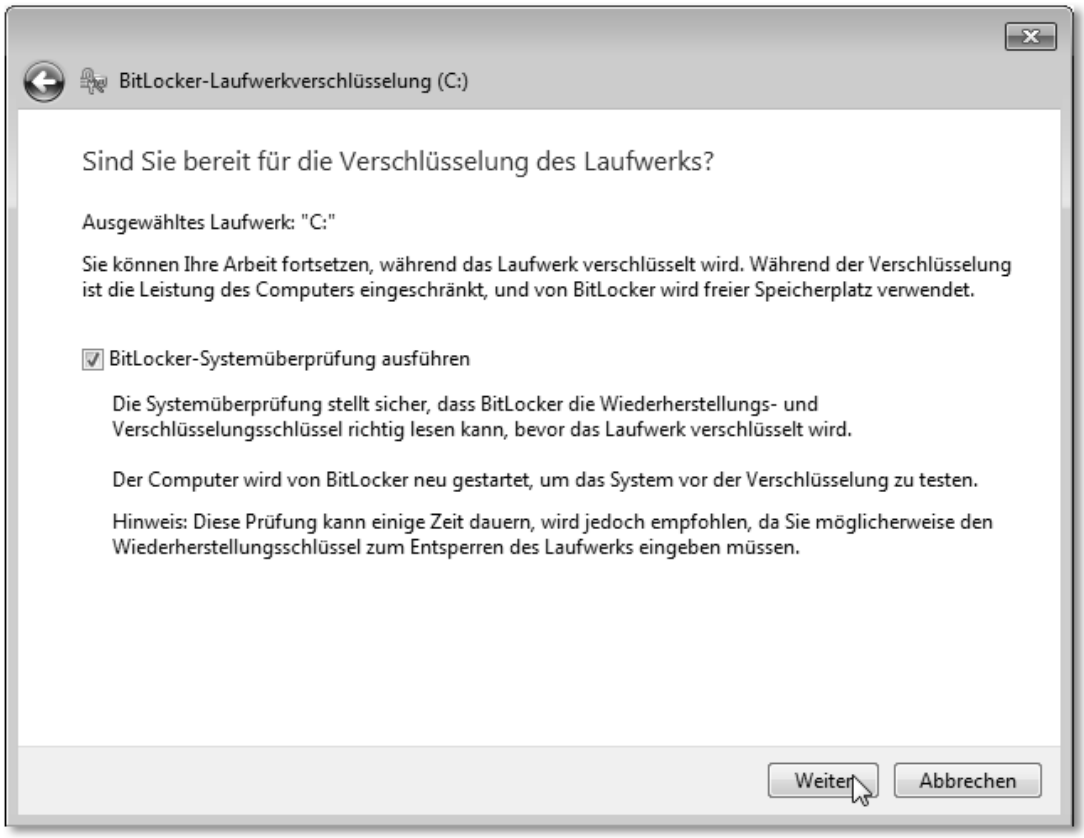


Abbildung 12.141 Letzte Warnung vor dem Beginn. Sicherheitshalber sollten Sie die BitLocker-Systemüberprüfung ausführen.

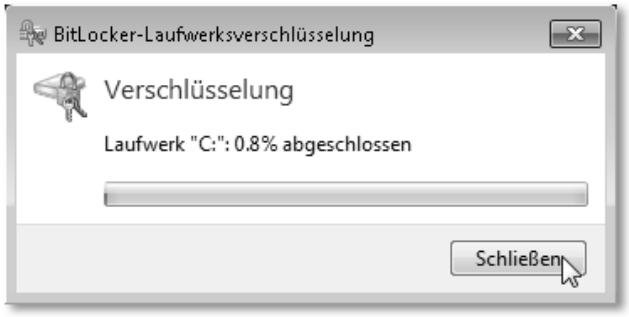


Abbildung 12.142 Danach läuft die Verschlüsselung im Hintergrund. Derweil kann das Laufwerk verwendet werden.

Daraus lässt sich ableiten, dass es nicht unbedingt eine gute Idee ist, größere Datenmengen auf eine Festplatte zu kopieren, die gerade verschlüsselt wird.

Falls Sie sich fragen, wie ein BitLocker-Wiederherstellungsschlüssel aussieht und ob dieser sinnvoll ausdruckbar ist, zeigt Abbildung 12.145 einen solchen. Die ID des Wiederherstellungsschlüssels dient, wie der Name ja schon besagt, zur Identifikation des Schlüssels. Den Schlüssel einzugeben, ist natürlich mühsam, aber eindeutig auch von einem »Papierspeicherort« zu erledigen.

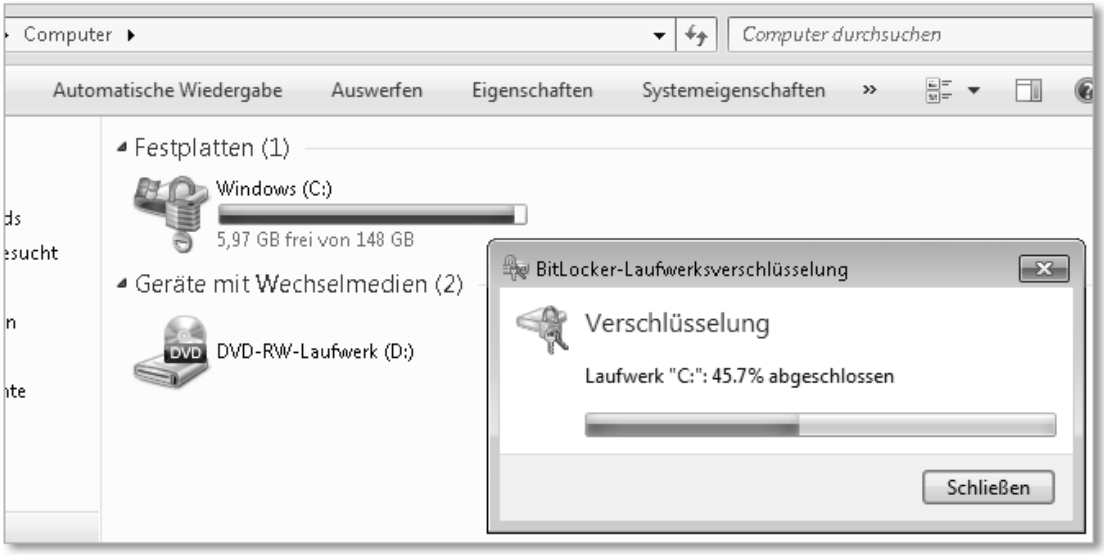


Abbildung 12.143 Während die Verschlüsselung läuft, wird ein recht geringer Prozentsatz freien Speichers angezeigt.

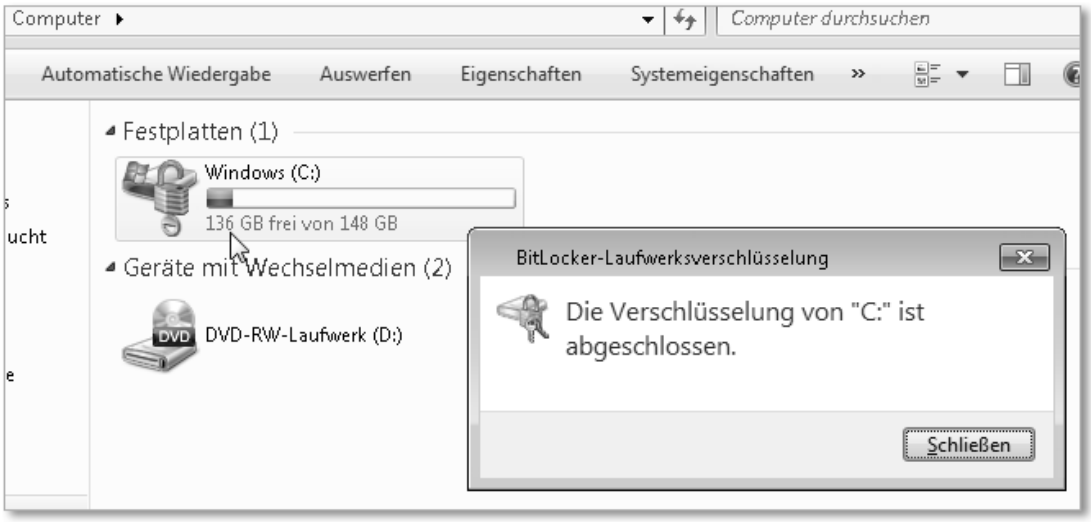


Abbildung 12.144 Nach Abschluss der Verschlüsselung ist so viel freier Speicher wie erwartet verfügbar.

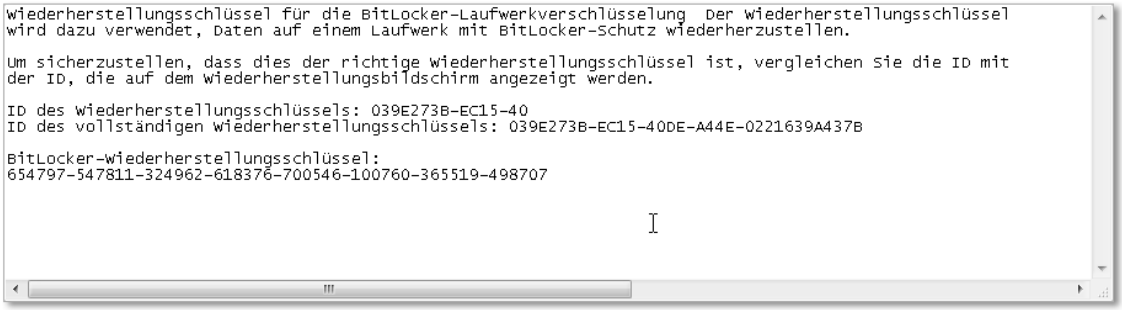


Abbildung 12.145 So (letzte Zeile) sieht übrigens ein BitLocker-Wiederherstellungsschlüssel aus.

12.7.3 BitLocker To Go auf einem einzelnen PC einrichten

Eine Neuerung in Windows 7 ist *BitLocker To Go*. Diese spezielle BitLocker-Variante ist für Wechselmedien gedacht, also für die Verschlüsselung von USB-Sticks, USB-Festplatten und sonstigen Medien. Eine Besonderheit der Wechselmedien ist, dass diese eventuell auch auf einem anderen PC geöffnet werden sollen.

Einrichten

Die Einrichtung von *BitLocker To Go* ist absolut simpel – eine spezielle Partitionierung, wie bei einer Systemplatte ist nicht notwendig. Wenn ein Wechselmedium vorhanden ist, wird dies im Konfigurationsdialog der BitLocker-Laufwerksverschlüsselung angezeigt. Die Konfiguration beginnt mit einfachem Klick auf den entsprechenden Befehl (Abbildung 12.146).

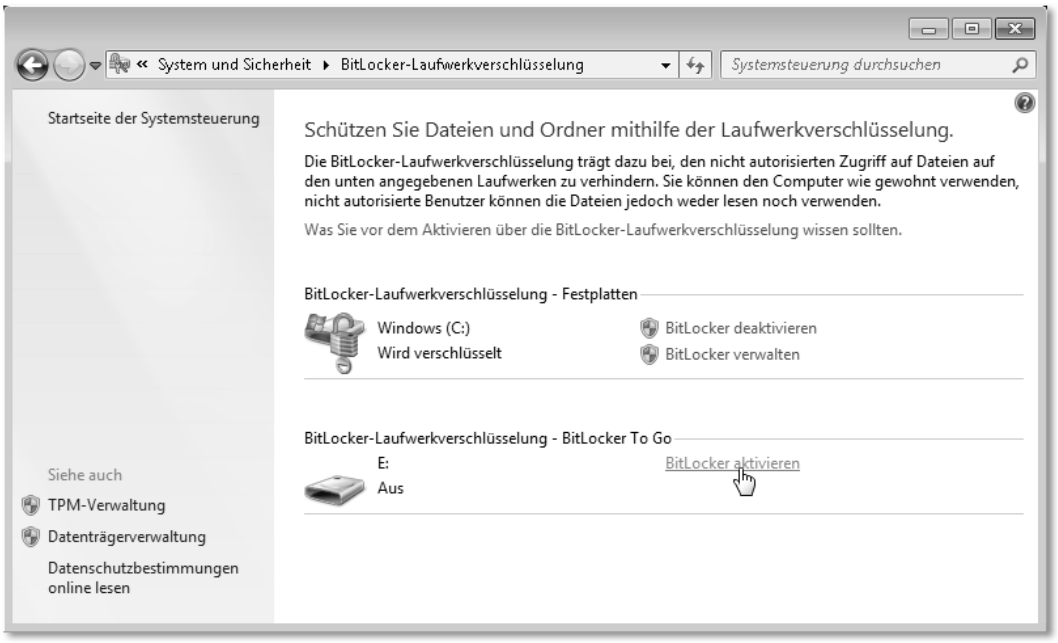


Abbildung 12.146 Ist ein Wechselmedium am PC angeschlossen, wird dessen Verschlüsselung angeboten.

Der Assistent erkundigt sich zunächst nach einer Methode zum Entsperren des Laufwerks, wobei einerseits ein Kennwort eingegeben oder die Verwendung einer Smartcard definiert werden kann (Abbildung 12.147).

Neben dem Kennwort zum Entsperren des Laufwerks wird auch ein Wiederherstellungsschlüssel erzeugt. Dieser wird beispielsweise benötigt, wenn das Kennwort zum Entsperren verloren wurde.

Zur Speicherung des Wiederherstellungsschlüssels werden zwei Möglichkeiten angeboten, nämlich das Speichern in eine Datei (auch auf einem Netzlaufwerk) oder das Ausdrucken des Schlüssels (Abbildung 12.148).

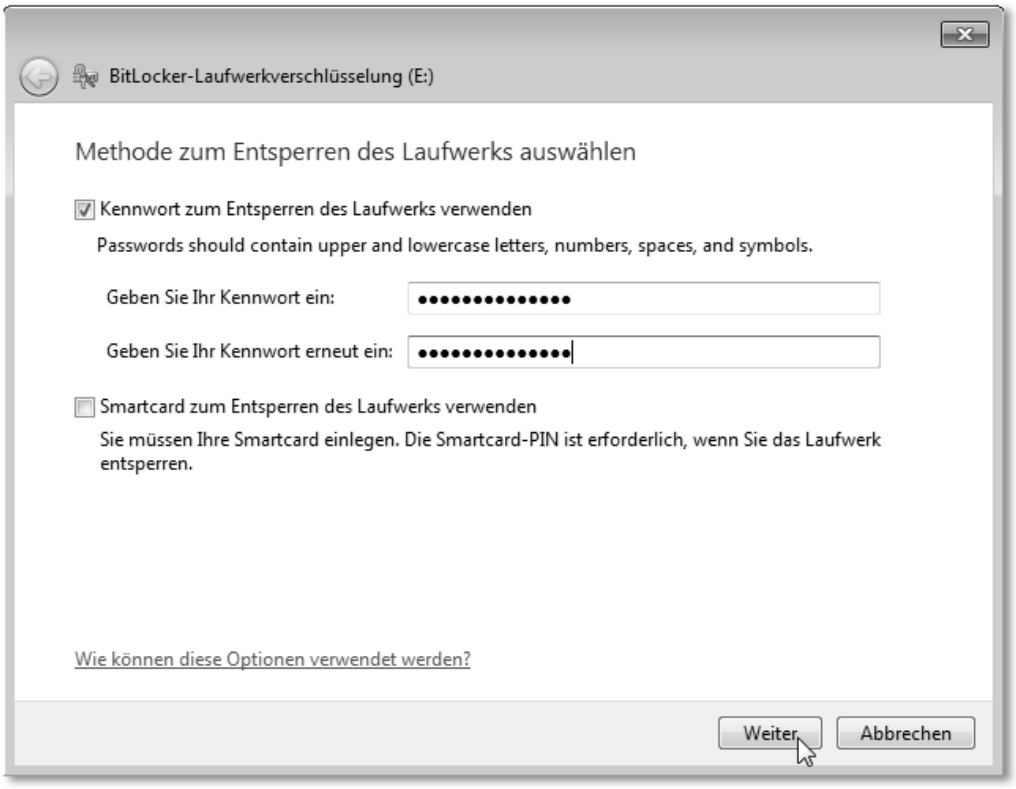


Abbildung 12.147 Zum Entsperren des Laufwerks müssen Sie ein Kennwort eingeben.

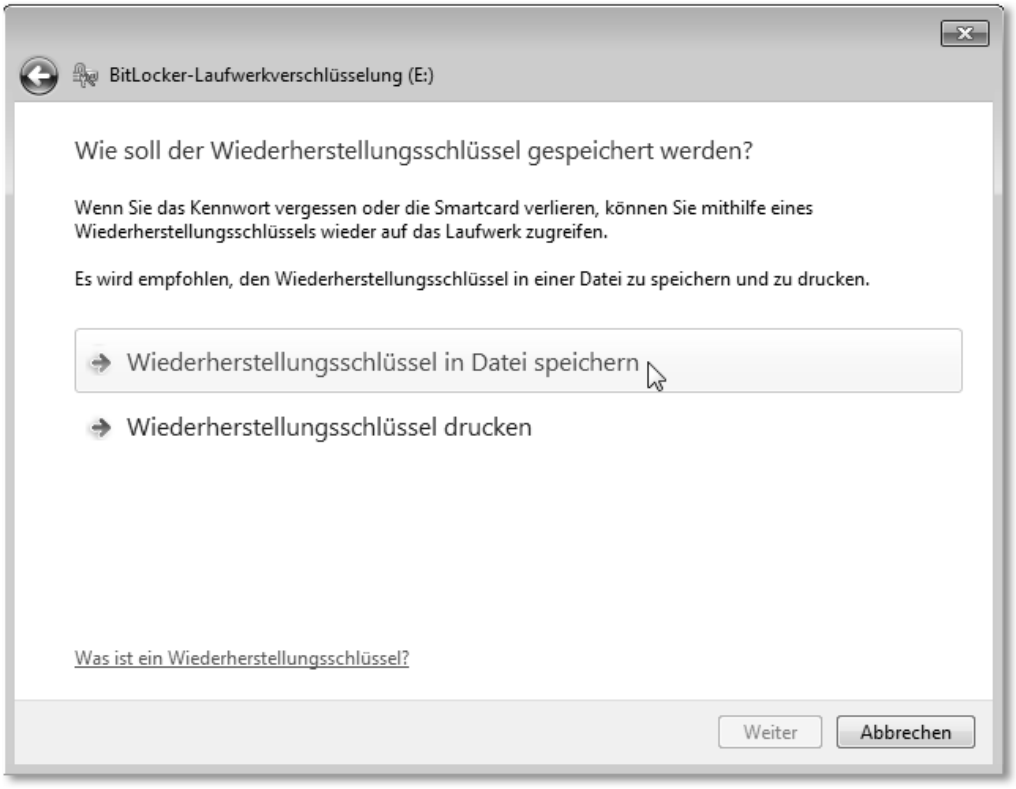


Abbildung 12.148 Den Wiederherstellungsschlüssel können Sie in einer Datei speichern oder ausdrucken.

Nach Abschluss der Verschlüsselung erscheint das Wechselmedium mit einem Schloss gekennzeichnet im Explorer (Abbildung 12.149). Über den Kontextmenü-Punkt BitLocker verwalten gelangen Sie zu einigen hilfreichen Dialogen (Abbildung 12.150), deren Bedeutung wohl nicht näher erläutert werden muss.

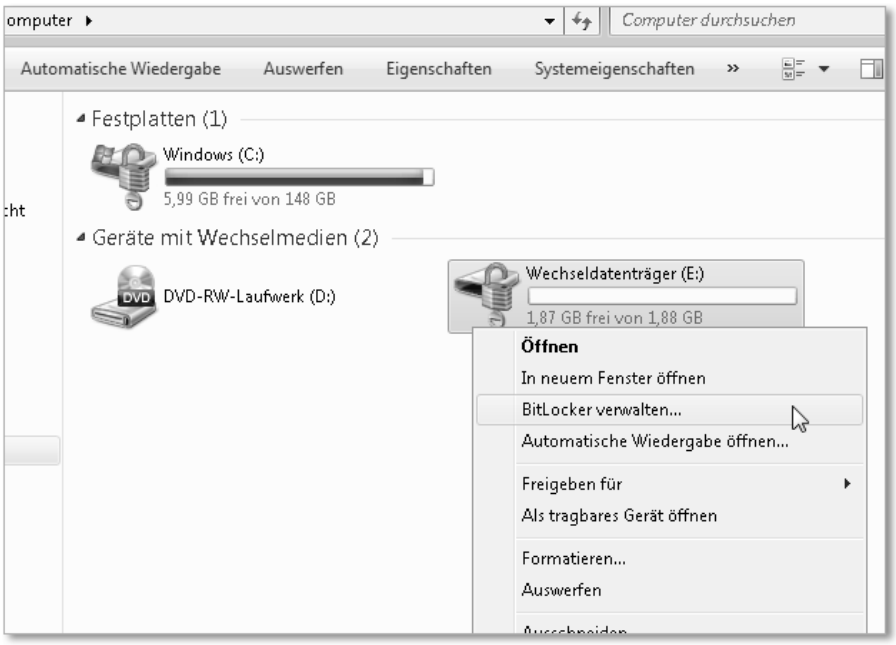


Abbildung 12.149 Zugriff auf die BitLocker-Verwaltung für einen Wechseldatenträger erhält man über den entsprechenden Menüpunkt im Kontextmenü.

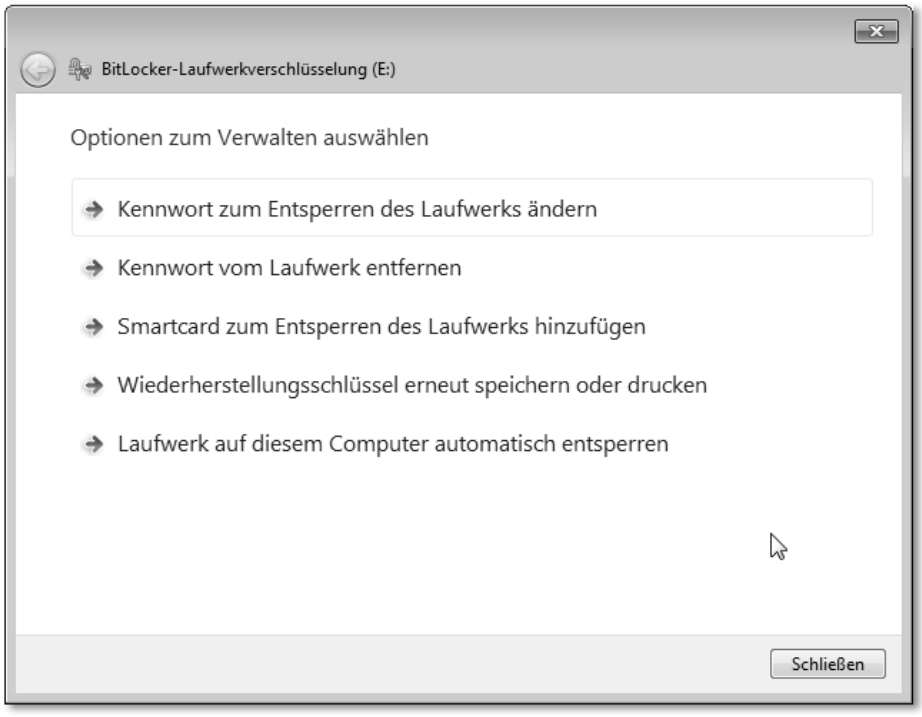


Abbildung 12.150 Diese Optionen stehen für einen mit BitLocker To Go geschützten Wechseldatenträger zur Verfügung.

Auf ursprünglichem PC öffnen

Wenn Sie einen mit *BitLocker To Go* verschlüsselten Wechseldatenträger an den PC anschließen, erscheint unmittelbar nach dessen Erkennung der Dialog aus Abbildung 12.151: eine simple Kennwortabfrage mit der Option, das Kennwort zu merken und den Datenträger auf diesem PC demnächst ohne diese Abfrage zu öffnen.

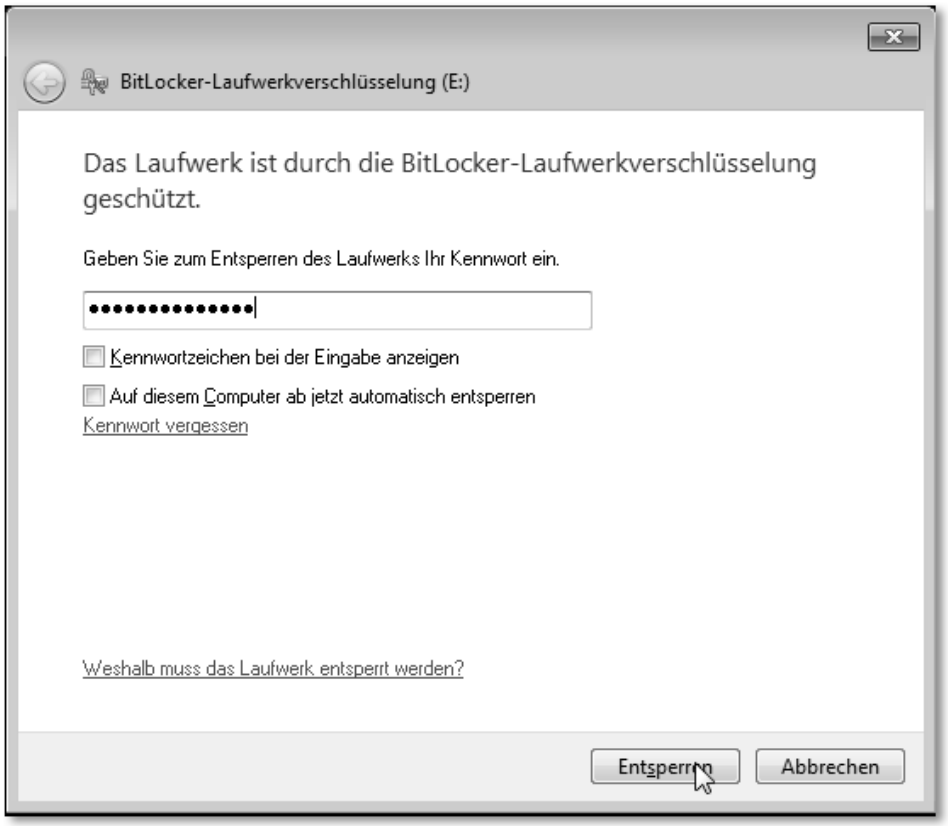


Abbildung 12.151 Wenn ein verschlüsseltes Wechselmedium erkannt worden ist, wird das Entsperrungskennwort erfragt.

Wenn Sie das Kennwort des Wechseldatenträgers vergessen haben, was schließlich auch in den besten Familien vorkommen kann, gibt es den Hoffnung machenden Menüpunkt KENNWORT VERGESSEN (Abbildung 12.151). Wenn Sie diesen gewählt haben, erscheint der Dialog aus Abbildung 12.152, in dem Sie die Eingabe des Wiederherstellungsschlüssels wählen können. Um den richtigen Wiederherstellungsschlüssel zu identifizieren, dient die Angabe der ID (in diesem Fall D0C3C4D8).

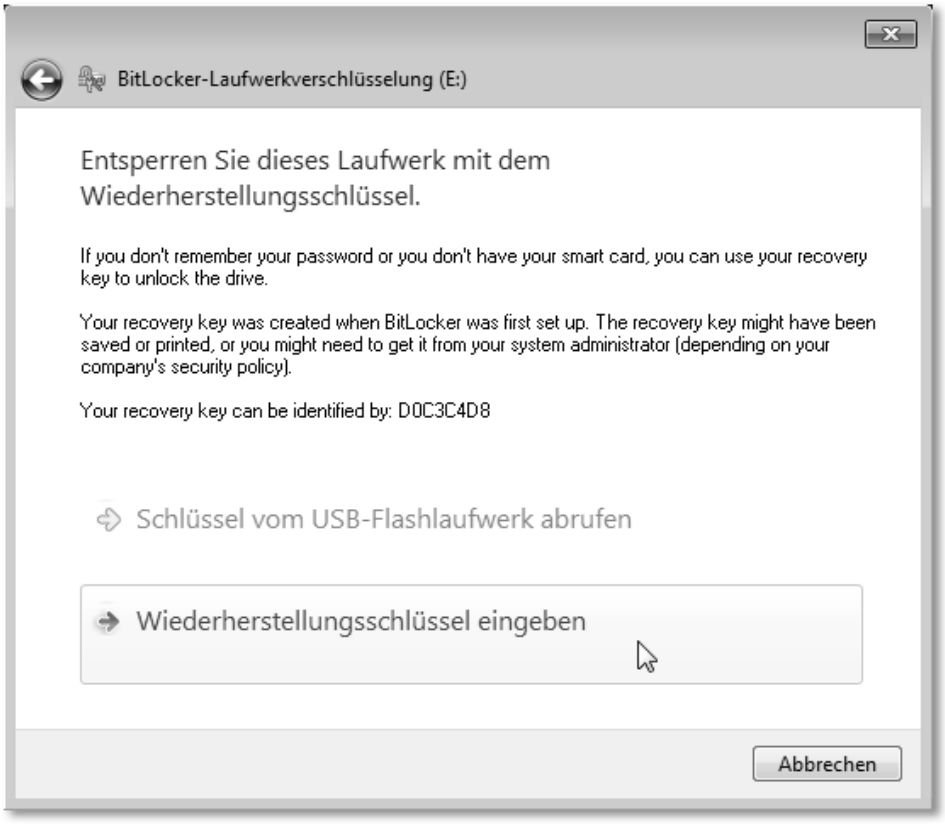


Abbildung 12.152 Wenn das Kennwort in Vergessenheit geraten ist, kann das Laufwerk mit dem Wiederherstellungsschlüssel entsperrt werden.

Auf einem Nicht-Windows 7-PC öffnen

Nun kann man wohl davon ausgehen, dass nicht plötzlich sämtliche PCs dieser Welt mit Windows 7 ausgestattet sein werden. Was passiert, wenn Sie einen mit *BitLocker To Go* verschlüsselten Datenträger auf einem PC mit beispielsweise Windows Vista lesen möchten?

Standardmäßig wird auf dem verschlüsselten Wechseldatenträger eine *BitLockerToGo.exe* gespeichert – dies lässt sich übrigens über eine Gruppenrichtlinie unterbinden (Abbildung 12.153).

Die Datei *BitLockerToGo.exe* enthält das *BitLocker To Go*-Lesetool. Es dient, wie der Name unschwer vermuten lässt, zum Lesen (!) von Daten von verschlüsselten Datenträgern. Ein Mounten des Datenträgers ist nicht möglich, ebensowenig das Schreiben (es ist ja auch ein *Lese*tool). Nach dem Start erkundigt sich das *BitLocker To Go*-Lesetool nach dem Kennwort (Abbildung 12.154).

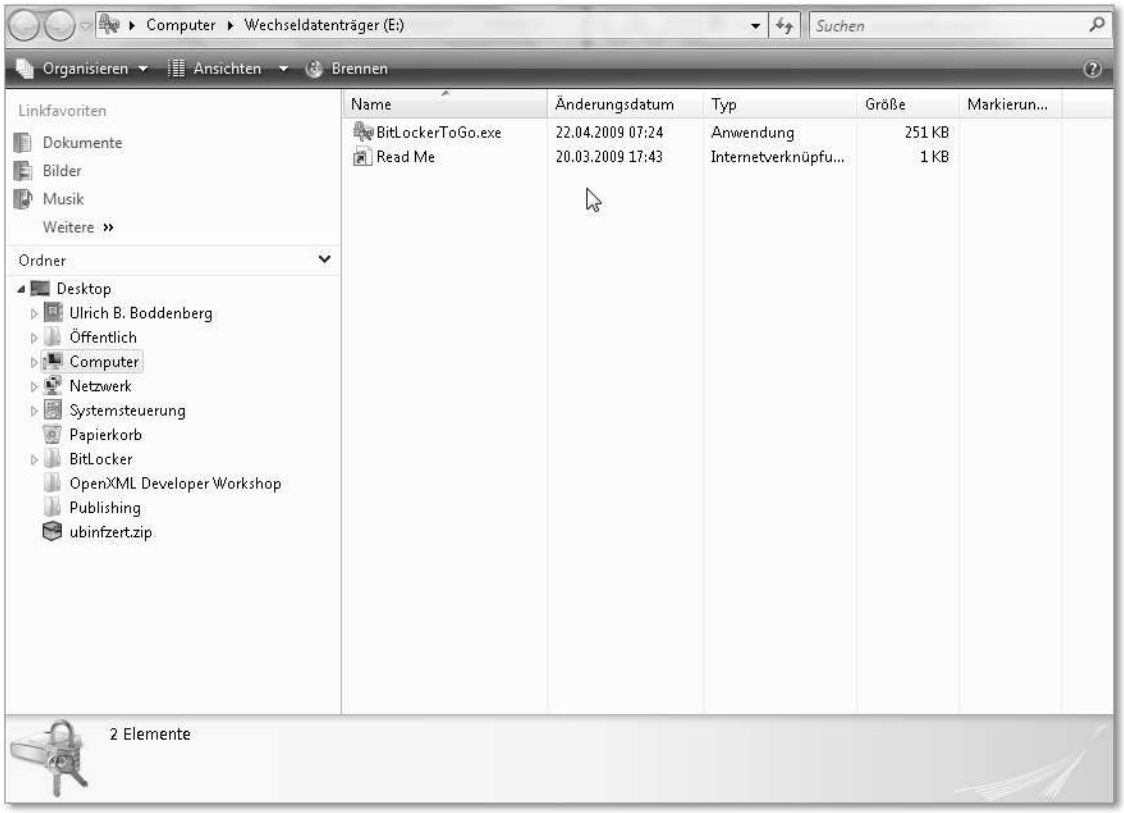


Abbildung 12.153 Auf dem USB-Stick befindet sich eine »BitLockerToGo.exe«-Datei.

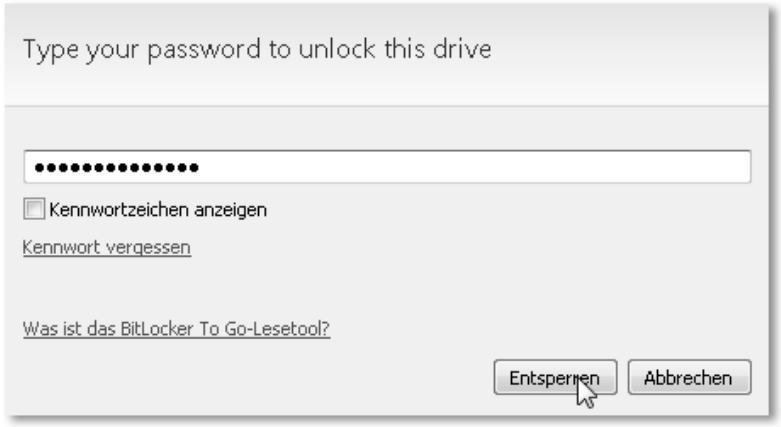


Abbildung 12.154 Beim Start der Anwendung wird das Kennwort abgefragt.

Das Programm zeigt nach erfolgreicher Kennworteingabe die vorhandenen Dateien an, und per Drag&Drop können die Dateien herauskopiert werden. Ein Verändern oder Hinzufügen von zusätzlichen Dateien ist nicht möglich (Abbildung 12.155).

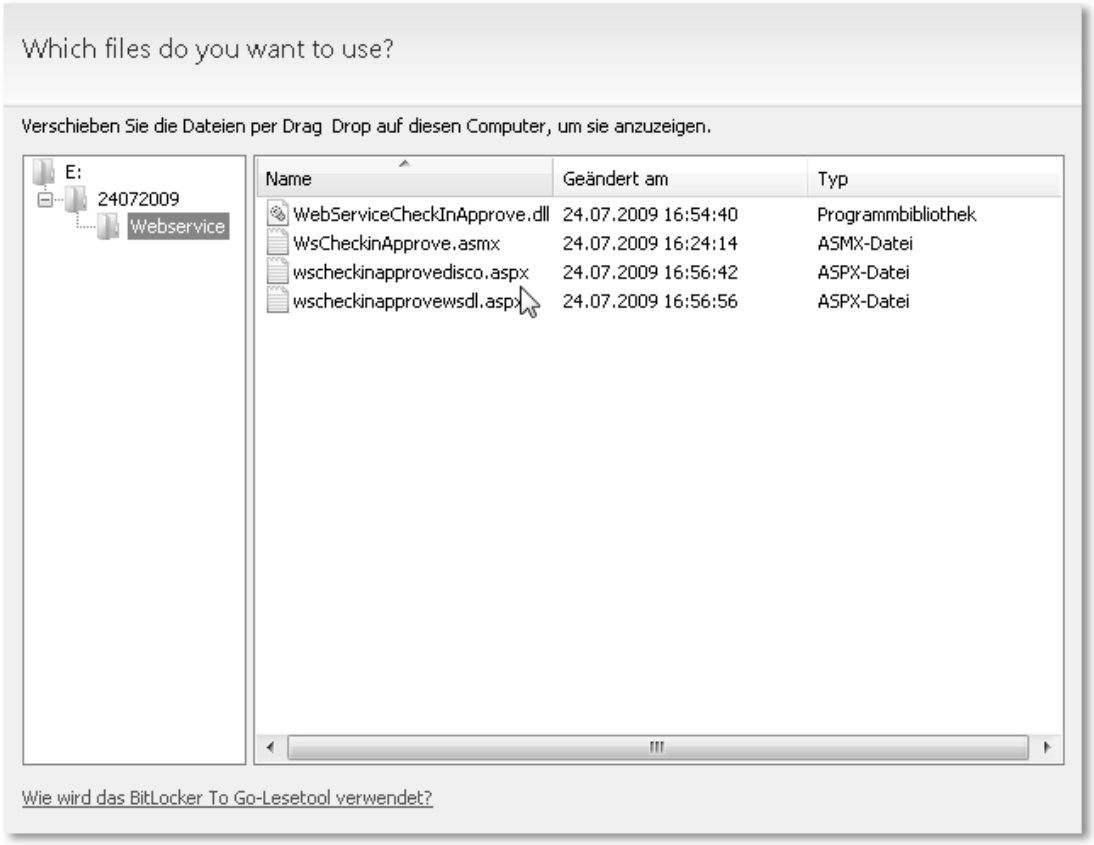


Abbildung 12.155 Die Dateien können mit dem BitLocker-Lesetool von dem verschlüsselten Wechseldatenträger herunterkopiert werden.

12.7.4 AD-Integration

In einer größeren Umgebung mit vielen BitLocker-Installationen ist es durchaus empfehlenswert, die Active Directory-Integration zu nutzen. Diese bringt zwei Vorteile:

- Steuerung der Einstellung über Gruppenrichtlinien
- Speichern der Wiederherstellungsschlüssel im Active Directory

Das Sichern der Schlüssel ist insbesondere auch deshalb wichtig, weil Benutzer Wechselmedien mit BitLocker To Go auch ohne Adminberechtigungen verschlüsseln können.

In den nächsten Abschnitten zeige ich Ihnen, wie Sie die AD-Integration implementieren und nutzen. Man kann wohl getrost davon ausgehen, dass der Durchschnittsanwender die Sicherung seiner Wiederherstellungsschlüssel, sei es durch Speichern der Datei oder Ausdrucken, mit nicht allzu großer Priorität durchführen wird.

AD vorbereiten (Schema-Erweiterung durchführen)

Wenn Sie eine Windows-Server-2008-Domäne betreiben, haben Sie nichts weiter zu tun, denn im Active Directory-Schema auf diesem Stand sind schon die entsprechenden Attribute vorhanden. Dies lässt sich, hinreichend große Neugier vorausgesetzt, mit dem *Active Directory-Schema-Manager* nachprüfen (Abbildung 12.156).

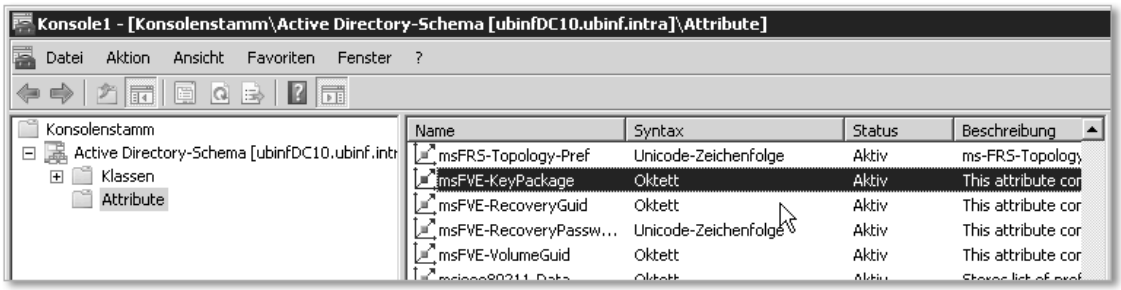


Abbildung 12.156 Im Active Directory gibt es einige Attribute für das Speichern der BitLocker-Informationen.

Sofern Sie eine Windows Server 2003-Domäne betreiben, müssen Sie eine Schema-Erweiterung durchführen:

- Suchen Sie im Microsoft Download Center nach dem Stichwort *BitLockerTPMSchemaExtension.ldf*. Es wird eine EXE-Datei namens *Configuring AD to Back up BitLocker and TPM Recovery Information.exe* gefunden, die unter anderem die LDF-Datei enthält.
- Diese Schema-Erweiterung führen Sie mit folgendem Befehl aus:

```
ldifde -i -v -f BitLockerTPMSchemaExtension.ldf -c "DC=X"
"DC=ubinf,DC=intra"
```

Nach Ausführung der Schema-Erweiterung können Sie direkt loslegen.

Manuelle Schema-Erweiterung

Hierzu noch eine Anmerkung: Ich habe den Fall erlebt, dass es in einer *Windows Server 2008*-Domäne, die durch Migration einer 2003-Umgebung entstanden ist, beim Speichern von Schlüsseln im Active Directory zu unerklärlichen Fehlermeldungen kam. Der Grund war, dass bei der Migration offensichtlich die Schema-Erweiterung nicht korrekt erledigt wurde. Eine manuelle Durchführung der Schema-Erweiterung, wie ich sie oben gezeigt habe, löste das Problem.

Gruppenrichtlinien konfigurieren

Wenn Sie möchten, dass BitLocker den Wiederherstellungsschlüssel und andere Informationen im Active Directory speichert, müssen Sie dies über Gruppenricht-

linien konfigurieren. Wie Sie auf Abbildung 12.157 erkennen können, gibt es sowohl einige übergreifende Konfigurationsoptionen als auch spezielle für Betriebssystemlaufwerke, fest eingebaute Laufwerke und Wechseldatenträger. Auf der Abbildung ist übrigens die Einstellung gezeigt, die dafür sorgt, dass der Client beim Aktivieren von BitLocker den Wiederherstellungsschlüssel im Active Directory speichert.

Darüber hinaus existieren noch diverse weitere Einstellungen, die Sie einmal selbst erkunden sollten – alle Optionen sind ausführlich beschrieben.

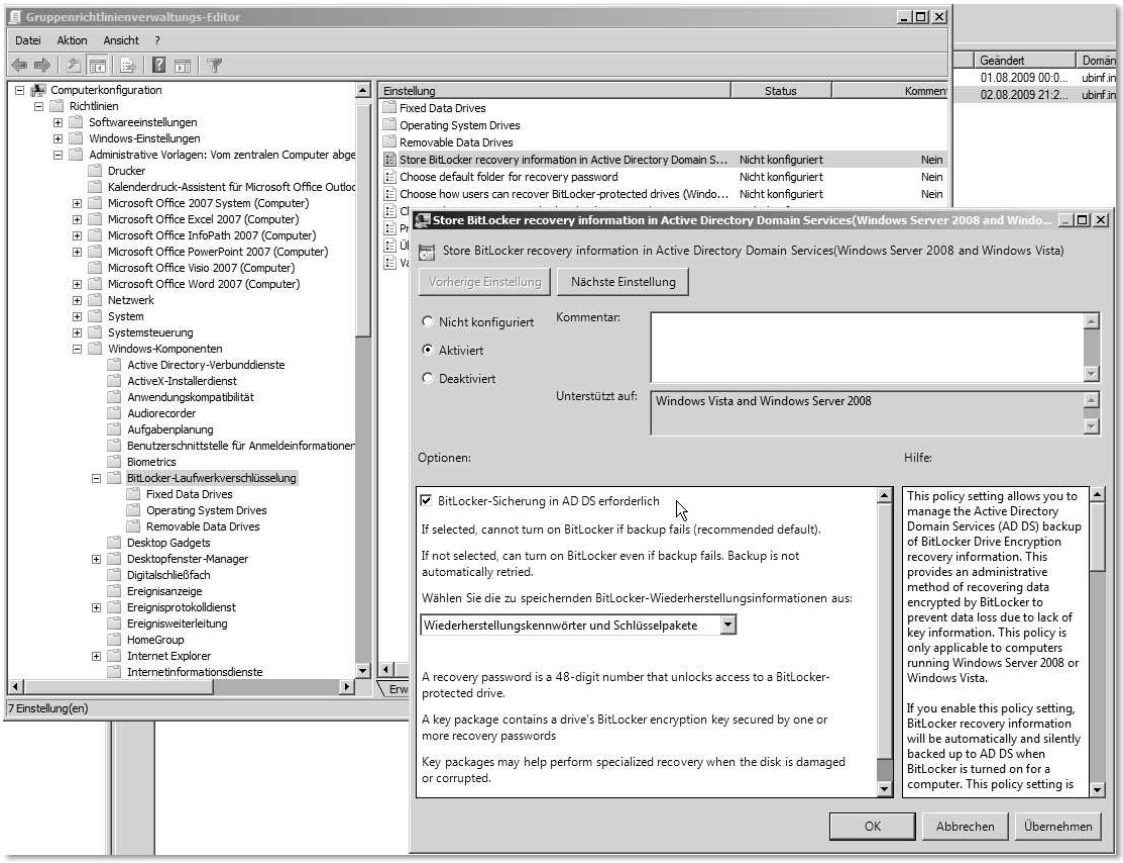


Abbildung 12.157 Per Gruppenrichtlinie konfigurieren Sie, dass Wiederherstellungskennwörter und Schlüsselpakete im AD gesichert werden.

Ein weitere wichtige Einstellung findet sich nicht unter ADMINISTRATIVE VORLAGEN • WINDOWS-KOMPONENTEN • BITLOCKER-LAUFWERKSVERSCHLÜSSELUNG, sondern unter ADMINISTRATIVE VORLAGEN • SYSTEM • TRUSTED PLATFORM MODULE-DIENSTE. Auf Abbildung 12.158 sehen Sie den Konfigurationsabschnitt, in dem festgelegt wird, dass die Besitzerinformationen des *Trusted Platform Module* im Active Directory gespeichert werden sollen.

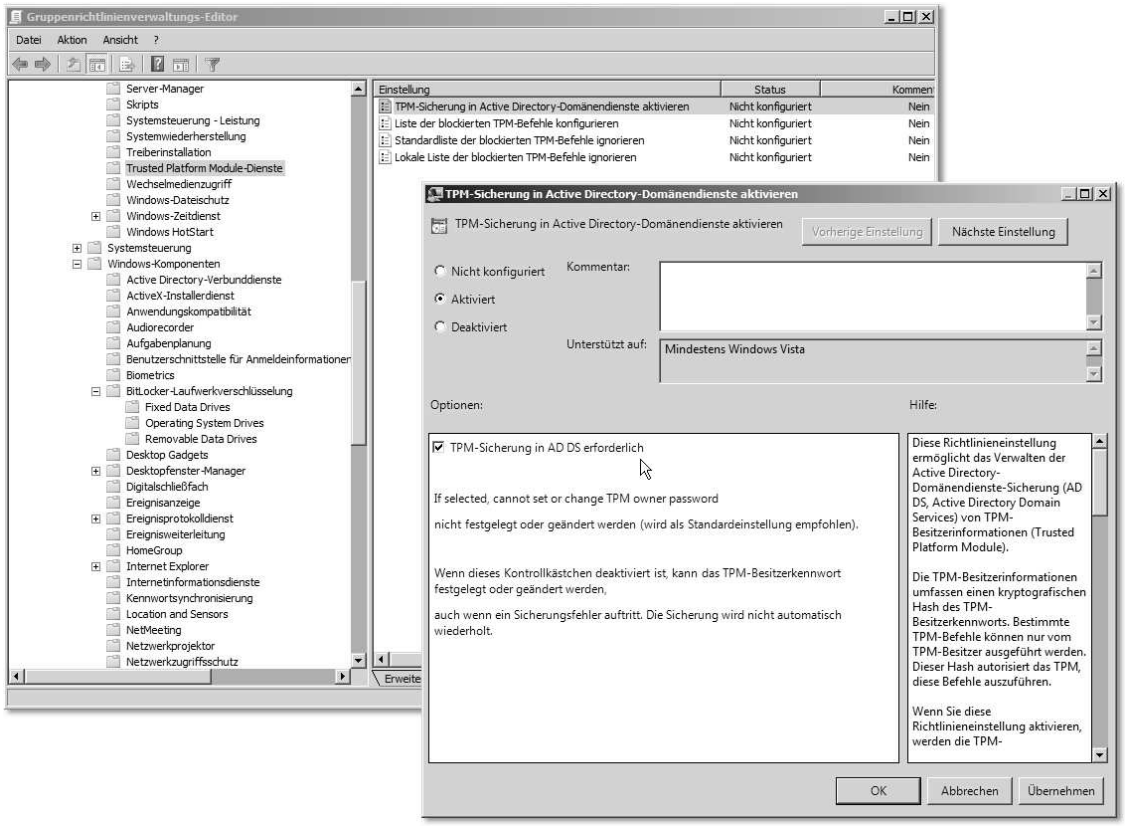


Abbildung 12.158 Die Besitzer-Informationen des TPM-Chips werden ebenfalls im AD gespeichert, wenn Sie die entsprechende Gruppenrichtlinie aktivieren.

Ein weiterer interessanter Aspekt, der über Active Directory-Gruppenrichtlinien konfiguriert werden kann, sind die *Datenwiederherstellungs-Agenten* (*Data Recovery Agents*, DRA). Datenwiederherstellungs-Agenten sind Zertifikate, die sozusagen »mit eingeschlüsselt« werden. Der Datenwiederherstellungs-Agent ist neben dem bei der Aktivierung von BitLocker generierten Wiederherstellungsschlüssel eine Möglichkeit, ein BitLocker-Laufwerk zu entschlüsseln.

Auf Abbildung 12.159 und Abbildung 12.160 ist zu sehen, wie ein Datenwiederherstellungs-Agent hinzugefügt wird. Wie ich bereits erwähnt habe, ist der Datenwiederherstellungs-Agent ein Zertifikat. Es muss entweder im lokalen Zertifikatsspeicher oder als **.cer*-Datei vorhanden sein.

Es ist möglich, mehrere Datenwiederherstellungs-Agenten für BitLocker zu definieren.

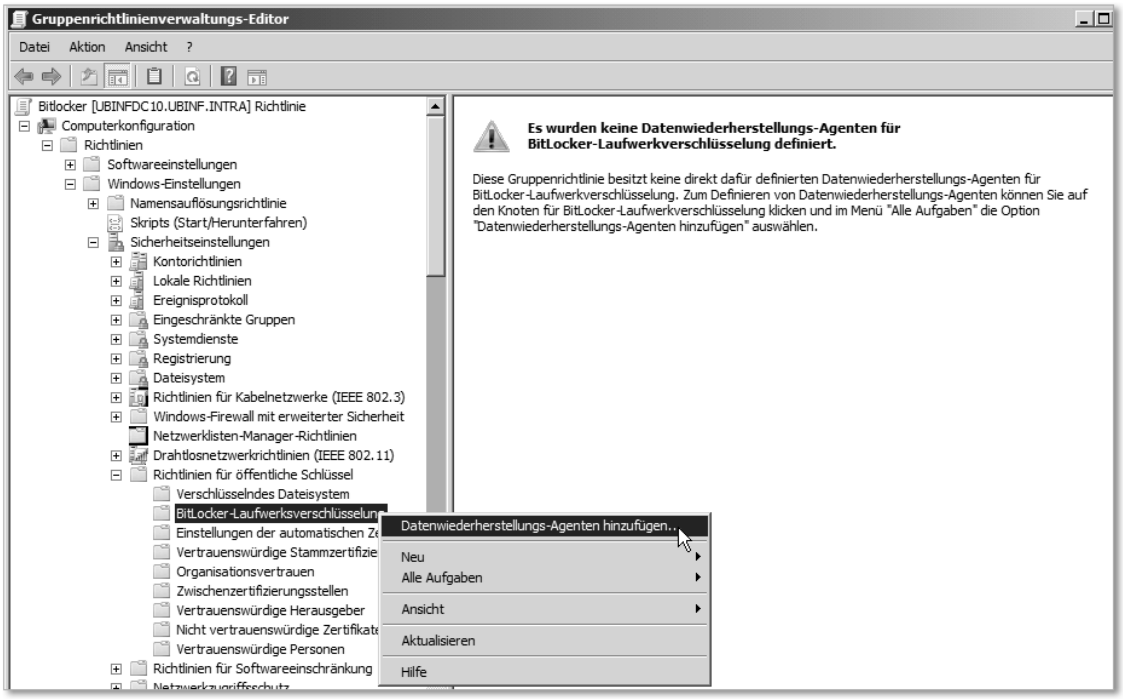


Abbildung 12.159 Wenn Sie einen Wiederherstellungs-Agenten hinzufügen möchten, finden Sie einen entsprechenden Punkt in den Gruppenrichtlinien.

Abbildung 12.160 Der Wiederherstellungs-Agent ist ein Zertifikat, das im lokalen Zertifikatsspeicher des Servers vorhanden ist, auf dem die Gruppenrichtlinie konfiguriert wird.

Das Zertifikat ist schutzbedürftig

Bedenken Sie, dass das Zertifikat absolut schutzbedürftig ist. Wer dieses Zertifikat hat, kann alle Laufwerke entschlüsseln, in denen dieses als Wiederherstellungs-Agent integriert ist.

Weiterhin müssen Sie dafür sorgen, dass Sie dieses Zertifikat nicht verlieren. Wenn dies doch passiert und das private Teil des Zertifikats nicht mehr verfügbar ist, haben Sie umsonst einen Datenwiederherstellungs-Agenten definiert.

Damit ein Datenwiederherstellungs-Agent in die BitLocker-Verschlüsselung eines Laufwerks integriert wird, muss die Gruppenrichtlinie beim Aktivieren von BitLocker vorhanden sein. Oder anders gesagt: Der Datenwiederherstellungs-Agent wird nicht nachträglich integriert.

TPM initialisieren

Das *Trusted Platform Module* (TPM) muss im BIOS des PCs aktiviert werden – das ist die erste Voraussetzung. Der nächste Schritt ist dann die Initialisierung des Moduls, was aus Windows 7 heraus erledigt wird.

Wenn Sie wie zuvor (Abschnitt 12.7.3) einfach mit der BitLocker-Aktivierung beginnen und das *Trusted Platform Module* noch nicht initialisiert ist, wird dies quasi nebenbei erledigt.

Sie können die TPM-Initialisierung aber auch gezielt mit dem TPM-Management-Werkzeug vornehmen. Sie starten es über den Aufruf von *tpm.msc*.

Wenn der PC »frisch« ist, also das TPM noch nicht initialisiert wurde, ergibt sich die auf Abbildung 12.161 gezeigte Situation: Das TPM ist aktiviert, aber der Besitz wurde noch nicht übernommen.

Falls das TPM als deaktiviert aufgeführt ist, müssen Sie es im BIOS des PCs aktivieren.

Bei der Initialisierung werden Sie, wie gewohnt, von einem Assistenten geführt. Der erste Schritt ist die Erstellung eines TPM-Besitzerkennworts. Es wird empfohlen, dieses automatisch erstellen zu lassen (Abbildung 12.162). Der zweite Schritt ist das Speichern des erzeugten (oder eingegebenen) Kennworts. Sie können es speichern oder ausdrucken (Abbildung 12.163).

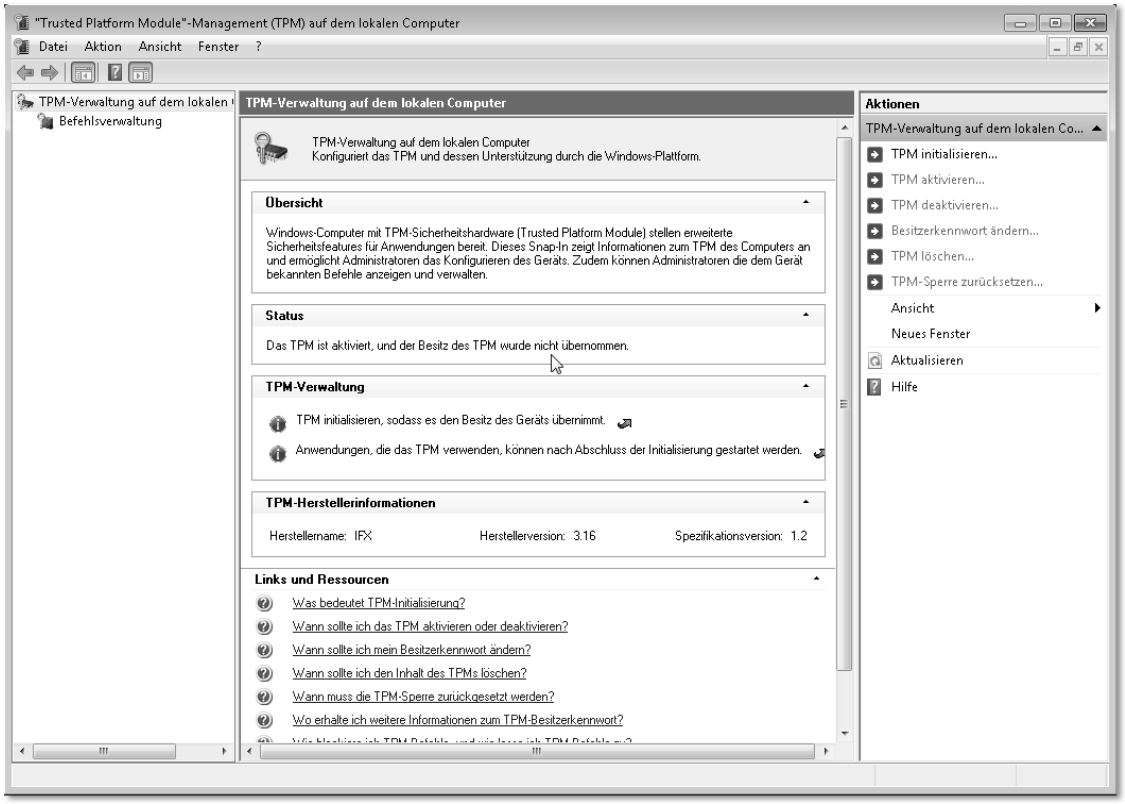


Abbildung 12.161 Direkt nach dem Start des PCs ist das »Trusted Platform Module« noch nicht initialisiert.

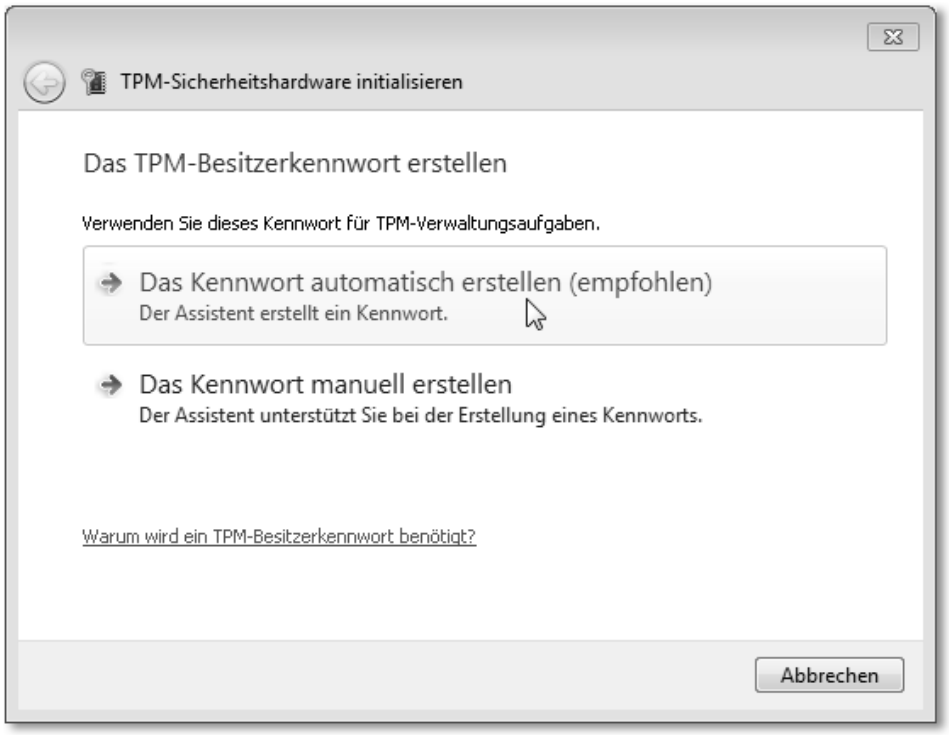


Abbildung 12.162 Das TPM-Besitzerkennwort sollte automatisch erstellt werden.

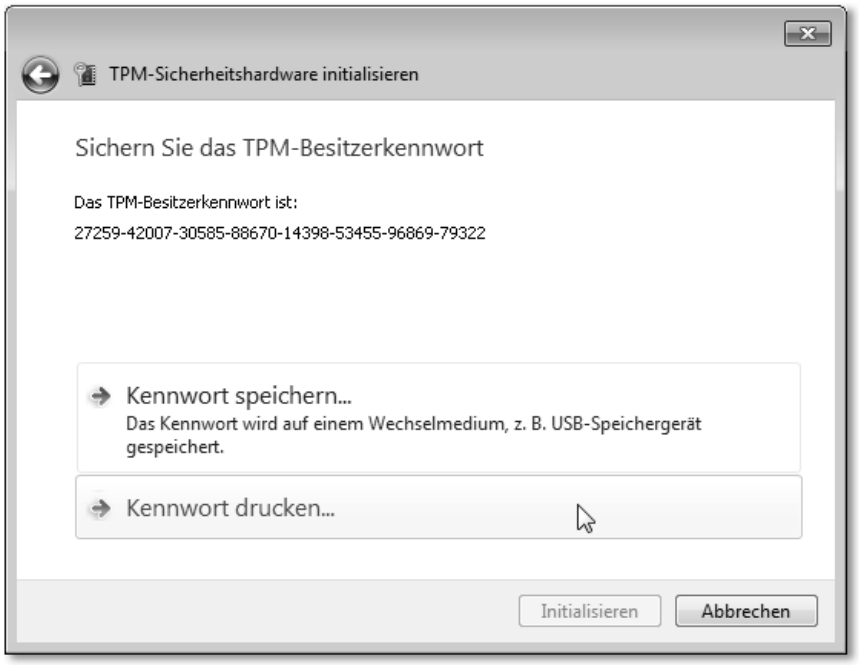


Abbildung 12.163 Das TPM-Besitzerkennwort kann entweder als Datei gespeichert oder ausgedruckt werden.

Nach ein paar Augenblicken ist die Initialisierung abgeschlossen, und nun können Anwendungen, die TPM benutzen, aktiviert werden – insbesondere also BitLocker (Abbildung 12.164).

Abbildung 12.164 Erst wenn die Initialisierung des TPM abgeschlossen ist, kann BitLocker verwendet werden.

Wenn Sie nun *tpm.msc* aufrufen, wird angezeigt, dass der Besitz des TPM übernommen wurde (Abbildung 12.165). Die zur Verfügung stehenden Menüpunkte (nicht auf der Abbildung zu sehen) haben sich übrigens auch geändert.

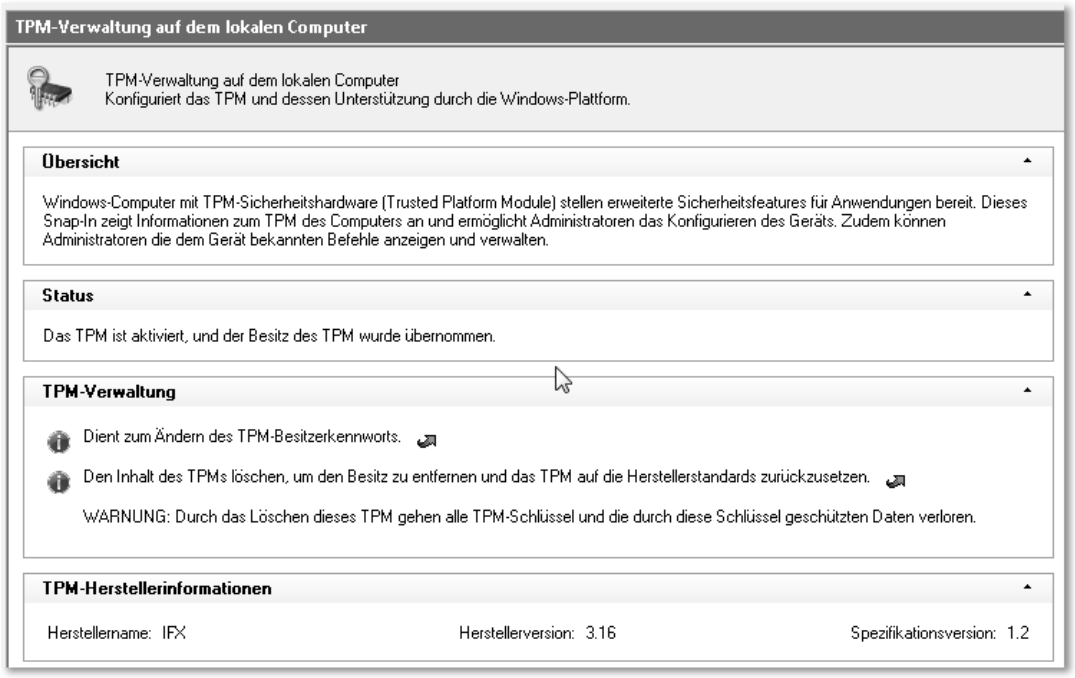


Abbildung 12.165 Nach der Initialisierung sehen Sie diese Anzeige – alles ist startklar.

Abbildung 12.166 zeigt, was in der Kennwortdatei gespeichert wird. Insbesondere sind dies der Besitzer des TPM und das Kennwort.

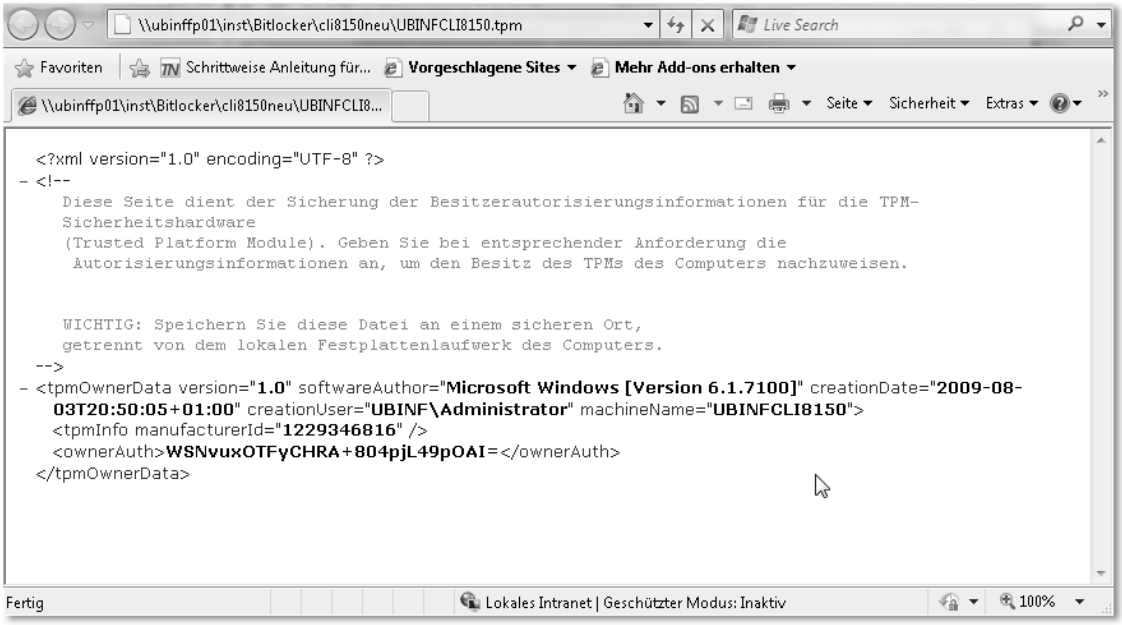


Abbildung 12.166 Dies sind die Informationen, die bei der Initialisierung des TPM gespeichert werden.

BitLocker aktivieren

Ist der TPM-Chip aktiviert, können Sie BitLocker aktivieren. Diesen Vorgang starten Sie wie gehabt aus der BitLocker-Verwaltung. Der Assistent wird Sie zunächst fragen, ob beim Start eine PIN, ein Systemstartschlüssel oder kein zusätzlicher Schlüssel benötigt wird. Diese Einstellung kann natürlich auch über eine Gruppenrichtlinie festgelegt werden (Abbildung 12.167).

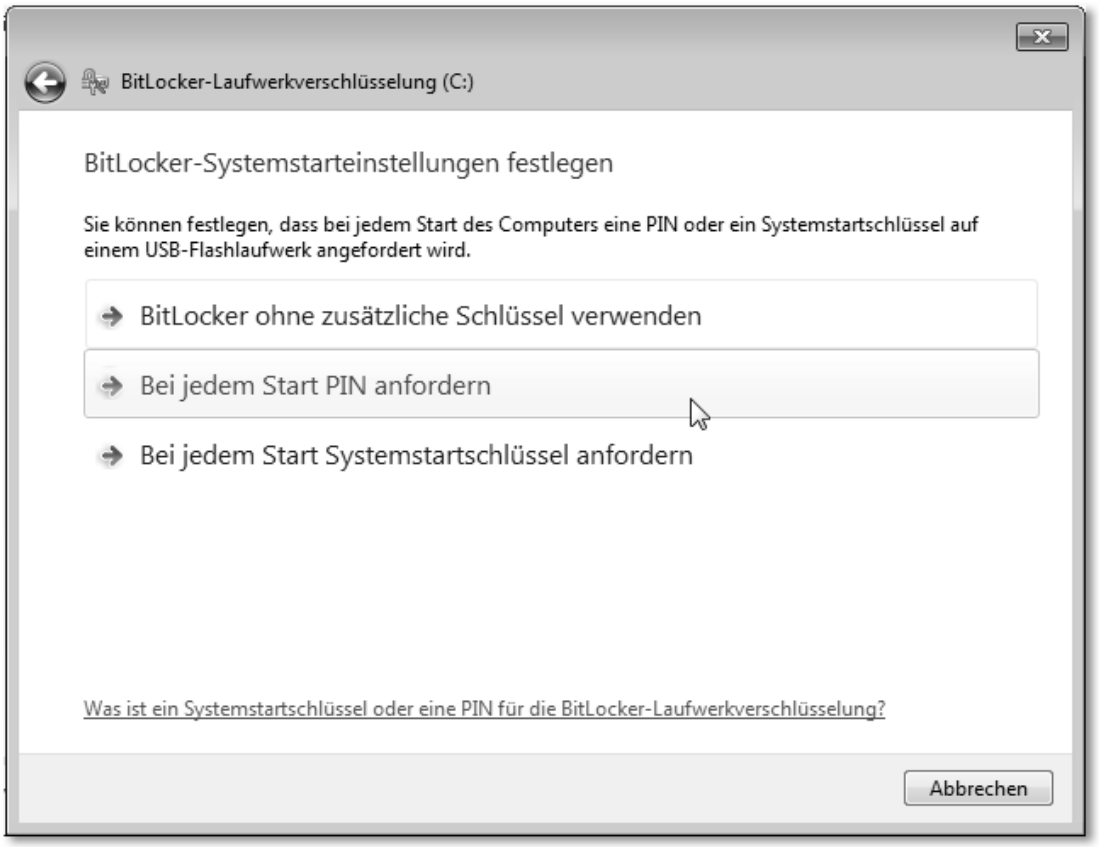


Abbildung 12.167 Entscheiden Sie, ob ein zusätzlicher Schlüssel beim Start angefordert werden soll (dies können Sie auch über eine Gruppenrichtlinie festlegen).

Wenn Sie sich für die PIN entschieden haben, wird diese im nächsten Schritt abgefragt (Abbildung 12.168). Sie werden diese fortan bei jedem Systemstart angeben müssen, sonst erhalten Sie keinen Zugriff. Falls Sie nach einem vier Wochen langen Malediven-Urlaub die PIN vergessen haben, hilft der Wiederherstellungsschlüssel.

Per Gruppenrichtlinie wurde konfiguriert, dass der Wiederherstellungsschlüssel im Active Directory gespeichert werden soll. Mit dem ADSI-Editor können Sie kontrollieren, ob das tatsächlich geschehen ist. Abbildung 12.169 zeigt das Ergebnis: Ja, es hat funktioniert.

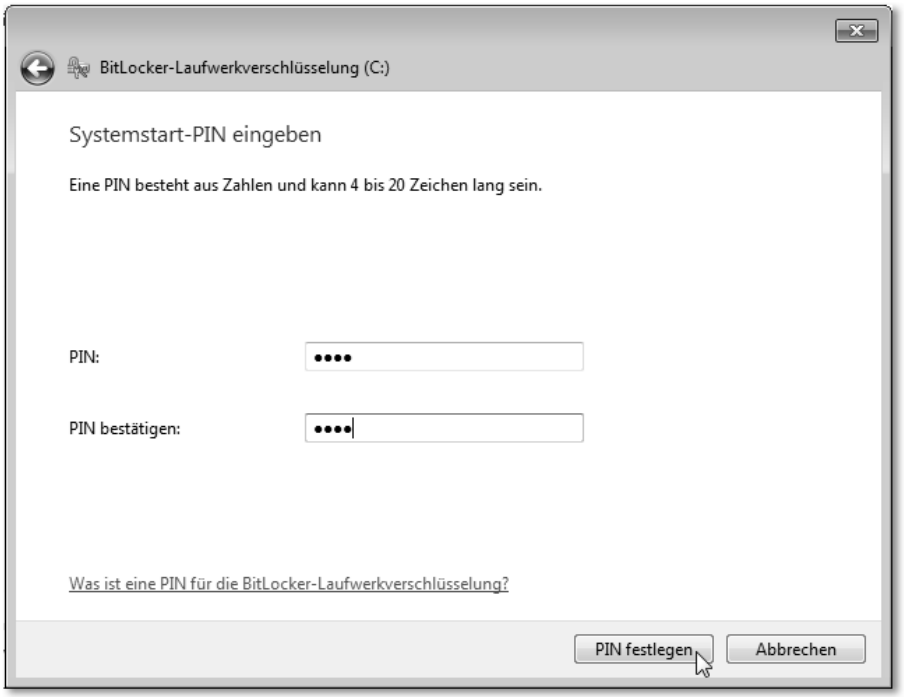


Abbildung 12.168 Falls Sie sich für die PIN entschieden haben, wird diese abgefragt.

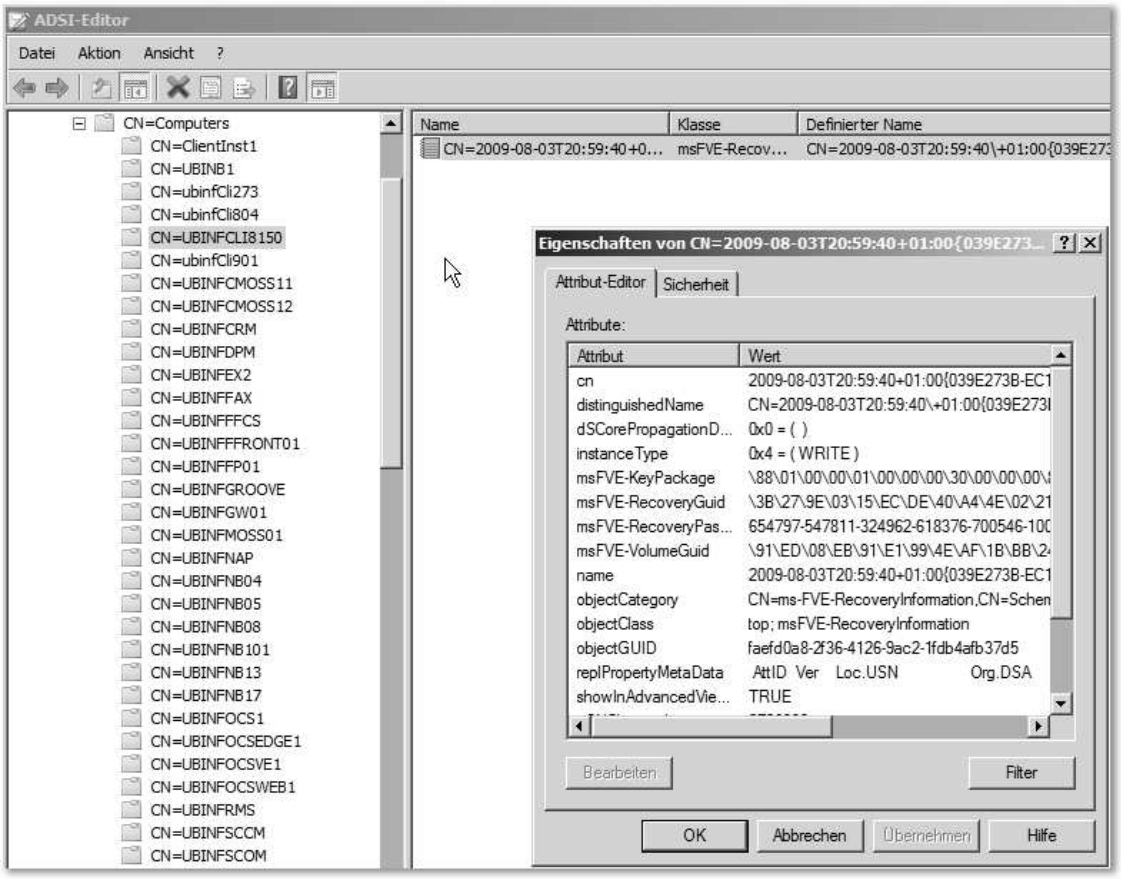


Abbildung 12.169 Im Active Directory-Objekt des Computers werden die Informationen hinterlegt – sofern dies per Gruppenrichtlinie so konfiguriert worden ist.

Im Active Directory lässt sich übrigens per Gruppenrichtlinie konfigurieren, dass BitLocker für ein Laufwerk nur aktiviert werden kann, wenn der Wiederherstellungsschlüssel im Active Directory gespeichert worden ist. Diese Einstellung finde ich durchaus sinnvoll, denn sie verhindert, dass BitLocker in einem Offline-Szenario aktiviert wird, und das Wiederherstellungskennwort bleibt unbekannt. Insbesondere bei *BitLocker To Go*, das von den Benutzern selbst für Wechselmedien aktiviert werden kann, könnte das durchaus vorkommen.

Abbildung 12.170 zeigt schließlich noch den Inhalt der gespeicherten Datei mit dem Wiederherstellungsschlüssel, der dort nebst ID aufgeführt ist. Die Druckausgabe sieht übrigens exakt genauso aus.

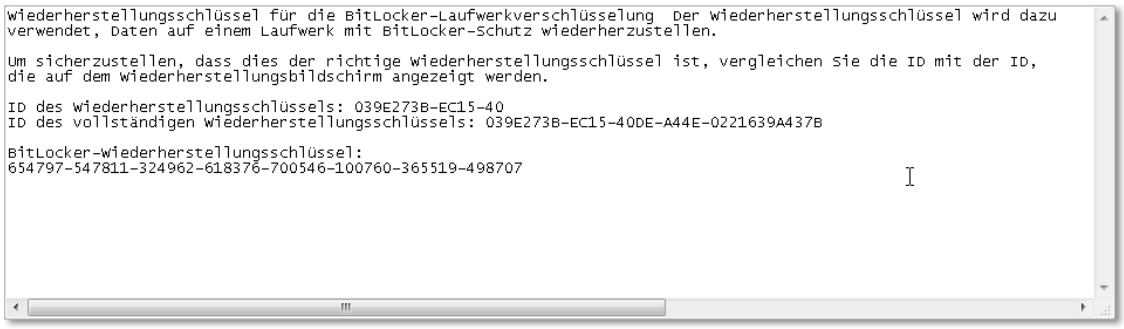


Abbildung 12.170 Die BitLocker-Wiederherstellungsschlüssel und die zugehörige ID werden auch als Datei gespeichert oder können gedruckt werden.

12.7.5 Wiederherstellen

Im Normalfall arbeitet BitLocker vollkommen »unauffällig« und fragt die Benutzer lediglich nach einer PIN oder einem Kennwort. Ein wenig spannender wird es, wenn tatsächlich ein Wiederherstellungsvorgang durchgeführt werden muss, wofür es beispielsweise folgende Fälle gibt:

- Eine verschlüsselte Festplatte muss an einen anderen Computer angeschlossen werden, weil das ursprüngliche System defekt geworden ist.
- Das TPM-Modul könnte gelöscht oder neu initialisiert worden sein. Dies könnte etwa beim versehentlichen »Herumspielen« (Testen) passieren oder wenn das Mainboard (und damit auch der TPM-Chip) wegen eines Defekts getauscht worden ist.
- Bei Verwendung von *BitLocker To Go* könnte das Kennwort vergessen worden sein. Ähnliches könnte auch passieren, wenn Sie die PIN des Startvolumes vergessen haben.

Im Grunde genommen besteht der Wiederherstellungsvorgang darin, den Wiederherstellungsschlüssel einzugeben. Dies kann entweder durch manuelle Ein-

gabe geschehen (z. B. wenn der Schlüssel ausgedruckt worden ist) oder durch Einspielen der gespeicherten Schlüsseldatei.

BitLocker-Kennwortwiederherstellungs-Viewer

Wie Sie zuvor gesehen haben, kann das Wiederherstellungskennwort im Active Directory gespeichert werden. Um es komfortabel auslesen zu können, gibt es den *BitLocker-Kennwortwiederherstellungs-Viewer*. Dieses Utility ist eine Erweiterung des *Active Directory-Benutzer und -Computer*-Konfigurationswerkzeugs. Es muss allerdings aktiviert werden:

- In Windows 7 mit installierten Remoteserver-Verwaltungstools (RSAT, *Remote Server Administration Tools*) muss es in dem Dialog zum Aktivieren von Windows-Features aktiviert werden (Abbildung 12.171).
- In Windows Server 2008 wird es im *Assistenten zum Hinzufügen von Features* des Server-Managers aktiviert (Abbildung 12.172)

Abbildung 12.171 Unter Windows 7 wird der »BitLocker-Kennwortwiederherstellungs-Viewer« im Rahmen der »Remoteserver-Verwaltungstools« installiert. Er muss anschließend aktiviert werden.

Wenn Sie auf einem System mit aktiviertem BitLocker-Kennwortwiederherstellungs-Viewer im *Active Directory-Benutzer und -Computer*-Werkzeug die Eigenschaften eines Computers aufrufen, wird eine Registerkarte namens BitLocker-Wiederherstellung vorhanden sein. Dort sind alle BitLocker-Wiederherstellungsschlüssel für die Datenträger aufgelistet, deren Verschlüsselung mit diesem Computer aktiviert wurden? (Abbildung 12.173).

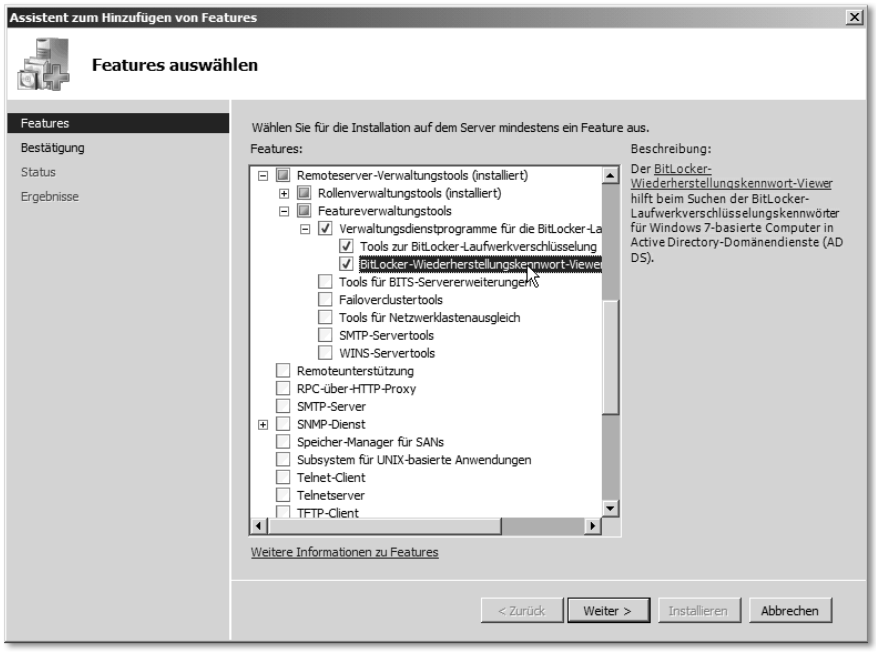


Abbildung 12.172 Auf einem Windows-Server-2008-System ist der »BitLocker-Wiederherstellungskennwort-Viewer« ein Feature, das Sie noch aktivieren müssen.

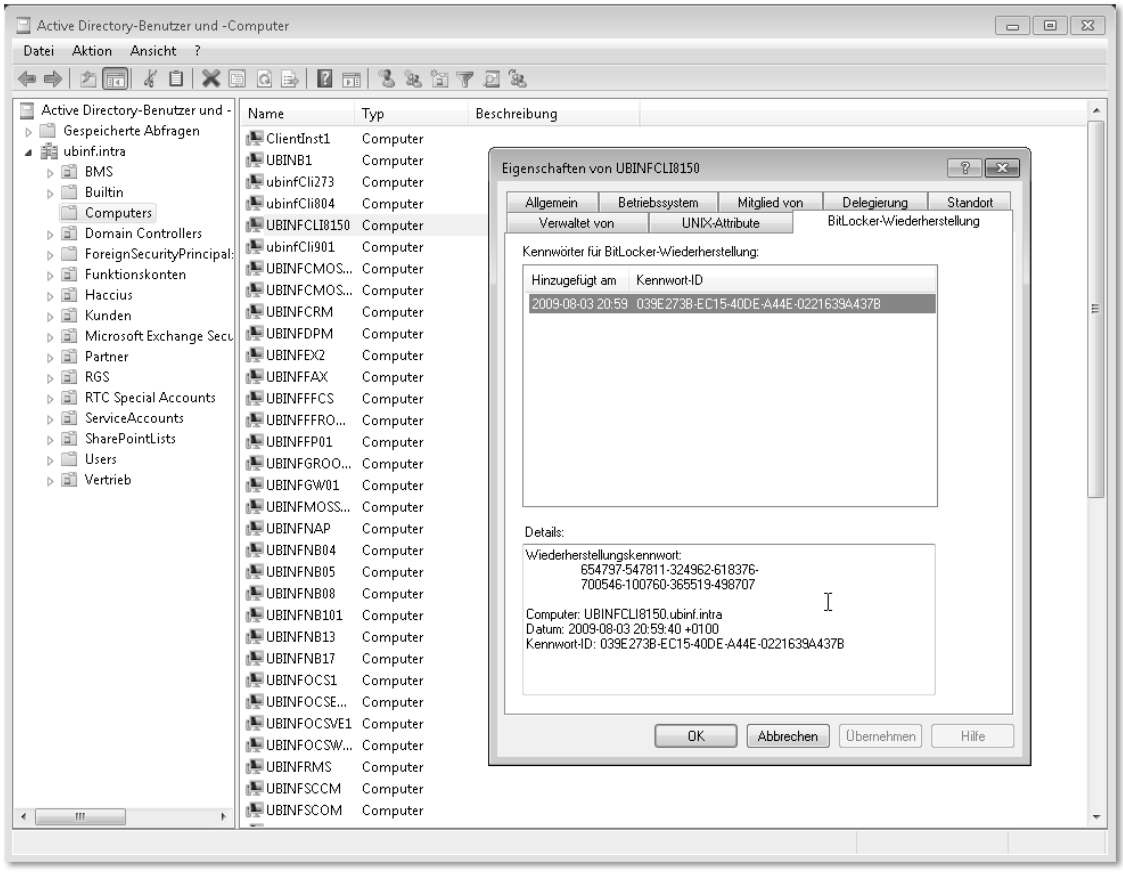


Abbildung 12.173 In den Eigenschaften des Computers werden die zugeordneten Wiederherstellungsschlüssel angezeigt.

Gerade bei Wechselmedien ist es möglich, dass Sie nicht mehr feststellen können, mit welchem Computer die Aktivierung der BitLocker-Verschlüsselung vorgenommen worden ist. Für diese Zwecke gibt es im Kontextmenü des Domänenknotens des *Active Directory-Benutzer und -Computer*-Werkzeugs den Menüpunkt KENNWORT FÜR BITLOCKER-WIEDERHERSTELLUNG SUCHEN. Den Dialog dazu sehen Sie auf Abbildung 12.174. Geben Sie die bei der Wiederherstellung angegebene Kennwort-ID ein, und klicken Sie auf die Schaltfläche SUCHEN. Der Wiederherstellungsschlüssel wird umgehend angezeigt.

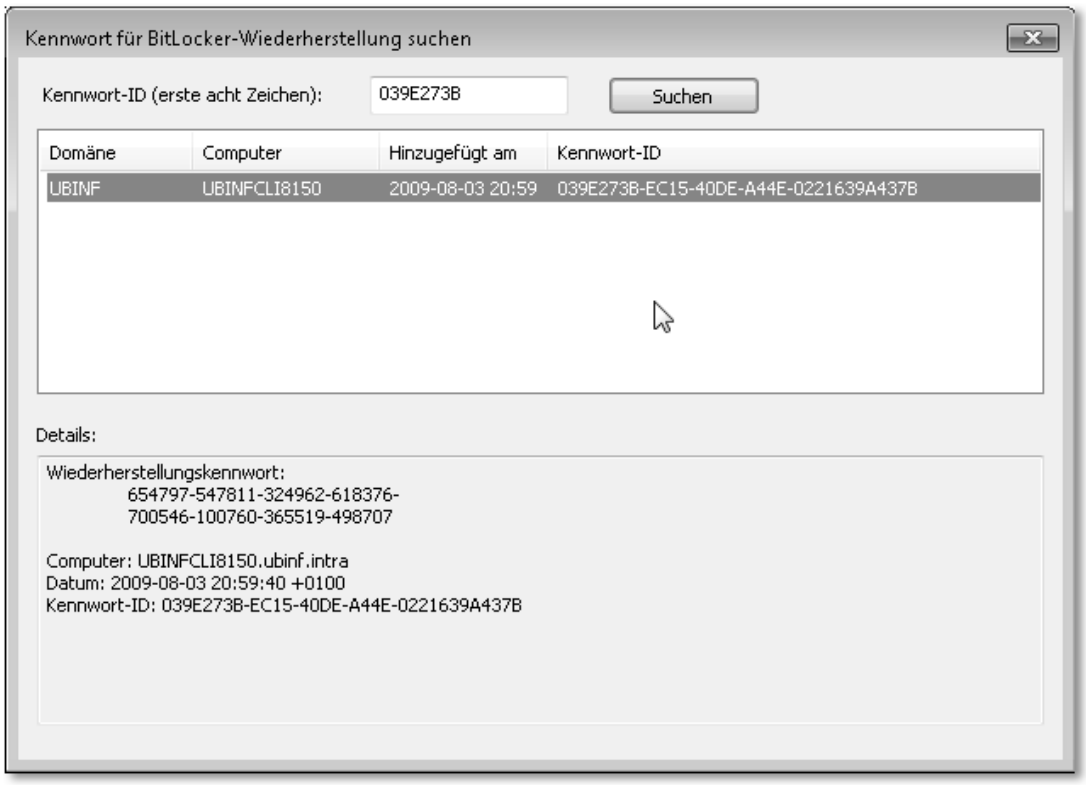


Abbildung 12.174 Die Suchfunktion für das Finden eines BitLocker-Wiederherstellungsschlüssels

Wahrscheinlich fragen Sie sich, wie die BitLocker-Wiederherstellungsschlüssel geschützt sind und wer darauf zugreifen darf. Ein Blick in das Active Directory mittels des ADSI-Editors beantwortet die Frage (Abbildung 12.175):

- Administratoren können lesend zugreifen.
- Normale Benutzer und auch das Computerkonto selbst haben keinen Zugriff auf diese Daten.

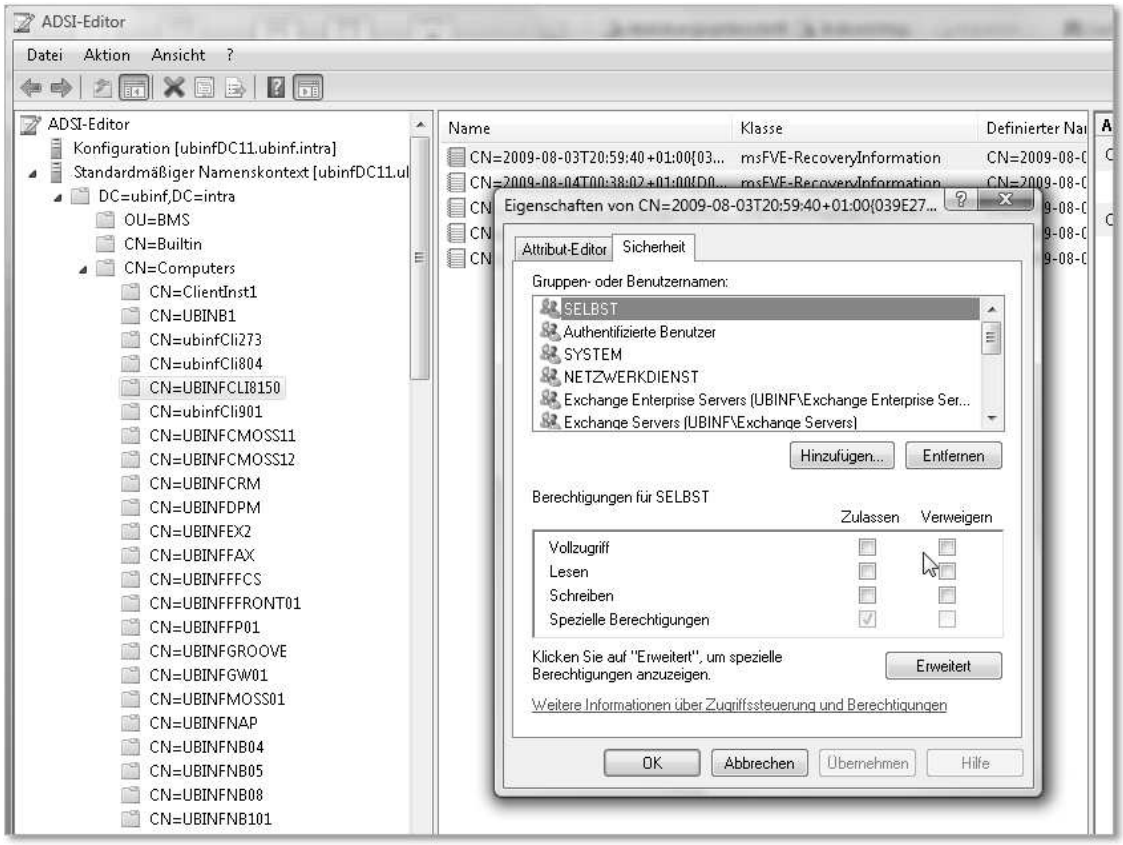


Abbildung 12.175 Auf das im AD gespeicherte Wiederherstellungskennwort können nur Administratoren zugreifen – auch das Computerkonto selbst kann nicht lesend darauf zugreifen.

BitLocker To Go-Kennwort vergessen

Die Entsperrung von mit *BitLocker To Go* geschützten Laufwerken ist ebenfalls unproblematisch. Wenn Windows 7 das Medium erkannt hat, wird das Passwort erfragt. Wenn dieses unbekannt ist – entweder weil der Benutzer es vergessen hat oder weil das Laufwerk ohne Mithilfe des Benutzers entsperrt werden muss (beispielsweise weil dieser im Urlaub, längerfristig krank oder nicht mehr in der Firma ist) –, klickt man auf KENNWORT VERGESSEN (Abbildung 12.176). Daraufhin gelangt man zu den Dialogen aus Abbildung 12.177 und führt die Entsperrung mittels des Wiederherstellungsschlüssels aus.

Hier schlägt nun die Stunde der Active Directory-Integration. Die Verschlüsselung von Wechselmedien kann von einem normalen Benutzer (Nicht-Admin) initiiert werden, was ja durchaus gewollt ist. Das Problem wird allerdings sein, dass es kaum durchsetzbar sein wird, dass die Wiederherstellungsschlüssel an einem zentralen Speicherort aufbewahrt werden – im Zweifelsfall auch auf Papier.

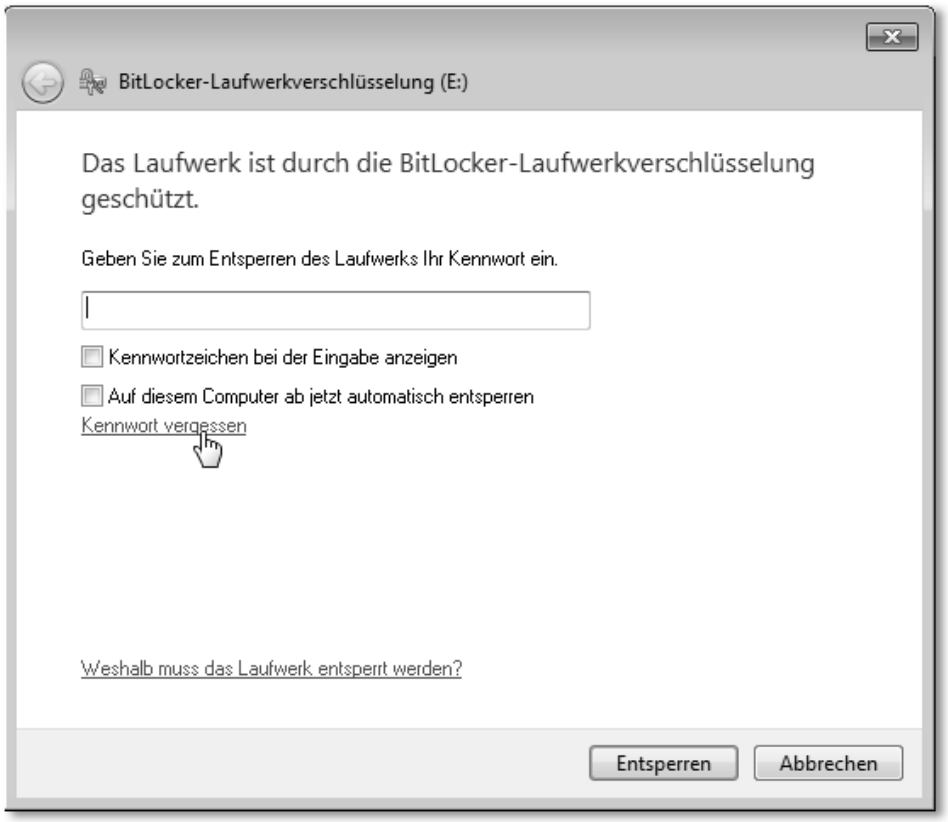


Abbildung 12.176 Wenn das Kennwort eines mit BitLocker To Go verschlüsselten Datenträgers vergessen worden ist, kann der Benutzer den Menüpunkt »Kennwort vergessen« wählen.

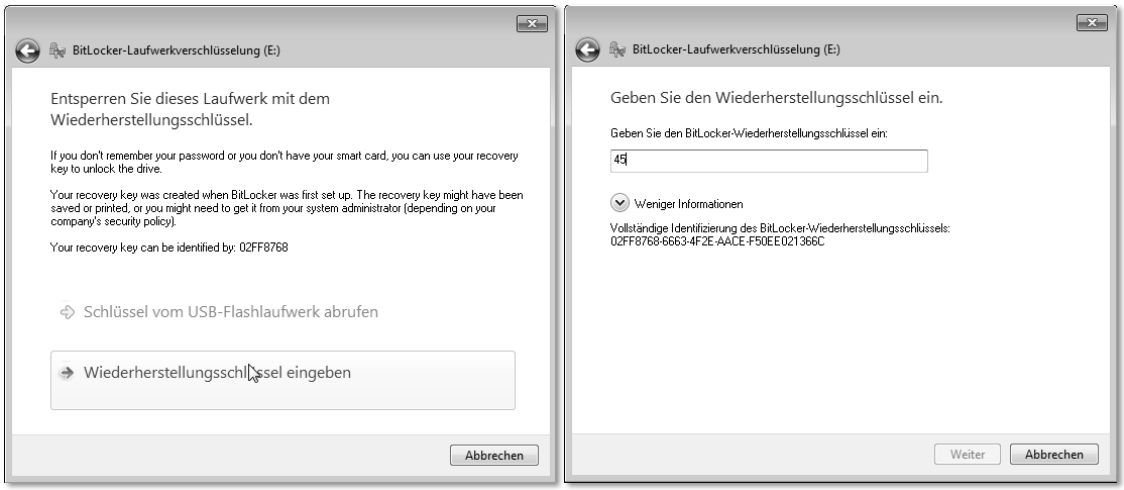


Abbildung 12.177 Wenn das Kennwort vergessen wurde, kann die Entsperrung des Laufwerks über den Wiederherstellungsschlüssel erfolgen.

Wenn Sie nun per Gruppenrichtlinie festgelegt haben, dass Wiederherstellungsschlüssel im Active Directory gespeichert werden, wird der *BitLocker To Go*-Wiederherstellungsschlüssel bei dem Computerobjekt, auf dem die BitLocker-Akti-

vierung des Mediums durchgeführt wurde, gespeichert. Wie Sie auf Abbildung 12.178 sehen, können beliebig viele Wiederherstellungsschlüssel auf einem Computer gespeichert werden.

Auf welchem Computer der Wiederherstellungsschlüssel gespeichert wurde, ist letztendlich egal – die Suchfunktion hilft (Abbildung 12.174).

BitLocker-Aktivierung

Sie können per Gruppenrichtlinie definieren, dass die BitLocker-Aktivierung eines Datenträgers nur möglich ist, wenn die Wiederherstellungsinformationen direkt ins Active Directory geschrieben werden können. Eine BitLocker-Aktivierung ist dann zwar offline nicht möglich, was aber ein vergleichsweise geringes Problem ist im Vergleich zu einer nicht möglichen Entsperrung aufgrund eines nicht vorhandenen Wiederherstellungsschlüssels.

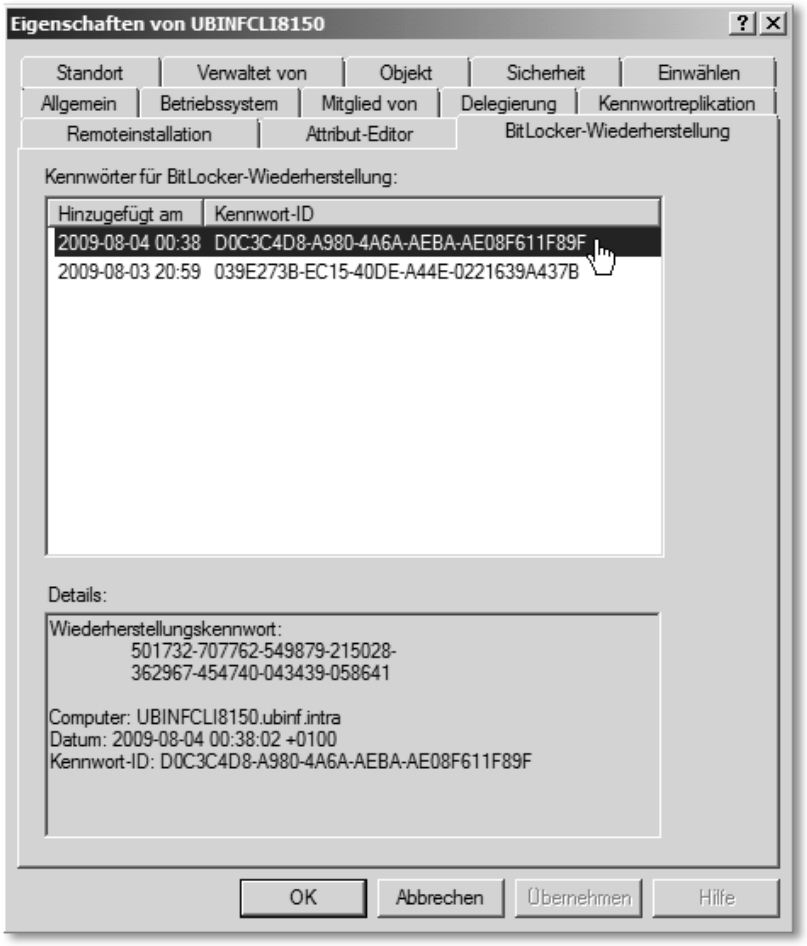


Abbildung 12.178 Wenn auf einem Computer für einen Datenträger die »BitLocker To Go«-Verschlüsselung aktiviert wurde, ist der Wiederherstellungsschlüssel in dessen AD-Objekt gespeichert.

Verwendung eines Datenwiederherstellungs-Agenten (Data Recovery Agent)

Weiter vorn habe ich erwähnt, dass ein Datenwiederherstellungs-Agent »eingeschlüsselt« werden kann. Damit ist eine Entsperrung des Datenträgers auch ohne Kenntnis des Wiederherstellungsschlüssels möglich.

Die Entsperrung mittels des Datenwiederherstellungs-Agenten ist allerdings nur mit der Kommandozeile möglich, was ja aber grundsätzlich auch kein Problem ist.

Die beiden Voraussetzungen dafür, dass die Nutzung des Datenwiederherstellungs-Agenten möglich ist, sind folgende:

- Die Verwendung des Datenwiederherstellungs-Agenten muss zum Zeitpunkt der BitLocker-Aktivierung des Datenträgers per Gruppenrichtlinie aktiv gewesen sein – nachträglich geht das nicht.
- Das Zertifikat des Datenwiederherstellungs-Agenten (letztendlich ist das ja »nur« ein Zertifikat) muss zusammen mit dem privaten Schlüssel im Zertifikatsspeicher des Computers vorhanden sein, der die Entsperrung durchführen soll.

Im Grunde genommen müssen Sie nun lediglich zwei Befehle kennen:

- `manage-bde -protectors -get <drive letter>` dient dazu, die aktiven »Beschützer« (*Protectors*) aufzulisten. Hier wird auch der Datenwiederherstellungs-Agent (*Data Recovery Agent*) mit einem *Certificate Thumbprint* (Zertifikats-Fingerabdruck) aufgeführt sein.
- `manage-bde -unlock E: -Certificate -ct <Zertifikats-Fingerabdruck>` initiiert die Entsperrung. Den Fingerabdruck des Zertifikats können Sie aus der Ausgabe des zuvor beschriebenen Befehls kopieren. Die Entsperrung funktioniert natürlich nur, wenn das Zertifikat mit einem privaten Schlüssel im lokalen Zertifikatsspeicher vorhanden ist.

12.8 Virenschutz

In einem Kapitel zum Thema Sicherheit darf das Thema Virenschutz natürlich nicht vergessen werden, das ich in diesem Buch aber nicht weiter behandeln werde – die Vielfalt der auf dem Markt verfügbaren Virenschutzlösungen ist einfach zu groß, und folglich hätte jeder Leser eine andere Präferenz.

Achten Sie darauf, dass die von Ihnen eingesetzte Lösung wirklich für Windows 7 zertifiziert ist, bevor Sie sie auf die Clients loslassen! Ist ein Virenscanner nicht voll mit Windows 7 kompatibel, gibt es unter Umständen massive Probleme, bis hin zum Bluescreen.

In Milet aber hatte Tissaphernes, als er Kunde erhielt, dass eine Partei dasselbe beabsichtige, nämlich zu Kyros abzufallen, einige derselben hinrichten lassen, andere vertrieben.

13 Mobile Clients

Ein nicht geringer Teil der Windows 7-Installationen wird auf Notebooks laufen. Wenn ein Notebook für einen Anwender nicht nur deshalb beschafft wird, weil es auf dem Schreibtisch besser aussieht, ansonsten aber nie mobil eingesetzt wird, gibt es natürlich keine besonderen Anforderungen an das Thema »Mobilität«. Ist das Notebook aber tatsächlich ein mobiler Arbeitsplatz, mit dessen Hilfe der Benutzer an jedem Punkt der Welt arbeiten können soll, muss das Betriebssystem schon ein wenig mehr drauf haben, als nur damit umgehen zu können, dass der Computer zeitweise vom Akku und nicht aus der Steckdose versorgt wird. Man kann wohl getrost davon ausgehen, dass ein mobiler Benutzer im Windows 7-Zeitalter auf seinem Notebook deutlich mehr tun möchte, als offline einen Brief zu schreiben und die Datei dann beim nächsten Aufenthalt in der Firma auf den zentralen Fileserver zu kopieren. Im Grunde genommen muss für einen mobilen Mitarbeiter mit Notebook genau dasselbe Leistungsspektrum zur Verfügung stehen, das er auch zur Verfügung hätte, wenn er sich im Unternehmens-LAN aufhält.

Dies ist übrigens keine im stillen Kämmerlein eines IT-Beraters entstandene Vision, sondern schon heute Business-Anforderung vieler Unternehmen: Die im Außendienst tätigen Mitarbeiter kommen hin und wieder zu Team-Meetings und -Briefings ins Unternehmen.

Um die für diese Szenarien notwendige Konnektivität bereitzustellen, genügt es allerdings nicht, nur das Clientbetriebssystem zu betrachten. Vielmehr muss auch die Serverseite betrachtet werden, schließlich soll dorthin ja die Verbindung aufgebaut werden. Einer der Schwerpunkte dieses Kapitels wird *DirectAccess* sein, die neue Zugriffslösung von Microsoft, die neu mit Windows 7 und Windows Server 2008 R2 verfügbar ist.

Es gibt aber durchaus auch Windows 7-Neuerungen, die nicht so tief in die gesamte Infrastruktur eingreifen und Änderungen im Serverumfeld erfordern; zu nennen wären hier Features wie *Mobile Broadband* oder *VPN Reconnect*.

Bevor es richtig mit Technik losgeht, möchte ich Ihnen allerdings einige allgemeine Gedanken vorstellen.

Sicherheit und Mobilität

Etliche Themen passen sowohl in das Kapitel zum Thema Mobilität als auch in das Kapitel über Sicherheit. Ein Paradebeispiel ist *BitLocker* – eine Technologie, die eigentlich erst in mobilen Szenarien so richtig Sinn macht, in diesem Buch gleichwohl aber beim Thema *Sicherheit* (Kapitel 12) besprochen wird.

Ebenso könnte man Themen wie *DirectAccess* auch im Kapitel *Sicherheit* einsortieren – hier sehe ich aber den Schwerpunkt eher im Bereich der Mobilität. Die Kapitel zu Sicherheit und Mobilität ergänzen sich also.

13.1 Gedanken zum Thema

In Umfragen unter IT-Verantwortlichen kommt mit schöner Regelmäßigkeit heraus, dass zu den aus deren Sicht wichtigsten Themen auch »Mobilität« zählt. Nun zeigt sich aber, dass der Begriff durchaus erklärungsbedürftig ist. Bei genügend oberflächlicher Betrachtung und mit viel Euphemismus lässt es sich natürlich schon als »Gipfel der Mobilität« ausgeben, wenn für Mitarbeiter Notebooks beschafft werden.

Nach meiner Definition ist das Ziel der Mobilitätsüberlegungen nicht, dass die Mitarbeiter in der Lage sind, im Hotelzimmer oder zu Hause einen Brief auf dem Notebook zu tippen. Vielmehr muss das Ziel sein, dass der Zugriff auf alle wesentlichen Informationen und Prozesse jederzeit und von überall her möglich ist. Hierbei ist es zunächst wichtig, keinesfalls die Sicherheitsaspekte aus den Augen zu verlieren. Andererseits müssen Sie sich in die Arbeitsabläufe von mobilen Mitarbeitern hineinversetzen, wobei es im Wesentlichen zwei Situationen gibt:

- Zum einen gibt es den Mitarbeiter, der abends im Hotelzimmer sitzt und beispielsweise seine Besuchsberichte im CRM-System hinterlegt. Dieser Benutzer wird vermutlich sein eigenes Notebook verwenden und mit einer UMTS-Karte mehr oder weniger glücklich sein.
- Auf der anderen Seite ist eine »wirklich mobile« Situation zu nennen, bei der jemand kurz vor dem Einsteigen in den Flieger noch schnell die E-Mails checken möchte oder vor dem Kundentermin auf dem Parkplatz noch eben die offenen Bestellungen des Kunden in komprimierter Form einsehen will.

Im ersten Fall dürfte die Realisierung nicht weiter kompliziert sein, denn hier genügt vermutlich in der Tat eine »normale« VPN-Verbindung. Sofern die Anwendung, mit der gearbeitet wird, nicht über die Weitverkehrsverbindung auf Ac-

cess-Datenbanken oder dergleichen zugreift, dürfte das auch recht ordentlich funktionieren. Gegebenenfalls können auch die Terminaldienste helfen.

So »richtig mobil« wird es, wenn mit Smartphone, PDA und Co. auf die Unternehmensdaten zugegriffen werden kann. Dies bedingt natürlich eine zusätzliche »Aufbereitung« der Daten – die Displays sind eben doch vergleichsweise klein und die Bedienmöglichkeiten eher eingeschränkt. Man darf aber keinesfalls vergessen, dass die kleinen Mobilgeräte einige ganz wesentliche Vorteile haben:

- Die kleinen Geräte kann man ohne Probleme immer dabei haben. Bei einem »normalen« Notebook ist das ja doch eine ziemliche »Schlepperei«. Ich nehme beispielsweise auf Flug- oder Bahnreisen nur höchst ungern ein Notebook mit.
- Die Mobilgeräte sind sofort betriebsbereit. Wenn man kurz den Posteingang überprüfen oder schnell noch einige »Eckdaten« des Kunden checken möchte, soll das möglichst innerhalb von Sekunden gehen. Mit einem konventionellen Notebook braucht man schon eine Minute, bis man es aufgebaut und eingeschaltet hat und das Gerät hochgefahren ist. Bis dann eine UMTS-Verbindung ins Unternehmensnetz aufgebaut und die benötigte Anwendung aufgerufen ist, ist weitere Zeit verstrichen – Zeit, die man eben eventuell nicht hat.

Nun verhält es sich freilich so, dass es »Paradebeispiele« für die Nutzung mit Mobilgeräten gibt: Der *Exchange Server* ist in seiner Unterstützung für den Zugriff natürlich absolut vorbildlich. Auch *SharePoint* bietet seit Version 2007 in gewissen Grenzen Unterstützung für mobile Geräte. Bei den meisten Anwendungssystemen sind die Möglichkeiten aber eher »bescheiden«. Das wird sich jedoch vermutlich nach und nach ändern.

Des Weiteren bedingt der »Jederzeit-und-von-überall-Zugriff« auch, dass die Unternehmen sich Gedanken über Verfahren, Prozesse und Vorgehensweisen machen, die sich im Laufe der Zeit etabliert haben, und Verbesserungen umsetzen: Absolut katastrophal für die mobile Nutzung ist beispielsweise, wenn wesentliche Kundendaten in Excel-Tabellen vorgehalten werden; das gilt nicht nur für den Einsatz von Mobilgeräten, sondern auch bei der Verwendung von Notebooks.

Die momentan immer populärer werdenden *Netbooks*, die mit Windows 7 auch vernünftig betrieben werden können, positionieren sich als »dritter Weg« zwischen Notebook und Smartphone/PDA. Diese Geräte laufen mit »normalen« Betriebssystemen wie eben Windows 7, verfügen über Tastaturen, sind aber deutlich kleiner und leichter als ein normales Notebook.

Nichtdestotrotz bleibt die Herausforderung, grundsätzlich über die mobile Anwendungslandschaft nachzudenken – vermutlich werden Sie da an Themen wie Datenhaltung und Zugriff deutlich arbeiten müssen.

Grundsätzlich empfehle ich meinen Kunden, bei jeder Veränderung in der Applikationslandschaft über die Frage nachzudenken, ob ein mobiler Zugriff auf die Daten in Zukunft notwendig sein könnte und wie dieser zu realisieren ist. Auch wenn das erst ein Thema für das nächste Jahr ist, gehören solcherlei Aspekte heute einfach zu einer ganzheitlichen und nachhaltigen Planung dazu.

Zu prüfen ist jeweils auch, ob es genügt, wenn Daten in Online-Szenarien zur Verfügung stehen oder ob auch eine Offline-Nutzung erforderlich ist.

Bevor man sich für die Nutzung einer Technologie entscheidet, muss eine Antwort auf die Frage gefunden werden, ob sich die Investitionen auch in irgendeiner Form amortisieren. Eine Investition rechnet sich beispielsweise, wenn die Betriebskosten gesenkt werden können oder aber die Produktivität der Benutzer gesteigert werden kann. Bei Lösungen aus dem Bereich »Business Productivity«, zu denen unzweifelhaft auch der Einsatz von Mobilgeräten gehört, ist die Messbarkeit der erreichten Verbesserungen häufig ein Problem. Dass ein Produktivitätszuwachs der Außendienstmitarbeiter erreicht wird, wenn diese zum Abrufen und Schreiben von Mails oder zur Pflege des CRM-Systems nicht jedes Mal erst ins Büro fahren müssen, liegt auf der Hand. Im Einzelnen ergeben sich diese Vorteile:

- Die Außendienstmitarbeiter sparen im Schnitt eine Stunde Zeit pro Person und Tag, weil sie eben direkt von zu Hause aus zu Kunden aufbrechen können.
- Im Zweifelsfall kann man vielleicht auch noch Fahrtkosten im Sinne von Treibstoff, zusätzliche Abnutzung des Fahrzeugs etc. aufführen. Sagen wir, jeder Außendienstmitarbeiter fährt täglich 50 km weniger.
- Die Reaktionszeit, mit der die Außendienstmitarbeiter auf Mails reagieren, sinkt, was im besten Fall zu einer höheren Kundenzufriedenheit führt.
- Die Güte der erfassten Daten im CRM-System dürfte sich auch verbessern, denn schließlich muss der Mitarbeiter die Daten nicht erst auf Zetteln notieren oder aber hoffen, dass er nicht zwischenzeitlich die Hälfte vergisst.

Diese Vorteile werden die meisten Entscheider begreifen, kompliziert wird es aber bei der Messbarkeit der erreichten Verbesserungen:

- Führt die täglich eingesparte Fahrtstunde eines Außendienstmitarbeiters tatsächlich zu einem höheren Ertrag des Unternehmens? Wenn ein Servicetechniker dadurch pro Tag einen zusätzlichen Auftrag ausführen kann, wird jeder überzeugt sein. Bei einem Vertriebsmitarbeiter liegt ist der Fall schon schwieriger: Natürlich hilft auch ihm eine zusätzliche produktive Stunde, der Rückschluss, dass er dann nachweislich pro Tag zusätzliches Umsatzvolumen in Höhe von EUR 15.000 reinholt, ist in den meisten Fällen aber leider zu gewagt.

Auch die anderen genannten Punkte könnten, je nach Gesprächspartner, zu mehr oder weniger fruchtlosen Diskussionen führen. Die Vorteile im Business-Productivity-Bereich sind definitiv nicht so einfach messbar wie bei einem Projekt zur Serverkonsolidierung und/oder Plattform-Vereinheitlichung im Rechenzentrum, in dessen Folge direkt ein Drittel der bestehenden Wartungsverträge gekündigt werden kann.

Wenn Sie ein Mobility- oder ganz allgemein ein Business-Productivity-Projekt planen, sollten Sie über die Fragen der Messbarkeit sehr sorgfältig nachdenken – und zwar im Vorfeld des Gesprächs mit dem Entscheider und nicht erst, wenn er Sie danach fragt. Ein Stück weit hängt die Argumentationslinie natürlich auch von dem Blickwinkel ab, mit dem die entsprechende Person an die Angelegenheit herangeht:

- Wenn die Argumentationslinie »100 Mitarbeiter sparen pro Tag eine Stunde Zeit« genügt, haben Sie gute Karten. Die Mitarbeiter werden die Zeit sparen, ich kann Ihnen nur nicht versprechen, ob dies messbar zu mehr Umsatz führt.
- Wenn Sie genau nachweisen müssen, dass das Unternehmen durch die Maßnahme entweder mehr Geld einnimmt und/oder weniger Geld ausgibt, wird es auf jeden Fall komplizierter. Bei Projekten zur Servicesteuerung wird dies noch vergleichsweise überzeugend zu rechnen sein, aber im eher vertrieblichen Umfeld wird es in diesem Moment kompliziert: Wie versichern Sie glaubhaft, dass jeder Vertriebsaußendienst-Mitarbeiter EUR 15 000 zusätzlichen Umsatz in der gesparten Stunde akquiriert?
- Die dritte Argumentationslinie ist die *Notwendigkeit*. Dazu drei Beispiele:
  - Wenn Sie zufällig zu einer Branche gehören, in der die Kommunikation per E-Mail überhaupt keine Rolle spielt und in absehbarer Zeit auch nicht spielen wird, brauchen Sie sich natürlich keine Sorgen zu machen, wenn Ihre Außendienstmitarbeiter unter Umständen tagelang keine Mail lesen. Ansonsten bleibt Ihnen gar nichts anderes übrig, als einen mobilen Mailclient bereitzustellen. Kaum ein Kunde hat allzu großes Verständnis dafür, wenn Anfragen tagelang liegen bleiben, weil der angeschriebene Mitarbeiter eine Woche auf Geschäftsreise ist. Auch firmenintern ist es nicht allzu gut, wenn Geschäftsprozesse stocken, weil der Mitarbeiter nicht antwortet – da er gar nicht erst die Frage erhalten hat.
  - Wenn in Ihrem Unternehmen ein taggenaues Forecasting der Umsätze erwartet wird, müssen Sie den Vertriebsmitarbeitern einen Weg zur Verfügung stellen, diese Daten einzutragen. Eine Zugriffsmöglichkeit über ein Mobilgerät würde das Problem lösen.

- Wenn es Mitarbeiter gibt, die jederzeit Kenntnis über aktuelle Daten haben sollen, müssen diese eine Zugriffsmöglichkeit haben. Beispiele sind Abteilungs- und Bereichsleiter, die jederzeit Überblick über die Situation in den von ihnen verantworteten Unternehmensbereichen haben sollen. Ein anderes Beispiel sind Vertriebsmitarbeiter, von denen die tägliche Überwachung der Außenstände oder Lieferrückstände der jeweiligen Kunden verlangt wird.

Bei der Überlegung, ob das Unternehmen eine mobile Lösung benötigt, sollte die Entwicklung der Arbeitswelt nicht außer Acht gelassen werden. Dies wird im folgenden Abschnitt vertieft.

13.1.1 Arbeitswelt – gestern heute und morgen

Die Einführung mobiler Technologien ist kein Selbstzweck, sondern soll das Business in die Lage versetzen, erfolgreicher zu sein. Dabei geht es zumeist um bessere und gleichzeitig preiswertere Produkte oder Dienstleistungen, die in einer noch höheren Zahl als bisher verkauft werden sollen. Alle Unternehmensbereiche müssen mitarbeiten:

- Die Produktentwicklung muss das vorhandene Wissen ständig erweitern, Erfahrungen, die das Unternehmen auf dem Markt macht, einfließen lassen und noch bessere Produkte auf den Markt bringen.
- Die Produktion (im Dienstleistungsbereich die ausführenden Personen) muss sowohl effektiv als auch effizient sein und einem Prozess stetiger Verbesserung unterworfen sein.
- Der Vertrieb muss sein bestehendes Beziehungsnetz einerseits pflegen, andererseits ausbauen. Er muss die Kunden begeistern und letztendlich dazu bringen, die Produkte/Dienstleistungen des Unternehmens zu kaufen.
- Die Aufgabe des Managements ist es, die unterschiedlichen Bereiche zu synchronisieren und dafür zu sorgen, dass, vereinfacht gesagt, das Gesamtergebnis stimmt. Hierbei wird das Management unter anderem von Einheiten wie dem Controlling unterstützt.

Hinter all diesem Tun steckt das Ziel, ein ertragreiches Geschäft zu realisieren. Und im Grunde genommen hat sich das grundlegende zuvor skizzierte Verfahren, wenn man es hinreichend stark abstrahiert, in den vergangenen Jahrzehnten nicht geändert und wird dies auch in den nächsten Jahrzehnten nicht tun. Die Unterschiede zwischen den Jahren 1970, 2000 und 2030 bestehen darin, dass sich die Rahmenbedingungen und die Art des tatsächlichen Handelns geändert haben. Um es vereinfacht zu sagen, wird ein Unternehmen, das zwar perfekte Produkte/Dienstleistungen anbietet, aber mit den Methoden von 1970 arbeitet, heute keinesfalls erfolgreich sein können.

Gestern

Vielleicht können Sie sich noch erinnern, wie die Welt vor 25 Jahren aussah? Wenn ich Fotos aus dieser Zeit betrachte, fallen mir drei Dinge ins Auge:

- Erstens sehen die Autos ganz anders aus als heute.
- Zweitens haben die Menschen ganz erstaunliche Frisuren und Kleider.
- Drittens haben nicht 30 % der Menschen, die Sie auf diesen Bildern sehen, ein Mobiltelefon am Ohr. Die Quote liegt ziemlich genau bei 0 %. Nicht, dass es nicht schon Mobiltelefonie gegeben hätte, ein B-Netz-Gerät füllte aber einen deutlichen Teil des Kofferraums.

Vor mehr als 25 Jahren, nämlich am 12.08.1981, war der erste Auftritt des IBM 5150 am Markt. Und damit haben wir auch bereits die beiden Technologien, die beim Thema Mobilität die Hauptrollen spielen: *Mobilfunk* und der *Persönliche Computer*«. In dieser Zeit waren Computer in Unternehmen zwar durchaus nichts Ungewöhnliches, schließlich markiert der 12.08.1981 nicht den Beginn der Computernutzung, sondern »nur« das Entstehen einer Plattform. Wir können aber festhalten, dass sowohl die vorhandenen Großrechner als auch die Systeme der mittleren Datentechnik primär dazu verwendet wurden, Daten zu verwalten, die aus den Bereichen Buchhaltung, Materialwirtschaft, Warenwirtschaft oder Vertragsverwaltung kommen. In dieser Zeit hatten weder die E-Mail noch das Internet (beides gab es ja auch schon vor dem Entstehen des PCs) irgendeine breitere praktische Bedeutung für das Geschäftsleben. Ein weiterer Aspekt ist die Erreichbarkeit von Mitarbeitern: Wenn irgendjemand auf Geschäftsreise war, war er eben nicht erreichbar. Punkt.

Die Geschäftsprozesse waren bei allen Unternehmen nach heutigen Maßstäben nicht schnell, das ist auch nicht zu erwarten, wenn das Transportmedium primär ein Blatt Papier ist. Da aber alle Unternehmen auf diese Weise arbeiteten, war diese, aus heutiger Sicht nicht mehr akzeptable Vorgehensweise in Ordnung.

Heute

Betrachten wir die Zeit seit dem Jahr 2000, haben sich gegenüber dem zuvor beschriebenen »Gestern« diverse neue Szenarien entwickelt:

- An den meisten Arbeitsplätzen steht heute ein Computer, und im Büro ist jeder Arbeitsplatz computerisiert.
- E-Mail ist mittlerweile in vielen Fällen das wichtigste Kommunikationsmedium, ansonsten rangiert es in seiner Bedeutung nur knapp hinter dem Telefon.
- Generell ist das Internet eine Informationsquelle bzw. ein Kommunikationsweg, der innerhalb weniger Jahre den Alltag vieler Unternehmen und das

Verhalten der Menschen umgekrempelt hat: Benötigt man Informationen (gleich welcher Art), startet man den Browser. Noch vor einigen Jahren habe ich dem Hersteller, dessen Produkt mich interessierte, eine Postkarte geschickt und um Übersendung einer Produktbroschüre gebeten.

- Insbesondere dank DSL sind performante und ständig aktive Internetanbindungen auch für Privatpersonen bezahlbar. Ich hatte vor ein paar Jahren die Vision, dass in jeder Firma oder in jedem Haushalt eine permanente Internetverbindung existiert, interessant, aber nicht realistisch gefunden. Mittlerweile ist dieser Zustand weitgehend erreicht.
- Die Unternehmen begreifen den Computer nicht nur als bessere elektronische Schreibmaschine, sondern als ein Werkzeug, mit dem sich Geschäftsprozesse abbilden lassen (Workflows).
- Die Verbreitung von Mobiltelefonen ist mittlerweile so hoch, dass man eine Person im Alter zwischen 15 und 65, die nicht mit einem Handy herumläuft, mit der Lupe suchen muss. Bereits seit einiger Zeit gibt es deutlich mehr Mobiltelefon- als Festnetzanschlüsse.
- Mobile Datenübertragung ist seit GPRS und UMTS ebenfalls »Alltag« geworden – zumindest technisch. In vielen Unternehmen ist der mobile Zugriff auf die Daten allerdings noch kein Thema.

Verlassen wir für einen Moment die eher technische Betrachtung, und schauen wir auf die Geschäftsabläufe. Ein wesentlicher Aspekt ist, dass das Business mobiler wird. Ein interessantes Beispiel sind die ausländischen Absatzmärkte: Vor zwanzig Jahren wurden Geschäfte im Ausland primär von Konzernen oder den ganz großen Mittelständlern getätigt. Mittlerweile haben sogar kleinere Mittelständler Kunden oder Lieferanten im europäischen oder gar weltweiten Ausland, und häufig werden auch Fertigungsstätten im Ausland betrieben. Das Fazit ist, dass die Mitarbeiter häufiger und länger unterwegs sind bzw. sein werden. Die Erreichbarkeit per Telefon ist dank Mobiltelefon kein Problem, ein mobiler Mitarbeiter benötigt aber noch mehr – und zwar jede Menge an Daten:

- Ganz oben in der Liste steht der Zugriff auf E-Mail, Kontakt- und Termindaten.
- Ein Vertriebsmitarbeiter muss Einträge im CRM-System lesen und vornehmen können.
- Ein Servicemitarbeiter benötigt Zugriff auf die Außendienststeuerung und soll möglichst elektronisch seine Leistungen erfassen und in die Zentrale melden.
- Etliche Mitarbeiterrollen benötigen lesenden Zugriff auf Kenndaten des Unternehmens, beispielsweise gebuchte Umsätze, Lieferrückstände, offene Posten und vieles andere mehr.

- Wer nur selten im Büro ist, benötigt im Grunde genommen Zugriff auf sämtliche für ihn relevanten Informationstypen. Das beginnt bei allgemeinen Unternehmensinformationen, die in einem Intranet stehen, und reicht bis zu projektspezifischen Listen oder Berichten.

Nun ist es keinesfalls so, dass nur Mitarbeiter mit Auslandsverwendung mobiler werden. Viele Mitarbeiter verdienen Geld dadurch, dass sie beim Kunden sind, beispielsweise Vertriebs- oder Servicemitarbeiter. Diese sollten möglichst nicht dadurch, dass sie immer wieder ins Büro fahren müssen, von produktiven Aufgaben (also mit Kunden zu sprechen oder etwas zu montieren oder zu betreuen) abgehalten werden. Da es gleichzeitig aber notwendig ist, dass die Mitarbeiter E-Mails beantworten, das CRM-System pflegen, Daten einsehen und vieles andere mehr, ist es zwingend erforderlich, dass Sie sich darüber Gedanken machen, wie das funktionieren kann. Sie haben im Grunde genommen drei Möglichkeiten:

- Sie ignorieren das Problem. Das führt nun zwar nicht zur sofortigen Insolvenz der Firma, Ihre Kunden werden aber feststellen, dass die Mitbewerber schneller im Service, besser bei der Betreuung und dergleichen sind. Stellen Sie sich einfach vor, Ihre Firma würde arbeiten wie vor 30 Jahren, also mit einem Kundenordner aus Papier, Schreibmaschine und handgeschriebenen Lieferscheinen. Ich denke, dass die Firma nicht mehr wettbewerbsfähig ist, egal wie gut die Produkte sind. Auch wer auf dem Status des Jahres 2000 stehen bleibt, wird spürbare Probleme bekommen, weil der Mitbewerb schneller, schlanker und kundenorientierter ist.
- Die zweite Möglichkeit ist, dass Sie alle Mitarbeiter im Außendienst mit Notebooks nebst UMTS-Karten ausrüsten. Das ist schon nicht schlecht – bis der Datenzugriff steht, ist es aber ein langer Weg (Notebook aufklappen, Betriebssystem hochfahren, mit der Datenkarte einwählen etc.). Wer viel im Außendienst unterwegs ist, kennt die Anforderung, dass man Informationen eben »schnell mal zwischendurch« abrufen oder erfassen möchte, also innerhalb von 10 Sekunden Mails checken oder ganz schnell die Telefonnummer des Kontakts suchen oder die gerade gefundene Verkaufschance im CRM-System eintragen. Ich bin mein ganzes Berufsleben im Außendienst gewesen, und ich kann Ihnen versichern, dass es unglaublich nervig ist, wenn man für eine kleine Information relativ großen Aufwand treiben muss. Falls Sie Innendienst-Mitarbeiter sind, können Sie einen Tag lang versuchen, den PC jedes Mal, wenn Sie etwas recherchiert oder erfasst haben, auszuschalten. Nach spätestens einem Tag wissen Sie, was ich meine: Es ist maximal grausam, sich mehrmals am Tag den Startvorgang des PCs anzuschauen.
- Smartphones und PDAs bieten zwar nur eine stark reduzierte Displaygröße, dafür sind sie aber wirklich mobil und sofort nach dem Einschalten einsatzfä-

hig. Für »echte Mobilitätsanforderungen« sind die kleinen Mobilgeräte deutlich geeigneter als ein Notebook mit UMTS-Karte, allerdings wird spezielle Software benötigt. Da es zumindest für die Pocket-PC-Geräte Browser und Terminaldienste-Clients gibt, könnte man auf die Idee kommen, so auf die Standardanwendungen oder -Webapplikationen zuzugreifen. In der Praxis wird das Ergebnis allerdings enttäuschend sein: Auch wenn der Terminaldienste-Client grundsätzlich den Desktop anzeigen kann, ist ein sinnvolles Arbeiten kaum möglich, weil man primär mit dem Hin- und Herschieben des sichtbaren Bildschirminhalts beschäftigt ist. Die Nutzung von Webapplikationen, die für Desktop-Browser vorgesehen sind, wird ebenso unbefriedigend verlaufen: Einerseits setzt eine Webapplikation zumeist eine Auflösung von 800 × 600 Pixel oder höher voraus, andererseits können die Browser von Mobilgeräten nicht sonderlich gut mit der exzessiven Nutzung von JavaScript- oder Flash-Inhalten umgehen.

Fakt ist, dass die *Windows Mobile*-Geräte die neuen Mobilitätsanforderungen in den meisten Fällen am besten erfüllen können. Voraussetzung ist aber, dass eine entsprechende Applikationsinfrastruktur vorhanden ist: Benötigt werden sowohl die auf dem Mobilgerät laufenden Anwendungen als auch eine Serverlandschaft, die Daten und Informationen in geeigneter Form bereitstellen kann. Das mobile Messaging ist Vorreiter, hier ist heute schon ein sehr hoher Erfüllungsgrad erreicht. Andere Anwendungen sind ebenfalls mobil nutzbar, teils mit speziellen Clients (wie bei *Microsoft Dynamics CRM*) oder mit Anpassungen (z. B. *Microsoft SQL Server Reporting Services*).

Morgen

In den vergangenen Jahren ist, nach dem Platzen der Dot-Com-Blase, primär auf eine Kostenreduktion beim Betrieb des IT-Systems geachtet worden. Die Benutzereffizienz ist dabei deutlich auf der Strecke geblieben. *Benutzereffizienz* bedeutet, dass die Benutzer über geeignete Arbeitswerkzeuge (Software/Hardware) verfügen müssen, um problemlos und schnell sämtliche benötigten Informationen finden und bearbeiten zu können. Hierbei darf es auch keine Rolle mehr spielen, wo der Benutzer sich befindet – im Zeitabschnitt »Morgen« wird für viele Personen der Arbeitsmittelpunkt nicht mehr das Büro sein.

Die morgige Arbeitswelt wird sich in Stichworten folgendermaßen beschreiben lassen:

- Immer mehr Mitarbeiter sind mobil. »Mobil« bedeutet in diesem Zusammenhang nicht, dass die Mitarbeiter hin und wieder eine Dienstreise machen, sondern dass der Arbeitsmittelpunkt nicht mehr ein Schreibtisch im Büro mit einem PC darauf ist. Da die Mitarbeiter im Zweifelsfall nur einmal pro Woche,

einmal pro Monat oder noch seltener im Büro sind, sind sie auf einen mobilen Datenzugriff angewiesen.

- Da die Menge und die Bedeutung der IT-mäßig abgebildeten Geschäftsprozesse steigen, müssen diese auch von der mobilen Arbeitsumgebung bedienbar sein. Ein »Eben-mal-Reinschauen« ist genauso normal wie das Abhören der Handy-Mailbox.
- Es ist also nicht nur normal, ein Mobiltelefon dabei zu haben, sondern eine IP-Adresse mit ständiger Kommunikation mit den Servern im Unternehmen wird die Regel sein.
- Da die Kosten für mobile Datenübertragung weiter sinken werden, wird es in kaum einem Unternehmen mehr eine Diskussion darüber geben, ob man diese Technologie implementiert oder weiter ausbaut. Heute überlegt kein Unternehmen mehr, ob es Außendienstmitarbeiter mit Mobiltelefonen ausstattet; morgen gehört das mobile Datenendgerät zur Grundausstattung.

Dass diese sehr mobile Arbeitswelt entstehen wird, steht außer Frage. Offen ist aber, wie die Unternehmen es schaffen, ihre IT-Strukturen darauf auszurichten. Wenn das Wissen des Unternehmens im Wesentlichen lediglich in Form von Millionen Word- und Excel-Dateien im Dateisystem vorhanden ist, wird der Weg sicherlich beschwerlich werden. Der erste Schritt, nämlich zur mobilen Mail, ist vergleichsweise schnell und einfach umzusetzen. Die nächsten Schritte sind komplexer: Wenn beispielsweise das Kundenmanagement mit Excel-Tabellen durchgeführt wird, hat ein mobiler Anwender so gut wie keine Chance, sinnvoll auf diese Daten zuzugreifen und Änderungen vorzunehmen. »Management per Excel« ist in vielen Unternehmen, auch bei großen Mittelständlern, nach wie vor weit verbreitet. Es wird sich nicht vermeiden lassen, das Thema *Datenhaltung* sehr ganzheitlich und nachhaltig anzugehen, um die Anforderungen erfüllen zu können, die vom Business an die IT gestellt werden. Die Anforderungen heißen:

- Die Benutzer müssen Informationen problemlos finden können, das Wissen der Firma muss im Zugriff sein.
- Die Benutzer müssen gemeinsam an Datenbeständen arbeiten können, und zwar ohne »Collaboration per E-Mail« zu betreiben, d. h. durch ständiges Versenden von Dateianhängen.
- Die Geschäftsprozesse sollen elektronisch abgebildet werden. Hier kommt übrigens das Thema *Workflow* ins Spiel.
- Mobile Benutzer müssen uneingeschränkten Zugriff auf alle relevanten Daten haben.

Neben diesen primär auf den Datenzugriff abzielenden Forderungen wird in der zukünftigen Arbeitswelt die Echtzeitkommunikation (*Real Time Collaboration*) einen großen Stellenwert haben. Hierbei geht es um:

- Präsenzinformationen
- Instant Messaging
- Application Sharing
- Videokonferenz
- Voice

In diesem Zusammenhang möchte ich insbesondere auf den letztgenannten Punkt hinweisen, nämlich die Sprachkommunikation. Bislang sind Sprache und der »Rest der Kommunikation« zwei getrennte Welten. Auf der einen Seite steht die Telefonanlage mit Systemtelefonen, auf der anderen die Computerwelt mit Desktops und Servern. Es ist damit zu rechnen, dass sich in vielen Unternehmen das Thema Sprachkommunikation mehr und mehr in Richtung der IT bewegt – schließlich ist jeder PC und übrigens auch jedes *Windows Mobile*-Gerät in der Lage, Sprachkommunikation zu betreiben. Produkte wie der *Microsoft Office Communications Server* fungieren in diesem Szenario als zentrale »Vermittlungsstelle«.

13.1.2 Kosten

Ein häufig diskutiertes Thema sind die Kosten der mobilen Datenübertragung – zumindest dann, wenn UMTS-Verbindungen ins Spiel kommen.

Ich möchte nun überhaupt nicht wegdiskutieren, dass es Geld kostet, wenn ein Unternehmen seine Mitarbeiter nicht nur mit Notebooks, sondern auch für die UMTS-Datenübertragung ausrüstet. Wie Sie auf Abbildung 13.1 sehen können, kostete bei *T-Mobile Deutschland* im August 2009 eine Datenflatrate 33,57 EUR (zzgl. MwSt, Preisangaben unverbindlich und nur zur Orientierung).

Ich bin absolut davon überzeugt, dass sich diese Investition für das Unternehmen rechnen wird – auch wenn man es wahrscheinlich nur schwer in Euro und Cent gegenrechnen kann. Die Zeit, die ein Mitarbeiter durch mobilen Zugriff auf das Unternehmensnetz sparen kann, ist signifikant. Wenn Sie nicht nur einen Flatrate-Datentarif beschaffen, sondern mehrere Mitarbeiter ausrüsten, dürften die Preise noch »angenehmer« werden – fragen Sie einfach beim Mobilfunkanbieter Ihres Vertrauens nach.

Weiterhin bleibt anzumerken, dass vermutlich alle Unternehmen schon wesentlich mehr Geld für wesentlich weniger sinnvolle Maßnahmen ausgegeben haben als diesen monatlichen Betrag für die UMTS-Konnektivität.

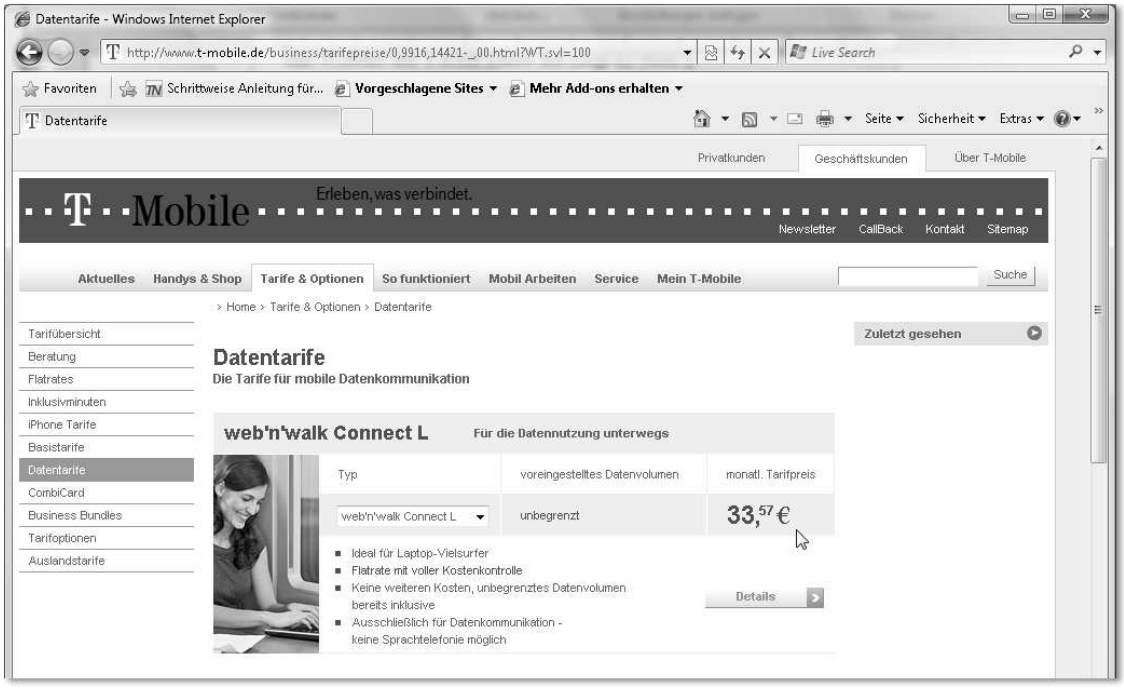


Abbildung 13.1 Datenflatrates sind durchaus bezahlbar. (Beispiel: T-Mobile Deutschland, Stand 08/2009)

13.2 DirectAccess

Eines der spannendsten Beispiele für neue Mobilitäts-Features in Windows 7 ist sicherlich *DirectAccess*. Im Zusammenhang mit dieser Technologie findet man Aussagen wie »das VPN der nächsten Generation«. Obwohl man mit solch euphorischen Aussagen sicherlich vorsichtig sein sollte, hat DirectAccess sicherlich das Potenzial, in Unternehmen mit mobilen Mitarbeitern eine wertvolle Erweiterung zu werden. Etwas salopp gesagt, wird der mobile Client mit DirectAccess »nahtlos« in das Unternehmens-LAN integriert. Sobald der Client eine IP-Verbindung aufbaut, wird geprüft, ob er sich im Unternehmensnetz befindet. Ist dies nicht der Fall, baut er direkt und ohne weiteres Zutun des Benutzers eine Verbindung dorthin auf. Er ist also sozusagen »always-on« im LAN, was zahlreiche Vorteile hat:

- Der Benutzer kann einfach auf lokale Ressourcen zugreifen, und zwar ohne dass er erst mehr oder weniger umständlich VPN-Verbindungen aufbauen muss.
- Das Management von Clients, die sich selten im Unternehmens-LAN befinden, verbessert sich. Zum einen kann jeder beliebige Prozess auf Server im LAN zugreifen – beispielsweise für Windows-Updates (WSUS), für Softwareverteilungs- und Inventarisierungszwecke und dergleichen mehr.

- Weiterhin ist es möglich, auf dem LAN auf den Client zuzugreifen, was ebenfalls für Management-Werkzeuge interessant sein könnte.

Etliche meiner Kunden interessieren sich sehr für die Möglichkeiten von DirectAccess und haben es bereits sehr früh getestet – die Technologie hat also durchaus eine hohe Praxisrelevanz.

Die wichtigsten Voraussetzungen

Bevor Sie sich mit Begeisterung auf DirectAccess stürzen, möchte ich auf einige wesentliche Voraussetzungen hinweisen. DirectAccess ist nämlich nicht »mal eben so« implementiert. Die wichtigsten Voraussetzungen:

- DirectAccess-Clientfunktionalität ist nur in der *Enterprise*- und der *Ultimate*-Edition von Windows 7 enthalten.
- Es wird ein *Windows Server 2008 R2* als DirectAccess-Server benötigt.
- Der DirectAccess-Server benötigt zwei aufeinanderfolgende öffentliche IP-Adressen. Hierbei muss es sich um geroutete Adressen handeln, NAT ist nicht möglich.
- Mindestens ein DNS-Server muss auf einem *Windows Server 2008*-Domänencontroller (DC) laufen. Dieser DC muss auf *Windows Server 2008 SP2* oder *Windows Server 2008 R2* basieren.
- Da diverse Zertifikate benötigt werden, ist eine eigene PKI unumgänglich. Die zugehörige Zertifikatssperrliste muss aus dem öffentlichen Internet abrufbar sein.
- DirectAccess basiert auf IPv6. Die Server, auf die DirectAccess-Clients zugreifen sollen, müssen über ein aktiviertes IPv6 verfügen. Alternativ kann NAT-PT zur Umsetzung zwischen IPv4- und IPv6-Adressen verwendet werden. Eine solche Funktionalität müsste allerdings von einem Drittthersteller bezogen werden, Windows Server 2008 enthält keine NAT-PT-Funktionalität.

Aus diesen Voraussetzungen ergibt sich, dass DirectAccess keine Technologie für ein kleines Unternehmen ist, dessen Geschäftsführer einen komfortablen mobilen Zugriff auf Unternehmensdaten wünscht.

Wenn Sie ohnehin Windows 7-Enterprise- oder Ultimate-Edition-Clients einsetzen, sind die zusätzlichen Kosten für die Implementation vergleichsweise gering.

13.2.1 Funktionsweise

Auf Abbildung 13.2 ist die Funktionsweise von DirectAccess vereinfacht dargestellt:

- Befindet sich der Client im Internet, greift er auf Ressourcen, die nicht im Unternehmens-LAN liegen (beispielsweise öffentliche Webserver), direkt zu. Bei »normalen« VPNs ist das Verhalten bekanntlich anders: Dort wird bei einer aktiven VPN-Verbindung sämtlicher Verkehr über das VPN geleitet, d. h., auch die Webzugriffe der Benutzer werden darüber geleitet. Auf den ers-

ten Blick hört sich das vielleicht gar nicht schlecht an, da die Webzugriffe sich so kontrollieren bzw. filtern lassen. Wenn allerdings die Zugriffe von vielen weltweit verteilten Benutzern immer über die Zentrale erfolgen müssen, resultiert das in einem signifikanten Bandbreitenbedarf – bei einigermaßen begrenztem Nutzen.
Also: Datenverkehr, der nicht Ressourcen im Unternehmens-LAN betrifft, erfolgt direkt.

Hinweis

Sofern bei den mobilen Clients ein Proxy eingetragen ist, wird dieser Verkehr über diesen geführt und somit dann doch durch das Unternehmen transportiert. Es empfiehlt sich also, die Clients so zu konfigurieren, dass unterwegs kein Proxy verwendet wird.

- Greift der Client auf eine Ressource im Unternehmens-LAN zu, wird der Verkehr verschlüsselt über das Internet zum DirectAccess-Server geleitet. Von dort werden die Datenpakete dann zum jeweiligen Server im Unternehmens-LAN transportiert.

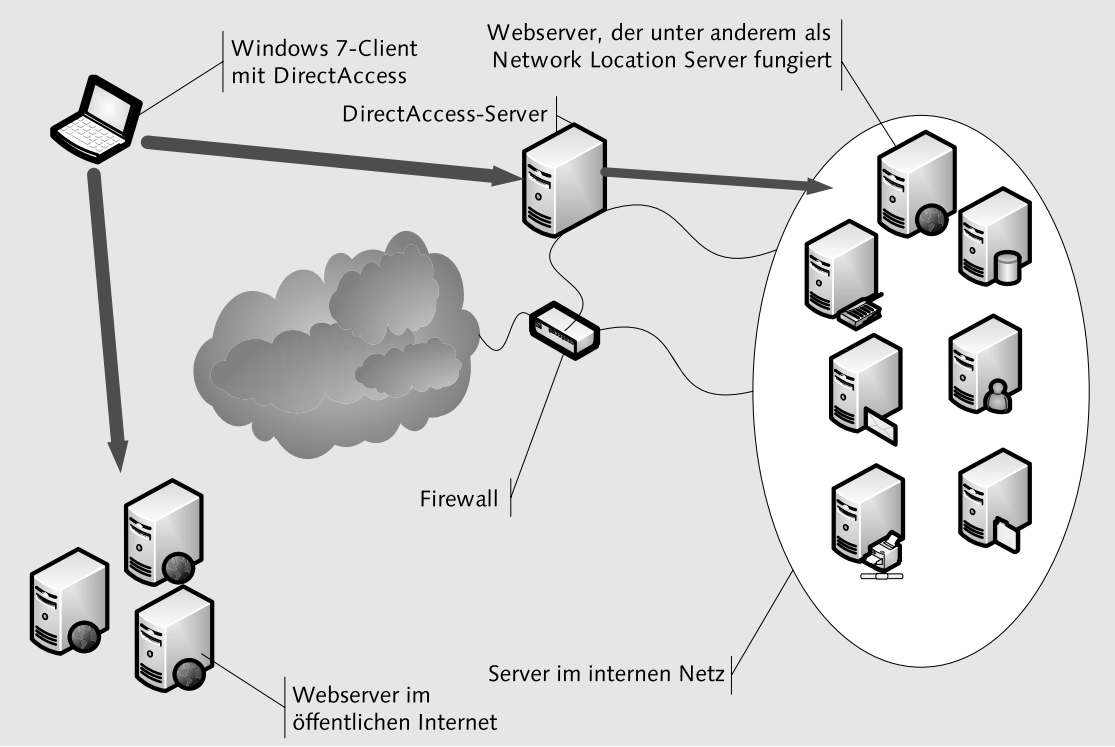


Abbildung 13.2 Das Funktionsprinzip von DirectAccess

Wenn Sie Abbildung 13.2 betrachten, sieht das auf den ersten Blick nicht deutlich anders als ein »normales« VPN aus. Sie werden im Laufe des Kapitels aber sehen, dass es diverse Unterschiede gibt, die in letzter Konsequenz dazu führen, dass die

Clients sozusagen vollständig ins Unternehmensnetz integriert sind. Dazu ein kleines Beispiel: Wird der Client eingeschaltet und hat er Verbindung zum Internet, ist er mit dem Unternehmensnetz verbunden – auch ohne einen angemeldeten Benutzer. In diesem Moment können bereits Management-Aufgaben laufen, wie beispielsweise das Herunterladen von Patches vom zentralen WSUS-Server, das Verteilen von Software, das Inventarisieren und vieles andere mehr.

13.2.2 Einige Technologiegrundlagen

In diesem Abschnitt möchte ich einige Technologiegrundlagen vorstellen, die von DirectAccess genutzt werden.

IPv6 und Tunnelmechanismen

DirectAccess basiert auf IPv6.

Ich möchte etwas deutlicher werden: DirectAccess ist ohne IPv6 nicht funktionsfähig. Da die meisten Unternehmen und Organisationen in Europa die Infrastruktur (noch) nicht auf IPv6 umgestellt haben, überlegen Sie sich jetzt vielleicht, das Buch direkt zuzuklappen und die Hoffnung auf DirectAccess zu begraben. Das ist aber vermutlich nicht notwendig, da letztendlich »nur« die Kommunikation zwischen dem DirectAccess-Server und dem vom Client angesprochenen Server über IPv6 laufen muss. Es ist nicht notwendig, dass außerhalb des Rechenzentrums das neue IP-Protokoll verwendet wird, was ein komplexeres IPv6-Konzept bedingen würde.

Weiterhin ist anzumerken, dass kaum ein Provider in der Lage ist, IPv6-Zugang zum Internet anzubieten. Der Datenverkehr über das Internet muss also über IPv4 laufen. Abbildung 13.3 zeigt das anhand einer kleinen Skizze:

- Der DirectAccess-Client spricht die Ressourcen im internen LAN über deren IPv6-Adressen an.
- Die IPv6-Pakete werden über das Internet mittels eines Tunnelmechanismus transportiert. Die Nutzung des IPv4-Internets ist also kein Problem.
  Sofern Ihnen dieses Buch in einigen Jahren wieder in die Hand fällt, wenn IPv6 flächendeckend zur Realität geworden ist: Die Übertragung durch das Internet kann auch über IPv6 erfolgen.
- Die Datenübertragung vom DirectAccess-Server zu den Servern im internen LAN erfolgt über IPv6.

IPv6 ist Vorraussetzung

Aus der Skizze folgt übrigens eine wirklich wichtige Erkenntnis: Die Server im internen Netz, auf die per DirectAccess zugegriffen werden soll, müssen (!) IPv6 sprechen.

Mit *Windows Server 2003* und *Windows Server 2008* ist das kein Problem, ältere Maschinen scheiden aus.

Sofern Sie unbedingt per DirectAccess auf auf einen NT-Server oder Windows 2000-Server zugreifen müssen, gibt es einen Workaround in Form von *NAT-PT*. NAT-PT dient vereinfacht gesagt als Brücke zwischen IPv6 und IPv4. Diese Funktionalität ist aber in *Windows Server 2008 R2* nicht vorhanden, müsste also von einem Drittthersteller gekauft werden. (*Cisco* verfügt beispielsweise über Geräte mit dieser Funktion.)

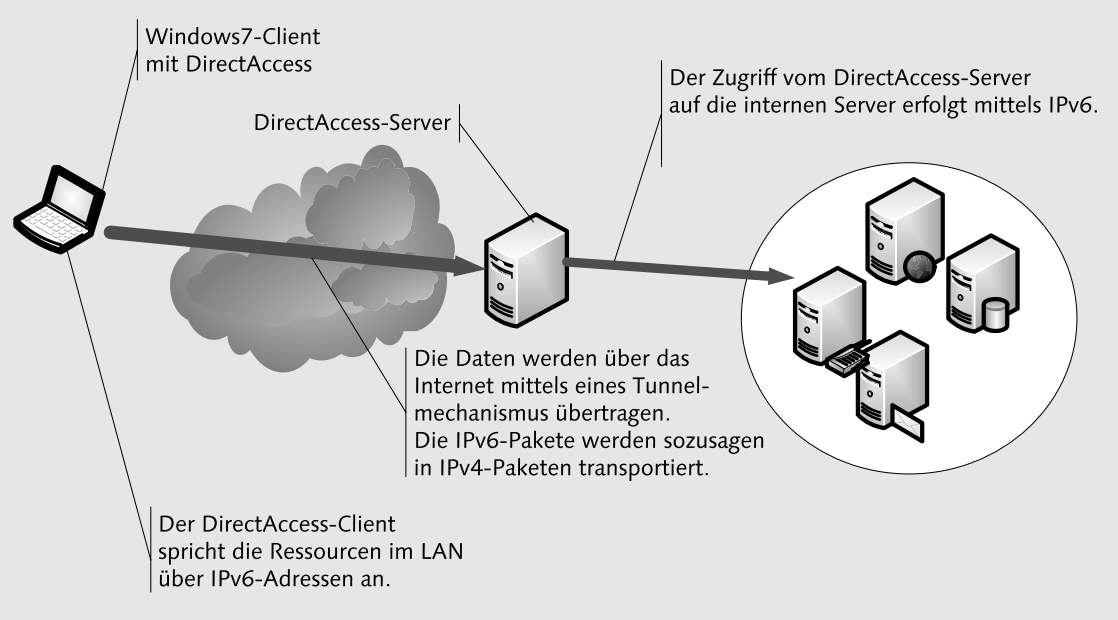


Abbildung 13.3 Die IPv6-Pakete werden über das IPv4-Internet mithilfe eines geeigneten Tunnelmechanismus übertragen.

Folgende Tunnelmechanismen können zum Einsatz kommen:

- *ISATAP*: Diese Technologie wird eingesetzt, um IPv6-Datenpakete durch ein IPv4-Intranet zu tunneln.
- *6to4* wird eingesetzt, um IPv6-Datenpakete durch das IPv4-Internet zu transportieren. Das Problem bei 6to4 ist, dass keine NATs zwischen dem DirectAccess-Client und dem DirectAccess-Server liegen dürfen.
- *Teredo* wird eingesetzt, um IPv6-Datenpakete durch das IPv4-Internet zu tunneln, wenn zwischen dem DirectAccess-Client und dem DirectAccess-Server NATs existieren.

Kurz zur Erklärung des NAT-Szenarios: NAT bedeutet *Network Address Translation* und ist eine Technologie, die dann angewendet wird, wenn ein Client mit einer privaten IP-Adresse mit einem System im Internet kommunizieren möchte. Ein im DirectAccess-Umfeld typischer Fall ist auf Abbildung 13.4 skizziert:

- Der Client befindet sich im (privaten) Homeoffice-LAN eines Mitarbeiters. Vermutlich hat dieser einen einfachen DSL-Router, der die interne IP-Adresse des Clients in die öffentliche IP-Adresse des Routers umsetzt.
- Die Komponenten des Homeoffice-LANs müssen übrigens von IPv6 nichts wissen, da die Tunnelung bereits auf dem DirectAccess-Client erfolgt.

In diesem Szenario muss Teredo verwendet werden, 6to4 ist nicht NAT-fähig. Durch Nutzung von Teredo kann es aber problemlos eingesetzt werden.

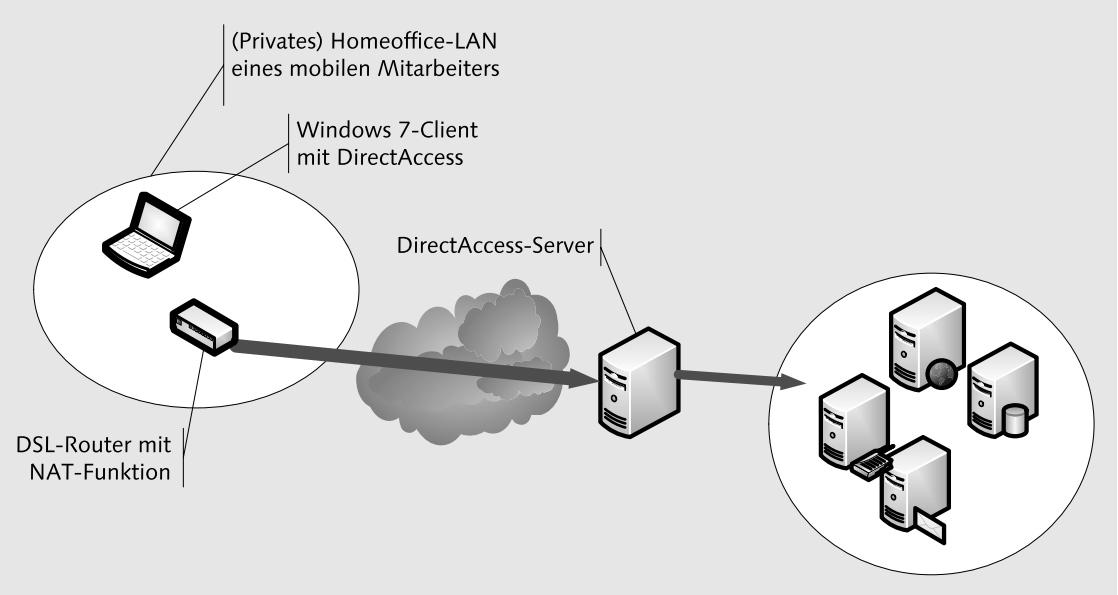


Abbildung 13.4 DirectAccess verträgt NAT-Komponenten auf dem Übertragungsweg zwischen dem DirectAccess-Client und dem DirectAccess-Server.

Der DirectAccess-Client ermittelt den zu verwendenden Tunnelmechanismus automatisch. Sofern 6to4 und Teredo nicht funktionieren, wird *IP-HTTPS* verwendet, was allerdings unter Performance-Gesichtspunkten ungünstiger ist.

Beim IPv6-Tunneling muss der Client natürlich wissen, wohin, also zu welchem IPv4-System, die Pakete getunnelt werden sollen. Dies wird in der Konfiguration der jeweiligen Tunnelmethode festgelegt. Auf Abbildung 13.5 ist zu erkennen, dass das »Ziel« des Tunnels die eine öffentliche IP-Adresse des DirectAccess-Servers ist. Die Konfiguration erfolgt über eine Gruppenrichtlinie, die die DirectAccess-Konfigurationsanwendung automatisch erzeugt.

Abbildung 13.5 Das Relay für die IPv6-Tunnelmechanismen wird durch eine Gruppenrichtlinie konfiguriert.

IPSec

Die Datenübertragung durch das Internet erfolgt geschützt mittels IPSec (*Internet Protocol Security*). Es ist ein Sicherheitsprotokoll für die Kommunikation über IP-Netze und gewährleistet Vertraulichkeit, Authentizität und Integrität. IPSec arbeitet auf der Vermittlungsschicht des TCP/IP-Protokollstacks.

Für die IPSec-Authentifizierung werden bei der Verwendung mit DirectAccess Zertifikate verwendet, weshalb eine eigene PKI (*Public Key Infrastructure*) zwingend erforderlich ist.

Man könnte über IPSec viele hundert Seiten schreiben – das möchte ich hier aber nicht tun, da die notwendigen Richtlinien durch den DirectAccess-Installationsassistenten erzeugt werden.

Namensauflösung und NRPT

Namen von internen (also im LAN stehenden) Servern müssen notwendigerweise von einem internen DNS-Server aufgelöst werden. Für den Zugriff auf externe Ressourcen kann prinzipiell jeder beliebige im Internet stehende DNS-Server verwendet werden. Das bedeutet, dass je nach angefragtem Namen unterschiedliche DNS-Server verwendet werden müssen. Vor Windows 7 wäre diese Herausforderung nicht zu bewältigen gewesen – das neue Betriebssystem löst dies über NRPT (*Name Resolution Policy Table*). NRPT ist, wie der Name ja auch schon vermuten lässt, eine Tabelle, die definiert, für welche Namensräume welcher DNS-Server befragt werden soll. Das Ergebnis sieht dann so aus wie auf Abbildung 13.6:

- Wird eine externe Ressource angefordert, wird der DNS-Server verwendet, der vom jeweiligen Internetprovider bzw. Mobilfunkanbieter vorgegeben wird.
- Wenn eine interne Ressource benötigt wird, wird die DNS-Anfrage über IPSec und den DirectAccess-Server an einen DNS-Server im Unternehmens-LAN geleitet.

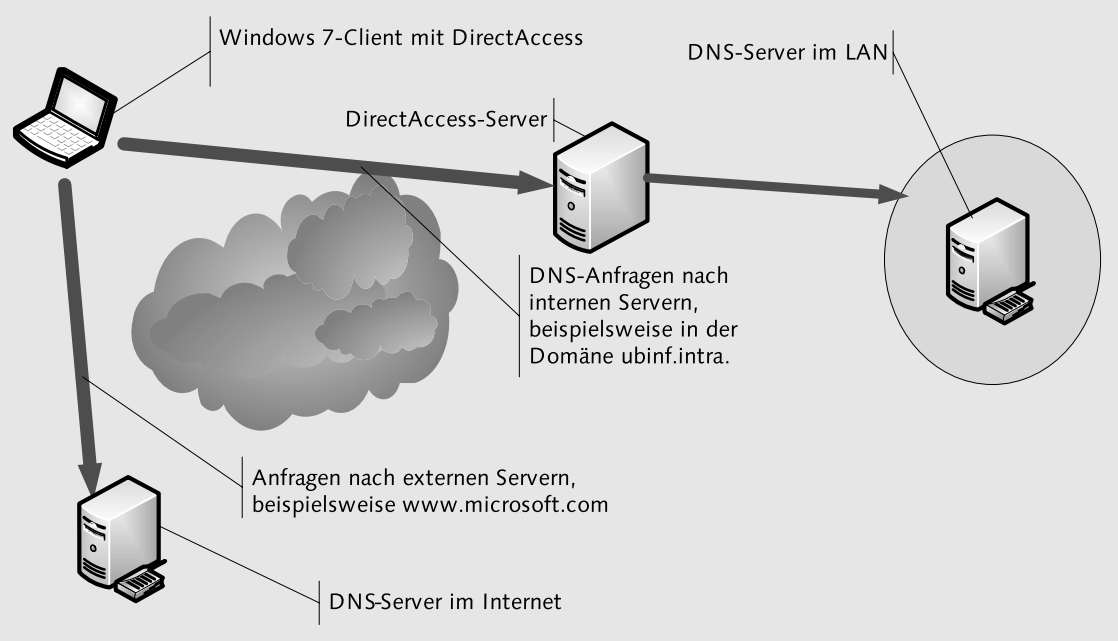


Abbildung 13.6 Namensauflösung mittels NRPT

Abbildung 13.7 zeigt, wie das Ganze auf einem Client aussieht. Mithilfe des Befehls `netsh name show pol` kann die NRPT ausgegeben werden. In diesem Fall ist konfiguriert, dass für Hosts im Namensraum *ubinf.intra* der DNS-Server *2002:a21e:…* verwendet werden soll.

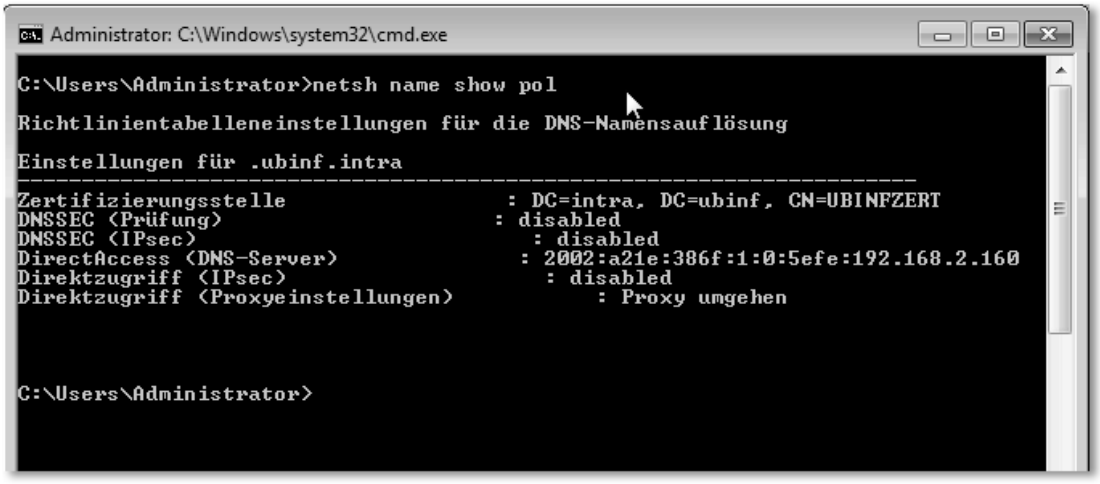


Abbildung 13.7 Die Anzeige der Name Resolution Policy Table (NRPT)

Nur außerhalb des LANs

Die Konfiguration gilt nur, wenn der Client sich außerhalb des Unternehmensnetzes befindet. Innerhalb des LANs wird die Namensauflösung »ganz normal« durchgeführt.

Eine wesentliche Komponente bei DirectAccess ist also die Fähigkeit, zu unterscheiden, ob sich der Client im LAN oder außerhalb befindet.

Network Location Server

Eine wirklich wichtige Fähigkeit eines DirectAccess-Clients ist es, zu erkennen, ob er sich im Unternehmens-LAN oder außerhalb desselben befindet. Dazu wird ein *Network Location Server* verwendet. Das hört sich deutlich komplizierter an, als es in Wirklichkeit ist. Als Network Location Server kann ein beliebiger im LAN stehender Webserver verwendet werden.

Ein DirectAccess-Client probiert beim Initialisieren der Netzwerkverbindung, ob der Network Location Server direkt erreicht werden kann (also ohne über den DirectAccess-Server zu gehen). Ist dies der Fall, befindet er sich also im Innenbereich des Netzes. Kann er den Network Location Server nicht direkt erreichen, versucht er es über den DirectAccess-Weg.

Vorraussetzungen

Der Network Location Server sollte auf einem hochverfügbaren Webserver installiert werden. Ist dieser Server nämlich nicht erreichbar, erkennen die DirectAccess-Clients nicht, dass sie sich im Innenbereich befinden, und versuchen einen Verbindungsaufbau über den DirectAccess-Server.

Der Network Location Server muss auf einen nicht authentifizierten Zugriff ohne Fehlermeldung antworten. Webapplikationen, die eine Benutzerauthentifizierung fordern (wie beispielsweise *SharePoint* oder *Outlook Web Access*) scheiden also aus. Nichtsdestotrotz könnte man natürlich auf einem hochverfügbaren SharePoint-NLB-Cluster eine weitere IIS-Website einrichten, die auf einen anonymen Zugriff mit »OK« antwortet.

Die Network-Location-Server-Website muss mit einem SSL-Zertifikat geschützt sein. Die Sperrliste der Zertifizierungsstelle muss für den im Internet befindlichen Client erreichbar sein, d. h. sich auf einem öffentlich zugänglichen Webserver befinden. Das ist nicht allzu kompliziert zu realisieren – aber ein weiterer Schritt, der erledigt werden muss.

Zertifikate

Die IPSec-Kommunikation beruht, zumindest bei DirectAccess, darauf, dass die Clients über Zertifikate authentifiziert werden. Sie benötigen dazu eine eigene ins Active Directory integrierte PKI (*Public Key Infrastructure*).

Wie ich bereits zuvor erwähnt habe, muss die Zertifikatssperrliste öffentlich erreichbar sein – das dürfte bei den meisten Unternehmens-PKIs derzeit nicht der Fall sein.

Hinweis

Den Aufbau einer eigenen PKI habe ich in Abschnitt 5.8, »Die Active Directory-Zertifikatdienste«, recht ausführlich erläutert.

13.2.3 Vorbereitende Maßnahmen

Bevor Sie tatsächlich mit der Installation des DirectAccess-Servers beginnen, gibt es etliche »Handgriffe«, die Sie im Vorfeld ausführen müssen.

Domänencontroller und DNS-Server

Sie brauchen in Ihrer Domäne mindestens einen DNS-Server, der auf einem Domänencontroller läuft. Der Versionsstand dieser Maschine muss *Windows Server 2008 SP2* oder *Windows Server 2008 R2* sein.

Auf dem DNS-Server entfernen Sie ISATAP von der *Global Query Block List,* und zwar mit folgendem Befehl:

```
dnscmd /config /globalqueryblocklist wpad
```

PKI einrichten

Sofern in Ihrem Unternehmen noch keine Zertifizierungsstelle vorhanden ist, müssen Sie eine einrichten, da Sie eine eigene PKI betreiben müssen. In Abschnitt 5.8 finden Sie eine recht ausführliche Beschreibung dazu.

Auch wenn Sie eine interne PKI betreiben, ist es durchaus möglich, dass Sie keinen öffentlich erreichbaren Sperrlisten-Verteilungspunkt eingerichtet haben. Um dies zu realisieren, gehen Sie wie folgt vor (Abbildung 13.8):

- Rufen Sie die Eigenschaften der Zertifizierungsstelle auf.
- Fügen Sie einen neuen Verteilungspunkt hinzu. Geben Sie die gewünschte HTTP-Adresse ein, und fügen folgende Variablen an: <CAName>, <CRLNameSuffix> und <DeltaCRLAllowed>. Wählen Sie die auf der Abbildung gezeigten Einstellungen.
- Wenn Sie die Sperrlisten automatisch veröffentlichen möchten, müssen Sie noch einen weiteren Verteilungspunkt anlegen, der über eine UNC-Adresse (*server**freigabe*) verfügt. Wählen Sie die Einstellung Sperrlisten an diesem Ort veröffentlichen, aktivieren Sie aber nicht die Einbeziehung des Verteilungspunkts in das Zertifikat.

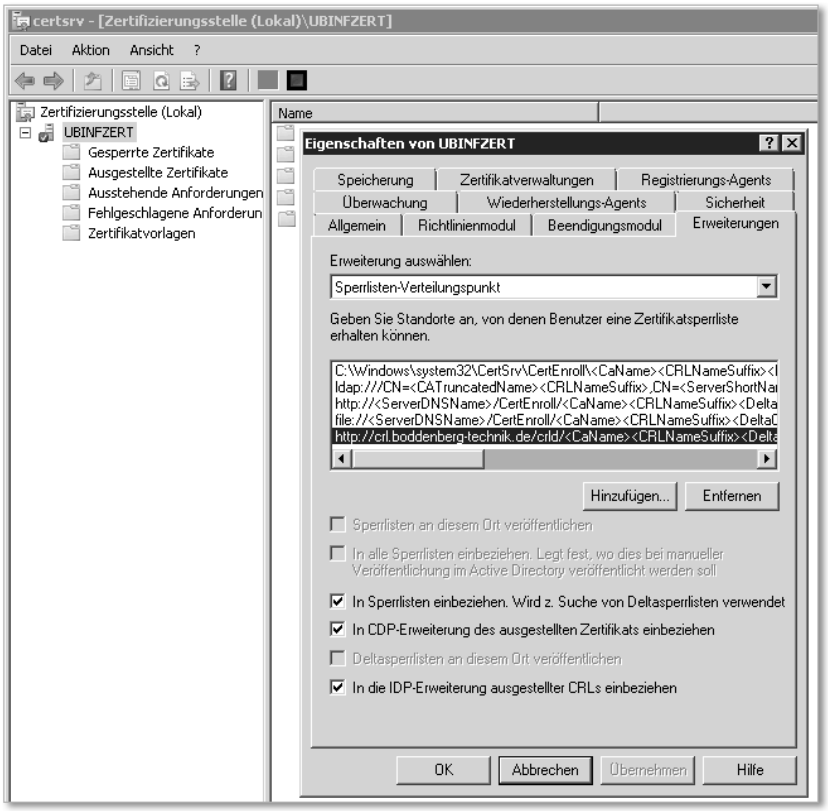


Abbildung 13.8 Sie müssen einen öffentlich erreichbaren Verteilungspunkt einrichten.

In den ausgestellten Zertifikaten ist der neue öffentlich verfügbare Sperrlisten-Verteilungspunkt eingetragen. Dies ist auf Abbildung 13.9 gezeigt.

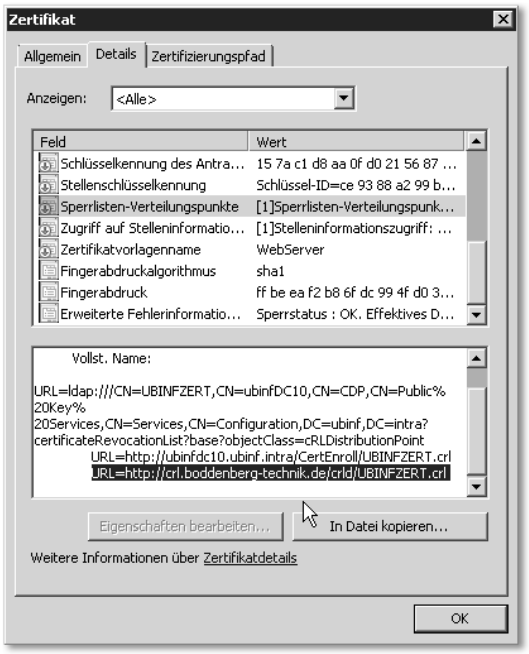


Abbildung 13.9 Zur Kontrolle: In den ausgestellten Zertifikaten ist der öffentliche Verteilungspunkt aufgeführt.

Verteilungspunkt für Zertifikatssperrliste anlegen

Die Zertifikatssperrliste muss nun noch auf einem Webserver veröffentlicht werden. Dies ist schnell erledigt. Abbildung 13.10 zeigt den »Sollzustand« bei Verwendung eines IIS7:

- Rufen Sie den *Internetinformationsdienste-Manager* auf.
- Wählen Sie die Website aus, die die Sperrliste enthalten soll.
- Legen Sie ein neues virtuelles Verzeichnis an.
- Konfigurieren Sie, dass das Durchsuchen des Verzeichnisses zulässig ist.
- Gestatten Sie anonymen Zugriff.

Sofern die Zertifizierungsstelle automatisch die Sperrlisten in das virtuelle Verzeichnis kopieren soll, müssen Sie entsprechende Dateisystemberechtigungen setzen.

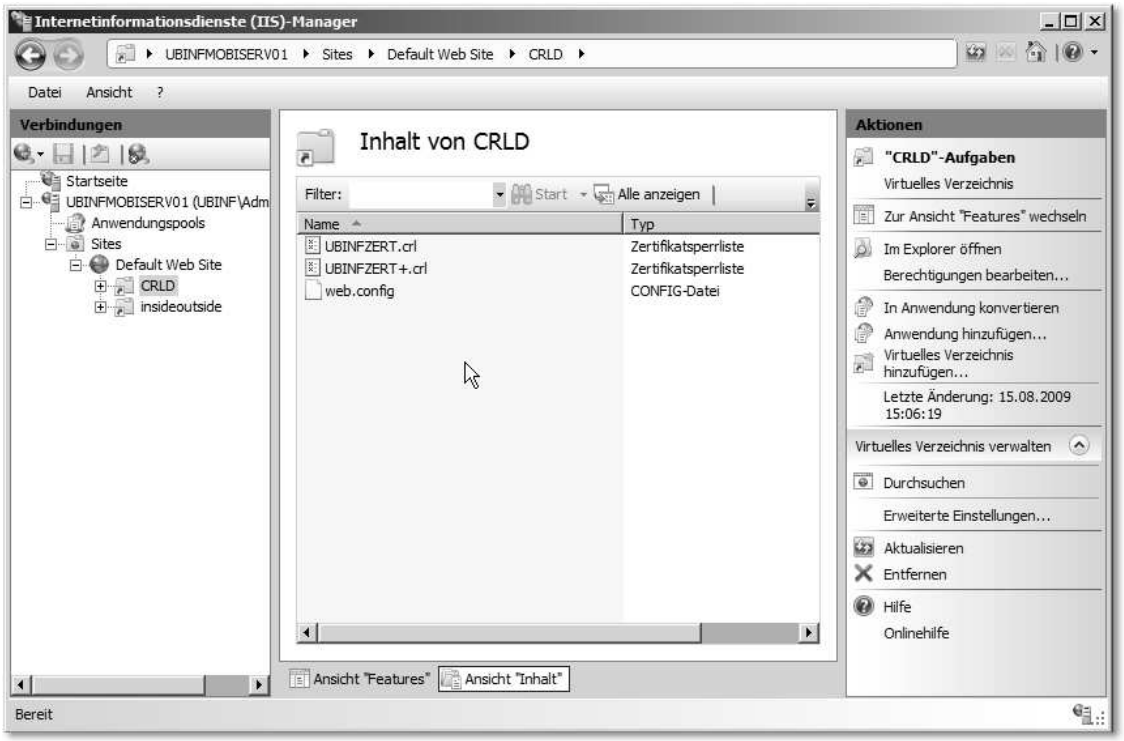


Abbildung 13.10 So muss ein mit dem IIS erzeugter Verteilungspunkt für die Zertifikatssperrliste aussehen.

Besser intelligent

Es ist nach heutigen Maßstäben keine gute Idee, den Webserver direkt in die DMZ zu stellen und nur mit einem Portfilter zu schützen. Besser ist die Veröffentlichung mit intelligenten Systemen wie dem *Microsoft ISA Server*.

Zertifikate anfordern und Auto Enrollment für Zertfikate

Die beteiligten Clients und der DirectAccess-Server benötigen Computerzertifikate. Diese dienen zur sicheren Authentifizierung des Computers beim Aufbau der IPSec-Verbindung.

Sie haben grundsätzlich zwei Möglichkeiten, um das Zertifikat auf die Systeme zu bekommen:

- Sie installieren es per Hand (wie nachfolgend gezeigt wird).
- Sie konfigurieren das *Auto Enrollment* des Zertifikats. Ist dies geschehen, holen sich die Clients selbstständig ein Computerzertifikat und erneuern dies, sobald das notwendig wird.

In den folgenden beiden Abschnitten führe ich Ihnen beide Varianten vor.

Zertifikat manuell anfordern

Um ein Computerzertifikat manuell anzufordern, gehen Sie wie folgt vor:

- Öffnen Sie die *Microsoft Management Console* (MMC).
- Fügen Sie das Snap-In ZERTIFIKATE hinzu.
- Wählen Sie den Zugriff auf den Zertifikatspeicher des Computers.
- Rufen Sie im Kontextmenü des Knotens EIGENE ZERTIFIKATE den Menüpunkt NEUES ZERTIFIKAT ANFORDERN auf (Abbildung 13.11).

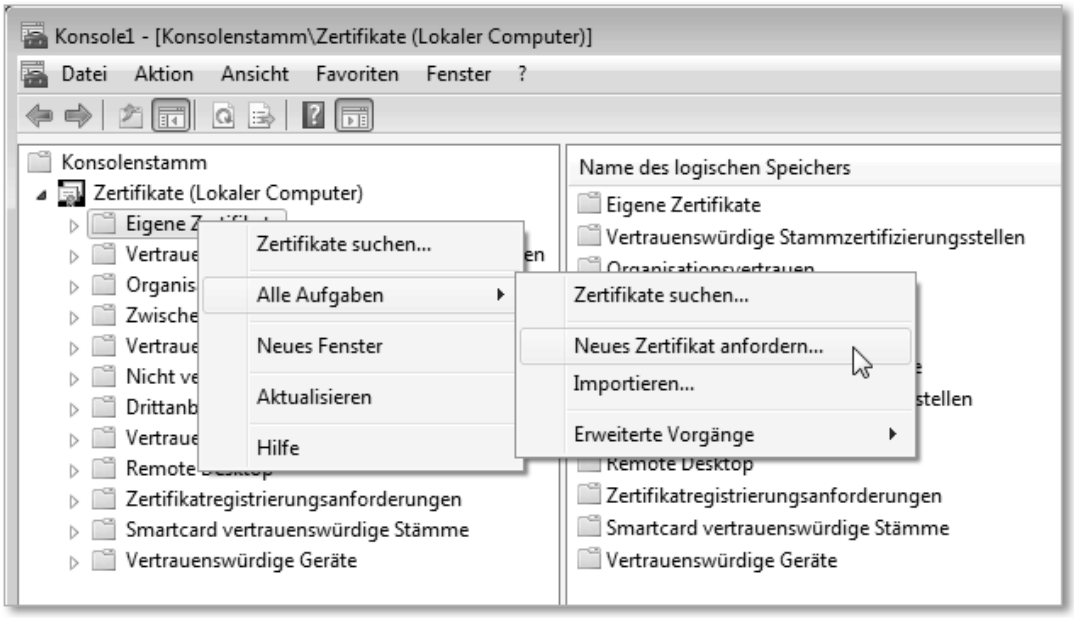


Abbildung 13.11 Im Zertifikate-Snap-In kann ein neues Zertifikat angefordert werden.

- Es startet ein Assistent, der Ihnen die Active Directory-Registrierungsrichtlinien anzeigt. Wählen Sie dort den Punkt COMPUTER, um ein Computerzertifikat anzufordern (Abbildung 13.12).
- Wenn die Zertifizierungsstelle für die automatische Ausstellung von Zertifikaten konfiguriert ist, wird Ihr Zertifikat binnen weniger Sekunden ausgestellt und im Zertifikatspeicher des Computers vorhanden sein.

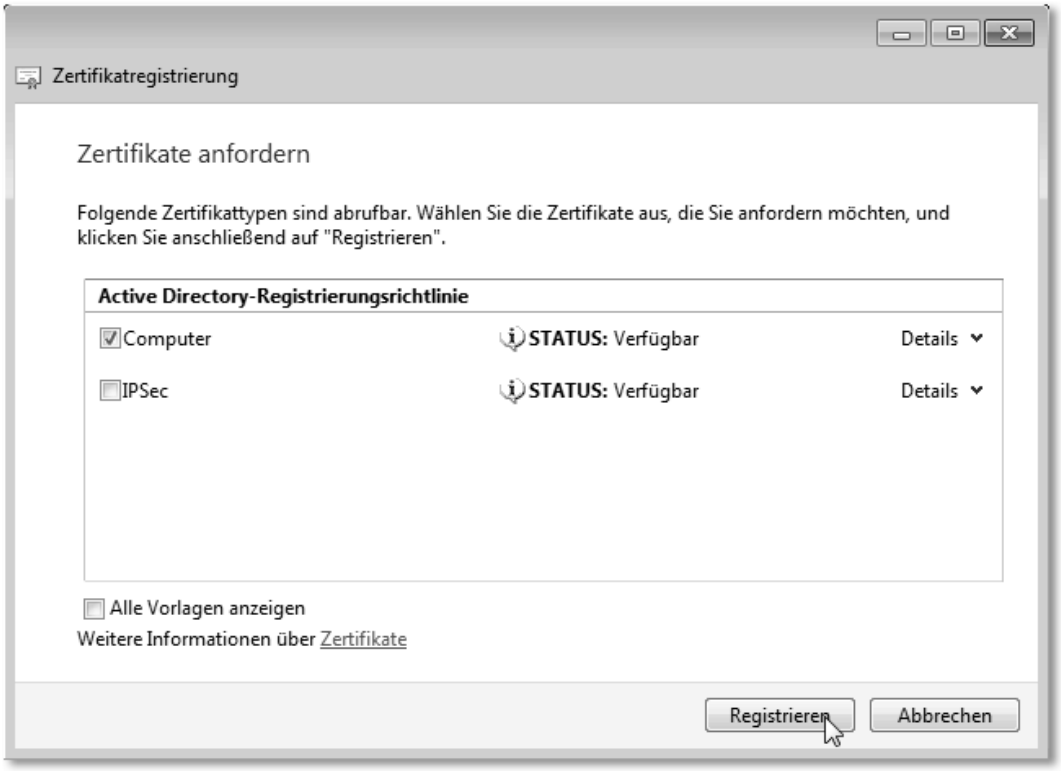


Abbildung 13.12 Es wird ein Zertifikat vom Typ »Computer« benötigt.

Auto Enrollment

Wenn Sie nicht nur über einige wenige Systeme verfügen, ist die automatische Zertifikatanforderung (*Auto Enrollment*) eine feine Angelegenheit. Die Clients fordern dann selbstständig ein Zertifikat an. Sofern es abläuft und erneuert werden muss, wird die Anforderung ebenfalls automatisch durchgeführt. Auto Enrollment ist mittels einer Gruppenrichtlinie schnell konfiguriert:

- Legen Sie ein neues Gruppenrichtlinien-Objekt an. Da in Zukunft sämtliche Computer Ihres Unternehmens bzw. Ihrer Organisation ein Computerzertifikat brauchen werden, kann das Gruppenrichtlinienobjekt direkt mit der Domäne verknüpft werden.
- Navigieren Sie zum Knoten COMPUTERKONFIGURATION • RICHTLINIEN • WINDOWS-EINSTELLUNGEN • SICHERHEITSEINSTELLUNGEN • RICHTLINIEN FÜR ÖFFENTLICHE SCHLÜSSEL • EINSTELLUNGEN DER AUTOMATISCHEN ZERTIFIKATSREGISTRIE-

RUNG, und wählen Sie im dortigen Kontextmenü die Erstellung einer neuen AUTOMATISCHEN ZERTIFIKATANFORDERUNG (Abbildung 13.13).

- Wählen Sie aus den zur Verfügung stehenden Zertifikatvorlagen diejenige mit der Bezeichnung COMPUTER (Abbildung 13.14).

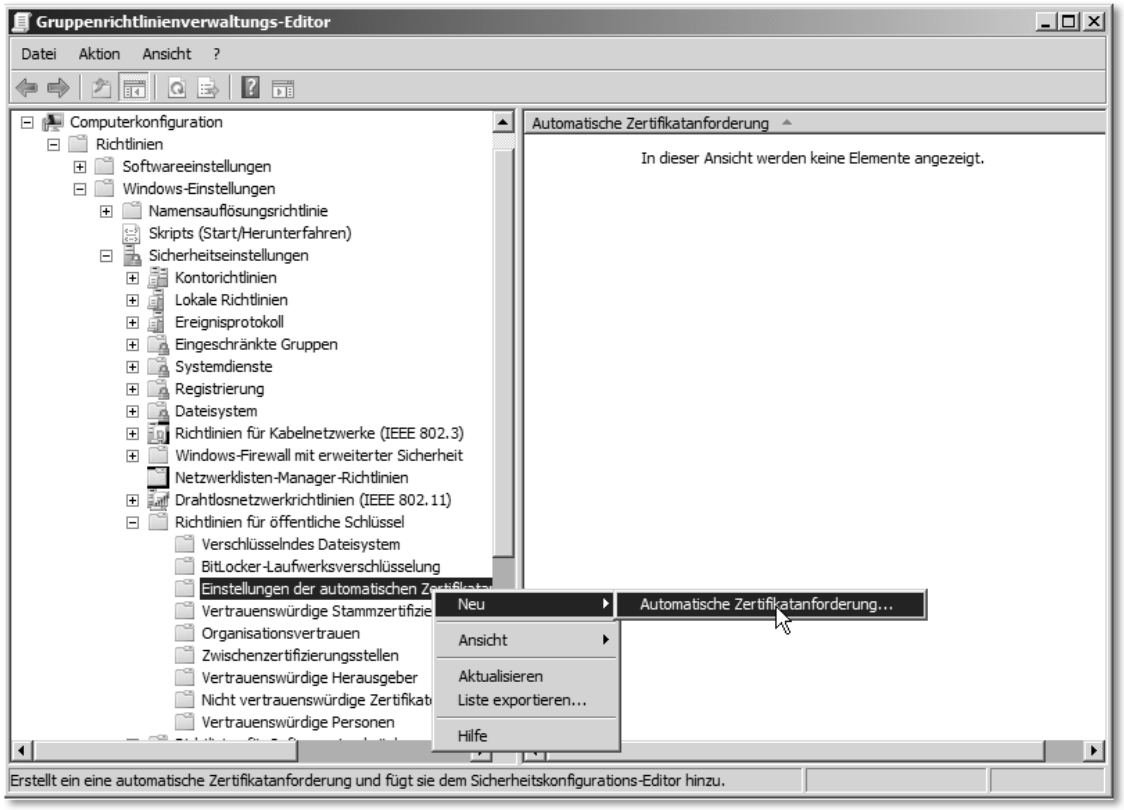


Abbildung 13.13 Zum automatischen Ausrollen des Zertifikats wird eine Gruppenrichtlinie zur »Automatischen Zertifikatanforderung« konfiguriert.

Abbildung 13.14 Ein Computerzertifikat soll automatisch angefordert werden.

Damit ist das Auto Enrollment konfiguriert. Sie können die Ausführung der Richtlinie mit dem Befehl `gpupdate /force` erzwingen. Im Zertifikatspeicher des Computers sollte direkt ein entsprechendes Zertifikat vorhanden sein.

Sicherheitsgruppe anlegen

Nicht jeder Client ist automatisch zur Nutzung von DirectAccess berechtigt. Die Berechtigungssteuerung erfolgt über die Mitgliedschaft in einer Sicherheitsgruppe.

Legen Sie also eine Sicherheitsgruppe an, in der die Computer Mitglied werden, die Berechtigungen erhalten sollen. Falls es für Sie übersichtlicher zu administrieren ist, können Sie auch mit mehreren Gruppen arbeiten.

IP-Konfiguration der Server aktualisieren

Im nächsten Schritt müssen Sie die IP-Konfiguration aller Server anpassen, auf die DirectAccess-Clients zugreifen sollen. Auch wenn auf den Servern IPv6 aktiviert ist, haben diese keine ISATAP-Adresse. Eine solche wird aber für den Zugriff über den IPSec-Tunnel benötigt.

Durch die Eingabe von `sc control iphlpsvc paramchange` wird dem Server gestattet, sich selbst als ISATAP-Host zu konfigurieren. Auf Abbildung 13.15 sehen Sie die durch diesen Befehl bewirkten Änderungen.

Wenn alles korrekt funktioniert, registrieren die Server, die durch den zuvor genannten Befehl als ISATAP-Host konfiguriert worden sind, einen zweiten DNS-Eintrag. Auf Abbildung 13.16 sehen Sie, dass *ubinfMobiServ01* und *ubinfNAP* im DNS über einen IPv4- und einen IPv6-Eintrag verfügen. *ubinfMOSS01* ist nicht als ISATAP-Host konfiguriert und ist demzufolge im DNS nur mit der IPv4-Adresse verzeichnet.

Hinweis

Ein Hinweis zur Vermeidung von Missverständnissen: Sie brauchen die IPv6-Einträge nicht manuell vorzunehmen; die Server sollten diese selbst anlegen. Sofern das nicht funktioniert, sollten Sie die DNS-Konfiguration überprüfen.

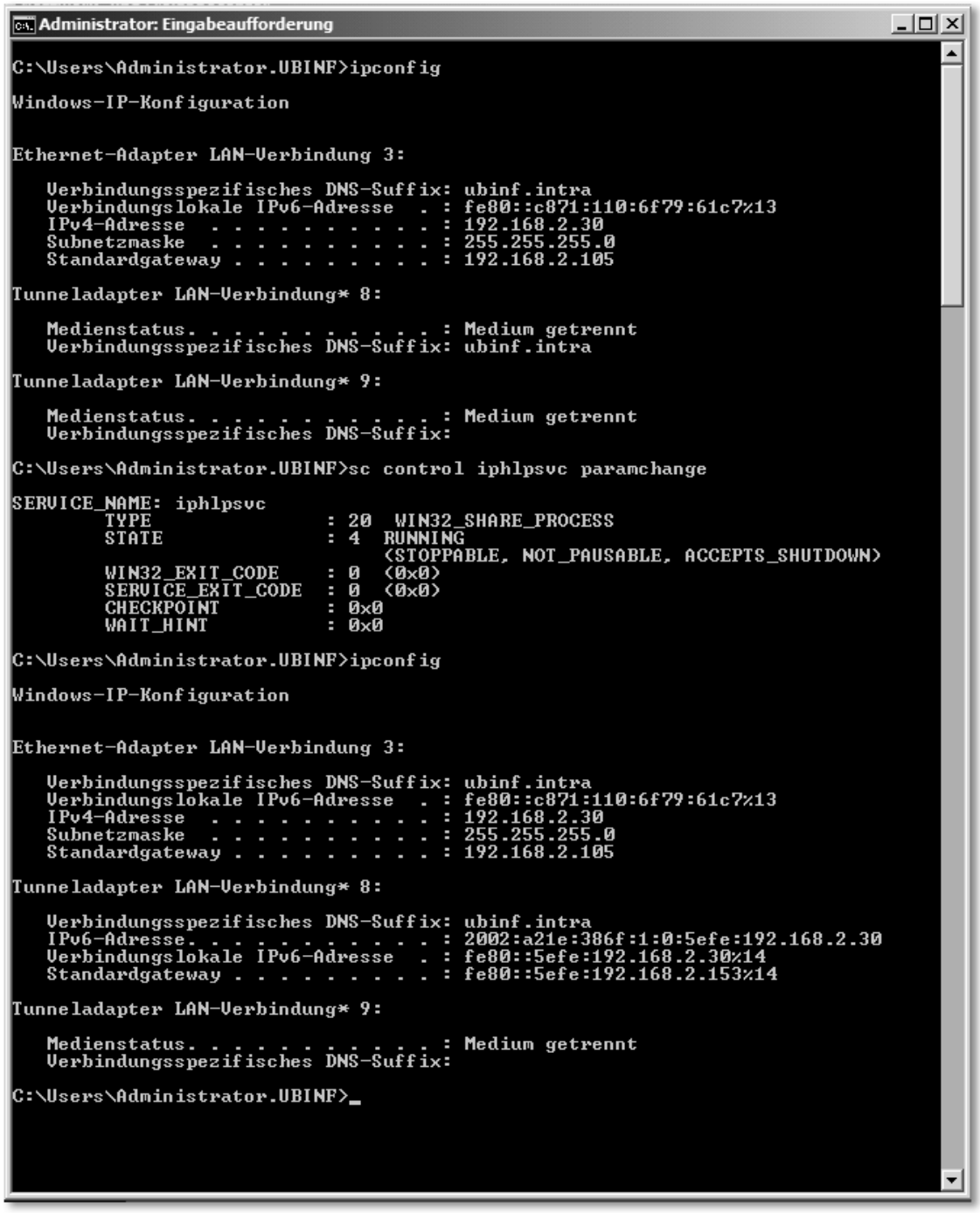


Abbildung 13.15 Aktualisieren der IP-Konfiguration, um die ISATAP-Adresse hinzuzufügen

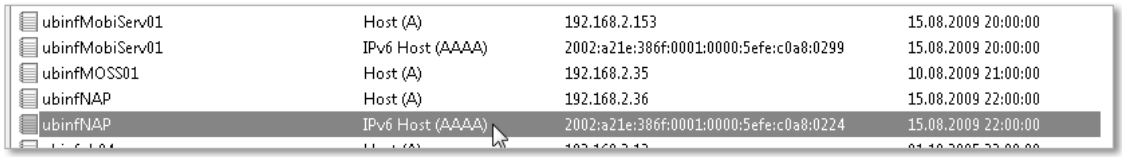


Abbildung 13.16 Als ISATAP-Host konfigurierte Server sollten zwei DNS-Einträge haben.

IPv6- und IPv4-ICMP-Anforderungen zulassen

In diesem Schritt geht es darum, ICMP-Anforderungen (inbesondere PING für IPv4 und IPv6 zuzulassen. Beim DirectAccess-Server ist dies notwendig, weil ansonsten das Teredo-Tunneling-Protokoll nicht funktioniert. Sie können nun entscheiden, ob Sie diese Einstellung direkt in der Windows-Firewall des DirectAccess-Servers vornehmen oder aber per Gruppenrichtlinie konfigurieren.

Da es in der Einführungsphase recht praktisch ist, verschiedene Maschinen anpingen zu können, ist die Variante der Verteilung über Gruppenrichtlinien nicht uninteressant, um alle oder zumindest bestimmte Gruppen von Systemen dazu zu bringen, auf Ping-Anforderungen zu antworten.

Wenn Sie sich für die Gruppenrichtlinienvariante entscheiden, sehen Sie auf Abbildung 13.17, wo sich die entsprechende Einstellung findet. Mit dem Menüpunkt Neue Regel starten Sie den Assistenten, den Sie bereits aus Abschnitt 12.4.5, »Eine Regel selbst erstellen«, kennen.

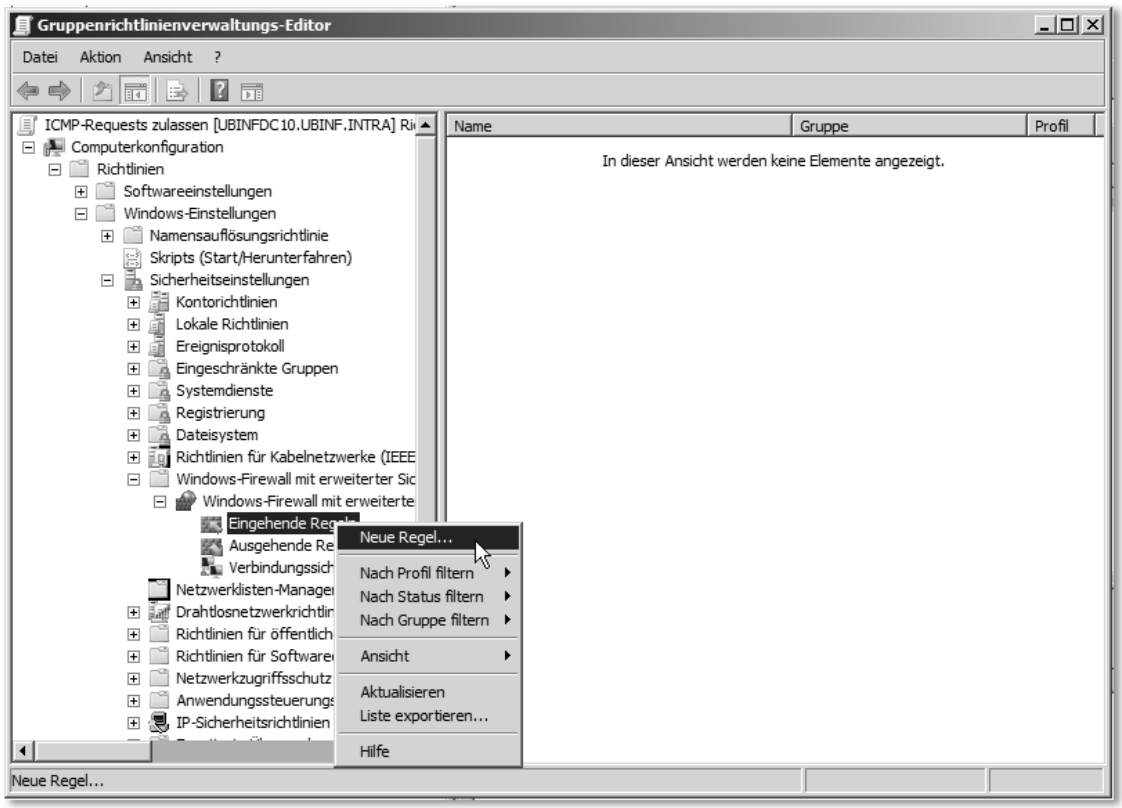


Abbildung 13.17 Erstellen einer Gruppenrichtlinie zum Hinzufügen einer Firewall-Regel

Um ICMP-Anforderungen zuzulassen, wählen Sie die Erstellung einer benutzerdefinierten Regel, legen die Gültigkeit für alle Programme fest und wählen dann als Protokolltyp ICMPv6 bzw. ICMPv4 aus (Abbildung 13.18). Mit der Schaltflä-

che Anpassen gelangen Sie zu einem Dialog, mit dem Sie die einzelnen Funktionen des ICMP-Protokolls separat aktivieren und deaktivieren können.

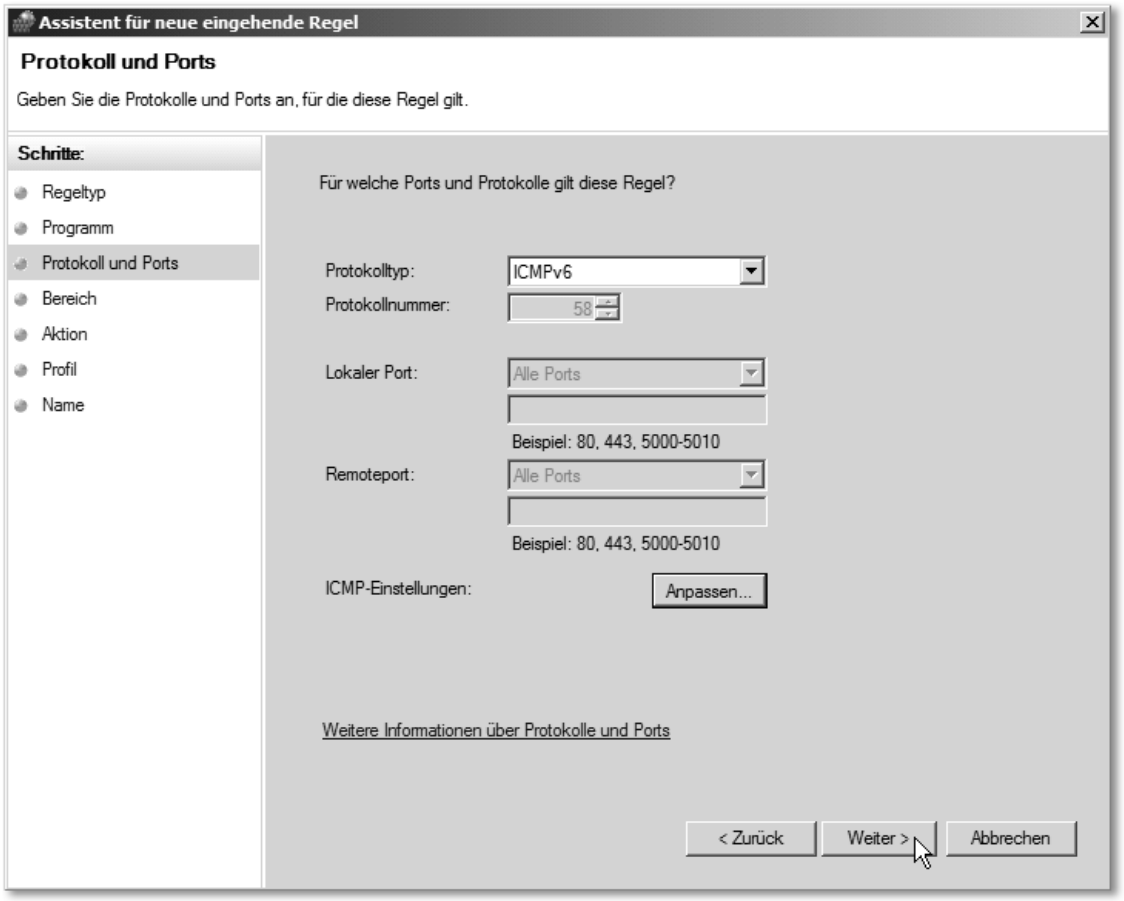


Abbildung 13.18 Zulassen von ICMPv6

Network Locator Server vorbereiten

Der *Network Locator Server* ist, trotz des spannenden Namens, vermutlich die am wenigsten komplizierte Komponente in der gesamten DirectAccess-Landschaft. Dieser Server muss ein Webserver im Innenbereich sein, der auf eine anonyme Anfrage eines Webclients Daten liefert. Die Webanwendung kann beliebig sein, sie muss lediglich mit einer OK-Meldung (Statuscode 200) antworten. *SharePoint* oder *Outlook Web Access*, die im Normalfall im Intranet eine Windows-Authentifizierung verlangen, sind nicht geeignet.

Der Network Location Server sollte hochverfügbar ausgelegt sein, er muss jederzeit verfügbar sein, und zwar von allen Standorten Ihres Unternehmens aus. Empfehlenswert ist also die Ausführung auf einem NLB-Cluster (*Network Load Balancing*).

Weiterhin muss die als Network Location Server vorgesehene Webanwendung mit einem gültigen Zertifikat ausgestattet sein.

DirectAccess-Server vorbereiten

Nun geht es an die Vorbereitung des DirectAccess-Servers. Hier nochmals die Voraussetzungen:

- Das Betriebssystem muss Windows Server 2008 R2 sein.
- Der Server muss über zwei Netzwerkkarten verfügen, eine externe und eine interne. Benennen Sie die Netzwerkadapter entsprechend. Wenn diese *Adapter 1* und *Adapter 2* heißen, ist die Zuordnung bei den nächsten Schritten unübersichtlich.
- Die externe Netzwerkkarte muss über zwei aufeinanderfolgende öffentliche IP-Adressen verfügen. Diese öffentlichen IP-Adressen müssen geroutet sein, mit genatteten IP-Adressen funktioniert es nicht (Abbildung 13.19).
- Auf der Registerkarte DNS der TCP/IP-Einstellungen der internen Netzwerkkarte muss das primäre DNS-Suffix eingetragen werden.

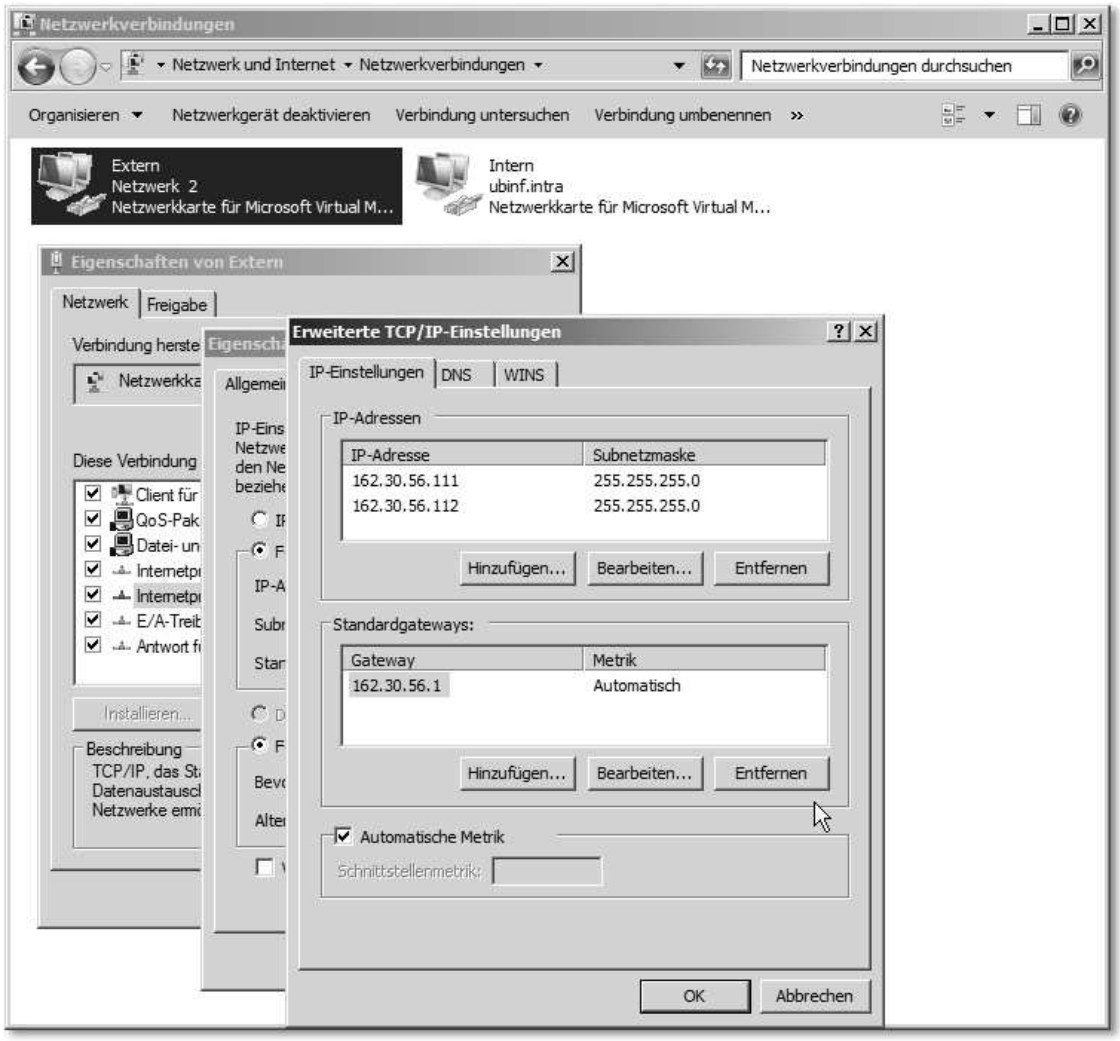


Abbildung 13.19 Die IP-Konfiguration des DirectAccess-Servers. Benötigt werden zwei aufeinanderfolgende öffentliche IP-Adressen.

Wichtig ist, dass die Netzwerkkarten den richtigen Netzwerkstandorten zugeordnet sind. Im NETZWERK- UND FREIGABECENTER muss sich in etwa das Szenario aus Abbildung 13.20 ergeben.

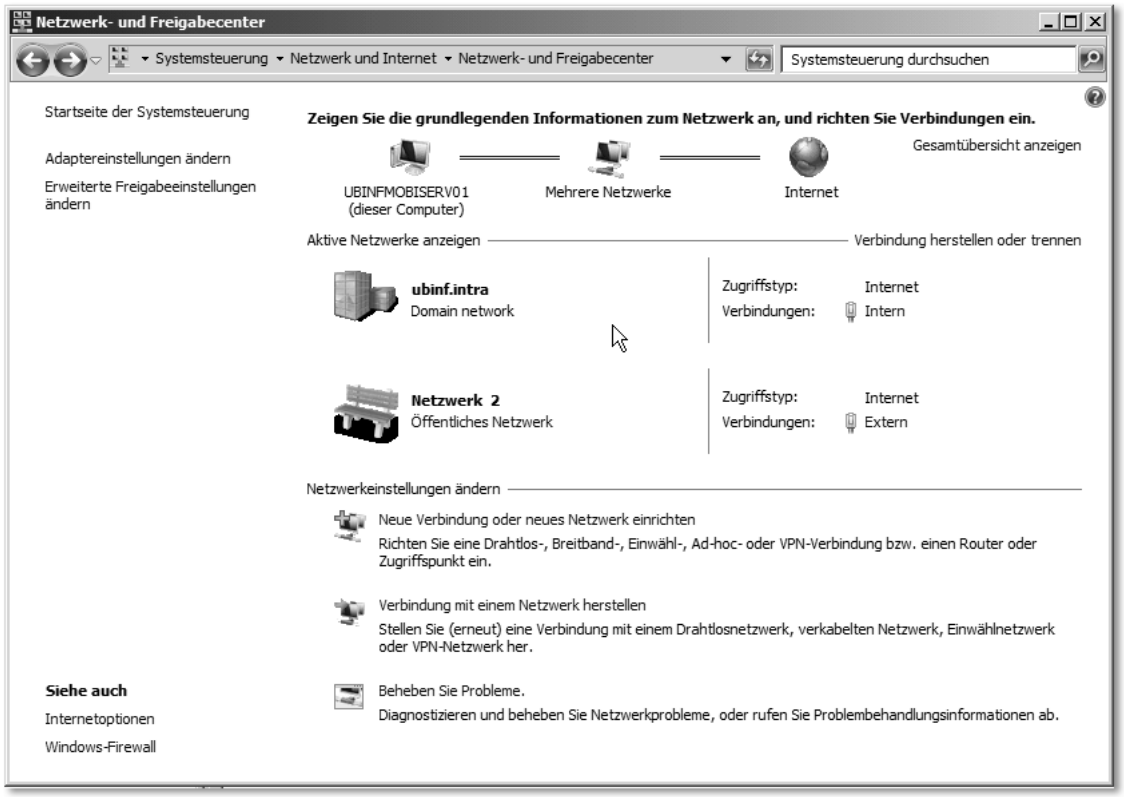


Abbildung 13.20 Die Netzwerkstandorte müssen korrekt zugeordnet sein.

Wenn die Netzwerkkonfiguration in Ordnung ist, fordern Sie noch ein Zertifikat mit dem öffentlichen Namen des Servers an, beispielsweise *da.boddenberg-technik.de*. Über diese URL wird die Verbindung über IP-HTTPS versucht, wenn die Benutzung der Tunneling-Protokolle 6to4 und Teredo nicht möglich ist.

Das Zertifikat für den internen Namen wird durch die zuvor konfigurierte Gruppenrichtlinie angefordert und installiert.

13.2.4 DirectAccess installieren und einrichten

Nach langen Vorbereitungen geht es nun – endlich – an die eigentliche Installation von DirectAccess.

DirectAccess-Verwaltungskonsole installieren

Der erste Schritt ist die Installation des Features DIRECTACCESS-VERWALTUNGSKONSOLE. Außerdem benötigen Sie das Feature GRUPPENRICHTLINIENVERWAL-

TUNG. Diesen Schritt führen Sie wie gewohnt mit dem Server-Manager durch (Abbildung 13.21).

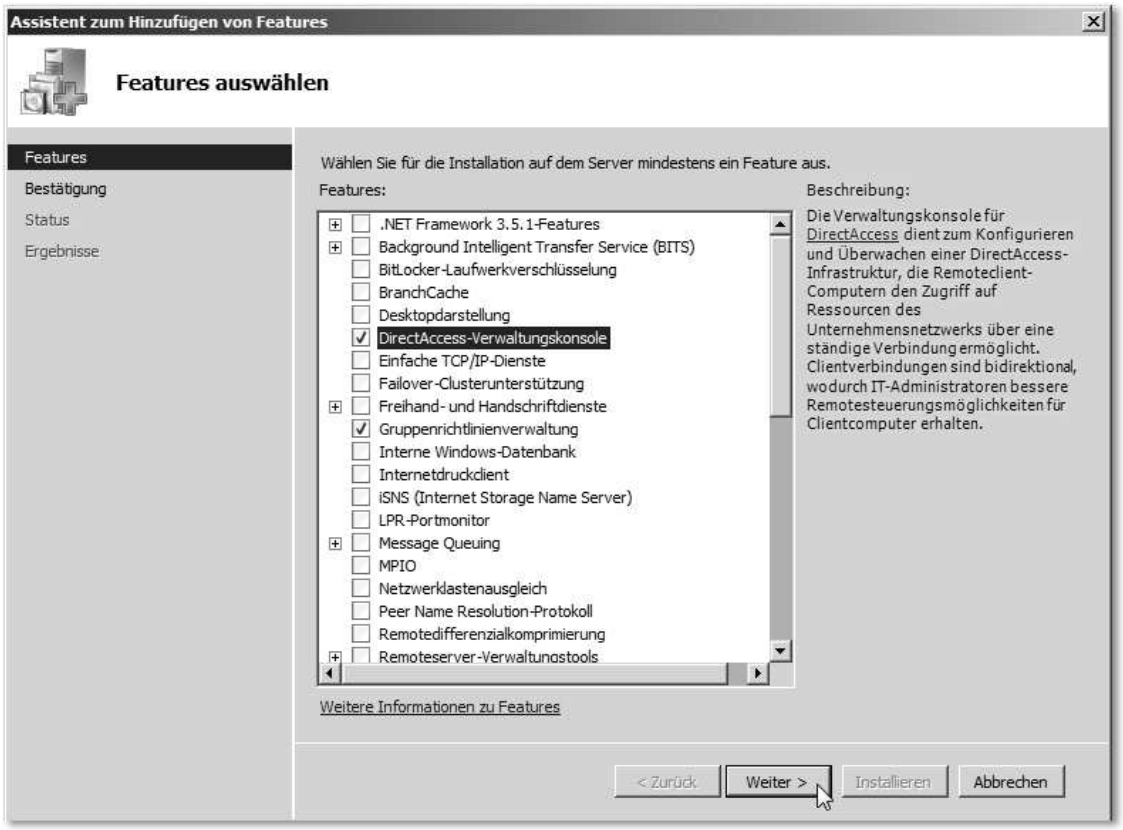


Abbildung 13.21 Der erste Schritt ist das Hinzufügen der DirectAccess-Verwaltungskonsole. Weiterhin wird die Gruppenrichtlinienverwaltung benötigt.

Ersteinrichtung mit der DirectAccess-Verwaltungskonsole

Wenn Sie die DirectAccess-Verwaltungskonsole starten, sehen Sie die Skizze aus Abbildung 13.22. Das sieht nun zunächst so aus, als ob nur Schritt 1, Schritt 2, Schritt 3 und Schritt 4 ausgeführt werden müssten – ziemlich einfach, oder?

Wenn alle Vorbereitungsmaßnahmen richtig durchgeführt worden sind, müssen Sie in der Tat jetzt nicht mehr tun, als vier Schritte zu durchlaufen, *aber*: Erfahrungsgemäß gibt es bei so vielen durchzuführenden Schritten noch immer einen kleinen Bug.

Schritt 1: Remoteclients

Der erste Schritt ist nun wirklich simpel durchzuführen: Sie müssen lediglich eine oder mehrere Gruppen auswählen, in der bzw. denen die für DirectAccess berechtigten Computer Mitglied sind (Abbildung 13.23).

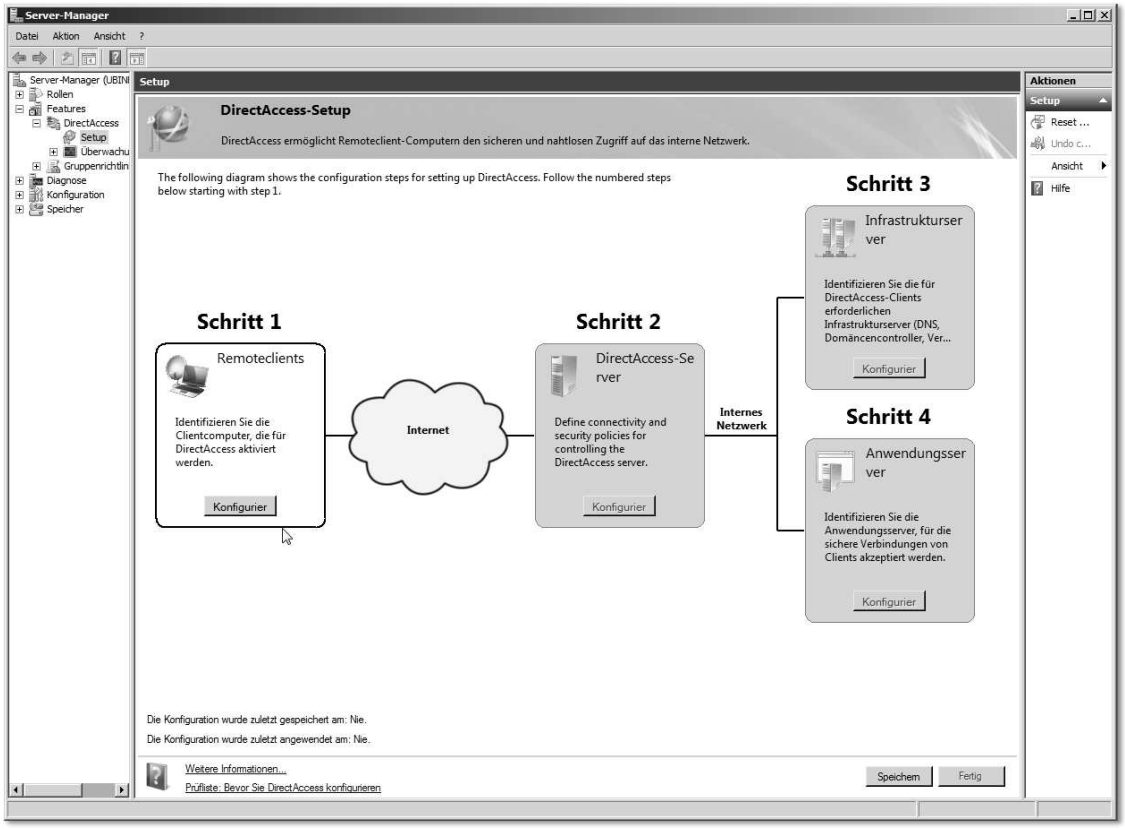


Abbildung 13.22 Die DirectAccess-Konfiguration erfolgt mit diesem Werkzeug.

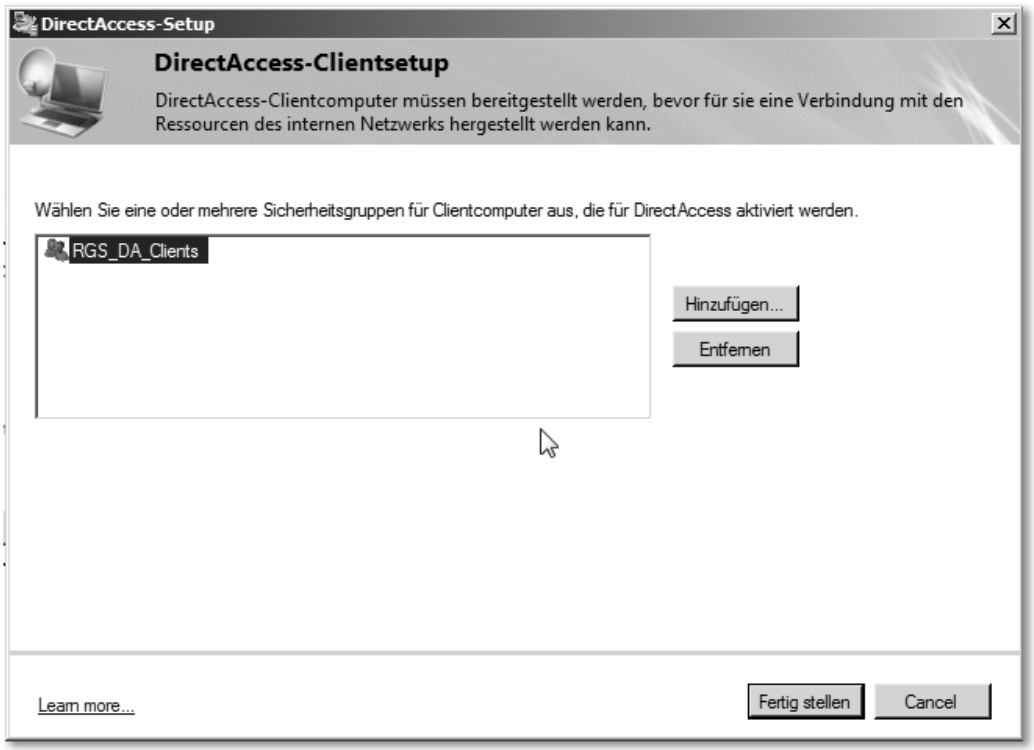


Abbildung 13.23 Tragen Sie hier die Gruppen ein, die die PCs enthalten, die Zugriff per DirectAccess erhalten sollen.

Schritt 2: DirectAccess-Server

Im zweiten Schritt geht es um die Konfiguration des DirectAccess-Servers. Auf der ersten Dialogseite legen Sie fest, welche Netzwerkschnittstelle die interne und welche die externe ist (Abbildung 13.24). In diesem Dialog werden die zuvor festgelegen Namen der Netzwerkadapter angezeigt – ich habe diese INTERN und EXTERN genannt. Jetzt wäre es ziemlich blöd, wenn die Namen NETZWERKADAPTER 1 und NETZWERKADAPTER 2 lauteten.

Weiterhin können Sie festlegen, dass für Remotebenutzer eine Smartcard-Authentifizierung erforderlich ist.

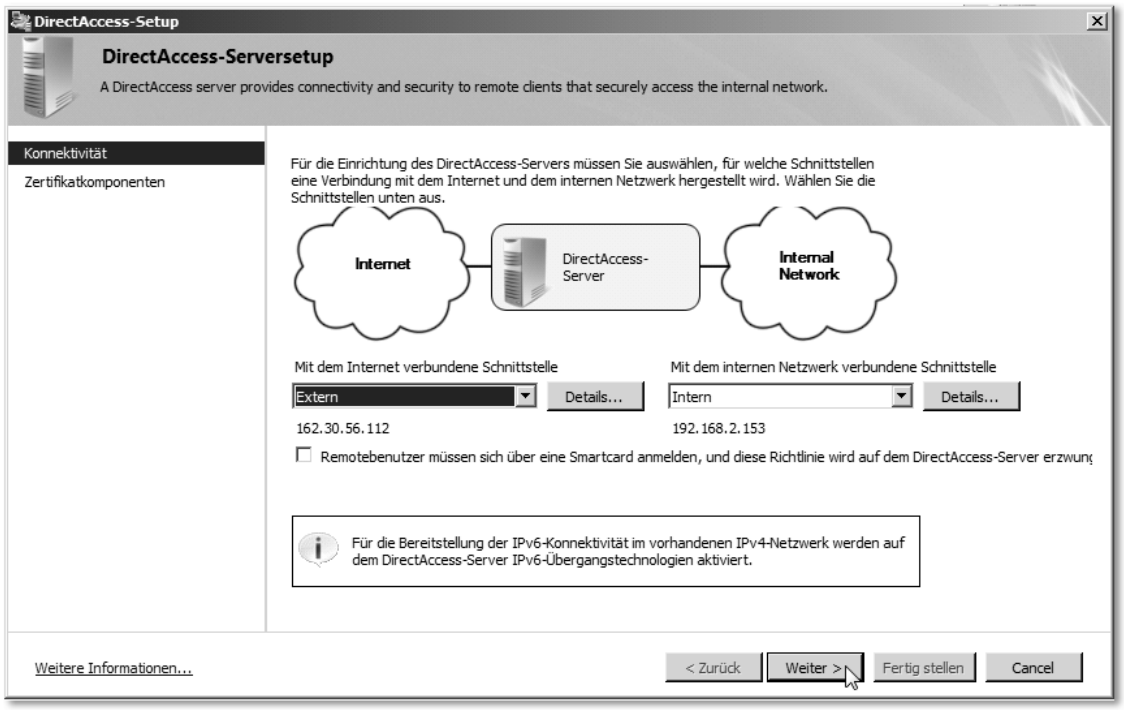


Abbildung 13.24 Legen Sie die Netzwerkschnittstellen für das Internet und den internen Zugriff fest.

Auf der zweiten Dialogseite dieses Konfigurationsabschnitts wählen Sie die zu verwendenden Zertifikate (Abbildung 13.25):

- Zunächst wählen Sie das Stammzertifikat aus.
- Dann wählen Sie das Zertifikat aus, das verwendet wird, wenn über IP-HTTPS auf den Server zugegriffen wird (diese Option wird gewählt, wenn über die Tunnelmechanismen eine Verbindung nicht möglich ist). Dieses Zertifikat für die externe Kommunikation ist in einem der vorherigen Schritte auf dem DirectAccess-Server installiert worden.

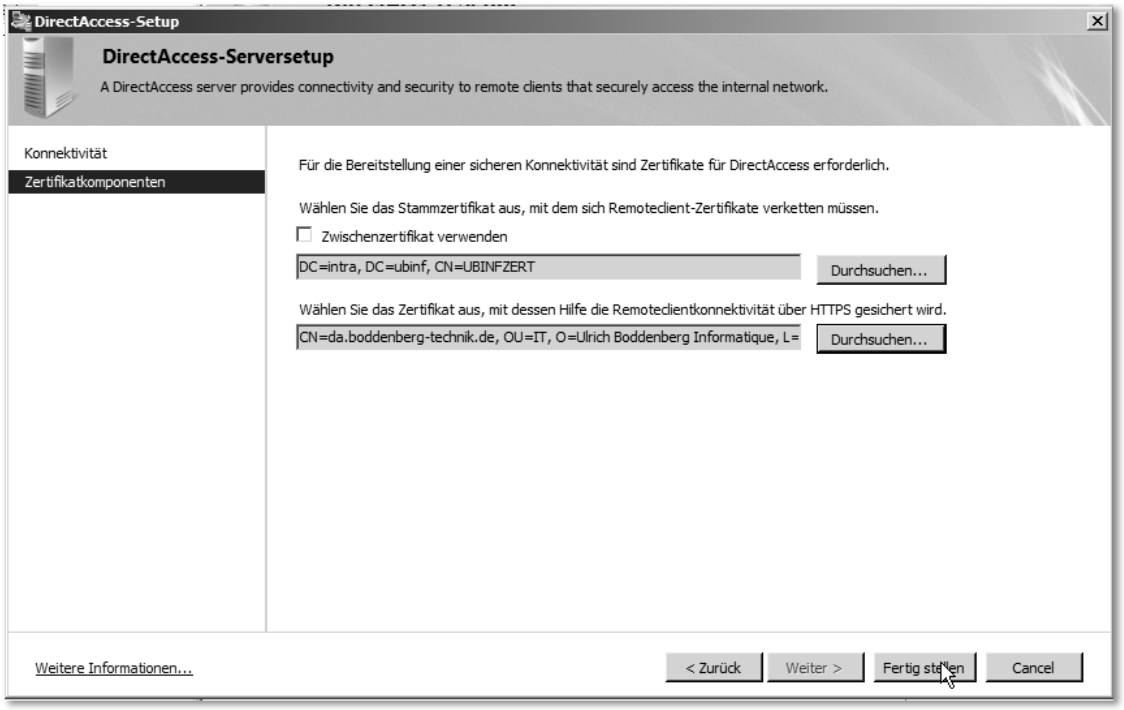


Abbildung 13.25 Auswahl der Zertifikate, die auf dem DirectAccess-Server verwendet werden sollen

Schritt 3: Infrastrukturserver

Im dritten Schritt konfigurieren Sie die Infrastrukturserver.

Der erste Konfigurationsdialog dieses Abschnitts beschäftigt sich mit dem *Network Location Server* (Abbildung 13.26). Hier haben Sie zwei Möglichkeiten:

- Die empfohlene Möglichkeit ist die Eingabe einer URL, die auf einen internen hochverfügbaren Server (z. B. einen NLB-Cluster) verweist. Mit der Schaltfläche ÜBERPRÜFEN können Sie die Erreichbarkeit dieses Servers kontrollieren.
- Die Alternative wäre, die Network-Location-Server-Funktionalität auf den DirectAccess-Server zu legen. In diesem Fall wählen Sie ein Zertifikat aus.

  Der Nachteil dieser Konfiguration ist, dass der DirectAccess-Server vermutlich nicht hochverfügbar ausgelegt ist. Steht der Network Location Server nicht zur Verfügung, können die Clients nicht mehr feststellen, ob Sie sich im internen oder externen Netz befinden.

Der nächste Dialog dieses Abschnitts dient zur Eingabe der Namenssuffixe und des zuständigen DNS-Servers. Benötigt wird hier die ISATAP-Adresse (Abbildung 13.27). An dieser Stelle möchte ich Sie noch auf zwei Anforderungen hinweisen:

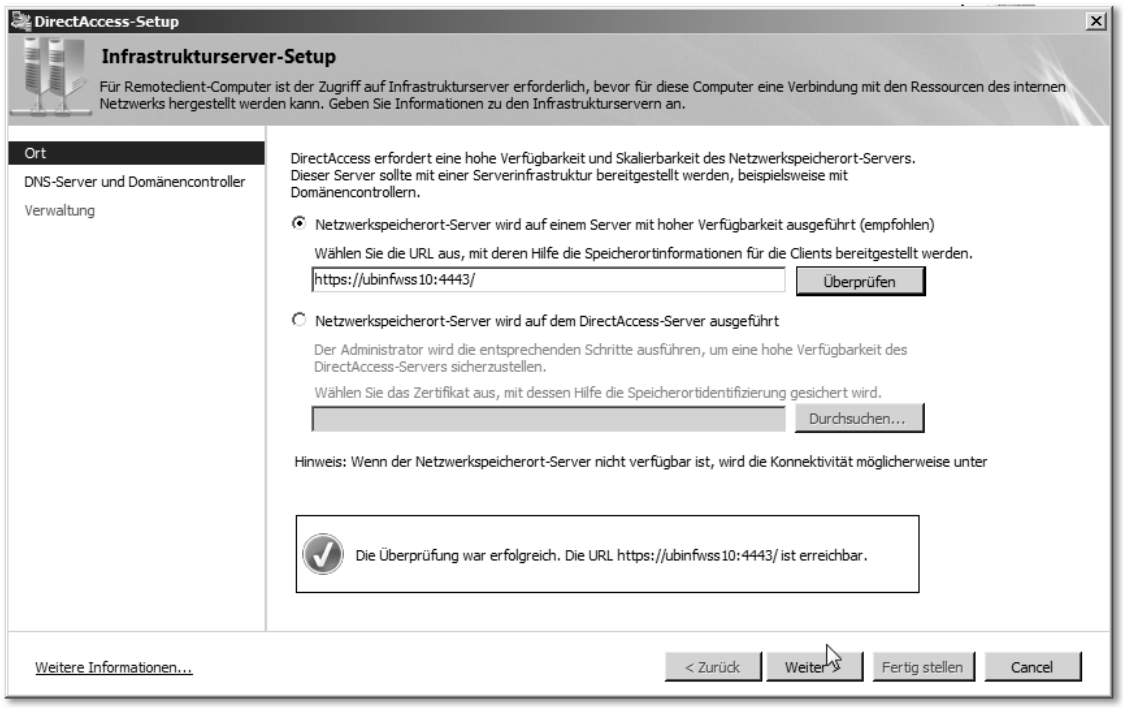


Abbildung 13.26 Wählen Sie den Network Location Server aus.

- Der DNS-Server muss sich auf einem Domänencontroller befinden.
- Der Server muss mindestens mit *Windows Server 2008 SP2* oder *Windows Server 2008 R2* laufen.

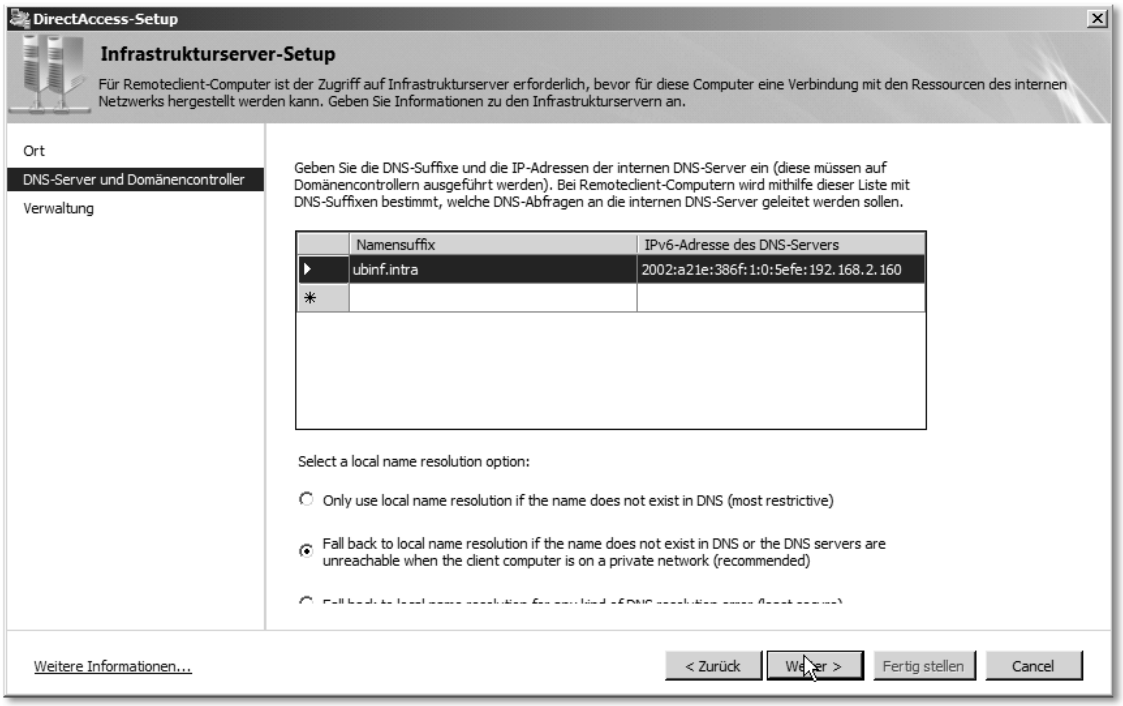


Abbildung 13.27 Konfigurieren Sie mindestens einen Domänencontroller/DNS-Server.

Im dritten und letzten Dialog des Konfigurationsabschnitts werden die IP-Adressen der Server angegeben, die Zugriff auf die verbundenen Clients haben sollen. Dies können beispielsweise Management-Server sein oder Admin-PCs, die per Fernsteuerung zugreifen sollen (Abbildung 13.28).

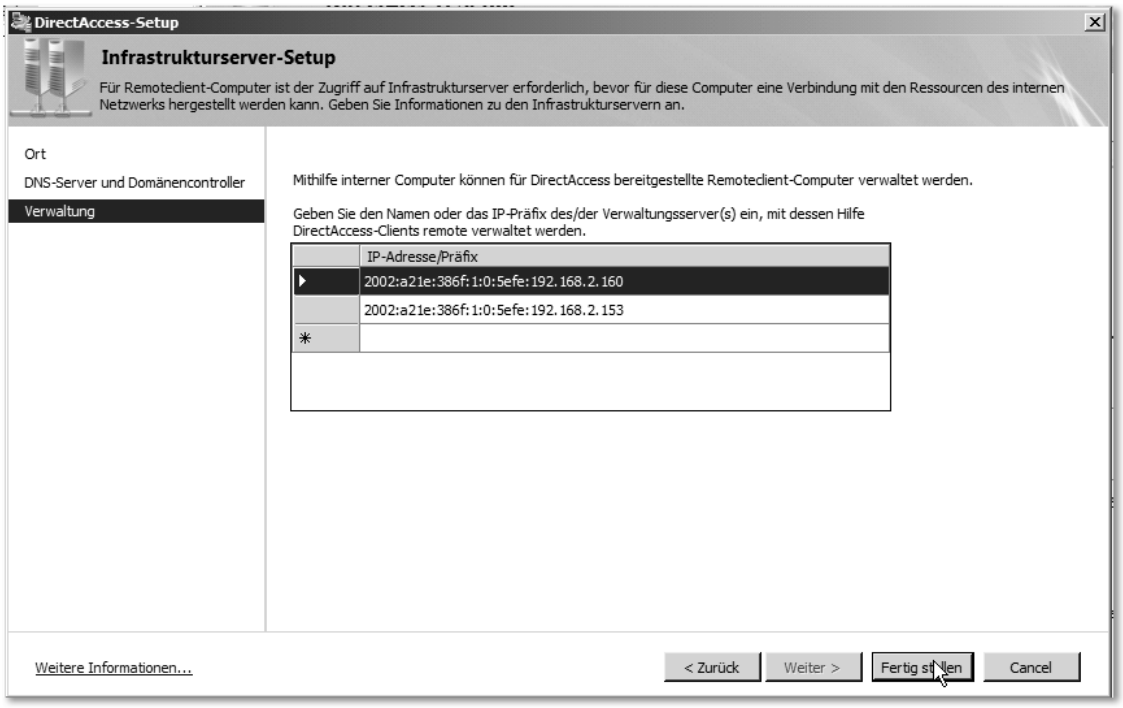


Abbildung 13.28 Die hier angegebenen Server können die DirectAccess-Clients verwalten, sprich: aktiv auf diese Clients zugreifen.

Schritt 4: Anwendungsserver

Im vierten Konfigurationsschritt legen Sie fest, auf welche Anwendungsserver die DirectAccess-Clients zugreifen können. Die in Abbildung 13.29 gezeigte Einstellung lässt den Zugriff auf sämtliche Anwendungsserver des internen Netzes zu – vorausgesetzt, diese haben eine ISATAP-Adresse. Verschiedene weitere Optionen stehen zur Verfügung, die im Dialog hinreichend erläutert sind.

... und nun: speichern und anwenden

Wenn Sie ein wenig zurückblättern, und zwar zur Abbildung 13.22, werden Sie sehen, dass es rechts unten im Dialog zwei Schalter, nämlich Speichern und Fertig gibt. Ein Klick auf die letztgenannte Schaltfläche sorgt dafür, dass die aktuell gespeicherte Konfiguration angewendet wird – vergessen Sie also nicht, erst zu speichern!

Wenn Sie die Konfiguration durch einen Klick auf Fertig anwenden, erscheint zunächst ein Überprüfungsdialog, den Sie bestätigen müssen (Abbildung 13.30).

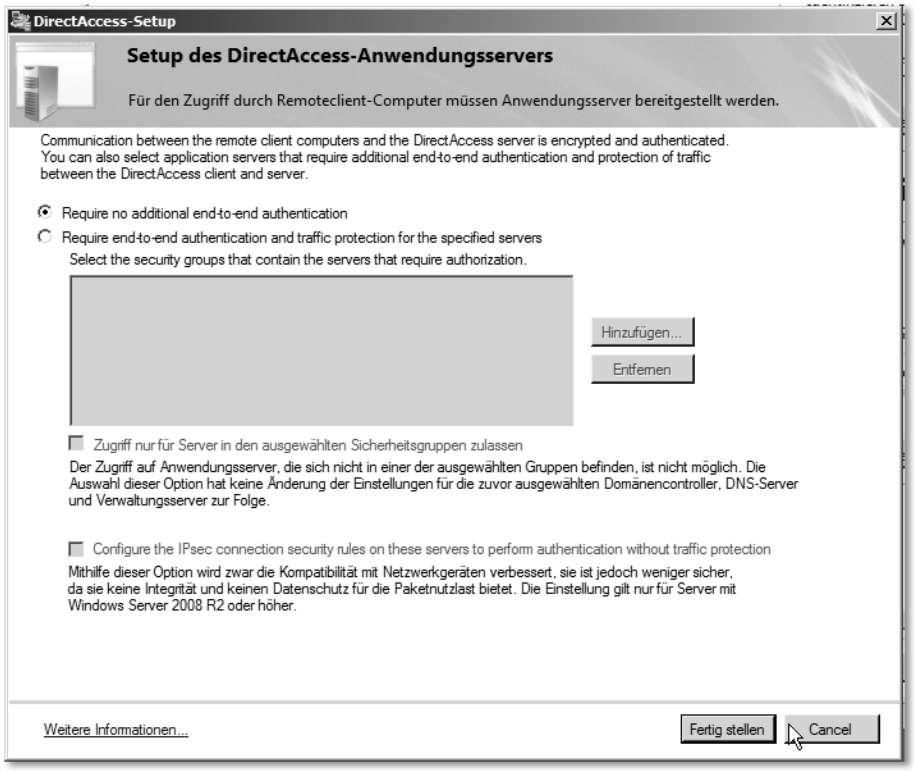


Abbildung 13.29 Auf dieser Dialogseite legen Sie fest, auf welche internen Server zugegriffen werden kann.

Abbildung 13.30 Vor dem Anwenden der neuen Konfiguration sehen Sie diese Zusammenfassung.

Das Übernehmen der Konfiguration dauert einige Sekunden. Wenn Sie den währenddessen eingeblendeten Dialog betrachten, werden Sie feststellen, dass vorwiegend Gruppenrichtlinienobjekte erzeugt werden (Abbildung 13.31). In der Tat erfolgt die Konfiguration des DirectAccess-Gesamtsystems über Gruppenrichtlinien – die Details werde ich Ihnen im weiteren Verlauf zeigen.

Abbildung 13.31 Beim Anwenden der Konfiguration werden unter anderem Gruppenrichtlinienobjekte erstellt.

Monitoring

Die DirectAccess-Verwaltungskonsole verfügt über einen Knoten namens ÜBERWACHUNG. Hier können Sie auf einen Blick erkennen, ob der Zustand des DirectAccess-Servers in Ordnung ist. Abbildung 13.32 zeigt einen voll funktionsfähigen DirectAccess-Server.

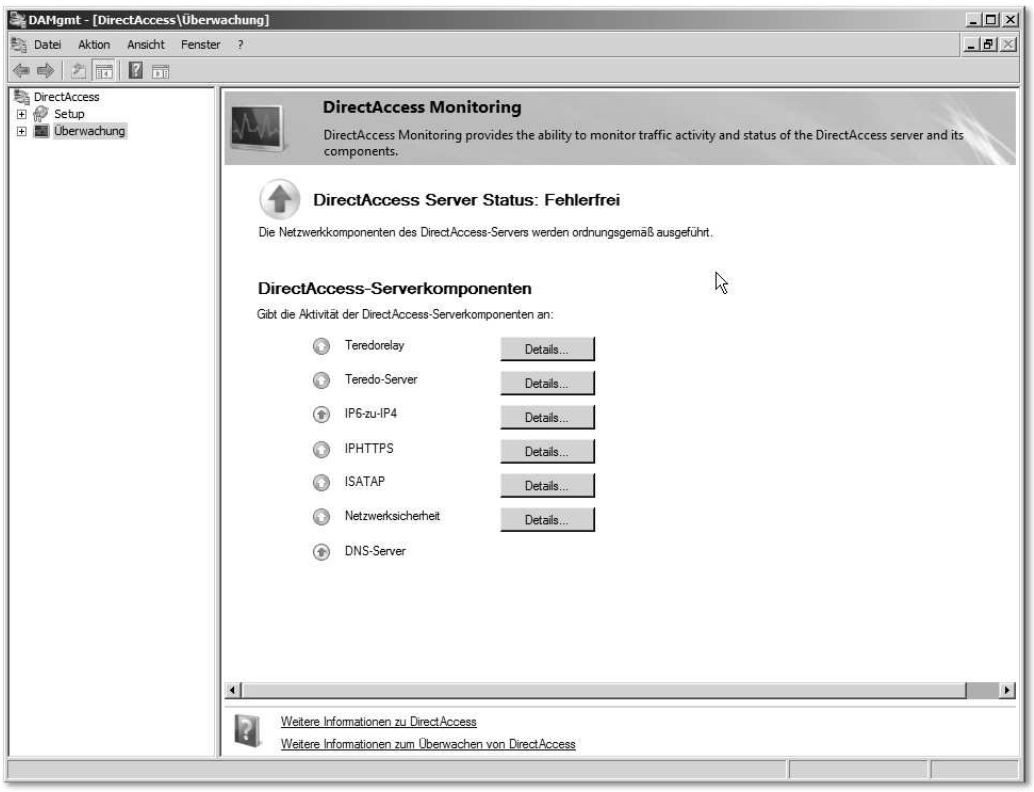


Abbildung 13.32 Diese Seite zeigt den Status des DirectAccess-Servers auf einen Blick.

Die Anzeige ist auf den ersten Blick ein wenig verwirrend, vielleicht sogar ein wenig erschreckend. Wenn die Anzeige der DirectAccess-Serverkomponenten gelb ist, bedeutet das in diesem Fall nicht, dass ein problematischer Betriebszustand vorliegt, sondern lediglich, dass derzeit keine Verbindungen über diese Komponente bestehen. Auf der Abbildung ist nur die Komponente IP6-zu-IP4 (6to4) aktiv, denn in der abgebildeten Umgebung sind in diesem Moment nur über dieses Tunneling-Protokoll Clients verbunden.

Ein Klick auf die jeweils bei einer Komponente vorhandene Details-Schaltfläche öffnet den Systemmonitor und zeigt detaillierte Verbindungsinformationen.

13.2.5 Ein wenig genauer hingeschaut …

Vielleicht wundern Sie sich, dass es keine »irgendwie sichtbare« Clientkomponente von DirectAccess gibt, auch die Eingriffsmöglichkeiten in den DirectAccess-Server halten sich auf den ersten Blick sehr in Grenzen. Die DirectAccess-Verwaltungskonsole erscheint ja auch nicht sehr funktionsreich zu sein.

Die Lösung liegt darin, dass die Steuerung der Clients komplett über Gruppenrichtlinien erfolgt, und auch die Kommunikation der DirectAccess-Verwaltungskonsole mit dem Server erfolgt über diesen Weg. Im Grunde genommen ist das optimal, weil so direkt eine Verteilung der Einstellungen sichergestellt ist. Um ein wenig hinter die Kulissen zu schauen, was ich nun vorhabe, müssen Sie somit Gruppenrichtlinien anschauen.

Wenn Sie die in der DirectAccess-Verwaltungskonsole erstellte Konfiguration anwenden, werden zwei Gruppenrichtlinien erstellt, die direkt mit der Domäne verknüpft sind. Die Namen beginnen mit DirectAccess-Richtlinie, dann folgt eine GUID. Eine dieser Richtlinien wird zur Konfiguration des Servers verwendet, die andere zur Clientkonfiguration. Über Sicherheitseinstellungen wird sichergestellt, dass die Gruppenrichtlinie nur auf den DirectAccess-Server bzw. nur auf Clients, die Mitglied in einer der berechtigten Gruppen sind, angewendet werden. Abbildung 13.33 zeigt die entsprechenden Einstellungen der Gruppenrichtlinie zur Konfiguration des DirectAccess-Servers. Bei der anderen Richtlinie ergibt sich ein analoges Bild – dort sind die in Konfigurationsschritt 1 angegebenen Gruppen mit Leseberechtigung aufgeführt.

DirectAccess basiert im Wesentlichen auf IPSec, und dieses basiert auf Richtlinien, die von der DirectAccess-Verwaltungskonsole erzeugt werden. Abbildung 13.34 zeigt einen Auszug aus der Gruppenrichtlinie für den DirectAccess-Server:

- Sie sehen, dass einige Verbindungssicherheitsrichtlinien im gleichnamigen Konfigurationsabschnitt der Windows-Firewall angelegt worden sind.

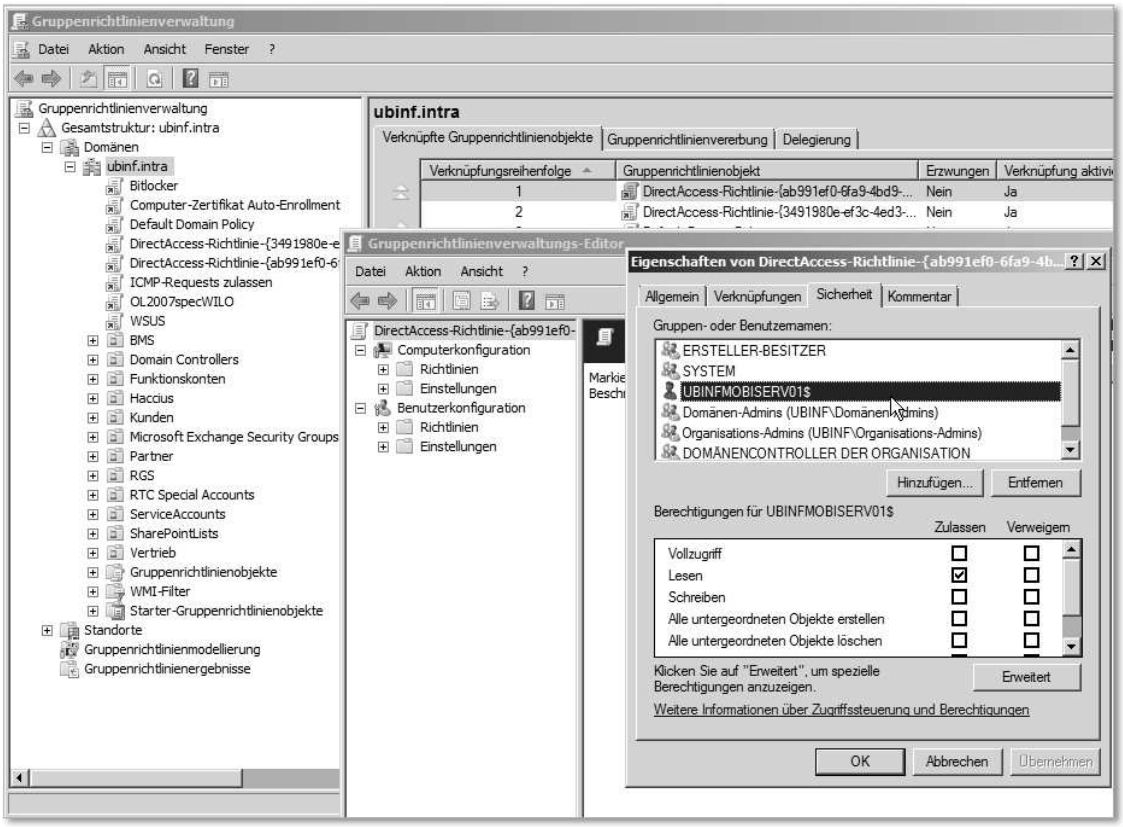


Abbildung 13.33 Auf eines der Gruppenrichtlinienobjekte kann nur der DirectAccess-Server zugreifen. Das andere kann nur von den DirectAccess-Clients gelesen werden.

- Die Richtlinien beziehen sich auf die Verbindung zwischen dem DirectAccess-Server und den Anwendungsservern im Innenbereich des Netzes, auf die Verbindungen zu den DNS-Servern und auf die zu den Verwaltungsservern.
- In der Verwaltungsserver-Richtlinie können Sie erkennen, dass die IP-Adressen der Verwaltungsserver als Endpunkte angegeben sind (vergleiche auch Abbildung 13.28).

Ich habe weiter vorn erwähnt, dass die IPSec-Authentifizierung mit Zertifikaten erfolgt. Dies lässt sich ebenfalls in den angelegten Richtlinien nachvollziehen: Abbildung 13.35 zeigt eine Verbindungssicherheitsrichtlinie für DirectAccess-Clients: Sie sehen, dass als Authentifizierungsmethode COMPUTERZERTIFIKAT angegeben ist, außerdem ist die ausgebende Zertifizierungsstelle hinterlegt.

Ein weiteres Beispiel ist die Definition der *Network Resolution Policy Table* (NRPT), der Tabelle also, die auf dem Client dafür sorgt, dass in einem externen Szenario (d. h. wenn sich der Client nicht im internen Netz befindet) die DNS-Anfragen für interne Ressourcen an den internen DNS-Server geleitet werden.

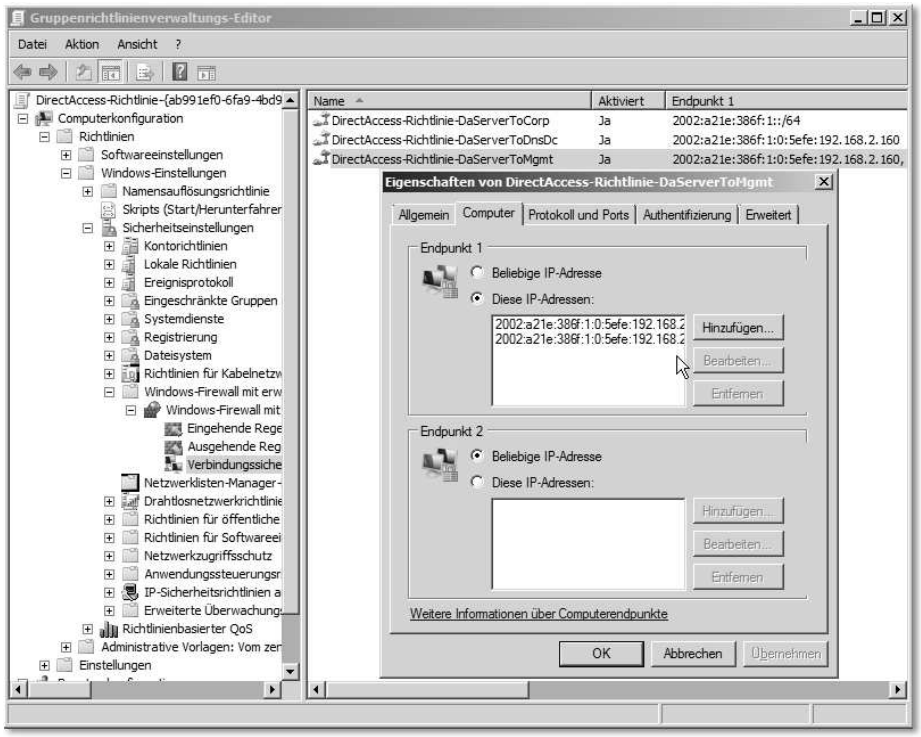


Abbildung 13.34 Die Verbindungssicherheitsrichtlinien für den DirectAccess-Server – hier für die Verwaltungsserver

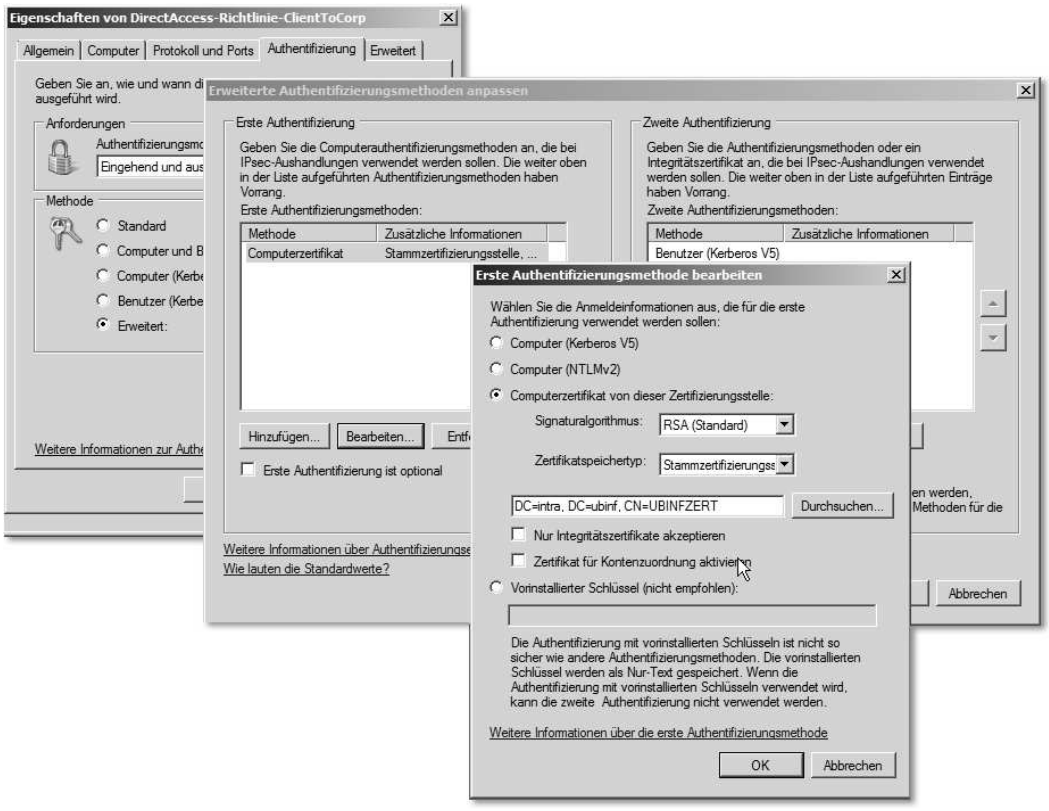


Abbildung 13.35 Ein Blick auf die Verbindungssicherheitsrichtlinien der DirectAccess-Clients. Hier ist zu sehen, dass die Authentifizierung auf Basis von Zertifikaten erfolgt.

Die NRPT wird mittels Einstellungen im Konfigurationsabschnitt WINDOWS-EINSTELLUNGEN • NAMENSAUFLÖSUNGSRICHTLINIE vorgenommen – die Konfiguration erfolgt auch hier über die DirectAccess-Verwaltungskonsole. Wenn Sie Abbildung 13.36 genau betrachten, werden Sie die Einstellung finden, dass Ressourcen aus dem Namensraum UBINF.INTRA über den DNS-Server 2002:a21e:... aufgelöst werden sollen.

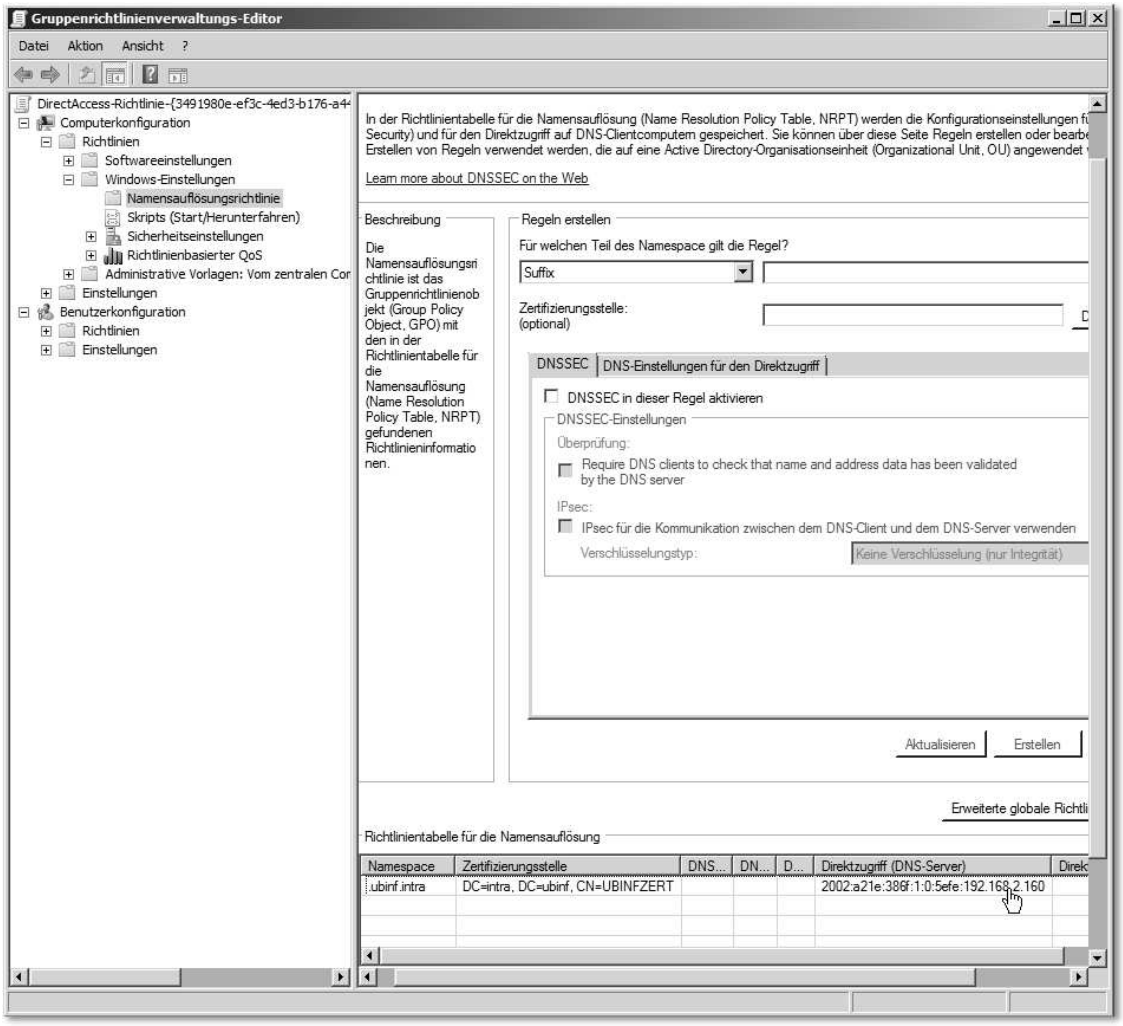


Abbildung 13.36 Die NRPT (Name Resolution Policy Table) für die Clients wird in dieser Richtlinie konfiguriert.

Grundsätzlich könnte die Konfiguration auch komplett ohne die DirectAccess-Verwaltungskonosole, einfach durch Anpassen der Gruppenrichtlinien erfolgen. Das würde zwar niemand ernsthaft tun wollen – Sie sehen aber den von den Entwicklern eingeschlagenen Weg: Sämtliche Konfigurationsinformationen werden per Gruppenrichtlinie gesteuert.

13.2.6 Aus der Clientperspektive

Für die Benutzer ist DirectAccess eine wunderbare Angelegenheit: Das komplette interne Netz (jedenfalls der Teil mit ISATAP-Adressen, der vom Administrator zugelassen ist) steht zur Verfügung, und man braucht nichts weiter zu tun. Es gibt also kein Herumfummeln mit einem VPN-Client – alles läuft, und zwar sofort.

DirectAccess-Client

Wenn ein Client ein DirectAccess-Client werden soll, ist es erforderlich, dass der PC bzw. das Notebook einmal im Unternehmensnetz war. Ansonsten bekäme er bzw. es nicht die Gruppenrichtlinien und somit keine DirectAccess-Konfiguration.

IP-Konfiguration

Abbildung 13.37 zeigt die IP-Konfiguration eines per DirectAccess verbundenen Clients:

- Der Client hat eine öffentliche IP-Adresse, könnte also beispielsweise mit einer UMTS-Karte ausgestattet sein.
- Der Client verfügt über eine ISATAP-Adresse (2002:....).

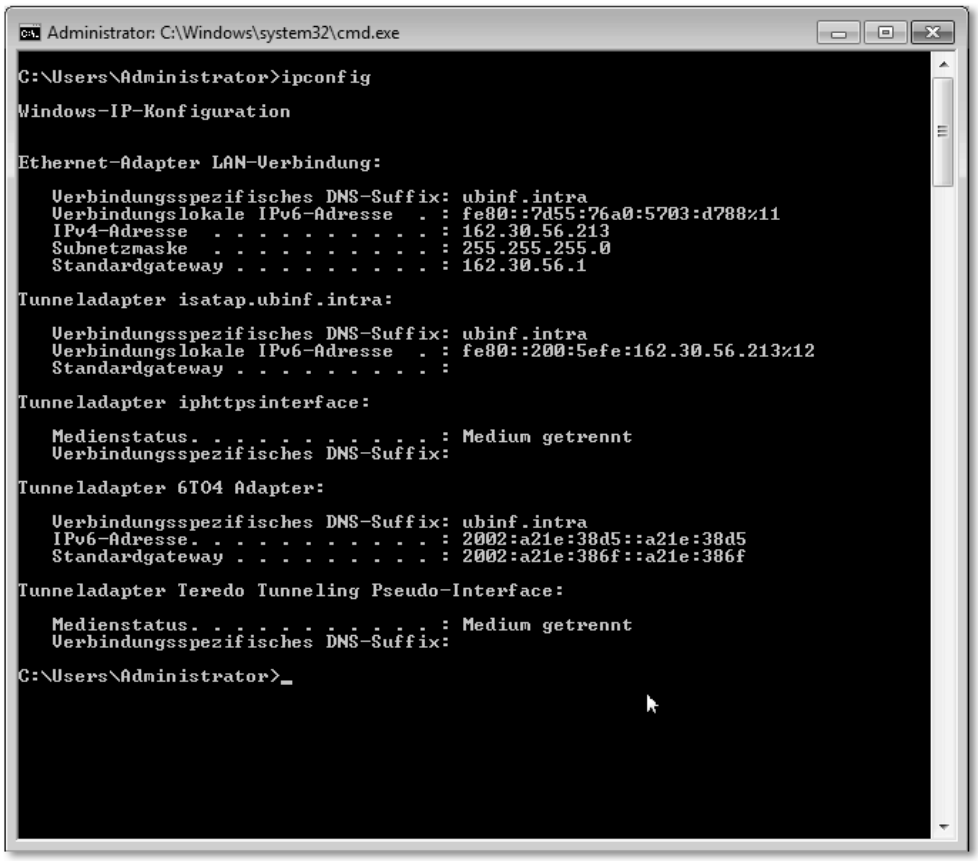


Abbildung 13.37 Die IP-Konfiguration des über das Internet verbundenen DirectAccess-Clients

NRPT

Eine wesentliche Voraussetzung für die Nutzung von DirectAccess ist die NRPT. Mit dem Befehl `netsh name show pol` wird das gesamte (per Gruppenrichtlinie konfiguierte) Regelwerk angezeigt, und mit `netsh name show eff` werden die momentan aktiven DNS-Auflösungsregeln gezeigt: Auf Abbildung 13.38 ist ein Client zu sehen, der momentan mit dem Internet verbunden ist. Namensauflösungen für den Namensraum `ubinf.intra` werden von einem internen Server aufgelöst, der über eine ISATAP-Adresse erreichbar ist.

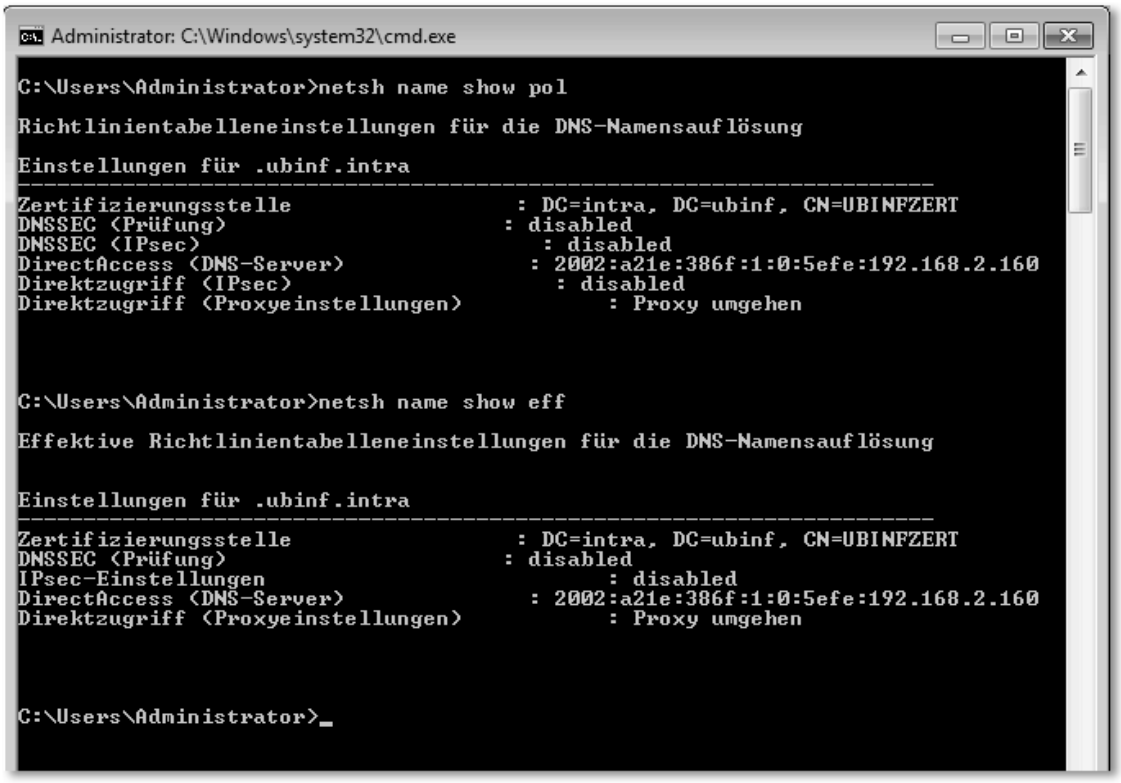


Abbildung 13.38 Die NRPT-Konfiguration, wenn der DirectAccess-Client über das Internet verbunden ist

Wie das Ganze aussieht, wenn der Client sich im Unternehmensnetz befindet, ist auf Abbildung 13.39 gezeigt:

- Das in der NRPT-Tabelle enthaltene Regelwerk (`netsh name show pol`) bleibt unverändert.
- Da der PC sich im Innenbereich befindet, werden Suchanfragen nach internen PCs nicht über DirectAccess geleitet, sondern direkt einem »normalen« Nameserver zugewiesen. Dies wird dadurch erreicht, dass von DirectAccess in die NRPT eingegriffen wird.

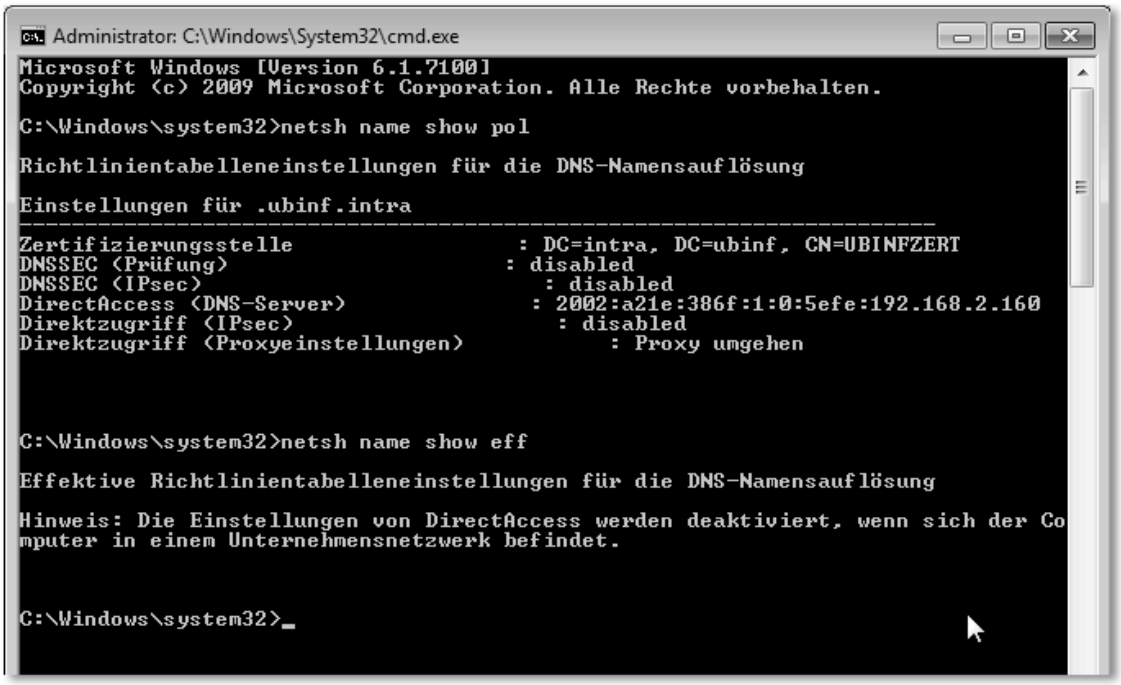


Abbildung 13.39 Dieses Bild ergibt sich, wenn der Client im Unternehmens-LAN ist.

Registrierung im DNS

Ein Client, der im internen Netz startet, registriert Namen und IP-Adressen im DNS – das ist nun nicht neu. Da ein DirectAccess-Client in in letzter Konsequenz ebenfalls eine interne Maschine ist, registriert er brav seinen Namen und seine IP-Adresse. Ein Blick ins DNS (Abbildung 13.40, markierter Eintrag) zeigt, dass der Client nur eine IPv6-Adresse hat. Das ist auch korrekt, denn über eine IPv4-Adresse ist er in der Tat auch nicht zu erreichen, wenn er über DirectAccess mit dem Unternehmensnetz verbunden ist.

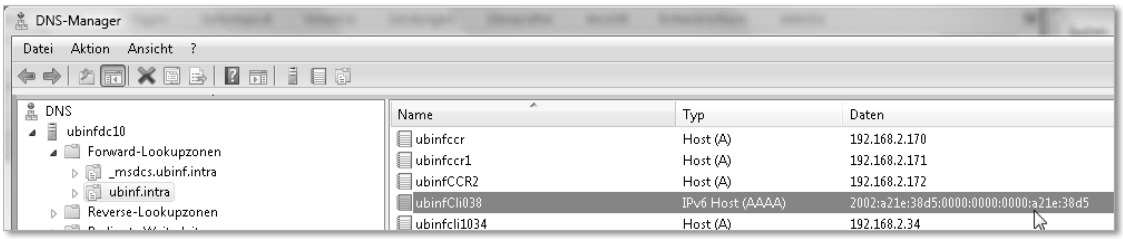


Abbildung 13.40 Ist der Client über das Internet verbunden, ist für ihn nur eine IPv6-Adresse konfiguriert.

Wenn der Client zu einem späteren Zeitpunkt im Unternehmensnetz eingeschaltet wird, wird er sowohl die IPv4- als auch die IPv6-Adresse registrieren – dann ist er ja auch über beide Varianten erreichbar.

Zugriff auf das Unternehmens-LAN

Wir kommen nun zu dem vermutlich spannendsten Test, nämlich zum Zugriff auf interne Server des Unternehmensnetzes. Ich muss Sie allerdings enttäuschen, denn es gibt da nicht viel zu zeigen – es klappt einfach.

Abbildung 13.41 zeigt zunächst einen Ping-Vorgang auf einen Server, der über eine ISATAP-Adresse verfügt: Der Name wird aufgelöst, und der Server antwortet auf die Pings.

Als Zweites habe ich den Namen eines Servers, der nur über eine IPv4-Adresse verfügt, angegeben (`ubinfex2`). Er wird nicht gefunden. Der Server ist zwar im Netz vorhanden, da er aber über keine IPv6-Adresse verfügt, steht er für den DirectAccess-Client nicht zur Verfügung.

Ältere Server

Falls Sie mittels DirectAccess auf einen älteren Server (Windows 2000 oder älter) zugreifen möchten, müssen Sie NAT-PT einsetzen. Diese Technologie ist aber nur von Drittherstellern (z. B. *Cisco*) erhältlich.

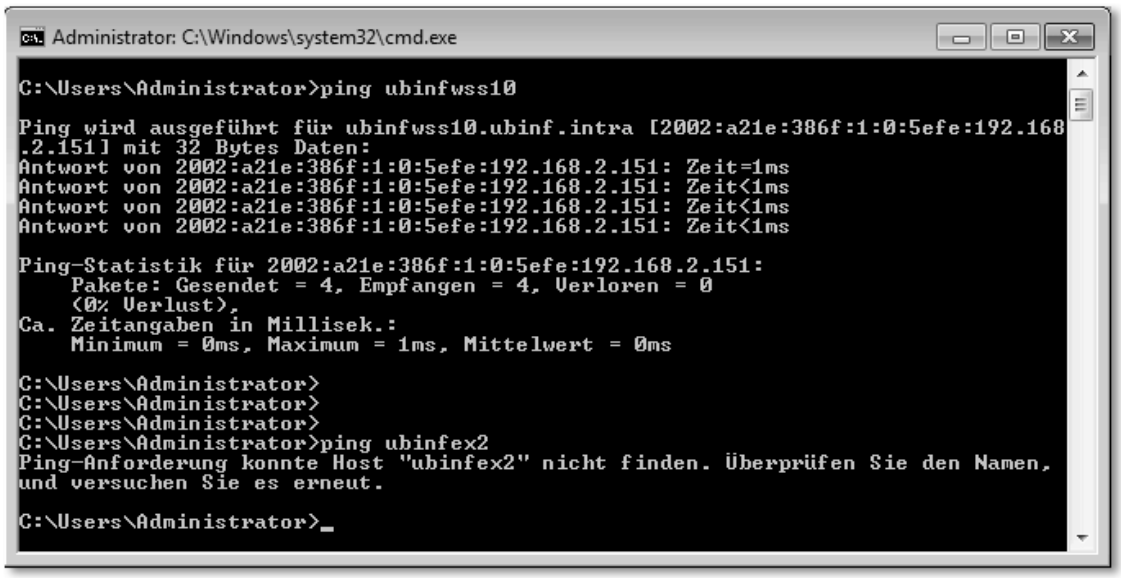


Abbildung 13.41 Die Namen von IPv6-Servern mit ISATAP-Adresse können aufgelöst werden. Dies ist mit Nur-IPv4-Clients nicht möglich. Diese werden einfach nicht gefunden.

Abbildung 13.42 zeigt den Zugriff über DirectAccess auf einen Dateiserver mit Freigaben – es ist kein Unterschied zu erkennen, der Benutzer kann so arbeiten, als wäre er im LAN.

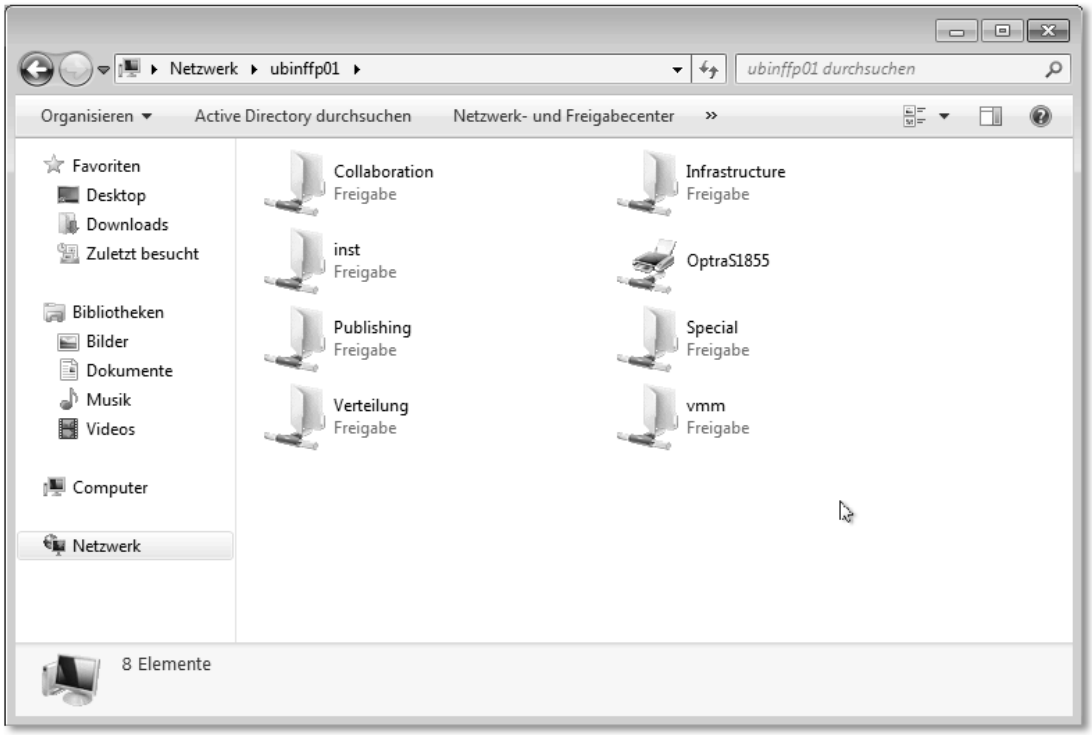


Abbildung 13.42 Sehen Sie einen Unterschied? Der Zugriff auf diesen Dateiserver erfolgt über DirectAccess.

Zugriff auf den DirectAccess-Client

Der Zugriff funktioniert nicht nur vom im Internet befindlichen Client in Richtung der internen Server, sondern auch umgekehrt. Auf Abbildung 13.43 habe ich von einem als Verwaltungsserver definierten System (Abbildung 13.28) ein Ping auf den über DirectAccess verbundenen Client abgesetzt. Siehe da, es funktioniert.

Da der DirectAccess-Client seine IP-Adresse beim Verbindungsaufbau mit dem Unternehmensnetz auf dem internen DNS-Server registriert, kann er einfach mit seinem Namen aufgerufen werden.

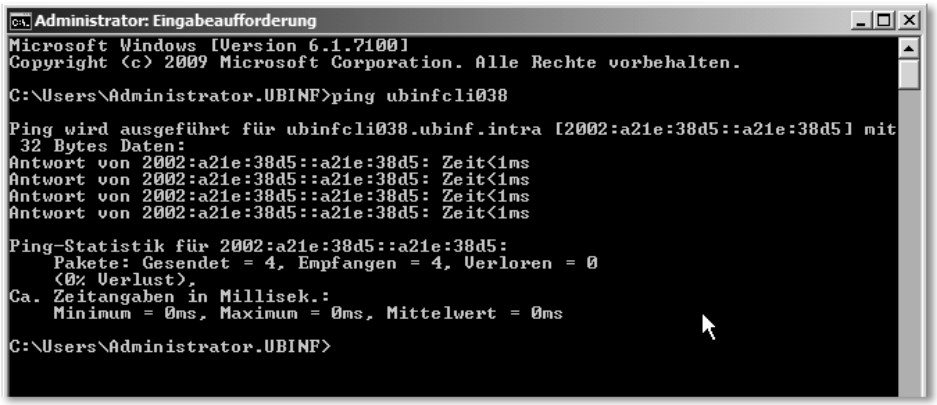


Abbildung 13.43 Der über das Internet angebundene DirectAccess-Client kann von den als Verwaltungsserver konfigurierten Systemen angesprochen werden.

Hierzu gibt es noch zwei wichtige Anmerkungen

- Der Zugriff auf die DirectAccess-Clients ist nur von den Maschinen aus möglich, die als Verwaltungsserver eingetragen sind.
- Der Zugriff ist auch möglich, wenn kein Benutzer angelegt ist. Sie könnten beispielsweise auf einen eingeschalteten PC per Remotedesktop zugreifen und sich anmelden.

13.2.7 Noch mehr DirectAccess

Man könnte problemlos noch mehr über DirectAccess berichten. So wäre es sicherlich nicht uninteressant, einmal die Netzwerkkonfiguration bei einem Teredo- oder IP-HTTPS-Zugriff zu untersuchen – das funktioniert genauso unproblematisch, wenn die Konfiguration erst einmal steht.

Weiterhin möchte ich darauf hinweisen, dass DirectAccess und NAP integriert sind. NAP ist eine wichtige Sicherheitstechnologie, mit deren Hilfe verhindert werden kann, dass ein Client, der beispielsweise nicht über ausreichend aktuelle Virenschutz-Pattern verfügt, auf das Netz zugreift.

Ist NAP aktiviert, lässt sich verhindern, dass ein Client, der nicht den Unternehmensrichtlinien entspricht, über DirectAccess auf das Netz zugreift.

13.2.8 Die Sicherheit

Der Schwachpunkt in Sachen Sicherheit bei DirectAccess ist wohl nicht, dass ein potenzieller Datendieb die IPSec-Verschlüsselung bricht. Die Bedrohung ist viel naheliegender: Wenn ein Notebook mit DirectAccess-Zugriff gestohlen wird und dieses beim Einschalten nicht nach einem Benutzerkennwort fragt – dann ist der Datendieb »drin« (im Unternehmensnetz). Für DirectAccess-Notebooks sollten also folgende Richtlinien durchgesetzt werden:

- aktivierte BitLocker-Verschlüsselung
- Nach einigen Minuten ohne Benutzeraktivität sollte sich das Notebook sperren.
- Weiterhin sollte das Gerät beim Aufwachen aus dem Ruhezustand und generell beim Systemstart ein Kennwort anfordern.

13.3 BranchCache

IT-Verantwortliche in Unternehmen mit mehreren Standorten träumen im Allgemeinen von einer möglichst zentralisierten Umgebung: Je weniger Server in den Niederlassungen vorhanden sind, desto weniger ist zu administrieren. Problema-

tisch ist allerdings, dass über WAN-Verbindungen dann doch nicht so schnelle Zugriffe zu realisieren sind wie mit einem lokalen Server am Standort.

Neben dem Konsolidierungsgedanken gibt es aber durchaus auch Anforderungen, die sich ohnehin nicht einfach durch lokale Server lösen lassen würden – unabhängig davon, dass kaum eine IT-Organisation ohne Not zig Server in Niederlassungen haben möchte. Im Allgemeinen müssen die Benutzer in den Niederlassungen mehr oder weniger häufig auf Daten aus der Zentrale zugreifen, beispielsweise auf Dateien, das Intranet oder auch WSUS. Damit kommen wir zu dem Problem, dass dieselben Daten vielfach über die WAN-Verbindung transportiert werden:

- Die Excel-Tabelle mit den Vertriebszahlen des letzten Monats wird von jedem Benutzer der Niederlassung geladen.
- Jeder Anwender der Niederlassung holt das 12 MB große PowerPoint-Dokument mit der neuesten Unternehmenspräsentation.
- Das stark mit Bildern angereicherte Intranet benötigt auch ein Stück von der knappen Bandbreite, insbesondere um die diversen Grafiken zu übertragen.
- Auch Funktionen wie WSUS konsumieren, zumindest temporär, einen erheblichen Teil der wertvollen WAN-Verbindungen, nämlich dann, wenn jeder Computer in der Niederlassung die neusten Patches bzw. Service Packs vom zentralen WSUS-Server holt.

Nun kann man auf die zuvor genannten Anforderungen natürlich mit mehr oder weniger komplexen Replikationslösungen reagieren, einen lokalen WSUS-Server aufbauen und ähnliche Maßnahmen ergreifen. Das widerspricht dem Konsolidierungsgedanken und ist teilweise auch nicht ganz trivial umzusetzen. Einen zweiten WSUS-Server aufzubauen, ist zunächst nicht schwierig, und auch die Gruppenrichtlinien, die dafür sorgen, dass der jeweils am Standort vorhandene WSUS-Server verwendet wird, sind schnell erstellt. Bei einer Replikationslösung für das Dateisystem sieht die Sache dann allerdings nicht mehr ganz so simpel aus.

Mit Windows Server 2008 und Windows 7 gibt es nun die Funktion *BranchCache*, die das Leben wieder ein wenig einfacher machen wird.

13.3.1 Voraussetzungen

Betrachten wir zunächst die Voraussetzungen: BranchCache optimiert die HTTP-, BITS- und SMB-Kommunikation zwischen Windows 7-Clients und Windows-Server-2008-*R2*(!)-Servern. Liegen Daten auf älteren Servern (inklusive Windows Server 2008 ohne R2), kann deren Übertragung nicht mittels BranchCache optimiert werden.

Somit lautet die erste Voraussetzung: Die Daten müssen auf Windows Server 2008 *R2*-Servern liegen. Achten Sie unbedingt auf diese Version, wenn Sie *BranchCache* verwenden wollen..

Auf der Clientseite ist natürlich *Windows 7* Pflicht. BranchCache ist in den Editionen *Enterprise* und *Ultimate* enthalten – und damit wäre auch schon die zweite Voraussetzung definiert.

Die dritte Voraussetzung ist, dass die Datenübertragung über eines der für BranchCache aktivierten Protokolle erfolgt:

- *HTTP/HTTPS*: Mit BranchCache lässt sich also die Übertragung von Webinhalten optimieren.
- *SMB*: Die Übertragung von Daten von Fileshares wird durch BranchCache optimiert.
- *BITS*: Anwendungen, die BITS (*Background Intelligent Transfer Service*) zum Übertragen von Dateien verwenden, profitieren ebenfalls von BranchCache.

BranchCache wirkt also nicht auf irgendeine zauberhafte Weise bei der Übertragung von Clients von Datenbankprogrammen mit.

13.3.2 Funktionsweise

BrancheCache verfügt über zwei Modi, nämlich *Verteilter Cache* und *Gehosteter Cache*. Ersterer implementiert an den Außenstandorten eine Art Peer-to-Peer-Modell, bei Letztgenanntem wird ein dedizierter Server in der Niederlassung implementiert, der als Cache fungiert.

Verteilter Cache

Im Modus *Verteilter Cache* wird eine Art Peer-to-Peer-Betriebskonzept umgesetzt. Abbildung 13.44 zeigt den Ablauf, wenn ein Client eine Datei anfordert, die noch nicht im Cache eines anderen Clients am Standort vorhanden ist:

1. Der Client übermittelt eine Anfrage an einen Server in der Zentrale. In einer Erweiterung des Protokolls (HTTP, BITS, SMB) teilt er dem Server mit, dass er für BranchCache aktiviert ist.
2. Der Server antwortet mit Informationen über die Datei, sendet aber nicht die Datei selbst.
3. Der Client wird nun versuchen, in seinem lokalen Netzwerksegment, also in der Niederlassung, einen anderen Client zu finden, der diese Datei bereits geladen hat. Dies geschieht über einen UDP-Broadcast. Es gibt übrigens ein spezielles Protokoll, nämlich das *BranchCache Retrieval Protocol* (MS-PCCRD).

In diesem Fall antwortet kein Client – bisher hat noch niemand die Datei heruntergeladen.

4. Nun wendet sich der Client wieder an den Server und fragt die Datei nochmals an. Diesmal meldet er sich nicht als BranchCache-Client, sodass der Server »ganz normal« die Datei übermittelt. Der PC speichert die Datei in seinem lokalen Cache.

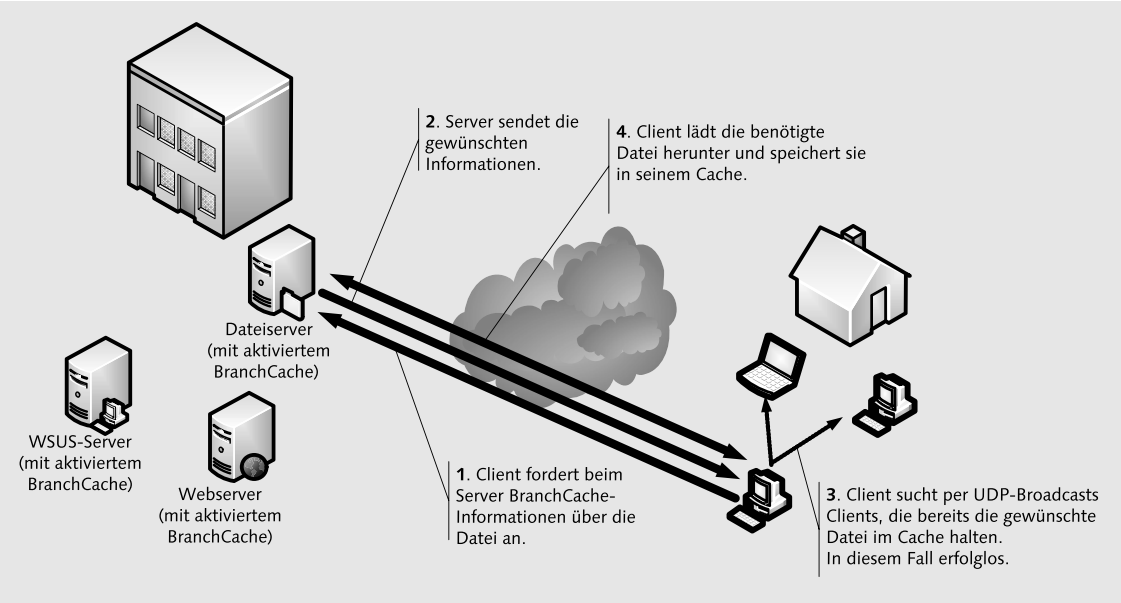


Abbildung 13.44 BranchCache im Modus »Verteiler Cache«: Ein Client benötigt eine Datei, die noch nicht an dem Standort vorhanden ist.

Wenn nun ein zweiter Client dieselbe Datei anfordert, läuft das so wie auf Abbildung 13.45 ab:

1. Der Client übermittelt eine Anfrage an einen Server in der Zentrale. In einer Erweiterung des Protokolls (HTTP, BITS, SMB) teilt er dem Server mit, dass er für BranchCache aktiviert ist.
2. Der Server antwortet mit Informationen über die Datei, sendet aber nicht die Datei selbst.
3. Der Client sucht per UDP-Broadcast einen Client in seinem Netzwerksegment, der diese Datei bereits im Cache hat.
4. Die Suche ist erfolgreich: Ein anderer Client teilt mit, dass er über die benötigte Datei verfügt.
5. Der anfordernde Client lädt die Datei nun von einem anderen lokalen Client herunter. Nach Abschluss der Übertragung prüft er die erhaltene Datei daraufhin, ob sie mit den vom Server erhaltenen Informationen übereinstimmt.

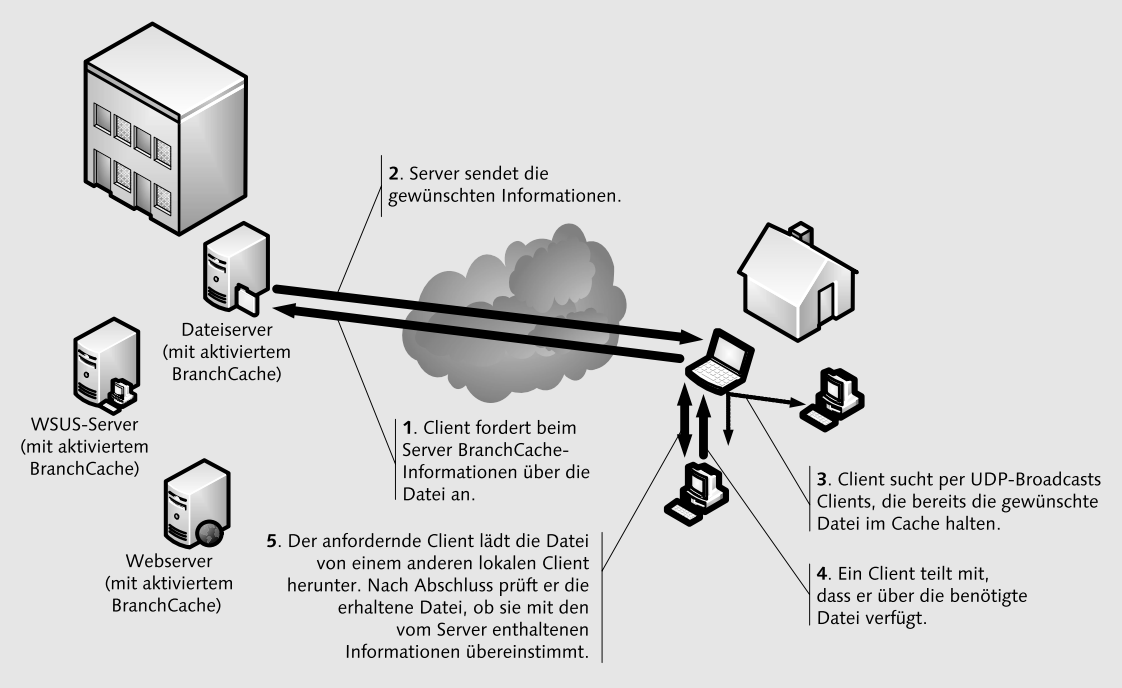


Abbildung 13.45 BranchCache im Modus Verteiler Cache: Ein anderer Client fordert eine Datei an, die bereits im Cache eines Standort-PCs vorhanden ist.

BranchCache funktioniert also auch an einem Standort ohne jegliche Serverinfrastruktur – es stört aber auch nicht, wenn lokale Server vorhanden sind.

Wenn ein oder mehrere Clients offline sind, hat das auf das Funktionieren des Systems keine Auswirkungen. Benötigt ein Client eine Datei, broadcastet er durch sein lokales Netz. Wenn kein anderer PC online ist, findet er eben keine lokale Kopie der gesuchten Datei.

Es spielt dem Modus *Verteilter Cache* von BranchCache natürlich absolut in die Hände, dass heute jeder PC und jedes Notebook dramatisch viel mehr Speicherkapazität hat, als für das Ausführen des Betriebssystems nebst Applikationen benötigt wird. Insofern kann dieser ansonsten brach liegende Speicherplatz natürlich genutzt werden, beispielsweise für BranchCache. Standardmäßig werden fünf Prozent des auf dem PC insgesamt zur Verfügung stehenden Speicherplatzes abgezweigt. Dieser Wert kann über eine Gruppenrichtlinie geändert werden.

Gehosteter Cache

Der Modus *Gehosteter Cache* unterscheidet sich von der zuvor vorgestellten Variante insbesondere dadurch, dass eine dedizierte Maschine die Cache-Funktion übernimmt. Es gibt also keinen Peer-to-Peer-Betrieb mehr, sondern es wird eine dedizierte Client-Server-Architektur verwendet. Der Vorteil ist, dass dieser Cache immer da ist und sämtliche Dateien kennt, die an diesem Standort hteruntergela-

den worden sind. Beim *Verteilten Cache* wird es immer Qualitätsunterschiede geben, weil nicht jederzeit sämtliche Clients eingeschaltet sein werden und Notebooks vermutlich ohnehin häufig unterwegs sind. Der Nachteil beim *Gehosteten Cache* ist, dass ein Server mit dem Betriebssystem *Windows Server 2008 R2* benötigt wird. Wenn aber ohnehin ein kleiner Server an dem Standort vorhanden sein muss (für welche Aufgaben auch immer), kann er diese Funktion natürlich übernehmen.

Welche Maschine der *Gehostete Cache* ist, wird für die Clients des Standorts per Gruppenrichtlinie festgelegt.

Abbildung 13.46 zeigt den Ablauf, wenn die von einem Client angeforderte Datei noch nicht auf dem *Hosted Cache* vorhanden ist:

1. Der Client übermittelt an einen Server in der Zentrale eine Anfrage. In einer Erweiterung des Protokolls (HTTP, BITS, SMB) teilt er dem Server mit, dass er für BranchCache aktiviert ist.
2. Der Server antwortet mit Informationen über die Datei, sendet aber nicht die Datei selbst.
3. Der Client fragt auf dem *Hosted-Cache*-Server nach, ob die Datei dort vorhanden ist – in diesem Fall ist sie das nicht.
4. Nun wendet sich der Client wieder an den Server und fragt die Datei nochmals an. Diesmal meldet er sich nicht als BranchCache-Client, sodass der Server »ganz normal« die Datei übermittelt. Der PC speichert die Datei in seinem lokalen Cache.
5. Nach Abschluss des Downloads bietet der Client die Datei dem *Hosted Cache* an. Dieser wird sie anfordern und für andere Clients bereithalten. Auf diese Weise verfügt der *Hosted Cache* über sämtliche Dateien, die von Clients der Niederlassung angefordert wurden.

Bleibt noch die Frage zu klären, wie der Ablauf ist, wenn die Datei auf dem *Hosted Cache* vorhanden ist. Die Antwort finden Sie auf Abbildung 13.47:

1. Der Client übermittelt an einen Server in der Zentrale eine Anfrage. In einer Erweiterung des Protokolls (HTTP, BITS, SMB) teilt er dem Server mit, dass er für BranchCache aktiviert ist.
2. Der Server antwortet mit Informationen über die Datei, sendet aber nicht die Datei selbst.
3. Der Client fragt auf dem *Hosted-Cache*-Server nach, ob die Datei dort vorhanden ist. Wenn sie vorhanden ist, erhält der Client die Datei und gleicht sie mit den vom Zentralserver empfangenen Daten ab.

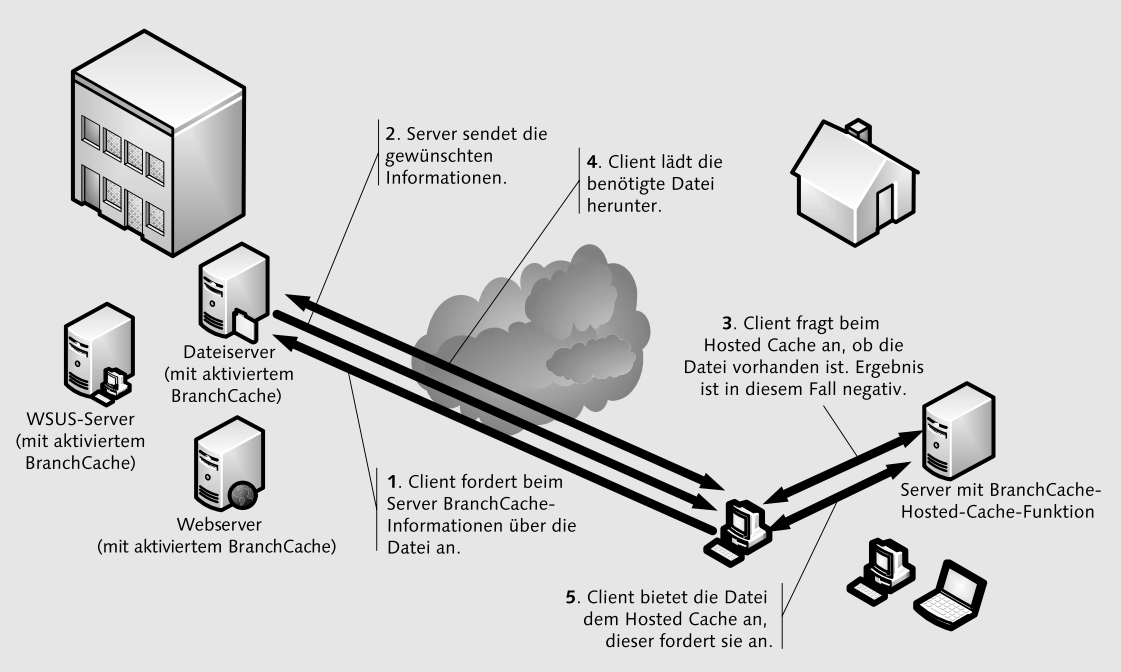


Abbildung 13.46 BranchCache im Modus »Gehosteter Cache«: Hier benötigt ein Client eine Datei, die auf dem Cache noch nicht vorhanden ist.

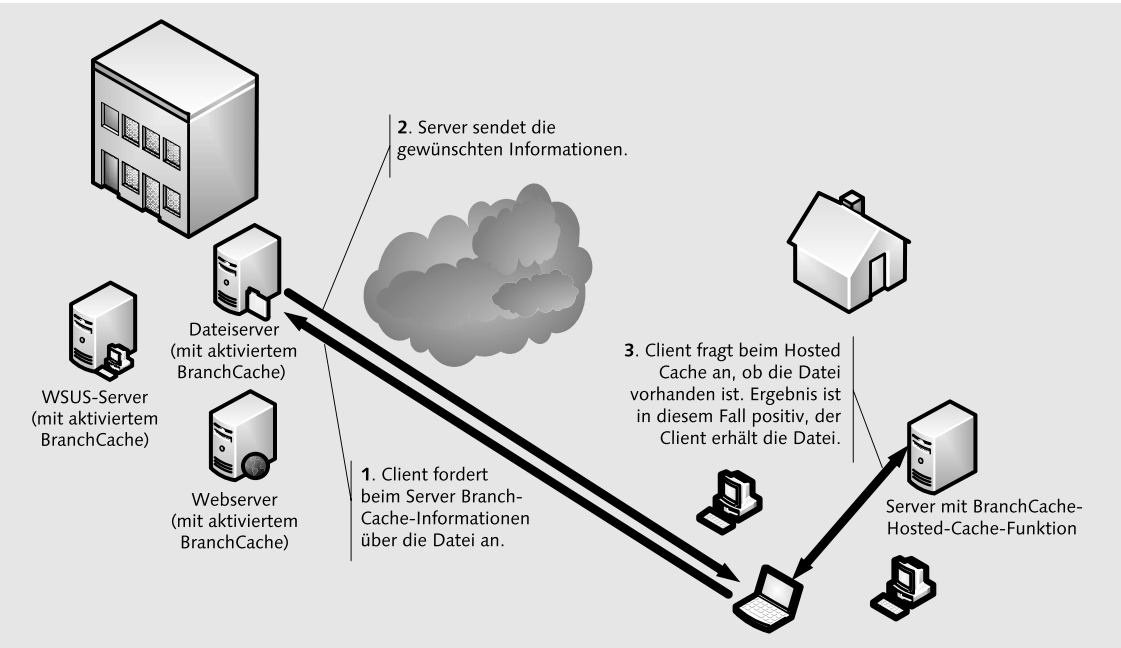


Abbildung 13.47 BranchCache im Modus »Gehosteter Cache«: In diesem Fall ist die benötigte Datei bereits auf dem Cache vorhanden.

13.3.3 Server konfigurieren

Die Konfiguration von BranchCache ist recht simpel. Auf Windows Server 2008 R2 gibt es ein Feature namens BranchCache, das ohne weitere Konfigurationsmaßnahmen installiert wird (Abbildung 13.48).

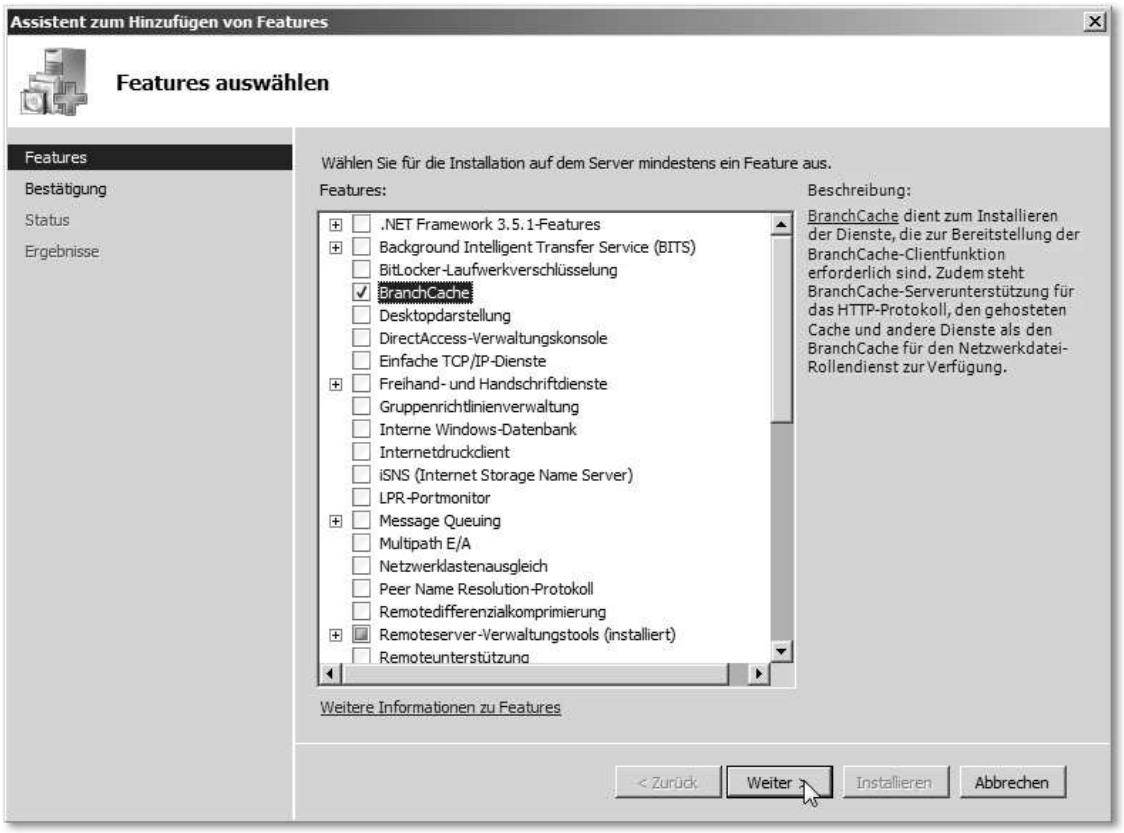


Abbildung 13.48 In Windows Server 2008 R2 existiert das Feature »BranchCache«.

Wenn dieser Server HTTP- oder BITS-Daten zur Verfügung stellt, sind Sie mit Installation und Konfiguration bereits fertig – alles läuft. Kontrollen Sie vorsichtshalber, ob der Dienst *BranchCache* auch tatsächlich läuft, normalerweise dürfte das aber der Fall sein.

Wenn die BranchCache-Clients Daten per SMB anfordern, also auf Dateifreigaben zugreifen, ist ein wenig mehr zu tun:

- Zunächst muss der Rollendienst BranchCache für Netzwerkdateien hinzugefügt werden. Dies initiieren Sie im Server-Manager im Konfigurationsbereich der Rolle Dateidienste (Abbildung 13.49).
- Im nächsten Schritt legen Sie fest, für welche Dateifreigaben die Hashveröffentlichung für BranchCache durchgeführt werden soll (Abbildung 13.50).

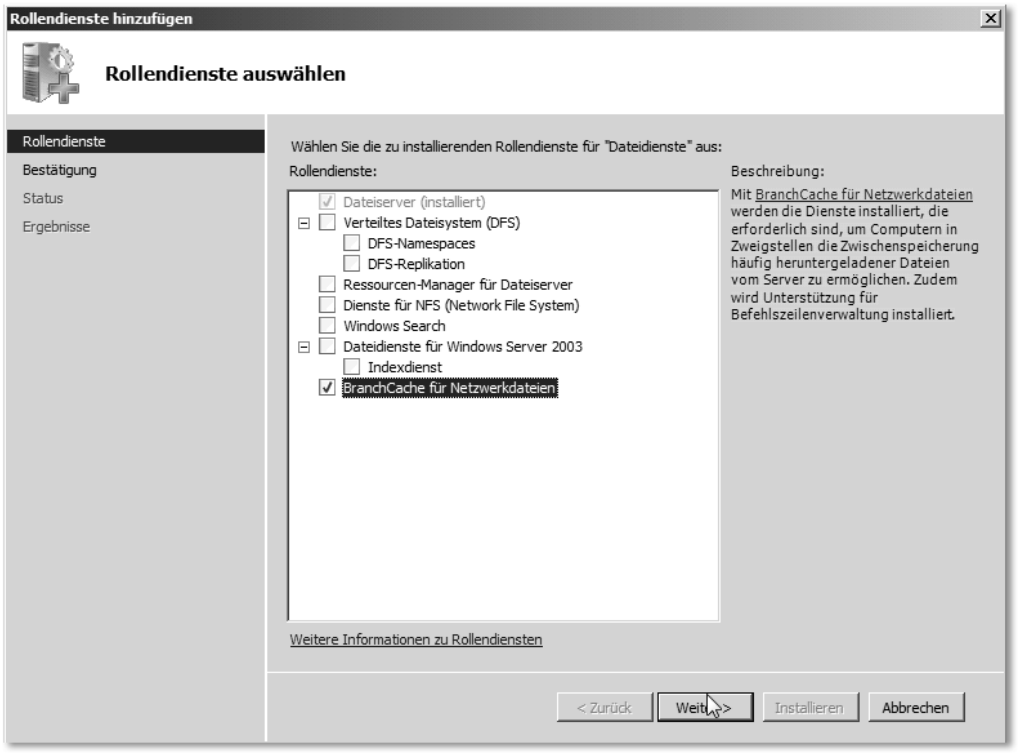


Abbildung 13.49 Wenn SMB-Datenverkehr mit BranchCache optimiert werden soll, muss der Rollendienst für Netzwerkdateien hinzugefügt werden.

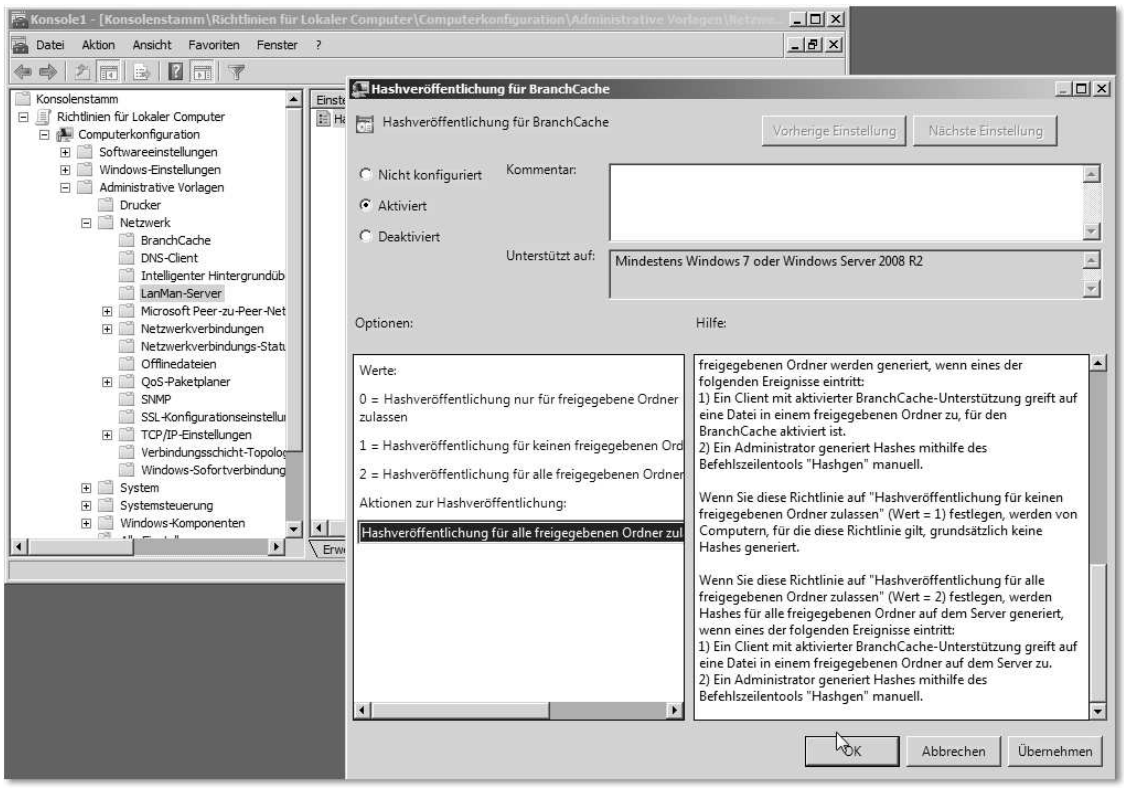


Abbildung 13.50 Mit dieser Gruppenrichtlinien-Einstellung legen Sie fest, ob BranchCache für Dateifreigaben aktiv sein soll.

Hier stehen zunächst drei recht allgemein gehaltene Optionen zur Verfügung: keine Hashveröffentlichungen für Dateifreigaben, Hashveröffentlichung für alle Dateifreigaben und Hashveröffentlichung für mit BranchCache aktivierte Dateifreigaben. Wenn Sie sich für die letztgenannte Option entscheiden, ist noch ein wenig »Nacharbeit« erforderlich.

Die Konfiguration der Hashveröffentlichung erfolgt entweder in einem Gruppenrichtlinien-Objekt (wenn mehrere Server für die BranchCache-Nutzung aktiviert werden sollen) oder in der LOKALEN RICHTLINIE. Letztgenannte erreichen Sie, wenn Sie die MMC (*Microsoft Management Console*) öffnen und das Snap-In GRUPPENRICHTLINIENOBJEKT-EDITOR hinzufügen.

Wenn Sie BranchCache nur auf den dafür aktivierten Freigaben zulassen möchten, müssen Sie noch wissen, wie Sie die Dateifreigabe konfigurieren müssen. Nichts leichter als das (Abbildung 13.51):

- Öffnen Sie in der Verwaltung das Werkzeug FREIGABE- UND SPEICHERVERWALTUNG.
- Rufen Sie das Kontextmenü der Freigabe auf, und wählen Sie auf der Registerkarte FREIGABE die Schaltfläche ERWEITERT.
- In dem Dialog, der nun erscheint, wählen Sie BRANCHCACHE AKTIVIEREN. Falls diese Checkbox grau dargestellt, also nicht anwählbar ist, liegt das vermutlich darin, dass der Rollendienst nicht installiert ist.

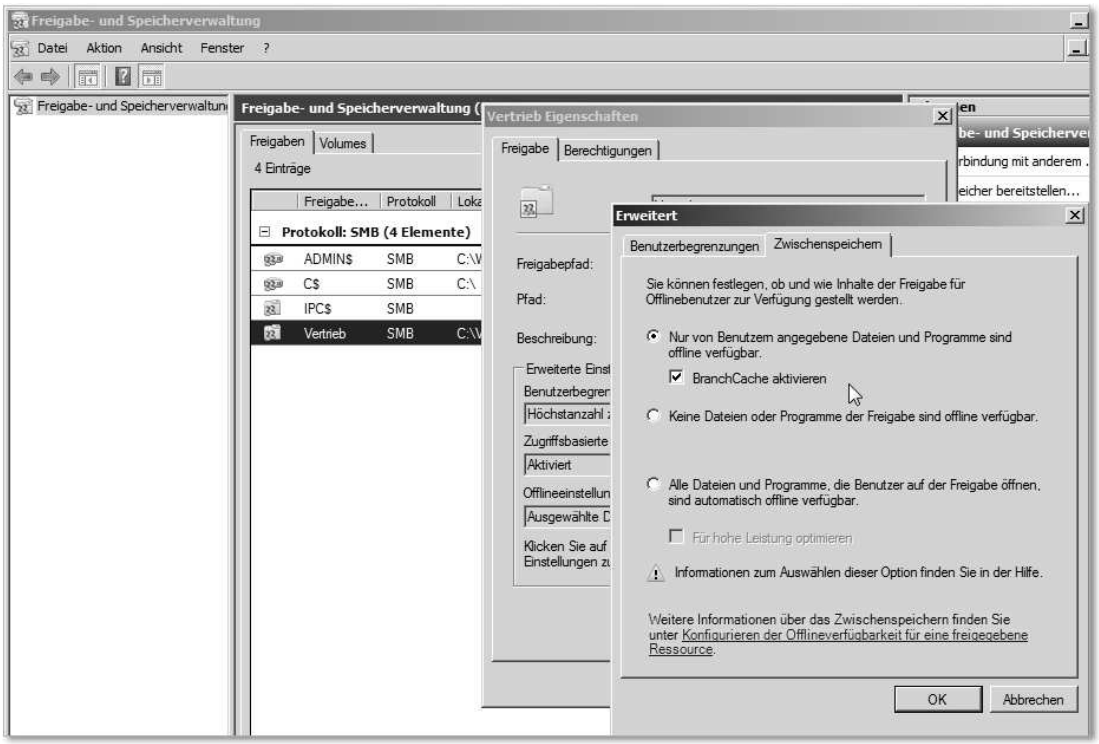


Abbildung 13.51 Für jede Dateifreigabe kann BranchCache separat aktiviert werden.

13.3.4 Clients konfigurieren

Auf den Windows 7-Clients (nur in den Versionen *Enterprise* und *Ultimate*!) ist die BranchCache-Software bereits installiert, allerdings muss die Funktion aktiviert werden. Dies erledigen Sie per Gruppenrichtlinie.

Die Einstellungen für BranchCache finden Sie unter COMPUTERVERWALTUNG • RICHTLINIEN • ADMINISTRATIVE VORLAGEN • NETZWERK • BRANCHCACHE. Sie konfigurieren dort beispielsweise, ob BranchCache überhaupt aktiv sein soll, in welchem Modus es betrieben wird oder wie viel Speicherplatz der Gesamtkapazität der Client zur Verfügung stellen soll (Abbildung 13.52).

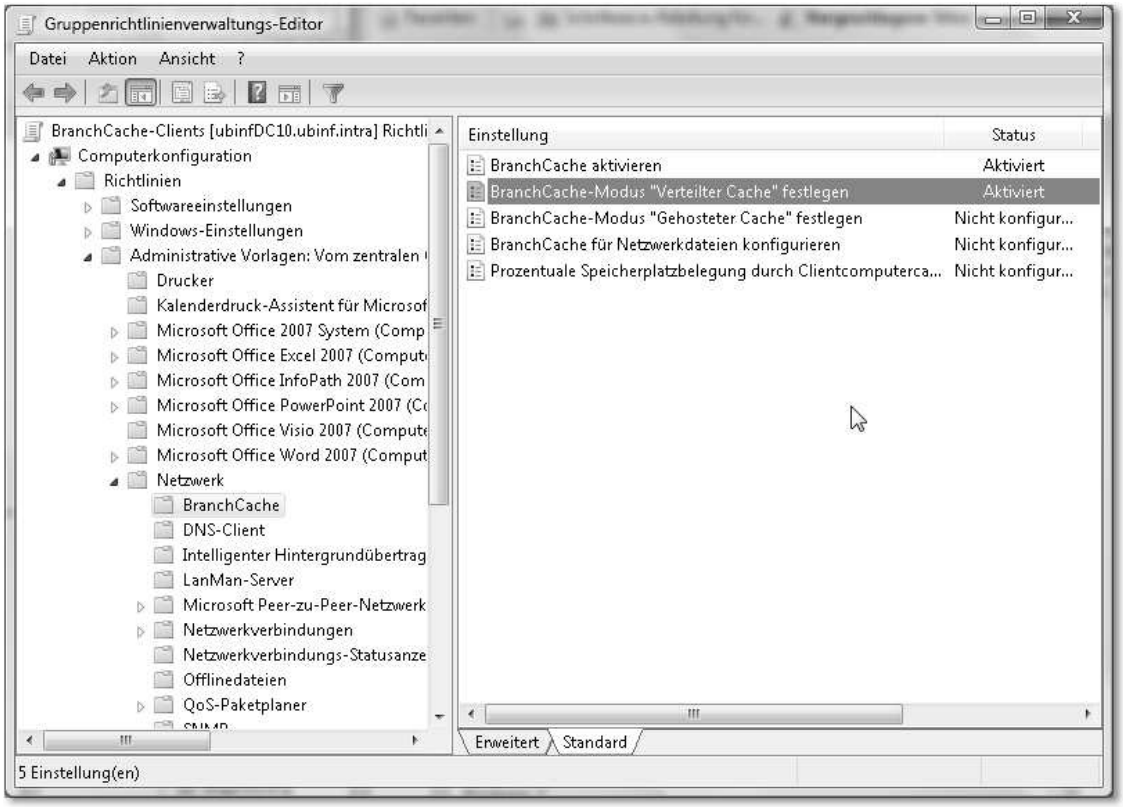


Abbildung 13.52 Die Grundkonfiguration der Clients erfolgt mit diesen Gruppenrichtlinien-Einstellungen.

Auf einem Windows 7-Client dürfte die Windows-Firewall aktiviert sein – wenn nicht: Gehen Sie über Los zurück, und ziehen nicht DM 4.000 ein. Im Ernst: Eine aktivierte Windows-Firewall auf einem Client ist im Jahr 2009 (und später) nicht akzeptabel.

Da bei der Aktivierung von BitLocker nicht automatisch die benötigten Löcher in die Windows-Firewall gebohrt werden, sollten Sie dies ebenfalls direkt erledigen – natürlich per Gruppenrichtlinie:

- Navigieren Sie im Gruppenrichtlinienobjekt-Editor zu dem auf Abbildung 13.53 gezeigten Konfigurationsbereich für die Windows-Firewall.
- Fügen Sie eine neue vordefinierte Regel hinzu, und zwar für den Inhaltsabruf (Abbildung 13.53).
- Eine zweite Regel wird, sofern Sie im Modus *Verteilter Cache* arbeiten, für die *Peerermittlung* benötigt – die PCs der Niederlassung sollen sich ja auch finden können. Wie Sie auf Abbildung 13.54 sehen können, gibt es drei vordefinierte BranchCache-Regeln, und die Peerermittlung ist auch dabei.

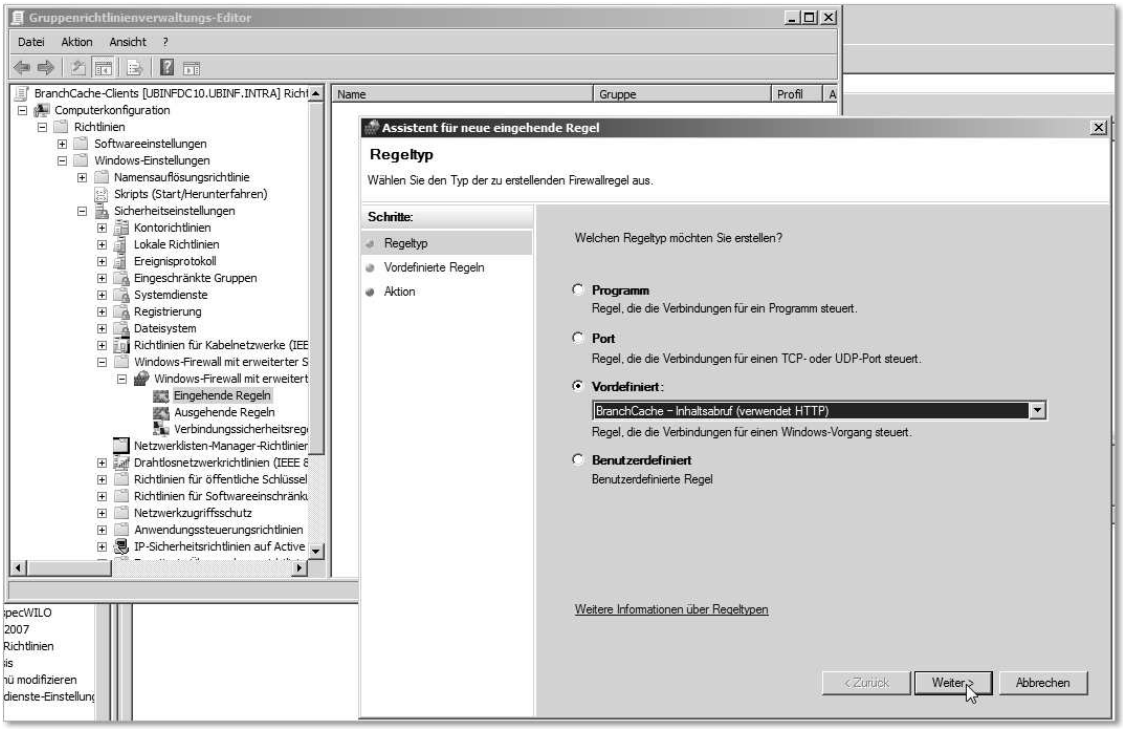


Abbildung 13.53 Zwei Firewallregeln müssen hinzugefügt werden – das geht auch per Gruppenrichtlinie.

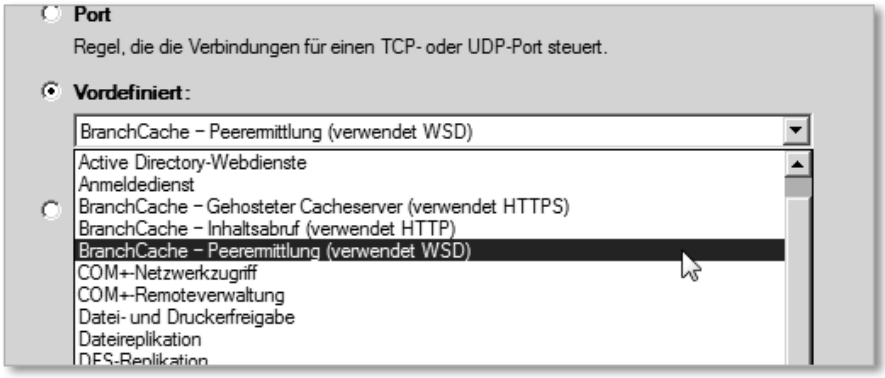


Abbildung 13.54 Es gibt drei vordefinierte Regeln für BranchCache.

Sie können nun die neu erstellte Gruppenrichtlinie auf einem Client anwenden (`gpupdate /force`) und mit dem Kommando `netsh branchcache show status all` kontrollieren, ob wirklich alles in Ordnung ist. Wenn beispielsweise eine Firewallregel fehlen würde, erhielten Sie einen entsprechenden Hinweis (Abbildung 13.55).

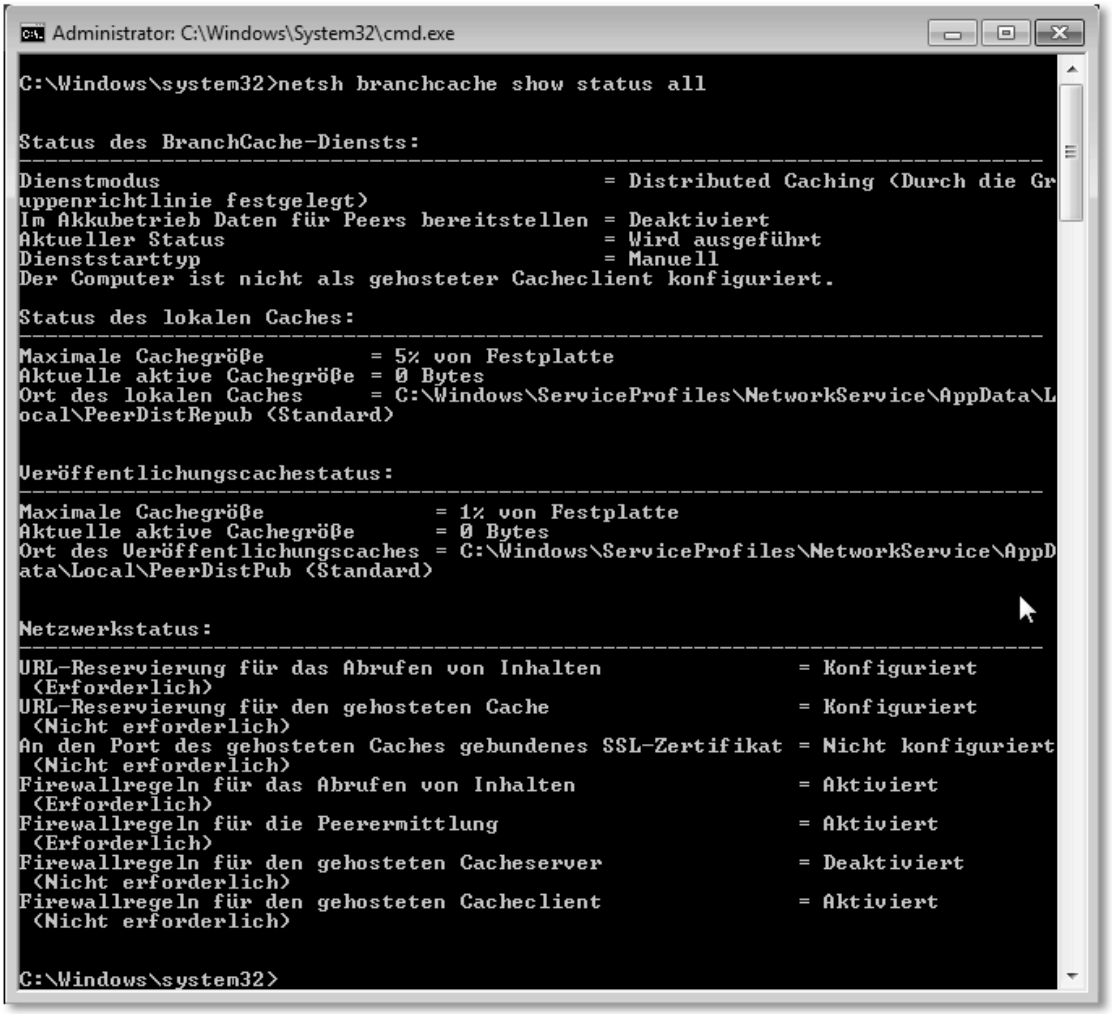


Abbildung 13.55 So sieht ein korrekt installierter BranchCache-Client für den Modus »Verteilter Cache« aus.

Sie können übrigens recht einfach kontrollieren, ob der Cache arbeitet. Das Kommando `netsh branchcache show status all` zeigt auch die aktuelle Speicherplatznutzung des Caches: Auf Abbildung 13.56 sind die ersten knapp 200 k eingetroffen.

Abbildung 13.56 Die ersten Bytes sind im lokalen Cache.

Falls Sie zunächst BranchCache im LAN ausprobieren oder aber sehr schnelle WAN-Verbindungen haben, werden Sie unter Umständen feststellen, dass Dateien von einem Dateiserver nicht gespeichert werden. Des Rätsels Lösung ist, dass Netzwerkdateien standardmäßig nur gespeichert werden, wenn die Roundtrip-Zeit der WAN-Verbindung größer als 80 ms ist. Diesen Wert können Sie mit der Gruppenrichtlinien-Einstellung aus Abbildung 13.57 ändern: Wenn Sie den Wert auf 0 setzen, wird immer zwischengespeichert, egal wie schnell die Verbindung ist.

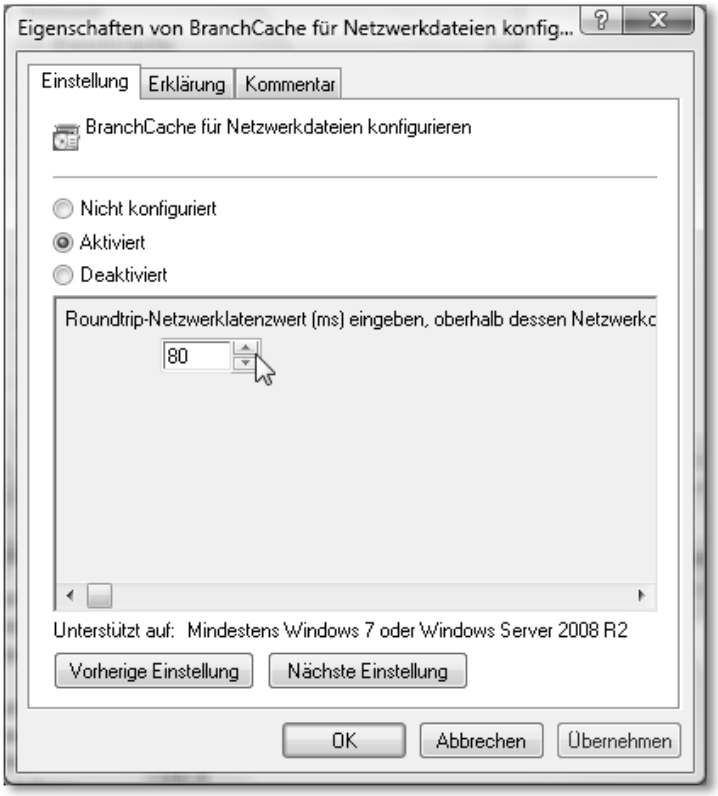


Abbildung 13.57 Dies ist ein wichtiger »Tuning-Parameter« für das Zwischenspeichern von Netzwerkdateien.

13.3.5 Hosted Cache

Die Aktivierung des Modus *Hosted Cache* gestaltet sich ebenfalls nicht weiter kompliziert. In den nächsten beiden Abschnitten zeige ich Ihnen, wie Sie vorgehen.

Konfiguration des Servers

Die Hosted-Cache-Funktion kann nur von einem *Windows Server 2008 R2* wahrgenommen werden, ein Windows 7-Client kann das nicht erfüllen.

Die erste vorbereitende Maßnahme ist, dass der Server, der als Hosted Cache fungieren soll, ein Computerzertifikat benötigt. Wenn Sie generell das *Auto Enroll-*

ment von Computerzertifikaten konfiguriert haben, dürfte das bereits der Fall sein, ansonsten müssten Sie ein Zertifikat von der eigenen PKI erzeugen lassen (das ist im Abschnitt 13.2.3, »Vorbereitende Maßnahmen« beschrieben). Im Klartext benötigen Sie also – mal wieder – eine eigene PKI.

Das Zertifikat muss sich im Zertifikatsspeicher »Computer« befinden. Wenn Sie das kontrollieren, können Sie direkt das Zertifikat anzeigen lassen und den Fingerabdruck kopieren (Abbildung 13.58).

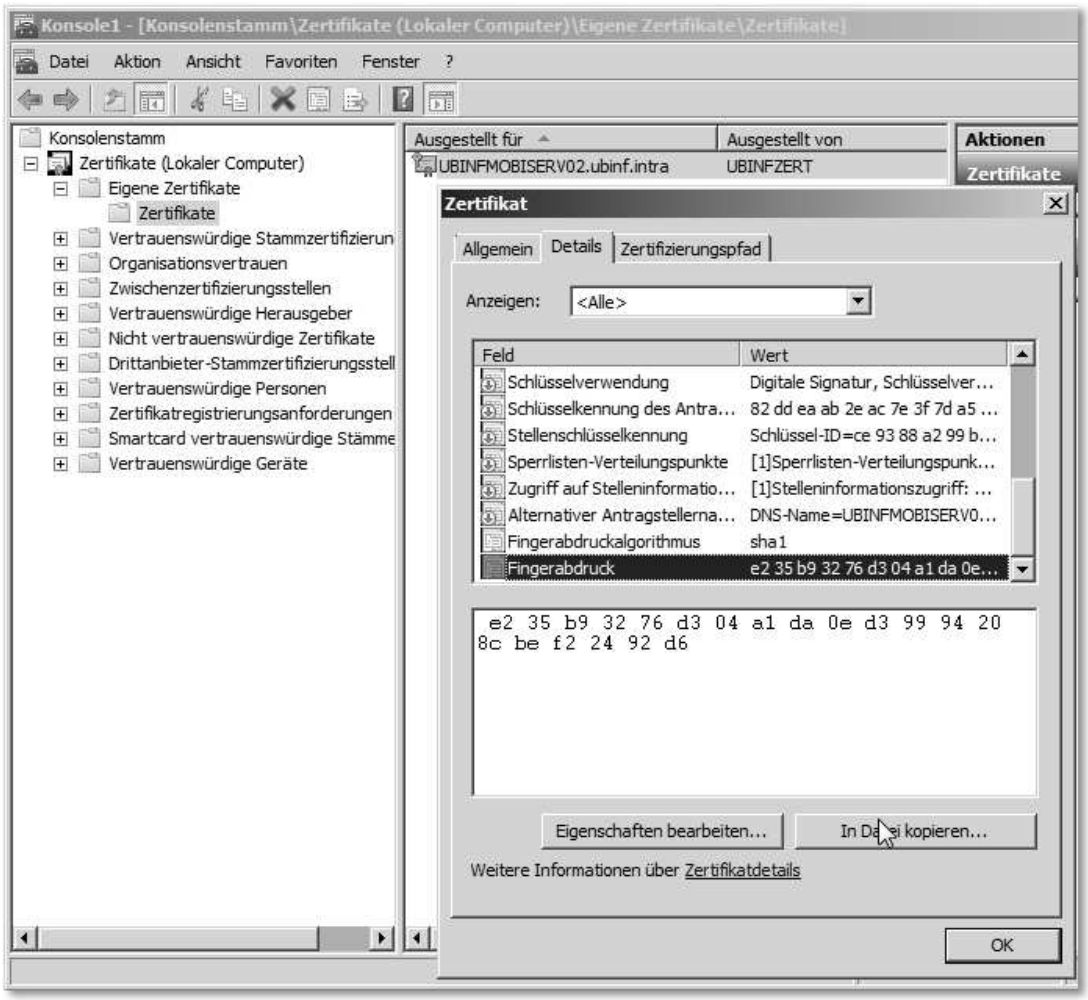


Abbildung 13.58 Der Server, der als Hosted Cache fungiert, benötigt ein Zertifikat.

Ist das Zertifikat vorhanden, können Sie mit der Installation starten, die zunächst aus dem Hinzufügen des BranchCache-Features besteht.

Dann ordnen Sie das Zertifikat der Anwendung (BranchCache) zu. Weiterhin macht es Sinn, den zur Verfügung stehenden Speicherplatz zu erweitern. Beide Maßnahmen müssen Sie mit dem *netsh*-Kommandozeilenwerkzeug vornehmen. Auf Abbildung 13.59 sind die Befehle gezeigt.

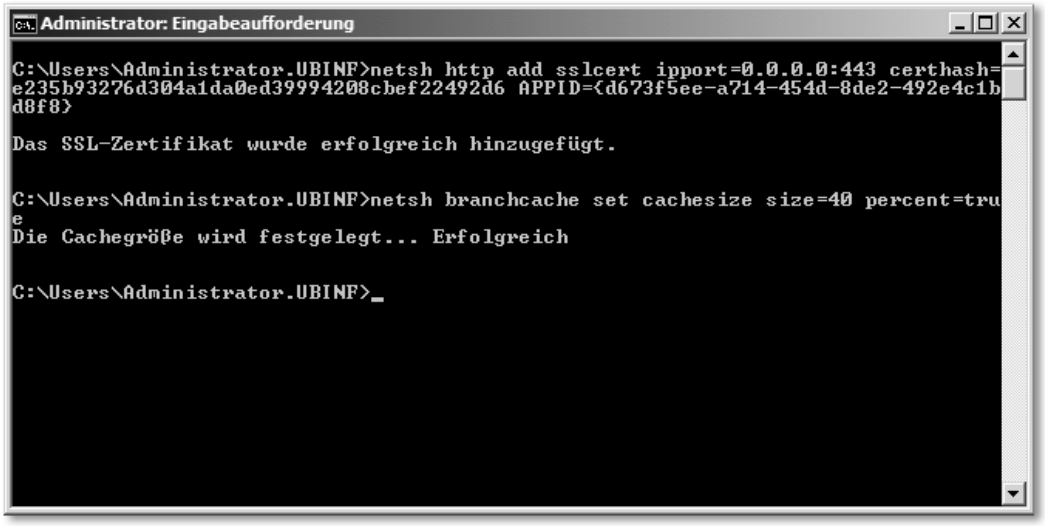


Abbildung 13.59 Installation des Zertifikats und Festlegen der Cachegröße

Clientkonfiguration

Die Clientkonfiguration nehmen Sie wie gewohnt über eine Gruppenrichtlinie vor: Sie müssen nur die auf Abbildung 13.60 gezeigte Einstellung setzen, in der der Speicherort des gehosteten Caches, also der Name des Servers, angegeben wird.

Beachten Sie, dass der Name exakt (!) mit dem Namen übereinstimmen muss, für den das Zertifikat ausgestellt ist.

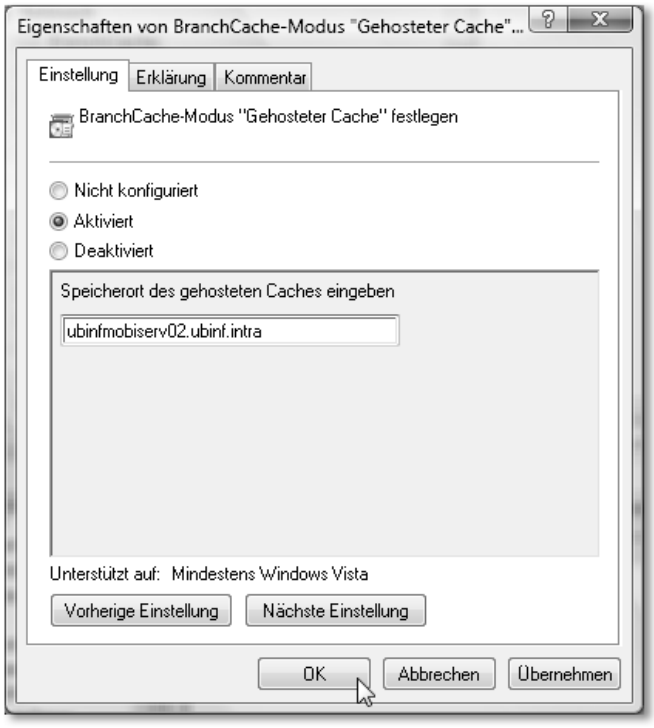


Abbildung 13.60 In der Gruppenrichtlinie wird der Speicherort des gehosteten Caches eingetragen.

13.3.6 Fazit

BranchCache dürfte sich in vielen Unternehmen als typisches *QuickWin* herausstellen: wenig Implementationsaufwand, keine Umgewöhnung für den Benutzer, aber »alles wird besser«.

Das Problem dürfte zunächst sein, dass die meisten Unternehmen und Organisationen ihre Datenbestände noch nicht auf *Windows Server 2008 R2*-Servern aufbewahren – und das ist eine Voraussetzung für die Nutzung von BranchCache.

13.4 VPN Reconnect

Wenn Sie über ein VPN auf Daten zugreifen, werden Sie folgendes Problem kennen: Sobald die VPN-Verbindung unterbrochen wird, wird der komplette Tunnel geschlossen und muss neu aufgebaut werden – mit mehr oder weniger großen Auswirkungen auf die Arbeitsumgebung. Zum Vergleich: Wenn eine »normale« Netzwerkverbindung kurzzeitig »weg« ist, beispielsweise weil Sie das Notebook aus der Dockingstation ziehen und auf WLAN-Betrieb umschalten, ist die Netzwerkverbindung »einfach wieder da«.

Gerade wenn der Verbindungsaufbau über eine Mobilfunkverbindung erfolgt, ist ein Verbindungsabbruch denkbar – und der VPN-Tunnel ist komplett weg.

Windows 7 löst das Problem mittels *VPN Reconnect*. Vereinfacht dargestellt funktioniert das so, dass der VPN-Tunnel auch bei einem Verbindungsabbruch für eine definierte Zeit erhalten bleibt. Sobald die Verbindung wieder aufgebaut werden kann, ist der VPN-Tunnel wieder aktiv, und Daten können übertragen werden. Das hört sich so weit gut an – und ist es auch. Der Haken an der Sache ist, dass es nicht mit PPTP-, L2TP- und SSTP-Verbindungen funktioniert. VPN Reconnect wird nur für den VPN-Typ IKEv2 unterstützt. Sie können das übrigens auch im Konfigurationsdialog erkennen (Abbildung 13.61):

- Wenn Sie als VPN-Typ IKEv2 wählen, ist die Schaltfläche Erweiterte Einstellungen aktiviert. (Auf dem Bild ist sie nicht zu sehen, da sie durch die Dropdown-Liste verdeckt wird.)
- In dem Dialog zur Konfiguration der erweiterten Eigenschaften haben Sie dann die Möglichkeit, eine Netzwerkausfall-Zeit zu konfigurieren. Dies ist die Zeit, während der ein VPN-Tunnel aufrechterhalten wird, obwohl die Verbindung nicht mehr vorhanden ist. Nach Ablauf der hier definierten Zeit ohne Verbindung muss der VPN-Tunnel neu aufgebaut werden.

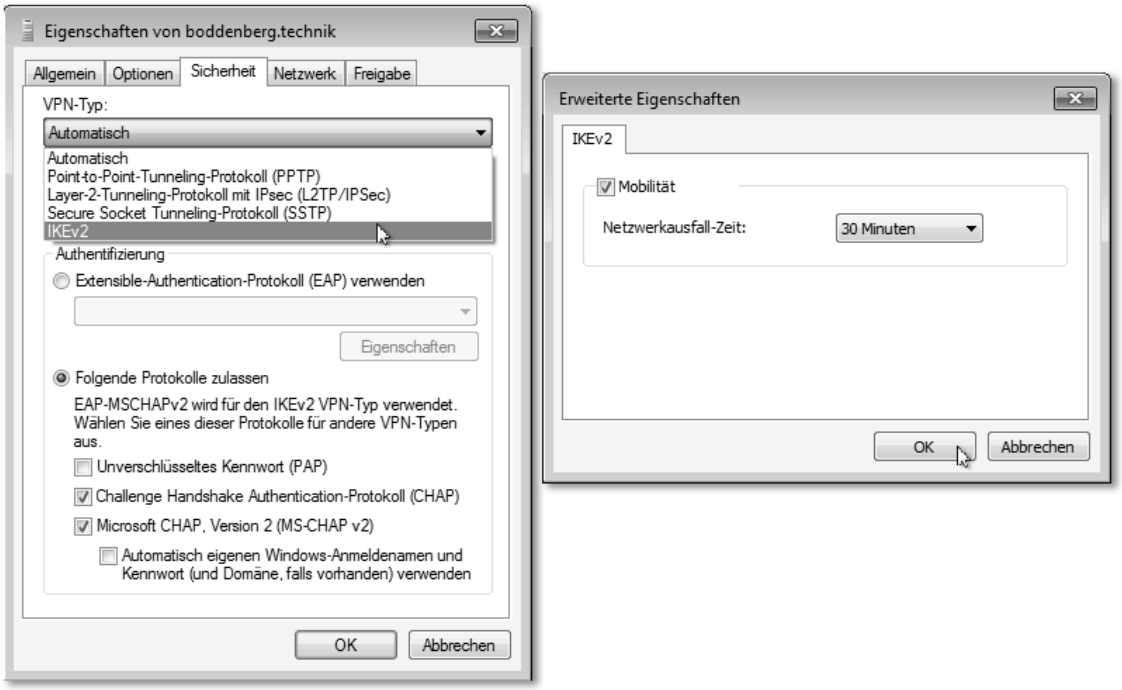


Abbildung 13.61 VPN Reconnect steht nur beim VPN-Typ IKEv2 zur Verfügung.

13.5 Mobile Broadband

Die Anzahl der mobilen Benutzer, die für den Verbindungsaufbau UMTS verwenden, dürfte nach wie vor deutlich steigen. Da mittlerweile etliche Notebooks bereits ab Werk mit eingebauten UMTS-Modems und im Deckel befindlichen Antennen bestellbar sind, dürfte die Attraktivität dieser für mobile Menschen wirklich praktischen Verbindungsmöglichkeit noch steigen – zumal UMTS-Flatrates im absolut bezahlbaren Rahmen liegen. Wenn ich einen Blick in die Zukunft wagen soll, würde ich sagen, dass in absehbarer Zeit die werksseitige Ausstattung eines Notebooks mit UMTS genauso normal sein wird wie mit WLAN.

Leider ist bisher (!) die Nutzung von UMTS nicht so unproblematisch wie die WLAN-Nutzung. Der Grund ist, dass die Steuerung und Verwaltung der WLAN-Konnektivität seit Urzeiten (na ja, seit XP) fest in das Windows-Betriebssystem integriert ist, während für die UMTS-Nutzung die Software der Kartenhersteller bzw. Mobilfunkprovider genutzt werden muss. Um es einmal vorsichtig zu formulieren, ist die Begeisterung der Anwender im Allgemeinen eher nicht so sonderlich hoch. Das beginnt bei umständlicher Bedienung und nicht immer stabiler Funktion und endet bei schlechter Automatisierbarkeit der Installation und mangelhafter Verwaltbarkeit – viele Unternehmen haben ja nicht nur ein oder zwei UMTS-Notebooks, sondern unter Umständen Hunderte. Somit ist ein zentralisiertes Management eigentlich Pflicht.

Mit Windows 7 gibt es Abhilfe: Ein neues Treibermodell namens *Mobile Broadband* ist vorhanden. Mit Mobile Broadband wird die Steuerung der UMTS-Konnektivität genauso nahtlos in Windows integriert sein, wie Sie das vom WLAN kennen.

Voraussetzung ist, dass die jeweiligen Kartenhersteller entsprechende *Mobile-Broadband*-kompatible Treiber liefern. Erfreulicherweise haben die wesentlichen Hersteller (wie beispielsweise *Option* und *Qualcomm*) bereits Anfang 2009 ihre Zusage für die Unterstützung dieses Modells gegeben.

Zu dem Zeitpunkt, als dieses Buch geschrieben wurde, lagen mir allerdings noch keine *Mobile-Broadband*-fähigen UMTS-Karten vor, sodass ich die Funktionalität nicht vorführen kann.

Kyros nahm die Vertriebenen auf, zog ein Heer zusammen, belagerte Milet zu Wasser und zu Land und suchte die Verbannten wieder in ihr Vaterland zurückzuführen. Dies war für ihn ein zweiter Vorwand, Truppen zu sammeln.

14 Suchen und Finden

Die meisten meiner Kunden messen Ihre Datenbestände mittlerweile in Terabytes. In Gesprächen kommt irgendwann der Punkt, an dem es heißt: »Wir haben zwar ohne Ende Daten, aber das ist ein einziges großes Datengrab. Bis auf 5 % könnten wir alles löschen, und keiner würde es merken«.

Vielleicht (!) würde sich der Budget-Verantwortliche für die Beschaffung der Speichersysteme sogar freuen, wenn er eine Weile keine Investitionen zu tätigen braucht – langfristig wäre das aber ein fataler Ansatz.

Ich zitiere an dieser Stelle gern Paul »Red« Adair, der Ölbohrplattform-Feuerwehrmann. Ich habe ein Interview gelesen, in dem er gefragt wurde: »Paul, Du machst mit Deinem Team einen gefährlichen Job, aber Ihr habt nie einen Kollegen im Einsatz verloren. Woran liegt das?« Paul antwortete sinngemäß, dass er alles aufschreibt und somit über eine immense Wissensquelle verfügt, die er im Laufe der Jahre selbst geschaffen hat.

Es kann nicht schaden, sich ein wenig an Paul zu orientieren: Das Video von Ihrer Firmenweihnachtsfeier von 2001 hat sicherlich nur einen gewissen Kuriositätenwert, eine Projektdokumentation aus demselben Jahr könnte aber durchaus eine wertvolle Hilfe sein, falls damals eine Fragestellung bearbeitet wurde, die sich gerade wieder stellt.

Ihre Daten sind also nicht lästiger Ballast, den man vorhalten, sichern und gegebenenfalls wiederherstellen muss, sondern wertvolles Unternehmenswissen. Gut, es kann durchaus Grenzwertiges geben (wie das Video der Firmenweihnachtsfeier), aber im Allgemeinen sind Ihre Daten erstens zu wertvoll, um gelöscht zu werden, und zweitens ebenfalls zu wertvoll, um nicht gefunden zu werden.

Ich reite deshalb so auf dem Thema »Unternehmenswissen« herum, weil immer wieder gern angeführt wird, dass man viel Speicherplatz sparen könne, wenn die Benutzer den »ganzen alten Krempel« löschen würden. Als Hilfsmittel zur Benut-

zerdisziplinierung wird dann über Quotas nachgedacht, und es werden E-Mails herumgeschickt, die besagen, dass man bitte alles löschen möge, was nicht unbedingt gebraucht wird.

Nein, ich bin nicht für die Verschwendung von Speicherplatz, ich bin aber noch viel weniger dafür, Unternehmenswissen zu löschen.

Damit aus dem Datengrab jedoch tatsächlich nutzbares Unternehmenswissen wird, ist es erforderlich, dass die Benutzer auch eine realistische Chance haben, Daten wiederzufinden. Es gibt zwei einander ergänzende Ansätze:

- Es hat sich im Laufe der Zeit gezeigt, dass das Dateisystem als Dokumentablage (oder besser: Wissensspeicher) maximal ungeeignet ist. In einem Dateisystem kann im Grunde genommen nur eine hierarchische Baumstruktur implementiert werden, und es ist nicht möglich, Dokumente mit zusätzlichen Metadaten zu versehen. Mit Systemen wie *SharePoint* lässt sich hier gewaltig etwas tun – das ist aber nicht Thema dieses Buchs.
- Neben einer besseren Organisation und Strukturierung der Daten wäre es hervorragend, »einfach« per Stichworteingabe suchen zu können. Eine für den Benutzer recht simple Stichwortsuche, wie sie beispielsweise von Google angeboten wird, liefert zwar auch eine Menge Informations-Schrott, ist aber trotzdem extrem hilfreich.

Suchtechnologien

Suche ist generell ein wichtiges Thema für Microsoft. Neben der in Windows integrierten Suche gibt es eine Produktfamilie *Enterprise Search*, zu der beispielsweise der *Search Server 2008* und die Suchfunktionalität im *SharePoint Server 2007* zählen.

Suchtechnologien sind kein Thema für dieses Buch, ich möchte es Ihnen aber ans Herz legen, sich damit zu beschäftigen. Ein erster Anlaufpunkt kann die Website *http://www.microsoft.com/enterprisesearch/en/us/default.aspx* sein.

14.1 Die Desktop-Suche

Dies Desktop-Suche ist grundsätzlich nicht neu, bereits zu Zeiten von *Windows XP* gab es diese Funktionalität zum Nachinstallieren. *Windows Vista* wurde standardmäßig damit ausgeliefert, und *Windows 7* enthält die derzeit aktuelle Version.

Vielleicht fragen Sie sich, warum man sich in einem Unternehmensnetz überhaupt mit Desktop-Suche beschäftigen soll – schließlich sollen die Daten ja auf Servern und nicht auf Clients gespeichert werden. Die lokale Suche von Windows 7 bedient auch jenseits solcher Themen wie *Search Federations* nicht nur das Durchsuchen von Dateien:

- Die Suche hilft Ihnen, schnell Programme zu finden.
- Die Suche unterstützt Sie beim Finden von Elementen in Ihrem Postfach.

14.1.1 Funktion für den Anwender

Zunächst gebe ich Ihnen einen kurzen Überblick über die Standard-Suchfunktionen für den Anwender. Gibt der Anwender im Suchfeld des Startmenüs einen Begriff an, werden die Suchergebnisse gegliedert nach Programmen, Dokumenten und Outlook-Objekten angezeigt (Abbildung 14.1). Auch um System-Werkzeuge wie beispielsweise *regedit* zu finden, verwende ich diese Funktion. Um Word zu starten, gebe ich übrigens einfach »Word« im Suchfeld an und klicke mich nicht durch das Startmenü.

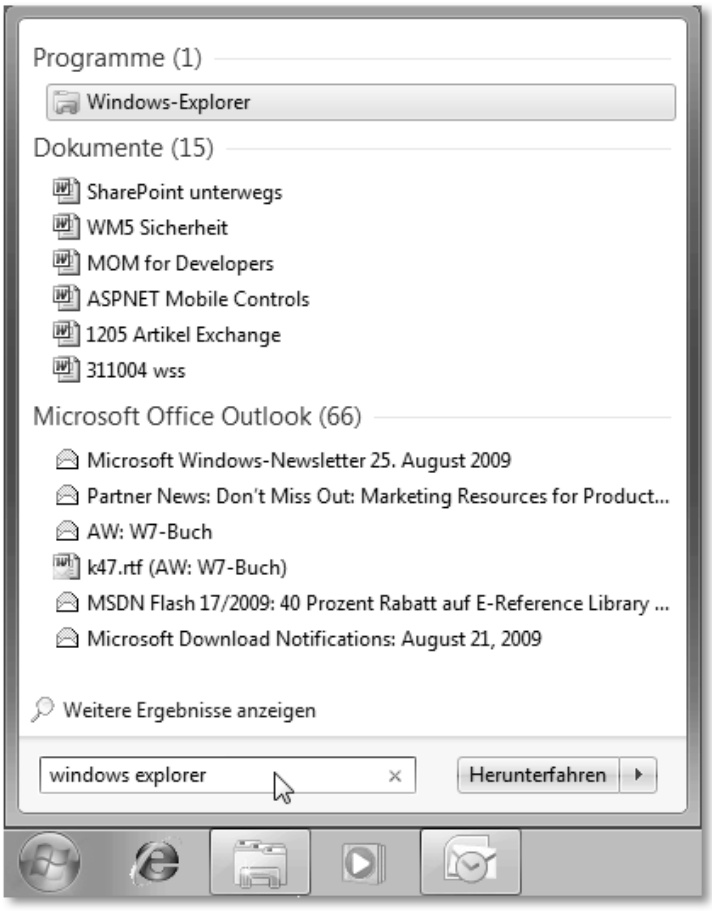


Abbildung 14.1 Ohne dass etwas konfiguriert werden müsste, findet die Desktop-Suche Programme und lokale Inhalte.

Weiterhin gibt es natürlich weiterhin ein Suchfeld im Windows-Explorer. Um die Suche einzugrenzen, können die Anwender Filterkriterien definieren (Abbildung 14.2). Sie werden übrigens feststellen, dass die Suche sehr flott ist – vorausgesetzt, es wird nicht mit einem prähistorischen PC gearbeitet.

Zu erwähnen ist noch, dass die Suche keine Sicherheitslücke darstellt. Der Fall ist vielleicht ein wenig konstruiert, verdeutlicht aber das Prinzip: Wenn sich zwei Benutzer einen PC teilen, findet der eine Benutzer nicht die Dateien des anderen. Auch die Anzeige des Dateinamens könnte (!) ja schon geheime Informationen verraten – keine Sorge, das passiert nicht.

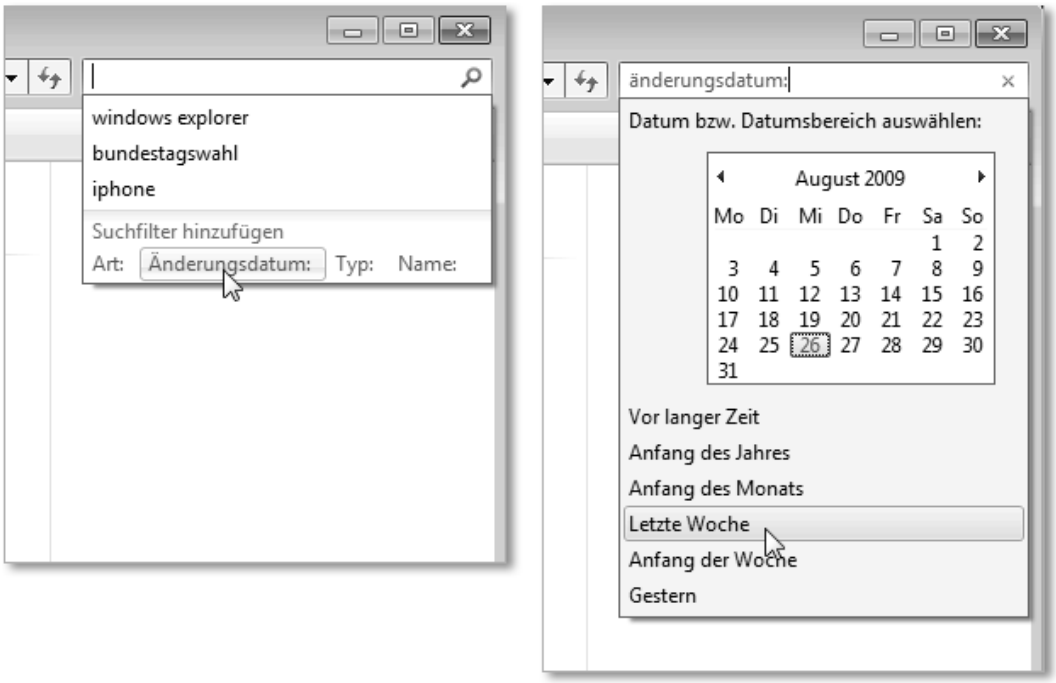


Abbildung 14.2 Die Benutzer können mit Filtern arbeiten.

14.1.2 Konfiguration über Gruppenrichtlinien

Die lokale Suche kann selbstverständlich über Gruppenrichtlinien konfiguriert werden. Die wesentlichen Stellen sind:

- Computerkonfiguration • Richtlinien • Administrative Vorlagen • Windows-Komponenten • Suche
- Benutzerkonfiguration • Richtlinien • Administrative Vorlagen • Windows-Komponenten • Suche

Es gibt darüber hinaus noch einige andere interessante Optionen. So können Sie beispielsweise in Benutzerkonfiguration • Richtlinien • Administrative Vorlagen • Startmenü und Taskleiste ein Suchfeld im Startmenü einblenden lassen.

Auf Abbildung 14.3 ist der Konfigurationsabschnitt Suche der Computerkonfiguration gezeigt. Sie sehen, dass es schon allein hier eine erhebliche Menge von Konfigurationsoptionen gibt – 30 Stück.

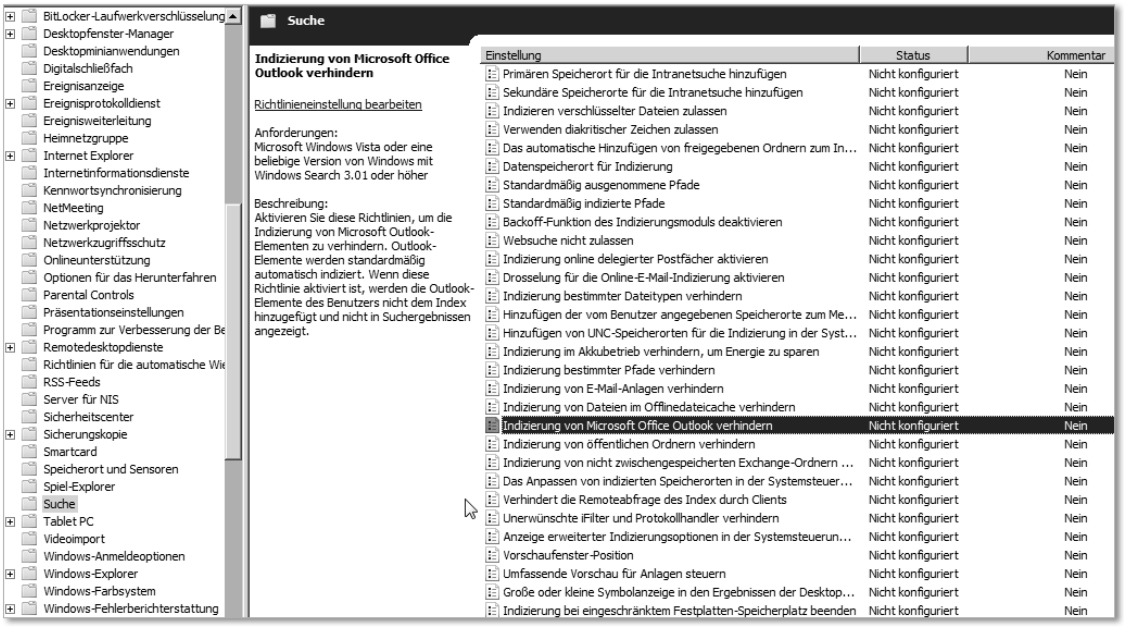


Abbildung 14.3 Die Suche kann mithilfe von Gruppenrichtlinien konfiguriert werden.

14.2 Search Federations

Die zuvor beschriebene klassische Desktop-Suche »krankt« daran, dass sie eben nur lokale Inhalte durchsuchen kann. Die Möglichkeit, auch externe Inhalte auf komfortable integrierte Weise zu durchsuchen, wäre durchaus attraktiv – und das lässt sich mit *Search Federations* realisieren. Kurz gesagt geht es darum, dass externe Suchindizes aus der Windows 7-Suchoberfläche heraus angesprochen werden können. Die Suchergebnisse (beispielsweise von einer Suche in Ebay oder YouTube) werden dann so angezeigt, als wenn es sich um lokale Inhalte handeln würde. Ebendies gilt übrigens auch für Suchergebnisse von internen Systemen wie *Search Server* oder der Suche von *SharePoint Server*.

Search-Federation-Konzept

Das *Search-Federation*-Konzept ist übrigens nichts, was Microsoft allein und völlig proprietär entwickelt hätte. Weitere Informationen finden Sie unter *http://www.opensearch.org*.

Der Definition des Zugriffs auf die Inhaltsquellen erfolgt über Suchconnectoren. Diese werden mit einer *.osdx*-Datei definiert. Hat ein Windows 7-System Zugriff auf eine solche Datei, findet sich in deren Kontextmenü der Menüpunkt SUCHCONNECTOR ERSTELLEN.

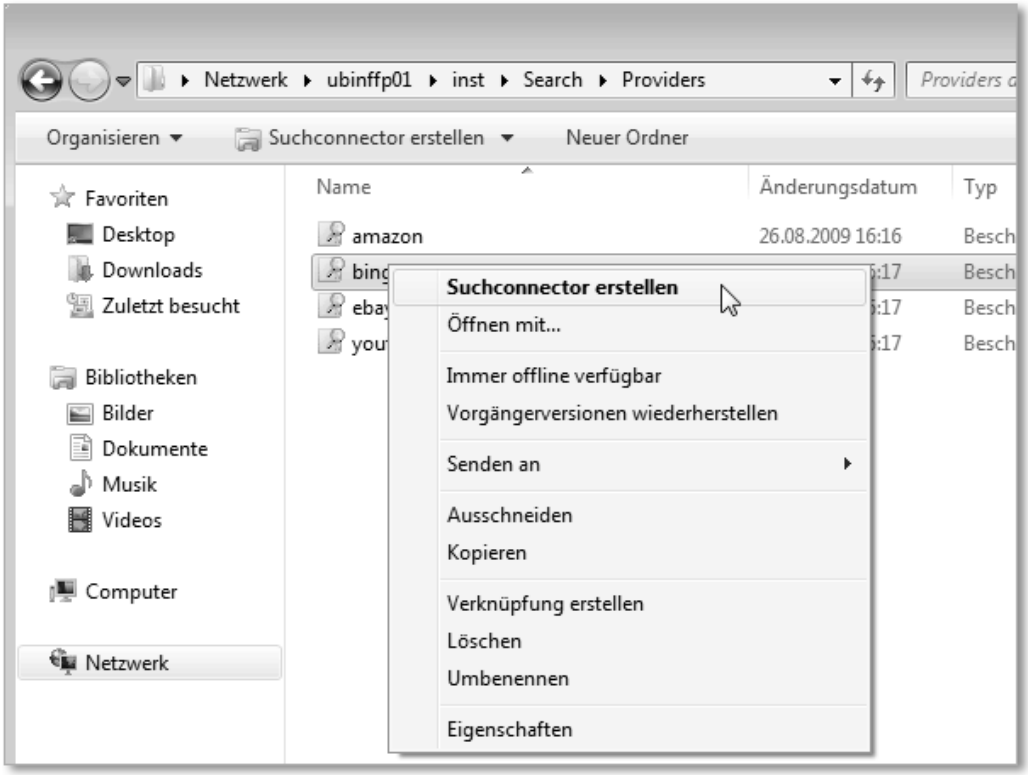


Abbildung 14.4 Eine .osdx-Datei enthält die Definition für eine externe Suchquelle. Daraus kann ein Suchconnector hinzugefügt werden.

Eine *.osdx*-Datei ist nichts dramatisch Kompliziertes. Es handelt sich, wie das »X« am Ende vermuten lässt, um ein XML-Dokument. Listing 14.1 zeigt eine Definitionsdatei zum Zugriff auf Microsofts Suchmaschine *Bing*.

Dies ist nun zwar nur ein ganz simples Beispiel, zeigt aber in etwa Aufbau und Möglichkeiten. Wenn Sie mithilfe von *Google* oder *Bing* Beispiele für *.osdx*-Dateien suchen, werden Sie Beispiele für die wesentlichen Quellen finden.

```
<?xml version="1.0" encoding="UTF-8"?>

<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/"
 xmlns:ms-ose="http://schemas.microsoft.com/opensearchext/2009/">

 <ShortName>Bing!</ShortName>

 <Description>Search Bing via Windows 7 Search.</Description>

 <URL type="application/rss+xml" template="http://www.bing.com/
search?q={searchTerms}&amp;format=rss"/>

 <URL type="text/html" template="http://www.bing.com/
search?q={searchTerms}"/>

</OpenSearchDescription>
```

Listing 14.1 Definition eines Providers zum Durchsuchen von Microsofts Suchmaschine Bing

Wenn Sie (wie auf Abbildung 14.4 gezeigt) einen Suchconnector hinzufügen, wird zunächst die Sicherheitsabfrage aus Abbildung 14.5 erfolgen. Websites könnten zukünftig durchaus *.osdx*-Dateien zum Download anbieten, mit denen sich diese recht einfach in die Suche einbinden lassen – eine kurze Besinnung, ob für die eine oder andere Website wirklich ein Suchconnector hinzugefügt werden soll, kann wohl nicht schaden.

Das eigentliche Hinzufügen des Suchconnectors ist in Sekundenbruchteilen erledigt. Danach wird der Suchconnector in den Favoriten vorhanden sein – und Sie können mit dem Durchsuchen der Quelle beginnen (Abbildung 14.6).

Abbildung 14.5 Sicherheitsabfrage vor dem Hinzufügen des Suchconnectors

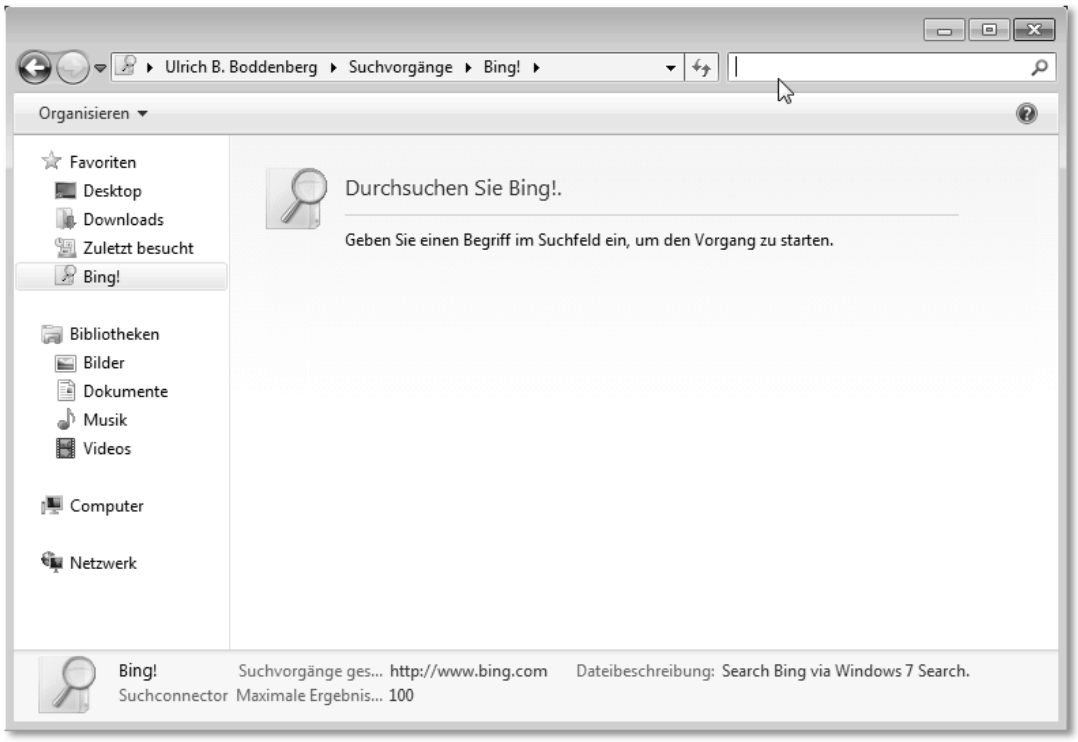


Abbildung 14.6 Nach dem Hinzufügen des Suchconnectors können Sie direkt mit Suchen beginnen.

Abbildung 14.7 zeigt das Ergebnis einer Suche bei *Bing*. Sie sehen, dass der BING-Eintrag in den Favoriten ausgewählt werden muss, dann wird einfach der Suchbegriff eingegeben – und kurze Zeit später sind die Ergebnisse da. Wenn Sie das Vorschaufenster aktivieren, werden die gefundenen Inhalte dort angezeigt.

Auf Abbildung 14.8 ist zu sehen, dass die Darstellung der Suchergebnisse nicht nur rein textbasiert erfolgen kann, vielmehr können auch im Suchergebnis enthaltene Bilder angezeigt werden – im Bild sehen Sie eine Suche bei *YouTube*.

Um die Vorteile von Search Federations zu erkennen, müssen Sie den Arbeitsprozess des Benutzers durchdenken. Auf den ersten Blick ist es nämlich gar nicht unbedingt »der große Hit«: Na ja, man kann aus dem Explorer heraus externe Ressourcen wie *Bing* oder *YouTube* durchsuchen oder auch auf die Suchergebnisse des *SharePoint Servers* zugreifen. Und? Das kann man mit den jeweiligen Weboberflächen genauso gut, vielleicht sogar noch etwas besser.

Der Charme der Lösung liegt nun gerade darin, dass es eben unter *einer* Oberfläche passieren kann. Die Anwender können mit einem Mausklick unterschiedliche Quellen abfragen und müssen nicht extra die zugehörigen Websites aufrufen. Etwas pathetisch ausgedrückt bringen Sie das Wissen des Unternehmens oder gar das Wissen der Welt in den Windows-Explorer – und es ist mit zwei Mausklicks abrufbar.

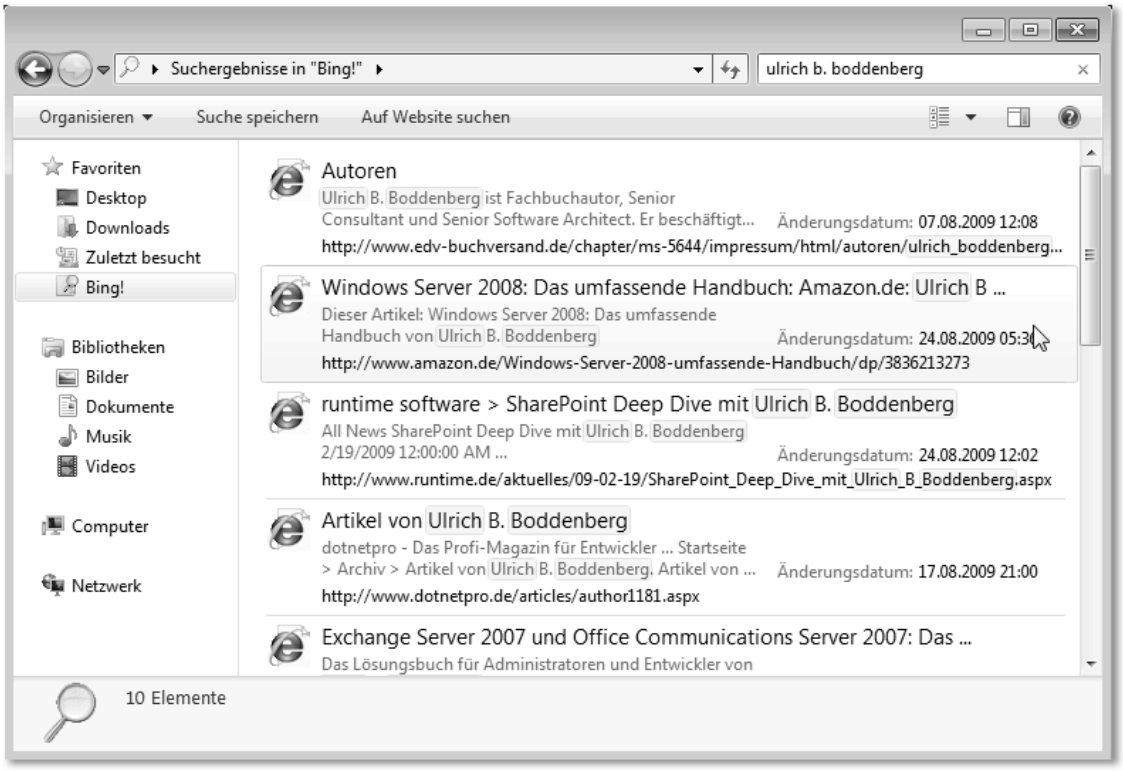


Abbildung 14.7 Die Ergebnisse eines Suchvorgangs bei Bing

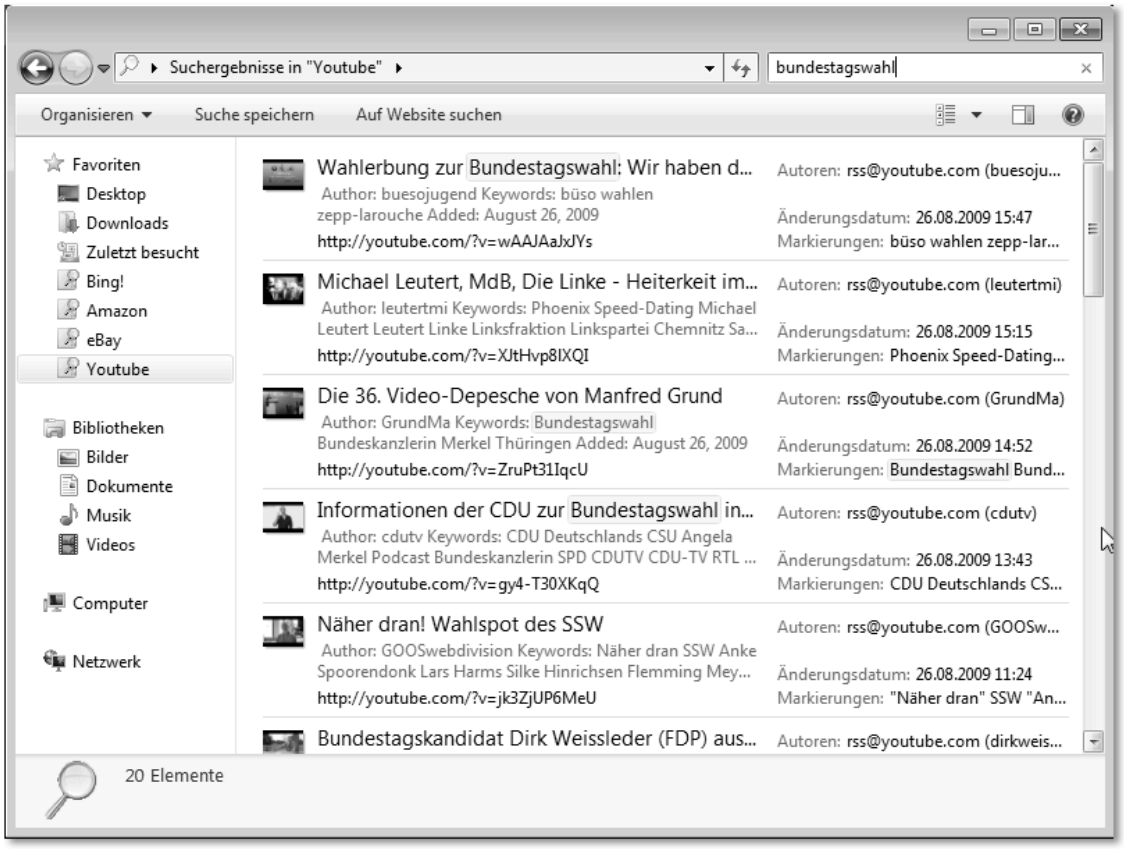


Abbildung 14.8 Bei der YouTube-Suche wird deutlich, dass auch eine komplexere Präsentation der Suchergebnisse, beispielsweise mit einem kleinen Bild, erfolgen kann.

14.3 Bibliotheken

Wenn Sie ein wenig im Windows-Explorer herumgeklickt haben, werden Sie mehr oder weniger bewusst die Bibliotheken wahrgenommen haben (Abbildung 14.9). Auf den ersten Blick erinnert das zwar sehr an die EIGENEN DATEIEN, aber Bibliotheken sind erstens neu, und zweitens können sie auch mehr als ein simpler Unterordner in den EIGENEN DATEIEN.

Im Kontextmenü des Knotens BIBLIOTHEKEN findet sich ein Menüpunkt zum Erstellen einer neuen Bibliothek. In Abbildung 14.10 habe ich eine neue Bibliothek namens ZEITSCHRIFTEN angelegt; es wird der Hinweis angezeigt, dass noch keine Ordner in diese neue Bibliothek aufgenommen wurden, sie ist also leer. Der Bibliothek können ein oder mehrere Ordner hinzugefügt werden. Dabei werden keine Dateien bewegt. Eine Bibliothek ist also sozusagen eine Sammlung von Links auf Ordner, die lokal oder im Netzwerk liegen können.

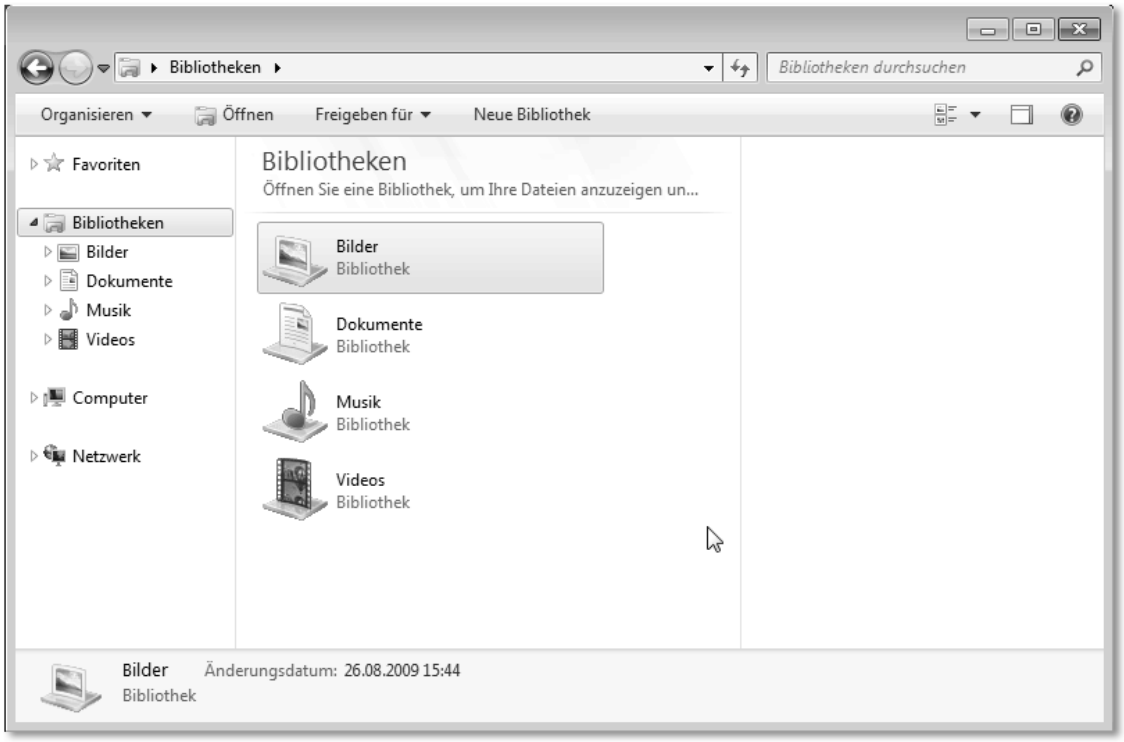


Abbildung 14.9 Neu in Windows 7: die Bibliotheken

Wenn Sie einen Netzwerkordner hinzufügen möchten, muss eine der folgenden Voraussetzungen erfüllt sein:

- Der Inhalt der Freigabe muss auf dem PC offline zur Verfügung stehen.
- Die Freigabe muss auf dem Dateiserver indiziert worden sein.

Sofern beides nicht zutrifft, erscheint die auf Abbildung 14.11 gezeigte Fehlermeldung: Nicht indizierte Netzwerkadressen können nicht in eine Bibliothek aufgenommen werden.

Abbildung 14.10 Einer Bibliothek können Sie beliebig viele bestehende Ordner hinzufügen.

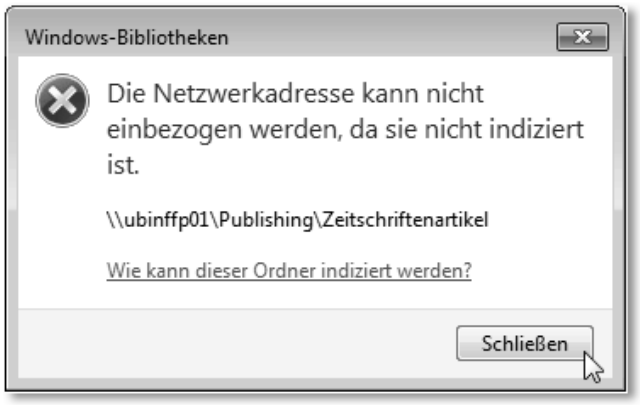


Abbildung 14.11 Nicht indizierte Netzwerkfreigaben können einer Bibliothek nicht hinzugefügt werden.

14.3.1 Dateifreigabe indizieren und zu Bibliothek hinzufügen

Auch wenn Sie auf einem *Windows Server 2008* oder *Windows Server 2008 R2* die Rolle DATEISERVER installiert haben, ist die Suche nicht aktiv (Abbildung 14.12). Ihre erste Aufgabe ist es also, den Rollendienst WINDOWS SEARCH hinzuzufügen. Das Hinzufügen eines Rollendiensts zu einer bestehenden Rolle wird aus dem Server-Manager initiiert. In dem Installationsassistenten wählen Sie einfach den Rollendienst aus – mehr ist (fast) nicht zu tun (Abbildung 14.13).

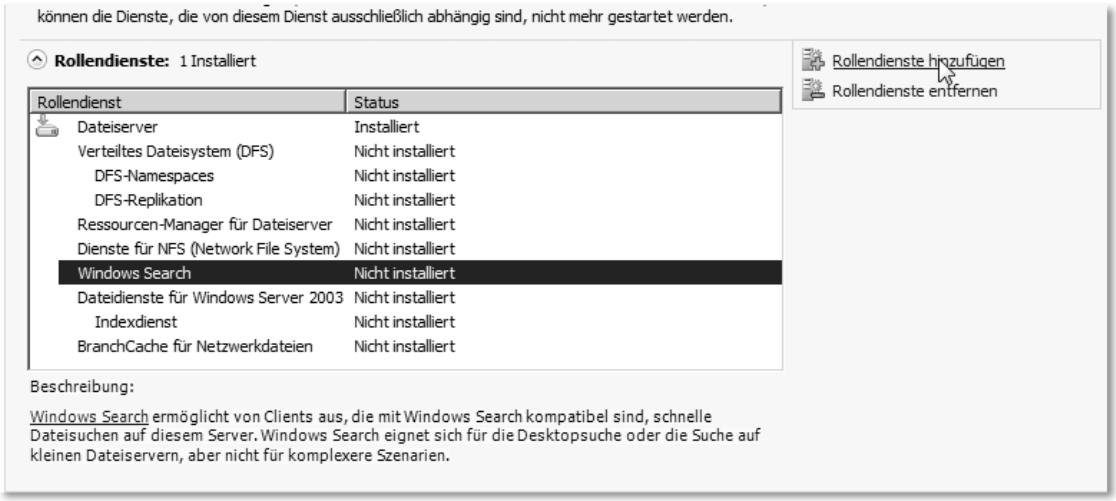


Abbildung 14.12 Der Rollendienst »Windows Search« ist standardmäßig nicht installiert.

Der Installationsassistent wird direkt von Ihnen wissen wollen, welche Volumes indidziert werden sollen. Auf Abbildung 14.14 können Sie allerdings sehen, dass die Festlegung hier nur sehr allgemein für das komplette Volume getroffen werden kann. In vielen Fällen dürfte das nicht ausreichen.

Stellen Sie sich beispielsweise einen sehr großen Fileserver mit einem 2 TB großen Volume vor, von dem nur ein Viertel mit *Windows Search* und der Rest mit

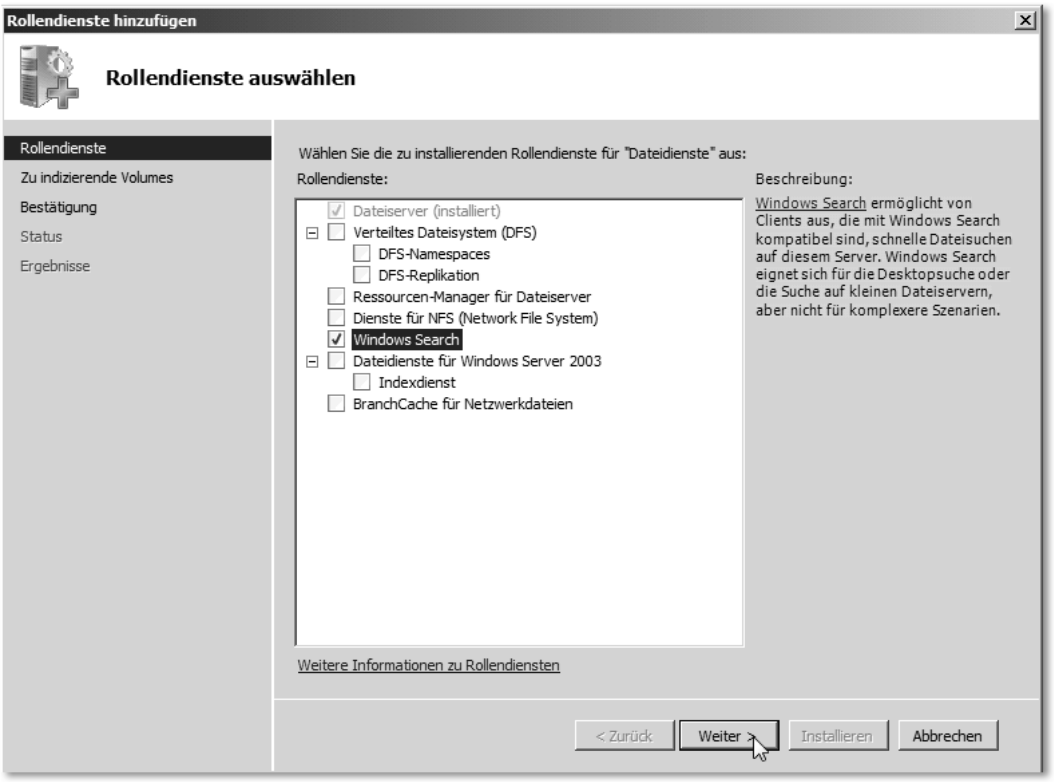


Abbildung 14.13 Hinzufügen des Rollendiensts »Windows Search«

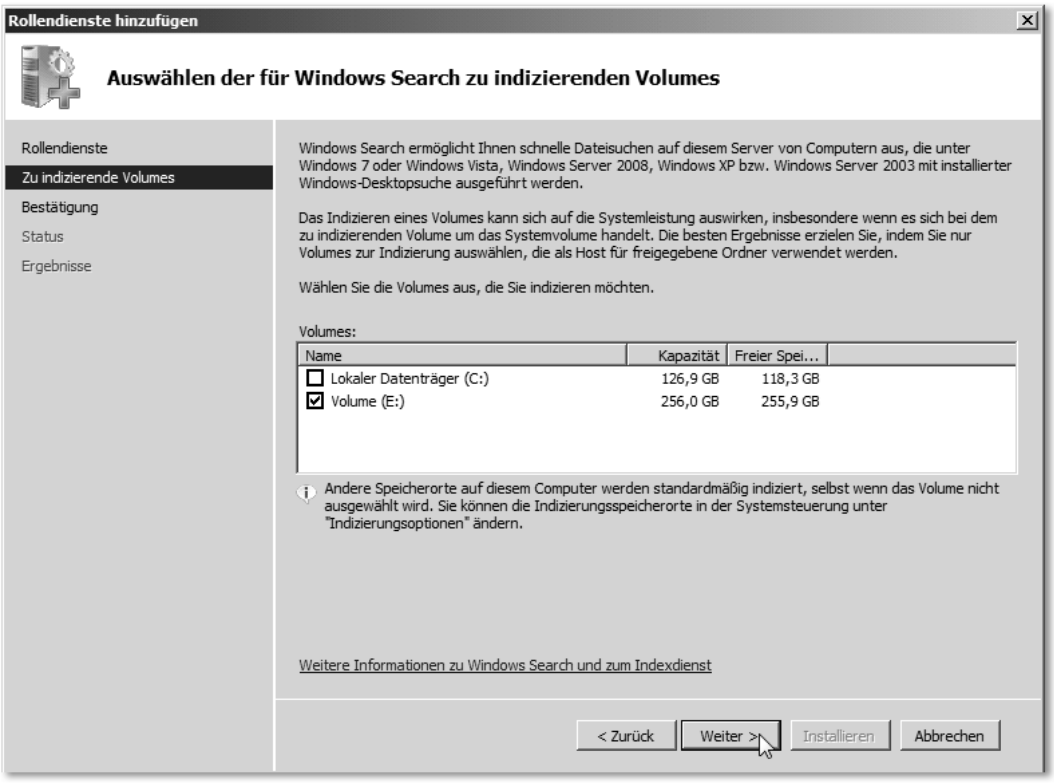


Abbildung 14.14 Windows Search kann direkt für ein oder mehrere Volumes aktiviert werden – Sie können das aber auch später etwas granularer erledigen.

der *SharePoint-Server*-Suchmaschine indiziert werden soll. Es wäre dann schon recht unschön, zig hundert Gigabyte völlig unnötigerweise zu indizieren. Falls in Ihrer Umgebung eine granularere Auswahl notwendig ist, wählen Sie in diesem Dialog zunächst nichts aus und konfigurieren die zu indizierenden Ordner später.

Um Windows Search auf dem Dateiserver zu konfigurieren, rufen Sie das Applet *Indizierungsoptionen* auf. Bei *Windows Server 2008* findet es sich in der Systemsteuerung, und bei *Windows Server 2008 R2* geben Sie einfach im Suchfeld des Startmenüs den Suchbegriff »Indizierungsoptionen« ein.

Das Konfigurations-Applet bietet nicht allzu viele Einstellungen. Die wichtigste ist die Definition der INDIZIERTEN ORTE. Auf Abbildung 14.15 ist übrigens noch eine weitere recht interessante Anzeige zu erkennen, nämlich die Anzahl der indizierten Elemente – nicht uninteressant, um abzuschätzen, ob eine plausible Anzahl von Elementen indiziert worden ist.

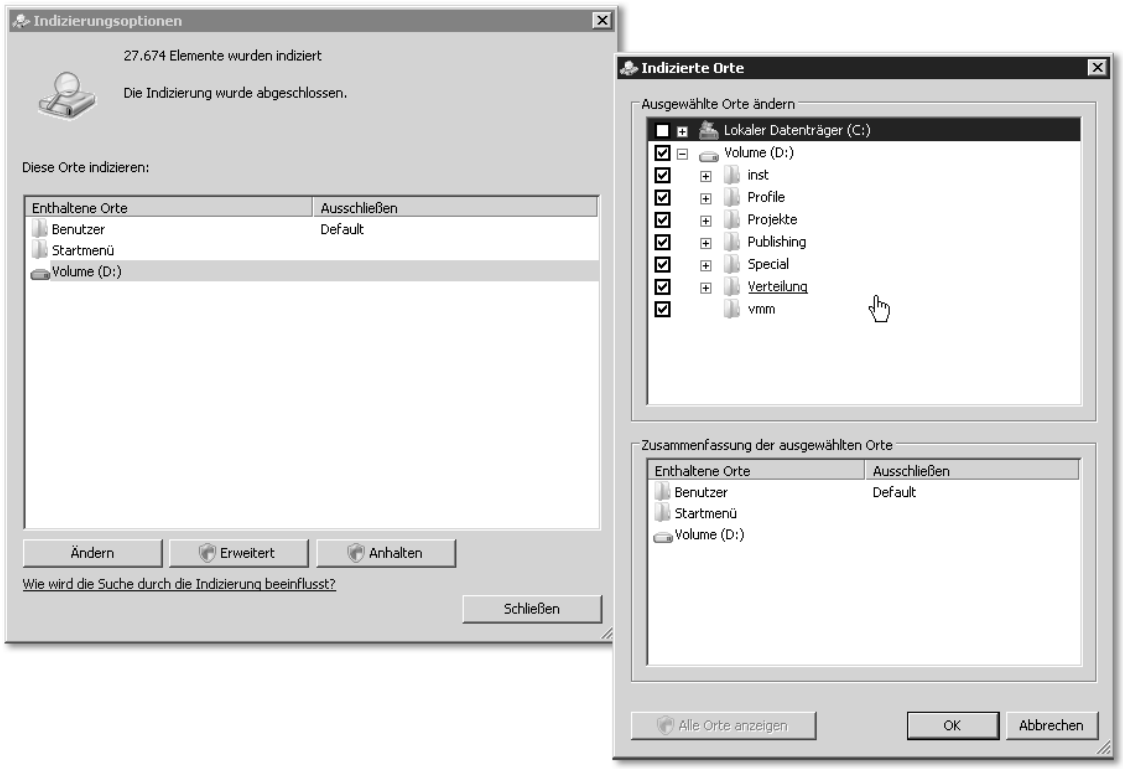


Abbildung 14.15 In den Indizierungsoptionen können Sie genau festlegen, welche Ordner indiziert werden sollen.

Wenn Sie die Schaltfläche ERWEITERT wählen, gelangen Sie zu dem Dialog aus Abbildung 14.16.

Die vermutlich wichtigste Option findet sich auf der Registerkarte INDEXEINSTELLUNGEN im Abschnitt INDIZIERUNGSORT: Sie können dort festlegen, an welchem (Speicher-)Ort die Indexdateien erstellt werden sollen. Dazu ist zu sagen, dass die

Indexdateien mitunter sehr groß werden können, man geht von 10 bis 40 % des indizierten Volumens aus – der wahre Wert dürfte im Allgemeinen aber eher in der vorderen Hälfte dieser Spanne liegen. Je nachdem, welches Datenvolumen Sie indizieren, dürfte der vorgeschlagene Standardspeicherort auf Laufwerk *C:* sehr ungünstig sein.

Auf der Registerkarte DATEITYPEN sind die zu indizierenden Dateitypen aufgelistet. Beachten Sie, dass auf einem Windows Server 2008-System (ohne R2) die neuen 2007er-Office-Formate nicht vorhanden sind – bei der R2-Version sind sie aber da.

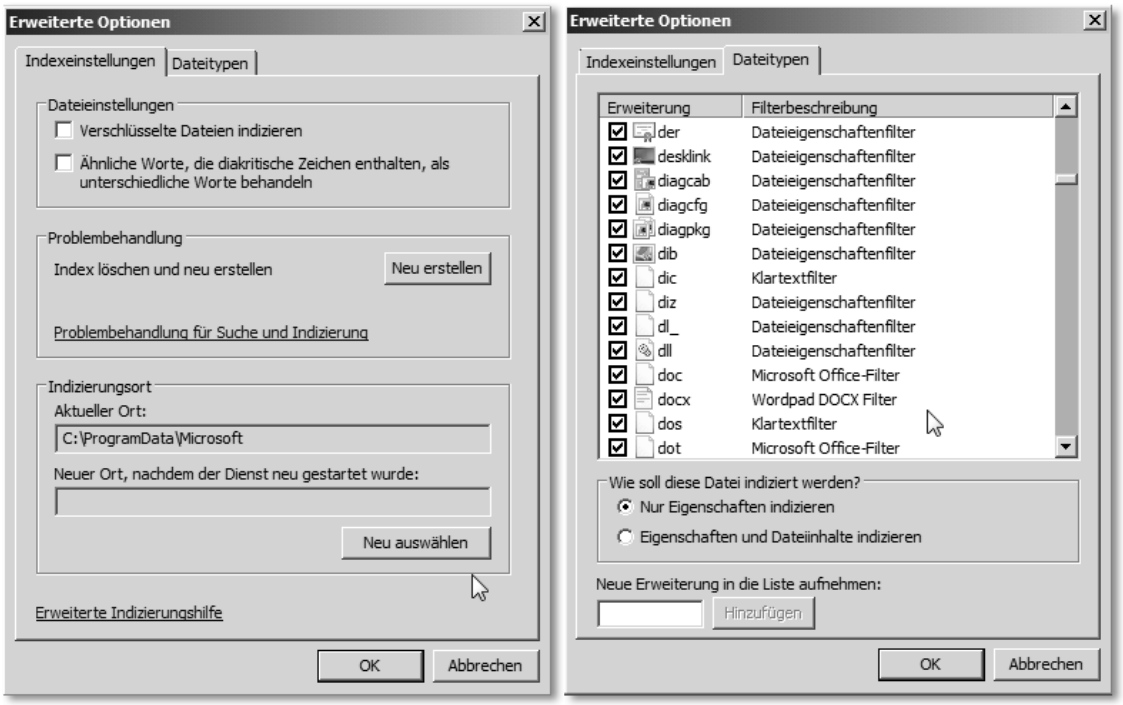


Abbildung 14.16 Weitere Konfigurationsoptionen sind beispielsweise der Indizierungsort oder die zu indizierenden Dateitypen.

14.3.2 Anwenden

Den ersten Ordner der Bibliothek können Sie mit der unübersehbar platzierten HINZUFÜGEN-Schaltfläche (Abbildung 14.10) in eine Bibliothek integrieren. Egal ob es sich um einen Netzwerkordner oder einen lokalen handelt, sein Inhalt ist sozusagen »nahtlos« in die Bibliothek integriert. Es gibt zwar einen unübersehbaren Hinweis auf die eigentliche Lokation der Daten, der den meisten Benutzern aber herzlich egal sein dürfte. Der Sinn und Zweck der Bibliotheken ist ja auch, dem Benutzer einen einfachen Zugriff auf für ihn wichtige Daten zu ermöglichen. Erfahrungsgemäß stehen Anwender mit komplex verschachtelten Bäumen deutlich auf Kriegsfuß – die Bibliotheken könnten da ein praxisgerechtes Hilfsmittel sein (Abbildung 14.17).

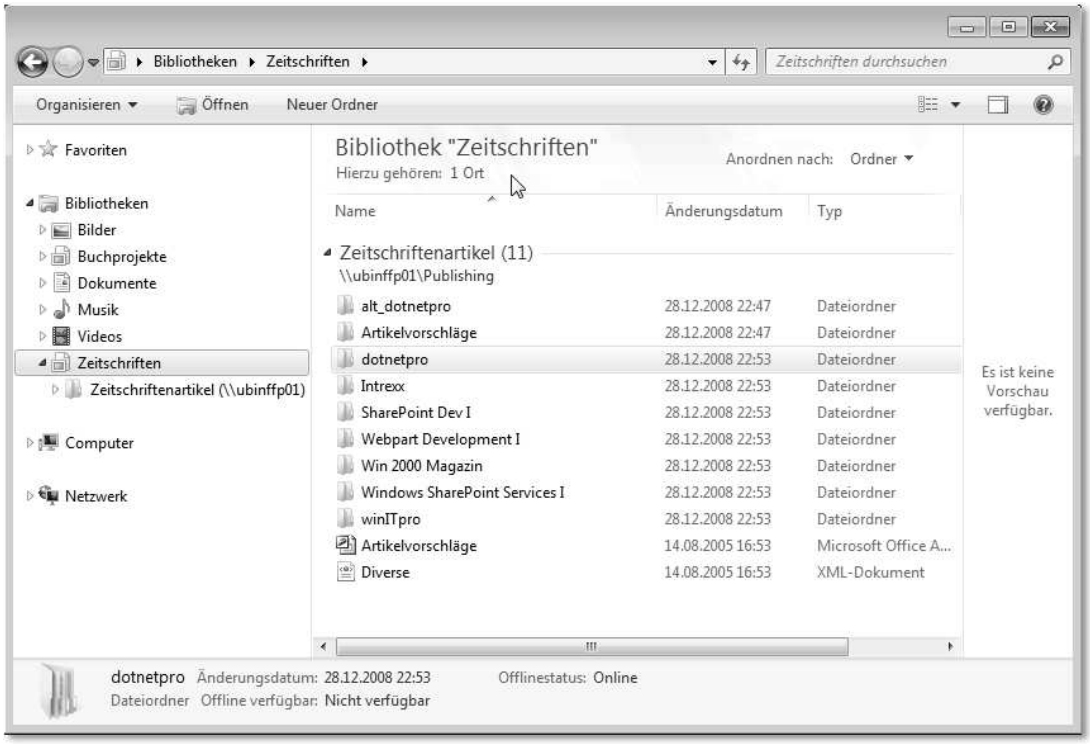


Abbildung 14.17 Hier ist eine Netzwerkfreigabe der Bibliothek hinzugefügt worden.

Wenn Sie der Bibliothek einen oder mehrere weitere Ordner hinzufügen möchten, beispielsweise weil mehrere Abschnitte des Dateisystembaums zum Thema passen, ist das problemlos möglich – die Funktion ist aber gut versteckt: Wie Sie auf Abbildung 14.17 sehen können, befindet sich direkt unterhalb der Überschrift der Bibliothek eine Angabe, wie viele »Orte« (sprich: Ordner, die Übersetzung ist hier ziemlich inkonsequent) in dieser Bibliothek verlinkt sind. Wenn Sie auf den Schriftzug 1 Ort klicken, wird der Dialog aus Abbildung 14.18 gezeigt, mit dem Sie beliebig Ordner bzw. Orte hinzufügen und/oder löschen können.

Das Suchen kann über alle Bibliotheken oder in einer Bibliothek oder auch in einem Verzeichnis eines zur Bibliothek hinzugefügten Ordners erfolgen. Es hängt ganz davon ab, was in der Baumansicht selektiert ist, wenn Sie den Suchbefehl erteilen. Die Suche geht angenehm zügig vor sich, da der Index des entfernten Servers verwendet wird. Der Grund, weshalb nur indizierte Netzwerkordner verwendet werden können, liegt übrigens auf der Hand: Würde der Benutzer bei einem 1,5 TB großen Netzwerkordner mit Millionen kleiner Dateien eine nicht indizierte Suche starten, wäre das System unter Umständen mehrere Stunden lang beschäftigt. Wenn das fünfzehn Leute gleichzeitig machen, zwingt das im schlechtesten Fall Netz und Server in die Knie.

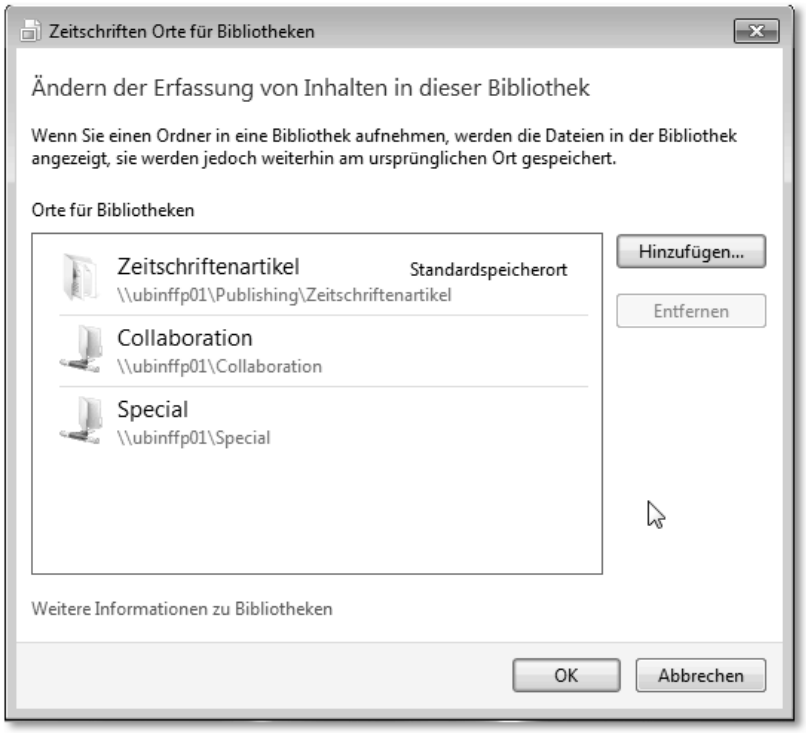


Abbildung 14.18 Es ist kein Problem, einer Bibliothek mehrere Netzwerkfreigaben hinzuzufügen.

Abbildung 14.19 zeigt nun die Suche in der Bibliothek. Wird einer der gefundenen Einträge selektiert, wird im Vorschaufenster ein grober Überblick über den Inhalt angezeigt.

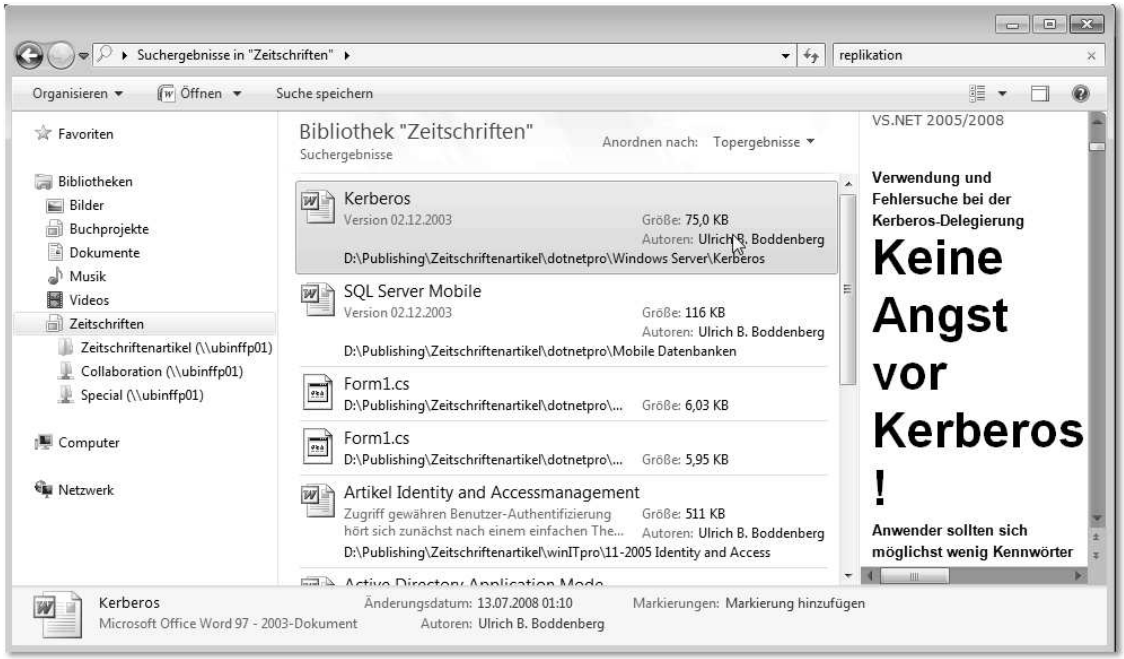


Abbildung 14.19 Hier wurde innerhalb der Bibliothek gesucht. Rechts sehen Sie die Vorschau des selektierten Eintrags.

Zum König aber sandte er und bat, es möchten doch diese Städte lieber ihm, seinem Bruder, verliehen werden, als dass sie unter Tissaphernes ständen; und seine Mutter unterstützte dieses Gesuch.

15 Mehrsprachige Umgebungen

Wenn Sie in einem etwas größeren Unternehmen tätig sind, betreuen Sie vermutlich auch Niederlassungen in nicht deutschsprachigen Gebieten. Für die Kollegen aus der Schweiz, die dieses Buch lesen, ist das »Sprachenproblem« vermutlich noch viel näher als für Österreicher und Deutsche.

Etliche international tätige Unternehmen, auch aus dem mittelständischen Umfeld, sind mittlerweile dazu übergegangen, Englisch zur »IT-Sprache« zu erheben, und installieren schlicht und ergreifend alles in dieser Sprache. Das kann man machen, es ist aber nicht optimal:

- Die meisten Benutzer fühlen sich »irgendwie besser aufgehoben«, wenn sie in ihrer jeweiligen Muttersprache arbeiten können.
  Obwohl man heute davon ausgehen könnte, dass jeder in der Schule ein paar Jahre Englisch gelernt hat, ist der Umgang mit dieser Sprache für die meisten Menschen dann doch nicht so normal wie für uns IT-People, die täglich Dokumentationen und Whitepapers in dieser Sprache lesen und in internationalen Communitys unterwegs sind.
  Ich selbst halte mich für einigermaßen polyglott – aber wenn ich die Wahl habe, entscheide ich mich im Allgemeinen auch für meine Muttersprache.
- Die Sprache eines Betriebssystems hat nicht nur Auswirkungen auf die Anzeigesprache, auch Features wie Sprachein- und -ausgabe sind von dessen Lokalisierung abhängig. Das ist zwar in den meisten Fällen eher noch ein futuristischer Gedanke, solche alternativen Formen der Interaktion werden aber in nächster Zukunft zum Einsatz kommen.

Nun besteht der Computer nicht nur aus dem Betriebssystem, sondern verfügt über mehr oder weniger viele Anwendungsprogramme. Bei diesen stellt sich natürlich auch die Frage, ob diese in allen benötigten Sprachversionen vorliegen. Es ist anzunehmen, dass die meisten Softwarehersteller nicht eine solch große Sprachenvielfalt wie Microsoft anbieten können. Aber auch dann, wenn Sie nicht alles

vom Betriebssystem bis zu jeder einzelnen Anwendung in der Muttersprache eines Benutzers anbieten können, dürfte bereits eine lokalisierte Betriebssystemumgebung auf Zustimmung stoßen.

Mehrsprachigkeit

Bezüglich der Mehrsprachigkeit von Windows 7 gibt es zwei Optionen:

- MUI (*Multilingual User Interface Pack*): Diese Pakete, die eine weitgehend vollständige Übersetzung der Umgebung bieten, können nur mit den Editionen *Enterprise* und *Ultimate* eingesetzt werden.
  Prüfen Sie in Ihren Lizenzverträgen, ob Sie zur Nutzung eines MUI berechtigt sind oder ob zusätzliche Lizenzkosten anfallen!
- LIP (*Language Interface Pack*): Die LIPs sind frei erhältlich, übersetzen allerdings nicht sämtliche Komponenten des Betriebssystems. Die »Grundsprache« wird also hin und wieder erscheinen.

Die Frage aller Fragen ist natürlich, welche Sprachen als MUI verfügbar sind. Zurzeit (Spätsommer 2009) unterstützt die *Languge-Pack*-DVD 35 Sprachen. Auf Abbildung 15.1 sehen Sie die Lokalisierungskürzel der Sprachen. Ohne in den Verdacht kommen zu wollen, Minderheiten zu diskriminieren, kann man wohl sagen, dass die wesentlichen Sprachen vorhanden sind – zumindest aus europäischer Perspektive.

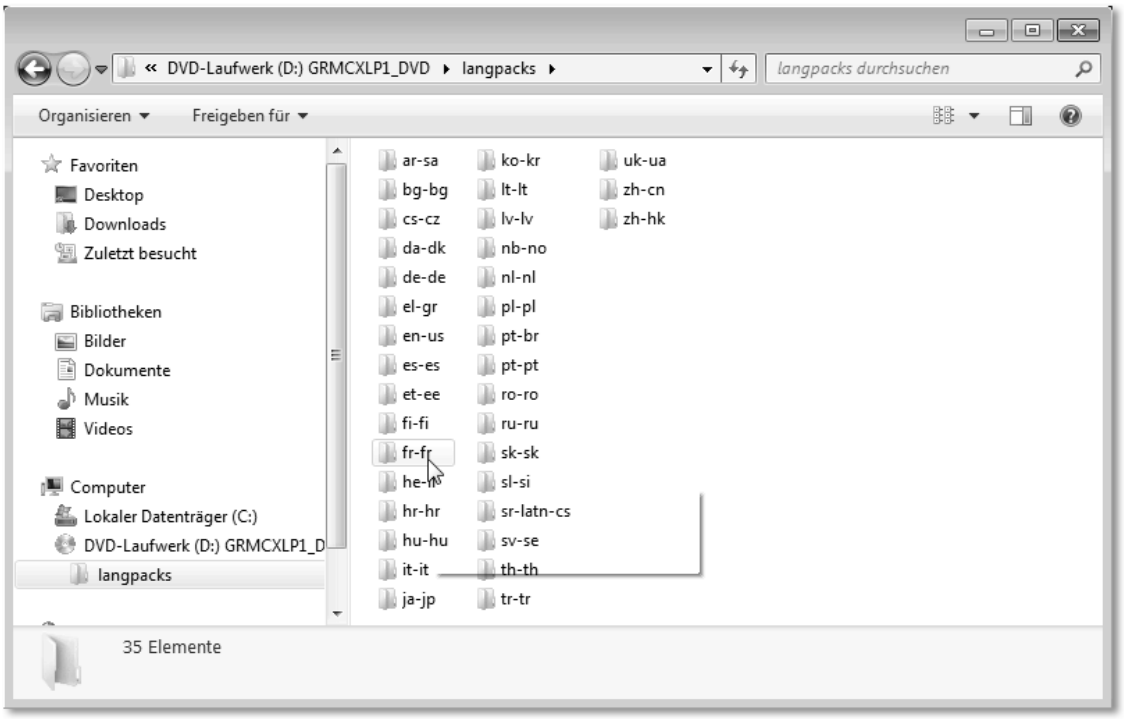


Abbildung 15.1 Die Language-Pack-DVD unterstützt momentan 35 Sprachen.

15.1 Sprache manuell auf einem bestehenden Betriebssystem installieren

Eine Möglichkeit ist die Installation eines Language Packs auf einem bereits laufenden Betriebssystem. Dabei spielt es keine Rolle, welches die ursprüngliche Betriebssystemsprache ist. Die Zeiten, in denen spezielle multilinguale Betriebssystemversionen benötigt wurden, sind zum Glück vorbei – Sie können also zu einer beliebigen Windows 7-*Enterprise* oder -*Ultimate*-Installation weitere Sprachen hinzufügen.

Der Ausgangspunkt ist die Rubrik Zeit, Sprache und Region der Systemsteuerung. Dort findet sich ein Abschnitt Region und Sprache, in dem es den Menüpunkt Anzeigesprachen installieren und deinstallieren gibt (Abbildung 15.2).

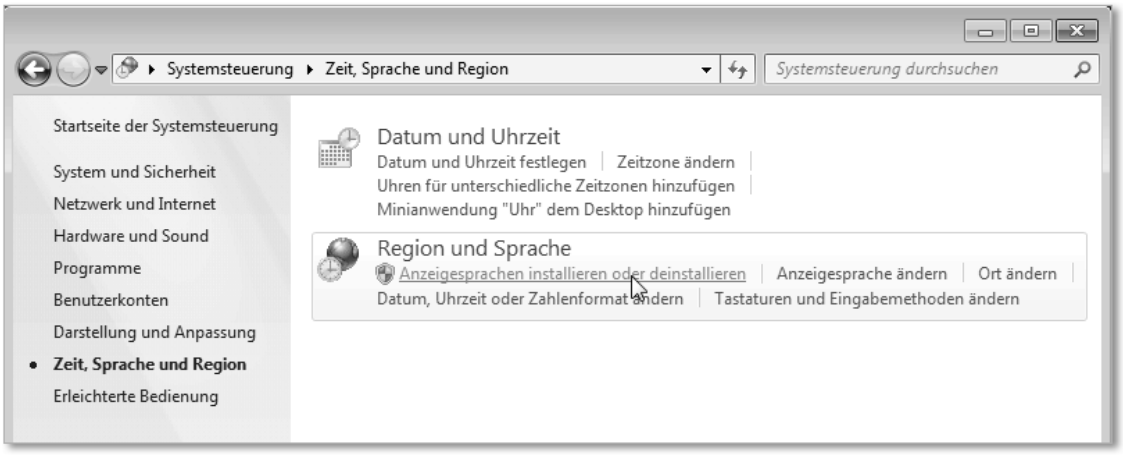


Abbildung 15.2 In der Systemsteuerung finden Sie einen Menüpunkt zum Installieren von Sprachen.

Das Installieren einer neuen Sprache ist simpel: Ein Assistent möchte zunächst von Ihnen wissen, ob Sie Anzeigesprachen installieren oder deinstallieren möchten (Abbildung 15.3). Zunächst geht es um das Installieren, anzumerken sei aber, dass jede Sprache bis auf die ursprüngliche Sprache auch genauso problemlos wieder entfernt werden kann.

Als Installationsmethode für die Sprache können Sie *Windows Update* verwenden oder auf eine lokale Datei zurückgreifen. Für dieses Beispiel habe ich die Multilanguage-DVD genutzt, entscheide mich also für die manuelle Installation (Abbildung 15.4).

Nach der Auswahl der Sprachdatei (**.cab*) werden die Informationen dazu angezeigt, also Sprache, Typ (MUI oder LIP) und Grösse. Sie sehen auf Abbildung 15.5, dass ein MUI-Paket eine ganz beachtliche Größe aufweist – das sind also nicht nur ein paar lokalisierte Menüeinträge.

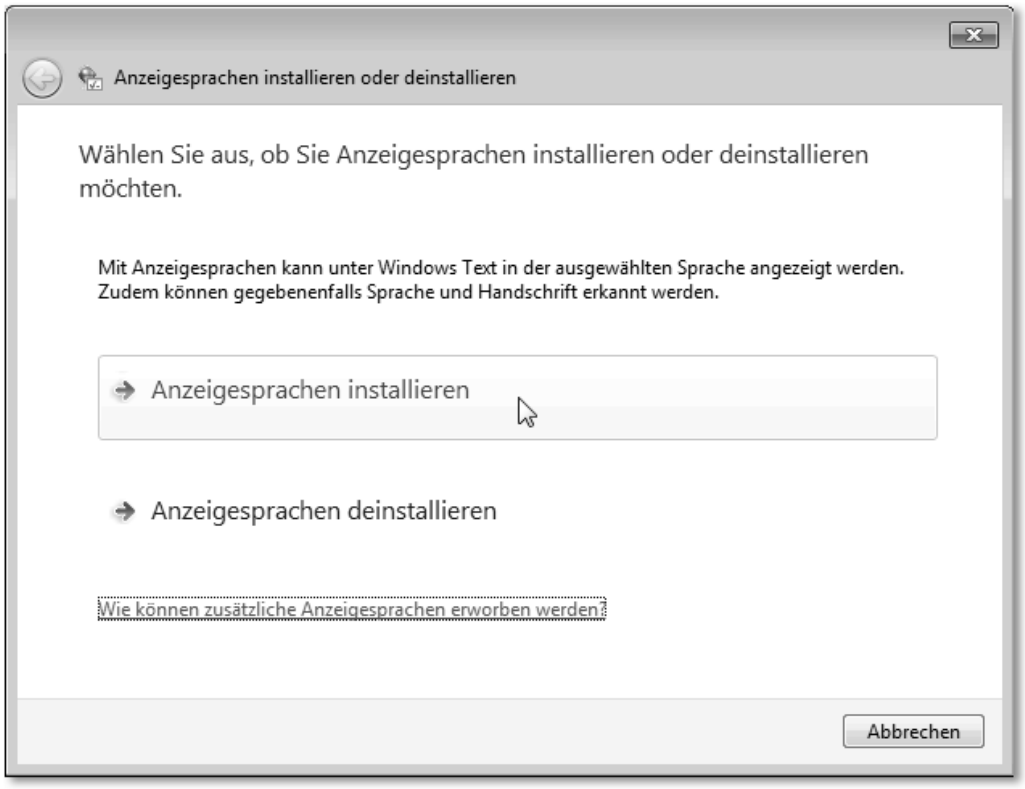


Abbildung 15.3 Sie können Anzeigesprachen installieren oder deinstallieren.

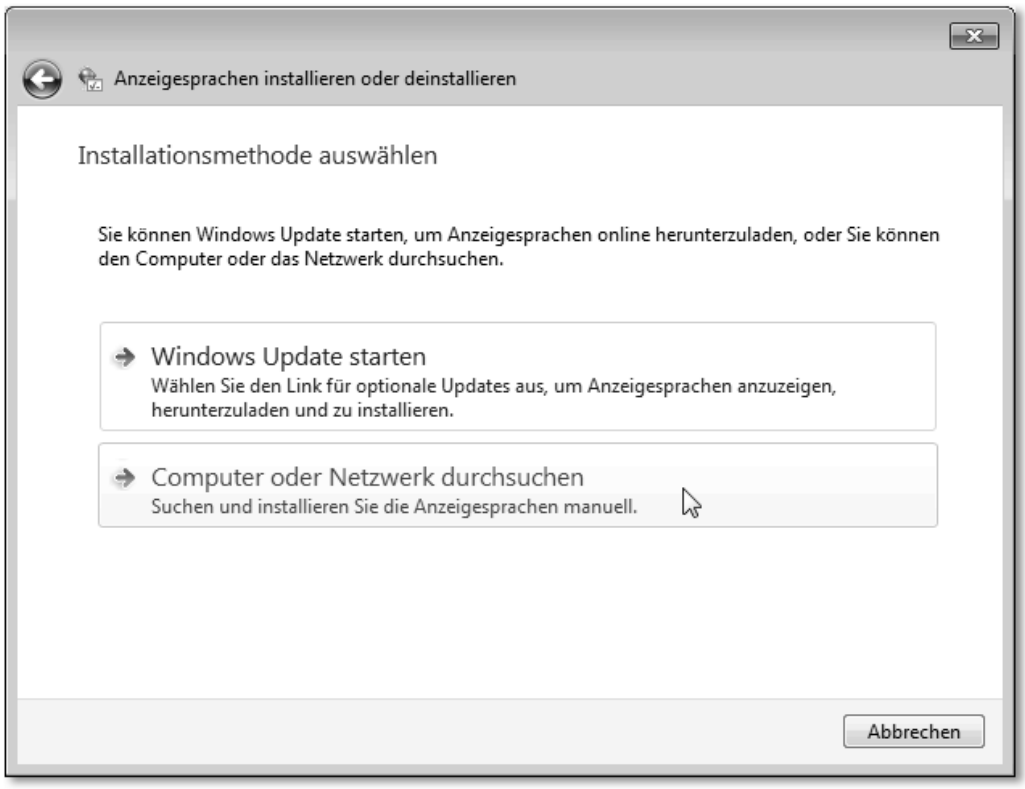


Abbildung 15.4 Wenn die Multilanguage-DVD vorliegt, erfolgt die Installation am besten von dieser.

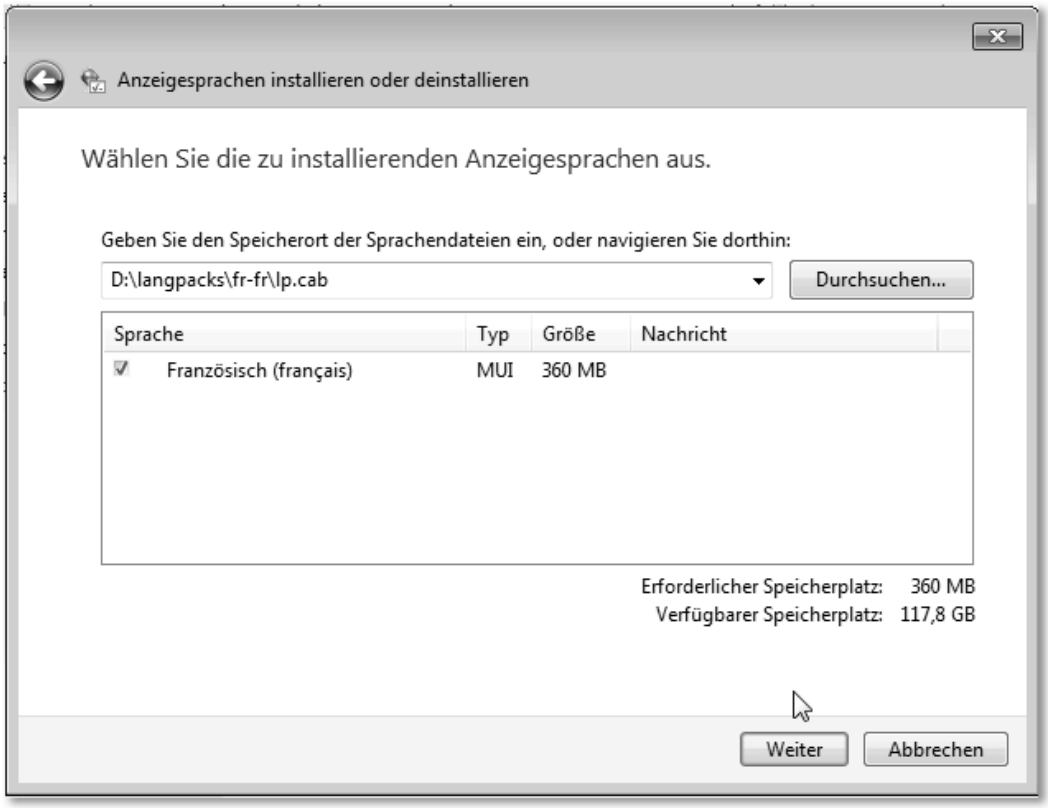


Abbildung 15.5 Die Details zu dem gewählten Sprachpaket

Die nun startende Installation wird eine gute Weile benötigen – meiner Erfahrung nach mehrere Minuten. Nach dem Abschluss des Vorgangs gelangen Sie zu dem Dialog aus Abbildung 15.6. Sie können direkt die Anzeigesprache ändern und diese auch zur Systemsprache machen. Letztgenanntes geschieht durch das Aktivieren der Checkbox Anzeigesprache für Willkommensseite…

Wenn Sie eine neue Sprache zur Systemsprache machen, ist ein Neustart notwendig (Abbildung 15.7). Wenn Sie die Checkbox nicht gesetzt haben, bezieht sich die Aktivierung der neuen Sprache nur auf das aktuelle Benutzerkonto. Die Willkommensseite und die Meldungen beim Hochfahren des Systems bleiben dann in der »alten« Sprache. Sie brauchen natürlich nach der Installation die Sprache nicht zu wechseln, sondern können den Dialog einfach schließen.

In diesem Beispiel habe ich die Systemsprache gewechselt. Dazu zeige ich Ihnen zwei interessante Screenshots:

- Auf Abbildung 15.8 ist zu sehen, dass meine ursprünglich deutsche Windows 7-Version nun auch die Meldungen beim Hochfahren auf Französisch ausgibt.
- Auch die Willkommensseite erscheint nun in Französisch (Bienvenue, Abbildung 15.9). Weiterhin können Sie sehen, dass die *Ultimate Edition* in Frankreich die Édition Intégrale ist.

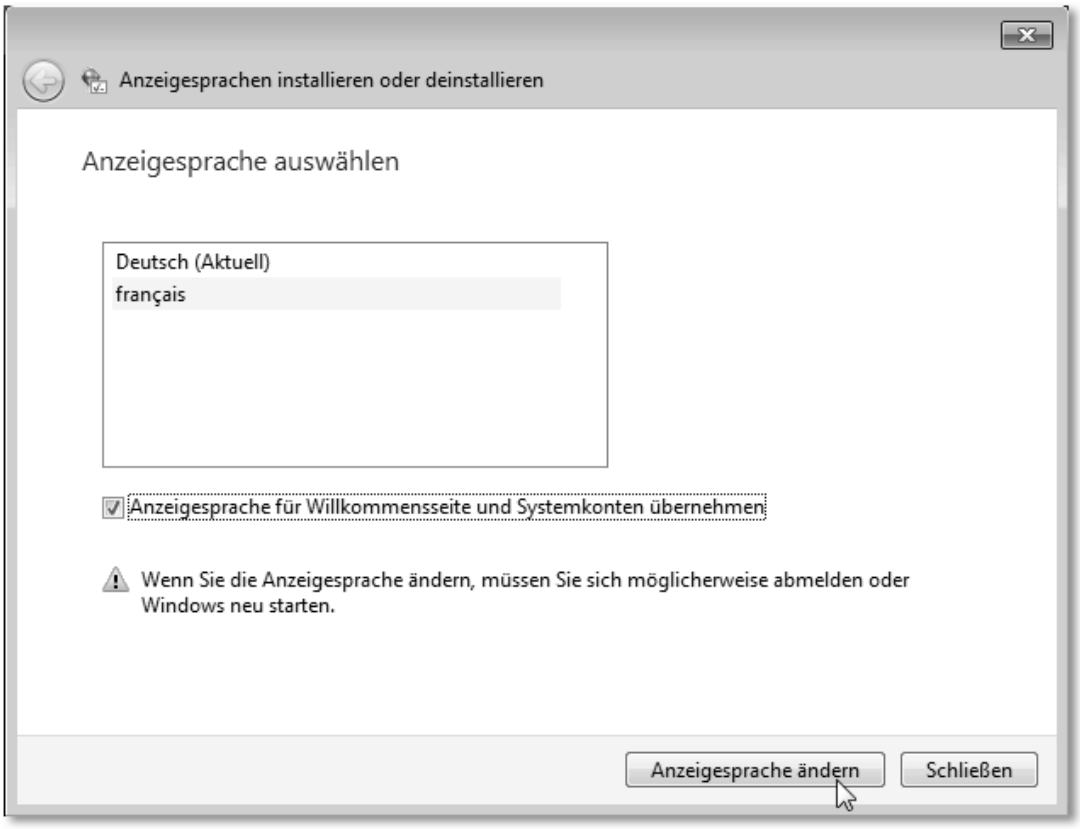


Abbildung 15.6 Wenn eine Sprache »Hauptsprache« des Systems werden soll, müssen Sie die Checkbox setzen.

Abbildung 15.7 Wenn Sie eine neue Anzeigesprache zur Systemsprache machen, ist ein Neustart erforderlich.

Zwischen installierten Sprachen zu wechseln ist übrigens in der Systemsteuerung ganz einfach. Auf Abbildung 15.10 sehen Sie, dass die auf dem System installierten Sprachen in der Auswahlliste angezeigt werden. Dieser Dialog erfordert übrigens keine erhöhten Berechtigungen, da er nicht die Systemsprache wechselt – die Sprache der Willkommensseite ändert sich beispielsweise nicht.

Abbildung 15.8 Sogar der Start erfolgt nun auf Französisch.

Abbildung 15.9 Aha: Die Ultimate-Edition ist im französischen Sprachraum die »Édition Intégrale«.

Der Benutzer muss sich einmal ab- und wieder anmelden, dann ist die gewählte Sprache aktiv. Wie Sie auf Abbildung 15.11 sehen können, wird bei Änderung der Sprache das komplette Menü angepasst, außerdem werden die Namen von Standardordnern wie *Program Files* entsprechend angepasst.

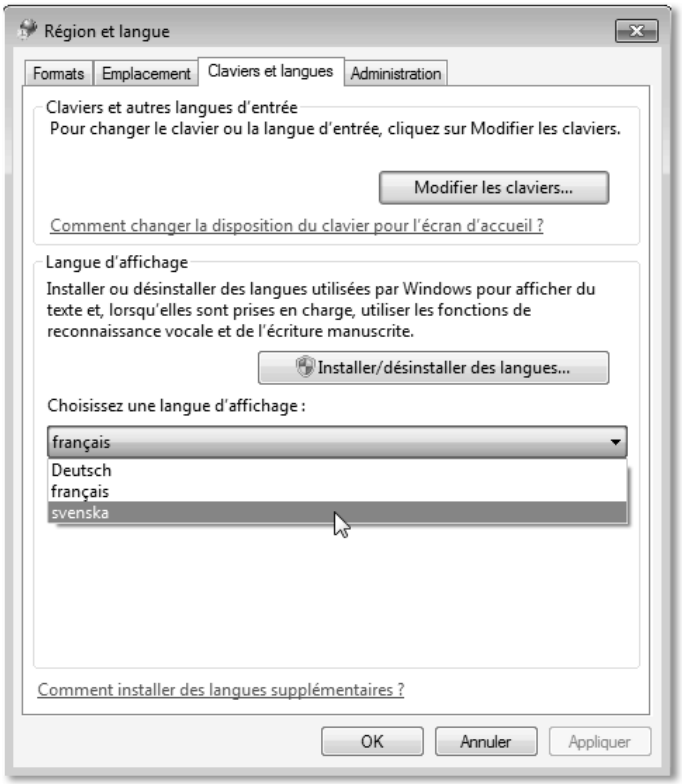


Abbildung 15.10 Die Anzeigesprache kann mit einem Mausklick umgeschaltet werden – das bezieht sich aber nicht auf die Willkommensseite und die Systemkonten.

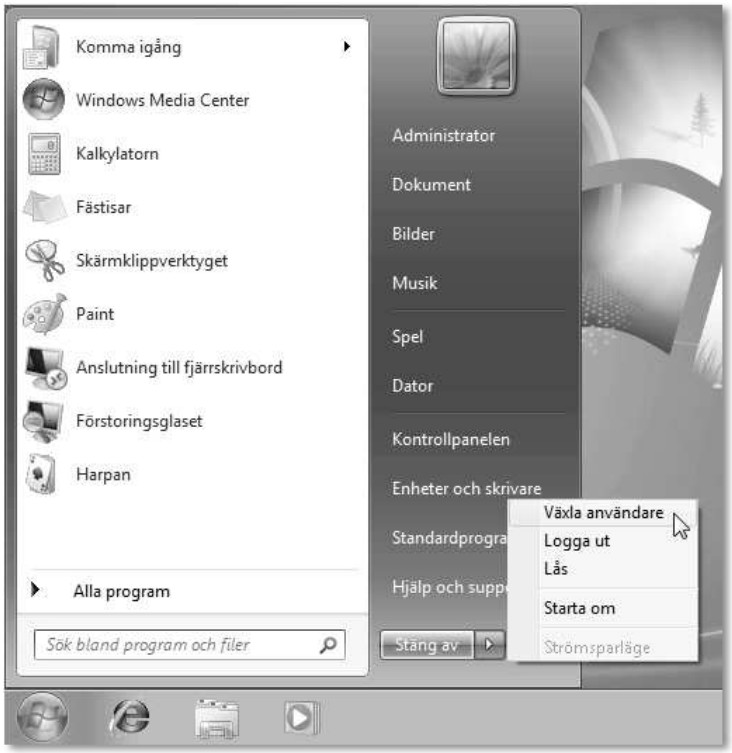


Abbildung 15.11 ... und schon können die Anwender für den nächsten Einkauf bei IKEA trainieren.

Hervorzuheben ist, dass ein Windows 7-Computer wirklich polyglott sein kann:

- Die Systemsprache (z. B. Willkommensseite) kann Deutsch sein.
- Ein Benutzer kann mit einer russischen Oberfläche arbeiten.
- Ein anderer kann die Anzeigesprache auf Französisch stellen.

Die Anzeigesprache des Benutzers ist von seinem Benutzerprofil abhängig, insofern ist die mehrsprachige Nutzung wirklich nachhaltig, ganzheitlich und flexibel möglich.

15.2 Multilingual von Anfang an

Es wäre natürlich sehr unschön, wenn Sie in einem mehrsprachigen Unternehmen die verwendeten Sprachen umständlich einzeln nachinstallieren müssten.

Sie haben bereits beim Deployment die Möglichkeit, dem Installationsimage alle benötigten Sprachen mitzugeben und die Standard-Sprache zu setzen:

- Sie können die benötigten Sprachpakete in das Image integrieren. In Abschnitt 6.10.3, »Packages verwalten«, habe ich vorgeführt, wie das grundsätzlich gemacht wird.
- Mit dem Kommandozeilenwerkzeug *dism* können Sie einige »internationale Optionen« (wie beispielsweise die Systemsprache oder das standardmäßige Tastaturlayout) festlegen. Auf Abbildung 6.96 ist der Aufruf des Werkzeugs zu sehen.

15.3 Profile

Die Spracheinstellungen werden im Profil gespeichert und bei der Anmeldung auf einem PC mit mehreren installierten Sprachen berücksichtigt. Mehr erfahren Sie in Abschnitt 5.2.2, »Servergespeicherte Profile in mehrsprachigen Umgebungen«.

So wusste der König nichts von den gegen ihn gerichteten Absichten, sondern glaubte, er mache den Aufwand für das Heer wegen des Krieges mit Tissaphernes.

16 Client-Management mit System Center Configuration Manager 2007 R2 (SCCM)

In einem Buch über den aktuellen Windows-Client darf die Betrachtung über ein Client-Management-System nicht fehlen. Natürlich ist das Management der Umgebung (im weiteren Sinne) bereits im Standardumfang von Windows 7 und Windows Server 2008 (R2) ein stark berücksichtigtes Thema. Es gibt aber durchaus noch Raum für Systeme, die eine erweiterte Funktionalität bieten. Einige Beispiele:

- Die *Inventarisierung* der Clientlandschaft – und zwar sowohl bezüglich Hardware- als auch Software-Inventar – ist mit »Bordmitteln« ein weißer Fleck auf der Landkarte.
- Die *Softwareverteilung* ist zwar über Gruppenrichtlinien rudimentär möglich, allerdings bleiben auf diese Weise diverse Wünsche unerfüllt.
- Die *Betriebssystemverteilung* ist mit den *Windows Deployment Services* zwar in guter Qualität vorhanden, könnte aber ein wenig ergänzt werden, beispielsweise um die automatische Nachinstallation von Softwarepaketen.
- Auch die Unterstützung der Benutzer durch den *Helpdesk* wird mittlerweile durch alle im Markt verbreiteten Client-Management-Systeme abgebildet. Hierzu gehört beispielsweise eine Fernsteuerungsfunktion, der Online-Abruf der Inventarinformationen und dergleichen mehr.

Ein in der Praxis bewährtes System ist Microsofts *System Center Configuration Manager*, den ich Ihnen in diesem Kapitel vorstellen möchte.

Drittherstellerlösungen

An dieser Stelle sei nochmals betont, dass es durchaus attraktive Drittherstellerlösungen gibt. Wenn bei Ihnen eine Entscheidung für ein solches System ansteht, lohnt es sich durchaus, sowohl Funktionalität als auch Preise zu betrachten.

Der Ahn des *System Center Configuration Manager* (SCCM) ist der *Systems Management Server* (SMS). SMS hatte lange Zeit den Ruf, dass er zwar durchaus funktioniere, aber im Vergleich zu Konkurrenzprodukten doch etwas »angestaubt« sei. Ob man eine Softwarelösung gut findet oder eine andere bevorzugt, ist natürlich immer auch ein wenig subjektiv. Für mein Gefühl hat Microsoft mit dem *Configuration Manager* eine sehr interessante System-Management-Lösung entwickelt, die vor allem auch dadurch besticht, dass viele andere Microsoft-Technologien recht nahtlos dort integriert werden können.

Ich denke aber, dass man ganz deutlich sagen muss, dass der Configuration Manager das komplexeste Produkt der *System-Center*-Reihe ist. Dies spricht aber nicht gegen das Produkt, sondern zeigt, dass das System-Management ein außerordentlich komplexes und vielfältiges Thema ist. Es reicht von einfacher Inventarisierung bis hin zur vollautomatischen Verteilung von Betriebssystemen.

Einen ersten Überblick über die Vielfalt des Configuration Managers gewinnt man bereits, wenn man einen Blick auf die Administrationskonsole riskiert. Abbildung 16.1 zeigt den wirklich sehr umfangreichen Baum, der sowohl zu Konfigurations- als auch zu Aktionsmöglichkeiten führt.

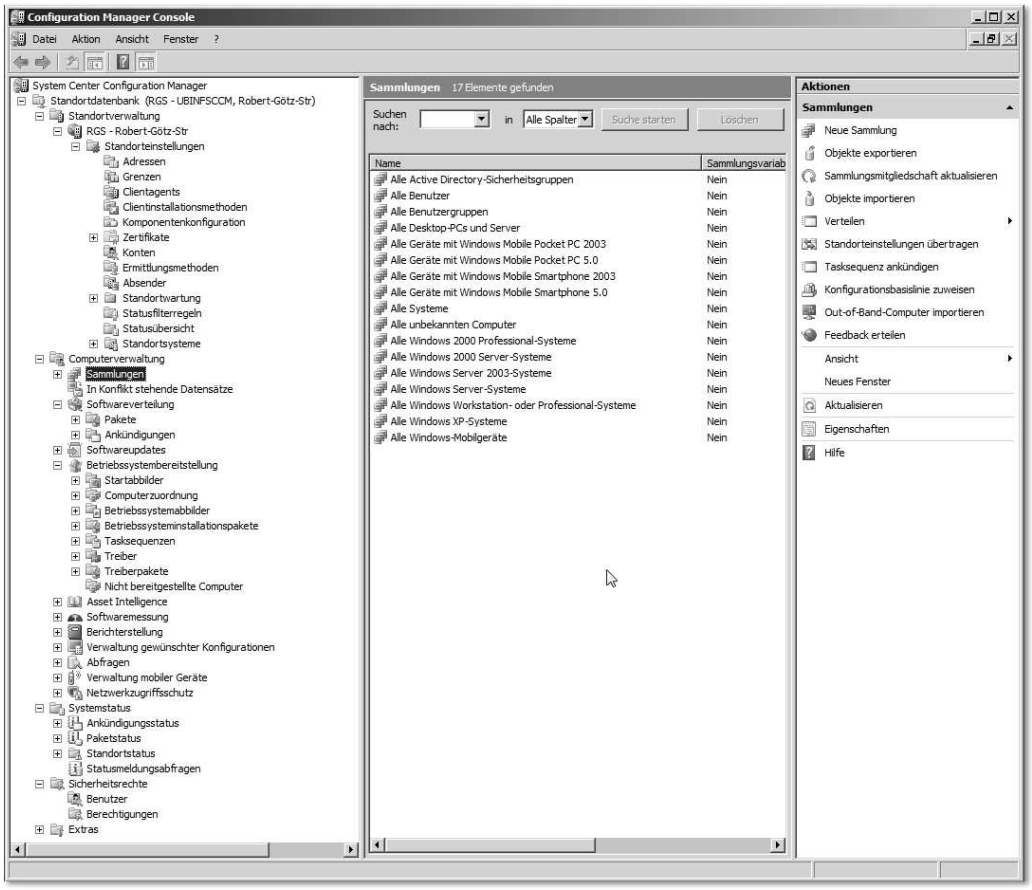


Abbildung 16.1 Einstellmöglichkeiten und Funktionen ohne Ende – die Konsole des Configuration Managers

16.1 Grundprinzipien

In diesem Abschnitt möchte ich Ihnen einige Grundprinzipien zum Configuration Manager vermitteln.

16.1.1 Standorte und (Server-)Rollen

Das wichtigste Element in einer *Configuration-Manager*-(CM-)Umgebung ist der Standort. Ein Standort zeichnet sich dadurch aus, dass ein CM-System dort vorhanden ist und die Configuration-Manager-Clients verwaltet.

Es gibt zwei Arten von Standorten:

- *Primäre Standorte* sind weitgehend autark und verfügen über eine eigene Datenbank, in der deren Clients gespeichert sind.
- *Sekundäre Standorte* sind stets einem primären Standort zugewiesen und nutzen dessen Datenbank.

In großen Organisationen kann eine beliebig komplexe Hierarchie von primären und sekundären Standorten aufgebaut werden. Hierbei ist aber stets zu beachten, dass ein sekundärer Standort stets einem primären untergeordnet sein muss.

Abbildung 16.2 zeigt die zu konfigurierenden STANDORTEINSTELLUNGEN. Hier wird unter anderem konfiguriert, welche GRENZEN ein Standort hat (ob er z. B. deckungsgleich mit einem Active Directory-Standort ist), welche Ermittlungsmethoden angewendet oder welche Agenten auf den Clients installiert werden sollen.

In der Abbildung ist der Knoten STANDORTSYSTEME aufgeklappt. Dort sind, wie erwartet, die vom Configuration Manager verwendeten Serversysteme aufgeführt. Die Standortsysteme führen eine oder mehrere Rollen aus, was auf dem Screenshot ebenfalls zu erkennen ist: Der Server *UBINFSCCM* ist unter anderem Verteilungspunkt und Verwaltungspunkt.

Einem bestehenden Standortsystem können weitere Rollen hinzugefügt werden. Weiterhin können Rollen auf zusätzlichen Servern installiert werden. Abbildung 16.3 zeigt den Dialog zum Hinzufügen von Configuration-Manager-Rollen zu einem neuen Server – immerhin gibt es zwölf Stück. Beachten Sie, dass Sie in dieser Auflistung nicht die Rolle STANDORTSERVER finden werden; die Rolle STANDORTSERVER gibt es pro Standort nur einmal, und diese hat der erste Server, der am Standort vorhanden ist.

Ich möchte nun nicht jede einzelne Rolle besprechen – teilweise erschließt sich die Funktion ja bereits aus dem Namen –, ich möchte allerdings auf zwei besonders wichtige Rollen hinweisen:

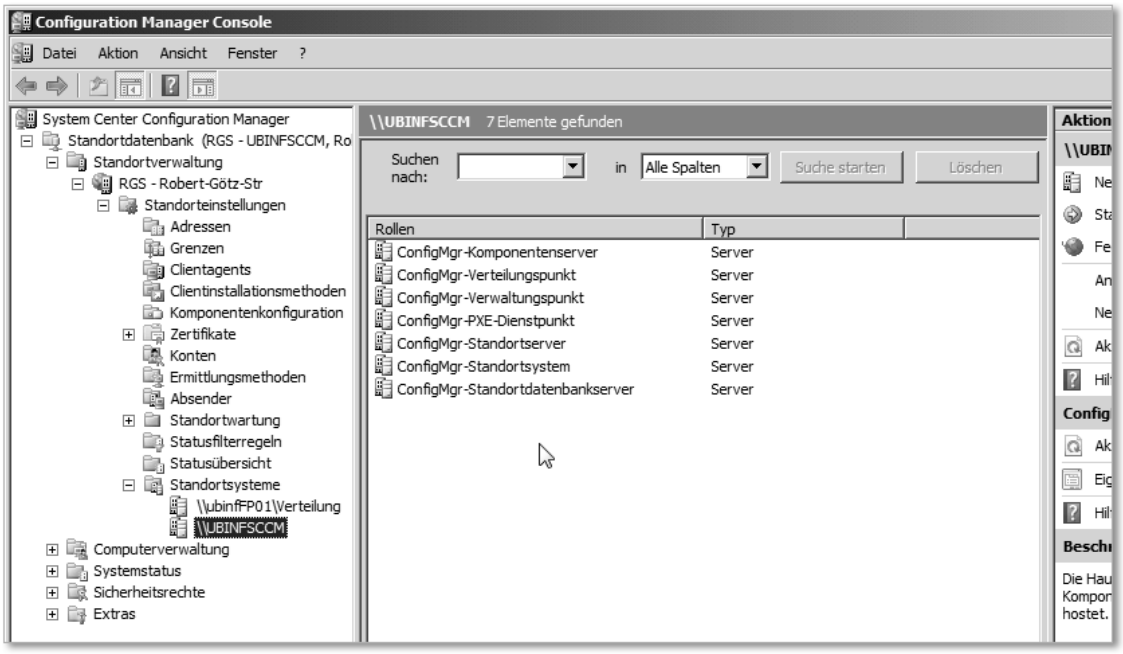


Abbildung 16.2 Ein Standort enthält ein oder mehrere Standortsysteme.

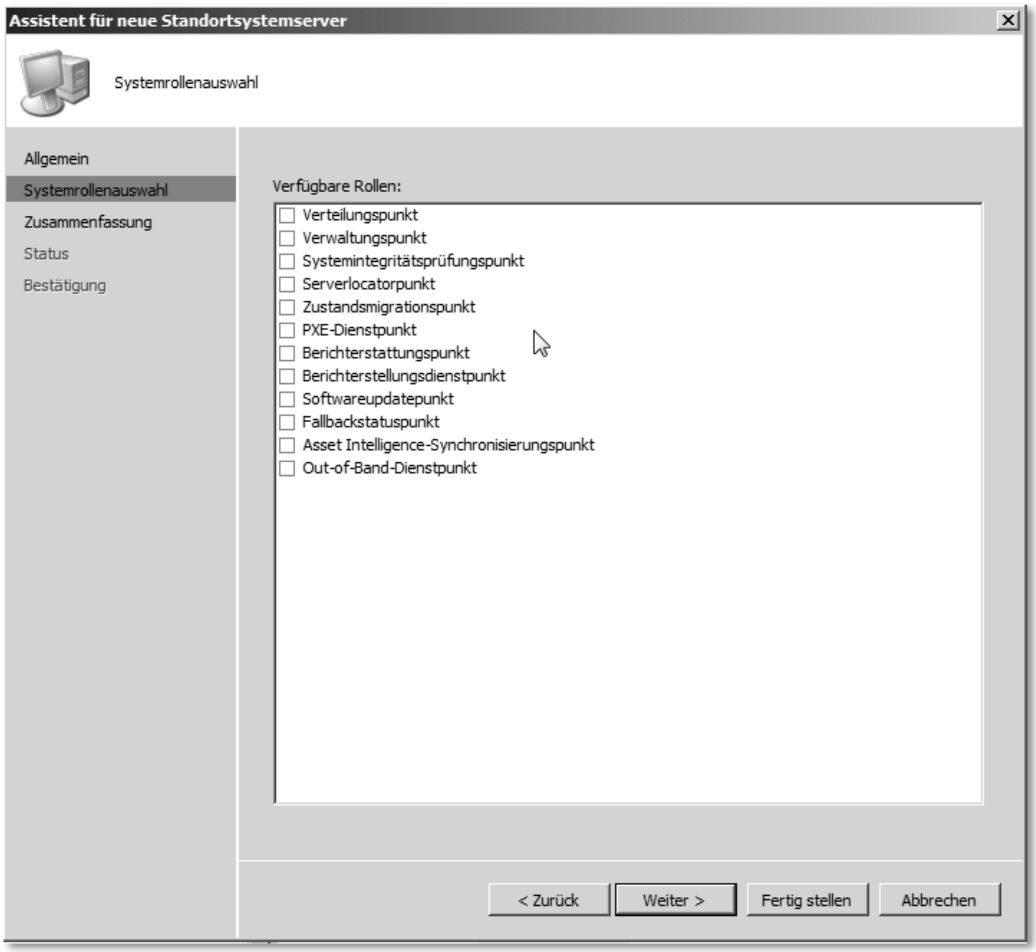


Abbildung 16.3 Einem Server können eine oder mehrere Rollen zugewiesen werden.

- VERWALTUNGSPUNKT: Dies ist die Rolle, mit der die Configuration-Manager-Agenten kommunizieren.
- VERTEILUNGSPUNKT: Von dieser Rolle können Clients beispielsweise zu installierende Softwarepakete erhalten.

Abbildung 16.4 zeigt einige Zusammenhänge:

- Die Clients (bzw. die Configuration-Manager-Agenten auf den Clients) kommunizieren in erster Linie mit einem *Verwaltungspunkt*.

  Dort liefert der Client einerseits Daten ab (beispielsweise über sein Inventar) und erhält andererseits Anweisungen, etwa welche Softwarepakete installiert werden sollen.
- Wenn ein Client Software installieren soll, erhält er diese von einem *Verteilungspunkt*.

  Dieser Verteilungspunkt kann ein normaler Dateiserver sein, letztendlich kann sogar ein Clientsystem als Zweigverteilungsserver eingerichtet werden.
- Die Synchronisation von Paketen zwischen Verteilungspunkten übernimmt der *Configuration-Manager-Server*.

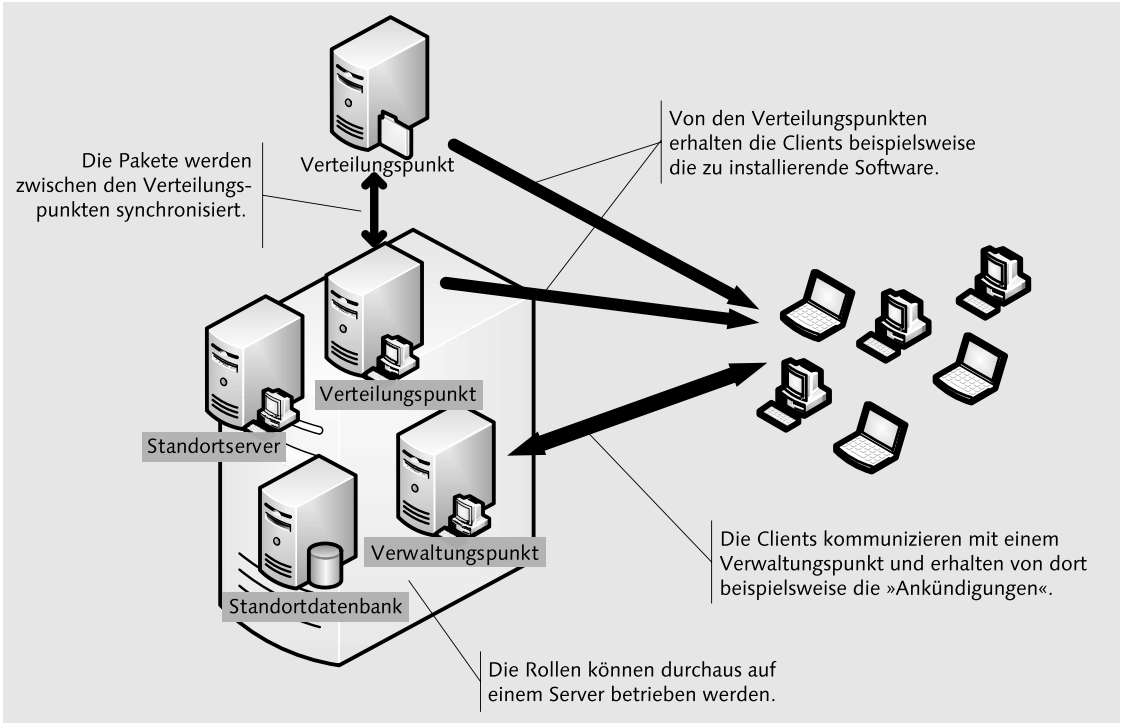


Abbildung 16.4 »Verwaltungspunkt« und »Verteilungspunkt« gehören zu den wichtigsten Rollen.

Sie brauchen sich keine Sorgen zu machen, dass Sie für den Configuration Manager einen riesigen Park von Servern benötigen. In einer kleinen oder mittleren Organisation können durchaus sämtliche Rollen auf einem System installiert werden.

16.1.2 Sammlungen

Eines der wesentlichen Konzepte des Configuration Managers ist das der Sammlungen. Wenn Sie beispielsweise Softwarepakete verteilen, erfolgt dies grundsätzlich an Sammlungen. Auch wenn Sie eine Applikation an einen einzelnen Computer verteilen möchten, geht dies nur über diesen Weg. Es würde dann an eine Sammlung verteilt, die nur einen Computer enthält.

In Abbildung 16.5 sehen Sie, dass standardmäßig bereits diverse Sammlungen enthalten sind. Die Sammlung Alle Systeme enthält, wie ja auch nicht anders zu erwarten, sämtliche vom Configuration Manager gefundenen Computer.

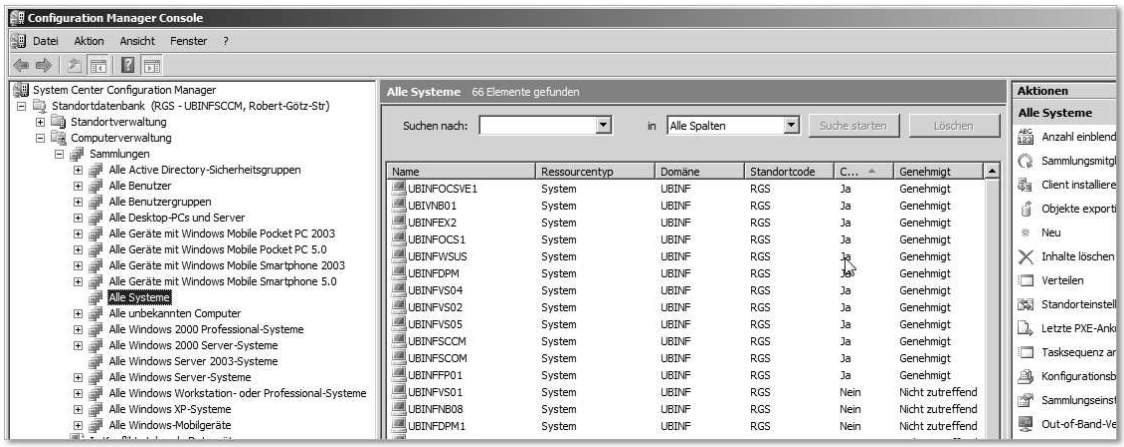


Abbildung 16.5 In der Sammlung »Alle Systeme« sind alle vom Configuration Manager erkannten Systeme aufgeführt.

Einer der Vorteile der Arbeit mit Sammlungen besteht darin, dass deren Mitglieder auf Basis von Abfragen, also dynamisch, ermittelt werden können. In Abbildung 16.6 ist die Abfrage zu sehen, die der Sammlung Alle Windows Server 2003-Systeme zugrunde liegt.

Die Abfrage ermittelt alle Systeme, bei denen im Feld OperatingSystemNameandVersion die Zeichenkette Server 5.2 enthalten ist. Das Bauen von Abfragen für eigene Sammlungen wird hin und wieder notwendig sein; die Abfragen kann man sich aber auch mehr oder weniger »zusammenklicken«. Es ist also nicht zwingend notwendig, selbst SQL-Abfrageanweisungen zu formulieren.

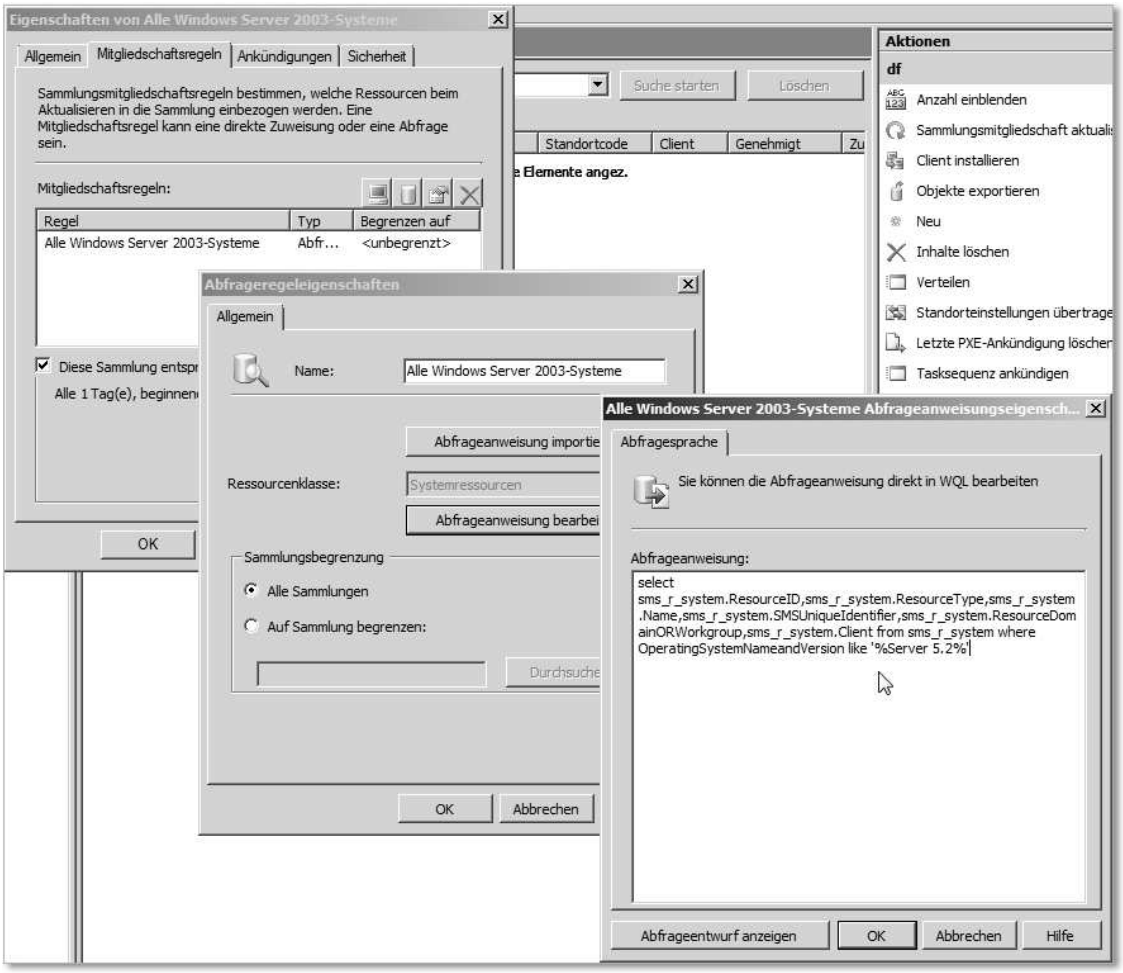


Abbildung 16.6 Die Mitglieder von Sammlungen werden dynamisch mithilfe von Abfragen ermittelt.

16.1.3 Pakete und Ankündigungen

Sammlungen ist der erste wesentliche Configuration-Manager-Begriff, der zweite heißt *Ankündigungen*. Hinter einer Ankündigung verbirgt sich letztendlich ein Auftrag an einen Client, etwas zu tun, beispielsweise ein Softwarepaket zu installieren.

Der Knoten ANKÜNDIGUNGEN findet sich gemeinsam mit dem Knoten namens PAKETE unterhalb der SOFTWAREVERTEILUNG (Abbildung 16.7). Das macht grundsätzlich auch Sinn, denn häufig werden Ankündigungen dazu verwendet, um ein Software-Paket zu verteilen. An dieser Stelle sei allerdings darauf hingewiesen, dass es Ankündigungen auch für andere Zwecke geben kann, beispielsweise für das Initiieren einer Betriebssystemverteilung.

Bei »Paketen« handelt es sich um zu verteilende Softwarepakete, wobei hier nicht unbedingt immer die Installation einer Software das Ziel sein muss. Ein Paket

kann auch verwendet werden, um eine ausführbare Datei zu starten, die beispielsweise ein BIOS-Update durchführt oder dergleichen tut.

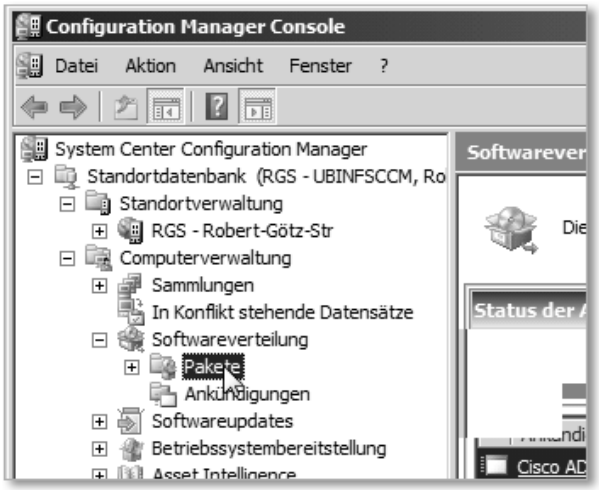


Abbildung 16.7 »Pakete« und »Ankündigungen« sind unter dem Knoten »Softwareverteilung« zu finden. Es können aber auch andere »Jobs« als die Installation von Paketen angekündigt werden.

Hinweis

Die Arbeit mit Paketen und Ankündigungen wird sehr ausführlich in einem der folgenden Abschnitte vorgeführt, weshalb ich an dieser Stelle nicht näher auf die Feinheiten eingehen möchte.

16.2 Agenten ausrollen

Bevor Sie ein System mit dem Configuration Manager verwalten können, muss zunächst der Agent auf selbigem installiert werden. Natürlich muss kein Mitarbeiter abgestellt werden, der jeden einzelnen PC besucht und per Hand den Client installiert, vielmehr gibt es ein automatisiertes Verfahren, das ich Ihnen im Folgenden kurz vorstellen möchte.

16.2.1 Ermittlungsmethoden

Der erste Schritt bei der Installation von Agenten ist die Ermittlung. Kurz gesagt verbirgt sich dahinter, dass der Configuration Manager automatisch die verwaltbaren Objekte ermittelt. Wie Sie in Abbildung 16.8 sehen können, gibt es sechs Ermittlungsmethoden, die zum einen verschiedene Objekttypen suchen (Systeme, Benutzer, Gruppen) und zum anderen mit verschiedenen Verfahren arbeiten (Active Directory, Netzwerkermittlung).

Die Ermittlungsmethoden verfügen jeweils über einen Eigenschaftendialog, in dem die Methode aktiviert bzw. deaktivert werden kann, zudem gibt es einige Einstellmöglichkeiten. Bei der in Abbildung 16.8 gezeigten ACTIVE DIRECTORY-SYSTEMERMITTLUNG werden die zu durchsuchenden Container, die Abfragehäufigkeit und die zu ermittelnden Attribute festgelegt.

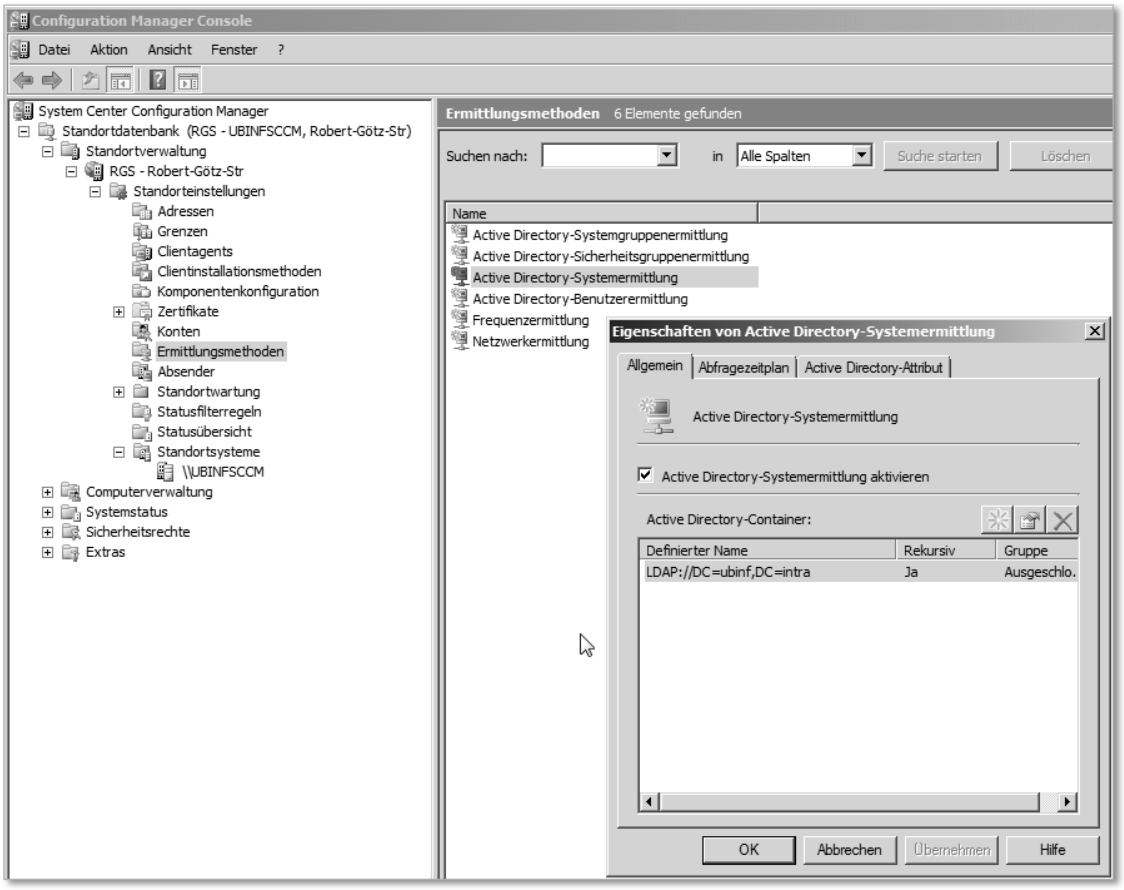


Abbildung 16.8 Es gibt sechs Ermittlungsmethoden, um zu verwaltende Objekte zu lokalisieren.

Nach Durchführung der Ermittlung werden die gefundenen Objekte in den SAMMLUNGEN auftauchen (sie sind unterhalb des Knotens COMPUTERVERWALTUNG zu finden).

Asynchronität

Beachten Sie, dass der Configuration Manager asynchron arbeitet. Selbst wenn Sie die Checkbox für das sofortige Ausführen der Ermittlung gesetzt haben, kann es eine Weile dauern, bis die Ermittlungsergebnisse angezeigt werden.

16.2.2 Clientinstallationsmethoden

Bei Einstellmöglichkeiten für die CLIENTINSTALLATIONSMETHODEN geht es darum, wie Agenten automatisch (!) auf die innerhalb der Standortgrenzen ermittelten Systeme gebracht werden. Die bequemste und meistgenutzte Möglichkeit ist die *Clientpushinstallation*, bei der der Configuration Manager den Agenten ohne weitere Mitwirkung von anderen Systemen oder Administratoren installiert.

Die Nutzung des *Softwareupdatepunkts* setzt eine aktive WSUS-Infrastruktur voraus und bedingt einige weitere Eingriffe in die Konfiguration, weshalb die Clientpushinstallation zumeist der bequemere Weg sein dürfte.

Es gibt übrigens durchaus noch weitere Möglichkeiten der Clientinstallation, beispielsweise:

- Installation über Gruppenrichtlinien,
- Installation über ein Anmeldeskript,
- Installation durch Integration in die Installationsimages,
- und natürlich die manuelle Installation (hinlaufen, Datenträger einlegen, Installation starten).

In dem Dialog aus Abbildung 16.9 ist übrigens konfiguriert, dass der Configuration-Manager-Agent automatisch (!) auf jeder Arbeitsstation und jedem Server, der innerhalb der Standortgrenzen gefunden wird, per Pushinstallation installiert wird.

Wenn Sie keine automatische Installation wünschen, muss die oberste Checkbox, CLIENTPUSHINSTALLATION AUF ZUGEWIESENEN RESSOURCEN AKTIVIEREN, ausgeschaltet werden. Das Abschalten dieser Automatik nimmt Ihnen jedoch nicht die Möglichkeit, im Kontextmenü eines Computerobjekts, beispielsweise in einer Sammlung, manuell die Pushinstallation zu initiieren.

Im Normalfall dürfte es aber durchaus gewollt sein, dass die Systeme automatisch mit dem Configuration-Manager-Agenten versorgt werden.

Hinweis

Auch an dieser Stelle sei darauf hingewiesen, dass das *System Center* nicht sofort mit der Agenteninstallation beginnt, wenn Sie die automatische Installation aktivieren und den Dialog speichern.

Es kann durchaus sein, dass die Installation beispielsweise erst am nächsten Tag durchgeführt wird – also ist Geduld angesagt.

Ob ein Client bereits über den Configuration-Manager-Agenten verfügt, können Sie beispielsweise in der Anzeige einer Sammlung sehen: Dort gibt es eine Spalte CLIENT, die entweder auf JA oder auf NEIN gesetzt ist.

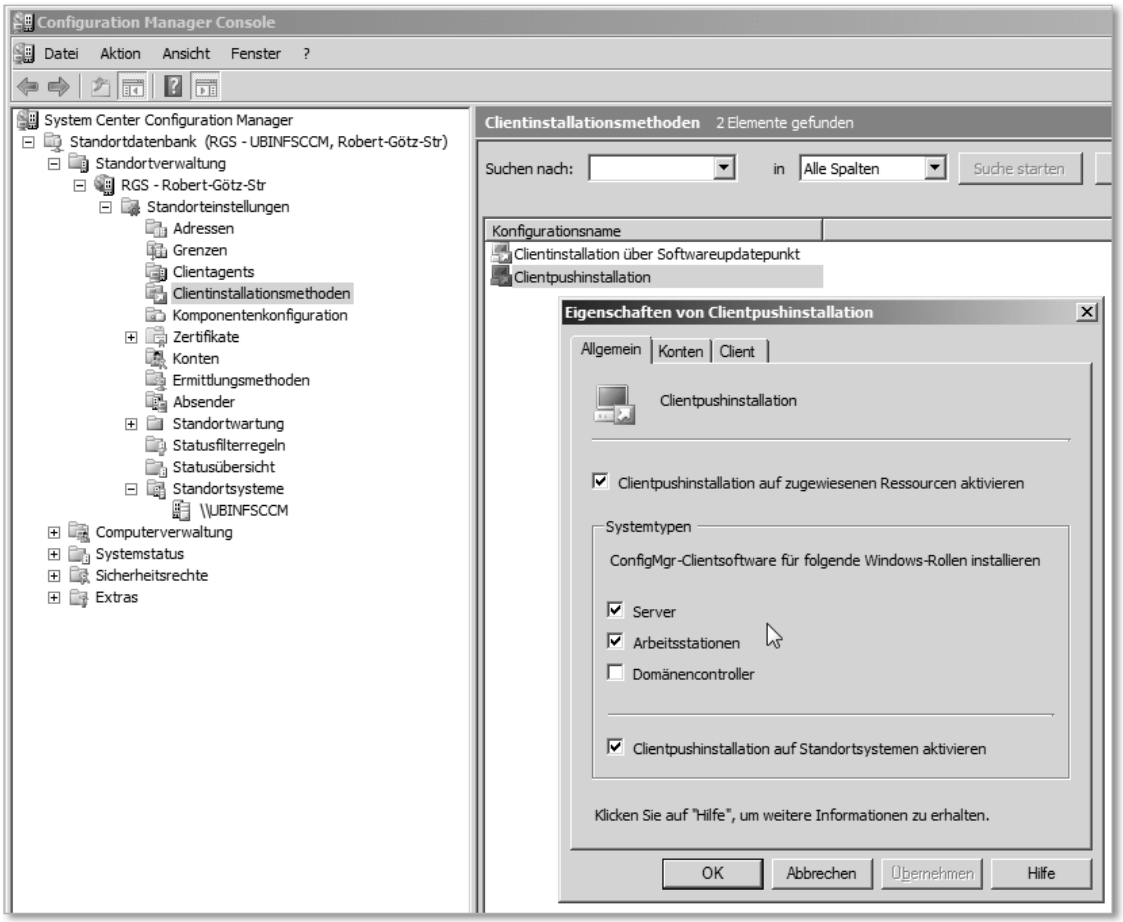


Abbildung 16.9 Für die Installation der Agenten stehen zwei Möglichkeiten zur Verfügung.

16.2.3 Clientagenten

Nun haben Sie zwar bereits erfahren, wie die Configuration-Manager-Agenten installiert werden, allerdings gibt es noch etliches über die Agenten selbst zu berichten. Wie Sie in Abbildung 16.10 sehen können, besteht die Clientkomponente von Configuration Manager aus zehn einzelnen Agenten, die separat aktiviert und konfiguriert werden können. Eine Sonderrolle hat der COMPUTERCLIENT-AGENT inne, der sozusagen der Basis-Agent ist und demzufolge auch nicht abgeschaltet werden kann. Alle anderen Agenten können Sie Ihren Bedürfnissen entsprechend aktivieren bzw. deaktivieren.

Wenn Sie an der Konfiguration eines Agenten Änderungen vornehmen, werden diese automatisch auf die Clients verteilt. Der Richtlinienabruf (zu konfigurieren im COMPUTERCLIENT-AGENT, also dem Basis-Agenten) erfolgt in einem Intervall von standardmäßig 60 Minuten. Entsprechend lange kann es also dauern, bis etwaige Änderungen von den Clients angewendet werden.

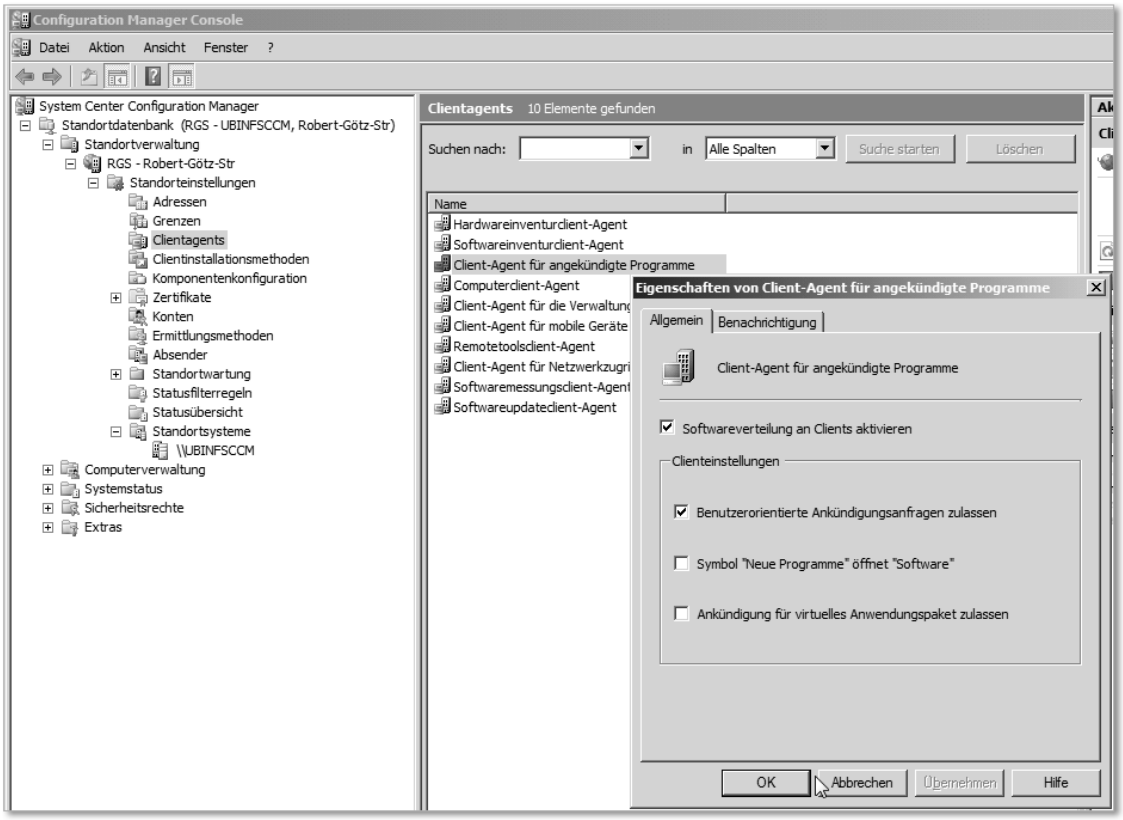


Abbildung 16.10 Der Configuration Manager verfügt über zehn Agenten, die einzeln aktiviert und konfiguriert werden können.

16.3 Inventar und Berichte

Sofern Sie den HARDWAREINVENTURCLIENT-AGENT und den SOFTWAREINVENTURCLIENT-AGENT (Abbildung 16.10) nicht ausgeschaltet haben, werden recht detaillierte Daten zu den verwalteten Systemen gesammelt. Für viele Organisationen sind die Inventardaten sogar wesentlich wichtiger als die übrigen Funktionen, wie Software- oder Betriebssystemverteilung.

Auch wenn es in diesem Windows 7-Buch nicht weiter besprochen wird, ist zu erwähnen, dass Sie die standardmäßig gesammelten Informationen beliebig erweitern können. Die Inventarisierung kann also mehr oder weniger beliebig individualisiert werden.

Ich werde Ihnen in den nachfolgenden Abschnitten zeigen, wie man mit Abfragen und Berichten arbeitet und den *Ressourcen-Explorer* verwendet. Nicht unerwähnt bleiben soll, dass die Inventardaten eine wesentliche Rolle bei der Verteilung von Software spielen: Wenn eine Software nur auf Windows 7-Clients mit mindestens 1,5 GB freiem Speicherplatz auf dem C:-Laufwerk, einem Hauptspeicherausbau von mindestens 2 GB und einer bestimmten Grafikkarte installiert

werden kann, helfen Ihnen die Inventardaten sicherzustellen, dass es keine Unfälle gibt, beispielsweise weil eine Installation auf unpassender Hardware versucht wird.

Konfiguration

Die Sammlung des Hard- und Softwareinventars erfolgt standardmäßig einmal pro Woche. Sie konfigurieren diese Einstellung in den Eigenschaften der jeweiligen Agenten (Abbildung 16.10).

16.3.1 Abfragen

Mit Abfragen können Sie schnell und einfach Fragen zum Inventar beantworten. Die Vielfalt der Anwendungsfälle für Inventarabfragen dürfte nahezu unbegrenzt sein; zu diesem Zweck ist es relativ einfach möglich, eigene Abfragen zu formulieren.

Standardabfragen

Wie Sie in Abbildung 16.11 sehen können, sind bereits einige Standardabfragen vorhanden. Diese brauchen Sie nur selektieren, und schon erscheint im rechten Bereich der Configuration-Manager-Konsole das Ergebnis.

Viel mehr ist zu den standardmäßig vorhandenen Abfragen nicht zu sagen. Interessanter wird es dann im nächsten Abschnitt, in dem es um das Erstellen eigener Abfragen geht.

Eigene Abfragen erstellen

Da die Fragen, die Administratoren und IT-Verantwortliche an die Inventardatenbank haben, sehr vielfältig sein werden, reichen die Standardabfragen natürlich nicht aus: Es müssen eigene her!

Bei der Erstellung eigener Abfragen können Sie sich entweder von grafischen Dialogen helfen lassen, oder Sie formulieren von Hand SQL-Abfragen. Letztendlich erstellen die grafischen Werkzeuge auch nur eine SQL-Abfrage. Diese ist auch jederzeit zugänglich.

Abbildung 16.12 zeigt den ersten Dialog beim Erstellen einer neuen Abfrage. Sie sehen, dass Sie zunächst einen Objekttyp auswählen können. Weiterhin kann die Abfrage auf Wunsch auf eine Sammlung begrenzt werden. Die Details erstellen Sie mit einem weiteren Dialog, den Sie über die Schaltfläche Abfrageanweisung bearbeiten erreichen.

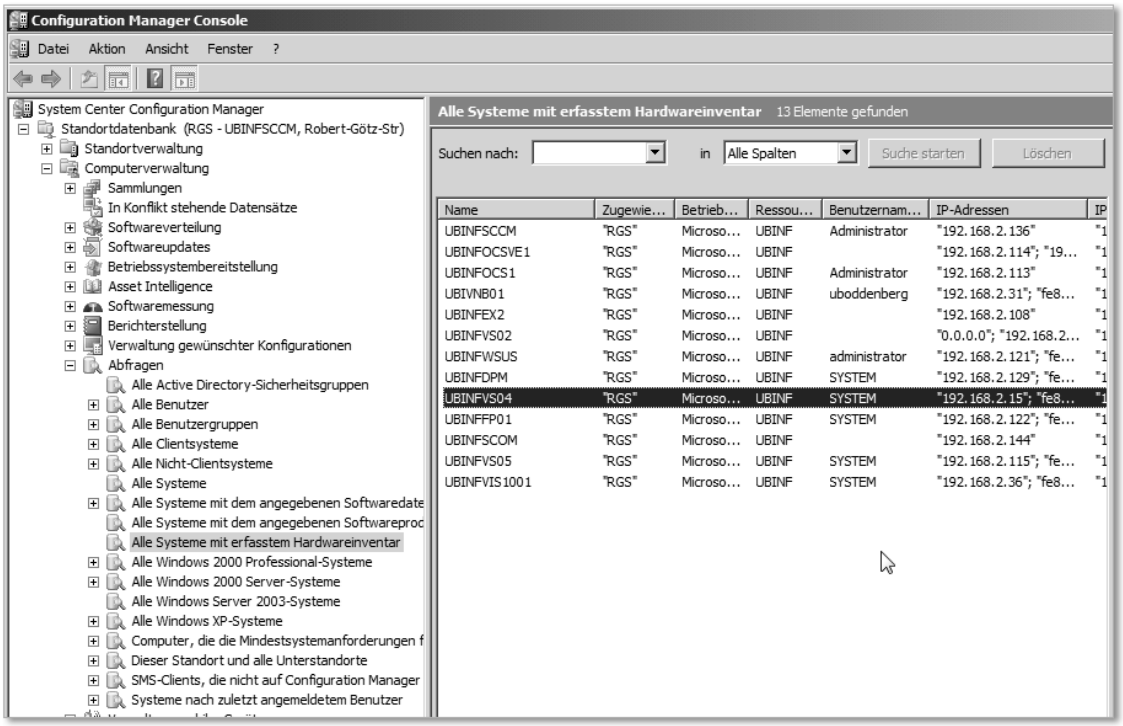


Abbildung 16.11 Um die Standardabfragen auszuführen, brauchen Sie diese einfach nur anzuklicken.

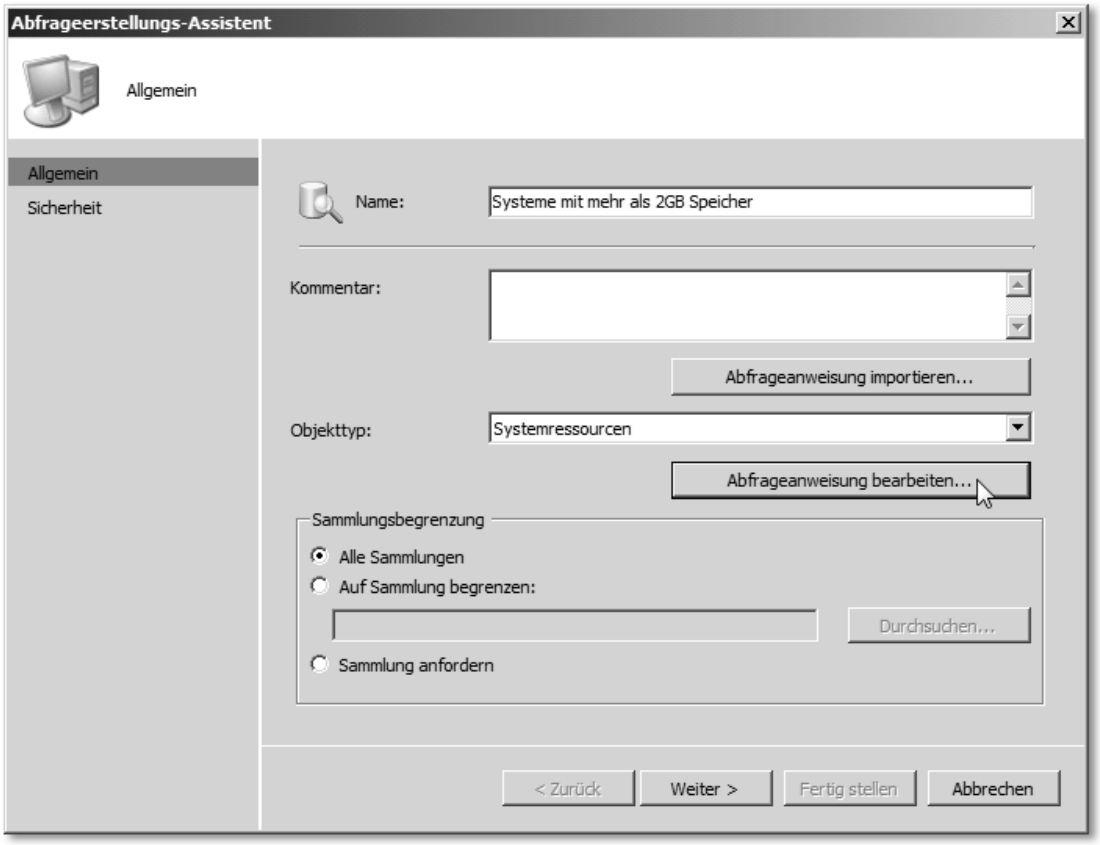


Abbildung 16.12 Die erste Dialogseite beim Erstellen einer neuen Abfrage

Beim Definieren der Abfrageanweisung gibt es zwei wesentliche Aufgaben:

- Sie müssen definieren, welche Attribute im Ergebnis der Abfrage angezeigt werden sollen. Abbildung 16.13 zeigt die notwendigen Einstellungen, um den Namen des gefundenen Systems anzuzeigen. Auf Wunsch kann die Ausgabe auch sortiert werden. Es können beliebig viele Attribute angezeigt werden.
- In Abbildung 16.14 wird definiert, dass nur Systeme mit mehr als 2 000 000 Byte Hauptspeicher (physischer Speicher) in der Ergebnismenge vorhanden sein sollen.

  Es können beliebig viele Kriterien eingegeben werden, die UND-verknüpft werden.

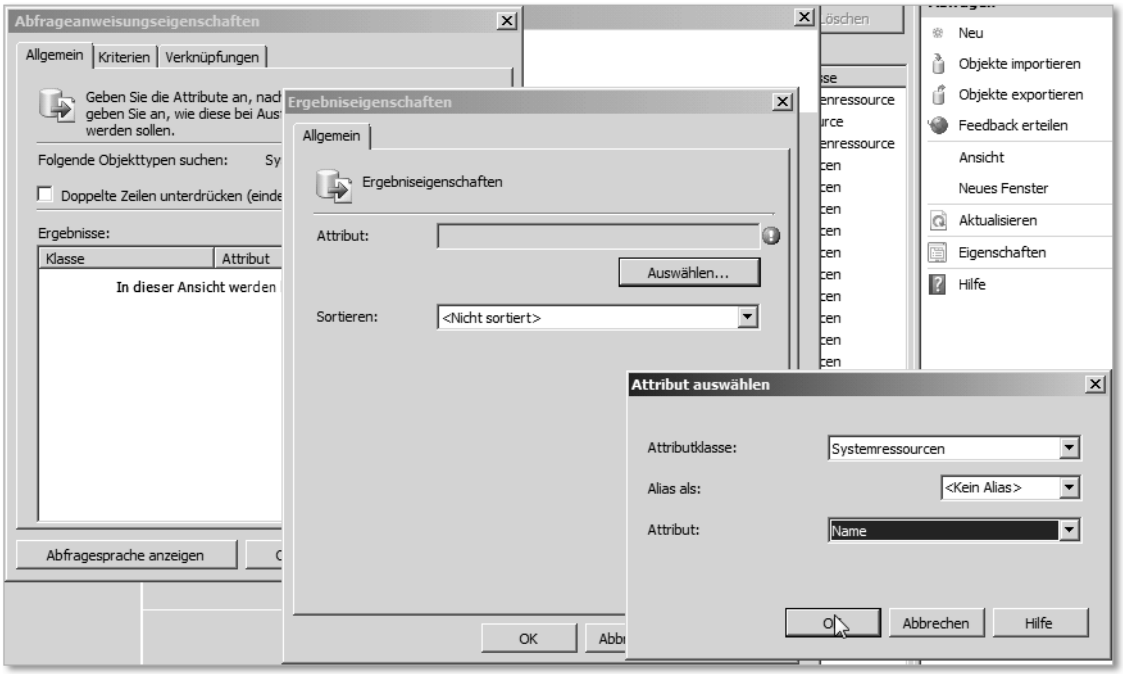


Abbildung 16.13 Hier legen Sie fest, welche Attribute der gefundenen Objekte angezeigt werden sollen.

Auf den Abbildungen sehen Sie übrigens eine Schaltfläche ABFRAGESPRACHE ANZEIGEN. Diese zeigt die resultierende SQL-Anweisung, wobei Sie diese auf Wunsch auch bearbeiten können.

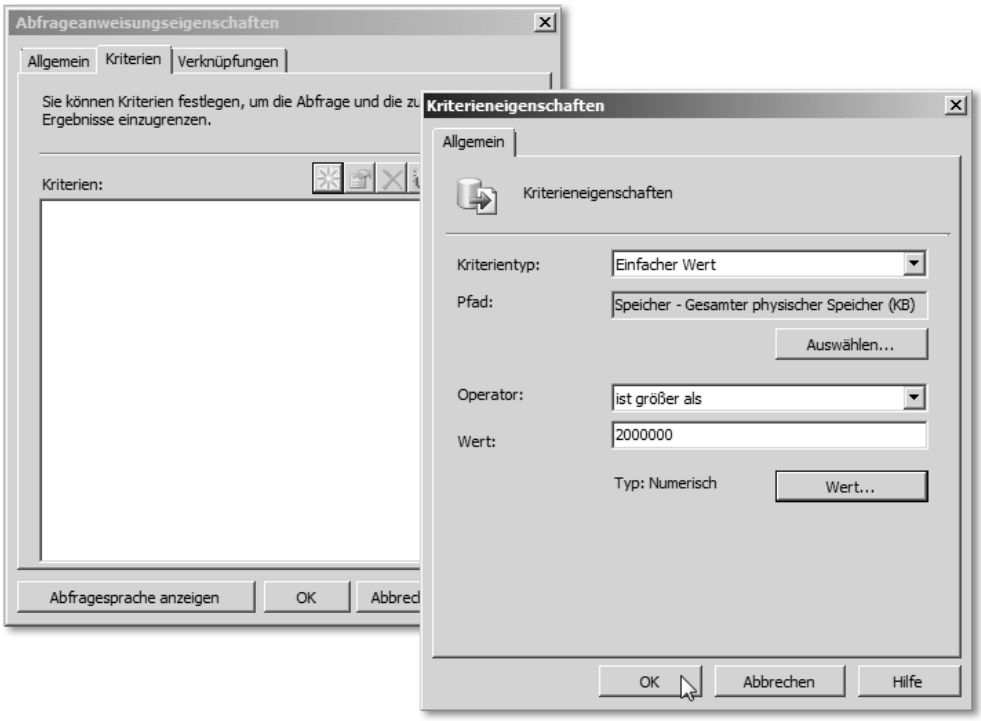


Abbildung 16.14 Mit diesem Dialog können Sie Kriterien definieren.

16.3.2 Ressourcen-Explorer

Falls Sie zu einem System sämtliche gespeicherten Inventarinformationen einsehen möchten, steht der *Ressourcen-Explorer* zur Verfügung. Sie können ihn aus dem Kontextmenü eines Eintrags in der Liste der Abfrageergebnisse oder einer Sammlung aufrufen (Abbildung 16.15).

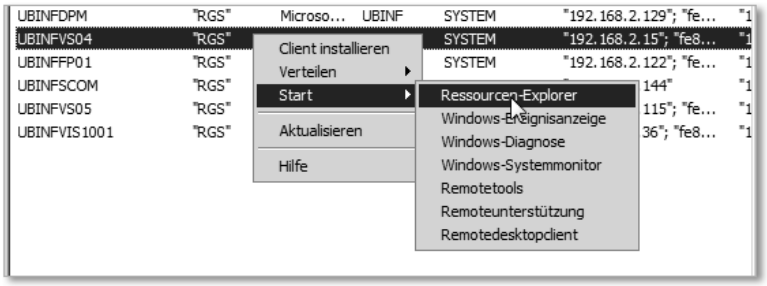


Abbildung 16.15 So rufen Sie den Ressourcen-Explorer auf.

Der Ressourcen-Explorer kennt drei Hauptbereiche:

- Hardware
- Hardwareverlauf (Hier werden Änderungen der Hardwarekonfiguration angezeigt, beispielsweise die Zu- oder Abnahme des physikalisch vorhandenen Hauptspeichers.)
- Software

Abbildung 16.16 zeigt die inventarisierten Hardwareressourcen einer Maschine. Die Daten werden in einer Baumstruktur dargestellt, wobei die meisten Hardwarefragen durch die Vielfalt der Einträge schon recht weitgehend beantwortet werden dürften. Welche Inventardaten gesammelt werden sollen, können Sie übrigens anpassen, sodass auch spezielle Szenarien abgedeckt werden können.

Leider muss angemerkt werden, dass die Hardwareinventur teilweise etwas oberflächlich ist. Wie Sie an Abbildung 16.16 sehen, wird zwar der vorhandene physische Speicher angezeigt, allerdings erhalten Sie keine Informationen über die Größe oder das Timing der verwendeten Module oder die vorhandenen Slots. Da können andere Lösungen deutlich mehr – wobei die Frage zu erörtern bliebe, ob diese zusätzlichen Informationen in der Praxis überhaupt relevant sind.

Abbildung 16.17 zeigt einen Blick in das Softwareinventar. Wie Sie sehen, ist auf meinem Notebook *Corel Paint Shop Pro XI* installiert – da Sie über die vorhandenen Softwarepakete auch Abfragen machen können, lassen sich diverse lizenzierungsrelevante Informationen gewinnen.

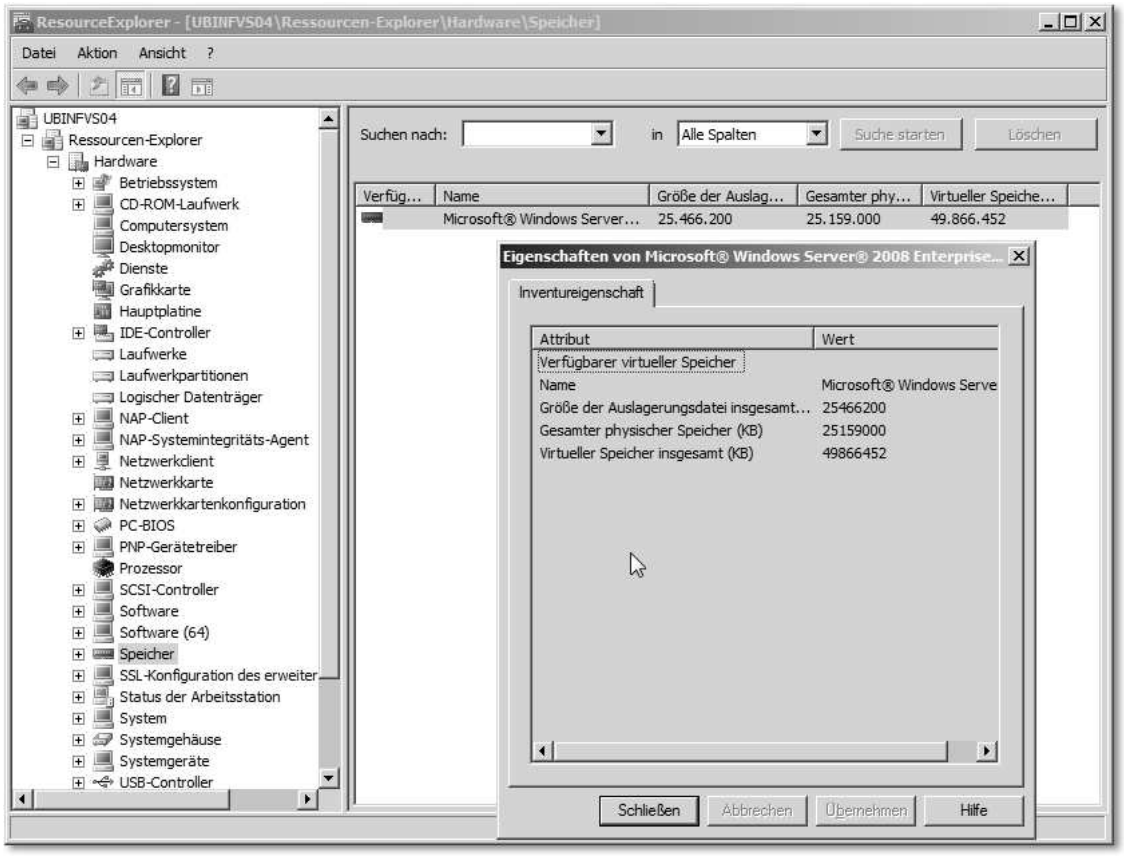


Abbildung 16.16 Dies sind die in der Datenbank gespeicherten Hardwareinventarinformationen – eine hübsche Anzahl, teilweise aber auch recht oberflächlich.

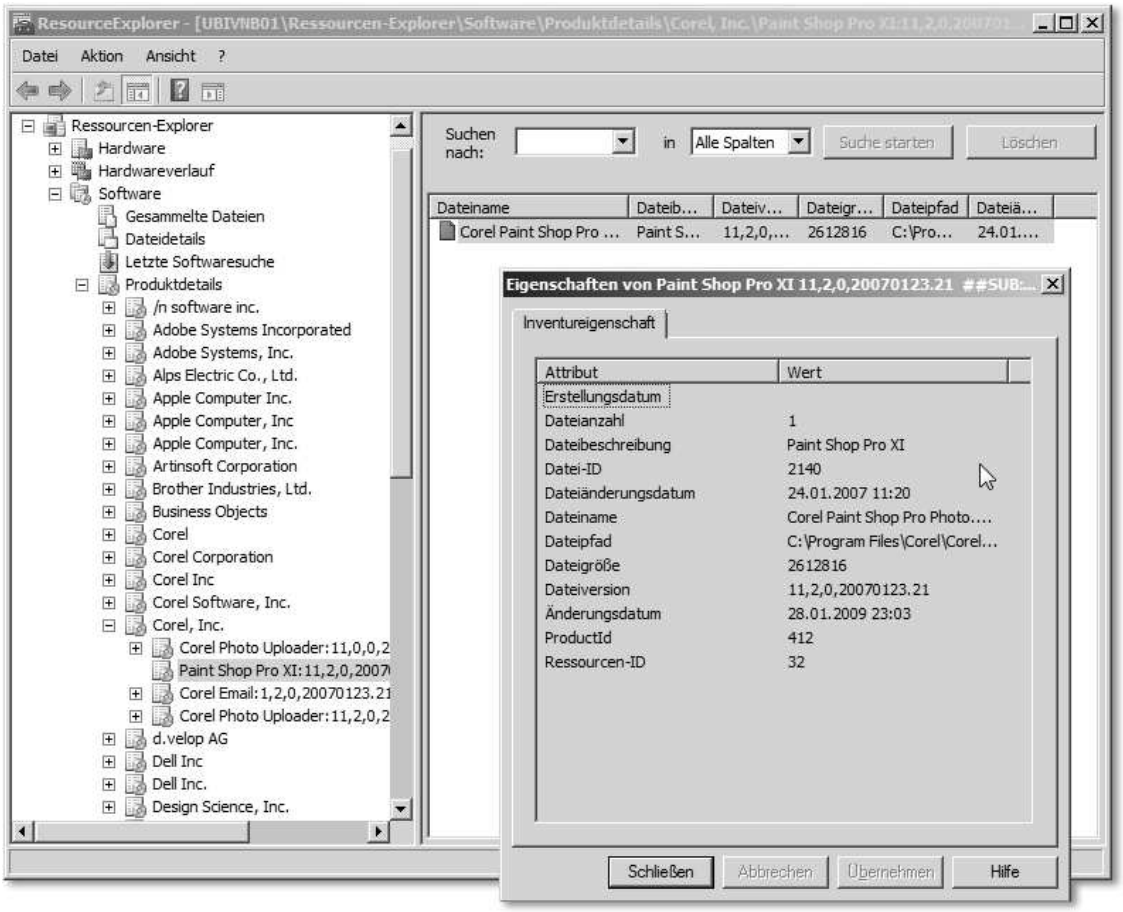


Abbildung 16.17 Die gefundenen Softwareprodukte werden in dieser Rubrik des Ressourcen-Explorers angezeigt.

Weniger schön ist die Gliederung mit fünf unterschiedlichen Corel-Einträgen (COREL, COREL CORPORATION, COREL INC usw.). In den Eigenschaften des Softwareinventurclient-Agenten lassen sich diese Permutationen auf der Registerkarte INVENTURNAMEN zusammenfassen.

16.3.3 Berichte

Die Abfragen liefern zwar alle notwendigen Informationen, wenn Sie managementfähige Ausgaben benötigen, reicht das aber nicht aus – es müssen richtige Berichte her. In der Managementkonsole ist Ihnen vielleicht bereits der Knoten BERICHTE aufgefallen. Vermutlich werden Sie dann aber eine Möglichkeit zum Aufrufen der Berichte vergeblich gesucht haben.

Die Ursache dafür ist, dass standardmäßig die Systemrolle BERICHTERSTATTUNGSPUNKT nicht installiert ist. Sie können diese Rolle beispielsweise dem Configura-

tion-Manager-Standortserver hinzufügen – und schon gibt es im Kontextmenü eines Berichts den Menüpunkt Ausführen (Abbildung 16.18 und Abbildung 16.21).

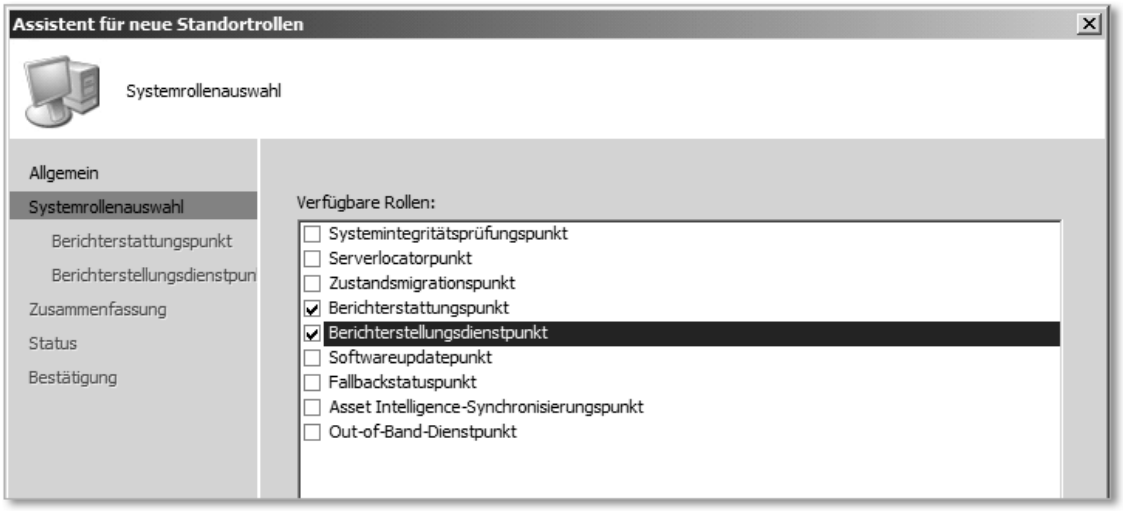


Abbildung 16.18 Bevor Sie mit Berichten arbeiten können, müssen Sie einen Berichterstattungspunkt installieren.

Das Berichtswesen des Configuration Managers ist webbasiert. In Abbildung 16.19 sehen Sie die Hauptseite der webbasierten Berichtsausgabe. Sofern der Bericht Eingabeparameter entgegennimmt, können Sie diese natürlich ebenfalls in der Weboberfläche angeben.

Für die Anzeige öffnet sich dann ein separates Browserfenster. In Abbildung 16.20 sehen Sie den Bericht über Systeme mit weniger als 2000 MB freier Festplattenkapazität – das sieht doch schon ganz ordentlich aus, oder?

Im Knoten Berichte der Konsole können Sie die vorhandenen Berichte anpassen und natürlich auch neue erstellen. Um vorhandene Berichte anzupassen, wählen Sie den Menüpunkt Eigenschaften. Sie können dann die zugrunde liegende SQL-Anweisung bearbeiten, die Berechtigungen bearbeiten und einiges andere mehr. Falls der in Abbildung 16.21 gezeigte Menüpunkt Ausführen nicht vorhanden ist, müssen Sie die Rolle Berichterstattungspunkt installieren (Abbildung 16.18).

Wenn Sie auf Ausführen klicken, wird sich übrigens ein Browserfenster öffnen und direkt den ausgewählten Bericht zeigen – das sieht dann so aus, wie in Abbildung 16.22 gezeigt.

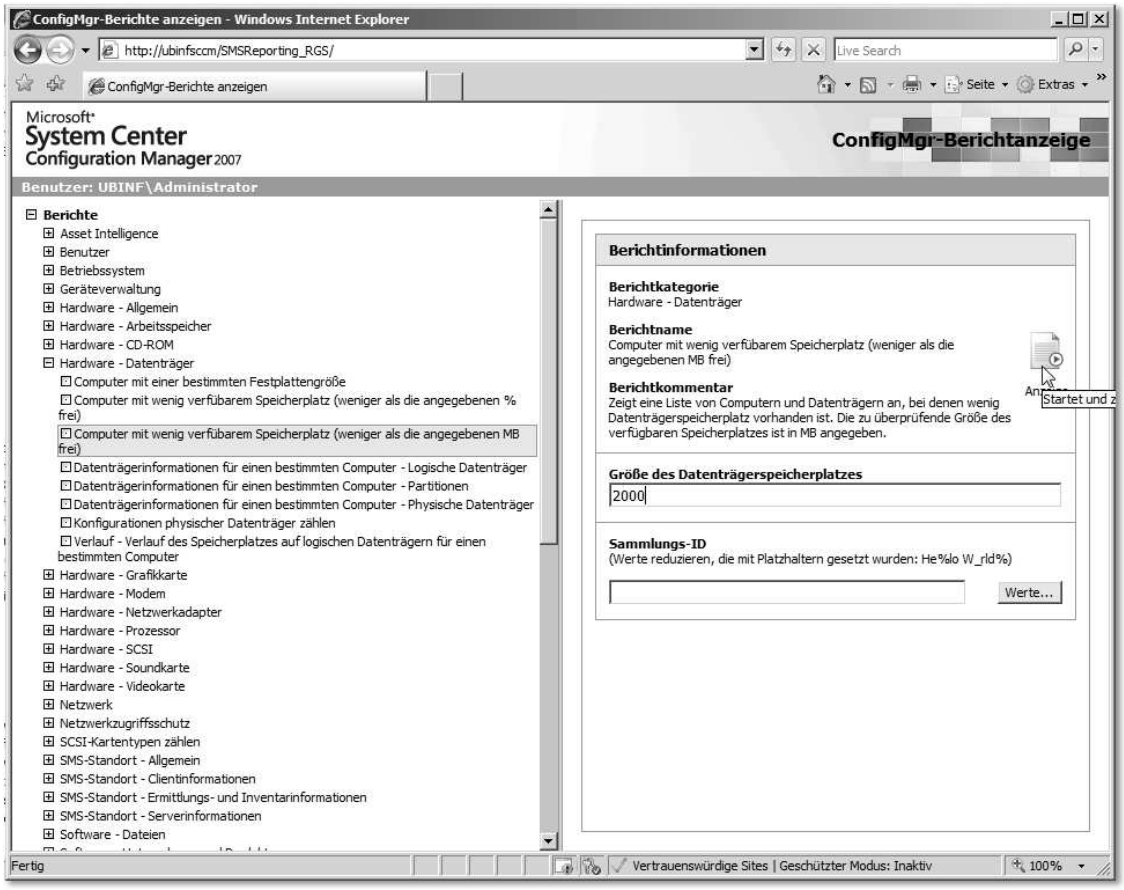


Abbildung 16.19 Die Liste der standardmäßig vorhandenen Berichte in der Weboberfläche

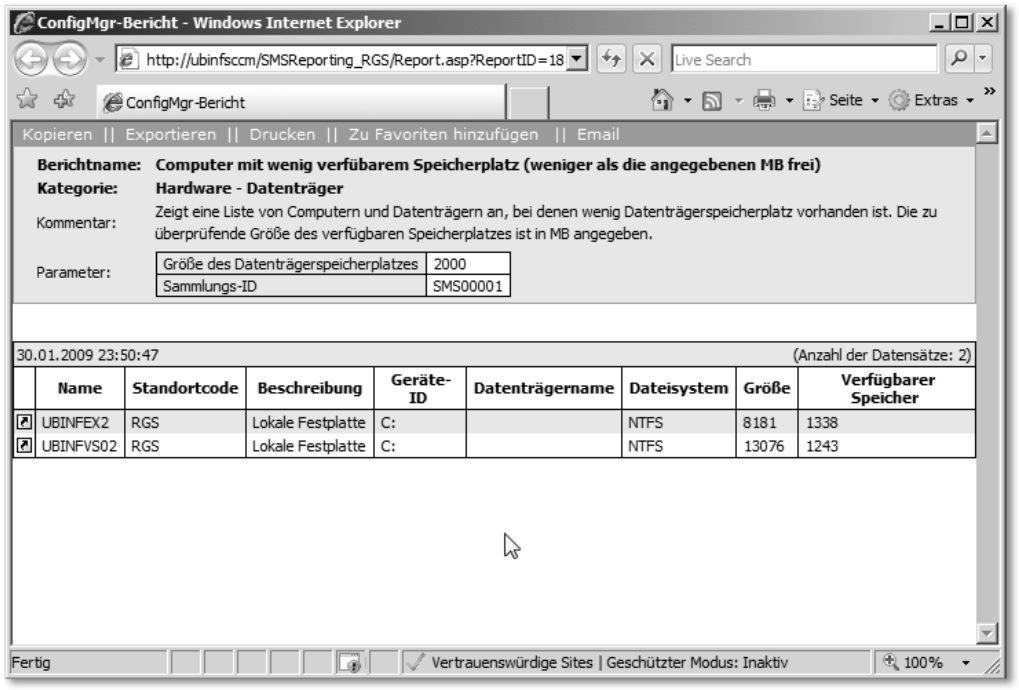


Abbildung 16.20 Dieses sind die Systeme mit weniger als 2000 MB freiem Speicherplatz auf einem Datenträger.

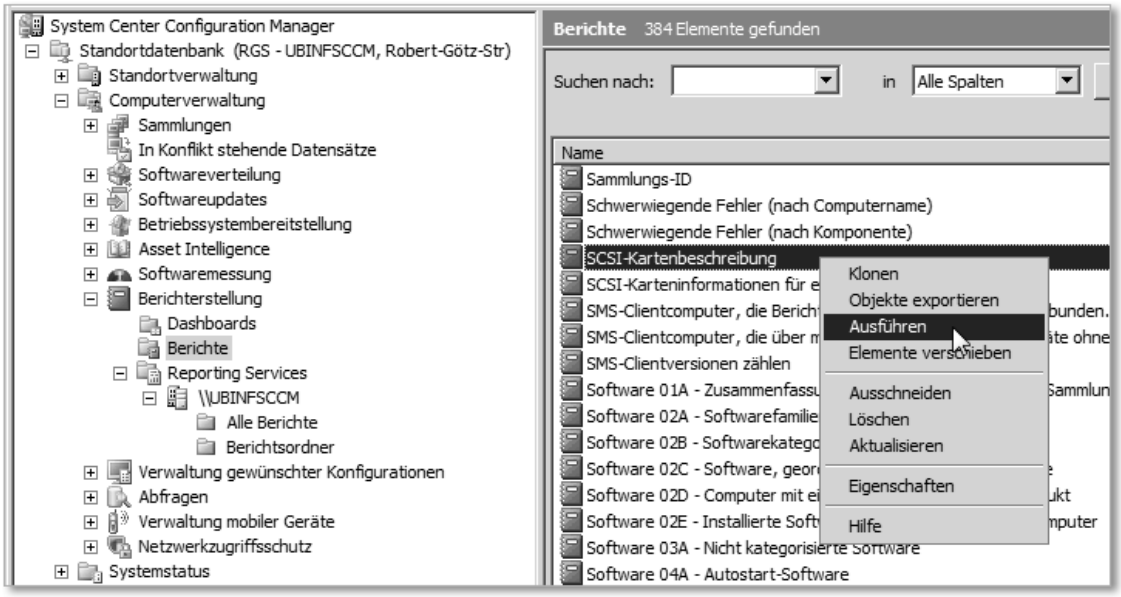


Abbildung 16.21 In der Konsole können neue Berichte erstellt und natürlich auch aufgerufen werden.

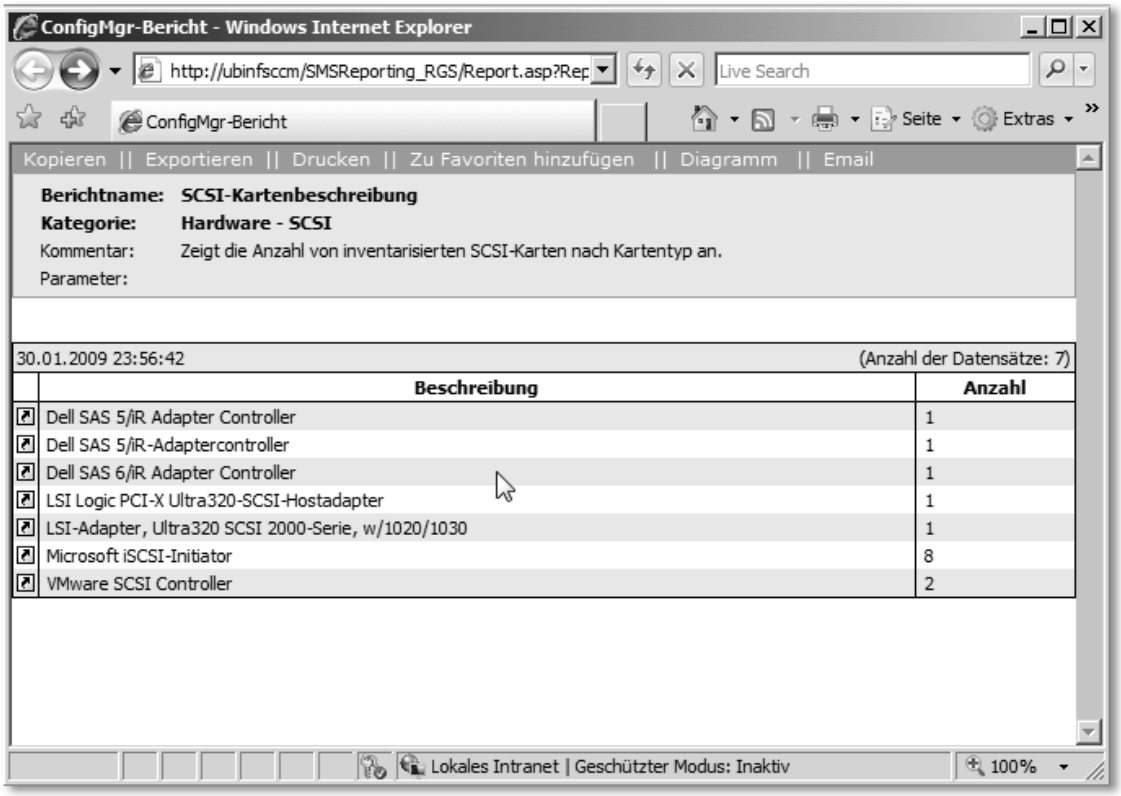


Abbildung 16.22 Der aus der Konsole aufgerufene Bericht wird ebenfalls als Webseite angezeigt.

16.4 Softwareverteilung

Ein großer Teil der Configuration-Manager-Installationen (und die Installationen seiner Vorgängerversionen, also SMS) wird wegen der Softwareverteilung eingeführt worden sein. In der Tat spielt die Softwareverteilung bereits in Organisationen mittlerer Größe eine wesentliche Rolle, denn es ist schlicht und ergreifend unmöglich, dass die IT-Mitarbeiter in mehr oder weniger regelmäßigen Abständen die PCs »besuchen«, um neue Softwareprodukte und/oder Updates einzuspielen.

Ich möchte Ihnen in diesem Abschnitt recht ausführlich zeigen, wie man eine Softwareverteilung mit dem Configuration Manager initiiert und durchführt – so erhalten Sie einen guten Eindruck von der Vorgehensweise mit diesem Produkt. Wer sich bereits mit Softwareverteilung beschäftigt hat, wird wissen, dass in vielen Fällen die Herausforderung nicht darin besteht, die eigentliche Verteilung eines Pakets durchzuführen, sondern darin, das Installationspaket so anzupassen, dass das Ergebnis der Verteilung dann letztendlich Ihren Vorstellungen entspricht: Bei der Installation von *Microsoft Office* kann beispielsweise über *Transform-Dateien* bestimmt werden, welche Bestandteile des Gesamtpakets installiert werden sollen. Es könnte auch Applikationen geben, die über keine verwendbare Installationsroutine verfügen und erst gepackt werden müssen. Es könnte (!) also neben der Beherrschung des Configuration Managers noch etliche andere Aufgabenstellungen geben.

16.4.1 Paketerstellung

Im ersten Schritt müssen Sie ein Configuration-Manager-Paket erstellen. In diesem Beispiel verteile ich die Runtime-Version des *PowerPoint 2007-Viewers*. Dieses Produkt ist kostenlos im Microsoft Download Center erhältlich. Es ist sehr einfach zu installieren, weil lediglich die heruntergeladene EXE-Datei ausgeführt werden muss; eine weitergehende Individualisierung ist nicht notwendig.

»Paketerstellung« bedeutet im Sinne dieses Abschnitts, dass um die Installationsdatei herum ein Configuration-Manager-Paket erzeugt wird, das die notwendigen Metadaten enthält. Es bedeutet nicht (!), dass eine Snapshot-Installation oder dergleichen erstellt wird.

Begriffserklärung

Bei einer Snapshot-Installation wird der Zustand eines Referenz-Computers vor und nach der Installation verglichen, und es werden die Änderungen (z. B. zusätzliche Dateien, Einträge in der Registry u. a.) ermittelt. Diese Änderungen werden dann in ein Installationspaket geschrieben, das auf anderen Computern ausgeführt wird. Das heißt, die Änderungen werden vorgenommen, und so wird die Software installiert.

Es gibt durchaus Softwareprodukte, die nur über diesen Weg zu installieren sind. Im Allgemeinen ist heute aber zu empfehlen, die Installationsroutinen der jeweiligen Hersteller zu verwenden. Das führt im Normalfall zu den besseren Ergebnissen und ist wesentlich (!) einfacher.

Das Ergebnis der Verteilung eines Configuration-Manager-Pakets muss übrigens nicht notwendigerweise die Installation einer Software sein. Das Paket kann beispielsweise auch eine Applikation aufrufen, die ein BIOS-Update durchführt.

Paket erstellen

Das Erstellen des Configuration-Manager-Pakets beginnt im Kontextmenü des gleichnamigen Knotens in der Rubrik SOFTWAREVERTEILUNG. Interessant sind die Möglichkeiten, die Sie in Abbildung 16.23 sehen:

- PAKET startet einen Assistenten, mit dem Sie ein Paket von Grund auf erstellen können. Dies ist beispielsweise dann notwendig, wenn die zu installierende Software eine EXE-Datei als Installationsprogramm verwendet.
- Ein VIRTUELLES ANWENDUNGSPAKET ist ein Paket für die Verwendung mit der Applikationsvirtualisierungslösung *App-V*.
- Falls Sie bereits eine Definitionsdatei für ein Configuration-Manager-Paket haben, beispielsweise vom Hersteller der Software, können Sie diese mit dem Menüpunkt PAKET AUS DEFINITION einlesen.

  Falls Sie eine MSI-Datei verteilen möchten, können Sie ebenfalls diese Option wählen; aus der MSI-Datei können wesentliche Angaben (z. B. der Name der Software, der Hersteller etc.) extrahiert werden.

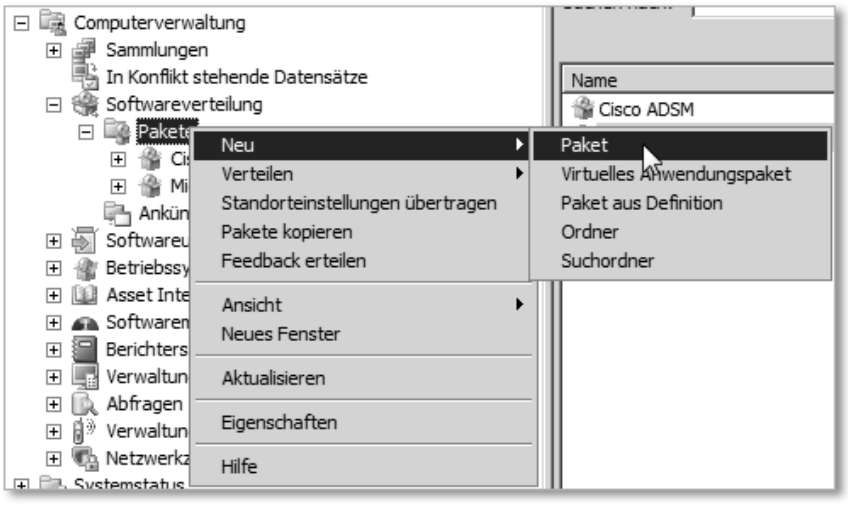


Abbildung 16.23 Hier beginnt das Erstellen eines neuen Pakets.

Bei der Erstellung eines neuen Pakets werden zunächst einige grundlegende Daten abgefragt; Abbildung 16.24 zeigt den Dialog. So simpel geht es aber nicht

weiter, denn auf den nächsten Dialogseiten werden »harte Configuration-Manager-Fakten« abgefragt.

An dieser Stelle sei darauf hingewiesen, dass die hier eingetragenen Informationen nur zur Identifizierung des Pakets für menschliche Administratoren benötigt werden. Sie können also auch »Hugo«, »Klara« und »Emil« in die Felder schreiben – funktionieren würde es trotzdem.

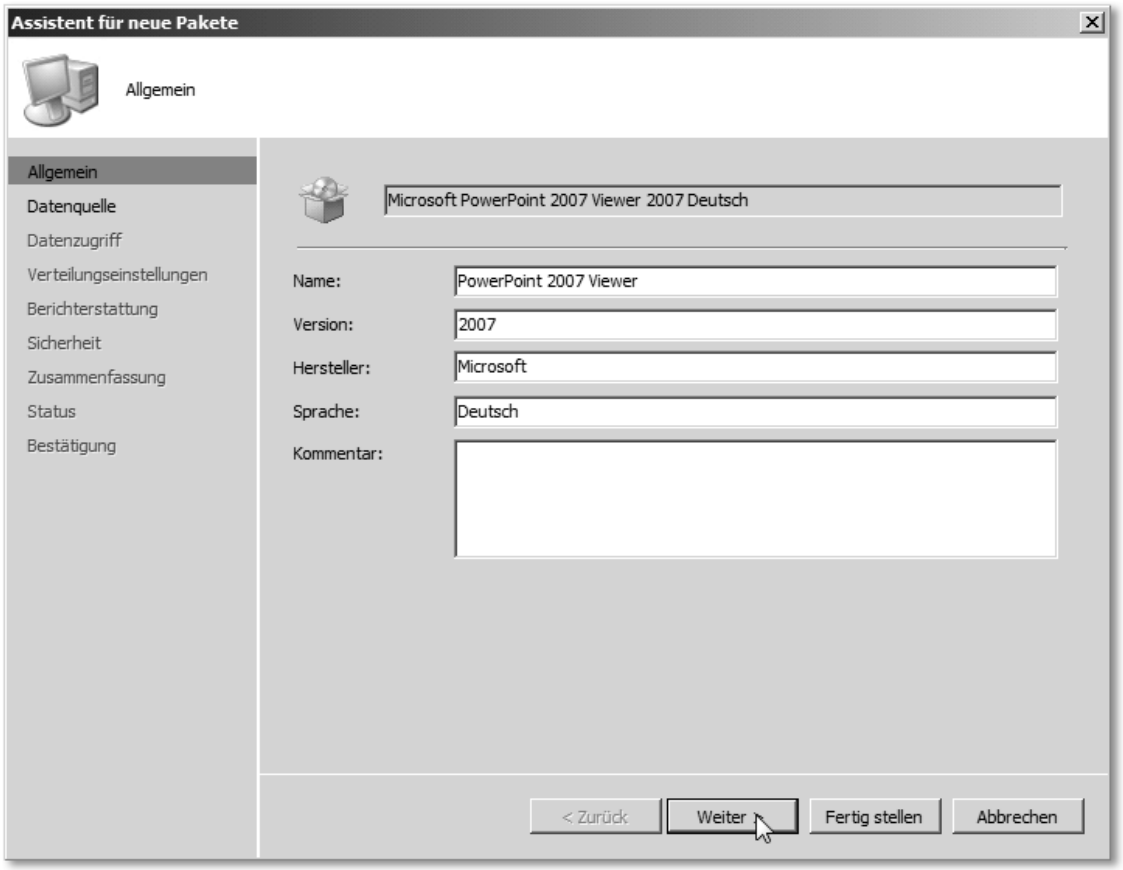


Abbildung 16.24 Einige grundlegende Daten werden zu dem Paket erfasst.

Auf der nun folgenden Dialogseite geht es um die Frage, ob das Paket Quelldateien enthält. Genauer gesagt geht es um Dateien, die sich noch nicht auf den Ziel-PCs befinden. Wenn Sie neue Software installieren, dürfte das stets der Fall sein; wenn Sie im Rahmen des Pakets hingegen eine *netsh*-Anweisung (*netsh* ist ein standardmäßig vorhandenes Kommandozeilenwerkzeug zur Anpassung der Konfiguration) ausführen möchten, benötigt das Paket keine Quelldateien, da *netsh* auf jedem Windows-PC vorhanden ist.

Falls das Paket Quelldateien enthält, müssen Sie einen Pfad zum Quellverzeichnis angeben – das ist einleuchtend (Abbildung 16.25). Interessant sind die beiden Optionen:

- Eine komprimierte Kopie…: Wenn diese Option aktiviert ist, wird auf dem Standortserver eine Kopie der Quelldateien erstellt und von dort aus auf die Verteilungspunkte verteilt. Diese Option ist sinnvoll, wenn damit zu rechnen ist, dass die Quelldateien in absehbarer Zeit nicht mehr am jetzigen Speicherort zu finden sind. Dies ist beispielsweise dann denkbar, wenn die Quelldateien von einer CD/DVD eingespielt werden.
- Dateien immer aus dem Quellverzeichnis abrufen bewirkt, dass die Verteilungspunkte direkt aus dem Quellverzeichnis aktualisiert werden. Wenn also die Quelldateien auf einer Dateiserver-Freigabe liegen und dort mit Sicherheit nicht gelöscht werden, können Sie diese Option wählen.

In der Dialogseite aus Abbildung 16.26 legen Sie fest, wo die Paketdateien gespeichert werden sollen. Standardmäßig werden diese in der allgemeinen Paketfreigabe des Configuration Manager gespeichert. Es kann aber auch eine separate Freigabe erstellt werden.

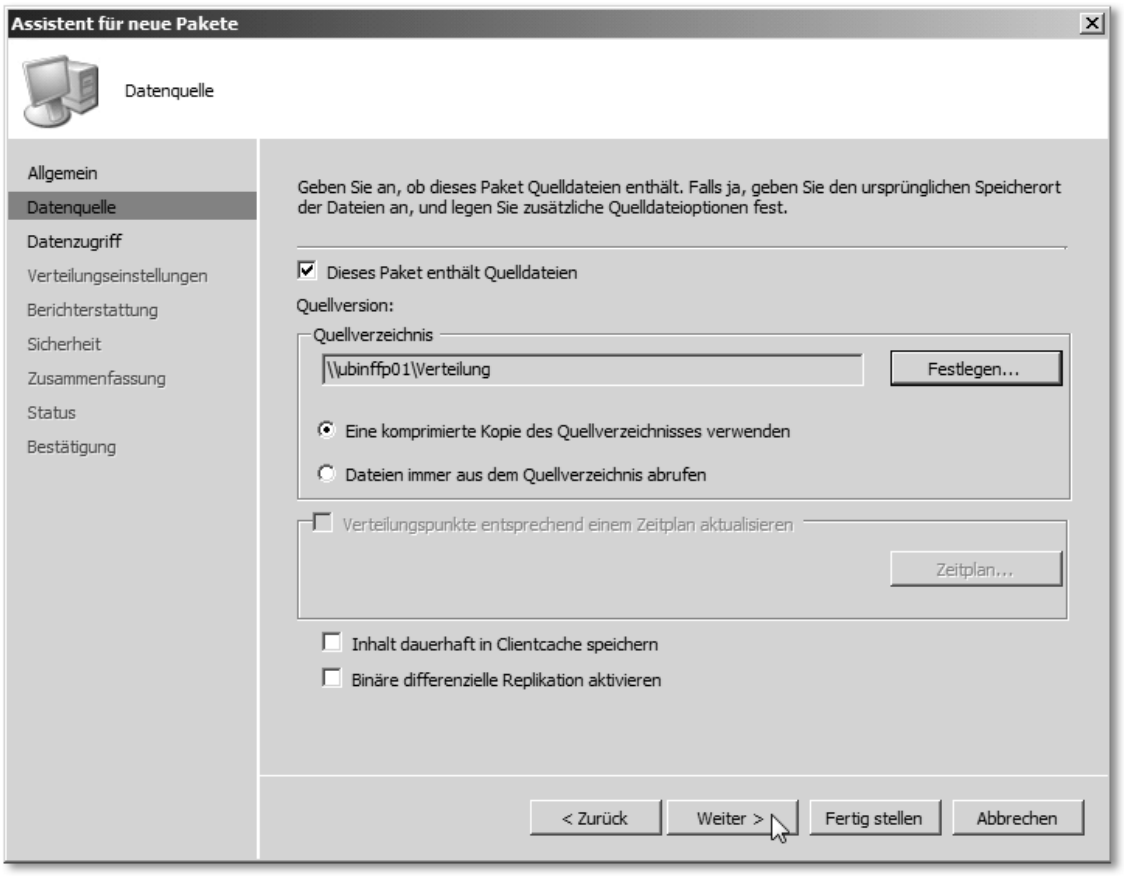


Abbildung 16.25 Wenn das Paket Quelldateien enthält, wird ein Quellverzeichnis angegeben.

In einer größeren Umgebung, die sich über mehrere Standorte verteilt, ergibt sich noch die Frage, wie der Versand des Pakets an untergeordnete Standorte durchgeführt wird.

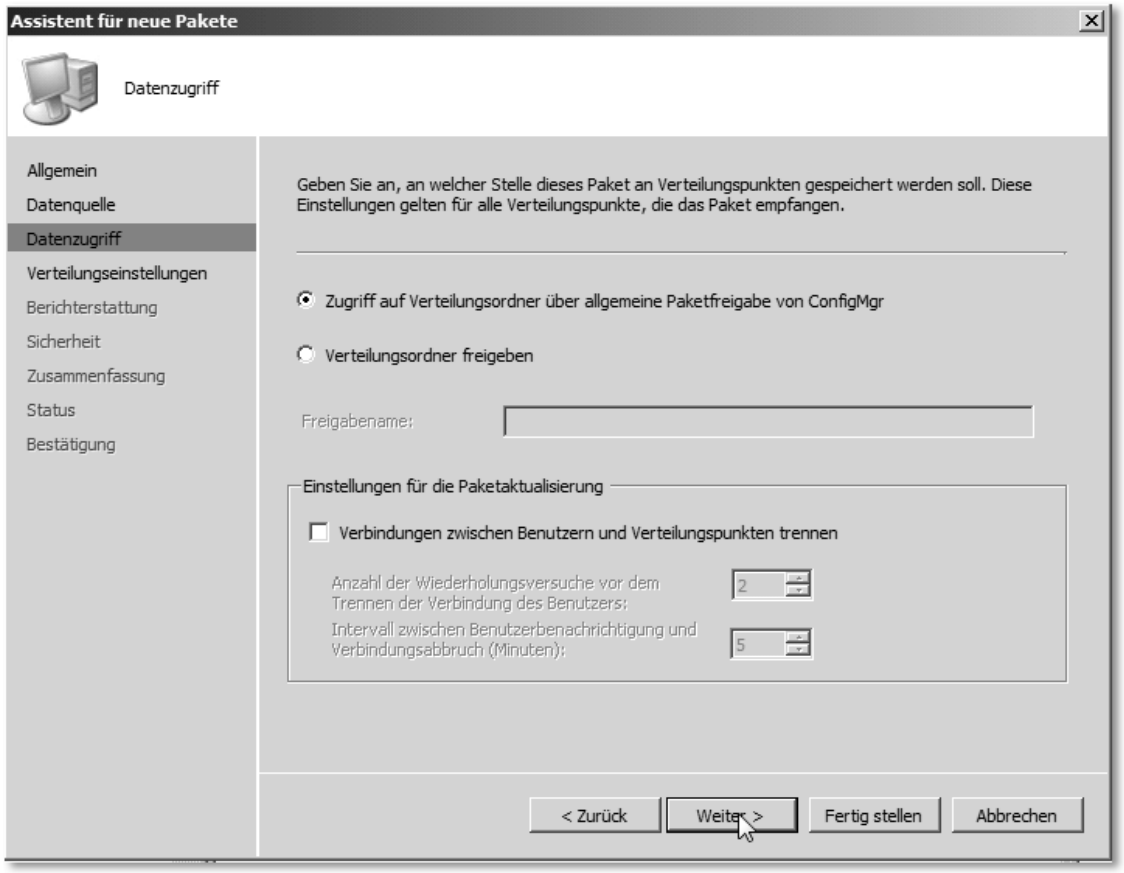


Abbildung 16.26 Hier wird erfasst, wo die Paketdateien gespeichert werden sollen.

Hier gibt es standardmäßig verschiedene Möglichkeiten, unter anderem auch einen ISDN-Sender und einen X.25-Sender – im Zeitalter von Internet und VPN dürfte hier aber immer der Standardsender in Frage kommen (Abbildung 16.27).

Auf dieser Dialogseite finden Sie auch eine Einstellung für ZWEIGVERTEILUNGSPUNKTE – dies können beispielsweise Freigaben auf normalen PCs sein, die in einer kleineren Niederlassung vorhanden sind. Für diese ist eine Sonderbehandlung möglich, bei der die Installation per Postversand der Paketdateien nebst Einspielen durch eine Person vor Ort erfolgt.

Für die Kommunikation zwischen Configuration-Manager-Standorten gibt es diese Post-Option übrigens auch: Sie trägt dort den hübschen Namen COURIER SENDER.

Sie haben nun zwar ein Paket erstellt, allerdings hat dieses noch keinerlei Funktion; ich zeige Ihnen daher im nächsten Abschnitt, wie Sie den Configuration-Manager-Agenten dazu bringen, die Installation auch tatsächlich zu starten.

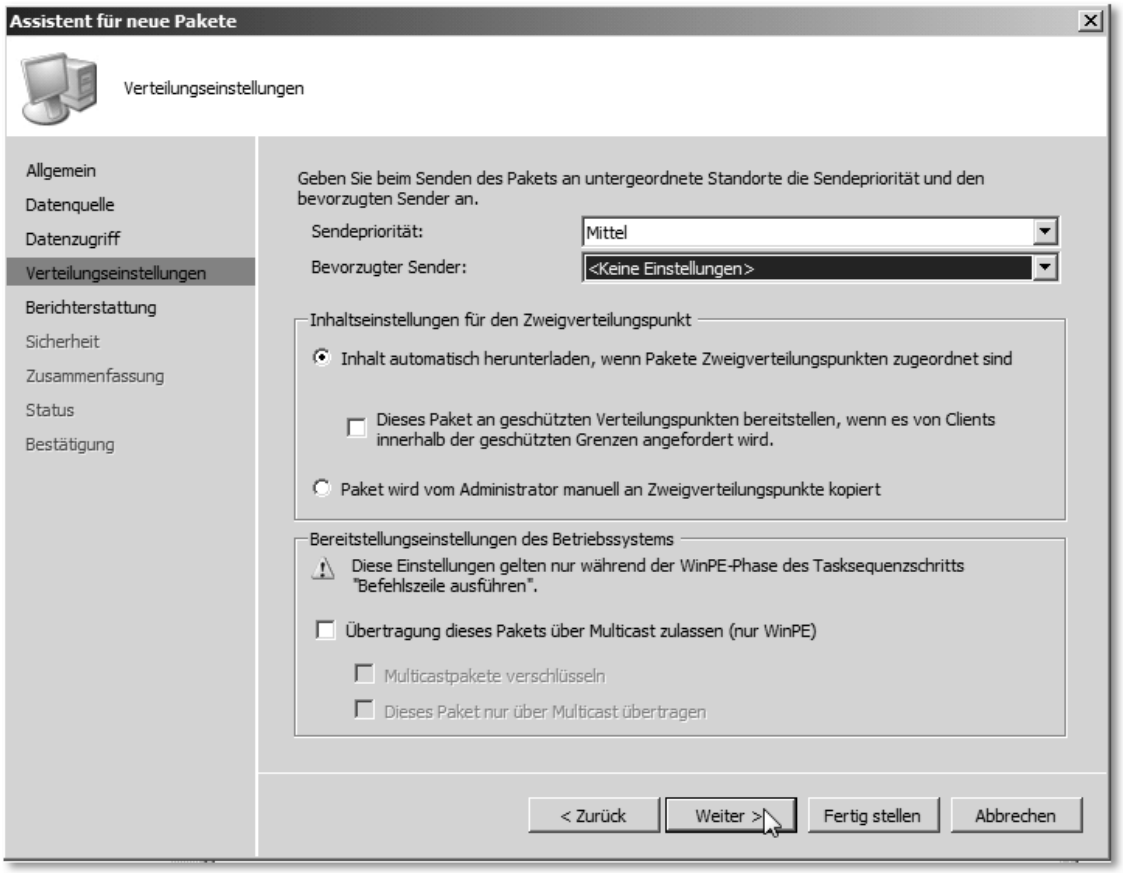


Abbildung 16.27 Dies sind die Einstellungen für die Distribution des Pakets an die Verteilungspunkte.

Programm hinzufügen

Erweitern Sie nun das neu erzeugte Paket. Sie werden einige untergeordnete Knoten vorfinden, von denen uns zunächst PROGRAMME interessiert. Stellen Sie sich vor, dass eine Installations-CD ins Laufwerk eingelegt ist – gut, aber das hilft zunächst für die Installation recht wenig, denn irgendjemand muss den Installationsvorgang starten. Ungefähr so können Sie sich die Funktion der Programme innerhalb eines Pakets vorstellen – der Vergleich passt zwar nicht ganz, Fakt ist aber, dass die Installation nicht beginnen wird, wenn Sie das Installationsprogramm nicht als Programm innerhalb des Pakets eintragen. Der Vorgang wird von einem Assistenten begleitet, den Sie so aufrufen, wie es in Abbildung 16.28 gezeigt ist.

Auf der ersten Dialogseite des Assistenten wird schlicht und ergreifend die auszuführende Befehlszeile eingetragen, in diesem Fall der Aufruf des Installationsprogramms (Abbildung 16.29).

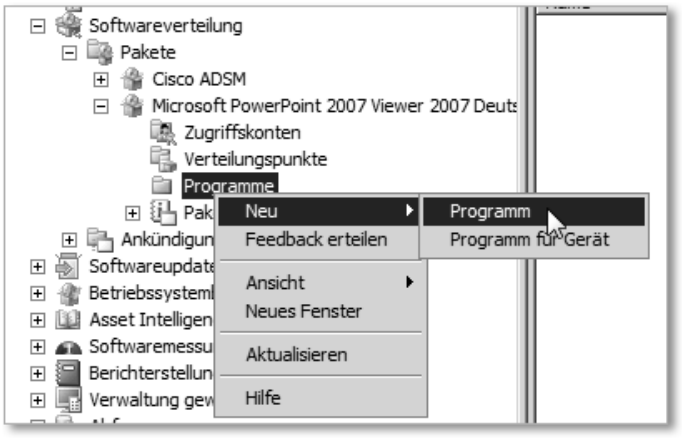


Abbildung 16.28 Sie können dem neu erstellten Paket ein oder mehrere Programme hinzufügen.

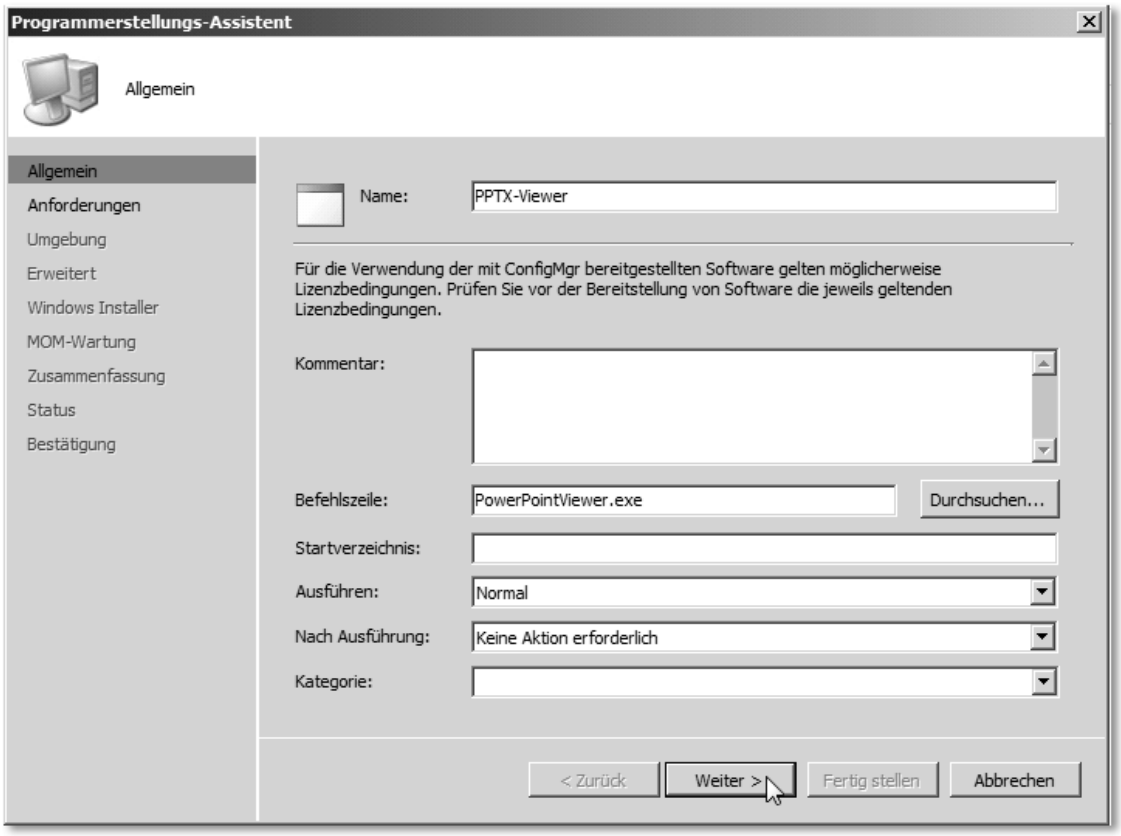


Abbildung 16.29 Als Programm geben Sie die (ausführbare) Installationsdatei an. Eventuelle Parameter wie »/quiet« können Sie hier ebenfalls konfigurieren.

Bedenken Sie, dass eventuell Aufrufparameter erforderlich sind, um eine automatische Installation durchzuführen. Ansonsten könnte es passieren, dass das Installationsprogramm in einem Willkommensbildschirm steht und es nicht weitergeht. Im Fall des *PowerPoint-Viewer*-Installationsprogramms lautet der Parameter `/quiet`. Dieser wird hinter dem Programmaufruf in der Befehlszeile eingetragen.

Zu dem Programm können noch diverse weitere Parameter konfiguriert werden. In Abbildung 16.30 sehen Sie eine Dialogseite, auf der Sie unter anderem spezifizieren können, auf welchen Clientplattformen das Programm ausgeführt werden kann.

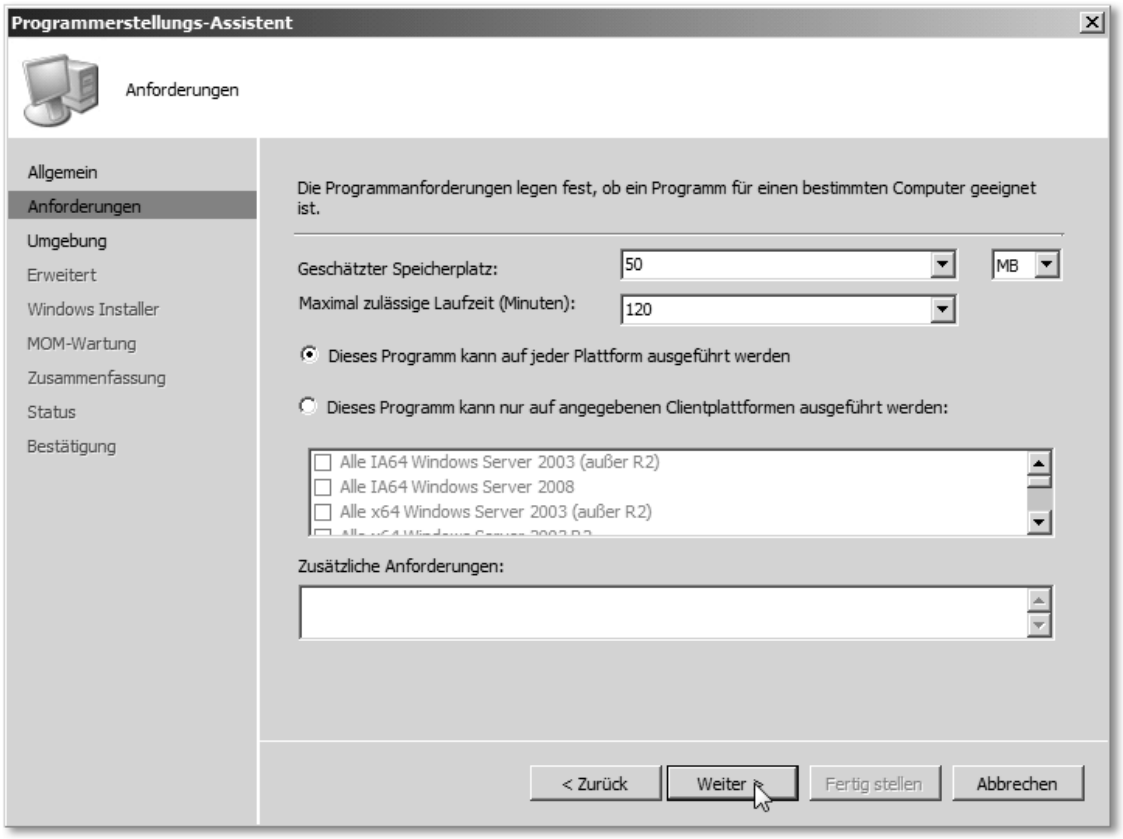


Abbildung 16.30 Bei einem Programm können Sie Plattformeinschränkungen konfigurieren und Angaben zu Speicherplatz und Laufzeit machen.

Abbildung 16.31 und Abbildung 16.32 zeigen weitere Dialogseiten, die eine genaue Definition der Ausführung des Programms ermöglichen. Dies sind zum Teil absolut fundamentale Aspekte, die ich hier aber nicht im Detail diskutieren möchte. Die Optionen sind weitgehend selbsterklärend.

Verteilungspunkte verwalten

Ein Configuration-Manager-Client erhält die zur Ausführung des Pakets notwendigen Dateien von einem Verteilungspunkt. Sie müssen also den Configuration Manager anweisen, das Paket auf die gewünschten Verteilungspunkte zu kopieren. Unterhalb des Pakets befindet sich ein Knoten VERTEILUNGSPUNKTE, in dessen Kontextmenü der Assistent zum VERWALTEN DER VERTEILUNGSPUNKTE aufgerufen werden kann (Abbildung 16.33).

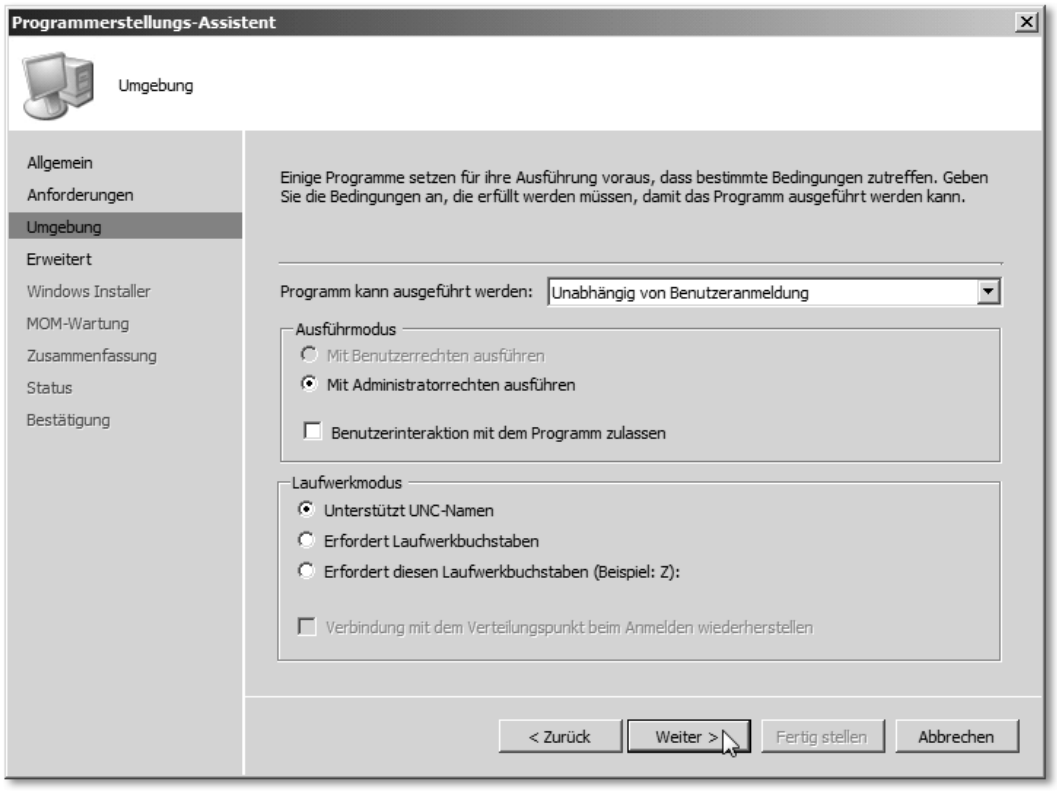


Abbildung 16.31 Auf dieser Dialogseite konfigurieren Sie beispielsweise, dass die Ausführung unabhängig von der Benutzeranmeldung mit Administratorrechten erfolgen soll.

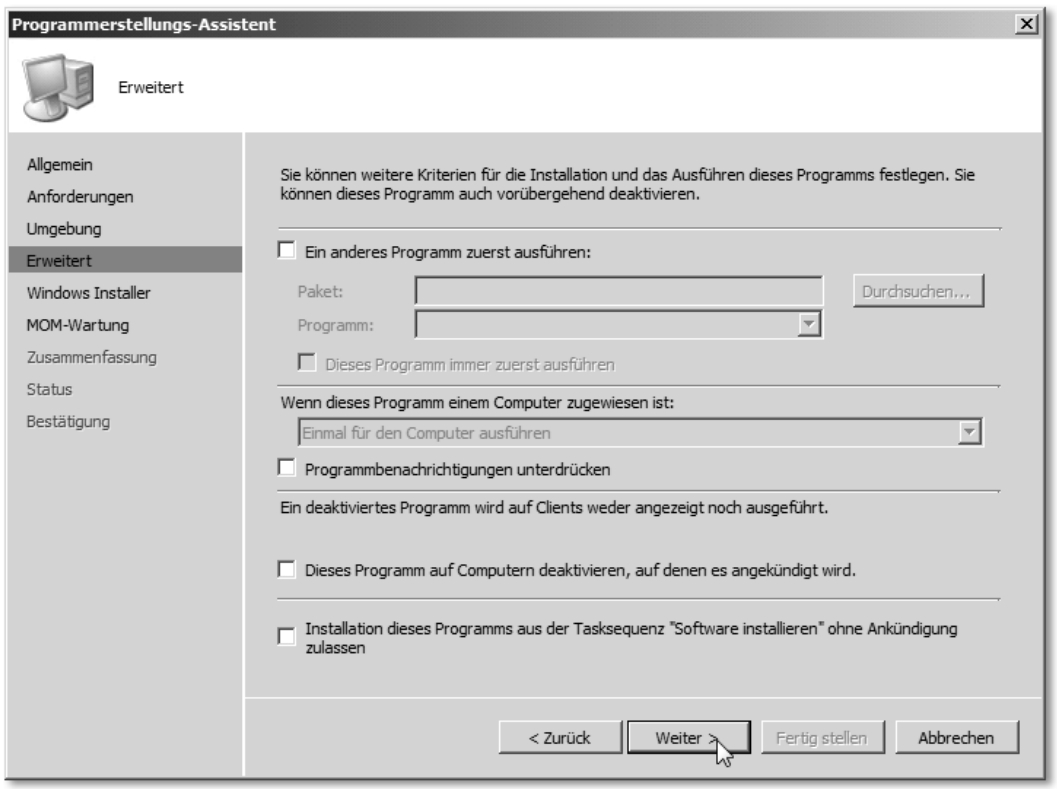


Abbildung 16.32 Hier können Sie diverse weitere Feinheiten festlegen.

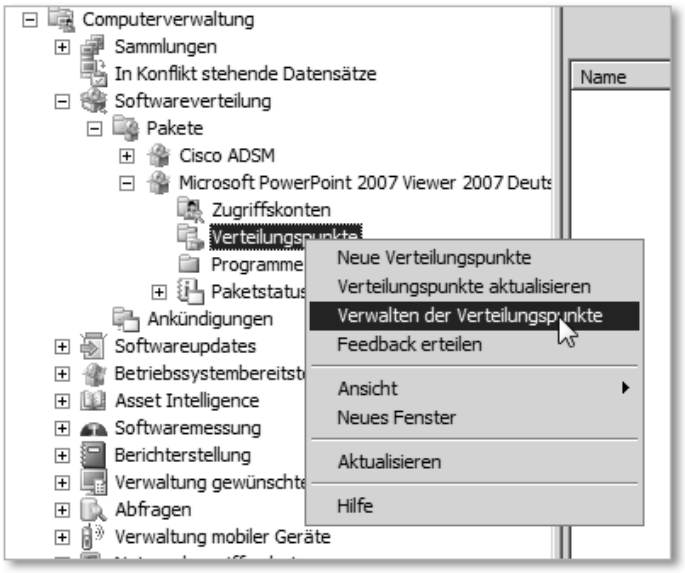


Abbildung 16.33 Damit die Clients das Paket ausführen können, müssen Sie einen oder mehrere Verteilungspunkte konfigurieren.

Der Assistent kann verschiedene Aufgaben ausführen, beispielsweise das Paket in neue Verteilungspunkte kopieren, vorhandene Verteilungspunkte aktualisieren und einiges andere mehr (Abbildung 16.34).

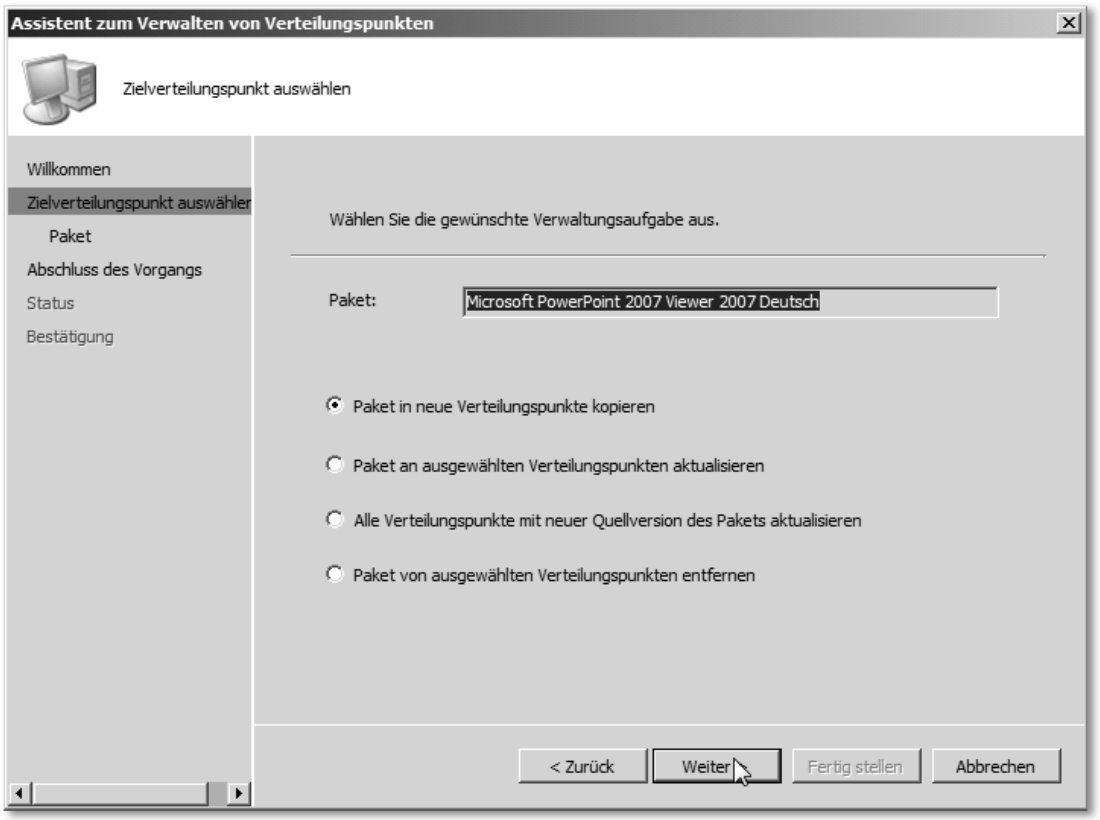


Abbildung 16.34 Mit diesem Assistenten können Sie neue Verteilungspunkte konfigurieren oder bestehende aktualisieren.

Wenn Sie die Funktion zum Kopieren des Pakets in neue Verteilungspunkte ausgewählt haben, ist der nächste Schritt die Auswahl der Verteilungspunkte. Es werden alle Verteilungspunkte des Standorts angezeigt, die Sie dann selektieren können (Abbildung 16.35).

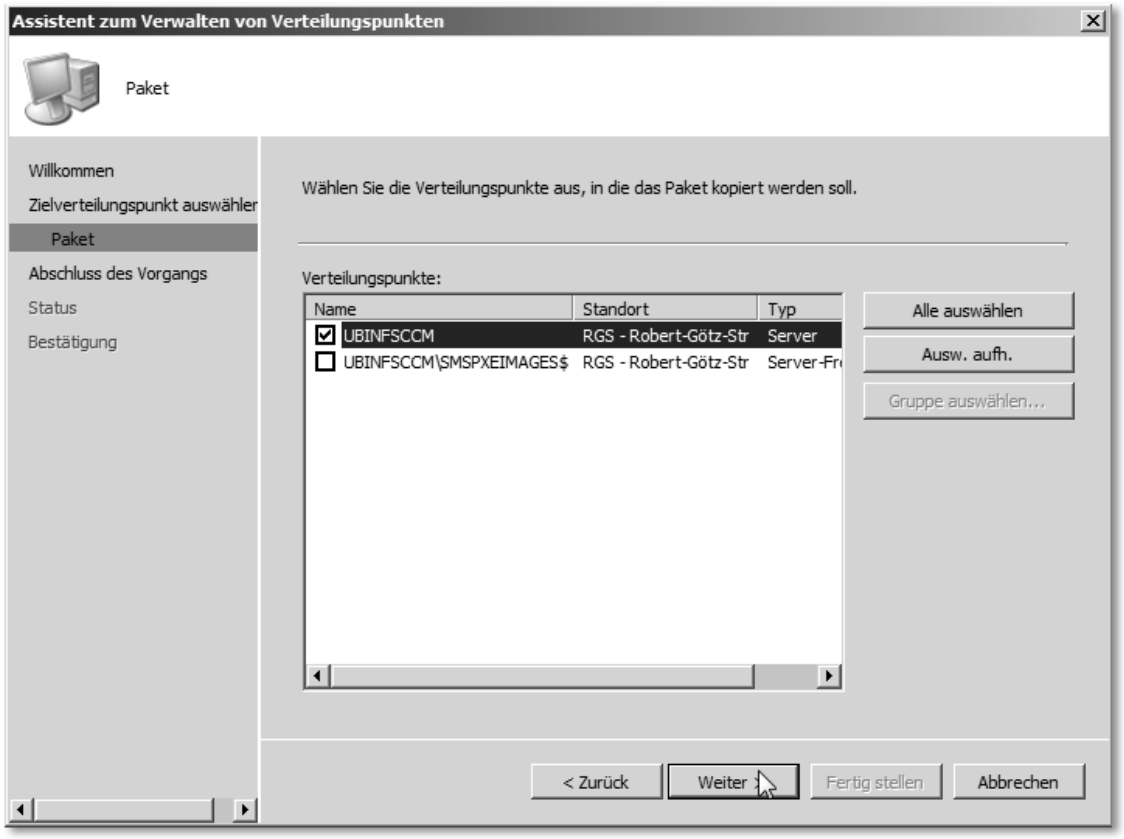


Abbildung 16.35 Auswahl der Verteilungspunkte

Ob das Paket auf den Verteilungspunkten angekommen ist, können Sie unterhalb des Knotens PAKETSTATUS prüfen. In der Übersicht aus Abbildung 16.36 sehen Sie, dass es keine Fehler gegeben hat. Das Paket kann also nun angekündigt werden.

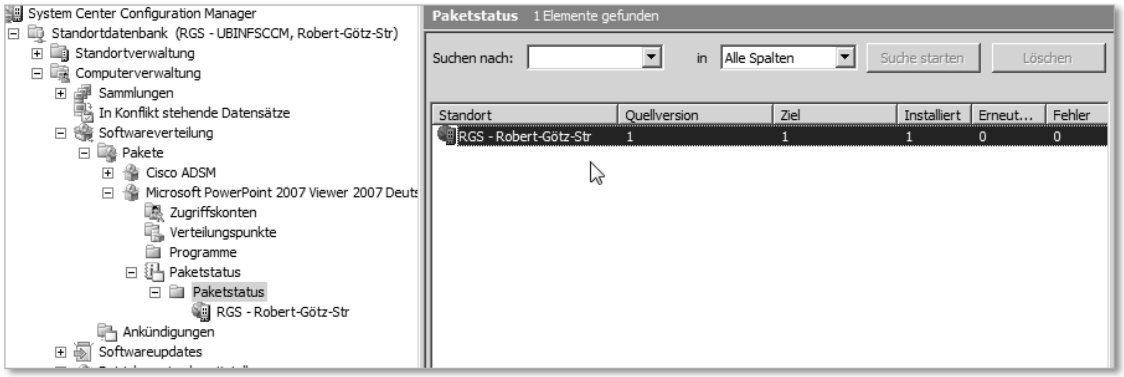


Abbildung 16.36 Hier können Sie kontrollieren, ob das Paket auf den Verteilungspunkten angekommen ist.

16.4.2 Ankündigung erstellen

Damit das Paket auf einem oder mehreren Systemen installiert wird, muss es angekündigt werden. Dies können Sie beispielsweise dadurch initiieren, dass Sie im Kontextmenü einer Sammlung den Menüpunkt VERTEILEN • SOFTWARE wählen.

Die Verteilung von Software ist grundsätzlich nur an Sammlungen möglich, allerdings verfügen die Einträge von PCs ebenfalls über diesen Menüpunkt. Im Hintergrund wird dann eine Sammlung angelegt, in der sich nur das eine System befindet.

Das Ankündigen eines Pakets kann übrigens auch im Kontextmenü eines Pakets initiiert werden. Der Menüpunkt heißt auch VERTEILEN • SOFTWARE. Wenn Sie im Kontextmenü einer Sammlung oder eines PCs beginnen, ist der erste Schritt die Auswahl des anzukündigenden Pakets (Abbildung 16.37).

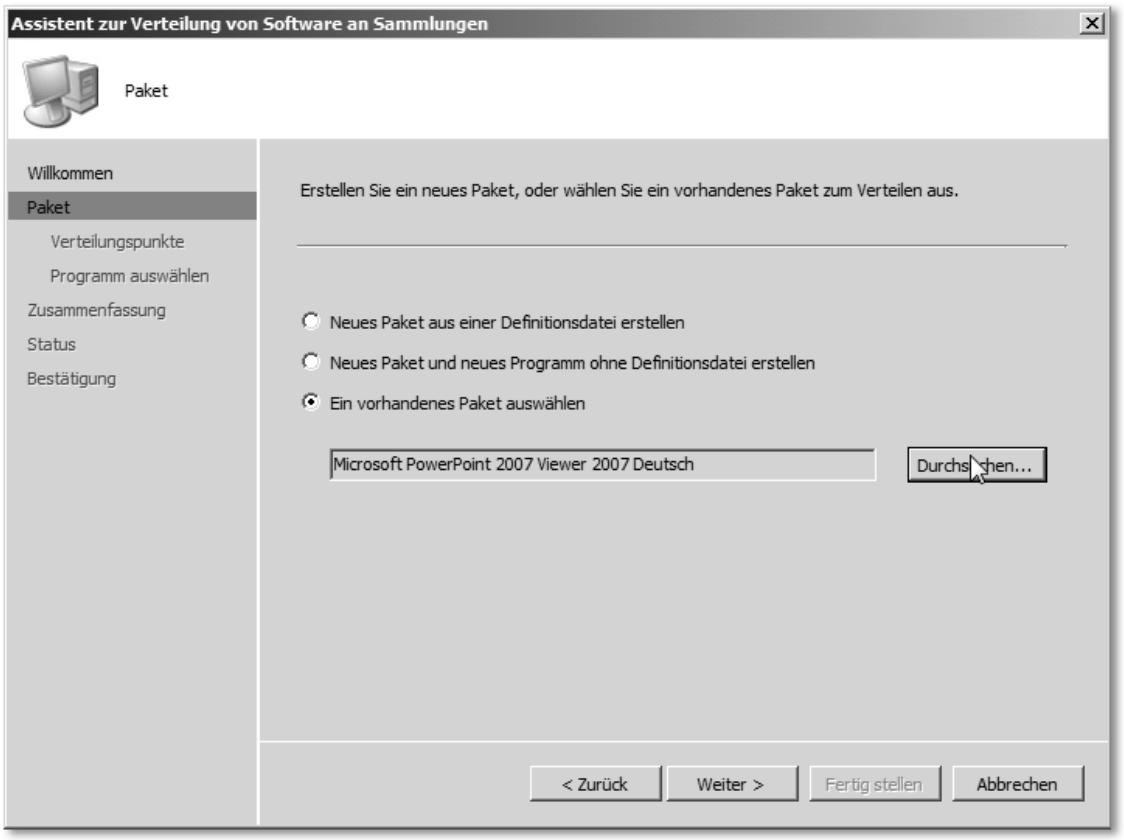


Abbildung 16.37 Der Assistent zur Ankündigung eines Pakets

Im nächsten Schritt legen Sie die zu verwendenden Verteilungspunkte fest. Wenn beim Paket bereits Verteilungspunkte zugewiesen sind, werden diese ausgewählt sein (Abbildung 16.38). Sofern das Paket mehrere Programme enthält, wählen Sie das auszuführende Programm aus (Abbildung 16.39).

Abbildung 16.38 Sie können auswählen, welche Verteilungspunkte genutzt werden sollen.

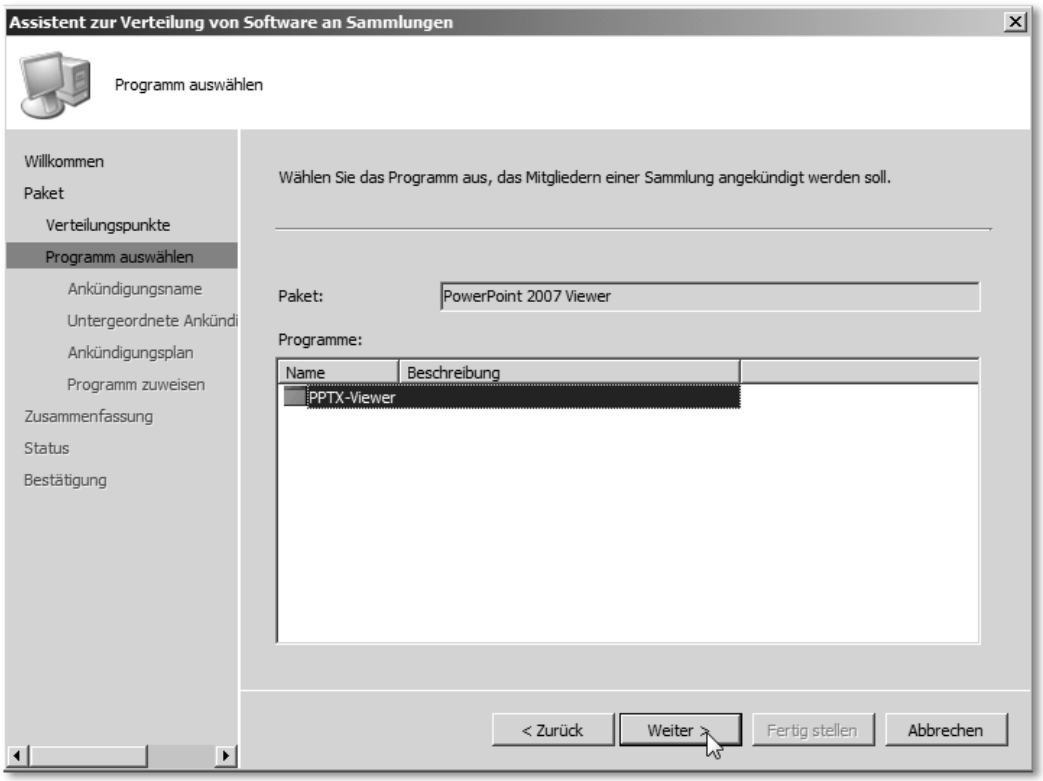


Abbildung 16.39 Angekündigt wird ein Programm aus dem Paket, in diesem Fall also das Installationsprogramm für den PowerPoint-Viewer.

Für die Ankündigung konfigurieren Sie nun noch einige Eigenschaften. So vergeben Sie beispielsweise einen Namen und legen den Zeitraum fest, in dem das Paket angekündigt werden soll. In vielen Fällen werden Sie vermutlich nur die Startzeit konfigurieren (Abbildung 16.40).

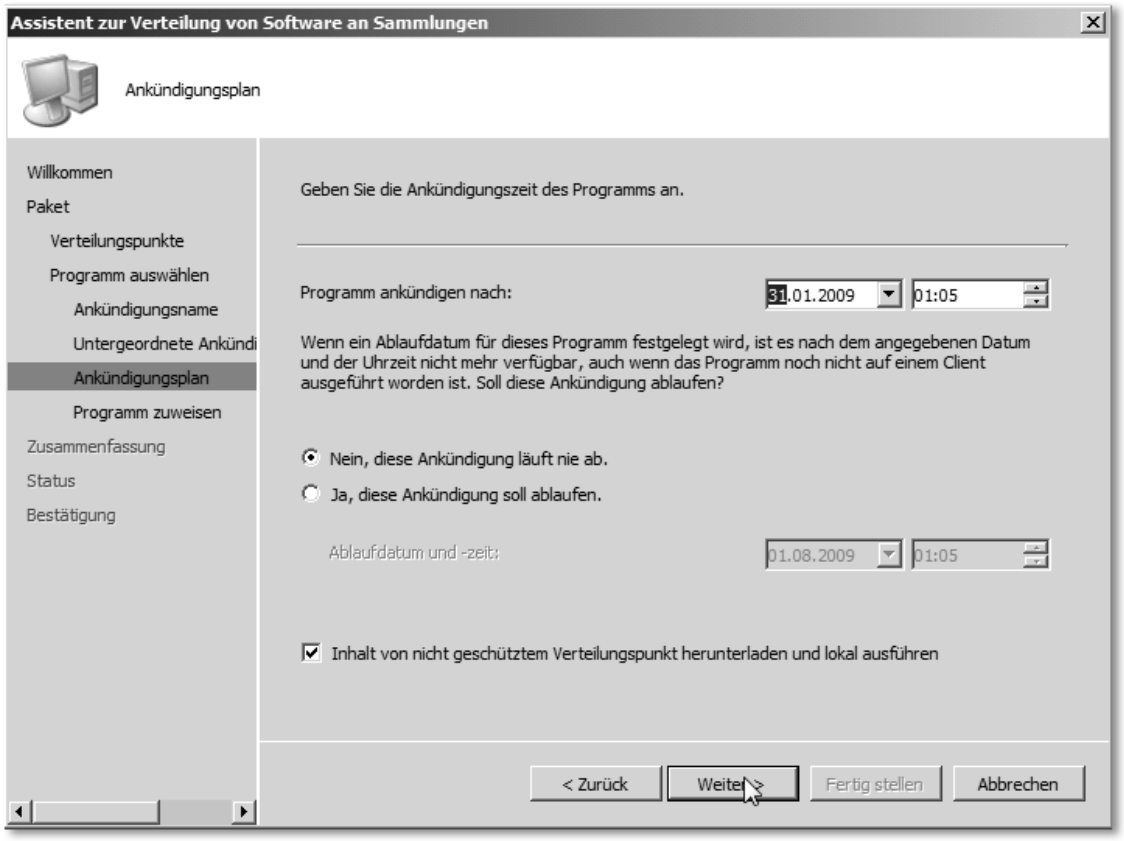


Abbildung 16.40 Hier legen Sie fest, in welchem Zeitraum das Programm angekündigt werden soll.

Im Dialog aus Abbildung 16.41 müssen Sie eine wichtige Entscheidung treffen, nämlich ob das Programm zugewiesen werden soll oder eben nicht. Wenn Sie möchten, dass tatsächlich eine Installation durchgeführt wird, muss das Programm zugewiesen werden.

Wenn Sie das Programm nicht zuweisen, wird es nicht direkt installiert, sondern liegt sozusagen in Wartestellung, und der Benutzer kann die Installation initiieren.

Wenn der Configuration-Manager-Agent auf dem Client die Ankündigung empfangen hat, wird er mit der Ausführung des Programms, also mit der Installation beginnen.

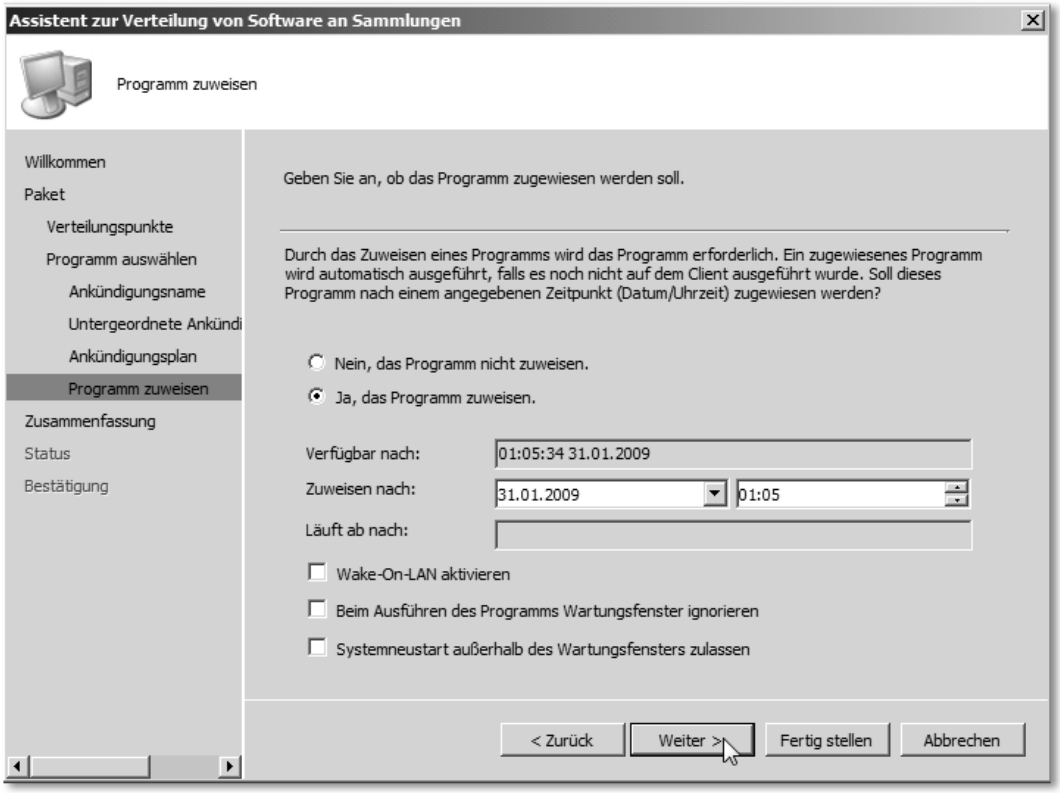


Abbildung 16.41 Wenn das Programm zugewiesen wird, wird es installiert. Hier gibt es noch einige weitere Einstellmöglichkeiten.

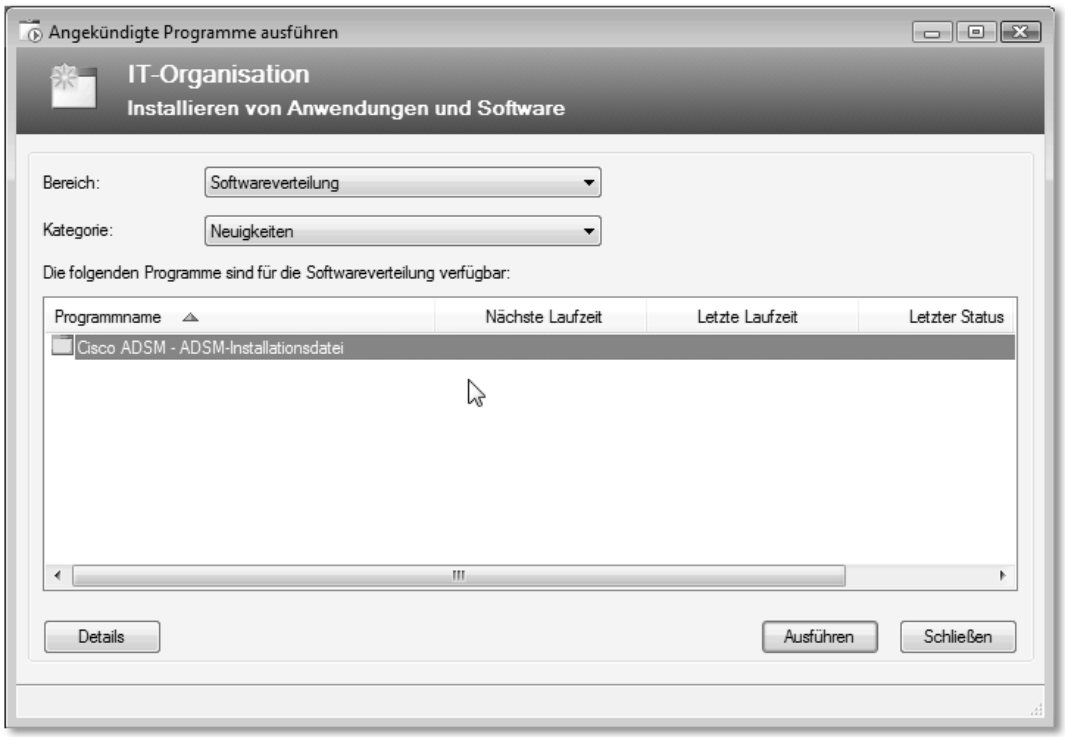


Abbildung 16.42 Wenn Sie das Programm nicht zuweisen, kann der Benutzer bei Bedarf die Installation selbst auslösen.

Nicht zugewiesene Programme

Wenn das Programm nicht zugewiesen wird (Abbildung 16.41), wird nicht direkt eine Installation durchgeführt. Vielmehr wird es sich in der Liste der angekündigten Programme finden. Den in Abbildung 16.42 gezeigten Dialog mit der Liste der angekündigten, aber nicht zugewiesenen Programme erreichen Sie über die Systemsteuerung. Der Benutzer kann die Installation dann selbst initiieren.

16.5 Betriebssystem verteilen

Neben der Installation von Applikationen ist die Installation des Betriebssystems eine wesentliche Aufgabe. Diese Aufgabe kann im Leben eines PCs durchaus mehrmals vorkommen:

- bei der Erstinstallation des PCs
- bei einem Upgrade des Betriebssystems, wenn beispielsweise XP nach Windows 7 migriert wird
- Falls der PC softwaremäßig unbrauchbar geworden ist, also beispielsweise nicht mehr startet, ist es im Allgemeinen einfacher, den PC neu aufzusetzen, als lange nach einem Fehler zu suchen bzw. zu versuchen, diesen zu beheben.

Hinweis

An dieser Stelle sei auf Kapitel 6, »Deployment«, verwiesen, in dem sehr ausführlich die Verwendung der *Windows Deployment Services* und die Arbeit mit den *WIM-Images* beschrieben sind.

Dies ist auch die Grundlagentechnologie, die von der SCCM-Betriebssysteminstallation verwendet wird – SCCM baut noch diverse Funktionalität drumherum.

Bei der Installation eines Betriebssystems ist eine der Anforderungen, dass Sie eine Bootumgebung benötigen, denn es ist ja entweder kein Betriebssystem vorhanden (neuer PC) oder es soll neu installiert werden, womit dann das bestehende installierte Betriebssystem auch nicht weiterhilft.

Ein recht eleganter Weg ist das Booten aus dem Netz. Mittlerweile unterstützt jeder PC dieses Verfahren – und Configuration Manager kann ebenfalls mit über das Netz bootenden Clients umgehen.

Das Configuration-Manager-System auf die Unterstützung des Bootens aus dem Netz vorzubereiten, ist nicht ganz trivial, unter anderem deshalb, weil die *Bereitstellungsdienste* von *Windows Server 2008* benötigt werden. Ich möchte das Setup

in diesem Buch nicht weiter behandeln, sondern mich auf die Vorstellung des Verfahrens konzentrieren.

Es gibt hier letztendlich drei Schritte:

- *Erstellung eines Referenz-PCs*: Wenn dieser so weit installiert und konfiguriert ist, wird er mit SYSPREP behandelt.
- *Erfassung des Referenz-PCs*: Dabei bootet dieser aus dem Netz und wird dann »ge-imagt«.
- *Ausrollen des Images auf beliebig viele weitere PCs*: Diese booten aus dem Netz und werden dann mit dem Image »betankt«. Weiterhin müssen Sie einige Individualisierungen vornehmen, wie beispielsweise das Benennen des PCs, das Beitreten zur Domäne und vieles andere mehr.

Anzumerken wäre, dass die Bereitstellung über Images nicht der einzige mögliche Weg ist – auch eine frische, unbeaufsichtigte Installation ist möglich. Der Trend geht aber seit einiger Zeit eher zur Image-Installation, übrigens mit gutem Erfolg.

16.5.1 Referenz-PC vorbereiten

Wenn Sie sich für die Installation per Image entschieden haben, müssen Sie zunächst einen Referenz-PC (oder Master-PC, wie immer Sie das Gerät nennen möchten) installieren. Auf diesem installieren Sie das Betriebssystem gemäß Ihren Vorstellungen. Sie können in diese Installation auch die wesentlichen Softwarepakete integrieren, beispielsweise *Microsoft Office* und die *SAP GUI*. Alternativ können Sie die Programme auch im Anschluss an die Betriebssysteminstallation von der Softwareverteilung installieren lassen.

Falls das Image auf PCs mit unterschiedlichen Hardwarekonfigurationen installiert werden soll, müssen Sie alle benötigten Treiber in »einbauen«. Alternativ können Sie den Configuration Manager zur Installationszeit Treiber hinzufügen lassen.

Ein wesentlicher Arbeitsschritt ist, dass Sie nach Fertigstellung der Installation auf dem Referenz-PC *SYSPREP* ausführen. Hierbei handelt es sich um eine seit *Windows 2000* bekannte Applikation, die die Installation sozusagen zurücksetzt. Wenn ein neuer PC von einem mit SYSPREP behandelten Image installiert wird, wird beim ersten Start der Neueinrichtungsvorgang durchgeführt. Es wird übrigens auch eine neue SID erzeugt, sodass Nachbehandlungen mit *NewSID* (einem *SysInternals*-Werkzeug) entfallen können (Abbildung 16.43).

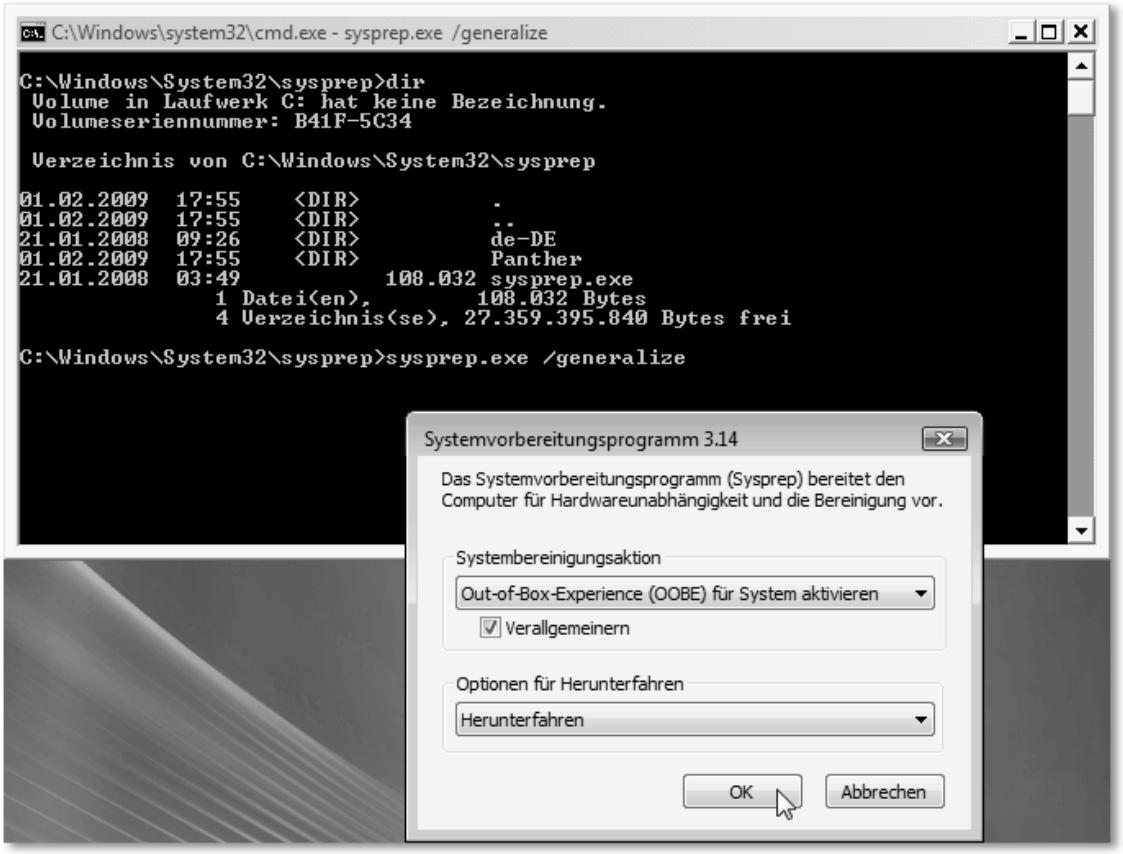


Abbildung 16.43 Der fertig vorbereitete PC wird mit SYSPREP behandelt.

SYSREP

Die Behandlung der Installation mit SYSPREP ist übrigens keinesfalls nur optional, Sie müssen (!) das tun! Es ist ansonsten beispielsweise möglich, dass bereits die im nächsten Schritt besprochene Erfassung des Images nicht funktioniert.

Anzumerken sei noch, dass der Referenz-PC auf keinen Fall ein Domänenmitglied sein darf – eine Arbeitsgruppe genügt. Sofern Sie Software benötigen, die nur auf Domänenmitgliedern installiert werden kann, kann die Installation erst erfolgen, wenn der neue (!) Client in die Domäne gebracht worden ist.

16.5.2 Ein Image mit PXE-Boot erfassen

Wenn Sie den Referenz-PC fertig installiert und mit SYSPREP vorbereitet haben, müssen Sie ein Image erzeugen. Microsoft verwendet seit einiger Zeit das WIM-Format (*Windows Imaging Format*), auf das die weiteren Verfahren im Configuration Manager abgestimmt sind. Es sind nun unterschiedliche Wege für das Erzeugen des Images möglich. Ich zeige Ihnen hier den meiner Meinung nach elegantesten Weg: Der Referenz-PC wird über das Netz gebootet, und es wird automatisch ein Image erfasst.

Da es über die Vorgehensweise nur recht verstreute Informationen gibt, zeige ich Ihnen den kompletten Vorgang, damit Sie sich ein realistisches Bild machen können.

Computer importieren

Da der Referenz-PC kein Domänenmitglied ist, wird er dem Configuration Manager nicht bekannt sein. Der erste Schritt besteht darin, manuell einen Eintrag im Configuration Manager zu erzeugen, da Sie ansonsten keine Aufgabe, nämlich die Image-Erfassung, zuweisen können. Der aufzurufende Menüpunkt heißt Computerinformationen importieren und findet sich im Kontextmenü des Knotens Computerzuordnung (Abbildung 16.44).

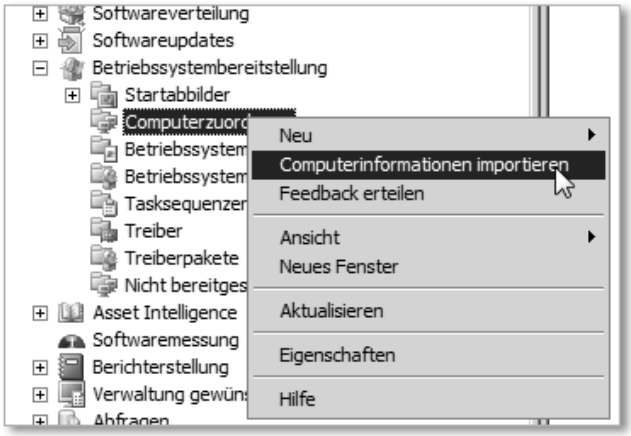


Abbildung 16.44 Zunächst müssen Sie die Computerinformationen importieren.

Der Assistent zum Importieren von Computerinformationen kennt zwei Arbeitsmodi: Entweder kann ein einzelner Computer importiert werden, oder es kann eine Importdatei (im CSV-Format) eingelesen werden (Abbildung 16.45).

Im zweiten Fall muss nur ein einziger Computer zugeordnet werden, somit brauchen Sie nicht über den Weg einer Importdatei zu gehen. Falls Sie in einem Rutsch mehrere Dutzend neue auszurollende Maschinen importieren möchten, ist das Verfahren über die Datei sehr angenehm – insbesondere dann, wenn Ihr Lieferant die wesentlichen Lieferinformationen elektronisch übergibt.

Beim Import eines Computers werden im Wesentlichen der Computername und die MAC-Adresse benötigt. Dies ist auch einleuchtend, denn wenn der neue PC über das Netzwerk gebootet wird, haben die Configuration-Manager-Komponenten zunächst im Wesentlichen nur die Möglichkeit, einen PC anhand der besagten MAC-Adresse zu identifizieren (Abbildung 16.46).

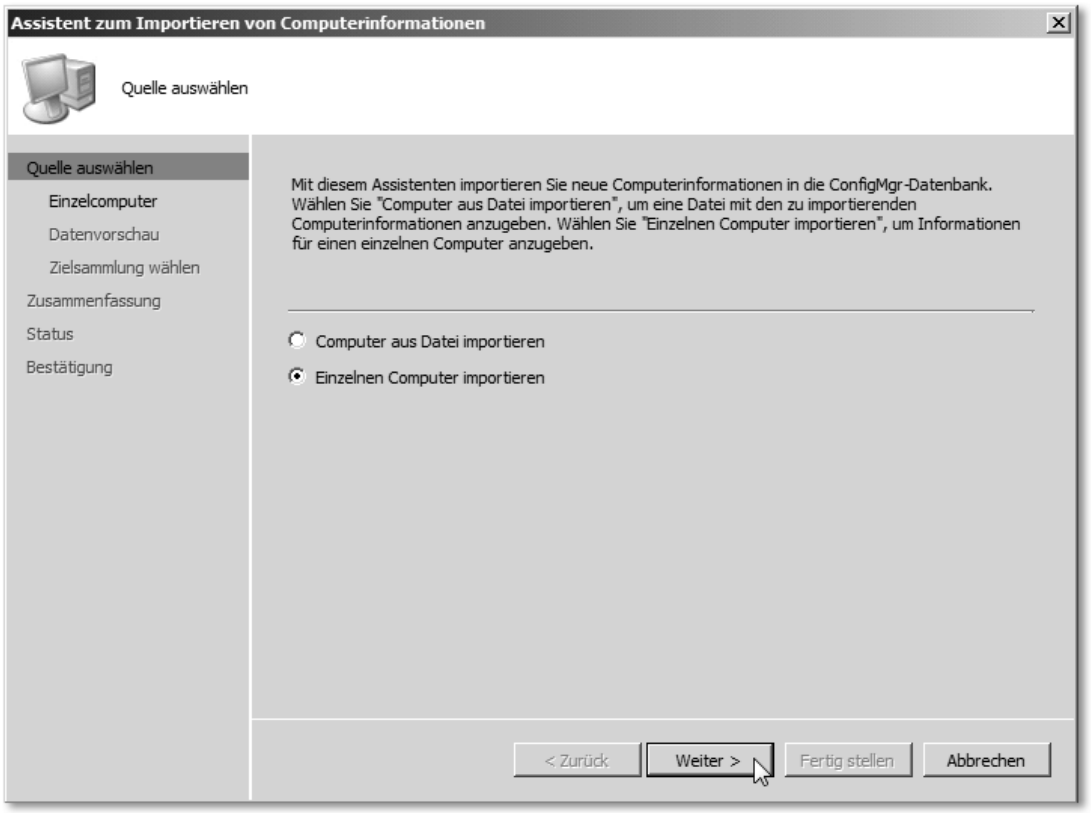


Abbildung 16.45 In diesem Fall werden nur die Daten eines Computers benötigt. Wenn Sie Dutzende oder Hunderte von Systemen ausrollen, ist die Importfunktion recht praktisch.

Für diesen Computer, den Sie sinnvollerweise in einer separaten Sammlung platzieren lassen (der Assistent fragt im Verlauf nach einer Zielsammlung), existiert nach dem Anlegen ein Eintrag im Configuration Manager. Rufen Sie diesen auf, und fügen Sie die Variable `OSDTargetSystemRoot` hinzu. Als Wert wird der Pfad zum Windows-Verzeichnis des zu erfassenden Images konfiguriert, vermutlich *c:\windows* (Abbildung 16.47).

Sehr ernste Warnung

Das Setzen dieser Variablen sieht »irgendwie trivial« aus. Vergessen Sie es trotzdem nicht!

Ist diese Variable nicht gesetzt, wird die Image-Erfassung mit einer eher mysteriösen (zumindest nicht aussagekräftigen) Fehlermeldung abbrechen! Nach diesem Fehler kann man stundenlang verzweifelt suchen – setzen Sie die Variable also lieber direkt.

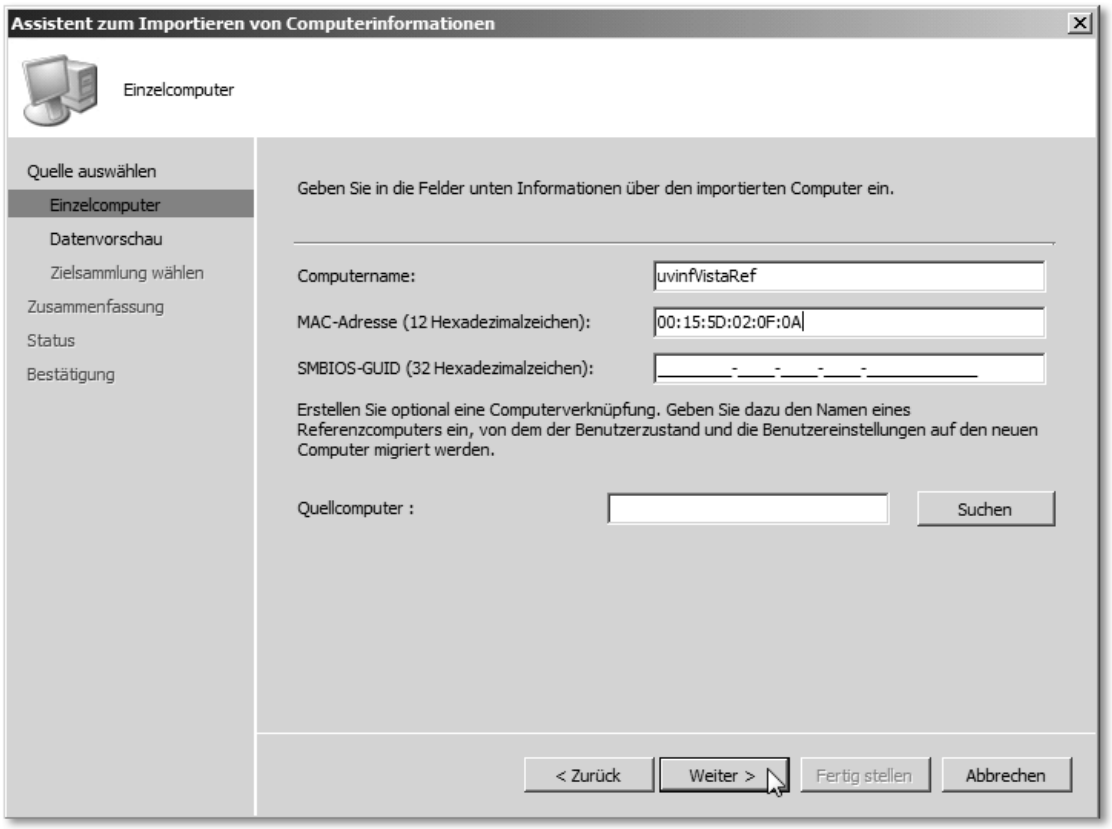


Abbildung 16.46 Beim Import eines Computers werden mindestens der Computername und die MAC-Adresse benötigt.

Abbildung 16.47 Diese Variable müssen Sie unbedingt (!) in den Eigenschaften des Computerobjekts setzen – sonst schlägt der Erfassungsvorgang fehl.

Tasksequenz erstellen

Es gibt insbesondere, aber nicht nur bei der Betriebssystembereitstellung Abfolgen von Schritten, die hintereinander ausgeführt werden müssen. Dies lässt sich über eine Tasksequenz konfigurieren. In diesem Fall wird die Tasksequenz zwar nur aus einem Schritt (nämlich »Erfasse Image«) bestehen, bei der Verteilung des Images, was ich Ihnen später vorführen werde, können die Tasksequenzen dann aber zeigen, was in ihnen steckt.

Abbildung 16.48 ist eine kleine Suchhilfe und zeigt Ihnen den Menüpunkt zum Aufruf des Assistenten.

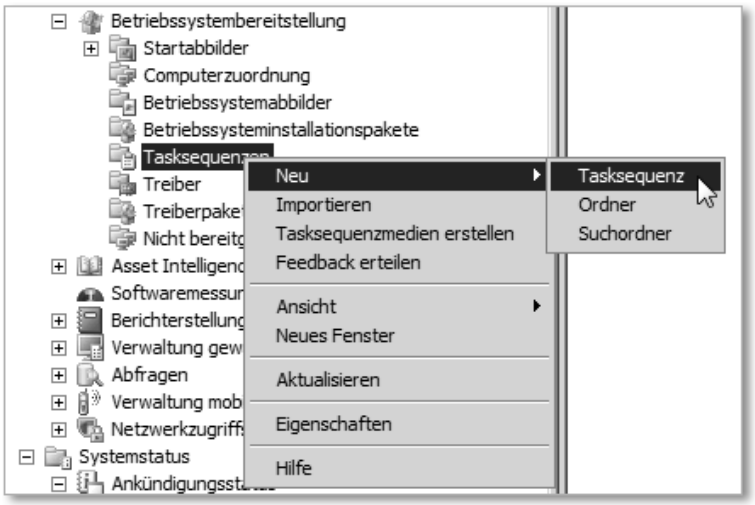


Abbildung 16.48 Hier erstellen Sie eine neue Tasksequenz.

Der Assistent zum Erstellen einer neuen Tasksequenz bietet drei Möglichkeiten, von denen Sie die dritte, also NEUE BENUTZERDEFINIERTE TASKSEQUENZ ERSTELLEN, auswählen. Der mittlere Punkt hört sich zwar verlockend an, passt aber nicht ganz, wenn Sie bereits über einen fertigen Referenz-PC verfügen, der nur noch auf sein Imaging wartet (Abbildung 16.49).

Startabbilder

Die Startabbilder müssen auf einen normalen Verteilungspunkt gebracht werden, was Sie mit einem Assistenten erledigen können. Wenn Sie das versäumen, wird es wieder mysteriöse Fehlermeldungen geben, die schwer zu entschlüsseln sind.

Die Startabbilder liegen bereits auf einer Serverfreigabe namens *SMSPXEIMAGES$*. Das genügt zwar für den Startvorgang, nicht aber für die Ausführung von Tasksequenzen. Achten Sie darauf. Ich habe vor einiger Zeit stundenlang den »Fehler« gesucht – Sie sollten mir das nicht nachmachen.

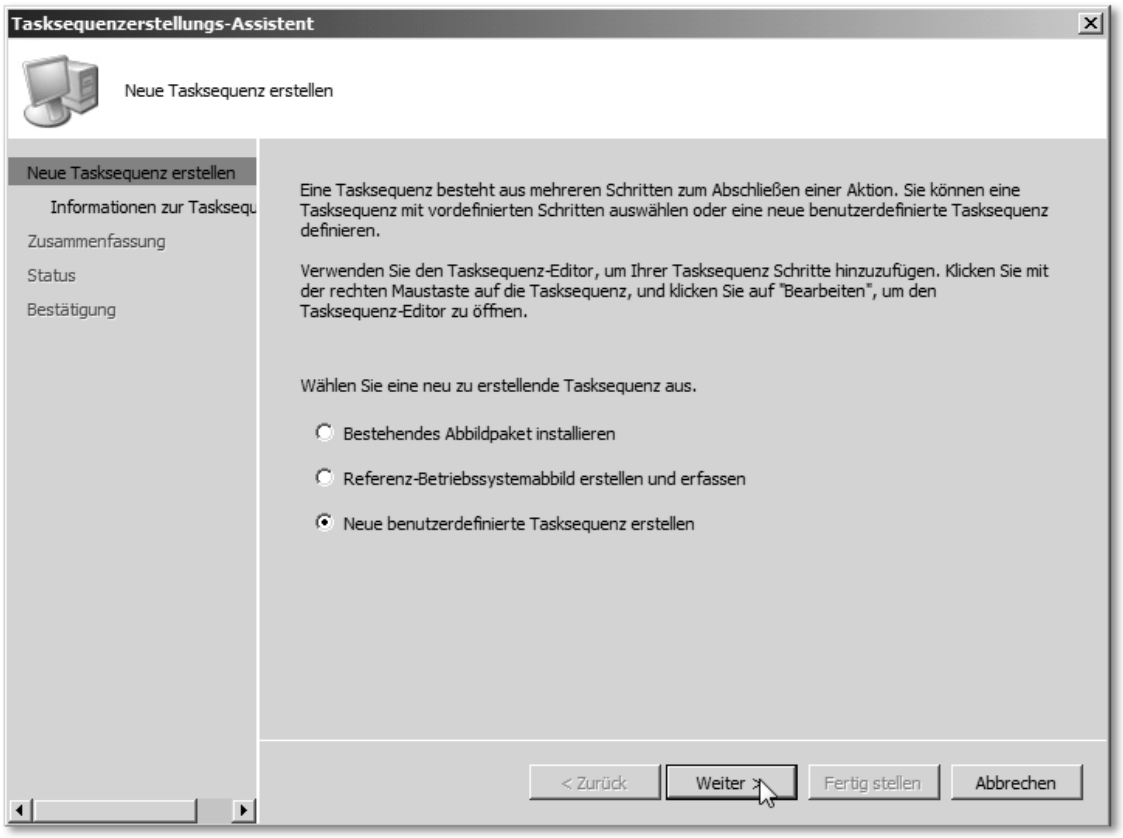


Abbildung 16.49 Erstellen Sie eine neue benutzerdefinierte Tasksequenz.

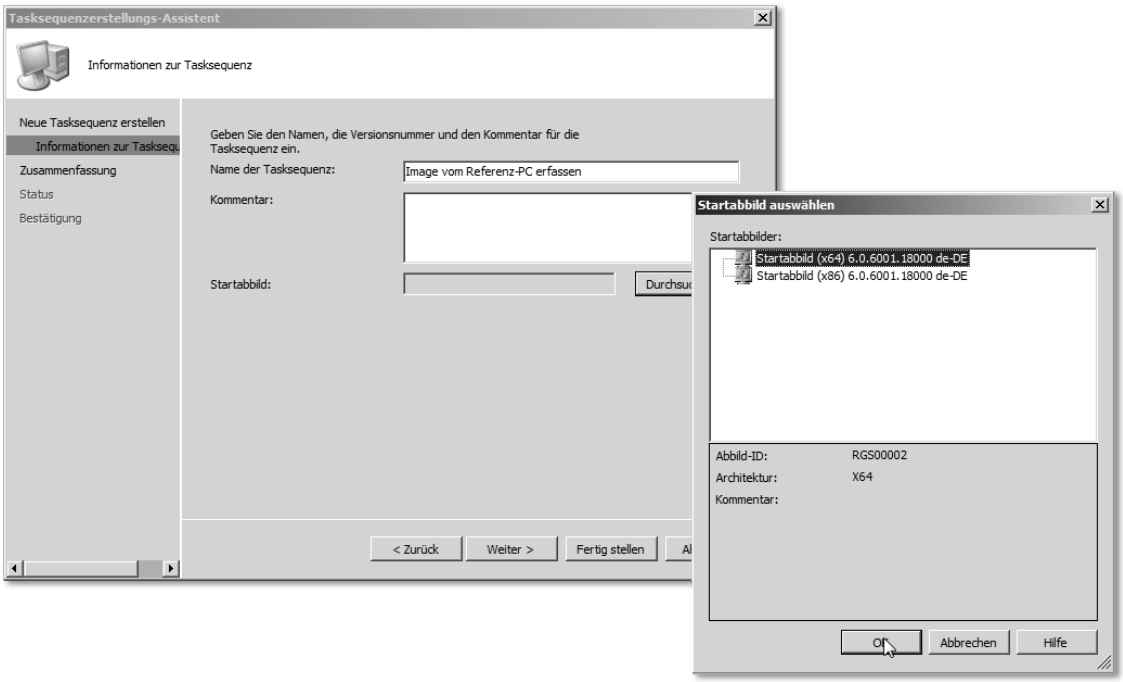


Abbildung 16.50 Hier wählen Sie das Startabbild aus, von dem gebootet werden soll.

Der Assistent wird nun nur von Ihnen wissen wollen, welches Startabbild verwendet werden soll. Standardmäßig bringt der Configuration Manager ein x86- und ein x64-Startabbild mit. Bei Bedarf können Sie eigene Startabbilder hinzufügen.

Wenn die Tasksequenz angelegt ist, wählen Sie in deren Kontextmenü den Menüpunkt BEARBEITEN (Abbildung 16.51). Dieser bringt Sie direkt zum Tasksequenz-Editor. Abbildung 16.52 zeigt den gerade geöffneten Tasksequenz-Editor, in dem bislang noch keine auszuführenden Schritte definiert sind. Wie Sie am aufgeklappten HINZUFÜGEN-Menü sehen können, gibt es diverse ausführbare Funktionen, von denen uns momentan aber nur BETRIEBSSYSTEMABBILD ERFASSEN interessiert.

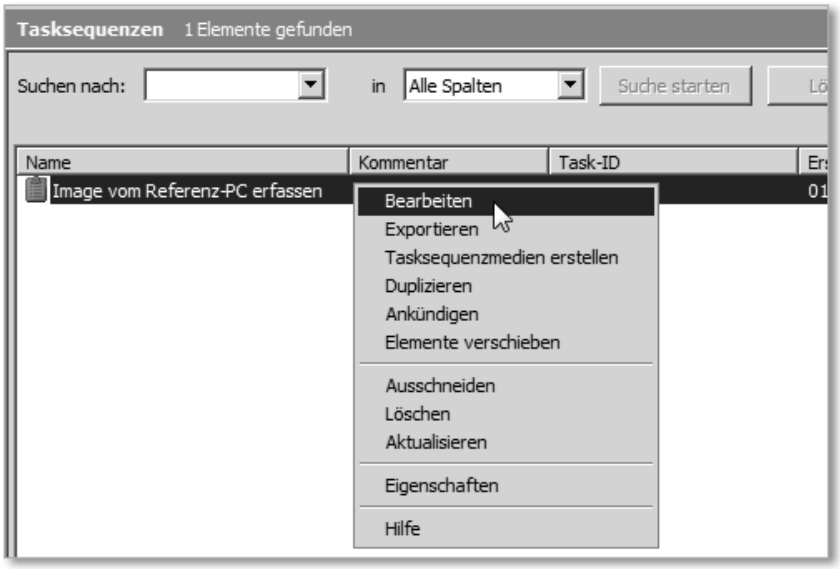


Abbildung 16.51 Rufen Sie das Bearbeiten der neu erstellten Tasksequenz auf.

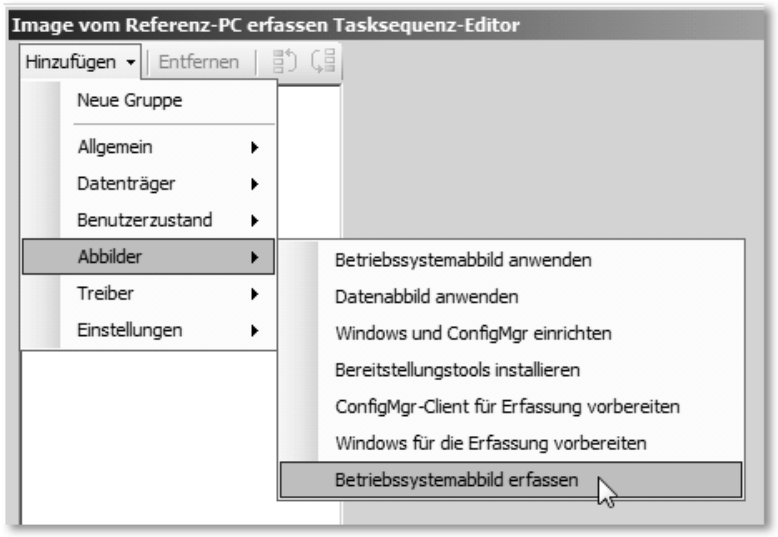


Abbildung 16.52 Im Tasksequenz-Editor können Sie jeden Schritt definieren und konfigurieren.

Abbildung 16.53 zeigt die Eigenschaften der BETRIEBSSYSTEMABBILD ERFASSEN-Funktion. Im Wesentlichen können Sie hier das Ziel (Dateifreigabe) sowie die für den schreibenden Zugriff benötigten Anmeldeinformationen erfassen.

Wenn Sie die Einträge vorgenommen haben, schließen Sie den Tasksequenz-Editor und kündigen die Tasksequenz an – was im nächsten Abschnitt beschrieben wird.

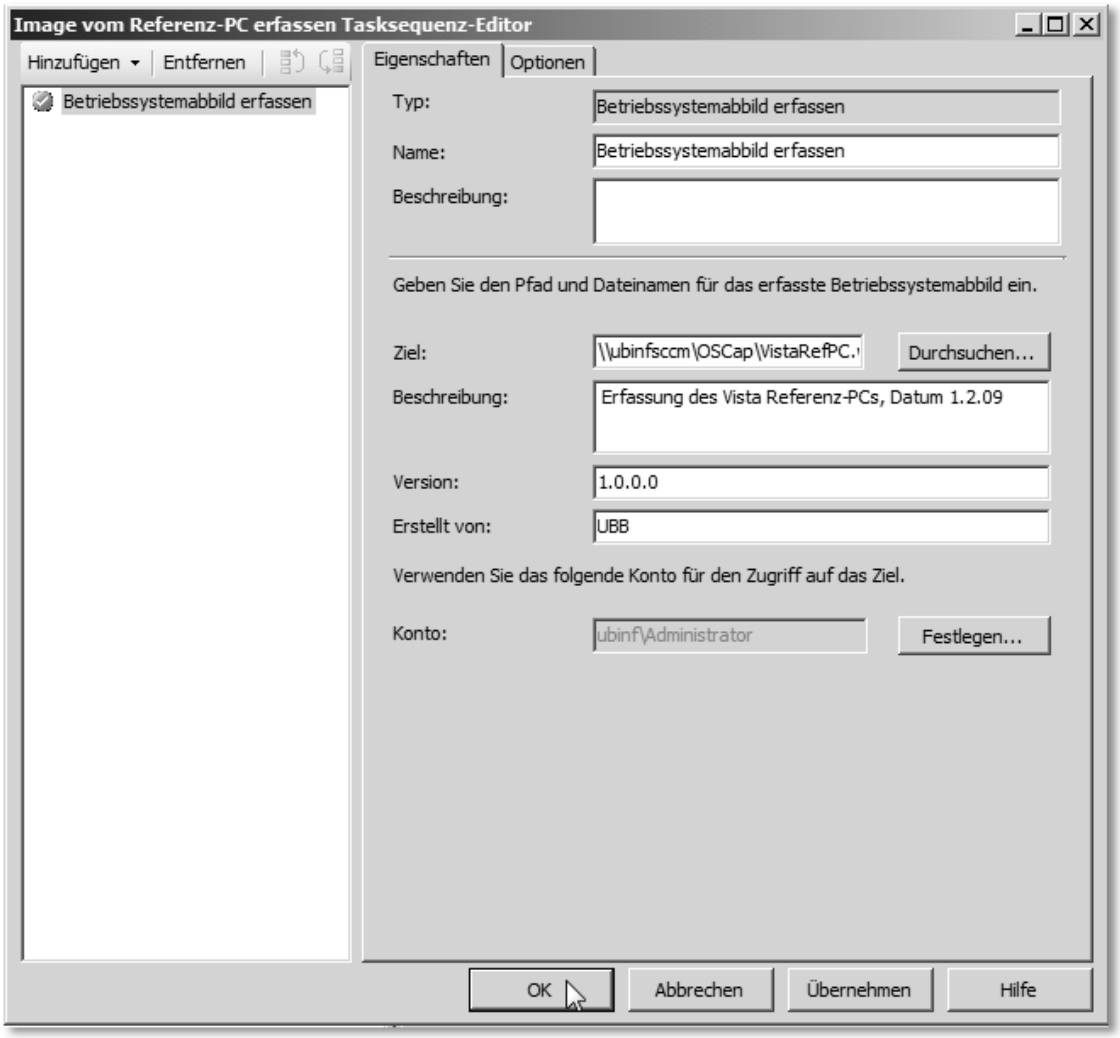


Abbildung 16.53 Die Konfiguration des Schritts »Betriebssystemabbild erfassen«. Wählen Sie den Pfad und Dateinamen aus, unter dem das Abbild gespeichert werden soll.

Tasksequenz ankündigen

Genauso, wie bei der Softwareverteilung ein Programm angekündigt wird, muss auch die erstellte Tasksequenz angekündigt werden. Im Kontextmenü der Tasksequenz finden Sie einen entsprechenden Menüpunkt.

Das Erstellen der Ankündigung ist weiter nicht kompliziert. Allerdings sind zwei »lebenswichtige« Einstellungen zu beachten:

- Auf der ersten Dialogseite muss die Checkbox Diese Tasksequenz für Startmedien und PXE verfügbar machen ausgewählt sein (Abbildung 16.54).
- Später wird eine Dialogseite angezeigt, auf der Sie festlegen müssen, dass auf die Inhalte direkt vom Verteilungspunkt aus zugegriffen werden soll (Abbildung 16.55).

Hinweis

An dieser Stelle möchte ich noch darauf hinweisen, dass Sie die Ankündigung der Tasksequenz für eine Sammlung vornehmen. Es empfiehlt sich also, eine Sammlung einzurichten, in der dieser Referenz-PC das einzige Mitglied ist.

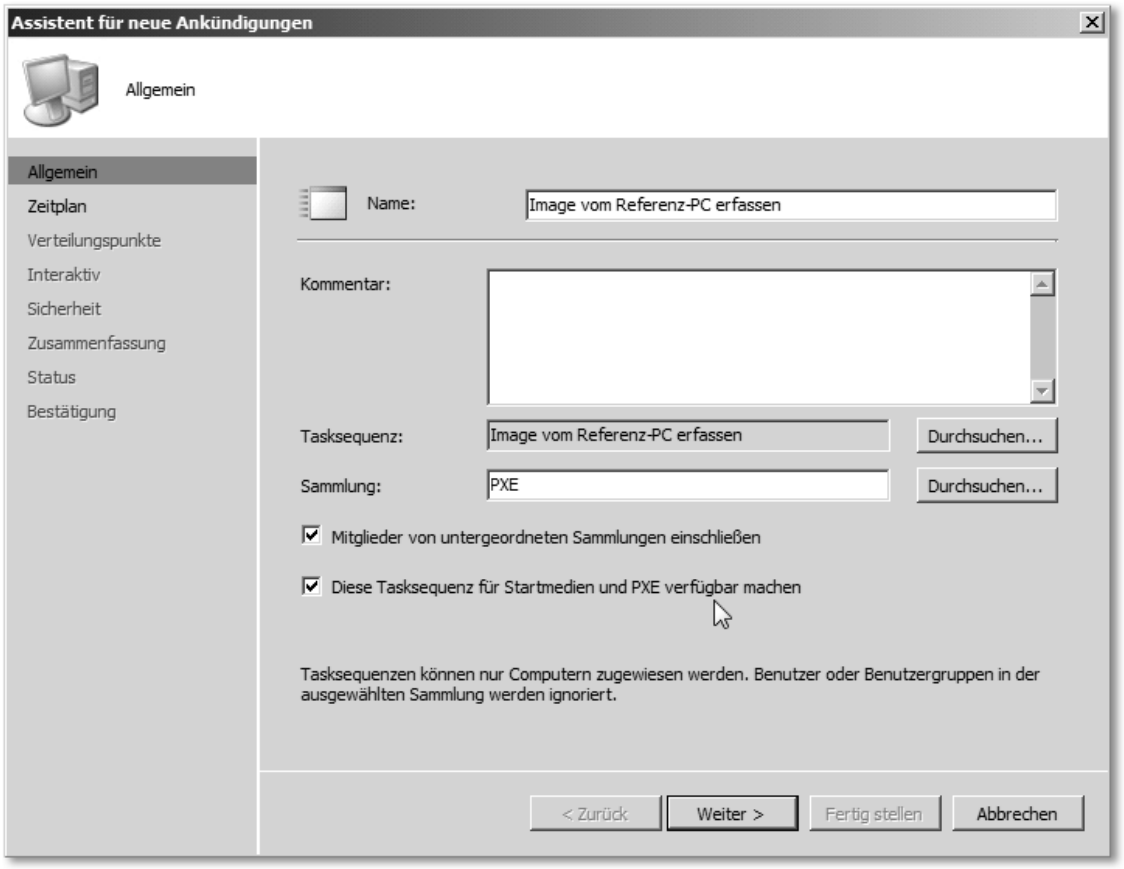


Abbildung 16.54 Wichtig ist, dass Sie die Tasksequenz für PXE verfügbar machen.

PXE-Boot durchführen und Image erfassen

In diesem Abschnitt möchte ich Ihnen einen Eindruck davon vermitteln, wie die PXE-Bootsequenz nebst Erfassung des Images aussieht. Zunächst ist es natürlich erforderlich, dass die im jeweiligen Gerät verwendete Netzwerkkarte den Bootvorgang aus dem Netz unterstützt – das dürfte aber bei jedem einigermaßen modernen Gerät gegeben sein.

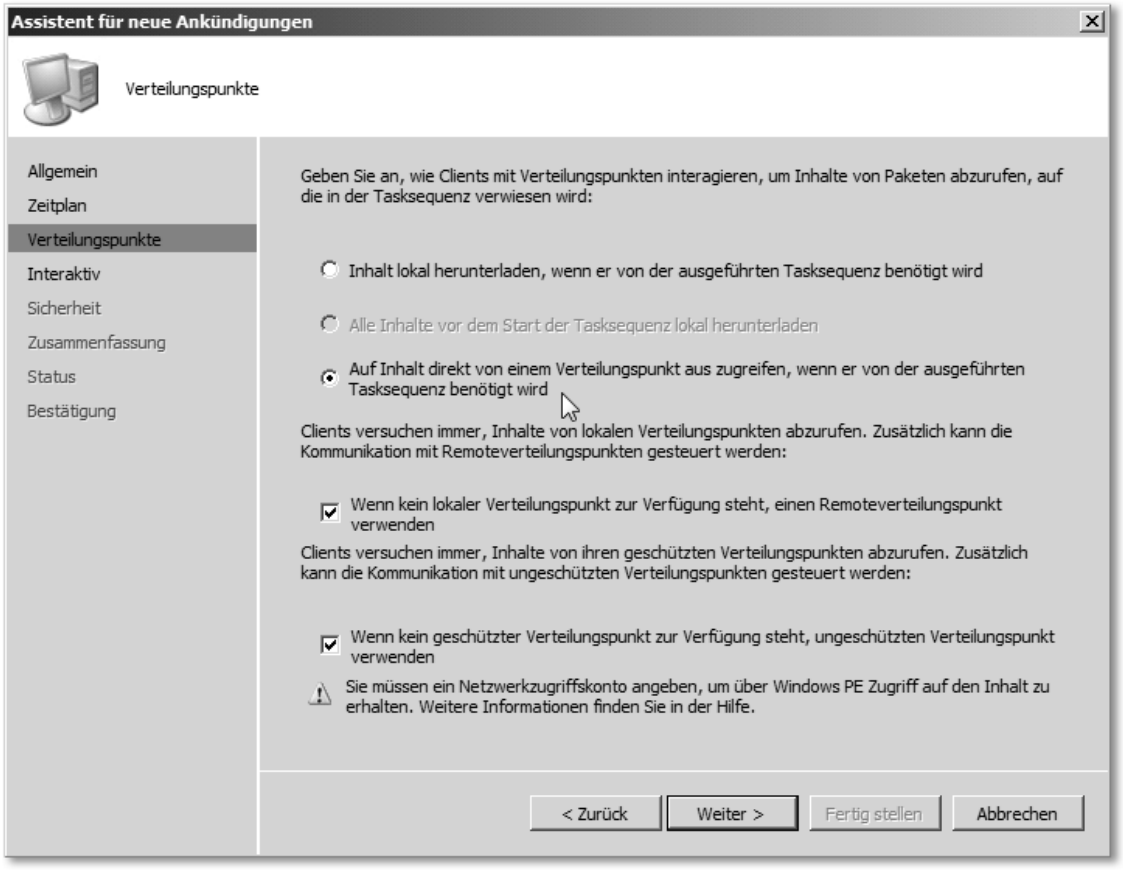


Abbildung 16.55 Bei einer Ankündigung für eine »PXE-Aufgabe« muss die Option »Auf Inhalt direkt von einem Verteilungspunkt…« gewählt sein.

Der eigentliche Bootvorgang stellt sich auf dem Client in etwa so dar, wie in Abbildung 16.56 zu sehen ist. Sofern ein Client einen Netzwerkbootvorgang versucht, für ihn aber keine angekündigte Tasksequenz vorliegt, bricht der Vorgang ab, und er startet von einem lokalen Medium, also von Festplatte oder CD/DVD.

Wenn Sie mit den standardmäßig vorhandenen Startabbildern (den Boot-Images) arbeiten, wird Windows PE gestartet werden. Sie werden zunächst den Eindruck haben, dass es sich um einen normalen Startvorgang handelt. Nach einigen Sekunden werden Sie dann die Darstellung aus Abbildung 16.57 sehen. Wenn der Vorgang so weit gekommen ist, war auf jeden Fall das Starten über das Netzwerk erfolgreich.

In der Konfiguration des PXE-Dienstpunkts kann hinterlegt werden, dass vor dem Ausführen einer Tasksequenz eine Kennwortabfrage erfolgen soll. Diese Abfrage zu fordern, ist durchaus keine ganz schlechte Idee. Benutzer können zwar nicht vom Netz booten, solange keine PXE-Ankündigung vorhanden ist. Falls dies versehentlich aber doch der Fall sein sollte, ist dieses Kennwort eine weitere Schutzmaßnahme gegen eventuellen Missbrauch.

```
Hyper-V
PXE Network Boot 07.12.2007
(C) Copyright 2007 Microsoft Corporation, All Rights Reserved.


CLIENT MAC ADDR: 00 15 5D 02 0F 0A  GUID: 66C67B67-574E-44C9-884D-12657BAD562C
CLIENT IP: 192.168.2.34  MASK: 255.255.255.0  DHCP IP: 192.168.2.160
GATEWAY IP: 192.168.2.105

Downloaded WDSNBP...

Architecture: x64

The details below show the information relating to the PXE boot request for
this computer. Please provide these details to your Windows Deployment Services
Administrator so that this request can be approved.

Pending Request ID: 587

Contacting Server: 192.168.2.136.
TFTP Download: smsboot\x64\pxeboot.com

Press F12 for network service boot
```

Abbildung 16.56 So sieht die PXE-Boot-Sequenz auf dem Client aus.

Abbildung 16.57 Wenn Sie diesen Startbildschirm sehen, hat der eigentliche Startvorgang über das Netzwerk funktioniert.

Es könnte ansonsten sein, dass ein experimentierfreudiger Benutzer eine Tasksequenz aufruft, die den PC neu installiert (Abbildung 16.58).

Abbildung 16.58 Sie können die Ausführung der Tasksequenzen mit einem Passwort schützen.

Im nächsten Schritt wählen Sie die auszuführende Tasksequenz (Abbildung 16.59). Da für einen PC durchaus mehrere Tasksequenzen angekündigt sein können, ist diese Auswahl notwendig – auch wenn der Dialog aus Abbildung 16.59 ein wenig dürftig aussieht.

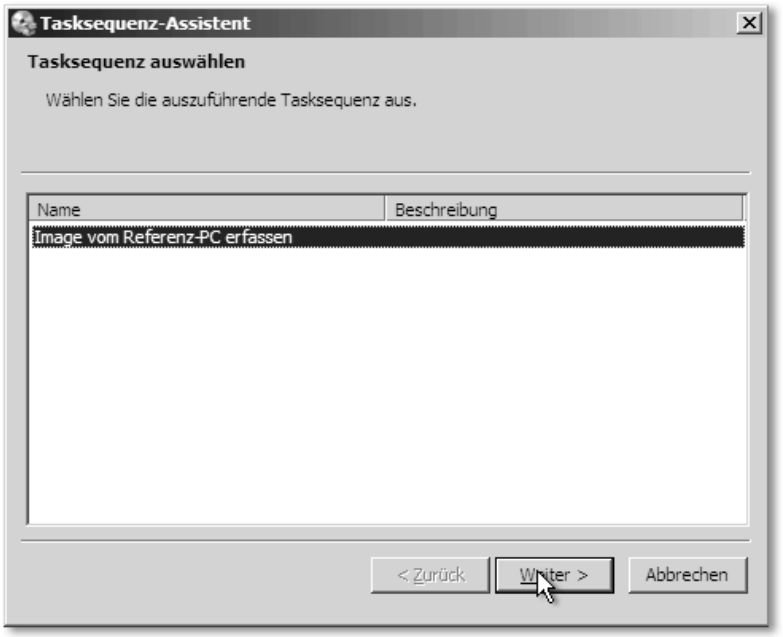


Abbildung 16.59 Hier wählen Sie die Tasksequenz aus, die abgearbeitet werden soll.

Wenn alles korrekt funktioniert, startet nach der Auswahl der Tasksequenz die Erfassung des Betriebssystemabbilds, was dann so aussieht wie in Abbildung 16.60.

Abbildung 16.60 So sieht die Anzeige bei der Erfassung des Betriebssystemabbilds aus.

Troubleshooting

Wenn Sie zwar die Tasksequenz auswählen können, danach aber nicht die in der Tasksequenz definierte Aktion beginnt, sondern eine Fehlermeldung erscheint, die mysteriöse Zugriffsprobleme nennt, könnte das daran liegen, dass die Startabbilder zwar auf der Server-Freigabe *SMSPXEIMAGES$* vorhanden sind, nicht aber auf dem regulären Verteilungspunkt. Fügen Sie also auch einen »normalen« Verteilungspunkt hinzu, dann sollte es funktionieren.

Betriebssystemabbilder sind natürlich einigermaßen groß, das WIM-Format komprimiert sie allerdings mit gutem Erfolg. Das in diesem Beispiel erfasste Vista-Image hat auf dem Referenz-PC ca. 9 GB Plattenkapazität benötigt. Die WIM-Datei ist erfreulicherweise nur ein wenig größer als 2,5 GB.

16.5.3 Einen neuen PC ausrollen

Nun wird es ernst: Ein oder mehrere neue PCs sollen mit dem erstellten Image »betankt« werden. Dazu gehört natürlich nicht nur, dass das Image auf den PC kommt, sondern auch die Vergabe des richtigen Rechnernamens und dergleichen mehr. Der Configuration Manager kann, wie Sie im Verlauf dieses Abschnitts sehen werden, all diese Aufgaben erledigen. Dabei ist es aber wichtig, dass der Referenz-PC, wie anfangs erläutert, mit SYSPREP behandelt wurde.

Hinweis

In diesem Beispiel zeige ich Ihnen die Installation eines neuen PCs, bei der keine Benutzereinstellungen übernommen werden. Sofern Sie nicht mit servergespeicherten Profi-

len (*Roaming Profiles*) arbeiten und der PC nicht für einen neuen Benutzer installiert wird, möchten Sie vermutlich die Profileinstellungen des Benutzers mitnehmen. Zu diesem Zweck ist das *User State Migration Tool* (USMT) in den Configuration Manager integriert. Ich werde Ihnen im Verlauf des Kapitels zwar den entsprechenden Konfigurationsdialog zeigen, aus Platzgründen aber nicht den kompletten Vorgang vorführen – ich kann Ihnen aber versichern, dass das funktioniert.

Betriebssystemabbild hinzufügen

Das zuvor erfasste Betriebssystemabbild (eine WIM-Datei) liegt zwar nun im Dateisystem; um damit wirklich arbeiten zu können, muss es einerseits als Betriebssystemabbild eingetragen und andererseits auf mindestens einem Verteilungspunkt vorhanden sein.

Zunächst fügen Sie dem Configuration Manager das Betriebssystemabbild mit dem gleichnamigen Menüpunkt hinzu. Abbildung 16.61 zeigt, wie das gemacht wird. Im Kontextmenü des hinzugefügten Betriebssystemabbilds findet sich ein Menüpunkt zum VERWALTEN DER VERTEILUNGSPUNKTE. Der Assistent entspricht dem Assistenten zur Verteilungspunktkonfiguration bei Paketen und wird hier daher nicht näher betrachtet (Abbildung 16.62).

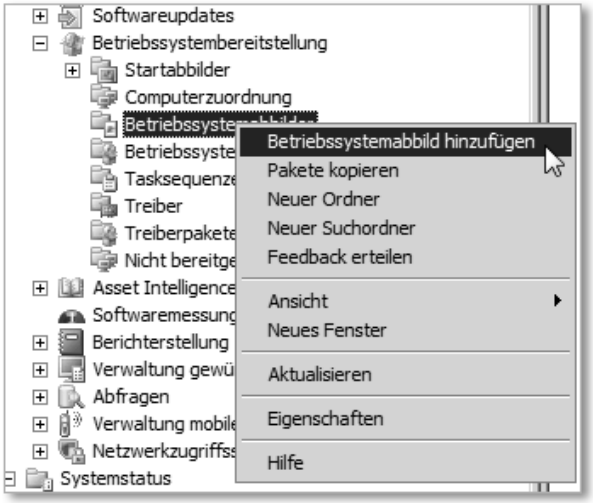


Abbildung 16.61 Das erfasste Betriebssystemabbild (WIM-Datei) muss noch hinzugefügt werden.

Wenn Sie das Betriebssystemabbild anklicken, werden einige grundlegende Informationen zum Betriebssystemabbild gezeigt. Sie sehen in Abbildung 16.63, dass in der Datei ein Datenträger enthalten ist, der eine Größe von ca. 36 GB hat und von dem ungefähr 10 GB belegt sind.

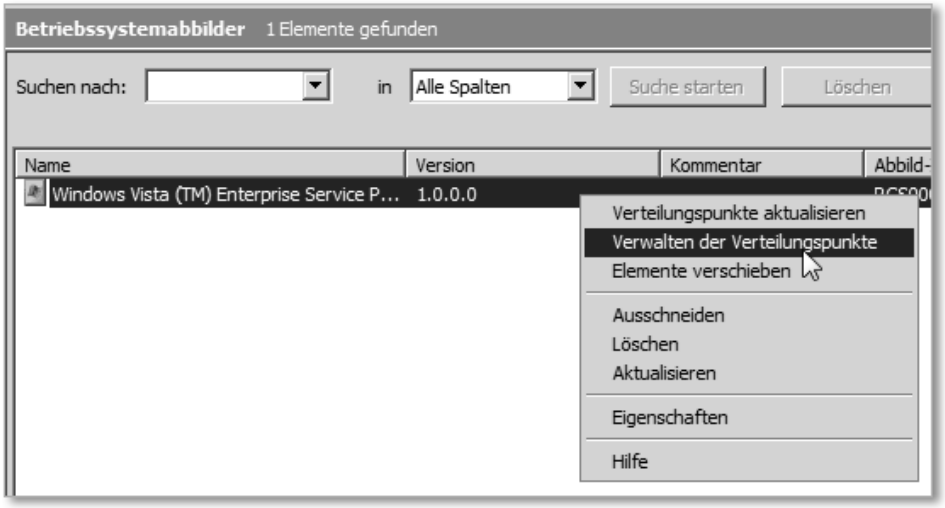


Abbildung 16.62 Für das Betriebssystemabbild müssen Sie Verteilungspunkte definieren.

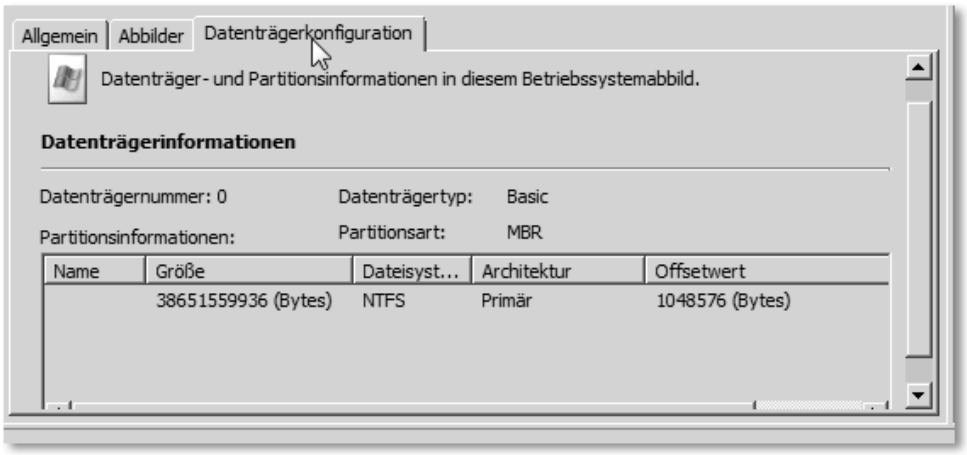


Abbildung 16.63 Einige grundlegende Informationen zu dem erfassten Betriebssystemabbild erhalten Sie auf diesen Registerkarten.

Tasksequenz erstellen

Um das Betriebssystemabbild an Clients zu verteilen, müssen Sie eine Tasksequenz erstellen. Diesmal verwenden wir die Vorlage Bestehendes Abbildpaket erstellen. Es wäre auch möglich, eine benutzerdefinierte Tasksequenz auszuwählen und die notwendigen Schritte manuell hinzuzufügen – es kann aber nicht schaden, sich das Leben ein wenig einfacher zu machen (Abbildung 16.64).

Der erste Schritt ist die Vergabe eines Namens und die Wahl eines Startabbilds (Abbildung 16.65). Achten Sie darauf, dass das Startabbild auf einem Verteilungspunkt vorhanden ist.

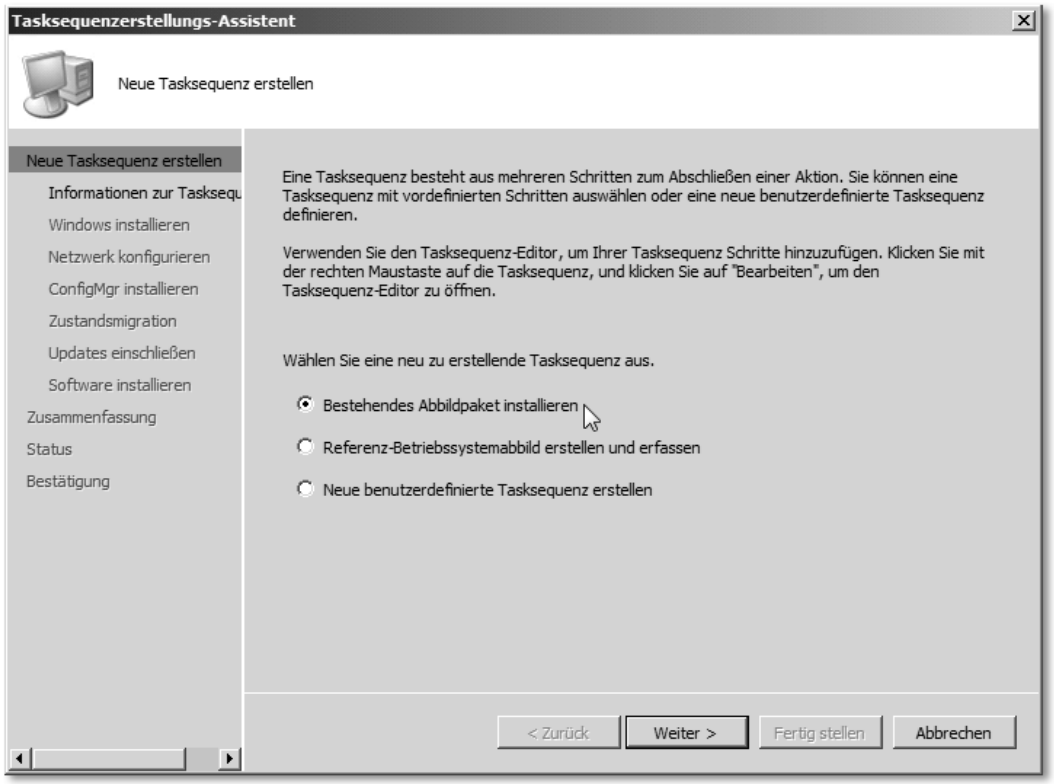


Abbildung 16.64 Beim Erstellen der Tasksequenz können Sie die Vorlage für ein »Bestehendes Abbildpaket installieren« verwenden.

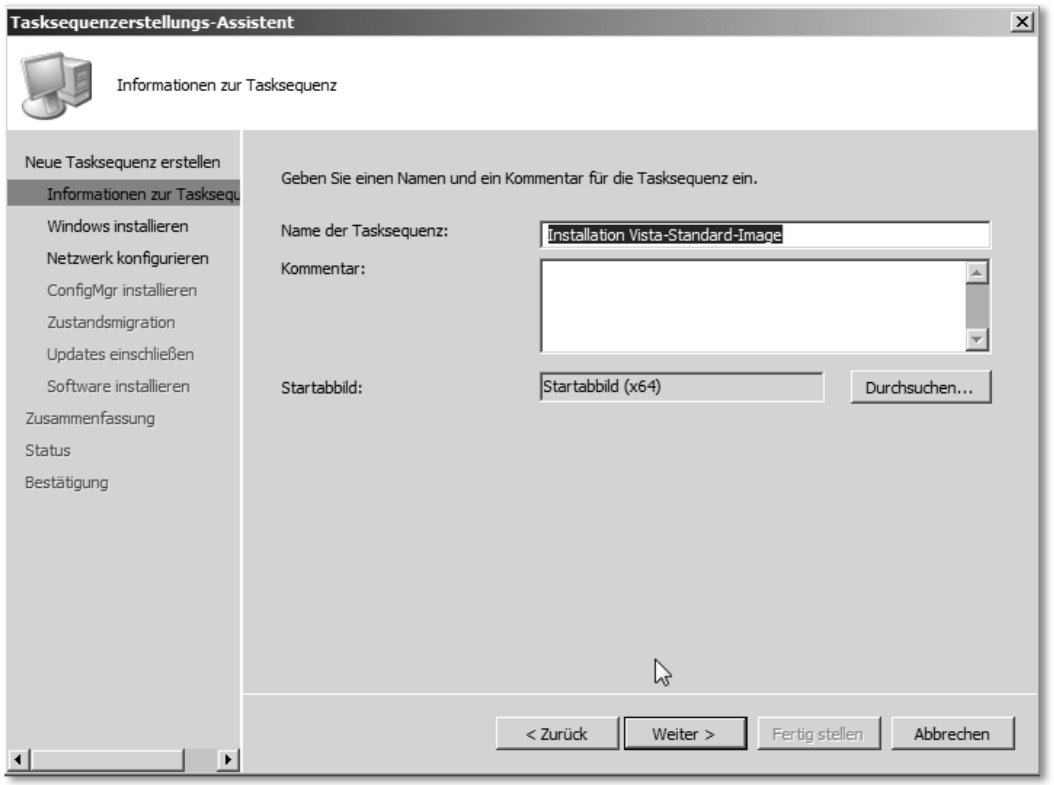


Abbildung 16.65 Hier wählen Sie das Startabbild aus, das Sie verwenden wollen.

Der zweite Schritt ist deutlich interessanter, denn hier wählen Sie zunächst das Betriebssystemabbild aus, das verwendet werden soll. Wie ich bereits zuvor erwähnt habe, können in einer WIM-Datei mehrere Abbilder vorhanden sein. Folglich muss auch ein Abbild ausgewählt werden (Abbildung 16.66). In der unteren Hälfte des Dialogs können Sie bereits einige Informationen für die Neueinrichtung des Betriebssystem hinterlegen. Beim Deployment eines Clientbetriebssystems wie Windows 7 ist der Serverlizenzierungsmodus übrigens nicht relevant.

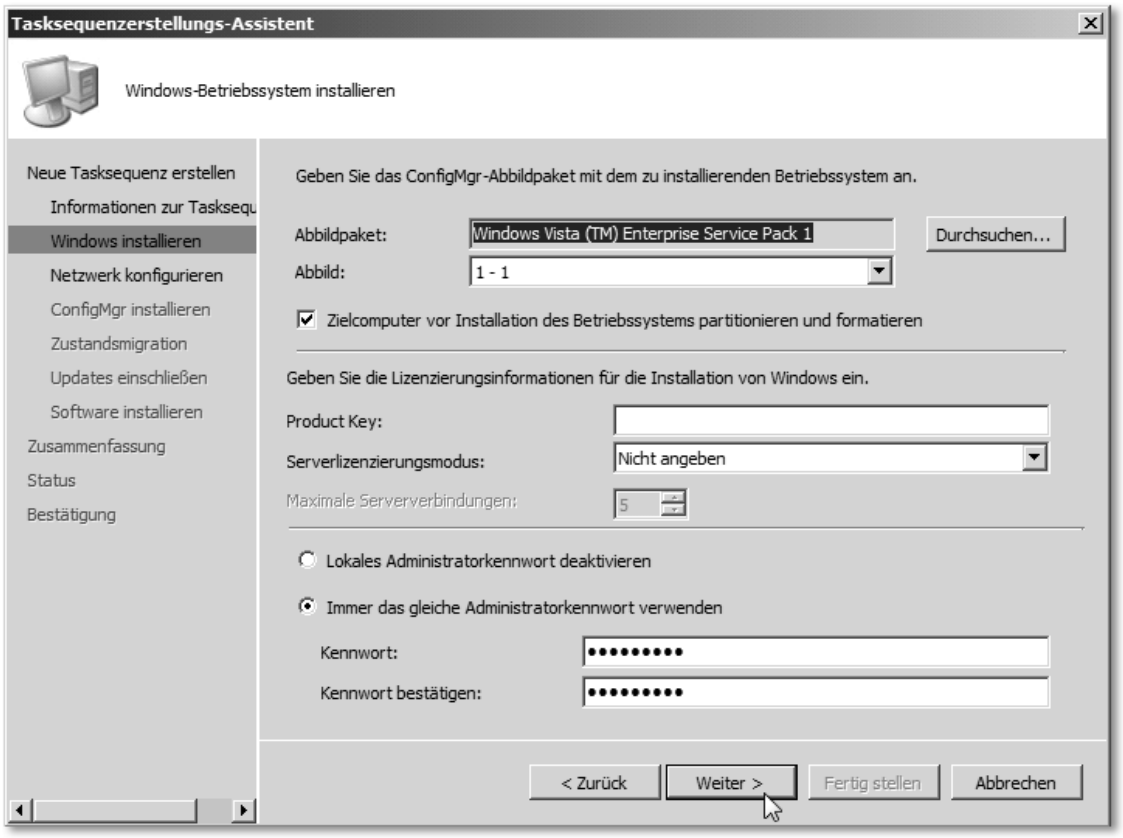


Abbildung 16.66 Neben dem Abbildpaket, das Sie verwenden wollen, können Sie einige Parameter für die Installation wählen.

Im Folgenden kann konfiguriert werden, dass der neu aufgesetzte PC einer Domäne beitreten soll. Auch die Organisationseinheit kann vorgegeben werden (Abbildung 16.67).

Ein weiterer wesentlicher Schritt beim Deployment eines PCs ist die Installation des Configuration-Manager-Clients. Hierfür müssen Sie das zu verwendende Paket angeben; die Angabe dieses Pakets ist nicht optional. Leider ist standardmäßig kein Paket vorhanden. Allerdings können Sie leicht eines aus der Definition erstellen (siehe den Menüpunkt SOFTWAREVERTEILUNG • PAKETE • NEU • PAKET AUS DEFINITION). Selektieren Sie also das entsprechend erstellte Paket (Abbildung 16.68).

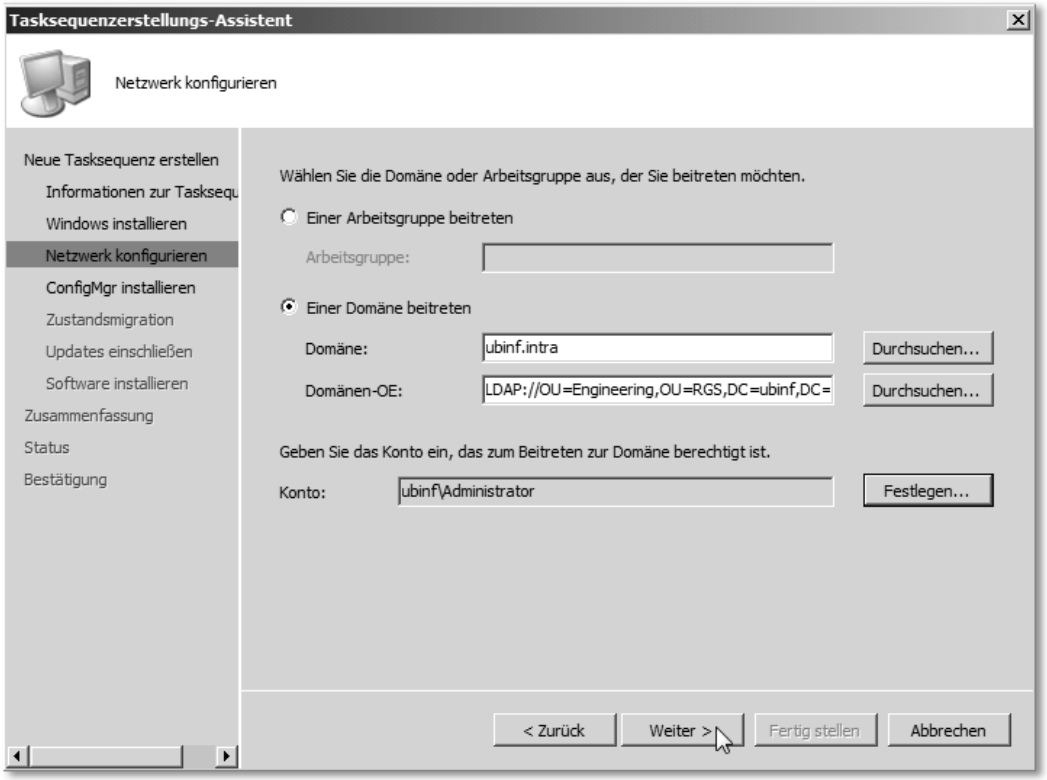


Abbildung 16.67 Der neu installierte PC kann automatisch einer Domäne beitreten.

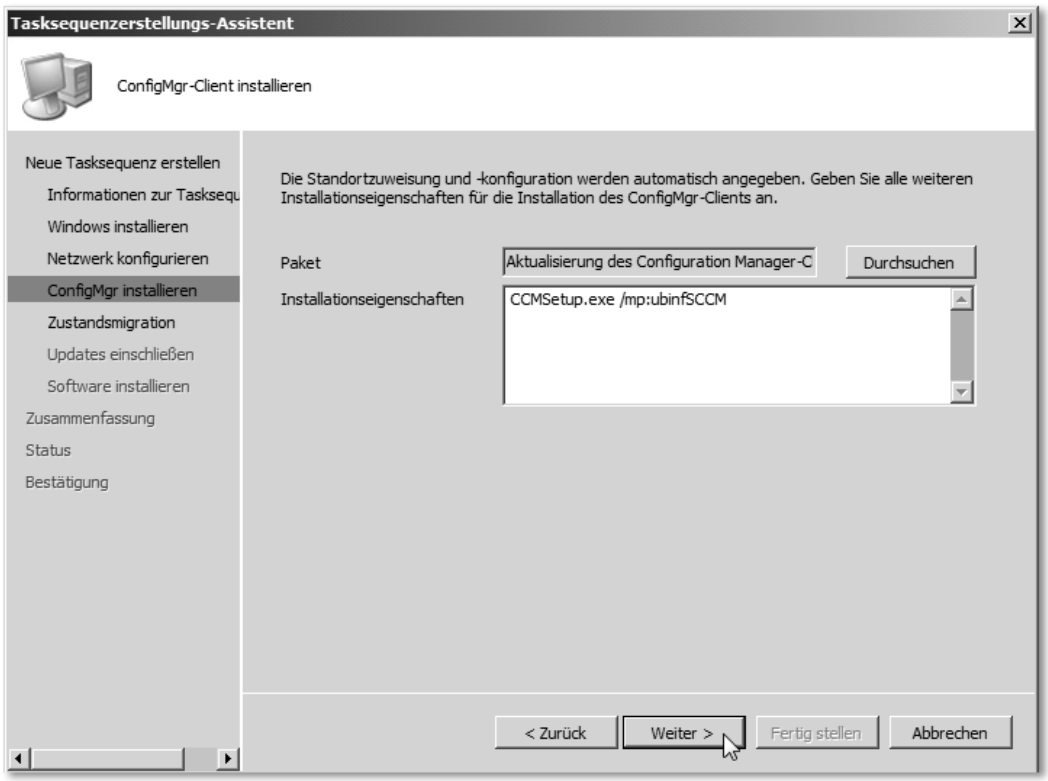


Abbildung 16.68 Hier wählen Sie ein Paket aus, das den Configuration-Manager-Client installiert.

In Abbildung 16.69 sehen Sie die Einstellungen für die Zustandsmigration. Diese Möglichkeit werden Sie verwenden, wenn in Ihrer Organisation keine servergespeicherten Profile (*Roaming Profiles*) verwendet werden und für einen bestehenden Benutzer ein neuer PC aufgesetzt oder auf dem vorhandenen PC das Betriebssystem neu installiert oder aktualisiert werden soll.

Die Idee dahinter ist, dass der Configuration Manager zunächst die ausgewählten Informationen (Benutzereinstellungen, Netzwerkeinstellungen, Windows-Einstellungen) erfasst und dann auf das neu installierte Betriebssystem überträgt.

Hinweis

Das *User State Migration Tool*, das hinter dieser Funktion steckt, wird in Abschnitt 6.13 ausführlich vorgestellt.

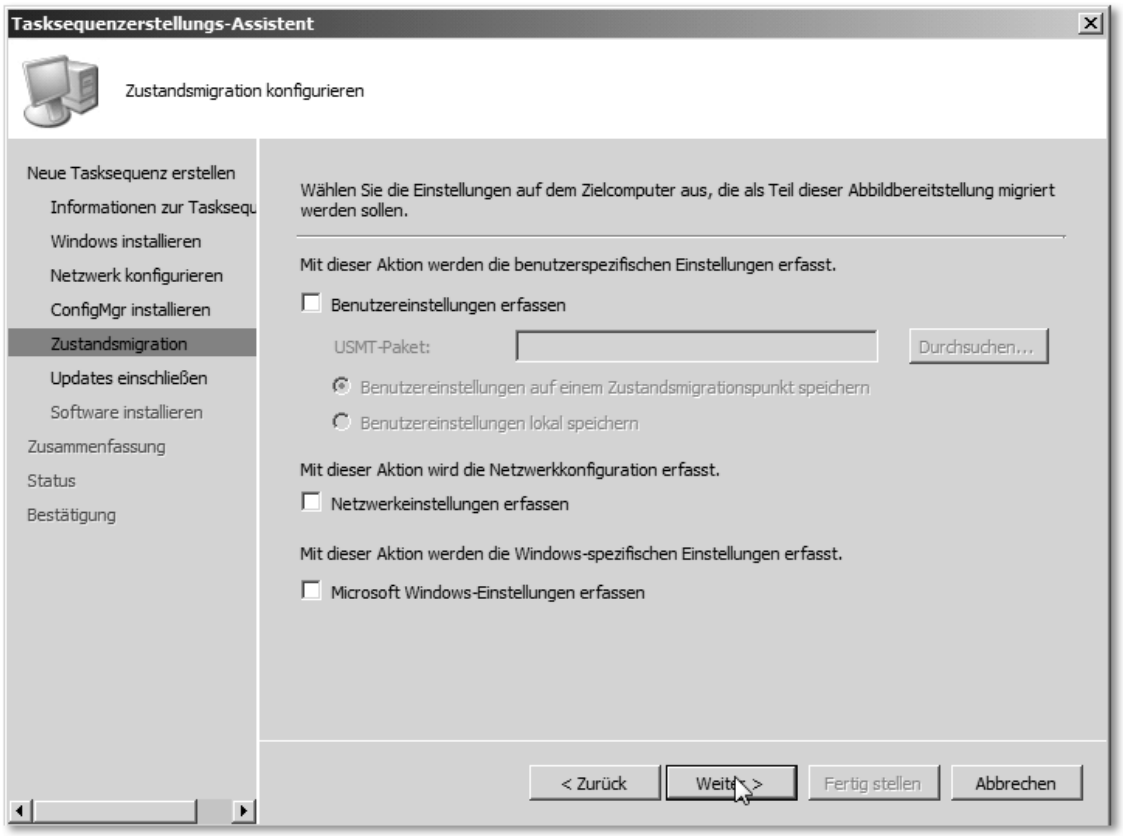


Abbildung 16.69 Falls ein bestehender PC übertragen werden soll, können Sie dies auf der Dialogseite »Zustandsmigration« konfigurieren.

Die letzte Dialogseite dient zur Konfiguration weiterer zu installierender Softwarepakete, die Sie aus der Menge der im Configuration Manager definierten Softwareverteilungspakete auswählen können (Abbildung 16.70). Dieses Feature ermöglicht beispielsweise folgende Vorgehensweise:

- Sie entwickeln ein Betriebssystem-Image für die gesamte Organisation. Der zugrunde liegende Referenz-PC enthält keine weiteren Softwarepakete oder tatsächlich nur solche, die wirklich jeder Anwender erhält.
- Dann erstellen Sie mehrere Tasksequenzen für die unterschiedlichen Abteilungen. Die Tasksequenzen unterscheiden sich in den Softwarepaketen, die im Rahmen dieses Vorgangs installiert werden:
  - PCs für den Vertrieb erhalten das *Office*-Paket, den Client für das CRM-System und *Microsoft MapPoint* für die geografische Analyse von Kundenpotenzialen.
  - PCs für die Buchhaltung werden mit dem *Office*-Paket, dem Client für die Finanzbuchhaltung und einigen Werkzeugen für die Finanzanalyse ausgerüstet.

Auf diese Weise ist es möglich, dass Sie nur ein Image pflegen und trotzdem vollautomatisch unterschiedliche Konfigurationen erstellen können.

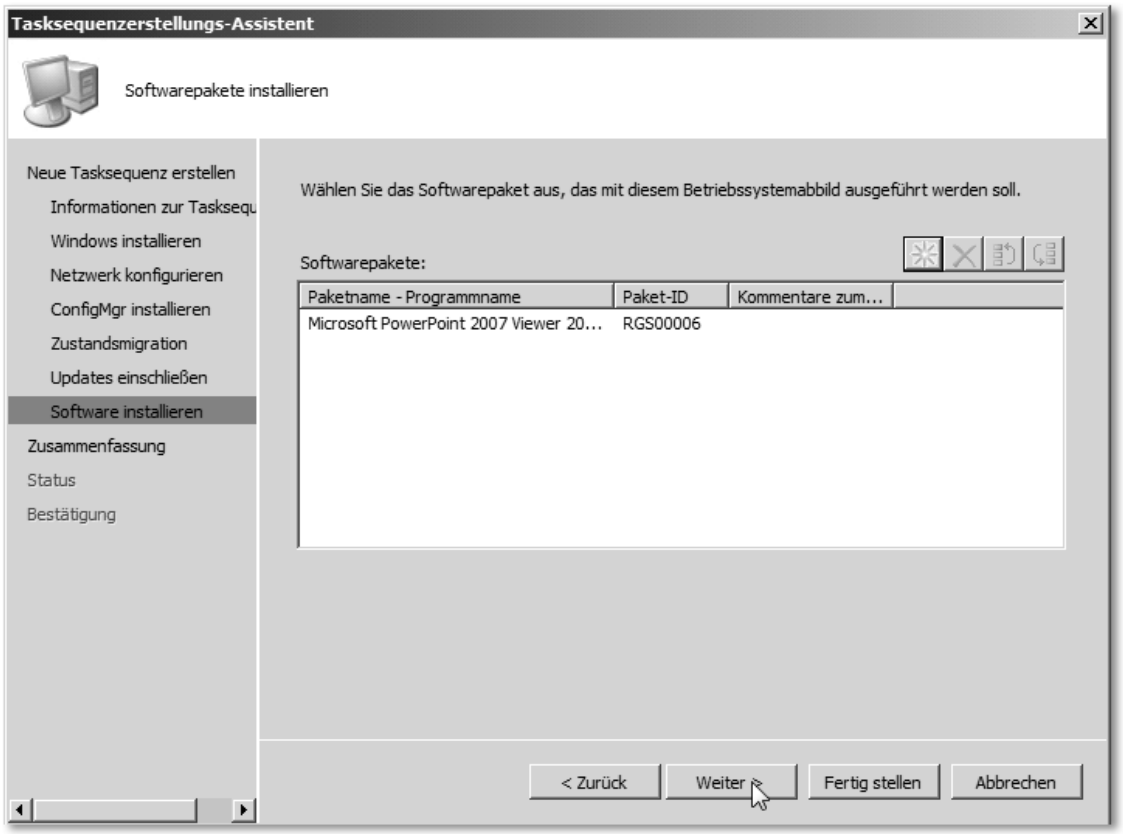


Abbildung 16.70 Ist das Betriebssystem-Image ausgerollt, können Sie direkt noch Softwarepakete nachschieben.

Wenn der Assistent die Tasksequenz erstellt hat, sollten Sie diese im Tasksequenz-Editor öffnen (Abbildung 16.71):

- Sie werden die einzelnen zuvor konfigurierten Schritte als Aufgabenschritte im Tasksequenz-Editor wiederfinden.
- Der erste Eintrag, nämlich NEUSTART MIT WINDOWS PE AUSFÜHREN, kann gelöscht werden, wenn Sie den Bootvorgang aus dem Netz manuell initiieren. Dieser Punkt macht dann Sinn, wenn die Tasksequenz einem bestehenden PC zugewiesen wird, der Configuration-Manager-Client ist. Dieser wird dann Windows PE booten und sich sozusagen selbst neu installieren – das ist beispielsweise praktisch bei Betriebssystem-Upgrades oder wenn ein PC »strubbelig« geworden ist und neu aufgesetzt werden soll.

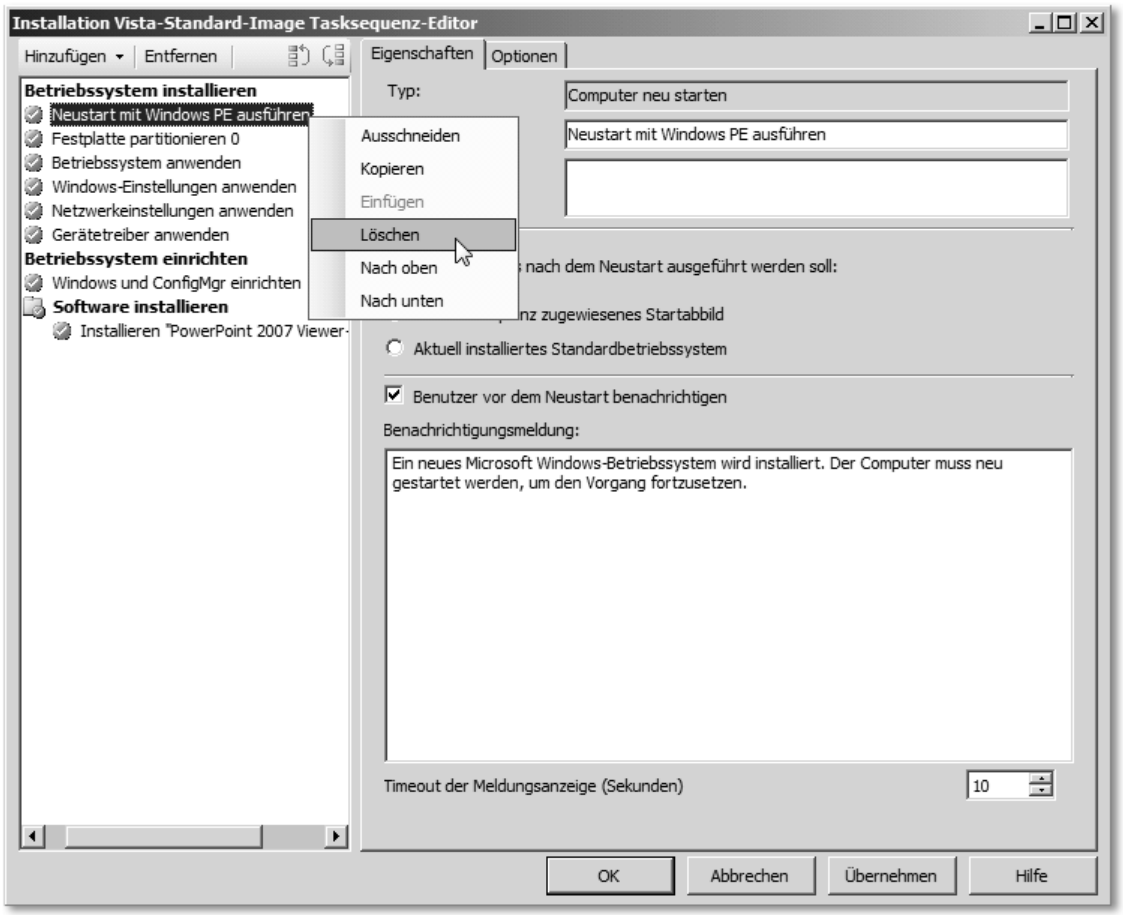


Abbildung 16.71 Die erzeugte Tasksequenz kann bearbeitet werden. Wenn ein PXE-Boot durchgeführt wird, ist der erste Eintrag überflüssig und wird entfernt.

Computer importieren und Ankündigung erstellen

Wie üblich muss die Tasksequenz angekündigt werden. Beachten Sie, dass neue PCs, also solche, die dem Configuration Manager bislang unbekannt sind, importiert werden müssen. Diesen Aspekt habe ich bereits im Zusammenhang mit dem Referenz-PC besprochen (siehe Abbildung 16.44ff.). Das Erstellen der Ankündigung können Sie im Kontextmenü der Tasksequenz initiieren (Abbildung 16.72).

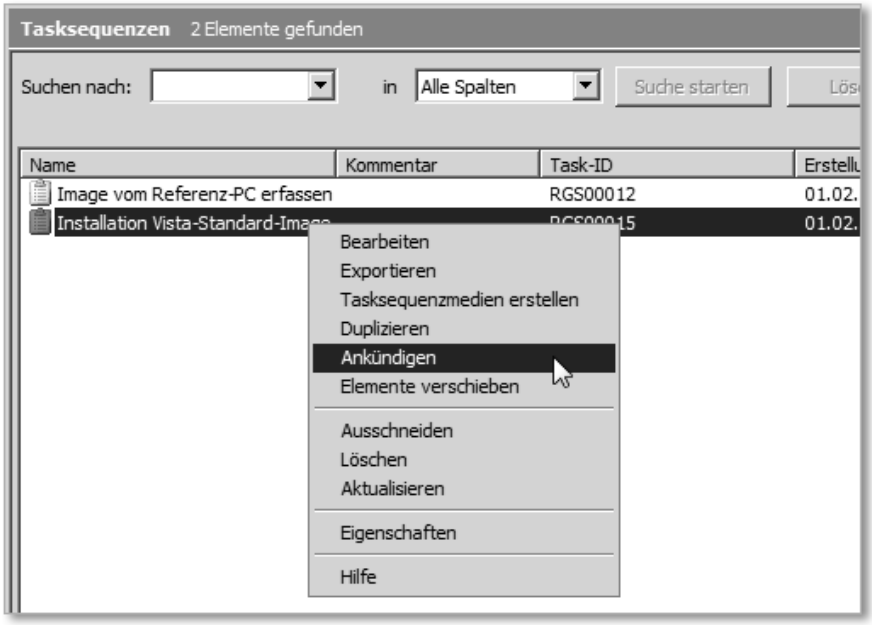


Abbildung 16.72 Nicht vergessen: Die Tasksequenz muss angekündigt werden!

Netzwerkboot durchführen und Image ausrollen

Zum Schluss möchte ich Ihnen noch das Ergebnis der Bemühungen vorführen. Wenn der PXE-Bootvorgang durchgeführt worden ist, werden die in der Tasksequenz definierten Schritte abgearbeitet (Abbildung 16.71). Wenn das Image übertragen ist, wird der Rechner neu gestartet. Da der Referenz-PC mit SYSPREP behandelt worden ist, wird der Neustart genauso ablaufen, wie es bei einem frisch von der CD/DVD installierten Betriebssystem der Fall wäre – die Ausgabe aus Abbildung 16.73 dürfte Ihnen bekannt vorkommen.

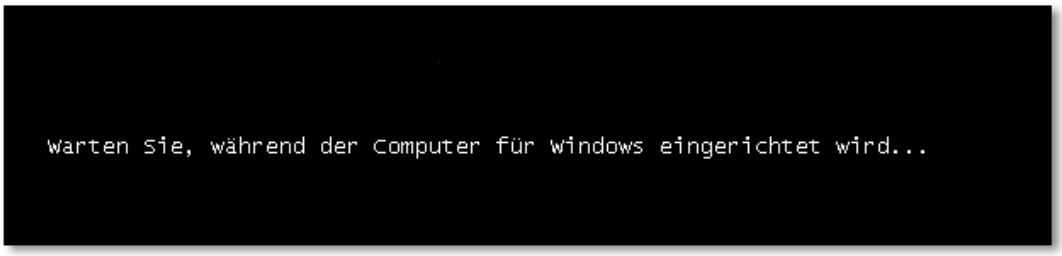


Abbildung 16.73 Wenn das mit SYSPREP behandelte Betriebssystem startet, verhält es sich so wie bei einer frischen Installation.

Dank SYSPREP und den Angaben, die Sie im Configuration Manager gemacht haben, wird der installierte PC den richtigen Namen tragen, Mitglied der Domäne sein und vieles andere mehr (Abbildung 16.74). Weiterhin werden der Configuration-Manager-Client und die sonstigen vorgegebenen Softwarepakete installiert worden sein – ein fertiger PC eben.

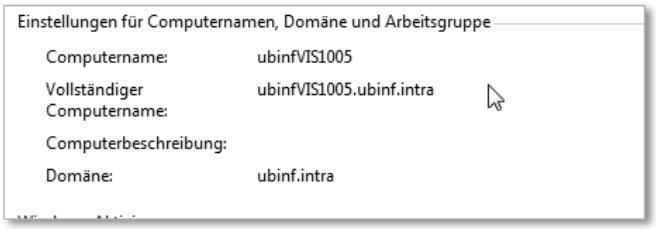


Abbildung 16.74 Ein Screenshot aus der Systemübersicht des neuen Clients: Der PC hat den richtigen Namen und ist Domänenmitglied.

16.6 Anwendersupport

Auch wenn die PC-Systeme perfekt gepflegt und mit der aktuellen Software ausgestattet sind, wird es hin und wieder Situationen geben, in denen Support erforderlich wird. Für diese gibt es prinzipiell drei Gründe:

- Der Anwender hat Probleme bei der Bedienung der Software, wobei kein technisches Problem vorliegt.
- Es gibt Fehler auf dem System.
- Das System ist zwar nicht in einer Fehlersituation, es gibt aber Anomalien, beispielsweise miserable Performance.

Zur Kategorie *Anwendersupport* würde ich im weiteren Sinne die Funktionen zählen, die hilfreich sind, wenn ein Benutzer anruft und Hilfe erbittet. Hierzu zählt natürlich einerseits die Fernsteuerung, mit der sich ein Helpdesk-Mitarbeiter direkt auf den PC aufschalten kann, andererseits würde ich dazu auch die Werkzeuge zählen, die den Helpdesk schnell und einfach mit Daten über den Systemzustand versorgen. Warum? Darum: Meldet ein Benutzer beispielsweise, dass er plötzlich nicht mehr drucken kann, könnte die Ursache darin bestehen, dass der Plattenplatz auf dem Spool-Datenträger (im Allgemeinen ist das Laufwerk *C:*) nur noch wenige Kilobyte beträgt. Dies können Sie sehr einfach mit der WINDOWS-SYSTEMDIAGNOSE überprüfen. Abbildung 16.75 zeigt das Kontextmenü eines Computerobjekts, wobei die im Supportfall hilfreichen Werkzeuge aufgeklappt sind.

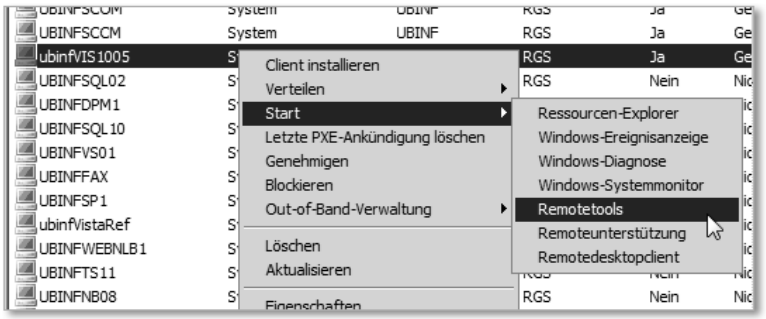


Abbildung 16.75 In einem Computerobjekt können diverse Aktionen gestartet werden.

16.6.1 Fernsteuerung

Der Klassiker für die Anwenderunterstützung ist ohne Zweifel die Fernsteuerung. In der Tat macht dieses Hilfsmittel Sinn, denn bevor ein Anwender dem Kollegen vom Helpdesk sein Problem mit Worten erklärt hat, können unter Umständen einige Minuten vergangen sein – ohne Garantie, dass das Problem dann wirklich verstanden wurde. »Mal eben schnell draufschauen« ist am einfachsten mit der Fernsteuerung zu machen. Selbst wenn die Benutzer im Helpdesk in einem Gebäude sitzen, ist der Einsatz der Fernsteuerung sinnvoll – ansonsten ist ein Großteil der Helpdesk-Mitarbeiter damit beschäftigt, im Haus herumzulaufen.

Die Funktion der Fernsteuerung wird clientseitig durch den *Remotesteuerungs-Agenten* übernommen. Unter diesem Begriff finden sich in der Standortkonfiguration einige Konfigurationsmöglichkeiten. Da es keinen »Stealth-Modus« geben darf, bei dem jemand ungefragt den Bildschirm des Benutzers beobachten könnte, muss das System so konfiguriert sein, dass der Anwender zunächst um Erlaubnis gefragt werden muss.

Wenn der Administrator also die Fernsteuerungssitzung beginnt (Abbildung 16.75), wird er zunächst eine Meldung sehen, in der ihm mitgeteilt wird, dass die Erlaubnis des Benutzers eingeholt wird (Abbildung 16.76). Abbildung 16.77 zeigt den Vorgang aus Anwender-Sicht: Der Anwender muss dem Helpdesk-Mitarbeiter die Remotesteuerung erlauben.

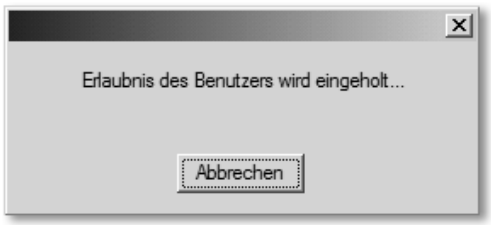


Abbildung 16.76 Wenn ein Helpdesk-Mitarbeiter eine Remotesitzung starten möchte, muss er zunächst auf die Freigabe durch den Benutzer warten.

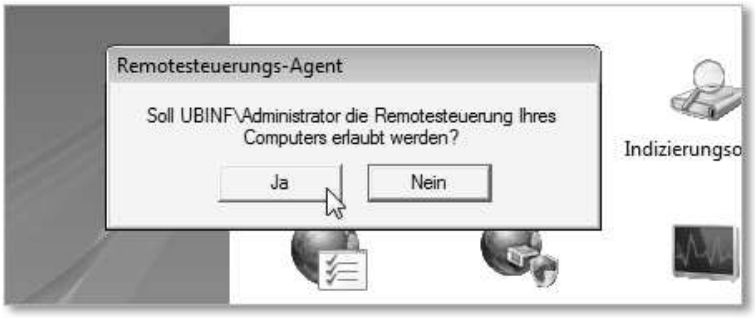


Abbildung 16.77 Aus Benutzersicht sieht es in diesem Moment so aus.

Es gibt noch folgende Aspekte zu erwähnen:

- Je nach Konfiguration wird der Benutzer optisch (durch ein kleines Symbol in der Taskleiste, das Sie in Abbildung 16.78 sehen) und optional akustisch benachrichtigt, wenn die Remotesteuerung aktiv ist.
- Die Remotesteuerung kann nur von Helpdesk-Mitarbeitern initiiert werden, die direkt oder indirekt (Gruppenmitgliedschaft) in der Konfiguration des Remotetoolsclient-Agenten hinterlegt sind.
- Der Start und das Ende der Fernsteuerungssitzung werden protokolliert, sodass diese im Zweifelsfall auch nachvollziehbar sind.

Abbildung 16.78 Hier sehen Sie die laufende Remotesitzung aus Sicht des Helpdesk-Mitarbeiters. Beachten Sie auch das Fernsteuerungssymbol in der Taskleiste (in der Nähe der Uhrzeit).

Hinweis

Damit die Fernsteuerung funktioniert, müssen einige Löcher in die Windows-Firewall gebohrt werden – sofern diese denn aktiv ist.

16.6.2 Sonstige Hilfsmittel

Ein Administrator kann sich auf zwei Arten einen Überblick über die installierte Hard- und Software verschaffen:

- Er kann mit dem *Ressourcen-Explorer* arbeiten, was übrigens in Abschnitt 16.3.2 beschrieben ist.
- Er kann die *Windows-Diagnose* aufrufen (Abbildung 16.79).

Der Unterschied zwischen diesen beiden Möglichkeiten ist in erster Linie, dass der Ressourcen-Explorer ein Offline-Werkzeug ist (sprich: Daten aus der Configuration-Manager-Datenbank anzeigt), während die Windows-Diagnose »online« auf das System schaut. Da das Hardware-Inventar standardmäßig nur einmal pro Woche aktualisiert wird, kann man sich auf solche Parameter wie den freien Festplattenplatz nur begrenzt verlassen.

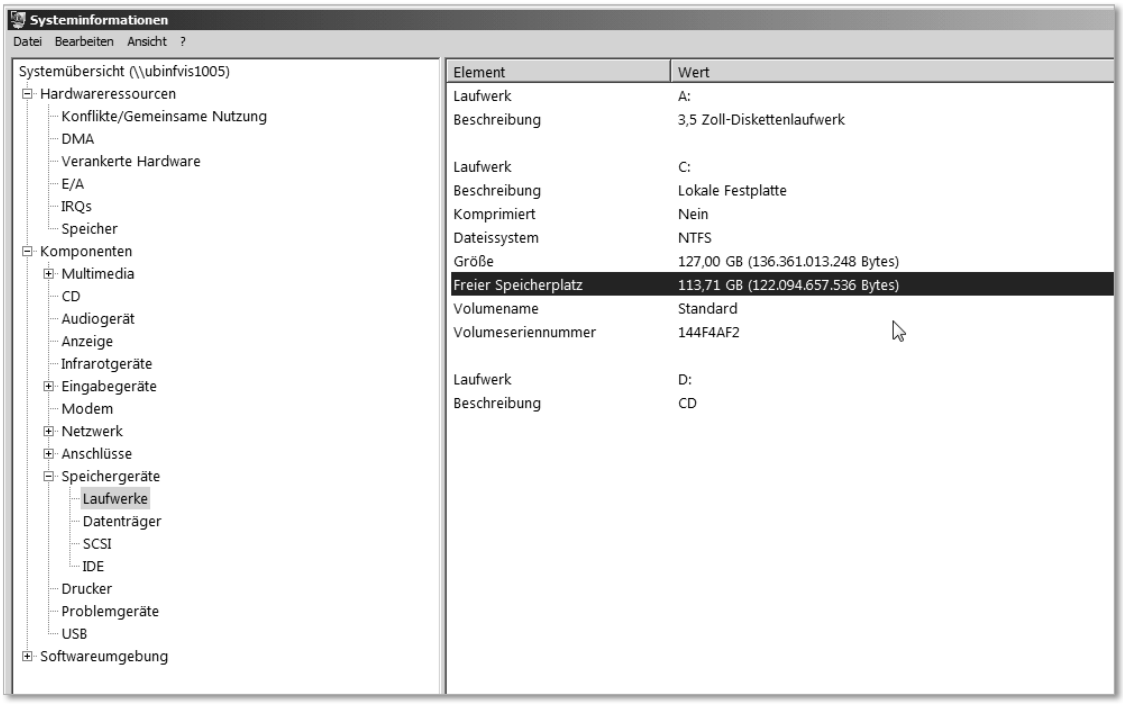


Abbildung 16.79 Für einen Echtzeit-Blick auf ein System eignet sich die Windows-Diagnose.

Ansonsten kann man die Ereignisanzeige und den Systemmonitor (zur Performance-Aanalyse) direkt aus dem Kontextmenü eines Computerobjekts starten.

16.7 Sonstige Funktionen des Configuration Managers

Zunächst werden die Verteilung von Software und Betriebssystemen sowie die Verwaltung des Inventars die Gründe sein, derentwegen der Configuration Ma-

nager beschafft, implementiert und betrieben wird – daher habe ich diese auch im Detail vorgestellt, damit Sie sich ein Bild von der Arbeit mit dieser Software und deren Möglichkeiten machen können.

Wenn Sie die Baumansicht der Configuration-Manager-Konsole anschauen, werden Sie etliche Punkte entdecken, die bislang unerwähnt geblieben sind (Abbildung 16.80). Einige Beispiele:

- Der Configuration Manager verfügt über eine Funktion für SOFTWAREUPDATES. Das ist letztendlich eine Erweiterung für den altbekannten WSUS.
- Mit der VERWALTUNG GEWÜNSCHTER KONFIGURATIONEN können Sie sicherstellen, dass es auf verwalteten Systemen nur den Regeln entsprechende Konfigurationen gibt. Sollte es Verstöße geben, werden Sie benachrichtigt.
- Mit der SOFTWAREMESSUNG können Sie sich ein Bild darüber machen, wie oft bestimmte Softwareprodukte aufgerufen werden. Typisches Beispiel: 300 Benutzer haben angekreuzt, dass unbedingt *Visio* in der neuen Version benötigt wird. Im Unternehmen ist dieses Programm in der vorhandenen Version aber im vergangenen Jahr nur 17-mal gestartet worden – wird *Visio* also wirklich dringend gebraucht?

An dieser Stelle sei noch erwähnt, dass Sie den Gesundheitszustand des Configuration-Manager-Systems unterhalb von SYSTEMSTATUS • STANDORTSTATUS einsehen können. Dort erhalten Sie auch detaillierte Protokolle.

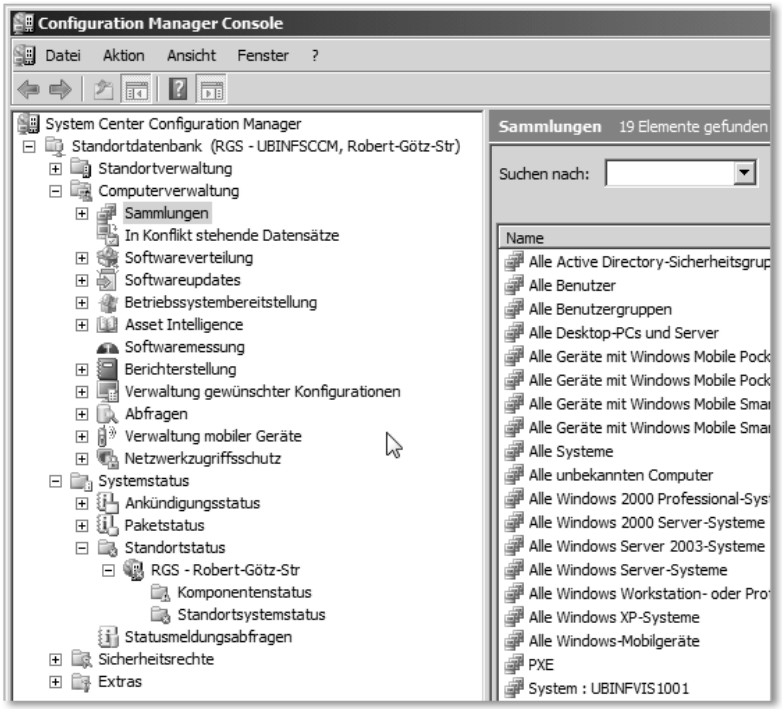


Abbildung 16.80 Der Configuration Manager kann mehr, als »nur« Software und Betriebssysteme zu verteilen.

Ich hatte eingangs bereits erwähnt, dass der Configuration Manager eines der komplexesten Microsoft-Produkte ist. Wenn Sie die Vielfalt an Möglichkeiten betrachten (Abbildung 16.80), werden Sie verstehen, warum das so ist. Dabei wäre anzumerken, dass die Komplexität nicht nur aufgrund der Vielfalt entsteht, sondern weil jedes einzelne Themengebiet in sich recht komplex ist.

Ich würde diese Komplexität übrigens nicht als Nachteil ansehen – im Gegenteil, das Produkt kann eben auch sehr viel. Man muss sich allerdings schon mit dem Thema beschäftigen.

Index

.NET
  CardSpace 106
  WCF 106
  Windows Communication Foundation 106
  Windows Presentation Foundation 106
  Windows Workflow Foundation 106
  WPF 106
  WWF 106
.NET Compact Framework 98
.NET Framework 93, 98
.osdx-Datei 705
6to4 647

A

ACT 351
Activation Count 330
Active Directory-Domänendienste
  Administrative Vorlagen 414
Active Directory-Zertifikatdienste 109
  AD CS 109
  Anwendungsrichtlinien 140
  Anwendungsszenarien 109
  Architekturen 149
  Auto Enrollment 655
  Clientsicht 129
  Doppelte Vorlage 137
  Enterprise-Zertifizierungsstelle 121
  Erweiterte Zertifikatsanforderung 146
  Gültigkeit des Stammzertifizierungsstelle 125
  Installation 119
  Intermediate CA 148
  Issuing CA 149
  Mehrstufige Architekturen 146
  Public Key Infrastructure 119
  Rollen 147
  Root CA 122, 147
  Sperrlistenverteilungspunkt 652
  Stammzertifizierungsstelle 147
  Standalone-Zertifizierungsstelle 121
  Subordinate CA 123
  Weboberfläche 143
  Zertifikat anfordern 131
Active Directory-Zertifikatdienste (Forts.)
  Zertifikatdatenbank wiederherstellen 127
  Zertifikatsvorlagen 131, 135
  Zertifizierungspfad 134
  Zertifizierungsstelle 122
AD CS 109
AD-Integration
  BitLocker 611
ADM 438
Administrative Vorlagen 414
ADMX 438
Advanced Group Policy Management 393
  Benutzerberechtigungen 403
  Installation 394
  Verwendung 398
AGPM 393
Aktivierung 309
  Benachrichtigung 315
  Fazit MAK vs. KMS 337
  Grace Period 312
  Key Management Service 330
  Key Management System 310
  MAK Independent Activate 325
  MAK Proxy Activate 326
  Multiple Activation Key 310
  OOB 312
  OOT 313
  Produktgruppen 311, 333
  Produkt-Keys 309
  Reduced Functionality Mode 315
  Remaining Activations 321
  RFM 315
  slmgr.vbs 323
  VAMT 318
  VAMT, Clients konfigurieren 319
  Volume Activation 2.0 311
  Volume Activation Management Tool 318
  Zeitfenster 312
Aktivierung → Produktaktivierung
Aktivierung → Volumenlizenzen
AMD-V 372
Anabasis 17
Ankündigungen 733
Antwortdatei 192, 242

Anwendersupport 787
Anwendungsidentität 581
Anwendungsserver
DirectAccess 669
Anycast 77
Anzeigesprachen installieren 719
Application Compatibility Toolkit 351
Analysieren 360, 364, 365
Community-Informationen 360
Daten sammeln 355
Datenübertragung 363
Developer and Tester Tools 366
eigene Analysen durchführen 365
Installation 352
Probleme, automatisch ermittelte 364
Application Compatibility Toolkit → ACT
Application Platform Optimization 52
Application Virtualization 389
Applikationen 351
Applikationskompatibilität 351, 360, 364, 365
XP Mode 371
AppLocker 579
Ausführbare Regel 585
Beispiel 581
DLL 585
Editionen 581
Erzwingung konfigurieren 586
Gruppenrichtlinien 593
Konfiguration 581
Regeln automatisch generieren 588
Regeln erstellen 588
Regeln manuell erstellen 591
secpol.msc 581
Skriptregel 585
Standardregeln erzeugen 583
Voraussetzungen 581
Windows Installer-Regel 585
App-V 389, 391
Arbeitswelt, mobile Geräte in der 636
ASP.NET Runtime 98
Asset Inventory Service 393
Ausführbare Regel 585
Auto Enrollment 655
Automatische Genehmigung
WSUS 505
Automatische Namensvergabe 249
Automatischer Modus (VPN) 177
autounattend.xml 200

B

Benutzerkonfiguration
Gruppenrichtlinien 413
Benutzerkontensteuerung 595
Benutzerkontensteuerung → User Account Control
Benutzerspezifische GPOs 430
Berechtigungssatz 104
Berichte 738
WSUS 513
Betriebssystem verteilen 763
Betriebssystemverteilung
System Center Configuration Manager 727
Better Together 47
Bibliotheken 709, 714
Bing 708
BitLocker 597
AD-Integration 611
aktivieren 620
Data Recovery Agent 629
Data Recovery Agents 614
Datenwiederherstellungs-Agenten 629
Datenwiederstellungs-Agenten 614
DRA 614, 629
Edtionen 598
einrichten 600
Festplattenkonfiguration 599
Gruppenrichtlinien 612
Kennwortwiederherstellungs-Viewer 623
Schema-Erweiterung 612
TPM initialisieren 616
TPM-Modul 598
Trusted Platform Module 598
Voraussetzungen 598
Wiederherstellen 622
Wiederherstellungsschlüssel 600
BitLocker To Go 598
BitLockerToGo.exe 609
Editionen 598
einrichten 605
Kennwort vergessen 626
Lesetool 609
Nicht-Windows-7-PC 609
Wiederherstellungsschlüssel 605
BitLocker To Go-Lesetool 609
BitLocker-Kennwortwiederherstellungs-Viewer 623

BitLockerToGo.exe 609
boot.wim 206
BranchCache 681
Clients konfigurieren 691, 696
Editionen 683
Funktionsweise 683
Gehosteter Cache 685
Hosted Cache 694
Server konfigurieren 688, 694
Verteilter Cache 683
Voraussetzungen 682
Brandbekämpfung 50
Business Productivity Infrastructure Optimization 52
Business Value 25

C

CALs 68
CardSpace 106
CASpol 102
Clientagenten 737
Clienthardwarefilter 284
Clientinstallationsmethoden 736
Client-Management 727
CMAK 179
Code Access Security 102
Code Access Security → CASpol
Codegruppe 104
Codesignatur 115
Common Language Runtime 97
Computerkonfiguration 413
Confirmation ID 327
Connection Manager Administration Kit 179
Core Infrastructure Optimization 52
Core IO 52

D

DaRT 391
Data Recovery Agent 629
Data Recovery Agents
BitLocker 614
Dateifreigabe indizieren 711
Datengrab 701
Datenwiederherstellungs-Agenten 629
BitLocker 614
Deployment 62, 185
Antwortdatei 192, 242
autounattend.xml 200
boot.wim 206
Clienthardwarefilter 284
Deployment Image Servicing and Management Tool 268
Deployment-Prozess 189
DISM.exe 268
Domänenbeitritt gelingt nicht 247
Features aktivieren 277
Image-Pflege 267
In-Place-Migration 306
Installation mit Antwortdatei durchführen 200
Installation verallgemeinern 202
Installationsabbildfilter 284
Installationsimage vorbereiten 191, 232
MAC-Adresse 252
Mehrsprachige Umgebungen 725
Mini-Setup (Sysprep) 242
Multicastübertragungen 292
Namensvergabe 249
netbootGUID 253
Packages verwalten 275
Panther-Verzeichnis 202
Pre-Boot Execution Environment 212
Profile 187
Prozess 189
PXE 212, 228
PXE-Antwortrichtlinie 259
PXE-Bootvorgang 224
Re-Imaging-Recht 187
setupact.log 291
Standardisierung 185
Sysprep 202, 209
Testumgebung 190
TFTP 228
Tool zur Abbildverwaltung für die Bereitstellung 268
Treiber 267, 282
Treiber verwalten 272
Treiberpaket hinzufügen 287
UnsecureJoin 244
User State Migration Tool 299
USMT 299
vorab bereitstellen 251
WAIK 185
WDS 211

Deployment (Forts.)
WDS-Startvorgang automatisieren 232
WDSUTIL 253
WIM 191
WIM erzeugen 207
WIM-Image 267
WIM-Image mounten 269
WIM-Image unmounten 279
Windows Automated Installation Kit 185
Windows Imaging Format 191
Windows System Image Manager 192
Windows-Bereitstellungsdienste 211
WinPE-Startimage erzeugen 204
Deployment Image Servicing and Management Tool 268
Deployment-Prozess 189
Desktop Optimization Pack 387
Desktop-Suche 702
Developer and Tester Tools 366
DHCP
NAP 529
DHCP-Server
NAP (Vorbereitung) 542
Diagnostic and Recovery Toolset 391
DirectAccess 643
6to4 647
Anwendungsserver 669
Clientperspektive 676
DirectAccess-Server 662
DirectAccess-Server konfigurieren 666
DNS-Registrierung 678
DNS-Server 652, 667
Domänencontroller 652
Editionen 644
Ersteinrichtung 664
Funktionsweise 644
globalqueryblocklist 652
Gruppenrichtlinien 672
installieren 663
IP-HTTPS 648, 666
IP-Konfiguration 676
IP-Konfiguration aktualisieren 658
IPSec 649, 672
IPv6 646
ISATAP 647, 658
Monitoring 671
Name Resolution Policy Table 649
Namensauflösung 649
NAT 647
DirectAccess (Forts.)
NAT-PT 647
Network Location Server 651, 667
Network Locator Server 661
Netzwerkstandorte 663
NRPT 649, 677
PKI einrichten 652
Remoteclients 664
Sicherheitsgruppe 658
Sperrlisten-Verteilungspunkt 652
Technologiegrundlagen 646
Teredo 647
Tunnelmechanismen 646
Verwaltungskonsole 663
Voraussetzungen 644
Vorbereitende Maßnahmen 652
Zertifikate 651
Zertifikate anfordern 655
DISM.exe 268
DLL-Hölle 390
DNS-Registrierung
DirectAccess 678
Domänenbeitritt gelingt nicht 247
DRA
BitLocker 614, 629
DWORD 91

E

EAP 166
Editionen 65
BitLocker 598
BranchCache 683
DirectAccess 644
Multilanguage 719
Vergleichstabelle 67
Einstieg 57
Einwahlberechtigung 164
Encrypting File System 117
Enterprise Desktop Virtualization 388
Enterprise Edition 66
Ermittlungsmethoden 734
Erzwingung konfigurieren (AppLocker) 586
Erzwingungsclient 522
Extended Supportphase 46
Extensible Authentication Protocol 166

F

Features aktivieren 277
Fernsteuerung 788
Festplattenkonfiguration
BitLocker 599
Filter
Gruppenrichtlinien 426
FPP 189
Fremdsprachen 717
Full Packaged Product 189
Funktionsweise
BranchCache 683
DirectAccess 644
Key Management Service 329

G

Gateway-Architektur 153
Gehosteter Cache 685
Gemeinsamer geheimer Schlüssel 525
Geräte 107
Global Unicast Addresses 78, 81
globalqueryblocklist 652
Grace Period 312
Gründe für ein neues Betriebssystem 35
Bedienung 43
Deployment 40
Funktionalität 39
Management 40
Mobile Szenarien 44
Moderne Plattform 35
Sicherheit 42
Softwarearchitektur 37
Support-Situation 45
Gruppen
WSUS 502
Gruppenrichtlinien 409
Abarbeitungsreihenfolge 427
ADM 438
Administrative Vorlagen 414
ADMX 438
Advanced Group Policy Management 393
Anwendungsbeispiel 410
AppLocker 593
bearbeiten 450
Benutzerkonfiguration 413
Benutzerspezifische GPOs 430
BitLocker 612
Gruppenrichtlinien (Forts.)
Computerkonfiguration 413
DirectAccess 672
Filter 426
gPLink 418
Gruppenrichtlinienergebnisse 464
Gruppenrichtlinienmodellierung 459
Gruppenrichtlinienobjekt-Editor 412
Gruppenrichtlinienverwaltung 412
Lokale GPOs 429
Lokales Richtlinienobjekt 429
Loopback-Verarbeitung 473
Preferences 474
Sicherheit 424
Sichern 436
Softwareeinstellungen 413
Softwareverteilung 470
Starter-Gruppenrichtlinienobjekte 432
Suche 704
SYSVOL-Verzeichnis 416
Vererbung 420
Verknüpfungen 456
Verteilung 415
Voreinstellungen 474
Vorrang 424
Windows-Einstellungen 414
Windows-Firewall 570
WMI-Filter 466
WSUS 509
Zentraler Speicherort 441
Zuweisen 450

H

Hardware 48
HKEY_CLASSES_ROOT 89
HKEY_CURRENT_CONFIG 89
HKEY_CURRENT_USER 89
HKEY_LOCAL_MACHINE 89
HKEY_USERS 89
Home Basic Edition 66
Home Premium Edition 66
Hosted Cache 694
http mit SSL-Verschlüsselung 111

I

IKEv2 152, 697
Image-Pflege 267

IMAGEX.exe 205
Infrastrukturoptimierung 50
In-Place-Migration 306
Installation ID 327
Installation verallgemeinern 202
Installationsabbild 219
Installationsabbildfilter 284
Installationsimage vorbereiten 191, 232
Integritätsrichtlinien 521, 539
Intel VT 372
Intermediate CA 148
Inventar 738
Inventarisierung 727
IP-HTTPS 648, 666
IPSec 168
DirectAccess 649, 672
IPv4 73
IPv6 73
Abschalten 83
Adressierung 75
Adresssyntax 76
Adresstypen 77
DirectAccess 646
Global Unicast Addresses 81
Link-Local Addresses 78
Stateful 82
Stateless 82
Unique Local Addresses 80
Unterschiede zu IPv4 74
Vergabe von Adressen 82
IPv6 → Protokolle
IP-Verschlüsselung 116
ISATAP 647, 658
Issuing CA 149

K

Kein Vorrang 425
Kennwortwiederherstellungs-Viewer 623
Key Management Service 329
Funktionsweise 329
Installation 334
MAK vs. KMS 337
Produktgruppen 333
Key Management System 310
Zeitfenster 314
KMS
Activation Count 330
KMS → Key Management System
Kompatibilität
Applikationen 351
Kosten
Mobilität 642
Kunaxa 17

L

L2TP 152, 168
Language Interface Pack 718
Language Pack 718
Link-Local Addresses 77, 78
LIP → Language Interface Pack
Lizenzen 65
Lizenzverträge 69
LoadState.exe 299
Lokale GPOs 429
Lokale Profile 84
Lokales Richtlinienobjekt 429
Loopback-Verarbeitung 473
Loopback-Verarbeitungsmodus 473

M

MAC-Adresse 252
Mainstream Support 46
MAK → Multiple Activation Key
manage-bde 629
Managed Applications 97
Managed Web Applications 98
Management 63
MDOP → Microsoft Desktop Optimization Pack
MED-V → Microsoft Enterprise Desktop Virtualization
Mehrsprachige Umgebungen 717
Deployment 725
Profile 725
Mehrstufiges NAP-Konzept 524
Messbarkeit 634
Microsoft Desktop Optimization Pack 387
Advanced Group Policy Management 393
Application Virtualization 389
App-V 389
Asset Inventory Service 393
Diagnostic and Recovery Toolset 391
Enterprise Desktop Virtualization 388
MED-V 388

Microsoft Desktop Optimization Pack (Forts.)
System Center Desktop Error Monitoring 406
Microsoft Desktop Optimization Pack → MDOP
Microsoft Enterprise Desktop Virtualization 372, 388
MigApp.XML 302
MigDocs.XML 302
MigUser.XML 302
Mini-Setup (Sysprep) 242
Mobile Broadband 698
Mobile Clients 631
Mobilität 61, 631
Gedanken zum Thema 632
Kosten 642
Monitoring
DirectAccess 671
MUI → Multilingual User Interface Pack
Multicast 77
Multicastübertragungen 292
Multilanguage
Editionen 719
LIP 718
MUI 718
Servergespeicherte Profile 86
Sprache installieren 719
Voraussetzungen 719
Multilanguage → Sprachen
Multilingual User Interface Pack 718
Multiple Activation Key 310, 323
Aktivieren am PC 323
DNS-Fehlermeldung 323
MAK Independent Activate 325
MAK Proxy Activate 326
VAMT, verwalten mit 321
Zeitfenster 313

N

Name Resolution Policy Table 649
Namensauflösung
DirectAccess 649
Namensvergabe 249
NAP Enforcement Points 516
NAP → Network Access Protection
NAP-Agent 522
NAP-Erzwingungspunkte 516
NAT 647
NAT-PT 647
netbootGUID 253
Network Access Protection 516
Agent 522
Client vorbereiten 522
Clientperspektive 544
DHCP 529
DHCP-Server vorbereiten 542
Funktionsweise 517
Gemeinsamer geheimer Schlüssel 525
Integritätsrichtlinien 539
Kommunikationsvorgänge 520
Mehrstufiges Konzept 524
Netzwerkmonitor 549
Netzwerkrichtlinien 536
Netzwerkrichtlinienserver 520
RADIUS-Proxyserver 527, 530
RADIUS-Remoteservergruppe 527
Systemintegritätsprüfungen 540
Verbindungsanforderungsrichtlinien 535
Network Location Server 667
DirectAccess 651
Network Locator Server 661
Network Policy Server 520
Netzwerkmonitor
NAP 549
Netzwerkrichtlinien 521, 536
Netzwerkrichtlinien- und Zugriffsdienste 154, 515
Netzwerkrichtlinienserver 520
Installation 530
NAP 520
Network Policy Server 520
NPS 520
Netzwerkstandorte
DirectAccess 663
Windows-Firewall 553
Neuerungen im Überblick 59
Deployment 62
Management 63
Mobilität 61
Sicherheit 60
Suche 64
Neuerungen im Überblick → Was ist neu?
NPS → Network Policy Server
NRPT
DirectAccess 649, 677

O

OEM 189
OOB → Out of Box
OOT → Out of Tolerance
opensearch 705
Original Equipment Manufacturer 189
osdx-Datei 705
Out of Box 312
Out of Tolerance 313

P

Packages verwalten 275
Pakete 733
Panther-Verzeichnis 202
Paul Adair 701
PPTP 152, 166
Pre-Boot Execution Environment 212
Preferences
Gruppenrichtlinien 474
Pre-Shared Key 168
Primäre Standorte 729
Produktaktivierung 309
Produktgruppen 311
Aktivierung 333
Produkt-Keys 309
Professional Edition 66
Profil
Windows-Firewall 553
Profile 84, 187
Mehrsprachige Umgebungen 725
Zwischenspeichern 87
Protokolle
IPv4 73
IPv6 73
PSK 168
Public Key Infrastructure 119
PXE 212, 228, 765
Antwortrichtlinie 259
Bootvorgang 224

Q

QWORD 91

R

RADIUS-Proxyserver 527, 530
RADIUS-Remoteservergruppe 527
Recovery Environment 339
Reduced Functionality Mode 315
Registry 89
DWORD 91
QWORD 91
Reifegrade 50
Re-Imaging-Recht 187
Remaining Activations 321
Remote Server Administration Tools 623
Remoteclients
DirectAccess 664
Remoteinstallationsordner 225
Remoteserver-Verwaltungstools 623
Remote-Standorte
Windows-Bereitstellungsdienste 292
Ressourcen-Explorer 742
RFM 315
Roaming Profiles 84
Root CA 147
Routing und RAS 156
RSAT 623
Rückblick
DOS 27
Windows 3.0 28

S

SAM 70
Sammlungen 732
SB 189
ScanState.exe 299
SCCM → System Center Configuration Manager
Schema
BitLocker 612
SCOM 406
Search Federations 705
secpol.msc 581
Secure Socket Tunneling Protocol 171
Security 481
Security Identifier 242
Sekundäre Standorte 729
Servergespeicherte Profile 84
in mehrsprachigen Umgebungen 86
setupact.log 291

SHA 519
Sichere E-Mail 112
signieren 114
verschlüsseln 112
Sicherheit 60, 481
Gruppenrichtlinien 424
WLAN-Access-Point 487
SID 242
Site-Local Addresses 77
Skriptregel 585
slmgr.vbs 323
Smartcard 117
SMS 728
SoftGrid 391
Softricity 391
Software Asset Management 70
Softwarearchitektur 37
Softwareeinstellungen 413
Softwareverteilung 727, 748
Gruppenrichtlinien 470
SoH 519
Special Addresses 78
Sperrlisten-Verteilungspunkt 652
Sprache installieren 719
Sprachen 717
SSoH 519
SSTP 152, 171
Troubleshooting 176
Stammzertifizierungsstelle 147
Standardisierung 185
Standardregeln erzeugen
AppLocker 583
Standorte
System Center Configuration Manager 729
Startabbild 219
Starter Edition 66
Starter-Gruppenrichtlinienobjekte 432
Startpartition 600
Startvorgang automatisieren 232
Stateful 82
Stateless 82
Suchconnector 707
Suche 64, 701
Bibliotheken 709
Bibliotheken anwenden 714
Dateifreigabe indizieren 711
Desktop-Suche 702
Gruppenrichtlinien 704
Suche (Forts.)
Search Federations 705
Suchconnector 707
Support-Situation 45
Sysprep 202, 209
System Builder 189
System Center Configuration Manager 727, 728
Agenten 734
Ankündigung erstellen 759
Ankündigungen 733
Anwendersupport 787
Berichte 738, 744
Betriebssystem verteilen 763
Betriebssystemverteilung 727
Clientagenten 737
Clientinstallationsmethode 736
Ermittlungsmethoden 734
Fernsteuerung 788
Grundprinzipien 729
Inventar 738
Inventarisierung 727
Pakete 733
Paketerstellung 748
primäre Standorte 729
Programm hinzufügen 753
PXE 765
Ressourcen-Explorer 742
Sammlungen 732
sekundäre Standorte 729
Softwareverteilung 727, 748
Standorte 729
Tasksequenz 772
Verteilungspunkt 731
Verteilungspunkte verwalten 755
Verwaltungspunkt 731
System Center Desktop Error Monitoring 406
System Center Operations Manager 406
System Health Agents 519
System Statement of Health 519
Systemintegritätsprüfungen 522, 540
Systempartition 600
SYSVOL-Verzeichnis 416

T

Tasksequenz 772
Technologiegrundlagen 71
.NET Framework 93
Active Directory-Zertifikatdienste 109
DirectAccess 646
Geräte 107
Netzwerk 71
Profile 84
Registry 89
VPN 151
Windows-Funktionen 92
Teredo 647
Terminaldienste
Gruppenrichtlinien 474
Loopback-Verarbeitungsmodus 473
TFTP 219, 228
Tool zur Abbildverwaltung für die Bereitstellung 268
TPM initialisieren 616
tpm.msc 616
TPM-Modul 598
Transition Addresses 78
Treiber 267, 282
verwalten 272
Treibergruppe einrichten 283
Treiberpaket hinzufügen 287
Trusted Platform Module 598, 616
Tunneling-Protokolle 152
Tunnelmechanismen
DirectAccess 646

U

UAC 595
Ultimate Edition 66
UMTS 642
Unicast 77
Unique Local Addresses 78, 80
Unmanaged Applications 97
UnsecureJoin 244
Updates genehmigen 505
USB-Untertützung
Windows Virtual PC 381
User Account Control 595
User State Migration Tool 299
Dateitypen 303
MigApp.XML 302
Was kann migriert werden? 303
User State Migration Tool → USMT
USMT 299

V

VAMT 318
Clients konfigurieren 319
MAK Independent Activate 325
MAK Proxy Activate 326
Manage MAKs 321
Multiple Activation Keys verwalten 321
Remaining Activations 321
Windows-Firewall 319
Verbindungsanforderungsrichtlinien 521, 535
Verbindungs-Manager-Verwaltungskit 179
Verbindungssicherheitsregeln 575
Vergleichstabelle Editionen 67
Versionsnummern 57
Verteilter Cache 683
Verteilungspunkt 731
Verwaltungspunkt 731
Virtual PC 371
Volume Activation 2.0 311
Volume Activation Management Tool 318
Volumenlizenzen
Aktivierung 309
Voraussetzungen
BranchCache 682
DirectAccess 644
Multilanguage 719
Vorinstallierter Schlüssel 168
Vorrang
Gruppenrichtlinien 424
VPN 151
Automatischer Modus 177
CMAK 179
Connection Manager Administration Kit 179
EAP 166
einrichten 159
Einwahlberechtigung 164
Extensible Authentication Protocol 166
Gateway-Architektur 153
IKEv2 152
IPSec 168
L2TP 152, 168

nächste Generation 643
PPTP 152, 166
Pre-Shared Key 168
PSK 168
VPN (Forts.)
Routing und RAS 156
Secure Socket Tunneling Protocol 171
Server, Grundkonfiguration 154
SSTP 152, 171
Technologiegrundlagen 151
Tunneling-Protokolle 152
Verbindungs-Manager-Verwaltungskit 179
Vorinstallierter Schlüssel 168
VPN einrichten 159
VPN-Server, Grundkonfiguration 154
VPN Reconnect 697

W

WAIK 185
DISM.exe 268
Installation 190
WSIM 192
WAN-Miniport-Treiber 152
Wartungsservergruppen 522
Was ist neu? 59
WCF 106
WDS → Windows-Bereitstellungsdienste
WDS-Startvorgang automatisieren 232
WDSUTIL 240, 253
Weboberfläche
Active Directory-Zertifikatdienste 143
Wiederherstellen
BitLocker 622
Wiederherstellungsschlüssel 600
BitLocker To Go 605
WIM 191, 219
Features aktivieren 277
Image mounten 269
Image-Pflege 267
Multicastübertragung 294
Packages verwalten 275
Treiber verwalten 272
unmount 279
WIM erzeugen 207
WIM-Image 267
Windows 1, 2 und 3 26
Windows 2000 Professional 32
Windows 7 XP Mode 91, 371
Windows Automated Installation Kit 185
Windows Communication Foundation 106
Windows Imaging Format 191
Windows Installer-Regel 585
Windows NT 3.1 29
Windows NT 4 30
Windows PE 339
Windows Presentation Foundation 106
Windows RE 339
anpassen 347
Image erstellen 343
Standardfunktionalität 341
Windows-Bereitstellungsdienste 343
Windows RE → Recovery Environment
Windows Server Update Services 489
Automatische Genehmigung 505
Berichte 513
Erstkonfiguration 494
Funktionsweise 490
Gruppen 502
Gruppenrichtlinien 509
Installation 491
Konfiguration 501
Updates genehmigen 505
Updates manuell genehmigen 507
Windows Server Update Services 489
wuauclt 511
Windows System Image Manager 192
Windows Virtual PC 371, 381
Neuerungen 381
USB-Unterstützung 381
VM anlegen 382
Windows Vista 34
Windows Workflow Foundation 106
Windows XP 33
Windows-Bereitstellungsdienste 211
Abbilder hinzufügen 219
Antwortdatei 233
Automatisierung Windows-Setup 242
Bereitstellungsdienste anpassen 239
Bereitstellungsdienstclient automatisieren 233
Erstkonfiguration 215
Installationsabbild 219
Installieren 213
MAC-Adresse 252
Multicastübertragungen 292

Windows-Bereitstellungsdienste (Forts.)
netbootGUID 253
PXE 228
PXE-Antwortrichtlinie 259
PXE-Bootvorgang 224
Remoteinstallationsordner 225
Remote-Standorte 292
Startabbild 219
Startvorgang automatisieren 232
Testdurchlauf 223
TFTP 228
Treiber 267, 282
Treibergruppe einrichten 283
Treiberpaket hinzufügen 287
vorab bereitstellen 251
Voraussetzungen 212
WDSUTIL 253
Windows RE 343
Windows-Setup automatisieren 242
Windows-Einstellungen 414
Windows-Firewall 551
Grundkonfiguration 555
Gruppenrichtlinien 570
Isolierungsregel 576
Netzwerkstandorte 553
Profil 553
Regel aktivieren 563
Regel selbst erstellen 565
Regeln 557
VAMT 319
Verbindungssicherheitsregeln 575
Windows-Funktionen 92
WinPE-Startimage erzeugen 204
WMI-Filter 466
WPF → Windows Presentation Foundation
WSIM → Windows System Image Manager
WSUS → Windows Server Update Services
WWF → Windows Workflow Foundation

X

Xenophon 17
XP Mode 91, 371
AMD-V 372
Applikationen installieren 377
Installation 373
Intel VT 372
XP Mode (Forts.)
Nachteile 380
Startmenü 377
Voraussetzungen 372

Y

YouTube 708

Z

Zeitfenster 312
Zentraler Netzwerkrichtlinienserver 525
Zertifikatdatenbank wiederherstellen 127
Zertifikate
DirectAccess 651
Zertifikatsdienste 109
Zertifikatsvorlagen 131, 135
Zertifizierungspfad 134
Zugriffslizenzen 68